資料１

サイバーセキュリティ 2020（案）

資料１－１　サイバーセキュリティ 2020（案）の全体概要

資料１－２　サイバーセキュリティ 2020（案）の概要

資料１－３　2020 年度に実施すべき施策に関する意見募集の結果の概要

資料１－４　2020 年度に実施すべき施策に関する意見募集の結果一覧

資料１－５　サイバーセキュリティ 2020（案）

サイバーセキュリティ2020（2019年度年次報告・2020年度年次計画）（案） 全体概要

資料1-1

年次報告・年次計画は、サイバーセキュリティ基本法に基づく戦略を的確に実施するために作成するもの。今回は、事業者や個人向けに、動向と政策を分けて整理し解説も充実

１部「サイバーセキュリティを巡る動向」	直近のサイバーセキュリティを取り巻く環境を解説するとともに、主なサイバーセキュリティ事案や国際的な動向などを整理
２部「我が国のサイバーセキュリティ政策」	1章及び2章で、基本的枠組みと、戦略に基づく取組を年次報告と年次計画の一連の流れを示すように整理 3章で、現行戦略の最終年度を迎えるに当たり、大局的な視点で、現状の認識を踏まえた加速・強化すべき取組を整理

1部 サイバーセキュリティを巡る動向

■サイバーセキュリティを取り巻く環境（１章）

- **新型コロナウイルス感染症への対応**
- **新しいデジタル技術の活用とリスクマネジメント ～DX with Cybersecurity～**
- **情報共有の推進と共助の取組**

■2019年度のサイバーセキュリティに関する情勢（２章）

サイバーセキュリティ事案
- □ 新型コロナウイルス感染症に乗じたサイバー攻撃
- □ Emotet　□ キャッシュレス決済の不正利用　等

国際的な動向
諸外国の政策やサイバー空間における国際法の適用に関する議論　等

2部 我が国のサイバーセキュリティ政策

■基本的枠組み（サイバーセキュリティ基本法、サイバーセキュリティ戦略、サイバーセキュリティ政策の推進体制）　（１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（２章）

戦略の体系に沿って、各府省庁が実施する施策の2019年度実績及び評価と、2020年度の取組について包括的に整理（各施策の一覧表は、別添１・別添２）

■現状の認識を踏まえた加速・強化すべき取組（３章）

現状から見えてきたこと	新たな情報通信サービスの普及、新型コロナ感染症対策としてのテレワークなどの積極的活用、急速な状況変化を逃さないサイバー攻撃の発生といった動向から見えてきたことを整理
今後の検討に当たっての視点	戦略で掲げたサイバーセキュリティエコシステムの概念を踏まえ、異なる主体が自らの役割をしっかりと認識しながら、緊密に連携して取り組んでいくことが重要。対策を進めていくに当たって、自助・共助・公助の考え方を重要なフレームワークと捉えて、検討の観点を整理
今後加速・強化して取り組むことが重要な事項	現状から見えてきたことや今後の検討に当たっての視点を踏まえながら、現在の戦略の実行に当たって、今後加速・強化して取り組むことが重要な事項を整理

別添

別添１ 2020年度のサイバーセキュリティ関連施策 / 別添２ 2019年度のサイバーセキュリティ関連施策の実施状況 / 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４ 政府機関等における情報セキュリティ対策に関する統一的な取組 / 別添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６ サイバーセキュリティ関連データ集 / 別添７ 担当府省庁一覧（2020年度年次計画） / 別添８ 用語解説

サイバーセキュリティ2020（１部 サイバーセキュリティを巡る動向）の概要

資料1-2

- 新型コロナウイルス感染症への対応をはじめ、直近のサイバーセキュリティを取り巻く環境の概観や基本的な考え方について解説
- また、2019年度に、政府機関、事業者、国民一般等において確認された国内外の主なサイバーセキュリティ事案等を整理
- さらに、諸外国の政策や、サイバー空間における国際法の適用に関する議論など、サイバー空間に係る国際的な動向を整理

【サイバーセキュリティを取り巻く環境】

○新型コロナウイルス感染症への対応

※1 令和２年３月28日（令和２年４月７日改正版）新型コロナウイルス感染症対策本部決定

・「新型コロナウイルス感染症対策の基本的対処方針」※1にて、事業者においては、テレワークなどを活用することで、さらに接触の機会を減らすことを協力して行っていく必要があるとされた。

・こういった状況を注視しつつ、基本的な対策方法などについて効果的に周知活動を進めていくことが重要

<これまでの主な政府の動き>

NISC	総務省	経産省
一般・政府機関等・重フラ事業者等に向けた「テレワークを実施する際にセキュリティ上留意すべき点について」を公開	対策の考え方や対策例を示す「テレワークセキュリティガイドライン（第4版）」について改めて周知	直近の状況及び今後のデジタル化の急加速に対応するための取組を促す「産業界へのメッセージ」を発出

○新しいデジタル技術の活用とリスクマネジメント ～DX with Cybersecurity～

・企業が新たなデジタル技術を活用する効果を最大限に享受するためには、デジタル技術を使って何を実現したいのかを明らかにするとともに、事業に致命的な影響を与えるリスクの洗い出しを行うことが重要。そのリスクの１つとしてデジタル技術の活用に対応するサイバーセキュリティへの対応は最も重要な柱

・また、新たなデジタル技術へのアクセシビリティは、攻撃者が排除されるものではないことも踏まえ、サイバー攻撃に対して、防御側におけるセキュリティ対応能力の効果・効率を向上させるDXを推進することも重要

○情報共有の推進と共助の取組

サイバー攻撃の複雑・巧妙化が進む現状において、被害を受けた組織等からの迅速な情報共有の重要性は増している。サイバー攻撃等の情報を一定のコミュニティに共有する動きが一層活発化している中、運用の充実化や多様な枠組みの役割分担等によって、効果的、効率的に情報共有を進めることが重要

【2019年度の主なサイバーセキュリティ事案】

業務・機能・サービス障害

・新型コロナウイルス感染症に乗じ、国外において、医療関連機関などに対するサイバー攻撃が発生。ITインフラが停止するなどの影響

・米国の自治体においてランサムウェア被害が数多く発生。行政業務に支障を来すなどの影響

情報の毀損及び漏えい

・Emotetの再流行が広がり、多くの組織で情報流出等の被害を公表

・大手電機会社が、自社のネットワークに不正アクセスを受け、個人情報と企業秘密が流出した可能性があることを公表

・情報機器の処分等を営む企業において、従業員が行政文書が蓄積されたHDDを盗み出し、転売をしていたことが発覚

金銭の窃取・詐取等

・2019年７月にサービスを開始したキャッシュレス決済（コード決済）サービスが不正アクセスを受け、約3800万円の被害

・インターネットバンキングに係る不正送金事犯について、2019年９月から被害が急増し、発生件数1872件、被害額約25億2100万円

【政府機関等に対する攻撃の高度化・巧妙化】

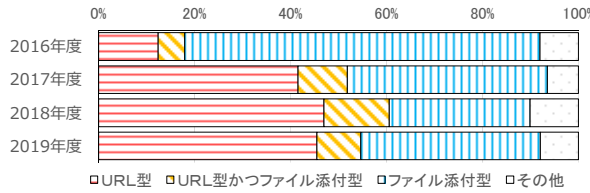
2019年度の政府機関に対する不審な通信の検知数は 2018年度から減少したものの（図表１）、政府機関等に対する実質的な脅威度は引き続き高い状況にある。標的型攻撃については、より巧妙化されたメールも確認されている。また、2017年度を境として、ファイル添付型(不審なファイルを添付)に代わってURL型(不審なURLを記載)の不審メールの比率が増加（図表２）。

図表１　政府機関におけるマルウェア感染の疑いや標的型攻撃等の検知件数※2

年度	2017年度	2018年度	2019年度
マルウェア感染の疑い	169	111	55
標的型攻撃	57	66	30
その他※3	0	5	5

（件）

図表２　政府機関等に対する不審メールの傾向



※2 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、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等を分析しノイズとして除去した上で、引き続き警戒を要するイベントについて集計

※3 調査行為とみられる通信やタイポスクワッティングの疑いのある通信。

【国外の動き】

○諸外国の政策

米国
・新たな国家サイバー戦略（2018/9）
・サイバーセキュリティ人材の強化を目的とした大統領令（2019/5）
・情報通信技術等のサプライチェーンの保護に関する大統領令（2019/5）

EU
・一般データ保護規則(GDPR)成立（2018/5 施行）
・欧州サイバーセキュリティ法成立（2019/6 施行）
・5Gネットワークのサイバーセキュリティに関するツールボックス（2020/1）

中国
・サイバーセキュリティ法の施行及び同法に基づく関連規制を制定（2017/6）

ロシア
・情報安全保障ドクトリン公表。サイバー空間における安全保障を目的としたサイバーセキュリティ政策の方向性を明示（2016/12）

○サイバー空間における国際法の適用に関する議論

2019年12月、第6会期国連政府専門家会合(GGE)が立ち上がり議論を深化

（参考）新型コロナウイルス感染症への対応と今後の取組

- **新型コロナウイルス感染症への対応として、様々な場面でインターネットの利用や新たなデジタル技術の活用が増加することが想定される。**
- **今後は、新しい生活様式の定着に向けて、テレワークの導入や活用だけではなく、サービスの提供自体などにも新たなデジタル技術を活用することも想定され、このような状況を注視してサイバーセキュリティ対策を進めていくことが重要。**

これまでの主な政府の動き

※ 令和２年３月28日（令和２年４月７日改正版）新型コロナウイルス感染症対策本部決定

「新型コロナウイルス感染症対策の基本的対処方針」※において、事業者においては、テレワークなどを活用することで、さらに接触の機会を減らすことを協力して行っていく必要があるとされた。こういった状況を注視しつつ、基本的な対策方法などについて効果的に周知活動を進めていくことが重要

NISC

- 国民一般に向けて、注意すべき基本的なポイントを周知（3/27）
- 政府機関等・重要インフラ事業者等に向けて、テレワークを導入する際のセキュリティ上留意すべき点について注意喚起（4/7及び4/9）
  （「**テレワークを実施する際にセキュリティ上留意すべき点について**」をHPに公開（4/14））
- 新しい生活様式の実践に向けて、「**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**」をHPに公開（6/11）

総務省

- テレワークの積極的な活用について周知するとともに、テレワーク関連支援情報やセキュリティ確保に関する情報をHPに公開（2/25）
- テレワークの導入に当たってのセキュリティ対策の考え方や対策例を示す「**テレワークセキュリティガイドライン（第４版）**」について改めて周知
- より具体的で分かりやすく実践的な内容のチェックリストを策定中であり、また、セキュリティの専門的な相談に対応できる窓口を設置しており、これらについても幅広く周知

経産省

- 直近の状況及び今後のデジタル化の急加速に対応するためのサイバーセキュリティの取組を促す「**産業界へのメッセージ**」を公表（4/17）
  ①新型コロナウイルスを騙る不正アプリや詐欺サイト、フィッシングメール/SMSに注意すること
  ②NISCやIPA、JPCERT等の専門機関からの注意喚起を定期的に確認すること
  ③アップデート等の基本的な対策を実施すること
  ④ランサムウェアに感染した事態に備えてシステムやデータのバックアップと復旧手順を確認すること

新しい生活様式の定着に向けた今後の取組

新しい生活様式の定着に向けて、更にデジタル化を推進していく必要性が明らかとなる状況を踏まえ、サイバーセキュリティ対策を進めていくことが重要

＜主な具体的取組＞

- ✓政府機関等においては、機関外での業務実施機会や複数の政府機関等が外部サービスを利用して連携する機会が増えたことを踏まえ、かかる環境下での情報セキュリティに対する特有の留意点や考え方を示していくことが有用であり、統一基準への追記を始め、必要な発信を行っていく。（NISC）
- ✓中小企業等に向けては、これまで未導入だった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。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）
- ✓テレワークの推進に当たり、デジタルで様々なやり取りを完結できる環境の構築に向けて、電子データの信頼性を確保するトラストサービスを推進する。（総務省）
- ✓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・セーフティ要求の検討等に資する「IoTセキュリティ・セーフティ・フレームワーク」を策定する。（経産省）

サイバーセキュリティ2020（２部３章　現状の認識を踏まえた加速・強化すべき取組）の概要

➢ **新たな情報通信サービスの普及、新型コロナ感染症対策としてのテレワークなどの積極的活用、急速な状況変化を逃さないサイバー攻撃の発生といった状況に着目し、自助・共助・公助の観点から、現在の戦略の実行に当たり特に加速・強化すべき取組をまとめ、今後の次期戦略につなげるものとして整理。**

1 現状から見えてきたこと

- 1.1 新型コロナウイルス感染症対応を踏まえたDXの推進とサイバーセキュリティ対策（DX with Cybersecurity）
- 1.2 クラウドサービスの利用拡大に伴う防御範囲・手法の転換
- 1.3 5Gの商用サービス開始とそれに伴うデータ活用の高度化
- 1.4 サプライチェーン・リスクの拡大と予見性の確保
- 1.5 国際的な議論の高まりと統一的な国際ルールへの期待

2 今後の検討に当たっての視点

2.1 リスクマネジメントの実施と戦略的行動

セキュリティを、DXを成功させる上での重要な機能と位置付けた上で、リソースの制約を意識しつつ、リスクマネジメントを進めることが重要

2.2 情報共有体制の積極的活用による共助の強化

情報共有体制の運用の充実化や多様な枠組みが存在し、それらの役割分担によって、効果的、効率的に情報共有を進めることが重要

2.3 政府に期待される役割

自助や共助の取組を過不足なくサポートするという役割を意識し、インセンティブ構造を明確にすることで仕組みをデザインして社会全体として効果を最大化。また、国際場裡においては、有志国等との連携協力を質・量とも高めていくことなどが重要

3 今後加速・強化して取り組むことが重要な事項

- 3.1(1) サプライチェーン全体のサイバーセキュリティ対策の強化
- 3.2(1) 重要インフラ対策の推進
- 3.2(2) 政府機関対策の推進
- 3.2(3) 東京2020大会を踏まえた未来につながる成果の継承
- 3.3(1) 情報共有と重層的な国際連携の枠組み
- 3.3(2) 海外支援戦略
- 3.4(1) DX with Cybersecurityの実現に向けた人材育成
- 3.4(2) 政府機関等のサイバーセキュリティを支える人材の確保・育成
- 3.4(3) 研究開発の推進
- 3.4(4) 普及啓発の推進

参考資料

（２部２章（主な昨年度の取組実績、評価及び今年度の取組））

サイバーセキュリティ2020（２部２章）の概要（１/５）

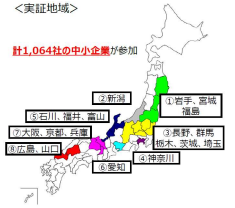
２部２章（主な昨年度の取組実績、評価及び今年度の取組）

１．経済社会の活力の向上及び持続的発展

昨年度の実績

- 経営層の意識改革等を目的に、企業のサイバーセキュリティ対策実施状況の可視化ツールや「サイバーセキュリティ関係法令Q&Aハンドブック」等を公開
- サプライチェーン全体の対策強化に向け、CPSF※の社会実装の推進や、中小企業向けにセキュリティ対策支援に関する実証事業等を実施　※サイバー・フィジカル・セキュリティ対策フレームワーク（経産省）
- 安全なIoTシステムの構築に向け、パスワード設定等に不備のあるIoT機器を調査及び注意喚起する取組「NOTICE」や、IoT機器の特性や利用方法等を踏まえて整理したセキュリティ要件を満たす機器の利用を推奨する施策等を実施

サイバーセキュリティお助け隊実証事業



NOTICEの広報ポスター

評価

経営層の意識改革やサイバーセキュリティに対する投資の促進等については、引き続き、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が必要であるとの認識を広げる取組を促進していくことが重要。また、中小企業をはじめサプライチェーン全体の対策強化の取組が着実に進展している中、取組の一層の強化に向けて、既存の制度の周知強化も含め、関係省庁が連携して各種取組を推進していくことが重要。安全なIoTシステムの構築については計画どおりに進捗しているものの、例えば、NOTICEにおける注意喚起後に改善が見られない利用者への有効な注意喚起手法の検討など、今後、整備した枠組み等が円滑に実施されるようフォローしていくことが求められる。

今年度の取組

- 経営層の意識改革等に向けては、これまでに整備したツールの改善や活用の促進を進める。
- サプライチェーン全体の対策強化に向けては、技術検証体制の整備等サプライチェーン・リスクに対応するための取組や、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実態やニーズをよりきめ細かく把握する取組などを進める。
- 安全なIoTシステムに構築に向けて、産官学民及び民間企業相互間の連携により、脆弱なIoT機器の対策を進める。

サイバーセキュリティ2020（２部２章）の概要（２/５）

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

２．国民が安全で安心して暮らせる社会の実現

昨年度の実績

- 重要インフラの安全性・持続性確保の観点から、指針※を改定したほか、官民の枠を超えた訓練・演習の実施等、第４次行動計画に基づく各施策を実施

※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）（NISC）

- 政府機関等全体のセキュリティ対策強化に向け、次期統一基準群の改定に向けた検討を行ったほか、適切な水準が確保されたクラウド利用のため、「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の基本的枠組み」を決定。また、サイバーセキュリティに関する技術・能力を競う競技会を実施
- 東京2020大会に向け、重要サービス事業者等に対するリスクアセスメントの促進及びサイバーセキュリティ対処調整センターにて情報提供を実施
- 従来の枠を超えた情報共有・連携体制の構築として、サイバーセキュリティ協議会においては、協議会構成員の募集を３回行い、協議会構成員は漸次拡大するとともに、協議会の特性を活かした迅速な情報共有を行ったほか、運用ルールの見直しを実施

評価

重要インフラ防護、政府機関等の対策強化、東京2020大会のセキュリティ確保、従来の枠を超えた情報共有・連携体制の構築等、各種取組は着実に進展。今後、第４次行動計画、統一基準群については、それぞれ、昨今の環境変化や対策状況を踏まえて、次の改定に向けた検討が求められる。また、対処調整センターや協議会等、昨年度取組を開始したものについては、実際の運用の経験等を踏まえ、充実・強化していくことが重要である。

今年度の取組

- 重要インフラ防護、政府機関等の対策強化、東京2020大会のセキュリティ確保、従来の枠を超えた情報共有・連携体制の構築等について、既存の枠組みに基づく取組を着実に進めていくとともに、2019年度に発生又は明らかになった事案や運用の状況等も踏まえて、運用の充実・強化や枠組みの見直しなどを進めていく。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

３．国際社会の平和・安定及び我が国の安全保障への寄与

昨年度の実績

- G20大阪サミット等における共同声明や意見交換を通じて、サイバー面での協力を強化していくことを確認。また、サイバー空間における法の支配の推進に寄与することを目指し、今期国連政府専門家会合に参画し、国連におけるサイバーセキュリティに関する議論に積極的に貢献
- サイバー空間を悪用したテロ組織の活動等に係る情報の収集・分析の強化や、ARF※の枠組等を通じ、今後取り組むべき信頼醸成について議論を実施

※ASEAN Regional Forum

- 13の国と地域の間で二国間協議を開催するとともに、多国間対話等を通じ、国際協調・協力を推進。また、事故対応等に係る国際連携の強化に向けた演習や能力構築支援を実施

日・ASEANサイバーセキュリティ政策会議

評価

サイバー空間における法の支配の推進や国際協力・連携の深化が着実に進展。今後は、継続的に関係国と連携しつつ、今期国連政府専門家会合への関与等を通じて、更なる議論の深化を図るとともに、既に合意された規範について国際社会が実施するよう促していく必要がある。

今年度の取組

- 法の支配の推進については、国連政府専門家会合における議論が報告書の作成に向けて加速することから、規範の形成・普遍化についての議論を深化させ、責任ある国家の行動規範及び国家実行を積み重ねていく。
- また、引き続き、サイバー攻撃に対する国家の強靭性を確保するとともに、積極的に能力構築支援等を行うなど国際協力・連携の深化に取り組む。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

４．横断的施策

昨年度の実績

- サイバーセキュリティ人材の育成・確保を強化すべく、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うとともに、施策間の連携を促進。また、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、仮運用を開始
- 研究・技術開発の推進のため、「我が国におけるサイバーセキュリティ研究・技術開発の取組方針」を策定するとともに、方針に基づいて取組を実施
- 普及啓発の観点では、「サイバーセキュリティ意識・行動強化プログラム」に沿って具体的な取組を実施。また、「サイバーセキュリティ月間」において、認知度の高いコンテンツとのタイアップ
  （ソードアート・オンライン-アリシゼーション-War of Underworld）を行い、若年層に重点を置いたキャンペーン等を実施

TVアニメ『ソードアート・オンライン・アリシゼーション War of Underworld』とタイアップ

評価

戦略マネジメント層及び実務者層・技術者層の育成等の取組は着実に進展しているが、人材の育成・確保は継続して進めていく必要がある。研究開発については、研究・技術開発の取組方針に基づき、引き続き、取組を推進していくことが求められる。普及啓発の取組は、サイバーセキュリティ月間において、インフルエンサーの発信※によって、若年層でもよりリーチしにくい層に対しての普及啓発を図ることができたこと等も踏まえ、今後の検討を進めていくことが重要である。

※本年はInstagramやTwitterなどで多くのフォロワーを持つ、いわゆるインフルエンサーにサイバーセキュリティに関する普及啓発の投稿を依頼

今年度の取組

- 人材育成については、サイバーセキュリティ人材育成取組方針に基づき、関係施策を推進していく。
- 研究開発の推進に向けては、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、国内産業の育成・発展に向けた支援策、攻撃把握・分析・共有基盤の強化や暗号等の基礎研究の促進の取組等を推進するとともに、産学官連携の研究振興策について議論を進める。
- また、普及啓発については、普及啓発全体を表す代表的な指標をモニタリングし、PDCAサイクルを着実に推進していくほか、GIGAスクール構想における学校現場に一人一台の端末を配布するタイミングをきっかけとして、児童生徒がインターネットやセキュリティについて学ぶための資料の作成等を実施するなどにより、理解を深める。

サイバーセキュリティ2020（２部２章）の概要（５/５）

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

５．推進体制

昨年度の実績

- 内閣サイバーセキュリティセンターを中心に、関係機関とのパートナーシップに基づく国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合やIWWN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推進
- 戦略の趣旨を国内外の関係者に向け効果的に発信することを目的に、サイバーセキュリティ2019の冊子を制作。内閣官房及び関係府省庁において、戦略のカラー冊子やサイバーセキュリティ2019の冊子を活用するなどして、各種セミナーでの説明等を通じて、戦略等の発信を実施

サイバーセキュリティ戦略

サイバーセキュリティ2019

評価

戦略の国内外の関係者への更なる浸透を図るため、引き続き、取り組むことが重要。戦略で掲げたサイバーセキュリティエコシステムの実現には、あらゆる主体がセキュリティに取り組むインセンティブを生み出すことが重要であり、全体として統一感を持って、考え方を浸透させていくために、戦略の基本的な考えを示しつつ、官民の個別の取組に反映しやすいように説明を行うなど、国内外の関係者との一層の連携の強化を図り、戦略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は、既に構築している仕組みの機能向上を図るとともに、連携体制についても逐次見直しを実施する。
- また、全ての主体に関する自律的な取組を促進するため、引き続き、国内外の関係者へ戦略及びこれに基づく年次計画等の発信を行う。加えて、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ていく。

「サイバーセキュリティ戦略」に基づき、2020年度に実施すべき施策に関する意見募集の結果の概要

■ 実施方法：NISCのWebページ、内閣官房のWebページ、電子政府の総合窓口（e-Gov）に掲載して公募

■ 実施期間：令和２年（2020年）１月30日（木）～２月28日（金）

■ 意見総数：13者から26件【７企業・団体から延べ17件、６個人から延べ９件】

【意見の種類】

・2020年度に実施すべき施策（サイバーセキュリティ2020）に関する意見：25件

- ・経済社会の活力の向上及び持続的発展：９件
- ・国民が安全で安心して暮らせる社会の実現：９件
- ・国際社会の平和・安定及び我が国の安全保障への寄与：１件
- ・横断的施策：６件
- ・推進体制：０件

・その他の意見：１件

■ （参考）提出者名：

一般社団法人コンピュータソフトウェア協会セキュリティ委員会、日本ヒューレット・パッカード株式会社、株式会社クロイツ、サウスプルーム株式会社、ヤフー株式会社、情報セキュリティ教育事業者連絡会(ISEPA)、日本ネットワークセキュリティ協会事業コンプライアンス部会、個人（６人）

2020年度に実施すべき施策に関する意見募集の結果一覧

資料1－4

通しNo	提出者	該当箇所	意見の要旨	主な考え方
1	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	セキュアコーディングの重要性の啓発、ISACでの情報連携および各プログラミング言語のセキュアコーディングガイドの整備が必要。	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に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
2	個人（2）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	サイバーセキュリティー対策における政策の提案__1 「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。 例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。	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対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
3	個人（2）	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	サイバーセキュリティー対策における政策の提案__2 具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。	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対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
4	日本ヒューレット・パッカード株式会社	4．1．1　新たな価値創出を支えるサイバーセキュリティの推進	ユーザー識別（本人確認）や認証、認可、アクセス制御といったセキュリティ機能において、FIDO認証などの新しい標準化技術の活用を選択肢の一つとして考慮すべき	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に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
5	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．2　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	ソフトウェアで利用しているOSSが不明確であるといったサプライチェーン・リスクに対処するため、SBOMが作成できるシステムを安価に利用できるようなシステムの構築を望みます。	「サイバー・フィジカル・セキュリティ対策フレームワーク」に基づくセキュリティ対策の具体化・実装を推進するため設置されたタスクフォース（TF）のひとつ「ソフトウェアTF」において、ソフトウェア管理手法、脆弱性対応、OSS利活用等について検討しております。年次計画においても、ご指摘のOSSの活用に係るリスクを含めて適正なソフトウェア管理手法の在り方について検討を進めることとしています。
6	一般社団法人コンピュータソフトウェア協会　セキュリティ委員会	4．1．2　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	中小企業へのPSIRT構築の支援およびソフトウェアの発注者にも開発におけるPSIRTの必要性を理解いただく啓発活動が必要。	サイバーセキュリティ戦略の中小企業の取組の推進に当たっての賛同意見として承りました。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
7	株式会社クロイツ	4．1．2　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	資金力の無い中小企業でも有効な対策を行うことが出来るようにもっと簡単に助成金、補助金が使えるようにしてほしい。また、現状のサイバー攻撃は対策ソフトだけで防ぐ事が難しく組織のルールや環境づくり、スタッフ研修と言った基礎的な事が重要です。そちらにも重点を置いた助成をした方が良い。	サイバーセキュリティ戦略における中小企業の取組の推進に当たっての賛同意見として承りました。 御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただき、年次計画に基づき引き続き中小企業の取組を推進してまいります。
8	個人（6）	4．1．2　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	中小企業のサーバやネットワークがほんとうにセキュリティ対策をしているのかの技術的調査と支援をすべき	サイバーセキュリティ戦略における中小企業の取組の推進に当たっての賛同意見として承りました。 御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただき、年次計画に基づき引き続き中小企業の取組を推進してまいります。

2020年度に実施すべき施策に関する意見募集の結果一覧

資料1－4

通しNo	提出者	該当箇所	意見の要旨	主な考え方
9	日本ヒューレット・パッカード株式会社	4．1．3　安全なIoTシステムの構築	安全なIoTシステム構築のためには多層的な観点での防御が必要と考えております。既にIoTシステムに関するサイバーセキュリティはIoT推進コンソーシアムにより「IoTセキュリティガイドライン」として公開されていると理解しております。今後はこれらの対策に加え、AIを用いたIoTデバイス属性の特定や不正端末の識別、防御といった観点も重要となる	ご指摘の通り、サイバーセキュリティへのAIの活用は重要な観点であると考えます。いただいた御意見は今後の検討の参考とさせていただきます。
10	サウスプルーム株式会社	4．2．1　国民・社会を守るための取組	クラウドのような外部組織でのデータ管理が中心の現在では、サーバそのものがハッキングされれば、企業、団体及び個人がセキュリティ対策を行ったとしても、他と通信する過程で全てのデータが抜き取られてしまう。 政府若しくは政府の関連団体がハッキングされている事実を掌握した上で、該当企業、団体への指導警告を徹底し、対策を取らせ、少しでも被害を縮小する方向に舵をとらなければならない。	我が国のサイバーセキュリティの確保に当たっては、サイバー攻撃対策が重要と考えております。 これまでもサイバー攻撃の被害を受けていることを把握した場合には、JPCERT/CCに情報提供し、JPCERT/CCを通じて被害を受けた組織・機関等に対して情報提供・注意喚起を行ってきておりますが、ご指摘についても今後のこうした取組に際して参考とさせていただきます。
11	日本ヒューレット・パッカード株式会社	4．2．1　国民・社会を守るための取組	政府機関の情報システムや国民向けサービスにおける認証機能の実装において、標準化技術であるFIDO認証を一つの選択肢として考慮すべきである。	多様な認証方式があると認識しているところ、いただいた御意見については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
12	日本ヒューレット・パッカード株式会社	4．2．1　国民・社会を守るための取組	各企業・団体に対し、「サイバーセキュリティ保険」の必要性・緊急性の更なる啓発と普及が必要である	ご指摘のとおり、サイバーセキュリティ保険の利用拡大に向けた更なる啓発と普及が重要と考えており、年次計画においては、サイバーセキュリティお助け隊の取組や、Security　Action制度との連携により、サイバーセキュリティ保険の活用や普及・啓発に向けた取組を進めることとしています。いただいたご意見は今後の取組の参考とさせていただきます。
13	サウスプルーム株式会社	4．2．2　官民一体となった重要インフラの防護	政府機関等からガイドラインの発行ができれば、ハッキングに対応する企業も増え、状況が改善することが考えられる。 公的な組織・団体が、ハッキングを受けたサーバの情報を入手し、被害サーバの管理企業や団体等に通知ないし指導できれば、被害サーバの管理企業や団体はその事実に向き合い対策しなければならなくなるだろう。 日本国内で年間5万台以上のサーバがハッキングされ、管理者権限を奪われていて、ほとんどがその事実に気づいていないことから、様々な情報が流出し国としても大きな損失を出しているという点にどのように対策するか検討していただくことが重要である。	我が国のサイバーセキュリティの確保に当たっては、それぞれの組織・機関が主体的にセキュリティ対策に取り組むことが重要であると考えております。 NISCとしては、これまでもこうした取組を支援すべく、様々な取組を行っていますが、ご指摘についても今後の施策を検討・実施する際に参考とさせていただきます。
14	ヤフー株式会社	4．2．2　官民一体となった重要インフラの防護	セキュリティクリアランス制度が無い状況が、官民連携と国際連携の両面において足枷になる恐れがあるため、セキュリティクリアランス制度の早期創設の検討を望む	頂いた御意見については、今後のサイバーセキュリティ政策の検討や実施の推進に当たって参考とさせていただきます。

2020年度に実施すべき施策に関する意見募集の結果一覧

資料1－4

通しNo	提出者	該当箇所	意見の要旨	主な考え方
15	個人（4）	4．2．3　政府機関等におけるセキュリティ強化・充実	省庁および地方公共団体から発注・委託する場合において委託先に求めるべき情報のセキュリティ基準を欧米NIST SP800-171等にならい強化することを提案するとともに、日本の組織では、最高情報責任者等「組織の上級職員」が依然として不在および極度に不足している状況であることから、人材の育成とそのスキル認定、およびその必要性の理解が急務である。	省庁に関しては、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（平成30年度）においては、政府機関の外部委託に係る規定を載せており、外部委託先における情報セキュリティ対策の実施を求めております。引き続き、この取組を推進していきます。 また、地方公共団体に関しては、「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」において、外部委託先における情報セキュリティ対策の実施等を求めています。 御意見については、このような施策の検討や実施の推進に当たって参考にさせていただきます。
16	サウスプルーム株式会社	4．2．3　政府機関等におけるセキュリティ強化・充実	日本で情報流出が無差別に発生している現実を踏まえて、公共及び主要インフラのセキュリティ状況を正確に把握し、PDCAのサイクルを実施することをお願いします。	政府機関においては、最新のサイバーセキュリティ状況を政府統一基準群に反映し、これに基づいた各機関の情報セキュリティ監査の他、サイバーセキュリティ本部による監査により、セキュリティ状況を把握し、その結果に応じた、セキュリティ対策の改善を実施しています。 また、情報通信、電力、金融等14分野の重要インフラについては、サイバーセキュリティ対策に関する「行動計画」を策定し、安全基準の指針の整備、官民での情報共有の促進、演習による対処能力の向上等の取組を実施しています。 引き続き、関係機関が密接に連携し、サイバーセキュリティを確保できるよう、これらの取組を進めてまいります。
17	個人（5）	4．2．4　大学等における安全・安心な教育・研究環境の確保	私立大学についても，国立大学と同様に，情報セキュリティの計画（ロードマップ）や進捗状況／実施状況を文科省に報告させる仕組みを導入するべきと考える。	ご指摘の箇所については、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）』（令和元年５月２４日付）において、私立を含めた大学等に対し「サイバーセキュリティ対策等基本計画」の策定を求めており、フォローアップを行う上での参考とさせていただきます。
18	サウスプルーム株式会社	4．2．6　従来の枠を超えた情報共有・連携体制の構築	中国ブラックマーケットのハッカー達に好きなようにハッキングされている現状を脱却するためには、中国ブラックマーケットのリアルタイムな情報を入手し、その情報を即時分析し、対策する必要がある。	我が国のサイバーセキュリティの確保に当たっては、ご指摘のように様々な情報を収集し、必要に応じて民間とも情報共有することが重要と考えております。 これまでもこうした観点から様々な取組みを行ってきていますが、ご指摘についても今後の施策の検討や実施に当たっての参考とさせていただきます。
19	サウスプルーム株式会社	4．3．2　我が国の防御力・抑止力・状況把握力の強化	政府機関主導でホワイトハッカーの育成及び採用を精励し、また検証の現場にそのホワイトハッカーを人員として配置し、攻撃の再現、ハッカー目線の見識から分析し対策を講じる必要があります。	サイバーセキュリティ戦略において、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・確保も引き続き行っていくこととしております。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。

2020年度に実施すべき施策に関する意見募集の結果一覧

資料1－4

通しNo	提出者	該当箇所	意見の要旨	主な考え方
20	個人（1）	4．4．1　人材育成・確保	公的な職場においては、セキュリティチームも当然必要だが、その基盤となる人材も育てるべきではないか。そのためにも、公務員の採用方法に関して現場が必要だと感じる人材を雇用するための制度や、人材を育成するための職場環境が必要ではないか。	サイバーセキュリティ戦略における人材育成・確保の推進に当たっての賛同意見として承りました。同戦略においては、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・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。 政府機関においても、常勤・非常勤を問わず、様々な方法により即戦力の高度専門人材の確保に取り組んでいるほか、部内育成の専門人材の確保・育成に向け、有為な人材の確保や研修等に積極的に取り組んでいるところであり、御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
21	個人（3）	4．4．1　人材育成・確保	ITの質を向上させるためにも、良い人材をこちらの意思で正職員として雇える様制度を整えて頂きたい。	サイバーセキュリティ戦略における人材育成・確保の推進に当たっての賛同意見として承りました。同戦略においては、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・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
22	情報セキュリティ教育事業者連絡会(ISEPA)	4．4．1　人材育成・確保	「セキュリティ業務の整理」と「人材のセキュリティスキル見える化」による実効性のある政策実行を望みます。	サイバーセキュリティ戦略において、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・確保を強化するとともに、人材の多様性の確保を推進していくことが重要としております。ご指摘いただいた点も踏まえ、年次計画においては、特に、産業サイバーセキュリティ研究会WG2において、御指摘の「セキュリティ業務の整理」と「人材のセキュリティスキル見える化」をITSS＋（セキュリティ領域）の改定等により進めることとしています。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。
23	日本ネットワークセキュリティ協会事業コンプライアンス部会	4．4．1　人材育成・確保	法令に抵触しないよう過度に意識するあまり、競争力が海外に比べて劣っている懸念もあり、こうした委縮効果が生じないような環境整備を求める。	NISCにおいては、事業者が適切にサイバーセキュリティ対策を講じる上で、不正アクセス禁止法を含め参照すべき関係法令をQ&A方式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック」を作成し、NISCウェブサイトで公表（※）するなど環境整備を図ったところです。 （※）https://www.nisc.go.jp/security-site/files/law_handbook.pdf
24	個人（2）	4．4．2　研究開発の推進	「サイバーセキュリティー対策」における構造では、「科学技術（サイエンステクノロジー）」の「詳細（ディタイル）」を明確に導入する事が望ましい。	先端技術を利活用したイノベーションを支えるサイバーセキュリティ対策の推進に関する賛同意見として承りました。内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
25	日本ヒューレット・パッカード株式会社	4．4．2　研究開発の推進	市場にはすでにNIST SP800-193に準拠したICT機器などが販売されている状況にあります。すでに利用可能状態にある技術をどう利活用していくかという次のフェーズを本格検討すべき時期に来ており、「研究・技術開発」のみならず「実用化、利活用」を念頭に置いた施策をご検討いただくのが相当である	サイバーセキュリティ研究・技術開発取組方針において、社会実装までのプロセスを念頭に置きつつ取組を進めることが重要としております。御意見については、今後の取組の検討や実施の推進に当たっての参考とさせていただきます。

2020年度に実施すべき施策に関する意見募集の結果一覧

資料1－4

通しNo	提出者	該当箇所	意見の要旨	主な考え方
26	個人（2）	－	・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人 高度人材での導入で社会水準の向上 による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準 で の基準 による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案	本意見募集と直接関係ないと考えられますが、ご意見として承ります。

資料１－５

サイバーセキュリティ2020（案）
（2019年度年次報告・2020年度年次計画）

令和２年（2020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＞

はじめに

新型コロナウイルス感染症への対応としての新しい生活様式への移行は、そのままデジタル技術の経済社会へのより深い浸透を意味し、その実現にはDX with Cybersecurityの取組が重要な要素になることは間違いない。正にサイバー空間と実空間の一体化の急速な進展であり、この状況に合わせて的確にサイバーセキュリティの対応を進めていくことが重要である。

サイバーセキュリティ戦略（2018年７月27日閣議決定。以下「戦略」という。）においては、サイバーセキュリティ戦略本部は、戦略を的確に実施していくため、３年間の計画期間内において、年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映することとしている。

戦略においては、サイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）の目的である「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和及び安定並びに我が国の安全保障に寄与すること」によって政策目的を整理し、それぞれの目的に沿って、施策を推進することとしている。本書においても、この政策目的によって整理を行っている。また、取組を進めるに当たっては、戦略の「目指すサイバーセキュリティの基本的な在り方」において示す３つの観点（「サービス提供者の任務保証」、「リスクマネジメント」、「参加・連携・協働」）を踏まえることとしている。

2019年度年次報告・2020年度年次計画である本書は、２部構成とし、「１部　サイバーセキュリティを巡る動向」と「２部　我が国のサイバーセキュリティ政策」を分けて整理を行った。２部においては、１章で基本的枠組みを解説した上で、２章で戦略に基づく昨年度の取組実績、評価及び今年度の取組を、戦略の事項に沿って、報告と計画を一連の流れを示すように整理を行っている。また、２部３章においては、現行の戦略における計画期間の最終年度を迎えるに当たって、過去２年間の取組を振り返りつつ、大局的な視点で、現状の認識を踏まえた加速・強化すべき取組を整理した。新型コロナウイルス感染症への対応と、それを踏まえた2020年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[1]（以下「東京2020大会」という。[2]）の開催スケジュールの変更への対応については、短期的には既に示されている基本的枠組みに基づいて取組を推進していくこととしつつ、中長期的には新たな生活様式の定着などに対応するための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ていくことが重要であることを示した。

本書は、各府省庁の施策を示すものではあるが、事業者や個人により参照されることも意識して、基本的な考え方についての説明も充実させた。それぞれの主体が、サイバーセキュリティを巡る状況の概観を認識・理解するとともに、リスクマネジメントの手法に則って定点確認やBCPの作成・再検討を行う端緒とするなど、「参加・連携・協働」の主体である事業者や個人が、自らの様々なリスクと向き合い、自らの事業や生活を見つめなおすことで、サイバーセキュリティ対応を進める契機となることを望んでいる。本書の名称は、昨年度までの年次報告・年次計画の内容を踏まえた上で、より理解を促すために再整理を行ったものであり、これまでの年次報告・

[1] 東京オリンピックは2021年７月23日から同８月８日に、東京パラリンピックは同８月24日から同９月５日に開催されることが2020年３月30日に決定された。

[2] 2018年７月に閣議決定された戦略では「2020年東京大会」という略称を用いていたものの、本書では「東京2020大会」と表記する。

年次計画を継続するものであることから、「サイバーセキュリティ2020」とする。本書において整理した施策の推進が、より豊かな国民生活の実現に資するものとなることを願っている。

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

本編

本編

1部　サイバーセキュリティを巡る動向

1章　サイバーセキュリティを取り巻く環境

1　新型コロナウイルス感染症への対応

2020年4月7日、新型コロナウイルス感染症に関する緊急事態宣言が発出され、「新型コロナウイルス感染症対策の基本的対処方針」（2020年3月28日（2020年4月7日改正版）新型コロナウイルス感染症対策本部決定）において、不要不急の外出など外出自粛の要請等を強力に行い、人と人との接触を徹底的に低減する旨の考え方が示され、事業者においては、テレワークなどを活用することで、さらに接触の機会を減らすことを協力して行っていく必要があるとされた。

こういった状況に対応するため、内閣サイバーセキュリティセンター（以下「NISC」という。）では、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を踏まえ、2020年3月27日に、国民一般向けに、テレワークを導入する際にセキュリティ上注意すべきポイントをホームページで公開するとともに、同4月7日及び9日に、政府機関等及び重要インフラ事業者等向けに、テレワークを導入する場合、セキュリティ上のリスクを把握し、適切に管理するよう、テレワークにかかる留意事項について注意喚起を行った。これらの内容については、テレワークの導入の必要性が高まっている中、国民一般の参考となるような内容でもあることから、同4月14日、周知対象の機関等や事業者のみならず、広く活用できるようホームページで「テレワークを実施する際にセキュリティ上留意すべき点について」の公開を行った。

新型コロナウイルス感染症の拡大を防止するためには、多くの人が集まる場所での感染の危険性を減らすことが重要であり、通勤ラッシュや人混みを回避し、在宅での勤務も可能となるテレワークは、その有効な対策であることから、総務省では、2020年2月25日に、可能な限り、テレワークの積極的な活用を行うよう周知を行うとともに、新型コロナウイルス感染症対策関連のホームページにおいて、新型コロナウイルス感染症対策としてのテレワークの積極的な活用の参考となるよう、テレワーク関連支援情報やセキュリティ確保に関する情報を掲載した。その中で、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示す「テレワークセキュリティガイドライン（第4版）」について改めて周知を行っている。また、新型コロナウイルス感染症の影響により、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、このガイドラインについて、より具体的で分かりやすく、実践的な内容のチェックリストの策定に向けた検討を開始するとともに、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2020年7月から開設している。このような取組も併せて幅広く周知していくことで、これからテレワークを導入する企業のセキュリティ対策だけでなく、テレワーク導入済企業におけるセキュリティ対策を強化していくことも期待されている。また、テレワークの推進に当たっては、デジタルで様々なやり取りを完結できる環境の構築が必要であり、電子データの信頼性を確保する基盤として、送信元のなりすましや電子データの改ざん等を防止することが重要であり、総務省においては、その仕組みであるトラストサービスを推進している。

経済産業省は、新型コロナウイルス感染症関連のホームページにおいて、企業を支援する

ための施策として、在宅勤務の推進、テレワーク導入に関する費用及び企業によるテレワーク支援についての情報提供を行っている。また、2020年4月17日、産業サイバーセキュリティ研究会において、新型コロナウイルスに乗じたサイバー攻撃の増加の状況を示した。海外においては、新型コロナウイルス対策を行っている医療関連機関に対するサイバー攻撃が確認されており、混乱に乗じたフィッシングメールや偽アプリ、フェイクニュースなども増加していることをまとめている[3]。同日、産業サイバーセキュリティ研究会は、直近の状況及び今後のデジタル化の急加速に対応するためのサイバーセキュリティの取組を促す「産業界へのメッセージ」を公表し、今般の事態を受け、今後、更にデジタル化を推進していくことの必要性が明らかになる中、改めてITシステムや制御システムのセキュリティ対策の強化をお願いするため、取り組んでいただきたいこととして、①「新型コロナウイルスを騙る不正アプリや詐欺サイト、フィッシングメール/SMSに注意すること」、②「NISCやIPA、JPCERT等の専門機関からの注意喚起を定期的に確認すること」、③「アップデート等の基本的な対策を実施すること」、④「ランサムウェアに感染した事態に備えてシステムやデータのバックアップと復旧手順を確認すること」を示した。中小・小規模事業者向けには、IT導入補助金を拡充するとともに、「通勤削減・人と人との接触削減のお願い」において、具体的なアクションを示すとともに、テレワークの導入に向けての情報提供を行っている。

また、新型コロナウイルス感染症やそれに伴う経済対策との関係性が明確に確認されてはいないものの、インターネット上で、日本の公的機関や企業等を模倣した多数のホームページが確認されており、NISCにおいては、2020年5月13日、SNS上において注意喚起を行い、URLのドメイン名を必ず確認すること、不審な場合には、安易にアクセスしたり、当該ページの何かをクリックしないことなど、国民に向けて注意点を周知し、適切な対応を促している。また、一般財団法人日本サイバー犯罪対策センター（JC3）においても、同5月14日、ホームページ上において同様の注意喚起を行っている。特別定額給付金や持続化給付金の電子申請も受け付けられており、一般向けの注意喚起については、継続して取り組むことが重要である。

基本的なサイバーセキュリティ対策としては、新型コロナウイルス感染症の発生後においても従来から指摘されている対策を確実に実践していくことが有効である。新型コロナウイルス感染症への対応を機に新たにインターネットを利用する場面が増加することへの対応としても、基本的な対策方法などについて効果的に周知活動を進めていくことが重要である。

緊急事態宣言は、2020年5月25日に解除宣言が行われたが、緊急事態措置の終了に当たって、環境変化に伴うリスクへの注意喚起として、同5月26日、独立行政法人情報処理推進機構（以下「IPA」という。）において、「テレワークから職場に戻る際のセキュリティ上の注意事項」を公表した。また、NISCにおいては、緊急事態措置が終了した後においても新しい生活様式の実践に向けて、テレワークの活用等の取組を継続的に行っていくため、情報セキュリティ上留意すべき点について、政府機関等、重要インフラ所管省庁それぞれに向けて注意喚起、事務連絡を発出するとともに、国民向けにも周知を行い、同6月11日、広く活用できるようホームページで「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」の公開を行った。

今回、個人用IoT機器であっても、緊急対応として社会インフラに関わる目的で活用せざ

[3] 第4回産業サイバーセキュリティ研究会（2020年4月17日）資料3「第4回産業サイバーセキュリティ研究会＜電話会議＞事務局説明資料」

るを得ない状況も多かったと推測されるなど、従来の対応の前提を越える状況も生じていたと考えられる。引き続き新しい生活様式の定着が求められており、テレワークの実施等人と人との接触数の削減のための取組が求められている中、状況を客観的に分析した上で、新しいデジタル技術の活用動向に合わせてサイバーセキュリティ対策を進めていくことが重要である。

2　新しいデジタル技術の活用とリスクマネジメント　～DX with Cybersecurity ～

戦略において、「任務保証」「参加・連携・協働」と並ぶ３つの観点の１つとして「リスクマネジメント」を示した。NISC としては、リスクマネジメントの基本的な考え方として、業務やサービスを遂行する際に生じ得るリスクについてのアセスメントを実施した上、残存リスクについては、リスクが顕在化した際の対応体制を整えるという２つのポイントを示している。

デジタル技術を活用した変革とそれを実行する上での体制や組織内の仕組みの構築のそれぞれについて取組が進められているが、重要な機能においても新しいデジタル技術を採用するに当たっては、この２つを一体的に検討を行うことが重要であり、また、自らが遂行すべき業務やサービス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という「任務保証」の観点からも検討が行われることも重要である。そのためには、リスクを特定・分析・評価し、リスクをコントロールするため、「リスクマネジメント」の考え方に沿って対応を進めることがより重要である。企業活動についても、国民生活についても、様々なリスクを考えなければならないが、そのリスクを把握することはできたとしても、全てのネガティブリスクをゼロにすることはできない。まずは、どのようなリスクが存在しているのか全体像を把握した上で、有効な対策を検討し、残存リスクが顕在化した場合の対応体制を明確化しておくことが重要である。

今後は、新型コロナウイルス感染症への対応として、人と人との接触を削減するため、テレワークの導入や活用だけではなく、サービスの提供自体にも新たなデジタル技術を活用することも想定される。これは、正に、これまでに提唱されてきた DX を推進していくことに他ならない。企業が新たなデジタル技術を活用する効果を最大限に享受するためには、まずはコアとなる事業も含めて、包括的に業務の見直しを行うことからはじめ、どのようなデジタル技術を使って何を実現したいのかを明らかにする必要がある。そのプロセスの一環においては、事業継続に致命的な影響を与えるリスクの洗い出しを行うことが重要であり、そのリスクの１つとして、新たなデジタル技術の活用に対応するサイバーセキュリティへの対応は最も重要な柱となるものである。緊急事態宣言を受けた企業活動については、東京 2020 大会に向けた取組として関係省庁・団体が連携して進めてきた「テレワーク・デイズ」や働き方改革推進の動きを受け、テレワーク環境の整備を進めていた企業は、その環境を活用することもできた。一方で、緊急事態宣言の後に新たにテレワーク環境を整備しようとした企業は、システム上の制約などが生じ結果的に業務に制約を生じたという状況もあったと考えられる。DX 推進に当たっては、サイバー攻撃を受けた際の対応などを業務継続計画（BCP）の中に位置づけ、体制や対応手順を明確化しておくことが重要であるが、そのことは、結果的に、BCP のシナリオとして想定するサイバー攻撃を受けた場合の対策となるだけでなく、不測の事態への包括的な対応力を強化することにもつながることが期待される。

新たなデジタル技術へのアクセシビリティは、万人に与えられるものであって、攻撃者が

排除されるものではない。防御側は、進化するサイバー攻撃に対し、それに備えたリソースの確保が求められるとともに、サイバー攻撃の複雑・巧妙化への対応として、防御側のサイバーセキュリティ対策に新たなデジタル技術を応用し、サイバーセキュリティ対策自体の高度化や効率化も期待されるところである。例えば、未公開脆弱性を突いた攻撃（ゼロデイ攻撃）等の巧妙な攻撃に対しては難易度の高い対応が求められるとともに、脆弱性情報や脅威情報の収集及びセキュリティのアラート分析・判断・対応などの業務は煩雑で、組織を疲弊させる。その結果、対応に遅れが生じるなどして適切な対応がとれなかった際には、単に攻撃への対応効率を損なうというだけではなく、致命的な被害を受けるおそれもある。このため、防御側において、システムログ及びネットワークトラフィックの分析基盤やIT資産管理ソフトウェアなどの可視化技術、脅威情報共有の機械化や脅威情報及び各種セキュリティ機器の連携によるインシデント対応の自動化技術といったデジタル技術を活用することにより、組織のサイバーセキュリティ対応能力の効果・効率を向上させるためにDXを推進することも重要な課題である。

さらに、現在の多様かつ流動的な企業間のつながりが存在する社会においては、サプライチェーン全体のサイバーセキュリティを向上させる観点から、中小企業・小規模事業者において、新たなデジタル技術の活用を推進していくことと、基本的なサイバーセキュリティ対策の方法を併せて普及させていくことが重要である。サプライチェーン全体のサイバーセキュリティ対策を誰の責任においてどこまで行うか、といった視点も重要である。

後述のように、諸外国においても国家安全保障の観点からのサイバーセキュリティの重要性は増している。同時に、安全保障の裾野は経済・技術分野に急速に拡大しており、DX推進におけるサイバーセキュリティの確保もそうした安全保障と経済を横断する領域の課題の一つと言える。こうした中、政府においては、経済分野における国家安全保障上の課題について、俯瞰的・戦略的な対応を迅速かつ適切に行うべく、2020年４月、国家安全保障局に経済班が設置された。また、昨年度、総務省にデジタル国際戦略室、外務省に新安全保障課題政策室、経済産業省に経済安全保障室が設置されている。

3　情報共有の推進と共助の取組

サイバーセキュリティは、本来、各々の組織において取り組むべきものであるが、サイバー攻撃が複雑・巧妙化し、脅威の変化が早い現状において、一組織の対応では限界があり、また、被害を受けた組織等から迅速な情報共有が行われなければ、攻撃手口や対策手法等を共有することができず、同様の手口によるサイバー攻撃の被害が拡大するおそれがある。

そのため、近年においては、サイバーセキュリティの確保のために、複数の組織が連携して情報共有を行うことの重要性が増しており、サイバーセキュリティに関する情報を一定のコミュニティにおいて共有する動きが一層活発化している。

具体的には、2018年12月に改正された基本法に基づき、国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うためのサイバーセキュリティ協議会が 2019 年４月に組織され、官民又は業界を超えた多様な主体が参加している。同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、これまで各組織に分散して存在し、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始めるなど、

一定の成果が得られたところである。引き続き、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かつ確実に共有されるとともに、より多くの主体が参加する重厚な体制が構築されるよう、協議会の運用を充実・強化させていくことが重要である。

NISCにおいては、官民・分野横断的な情報共有体制や重要インフラ事業者等における事業継続計画に関する実効性の検証及び課題の抽出を行うことにより、障害対応体制の強化を図ることを目的として、2006年度から分野横断的演習を実施している。一方で、ISACにおける情報共有においては、分野別の特性について配慮する必要もある。分野によって、歴史的背景や製品・サービスに関するルールなどについて事情が異なる点があり、また、同じ分野の中でも規模の違いによって前提としているシステムや体制が異なることから、同じ分野の同じ規模の事業者の間でノウハウや手法を共有することが有効となることもある。このような状況においては、情報共有を行う当事者同士の信頼関係の醸成が必要であり、分野横断的な枠組みではなく、環境が近い事業者に限定した枠組みによることで、より実践的な情報共有が図られるとの意見もある。

また、サイバー空間においては、事象の影響が容易に国境を越えることから、海外で生じたサイバー事案は常に我が国にも容易に影響を及ぼす可能性がある。そのため、平時からサイバー攻撃の情報や脅威情報を共有するとともに、国際サイバー演習への参加や共同訓練等を通じて、連携対処能力の向上を図ることにより、事故発生時に適切に国際連携しながら対処することが重要である。

このように情報共有の在り方は、単に全ての情報を１つの枠組みに集約すればよいというものではない。秘匿性を確保すべきものの、特定の分野にとっては価値の高い情報であり、その範囲で共有を行うことが総合的に適切であるような状況なども考えられる。多様な情報共有の枠組みが存在し、それらの役割分担によって、効果的、効率的に情報共有を進めていくことが重要である。また、情報共有活動は、枠組みを設定しただけで目的を達することができない。信頼を醸成しながら少しずつ活動の幅を広げていくなど、運用を充実させて絶やさないことが重要である。共助の仕組みは、便乗する者が大宗となれば活動を維持することが難しく、参加する構成員が各々の能力に応じた貢献を行うことも必要となってくる。それぞれの枠組みにおいて、構成員に対するインセンティブにも配慮してルールを設定しつつ、柔軟に対応できる体制も重要である。国は、そういった事情も踏まえて運用やサポートを行っていくことが重要である。

2章　2019年度のサイバーセキュリティに関する情勢

1　主なサイバーセキュリティ事案

サイバー攻撃による経済的・社会的損失については、現行戦略で、「実際に、IoT、仮想通貨を含むFintech、重要インフラ、サプライチェーンを狙った攻撃等により、従来の情報漏えいに加えて、直接的な金銭被害、業務・サービス障害が国内外で生じ、経済社会の持続的な発展や国民生活の安全・安心等を脅かす事例が生じている。」とされ、「業務・機能・サービス障害」「情報の毀損及び漏えい」「金銭の窃取・詐取等の被害」の３点に整理されていることを踏まえ、それぞれの分類に基づき、2019年度に発生した主なサイバーセキュリティ事案について以下に記述する。

1.1　業務・機能・サービス障害

AI・IoT等を活用したインフラ保安の合理化、自動運転等新たなモビリティサービスやオンライン診療及びスマート農業などの推進、行政サービスのデジタル化など、サイバー空間と実空間の一体化が進む一方、IoTを介した環境情報の取得やデータ分析結果に基づく自動制御など、サイバー空間と実空間の更なる一体化に伴って新たに発生する処理は未知の脆弱性を生むおそれがある。仮にサイバー攻撃を受け、IoT機器の意図しない作動や制御系システムの障害を招いた場合には、それを起点として、通信障害、交通混乱や停電等の社会の機能障害、人命や生活へのリスクを含む国民の安全・安心、国家の根幹をも揺るがす事態が生じる可能性がある。

2019年度には、国外において、ランサムウェアの感染により自治体の行政や工場の操業に影響を与えた事例や、年度末より流行が広がった新型コロナウイルス感染症に乗じたサイバー攻撃により医療関連機関においてITインフラが停止した事例などが確認されている[4]。また、国内においても、システム障害や自然災害等、サイバー攻撃に因らないサービス障害が発生している。

業務・機能・サービス障害の影響を与えるサイバー攻撃については、ランサムウェア被害によるものが複数確認されているところ、昨今、DDoS攻撃を示唆して金銭を要求する手口も確認[5]されている。このような動向も踏まえ、注目を集めるイベント等を狙った政治的目的や精神的目的による業務・機能・サービス障害に係るサイバー攻撃のみならず、経済的利益目的によるサイバー攻撃の脅威の高まりにも、警戒を強めることが重要である。

(1)　国際的なイベントに伴うサイバー攻撃の脅威

オリンピック・パラリンピックをはじめとするスポーツの祭典などの非日常のイベントは、世界的に注目度を集めるとともに、人々の気持ちに隙を生むため、政治的及び精神的目的を持つ攻撃者にとって攻撃のインセンティブを高めてしまうと考えられる。2019年度に我が国で開催されたラグビーワールドカップ2019においては、大きな支障を来すことなく、円滑な大会の運営が進められたが、今後、東京2020大会などが控えている中、こうした国際的なイベントの円滑な遂行を目指すためにも、大きな影響を及ぼし得る重要サービスを中心に、過去の事例や教訓を踏まえた対策強化が大切である。2019

[4] 2020年度には、国内における業務・機能・サービス障害について、2020年６月に大手自動車会社において、社内ネットワークシステムがサイバー攻撃を受けて障害が発生したとの報道も確認されている。
[5] https://www.jpcert.or.jp/newsflash/2019103001.html

年度には、国外において、オリンピックの公式SNSアカウントがハッキングされる事案や大会関係者を狙ったものと考えられる不審メールが確認[6]されており、引き続き注視が必要である。

(2)　重要インフラ分野等のサービス障害

重要インフラ分野等で発生した事案は、「2章3 重要インフラ分野等におけるサイバーセキュリティに関する情勢」でも詳述するが、2019年度は、米国の自治体においてランサムウェア被害が数多く発生しており、ランサムウェア感染によってコンピュータシステムが利用できなくなり行政業務に支障を来すなどの影響が発生している。

国内においては、サイバー攻撃に因らないサービス障害が複数発生しており、自治体向けクラウドサービスの障害により自治体の行政やウェブサイト閲覧等に影響が生じた事例などが確認されている。

(3)　インターネットサービス等のサービス障害

一般的なインターネットサービスなどが狙われて、国民の生活に影響を与える事例も存在しており、国内において、外部からの大量のアクセスを受けサーバが機能停止すること（DDoS攻撃）によりウェブサイトの閲覧障害が発生した事例が確認されている。

DDoS攻撃については、2016年、マルウェア「Mirai」により史上最大規模のDDoS攻撃が引き起こされた事例（Miraiに感染した10万台を超えるIoT機器から、ある米国企業のDNSサーバに大量の通信が送り込まれ、数多くのサイトにアクセスしにくくなる等の影響を与えたもの）があるが、2019年において、その亜種が機能を拡張し、攻撃活動を進化させていく様子が確認[7]されている。亜種の中には、制御系システムに関する脆弱性を狙う攻撃コードを含むものもあり、今後は、汎用的なIoT機器だけに留まらず、専門性の高い機器へも攻撃対象を拡大していくおそれがある。

1.2　情報の毀損及び漏えい

情報漏えいについては、引き続き、多くの被害が確認されており、氏名、住所、生年月日などの個人情報やWebサービス等の認証情報、銀行口座情報、クレジットカード情報など個人が社会活動の一環で利用するサービスに関する機微な情報を窃取する事案が発生しているとともに、企業経営や安全保障に影響を与える可能性のある営業情報、技術情報、知的財産などの機密情報が窃取される事案も表面化してきている。

また、「成長戦略実行計画（2019年6月21日閣議決定）」において、リアルデータや実空間での知識をいかし、サイバー空間への取組を官民上げて強化する必要があるとされているところ、企業等がデータの利活用により新製品やサービス等の新たな価値を生み出していくに当たって、そうした価値創出の源泉となるデータ自体が攻撃の対象となることも想定される。

個人情報や機密情報等の漏えいは、損害賠償請求の対象となるおそれがあるだけでなく、組織・企業の信頼失墜による競争力の低下や国家・社会・個人の安全への悪影響につながるおそれがある。

2019年度においては、ばらまき型メールによるEmotetの再流行が広がり、数多くの組

[6] https://blog.trendmicro.co.jp/archives/24169
[7] 出典：NICTER観測レポート2019

織・企業において情報流出等の被害が公表される事態が起こっている。また、外部からの不正アクセスによる機密情報等を狙った標的型攻撃や、内部不正による情報漏えいも複数確認されるなど、引き続き、多くの事案が発生している。また、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行う組織において、2019年には前年の約2.8倍の数のフィッシングに関する報告が寄せられた[8]ことが公表されている。攻撃者は様々なサービスや組織に偽装しており、2019年度末には、新型コロナウイルス感染症に関連したフィッシングの手口も確認されている。

今後、クラウドサービスを利用する組織・企業がさらに増加していく中、情報公開範囲の設定誤りや不十分なアクセス制限などの情報管理上の問題による情報漏えいも懸念されるとともに、価値のある情報がクラウドサービスへ集中していくことにより攻撃者の関心がそちらに向いていくおそれもある。クラウドサービスが攻撃を受けた場合には、多数の事業者に影響を及ぼす可能性もあり、サービス提供者及び利用者のそれぞれの責任範囲において、適切な対策を施すことが重要となる。

(1)　Emotetによる大規模なばらまき型攻撃

Emotetは2014年に存在が確認されたマルウェアであるが、機能追加による進化を遂げ、2019年度には、国内においても数多くの組織・企業にて感染被害が確認されている。進化したEmotetは感染端末のメールアカウントや本文などを窃取する機能があり、それを悪用することで、例えば取引先の担当者からの返信メールなどを装うことで、ユーザに不正なファイルやURLを開かせることを誘い、感染を広げていく。また、国外ではEmotetの多機能性を活かして、他のマルウェアの感染につなげる事例も確認されている。今後、新たな機能が追加されるなどした場合には、脅威が高まるおそれがあり、引き続きの警戒が重要である。

(2)　特定の企業を狙う標的型攻撃による情報漏えい

2020年1月、国内の大手電機会社が、自社のネットワークが不正アクセスを受け、個人情報と企業秘密が流出した可能性があることを公表した。当該企業の報告書では、未公開脆弱性を突いた攻撃を受けたことが言及されている。また、そのほかには、複数のショッピングサイト等のインターネット上のサービスにおいて、脆弱性等を悪用した不正アクセスを受け、クレジットカード情報等の個人情報が漏えいしたおそれがあることが公表されている。

また、国外においては、米国大手金融にて、セキュリティ機器の設定不備等を原因に不正アクセスを受け、クラウド上に保持していた1億600万人の個人情報が漏えいした事案が発生している。

(3)　内部不正による情報漏えい

2019年12月、国内の情報機器の処分や再生事業を営む企業において、行政文書が蓄積されたハードディスクドライブ(HDD)について、従業員がデータ消去作業前に盗み出し、ネットオークションを通じて転売していたことが明らかになった。そのほか、ある自治体において、勤務先のサーバに対して、勤務先の職員のID・パスワードを無断で使用して不正アクセスし、データを不正に入手した事案などが発生している。

[8] 出典：フィッシングレポート2020

また、国外においては、サイバー関連事業者の従業員が顧客サポートのデータベースに不正アクセスを行い、約６万８千人分の顧客情報を第３者に販売していた事案が公表されている。

1.3　金銭の窃取・詐取等

2019年10月、 キャッシュレス・ポイント還元事業が開始され、2020年４月には、全国約110万店の店舗が事業に参加するなど、官民連携によるキャッシュレスの促進が図られている。ある調査では、当該事業により、４割を超える消費者が「キャッシュレス支払いを始めて利用した」又は「新たに支払い手段を増やした」と回答[9]しており、キャッシュレス決済の普及が広がっていることがうかがえる。今や様々な経済活動に伴う送金や支払において、キャッシュレス決済をはじめとしたFintechは人々の生活に密接に関わりのあるものとなってきている。

他方、多くの企業が新しいサービスを創出することに伴って、未知のシステムの脆弱性を突いた不正アクセスや巧妙な手口のフィッシング詐欺など、新たなセキュリティ上の問題が生じることも懸念される。

2019年度には、何らかの手段で取得された多数のID・パスワードを悪用してシステムの不正利用を行う手口や、ワンタイムパスワード認証を突破するフィッシングの手口による被害が確認されており、中には被害を受けた結果、サービス廃止に至った事案も発生している。

攻撃者は、システムや人の脆弱性に目をつけ、より低い労力で多くの利益を得られる手口や対象を狙う傾向にあると考えられ、例えば、人の脆弱性を突いた攻撃として、過去から存在する手口にビジネスメール詐欺などが存在するが、今後、AIのような新たな技術の浸透が進むにつれて、AIを駆使した文章や音声及び動画等の偽装による詐欺の手口なども懸念される。

(1)　キャッシュレス決済サービスの不正利用

2019 年７月にサービスを開始したコード決済サービスが、不正アクセスを受け、約3,800万円の被害を受けた事案が発生している。何らかの手段で取得された多数のID・パスワードを悪用してサービスを不正利用された可能性が高いとみられ、システム上の認証レベルの検討が十分でなかったこと等が原因とされており、抜本的な対応を完了するには相応の期間を必要とすること等を理由に、サービスの廃止に至った。そのほか、スミッシング（SMSを使ったフィッシングサイトに誘導する手口）によるスマートフォン決済サービスの不正利用なども確認されており、普及の進むキャッシュレス決済サービスに対するセキュリティ上のリスクが表面化してきている。

(2)　インターネットバンキングに係る不正送金事犯

2019 年のインターネットバンキングに係る不正送金事犯による被害は、発生件数1,872件、被害額約25億2,100万円で、発生件数は過去最多の2014年に次ぐ件数となり、被害額も2018年と比べて大幅に増加している[10]。2016年以降、発生件数、被害額共に減少傾向にあったところ、2019年９月から被害が急増している。被害の多くは、SMSや

[9] 出典：未来投資会議（第36回）資料
[10] 出典：令和元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（警察庁）

電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられており、誘導されたフィッシングサイトで、インターネットバンキングのID・パスワード、ワンタイムパスワード等を窃取されて金融機関のウェブサイトから不正送金される被害などが確認されている。

(3)　ランサムウェア

国内において、ランサムウェアの被害は減少傾向[11]にある。ただし、2017年に盛り上がりを見せた「WannaCry」に関連するポートへのスキャンが沈静化していないことが観測されている[12]とともに、ランサムウェアに感染した端末の機密情報を暴露する脅迫の手口が登場するなどの変化も確認されており、その脅威はいまだ衰えていない。

国外においては、米国の自治体などを標的としたランサムウェア攻撃が数多く発生している状況であり、現時点では、米国と比べ、日本におけるランサムウェアの被害は小さいと思われるものの、日本の各組織においても、あらかじめ対応策を検討、実施しておくことが重要である。

[11] 出典：トレンドマイクロレポート2019年年間セキュリティラウンドアップ
[12] 出典：NICTER観測レポート2019

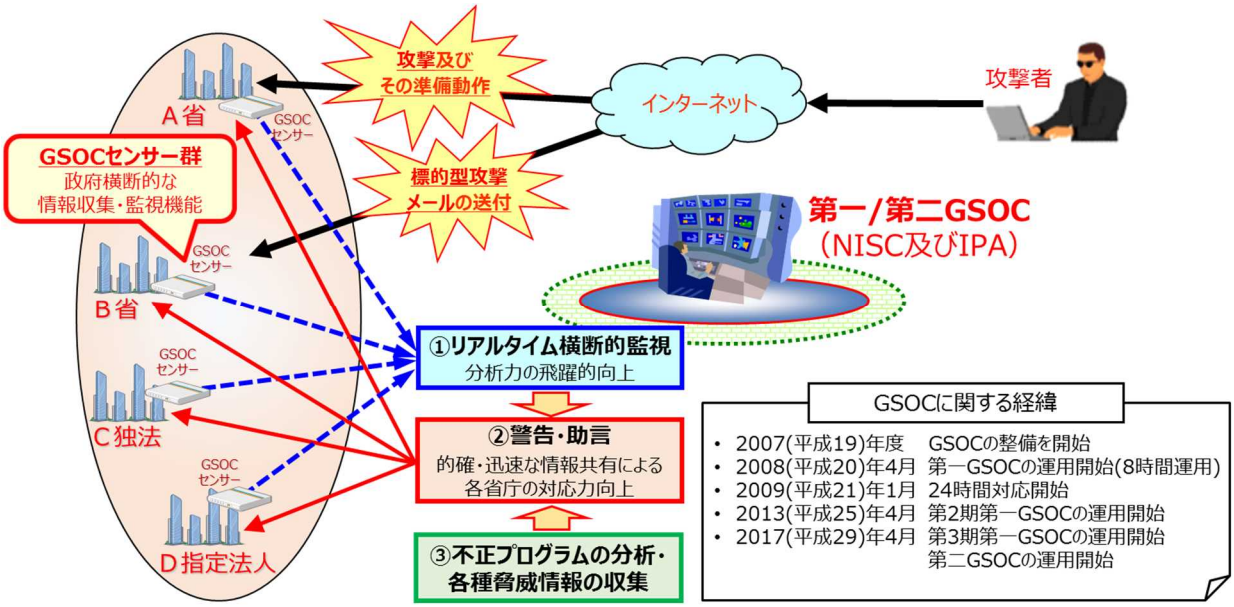
2　政府機関等におけるサイバーセキュリティに関する情勢

2.1　政府機関等[13]におけるサイバーセキュリティに関する体制

政府機関等におけるサイバーセキュリティ対策について、政府横断的な立場から推進するため、2008年４月からNISCにおいて政府機関に対する情報セキュリティ横断監視・即応調整チーム（第一GSOC [14]）を、また、2017年４月からNISCの監督の下、IPA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



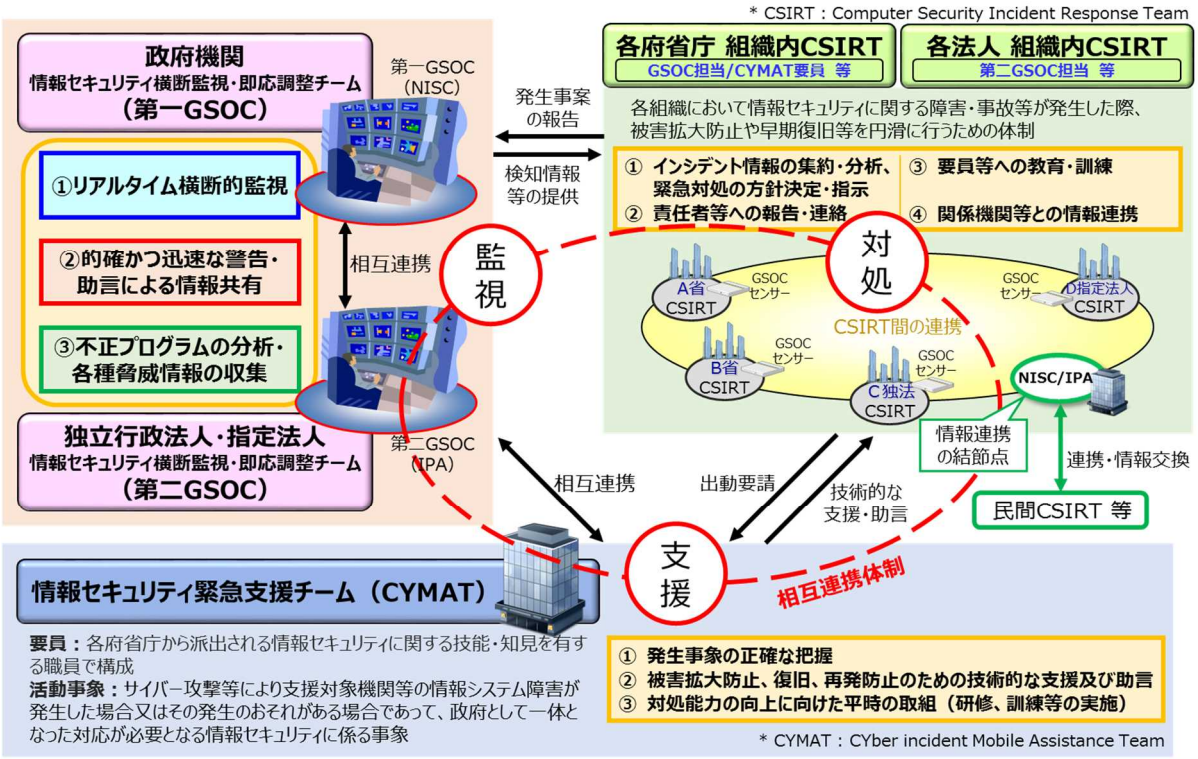
また、NISCは各府省庁の要請により情報セキュリティ緊急支援チーム（CYMAT[15]）を派遣し、技術的な支援・助言を実施している。

