サイバーセキュリティ2019
(2018年度報告・2019年度計画)

令和元年（2019年）５月23日

サイバーセキュリティ戦略本部

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

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

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

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

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

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

＜目次＞

はじめに 1

1部　年次報告（2018年度） 4

1章　サイバー空間と実空間の一体化の進展に伴う動向と対処方針 4

1　本章の位置づけ 4

2　変わりゆくサイバー空間とそれに伴う脅威の深刻化 5

2.1　新たなサイバーセキュリティ戦略の位置づけ 5

2.2　新戦略で目指す姿とサイバー空間における脅威の状況 5

2.3　主なトピック 13

3　新戦略に基づく対処方針 19

3.1　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～ . . 19

3.2　積極的サイバー防御　～事前の能動的な取組～ 20

3.3　2020年東京大会とその後を見据えた対処態勢の強化 22

2章　2018年度のサイバーセキュリティに関する情勢 23

1　サイバーセキュリティの基本的な枠組みに関する情勢 23

2　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 26

3　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 29

3.1　政府機関等におけるサイバーセキュリティに関する体制 29

3.2　2018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 30

3.3　2018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 36

4　サイバー空間に係る国際的な動向 37

3章　2018年度のサイバーセキュリティ関連施策の取組実績と評価 39

1　経済社会の活力の向上及び持続的発展 39

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 39

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 40

1.3　安全なIoTシステムの構築 41

2　国民が安全で安心して暮らせる社会の実現 42

2.1　国民・社会を守るための取組 42

2.2　官民一体となった重要インフラの防護 44

2.3　政府機関等におけるセキュリティ強化・充実 46

2.4　大学等における安全・安心な教育・研究環境の確保 47

2.5　2020年東京大会とその後を見据えた取組 48

2.6　従来の枠を超えた情報共有・連携体制の構築 49
2.7　大規模サイバー攻撃事態等への対処態勢の強化 50
3　国際社会の平和・安定及び我が国の安全保障への寄与 51
3.1　自由、公正かつ安全なサイバー空間の堅持 51
3.2　我が国の防御力・抑止力・状況把握力の強化 51
3.3　国際協力・連携 52
4　横断的施策 54
4.1　人材育成・確保 54
4.2　研究開発の推進 55
4.3　全員参加による協働 57
5　推進体制 59
2部　年次計画（2019年度） 62
1章　2019 年度のトピックとなる取組 62
1　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～ 62
1.1　サービス提供者関連 62
1.2　全ての主体関連 64
1.3　国際協力・連携関連 65
1.4　研究開発関連 66
2　積極的サイバー防御 ～事前の能動的な取組～ 67
2.1　政府関係者の取組 67
2.2　従来の枠を超えた取組 69
3　2020 年東京大会とその後を見据えた対処態勢の強化 71
3.1　2020 年東京大会に向けた対処態勢 71
3.2　大規模サイバー攻撃事態等への対処態勢 72
2章　2019 年度の各種施策一覧表 73
1　経済社会の活力の向上及び持続的発展 73
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 73
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 74
1.3　安全な IoT システムの構築 76
2　国民が安全で安心して暮らせる社会の実現 77
2.1　国民・社会を守るための取組 77
2.2　官民一体となった重要インフラの防護 80
2.3　政府機関等におけるセキュリティ強化・充実 83
2.4　大学等における安全・安心な教育・研究環境の確保 86
2.5　2020 年東京大会とその後を見据えた取組 87
2.6　従来の枠を超えた情報共有・連携体制の構築 88

2.7　大規模サイバー攻撃事態等への対処態勢の強化 89
3　国際社会の平和・安定及び我が国の安全保障への寄与 90
3.1　自由、公正かつ安全なサイバー空間の堅持 90
3.2　我が国の防御力・抑止力・状況把握力の強化 91
3.3　国際協力・連携 94
4　横断的施策 96
4.1　人材育成・確保 96
4.2　研究開発の推進 99
4.3　全員参加による協働 102
5　推進体制 104

別添１　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 .. 105
別添２　2018年度のサイバーセキュリティ関連施策の実施状況 131
別添３　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 . 195
別添４　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 . 239
別添５　サイバーセキュリティ関連データ集 329
別添６　担当府省庁一覧（2019年度計画） 351
別添７　用語解説 355

はじめに

サイバー空間は、実空間との一体化が進展し、経済社会の必要不可欠な基盤となり、人々の生活に様々な恩恵をもたらしている。一方で、これに伴い、悪意ある主体による活動も多様化・巧妙化してきており、経済的・社会的損失が生ずる可能性が飛躍的に高まり、今後、脅威は更に深刻化することが予想される。サイバーセキュリティの確保は、成長戦略を実現するための基盤であるだけでなく、我が国の安全保障・危機管理にとっても極めて重要な課題である。

こうした中、サイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）に基づき、2018年７月、約３年ぶりに新たなサイバーセキュリティ戦略（2018年７月27日閣議決定。以下「新戦略」という。）を今後３年間の基本的な計画として策定した。その後、新戦略に基づく１期目の年次計画であるサイバーセキュリティ2018に基づき、具体的な取組を推進してきたところである。

本書では、2018年度における我が国を取り巻くサイバーセキュリティに関する情勢及びサイバーセキュリティ2018に掲げられた具体的な施策の実施状況等を年次報告としてまとめた。また、これまで、政府が実施する具体的な施策は年次報告とは別の冊子にまとめていたが、新戦略で「本部は（中略）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」とされて相互に関連があるため、本書では、１部を年次報告（2018年度）、２部を年次計画（2019年度）とし、冊子を統合・一本化した。また、関係機関の協力を得て、記載の根拠となるデータを充実化した。

本編に記載のとおり、１部の年次報告で特記すべき点としては、①新戦略の策定（2018年７月27日）、②政府機関等の情報セキュリティ対策のための統一基準群の改定（2018年７月25日）、③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（基本法の改正の成立（2018年12月5日））などが挙げられる。このうち、新戦略はサイバーセキュリティに係る共通の理解と行動の基礎となるため、１部１章でサイバー空間における脅威の動向と主なトピックを加え、その目指す姿と対処方針などのポイントを改めて整理した。また、２部の年次計画では、２部１章で、新たに、新戦略の対処方針に関する国内外の関係者の理解・浸透を図るため、対処方針別にトピックとなる取組を抽出し、その狙いとポイント、主な施策の例を整理した。なお、２部２章では、昨年度と同様、新戦略の体系に沿って、各目的・領域別に、具体的な施策を網羅的に示した。

本書は、新戦略の閣議決定後に初めて作成する年次報告とそれを反映した年次計画を統合・一本化したものである。新戦略に基づき、自律的にサイバーセキュリティに取り組むとともにサイバー空間が持続的に発展する姿（サイバーセキュリティエコシステム）を目指すためには、官民データ活用推進基本法（平成28年法律第103号）等に基づく取組と同時並行的に、サイバーセキュリティの取組に関し、政府機関等は元より、重要インフラ事業者等や企業、そのサービスの恩恵を享受する利用者を含む全ての主体が「参加・連携・協働」していく必要がある。

2018年度の報告も統合した本書の名称は、「人々が美しく心を寄せ合う中で文化が生まれ育つ」との意味が込められた令和[1]の時代においても、協調して施策を推進する文化を引き続き育んでいく観点とともに、名称の継続性も尊重して、「サイバーセキュリティ2019」とした。

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。

[1]安倍内閣総理大臣記者会見（平成31年４月１日）（抜粋）
この「令和」には、人々が美しく心を寄せ合う中で文化が生まれ育つという意味が込められております。

１部　年次報告（2018年度）

1部　年次報告（2018年度）

1章　サイバー空間と実空間の一体化の進展に伴う動向と対処方針

1　本章の位置づけ

昨今、AI、IoT、Fintech、ロボティクス、３Dプリンター、AR/VRなどの知見や技術・サービスが社会に定着し、狩猟社会、農耕社会、工業社会、情報社会からSociety 5.0（超スマート社会）へのパラダイムシフト、サイバー空間と実空間の一体化が進展している。インターネットを通じて、いつでもどこでも、実空間とほぼ同様の社会経済活動を行うことできるようになるだけでなく、サイバー空間を通じて、これまでにできなかったことが次々に実現してきている。時間や場所の制約に捉われず、データの共有・分析等が可能という特質を持つサイバー空間は、人間の活動空間を拡大させている。こうした潮流の中、特定のグローバル企業が先導する激しい国際競争の下、様々なサービスを提供する企業は、中長期的な成長のために、また、それのみならず、事業を継続していくためにも、サイバー空間の利用を避けることはできない。これは、サービスの恩恵を享受する全ての利用者（個人・組織等）にとっても同様である。

一方で、サイバー空間を利用して恩恵を受ける主体は、同時に、サイバー空間における脅威から逃れられない。時間や空間の制約を受けないという特徴を有し、ほぼ無制限にデータ共有・分析等が可能であるサイバー空間を利用し、活動を拡大するのは、悪意ある主体にとっても同様であり、その活動は巧妙化・多様化してきているからである。「情報の毀損及び漏えい」に加え、直接的な「金銭の窃取・詐取等の損害」、さらには、「業務・機能・サービス障害」などが引き起こされる事案が国内外で生じており、国家の関与が疑われる大規模な事案も発生している。サイバー空間上の社会経済活動が飛躍的に増えて恩恵がもたらされれば、その一方で、この空間における脅威が社会経済に与える影響が質量ともに拡大していく。必然的に、サイバーセキュリティの確保は、全ての主体の課題となってきている。

こうした認識の下、政府は、2018年７月、新戦略を策定し、「サイバーセキュリティエコシステム」を目指す姿として掲げた。これは、生活の基盤となる様々なモノやサービスを提供する責任がある政府機関等や重要インフラ事業者等、企業に加え、そのサービスの利用者（個人・組織等）を含めた「全ての主体」が、サイバーセキュリティに関する自律的な取組を行うことで、一種の生態系のようにサイバー空間が持続的に発展していくという概念である。

2000年以降、政府機関等や重要インフラ事業者等は、各種の対策基準や行動計画の策定など様々な取組を進めてきた。基本法は、その目的として、「経済社会の活力の向上及び持続的発展」を最初に掲げており、サイバーセキュリティの確保とともにサイバー空間が発展することを通じて、経済社会の持続的発展を目指すことが重要である。今後、中小企業やそのサービスの利用者にも多大な影響を与えるような、経済社会への影響力を有する企業は、サイバーセキュリティの確保にとっても、根幹となっていくと考えられる。新戦略の推進にあたり、特に、こうした企業の経営層への理解・浸透を図ることを通じて、中小企業や若年層を含む全ての主体の意識が高まり行動につながるというような波及が重要であり、期待される。

以上を踏まえ、本章は、2018年度を中心とした近年の適切なトピックを選び、サイバーセキュリティの確保にあたって、新戦略の理解を深め、実践していくための参考として活用されることを目指し、作成したものである。

2　変わりゆくサイバー空間とそれに伴う脅威の深刻化

2.1　新たなサイバーセキュリティ戦略の位置づけ

新戦略は、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サイバーセキュリティ戦略（2015年９月閣議決定。以下「2015年戦略」という。）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７月～2021 年７月）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、2015年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。

新戦略では、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、サイバー空間の持続的な発展のため、全ての主体が自律的にサイバーセキュリティに取り組む方針を定めた。こうした方針の下、各種ガイドラインの作成や相談窓口の設置、税制優遇措置などの企業に関する施策を含め、各種施策を盛り込んだ年次計画を策定した。

政府は、新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、取り組んでいくこととしている。

2.2　新戦略で目指す姿とサイバー空間における脅威の状況

(1)　サイバーセキュリティを通じたサイバー空間の持続的発展

新戦略で目指すのは、サイバーセキュリティの取組が自律的に行われるとともに、こうした官民の取組によりサイバー空間が持続的に発展することを通じて、Society 5.0 の実現に寄与することである。

Society 5.0は、サイバー空間とフィジカル（実）空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立する「人間中心の社会」である。これまでの情報社会では、インターネット上の膨大な情報から必要な情報を人の手で収集・分析するのに限界があったが、Society 5.0は、人工知能・IoTの活用で、情報の共有・分析が進展し、分野を越えて、人々に様々な恩恵をもたらす社会になるとされる[2]。言い換えれば、次に目指す社会は、サイバー空間と実空間の間でデータが循環して、相互に作用し、これを前提とした様々なサービスが提供され、人々の生活に浸透し、恩恵をもたらす社会である。

近年、具体的な潮流として、インターネット利用者数が増加し、スマートフォンの個人保有率が大きく伸び、SNSの利用割合も伸びているように、サイバー空間上でコミュニケーションを行うことが日常的になり、経済活動においてもネットショッピングや株取引・オンラインバンキング、キャッシュレスサービスの利用が進むなど新サービスが次々登場している。こうした潮流の中、我が国が目指すSociety 5.0では、自動運転など、AI（人工知能）やロボットによって様々な分野で自動化が進むことや、消費者のニーズの変化を的

[2]出典：内閣府資料

確に捉えた商品・サービスの提供、人の健康状態に応じた健康・医療・介護サービスなどが可能になるとされている[3]。また、こうしたSociety 5.0時代にふさわしい行政サービスという観点でも、政府において、行政サービスのデジタル化の推進や、情報システムのクラウド化などの合理化に関する方策の検討が行われている。

(2)　目指す企業経営とサイバーセキュリティの姿　～DX with Cybersecurity～

企業経営にとっても、デジタル化の推進は、新サービスの創出の観点はもちろん、競争環境の下で事業継続するという観点でも重要な課題であり、デジタル化の推進を含むサイバー空間の利用は避けられない課題である。言い換えれば、サイバーセキュリティに取り組まず発展しないまま終わるか、サイバーセキュリティに取り組みながらサイバー空間を有効に活用してビジネスの継続・発展を目指すのかの二者択一を迫られている状況である。今後、国際競争を勝ち抜くためには、サイバー空間を活用して、効率化を追求するとともに、我が国で長年培われてきた顧客重視のきめ細かな商慣習のうち、強みにできる部分も生かし、質を向上させて新しい製品やサービス等の新たな価値を生み出していくとの観点も重要である。

いわゆる「デジタルトランスフォーメーション（DX：Digital transformation)」には、これと同時に、サイバーセキュリティ対策を組み込んでいくこと（DX with Cybersecurity）が、経営課題として求められている[4]。あらゆる産業におけるユーザ企業は、デジタル技術を駆使する「デジタル企業」となることを目指すべき[5]であり、そこに、サイバーセキュリティの確保も含まれなければならない。このように、あらゆる企業が、事業を継続して新たな価値を創出できる「デジタル企業」となるためにサイバーセキュリティの確保に同時に取り組むことを想定し、新戦略では、「サイバーセキュリティ対策をやむを得ない「費用」ではなく、事業継続や新たな価値創出のために不可欠な「投資」であると捉えられるようにする」とされている。

また、新戦略では、「官民のデータ利活用が更に進むと、IoT、サプライチェーン、オープンイノベーションの脆弱な部分を狙う動き（中略）が発生する懸念は高まる」とされており、様々な企業の協業の中で、新しい製品・サービスを創出していくには、サプライチェーン全体が、サイバーセキュリティの確保について同時に、協調して取り組むことが必須である。

こうしたことも踏まえ、新戦略では、自律的な取組の３つの観点として、「参加・連携・協働」とともに、自らの責任で遂行すべき業務・サービスを見定めて取り組む「任務保証」と、完全なリスクの除去は不可能であると認識してリスクを許容し得る程度まで低減する対応を行う「リスクマネジメント」の考え方が明記された。

