サイバーセキュリティ 2021（案）
（2020 年度年次報告・2021 年度年次計画）

令和３年（2021 年）〇月〇日

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＞

本編

本編

１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

2020 年からの新型コロナウイルス感染症への対応を余儀なくされている中､その結果として、「ニューノーマル」とも呼ばれる新たな生活様式が浸透し、テレワークや ICT 教育、オンライン診療などの取組が加速的に進展しつつある。

例えば、テレワークの普及状況についてみてみると、週１日以上在宅勤務の割合は、2020 年５月をピークに一過的に増加し、以降揺り戻しの動きは見られるものの、新型コロナウイルス感染症の拡大前よりも高い水準で推移している（2020 年３月:8.9%、５月：20.4%、７月：16.9%、10 月：16.0%）[2]。

また、児童生徒の１人１台端末と高速大容量の通信ネットワークを一体的に整備する「GIGA スクール構想」については､当初は 2023 年度までの４年計画で整備を進めていく予定だったが、コロナ禍も踏まえ、スケジュールの大幅な前倒しが行われた。整備された ICT 環境の活用に向け、学校における ICT 環境整備の設計等の支援を行う「GIGA スクールサポーター」や、日常的な教師の ICT 活用の支援等を行う「ICT 支援員」の配置が推進されている。

加えて、オンライン診療をとりまく状況をみると、2020 年４月の厚生労働省の通知[3]により、感染防止のための非常時の対応として､「初診から電話や情報通信機器を用いた診療により診断や処方をして差し支えない」という見解が示されたことを踏まえ、オンライン診療が進展される素地が整いつつある。

このほか、コロナ禍への対応を通じ、新たなサービスの官民での活用も進展している。例えば、新型コロナウイルス感染症陽性者との接触を通知し、保健所における積極的疫学調査を補完するために、新型コロナウイルス接触確認アプリ（COCOA）の利用が推奨されている（2021 年６月 30 日時点でのダウンロード数：2,856 万件）[4]。

かかる環境変化に応じ、政府としては、デジタル社会の形成に向けた司令塔として「デジタル庁」の設置が予定されており､「誰一人取り残さない、人に優しいデジタル化」の実現を目指して「デジタルの活用により、一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」をビジョンに掲げるデジタル改革を推進することとしている。

一方で、こうしたデジタル化の進展に伴い、リスクの変容もみられる。業務、製品・サービスのデジタル化が加速していく中で、テレワーク時にも使用する遠隔接続を悪用した攻撃、クラウドサービスを標的とした攻撃やデジタルサービス連携の間隙を突く攻撃がみられている。クラウドサービスの利用拡大やサプライチェーンが複雑化していく中で、影響が拡大する可能性が懸念されており、従来のサイバーセキュリティ対策の主要な前提ともなっていた「境界型

[2] 国土交通省「令和２年度テレワーク人口実態調査」（2021 年 3 月 19 日）
https://www.mlit.go.jp/report/press/content/001391381.pdf
[3] 厚生労働省「新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いについて」（2020 年 4 月 10 日事務連絡） https://www.mhlw.go.jp/content/R20410tuuchi.pdf
[4] 厚生労働省 HP https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html

セキュリティ」の考え方の限界も顕在化しつつある。

これらの状況を例証するデータとして、遠隔でコンピュータへのアクセスを行うリモートデスクトップに対する攻撃が大幅に増加しており、2020年3月の世界各地でのパンデミック発生に伴うロックダウン前後で顕著な差が出ている（2020年2月：9,310万件 ⇒ 2020年3月：2億7,740万件 ⇒ 2021年2月：3億7,750万件）。また、日本でも同様の傾向がみられる（2020年2月：21.5万件 ⇒ 2021年2月：86.5万件）[5]。

また、クラウドサービスを標的とした攻撃においても、クラウドサービスを狙った攻撃の増加が指摘されている（2020年1月～4月の期間で企業のクラウドサービス利用が50%増加した一方で、クラウドアカウントに対する外部からの攻撃が630%増加している。これら外部からの攻撃の大半はコラボレーションサービスを標的とし、盗取した認証情報を悪用したクラウドアカウントへの大規模な不正アクセスであったとされている）[6]。

こうしたリスクの変容に対し、経済社会全体においても、個々の企業活動においても、デジタル化の進展とあわせてサイバーセキュリティ確保に向けた取組が同時に推進されなければ、デジタル改革の実現はなし得ない。現時点では、デジタル化の進展が見込まれる（70%以上の企業で、今後3～5年後の商品・サービスのデジタル化の予算が増加することが見込まれる）[7]一方、それに伴う適切なセキュリティ対策が行われないおそれ（デジタルトランスフォーメーション（以下「DX」という。）推進に伴うセキュリティ対策の見直し状況について「実施済み」もしくは「一部実施」の企業は他国に比べ少なく（日本：21.7%、米国：73.7%、豪州：77.3%）、自社でセキュア開発を行う体制が整っている企業も他国に比べ少ない（日本:30.3%、米国:89.5%、豪州：87.2%））[8]もあり、様々な主体が「DX with Cybersecurity」を意識することが求められていると言えよう。

1　経営層の意識

サイバーセキュリティ対策の推進に当たっては、経営層がリーダーシップを発揮し対策を指示することが重要であるが、足元では、経営層の関与は大きく進展しておらず、他国と比べても依然としてその水準は低いと言える。実際に、経営幹部が企業を取り巻くセキュリティリスクの深刻さを重要視し、経営会議等で重大なセキュリティリスクや対策の重要性について審議・報告される企業は4割程度のまま推移しているというデータも存在する[9]。また、情報セキュリティ対策実施のきっかけや理由をみると、米国や豪州では過半数の企業が経営層のトップダウン指示である（日本：23.4%、米国：56.4%、豪州：61.4%）のに対し、日本では自社でのセキュリティインシデントを契機とする企業が多い（日本：30.7%、米国：19.3%、

[5] Kaspersky「コロナ禍の1年：リモートデスクトッププロトコルへの攻撃が高い水準を維持」（2021年4月6日）
https://blog.kaspersky.co.jp/attacks-on-rdp-during-pandemic-year/30354/
[6] McAfee「クラウドの採用とリスクに関するレポート（在宅勤務編）」（2020年6月9日）
https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2020060901
[7] （一社）日本システムユーザー協会「企業IT動向調査報告書2021（2020年度調査）」（2021年4月28日）
https://juas.or.jp/cms/media/2021/04/JUAS_IT2021.pdf
[8] 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2020」（2020年12月15日）
https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1
[9] （一社）日本システムユーザー協会「企業IT動向調査報告書」における複数年の調査結果を確認。

豪州：19.8%）[10]。加えて、最高情報セキュリティ責任者（CISO）の組織内の位置づけについては、欧米では経営層（日 31.9%、米 46.8%、欧 28.5%）もしくは経営層直下（日 31.7%、米 35.5%、欧 43.4%）とする企業が多数であるのに比べ、日本では非経営層である情報システム部門のトップとしている企業（日 38.7%、米 20.7%、欧 24.7%）が多い[11]。

この要因の一つとして、経営層がサイバーセキュリティに係るリスクを、企業損失ひいては企業価値の毀損に直結する経営上の課題とみなしていない（あるいは相対的にその優先度が低い）ことが指摘されている。例えば、新型コロナウイルス感染症の拡大により、リモートワークを導入した結果、コンピュータウイルス感染等のサイバー攻撃によるリスクを、優先して着手が必要と思われる経営リスクとして挙げる企業が増えている（疫病の蔓延（パンデミック）等の発生：34.4%、異常気象（洪水）異常気象（洪水・暴風など）、大規模な自然災害（地震・津波・火山爆発・地磁気嵐）：30.9%、サイバー攻撃・ウイルス感染等による情報漏えい：21.3%）[12]一方で、セキュリティ対策の情報開示状況を公開とする企業の比率は、欧米諸外国に比べ低水準である（日本：33.6%、米国：78.4%、英国：82.2%）[13]。

しかしながら、新型コロナウイルス感染症への対策を余儀なくされることにより、6割の企業が「コロナ禍前に事業が戻らない」とするアンケート結果[14]もある中、DX の必要性について経営層の意識は変わりつつあるとも考えられる。こうした変化を踏まえ、政府としても企業の DX を推進する取組が行われている。例えば、情報処理促進法に基づき、DX に向けた戦略や推進体制などの整備等、経営者に求められる事柄をとりまとめた「デジタルガバナンス・コード」を策定し、同コードを実践する企業を認定する DX 認定制度の整備を行っている。

こうした取組と連動し、経営層によ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を進めることで、サイバーセキュリティを前提とした DX を推進していく「DX with Cybersecurity」を推進する経営に取り組む必要がある。2017 年 11 月に公開された「サイバーセキュリティ経営ガイドライン Ver2.0」のダウンロード数は 2021 年５月末時点で累計 10 万件と、活用が広がっており、これらの更なる活用促進に向け、「サイバーセキュリティ経営ガイドライン Ver2.0 実践のための経営プラクティス集」や「サイバーセキュリティ体制構築・人材確保の手引き」の策定が行われており、これらの更なる活用が期待される。

2　地域・中小企業

中小企業では人材等の制約が顕著であり、大企業以上にセキュリティ対策が進んでいない。実施しているセキュリティ対策は、ウイルス対策ソフト・サービスの導入（中小企業：80.4%、大企業：91.9%）のみという中小企業が多く、メールフィルタリング（中小企業：11.6%、大企

[10] 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 2020」（2020 年 12 月 15 日）
https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1
[11] （独）情報処理推進機構「企業の CISO や CSIRT に関する実態調査 2017」（2017 年 4 月 13 日）
https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html
[12] デロイトトーマツ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020 年版」（2021 年 3 月 2 日）
https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/news-releases/nr20210302.html
[13] 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 2020」（2020 年 12 月 15 日）
https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1
[14] ㈱INDUSTRIAL-X「企業の DX 実現に向けた課題とコロナ前後の意向に関する調査」（2020 年 6 月 25 日）
https://prtimes.jp/main/html/rd/p/000000010.000051016.html

業：50.6%）やWeb閲覧フィルタリング（中小企業：11.1%、大企業：58.8%）など他のセキュリティ製品の導入において、大企業と実施状況の差異が顕著である[15]。また、中小企業では、社内にサイバーセキュリティ対策を行える人材がいないことが、セキュリティ対策を実施する際の障害となっている（中小企業：42.8%、大企業：26.3%）[16]との指摘がなされて久しい。

中小企業においては、リソースの制約が大きい中で、安価で利用しやすいサービスの需要が大きいところ、2019年・2020年には、「サイバーセキュリティお助け隊サービス」の実証事業が行われ、中小企業向けのサービスや簡易サイバー保険のビジネス化に向けた課題抽出が行われた。この中で、具体的に、過去に構築されたウェブサイトなどのシステムに対する脆弱性対策が行われないまま放置されていることや、リスク診断等の簡易ツールやセキュリティインシデントレポートを用意しても自主的に活用できる企業が少ない、といった課題が抽出されている[17]。また、地域による課題解決・付加価値創出の場として、「地域 SECUNITY」の形成が少しずつ全国に広がりつつあり、2020年2月には当該コミュニティづくりにおけるプラクティス集が策定されたところ、こうした先進事例の横展開に活用されることが期待される。

3　新たな価値創出を支えるサプライチェーン等の基盤

サイバー空間とフィジカル空間が高度に融合するSociety5.0の実現に向けて、今後は、あらゆる主体が相互連関・連鎖を自由に形成することで新たな価値を創造することが期待される。一方で、その信頼性を確保する観点から、このように新たに形成される相互連関・連鎖の下で生じる課題に適切に対応していくことが必要となる。これらサイバー空間の信頼構築の基盤となるサプライチェーンやデータ流通、セキュリティ製品・サービス、新技術の社会実装をとりまく状況について、以下に示す。

前項のとおり、中小企業において、人材等が制約となり、セキュリティ対策をすすめることへの困難性が大企業以上にある中で、サイバーセキュリティに係る観点では、サイバー攻撃の起点となり得る箇所の拡大や実空間への影響の増大が懸念されるなど、サプライチェーン全体を見渡したリスク管理の重要性は増していくと考えられる。自らの製品・サービスに係る「任務保証」を実現するためには、そのサプライチェーンを含めて適切に管理していくことが求められるが、他国以上に、その管理・対策状況が十分に進んでいるとは言えない状況にある（物品調達先のセキュリティ対策状況を十分に確認できていると回答した割合：（日本）24.0%、（米国）42.9%、（欧州）44.1%）[18]。

経済産業省においては、企業の壁を越え、サプライチェーン全体でのサイバーセキュリティ対策を促すため、「サイバー・フィジカル・セキュリティ対策フレームワーク」に基づき、

[15] (独)情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017」(2017年4月13日)
https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html
[16] (独)情報処理推進機構「2016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」(2017年8月8日)
https://www.ipa.go.jp/security/fy28/reports/sme/
[17] 経済産業省「第7回 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（経営・人材・国際)」事務局説明資料より（2021年2月18日）
[18] (独)情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017」(2017年4月13日)
https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

電力、ビル、自動車等の分野別や、IoT セキュリティなどの分野横断的なセキュリティガイドラインの整備を推進している。

また、企業活動のみならず、経済社会のデジタル化が進展をする中で、データそのものが様々な価値を持つようになると想定され、データ流通において真正性・完全性が確保されることが重要である。特に活用が期待される「トラストサービス」に係る市場は、2030 年頃には、1,035 億円に達すると推計される[19]など、今後の普及が期待される。これらトラストサービスについて、近年、その制度化等の取組が進められている。具体的には、タイムスタンプについては、2021 年 4 月に「時刻認証業務の認定に関する規程」を公布、国による認定制度が整備された。e シールについては、e シールの利用が有効なユースケースや我が国の e シールの在り方等について検討が行われており、その結果を踏まえて、今後、技術上・運用上の基準等を整理した指針が作成される予定である。電子署名については、リモート署名の電子署名法上の位置づけが示されるなど、電子署名法上の電子署名の利便性の改善に向けた取組が実施されている。

さらに、今後は、サプライチェーン・リスクへの懸念に加え、オープン API [20]や OSS [21]の活用が一般的となったことで開発者自身もシステム全体のリスクを把握する困難性が高まっている中で、自社製品等の信頼性を企業内外に示す観点から、第三者による客観的な検証への需要が拡大し、そうした需要に応えるビジネスが産業として一層重要になっていくと考えられる。

加えて、サイバーセキュリティに係る製品・技術の日系企業のシェアをみると、例えば、ウイルス対策ソフトでは 14.7%、ゲートウェイセキュリティに至っては 1.0%といったデータ[22]があるなど、他国への依存について指摘されて久しい。海外のセキュリティ技術を導入・運用するビジネスモデルは、研究開発投資を抑え、事業上のリスクを極小化することができる一方で、利益率が低く、また、コア技術に係るノウハウ・知見を蓄積することが難しい側面がある。また、データが集まらないことで、研究開発できず、故に技術を作れない、そして技術が普及せず、データが集まらない、という負の循環を生むおそれもあり、こうした状況の打破が必要である。

4　デジタル／セキュリティ・リテラシー

我が国におけるインターネット利用者の割合は既に８割を超え（2020 年８月：83.4%）[23]、インターネットの平均利用時間も増加傾向にあることから、国民のサイバー空間への参画は更に進展している。特に若年層と高齢者層におけるインターネット利用者の割合が増加していることを踏まえると（2020 年８月：（６～12 歳）80.7% ／ （80 歳以上）25.6%）、これま

[19] 総務省「トラストサービス検討ワーキンググループ 最終報告書」（2019 年 11 月 28 日）における(株)三菱総合研究所による試算
[20] API（Application Programming Interface）
[21] OSS（Open Source Software）
[22] (独)日本貿易振興機構「拡大するサイバーセキュリティー市場」（2018 年 12 月 26 日）
https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html
[23] 総務省「令和 2 年通信利用動向調査」（2021 年 6 月 18 日）
https://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html

で以上に幅広い国民が、サイバー空間の恩恵を享受するようになってきていると言える。

一方で、サイバー空間における攻撃者は、セキュリティ対策が最も手薄な部分を狙って攻撃を行い、そこを起点としてネットワークやシステム全体に攻撃を展開させていくという手法を取ることが知られている。したがって、サイバーセキュリティを確保するためには、一部のネットワークやシステムだけを集中的に防御したり、一部の専門家だけが対処したりすれば事足りる訳ではなく、サイバー空間に参画する者全体の意識・行動の底上げが必要である。例えば、新型コロナウイルス感染症の影響等で在宅勤務が増加している状況において、フィッシングメール、不正アプリなどによるサイバー攻撃に対抗するためには、いわゆる従来から取り組まれている「境界型セキュリティ」の考え方に沿って企業のシステム部門が社内ネットワークのセキュリティ対策を実施するだけでは不十分であり、自宅環境においても、個人が利用する機器等に適切なセキュリティ対策を実施する必要がある。ここには、ネットワークやシステムに対する物理的な対策だけでなく、怪しいURLにアクセスしない、ショルダーハッキングに注意する、などといった、日常生活における基本的なリテラシーの向上も含まれている。同様に、GIGAスクール構想により今後各種学校等でICT教育、また新型コロナウイルス感染症の状況を踏まえ遠隔教育が継続ないし増加していくことからも、児童生徒をはじめとする若年層やその保護者といった個人レベルでのセキュリティ対策の実施・素養（リテラシー）の向上が重要性を増してきている。

しかし、現状を鑑みると、そのようなセキュリティ対策の実施状況やその基本的な知識及びリテラシーに関して、社会全体でのギャップが存在している。例えば、「セキュリティソフト・サービスの導入・活用」等の技術的な対策は若年層ほど実施率が高い一方、「怪しいと思ったウェブサイトに行き着いたら先に進まない、情報を入力しない」等のリテラシー面の意識は年代が上がるほど高い[24]。また、インターネットや情報に関する倫理教育の受講経験については、若年層では過半数が受講した経験があるにも関わらず、特に高齢者層では依然として低い傾向にある（10代：62.1%、20代：37.0%、30代：22.6%、40代：17.0%、50代：14.1%、60代：15.5%、70代以上：12.3%）[25]。そのような状況下でも、インターネットをパソコン経由で利用する者の63%超、スマートデバイス経由で利用する者の71%超が、インターネット利用中にフィッシングメールを始めとする何らかの脅威に遭遇した経験を有しており[26]、国民一人一人がサイバーセキュリティの重要性を理解し、適切に対策を実施できるようにするための取組を進めることが急務であると考えられる。

具体的に進みつつある取組として、若年層のセキュリティ対策・リテラシー向上に向けた取組を含むICT教育の充実が挙げられる。GIGAスクール構想の実現を目指すにあたって、サイバーセキュリティをどのように確保するかは避けて通れない問題である。特に若年層のリテラシー向上という観点では、情報セキュリティを学習内容に含む中学校での技術・家庭科の内容の充実や高等学校の「情報I」の必修化をはじめ、情報モラル教育の推進、教職課程の

[24] (独)情報処理推進機構「2020年度 情報セキュリティの脅威に対する意識調査」(2021年3月4日)
https://www.ipa.go.jp/security/economics/ishikichousa2020.html
[25] IPA「2020年度 情報セキュリティの倫理に対する意識調査」概要報告書
https://www.ipa.go.jp/files/000088910.pdf
[26] IPA「2020年度 情報セキュリティの脅威に対する意識調査」概要報告書
https://www.ipa.go.jp/files/000088916.pdf

見直しといった取組が、新型コロナウイルス感染症に係る状況に伴い、加速的に推進されている。また、高齢者層を対象としたデジタル活用支援員の配置や携帯電話ショップを中心としたデジタル活用支援事業の推進も、セキュリティ対策・リテラシーの向上に資する取組の１つとして期待される。

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・社会を守るためのセキュリティ基盤の構築

サイバー空間は、我々の生活におけるある種の「公共空間」として、より一層の重みを持つようになってきている。例えば、我が国においてクラウドサービスを一部でも利用している企業の割合は64.7%であり、多くの企業が「非常に効果があった」又は「ある程度効果があった」とクラウドサービスの効果を実感している[27]。また、我が国の電子商取引の市場規模を見れば、2019 年の消費者向け電子商取引（BtoC-EC）市場規模は 19 兆 3,609 億円（前年比 7.65%増）、個人間電子商取引（CtoC-EC）市場規模は 1 兆 7,407 億円（前年比 9.5%増）、企業間電子商取引（BtoB-EC）市場規模は 352 兆 9,620 億円（前年比 2.5%増）と、いずれも拡大している[28]。

他方、こうした「公共空間」たるサイバー空間の様々なサービスにおいて、サイバー攻撃、設定の不備、サービス提供者と利用者間の認識の相違や相互理解の不足等、様々な要因により、予期せぬ情報流出や業務への影響といった被害が発生していることも事実である。

このように我々の生活や経済活動に密接にかかわるサイバー空間が、日進月歩に変化する技術やサービスの実装により間断なく高度化し、サービス提供者の主体が変わりうる実態を踏まえ、国は、サイバー空間に関わるあらゆる国民や主体が、サイバー空間に参画するに際して安心感と安全に対する予見性を持つことができるよう、サイバー空間全体を俯瞰しつつ、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必要がある。また、サイバー空間におけるあらゆるサービスの提供主体は、これまでの「任務保証」という考え方を深め、海外拠点、取引先等、自らのサービス提供に係る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といった連携を推進する等、サイバー空間の変容に適合したリスクマネジメントを講ずることが求められる。

国は、サイバー空間について実空間と変わらぬ安全・安心を確保するため、サイバー空間を悪用する犯罪者や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し、深刻なサイバー攻撃に対しては、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至る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作り等の政策措置の展開を一体的に推進する包括的なサイバー防御策を行っていく必要がある。加えて、現在認知されているサイバー攻撃の多くが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目的としていることや、我が国の国民生活や経済社会活動の根幹を支える基盤において実装されている IT システムに起因するインシデントがそれら基盤の機能停止に直結するリスクを踏まえ、経済安全保障の観点も含めた横断的な防護対策や信頼

[27] 総務省「令和2年「情報通信に関する現状報告」（令和2年版情報通信白書）」（2020年8月4日）
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000149.html）

[28] 経済産業省「令和元年度内外一体の経済成長戦略構築にかかる国際経済調査事業（電子商取引に関する市場調査）報告書」（2020年7月22日）
https://www.meti.go.jp/press/2020/07/20200722003/20200722003.html

性確保に向けた取組も必要である。

こうした取組を通じて、サイバー空間に係るあらゆる主体の自助・共助・公助からなるセキュリティ環境を構築し、もって、国全体のリスクの低減とレジリエンスの向上を図ることが必要である。

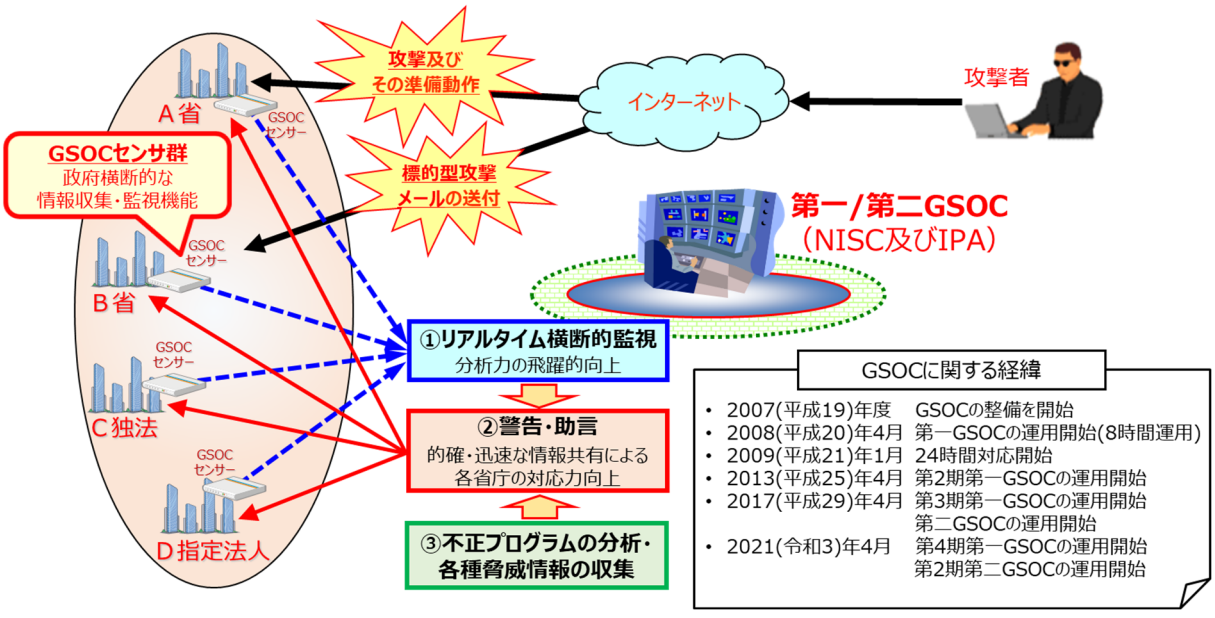
2　経済社会基盤を支える各主体における情勢①（政府機関等）

2.1　政府機関等[29]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月から内閣サイバーセキュリティセンター（以下「NISC」という。）において政府機関情報セキュリティ横断監視・即応調整チーム（第一GSOC[30]）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基本法に基づく指定法人（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



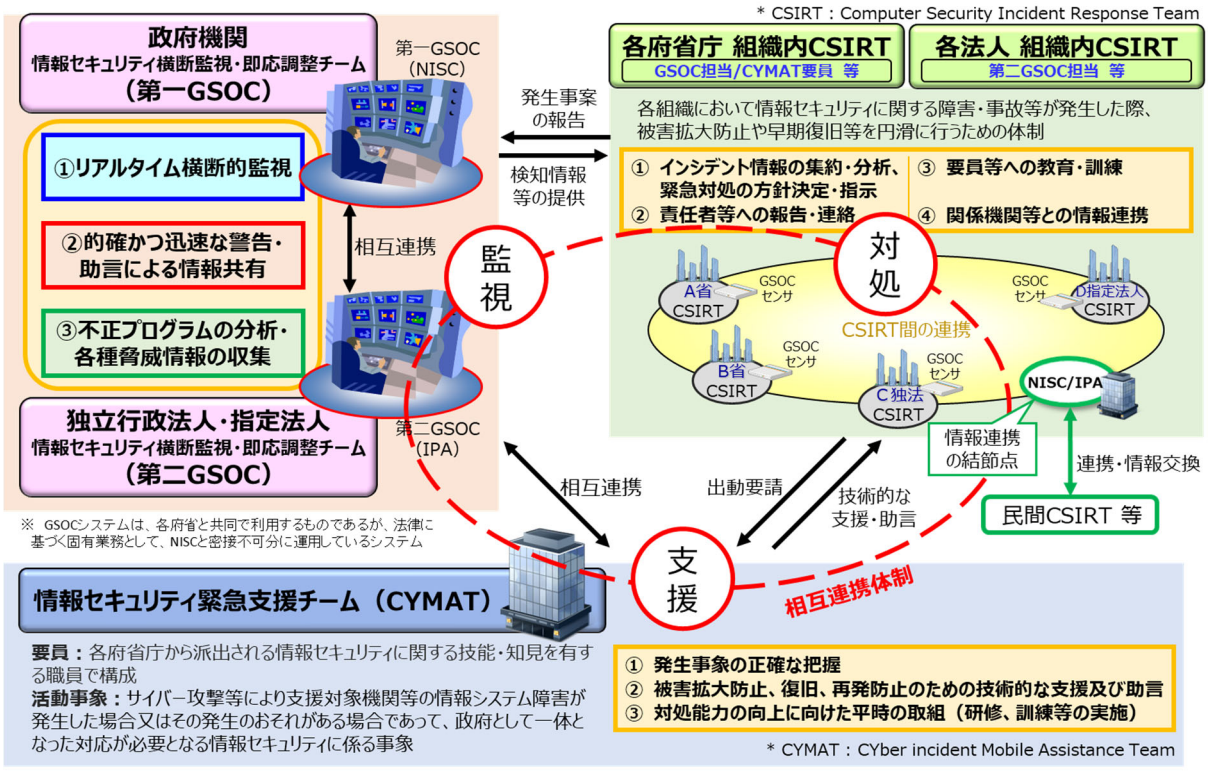
また、NISCは各府省庁の要請により情報セキュリティ緊急支援チーム（CYMAT[31]）を派遣し、技術的な支援・助言を実施している。

[29] 本章では、府省庁及びオブザーバ機関（府省庁等）並びに独立行政法人及び基本法に基づく指定法人（独立行政法人等）を総称して「政府機関等」という。
[30] GSOC（Government Security Operation Coordination team）
[31] CYMAT（CYber incident Mobile Assistance Team）

一方、各府省庁や各法人はそれぞれ組織内 CSIRT[32]を設置し、自組織の情報システムの構築・運用を行うとともに、サイバー攻撃による障害等の事案が発生した場合には、情報システムの管理者としての責任を果たす観点から、自ら被害拡大の防止、早期復旧のための措置、原因の調査、再発防止等の対応を実施している。

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　2020 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[33]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、2017 年度から検知・解析機能の強化やセンサーの増強を図った第３期第一 GSOC システムの運用を開始しているが、対応能力等のリソースの有効活用等を目的として、分析等の機械的処理を含むセンサー性能の向上を図り自動化を進めたことに伴い、統計処理方法を変更することとしたため、以下の図表において 2016 年度以前の件数と 2017 年度以降の件数

[32] CSIRT（Computer Security Incident Response Team）
[33] 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 2020 年度の情報セキュリティインシデント一覧」を参照。

は単純比較できなくなっている。

（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となる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、標的型攻撃によりもたらされた不正プログラムが行うもの、これらに該当するとの疑いがあるもの等を指す。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。）[34]の件数について、以下に示す。

前提として、前年度までに対策済み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、当年度に GSOC 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。

2020 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発生しているものの、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[35]。第一 GSOC における具体的な状況は次のとおりである。

ウェブアプリケーションの脆弱性や設定不備を狙った攻撃は、2017 年度以降「Apache Struts」を狙った通信が目立っていたが、このような攻撃に対する対策が進んだ結果、2019 年度までに検知件数が大幅に減少した。2020 年度においては、同様の攻撃として「Oracle WebLogic Server」の脆弱性を狙った通信が 59 件検知されたが、傾向としては、脆弱性が公開されてから対策が完了するまでの短期間のみ検知された。

ポリシー違反の疑いがある通信については、2017 年度には 3,614 件検知していたが、そ

[34] 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 システムでは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。

[35] 第二 GSOC は、2017 年度に運用を開始して間もなく、センサーでの検知に当たり不要と判断できるノイズの除去について継続して調整中であり、状況確認等のため検知ルールの追加や削除を行ったことから、2019 年度においては約 221 万件と高い値となっていたが、2020 年度には約 26 万件と減少している。

のうち 3,479 件を占めていたリモートアクセスアプリケーションの使用を取りやめたため 2018 年度に９件、2019 年度に４件、2020 年度に 15 件と検知数が大幅に減少した。また、P2P 通信を行うファイル共有サービスによる通信を 2018 年度に９件、2019 年度に４件検知していたが、検知ルールの調整が進んだことや、各機関において許可されたもの以外のアプリケーションの使用制限が進んでいることから、2020 年度は検知数が０件となった。また、マルウェア感染の疑いや標的型攻撃等の検知件数は図表１－２－３のように推移している。

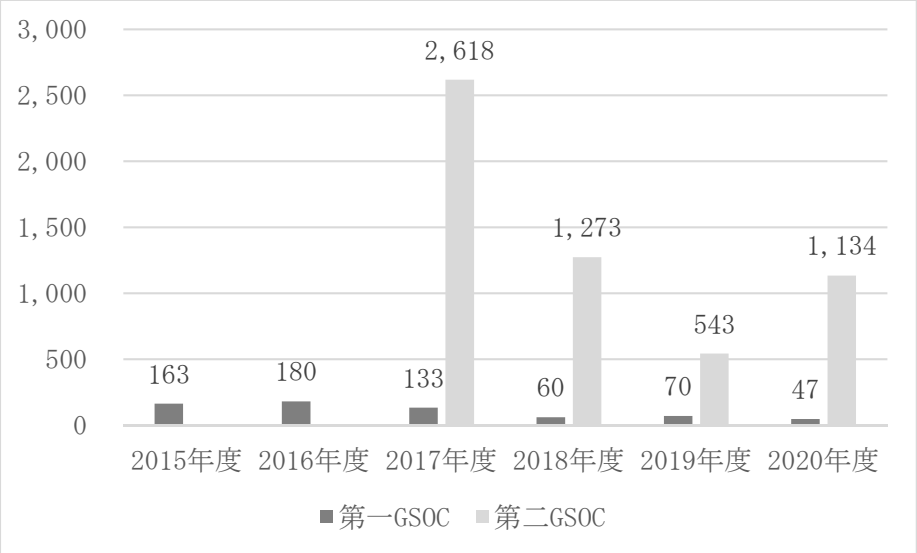
図表１－２－３　マルウェア感染の疑いや標的型攻撃等の検知件数

年度	2017 年度	2018 年度	2019 年度	2020 年度
マルウェア感染の疑い	169	111	55	245
標的型攻撃等	57	71	35	15

（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、2020 年度においては、第一 GSOC では 47 件、第二 GSOC では 1,134 件[36]の通報を行った（図表１－２－４）。

図表１－２－４　GSOC センサー監視等による通報件数の推移



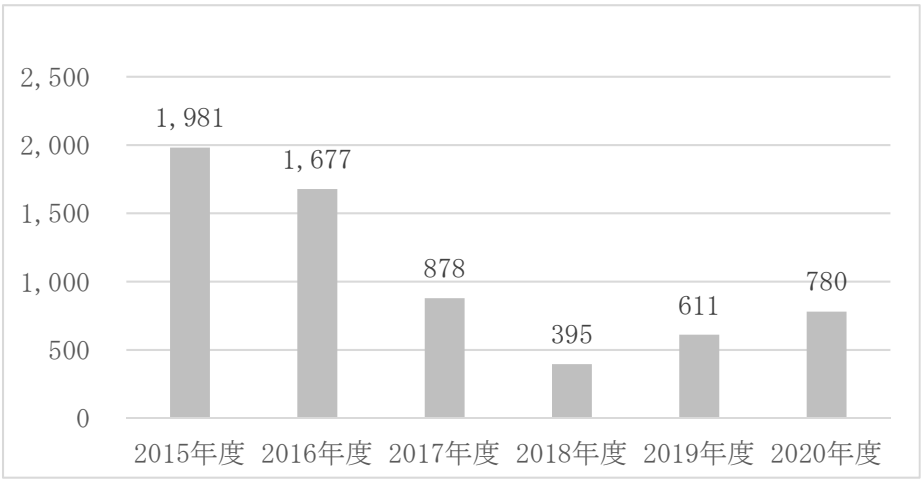
（３）不審メール等に関する注意喚起

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、情報を集約し注意喚起等を行っている。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

[36] 第二 GSOC では、特定の監視対象法人において、一定期間にわたり継続的に過検知が発生（当該法人による調査の結果、インシデントではない過検知であることを確認）したため、通報件数も多くなった。当該検知に伴う通報を除くと、通報件数は前年度よりも減少している。

もの等について、政府機関等に対して一斉に注意喚起を行っており、2020 年度においては GSOC から 780 件の注意喚起を行った（図表１－２－５）。

図表１－２－５　不審メール等に関する注意喚起の件数



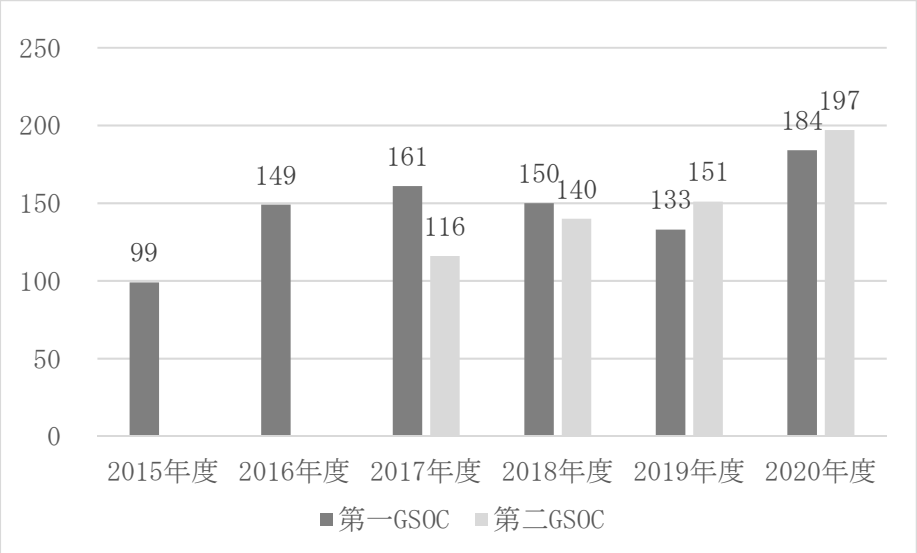
この注意喚起の件数は 2018 年度まで減少傾向にあったが、2019 年度後期以降、我が国においてもマルウェア「Emotet（エモテット）」が流行したことを踏まえ、これらに関する注意喚起を行ったため、増加した（コラム参照）。不審メールの中には、実在する組織やその所属職員とのやりとりに、その職員になりすまして返信する形で送付されるものもあるため、より一層の注意が必要である。

（４）ソフトウェアの脆弱性情報の配信

GSOC では、ウェブサイト等への攻撃を始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対策情報等を政府機関等に配信し、注意喚起を行っている。2020 年度においては、第一 GSOC から 184 件、第二 GSOC から 197 件の脆弱性情報等を配信した（図表１－２－６）。

政府機関等におけるテレワークの拡大等により利用するソフトウェアが増加していることを踏まえ、第一 GSOC、第二 GSOC ともに、2020 年度は脆弱性情報の配信対象とするソフトウェアを増加したため、2019 年度と比べ脆弱性情報の配信数が増加している。

図表１－２－６　GSOC が配信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、2020 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、VPN 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。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　2020 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、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。

2020 年度も、職員や委託先事業者の過失等による意図せぬ情報流出にかかる情報セキュリティインシデントが散見された。

具体的には BCC で送付すべき一斉送信メールを To で送付してメールアドレスが流出した事案、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 Web 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。

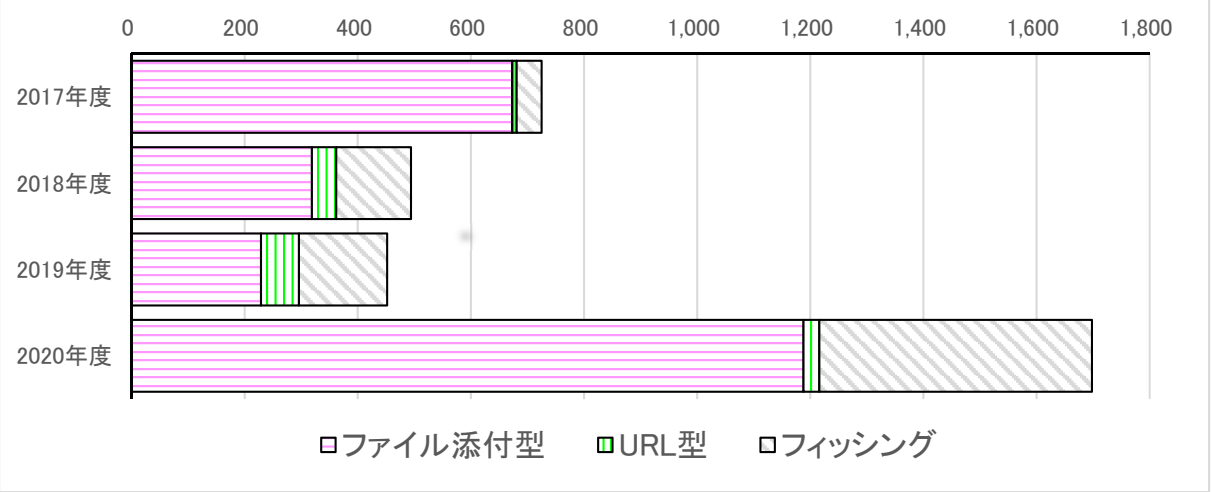
コラム～政府機関等に対する不審メールの傾向～

○　不審メールの傾向について

図表１－２－７は、政府機関等から GSOC に対して解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毎にまとめたものの推移を示したものである。2017 年度から 2019 年度までは、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。）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。）が増加する傾向が続いていたが、2020 年度においてはファイル添付型が大幅に増加した。これについては、マルウェア「Emotet」に関連する不審メールが多数確認されたためである。

また、フィッシングメールについては、近年の増加傾向が継続しているところ、2020 年において顕著な増加が見られた。フィッシングについては現在も活発に行われている状況であり、今後も増加する可能性があると思料される。

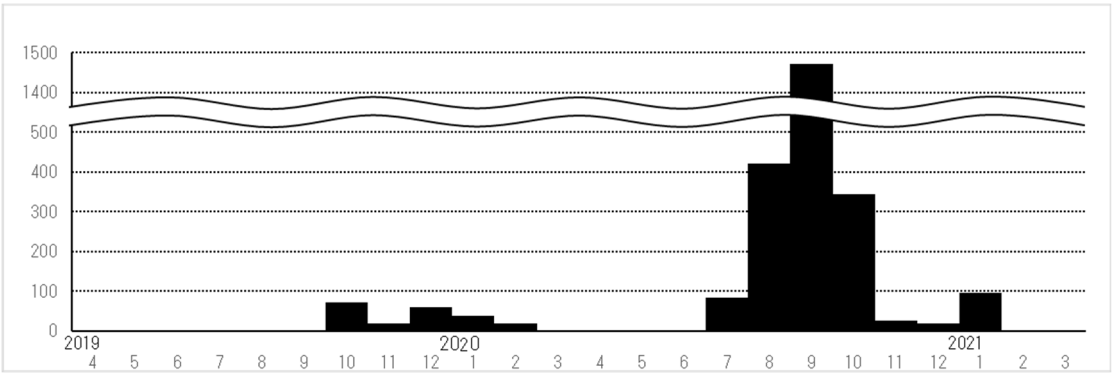
図表１－２－７　不審メールの傾向



○　不審メールで利用されていたマルウェアの動向

2020 年度に取り扱った不審メールから最も多く確認されたマルウェアは、2019 年度から継続して確認されていた Emotet に関連するもので、2020 年２月から 7 月にかけては一旦取り扱い件数が減少したものの、８月から 10 月にかけては一転して大量の不審メールが政府機関等に送りつけられる状況が確認された。

図表１－２－８　Emotet 取扱件数の推移（2019 年４月～2021 年３月）



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、攻撃者により様々な機能が追加された結果、他のマルウェアに感染させる手段としても用いられている。Emotetの感染を狙った不審メールの特徴としては、メール添付又はメール内に記載されたリンク先からダウンロードさせたマクロ付きのMicrosoft Wordファイルを開かせ、Emotet本体をダウンロード・感染させる形式をとることと、不審メールが過去に窃取した実在のメールアカウント・メール内容を用いて、正規のメールになりすましたものが多く確認されたことが挙げられる。

Emotetについては、2021年１月に欧米各国法執行機関によってEmotetをコントロールするサーバが差し押さえられた（いわゆる「Emotetのテイクダウン」＊）後は、GSOCに解析依頼された不審メールからは確認されていない状況となっている。しかしながら、他のマルウェアにおいてもEmotet同様の感染手法を用いるものが確認されていることから、今後も継続して不審メールに対する警戒を行う必要がある。

＊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。その後、同法執行機関が把握した日本国内のEmotet感染端末の情報が警察庁に情報提供されたため、２月から、警察庁、総務省、一般社団法人ICT-ISAC及びISPが連携して、日本国内の利用者を特定し、注意喚起を行う取組を進めている。

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

警察庁“マルウェアに感染している機器の利用者に対する注意喚起の実施について”
https://www.npa.go.jp/cyber/policy/mw-attention.html

2.4　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

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、「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」（以下「統一基準群」という。）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ことが重要な課題として、現在、2021 年度中の統一基準群改定に向け作業を進めている。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むこととしている。

引き続き、クラウドサービスを始めとする IT 技術の最新動向などの情勢を見据えて、その脅威とリスクなどを分析し、中長期的にセキュリティ対策が必要な方向性を定め、統一基準群の定期的な見直しを図り、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）

2020 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）新型コロナウイルス感染症

新型コロナウイルス感染症の世界的拡大に伴い、国内外を問わず、重要インフラ分野等において、新型コロナウイルス感染症に関連したシステム障害やサイバー攻撃が多数発生した。また感染症への対応として、テレワークの利用が急速に拡大するにつれ、遠隔会議システムや VPN 機器を始めとしたリモートアクセスを支える重要機器の脆弱性が顕在化した。

国内では、2020 年５月、新型コロナウイルス感染症の対策として、特別定額給付金のオンライン申請を開始したが、申請に必要となるマイナンバーカードの電子証明書関係手続の処理遅延や重複申請等のトラブルが発生した。2020 年 10 月、特別定額給付金の給付を騙ったフィッシングメールが多数確認された。国外では、2020 年 12 月、欧州医薬品庁(EMA)がサイバー攻撃を受け、米国の製薬会社ファイザーとドイツのバイオ医薬品企業ビオンテックが開発したワクチン候補の規制当局への承認申請に関する文書が不正アクセスされた。また、2021 年１月、英国の国民保健サービス(NHS)は、新型コロナウイルス感染症のワクチン接種の希望の有無を問うフィッシングメールを確認した。

こうした事例を踏まえ、多様な経路・手段による攻撃が想定され得ることを前提にセキュリティ意識を高く持つことが必要であり、リモートアクセス環境を構成する機器に対する迅速なアップデートや適切な設定を含めた管理の厳格化、更には、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がより一層求められている。

（2）経営層関与の重要性

サイバー攻撃やシステム障害が事業継続に大きな影響を与える事例や経営層の責任に発展する事例もあった。2020 年 8 月、ニュージーランド証券取引所への DDoS 攻撃により、同取引所のウェブサイト及びシステムがダウン、市場情報が提供できなくなることから 4 日間連続で取引を一時停止し、財務大臣が政府通信保安局とサイバー犯罪対策当局に支援を要請する事態が発生した。攻撃が続く中、同取引所は、万が一、ウェブサイトがダウンした場合でも、別の取引プラットフォームによる情報提供で取引が継続できるよう金融市場当局と事前合意し、取引停止による影響の最小化を図った。2020 年 10 月、日本のある証券取引所で、株式売買システムの障害により、全銘柄の売買を終日停止した。全銘柄の売買終日停止は、1999 年の取引全面システム化以降初めての事態であり、原因は設定がマニュアルどおりに動作しなかったことに起因、社長は辞任した。この事例では、障害が発生したものの、早い段階で取引終日停止を決定した経営判断があり、障害発生日に行われた会見では、経営者による技術面も含めた説明対応があった。

他方、キャッシュレス手段による電子決済サービスが普及する中、これに伴うトラブルも発生した。2020 年 9 月、複数の銀行において、大手通信会社が提供する電子決済サービスの口座への不正引出が発生、比較的被害の大きかったある銀行は、その他の電子決済サービスでも同様の被害を確認、電子決済サービス事業者と連携して全額を補償し、2 要素認証を導入した。電子決済サービスをめぐっては、2019 年 7 月、あるスマートフォン決済サービスにおいて、サービス開始直後に不正利用が発生、初動対応の不手際などから、3 か月でサービス廃止に至った事例がある。これらは、本人確認や利用者認証の甘さが原因であり、他の決済サービスで不正利用対策として使用されている 2 要素認証が適切に実装されていないなど、システム設計上の問題が再度繰り返された。

総じて、リスク管理体制やインシデント体制の構築など、サイバーセキュリティインシデントは経営上の課題として経営層が率先して取り組むべきものであり、これらの事例は、経営層関与の重要性を改めて示唆するものと言える。

（3）クラウド環境への対応

クラウドサービスの障害や設定不備によって重要インフラ事業者等が提供するサービスに影響を与えた事例が相次いで報告された。2020 年 5 月、国内ベンダーが提供する自治体向けクラウドサービスでシステム障害が発生、復旧するまで一部の自治体でメールの送受信等に影響が生じた。2020 年 6 月、別の国内ベンダーが提供するクラウドサービスでシステム障害が発生、同サービスを利用していた複数の自治体で、ウェブサイトの閲覧障害が生じた。

2020 年 12 月、米国系ベンダーは、クラウド型顧客関係ソリューションにおいて、設定が適切に行われていない場合、一部の情報が第三者から閲覧される可能性があると発表、特に、

2021年2月以降、このソリューションを利用していた国内の複数の自治体が同様の可能性を公表する事態となった。

このように、クラウドサービスは利便性が高い反面、障害等の発生により重要インフラ事業者等が提供するサービスに影響が生じることから、外部サービスであるクラウドサービスを利用するに当たっては、利用契約で担保されている内容を踏まえつつ、適切な防御措置が必要であることを示す結果となった。

（4）サイバー攻撃

①ランサムウェアまん延とその対応策

国外では、医療機関や自治体においてランサムウェア被害が数多く発生した。2020年9月、米国サイバーセキュリティ・インフラセキュリティ庁(CISA[37])と MS-ISAC[38]は、米国の政府機関、州、重要インフラ等に対する攻撃を踏まえ、共同で「RANSOMWARE GUIDE」を公開した。また2020年10月、CISA、米国連邦捜査局(FBI[39])及び米国保健社会福祉省(HHS[40])は、ヘルスケア及び公衆衛生セクターを対象としたランサムウェアの活動に関する共同セキュリティアドバイザリーを公開した。

一般的に、米国を含む諸外国で発生したサイバー攻撃は、数年遅れて我が国で発生する傾向がある中、国内では、2020年11月、大手ゲーム会社の一部機器が不正アクセスによりランサムウェアに感染し、顧客や取引先等の約1.6万件の個人情報の流出を確認、最大約39万件の個人情報が流出した可能性があることが判明した。ランサムウェアにせよ、大規模かつ巧妙なサイバー攻撃があったが、その初期段階の侵入ベクトルの大元はネットにさらされている機器の脆弱性の不十分な管理が原因であること、その背景には、コロナ禍のテレワークなどがある点に留意する必要がある。

②治安当局の出動

2019年に多くの国内の組織で感染が確認されたマルウェア Emotet は、攻撃活動が休止しているとみられていたが、2020年7月以降、マルウェア Emotet の活動が再開し、同マルウェアへの感染が重要インフラ分野等において数多く報告された。2020年7月、複数の自治体で自治体職員を騙った Emotet に関連するメールが確認されたことを受け、NISC は自治体から届いたメールに不審な点がある場合は本文中の URL や添付ファイルを開かないよう注意喚起を行った。2020年8月、国内の大手自動車販売店では、同社を騙る大量のなりすましメールも確認され、調査の結果、全78拠点のうち、11拠点の PC で Emotet の感染が判明した。こうした中、2021年1月、欧州刑事警察機構(Europol)は、欧州司法機構(Eurojust)との調整を通じ、8か国(オランダ、ドイツ、フランス、リトアニア、カナダ、米国、英国、ウクライナ)の法執行機関の連携の結果、マルウェア Emotet の攻撃インフラを制御下に置くことに成功したと発表した。Emotet の被害はこれにより沈静化したものの、今後、同様の手法をとるマルウェアや攻撃が出現する蓋然性も高いため、引き続き留意する必要がある。

[37] CISA (Cybersecurity and Infrastructure Security Agency)
[38] MS-ISAC (Multi-State Information Sharing and Analysis Center)
[39] FBI (Federal Bureau of Investigation)
[40] HHS (Health and Human Services)

③脆弱性を突いた巧妙な攻撃

2020年８月、Netlogonの特権昇格が可能な脆弱性が公開、本脆弱性を悪用し、ドメインコントローラーを侵害する事例が多数確認された。2021年３月、Microsoft Exchange Serverの脆弱性が公開、セキュリティ更新プログラムの公開前から本脆弱性を悪用した攻撃が確認された。昨今の脆弱性は、脆弱性情報の公開から攻撃発生までの時間が短いことも多く、迅速なパッチの適用、パッチが適用できない場合の適切な管理策の実行、侵害された場合の調査等、重要インフラ事業者等にも迅速な対応が求められる。

（５）自然災害

2019年度に引き続き、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。2020年9月、大型で非常に強い令和2年台風第10号が発生し、九州・中国・四国地方では最大約53万戸の停電が生じた。台風10号は、電柱の折損本数は少なかったものの、被災した配電線は748回線と、2019年の令和元年台風第19号を上回る水準となった。2020年12月、大雪に伴う倒木等により、兵庫県北部及び新潟県を中心に停電が断続的に発生し、兵庫県内では最大約9,220戸の停電が発生し倒木による立入困難箇所等により停電の解消までには時間を要した。大規模な自然災害が発生した際、災害情報を求めて、地方自治体のウェブサイトへのアクセスが集中し、つながりづらい状態が過去と同様に生じた。

災害時のアクセス集中時においては、円滑なコミュニケーション手段の提供が重要である。

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」）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　東京大会に向けた取組から得られた知見等の活用

新型コロナウイルス感染症の拡大の状況等を踏まえ、東京大会は１年延期が決定された。大会に向けたサイバーセキュリティ確保のための取組は、この１年で更に深化したものの、

サイバーセキュリティを取り巻く情勢は刻一刻変化していることから、新たに発生・判明した事象等を踏まえて大会に臨む必要があり、そのような変化に迅速かつ的確に対応できるような敏捷性と発生した事象を俯瞰的に見た上で解決しようとする姿勢が求められる。

特に、多くの重要サービス事業者等においてもテレワークが実施されるようになり、新たに必要となるセキュリティ対策や対処態勢を検討することもできない中で、テレワーク環境を構築・運用せざるを得ない重要サービス事業者等も少なくないと想定される。そのため、テレワーク環境下においても、従前から実施している対策・態勢が有効に機能するかどうかを確認するような取組をすすめている。

2018年戦略において「未来につながる成果の継承」として言及されている、整備した仕組み、その運用経験及びノウハウをレガシー化するための検討については、大会終了後に詳細な結果を整理した上で正確な評価を行うことが重要である。しかしながら、大会後に結果の整理を開始したのでは、レガシーとなり得る現在の取組を長期間に渡り止めてしまうことになり、取組の継続性を損なうことになるため、既に成果が出ている取組については大会後の速やかな実施に向けた検討を開始した。

大会に向けたサイバーセキュリティの確保には、様々な事業者等が異なる役割を担っているが、自力で解決できない課題とその解決に向けた支援のニーズを持っている事業者等も少なくないことから、大会後における取組の検討に当たっても、多様な課題と解決に向けた支援のニーズに対応できるようにすることが不可欠である。

東京大会後における取組の検討に当たっては、単に、リスクアセスメントの手法を全国の重要インフラ事業者等に普及すること、JISP[41]を活用した情報共有体制への参加を希望する組織に拡大することだけでは十分と言えない。大会に向けた取組を定常的・継続的な国の施策に昇華させるためには、多様な経験と高度な知見を有する第三者からの意見も踏まえた検討が必要なことから、2021年1月「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。）を内閣サイバーセキュリティセンター長主催の私的懇談会として設置し、次の基本方針により検討を重ねている。

- 国内組織（経済社会を支える組織とそれを支えるベンダー）が、必要最低限のサイバーセキュリティを確保できること、最近のサイバー攻撃事情（APT激化やSPC攻撃）に対応できることを目指し、東京大会向けに構築した対処体制を継続的なものとし、重大なインシデント発生時等に関係組織が一丸となって対処可能となるようにする。
- デジタル化の機会と影響があらゆる主体に例外なく及び、セキュリティインシデントの与える影響の範囲、深刻度が増大する中、セキュリティ対策の強化が急務となる領域等に対して、東京大会に向けて取り組んだリスクマネジメントを始めとした効果的なセキュリティ対策の支援を継承する。
- 公益性の高い取組に重点化するなど、民間における取組との切り分けを意識しつつ、メリハリをつけて取組を進める。

[41] JISP（Japan cyber security Information Sharing Platform）

・大規模国際イベントにおけるサイバーセキュリティ上のリスクの高まりを踏まえ、東京大会に向けた取組で得られた知見、ノウハウを活用して大規模国際イベントのセキュリティ対策を促進する。

サイバー空間におけるリスクの高まりを踏まえ、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、大規模サイバー攻撃事態等に対する即応力を確保する。

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活かすことで、大阪・関西万博をはじめとする、今後の大規模イベントの際はもちろんのこと、我が国のサイバーセキュリティの確保に関する全体的な能力の底上げを推進する。

全世界的に影響を与えたサイバーセキュリティ事案等をきっかけに設置されたサイバーセキュリティ協議会、東京大会を機に設置されたサイバーセキュリティ対処調整センター等の情報共有体制間の連携を進め、外部組織との連携や調整の在り方について具体的に検討する。

例えば、分野・課題などに応じた情報共有・連携体制を確立するとともに、それらを有機的に連携させ、多層的かつ包括的なサイバー防御に資する情報共有・連携体制を整備していく。

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。

3章　サイバー空間に係る国際的な動向

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

米国においては、2020年度には、SolarWinds社Orion製品やMicrosoft Exchangeサーバ等の脆弱性について連邦政府機関に対して対応を求める５度の緊急指令が発出された 。特に2020年12月に緊急指令が発出されたSolarWinds社Orion製品の脆弱性を悪用した攻撃に関しては、ロシア起源であると見込まれる旨の発表をした。2021年１月にはバイデン政権が誕生し、2021年３月に公表された国家安全保障戦略暫定指針においては、サイバーセキュリティを最優先事項として位置づけ、同盟国とのパートナーシップの価値を強調し、民間部門との連携を重視するとされた。加えて、2021年度国防授権法により、ホワイトハウスにナショナル・サイバー・ダイレクターを新設することとされており、政府全体としての体制や取組の強化が図られている。5Gについては、2020年６月に連邦通信委員会により、ファーウェイを安全保障上の脅威にあたる企業として、米国政府から補助金を受けた米国内の通信企業に対し、同社製品の購入を禁じる規制を施行した。同年８月には、ファーウェイを含めた中国企業５社の製品を利用する企業と米国政府機関が契約することを禁じる規制が施行された。

EUにおいては、2020年12月に新たなサイバーセキュリティ戦略が公表された 。オープンなインターネットやサプライチェーンを巡り地政学的な緊張が脅威と切り離せず、サイバー攻撃・偽情報というハイブリッドな脅威も顕在化する中で、Thinking Global, Acting European と打ち出した上で、①強靱性、技術主権とリーダーシップ、②防止、抑止、対処のための運用能力の構築、③協力強化を通じたグローバルでオープンなサイバー空間の推進、④欧州関係機関におけるサイバーセキュリティの確保を行うこととしている。2021年５月、ロシア連邦軍参謀本部情報総局（GRU）の一部門や中国、北朝鮮の企業など４組織・計８名を対象として、サイバー攻撃に対する制裁措置の発動を決定し、EUへの渡航禁止や資産凍結を科す他、制裁対象への資金提供も禁止した。また、2020年10月、2015年のドイツ連邦議会へのサイバー攻撃を理由として、GRUの一部門及び２個人に制裁措置を発動した。

英国においては、2021年３月に「安全保障、防衛、開発及び外交政策の統合的見直し」が実施された。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見込みとしつつ、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・抑止といった５つの優先事項を掲げている。5Gについては、2020年７月、同国の5G整備からファーウェイの機器を2027年末までに段階的に排除する方針を掲げた。

豪州においても、2020 年８月にサイバーセキュリティ戦略が公表され、「豪州市民、ビジネス、皆が依存する必要不可欠なサービスにとってより安全なオンライン社会」をビジョンとして、10 年に渡り 16.7 億豪ドルを本戦略に基づき投資予定とし、特に重要インフラ防護を強化する方針としている。

中国については、2020年７月、データ活動に対する安全審査やデータの輸出規制についての規定を設ける中国データセキュリティ法（草案）が公表された。加えて、2020年９月にはデー

タセキュリティリスクに対処するための３つの原則を掲げるグローバルデータセキュリティイニシアティブを発表している。

ロシアについては、2016 年 12 月、「情報安全保障ドクトリン」を公表し、サイバーセキュリティ政策の方向性を明示している。

北朝鮮については、2021 年３月には、国連安全保障理事会の北朝鮮制裁委員会専門家パネルが北朝鮮に対する国連安保理決議の履行状況に関する最終報告書を発表し、北朝鮮がサイバー攻撃により他国の軍事技術への違法なアクセスや金融機関、暗号資産取引所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等金銭窃取を行っていることが指摘されている。

加えて、サイバー分野における多国間連携も活発である。2019 年 10 月には ASEAN・米サイバー政策対話の共同議長声明が 、2019 年８月にはサイバーセキュリティ協力に関する ASEAN・EU 声明が 、さらに 2020 年 12 月には、第１回 ASEAN・中国サイバー対話における共同議長声明が発出されている 。

サイバー空間における国際法の適用については、サイバーセキュリティに関する国連政府専門家会合（GGE）は、2018 年国連総会決議に基づき、2019 年に第６会期が立ち上がり、2021 年５月に報告書が採択された。また、2018 年国連決議に基づき、サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG）が立ち上げられ、2021 年３月に全会一致で報告書が採択された。

2019 年 G20 大阪サミットで日本が提示した DFFT[42]（信頼性のある自由なデータ流通）については、2020 年 G20 リヤド・サミットにおいても、首脳宣言において、デジタル技術はパンデミックの対応を強化し、経済活動の継続を促進する上で鍵となる役割を果たしてきたとされ、DFFT 及びデジタル経済を促進することの重要性が認識された。加えて、デジタル経済の安全性を促進することの重要性を認識し、「デジタル経済におけるセキュリティに関するＧ20 事例集」を歓迎することとなった。

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、国際社会全体との連携や協力、法の支配によるサイバー空間の安定化を進めていくことが不可欠であることから、我が国としてもこうした法の支配の推進に積極的に寄与し、国際連携を進めていくとともに、各国の動向を踏まえ、国内のサイバーセキュリティ対策を強化していくことが必要である。

[42] DFFT（Data Free Flow with Trust）

4章　横断的施策

1　研究開発

サイバーセキュリティ分野におけるアカデミックな研究が国際的に急成長している。トップカンファレンス[43]での論文投稿は、2000年に比し約4倍以上となる2000本超が毎回投稿される規模[44]となっており、採択を巡って切磋琢磨が行われている。

アカデミックな研究にあって、プレーヤーは、コンピュータサイエンスを主導してきた米国主要大学に留まらない。大手IT企業や欧州等の大学等が参画しており、これらプレーヤーの国際共著論文や産学共同研究などコラボレーションが非常に活発になっている。

また、コロナ禍で明らかになったように、我が国のデジタル化は焦眉の急であるが、サイバーとリアルが融合するSociety5.0において、多様なイノベーションによりデジタル化がもたらすメリットを最大化できるよう、サイバーセキュリティの確保が求められている。国際的にも、科学的基礎に基づくセキュリティ対策がより重要性を増すと考えられるところ、アカデミックな研究の発展への期待は高く、産学官連携の機会とポテンシャルは小さくないと考えられる。

こうした取組促進の観点も踏まえ、組織・分野の枠を超えた時限的な研究体制（ネットワーク型研究所）を構築する、国立研究開発法人科学技術振興機構（JST）の「戦略的創造研究推進事業（新技術シーズ創出)」では、令和３年度の７つの戦略目標のうちの１つとして、サイバーセキュリティ分野に関連する「Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術」が定められており、今後、サイバーセキュリティ分野の研究者による活用が期待される。

我が国として推進すべき実践的な研究開発については、「サイバーセキュリティ研究・技術開発取組方針」[45]に基づき、各府省庁を中心に取組が進められているが、研究開発の推進にはIT関連技術の進展に応じた観点も重要と考えられる。中長期的な視点から技術トレンドを捉え研究開発を推進していくことが重要であり、特に、AI（人工知能）技術・量子技術の進展を見据えた対応が求められている。

AI（人工知能）技術については、近年、加速度的に発展しており、世界の至るところでその応用が進むことにより、広範な産業領域や社会インフラなどに大きな影響を与えている。サイバーセキュリティとの関係では、図表１－２－９の通り、（ａ)AIを活用したサイバーセキュリティ対策、（ｂ）AIを使ったサイバー攻撃、（ｃ）AIそのものを守るセキュリティの3つの観点があると考えられる。

図表１－２－９　AIセキュリティに関する研究動向[46]

[43] 国際的に著名でアカデミックな研究発表の場として主要と考えられている研究集会（カンファレンス)。サイバーセキュリティに係る分野では、IEEE Security & Privacy、ACM CCS、USENIX Security、NDSS の四つがそれに当たるほか、そのうち暗号研究分野では、Crypto、Eurocrypt が著名。これらのカンファレンスでは、論文が投稿された後、ピアレビューで査読され採択されたもののみが論文（プロシーディング論文）として研究発表される。

[44] “System Security Circus v2.0” （2021年5月7日） http://s3.eurecom.fr/~balzarot/notes/top4_v2/

[45] 2019年5月19日 研究開発戦略専門調査会決定

[46] 第14回研究開発戦略専門調査会（2020年11月25日）資料
https://www.nisc.go.jp/conference/cs/kenkyu/dai15/pdf/15shiryou0202.pdf

量子技術については、近年、国際的な注目が急速に高まっており、米国、欧州、中国をはじめ、将来の経済・社会に大きな変革をもたらす源泉あるいは革新技術として位置づけ、国を挙げた取組が推進されている状況にある。量子コンピュータの進展により、現代のインターネットセキュリティを支える公開鍵暗号技術が解読される可能性が生じ、国際的に耐量子計算機暗号に関する検討が進められている。一方、耐量子計算機暗号においても危殆化のリスクがあるため、米国や中国をはじめ、各国が安全保障にも関わる重大脅威との認識の下、原理的に安全性が確保される量子通信・暗号に関する研究開発を急速に進めている。

我が国においては、大手 IT 企業による世界最高速の BB84 量子暗号装置の製造や、大学などによる耐量子暗号アルゴリズムを含む理論研究、さらに量子鍵配送ネットワークのテストベッドの長期運用実績など、世界をリードする様々な取組がなされている。

さらに、「量子技術イノベーション戦略（最終報告）」[47]に基づき、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要デジタル情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発や、その事業化・標準化等に取り組んでいる。

2　IT・セキュリティ人材

他国と比べても、我が国においては、セキュリティ対策に携わる人材の不足感が大きいと言われて久しいが、セキュリティ対策に当たる実務者層・技術者層の育成は一定の取組の進展が見られる。一方で、例えばユーザ企業（非 IT 企業）では、IT 人材の不足傾向が拡大して

[47] 2020 年 1 月 21 日統合イノベーション戦略推進会議決定

おり（IT 人材が大幅に不足していると回答した企業の割合：(2015 年度）20.5% ⇒（2019 年度)33.0%）[48]、セキュリティ人材も同様の傾向と推測される。

セキュリティ対策に携わる人材の不足感について人材種別でみると、「セキュリティリスクを評価・監査する人」や「ログを監視・分析する人」以上に、「セキュリティ戦略・企画を策定する人」が不足しているとのデータ[49]も存在する。様々な有識者からも、「セキュリティを全社的にリードし社内調整を進められる人材が必要」「ある業界では現場の技術者は足りてきているが、知見を有する戦略マネジメント層等が不足」といった指摘[50]がなされている。

スペシャリストが必要な領域はベンダー企業に入ってもらうことも一般的である一方、中長期的にはユーザ企業におけるデジタル対応能力が企業の競争力の源泉になっていく、との見通しもある中で、セキュリティ対策を内製化していくことも求められるであろう。このため、中長期的な観点から、企業・組織内部において、セキュリティ対応を全社的にリードし社内調整を進められる人材が必要になると考えられる。また、人材の不足感や取組状況は業界ごとに状況が異なるが、今後は業種や企業規模を問わず、様々な企業においてこうした人材面での要請は高まるであろう。

なお、人材の不足感に関する調査においても不足数のうち多くが、ユーザ企業（非 IT 企業）の情報システム部門に所属していない人材であると試算されている[51]。

また、人材の不足感のみならず、現状の IT・セキュリティ人材の所在をみてみると、我が国においては特に、ベンダー企業に固定化・偏在している状況がみてとれる（日本ではベンダー企業に 72.0%（約 75 万人）が所在しているのに対し、米国では 34.6%（約 145 万人）というデータが存在する）[52]。一方で、我が国におけるユーザ企業のデジタル化の進展にあわせて、セキュリティ対策が確保されるためには、中長期的な観点から人材育成はもちろん、即戦力となるこれら人材の流動性の向上やマッチングの機会の確保に取り組む必要がある。

こうした新たなセキュリティ人材の流動モデルの一つとして、副業・兼業といった新たな形態の活用が考えられる。副業・兼業を希望する者は増加傾向にあり（2002 年の 182 万人から、2017 年には 230 万人に増加）[53]、デジタル化の推進に応じて今後更に増加することが見込まれる。コロナ禍への対応を余儀なくされることなどから、テレワークの浸透にとどまらず、副業・兼業といった新しい形態での雇用のあり方もその素地が整いつつある[54]。

また、今後、公的機関においては、デジタル改革に伴い、中央省庁における「民間、自治体、政府を行き来しながらキャリアを積める環境整備」が進展するとともに、特に地方においても、「GIGA スクール構想」の推進や、自治体における DX の推進に応じて、IT・セキュリティ人材に対する需要も現に表れてきており、人材側の関心も高まっていると考えられる（民

[48] (独)情報処理振興機構「人材白書 2020」(2020 年 8 月 31 日)　https://www.ipa.go.jp/jinzai/jigyou/about.html
[49] NRI セキュアテクノロジーズ(株)「企業における情報セキュリティ実態調査」における複数年の調査結果を確認。
[50] 普及啓発人材育成専門調査会（2021 年 1 月 21 日）議事録より抜粋。
[51] 経済産業省「IT 人材の最新動向と将来推計に関する調査結果」(2016 年 6 月 10 日)
[52] (独)情報処理推進機構「IT 人材白書 2017」(2017 年 4 月 25 日)　https://www.ipa.go.jp/files/000059087.pdf
[53] 総務省「就業構造基本調査」(2018 年 7 月 13 日)
[54] 従来、「副業・兼業」を認めるに当たっては、労働時間管理のあり方が論点になっていたが、2020 年 9 月に厚生労働省が「副業・兼業に関するガイドライン」を改訂し、「労働時間の自己申告制を設け、申告漏れや虚偽申告の場合には、兼業先での超過労働によって上限時間を超過したとしても、本業の企業は責任を問われない」ことを明確化。今後、ガイドラインの分かりやすいパンフレットや、労働時間の申告の際に活用できる様式の丁寧な周知等を図っていくこととされている。

間人材の約8割が官公庁での仕事に興味があり、うち3割が「副業・兼業」を希望するとのデータも存在する）[55]。

一方で、サイバー攻撃による脅威が巧妙化・複雑化し、海外ではインフラや制御系システムを狙った攻撃も見られている。米国の都市水道局の例では、水道における産業用制御系システムを対象とした不正アクセスによって、飲用水に含まれる水酸化ナトリウムの量が一時的に通常の約100倍に上昇した。この事例では、オペレーターが異常に気付き即座に設定を戻したため、実際の被害はなかったとされる[56]が、被害範囲の拡大を抑止するためにも、こうした産業分野において実践的に対処する人材が今後ますます必要とされる。

最後に、セキュリティ人材のダイバーシティについてみてみると、IT・サイバーセキュリティ分野における幅広い人材確保の観点から、IT人材全体では女性割合が徐々に増加しているものの、高い水準にあるとは言えない（IT人材に占める女性の割合が0%である企業は、IT企業で8.2%、ユーザ企業のIT部門で33.0%）[57]。なお、日本国外ではサイバーセキュリティにかかわる戦略においてジェンダーバランスに言及されている例もあり、例えば、英国では「サイバーセキュリティ分野におけるジェンダー不均衡に対処し、才能を発揮できるよう、より多様なバックグラウンドを持つ人々を採用する」と政策文書に明記されている[58]。

3　国民の意識・行動

IPAが発表している「情報セキュリティ10大脅威 2021」[59]によれば、2020年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案は、大企業をはじめとする堅牢なセキュリティ対策を講じている組織を狙った高度な技術を用いたサイバー攻撃だけでなく、標的型メール攻撃やランサムウェアおよびビジネスメール詐欺、また新型コロナウイルス関連のものを含む不審メールや不審サイトによる個人情報の搾取といった、セキュリティ対策の行き届いていない中小企業や一般国民の心の隙を突く古典的・比較的単純な攻撃も衰える気配はない。例えば、インターネットバンキングにおける不正送金の発生件数は高止まりしている（2019年：1,872件、2020年：1,734件）[60]。

一方で、こういった脅威による被害を防止・低減するためのセキュリティソフトやサービス、ファイアウォール機器やセキュリティゲートウェイ機器の利用といった基本的な情報セキュリティ対策の実施状況は、個人・組織ともに十分な水準には至っておらず（フィッシングや詐欺サイトへのアクセスを防止するセキュリティソフトやサービスの利用率：39.2%、ファイアウォール機器やセキュリティゲートウェイ機器の利用率：34.1%）[61]、インターネット利用に関連するトラブルに不安を感じる人の割合も年を追うごとに増加の傾向を見せてお

[55] (株)ビズリーチ調査（2020年12月7日）　https://www.bizreach.co.jp/pressroom/pressrelease/2020/1207.html
[56] 経済産業省 第8回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）第6回 WG1分野横断サブワーキンググループ 合同会議（2021年3月15日）
[57] (独)情報処理振興機構「人材白書2020」（2020年8月31日）　https://www.ipa.go.jp/jinzai/jigyou/about.html
[58] “National Cyber Security Strategy 2016 to 2021”（NCSC, 2016）
[59] (独)情報処理推進機構（2021年3月26日）　https://www.ipa.go.jp/security/vuln/10threats2021.html
[60] 警察庁「令和２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」（2021年3月4日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf
[61] IPA「2020年度 情報セキュリティの脅威に対する意識調査」概要報告書
https://www.ipa.go.jp/files/000088916.pdf

り（2016年：61.6%、2017年：66.8%、2018年：70.7%、2019年：75.0%）[62]、引き続き国民一人一人による着実な意識・行動の強化が必要な状況である。

この現状は、各府省庁が実施しているサイバーセキュリティに関する各種普及啓発施策が、国民に対して十分に行き届いていない、あるいは意識・行動の強化に向けた具体的な行動にまで繋げられていない結果とも推測される。若年者や高齢者、中小企業が取り組むべき基本的事項を確実に実行するため、何を、どうすればよいか、より具体的に分かりやすく伝えることで、実際の行動変容を促し、セキュリティ対策を広く普及していくための取組を、各府省庁や関係機関と連携して更に強化していく必要がある。

[62]（独）情報処理推進機構「2016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」（2017年8月8日）
https://www.ipa.go.jp/security/fy28/reports/sme/

2部　我が国のサイバーセキュリティ政策

1章　基本的な枠組み

基本法第12条に基づき策定された2018年戦略は、策定後３年間を計画期間としており、2021年に計画期間を終えることから、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、基本的な考え等と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盛り込んだ新たな戦略を2021年に決定する見込みである（以下「2021年戦略」という。）。

今般、国は、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」というデジタル社会のビジョンを掲げ、デジタル改革を推進している。2020年12月25日には、「デジタル社会の実現に向けた改革の基本方針」を閣議決定し、「IT基本法（中略）の全面的な見直しを行うとともに、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新たな司令塔としてデジタル庁（仮称）を設置する」とした。これを踏まえて、2021年2月9日に「デジタル社会形成基本法案」「デジタル庁設置法案」等が第204回通常国会に提出され、2021年５月12日可決成立し、2021年９月１日にデジタル庁が設置される。

国民一人ひとりが安心して参加できるデジタル社会を形成するためには、デジタル技術の悪用への対応も求められており、サイバーセキュリティの確保を図ることとされている。以下、サイバーセキュリティ基本法と、戦略及び、我が国のサイバーセキュリティ政策の推進体制について概説する。