一方、各府省庁や各法人はそれぞれ組織内CSIRT[16]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）。

[13]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。
[14] GSOC（Government Security Operation Coordination team）
[15] CYMAT（CYber incident Mobile Assistance Team）
[16] CSIRT（Computer Security Incident Response Team）

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　2019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[17]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Web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、

[17] 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2019年度の情報セキュリティインシデント一覧」を参照。

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

センサーによる横断的な監視や政府機関等のWeb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。）[18]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。

2019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年度に引き続き低い水準となった[19]。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、「Apache Struts」を狙った通信が多数検知された2017年度は1,545件を数えたが、2018年度からはこのような攻撃に対する対策が進んだ結果、当該攻撃に係る通信は確認を要するイベントではなくなっており、2018年度に11件、2019年度に23件検知したのみであった。

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件検知しており、そのうち3,479件は特定のリモートアクセスアプリケーションの通信が占めていたが、当該通信が発生した機関においてそれ以降このアプリケーションの使用を取りやめたため、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件検知したのみとなっている。これについては、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、検知件数が少なくなっていると考えられる。

また、マルウェア感染の疑いや標的型攻撃の検知件数は図表１－２－３のように推移している。

[18] 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。

[19] 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
マルウェア感染の疑い	169	111	55
標的型攻撃	57	66	30
その他	0	5	5

(件)

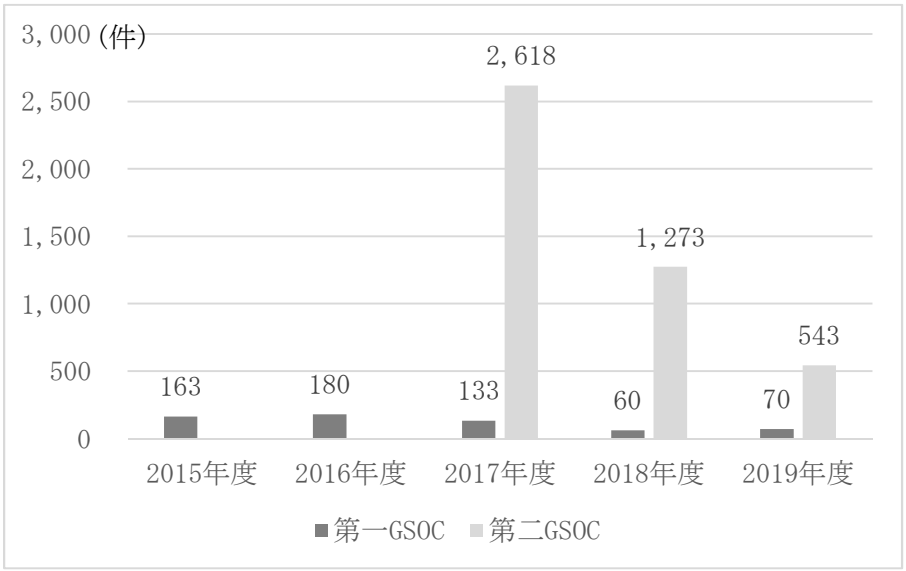
そのほか、2019年度は調査行為とみられる通信やタイポスクワッティングの疑いのある通信を合わせて５件検知した。一方、確認を要するイベントとして検知するような顕著なDoS攻撃は無かった。

また、第二GSOCにおいては、ウェブアプリケーションの脆弱性を狙った攻撃や不審メールの検知が多かった。

(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、2019年度においては、第一GSOCでは70件、第二GSOCでは543件の通報を行った（図表１－２－４）。なお、2017年度に運用を開始した第二GSOCでは、対象機関のシステムや業務等の特性に応じた詳細な分析に基づく通報の実施に係る判断基準について、一部の法人と引き続き調整を継続していることから、第一GSOCと比べて通報件数が多くなっている。

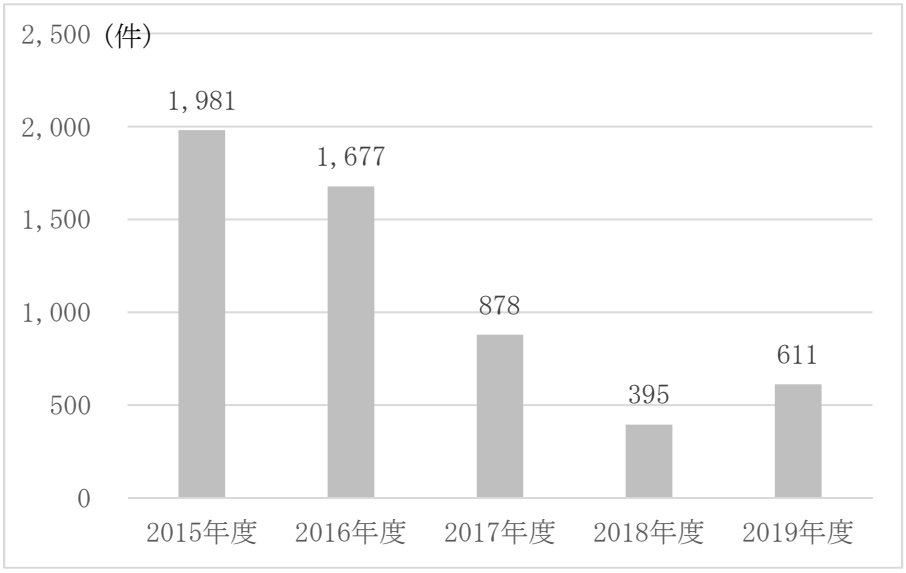
図表１－２－４　GSOCセンサー監視等による通報件数の推移



(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、2019年度においてはGSOCから611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



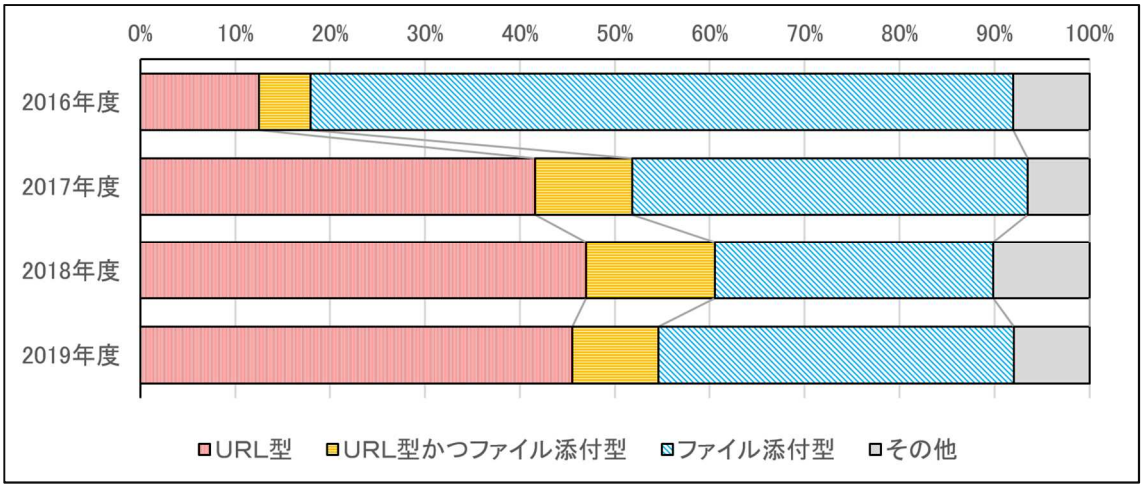
この注意喚起の件数は2018年度まで減少傾向にあったが、2019年度は後期にかけて我が国においてもマルウェア「Emotet」が流行したことを踏まえ、これらに関する注意喚起を行ったため、増加した。不審メールの中には、実在する組織やその所属職員とのやりとりに、その職員になりすまして返信する形で送付されるものもあるため、より一層の注意が必要である。

コラム　～政府機関等に対する不審メールの傾向～

○　不審なファイルに導く手法の傾向

図表１－２－６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における、不審なファイルに導く手法の割合を示したものである。2017 年度を境として、メール本文に URL を記載し、不審なファイルをダウンロードするサイトへアクセスさせる手法（以下「URL 型」という。）が増加し、その後も不審なファイルをメールに添付する手法（以下「ファイル添付型」という。）とほぼ同じ割合という状況が続いている。

図表１－２－６　不審メールの傾向



○　マルウェア「Emotet」の爆発的流行

2019年度は、マルウェア「Emotet」に関連する不審メールが世界的に広まり、政府機関等でも大量に受信した。GSOCへの解析依頼は2018年度下期からあったが、2019年６月から９月の間なくなり、10月から2020年２月にかけて急増した。

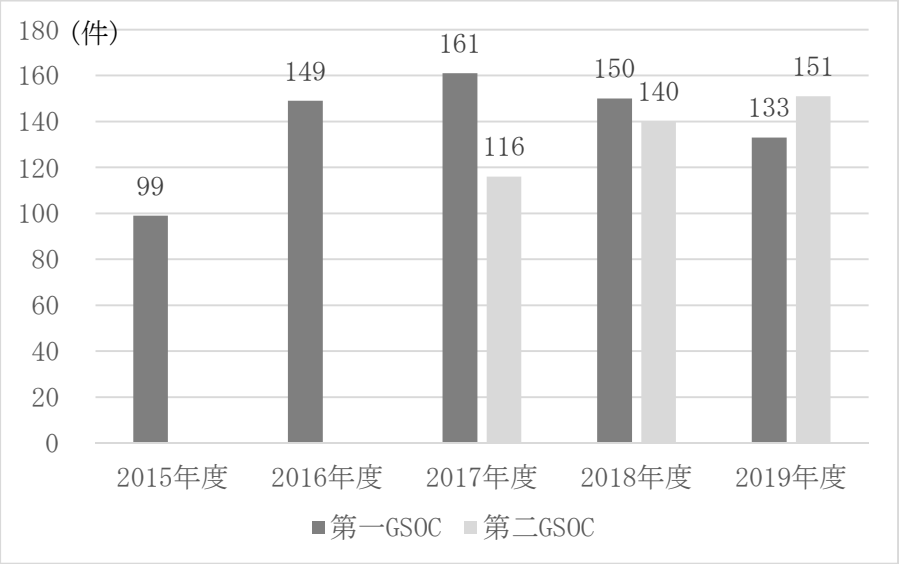
Emotetは、2014年にバンキング型トロイの木馬として初めて検出された。攻撃者により様々な機能が追加された結果、現在は他のマルウェアに感染させる入り口として使われている。Emotetの拡散手法として、Emotetのダウンローダであ るMicrosoft Wordファイルが添付されたファイル添付型と、ダウンローダのURLが記載されているURL型を確認しているが、2019年10月以降は、昨年度のコラムで紹介した「過去に送付したメールへの返信メールを装う手法」が多く用いられているという特徴がある。これは、受信者に不信感を抱かせずに感染させる目的で、Emotetに感染したコンピュータに保存されていたメールやアドレス帳の情報を窃取して利用するよう、機能が高められた結果と思われる。

(4) ソフトウェアの脆弱性情報の配信

GSOCでは、Web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。2019年度においては、第一GSOCから133件、第二GSOCから151件の脆弱性情報等を配信した（図表１－２－７）。

第一GSOCにおいては、配信数の緩やかな減少に比べて、脆弱性を狙った確認を要するイベント検知件数は前述のとおり急激に減少しており、政府機関等のソフトウェアの脆弱性に対する対策の迅速化が進んでいるものと考えられる。第二GSOCにおいては、独立行政法人等の組織数が府省庁等に比べて多く、その分使用するソフトウェアの種類も多いとみられるため、幅広い種類のソフトウェアの脆弱性情報を配信しており、第一GSOCとは異なる傾向となっている。

図表１－２－７　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、2019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、ICTの発展に伴い、クラウドサービスを悪用して正常な挙動に偽装する攻撃や、検知が難しいとされるスクリプトを用いた攻撃、関係者からの返信を装い自然な日本語を用いたメールによる攻撃など、高度化・巧妙化した手口の攻撃が発生している。さらに、政府機関等に対して直接攻撃が行われなくても、関連組織や取引先企業等が攻撃を受け、そのインフラを踏み台にした攻撃やその構成員を騙ったメールによる標的型攻撃が行われることも考えられる。

このように、政府機関等に対する実質的な脅威度は引き続き高い状況にあると考えられ、これらの攻撃に対応するためには、組織内のIT資産管理の徹底と脆弱性への迅速な対応、境界監視をすり抜け内部へ侵入されることも念頭に置いた対策が重要である。

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

2.3　2019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。

2019年度も、職員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。

個人情報が記載されているファイルが入っているノートPCやUSBメモリ等を出張時に盗まれた事案や、BCCで送付すべき一斉送信メールをToやCCで送付してメールアドレスが流出した事案、関係者にのみ公開すべきファイルがサーバの設定ミス等で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、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。

3　重要インフラ分野等におけるサイバーセキュリティに関する情勢

2019年度、国内外において重要インフラ分野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。

国外の事例としては、米国の自治体においてランサムウェア被害が数多く発生した。2019年５月には、フロリダ州リビエラビーチ市において、端末がランサムウェアに感染し市のコンピュータシステムが利用できなくなり、65ビットコイン(約6,400万円相当)を支払うこととなった。６月には、フロリダ州レイク・シティ市において、端末がランサムウェアに感染し、42ビットコイン(約5,400万円相当)を支払うこととなった。こうした状況を受け、全米市長会議は、ランサムウェアによる攻撃を受けても身代金を支払わないという決議を採択した。さらに、12月には、ランサムウェア等のサイバー攻撃の未然防止及び発生時のインシデントレスポンスを目的として、米国国土安全保障省(DHS)国家サイバーセキュリティ通信統合センター(NCCIC)配下にHunt and Incident Response Team(HIRT)を発足させ、連邦政府レベルで未然防止と迅速な対応を行えるようにした。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ことから、こうした動きに注視する必要がある。

サイバー攻撃やシステム障害が事業継続に対して大きな影響を与える事例もあった。2019年３月、ノルウェーの大手アルミニウム製造業者Norsk Hydro社がサイバー攻撃によりランサムウェアに感染した。複数の事業に影響が発生し、工場の操業を手動による操作に切り替えて運用した。本事案による同社の損失は、2019年１～６月の間で約65～77億円相当と見積もられている。2018年10月及び2019年３月に相次いで発生した米国の大手航空機製造業者ボーイング社製の旅客機737MAXの墜落事故は、機体の電子制御システムの不具合が一因とみられ、同型機の全世界での運航停止へとつながった。本事案に関連した費用が積み重なった結果、同社の2019年通期決算は大幅な赤字となった。このように、重要インフラ分野におけるシステムの不具合が会社経営に大きな影響を与えた。

国内では2020年１月30日、サイバーセキュリティ戦略本部において「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の基本的枠組み」が決定され、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促進に関し、一定の方向性が示された。他方、クラウドサービスの障害によって複数の事業者のサービスに影響を与えた事例が相次いで報告された。2019年８月には、米国系ベンダー２社がそれぞれ国内で提供するクラウドサービスの障害が発生し、国内の様々な業種のサービスにおいて影響が発生した。11月には、国内ベンダー２社で障害が発生し、重要インフラサービスにも支障を来した。12月には、自治体向けクラウドサービスにおける障害が原因で、50を超える自治体で戸籍の証明書発行、ウェブサイト閲覧等のサービス提供に影響が発生した。2020年２月には、米国系ベンダーの障害によって、複数の銀行においてATMやインターネット取引等が利用できなくなった。このように、クラウドサービスは利便性が高い反面、障害発生により重要インフラ事業者等が提供するサービスへの影響が生じることが明らかとなった。クラウドサービスを利用する重要インフラ事業者等は、外部サービスであるクラウドサービスの利用に際しては、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。

クラウドサービスにおける障害と同様に、外部サービス利用時の委託契約の課題が浮き彫りとなる事例が発生した。2019年12月、ある自治体がリース契約で調達した行政文書が蓄積されたハードディスクドライブ(HDD)について、契約満了に伴い返却したところ、下請事業

者の従業員が盗み出し、ネットオークションを通じて転売、落札者が市販のソフトで内容を復元した事案が発生した。自治体がリース企業と締結した契約においては、機器返却後には契約相手方が「データ復旧が不可能とされている方法によりデータ消去作業を行う」としており、自治体はデータ消去証明書の提出を求めていたが、証明書は提出されていないままの状態が継続していた。本事案では、適切な契約を締結しても契約に従った行為が履行されないままの状態になっていたことが課題として挙げられる。サプライチェーンマネジメントに注目が集まる今日において、データのライフサイクル全体を視野に入れたサプライチェーンマネジメントの実効性をどのように担保するのかを問いかけるものとして着目すべき事案である。

2019 年 10 月１日の消費税率改定に伴うキャッシュレス・消費者還元事業が開始されるまでに、様々な事業者がキャッシュレス手段による決済サービスを開始した。他方、これに伴う様々なトラブルも発生した。2019 年７月には、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したが、初動対応の不手際などから、３か月でサービスを廃止するに至った。不正利用の原因は、攻撃者がどこかで不正に入手した ID・パスワードを用いたリスト型攻撃である可能性が高いが、根本的には、他の多くの決済サービスにおいて不正利用対策として使用されている２段階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あった。セキュリティ・バイ・デザインの考え方を念頭に置き、システム設計、構築がなされないと経営問題にまで発展する典型的な事案といえる。

2019 年度は、マルウェア「Emotet」への感染が重要インフラ分野等においても数多く報告された。５月には、医療機関において、職務用パソコン端末へ送信されたメールの添付ファイルを職員が開封した結果、「Emotet」に感染し、当該職員のメールボックス内のメールを窃取され、職員をかたったなりすましメールが多数送信された。2019 年秋頃からは国内で同様の被害が増加し、複数の情報セキュリティ関係機関やサイバー関連事業者が注意喚起を行っているが、マルウェアは日々巧妙に進化しており、予断を許さない状況が続いている。

2018 年度に引き続き、2019 年度も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。2019 年９月には、関東地方に令和元年房総半島台風（台風第 15 号）が直撃し、関東広域で最大約 93 万戸の停電が発生した。特に千葉県内では送配電設備の被害が大きく、復旧作業に時間を要した。電力会社は、停電が発生した後、情報発信を行ったものの、復旧見通しを何度も延期することとなり、被災者の混乱を招いた。10 月には、東日本に令和元年東日本台風（台風第 19 号）が直撃し、関東地方や甲信地方、東北地方等で記録的な大雨となり、甚大な被害をもたらした。台風の接近に伴い各地方自治体は、台風に関連する災害情報を発信したが、複数の自治体のウェブサイトではアクセスが集中し、つながりづらい、表示速度が極端に低下する、接続できないといった障害が生じた。災害発生時に適切な情報を的確なタイミングで発信できるよう、平時から備えておくことが課題である。

2019 年５月には、改元に伴い過去最長の 10 連休となり、システム障害の発生が懸念されていた。そのため、10 連休を迎えるに当たり、事前に政府機関や各事業者等は注意喚起を実施した。多少の混乱はあったものの、総じて、国民生活に支障を生じさせるようなシステム障害は発生しなかった。10 月１日には、消費税率が改定された。同日前後には、軽減税率の計算誤りなどのシステム障害が発生したが、大きな混乱は生じなかった。こうした稀に発生する大きな社会システム変更で得られた知見を適切に記録し、知見を共有する取組が重要となる。

4　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、トランプ大統領が2017年５月に米国連邦政府のネットワーク及び重要インフラ事業者のサイバーセキュリティ強化に関する大統領令[20]に署名し、関係機関は同大統領令に基づく報告書を発表。2018年９月、新たな国家サイバー戦略を公表し、「連邦政府のネットワークと重要インフラの保護」、「デジタルエコノミーの繁栄」、「サイバー抑止イニシアティブの立ち上げ」、「開放的で相互運用性があり、安全で信頼できるインターネットの維持」等に言及している。また、同11月に国土安全保障省の機構改組で同省内に設置されたサイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA[21]）において、官民協力を推進し、あらゆる脅威やリスクから重要インフラを防護する体制が強化されている。2019年５月には米国におけるサイバーセキュリティ人材の強化を目的とした大統領令[22]が発令された。また、2018年８月、2019年度国防授権法が制定され、2019年５月には、情報通信技術及びサービスのサプライチェーンの保護に関する大統領令[23]が署名される等、国家安全保障の観点からのサイバーセキュリティの重要性が高まるとともに、サプライチェーン・リスク対策も強化している。

欧州連合（EU）では、2017年７月、欧州理事会において「サイバー外交ツールボックス」が承認され抑止力の強化が図られるとともに、2018年12月、欧州サイバーセキュリティ機関（ENISA[24]）の権限拡大や認証枠組みの導入を含むサイバーセキュリティ法が成立した他、加盟国におけるNIS指令[25]の国内法化がなされる等、欧州一体としてサイバーセキュリティ対策を強化している。また、2018年５月に、一般データ保護規則（GDPR）[26]が施行されている。さらに、サプライチェーン・リスクに関しては、2020年１月に5Gネットワークのサイバーセキュリティに関するツールボックスを策定し、加盟国に対し、機器供給者のリスク評価等を促している。

中国は、2017年６月、「サイバーセキュリティ法」を施行し、同法に基づく関連規制（ネットワーク製品及びサービスの安全審査弁法、個人情報及び重要データの越境安全評価法、重要情報インフラ保護弁法等）を制定した。ロシアは、2016年12月、「情報安全保障ドクトリン」を公表し、サイバー空間におけるロシア連邦の安全保障を目的としたサイバーセキュリティ政策の方向性を明示している。

---

[20] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

[21] Cybersecurity Infrastructure Security Agency

[22] Presidential Executive Order on America's Cybersecurity Workforce

[23] Presidential Executive Order on Securing the Information and Communications Technology and Services Supply Chain

[24] 2019年６月に施行された欧州サイバーセキュリティ法に基づき、ENISAの名称が、欧州ネットワーク・情報セキュリティ機関（European Network and Information Security Agency）から欧州サイバーセキュリティ庁（European Union Agency for Cybersecurity）に変更された。

[25] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

サイバー空間における国際法の適用に関する議論については、「2部3章1.5 国際的な議論の高まりと統一的な国際ルールへの期待」でも詳述するが、第５期サイバーセキュリティに関する国連政府専門家会合（GGE）[27]は、国際法の適用の在り方等について、参加国の意見が一致せず、コンセンサス報告書を発出することがかなわなかったものの、2018年国連総会決議に基づき、2019年12月に第６会期が立ち上がり、新たな報告書作成に向けて議論を深めている。また、2018年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オープン・エンド作業部会も2019年６月に組織会合が開催され、2020年の国連総会において報告書を提出するべく議論を進めている。そのほかG7においては、2019年４月ディナール外相会合の外相共同コミュニケにおいて、悪意のあるサイバー活動を非難し、そのような活動を防止する目的の措置を発展させるよう協力を強化すべき旨再確認し、「サイバー規範イニシアチブに関するディナール宣言」を発出した。2019年６月に開催されたG20大阪サミットにおいては、第２セッション「イノベーション」において、安倍総理から、イノベーションは経済発展と社会的課題の解決を両立する鍵であり、中でも発展著しいデジタル化に際して、データの自由な流通が不可欠である旨指摘した上で、「信頼性のある自由なデータ流通（Data Free Flow with Trust：DFFT)」の考え方を提示した。また、本セッションに先立って開催された「デジタル経済に関する首脳特別イベント」における「大阪トラック」の立ち上げに言及しつつ、今後、同トラックを通じ、WTOでの電子商取引をはじめとするデジタル時代のルール作りを進めていきたい旨述べた。また、AI等の先端技術の活用にも「信頼」が不可欠である旨強調し、G20・AI原則の重要性についても言及した。首脳宣言において「我々は、デジタル経済におけるセキュリティを促進すること及びセキュリティギャップと脆弱性に対処することの重要性が高まっていることを認識する。我々は、知的財産の保護の重要性を確認する。モノのインターネット（IoT）を含む新興技術の急速な広がりに伴い、デジタル経済におけるセキュリティについて進行中の議論の価値は高まっている。我々、G20構成国は、これらの緊急の課題への更なる取組の必要性を認識する。」旨明記された。さらに、「テロ及びテロに通じる暴力的過激主義（VECT）によるインターネットの悪用の防止に関するG20大阪首脳声明」において「オンラインプラットフォームに対し、法の支配はオフライン同様にオンラインでも適用されるという中核的な原則を遵守する」ことを強く促すこととされた。

サイバー攻撃に一国のみで対応することは容易ではなく、国際社会全体との連携や協力、法の支配による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。

[27] 国連総会決議（A/RES/70/237）に基づき、2016年８月から2017年６月まで４回の会合（合計20日）を開催。

2部　我が国のサイバーセキュリティ政策

1章　基本的枠組み

基本法第12条に基づき2015年に策定された旧サイバーセキュリティ戦略（2015年９月閣議決定。以下「旧戦略」という。）は、策定後３年間を計画期間としており、2018年に計画期間を終えることから、政府は、サイバー空間と実空間の一体化に伴う脅威の深刻化を踏まえ、2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間の諸施策の目標及び実施方針を盛り込んだ新たな戦略を2018年７月に決定した。

また、従来の枠を超えた情報共有・連携体制の構築に向けた取組として、サイバー攻撃による被害の発生及び被害の拡大を防止するためのサイバーセキュリティ協議会の組織などを柱とするサイバーセキュリティ基本法の一部を改正する法律（平成30年法律第91号）が成立（2018年12月５日）し、2019年４月１日に施行された。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、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。

基本法については、サイバーセキュリティ対策において参照すべき関係法令を Q&A 形式で解説する「サイバーセキュリティ関係法令 Q&A ハンドブック」（2020 年３月２日公開） において概説されている。

2　サイバーセキュリティ戦略について

現行のサイバーセキュリティ戦略は、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旧戦略を初めて改定したものであり、基本法に基づく２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 年以降の目指す姿も念頭におきつつ、今後３年間（2018 年～2021 年）の諸施策の目標と実施方針を国内外に示すものである。また、一部の国家において見られるサイバー空間を管理・統制する潮流に対し、「こうした管理・統制の強化はサイバー空間の自律的・持続的な発展の可能性を閉ざす」との認識の下、「自由、公正かつ安全なサイバー空間」という基本的な理念をはじめとした、旧戦略で示した我が国の基本的な立場を堅持することを示したものでもある。

戦略では、サイバー空間と実空間の一体化の進展に伴い、脅威が深刻化しているとの認識の下、サイバーセキュリティの基本的な在り方として、持続的に発展するサイバー空間が維持される姿を「サイバーセキュリティエコシステム」とし、３つの観点（①任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進することが示された。これは、旧戦略で示した施策実施に当たっての３つのアプローチ（①後手から先手へ、②受動から主導へ、③サイバー空間から融合空間へ）を、具体的な取組を進めるに当たっての方針の参考となるよう、３つの観点として再整理したものである。

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、内閣サイバーセキュリティセンター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。

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

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

【昨年度の取組実績】

企業が直面するサイバーセキュリティに係るリスクが高まっている中、全ての産業分野においてサイバーセキュリティに取り組む必要があるとの認識を広げる必要がある。また、その取組をリスクマネジメントの一環と捉え、自然な形で対策が組織に浸透していくことが重要である。これらを踏まえ、以下の取組等を実施した。

経営層の意識改革に向けた取組としては、グループ経営を行う上場企業を対象とするグループ・ガバナンス・システムに関する実務指針（グループガイドライン）にサイバーセキュリティ対策の在り方を位置付けた。また、2019年３月に公開した「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」に関して、2018年度に収集していない指示項目を中心にプラクティスを収集し改定を実施するとともに、企業のサイバーセキュリティ対策の実施状況を可視化するツールのβ版を2020年３月に公開した。さらに、企業における平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、情報の取扱いに関する法令や情勢の変化等に伴い生じる法的課題等を可能な限り平易な表記で記述した「サイバーセキュリティ関係法令Q&Aハンドブック」を2020年３月に公表した。

サイバーセキュリティに対する投資の促進に関する取組としては、民間企業におけるサイバーセキュリティ対策の情報開示の促進に資するよう、参考となり得る事例等をまとめた「サイバーセキュリティ対策情報開示の手引き」を、2019年６月に公表した。

先端技術を利活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の観点では、コラボレーション・プラットフォームの開催に加え、地域に根差したセキュリティコミュニティの形成を促進するために、東北や中国地域等で地方版コラボレーション・プラットフォームを開催した。また、カンボジアにおける教育プログラムの展開可能性の調査や、インドにおけるサイバー攻撃に強い電力制御システム（SCADA）の導入のための現地の電力企業向け研修を実施した。

【評価】

経営層の意識改革に関しては、企業のサイバーセキュリティ対策の実施状況を可視化するツールのβ版や、「サイバーセキュリティ関係法令Q&Aハンドブック」など、2019年度も取組の推進に資するツールの整備を進めた。今後も引き続き、これらの活用を促進するとともに、「取締役会の実効性評価」の評価項目においてサイバーセキュリティへの経営層の関与を組み込むことなど、経営層の関与を高めるための取組を進めていくことが重要である。また、サイバーセキュリティに対する投資の推進や、先端技術を利活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に関しても、これまでに整備したツールの活用促進を進めていくことが重要である。

【今年度の取組】

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、必要に応じてフォローアップや見直しを図る。

具体的には、経営層の意識改革については、取締役会の関与や投資家への啓発に向けた、サイバーセキュリティへの経営層の関与に関する、取締役会実効性評価への組み込み促進や、サイバーセキュリティ経営ガイドラインの普及、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の可視化ツール開発を行う。

サイバーセキュリティに対する投資の促進については、「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」や「サイバーセキュリティ対策情報開示の手引き」の普及や、「情報セキュリティサービス基準」に関する、サービスの拡張も含めた更なる改善を図っていく。

先端技術を利活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については、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や調査を実施する。また、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～」や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の普及啓発を図る。加えて、「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」、クラウドセキュリティ監査制度等の普及を図る。さらに、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。

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

【昨年度の取組実績】

サプライチェーン全体に対して、一貫性をもった必要な対策が実装されることが不可欠であることを踏まえ、以下の取組等を実施した。

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）」において策定した「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・普及に取り組むとともに、ビルシステムのセキュリティに関するガイドラインの第１版の公表をはじめ、各産業分野におけるセキュリティ対策の検討を進めた。また、サイバー空間とフィジカル空間のつながりにおける信頼性確保等について議論する「第２層タスクフォース」や、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」、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」を立ち上げ、それぞれ検討を行った。

また、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に関しては、「戦略的イノベーション創造プログラム（SIP）」において、サイバー・フィジカル・

セキュリティ対策基盤の構築に向けて、基本方式の設計やデモシステムの開発を実施するとともに、2020年度から予定している実証実験の準備を進めた。

中小企業の取組の促進に向けては、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に関する仕組みの構築を目的とした実証事業である「サイバーセキュリティお助け隊」を全国８地域で実施した。約1,000社の中小企業が実証に参加し、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難な中小企業があり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、サービス購入費用が中小企業にとって許容可能な価格である必要があること等、中小企業の実態・ニーズが明らかとなった。また、SECURITY ACTIONを引き続き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るとともに、「中小企業の情報セキュリティ普及推進協議会」において、SECURITY ACTION制度の普及促進及び二つ星の次の取組の方向性を協議した。

【評価】

サイバーセキュリティ対策指針の策定に関しては、「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の周知・普及をはじめとして、着実に取組を進めた。

また、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に関しても、SIPにおける研究開発や、産業サイバーセキュリティ研究会におけるタスクフォースの立ち上げなど、着実に取組を進めた。

中小企業の取組の促進については、対策集の取りまとめや仕組みの検討を進めており引き続き、中小企業における取組の一層の強化に向けて、既存の制度の周知強化も含め、関係省庁が連携して各種取組を推進していくことが重要である。

【今年度の取組】

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に関しては、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。そのほか、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。また、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、引き続き、第２層タスクフォースにおいて、IoT機器等に求められるセキュリティ要求等の検討に資するフレームワーク等に関する検討を進める。さらに、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た取組を進める。

中小企業の取組の促進に関しては、引き続き、「小さな中小企業とNPOの情報セキュリティハンドブック」や「中小企業の情報セキュリティ対策ガイドライン」の周知を行う。また、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。さらに、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行い、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する。加えて、「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を実施しつつ、「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。

1.3　安全なIoTシステムの構築

【昨年度の取組実績】

サイバー空間につながる様々なモノが急速に広がっており、経済社会の発展に不可欠なインフラとしてのサイバー空間に悪影響を及ぼし得る脆弱なモノ（機器）のサイバーセキュリティ対策が喫緊の課題となっている。こうした状況を踏まえ、安全なIoTシステムの構築に向けて以下の取組等を実施した。

IoTシステムにおけるサイバーセキュリティの体系の整備に関しては、「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」（2019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。

国際標準化に関しては、安全なIoTシステムの構築に向けて、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC 1/SC 27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえた国際標準化の推進等を実施した。

また、ネットワーク上の脆弱なIoT機器の対策については、総務省において、国立研究開発法人情報通信研究機構（以下「NICT」という。）がパスワード設定等に不備がありサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、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」を実施するとともに、NICTのサイバー攻撃観測網（NICTER）によりマルウェアに感染していることが検知された機器の利用者への注意喚起を行う取組を実施した。経済産業省においては、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機器等で構成されるサイバー空間とフィジカル空間のつながりにおける信頼性の確保等について議論する第２層タスクフォースを立ち上げ、検討を行った。内閣官房においては、NOTICE施策等、IoTセキュリティに関する取組状況の把握、意見交換を行い、警察庁においては、サイバー犯罪対策について講演を行った。

ライフサイクルを見通したIoT機器のサイバーセキュリティ対策について、官民が連携して、それぞれのIoT機器について、その特性や利用方法等を踏まえつつ必要なサイバーセキュリティの要件を整理し、その要件を満たすIoT機器の利用を推奨するための施策を実施した。総務省においては、電気通信事業法の枠組みにおいて端末設備等規則を改正し、強制規格としての技術基準が策定され、2020年４月１日から施行した。また、この施行に先立ち、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１版）」を2019年４月22日に公表した。経済産業省においては、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進め、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策定作業を進めた。

【評価】

IoTシステムにおけるセキュリティの体系の整備については、「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」（2019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が盛り込まれるなど、継続的な取組が進められている。また、国際会合等における、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に向けた取組も着実に進められている。

ネットワーク上の脆弱なIoT機器の対策については、「参加・連携・協働」の観点で各々が平時から講じる基本的な取組を促進する側面もある一方で、攻撃を受ける蓋然性のあるIoT機器を事前に調査して注意喚起するという点で積極的サイバー防御の取組とも言える。その取組である「NOTICE」は、2019年度は延べ2,249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が、注意喚起対象について、電気通信事業者を通じて利用者に通知しても、なお改善が見られないような利用者もいることから、より有効な注意喚起手法が課題となっている。

【今年度の取組】

IoTシステムにおけるセキュリティの体系の整備については、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。また、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。さらに、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。国際標準化については、専門機関と連携して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しつつ、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。加えて、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。

脆弱性対策に係る体制の整備については、ネットワーク上の脆弱なIoT機器の対策についての現状の課題をふまえ、引き続き、産官学民及び民間企業相互間の連携と役割分担の下でネットワーク上の脆弱なIoT機器の対策を進めていく必要がある。具体的には、総務省における「NOTICE」の取組について、2019年度は注意喚起状況について電気通信事業者間での情報共有を行うなどにより注意喚起手法の改善を図っており、引き続き電気通信事業者と連携した対応を実施する。また、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ており、その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は、引き続き、第２層タスクフォースにおいて、IoT機器等に求められるセキュリティ要求等の検討に資するフレームワーク等に関する検討を進めるとともに、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を推進するため、ガイドラインの策定及びガイドラインを活用した対策について引き続き検討する。また、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も開始する。

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

【昨年度の取組実績】

サイバー犯罪・サイバー攻撃の複雑・巧妙化を背景に、積極的サイバー防御を推進した。具体的な実施内容としては、経済産業省において、IPAを通じて脆弱性対策情報の発信や、ウェブサイトの攻撃兆候検知ツールを引き続き提供し利用拡大を図った。また、IPA及びJPCERT/CCを通じ、脆弱性関連情報の届出について受付及び脆弱性対策情報の公表をすることで脆弱性関連情報を共有する取組を着実に運用した。フィッシング攻撃についても、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るとともに、フィッシングサイトの閉鎖の調整を行った。総務省において、ICT-ISACが中心となって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し、被害を未然に防止する取組を継続して促進した。

こうした取組に加え、先端技術の普及を見込んだ研究開発や対策が求められている。自動運転については、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、ドローンについては、関係府省庁及び関係業界等による「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、「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」を決定した。また、金融庁において、日本暗号資産取引業協会が暗号資産交換業者のサイバーセキュリティ強化を目的とした自己点検チェックリストを策定する際に支援するとともに、暗号資産の不正流出事案が発生した際には、再発防止を目的に同協会と情報共有を行った。加えて、金融庁における立ち入り検査の実施等を通じて、暗号資産交換業者のサイバーセキュリティ対策の実施状況等をモニタリングするなど、暗号資産交換業者のサイバーセキュリティ強化に向けた取組を行った。

また、安心・安全なサイバー空間の利用環境の構築に必要な各種セキュリティに係るガイドライン等を金融分野、電気通信分野、医療分野をはじめとした各分野で作成・改定するなどの取組を実施した。

サイバー犯罪への対策については、国民一人一人の自主的な対策を促進する目的で、インターネット利用者等の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のため、各種ウェブサイトや講演会を始めとする様々な媒体・機会を活用し、対象者に応じた内容での広報啓発活動が行われた。

例えば、警察庁において、SNSに起因する事犯の児童の被害防止を図るためのリーフレットを作成し、都道府県警察を通じて配布したほか、都道府県警察において、教育機関関係者、地方公共団体職員、インターネットの利用者等を対象としたサイバーセキュリティに係る講演を実施した。

また、不正アクセス防止対策、フィッシング対策、企業情報の漏えいを狙ったサイバー攻撃対策、インターネット上における児童ポルノ流通防止対策、偽サイト対策等について、対策に資する情報の共有を始めとする官民が連携した取組を実施した。

例えば、警察庁及び都道府県警察において、サイバー防犯ボランティア の活動を支援すべく、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警察庁ウェブサイトで紹介し、研修会を開催するなどして、団体の拡大と取組の活性化を図っている。

さらに、サイバー犯罪等に係る専門的・技術的な研修等を実施し、サイバー犯罪対策・対処等に従事する職員の能力向上を図った。

例えば、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サイバーレンジ（人材育成基盤装置）を活用した実践的な研修を実施している。

【評価】

安心・安全なサイバー空間の利用環境たる情報システム等は、人間が作るものであるが故に、意図しない脆弱性が残り、その脆弱性を完全に除去することが難しく、またその脆弱性を突いた攻撃が行われる。そのため、脆弱性情報や修正プログラム、フィッシングサイト情報等の公表や共有だけでなく、攻撃兆候検知ツールの機能改善の検討や利用拡大を図る等の地道な対策が引き続き求められる。

自動運転については、自動走行の開発の核となる自動車工学とサイバーセキュリティを含むソフトウェアエンジニアリングの両方を担える人材育成等へ評価環境（テストベッド）を活用するなど進捗しているため、今後は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っていく必要がある。暗号資産においては、自主規制団体と連携を図りながら、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、事業者のサイバーセキュリティ強化を図っていく必要がある。

また、積極的サイバー防御を行っていくためには、技術的なサイバーセキュリティ対策だけでなく、各事業者等への周知とその浸透と、関係団体との連携を図っていく必要がある。そのためにも、業界問わず、策定したセキュリティ評価ガイドラインを継続的に更新する等の運用体制が求められる。

サイバー犯罪への対策については、様々な広報啓発活動や官民連携による対策が行われ、国民・社会を守るための取組が広がっている。

具体的には、警察庁及び都道府県警察が支援するサイバー防犯ボランティアについては、2019年末時点において、274団体（前年比＋30団体）、9,625名（前年比＋603名）が活動しており、大学生等若い世代を中心として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を行っている。団体数及び構成員が順調に増えていることから、インターネット上の違法情報・有害情報の流通・閲覧防止の効果が増すことが期待され、ひいてはサイバー犯罪対策としても有用な取組であると評価できる。

また、警察大学校サイバーセキュリティ対策研究・研修センターにおいて実施した実践的な研修の実施等により、サイバー犯罪の捜査員に対して、より高度な技術的知見を習得させることができ、また幹部職員に対しては、適切な捜査方針を立てる上で必要となる知見を習得させることができた。これらにより全国警察におけるサイバー空間の脅威への対処能力が向上し、サイバー犯罪対策として有用な取組であると評価できる。

【今年度の取組】

先行的防御を可能にするための脅威情報の共有・活用の促進、攻撃者の情報を集めるための攻撃誘引技術の活用、ボットネット対策等、サイバー犯罪・サイバー攻撃による被害を未然に防止できるような取組を継続的に推進していく中で、ウェブサイトの攻撃兆候検出ツールについては、企業のウェブサイト運営者等への提供に加え、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ことで利用拡大を図る。また、重要インフラについては、各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していくとともに、情報セキュリティを更に高めるため、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ていく。

また、安全・安心なサイバー空間の利用環境がサイバー攻撃を受けて不正操作された場合には人命に影響を及ぼす事態が生じないような対策として、自動運転については、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ていく。ドローンについても、「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していく。

サイバー犯罪への対策については、様々な取組が広がっている一方で、サイバー犯罪の検挙件数は、2019年中も高い水準にあるほか、2019年における不正送金事犯の急増やSNSに起因する事犯による被害児童数の増加等情勢の変化に適切に対応すべく、引き続き効果的な広報啓発や官民連携による対策を推進していく。

また、サイバー犯罪の手口やサイバー犯罪に使われる技術について、新たなものが次々と登場していることを踏まえ、サイバー犯罪対策等に従事する職員の能力向上等に継続的に取り組んでいく。

2.2　官民一体となった重要インフラの防護

【昨年度の取組実績】

国民生活・社会経済活動は、様々な社会インフラによって支えられており、その中でも特にその機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして、官民が一丸となり防護していく必要がある。重要インフラ防護に当たっては、官民の共通の行動計画として、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（2017 年４月 18 日サイバーセキュリティ戦略本部決定　2018 年７月 25 日、2020 年１月 30 日サイバーセキュリティ戦略本部最終改定。以下「第４次行動計画」という。）を策定し、これに従って必要な施策を実施している。

「安全基準等の整備及び浸透」については、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、重要インフラの各分野の安全基準等で規定されることが望まれる項目を整理し、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（2018 年４月４日サイバーセキュリティ戦略本部決定　2019 年５月 23 日サイバーセキュリティ戦略本部改定。以下「指針」という。）として策定・公表している。2019 年５月には同指針を改定し、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施することにより適切な設備の設置及び管理を行う仕組みを構築することや、システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うことを対策項目として追加した。また、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実施し、安全基準等の浸透状況等を確認した。そのほか、制度的枠組みについても整理し、各分野に応じた取組を進めていくことを確認した。

「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、「「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。）を策定した。

「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。2019 年度は、東京 2020 大会を見据え、東京 2020 大会期間中のシナリオに基づき、通常とは違う連絡体制及び連絡頻度における NISC をはじめとした政府内連携の確認や試行中であった「情報共有の手引書」による情報提供の手順や情報連絡様式の周知徹底、迅速かつ的確な情報伝達の確認を行った。東京 2020 大会に向けた大規模な演習としての注目度もあり、参加者数は過去最大の 4,967 名に増加している。また、事後の意見交換会も実施し、

分野間での情報共有を促進した。これらの取組を通じて、重要インフラサービス障害対応体制の総合的な強化が図られている。

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

「リスクマネジメント及び対処態勢の整備」については、東京2020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Web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、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の改定を行った。さらに、東京2020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大会に向けG20、ラグビーワールドカップ2019での運用を実施したほか、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。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、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、国土交通省において、(一社) 交通ISACの設立に向けた取組への支援を行ったり、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」を立ち上げたりするなど、協力関係拡大や充実を図る動きが進んでいる。

また、経済産業省による電力分野における「電力サイバーセキュリティ対策会議」の開催等によって、経営層を交えたサイバーセキュリティの取組の推進が行われたほか、総務省による集合研修・eラーニング研修や実践的サイバー防御演習（CYDER）実施等の人材育成の取組等についても着実に推進されている。加えて、総務省は、(一社) 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。

【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、東京2020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、サイバーセキュリティを取り巻く情勢を踏まえて指針の改定を行った。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。また、制度的枠組みを含めて、望ましい安全基準等の在り方について検討していく必要がある。

「情報共有体制の強化」については、情報共有の取組をさらに促進し、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改善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、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、東京2020大会の関連事業者等が実施したリスクアセスメントの取組について検証し、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、取組を継続して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、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て広報が行われており、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、東京2020大会後予定されている「重要インフラの情報セキュリティ対策に係る第４次行動計画」（2017年４月18日サイバーセキュリティ戦略本部決定。2020年１月30日最終改定）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、情報共有を容易にする環境整備（連絡形態の多様化、情報共有システムの整備・高度化）や共有情報の理解浸透（共有範囲の明確化）等、「情報共有の手引書」を活用しつつ、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、自職場参加の推奨等により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、2019年度に行った「情報共有の手引書」を活用した官民の情報共有訓練の強化と、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の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、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とともに、リスクアセスメントの取組を継続的かつ有効に機能させるべくモニタリング及びレビューの強化を推進していく。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、Web サイト、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、随時施策に反映させていく。

2.3　政府機関等におけるセキュリティ強化・充実

【昨年度の取組実績】

政府機関等[28]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、複雑・巧妙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。

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。）を策定しており、各政府機関等は、統一基準群を踏まえ統一基準と同等以上の情報セキュリティ対策が可能となるよう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。

2018年度に統一基準群を改定したことから、政府機関等がセキュリティポリシーの改定を速やかに行えるように必要な支援等を実施した。また、デジタル・ガバメント実行計画（2019年12月20日改定（閣議決定））を踏まえ今後クラウド・バイ・デフォルトの原則に則った政府情報システムの整備が一層進展すると見込まれること等を受け、クラウドサービス利用時における政府機関等が行うべき情報セキュリティ対策等について次期統一基準群改定に向けた検討を進めた。当該基準に基づいた監査や、不正な通信の監視等の取組等を通じても、政府機関等全体としての対策の水準の向上が推進されてきている。

第２に、当該基準に基づいた監査として、政府機関等への監査を実施（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

[28] 本章では、府省庁、独立行政法人及び基本法に基づく指定法人を総称して「政府機関等」という。

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、インシデント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。

第４に、政府機関のクラウドサービスの利用推進に当たっては、内閣官房においてクラウドサービスの利用状況の把握に努めるとともに、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、2020年度中のサービス提供開始を目指し、クラウドサービスを活用した新たな政府専用クラウドの整備を進めている。また、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促進のため、経済産業省及び総務省において制度の実現可能性に関する実証結果も踏まえた取りまとめを行ったほか、サイバーセキュリティ戦略本部において「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の基本的枠組み」（2020年１月30日　サイバーセキュリティ戦略本部決定）（以下「基本的枠組み」という。）の決定を行った。

第５に、政府機関等に対するサイバー攻撃の発生に備え、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、各政府機関等の事案対処能力や情報セキュリティに係る知識を向上させる取組を行った。2019年度には、CYMATが支援対象機関に対して具体的な支援及び助言を行う機会はなかった。そのほか、政府関係機関のサイバー攻撃対処能力の向上を目的として、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。

第６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ものを調達する際には、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。取組開始以来、2020年３月までにおいて、NISCから各府省庁に向け、1,952件の助言を行い、その内83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ものとして交換やリスク軽減策を提案した。

第７に、災害・事故等の非常時でも、政府機関等の果たすべき重要な役割（業務継続計画における非常時優先業務の実施・継続）が情報システムの停止を原因として遂行できなくなることを避けるために、情報システム運用継続計画のガイドラインを定め、政府機関等に対して必要な計画を事前に策定し、継続的に維持・改善を行い、危機的事象発生時に計画を適切に実施することを求めている。今回、新型コロナウイルス感染症等の影響によりテレワークの必要性が高まった際にも、政府機関等の情報システムの運用継続に必要なITリソースとそのセキュリティの確保がされるよう、情報システム運用継続計画のガイドラインの改定を行うこととした。

【評価】

政府機関等のセキュリティポリシー改定を支援等することにより、情報セキュリティ水準の維持・向上が図られるとともに、次期統一基準群改定に向けて、必要な知見が得られた。

NISCが行った監査及び侵入検査においては、各機関が今後の対策を強化する上での必要な助言等を行い、各機関が助言等に応じて必要な改善を実施することにより、更なる対策の底上げが図られた。あわせて、 GSOCによる政府横断的な監視により、政府機関等におけるインシデントの未然防止が図られた。

また、基本的枠組みが決定されたことで、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促進に関し、一定の方向性が示された。基本的枠組みに基づく「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、2.3において「本制度」という。）を活用することにより、これまでは各政府機関が個別にクラウド事業者のセキュリティ対策を確認し調達を行っていたところ、統一的なセキュリティ要求基準による効率的な調達が可能となるほか、実効性のあるセキュリティ評価制度により政府機関のセキュリティレベルの強化が図られる。

さらに、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。

加えて、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、より実効性のある対策を行う体制が整えられた。

【今年度の取組】

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、今後の情報セキュリティ対策を強化するために必要な助言等の取組を行い、自律的なセキュリティ水準の向上を促す仕組みを確立する。また、監査及び侵入検査（ペネトレーションテスト）で得られた知見を、統一基準群の改定作業等を含めた政府全体のセキュリティ水準向上に資する取組に反映する。

また、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り、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していく。

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促進については、基本的枠組みを踏まえ、2020年度内に、全政府機関が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本制度の立ち上げを行い、統一的なセキュリティ要求基準の明確化による調達の効率化を目指す。本制度立ち上げに向けては、セキュリティ要求基準等の策定を進めるとともに、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議等において、政府全体のコンセンサスを得つつ、作業を進める。また、本制度の定着状況も踏まえ、独立行政法人や指定法人も将来的に対象としていく。加えて重要産業分野をはじめとする民間分野に対しても、本制度の周知を進める。

各政府機関等の事案対処能力や情報セキュリティに係る知識を向上させる研修・訓練を行うことにより、CYMAT、CSIRT要員等について、知見の向上やインシデントへの対応能力向上などが図られていることから、サイバーセキュリティに係る脅威・事案情報を踏まえつつ、今後も引き続き、取組を推進していく。

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、2020年６月には、「申合せ」を改正し、独立行政法人及び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ところであり、引き続きサプライチェーン・リスク対策を推進していく。

引き続き、政府機関等における情報セキュリティ水準の維持・向上が図られるよう、継続的に取組を推進していく。

2.4　大学等における安全・安心な教育・研究環境の確保

【昨年度の取組実績】

大学等は、多様な構成員によって構成され、多岐にわたるIT資産、多様なシステムの利用実態を有する。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複雑・巧妙化が生じており、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、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着実かつ継続的に行うとともに、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。

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。

文部科学省では、大学等におけるサイバーセキュリティ対策の強化について検討し、その徹底を図るために、2018年４月にワーキンググループを設置し、2019年５月に大学等が取り組むべき事項について取りまとめ、全国の大学等に通知を発出し、サイバーセキュリティ対策等の強化を依頼した。

また、大学等の最高情報セキュリティ責任者、戦略マネジメント層、CSIRT構成員、情報セキュリティ監査担当者等に対して、統一基準群やポリシー等のマネジメントに関わる知識、サイバー攻撃にかかる攻撃手法と防御方法、情報セキュリティインシデントへの対応等の、大学等におけるリスクマネジメントや事案対応に資する各層別研修及び実践的な訓練・演習をのべ約800名に対し実施した。大学等の自律的な取組を促進するために、大学等の保有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）を10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。）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実施するとともに、最高情報セキュリティ責任者、CSIRT構成員を対象としたインシデントマネジメント研修等を実施した。また、実環境から収集したサイバー攻撃情報にランダム化処理等を施したベンチマークデータを生成するシステムを開発し、サイバー攻撃に関わるデータ解析技術の開発に向けた取組を進めた。

【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」において、大学等の多様性を踏まえたサイバーセキュリティ対策の推進に資するガイドライン等の策定に向けた検討を行い、大学等に対し通知を行うことにより、大学等のサイバーセキュリティ対策等の強化を図った。

また、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演習を行うとともに、大学等の情報システムに対する脆弱性診断を実施し、大学等における自律的かつ組織的な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】

「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」において、ガイドライン等作成に向け、引き続き検討を行う必要がある。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内容の充実を図り、大学等の情報システムに対する脆弱性診断の対象を２法人追加し、12法人とする。

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。

2.5　東京2020大会とその後を見据えた取組

【昨年度の取組実績】

引き続き、サイバーセキュリティ基本法に基づく戦略に基づき、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、対処態勢の整備とともに未来につながる成果の継承のための取組を推進した。

リスクマネジメントの促進については、重要サービス事業者等を対象とする第５回目のリスクアセスメントの実施を依頼、提出された実施結果について横断的に分析し各事業者等にフィードバックを実施した。

また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況をNISCが検証する横断的リスク評価の第２、３回目を実施した。第２、３回目の取組においては、重要サービス事業者等（競技会場（レガシー部分[29]）を含む。）を対象に検証（実地又は書面）した。なお、競技会場のオーバーレイ部分[30]の対策の整備状況及び監督状況については、大会組織委員会を対象に検証を行った。

対処態勢の整備については、サイバーセキュリティ対処調整センターを2019年４月に設置し、恒常的に情報共有システムを使用した関係組織・機関への迅速な情報提供を実施したほか、大会までの大規模イベントである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2019等においては、ラグビーワールドカップ2019組織委員会、会合の現地事務局等に

[29] 既設の設備及び新規に導入される設備のうち大会後も使用される設備
[30] 新規に導入される設備のうち大会後に撤去される設備

連絡要員を派遣し、大会の対処態勢と同等の態勢で運用するとともに、情報共有及びインシデント発生時の対処に係る訓練・演習を実施して多くの運用経験と教訓を得た。また、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。

これらの運用経験と教訓をもとに、情報共有・事案発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して、対応手順等について改善を実施した。また、５社との間で締結した基本合意書に基づき提供されたサイバー脅威情報について、重要サービス事業者等を含む関係する組織に共有を開始した。

未来につながる成果の継承については、東京2020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、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開始できるように準備を行っている。

また、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ほか、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。

さらに、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」を実施し、2019年度は延べ193人が受講した。

【評価】

リスクマネジメントの促進については、計画どおりに進捗しているものの、完璧な対策は不可能であることから、今後は、この施策を大会まで繰り返し実施して、引き続きリスクの低減と新たなリスクへの対応を促していくとともに、残存リスクが顕在化した場合の対処体制の強化を促進していく必要がある。

対処態勢の整備についても、計画どおり進捗しており、基本的な運用体制は確立されたところであるが、いかなる状況においても迅速的確な対応を行うためには、大会まで引き続き訓練演習を繰り返して対処態勢の完成度を上げていく必要がある。

また、2019年度には様々な事案が発生又は明らかになったことなどから、これらを踏まえた上で対処態勢の整備・運用に関する取組を見直す必要がある。

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、正に仕組みを整備し、運用経験を積み重ねている過程にあるもののこれまでに構築した仕組みとその運用経験等において明らかになった課題については、大会終了を待つことなくレガシー化するための準備を進めて行く必要がある。

【今年度の取組】

引き続き、戦略に基づき東京2020大会に向けた態勢の整備及び未来につながる成果の継承のための取組を推進する。

具体的には、内閣官房等において、2019年度に発生又は明らかになった事案等を踏まえた上で、リスクマネジメントの促進と対処態勢の整備・運用を推進することとし、「リスクマネジメントの促進」については、引き続き、重要サービス事業者等のリスクアセスメントにおいて、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ほか、残存リスクが顕在化した場合の対応体制の強化を促進するとともに、「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。

また、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。

さらに、「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。

未来につながる成果の継承については、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。

2.6　従来の枠を超えた情報共有・連携体制の構築

【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の一部を改正する法律第17条に基づき、2019年４月１日に、国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うためのサイバーセキュリティ協議会が組織された。

本協議会では、これまでサイバーセキュリティ分野における既存の様々な情報共有体制において活動の活性化を妨げていた要因を洗い出し、これを法律改正等によって改善を図ることにより、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・連携体制を構築していくことを目標としている。

今回の法改正では、協議会の構成員が相互に安心して情報共有を行うために必要不可欠な遵守事項（守秘義務及び情報提供義務）等が法定化された。また、協議会の組織及び運営に関し必要な事項は、協議会において定めることとされている（基本法第17条第６項）ところ、多様な主体がそれぞれ安心して協議会に加入し、情報共有活動に参加することができるよう、きめ細やかな運用ルール（規約等）の整備を図った。

サイバー攻撃の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、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していくことが重要であり、多様な主体を確保していくことが必要である。そのため、本協議会では、2019年４月、９月と第１期及び第２期の協議会構成員の募集を行い、官民又は業界を超えた、全155者の多様な主体が参加しており、2020年３月に第３期構成員の募集を行ったところである。

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し共有し、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等に主眼があり、真に有益で、他では得られない情報にしぼりこんで共有を行っている。具体的には、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、2020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46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13件と、協議会の特性を活かした迅速な情報共有が実施された。

【評価】

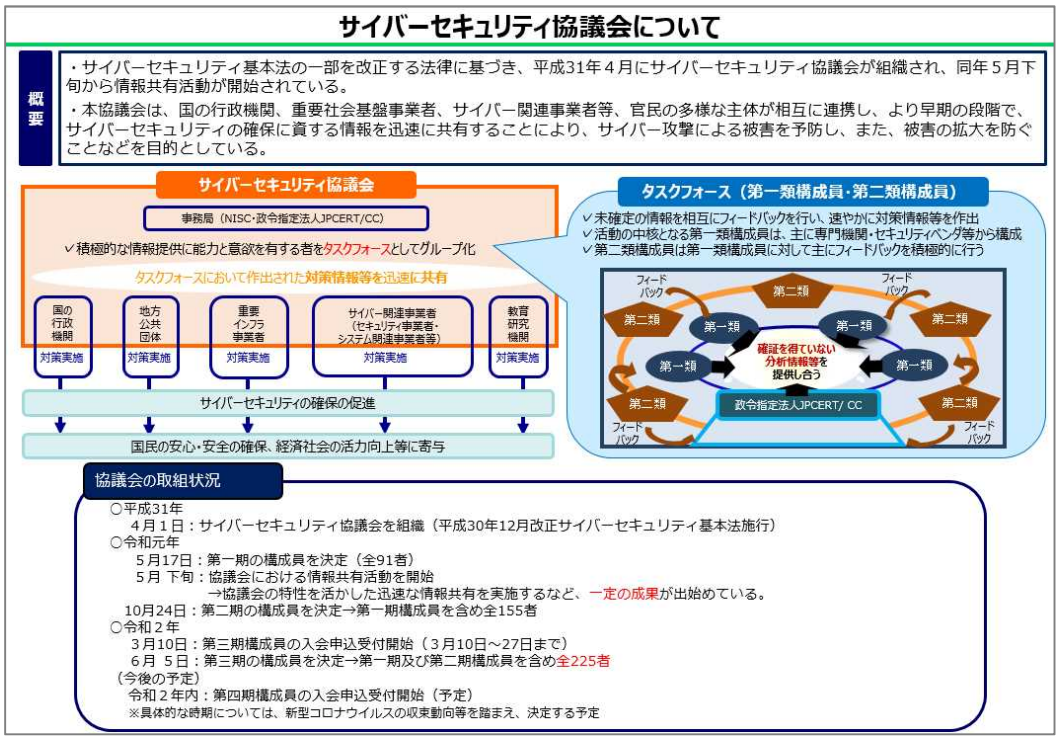
本協議会は、これまでの実際の運用の経験や各主体の意見を丁寧に踏まえ、サイバーセキュリティ協議会規約等の運用ルールの見直しを行ってきた。また、2019年度中に協議会構成員の募集を３回行い、協議会構成員は漸次拡大しており、計画どおりの進捗が図られた。さらに、これまで各組織に散らばって存在し、協議会がなければ早期に共有されることがなかったであろう機微な情報が、上記のとおり、徐々に組織の壁を越えて共有され始めるなど、一定の成果が得られたところである。

【今年度の取組】

これまでの実績及び評価を踏まえ、今後の協議会の基本的な方針として、これまでの協議会の運用を充実・強化させていく。具体的には、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、協議会の取組や参加に関するメリット等がより伝わるよう広報し、協議会への参加を広く呼び掛けるなど、より多くの主体が協議会に参加する重厚な体制を構築することを目指していく。この点、2020年６月に第３期構成員が決定され、第１期及び第２期構成員を含め全225者の多様な主体が協議会に参加しており、2020年内に第４期構成員の募集を行う予定（具体的な時期については、新型コロナウイルスの収束動向等を踏まえ決定する予定）である。

また、真に有益で、他では得られない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かつ確実に共有される重厚な体制を構築することを目指していく。

図表２－２－１　サイバーセキュリティ協議会の概要について



2.7　大規模サイバー攻撃事態等への対処態勢の強化

【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、2018年度に関係省庁及び重要インフラ事業者等と共に実施した大規模サイバー攻撃事態等対処訓練の結果を踏まえて、政府の初動対処態勢の見直しや環境整備を行った。

また、警察庁においては、大規模産業型制御システム模擬装置を用いて、産業制御システムを対象としたサイバー攻撃に係る調査・検証及び関係機関と連携した制御システムに係る共同研究を行い、これらの結果をもとに対処担当の警察職員に対する訓練を実施するとともに都道府県警察においては、重要インフラ事業者等との共同対処訓練を実施するなど、現場レベルでの対処能力の向上を図った。

さらに、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対処態勢の強化を図った。

【評価】

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進んでいる。

具体的には、内閣官房において、大規模サイバー攻撃事態対処訓練の結果を踏まえて、政府の初動対処体制の見直しや環境整備が行われたことで、事態発生時の対応がより的確・迅速に行えるようになった。

また、警察庁においては、訓練を通じて産業制御システムを対象としたサイバー攻撃の対処を担当する警察職員の能力を向上させたほか、関係機関と共同研究を行うことにより、社会全体におけるサイバー攻撃への対処能力の向上につながるものとして評価できる。

さらに、経済産業省においては、JPCERT/CCを通じ被害の発生及び拡大抑止のための関係者間調整を14,586件(2020年３月末現在)行ったほか、重要インフラ事業者に対する情報セキュリティ上の脅威及びその対策についての早期警戒情報の発行を40件（2020年３月末現在）行った。これら情報共有の取組は社会全体におけるサイバー攻撃への対処態勢の強化につながったものであると評価できる。

【今年度の取組】

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がなされている。

他方、海外で発生したサイバー攻撃による大規模事案を鑑みれば、大規模サイバー攻撃事態等発生時の影響は大きく、その備えが十分であると予断してはならない。

IoT機器の増加等、社会情勢の変化も踏まえると、サイバー攻撃による被害は、実空間へも大きく波及し、国民生活に多大な影響を与えかねない。そのため、様々な分野のサービスが同時多発的に被害を受けることを想定するなど、被害が大規模になることを想定し、実空間における混乱への対処も踏まえた訓練を実施し、更なる対処態勢の強化に取り組む必要がある。

3　国際社会の平和・安定及び我が国の安全保障への寄与

3.1　自由、公正かつ安全なサイバー空間の堅持

【昨年度の取組実績】

G20大阪サミット等における首脳・閣僚級の共同声明や意見交換を通じて、サイバー面での協力を強化していくことを確認した。G20大阪首脳宣言においては、「デジタル経済におけるセキュリティを促進すること及びセキュリティギャップと脆弱性に対処することの重要性が高まっていることを認識する」旨確認された。また、13か国・地域との間で実施している二国間サイバー協議や多国間会合、その他の多国間会議を通じ、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等に対しては、有志国、民間団体等とも連携しつつ、パブリックコメントの提出、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、我が国は今期サイバーセキュリティに関する国連政府専門家会合に専門家委員を参画させているほか、国連オープン・エンド作業部会にもその組織会合から参加しており、国連におけるサイバーセキュリティに関する議論に積極的に貢献するとともに、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、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各国との連携を強化しており、二国間の刑事共助条約・協定の下での共助の迅速化や、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。また、G7ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合（2019年10月）やASEAN+3サイバー犯罪会議（2019年７月）への参加等を通して、外国捜査機関職員との情報交換を積極的に推進するとともに、協力関係の醸成に努めた。

【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か国・地域との間で実施している二国間サイバー協議や多国間会合、その他の多国間会議等の場を活用して、継続的に関係国と連携しつつ、今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国連オープン・エンド作業部会への関与等を通じて、サイバー空間における国際的なルール及び規範について、更なる議論の深化を図るとともに、既に合意された規範について国際社会が実施するよう促していく必要がある。また、サイバー空間の自律的・持続的な発展を阻害するような動きに対し、引き続き学術界・民間の取組と政府の努力を有機的に結合させ、我が国の考え方を発信することによって、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超えるものであり、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。日本政府において、各二国間協議や国連専門家会合等の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、それらに我が国の意向を反映させるとともに、国内外での国際法・規範の普及に取り組んでいく。2020年度には、国連政府専門家会合における議論が報告書の作成に向けて加速し、また国連オープン・エンド作業部会による報告書の提出も予定されていることから、規範の形成・普遍化についての議論を深化させ、責任ある国家の行動規範及び国家実行を積み重ねていくことで、規範に反する行動を抑止する。

加えて、新型コロナウイルス感染症に関連したサイバー攻撃の発生も念頭に、規範の形成・普遍化についての議論を深化させ、責任ある国家の行動規範及び国家実行を積み重ねていくことで、規範に反する行動を抑止する。例えば、2020年５月に開催された国連安保理アリア・フォーミュラ会合（サイバー空間の安定化、紛争予防、能力構築）では、新型コロナウイルス感染症に関連した医療セクターに対するサイバー攻撃への懸念を表明し、同６月に開催された国連オープン・エンド作業部会非公式会合においては、豪州、チェコ、エストニア、カザフスタン及び米国と共に、医療サービス及び医療機関への攻撃についての共同提案を行っている。

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ための取組を行った。また、防衛省において、各自衛隊の防護システムの機能拡充、訓練、研究等の取組を行い、自らのネットワーク・インフラの防護の強化に努めた。また、防衛省の「保護すべき情報」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、米国の新たな基準と同程度まで強化するべく検討を推進する等、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、こうしたテロ組織の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てきた。

サイバー攻撃に対する抑止力の向上に関しては、実効的な抑止のための対応として、中国を拠点とするAPT10といわれるグループによるサイバー攻撃に関し、事前に米英等の有志国と緊密に連携しつつ、我が国としても米英等による非難声明を支持する形で2018年12月に外務報道官談話を発出した。また、2018年12月に策定された新たな防衛計画の大綱において、「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」が明記されたことから、当該能力を含めた防衛省・自衛隊のサイバー防衛能力の抜本的強化を図るため、実践的サイバー演習環境を整備する等の取組を進めている。また、信頼醸成措置については、特にARFの枠組みを通じ、サイバーセキュリティに関する会期間会合を設立し、2020年１月には第５回目となる専門家会合を開催したところであり、地域・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について議論を行った。

サイバー空間の状況把握の強化に関しては、関係機関の能力向上については、各対処機関は、高度なサイバー攻撃からの防護、脅威認識等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の動向等の情報収集・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・状況把握力の強化のための取組を強化することが求められる。

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、関連する主体間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、有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が求められ、更なる海外関係機関との脅威情報連携も必須である。

【今年度の取組】

サイバー空間における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容易に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。政府機関、重要インフラ事業者、先端技術を有する企業・学術機関等への攻撃も発生しており、その中には国家の関与が疑われる事案も存在する。2019年９月には、国連安全保障理事会の北朝鮮制裁委員会の専門家パネルにより、北朝鮮が各国の金融機関に対するサイバー攻撃を通じ金銭窃取を行っていると報告されている。また、昨今では新型コロナウイルス感染症に関連し、経済犯的なサイバー詐欺事案に加え、重要インフラ等に対するサイバー攻撃も海外で認知されており、米・英・チェコ等においては、特に医療機関を狙ったサイバー攻撃に関する注意喚起が行われている。

このような状況を踏まえ、知見の共有・政策調整としては、13の国と地域の間で二国間協議を開催し、情勢認識、両国におけるサイバー政策、国際場裡における協力、能力構築支援等、二国間協力について幅広く議論を行った。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、日・ASEANにおけるサイバーセキュリティ政策の相互理解と連携を強化するとともに、共通課題の解決に向けた協力活動を拡充したほか、ISPを対象にワークショップを開催し、合同サイバー攻撃対応演習を実施した。また、Meridian会合、FIRST等の多国間会議に参加し、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きた。

平時からのサイバー脅威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、事故対応等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たほか、有志国を我が国の分野横断的演習に招へいしてワークショップを実施する等、連携体制の強化に努めた。また、ICT-ISACをはじめとする日米間でのISAC連携を進めてきた。

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）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、2019年９月、米国務省及びエネルギー省をはじめとした日米の官民の専門家と協力し、インド太平洋地域向けに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、防衛省においては、2020年１月、ベトナム人民軍要員を対象としたインシデント対応能力向上に資するサイバーセキュリティセミナーを実施した。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、JICA事業を通じてサイバーセキュリティ政策能力向上に資する研修機会を提供した。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・有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、従来からの能力構築支援に加えて、同地域のサイバーセキュリティ対策の底上げに資す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、有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、有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となる。このため、途上国に対するサイバーセキュリティ能力構築支援は、先進国の責務であり、我が国は、ASEAN加盟国を始め、世界各国を対象に積極的に能力構築支援を行うこととしている。特に日・ASEANサイバーセキュリティ政策会議は、ASEAN加盟国との中核的な役割を担っている。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に引き続き取り組む。

4　横断的施策

4.1　人材育成・確保

【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、普及啓発・人材育成専門調査会において、人材育成に関する政府の取組を整理・更新するとともに、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い施策間の連携を促進している。

サイバーセキュリティ人材育成取組方針の推進については、普及啓発・人材育成専門調査会において、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うとともに、施策間の連携を促進した。また、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、仮運用を開始した。

戦略マネジメント層の育成・定着に向けた取組としては、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、2018年度に検討したモデルカリキュラムの活用等に関する今後の取組の方向性について議論を行った。また、IPAにおいては、産業サイバーセキュリティセンターを通じた中核人材及び戦略マネジメント層等の育成において、これまでの２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にも取り組んだ。さらに、2018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等を踏まえ、「セキュリティ組織管理」コースと「セキュリティ実務管理」コースの２つのコースに分け、2020年２月に実施した。

実務者層・技術者層の育成に関しては、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。また、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。また、各種資格・試験に関しては、2019年10月時点の情報処理安全確保支援士（登録セキスペ）は19,417人となった。また、登録セキスペの更なる活用のため、IPAのホームページ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。また、登録セキスペ制度の信頼性を向上するため、第200回臨時国会において、登録の更新制導入などの法改正を行い2019年12月に公布された。

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、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）の改訂案を作成した。さらに、新学習指導要領の実施を見据え、「小・中・高等学校を通じた情報教育強化事業」において、教科等横断的な情報活用能力の育成に係るカリキュラム・マネジメントの在り方について、実践的な研究を実施し、成果を取りまとめた。教員等を対象とした情報モラル教育指導者セミナーについても実施した。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」についても、継続的に取組を進めた。さらに、「未踏IT人材発掘・育成事業」においては、セキュリティ・キャンプの講師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。

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2019年８月末行った。また、各府省庁において同計画に基づく体制の整備として機構・定員要求、適切な処遇の確保として俸給の調整額の要求を行い、それぞれ成果が見られた。ほかにも、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。