今後、こうした考え方の理解・浸透を図り、サイバー空間の持続的発展を通じて、Society 5.0の実現に寄与していくことが求められている。

---

[3]出典：未来投資戦略2018

[4] 経団連サイバーセキュリティ経営宣言（2018年３月）では、「いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。」とされている。

[5]出典：DXレポート（平成30年9月7日経済産業省デジタルトランスフォーメーションに向けた研究会）

(3)　身近にあるサイバー空間における脅威とその影響の拡大

新戦略では、脅威について、「AIやIoTなどの技術・サービスが人々に多くの恩恵をもたらす可能性がある一方で、こうした技術・サービスを提供する者がこれらを制御できなくなるおそれは常に内在」とし、実際に、制御できなくなれば、「多大な経済的・社会的な損失が生じ得る」としている。

そもそも、こうした損失を引き起こす「サイバー攻撃」には様々な類型があり、外延が定まっているわけではないが、一般的には、「インターネットやコンピュータを悪用することにより、情報の窃取や改ざんを行うこと等」を意味する[6]。これに対する「サイバーセキュリティの確保」とは、一般的に「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」を意味しており[7]、「外部からの侵入を防ぐ」等の安全性の確保に加え、「障害等が発生しても迅速に復旧すること」等の信頼性の確保の観点が含まれていることに留意が必要である。

①　サイバー空間における脅威による影響

サイバー攻撃による経済的・社会的損失については、新戦略で、「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。」とし、「業務・サービス障害」、「情報漏えい」、「金銭被害」の３点に整理されている。近年、こうした損失を生じさせることを目的とした悪質な攻撃が多様化・巧妙化しており、国家の関与が疑われるような組織的で高度な攻撃手法なども登場している。

なお、サイバー攻撃により、どのような被害実態があるのかを適切に把握することは重要であるが、その被害実態の金銭的価値への換算については、事案ごとに様々な事情があるため単純な試算は困難であり、慎重な検討が必要である。すでに、様々な試算モデルなどの取組[8]が行われており、こうした試みも注視しつつ、サイバー攻撃による被害の実態を適切に把握するよう努めることが重要である。

（ア）業務・サービス障害

新戦略で、「業務・機能・サービス障害による社会への多大な影響」とされ、具体的には、「重要インフラサービスの障害やIoT機器の意図しない作動により、様々な業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ」としている。これまで、我が国で、これに当たる大きな事案は生じていないが、2016年には、ウクライナで、変電所がサイバー攻撃を受けて停電が発生する事案が、2017年には、英国の多数の病院で医療サービスが中断する被害が生じた事案がある。

---

[6] 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。

[7] 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。

[8] サイバーセキュリティ戦略本部普及啓発・人材専門調査会第10回会合（平成30年12月19日）資料２-２参照

（イ）情報漏えい

新戦略で、「情報の毀損及び漏えいによる競争力低下」とし、「情報の毀損」も併せて整理されている。具体的には、「個人情報、営業秘密、価値あるデータを始めとした情報の漏えいは、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・企業の社会的評価・信頼の低下を招くおそれがある。」とし、経済的な損失に加えた、信頼性の損失（いわゆるレピュテーションリスク）のおそれが指摘されている。我が国で、これに当たる事案として、2015年に日本年金機構の保有する個人情報約125万件が流出した事案がある。

（ウ）金銭被害

新戦略で、「金銭の窃取・詐取等の損害」として整理されている。具体的には、「仮想通貨交換業者への不正アクセスやビジネスメール詐欺で巨額の金銭的な被害が発生した事例が生じている。」とされ、2018年、我が国において暗号資産（仮想通貨）の窃取の事案が相次いで発生した。また、2017年には偽の請求書メールによる３億円の詐欺被害が生じた事案など、人間の脆弱性を狙って金銭を詐取する事案が相次いでいる。

②　サイバー空間における攻撃者優位の状況

サイバーセキュリティに効果的に取り組むためには、「彼を知り己を知る」という意味で、こうしたサイバー攻撃を行う悪意ある主体とそのグループ（以下「攻撃者」という。）とともに、これを防御する主体（以下「防御側」という。）の置かれた環境・状況を正確に把握・分析することが求められる。

攻撃者と防御側が置かれた環境について、新戦略では、「この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。」とし、攻撃者について、「攻撃プログラムを含むデータや情報を容易に複製・流通させることが可能」、「進展するAIやブロックチェーン 等の技術も柔軟に取り入れて自由に利用できる。」とし、「防御側と比べて非対称な優位性」があると結論づけている。一方で、防御側について、新戦略では、「防御側の体制が従前の制度や技術体系を前提としている場合には、その優位性が高まると考えられる。」としている。

まとめると、その優位性は、攻撃者はサイバー空間の特性を生かして、場所・時間の制約を受けずに攻撃できることと、攻撃を隠匿する技術を含む多様な技術を低コストで利用できるという点、一方で、防御側はその従前の制度や技術体系の制約を受ける点に集約される。

（ア）攻撃者の状況　～時間・場所の無制約、低コストかつ豊富な手段～

サイバー空間は、いつでも国境を越えてどこからでも参加でき、恩恵をもたらす一方で、攻撃に悪用することも可能である。こうした悪用された場合のサイバー空間の特徴を示す調査として、2017年に行われた実証実験によれば、インターネットに接続された脆弱なIoT機器が、最短で38秒でマルウェアに感染したとの報告[9]もある。それを誰もが観測できるわけではない。言うなれば、目に見えない犯罪者が常に家の周りを徘徊しているともいえ、脆弱なIoT機器が鍵のかかっていない家に

[9]出典：ＩｏＴマルウェア駆除と感染防止に関する実機を用いた実証実験（2017年横浜国立大学）

たとえられることもあるが、このような比喩だけでは十分に説明しきれない脅威がある。

攻撃者は、単独で攻撃する場合でも、年齢・性別・資格などに関わらず、実態上、サイバー空間上の攻撃プログラムなどを容易に入手・複製できるため、高いコストをかけずに、攻撃のための手段を手にすることができる。悪用できる技術の中には、発信元を秘匿化するソフト[10]があり、実際に、暗号資産（仮想通貨）流出に関して初摘発された事案で用いられたとする報道もある。また、IoT機器を乗っ取り、これを踏み台にして、攻撃元を偽装することも可能である。また、外部の資源を利用することも容易である。一般に見えないダークウェブと呼ばれるサイバー空間上の市場で、攻撃用の様々なツールの売買や攻撃を請け負う業者が存在するとの調査結果[11]もある。さらに、サイバー空間上で多数の協力者を募ることや、IoT機器を乗っ取ることなどができれば、勝手に他人の資源を用いることも可能になる。これに加え、国家の関与が疑われる事例では、その後ろ盾や暗黙の支援があると考えられる。このように、攻撃者は、既存の制度や技術体系に縛られることなく、豊富な人的資源・コンピュータ資源を用いることが可能である。

（イ）防御側の状況 ～限られた資源、脆弱性の完全除去は不可能、攻撃者特定困難～

防御側は、一般的に、従前の制度や技術体系の枠内での対応をせざるを得ず、使用できる資源は限られており、柔軟な対応が難しい。また、そもそも、利用する情報システム等とそれを運用・操作する人間の脆弱性を完全に除去することは不可能である。

情報システム等について、人間が作るものであるがゆえに、その脆弱性を完全に除去するのは難しく、意図しない脆弱性が残ることがある。また、悪意のある攻撃者が脆弱性を組み込む場合があり得る。こうしたことに対して、セキュリティ・バイ・デザインに基づく取組とともに、引き続き、脆弱性情報の公表や修正プログラムによる対応等を日々、地道に行っていくことが求められる。

また、情報システム等を操作して重要な決定を行う主体たる人間が、実空間と同様、誤解、思い込みなど正常な判断ができない状態で操作を行えば、誤作動等を引き起こし得る。こうした人間の脆弱性は、誰でも持っているものであり、完全に除去することは不可能である。近年、こうした人間心理の隙を利用した攻撃、いわゆる「ソーシャルハッキング」が注目されている。具体的には標的型攻撃やビジネスメール詐欺など大きな事案が生じた例もある。攻撃者が、防御側の親しい相手や上司などに偽装することや、判断を急がされる、防御側の欲望や恐怖心を刺激するなどにより、正常な判断を阻害する事例が見られる。また、非日常のイベントの開催などの要因によっても、正常な判断が阻害される状況が考えられる。

さらに、防御側は、攻撃そのものに気づかない場合や、原因究明に時間を要し、その明確な証拠を収集することは困難であること、信頼性の損失（いわゆるレピュテーションリスク）を恐れて、公開を原則とする民事訴訟を起こすことも難しい[12]ため、攻撃者の特定のために資源を投入しづらい問題もある。防御側は、完全な対

[10] Tor等
[11] 出典：McAfee Labs脅威レポート（2018年12月）
[12] 「サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か」（林紘一郎、田川義博著2018年11月）参照

策は難しく、かつ、攻撃者を特定して対処することは、少なくとも、単独では困難な状況である。

③　サイバー空間における脅威の影響が広がる可能性

こうした攻撃者優位の状況で、サイバー空間における脅威が深刻化する中、攻撃者の実態を把握しつつ、近年の動向を踏まえて脅威がどのように変化していくのか、今後の可能性について想定することも重要である。

攻撃者の実態について、完全な把握は不可能であるが、民間事業者による調査結果（2018 年６月）[13]によれば、見落としがちな内部の攻撃者の存在や、組織犯罪グループの割合が大きいという傾向が分かる。攻撃者の目的について、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。以下「2013年戦略」という。）では、「初期のサイバー攻撃には、自己顕示欲（中略）等を目的とした愉快犯（中略）が多かった。（中略）金銭や示威を目的とするものが出現し、最近では国家や企業の機密情報等を窃取しようとするもの、重要なデータやシステムを破壊しようとするものが顕在化」としている。前述の民間事業者による調査では、「サイバー犯罪のほとんどが、金銭的な目的を動機」とし、愉快犯やスパイ活動もあるとしている。

これらも踏まえ、攻撃者の目的を整理すると、精神的目的（愉快犯等）、経済的利益目的（金銭入手等）、政治的目的（スパイ活動等）の３類型に整理できる。

精神的目的の攻撃については、暗号資産（仮想通貨）流出で初摘発された事案では、犯人が若年層であり、動機がゲーム感覚であったとする報道もあった。近年、若年層の不正アクセス禁止法違反の検挙が他の世代に比べて高い[14]ことも踏まえると、情報モラル・倫理を含むリテラシー教育が重要である。加えて、サイバー空間に係る高度な技術を有する技術者を、攻撃者にさせないための取組も引き続き求められる。

経済的利益目的の攻撃については、昨今、割りの良い犯罪として、分業化が進み、産業化しており、現在の脅威の中核をなしていると指摘されている。こうした目的の前段階で、個人情報や認証情報を窃取する動きもある。いかに安いコストで多額の金銭を得られるかという費用対効果の観点で攻撃が行われるため、攻撃に係るコストをいかに高くできるかという視点での対処が有効であり、基本的な対策の徹底等が重要である。

政治的目的の攻撃には、国家の関与が疑われるものなどが指摘され、脅威は高まっており、それ以外にもハクティビストによるものもあると指摘される。これらは、経済社会に与えられる影響が大きければ、コストのかかる手法であっても、組織的な支援の下で、実行されるおそれがある。政府機関等や重要インフラ事業者等、経済社会に大きな影響力がある企業は、こうした攻撃を念頭におき、基本的な対策の徹底に加え、事前の積極的な防御策の強化や、迅速な復旧を含む対処態勢の構築に取り組むことが重要である。

併せて、自然災害などのサイバー攻撃に因らない要因により重要インフラサービス障害が生じた事例もあり、障害発生時点では要因が明確にならず、サイバー攻撃による障害が含まれることがあり得るため、対処態勢の構築においても、サイバー空間と実空間

[13]　出典：2018年度データ漏洩/侵害調査報告書（Verisonの調査（2018年６月）。65か国、67組織の協力を得て、53,308件のインシデントを対象にした調査）全体の約４分の３が外部の攻撃者（うち半数が組織犯罪グループで、約12%が国家の関与が疑われるとしている。）、残りは内部の攻撃者が関わっている。サイバー犯罪のほとんどが、金銭的な目的を動機とし具体的に76%が金銭を奪う目的、愉快犯が10%程度、スパイ活動20%程度としている。

[14]出典：サイバーセキュリティ意識・行動強化プログラム（2019年１月）参考16

の一体化の進展を踏まえ、連携・協働していくことが求められる。

こうした実態がある中、国際的なイベントの開催、サイバー空間利用の裾野拡大、先端技術・サービスの利用拡大の３点から、脅威が広がる可能性が高まっている。

（ア）国際的なイベントの開催に伴う脅威　～攻撃インセンティブの高まり～

G20やオリンピック・パラリンピック等の国際的なイベントは、非日常のイベントであり、最高度の注目を集めるため、攻撃のターゲットとなるおそれがあると考えられる。具体的に、政治的及び精神的目的の攻撃者にとって、攻撃のインセンティブを高めてしまうと考えられる。経済的利益目的の攻撃者の観点からも、観戦チケットの販売を含む様々なサービスや、国籍を超えた多数の利用者が関わることになり、非日常のイベントであるがゆえに人間の脆弱性が高まる可能性があるため、攻撃のインセンティブが高まると考えられる。実際に、2012年ロンドン大会、2016年リオデジャネイロ大会、2018年平昌五輪大会で、各々、様々なサイバー攻撃が確認されている。

非日常という視点では、自然災害が発生すれば、そのような状況となり、人間の脆弱性も高まると考えられ、これまでの自然災害発生時にもサイバー攻撃が増加したとの指摘もあり、こうした視点にも留意することが重要である。

今後、我が国において、2019年には、G20、ラグビーワールドカップ、2020年東京オリンピック・パラリンピック競技大会（以下「2020年東京大会」という。）など我が国で開催される国際的なイベントが予定されており、過去の事例や教訓を踏まえた対策強化が引き続き求められる。

（イ）利用の裾野拡大に伴う脅威　～脆弱性がある人間とIoTの増加～

IoT機器の普及、SNS・ネットショッピングの利用拡大等が人々の生活に様々な恩恵をもたらす一方で、IoT機器を狙った攻撃が増加し、ランサムウェア（身代金攻撃）の被害が発生している。今後も意識が高くない個人や企業が狙われるおそれがあるとの指摘がある。

スマートフォンの普及が爆発的に進んでおり、今後も、脆弱性を内在しつつ、サイバー空間に参加する人間が増大すると見込まれる。人間の脆弱性は前述のとおりであるため、これに関連する脅威は高まると予想される。

また、サイバー空間を構成するIoT機器について、2017年時点で275億個あり、2020年には約400億個になると予想されており、普及が進むと予想される。そもそもIoT機器は、「IoTセキュリティガイドライン ver1.0」（2016年７月IoT推進コンソーシアム）で整理されたように、ライフサイクルが長い、監視が行き届きにくい、機能・性能が限られた機器が存在するといった特徴があり、サイバーセキュリティ上の問題や攻撃の検知がしづらく、対策が難しいという問題がある。

以上のように、サイバー空間の生活への普及・浸透に伴い、サプライチェーンなどの脆弱な部分を狙う動きが高まり、人間の脆弱性とIoT機器の問題に起因する脅威が広がるおそれがあるため、必要な対策を重点的に進めることが重要である。