1　サイバーセキュリティ基本法について

サイバーセキュリティ基本法は、デジタル社会形成基本法（同法が2021年９月１日に施行されるまでは高度情報通信ネットワーク社会形成基本法）とあいまって、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もの（同法第１条）であり、サイバーセキュリティという概念を法的に位置付け（同法第２条）、総則（基本理念や国や地方公共団体といった関係者の責務や国民の努力等）、サイバーセキュリティ戦略、基本的施策に関する規定等から構成されている。また、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、内閣に、サイバーセキュリティ戦略本部を設置することを規定している（同法第25条）。

同本部の所掌事務として具体的に明記されている主なものを抜粋すると、以下のとおりである（同法第26条第１項各号）。

①サイバーセキュリティ戦略の案の作成

②国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく監査

③国の行政機関、独立行政法人及び指定法人で発生したサイバーセキュリティに関する重

大な事象に対する原因究明調査

④サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整

⑤その他サイバーセキュリティに関する重要施策に関する、企画に関する調査審議、施策の実施の推進及び総合調整

また、基本法は、「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全の確保並びに我が国の安全保障に寄与すること」を目的としている（同法第１条）。戦略においても、この３つの領域に政策目的を整理し、それぞれの目的に沿って、施策を推進している。

2　サイバーセキュリティ戦略について

2021 年戦略は、基本法に基づき、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に策定した 2015 年戦略、2018 年戦略に続いて改定するものであり、基本法に基づく３回目の「サイバーセキュリティに関する基本的な計画」である。

その位置づけと狙いは、我が国が 2020 年代初めの今後３年間にとるべき諸施策の目標と実施方針を国内外に示すものであると同時に、未曽有のコロナ禍への対応から得られた教訓、デジタル改革、そして東京大会という世界的イベントでの対応を通じた経験や安全保障環境の変化等の時代認識を踏まえ、我が国としてのサイバーセキュリティに取り組む決意を、あらゆる主体、各国政府、攻撃者に対して発信するものである。

戦略では、これらの時代認識からサイバー空間をとりまく課題認識を整理し、特にデジタル改革の推進にあたっては、サイバー空間の公共空間化が進展し、またサイバー空間において提供される多様なサービスは、クラウドの普及やサプライチェーンの複雑化等により、各主体間の相互連関・連鎖の関係がより進展することから、従来の戦略で掲げた５つの基本原則（①情報の自由な流通の確保、②法の支配、③開放性、④自立性、⑤多様な主体の連携）を堅持しつつ、加えてこれまで以上に必要性が増している「自由、公正かつ安全なサイバー空間」の確保を目指すという基本的な考えも堅持し、基本法に掲げた目的を達成するための施策を示している。

政府は、戦略を確実に実行するため、サイバーセキュリティ戦略本部の下、関係府省庁が連携して、年次計画に基づき、サイバーセキュリティ政策の推進に取り組んでいくこととしている。

3　サイバーセキュリティ政策の推進体制について

サイバーセキュリティの確保を通じて、情報通信技術及びデータの利活用を促進し、経済・社会活動の基盤とすること、我が国の安全保障を万全のものとすることは、従来からの我が国政府の方針である。この方針の下、政府においては、関係機関がそれぞれの機能を果たし、

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ことが肝要である。

そのサイバーセキュリティ対策の推進体制としては、2000年の省庁ホームページ連続改ざんの事案を機に、内閣官房に情報セキュリティ対策推進室が設置され、政府機関対策と重要インフラ対策を二つの柱として、情報セキュリティに関するガイドラインや行動計画が策定され、2005年に同推進室が情報セキュリティセンターに改組された。

その後、基本法に基づくサイバーセキュリティ政策の推進体制として、内閣官房長官を本部長とするサイバーセキュリティ戦略本部が2015年１月に内閣に設置された。同本部は、IT政策を所管する高度情報通信ネットワーク社会推進戦略本部（デジタル庁発足後は廃止）と、安全保障政策を所管する国家安全保障会議と緊密に連携して、閣僚本部員５省庁（デジタル庁発足後は６省庁）やサイバーセキュリティの確保がもと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、同本部の事務局として、NISCが内閣官房に設置されており、同センターを中心に関係機関の一層の能力強化を図るとともに、同センターにおいて、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。

なお、デジタル庁発足以降において、デジタル庁はデジタル社会の形成に関する重点計画を作成する中で、「サイバーセキュリティの確保等に関し政府が迅速かつ重点的に講ずべき施策」も定めることとされており、サイバーセキュリティ戦略本部の意見を聴くこととされている（デジタル社会形成基本法案第37条第２項第14号、第４項）。また、デジタル庁は情報システムの整備・管理の基本的な方針を策定することとなるが、この中でサイバーセキュリティに関する基本的な方針も示されるところ、当該部分については、デジタル庁がサイバーセキュリティ戦略本部と緊密に連携して作成することとされている。

２章　戦略に基づく昨年度の取組実績、評価及び今年度の取組

2020 年度のサイバーセキュリティ関連施策の取組実績及び評価について、別添２は現行戦略の体系に沿って整理しているが、本章は年次報告と年次計画の一連の流れを示すため、2021 年戦略の体系に沿って整理している。

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

【昨年度の取組実績】

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うことで更なる組織能力の向上を図るため、「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、普及啓発を促進しており、当該ガイドラインのダウンロード数は、2021 年１月末時点で 10 万件を超えた。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」の普及を実施し、IPA がプラクティス集の課題やニーズに関する調査を実施し、来年度以降の強化の方向性を確認した。また、更なる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、「経営ガイドライン実践状況の可視化ツール」のβ版を策定し、それを基にユーザ企業及び投資家等ステークホルダーへのヒアリングを実施した。その結果を踏まえ、Ver1.0 の策定に着手した。

また、2019 年６月に公表された「グループ・ガバナンス・システムに関する実務指針」において、グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方が位置づけられたことを踏まえ、講演での周知等を通じて、企業による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実践を後押しした。さらに、サイバーセキュリティへの経営層の関与を引き続き促進するため、投資家等との意見交換などを通じ、取締役会のサイバーセキュリティへの関与の促進や投資家に対するサイバーセキュリティの啓発を実施した。

加えて、「サイバーセキュリティ対策情報開示の手引き」の普及を図るため、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総務省が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。当該分科会は、日経 225（日経平均株価銘柄）を対象に開示情報から各社のサイバーセキュリティの取組姿勢に関する調査を行い、2020 年 11 月に調査結果を公表した。

【評価】

サイバーセキュリティ経営ガイドラインの普及および各社のサイバーセキュリティ経営実施状況の共有について、サイバーセキュリティ経営ガイドラインの普及促進（Step 1）は着実に推進している。さらに、自社状況の可視化（Step 2）、投資家等ステークホルダー向け可視化（Step 3）に向けた可視化ツール開発も進行している。

今後は、これらの手引きやツール等の活用促進とともに、整備が進んでいるデジタル経

営の推進に向けた各種インセンティブ施策と連動し、サイバーセキュリティに係る取組の可視化等が更に進むことが重要である。

また、経営層が自社の競争力の源泉たるデジタルサービス等に内在するリスクの所在を適切に把握できるようにする観点から、必要な「プラス・セキュリティ」知識を補充できる環境整備を推進することが重要である。

【今年度の取組】

「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。また、サイバーセキュリティ経営ガイドライン実践のため、「経営ガイドライン実践状況の可視化ツール Ver1.0」の開発・リリース、その利用促進を行い、を企業内での取組の可視化及びステークホルダーに対する取組の可視化を推進する。また、「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」の改訂と普及啓発を実施する。

また、「取締役会の実効性評価」にサイバーセキュリティを盛り込むことの重要性を引き続き周知するとともに、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。

加えて、「サイバーセキュリティ対策情報開示の手引き」の活用促進に向けた取組を引き続き継続する。

上記の取組を踏まえ、特にデジタル化に取り組む企業におけるサイバーセキュリティに係る取組状況について、適切に状況調査・フォローアップを行い、取組推進に当たっての課題の把握に努める。また、経営層に必要な「プラス・セキュリティ」知識を補充できる環境整備に向けて、モデルカリキュラムの構築を推進する。

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

【昨年度の取組実績】

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・プラットフォームについて、2020 年度は新型コロナウイルス感染症の拡大防止を留意しつつオンラインで計４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行った。地域に根差したセキュリティ・コミュニティ（地域 SECUNITY）の形成を促進するため、経済産業局や総合通信局が地域の業界団体・事業者、セキュリティ関係機関、保険会社など連携し様々な主体の連携によるセミナーや演習などを実施した。

また、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った。同制度の三大都市圏を除く地域における普及を目的として 18 箇所で普及セミナーを実施したほか、地域の団体組織等の主催するセミナーについても 72 箇所に対し講師を派遣し、同制度の普及を図った。自己宣言者数は全国で 112,966 件（一つ星：98,637 件、二つ星：14,329 件）に増加し、このうち三大

都市圏を除く地域においても自己宣言者数は48,668件となった。

損害保険会社、ITベンダー、地元の団体等の連携による中小企業向けのセキュリティサービス（サイバーセキュリティお助け隊サービス）の実証について、2019年度の実証で得られた知見を基に、地域特性・産業特性等を考慮したマーケティング、機器・ソフトウェア・サービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、全国13地域と2業種で実施。約1,100社の中小企業が実証に参加し、中小企業におけるセキュリティ対策の課題や、産業別でのセキュリティ対策の実態等が明らかになった。

中小企業における情報セキュリティ投資促進の施策として、セキュリティにも配慮した安心安全なクラウドサービス利用の促進等のために、スマートSMEサポーター（中小企業のIT活用を支援するITベンダー等）として認定した事業者について、特設サイトにて「クラウドサービスの安全・信頼性に関する情報」「セキュリティ対策状況」「利用終了時のデータの取扱い」等を開示し、中小企業に情報提供を行った。また、セキュリティ対策の普及啓発を行うとともに、専門家等を派遣して、セキュリティマネジメント指導を395社の中小企業に対して実施した。

中小企業におけるセキュリティ対策強化に資するため、「中小企業の情報セキュリティ対策ガイドライン」の普及を図るとともに、実践に関する企業内及び地域で活躍する指導者の拡大に向けた「講習能力養成セミナー」を全国12箇所において開催・録画配信（オンデマンド形式）し、中小企業の経営者、社内教育担当者等合計約400名が参加、オンデマンド形式による録画配信についても約550名が視聴した。商工団体・税理士会・社会保険労務士会等の指導員等を対象とする研修会、警察・自治体・中小企業団体等が主催する中小企業向けセミナー等30箇所以上に講師を派遣した。

【評価】

コロナ禍への対応を余儀なくされること等を通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域・中小企業、そしてサイバー空間とは繋がりのなかった業種・業態の企業にも例外なく広がっていくと想定される。一方で、中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たっては、セキュリティ専任の人材を配置できないなど、知見や人材等のリソース不足に直面しており、これらの課題への対処が必要である。

このため、地域でのコミュニティづくりや、中小企業が利用しやすい安価かつ効果的なセキュリティサービス・簡易サイバー保険の普及に向けた取組をさらに発展させ、持続的な体制を構築することが重要である。

【今年度の取組】

「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ことが重要である。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、経済産業局、総合通信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等を引き続き実施する。

また、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」の商標使用権を付与するスキームを構築し、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）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や情報セキュリティへの投資、民間のお助け隊サービスの普及支援を推進していく。また、「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とともに、中小企業のみならず発注元となる大企業等においてもより有意義なものとなるよう制度の在り方についても検討を進める。

このほか、「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とともに、スマート SME サポーターとして認定した中小企業への情報提供等の取組を進める。今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定されるところ、上記ガイドラインの普及を通じてクラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。

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

【昨年度の取組実績】

サプライチェーンの信頼性確保に向けては、経済産業省産業サイバーセキュリティ研究会において、これまでに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である「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 2019 年４月に策定するとともに、産業界におけるセキュリティ対策の具体化・実装の促進に向けて、当該フレームワークに基づき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が進められている。また、2020 年 11 月に、大企業と中小企業がともにサイバーセキュリティ対策を推進するために設立された「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)」による、サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底などを含む「基本行動指針」の実践と地域・中小企業を含めたサプライチェーンのサイバーセキュリティ対策などの産業界全体の活動を支援。

データ流通における信頼性確保に向けては、前述の産業界におけるセキュリティ対策の具体化・実装を促進に向けた取組の一つとして、経済産業省産業サイバーセキュリティ研

究会第３層タスクフォースにおいて、主体間を転々流通するデータに関するリスクポイントの洗い出しを可能にする観点から、データマネジメントに関する定義を明確化し、フレームを設定する取組が進められている。また、各種「トラストサービス」については、タイムスタンプについては、2021 年４月に「時刻認証業務の認定に関する規程」を公布、国による認定制度が整備された。e シールについては、e シールの利用が有効なユースケースや我が国の e シールの在り方等について検討が行われており、その結果を踏まえて、今後、技術上・運用上の基準等を整理した指針が作成される予定である。電子署名については、リモート署名の電子署名法上の位置づけが示されるなど、電子署名法上の電子署名の利便性の改善に向けた取組が実施されている。

我が国セキュリティ製品・サービスの信頼性確保に向けては、「情報セキュリティサービス審査登録制度」の運用やそのサービスリストの改善が進められているほか、包括的なサイバーセキュリティ検証基盤を構築する「Proven in Japan」促進に向けた取組が進められている。具体的には、セキュリティ製品の有効性検証・実環境における試行検証を実施しそのアプトプットを「コラボレーション・プラットフォーム」で発表、ビジネスマッチングを行ったほか、攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた「手引き」の作成等を実施した。

先端技術・イノベーションの社会実装に向けては、例えば、SIP 第２期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」において、IoT 機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、IoT システム・サービス及びサプライチェーン全体のセキュリティを確保することを目的とした各種研究開発、社会実装に向けた取組が進められている。また、海外展開に向けて、サイバーセキュリティ製品に関する世界最大のビジネスカンファレンスである米国「RSA Conference」への出展支援や、IoT セキュリティに関する国際標準化に向けた取組を継続的に実施している。

【評価】

サイバー空間と実空間が高度に融合する Society5.0 の実現に向けて、今後は、あらゆる主体が相互連関・連鎖を自由に形成することで新たな価値を創造することが期待される。一方で、その信頼性を確保する観点から、このように新たに形成される相互連関・連鎖の下で生じる課題に適切に対応していくことが必要となる。

「サイバー・フィジカル・セキュリティ対策フレームワーク」等も踏まえ、我が国において、新たな価値創出を支えるサプライチェーン等の信頼構築の基盤となる、サイバーセキュリティ確保に向けた取組を進める必要がある。

【今年度の取組】

サプライチェーンの信頼性確保に向けては、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引き続き進めるとともに、上記の「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」の取組を引き続き支援する。具体的には、当該コンソーシアムと連携し、前項に示した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スキームの活用を、コンソーシアムに参加する経済団体、業種別業界団体を通じて、地域・中小企業を含むサプライチェーンを構成する様々な事業者に対して働きかけるとともに、産学官連携や経営層の啓発、地域・業界別の取組等を支援する。

データ流通における信頼性確保に向けては、データマネジメントに関する定義の明確化等を行い、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。また、各種「トラストサービス」については、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。

我が国セキュリティ製品・サービスの信頼性確保に向けては、まず、「情報セキュリティサービス審査登録制度」に基づくサービスリストについて、政府調達等での利用促進に向けた検討を進める。また、検証ビジネスの市場形成に向け、検証の実施に当たり検証事業者・依頼者双方が参照できる「手引き」の詳細化や、検証事業者の信頼性を可視化する取組の検討に取り組む。

先端技術・イノベーションの社会実装に向けては、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、様々な産業分野を念頭に置いた社会実装の促進に取り組むほか、海外展開や国際標準化に向けた取組を継続する。また、NICT を通じて、我が国独自のサイバーセキュリティ情報を国内で収集・生成・提供する「サイバーセキュリティ統合知的・人材育成基盤（通称：CYNEX)」の運用を開始し、産学に開放していく。

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

【昨年度の取組実績】

GIGA スクール構想の実現に向けた取組を踏まえ、内閣官房と文部科学省が連携し、小中学生を対象として、サイバーセキュリティ上注意すべきポイントを効果的に理解できるよう、普及啓発リーフレットを作成した。また、当該リーフレットについてホームページ等を用いて普及啓発を図ったほか、全国の都道府県教育委員会に周知も行った。また、教員等を対象とした情報モラル教育指導者セミナーも実施した。

総務省では、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、団体並びに文部科学省と協力し、全国で 1,208 件の出前講座を実施したほか、2021 年３月に「インターネットトラブル事例集（2021 年版)」を公表した。

経済産業省では、IPA を通じて、第 15 回情報モラル・セキュリティコンクールを開催し、全国の小中高生から、標語作品 45,244 点、ポスター作品 5,383 点、４コマ漫画作品 6,672 点、書写（硬筆）2,570 点、活動事例 12 点、合計 59,881 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 12 校の応募の中から「優

秀活動事例賞」に７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、若年層の情報モラル/セキュリティ意識の醸成と向上に寄与した。

【評価】

GIGA スクール構想の実現に向けては、情報モラル教育指導者セミナーを開催し、学校における情報モラルの指導の徹底の要請が行われている。また、ひろげよう情報モラル・セキュリティコンクールにより、作品を制作する児童・生徒に、インターネットを利用する上での情報モラル/セキュリティについて、意識するきっかけ作りが行われている。さらに、コンクールの応募を基に、学校内での情報モラル/セキュリティの指導教育に力を入れるなど、作品を制作する児童・生徒だけでなく、学校関係者や保護者にもインターネットを利用する上での啓発意識が高まっているほか、受賞作品のパネルは、各地域でのイベント等に貸し出され、一定の評価を得ていると考えられる。

引き続き、若年層への情報モラル/セキュリティ意識の醸成と向上を図るきっかけとして、コンクールへの参加を促していくことに加え、サイバーセキュリティやインターネット利用における注意点に関する普及啓発の取組を推進していく必要がある。

【今年度の取組】

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。

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と共に、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。

文部科学省において、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（セキュリティを含む）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。また、新学習指導要領における情報活用能力の育成に資するため、デジタル活用支援の取組と連動をしながら、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モラル（セキュリティを含む）を含めた情報活用能力を培う教育を一層推進する。さらに、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（セキュリティを含む）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。

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。

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

サイバー空間の公共空間化を踏まえ、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、安心・安全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、様々な取組を推進している。

【昨年度の取組実績】

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）を通じ、脆弱性情報公表に係る制度を着実に実施し、「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した。

経済産業省において、IPA を通じ、NIST 脆弱性対策データベース「NVD」と「JVNiPedia」との連携、CVSS バージョン 3.1 計算ソフトウェアの提供、CVSS 解説動画の公開など、脆弱性対策情報の発信、対策基盤の整備を推進し、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、脅威情報構造化記述形式 STIX の普及啓発を推進し、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。さらに、各種講演等で icat の紹介を行い、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、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」の公開を継続、「企業ウェブサイトのための脆弱性対応ガイド」を改訂し、IPA セミナーにおいて AppGoat を利用した脆弱性解説を行うことで、脆弱性対策の普及促進と AppGoat 利用拡大を図った。

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、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 を通じて実施した。また、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うとともに、ブラウザやウィルス対策ソフト・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エアやサービス 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。さらに、製品開発者に対するミーティングを実施し、CVSS[63]、 CWE[64]の改定や拡充に向けて国内での普及啓発を図るとともに、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った。

[63] CVSS (Common Vulnerability Scoring System)
[64] CWE (Common Weakness Enumeration)

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）等を促進した。具体的には、海外捜査機関の情報をもとに、警察庁、一般社団法人 ICT-ISAC、各 ISP と連携し、2021 年２月下旬よりマルウェア（Emotet）に感染している機器の利用者に対する注意喚起を実施した。また、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。さらに、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た。具体的には、電気通信事業者がフロー情報分析を行い C&C サーバを検知することについて、通信の秘密の規定との関係などの法的課題や技術的課題の本格的な整理・検討に向けて準備を進めた。

内閣官房において、国際標準化機関である ITU-T SG17 及び ISO/IEC JTC1/SC27、SC41 において「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」等を基本とした勧告案及び規格案の検討を促進した。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した。

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、フレームワークの周知・普及、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とともに、2019 年に設置した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、引き続き検討を行った。また、IoT 機器に求められる機能の要求を明確化するとともに、2019 年に設置した第２層タスクフォースにおいて検討を行い、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「IoT セキュリティ・セーフティ・フレームワーク」を策定した。

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）の下で開催したスマートホーム SWG（一般社団法人電子情報技術産業協会スマートホームサイバーセキュリティ WG）を活用して、家電など家庭で使われる IoT 機器のサイバーセキュリティの確保のための必要な対策について、関連する事業者と連携しながら検討を行い、スマートホーム分野のサイバー・フィジカル・セキュリティ対策ガイドラインの案について、パブリックコメントを実施し、コメントを踏まえた検討を進めた。また、IPA を通じ、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の国際標準化について中心的役割を担うとともに、日本の意見を反映させた。WG3 では、ISO/IEC15408 ベースの車載機器のセキュリティ評価基準に関する議論が開始され、エディタとして参加している。また、ハードウェアトロイを検知するハードウェアモニタリング回路の評価手法、多数の開発者が関わる脆弱性の取り扱いに際しての指針、量

子鍵配信のセキュリティ要件及びそのテスト手法に関する標準化についての議論が開始されており、日本からの意見が反映されるよう、国内関係者との情報共有や支援を行っている。

2020 年 11 月に、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を推進するため、産業界が一丸となった「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」を設立した。本コンソーシアムとも連携し、「サイバーセキュリティお助け隊」の商標使用権を付与するスキームを検討した。

総務省において、市場に流通する端末機器（IoT 機器を含む）について、電気通信事業法令に基づく技術基準への適合状況を確認した。また、運用方法や解釈等を定めた「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版）」を 2020 年９月１日に公表した。

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た利用者への注意喚起を行う取組「NOTICE」を実施し、注意喚起対象の検出と電気通信事業者への通知を行った。また、2020 年９月には、調査の際に入力する識別符号を追加等するため実施計画の変更を行った。

2019 年度のスマートシティセキュリティに関する調査結果や有識者会合での検討の結果を整理し、「スマートシティセキュリティガイドライン（第 1.0 版）」として 2020 年 10 月に公表した。その後、国内の先行的なスマートシティのセキュリティ取組の調査や、有識者会合における検討を実施し、様々なユースケースを想定したスコープの整理やスマートシティ特有の観点で考慮すべきセキュリティ事項について整理した「スマートシティセキュリティガイドライン（第 2.0 版）」の改定案及び当該ガイドラインのガイドブック（案）を作成した。また、「スマートシティ官民連携プラットフォーム」の下に設置されている「スマートシティのセキュリティ・セーフティ分科会」において、スマートシティのセキュリティ対策に関するチェックシートのあり方について議論した。

金融庁において、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り組みを行った。

自動運転関連では、国土交通省において、自動車の安全基準の国際調和等を審議する唯一の場である国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論に、独立行政法人自動車技術総合機構交通安全環境研究所と連携のもと参画し、2021 年１月に自動車サイバーセキュリティの国際基準が発効した。またこれと同時に国際基準を国内基準に取り入れた。

また、経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクへの対応に向けて、2018 年度に車両内の電子システムを模擬した評価環境（テストベッド）を構築したところ。2020 年度は、同評価環境をサプライヤー等による部品レベルでの性能評価に利用する方策を検討するなど、活用方法の更なる拡大を図った。

また、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 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についての調査を実施した。

ドローン関連では、2020 年９月に「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」を小型無人機に関する関係府省庁連絡会議の申合せにより決定した。これに基づき、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き換えや、業務の性質等に応じた情報流出防止対策を推進し、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ることとした。また、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。

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、2019 年度に構築した 5G ネットワークの仮想環境を仮想化通信プラットフォーム、MEC（モバイルエッジコンピューティング）仮想化基盤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。

経済産業省及び総務省において、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を 2020 年 8 月 31 日に施行し、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。

「政府共通プラットフォーム第二期整備計画」に基づき、クラウドサービスを活用した第二期政府共通プラットフォームを整備して、2020 年 10 月からサービス提供を開始し、利用システムに対して移行支援を実施した。

安全性が評価されたクラウドサービスの利用に関して、サイバーセキュリティ戦略本部決定（2020 年１月 30 日）において示された基本的枠組みに基づき、2020 年６月に ISMAP の立ち上げを行った。ISMAP においては、2020 年８月にクラウド事業者の監査を行う監査機関を選定・公表するとともに、2021 年３月に、安全性が評価されたクラウドサービスリストの公開を行った。

技術検証体制の整備に向けた事業として、実際の製品に不正機能や当該機能につながりうる未知の脆弱性等が存在しないかどうかの技術的検証の試行を実施した。また、不正機能及び未知の脆弱性に関してその検出方法等の検討に関する技術的な調査を実施した。

サイバー犯罪への対策としては、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各種サイバーセキュリティ関連施策を広報し、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、警察庁ウェブサイトや SNS において、サイバー犯罪の発生状況について広報、注意喚起を行い、警察庁ウェブサイト「@police」において、リモートデスクトップサービスや 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。

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、2021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を推進した。

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　～ネットの落とし穴に踏み込まないで～」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。

警察庁において、2020年中の不正アクセス行為の発生状況等を2021年３月４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。また、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、一般財団法人日本サイバー犯罪対策センター（以下、「JC3[65]」という。）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。

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。都道府県警察において、2020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を活用し、サイバー防犯ボランティア活動への支援を実施した。

警察庁において、解析用資機材を整備し対処能力を強化し、関係会合への参加や技術協力を通じて関係機関との連携を推進し、最新の技術情報を収集しつつ複雑化する不正プログラムの解析を実施した。

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、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を実施した。また、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。

警察庁において、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。

検察当局においては，サイバー刑法の違反事実を含むサイバー犯罪に対し，事案に応じて法と証拠に基づき適切に対応した。

警察庁において、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

[65] JC3（Japan Cybercrime Control Center）

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。また、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キングを推進するため、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。

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対応を行った。

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連携強化を図った。

経済産業省において、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。

経済産業省において、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。

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、必要な対応を行った。

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するなど必要な対応を行った。

【評価】

脆弱性関連情報、フィッシングサイトの URL、マルウェア関連情報、C&C サーバ関連情報、サイバー攻撃観測・分析結果といった各種の情報を関係者に提供し、様々な分野において教育、普及啓発、質問対応を行い、サイバー犯罪に係る様々な対策を実施した。また、IoT、暗号資産、自動運転、ドローンといった様々な分野においてサイバーセキュリティに係る施策を推進した。

このように、関係省庁において必要に応じて官民の関連する主体と連携しつつ様々な取組を推進し、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に貢献した。

【今年度の取組】

国は、深刻なサイバー攻撃に対して、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至る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作り等の政策措置の展開を一体的に推進する包括的なサイバー防御策について、関係主体との連携も図りつつ、持ち得る全ての能力と手段を活用して展開する。そのために必要な、包括的なサイバー防御の総合的に調整を担うナショナルサート機能等の強化及び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について検討を推進する。

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。

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。

経済産業省において、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[66]、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。また、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。さらに、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。加えて、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。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。

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。また、ソフトウェア製品や情報システムの開発

[66] SCAP (Security Content Automation Protocol)

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。

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。

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。また、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。加えて、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。

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。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。また、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。

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。また、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。また、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。

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。

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。

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。

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。

金融庁において、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「日本仮想通貨交換業協会」と連携を図る。

自動運転関連では、国土交通省において、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、国際基準の適合性に係る審査体制の整備を進める。

また、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。

ドローン関連では、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。

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。

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。

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。

内閣官房、総務省及び経済産業省において、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。

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。

サイバー犯罪への対策としては、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。

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。

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。

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。

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。

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。

警察庁において、サイバー空間の脅威に対処するため、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。

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。

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・分析結果やサイバーセキュリティ統合知的・人材育成基盤（通称 CYNEX）の分析結果を、NISC をはじめとする政府機関への情報提供等を通じ産学官連携強化を図る。

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。

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。

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するなど必要な対応を行う。

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、それに必要となる新たな技術開発を推進する。

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

【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。

この点を踏まえ、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を構築すべく、官民双方がクラウドサービスを採用し、継続的に利用していくため、2020 年度に ISMAP の運用を開始した。

また、内閣府において、2020 年 10 月以降、年末調整及び確定申告手続きにおいて、民間送達サービスに届いた各種控除証明書のデータを、マイナポータルを通じて一括取得し、自動入力ができる仕組みとした。

さらに厚生労働省において、資格確認法定化等を定めた「医療保険制度の適正かつ効率的な運営を図るための健康保険法等の一部を改正する法律」（令和元年法律第９号）に基づき、2021 年３月からのマイナンバーカードの健康保険証利用の仕組みの導入に向けて、システム構築を実施した。

【評価】

ISMAP の運用開始に関しては、新型コロナウイルス感染症の影響をはじめとする経済社会の環境変化によるクラウドサービスの利用拡大に伴い、当該サービスを標的とする脅威が増加している中で、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、制度の充実化並びに見直しを継続して取り組むことが求められる。

官民の認証連携、データ連係については、今回のマイナポータルを介した各種控除証明書のデータ連係、地方自治体によるオンライン申請の受付の実装並びにマイナンバーカードの健康保険証利用を実装したことにより、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、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。

また内閣官房、総務省及び経済産業省において、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。

さらに内閣府において、デジタル・ガバメントの基盤であるマイナポータルの UI・UX について、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もと、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。具体的には、2021 年５月頃までに、マイナポータルに LGWAN との接続機能を実装したことにより、全ての地方公共団体よりオンライン申請の受付を可能とする。

加えて厚生労働省において、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。

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）

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、2020 年７月に次期統一基準群の改定骨子を策定し、2021 年度中の改定に向けた作業を進めた。次期改定では、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つのテーマを掲げている。

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、政府機関等の情報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（ペネトレーションテスト）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、近年のサイバー攻撃事例や手法、最新の技術動向等を踏まえ、政府機関等と GSOC 間における効果的かつ効率的な連携を可能とする機能を実装した第４期第一 GSOC システムの構築を行った。

第４に、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、令和２年６月に決定した「申合せ」により、委託先等において重大な情報セキュリティ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。

第５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、情報通信技術（IT）総合戦略室や NISC 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、独立行政法人及びサイバーセキュリティ基本法に定める指定法人を取組の対象に加えることとした。2020 年４月から 2021 年３月までにおいて、内閣サイバーセキュリティセンターから各府省庁に向け、機器等リスト延べ 3,515 件について助言を行い、その内 190 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６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、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った。そのほか、政府機関等の職員を対象に、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」を実施した。

【評価】

昨年度の取組実績における評価として、まず、次期統一基準群の改定骨子の策定過程に

おける各政府機関等との対話を通じて、今後目指すべき情報セキュリティ対策の在り方についての共通認識を得られ、監査及び侵入検査においては、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。なお、第４期第一GSOCシステムの構築により、政府横断的なサイバーセキュリティの強化が図られた。

また、委託先等における政府機関が管理する要保護情報に係る適切な取扱いの取組においては、令和２年６月の「申合せ」に基づき、報告を受けた政府機関の委託先等において発生した情報セキュリティ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、NISCは政府機関への注意喚起等を行い、各政府機関は必要な対策を実施することで、政府機関が管理する要保護情報に対するサイバーセキュリティの強化が図られた。

さらに、政府調達におけるサプライチェーン・リスク対策については、より実効性のある対策を行う体制が整えられた。

加えて、政府機関等における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要員等に対しては、研修・訓練を行うことで、各機関のCSIRT要員において知見の向上やインシデントへの対応能力向上など、各機関においてインシデントに備えた更なる体制強化が図られた。

【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、これまでの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、

・統一基準群の改定を実施するとともに、改定後の統一基準群を踏まえた各政府機関等のセキュリティポリシー改定に係る支援等の実施

・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侵入検査（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、政府機関等とGSOC間における効果的かつ効率的な連携を推進する。更に、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

・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に資する

研修・訓練を通した、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

・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。

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）

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。

【昨年度の取組実績】

「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「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情報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、コロナ禍をきっかけとし、重要インフラ事業者等向け注意喚起のうちテレワーク実施に係る留意点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。

「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・対処を行う「分野横断的演習」を毎年実施している。2020年度は、テレワークが広く実施されるようになったことに鑑み、テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応、東京大会を見据えた情報共有体制の確認を行った。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4,721名となった。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処態勢の整備」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、2020年４月、国土交通省による支援のもと、重要インフラ事業者等（航空、空港、鉄道、物流）から構成される（一社）交通ISACが設立されるとともに、経済産業省において、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）」と連携し、大企業と中小企業を含めた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、公式サイト上で重要インフラ関係規定集を取りまとめ公式サイト上で公表したりするなど、セキュリティ取組の一層の強化を図った。

【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、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、東京大会後に予定されている同計画の改定に向け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、来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いる。引き続き、経営層への働きかけ等を着実に行いつつ、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、東京大会後予定されている「第４次行動計画」の改定に向けた評価・見直し作業と歩調を合わせて以下の取組を行う。

「安全基準等の整備及び浸透」については、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、制度的枠組みを必要に応じて適切に改善する取組を継続する。

「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急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、効果的かつ迅速な情報共有に資するため、脅威の動向や環境変化に柔軟に対応できるよう検討を行い、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。更なるセプターカウン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。

「障害対応体制の強化」については、分野横断的演習において、さら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。

セプター訓練においても、引き続きその機会を有効に活用し、「往復」訓練をベースとし、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を実施する。

「リスクマネジメント及び対処態勢の整備」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。また、セプターカウンシルや分野横断的演習等を通じて引き続き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。

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）

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の下に置かれた「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ガイドライン」の検討を進めてきた。

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、求められる役割毎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侵入検査（ペネトレーションテスト）を昨年度から２法人増加して 12 法人に対し実施した。

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、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、更なる攻撃データ解析技術の開発に資するため、これを研究データとして共有する枠組を整備した。

【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では、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ガイドラインの素案を作成した。

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。更に、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ティ対策強化に係る取組の促進を図った。

国立情報学研究所（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】

昨年度、「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作成したガイドライン素案について、引き続き、外部専門家の意見を踏まえつつ、各種会議・会合等で素案に関する説明会を開催し、ガイドラインの普及に努めていく。

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侵入検査（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。

国立情報学研究所（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。

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

【昨年度の取組実績】

2018年12月に改正されたサイバーセキュリティ基本法に基づき、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2020年6月に第3期構成員を決定するとともに、2020年12月から2021年1月にかけて第4期構成員の募集を行い、同年3月に第4期構成員を決定し、官民又は業界を超えた全266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拾え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おき、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。

例えば、新型コロナウイルスに関連したファイル名を用いるなど攻撃の手口等に変化が見られる標的型攻撃について、未確証の情報を含めた対策情報等を協議会構成員等に共有している。

この点、2021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44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12件と、協議会の特性を活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、サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、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。

重要サービス事業者等を対象に、第6回のリスクアセスメントの取組として大会延期や新型コロナウイルス感染症の拡大に伴う環境変化を踏まえたリスクの見直し、残留リスクが顕在化した場合の対処体制の強化を推進した。

各事業者等から提出されたリスクアセスメント結果を分析し、個別にフィードバックを実施するとともに、必要に応じ助言を実施した。

横断的リスク評価において、重要サービス事業者等（会場（レガシー部分）を含む。）に

対して引き続き検証を実施するとともに、2019 年度の横断的リスク評価で対象とした重要サービス事業者等における改善状況についてフォローアップを行った。

サイバーセキュリティ対処調整センターで構築した情報共有システムにより脅威情報等を提供するとともに、同システムを活用して重要サービス事業者等が参加する演習を２回実施した。

【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、2020 年内に第４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。

東京大会に向けた取組に関しては、新型コロナウイルス感染症の拡大に伴う環境の変化を考慮して、2019 年来の取組を繰り返し実施することにより全体的な成果は着実に上がっているものの、新型コロナウイルス感染症の拡大によって一部の事業者を対象にした取組を実施することができなかった。そのため、大会直前まで可能な限り取組を推進することが必要である。

【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、サイバー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。また、体制強化のため、2021 年内に第５期構成員の募集を行う予定。

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。

2.7　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、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、産業制御システムを対象としたサイバー攻撃の対処担当の警察職員に対する訓練を実施し、対処能力の向上を図った。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共同対処訓練を実施し、現場レベルでの対処態勢強化を図った。

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。

【今年度の取組】

サイバー空間と実空間の一体化がますます進展するなか、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、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引き続き実施する。

3　国際社会の平和・安定及び我が国の安全保障への寄与

3.1　「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、2020年G20リヤド・サミットにおいても、デジタル経済とともに促進することの重要性が確認された。また、13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、2020年度には第3回日中韓サイバー協議を実施した他、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（WTO）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等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、2020 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可能性等について、メンバー国として積極的に議論を重ねてきた。同じく、OEWG 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、コンセンサスによる報告書の発出に貢献した。他各種国際会議等での議論等を通じ、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 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はかるとともに、サイバー犯罪条約の締約国会合に参加した。さらに、サイバー犯罪に関する新条約の議論においては、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った。

【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 13 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、第６期サイバーセキュリティに関する国連政府専門家会合や OEWG 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、サイバー空間の自立的・持続的な発展を阻害するような動きに対し、引き続き学術会・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・規範づくりに積極的に関与し、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。

3.2　我が国の防御力・抑止力・状況把握力の強化

【昨年度の取組実績】

国家の強靭性の確保に関しては、我が国の安全保障に関係する政府機関の任務遂行を保証するため、自衛隊の任務保証に関連する主体との連携を深化させる取組をおこなった。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検討を進める等、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 月に策定された新たな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くため、2020 年度予算案において所要の事業を計上するとともに、各種取組を実施した。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１月に、オンラインにて、サイバーセキュリティに関する ARF 会期間会合のための第６回専門家会合を、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及びサイバーセキュリティに関する幅広い問題を議論した。なお、2021 年３月に行われた日米安全保障協議委員会、日米外相会談及び日米防衛相会談においては、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行く必要がある。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を取り巻く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、我が国の安全保障上の利益を守るため、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。

3.3　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、13 の国・地域との間でサイバー協議を実施しており、2020 年度には第３回日中韓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、Meridian 会合、FIRST 等に参画し、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。

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、「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（基本方針）」（2016 年 10 月）（以下「基本方針」という。）に基づいて、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きた。例えば、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３月、米国国土安全保障省・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（DHS/CISA）、国務省、エネルギー省をはじめとした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制御システムに関する日米サイバー演習を実施した。また、外務省及び警察庁がシンガポール政府及びインターポール（ICPO）と協力し、ASEAN 地域の法執行機関に対して 2016 年 10 月以降、継続してサイバー犯罪対策能力向上に資する研修機会を提供したほか、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及びサイバー攻撃防御等に資する研修機会を提供し、またインドネシアやベトナムで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、特に ASEAN 地域でのサイバーセキュリティ対策の向上に寄与するとともに、我が国との連携をさらに深めた。

【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による実務的な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 CERT として情報収集と情報発信の両面での能力強化が必要である。また、事故対応等に係る国際連携については、同盟国・同志国との演習の実施やワークショップの開催を通じて、更に困難な事案にも適切に連携・対処できるよう、演習の内容の高度化を進めていく必要がある。

能力構築支援については、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、能力構築支援については、基本方針の改訂に向けた検討を行う。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、総務省において、ワークショップの開催等を通じた我が国と 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の促進に引き続き取り組むとともに、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。

4　横断的施策

4.1　研究開発の推進

【昨年度の取組実績】

サイバー空間におけるイノベーションの進展とそれに対するサイバー攻撃の脅威を踏まえた、実践的なサイバーセキュリティの研究開発等が必要であるとの認識のもと、「サイバーセキュリティ研究・技術開発取組方針」に基づき以下の取組等を実施した。

サプライチェーン・リスクに対応するためのオールジャパンの技術検証体制の整備に関しては、関係府省と連携し、技術検証体制の整備に向け、実際の製品に不正機能や当該機能につながりうる未知の脆弱性等が存在しないかどうかの技術的検証の試行、および不正機能及び未知の脆弱性に関して技術的な調査を実施した。また、「サイバー・フィジカル・

セキュリティ対策基盤」に関して、IoT システムのセキュリティを保証する技術や、トラストリストを構築・確認する技術等について、研究開発を行うとともに、実証実験を通じて要素技術を確立した。さらに、5G ネットワークのセキュリティ検証に必要となる仮想環境の拡充や、ハードウェアチップの不正回路や不正動作を検知する技術の改良及び基礎的な検証といった、検証に関する技術開発に向けた取組を実施した。

国内産業の育成・発展に向けた支援策の推進に関しては、セキュリティ製品の有効性検証・実環境における試行検証の実施及び検証を実施した製品の「コラボレーション・プラットフォーム」でのビジネスマッチングや、情報セキュリティサービス審査登録制度のプロモーション活動および改善に向けた制度の活用状況・ニーズ調査等により、日本発のサイバーセキュリティ製品・サービスの創出・活用を推進した。また、中小企業のサイバーセキュリティへの意識向上や情報セキュリティ投資の促進に関する取組として、中小企業への専門家等の派遣によるセキュリティマネジメント指導や、スマート SME サポーター（中小企業の IT 活用を支援する IT ベンダー等）として認定した事業者の、「クラウドサービスの安全・信頼性に関する情報」、「セキュリティ対策状況」、「利用終了時のデータの取扱い等の情報提供」を行った。さらに、「コラボレーション・プラットフォーム」の開催や、地域に根差したセキュリティ・コミュニティ（地域 SECUNITY）形成を促進するための取組等により、サイバーセキュリティビジネスの振興・活性化を推進した。

攻撃把握・分析・共有基盤の強化に関しては、サイバー攻撃観測技術の高度化、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、アラート自動分析技術の高度化等のアドバンスト・サイバーセキュリティ技術、および STARDUST による攻撃活動の収集や検知技術等の研究開発を行う一方で、CURE によるインシデント情報等の集約・横断分析等の高度化を図り定常運用等を開始した。また、脆弱な IoT 機器のセキュリティ対策のため、広域ネットワークスキャン技術の改良及び総合的な実証評価を実施するとともに、AI 技術も駆使した IoT マルウェアの挙動検知技術や感染した IoT 機器を無害化・無機能化する技術の設計及びプロトタイプ開発を実施した。さらに、脆弱性関連情報の届出受付・公表に係る制度を着実に実施し、JVNiPedia と MyJVN の円滑な運用により脆弱性関連情報を利用者に提供した。

暗号等の基礎研究の推進に関しては、人工知能基盤技術の構築とセキュリティ、プライバシーに関する基盤技術の研究等のほか、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、基準の作成等の実施や、暗号を安全に利活用するための取組などについて検討、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等を実施した。また、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進めたほか、堅牢な量子暗号通信網の実現に向けて量子暗号通信の更なる長距離化技術の研究開発及び、量子セキュリティ拠点の形成に向けた整備を行った。さらに、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搭載可能な量子暗号通信技術の研究開発を実施した。

産学官連携の研究・技術開発のコミュニティ形成に関しては、研究開発戦略専門調査会

及びそのワーキンググループ（研究・産学官連携戦略ワーキンググループ）において具体化検討を行い、その考え方や推進方策を整理し、「サイバーセキュリティ研究開発戦略」（2017 年７月 13 日サイバーセキュリティ戦略本部決定）への反映・改訂に向けた検討を行った。

【評価】

サプライチェーン・リスクに対応するためのオールジャパンの技術検証体制の整備に関しては、技術検証に関する技術動向調査や 5G ネットワークのセキュリティの整備、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開発、潜伏的な脆弱性の検知・対処を実現するための研究等がなされており、引き続き、技術検証の体制整備に向けた取組を継続し、政府調達における活用等を進めていく必要がある。

国内産業の育成・発展に向けた支援策の推進に関しては、セキュリティ製品・サービスの有効性の検証の実施およびその結果を基にしたビジネスマッチング等の進展があった。また、中小企業のセキュリティ意識向上及び対策強化に関する取組、情報交流の場やセキュリティ・コミュニティ形成の促進の取組等がなされており、引き続き、国内のセキュリティ産業の育成・発展に関する取組を継続していく必要がある。

攻撃把握・分析・共有基盤の強化に関しては、サイバー攻撃観測技術、分析技術に関する研究開発を行いながら、STARDUST や CURE の高度化を図るとともに、脆弱な IoT 機器のセキュリティ対策技術に関する研究開発を進める等、引き続き、攻撃の増加や高度化する攻撃に対応するための取組を継続していく必要がある。

暗号等の基礎研究の促進に関しては、量子鍵配送や量子暗号通信技術の研究開発、既存の暗号技術の監視、新世代暗号に係る調査等の取組がなされており、引き続き、実用化等に向けた取組を継続していく必要がある。

産学官連携の研究・技術開発のコミュニティ形成に関しては、昨年度の検討の結果整理された基本的な考え方や推進方策について、本年４月に「サイバーセキュリティ研究開発戦略」を改訂したところであり、今後、我が国のサイバーセキュリティ研究分野の国際競争力の強化、産学官エコシステムの構築に向けて、その推進方策の実行が求められる。

また、上記の取組のほか、IT 関連技術の進展に応じ、中長期的な技術トレンドを捉え研究開発を推進していくことが重要である。具体的には、AI 技術の進展を見据え、AI を活用したサイバーセキュリティ対策（AI for Security）だけではなく、AI そのものを守るセキュリティ（Security for AI）についても技術課題の検討が必要である。また、量子技術の進展を見据え、耐量子計算機暗号等に関する先進的な研究を推進するだけではなく、量子通信・暗号に関する研究開発等に取り組む必要がある。

【今年度の取組】

サプライチェーン・リスクに対応するためのオールジャパンの技術検証体制の整備に関しては、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、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、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の推進や、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整備と対策の共有、ハードウェアチップの不正回路を検知する技術や不正動作を検知する技術の改良及び検証実施など、検証に関する技術開発に向けた取組を進める。さらに「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等の更なる検討を行う。

国内産業の育成・発展に向けた支援策の推進に関しては、サイバーセキュリティ製品・サービスの有効性検証基盤の運用・改善や、情報セキュリティサービス審査登録制度の改善、等により、日本発のサイバーセキュリティ製品・サービスの創出・活用を推進する。また、「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スキームを構築や、「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）」との連携により、中小企業のサイバーセキュリティへの意識向上や情報セキュリティ投資の促進に関する取組を推進するとともに、情報交流の場（コラボレーション・プラットフォーム）の開催によるサイバーセキュリティビジネスの振興・活性化や、地域に根差したセキュリティ・コミュニティ（地域 SECUNITY）の形成を推進する。

攻撃把握・分析・共有基盤の強化に関しては、サイバー攻撃観測技術の高度化、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、アラート自動分析技術の高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とともに、STARDUST による攻撃活動の収集や検知技術等の研究開発を行う。また、脆弱な IoT 機器のセキュリティ対策のため、広域ネットワークスキャン技術の改良及び総合的な実証評価を実施するとともに、AI 技術も駆使した IoT マルウェアの挙動検知技術や感染した IoT 機器を無害化・無機能化する技術に関して、評価・改良を実施する。さらに、脆弱性情報公表に係る制度を着実に実施するとともに、脆弱性関連情報をより確実に利用者に提供する取組を行う一方で、サイバーセキュリティ情報を国内で収集・生成・提供するためのシステム基盤の構築を構築し、早期に運用を開始する。

暗号等の基礎研究の促進に関しては、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の推進や、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、基準の作成等の実施や、暗号を安全に利活用するための取組等の検討、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等を実施しつつ、次期 CRYPTREC 暗号リストの改定作業に着手する。また、距離に依らない堅牢な量子暗号通信網や、衛星系と地上系を統合した量子暗号通信網の実現に向けた研究開発、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、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等を推進する。さらに、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、企業・国家等重要インフラ分野において、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。

産学官連携の研究・技術開発のコミュニティ形成に関しては、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、関係府省における研究及び産学官連

携振興施策の活用促進と、産学官エコシステム構築に向けた取組を推進する。また、研究開発戦略専門調査会等を通じて、研究コミュニティとの議論を継続するとともに、産学官の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。

4.2　人材の確保、育成、活躍促進

【昨年度の取組実績】

サイバー攻撃の脅威が広がる中、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材の育成・確保を強化していく必要がある。このため、人材育成や普及啓発に関する官民の様々な取組を集約するポータルサイトを構築し、2020年７月より試行運用を開始している。サイバーセキュリティの確保に向けては、一部の専門家の取組だけではなく、各主体がそれぞれの役割を遂行する観点から、主体的に取り組むことが求められる。2018 年サイバーセキュリティ戦略に基づき、(1)戦略マネジメント層の育成・定着、(2)実務者層・技術者層の育成、(3)人材育成基盤の整備、(4)各府省庁における取組を進めることとしてきた。

戦略マネジメント層の育成・定着に向けた取組としては、IPA 産業サイバーセキュリティセンターを通じた 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を育成する「中核人材育成プログラム」の第４期プログラムを、３年間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実施。また、高度な経営判断を補佐する戦略マネジメント機能を担う人材に必要なセキュリティ対策の知識とスキルに関するセミナーとして「戦略マネジメント系セミナー」を実施した。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にも取り組んだ。「戦略マネジメント系セミナー」については、これまで２年間の経験、受講生のアンケート結果や新型コロナ感染症の状況等を踏まえ、2021 年２月にオンライン（オンデマンド形式）で実施した。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、IPA 等による国立高専機構への教材の提供や、IPA と教員間での議論等を実施した。

実務者層・技術者層の育成に関しては、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）を実施し、2020 年度は全国 47 都道府県において計 2,648 人が受講した。国立高等専門学校機構の情報セキュリティ人材育成プログラムに参加する高等専門学校を対象に、サイバーセキュリティ講義を実施した。都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。防衛省において、CSIRT 要員に対するインシデント対処訓練や国内外の大学院等への留学、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の体制拡充、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た。また、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た。

また、各種資格・試験に関しては、2020 年 10 月時点の情報処理安全確保支援士（登録セキスペ）は 19,752 名となった。登録セキスペの更なる活用のため、IPA の HP で登録状況を公表するとともに、支援士制度の普及の周知等を行った。また、2020 年５月の改正法の施行に伴い 2020 年 10 月に初めての登録の更新が行われた。これまで義務講習の実施機関は IPA のみであったが、改正法の施行により、一定の条件を満たした民間企業の行う講習（特定講習）も対象の追加となり、この特定講習の対象となる講習を定めた。情報処理安全確保支援士制度の義務講習のうち、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、企業におけるセキュリティ関連タスクのまとまりを整理した ITSS+（セキュリティ領域）の分野から、選択できるように特定講習を定めた。ITSS+（セキュリティ領域）について、2020 年９月に公表した「サイバーセキュリティ経営ガイドライン」の付録Ｆ「サイバーセキュリティ体制構築・人材確保の手引き」の中で改訂を行い、使い方のガイドをまとめた。

人材育成の基盤の整備や若年層向けの取組としては、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に関する内容を含む公共職業訓練を実施した（28 コース・受講者数 371 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（2021 年４月１日時点の情報関係の指定講座数４講座）。専門実践教育訓練給付の対象に、ITSS レベル３相当以上の資格取得を目指す「一定レベル以上の情報通信分野」及び「第四次産業革命スキル習得講座」の教育訓練を指定した（2021 年４月１日時点の指定講座数 82 講座）。「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」における、セキュリティ分野の人材育成の取組として、学部３～４年生の学生を対象とした質の高い情報技術人材育成の取組推進や、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・実施した。2020 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。若年層を対象にしてサイバーセキュリティに関する能力が突出した人材の発掘・育成を行う「セキュリティ・キャンプ」や「SECCON2019」「SecHack365」においても、継続的に取り組みを進めた。さらに、「未踏 IT 人材発掘・育成事業」においては、2019 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、セキュリティをテーマとするプロジェクトの応募の促進を図った。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 等での公表や、各種会議で周知を行い、独立行政法人教職員支援機構と連携し、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や、教員等を対象とした情報モラル教育指導者セミナーを 2021 年２月までに実施した。

政府機関におけるセキュリティ・IT 人材の確保・育成については、「サイバーセキュリテ

ィ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」の見直しを行い政府部内のセキュリティ人材の充実を図った。また、各府省庁において同計画に基づく体制の整備と、適切な処遇の確保に関する取組についての一定の成果が見られた。また橋渡し人材の育成に向けた情報システム統一研修の実施、各府省庁へのヒアリング等を通じた「サイバーセキュリティ人材育成総合強化方針」に基づく取組の進捗状況の把握や今後の方向性についての検討等を行った。

さらに、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し、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。

【評価】

サイバー攻撃が巧妙化・複雑化する中、企業が事業継続を確固なものとしつつ、新たな価値を創出していくためには、サイバーセキュリティ確保に向けた人材の育成・確保が不可欠である。また、政府機関においても例外ではなく、サイバーセキュリティ対策とデジタル化 を一体として捉え、政策の企画・立案を進めて行くことが求められる。我が国におけるサイバーセキュリティ人材の不足が指摘されて久しいが、一方で、実務者層・技術者層の育成に向けては、資格・試験や演習、学び直しの促進等の官民の取組も進展している。こうした現状認識やデジタル化に向けた取組の広がりを踏まえれば、「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。

また、デジタル化がそれに応じた脅威への対処とあわせて推進されていくためには、サイバーセキュリティに係る人材が、男女等を問わず多様な視点や優れた発想で幅広く活躍できる環境をつくり、次代を担う優秀な人材を引きつけられる好循環を生むことが重要である。関係府省庁と連携の下、「DX with Cybersecurity 実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性」（2021 年６月）に基づき、産学官の連携を図りつつ、社会全体で「DX with Cybersecurity」を推進していくための関係施策を推進していく必要がある。

【今年度の取組】

「DX with Cybersecurity」に必要な人材に係る環境整備に向けては、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環境を整備することが重要である。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」の充実を図ることが重要である。このため、環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指していく。

需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内にお

いて、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む）が、今後デジタル化に様々に関わるためにITリテラシーや「プラス・セキュリティ」知識を補充しなければならない必要性は増しており、潜在的な大きな需要が存在すると考えられる。このため、様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行われることや、職員研修等の機会が提供されることが重要であり、こうした需要の顕在化につながる取組を企業・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、IPAによる戦略マネジメント層向け系セミナーをはじめ、国や人材育成プログラム等を提供する関係機関・企業・教育機関等が、先導的・基盤的なプログラム提供を図ることに加え、趣旨に適うプログラムを一覧化したポータルサイト等を通じて官民の取組の積極的な発信を行うなど、企業・組織の需要者からみて供給側の一定の質が確保・期待される仕組みの構築を図る。

加えて、「DX with Cybersecurity」の推進に向けては、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取り組むことが重要である。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、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。学び直しの機会の提供としては、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観点から、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とともに、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、サイバーセキュリティに関する内容を含む教育訓練を指定する。

巧妙化・複雑化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大、制御系システムを対象とする攻撃等もみられる中で、実践的な対処能力を持つ人材育成の重要性は一層増しており、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、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)を引き続き実施する。NICTを通じて、我が国独自のサイバーセキュリティ情報を国内で収集・生成・提供する「サイバーセキュリティ統合知的・人材育成基盤（通称：CYNEX)」の運用を開始する。若年層のICT人材を対象にしたトップレベル開発層のセキュリティ人材育成のため、「SecHack365」の取組を引き続き実施する。IPAの「産業サイバーセキュリティセンター」を通じた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（中核人材育成プログラム）にも引き続き取り組んでいく。「成長分野を支える情報技術人材の育成拠点の形成（enPiT)」においても産学連携し、社会人学生の学び直しを促進し、サイバーセキュリティに係る素養の向上を図る。

なお、「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も重要であり、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。さらに全国の高等専門学校生が共同で利用できる実践的な演習のための仮想空間（サイバーレンジ）の提供に向けた取組や、教育プログラムの開発を進める。また、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、産学官による情報交換を促進する。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、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。

政府機関におけるセキュリティ・IT 人材の確保・育成については、「デジタル社会の実現に向けた改革の基本方針」に基づき、「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」を改定し、デジタル人材の採用計画や育成・キャリアパスの策定のための基本的な考え方、研修の充実・強化方策を新たに示すとともに、この改定を踏まえ、各府省において「セキュリティ・IT 人材確保・育成計画」についても改定を行う。また、総合職試験（工学区分）や一般職試験（電気・電子・情報区分）等の合格者の積極的な採用に努めるとともに、優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境を整備する。さらに、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引き続き促進する。加えて、高度なサイバー犯罪や安全保障への対応等を行うため、CSIRT 要員に対するインシデント対処訓練や国内外の大学院等への留学、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の体制拡充、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

【昨年度の取組実績】

内閣官房では、「サイバーセキュリティ意識・行動強化プログラム」に基づき、普及啓発・人材育成専門調査会において、サイバーセキュリティの普及啓発に係る状況を特徴づける事項について、継続的に収集しうる代表的かつ客観的なデータを前広に収集・整理すると共に、普及啓発・人材育成施策に関するポータルサイトを運用し、掲載施策の見やすさ向上やサイバーセキュリティ月間と連携した関連行事の掲載等を実施した。また、主に一般国民向けに、緊急時における注意・警戒情報やサイバーセキュリティに関する普及啓発情報等について、媒体の特徴に合わせた情報発信を行うと共に、サイバーセキュリティ月間では各種啓発主体と連携して、「サイバーセキュリティ意識・行動強化プログラム」を踏まえ、若年層に重点を置いたキャンペーンや普及啓発イベント動画のオンライン配信を行い、普及啓発活動に取り組んだ。また、全国の公立図書館に普及啓発冊子を送付し、インターネット上でも公開するなど、地域に偏らない普及啓発活動を行った。

経済産業省において、IPA を通じて、2019 年度に作成した講義要領及び教材を基に最新事例等を追加しながら、インターネット安全教室を開催し、教育関係者及び小中高校生からシニア層までを含むホームユーザにむけ、SNS の安全な利用方法を含む情報セキュリティに関する啓発を行った。また、「教育関係者等向けインターネット安全教室」を、全国を

経済産業局の存在する９ブロック（北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄）に分割し、ブロック毎に各ブロックの都道府県数分行うこととし、計 53 回開催し、4,151 名が参加した（2021 年３月末）ほか、「ホームユーザ向け安全教室」を全国 60 か所で開催し 8,321 名が参加、その他 IPA 講師によるインターネット安全教室を 11 回実施し 2,133 名が参加した（2021 年３月末）。なお、2020 年度は、新型コロナウイルス対策のため、オンラインで開催するなどの工夫を行った。

総務省において、安全に無線 LAN を利用できる環境の整備に向けて、無線 LAN 利用時のセキュリティガイドラインとして「Wi-Fi 利用者向け 簡易マニュアル」及び「Wi-Fi 提供者向け セキュリティ対策の手引き」を改定したことに加え、安全な無線 LAN 環境の整備のためのリテラシー向上のため、オンライン動画講座の開講及び SNS を通じた周知啓発活動等を実施した。また、新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、より具体的で分かりやすく、実践的な内容のガイドラインを策定したほか、セキュリティ対策に関する専門的な相談に対応できる窓口を設置した。

【評価】

2018 年１月に策定した「サイバーセキュリティ意識・行動強化プログラム」に沿って、各府省庁において具体的な取組が着実に進められていると考えられる。引き続き、各府省庁をはじめとした関係機関と連携して取組を推進し、プログラムの内容・効果の定期的な評価・見直しを実施すると共に、サイバーセキュリティ月間をはじめとする各種啓発主体と連携した取組を進めていくほか、普及啓発・人材育成専門調査会で検討した政策課題へのアプローチとして、人材育成に資する官民幅広いプログラムや教材、先行事例等を掲載することで、ポータルサイトの改善・充実を図る必要がある。

例えば、個別の取組（インターネット安全教室）をみても、インターネットの普及は著しく、幅広い年齢層に向けて、IPA の啓発映像を基にクイズなどを組み込みながら実施するプログラムの理解度は非常に高く、参加者のアンケートの中で、「よく理解できた」「まあまあ理解できた」の割合が 99％と非常に高かった。

しかし、取組全般として、新型コロナウイルス対策のため、在宅学習やテレワークが増加し、インターネットを利用する頻度が高まるに伴いインターネットを使った被害や事件も増加する中、安全な使い方だけでなく、最近の事件やその手口、被害にあわないための対策などの情報も合わせて、一般の利用者に向けて啓発していく必要性がある。これらに加え、新型コロナウイルス感染症の状況を踏まえ、無線 LAN（Wi-Fi）の安全な利用やテレワークセキュリティの確保をはじめとするセキュリティ動向や、テレワーク環境等の社会情勢の変化に対応したコンテンツの不断の改善を進める必要がある。

【今年度の取組】

「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、高齢者への対応を含め、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。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と共に、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。また、「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、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ことに加え、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、必要に応じて見直しを行う。

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する。

総務省では、無線 LAN の使用にあ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。また、「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の検討を行う。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。

5　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。

そこで、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、2020 年度は、約 900 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 23 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、国立研究開発法人情報通信研究機構（以下「NICT」という。）とのパートナーシップ等に基づき、2020 年度は研究開発戦略専門調査会に計３回、また研究・産学官連携戦略 WG に計７回出席いただき、サイバーセキュリティ研究開発戦略の改訂や 2021 年戦略の検討に向けて、研究・産学官連携の推進方策等に関する意見交換を行った。

さらに、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、サイバーセキュリティ 2020 の全体版及び概要をまとめた簡略版の冊子を制作した。

【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、戦略及びこれに基づくサイバーセキュリティ 2020 の冊子の制作・各種セミナーを通じた国内外の関係者への発信等により、関係機関及び政府一体となったサイバーセキュリティ対策の推進が図られた。一方で、新型コロナウイルス感染症の拡大に伴う各種イベントの中止やオンライン開催への切替により、戦略及びサイバーセキュリティ 2020 の冊子を使った周知広報活動の機会が減少したことから、今後は実開催のみならず、イベントのオンライン開催を踏まえた従来とは異なる環境変化に柔軟に対応するため、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、新たに 2021 年戦略が策定されることから、2021 年戦略で掲げた「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は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、2021 年戦略及びサイバーセキュリティ 2021 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、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。

別添１　2021年度のサイバーセキュリティ関連施策

別添１　2021 年度のサイバーセキュリティ関連施策

2021 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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・経営層によるサイバーセキュリティに係るリスク把握や企業情報開示といったプラクティスの普及促進も期待されるところ、企業の取組状況のフォローアップにもあわせて取り組む。 ・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あ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
（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。
（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。
（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。
（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	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。
（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。
（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。

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・「共助」の考え方に基づく、地域のコミュニティづくりにおいて、その機能を引き続き発展させ、専門家への相談に留まらず、ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など、リソース不足を踏まえた地域による課題解決・付加価値創出が行われる場の形成を促進するとともに、先進事例の共有を通じて全国への展開に取り組む。 ・中小企業を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムとも連携しつつ、一定の基準を満たすサービスに商標使用権を付与するための審査・登録、セキュリティ対策の自己宣言等の取組を推進するとともに、中小企業向け補助金における自己宣言等の要件化等を通じたインセンティブ付けに取り組む。 ・クラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。		
項番	担当府省庁	2021 年度　年次計画
（ア）	総務省	総務省において、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）
（イ）	総務省	総務省において、地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を継続し、エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築する。

（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。
（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。
（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。
（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。実施にあたっては、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。
（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。
（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。
（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。

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別及び産業横断的なガイドライン等の策定や活用促進を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

・様々な産業分野の団体等が参加し、サプライチェーン全体でのサイバーセキュリティ対策強化を目的として意識喚起や取組の具体化を行うコンソーシアムの取組を支援する。

・一定の基準を満たす中小企業向けサービスの審査・登録や利用推奨、サイバーセキュリティ強化に向けた取組状況の可視化を行うことで、サプライチェーンを通じて地域・中小企業に取組を広げる。

項番	担当府省庁	2021 年度　年次計画
（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。
（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。
（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。
（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）

(2) データ流通の信頼性確保

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・リスクポイントの洗出しの観点から、データマネジメントに関する定義の明確化等を行い、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
(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）
(イ)	内閣官房 総務省 法務省 経済産業省	総務省、法務省及び経済産業省において、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、内閣官房において、包括的データ戦略を踏まえトラスト基盤を整備する。

(3) セキュリティ製品・サービスの信頼性確保

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・セキュリティ製品・サービスの有効性検証を行う基盤整備や実環境における試行検証を通じてビジネスマッチングを促進するほか、一定の基準を満たすセキュリティサービスを審査・登録しリスト化する取組や当該サービスの政府機関における利用促進に取り組む。 **・検証ビジネスの市場形成に向け、国としても、検証事業者の信頼性を可視化する取組の検討に取り組む。**

項番	担当府省庁	2021 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)	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。
(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。
(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さらに促進する。

(4) 先端技術・イノベーションの社会実装

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し、安全保障の観点から情報管理に留意しつつ、産学官の結節点として、当該情報を産官学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
(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。
(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。
（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 SECUNITY）の形成を各地域の経済産業局等と連携し推進する。
（エ）	内閣府	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。
（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）
（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。
（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～」、「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。
（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）
（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さらに促進する。（再掲）
（コ）	経済産業省	経済産業省において、引き続き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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・サイバー空間の基盤は人々のくらしにとっての基礎的なインフラとなりつつある中、「誰一人取り残さない、人に優しいデジタル化」 を進め、その恩恵を享受していくためには、国民一人ひとりが自らの判断で脅威から身を守れるよう、サイバーセキュリティに関する素養・基本的な知識・能力（いわゆるリテラシー）を身に付けていくことが必須である。

・デジタル活用の機会、またそれに応じたデジタル活用支援の取組と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。

・「GIGA スクール構想」の推進に当たっては、教師の日常的な ICT 活用の支援等を行う支援員等の配置や教職課程における ICT 活用指導力の充実を図るとともに、児童生徒に対し、端末整備にあわせた啓発や、動画教材等を活用した情報モラルに関する教育を推進する。

・インターネット上の偽情報の流布については、個人の意思決定や社会の合意形成に不適切な影響が与えるおそれがあることから、民間の自主的取組の慫慂を含め、幅広く周知啓発を行う。

項番	担当府省庁	2021 年度　年次計画
（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。
（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。
（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）
（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。

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

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・国は、関係主体と連携しつつ、サイバー空間を構成する技術基盤やサービスの可視化とインシデント発生時のトレーサビリティの向上に取り組むことで、各主体がニーズに合った適切なリスクマネジメントを選択できるような環境を醸成する

・トレーサビリティの確保やサイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

・各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は関係主体と連携して環境づくりに取り組んでいく。

・国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講じることによって、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
（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。
（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、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。
（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、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。
（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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・各主体の自助及び共助によるリスクマネジメントの向上に資するため、「セキュリティ・バイ・デザイン」の考え方に基づく基盤構築などの指針等を策定するとともに、サイバー空間のトレーサビリティや可視化の向上に官民が一体となって取り組む。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

①サイバーセキュリティを踏まえたサプライチェーン管理の構築

・国はサイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別・産業横断的なガイドライン等の策定を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

・国は中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。

・国は機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼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を毀損する攻撃に対する検知・防御の仕組みの構築を推進する。

②IoT や 5G 等の新たな技術やサービスの実装における安全・安心の確保

・国はサイバー攻撃に悪用されるおそれのある機器を特定し注意喚起を進めていくとともに、「セキュリティ・バイ・デザイン」の考え方に基づいて、安全な IoT システムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施する。

・セーフティの観点からの対策とサイバーセキュリティ対策を組み合わせることが求められるところ、国はそのようなセキュリティとセーフティの融合に対応したフレームワークの活用を推進する。

・国は全国及びローカル 5G のネットワークのサイバーセキュリティを確保するための仕組みの整備や、サイバーセキュリティを確保した 5G システムの開発供給・導入を促進する。

・国は自動運転、ドローン、工場の自動化、スマートシティ、暗号資産、宇宙産業等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通じて、安心・安全を確保する。

項番	担当府省庁	2021 年度　年次計画
（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。
（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。
（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、ユーザー組織における、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。

（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。
（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。
（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。
（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。
（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。
（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。
（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）
（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）
（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。
（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。
（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。
（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。
（タ）	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。
（チ）	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。
（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。
（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。

（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。
（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）
（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。
（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。
（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。
（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。
（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。
（ヒ）	内閣府 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。
（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。

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

③利用者保護の観点からの安全・安心の確保

・利用者が安心して通信サービスを利用してサイバー空間において活動できるようにする観点から、必要に応じて関係法令に関する整理を行いながら、安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する。

・多数の公的機関、企業及び国民が利用するサービスについては、その社会的基盤（プラットフォーム）としての役割に鑑み、国はより一層のサプライチェーン管理を含めたサイバーセキュリティ対策を促進する。

項番	担当府省庁	2021 年度　年次計画
（ヘ）	内閣官房 金融庁 総務省 厚生労働省 経済産業省 国土交通省	重要インフラ所管省庁及び重要インフラ事業者等は、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もとに、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。
（ホ）	総務省	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。
（マ）	内閣官房 総務省 経済産業省	内閣官房、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。

(2) 新たなサイバーセキュリティの担い手との協調

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・国は常にサイバー空間に登場する新たな技術やサービスを把握し、これらによるサイバー空間の各主体への相互影響度やその深刻度の分析を行い、それぞれの主体においてサイバーセキュリティへの確保に責任ある対応を果たせるような環境づくりを行う。

・国は、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、政府機関や重要インフラ事業者等の利用者がクラウドサービスを利用する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利用者、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
（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）
（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。
（ウ）	総務省	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）
（エ）	内閣官房 総務省 経済産業省	内閣官房、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）

(3) サイバー犯罪への対策

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・国はサイバー空間を悪用する犯罪者や、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

・犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働きかけ等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐほか、情報の共有・分析、被害の未然防止、人材育成等の観点から、官民が連携したサイバー犯罪対策を推進するとともに、国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯に係るボランティア等の関係機関・団体と連携し、広報啓発等を推進する。

・攻撃者との非対称な状況を生んでいる環境・原因を改善するため、国は諸外国における取組状況等を参考にしつつ、関連事業者との協力や国際連携等必要な取組を推進する。

項番	担当府省庁	2021 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、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。
（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。
（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。

（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。
（キ）	経済産業省	経済産業省において、今後ますます高度化・複雑化が予想されるサイバー攻撃等の最新の手口や被害実態等の情報、また、ビッグデータ・AI の実装が進展する第四次産業革命を背景に多様化する営業秘密の管理方法等の情報を共有する場として、産業界及び関係省庁と連携して「営業秘密官民フォーラム」を開催するとともに、参加団体等に営業秘密に関するメールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行う。
（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。
（ケ）	内閣府	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、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）
（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。

(4) 包括的なサイバー防御の展開

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
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
（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。

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
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
（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。

（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。

(5)サイバー空間の信頼性確保に向けた取組

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
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
（ア）	内閣府	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）
（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。
（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もとに、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）
（エ）	内閣官房 総務省 経済産業省	内閣官房、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）

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・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
（ア）	内閣官房	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。
（イ）	内閣府	内閣府において、デジタル・ガバメントの基盤であるマイナポータルの 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もと、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。
（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。
（エ）	内閣官房 総務省 経済産業省	内閣官房、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）

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）

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・各政府機関は、社会全体のデジタル化と一体としてサイバーセキュリティ対策を進め、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく。

・各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は各府省と共同で整備・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じる。

・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。併せて、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
（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、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。
（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。
（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。
（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。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）	内閣官房	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。
（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。
（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、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り組みを進める。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。

（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（ツ）	内閣官房	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。
（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。
（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。
（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。
（ニ）	内閣官房	内閣官房において、独立行政法人等における統一基準群等に基づく施策の取組状況について、IPA との連携等により、引き続き情報セキュリティ対策とその維持改善するための体制の整備及び運用状況に係る現状を把握し、独立行政法人等に対して改善のために必要な助言等を行う。なお、これまでに行った監査の結果に対する改善計画については、フォローアップを実施する。
（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。
（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。
（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。
（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。
（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。
（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。

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進する。 ・重要インフラ分野が全体として今後の脅威の動向、システム、資産を取り巻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
（ア）	内閣官房 金融庁 総務省 厚生労働省 経済産業省 国土交通省	重要インフラ所管省庁及び重要インフラ事業者等は、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もとに、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）
（イ）	内閣官房	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。 「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進する。 「情報共有体制の強化」については、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。 「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。 「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。 「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。 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。
（ウ）	内閣官房	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。（再掲）
（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、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。

（オ）	内閣官房 総務省 経済産業省 金融庁	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 ・内閣官房において、重要インフラ事業者等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。
（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。
（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）	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。
（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。
（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て連携・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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(2)地方公共団体に対する支援

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・国は、地方公共団体において適切にセキュリティが確保されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。 **・国は人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。** **・新たな時代の要請に柔軟に対応できるよう、国は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かか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
(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。
(イ)	内閣官房 内閣府 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。
(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。
(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
(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。
(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。
(キ)	内閣府	内閣府において、デジタル・ガバメントの基盤であるマイナポータルの 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もと、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）
(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）

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）

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・国は大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する研修や訓練・演習の実施、事案発生時の初動対応への支援や、情報共有等の大学等の連携協力による取組を推進する。 ・先端的な技術情報等を保有する大学等については、国は組織全体に共通して実施するセキュリティ対策のみならず、当該技術情報等を高度サイバー攻撃から保護するために必要な技術的対策や、サプライチェーン・リスクへの対策を強化できるよう取組を支援する。		
項番	担当府省庁	2021 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。
（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・連携と東京大会に向けた取組から得られた知見等の活用

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。 ・国はナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は東京大会の運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。		
項番	担当府省庁	2021 年度　年次計画
（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。
（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。
（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。
（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。
（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。

(1)分野・課題ごとに応じた情報共有・連携の推進

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・各主体との緊密な連携の下、国は 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
（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	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。
（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。
（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 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。
（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。
（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、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。
（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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・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
（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。
（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）

2.7　大規模サイバー攻撃事態等への対処態勢の強化

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・国は平時から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化する。
・国は分野や地域のコミュニティを活用してサイバー攻撃への対処態勢の強化に努めるとともに、官民連携により情報収集・分析・共有機能を強化する。
・国及び各主体は官民連携の取組等を通じてセキュリティ人材を育成及び活用することで、大規模サイバー攻撃事態等への対処を強化する。

項番	担当府省庁	2021 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。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。
（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	警察庁及び都道府県警察において以下の取組を推進することにより、サイバー攻撃対処態勢の強化を推進する。 ・都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処態勢の強化を推進する。 ・警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。 ・警察庁及び都道府県警察において、分析官等の育成や、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理、アトリビューションを一層進めるための環境を整備するなど、サイバー攻撃に関する情報収集・分析の高度化を図る。 ・警察庁において、都道府県警察のサイバー攻撃対策担当者を対象に、大規模産業型制御システムに関するサイバー攻撃対策に係る訓練を実施する。 ・大規模産業型制御システム模擬装置を活用して、制御システムに対するサイバー攻撃手法及びその対策手法について検証を推進する。 ・警察庁において、サイバー空間の脅威への危機管理に臨むため、サイバー空間に関する観測機能の強化、サイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。
（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）	内閣府	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。
（カ）	警察庁	都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、以下の取組を実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処能力の向上を推進する。 ・重要インフラ事業者等に対し、各事業者におけるサイバーセキュリティ対策の状況を確認するとともに各事業者等の特性に応じた情報提供や保有するシステムに対するぜい弱性試験を実施する。 ・事案発生を想定した共同対処訓練を実施する。 ・サイバーテロ対策協議会を通じて、参加事業者間の情報共有を推進する。
（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、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）
（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）

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、引き続き国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため積極的な役割を果たしていく。
・コロナ禍において医療機関へのサイバー攻撃が多くの国で見られ、こうした攻撃を抑止し、また、重要インフラを防護するためにもサイバー空間において法の支配を推進する
・国連等においては、サイバー空間においても既存の国際法の適用を前提とし、サイバー空間における規範などの実践にも積極的に取り組んでいく立場から、国際法の適用に関する我が国の見解を積極的に発信し、自由、公正かつ安全なサイバー空間の確保のため同盟国・同志国と連携していく。
・我が国の安全保障及び日米同盟全体の抑止力向上の取組に資するよう、国内外における国際法の適用に関する議論・規範の実践の普及に取り組んでいく。
・サイバー犯罪対策については、サイバー犯罪に関する条約等既存の国際的枠組み等を活用し、条約の普遍化及び内容の充実化を推進するとともに、国連における新条約策定に関する議論に十分関与することを通じ、サイバー空間における法の支配及び一層の国際連携を推進する。