また、「サイバーセキュリティ・情報化審議官」等を対象とした研修を実施し、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て、各府省庁におけるセキュリティ対策の司令塔として必要な知識・能力の向上に努めた。さらに、一定の専門性を有する人材を育成するため、全府省庁のセキュリティ担当者を対象とした「CISSP入門講座」を実施した。

【評価】

戦略マネジメント層の育成に関しては、関係機関の取組により重要性の認識が拡大しつつあるが、DX with Cybersecurityの進展に伴って、戦略マネジメント層の役割はより一層重要になると考えられる。このため、今後、関係主体が連携しつつ、より効果的なカリキュラムの構築・実施等に取り組むことが重要である。

実務者層・技術者層の育成に関しては、各機関・事業において各種取組が着実に進んでおり、参加者や受講者数も増加している。今後も継続的に人材の育成・確保を進めていく必要がある。

人材育成基盤、若年層に係る取組に関しては、知識技術体系やモデルカリキュラムの検討が進むとともに、学校教育において、児童生徒への教育の充実や教員を対象とした取組も進められている。また、突出した能力を有する人材育成として、セキュリティ・キャンプやSECCON等の取組も実施されている。これらの取組を引き続き推進していくことが重要である。

各府省庁におけるセキュリティ人材の確保・育成の強化のため、政府機関におけるセキュリティ・IT人材の確保・育成を推進し、体制の整備、有為な人材の確保等が行われており、今後も、引き続き、セキュリティ人材の充実に資する取組を継続することが求められる。国際連携の推進に関しては、引き続き具体的取組の実施に向けて検討を行っていく必要がある。

【今年度の取組】

経営層の意識改革や戦略マネジメント層、実務者層・技術者層の育成に関して、関係府省庁と連携の下、「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、必要に応じてフォローアップや見直しを図る。

戦略マネジメント層の育成・定着については、関係府省庁や各種団体等と連携して、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普及に取り組むとともに、その育成を促す。また、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。また、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。加えて、関係府省庁や各種団体等と連携して、

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普及に取り組むとともに、その育成を促す。

実務者層・技術者層の育成については、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。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）を実施する。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、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。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。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る。

若年層の育成については、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、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を一層推進する。また、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。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。

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、引き続き、体制の整備・人材の拡充、有為な人材の確保、一定の専門性を有する人材の育成や適切な処遇の確保、橋渡し人材のスキル認定の推進を含む政府部内のセキュリティ人材の充実に係る諸施策をより一層推進する。また、内閣官房等の関係機関で連携し、「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等を踏まえ、当該方針の見直し等に向けて取り組む。

4.2　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」を2019年５月に策定するとともに、同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としては、技術検証に関する技術動向や諸外国の制度の状況についての調査を実施した。また、第５世代移動通信システム（5G）ネットワークのセキュリティを担保できる仕組みの整備や、

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開発、スマートシティのセキュリティ要件についての国内外の実例調査や議論を実施した。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」の周知・普及や各産業分野におけるセキュリティ対策の検討、制御システムの挙動からサイバー攻撃を検知・予測する技術開発や、高度な攻撃意図を伴う潜伏的な脆弱性の検知・対処を実現するための研究を行った。

国内産業の育成・発展に向けた支援策の推進としては、セキュリティ製品・サービスの有効性のトライアル検証の実施や、製品・サービス導入事例公表のための手引書の作成、「情報セキュリティサービス審査登録制度」のプロモーションを実施した。また、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実施や、IT導入補助金、財政投融資制度、コネクテッド・インダストリーズ税制等を用い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。さらに、コラボレーション・プラットフォームを通じた情報交流を行いセキュリティコミュニティの形成を促進した。

攻撃把握・分析・共有基盤の強化としては、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、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、サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）による集約データ間の突合分析を含む試験運用を行った。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の研究開発を進めるとともに、IoTマルウェアの挙動検知技術の基本方式の設計を行った。

暗号等の基礎研究の促進としては、量子ビットの高集積化技術や高品質な量子ビット等の開発や、集積回路の構造の最適化及び集積実装の技術開発、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実施、ビッグデータ統合利活用促進のためのセキュリティ基盤技術などの支援を実施した。また、柔軟なアクセス制御が可能な関数暗号などの暗号技術を提案や、CRYPTREC暗号リストに掲載された暗号技術の監視、新世代暗号に係る調査、量子コンピュータや新たな暗号技術の動向等を踏まえた次期CRYPTREC暗号リストが満たすべき条件の整理を実施した。さらに、量子暗号を用いた電子カルテデータのシステム開発や、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としては、研究開発戦略専門調査会等を通じて、国際的な研究動向や産学官連携事例について分析を行うとともに、研究コミュニティとの議論を行った。また、専門機関と連携し、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の策定・勧告に向けた取組を推進した。また、米国サンフランシスコで開催されたRSAカンファレンスにて、ジャパン・パビリオンの出展支援を実施した。さらに、WG2コンビーナ、WG3副コンビーナとして、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った。そのほか、専門家等との議論を経て、「サイバーセキュリティ関係法令Q&Aハンドブック」を取りまとめた。

【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トライアル検証の実施や、中小企業向けのセキュリティ対策支援の実証事業の実施、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、引き続き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行うとともに、研究振興策について議論を進めることが重要である。また、我が国の研究開発成果等の国際標準の策定・勧告に向けた取組推進や、国際的なイベントへの出展、国際的な機関での国際標準化について中心的役割を担う等の取組がなされており、引き続き、国際的な影響力の向上にむけた取組を行うとともに、産学官連携のコミュニティ形成に関する取組を継続していく必要がある。

これらの状況を踏まえつつ、今後も「サイバーセキュリティ研究・技術開発取組方針」に基づき、取組を推進していく。

【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の整備に向けた取組を進める。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を推進や、5Gネットワーク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。

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・サービスの有効性を検証する基盤の構築や、ビジネスマッチングの実施、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、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）を開催することで、サイバーセキュリティビジネスの振興・活性化を図る。

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、CUREによるインシデント情報等の集約・横断分析等の

高度化と定常運用等を実施する。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。

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する。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、次期CRYPTREC暗号リストが満たすべき条件の整理を進めるほか、堅牢な量子暗号通信網の実現に向けた技術を確立、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等を行う。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。

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等を通じて、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。

4.3　全員参加による協働

【昨年度の取組実績】

サイバー空間で活動する主体としての国民一人一人がサイバーセキュリティに対する意識・理解を高め、サイバー空間における様々なリスクに対処できることが不可欠になっていることを踏まえ、以下の取組等を実施した。

2019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関しては、フォローアップに向け、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収集・整理した。

若年層への普及啓発の観点では、子供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。2019年度は、2019年４月から2020年３月までの間、2,660件の出前講座を実施した。また、2020年３月に、「インターネットトラブル事例集（2020年版）」を公表した。

一般向けの普及啓発の観点では、教育関係者等が児童・生徒・学生等に指導する際に使用可能な教材７テーマ（SNSや情報セキュリティ等）22種類とともに、指導するポイントをまとめた講義要領を作成、試行版を2019年11月に公開した。また、作成した教材を使用して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ーに向けて、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。さらに、「教育関係者等向けインターネット安全教室」を47都道府県で１回以上計50回開催した。また、一般向けの情報発信に関しては、サイバーセキュリティに関する注意・警戒情報等の発信を、各種媒体を用いて引き続き実施した。「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」や「インターネットの安全・安心ハンドブック」の内容の見直しを行った。また、一般からの相談対応に関しては、情報セキュリティ安心相談窓口や標的型サイバー攻撃特別相談窓口で相談対応を引き続き行うとともに、情報収集に努め、調査や分析を行い、各種対応を行った。

サイバーセキュリティ月間に関しては、産学官民の各種啓発主体による関連行事が計156件登録された。また、「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イベントの動画配信を行った。

利用者によるサイバーセキュリティの取組実施に向けた、事業者や関係団体等による活動の促進の観点では、安全に無線LANを利用できる環境の整備に向けて、「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」の改定検討を行った。

【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を着実に進めた。同プログラムのフォローアップに取り組むとともに、情報発信活動や相談窓口対応を引き続き実施していくことが必要である。

サイバーセキュリティ月間に関しては、各地域の関連行事は新型コロナウイルス感染症の影響で開催数が減少したものの、開催予定として登録のあったイベント数は前年同程度であり、意識醸成の機運が維持されていると考えられる。また、「サイバーセキュリティ意識・行動強化プログラム」を踏まえた若年層に重点を置いたキャンペーンやイベントについては、こちらも新型コロナウイルス感染症の影響でイベントの開催が中止になったものの、実施予定であったイベントの動画を撮影し、普及啓発に資するようYouTubeにて配信した。コンテンツとのタイアップについて大きな反響が得られた。さらに、本年はInstagramやTwitterなどで多くのフォロワーを持つ、いわゆるインフルエンサーにサイバーセキュリティに関する普及啓発の投稿を依頼し、発信してもらうことで、若年層でもよりリーチしにくい層に対して普及啓発することができた。これらの結果も踏まえ、来年度に向けた検討を進めていくことが必要である。

【今年度の取組】

普及啓発プログラムにおいて、各府省庁が実施する施策の効果を整理しつつ、普及啓発全体を表す代表的な指標をモニタリングし、PDCAサイクルを着実に実施する。また、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、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。また、GIGAスクール構想における学校現場に一人一台の端末を配布するタイミングをきっかけとして、児童生徒がインターネットやセキュリティについて学ぶための資料の作成等を実施することで、若年層のセキュリティに対する理解を深める。さらに、サイバーセキュリティ月間を引き続き実施しつつ国民一人一人の理解を深め、サイバーセキュリティというものが専門家だけの努力に頼るものではなく、全員参加で成し遂げるものであるという機運を引き続き醸成する。新型コロナウイルス感染症への対応を機に、様々な場面でインターネットの利用や新たなデジタル技術の活用が増加することが想定されるため、そのような状況に応じて、サイバーセキュリティに関する普及啓発活動を適切に実施することが重要である。

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、2019年度は、約800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、国際担当者間の会合や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。

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2019の本編及び概要をまとめた冊子を制作した。

内閣官房及び関係省庁において、戦略及びこれに基づくサイバーセキュリティ2019の冊子を活用し、各種セミナーでの説明等を通じて、計23件のイベント等で、国内外の関係者2,200名超に対して、戦略等の発信を行い、周知を行った。

【評価】

推進体制については、パートナーシップに基づく取組や、戦略及びこれに基づくサイバーセキュリティ2019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。一方で、戦略で掲げたサイバーセキュリティエコシステムの実現には、あらゆる主体がセキュリティに取り組むインセンティブを生み出すことが重要である。全体として統一感を持って、考え方を浸透させていくために、戦略の基本的な考えを示しつつ、官民の個別の取組に反映しやすいように説明を行うなど、国内外の関係者との一層の連携の強化を図り、戦略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は、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、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、国内外の関係者へ戦略及びこれに基づく年次計画等の発信を行う。加えて、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ていく。

3章　現状の認識を踏まえた加速・強化すべき取組

2018年7月に戦略を閣議決定してから2年近くが経過している。次々と新たな情報通信サービスが提供され普及が進んでいく状況、新型コロナウイルス感染症対策の一環としてテレワークの活用などが積極的に進められる状況、そういった状況変化を逃さずにサイバー攻撃が発生している状況など、戦略決定後に顕著になった動向に着目し、社会の隅々にまで新しい情報通信技術を活用していく潮流が決定的となっている今回の変革期に対応していく観点から、現在の戦略の実行に当たり特に加速・強化すべき取組をまとめ、今後の次期戦略の検討につなげるものとして整理した。

1　現状から見えてきたこと

1.1　新型コロナウイルス感染症対応を踏まえたDXの推進とサイバーセキュリティ対策（DX with Cybersecurity）

新型コロナウイルス感染症の影響により、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、混乱に乗じて、ランサムウェアや不正アプリ等による攻撃が海外を中心に急増している。今後は、テレワークに限らず、患者・感染者との接触機会を減らす観点から、更なるデジタル化の推進の必要性が明らかになる中、それと一体的に、改めてITシステムや制御系システムのセキュリティ対策の徹底と強化が求められる状況となっている。

新型コロナウイルス感染症対策の観点に加え、近年取組が進められているクラウドサービスや5G、IoT・AIといった新しい技術の導入は、既存のワークフローの効率化や新しい付加価値の創造を実現するものでもある。DXの推進においては、不測の事態が生じた際のダメージも見込んで対策を講じつつ、新しい技術を余すところなく使い尽くすことが重要である。例えば、医療におけるロボットアームを用いた遠隔地からの手術など、フィジカルな機器の操作を伴う仮想現実については、作業の最中に通信が途絶しないよう対策を講じることは当然のことではあるが、仮に通信が途絶したとしても致命的な影響を及ぼさない工夫が不可欠である。現在のサイバーセキュリティ戦略やそれに基づくサイバーセキュリティ2019においては、サイバー攻撃を受けてから対応するのではなく、事前に、能動的に防御していく「積極的サイバー防御」の考え方を示しているが、この考え方は、DXの推進に際しても重要である。その前提として、分析を的確に行う能力の獲得とその運用も重要となる。情報システムに関わる全ての組織（現在の社会においては、ほぼ全ての組織）が、この考え方を実践できる環境を整えていくことが重要であり、知識やノウハウの普及啓発を進めることが重要である。また、国、地方公共団体、重要社会基盤事業者及びサイバー関連事業者その他の事業者においては、DX推進を、関係者は認識をしているのに対策が進まない、という構造的課題への効果的な対応を進めていく機会と捉えることも重要であり、それに併せて、リスクに対する認識[31]について是正を徹底し、リスクマネジメントの考え方を浸透させていくことも非常に重要な取組である。DXを用いた事業計画の立案にあわせ、潜在するリスクの分析を行い、獲得したい豊かさと受け入れる好ましくない影響のバランスを取ることが重要である。

[31] 国際標準化機構（ISO）において、リスクは「目的に対する不確かさの影響」と定義 され、「影響」には好ましいもの、好ましくないものの両方が含まれる。

1.2　クラウドサービスの利用拡大に伴う防御範囲・手法の転換

基本法においては、情報、情報システム、情報通信ネットワークを保護すべき客体としている。システムを管理する者の対策としては、これまでは、求められる信頼性に応じて情報通信ネットワークを分割し、その境界にファイアウォール等を設置してアクセスを制限することを軸として情報システムに対策を講じ、その中に保存されている情報を保護するという境界防御を基本的な考え方としてきた。

近年、柔軟なサービス展開やテレワークの推進などを実現するため、クラウドサービスを活用するケースが民間企業等で増えている。また、政府機関等においても、「政府情報システムのためのセキュリティ評価制度（ISMAP)」の利用によるクラウドサービスの調達の取組も進められているところである。

クラウドサービスの活用は、新しいサービスを簡便に提供したり多様な働き方を実現したりする一方で、不特定多数のユーザに対して提供されるクラウドサービスにおいては自組織の管理の範囲外のネットワークの利用が前提となることなどに伴い、従来重視されてきた自らのシステムやネットワークの境界を守ることによる対策だけでは、セキュリティを確保するには十分と言えず、通信データ自体の暗号化による保護などの利用実態を踏まえた対策も重要になる。今後は、クラウドサービスの採用が一段と進み、周辺システムに限らず、基幹システムなどの重要なシステムにおいても導入が進められていくことが予想され、システム・サービス防御の在り方についても、境界防御の考え方だけではなく、データのセキュリティを確保する観点に基づく複層的な対策などが重要になる。

クラウドサービスは、これまで機器内通信として行われてきた情報処理を、情報通信ネットワーク全体で役割を分担する技術でもあり、クラウドサービスを活用する際に情報を保護する対策を進めていくためには、ネットワーク技術者の視点が不可欠である。クラウドサービスは、資源の最適配分を実現する技術として、IaaS、SaaS ともに、今後、社会における役割が大きくなっていくと考えられるものであり、サイバーセキュリティの観点からも十分なリスク評価が行われ、それに基づく対策が施されながら、十分な活用が進んでいくことが期待される。

1.3　5G の商用サービス開始とそれに伴うデータ活用の高度化

5G の特徴としては、「超高速」「超低遅延」「多数同時接続」の３つが挙げられることが多い。このうち「多数同時接続」については、IoT 機器の普及を後押しするために不可欠な要素であるとともに、サイバーセキュリティの観点からは、ネットワークに接続されるノード数を爆発的に増加させる脅威と捉えることも重要である。

また、AI 技術を実装した運行管理システムにより、動体制御のトランザクションの処理能力を飛躍的に向上させることが期待されているが、5G のような通信基盤上で、アクチュエータの自動制御を実現できるようになれば、新たなデバイスやサービスの創出の開発が活発になっていくことが想定される。

結果として、工場・家庭などの場所や用途を問わず、あらゆる機械の制御系システムに対してネットワーク接続が促進される可能性が高く、他方、攻撃者の視点に立つと不正アクセスの対象とし得る接続点が増えることになることから、製造ラインや家電製品など、

幅広い場面における IoT 機器を含めたサイバーセキュリティ対策が重要になる。

こういった変化に対応するためには、機器の製造メーカー／サービス提供者やそのユーザ企業、最終消費者といった関係者を巻き込んで、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進めていくことが重要になり、我が国全体にとってのサイバーセキュリティ政策としても、より多くの主体が実践的な対策を取ることができるよう、協力体制を構築していくことが重要になる。あわせて、これまでは主に情報端末を中心に進められてきたサイバーセキュリティ対策の対象の拡大についても検討することが重要である。

また、AI・IoT 技術の発展などによって、データの活用が一層高度化することが予想される。IoT 機器の普及は、膨大な情報を提供し続けるセンサネットワークの構築が進むことを意味し、その IoT ネットワークによって提供されたデータは、AI の学習用データとして重要な資源となるものである。医療分野や交通分野といった高い付加価値を実現すると同時に、高い信頼性が求められる領域でのデータ活用も期待される中、価値の源泉でもあり、信頼性確保の礎でもあるデータをどのように守るのかといった視点がサイバーセキュリティの観点において新たに求められている。

5G の特徴として、超高速・低遅延・多数同時接続が挙げられるのは、リアルタイム性の高い分野への応用が期待されるためでもあり、これらの機能を最大限に生かすための基盤としてもクラウドサービスと一体となって活用が進められていることが想定される。

1.4　サプライチェーン・リスクの拡大と予見性の確保

製造ラインや家電製品など、幅広い場面へのネットワークの広がりを伴う新たな情報通信技術や機器を活用したデジタル化の実現に向けて、それに関係する事業者間の関係が生まれている。グローバルな規模で、これまで取引がなかった異なる業種の企業間取引が生まれるなど、発注者や受注者／子会社やその下請事業者、孫請け事業者など関係する主体のつながりが複雑になりつつある。一方で、このような形態においては、サプライチェーンのつながりの端で起こったサイバーセキュリティの問題が、実空間、さらには、経済社会全体にこれまで以上に広く波及し、甚大な悪影響を及ぼすおそれがある。

サプライチェーンとは、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であり、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、システムやサービスの設計から運用・保守・廃棄に至るライフサイクルに関わる事業活動のつながりを含めてサプライチェーンと呼ばれることがある。ITにおけるサプライチェーン・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を考慮する必要があり、システムやサービスに悪意のある機能等が組み込まれ、情報窃取・破壊・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。第一義的には、サービス提供の主体、製品開発の主体などの各主体が自身の責任で管理下のセキュリティリスクを低減する取組が重要となるが、一方で複雑化したサプライチェーンにおいて、各主体の責任範囲が不明瞭となっている実態もあると想定されることから、各主体が守るべき範囲や実施すべきセキュリティ対策について整理することも重要である。

また、昨今、委託先の従業員が情報を盗み出した事案や企業の子会社や海外拠点が攻撃

を受けそこから被害が広がった事案が発生しており、サービス提供企業が自社のガバナンスの効力が及ぶ範囲において十分な対策を施していながら、ガバナンスの効かない委託先や調達元のセキュリティ対策が不適切である場合などに、そこを攻撃者に狙われて被害が発生することも懸念される。そのため、各主体の責任範囲の明確化に加え、サプライチェーン全体の各要素におけるリスクシナリオを把握した上で、過去の事例なども踏まえながら、予見が可能なリスクについては取引先等の関係する主体に対する能動的な働きかけや自主的な予防対策を検討することも重要である。

1.5　国際的な議論の高まりと統一的な国際ルールへの期待

国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することは極めて重要である。サイバー空間における規範については、2018 年 12 月の国連総会決議に基づき設置された第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（GGE）が 2019 年 12 月から開催されている。GGE は、国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展に関して、事務総長により選出された 25 か国の政府専門家で構成され、これまでも 2010 年、2013 年及び 2015 年に規範等を提示した GGE 報告書を作成してきている。特に、2015 年の GGE 報告書で示された 11 の規範は国連総会でコンセンサス採択されており、本分野における国際的な議論の重要なベースとなっている。第６期 GGE の活動も、こうした経緯を踏まえ、①脅威認識、②責任ある国家の行動に関する規範、③信頼醸成措置、④能力構築、⑤国家による情報通信技術利用における国際法の適用について議論し、2021 年央を目処に国連事務総長に報告書を提出することが求められている。また、GGE での作業と並行して、2018 年 12 月の国連総会決議に基づき、国連全加盟国が参加できるオープンエンド作業部会（OEWG）が 2019 年９月より開催されており、本年秋の国連総会に報告書が提出される予定となっている。新型コロナウイルス感染症の世界的な流行の影響により、これら作業日程が影響を受ける可能性もあるが、我が国としては今後とも GGE と OEWG の作業が相乗効果をもたらすように議論を主導していく必要がある。特に、「責任ある国家の行動」に背馳する行為（作為・不作為）は当該国の国家責任を発生させ得るものであり、その態様に応じて被害を受けた国による自衛権の発動から国際法上許容される対抗措置の発動等、様々な帰結をもたらすことにつき、明確なコンセンサスを形成すべく主導的な役割を果たしていかなければならない。

また、サイバー犯罪に関する条約（ブダペスト条約）については、我が国は 2012 年に同条約を締結し、同条約の有効性を未締約国に対して鋭意発信してきている。他方、2019 年 12 月の国連総会においては、サイバー犯罪に関する新条約策定に向けた決議案が採択されたところ、我が国としてはブダペスト条約の一層の普遍化・強化こそが最優先課題との立場ではあるが、同様の考えに立つ関係国と連携しつつ、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関連の議論が行われるよう役割を果たしていく必要がある。

このようにサイバー空間における法の支配・法規範等を巡る国際的な議論は継続的に進行しており、我が国としてかかる議論や作業等に積極的に関与・貢献し、それらの国内外での普及啓発活動、その他の国際連携・協力に取り組んでいく。そうした国際的な努力の積み重ねにより、経済事犯等のサイバー犯罪者から、国家主体乃至その意を受けたサイバー攻撃者に至るまで、悪意のある者による活動を少しでも抑止し得るような国際社会のル

ール・慣行・環境を定着・発展させていくことが大目標である。

2　今後の検討に当たっての視点

現在の戦略では、その基本的な在り方として、「サイバーセキュリティエコシステム」を掲げた。これは、「全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ（中略）サイバー空間が進化していく姿」を、「一種の生態系」にたとえて呼称することとした概念である。前述のような現状から見えてきたことがある中、新たな技術の活用による果実を最大限に享受するためには、全体像を俯瞰した上で、異なる主体が緊密に連携して、無駄なく首尾一貫した対策を進めていくことが重要である。サイバー空間においては、技術の進展が早く、攻撃者優位とされる環境でもあることから、それぞれが自らの役割をしっかりと認識しながら、連携して取り組んでいくことが重要である。サイバーセキュリティ対策を進めていくに当たっては、従来から、自助・共助・公助の考え方が重要な観点であるが、今後の対策においても、引き続き重要なフレームワークとなっていくと考えられる。

2.1　リスクマネジメントの実施と戦略的行動

システムを保有・管理するに当たっては、まずは、事業者等自身が責任をもって対策を講じることが基本となる。システムをどのように事業に活用するかは重要な経営課題であり、一度致命的なセキュリティインシデントが発生すると、組織の内外において安全サイドへの要求が時に過大に強くなることで事業スピードの低下につながるおそれがあるとともに、改善する機会も与えられずに顧客が代替サービスに乗り換えてしまうなどの組織の危機につながるおそれもある。そのため、サイバーセキュリティは、経営層から現場まで、企画・事業部門から情報システム部門までの全体的な問題と捉え、DX を成功させる上での重要な機能として位置付けられることが重要である。

今後、クラウドサービス、5G 等の新しいデジタル技術の普及を背景に、組織を超えたつながりやサイバー空間と実空間のつながりが経済社会全体にさらに広がっていくと、１つのインシデントがこれまで以上に広い範囲に影響を与えるおそれがある。また、新たな技術の導入に当たっては、技術そのものに加え、利用方法によっても、未知の脆弱性が生ずる可能性があり、見落とされた場合には、潜在的に大きなリスクを抱えてしまうおそれがある。さらに、複雑化が進むサプライチェーンにおいて、脆弱性が生じた際の各企業の責任が曖昧になっていると、その対応に遅れが生じ、攻撃の端緒を与えることとなってしまうことも想定される。

分野や組織を超えたインシデントの連鎖被害への対処は、まずはリスクを正確に把握することが前提となるが、政府のサポートの仕組みや官民連携の活用も組み入れた形でリスクアセスメントを適切に行い、残存リスクに対しては、サイバーセキュリティにおける保険も活用するなどの事前の対策の推進が重要である。リスク分析の本質はシナリオの多様性を前提とすることにあり、対策に当たっては、クラウドサービスや IoT 機器などを利用した DX 推進等の動向にあわせたセキュリティポリシーなどの改善を行うことが重要である。また、多種多様な組織のつながりが広がっていく社会においては、各主体の責任を明確化することで対策の推進を図ることが重要であり、例えば、システム構築の発注における委託元と委託先の責任分界点を明確に整理していくことなどが重要である。この点にお

いては、委託元・委託先ともに、委託先の責任の範囲を明確にしたいと考えているものの、委託元においては「専門知識・スキル不足」といった課題が、委託先においては「契約を見直す機会の不存在」「コスト増を受け入れてもらえない」「契約時点で要求事項が不明瞭」といった課題があることを指摘した調査[32]もあり、実態を踏まえて対応を進めることが重要である。

リスクマネジメントの実施に当たっては、自組織のシステムや IoT 機器、その他の情報資産を全て洗い出し、それぞれの情報資産のセキュリティリスクと対応内容を明確化する必要があるが、最初のステップとなる情報資産の洗い出しがボトルネックとなって進まない企業も多いと想定される[33]。人材やスキル不足など、リソースにおける制約がある場合には、まずは現在のリソースで何ができるかを考え、例えば、重要度の高い領域からスモールスタートで始めるなど、最終的に目指す目標と当座の現実的な目標を分けて立てることも一つの進め方である。

国としては、自助の取組を進める上での基本的な考え方を示すなど、取組の手間を軽減するためのサポートを提供することも重要である。事業者等の対応を促していくため、これまで進めてきた基準を示すことなどによる環境整備の成果を踏まえつつ、リスクマネジメントの考え方を実践しやすくするため、典型的なケースにおける事例を共有するなど、事業者が、具体的に自組織に当てはめようとしたときのサポート体制などについても充実させることを検討していくことが重要である。

2.2　情報共有体制の積極的活用による共助の強化

戦略においては、「サイバーセキュリティエコシステムの実現」という考え方を示してきた。システムの管理においては、各保有者が責任をもって対策を講じることが基本ではあるものの、対応を共同で行うことがサイバーセキュリティ対策として有効に働くこともある。例えば、新たな攻撃手法での被害が発生した際、被害組織等から他の組織への迅速な情報共有により、攻撃手口や対策手法を他の組織が知ることができるようにすることで、同様の手口によるサイバー攻撃の被害の拡大を防ぐことが可能となり、社会全体の被害を最小限に留めるためにも、情報共有の取組を強化していくことが重要である。また、ビジネスメール詐欺などのケースでは、取引相手が管理する情報がサイバー攻撃により窃取されることが、自組織にとって脅威となるものであり、サイバーセキュリティ対策としては各組織が自らの情報システムの対策を講じるだけでは十分とは言い切れないものである。これを防ぐための取組については、特定の誰かの取組として位置付けるということではなく、例えば、取引相手のシステムに関する不審な挙動やその予兆に気づいた時には、端緒となる情報として広く提供を行うなど、自分の管理する範囲のシステムを守ることだけに捕らわれず、全ての主体が、社会全体におけるサプライチェーンを含めたサイバーセキュリティ対策の推進者であるという意識を持つことが重要である。

既に、多くの分野で ISAC の活動が展開されているが、サービスの提供において競合他社となることがあるとしても、サイバーセキュリティ対策においては、リスクを共有するパートナーであるという考え方を明確に共有した上で取組を進めている例もある。事業ごと

[32] 出典：IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査（IPA）
[33] 参考：企業の CISO 等やセキュリティ対策推進に関する実態調査（IPA）

に業法の歴史的背景や提供する製品・サービスに関するルールの違いといった事情などがあり、分野ごとの特性に十分配慮しつつ、共助の取組を深めていくことは、新たな技術の導入が進められていく中にあって、より質の高いサイバーセキュリティ対策を低コストで実現できる工夫にもなっている。また、人材の教育の観点でも、同じ分野においては、共同で取り組むことで、効率化が図られるだけでなく、高度な人材の確保にも効果を期待できるものでもある。

「1部1章2 情報共有の推進と共助の取組」でも詳述したが、情報共有活動は、枠組みを設定しただけでは目的を達することができず、信頼を醸成しながら少しずつ活動の幅を広げていくなど、運用を充実させて絶やさないことが重要である。さらに、情報共有の在り方は、単に全ての情報を１つの枠組みに集約すればよいというものではなく、特定の分野にとっては価値の高い情報については、秘匿性を確保しつつ、その分野の範囲で共有を行うことが総合的に適切であるような状況なども考えられる。そのため、多様な情報共有の枠組みが存在することが重要であり、それらの役割分担によって、効果的、効率的に情報共有を進めていくことに意味がある。

2.3　政府に期待される役割

「自助、共助、公助」という考え方は、社会全体のサイバーセキュリティの対応力を高めていくためにも意識すべき視点である。それぞれの主体が自分の役割を自覚することを前提としなければならないが、そのためには、一般の市民や企業に対して、その自覚を促すための取組も必要である。本章１において示したとおり、ネットワークに接続する機器が、国民生活に今後益々浸透していくことが想定される状況にあり、国民一般のリテラシー向上を図ることが重要である。戦略においては、「参加・連携・協働」という観点を示している。これは、全ての関係者が当事者意識をもって対応を進めるという考え方を示したものであるが、国は、自助や共助の取組を過不足なくサポートするという自らの役割も意識しつつ、インセンティブ構造を明確にすることで仕組みをデザインし、社会全体として効果を最大化するという姿勢が期待されている。

また、前述のとおり、ITにおける世界的なサプライチェーンに内在するサイバーセキュリティ上の課題や、国家又は国家の支援を背景とするとみられるサイバー攻撃が、政府機関や重要インフラ産業あるいは重要な知的財産を有する企業等を標的として世界各地で頻発してきており、新たなサプライチェーン対策、重要インフラ・政府機関保護等の諸政策を推進するとともに、国際場裡においては、悪意あるサイバー活動を抑止するためのサイバー空間における法の支配の推進及び脅威情報の共有を始めとする有志国等との連携協力を質・量とも高めていくことが重要である。他方で、上述の「参加・連携・協働」の考え方にも示されているとおり、政府あるいは政府間国際協力のみでそれを実現することはできない。政府、民間企業、大学や研究機関、市民団体、個人等様々な主体と機動的かつ密接に連携・協力することが不可欠であり、そうした状況を現出するために政府が必要な範囲で触媒役を果たし、全ての主体が「マルチステークホルダー」として一致協力して、我が国の広義の国益及び安全を確保していくことが求められている。

3　今後加速・強化して取り組むことが重要な事項

3.1　経済社会の活力の向上及び持続的発展

(1)　サプライチェーン全体のサイバーセキュリティ対策の強化

サイバー空間とフィジカル空間の一体化により、新たな技術の実装化が様々な分野で発生しており、攻撃の起点も拡大している。また、センサーなど、サイバー・フィジカル間の転写機能を持つ機器等のセキュリティの問題について、より重要な課題として取り組む必要がある。

こうした点を踏まえ、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対策を強化するため、2019年４月に策定したサイバー・フィジカル・セキュリティ対策フレームワークの各産業分野への実装・具体化を進めていくことが重要である。加えて、IoT機器の多様なセキュリティ上の課題に対応するセキュリティ・セーフティ要求の在り方や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も、国内外の動向を踏まえながら検討を行っていくことが重要である。また、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。

また、中小企業を含むサプライチェーン全体において、我が国のサイバーセキュリティ対策が海外製品や海外由来の情報に大きく依存しており、サイバー攻撃情報の実データの収集・分析に基づく知見の集積及びこれらに基づくセキュリティ技術・製品の開発並びに関連する人材育成が我が国で進まない状況を回避・脱却するため、国内のサイバーセキュリティ情報を収集・生成・提供するためのシステムを中小セキュリティ事業者を含む産学官連携のオープン・イノベーションのための基盤として構築・運用するとともに、製品開発や人材育成を促進する。

3.2　国民が安全で安心して暮らせる社会の実現

(1)　重要インフラ対策の推進

2019年度には、国内において、複数の事業者のサービスに影響を与えたクラウドサービスの障害事例が相次いで報告されたほか、リース契約満了後に返却した機密情報が蓄積されたハードディスクドライブが流出し、外部サービス利用時の委託契約の課題が浮き彫りになり、外部サービスの利用に際しては、利用契約で担保されている内容を踏まえつつ、適切な防護措置が必要なことや、データのライフサイクル全体を視野に入れたサプライチェーンマネジメントの実効性担保に関する課題が明確となった。また、サービス開始直後に不正利用が発生し、サービス廃止に至った事例が発生したことや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際、情報発信の在り方が課題となり、セキュリティ・バイ・デザインの考え方や障害対応に平時から備えておくことの重要性が再認識された。さらに、国外では、ランサムウェアの被害が数多く発生したが、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ことから、こうした動きに注視する必要がある。

これら昨今の環境変化や新型コロナウイルス感染症対策の動向を踏まえて、重要インフラ事業者等による継続的なサービス提供を行う際のリスクを的確に把握し、それらに対してどのように対応していくべきなのかを引き続き検討していく。その際、国内外、組織内外と適切に情報共有できるよう、情報共有体制の更なる強化を図り、また、組織全体としての体制の在り方を検討し、対処態勢の整備の推進、障害対応体制の強化を図るとともに、これらの取組を反映した安全基準の在り方を検討する。

なお、これらの検討は、東京2020大会後予定されている「重要インフラの情報セキュリティ対策に係る第４次行動計画」（2017年４月18日サイバーセキュリティ戦略本部決定。2020年１月30日最終改定）の改定に向けた評価・見直し作業と歩調を合わせて行う。

(2)　政府機関対策の推進

統一基準の初版が制定された2005年には、政府機関の情報セキュリティ対策において「情報セキュリティ水準の高い府省庁と低い府省庁の格差が大きい」「急激に変化するIT環境に対応した情報セキュリティ対策を実施する人材が全体的に不足している」等の問題が明らかになっていたことから、これらを解消するべく統一基準が制定された。初版制定から約10年経過した2014年度の改定の際に、政府機関の情報セキュリティ対策水準もある程度向上したとして、各府省庁の組織や取り扱う情報等の特性に応じて、個々に最適な情報セキュリティポリシーを定め、それを実行することに重点を置く運用を目指す見直しを行い、2016年度と2018年度に情勢に応じた改定を行い現行統一基準群となっている。

2021年度の統一基準改定においては、クラウドサービス利用時の基本的なセキュリティ対策についての追記のほか、社会的に話題となった機器廃棄時の漏えい対策として情報の暗号化等についての追記を検討している。また、新型コロナウイルス感染症への対策として政府機関等においても機関外での業務実施機会や複数の政府機関等が外部サービスを利用して連携する機会が増えたことを踏まえ、かかる環境下での情報セキュリティに対する特有の留意点や考え方を示していくことが有用であり、統一基準への追記を始め、必要な発信を行っていく。そのほか、新型コロナウイルス感染症対策そのものへのデジタル技術の適用や行政手続のオンライン化が急務となる中、統一基準に示している情報セキュリティの観点に基づく試験の実施の遵守事項については、適切な実施・運用がなされるよう、必要な対応を行う。

統一基準の改定により、各政府機関等の情報セキュリティポリシーが順次改訂され、ポリシーレベルにおける情報セキュリティ水準の引き上げが行われるが、現場の運用レベルでの水準を引き上げていくことも肝要であり、各機関等のさらなる努力が必要となる。

また、これまでも国の行政機関等が所掌する情報システムに関する情報セキュリティインシデントに関し報告を求めているところであるが、外部委託により民間事業者に政府が管理する情報を取り扱わせる際の委託業務において発生した情報セキュリティインシデントについて、報告を求めることを改めて政府決定に位置付けることとする。

(3)　東京2020大会を踏まえた未来につながる成果の継承

オリンピック憲章では、オリンピック競技大会の有益な遺産（レガシー）について、開催都市のみならず、開催国としても引き継ぐことが期待されている。1964年東京大会は、新幹線、首都高速道路、ごみのない美しい街並みなど、現在にも残る数々のレガシーが生み出された。1964年東京大会のレガシーとして今日に残っているものは、大会前からの官民を挙げた不断の準備・努力によって成し遂げられた成果が大会において高く評価され、大会後に継続されて現在も残っているものである。後世においても高く評価されるようなレガシーを残すためには、多数の関係組織が既に様々な取組を行っている現在の状況を考えた場合、大会の成功だけを考えた一過性の取組ではなく、大会後の持続性をも見据えた上で取組を実施することが効果的である。

新型コロナウイルス感染症拡大の状況等を踏まえ、東京2020大会は１年延期が決定されたが、大会に向けたサイバーセキュリティ確保のための取組の中には既に成果を上げつつあるものもあり、こうした取組を大会まで引き続き行っていくことが重要である。一方で、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た取組を大会に向けて行う必要がある。

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実施することが重要であるとともに、レガシーとして恒久的な国の施策に昇華するために、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である。ただし、大会後に整理等を行っている期間において、レガシーとなり得る取組を完全に止めてしまうことは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ような取組については大会後も速やかに実施することとし、レガシー化のための検討結果を踏まえて適切に修正を行っていくことが望まれる。

また、大会後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事業者に普及させることや、JISPを活用した情報共有体制を全国の重要インフラ事業者や参加を希望する事業者やスポーツ関連団体等まで拡大することだけでは十分だとは言えない。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やニーズを持っている事業者等も少なくないことから、大会後の検討に当たっても、多様な課題とニーズに対応できるようにすることが不可欠である。サイバーセキュリティを取り巻く情勢は日々変わってきていることから、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、大会後の検討に当たっては求められる。

3.3　国際社会の平和・安定及び我が国の安全保障への寄与

(1)　情報共有と重層的な国際連携の枠組み

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容易に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。サイバー攻撃・脅威に関する情報を、国際場裡においても各国の政府・民間機関と連携して迅速に共有することが、続いて行われ得る類似のサイバー攻撃を阻止し被害を最小化することにつながることは、国内においてサイバーセキュリティ協議会等での官民情報連携やセ

プターカウンシル・ISAC等における分野毎の民民連携の場合と基本的に同様である。また、個別情報の共有・連携に加えて、我が国は欧米諸国やアジア太平洋地域の13の国・地域とサイバー政策協議を実施し、サイバー空間における脅威認識や主要政策等についてハイレベルで省庁横断的な二国間協議を実施するとともに、内閣官房・各府省庁は別途それぞれのカウンターパート機関と実務的な国際連携を行うといった重層的な枠組みが発展してきている。CERT間では、IWWNやASEAN、FISRT等マルチの場や、各国とのバイの関係を通じて平時より情報交換を実施している。

サイバー空間における安全保障を取り巻く環境が厳しさを増す中、サイバー攻撃・脅威に関する迅速な情報共有を国際的に一層推進していくことが肝要である。特に新型コロナウイルスの感染が拡大する中、リモートでの国際的な情報共有・連携はむしろ活発化している一方で、リアルの国際会議や要人往来については中止又は延期が相次ぎ、これまでのような様態や頻度での対話は当面不可能になっている。こうした状況において、定期協議等の枠組みで連携・協力しているカウンターパート機関と、どのようにして従来と同等の機微にわたる、あるいは自由闊達な議論を実施していくのか模索する必要がある。また、このような確立したカウンターパート機関以外についても、地政学上等の重要性等にも鑑み、リソースを適切に按分しながら、協力チャネルを新規開拓・拡大していく必要もある。このように国際場裡において、自由・公正かつ安全なサイバー空間を実現するという我が国の理念や立場、政策等についてあらゆる機会を捉えて積極的に国際社会に対して発信していくことで、日本のプレゼンスを高めるとともに、国際社会の平和と安定に寄与していく。

(2)　海外支援戦略

2010年度に設立された「日・ASEANサイバーセキュリティ政策会議」等の場を通し、内閣官房を中心とした関係省庁との緊密な連携の下、ASEANを中心とした各国政府の能力構築支援を継続的に推進している。これらの取組を通し、各国政府のサイバーセキュリティ対応能力の継続的な向上を図るとともに、各国政府機関との友好的で緊密な関係が構築されている。

近年は、各国政府の能力向上に伴い、重要インフラ防護に対する技術面及び制度面での支援等、これまでの政府主体で可能な範囲を超えた支援ニーズが高まりつつある。このようなニーズに対し、過去10年にわたる支援により培った政府間の友好関係を維持しつつ、これをASEANで事業活動を行う産学を含めた多層的な協力関係に深化させるための方策について検討を行う。その際、政府は、各主体が能動的に取組を進め、それらの取組が一体となって長期的に効果を発揮できるよう、各主体におけるニーズや課題を十分に分析・把握する。また、各国における関連政策の進捗状況に鑑み、それぞれに適切な目標を定め、きめ細やかな支援を実施することとする。本検討を通して、ASEAN各国及びASEAN地域全体におけるサイバーセキュリティ対応能力のさらなる向上を図るとともに、ASEANとの経済的関係も深い我が国のサプライチェーンの安全確保を促す。また、我が国のサイバーセキュリティ戦略の基本的な在り方である「サイバーセキュリティエコシステム」の実現のためには、国際社会での存在感が高まりつつあるASEANとの関係強化は共助の観点からも重要であり、ASEAN地域における人材育成等も含めた長期的な視点で議論を行うことで、より効果が高まると考えられる。

3.4 横断的施策

(1) DX with Cybersecurity の実現に向けた人材育成

DXの進展と、それに伴うITを活用した新たな事業に取り組む企業・団体の増加は、日本の生産性や競争力向上の鍵と考えられる一方、サイバーセキュリティの確保が不十分なためセキュリティインシデントが発生し、結果として事業・サービスの廃止を余儀なくされる事例が生じることも懸念される。今後、DXと同時にサイバーセキュリティ対策を組み込んでいくことが求められることを踏まえ、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、企業等内におけるIT・サイバーセキュリティ関係の体制構築・人材育成といった点について検討していくことが必要である。

特に人材育成の観点では、DX経営推進者やDX事業推進者等、企業等の組織でDXを推進する人材がいわゆる「プラスセキュリティ」を実現するために必要な人材育成体系や人材流動性の状況、企業等内の各種のSIRT（セキュリティインシデントレスポンスチーム）に関する取組の現状を踏まえ、企業等の組織でDX経営・DX事業等のDXを推進する人材がサイバーセキュリティを含むリスクマネジメントの観点を適切に盛り込んだ経営や事業を実践する、DX with Cybersecurityの実現に資するための議論を進めていくことが必要である。

(2) 政府機関等のサイバーセキュリティを支える人材の確保・育成

年金機構事案を契機に2016年３月にサイバーセキュリティ人材育成総合強化方針を策定し、４年にわたって人材確保・育成に取り組んできた。

サイバー攻撃が複雑・巧妙化する中、政府機関等のサイバーセキュリティを確保するため、それらを支える人材の確保・育成は引き続き重要である。このため、これまでの取組の進捗状況や成果・課題を把握し、各府省庁における実情等を踏まえ、実質的な人材の量と質の向上のための取組の方向性を検討することが必要である。

(3) 研究開発の推進

2019年５月に策定した「研究・技術開発取組方針」も踏まえつつ、我が国としてのサイバーセキュリティ対策を継続的に高度化していくため、サイバーセキュリティの研究及び産学官連携の基盤構築に向けた議論を進めていく必要がある。研究開発の具体的内容と研究開発の活性化の両面で更なる検討を進めていくことが重要である。

特に、国際的に研究発表が伸びており、我が国でも伸びつつある実践的なサイバーセキュリティの研究分野に着目し、研究開発自体の推進や産学官連携の活用について議論し、日本独自の技術を生み出していくことや、優秀な人材の育成・確保していくことの基盤となる、サイバーセキュリティの研究及び産学官連携の基盤構築に向けた検討を進めていくことが重要である。また、こうした研究開発の成果を、実際のセキュリティ対策の製品・技術等に結びつけていくことも重要である。

(4)　普及啓発の推進

AIやIoTの生活への浸透に伴い、インターネット利用への不安感の拡大が見られる。また、具体的対策の実施状況としては、日常的な対策等において向上の傾向が見られる一方、インターネットバンキングの不正送金被害は直近では発生件数の増加も見られる。

こうした中、引き続き関係者が密接に連携して普及啓発活動が進められるよう、2019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」で重点対象とした中小企業、若年層、地域を中心に、代表的・客観的なデータを継続的に参照し、同プログラム全体の効果を評価する。特に、普及啓発・人材育成専門調査会等を活用し、プログラム全体としてのPDCAサイクルを実施することで、本プログラム全体の効果を評価し、各施策における重点的な取組内容を調整するなどの対応につなげていく。

（本ページは白紙です。）

別添１　2020年度のサイバーセキュリティ関連施策

別添１　2020 年度のサイバーセキュリティ関連施策

2020 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

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
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。
（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。

（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。
（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。

(3) 先端技術を利活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
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

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推進

(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
（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。

（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。

(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
（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。
（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。
（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。
（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。

(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
（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。
（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）
（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）

（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。
（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。
（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。

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の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
（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。
（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。
（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。
（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。
（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。

(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
（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。
（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。

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
（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。

(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
（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。
（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。
（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（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。
（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）	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。
（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。
（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。

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
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

（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 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。
（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。
（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。

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
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

（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。

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
（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。
（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。

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
（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）
（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。
（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。
（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。

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
（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。

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
（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。

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
（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。
（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。
（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。
（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。

(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
（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）	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。
（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。
（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。
（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。
（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。
（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。
（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。

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
（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。
（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。

（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、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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。

(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
（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。

(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
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。
（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。

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
（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。
（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。
（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。

(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
（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。
（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。
（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。

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
（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。
（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。
（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。）

(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
（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。
（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。
（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。

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
（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）	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。
（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。
（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。
（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。
（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。
（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。
（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。
（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）	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。
（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。

(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
（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。

(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
（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。

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
（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。
（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、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）
（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。
（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。
（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。
（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。

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
（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。

(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
（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。
（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。

(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
（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。

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
（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。
（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）	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。

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
（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。
（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。

（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。
（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。
（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。
（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。
（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。

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
（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。
（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。
（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。

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
（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。
（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。
（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。

(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
（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
（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。

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
（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。
（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

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
（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 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。

（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。
（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。
（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。
（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。
（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。
（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。

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
（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）	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）	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。

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
（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。

(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
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。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。

(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
（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）
（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。

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
（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）

（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。
（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。
（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。

(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
（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。
（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。
（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。
（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。

(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
（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）	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）
（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。
（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。
（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。
（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。

（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、周知及び普及を図る。
（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。

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
（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。
（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。
（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。
（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。
（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。
（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。

(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
（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。
（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。
（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。
（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。
（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。

（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、大学における情報技術人材の育成強化を目指す。
（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、大学における情報技術人材の育成強化を目指す。

(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
（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。
（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。
（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。
（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。

(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
（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。

4.2　研究開発の推進

(1)実践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
（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）
（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）
（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基礎的な検証を実施する。
（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）
（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）
（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、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。

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
（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）

（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）
（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）
（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）
（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）

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
（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。
（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。
（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。
（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。
（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	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）

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
（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。
（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、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。
（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）
（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。（再掲）
（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。
（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。
（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。
（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。

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
（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。

（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。
（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）
（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）

(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
（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。

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
（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。

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
（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）
（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。
（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。
（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。
（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。
（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。

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
（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。

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
（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。
（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。
（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。
（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。
（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。
（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）
（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）
（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。
（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）

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
（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。
（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。
（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。

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
（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	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。
（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）
（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）
（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）

別添２　2019 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	2019 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、必要に応じてフォローアップや見直しを図る。	・普及啓発・人材育成専門調査会において、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うとともに、施策間の連携を促進した。
（イ）	経済産業省	経済産業省において、コーポレート・ガバナンス・システム研究会（第２期）における議論を踏まえ、グループ内部統制システム上の重要なリスク項目としてサイバーセキュリティを認識し、「サイバーセキュリティ経営ガイドライン」などを参照してセキュリティ対策の在り方に関する検討の必要性を盛り込んだグループガバナンスの在り方に関するガイドラインを策定する。	・経済産業省において、コーポレート・ガバナンス・システム研究会（CGS 研究会）（第２期）において、サイバーセキュリティを内部統制システム上の重要なリスク項目として位置づけることを検討し、グループ経営を行う上場企業が対象のグループ・ガバナンス・システムに関する実務指針（グループガイドライン）にサイバーセキュリティ対策の在り方を位置づけた。（2019 年６月）
（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、実効性評価の第三者評価を実施する外部専門組織と連携して促進する。	・経済産業省において、 ・投資家向けの説明会において、「取締役会の実効性評価」の中にサイバーセキュリティへの経営層の関与を評価項目として組み込むことの重要性を周知した。また、「取締役会の実効性評価」に関する第三者評価を実施する機関との連携を強化し、実効性評価へのサイバーセキュリティへの経営層の関与に関する評価項目の組み込みを促進した。 ・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 を 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。
（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、「サイバーセキュリティ経営ガイドライン」の改訂の検討を行い、説明会等を通じて、当該ガイドラインの普及を図るとともに、更なるサイバーセキュリティ経営への意識の定着のため、改訂を含めた検討を進める。	・経済産業省において、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」の普及を図った。 ・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（以下、可視化ツール）を作成し、2020 年３月 25 日にベータ版を公開した可視化ツールはサイバーセキュリティ経営ガイドライン付録をベースに作成されたもので、約 40 問の設問に回答することにより、自社のサイバーセキュリティ対策状況を容易に可視化できるツールである。自社の状況把握だけでなく、業界平均との比較等も可能となる。
（オ）	内閣官房	内閣官房において、サブワーキンググループの運営を継続し、有識者の意見も踏まえつつ、サイバーセキュリティ関係法令集の策定に向けて検討を進め、ハンドブック（仮）として成果物を取りまとめる。	・サブワーキンググループ及びタスクフォースにおける議論を経て、「サイバーセキュリティ関係法令 Q&A ハンドブック」を取りまとめ、2020 年３月２日に NISC のウェブサイトで無料公開を行うなど、周知啓発を図った。

(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	2019 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、プラクティス検討会を中心に、「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」の継続的な事例収集を行い、継続的な更新を行う。また、企業のサイバーセキュリティ対策の実施状況を可視化するツールを作成する。	・経済産業省において、2019 年３月に公開した「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」に関して、2018 年度に収集していない指示項目を中心にプラクティスを収集し、改定を実施した。また、企業のサイバーセキュリティ対策の実施状況を可視化するツールの β 版を策定し、公開した。
（イ）	総務省	総務省において、企業の情報開示の実例も盛り込んだ「サイバーセキュリティ対策情報開示の手引き」を策定、公表し、その普及を図る。	・サイバーセキュリティタスクフォースの下で「情報開示分科会」 を開催。　同分科会において、民間企業のサイバーセキュリティ対策の情報開示に関する課題を整理し、民間企業における サイバーセキュリティ対策の情報開示を促進するために必要な方策等について検討を実施し、その検討結果を踏まえ民間企業にとって参考となり得る情報開示の事例等をまとめた「サイバーセキュリティ対策情報開示の手引き」（案）を作成し、意見公募を経て 2019 年６月に公表を行った。
（ウ）	経済産業省	経済産業省において、本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審査登録制度のよりよい利用についての検討を行い、競争力強化やサイバーセキュリティの成長産業化に取り組む。	・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。また、政府調達時や、税制優遇措置又は補助金給付を受ける際に、登録サービスの利用を推奨することで、制度の活用や普及の促進を行った。結果、2019 年度は、登録サービス件数を約 100 件から約 170 件まで増加させた。
（エ）	総務省 経済産業省	総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、それに必要となるシステムやサイバーセキュリティ対策製品等の導入に対して税額控除等を措置するコネクテッド・インダストリーズ税制の活用を促すことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進する。また、2018 年度の実績を踏まえ事例の紹介や経産省 HP でのニーズ調査などを用い、税制の更なる活用促進策を見いだし、ニーズに沿った周知・広報を強化する。	・総務省及び経済産業省において、説明会等を通じた制度周知を行ったほか、HP における事例の紹介等を実施し、制度の更なる活用を促すことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進した。
（オ）	経済産業省	経済産業省において、IPA を通じ、サイバーセキュリティお助け隊の実証事業を全国で実施し、中小企業の実態や求めるサービス内容、レベル等を明らかにするとともに、中小企業のサイバーセキュリティ意識向上を図る。実証結果を基に、セキュリティベンダー、損害保険会社等連携し、中小企業が利用し易い、支援体制、サイバー保険について検討、構築し、普及を図る。	・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８地域で実施し、約 1,000 社の中小企業が実証に参加した。実証により、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難な中小企業があり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、サービス購入費用が中小企業にとって許容可能な価格である必要があること等、中小企業の実態・ニーズが明らかになった。
（カ）	総務省	総務省において、総合通信局、地域の事業者、保険会社、セキュリティ関係機関等の関係者間において、サイバーセキュリティに関する情報共有を促進する取組を実施する。	・総務省において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新たなセミナーや演習などを実施。

(3) 先端技術を利活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	2019 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、不正競争防止法改正を踏まえ、適切なデータ共有・利活用に関する指針の策定に向けた検討を行う。	・データ共有・利活用に関する指針策定に向けた「企業におけるデータ利活用・保護の戦略立案のための手引書（案）の作成」に係る検討会を実施した（全７回）。2018 年に実施した企業のデータ利活用状況調査を踏まえ、企業がさらに積極的にデータ利活用を行うためのポイント集等を作成するための支援調査を実施した。 ・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（2019 年度２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。2019 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～」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。	・「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った。
（エ）	文部科学省	文部科学省において、2019 年１月１日に施行された改正著作権法によって、いわゆる非享受目的の利用に係る権利制限規定（著作権法第 30 条の 4）が創設されたことに伴い、「リバースエンジニアリングを行うこと」「解析やその訓練のために必要なプログラム等を保全し、コピーを作成すること」「セキュリティ上の調査のためのデバッグ等の解析」なども著作権違反にならないことを明確化するよう、ガイドラインを整備し、周知を行う。	・2019 年 10 月 24 日、いわゆる非享受目的の利用に係る権利制限規定（著作権法第 30 条の４）を含む「柔軟な権利制限規定」の趣旨・内容・解釈や具体的なサービス・行為の取扱い等について、文化庁としての基本的な考え方を示した「デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方」を策定、公表した。
（オ）	経済産業省	経済産業省において、IPA を通じ、サイバーセキュリティビジネスの振興・活性化を図るため、サイバーセキュリティ対策におけるニーズの明確化・具体化、シーズの発掘やビジネスマッチングを行う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）を継続して開催する。また、コラボレーション・プラットフォームの地方開催についても検討を進める。	・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２～３か月に１度の頻度で開催し、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。また、地域に根差したセキュリティコミュニティの形成を促進するために、東北や中国地域等で地方版コラボレーション・プラットフォームを開催した。

（カ）	経済産業省	経済産業省において、日本のセキュリティニーズに応じた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。	・経済産業省において、我が国発のサイバーセキュリティ製品・サービスの創出・活用を促進するため、有識者会議を開催し、製品の公募を実施し、選定された製品の検証項目を策定した。さらに、その検証項目に従って実施されたセキュリティ製品の検証結果を評価・公表することで、各製品の有効性評価の結果を公表するという施策のトライアルを実施した。 ・また、ユーザが導入した製品・サービスを、製品・サービス導入事例として安全に公表するための手引書として「試行導入・導入実績公表の手引き」を作成した。
（キ）	経済産業省	経済産業省において、ASEAN やインド等の新興国に対し、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。	・カンボジアにおいて、日本仕様の運用技術に関する人材育成やサイバー攻撃への対応策など教育プログラムの展開可能性の調査を実施した。また、インドにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入のため、現地の電力企業向けに研修を実施した。
（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、規模を拡大し実施する。	・2020 年２月 24 日から 28 日まで米国サンフランシスコで開催された RSA カンファレンスについて、我が国２年目となるジャパン・パビリオンの出展支援を実施。※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	2019 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、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、データそのものの信頼性確保や、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。	・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・普及や、ビルシステムのセキュリティに関するガイドラインの第１版の公表を始め、各産業分野におけるセキュリティ対策の検討を引き続き推進した。また、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を立ち上げ、それぞれ検討を行った。

(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	2019 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実証実験に向けた準備を着実に進める。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。	・５年間のプロジェクト活動の２年目として着実に推進し、基本方式の設計とデモシステムの開発を実施した。 ・2020 年度から予定している特定分野での実証実験の準備を着実に進めるとともに、グローバル連携や関係省庁連携を行い、社会実装に向けて取り組んだ。
（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、IoT 機器に求められる機能の要求を明確化すると共に、産業界の自主活動を含めたラベリングの仕組み、認証制度の在り方を検討する。	・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 機器等に求められる機能の要求を明確化するとともに、産業界の自主活動を含めたラベリングの仕組み、認証制度の在り方等を議論する第２層タスクフォースを立ち上げ、検討を行った。
（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た取組を進める。	・技術検証体制の整備に向け、技術検証に関する技術動向や諸外国の制度の状況について調査を実施した。

(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	2019 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、政府広報等を用いて普及を図った。
（イ）	総務省	総務省において、総合通信局、地域の事業者、保険会社、セキュリティ関係機関等の関係者間において、サイバーセキュリティに関する情報共有を促進する取組を実施する。（再掲）	・総務省において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新たなセミナーや演習などを実施。

（ウ）	経済産業省	経済産業省において、IPA を通じ、サイバーセキュリティお助け隊の実証事業を全国で実施し、中小企業の実態や求めるサービス内容、レベル等を明らかにするとともに、中小企業のサイバーセキュリティ意識向上を図る。実証結果を基に、セキュリティベンダー、損害保険会社等連携し、中小企業が利用し易い、支援体制、サイバー保険について検討、構築し、普及を図る。（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８地域で実施し、約 1,000 社の中小企業が実証に参加した。実証により、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難な中小企業があり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、サービス購入費用が中小企業にとって許容可能な価格である必要があること等、中小企業の実態・ニーズが明らかになった。
（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「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、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」の普及を図った。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、説明会等において「中小企業の情報セキュリティ対策ガイドライン」の普及を図った。
（オ）	経済産業省 総務省	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、中小企業等の生産性向上に資する IT 導入等の促進とあわせて、セキュリティに係る意識向上やその対策に向けた具体的な取組を促す。 ・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、中小企業に対して、日本政策金融公庫による特別利率での融資も更に実施する。 ・総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、システムやセンサー・ロボット、セキュリティ対策製品等の導入に対する税制措置の活用を促し、事業者のセキュリティ対策の強化と生産性向上を同時に促進する。	・経済産業省において、 ・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 を 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。 ・中小企業の IT 活用を支援する IT ベンダー等をスマート SME サポーターとして認定し、中小企業向けに、特設サイトで「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」等の情報を開示する仕組みを構築した。 ・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 382 社の中小企業に対し実施した。 ・中小企業で対策が進んでいないネットワークセキュリティの更なる普及促進に向けて、財政投融資制度による特別利率での融資を実施した。また、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット、セキュリティ対策製品等の導入に対して、特別償却 30%又は税額控除３%（賃上げを伴う場合は５%）を措置するコネクテッド・インダストリーズ税制を引き続き運用するなど支援策を強化した。 ・総務省及び経済産業省において、説明会等を通じた制度周知を行ったほか、HP における事例の紹介等を実施し、制度の更なる活用を促すことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進した。

（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。また、「SECURITY ACTION 制度」の更なる周知を図り、参画企業の拡大に取り組むとともに、ニーズに応じた制度の見直しについて検討を行う。	・「講習能力養成セミナー」を全国 13 箇所において開催し、中小企業の経営者、社内教育担当者等合計約 935 名が参加した。 ・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のセミナー等へ合計 51 箇所に講師を派遣し、約 3,060 名が受講した。 ・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 を 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。 ・上記活動の中で SECURITY ACTION 申込受付を実施し、自己宣言者 93,406 件（一つ星：80,985 件、二つ星：12,421 件）、普及賛同企業等が 88 件に増加した。また、「中小企業の情報セキュリティ対策ガイドライン」のダウンロード数が累計 370,000 程度に増加した。 ・「中小企業の情報セキュリティ普及推進協議会」を４回開催し、SECURITY ACTION 制度の普及促進及び二つ星の次の取り組みの方向性を協議した。

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	2019 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、経費の見積もりの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。具体的には、研究開発戦略専門調査会等を通じ、関係省庁の IoT システムのセキュリティに関する取組について情報共有を行うとともに、着実な取組が行われているかどうか、確認する。	・「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。具体的には、各種講演活動や関係省庁の IoT セキュリティに関する取組との連携を図る等、取組を継続する。	・各省庁の IoT セキュリティに関連する取組との連携を図る等、協働を進めた。

（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 推進コンソーシアム IoT セキュリティ WG 等を通じて、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 2020 年 3 月に更新した（なお、消費者庁で把握した判決情報には、IoT 機器のソフトウェアの脆弱性によるインシデントに関する訴訟情報はなかった）。
（オ）	内閣官房	内閣官房において、IoT システムの設計・開発・運用に係る概念について、国内で官民が連携してモノ・ネットワーク、システム等に関する各種基準等への組込みを促進するため、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、積極的に取り組む。具体的には、日本提案の国際標準化に向け、国内委員会に参加する等、有識者と議論・連携しながら、着実に標準化プロセスを進める。	・国際標準化機関である ISO/IEC の JTC1 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」等を基本とした国際標準化活動を推進した。

(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	2019 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 経済産業省	内閣官房及び関係省庁において、ネットワーク上の脆弱な IoT 機器の効果的な対策等のための体制について、官民の関係者の取組全体を把握しつつ、引き続き検討する。	[NISC] ・サイバーセキュリティ関係施策に関する重点を図る分野として、IoT 機器の脆弱性について、ネットワーク上の脆弱な IoT 機器の対策のための IoT セキュリティに関する取組（総務省・サイバーセキュリティ TF、NOTICE 施策）状況の把握、意見交換を行った。 [警察庁] ・警察庁において、サイバー犯罪対策について講演を行った。 [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）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」を実施するとともに、NICT のサイバー攻撃観測網（NICTER）によりマルウェアに感染していることが検知された機器の利用者への注意喚起を行う取組を実施した。 [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 機器等に求められる機能の要求を明確化するとともに、産業界の自主活動を含めたラベリングの仕組み、認証制度の在り方等を議論する第２層タスクフォースを立ち上げ、検討を行った。
（イ）	総務省 経済産業省	・総務省及び経済産業省において、IoT 推進コンソーシアム IoT セキュリティ WG 等を通じて、IoT 機器のセキュリティ対策を推進する。 ・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）の改正省令を施行する。施行に先立ち、運用方法や解釈等を定めるガイドラインを策定する。 ・経済産業省において、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下で開催しているスマートホーム 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進め、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を策定する。	[総務省] ・電気通信事業法の枠組みにおいて端末設備等規則を改正し、強制規格としての技術基準が策定され、2020 年４月１日から施行した。また、この施行に先立ち、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１版）」を 2019 年４月 22 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進め、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策定作業を進めた。
（ウ）	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）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、2019 年度は延べ 2,249 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。

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	2019 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、フェイクニュースや偽情報への対策のため、「プラットフォームサービスに関する研究会」を開催し、表現の自由に留意しながら、欧州の動向も参考にしつつ、ユーザリテラシー向上及びその支援方策、また、ファクトチェックの仕組みやプラットフォーム事業者との連携等の自浄メカニズムなどについて検討を行う。	・プラットフォームサービスに関する研究会の最終報告書を取りまとめ・公表した。

(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	2019 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。2019 年度においては、ソフトウェア製品の届出 244 件、ウェブアプリケーションの届出 1,032 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、128 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、2019 年度においては、脆弱性対策情報を約 19,000 件（累計：約 116,000 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への対応など、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。	・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・啓発活動を行う。	・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（新たなファジングツールの導入方法及び、利用方法等）、公開資料（ファジング実践資料）の拡充を行い、関係者と連携を図りつつ普及・啓発活動を推進した。

（オ）	経済産業省	経済産業省において、フィッシング対策協議会及び JPCERT/CC 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。2019 年度は、2020 年３月末現在で 12943 件のフィッシングサイト閉鎖の対応を行った。そのうち 71%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収集・分析するとともに、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、「情報セキュリティ EXPO」等のイベント、各種講演等で icat の紹介を行い、icat サービスの普及促進を図った。また、icat の利用サイト数は約 1,200 サイトとなった。
（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、攻撃検出条件の見直しを検討する。	・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、2019 年度のダウンロード数は 3,156 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「ウェブサイト開設等における運営形態の選定方法に関する手引き」、「安全なウェブサイトの運用管理に向けての 20 ヶ条」の公開を継続した。また、AppGoat V3.0 を活用した脆弱性対策の普及促進を図るため、IPA 及び高等専門学校にて高等専門学校の教員向け講習を行い、教材としての AppGoat 利用拡大を推進した。
（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。	・経済産業省において、JPCERT/CC を通じて、2019 年度は国内でのカンファレンス及び事業者など向けのセキュアコーディングに関するセミナーを開催するとともに、Software Bill of Materials に関する勉強会を１回実施、開発者ミーティングを２回実施した。
（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）を促進した。
（サ）	総務省	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。

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	2019 年度　年次計画	取組の成果、進捗状況
（シ）	経済産業省	経済産業省において、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。
（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。	[NISC] ・重要インフラ所管省庁と協力し、各重要インフラ分野の制度的な枠組みの現状を取りまとめた。 ・第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、「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）」を 2019 年５月に改定し、本指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。また、サイバーセキュリティを取り巻く情勢を踏まえ、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」を追加した。 ・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実施し、安全基準等の浸透状況等を確認した。 ・重要インフラ所管省庁における安全基準等の分析・検証、改定の実施状況等について調査を実施し、安全基準等の改善状況を確認した。 [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、「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版）」及び「事業用電気通信設備規則」について、改善に向けた分析・検証を行っている。 ・放送分野については、放送設備等のサイバーセキュリティ確保に関する省令改正を実施したほか、「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、改善に向けた分析・検証を行っている。 ・ケーブルテレビ分野については、「ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン」について、改善に向けた分析・検証を行っている。加えて、放送設備等のサイバーセキュリティ確保に関する省令改正を実施した。 [厚労省] ・水道分野については、「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。 ・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」の改定素案を策定した。 [経済産業省] ・電力分野においては日本電気技術規格委員会の「スマートメーターシステムセキュリティガイドライン」、「電力制御システムセキュリティガイドライン」の改定を踏まえ「電気設備の技術基準の解釈」の改正を行った。 ・石油分野においては「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」の改定を実施した。 ・ガス分野においては「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」を廃止し、新たに「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」を策定した。 [国土交通省] ・航空、空港、鉄道及び物流分野については、国土交通省において「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、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」を作成している。

（セ）	金融庁	金融庁において、資金決済法等の改正の趣旨を踏まえ、サイバーセキュリティの強化に向け、日本仮想通貨交換業協会における実効的な自主規制機能の発揮を促すとともに、同協会と連携しながら、暗号資産交換業者におけるサイバーセキュリティ対策の実施状況等のモニタリングを行う。	・金融庁において、日本仮想通貨交換業協会が暗号資産交換業者のサイバーセキュリティ強化を目的とした自己点検チェックリストを策定する際に支援するとともに、暗号資産の不正流出事案が発生した際には、再発防止を目的に同協会と情報共有を行った。加えて、金融庁における立ち入り検査の実施等を通じて、暗号資産交換業者のサイバーセキュリティ対策の実施状況等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。
（ソ）	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構築に向け、引き続き検討の深化を図る。	・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、2020 年２月の自動運転専門分科会に基準案を上程した。また、2019 年に交通安全環境研究所において、新たに「情報セキュリティ審査準備室」を設立し、サイバーセキュリティの国際基準の適合性に係る審査体制の整備を進めている。
（タ）	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 年度以降、自動走行の開発の核となる自動車工学とサイバーセキュリティを含むソフトウェアエンジニアリングの両方を担える人材が不足している事から、人材育成等に活用する。また、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。	・2018 年度事業で構築した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）を警察大学校での研究開発に活用。また、情報系大学に対して同テストベッドを貸し出し、自動走行におけるサイバーセキュリティ実装手法を体験頂いた。同取組を通じて、自動走行の開発の核となる自動車工学とサイバーセキュリティを含むソフトウェアエンジニアリングの両方を担える人材の確保及び育成を図ったところ。
（チ）	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。	・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。
（ツ）	内閣官房	空の産業革命に向けた総合的な検討の検討体制を整理し、専門家等が検討を進めるとともに、内閣官房及び関係省庁等による「小型無人機に係る環境整備に向けた官民協議会」の場に報告し、引き続き論点整理を進める。	・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、「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」を決定した。

(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	2019 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、関係省庁との連携によるスマートフォンに関する青少年に対する有害環境対策の徹底等、スマートフォンの安全利用のための環境整備に向けた取組を実施する。	・SNS に起因する事犯の児童の被害防止を図るためのリーフレットを作成し、各都道府県警察に配布するとともに、警察庁ウェブサイトに掲載した。 ・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。 ・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、2020 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。
（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。	・不正アクセス防止対策に関する官民意見集約委員会による情報セキュリティ・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推進した。 ・2019 年中の不正アクセス行為の発生状況等を 2020 年３月５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。
（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、2019 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、2019 年末現在の全国のサイバー防犯ボランティア数は、274 団体 9,625 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や事業者からの個別の相談への対応を通じて、個別事案に関する個人情報保護法の解釈に対応する。	・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計 140 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 16,518 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・研修センターについて、最新のサイバー空間情勢に応じた授業項目の見直しを行うとともに、同センターを通じてサイバー犯罪・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始めとする全部門の捜査員を対象に、当該センターで実施した研究の成果を活用しつつ、実際の事案を想定した演習を多く取り入れるなど、サイバー空間における警察全体の対処能力の底上げに資する研修を実施する。	・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、同センターで実施した研究の成果を活用しつつ、サイバーレンジ（人材育成基盤装置）による実際の事案を想定した演習を多く取り入れるなど、高度かつ実践的な研修を実施した。
（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。	・デジタルフォレンジック用資機材等を整備し、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。	・検察当局及び都道府県警察において、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、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研修及び民間企業への講義委託の積極的な実施、官民人事交流の推進、技術的に高度な民間資格の活用等、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。	・JC3 と連携し、急増した不正送金事犯や改ざんされた EC サイトに係る注意喚起を実施したほか、捜査の過程で把握したリスト型攻撃ツールを JC3 と分析、広報するなどして、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、フィッシング対策協議会および JPCERT/CC 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。	・経済産業省において、2019 年度は複数の海外団体の発信するフィッシング対策関連の情報収集を行った。
（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、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す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	2019 年度　年次計画	取組の成果、進捗状況
(ア)	内閣官房 金融庁 総務省 厚生労働省 経済産業省 国土交通省	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、自然災害の多発やサイバーセキュリティ戦略の改定等、指針第５版とりまとめ後の環境変化等を踏まえた「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」の改定とそれに基づく、各分野の安全基準等の整備・浸透を促進する。 「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次行動計画に基づき、５つの施策群（安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化）に関する取組を実施した（「安全基準等の整備及び浸透」については、(ス)・(ソ)及び 2.1(1)（ス）、「情報共有体制の強化」については(コ)・(ツ)、(2)(ア)及び 2.6(ア)、「障害対応体制の強化」については(テ)、「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、2019 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。 ・耐災害性能が向上する電波監視施設の更改を行い、また、同施設のセンサー26 か所を 2019 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設置した。
(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「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」に基づき、関係事業者等の取組を更に推進する。	・2018 年６月１日に「割賦販売法の一部を改正する法律（平成 28 年法律第 99 号）」を施行し、同法において規定するセキュリティ対策の実務上の指針である「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 2019」（クレジット取引セキュリティ対策協議会）に記載された関係事業者等の取組を促進した。
(エ)	厚生労働省	厚生労働省において、保険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、当該仕組みにおけるセキュリティ対策強化について、必要な実証等を行う。	・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、「保健医療情報を全国の医療機関で確認できる仕組みに関わる調査事業」において、リスクアセスメントの検討等を行った。
(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。 ・医療機器のサイバーセキュリティの確保に関するガイダンスについて（薬生機審発 0724 第１号、薬生安発 0724 第１号、平成 30 年７月 24 日厚生労働省医薬・生活衛生局医療機器審査管理課長、同医薬安全対策課長通知）を医療機器の製造販売業者向けの講習会にて周知し、製造販売業者が行うべきサイバーセキュリティへの取組及び対応を具体的に提示した。
（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）において、新たなサイバーセキュリティリスクについても考慮しながら、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の場の場で、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、2019 年度中に４回開催した。
（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中小事業者へ拡大すると共に、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。	・分野横断的演習の参加者が年々増えており、セキュリティの取組の輪が広がっている。
（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の高度化を図り、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ほか、情報共有の対象機関を拡大した。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・強化していくと共に、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	2019 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。 また、2020 年東京オリンピック・パラリンピック競技大会に関係する重要なサービスについても、安全かつ持続的に提供できるよう、この取組を継続して推進する。 ・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に対し、「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」に基づくリスクアセスメントの実施（継続的な見直しを含む）の浸透に向けた取組を行う。 ・重要インフラ事業者等の事業継続計画及びコンティンジェンシープランに対し、盛り込まれるべき「サイバー攻撃リスクの特性並びに対応及び対策の考慮事項」の浸透に向けた取組を行う。	・オリパラ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」の Web サイトへの掲載や説明会で配布することで浸透を図った。また、当該ガイドラインを重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加した「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」について、2019 年５月のサイバーセキュリティ戦略本部において、「データ管理」の脅威例、リスク源の例を追加する改定を行った。 ・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、分野横断的演習のテキストブックに掲載するとともに、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。