（ウ）先端技術の利活用に伴う脅威　～AIとサイバーセキュリティ～

今後、AI、 Fintech、自動運転車、ドローン等の先端技術・サービスの利用拡大が予想され、脅威が生じるおそれがある。既存かつ普及した情報システム等でも新たな脆弱性が発見されることは少なくないが、こうした先端技術の場合は、特に、

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高まる。

暗号資産（仮想通貨）やインターネットバンキングなどFintechはもちろん、特に、自動運転車などについては様々な制度整備など普及に向けた取組が行われており、将来の普及を見込み、様々な可能性を考慮して、先手を打って対策を進める必要がある。

サイバーセキュリティの観点で共通した課題として、前述したIoTの問題に加え、AIがあると考えられ、これについて整理する必要がある。

AIについては、「人間中心のAI社会原則（2019年３月統合イノベーション戦略推進会議決定）」では、「人間がAIに過度に依存したり、人間の行動をコントロールすることにAIが利用される社会を構築するのではなく」とし、あらゆる人間の活動がAIに置き換えられる世界を目指さないことを明確にしている。新戦略では、「昨今の計算機科学の知見が進展し、（中略）深層学習は、その登場により、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。」等とされており、サイバーセキュリティも含む様々な分野でAIを活用していく傾向がある。

今後、AIが人間に代わって重要な決定を行うような状況になれば、AIが攻撃の対象になる可能性がある。AIとサイバーセキュリティの関係については様々な議論があるが、集約すると、「AIを利用した攻撃」、「AI自身による自律的な攻撃」、「AIへの攻撃」、「AIを利用したセキュリティ対策」の４つの類型に整理できる。

ⅰ）AIを利用した攻撃

様々なサイバー攻撃にAIを活用する類型であるが、例えば、ボットを利用してコンサートチケットを買い占める試みがあったとの指摘があり、また、SNSのデータの自動収集と採取したデータからのフィッシング攻撃も試みられたとの報告[15]もあり、AIを利用した攻撃は、現実的になりつつある。また、パスワードの推測、個人認証のなりすましなどにAIが活用される懸念の指摘もあった。さらに、新戦略では、脅威の深刻化の類型として「民主主義の根幹を揺るがす事態も生ずるおそれがある」としているが、2018年において、自然言語処理において画期的な発展があった[16]との指摘も踏まえ、こうした事態が生ずる可能性も考慮し、引き続き注視することが求められる。

ⅱ）AI自身による自律的な攻撃

AIを人間が制御できなくなり、自律的にサイバー攻撃を行う可能性の指摘もある。一方で、小説等の創作においても、AIは創作本能を持たず、人間からの「○○を作って」という働きかけは必要[17]とされており、現時点では、AI自身で課題を作って攻撃するような世界は現実的ではない。一方で、音楽や小説等の創作物について、（創作的寄与が認められないような）簡単な指示でAIが自律的に生成する世界は現実的なものとなっており、新戦略でも、自律的なAIについて、「権利侵害や事故を起こした場合の責任を誰が負うのかといった問

[15]出典：情報セキュリティ10大脅威2019（IPA）
[16] Elmo、BERT等
[17]出典：次世代知財システム検討委員会報告書（平成28年４月）

題が生ずる可能性がある」とされ、人間の関与がない中で、AI兵器などAIがサイバー攻撃を行い、権利侵害を起こした場合の責任は誰が負うのかという問題は、サイバーセキュリティの世界でも生じ得るため、状況を注視していくことが求められる。

iii）AIへの攻撃

深層学習するAIを前提としておいた場合、AIにフェイクデータを学習させること、いわゆる「敵対的学習」が考えられる。この点、実証段階ではあるが、民間企業のAIチャットロボットにおける事例がある。ただし、程よく誤動作するノイズを組み込むことは技術的に難しく、不正侵入する方が簡単との指摘もあり、技術的には可能なものの、費用対効果の観点で合理的な状況ではなく、現時点では顕在化していない。今後、AIへの人間の関与が減り、重要な決定（投資判断、診断など）についてAIが自律的かつ最終的に行うことが定着すれば、こうした攻撃が現実的なものとなる可能性があり、状況を注視していくことが求められる。

iv）AIを利用したセキュリティ対策

サイバーセキュリティ対策にAIを活用する試みは、新戦略で「サイバーセキュリティにおいても、こうした可能性を持つAIは、例えば、マルウェアの自動検知などの対策の自動化に活用されつつある。」とあるように、すでに、様々な試みがある。

検知の精度は上がる一方で、検知の精度が上がる理由を説明できないとの課題もある。新しい攻撃、個別具体的な対策は難しく、マルウェアを次から次に大量に自動生成するAIがでてくると対応が難しいとの指摘もあった。また、AIを利用した対策を逆用し、攻撃に用いることも考えられる。実際に、AIによる対策を解析し、それを回避する方法として、一般的でない拡張子を持つファイルの利用など、防御側の検知を回避する攻撃方法が編み出されているとの報告[18]もある。

今後、AIを利用した攻撃、こうしたAIを利用した対策を逆用した攻撃も念頭におき、サイバーセキュリティ対策におけるAIの活用について、先手を打って、研究開発を進めることが重要である。現時点では、AIに何を解決させたいのかという課題設定や、AIの判断をどう解釈するのかという問題は引き続き人間が担うことになるため、サイバーセキュリティの観点でも、AIを使いこなす人材育成も求められる。

2.3　主なトピック

(1)　業務・機能・サービス障害

インフラメンテナンスの効率化や新たなビジネスの創出等を目的に、IoTの導入などの現場のデジタル化が進展している。今後、IoT機器から得られるデータの利用が事業の前提となることや制御系システムが外部のネットワークと繋がる状況となれば、万が一、攻撃

[18]情報セキュリティ10大脅威2019（IPA）

を受けた場合や自損事故及び自然災害に起因して、重要インフラサービスの障害やIoT機器の意図しない動作により、通信障害、交通混乱や停電といった事態が発生することも可能性として想定される。その可能性が現実的なものとなれば、国家や悪意を持つ団体のターゲットとなるおそれに加え、社会的な注目を求める愉快犯による犯行などの脅威の高まりが懸念される。また、最近ではサイバー攻撃に因らない重要インフラサービス障害が発生しており、社会に多大な影響を与えた事例[19]が多く確認されている。

国外においては、ウクライナの国営電力会社の変電所がサイバー攻撃を受けて停電する事例が生じている。国内においては未だサイバー攻撃を起因とする大規模な事案は確認されていないが、2020年に開催を控える「東京オリンピック・パラリンピック競技大会」において、会場のシステム異常、HPの閲覧障害などが発生した場合、大会の運営に影響を及ぼすことが想定されるため、その対策には万全を期す必要がある。

最近の傾向として、国外からのスキャン活動が増えているというデータが観測されており、これに対してサイバー関連事業者からは、何らかの準備のために調査をしている可能性があるという指摘もあり、一層、警戒を強める必要がある。

①　国際的なイベントに伴うサイバー攻撃事例

オリンピック・パラリンピック等の国際的なイベントでは、攻撃のインセンティブが高まることを背景に、過去の大会では図表１－２－１のような状況が確認されている。いずれも大会の運営に支障を来すような事案は発生していないものの、注目を集めるイベントが攻撃のターゲットとなることがこれらの状況からも推定される。

図表１－２－１

大会	確認された状況
2012年ロンドン大会	・大会公式サイトに対して約２億件の悪意ある接続要求 ・開会式直前にオリンピックスタジアムへの電源系への攻撃情報を入手し、必要な対処を実施　等
2016年リオ大会	・大会公式サイトに対する執ようなサイバー攻撃 ・大会関係組織の一部のWebの改ざん　等
2018年平昌大会	・大会準備期間に約６億件、大会期間中に約550万件のサイバー攻撃 ・開会式においてサイバー攻撃に起因して一部のサービスが利用不可 等の報道あり

我が国においては、2019年６月のG20、９月のラグビーワールドカップ、2020年東京大会と複数の国際的に注目を集めるイベントが控えている。これらのイベントの成功は重要であり、イベントの円滑な遂行を目指すためにも、運営に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求められる。

②　重要インフラ等のサービス障害

サイバー攻撃によって、重要インフラ等が被害に遭い、大規模な社会的混乱等が引き起こされる状況が現実のものとなりつつある。国外では、2015年12月と2016年12月にサイバー攻撃によりウクライナにおいて停電が発生した事例や、2017年５月にランサムウェア「WannaCry」により英国の国民保険サービス関連システムが停止し、多数の病院で医療サービスが中断するなどの事例が確認されている。

[19] 平成30年台風21号、平成30年北海道胆振東部地震によるもの等

2018年度には、我が国でも、ランサムウェアの感染により、７月に交通機関における一般業務系での障害、10月に医療機関での障害が発生した事例[20]などが確認されている。医療機関の事例では、奈良県の病院において電子カルテシステムが被害に遭い、約２日間にわたって使用できない状態に陥った。結果として、システムが復旧するまでの間、紙カルテ及び伝票運用による診療を行うなどの業務支障が発生している。ランサムウェアは金銭獲得を目的として、感染した対象に保存されているファイルを暗号化するなどして不当に金銭を要求するものであるが、暗号化されたファイルが重要情報や基幹システムのシステムファイル等であった場合は、事業継続にも影響をおよぼす可能性がある。

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、過去には、2016年10月に、IoTの爆発的な普及を背景として、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がある。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、その結果、数多くの大手インターネットサービスやニュースサイトにアクセスしにくくなる等の影響を与えた。

近年において、IoT機器がますます社会へ普及し、人々の生活に様々な恩恵をもたらす一方で、IoT機器を狙ったサイバー攻撃はさらに高度化しており、2018年に観測されたデータ[21]では、IoT機器固有の脆弱性を狙う攻撃活動が増加している。また、スマートフォンの代表的OSであるAndroidOSを感染対象とするマルウェアも確認されており、AndroidOSを搭載したテレビやカーナビシステム等の多様なIoT機器を狙った攻撃も登場[22]してきている。

(2)　情報の毀損及び漏えい

情報漏えいについては、過去には、2015年の日本年金機構における個人情報の流出事案や、2016年の大学における研究成果の流出事案などが発生しており、その他にも多くの事案が発生している。昨今は、それらに加えて、ものづくりや医療等の「現場」から得られる豊富な「リアルデータ」[23]についても活用が進んでおり、今後、その価値は高まっていくと考えられる。価値の高い情報は、売買による金銭獲得や別のサイバー攻撃への悪用などの目的で窃取されるおそれがあり、情報を毀損した際にはサービス障害が発生することも想定される。

2018年度においても、国内の事業者が提供するファイル共有サービスに不正アクセスを受けて顧客情報が漏えいした事例や大学等に対するフィッシングメールにより個人情報が漏えいした事例など、引き続き、多くの事案が発生しており、国外でも、大手SNSサービスにおける大規模な個人情報漏えい事案などが確認されている。

最近は、情報を窃取するための手口が更に高度なものになってきており、既存の有名サイトやクラウドサービスを模倣した画面で利用者の目を欺き、個人情報を窃取する事例なども登場してきている。また、個々の事案との直接的な関連は不明であるが、漏えいした

[20] https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/press-release.pdf
[21] https://www.nict.go.jp/press/2019/02/06-1.html
[22] https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf
[23] 未来投資戦略2018

情報を悪用して巧妙なフィッシングメールを仕掛ける事例も確認されており、情報漏えいに端を発する被害が表面化している。

①　個人及び企業における情報漏えい

個人を対象とした情報窃取を狙う攻撃については、多種多様な手口を用いて、人間の脆弱性を突いた攻撃が登場している。2018年度においては、大手インターネットサービスや宅配業者を装い、アカウントの期限切れや不在通知などを訴えかけて正規なサイトに巧妙に似せて作ったサイトへ誘導して、スマートフォンへの不正アプリのインストールやクラウドの認証情報を窃取した上で個人情報などを窃取するような攻撃が確認されている。

また、引き続き、企業も攻撃のターゲットとなっており、2019年1月には、国内の事業者が提供するファイル共有サービスが不正アクセスを受けて、利用者のログイン用メールアドレスやパスワード等を含む約480万件の顧客情報が漏えいしたことが明らかになった。その他、国外では、2018年9月に、米国大手SNSサービスにおいて、サービスの脆弱性に起因して、数千万件の利用者情報が流出したおそれがあることが公表されている。

②　自治体・大学等における情報漏えい

2018年度には、自治体や大学等における情報漏えい事例も多く確認されている。自治体においては、情報管理に対する意識の低さに起因する情報漏えいが確認されている他、大学においては、管理者を装ったフィッシングメールで有名クラウドサービスの認証画面に似せたサイトへ誘導され、有名クラウドサービスの認証情報が窃取されることにより、個人情報が漏えいした事例などが複数の大学で発生している。

また、2018年7月、国立研究開発法人産業技術総合研究所は同年2月に明らかになった外部からの不正アクセスによる被害の報告書を発出[24]し、未公表の研究情報や個人情報が外部に漏えいしたおそれがあることが明らかになった。

③　国家の関与が疑われる事例

研究情報や産業技術などの機密情報を狙った国家の関与が疑われる攻撃などの存在も指摘されている。近年、国外に拠点を置くAPT10といわれるグループからの日本の民間企業、学術機関等を対象とした長期にわたる広範な攻撃が確認されており、これに対し、2018年12月20日から21日にかけて、英国・米国等がAPT10に関する声明文を発表し12月21日、我が国もこれらの国を支持し、外務報道官談話を発出[25]している。また、2018年11月には米国大手ホテル事業者における最大約3.8億人分の顧客情報の流出が報道されており、これに対して、ポンペオ米国務長官はインタビューで国家の関与があったという見方を示している。

(3)　金銭の窃取・詐取等

今や様々な経済活動に伴う送金や支払において、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。金銭が電子情報となってサイバー空間上で扱われるようになるとともに、サイバー攻撃の脅威にさらされることとなってきており、過去にもインターネットバンキングの不正送金や暗号資産（仮想通貨）の流出被害などが発生している。

[24] https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf
[25] https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

近年、政府はキャッシュレス社会の実現[26]をめざし、キャッシュレス決済の普及等を進めており、これらの推進を図るとともに、これにより高まる脅威への対応も必要である。攻撃者はより低い労力で多くの利益を得られる分野を狙う傾向にあると考えられ、過去に攻撃を受けるなどした分野においては一定程度対策が進む中、対策が十分でない分野や攻撃が成功した場合に多額の損失が想定される対象については、基本的な対策の徹底等が重要である。

実際の攻撃として、2017年度に猛威を振るったランサムウェアに関しては、感染の原因となる脆弱性への対応が進む中、検出台数の伸びが鈍化しているものの、特にフィッシングをはじめとする人間の心理を突いた攻撃は対策が難しく、引き続き多くの攻撃が確認されている。

攻撃者は、より多額の金銭を得るためにより巧妙な手口を使ってきており、2018年度には国内において、不正に窃取したアカウントやパスワードを悪用して、メール本文に実際に使用されたパスワードを記載した脅迫メール[27]なども登場している。また、その他の傾向としては、従来型のインターネットバンキングにおける不正送金事案は事業者側の対策が一定程度進んだことで被害が減少傾向[28]にある一方で、暗号資産（仮想通貨）をマイニングするマルウェア（以下「マイニングマルウェア」という。）については、2018年度第1四半期において2017年度に比べて増加し、暗号資産（仮想通貨）の価値の下落に伴い、その後、減少するなどの動きがあった。このように、暗号資産（仮想通貨）の価値の変動に合わせ、今後ターゲットが別の対象に移っていく可能性もある。