項番	担当府省庁	2021 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、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。
(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。
(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。
(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。

(2)サイバー空間におけるルール形成

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会のルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく。 **・健全なサイバー空間の発展を妨げるような国際ルールの変更を目指す取組については、同盟国・同志国や民間団体等と連携して対抗する。**

項番	担当府省庁	2021 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。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。
(イ)	外務省 経済産業省	経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（デジタル保護主義）を取る諸外国に対し、対話、意見交換、パブリックコメントの提出等を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、主要国の規制情報等を収集しつつ、民間団体とも連携して働きかけを行う。

3.2　我が国の防御力・抑止力・状況把握力の強化

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
・安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う省庁、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。 **・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	2021 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。
(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。

(1)サイバー攻撃に対する防御力の向上

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より
①任務保証 **・政府においては、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	2021 年度　年次計画
(ア)	防衛省	防衛省において、対処機関としてのサイバー攻撃対処能力向上のため、最新技術及び部外の優れた知見を活用して、サイバー防護分析装置、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続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。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。
（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。
（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。
（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。

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

②我が国の先端技術・防衛関連技術の防護

・宇宙関連技術、原子力関連技術、その他先端技術等我が国の安全保障に関連する技術等につき、リスク低減を含めた一層の防護が必要である。

・防衛産業については、新たな情報セキュリティ基準の策定や官民連携の一層の強化等によりセキュリティ確保の取組を進めていく。

・国の安全保障を支える重要インフラ事業者や先端技術・防衛関連技術産業、研究機関といった関係事業者と国の一層の情報や脅威認識の共有及び連携を図る。

項番	担当府省庁	2021 年度　年次計画
（カ）	内閣官房 文部科学省	科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。 ・内閣官房において、先端的な技術を保有する国立研究開発法人が、自立的に情報セキュリティ対策を講じていくことができるよう、引き続き国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促す。 ・文部科学省において、先端的な技術情報を保有する大学等に関して、SINET へのサイバー攻撃を検知するシステム等を用いて警報分析及び該当する連携機関への情報提供等を行う「NII-SOCS」の取組を支援するなどし、大学等におけるサイバー攻撃による情報漏えいを防止するための取組を促進する。
（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。
（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。
（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。

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

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
（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	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。

（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。

(2)サイバー攻撃に対する抑止力の向上

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

①実効的な抑止のための対応

・サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。

・我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用していくとともに、サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含め、然るべく対応していく。

・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。

②信頼醸成措置

・偶発的又は不必要な衝突を防ぐため、国境を越える事案が発生した場合に備え、信頼醸成措置として国際的な連絡体制を平素から構築することが重要である。

項番	担当府省庁	2021 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。
（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）	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。
（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。

(3)サイバー空間の状況把握の強化

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

①関係機関の能力向上

・関係機関におけるこうした能力を質的・量的に引き続き向上させ、関係機関の全国的なネットワーク・技術部隊・人的情報も駆使しながらサイバー攻撃等の更なる実態解明を推進する。

・高度な分析能力を有する人材の育成・確保、サイバー攻撃等を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンスに係る取組を進める。

②脅威情報連携

・国家の関与が疑われるサイバー攻撃、非政府組織による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係省庁及び同盟国・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
（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。
（イ）	警察庁	・アトリビューションの強化に向けて、警察庁において、サイバー空間の脅威に対処するため、捜査で得た手口の情報等を活かし、JC3 を通じた産学官連携した取組を進める。

		・サイバー空間において実空間と同様に法の支配という原則を貫徹するため、アトリビューションの強化等、攻撃者の特定、責任追及を可能とする方法の検討に着手する。 ・犯罪の行為者に帰責する健全な社会認識の必要性が再確認されるよう、アトリビューションによって判明した犯行手口や犯罪者の動向等の情報を、国民に積極的かつ効果的に発信する等、仕組みの構築について検討する。
（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）
（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。
（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。
（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 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。
（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。
（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。
（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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・平素から実務的な国際連携を実施する重層的な枠組みを強化し、同盟国・同志国との連携を強化する。
・「自由で開かれたインド太平洋（Free and Open Indo-Pacific: FOIP）」の実現に向けた、サイバーセキュリティ分野における米豪印や ASEAN 等との協力についても積極的に推進する。
・民間における情報共有に係る国際連携も拡大するとともに、国際場裡で我が国の立場を主張できる官民の人材を確保し、他国への人材派遣や国際会議への参加等を通じて育成する。
・我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。

項番	担当府省庁	2021 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。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。
(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。
(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。
(オ)	警察庁 法務省	警察庁及び法務省（公安調査庁）において、サイバー攻撃対策を推進するため、以下の取組を実施する。 ・警察庁において、外国治安情報機関等との情報交換等国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を継続的に実施する。 ・法務省（公安調査庁）において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等の国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を引き続き強化する。（再掲）
(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。
(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。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。
(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 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。
(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。

(2)サイバー事案等に係る国際連携の強化

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・サイバー攻撃関連情報（脆弱性情報や IoC 情報など）に関する平素からの国際的な情報共有を引き続き強化し、他国と共同した情報発信を検討する。 **・我が国が国際サイバー演習等を主導して連携対処のための信頼関係を構築するとともに、情報のハブとなり、サイバーコミュニティにおける国際的なプレゼンスの向上を図る。**		
項番	担当府省庁	2021 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掲示を行い、効率的な対処のためのオペレーション連携を実現することやインターネット上のサイバーセキュリティに関する環境改善のための検討を進める。
(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。 ・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・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。

(3)能力構築支援

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・我が国の基本的な理念の下、産官学連携や外交・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つなげていく。** **・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。** **・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
(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。
(イ)	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。
(ウ)	経済産業省	経済産業省において、IPA 産業サイバーセキュリティセンター（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。

（エ）	防衛省	防衛省において、東南アジア各国等との間で、防衛当局間の IT フォーラムや ADMM プラス 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）

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・中長期的観点から研究及び産学官連携を振興し、研究開発の国際競争力の強化と産学官にわたるエコシステムの構築に取り組んでいく。 **・関係府省が提供する、科学的理解やイノベーションの源泉となるような研究及び産学官連携の振興施策の活用を促進し、研究コミュニティの自主的な発展努力と相まった、重点的な研究・産学官連携の強化を図る。これとあわせ、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。**		
項番	担当府省庁	2021 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。 ・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。
（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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備 **・国内産業の育成・発展に向けた支援策の推進** **・攻撃把握・分析・共有基盤の強化** **・暗号等の研究の推進** **・戦略期間において、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
（ア）	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。（再掲）
（イ）	内閣府	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）

（ウ）	総務省	総務省において、Society5.0 における重要な者会基盤となる第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。
（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。
（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）
（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さらに促進する。（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、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、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）
（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）
（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 SECUNITY）の形成を各地域の経済産業局等と連携し推進する。（再掲）
（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）
（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。
（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。
（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。
（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。
（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。
（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）
（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）
（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）
（ナ）	総務省	総務省において、量子コンピュータ時代において国家・重要機関間の機密情報を安全にやりとりするために、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。
（ニ）	総務省	総務省において、盗聴や改ざんが極めて困難な量子暗号通信を、超小型衛星に活用するための技術の確立に向けた研究開発を引き続き推進する。
（ヌ）	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。
（ネ）	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。（再掲）
（ノ）	内閣官房	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。 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。） 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）

(3) 中長期的な技術トレンドを視野に入れた対応

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・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	2021 年度　年次計画
（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。
（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。
（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	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）

4.2　人材の確保・育成・活躍促進

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・「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
（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。
（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。
（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。

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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
①「プラス・セキュリティ」知識を補充できる環境整備 ・経営層や、特に企業・組織内で DX を推進するマネジメントに関わる人材層をはじめとして、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要である。同時に、経営層の方針を踏まえた対策を立案し実務者・技術者を指導できる人材の確保に向けた取組も重要であり、これらの取組により「戦略マネジメント層」の充実を図る。 ・ IT リテラシーや「プラス・セキュリティ」知識に係る研修・セミナー等の人材育成プログラムは、社会的に必ずしも普及していないと考えられる。このため、環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指していく。需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内において、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む）が、今後デジタル化に様々に関わるために IT リテラシーや「プラス・セキュリティ」知識を補充しなければならない必要性は増しており、潜在的な大きな需要が存在すると考えられる。このため、様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行われることや、職員研修等の機会が提供されることが重要であり、こうした需要の顕在化につながる取組を企業・組織等に促す普及啓発を、国や関係機関・団体が先導して行う。また、国や人材育成プログラム等を提供する関係機関・企業・教育機関等が、先導的・基盤的なプログラム提供を図ることに加え、趣旨に適うプログラムを一覧化したポータルサイト等を通じて官民の取組の積極的な発信を行うなど、企業・組織の需要者からみて供給側の一定の質が確保・期待される仕組みの構築を図る。これとあわせ、対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。 ②企業・組織内での機能構築、人材の流動性・マッチングに関する取組 ・企業・組織内での機能構築や IT・セキュリティ人材の確保・育成に関するプラクティス実践の促進に向け、人材ニーズに係る実態把握とあわせ、実際のインシデントを踏まえた普及啓発や、参考となる手引き資料の活用促進、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
（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。
（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。
（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（ユーザーインターフェイス）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。
（エ）	経済産業省	経済産業省において、IPA の「産業サイバーセキュリティセンター」を通じ、以下の取組を実施する。 ・これまで実施してきた人材育成事業の経験や受講生からのアンケート結果等を踏まえ、必要に応じて中核人材育成プログラムの見直しを行いながら、IT と OT 双方のスキルを核とした上でビジネススキルやマネジメントスキル・リーダーシップをバランスよく兼ね備えた、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に引き続き取り組む。 ・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。
（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。
（カ）	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）
（キ）	総務省	総務省において、地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を継続し、エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築する。（再掲）
（ク）	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。（再掲）
（ケ）	内閣官房	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。
（コ）	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。 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。
（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 SECUNITY）の形成を各地域の経済産業局等と連携し推進する。（再掲）

(2) 巧妙化・複雑化する脅威への対処

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・実務者層・技術者層の育成に向けては、資格制度の整備・改善、若年層向けのプログラムや制御系システムに携わる実務者を対象とするプログラムの実施、演習環境の提供、学び直しの促進など、官民で取組の推進が行われてきているところ、近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく。また、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう、講師の質の担保等に留意しつつ、産学に開放する。

・多様な人材の活躍等の先進事例の発信、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にもあわせて取り組む。

項番	担当府省庁	2021 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。
（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）	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（ユーザーインターフェイス）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）
（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）
（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。
（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。
（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。
（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。
（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ィア・技術を有する人材を発掘・育成する「未踏 IT 人材発掘・育成事業」を実施し、プロジェクトマネージャーに引き続きセキュリティを専門とした人材を採用する。
（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。

(3) 政府機関における取組

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より		
・外部の高度専門人材を活用する仕組みの強化や、新たに創設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向けた方針に基づき、政府機関全体で取組を強化していく。 **・各府省庁において人材確保・育成計画を作成し、「サイバーセキュリティ・情報化審議官」等による司令塔機能の下、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保についても着実に取り組むとともに、毎年度計画のフォローアップを行い、一層の取組の強化を図る。** **・外部の高度専門人材を活用するだけでなく、政府機関等内部においても独自に高度専門人材を育成・確保する。**		
項番	担当府省庁	2021 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「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。
（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。
（ウ）	内閣官房 総務省	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、内閣官房及び総務省（デジタル庁設置後はデジタル庁）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。
（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。全国の警察職員に対して、サイバーレンジの遠隔学習を活用し、警察業務に必要となる演習を行わせることで、サイバー空間の脅威への警察全体の対処能力の底上げを推進する。

（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）
（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。
（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

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・普及啓発に向け産学官民の関係者が円滑かつ効果的に活動できるよう、「全員参加による協働」に向けた具体的なアクションプランを策定し、地域・中小・若年層を重点対象として、取組推進を行ってきた。

・デジタル改革の推進により、サイバー空間に参加する層が広がることが予想される中で、当該アクションプラン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
（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）
（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。
（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。
（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。
（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。
（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）
（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）
（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つつ、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。
（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。
（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）のもと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。
（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）

（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。
（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。
（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。

5　推進体制

2021 年戦略（2021 年～2024 年の諸施策の目標と実施方針）案より

・デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを有効活用しつつその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。

・危機管理対応についても一層の強化を図ることが必要である。

・安全保障にかか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
（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。
（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）
（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）
（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）
（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。

別添２　2020 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

1.1　新たな価値創出を支えるサイバーセキュリティの推進

(1) 経営層の意識改革

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催による、経営層の意識改革 **・対策の可視化など、経営層に訴求するための施策の推進** **・企業が参照すべき法制度に関する整理**			
項番	担当府省庁	2020 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、経営層の意識改革や戦略マネジメント層、実務者層・技術者層、若年層の育成に関して、関係府省庁との連携の下、「サイバーセキュリティ人材育成取組方針」（2018 年６月）に基づき、産学官の連携を図りつつ、関係施策を推進していくとともに、DX 時代の新たな事業・サービスを提供する上で重要となる企業内における IT・サイバーセキュリティ関係の体制構築・人材育成等について議論を進める。	・普及啓発・人材育成専門調査会において、経営層の意識改革や人材育成に関する産学官の多様な取組について、関係機関の間で情報共有を行った。また、DX with Cybersecurity の推進を目的として、政策議論のための補助フレームワークを作成し、今後 DX を実現するための人材の確保、育成、活躍の促進に係る政策課題について議論・検討を深めた。また、議論の成果の一部は、経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」にも反映を行った。
（イ）	経済産業省	経済産業省において、2019 年６月に公表された「グループ・ガバナンス・システムに関する実務指針」において、グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方が位置づけられたことを踏まえ、企業による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実践を更に後押ししていく。	・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。
（ウ）	経済産業省	経済産業省において、取締役会のサイバーセキュリティへの関与を促すとともに、投資家に対するサイバーセキュリティの啓発を行う観点から、上場企業において行われる「取締役会の実効性評価」の評価項目について、サイバーセキュリティへの経営層の関与をその評価項目として組み込むことを引き続き促進する。	・経済産業省において、投資家等との意見交換などを通じ、取締役会のサイバーセキュリティへの関与の促進や投資家に対するサイバーセキュリティの啓発を実施した。
（エ）	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。 ・更なる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、可視化ツールの Ver1.0 開発とそのためのユーザ企業向け β 版テストを行う。	・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 2021 年３月末時点で 10 万件を超えた。 ・「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」Ver1.0 開発のため、β 版ベースでユーザ企業及び投資家等ステークホルダーへのヒアリングを実施。その結果を Ver1.0 の企画としてまとめ、Ver1.0 開発に着手した。

(2) サイバーセキュリティに対する投資の推進

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・企業の積極的な情報発信・開示に向けたベストプラクティスの共有やガイドラインの策定 **・情報発信・開示の状況についての継続的な把握・評価** **・投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくり** **・企業に対するサイバーセキュリティの促進策のフォローと措置の検討** **・サイバーセキュリティ保険の活用を推進するための方策についての検討**			
項番	担当府省庁	2020 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、「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」の普及を図る。 ・可視化ツールβ版について、投資家等ステークホルダーが活用できるかの調査を実施する。	・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」の普及を実施。さらに、IPA がプラクティス集の課題やニーズに関する調査を実施、来年度以降の強化の方向性を確認した。 ・「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」β版を使って投資家等ステークホルダーへのインタビュー調査を行い、可視化ツール Ver1.0 の企画に反映した。
（イ）	総務省	総務省において「サイバーセキュリティ対策情報開示の手引き」の普及を図る。	・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。当該分科会は、日経 225 を対象に開示情報から各社のサイバーセキュリティの取組姿勢に関する調査を行い、2020 年 11 月に調査結果を公表した。
（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、サービスの拡張も含め、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、2020 年度は、登録サービス件数を約 170 件から約 240 件まで増加させた。また、制度の更なる改善を図るため、ユーザ・ベンダー双方への本制度の活用状況・ニーズ調査を実施した。制度利用者からの要望を踏まえ、利用者にとってより分かりやすいものにすべく、基準適合サービスリストを改善した。
（エ）	総務省 経済産業省	経済産業省及び総務省において、2020 年度中に施行予定である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、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。	・経済産業省及び総務省において、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を 2020 年８月 31 日に施行し、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。
（オ）	経済産業省	経済産業省において、2019 年度事業で明らかになった中小企業の実態・ニーズを踏まえ、地域特性・産業特性等を考慮したマーケティング、機器ソフトウェアサービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、損害保険会社、IT ベンダー、地元の団体等の連携による地域実証を 2020 年度に実施する。この実証を通して中小企業のサイバーセキュリティへの意識向上を図るとともに、中小企業の実態やニーズをよりきめ細かく把握し、2021 年度以降に民間による中小企業が活用しやすいサイバーセキュリティ簡易保険含めた対策支援サービスの創出を目指す。	・経済産業省において、損害保険会社、ＩＴベンダー、地元の団体等がコンソーシアムを組む、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を全国で 15 件実施し、約 1,100 社の中小企業が実証に参加した。実証により、中小企業におけるセキュリティ対策の課題や、産業別でのセキュリティ対策の実態等が明らかになった。

（カ）	総務省	総務省において、地域に根ざしたセキュリティコミュニティの形成に向け総合通信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。	・総合通信局や地域の事業者、セキュリティ関係機関など様々な主体による地域に根ざしたセキュリティコミュニティの形成に向け既存の情報共有体制におけるセミナーや演習などについて、2020 年度は昨年度の３地域からさらに拡大し、５地域において実施した。

(3) 先端技術を利用したイノベーションを支えるサイバーセキュリティビジネスの強化

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より

・先端技術の利用に伴うサイバーセキュリティリスクの分析・明確化とそれに基づくガイドラインの策定や普及等

・先端技術のリスク分析や脅威への対策に係る研究開発の推進

・セキュリティ・バイ・デザインの考え方を基本とした取組

・先端技術の利用を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチング、サイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築

・我が国の高いサイバーセキュリティが確保されたモノやサービス等のトップセールスや展示会等を活用したアピール、国際展開をしやすいビジネス環境の整備

項番	担当府省庁	2020 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、IPA を通じ、営業秘密保護に関する対策等を推進するための情報発信を行うとともに、営業秘密保護に係る状況を調査する。 ・2016 年度に実施した同趣旨の調査から４年が経過するため、2020 年度は、2016 年以降の秘密情報漏えいに関する判例を調査するとともに、2016 年以降の社会動向の変化に伴う営業秘密保護対策の実態を把握する。	・営業秘密保護に関する指針策定に向けた情報収集のため、「企業における営業秘密管理の実態調査 2020」を実施。2016 年に実施した企業の営業秘密の管理状況調査を踏まえ、企業が営業秘密の管理や漏えい対策を強化するための施策に資すための調査を実施した。 ・INPIT と連携し、営業秘密保護知財戦略セミナーにて営業秘密に関する動向や保護の対策について講演を実施した（2020 年度１回）。 ・経済産業省知的財産政策室と連携し、営業秘密官民フォーラムが発行する営業秘密保護メールマガジン事務局業務を実施。2020 年度に 12 回発行した。
（イ）	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等の情報の管理に係る認証制度について、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等の情報の管理に係る認証制度を、HP や講演等において周知した。
（ウ）	総務省 経済産業省	総務省及び経済産業省において、引き続き、「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」、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、クラウドサービスのセキュリティに関する国際規格等と「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２版）」との整合性に関する調査を実施。当該調査結果を踏まえ、有識者会合における検討を行い、当該ガイドラインの改定案を作成した。 ・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。
（エ）	総務省	我が国独自のサイバーセキュリティ情報を国内で収集・生成・提供するためのシステム基盤の構築、及びこれらの情報を活用した製品検証環境や演習環境の構築のための検討を行う。	・総務省において、NICT を通じて、サイバーセキュリティ統合知的・人材育成基盤（通称：CYNEX）として、我が国独自のサイバーセキュリティ情報を国内で収集・生成・提供するためのシステム基盤の構築、及びこれらの情報を活用した製品検証環境や演習環境の構築を開始した。

（オ）	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、地方版コラボレーション・プラットフォームを各地域の経済産業局等と連携し開催する。	・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 2020 年度は計４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 SECUNITY）の形成を促進するため、全国各地で経済産業局等によるセキュリティに関する取組等を実施。2021 年２月には「地域 SECUNITY 形成・運営のためのプラクティス集」（第１版）を取りまとめ、公開した。
（カ）	経済産業省	経済産業省において、日本発のサイバーセキュリティ製品・サービスの創出・活用を推進するため、セキュリティ製品・サービスの有効性を検証する基盤を構築する。また、2019 年度にトライアル検証を実施したセキュリティ製品・サービスのビジネスマッチングを実施する。	・2019 年度にトライアル検証を実施した２製品について、コラボレーション・プラットフォームでビジネスマッチングを実施。2019 年度に得られた製品評価のノウハウ等知見を活かし、2020 年度も有効性検証基盤の構築に関する議論と運用を実施。２製品を選定、検証を行った。
（キ）	経済産業省	経済産業省において、引き続き、ASEAN、インド太平洋地域の新興国に対し、電力をはじめとした重要インフラ分野におけるサイバーセキュリティに関する意識啓発、知見・能力の構築支援を通じて、日本製のセキュリティを備えた質の高いインフラ輸出に向けた環境整備を行う。	・経済産業省において、ベトナムのスマートシティ化におけるセキュアなインフラの海外展開に係る F/S 実施に向けた後押しを行った(が、コロナ禍による渡航制限のため実施に至らなかった)。
（ク）	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。	・新型コロナウイルスの影響で米国サンフランシスコで開催される予定だった RSA カンファレンスが延期されたため施策は未実施。 ※RSA カンファレンスは参加者約 42,500 人、出展企業約 700 社の世界最大希望のセキュリティ産業に関するカンファレンス。

1.2　多様なつながりから価値を生み出すサプライチェーンの実現

(1) サイバーセキュリティ対策指針の策定

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サプライチェーンにおいて、運用レベルでの対策が実施できるような業種横断的な指針の策定 **・IoT 機器や組織等に求められる具体的な対応策の産業分野毎の提示**			
項番	担当府省庁	2020 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。	・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、フレームワークの周知・普及、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とともに、2019 年に設置した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、引き続き検討を行った。

（イ）	総務省	総務省においてスマートシティのプラットフォームを含むレイヤー構造や様々なユースケースを踏まえたセキュリティ要件について、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。	・2019 年度のスマートシティセキュリティに関する調査結果や有識者会合での検討の結果を整理し、「スマートシティセキュリティガイドライン（第 1.0 版）」として 2020 年 10 月に公表した。その後、国内の先行的なスマートシティのセキュリティ取組の調査や、有識者会合における検討を実施し、様々なユースケースを想定したスコープの整理やスマートシティ特有の観点で考慮すべきセキュリティ事項について整理した「スマートシティセキュリティガイドライン（第 2.0 版）」の改定案及び当該ガイドラインのガイドブック（案）を作成した。また、「スマートシティ官民連携プラットフォーム」の下に設置されている「スマートシティのセキュリティ・セーフティ分科会」において、スマートシティのセキュリティ対策に関するチェックシートのあり方について議論した。

(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・要件の確認等による信頼を創出する仕組みの構築 **・信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築** **・トレーサビリティを確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みの検討**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ア）	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製造・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。	・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」において、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進すべく、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、研究開発を行うとともに、実証実験を通じて要素技術を確立した。
（イ）	経済産業省	IoT 機器等を活用して制御系システムを含めた拠点の無人化等の推進が見込まれる中、フィジカル・サイバー間をつなげる機器・システムにおけるセキュリティ・セーフティ要求の強度を適切に検討するため、それらの機器・システムのカテゴライズ及びセキュリティ・セーフティ要求の検討に資する「IoT セキュリティ・セーフティ・フレームワーク」を 2020 年内に策定するとともに、末端の制御系システムにふさわしいセキュリティ対策に関して検討を開始する。 また、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を促進するため、産業界と連携して、2020 年度中に必要な体制を立ち上げ、参加企業によるリスクマネジメント強化のための基本行動指針の順守を促す。あわせて、一定の基準を満たしたセキュリティサービスを活用する中小企業を可視化し、適切なセキュリティ対策に取り組む中小企業と本体制に参画する大企業・業界団体との取引を促進する。	・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、IoT 機器に求められる機能の要求を明確化すると共に、2019 年に設置した第２層タスクフォースにおいて検討を行い、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「IoT セキュリティ・セーフティ・フレームワーク」を策定した。 ・2020 年 11 月に、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を推進するため、産業界が一丸となった「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」を設立した。本コンソーシアムとも連携し、「サイバーセキュリティお助け隊」の商標使用権を付与するスキームを検討した。

（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の整備に向けて、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に関する技術検証体制の整備を進める。	・技術検証体制の整備に向けた事業として、実際の製品に不正機能や当該機能につながりうる未知の脆弱性等が存在しないかどうかの技術的検証の試行を実施した。また、不正機能及び未知の脆弱性に関してその検出方法等の検討に関する技術的な調査を実施した。
（エ）	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、2019 年度に構築した 5G ネットワークの仮想環境を仮想化通信プラットフォーム、MEC（モバイルエッジコンピューティング）仮想化基盤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。	・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、2019 年度に構築した 5G ネットワークの仮想環境を仮想化通信プラットフォーム、MEC（モバイルエッジコンピューティング）仮想化基盤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。

(3) 中小企業の取組の促進

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・中小企業を対象としたサイバーセキュリティ対策の事例集の作成 **・サイバーセキュリティ保険の活用促進** **・中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化** **・中小企業が自主的に宣言できる仕組みなどの可視化の取組促進、インセンティブの仕組みとの連携**			
項番	担当府省庁	2020 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、「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。	・2018 年度に作成した「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、講演等により普及を図った。
（イ）	総務省	総務省において、地域に根ざしたセキュリティコミュニティの形成に向け総合通信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）	・総合通信局や地域の事業者、セキュリティ関係機関など様々な主体による地域に根ざしたセキュリティコミュニティの形成に向け既存の情報共有体制におけるセミナーや演習などについて、2020 年度は昨年度の３地域からさらに拡大し、５地域において実施した。
（ウ）	経済産業省	経済産業省において、2019 年度事業で明らかになった中小企業の実態・ニーズを踏まえ、地域特性・産業特性等を考慮したマーケティング、機器ソフトウェアサービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、損害保険会社、IT ベンダー、地元の団体等の連携による地域実証を 2020 年度に実施する。この実証を通して中小企業のサイバーセキュリティへの意識向上を図るとともに、中小企業の実態やニーズをよりきめ細かく把握し、2021 年度以降に民間による中小企業が活用しやすいサイバーセキュリティ簡易保険含めた対策支援サービスの創出を目指す。（再掲）	・経済産業省において、損害保険会社、IT ベンダー、地元の団体等がコンソーシアムを組む、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を全国で 15 件実施し、約 1,100 社の中小企業が実証に参加した。実証により、中小企業におけるセキュリティ対策の課題や、産業別でのセキュリティ対策の実態等が明らかになった。
（エ）	経済産業省	経済産業省において、営業秘密保護や事業継続性の観点からも経営層がサイバーリスクを重要課題として把握し、人材育成等経営資源に係る投資判断を行い、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。また、IPA を通じて、中小企業における情報セキュリティ対策の実施を促すため、中小企業支援団体との連携強化や地域での説明会の拡充等を通じて、地域も含め更なる「中小企業の情報セキュリティ対策ガイドライン」の普及を図る。	・経済産業省において、講演等の場で「サイバーセキュリティ経営ガイドライン」や「中小企業の情報セキュリティ対策ガイドライン」の普及啓発を実施。サイバーセキュリティ経営ガイドラインのダウンロード数は 2021 年３月末時点で 10 万件を超えた。

（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、以下の取組を実施する。 ・経済産業省において、セキュリティにも配慮した安心安全なクラウドサービス利用の促進等のために、認定された IT ベンダーのセキュリティ関連の取組状況等を開示し、その制度の普及促進を図る。 ・経済産業省において、セキュリティ対策の普及啓発を行うとともに、専門家等を派遣して、セキュリティマネジメント指導を実施する。	・経済産業省において ・スマート SME サポーター（中小企業の IT 活用を支援する IT ベンダー等）として認定した事業者について、特設サイトにて「クラウドサービスの安全・信頼性に関する情報」、「セキュリティ対策状況」、「利用終了時のデータの取扱い」等を開示し、中小企業に情報提供を行った。 ・セキュリティ対策の普及啓発を行うとともに、専門家等を派遣して、セキュリティマネジメント指導を 395 社の中小企業に対して実施した。
（カ）	経済産業省	経済産業省において、IPA を通じ、中小企業におけるセキュリティ対策強化に資するため、「中小企業の情報セキュリティ対策ガイドライン」の普及を図るとともに、実践に関する企業内及び地域で活躍する指導者の拡大に向けた「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を実施する。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を踏まえ、講演内容等の見直しを図る。また、「SECURITY ACTION 制度」の更なる周知を図り、参加企業の拡大に取り組むとともに、三大都市圏を除く地方での普及に取り組む。また、ニーズに応じた制度の見直しに向けて、大企業など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関する調査を実施する。	・「講習能力養成セミナー」を全国 12 箇所において開催するとともに、同講演を録画配信（オンデマンド形式）し、中小企業の経営者、社内教育担当者等合計約 400 名が参加、オンデマンド形式による録画配信についても約 550 名が視聴した。 ・商工団体・税理士会・社会保険労務士会等の指導員等を対象とする研修会、警察・自治体・中小企業団体等が主催する中小企業向けセミナー等 30 箇所以上に講師を派遣した。 ・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った。また、同制度の三大都市圏を除く地域における普及を目的として 18 箇所で普及セミナーを実施したほか、地域の団体組織等の主催するセミナーについても 72 箇所に対し講師を派遣し、同制度の普及を図った。 ・「SECURITY ACTION」制度は、自己宣言者数は全国で 144,847 件（一つ星：130,480 件、二つ星：14,367 件）に増加し、このうち三大都市圏を除く地域においても自己宣言者数は 63,194 件となった。

1.3　安全な IoT システムの構築

(1) IoT システムにおけるサイバーセキュリティ体系の整備と国際標準化

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・各主体の間での共通認識の醸成と、役割や機能の明確化を図った上での、協働した取組の推進 **・官民の各主体が抱える課題やそれぞれの取組の可視化と情報共有を行うための仕組みの構築** **・安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組**			
項番	担当府省庁	2020 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、IoT システムに係る新規事業がセキュリティ・バイ・デザインの考え方に基づき取り組まれるよう、予算重点化方針にこうした考え方を盛り込むとともに、各府省庁等において、こうした考え方に基づく取組が行われるよう働きかけを引き続き行う。	・「サイバーセキュリティ関係施策に関する令和２年度予算重点化方針」（令和元年５月 23 日サイバーセキュリティ戦略本部決定）において、「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」を踏まえることや、IT 利活用等を目指す施策についても、セキュリティ・バイ・デザインの考え方を盛り込むことに留意することを示した。
（イ）	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。	・海外のカウンターパートへの取組紹介のとりまとめなど、必要に応じて対応を行った。

（ウ）	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、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。 ・経済産業省において、IPA を通じて、様々な製品やシステムがつながる IoT において重要なセキュリティ・セーフティのうち、特に IoT 社会で関心の高いセキュリティに着目し、我が国産業界の競争力を強化するとともに、国際的な IoT のセキュリティレベルの向上を目指すために、日本主導で進めている遵守すべきセキュリティの基本的な枠組みの国際標準化を引き続き推進する。	・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。
（エ）	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。	・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 2021 年３月に更新した。
（オ）	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。	・国際標準化機関である ITU-T SG17 及び ISO/IEC JTC1/SC27、SC41 において「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」等を基本とした勧告案及び規格案の検討を促進した。

(2) 脆弱性対策に係る体制の整備

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・IoT 機器に必要なサイバーセキュリティに関する要件の整理と、その要件を満たす IoT 機器の利用の推奨 **・パスワード設定に不備のある機器の調査・特定を行い、利用者への注意喚起を円滑に行えるような所要の制度整備** **・我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献**			
項番	担当府省庁	2020 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、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、スマートホーム SWG において引き続きスマートホーム分野のサイバー・フィジカル・セキュリティ対策ガイドラインの活用等についても検討を進める。	［総務省］ ・市場に流通する端末機器（IoT 機器を含む）について、電気通信事業法令に基づく技術基準への適合状況を確認した。また、運用方法や解釈等を定めた「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版）」を 2020 年９月１日に公表した。 ［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 WG1（制度・技術・標準化）の下で開催したスマートホーム SWG（一般社団法人電子情報技術産業協会スマートホームサイバーセキュリティ WG）を活用して、家電など家庭で使われる IoT 機器のサイバーセキュリティの確保のための必要な対策について、関連する事業者と連携しながら検討を行い、スマートホーム分野のサイバー・フィジカル・セキュリティ対策ガイドラインの案について、パブリック・コメントを実施し、コメントを踏まえた検討を進めた。

（イ）	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。	・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た利用者への注意喚起を行う取組「NOTICE」を実施し、2020 年度は延べ 12,804 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、2020 年９月には、調査の際に入力する識別符号を追加等するため実施計画の変更を行った。

2　国民が安全で安心して暮らせる社会の実現

2.1　国民・社会を守るための取組

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・全ての主体が、自主的にセキュリティの意識を向上させ、主体的に取り組むとともに、連携して多層的にサイバーセキュリティを確保する状況を作り出していく			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（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設置、プラットフォーム事業者による適切な対応及び透明性などの確保、ICT リテラシー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、関係者で構成するフォーラムを設置した。また、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、「プラットフォームサービスに関する研究会」を通じ、プラットフォーム事業者へのヒアリングを通じてモニタリングを行った。

(1) 安全・安心なサイバー空間の利用環境の構築

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・脅威に対して事前に積極的な防御策を講じる「積極的サイバー防御」の推進			
項番	担当府省庁	2020 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、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。	・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。2020 年度においては、ソフトウェア製品の届出 255 件、ウェブアプリケーションの届出 734 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、149 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、2020 年度においては、脆弱性対策情報を約 10,000 件（累計：約 127,000 件）公開した。
（イ）	経済産業省	経済産業省において、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。	・経済産業省において、IPA を通じ、 ・NIST 脆弱性対策データベース NVD と JVN iPedia との連携、CVSS バージョン 3.1 計算ソフトウェアの提供、CVSS 解説動画の公開など、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、脅威情報構造化記述形式 STIX の普及啓発を推進した。

（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。	・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 を通じて実施した。
（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（ファジング技術）の調査、公開資料の拡充を行い、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。	・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。
（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。	・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。2020 年度は、2021 年３月末現在で 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 70%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、ブラウザやウィルス対策ソフト・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エアやサービス 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。
（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。	・経済産業省において、IPA を通じ、各種講演等（2020 年の講演：12 件）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 980 サイトとなった。 ・icat の表示サイズを任意に指定可能とする改善を図った
（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。	・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、2020 年度のダウンロード数は 3,366 件と、利用拡大を図った。
（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。	・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」の公開を継続、「企業ウェブサイトのための脆弱性対応ガイド」を改訂した。また、IPA セミナーにおいて AppGoat を利用した脆弱性解説を行うことで、脆弱性対策の普及促進と AppGoat 利用拡大を図った。
（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。	・経済産業省において、JPCERT/CC を通じて、2020 年度は製品開発者に対するミーティングを 2 回実施した。うち 1 度は、CVSS(Common Vulnerability Scoring System), CWE(Common Weakness Enumeration)に関する説明会とし、改定や拡充に向けて国内での普及啓発を図った。また、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った。

（コ）	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。	・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）等を促進した。 ・具体的には、海外捜査機関の情報をもとに、警察庁、一般社団法人 ICT-ISAC、各 ISP と連携し、2021 年２月下旬よりマルウェア（Emotet）に感染している機器の利用者に対する注意喚起を実施した。
（サ）	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。	・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。
（シ）	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。	・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た。 ・具体的には、電気通信事業者がフロー情報分析を行い C&C サーバを検知することについて、通信の秘密の規定との関係などの法的課題や技術的課題の本格的な整理・検討に向けて準備を進めた。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サービスの全体の基盤となる信頼できる情報インフラの整備の促進 **・仮想通貨交換業者との連携及び対応の推進** **・自動運転車やドローンに関するセキュリティ対策の推進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ス）	経済産業省	経済産業省において、引き続き、高水準・高信頼の検証サービスに向けた体制整備を推進するとともに、信頼できるセキュリティ製品・サービスのマーケット・イン促進のための環境整備を推進する。	・IoT 機器等の信頼性を高度に検証するハイレベルな検証サービスの普及拡大に向けた実証を実施。また、日本初のサイバーセキュリティ製品のマーケットインを促進するため有効性確認等を実施。

（セ）	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、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。 加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、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における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、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。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。	［NISC］ ・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情報セキュリティ対策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、毎年度、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。 ［金融庁］ ・金融分野については、FISC において「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（第５版）改定版」の内容を包括した、「金融機関等コンピューターシステムの安全対策基準・解説書」を作成している。 ［総務省］ ・電気通信分野については、「事業用電気通信設備規則」、「情報通信ネットワーク安全･信頼性基準」及び「電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）」について、改善に向けた分析・検証を行っている。 ・放送分野における「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」と、ケーブルテレビ分野における「ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン」について統合し、より効率的な運用・情報共有を図ることとした。 ［厚生労働省］ ・水道分野については、令和２年４月に施行された「水道施設の技術的基準を定める省令の一部を改正する省令」（厚生労働省令第 59 号）において、水道事業の施設基準としてサイバーセキュリティ対策を位置付けた。 ・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」を第 5.1 版に改定した。 ［経済産業省］ ・電力分野においては「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」の改定を実施した。 ・ガス分野においては「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領」の改定を実施した。 ［国土交通省］ ・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。
（ソ）	金融庁	金融庁において、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」と連携を図りながら、特に 2020 年５月１日に施行された改正資金決済法で新たに盛り込まれた観点(顧客の暗号資産は、原則として信頼性の高い方法で管理することを義務付け等)を踏まえつつ、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のモニタリングを行うことで、業者のサイバーセキュリティ強化を図る。	・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り組みを行った。
（タ）	国土交通省	国土交通省において、独立行政法人自動車技術総合機構交通安全環境研究所と連携し、自動車の安全基準の国際調和等を審議する唯一の場である国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論を議長国として引き続き主導するとともに、国際基準の適合性に係る審査体制の整備を進める。	・自動車の安全基準の国際調和等を審議する唯一の場である国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論に、独立行政法人自動車技術総合機構交通安全環境研究所と連携のもと参画し、2021 年１月に自動車サイバーセキュリティの国際基準が発効した。またこれと同時に国際基準を国内基準に取り入れた。

（チ）	経済産業省 国土交通省	経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによ るサイバーセキュリティリスクへの対応に向けて、2018 年度に車両内の電子システムを模擬した評価環境（テストベッド）を構築したところ。2019 年度は、同評価環境を警察大学校での研究開発に活用。引き続き、サプライヤー等による部品レベルでの性能評価に利用するなど、活用方法の更なる拡大を図る。	・経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクへの対応に向けて、2018 年度に車両内の電子システムを模擬した評価環境（テストベッド）を構築したところ。2020 年度は、同評価環境をサプライヤー等による部品レベルでの性能評価に利用する方策を検討するなど、活用方法の更なる拡大を図った。
（ツ）	内閣府 経済産業省 総務省	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についての調査を実施する。	・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 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についての調査を実施した。
（テ）	内閣官房	2020 年３月 31 日の「小型無人機に係る環境整備に向けた官民協議会」において決定した、「小型無人機の有人地帯での目視外飛行実現に向けた制度設計の基本方針」に基づき、必要な制度整備等を推進する。	・2020 年９月に「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」を小型無人機に関する関係府省庁連絡会議の申合せにより決定した。これに基づき、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き換えや、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ることとした（2021 年度予算に基づく 2021 年４月以降の調達から開始）。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の開発を実施中。

(2) サイバー犯罪への対策

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバー犯罪の実態把握、取締りの推進 **・官民が連携したサイバー犯罪対策の推進** **・サイバー空間における事後追跡可能性の確保に必要な取組の実施**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ア）	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を対象として、情報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。	・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、2021 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（2020 年中は 18,166 件実施）を推進した。 ・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　～ネットの落とし穴に踏み込まないで～」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。 ・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。 ・警察庁ウェブサイトや SNS において、サイバー犯罪の発生状況について広報するとともに、注意喚起を行った。 ・警察庁ウェブサイト「@police」において、リモートデスクトップサービスや 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。
（イ）	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。	・2020 年中の不正アクセス行為の発生状況等を 2021 年３月４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。 ・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。

（ウ）	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、安全で安心なインターネット空間の醸成に向けた取組を推進する。	・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。 ・都道府県警察において、2020 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を活用し、サイバー防犯ボランティア活動への支援を実施した。その結果、2020 年末現在の全国のサイバー防犯ボランティア数は、262 団体 8,161 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。
（エ）	内閣府	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。	・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 96 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 15,416 件対応した。
（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。	・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となる演習を実施した。
（カ）	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。	・解析用資機材を整備し、対処能力を強化した。 ・関係会合への参加や技術協力を通じて、関係機関との連携を推進した。 ・最新の技術情報を収集しつつ、複雑化する不正プログラムの解析を実施した。 ・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、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を実施した。また、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。
（キ）	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。	・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。
（ク）	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。	・検察当局においては，サイバー刑法の違反事実を含むサイバー犯罪に対し，事案に応じて法と証拠に基づき適切に対応した。
（ケ）	総務省	総務省において、NICT を通じ、引き続き、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。

（コ）	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。
（サ）	警察庁	警察庁において、新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）の悪用等急速に悪質巧妙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。
（シ）	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、日本版 NCFTA である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。	・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。 ・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キングを推進するため、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。
（ス）	経済産業省	経済産業省において、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシング詐欺被害の抑制のため、情報収集や情報提供を進める。国内については、フィッシング対策協議会のウェブページでの緊急情報の発信等を通じた一般向けの啓発活動を継続しつつ、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。	・経済産業省において、2020 年度は APWG や M3AAWG など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。
（セ）	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必要な対応を行う。	・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。
（ソ）	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す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。

2.2　官民一体となった重要インフラの防護

(1) 行動計画に基づく主な取組

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・重要インフラ行動計画に基づく取組の推進及び同計画の見直し **・面としての防護の強化及び情報共有の促進・拡充**			
項番	担当府省庁	2020 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。 「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進する。 「情報共有体制の強化」については、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。 「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。 「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。 「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。	・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）に関する取り組みを実施した（「安全基準等の整備及び浸透」については(ス)及び 2.1(1)(セ)、「情報共有体制の強化」については(コ)・(チ)・(ナ)、(2)(ア)及び 2.6(ア)、「障害対応体制の強化」については(ツ)、「リスクマネジメント及び対処態勢の整備」については(サ)、「防護基盤の強化」については(ク)に各取組内容を記載）。
（イ）	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。	・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、2020 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17 か所を 2020 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。
（ウ）	経済産業省	経済産業省において、安全・安心なクレジットカードの利用環境整備のため、クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」に基づき、関係事業者等の取組を更に推進する。	・令和２年改正割賦販売法においてセキュリティ対策義務の対象が拡充されたこと等に伴い、同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 2021 年３月に改訂し、関係事業者の取組を促進した。
（エ）	厚生労働省	保健医療情報を医療機関等で確認できる仕組みを推進していく中で、これまでの実証結果等を踏まえ、情報連携の必要性や技術動向、費用対効果等を検証しつつ、医師や患者の抵抗感、厳重なセキュリティと高額な導入負担など、推進に当たっての課題を踏まえた対応策の検討を進めていく。	・厚生労働省において、保健医療情報を医療機関で確認できる仕組みを推進していく中で、「特定健診や薬剤情報以外のオンライン資格確認等システムにある情報を全国の医療機関等で確認できる仕組み調査研究一式」において、地域実証、技術検証等を実施して、技術・運用及びセキュリティ等に係る課題・対応策等の検討を行った。
（オ）	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。	・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。

（カ）	厚生労働省	厚生労働省において、医療機器の安全性を担う医療機器製造販売業者、組織としての対策を行う医療機関、脆弱性や攻撃の分析を行うセキュリティ機関、自治体等と連携・協調して対応する。	・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。 ・2020 年５月には、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。
（キ）	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。	・経済産業省において、電力分野のサイバーセキュリティに関する今後の取り組み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、2020 年度中に３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た。
（ク）	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。
（ケ）	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するとともに、IPA 等、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。
（コ）	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。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
①リスクマネジメントの推進 **・リスクマネジメントの活動全体が継続的かつ有効に機能することに資する取組の推進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（サ）	内閣官房	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。	・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とりまとめ、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。
（シ）	金融庁	金融庁において、大規模な金融機関に対して、そのサイバーセキュリティ対応能力をもう一段引き上げるため、「脅威ベースのペネトレーションテスト」をグループ会社に拡大する等、グループベースでのリスクマネジメントの高度化を促していく。	・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）驚異ベース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、取組状況を確認。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
② 安全基準等の改善・浸透 **・安全基準等を改善する取組の継続的な推進** **・安全等を維持する観点を踏まえた制度的枠組みの適切な改善**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ス）	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、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。 加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、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における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、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。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）	［NISC］ ・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情報セキュリティ対策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、毎年度、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。 ［金融庁］ ・金融分野については、FISC において「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（第５版）改定版」の内容を包括した、「金融機関等コンピューターシステムの安全対策基準・解説書」を作成している。 ［総務省］ ・電気通信分野については、「事業用電気通信設備規則」、「情報通信ネットワーク安全･信頼性基準」及び「電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）」について、改善に向けた分析・検証を行っている。 ・放送分野における「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」と、ケーブルテレビ分野における「ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン」について統合し、より効率的な運用・情報共有を図ることとした。 ［厚生労働省］ ・水道分野については、令和２年４月に施行された「水道施設の技術的基準を定める省令の一部を改正する省令」（厚生労働省令第 59 号）において、水道事業の施設基準としてサイバーセキュリティ対策を位置付けた。 ・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」を第 5.1 版に改定した。 ［経済産業省］ ・電力分野においては「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」の改定を実施した。 ・ガス分野においては「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領」の改定を実施した。 ［国土交通省］ ・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。
（セ）	総務省	総務省において、ネットワーク IP 化の進展に対応して、ICT サービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。	・2019 年度に発生した電気通信事故の原因及び対応策等について分析・評価を行い、2020 年９月に公表した。 ・2019 年度に発生した「令和元年房総半島台風」、「令和元年東日本台風」における、広域かつ長期間の停電による電気通信サービスの大規模な障害を発生を踏まえた通信インフラの予備電源の長時間化に係る規定の見直し等について、2020 年６月に情報通信ネットワーク安全・信頼性基準を改正した。

（ソ）	厚生労働省	厚生労働省において、クラウド技術の進展等の技術動向等を踏まえた上で「医療情報システムの安全管理に関するガイドライン」の改定作業を行い、改定した内容について普及啓発に取り組む。	・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」を第 5.1 版に改定し、改定した概要についてホームページ上に掲載した。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。
（タ）	厚生労働省	2019 年度より実施している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において、2021 年度までの 3 年間の計画で、医療機関及び製造販売業者における、国内外での医療機器のサイバーセキュリティ対応状況を調査し、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を行い、医療機器のサイバーセキュリティ対策においてより具体的な対応策を検討する。	・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である。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
③深刻度評価基準 **・サイバー攻撃による重要インフラサービス障害等に係る深刻度評価基準の策定**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（チ）	内閣官房	内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に従い、情報共有体制の強化について次のとおり検討を進める。 ・効果的かつ迅速な情報共有に資するため、情報共有体制の改善に係る検討を行う。 ・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。	・「情報共有の手引書」を活用しつつ、情報共有を行い、コロナ禍をきっかけとし、重要インフラ事業者等向け注意喚起のうちテレワーク実施に係る留意点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。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
④官民の枠を超えた訓練・演習の実施 **・官民の枠を超えた様々な規模の主体間での訓練・演習の実施**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ツ）	内閣官房 総務省 経済産業省 金融庁	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 ・内閣官房において、重要インフラ事業者等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。	[NISC] ・内閣官房において、2020 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。 [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、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、2020 年度は、重要インフラ事業者等の民間事業者として 193 人が受講した。 [経済産業省] ・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３年間実施した。その経験及び第１期～第３期の修了者約 230 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４期「中核人材育成プログラム」を 2020 年７月に開講した。 [金融庁] ・金融業界全体のインシデント対応能力の向上を図ることを目的として、2020 年 10 月に金融機関約 110 社がサイバー演習（DeltaWallⅤ）に参加。今回新たに「インシデント対応能力のより一層の高度化を図ること」を目的に、社内でのディスカッションを通じてインシデント対応における社内エスカレーションから経営層の意思決定までの実効性を検証する演習を実施したほか、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。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
⑤制御系システムのセキュリティ対策 **・制御系システムの特性を踏まえたセキュリティ対策の実施** **・制御系システムに関する人材育成及び脅威情報の収集・分析・展開等の推進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（テ）	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、対象システム調査や情報提供の効率化を検討し、通知件数の増加を目指す。	・経済産業省において、JPCERT/CC を通じて、SHODAN などの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１件(2021 年３月末時点)について、その保有組織に対して情報提供した。
（ト）	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、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に向けた検討を行う。	・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の素案を策定した。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について利用状況を確認し、活用促進策や課題の検討を行った。
（ナ）	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。	・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の調査を行った。また、制御機器・システムの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。
（ニ）	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。	・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等も踏まえて、自動車産業分野等において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の策定を進めている。

(2) 地方公共団体のセキュリティ強化・充実

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より
・サービス障害や人為的ミスによるマイナンバーを含む情報漏えいへの対策 **・セキュリティポリシーに関するガイドラインの更新** **・業務用ネットワークのセキュリティレベルの確保** **・セキュリティ人材の確保・育成及び体制の充実を支援する取組の推進** **・官民の認証連携に関する環境整備**

項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（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。	［NISC］ ・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、コロナ禍をきっかけとし、地方公共団体を含む重要インフラ事業者等向け注意喚起のうちテレワーク実施に係る留意点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。 ［総務省］ ・情報セキュリティに係る脅威情報（インシデント情報）や脆弱性情報を収集・分析し、地方公共団体の情報セキュリティ確保に必要な情報を提供した。 （実績） 緊急連絡等注意喚起情報：114 件
（イ）	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。	【動画配信・ライブ研修】 （１）情報セキュリティ対策セミナー 定員 100 名　年５回実施 （２）情報セキュリティマネジメントセミナー 定員 54 名　年３回実施 （３）情報セキュリティ監査セミナー 定員 54　年３回実施 【e ラーニングによる情報セキュリティ研修実施状況】 実施期間 2020 年７月 28 日～12 月 25 日 受講者数 593,666 名
（ウ）	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。	・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 上のウェブサイトを用いて提供した。 （実績） メルマガ・ニュース発行：50 件

（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。	・地方公共団体が訓練ツールを用いた緊急時対応訓練を開催し、地方公共団体のインシデント即応体制の強化を図った。 （実績） 延べ 100 団体が参加 ・自治体 CSIRT 協議会の運営を支援し、CSIRT 構築に係る講習会、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 構築の手引きを提供し、CSIRT 設置の促進を図った。 （実績） CSIRT 構築に係る講習会：延べ 80 団体 技術講習会：延べ 39 団体 ブラインド方式によるインシデント対応訓練：10 団体
（オ）	内閣官房 内閣府 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を検討し、「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」の改定を実施するとともに、次期「自治体情報セキュリティクラウド」の構築にかかる要件等の地方公共団体への提示を行う。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、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、監視・監督機能を強化し、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。	［総務省］ ・「三層の対策」の効果や課題、行政手続のオンライン化の推進など新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策の検討を行い、令和２年 12 月 28 日に「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。 ・次期自治体情報セキュリティクラウドの標準要件を決定し、令和２年８月 18 日に地方公共団体及びクラウドサービス事業者への提示を行った。 ・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。 （実績） 自治体情報セキュリティ向上プラットフォーム：724 団体 ［個人情報保護委員会］ ・高い専門性や幅広い知識を有する人材を育成する観点から、他府省との人事交流や外部機関等において実施されるセキュリティ・IT 関連の研修等の受講促進に注力した。また、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を運用し、適切に監視を行った。
（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、開催方法等の工夫を引き続き行うとともに、各都道府県において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。	・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、2020 年度は、地方公共団体（広域連合等を含む。）から 1,778 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）	内閣府	内閣府において、デジタル・ガバメントの基盤であるマイナポータルを活用し、マイナンバーカードによる厳格な本人確認のもと、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、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。	・2020 年 10 月以降、年末調整及び確定申告手続において、民間送達サービスに届いた各種控除証明書のデータをマイナポータルを通じて一括取得し、自動入力できる仕組みとした。 ・2021 年５月頃までに、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、オンライン申請の受付が可能となる。

（ク）	厚生労働省	2021 年３月からのマイナンバーカードの健康保険証利用の仕組みの導入に向けて、システム構築等の準備を進める。また、マイナンバーカードの健康保険証利用の仕組みの導入に向けて、医療情報化支援基金を活用し、医療機関・薬局のシステム整備の支援を行う。	・資格確認の法定化等を定めた「医療保険制度の適正かつ効率的な運営を図るための健康保険法等の一部を改正する法律」（令和元年法律第９号）が 2019 年５月 15 日成立。マイナンバーカードの健康保険証利用の仕組みの 2021 年３月からの運用開始に向けて、システムを構築した。

2.3　政府機関等におけるセキュリティ強化・充実

(1) 情報システムのセキュリティ対策の高度化・可視化

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・対処能力の向上に加え、新たな防御技術を活用したより効果的な取組 **・情報システムの防御能力の向上と状態の把握** **・政府機関等における横断的な連携の高度化による被害の発生・拡大の防止**			
項番	担当府省庁	2020 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、政府機関等における情報システムのセキュリティ対策の進捗状況を把握するとともに、取組の促進に向けて必要な支援を行う。また、政府機関等全体としての情報セキュリティ水準の維持・向上を図るべく、最新の技術動向などを踏まえ、次期統一基準群改定に係る作業を行う。	・内閣官房において、2019 年度にとりまとめた次期統一基準群の改定コンセプトに基づき、2020 年７月に次期統一基準群の改定骨子を策定し、修正案の作成に着手した。
（イ）	内閣官房	内閣官房において、政府機関等の情報システムの調達におけるセキュリティ・バイ・デザインを推進するため、NISC が公表している関連の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、クラウドサービスの調達への対応等を踏まえた記載内容の見直し及び所要の改定を行う。	・内閣官房において、政府機関等の情報システムの調達におけるセキュリティ・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、クラウドサービスの調達への対応等を踏まえた記載内容の見直しの検討を行った。
（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 において、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容の見直しの準備として、CCRA における国際共通プロテクション・プロファイル（PP）の策定状況、日本を含む各国のプロテクション・プロファイルの策定状況の調査を行った。 ・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実施した。
（エ）	経済産業省	経済産業省において、IPA を通じ、CCRA などの海外連携、セキュリティ評価に係る国際基準の作成や各国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、情報収集を実施する。	・IPA において、CCRA の会合などに参加し、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。

（オ）	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を検討する。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。	・IPA において、統一基準(2018 年度版）で運用上のセキュリティ確保を求められている特定用途機器のうち、その形態が多様なネットワークカメラを対象に、JISEC の評価基準である CommonCriteria を用いた試行評価を実施し、技術的実効性を確認した。また、その結果を基に政府機関や自治体が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の作成に着手しセキュリティ機能要件を取りまとめた。 ・IPA において、JISEC の主要の評価対象製品分野である複合機のベンダーの業界団体である JBMIA(一般社団法人ビジネス機械・情報システム産業協会）の WG に参加し、そこでの議論を基に製品実装上の課題や他製品分野との要件の整合性維持に対応するためのテスト手法等に関する補足事項を「申請案件についてのガイドライン」に追記し改版を公開。申請者に対する利便性の向上を図った。
（カ）	経済産業省	経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するため IPA の運用する暗号モジュール試験及び認証制度（JCMVP）の普及を図るとともに、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。また、各国政府の暗号政策に関する実施体制や法制度の調査と合わせ、海外での認証制度の最新動向等の調査を実施する。	・経済産業省において、IPA を通じ、 ・「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９件発行した（その他、申請受付中５件）。 ・JCMVP 認証書を１件発行した。 ・サプライチェーン・リスクが重大なセキュリティ課題として認識されるようになってきている現状を鑑み、運営審議委員会を開催し、サプライチェーン・リスク等に対処するための JCMVP 規程類の大規模な改正を実施した。 ・暗号技術や規格化の動向を踏まえ、JCMVP 技術審議委員会を開催し、承認されたセキュリティ機能の見直しを実施した。 ・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。 ・各国政府の暗号政策に関する調査の一項目として、海外での認証制度についての最新動向の調査を実施した。
（キ）	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、政府機関等に対する新たなサイバー攻撃の傾向や情勢等について、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。	・2020 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。
（ク）	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、外部委託先が取り扱う政府が管理する情報が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行う仕組みを導入し、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、政府機関への注意喚起・調査を実施した。加えて、その他内外の情報セキュリティインシデントの状況も踏まえつつ、政府機関への影響が大きいと判断される事案についても注意喚起・調査を行った。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。

（ケ）	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を通じて、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の取組状況を調査し、その結果を取りまとめ報告した。
（コ）	内閣官房	内閣官房において、大規模災害やサイバー攻撃等における、情報システムを用いる業務についての復旧対策を強化するため、2019 年度に検討した改定案を踏まえて、「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）～」について、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等を盛り込んだ改定版を作成する。	・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、情報システムの運用に係わる新型コロナウイルス感染拡大等の影響及び対策事例を調査し、感染症対策に係わる検討事項を整理した。また、整理した検討事項を、2020 年度に作成した「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）～」の改定案へ盛り込み、有識者及び各府省庁の意見照会等を経た改定版を作成した。
（サ）	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。 加えて、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進めるため、タスクフォースを開催する。	・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。加えて、量子コンピュータ時代に向けた暗号の在り方検討タスクフォースを設置し、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進めた。
（シ）	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、2019 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、2020 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結果等を踏まえ、内閣官房と連携し、当該法人の情報セキュリティポリシーと政府統一基準の齟齬を改定するよう助言するなど必要な助言を行った。
（ス）	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各府省庁の調達案件に対し、助言を行う。2020 年度からは各府省庁に加え、独立行政法人及び指定法人に対しても助言を行う。	・2018 年 12 月に決定された、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」において、独立行政法人及び指定法人を取組の対象に加えた。「申合せ」に基づき、2020 年４月から 2021 年３月までに、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 3,515 件の助言を行い、その内 190 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。
（セ）	内閣官房	内閣官房において、東京 2020 大会とその後を見据えて、IPA の実施する独立行政法人等に係る監視業務も含めて、インシデント発生前及び発生時の情報提供の迅速化・高速化に資する GSOC システムの検知・解析機能を始めとした機能強化等を図るなど、政府機関等における端末等での新たな監視手法等の導入状況も踏まえつつ、政府機関等と次期 GSOC における効果的かつ効率的な連携を推進する。	・近年のサイバー攻撃事例や手法、最新の技術動向等を踏まえ、政府機関等と GSOC 間における効果的かつ効率的な連携を可能とする機能を実装した第４期 GSOC システム（2021 年度から運用を開始）の構築を行った。

(2) クラウド化の推進等による効果的なセキュリティ対策

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・政府プライベート・クラウドとしての政府共通プラットフォームへの移行を含むクラウド化の推進 **・信頼できるクラウドの利用を促進する方策の検討** **・政府機関のインターネット接続口の適切な集約の推進とともに、境界監視ポイントの集約の検討**			
項番	担当府省庁	2020 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、政府共通プラットフォーム第二期整備計画に基づき、IT リソースの効率的利用による政府情報システムの整備及び運用の効率化、政府情報システムの質の向上並びに政府の IT ガバナンスを支える基盤としての役割を果たすことを目的として、クラウドサービスを活用した新たな政府のプライベートクラウドを整備し、2020 年度（令和２年度）中にサービス提供開始を目指す。	・「政府共通プラットフォーム第二期整備計画」に基づき、クラウドサービスを活用した第二期政府共通プラットフォームを整備して、2020 年 10 月からサービス提供を開始し、利用システムに対して移行支援を実施した。
（イ）	内閣官房 総務省 経済産業省	内閣官房、総務省及び経済産業省において、2020 年度内に、全政府機関がクラウドサービスのセキュリティ評価制度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、取組を進める。	・安全性が評価されたクラウドサービスの利用に関して、サイバーセキュリティ戦略本部決定（2020 年１月 30 日）において示された基本的枠組みに基づき、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）」（以下「ISMAP」という。）の立ち上げを行った。 ・ISMAP においては、2020 年８月にクラウド事業者の監査を行う監査機関を選定・公表するとともに、2021 年３月に、安全性が評価されたクラウドサービスリストの公開を行った。
（ウ）	内閣官房 総務省	内閣官房及び総務省において、政府機関のインターネット接続口の集約を推進し、GSOC による境界監視の効率化を引き続き検討する。	・セキュリティ対策の効率化の観点も踏まえつつ、第４期 GSOC システムの構築を行った。

(3) 先端技術の活用による先取り対応への挑戦

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・新しい設計思想の下で誕生した情報技術の活用の可能性の検討			
項番	担当府省庁	2020 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、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への反映等により周知を行う。	・内閣官房において、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」の見直しに合わせて高度なセキュリティ機能を備える OS を搭載したスマートフォンやタブレット端末の利用に係る記載の追加について検討を行った。

(4) 監査を通じたサイバーセキュリティの水準の向上

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・組織横断的な分析により抽出される傾向や課題を踏まえたサイバーセキュリティ水準向上の促進 **・IT 資産管理情報を活用した効果的かつ効率的な監査の実施**			
項番	担当府省庁	2020 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、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。	・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、2020 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。さらに、厚生労働省及び日本年金機構に対する施策の評価を行った。
（イ）	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、2019 年度に侵入検査を実施した情報システムのうち、提出された改善計画において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。	・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った。また、2019 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。
（ウ）	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。	・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、2020 年度は、31 の国の独立行政法人等（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、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。
（エ）	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、2020 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、2019 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。	・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、2020 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セキュリティの改善・維持のため、有益な助言等を行った。また、2019 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。

(5) 組織的な対応能力の充実

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・事案対応を行うチームを中心に事案対応能力や情報セキュリティに係る知識の向上 **・情報セキュリティ緊急支援チームの要員の対処能力の向上**			
項番	担当府省庁	2020 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、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。	・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、民間事業者が保有するフォレンジック調査、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。
（イ）	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ともに、より連携を強化するための新たな取組を検討する。	・CSIRT 会合は、2020 年度は３回開催する予定だったが、新型コロナウイルスの感染拡大防止の観点から、全ての回で開催中止となった。
（ウ）	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、要請に応じて、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り教育機会の付与に取り組む。	・内閣官房において、政府機関や独法・指定法人等の職員向けに、2018 年度版統一基準の解説及び情報セキュリティ監査をテーマとした NISC 勉強会を資料配付により開催した。 ・内閣官房において、2021 年４月に実施される国家公務員合同初任者研修における研修カリキュラムの中で使用する資料等について、近年のサイバーセキュリティに関する情勢を踏まえて作成し、人事院に提供した。

（エ）	内閣官房 総務省	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、以下の訓練及び演習を実施する。 ・内閣官房において、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。 ・内閣官房において、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、政府機関等のサイバー攻撃対処能力の更なる向上に向けた推進方策を検討する。 ・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）を実施する。	・内閣官房において、府省庁における CSIRT 要員を対象とし、インシデント発生時における適切かつ円滑な対処を企図した訓練及び演習を全 22 府省庁個別に実施した。CISO 等の幹部との連携も実践することで、組織的対処能力の向上も図った。2020 年度は、訓練成果の実感を高めるため、最新事例や業務継続の観点を取り込んだ訓練シナリオを採用した。また、訓練直後に CSIRT 要員へのヒアリングを府省庁個別に行い、対処状況の確認及び助言を実施し、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。 ・内閣官房において、インシデント発生時における対処能力の向上を図るため、府省庁、独立行政法人及び指定法人における CSIRT 要員に対して、技術的事項の習得に重点を置いた研修を 2020 年度は４回実施した。 ・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年間を通じて実施した。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 ・内閣官房において、政府関係職員のサイバー攻撃解析・対処能力の向上及び人材発掘を目的として、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「令和２年度 NISC-CTF」をオンライン形式で開催した。 ・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、2020 年度は、国の行政機関や独立行政法人等から 677 人が受講した。

2.4　大学等における安全・安心な教育・研究環境の確保

(1) 大学等の多様性を踏まえた対策の推進

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・大学等における計画等に基づく自律的かつ組織的な取組の促進 **・サイバーセキュリティに関するガイドライン等の策定と普及** **・各層別研修及び実践的な訓練や演習の実施** **・事案発生時の初動対応への支援**			
項番	担当府省庁	2020 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、大学等に対し策定を求めた「サイバーセキュリティ対策等基本計画」が着実に実施されるよう、フォローアップを行う。 ・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」（「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。	・国立情報学研究所（NII）において、「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（平成 30 年度版）」に対応した「高等教育機関の情報セキュリティ対策のためのサンプル規程集」を、2021 年３月に公開した。情報格付け基準、情報格付け取り扱い基準の見直しや情報発信ガイドライン等最新の情勢に合わせて見直を行った。
（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およそ 800 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	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、フォレンジック手法の整備、またさらなる外部のセキュリティ機関等との連携強化を行う。	・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。また、さらなる外部のセキュリティ機関等との連携強化を行い、サイバーセキュリティアドバイザーを増員した。

(2) 大学等の連携協力による取組の推進

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバー攻撃への監視能力の機能維持・強化 **・戦略マネジメント層の育成に向けた共同研究や技術職員への研修の実施** **・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への支援**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ア）	文部科学省	国立情報学研究所（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、国立大学法人等へのサイバー攻撃の情報提供を引き続き実施するとともに、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充実させる。また、NII-SOCS 参加機関において自機関への攻撃情報を自ら解析できる仕組みの構築、提供を図る。	・国立情報学研究所（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に、国立大学法人等へのサイバー攻撃の情報提供を実施した。また、インシデント発生時の危機管理を考えるきっかけを目的とし国立大学法人等の CSIRT 担当者を対象とした「インシデントマネジメント研修」をオンラインにて１回実施し、インシデント対応手順に関して複数の大学間で情報交換を行う事ができた。また、「NII-SOCS 参加機関において自機関への攻撃情報を自ら解析できる仕組み」について構築し提供を図った。

（イ）	文部科学省	国立情報学研究所（NII）において、国立大学法人等のサイバー攻撃耐性を向上させるため、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提供、共有することで、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提供するシステムを構築し、参加機関に対して研究用データとしての提供を開始した。
（ウ）	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、「学術系 CSIRT 協議会」にオブザーバーとして参加し、複数の大学等の事案対応を行うチームにおいてサイバー攻撃に関する情報や共通課題、事案対応の知見等の共有を行った。 ・また、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において共有を行った。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、同知見について共有を行った。

2.5　東京 2020 大会とその後を見据えた取組

(1) 東京 2020 大会に向けた態勢の整備

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・「セキュリティ幹事会」で決定された基本戦略に基づく取組の推進 **・大会の安全に関する情報の集約等の取組の推進** **・リスク評価及び明らかになったリスクへの対策の促進** **・「サイバーセキュリティ対処調整センター」の構築の推進と連絡調整態勢の整備**			
項番	担当府省庁	2020 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、引き続き、リスクマネジメントの促進と対処態勢の整備・運用を推進する。 ・「リスクマネジメントの促進」については、NISC が作成した手順に基づくリスクアセスメントの取組及び横断的リスク評価の取組を繰り返し実施する。情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、残存リスクが顕在化した場合の対応体制の強化を促進させる。 ・「対処態勢の整備・運用」については、大会まで重要サービス事業者、大会組織委員会、東京都等が参加する情報共有及びインシデント発生時の対処支援調整等の訓練・演習を実施し、大会関係組織間で緊密に連絡調整を図るための態勢を整備する。	・東京大会に向けた取組に関しては、引き続き、サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、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。 ・重要サービス事業者等を対象に、第６回のリスクアセスメントの取組として大会延期や新型コロナウイルスの感染拡大に伴う環境変化を踏まえたリスクの見直し、残留リスクが顕在化した場合の対処体制の強化を推進した。 ・各事業者等から提出されたリスクアセスメント結果を分析し、個別にフィードバックを実施するとともに、必要に応じ助言を実施した。 ・2019 年度の横断的リスク評価で対象とした重要サービス事業者等（会場（レガシー部分）を含む。）における改善状況についてフォローアップを実施した。 ・横断的リスク評価において、重要サービス事業者等（会場（レガシー部分）を含む。）に対して引き続き検証を実施した。 ・サイバーセキュリティ対処調整センターで構築した情報共有システムにより脅威情報等を提供するとともに、同システムを活用して重要サービス事業者等が参加する演習を２回実施した。

（イ）	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する。	・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。
（ウ）	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する。（※セキュリティ調整センターについては 2020 年３月に設置。大会の延期の決定に伴い一旦廃止。）	・2021 年３月に設置した「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、本番を見据えた実践的な訓練を実施し、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した。

(2) 未来につながる成果の継承

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・東京 2020 大会の態勢整備のための各種施策の継続推進 **・整備した仕組み、運用経験及びノウハウの活用** **・「サイバーセキュリティ対処調整センター」のナショナル CSIRT としての活用** **・「リスクアセスメント」の手法の全国の事業者等への適用とそのための整備・普及**			
項番	担当府省庁	2020 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、東京 2020 大会に向けた態勢の整備等を最優先に推進するとともに、整備した仕組み、その運用経験及びノウハウをレガシーとするため、有効な点、反省点を整理して、大会後に適切に評価できるような工夫及びレガシーとするに当たっての課題について検討を実施する。	・未来につながる成果の継承については、2020 年東京大会に向けた態勢の整備等を最優先に推進した。整備した仕組み、その運用経験及びノウハウをレガシーとするため、第三者の意見を踏まえた上での検討を開始できるように有識者会議を設置し検討を開始した。検討結果を次期戦略へ反映させる方向で検討を進めている。
（イ）	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。	［警察庁］ ・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。 ［法務省］ ・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。
（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」を通じ、東京 2020 大会の大会関連組織のセキュリティ担当者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演習である「サイバーコロッセオ」について、大会の延期等の状況を鑑みた上で、大会組織委員会と緊密な連携を図りながら実施する。	・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、東京オリンピック・パラリンピック競技大会の大会関連組織のセキュリティ担当者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演習である「サイバーコロッセオ」を実施し、2020 年度は延べ 168 名が受講した。

2.6　従来の枠を超えた情報共有・連携体制の構築

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・ISAC を含む既存の情報共有の推進			
項番	担当府省庁	2020 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）	・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。
（イ）	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。 ・2020 年度は新たに 14 組織が参加し、15 業界 275 組織の体制で運用。6,202 件の情報提供を受け、147 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。
（ウ）	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。	・ICT-ISAC の会員企業を順次拡大し、ICT-ISAC を核とした通信事業者、放送事業者、CATV 事業者、セキュリティベンダー等の情報通信分野全体における情報共有を促進した。また、日米 ISAC 間での脅威動向や対策の取組に関する意見交換会を開催し、日米の情報通信分野 ISAC 組織間における情報共有を行った。
（エ）	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。	・国土交通省において、法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」が、2020 年４月に一般社団法人として設立され、2021 年３月現在 79 会員まで増加している。
（オ）	金融庁	金融庁において、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、2020 年５月現在、「金融 ISAC」の加盟社は 421 社（正会員）まで増加。
（カ）	厚生労働省	厚生労働省において、医療分野及び水道分野における ISAC 等のサイバーセキュリティ対策に関する情報共有のあり方について引き続き検討を行う。医療分野については、医療機関、医療機器メーカー、製薬メーカー、検査機器メーカー等と連携のあり方や支援のあり方について、引き続き検討を行う。	・水道分野については、水道分野の ISAC について、海外の事例を調査・情報収集しているところである。 ・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・相談体制の試行を行った。また、医療機関と各メーカー等との連携のあり方について検討を行い、医療機器メーカーとの連携促進を目的に、医療セプターに一般社団法人日本医療機器産業連合会をオブザーバーとして加入できるように協力した。
（キ）	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。	・2020 年 10 月に開催したクレジットセプター運営会議において、JPCERT/CC からサイバー攻撃の動向等に関する講演・意見交換を行った。
（ク）	経済産業省	経済産業省において、2020 年度以降、自動車業界の「J-Auto-ISAC」等の情報共有機関等に対して、サプライヤー等の更なる参加を促し、同機関等を通じた情報共有網の更なる拡充を進める。	・自動車業界の「J-Auto-ISAC WG」等の情報共有体制の活動が進み、2021 年２月に日本自動車工業会及び日本自動車部品工業会による一般社団法人 J-Auto-ISAC が設立。同機関等を通じ、情報共有・解析及びソフトウェア人材育成等を進める。

（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、22 件の「早期警戒情報」を発行した（2021 年３月末現在）。 ・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：2021 年３月末現在）。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、12 件の月次ニュースレター、65 件のニュースクリップなどの情報発信を行った。（全て 2021 年３月末時点）
（コ）	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、捜査で得た手口の情報等を活かし、一般財団法人日本サイバー犯罪対策センター（JC3）を通じた産学官連携した取組を進める。	・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。
（サ）	総務省	総務省において、ICT-ISAC に設立された「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、当該取組について、ローカル 5G の免許手続との連動や円滑な活動の支援を実施する。	・総務省において、ローカル 5G の免許人に対し、ICT-ISAC の「5G セキュリティ推進グループ」の周知・啓発を行った。また、当該グループにおいて検討を進めているローカル 5G のセキュリティに関するガイドラインの作成に向けた情報収集のためのアンケート調査を、総務省から免許人に対して配布した。

(1) 多様な主体の情報共有・連携の推進

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・情報共有に十分な知見を有する専門機関を含む官民の多様な参加主体が、安心して相互に情報共有を図るための体制の構築 **・官民、業界、国内外といった枠を超えた情報共有・連携の推進** **・既存の情報共有体制についての連携や統合の検討**			
項番	担当府省庁	2020 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、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、より多くの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、2020 年６月に第３期構成員を決定するとともに、2020 年 12 月から 2021 年１月にかけて第４期構成員の募集を行い、同年３月に第４期構成員を決定し、官民又は業界を超えた全 266 者の多様な主体に参加していただいている。

(2) 情報共有・連携の新たな段階へ

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・積極的に情報提供に協力する者ほど恩恵を享受できる仕組みの検討 **・情報処理の自動化の推進** **・参加主体が従来の枠を超えて共存・発展する関係構築に向けた環境整備の推進**			
項番	担当府省庁	2020 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。	・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３月末時点で、協議会において取り扱った情報の件数は全 44 件（うち昨年度からの継続案件６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 12 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。

2.7　大規模サイバー攻撃事態等への対処態勢の強化

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化 **・サイバー空間における情報収集・分析機能及び緊急対処能力の向上**			
項番	担当府省庁	2020 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、東京 2020 大会を見据え、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、新型コロナウイルス感染症に係る状況を踏まえつつ、2020 年度上半期に大規模サイバー攻撃事態等への対処能力維持のための訓練を行う。	・2020 年度上半期に大規模サイバー攻撃事態等対処訓練を関係省庁とともに実施し、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。一方、2020 年度下半期に東京 2020 大会を見据え、大規模サイバー攻撃事態等対処訓練を計画していたところ、新型コロナウイルス感染症に係る状況に鑑み、年度中の実施を見送った。なお、当該訓練は、2021 年度上半期（東京 2020 大会前）に延期して実施することを予定している。
（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。	・大規模サイバー攻撃事態等対処訓練に参加し、大規模なサイバー攻撃発生時における初動対処（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	警察庁及び都道府県警察において以下の取組を推進することにより、サイバー攻撃対処態勢の強化を推進する。 ・都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処態勢の強化を推進する。 ・警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。 ・警察庁及び都道府県警察において、分析官等の育成や、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理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。	・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・警察庁において、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、重要インフラ事業者等への個別訪問、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もとに対処の任につく警察職員へ教養を実施したほか、関係機関と連携して制御システムに係る情報収集や共同研究を行った。 ・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、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）	・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、22 件の「早期警戒情報」を発行した（2021 年３月末現在）。 ・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：2021 年３月末現在）。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、12 件の月次ニュースレター、65 件のニュースクリップなどの情報発信を行った。（全て 2021 年３月末時点）
（オ）	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公開情報の収集・分析等を通じた知見の蓄積を図り、被害組織における迅速な対応・復旧に向けた計画作りを支援する。国際イベントに対するサイバー攻撃を念頭においた情報収集と、関係組織への情報提供を実施する。	・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 102 件行うとともに、うち 17 件に対してオンサイトでレスキュー活動を実施した。