（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（金融機関に対する脅威動向の分析を踏まえて作成した攻撃シナリオに基づく実践的な侵入テスト）」等、より高度な評価手法の活用を促していく。	・金融庁において、大規模な金融機関に対して、「脅威ベースのペネトレーションテスト」の活用を促した結果、多くの金融機関で同テストの活用が進められた。

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 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	2019 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] ・重要インフラ所管省庁と協力し、各重要インフラ分野の制度的な枠組みの現状を取りまとめた。 ・第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、「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）」を 2019 年５月に改定し、本指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。また、サイバーセキュリティを取り巻く情勢を踏まえ、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」を追加した。 ・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実施し、安全基準等の浸透状況等を確認した。 ・重要インフラ所管省庁における安全基準等の分析・検証、改定の実施状況等について調査を実施し、安全基準等の改善状況を確認した。 [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、「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版）」及び「事業用電気通信設備規則」について、改善に向けた分析・検証を行っている。 ・放送分野については、放送設備等のサイバーセキュリティ確保に関する省令改正を実施したほか、「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、改善に向けた分析・検証を行っている。 ・ケーブルテレビ分野については、「ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン」について、改善に向けた分析・検証を行っている。加えて、放送設備等のサイバーセキュリティ確保に関する省令改正を実施した。 [厚労省] ・水道分野については、「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。 ・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」の改定素案を策定した。 [経済産業省] ・電力分野においては日本電気技術規格委員会の「スマートメーターシステムセキュリティガイドライン」、「電力制御システムセキュリティガイドライン」の改定を踏まえ「電気設備の技術基準の解釈」の改正を行った。 ・石油分野においては「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」の改定を実施した。 ・ガス分野においては「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」を廃止し、新たに「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」を策定した。 [国土交通省] ・航空、空港、鉄道及び物流分野については、国土交通省において「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、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」を作成している。

（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。	・2018 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、2019 年８月に公表した。 ・上記の事故等の発生状況の分析結果や、有識者からの意見を踏まえ、セルラーLPWA 等を利用した IoT 向けサービスの本格化に向け、2019 年６月にセルラーLPWA に係る重大な事故の基準の追加等に係る電気通信事業法施行規則等の改正を行った。
（ソ）	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、官民双方が一層安心・安全にクラウドサービスを採用し、継続的に利用していくため「クラウドサービスの安全性評価に関する検討会」について、2020 年秋の全政府機関等での安全性評価制度の利用開始とその後の重要産業分野等への評価結果の活用の推奨に向け、2019 年度中に制度の実証ととりまとめを行う。 ・内閣官房において、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」に、「データ管理の在り方」を追加する改定を行う。	［経済産業省］ ・「クラウドサービスの安全性評価に関する検討会」の議論の過程において、制度の実現可能性に関する実証を行うとともに、当該実証の結果も踏まえたとりまとめを行った。 ［NISC］ ・「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）」を 2019 年５月に改定し、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対策項目として「データ管理」を追加した。 ［内閣官房・総務省・経済産業省］ ・サイバーセキュリティ戦略本部第 23 回会合において、「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の基本的枠組みについて」の決定を行った。
（タ）	厚生労働省	厚生労働省において、「医療情報システムの安全管理に関するガイドライン」（第５版）の分かりやすい資料を公開することで普及に取り組む。	・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」（第５版）の分かりやすい資料を作成し、ホームページ上に公表した。
（チ）	厚生労働省	厚生労働省において、2019 年度より３年間の予定で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を実施することとしており、これにより医療機関及び製造販売業者における、国内外における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おり、順調に進捗している。

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	2019 年度　年次計画	取組の成果、進捗状況
（ツ）	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。 ・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、及び分野横断的な情報を内閣官房に集約する仕組みの検討を進める。 ・効果的かつ迅速な情報共有に資するため、情報共有体制構築に係る検討を行う。 ・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。 ・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	2019 年度　年次計画	取組の成果、進捗状況
（テ）	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 に立ち上げた「産業サイバーセキュリティセンター」において、これまでの２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む。 ・金融庁において、参加金融機関および金融業界全体のセキュリティレベルの底上げを図るため、対象業態の拡充や 2020 年東京大会の開催を踏まえたシナリオを策定し、より実効性の高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、2019 年 11 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分野横断的演習を実施した。 [金融庁] ・金融庁において、金融業界全体のインシデント対応能力の向上を図ることを目的として、2019 年 10 月に金融機関約 120 社が参加し、東京 2020 大会の開催を踏まえたシナリオにより、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）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、2019 年度は、重要インフラ事業者等の民間事業者から 320 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２年間実施した。その経験及び第１期、第２期の修了者約 150 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 70 名の受講生を受入れ、第３期「中核人材育成プログラム」を 2019 年７月に開講した。

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	2019 年度　年次計画	取組の成果、進捗状況
（ト）	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 34 件(2020 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。
（ナ）	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て行う。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策定に着手した。

（ニ）	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。	[NISC] ・我が国で使用される制御機器・システムについて、現状の規格について調査や、実際に運用を行っている事業者等への調査を行った。 [経済産業省] ・経済産業省において、JPCERT/CC を通じ、2013 年度に整えられた、制御システムの脆弱性届出の体制に基づき、脆弱性情報の受付、調整を行った制御システム関連脆弱性調整件数は、17 件（2020 年３月末時点）である。
（ヌ）	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	2019 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。 [総務省] ・神奈川県においてリース契約等により返却した物品からの情報流出事案を受けて、情報システム機器の廃棄等時におけるセキュリティの確保についての事務連絡を地方公共団体に発出した。 ・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、地方公共団体の内部環境からパブリッククラウドに接続するためのセキュリティ要件及び自治体職員による庁内情報環境へのリモートアクセスに関するセキュリティ要件を内容とする中間報告をとりまとめ、地方公共団体へ情報提供した。 ・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：73 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。	【集合研修実施状況】 （１）情報セキュリティ対策セミナー 年五回実施　受講者数 396 名 （２）情報セキュリティマネジメントセミナー 年三回実施　受講者数 158 名 （３）情報セキュリティ監査セミナー 年二回実施　受講者数 88 名 【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 2019 年８月５日～2020 年１月 21 日 受講者数 456,571 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。また、地方公共団体の外郭団体での情報セキュリティインシデントも発生していることから、LGWAN メール以外の媒体(インターネットメール)により情報提供を行う外郭団体数の増加を図る。	・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 WEB サイトを用いて提供した。 （実績） メルマガ・ニュース発行：37 件
（エ）	総務省	総務省において、関係機関と協力の上、サーバやネットワーク機器等における脆弱性診断を地方公共団体自らが実施できるよう支援する。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。	・地方公共団体自らが脆弱性診断を実施できるようセルフ診断ツールを提供した。また、地方公共団体が訓練ツールを用いた緊急時対応訓練を実施、訓練のコーディネーターを派遣した。これにより訓練の企画段階から実施までを支援し、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） 13 地域、152 団体が参加 ・自治体 CSIRT 協議会の運営を支援し、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） 技術講習会：49 団体 ブラインド方式によるインシデント対応訓練：37 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、地方公共団体のセキュリティ強化対策を推進するため、情報システムの強靭性の向上や自治体情報セキュリティクラウドの状況に係るフォローアップを実施するとともに、関係機関と協力の上、地方公共団体のセキュリティ確保に資するため、引き続き、「自治体情報セキュリティ向上プラットフォーム」を活用し、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ていく。さらに、情報連携に利用する情報提供ネットワークシステムについて、インターネットと分離する、セキュリティ分析・早期インシデント検知を行う等の対策を講じており、引き続き高いセキュリティ確保をすべく、適切な管理・監督・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］ ・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：664 団体 ・総務省が設置・管理する情報提供ネットワークシステムについては、ログ情報等統合分析・監査機能を用いてセキュリティ分析・早期インシデント検知を行う等のセキュリティ対策を講じた上で、適切な管理を実施しており、2019 年度においても、セキュリティインシデントは生じていない。 ［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行った上で、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、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、開催場所については従来は県庁所在地での開催を原則としていたところ、参加実績を踏まえた変更・追加を行うとともに、同一地域での開催日を分散化するとした工夫を行った上で、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、2019 年度は、地方公共団体から 1,815 人が受講した。
（キ）	内閣官房 内閣府	内閣府において、2017 年 11 月に本格運用を開始したマイナポータルを活用し、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。	・2019 年 11 月から自己情報取得 API の公開によるデータ連携を開始した。あわせて、民間事業者等が自己情報取得 API を利用する場合に必要な事項を定めた訓令を整備した。
（ク）	厚生労働省	厚生労働省において、マイナンバーカードの健康保険証としての活用について、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案を踏まえ、2020 年度の導入を目指して必要な準備を進めていく。	・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、システム構築を進めている。

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	2019 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、次期統一基準群改定に係るコンセプトについて検討を行う。	・内閣官房において、エンドポイントにおける不正プログラムの挙動等の検知、IT 資産管理の自動化等による効率的な情報収集及びデータ保護等の対策の導入状況について、政府機関等を対象とした調査を行い、統一基準群改定に向けた検討を行った。また、各府省庁のセキュリティポリシー策定支援を行うとともに、2018 年度統一基準群改定後の動向を踏まえ、次期統一基準群改定に向けて、改定コンセプトの検討を行った。
（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の動向、政府機関等における情報システムの調達状況を踏まえた対策内容の見直しを行う。	・内閣官房において、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」の改定に向け、有識者等との意見交換を通して、盛り込むべき対策内容の検討を行った。なお、当該マニュアルについては、統一基準の改定（2018 年７月）及びデジタル・ガバメント推進標準ガイドラインの改定（2019 年２月）に伴う所要の反映作業も行った（2020 年９月公開）。
（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、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。	・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。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、政府機関や自治体から要望のあった入退管理システムについて、2018 年度事業である「入退管理システムにおける情報セキュリティ要件に関する調査」を基に、調達者がセキュリティ要件を調達仕様書に指定する際、あるいは供給者が自己チェックを行う際に参照できる「入退管理システムにおける情報セキュリティ対策要件チェックリスト」を策定し公開。 ・IPA において、JISEC の主要な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、そこで要望のあったプロテクション・プロファイルでの乱数生成や通信路におけるテストについての補足を「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。	・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 15 件発行した（その他、申請受付中３件）。 ・暗号技術や規格化の動向を踏まえ、JCMVP 技術審議委員会及び暗号アルゴリズム実装試験要件 WG 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、２つの試験機関の審査を実施した。
（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。	・情報セキュリティインシデントの未然防止のための主な取組として、IPA が運用している独立行政法人等に対する不正な通信の監視体制と連携しつつ、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。
（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公開された脆弱性等への対応やサイバー攻撃に係る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併せて、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、府省庁及び独法等を対象とした監査において指摘が多かった管理者アカウントの管理状況の調査を実施した。また、2018 年度の統一基準群にて記載が追加された「IT 資産管理ソフトウェア」「デジタル著作権技術」「未知の不正プログラム対策ソフトウェア」について、導入状況の調査を実施した。なお、統一基準の適用範囲の変更に伴い、府省庁に加え、独法等も調査対象とした。
（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、府省庁、独立行政法人及び指定法人に対して、標的型攻撃に対する多重防御の取組を推進し、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、大規模サイバー攻撃や大規模災害発生時における、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、前年度の調査結果に基づいた具体的施策を検討し、実施する。	・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、前年度の調査結果に基づき「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案を 2019 年度に作成した。
（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。	・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、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に暗号技術検討会を開催した。 ・量子コンピュータ時代を見据え、2023 年に改定予定の次期 CRYPTREC 暗号リストの在り方を検討するタスクフォースを新設し、３回会合を開催した。 ・NICT 及び IPA を中心に暗号技術評価委員会及び暗号技術活用委員会を開催し、量子コンピュータが共通鍵暗号の安全性に及ぼす影響についての調査報告、及び暗号鍵管理システム設計指針（基本編）と TLS 暗号設定ガイドラインの作成を行った。 ・CRYPTREC シンポジウム 2019 を開催し、CRYPTREC 成果の対外アピールを実施した。
（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、監査等を通じて、当該法人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、当該法人が実施する監査について、内閣官房と連携し、必要な助言を行った。
（ス）	内閣官房	内閣官房において、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。	・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」に基づき、2020 年３月までに、各府省庁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 1,952 件の助言を行い、その内 83 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、2020 年東京オリンピック・パラリンピック競技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、今後の技術動向等を踏まえつつ、GSOC システムの検知・解析機能を始めとした機能強化の検討や、政府機関等と GSOC システムにおけるより効果的かつ効率的な連携の実現に向けた検討を行った。

(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	2019 年度　年次計画	取組の成果、進捗状況
（ア）	内閣官房 総務省	政府機関のクラウド化を推進する観点から、以下の取組を行う。 ・内閣官房において、引き続き、政府機関におけるクラウドサービスの利用状況を適宜調査し、課題等の把握に努める。 ・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 リソースの柔軟性やコスト低減等を目的として、新たな政府のプライベート・クラウドとしての第二期政府共通プラットフォームの整備に向けた作業を推進する。	[NISC] ・内閣官房において、政府機関におけるクラウドサービスの利用状況に関して、状況の把握を行い、安全なクラウドサービスの利用を促進する方策の検討に活用した。 [総務省] ・政府共通プラットフォーム第二期整備計画に基づき、新たな政府のプライベート・クラウドとしての第二期政府共通プラットフォームの 2020 年度中の運用開始に向けて設計・開発を進めている。
（イ）	総務省 経済産業省	総務省及び経済産業省において、官民双方が一層安心・安全にクラウドサービスを採用し、継続的に利用していくため「クラウドサービスの安全性評価に関する検討会」について、2020 年秋の全政府機関等での安全性評価制度の利用開始に向け、2019 年度中に制度の実証ととりまとめを行う。	・「クラウドサービスの安全性評価に関する検討会」の議論の過程において、制度の実現可能性に関する実証を行うとともに、当該実証の結果も踏まえたとりまとめを行った。 ・サイバーセキュリティ戦略本部第 23 回会合において、「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の基本的枠組みについて」の決定を行った。
（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、次期 GSOC システムの構築に向けた検討を進めた。

(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	2019 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、2018 年度において作成した調査内容に基づき業務利用の可能性等に関する検討を行う。	・内閣官房において、サイバー攻撃に対する高い耐性の点で有望視される複数の技術について、最新の状況を調査し、政府機関等における利用可否の検討を行った。

(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	2019 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、2019 年度は、11 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、2018 年度に実施した被監査主体への監査結果について、ヒアリング等により改善状況のフォローアップを行った。さらに、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、自衛隊が有する知識・経験を活用しつつ、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、侵入検査を実施した国の行政機関については、フォローアップを実施する。	・内閣官房において、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、自衛隊が有する知識・経験を活用しつつ、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、2018 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ったものを対象として、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、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、2019 年度までに全ての独立行政法人等（以下「被監査主体」という。）への監査を実施した。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、2018 年度に実施した被監査主体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。
（エ）	内閣官房	内閣官房において、独立行政法人等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、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、IPA との連携等により引き続き実施し、問題点の改善に向けた助言等を行う。侵入検査を実施した法人については、フォローアップを実施する。また、独立行政法人等における情報セキュリティ対策の実施状況を明らかにし、その結果を踏まえ、所管する府省庁と協力しセキュリティ対策の強化を図る。	・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、2019 年度までに全ての独立行政法人等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、2018 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	2019 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をより適切に実施するため、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引き続き取り組むとともに、民間事業者の知見を活用するための方策を講じる。	・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、各府省庁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の更なる活性化を図る。	・内閣官房において、府省庁における CSIRT 要員を対象としたコミュニティを運営した。また、独法等を対象としたコミュニティの立ち上げに向けた試行会合を開催した。今年度は、自組織の CSIRT をよりよくするにはどうしたら良いかを題材とし、専門家を交えた講義及びグループワークを実施した。また府省庁 CSIRT が警戒すべきサイバー犯罪について学ぶなどにより実践的な取組を実施し、府省庁の CSIRT 体制の強化やインシデント対処能力の向上を支援した。
（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等を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の合同研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。	・内閣官房において、政府機関や独法・指定法人等の職員向けに、2018 年度版統一基準の改定ポイントや情報セキュリティ監査、府省庁・独法等マネジメント監査・ペネトレーションテストの実施結果の分析から得られた課題の傾向と対策等をテーマとした NISC 勉強会を開催した。 ・内閣官房において、2020 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	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、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。2019 年度は、訓練成果の実感を高めるため、最新事例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年間を通じて実施した。
	内閣官房	内閣官房において、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、情報セキュリティ緊急支援チーム（CYMAT）要員等に対する研修と実習等を実施するとともに、CYMAT における対処能力の向上に関する情報収集に取り組む。	・内閣官房において、サイバー攻撃等の発生時における対処能力の向上を図るため、インシデント発生時の対応等について、情報セキュリティ緊急支援チーム(CYMAT)要員等に対して、技術的事項の習得に重点を置いた研修を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た。

	内閣官房	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。	・政府関係機関のサイバー攻撃対処能力の向上を目的として、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「NISC-CTF」を開催した。
	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、国の行政機関におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。	・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、国の行政機関や独立行政法人等におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施し、2019 年度は、国の行政機関や独立行政法人等から 955 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	2019 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、大学等の多様性を踏まえ、大学等が自律的かつ組織的に取り組むべきサイバーセキュリティ対策について検討を行い、大学等の取組を促進するとともに、当該対策の推進に資するガイドライン等について検討する。また、国立情報学研究所（NII）において、政府統一基準に準拠したセキュリティポリシーおよびそのためのセキュリティ対策を実現するため、「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」を改訂する。	・文部科学省において、大学等の多様性を踏まえ、大学等だが自律的かつ組織的に取り組むべきサイバーセキュリティ対策について検討を行い、大学等の取り組みを促進するため、大学等に対し「サイバーセキュリティ対策等基本計画」の策定を求めた。 ・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」を改訂・公開し、政府統一基準群への準拠性を高めるための構成見直しやクラウドサービス上で要機密情報を扱う場合についての解説を追加した。
（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・演習を実施する。	・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・演習として CISO マネジメント研修・戦略マネジメント層研修・CSIRT 研修（基礎・応用・実践編）・監査担当者研修を、年間で延べ合計 800 人程度に対し実施した。
（ウ）	文部科学省	文部科学省において、外部のセキュリティ機関等と連携し、大学等で発生した事案の初動対応や対処後の事案検証等において必要な支援を行う体制の整備を引き続き進める。	・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）を整備し、外部のセキュリティ機関等と連携し、大学等で発生した事案の初動対応や対処後の事案検証等において必要な支援を行う体制の整備を整備した。

(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	2019 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に、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。	・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実施した。また、インシデント発生時の危機管理機能向上に向けた契機とするため、国立大学法人等の CISO や 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２回実施した。このうち１回は、情報通信技術に関して大学等が連携・協働する「大学 ICT 推進協議会」と連携し、同協議会 2019 年度年次大会において公開型として実施することで、より幅広い大学等のサイバーセキュリティ担当者も受講可能とした。
（イ）	文部科学省	国立情報学研究所（NII）において、サイバー攻撃耐性を向上させるため、国立大学法人等において、M2M を含み学術評価に適したデータを実環境から継続的に収集、匿名処理し、研究データを作成、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、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）で検知、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を生成するシステムを開発し、データ解析技術の開発に向けた取組を進めた。
（ウ）	文部科学省	文部科学省において、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	2019 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し、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。 ・「対処態勢の整備・運用」については、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・訓練等を実施するとともに、G20（金融・世界経済に関する首脳会合）、ラグビーワールドカップ 2019 等において、サイバーセキュリティ対処調整センター及び情報共有システムを運用し、運用態勢の確認、改善を実施する。	・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。 ・リスクマネジメントの促進については、重要サービス事業者等を対象とする第５回目のリスクアセスメントの実施を依頼、提出された実施結果について横断的に分析し各事業者等にフィードバックを実施した。また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況を NISC が検証する横断的リスク評価の第２、３回目を実施した。第２回以降の取組においては、重要サービス事業者等（競技会場（レガシー部分）を含む。）を対象に検証（実地又は書面）した。なお、競技会場のオーバーレイ部分の対策の整備状況及び監督状況については、組織委を対象に検証を行った。 ・対処態勢の整備については、サイバーセキュリティ対処調整センターを 2019 年４月に設置し、恒常的に情報共有システムを使用した関係組織・機関への迅速な情報提供を実施したほか、大会までの大規模イベントである 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は、ラグビーワールドカップ組織委員会、会合の現地事務局等に連絡要員を派遣し、大会の対処態勢と同等の態勢で運用するとともに、情報共有及びインシデント発生時の対処に係る訓練・演習を実施し多くの運用経験と教訓を得た。これらの運用経験と教訓をもとに、情報共有・事案発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して、対応手順等について改善を実施した。また、サイバー脅威情報の提供について５社から協力を受けることを決定した。
（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 2020 年東京オリンピック・パラリンピック競技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。

(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	2019 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、2020 年東京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あたっての課題について検討を実施する。	・東京 2020 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の検討を進めている。
（イ）	警察庁 法務省	警察庁及び都道府県警察において、2020 年東京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する。また、法務省（公安調査庁）において、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、2020 年東京オリンピック・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、更なる内容の充実と受講機会の拡大を図りつつ実施する。	・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 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」を実施し、2019 年度は延べ 193 人が受講した。

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	2019 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・強化していくと共に、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参加組織の拡大、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。 ・2019 年度は新たに 3 組織が参加し、15 業界 262 組織の体制で運用。2,303 件の情報提供を受け、225 件の情報共有を実施。 ・STIX/TAXII による脅威情報の表現形式について、調査・検討を実施。

（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 連携ワークショップを開催し、日米の情報通信分野 ISAC 組織間における情報共有・連携に係る覚書を締結した。
（エ）	国土交通省	国土交通省において、重要インフラ事業者（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」（仮称）について、事業者の情報共有を支援するとともに、事業者が参加する検討会を開催し、2020 年度の本格運用に向けて、運営形態等を検討・議論する。	・国土交通省において、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」の運営形態等について事業者による検討・議論の支援を行った。また、2019 年 11 月に、事業者有志による一般社団法人交通 ISAC 設立準備委員会が設置されたことから、2020 年４月に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。
（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３月現在、「金融 ISAC」の加盟社は 386 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。	・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、医療分野のサイバーセキュリティ対策について国内外の事例の調査や有識者による意見交換会を実施し、情報共有のあり方等について検討を行った。
（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。	・2019 年 12 月に開催したクレジットセプター運営会議において、クレジットカード会社、決済代行会社に対して、JPCERT/CC を通じたサイバー攻撃等に関する情報提供、意見交換を行った。
（ク）	経済産業省	経済産業省において、2019 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」（情報共有機関）に対して、サプライヤー等の一部参加を実現。2020 年４月現在、「J-Auto-ISAC」の加盟社は 14 社まで増加。
（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、40 件の「早期警戒情報」を発行した（2020 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 14,586 件：2020 年３月末現在）。また制御システムの関係者向けに 11 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、32 件のニュースクリップなどの情報発信を行った。（全て 2020 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。	・JC3 と連携し、急増した不正送金事犯や改ざんされた EC サイトに係る注意喚起を実施したほか、捜査の過程で把握したリスト型攻撃ツールを JC3 と分析、広報するなどして、被害防止対策を実施した。

(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	2019 年度　年次計画	取組の成果、進捗状況
（ア）	内閣官房	2019 年４月に組織されたサイバーセキュリティ協議会について、そ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、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、2019 年４月、９月と第１期及び第２期の協議会構成員の募集を行い、官民又は業界を超えた、全 155 者の多様な主体に参加していただいている。 なお、2020 年３月に第３期構成員の募集を行ったところである。

(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	2019 年度　年次計画	取組の成果、進捗状況
（ア）	内閣官房	2019 年４月に組織されたサイバーセキュリティ協議会において、国も率先して自ら保有する情報を適切に提供していく。加えて、協議会の実際の運用の経験や各主体の意見を丁寧に踏まえ、必要に応じて運用ルールやシステムを不断に見直しつつ、例えばリコールの要因となる情報等、国民の生命・身体を保護するため不可欠な情報を含め、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始めている。2020 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 46 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 13 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	2019 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、2020 年東京大会を見据え、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。	・2019 年度においても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、2020 年度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。	・2018 年度に実施した訓練の結果を踏まえて、大規模なサイバー攻撃発生時における初動対処のための環境整備等必要な措置をした。また、あらゆる機会を通じて、初動対処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する。 ・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、産業制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果を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、40 件の「早期警戒情報」を発行した（2020 年３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 14,586 件：2020 年３月末現在）。また制御システムの関係者向けに 11 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、32 件のニュースクリップなどの情報発信を行った。（全て 2020 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、我が国経済社会に被害をもたらすおそれが強く、一組織で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。	・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 139 件行うとともに、うち 20 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、個人情報等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。	・2019 年度においては、前年度に引き続き、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や、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、個人情報の適正な取扱いを確保する観点から、事業者や国民に対し、委員会ウェブサイトを通じて情報発信を行った。

（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 設立や組織内 CSIRT 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。	・経済産業省において、日本シーサート協議会の運営委員及び事務局業務を通じ、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。同協議会の加盟組織数は 2019 年３月末時点では 351 組織であったが、2020 年３月末現在で 355 組織となり、サイバーセキュリティにかかる緊急時及び平常時の相互連携が可能な国内組織が増えた。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、2020 年東京大会の開催を控え、大規模インシデント等の発生に備え、官民が一体となった危機管理態勢の構築に取り組む。	・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	2019 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、2019 年度は G20 が日本で開催されるところ、開催国として、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。	・2019 年６月に開催された G20 大阪サミットで、安倍総理は、発展著しいデジタル化に際して、DFFT（信頼ある自由なデータ流通）の考え方を提示したところ、各首脳からは、デジタル経済の国際的なルール作りの重要性について発言があったほか、DFFT の考え方が参加者間で共有された。 ・2019 年８月に開催された G7 ビアリッツ・サミットで、G7、豪州、チリ、インド及び南アフリカ共和国の首脳は OECD 事務総長とともに、「開かれた自由で安全なデジタル化による変革のためのビアリッツ戦略」に合意し、データ等の越境流通がプライバシー、データ保護、知的財産権及びセキュリティ等の諸課題を提起する一方で DFFT はデジタル化による変革の機会を生かすものであることが表明された。

(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	2019 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。安倍首相が 2019 年１月に出席した世界経済フォーラム年次総会（ダボス会議）において、「DFFT（信頼ある自由なデータ流通）のための体制を作り上げる」と述べたことを踏まえ、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、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。 ・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。	・経済産業省及び外務省において、 ・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 のサービス貿易理事会、TBT 委員会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。 ・上記のような国内規制により、我が国企業を含む外国企業の活動に悪影響が及ばないよう、対象国当局との協議、有志国等との情報交換を行った。 ・また、中国、ベトナム等に対し、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った。

(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	2019 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。昨年の国連総会決議に基づき、国連サイバー政府専門家会合（UNGGE）第６会期及び OEWG（Open-ended Working Group）が立ち上がる予定であるところ、責任ある国家の行動規範に係る議論について、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、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。 ・2019 年、国連政府専門家会合（UNGGE）においても、メンバー国として議論に積極的に貢献。同じく、新たに設置された国連オープンエンド作業部会（OEWG）等、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、我が国の立場を積極的に発信。国際的なルール及び規範作りに積極的に関与している。

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
・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	2019 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、刑事共助条約を締結済みのアメリカ合衆国との間で中央当局間実務者協議を実施し、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、我が国のサイバー犯罪情勢に関係の深い国々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、ICPO 等の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 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合（2019 年 10 月）、ASEAN+3 サイバー犯罪会議（2019 年７月）等に参加し、外国捜査機関職員との情報交換を積極的に推進するとともに、協力関係の醸成に努めた。 ・外国捜査機関等との連携強化を目的として、サイバー犯罪に係るリエゾンを派遣した。 ・サイバー犯罪捜査において、外国捜査機関からの協力を得る必要がある場合には、刑事共助条約（協定）や ICPO、サイバー犯罪に関する 24 時間コンタクトポイント(2019 年６月現在、86 の国及び地域が参加）等の枠組みを活用し、外国捜査機関に対して積極的に国際捜査を推進した。

（エ）	外務省	外務省において、我が国が 2012 年７月にサイバー犯罪に関する条約を締結し、同年 11 月から我が国について同条約の効力が生じたことを受け、引き続き、アジアで最初の同条約締約国として、アジア地域への能力構築支援等を通じて同条約の普遍化に取り組む。	・2019 年 11 月に仏ストラスブールで開催されたサイバー犯罪に関する条約の普遍化や能力構築に関する会合であるオクトパス会合に参加し、サイバー犯罪に関する条約の有効性を発信するとともに、アジアの同条約未締約国を招いたイベントを実施し、同条約の活用や締結に向けた隘路について議論を行うなどして、同条約締結に向けた働きかけを行った。

3.2　我が国の防御力・抑止力・状況把握力の強化

(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	2019 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への個別訪問を行い、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、重要インフラ事業者等への個別訪問、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。
（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）を実施していく。	・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、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を実施するとともに試作品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において設計を実施する。	・防衛省において、移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究試作において設計を実施した。

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	2019 年度　年次計画	取組の成果、進捗状況
（キ）	防衛省	防衛省において、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・リスク及びその対策について、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。	・サプライチェーン・リスクに係る調査研究を通じて、最新の情報を入手・分析を実施した。
（ク）	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対して、SINET に設置した検知システム等を用いて警報分析及び各連携機関への通知を行う NII-SOCS の運用など、サイバー攻撃による情報の漏えいを防止するための取組を促すとともに、支援する。	［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。
（ケ）	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、米国の新たな基準と同程度まで強化する改正を行うべく、官民間での議論を行いながら検討を進める。	・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、米国の新たな基準と同程度まで強化する改正を行うべく、官民間での議論を行いつつ情報セキュリティ基準改正案の検討を実施した。

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			
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	2019 年度　年次計画	取組の成果、進捗状況
（コ）	内閣官房	内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。	・内閣情報官の下に、サイバー問題やテロ問題等について関係省庁が収集した情報等を集約し、それらを基にして総合的な分析を行い、その分析結果等は、関係省庁や官邸要路に適時適切に報告された。 ・サイバー空間上のテロに関する情報の集約体制の強化のため、２名増員。

（サ）	警察庁 法務省	警察庁および法務省（公安調査庁）において、サイバー空間におけるテロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする態勢を拡充し、人的情報やオープンソースの情報を幅広く収集する等により、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の活動への対策について、国際社会との連携を推進する。	［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、サイバー空間における公然情報のモニタリング調査に対する取組を通じ、過激思想の伝播活動を含む国際テロ組織等の動向の把握・分析を強化した。また、サイバー空間上における国際テロ組織等の動向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。

(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	2019 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	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。	・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、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。また、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。	・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	2019 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、相互の理解をさらに深めている。 ・特に ARF の枠組みでは、2018 年、サイバーセキュリティに関する会期間会合の立上げ以降、信頼醸成に関する議論を積み重ね、我が国提案によるものも含め複数の信頼醸成措置に関する提案について合意し、具体的な取組を着実に推進してきている。直近では、2020 年１月、第５回目となる専門家会合を開催した。
（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 25 の経済地域の 29 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(2020 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、APCERT が主催する APCERT Drill、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。 ・TSUBAME ワーキンググループへの参加継続意志の確認を通じて、各国との TSUBAME の活用したインシデント対応について参加メンバーに理解を求めた。

(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	2019 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。 ・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実施する。	［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。（再掲） ・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する。（再掲） ・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、産業制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果をもとに対処の任につく警察職員へ教養を実施した。 ・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、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。また、より高度な観測能力を実現するためにシステムの刷新を図る。	・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。	・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、防衛省の展示ブースへの来訪者に対し、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。
（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	2019 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。	・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・分析を実施し、随時、その結果を関係機関に提供した。
（コ）	内閣官房	内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。	・政府内の脅威情報共有・連携体制の強化を推進しているところ。
（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、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強化を推進するなど協力関係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。FIRST 会合に参加し、サイバー攻撃手法等に関する情報交換等国際的な連携を推進した [法務省] ・法務省（公安調査庁）において、諸外国関係機関との情報交換を強化するなどして、サイバー攻撃に関する情報収集・分析を継続的に実施した。

3.3　国際協力・連携

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	2019 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、ICSJWG、RSA カンファレンス、Black Hat 等の会議に参加し、各国政府、ベンダー、その他のステークホルダーの知見・技術動向、サイバー環境の潮流に関する情報に接する機会を積極的に設け、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	2019 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。	［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、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、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。 ［総務省］ ・日本及び ASEAN の ISP 間の情報共有を促進する「第 10 回 ISP 向け日 ASEAN 情報セキュリティワークショップ（2019 年 12 月、タイ）を開催し、日 ASEAN の ISP の取組の共有及びさらなる連携方策の議論を行うとともに、合同サイバー攻撃演習を実施した。
（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推進していく。	・防衛省において、ADMM プラス EWG(2019 年５月、８月)への参加やベトナムに対するサイバーセキュリティに関する能力構築支援事業（2020 年１月）の実施を通じ、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）の更なる定着を図るため、2019 年８月にフィリピンにおいて責任者会議を開催し、今後の展開等について討議を行った。また、2020 年２月には、ITPEC 試験合格者で特に優秀な者として選出したアジアトップガン人材を日本に招き、日本の IT 企業との交流などを行うとともに、独立行政法人情報処理推進機構（IPA）が参加者を帰国後に試験の普及活動を行う人材として、ITPEC アンバサダーに任命した。加えて、フィリピン、ベトナムにおいて、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、昨年策定された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７回日米サイバー対話を開催し、日米両国の政府横断的な取組の必要性を踏まえ、前回日米サイバー対話等のフォローアップを行うとともに、日米双方の関係者が、情勢認識、両国におけるサイバー政策、国際場裡における協力、能力構築支援等、サイバーに関する日米協力について幅広く議論を行った。

（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。	・「第４回日米 ISAC 国際連携ワークショップ」及び「サイバーセキュリティ国際シンポジウム」（2019 年 11 月、東京）を開催した。米国より DHS（国土安全保障省）、National Council of ISACs、Comm-ISAC 及び IT-ISAC が参加し、ICT-ISAC をはじめとする日本国内の ISAC 関係団体との間で脅威情報の共有等に関する意見交換・議論を行うとともに、ICT-ISAC と IT-ISAC がサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的に、覚書を締結した。
（カ）	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や技術共有等に取組む。	・2019 年 12 月に英国立サイバーセキュリティセンター（NCSC）を訪問し、中小企業へのセキュリティ対策の普及啓発状況や、産業サイバーセキュリティ(OT セキュリティ)分野の人材育成の取組に関する意見交換を実施した。
（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深化させていく。	・防衛省において、日米２+２（2019 年４月）や、日米 CDPWG 第７回会合（2019 年 10 月）を含め、各種レベルで米国と協議を実施、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、昨年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、欧州各国との連携を強化する。 ・防衛省において、日英防衛当局間サイバー協議、日 NATO サイバー防衛スタッフトークスや NATO 主催の演習への参加等を通じ、欧州各国とのサイバー防衛協力を引き続き推進していく。	［NISC、外務省］ ・第４回日 EU サイバー対話（2019 年６月ブリュッセル）、第５回日仏サイバー協議（2019 年７月レンヌ）、日中韓サイバー協議（2019 年 11 月北京）、日露サイバー協議（2019 年 11 月東京）、第２回日ウクライナサイバー協議（2020 年１月東京）、第５回日英サイバー協議（2020 年１月東京）等を開催し、サイバーセキュリティに関する政策や国内動向に係る意見交換を行った。 ［防衛省］ ・防衛省において、2019 年３月より NATO サイバー防衛協力センター(CCDCOE)に防衛省職員を派遣している他、日 NATO サイバー防衛スタッフトークスの開催、NATO サイバー防衛演習への参加等を通じ、欧州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。	・Meridian 会合、FIRST 等に参加し、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、国際強調・協力の推進に努めた。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、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、サイバー攻撃手法等に関する情報交換等国際的な連携を推進した。

（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、 ・JIWG プレナリ会合に１回参加し、2019 年度の活動報告と 2020 年度の活動計画を協議した。また、JHAS 会合に６回、JEDS/JTEMS 会合に１回参加するとともに、同時期に開催される各種会合等に参加して、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。特に、EU Cybersecurity Act 施行に伴う認証制度改革の情報収集に努めた。 ・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、脅威認識の共有などを通じて、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	2019 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。 ・有志国を分野横断的演習に招へいし、我が国の重要インフラ防護に向けた具体的取組に関する理解促進を図るとともに、国際演習ワークショップを実施し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、サイバーグリーン)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、国内３組織、海外 12 組織にデータ提供を行い、対策の検討を促した。また、2019 年にシンガポールで開催した APCERT 年次会合にて Mejiro データ分析について講演を行い、活動の周知を図った。
（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、アフリカ地域を中心に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 運用規約の見直しを行い、12 か月以上にわたりセンサの稼働が停止している、あるいは再稼働の意思が確認できない組織については、メンバ組織から除名することを規定し、より TSUBAME ワーキンググループを実効性の伴った情報共有体へと活動の改善を行った。

（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。 ・インドネシアで開催した FIRST TC を通じて約 40 名の技術者を対象に Active Directory ログ分析ハンズオンを実施した。 ・ウガンダでの約 20 名の技術者を対象にした制御セキュリティに関するトレーニングを実施した。

(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	2019 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、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を通じて、ASEAN 加盟国のサイバー犯罪対策能力構築支援を行う。その他国際機関などと連携したプロジェクトについても検討する。	[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、日英共催 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を行った。 ・日・ASEAN サイバーセキュリティ政策会議人材育成 WG を継続して開催し、日・ASEAN におけるサイバーセキュリティ人材の育成の方策の議論を進めた。 ・2019 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] ・2019 年 11 月、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て、JICA 国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）を実施した。 ・2020 年１～２月、警察庁と JICA の連携の下、海外 13 か国の捜査機関等からサイバー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）を実施した。 [総務省] ・「日 ASEAN サイバーセキュリティ能力構築センター」を 2018 年９月にタイ・バンコクに設立し、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護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。 ・APT 加盟国を対象とした研修（2020 年２月、東京）及び APT 幹部ワークショップ（2020 年２月、東京）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うとともに、意見交換等を実施した。 [外務省] ・JICA 事業を通じた支援として、2019 年にインドネシア「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」を開始し、2020 年１月までに延べ 100 名以上の人材育成に協力。また、日本国内での研修として「ASEAN 地域のサイバーセキュリティ対策強化のための国際法・政策能力向上」（９か国 17 名）やベトナム向け「サイバーセキュリティ及びサイバー犯罪対処能力強化」（10 名）を受け入れるなど、ASEAN を中心として能力構築支援を展開。 ・このほか、JICA による研修事業「サイバー犯罪対処能力向上」（13 か国 13 名）、「ICT 実践力強化のためのコア人材育成（C）情報セキュリティコース」（４か国 10 名）の受入等を通じ、内閣官房、警察庁、総務省、経済産業省をはじめとする関係府省庁・機関との密接な連携の下、積極的に途上国の能力構築に協力。 ・日 ASEAN 統合基金（JAIF）を活用した「ASEAN サイバー能力向上プロジェクト」について実施期間終了後もフェーズ２として継続して実施することとしたほか、UNODC が 2019 年度に実施した東南アジアにおけるダークウェブの調査等に関するプロジェクトへの拠出を行った。第４回日・ASEAN サイバー犯罪対策対話は 2020 年度に実施予定。

（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）が米国政府と協力し、ASEAN をはじめとしたアジア太平洋地域の国々に対する産業サイバーセキュリティの共同演習実施等を通じた能力構築支援を行う。	・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）は、日米の官民の専門家と協力し、2019 年９月９～12 日に ICSCoE 中核人材育成プログラム受講生 69 名及びインド太平洋地域の 14 の国・地域（ブルネイ、カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、シンガポール、タイ、ベトナム、インド、バングラデシュ、スリランカ、ニュージーランド、台湾）からの参加者 35 名へ、制御システムのサイバーセキュリティに関する講演及び演習を実施した。

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	2019 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、必要に応じてフォローアップや見直しを図る。（再掲）	・普及啓発・人材育成専門調査会において、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うとともに、施策間の連携を促進した。
（イ）	内閣官房	内閣官房において、関係機関と連携し、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、対象となる層や伝達手法の見える化及び連携を推進するための検討を行う。	・関係機関の協力のもと、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、仮運用を開始した。
（ウ）	総務省	総務省において、地域におけるサイバーセキュリティ人材育成のエコシステムの構築に向け、地域の中小企業や自治体のサイバーセキュリティに関する意識向上や取組を促進するための研修等を行う。	・総務省において、地域におけるサイバーセキュリティ人材育成の育成のため、地域のコミュニティや企業、教育機関等と連携して新たなスキームによる人材育成の方策を実証するためのモデル事業（①地域のセキュリティリーダーの育成、②地域でのセキュリティ人材のシェアリング、③地域でのセキュリティ人材のシェアリング）を実施した。

(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	2019 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 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２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実施し、対策強化に繋げる。 ・2018 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、必要に応じてカリキュラム等を見直した上で、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 2019 年秋から開始する。	・これまでの２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。 ・2018 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等を踏まえ、「セキュリティ組織管理」コースと「セキュリティ実務管理」コースの２つのコースに分け、2020 年２月に実施した。
（イ）	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ため、教える側の質的向上・量的拡充のため、「学」の教員向けに IPA、JPCERT/CC により、FD（Faculty Development）等の研修機会の提供を実施していく。	・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 により、FD（Faculty Development）等の研修機会の提供を実施。
（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、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。
（エ）	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、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普及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、2018 年度に検討したモデルカリキュラムの活用等に関する今後の取組の方向性について議論を行った。

(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	2019 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、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った上で、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、2019 年度は全国 47 都道府県において計 3,090 人が受講した。
（エ）	文部科学省	文部科学省において、高等専門学校における情報セキュリティ教育の強化のため、企業等のニーズを踏まえた技術者のセキュリティ教育に必要な教材・教育プログラム開発等に必要な予算を確保し、（独）国立高等専門学校機構において、教育プログラムの開発等を進める。2016 年より、段階的に整備を進めてきた情報セキュリティ教育の演習拠点（10 拠点）について、日々進歩しているサイバー攻撃技術に対応するための定期的な環境更新（アップデート）を図るとともに、「情報セキュリティ人材」の発掘・育成を実行する。	・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。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。2020 年度予算においても（独）国立高等専門学校機構運営費交付金に情報セキュリティ人材育成に係る予算を計上。教育プログラムの開発について、引き続き実践・検証を進める。
（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。（30 コース・受講者数 443 人） ・一般教育訓練給付の対象に、サイバーセキュリティに関する内容を含む情報関係分野の教育訓練を指定した。（2019 年 10 月 1 日時点の情報関係の指定講座数 330 講座） ・速やかな再就職及び早期のキャリア形成に資する教育訓練を対象とした特定一般教育訓練給付を創設。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。（2019 年 10 月 1 日時点の情報関係の指定講座数３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。（2019 年 10 月 1 日時点の指定講座数 65 講座）
（カ）	経済産業省	経済産業省において、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。	・2019 年 10 月時点の情報処理安全確保支援士（登録セキスペ）は 19,417 人となった。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。また、登録セキスペ制度の信頼性を向上するため、第 200 回臨時国会において、登録の更新制導入などの法改正を行い 2019 年 12 月に公布された。
（キ）	経済産業省	経済産業省において、国家試験である情報処理技術者試験において、組織のセキュリティポリシーの運用等に必要となる知識を問う「情報セキュリティマネジメント試験」について、引き続き、IPA を通じて広報活動を実施する。	・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、独立行政法人情報処理推進機構を通じて広報活動を実施した。
（ク）	経済産業省	経済産業省において、情報セキュリティ人材を含めた高度 IT 人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について、周知及び普及を図る。	・年に２回（春・秋）実施している情報処理技術者試験（うち IT パスポート試験については毎月実施）の普及を図るべく、独立行政法人情報処理推進機構を通じて広報活動を実施した。また、IT パスポート試験については、2019 年４月からセキュリティの出題を強化した。

（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、 ・教育関係者等が児童・生徒・学生等に指導する際に使用可能な教材を７テーマ（SNS や情報セキュリティ等）22 種類とともに、指導するポイントをまとめた講義要領を作成、試行版を 2019 年 11 月 28 日に、正式版を 2020 年３月 30 日に公開し、10,963 ダウンロードされた（2020 年３月末）。 ・作成した教材を使用して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ーにむけ、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 47 都道府県で１回以上計 50 回開催し、3,426 名が参加した（2020 年３月末）。 ・「ホームユーザー向け安全教室」を全国 52 か所で開催し 5,434 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 33 回実施し 5,160 名が参加した（2020 年３月末）。

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	2019 年度　年次計画	取組の成果、進捗状況
（コ）	経済産業省	経済産業省において、IPA を通じ、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、2019 年８月 13 日～17 日にかけて「セキュリティ・キャンプ全国大会」を実施し 76 名が参加するとともに、2019 年より全国大会修了生（25 歳以下）の次のステップとして「セキュリティ・ネクストキャンプ」を新設し、６名が参加した。さらに、2019 年９月から 2019 年 12 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 10 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、2018 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	経済産業省において、若手情報セキュリティ人材の育成の観点から、NPO 日本ネットワークセキュリティ協会が実施する情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF」に対する後援等を通じて、普及・広報の支援を行う。	・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するとともに、2019 年 12 月 21 日～22 日に実施された「SECCON2019 決勝大会」国際大会において、最も優秀な成績を収めたチームを対象として経済産業大臣賞を付与した。
（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。 ・部外で開催される CTF に協賛し、防衛省のブースを展示し、来訪者との質疑等を実施した。
（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	2019 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）を抜本的に見直し、セキュリティ人材の専門分野を整理するとともに、各専門分野で情報処理安全確保支援士等が活躍するためのキャリアアップへの道筋を描く。	・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)の改訂案を作成。
（イ）	文部科学省	文部科学省において、新学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する。特に、各学校における指導の改善・充実に向けて、教科等横断的な情報活用能力の育成に係るカリキュラム・マネジメントの在り方等に関する実践的な研究を実施する。	・新学習指導要領の実施を見据え、「小・中・高等学校を通じた情報教育強化事業」において、教科等横断的な情報活用能力の育成に係るカリキュラム・マネジメントの在り方について、実践的な研究を実施し、成果を取りまとめた。
（ウ）	文部科学省	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、新学習指導要領の趣旨を踏まえ、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、2020 年１月 27 日～１月 31 日に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済。
（エ）	文部科学省	文部科学省において、最新のトラブルや被害の状況等を踏まえ、2018 年度に改善した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について、2020 年２月までに実施済。
（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５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、2019 年度は、45 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、参加大学数、連携企業を増加させる取組を推進することにより、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。なお、社会人を対象とした enPiT-Pro において外部有識者による中間評価を実施した。

（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、参加大学数、連携企業を増加させる取組を推進することにより、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。なお、社会人を対象とした enPiT-Pro において外部有識者による中間評価を実施した。

(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	2019 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、各府省庁が PDCA サイクルを更に充実させることにより、「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、体制の整備・人材の拡充、有為な人材の確保、一定の専門性を有する人材の育成や適切な処遇の確保を含む政府部内のセキュリティ人材の充実に係る諸施策をより一層推進する。また、内閣官房等の関係機関で連携し、「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等を踏まえ、今後のセキュリティ人材等の充実に向けた取組の方向性について検討を行う。	・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、2020 年東京オリンピック・パラリンピック競技大会の成功等に向けて、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。	［NISC］ ・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。 ［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」を実施し、2019 年度は延べ 193 人が受講した。
（ウ）	内閣官房 総務省	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、認定の手続規定の整備等を含め、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 2019 年度情報システム統一研修を実施（集合研修については、10 コース 37 回実施し、延べ 1,625 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 14,997 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	2019 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、研究・技術開発に資する産学官連携による体制構築の検討を含め、我が国のサイバーセキュリティの研究・技術開発に関する取組方針を取りまとめると共に、関係機関との連携の下、施策を推進する。	・2019 年5月に、「研究開発戦略専門調査会」において、「サイバーセキュリティ研究・技術開発取組方針」を取りまとめた。また、研究開発戦略専門調査会等を通じて、国際的な研究動向や産学官連携事例について分析を行うとともに、研究コミュニティとの議論を行った。

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	2019 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た取組を進める。（再掲）	・技術検証体制の整備に向け、技術検証に関する技術動向や諸外国の制度の状況について調査を実施した。
（イ）	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１期「重要インフラ等におけるサイバーセキュリティの確保」により、2020 年東京オリンピック・パラリンピック競技大会を支える重要インフラに導入して有効性を実証し、将来の国内インフラ産業の安定運用やインフラ輸出に貢献するための研究開発・社会実装を行う。本プロジェクトでは、制御・通信機器のセキュリティ確認技術、動作監視・解析技術等を開発する。プロジェクトの最終年度として、幅広い分野に横展開するための技術開発及び社会実装を進める。	・５年間のプロジェクトの最終年度として、運用性を拡張し構成変更に自動的に対応する等、重要インフラだけでは無く製造等の幅広い分野に横展開のために必要な技術開発を行った。 ・数千台レベルのサーバ機器に対応する改ざん検知技術や、物理・仮想混在の高速通信環境における動作監視技術の開発等、研究開発の技術的な目標を達成した。 ・改ざん検知技術や動作監視・解析技術等開発技術の商用サービス化及び通信事業者を始めとした重要インフラ事業者による実装を進めた。
（ウ）	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実証実験に向けた準備を着実に進める。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）	・５年間のプロジェクト活動の２年目として着実に推進し、基本方式の設計とデモシステムの開発を実施した。 ・2020 年度から予定している特定分野での実証実験の準備を着実に進めるとともに、グローバル連携や関係省庁連携を行い、社会実装に向けて取り組んだ。

（エ）	総務省	総務省において、IoT システムの基盤技術となる第５世代移動通信システム（５Ｇ）に係る各構成要素におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、対策の共有等を図る。	・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、ソフトウェアの検証に必要となる仮想環境の基本部分の構築及び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。
（オ）	総務省	総務省において、チップの設計回路の解析や各種システム／サービスの挙動や動作の観測を通じた悪性機能を検出する技術の研究開発を実施する。	・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開発を行った。
（カ）	総務省	総務省において、スマートシティのセキュリティ要件について、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て検討し、具体化を図る。	・スマートシティのセキュリティ要件について、国内外の実例調査やワーキンググループでの議論を実施。内閣府、国土交通省等と連携しスマートシティのアーキテクチャに対応したセキュリティの在り方について、ユースケースを交えて検討を行った。また、総務省においてセキュリティベンダーや業界団体と連携しスマートシティ官民連携プラットフォームにおいてスマートシティセキュリティ・セーフティ分科会を立ち上げ、2020 年１月よりスマートシティのセキュリティ・セーフティの実現に向けて議論を開始した。
（キ）	経済産業省	経済産業省において、日本のセキュリティニーズに応じた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。（再掲）	・経済産業省において、我が国発のサイバーセキュリティ製品・サービスの創出・活用を促進するため、有識者会議を開催し、製品の公募を実施し、選定された製品の検証項目を策定した。さらに、その検証項目に従って実施されたセキュリティ製品の検証結果を評価・公表することで、各製品の有効性評価の結果を公表するという施策のトライアルを実施した。 ・また、ユーザが導入した製品・サービスを、製品・サービス導入事例として安全に公表するための手引書として「試行導入・導入実績公表の手引き」を作成した。
（ク）	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に設置した 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、データそのものの信頼性確保や、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。（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・普及や、ビルシステムのセキュリティに関するガイドラインの第１版の公表を始め、各産業分野におけるセキュリティ対策の検討を引き続き推進した。また、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を立ち上げ、それぞれ検討を行った。
（ケ）	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。

（コ）	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取り組む。	・多種多様なものが接続される複雑なシステムで必要となる、柔軟なアクセス制御が可能な関数暗号などの暗号技術を提案した。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」作成において、ソフトウェア工学や情報セキュリティの観点からその完成に貢献した。
（サ）	経済産業省	経済産業省において、制御システムの挙動を解析し、サイバー攻撃を検知・予測する技術開発や、可用性を確保した脆弱性への対処技術に関して、期間および規模を拡大した監視・検知により、高度な攻撃意図を伴う潜伏的な脆弱性の検知・対処を実現するための研究を行う。	・経済産業省において、関係省庁と連携し SIP を通じて、制御システムの挙動を解析し、サイバー攻撃を検知・予測する技術開発や、可用性を確保した脆弱性への対処技術に関して、期間及び規模を拡大した監視・検知により、高度な攻撃意図を伴う潜伏的な脆弱性の検知・対処を実現するための研究を行った。

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			
・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	2019 年度　年次計画	取組の成果、進捗状況
（シ）	経済産業省	経済産業省において、日本のセキュリティニーズに応じた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。（再掲）	・経済産業省において、我が国発のサイバーセキュリティ製品・サービスの創出・活用を促進するため、有識者会議を開催し、製品の公募を実施し、選定された製品の検証項目を策定した。さらに、その検証項目に従って実施されたセキュリティ製品の検証結果を評価・公表することで、各製品の有効性評価の結果を公表するという施策のトライアルを実施した。 ・また、ユーザが導入した製品・サービスを、製品・サービス導入事例として安全に公表するための手引書として「試行導入・導入実績公表の手引き」を作成した。
（ス）	経済産業省	経済産業省において、本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審査登録制度のよりよい利用についての検討を行い、競争力強化やサイバーセキュリティの成長産業化に取り組む。（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。また、政府調達時や、税制優遇措置又は補助金給付を受ける際に、登録サービスの利用を推奨することで、制度の活用や普及の促進を行った。結果、2019 年度は、登録サービス件数を約 100 件から約 170 件まで増加させた。
（セ）	経済産業省	経済産業省において、IPA を通じ、サイバーセキュリティお助け隊の実証事業を全国で実施し、中小企業の実態や求めるサービス内容、レベル等を明らかにするとともに、中小企業のサイバーセキュリティ意識向上を図る。実証結果を基に、セキュリティベンダー、損害保険会社等連携し、中小企業が利用し易い、支援体制、サイバー保険について検討、構築し、普及を図る。（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８地域で実施し、約 1,000 社の中小企業が実証に参加した。実証により、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難な中小企業があり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、サービス購入費用が中小企業にとって許容可能な価格である必要があること等、中小企業の実態・ニーズが明らかになった。

（ソ）	経済産業省 総務省	・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。（再掲） ・経済産業省において、中小企業等の生産性向上に資する IT 導入等の促進とあわせて、セキュリティに係る意識向上やその対策に向けた具体的な取組を促す。 ・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、中小企業に対して、日本政策金融公庫による特別利率での融資も更に実施する。 ・総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、システムやセンサー・ロボット、セキュリティ対策製品等の導入に対する税制措置の活用を促し、事業者のセキュリティ対策の強化と生産性向上を同時に促進する。	・経済産業省において、 ・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 を 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。 ・中小企業の IT 活用を支援する IT ベンダー等をスマート SME サポーターとして認定し、中小企業向けに、特設サイトで「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」等の情報を開示する仕組みを構築した。 ・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 382 社の中小企業に対し実施した。 ・中小企業で対策が進んでいないネットワークセキュリティの更なる普及促進に向けて、財政投融資制度による特別利率での融資を実施した。また、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット、セキュリティ対策製品等の導入に対して、特別償却 30%又は税額控除３%（賃上げを伴う場合は５%）を措置するコネクテッド・インダストリーズ税制を引き続き運用するなど支援策を強化した。 ・総務省及び経済産業省において、説明会等を通じた制度周知を行ったほか、HP における事例の紹介等を実施し、制度の更なる活用を促すことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進した。
（タ）	経済産業省	経済産業省において、IPA を通じ、サイバーセキュリティビジネスの振興・活性化を図るため、サイバーセキュリティ対策におけるニーズの明確化・具体化、シーズの発掘やビジネスマッチングを行う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）を継続して開催する。また、コラボレーション・プラットフォームの地方開催についても検討を進める。（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２～３か月に１度の頻度で開催し、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。また、地域に根差したセキュリティコミュニティの形成を促進するために、東北や中国地域等で地方版コラボレーション・プラットフォームを開催した。

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	2019 年度　年次計画	取組の成果、進捗状況
（チ）	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に基づき、AI 技術を駆使することで、マルウェアの攻撃挙動の解析を自動化し、早期警戒情報を導出する技術の研究開発を実施する。	・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に基づき、AI 技術を駆使することで、IoT マルウェアの挙動検知技術の基本方式の設計を実施した。

（ツ）	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サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）を構築するとともに、CURE に基づく自動対策技術の確立等を行う。	・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サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）を開発・実装するとともに、NICT 内における集約データ間の突合分析を含む試験運用を行った。
（テ）	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、通信量の抑制と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のための研究開発を進め、詳細な技術仕様の検討と性能評価を行う。	・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、通信量の抑制と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のための研究開発を進め、詳細な技術仕様の検討と性能評価を行った。
（ト）	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。
（ナ）	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。2019 年度においては、ソフトウェア製品の届出 244 件、ウェブアプリケーションの届出 1,032 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、128 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、2019 年度においては、脆弱性対策情報を約 19,000 件（累計：約 116,000 件）公開した。
（ニ）	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。また、より高度な観測能力を実現するためにシステムの刷新を図る。（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 25 の経済地域の 29 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(2020 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、APCERT が主催する APCERT Drill、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。 ・TSUBAME ワーキンググループへの参加継続意志の確認を通じて、各国との TSUBAME の活用したインシデント対応について参加メンバーに理解を求めた。

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			
・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	2019 年度　年次計画	取組の成果、進捗状況
（ヌ）	文部科学省	文部科学省において、2018 年度に開始した「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。	・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、①量子ビットの高集積化技術や高品質な量子ビット（高忠実度、長コヒーレンス時間）等の開発、②量子コンピュータ上での実用上の優位性を示すことができるアプリケーションの開拓、③クラウドサービスによる利用者への提供を目指すための集積回路の構造の最適化及び集積実装の技術開発を実施した。
（ネ）	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、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 2019 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、革新的な人工知能基盤技術の構築を進めるとともに、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、ビッグデータ等に関する戦略目標の下、ビッグデータ統合利活用促進のためのセキュリティ基盤技術などサイバーセキュリティを含む研究課題に対する支援を実施した。
（ノ）	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取り組む。（再掲）	・多種多様なものが接続される複雑なシステムで必要となる、柔軟なアクセス制御が可能な関数暗号などの暗号技術を提案した。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」作成において、ソフトウェア工学や情報セキュリティの観点からその完成に貢献した。
（ハ）	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。	・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。
（ヒ）	総務省	総務省において、NICT を通じ、情報理論的安全性（暗号が情報理論的な意味で無条件に安全である性質）を具備した量子暗号等を活用した量子情報通信ネットワーク技術の確立に向け、実用性の向上とアプリケーションの拡大に向けた研究開発及び国際標準化を推進する。	・量子鍵配送ネットワーク技術の成果を盛り込んだ国際標準勧告が、ITU-T SG13 において、Y.3800 勧告として成立した。また、量子暗号を用いて顔認証に際してやりとりされる情報が盗聴・窃取されない技術を開発した。さらに、量子暗号を用いることにより、電子カルテデータを安全にバックアップした上で、災害時には迅速にデータを復元できるシステムを開発した。

（フ）	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）。
（ヘ）	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、及び日本提案暗号の標準化準備のための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（2019 年４月テルアビブ会合は日本から参加、2019 年 10 月パリ会合）として、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。 ・日本技術の標準化作業を推進しており、WG2 では日本から新規提案された「秘密計算」の規格化が始まることが合意された。今後、日本からエディタを出す予定であり、標準化を支援していく。 ・同じく、WG3 では、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委託事業「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／高度な IoT 社会を実現する横断的技術開発／複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発」が取り組んでいる PUF の国際標準化を支援しており、Part1 は国際標準化完了一歩手前の DIS 投票にこぎつけた。また、中国が主導する量子鍵配送について日本からも対抗技術を提案する支援を実施している。

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			
・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	2019 年度　年次計画	取組の成果、進捗状況
（ホ）	内閣官房	内閣官房において、研究・技術開発に資する産学官連携による体制構築の検討を含め、国産のサイバーセキュリティ製品・サービスの育成も見据えた、我が国のサイバーセキュリティの研究・技術開発に関する取組方針を取りまとめると共に、関係機関との連携の下、施策を推進する。	・2019 年５月に、「研究開発戦略専門調査会」において、「サイバーセキュリティ研究・技術開発取組方針」を取りまとめた。また、研究開発戦略専門調査会等を通じて、国際的な研究動向や産学官連携事例について分析を行うとともに、研究コミュニティとの議論を行った。
（マ）	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、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した。
（ミ）	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、規模を拡大し実施する。（再掲）	・2020 年２月 24 日から 28 日まで米国サンフランシスコで開催された RSA カンファレンスについて、我が国２年目となるジャパン・パビリオンの出展支援を実施。※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。

（ム）	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、及び日本提案暗号の標準化準備のための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（2019 年４月テルアビブ会合は日本から参加、2019 年 10 月パリ会合）として、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。 ・日本技術の標準化作業を推進しており、WG2 では日本から新規提案された「秘密計算」の規格化が始まることが合意された。今後、日本からエディタを出す予定であり、標準化を支援していく。 ・同じく、WG3 では、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委託事業「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／高度な IoT 社会を実現する横断的技術開発／複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発」が取り組んでいる PUF の国際標準化を支援しており、Part1 は国際標準化完了一歩手前の DIS 投票にこぎつけた。また、中国が主導する量子鍵配送について日本からも対抗技術を提案する支援を実施している。
（メ）	内閣官房	内閣官房において、サブワーキンググループの運営を継続し、有識者の意見も踏まえつつ、サイバーセキュリティ関係法令集の策定に向けて検討を進め、ハンドブック（仮）として成果物を取りまとめる。（再掲）	・サブワーキンググループ及びタスクフォースにおける議論を経て、「サイバーセキュリティ関係法令 Q&A ハンドブック」を取りまとめ、2020 年３月２日に NISC のウェブサイトで無料公開を行うなど、周知啓発を図った。

(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	2019 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、各府省庁と連携し、中長期を視野に、様々な領域の研究との連携についての調査等を検討する。	・研究開発戦略専門調査会をはじめとして、中長期的な研究開発の課題について、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	2019 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・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	2019 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、関係機関と連携し、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、対象となる層や伝達手法の見える化及び連携を推進するための検討を行う。（再掲）	・関係機関の協力のもと、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、仮運用を開始した。
（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して役立つ情報等について、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、引き続き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 12,344 件の相談に対応した。 ・標的型サイバー攻撃特別相談窓口では、情報収集に努め、標的型サイバー攻撃の相談対応を 392 件実施した。これを通じて、標的型攻撃メールや不審ファイル、公開情報となっているサイバー脅威情報を 489 件入手した。入手した情報の調査と相談内容の分析を行い、状況などからレスキュー対応が必要と判断した組織に対し、ヒアリングや、相談者自身による調査対応の支援等を実施した。
（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 HP 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、ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保やデータの完全性の確保等を実現するためのトラストサービスの在り方について検討を行う。	・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、電子署名法に関する要望を踏まえて、電子署名法施行規則第５条に定める利用者の真偽の確認方法について、新たな確認方法を告示にて追加し、利用者の真偽の確認方法の選択肢を広げることで、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、トラストサービスに関する有識者会合にてトラストサービスの在り方等について検討を行い、2020 年２月に最終取りまとめを行った。
（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、JPCERT/CC を通じて、次のことを実施した。 ・注意喚起を 49 件、注意喚起以外の情報の提供として、29 件(日本語 16 件/英語 13 件)のブログ及び 38 件のサイバーニュースフラッシュによる脅威及び対策に関する情報を提供した。 ・MalConfScan をはじめとするインシデント対応に資するツールを３件オープンソースとして公開した。 【安心相談窓口】 ・経済産業省において、IPA を通じ、「安心相談窓口だより」を 5 件公表した。 ・経済産業省において、IPA を通じ、「安心相談窓口公式 Twitter」にて 78 件の情報を発信した。 【J-CSIP、早期警戒パートナーシップ】 ・経済産業省において、IPA を通じ、「緊急対策情報」を 12 件、「注意喚起情報」を 27 件公表した。また、ウイルス・不正アクセス届出制度の届出情報を基に、事例レポートを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。	・「講習能力養成セミナー」を全国 13 箇所において開催し、中小企業の経営者、社内教育担当者等合計約 935 名が参加した。 ・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のセミナー等へ合計 51 箇所に講師を派遣し、約 3,060 名が受講した。 ・上記活動の中で、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ったことで利用促進を図り、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約 132,420 名程度に増加した。

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			
・「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	2019 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、各地で関連行事を行うとともに、「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イベントを行い、普及啓発活動に取り組んだ。

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	2019 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」について、最新の状況を踏まえて内容の見直しを行った。
（コ）	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、7,955 件ダウンロードされた。
（サ）	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。2018 年度には、e-ネットキャラバンの保護者・教職員等向け講座の内容に、若者が使う主要な SNS の解説等を加えており、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。	・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。2019 年度は、2019 年４月から 2020 年３月までの間、2,660 件の出前講座を実施した。また、2020 年３月に、「インターネットトラブル事例集（2020 年版）」を公表した。
（シ）	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４か所で開催することにより普及啓発を実施した。
（ス）	文部科学省	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、新学習指導要領の趣旨を踏まえ、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、2020 年１月 27 日～１月 31 日に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済。

（セ）	文部科学省	文部科学省において、最新のトラブルや被害の状況等を踏まえ、2018 年度に改善した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について、2020 年２月までに実施済。
（ソ）	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 15 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 47,226 点、ポスター 4,723 点、４コマ漫画 6,578 点、書写（硬筆）2,140 点、合計 60,682 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 15 校の応募の中から「優秀活動事例賞」に９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。
（タ）	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、 ・教育関係者等が児童・生徒・学生等に指導する際に使用可能な教材を７テーマ（SNS や情報セキュリティ等）22 種類とともに、指導するポイントをまとめた講義要領を作成、試行版を 2019 年 11 月 28 日に、正式版を 2020 年３月 30 日に公開し、10,963 ダウンロードされた（2020 年３月末）。 ・作成した教材を使用して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ーにむけ、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 47 都道府県で１回以上計 50 回開催し、3,426 名が参加した（2020 年３月末）。 ・「ホームユーザー向け安全教室」を全国 52 か所で開催し 5,434 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 33 回実施し 5,160 名が参加した（2020 年３月末）。

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	2019 年度　年次計画	取組の成果、進捗状況
（チ）	総務省	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、引き続き利用者・提供者において必要となるセキュリティ対策に関する検討を行うとともに、利用者・提供者に対する周知啓発を実施する。	・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、「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」の改定検討を行った。また、無線 LAN の安全な無線 LAN 環境の整備のためのリテラシー向上として、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。
（ツ）	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を含めたサイバーセキュリティに関する現状把握及び対策を実施する際に参考となる最新の動向の収集・分析・報告書の公表等により、サイバー空間利用者への啓発を推進する。	・「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書を公開（４月）し、委託元と委託先の間のセキュリティに関する責任範囲について現状と課題を整理した。また、この調査結果について講演を実施した（２回）。 ・企業が安全にデータ利活用を行うためのデータ利活用ガイドライン作成に向けた調査事業「企業におけるデータ利活用・保護の戦略立案のための手引書（案）」を実施した。

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	2019 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。また、総合的分析機能の強化を図る。 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（iBox）により、国内外のインシデント及びサイバー攻撃に関する情報の共有を行うなど、関係機関の一層の能力強化を行った。2019 年度は、約 800 件の情報を接受した。また、国際担当者間の会合や 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。さらに、NICT と締結した研究開発や技術協力等に関するパートナーシップに基づいて NICT との協力体制を整備し、サイバーセキュリティ対策に係る技術面の強化を図る。
（イ）	内閣官房	内閣官房において、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、2020 年東京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 2019 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 2019 の本編及び概要をまとめた冊子を制作した。 ・内閣官房及び関係省庁において、2018 年戦略及びこれに基づくサイバーセキュリティ 2019 の冊子を活用し、各種セミナーでの説明等を通じて、計 23 件のイベント等で、国内外の関係者 2,200 名超に対して、2018 年戦略等の発信を行い、周知を図った。
（ウ）	内閣官房	内閣官房において、2020 年東京大会を見据え、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。（再掲）	・2019 年度においても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、2020 年度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。（再掲） ・「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し、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。 ・「対処態勢の整備・運用」については、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・訓練等を実施するとともに、G20（金融・世界経済に関する首脳会合）、ラグビーワールドカップ 2019 等において、サイバーセキュリティ対処調整センター及び情報共有システムを運用し、運用態勢の確認、改善を実施する。	・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。 ・リスクマネジメントの促進については、重要サービス事業者等を対象とする第５回目のリスクアセスメントの実施を依頼、提出された実施結果について横断的に分析し各事業者等にフィードバックを実施した。また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況を NISC が検証する横断的リスク評価の第２、３回目を実施した。第２回以降の取組においては、重要サービス事業者等（競技会場（レガシー部分）を含む。）を対象に検証（実地又は書面）した。なお、競技会場のオーバーレイ部分の対策の整備状況及び監督状況については、組織委を対象に検証を行った。 ・対処態勢の整備については、サイバーセキュリティ対処調整センターを 2019 年４月に設置し、恒常的に情報共有システムを使用した関係組織・機関への迅速な情報提供を実施したほか、大会までの大規模イベントである 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は、ラグビーワールドカップ組織委員会、会合の現地事務局等に連絡要員を派遣し、大会の対処態勢と同等の態勢で運用するとともに、情報共有及びインシデント発生時の対処に係る訓練・演習を実施し多くの運用経験と教訓を得た。これらの運用経験と教訓をもとに、情報共有・事案発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して、対応手順等について改善を実施した。また、サイバー脅威情報の提供について５社から協力を受けることを決定した。

（本ページは白紙です。）

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、2019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2020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

2019 年度の総合評価・2020 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　原　邦彰

令和元年度は、従来の標的型攻撃メールに加え、ランサムウェアなどを使用した攻撃、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、東京2020大会を控え、国内における「EMOTET（エモテット）」の感染が拡大していることからも、政府機関に対するサイバー攻撃の脅威が大きい状況が続いているものと考えられる。

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

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

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

しかし、日々技術が進歩するとともに新たな脆弱性も発見される情報通信分野において、情報セキュリティ対策に終わりはない。また、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、技術の高度化により攻撃自体が検知されず潜在・巧妙化し、かつ執拗となっているとも指摘され、クラウド型のサービスについても新たな脅威が報告されている。

このような状況を踏まえ、内閣官房では令和２（2020）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

2019 年度の総合評価・2020 年度の全体方針

最高情報セキュリティ責任者
総務主幹　佐藤　則夫

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。

令和元年度においては、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するとともに、NISC が実施したマネジメント監査における指摘事項に対して、情報セキュリティ対策を実施した。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２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

2019 年度の総合評価・2020 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　西　浩明

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、組織として必要な情報セキュリティの確保とその継続的な強化等の対策に取り組むことが不可欠である。