①　人間の脆弱性を狙って金銭を詐取する事例

2018年度は、過去最大規模のフィッシング詐欺が発生[29]している。攻撃者は金融機関や大手IT企業を装ったメール等により、クレジットカード情報等の個人情報を窃取し、悪用することにより金銭を獲得する。その他にも、性的な映像をばらまくと脅迫し人の羞恥心につけこんで金銭を要求するような新たな手口も確認[30]されている。

また、企業を狙った手口として、国内において日本語が使用されたビジネスメール詐欺が確認[31]されている。従来から英語のメールによるものは確認されていたが、海外との取引等がない国内の企業においてもビジネスメール詐欺の脅威が高まっている。中には、実際のCEOを騙って企業の財務担当者を騙そうとするもの[32]も出てきており、手口が巧妙化している。

②　ランサムウェアの事例

ランサムウェアは2017年の「WannaCry」をはじめ、様々な種類のものが登場しており、一時期の盛り上がりに比べると少し落ち着いてきているものの、継続して攻撃が確認されている。2018年においても、国内で引き続き被害は発生しており、鉄道、病院、大学、サービス業などでランサムウェアに感染する事例が起こっている。また、海外においては、ランサムウェア「SamSam」に関して主に米国の企業の間で被害が発生しており、2018

[26] 日本経済再生本部 経済政策の方向性に関する中間整理（平成30年11月）
[27] https://www.jpcert.or.jp/newsflash/2018080201.html
[28] https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf
[29] https://is702.jp/news/3456/
[30] https://www.ipa.go.jp/security/anshin/mgdayori20181010.html
[31] https://www.ipa.go.jp/security/announce/201808-bec.html
[32] https://blog.trendmicro.co.jp/archives/19654

年７月時点で約 6 億 7 千万円の被害があったことが報告[33]されている。ランサムウェアは依然として攻撃者が効率よく利益を得られる攻撃であり、今後も、引き続き警戒が求められる。

③　暗号資産（仮想通貨）の事例

暗号資産（仮想通貨）の窃取を目的としたサイバー攻撃は国内外で発生しており、国内でも、2018 年１月に約 580 億円相当の被害が発生した事例や、2018 年８月に約 1500 万円相当の被害が発生した事例、2018 年９月に約 70 億円相当の被害が発生した事例などが発生している。

また、感染した PC の CPU 等の計算処理能力を利用したマイニングマルウェアも継続して確認されている。2018 年度は、2017 年度に比べてその数が増加しており、世界全体では 2018 年にマイニングマルウェアの検出台数が 100 万件を超え、前年比約 237%の急増を示しているとの報告[34]もある。

[33] https://www.sophos.com/ja-jp/press-office/press-releases/2018/08/samsam-the-almost-6-million-ransomware.aspx
[34] トレンドマイクロ 2018 年 年間セキュリティラウンドアップ（平成 31 年２月）

3　新戦略に基づく対処方針

3.1　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～

今後、高まると想定される脅威に対し、サイバーセキュリティの確保を通じて、サイバー空間の持続的な発展(Society 5.0)を支えていく必要がある。新戦略では、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。

そのイメージとしては、実空間との一体化が進んだサイバー空間で、サイバーセキュリティの確保とともに新たな価値が創造（イノベーション創出）され、それにより生じる富を原資に、投資・研究開発・人材育成が行われ、更なるイノベーションが生み出されていくとの循環が自然に行われる生態系である。また、国民一人一人が、手洗い・うがいといった公衆衛生活動や、信号を遵守するといった交通安全活動と同様に、サイバーセキュリティに関する基本的な意識・理解を醸成し、様々なリスクに自律的に対処していく姿が考えられる。さらに、容易に国境を越えるサイバー空間における法の支配の確立のため、国際連携・協力が自律的に行われることも含まれると考えられる。その他、研究開発・人材育成などの横断的な取組も含め、サイバーセキュリティに関する様々な取組が自律的に行われ、その実施状況を検証して次の取組に反映していくといった循環も想定される。

こうした状態を作り出していくために、新戦略では、「３つの観点（①「サービス提供者の任務保証」(以下「任務保証」という。)、②「リスクマネジメント」、③「参加・連携・協働」）からサイバーセキュリティに関する官民の取組を推進する」と明記された。

(1)　全ての主体にとって必要な観点　～「参加・連携・協働」～

このうち、参加・連携・協働は、サイバー空間上のサービスを享受する利用者を含む、全ての主体にとって必要な観点である。新戦略では、「サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が、平時から講じる基本的な取組」とされており、その基本的な取組には、各個人のパスワードの適切な管理・パッチ適用による脆弱性の解消・ウイルス対策ソフトのインストールなどの対策に加えて、ベストプラクティスやインシデント情報の共有を行い、個人と組織間で相互に連携・協働するなどが含まれる。

(2)　サービス提供者を主に想定した観点　～「任務保証」、「リスクマネジメント」～

任務保証とリスクマネジメントは、様々な製品やサービスを提供する政府機関等や重要インフラ事業者等、企業などの「サービス提供者」を主に想定した観点である。任務保証は、新戦略で、「サイバーセキュリティ（中略）を目的化するのではなく、各々の組織の経営層・幹部が（中略）業務やサービス（中略）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」とされ、業務・サービスあってのサイバーセキュリティであるとの考え方を明確にしている。また、「一部の専門家に依存するのではなく」とも明記されており、経営層の自律的な取組が必要であるとされている。

リスクマネジメントは、新戦略で、「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」とされている。リスクとは、本来、不確実さを意味し、プラス面もマイナス面もある。そのため、本質的に、完全なリスクの除去が不可能なのは当然である。組織の任務の遂行のため、その有す

る有限の資源をどのように使い、リスクに対応していくのかという課題は、組織の任務を認識し、組織を指揮統制する経営層にしかできない。なお、新戦略では、サイバー空間の恩恵を享受する以上、個人にとっても、リスクマネジメントの考え方は求められるとしていることにも留意が必要である。

3.2　積極的サイバー防御　～事前の能動的な取組～

サイバー空間において、攻撃者優位の状況がある中、脅威に対して適切な対処を行うためには、攻撃者の実態を把握し、そのリスクを特定・評価し、それに応じた対処が求められる。「2.2(2)③サイバー空間における脅威の影響が広がる可能性」で整理したとおり、攻撃者の目的は、精神的目的（愉快犯等）、経済的利益目的（金銭入手等）、政治的目的（スパイ活動等）が考えられるが、このうち、経済的利益目的以外の、精神的目的及び政治的目的の攻撃については、政府機関や重要インフラ事業者等、経済社会に大きな影響力がある企業が標的にされ、たとえ、基本的な対策によって攻撃に係るコストをあげたとしても、攻撃を抑止できないおそれがある。新戦略でも「サイバー犯罪・サイバー攻撃は複雑化・巧妙化しており、攻撃の種類も多種多様となっていることから、従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行う必要がある」とされ、特に、政治的目的の攻撃では、国家の関与が疑われるものなどの組織的な支援の下の攻撃の可能性があり、こうしたことを念頭におき、事前の積極的な防御策の強化が求められる。

(1)　新戦略における「積極的サイバー防御」の概念と位置づけ

新戦略では、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、「積極的サイバー防御」の構築を掲げた。これは、「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」である。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取組を行うことであり、具体的には、「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」があげられている。なお、関連で、英国の戦略で掲げるActive Cyber Defence（ACD）（事業者と協力した、常時からの積極的防御策）[35]があるが、法制度上の違いからその範囲に相違点もある一方で、広い意味で類似点があると考えられる。ただし、英国でも、ACDは平素からのISPと協力したネットワーク防御を意味しており、Offensive Cyber（サイバー攻撃能力）やhack back（逆ハック、サイバー反撃）のような取組とは明確に区別されており、新戦略で掲げる積極的サイバー防御にもこれらが含まれないことに留意が必要である。

積極的サイバー防御の位置づけについては、これまでのサイバーセキュリティに関する基本計画の歴史を踏まえて整理することが重要である。政府として、初めて策定したサイバーセキュリティ政策に関する基本的な計画（第1次基本計画（平成18年（2006年）決定）で、情報の取り扱いや対策のルールを定めるといった事前対策に特に焦点を当てた取組が推進され、第２次基本計画（平成21年（2009年））では「事故前提社会」への対応力強化の実現を謳って事後対応に重点が置かれた。その後、2013年戦略では、これらの継続とともに次元を変えた取組が必要とされ、「サイバー空間の衛生」の概念が提示されて、予

[35] Annual Review2018では、「1年間で13万8,398のフィッシングサイトを除去し、英国へのフィッシング攻撃の割合を5.3%から2.4%に減少させることに成功し、毎月平均10,975件の悪意あるドメインがブロックされている」という報告がある。

防的な取組の必要性が指摘された。基本法に基づく初めての戦略であった 2015 年戦略では、「後手から先手へ」というアプローチが明記され、「社会変化や、今後発生し得るリスクを分析し（中略）先手を打って必要な政策を展開する」とされた。このような潮流を受けて、「積極的サイバー防御」に関連する取組については、模索が続けられてきた。

新戦略では、サイバーセキュリティエコシステムを推進するため、サービス提供者を主に想定した観点である「任務保証」及び「リスクマネジメント」に関し、これを具体化した取組の実施方針として、「積極的サイバー防御」が明記された。これは、完全な事前対策でも、事後対応であるわけではなく、その間にある、脅威に対して、予兆段階においても、リスクに応じて事前に積極的に取り得る防御策を講じることと位置づけられるものである。

(2) 「積極的サイバー防御」に関連する取組とその広がり

こうした考え方は、電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律（平成30年法律第24号。以下「NICT法改正」という。）に基づくIoT機器の調査等の取組や、政府機関等の情報セキュリティ対策のための統一基準群の改定（2018年７月）に基づく取組、同統一基準群に記載されたサプライチェーン・リスク対策に係る考え方に関する申合せ（2018年12月）、基本法の改正（2018年12月）によるサイバーセキュリティ協議会などに反映されており、深刻化する脅威に対し、政府機関等が積極的に取り組むことを示したものとなっている。

NICT法改正では、脆弱なIoT調査（NOTICE[36]）については、サイバー攻撃を受けてから対応するのではなく、サイバー攻撃に悪用されるおそれのあるIoT機器を調査して、注意喚起することができるような法整備を行うという先進的で、積極的な取組となっており、まさに、「積極的サイバー防御」を体現した取組であると言える。

また、改定された統一基準群でも、未知の不正プログラムに係る被害の未然防止のための端末等での挙動検知や、情報漏えいが起きた場合でもデータが保護される対策など、事案が生じることを予測した上での新しい技術による対策を積極的に行うことを促すものとなっている。

さらに、基本法の改正に基づき、2019年４月に組織されたサイバーセキュリティ協議会は、こうした取組を政府機関等や重要インフラ事業者等に限らず、それ以外の企業にも門戸を広げた取組となっている点や、予兆段階で情報共有に取り組む仕組みを整えている点が画期的である。今後、従来の枠を超えた新たな情報共有・連携体制の構築が謳われ、積極的サイバー防御の取組の広がりの可能性を示している。

こうした潮流の中、企業においても、ダークウェブから将来の攻撃を予測し、対策を行う取組が行われてそれが功を奏し被害を免れた事例の報道があった。また、このような対策の方が、攻撃を受ける前提の対策よりも、むしろ予算を取りやすく、実施したいとの要望が企業からサイバー関連事業者に寄せられたとの指摘もあった。また、先手を打った対策の促進として、バグバウンティ[37]の取組があり、一定の成果をあげているとの指摘もあった。

今後、ますます、生活の基盤となる様々なモノやサービスを提供する責任のある政府機関等や重要インフラ事業者等、企業にとっては、自動運転や暗号資産（仮想通貨）などの先端技術の普及も見込み、先手を打ってこれに関する研究開発や対策を行うことなどを含

[36] National Operation Towards IoT Clean Environment
[37]脆弱性などを見つけた人に報奨金を与える仕組み

め、積極的サイバー防御の取組を進めていくことの重要性が増すと考えられる。

3.3　2020年東京大会とその後を見据えた対処態勢の強化

2020年東京大会は、前述したとおり、攻撃者を刺激し、リスクが高まることが想定される。大会の円滑な開催と運営のために、大会に関係する重要なサービスを担う事業者のリスクマネジメントと対処態勢の構築と訓練・演習を通じた強化が重要であり、こうした考えの下で、政府・関係者一丸となって、取り組むことが重要である。

2020年東京大会が無事成功で終わったとしても、「任務」を担う政府機関等や重要インフラ事業者等、企業にとって、サイバー攻撃への対処態勢の強化は重要な課題である。リスクを完全に除去できない以上、不正侵入を防ぐといった安全性の確保に加え、攻撃を受けた時の復旧、すなわち、信頼性確保に向けた取組の重要性は増している。

事後対応能力については、2005年の第1次基本計画でも指摘され、2009年の第2次基本計画でその強化が謳われ、その後も継続が必要とされたように、永遠の課題である。攻撃を受けた際の対処に係る体制、計画を整備し、地道な訓練・演習といった取組を継続することが求められる。加えて、サイバー空間に係る動向を把握し、そのリスクに応じて訓練・演習内容の不断の見直しを図っていくことが重要であり、その積み重ねのみが、被害やその拡大を防止する強力な対処態勢を実現するのであり、不断の取組が求められる。

2章　2018年度のサイバーセキュリティに関する情勢

1　サイバーセキュリティの基本的な枠組みに関する情勢

基本法第12条に基づき策定された2015年戦略は、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戦略を決定した。

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、新戦略の策定に至る経緯や概要及び、同戦略の取組に関連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案に関する経緯や概要について概説する。

1.1　新たなサイバーセキュリティ戦略の策定について

2015年戦略の計画期間（2015年９月～2018年９月）が残すところ約１年となったサイバーセキュリティ戦略本部会合（以下「本部会合」という。）第14回会合において、加速・強化すべき施策を取りまとめ、新戦略の策定等につなげることが明記された「2020年及びその後を見据えたサイバーセキュリティの在り方について―サイバーセキュリティ戦略中間レビュー―」（2017年７月13日サイバーセキュリティ戦略本部決定。以下「2015年戦略中間レビュー」という。）が決定された。これを踏まえ、2018年１月の第16回本部会合では、「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」（2018年１月17日サイバーセキュリティ戦略本部決定。）が決定された。ここでは、検討すべき事項として「サイバー空間の将来像と新たな脅威の予測」等の３点を掲げ、「あらゆる主体が参加し、実空間（フィジカル空間）との一体化が加速的に進展するグローバルなサイバー空間の将来像を視野に入れつつ、それを支えるサイバーセキュリティの基本的な在り方を明確にし、次期戦略の策定に係る検討を開始する。」された。

その後、有識者本部委員等の関係者から意見聴取等を随時実施し、検討が進められ、同年４月の第17回本部会合では、新戦略の骨子案が示された。この中で、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、2015年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あ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。

この後、第18回本部会合において、新戦略のパブリックコメント案（2018年６月７日サイバーセキュリティ戦略本部決定）が示され、同年６月７日から６月21日まで一般からの意見募集を行ったところ、16の企業・団体及び11の個人等から97件の意見が寄せられた。こうした意見も踏まえ、更に検討を進め、第19回本部会合において、新戦略の案（2018年７月25日サイバーセキュリティ戦略本部決定）が決定された。同案は、新戦略として、2018年７月27

日に閣議決定され、同日、基本法第12条第５項において準用する同条第４項の規定に基づき、国会報告された。

1.2　サイバーセキュリティ基本法の一部を改正する法律の経緯について

サイバーセキュリティの確保は、本来、個々の組織が自主的に取り組むべきものであるが、サイバー攻撃が複雑化し、脅威の変化が早い現状においては、個々の組織が単独で有効な分析を行い、確証をもって効果的な対策を迅速に講じることに限界が生じており、また、サイバー攻撃は、同時並行的に多くの組織を対象とするケースも多いため、迅速な情報共有が行われなければ、攻撃手法や対策の方法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。