（カ）	内閣府	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事案の詳細の把握に努めるとともに、必要に応じて事業者に対し指導・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。	・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個人情報取扱事業者において適切に実施されるよう、関係省庁とともに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、個人情報等の漏えいを取り巻く状況や EC サイトに対する不正アクセスの動向等についての意見交換を行うとともに、委員会に報告された漏えい等事案について情報共有等を行った。また、EC サイトにおいて、システム変更時の設定の不具合により、ログインしているユーザとは別のユーザの個人情報が表示されるという事象について、他の多くのウェブサイトでも発生しうるものであったため、委員会ウェブサイトにおいて、本事象の公表及び同種事象の発生防止のための注意喚起を行った。
（キ）	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。	・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 2020 年３月末時点では 388 組織であったが、2021 年３月末現在で 407 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。
（ク）	金融庁	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」を立ち上げ、連携態勢の強化に取り組む。	・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。

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堅持

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・グローバル規模で自由、公正かつ安全なサイバー空間を実現するための、国際場裡における理念の発信、サイバー空間における法の支配の推進			
項番	担当府省庁	2020 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。特に 2020 年度は、国連政府専門家会合が本格化するところ、国際会議の場において、サイバーセキュリティに関する自由、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。	・2020 年、国連政府専門家会合（UNGGE）においてメンバー国として法の支配の推進のため議論に積極的に貢献した他、国連オープンエンド作業部会（OEWG）の報告書がとりまとめられ、国際法がサイバー空間に適用されること等が確認された。 ・2019 年 G20 大阪サミットで日本が提示した DFFT（信頼ある自由なデータ流通）については、2020 年 G20 リヤド・サミットにおいても、DFFT 及びデジタル経済を促進することの重要性が認識された。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・日本型のサイバーセキュリティの基本的な在り方の発信、サイバー空間の発展を妨げるような国際ルールの変更等を目指す取組への対抗			
項番	担当府省庁	2020 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、我が国の意見表明や情報発信に努める。2019 年６月、G20 大阪首脳宣言において、デジタル経済における DFFT（信頼性のある自由なデータ流通）等を促進する必要性が合意されたことを踏まえ、越境データ規制、ソースコード開示、国家によるインターネットの資源管理等、自由な情報の流通を阻害するような動きに対抗し、自由、公正かつ安全なサイバー空間を実現する。 また、サプライチェーン・リスク対策には国際連携が重要であるところ、関係国と連携して対策を進める。	・米英等を始めとする、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、能力構築支援、サプライチェーン・リスク、データの自由な流通等のサイバーに関する最近の諸課題について議論を行い、相互の理解を深めている。 ・米英等も参加するサイバーセキュリティに関する有志国会合へ参加し，自由，公正かつ安全なサイバー空間の実現を阻害するような動きやサプライチェーン・リスクを念頭に，様々な取組に関して議論した。 ・各種国際会議等での議論やパネルディスカッション等を通じ、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。
（イ）	経済産業省 外務省	経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（デジタル保護主義）を取る諸外国に対し、対話、意見交換、パブリック・コメントの提出等を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、主要国の規制情報等を収集しつつ、民間団体とも連携して働きかけを行う。	・中国、ベトナム等のサイバーセキュリティ法及び関連法・施行規則に関し、WTO での議論等を通じて、要件・定義・手続きの明確化、透明性の確保、貿易制限的な運用を行わないこと等を要請した。

(2) サイバー空間における法の支配の推進

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論への積極的な関与			
項番	担当府省庁	2020 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、各二国間協議や国際専門家会合等の多国間協議に参画し、多国の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、それらに我が国の意向を反映させる。一昨年の国連総会決議に基づき、サイバーセキュリティに関する国連政府専門家会合（UNGGE）第６会期及び OEWG（Open-ended Working Group）が立ち上がり、責任ある国家の行動規範に係る議論について、引き続き積極的に参加していく。	・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。 ・米英等も参加するサイバーセキュリティに関する有志国会合へ参加し、自由、公正かつ安全なサイバー空間の実現を阻害するような動きやサプライチェーン・リスクを念頭に、サイバー空間における国際法の適用や国際的なルール・規範作り等を含め、様々な取組に関して議論した。 ・2020 年は新型コロナウイルス感染症により、対面での公式会合の開催に至らなかったものの、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可能性等について、メンバー国として積極的に議論を重ねてきた。同じく、国連オープンエンド作業部会（OEWG）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、コンセンサスによる報告書の発出に貢献した。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバー犯罪に関する条約、刑事共助条約、ICPO 等の枠組みを活用した国際機関、外国法執行機関、外国治安情報機関等との間における国際捜査共助や情報交換等による国際連携			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（イ）	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。
（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。	・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）	外務省	外務省において、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、UNODC プロジェクトへの拠出、第 14 回国連犯罪防止刑事司法会議（京都コングレス）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いつつ、サイバー犯罪に関する条約の普遍化に取り組む。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、関係国と連携して取り組む。	・日 ASEAN 統合基金を活用し、ICPO が現在実施中の 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２年度通常予算及び令和元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。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遍化に取り組んだ。さらに、京都コングレスの政治宣言において各国の法執行機関等が技術の発展に応じた能力構築を促進することを確認した。 ・サイバー犯罪に関する新条約の議論においては、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。

3.2　我が国の防御力・抑止力・状況把握力の強化

(1) 国家の強靭性の確保

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
①任務保証 ・政府機関及び重要インフラ事業者等におけるサイバーセキュリティの確保の推進 ・防衛省・自衛隊のサイバー攻撃対処を行う部隊の能力向上、自らの活動が依存するネットワーク・インフラの防護強化、自衛隊の任務保証に関連する主体との連携の深化			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
(ア)	警察庁	都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、以下の取組を実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処能力の向上を推進する。 ・重要インフラ事業者等に対し、各事業者におけるサイバーセキュリティ対策の状況を確認するとともに各事業者等の特性に応じた情報提供や保有するシステムに対するぜい弱性試験を実施する。 ・事案発生を想定した共同対処訓練を実施する。 ・サイバーテロ対策協議会を通じて、参加事業者間の情報共有を推進する。	・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。政府機関及び重要インフラ事業者等におけるサイバーセキュリティを確保するため、引き続き当該取組を推進する。
(イ)	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続監視等を強化するための最新技術を適用していく。	・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。
(ウ)	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より一層深化させていく。	・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、事案発生を想定した共同訓練及び脅威情報等の情報共有を実施した。また、自衛隊の任務保証に関連する主体との連携を深化させるため、重要インフラへのサイバー攻撃等に起因する障害が発生した場合の情報共有について関係省庁との意見交換を実施した。
(エ)	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・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）を実施した。
(オ)	防衛省	防衛省において、サイバー攻撃等によって防衛省・自衛隊の情報通信基盤の一部が損なわれた場合においても、運用継続を実現するためのサイバーレジリエンス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、サイバー攻撃等によって防衛省・自衛隊の情報通信基盤の一部が損なわれた場合においても、運用継続を実現するためのサイバーレジリエンスに関する研究試作について試験評価を実施した。
(カ)	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を実施するとともに試作品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を実施した。
(キ)	防衛省	防衛省において、装備品内部の情報処理機能を標的としたサイバー攻撃へ対処する技術の検討を実施する。	・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対処する技術の検討を実施した。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 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 **・防衛産業において、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組の実施** **・国立研究開発法人や先端的な技術情報を保有する大学等における対策の促進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ク）	防衛省	防衛省において、サプライチェーン・リスクに係るサイバーセキュリティの動向に係る調査研究を実施し、サプライチェーン・リスク対策の維持・強化に努める。	・防衛省において、情報システムのサプライチェーン・リスクに係るサイバーセキュリティの動向の調査研究を実施し、サプライチェーン・リスク対策の維持等に努めた。また、サプライチェーン・リスク対策に係る規則を改正し、実効性の更なる向上を図った。
（ケ）	内閣官房 文部科学省	科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。 ・内閣官房において、先端的な技術を保有する国立研究開発法人が、自立的に情報セキュリティ対策を講じていくことができるよう、引き続き国立研究開発法人相互の協力の枠組みを通じて取組を促す。 ・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。	［NISC］ ・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への対策を引き続き推進した。 ・ガバナンス体制の確立に向けた支援を行うとともに、国立研究開発法人の業務特性に応じた課題への検討結果を盛り込み公表した統一基準に基づき、マネジメント監査及び侵入検査（ペネトレーションテスト）を行い有益な助言等を行った。 ・また、国立研究開発法人協議会に対する情報提供や助言を通じて国立研究開発法人相互の協力による自立的活動の向上を支援した。 ［文部科学省］ ・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。
（コ）	防衛省	2020 年度中に、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を米国の新たな基準と同程度まで強化する改正を実施する。	・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た。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 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 **・サイバー空間におけるテロ組織の活動に関する情報の収集・分析の強化その他の必要な措置の実施**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（サ）	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。

（シ）	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、人的情報やオープンソースの情報を幅広く収集するなどにより、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。	[警察庁] ・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・分析を推進した。 [法務省] ・法務省（公安調査庁）において、新型コロナウイルスの感染拡大をめぐる情勢も踏まえ、人的情報やサイバー空間におけるオープンソースの情報を幅広く収集すること等により、過激思想の伝播活動を含むテロ組織等の動向に関する情報収集・分析を強化し、得られた情報を適時適切に関係機関に提供した。
（ス）	外務省	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である GIFCT（Global Internet Forum to Counter Terrorism）の独立諮問委員として、外務省においては、「サイバー空間におけるテロ組織の活動」への具体的な対策についての議論に参加し、企業による自発的な取組を引き続き推進する。	・GIFCT（Global Internet Forum to Counter Terrorism）の諮問委員会は，2020 年６月に正式に発足（議長選出）し、2020 年 10 月から２ヶ月に１回のペースで会合（オンライン）を開催している。 ・諮問委員会は多様なメンバー（政府，学術会，NGO）からなり、外務省国際安全・治安対策室長が日本の諮問委員として議論に参加している。 ・オンライン上での拡散を防ぐべきコンテンツとして，いわゆるイスラム過激主義コンテンツのみならず、欧米では極右関連コンテンツなどを含むべきという議論が主流となる中、諮問員会においては、企業の対応のあり方等について、様々な立場の諮問委員による活発な議論が行われており、その結果は GIFCT（企業のコンソーシアム）にもインプットされている。

(2) サイバー攻撃に対する抑止力の向上

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
①実効的な抑止のための対応 **・我が国の安全保障を脅かすようなサイバー空間における脅威への、同盟国・有志国と連携し、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用した対応** **・法執行機関、自衛隊を始めとする関係機関の能力強化**			
項番	担当府省庁	2020 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 月に策定された新たな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くため、2020 年度予算案において所要の事業を計上した。
（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。	・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、「サイバー攻撃特別捜査隊」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。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
②信頼醸成措置 **・偶発的、不必要な衝突を防ぐための、国際的な連絡体制の構築** **・二国間・多国間協議における情報交換、政策対話等を通じた信頼醸成**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（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、サイバー攻撃を発端とした不測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。	・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二国間協議を通じて、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、相互理解を深めてきた。 ・特に ARF の枠組では、2021 年１月に、オンラインにて、サイバーセキュリティに関する ARF 会期間会合のための第６回専門家会合を、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及びサイバーセキュリティに関する幅広い問題を議論した。
（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。	・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 24 の経済地域の 28 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（2021 年３月末時点） ・FIRST、APCERT 等の CSIRT コミュニティイベント積極的に参加し、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

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
①関係機関の能力向上 **・関係機関の情報収集・分析能力の質的・量的向上** **・高度な分析能力を有する人材の育成・確保、サイバー攻撃を検知・調査・分析等するための技術の開発・活用** **・カウンターサイバーインテリジェンスに係る取組の推進**			
項番	担当府省庁	2020 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。	・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 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を推進するなど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、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］ ・都道府県警察においてサイバー攻撃に係る捜査を推進するとともに、警察庁において、サイバーインテリジェンス情報共有ネットワークを通じて民間事業者等から提供された情報や、海外の捜査機関外国治安情報機関等から寄せられた情報を集約し、分析することで、サイバー攻撃の実態解明を推進した。 ・警察庁において、サイバー空間の脅威に関する知見を有するセキュリティ関連事業者に対し、サイバー攻撃に関する情報について調査を委託し、情報の提供を受けた。 ［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、得られた情報を適時適切に関係機関に提供した。
（ウ）	警察庁	警察庁及び都道府県警察において､以下の取組を推進することによりサイバー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、重要インフラ事業者等への個別訪問、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もとに対処の任につく警察職員へ教養を実施したほか、関係機関と連携して制御システムに係る情報収集や共同研究を行った。 ・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）	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
（オ）	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回発行した。 ・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、１回遠隔によるトレーニングを実施した。
（カ）	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。

（キ）	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。	・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。 ・部外団体が主催するセキュリティコンテストに協賛し、防衛省・自衛隊でのサイバー業務に関する紹介等を実施した。 ・人材確保の新たな方法として、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とした「防衛省サイバーコンテスト」を開催した。
（ク）	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。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
②脅威情報連携 **･同盟国･有志国との脅威情報共有の推進** **･政府内の脅威情報共有･連携体制の強化**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ケ）	内閣官房	内閣官房において、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の動向等の情報収集・分析を継続的に実施していく。	・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。
（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。
（サ）	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、諸外国関係機関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・分析を引き続き強化する。	［警察庁］ ・警察庁において、諸外国関係機関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ている。 ［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

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・国際場裡での我が国の立場を主張できる官民の人材を確保し、育成する。			
項番	担当府省庁	2020 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、各国機関との連携、FIRST、RSA カンファレンス、Black hat 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技術者等と切磋琢磨しながら研鑽を積む場を増やす。	・FIRST 年次会合、Black Hat USA 等の会議にオンライン参加したほか、各国政府、ベンダー、その他のステークホルダーのイベントにも参加し、知見・技術動向、サイバー環境の潮流に関する情報への接点や意見交換の機会を積極的に設けた。また、NISC 主催の演習を開催し関係者のスキル向上を図った。

(1) 知見の共有・政策調整

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバーセキュリティに関する二国間の協議や国際会議を通じた、互いのサイバーセキュリティ政策や戦略、体制の情報交換の実施 **・戦略的パートナー国とのサイバーセキュリティ施策に関する協力・連携の強化**			
項番	担当府省庁	2020 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政策の底上げに資する実務的な協力活動の充実を進める。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によって培われた知見や経験の相互共有を促進する。	・「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（基本方針）」（2016 年 10 月）に基づいて、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みを行った。 ・日・ASEAN サイバーセキュリティ政策会議を継続して開催し、日・ASEAN におけるサイバーセキュリティの相互理解と連携を強化した。特に、重要インフラ分野のセキュリティ確保に対する協議及び能力構築支援を通じ、各国政府との情報連絡体制の強化及び対処能力の向上が図られた。
（イ）	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、ADMM プラス EWG(2021 年３月）への参加を通じ、東南アジア各国との連携強化に努めた。
（ウ）	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。	・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、2020 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（タイ、ベトナム、モンゴル）のみでの実施となった。加えて、タイ、バングラデシュにおいて、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。
（エ）	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国家サイバー戦略等も踏まえつつ、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、同盟国である米国とのサイバー空間に関する幅広い連携を強化する。	・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、３月中旬に開催した日米 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。

（オ）	総務省	総務省、外務省及び関係府省庁において、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にて一致した、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、引き続き米国との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。	・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。
（カ）	経済産業省	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や技術共有等に取り組む。	・経済産業省において、IPA を通じ、日本の暗号モジュール試験及び認証制度 JCMVP において採用した、ISO/IEC 19790:2012 に基づく暗号モジュール認証の取組みとその知見を、2020 年９月にオンライン開催された International Cryptographic Module Conference（ICMC）2020 において発表し、米 NIST 及び加 CCCS を含む北米 Cryptographic Module Validation Program（CMVP）と共有を図った。また、2021 年３月にオンライン開催された The International Conference on the EU Cybersecurity Act に参加し、EU Cybersecurity Act 施行に伴う認証制度改革の情報収集に努めた。
（キ）	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、新たな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、2+2（2021 年３月）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。
（ク）	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、引き続き二国間協議の枠組みを通じ、2018 年に策定された我が国のサイバーセキュリティ戦略やＥＵ・欧州各国のサイバーセキュリティ体制強化の動きを踏まえつつ、欧州等各国との連携を強化する。 ・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。	［NISC、外務省］ ・欧州諸国とは、当局間会合等を実施し、サイバーセキュリティに関する政策に係る意見交換を行った。 ・その他、2020 年 12 月に開催された第５回日中韓サイバー協議では、最近のサイバー環境やサイバー分野における各国の施策、新型コロナウイルス感染症がサイバーセキュリティに及ぼす影響等について意見交換を行うとともに、国連サイバー政府専門家会合（UNGGE）や国連オープンエンド作業部会（OEWG）を始めとする国際的なプロセス、サイバー問題等に関する日中韓協力が可能な分野について議論を行った。 ［防衛省］ ・防衛省において、2019 年３月より NATO 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。
（ケ）	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、国際的な会議の場等を活用し、二国間協議に加え、各国とのサイバーセキュリティ分野における関係を引き続き強化する。	・オンラインで開催された Meridian 会合、FIRST 年次会合等に参加し、次年度の活動計画について議論した。 ・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、能力構築支援、サプライチェーン・リスク、データの自由な流通等のサイバーに関する最近の諸課題について議論を行い、相互の理解を深めている。
（コ）	警察庁	・警察庁において、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国際的な連携強化を推進する。 ・FIRST 会合等に参加し、情報交換等国際的な連携を通じて、諸外国関係機関との連携強化を図る取組を実施する。	・警察庁において、諸外国関係機関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。 ・FIRST 会合等に参加し、情報交換等国際的な連携を通じて、諸外国機関との連携強化を図る取組を実施した。

（サ）	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 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。	・経済産業省において、IPA を通じ、 ・JHAS オンライン会合に６回、ToR サブグループのオンライン会合に 10 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。 ・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。
（シ）	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。	・防衛省において、諸外国と脅威認識の共有やサイバー攻撃対処に関する意見交換等を行った。

(2) 事故対応等に係る国際連携の強化

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・CERT 間連携の強化 **・国際サイバー演習への参加、共同訓練等を通じた連携対処能力の向上**			
項番	担当府省庁	2020 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等のサイバー空間に関する多国間の情報共有枠組み等に参画し、我が国の情報収集及び情報発信の両面での能力強化を行う。また、インシデント対応演習や机上演習等を通じて、各国との情報共有や国際連携、信頼醸成を推進し、インシデント発生時の国外との情報連絡体制を整備する。	・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。 ・ASEAN 加盟国とリモートサイバー演習及び机上演習を実施し、、インシデント対応にかかる連携対処能力の向上を進めた。また欧米及び ASEAN 諸国と共に国際サイバーセキュリティワークショップ・演習を実施し、相互理解促進と信頼関係構築の一助とした。
（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・対策を強化するため、サイバーセキュリティに関する比較可能な指標の掲示(Mejiro プロジェクト)を通じて、効率的な対処のためのオペレーション連携を実現するための基盤構築に資する開発、運用協力体制の検討を進める。	・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提供を行うとともに、２回の解説を行い、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。	・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 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。
（エ）	経済産業省	経済産業省において、JPCERT/CC を通じ、以下の取組を行う。 ・アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担う CSIRT の構築及び運用、連携の継続的な支援。JPCERT/CC の経験の蓄積をもとに新規開発したサイバー攻撃に対処するためのツールの提供を行う。 ・アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内 CSIRT 構築セミナー等の普及・啓発、サイバー演習の引き続きの実施。 ・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。	・経済産業省において、JPCERT/CC を通じ、次のことを実施した。 ・アフリカ地域を対象とした FIRST のイベントにおいて、Covid-19 に関連するインシデントへの対応事例などについて講演を行った。

(3) 能力構築支援

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・様々な政策手段を活用した開発途上国における能力構築支援の実施			
項番	担当府省庁	2020 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	・内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、新型コロナウイルス感染症に係る状況を踏まえつつ、各国における効果的な能力構築支援に積極的に取り組む。特に、日 ASEAN サイバーセキュリティ政策会議等を通じた日本の取組の紹介、サイバーセキュリティ政策能力向上等の研修機会の提供等の JICA 事業を通じた支援、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」による ASEAN 加盟国向けの防御演習等を実施する。 ・外務省において、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、UNODC プロジェクトへの拠出、第 14 回国連犯罪防止刑事司法会議（京都コングレス）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いつつ、サイバー犯罪に関する条約の普遍化に取り組む。（再掲）	[NISC] ・「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（基本方針）」（2016 年 10 月）に基づいて、内閣官房を中心とした関係省庁の緊密な連携の下で、ASEAN 諸国向けサイバーワークショップを実施する等、政府全体で ASEAN を中心とした開発途上国向け支援の取組みを行った。 ・日・ASEAN サイバーセキュリティ政策会議の活動において、リモートサイバー演習と机上演習を開催したほか、重要インフラ防護に関して日・ASEAN の状況を共有し、各国の能力構築を進めた。 ・2020 年において、各国政府関係機関ウェブサイトの改ざん事案を検出して通知・対処を行うプログラムの実施を通じ、各国政府との情報連絡体制の強化及び対処能力の向上が図られた。 [警察庁] ・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 2020 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 15 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へいし、サイバー空間の脅威への対処に関する知識・技術を習得させるとともに、外国捜査機関等との協力関係を強化することを目的とした JICA 課題別研修（サイバー犯罪対処能力向上）をの実施したを目指したものの、新型コロナウイルス感染症の感染拡大の影響により 2020 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。 [総務省] ・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」において、ASEAN 加盟国の政府職員、重要インフラ事業者の職員等を対象とした実践的サイバー防護演習や若手エンジニア向けサイバーセキュリティ競技等をオンライン形式を中心に実施した。また、オンラインで学習可能なサイバーセキュリティ講座を ASEAN 各国に提供した ・APT 加盟国を対象とした研修（2021 年２月、オンライン）において、我が国のサイバーセキュリティ政策について情報共有を行った。 [外務省] ・新型コロナウィルス感染症の拡大に伴い、限定的な活動を余儀なくされたものの、2019 年度に開始したインドネシア「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、リモートで「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」元研修員向けのフォローアップセミナー（８か国 11 名）や「サイバー攻撃防御演習」の研修（14 か国 30 名）などの能力構築支援を展開した。 ・日 ASEAN 統合基金を活用し、ICPO が現在実施中の 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２年度通常予算及び令和元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。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遍化に取り組んだ。さらに、京都コングレスの政治宣言において各国の法執行機関等が技術の発展に応じた能力構築を促進することを確認した。 ・サイバー犯罪に関する新条約の議論においては、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。

（イ）	経済産業省	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）が日米の官民の専門家と協力し、ASEAN をはじめとしたインド太平洋地域の国・地域に対する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。	・経済産業省において、2021 年３月８～12 日、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）と連携し、インド太平洋地域向けに制御システムのサイバーセキュリティに関する演習をオンラインで実施。本演習の一部分として、日本、米国、EU は初めて、ポスト・コロナにおけるサイバーセキュリティに関する日米欧セミナーを開催。インド太平洋地域から招聘した研修生 40 名に加え、情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）の中核人材育成プログラムの研修生が参加。

4　横断的施策

4.1　人材育成・確保

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・人材の需要と供給を相応するための好循環を形成するため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化			
項番	担当府省庁	2020 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、経営層の意識改革や戦略マネジメント層、実務者層・技術者層、若年層の育成に関して、関係府省庁との連携の下、「サイバーセキュリティ人材育成取組方針」（2018 年６月）に基づき、産学官の連携を図りつつ、関係施策を推進していくとともに、DX 時代の新たな事業・サービスを提供する上で重要となる企業内における IT・サイバーセキュリティ関係の体制構築・人材育成等について議論を進める。（再掲）	・普及啓発・人材育成専門調査会において、経営層の意識改革や人材育成に関する産学官の多様な取組について、関係機関の間で情報共有を行った。また、DX with Cybersecurity の推進を目的として、政策議論のための補助フレームワークを作成し、今後 DX を実現するための人材の確保、育成、活躍の促進に係る政策課題について議論・検討を深めた。また、議論の成果の一部は、経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」にも反映を行った。
（イ）	内閣官房	内閣官房において、2019 年度に構築した普及啓発・人材育成施策に関するポータルサイトについて、関係機関とも連携しつつ、各施策がより活用されるよう、関係者の意見も踏まえて改善を図る。	・ポータルサイトを運用し、掲載施策の見やすさ向上やサイバーセキュリティ月間と連携して関連行事を掲載するなど実施した。
（ウ）	総務省	総務省において、2019 年度の取組結果を踏まえ、地域で自立したサイバーセキュリティ人材の育成が行われる仕組みとなるよう実証的調査を継続するとともに、調査成果を調査対象地域以外でも活用できるよう横展開を進める。	・総務省において、地域で自立したサイバーセキュリティ人材の育成が行われる人材のエコシステムが構築できるよう実証的調査を 2019 年度に引き続き沖縄で実施するとともに、その継続的展開のための検討を進めた。
（エ）	総務省	サイバーセキュリティ関連情報の大規模集約に基づく横断分析、国産セキュリティ技術の検証、実践的な高度セキュリティ人材育成に寄与するサイバーセキュリティ統合知的基盤構築のための検討を行う。	・総務省において、NICT を通じて、サイバーセキュリティ統合知的・人材育成基盤（通称：CYNEX）として、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ための基盤、及び民間・教育機関等における自立的な人材育成のための基盤の構築を開始した。

(1) 戦略マネジメント層の育成・定着

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・「戦略マネジメント層」に関する経営層の理解の促進と産業界と連携したその定着 **・戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進**			
項番	担当府省庁	2020 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、関係府省庁や各種団体等とも連携し、2018 年度に作成したモデルカリキュラムも活用しつつ、戦略マネジメント層の育成に取り組むとともに、その育成を促す。	・普及啓発・人材育成専門調査会等をはじめとして、戦略マネジメント層育成に関する取組状況を把握し、今後の取組の方向性について議論を行った。また、2018 年度に作成したモデルカリキュラムを活用したプログラムの実施を通じて課題を抽出した。
（イ）	経済産業省	経済産業省において、IPA の「産業サイバーセキュリティセンター」を通じ、 ・これまでの３年間の実施経験や受講生のアンケート結果を踏まえ、不断に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引き続き取り組む。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引き続き実施し、対策強化につなげる。 ・2019 年度に実施した「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。	・これまでの３年間の実施経験や受講生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、これまで２年間の経験、受講生のアンケート結果や新型コロナ感染症の状況等を踏まえ、2021 年２月にオンライン（オンデマンド形式）で実施した。
（ウ）	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、国立高専機構の教員向けに、IPA、JPCERT/CC 等により、FD（Faculty Development）等の研修機会の提供を実施。	・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、 IPA 等による国立高専機構への教材の提供や、IPA と教員間での議論等を実施した。
（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。	・「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、産学連携による実践的な教育ネットワークを構築し、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。2020 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。

(2) 実務者層・技術者層の育成

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・学び直しによるスキルの開発や実践的な演習			
項番	担当府省庁	2020 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情報セキュリティ人材育成プログラムに参加する高等専門学校を対象に、サイバーセキュリティ講義を実施した。
（イ）	警察庁	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。（再掲）	・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。

（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」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、2020 年度は全国 47 都道府県において計 2,648 人が受講した。
（エ）	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を進めてきた。併せて、これらの拠点について、ハード、ソフト両面について定期的なアップデートを進めるとともに、全国の高等専門学校生が共同で利用できる実践的な演習のための仮想空間（サイバーレンジ）の提供に向けた取組を進めている。教育プログラムの開発を進めるなど、引き続き、サイバーセキュリティ人材の育成を進める。	・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を進めてきた。2020 年度には、これらの拠点の環境整備、情報モラル教育に係る教材の改善、サイバーセキュリティ教育に係る教材の開発・全国展開を進めるとともに、すべての学生が受講するサイバーセキュリティを含む情報教育のカリキュラム案を策定した。また、学生のスキルアップ等を目的に、警察庁や民間企業と連携した出前授業やセキュリティコンテストなどを開催した。
（オ）	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とともに、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、サイバーセキュリティに関する内容を含む教育訓練を指定する。	・サイバーセキュリティに関する内容を含む公共職業訓練を実施した。（28 コース・受講者数 371 人） ・特定一般教育訓練として、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。（2021 年４月１日時点の情報関係の指定講座数４講座） ・専門実践教育訓練給付として、ITSS レベル３相当以上の資格取得を目指す「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。（2021 年４月１日時点の指定講座数 82 講座）
（カ）	経済産業省	経済産業省において、新たに導入する登録の更新制などを含め、情報処理安全確保支援士制度の着実な実施に向けて必要な措置を講じるとともに、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。	・情報処理安全確保支援士の登録者数は、2020 年 10 月時点で、19,752 名となった。また、登録セキスペの更なる活用のため、IPA の HP で登録状況を公表するとともに、支援士制度の普及のため、企業や団体への周知等を行った。 ・2020 年５月の改正法の施行に伴い 2020 年 10 月に初めての登録の更新が行われた。また、これまで義務講習の実施機関は独立行政法人情報処理推進機構のみであったが、改正法の施行により、一定の条件を満たした民間企業の行う講習（特定講習）も対象の追加となり、この特定講習の対象となる講習を定めた。
（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については、新型コロナウイルス感染症の拡大防止のため４月に予定していた試験は中止となった。また、10 月の試験についても実施に必要な会場が確保できなかったことから延期することとした。このため、実施方法をコンピュータを利用する方式に変更することで試験を可能とした。
（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、周知及び普及を図る。	・情報処理技術者試験については、新型コロナウイルス感染症の拡大防止のため４月に予定していた試験は中止となった。また、10 月の試験についても実施に必要な会場が確保できなかったことから一部試験区分を延期することとし、コンピュータを利用する方式に変更することで試験の実施を可能とした。

（ケ）	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。	・経済産業省において、IPA を通じて、 ・2019 年度に作成した講義要領及び教材を基に最新事例等を追加しながら、インターネット安全教室を開催し、教育関係者及び小中高校生からシニア層までを含むホームユーザにむけ、SNS の安全な利用方法を含む情報セキュリティに関する啓発を行った。 ・「教育関係者等向けインターネット安全教室」を、全国を経済産業局の存在する９ブロック（北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄）に分割し、ブロック毎に各ブロックの都道府県数分行うこととし、計 53 回開催し、4,151 名が参加した（2021 年３月末）。 ・「ホームユーザ向け安全教室」を全国 60 か所で開催し 8,321 名が参加、その他 IPA 講師によるインターネット安全教室を 11 回実施し 2,133 名が参加した（2021 年３月末）。 ・2020 年度は新型コロナウイルス対策のため、オンラインを通じての開催をするなどの工夫を行った。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（コ）	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、2020 年 10 月 18 日～12 月６日にかけて「セキュリティ・キャンプ全国大会」を実施し 84 名が修了するとともに、全国大会修了生の次のステップとして実施している「セキュリティ・ネクストキャンプ（25 歳以下）」では７名が修了した。さらに、2020 年９月から 2021 年３月にかけて、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・キャンプ地方大会」を全国７箇所で実施した。
（サ）	経済産業省	経済産業省において、IPA を通じ、IT を駆使してイノベーションを創出することのできる独創的なアイディア・技術を有する人材を発掘・育成する「未踏 IT 人材発掘・育成事業」を実施し、プロジェクトマネージャーに引き続きセキュリティを専門とした人材を採用する。	・「未踏 IT 人材発掘・育成事業」を実施し、2019 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、セキュリティをテーマとするプロジェクトの応募の促進を図った。
（シ）	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。	・NPO 日本ネットワークセキュリティ協会が主催する「SECCON2019」に対して、経済産業省として後援した。
（ス）	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。	・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。 ・防衛省サイバーコンテストを開催し、サイバー人材の発掘に係る取組を実施した。
（セ）	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。	・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、指揮システムを模擬した環境を構築して、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引き続き実施した。

（ソ）	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。

(3) 人材育成基盤の整備

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討 **・教育課程内での情報活用能力の育成、情報モラル教育** **・教員の研修の充実** **・自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備** **・大学・高等専門学校等の高等教育段階における情報技術人材の育成**			
項番	担当府省庁	2020 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、セキュリティ人材の役割・スキルを定めた ITSS+（セキュリティ領域）の改訂版の公表や、企業における当該改訂版の使い方のガイドをまとめる。また、情報処理安全確保支援士の活躍促進に向けて、義務講習と ITSS+（セキュリティ領域）を関連づけることで、キャリアアップの道筋を描く。	・企業におけるセキュリティ関連タスクのまとまりを整理した ITSS+（セキュリティ領域）について、2020 年９月に公表した「サイバーセキュリティ経営ガイドライン」の付録Ｆ「サイバーセキュリティ体制構築・人材確保の手引き」の中で改訂を行い、使い方のガイドをまとめた。 ・情報処理安全確保支援士制度の義務講習のうち、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）の分野から、選択できるように特定講習を定めた。
（イ）	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 等で公表するとともに、各種会議において周知した。
（ウ）	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、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 11 月～12 月にかけて 5 回実施し、865 名が受講した。
（エ）	文部科学省	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。	・教員等を対象とした情報モラル教育指導者セミナーを 12 月～２月にかけて４回実施し、各回 100 名の申込者があった。
（オ）	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、育成プログラムを３コースから６コースに細分化した上で、共通カリキュラム（倫理、習慣化、アイデア発想、セキュアバイデザイン、ビジネス等）を設定するなどの改善を行った上で実施し、2020 年度は 41 名（事業開始から計 171 名）が修了した。

（カ）	文部科学省	文部科学省においては産学連携による PBL（課題解決型学習）等の実践的なサイバーセキュリティ教育について、各大学の進捗状況を踏まえ、参加大学数、連携企業数を増加させる取組を推進することや、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、大学における情報技術人材の育成強化を目指す。	・「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、学部３～４年生の学生を対象とした質の高い情報技術人材を育成する取組を推進するとともに、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。2020 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。
（キ）	文部科学省 経済産業省	文部科学省及び経済産業省において、高度な IT の知識と経営などその他の領域における専門知識を併せもつハイブリッド型人材の育成を進める。文部科学省においては産学連携による PBL（課題解決型学習）等の実践的なサイバーセキュリティ教育について、各大学の進捗状況を踏まえ、参加大学数、連携企業数を増加させる取組を推進することや、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、大学における情報技術人材の育成強化を目指す。	・「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、学部３～４年生の学生を対象とした質の高い情報技術人材を育成する取組を推進するとともに、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。2020 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) 各府省庁におけるセキュリティ人材の確保・育成の強化

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・各府省庁におけるセキュリティ人材の着実な確保・育成を継続 **・毎年度、計画の見直しを行い、一層の取組の強化**			
項番	担当府省庁	2020 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取りまとめ等、当該方針の見直し等に向けて取り組む。	・内閣官房の主導により、各府省庁が「サイバーセキュリティ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、諸施策を推進することにより、政府部内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「サイバーセキュリティ人材育成総合強化方針」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。
（イ）	内閣官房	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。	・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。
（ウ）	内閣官房 総務省	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」の見直し等に向けた議論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、内閣官房及び総務省において、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。	・内閣官房及び総務省において、橋渡し人材の育成に向けた研修内容等を見直した 2020 年度情報システム統一研修を実施（集合研修については、8 コース 29 回実施し、延べ 1,069 名が修了、e ラーニングについては、11 コース 44 回実施し、延べ 16,868 名が修了）したほか、橋渡し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。

（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。	・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５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し、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。

(5) 国際連携の推進

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・国際的な基準を踏まえた人材育成プログラムの認定など海外組織との間での連携を促すための仕組み作り **・海外におけるサイバーセキュリティ人材の能力構築への貢献**			
項番	担当府省庁	2020 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、関係府省と連携しつつ、「サイバーセキュリティ研究・技術開発取組方針」に基づく施策を推進する。また、国内外における人材育成施策の質の確保方策等について調査を実施する。	・人材育成施策の質の確保方策等に関する調査を通じ、海外関連施策の調査を実施した。

4.2　研究開発の推進

(1) 実戦的な研究開発の推進

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・不正なプログラムや回路が仕込まれていないことの検証を行うための体制の整備とそのための研究開発 **・サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発** **・機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発**			
項番	担当府省庁	2020 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の整備に向けて、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に関する技術検証体制の整備を進める。（再掲）	・技術検証体制の整備に向けた事業として、実際の製品に不正機能や当該機能につながりうる未知の脆弱性等が存在しないかどうかの技術的検証の試行を実施した。また、不正機能及び未知の脆弱性に関して技術的な調査を実施した。
（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製造・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）	・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」において、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進すべく、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、研究開発を行うとともに、実証実験を通じて要素技術を確立した。

（ウ）	総務省	総務省において、Society5.0 における重要な者会基盤となる第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仮想化通信プラットフォーム、MEC（モバイルエッジコンピューティング）仮想化基盤まで拡充し、それによる脆弱性評価・検証を行うとともに、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等の開発を実施した。
（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基礎的な検証を実施する。	・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基礎的な検証を実施した。
（オ）	経済産業省	経済産業省において、日本発のサイバーセキュリティ製品・サービスの創出・活用を推進するため、セキュリティ製品・サービスの有効性を検証する基盤を構築する。また、2019 年度にトライアル検証を実施したセキュリティ製品・サービスのビジネスマッチングを実施する。（再掲）	・2019 年度にトライアル検証を実施した２製品について、コラボレーション・プラットフォームでビジネスマッチングを実施。また、2019 年度に得られた製品評価のノウハウ等知見を活かし、2020 年度も有効性検証基盤の構築に関する議論と運用を実施。２製品を選定、検証を行った。
（カ）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化）にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、更なる検討を行う。（再掲）	・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、フレームワークの周知・普及、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とともに、2019 年に設置した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、引き続き検討を行った。
（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。	・経済産業省「IoT 推進のための横断的な技術開発事業」において、2016 年度及び 2017 年度より、データの収集、蓄積、解析、セキュリティの４つの領域における技術開発を実施。また、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、2018 年度より、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を開始するとともに、2019 年度には、オープンアーキテクチャ「RISC-V」を用いてセキュリティ基盤技術を開発する技術研究組合が設置された。2020 年度には、RISC-V プロセッサをベースとしたセキュア MCU、セキュア OS の FPGA 実装を完了した。
（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、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、先端的技術の基礎研究に引き続き取り組む。	・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の研究を進め、世界で初めて理論限界を達成する放送暗号を提案する等の成果を挙げた。AI が搭載されたシステムの安全性や信頼性を保証するための「機械学習に関する品質マネジメントガイドライン」を日本語及び英語でまとめて公開した。ハードウェアセキュリティに関して、これまで発表されてきた攻撃を分類、整理したデータベースを公開した。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバーセキュリティの研究開発の成果の普及や社会実装の推進			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ケ）	経済産業省	経済産業省において、日本発のサイバーセキュリティ製品・サービスの創出・活用を推進するため、セキュリティ製品・サービスの有効性を検証する基盤を構築する。また、2019 年度にトライアル検証を実施したセキュリティ製品・サービスのビジネスマッチングを実施する。（再掲）	・2019 年度にトライアル検証を実施した２製品について、コラボレーション・プラットフォームでビジネスマッチングを実施。2019 年度に得られた製品評価のノウハウ等知見を活かし、2020 年度も有効性検証基盤の構築に関する議論と運用を実施。２製品を選定、検証を行った。
（コ）	経済産業省	経済産業省において、情報セキュリティサービス審査登録制度の普及促進を図るとともに、サービスの拡張も含め、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、2020 年度は、登録サービス件数を約 170 件から約 240 件まで増加させた。また、制度の更なる改善を図るため、ユーザ・ベンダー双方への本制度の活用状況・ニーズ調査を実施した。制度利用者からの要望を踏まえ、利用者にとってより分かりやすいものにすべく、基準適合サービスリストを改善した。
（サ）	経済産業省	経済産業省において、2019 年度事業で明らかになった中小企業の実態・ニーズを踏まえ、地域特性・産業特性等を考慮したマーケティング、機器ソフトウェアサービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、損害保険会社、IT ベンダー、地元の団体等の連携による地域実証を 2020 年度に実施する。この実証を通して中小企業のサイバーセキュリティへの意識向上を図るとともに、中小企業の実態やニーズをよりきめ細かく把握し、2021 年度以降に民間による中小企業が活用しやすいサイバーセキュリティ簡易保険含めた対策支援サービスの創出を目指す。（再掲）	・経済産業省において、損害保険会社、ＩＴベンダー、地元の団体等がコンソーシアムを組む、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を全国で 15 件実施し、約 1,100 社の中小企業が実証に参加した。実証により、中小企業におけるセキュリティ対策の課題や、産業別でのセキュリティ対策の実態等が明らかになった。
（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、以下の取組を実施する。 ・経済産業省において、セキュリティにも配慮した安心安全なクラウドサービス利用の促進等のために、認定された IT ベンダーのセキュリティ関連の取組状況等を開示し、その制度の普及促進を図る。 ・経済産業省において、セキュリティ対策の普及啓発を行うとともに、専門家等を派遣して、セキュリティマネジメント指導を実施する。 （再掲）	・経済産業省において、セキュリティ対策の普及啓発を行うとともに、専門家等を派遣して、セキュリティマネジメント指導を 395 社の中小企業に対して実施した。 ・また、スマート SME サポーター（中小企業の IT 活用を支援する IT ベンダー等）として認定した事業者について、特設サイトにて「クラウドサービスの安全・信頼性に関する情報」、「セキュリティ対策状況」、「利用終了時のデータの取扱い」等を開示し、中小企業に情報提供を行った。
（ス）	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、地方版コラボレーション・プラットフォームを各地域の経済産業局等と連携し開催する。（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 2020 年度は計４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 SECUNITY）の形成を促進するため、全国各地で経済産業局等によるセキュリティに関する取組等を実施。2021 年２月には「地域 SECUNITY 形成・運営のためのプラクティス集」（第１版）を取りまとめ、公開した。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・政府機関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、攻撃活動を把握、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（セ）	総務省	総務省において、ダークネット、ハニーポット等の多くの手段により収集したデータを用い、AI 技術も駆使した IoT マルウェアの挙動検知技術の改良及び IoT マルウェアの駆除技術の基本方式の設計を行うとともに、両技術のプロトタイプ開発を実施する。 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、基本方式の設計及びプロトタイプ開発を実施する。	・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の改良及び IoT マルウェアの駆除技術の基本方式の設計を行うとともに、両技術のプロトタイプを開発した。 ・また、感染した IoT 機器を安全に無害化・無機能化する技術に関して、基本方式の設計及びプロトタイプ開発を実施した。
（ソ）	総務省	総務省において、NICT を通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の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、サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）について、各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等の集約を更に進めるとともに、異種情報間の横断分析等の更なる高度化を図り定常運用を開始する。	・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、サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）について、各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等の集約を更に進めるとともに、異種情報間の横断分析等の更なる高度化を図り定常運用を開始した。
（タ）	総務省	総務省において、脆弱な IoT 機器のセキュリティ対策のための、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、改良及び総合的な実証評価を行い、技術を確立する。	・総務省において、脆弱な IoT 機器のセキュリティ対策のための、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、改良及び総合的な実証評価を行った。
（チ）	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。
（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）	・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。2020 年度においては、ソフトウェア製品の届出 255 件、ウェブアプリケーションの届出 734 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、149 件を公表した。また、「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、2020 年度においては、脆弱性対策情報を約 10,000 件（累計：約 127,000 件）公開した。
（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）	・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 24 の経済地域の 28 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(2021 年 3 月末時点) ・FIRST、APCERT 等の CSIRT コミュニティイベント積極的に参加し、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。

（ト）	総務省	サイバーセキュリティ関連情報の大規模集約に基づく横断分析、国産セキュリティ技術の検証、実践的な高度セキュリティ人材育成に寄与するサイバーセキュリティ統合知的基盤構築のための検討を行う。（再掲）	・総務省において、NICT を通じて、サイバーセキュリティ統合知的・人材育成基盤（通称：CYNEX）として、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ための基盤、及び民間・教育機関等における自立的な人材育成のための基盤の構築を開始した。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より
・先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発 **・計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術の研究開発**

項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ナ）	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 プロジェクトを立ち上げ、研究開発を推進する。	・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「超電導量子コンピュータの研究開発」のもとでは、①16 量子ビットチップの作製および超伝導回路・パッケージ開発に成功し、コヒーレンス、量子エラーなどの基本特性評価の実施、②量子ビットチップの大型化を推進し、64 量子ビットチップ回路を設計・作製について、技術開発を実施した。
（ニ）	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、既存の戦略目標に加え、IoT に関する戦略目標を 2020 年度に新たに設定し、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。	・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、戦略目標「Society 5.0 時代の安心・安全・信頼を支える基盤ソフトウェア技術」を新たに設定し、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実施した。
（ヌ）	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、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、先端的技術の基礎研究に引き続き取り組む。（再掲）	・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の研究を進め、世界で初めて理論限界を達成する放送暗号を提案する等の成果を挙げた。AI が搭載されたシステムの安全性や信頼性を保証するための「機械学習に関する品質マネジメントガイドライン」を日本語および英語でまとめて公開した。ハードウェアセキュリティに関して、これまで発表されてきた攻撃を分類、整理したデータベースを公開した。

（ネ）	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。 加えて、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進めるため、タスクフォースを開催する。（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。加えて、量子コンピュータ時代に向けた暗号の在り方検討タスクフォースを設置し、量子コンピュータや新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進めた。
（ノ）	総務省	総務省において、NICT 等を通じて、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の、距離に依らない堅牢な量子暗号通信網の実現に向けた技術を確立する。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行う。	・総務省において、地上系の量子暗号通信のさらなる長距離化技術（長距離リンク技術及び中継技術）の研究開発「グローバル量子暗号通信網構築のための研究開発」を開始した。 ・情報通信研究機構において、量子セキュリティ拠点の形成に向け、情報通信研究機構の小金井本部内において、2020 年度より当該拠点の整備を開始した。
（ハ）	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推進する。	・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を実施（研究開発期間は 2018 年度～2022 年度）。
（ヒ）	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 PUF セキュリティの ISO 採録に向けた支援、及び日本提案の秘密計算や量子鍵配送の標準化検討作業での支援を引き続き実施する。	・経済産業省において、IPA を通じ、 ・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の国際標準化について中心的役割を担うとともに、日本の意見を反映させた。 ・WG3 では、ISO/IEC15408 ベースの車載機器のセキュリティ評価基準に関する議論が開始され、エディタとして参加している。また、ハードウェアトロイを検知するハードウェアモニタリング回路の評価手法、多数の開発者が関わる脆弱性の取り扱いに際しての指針、量子鍵配信のセキュリティ要件及びそのテスト手法に関する標準化についての議論が開始されており、日本からの意見が反映されるよう、国内関係者との情報共有や支援を行っている。 ・エディタとして多大な貢献をした生体認証のセキュリティ要件及びそのテスト手法が産業界にインパクトがある標準として ISO から公表された。 ・NEDO による委託事業の成果として取り組んでいる PUF の国際標準化を支援しており、Part1 の国際標準化が完了した。

（フ）	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を目指した開発を進める。	・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を目指した開発を進めており、その実用化と実証実験として、量子セキュアクラウドを医療分野に世界で初めて適用し、高知と東京を含む 800km 圏内に１万人分の電子カルテデータを分散保管した状態から、衛星経由で患者の電子カルテを探索したところ、９秒以内に見つけ出して（高速計算）、安全に取り寄せること（暗号通信）に成功した。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より

・海外のイベント等への積極的な参加等を通じた、国際的な情報発信、共同研究の実施や研究成果の国際標準化等の研究開発に係る官民の国際連携の強化

・サイバーセキュリティ対策における制度上の課題に関する調査・研究

項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ヘ）	内閣官房	内閣官房において、関係府省と連携しつつ、「サイバーセキュリティ研究・技術開発取組方針」に基づく技術検証体制の整備や国内産業の育成・発展に向けた支援等の施策の推進を図る。また、産学官連携の研究・技術開発のコミュニティ形成に向け、研究コミュニティとの議論を行うとともに、研究振興策について議論を進める。	・「サイバーセキュリティ研究・技術開発取組方針」において示された方向性の１つである「産学官連携の研究・技術開発のコミュニティ形成」に関し、研究開発戦略専門調査会及びそのワーキンググループ（研究・産学官連携戦略ワーキンググループ）において具体化検討を行い、その考え方や推進方策を整理した。
（ホ）	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、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。	・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した。
（マ）	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）	・新型コロナウイルスの影響で、米国サンフランシスコで開催される予定だった RSA カンファレンスが延期されたため施策は未実施。※RSA カンファレンスは参加者約 42,500 人、出展企業約 700 社の世界最大希望のセキュリティ産業に関するカンファレンス。

（ミ）	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 PUF セキュリティの ISO 採録に向けた支援、及び日本提案の秘密計算や量子鍵配送の標準化検討作業での支援を引き続き実施する。（再掲）	・経済産業省において、IPA を通じ、 ・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の国際標準化について中心的役割を担うとともに、日本の意見を反映させた。 ・WG3 では、ISO/IEC15408 ベースの車載機器のセキュリティ評価基準に関する議論が開始され、エディタとして参加している。また、ハードウェアトロイを検知するハードウェアモニタリング回路の評価手法、多数の開発者が関わる脆弱性の取り扱いに際しての指針、量子鍵配信のセキュリティ要件及びそのテスト手法に関する標準化についての議論が開始されており、日本からの意見が反映されるよう、国内関係者との情報共有や支援を行っている。 ・エディタとして多大な貢献をした生体認証のセキュリティ要件及びそのテスト手法が産業界にインパクトがある標準として ISO から公表された。 ・NEDO による委託事業の成果として取り組んでいる PUF の国際標準化を支援しており、Part1 の国際標準化が完了した。

(2) 中長期的な技術・社会の進化を視野に入れた対応

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・人文社会学的視点も含めた様々な領域の研究との連携、融合領域の研究を促進			
項番	担当府省庁	2020 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、各府省庁とも連携し、様々な領域の研究の観点も念頭に置き、サイバーセキュリティの研究開発に関する課題について議論を進める。	・研究開発戦略専門調査会において、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、議論を行った。

4.3　全員参加による協働

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・サイバーセキュリティの普及啓発に向けた総合的な戦略及び具体的なアクションプランの策定			
項番	担当府省庁	2020 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。	・普及啓発・人材育成専門調査会において、サイバーセキュリティの普及啓発に係る状況を特徴づける事項について、継続的に収集しうる代表的な客観的なデータを前広に収集・整理した。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・必要な情報発信や国民からの相談対応 **・産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、関係者による実践を推進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（イ）	内閣官房	内閣官房において、2019 年度に構築した普及啓発・人材育成施策に関するポータルサイトについて、関係機関とも連携しつつ、各施策がより活用されるよう、関係者の意見も踏まえて改善を図る。（再掲）	・ポータルサイトを運用し、掲載施策の見やすさ向上やサイバーセキュリティ月間と連携して関連行事を掲載するなど実施した。
（ウ）	内閣官房	内閣官房において、個人や組織のセキュリティ意識向上のため、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。	・主に一般国民向けに、緊急時における注意・警戒情報やサイバーセキュリティに関する普及啓発情報等について、媒体の特徴に合わせた情報発信を行った。
（エ）	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。	・情報セキュリティ安心相談窓口にて、電話、メール、FAX 等で 9,355 の相談に対応した（電話 6,582 件、メール 2,695 件、FAX その他 78 件）。 ・経済産業省において、IPA を通じ、高度なサイバー攻撃を受けた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に対して「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 406 件実施した。
（オ）	総務省 法務省 経済産業省	総務省、法務省及び経済産業省において、電子署名などのトラストサービスの利活用等に関するセミナーの開催及びホームページを活用した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、認定認証事業者に対する説明会の開催、民間事業者等からの電子署名に関する相談対応等を行うことで、企業における電子署名の利活用の普及促進策を検討・実施する。また、総務省において、トラストサービスの認定の仕組みを検討する。	・トラストサービスに関するワークショップの開催等を通じて、電子署名をはじめとするトラストサービスの普及促進を図った。また、電子署名法上の電子署名の使い勝手の改善に関する要望を踏まえ、リモート署名についての回答書の作成や、サービス提供事業者自身の署名鍵により暗号化等を行うサービスについての Q&A の公表を通じて、より一層電子署名の普及促進を図った。また、総務省においては、タイムスタンプについて、2020 年３月より「タイムスタンプ認定制度に関する検討会」を計 11 回開催、2021 年３月に取りまとめを行い、国による認定制度を創設、e シールについては、2020 年４月より「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」を計 11 回開催し、ユースケースの検討を実施するとともに、信頼のおけるサービス・事業者に求められる技術的要件等について整理を行った。
（カ）	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。	・経済産業省において、IPA を通じ、「安心相談窓口だより」を 12 件（内８件は更新）公表した。 ・経済産業省において、IPA を通じ、「安心相談窓口公式 Twitter」にて 126 件の情報を発信した。 ・経済産業省において、IPA を通じ、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、統計情報レポートを１件、事例紹介レポートを２件公表した。

（キ）	経済産業省	経済産業省において、IPA を通じ、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により情報の周知を行う。特に中小企業に対しては、セキュリティに関する身近な専門家を自らで検索することができる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。なお、セキュリティプレゼンター制度については、中小企業のみならず普及に取り組む専門家を支援する制度でもあることから、地域の専門家の自発的な普及活動を促すため、シンプルで活用しやすい制度へと見直しを図る。	・「講習能力養成セミナー」を全国 12 箇所において開催するとともに、同講演を録画配信（オンデマンド形式）し、中小企業の経営者、社内教育担当者等合計約 400 名が参加、オンデマンド形式による録画配信についても約 550 名が視聴した。 ・商工団体・税理士会・社会保険労務士会等の指導員等を対象とする研修会、警察・自治体・中小企業団体等が主催する中小企業向けセミナー等 30 箇所以上に講師を派遣した。 ・上記活動等を通じて IPA が作成する情報セキュリティ啓発資料や情報セキュリティ対策支援サイトのツール等の周知を行うとともに、サイト内のサービスを一つの利用者番号で活用できるようにするなどユーザの利便性を高める見直しを通じて利用促進を図り、情報セキュリティ対策支援サイトへの登録ユーザ数が累計で 147,000 名を超えた。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・「サイバーセキュリティ月間」のさらなる充実			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ク）	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。	・「サイバーセキュリティ月間」では各種啓発主体と連携して、「サイバーセキュリティ意識・行動強化プログラム」を踏まえ、若年層に重点を置いたキャンペーンや普及啓発イベント動画のオンライン配信を行い、普及啓発活動に取り組んだ。また、全国の公立図書館に普及啓発冊子を送付し、インターネット上でも公開するなど、地域に偏らない普及啓発活動を推進した。

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・国民向けのわかりやすい解説書の作成・普及 **・学校教育を通じた、情報モラル教育の一部としてのサイバーセキュリティ教育の推進**			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ケ）	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。	・「インターネットの安全・安心ハンドブック」における内容のうち、サイバーセキュリティ月間にあわせて若年層が親しみやすい構成として基本的な知識を紹介したパンフレットの作成を行った。
（コ）	内閣官房	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児童生徒一人一台端末整備施策と連携した、サイバーセキュリティに関する普及啓発コンテンツを作成・普及する。	・GIGA スクール構想の実現に向けた取組を踏まえ、内閣官房と文部科学省で連携し、小中学生を対象として、サイバーセキュリティ上注意すべきポイントを効果的に理解できるよう、普及啓発リーフレットを作成した。また、内閣官房と文部科学省において、当該リーフレットについて、ホームページ等を用いて普及啓発を図ったほか、文部科学省において、全国の都道府県教育委員会に周知も行った。
（サ）	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。	・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、6,556 件ダウンロードされた。

（シ）	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、多くの青少年が初めてスマートフォン等を手にする春の卒業・進学・新入学の時期に特に重点を置き、関係府省庁と協力して啓発活動を集中的に展開する「春のあんしんネット・新学期一斉行動」の取組や「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を行う。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。	・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。2020 年度は、1,208 件の出前講座を実施した。また、2021 年３月に、「インターネットトラブル事例集（2021 年版）」を公表した。
（ス）	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。	・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か所で開催することにより普及啓発を実施した。 （実績）栃木県（オンライン開催：視聴回数 2,584 回）、岡山県（75 名）及び神奈川県（オンライン開催：視聴回数 887 回） ※2020 年度は３か所で実施
（セ）	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。（再掲）	・独立行政法人教職員支援機構と連携し、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 11 月～12 月にかけて５回実施し、865 名が受講した。
（ソ）	文部科学省	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。（再掲）	・教員等を対象とした情報モラル教育指導者セミナーを 12 月～２月にかけて４回実施し、各回 100 名の申込者があった。
（タ）	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。	・経済産業省において、IPA を通じて、第 16 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 45,244 点、ポスター作品 5,383 点、４コマ漫画作品 6,672 点、書写（硬筆）2,570 点、活動事例 12 点、合計 59,881 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 12 校の応募の中から「優秀活動事例賞」に７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。
（チ）	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。（再掲）	・経済産業省において、IPA を通じて、 ・2019 年度に作成した講義要領及び教材を基に最新事例等を追加しながら、インターネット安全教室を開催し、教育関係者及び小中高校生からシニア層までを含むホームユーザにむけ、SNS の安全な利用方法を含む情報セキュリティに関する啓発を行った。 ・「教育関係者等向けインターネット安全教室」を、全国を経済産業局の存在する９ブロック（北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄）に分割し、ブロック毎に各ブロックの都道府県数分行うこととし、計 53 回開催し、4,151 名が参加した（2021 年３月末）。 ・「ホームユーザ向け安全教室」を全国 60 か所で開催し 8,321 名が参加、その他 IPA 講師によるインターネット安全教室を 11 回実施し 2,133 名が参加した（2021 年３月末）。 ・2020 年度は新型コロナウイルス対策のため、オンラインを通じての開催をするなどの工夫を行った。

戦略（2018 年７月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より			
・利用者がサイバーセキュリティの取組を適切に実施できるよう事業者や関係団体等の取組が促進される環境の整備、サイバーセキュリティの確保に資するガイドラインの整備とその着実な実施を推進			
項番	担当府省庁	2020 年度　年次計画	取組の成果、進捗状況
（ツ）	総務省	総務省において、必要なセキュリティ対策のポイントをまとめた「Wi-Fi 利用者向け 簡易マニュアル」及び「Wi-Fi 提供者向け セキュリティ対策の手引き」について 2020 年度の早期に改訂を行うとともに、観光関係機関や病院、学校等を含めて周知を実施していくなど、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。	・経済産業省において、IPA を通じて、 ・2019 年度に作成した講義要領及び教材を基に最新事例等を追加しながら、インターネット安全教室を開催し、教育関係者及び小中高校生からシニア層までを含むホームユーザにむけ、SNS の安全な利用方法を含む情報セキュリティに関する啓発を行った。 ・「教育関係者等向けインターネット安全教室」を、全国を経済産業局の存在する９ブロック（北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄）に分割し、ブロック毎に各ブロックの都道府県数分行うこととし、計 53 回開催し、4,151 名が参加した（2021 年３月末）。 ・「ホームユーザ向け安全教室」を全国 60 か所で開催し 8,321 名が参加、その他 IPA 講師によるインターネット安全教室を 11 回実施し 2,133 名が参加した（2021 年３月末）。 ・2020 年度は新型コロナウイルス対策のため、オンラインを通じての開催をするなどの工夫を行った。
（テ）	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・リスク管理や秘密情報管理等のサイバーセキュリティ対策の実施時に参考となるガイドや最新の動向を収集・分析した報告書の公表等を行うことで、サイバー空間利用者への啓発を推進する。	・「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」」を実施し、ICT 環境の急速な変化によりセキュリティの対策状況や業務委託における取り決めに対する影響、あらたな脅威や脆弱性について実態を把握し、結果を公表(個人編 12 月、組織編１月）した。 ・営業秘密保護に関する指針策定に向けた情報収集のため、「企業における営業秘密管理の実態調査 2020」を実施。2016 年に実施した企業の営業秘密の管理状況調査を踏まえ、企業が営業秘密の管理や漏えい対策を強化するための施策に資すための調査を実施した。
（ト）	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に向けた検討を進めるとともに、新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、より具体的で分かりやすく、実践的な内容のガイドラインの策定を実施する。また、セキュリティ対策に関する専門的な相談に対応できる窓口を設置する。	・総務省において、テレワークセキュリティガイドラインの改定に向けた検討を進めるとともに、新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、より具体的で分かりやすく、実践的な内容のガイドラインの策定を実施する。また、セキュリティ対策に関する専門的な相談に対応できる窓口を設置した。

5　推進体制

戦略（2018 年 7 月 27 日閣議決定。2018 年～2021 年の諸施策の目標と実施方針）より
・関係機関の一層の能力強化 **・内閣サイバーセキュリティセンターにおいて、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実施** **・危機管理対応の一層の強化** **・東京 2020 大会に向けた産学官民の参加・連携・協働の枠組み構築及びサイバーセキュリティの確保に向けた取組の着実な履行**

項番	担当府省庁	2020 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。	・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、2020 年度は、約 900 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 23 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、2020 年度は研究開発戦略専門調査会に計 3 回、また研究・産学官連携戦略 WG に計 7 回出席をいただき、「サイバーセキュリティ研究開発戦略」の改訂や「次期サイバーセキュリティ戦略」の検討に向けて、研究・産学官連携の推進方策等に関する意見交換を行った。さらに、2018 年戦略及びこれに基づくサイバーセキュリティ 2020 の冊子の制作・各種セミナーを通じた国内外の関係者への発信などにより、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	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、引き続き、国内外の関係者へ 2018 年戦略及びこれに基づく年次計画等の発信を行う。また、関係者との意見交換を行って、サイバー攻撃による被害の実態を含むサイバー空間に係る動向の把握に努め、東京 2020 大会後を見据えた検討を進める。	・内閣官房において、2018 年戦略及びこれに基づくサイバーセキュリティ 2020 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 2020 の全体版及び概要をまとめた簡略版の冊子を制作した。一方、新型コロナウイルス感染拡大に伴うイベントの中止やオンライン開催により、発信の機会が減少。今後オンライン開催の場合は、メールで電子版を別途発信する等、環境に対応した周知広報活動を実施。
（ウ）	内閣官房	内閣官房において、東京 2020 大会を見据え、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、新型コロナウイルス感染症に係る状況を踏まえつつ、2020 年度上半期に大規模サイバー攻撃事態等への対処能力維持のための訓練を行う。（再掲）	・2020 年度上半期に大規模サイバー攻撃事態等対処訓練を関係省庁とともに実施し、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。一方、2020 年度下半期に東京 2020 大会を見据え、大規模サイバー攻撃事態等対処訓練を計画していたところ、新型コロナウイルス感染症に係る状況に鑑み、年度中の実施を見送った。なお、当該訓練は、2021 年度上半期（東京 2020 大会前）に延期して実施することを予定している。

（エ）	内閣官房	内閣官房において、引き続き、リスクマネジメントの促進と対処態勢の整備・運用を推進する。 ・「リスクマネジメントの促進」については、NISC が作成した手順に基づくリスクアセスメントの取組及び横断的リスク評価の取組を繰り返し実施する。情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、残存リスクが顕在化した場合の対応体制の強化を促進させる。 ・「対処態勢の整備・運用」については、大会まで重要サービス事業者、大会組織委員会、東京都等が参加する情報共有及びインシデント発生時の対処支援調整等の訓練・演習を実施し、大会関係組織間で緊密に連絡調整を図るための態勢を整備する。 （再掲）	・東京大会に向けた取組に関しては、引き続き、サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、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。 ・重要サービス事業者等を対象に、第６回のリスクアセスメントの取組として大会延期や新型コロナウイルスの感染拡大に伴う環境変化を踏まえたリスクの見直し、残留リスクが顕在化した場合の対処体制の強化を推進した。 ・各事業者等から提出されたリスクアセスメント結果を分析し、個別にフィードバックを実施するとともに、必要に応じ助言を実施した。 ・2019 年度の横断的リスク評価で対象とした重要サービス事業者等（会場（レガシー部分）を含む。）における改善状況についてフォローアップを実施した。 ・横断的リスク評価において、重要サービス事業者等（会場（レガシー部分）を含む。）に対して引き続き検証を実施した。 ・サイバーセキュリティ対処調整センターで構築した情報共有システムにより脅威情報等を提供するとともに、同システムを活用して重要サービス事業者等が参加する演習を２回実施した。
（オ）	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する。（※セキュリティ調整センターについては 2020 年３月に設置。大会の延期の決定に伴い一旦廃止。） （再掲）	・2021 年３月に設置した「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、本番を見据えた実践的な訓練を実施し、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＞

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（CISO）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 2020 年度当初までに定めた「対策推進計画」を基として、2020 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 2021 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

2020 年度の総合評価・2021 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

令和２年度は、従来の標的型攻撃メールに加え、クラウドサービスを狙った攻撃、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、新型コロナウィルス感染症に便乗する脅威もあることからも、政府機関に対するサイバー攻撃の脅威が大きい状況が続いているものと考えられる。

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

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

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

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

このような状況を踏まえ、内閣官房では令和３（2021）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、平成 29（2017）年度に導入した e ラーニングを改善した上で引き続き実施するほか、従来の資料配布や、NISC 等が主催する研修会への参加を一層促進する。

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

内閣法制局

2020 年度の総合評価・2021 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。

令和２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。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した。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」（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。

令和３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、統一基準群の改定等に伴う内閣法制局情報セキュリティポリシー関連規程の整備、NISC が実施するマネジメント監査、ペネトレーションテスト、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

2020 年度の総合評価・2021 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　柴﨑　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（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る。

2020 年度においては、コロナ禍におけるテレワークの急増を踏まえ、テレワーク実施者を対象とした e-ラーニングや Web 会議システム上の参加も認めた集合研修による情報セキュリティ教育を実施するとともに、「人事院におけるセキュリティ・ＩＴ 人材確保・育成計画」で定めた職員を対象として、NISC 等が実施する研修への参加を一層促進した。

また、Emotet（エモテット）と呼ばれるウイルスの感染を狙う標的型攻撃メール等最新の標的型攻撃メールの見分け方や報告手順を繰り返し周知し、不審なメールを受信した際のルールの遵守・徹底を図った。

職員の情報セキュリティ対策の実施状況について、全職員に情報セキュリティ対策を実施する上でのそれぞれの役割に応じて自己点検を行わせるとともに、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するなどにより自己点検としての PDCA を実施した。また、監査については、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実施するとともに、前年実施した監査のフォローアップを行い、情報セキュリティ対策の改善策の実施を確認した。

2021 年度においては、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等外部サービスの利用が増加するところ、外部サービスの利用によるリスクが生じないよう、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とともに、万が一情報セキュリティインシデントが発生した場合に組織として適切に対処するため情報セキュリティ責任者等と人事院 CSIRT の間の連携の強化に一層取り組むこととする。

また、2022 年 10 月に予定されている基幹 LAN システムの更改に向けて、新たに適用されるべき情報セキュリティ対策の検討を進めることとする。

内閣府

2020 年度の総合評価・2021 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 大塚 幸寛

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。標的型攻撃メール等、人間の心理的な隙や行動のミスにつけ込むソーシャルエンジニアリングの手法は年々巧妙化しており、外部からの不正アクセスによる情報漏えいとともに、データの改ざん、システムの乗っ取り等の脅威が増大している。

ところで、新型コロナウイルスの感染リスクが高まった昨年以来、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、一般行政端末の持ち運びを容易とするためシンクライアント端末を導入し、紛失等による情報漏えいのリスクを軽減する対策を講じているが、庁舎外で端末を操作する場合、ショルダーハッキングや公衆無線 LAN の利用等による情報の窃取など、ユーザに起因するリスクの増加に留意する必要がある。また、外部とデジタルデータのやり取りを行うニーズが一層増加する中、特にインターネットに露出した機器の脆弱性を突くサイバー攻撃にも備えておく必要がある。その他、パブリッククラウドを使用する情報システムにおいては認証情報やアクセス権限の設定管理を、また私物パソコンを利用する際には機密性に応じた運用ルール等を、各々徹底すべきである。

以上の状況を踏まえ、令和３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

2020 年度の総合評価・2021 年度の全体方針

最高情報セキュリティ責任者
長官官房審議官　小山永樹

近年，政府機関等を対象としたサイバー攻撃が頻発し，攻撃の手法も巧妙化・複雑化している状況にあり，宮内庁としても，情報セキュリティ対策の強化は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いることから，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，令和２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 会議やテレワーク環境を整備するなど，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対応を実施
○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 ラーニング等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における情報セキュリティ対策の推進

令和３年度においては，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，職員へ教育の充実を図る。具体的には，研修等の機会を通じて，改定した宮内庁情報セキュリティポリシー及び各種実施手順等の内容を周知するほか， 令和３年度中には，テレワーク環境が更に拡充されることから，テレワーク実施中の実施手順等の内容を周知し，改めて全職員の情報セキュリティに対する意識の向上を図る。さらに，マルウェアに感染した場合にも被害を最小化できるよう，情報セキュリティインシデント発生時の初動対応の在り方，日常的な情報の保存管理について，重点的な教育を行う。

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

2020 年度の総合評価・2021 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。

令和２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、コロナ禍でのテレワーク及びWeb 会議の利用の増加等を踏まえ、公正取引委員会の情報セキュリティ関係規程の見直しを行い、テレワーク及びWeb 会議に関連したセキュリティ対策を研修内容に盛り込んだほか、新たな脅威に対するリスク分析・評価を実施し、次年度の対策推進計画に反映させた。

令和３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初期対応訓練、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、東京オリンピック・パラリンピック競技大会を控え、サイバー攻撃の増加が懸念されるところ、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、私物のパソコン等を利用したテレワークの増加に対応できるよう、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。

個人情報保護委員会

2020 年度の総合評価・2021 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、平成 28 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、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。

令和３年度においては、政府機関におけるセキュリティ・IT 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」（令和元年９月 17 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

2020 年度の総合評価・2021 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　並木　稔

カジノ管理委員会では、2020 年度においては、2019 年度に策定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（以下「ポリシー等」という。）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ことにより、情報セキュリティ対策の定着を図った。また、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。

情報セキュリティ自己点検及び情報セキュリティ監査等の結果、ポリシー等は概ね遵守されている状況が確認された。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、2020 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。

警察庁

2020 年度の総合評価・2021 年度の全体方針

最高情報セキュリティ管理者
情報通信局長　砂田　務

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。

令和２年度においては、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、監査の結果を踏まえて情報セキュリティ対策の改善を推進した。また、警察庁及び都道府県警察の情報システムに対する脆弱性試験を実施し、情報セキュリティ対策の強化を図るとともに、情報セキュリティ意識の向上を図った。

令和３年度においても、引き続き、緊張感を持ち、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。

金融庁

2020 年度の総合評価・2021 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　白川　俊介

令和２年度は、新型コロナウイルス感染症が世界的に蔓延し、新しい生活様式への移行が急ぎ求められる状況となった。新型コロナウイルスへの対応として社会全体で幅広く実践されたテレワーク、サテライトワーク等の取組については、アフターコロナにおいても後戻りさせることなく、新しい生活様式・ビジネス様式として拡大・定着させ、社会全体のデジタル化を官民一丸となって一気呵成に実現する必要があるとの議論が規制推進会議等においてなされた。2020 年 7 月 8 日には、内閣府、規制改革推進会議、四経済団体の連名で「『書面、押印、対面』を原則とした制度・慣行・意識の抜本的見直しに向けた共同宣言」が発表された。

こうした社会情勢の変化に的確に対応していくため、金融庁としても行政手続きのオンライン化を進めるとともに、テレワーク等の非対面環境においても金融行政の遂行に支障が生じないように環境整備を急速に進めてきたところである。

一方で、官民共にデータの利活用や新たなデジタル技術の活用が進む中、政府機関等からの情報の窃取等を企図したサイバー攻撃への対策の重要性は著しく高まっているところである。金融庁では、サイバー攻撃等に対応するための技術的な対策を講じるとともに、専門事業者によるセキュリティ監査の受検、職員に対する標的型攻撃メール対処訓練や情報セキュリティ研修等の実施等を通じて職員の情報セキュリティへの意識向上を図り、当庁の情報セキュリティ水準の維持向上に努めてきた。

令和３年度においても、引き続きサイバー攻撃への対策やテレワーク環境への対応を行っていく。また、政府機関等の共通の取組として、情報セキュリティ対策のための統一基準群の改定が予定されており、その改定内容を踏まえ速やかに金融庁情報セキュリティポリシー等の改定を行う予定である。さらに、情報セキュリティに関する体制強化のため、内閣官房内閣サイバーセキュリティセンターや他省庁等と緊密に連携し、情報セキュリティへの対応に万全を期す。

消費者庁

2020 年度の総合評価・2021 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

令和２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により業務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高度化・巧妙化するサイバー攻撃の被害が報告されている。このような情勢の中においても、当庁においては、情報セキュリティ対策の運用が適切に行われており、重大な情報セキュリティインシデント等は発生していない。

システムによる情報セキュリティ対策としては、平成 30 年度に消費者庁ネットワークシステムの更改やシンクライアント端末、仮想デスクトップが導入されていたため、今回のテレワーク実施時には混乱なく対応することができた。また、主幹システムである消費者庁ネットワークシステムで採用しているネットワーク分離やログ統合監視機能等は、不正アクセスなどのサイバー攻撃に対する対策として有効に機能している。

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た。不審メール訓練は訓練内容を工夫し、問題点が確認できたことを踏まえて、職員向けの教育研修資料に最新の標的型攻撃の脅威や対応方法を追加するなど、組織全体として情報セキュリティのレベルの一層の引上げを図った。

令和３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は令和３年度も継続されることが想定され、引き続き、混乱やインシデントが発生することなくテレワーク等の環境においてもワーク・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。

また、令和３年度に予定される「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」の改定に基づき、当庁の情報セキュリティポリシー及び関連規程の改定を行い、その内容をｅラーニング等により教育・周知し、不審メール訓練やインシデント対応訓練などの実施により職員の意識を向上させるとともに、引き続き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、継続的な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

2020 年度の総合評価・2021 年度の全体方針

最高情報セキュリティ責任者
統括官 開出 英之

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。

令和２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。

令和３年度においては、「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」の見直しを踏まえ、復興庁情報セキュリティポリシー等の関係規程の改定を行うとともに、令和２年度に実施した情報セキュリティに関する自己点検や情報セキュリティ監査で明らかとなった課題等を踏まえ、情報セキュリティ教育のための研修教材の見直しの実施など、復興庁職員の更なる情報セキュリティ対策に対する意識の向上を図ることにより、復興庁全体の情報セキュリティ水準の維持・向上に取り組んでいくこととする。

総務省

2020 年度の総合評価・2021 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　田原 康生

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

○2020 年度の総合評価

2020 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、2019 年度から引き続き、総務省情報セキュリティポリシー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、省内では誤送信をはじめとした個人情報漏えい事案が多数発生したことから、省内の個人情報保護担当とも連携し、外部へのメール送信時のポップアップ表示の見直しや、端末起動時の注意喚起など、全職員が認識できる形の周知を徹底した。また、特別給付金の偽サイトに関しては、総務省ホームページや公式 SNS による注意喚起も行った。

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

○2021 年度の計画

(1) 情報セキュリティ対策推進体制の一層の強化

2021 年度においては、総務省の情報セキュリティ対策推進体制の強化を図るため、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