2019年度においては、階層別の集合研修や全職員を対象としたe-ラーニングのほか、テレワークを希望する職員を対象としたe-ラーニング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、全職員を対象とした標的型メール攻撃訓練を実施し、その結果と標的型メール攻撃の際の対処方法について周知するとともに、不審なメールを受領した際に求められる人事院CSIRTへの報告等の意識を向上させるためのアンケートを実施した。

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。

2020年度においては、外部委託により民間事業者に要保護情報を取り扱わせる場合、定められた情報セキュリティ対策の実施が徹底されるよう、外部委託業務調達仕様書等の事前確認や実地監査等の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取り組むこととする。

また、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努めることとする。

内閣府

2019 年度の総合評価・2020 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。

内閣府では、次世代アンチウイルスによる不審なファイルの実行制御、メール誤送信防止機能の強化、Webアクセス分離の実装等によりセキュリティ対策を強化してきた。また、「働き方改革」の一環として一般行政端末の持ち運びを容易とするにあたり、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。ただし、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。

以上の状況を踏まえ、令和２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、ウェブサイトの常時暗号化（TLS化）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

2019 年度の総合評価・2020 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。

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，令和元年度においては，主に以下の取組を実施した。

○政府機関の情報セキュリティ対策のための統一基準群の改定を踏まえた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改定

○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の更新に伴う情報セキュリティ対策の強化

令和２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，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とともに，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

2019 年度の総合評価・2020 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　東出　浩一

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。

令和元年度においては、技術的な対策として公正取引委員会内ネットワークがインターネット分離環境に移行したため、分離環境下でも有効な訓練内容に変更した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ｅラーニング研修のほか、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集合研修や情報システム担当者向けの集合研修・ｅラーニング研修を実施し、職員の情報セキュリティに対する更なる意識向上を図った。さらに、政府統一基準群の改定、自己点検・監査等の結果を踏まえた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ったほか、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２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、東京2020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

2019 年度の総合評価・2020 年度の全体方針

最高情報セキュリティ責任者
事務局長　其田　真理

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２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

2019 年度の総合評価・2020 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

カジノ管理委員会においては、2019年度に、「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年度版）」（平成30年７月25日改定）、「府省庁対策基準策定のためのガイドライン（平成30年度版）」（平成30年７月25日改定）等に基づき、カジノ管理委員会情報セキュリティポリシー（以下「ポリシー」という。）及び下位規程を策定し、情報セキュリティ対策等について審議する情報セキュリティ委員会の設置を行うとともに、全職員にポリシー及び下位規程の周知徹底を図るため、情報セキュリティに関する教育や転入者に対する自己点検の実施を行った。また、GSOCやCYMAT等へ加入するとともに、内閣サイバーセキュリティセンター等の実施する各種研修へ参加した。

2020年度においては、カジノ管理委員会LANシステムが2020年3月末に稼働したことも踏まえ、ポリシー及び下位規程に基づき、情報セキュリティに関する教育、情報セキュリティ対策の自己点検、情報セキュリティ対策の監査、情報セキュリティに関する各種訓練や情報システムに対する点検等の実施を行い、情報セキュリティ対策の定着を図ることとする。

警察庁

2019 年度の総合評価・2020 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　彦坂　正人

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。

平成31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、それぞれのＣＳＩＲＴ担当者を招致した訓練等を実施した。

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、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２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

2019 年度の総合評価・2020 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

昨今、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は、一層複雑化・巧妙化を続けている。また、政府機関等の職員や外部委託先の社員による事務過誤や犯罪による情報漏洩も大きな脅威となっており、情報セキュリティの確保は、引き続き重要な課題となっている。

一方で、「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画について（2019 年６月 14 日閣議決定）」において、「世界最先端デジタル国家」へ目標を深化させていくことが表明され、ビッグデータ利活用等の IT の活用に関する様々な具体的施策が進められており、IT の利便性と情報セキュリティとの高いレベルでの両立が求められている。

こうした状況にあって、金融庁としても、サイバー攻撃等に対応するための網羅的な対策の必要性を強く認識しており、2019 年度においては、サイバーセキュリティの脅威に対して、脅威情報を収集して庁内システムの防御設定を行う、脆弱性情報を庁内に展開する等の早期警戒対応を強化してきた。また、情報セキュリティに関する教育の実施、情報セキュリティに関連する規則や手順等の改定、技術的対策の多重化・多層化等の継続した取組を行った。

2020 年度においては、これまでのサイバーセキュリティの脅威に対する取組を継続することとしつつ、加えて、インシデント対応体制の再確認等を行う。また、2019 年度の情報セキュリティに関する取組により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に関する取組への的確な対応を念頭におき、情報セキュリティ教育や情報システムに関する新たな技術的な対策の導入に向けた検討などに取組、PDCA の徹底により、情報セキュリティ水準の一層の向上を図っていくこととする。

消費者庁

2019 年度の総合評価・2020 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

国内では、標的型攻撃、ビジネスメール詐欺、ランサムウェアなどのサイバー攻撃の被害が依然として報告される中、当庁においては重大な情報セキュリティインシデント等は発生しておらず、適切な情報セキュリティ運用が行えたものと評価している。平成30年度に更改した当庁情報システムの根幹である消費者庁ネットワークシステムも、順調に運用されており、庁外からの不正アクセスなどの攻撃に対する対策強化に役立てられている。

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。例年どおり不審メール訓練を実施し、不審メールによる脅威と対応方法について職員への周知徹底を行った。また、従来の一般職員向けの情報セキュリティ教育に加えて最高情報セキュリティ責任者を始めとする責任者に対する教育を新たに開始し、組織としての情報セキュリティレベルの一層の引上げを図った。

サイバー攻撃の高度化・巧妙化は今後も進むと考えられることから令和２年度においても前年度と同様、ＰＤＣＡサイクルに従って情報セキュリティ対策を推進する。職員の情報セキュリティ意識向上のため、eラーニングによる教育を継続し、各責任者が行うべき具体的な対策の内容を充実させる。また、情報セキュリティ対策に係る自己点検や監査についても、実施内容の品質や精度の向上を図る。

復興庁

2019 年度の総合評価・2020 年度の全体方針

最高情報セキュリティ責任者
統括官　石田　優

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。

令和元年度（平成31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、平成30年度に引き続き、復興局を対象に情報セキュリティ監査を実施し、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２年度においては、令和元年度（平成31年度）に実施した情報セキュリティに関する自己点検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

2019 年度の総合評価・2020 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　竹内　芳明

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。

○2019年度の総合評価

2019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、前年度に改正した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を実施するなどの取組を行ってきたところであり、自己点検や監査等の結果から、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。

○2020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

2020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、省内の関係部局との連携強化を推進する。

情報セキュリティ対策推進体制とＰＭＯの連携を強化し、情報システム資産台帳の整備の徹底等を図る。

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の連携を強化し、マネジメント能力の向上を図る。

(2) 継続実施

2019年度に実施した施策及びリスク評価の結果を踏まえ、引き続き、以下の事項を重点的に実施する。

(ｱ) 東京2020大会に向けた情報セキュリティ教育・訓練の実施

東京2020大会の開催時期を考慮し、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対応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

従前より取り組んできた情報セキュリティ対策を着実に実施する。

- 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
- 最高情報セキュリティアドバイザーによる情報セキュリティ対策に関する専門的な助言の実施

(3) その他

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

2019 年度の総合評価・2020 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　伊藤　栄二

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，令和元年度は，当省の情報セキュリティポリシー（以下「ポリシー」という。）の更なる浸透を図るため，ポリシーに基づく教育，自己点検等の取組に加え，情報セキュリティマネジメントに係る内部監査を実施し，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。以下「人材育成計画」という。）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，ポリシーの浸透は着実に進んできているものの，ポリシーが確実に遵守され，必要な情報セキュリティ対策が当省全体で実行されるためには，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２年度上半期は，東京 2020 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，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

2019 年度の総合評価・2020 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　垂　秀夫

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，情報セキュリティ対策を最重要課題の一つとして位置づけ，省内の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等を通じ，職員の意識向上に取り組んできた。

2019 年度においては，不正プログラムを検知する内部対策，不正通信を遮断する出口対策等の不正プログラムの侵入を前提とした多層防御によるセキュリティ強化策を実施した。また，政府統一基準群の改定に伴い，2018 年度に改正した「外務省情報セキュリティポリシー」の職員への浸透を図り，各種研修，標的型メール攻撃に関する訓練等にて，情報セキュリティ対策についての教育・啓発を実施した。2019 年度は，G20 大阪サミット，第 7 回アフリカ開発会議（TICAD7），即位礼正殿の儀といった諸外国の要人が参加する大規模行事が行われたが，各行事において重大な情報セキュリティ・インシデントの発生は確認されなかった。これは関係省庁との連携の下，これまで継続的に取り組んできた各種対策が奏功したものと思われる。

2020 年度は，東京 2020 大会が予定されており，サイバー攻撃の脅威が高まることが想定される。また，2019 年度にはマルウェア感染を狙うメールも急増しており，その攻撃手法は巧妙化・高度化し，当省職員を標的とした不審メールが恒常的に送られてきていることから，情報セキュリティ対策をより一層進めていく必要がある。こうした状況を踏まえ，2020 年度は以下の取組等を通じ，攻撃への効果的な対処及び職員の情報セキュリティに対する更なる意識向上に努め，情報セキュリティの一層の確保に万全を期していく。

（１）リスクの低減やインシデント発生に対する効果的な対処に向けた取組
ア　ペネトレーションテスト等を通じ，情報システムの問題点の把握とその是正
イ　ネットワークシステム及び通信手段の更なる情報セキュリティ対策の強化・検討
ウ　NISC が実施する CSIRT 訓練，各種研修等への参加を通じた人材育成
エ　新たな脅威・攻撃，その対応策に関する情報収集，適時・迅速な対処
（２）情報セキュリティマインド向上のための教育・訓練の実施
ア　標的型メール攻撃等を想定した訓練
イ　昨今の情勢を踏まえた情報セキュリティに関する集合研修，e ラーニングの実施
ウ　情報セキュリティに関する自己点検の実施
エ　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

2019 年度の総合評価・2020 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。

2019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、内部監査や自己点検等の実施（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）
・ G20財務大臣・中央銀行総裁会議等の円滑な開催のため、関係部局と連携した情報セキュリティ対策措置の実施
・CSIRT体制を一層強化するため、システム統括部局において外部のセキュリティ専門家の支援を得るための具体的方策の検討
・CIO補佐官3名の最高情報セキュリティアドバイザーへの指名

新型コロナウイルス感染症対策に関連し、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目下の課題となっている。2020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

2019 年度の総合評価・2020 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　柳　　孝

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、外部からの直接的な攻撃のみならず、情報セキュリティインシデントにつながる可能性のある省内職員による人的ミスを防止するために必要な取組を引き続き行っていく必要がある。

なお、文部科学省本省と施設等機関（国立教育政策研究所及び科学技術・学術政策研究所）の連携をより強化し、施設等機関を含む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、より一層の指導・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) 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

2019 年度の総合評価・2020 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。また、令和元年度においては、外部委託に係る情報セキュリティ事案も見受けられたところである。

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、令和元年度においては、次の取組を重点的に実施した。

・東京2020大会に向けたサイバーセキュリティ対策の強化
・IT調達に係るサプライチェーン・リスク対応の強化
・平成30年度に改定した当省情報セキュリティポリシー及び関係規程に関する具体的な手続・対策を示した階層別研修の充実

令和２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。

・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（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資産管理機能の活用
・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

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

2019 年度の総合評価・2020 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　枝元　真徹

(1) 国内においては、依然として、組織を狙った巧妙な標的型メール攻撃が発生しているほか、電子メールのクラウドサービスやウェブメールのサーバが不正アクセスされ、情報の窃取や迷惑メール送信の踏み台にされる事案が多数発生するなど、サイバー攻撃は、より一層、巧妙化・深刻化が進んでいる状況である。

また、今年度は、新型コロナウイルスの感染予防対策としてテレワークの実施やウェブ会議サービスの利用が増加しており、これらに関連したリスクの高まりが想定される。

(2) このような中、農林水産省においては、省内の LAN システムについて、平成 28 年１月に、省内 18 システムのうち９システムを統合（第１次統合）し、平成 31 年３月に、残りの９システムを統合（第２次統合）したところである。これに伴い、サイバー攻撃の監視や情報セキュリティインシデント対処等の体制を本省に一元化するなど、LAN システムに関する情報セキュリティ対策の強化を図ったところである。

(3) また、情報セキュリティ推進体制の強化を図るため、平成 30 年度から外部委託により農林水産省最高情報セキュリティアドバイザーを確保し、発生した情報セキュリティインシデントについて、適切に対処するための助言や支援を得ながら、迅速かつ的確な初動対応等に当たっているところである。

(4) これらの状況を踏まえ、令和２年度においては、農林水産省における情報セキュリティ関係規程に基づく取組のほか、以下の取組を実施することとする。

ア 農林水産省 CSIRT 構成員、情報システムセキュリティ管理者等に対し、情報システムのセキュリティ対策に関する研修や情報セキュリティインシデントの発生を想定した実践的な演習等の実施

イ ソフトウェアの重大な脆弱性に関する注意喚起及び対策の実施状況の把握

ウ 平成 31 年４月に発足したサイバーセキュリティ協議会を通じたサイバー攻撃に係る情報共有の推進並びに当該情報を活用したサイバー攻撃の被害予防及び迅速かつ的確なインシデント対処

エ 外部委託により確保した農林水産省最高情報セキュリティアドバイザーの活用による情報セキュリティの確保の促進

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

2019 年度の総合評価・2020 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　糟谷　敏秀

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。

昨年度のラグビーワールドカップ、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してきている。また、民間企業等に対しても標的型攻撃と思われる不正アクセス事案が複数確認されるなど、攻撃対象の拡大とともに、手法も複雑化・巧妙化してきている。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、今年に入り新型コロナウイルス感染症対策としてテレワークの実施や外部の Web 会議サービスの利用ニーズが増加し、今後も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。

２０１９年度においては、２０１８年７月の「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。）の改定に伴う当省内の関連規程の改定、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、教育、自己点検等を実施するとともに、セキュリティ・ＩＴに係る人材の確保・育成に資するべくＮＩＳＣ等の実施するＣＳＩＲＴ訓練や各種研修等に参加した。

また、情報システムについても、基幹ＯＡシステムの更なるセキュリティ対策や精度向上、省内各部局で所管する業務用情報システムの情報セキュリティ対策の実施状況の確認及び対策を実施した。

２０２０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、２０１９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 会議の利用に係るセキュリティ確保のためのルールや環境を整備
（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）「経済産業省におけるセキュリティ・IT 人材確保・育成計画」（以下「人材確保・育成計画」という。）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
（４）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
（５）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
（６）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、情報共有等を実施

国土交通省

2019 年度の総合評価・2020 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　蒲生　篤実

近年では、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が多数観測・報告されており、東京2020大会を控え、より一層、複雑化・巧妙化・増加することが予想される。特に標的型メール攻撃については、やり取り型攻撃や複合的攻撃など、その手口が巧妙化し、政府機関等においても大きな被害が発生している。このような中、国土交通省では、情報セキュリティ対策を推進している。具体的には、令和元年度においては、主なものとして、以下の対策を実施した。

①「国土交通省情報セキュリティポリシー」の改定を受け新たに「情報セキュリティ対策推進体制に関する規程」の決定及び情報セキュリティポリシーに基づく９規程の改定
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。また、省内イントラネットの情報セキュリティ関連ページを充実
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、独立行政法人、重要インフラ分野、所管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の設立支援、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再周知等を実施

令和２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

2019 年度の総合評価・2020 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

地球温暖化対策をはじめとする環境問題に対し、世界全体の行動変容を促し対策を進めるためにも、環境省として情報発信を強化していくとともに環境省の働き方についても多様な働き方、緊急時の対応力強化に向けIT技術の利活用を含め改革していく必要がある。その一方で、信頼性のある情報発信やIT技術の効果的な利活用を行うためには、適切な情報セキュリティ対策が不可欠である。

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、情報の窃取だけでなく、情報システムの破壊や金銭的利益までをも目的とするように変化しているとの指摘がある。こうした変化に対しても、情報セキュリティ対策の見直しを行い、システム的な対策と人的な対策を継続して適切に強化することで、国民のための持続可能な社会づくりに対する安定的な取組に資する体制を確保する。

令和元年度は、マルウェア「Emotet」の感染被害が国内のみならず世界中で報告され、サプライチェーンリスクを含めたリスクマネジメントの重要性について、環境省としても認識を新たにしたところである。こうした外部脅威の動向について、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不注意で発生させることのないよう、改めて注意喚起を行った。

令和２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、令和元年度の取組の結果を踏まえて、教育内容など取組の見直しを行い、環境省の情報セキュリティ対策を総合的に強化する。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を検討あるいは見直しし、適切に実施する。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係る手続のための情報システム等、今後調達・構築されるシステムにおいては、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に取り組む。なお、新型コロナウイルス感染症により、様々なイベント、取組、事業等が影響を受けていることを踏まえ、情報セキュリティ対策への影響を可能な限り低減するよう留意する。

防衛省

2019 年度の総合評価・2020 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　鈴木　敦夫

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、2019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70名の増員）
・サイバー人材の確保・育成
・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

また、防衛省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、2020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「ちょっと待て　情報セキュリティは基本から　～そのクリック、安全ですか？～」とし、全職員に対して、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。更に部外有識者を招聘し、情報セキュリティ講習会を実施することで、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。

2020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、部外の高度人材を発掘するためのサイバーコンテストの開催など、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、2019年度に引き続き、防衛省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。

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

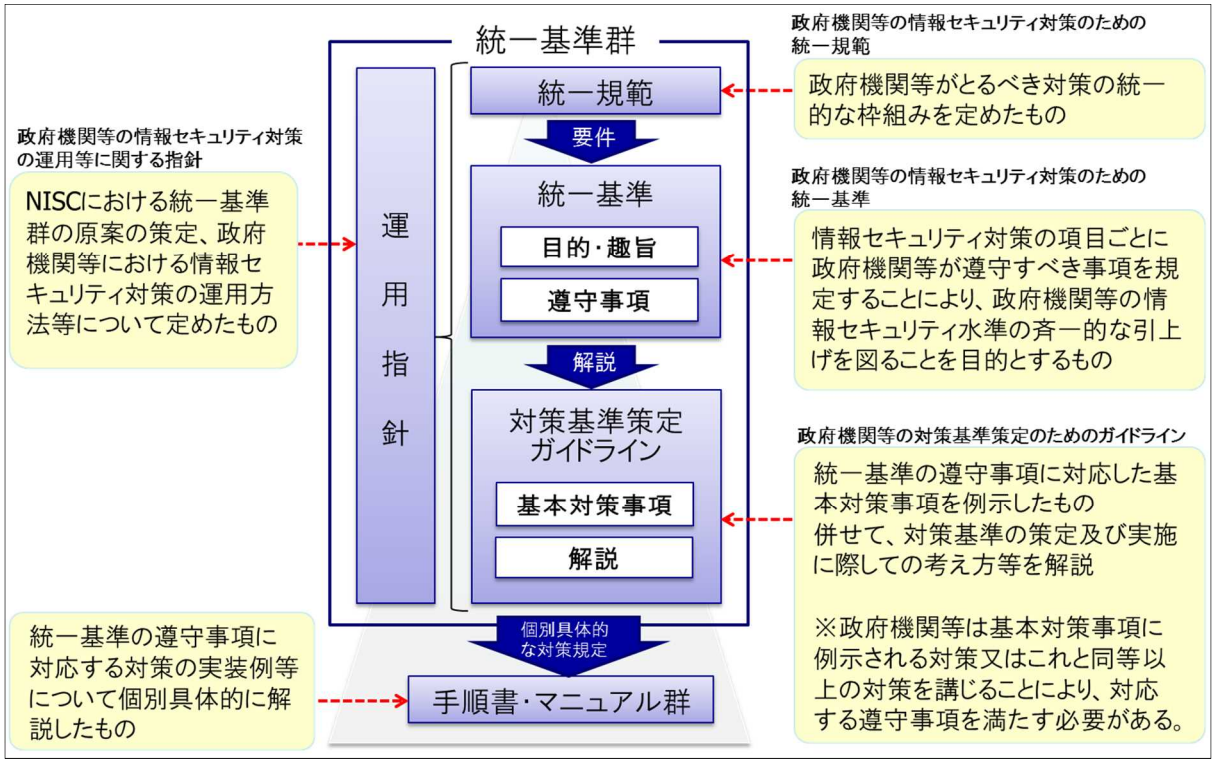
１　概要

「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、2019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。

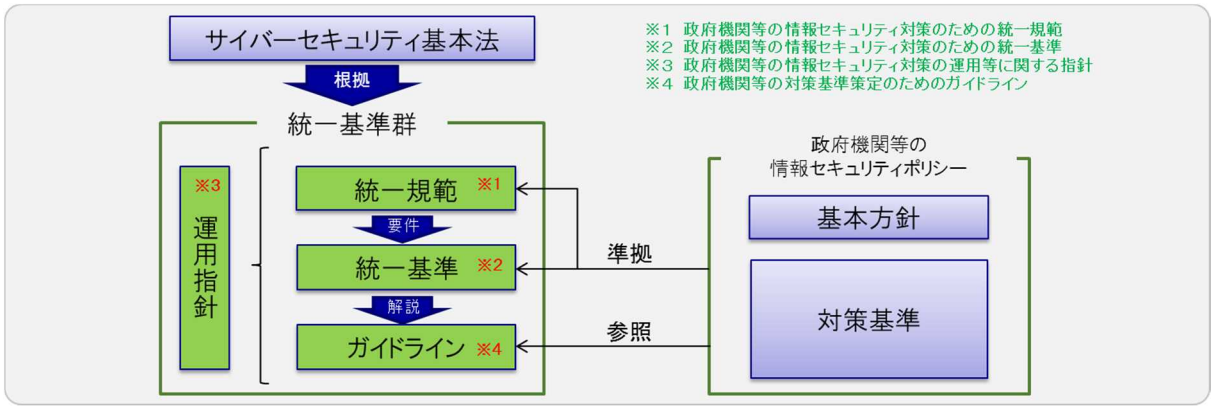
統一基準群（平成30年度版）の文書構成は、図表１のとおりである。

図表１　統一基準群の文書構成



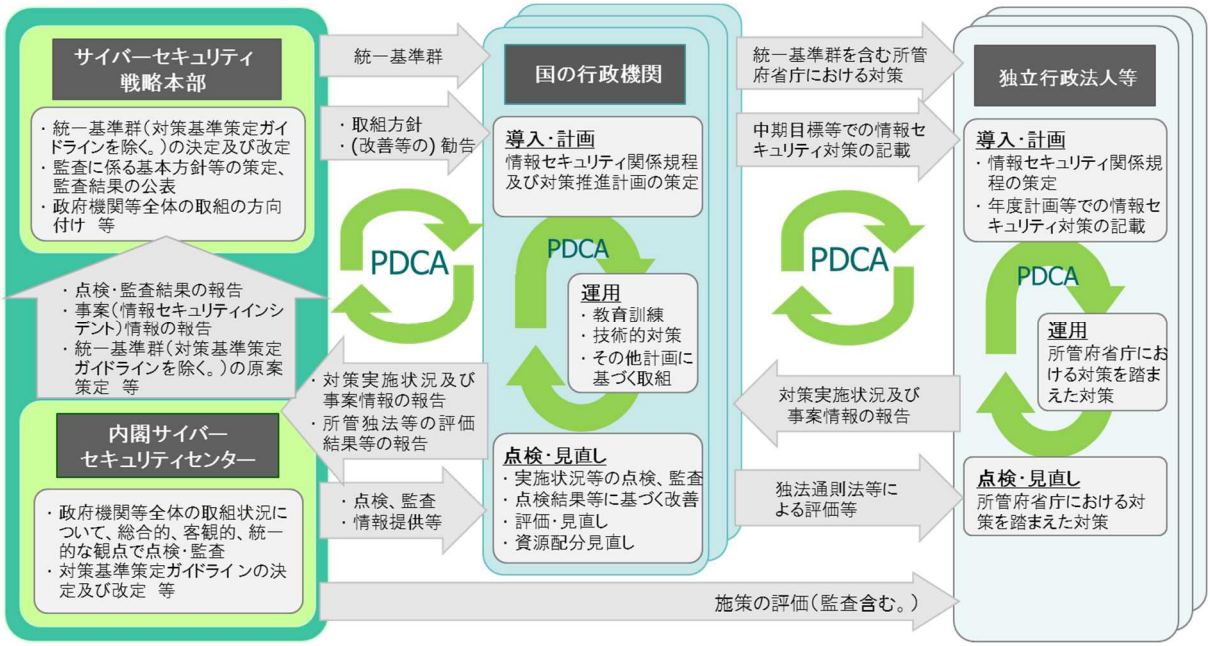
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等の情報セキュリティ対策のための統一基準（以下「統一基準」という。）」と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（図表２）。

図表２　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３）。

図表３　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　統一基準群の改定に係る検討

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が今後一層進展することが見込まれるが、従来からのオンプレミスでの情報セキュリティ対策とは異なり、クラウドサービスの利用に際しては、サービス提供者及びサービス利用者が各々の責任範囲において情報セキュリティ対策を実施することが求められる。また、政府機関等に向け、クラウドサービス提供者側の情報セキュリティ対策を評価する制度の立ち上げが予定されているところ、クラウドサービス利用者側の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脅威等の動向を踏まえ、統一基準群の改定に向けた検討を行い、2019年度に改定骨子の策定に着手した。

次期改定に向けては、クラウドサービス利用者側として特に気を付けるべき対策や考え方等について国際標準等を参考に記載を追加することや、近年発生したクラウドサービス利用における重大インシデントを踏まえた対策を追加する方向である。

これらを含む主な項目は、以下に示すとおりである。

（1）クラウドサービスの利用拡大を見据えた記載の充実

セキュリティ評価制度（仮称）の立ち上げも見据え、クラウドサービス利用者側として実施すべき対策や考え方に係る記載を追加。

（2）情報セキュリティ対策の動向を踏まえた記載の充実

政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえた記載の充実を図る。

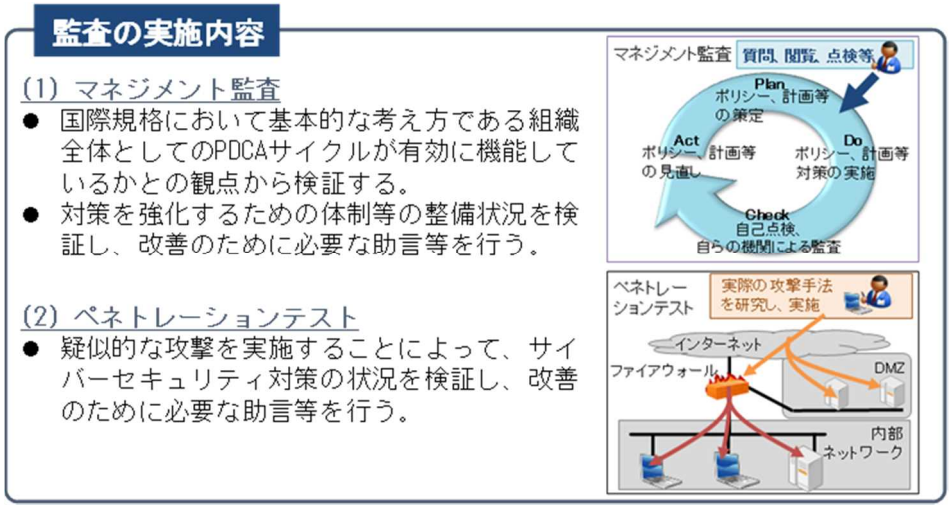
（3）多様な働き方を前提とした情報セキュリティ対策の整理

テレワークを行う場合のセキュリティ対策について、参照すべき統一基準上の規定や解説を整理することで、政府機関等が実施すべき対策の水準を明確にする。

別添４－２　サイバーセキュリティ基本法に基づく監査

１　2019 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、2019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

2019 年４月から 2020 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、11 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、業務継続性が重要となるシステムも対象として選定し、これらのシステムについては、可用性の観点に重点をおき監査を実施した。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、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

・不正プログラムの感染を想定した対応訓練において、利用者が感染画面を見落としたりしないようにするため、疑似不正プログラム（EICAR）を利用し、実際に不正プログラム対策ソフトウェアに検知させて、感染状態を体験させることで対処手順を確認していた事例

・情報セキュリティ対策の運用及び点検・監査等を評価するだけでなく、情報セキュリティマネジメントの推進等に関する幅広い取組を総合的に評価し、その結果を対策推進計画に取り込んでいた事例

・導入する機器やソフトウェアにおける情報セキュリティ対策の内容を明確にし、情報システムの構築において、必要な情報セキュリティ対策に漏れがないよう統一基準との対応チェックシートを用いて網羅的に確認していた事例

② 主な助言等

2019 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 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

マネジメント監査の実施対象外の 12 府省庁に対して、2018 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、ヒアリング等によりフォローアップを 2019 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。

2016 年度までの監査において、府省庁は対策状況を評価して改善を行う自律的な取り組

みを実施する等の情報セキュリティマネジメントシステムに課題が見られたが、2018 年度までの各府省庁における２回目の監査においては、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２回目の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。

フォローアップにおいて、各府省庁の 2018 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

2019 年４月から 2020 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 22 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 43 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。

2018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

2019 年４月から 2020 年３月までの間

2019 年度までに、全ての独立行政法人及び指定法人に対し監査を実施することとなっており、2019 年度で全ての独立行政法人及び指定法人に対し監査を実施した。

（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、29 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。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

・セキュリティ監視の運用において、「セキュリティインシデント」、「基盤システムインシデント」及び「脆弱性」を評価するための「インシデント評価値基準」を作成しており、初動対応の緊急度を決定するための判断基準を明確化することで、インシデント

発生時には、当該基準に基づいた評価の結果により、初動対応の緊急度を決定し、緊急度に応じた対応を行っていた事例。
・要機密情報の漏えいを防ぐため、暗号化の必要性の有無を検討し、認証された端末にインストールした暗号化・復号を行うソフトウェアにより全てのファイルを暗号化してサーバ保存する仕組みを構築していた事例
・情報セキュリティ対策の点検方法として、ISMS に基づいた管理手法及び企業経営における内部統制のリスク点検を準用した方法を取り入れ、実施され、情報セキュリティ推進活動に、企業経営や ISO の考え方・手法を取り入れ、情報セキュリティに対する課題の解決していた事例
・法人として、年間に数十か所の内部監査を行う監査計画を作成し、３年間でほぼ法人全体の監査が実施できるよう体制を整備し、さらに、外部の第三者による情報セキュリティ監査をも実施し、より有効な監査を実施していた事例

② 主な助言等

2019 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 2018 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

2018 年度に監査を実施した独立行政法人等 30 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。

2019 年度は 29 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、2018 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

2018 年４月から 2019 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、29 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 29 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。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。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。

2018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４－３　重点検査

１　概要

重点検査は、昨今の情報セキュリティに関する動向等を踏まえ、政府機関全体として分析・評価、課題の把握及び改善等が必要と考えられる項目について検査を実施し、各種対策の強化等に反映させることを目的とするものである。

２　検査項目と結果

検査項目		検査項目とした理由
最近の情報セキュリティ技術に関する調査	ＩＴ資産管理ソフトウェアの導入状況	NISC が情報セキュリティ対策に係る先進的な取組として導入を推奨している事項について、そのセキュリティ対策の実施状況を把握するため。
	デジタル著作権管理技術の導入状況	
	未知の不正プログラム対策ソフトウェアの導入状況	
管理者アカウントの管理状況の調査		政府機関において、管理者権限を持つアカウントの管理が適切に行われていることを確認するため。

（１）最近の情報セキュリティ技術に関する調査

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年度版）の基本対策事項において、IT資産管理ソフトウェア、デジタル著作権管理技術及び未知の不正プログラム対策ソフトウェアといった最近の技術が引用されたことを鑑み、各府省庁における導入・利用状況について検査を実施した。

ア　ＩＴ資産管理ソフトウェアの導入状況

IT資産管理ソフトウェアの導入状況については、基幹システムのような大規模なシステムにおいて主に導入されており、情報を効率的に収集する手法として各府省庁で利用されている。

利用については、端末の管理やサーバ機器を対象として、ハードウェア情報やソフトウェアの情報（インストールソフト、バージョン、セキュリティパッチ、更新プログラム）、ライセンス情報、ログ情報（操作ログ等）等を収集し、ハードウェアの資産管理、ソフトウェアライセンスの資産管理、インシデント対応、情報漏えい等対策（操作ログ取得、ログ分析等）、セキュリティパッチ、プログラムの更新等に活用している。

導入効果については、導入したほとんどのシステムにおいて効果があったと回答しており、導入による効果が高いことが確認できた。

イ　デジタル著作権管理技術の導入状況

デジタル著作権管理技術の導入状況については、基幹系システム、電子認証・入札系システム等で導入されており、コンテンツの著作権の管理・保護という利用目的の導入はされていない。

利用目的の多くは組織外部への情報漏えい防止を目的として活用している。また、導入した大半のシステムが、効果があったと回答しており、導入による効果が高いことが確認できた。

ウ　未知の不正プログラム対策ソフトウェアの導入状況

各組織の基幹システムについては高い導入率がみられた。使用製品としては、シグネチャマッチ型アンチウィルスソフトのオプション機能として提供されているものを利用している割合が大多数を占めている。

導入対象については端末だけではなくサーバへもほぼ同程度に進んでいる。それ以外のメールやWebアクセスの際にチェックを行うゲートウェイ型の製品も基幹システムにおいて同程度導入がされていた。

製品によっては誤検知、過検知への対応があるとしながらも、その効果が評価されていることが確認できた。

（２）管理者アカウントの管理状況の調査

政府機関等を対象としたペネトレーションテストにおいて、サーバやミドルウェア等の管理で使用される主体認証情報（ID、パスワード等）の管理不備に関する脆弱性が検出される例があった。識別コードと主体認証情報については、統一基準においても遵守事項として適切な管理を求めているところである。このことを踏まえ、攻撃者に知られると特に影響が大きい管理者権限を持つ識別コード及び主体認証情報（以下、「管理者アカウント」という。）の管理状況について検査を行った。

管理者アカウントを適切に管理するには、まず情報システムに存在する管理者アカウントを網羅的に把握していることが必要である。これについては、おおむね全てのシステムにおいて、納入時の完成図書に記載させるなど、何らかの適切な措置が講じられている状況である。また、管理者権限を持つ識別コード及び主体認証情報が攻撃者によって窃取された際の被害を最小化するため、おおむね全てのシステムにおいて、何らかの適切な措置が講じられている。その例としては、業務ごとに異なる識別コードを設定する、管理者アカウントに与える権限を業務に必要な最小限に限定するなどが挙げられる。

主体認証情報は、攻撃者に容易に推測されないよう、十分な強度を持つものを設定する必要がある。これについては、大半のシステムにおいて、パスワードポリシーを制定する、さらにパスワードポリシーに反するパスワードを技術的に設定不可とするなどの措置が講じられている。多要素認証を導入しているシステムも一定数見られた。また、大半のシステムにおいて、主体認証情報が実際に適切なものとなっていることを監査や運用報告書等で確認している。

管理者アカウントを持つ担当者が異動等により業務を離れる場合、当該アカウントを速やかに廃止する必要がある。これについては、おおむね全てのシステムにおいて、管理者アカ

ウントの廃止申請や定期的な必要性確認などにより、当該アカウントを廃止する手順となっている。

別添４－４　高度サイバー攻撃への対処

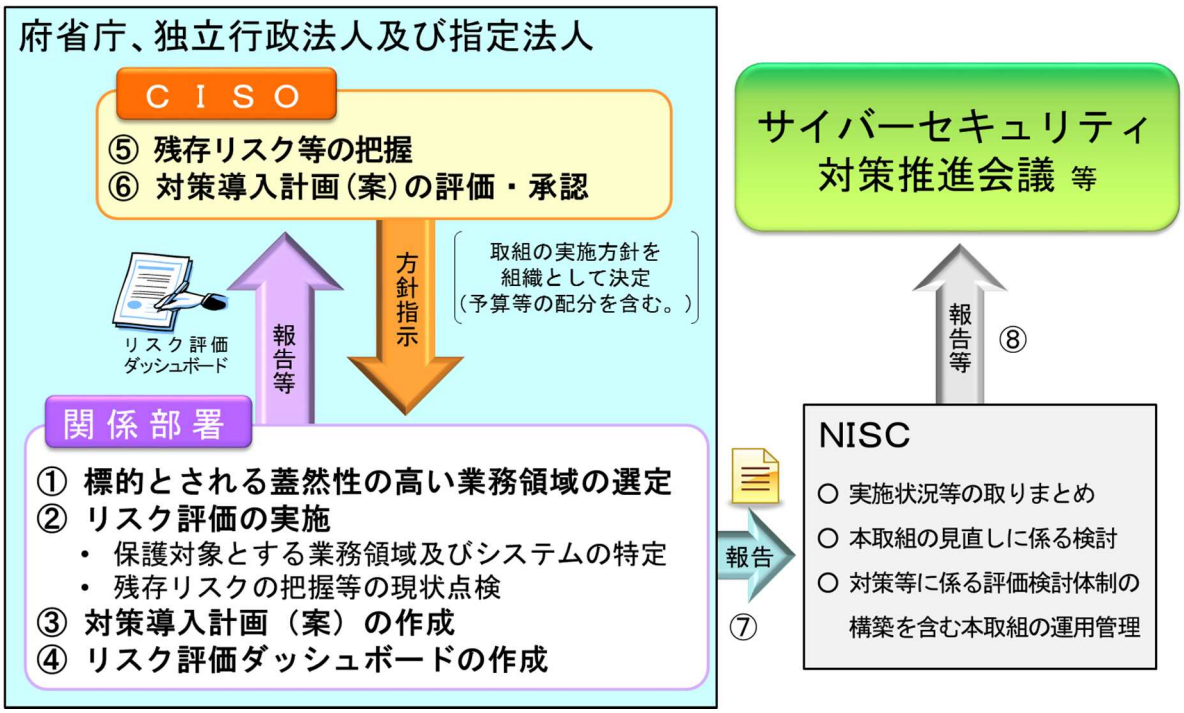
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

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。

2019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、2018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増しているが、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120の業務領域に使用されているおよそ50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。残るわずかな対策についても、今後のシステム更新等に合わせて計画的に対策の強化を図ることとしている。

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。

2019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、2018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増えており、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。具体的には、独立行政法人等全体で、ガイドラインに基づき保護対象に選定されたおよそ240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、遠隔操作用不正通信に係る対策や端末・サーバへの侵入拡大に係る対策などを中心に標的型攻撃に対する強化が図られていた。

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４－５　教育・訓練に係る取組

１　各府省庁 CSIRT 要員に対する訓練

（１）目的

各府省庁において、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。

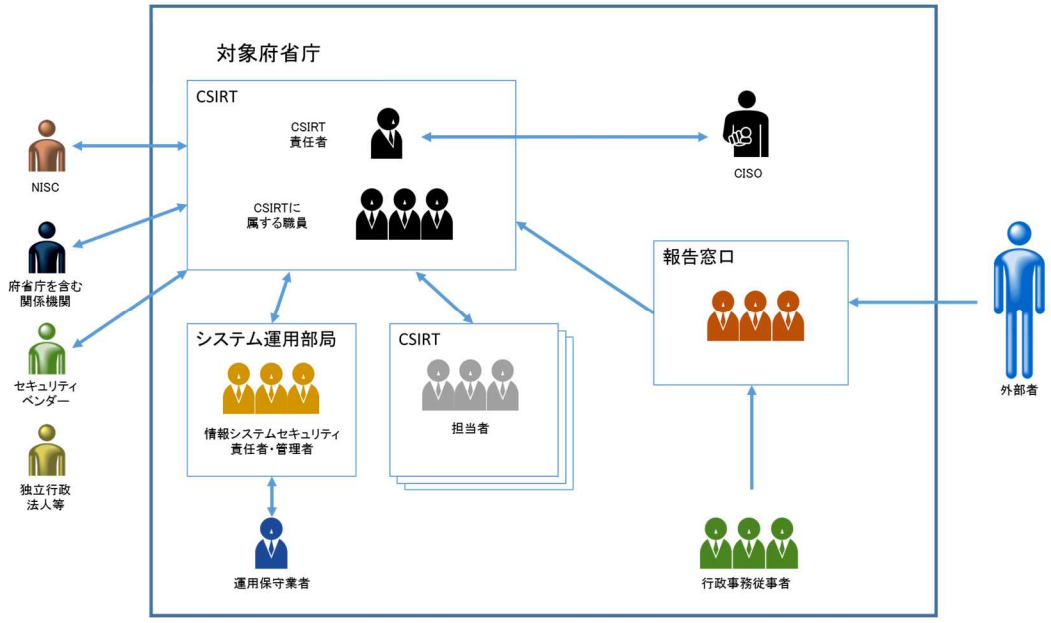
（２）概要

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。

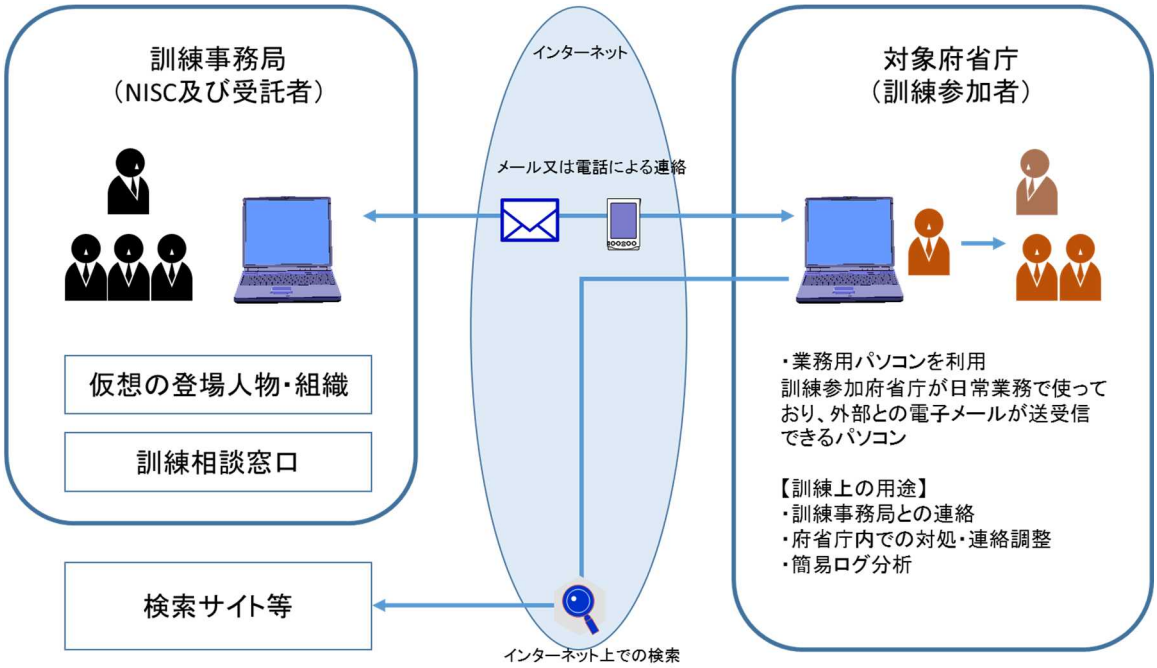
訓練参加者は、府省庁内外の様々な登場人物を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、状況に応じて通信ログ等の分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

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22府省庁参加）

（４）訓練時期

2020年１月～２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、2020年度以降のNISCの取組に反映していく。

２　各府省庁 CSIRT 要員に対する研修・勉強会

（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

各府省庁のCSIRT要員

（３）内容

No.	時期	テーマ	講師	参加人数
1	2019年 ６月～ 2020　年 １月	【CSIRT会合】 ・自府省庁のCSIRTをより良くしていくためにはどうすればよいか ・今のCSIRTで自組織を、日本を守れるのか？ ・府省庁CSIRTが警戒すべきサイバー犯罪　ほか	NISC職員、 外部講師	延べ約120名 （３回開催）
2	2019年 ７月～ 2020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 ・平成30・令和元年度のトピック　ほか	NISC職員、 外部講師	延べ約190名 （７回開催）
3	2020年 １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 ・グループディスカッション　ほか	外部講師	延べ約40名 （３回開催）

３　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独立行政法人等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

独立行政法人及び指定法人の CSIRT 要員

（３）内容

No.	時期	テーマ	講師	参加人数
1	2019 年 ７月～ 20209 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 ・平成 30・令和元年度のトピック　ほか	NISC 職員、 外部講師	延べ約 720 名 （７回開催）
2	2019　年 11 月	【CSIRT 会合（試行実施）】 ・CSIRT の現在地 ・グループディスカッション ・サイバーセキュリティ協議会の御紹介 ほか	NISC 職員、 外部講師	約 40 名 （１回開催）

４　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

No.	時期	テーマ	講師	参加人数
1	2019 年 ６月	・情報セキュリティ 10 大脅威とその対策 ・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）	外部講師 NISC 職員	延べ 280 名 （２回開催）

2	2019 年 ７月	・情報セキュリティ 10 大脅威とその対策 ・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）	外部講師 NISC 職員	延べ 81 名 （１回開催）
3	2019 年 ９月	・マネジメントシステム監査について	外部講師	延べ 184 名 （２回開催）
4	2019 年 12 月	・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）	NISC 職員	延べ 179 名 （２回開催）
5	2020 年 ３月	・マネジメント監査・ペネトレーションテスト実施結果の分析から得られた課題と対策	NISC 職員	（資料のみ配布）のみ配布）

図表３　NISC勉強会講義中の様子

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

2019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５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ぶとともに、情報セキュリティインシデントのケーススタディを通じたグループディスカッションを行ったほか、実機を用いた実習では、インシデントにおける攻撃側の行動と防御側の行動の双方の流れを体験した。

No.	時期	テーマ
1	2019 年 ５月	【座学①】 1. 令和 2 年度セキュリティ・IT 人材ポストに係る機構・定員要求等について 2. 次期 GSOC システムについて 3. 2020 年東京大会に向けた取組状況について（報告事項）
2	2019 年 ８月	【座学②】（IT 関係と合同実施） 1. デジタル手続法に基づく情報システム整備計画等の策定について 2. デジタル・ガバメント推進標準ガイドラインについて 3. 「サイバーセキュリティ戦略」等について 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」等について 5. 令和２年度機構・定員要求等について 6. サプライチェーン・リスク対応について 7. その他 8. 旅費業務の見直しに向けた改善案の点検について
3	2019 年 10 月	【座学③】 1. IoT 社会のサイバーセキュリティにおけるリスク・危機対応について 2. 政府の IT 調達に関する「申合せ」の運用について 3. その他
4	2019 年 12 月	【座学④】 1. インシデントハンドリングについて（座学） 2.「政府情報システムにおけるクラウドサービスの安全性評価制度の基本的枠組みについて（案）（仮称）」について
5	2020 年 ２月	【座学（演習）⑤】 1. サイバーセキュリティの取組強化等について

		2.クラウドサービスのセキュリティ評価制度に関する今後の調整について 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[1]。「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：2019 年８月～2019 年 12 月

受講者数：約 50 名

＜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	⑨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）(2)
②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）(1)	⑩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）(1)
③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)	⑪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）(2)
④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）(1)	⑫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）

[1]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。

⑤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)	⑬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）(1)
⑥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）	⑭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）(2)
⑦資産のセキュリティ（資産の保護）	⑮まとめと学力考査
⑧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）(1)	

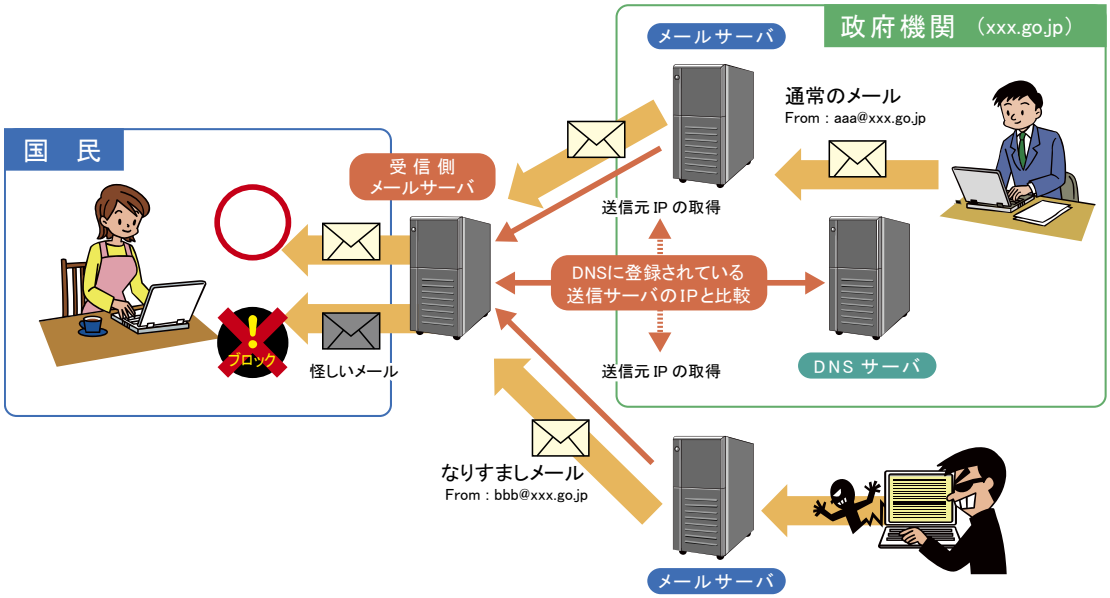
別添４－６　なりすまし防止策の実施状況

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[2]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。

[2] 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
2019 年１月末	69.7%	13.6%	16.7%
2020 年１月末	65.3%	16.5%	18.2%

※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、正当な電子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、適切な設定がされている割合がやや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の全体の約１割程度が消滅し、それを僅かに上回る新たなドメインが取得されているところであるが、その取得された一部のドメインで、推奨される設定がなされていない又は設定がなされていないSPFレコードを公開していることが、主な原因として挙げられる。今後は、新規のドメインに対し、然るべき設定がなされるよう、必要な取り組みを推進する。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[3]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。

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

別添４－７　暗号移行

2012年10月改定の「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」[4]に基づき、各政府機関で暗号移行が進められた。政府認証基盤及び電子認証登記所が発行する電子証明書は、2019年度末までに検証を終了した。

政府機関の暗号アルゴリズムに係る移行指針の改定概要

1　経緯

①電子政府システム（入札・申請等）において電子署名等のために広く使用されているSHA-1及びRSA1024と呼ばれる暗号方式の安全性の低下が指摘
②より安全な暗号方式（SHA-256及びRSA2048）への移行が必要であることから、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を策定

（H20年4月22日　情報セキュリティ政策会議決定）

2　政府機関における移行に向けた準備スケジュール

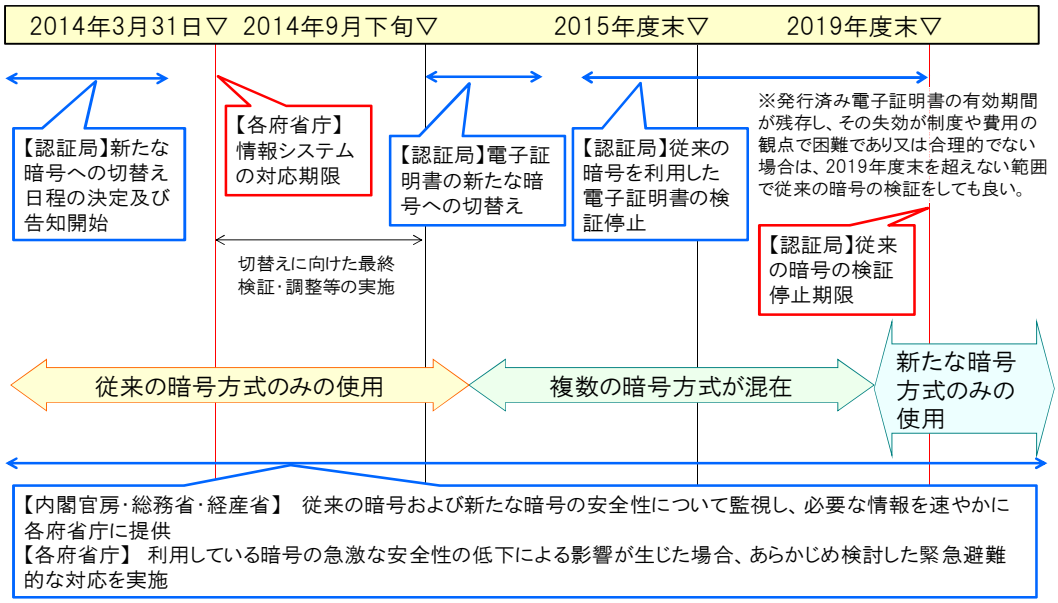
- 各府省庁が保有する情報システムの新たな暗号方式への対応時期　⇒「2013年度末まで」
- 新たな暗号方式による電子証明書の発行開始可能時期　⇒「2014年度早期」
- 従来の暗号方式による電子証明書の検証（有効性の確認）終了可能時期　⇒「2015年度早期」

（H21年2月3日　情報セキュリティ政策会議決定）

3　移行指針の改定概要

- 切替時期について各認証基盤との調整結果を踏まえ、以下のとおり改定
  政府認証基盤及び電子認証登記所が発行する電子証明書については、
  a.「2014年9月下旬以降、早期に」新たな暗号方式に切替
  b.「2015年度末までに」従来の暗号方式によって発行された証明書の検証を終了
  ただし、発行済み電子証明書の有効期間が残存し、やむを得ない場合は、「2019年度末まで」検証可

（参考）政府機関における暗号移行スケジュール



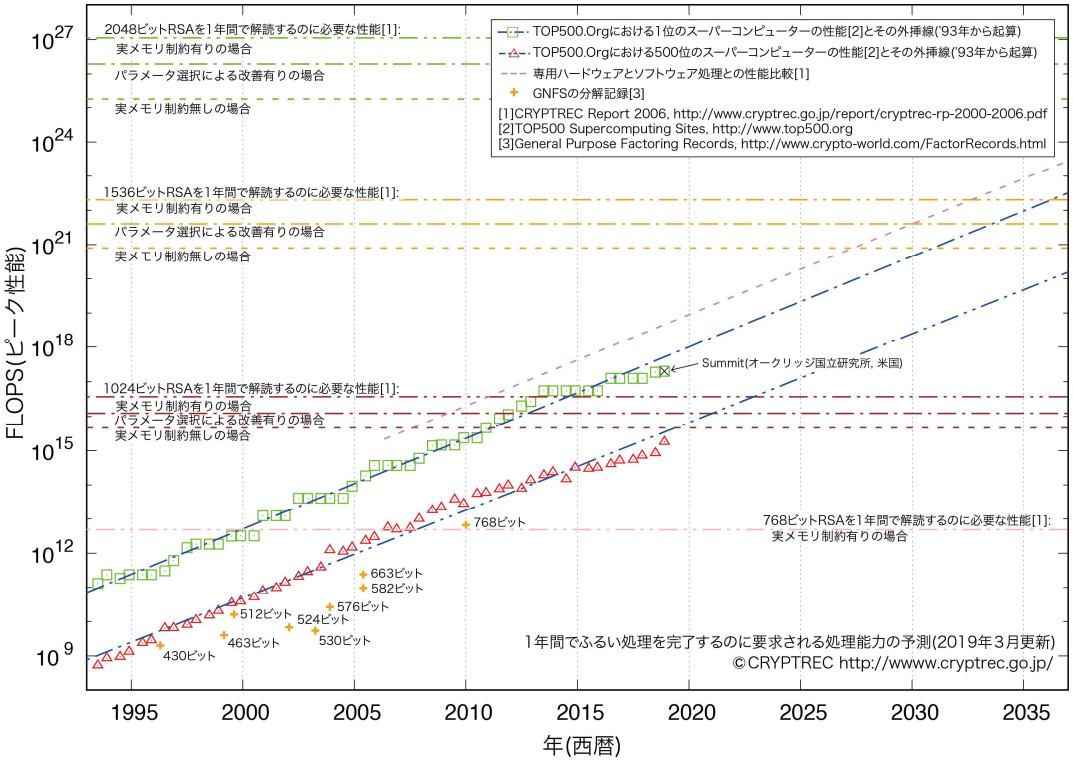
[4] https://www.nisc.go.jp/conference/suishin/index.html#2012_5
（第８回情報セキュリティ対策推進会議、2012 年 10 月 26 日）

（参考）暗号の危殆化

コンピュータの計算能力の向上により、セキュリティの基盤技術の一つである暗号技術の危殆化にも注視すべき状況となっている。2006年頃、当時のコンピュータの計算性能の向上予測から、従来政府機関で使われている公開鍵暗号アルゴリズムRSA（鍵長1024ビット）については、2010～2020年の間に危殆化する可能性があることが指摘された。

図表１は、計算機の出現年数に対して演算性能をプロットしたものである。出現当時、世界トップの性能を持つ計算機については（□）、世界500位相当の計算機は（△）でプロットされている。両者とも過去20年にわたりムーアの法則に近似した指数的な増加を示しているが、近年その性能の伸びは鈍化傾向にある。また、（＋）は学術会議等で報告された、実際に各ビット数の素因数分解を達成した計算機の演算性能を表している。

図表１　１年間でふるい処理を完了するのに要求される処理能力の予測（2019 年 3 月更新）[5]



[5] https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2018.pdf
「CRYPTREC Report 2018(暗号技術評価委員会報告)」(CRYPTREC)

別添４－８　独立行政法人、指定法人、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

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（2020年３月末日現在）

（２）調査時点

独立行政法人、指定法人　2019年12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

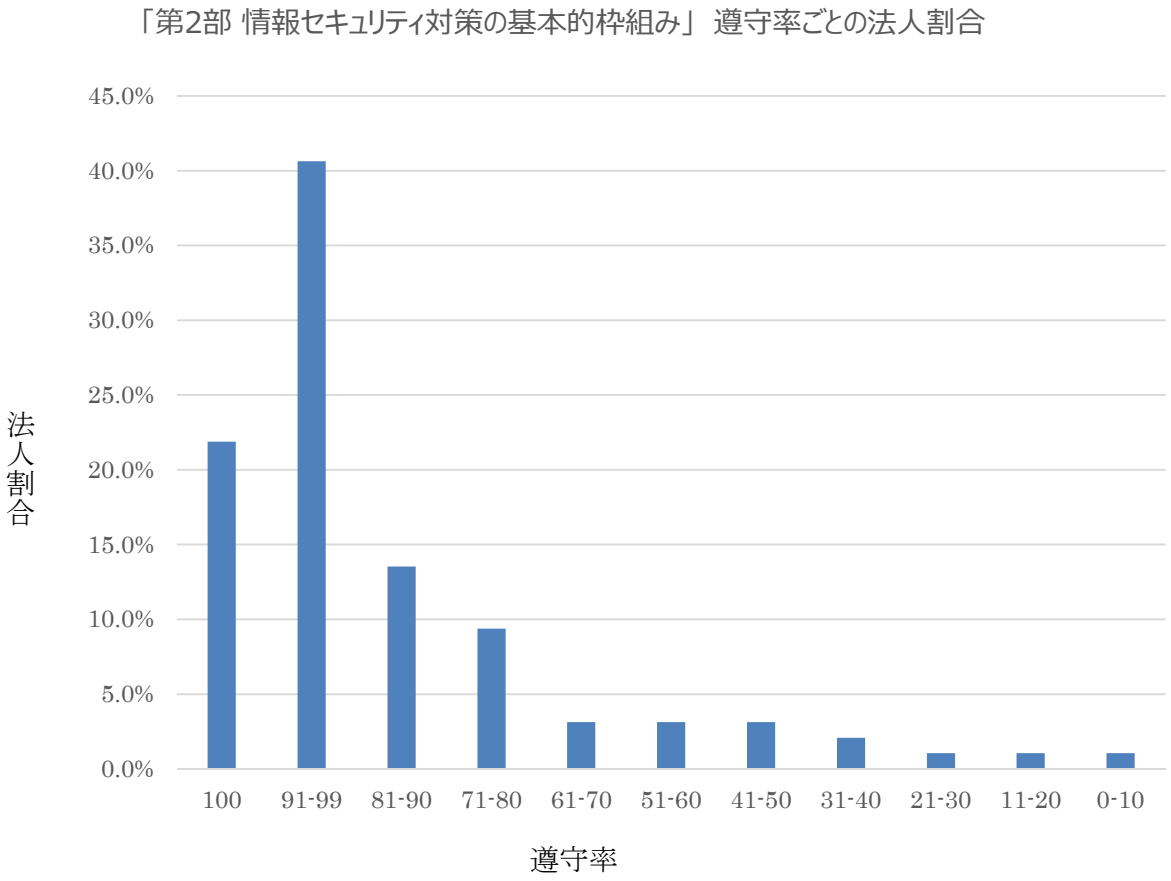
調査内容のガイドラインの構成は、部＞節＞款＞条＞項＞号＞基本対策事項、となっており、本報告での集計単位の遵守率とは、そこで要求されている遵守事項（条＞項＞号）および基本対策事項の全てに対する遵守率を示す。従って、部「第2部 情報セキュリティ対策の基本的枠組み」の遵守率100%とは、そこで要求されている遵守事項および基本対策事項（全160項目）全てを遵守していることを示す。同様に、款「2.1.1(1)　最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置」の遵守率100%とは、そこで要求されている遵守事項および基本対策事項（全6項目）全てを遵守していることを示す。

なお、法人割合とは、対象法人（96法人）を母数とした法人の割合を示す。

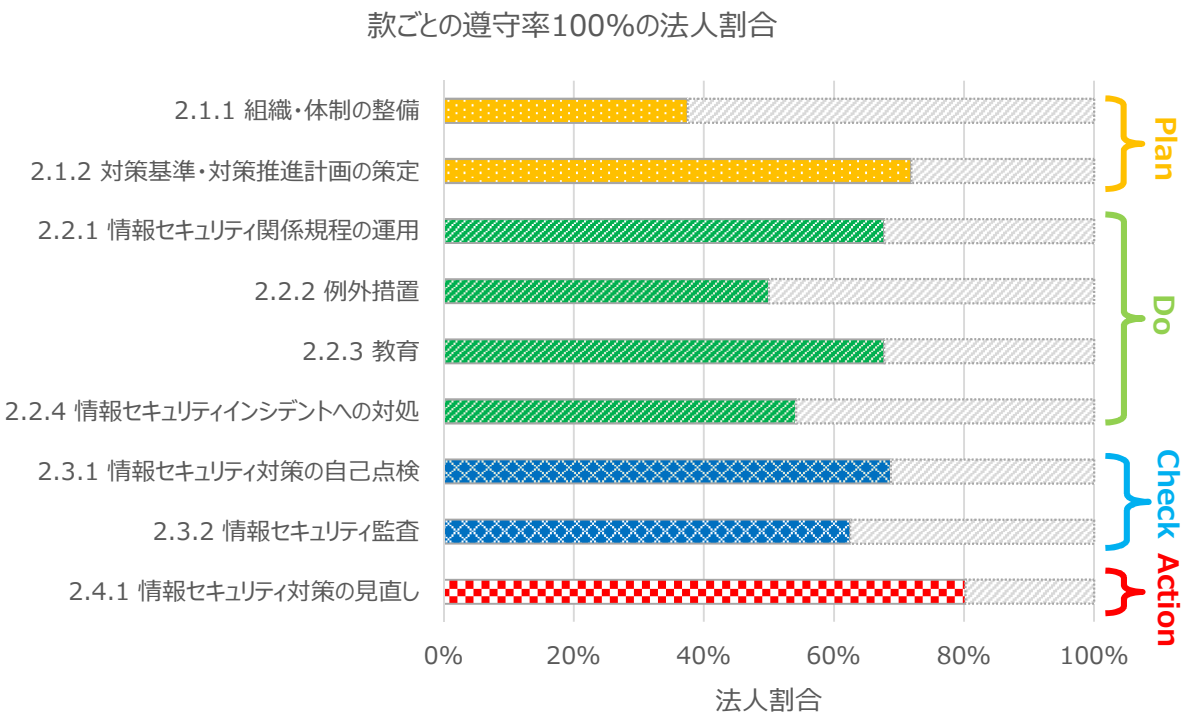
３　調査結果

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。

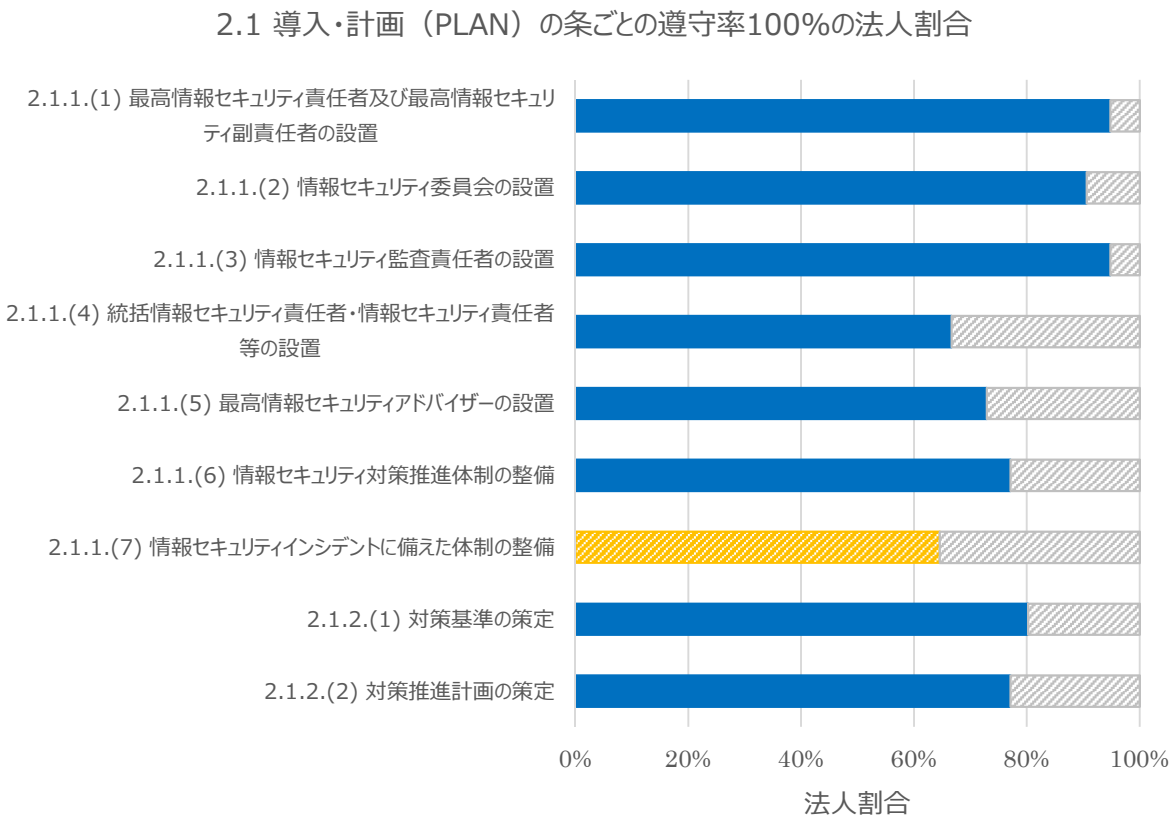


第２部の全てを遵守している法人の項番別の遵守割合については、以下のとおりであり詳細については、次ページ以降に記載する。



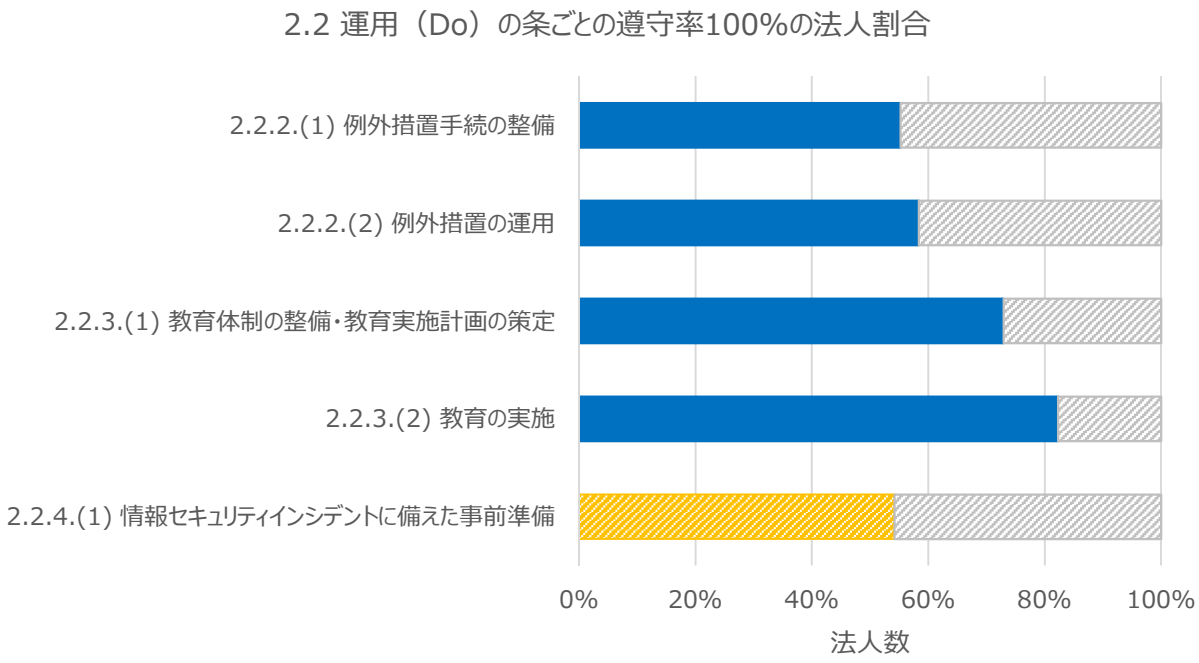
・統一基準の各款ごとの遵守割合では、各款の全てを遵守している法人は「2.1.1 組織・体制の整備」の遵守割合が 37.5%と最も低く、続いて「2.2.2 例外措置」、「2.2.4 情報セキュリティインシデントへの対処」の順となった。

（１）情報セキュリティ対策の導入・計画



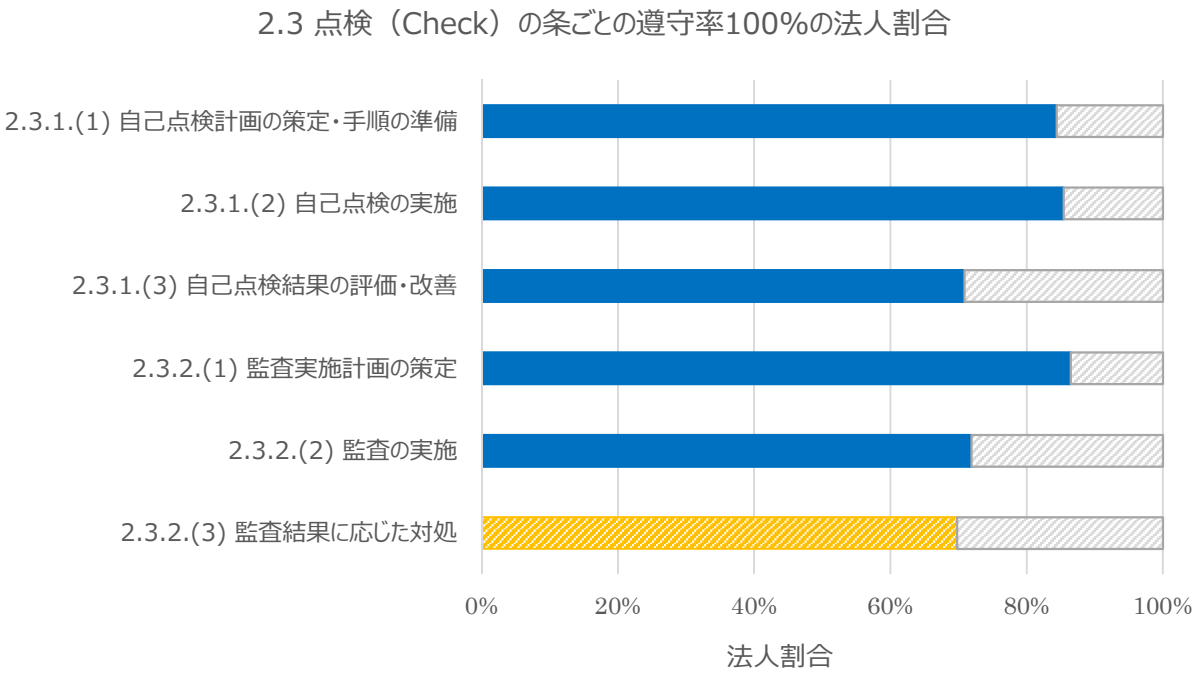
・「2.1　導入・計画」の各条の遵守率 100%の法人割合は、「2.1.1(7)　情報セキュリティインシデントに備えた体制の整備」の法人割合が 64.6%と最も低く、続いて「2.1.1.(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置」、「2.1.1.(5) 最高情報セキュリティアドバイザーの設置」の順となった。