そこで、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、既に複数の情報共有体制が設立され、着実に活動を行っている。しかし、他組織に対して情報提供を行うことについてはさまざまな課題も残されており、必ずしも常に迅速な情報共有が実施できているわけではない。

例えば、2017年に、日本を含む世界約150カ国以上で感染が確認され、英国の病院では診療・手術の中止等、業務に支障を及ぼす被害が発生したランサムウェア「Wannacry」等に関しても、攻撃手法や対策方法に関する情報を迅速に広く共有することができていたならば、他組織への被害の拡大を防ぐことができた可能性がある。

上記事案等を受けて、2017年７月にサイバーセキュリティ戦略本部が決定した「2015年戦略中間レビュー」においては、「情報共有・連携ネットワーク（仮称）の構築・運用」として、「迅速な集約・分析、効果的な対策の共有を行う情報連携体制を構築する」こととされた。

以上の状況を踏まえ、内閣官房は、官民を含めた多様な主体がサイバーセキュリティに関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予防し、また、被害の拡大を防ぐことを目的としたサイバーセキュリティ協議会を創設すること等を内容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案を2018年３月に第196回通常国会に提出した。

同法案は、同国会では成立せず継続審査となったが、第197回臨時国会において、2018年11月27日に衆議院で原案のとおり附帯決議なく可決され、また、同年12月５日に参議院で原案のとおり附帯決議なく可決・成立し、同月12日に、平成30年法律第91号として公布された。

同法の施行にあたって、2019年３月８日に、サイバーセキュリティ基本法の一部を改正する法律の施行期日を定める政令（平成31年政令第36号）及びサイバーセキュリティ戦略本部令の一部を改正する政令（平成31年政令第37号）が閣議決定された。

これらの政令により、サイバーセキュリティ基本法の一部を改正する法律の施行期日が2019年４月１日とされ、また、同法は、サイバーセキュリティ戦略本部の事務の一部（関係機関との連絡調整事務）を政令で定める法人に委託することができる旨を定めていたところ、当該法人として、一般社団法人ＪＰＣＥＲＴコーディネーションセンターが指定された。

図表２－１－１　新戦略の概要

図表２－１－２　サイバーセキュリティ基本法の概要（平成30年改正後）

サイバーセキュリティ基本法※の概要（平成30年改正後）

※平成26年11月12日公布。平成27年１月９日全面施行

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について規定

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針
② 国の行政機関等におけるサイバーセキュリティの確保
③ 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促進
④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■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促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■サイバーセキュリティ協議会（第17条）

⇒本部長及びその委嘱を受けた国務大臣が組織
⇒国の関係行政機関の長、地方公共団体、重要インフラ事業者、サイバー関連事業者等、官民の様々な主体を構成員として加えることが可能
⇒構成員に対する遵守事項（情報提供の協力、守秘義務）を規定

■犯罪の取締り及び被害の拡大の防止（第18条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第19条）

■産業の振興及び国際競争力の強化（第20条）

■研究開発の推進等（第21条）

■人材の確保等（第22条）

■教育及び学習の振興、普及啓発等（第23条）

■国際協力の推進等（第24条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置（第25条）

■所掌事務等（第26条）

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査、事象発生時の国内外の関係者との連絡調整その他総合調整等の実施

■組織等（第27条～第30条）

⇒内閣官房長官を本部長として、副本部長（サイバーセキュリティ戦略本部の事務を担当する国務大臣）、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣、総理が指定する国務大臣、有識者本部員で構成

■事務の委託（第31条）

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（守秘義務を規定）

⇒事象発生時の国内外の関係者との連絡調整の事務の一部を政令で定める法人に委託（守秘義務を規定）※JPCERT/CCを指定

■資料提供等（第32条～第37条）

第Ⅴ章．罰則

■罰則（第38条）

⇒協議会の事務に従事する者若しくは従事していた者又は戦略本部から事務の委託を受けた者が守秘義務に反した場合。1年以下の懲役又は50万円以下の罰金

2　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

2018年度、国内外において重要インフラサービスに関するインシデントが発生した。海外では、金融機関を狙ったサイバー攻撃事例やランサムウェアの報告が目立った。また、国内では、グローバルと同様に日本でも金融周りの事例やランサムウェア等によるサイバー攻撃、自損事故や自然災害に起因する重要インフラサービス障害が報告されている。

国外における主な事例としては、金融機関を狙ったサイバー攻撃事例やランサムウェアによるDoS攻撃等が挙げられる。2018年４月には、メキシコの中央銀行であるメキシコ銀行が提供する銀行間電子決裁システム(SPEI)を利用していた同国の複数の銀行がサイバー攻撃を受け、少なくとも４億ペソ(約2,000万米ドル)が不正送金により窃取された[38]。また、2018年８月には、インド最古の銀行「Cosmos Bank」が、同行のATMやSWIFT環境に対するサイバー攻撃により1,350万米ドルの被害にあった。このサイバー攻撃では世界28か国のATMで不正引き出しが行われた[39]。さらに2018年11月、パキスタンでは、ダークウェブフォーラム上で、同国のクレジットカードやデビットカード情報が公開されているということが、セキュリティ企業により発見された。同国の連邦捜査局(FIA)は、パキスタンのほぼ全ての銀行の顧客データが流出していることを明らかにした[40]。

2017年度は「WannaCry」や「NotPetya」等に代表されるランサムウェアが世界的に大流行したが、2018年度は、ランサムウェアによる攻撃総数自体は減少した。ランサムウェア感染により重要インフラサービスの提供に支障を来した事例が報告されていることから、その脅威は継続していると言える。例えば、2018年３月には、米国ジョージア州アトランタ市が被害を受けたランサムウェアは、同市の基幹システムを支える424のソフトウェアプログラムのうちの約３分の１を攻撃し、多くのオンラインサービスを停止させた。攻撃者は、身代金として51,000米ドル相当のビットコインを要求したが、同市は拒否し、結果としてシステムの復旧に要求額以上の費用を要することとなった[41]。この事例では、2015年に初めて確認されたランサムウェア「SamSam」が利用されていた。

国内においても、医療機関、交通機関等でランサムウェアによる感染事例が確認され、医療機関の事例では、電子カルテシステムがランサムウェアに感染し、約２日間にわたって使用できない状態に陥った。また、自治体に対するサイバー攻撃による情報窃取、ホームページ改ざん等の被害が多数見受けられた。特に、自治体に寄付すると税が控除される「ふるさと納税」を巡り、寄付金の詐取を目的とする偽サイトが多数存在することが明らかになった。実際に寄付金をだましとられる被害が確認されたことから、捜査機関が捜査を開始するとともに、総務省は寄付者に対して注意を促す通知を全国の自治体に発出するなどして対応した。また、フィッシング詐欺は、昨年に引き続き増加しており[42]、金融機関等を装ったメールを送り、フィッシングサイトに誘導させて、銀行口座番号、クレジットカード情報等を窃取するサイバー攻撃や、宅配業者の不在通知を装って、携帯電話番号と認証コードの窃取

[38] http://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf
[39] https://www.cosmosbank.com/press-release/
[40] https://bankislami.com.pk/wp-content/uploads/2018/10/Material-Information-Cyber-Attack-on-Debit-Cards.pdf
[41] https://www.atlantaga.gov/Home/Components/News/News/11520/672
[42] https://is702.jp/news/3456/

を目的としたサイトへ誘導するショートメッセージ(SMS)を送付する等のサイバー攻撃が確認されている。

業務委託に関するサプライチェーン・リスクも顕在化した。ある政府機関は2018年12月14日、マイナンバー等個人情報の記載のある書類のデータ入力を委託されていた業者が契約に反して別の業者に再委託していたことを発表した（書類にして約69万件）。当該委託されていた業者は、このほかにも当該業者によるマイナンバー等個人情報の記載のある書類のデータ入力の再委託に関する契約違反ないし法令違反が判明（書類にして約171万件）したことを発表した。また、このほか、一部自治体においても再委託に関する同様の問題が明らかになった。

自損事故や自然障害等、サイバー攻撃に因らない重要インフラサービス障害も目立った。自損事故の例としては、2018年６月、インターネット経由で株式を取引するシステムにおいて、２日半の間システムの利用に不具合が発生し、株式予約注文約１万件が影響を受けた。原因は、システム更新作業時の設定誤りによるものであった。

また、2018年９月、成田国際空港第２ターミナルの国際線搭乗手続き関連システムで発生した障害では、航空各社のネットワーク上でエアラインが旅客の搭乗手続き作業を行った際に通信が不安定になったことにより搭乗手続きに必要な手荷物情報が受信できなくなったため、出発階は一時、搭乗手続きを待つ旅客で混雑した。

さらに、2018年12月、国内の通信事業者が提供する通信サービスにおいて、４時間25分にわたり、約3,060万回線に影響を及ぼす通信障害が発生した。通信障害は、同者が提供する４G(LTE)携帯電話サービス、固定電話サービス、ブロードバンドサービスのほか、同者の回線を利用した他社の仮想移動体通信事業者(MVNO)サービスでも発生した。さらには、通信障害による二次的影響として、携帯端末向けの電子決済サービス、宅配ドライバーの集荷依頼/再配達の受付、携帯端末を使用した搭乗券確認業務等多岐にわたり、通信サービスと経済のつながりの深さを改めて浮き彫りにした。通信障害の原因は同者の通信インフラの中核を構成する他社製の通信機器(Mobility Management Entity：MME)のソフトウェアで使用していたデジタル証明書の有効期限切れであった。このデジタル証明書は、当該MMEの開発ベンダーによって、オペレータからは確認できない形で組み込まれており、同者が有効期限切れを事前に把握することが困難だったとされる。

自然災害では様々な脆弱性が浮かび上がった。2018年９月、関西地方を中心に猛威を振るった台風21号の影響により、交通や電力などのインフラに大きな被害を与えた。関西国際空港では、台風21号による高波の影響で、滑走路や旅客ターミナルが冠水し、また、関西国際空港連絡橋の橋桁にタンカーが衝突し、連絡橋が使用不能となり、空港の利用客と職員が同空港内に一時取り残された。さらに、2018年９月、北海道では、胆振地方中東部を震源として発生した「平成30年北海道胆振東部地震」により、国内初のエリア全域停電（ブラックアウト）が発生した。地震発生に伴い、北海道電力管内の約半分の電力を担う苫東厚真発電所（北海道厚真町）が停止したことに加え、電源系統周波数を調整する水力発電所と電源系統を繋ぐ多重化された送電線が地震によって使用できず、その結果ブラックアウトとなった。ブラックアウトから概ね全域に供給が回復するまで45時間程度要した。

自然災害等に関連した問題として、誤情報や偽情報の拡散があり、これらが重要インフラサービスに影響を及ぼすことがあった。北海道地震では、根拠のない誤情報や偽情報が交流サイト(SNS)や無料対話アプリを中心に拡散した。札幌市等北海道内の複数の自治体が、予

定がないのに「断水が始まる」といった誤った情報がインターネット上で拡散しているとして、ホームページ(HP)で注意喚起を行った。会員制交流サイト(SNS)への投稿のほか、通信アプリ「LINE」を介して、チェーンメールのように拡散したケースもあった。

SNSが問題を引き起こした反面、同社は、SNSを活用し、停電復旧情報等を効果的に発信することができた。北海道地震によって、同社の停電情報システムがダウンしたことから、2017年３月31日で閉鎖していた公式Twitterを復活させ、道内の停電復旧情報の逐次発信を行った。インターネットやSNSが普及した今日、公共サービスを担う重要インフラの非常時の情報発信の観点から参考となる事例である。

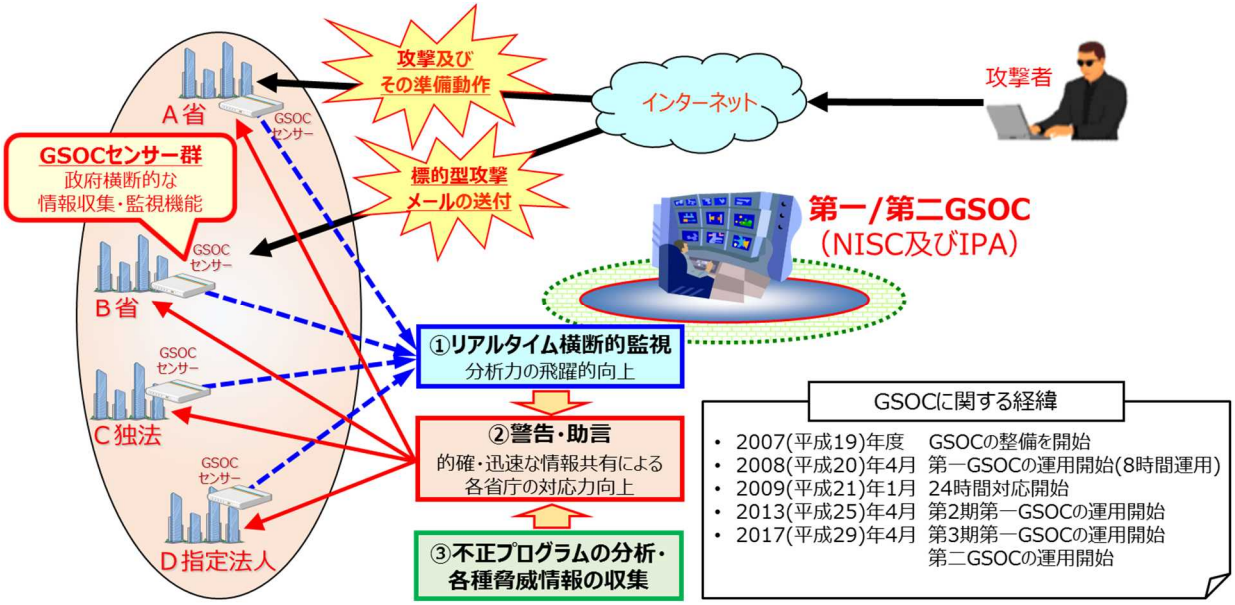
3　政府機関等におけるサイバーセキュリティに関する情勢

3.1　政府機関等[43]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[44]）を、また、2017年４月からNISCの監督の下、独立行政法人情報処理推進機構（IPA）（以下「IPA」という。）において独立行政法人及び基本法に基づく指定法人（以下「独立行政法人等」という。）に対する情報セキュリティ横断監視・即応調整チーム（第二GSOC）を設けている（以下、第一GSOCと第二GSOCを併せて「GSOC」という。）。

GSOCでは、24時間365日体制でサイバー攻撃等の不審な通信の横断的な監視、不正プログラムの分析や脅威情報の収集を実施し、各組織へ情報提供を行っている（図表２－３－１）。

図表２－３－１　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[45]）を派遣し、技術的な支援・助言を実施している。