2020 年度対策推進計画の実施状況やその評価を踏まえ、以下の事項を重点的に実施する。

(ｱ) 東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）に向けた情報セキュリティ教育・訓練の実施

東京大会の開催時期に向けて、職員及び情報システムセキュリティ責任者等に対する教育・自己点検、職員への不審メール提出訓練を計画的に実施する。

(ｲ) 情報セキュリティ対策の継続的な推進

引き続き情報セキュリティ対策を着実に実施する。

・ 各種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・リスクへの対応を行う。特に、新型コロナウイルス感染症対策として、デジタル技術を利活用する際にも、情報セキュリティ対策の徹底を求めていく。

・ 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する。

法務省

2020 年度の総合評価・2021 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　髙嶋 智光

法務行政は、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職務であり、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る。

かかる認識の下、サイバーセキュリティ戦略（平成３０年７月２７日閣議決定）において示された取組の方向性を踏まえ、令和２年度は、各組織における情報セキュリティマネジメントの実効性の更なる向上を図るため、当省の情報セキュリティポリシー（以下「ポリシー」という。）に基づく教育、自己点検等の取組をより効果的に実施し、当省全体としての情報セキュリティ水準の維持・向上を図った。また、セキュリティ対策と一体となった業務改革（ＢＰＲ）を推進していくに当たり重要となるセキュリティ・ＩＴに係る業務を担う人材の確保・育成のため、「法務省におけるセキュリティ・ＩＴ人材確保・育成計画」（平成２８年８月３１日最高情報セキュリティ責任者決定。）の見直しを行うとともに、同計画に基づき、セキュリティ・ＩＴ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、各取組を通じて、各組織における情報セキュリティマネジメントの定着は着実に進んできているものの、新型コロナウイルス感染症対策として急速に広まったテレワークやウェブ会議等の多様な働き方を前提として、職員一人一人がポリシーを確実に遵守し、当省全体としての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、各取組をより効果的に実施し、各組織における情報セキュリティマネジメントの更なる向上に努める必要がある。

さらに、サイバー空間における脅威の深刻化や多様な働き方の促進を踏まえ、新たな脅威の発生等、事案発生時に迅速かつ適切に対処することができるよう、職員個人の能力の強化はもとより、組織としての対処能力の向上を図る必要がある。特に令和３年度上半期は、延期されていた２０２０年東京オリンピック・パラリンピック競技大会の実施が予定されており、これらに伴う政府機関等へのサイバー攻撃の可能性に備え、事案対処に万全の準備を整える必要がある。

したがって、令和３年度は、各組織における情報セキュリティマネジメントの実効性の更なる向上を図るため、多様な働き方を前提として、ポリシーに基づく教育や自己点検等をより効果的に実施するとともに、サイバーセキュリティ対処能力の向上及びセキュリティ・ＩＴ人材の確保・育成を推進することとする。

外務省

2020 年度の総合評価・2021 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。

2020 年度においては、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、リモート形式による情報セキュリティ対策研修、NISC が行う CSIRT 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。また、新型コロナウイルス感染症の感染防止対策として Web 会議システムの業務利用やテレワークの積極的な活用を推進した結果、従来とは大きく異なり、要管理対策区域外における業務情報の取扱いが増えている。管理職員の監督が行き届かない自宅等においても適切に情報を取扱いつつ効率的な業務遂行を行うため、テレワーク環境の追加整備を行った。新しい働き方に適応した環境の整備は、職員によるシャドーIT の抑止にも繋がり、情報セキュリティ対策の観点からも適切であり、必要なものと認識している。

2021 年度は、次に掲げる取組を通じ、外務省情報セキュリティポリシー等に基づく、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、新たな働き方等を踏まえ、職員一人ひとりの情報セキュリティ水準の向上により一層努める。また、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も推進する。夏には東京 2020 オリンピック・パラリンピック競技大会が予定されており、大規模イベントに乗じたサイバー攻撃の脅威が高まることが想定されるところ、関係機関とも緊密に連携の上、情報セキュリティ対策の確保に引き続き万全を期していく。

- 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
- 最新のサイバー情勢を踏まえた外部専門家による情報セキュリティ研修
- 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

2020 年度の総合評価・2021 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　茶谷　栄治

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。

2020 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
・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（ただし新型コロナウイルス感染症への対応等により計画より遅延）
・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のセキュリティコンサルティング契約の締結
・CIO 補佐官４名の最高情報セキュリティアドバイザーへの指名

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。2021 年度は、こうした状況にもよく目配りしつつ、引き続き主に以下の項目に取組むこととする。

・「財務省セキュリティ・IT 人材確保・育成計画」（2016 年 8 月策定。以下「育成計画」）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）
・東京 2020 オリンピック・パラリンピック競技大会に向けて、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
・政府統一基準群を踏まえた財務省の情報セキュリティポリシーの改定
・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

2020 年度の総合評価・2021 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　　増子　宏

近年、教育、研究機関等において、攻撃者がターゲットとする特定組織の特性に応じて、当該組織にのみ適用する高度なサイバー攻撃の手法を用いて執拗に攻撃を行う「標的型攻撃」が疑われる事案の発生が増加しており、当該機関等を所管する文部科学省においても、更に高度なサイバー攻撃が行われる可能性を想定したセキュリティ対策を講じる必要がある。

本計画を策定するにあたり、統一基準群に基づき、「高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成２８年１０月７日サイバーセキュリティ対策推進会議決定)」（以下、「リスク評価等のガイドライン」という）に沿ってリスク評価を行った。

リスク評価等のガイドラインに示された対策セットについては、文部科学省本省の基幹システムである行政情報システムにおいて導入済みであったが、日々進化する脅威に対応するためには、対策セット以外の対策や、CSIRT 能力の強化といった対策を講じていく必要がある。

また、在宅勤務の普及により、Web 会議に利用する端末が増加していることから、IT 資産管理対策も必要となってきている。

施設等機関（国立教育政策研究所及び科学技術・学術政策研究所）については文部科学省本省との連携をより強化し、文部科学省全体として情報セキュリティ水準の底上げを図る観点から、更なる一層の指導・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、並びに、インシデント対処能力の向上を推進するとともに、全職員に対して情報セキュリティ意識を向上させるため、本年度は以下に掲げる取組を推進する。

(1) 情報セキュリティポリシーを全職員に浸透させるため、教育コンテンツの改善や内容の充実とともに実施体制を強化
(2) セキュリティ対策の強化が必要な事項に対する自己点検の実施
(3) 情報セキュリティ監査（準拠性監査及び情報システム脆弱性診断）の実施
(4) CSIRT 要員におけるインシデント・ハンドリング能力及び最先端のサイバーセキュリティに関する情報収集能力強化
(5) 施設等機関のセキュリティ強化のための取組
(6) 自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアの導入
(7) 情報セキュリティ関連規程の改訂
(8) 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

2020 年度の総合評価・2021 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　土屋 喜久

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、令和２年度においては、次の取組を重点的に実施した。

- 東京オリンピック・パラリンピック競技大会（以下「東京 2020 大会」という。）におけるサイバーセキュリティ対策の強化
- GSOC（Government Security Operation Coordination team。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 資産管理機能の導入
- 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への対応

令和３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。

- 「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」の見直し等に基づく当省情報セキュリティポリシー及び関係規程の改定
- 東京 2020 大会におけるサイバーセキュリティ対策の強化
- GSOC と連携した IT 資産管理機能の活用

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

2020 年度の総合評価・2021 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せず、原因究明を徹底するとともに、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し、省全体で実行に移すことが重要である。令和２年度においては、これらの内容を教育コンテンツに追加し、ｅラーニング、集合研修、自己点検など様々な手段を用いて、繰り返し職員への浸透を図った。

４　令和３年度においても、上記の取組を引き続き推進し、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を底上げする。

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ラーニングの確認テストは全問正解するまで繰り返し実施することとし、情報セキュリティに関するルールの職員への浸透を徹底する。

イ　前年度の情報セキュリティ監査で指摘の多かった項目は、改善を怠ることで情報漏えい等につながるそれがあるため、重点的に監査する。

また、民間企業等で発生した事案についても、当省で同様の事案が発生することを未然に防ぐため、監査項目として盛り込む。

ウ　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幹部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、発生した情報セキュリティインシデントへの迅速かつ的確な対処等に努めるものとする。

経済産業省

2020 年度の総合評価・2021 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　多田　明弘

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。

昨年からの新型コロナウイルス感染症の世界的な蔓延に加え、今後の東京 2020 大会等、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今後も増加し、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。

２０２０年度においては、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、経済産業省基盤情報システム（以下「基盤システム」という。）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つつ、Web 会議の利用に係るセキュリティ確保のためのルールや環境を整備した。

２０２１年度においては、これまでの取組みを継続することとしつつ、２０２０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ついて引き続きセキュリティ対策の維持・向上を図るとともに、テレワークや Web 会議の利用拡大に係るセキュリティ確保のためのルールや環境を整備・改善
（２）各部局で所管する業務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と対策の強化
（３）２０２１年度に予定している基盤システムの更改に向け、サイバー攻撃対策等に関して現在以上のセキュリティ水準とするべくシステムへの具体的な実装内容等を検討

（４）「経済産業省におけるセキュリティ・IT 人材確保・育成計画」に基づく取組の継続によるセキュリティ・ＩＴ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の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を実施

国土交通省

2020 年度の総合評価・2021 年度の全体方針

最高情報セキュリティ責任者
総合政策局長 石田 優

現行のサイバーセキュリティ戦略（平成30年7月27日閣議決定）の策定後に顕在化した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環境整備やクラウドサービスの導入が急展開しており、国土交通省をはじめ、独立行政法人や所管事業者等に対するサイバー攻撃も多数観測・報告されている。

このため、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、令和２年度には、以下のような対策を実施している。

① 電磁的記録媒体の廃棄に係るデータの確実な抹消が図られるよう「国土交通省情報セキュリティポリシー」を改定すると共に関係規程を改定、さらに「携帯電話・スマートフォン等による情報処理に関する規程」を新設
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、総務省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 CISO 連絡会議の開催、重要インフラ分野（航空、空港、鉄道、物流）の情報共有体制である（一社）交通 ISAC を中心とした情報共有網の拡充、所管事業者向けの情報セキュリティ対策のチェックリストの作成等を実施

令和３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

2020 年度の総合評価・2021 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　正田寛

脱炭素社会の実現に向けて、とりわけ気候変動問題の解決には、地球規模で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も、多様な働き方への対応、緊急時の対応力の強化、効果的な情報発信や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。その一方で、効果的かつ信頼性のある情報発信や IT 技術の有効活用を行うためには、適切な情報セキュリティ対策も不可欠である。

近年、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、広範な攻撃のリスクにさらされている。こうした変化に対応するため、情報セキュリティ対策の見直しを行い、システム及び人的な対策を継続して適切に強化することで、持続可能な社会づくりに資する安定的な情報システムの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。

令和２年度は、テレワークの実施やウェブ会議の利用が急速に拡大したことから、リモート接続環境の脆弱性を狙った不正アクセスや、クラウドサービスの利用に用いる認証情報を狙ったフィッシングメール等による攻撃と、それらによる被害の拡大が、日本国内だけではなく、多くの国で報告された。環境省としても、境界防御による多層防御に加え、新たな技術を活用した対処及び監視等の重要性を認識したところである。こうした外部脅威の動向については、教育等を通じて職員に周知する一方、通常業務において意図しない情報漏えいを発生させることのないよう、改めて注意喚起を行った。また、令和元年度に成立した改正動物愛護管理法の施行に伴い、施行に係る手続のための情報システムについて、要件定義／設計段階から情報セキュリティ対策の適切な実装に取り組んだ。

令和３年度においても、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する。情報セキュリティ監査や自己点検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る。また、令和３年度に予定されている「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」の改定に基づき、環境省情報セキュリティポリシー等の適切な見直しを行い、職員への周知を図る。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適切な確認と見直しを実施する。なお、様々なイベント、取組、事業等が新型コロナウイルス感染症の影響を受け、オンライン開催等 IT 技術の利用が拡大していることを踏まえ、令和４年度に

予定している環境省の基幹ネットワークシステムの更改においては、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検討し情報セキュリティ対策を適切に進める。

また、重要な情報システムついては、要件定義／設計段階から情報セキュリティ対策の適切な実装のために取り組む。

防衛省

2020 年度の総合評価・2021 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、２０２０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。

・サイバー防衛隊等の体制強化（約８０名の増員）
・サイバー人材の確保・育成（サイバーコンテストの開催）
・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、２０２１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「自分だけは「大丈夫」と思う心が狙われる」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、標的型攻撃等への対処に係るメール訓練を行った。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。

２０２１年度においては、引き続き、サイバー防衛隊等の体制を拡充するとともに、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キル人材の育成のための部外教育機関を活用した教育実施など、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、２０２０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、メール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。

（本ページは白紙です。）

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　「政府機関等の情報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

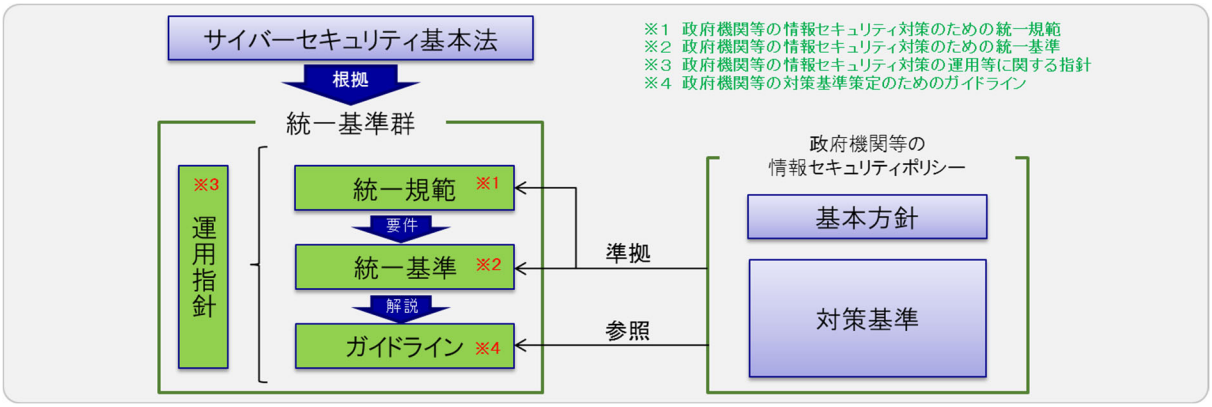
１　概要

「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」（以下「統一基準群」という。）は、サイバーセキュリティ基本法に基づく政府機関、独立行政法人及び指定法人（以下「政府機関等」という。）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づ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、2020年度時点では、2018年７月25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（平成30年度版）が運用されている。

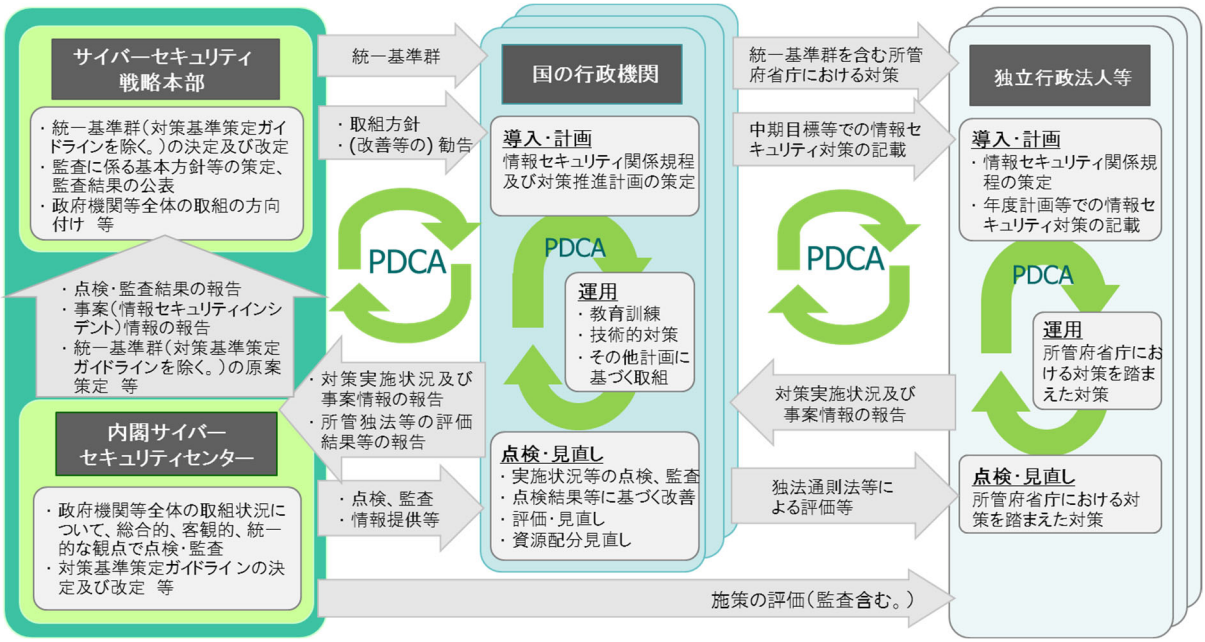
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等の情報セキュリティ対策のための統一基準（以下「統一基準」という。）」と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（図表１）。

図表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２）。

図表２　政府機関等における情報セキュリティのマネジメントサイクル



２　統一基準群の改定

政府機関等の情報システムの整備において、クラウド・バイ・デフォルト原則に則ったクラウドサービスの利用拡大が見込まれるところ、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年度中の改定に向け作業を進めている。

今回の改定では、①クラウドサービスの利用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つのテーマを掲げている（図表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する予定である。また、利用者側の設定不備による情報漏えいが後を絶たないことから、サービスの設定の誤りを防止するために、サービス提供者からの推奨される設定情報の入手や、設定の誤りを検知する機能や性能を監視する機能の利用に関する規定を追加する予定である。

（２）情報セキュリティ対策の動向を踏まえた記載の充実

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)に関する記載を追加する予定である。この他、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(*2)だけでは十分なセキュリティを担保できなくなってき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(*3)の考え方の導入について検討するよう記載を追加する予定である。

(*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。

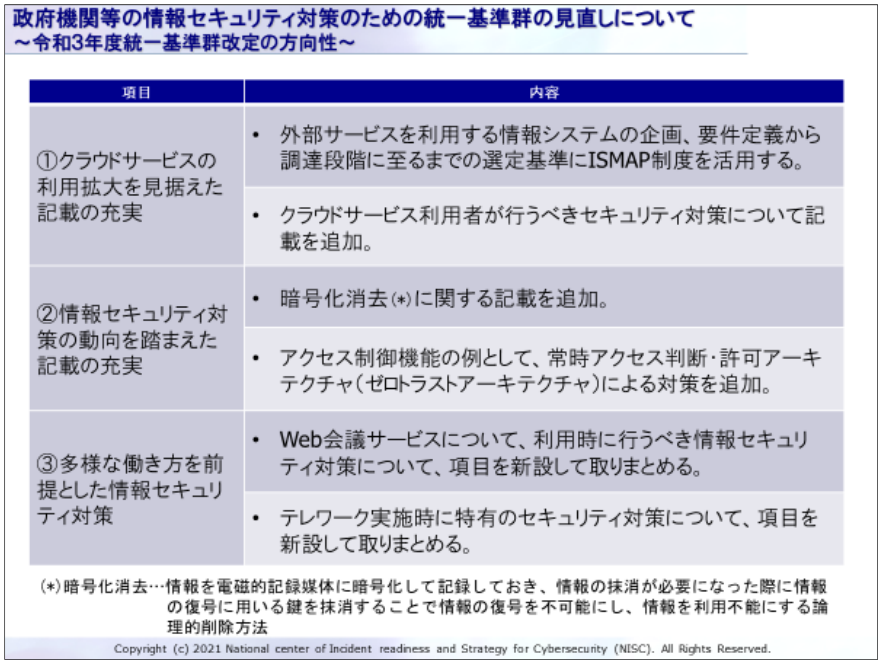
(*2)境界型防御…イントラネットなどの内部ネットワークとインターネットなどの外部ネットワークの接続点に境界を設け、外部ネットワークからの脅威に対する防御を行うことを基本とするセキュリティ対策の考え方。

(*3)ゼロトラスト・アーキテクチャ…データやサービス等のリソースへの全てのアクセスは一旦信頼できないものとしてその都度認証と権限確認を行うことで、仮に攻撃者が境界の内側に侵入してもリソースへアクセスするたびに認証と権限確認が行われるようになり、攻撃者による内部での自由な活動を阻害しようとするセキュリティ対策の考え方。

（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することを予定している。併せて、政府機関等においても利用が定着しつつあるWeb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する予定である。

図表３　令和３年度統一基準群改定の方向性



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について
～令和3年度統一基準群改定の方向性～

項目	内容
①クラウドサービスの利用拡大を見据えた記載の充実	• 外部サービスを利用する情報システムの企画、要件定義から調達段階に至るまでの選定基準にISMAP制度を活用する。
	• クラウドサービス利用者が行うべきセキュリティ対策について記載を追加。
②情報セキュリティ対策の動向を踏まえた記載の充実	• 暗号化消去(*)に関する記載を追加。
	• アクセス制御機能の例として、常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ）による対策を追加。
③多様な働き方を前提とした情報セキュリティ対策	• Web会議サービスについて、利用時に行うべき情報セキュリティ対策について、項目を新設して取りまとめる。
	• テレワーク実施時に特有のセキュリティ対策について、項目を新設して取りまとめる。

(*)暗号化消去…情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法

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

平成 30 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」（平成 30 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。

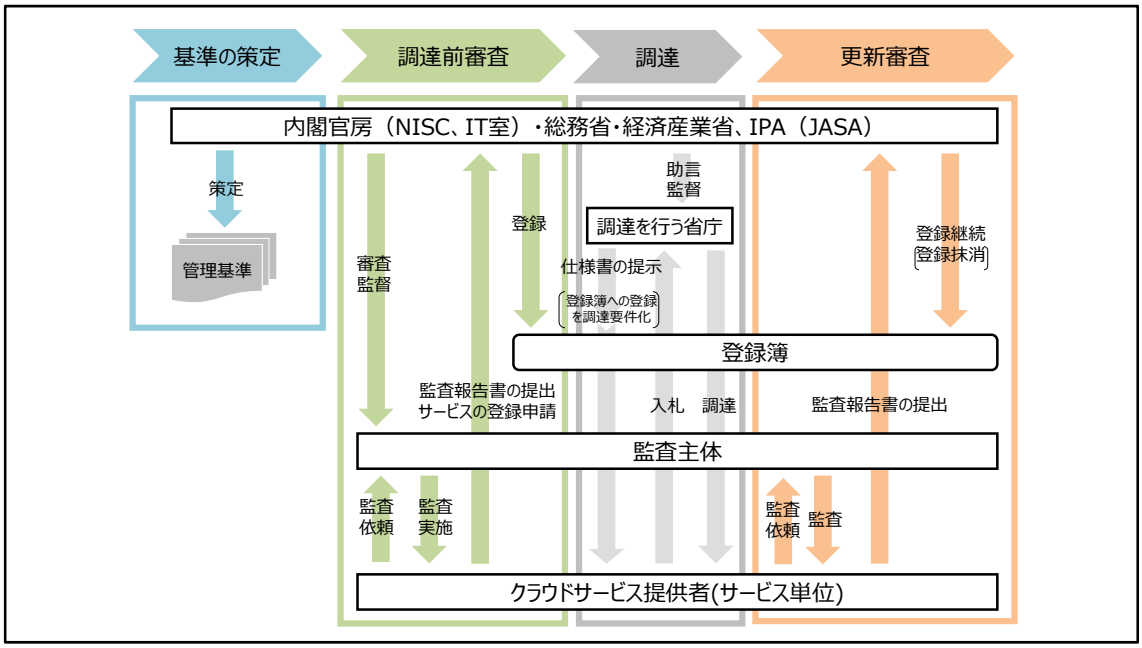
そうした状況から、「サイバーセキュリティ戦略」（平成 30 年７月 27 日閣議決定）において、「クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める」ことが位置付けられ、また、「デジタル・ガバメント実行計画」（令和元年 12 月 20 日閣議決定）において、クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備がされること及び安全性評価基準、安全性評価の監査の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう環境整備等について検討を進めることが位置付けられた。

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、令和２年６月に NISC・内閣官房情報通信技術(IT)総合戦略室・総務省・経済産業省の連携の下「政府情報システムのためのセキュリティ評価制度」（英語名：Information system Security Management and Assessment Program、通称：ISMAP（イスマップ）、以下「ISMAP」という。）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１のとおりである。

図表１　ISMAP の基本的流れ



２　ISMAP クラウドサービスリストの公開と今後の課題

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独立行政法人情報処理推進機構（IPA）が運用する ISMAP ポータルサイト[1]にて公開されている。今後も継続的に、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クラウドサービスについては ISMAP クラウドサービスリストの追加登録を行い、政府機関における ISMAP の利用を推進していくとともに、本制度の運用状況を踏まえ、当該基準等について見直しを行う。

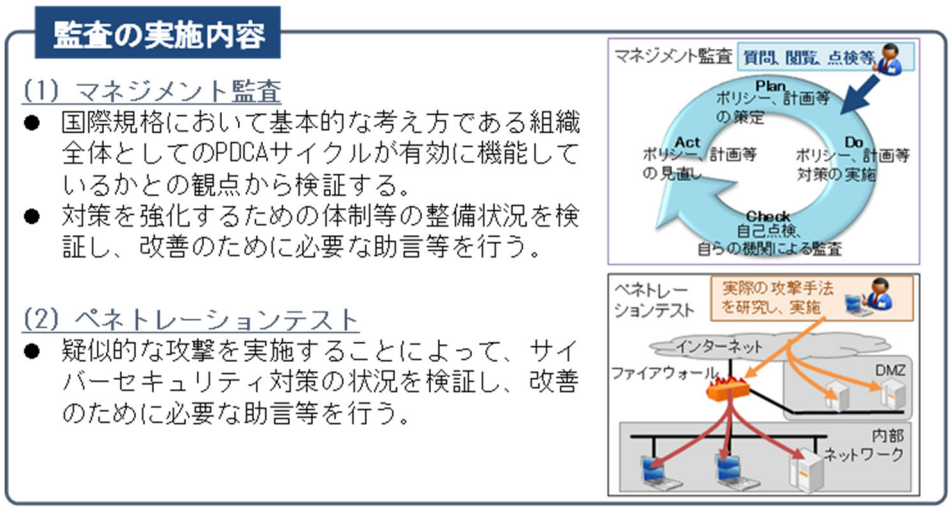
なお現段階では、ISMAP を利用したクラウドサービス調達は政府機関に要求されるものであるが、公開されるリスト等を民間等においても参照することで、クラウドサービスの適切な活用が推進されることが期待される。

[1] 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　2020 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、2020年度は、政府機関、独立行政法人及び指定法人（以下「政府機関等」という。）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。



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

2020 年４月から 2021 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（全 23 府省庁）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

「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」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、地方組織・外局等で管理・利用しているシステムを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

「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。2016 年 10 月 12 日改定、2019 年４月１日改定）に基づき、各府省庁への監査を実施し、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、各府省庁に対して、改善のための必要な助言等を行った。また、マネジメント監査の実施対象外の府省庁に対しては、2018 年度以前の監査結果を踏まえて各府省庁が策定した改善策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。

監査におけるグッドプラクティスの事例及び主な助言等並びに 2018 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 グッドプラクティスの事例

・内部監査において、毎年度異なる監査対象システムを選定し、管理部署及び利用部署への監査に加えて、委託先への監査も実施し、ヒアリングに加えて、現場視察、端末のセキュリティ対策に関する実機での確認等を監査担当である職員自身が実施している事例

・情報流出に係る対策として、機器等の調達分類ごとにデータ抹消方式や抹消結果の確認方法を漏れなくまとめた要件整理表を作成し、廃棄を確実に実施するための対策を講じていた事例

・「機器等の管理に関する実施手順」を新規に制定して現物の管理を強化するなど独自の取組を実施している事例

・外部委託や約款による外部サービスの利用にあたり、「想定されるリスク」、「業務利用に関するリスクの分析」、「リスクを低減する措置」、「リスクの評価結果」及び「リスク許容の可否」を検討した結果について、最高情報セキュリティアドバイザーが当該リスク対策の妥当性を確認している事例

② 主な助言等

2020 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

③ 2019 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

マネジメント監査の実施対象外の 11 府省庁に対して、2019 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 2020 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、改善策が概ね実施済となっていた。

2018 年度までの監査においてセキュリティポリシーの策定等の規定類や体制の整備や強化が進んでいたが、サイバーセキュリティ推進部局以外の部局が対策を講じる部分について、その対策水準の向上が求められる場合や、府省庁が自ら定めた規定の一部が適切に実施されていない等、規定の運用に課題が残っているものが発見された。

2019 年度の監査においても 2018 年度までの各府省庁における監査と同様の傾向が見られるものの、全体として指摘数は減少傾向に有り、情報セキュリティマネジメントシステムに係る課題についてはさらに改善が進んでいた。また、業務継続性が重要となるシステムについては、可用性を十分に考慮された設計となっていることが確認できた。

2020 年度の監査においては、情報セキュリティマネジメントシステムに係る課題についてはさらに改善が進んでいることが確認できた。一方、地方組織・外局等において独自に対策基準を策定している場合のPDCAサイクルを構成する主要な取組や情報を取り扱う区域の管理に係る運用について課題が見られた。

フォローアップにおいて、各府省庁の 2019 年度以前の監査に対する改善結果等を確認したところ、監査で発見された課題について、各省が策定した改善計画に沿って改善されており、さらなる対策水準の向上が確認できた。

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必要である。

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

2020 年４月から 2021 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（全 23 府省庁）が運用するインターネットに接続する基幹 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 49 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（以下「ホスト」という。）を選定し、インターネット（外部）から調査対象ホスト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）から調査対象ホスト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脆弱性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、侵入できる脆弱性等が発見された。このうち主なものは、サーバの管理等で使用されるパスワードについて、

その管理方法が適切でない、パスワード解析への耐性が十分でないなど、主体認証情報（ID・パスワード等）の管理不備に関するものであった。調査において侵入に利用できる脆弱性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、発見された脆弱性等については、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。

2019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

2020 年４月から 2021 年３月までの間

（２）マネジメント監査の実施対象

独立行政法人及び日本年金機構を含む指定法人（全 96 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

「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」等に基づく施策の取組状況について、独立行政法人情報処理推進機構（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

「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。2016年10月12日改定）に基づき、独立行政法人情報処理推進機構（IPA）に事務の一部を委託し、法人への監査を実施し、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。

監査におけるグッドプラクティスの事例及び主な助言等の状況は以下のとおりである。

① グッドプラクティスの事例

・情報担当や教職員向けなど職務別の研修や標的型メール攻撃訓練など多くの情報セキュリティ教育を実施し、さらに、CSIRT 要員向け教育には、全国 50 以上の拠点から各 1 名以上参加させるなど、法人全体として体制強化に取組んでいた事例
・委託先が運用保守業務を行う際に利用するリモートアクセス環境において、電子証明書による認証と識別コード及びパスワードによる認証を併用して VPN 接続をさせるとともに、接続した委託先がアクセス可能な範囲を論理的に制御し、さらに、通常、委託先からは接続不可の状態にしており、委託先がリモートアクセスをする際には、事前に作業申請を提出させ、内容を確認した上で都度接続可能な状態にし、接続許可を出していた事例
・IPA の情報セキュリティ対策ベンチマークを活用し、委託先選定時の評価を実施するほか、運用受託機関等には年次で自己診断等の結果を報告させ、情報セキュリティ対策状況等の評価を実施していた事例
・基幹 LAN システムに接続されている全サーバに対して、年 1 回の頻度で、使用しているソフトウェアに脆弱性が無いか確認するためのプラットフォーム診断を実施し、発見された脆弱性について対策を実施していた事例

② 主な助言等

2020 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かかる監査を実施し、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
- CSIRT 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

③ 2019 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

2019 年度に監査を実施した独立行政法人等 29 法人に対して、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改善計画通り対策が概ね実施されていることを確認した。

2020 年度は 31 法人のマネジメント監査を実施した。各法人は情報セキュリティ対策の推進に努力していた。一方、これらの法人においては多様な業務を背景とし、統一基準群のもとでの情報セキュリティ対策への取り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。

フォローアップにおいて、2019 年度に実施したマネジメント監査で発見された重要な事項への対策状況を確認したところ、一部遅延は見られるものの改善計画に基づいて対

策されており、情報セキュリティ水準の向上が確認できた。

今後各法人において、引き続き、多様な業務を踏まえつつ、統一基準群のもと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。

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

2020 年４月から 2021 年３月までの間

（２）ペネトレーションテストの実施対象

独立行政法人及び日本年金機構を含む指定法人（全 96 法人）のうち、31 の法人が運用するインターネットに接続する基幹 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 31 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る情報システムに対しての侵入可否調査を独立行政法人情報処理推進機構（IPA）に事務の一部を委託して実施した（ただし、IPA 及び日本年金機構の情報システムに対する侵入可否調査については NISC が自ら実施した）。具体的には、ホストを選定し、インターネット（外部）から調査対象ホストへの侵入可否調査及び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）から調査対象ホスト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脆弱性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、侵入できる脆弱性等が発見された。このうち主なものは、サーバの管理等で使用されるパスワードについて、パスワード解析への耐性が十分でないなどの主体認証情報（ID・パスワード等）の管理不備に関するものであった。また、本来は許可された利用者のみが閲覧可能とすべきサーバの管理画面に、認証等の手段を経ることなくアクセスできた例も見られた。調査において侵入に利用できる脆弱性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、発見された脆弱性等については、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。

2019年度に実施したペネトレーションテストの結果に対する改善計画において、提出時点で対策が未完了となっていた項目については、マネジメント監査と合わせてその後の進捗状況を確認するフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認した。

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

各府省庁において、情報セキュリティインシデント（以下「インシデント」という。）を認知した際に、初動対処、被害拡大防止、早期復旧等に取り組むに当たっては、府省庁関係者への報告やNISCへの連絡等を適時・適切に行い、幹部職員の指揮の下、組織として迅速かつ適切に対処することが重要である。

本訓練は、各府省庁におけるインシデント認知時に、府省庁CSIRT要員とCISOを含む幹部職員、関係部局、NISC等との報告・連携が確実に行われること、幹部職員による指揮の下で迅速かつ適切に組織的対処が行われることに主眼を置き、府省庁CSIRT要員のインシデント対応における対処能力及び対処手順の整備状況を評価するとともに、CSIRT要員の対処能力の向上を目的としたものである。

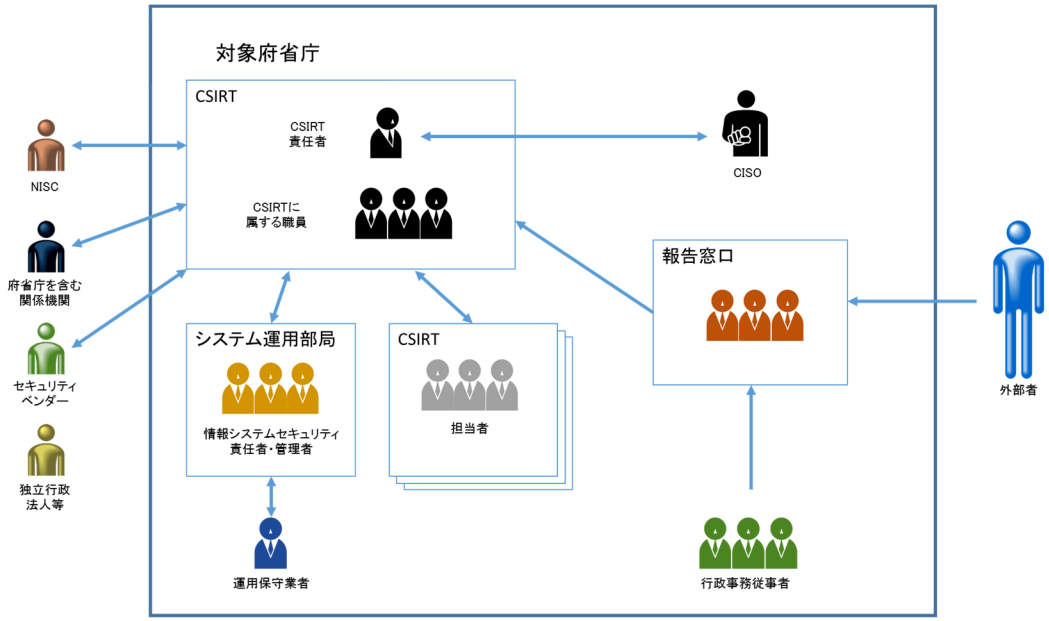
（２）概要

訓練参加者は、日常業務で使用している、外部との電子メールの送受信ができる業務用端末から電子メールを用いて、府省庁内外の様々な登場人物を演じる訓練事務局（NISC及び受託者）とのやりとりを通じて訓練を進行した。

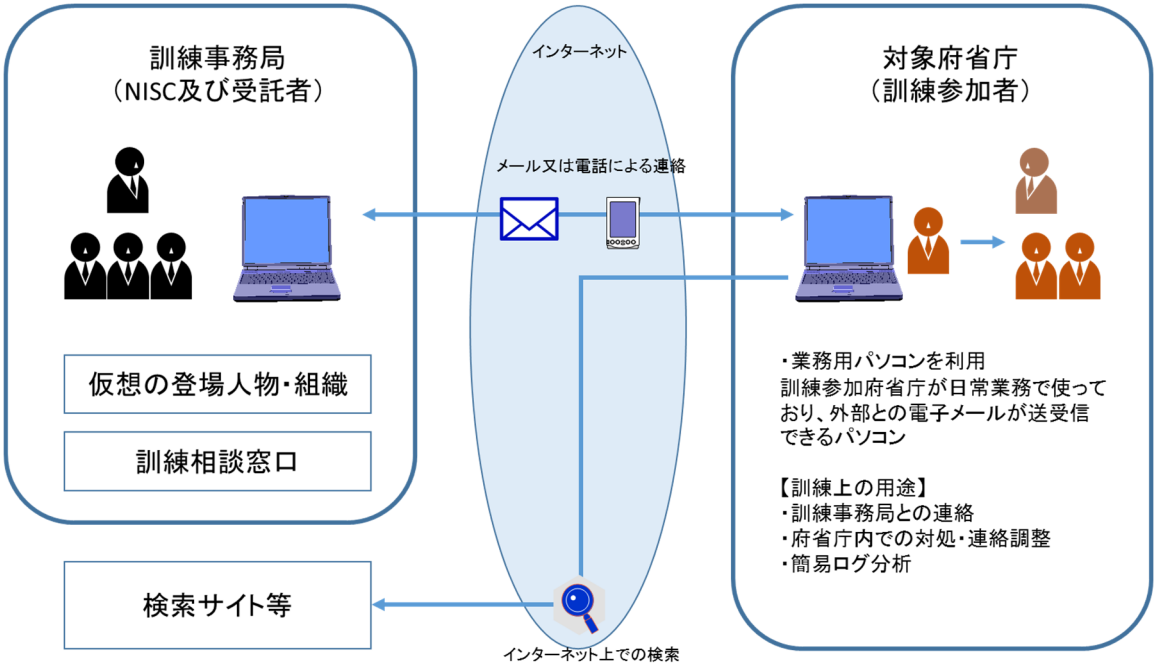
訓練参加者は、府省庁内外の様々な登場人物を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、状況に応じて通信ログ等の分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

図表１に本訓練の登場人物、図表２に本訓練の物理的環境を示す。

図表１　本訓練の登場人物



図表２　本訓練の物理的環境



（３）参加人数

約130人（全23府省庁参加）

（４）訓練時期

2020年11月～12月

（５）まとめ

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。更に、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、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、2021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、経験者や有識者による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した。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2021年度以降の取組に反映していく。

No.	時期	テーマ	講師	参加人数
1	2020 年７月～2021 年２月	【CSIRT 研修】 ・インシデント対処 ・デジタル・フォレンジック ・令和元・２年度のトピック　ほか	外部講師	講義資料（講師の説明音声入り）の配布のみ
2	2020 年 10 月	【CSIRT 向け講習会】※ インシデント対処に必要な基礎知識 ・組織を取り巻くセキュリティ脅威 ・インシデント対処の基礎 ・ケーススタディ　ほか	外部講師	約 40 名

※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

NISC職員による統一基準群の解説やマネジメント監査に係る説明により、情報セキュリティ関係職員の基本的な知見を向上させ、政府機関等における情報セキュリティの確保につなげること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

今年度は、IPAが公表している「情報セキュリティ　10大脅威とその対策（組織編）」の解説、「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」の初任者向けの解説、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についての資料を作成し、配布にて実施した。

No.	時期	テーマ	講師	参加人数
1	2020年 ６月	・情報セキュリティ　10 大脅威とその対策（組織編） ・政府機関等の情報セキュリティ対策のための統一基準群について（初級編コース）	―	資料配付にて実施
2	2020年 11月	・統一基準群に基づく情報セキュリティ監査について	―	資料配付にて実施

５　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

2020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や座学、実機を用いた演習等を３回実施した。

インシデントハンドリングにおいては、事前準備から対処、事後対応までの全体の流れを学んだ。実機を用いた実習では、攻撃者が残した攻撃証跡を確認し、攻撃の流れを理解した上で、原因と再発防止策をグループディスカッションし、インシデントレスポンスのマネジメント能力や即応能力といった知識を深めた。

No.	時期	テーマ
1	2020年 11月	【座学①】 中央省庁におけるサイバーセキュリティの歴史と今後取り組むこと

2	2021 年 ２月	【座学②】（IT 関係と合同実施） インシデントハンドリングについて（座学）
3	2021 年 ３月	【座学（演習）③】 インシデントハンドリング演習

６　各府省庁セキュリティ担当者向け研修

（１）目的

2016年３月に決定された「サイバーセキュリティ人材育成総合強化方針」（2016年３月31日サイバーセキュリティ戦略本部決定）に基づき、政府一体となって政府機関におけるセキュリティ・IT人材を本格的に確保・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[2]。「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：2020 年 10 月～2021 年１月
受講者数：約 69 名
実施回数：計６回（１回６時間）

＜カリキュラム概要＞

①CISSP 概要 8 ドメインに関するイントロダクション、セキュリティとリスクマネジメント（セキュリティ、リスク、コンプライアンス、法、規制、事業継続）
②資産のセキュリティ（資産の保護）、アイデンティティとアクセスの管理（アクセス制御と ID 管理）
③セキュリティの運用（概念、調査、インシデント管理、ディザスタリカバリ）

[2]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。

④セキュリティエンジニアリング（セキュリティ設計と構築）
⑤セキュリティの評価とテスト（セキュリティテストの設計、実行、分析）、通信とネットワークセキュリティ（ネットワークセキュリティの設計と保護）
⑥ソフトウェア開発セキュリティ（ソフトウェアセキュリティの理解、適用と執行）、まとめと学力考査

別添４－５　セキュリティ動向調査

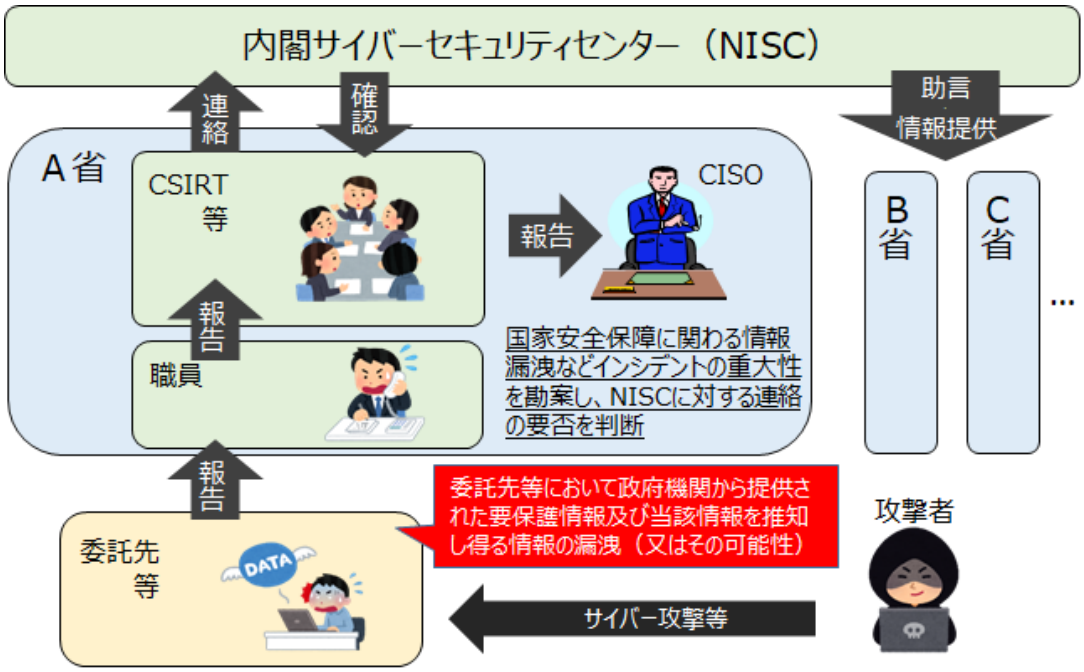
１　取組の概要

近年、政府機関の委託先がサイバー攻撃を受けたとの内容が続けて報道された。いずれも政府機関が管理する情報に対する情報セキュリティインシデントであり、委託先等における政府機関が管理する情報について、適正な管理を行うことは喫緊な課題となっている。

これまで、「政府機関等の情報セキュリティ対策のための統一基準」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、速やかに内閣サイバーセキュリティセンター（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ところである。しかし、外部委託先が取り扱う政府が管理する情報が、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。そこで、令和２年６月に「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１）。

報告の対象となる範囲は、政府機関が管理する情報であり、委託先等において政府機関から提供された要保護情報及び当該情報を推知し得る情報である。委託先等においてインシデントが発生した場合、各政府機関において最高情報セキュリティ責任者の指揮監督の下、速やかにインシデントの内容を把握し、国家安全保障に関わる情報漏えいなど重大なインシデントであると判断したときは、被害状況やインシデントの原因等を NISC に連絡を行う。NISC は、サイバーセキュリティの確保を図る観点から、必要に応じて、確認等を行うとともに、政府機関に必要な助言及び情報提供を行うものである。

図表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　申合せによる政府機関への注意喚起・調査

NISC では、前述の申合せにより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、政府機関への注意喚起等を実施した。令和２年度においては９件の報告があり、このうち、政府機関から委託を受けた事業者等からウェブサービスを介して情報が漏洩するインシデントについては、政府機関に対し、情報の外部漏えいの防止を徹底するとともに、委託先等（再委託先を含む。）における業務の実施場所、情報セキュリティ対策の実施内容及び管理体制等を把握し、必要に応じて是正する必要があるなどの注意喚起等を実施した（図表２）。

図表２　申合せにより実施した政府機関への注意喚起・調査

発出月	概要	実施区分
令和２年９月	「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」に係る留意事項等についての注意喚起等を実施	注意喚起・調査

（参考）申合せとは別に実施した政府機関への注意喚起・調査

その他内外の情報セキュリティインシデントの状況も踏まえつつ、政府機関への影響が大きいと判断される事案について注意喚起等を行った（図表３）。

図表３　申合せとは別に実施した政府機関への注意喚起・調査

発出月	概要	実施区分
令和２年８月	インターネットに流出した Facebook のアカウントに使われたメールアドレスの中に中央省庁職員の勤務先アドレスがあったと報じられたことから、勤務先アドレスを私的な SNS 等で利用することについての注意喚起を実施	注意喚起
令和２年 10 月	Wi-Fi 環境の整備状況等についての調査を実施	調査
令和２年 11 月	過去に脆弱性が確認されている SSL-VPN 装置の使用状況及び脆弱性対応の実施等についての調査を実施	調査
令和２年 12 月	SolarWinds Orion Platform 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を認識したとの情報が公開されたことを受け、公開情報を基に注意喚起を実施	注意喚起
令和２年 12 月	顧客関係管理ソリューション「Salesforce」の設定不備により意図しない情報が外部から参照される可能性があることを受け、サービスの利用状況や各種設定の確認・見直しを行うことなどについての注意喚起を実施。	注意喚起
令和３年２月	クラウドサービス「AWS」の東京リージョンでシステム障害が発生したことを受け、システム障害の有無等についての調査を実施	調査
令和３年３月	ファイル・データ転送アプライアンス「FileZen」の脆弱性に関する情報が公開されたことを受け、脆弱性対応の実施についての注意喚起等を実施	注意喚起・調査
令和３年３月	SNS サービス「LINE」において、個人情報等の管理上の懸念が報じられたことから、統一基準においては、約款による外部サービスにおける要機密情報の取扱いを禁止していることなどについての注意喚起等を実施	注意喚起・調査

別添４－６　高度サイバー攻撃への対処

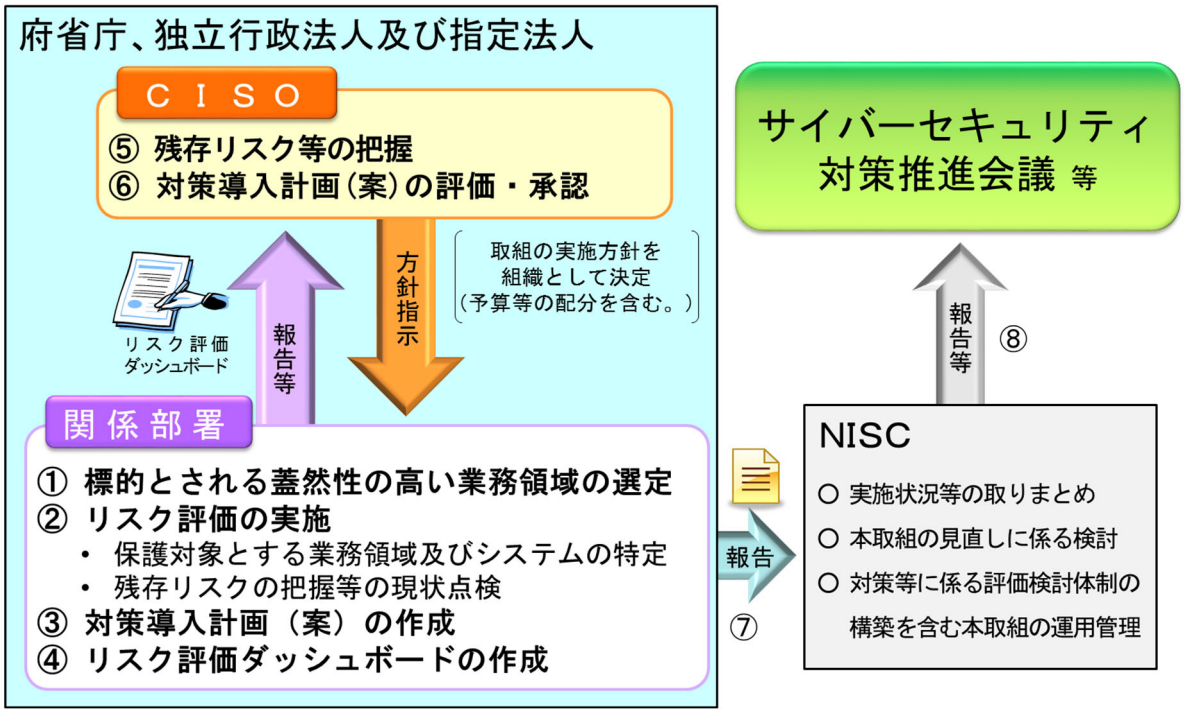
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

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、更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１）。

図表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、独立行政法人及び指定法人（以下「独立行政法人等」という。）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。

2020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、2019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増加しているが、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る。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130の業務領域に使用されているおよそ60の情報システムを対象として、重点的に取組が実施された結果、全てのシステムおいて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。

2020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、2019年度の初年度と比較し、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微減したものの、全体として高度サイバー攻撃への対策は強化され、着実に対策の強化は進められている。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250の業務領域に使用されているおよそ230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ほかに、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が増加している。

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ことから、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・情報にかかるリスク評価を適切に実施し、継続的に多重的な防御の仕組み等を実現するための資源を計画的に投入した対策を推進することが重要である。

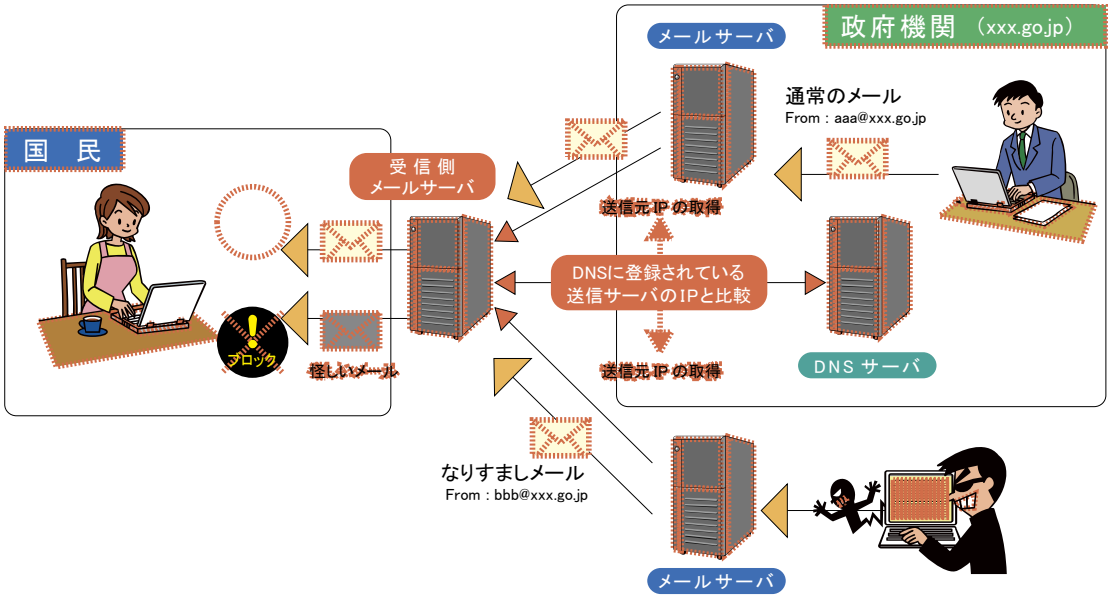
別添４－７　なりすまし防止策の実施状況

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、「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」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（Sender Policy Framework）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１　SPFを活用したなりすまし対策の概要



図表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[3]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。

[3] 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

2018年及び2019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２のとおり。

図表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
2020 年１月末	65.3%	16.5%	18.2%
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。

調査の結果、SPFの設定状況は、１年前と比較して、SPF設定なしも微増に留まり、SPF設定なしの全体に占める割合は横ばいに推移しているおり、全体としてはSPFの導入割合は変化していないが、SPFを適切に設定されていない割合が低下していることがわかった。

これはこの１年間で、政府機関のドメインが微増している中、新規に導入された政府ドメインの内、約半数程度が非推奨設定のドメインとなっている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[4]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(Domain-based Message Authentication, Reporting & Conformance)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(Domainkeys Identified Mail)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。

[4] MX レコード（外部とのメールを中継するメールエクスチェンジャを指定するための情報）が設定されていないドメイン名。

別添４－８　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（2021年３月末日現在）

②　調査時点

独立行政法人、指定法人　2021年３月末日

③　調査内容

統一基準の第２部（情報セキュリティ対策の基本的枠組み）の遵守事項と基本対策事項

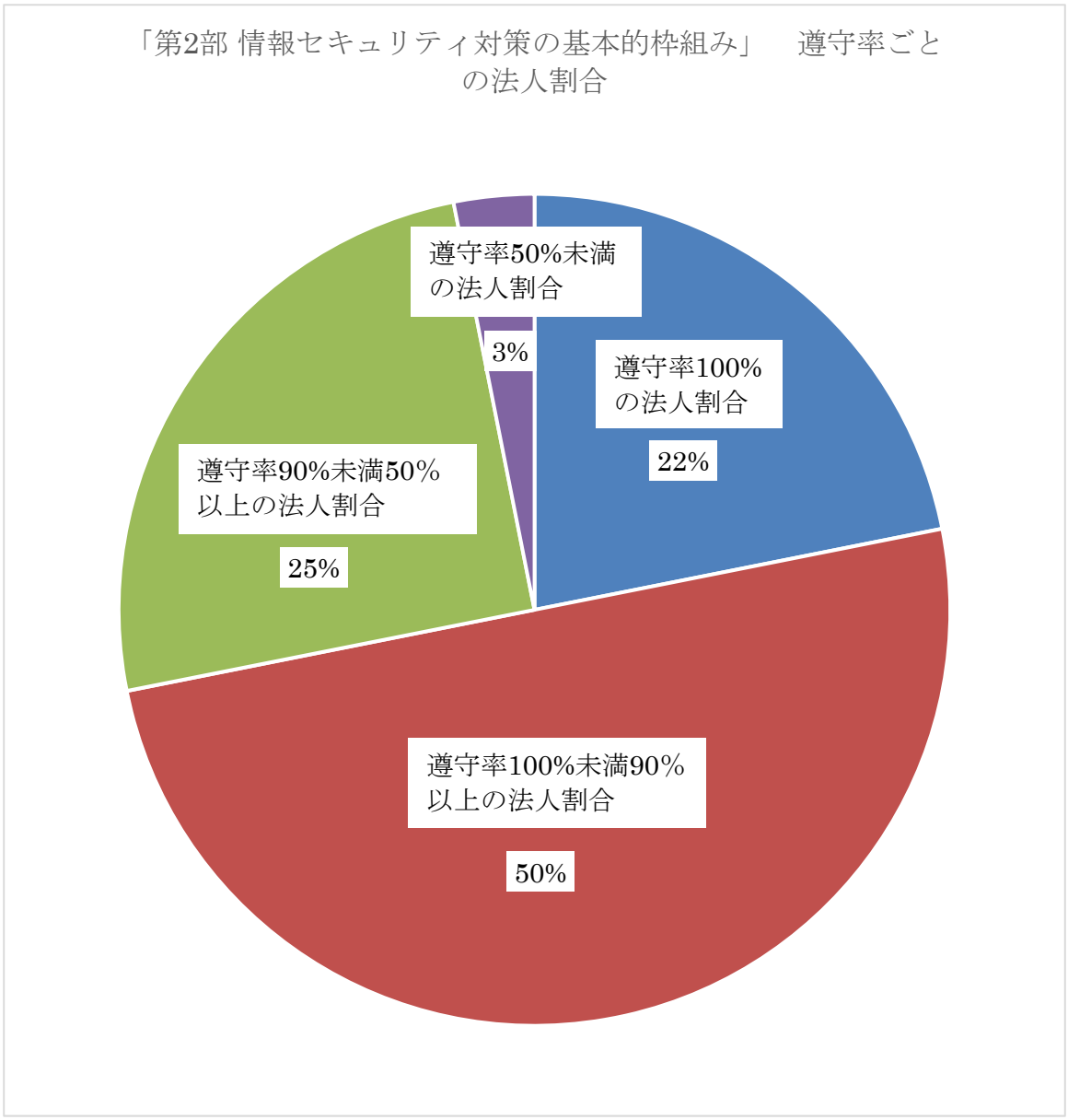
④　その他

統一基準のガイドラインの「第2部 情報セキュリティ対策の基本的枠組み」の遵守率100%とは、そこで要求されている遵守事項および基本対策事項（全160項目）全てを遵守していることを示す。

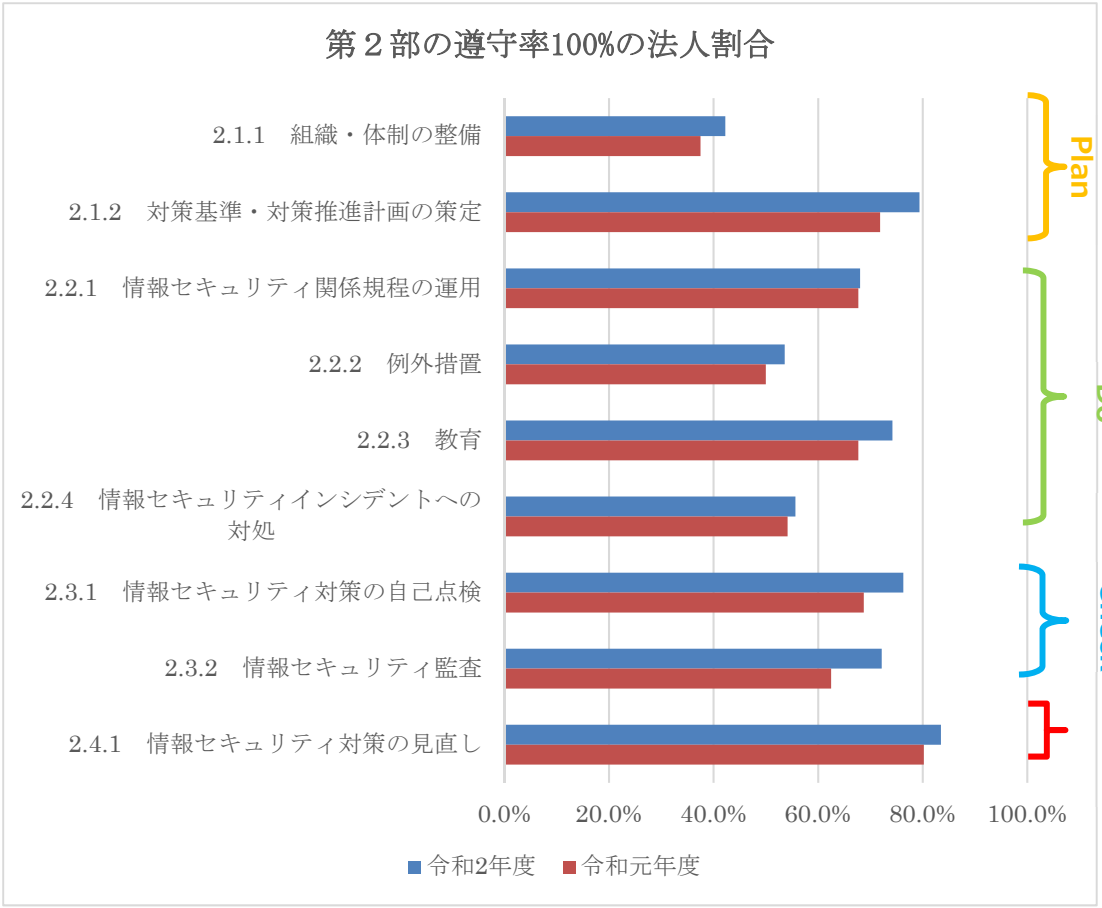
（３）調査結果

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。

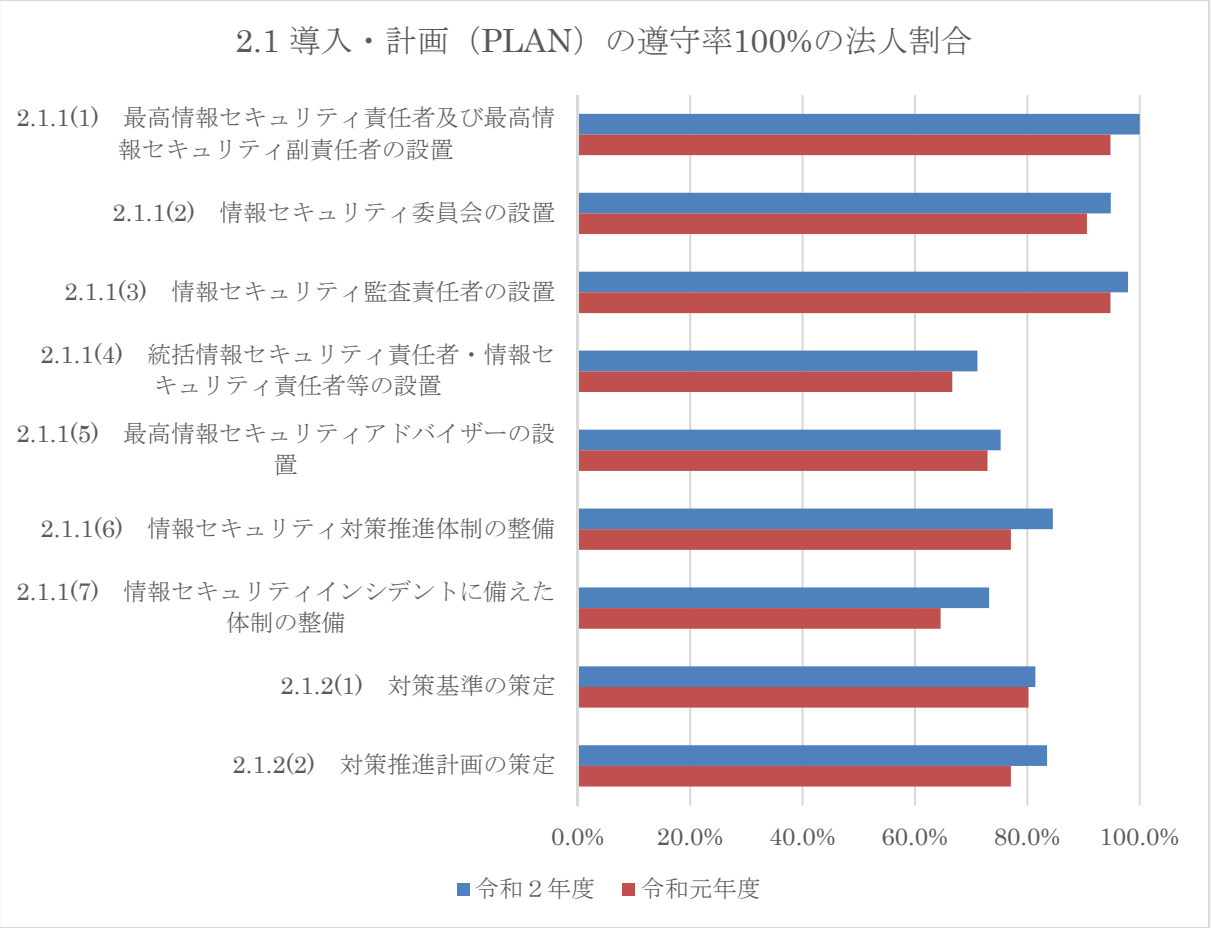


第２部の全てを遵守している法人の項番別の遵守割合については、以下のとおりであり詳細については、次ページ以降に記載する。



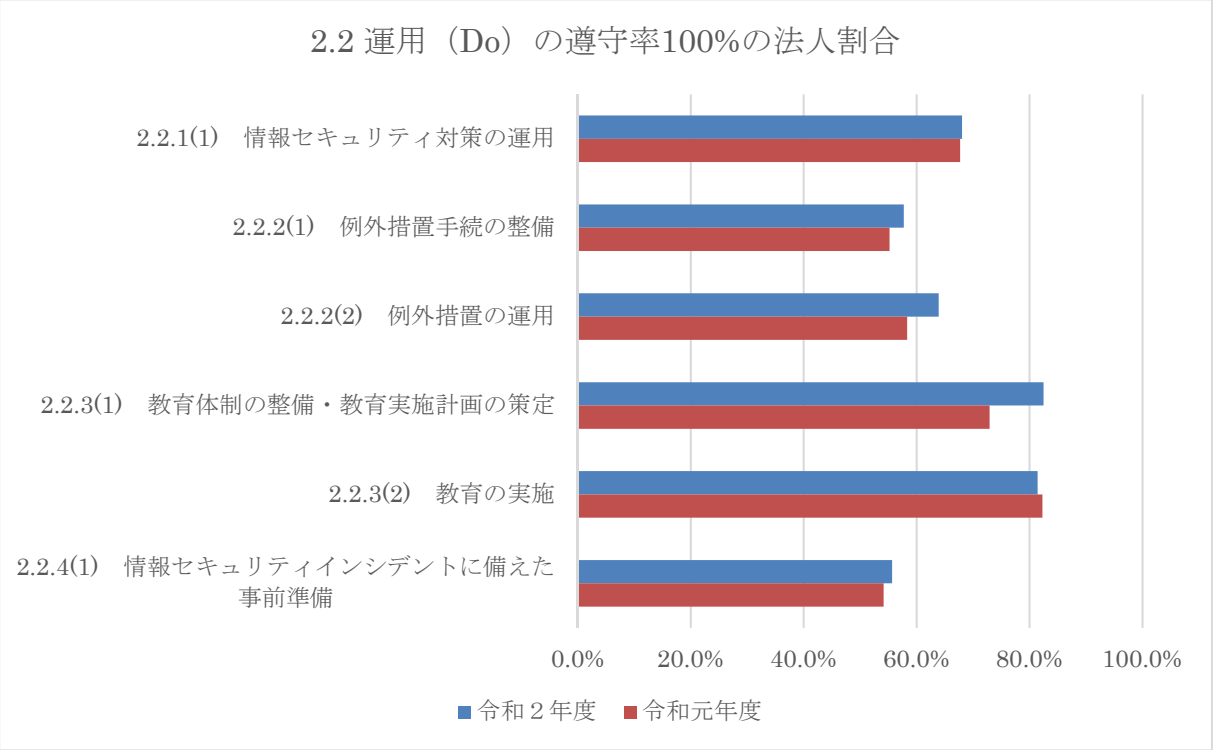
・統一基準の各款の遵守割合では、総じて改善傾向にあり、「2.1.1 組織・体制の整備」の遵守割合が最も低く、続いて「2.2.2 例外措置」、「2.2.4 情報セキュリティインシデントへの対処」の順となった。

①　情報セキュリティ対策の導入・計画



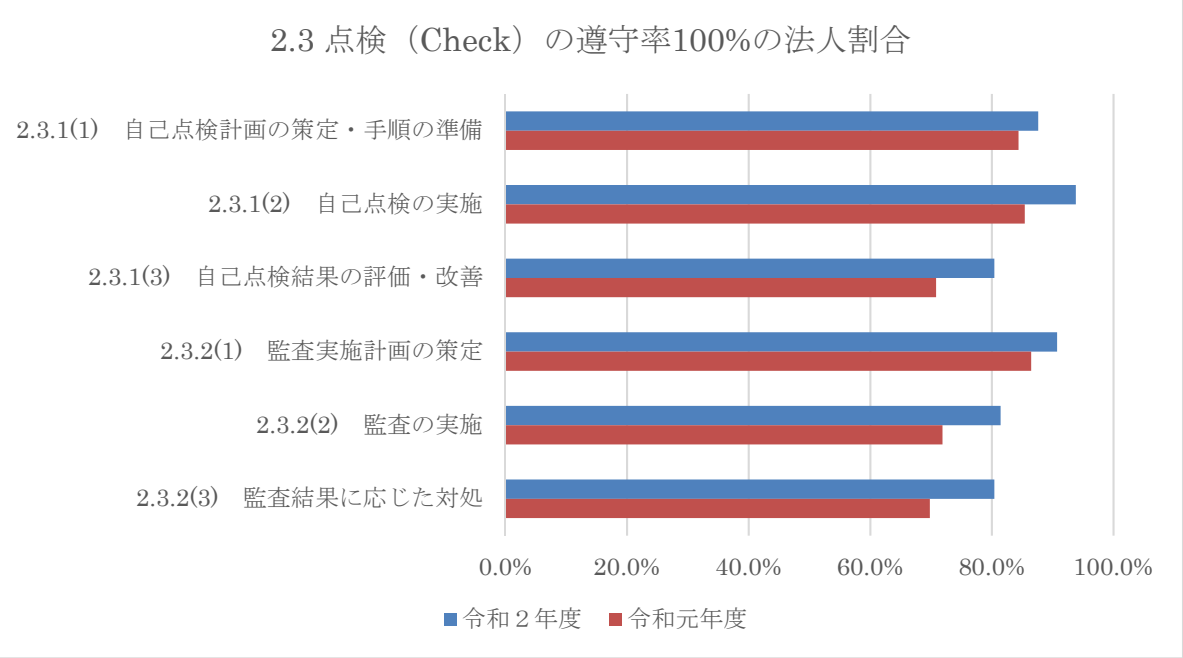
・「2.1　導入・計画」の各条の遵守率 100%の法人割合の伸び率は、総じて改善傾向にあり、「2.1.1(7) 情報セキュリティインシデントに備えた体制の整備」が最も高く、続いて「2.1.1(6)　情報セキュリティ対策推進体制の整備」、「2.1.2(2)　対策推進計画の策定」の順となった。
・「2.1.1(4)　統括情報セキュリティ責任者・情報セキュリティ責任者等の設置」の法人割合が最も低く、続いて「2.1.1(7) 情報セキュリティインシデントに備えた体制の整備」、「2.1.1(5) 最高情報セキュリティアドバイザーの設置」の順となった。

②　情報セキュリティ対策の運用



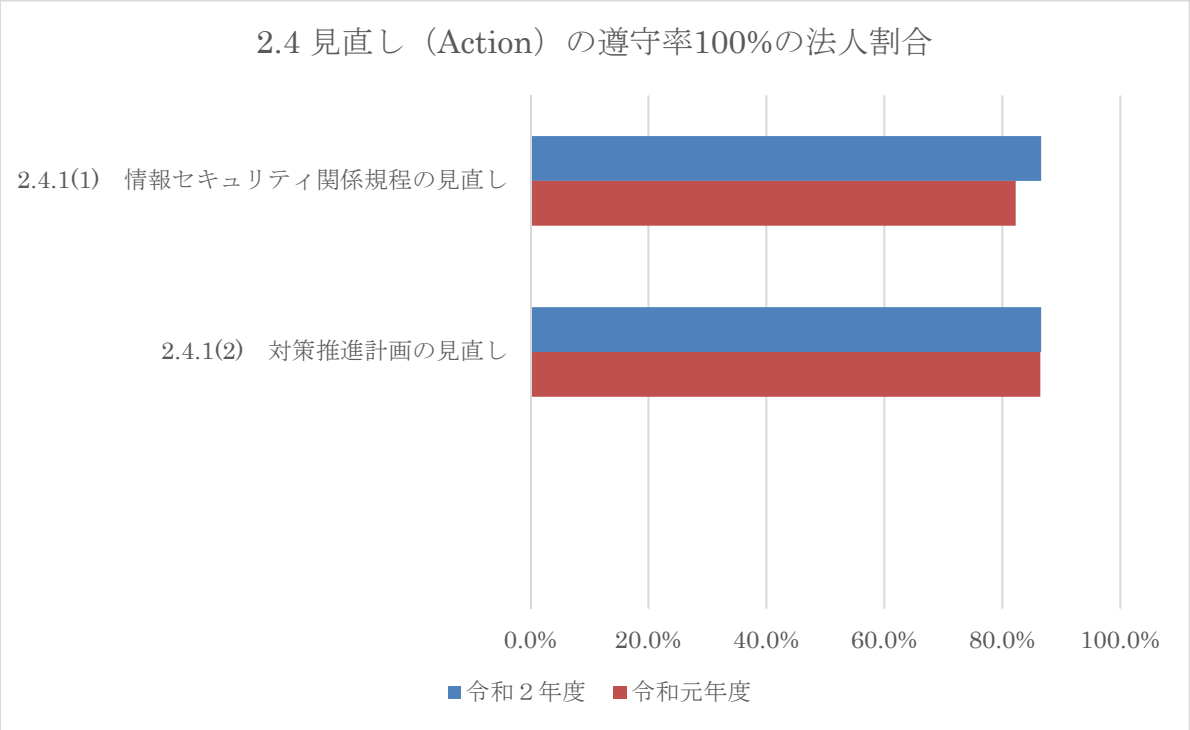
・「2.2 運用」の各条の遵守率 100%の法人割合の伸び率は、総じて改善傾向にあり、「2.2.3(1)　教育体制の整備・教育実施計画の策定」が最も高く、「2.2.2(2)　例外措置の運用」、「2.2.2(1)　例外措置手続の整備」の順となったが、「2.2.3(2)　教育の実施」は、減少した。
・「2.2.4.(1) 情報セキュリティインシデントに備えた事前準備」の法人割合が最も低く、続いて「2.2.2.(1) 例外措置手続の整備」、「2.2.2.(2) 例外措置の運用」の順となった。