（２）情報セキュリティ対策の運用



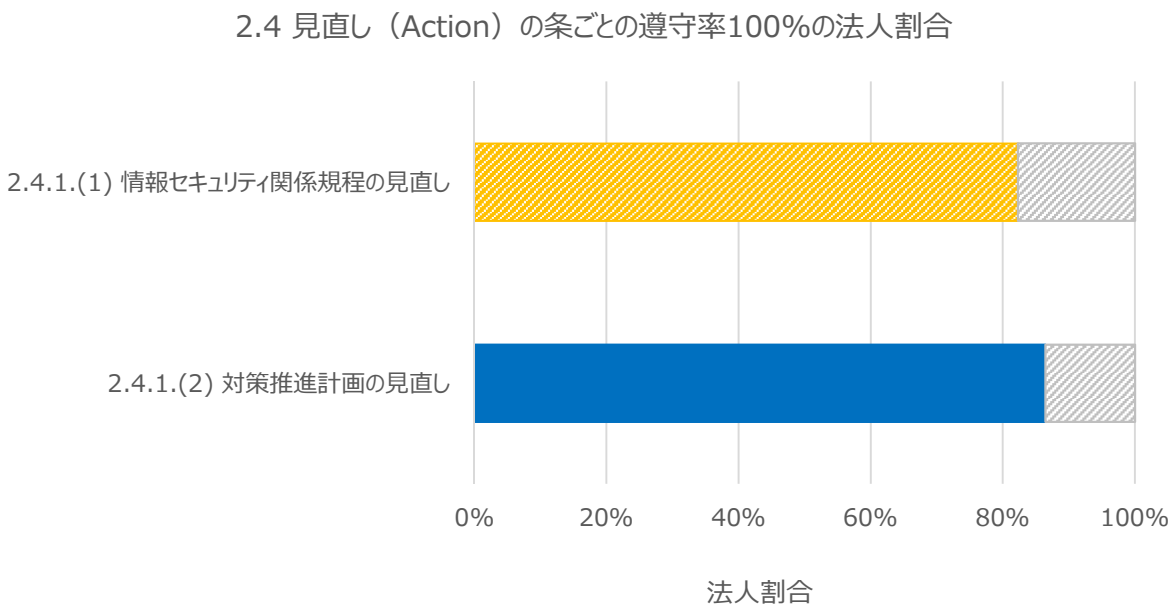
・「2.2 運用」の各条の遵守率 100%の法人割合は、「2.2.4.(1) 情報セキュリティインシデントに備えた事前準備」の法人割合が 54.2%と最も低く、続いて「2.2.2.(1) 例外措置手続の整備」、「2.2.2.(2) 例外措置の運用」の順となった。

（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%の法人割合は、「2.3.2.(3) 監査結果に応じた対処」の法人割合が 54.2%と最も低く、続いて「2.3.1.(3) 自己点検結果の評価・改善」、「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%の法人割合は、「2.4.1.(1) 情報セキュリティ関係規程の見直し」の法人割合が 82.3%と最も低くい結果となった。

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」に関して、そこで要求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の分布をみると、遵守率 90%以上の法人の割合は約 60%であり（うち遵守率 100%の法人は約 20%）、半数以上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%以下の法人の割合は８%あり、これらの法人の対策推進は急務である。また、情報セキュリティ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サイクルの観点からみると、P（導入・計画）「2.1.1 組織・体制の整備」の遵守率 100%の法人割合が 40%以下と低く、役割と責任を明確にした組織・体制の整備が必要だと推察する。

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

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（2020年３月末日現在）

（２）調査時点

国立大学法人、大学共同利用機関法人、国立高等専門学校　2020年3月末日

（３）調査内容

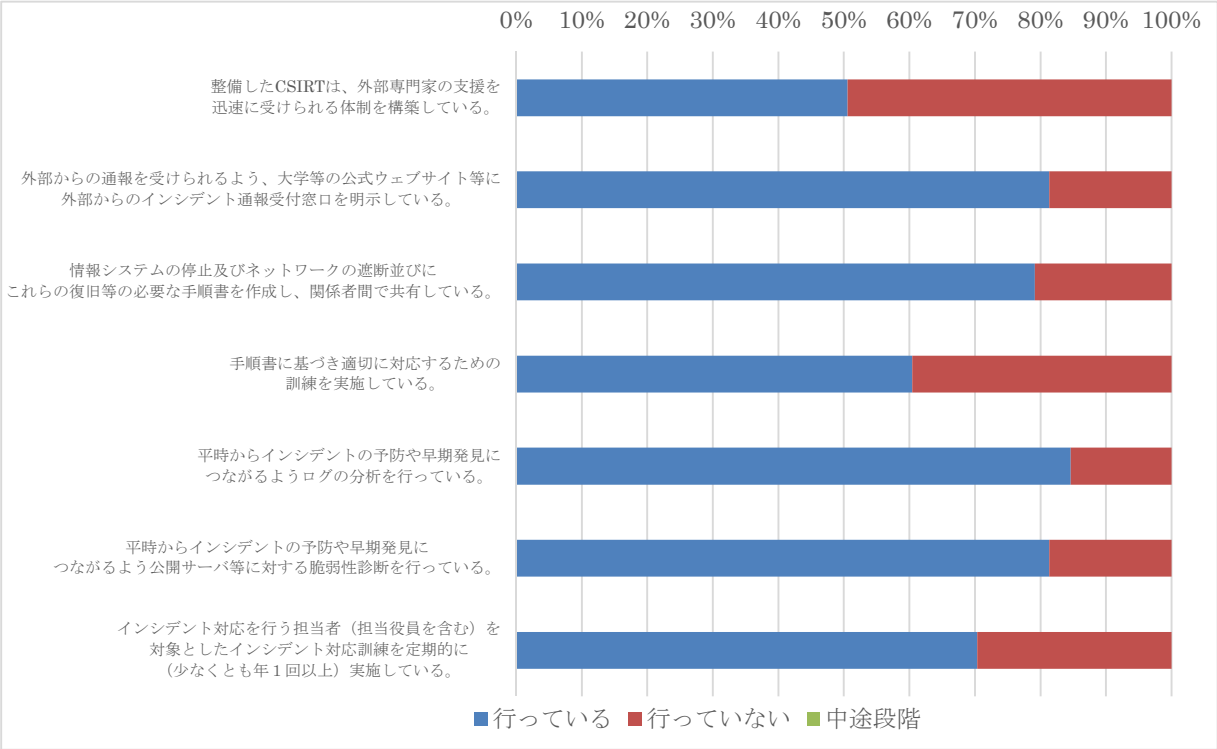
元文科高第５９号「大学等におけるサイバーセキュリティ対策等の強化について」の実施状況について回答を依頼した。

３　調査結果

国立大学法人、大学共同利用機関法人、国立高等専門学校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。

（１）実効性のあるインシデント対応体制の整備



91 法人についてはすべて CSIRT を整備済みであるため、その機能等について調査を行った。

・外部専門家の支援を迅速に受けられる CSIRT 体制を構築している法人は 46 法人（50%）である。

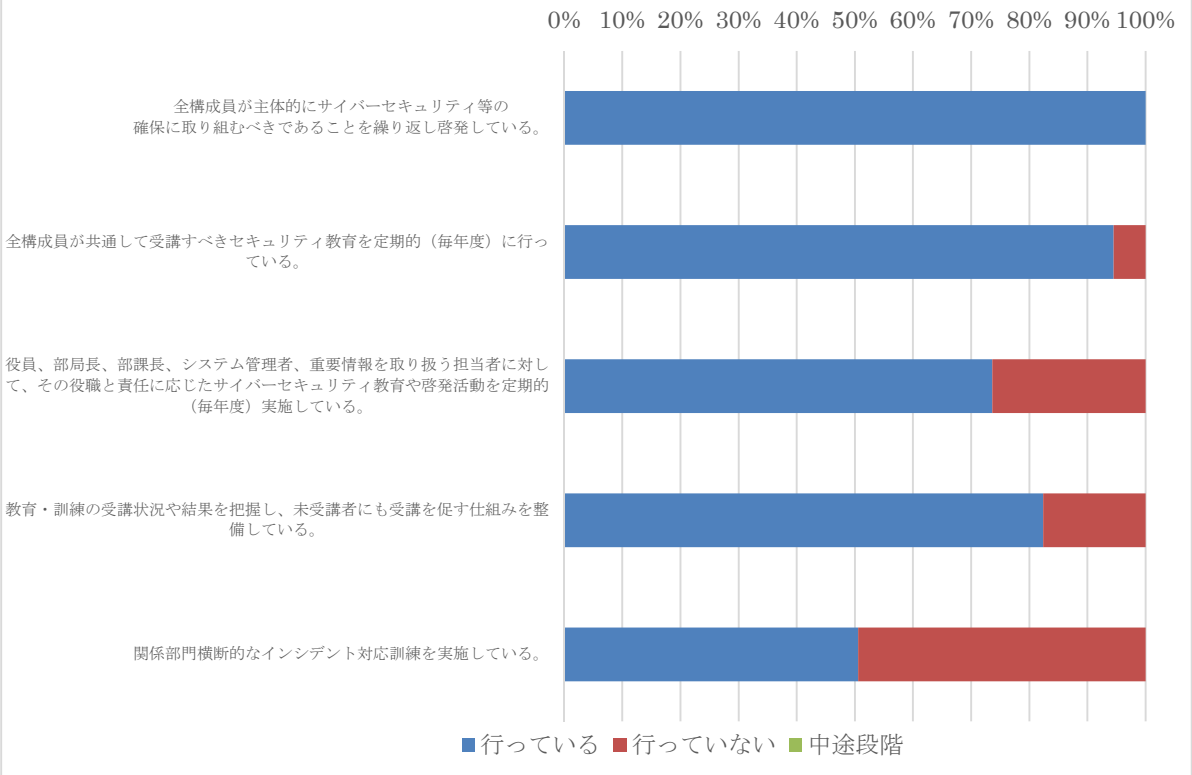
・外部からの通報を受けられるよう、大学等の公式ウェブサイト等に外部からのインシデント通報受付窓口を明示している法人は 74 法人（82%）である。

・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 72 法人（79%）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 55 法人（60%）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（70%）である。

（２）サイバーセキュリティ等教育・訓練・啓発活動の実施



・全構成員が主体的にサイバーセキュリティ等の確保に取り組むべきであることを繰り返し啓発している法人は 91 法人（100%）である。

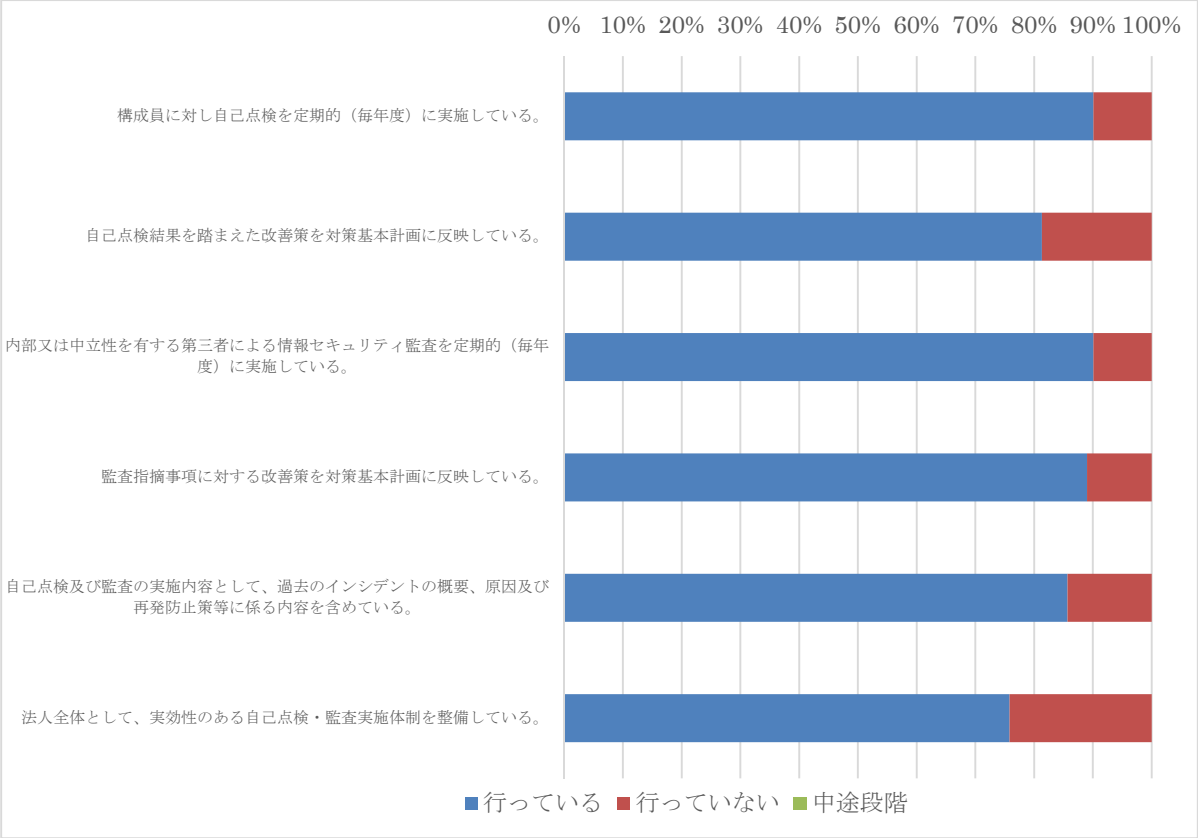
・全構成員が共通して受講すべきセキュリティ教育を定期的（毎年度）に行っている法人は 86 法人（95%）である。

・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 67 法人（74%）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（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 46 法人（50%）である。

（３）情報セキュリティ対策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（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 74 法人（81%）である。

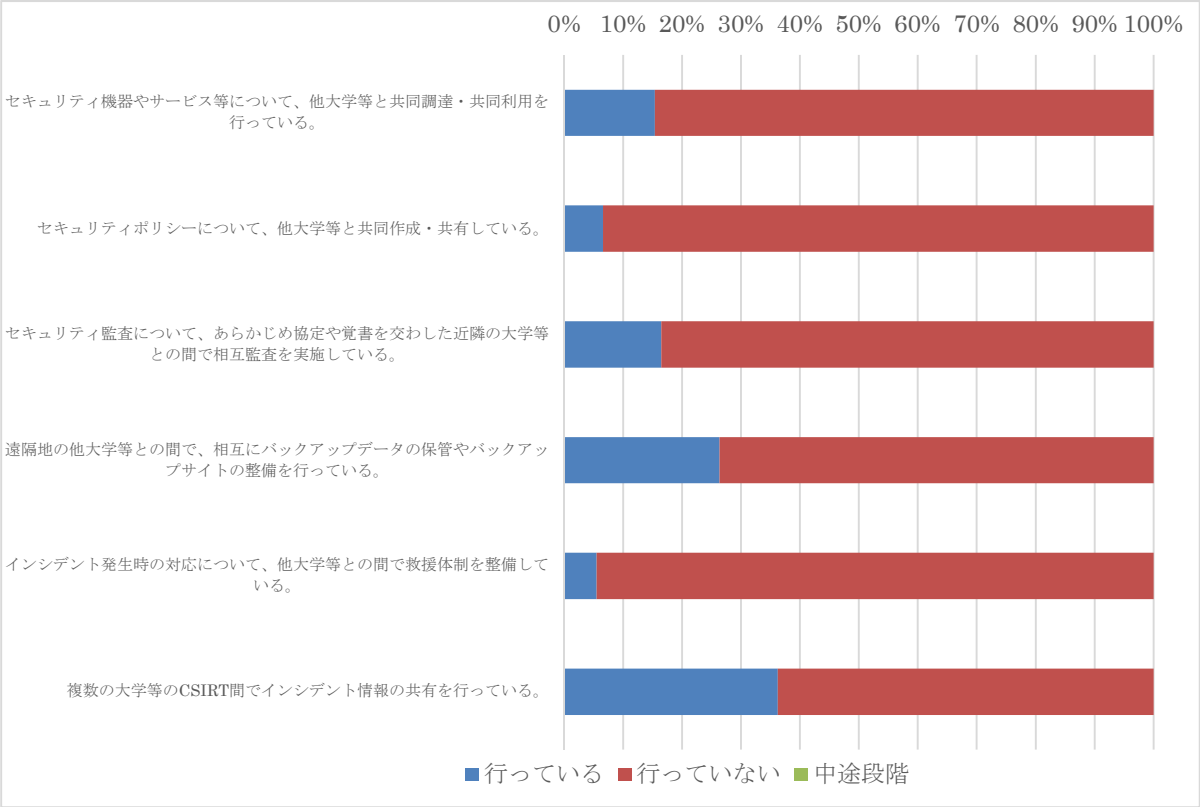
・内部又は中立性を有する第三者による情報セキュリティ監査を定期的（毎年度）に実施している法人は 82 法人（90%）である。

・監査指摘事項に対する改善策を対策基本計画に反映している法人は 81 法人（89%）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、78 法人（86%）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 69 法人（76%）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 14 法人（15%）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（7%）である。

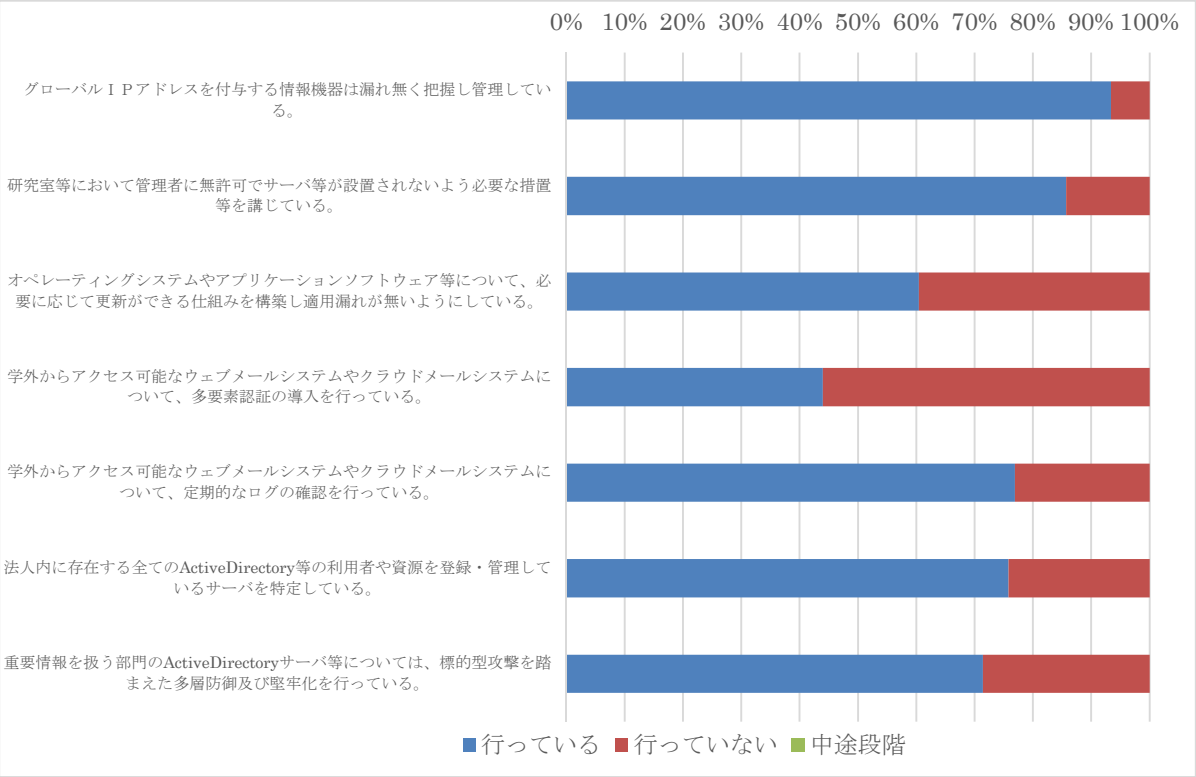
・セキュリティ監査について、あらかじめ協定や覚書を交わした近隣の大学等との間で相互監査を実施している法人は 15 法人（16%）である。

・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、24 法人（26%）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 5 法人（5%）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 33 法人（36%）である。

（５）必要な技術的対策の実施



・グローバルＩＰアドレスを付与する情報機器は漏れ無く把握し管理している法人は 85 法人（93%）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 78 法人（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 55 法人（60%）である。

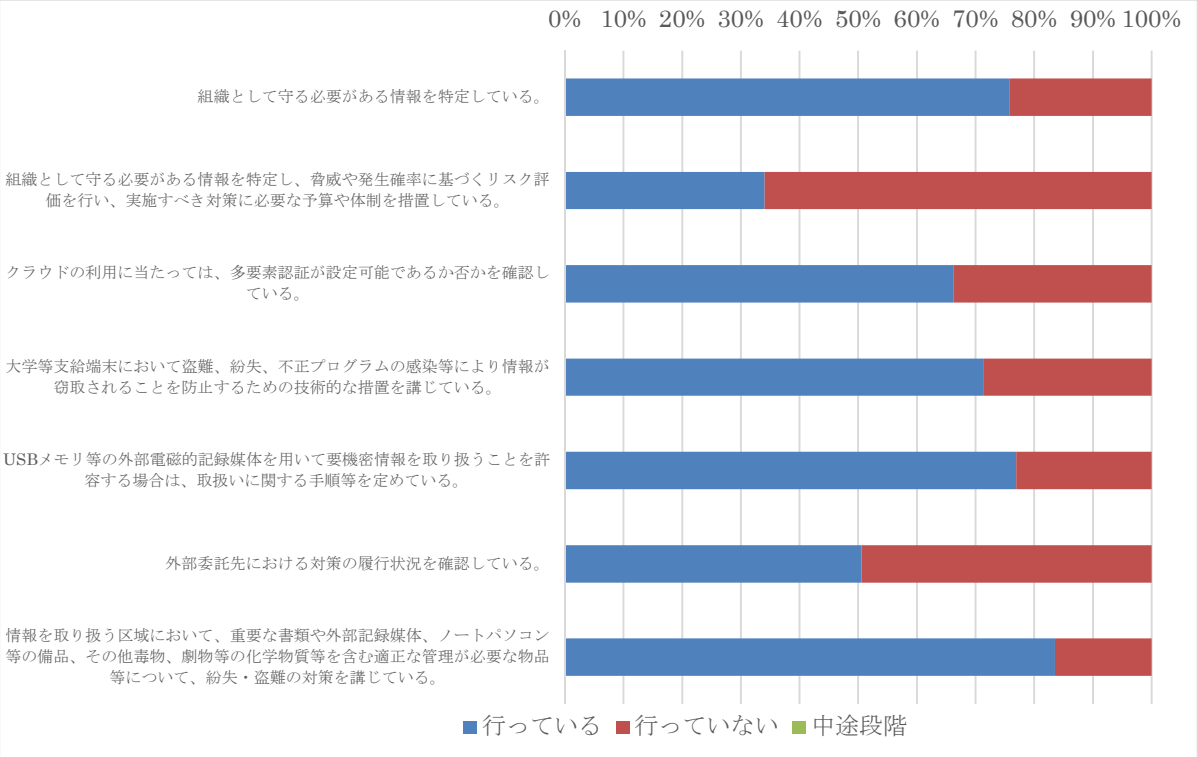
・学外からアクセス可能なウェブメールシステムやクラウドメールシステムについて、多要素認証の導入を行っている法人は 40 法人（44%）である。

・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、定期的なログの確認を行っている法人は 70 法人（77%）である。

・法人内に存在する全ての ActiveDirectory 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 69 法人（76%）である。

・重要情報を扱う部門の ActiveDirectory 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 65 法人（71%）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 69 法人（76%）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、実施すべき対策に必要な予算や体制を措置している法人は 31 法人（34%）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 59 法人（66%）である。

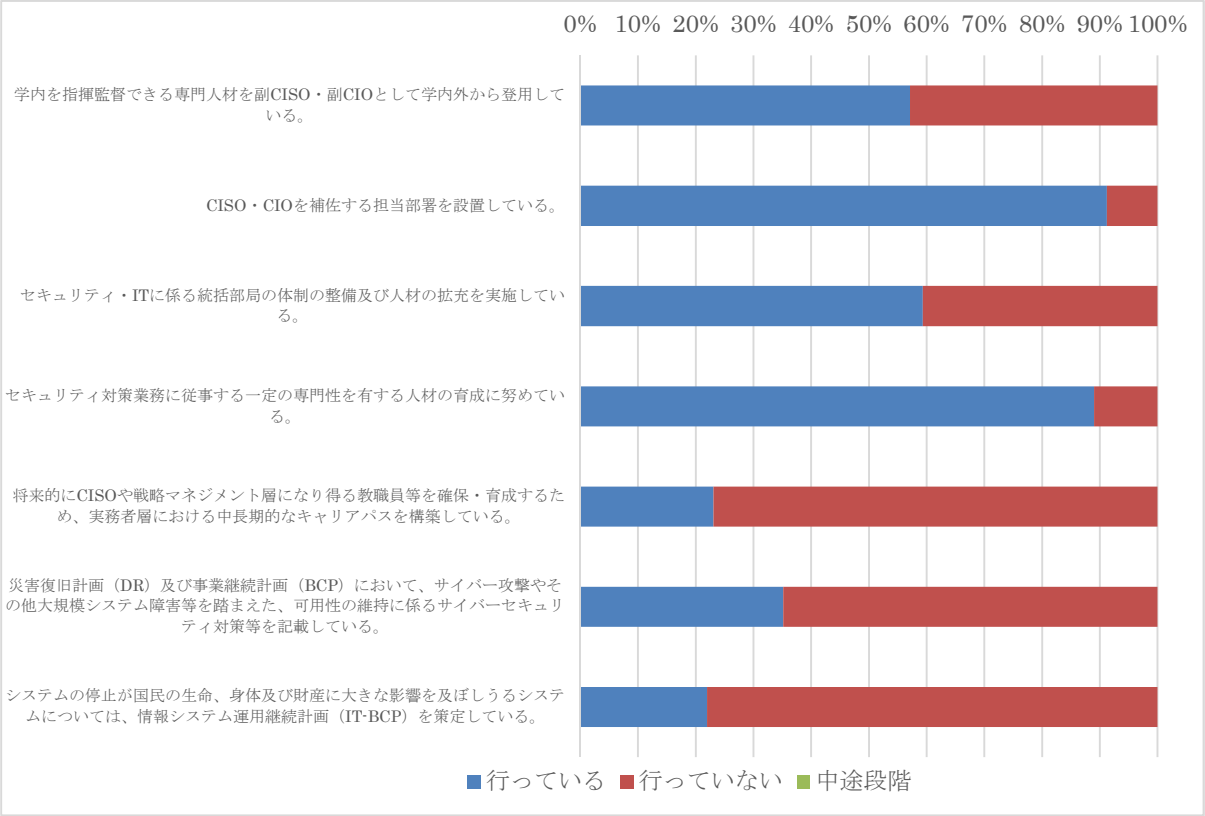
・大学等支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置を講じている法人は 65 法人（71%）である。

・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 70 法人（77%）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 46 法人（50%）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 76 法人（84%）である。

（７）国立大学法人等が対応すること



・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 52 法人（57%）である。

・CISO・CIO を補佐する担当部署を設置している法人は 83 法人（91%）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 54 法人（59%）である。

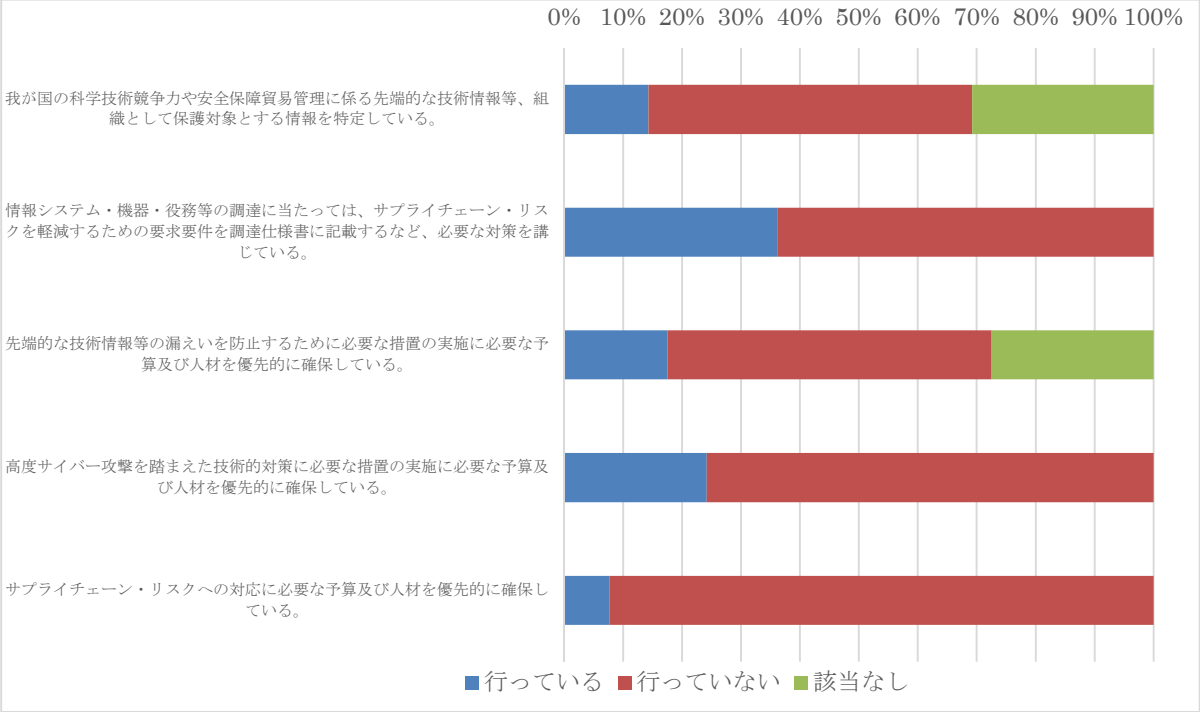
・セキュリティ対策業務に従事する一定の専門性を有する人材の育成に努めている法人は 81 法人（89%）である。

・将来的に CISO や戦略マネジメント層になり得る教職員等を確保・育成するため、実務者層における中長期的なキャリアパスを構築している法人は 21 法人（23%）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 32 法人（35%）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 20 法人（22%）である。

（８）先端的な技術情報等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 13 法人（14%）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 33 法人（36%）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 16 法人（18%）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 22 法人（24%）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 7 法人（8%）である。

４　各法人の対応

調査対象の法人にはすべて CSIRT が設置されているが、その機能や実効性については各法人で差が見られる。情報セキュリティインシデントへの備えとして、外部専門家の支援を迅速に受けられる体制の構築や、手順書に基づき適切に対応するための訓練体制を強化する等により、情報セキュリティインシデント発生時の初動対応のより一層の迅速化を図る必要がある。また、関係部門横断的なインシデント対応訓練についても実施し、情報セキュリティインシデント発生時の関係部門との連携についても併せて強化していく必要がある。

なお、セキュリティ機器の共同調達、ポリシーの策定、相互監査といった他機関との連携・協力については、効率化の観点から、各組織間での連携・協力を行っていくことが望ましいと考えられる。

必要な技術的対策については、情報セキュリティインシデント防止の観点から、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の構築を行う必要や、外部からアクセス可能なウェブメールシステム及びクラウドメールシステムについて、多要素認証などの対策を導入していく必要がある。

また、自律的かつ計画的な情報セキュリティ対策を実施していくためには、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、実施すべき対策に必要な予算や体制を措置する必要がある。また、外部委託先における対策の履行状況を確認することも重要である。

国立大学法人等が対応することとして、専門的人材としての副 CIO・副 CISO の設置を行うことや、将来的に CISO や戦略マネジメント層になり得る教職員等を確保・育成するため、実務者層における中長期的なキャリアパスを構築していくことが望まれる。また、BCP 体制の構築・見直しを通じ、大規模システム障害時の対応能力を高めることも重要である。

とりわけ、先端的な技術情報等を保有する大学等が対応することとして、先端的な技術情報等の漏えいの防止、高度サイバー攻撃を踏まえた技術的対策及びサプライチェーン・リスクへの対応に必要な予算及び人材の各大学等おける優先的・計画的な確保が望まれる。

以上から、大学等が教育・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にも、「サイバーセキュリティ戦略」に示された３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）を踏まえつつ、サイバー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着実かつ継続的に実施していくことが重要である。

別添４－９　政府機関等に係る 2019 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
2019 年	４月	【概要】千葉大学は 17 日、学外からアクセス可能なウェブサーバ上に、平成 18 年当時に工学部に開講されていた科目に関する学生 81 名の個人情報を、削除しないまま保管していたことを公表した。	その他
	５月	【概要】鹿屋体育大学は 13 日、学生１名のクラウドサービスアカウントに不正アクセスがあり、該当アカウントから 319 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
		【概要】佐世保共済病院は 31 日、放射線検査機器に接続したパソコンからコンピュータウイルスを検知した為、被害拡大防止のため全てのネットワークを遮断したことで、一部診療制限が発生していることを公表した。	その他
	７月	【概要】高齢・障害・求職者雇用支援機構石川職業能力開発短期大学校は 10 日、ウェブサイトにおいて利用していた外部サービスが原因で、利用者の画面に不適切なウェブサイトが表示されたことを公表した。	その他
		【概要】原子力規制庁は 12 日、新卒採用の一般職向け説明会の参加者 250 名に対して一斉送信する際、BCC ではなく誤って To で送信したと公表した。 【対応等】11 日に庁内全職員に対して注意喚起を実施し、原子力規制委員会における情報管理を一層徹底した。	意図せぬ情報流出
		【概要】日本年金機構は 23 日、国民年金納付督励業者から東京広域事務センターに送付された、個人情報が収録された国民年金納付督励事績データ DVD（収録情報は暗号化）を紛失したことを公表した。	その他
	８月	【概要】国立病院機構四国こどもとおとなの医療センターは２日、同院を退院した者 299 名分の個人情報が記録された USB メモリを紛失したことを公表した。	その他
		【概要】環境省が行っていた家電エコポイント制度、住宅エコポイント制度、復興住宅エコポイント制度のウェブサイトで用いていたドメインが第三者に取得され、無関係のウェブサイトとなっていることがわかった。 【対応等】22 日、環境省は当該ウェブサイトについて環境省とは関係ない旨及び残存する過去のリンクの削除について注意喚起した。	その他
		【概要】熊本労働局は 29 日、八代労働基準監督署において、電子申請によりある事業所から提出された「時間外・休日労働に関する協定届」を審査し、控えを送信する際に、誤って別の事業所の協定届の控えを送信したことを公表した。 【対応等】八代署は、職員に対し、書類の控えを送信する際は、添付ファイルの内容を必ず確認すると共に、宛先と添付ファイル内容に齟齬がないか、送信する前に他の職員の確認を受けるよう指示した。 また、熊本労働局は、局内の全ての各課室及び管下の全ての労働基準監督署、公共職業安定所に対して事案の概要を周知すると共に、個人情報漏えい防止の基本動作・確認作業の徹底を指示した。	意図せぬ情報流出
		【概要】富山大学は 30 日、同大学の学生 320 名分の個人情報が保存された USB メモリを紛失したことを公表した。	その他
	９月	【概要】国立成育医療研究センターは 25 日、看護職員ウェブサイトに不正アクセスがあったことを公表し、11 月１日、当該ウェブサイトが改ざんされ、ウェブメールサービス等を模倣したフィッシングサイトが設置されていたことを公表した。	外部からの攻撃
	10 月	【概要】大阪大学は３日、関係機関と大学との間で過去にやり取りされたメールに返信するような形で、大学を騙ったウイルス付きのメールが発信されている事を確認したと公表した。	外部からの攻撃
		【概要】金沢大学は４日、職員がメールにより誘導されたフィッシングサイトにより、同大学職員 25 名のメールアカウントのパスワードが窃取されたとともに、一部の侵害されたアドレスから９月 20 日～９月 27 日にかけて計 41,697 件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

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】神戸大学は 24 日、大学の構成員が過去にやり取りしたメールを引用するような形で、大学を騙ったウイルス付きのメールが発信されていることを確認したと公表した。	外部からの攻撃
	11 月	【概要】気象庁の報道発表を装った迷惑メールが出回った。 【対応等】６日、気象庁はウェブサイトで注意喚起した。	その他
		【概要】室蘭工業大学は８日、同大学のウェブサーバ上で同大学の学生 1,187 名及び同大学が設置した外部評価委員会委員等 14 名分の個人情報が記載されているファイルが外部から閲覧できる状態になっていたことを公表した。	その他
		【概要】島根大学は 15 日、同病院の患者 244 名分の個人情報が保存された USB メモリを紛失していたことを公表した。 ９月５日に USB メモリの所有者である医師に対し拾得者から連絡があったことから、担当教授へ報告があり、問題が明らかとなった。同院では９月 14 日に USB メモリを回収済み。	その他
		【概要】徳島大学は 20 日、同大学病院の医師が海外出張中に、患者の個人情報 3,217 件が保存された PC 及び同大学の職員の情報約 1,000 件が保存された業務用携帯電話を収めた鞄を盗まれたことを公表した。	その他
	12 月	【概要】地域医療機能推進機構は９日、群馬中央病院が運用している事務処理用 PC１台がマルウェア「Emotet」に感染していることを公表した。	その他
		【概要】自然科学研究機構は 26 日、総合研究大学院大学の学生が海外で車上荒らしの被害に遭い、研究関係者等の個人情報が含まれた機構資産 PC を紛失したと公表した。	その他
2020 年	１月	【概要】国立病院機構近畿中央呼吸器センターは 17 日、新薬開発の臨床試験に参加した患者 15 名分の治験データが匿名化されないまま新薬の開発主体である治験依頼者に提供されていたことを公表した。	意図せぬ情報流出
		【概要】省内で情報共有するためのメールが、外部の報道機関へ誤送信された。 【対応等】作業時の確認作業の徹底を指示した。	意図せぬ情報流出
		【概要】お茶の水女子大学は 28 日、同大学研究室メールサーバの脆弱なパスワードが設定されたメールアカウント１件が侵害され、308 万通のフィッシングメールの送信に悪用されたことを公表した。	外部からの攻撃
		【概要】神戸大学は 28 日、同大学病院において、患者の情報と口腔内及びその周辺の写真が保存されたデジタルカメラを紛失したことを公表した。	その他
	２月	【概要】東京農工大学は５日、同大学職員２名が使用しているメールアカウントの情報が窃取されたため不正アクセスを受け、個人情報が漏洩するとともにフィッシングメールの送信に利用されたことを公表した。	外部からの攻撃
		【概要】長岡技術科学大学は７日、同大学職員１名のメールアカウントの情報が窃取されたため不正アクセスを受け、当該アカウントから大量のスパム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】厚生労働省は 10 日、ハローワークシステムの不具合により、ハローワークが求人事業所に紹介した求職者の氏名等が、紹介先ではない事業所に誤って通知され、事業所（６社）が、別の求人事業所名（６社）と求職者氏名（６名）の記載が含まれたファイルを開封したことを公表した。 【対応等】原因となった機能のプログラム改修を行った。また、他の機能についても、同様の不具合がないか点検するとともに、今後のシステム開発においても同様の不具合を発生させないようシステム開発のルールを整備・徹底することとした。	意図せぬ情報流出
		【概要】厚生労働省東京労働局は 27 日、委託事業受託者において、３名に対して予約確認に関するメールを送信したところ、メール内容に誤って同日に送信した別の１名へのメール全文が付随してしまい、氏名及びメールアドレスが漏えいしたことを公表した。 【対応等】メール送信前におけるダブルチェックによる内容確認の徹底や、全職員に対して今回発生したメール誤送信の経緯、原因及び再発防止策を踏まえた個人情報の適正な管理についての研修を実施することについて、委託事業受託者に対して指示をした。	意図せぬ情報流出

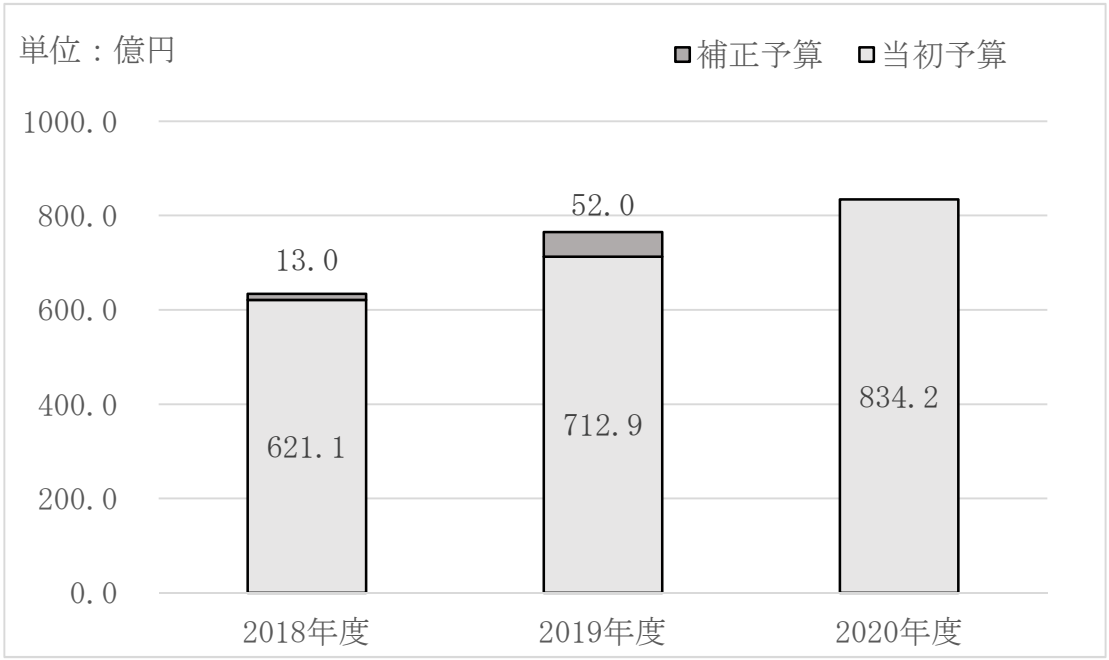
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】岡山大学は 28 日、同大学職員１名のメールアカウントの情報が窃取されたため不正アクセスを受け、当該アカウントから約 150 万件の迷惑メールが送信されたことを公表した。	外部からの攻撃
	３月	【概要】厚生労働省国立感染症研究所は４日、旧公式ウェブサーバからあるプライベートな掲示板に１件の不正な書き込みがあり、当該サーバを調査したところ、過去に設置したままであったアプリケーションに通常存在しないプログラムが起動されている証跡を発見したことを公表した。 【対応等】当該サーバの機能を閉鎖し、侵入方法の検証等を行うこととした。	外部からの攻撃
		【概要】鹿児島大学は 13 日、第三者からの不正ログインにより、Web サイト内のサイトマップページが改ざんされ、海外からの投稿記事が掲載されたことを公表した。	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

	2018 年度	2019 年度	2020 年度
当初予算額	621.1 億円	712.9 億円	834.2 億円
補正予算額	13 億円	52 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

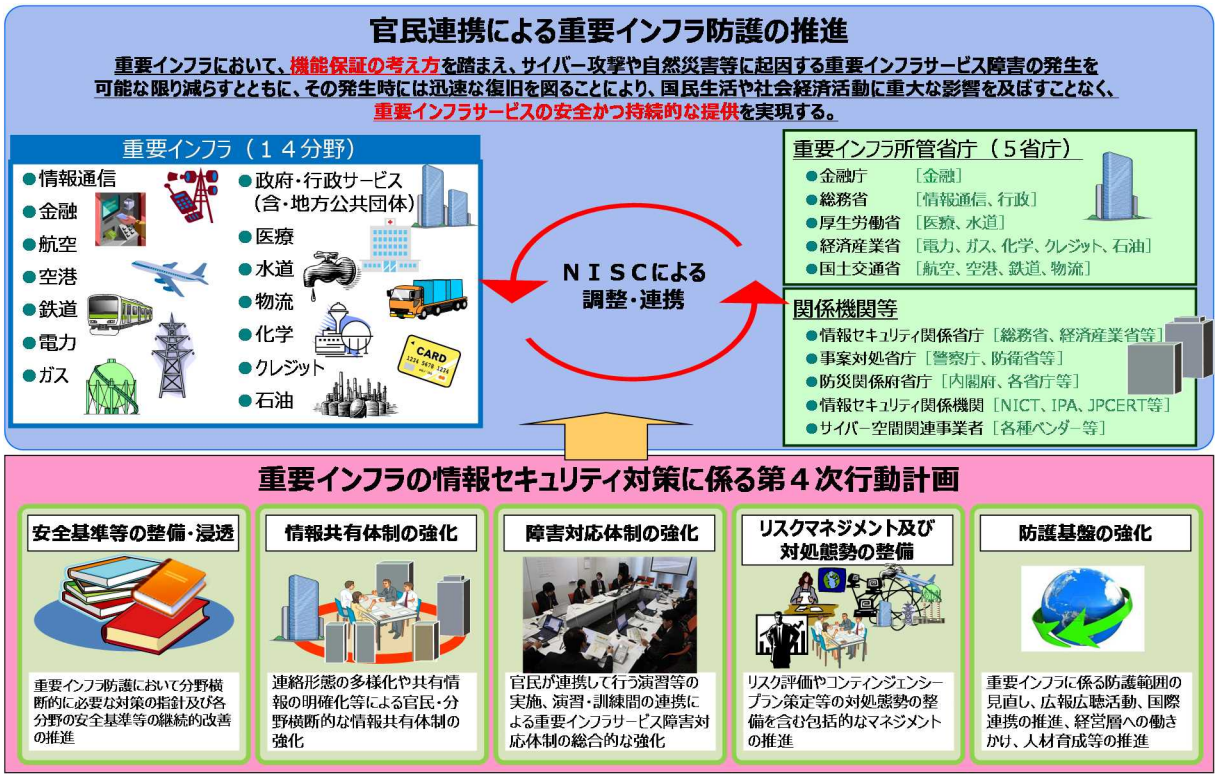
■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 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

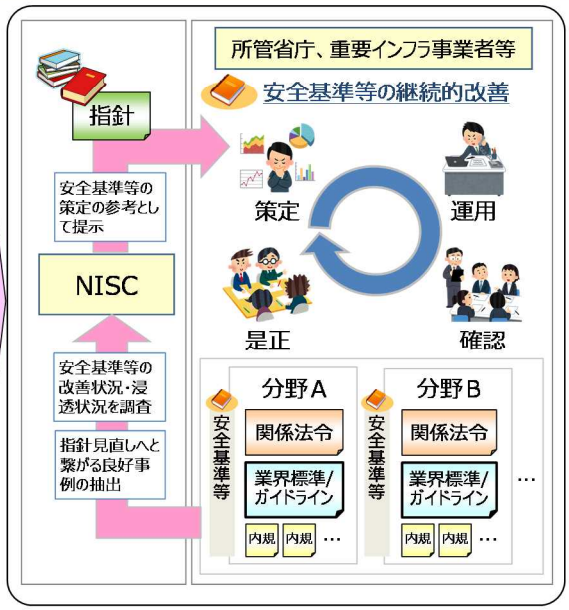
行動計画期間中の施策

（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

行動計画期間中の施策

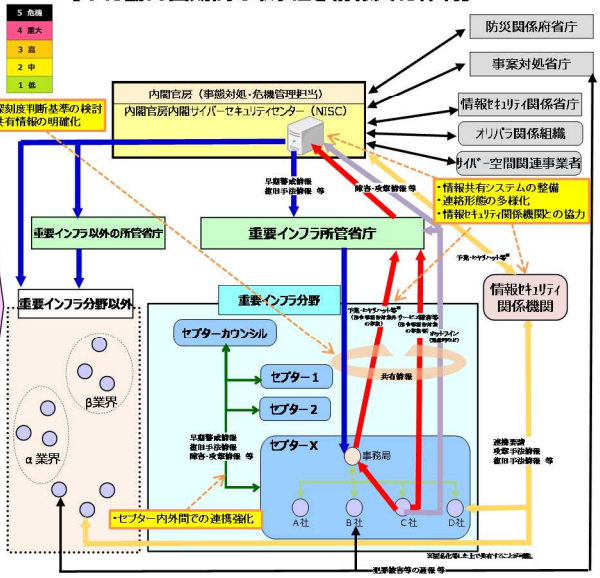
（１）情報共有体制の充実
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（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

【本行動計画期間で取り組む情報共有体制】



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

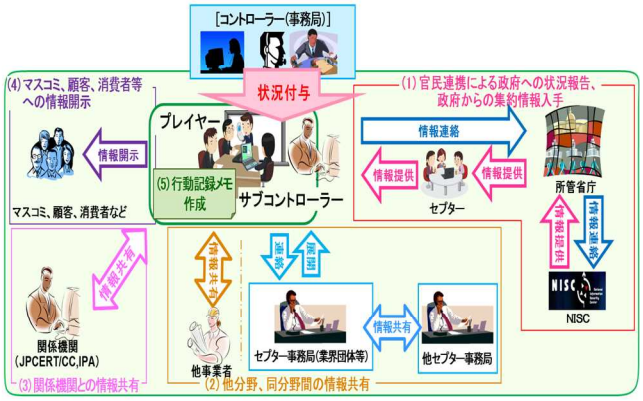
行動計画期間中の施策

（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。

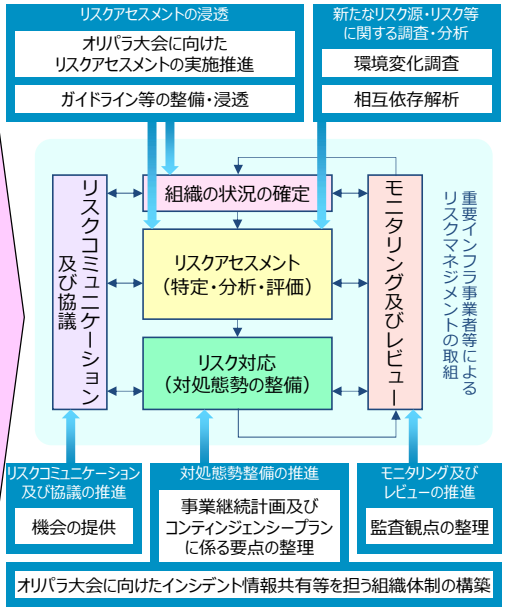
行動計画期間中の施策

（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次行動計画に基づく取組



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

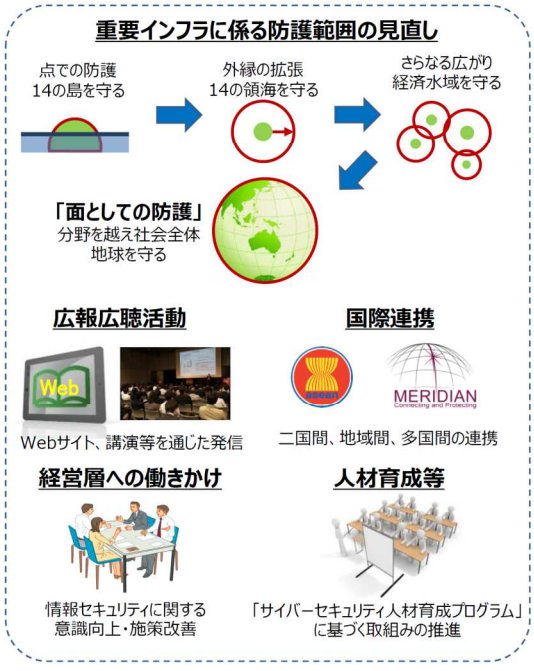
（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

（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

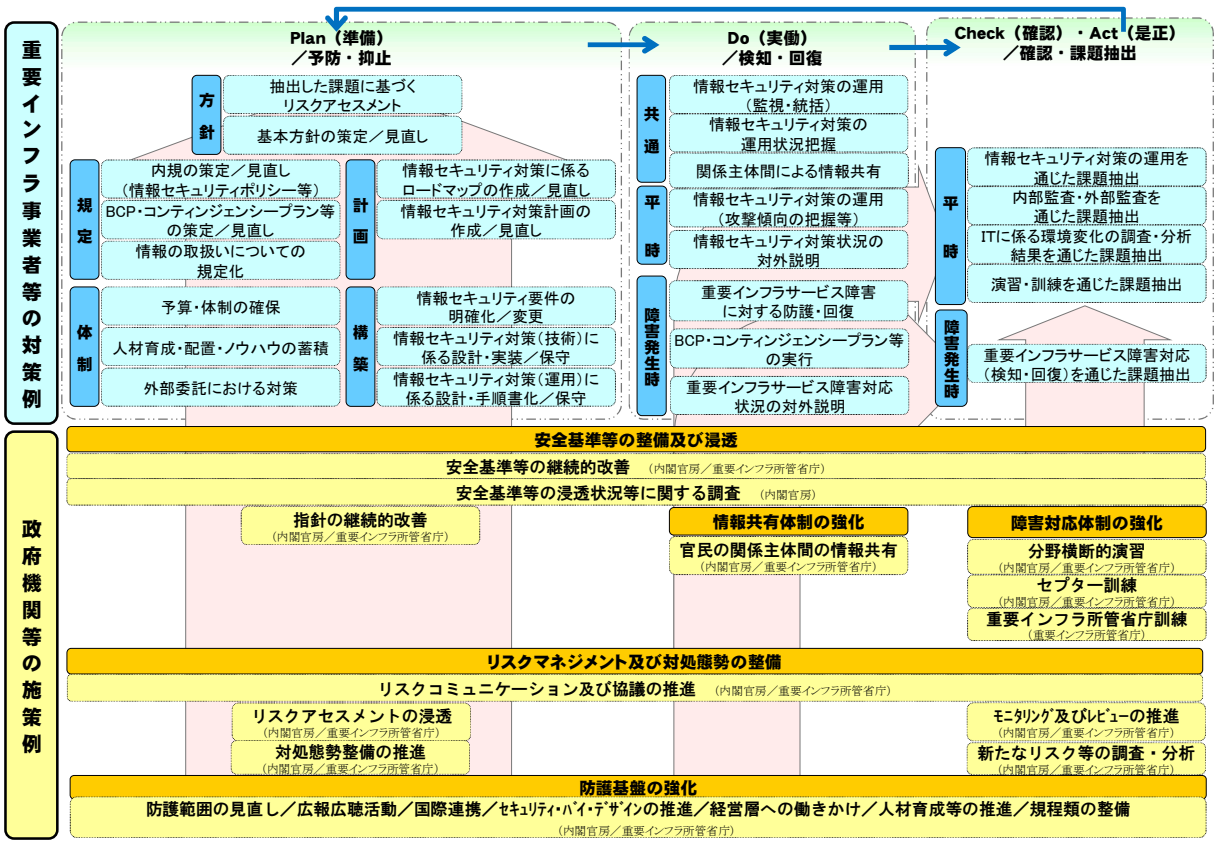
（４）経営層への働きかけ
- 情報セキュリティに関する経営層の意識向上のための働きかけ

（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

第４次行動計画に基づく取組



「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、2019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次行動計画は、第３次行動計画の基本的骨格（５つの施策）を維持しつつ、重要インフラを標的とするサイバー攻撃の状況やその背景としての社会環境・技術環境の変化を勘案し、策定したものである。この策定に当たっては、重要インフラサービスに重点を置き、「重要インフラサービスの安全かつ持続的な提供の実現」を重要インフラ防護の目的として明確化したほか、これまでの「IT障害」を「重要インフラサービス障害」とするなど、機能保証の考え方を踏まえたものとしている。

2019年度は、2018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、「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）」等の改定（2019年５月）、過去最大規模での分野横断的演習の実施（2019年11月）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2018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大会後に予定されている同計画の評価・見直しに向けた検討に着手していく。

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。

○安全基準等策定指針の改定

サイバーセキュリティを取り巻く情勢を踏まえ、「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）」を2019年５月に改定し、重要インフラの各分野の安全基準等において規定することが望まれる項目として、「災害による障害の発生しにくい設備の設置及び管理」及び「データ管理」を追加した。前者は、重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい配置とする等、適切な設備の設置及び管理を行う仕組みを構築すること、後者は、システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うことを求めるものである。

また、第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、同指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。

○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。2019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11件の安全基準等の改定（初版制定含む）が実施されたことを確認した。（参考：別添５－３）。

また、総務省は、放送設備に義務付ける技術基準を定める省令の一部を改正し、厚生労働省は、水道施設の技術的基準を定める省令の一部を改正することで、それぞれサイバーセキュリティに係る保安規程・技術基準の一部として位置づけた。

なお、各重要インフラ分野における制度的枠組みの現状については、内閣官房において取りまとめ、2019年10月の重要インフラ専門調査会に報告した。

○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。2019年度は2,205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、2018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おおむね増加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、引き続き、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、安全基準等の整備・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、2018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、「「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、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。その結果、重要インフラ事業者等から内閣官房に対して269件の情報連絡が行われ、内閣官房からは38件の情報提供を行っている（参考：別添５－５）。

なお、2019年度第４四半期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ための検討に着手し、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。

表１：重要インフラ事業者等との情報共有件数

年度	2015	2016	2017	2018	2019
重要インフラ事業者等から内閣官房への情報連絡件数	401 件	856 件	388 件	223 件	269 件
内閣官房からの情報提供件数	44 件	80 件	54 件	43 件	38 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。

○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

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、交通ISACの創設に向けた検討や、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、2019年４月の総会で決定した活動方針に基づき、2019年度に、運営委員会（３回)、相互理解WG（２回)、情報収集WG（３回)、総会準備WG（２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。また情報共有活動である「Web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、情報共有体制の改善に係る検討を行い、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。

〇分野横断的演習

第４次行動計画に基づく具体的な取組の方向性として「重要インフラの防護能力の強化」、「オリパラを見据えた演習」、「官民・政府機関内連携」及び「演習参加形態の整理」に取り組んだ（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」に基づく情報共有の手引書」について説明を実施し、情報共有の方法を明確化するよう、改善を図った。

2019年度は、全14分野が演習に参加し、参加者数は4,967に増加した。また、事後の意見交換会も実施し、分野間での情報共有を促進した。

表２　分野横断的演習参加者数の推移

年度	2016	2017	2018	2019
参加者数	2,084 名	2,647 名	3,077 名	4,967 名

2019 年度においては、重要インフラ全体での防護能力の底上げのため、見学会に代わり、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、９割弱の参加者から有意義であると回答を得た。

また、2018 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から、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 93%となっている。

一方で、演習当日における他部門参加については、参加者募集時や事前説明会における資料に加え、事前説明会で参加を促したものの、その参加率は広報部門 37%、防災・危機管理部門 27%に留まっている。

なお、分野横断的演習を含め組織内外で実施する演習・訓練への参加割合は、73.6%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	2016	2017	2018	2019
参加セプター	18	18	19	19
参加事業者等	2,020	2,106	2,005	1,958

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共に、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 Wall Ⅳ）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、自職場参加の推奨等により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、東京2020大会に関わる重要インフラ事業者等が、大会開催時に想定される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、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、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、自組織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を実施する。

(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（Web 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、Webサイトへの掲載や説明会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、2019年度におけるWebサイトの閲覧数は4830件、第５回説明会の参加者数は423人となっている。

また、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、内部監査等の観点を追加し、2018年４月に策定・公表した「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」について、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2019年５月に行った。さらに、重要インフラ事業者等への浸透を図るべく、重要インフラのセキュリティに関するカンファレンスなどで同手引書に関する説明を実施するとともに、各重要インフラ所管省庁へも説明を実施した。

○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（３回)、相互理解WG（２回)、情報収集WG（３回)、総会準備WG（２回))を支援したほか、分野横断的演習に関しても、説明会や意見交換会等のほか、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、説明会（15回）や情報交換会（１回）を開催し、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とともに、リスクマネジメントの取組を継続的かつ有効に機能させるべくモニタリング及びレビューの強化を推進していく。特に新型コロナウイルス感染症拡大防止対策に伴う、これまでと大きく異なる新たな生活様式の定着などに対応するための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ていくことが重要との観点から、これに伴う新たなリスクを的確に把握し、必要な対応を行っていくことに重点を置く。

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。

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

ア　取組の進捗状況

防護基盤の強化に向け、以下の取組を実施した。

○防護範囲の見直し

内閣官房はサイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しの検討を行った。

また、民間においても、ICT-ISAC、金融ISAC、電力ISAC等の活発な活動や交通ISACの創設に向けた検討など、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、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。

○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、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Web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おり、計画や指針の改定を行った際は、掲載内容を更新するとともに、報道資料等を通じてその内容を周知している。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。

○国際連携

内閣官房は、重要インフラ所管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Face-to-Face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、日英サイバー協議や日ウクライナサイバー協議における意見交換を行った。また、日米間、日独間、日豪間や日加間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、スイスで開催されたMeridian会合（2019年10月）や日ASEAN CIIPワークショップ（2019年７月）では、日本における官民連携の取組の紹介及び各国の取組等に関する意見交換を実施した。その他、分野横断的演習当日（2019年11月）に合わせて海外機関を対象とした演習見学会の開催や、「ASEAN地域のサイバーセキュリティ対策強化のための政策能力向上」研修（2020年１月）を通じて、日本における重要インフラ防護の取組を紹介した。

○経営層への働きかけ

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

さらに、経済産業省による電力分野における「電力サイバーセキュリティ対策会議」の開催等によって、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。

○人材育成等の推進

内閣官房は、「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。

○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経理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」を作成し、2019年４月に発行した。

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、Webサイト、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や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。	・第４次行動計画が改定されて重要インフラ分野に空港分野が追加されたことを受け、「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）」を 2019 年５月に改定し、本指針の対象となる重要インフラ事業者等に主要な空港・空港ビル事業者等を追加した。また、サイバーセキュリティを取り巻く情勢を踏まえ、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」をあわせて追加した。同改定版については、NISC の Web サイトで公表した。
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、「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）」を 2019 年５月に改定し、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」を追加した。同改定版については、NISC の Web サイトで公表した。
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）」に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」を追加し、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た。
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 Web サイトで公表している。 ・各重要インフラ分野における制度的枠組みの現状について取りまとめのうえ、2019 年 10 月の重要インフラ専門調査会において報告するとともに、NISC の Web 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してヒアリングを実施し、情報セキュリティ対策の取組事例を収集した。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 Web 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、各施策の改善に向けた取組の参考となるよう、重要インフラ専門調査会に報告するとともに、NISC の Web サイトで公表している。
(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。（2019 年度　情報連絡 269 件、情報提供 38 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。	・「「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、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。

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、2019 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。	・「「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、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。
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。（2019 年度のセプターカウンシル会合の回数は延べ 11 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提供に関し、検討を行った。
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。	・重要インフラ全体の防護能力の維持・向上を図る観点から、「より実践的な演習機会の提供」、「自職場参加の推進」、「重要インフラ全体での防護能力の底上げ」、「情報共有体制の実効性の向上」に重点をおきつつ、分野横断的演習を実施した。2019 年度は、4,967 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、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」に基づく情報共有の手引書」について説明を実施し、情報共有の方法を明確化するよう、改善を図った。
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 2019 年度分野横断的演習の企画・運営について検討した。 ・演習実施前に、演習の検証課題を提示すること等により、演習参加効果を向上させるための取組を実施した。 ・演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者等が各社の早期復旧手順や IT-BCP 等の有効性や実効性を確認する機会を提供した。 ・事後の意見交換会として、討議事項にセキュリティに関する対策や課題、顔の見える関係等に関する意見交換を含む機会を提供した。
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）。	・演習の概要、目的等を整理し、「テキストブック」として参加事業者等のサブコントローラー向け、プレイヤー向け及びセプター事務局向けそれぞれの版を作成し、参加事業者等、セプター事務局及び重要インフラ所管省庁に提供した。 ・自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。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、対外的に明確化した資料を作成し展開した。
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。 ・2019 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」に係る説明会（15 回）及び情報交換会（１回）を開催するなど、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（322 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った。
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 Web 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 Web 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、重要インフラを取り巻く環境の変化に伴う新たなリスク源等について調査した。
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、説明会や情報交換会等を開催し、リスクアセスメントの演習等を通じて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、説明会や意見交換会をそれぞれ開催した。
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者の増加等を通じて、セキュリティの取組の輪を拡大・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。
②Web 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 Web 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、計画や指針の改定を行った際は、掲載内容を更新するとともに、報道資料等を通じてその内容を周知している。 ・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、海外機関を対象とした分野横断的演習見学会の開催、Meridian 会合や 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。 ・国土交通省と連携し、一般財団法人運輸総合研究所が主催する交通分野の経営層向けのサイバーセキュリティ対策に関する検討会への参画及び関連セミナーに対する後援を通じ、支援・協力を行った。
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」を作成・発行した。
⑧関連規格を整理、可視化。	・重要インフラ所管省庁及び重要インフラ事業者等の安全基準等の整備に資するよう、サイバーセキュリティ、リスクマネジメント等の重要インフラ防護に関係する規格を整理し、「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）」に参考文献として記載している。
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。	・第三者認証制度について、第４次行動計画における取組内容の検討を行い、第三者認証を受けた製品の活用を推進していくこととしており、重要インフラ事業者等に対する働きかけに向け、メーカーとの意見交換等を通じた状況把握を実施した。
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、Society5.0 におけるセキュリティ対策の全体像を整理し、産業界が自らの対策に活用できるセキュリティ対策例をまとめた、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を 2019 年４月に策定した。 また、経済産業省において、経営者のリーダーシップの下でサイバーセキュリティリスクに対応するための仕組みの構築や委託先の状況把握等を行うべきであることが記載されている「サイバーセキュリティ経営ガイドライン」の普及啓発を行った。

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。	・総務省において、放送設備等のサイバーセキュリティ確保に関する省令改正を 2020 年３月に実施した。なお、2017 年８月に発生した大規模なインターネット障害を踏まえ、誤った経路制御情報やサイバー攻撃による障害等のネットワークを跨がって発生する障害に関する電気通信事業者間での情報共有等について、また、2018 年 12 月の携帯電話事業者からは確認できなかったソフトウェアに関する有効期限切れによる重大事故を踏まえ、ソフトウェアの信頼性向上対策について、「情報通信ネットワーク安全・信頼性基準」等を 2019 年３月に改正している。 ・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」の改定を検討しており、2020 年３月に改定素案を策定した。また、水道施設におけるサイバーセキュリティ対策を強化する観点から、水道施設の技術的基準を定める省令の一部を改正した（2020 年４月施行）。 ・航空、空港、鉄道及び物流分野については、国土交通省において「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、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」を作成している。 ・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、平成 30 年度に報告された電気通信事故について、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、2019 年 8 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。
⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各重要インフラ分野における現状を把握した上で、調査の回答を行った。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 Web サイトで公表している。
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 Web サイトで公表している。 ・浸透状況等の調査として、金融庁では「金融機関等のシステムに関する動向及び安全対策実施状況調査」を通じて、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」を立ち上げ、連携態勢の強化に取り組んだ。 ・総務省において、平成 30 年度に報告された電気通信事故について、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、2019 年 8 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。 ・厚生労働省において、医療機関におけるセキュリティ対策について、医療機関の実態や各国の状況等に関する知見を収集するとともに、情報共有の在り方について議論することを目的に、医療関係者との意見交換会を開催した。 ・国土交通省において、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」の運営形態等について事業者による検討・議論の支援を行った。また、2019 年 11 月に、事業者有志による一般社団法人交通 ISAC 設立準備委員会が設置されたことから、2020 年４月に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。

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。 ・2019 年４月に空港セプターがセプターカウンシルに加入した。
⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。	・重要インフラ所管省庁は、セプターカウンシル総会及び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。
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」を立ち上げ、連携態勢の強化に取り組んだ。 ・厚労省において、医療機器のサイバーセキュリティの確保に関するガイダンスについて（通知）を医療機器の製造販売業者向けの講習会にて周知し、製造販売業者が行うべきサイバーセキュリティへの取組及び対応を具体的に提示した。
(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、2019 年 10 月から 2020 年 1 月までの間に、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、2019 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、2019 年 11 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 2019 年度分野横断的演習への参加を促し、全体で過去最多の 4,967 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、2019 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。また、翌年度以降も視野に入れた課題、方向性についての議論を行う検討会に出席した。
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 Ⅳ）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。
(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。 ・総務省においては、内閣官房および東京 2020 大会に関係する地方公共団体と連携し、東京 2020 大会に係るリスクアセスメントの取組を実施した。
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、内閣官房と協力し、「機能保証に向けたリスクアセスメント・ガイドライン」等を踏まえ、東京 2020 大会の関連事業者等のリスクアセスメントを推進している。

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。	・内閣官房が実施した「ＥＵ諸国及び米国における情報共有体制に関する調査」等については、重要インフラ所管省庁において今後、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活用されている。
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、「金融分野のサイバーセキュリティレポート」として公表した。また、クラウドの活用事例（グッドプラクティス）や適切なリスク管理の在り方等について外部委託調査を実施し、2019 年６月に「クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書」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 2 月に「電力サイバーセキュリティ対策会議」を開催し、電力分野におけるサイバーセキュリティの取組の更なる推進を図った。 ・国土交通省は、内閣官房と連携し、一般財団法人運輸総合研究所が主催する交通分野の経営層向けのサイバーセキュリティ対策に関する検討会への参画及び関連セミナーに対する後援を通じ、支援・協力を行った。
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、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」の運営形態等について事業者による検討・議論の支援を行った。また、2019 年 11 月に、事業者有志による一般社団法人交通 ISAC 設立準備委員会が設置されたことから、2020 年４月に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。 ・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、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。
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。あわせて、攻撃手法及び復旧手法に関する情報等の収集を行い、事業者と共有した。

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（セプターカウンシル相互理解 WG）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。	・2019 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、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、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 Web 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、2019 年度分野横断的演習検討会及び拡大作業部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、2019 年度分野横断的演習検討会及び拡大作業部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・訓練を相互に視察し、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、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を実施したほか、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 Web 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。

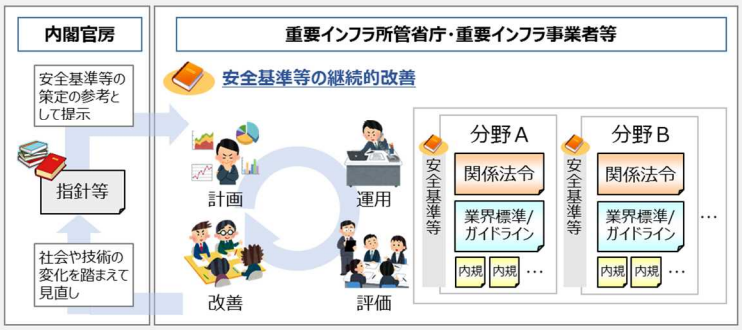
別添５－３　安全基準等の継続的改善状況等に関する調査

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24件）

※ 調査対象は02ページ参照

調査項目

①各安全基準等の**分析・検証**について
②各安全基準等の**改定**について
③各安全基準等の**指針への対応**について
④令和元年５月に指針に追加された項目の各安全基準等への記載内容について

【令和元年５月に指針に追加された項目】

- **データ管理**
  システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う。
  また、事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。
- **災害による障害の発生しにくい設備の設置及び管理**
  重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい配置とする等、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施することにより、適切な設備の設置及び管理を行う仕組みを構築する。

調査対象一覧（全 14 分野 24 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＜初版＞
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

- 2019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**11件の改定（初版制定含む）が実施**された。
- また、各安全基準等のそれぞれの制定主体において、**各重要インフラ分野の安全基準等の指針への対応について確認**が行われている。

分析・検証の主な契機・内容等

- 指針や関係法令・ガイドラインの改定、社会的・技術的な環境の変化、サイバーセキュリティに係るインシデントの発生等を踏まえた安全基準等の見直し
- 2020年東京オリンピック・パラリンピック競技大会（※1）の開催に万全を期すため、 サイバーセキュリティの観点から安全基準等の整備状況の確認

【安全基準等の分析・検証及び改定の際に参照された規格】
- 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群
- ISO/IEC 27001, 27002, 27017
- NIST重要インフラのサイバーセキュリティを改善するためのフレームワーク
- その他（各重要インフラ固有の規格・ガイドライン等）

（※1）令和２年３月30日に、東京オリンピックは令和３年７月23日から８月８日に、東京パラリンピックは同年８月24日から９月５日に開催されることが決定された。

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**（※2）ことを確認。
（※2）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。
- 令和元年５月に指針に追加された**「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」についても、安全基準等への反映が進められている**ことを確認。