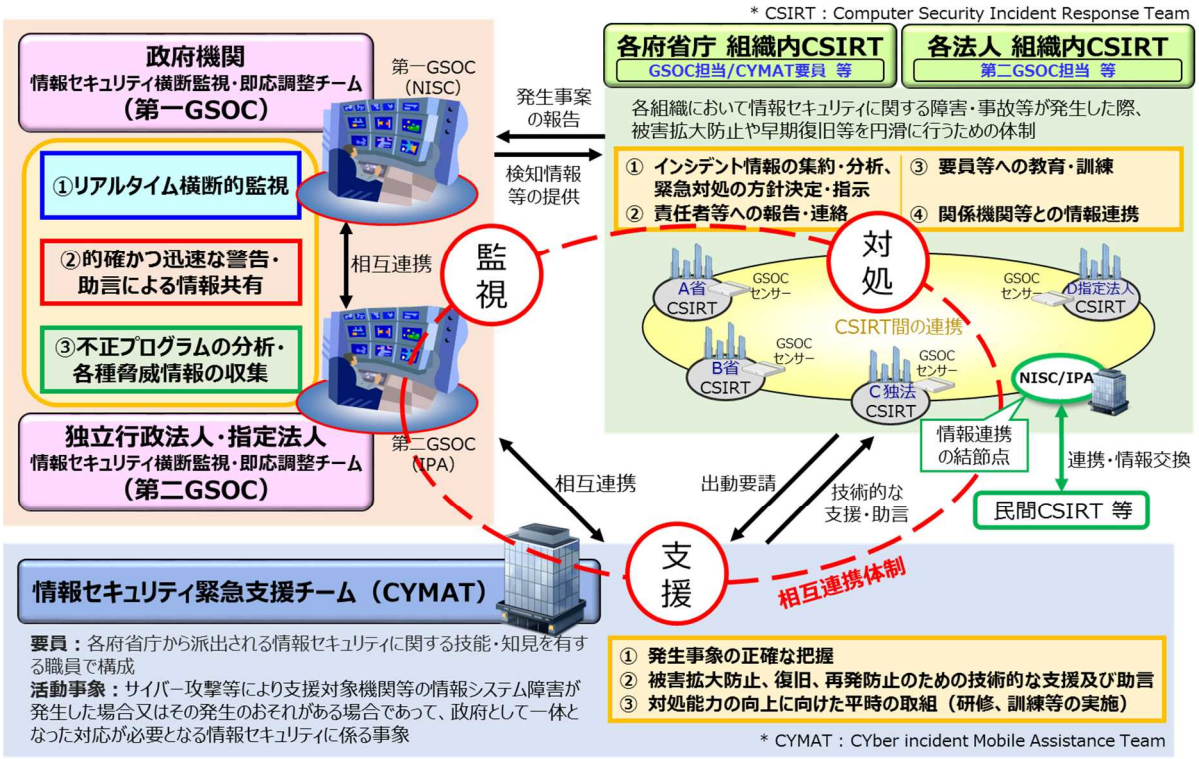
一方、各府省庁や各法人はそれぞれ組織内CSIRT[46]を設置し、自組織の情報システムの構築・運用を行うとともに、サイバー攻撃による障害等の事案が発生した場合には、情報システムの管理者としての責任を果たす観点から、自ら被害拡大の防止、早期復旧のための措置、原因の調査、再発防止等の対応を実施している。

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２－３－２）。

---

[43] 本章では、各府省庁、独立行政法人及び基本法に基づく指定法人並びにオブザーバ機関を総称して「政府機関等」という。
[44] GSOC（Government Security Operation Coordination team）
[45] CYMAT（CYber incident Mobile Assistance Team）
[46] CSIRT（Computer Security Incident Response Team）

図表２－３－２　政府機関等における情報集約・支援体制の枠組み



3.2　2018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[47]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検知や、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、

[47] 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５　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３－10　政府機関等に係る2018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。）[48]については、以下のような傾向がみられた。

① 対策の進展がみられる攻撃等について

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。

2018年度の第一GSOCにおいては、新たに発見された脆弱性やそれらを利用する攻撃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、件数としては低い水準となった[49]。第一GSOCにおける具体的な状況は次のとおりである。

2017年度に検知した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合わせて1,545件であったが、その内容について見ると、「Apache Struts」を狙った通信が1,364件検知されるなど、アプリケーションサーバを狙った攻撃が多かった。2018年度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、クロスサイトスクリプティングを狙った攻撃を11件検知したのみであった。

また、2017年度はポリシー違反の疑いがある通信を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、2018年度はP2P通信を行うファイル共有アプリケーションによる通信を９件検知したのみとなっている。ポリシー違反の疑いがある通信は2016年度から年々減少してきているが、考えられる要因として、前述のような事例があったほか、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等が挙げられる。

[48] 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。

[49] 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、2018年度においては約230万件と高い値となっている。

さらに、DoS攻撃については、2017年度には「Slow HTTP DoS」などといった攻撃を1,292件検知したものの、当該年度以外においては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。

② 引き続き警戒を要する攻撃等について

一方、2018年度の第一GSOCにおけるマルウェア感染の疑いや標的型攻撃の検知件数は図表２－３－３のように2017年度と同程度で推移しており、引き続き十分な警戒を要する状況である。そのほか、政府機関のドメイン（～.go.jp）に似せた紛らわしいドメインを用意しそのドメインに誤って送信されたメールを盗み見たと思料されるタイポスクワッティングの疑いを５件検知した。

図表２－３－３　引き続き警戒を要する攻撃等の検知件数

(件)

年度	2017年度	2018年度
マルウェア感染の疑い	169	111
標的型攻撃	57	66
タイポスクワッティングの疑い	0	5

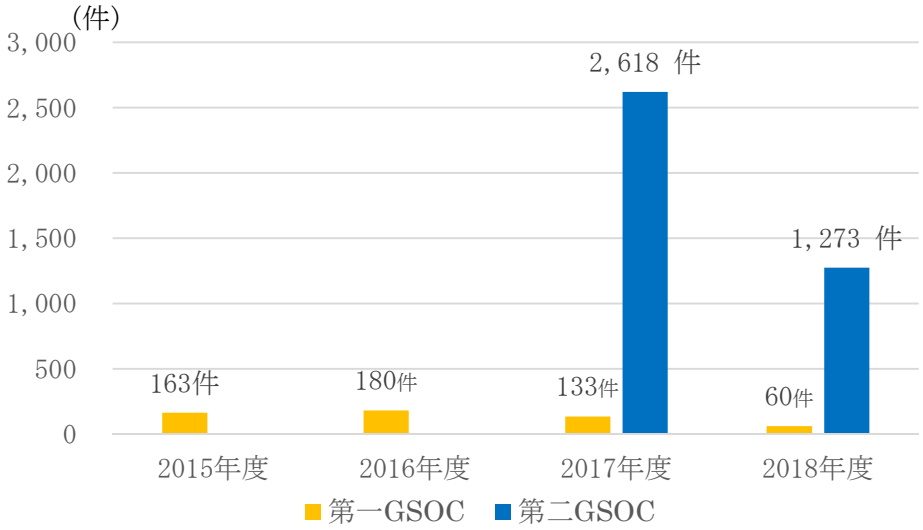
また、第二GSOCにおいては、ウェブアプリケーションの脆弱性や設定不備を狙った攻撃に係る検知が多く、特にコンテンツマネジメントシステム（CMS）を対象としたものが多かった。

ウェブアプリケーションの脆弱性や設定不備を悪用した攻撃の例としては、攻撃対象のサーバ上で任意のコマンドを実行するものや、ファイルを不正にアップロードするものが挙げられる。第二GSOCにおける監視活動においても、このような攻撃を検知しており、今後も対策の強化促進が必要である。

(2) 政府機関等への通報

確認を要するイベントを検知した際には、これを分析し、必要に応じ当該機関への通報を行っており、2018年度においては、第一GSOCでは60件、第二GSOCでは1,273件の通報を行った（図表２－３－４）。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を調整中であることから、第一GSOCと比べて通報件数が多くなっている。

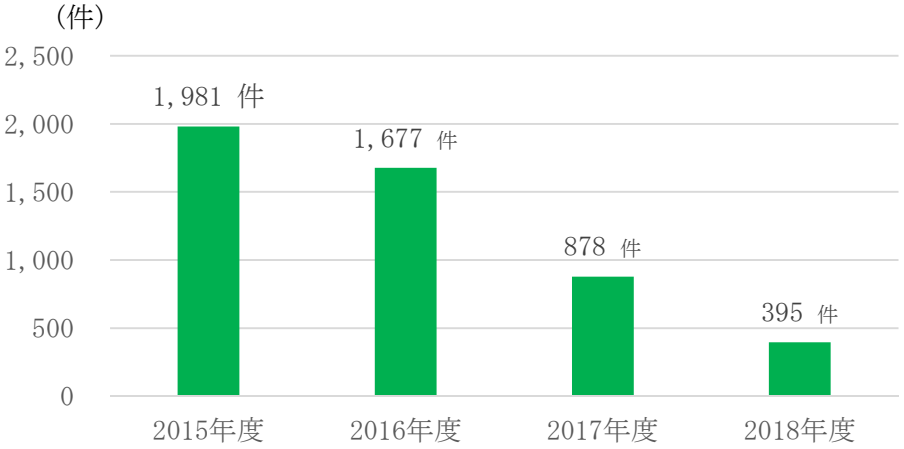
図表２－３－４　GSOCセンサー監視等による通報件数の推移



(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、2018年度においてはGSOCから395件の注意喚起を行った（図表２－３－５）。

図表２－３－５　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年々減少しているが、マルウェアの高度化が進む中、メールの文面が自然な日本語であったり、実在する組織やその所属職員の名前が用いられていたりするなど巧妙化してきていることや、暗号化通信の特性を悪用した攻撃もあることに留意しておく必要がある。

コラム①　～政府機関等に対する不審メールの傾向～

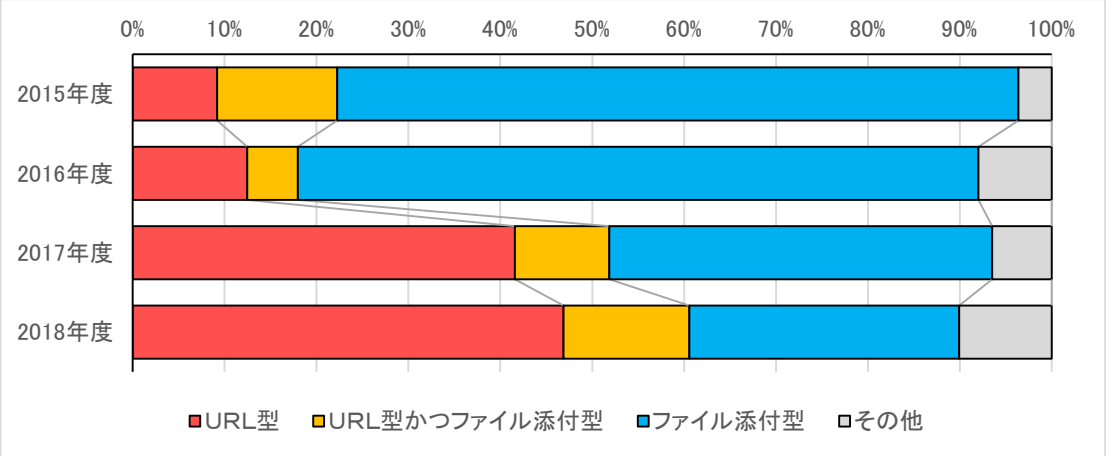
○　不審なファイルに導く手法の変化

図表２－３－６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。近年では、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。）に代わってメール本文に不審なURLを記載する手法（以下「URL型」という。）の比率が高まっており、その背景にはURL型はファイル添付型に比べセキュリティ装置で検知・排除されにくいことがあると考えられる。

URL型の不審メールには、記載されたURLにアクセスすることによってマルウェアがダウンロードされるものとフィッシングサイトが表示されるものとがあり、2018年度では、以前より後者の割合が増加している。フィッシングサイトへの接続は、単に情報を入力させて盗むだけでなくサイバー攻撃の前段階の場合もあることから、安易に不審なURLにアクセスしないよう継続的に周知することが重要である。

ファイル添付型の不審メールでは、Office形式のファイルの添付が多く、埋め込まれたマクロを用いてマルウェアとして機能するものが目立っている。

図表２－３－６　不審メールの傾向



○　送信元の偽装

GSOCにおいて解析した不審メールにおいて、正規のメールアカウントが不正にログインされ、不審メールの送信に使用された事例が散見された。中には、正規の利用者が送信したメールを引用したメールにマルウェアを添付する手口も確認された。図表２－３－７はその例である。

図表２－３－７　返信型の不審メールの例

かつては不審メールの多くで本文に英語が使われたり不自然な日本語が使われたりしていたが、返信型の不審メールでは、自然な日本語が使われ、以前自分が送信したメールの本文が取り込まれているため、不審なメールと判断することが著しく難しくなっている。

なお、返信型の不審メールを作成するにはメールアカウントに不正にログインしている場合が多いと考えられるが、覗き見られたメールから重大な情報漏えい事案に発展する可能性があるため、迅速な対処が必要である。

コラム②　～標的型メールにおける具体的手法～

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は、いわゆるばらまき型メールも多く含まれるが、攻撃者が政府機関等をターゲットにしたとみられる標的型メールも確認されている。

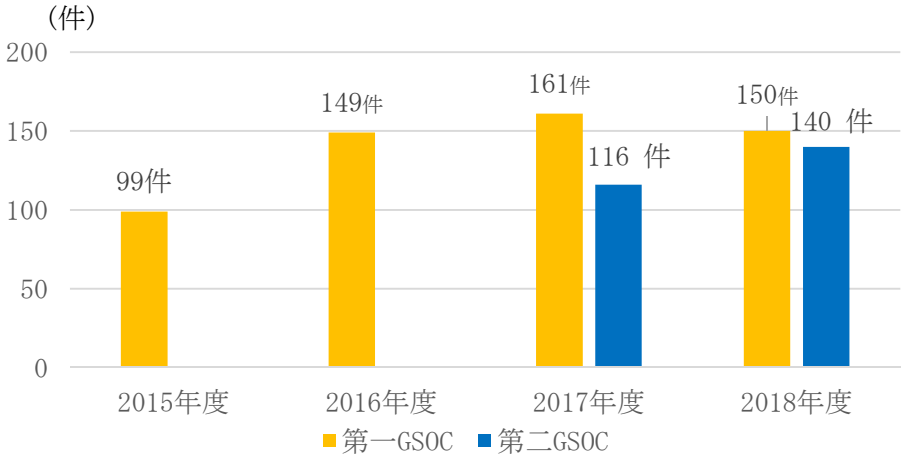
この標的型メールでは、非常に自然な日本語が用いられ、メール本文の末尾に公然情報からのものとみられる実在の政府機関や担当者氏名、連絡先などが付記されるだけでなく、その連絡先情報を一部改変して担当者に確認しにくくする細工も施されており、非常に精巧な作りとなっている。

標的型メールに添付されたファイルを見ると、その内容が時宜に適った政治経済に関するものや、実在する公的な会議に関するものであるなど、メールの受け手に不審感を与えないよう工夫されている。また、ファイル形式も一般的なOffice形式だけでなく、発表されたばかりの脆弱性を有する特殊なファイル形式のものを、他の一般的なファイル形式に偽装するなど、複雑かつ高度な手法が用いられている。

(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。2018年度においては、第一GSOCから150件、第二GSOCより140件の脆弱性情報等を配信した（図表２－３－８）。

図表２－３－８　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、脆弱性の公開に合わせた攻撃や、執拗な攻撃のほか、実在する人物になりすましたメールによる標的型攻撃が行われるなど、手口が高度化・巧妙化していることが分かった。よって、攻撃数そのものは大きく減少しているものの、その中身については、攻撃が効率的に行われるようになったと見ることができ、注意喚起を行った件数も決して少なくない状況であることも踏まえると、政府機関等に対する実質的な脅威度は引き続き高いままであると考えられる。

こうした状況を踏まえ、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、引き続き迅速かつ適切に対応していくこととしている。