③　情報セキュリティ対策の点検



・「2.3 点検」の各条の遵守率 100%の法人割合の伸び率は、総じて改善傾向にあり、「2.3.2(2)　監査の実施」が最も高く、続いて「2.3.1(3)　自己点検結果の評価・改善」、「2.3.2(3)　監査結果に応じた対処」の順となった。
・「2.3 点検」の各条の遵守率 100%の法人割合の「2.3.1(3)　自己点検結果の評価・改善」と「2.3.2(3)　監査結果に応じた対処」の法人割合が最も低く、続いて「2.3.2(2)　監査の実施」の順となった。

④　情報セキュリティ対策の見直し



・「2.4 見直し」の各条の遵守率 100%の法人割合の伸び率は、「2.4.1.(1) 情報セキュリティ関係規程の見直し」は増加したものの、「2.4.1(2)　対策推進計画の見直し」は微増であった。

（４）各法人及び所管府省庁の対応

今回、独立行政法人等を対象に、「情報セキュリティ対策の基本的枠組み」に関する遵守事項および基本対策事項の遵守状況の調査を行った。独立行政法人等の情報セキュリティ対策の現状を表す遵守率は総じて改善が見られるものの分布をみると、遵守率 90%以上の法人の割合は約 70%であり（うち遵守率 100%の法人は約 20%）、おおよその法人の情報セキュリティ対策水準は維持されていると推察する。一方、遵守率 50%未満の法人の割合は３%であった。また、全体では、「2.4.1　情報セキュリティ対策の見直し」の取り組みが進んでおり、「2.1.1 組織・体制の整備」については、遵守率が低かった。

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 法人
・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 法人

②　調査時点

2021 年３月末日現在

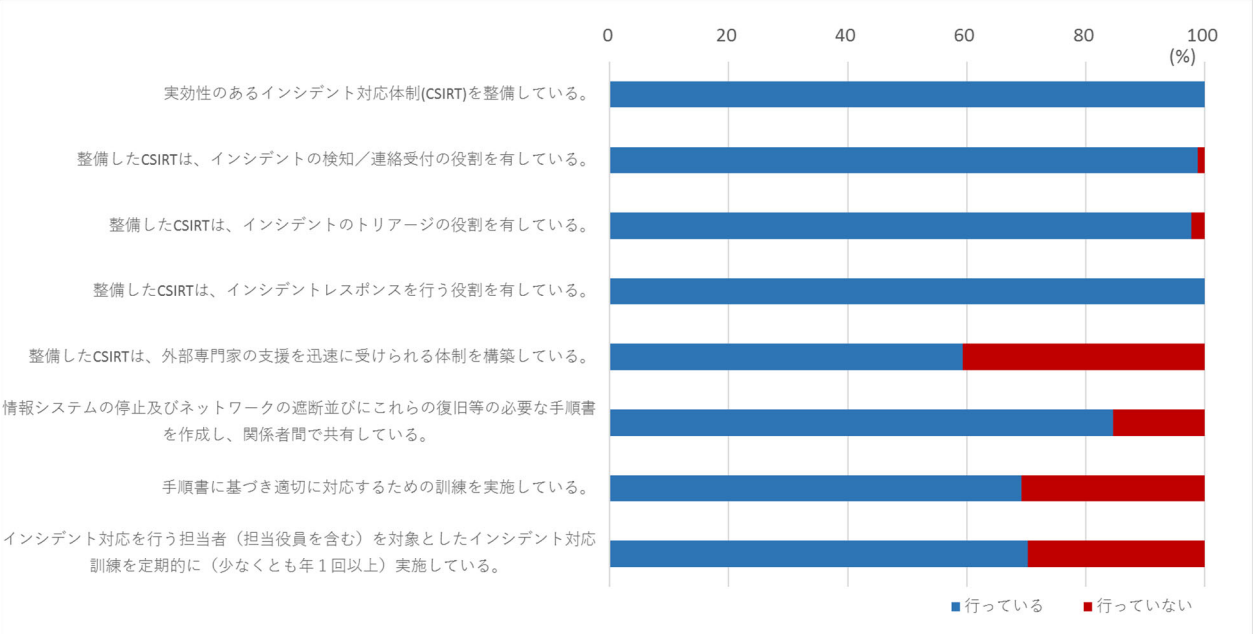
③　調査内容

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



②

・調査対象法人 91 法人の全法人において 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法人は 90 法人（約 99%）、インシデントのトリアージの役割を有している法人は 89 法人（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 法人（100%）である。

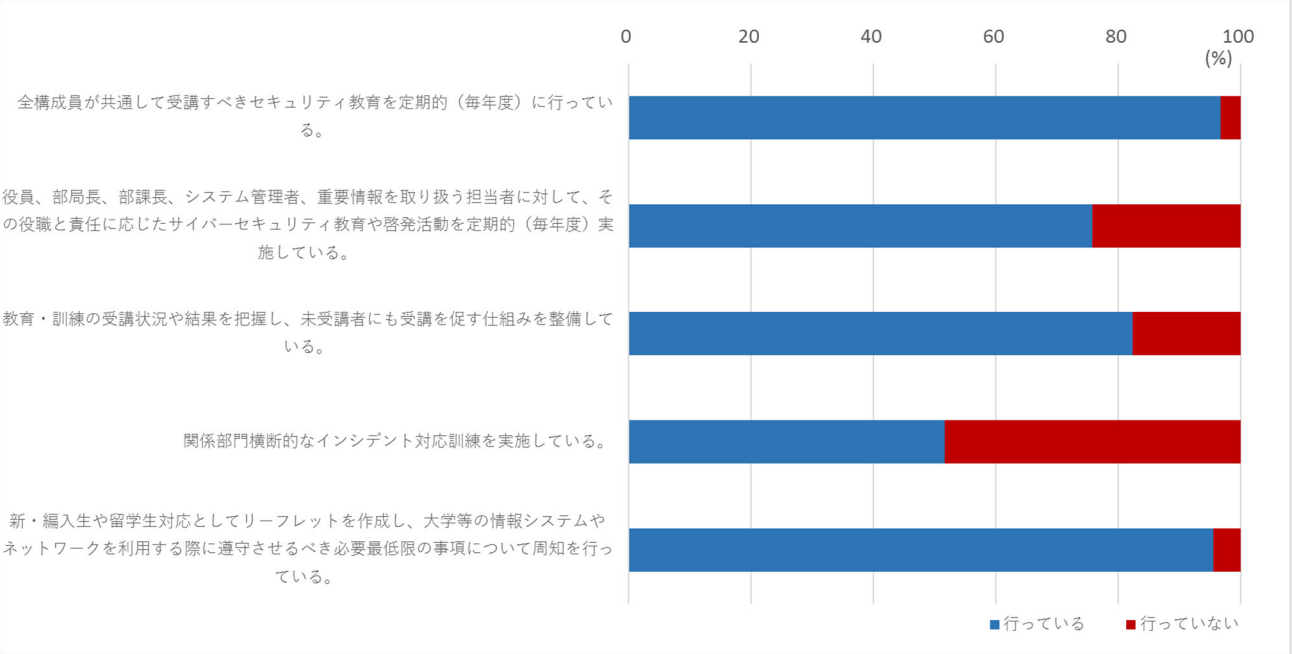
・外部専門家の支援を迅速に受けられる体制を構築している法人は 54 法人（約 59%）である。

・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法人は 77 法人（約 85%）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法人は 63 機関（約 69%）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に実施している法人は 64 法人（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）に行っている法人は 88 法人（約 97%）である。

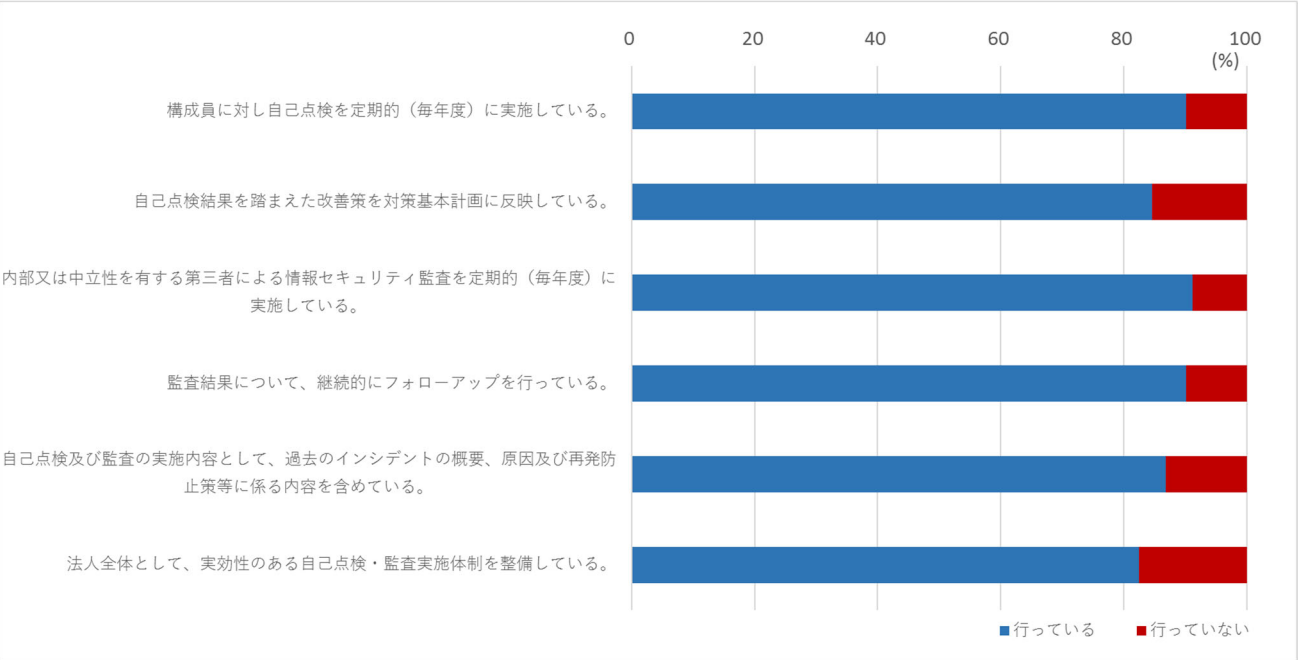
・役員、部局長、部課長、システム管理者、重要情報を取り扱う担当者に対して、その役職と責任に応じたサイバーセキュリティ教育や啓発活動を定期的（毎年度）実施している法人は 69 法人（約 76%）である。

・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法人は 75 法人（約 82%）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法人は 47 法人（約 52%）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法人は 87 法人（約 96%）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）に実施している法人は 82 法人（約 90%）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法人は 77 法人（約 85%）である。

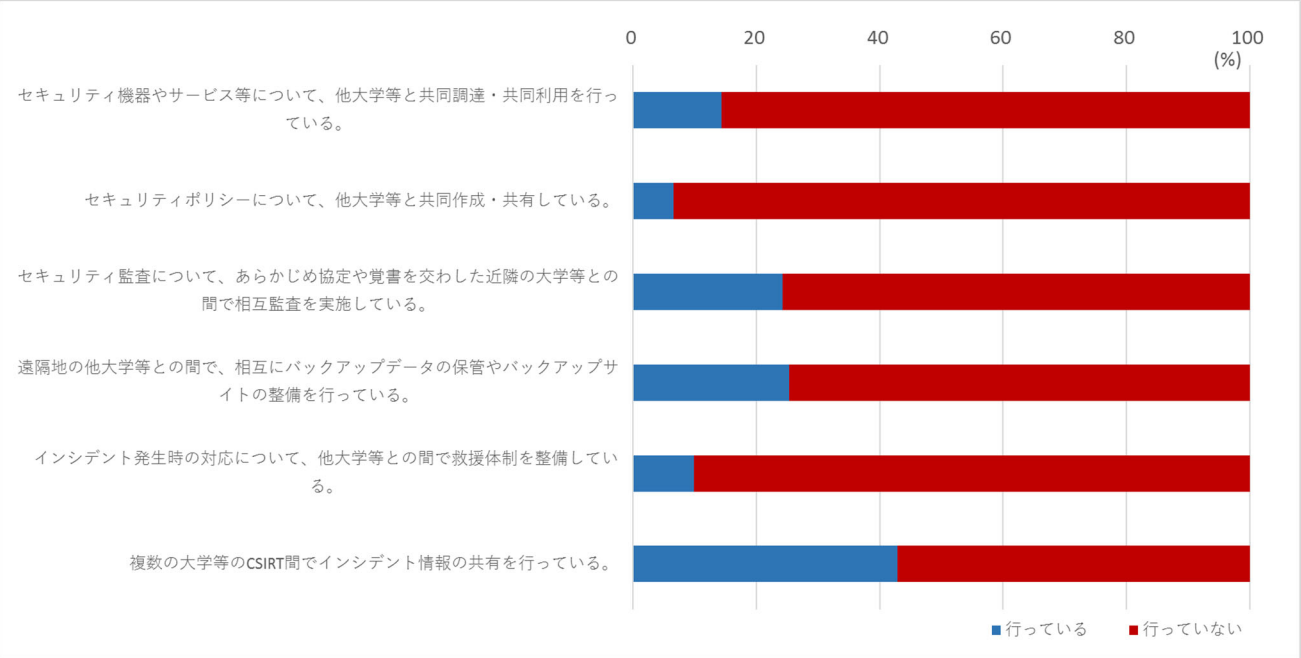
・内部又は中立性を有する第三者による情報セキュリティ監査を定期的（毎年度）に実施している法人は 83 法人（約 91%）である。

・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法人は 82 法人（約 90%）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法人は 79 法人（約 87%）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法人は 75 法人（約 82%）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法人は 13 法人（約 14%）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・共有している法人は 6 法人（約 7%）である。

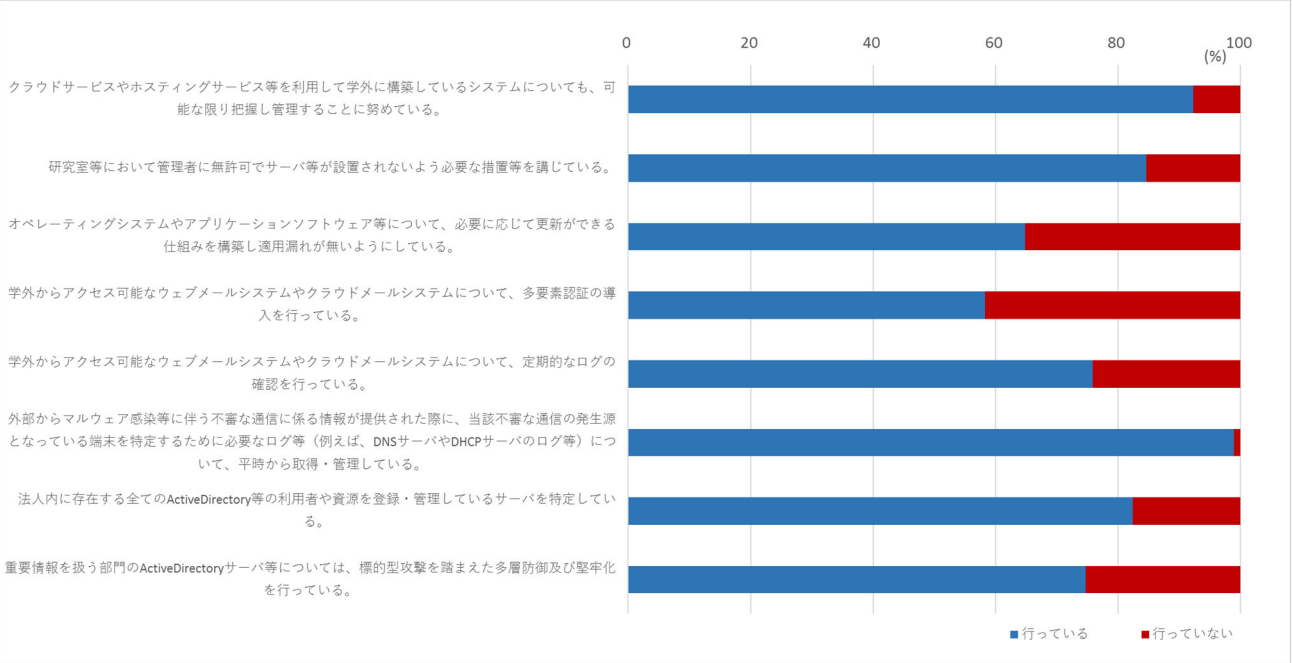
・セキュリティ監査について、あらかじめ協定や覚書を交わした近隣の大学等との間で相互監査を実施している法人は 22 法人（約 24%）である。

・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法人は 23 法人（約 25%）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法人は 9 法人（約 10%）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法人は 39 法人（約 43%）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法人は 84 法人（約 92%）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法人は 77 法人（約 85%）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法人は 59 法人（約 65%）である。

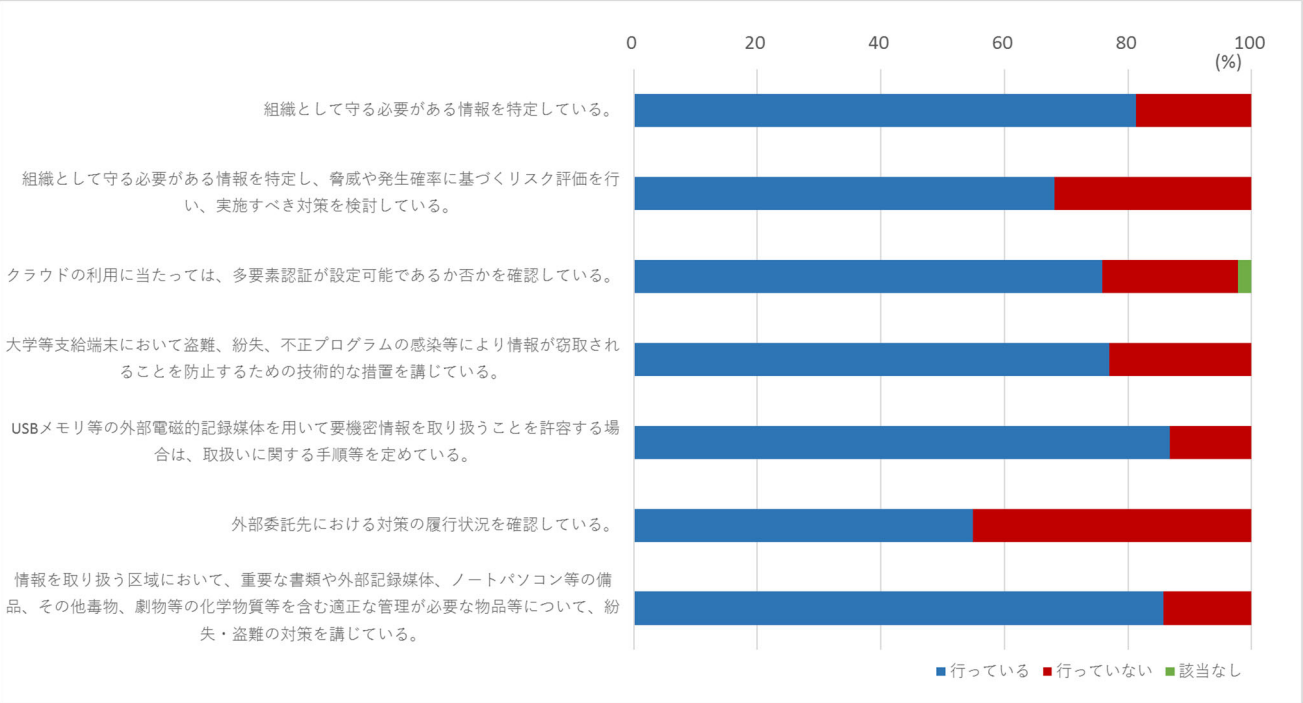
・学外からアクセス可能なウェブメールシステムやクラウドメールシステムについて、多要素認証の導入を行っている法人は 53 法人（約 58%）であり、また、定期的なログの確認を行っている法人は 69 法人（約 76%）である。

・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・管理している法人は 90 法人（約 99%）である。

・法人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法人は 75 法人（約 82%）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法人は 68 法人（約 75%）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法人は 74 法人（約 81%）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法人は 62 法人（約 68%）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法人は 69 法人（約 76%）である。

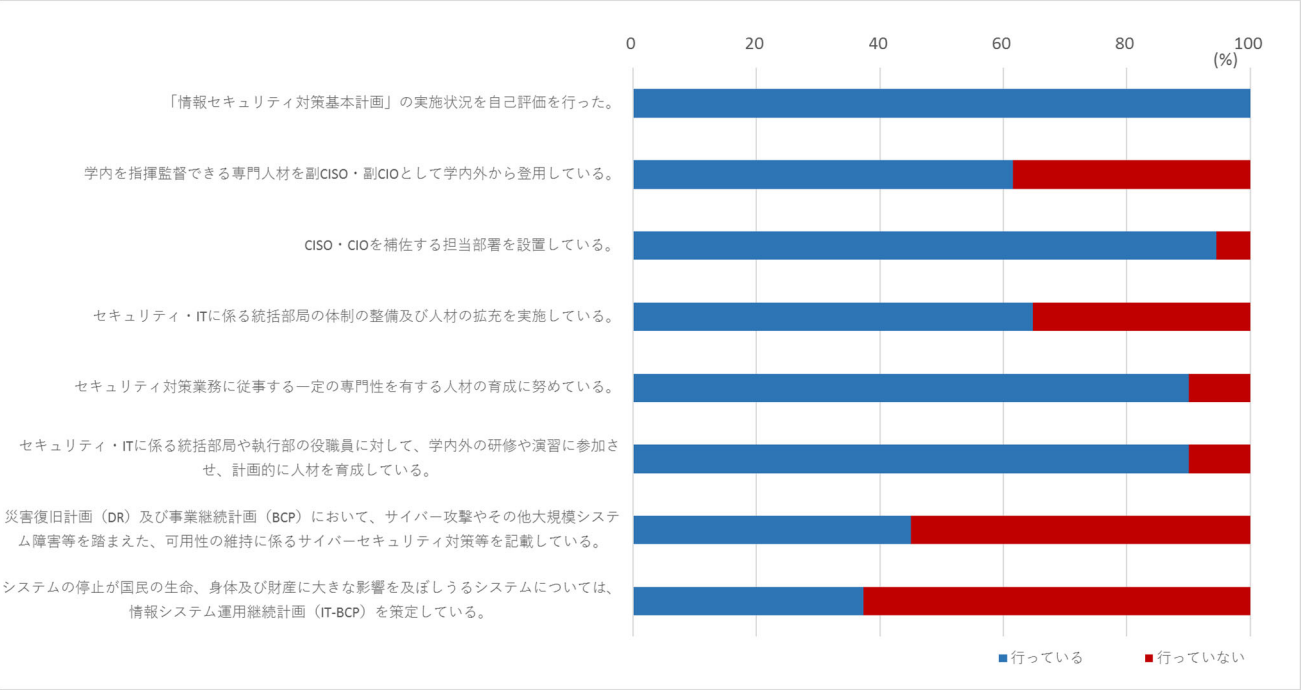
・大学等支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置を講じている法人は 70 法人（約 77%）である。

・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法人は 79 法人（約 87%）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法人は 50 法人（約 55%）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法人は 78 法人（約 86%）である。

⑦　国立大学法人等が対応すること



・全法人において「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ている。

・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法人は 56 法人（約 62%）である。

・CISO・CIO を補佐する担当部署を設置している法人は 86 法人（約 95%）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法人は 59 法人（約 65%）である。

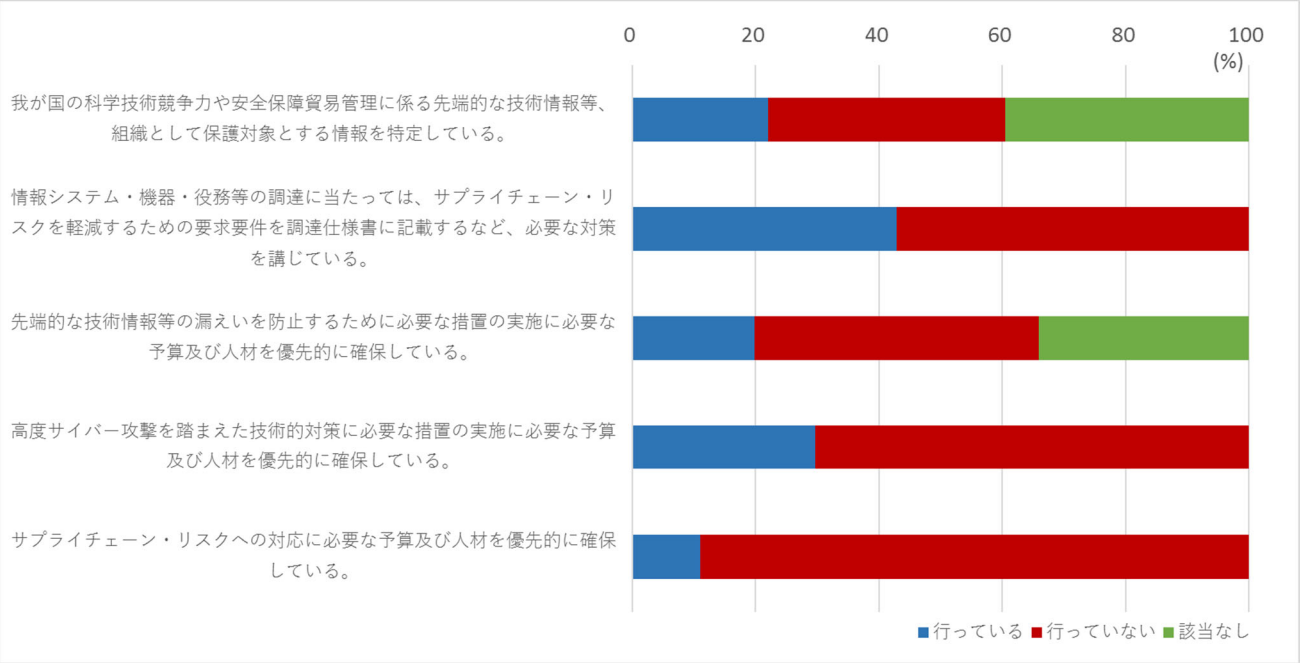
・セキュリティ対策業務に従事する一定の専門性を有する人材の育成に努めている法人は 82 法人（約 90%）である。

・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法人は 82 法人（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法人は 41 法人（約 45%）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）を策定している法人は 34 法人（約 37%）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法人は 20 法人（約 22%）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法人は 39 法人（約 43%）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法人は 18 法人（約 20%）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法人は 27 法人（約 30%）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法人は 10 法人（約 11%）である。

（４）各法人の対応

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、ごく一部の法人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、全法人必須の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に実施している法人は７割程度に留まった。訓練を実施していない法人については、訓練の実施、既に実施している法人については、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法人は９割程度であった。自己点検や監査は各法人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、全ての法人での実施が求められる。自己点検や監査を実施するにあたっては、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法人の構成員に引き継がれるようにすること、また、監査の実施内容として、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。

各法人においては、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、各法人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法人においては、これらの情報の窃取を目的としたサイバー攻撃の対象となり易いことについて認識しておく必要があり、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、各法人が教育、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を取れた対策の実施、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 2020 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
2020 年	５月	【概要】厚生労働省は５月 20 日、職業安定局所管の「雇用調整助成金等オンライン受付システム」に不具合が発生し、運用を停止したことを公表した。６月５日に運用を再開したが、同日、システムの不具合により、申請を行った事業者の添付書類が他の事業者（計 10 社）に閲覧可能となる事案が判明し、再度運用を停止した。その後、以下の対応を経て８月 25 日に稼働した。 【対応等】外部専門家による、厚生労働省及び受託者を対象としたプロジェクト管理を含むシステム監査を実施し、今回の事案が生じた原因の徹底的な究明を行い、その結果を踏まえ、必要な対応を行うこととした。	意図せぬ情報流出
	６月	【概要】原子力規制庁は６月２日、職員の在宅勤務用の個人メールアドレスを誤って登録したことにより、同庁から情報共有するために送信したメールが、４月 10 日から 48 通、第三者に送信されていたことを公表した。 【対応等】個人情報等を含む文書を送信する際は、暗号化やパスワード保護等を行うことを周知したほか、今後、庁内の情報セキュリティ研修においても指導を改めて徹底することとした。	意図せぬ情報流出
		【概要】国際協力機構は６月 12 日及び 30 日、「アフリカの若者のための産業人材育成イニシアティブ『修士課程及びインターンシップ』プログラム（ABE イニシアティブ）」の運営業務を委託している一般財団法人日本国際協力センター（JICE）が開発・運用している「ABE イニシアティブポータルサイト」に、第三者から不正なアクセスがあり、情報の一部が不正閲覧されたことを公表した。	外部からの攻撃
	７月	【概要】科学技術・学術政策研究所は７月１日、同所が構築・運営している博士人材データベースの登録者の一部の 1,497 名に対して委託先の運営事業者がメールを送信する際、同 1,497 名のメールアドレスがメール本文に記載される形で送信されてしまったことを公表した。 【対応等】当該メールの送信後 12 時間内に受信者に対して、謝罪するとともにメールを削除するよう連絡した。 後日、当該メールの受信者および博士人材データベースの関係者に当該インシデントの調査結果と再発防止策を伝達した。	意図せぬ情報流出
		【概要】石油天然ガス・金属鉱物資源機構は７月３日、５月の外国送金において、なりすましメールによって同機構が偽の請求書を受領し、当該請求書に記された指定口座へ送金していたことを公表した。	その他
		【概要】横浜国立大学は７月 10 日、教員が大学アカウントの受信メールをバックアップ用としてプライベートメールに自動転送をしていたところ、転送先で不正アクセスに遭い、一部のメールが第三者に閲覧された可能性があることを公表した。	外部からの攻撃
		【概要】公正取引委員会は７月 21 日、同委員会が実施している事業者に対する Web アンケートにおいて、一部の事業者が回答した内容が他の事業者に閲覧可能な状態になっていた可能性があることを公表した。 【対応等】更に十分に注意を払った上で事前のテストを実施させるなど、再発防止に取り組むこととした。	意図せぬ情報流出
	８月	【概要】日本芸術文化振興会は８月７日、同会ウェブサイトにおいて、外部からの不正アクセスにより、国立劇場メールマガジン登録者のメールアドレスの内 54,445 件が流出したことを公表した。	外部からの攻撃
		【概要】環境省は８月 11 日、石綿健康被害判定小委員会の委員が資料一式（紙媒体及び電子データを保存したハードディスク）を持参して帰宅する途中、当該資料一式を電車内に置き忘れて 紛失したことを公表した。 【対応等】「判定小委員会及び審査分科会で用いる資料の取扱いについて」を判定小委員会で定め、判定小委員会及び審査分科会における資料管理を一層徹底した。	その他
		【概要】名古屋大学は８月 24 日、医学部保健学科の教員が、学生の個人情報が保存された USB メモリ２本を紛失したことを公表した。	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】岡山大学は８月 26 日、同大学メールサービス利用者１名のメールパスワードが窃取され、８月 24 日に学外からの不正アクセスにより当該利用者のメールアドレスから約 2,000 件の迷惑メールが送信されたことを公表した。	外部からの攻撃
	９月	【概要】高齢・障害・求職者雇用支援機構は９月 18 日、機構関係者のパソコンがマルウェアに感染した疑いがあり、一部利用者に大阪支部高障業務課や 65 歳超雇用推進プランナー・高年齢者雇用アドバイザー等を騙ったマルウェア付きの電子メールが送信されるおそれがあることを注意喚起した。	外部からの攻撃
	10 月	【概要】内閣官房オリパラ事務局は 10 月６日、事務局の担当者が外部にメールを送付した際、送付先メールアドレスを誤って Bcc ではなく To で送信したことを公表した。 【対応等】メール誤送信防止機能及びその運用について局内に改めて周知徹底を図り、その上で、必要に応じ、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。	意図せぬ情報流出
		【概要】岡山大学は 10 月８日、同大学が研究室ウェブサイトの公開用に借用している外部クラウドサーバにおいて、同大学のアカウントを利用して大量のフィッシング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】総務省は 10 月 15 日、同省を騙るメールアドレスから、「二回目特別定額給付金の特設サイトを開設した」という偽の特設サイトに誘導するリンクが含まれたメールが送信されているとの情報が寄せられたことを公表した。 【対応等】特別定額給付金について、政府からメールなどでお知らせをすることはなく、上記以外のメールアドレスから総務省や行政機関を名乗ったメールが届いたとしても、情報の詐取などを目的としたものと考えられるとの注意喚起を実施した。	その他
		【概要】原子力規制庁は 10 月 27 日、同庁内からのメール送受信が不可となっていることをウェブサイト上で公表し、28 日の定例記者会見において、不正アクセスを受けたことを公表した。	外部からの攻撃
		【概要】土木研究所は 10 月 28 日、外部から職員１名のメールアドレスを偽装した約２万９千件の英文迷惑メールが送信されていたことを公表した。	外部からの攻撃
	11 月	【概要】国家公務員共済組合連合会虎の門病院は 11 月 13 日、第三者からの不正アクセスを受け、同院ウェブサイトが閲覧ができない状態になったことを公表した。	外部からの攻撃
		【概要】公正取引委員会は 11 月 26 日、電子メールを一斉送信する際に、同報者の電子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】職員に対する個人情報保護の重要性についての教育及び管理体制の更なる強化に取り組み、再発防止に努めることとした。	意図せぬ情報流出
		【概要】厚生労働省は 11 月 27 日、ハローワークシステムの機器更改を実施した際に委託業者によって撤去された旧サーバのバックアップ媒体を紛失したことを公表した。 【対応等】バックアップ媒体にデータが記録されていた者の特定作業を進め、連絡が可能な者に報告、謝罪し、再発防止に向けて手順書等の見直しを行った。	その他
		【概要】総務省関東総合通信局は 11 月 27 日、ケーブルテレビ事業者 55 社に対してメールを送信する際、公にしないとの条件でケーブルテレビ事業者３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て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。分かりやすいファイル名を用いることや公表の可否に応じて保存するフォルダを分けることなどについても徹底することとした。	意図せぬ情報流出

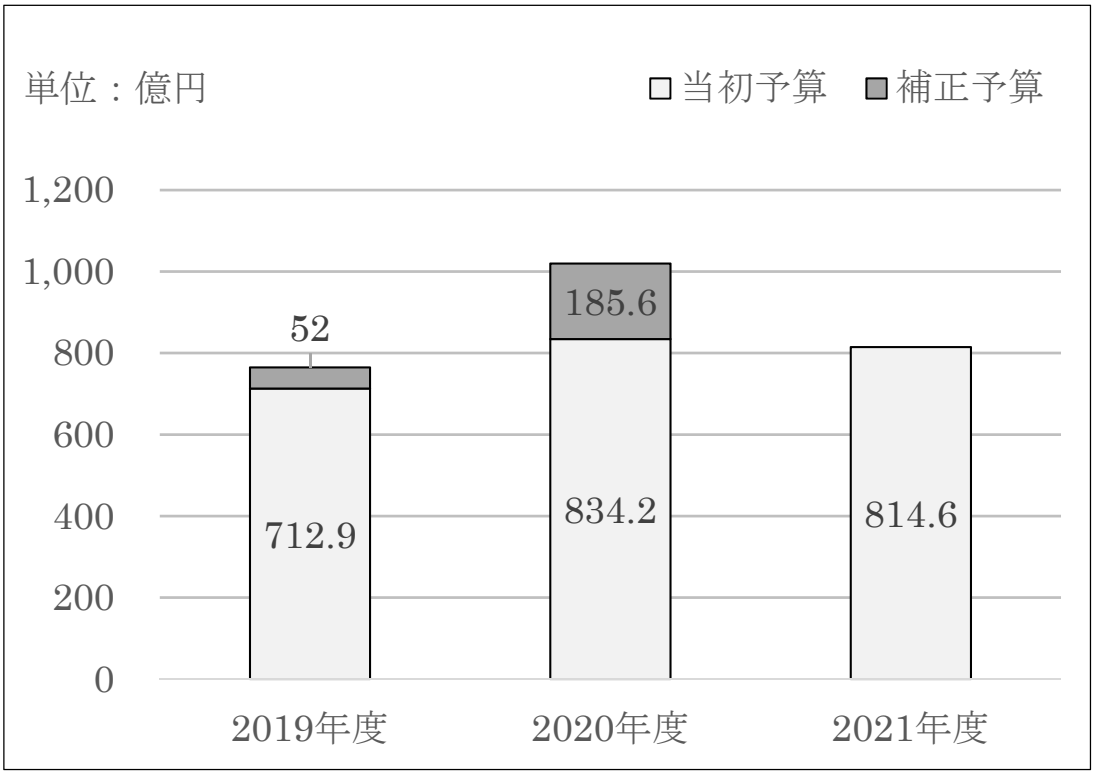
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
	12 月	【概要】大阪大学は 12 月９日、同大学の学内宿泊施設予約システム（RRS）のサーバに対し、学外から不正なアクセスがあり、RRS 利用者の個人情報が漏えいした可能性があることを公表した。	外部からの攻撃
		【概要】物質・材料研究機構は 12 月９日、職員１名のメールアカウントが部外者に不正に利用され、4,158 通の迷惑メールが送信されたことを公表した。	外部からの攻撃
		【概要】日本医療研究開発機構は 12 月 11 日、同機構で使用している人事関係システムにおいて、保守業者による保守作業中、保守用端末に対して不正なアクセスがあり、同機構の役職員、派遣職員及び退職者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
		【概要】年金積立金管理運用独立行政法人は 12 月 23 日、同法人職員が新聞記者などのメディアに対してメールを送信する際、メールアドレスを誤って Bcc ではなく To で送信したことを公表した。	意図せぬ情報流出
2021 年	１月	【概要】愛媛大学は１月４日、同大学学部用メールサービス利用者２名のメールアカウントとパスワードが学外者に不正に利用され、約 35,000 通の迷惑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】労働者健康安全機構東京労災病院は１月７日、患者の個人情報を保存した USB メモリを紛失したことを公表した。	その他
		【概要】国立成育医療研究センターは１月 13 日、「小児医療情報収集システム」に不正アクセスがあったことを公表した。	外部からの攻撃
		【概要】国際観光振興機構は１月 21 日、クラウド型情報管理システム内の情報の一部が第三者からアクセスしうる状態であったことを公表した。	その他
	２月	【概要】広島大学病院は２月２日、臨床検査技師が患者 59 人分の個人情報を保存した USB メモリを紛失したことを公表した。	その他
		【概要】東京芸術大学は２月 19 日、教員のノート PC 及び受験生から提出された受験関係書類が、保管していた学内研究室から盗まれたことを公表した。	その他
		【概要】公正取引委員会は２月 26 日、過去のアンケートで収集した個人情報が含まれる電子ファイルを、外部の２団体及び１事業者に対して電子メールで送信していたことを公表した。 【対応等】実効的な措置を講じるとともに、職員に対する個人情報保護の重要性についての教育及び管理体制の更なる強化に取り組むこととした。	意図せぬ情報流出
	３月	【概要】工業所有権情報・研修館は３月３日、委託先事業者の PC１台がマルウェアに感染し、個人情報（氏名やメールアドレス等）が外部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】国際協力機構は３月 16 日、同機構が運営する国際キャリア総合情報サイト「PARTNER」で利用している外部のクラウド型システムに対し、第三者から不正なアクセスがあり、情報の一部が不正閲覧されたことを公表した。	外部からの攻撃
		【概要】海洋研究開発機構は３月 16 日、職員になりすました VPN 接続による基幹ネットワークシステムへの不正アクセスがあったことを公表した。	外部からの攻撃
		【概要】名古屋大学は３月 30 日、医学部附属病院の教員が、ヘルプデスクを装った不審なメールに記載された URL にアクセスし、同大学のメールアドレス及びそのパスワードを入力したことにより、これらの情報が不正に第三者に取得され、個人情報が含まれる電子メールを閲覧された可能性があることを公表した。	外部からの攻撃

※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、公表内容を元に対応等を記載。

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

	2019 年度	2020 年度	2021 年度
当初予算額	712.9 億円	834.2 億円	814.6 億円
補正予算額	52 億円	185.6 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。



（本ページは白紙です。）

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

「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」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、ＰＤＣＡのうちＣＡ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（ＩＴ）に限らず、制御系（ＯＴ）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（ＩＳＡＣ※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

■ 上記先導的な取組みの、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ＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ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

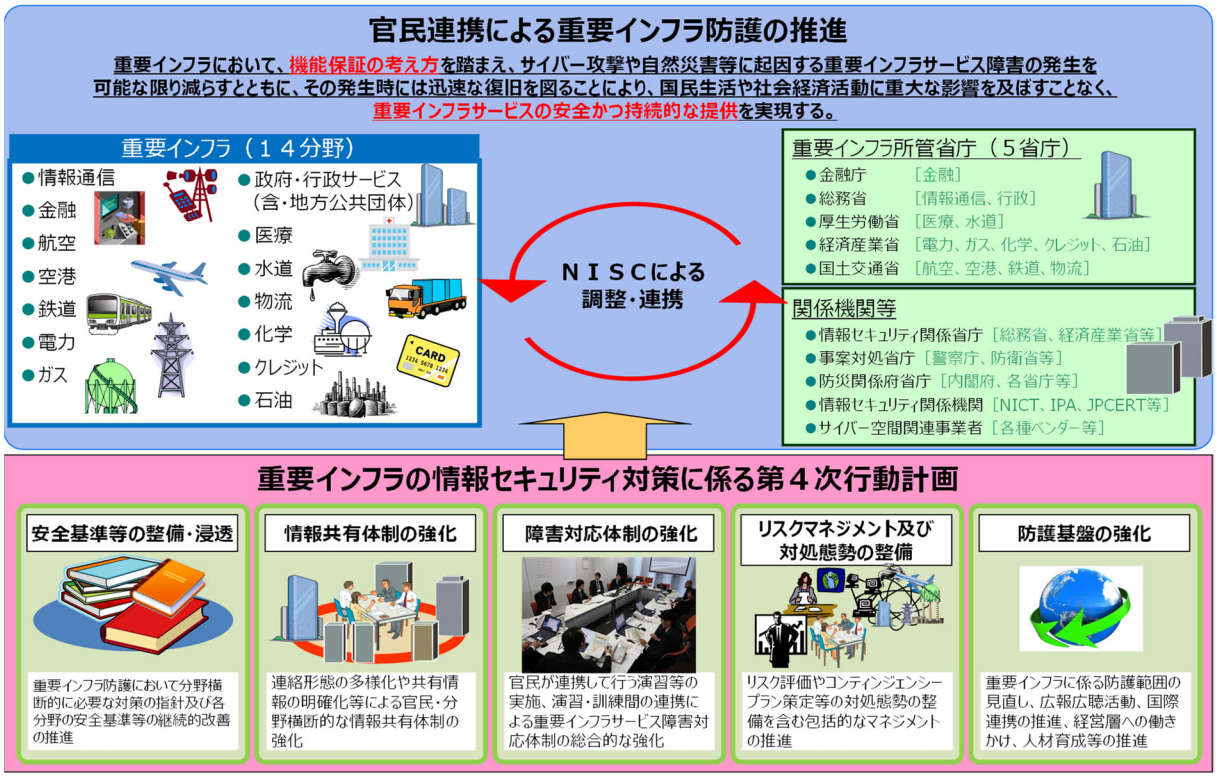
■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 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、官民が一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

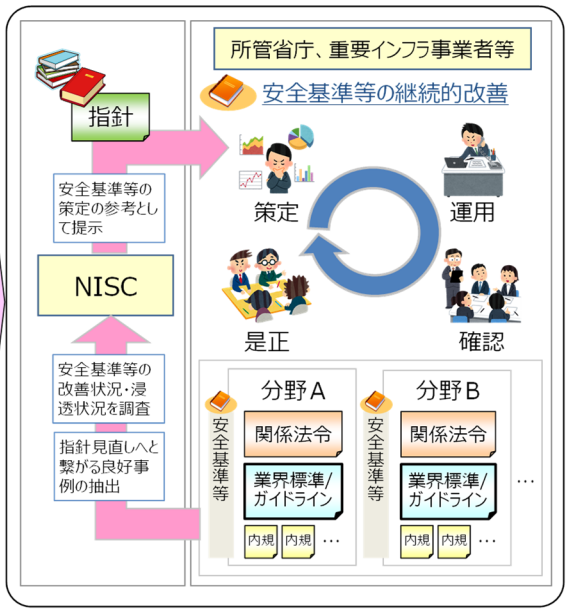
行動計画期間中の施策

（１）　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

（２）　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

（３）　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



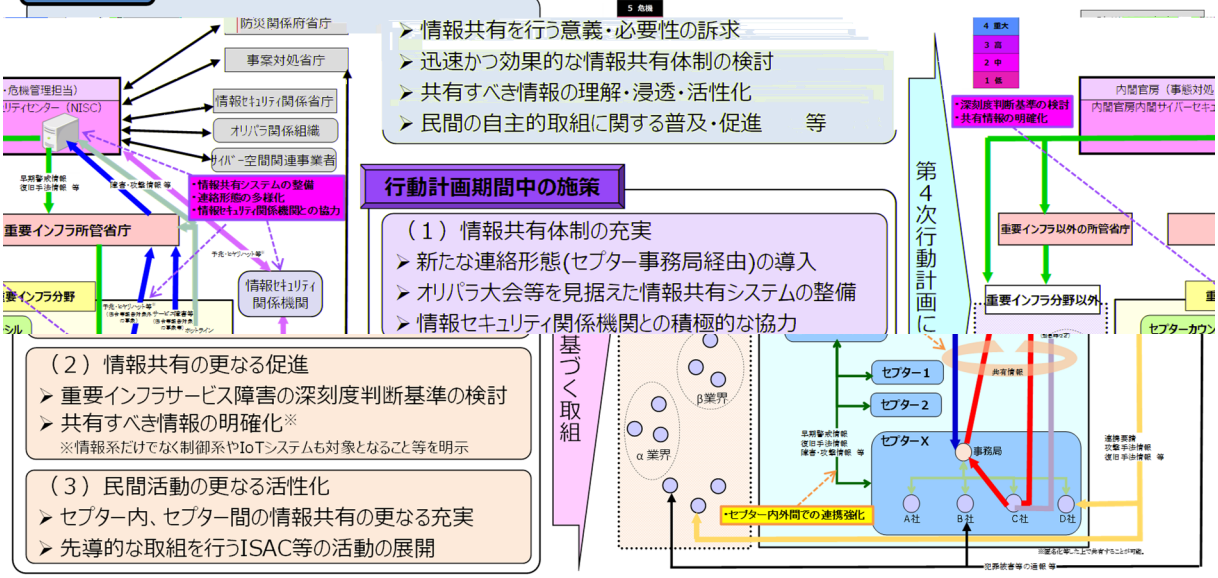
第４次行動計画　施策②：情報共有体制の強化

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

【本行動計画期間で取り組む情報共有体制】



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次行動計画に基づく取組

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

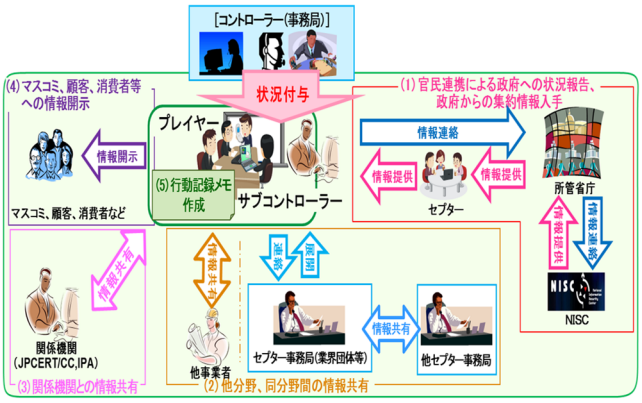
行動計画期間中の施策

（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画

（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

第４次行動計画に基づく取組

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

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。

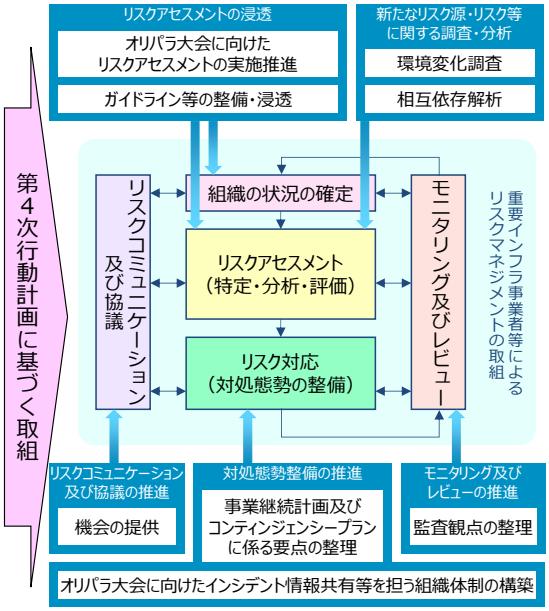
行動計画期間中の施策

（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

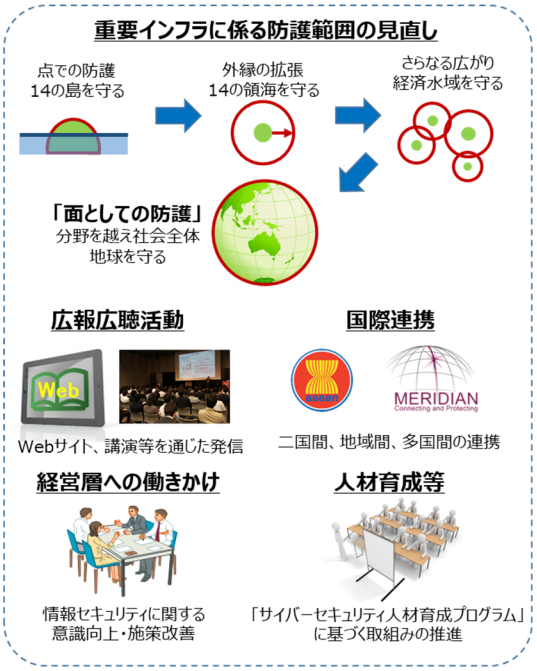
（１）重要インフラに係る防護範囲の見直し
- 「面としての防護」に向けた取組、国の安全等の確保の観点からの取組

（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

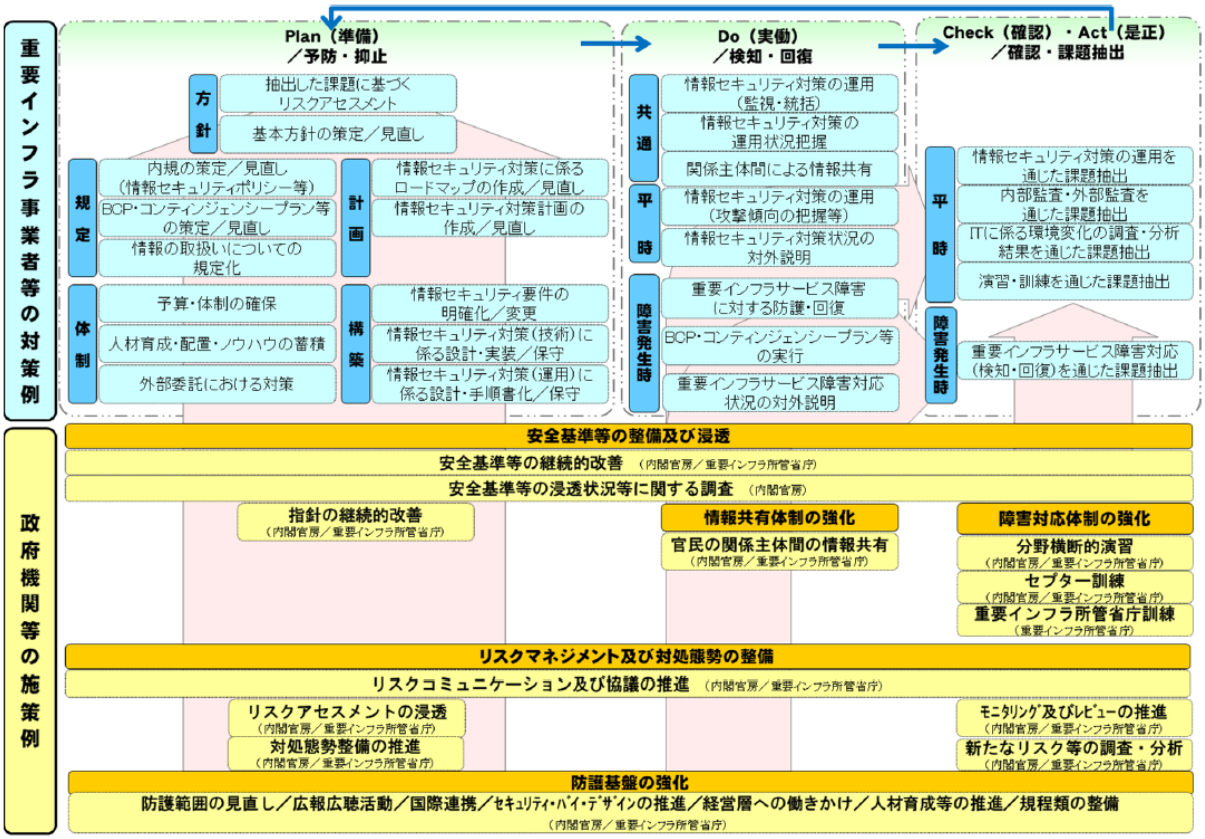
（３）国際連携の推進
- 国際的な情報セキュリティ対策の水準向上のための積極的な寄与

（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、2020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）。

(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。

2020年度は、2019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2019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次行動計画に基づく積極的な取組を引き続き推進するとともに、東京2020大会後に策定が予定されている新たなサイバーセキュリティ戦略の検討内容を踏まえながら、次期行動計画の検討を行っていく。

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。2020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８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。2020年度は2,162者から回答があり、今回の調査結果を「ベースラインとなる情報セキュリティ対策」と「先導的な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、2019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

第４次行動計画に基づき、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って情報共有体制を運営した。また、2019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309件の情報連絡が行われ、内閣官房からは64件の情報提供を行っている（参考：別添５－５）。

なお、2020年に入ってから新型コロナウイルス感染症の世界的な拡大が始まり、感染

拡大防止策として、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、緊急事態宣言が発出される前の2020年４月７日正午に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。また、2020年６月には、テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について事務連絡を発出した。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、2021年１月の再度の緊急事態宣言を受けて、テレワーク時のセキュリティ対策を意識するよう改めて注意喚起を発出した。この間、これまで以上に積極的に注意喚起を発出してきており、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
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
内閣官房からの情報提供件数	80 件	54 件	43 件	38 件	64 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、自然災害やクラウドサービスで生じた障害、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、増加に転じた。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。

〇セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、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・水道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シルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2020年４月の総会で決定した活動方針に基づき、2020年度に、運営委員会（４回）、情報収集WG（４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、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。

〇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急激な環境変化を的確に捉えた上で、情報セキュリティ対策への速やかな反映が必要であることを踏まえ、効果的かつ迅速な情報共有に資するため、脅威の動向や環境変化に柔軟に対応できるよう検討を行い、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。更なるセプターカウン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。2020年度は「テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応」、「東京2020大会時における対応」を特徴として取り組んだ。（参考：別添５－７）。

また、事前説明会において、「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」の浸透を図るため、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サイバー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。

2020年度は、全14分野が演習に参加し、参加者数は4,721名であった。

表２　分野横断的演習参加者数の推移

年度	2017	2018	2019	2020
参加者数	2,647 名	3,077 名	4,967 名	4,721 名

2020 年度は、テレワークの活用の急速な進展を踏まえ、テレワーク環境からの参加を25%の事業者等が実施した。また、東京 2020 大会を支える重要サービス事業者に該当する事業者等のうち、62%が東京 2020 大会を想定した体制で参加した。

さらに、2019 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98%となっている。

一方で、重要インフラ全体での防護能力の底上げのため、2019 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」を実施し、82%の参加者から有意義であると回答を得た。

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、76.4%であった。

〇セプター訓練

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
参加セプター	18	19	19	19
参加事業者等	2,106	2,005	1,958	1,995

実施に当たっては、重要インフラ事業者等に内閣官房から提供する情報が届いているかを事業者等に確認（疎通確認）する「往復」訓練をベースとし、実施日時を指定しない「抜き打ち訓練」の採用、通常の伝達手段が使用できないことを想定した代替手段の実効性の検証、自社における被害状況を確認の上、「被害あり」という仮定の下で、その旨を報告する方式の採用等、より実態に即した訓練を実施するとともに、疎通確認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、疎通確認がなぜできなかったのか、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。

〇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 WallⅤ）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

第４次行動計画に基づき、分野横断的演習については、さら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
・セプターカウンシ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

東京2020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」を提供している。内閣官房では、ウェブサイトへの掲載等での配布を通じて本ガイドラインの普及促進を図っており、2020年度におけるウェブサイトの閲覧数は3116件となっている。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、東京2020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（297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、2020年度におけるウェブサイトの閲覧数は2021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、2017年12月に2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議セキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、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のサイバーセキュリティ対処調整センターを設置し、東京2020大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用したほか、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。

○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、セプターカウンシルの活動（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）及び有識者部会（２回）をそれぞれ開催した。また、東京2020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態勢整備の強化を促進する。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。

新型コロナウイルス感染症拡大防止対策に伴うテレワークの導入や新たなデジタル技術の浸透によって、これまでにないセキュリティリスクが顕在化している。したがって、新たなデジタル技術の活用とサイバーセキュリティ対策を一体的に進めることが求められるため、これに伴うリスクの洗い出しや必要な対応を実施することを引き続き推進していく。

また、セプターカウンシルや分野横断的演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議の支援を行うとともに、経営層を含む内部のステークホルダー相互間のリスクコミュニケーション及び協議の推進への支援を継続して実施する。

(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。

〇防護範囲の見直し

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等の活発な活動や交通ISACの設立など、サイバーセキュリティに関する協力関係拡大や充実を図る動きが進んだ。

加えて、経済産業省において、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)」と連携し、大企業と中小企業を含めた産業界のサイバーセキュリティ対策を促進した。

〇広報広聴活動

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24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指針、サイバーセキュリティ基本法等の関係法令等を説明するとともに、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。

〇国際連携

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、国際的な情報共有の枠組みであるIWWNを活用し、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を行っている。また、2021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、2020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。

〇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。

また、経済産業省から企業経営者向けに、最近のサイバー攻撃の状況を踏まえた注意喚起を発出するなど、経営層を交えたサイバーセキュリティの取組が着実に推進された。

〇人材育成等の推進

内閣官房は、サイバーセキュリティ２０２０や「サイバーセキュリティ人材育成取組方針」（2018年６月サイバーセキュリティ戦略本部報告）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。

〇規格・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2020年８月に更新し、ウェブサイト上で公表した。

また、制御系機器・システムの第三者認証制度については、経済産業省において、CSSCを通じて、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。

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、引き続き内閣官房及び重要インフラ所管省庁が連携し、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように働きかけを行うとともに、そのような働きかけを通して知見を得て、重要インフラ防護施策を実態に即した実効的なものとする。

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人材育成取組方針」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。	・サイバーセキュリティを取り巻く情勢を踏まえ、指針において安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加する等の改定を行っており、この改定の内容を NISC のウェブサイトで公表するとともに、「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」（電子版）として新たに取りまとめ、同サイト上に掲載した。
②必要に応じて社会動向の変化及び新たに得た知見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、指針において安全基準等で規定されることが望まれる対策項目として「データ管理」及び「災害による障害の発生しにくい設備の設置及び管理」を追加する等の改定を行っており、この改定の内容を NISC のウェブサイトで公表するとともに、「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」（電子版）として新たに取りまとめ、同サイト上に掲載した。
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。 ・2020 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８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次期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。（2020 年度　情報連絡 309 件、情報提供 64 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あ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、考え方の整理について引き続き検討した。
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、運用に必要となる資源を確保。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラの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、2020 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 情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラの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 セプターカウンシルに参加するセプターと連携し、セプターカウンシルの運営及び活動に対する支援の実施。	・セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。(2020 年度のセプターカウンシル会合の回数は延べ７回)
⑨ セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の整備。	・セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の構築に向けた検討を実施した。
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。2020 年度は 4,721 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。また、シナリオ作成に際しては、テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応、東京 2020 大会を見据えた情報共有体制の確認やレピュテーションリスクにおける視点にも留意した。 ・事前説明会において、「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」の浸透を図るため、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サイバー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 2020 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。
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行う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。	・東京 2020 大会の関連事業者等に対して、機能保証の考え方を踏まえたリスクアセスメントの実施手順を記載した「機能保証のためのリスクアセスメント・ガイドライン」を 2016 年度に整備・公表している。 ・2020 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 2020 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（297 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 2020 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。 ・2020 年度往訪調査において、事業者に対して情報セキュリティに関するリスクへの対処について調査した。
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 2020 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 セプ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、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても、説明会を開催した。
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。	・2017 年 12 月にセキュリティ幹事会において決定された「サイバーセキュリティ対処調整センターの構築等について」に基づき、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のサイバーセキュリティ対処調整センターを設置し、東京 2020 大会までの大規模イベント（G20 大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用した。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。
⑨ リスク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 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の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指針、サイバーセキュリティ基本法等の関係法令等を説明するとともに、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、ウェブサイト上で公表した。
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関係す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関係す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、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「IoT セキュリティ・セーフティ・フレームワーク」を 2020 年 11 月に策定した。 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を講演会等で周知し、普及啓発を促進。ダウンロード数は 2021 年 1 月末時点で 10 万件を超えた。加えて、可視化ツール V1.0 開発のため、β 版ベースでユーザ企業及び投資家等ステークホルダーへのヒアリングを実施。その結果を V1.0 の企画としてまとめ、V1.0 開発に着手した。

② 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。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。	・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、2020 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、総務省は、2020 年 12 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、通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方及び災害に強い通信インフラの維持・管理方策について検討した結果を取りまとめた情報通信審議会からの一部答申を踏まえ、令和２年６月に「情報通信ネットワーク・安全・信頼性基準」の改定を行った。 ・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」を令和３年１月 29 日付で第 5.1 版に改定し、クラウド化の拡大を念頭において、クラウドの概要、クラウド利用に係る責任分界についての追記等を行った。 ・また、水道分野に関し、厚生労働省は、令和２年４月に施行された「水道施設の技術的基準を定める省令の一部を改正する省令」（厚生労働省令第 59　号）において、水道事業の施設基準としてサイバーセキュリティ対策を位置づけた。 ・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。
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。	・重要インフラ所管省庁は、各重要インフラ分野における検証等に寄与するため、所管のガイドライン等を改定若しくは改定の検討を行った。
④ 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透に向けた取組を実施。	・総務省において、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を改定し、地方公共団体における安全基準の整備等を支援した。 ・厚生労働省において、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。
⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・重要インフラ所管省庁は、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。
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。	・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。
(2)「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。	・重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあったＩＴの不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。

② 重要インフラ事業者等との緊密な情報共有体制の維持と必要に応じた見直し。	・重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ所管省庁内のとりまとめ担当部局と各重要インフラ分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2020 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とりまとめており、担当者の異動時には最新の情報を報告する体制をとることで、綿密な情報共有体制を維持している。 ・総務省において、令和元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とりまとめ、令和２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ている。 ・厚生労働省において、医療機関間のサイバーセキュリティに関する情報共有・相談体制の検討に向けて、医療機関同士が情報共有ツールを活用して情報交換を行う試行を令和 3 年１～3 月に実施した。医療分野のサイバーセキュリティ対策に関する意見交換においては医療機関のみならず、製薬メーカーの参画も得られた。 ・国土交通省において、法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」が、2020 年４月に一般社団法人として設立され、2021 年３月現在 79 会員まで増加している。
③ 重要インフラ事業者等からのシステムの不具合等に関する情報の内閣官房への確実な連絡。	・重要インフラ所管省庁は、①の情報共有体制のもと、重要インフラ事業者等からのＩＴ障害等に係る報告があった場合は、速やかに内閣官房へ情報連絡を行った。
④ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。	・重要インフラ所管省庁は、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・重要インフラ所管省庁は、セプターカウンシル総会及び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。
⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。	・重要インフラ所管省庁は、セプターカウンシル総会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。
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	・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、2020 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。
(3)「障害対応体制の強化」に関する施策	
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。	・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、2020 年 9 月に、全 19 セプターに対するセプター訓練を実施した。
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。	・重要インフラ所管省庁は、2020 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。
③ 分野横断的演習への参加。	・重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員などが、2020 年 12 月に実施された分野横断的演習に参加した。
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。	・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 2020 年度分野横断的演習への参加を促し、4721 名の参加者を得た。
⑤ 分野横断的演習の改善策検討への協力。	・重要インフラ所管省庁は、2020 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。
⑥ 必要に応じて、分野横断的演習成果を施策へ活用。	・重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。

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。	・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 Ⅴ）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、2020 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。
(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。	・重要インフラ所管省庁において、内閣官房と連携し、東京 2020 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。
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。	・重要インフラ所管省庁は、NISC が作成したリスクアセスメント・ガイドラインや手引書等の浸透状況を把握するための調査に協力した。
③ 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。	・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。
④ 本施策における調査・分析の施策へ活用。	・総務省においては、今後、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として「ＥＵ諸国及び米国における情報共有体制に関する調査」の活用が予定されている。
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。	・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。
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。	・金融庁において、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2018 年 10 月公表）に基づく取組みにおいて把握した実態や共通する課題等について、2020 年６月に「金融分野のサイバーセキュリティレポート」を公表した。また、サイバー空間の脅威を迅速に把握し、金融システム全体のセキュリティ向上等に取り組むため、2020 年７月に「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」を公表した。
(5)「防護基盤の強化」に関する施策	
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。	・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。
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。	・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
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。	・経済産業省において、2020 年 12 月、企業経営者向けに最近のサイバー攻撃の状況を踏まえた注意喚起を発出し、経営層を交えたサイバーセキュリティ対策の更なる推進を図った。また、2019 年度に引き続き「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。
④ 内閣官房と連携し、関連規格を整理、可視化。	・重要インフラ所管省庁は、内閣官房と連携し、国内外で策定される重要インフラ防護に関係する規格について、情報を収集した。

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。	・国土交通省において、法人設立及び情報共有等の事業活動が開始されるよう必要な支援を行った、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う体制である「交通 ISAC」が、2020 年４月に一般社団法人として設立され、2021 年３月現在 79 会員まで増加している。 ・経済産業省において、大企業と中小企業がともにサイバーセキュリティ対策を推進するために産業界が 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。	・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。	・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。	・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。	・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 セプターカウンシル等からの要望があった場合、意見交換等を実施。	・情報セキュリティ関係省庁とセプ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。	・2020 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。	・「サイバー攻撃特別捜査隊」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。	・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 セプターカウンシル等からの要望があった場合、意見交換等を実施。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
(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。	・事案対処省庁は、2020 年度分野横断的演習検討会にオブザーバーとして出席するとともに、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。	・事案対処省庁は、2020 年度分野横断的演習検討会にオブザーバーとして出席するとともに、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。	・ 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。
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。	・ 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。

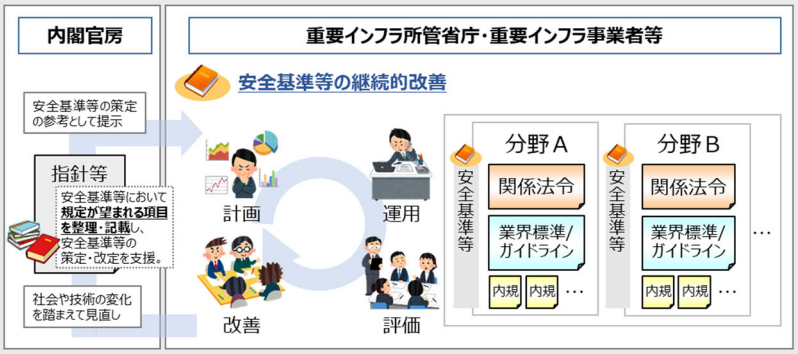
別添５－３　安全基準等の継続的改善状況等に関する調査

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26件）

調査項目

①各安全基準等の**分析・検証**の状況
②各安全基準等の**改定**の状況
③各安全基準等の**指針への対応**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26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4.1版）
	放送	・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	・ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン ・電気通信分野における情報セキュリティ確保に係る安全基準（第4.1版）　※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		・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

- 2020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**８件の改定が実施**（※）された。　※ うち１件は2021年４月１日の改定
- 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】
- 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
- 業務のデジタル化等の進展
- 新型コロナウイルス感染症の拡大　等

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**安全基準等を改定が行われている**（※）ことを確認。

（※）分析・検証の結果、自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**
  - 事業用電気通信設備規則
  - 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
- **社会的・技術的な環境の変化を踏まえた改定**
  - 情報通信ネットワーク安全・信頼性基準
  - 電気設備の技術基準の解釈
  - 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）
- **その他**
  - 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
  - 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

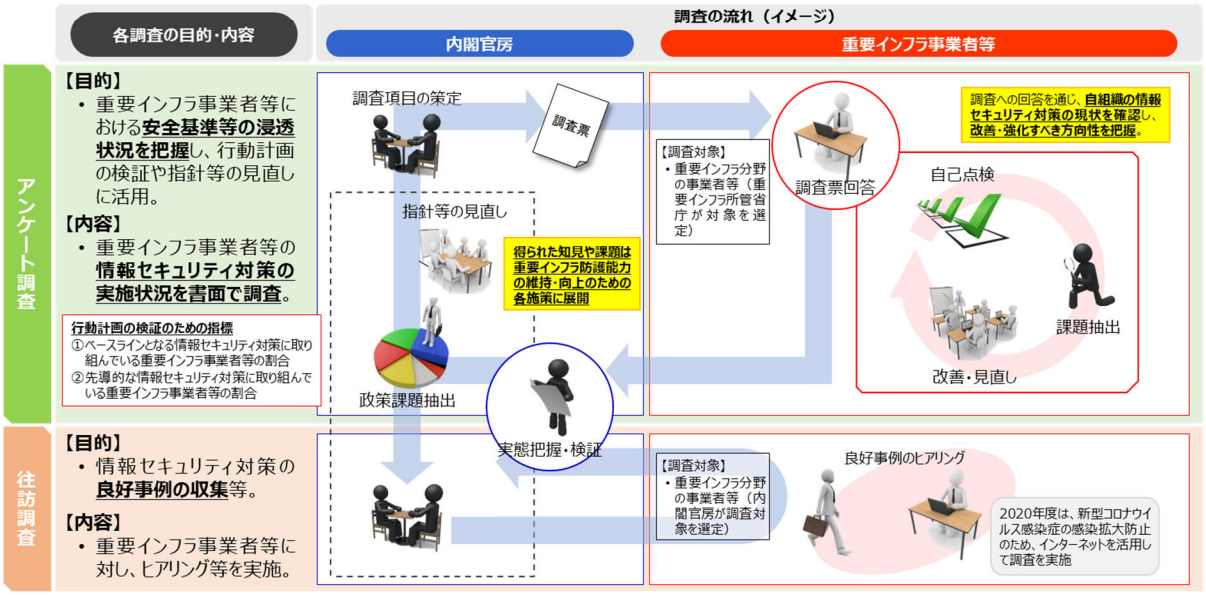
重要インフラ所管省庁及び重要インフラ事業者等で構成される業界団体において、各安全基準等の分析・検証や改定が行われ、**安全基準等の継続的な改善が着実に実施**されていることを確認。

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、2019年度に引き続き、**2020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。

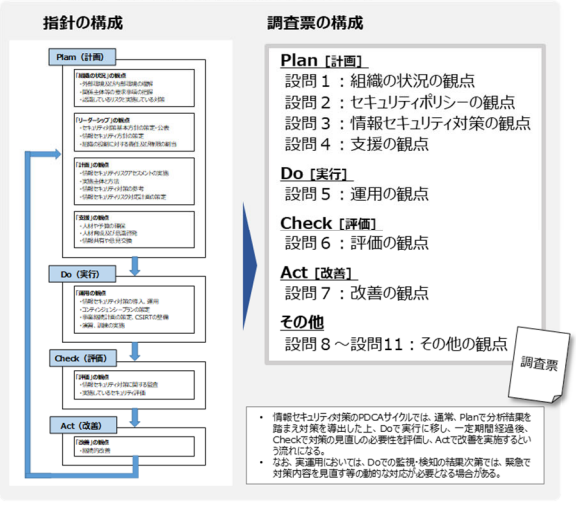
（注）これらの対策項目の実施の有無が当該事業者における情報セキュリティ対策のレベルを直ちに示すものではないことに留意する必要がある。指針においても、対策項目は「重要インフラ事業者等が採否を検討する」ものとされている。

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：2020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**

調査票の構成

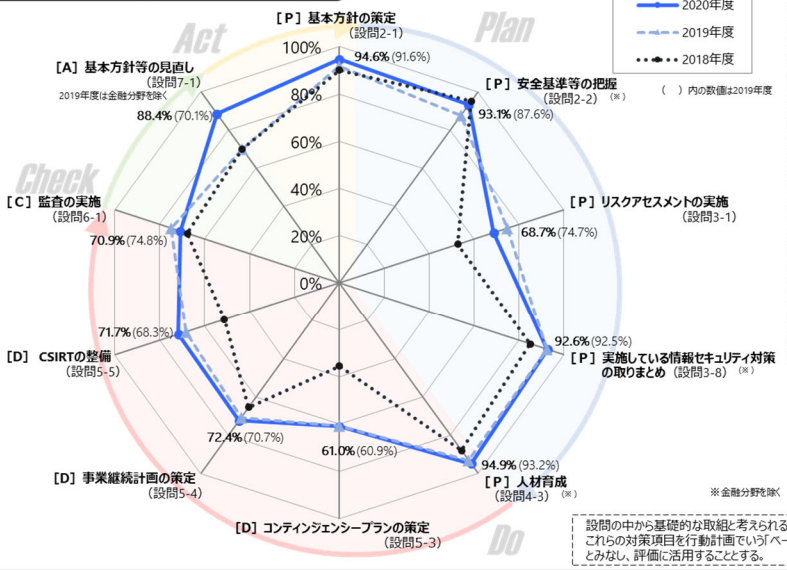
- 調査票では、これらの対策項目の実施状況が確認できるよう、指針の構成に沿って調査項目を設けることとした。



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2018年度から大きく向上**し、その傾向が継続していることから、**安全基準等の浸透は着実に進展**していると評価できる。一方で、引き続き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）、Act（改善）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自主的に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。

各取組の実施状況［過去度の調査との比較］



※ 以下の設問は、2018年度のデータがないため本欄に別記。

設問の中から基礎的な取組と考えられる対策項目を抽出して記載している。これらの対策項目を行動計画でいう「ベースラインとなる情報セキュリティ対策」とみなし、評価に活用することとする。

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、**複数の項目で実施状況はおおむね向上**している。
- 「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、引き続き実施状況が低い項目も見受けられるため、これらの実施状況も改善しており、**先導的な情報セキュリティ対策に関する取組も着実に進展**しつつあると評価できる。

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。　※金融分野を除く

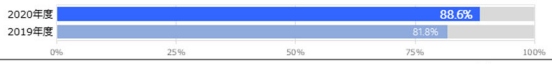
情報セキュリティ対策が単に情報システムの構築・運用の観点だけでなく、**企業経営の観点からも検討**されていること。	● 経営層からの関与がある（設問8-1）（※） 2020年度 81.8% 2019年度 62.5%
システムの構築・運用及び企業経営の**各責任者が定期的に、適切に相互関与する体制が整備**されていること。	● 経営層と定期的なレポーティング・対話の場が設けられている（設問8-2）（※） 2020年度 20.5% 2019年度 14.9%
守るべき重要インフラサービス及びサービス維持レベルを踏まえ、**自らがなすべき必要な対策が理解**されていること。	● 関係主体からの要求事項を整理している（設問1-2）（※） 2020年度 88.6% 2019年度 81.8% ● 機能保証の考え方を取り入れたリスクアセスメントを実施している（設問3-1）（※） 2020年度 25.7% 2019年度 21.1%
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**情報の開示などが取り組まれている**こと。	● 基本方針を策定し外部に公表している（設問2-1）（※） 2020年度 35.8% 2019年度 35.4%
情報セキュリティ対策の水準の向上のためには可能な限り**情報共有を行うという姿勢が積極的に評価される価値観が醸成**されていること。	● 関係主体と情報共有を行っている（設問4-5）（※） 2020年度 80.0% 2019年度 69.9%
事業における重要インフラサービス障害の発生について、これを隠すべきものではなく、重要インフラ事業者等内の情報セキュリティ対策に取り組む**関係者間で共有すべきものであるという認識が醸成**されていること。	● 関係主体と情報共有を行っている（設問4-5）（※）【再掲】 2020年度 80.0% 2019年度 69.9%