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**
  - 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）
  - 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
  - 電力制御システムセキュリティガイドライン
  - 電気設備の技術基準の解釈
  - 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
  - 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
  - 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
- **社会的・技術的な環境の変化を踏まえた改定**
  - 電気通信分野における情報セキュリティ確保に係る安全基準（第4.1版）【再掲】
  - 放送設備サイバー攻撃対策ガイドライン
  - 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
  - 電力制御システムセキュリティガイドライン【再掲】
  - スマートメーターシステムセキュリティガイドライン
- **サイバーセキュリティに係るインシデントを踏まえた改定**
  - 情報通信ネットワーク安全・信頼性基準【再掲】

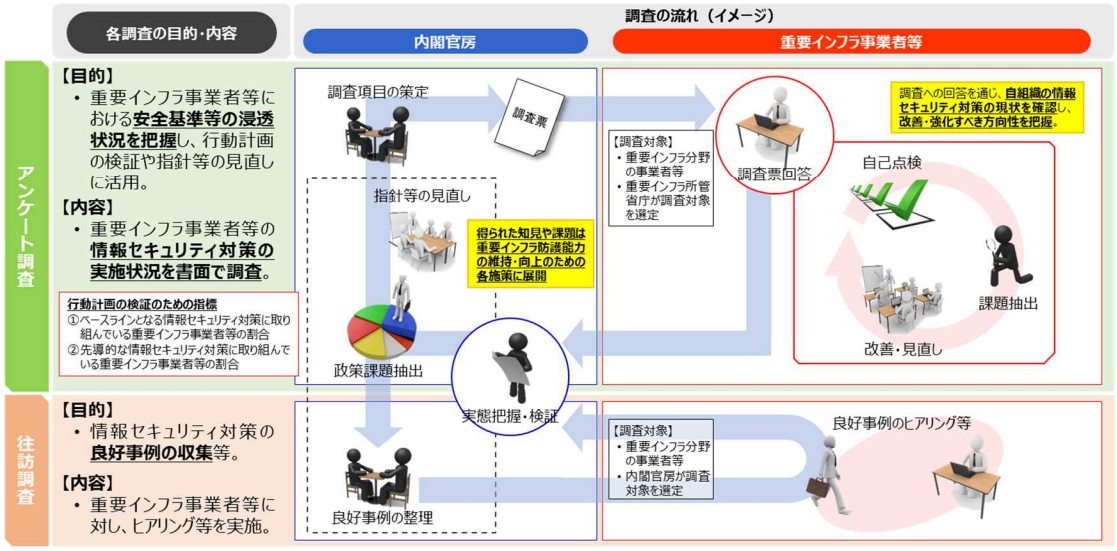
重要インフラ所管省庁及び重要インフラ事業者等で構成される業界団体において、各安全基準等の分析・検証や改定が行われ、**安全基準等の継続的な改善が着実に実施**されていることを確認。

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年度の調査では、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）の実施状況について調査**した。
- 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。

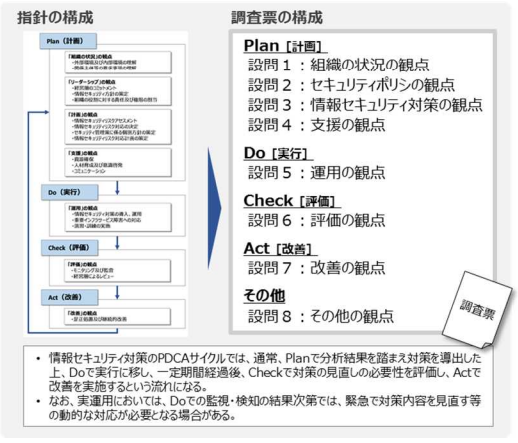
（注）これらの対策項目の実施の有無が当該事業者における情報セキュリティ対策のレベルを直ちに示すものではないことに留意する必要がある。指針においても、対策項目は「重要インフラ事業者等が採否を検討する」ものとされている。

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：2019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
調査方法	次のいずれか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**。

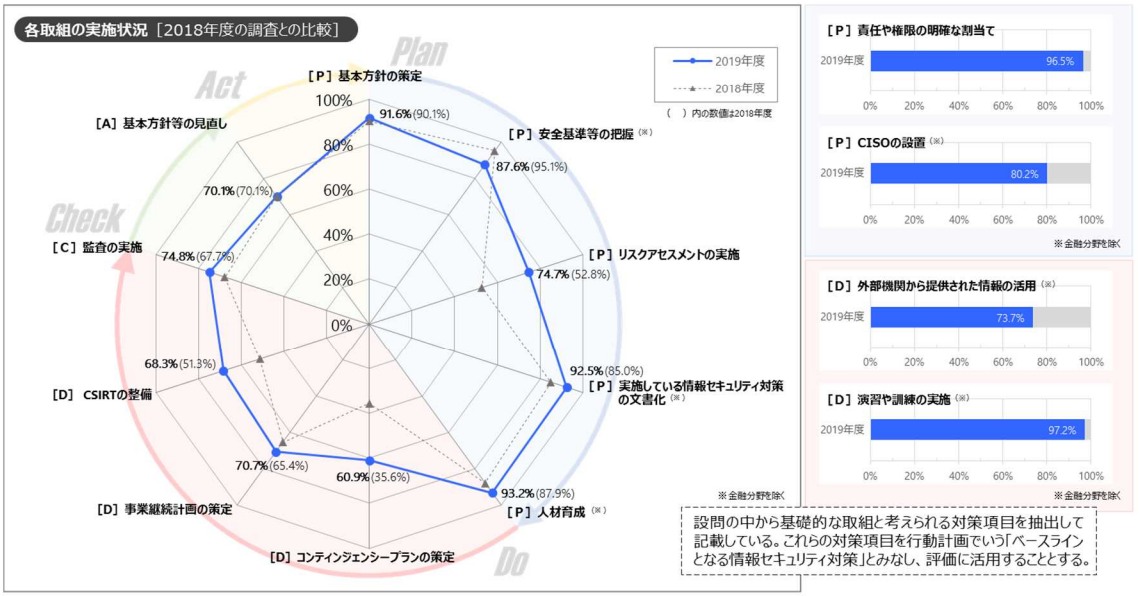
調査票の構成

- 指針は、PDCAサイクルの各段階において「安全基準等」で規定が望まれるとする情報セキュリティ対策（対策項目）を提示している。
- 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。



浸透状況調査（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

- 2019年度は、全重要インフラ分野（計14分野）の事業者等を対象に調査を行い、**2,205事業者から回答**（回答率65.4% 前年度比＋5.3pt）を得た。
- 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おおむね向上**しており、**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、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。

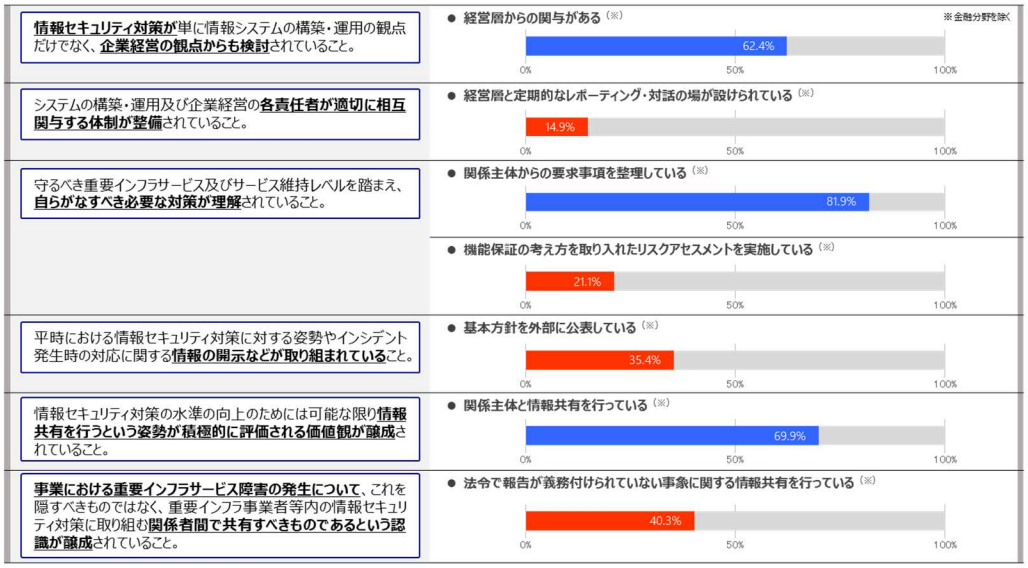


設問の中から基礎的な取組と考えられる対策項目を抽出して記載している。これらの対策項目を行動計画でいう「ベースラインとなる情報セキュリティ対策」とみなし、評価に活用することとする。

浸透状況調査（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が５割を超えており、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**していると評価できる。
- 一方で、「経営層との定期的なレポーティング・対話」「機能保証の考え方を取り入れたリスクアセスメント」等、実施状況が低い項目も見受けられることから、行動計画が示す理想とする将来像の実現に向けては、これらの改善を図っていく必要がある。

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



浸透状況調査（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。

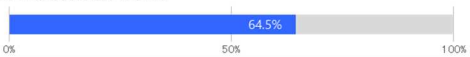
本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、**自らの情報セキュリティ対策の程度及び残存するリスクが認識**されていること。

- 関係主体からの要求事項を整理している（※）【再掲】　※金融分野を除く

- 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（※）【再掲】

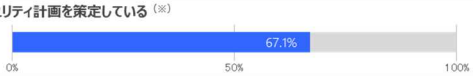
各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス障害に係る**リスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっている**こと。

- 内部環境及び外部環境を整理している（※）



- 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（※）【再掲】

- 情報セキュリティ計画を策定している（※）

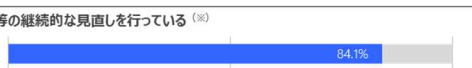


重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、**重要インフラサービス障害が国民生活や社会経済活動に重大な影響を与えるリスクを可能な限り低減**させることができていること。

- 情報セキュリティ対策のために適切に十分な資産配分を行っている（※）

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（※）



● 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。

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（※）【再掲】　※金融分野を除く

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。

実施形態	FY2016 計	FY2017 計	FY2018 計	FY2019 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
重要インフラ事業者等から NISC への情報連絡(※)	856	388	223	48	57	111	53	269
関係省庁・関係機関からの NISC への情報共有	41	19	7	6	3	6	1	16
NISC からの情報提供	80	54	43	10	8	8	12	38

※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 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
未発生の事象		予兆・ヒヤリハット	330	80	27	3	1	5	3	12
発生した事象	機密性を脅かす事象	情報の漏えい	30	15	13	4	5	1	3	13
	完全性を脅かす事象	情報の破壊	47	20	17	4	3	1	3	11
	可用性を脅かす事象	システム等の利用困難	80	143	97	19	27	84	28	158
	上記につながる事象	マルウェア等の感染	289	65	17	3	2	3	1	9
		不正コード等の実行	10	13	4	1	1	1	2	5
		システム等への侵入	26	17	14	4	5	3	2	14
		その他	44	35	34	10	13	13	11	47

※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 1Q	FY2019 2Q	FY2019 3Q	FY2019 4Q	FY2019 計
意図的な原因	不審メール等の受信	546	89	36	3	1	7	2	13
	ユーザＩＤ等の偽り	1	4	3	1	5	6	0	12
	DDoS 攻撃等の大量アクセス	23	31	17	3	4	7	6	20
	情報の不正取得	14	16	10	0	3	2	3	8
	内部不正	0	4	1	0	0	0	0	0
	適切なシステム等運用の未実施	19	15	14	4	3	3	1	11
偶発的な原因	ユーザの操作ミス	15	23	10	2	3	1	0	6
	ユーザの管理ミス	8	13	6	4	0	0	2	6
	不審なファイルの実行	243	42	16	3	1	2	1	7
	不審なサイトの閲覧	29	20	4	1	2	2	0	5
	外部委託先の管理ミス	20	41	29	8	4	18	9	39
	機器等の故障	22	32	27	3	4	47	8	62
	システムの脆弱性	56	36	19	5	3	3	5	16
	他分野の障害からの波及	0	10	6	0	0	4	0	4
環境的な原因	災害や疾病等	0	0	1	0	13	0	0	13
その他の原因	その他	34	29	29	5	7	11	10	33
	不明	92	57	46	10	12	20	11	53

（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

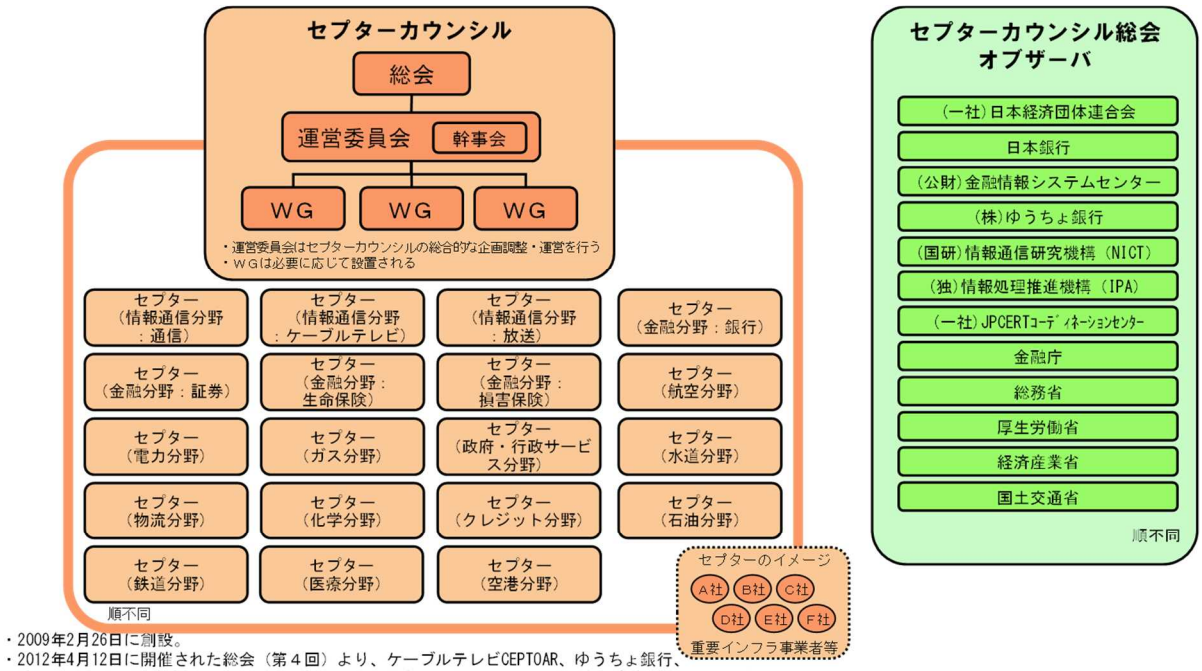
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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（2020 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

2020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	金融CEPTOAR連絡協議会				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
	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	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	GAS CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR
名称																			
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（の人数）	23社 1団体	316社 1団体	197社・団体	1,352社	272社 7機関	42社	47社	14社 1団体	8社	22社 1団体	14社 3機関	10社・団体	47 都道府県 1,741 市区町村	1グループ 19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）	398社・団体	359社	12社	3社・団体	—	—	—	—	—	—	15社・機関	182社・団体	—	382社	内容に応じ1,331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）、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）、サイバー口対策協議会（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

２０１９年度分野横断的演習　開催実績

＜事前説明会＞
日　程　：２０１９年９月１７日（火）、２０日（金）、２４日（火）、２５日（水）、２６日（木）
場　所　：東京会場、大阪会場、福岡会場（説明会の模様について、演習当日まで動画配信）
内　容　：①分野横断的演習の事前説明（個別シナリオの作成、演習における役割・実施要領　等）
②事業継続計画及びコンティンジェンシープランの重要性に関する説明

規程類の事前確認、個別検証課題の確認・調整

＜演習当日＞
日　時：２０１９年１１月８日（金）１０：４０～１７：００
場　所：東京会場、大阪会場、自職場
参 加 者：４，９６７名
【重要インフラ事業者等：１４分野】
【セプター：１４分野１９セプター】
【関係機関、分野横断的演習検討会有識者、政府機関　等】
演習内容：
【第1部】「情報連絡様式」を用いた情報連絡訓練として実施
演習参加事業者等が、情報連絡様式を用いて、所管省庁・セプター事務局を経由したNISCへの情報連絡を確実に実施することをねらいとした演習
【第2部】分野を横断した困難なインシデントへの対応演習として実施
より困難な状況を想定した内容での「情報連絡の徹底」及び「BCP発動検証」、「レピュテーションリスクへの対応」、「広報・報道対応」等をねらいとした演習


演習の模様


橋本大臣による挨拶

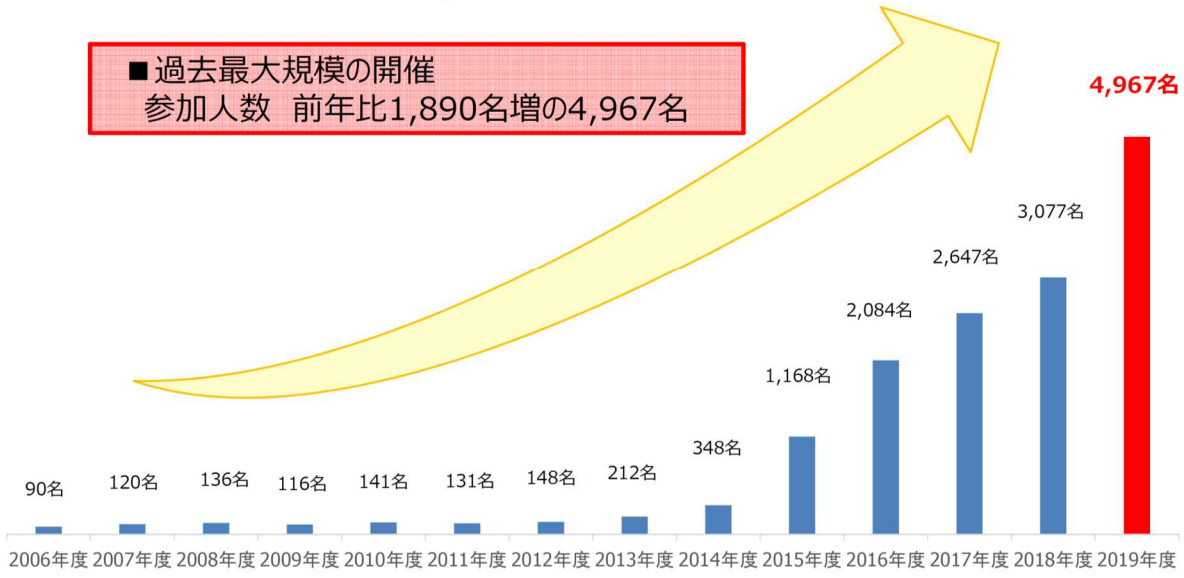
演習を通じた内規・体制等の課題抽出

＜意見交換会＞
日　時：２０１９年１２月１３日（金）１３：３０～１７：００
場　所：東京会場、大阪会場
参 加 者：２６４名（１７８組織）
内　容：①演習当日に得た気づき、改善に向けた取組み、困っていること、工夫していること等について、他の参加者事業者等と意見交換
②サイバーセキュリティの担当者相互の繋がり（顔の見える関係）を確保し、平素より情報交換が行える関係性を構築
③有識者講演　等

他事業者等との情報共有を通じた改善の促進

分野横断的演習の参加者の推移

- **本年度の参加登録者は4,967名**



2019 年度の取組

- 第4次行動計画に基づく重要システム障害時の情報連絡・情報提供の手順や情報連絡様式の周知徹底・連絡のスピードの確認
- オリパラ期間中のシナリオに基き、通常とは違う連絡体制及び連絡頻度におけるNISCをはじめとした政府内連携の確認
- 上記の体制や障害対応に係る手順等について、演習から知り得た知見を施策へ反映

2019年度の取組

重要インフラの防護能力の強化

- 大規模事案発生時のIT部門、危機管理部門、広報部門等の連携
- 各分野の実情に配慮した、事業者の演習参加の促進

オリパラを見据えた演習

- 重要サービス事業者を主体としたオリパラを想定した演習（ただし、必要に応じて重要サービス事業者以外も対象とする）
- 従来のシナリオよりも、より困難な内容を含む共通シナリオ
- 演習時計は共通のものとするとともに、演習時間を拡大
- 他の東京オリパラ大会関係のサイバー演習や情報共有のシステムとの連携を図る

官民・政府機関内連携

- 法令に基づく報告が必要となるような重要インフラサービス障害があった時の所管省庁への迅速な情報連絡
- NISC及び所管省庁における事業者からの情報連絡の効率的かつ正確な集約・分析・展開

演習参加形態の整理

- オリパラ重点等を踏まえて、演習当日のメイン集合会場は東京とする（ただし、地方にも１会場確保を検討）
- さらなる目職場参加の推進

2020 年度に向けた主な取組方針

・障害対応体制の強化による重要インフラ防護の推進
・対処態勢の整備及び情報共有体制の強化による重要インフラサービスの障害対応能力の維持・向上
・情報連携の活性化による重要インフラサービス障害対応に関する能力の維持・向上

2020年度に向けた主な取組方針

官民・政府機関内連携による情報共有体制の検証

- 情報共有に関する演習前の説明の充実
- 重要インフラサービス障害があった時や、社会的反響の大きい事案が発生したとき等の所管省庁への迅速かつ正確な情報連絡の実施
- **NISC及び所管省庁における事業者等からの情報連絡の効率的かつ正確な対応（集約・分析・展開等）の実施**
- **自職場環境（メール等）による演習参加を推進**
- 演習中における官民連携状況の可視化を検討

重要インフラ事業者等の実情を踏まえた演習の参加促進・効果的な実施

- **演習参加者のニーズに配慮した演習日程・時間、演習方式（模擬行動を主とした演習、机上学習を主とした演習等）及びニーズに適合した演習実施方式の検討**
- **集合会場における参加条件（演習会場内での情報共有等）及び臨場感の演出の検討**
- アンケート調査の重点化・深度化及びグッドプラクティスの抽出等を実施し、成果展開の内容充実化を図る

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

- **IT-BCPの発動等が求められる状況として、サイバーインシデントを起因とした危機事象に発展する内容を含むシナリオの検討**
- 参加者による独自の課題設定が可能な演習シナリオの検討

別添５－８　セプター訓練

セプター訓練（2019 年度）の概要

<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」の障害対応体制の強化の１つであり、各分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的としている。

<目的>

✓ 関係主体間における疎通確認を通じた 情報共有体制の実効性の検証
✓ 各主体、各経路における既存の手順等の改善、解決すべき課題の抽出

<参加者>

情報通信（電気通信、放送、ケーブルテレビ）、金融（銀行等、生命保険、損害保険、証券）、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、石油の計19セプター、1,958者

<実施期間>

2019年10月から2020年1月まで（セプター毎に異なる日時に実施）

<訓練の流れ>

1. NISCから、模擬の情報（注意喚起及び影響確認）を所管省庁へ送付
2. 所管省庁は、NISCから受領した情報をセプター事務局へ送付
3. セプター事務局は、所管省庁から受領した情報を訓練参加者へ送付
4. 訓練参加者は、受領報告（又は被害状況報告等）をセプター事務局又は所管省庁へ送付
5. セプター事務局又は所管省庁は受信状況をとりまとめの上、（所管省庁経由で）NISCへ報告

2019 年度セプター訓練の総括

✓ 2018年度に引き続き多くのセプターで新たな気付きや課題等が抽出され、セプターからのアンケート結果からも**本訓練の有用性が再確認された**。

✓ セプター訓練の参加事業者等は2,000者前後で横ばい状況である。
- 1,958者が訓練に参加（2018年度参加実績2,005者）

✓ 2018年に続き、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したが、疎通確認の割合は2018年度に比べ若干上昇（全体89%→91%）した**。
- 疎通確認割合100%は、2019年度は8セプターであった（2018年度も8セプター）
- 2018年度より疎通確認割合が9セプターにて上昇、５セプターにて低下した

✓ 2019年度は疎通確認が取れなかった事業者等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か、原因調査とその対策を実施**した。
- メール見過し予防としてのメール受信設定（受信フォルダや仕分けルール等）の再確認が必要
- 重要度の高い情報は、通常の連絡手段以外に電話等の連絡手段の併用が有効
- 一定時間待ってメール返信がない場合は電話等で確認を取ることが有効

✓ 2019年度セプター訓練開始前までに、2018年度訓練結果の**反映が半数程度できていなかった**。

セプター訓練の今後の方向性（案）

① 重要インフラ防護能力の維持・向上のため、セプター内での情報共有体制の点検・整備等に資する**本訓練の継続的な実施は重要**であり、NISCは今後も訓練機会を提供

② **全セプターにおいて事業者等への日程を連絡しない抜き打ち実施を継続**

③ 東京2020大会、分野横断的演習の開催時期（年度の後半）との関係及び所管省庁・セプター事務局の要望を踏まえ、以下を検討
- **2020年度のセプター訓練は年度の前半（７月予定）に実施**
- 訓練開始から3日以内に疎通確認ができなかった事業者等へのフォローとして**疎通確認が100%になるまで計測を実施**

④ 連絡先のメンテナンス等の徹底
- 本セプター訓練の機会だけでなく、定期的な連絡先の点検など検討
- 主担当単独での対応では、不在時の対応の遅延があるため、複数の担当者を登録するなど体制強化の検討

⑤ セプター訓練への事業者等の参加拡大を推奨

⑥ 訓練参加者は、疎通確認と合わせて、「被害あり」という仮定で模擬の情報連絡を実施することを推奨（※）
（※）訓練のオプションとしてご検討ください

⑦ 前回訓練での振り返り内容が対策に反映されているかについて検証

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、2019年1月1日～2019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、地域性や分野のバランスも考慮

2019 年度　調査対象事例　概要

- **“重要インフラ事業者が利用するサーバやメール環境への不正アクセス”**が複数分野の重要インフラ事業者等で発生したことから、各事業者における対応事例を調査。
- **”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2019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	改元に伴うシステム変更トラブルへの対応	利用者が、改元後に処理されるサービスの予約手続きを改元前に行ったところ、サービスの提供日が誤って表示されるトラブルが発生。	日付形式の切り替え日に関する認識が、店舗端末接続ネットワーク側との間で異なっていたため。
2	重要インフラサービスの一部業務の停止	重要インフラサービスで利用するデータベースのシステムファイルが破損したことにより、顧客がサービスを利用できなくなった。	不具合を改修する修正パッチを未適用であったため。
3	委託先のシステムトラブルに伴うサービス障害	複数の重要インフラ事業者が共同利用する業務システムにおいて障害が発生し、利用する複数の事業者において同時にサービス障害が発生。	大量データの処理が一時的に集中し、ホストコンピュータ上の通信制御ソフトウェアのリソースが枯渇したため。
4	重要インフラサービスの業務遅延	重要インフラサービスに遅延が生じたことから、業務スケジュール管理システム経由で業務スケジュールの組み換え処理を試みたが、システムが正常に動作せず、重要インフラサービスの業務遅延が拡大。	システムの処理タイミングの一部ずれが生じ、排他制御が適切に実施されなくなったため。
外部からのサイバー攻撃			
5	不審メールによるマルウェア「Emotet」への感染	重要インフラ事業者の職員が不審メールの添付ファイルを開封し、マクロを有効化したことで、端末がマルウェア「Emotet」に感染。感染後、感染端末を使用していた職員を騙るメールが、外部組織に送信。	重要インフラ事業者の職員が、外部から送信された不審メールの添付ファイルを開封してしまったため。
6	重要インフラ事業者が利用するサーバへの不正アクセス	重要インフラ事業者が利用するサーバが不正アクセスされ、同サーバから外部に不審なメールが送信。	コンテンツ管理システム(CMS)のプラグインの脆弱性を悪用され、サーバが不正アクセスされた可能性が高い。
7	クラウド型メールサービスに対する不正ログイン	重要インフラ事業者が利用するクラウド型メールサービスに対し、攻撃者が不正アクセスを実行し、重要インフラ事業者のメールアカウント経由で、当該事業者とは無関係なメールが大量に外部へ送信。	クラウド型メールサービスのログイン画面について、アクセス制御が十分でなかったため。

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, 4）から

- システム故障への対応方針を迅速に決定できるようにするために、重要インフラサービスにおける判断権者を事前に明確にしたうえで、**実効的な権限委譲について検討**することが重要。
- 重要インフラサービスの機能保証の考え方を踏まえ、**サービスの優先度に応じた段階的な復旧対応方針の策定**や**代替手段を用いた事業継続計画の整備**を事前に検討することが重要。
- システム故障発生時に、重要インフラサービスの関係者等に迅速に連絡できるよう、組織内だけでなく、**外部委託先や**当該サービスに関わる**システムを共同利用する他の事業者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。

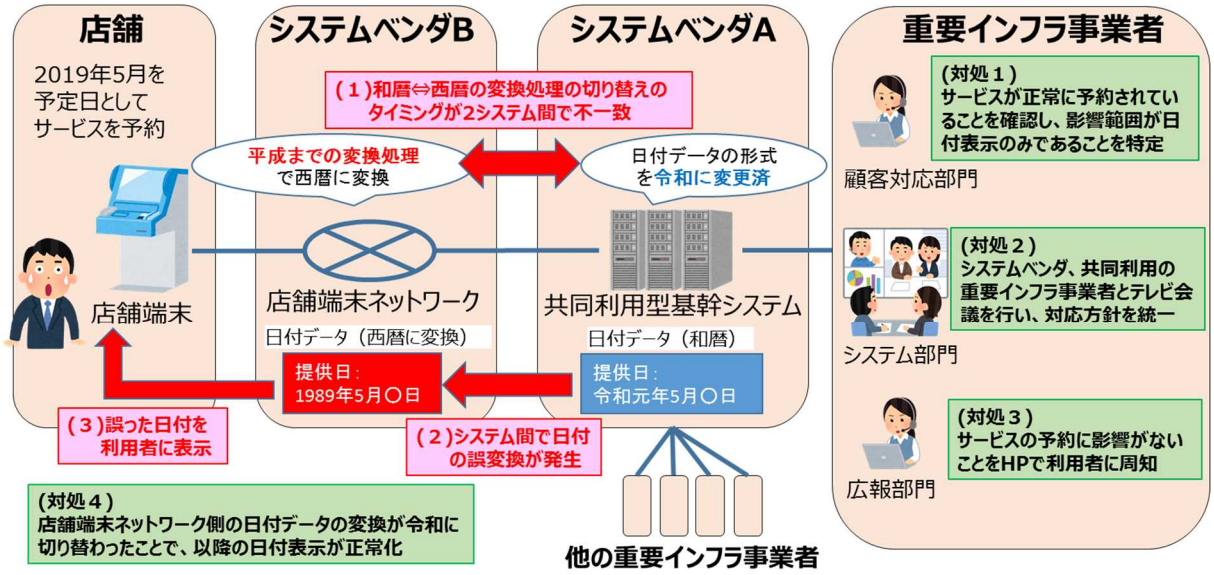
外部からのサイバー攻撃への対応事例（No. 5, 6, 7）から

- 他の重要インフラ事業者における類似のサイバー攻撃の被害を防止するため、事業者は**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。
- クラウドサービス利用時は、クラウドサービスの仕様やサービスの提供条件を十分確認したうえで、サービスに**適切な設定を行い、仕様を考慮した運用**を実施することが重要。
- 有識者に**技術的見解を確認できる体制の構築やベンダとの委託契約の締結**等を通じて、セキュリティインシデント発生時の技術的対応を迅速に実施できるようにすることが重要。

※　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　改元に伴うシステム変更トラブルへの対応

- 利用者が、2019年5月（改元後）に処理されるサービス（重要インフラサービスに該当）の予約手続きを同年4月（改元前）に行ったところ、サービスの提供日が「1989年5月○日」と表示されるトラブルが発生
- 重要インフラ事業者は、当該トラブルが予約に影響しないことを特定し、サービスを継続する対応を意思決定
- システムベンダや他の重要インフラ事業者と連携し、利用者への対応を統一して迅速にHP等で周知し、問い合わせ対応を行ったことで、分野全体で大きな混乱なく事態を収拾



【１　背景】

- 共同利用型の基幹システムは、店舗端末接続ネットワークを通じて、重要インフラサービスを店舗に提供する。
- 改元対応に向け、約２年前から、システムベンダとも連携し、影響調査や改修等を進めてきた。
- 処理が5月以降となるサービス予約の日付の形式（和暦）を、連休前の2019年（平成31年）4月26日に切り替え、令和の年号に対応した。

【２　検知】

- 4月26日、店舗端末の利用者から、サービス予約日の日付表示が1989年（平成１年）となる旨の問い合わせが、システムベンダBのコールセンター経由で重要インフラ事業者のシステム部門に寄せられた。
- システム部門の職員が店舗に出向き再現性を確認

【３　対処】

- 基幹システムでのサービス予約のステータス確認により、影響はサービス予約の日付表示のみのトラブルであることを特定すると共に、該当する利用者数を正確に把握
- システムベンダ及び共同利用の重要インフラ事業者と連携して、影響範囲と対応の選択肢を精査し、当該トラブルへの対応方針を統一
- 調査結果と対応方針を顧客対応部門に展開し、顧客からの問い合わせへの態勢を用意
- トラブル認識から3時間後に、ホームページ等を通じて、サービス予約に影響がないことを利用者に提供し、混乱が大きくなる前に事態を収拾

【４　原因】

- 日付形式の切り替え日に関する認識が、店舗端末接続ネットワーク側との間で異なっていたため。（２つのシステムの切り替えタイミングに関する試験項目の不足）

【５　再発に備えた対策】

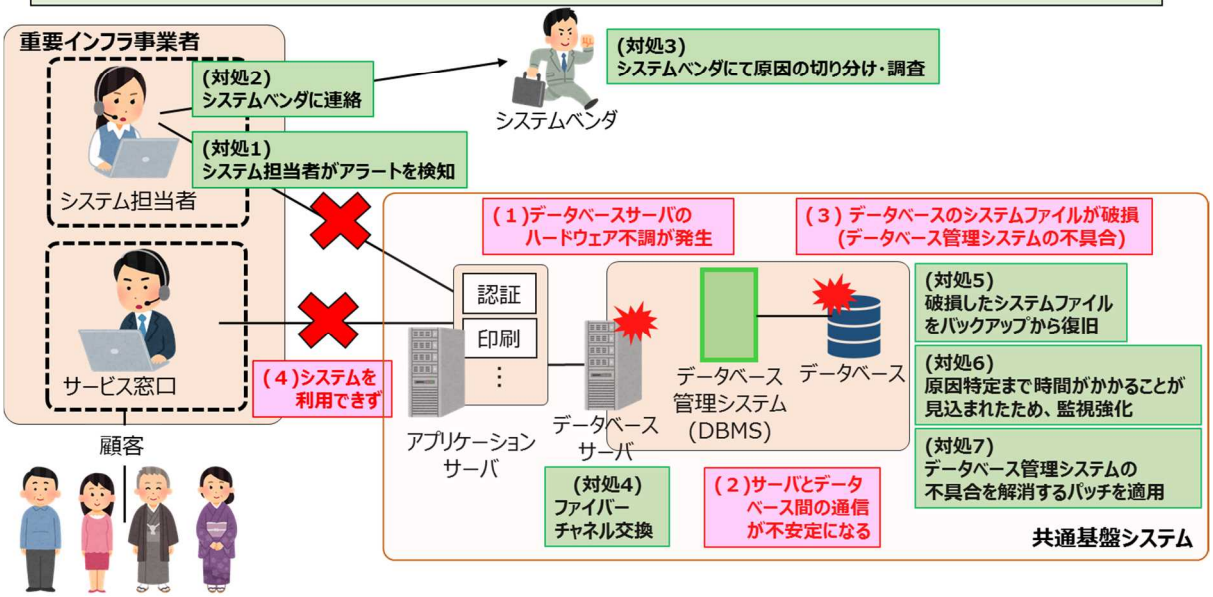
- システムの移行計画に関するプロジェクト管理方法（要件定義、試験観点抽出、コミュニケーションプロセス等）の見直し

【６　得られた気付き・教訓】

- **利用者への影響を抑えるため、敢えてサービスを止めない選択**
  システムベンダが提案した「サービス停止を伴うプログラム改修」等の選択肢もあった状況で、改修を実施する場合のリスクと、現状のままサービス継続することのリスクを正確に見極め、最も利用者に影響がない対応を選択した。
- **非常時に備えた権限移譲**
  重要インフラサービスに影響するシステム障害への対応方針の意思決定や公式HPへの案内掲載等の権限がシステム部門に委ねられていたため、一貫した対応を迅速に行うことができた。
- **顧客対応、広報と一体となった対応態勢**
  システム障害発生時に顧客対応、広報、システムの部門が密に連携して動くプロセスが、過去の経験から事業者内全体に定着しており、各部門が役割を迷いなく果たすことができた。
- **同分野の事業者と有事に協力できる関係**
  システムを共同利用する重要インフラ事業者同士が情報を共有できる関係が平時から構築されていたことが、利用者への統一的な対応に繋がり、分野全体で混乱を回避できた。

事例２　重要インフラサービスの一部業務の停止

- 重要インフラサービスで利用するデータベースのシステムファイルが破損したことにより、顧客がサービスを利用できなくなった。
- データベースサーバとデータベース間の通信が不安定になった際に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損したことが原因。
- 恒久対策として、データベースソフトの不具合を解消するパッチを適用。



【１　背景】

- 複数の業務において利用する、認証、印刷等の複数の機能を統合した、共通基盤システムを運用している。
- システムは、各機能が利用するデータを格納したデータベースサーバと接続している。
- システムにおいて、インシデント発生の1週間前から、業務に支障がないレベルの通信エラーが頻発していた。

【２　検知】

- システムを監視するシステム担当者がアラートの発生を確認し、障害を覚知した。
- システムを利用する複数の拠点から、印刷処理ができない旨の連絡が寄せられた。

【３　対処】

- インシデント発生前から通信エラーが頻発していたため、ハードウェア故障を疑い、ファイバーチャネルを交換した。
- 機器交換後、システムを再起動するも障害が復旧せず、データベースのシステムファイルの破損が判明した。
- サービスの優先度が高い業務から再開すべく、対応方針を決めた。また、バックアップファイルからシステムファイルを復元することで復旧し、業務を再開した。

【４　原因】

- データベースサーバのハードウェア不調により、サーバとデータベース間の通信が不安定になった。
- サーバとデータベース間の通信が不安定になった場合に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損した。
- 不具合を改修する修正パッチを未適用であった。

【５　再発に備えた対策】

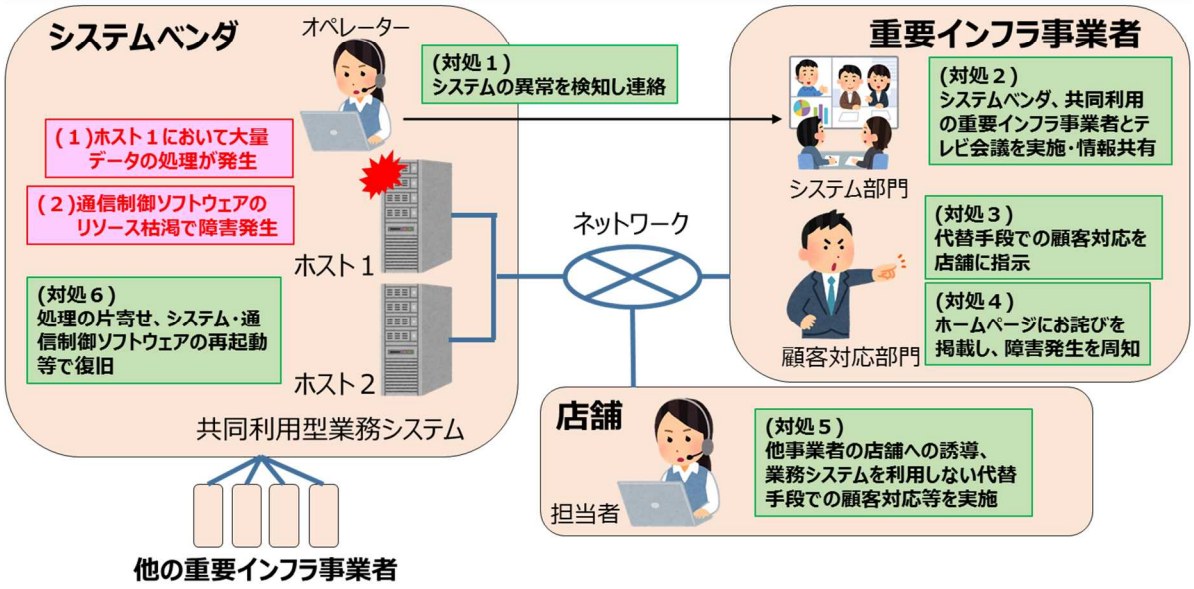
- データベース管理システムの修正パッチを適用した。
- データベースのシステムファイルを三重化した。
- ハードウェアが不調の場合に速やかに交換できるよう、システムの監視体制を強化した。

【６　得られた気付き・教訓】

- **サービスの優先度に応じた復旧対応方針の検討**
  障害発生時、サービスの優先度に応じて順次復旧できるよう、対応方針を決めた。
- **適時・的確な情報発信**
  事前に報道発表の基準・手順を策定していたことで、障害の発生や復旧見込みを適時・的確に公表できた。
- **インシデント対応体制の整備**
  複数の拠点に人員が配置され、距離が離れていたが、テレビ会議の利用により、円滑に連携できた。
- **平常時における対応の見直し**
  共通基盤システムでは、パッチ適用検証工数や適用することによる想定外の影響を鑑み、無条件に適用しない方がよいと考えていた。影響度の大きいパッチは検証の上、迅速な適用を検討するように対応方針を見直した。また、1週間前からインシデントの兆候(通信エラー)があり、対応について検討していたさなか、本事例が発生したことを踏まえ、今後障害につながる可能性が高い事象は早期に予防交換を含め対応することとした。

事例３　委託先のシステムトラブルに伴うサービス障害

- 複数の重要インフラ事業者が共同利用する業務システムにおいて障害が発生し、利用する複数の事業者において同時にサービス障害が発生。
- 重要インフラ事業者は、テレビ会議によりシステムベンダからの報告及び他事業者からの情報共有を受け、状況を把握。早期に代替手段での対応を店舗に指示、ホームページにお詫びを掲載するなどして、混乱を回避。
- 再発に備えた対策として、通信制御ソフトウェアのリソース監視強化、リソース枯渇時の対応マニュアルの策定、共同利用事業者の処理方法変更、他に同様の不備がないかを確認。



【１　背景】

- 業務システムの開発・運用・保守は、システムベンダに委託していた。
- 当該システムは、汎用機ホストコンピュータ2台の2系統によるロードシェア構成としており、複数の事業者で共同利用していた。

【２　検知】

- システムベンダのオペレーターがシステム障害発生を検知。
- 職員が障害の再現性を確認。

【３　対処】

- ホームページ上へのお詫びの掲載、他事業者の店舗への誘導、当該システムを利用しない代替手段での顧客対応等を実施。
- システムを共同利用する複数の事業者間で、テレビ会議システムを利用して情報共有。
- 2系統のうち、障害が発生していないホストコンピュータへ片寄せ。
- ホストコンピュータ、通信制御ソフトウェアを再起動。

【４　原因】

- 大量データの処理が一時的に集中し、ホストコンピュータ上の通信制御ソフトウェアのリソースが枯渇。

【５　再発に備えた対策】

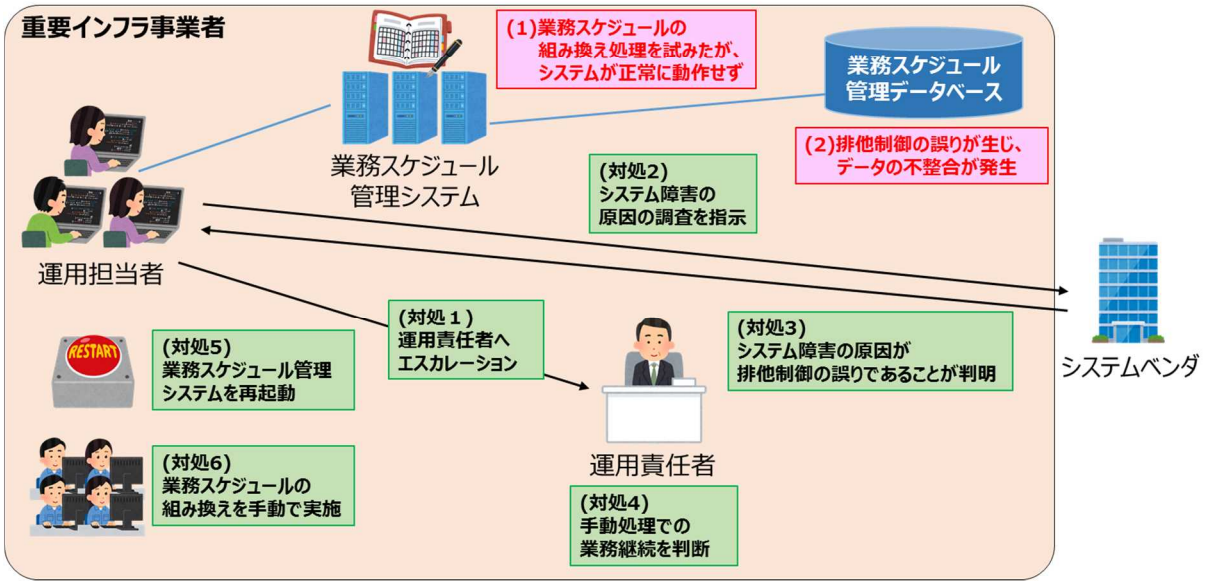
- 通信制御ソフトウェアのリソース監視強化。使用率がしきい値を超えた場合に警告メッセージを通知するようプログラムを変更。
- リソース枯渇時の対応マニュアルを策定。
- データ処理が集中しないよう、共同利用の事業者を順番に処理するように変更。
- 障害発生時、システムベンダから重要インフラ事業者の担当者への第一報がより迅速に伝えられるよう、初動対応を見直し。
- 業務システムの再点検(本件同様の不備の有無等)。

【６　得られた気付き・教訓】

- **緊急時の連絡体制整備**
  サービス提供支障発生時は、原因がシステム障害でも災害と同様の体制としていたことから、連絡体制が明確になっており、迅速な意思決定が行われた。また、権限移譲により、緊急時には、経営層へ情報共有するも、現場の判断に委ねられていたことが奏功した。
- **代替手段の準備**
  店舗では、システム障害が発生した場合に備えて、代替手段を確保していた。定期的に訓練していたため、大きな混乱もなく代替手段で顧客対応等を実施でき、事態の収拾につながった。
- **テレビ会議システムを利用した遠隔地との情報共有**
  システムベンダやシステムを共同利用する他の事業者とテレビ会議システムを利用して連携し、システムベンダからの障害状況・復旧目標等の情報、各事業者の対応状況等を情報共有したことが、全体として統一的・迅速な対応につながった。

事例４　重要インフラサービスの業務遅延

- 重要インフラサービスに遅延が生じたことから、業務スケジュール管理システム経由で業務スケジュールの組み換え処理を試みたが、システムが正常に動作せず、重要インフラサービスの業務遅延が拡大。
- 業務スケジュール管理システムにおいて、排他制御の誤りが発生し、データの不整合が生じたことが原因。
- 再発防止として、データベースから取得したデータが最新であるか否か確認する等、排他制御が確実に実施されるようにシステムを改修。



【１　背景】

- 重要インフラ事業者では、事象発生当日、重要インフラサービスの一部業務に遅延が生じていた。
- 本重要インフラサービスでは、業務に遅延が生じた場合、業務スケジュール管理システムを操作することで、業務スケジュールの組み換えが自動で実施されるようになっていた。
- 業務スケジュール管理システムでは、複数の運用担当者からの業務スケジュール組み換え操作を誤りなく処理するため、排他制御処理（データベースへの同時アクセスによりデータの不整合が生じないよう、データの読み書きを一時的に制限する処理）を行っていた。

【２　検知】

- 運用担当者が業務スケジュール管理システムで、業務スケジュールの組み換え処理を実行したが、変更が反映されなかったことで、事象を把握。

【３　対処】

- システムベンダに原因の調査を指示
- 業務スケジュール管理システムの再起動。
- 重要インフラサービスの進行状況の更なる遅延を防止するため、業務スケジュールの組み換えを手動で実施。

【４　原因】

- 関連システムの一部更改や通信回線速度の高速化の影響で業務スケジュールの組み換え処理の実行速度が向上し、一部処理のタイミングずれが生じたため、排他制御が適切に実施されなくなった。
- 排他制御の誤りにより、古いデータを基に業務スケジュールの組み換えが実施され、業務スケジュールデータに不整合が発生。

【５　再発に備えた対策】

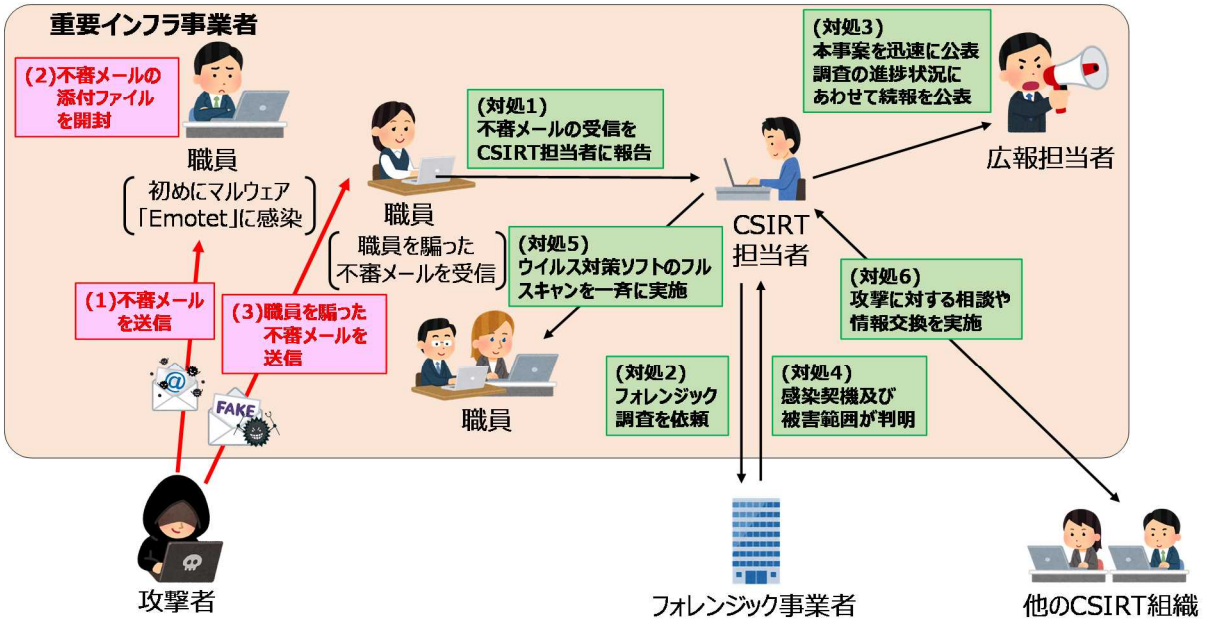
- 排他制御の誤りを防止するため、業務スケジュール管理システムにデータを取得、反映する際に、取得したデータが最新か否か確認する処理をシステムに追加。
- 排他制御の誤りを防止するため、業務スケジュールデータの参照時や更新時に同データにアクセスしている端末が存在するか否か迅速に確認できるよう、システムを改修。

【６　得られた気付き・教訓】

- **運用担当者を育成する取り組みの重要性**
  平時から、重要インフラ事業者では、有識者から運用担当者への業務ノウハウのレクチャや運用担当者間での勉強会の開催等、担当者のスキルを向上するための取り組みを定期的に実施していたため、障害発生時も、複雑な業務スケジュールの組み換え作業を手動で誤りなく実施できた。
- **障害発生時の迅速な判断**
  障害発生時における業務継続方針の決定権者が重要インフラ事業者内で明確になっており、本事案においても、手動での業務継続を迅速に判断できた。
- **排他制御の確実な実施**
  データの不整合が生じないようにするため、データベースから取得したデータが最新であるか否かの確認等、排他制御の仕組みが確実に実施されるようにシステムを設計することが重要。

事例５　不審メールによるマルウェア「Emotet」への感染

- 実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行。
- 重要インフラ事業者の職員が不審メールの添付ファイルを開封し、マクロを有効化したことで、端末がマルウェア「Emotet」に感染。感染後、感染端末を使用していた職員を騙るメールが、外部組織に送信。
- 再発防止策として、クラウド型メールサンドボックスの導入や職員に対する継続的なセキュリティ教育を実施。



【１　背景】

- 実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行していた。
  添付ファイル(Word形式)を開き、マクロを有効化することで、端末がマルウェア「Emotet」に感染した。
- 重要インフラ事業者では、スパムメールフィルタを導入済。
- 重要インフラ事業者は、CSIRT間の情報共有コミュニティに参加しており、他のCSIRTに相談しやすい状況にあった。

【２　検知】

- 重要インフラ事業者（発生組織）の職員になりすましたメールを別部署の職員が受信、発生組織へ連絡したことで、担当者が事象を把握。

【３　対処】

- マルウェア感染が疑われる端末について、フォレンジック事業者にフォレンジック調査を依頼。
- 重要インフラ事業者が管理する全ての端末に対して、ウイルス対策ソフトのフルスキャンを一斉に実施。
- 迅速に第一報を公表した後、詳細な調査結果が判明する度に、続報を公表。

【４　原因】

- 重要インフラ事業者の職員が、外部から送信された不審メールの添付ファイルを開封してしまった。

【５　再発に備えた対策】

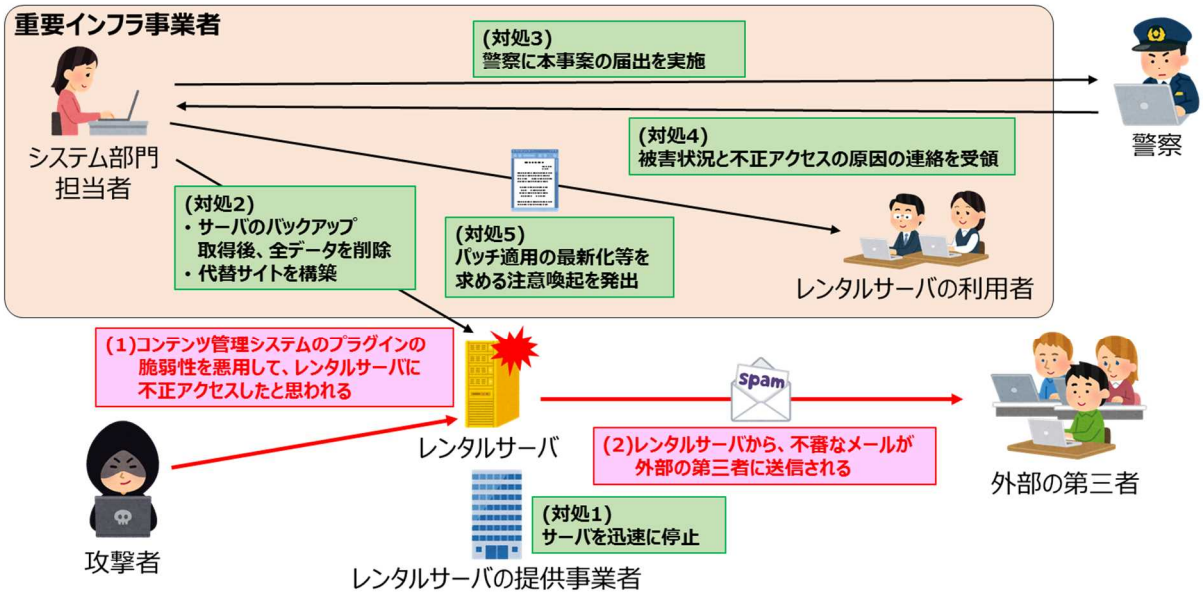
- 組織内のメールセキュリティ対策を強化し、比較的導入が容易なクラウド型のメールサンドボックスソリューションを導入。
- 攻撃の特徴や対策をまとめたリーフレットを全職員に配布。さらに、職員のセキュリティ知識の定着状況を確認するテストを実施。

【６　得られた気付き・教訓】

- **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、漏えいした情報を悪用した攻撃の二次被害を防止した。また、情報を公開したことで、他の重要インフラ事業者の対応にも貢献した。
- **情報共有コミュニティへの継続的な参加**
  日頃から情報共有コミュニティに継続的に参加していたことで、他のCSIRT組織と、本攻撃に対する相談や情報交換をしながら、対応を進めることができた。
- **不審メール受信時の報告体制の整備**
  重要インフラ事業者及び関連組織で、不審メール受信時の報告フローを定め、報告ツールを各端末にインストールしていたことで、本事案発生時にも、不審メールの受信がCSIRT組織に迅速にエスカレーションされた。
- **職員に対する継続的なセキュリティ教育**
  全職員に対し、不審メールの特徴をまとめた小型のリーフレットやマルウェア「Emotet」の概要を記載した文書を配布したり、セキュリティ知識の定着状況を確認するテストを実施したりすることで、職員のセキュリティ知識の底上げを図った。

事例６　重要インフラ事業者が利用するサーバへの不正アクセス

- 重要インフラ事業者が利用するサーバが不正アクセスされ、同サーバから外部に不審なメールが送信。
- サーバに導入していたコンテンツ管理システム(CMS)のプラグインの脆弱性を悪用し、攻撃者がサーバに不正アクセスした可能性が高いと考えられる。
- 重要インフラ事業者は、新たにサーバの運用契約をベンダと締結し、サーバのパッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。



【１　背景】

- 重要インフラ事業者のシステム部門がレンタルサーバを契約し、複数部署でサーバを共同利用していた。
- 重要インフラ事業者自身がサーバへのパッチ適用を実施していた。
- インシデント発生以前から、同レンタルサーバ上で構築されたWebサイトのレイアウトが崩れるといった事象が発生していた。

【２　検知】

- レンタルサーバの提供事業者が「当該重要インフラ事業者が利用するサーバから不審なメールが送信されている」と連絡したことで重要インフラ事業者は事象を把握。

【３　対処】

- レンタルサーバの提供事業者が、当該サーバを迅速に停止。
- バックアップ取得後、サーバの全データを削除し、別環境にて代替サイトを構築。
- システム部門が、レンタルサーバの利用者に対し、パッチ適用の最新化等を求める注意喚起を発出。
- 警察に本事案の届出を実施。

【４　原因】

- コンテンツ管理システム(CMS)のプラグインの脆弱性を悪用され、サーバが不正アクセスされた可能性が高い。

【５　再発に備えた対策】

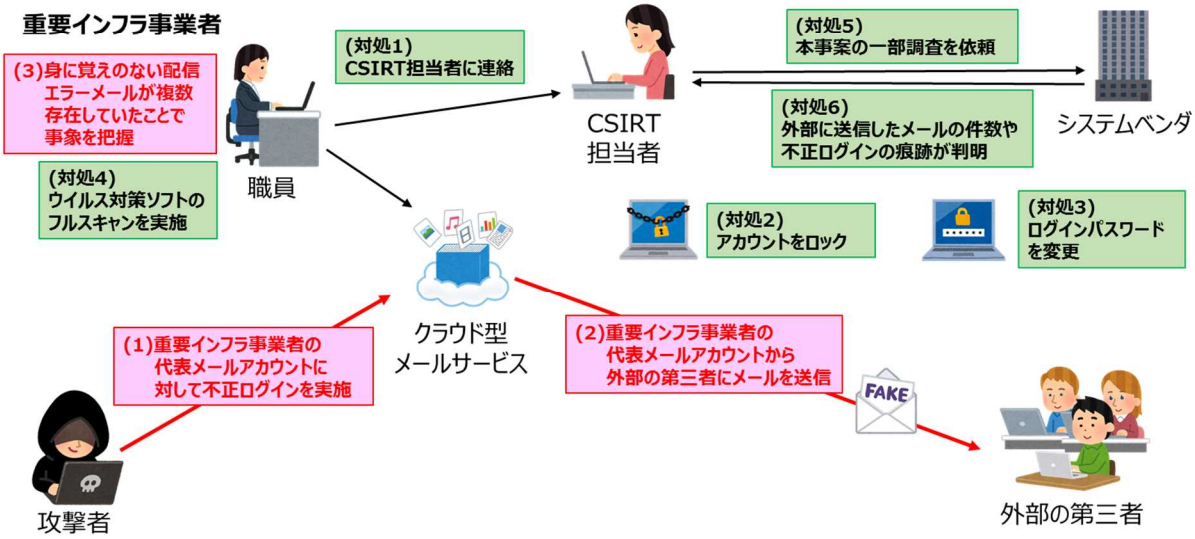
- 新たにベンダとサーバの運用契約を締結し、パッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。

【６　得られた気付き・教訓】

- **セキュリティインシデント及び障害発生時の対応体制の整備**
  有識者に技術的見解を確認できる体制の構築やベンダとの委託契約の締結等を通じて、セキュリティインシデントや障害発生時に、ログの確認やサーバの設定変更等の技術的対応について円滑に実施できる体制を整備することが重要。
- **サーバの資産管理の徹底**
  コンテンツ管理システムのプラグインの脆弱性は、攻撃の対象になり易いため、パッチが公開され次第、できる限り迅速にパッチを適用する等の管理策を講じる。また、自組織の端末やサーバの資産管理を徹底し、インストールしているソフトウェアの一覧やバージョン情報を正確に把握できるようにする。
- **初動対応マニュアル策定の重要性**
  複数部署が関わる複雑なサービス提供体制であったが、初動対応マニュアルを策定し、レンタルサーバの利用者に配布していたことで、被害極小化に向けた対応が迅速に実施できた。
- **迅速な予兆の検知**
  Webサイトのレイアウトが崩れている、身に覚えのないアカウントが作成されている、突然アカウントロックがかかっている等、通常と異なる挙動が確認された場合は、些細なことでもシステム管理者に報告するように、各システム担当者に対し意識づけを行う。

事例７　クラウド型メールサービスに対する不正ログイン

- 重要インフラ事業者が利用するクラウド型メールサービスに対し、攻撃者が不正アクセスを実行し、重要インフラ事業者のメールアカウント経由で、当該事業者とは無関係なメールが大量に外部へ送信。
- 重要インフラ事業者の職員が受信メールボックスを確認した際、身に覚えのない配信エラーメールが複数存在していることに気付き、本事象を把握。
- 再発防止として、クラウド型メールサービスのログイン画面へのアクセス制限や取得可能なログの整理と設定の見直しを実施。



【１　背景】

- 重要インフラ事業者では、クラウド型メールサービスを利用しており、同サービス上に、重要インフラ事業者配下の各組織の代表メールアカウントを作成していた。
- ログイン画面で、ID(メールアドレス)とパスワードを入力することで、メールサービスを利用可能であった。

【２　検知】

- 職員が自組織の代表メールアドレスを確認した際、身に覚えのない配信エラーメールが受信メールボックス内に複数存在していることに気付き、事象を把握。

【３　対処】

- 不正アクセスされたメールアカウントのロックを実施。
- 同メールアカウントを使用していた職員の端末全てに対し、ウイルス対策ソフトのフルスキャンを実施。
- 重要インフラ事業者配下の全ての組織のメールアカウントに対して、ログインパスワードを変更。
- クラウド型メールサービスのログ等をもとに、攻撃者が不正ログインしたアカウント経由で外部に送信したメールの件数や不正ログインの痕跡を特定。

【４　原因】

- クラウド型メールサービスのログイン画面について、どこからでもアクセスできるようになっていた。
- クラウド型メールサービスに対して、IDとパスワードのみでログインできるようになっていた。

【５　再発に備えた対策】

- クラウド型メールサービスのログイン画面にアクセス可能なIPアドレスを制限。
- クラウド型メールサービスのアクセスログ保存期間を見直し。
- Webフィルタリングソフトを用いて、過去に職員がアクセスしたフィッシングサイトをブロック。
- 職員に対するeラーニングやセキュリティ勉強会を実施。

【６　得られた気付き・教訓】

- **クラウド型メールサービスへのログイン強化**
  クラウド型メールサービスについては、業務要件を踏まえ、アクセス元IPアドレスを制限する若しくは、多要素認証を導入する等の不正ログイン対策を講じることが重要。
- **クラウド型メールサービスのログ保存期間の検討**
  クラウド型メールサービスを利用する前に、同サービスのアクセスログやメール送信ログ、メール受信ログ等のログデータの保存期間を十分検討し、万一のセキュリティインシデント発生時に、不正アクセスの原因や被害状況を調査できるようにする。
- **迅速な不正ログインの兆候の把握**
  クラウド型メールサービスの利用者が、身に覚えのない配信不能メールが受信メールボックスに存在する、メールの自動転送設定が追加されている等の異常を把握した場合は、迅速にシステム管理者に報告する旨、職員に教育することが重要である。また、コストは掛かるが、サービスのログを監視するサービスを契約することも選択肢としては考えられる。

（本ページは白紙です。）

別添６　サイバーセキュリティ関連データ集

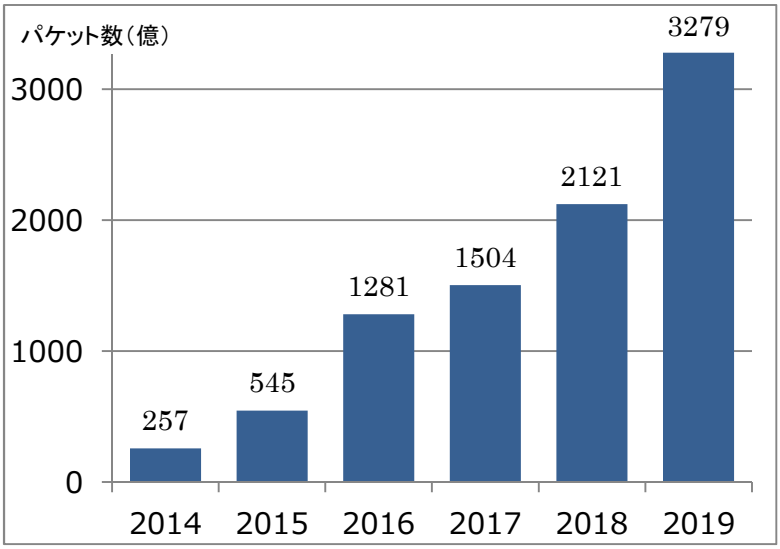
＜別添６－目次＞

データ 1 NICTER 観測結果

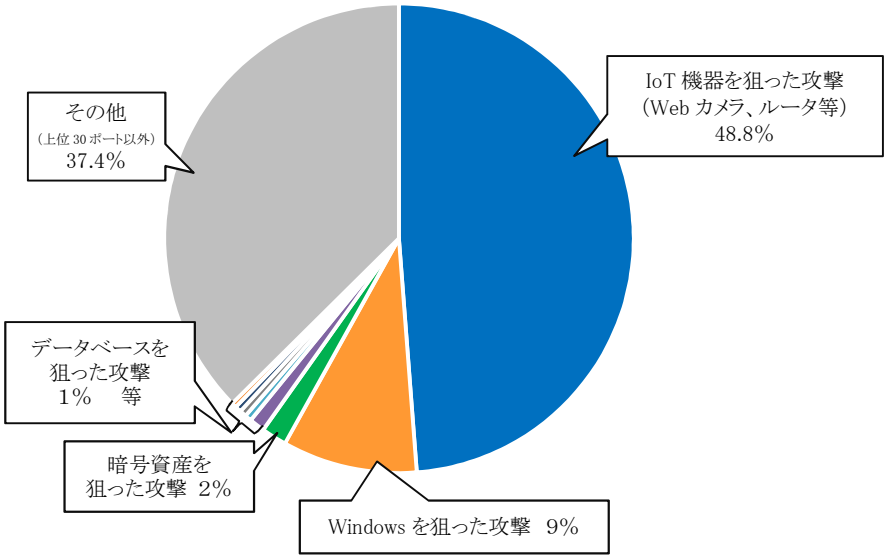
NICT において、未使用の IP アドレス 30 万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測したデータ。2019 年に観測された全サイバー攻撃 3,279 億パケットのうち、約半数が IoT を狙っていることなどが示されている。

そのほか、詳細は「NICTER 観測レポート 2019」（https://www.nict.go.jp/cyber/report.html）にて公開。

データ 1.1 ダークネットセンサによる攻撃の観測数



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）

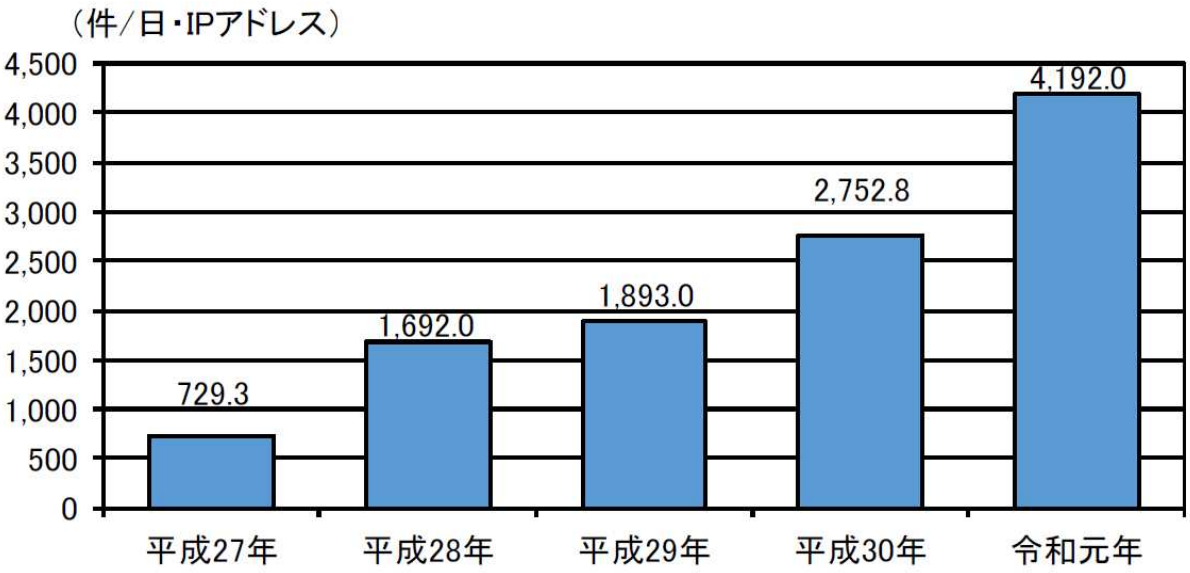


[1] NICTER で 2019 年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位 30 ポートまでを分析したもの。IoT 機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

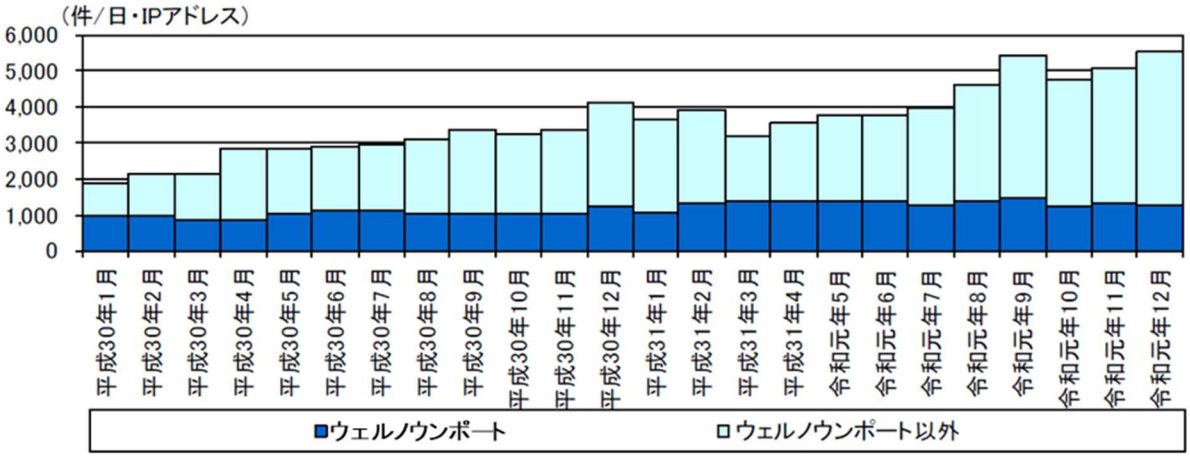
データ 2 警察庁 令和元年インターネット観測結果

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、平成 30 年を「前期」、令和元年を「今期」という。）