3.3　2018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。

2018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。

PCやUSBメモリ等記憶媒体の紛失・盗難事案や、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、誤って個人情報等が記載されているファイルをWebサイトに掲載し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。

4　サイバー空間に係る国際的な動向

サイバー空間はグローバルであり、我が国として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[50]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、同年11月、国土安全保障省に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[51]）が設置され、官民協力を進め、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た。また、2018年８月、2019年度国防授権法を策定し、2019年２月には、CISAが開催するサプライチェーンリスクマネジメントタスクフォースが開催される等、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、2018年12月、欧州ネットワーク・情報セキュリティ機関（ENISA[52]）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、また、2018年５月を期限として、NIS指令[53]の加盟国における国内法化が進められる等、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）[54]が施行されている。また、サプライチェーン・リスクに関しては、５Ｇネットワークのサイバーセキュリティに関する勧告を発出し、加盟国及びＥＵレベルでのリスク評価と連携した対応の強化を打ち出している。

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）を発行した。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。

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、第５次国連政府専門家会合（GGE）[55]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が、2018年国連総会決議に基づき、2019年に第６会期が立ち上がる予定となっている。また、G7においては、2018年４月トロント外相会合の外相共同コミュニケ及び「G7伊勢志摩サイバーグループ会合議長報告書」において、「悪意のあるサイバー行為を阻止し、抑止し、妨げ、対抗するための措置を展開するために協働し、適時にコストを課すことで、悪意のあるサイバー行為を行う者を抑止する」ことが確認されている。また、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

[50] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
[51] Cybersecurity Infrastructure Security Agency
[52] 欧州ネットワーク・情報セキュリティ機関（European Network and Information Security Agency）
[53] 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
[54] 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)
[55] 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。

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。2018年11月には、フランスが主導し、サイバー空間における「信頼」と「安全」を確保するためのマルチステークホルダーでの宣言として、Paris Call for trust and security in the cyberspaceが発表され、我が国もこれを支持している。また、同年11月には、サイバー空間の安定性に関する委員会（GCSC[56]）が、Norm Package Singaporeを発表している。

サイバー攻撃に一国のみで対応することは、容易ではなく、国際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。特に、2019年度にはG20が日本で開催されるところ、我が国は開催国としての立場を活用し、国際社会の連携を推進していく。

[56] Global Commission on the Stability of Cyberspace

3章　2018年度のサイバーセキュリティ関連施策の取組実績と評価

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

【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。

経営層の意識改革を目的として、経営層の意識調査や経営層向けのセミナー、「サイバーセキュリティ経営ガイドライン」の説明会を実施した。また、本社のみならずグループ企業のガバナンスの在り方の指針を示す「グループ・ガバナンス・システムに関する実務指針（仮称）」にサイバーセキュリティ対策の在り方を盛り込むとともに、「取締役会の実効性評価」にサイバーセキュリティへの経営層の関与を盛り込んだ。

さらに、企業が対策を講じる上で認識するべき関係法令集の作成のため、2018年10月より「サイバーセキュリティ関連法令の調査検討等を目的としたサブワーキンググループ」を開催した。

サイバーセキュリティに対する企業の投資の推進に関しては、「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」の公開や、企業のサイバーセキュリティ対策に関する情報開示を行うに当たって参照可能な手引きの策定に着手する等の取組を進めた。加えて、情報セキュリティサービス審査登録制度の基準に適合するサービスの台帳化を行い政府調達で活用することで、情報セキュリティサービスの利用促進を行った。また、税制施策やサイバー保険の推進を目的として、税制施策に関する説明会の実施やサイバー保険も活用した情報開示の仕組みの検討を行った。

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に関して、クラウドに係る取組としては、「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」に、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するとともに、事業者のセミナー等において、CSマークやクラウドセキュリティ認証の取得に向けて呼びかけ等を行った。

営業秘密保護に関する取組としては、各種情報発信を行うとともに、ハンドブックの改訂を見据え調査を実施し、2019年4月に報告書を公開した。また、「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を、HPや講演において周知した。

さらに、組込みソフトウェアに係る取組としては、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況などの実態と動向を把握するための調査・分析を行い、結果を公開するとともに、組込みソフトウェア開発向けコーディング作法について、ガイドとなる書籍の発行や民間団体と連携したセミナー等を通じて普及展開を図った。

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、メンバーを限定しない情報交流の場の構築等を行った。また、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、市場で流通させるための有効な施策について調査を行い、有効性検証やレーティング等の在り方について検討を行った。

【評価】

経営層の意識改革については、各省庁におけるセミナーや各種ガイドライン等の普及活動等を通じて一部への効果はあったと考えられるものの、調査[57]による企業の意識や対策の可視化結果を鑑みると、業種・業態や企業の規模等によっては取組が十分とは言い難い。引き続き、関係省庁が連携して各種取組を積極的に行っていく必要がある。

サイバーセキュリティに対する投資の推進については、プラクティス集の作成や手引書の検討等、取組は進んでいるものの、人材配置等のソフト面への投資や、税制や保険の認識、活用にはまだ至っていない企業の割合も高い[57]ため、普及や周知について取組を進める必要がある。

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は、各分野において導入資料の作成やその周知を図る取組がなされているため、より広い浸透を目指して引き続き取組を継続していく必要がある。

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

【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。

サイバーセキュリティ対策指針の策定に関しては、Society 5.0の実現に必要なセキュリティ対策の全体像を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進め、二度のパブリックコメントを実施した。これらを踏まえて、2019年４月に公表した。また、産業分野ごとにワーキンググループを開催し、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を進めた。特に、ビル分野においては「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」を2019年３月に取りまとめ、パブリックコメントを実施した。さらに、下請中小企業振興法の振興基準の改訂に伴い、下請ガイドラインについて業界団体と連携して、必要な見直しを実施するとともにセミナー等における周知や自主行動計画のフォローアップを行う等、取引適正化に向けた取組を実施した。

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、関係府省庁が連携し、技術開発から実証実験、認証制度の検討、グローバル協調にわたる総合的な研究開発計画を立案した。同様に研究開発計画に基づき公募により研究開発機関を決定し、概念設計を行う等研究開発を開始した。また、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を行うとともに、認証を含む確認の仕組みについて調査を行った。

中小企業においてはサイバー攻撃が経営に与えるインパクトが大きいこと、自社のみならず取引先まで影響が拡大する恐れがあることから、重点的な対策が必要である。このような中小企業における取組の促進に向けて、中小企業の実態を踏まえた対策集の取りまとめや、サイバー保険も活用した情報開示の仕組みの検討を実施した。また、セキュリティ対策の取組を自己宣言するSECURITY ACTION制度を補助金の要件とすることで、中小企業のセキュリティ意識向上と対策強化を図った。

[57] 「企業のサイバーセキュリティ対策に関する調査」（2019年５月 内閣サイバーセキュリティセンター）

【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」の策定に向けて着実に取組を実施した結果、公表に至った。今後は、本フレームワークの普及に向けた活動が重要となる。

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、ワーキンググループを開催する等、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を行うとともに、認証を含む確認の仕組みについて調査を行う等の一定の進展がある。さらに、仕組み構築のための研究開発については、研究開発機関を決定し、概念設計を行う等研究開発を開始する等、一定の取組を進めている。引き続きこれら取組を進めていく。

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いるところであるが、各種調査結果によれば、中小企業における取組の一層の強化を促進する必要があり、引き続き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必要がある。

1.3　安全なIoTシステムの構築

【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。また、セキュリティレベルや物理的安全性等の安全基準が異なる様々なモノ（IoT機器）のつながりが拡大する中、こうしたつながりは、新たな脅威を生む可能性がある。このような状況を踏まえ、官民が連携して、安全なIoTシステムの構築に取り組む必要があり、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平成31年度予算重点化方針」（平成30年７月25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。また、「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」を踏まえ、関係省庁との会合や講演を行うなど、各主体間での共通認識の醸成と情報共有を促進するとともに、各省庁のIoTセキュリティに関する取組との連携を図る等、協働を進めた。

国際標準化に関しては、国際標準化機関であるISO/IEC JTC 1/SC 41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、ISO/IEC JTC 1/SC 27及びITU-T SG17において「IoTセキュリティガイドライン」等を基本とした国際標準化活動を各々推進。国際会合にて作業原案や勧告草案を提案する等、国際標準化のプロセスを進めた。

また、IoT推進コンソーシアム IoTセキュリティWGを通じて、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた取組を推薦するために、各関係機関がそれぞれ取り組むべき事項を、「IoT 機器のセキュリティ対策に関する検討の方向性」として取りまとめた。

さらに、電子情報技術産業協会(JEITA)と連携して開催したスマートホームサイバーセキュリティワーキンググループを活用して、多岐に渡るステークホルダーと連携して、家庭で使用されるIoT機器のサイバーセキュリティの確保に求められるセキュリティ対策の方向性について検討を行った。

また、ネットワーク上の脆弱なIoT機器の対策については、所要の制度整備を行った上で、サイバーセキュリティ戦略本部からの意見[58]も踏まえ所要の手続きを進め、2019年２月より、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を行う取組（「NOTICE」）を開始し、取組を実施した。さらに、今後製品化されるIoT機器に関する対策として、IoT機器の技術基準にセキュリティ対策を追加するための改正省令を2019年３月に公布している。その他、内閣官房において、IoT機器のセキュリティ対策に関する体制等についても関係者との意見交換を行い検討した。

【評価】

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、「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、関係省庁との会合やセミナーでの講演、各省庁のIoTセキュリティに関する取組との連携を図る等、各主体間の共通認識の醸成と情報共有を促進した。また、国際標準化に関しては、ISO/IEC JTC 1やITU-T等におい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、国際標準化のプロセスを進める等一定の進捗があった。引き続き、これら課題を踏まえた取組を推進する必要がある。

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画期的な取組である。そのため、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進めるとともに、調査方法の高度化や実施体制の充実化等のサイバーセキュリティ戦略本部意見や調査結果を踏まえて発展させていく必要がある。また、IoT機器に関する各施策については、IoT機器の普及に伴う脅威の高まりを踏まえ、継続してフォローを行い、全体像を把握しながら取組を推進していくことが求められる。

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

【取組実績】

サイバー犯罪・サイバー攻撃の複雑化・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を通じてウェブサイトの攻撃兆候検知ツールを引き続き提供した。また、IPA及びJPCERT/CCを通じ、脆弱性関連情報について届出・受付・公表をすることで脆弱性関連情報を共有する取組が行われた。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情報提供や注意喚起が行われた。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促進した。

[58] サイバーセキュリティ戦略本部会合第19回会合及び第20回会合資料

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。経済産業省及び国土交通省において、自動運転について、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、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。また、金融庁において、一般社団法人日本仮想通貨交換業協会を資金決済法に基づく認定資金決済事業者協会として認定し、当協会において、システムリスク管理を含む自主規制規則を定め、各暗号資産交換業者における規則の遵守態勢等について指導等を行った。

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評価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周知徹底する取組がなされた。

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。具体的には、警察庁及び都道府県警察において、SNS等に関連した犯罪被害防止のための保護者向けの啓発活動が行われた。

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した官民が連携した取組を実施した。

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が図られた。

【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ゆえに、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。

今後実用化が見込まれる先端技術の一例たる自動運転の研究開発についても、自動車への新たなハッキング手法等を継続的に調査・分析することが必要である。暗号資産（仮想通貨）においても、自主規制団体による実効的な自主規制機能が発揮されるよう促していく必要がある。

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一方で、サイバー犯罪の検挙件数とサイバー犯罪に関する相談件数は、平成30年中も高い水準にある。そのため、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ことが必要である。

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することを踏まえると、サイバー犯罪対策等に従事する職員の能力向上やサイバー空間における事後追跡可能性の確保に継続的に取り組む必要がある。

2.2　官民一体となった重要インフラの防護

【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　平成30年７月25日サイバーセキュリティ戦略本部改定。以下「第４次行動計画」という。）を策定し、これに従って必要な施策を実施している。なお、第４次行動計画においては、13分野が重要インフラとして指定されていたが、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、2018年７月25日に新たに「空港分野」を追加し、14分野を重要インフラとして指定する改定を実施した。

「安全基準等の整備及び浸透」については 、重要インフラ各分野に横断的な指針として、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（2018年４月サイバーセキュリティ戦略本部決定。以下「指針」という。）を公表し、重要インフラ事業者等の自主的な取組を促すとともに、所管省庁等と連携し、各重要インフラ分野の安全基準等の改善状況の把握等を実施した。これらの取組により、関係主体が自主的に安全基準等の見直しの必要性を判断して改善するサイクルが浸透しており、安全基準等の改善が継続的に取り組まれている。また、自然災害の多発やサイバーセキュリティ戦略の改定等、第５版とりまとめ後の環境変化等を踏まえた指針の改定について方向性の承認を得た。

「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他、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実施した。

「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。2018年度は、空港分野を加えた全14分野が演習に参加し、参加者数は3,077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。

「リスクマネジメント及び対処態勢の整備」については、2020年東京大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のためのリスクアセスメント・ガイドライン」を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、同ガイドラインを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」を公表

した。さらに、2020年東京大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターを構築したほか、サイバーセキュリティ対処調整センターを含む、2020年東京大会に向けたサイバーセキュリティ体制の運用方針等について決定した。これら取組により、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た。特に、防護範囲の見直しでは、重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大、交通ISAC（仮称）の創設に向けた取組など、情報共有の輪を拡大・充実化する動きが生じている。

地方公共団体のセキュリティ強化・充実については、総合行政ネットワーク（LGWAN）による監視強化や自治体CSIRTの設立等、セキュリティ強化・充実に資する取組が着実に行われたほか、内閣府による情報照会・提供等の監視・監督やマイナポータルを活用した官民の認証連携等の取組、総務省による脆弱性診断ツールの提供、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）実施等の取組、厚生労働省によるマイナンバーカードの健康保険証としての活用に向けた取組等についても着実に推進された。

【評価】

第４次行動計画に基づく取組は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、同計画の見直しの必要性についても検討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、第５版とりまとめ後の環境変化等を踏まえた指針の改定について着実に進めていくことが望まれる。また、指針を浸透させる取組についても継続して推進することが望まれる。

「情報共有体制の強化」については、情報共有の取組をさらに促進し、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・分析すると共に、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、2020年東京大会の開催を踏まえたシナリオ策定等、より実効性の高い演習方法・内容等について検討を行った上で、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、必要に応じて対象の拡大や内容の改善を図るなど、発展させていく必要がある。

「リスクマネジメント及び対処態勢の整備」については、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、防護範囲見直しの取組が継続して行われているとともに、行動計画の枠組みについて国民等への理解を広められているなど、行動計画の全体を支える共通基盤の強化が着実に取組を進められており、引き続き、経営層への働きかけ等を着実に行いつつ、取組を継続することが望まれる。

地方公共団体のセキュリティ強化・充実については、引き続き、総合行政ネットワーク（LGWAN）の更なる強化やセキュリティ人材の育成等を継続的に取り組む必要がある。また、内閣府、総務省、厚生労働省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。

2.3　政府機関等におけるセキュリティ強化・充実

【取組実績】

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

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７月には、政府機関等が目指すべき情報セキュリティ対策の将来像も踏まえ統一基準群の改定が決定した。改定にあたっては、①未知の不正プログラムに係る被害の未然防止／拡大防止、②IT資産管理の自動化とそれによる脆弱性への迅速な対応、③事案が発生した際にも被害を無効化する、データ保護による情報漏えい対策の導入等をコンセプトとした規定がなされるなど、情報セキュリティ対策の強化・拡充が図られた。