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）

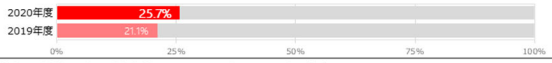
将来像②：「課題抽出」、「リスク評価」及び「対策の改善」に関する次の事項が十分に浸透している。

本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、**自らの情報セキュリティ対策の程度及び残存するリスクが認識**されていること。

- 関係主体からの要求事項を整理している（設問1-2）（※）【再掲】

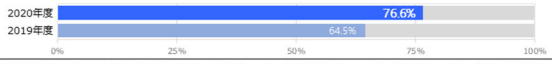


- 機能保証の考え方を取り入れたリスクアセスメントを実施している（設問3-1）（※）【再掲】

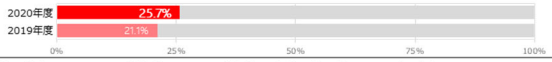


各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス障害に係る**リスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっている**こと。

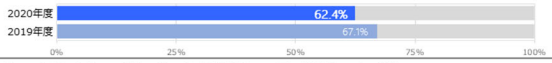
- 内部環境や外部環境を整理している（設問1-1）（※）



- 機能保証の考え方を取り入れたリスクアセスメントを実施している（設問3-1）（※）【再掲】

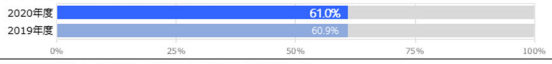


- 情報セキュリティ計画を策定している（策定中を含む）（設問3-9）（※）



重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、**重要インフラサービス障害が国民生活や社会経済活動に重大な影響を与えるリスクを可能な限り低減**させることができていること。

- コンティンジェンシープラン（CP）を策定している（設問5-3）（※）



- 事業継続計画（BCP）を策定している（設問5-4）

これらの取組が**対策の継続的な改善の原動力の一つとなっている**こと。

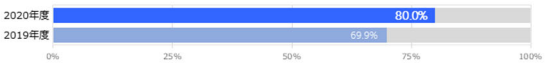
- 基本方針等の継続的な見直しを行っている（設問7-1）（※）

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。

※金融分野を除く

重要インフラサービス障害の発生状況等に関する情報の把握ができており、必要に応じて当該情報が各分野のセプターやセプターカウンシルを通じて**外部の関係主体と共有され、公式又は非公式の連携が行われている**こと。

- 関係主体と情報共有を行っている（設問4-5）（※）【再掲】



別添５－５　情報共有件数

「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	FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
重要インフラ事業者等からNISCへの情報連絡(※)	856	388	223	269	61	75	86	87	309
関係省庁・関係機関からのNISCへの情報共有	41	19	7	16	4	6	1	5	16
NISCからの情報提供	80	54	43	38	11	8	21	24	64

※1)重要インフラ事業者等からNISCへの情報連絡の事象別内訳は以下のとおり。

事象の類型			FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
未発生の事象		予兆・ヒヤリハット	330	80	27	12	3	4	13	8	28
発生した事象	機密性を脅かす事象	情報の漏えい	30	15	13	13	4	5	4	10	23
	完全性を脅かす事象	情報の破壊	47	20	17	11	4	4	3	1	12
	可用性を脅かす事象	システム等の利用困難	80	143	97	158	39	41	37	40	157
	上記につながる事象	マルウェア等の感染	289	65	17	9	4	4	3	7	18
		不正コード等の実行	10	13	4	5	0	1	1	1	3
		システム等への侵入	26	17	14	14	1	3	11	11	26
		その他	44	35	34	47	6	13	14	9	42

※2)上記事象における原因別類型は以下のとおり。（複数選択）

事象の類型		FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
意図的な原因	不審メール等の受信	546	89	36	13	2	4	0	3	9
	ユーザＩＤ等の偽り	1	4	3	12	0	5	2	2	9
	DDoS攻撃等の大量アクセス	23	31	17	20	4	3	1	2	10
	情報の不正取得	14	16	10	8	3	2	4	4	13
	内部不正	0	4	1	0	0	0	0	0	0
	適切なシステム等運用の未実施	19	15	14	11	4	3	7	9	23
偶発的な原因	ユーザの操作ミス	15	23	10	6	4	5	3	6	18
	ユーザの管理ミス	8	13	6	6	3	0	2	8	13
	不審なファイルの実行	243	42	16	7	0	4	1	2	7
	不審なサイトの閲覧	29	20	4	5	0	1	2	0	3
	外部委託先の管理ミス	20	41	29	39	9	12	15	20	56
	機器等の故障	22	32	27	62	10	11	13	5	39
	システムの脆弱性	56	36	19	16	3	3	22	10	38
	他分野の障害からの波及	0	10	6	4	2	2	2	1	7
環境的な原因	災害や疾病等	0	0	1	13	0	7	2	0	9
その他の原因	その他	34	29	29	33	9	9	6	11	35
	不明	92	57	46	53	18	14	18	18	68

（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

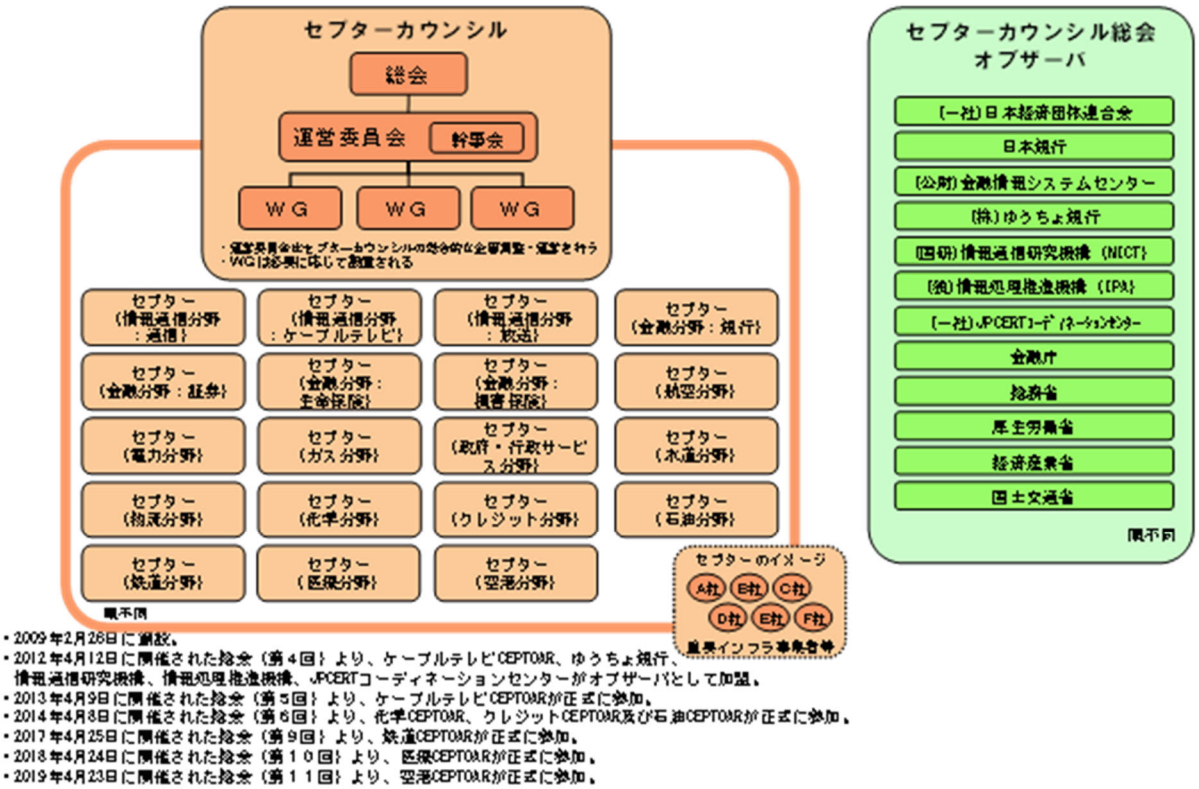
セプター（ＣＥＰＴＯＡＲ） Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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（2021 年４月 21 日現在）



- 2009年2月26日に創設。
- 2012年4月12日に開催された総会（第４回）より、ケーブルテレビCEPTOAR、ゆうちょ銀行、情報通信研究機構、情報処理推進機構、JPCERTコーディネーションセンターがオブザーバとして加盟。
- 2013年4月9日に開催された総会（第５回）より、ケーブルテレビCEPTOARが正式に参加。
- 2014年4月8日に開催された総会（第６回）より、化学CEPTOAR、クレジットCEPTOAR及び石油CEPTOARが正式に参加。
- 2017年4月25日に開催された総会（第９回）より、鉄道CEPTOARが正式に参加。
- 2018年4月24日に開催された総会（第１０回）より、医療CEPTOARが正式に参加。
- 2019年4月23日に開催された総会（第１１回）より、空港CEPTOARが正式に参加。

セプター特性把握マップ

2021年3月末日現在

重要インフラ分野	情報通信			金融				航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信	放送		銀行等	証券	生命保険	損害保険	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 IT統括部	(一社)生命保険協会 総務部経営企画・法務グループ	(一社)日本損害保険協会 IT推進部 品質管理グループ	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術エネルギー構造ユニット	地方公共団体情報システム機構 情報化支援戦略部	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	23社1団体	311社1団体	195社・団体	1,324社	281社7機関	42社	47社	14社1団体	8社	22社1団体	24社3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	51社	11社
NISCからの情報の展開先（構成員以外）	395社・団体	394社	11社	2社・団体	—	—	—	—	—	—	14社・機関	166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、サイバーディフェンス連携協議会、大学等（内容に応じ展開先を選定））																			

■ その他

既存事業領域を越える連携等

情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、制御システム(JPCERT/CCが提供するConPaS等)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC：セキュリティ情報全般)

別添５－７　分野横断的演習

2020年度　分野横断的演習について

1. 実施概要

内閣サイバーセキュリティセンターは、重要インフラ分野におけるサービス障害への対応能力の維持・向上を図ることを目的に、「分野横断的演習」を実施した。この演習は、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実施するサイバーセキュリティ対策が有効に機能しているかどうかを確認し、改善につなげるためのものである。

2. 演習の形態

- 机上演習

  昨年度までは集合会場で実施（一部は自職場）してきたが、今年度は新型コロナウイルス感染症対策のため、集合会場を使用せず、自職場から参加する方式とした。また、テレワーク環境からも参加した。

3. 実施時期

- 2020年12月8日（火）　13:00～17:00

4. 参加者

- 参加者全体：4,721名（656組織）
- 重要インフラ事業者［情報通信、金融、電力等の14分野］：4,047名（465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

5. 2020年度の特徴

- テレワークが広く実施されるようになったことに鑑み、テレワーク実施事業者において、テレワークに関するセキュリティリスクを勘案した対処体制の構築やインシデントへの対応が適切に行えるかどうかを確認
- 東京2020大会延期を踏まえ、東京2020大会時における対応についても考慮

6. 橋本大臣(当時)挨拶

演習開催にあたり、橋本聖子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担当大臣（サイバーセキュリティ戦略本部副本部長）(当時)の挨拶があった。橋本大臣は、参加者に対し、本演習を通じて課題を抽出・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。

橋本大臣(当時)挨拶（ビデオメッセージ）

7. “テレワーク環境”に関する演習実施状況

- 演習内でテレワークでの作業として実施されたものの例

・NISC等から得た情報提供を社内関係者に展開
・社内において発生したインシデントについて、セプ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
・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いた作業の実施
（障害やサービスの状況に関する情報収集・共有、サービスへの影響把握、復旧に向けた対策の検討・実施等）
・自社のサービス利用者に向けた、Webサイト、SNS等による情報発信

8. “東京2020大会”に関する演習実施状況

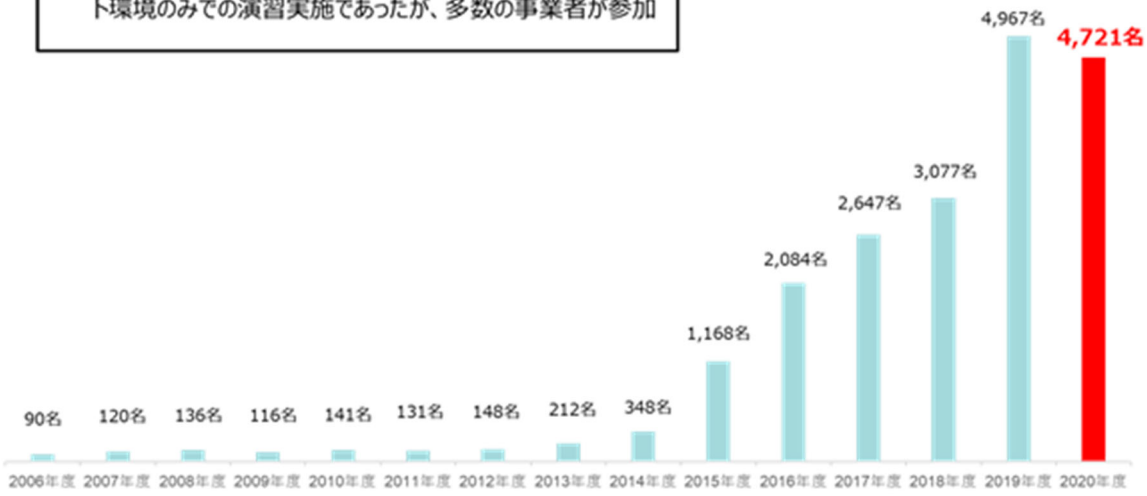
- 東京2020大会を想定した演習を実施したものの例

・空港運営部署も訓練に参加し、空港ターミナル内の旅客が滞留した場合を想定
・マスコミや顧客からの問い合わせが殺到する状況を想定
・東京2020大会に関係する事業所の複数システムにおいて、サイバー攻撃を受けた状況を想定

分野横断的演習の参加者の推移

- **本年度の参加登録者は4,721名**

本年度はコロナ禍であるため、集合会場を設定せず、リモート環境のみでの演習実施であったが、多数の事業者が参加



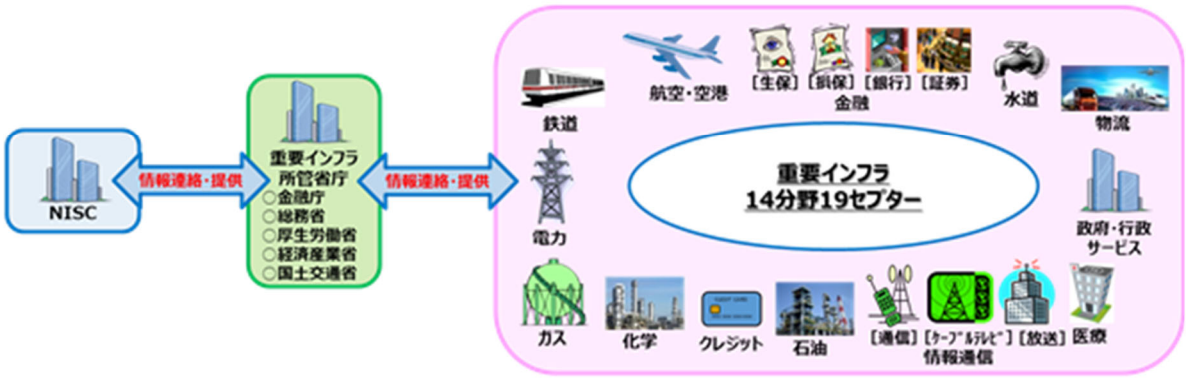
別添５－８　セプター訓練

2020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>
2020年9月15日、23日、30日（セプター毎に異なる日時に実施）



2020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、疎通確認率の向上、体制強化等の適切な改善に資する。

<方法>
✓ 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の各段階で疎通確認状況を把握する。
✓ 昨年関係者と協働して作成した「「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、レビューを行う。

<2020年度訓練におけるポイント>

✓ 連絡先のメンテナンス徹底等、前回訓練での振り返り内容が対策として反映されているか検証
　☞連絡先のメンテナンス不足は2019年度訓練で一番多かった課題
　☞新しい生活様式への移行が進み、テレワークの利用が拡大する中、連絡先の変更に注意
- 抜き打ちの訓練実施　☞より実践的な訓練の実施
- 疎通確認率把握及び疎通確認ができない主な原因の抽出とその対策の検討

2020年度セプター訓練結果のまとめ

✓ 全セプターにおいて事業者等には**日程を連絡しない抜き打ち訓練**を実施。

✓ **3日以内に疎通確認率100%となったのは、今年度は13セプター**（昨年度8セプター）。
☞3時間以内に100%応答が完了したのは４セプター、その後24時間以内に応答が完了したのが3セプター。
昨年度（3時間以内に応答3セプター、24時間以内に応答2セプター）に比べ増加したが、全体として迅速に実施できたとは言い難い。

✓ **疎通確認ができなかった事業者等について、アンケートで原因調査とその対策等**を確認。
☞昨年度の反省を生かして速やかな疎通確認ができた事業者がいる一方、一部においては、昨年と同様の原因（業務多忙による失念、担当者変更手続き漏れ、メールの見逃し）で疎通確認ができないケースが発生。

✓ **昨年度の訓練結果を踏まえた改善の内容及び、今年度の訓練を通じた課題や気付き等を確認**した。
☞17セプターが昨年度の訓練で得られた課題・気付き等の改善の検証ができたと回答。
☞今回の訓練において、18セプターが課題や気付き等を認識したと回答。

✓ 日常の情報共有体制、手引書等に関する課題や意見をアンケートで収集。

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、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、2020年1月1日～2020年12月31日の間に、重要インフラ事業者等から内閣サイバーセキュリティセンターに提出された情報連絡の事例の中から、主に以下の選定基準により選定しました。

- 重要インフラサービス及びその周辺サービスへの実害の有無
- 事案の重大さ・社会的影響（関心）の大きさ
- 類似事例の発生状況や今後発生する可能性
- 攻撃手口や被害の目新しさ
- 世の中のトレンド
- 他分野への波及の可能性
- 得られる気付き・教訓の有用性等

※その他、事案の対応の優劣、分野のバランスも考慮

2020年度　調査対象事例　概要

- "外部からのサイバー攻撃"や"重要インフラ事業者内でのインシデント"等、例年発生頻度の高い脅威は2020年も一定数発生しているが、対応を実際に経験したことで重要インフラ事業者が新たに気づいた課題や教訓等について調査。

No.	事例	影響	原因
システム故障に起因した重要インフラサービス障害			
1	ハードウエア故障に伴う重要インフラサービスの停止	基幹システムで障害が発生、さらに予備系システムへの自動切り替えに失敗し、重要インフラサービスを終日停止することとなった。	基幹システムで使用しているNAS(ネットワークストレージ)の故障
2	クラウドでのシステム障害に伴うサービスの停止	クラウドサービス基盤上に構築していた複数の重要インフラサービスが一時停止、顧客が当該サービスを利用できない等の影響が生じた。	クラウドサービス基盤のシステム障害
3	システム障害に伴う重要インフラサービスの業務遅延	業務システムのストレージがロックされたことにより、データが閲覧できなくなり、重要インフラサービスの業務が一時的に遅延した。	業務システムによるハードウエア障害の誤認識
外部からのサイバー攻撃			
4	連携サービス間の脆弱性を突いたサービスの不正利用	重要インフラサービスに関し、利用者から身に覚えのない利用履歴があるとの問合せが相次ぎ、サービスを一時停止した。	他事業者の仕様変更により生じた連携サービス間の脆弱性の悪用
5	重要インフラ事業者における2度のランサムウエア感染	重要インフラ事業者の職員が利用するサーバーのデスクトップ上のファイルが暗号化され、ファイルが使用不能となった。	サーバーのRDP(リモートデスクトッププロトコル)への総当たり攻撃
6	重要インフラ事業者における「WannaCry」の感染	重要インフラ事業者でマルウエア「WannaCry」の感染が拡大、重要インフラサービスに直接影響するネットワークで使用している複数の端末が再起動を繰り返した。	マルウエア「WannaCry」に感染した端末が重要インフラ事業者のネットワークに接続されたこと
7	重要インフラ事業者の偽サイトの確認	第三者が重要インフラ事業者のWebサイトをコピーした偽サイトを作成、その後、同事業者のWebサイトが有害サイトに判定された。	第三者による重要インフラ事業者のWebサイトをコピーした偽サイトの作成
8	問合せシステムを悪用した不正なメールの送信	第三者が重要インフラ事業者の問合せシステムを悪用し、不正なメールを送信、その後、同事業者のメールが正しく届かない事象が発生。	重要インフラ事業者のWebサイト上の問合せフォームの悪用
9	業務使用PCにおけるサポート詐欺	重要インフラ事業者の職員がWeb閲覧時に警告音が鳴り、ウイルス感染の警告と指定の番号に電話するよう案内が表示された。	業務用PCによるWeb閲覧

2020年度調査結果を踏まえた総論

総論

- 重要インフラ事業者等でシステム故障やサイバー攻撃による影響が発生、重大な重要インフラサービス支障が生じたことで、社会的問題に発展し、**経営の問題に直結するような事例も増加**している。
- 本状況下において、セキュリティ担当だけでは対応しきれないものもあることから、経営層の関与が一層重要となっており、重要インフラ事業者等の経営層が、**組織内全体の問題と捉え、サイバーセキュリティに関する問題に積極的に関与**することが必要。

得られた気付き・教訓　概要（各事案に共通する事項）

システム故障に起因した重要インフラサービス障害事例（No. 1, 2, 3）から

- 冗長化したシステムにおいて、予備系への自動切り替えに失敗する事例が複数確認されていることから、**設計通りの稼働が確保されているか定期的に確認**することが重要。
- システム障害の防止に十分努めることは必要であるが、障害発生による影響を抑える観点から、これに加えて、**レジリエンス(障害回復力)の強化に資する取組**を進めることが重要。
- システム障害発生時に備え、事業者が提供する**各サービスの主管部署、経営層、広報担当者、外部委託先等を含めた緊急連絡体制の整備、連絡手段の確保**、訓練の実施が重要。

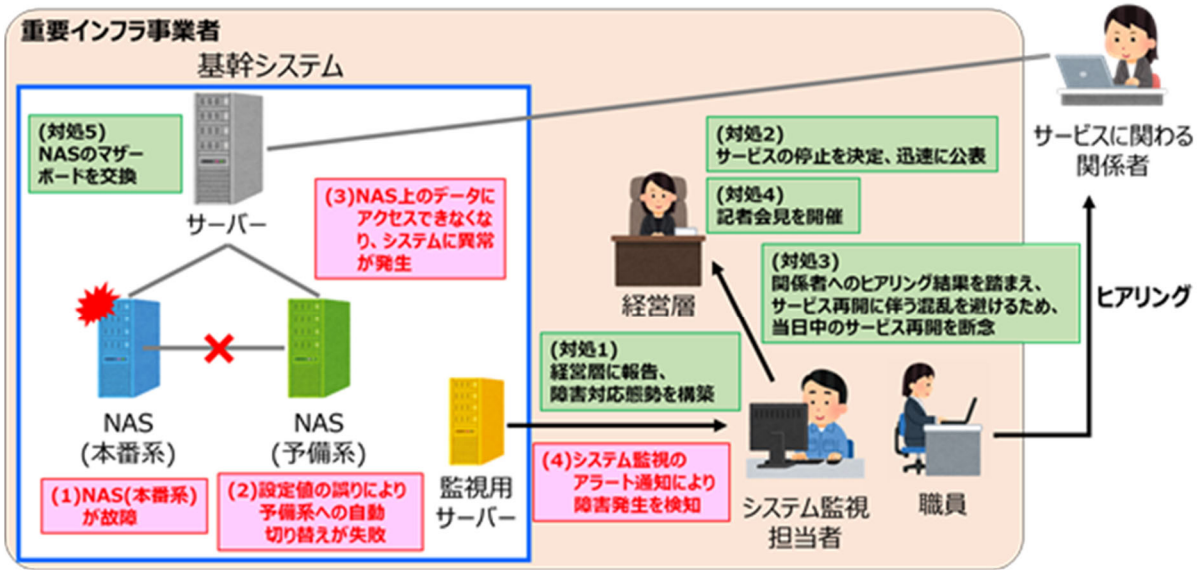
外部からのサイバー攻撃への対応事例（No. 4, 5, 6, 7, 8, 9）から

- インターネット等の外部ネットワークからアクセス可能な機器については、**セキュリティパッチを迅速に適用する、不要なポートやプロトコルを外部に開放しない**等の対策を講じることが重要。
- サイバー攻撃にかかる対応では、過去の類似事案が参考になることも多いため、情報共有体制への参画等を含めた**日頃から定期的に情報を収集・入手できる体制の確保**が必要。
- サイバー攻撃による二次被害等を防止するため、**迅速にサービスに対する影響を公表**し、その後も適時、**続報の公表を検討**することが重要。影響が不特定多数に及ぶ可能性がある場合は、Webサイトや SNS等の**複数経路による情報発信**も検討することが重要。

※　個々の事例ごとの他の気付き・教訓については、各事例の項を参照。

事例1　ハードウエア故障に伴う重要インフラサービスの停止

- 重要インフラ事業者の基幹システムで使用しているNAS(ネットワークストレージ)に障害が発生、当該システムは冗長化していたが、設定値の誤りにより、予備系への自動切り替えに失敗、NAS上のデータにアクセスできなくなり、事業者のルールに基づき、重要インフラサービス(以下「サービス」という)の停止を決定した。
- システムの再立ち上げにより当日中のサービス再開も可能だったが、事前にサービスに関わる関係者との取り決めなく、再開することが混乱を招くと重要インフラ事業者が判断、当日中のサービス再開を断念した。



【1　背景】

- 重要インフラ事業者では、従前からシステム障害発生時にサービスを停止する条件を定めていた。

【2　検知】

- システム監視のアラート通知により、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。
- 事業者のルールに基づき、サービスの停止を決定、迅速に公表。
- 事前にサービスに関わる関係者との取り決めなく、障害発生当日中にサービスを再開することが、サービスの混乱を招くと判断し、当日中のサービス再開を断念。
- サービス停止の謝罪及び停止に至った経緯等を説明する記者会見を開催。
- NAS(ネットワークストレージ)のマザーボード交換を実施、翌日には、サービスを再開できるようにした。

【4　原因】

- 本番系システムで利用していたNASが故障、それに伴い、システム障害が発生。
- 本来、予備系システムに自動で切り替わる設計だったが、NASの設置値の誤りにより、自動切り替えに失敗。
- NASの設定値は、システム構築時は正しいもの(自動切り替えされるもの)だったが、NASの製品仕様の変更により、誤ったもの(自動切り替えされないもの)に変わってしまった。

【5　再発に備えた対策】

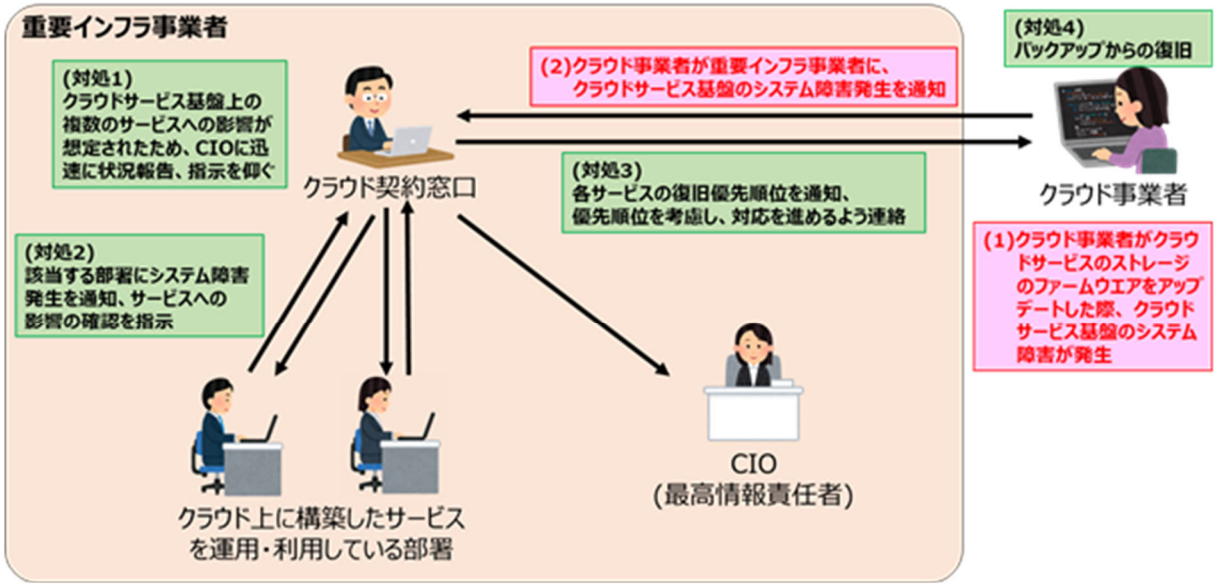
- システム障害時の予備系システムへの自動切り替えにかかる設定値の総点検を実施、自動切り替えが成功するかを確認。
- 障害発生当日にサービスを再開するための手続き、手順を関係者と検討し、今後は、サービスを迅速に再開できるようにした。

【6　得られた気付き・教訓】

- **設定どおりの稼働確保の重要性**
  冗長化したシステムに関して、システム障害発生時に自動で予備系システムに切り替わるか事前に確認することが重要。また、切り替わらなかった場合に備えて、切り替え手順の事前確認とその訓練の実施(BCPの確保)があわせて必要。
- **レジリエンス(障害回復力)の強化**
  システム障害の防止に十分務めることは必要であるが、これに加えて、レジリエンス(障害回復力)の強化に資する取組も必要。サービスの復旧に際しては、サービスに関わる関係者全体で適切な手順を検討・合意し、それに従い復旧を進めることが重要。
- **経営層の適切な関与**
  サイバーセキュリティを考慮したリスク管理及び危機管理体制、CSIRT活動等について、経営層と対応組織が適宜コミュニケーションをとり、経営層指示の元、関係者全体で、適切なサイバーセキュリティの確保に取り組むことが重要。
- **システム障害発生時の対応の明確化**
  障害発生時の対応を迅速に進めるため、障害発生時の対応、対応態勢、判断権者を明確化・マニュアル化しておくことが重要。

事例2　クラウドでのシステム障害に伴うサービスの停止

- クラウド事業者のクラウドサービス基盤でシステム障害が発生し、重要インフラ事業者のクラウドサービス基盤上に構築した複数の顧客向け重要インフラサービス(以下「サービス」という)が一時停止した。
- 重要インフラ事業者では、複数のサービスへの影響が想定されたことから、迅速にCIOに状況を報告し判断を仰ぎ、さらに、事前に定めていた各サービスの復旧優先順位に基づき、クラウド事業者と連携して、各サービスの復旧を進め、重要インフラサービスの障害による影響を最小限に抑えた。



【1　背景】

- 重要インフラ事業者とクラウド事業者は、クラウドサービス基盤の利用契約を締結、各部署は、クラウド基盤上に構築した重要インフラサービス(以下「サービス」という)を提供している。
- 重要インフラ事業者は、過去にも本事案と同一のクラウドサービス基盤でのシステム障害を経験していた。
- 上記事案対応時の反省から、重要インフラ事業者は、クラウド上のサービス一覧、各部署の緊急連絡先を事前に収集、サービスの復旧優先順位を定めていた。

【2　検知】

- クラウド事業者から、重要インフラ事業者のクラウド契約窓口に、クラウドサービス基盤のシステム障害発生にかかる連絡があり、本事象を認識。

【3　対処】

- CIO(最高情報責任者)に、システム障害発生を連絡、クラウド上の複数サービスへの影響が想定されたことから、状況を報告し、指示を仰いだ。
- クラウド契約窓口から該当する部署に、システム障害発生を通知、サービス影響の確認及び報告を指示。
- クラウド契約窓口から、クラウド事業者に対して、クラウド上の各サービスの復旧優先順位を通知、優先順位を考慮し、対応を進めるよう連絡。
- クラウドサービス基盤のバックアップから各サービスを復旧。

【4　原因】

- クラウド事業者が、クラウドサービスのストレージのファームウエアをアップデートした際、クラウドサービス基盤の障害が発生。

【5　再発に備えた対策】

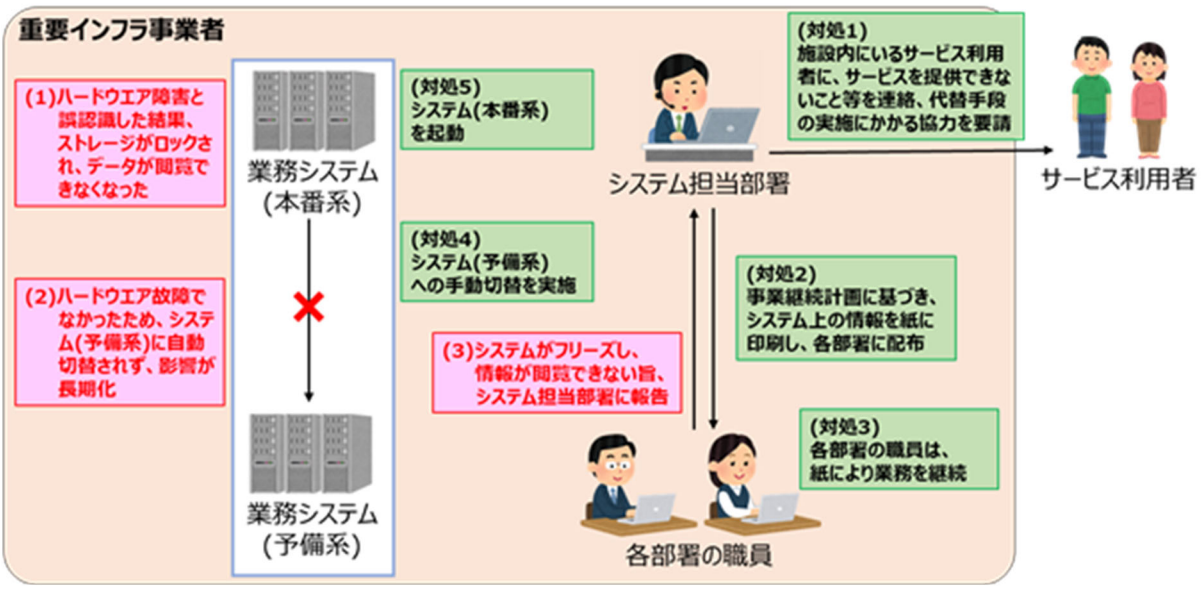
- 重要インフラ事業者とクラウド事業者でサービスレベルの合意(SLA(Service Level Agreement)の締結)を実施。

【6　得られた気付き・教訓】

- **クラウド事業者とのサービスレベルの合意(SLAの締結)**
  重要インフラ事業者がシステムに求められるサービスレベルを十分に考慮した上、クラウド事業者とサービスレベルを事前に合意(SLA(Service Level Agreement)を締結)、そのサービスレベルを踏まえ、重要インフラ事業者がシステム障害発生時の対応を検討することが重要。
- **バックアップの確実な取得**
  クラウドサービス利用時は、クラウド事業者と締結したSLAを踏まえ、クラウドでのシステム障害時にもサービスが安定的に供給できるよう、システム基盤や各サービスのバックアップを定期的かつ確実に取得する。
- **システム障害発生時の迅速な対応**
  特に、クラウド等の影響が多岐に渡るシステム障害では、サービスの継続に大きな影響を及ぼすことも想定されるため、クラウドを利用するサービスの一覧、各部署への連絡先、経営層や広報担当等の緊急連絡先を事前に把握し、迅速に対応できるようにすることが重要。
- **サービスの復旧優先順位の決定**
  重要インフラ事業者が複数のサービスを実施しており、並行でシステム復旧を進めることが難しい場合は、経営層の指示に基づき、復旧優先順位を定め、対応するアプローチが有効。

事例3　システム障害に伴う重要インフラサービスの業務遅延

- 業務システム(以下「システム」)で、ハードウエア障害が発生したと誤認識した結果、ストレージがロックされ、データが閲覧できなくなり、重要インフラサービスの業務が一時的に遅延、サービス利用者がサービスを受けられない等の事象が発生
- 事業継続計画に基づき、システム担当部署の職員がシステム上の情報を紙に印刷し、各部署の職員に配布。職員は、紙による事務処理等を行うことで、業務を継続。



【1　背景】

- 重要インフラ事業者では、業務システム(以下「システム」)上で表示される情報をもとに、サービス利用者にサービス提供や受付業務等を実施していた。
- システムは、2系統(本番系と予備系)にしており、ハードウエア故障時には、予備系に自動切替されるようになっていた。

【2　検知】

- 重要インフラ事業者の各部署の職員が、業務システムがフリーズし、情報が閲覧できない旨、システム担当部署に報告したことで、事象が判明。

【3　対処】

- 施設内にいるサービス利用者に対して、サービスを提供できないこと等を連絡し、代替手段の実施にかかる協力を要請。
- 事業継続計画に基づき、システムの情報を紙に印刷し、各部署に配布し、重要インフラサービスが継続できるようにした。
- 故障の原因が、ハードウエア故障でなかったことから、予備系に自動切替しなかったため、手動切替を実施。
- 別途、本番系を起動し、完全に復旧。

【4　原因】

- SAN(Storage Area Network)インターフェースの障害により、ハードウエア障害が発生したと誤認識し、ストレージがロックされ、データを読み取ることができなくなった。

【5　再発に備えた対策】

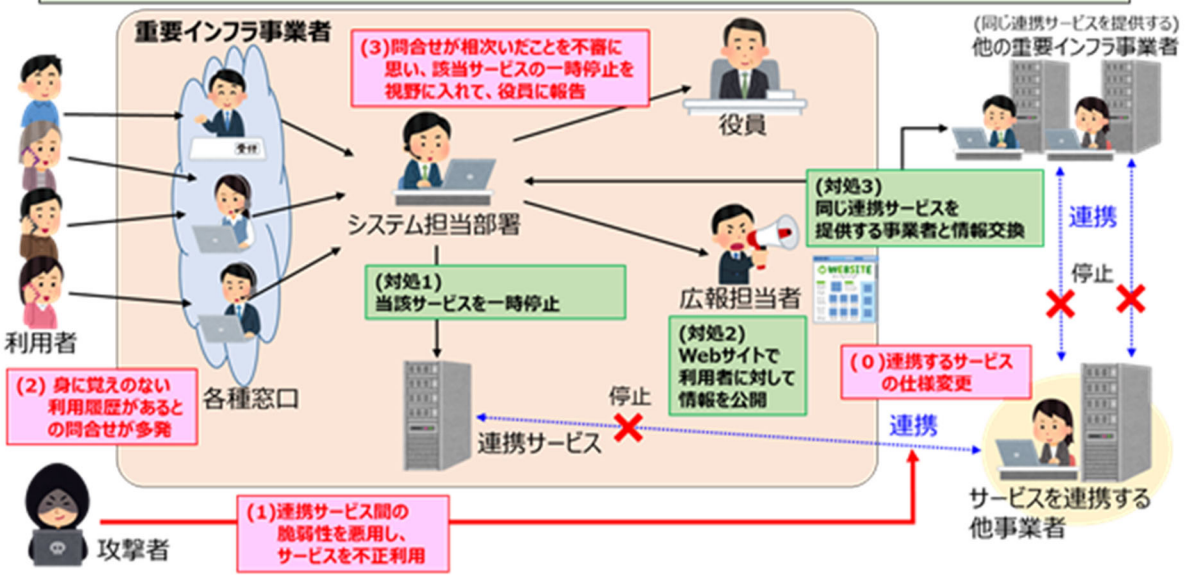
- システム(本番系と予備系)の独立性が担保されているか確認した。
- 本番系と予備系で同じストレージを参照していた部分は、障害時に当該ストレージを参照しない形で運用できるよう変更した。
- ストレージのロックを検知するプログラムを作成、当該プログラムを用いた定期的な監視により、障害を早期に検知できるようにした。
- 紙による業務継続手段は、緊急マニュアルに記載し、周知していたが、職員の定期的な異動等の理由により、運用が浸透せず、事象発生当日、職員に混乱が生じ、業務が遅延したことから、緊急時はシステム担当部署の職員を派遣する形に変更。

【6　得られた気付き・教訓】

- **システム(本番系と予備系)の独立性の確保**
  システム(本番系)の各箇所が故障した場合に、システム(予備系)が支障なく起動できるかを事前に確認しておくことが必要。
- **各部署の実態に即した業務継続計画の策定**
  システム障害は発生するという前提の下、各部署の業務継続計画の策定が必要。あわせて、業務継続計画を実行するための準備(職員への定期教育、現場への有識者の派遣等)も必要。
- **システム(予備系)への自動切替処理の検証**
  システム(本番系)の障害時に、システム(予備系)に自動切替されるかを検証することが必要。運用開始後、仕様追加や変更を行った際は、特に留意する。システム(本番系)の停止による検証が望ましいが、難しい場合は、机上での確認等を行う。

事例4　連携サービス間の脆弱性を突いたサービスの不正利用

- 重要インフラ事業者は、他事業者が提供するサービスと連携するサービスを提供していたが、利用者から身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領。
- システム担当部署は、問合せが短期間に相次いだことを不審に思い、役員まで報告、該当サービスを一時停止。原因は、サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性の悪用と判明。
- 再発防止策として、他事業者と連携する際のリスク評価に関する規定・要領を見直し、契約も変更。



【1　背景】

- 重要インフラ事業者では、他事業者が提供するサービスと連携するサービス(以下「連携サービス」という)を提供していた。
- 連携サービス開始後、連携する他事業者が仕様を変更したが、重要インフラ事業者では把握していなかった。
- 利用者から、身に覚えのないサービス利用履歴があるという問合せを受領することは平時からあったが、そのほとんどは利用者の勘違いによるものであった。
- 利用者から、自身のサービス利用履歴を確認したところ、身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領した。

【2　検知】

- システム担当部署は、同様の問合せが短期間に相次いだことを不審に思い、該当サービスの一時停止を視野に入れて、役員まで報告した。

【3　対処】

- 同日中にサービスを一時停止した。
- 同日中に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した。
- 同じ連携サービスを提供する他の重要インフラ事業者とも情報交換した。

【4　原因】

- サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性が悪用された。

【5　再発に備えた対策】

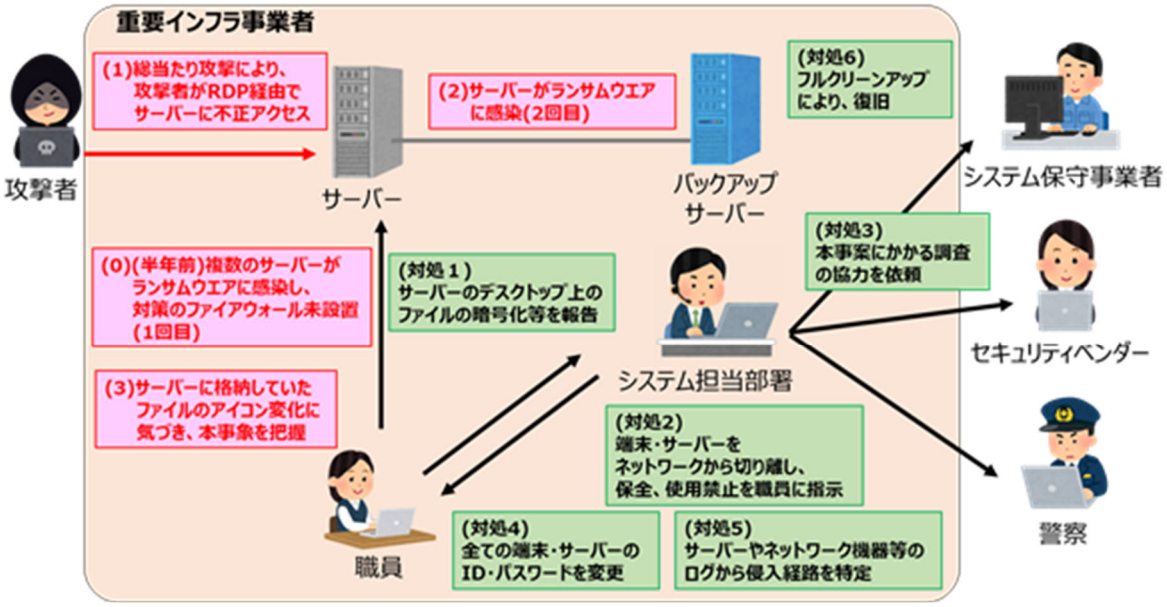
- 他事業者の仕様変更により生じた脆弱性を塞ぐよう、連携サービスを修正した。合わせて、他事業者でも、連携するサービスを修正した。
- 他事業者と連携する際のリスク評価に関する事業者内の規定・要領を見直し、これに合わせ、他事業者との契約を変更した。

【6　得られた気付き・教訓】

- **ヒヤリハット情報の迅速な共有体制の整備**
  普段あまり問題にならない報告でも、漏らさずに事業者内で素早く共有する体制が整っていたことで、事案を早期に覚知できた。
- **緊急時の統一した対応体制の構築**
  サイバー攻撃等の事案に対しても、災害時と同様に、緊急時の統一した対応体制の中で対応したことで、事案の覚知後、迅速にサービス停止の判断を実施、被害の拡大防止へつながった。
- **適時・的確な情報発信**
  緊急時対処マニュアルに基づき、迅速に第一報を公表し、その後も適宜必要なタイミングで情報を公表したことで、被害の早期発見へつながった。また、同じ連携サービスを提供していた他の重要インフラ事業者の対応にも貢献した。
- **他事業者と連携するサービスの仕様変更時のリスク評価**
  他事業者と連携するサービスを提供する際には、それぞれのサービスの仕様変更が脆弱性を生む可能性があることを認識し、双方で情報共有を密に行い、都度必要に応じてリスク評価等を実施することが重要である。

事例5　重要インフラ事業者における2度のランサムウェア感染

- 重要インフラ事業者の職員が、サーバーのデスクトップ上のファイルが暗号化されていることを認識。原因は、ランサムウエアの感染で、当該ランサムウエアは機密情報の窃取を伴うものではなかった。
- 重要インフラ事業者は、本事案の半年前にも、サーバーがランサムウエアに感染。その対策で、ファイアウォールを導入予定だったが、新型コロナ禍に伴い調達できず、2度目のランサムウエア感染が発生。



【1　背景】

- 2017年に登場したマルウエア「WannaCry」は、ファイル共有等で利用されるプロトコルSMBに関する脆弱性(MS17-010)を悪用し、感染を拡大する。
- 「WannaCry」には、感染端末上のファイルを暗号化するもの(ランサムウエア)と、暗号化を伴わないものが存在。

【2　検知】

- 重要インフラサービスに直接影響するネットワークで使用している複数の端末が、再起動を繰り返したことで、異常を把握。

【3　対処】

- システム保守事業者に端末再起動の原因調査を依頼。
- システム担当部署の職員が、端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断。
- 感染端末を特定し、ネットワークからの切り離しを実施。
- 感染端末は、クリーンインストール後にセキュリティアップデートを実施したうえでネットワークに再接続。

【4　原因】

- グローバルIPアドレスを割り当てた端末をインターネットに接続した際、適切な対策を講じていなかったことから、脆弱性を悪用され、「WannaCry」に感染。
- 「WannaCry」に感染した端末を、重要インフラ事業者のネットワークに接続、同ネットワーク内のパッチ未適用のシステム監視用サーバーを経由して、別のネットワークの端末に「WannaCry」の感染が拡大した。

【5　再発に備えた対策】

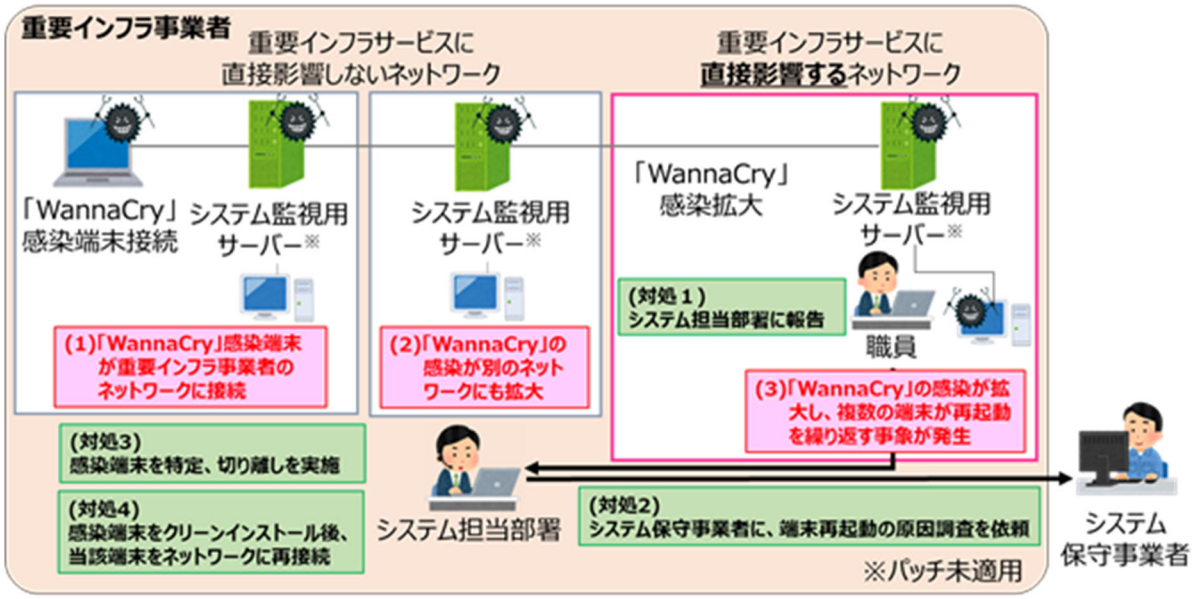
- 各ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように設定。
- 利用が終了した端末はクリーンインストールを必ず実施し、端末をネットワークに再接続する際には、ウイルス対策ソフトによるスキャンを必須とするように組織内のルールを変更。

【6　得られた気付き・教訓】

- **パッチ適用が困難な端末等に対する適切な管理策の検討**
  システムの制約上、迅速なセキュリティパッチ適用が困難な端末等について、不必要な通信の遮断、異常を早期に検知・対処できる仕組みの導入、定期的なバックアップの取得などの適切な管理策を検討し、対策を講じることが重要。
- **ネットワークに感染の恐れのある端末を接続する仕組みの検討**
  職場のネットワークに感染の恐れのある端末が接続されないようにするためには、検疫システムの導入を検討することが重要。システムの導入が難しい場合は、端末再利用時のルール(端末再利用時には、クリーンインストールやウイルス対策ソフトによるスキャンを必須化すること)を検討し、実施することが重要。
- **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は、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。
- **迅速に感染端末を特定する仕組みの検討**
  事案発生時に早期に影響範囲を特定し、対処するためには、EDR等の迅速に感染端末を特定する仕組みが重要。

事例6　重要インフラ事業者における「WannaCry」の感染

- 重要インフラ事業者のネットワークに、マルウエア「WannaCry」に感染した端末が接続、各ネットワークに設置しているパッチ未適用のシステム監視用サーバーを経由して、「WannaCry」の感染が拡大
- 本事案においては、すべての端末において、「WannaCry」によるファイルの暗号化は発生しなかった
- 重要インフラ事業者のシステム担当部署の職員が、感染端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断、ネットワークからの切り離しを実施



【1　背景】

- 2017年に登場したマルウエア「WannaCry」は、ファイル共有等で利用されるプロトコルSMBに関する脆弱性(MS17-010)を悪用し、感染を拡大する。
- 「WannaCry」には、感染端末上のファイルを暗号化するもの(ランサムウエア)と、暗号化を伴わないものが存在。

【2　検知】

- 重要インフラサービスに直接影響するネットワークで使用している複数の端末が、再起動を繰り返したことで、異常を把握。

【3　対処】

- システム保守事業者に端末再起動の原因調査を依頼。
- システム担当部署の職員が、端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断。
- 感染端末を特定し、ネットワークからの切り離しを実施。
- 感染端末は、クリーンインストール後にセキュリティアップデートを実施したうえでネットワークに再接続。

【4　原因】

- グローバルIPアドレスを割り当てた端末をインターネットに接続した際、適切な対策を講じていなかったことから、脆弱性を悪用され、「WannaCry」に感染。
- 「WannaCry」に感染した端末を、重要インフラ事業者のネットワークに接続、同ネットワーク内のパッチ未適用のシステム監視用サーバーを経由して、別のネットワークの端末に「WannaCry」の感染が拡大した。

【5　再発に備えた対策】

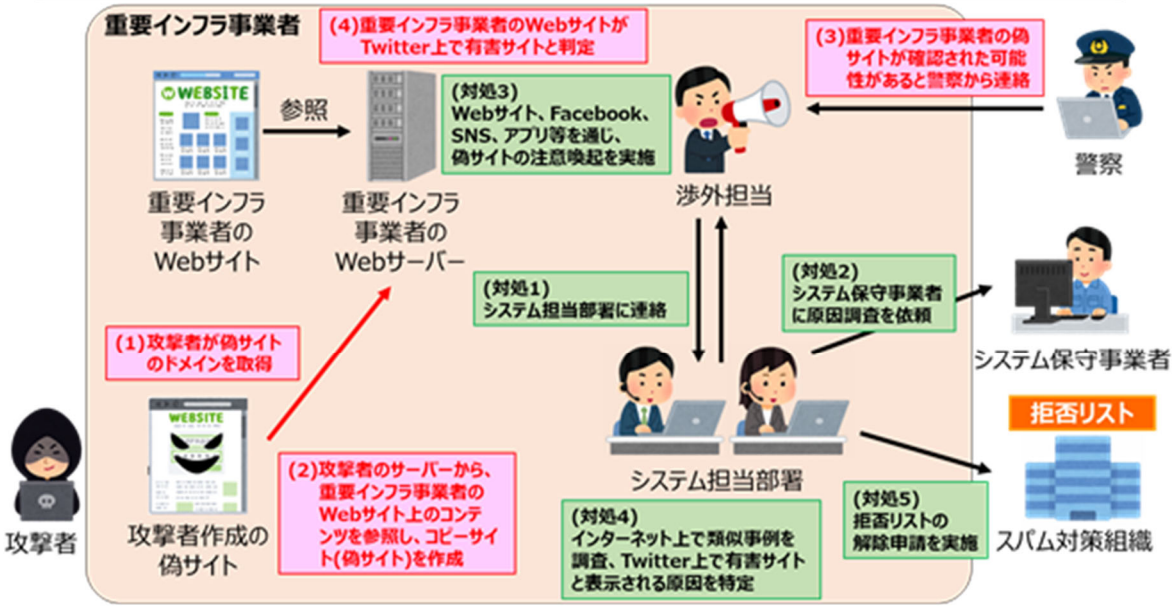
- 各ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように設定。
- 利用が終了した端末はクリーンインストールを必ず実施し、端末をネットワークに再接続する際には、ウイルス対策ソフトによるスキャンを必須とするように組織内のルールを変更。

【6　得られた気付き・教訓】

- **パッチ適用が困難な端末等に対する適切な管理策の検討**
  システムの制約上、迅速なセキュリティパッチ適用が困難な端末等について、不必要な通信の遮断、異常を早期に検知・対処できる仕組みの導入、定期的なバックアップの取得などの適切な管理策を検討し、対策を講じることが重要。
- **ネットワークに感染の恐れのある端末を接続する仕組みの検討**
  職場のネットワークに感染の恐れのある端末が接続されないようにするためには、検疫システムの導入を検討することが重要。システムの導入が難しい場合は、端末再利用時のルール(端末再利用時には、クリーンインストールやウイルス対策ソフトによるスキャンを必須化すること)を検討し、実施することが重要。
- **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は、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。
- **迅速に感染端末を特定する仕組みの検討**
  事案発生時に早期に影響範囲を特定し、対処するためには、EDR等の迅速に感染端末を特定する仕組みが重要。

事例7　重要インフラ事業者の偽サイトの確認

- 重要インフラ事業者のWebサイトをコピーしたサイトが確認された可能性がある旨、警察から連絡があり、調査したところ、偽サイトであることが判明したため、Webサイト、Facebook等で利用者に注意喚起を実施。
- 後日、上記の件が影響し、重要インフラ事業者のWebサイトがスパム対策組織により有害サイトと判定されたことから、重要インフラ事業者は、同組織が管理する拒否リストの解除申請を実施。



【1　背景】

- 本事案発生当時、国内外の事業者等のWebサイトをコピーした偽サイトが相次いで発見される事象が発生。

【2　検知】

【事象①：偽サイトが作成された事案】

- 重要インフラ事業者が、同事業者の偽サイトが確認された可能性があると警察から連絡を受け、事案が判明。

【事象②：Webサイトが有害サイトと判定された事案】

- 重要インフラ事業者の職員が、同事業者のTwitterを確認した際、ツイート内の同事業者のWebサイトへのリンクが有害サイトに判定されていたことで、事案が判明。

【3　対処】

【事象①：偽サイトが作成された事案】

- Webサイトの保守事業者に原因調査を依頼。
- 事業者のWebサイト、Facebook、SNS、アプリ等を通じて、偽サイトの確認に関する注意喚起を実施。

【事象②：Webサイトが有害サイトと判定された事案】

- 過去の他事業者の類似事案をインターネットで調査。
- スパム対策組織に対し、拒否リストの解除申請を実施。

【4　原因】

【事象①：偽サイトが作成された事案】

- 攻撃者が、自身が保有するサーバーから、重要インフラ事業者のWebサイト上のコンテンツを参照することで、コピーした偽サイトが作成された。

【4　原因】

【事象②：Webサイトが有害サイトと判定された事案】

- 重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、そのリストを参照していると思われるTwitterが、同ドメインを有害サイトに判定した。

【5　再発に備えた対策】

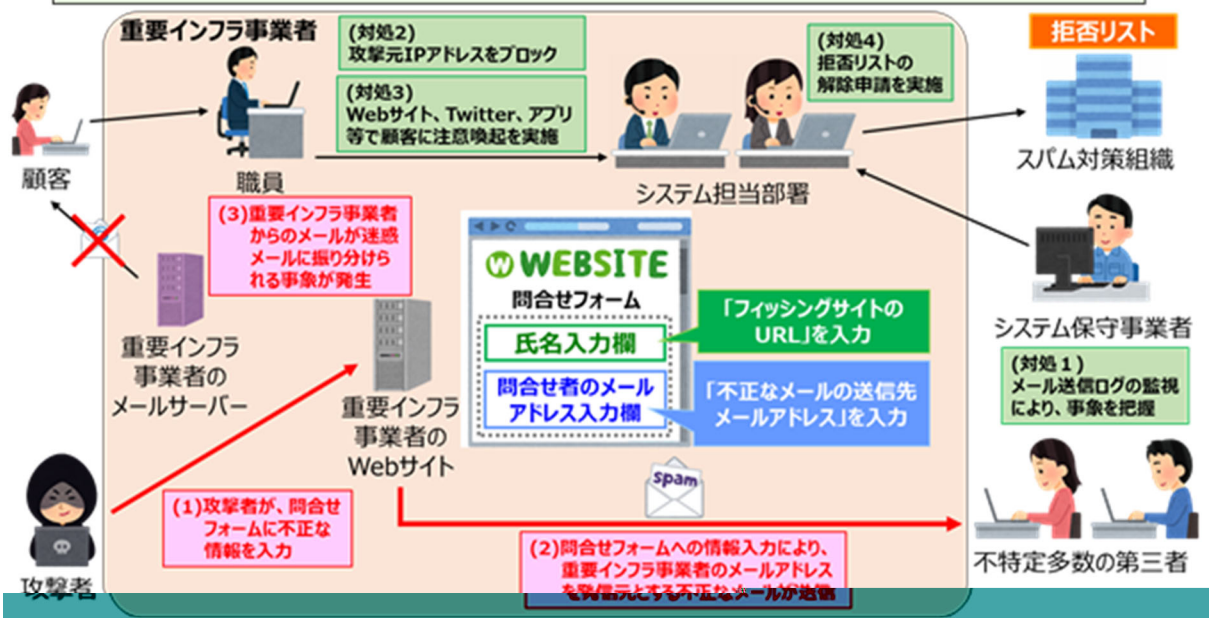
- 攻撃者のサーバーから、事業者の保有するWebサーバーへのリクエストがあった場合、ページを表示しないようアクセス制御を実施。

【6　得られた気付き・教訓】

- **サイバー攻撃事案にかかる情報の定期的な収集**
  サイバー攻撃にかかる対応では、過去の類似事案が参考になることも多いため、情報共有体制への参画等を含めた日頃から定期的に情報を収集・入手できる体制の確保が必要。
- **スパム対策組織の拒否リストの迅速な確認**
  自組織のWebサイトが有害サイトと判定された場合は、原因を特定、取り除いた後に、スパム対策組織の拒否リストに自組織のドメインが追加されていないか迅速に確認することが必要。
- **アクセス制御の適切な実施**
  自組織が管理するサーバー、ネットワーク機器等について、不正アクセスを防止するため、ファイアウォール等で適切にアクセス制御を実施し、任意のIPアドレスからは必要最小限の操作以外できないようにする、不正なIPアドレスからの通信は迅速に遮断する等の対策を講ずることが必要。

事例8　問合せシステムを悪用した不正なメールの送信

- 重要インフラ事業者のWebサイトに設置していた問合せフォームが踏み台として利用され、同事業者のメールアドレスから、不特定多数の第三者に不正なメール(フィッシングメール)が送信された。
- 後日、同事業者のドメインがスパム対策組織の拒否リストに追加されたことを契機に、同事業者が送信したメールが迷惑メールに振り分けられ、重要インフラ事業者の顧客に正しく届かない事象が発生。



【1　背景】

- 重要インフラ事業者では、同事業者のWebサイト上に、顧客からの問合せを受け付ける問合せフォームを設置。
- 重要インフラ事業者では、システム監視の一環で、メール送信ログを監視していた。

【2　検知】

【事象①：不正なメールが多数送信された事象】

- メール送信ログの監視により、同事業者のメールアドレスから、大量のメールが送信される事象を検知。

【事象②：同事業者のメールが正しく届かない事象】

- 顧客から、同事業者のドメインから送信したメールが、迷惑メールフォルダに振り分けられるとの連絡を受領。

【3　対処】

【事象①：不正なメールが多数送信された事象】

- 攻撃元IPアドレスをブロックした。
- 事業者のWebサイト、Twitter、アプリ等を通じて、本事象に関する注意喚起を実施。

【事象②：同事業者のメールが正しく届かない事象】

- スパム対策組織に対し、拒否リストの解除申請を実施。

【4　原因】

【事象①：不正なメールが多数送信された事象】

- 攻撃者が、問合せフォームの氏名入力欄に「フィッシングサイトのURL」を、問合せ者のメールアドレス入力欄に「不正なメールの送信先メールアドレス」を入力したため、問合せ受付メール(不正なメール)が第三者に届いた。

【4　原因】

【事象②：同事業者のメールが正しく届かない事象】

- 重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、同事業者が外部に送信した一部のメールが正しく届かない等の事象が発生した。

【5　再発に備えた対策】

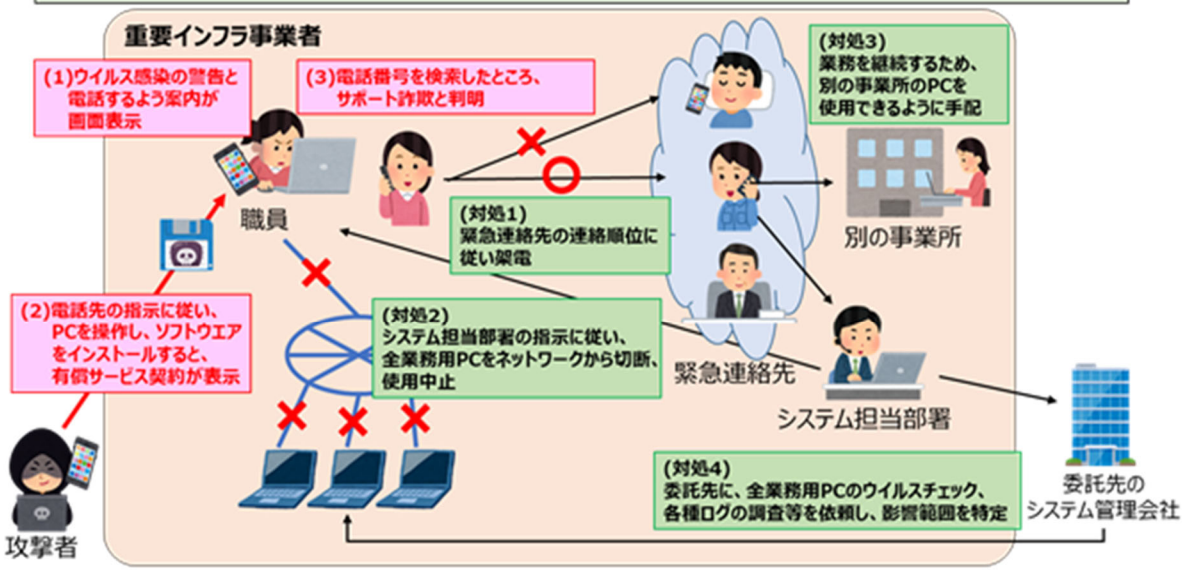
- 問合せフォームへの投稿が人間によるものか機械によるものかを判定する技術(CAPCHA)の導入。
- 連続投稿を防止する機能の追加等、一部プログラムを改修。

【6　得られた気付き・教訓】

- **平時におけるインシデント対処要員の育成**
  インシデント対処に関わる全要員に対して、CYDER等のサイバー防御演習の受講を義務付けていたことで、対処時における行動イメージが明確になり、当該事案でも各要員が迅速に情報を整理、関係者に対応状況を正確かつわかりやすく報告できた。
- **複数経路での情報発信**
  重要インフラ事業者が、複数経路(Webサイト、Twitter、アプリ等)で注意喚起情報を発信したことで、顧客に迅速に正確な情報を伝えることができ、大きな混乱も生じなかった。
- **スパム対策組織への迅速な拒否リスト解除申請**
  自組織のメール環境が悪用された場合、スパム対策組織の拒否リストに、自組織のドメインが追加される可能性があるという認識の下、先回りして拒否リストへの追加有無を確認することで、迅速に解除申請を実施でき、業務影響を抑えることが可能。

事例9　業務用PCにおけるサポート詐欺

- 被害組織の職員が、夜間、業務用PCでWeb閲覧した際、警告音が鳴り、ウイルス感染の警告と指定の電話番号へ連絡するよう案内が画面表示された。表示の電話番号へ連絡し、電話先の指示に従いPC操作を行うと、有償のサービス契約の情報が画面表示。
- 職員が不審に思い、同僚に相談、電話番号を検索したところ、サポート詐欺と判明。
- 再発防止として業務用PCを使う全職員に対し、最新の攻撃事例を交えたセキュリティ教育を定期的に実施。



【1　背景】

- Web閲覧時、偽のセキュリティ警告を画面表示等し、電話をかけさせ、PC遠隔操作等のソフトウエアのインストールを促し、対応費用としてプリペイドカード等を搾取する事案(サポート詐欺)が相次ぎ発生している。
- 被害組織の職員が、夜間、業務用PCでWeb閲覧した際、ウイルス感染の警告画面が表示され、警告音が鳴り、指定の電話番号へ連絡するよう画面表示された。
- 指定の電話番号へ連絡し、電話先の指示に従いPC操作を行うと、有償サービス契約が画面表示された。

【2　検知】

- 職員が不審に思い、同僚に相談し、指定の電話番号を検索したところ、サポート詐欺であることが判明した。

【3　対処】

- 職員は緊急時の連絡体制の連絡順位に従い、緊急連絡先に架電し、その後、システム担当部署の指示に従い、職員らは該当PCを含む被害組織内の全業務用PCをネットワークから切断、同PCを使用中止にした。
- システム担当部署は、委託先のシステム管理会社に、全業務用PCについて、ウィルスチェック、各種ログ調査等を依頼し、影響範囲を特定した。
- 業務用PCが使用中止になり、職員らは業務影響を抑えるべく、代替手段として別の事業所のPCを使用した。

【4　原因】

- 職員がWeb閲覧の際、画面表示に従いサポート詐欺の電話番号に連絡した。

【5　再発に備えた対策】

- 業務用PCを使う全職員に対し、最新のサイバー攻撃事例を交えたセキュリティ教育を月1回程度、実施することとした。
- 夜間や休日でも緊急時に対応できるように、連絡体制を見直し、委託先のシステム管理会社を含む緊急時の連絡体制を再確認し、事業者内でも全職員に再周知した。

【6　得られた気付き・教訓】

- **全職員に対する最新事例を交えた定期的なセキュリティ教育**
  最新の事例を交えたセキュリティ教育を全職員に対し定期的に実施することで、職員のセキュリティ知識や意識を底上げしたうえで、サイバー攻撃被害の未然防止を図った。
- **緊急時の連絡体制の浸透**
  職員が緊急時の連絡体制を把握しており、速やかに連絡できたことで、夜間にも関わらず対応がスムーズに行えた。夜間や休日は連絡が取れないこと等を考慮し、委託先等も含めて、迅速な連絡体制を構築、浸透させておくことが重要。
- **ソフトウエアのインストール権限の最小化**
  サポート詐欺等のサイバー攻撃による被害の拡大を防ぐため、職員にソフトウエアのインストール権限を原則与えず、インストールする場合は業務上必要最小限のものをシステム担当者が確認、許可とすることが重要。
- **業務を継続するため迅速な代替手段の確保**
  インシデント対応等により業務用PCが使用中止となり、早急に代替手段を確保したことで、必要最低限のPC作業を実施でき、影響を抑えて業務を継続できた。業務継続の観点から、事前に代替手段を検討することが重要。

別添６　サイバーセキュリティ関連データ集

＜別添６－目次＞

データ 1 NICTER 観測結果

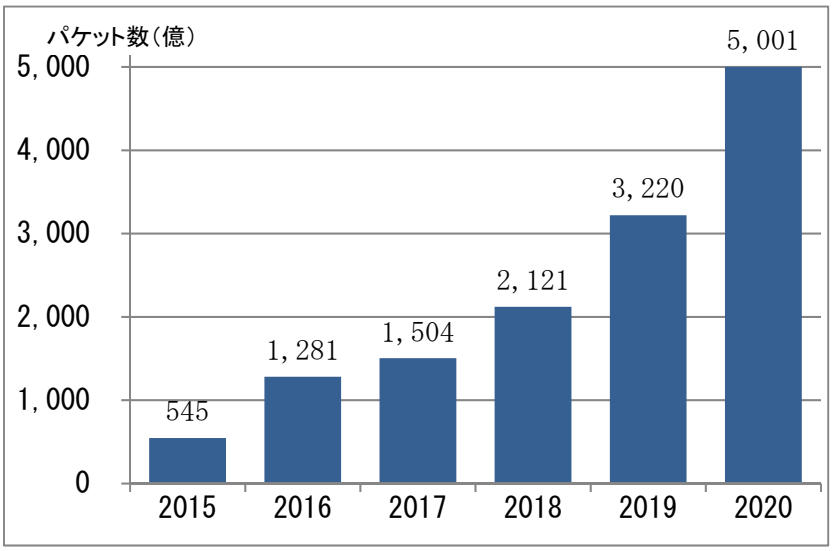
NICT において、未使用の IP アドレス 30 万個（ダークネット）を活用した大規模サイバー攻撃観測網である「NICTER」により、グローバルにサイバー攻撃の状況を観測したデータ。

詳細は「NICTER 観測レポート 2020」（https://www.nict.go.jp/cyber/report.html）を参照。

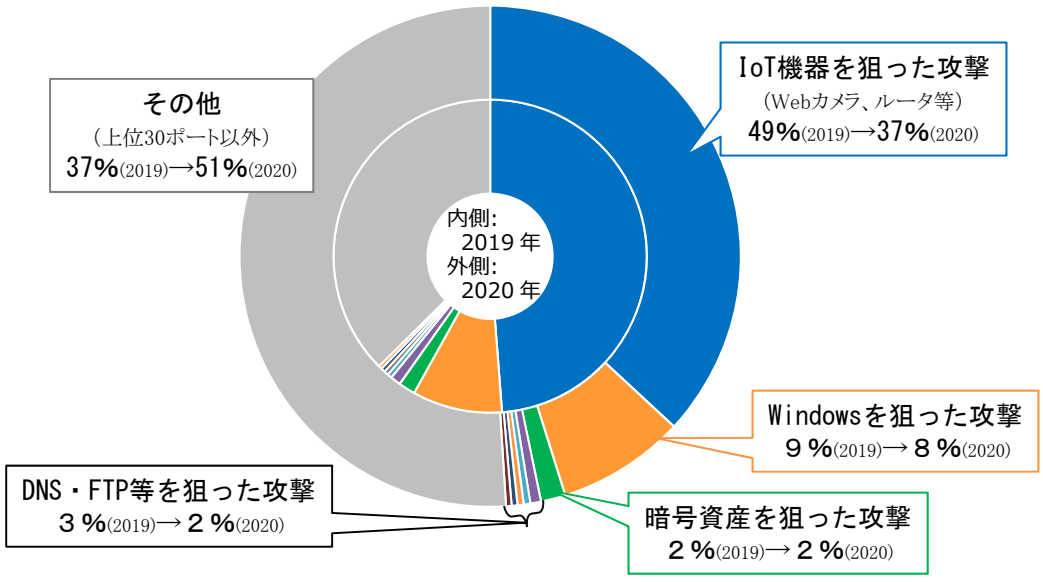
2020 年の 1 年間に観測されたサイバー攻撃関連通信は 5,001 億パケットであり、1 IP アドレス当たり 17 秒に 1 回のサイバー攻撃関連通信が観測されていることになる。

また観測された通信内容を分析すると、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 2019 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による攻撃の観測結果の内訳[1]（2019 年・2020 年）