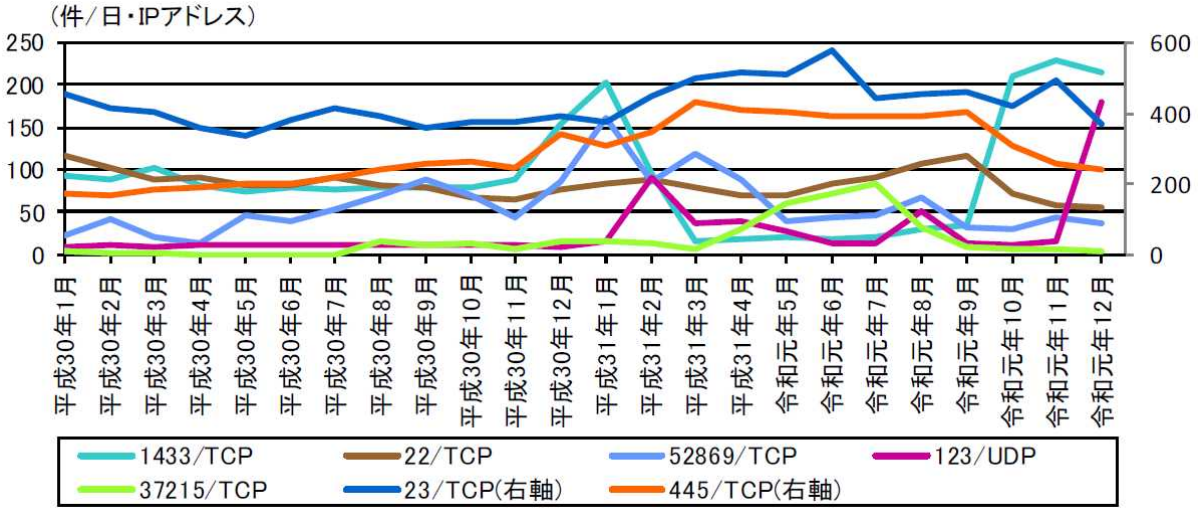
データ 2.1 センサーにおいて検知したアクセス件数の推移



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	461.78 件	＋19.3% （＋74.70 件）
2 位	2 位	445/TCP	357.42 件	＋59.7% （＋133.59 件）
3 位	3 位	1433/TCP	92.53 件	＋3.1% （＋2.78 件）
4 位	4 位	22/TCP	80.82 件	－4.8% （－4.12 件）
5 位	6 位	52869/TCP	66.41 件	＋33.6% （＋16.70 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	445/TCP	357.42 件	＋59.7% （＋133.59 件）	2 位	2 位
2 位	23/TCP	461.78 件	＋19.3% （＋74.70 件）	1 位	1 位
3 位	123/UDP	42.10 件	＋304.6% （＋31.69 件）	8 位	24 位
4 位	37215/TCP	28.51 件	＋366.5% （＋22.40 件）	15 位	33 位
5 位	52869/TCP	66.41 件	＋33.6% （＋16.70 件）	5 位	6 位

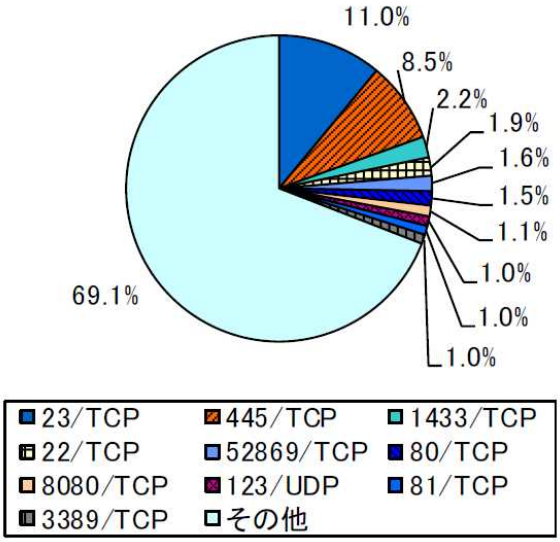
宛先ポート別検知件数（減少順位）

減少順位	ポート	今期件数 [2]	前期比 [2]	今期順位	前期順位
1 位	53/UDP	10.67 件	－70.2% （－25.15 件）	27 位	10 位
2 位	2000/TCP	1.57 件	－81.8% （－7.10 件）	170 位	27 位
3 位	2323/TCP	22.96 件	－18.1% （－5.06 件）	19 位	13 位
4 位	0/TCP	－ [3]	－ [3] （－4.25 件）	－ [3]	42 位
5 位	22/TCP	80.82 件	－4.8% （－4.12 件）	4 位	4 位

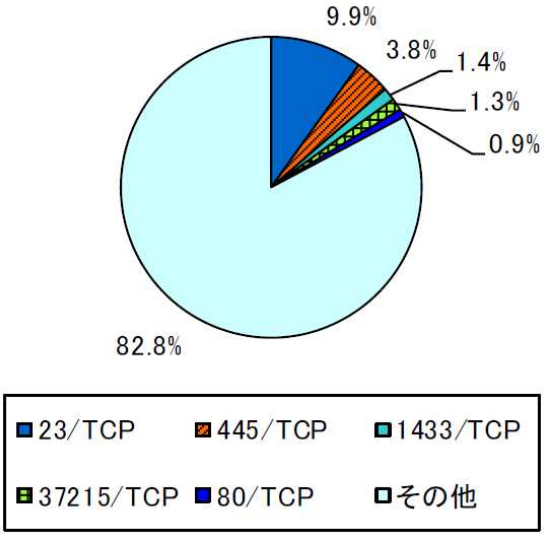
[2] 一日・1IP アドレス当たり。

[3] 今期のアクセス件数が僅かなため、今期件数、前期比及び今期順位は記載していません。

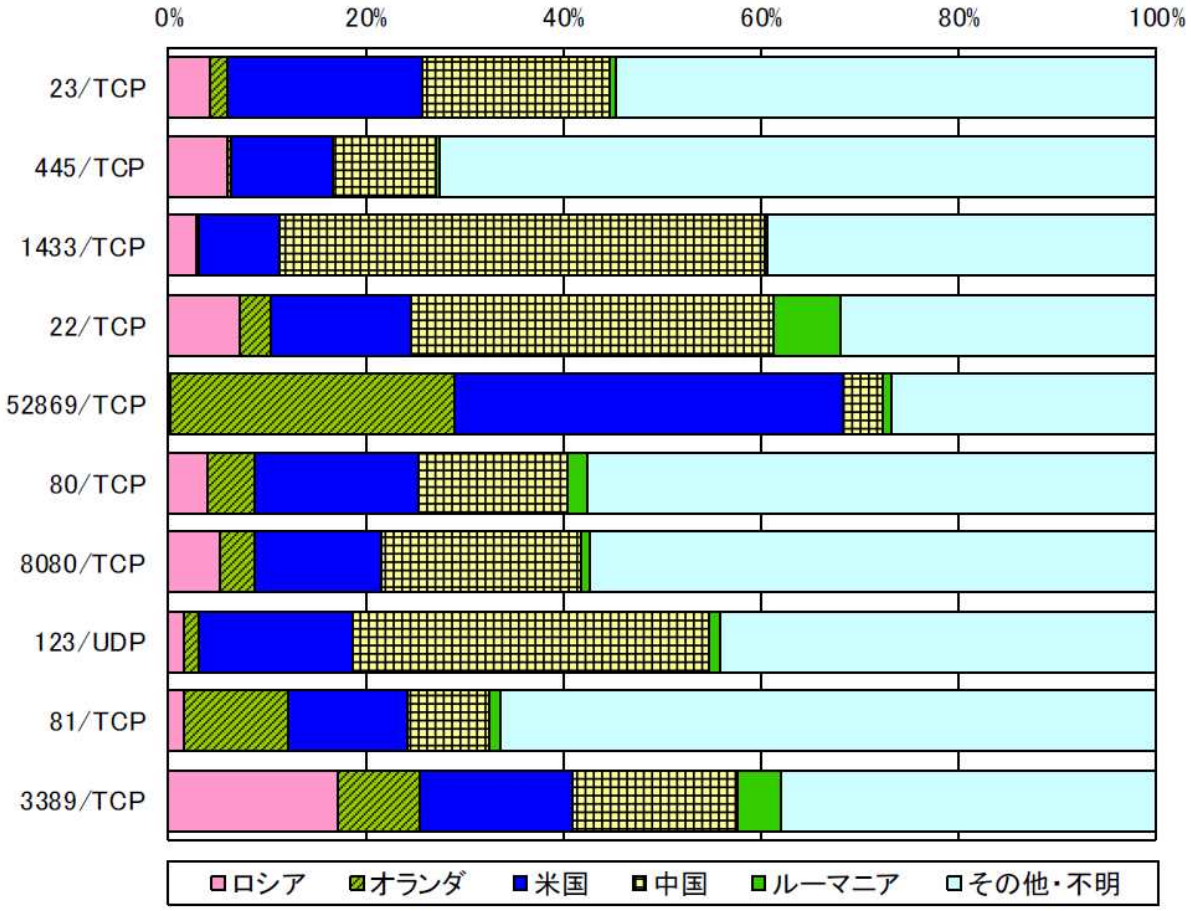
宛先ポート別比率（全て）[4]



宛先ポート別比率（日本国内）[5]



宛先ポート別上位の送信元国・地域別比率[6]

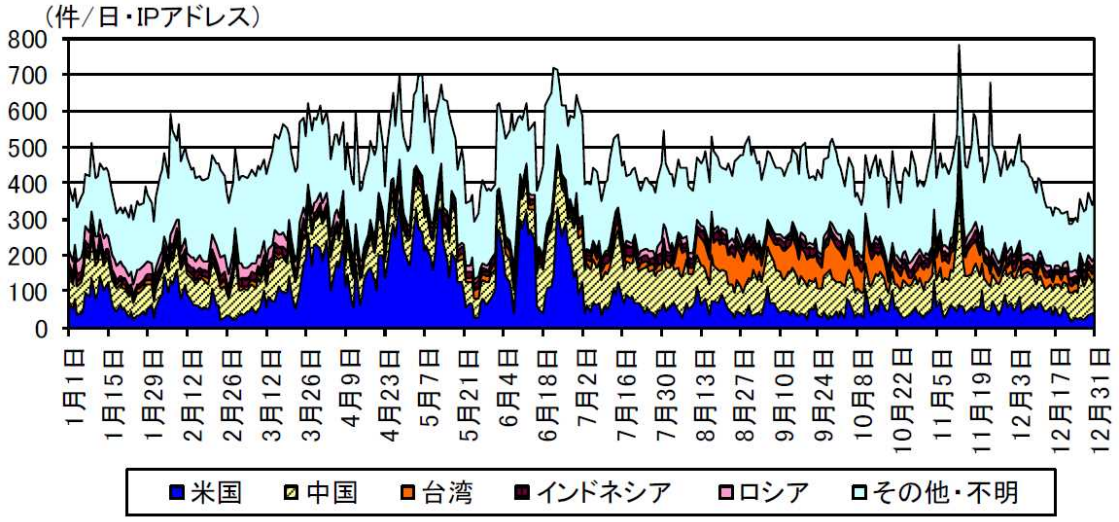


[4] 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがあります。以降の円グラフも同様。

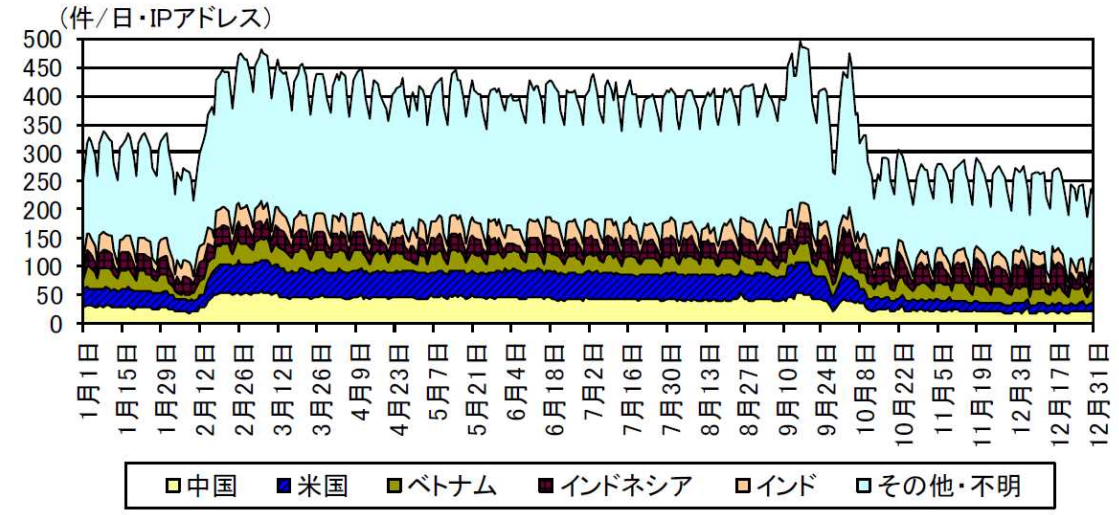
[5] 送信元 IP アドレスが日本に割り当てられているもののみ集計。

[6] 送信元国・地域については、判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。以降も同様の表記。

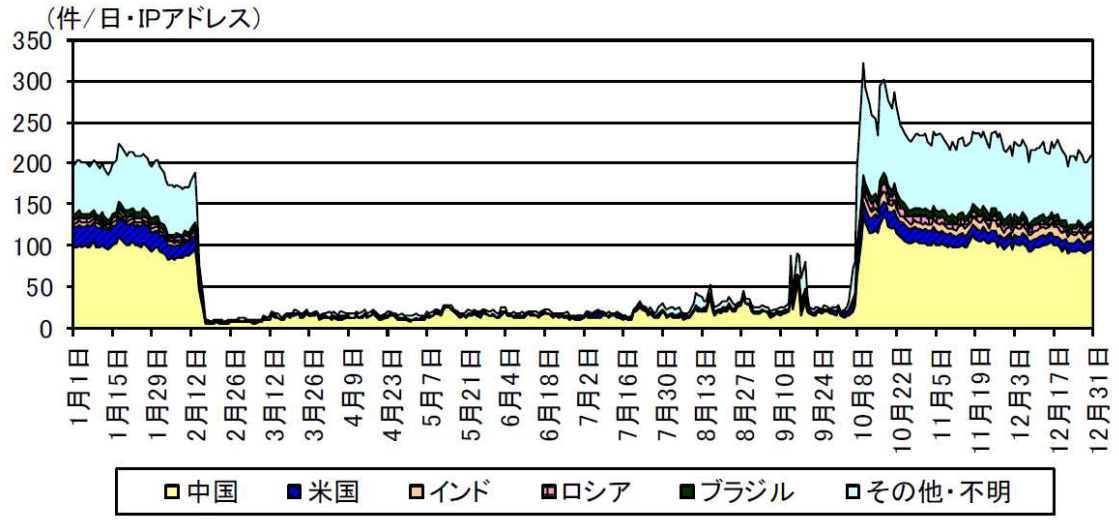
宛先ポート 23/TCP に対するアクセス件数の推移



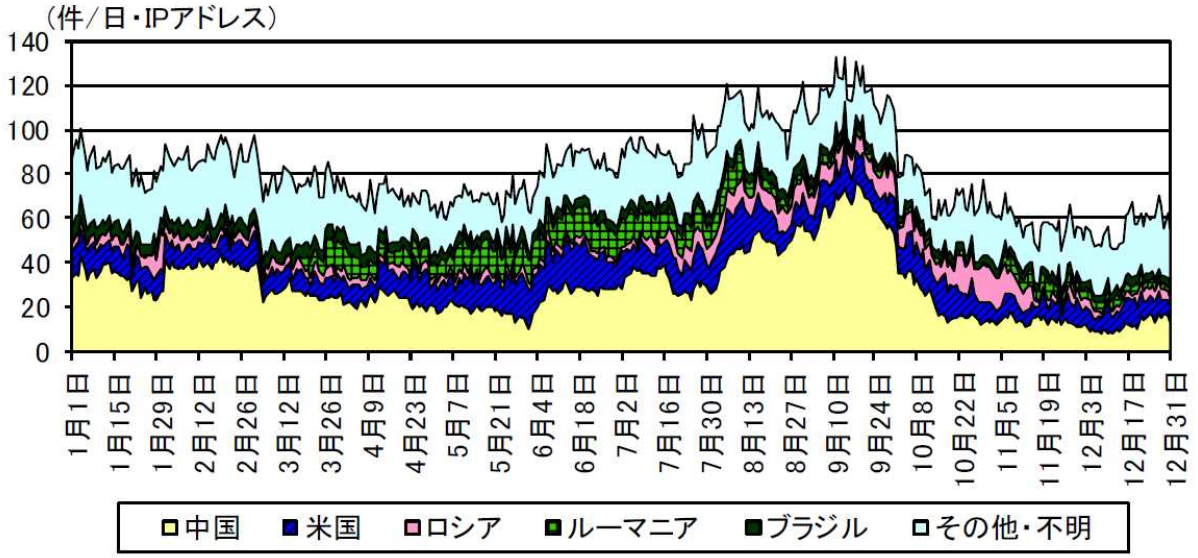
宛先ポート 445/TCP に対するアクセス件数の推移



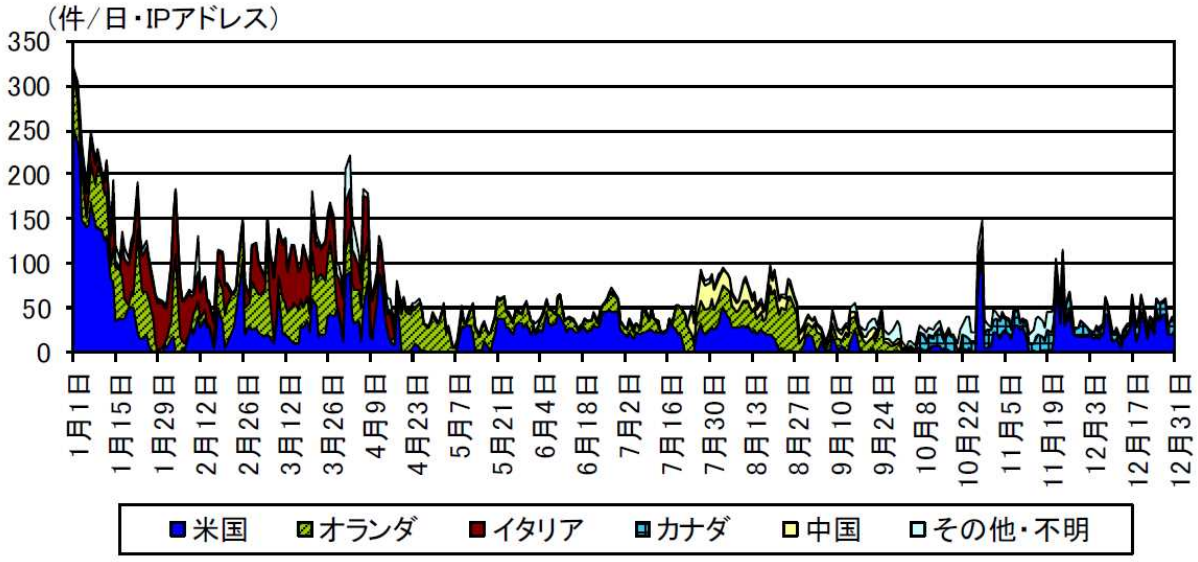
宛先ポート 1433/TCP に対するアクセス件数の推移



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 52869/TCP に対するアクセス件数の推移



データ 2.5 送信元国・地域別アクセス検知件数

送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [7]	前期比 [7]
1 位	1 位	ロシア	785.92 件	＋37.1%　（＋212.48 件）
2 位	4 位	オランダ	711.69 件	－332.6%　（＋547.19 件）
3 位	3 位	米国	582.84 件	＋68.4%　（＋236.83 件）
4 位	2 位	中国	522.18 件	＋34.7%　（＋134.49 件）
5 位	24 位	ルーマニア	114.30 件	＋696.4%　（＋99.95 件）

送信元国・地域別検知件数（増加順位）

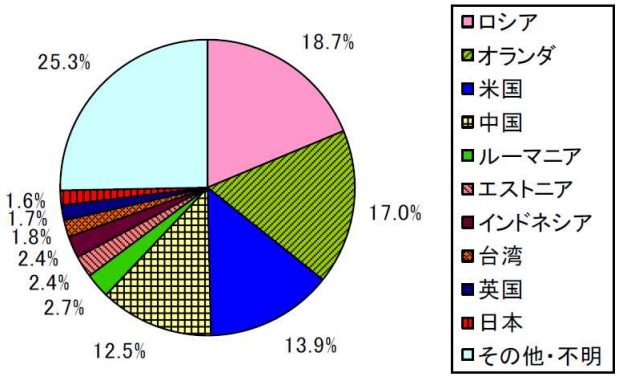
増加順位	国・地域	今期件数 [7]	前期比 [7]	今期順位	前期順位
1 位	オランダ	711.69 件	＋332.6%　（＋547.19 件）	2 位	4 位
2 位	米国	582.84 件	＋68.4%　（＋236.83 件）	3 位	3 位
3 位	ロシア	785.92 件	＋37.1%　（＋212.48 件）	1 位	1 位
4 位	中国	522.18 件	＋34.7%　（＋134.49 件）	4 位	2 位
5 位	ルーマニア	114.30 件	＋696.4%　（＋99.95 件）	5 位	24 位

送信元国・地域別検知件数（減少順位）

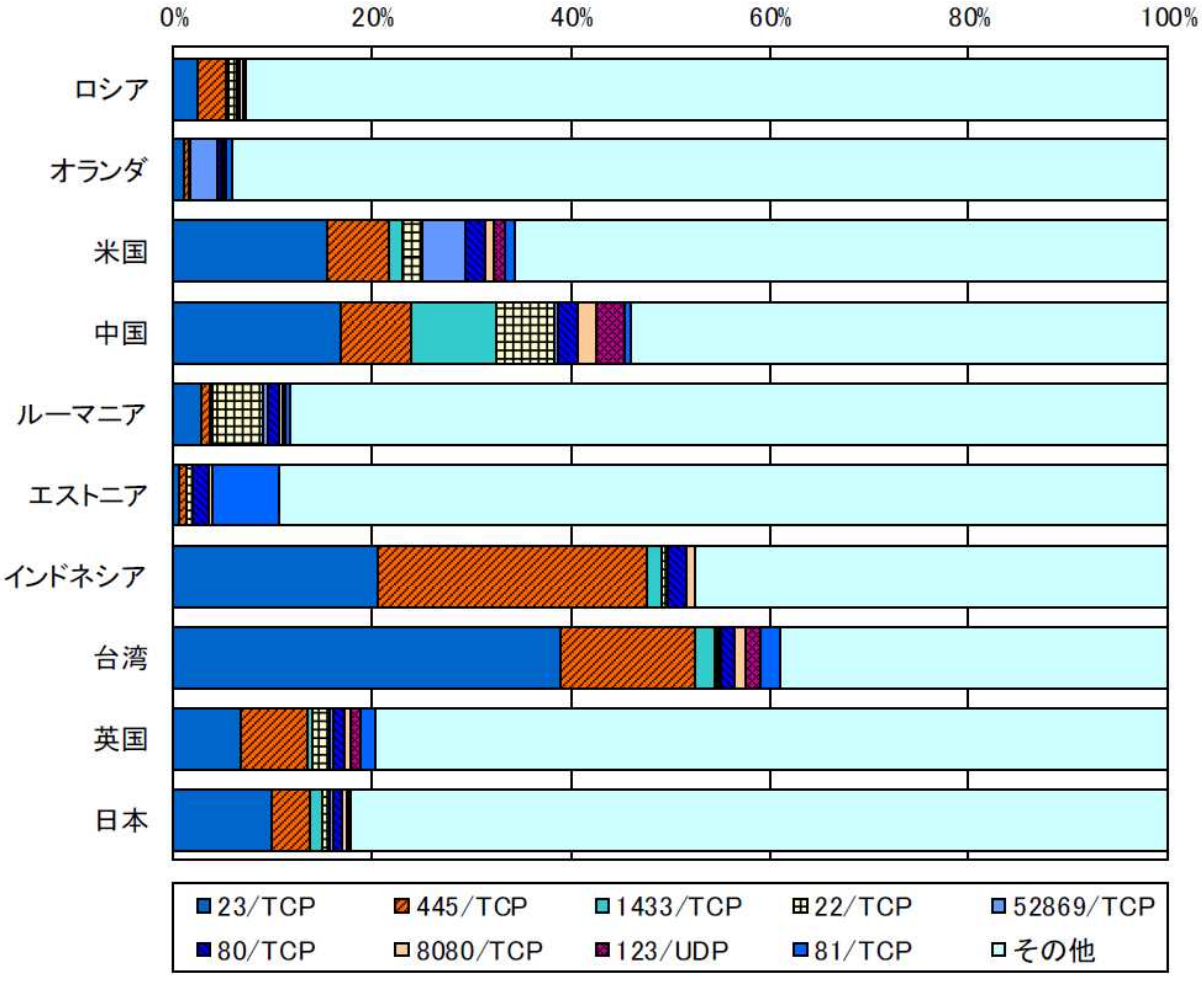
減少順位	国・地域	今期件数 [7]	前期比 [7]	今期順位	前期順位
1 位	チリ	8.55 件	－92.2%　（－100.80 件）	40 位	6 位
2 位	ウクライナ	52.85 件	－62.5%　（－87.98 件）	15 位	5 位
3 位	ドイツ	40.55 件	－33.7%　（－20.58 件）	20 位	11 位
4 位	イタリア	42.93 件	－27.8%　（－16.52 件）	19 位	12 位
5 位	ブラジル	67.06 件	－16.1%　（－12.89 件）	11 位	7 位

[7] 一日・1IP アドレス当たり。

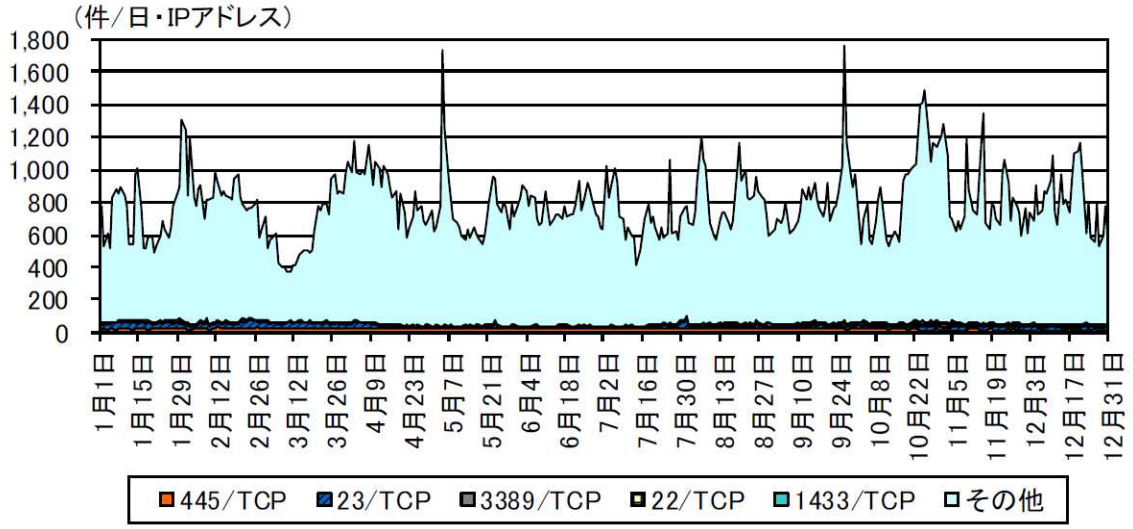
送信元国・地域別比率



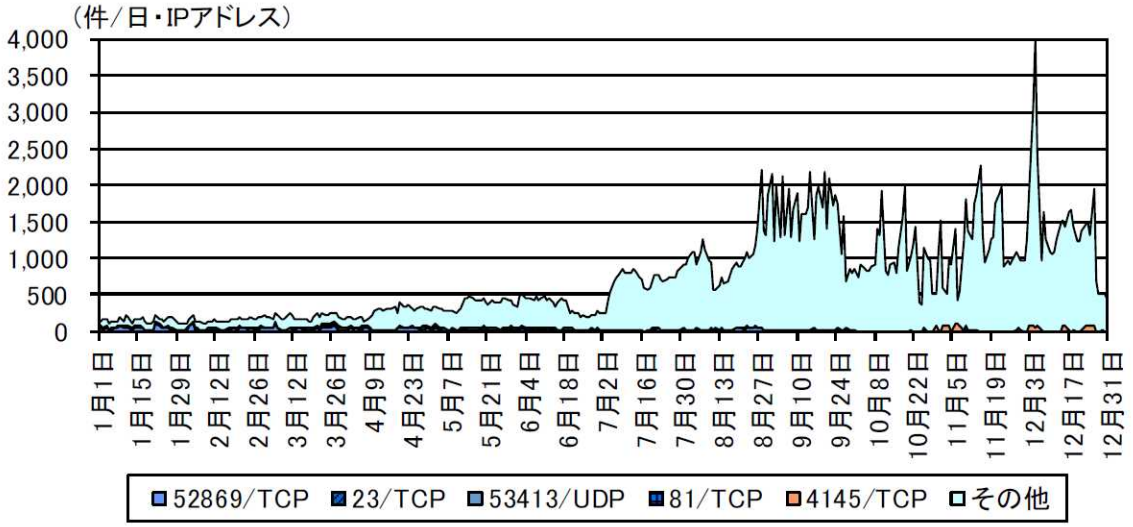
送信元国・地域別上位の宛先ポート別比率



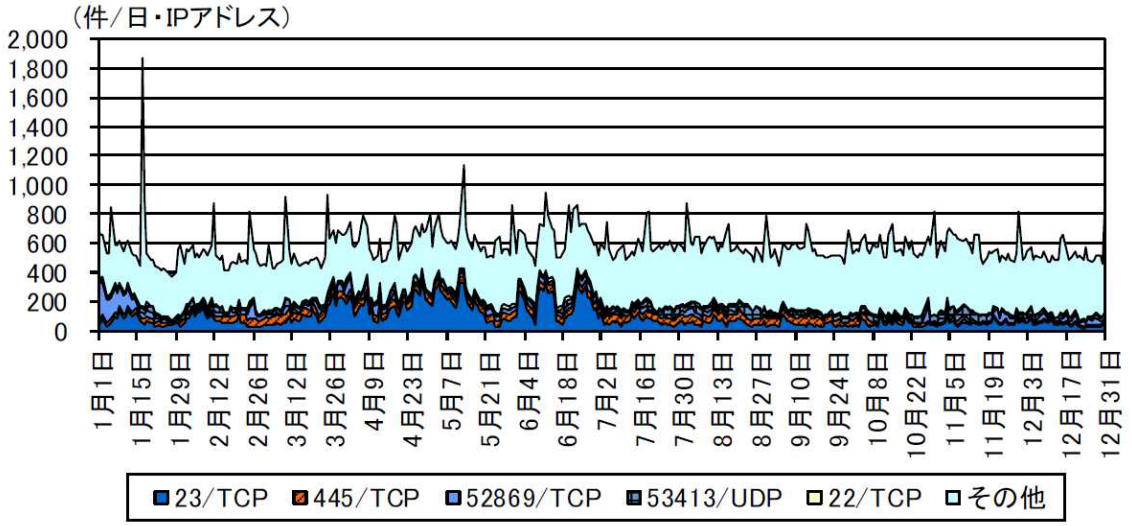
ロシアからのアクセス件数の推移



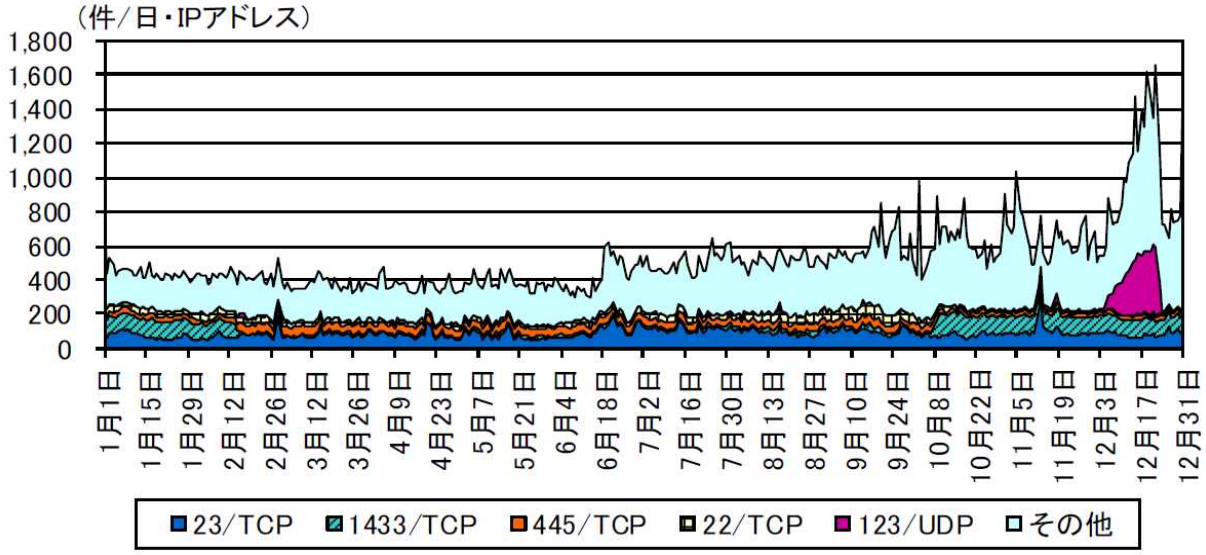
オランダからのアクセス件数の推移



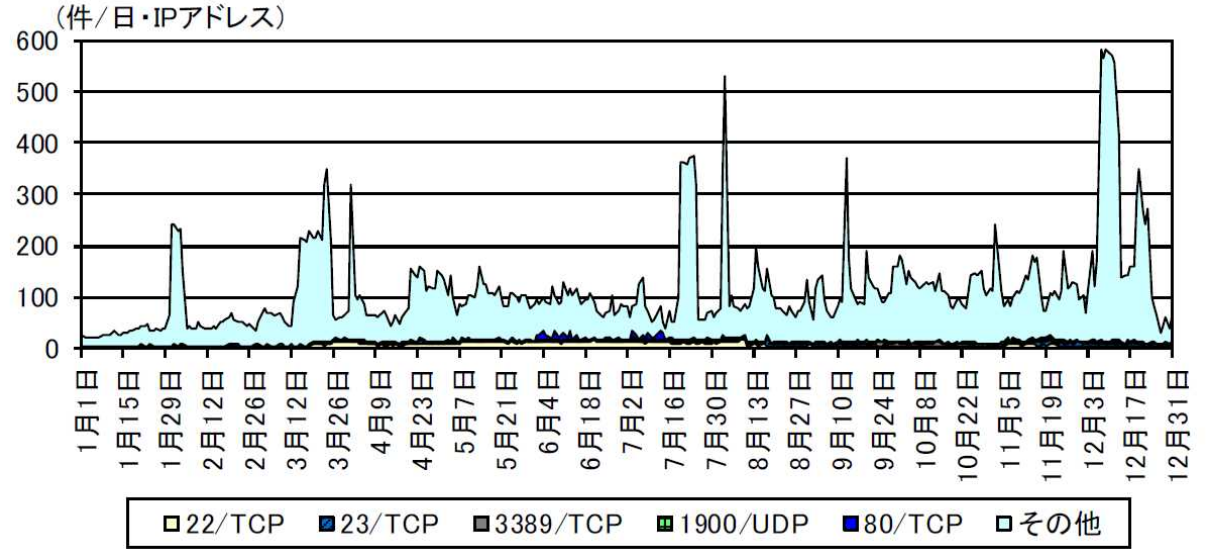
米国からのアクセス件数の推移



中国からのアクセス件数の推移



ルーマニアからのアクセス件数の推移

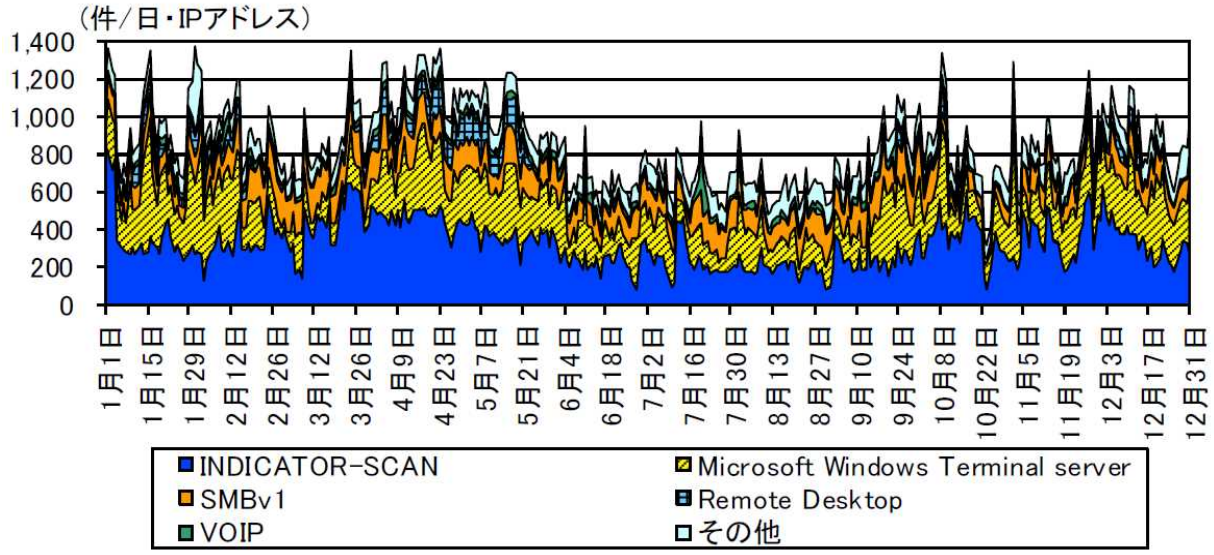


データ 2.6 不正侵入等の観測結果

不正侵入等の攻撃手法別検知件数

今期順位	前期順位	攻撃手法	今期件数[8]	前期比[8]	増加順位	減少順位
1 位	－[9]	INDICATOR-SACN[10]	327.42 件	—[9]	－[9]	－[9]
2 位	－[9]	Microsoft Windows Terminal server[11]	224.88 件	—[9]	－[9]	－[9]
3 位	－[9]	SMBv1[12]	134.19 件	—[9]	－[9]	－[9]
4 位	－[9]	Remote Desktop[13]	34.23 件	—[9]	－[9]	－[9]
5 位	－[9]	VOIP[14]	29.04 件	—[9]	－[9]	－[9]

不正侵入等の攻撃手法別検知件数の推移



[8] 一日・1IP アドレス当たり。

[9] 平成 31 年1月１日以降の不正侵入等の攻撃手法の検知については、攻撃手法の分類見直しを実施したため、前期との比較はありません。

[10] 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

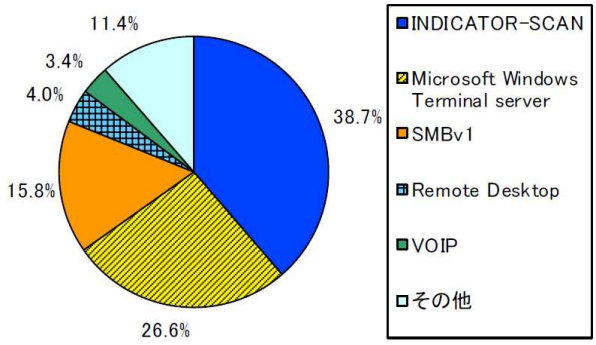
[11] Windows ターミナルサービスに対するスキャン活動等の検知

[12] SMBv1 に対するスキャン活動等の検知

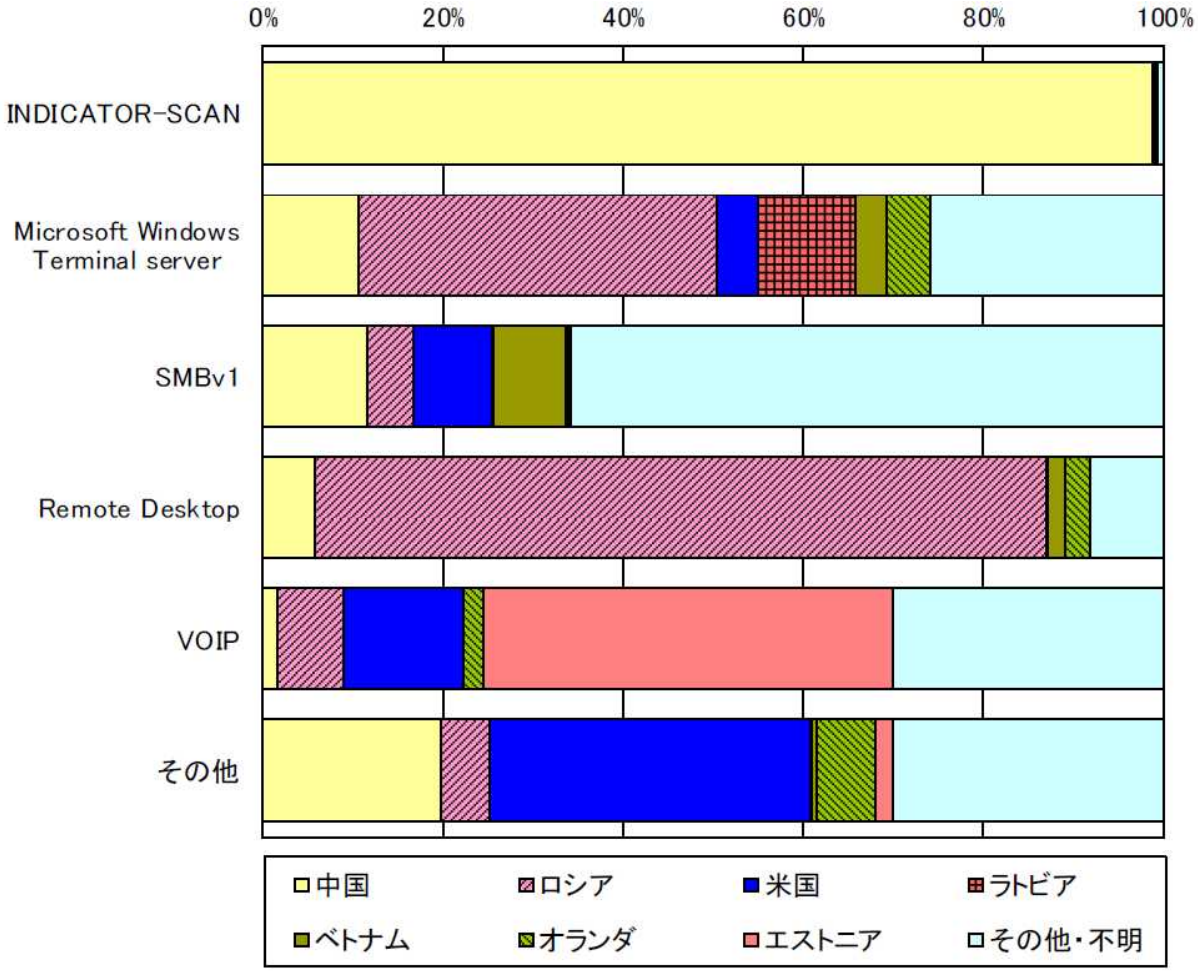
[13] リモートデスクトップサービスに対する攻撃の検知

[14] VOIP に対するスキャン活動等の検知

不正侵入等の攻撃手法別検知比率



不法侵入等の攻撃手法の国・地域別検知比率

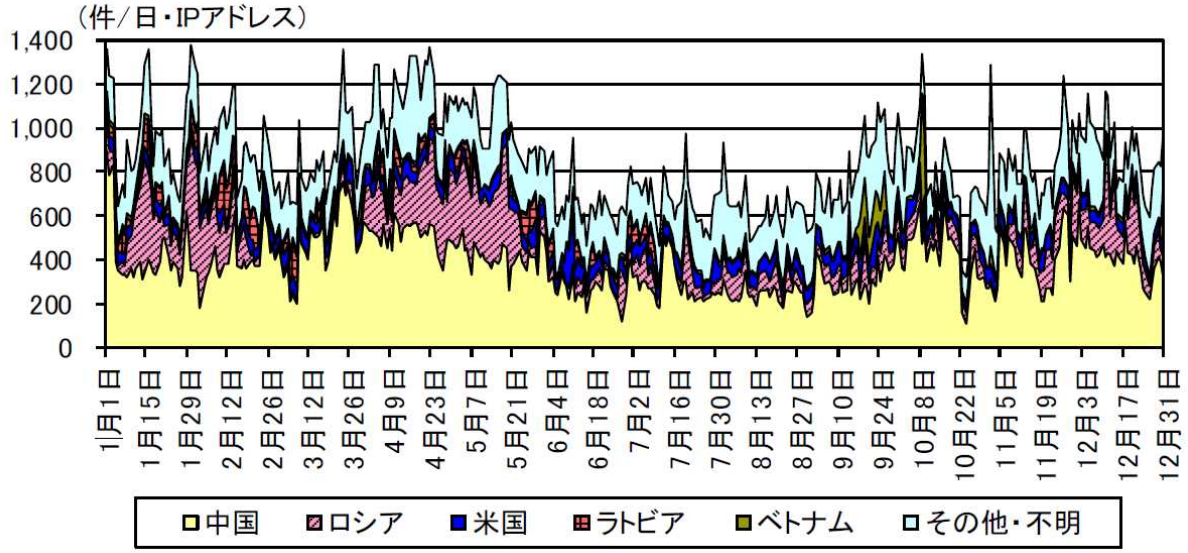


データ 2.7 送信元国・地域別アクセス検知件数

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[15]	前期比[15]
1 位	－[16]	中国	384.50 件	―[16]
2 位	－[16]	ロシア	131.32 件	―[16]
3 位	－[16]	米国	61.87 件	―[16]
4 位	－[16]	ラトビア	24.67 件	―[16]
5 位	－[16]	ベトナム	20.65 件	―[16]

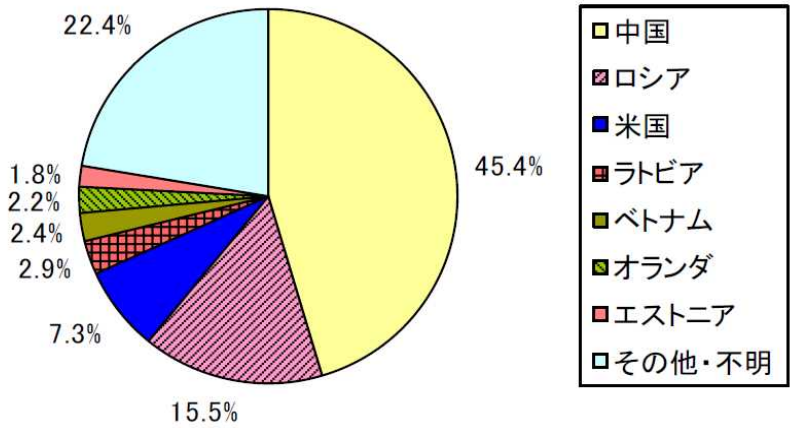
不正侵入等の送信元国・地域別検知件数の推移



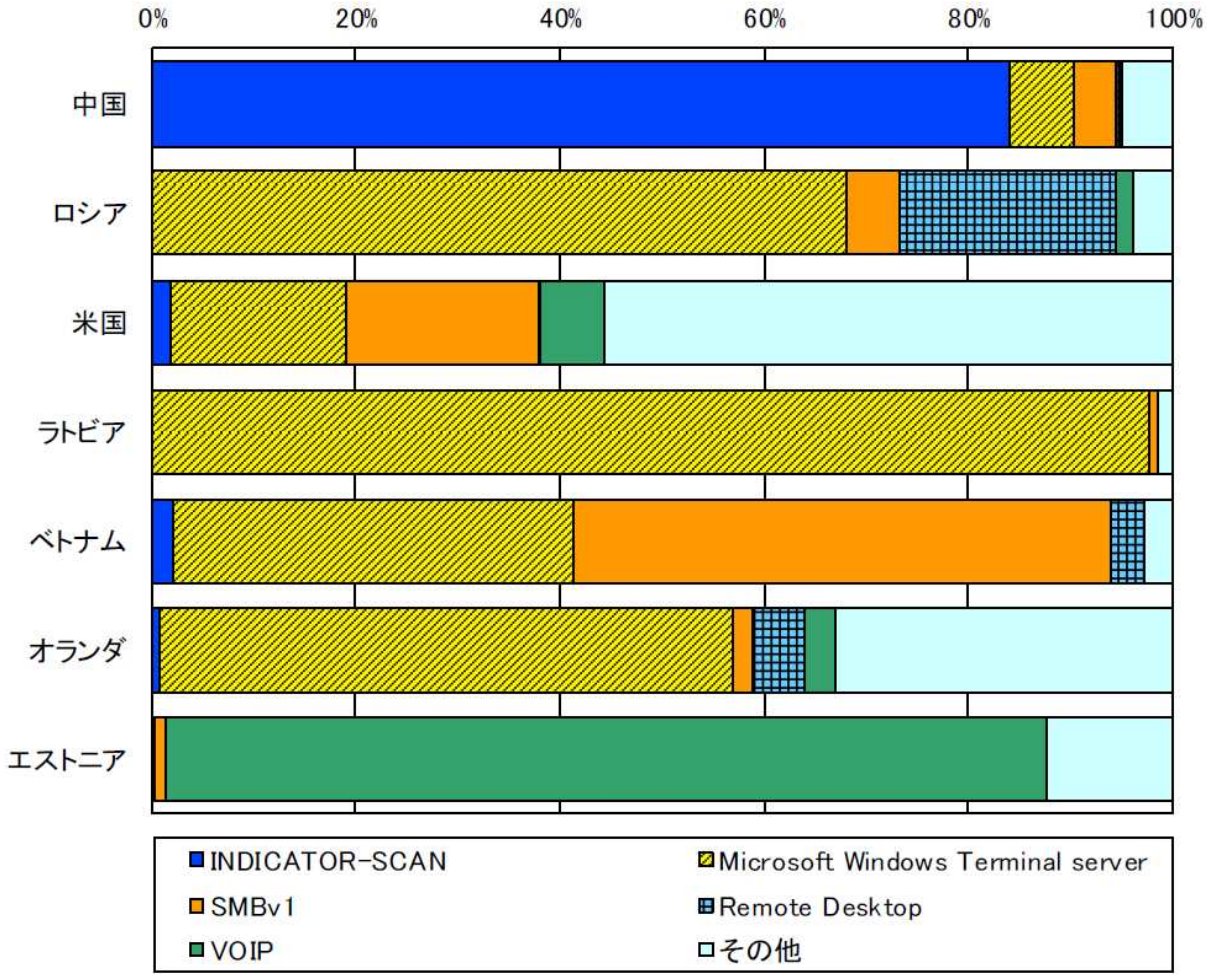
[15] 一日・1IP アドレス当たり。

[16] 平成 31 年1月１日以降の不正侵入等の攻撃手法の検知については、攻撃手法の分類見直しを実施したため、前期との比較はありません。

不正侵入等の送信元国・地域別検知比率

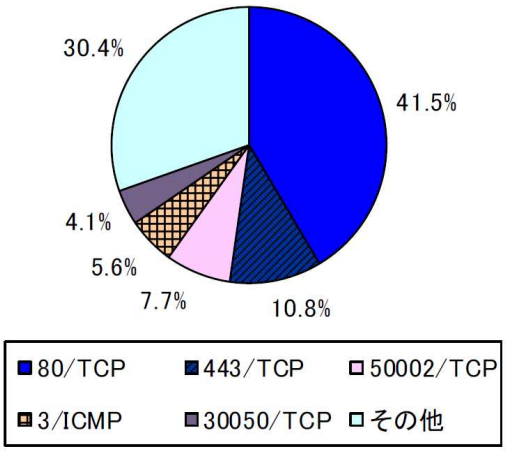


不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

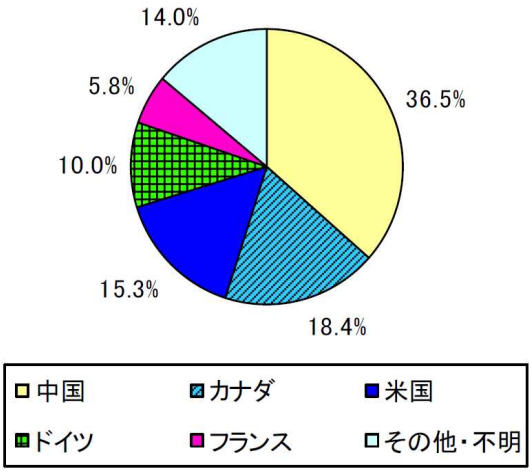


データ 2.8 DoS 攻撃被害の観測結果

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 [17]	前期比 [17]
1 位	1 位	80/TCP	3,847.79 件	−29%　(−1,569.70 件)
2 位	5 位	443/TCP	1,002.27 件	+32.4%　(+245.35 件)
3 位	− [18]	50002/TCP	711.76 件	―　[18]　(+711.75 件)
4 位	9 位	3/ICMP	516.10 件	+185.2%　(+335.13 件)
5 位	4 位	30050/TCP	381.79 件	−64.9%　(−704.88 件)

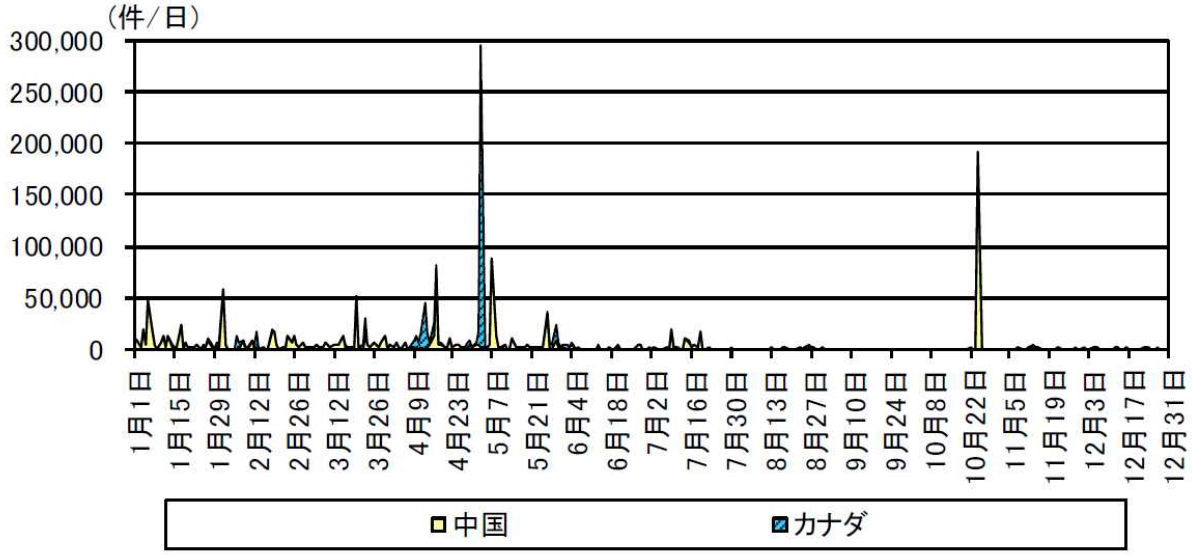
跳ね返りパケットの送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [17]	前期比 [17]
1 位	1 位	中国	3,388.53 件	−75.2%　(−10,248.27 件)
2 位	4 位	カナダ	1,709.88 件	+35.1%　(+444.11 件)
3 位	3 位	米国	1,419.61 件	+1%　(+13.40 件)
4 位	5 位	ドイツ	927.03 件	+307.6%　(+699.59 件)
5 位	2 位	フランス	541.12 件	−65.7%　(−1,036.26 件)

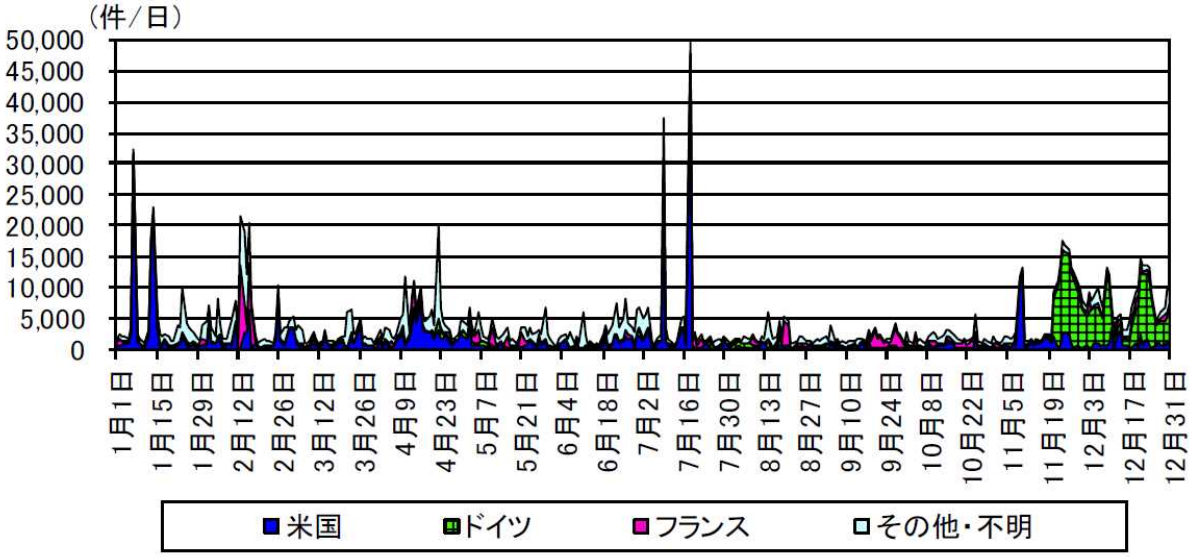
[17] 一日当たり。

[18] 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（中国、カナダのみ）



跳ね返りパケットの送信元国・地域別検知件数の推移（中国、カナダ以外）



データ 3 JPCERT/CC 2019 年度 TSUBAME 観測動向

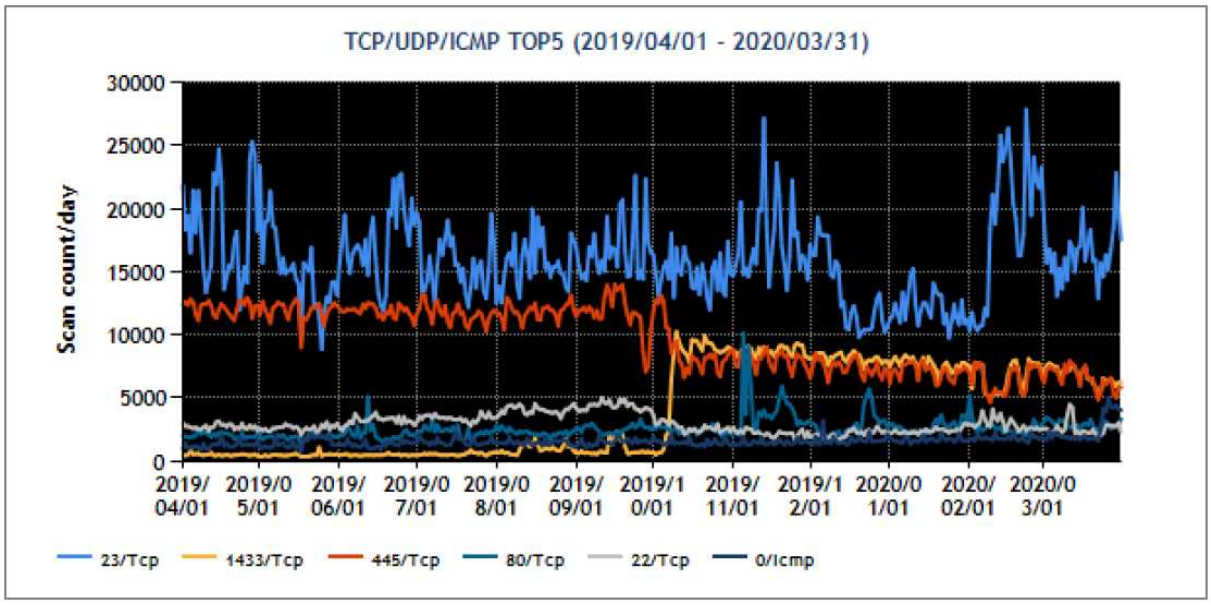
JPCERT/CC にて、不特定多数に向けて発信されるパケットを収集する観測用センサを開発し、海外の National CSIRT 等の協力のもと、これを各地域に複数分散配置した、インターネット定点観測システム（TSUBAME）を構築し運用されている。

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。

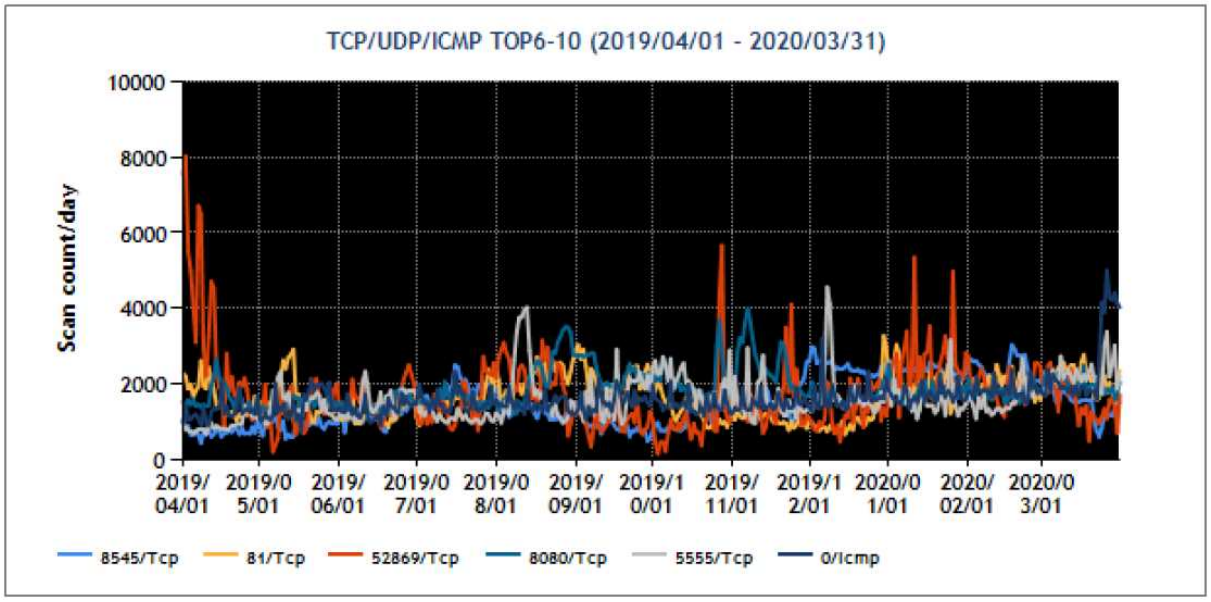
データ 3.1　宛先ポート別パケット数

宛先ポート別グラフ トップ 1-5（2019 年 4 月 1 日-2020 年 3 月 31 日）[19]



[19] 年間を通して、最も多く観測されたパケットは、23/TCP(telnet)宛の通信。このパケットは、Mirai 等のマルウェアに感染した機器が発信することがあり、JPCERT にて、通信元について調査したところ、監視カメラやレコーダー等の機器が見つかったことから、ユーザへの連絡対応等を行っている。2番目、3番目に多かった 445/TCP 宛、1433/TCP 宛についても、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。

宛先ポート別グラフ トップ 6-10（2019 年 4 月 1 日-2020 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			合計			累計
一つ星[20]	二つ星[21]	一つ星 [20]	二つ星 [21]	登録のみ	一つ星 [20]	二つ星 [21]	登録のみ	一つ星 [20]	二つ星 [21]	登録のみ	
243	297	58,461	8,618	5,497	22,281	3,506	5,532	80,985	12,421	11,029	93,406

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	累計 登録者数	令和 2 年度 4 月 1 日時点 登録者数[22]
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	20,762	20,413

[20] 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。

[21] 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。

[22] 累計登録者数から登録削除等 349 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 21 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[23]	情報処理安全確保支援士[24]	年度合計
平成 21 年度	応募者数		52,043	52,043
	受験者数		34,074	34,074
	合格者数		5,906	5,906
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	36,679	43,412	80,091
	受験者数	28,116	28,520	56,636
	合格者数	13,902	5,447	19,349

[23] 平成 28 年度新設。
[24] 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。

（本ページは白紙です。）

別添７　担当府省庁一覧（2020 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	
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	◎：NISC、経済産業省 〇：金融庁
(2)　サイバーセキュリティに対する投資の推進	◎：総務省、経済産業省
(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	◎：総務省、経済産業省
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	◎：総務省、経済産業省 〇：内閣府、国土交通省
(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	◎：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）
(3)　中小企業の取組の促進	◎：NISC、総務省、経済産業省
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の体系の整備と国際標準化	◎：NISC、消費者庁、総務省、経済産業省 〇：法務省
(2)　脆弱性対策に係る体制の整備	◎：NISC、警察庁、総務省、経済産業省
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	◎：総務省
(1)　安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、金融庁、総務省、厚生労働省、経済産業省、国土交通省 〇：内閣官房、内閣府、宮内庁、警察庁、消費者庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：小型無人機等対策推進室 ※内閣府（◎）：政策統括官（科学技術・イノベーション担当）
(2)　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
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	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 〇：警察庁
(2)　地方公共団体のセキュリティ強化・充実	◎：NISC、内閣府、総務省、厚生労働省 〇：内閣官房 ※内閣府：番号制度担当室、個人情報保護委員会 ※内閣官房：情報通信技術（IT）総合戦略室
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	◎：NISC、総務省、厚生労働省、経済産業省
(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	◎：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)　先端技術の活用による先取り対応への挑戦	◎：NISC
(4)　監査を通じたサイバーセキュリティの水準の向上	◎：NISC 〇：内閣府、消費者庁、総務省、外務省、財務省、

	文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省
(5)　組織的な対応能力の充実	◎：NISC、総務省 ○：人事院
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	◎：文部科学省 ○：NISC
(2)　大学等の連携協力による取組の推進	◎：文部科学省
2.5　2020 年東京大会とその後を見据えた取組	
(1)　2020 年東京大会に向けた態勢の整備	◎：NISC、内閣官房、警察庁 ※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
(2)　未来につながる成果の継承	◎：NISC、警察庁、総務省、法務省
2.6　従来の枠を超えた情報共有・連携体制の構築	◎：NISC、警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省
(1)　多様な主体の情報共有・連携の推進	◎：NISC
(2)　情報共有・連携の新たな段階へ	◎：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堅持	◎：NISC ○：外務省
(1)　自由、公正かつ安全なサイバー空間の理念の発信	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省
(2)　サイバー空間における法の支配の推進	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省
3.2　我が国の防御力・抑止力・状況把握力の強化	
(1)　国家の強靱性の確保	◎：NISC、内閣官房、警察庁、法務省、文部科学省、防衛省 ○：内閣府、総務省、外務省、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 ※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 ○：NISC、総務省、外務省 ※内閣官房：国家安全保障局、内閣情報調査室
3.3　国際協力・連携	◎：NISC ○：その他の府省庁
(1)　知見の共有・政策調整	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省
(2)　事故対応等に係る国際連携の強化	◎：NISC、経済産業省 ○：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
4.　横断的施策	
4.1　人材育成・確保	◎：NISC、総務省 ○：文部科学省、経済産業省
(1)　戦略マネジメント層の育成・定着	◎：NISC、文部科学省、経済産業省

(2)　実務者層・技術者層の育成	◎：警察庁、総務省、文部科学省、厚生労働省、経済産業省、防衛省 ○：NISC
(3)　人材育成基盤の整備	◎：総務省、文部科学省、経済産業省
(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	◎：NISC、総務省 ○：その他の府省庁
(5)　国際連携の推進	◎：NISC
4.2　研究開発の推進	
(1)　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）
(2)　中長期的な技術・社会の進化を視野に入れた対応	◎：NISC ○：その他の府省庁
4.3　全員参加による協働	◎：NISC、総務省、文部科学省、経済産業省 ○：法務省
5.推進体制	◎：NISC、内閣官房 ○：警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、経済産業省、国土交通省、防衛省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、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

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。
	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。
	APT10	中国を拠点とするサイバー攻撃集団。APTはAdvanced Persistent Threatの略で、「標的型攻撃」と訳される。米セキュリティ企業ファイア・アイが特定の組織に的を絞って攻撃する複数のハッカー集団を分類し、番号をつけて監視しており、「APT10」はその一つ。
	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。
	CC	Common Criteriaの略。ISO/IEC 15408のこと。情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
	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。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005年以降順次構築が進められ、2020年３月末現在、14分野で19セプターが活動。
	CERT/CC	Computer Emergency Response Team/Coordination Centerの略（サートシーシー）。サイバー攻撃情報やシステムの脆弱性関連情報を収集・分析し、関係機関に情報提供等を行っている非営利団体の一般的な名称。複数の国で設立されており、日本にはJPCERT/CCが設置されている。
	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。
	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	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	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	Fintech	Finance（金融）とTechnology（技術）を組み合わせた造語。ブロックチェーンやビッグデータ、AIといった新たな技術を活用し、多くが急速に普及したスマートフォンやタブレット等を通じて行われる革新的な金融サービス。
	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、2019年６月現在、世界92か国の官・民・大学等480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。

	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推進コンソーシアム	IoT推進に関する技術の開発・実証や新たなビジネスモデルの創出を推進するための体制を構築することを目的として、2015年10月に設立された産官学が参画・連携する組織。
	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。
	ISMS	Information Security Management Systemの略。情報セキュリティマネジメントシステム。
	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-D	International Telecommunication Union Telecommunication Development Sectorの略。ITUの電気通信開発部門。
	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。
	JTEMS	Joint Interpretation Library（JIL） Terminal Evaluation Methodology Subgroupの略。カード端末セキュリティに関する検討部会。
	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	M2M	Machine-to-Machineの略。ネットワークに繋がれた機器同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムのこと。例としては、情報通信機器（情報家電、自動車、自動販売機等）や建築物等に設置された各種センサー・デバイスを、ネットワークを通じて協調させ、エネルギー管理、施設管理、経年劣化監視、防災等の多様な分野のサービスを実現するなど。より広義の概念でIoT（Internet Of Things）と呼ばれることもある。
	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・システム研究機構の一員。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	OECD	Organisation for Economic Co-operation and Developmentの略。経済協力開発機構。
	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。
P	PBL	Project Based Learningの略。課題解決型学習。
	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。
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）。
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。
	グループガバナンス	子会社を保有しグループ経営を行う企業においてグループ全体の企業価値向上を図るためのガバナンス。
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。
	コーポレート・ガバナンス・システム	会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組みに関するシステム。
	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。
	サイバー関連事業者	主として、セキュリティソフトを開発、販売する事業者や、セキュリティに関するサービスを提供する事業者等のこと。サイバーセキュリティ基本法第７条では、「インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。」とされている。
	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エコシステム	2018年７月に策定された新戦略において目指す姿として掲げられた概念であり、全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を一種の生態系にたとえて呼称したもの。
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人材育成プログラム	サイバーセキュリティ関連人材の育成の方向性を示した「サイバーセキュリティ人材育成プログラム」を2017年４月18日にサイバーセキュリティ戦略本部にて決定。
サイバーセキュリティ戦略（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。
	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 27000:2014）
	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。
	セキュリティパッチ	発見された情報セキュリティ上の問題を解決するために提供される修正用のプログラムのこと。提供元や内容によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

	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）を参照。
	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。
た	タイポスクワッティング	任意の者がURLやメールアドレスを入力する際に打ち間違うことを期待して、正規ドメインと紛らわしいドメインを所有しておく行為。紛らわしいドメインへのアクセスやメール送信に対してマルウェアを感染させたり情報を窃取したりすればサイバー攻撃となる。
	ダウンタイム	システム等において障害が発生し、システム等が利用することができない期間のこと。
	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。
て	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）
	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。
	バックドア	外部からコンピュータに侵入しやすいように、“裏口”を開ける行為やその裏口のこと。バックドアがしかけられてしまうと、インターネットからコンピュータを操作されてしまうなどの可能性がある。
	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。
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。
	ブロックチェーン	ブロックチェーン技術のこと。電子署名とハッシュポインタを使用して改ざん検出が容易なデータ構造を持ち、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術（出典：日本ブロックチェーン協会「ブロックチェーンの定義」）。
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。
	ボットネット	マルウェアに感染したコンピュータ等により構成されたネットワークであり、攻撃者はネットワークを構成するコンピュータ等に対して一斉に指令を与えることができる。
	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。
	ポート	ポート番号。コンピュータが通信する際に通信先のプログラムを識別するための番号で、通常利用されるTCP/IPでは、65535番までである。通常、プロトコルに応じてポートが割り当てられている。例えば、FTPはTCPの21番ポート（制御用）と20番ポート（データ用）、HTTPはTCPの80番ポート、HTTPSはTCPの443番ポートを使用する。
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。
む	ムーアの法則	ゴードン・ムーア氏が集積回路に搭載する素子数の長期傾向について提唱したことに由来する法則。一般に、半導体の集積密度が２年で２倍になるといったように指数関数的に増加するもの等と受け止められている。
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。
	リバースエンジニアリング	Reverse engineering。ソフトウェアやハードウェアなどを解析・分解し、その仕組みや仕様、目的、要素技術などを明らかにすること。
	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。