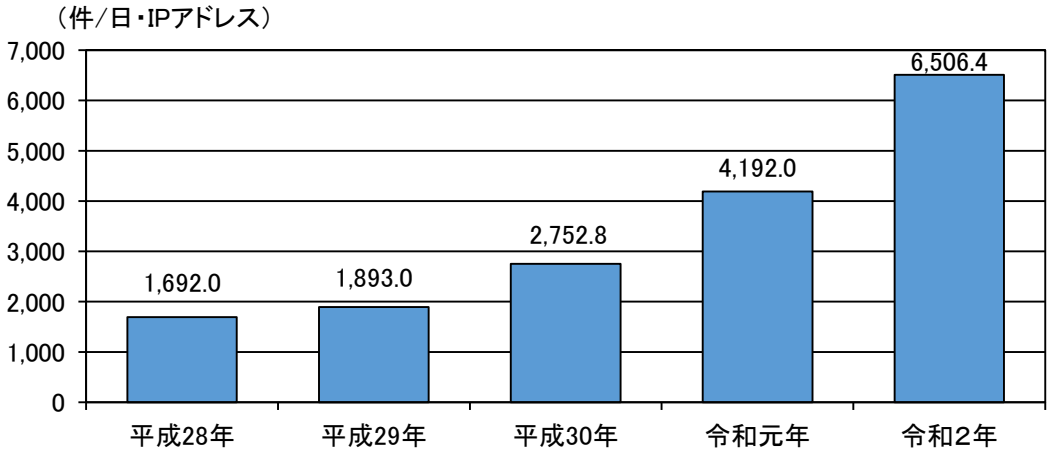


[1] NICTER で観測されたパケットのうち、調査目的パケット以外についてサービス種類（宛先ポート番号）ごとに上位 30 ポートまでを分析したもの。

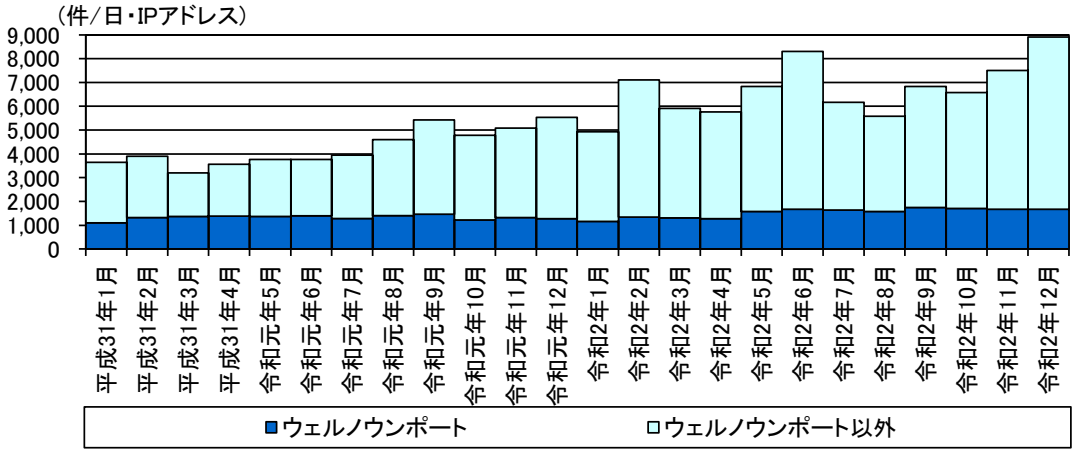
データ 2 警察庁 令和２年インターネット観測結果

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、令和元年を「前期」、令和２年を「今期」という。）

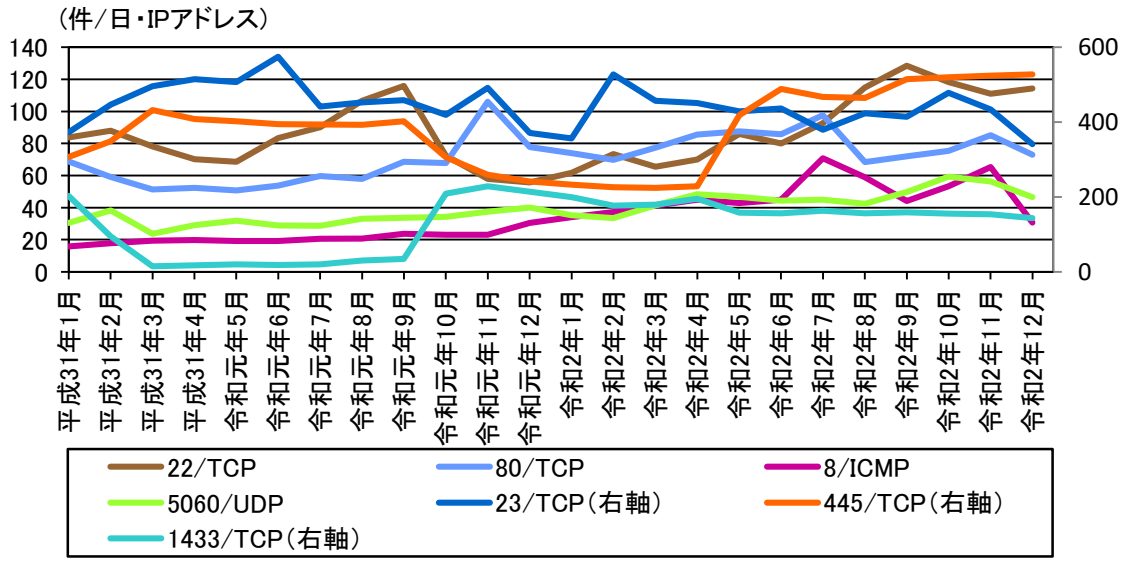
データ 2.1 センサーにおいて検知したアクセス件数の推移



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 [2]	前期比 [2]
1 位	1 位	23/TCP	426.53 件	－7.6% （－35.26 件）
2 位	2 位	445/TCP	403.61 件	＋12.9% （＋46.20 件）
3 位	3 位	1433/TCP	166.40 件	＋79.8% （＋73.87 件）
4 位	4 位	22/TCP	93.09 件	＋15.2% （＋12.27 件）
5 位	6 位	80/TCP	79.35 件	＋23.1% （＋14.88 件）

宛先ポート別検知件数（増加順位）

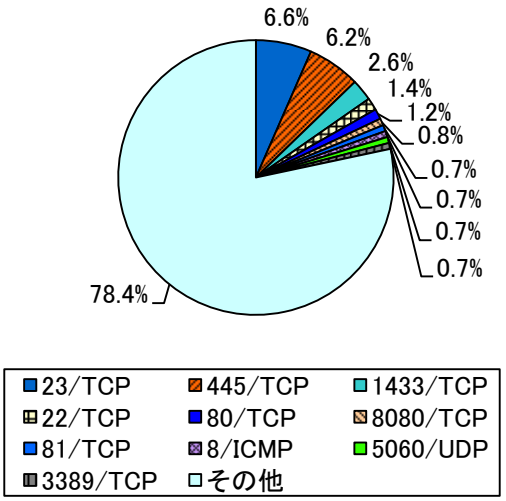
増加順位	ポート	今期件数 [2]	前期比 [2]	今期順位	前期順位
1 位	1433/TCP	166.40 件	＋79.8% （＋73.87 件）	3 位	3 位
2 位	445/TCP	403.61 件	＋12.9% （＋46.20 件）	2 位	2 位
3 位	8/ICMP	47.43 件	＋124.4% （＋26.29 件）	8 位	20 位
4 位	80/TCP	79.35 件	＋23.1% （＋14.88 件）	5 位	6 位
5 位	5060/UDP	45.80 件	＋41.2% （＋13.37 件）	9 位	14 位

宛先ポート別検知件数（減少順位）

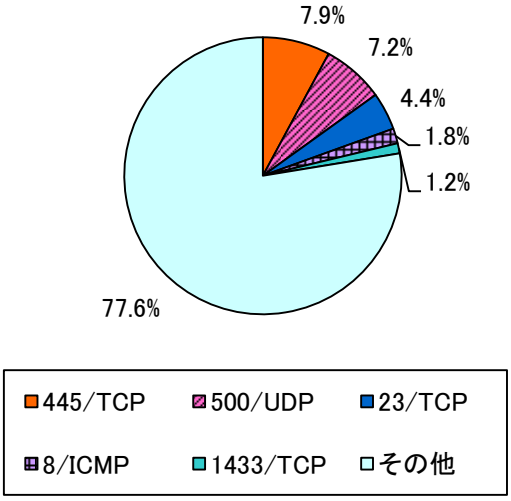
減少順位	ポート	今期件数 [2]	前期比 [2]	今期順位	前期順位
1 位	23/TCP	426.53 件	－7.6% （－35.26 件）	1 位	1 位
2 位	52869/TCP	40.31 件	－39.3% （－26.11 件）	12 位	5 位
3 位	37215/TCP	9.82 件	－65.6% （－18.69 件）	40 位	15 位
4 位	53413/UDP	25.79 件	－32.3% （－12.32 件）	17 位	12 位
5 位	60001/TCP	10.50 件	－40.0% （－7.01 件）	34 位	22 位

[2] 一日・1IP アドレス当たり。

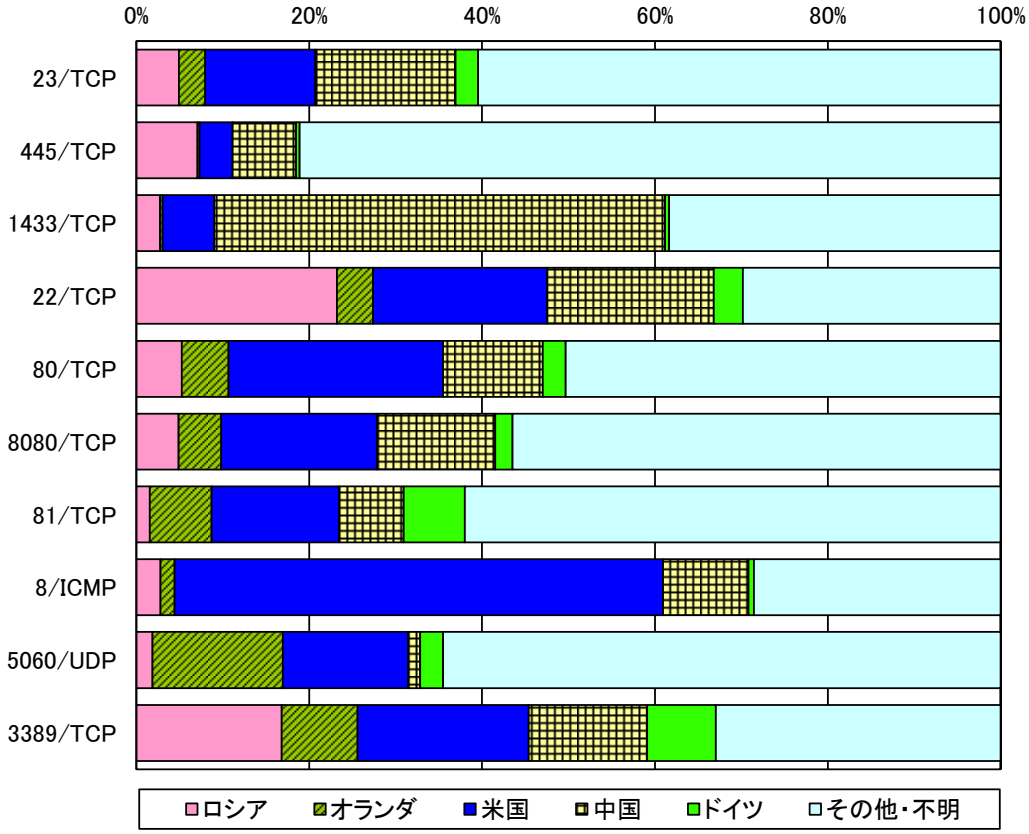
宛先ポート別比率（全て）[3]



宛先ポート別比率（日本国内）[4]

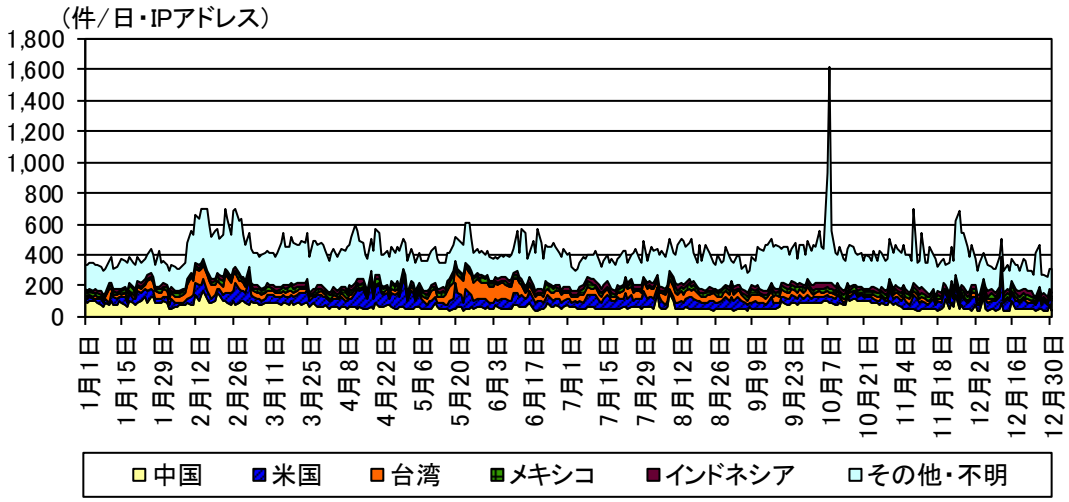


宛先ポート別上位の送信元国・地域別比率[5]

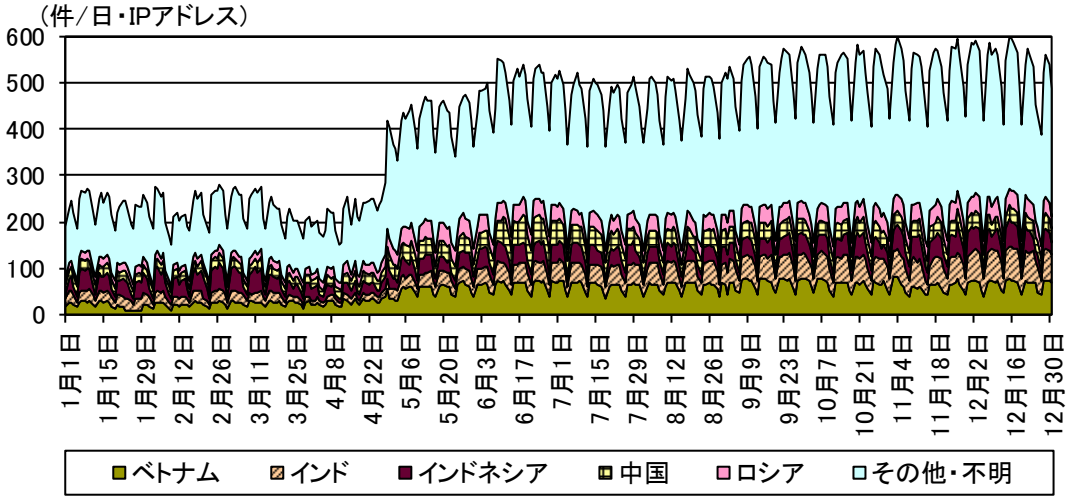


[3] 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがあります。以降の円グラフも同様。
[4] 送信元国・地域が日本国内であるもののみ集計。
[5] 送信元国・地域については、判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。以降も同様の表記。

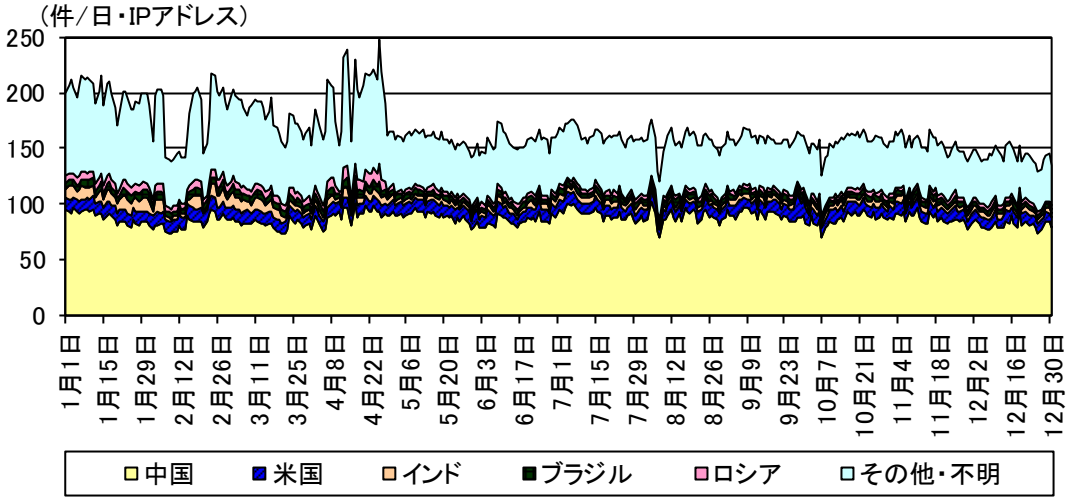
宛先ポート 23/TCP に対するアクセス件数の推移



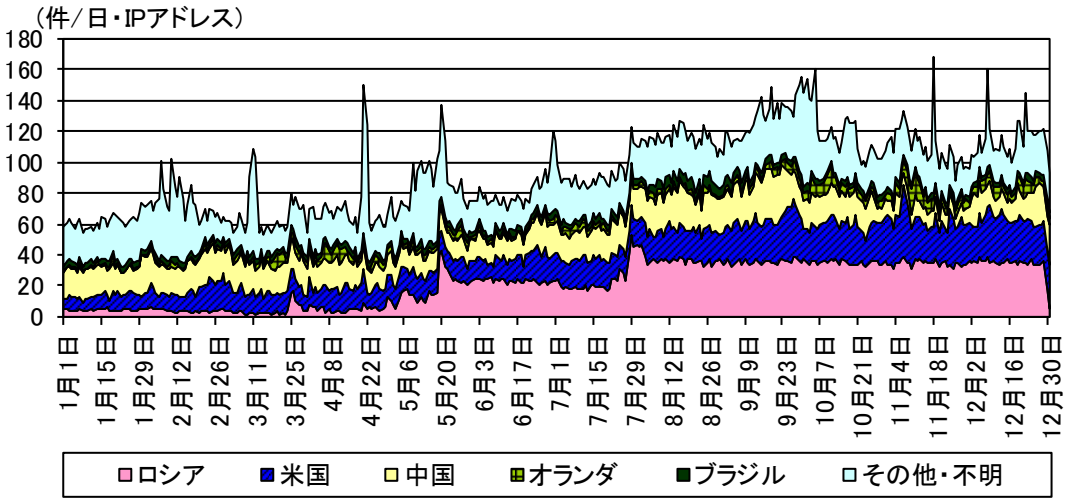
宛先ポート 445/TCP に対するアクセス件数の推移



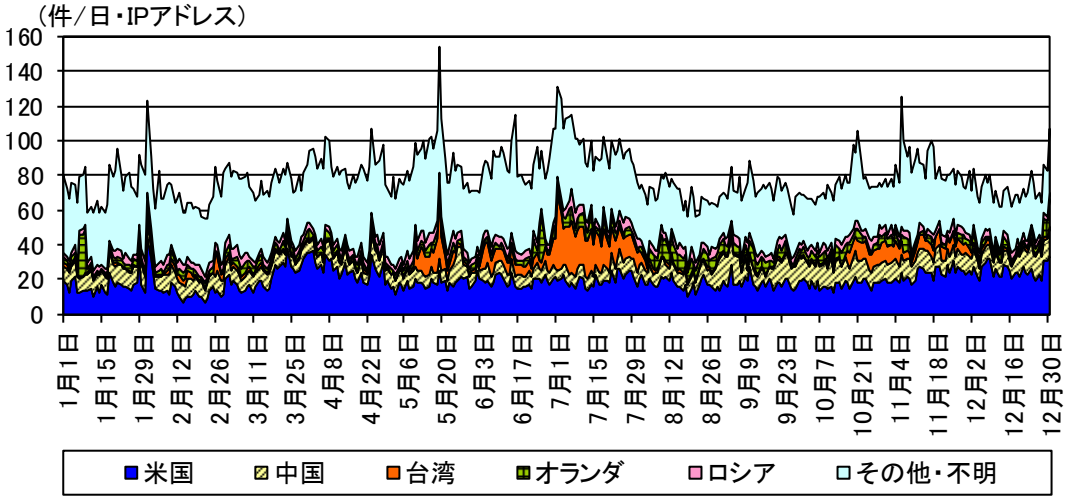
宛先ポート 1433/TCP に対するアクセス件数の推移



宛先ポート 22/TCP に対するアクセス件数の推移



宛先ポート 80/TCP に対するアクセス件数の推移



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 [6]	前期比 [6]
1 位	1 位	ロシア	1,374.23 件	＋74.9%　（＋588.31 件）
2 位	2 位	オランダ	1,118.65 件	＋57.2%　（＋406.96 件）
3 位	3 位	米国	1,038.47 件	＋78.2%　（＋455.62 件）
4 位	4 位	中国	761.92 件	＋45.9%　（＋239.75 件）
5 位	20 位	ドイツ	242.02 件	＋496.9%　（＋201.48 件）

送信元国・地域別検知件数（増加順位）

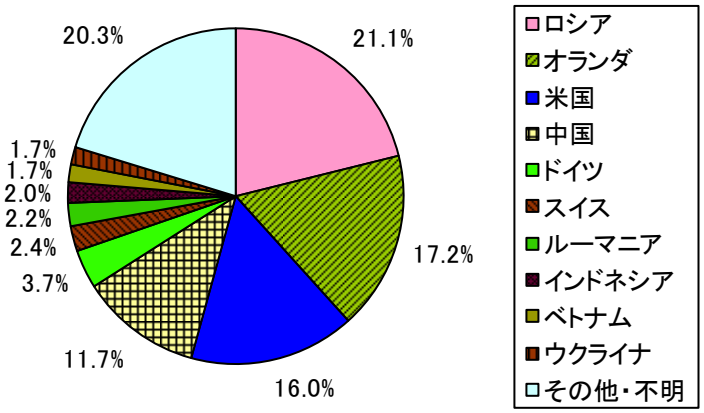
増加順位	国・地域	今期件数 [6]	前期比 [6]	今期順位	前期順位
1 位	ロシア	1,374.23 件	＋74.9%　（＋588.31 件）	1 位	1 位
2 位	米国	1,038.47 件	＋78.2%　（＋455.62 件）	3 位	3 位
3 位	オランダ	1,118.65 件	＋57.2%　（＋406.96 件）	2 位	2 位
4 位	中国	761.92 件	＋45.9%　（＋239.75 件）	4 位	4 位
5 位	ドイツ	242.02 件	＋496.9%　（＋201.48 件）	5 位	20 位

送信元国・地域別検知件数（減少順位）

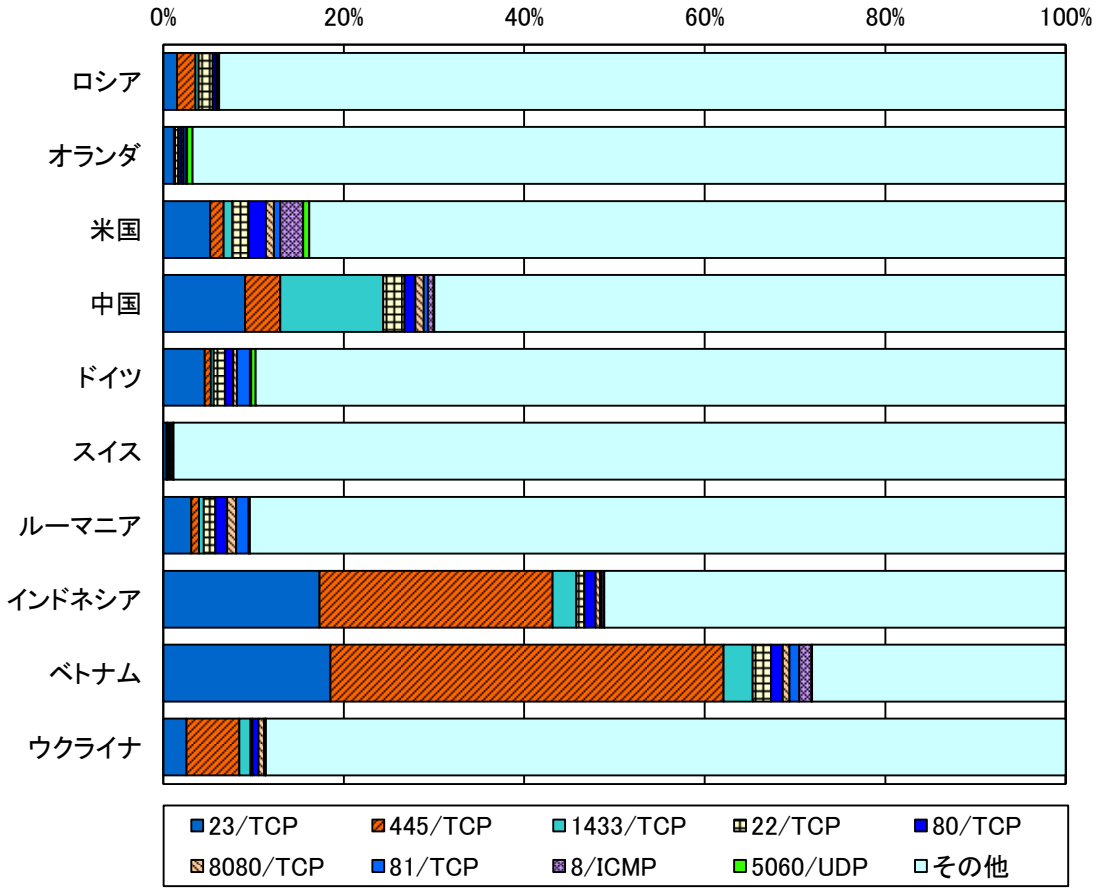
減少順位	国・地域	今期件数 [6]	前期比 [6]	今期順位	前期順位
1 位	エストニア	49.68 件	－50.4%　（－50.39 件）	20 位	6 位
2 位	スペイン	6.48 件	－84.9%　（－36.56 件）	48 位	18 位
3 位	リトアニア	22.82 件	－55.5%　（－28.45 件）	29 位	16 位
4 位	イタリア	26.91 件	－37.3%　（－16.02 件）	26 位	19 位
5 位	ラトビア	8.94 件	－49.5%　（－8.77 件）	41 位	31 位

[6] 一日・1IP アドレス当たり。

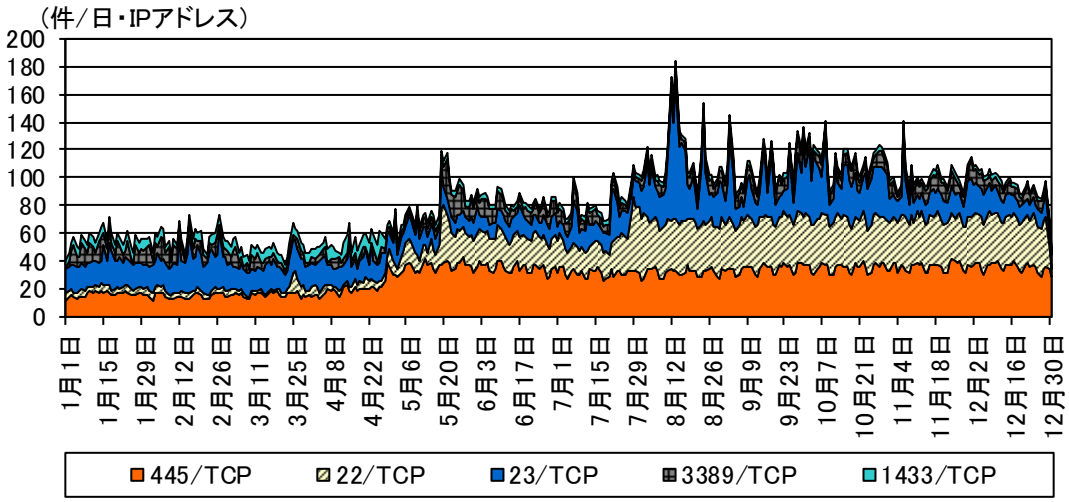
送信元国・地域別比率



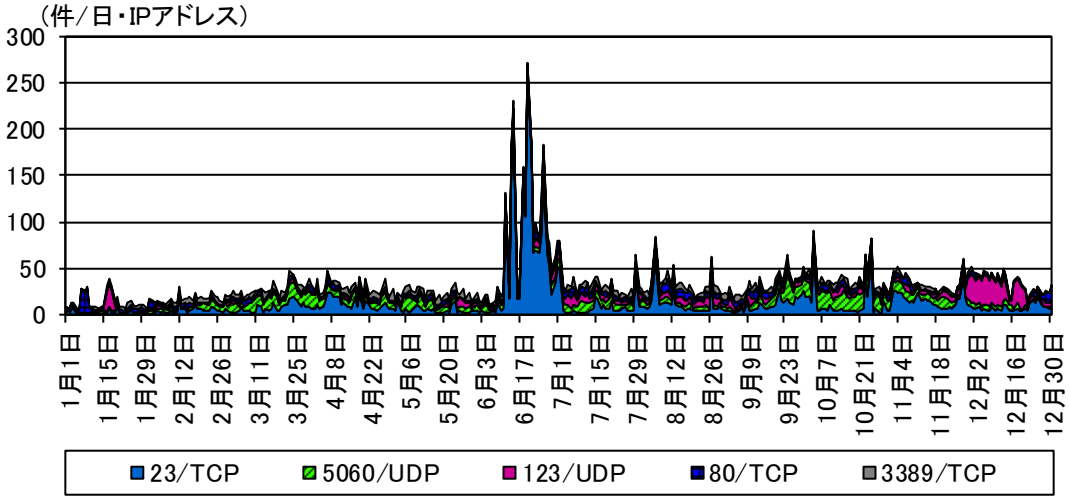
送信元国・地域別上位の宛先ポート別比率



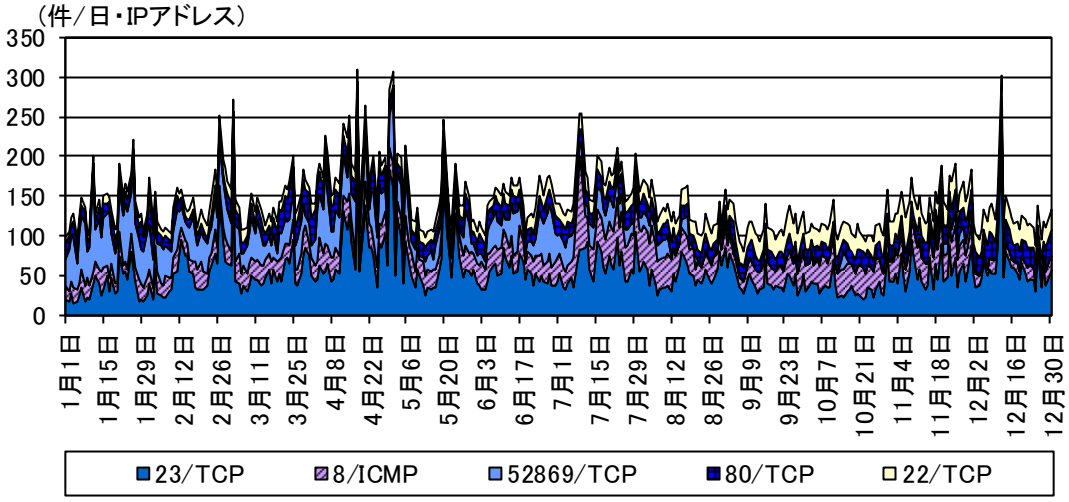
ロシアからの上位5ポートのアクセス件数の推移



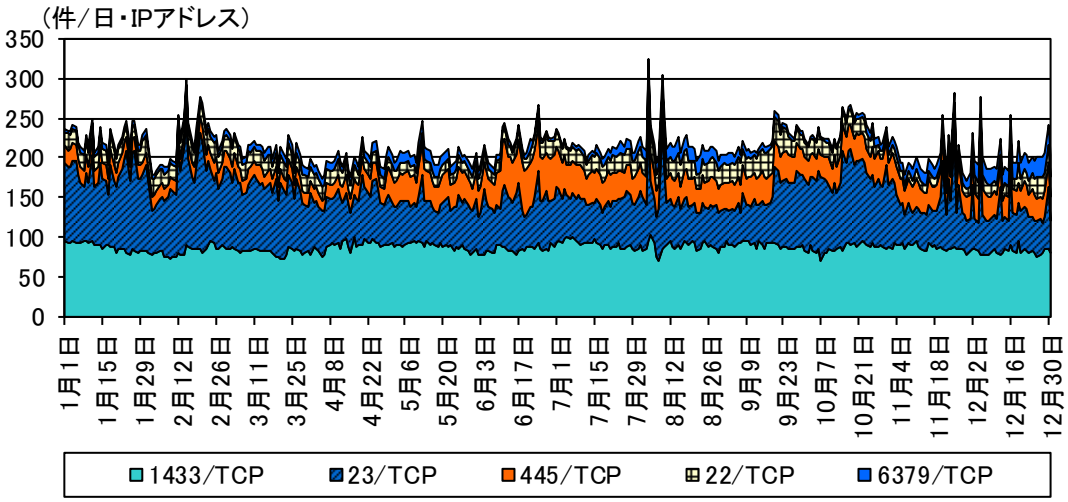
オランダからの上位５ポートのアクセス件数の推移



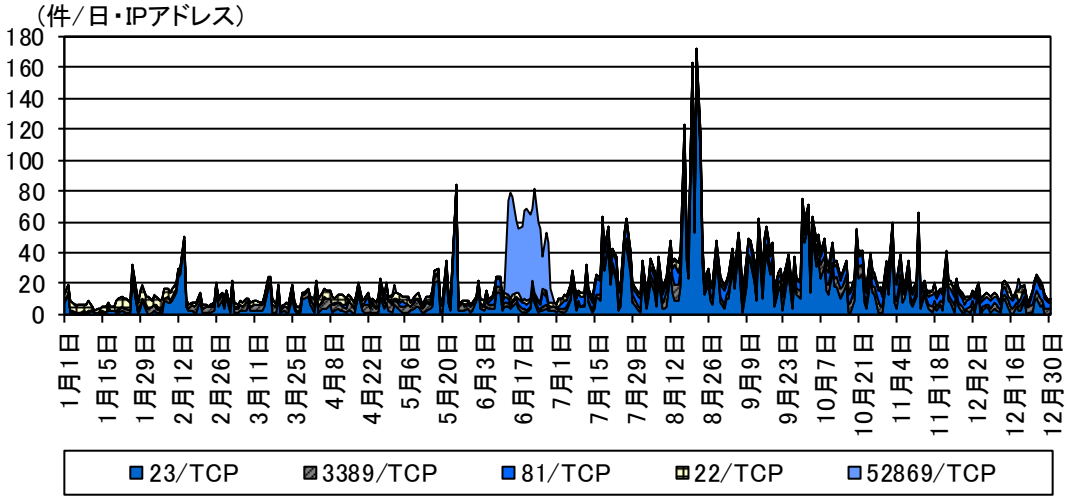
米国からの上位５ポートのアクセス件数の推移



中国からの上位５ポートのアクセス件数の推移



ドイツからの上位５ポートのアクセス件数の推移

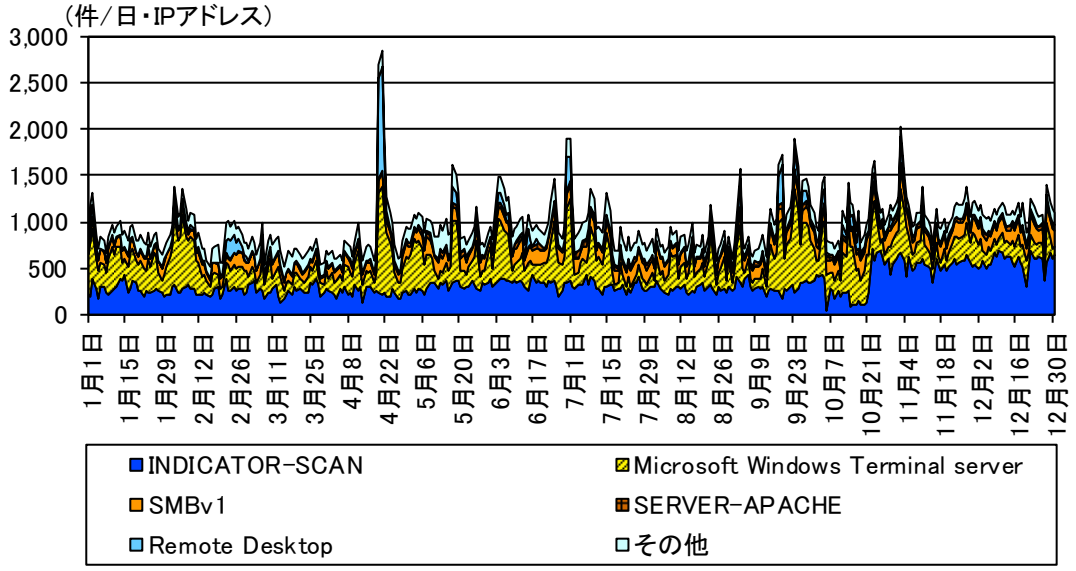


データ 2.6 不正侵入等の観測結果

不正侵入等の攻撃手法別検知件数

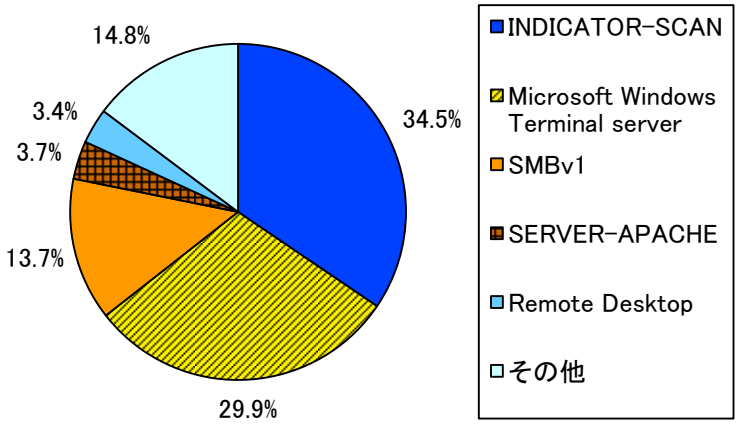
今期順位	前期順位	攻撃手法	今期件数 [7]	前期比 [7]	増加順位	減少順位
1 位	1 位	INDICATOR-SCAN[8]	332.60 件	＋1.6%　（＋5.18 件）		
2 位	2 位	Microsoft Windows Terminal server[9]	288.85 件	＋28.4%　（＋63.97 件）	1 位	
3 位	3 位	SMBv1[10]	132.56 件	－1.2%　（－1.63 件）		2 位
4 位	7 位	SERVER-APACHE[11]	35.33 件	＋222.2%　（＋24.37 件）	2 位	
5 位	4 位	Remote Desktop[12]	32.71 件	－4.4%　（－1.52 件）		3 位

不正侵入等の攻撃手法別検知件数の推移

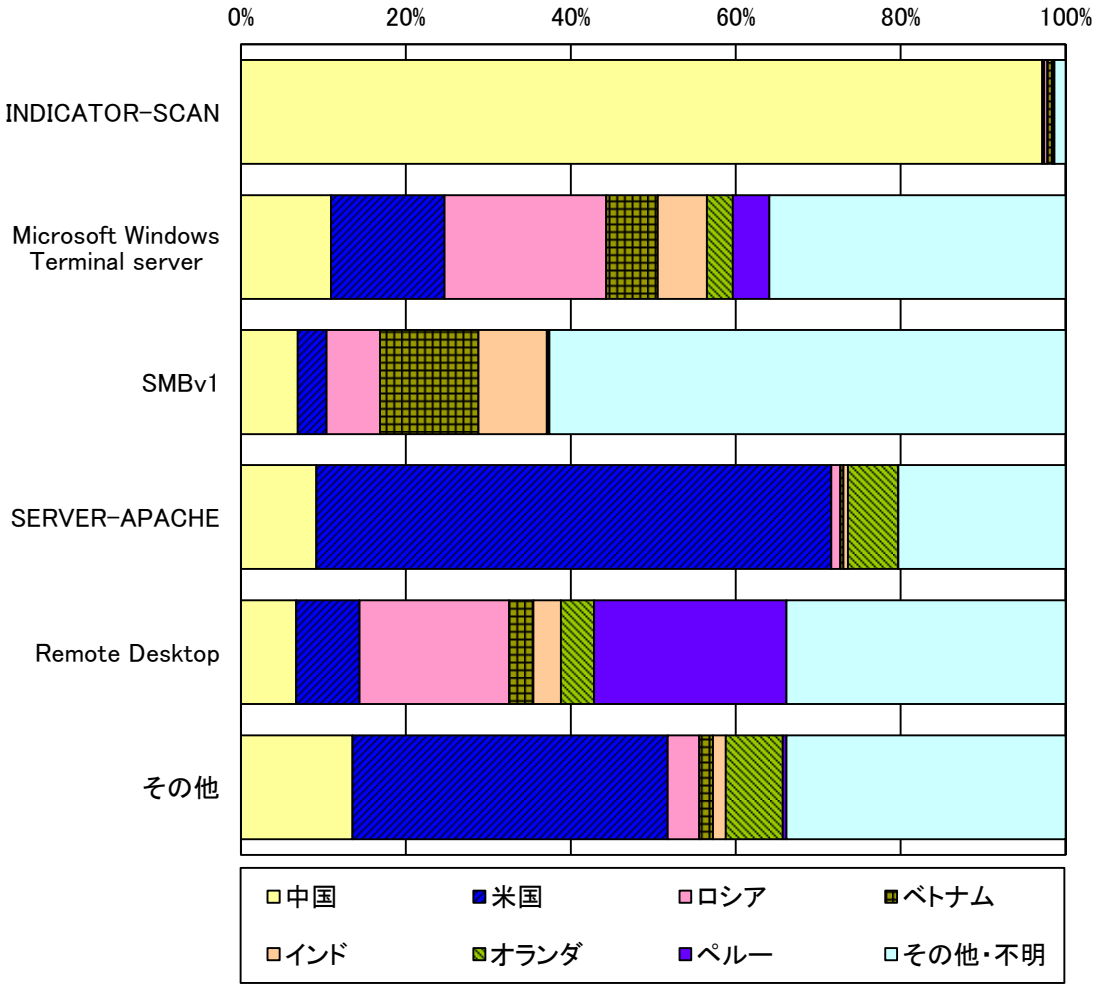


[7] 一日・1IP アドレス当たり。
[8] インターネット上の各種サービスに対するスキャン活動等の検知
[9] Windows ターミナルサービスに対するスキャン活動等の検知
[10] SMBv1 に対するスキャン活動等の検知
[11] Apache サービスに対する攻撃の検知
[12] リモートデスクトップサービスに対する攻撃の検知

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

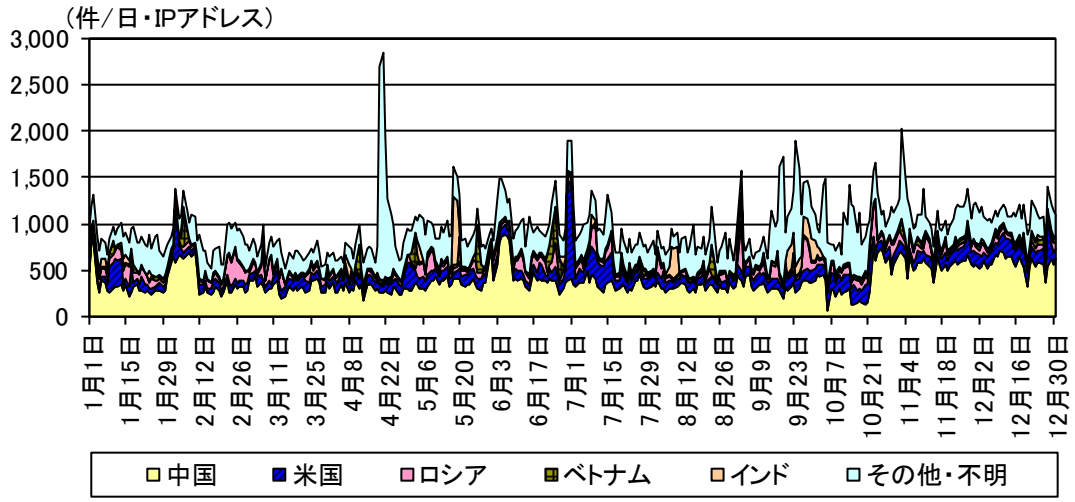


データ 2.7 送信元国・地域別アクセス検知件数

不正侵入等の送信元国・地域別検知件数（今期順位）

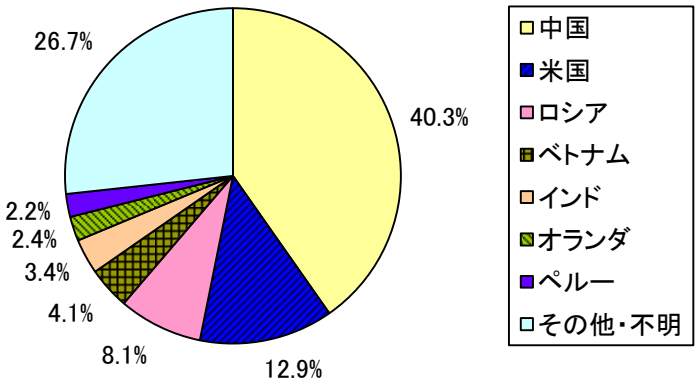
今期順位	前期順位	国・地域	今期件数[13]	前期比[13]
1 位	1 位	中国	388.45 件	＋1.0%　（＋3.96 件）
2 位	3 位	米国	124.25 件	＋100.8%　（＋62.38 件）
3 位	2 位	ロシア	78.20 件	－40.5%　（－53.12 件）
4 位	5 位	ベトナム	39.11 件	＋89.4%　（＋18.45 件）
5 位	10 位	インド	32.68 件	＋180.4%　（＋21.03 件）

不正侵入等の送信元国・地域別検知件数の推移

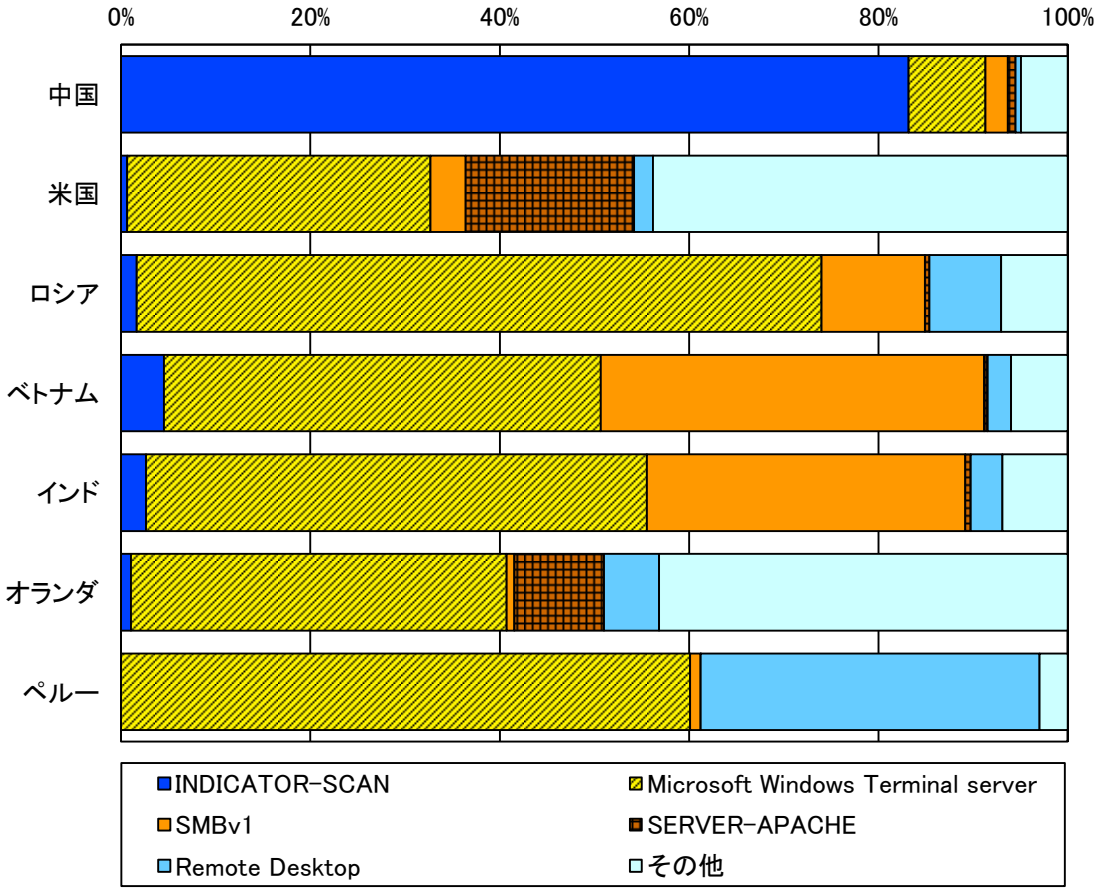


[13] 一日・1IP アドレス当たり。

不正侵入等の送信元国・地域別検知比率

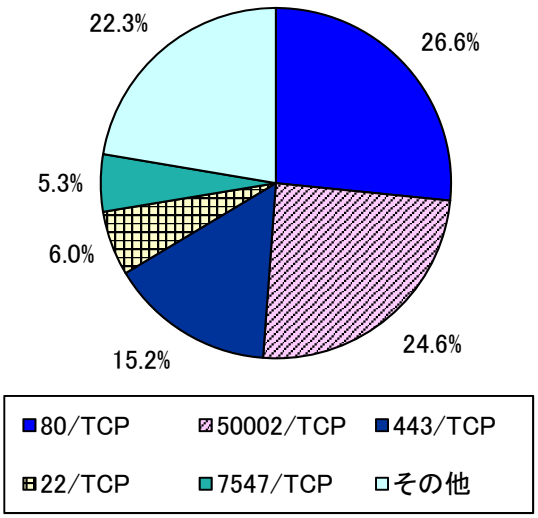


不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

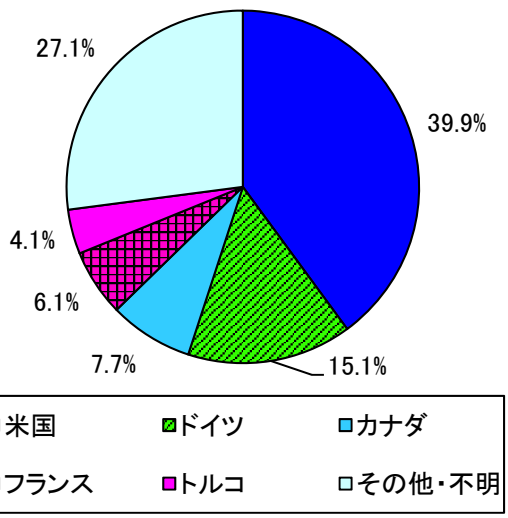


データ 2.8 DoS 攻撃被害の観測結果

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）

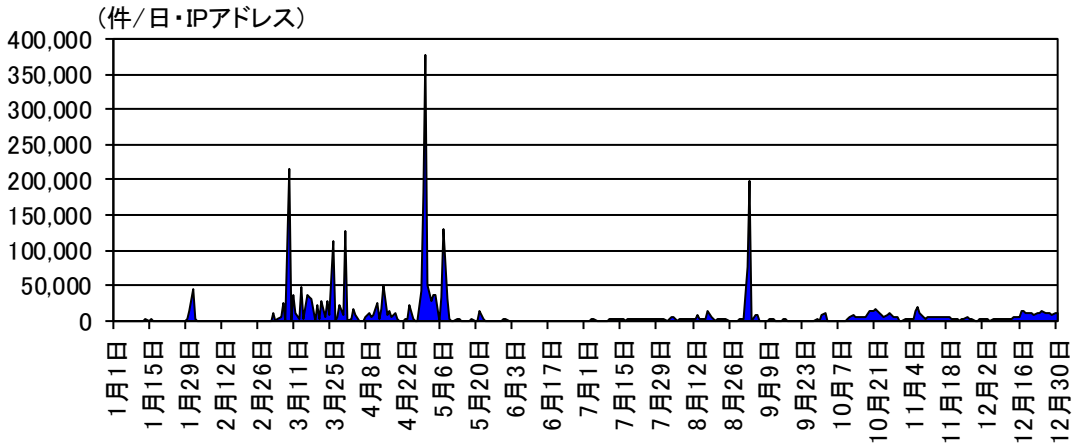
今期順位	前期順位	ポート	今期件数 [14]	前期比 [14]
1 位	1 位	80/TCP	5,857.73 件	＋52.2%　（＋2,009.94 件）
2 位	3 位	50002/TCP	5,414.95 件	＋660.8%　（＋4,703.19 件）
3 位	2 位	443/TCP	3,358.10 件	＋235.0%　（＋2,355.83 件）
4 位	15 位	22/TCP	1,315.31 件	－[15]　（＋1,265.15 件）
5 位	－[15]	7547/TCP	1,160.28 件	－[15]　（＋1,159.72 件）

跳ね返りパケットの送信元国・地域別検知件数（今期順位）

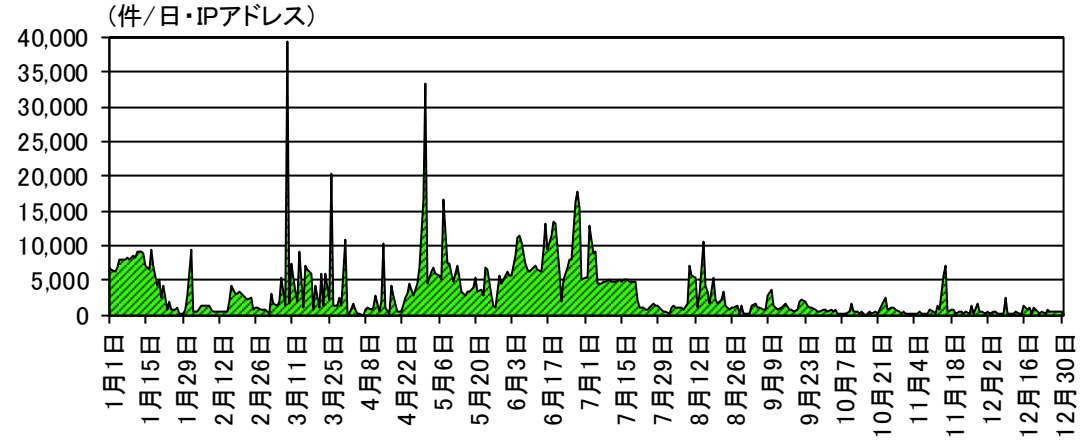
今期順位	前期順位	国・地域	今期件数 [14]	前期比 [14]
1 位	3 位	米国	8,795.25 件	＋519.6%　（＋7,375.63 件）
2 位	4 位	ドイツ	3,324.78 件	＋258.6%　（＋2,397.74 件）
3 位	2 位	カナダ	1,694.87 件	－0.9%　（－15.02 件）
4 位	5 位	フランス	1,352.14 件	＋149.9%　（＋811.02 件）
5 位	－[15]	トルコ	900.25 件	－[15]　（＋886.56 件）

[14] 一日当たり。
[15] 前期の検知件数が僅かなため、前期比及び前期順位は記載していません。

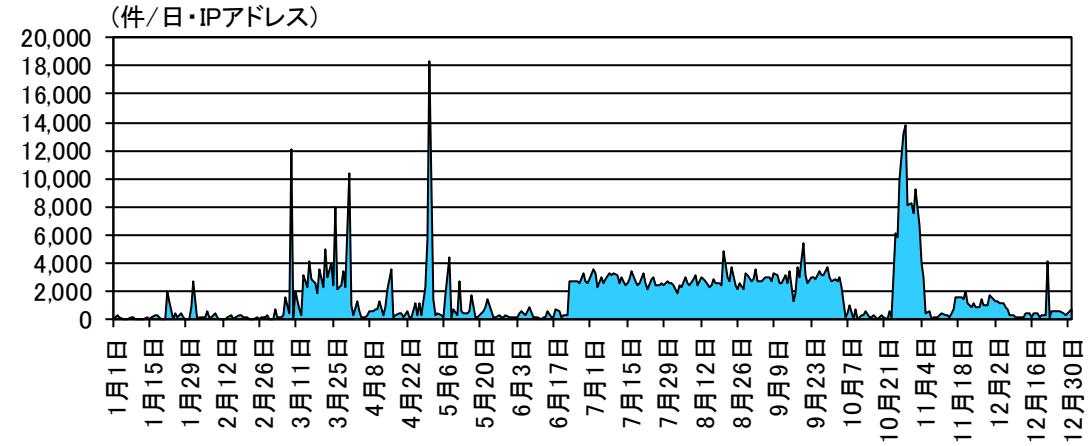
跳ね返りパケットの送信元国・地域別検知件数の推移（米国）



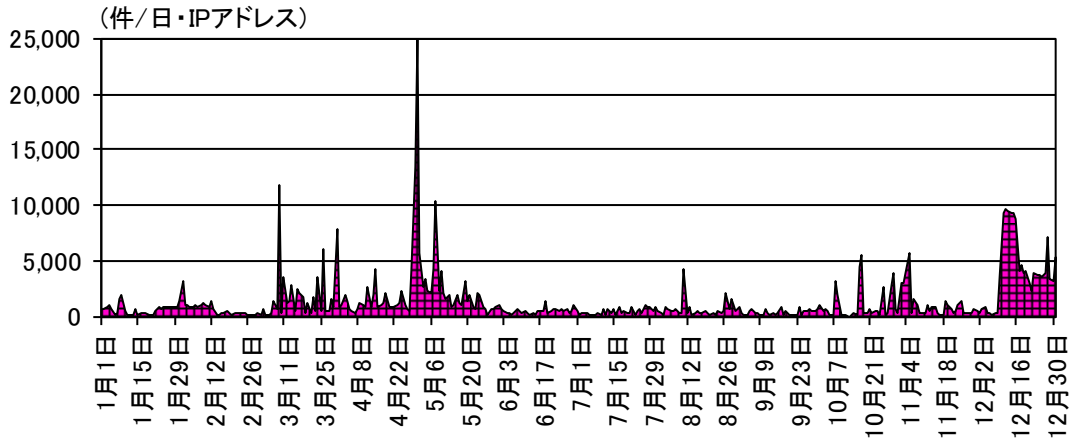
跳ね返りパケットの送信元国・地域別検知件数の推移（ドイツ）



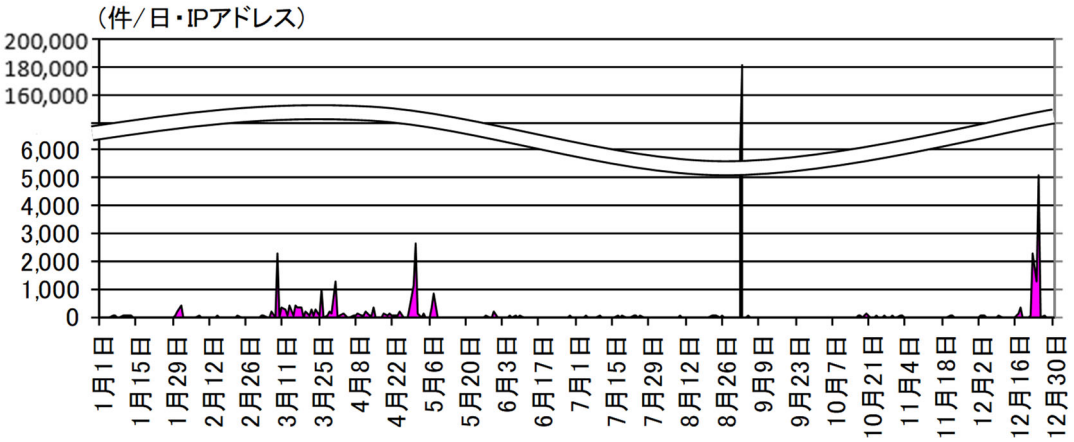
跳ね返りパケットの送信元国・地域別検知件数の推移（カナダ）



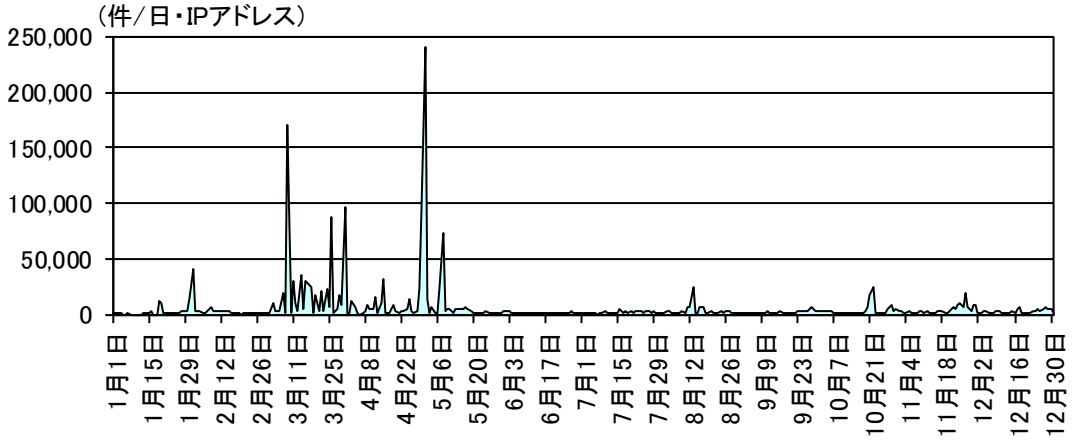
跳ね返りパケットの送信元国・地域別検知件数の推移（フランス）



跳ね返りパケットの送信元国・地域別検知件数の推移（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（その他・不明）



データ 3 JPCERT/CC 2020 年度 TSUBAME 観測動向

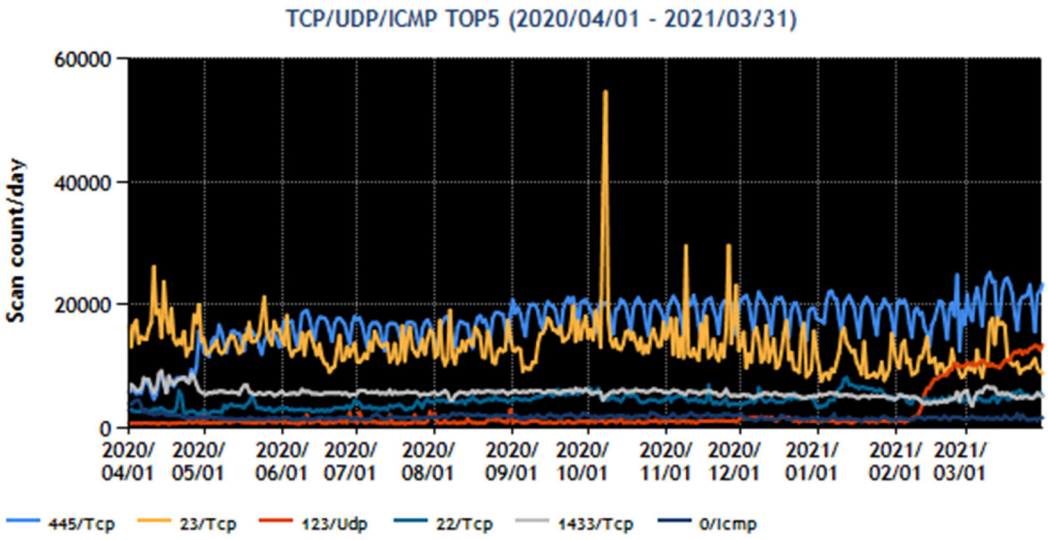
JPCERT/CC にて、不特定多数に向けて発信されるパケットを収集する観測用センサを開発し、海外の National CSIRT 等の協力のもと、これを各地域に複数分散配置した、インターネット定点観測システム（TSUBAME）を構築し運用されている。

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 のセンサで受信したパケットを宛先ポート別に集計してグラフ化し、JPCERT/CC の Web ページで公開されている（「JPCERT/CC 活動四半期レポート」（https://www.jpcert.or.jp/pr/）及び「JPCERT/CC インターネット定点観測レポート」（https://www.jpcert.or.jp/tsubame/report/））。

そのうち、TSUBAME で観測された宛先ポート別パケット数の上位１～５位及び６～10 位を１年間のアクセス先ポート別状況を抜粋して掲載。

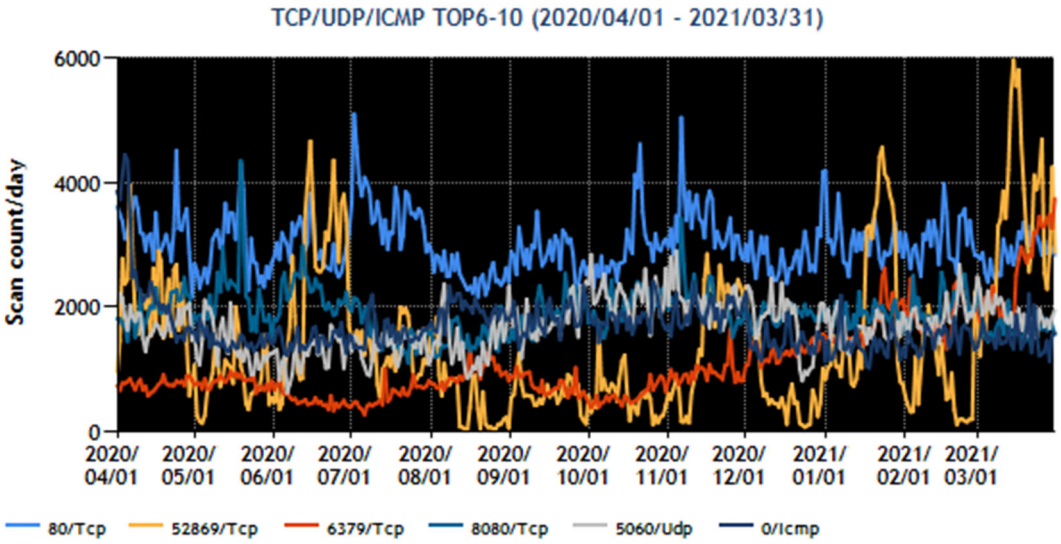
データ 3.1　宛先ポート別パケット数

宛先ポート別グラフ トップ 1-5（2020 年 4 月 1 日-2021 年 3 月 31 日）[16]



[16] 年間を通して、23/TCP(telnet)宛や、445/TCP 宛、1433/TCP 宛の通信が多くみられる。これらのパケットにはマルウェアの活動によるパケットの可能性があるため、送信元のユーザへの連絡対応等を行っている。445/TCP 宛の通信を行なっていたケースには、テレワーク用の共用スペースにおいてマルウェアに感染した Windows PC が持ち込まれ接続されていた事例があったとの報告も得た。

宛先ポート別グラフ トップ 6-10（2020 年 4 月 1 日-2021 年 3 月 31 日）



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。

平成 29 年度		平成 30 年度		令和元年度		令和2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]	合計
243	297	58,461	8,618	22,281	3,506	49,495	1,946	130,480	14,367	144,847

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。

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 登録者数	令和3年度4月1日時点 登録者数[19]
4 月登録	10 月登録	4 月登録	10 月登録	4 月登録	10 月登録	4 月登録	10 月登録	4 月登録		
4,172	2,822	2,206	8,214	1,052	1,200	1,096	307	804	21,873	20,178

[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 1,695 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。

年度＼試験区分		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

[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（2021 年度年次計画）

担当府省庁一覧

項目	担当府省庁 （◎：主担当、〇：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 〇：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 〇：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	◎：内閣官房、総務省、経済産業省 〇：法務省 ※内閣官房：情報通信技術（IT）総合戦略室
(3) セキュリティ製品・サービスの信頼性確保	◎：NISC、総務省、経済産業省
(4) 先端技術・イノベーションの社会実装	◎：NISC、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、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 〇：外務省、財務省、防衛省、その他の府省庁
(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、金融庁、消費者庁、総務省、厚生労働省、経済産業省、国土交通省 〇：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、情報通信技術（IT）総合戦略室 ※内閣府（◎）：政策統括官（科学技術・イノベーション担当） ※内閣官房（〇）：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、再生総合事務局 ※内閣府：（〇）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、内閣官房、総務省、経済産業省 ※内閣官房：情報通信技術（IT）総合戦略室
(3) サイバー犯罪への対策	◎：内閣府、警察庁、総務省、法務省、経済産業省 ※内閣府：個人情報保護委員会
(4) 包括的なサイバー防御の展開	◎：NISC、総務省
(5) サイバー空間の信頼性確保に向けた取組	◎：NISC、内閣府、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ※内閣府：個人情報保護委員会
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、内閣官房、内閣府、総務省、厚生労働省、経済産業省 ※内閣官房：情報通信技術（IT）総合戦略室 ※内閣府：番号制度担当室

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、内閣官房、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 ※内閣官房：情報通信技術（IT）総合戦略室
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、内閣府、総務省、厚生労働省 ○：内閣官房 ※内閣官房：情報通信技術（IT）総合戦略室 ※内閣府：個人情報保護委員会、番号制度担当室
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、内閣官房、警察庁、法務省 ※内閣官房：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推進本部事務局
(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、内閣府、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） ※内閣府：個人情報保護委員会
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 ※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：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 ○：警察庁、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、文部科学省、経済産業省
(2)　巧妙化・複雑化する脅威への対処	◎：総務省、文部科学省、経済産業省 ○：NISC
(3)　政府機関における取組	◎：NISC、警察庁、総務省、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、金融庁、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：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推進本部事務局、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。
	Apache Struts	Webアプリケーションを構築する際に必要となる諸機能を提供するオープンソースのフレームワーク。
	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。
	APT	Asia-Pacific Telecommunityの略。アジア太平洋電気通信共同体。アジア・太平洋地域の電気通信の開発促進及び地域電気通信網の整備・拡充を目的として1979年に設立。
	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）。セプターカウンシ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。
	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。
	CURE	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、サイバーセキュリティ研究及びセキュリティ・オペレーションの遂行に不可欠な各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等のサイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする仕組み。
	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。
	CWE	Common Weakness Enumerationの略。ソフトウェアにおける脆弱性を一意に識別するために分類しているものであり、脆弱性の原因や対策等を記載。
	CYMAT	CYber incident Mobile Assistance Teamの略（サイマット）。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。
D	DFFT	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。
	DDoS攻撃	Distributed Denial of Serviceの略。分散型サービス不能攻撃。多数のコンピュータを用いたDoS攻撃。大規模な攻撃では、遠隔操作される等により数万台以上のコンピュータが攻撃に用いられているケースもある。
	DII	Defense Information Infrastructureの略。防衛省の基盤的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。
	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。

	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。
I	icat	IPAの運営するサイバーセキュリティ注意喚起サービス。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。
	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セキュリティガイドライン	IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、2016年７月に策定。IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その関係者がセキュリティ確保の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ、明確化することによって、産業界による積極的な開発等の取組を促すとともに、利用者が安心してIoT機器やシステム、サービスを利用できる環境を生み出すことにつなげるもの。
	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。
	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障害	重要インフラの情報セキュリティ対策に係る第３次行動計画において使用された用語で、「ITの不具合のうち、重要インフラサービスの提供水準が同計画に記載された水準を下回るもの。」と規定。同第４次行動計画において、「重要インフラサービス障害」の用語に変更し、定義の明確化を図った。
	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。
	IT総合戦略本部	高度情報通信ネットワーク社会推進戦略本部のこと。ITの活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に適確に対応することの緊要性にかんがみ、高度情報通信ネットワーク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に、2001年１月、内閣に設置された。
	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-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。
	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。
	JISP	Japan cyber security Information Sharing Platformの略（ジスプ）。サイバーセキュリティ対処調整センターが提供し運用する情報共有プラットフォーム。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、参加組織からのインシデント報告に対して、要請に応じて助言及び対処支援調整を行うためのシステム。2019年４月から運用を開始している。
	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。
	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。
	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」を目指すわ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	Oracle WebLogic Server	Oracle社が開発販売するソフトウェア製品であり、Java EE（Webアプリケーション開発用の機能をセットにしたソフトウェア）でウェブアプリケーションを作成する際に利用されるアプリケーションサーバ。
	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。
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。
	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。
S	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。
	SECCON 2019	SECCON：SECurity CONtest 2019の略。情報セキュリティをテーマに多様な競技を開催する情報セキュリティイベントの2019年における名称。競技を通じた実践的情報セキュリティ人材の発掘・育成、技術実践の場の提供を目的とする。
	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発揮して、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）までを見据えて一気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。
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）」「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications）」の３つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」「１ミリ秒程度の遅延」「100万台/㎢の接続機器数」が挙げられている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	アクチュエータ	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。
	安全基準等	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」等の総称。ただし、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は含まない。

	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・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
	インシデント・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。
こ	公開鍵暗号（ISO/IEC18033-2/AMD1）	暗号化処理と復号処理で使う暗号鍵が異なるタイプの暗号方式で、復号処理で使う暗号鍵だけを秘密にしておけば暗号アルゴリズムとしての安全性が保たれ、暗号化処理で使う暗号鍵は公開してもよいという特長をもつ。
	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。
	サイバーインテリジェンス情報共有ネットワーク	サイバーインテリジェンスによる被害を防止するため、標的型メール攻撃等の情報窃取を企図したものと考えられるサイバー攻撃事案に係る情報を共有すべく、警察と情報窃取の標的となるおそれの高い先端技術を有する全国の事業者等で構成している組織。
	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、磁気的方式その他人の知覚によっては認識することができない方式（略）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（略）が講じられ、その状態が適切に維持管理されていることをいう。」とされている。
サイバーセキュリティ意識・行動強化プログラム	サイバーセキュリティ普及啓発について、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、2019年１月24日にサイバーセキュリティ戦略本部にて決定。
サイバーセキュリティお助け隊サービス	相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策を支援するサービス
サイバーセキュリティ基本法	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。
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人材育成取組方針	「サイバーセキュリティ人材育成プログラム」及び「サイバーセキュリティ戦略中間レビュー」を踏まえ、普及啓発・人材育成専門調査会及びその下に設置されたワーキンググループにおける検討の成果を取りまとめたもの。2018年６月７日にサイバーセキュリティ戦略本部に報告。
サイバーセキュリティ戦略（2018年戦略）	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、2015年９月４日に閣議決定された前戦略からのサイバー空間に係る現状認識を踏まえ、目指すサイバーセキュリティの基本的な在り方として、「持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進」を位置づけており、今後３年間の諸施策の目標及び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（2021年戦略）	2018年７月27日に閣議決定された上記2018年戦略は、2021年で計画期間を終了することから、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処調整センター	東京2020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。2019年４月１日に設置。
	サイバー犯罪条約	正式名称はサイバー犯罪に関する条約（通称ブダペスト条約）。サイバー犯罪に効果的かつ迅速に対処するために国際協力を行い，共通の刑事政策を採択することを目的とする条約。
	サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。経済産業省に設置した産業サイバーセキュリティ研究会WG1の下で検討を進め、2019年４月にVersion 1.0を策定。
	サイバーフォースセンター	警察庁情報通信局に設置。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・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社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。
	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	重要インフラの情報セキュリティ対策に係る第４次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営む者等のうち、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」における「対象となる重要インフラ事業者等」に指定された事業者及び当該事業者等から構成される団体。
	重要インフラ所管省庁	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。
	重要インフラの情報セキュリティ対策に係る第４次行動計画	重要インフラ防護に係る基本的な枠組みとして、重要インフラ防護に責任を有する政府と自主的な取り組みを進める重要インフラ事業者等との共通の行動計画を策定し、これを推進してきた。昨今のサイバー攻撃による急速な脅威の高まりや、東京2020大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。
	重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、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」。
	重要サービス事業者	東京2020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	重要インフラの情報セキュリティ対策に係る第４次行動計画における関係主体の一つ。警察庁サイバーフォースセンター、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人ICT-ISAC、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	重要インフラの情報セキュリティ対策に係る第４次行動計画における関係主体の一つ。警察庁、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
	情報通信ネットワーク安全・信頼性基準	1987年２月14日郵政省告示第73号。情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標としての基準を定めることにより、安全・信頼性対策の普及を促進し、もって情報通信ネットワークの健全な発展に寄与することを目的としているもの。
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。
	スマートホーム	IoT技術等によって家庭内の機器をネットワークでつなぎ、制御することで、生活者のニーズに応じた効率的かつ快適なサービスの提供を可能とした住まいのこと。
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・キャンプ実施協議会	次代を担う日本発で世界に通用する若年層のセキュリティ人材を発掘・育成するため、産業界、教育界を結集した講師による「セキュリティ・キャンプ」（22歳以下を対象）を実施し、それを全国的に普及、拡大していくことを目的とした協議会。なお、同協議会は2018年４月24日に「一般社団法人セキュリティ・キャンプ協議会」となったことが発表されている。
	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。2018年７月に策定された新戦略において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	CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略）。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。2005年以降順次構築が進められ、2021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	CEPTOAR-Council。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。
ち	地域SECUNITY	地域のセキュリティの関係者（公的機関、教育機関、地元企業、地元ベンダー等）が集まりセキュリティについての相談や意見交換を行うためのセキュリティコミュニティ
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	2017年４月18日総務省告示第152号。同年９月14日総務省告示第297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、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関等の情報セキュリティ対策のための統一規範」、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「政府機関等の情報セキュリティ対策のための統一基準」（平成30年７月25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」（平成30年７月25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こと。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、その当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っても、犯罪に悪用されている状態にあれば、これも犯罪インフラに含まれる。
ひ	ビジネスメール詐欺	巧妙に細工したメールのやり取りにより企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口のこと。
	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	ファイアウォール	外部のネットワークからの攻撃や不正なアクセスから自身のネットワークやコンピュータを防御するためのソフトウェアやハードウェア
	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SECUNITY）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関係する府省庁。
	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」があたる。
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に実施することで、安全性を高めること。
	リスクマネジメント	組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと。サイバー空間に本質的にある不確実さから、不可避的に導かれる観点。
	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。
	リモートデスクトップ	Microsoft Windows の遠隔操作に使用されるサービスで、主にポート3389/TCPを使用する。
	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。