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。

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、2017年度に実施した政府機関等への監査の結果について、ヒアリング等により改善状況のフォローアップを行った。さらに、政府機関等の情報システムに対して、攻撃者が実際に攻撃で行う手法を用いた疑似攻撃にて侵入検査（ペネトレーションテスト）を実施し、問題点を改善するための対応策について助言等を行った。

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。

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共に、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を策定し、設計開発業務に着手した。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クラウドサービスの安全性評価の方法について検討を行った。

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。2018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、１府12省庁対抗による競技形式のサイバー攻撃対処訓練であるNATIONAL 318(CYBER) EKIDEN 2019を実施した。

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月には、各府省庁において特に防護すべきシステムとその調達手続について「申合せ」を行い、2019年４月以降、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）総合戦略室や内閣サイバーセキュリティセンターの助言を得ることとした。

【評価】

統一基準群を改定することにより、各政府機関等において未知のマルウェアの被害の未然防止、拡大防止の対策が推進されることで、将来像を見据えたサイバーセキュリティ対策の体系の進化が図られた。

また、NISCが行った監査及び侵入検査において、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。

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、実効性のある対策を行う体制が整えられた。

引き続き、政府機関等におけるサイバーセキュリティ対策が推進されるよう、継続的に取組を推進していく必要がある。

2.4　大学等における安全・安心な教育・研究環境の確保

【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化・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、大学等においてサイバーセキュリティに関するインシデントが多数発生していることを踏まえ、大学等におけるサイバーセキュリティ対策の状況について把握するとともに、再発防止策を検討し、その徹底を図るために、2018年４月より、ワーキンググル

ープを開催した。ワーキンググループにおいては、当該対策の推進のため、大学等が取り組むべき事項、文部科学省が支援すべき事項等について検討を行った。

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・演習を試行的に行うとともに、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（ペネトレーションテスト）を実施した。

加えて、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に、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施するとともに、サイバー攻撃に関わるデータ解析技術の開発を促進するため、国立大学法人等の通信データのうち、M2Mを含めたサイバー攻撃に関するデータ等を収集して、データのフォーマットや匿名化を含めた提供方法について検討し、国立大学法人等研究機関へ提供する準備を整えた。

【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った。ガイドライン等作成に向けて、引き続き検討を行う必要がある。

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試行的に行うとともに、大学等の情報システムに対する脆弱性診断を実施した。2018年度は国立大学法人等を対象としたが、各層別研修については、2019年度より公私立大学を対象に加え実施する予定である。

さらに、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と情報セキュリティ担当者の研修を引き続き実施するとともに、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ける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、データ解析技術の開発を促進する必要がある。

2.5　2020年東京大会とその後を見据えた取組

【取組実績】

引き続き、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象としたリスクマネジメントの促進や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進した。

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（東京都、近郊県及び地方競技会場）を対象とする第３回リスクアセスメントの実施を依頼、各事業者等から提出された実施結果について、重要サービス分野内及び重要サービスを分野横断的に分析し、各事業者等へ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について、第１回として、電力、通信、水道、鉄道、放送分野等から５者を対象に実地検証、全重要サービス分野から20者を対象に書面検証を実施し、結果の取りまとめを行った。

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構築したほか、サイバーセキュリティワーキングチーム等における検討を更に進め、大会に向けたサイバーセキュリティ体制の運用方針等を関係府省庁、大会組織委員会、東京都等と協議の上、決定した。さらに、関係省庁において、サイバー攻撃対策の推進に向けて、脅威情報の収集・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周知及び活用を図った。

【評価】

リスクマネジメントの促進については、当初の計画どおり地方の競技会場まで対象を拡大してリスクアセスメントの取組を実施できた。2018年度から実施結果を分析して各事業者等にフィードバックしており、更なる効果が期待できる。

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、計画どおり進捗した。2019年４月にはサイバーセキュリティ対処調整センターの運用を開始したが、今後は段階的に訓練演習を重ねてその運用要領、運用手順に慣熟するとともに、G20やラグビーワールドカップ等、実際の運用の場を活用して更なる能力の向上と運用要領等の改善を行い、対処態勢の完成度を上げていく必要がある。

2.6　従来の枠を超えた情報共有・連携体制の構築

【取組実績】

2018 年 12 月に、サイバーセキュリティ基本法の一部を改正する法律が成立した。同法により改正された基本法第 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。

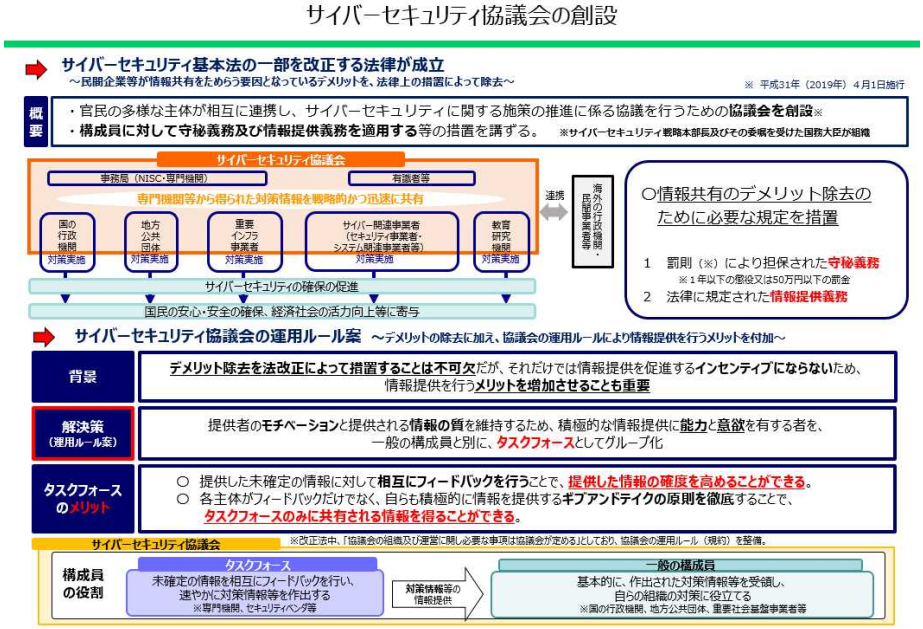
同協議会は、官民を問わず、また、業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことを目的としている。

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）を整備した。具体的には、各主体の自主性を最大限に尊重するためのルール、各主体が安心して情報の共有を行うことを可能にするためのルールや既存の情報共有体制との円滑な連携等を可能にするためのルールなど、様々な運用ルールの整備を図った。

【評価】

2019年4月にサイバーセキュリティ協議会が組織され、計画どおり進捗が図られた。今後は、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を迅速かつ確実に共有するとともに、より多くの主体が参加する重厚な体制を構築していく必要がある。

図表３－２－１　サイバーセキュリティ協議会の概要及び設立について



2.7　大規模サイバー攻撃事態等への対処態勢の強化

【取組実績】

関係省庁及び重要インフラ事業者等が参加する大規模サイバー攻撃事態等対処訓練を通じて、政府の初動対処態勢の整備や対処要員の能力強化が図られたほか、訓練を踏まえた対処態勢の見直しにも取り組まれている。都道府県警察においても、重要インフラ事業者等との共同対処訓練が実施され、現場レベルでの対処態勢強化が図られている。

警察庁では、大規模産業型制御システムを対象としたサイバー攻撃に係る調査・検証等にも取り組んでおり、この取組を通じた対処能力向上が期待できる。

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に大きく貢献している。

個人情報保護委員会においては、個人データ漏えい等事案防止を目的とした取組を実施した。

【評価】

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。

また、各対処機関においてそれぞれの能力向上に取り組むとともに、サイバー攻撃の対象となり得る事業者等を支援する取組についても充実・強化していく必要がある。

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

【取組実績】

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。また、実務レベルにおける二国間サイバー協議や有志国会合、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するような法制度に対しては、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、透明性の確保、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、次会期国連政府専門家会合の方向性等を含め、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ている。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（2018年10月、2019年3月）への参加や、日ASEANサイバー犯罪対策対話（2019年1月）の実施等を通して、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、次会期国連政府専門家会合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。

3.2　我が国の防御力・抑止力・状況把握力の強化

【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、防衛省の調達する情報システムに係る情報セキュリティ上のサプライチェーン・リスク対策としての、調達に係る関連規則

の整備等を通じて、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いる。

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12月に外務報道官談話を発出した。また、悪意ある主体によるサイバー空間の利用を妨げる能力に関しては、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、2019年度予算においてサイバー防衛隊の人員を約70名増員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、2019年１月には第３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している。

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でいる。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・分析を実施している。

【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。

3.3　国際協力・連携

【取組実績】

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いる。

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ているほか、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ている。また、ICT-ISACをはじめとする日米間でのISAC連携を進めている。

能力構築支援に関しては、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2016年10月）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いる。特に、経済産業省において、2018年9月10～14日、米国・国土安全保障省（DHS）及びNCCIC ICSから専門家5名を招聘し、ASEAN等向けに日米サイバー共同演習を実施した。また、総務省において、「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。防衛省においては、2019年３月11～15日、ベトナム人民軍要員15名を招へいし、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、我が国との連携を深めている。

【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諸国とは日・ASEANサイバーセキュリティ政策会議が10周年を迎えて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の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。

4　横断的施策

4.1　人材育成・確保

【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。

経営層が示す戦略の下、組織がマネジメントすべきリスクの一つとして、業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である「戦略マネジメント層」を担う人材が求められる。この戦略マネジメント層の育成・定着に関しては、必要な知識・スキル及びそれを学ぶカリキュラムを検討するとともに、実際に試行的取組を行い、成果を取りまとめた。また、企業の責任者クラス等を対象とした短期プログラムや戦略マネジメント層になることも見込まれる中核人材を育成するプログラムの実施、高等教育機関等における社会人学生の受け入れを実施した。

実務者層・技術者層の育成に関して、教育機関では、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。組織レベルでは、都道府県警察と重要インフラ事業者等との共同対処訓練を実施し、また、行政機関や地方公共団体等における実践的な演習を実施し、対処態勢の強化を推進した。

各種資格・試験に関しては、情報処理安全確保支援士の登録者数が増加するとともに、さらなる活用と普及のため登録状況の公表と企業や団体への周知を行い、また、情報セキュリティマネジメント試験の広報活動を実施した。

人材育成の基盤の整備や若年層向けの取組として、“学び直し”の指針であるITSS+について、新たな領域を公開した。教育段階に関しては、2020年度の新学習指導要領の実施を見据え、教科等横断的な情報活用能力の育成に係る、指導方法や教材の利活用等の研究を実施した。また、小中高校等の教員養成課程に、ICT活用の指導法等の内容を加えた。さらに、各地域で教員等を対象に研修を実施した他、教員等を対象とした情報モラル教育指導者セミナーも実施し、教員育成の充実を図った。

また、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「SECCON2018」、「SecHack365」を引き続き実施・協力した。さらに、ITを駆使してイノベーションを創出する人材を発掘・育成する未踏事業を引き続き実施する中で、プロジェクトマネージャーにはセキュリティ・キャンプの講師を登用し、セキュリティテーマ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、各府省庁において2018年８月末に、2016年に策定された「各府省庁セキュリティ・IT人材確保・育成計画」の見直しを行った。また、同計画に基づく体制の整備として機構・定員要求を行い、政府全体で約60のポスト増（機構新設や振替を含む）による体制強化を実現、適切な処遇の確保として、俸給の調整額の要求を行い、政府全体で約40のポストの適用が認められた。ほかにも、有為な人材を確保するための採用活動、処遇改善、研修の受講等の取組を推進した。

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、ケーススタディなどを通じて、当該審議官等の各府省庁におけるセキュリティ対策の司令塔機能として必要な知識・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。

さらに、人材育成に関しては、可能な限りグローバルな規模で切磋琢磨できるようにすべきであるという観点から、国内外の大学や公的機関等における取組について、関係機関へのヒアリングや調査会での議論を行った。また、ベトナム等にてサイバー攻撃に強い電力制御システム（SCADA）の導入のため支援を実施するとともに、導入に向けた理解を醸成するための研修を実施した。

【評価】

戦略マネジメント層の育成に関しては、各種調査やセミナーの実施により育成手法の研究が着実に進んでいるが、今後は、企業等においてその定着を図ることが重要な課題となる。引き続き、関係省庁が連携して、役割やスキルの見える化のためのモデル構築及び育成手法の確立・普及を目指して取組を推進していく必要がある。

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。これらを維持して引き続き人材の育成・確保を進めていく。

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等の一般の方を対象とした取組も実施されており、引き続き推進していく。

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・IT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。

4.2　研究開発の推進

【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、以下の取組等を実施した。

先進的な技術を用いた研究開発に係る取組としては、量子コンピュータに関するセキュリティやAI（人工知能）に関する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実施した。また、システムの品質、安全性、効率を向上、両立させるための革新的、先端的技術の基礎研究に取り組む活動や、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実施した。

サプライチェーンにおける信頼の確保に係る取組としては、不正なプログラムや回路が仕込まれていないことを技術的に検証するための体制整備に向けた検討を進めるとともに、不

正なハードウェアやソフトウェアの検出に関する課題についての国内外の動向調査や検証、未知のIoT回路を不正回路であるかどうか判定する技術や、電力波形をはじめとする複数の外部特徴量から不正機能を検知する技術の開発等を進めた。また、真贋判定技術と動作監視解析技術の検証を行い、安全性と有効性の評価を実施した。さらに、IoT機器向け暗号実装技術の最適化・高速化を行った。

攻撃活動の把握、分析、共有に係る取組としては、サイバー攻撃誘引基盤（STARDUST）を高度化し、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、情報共有のためのサイバーセキュリティ・ユニバーサル・リポジトリ（CURE）の構築や、自動対策技術の確立に向けた試験運用を行った。また、IoT機器の効率的な脆弱性検証に向けた、周波数の利用状況の自動推定による広域ネットワークスキャン技術や、スキャン時の無線通信量軽減に関する基礎技術の開発を行った。

暗号化技術などの基盤技術の研究開発に係る取組としては、量子鍵配送ネットワークの信頼性に関する、模擬医療データの分散ストレージ機能の実証や、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開始した。また、耐量子計算機暗号の標準化動向調査及び鍵管理ガイドラインの作成に向けた検討を行った。さらに、CRYPTREC暗号リストに掲載された暗号技術の監視や暗号政策の検討を進めた。

サイバーセキュリティの研究開発の成果の国際的な情報発信等に係る取組については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、我が国初となるジャパン・パビリオンの出展支援を実施した。また、ISO/IEC JTC 1/SC 27の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。

【評価】

先進的な技術を用いた研究開発に関しては、量子コンピュータやAI、IoTに係るサイバーセキュリティ確保の技術・製品・サービスの検討や研究がなされており、更なる技術向上に向け今後も引き続き取組を継続していく必要がある。

サプライチェーンにおける信頼の確保に関しては、不正回路や不正機能の検出技術やIoT機器向け暗号実装技術の強化が進められているが、引き続き、各要素技術の向上に向けた取組を継続するとともに、技術的検証等を行うための体制構築等に関する取組を推進する必要がある。

攻撃活動の把握、分析、共有に関しては、STARDUSTやCUREの強化や、広域ネットワークスキャンの技術開発などがなされているが、今後の攻撃の増加や高度化への対応に向け、引き続き取組を継続していく必要がある。

暗号技術などの基盤技術については、量子鍵配送や量子暗号通信技術に関する実証実験、耐量子計算機暗号に関する調査などがなされており、引き続き、実用化に向けて取組を継続していく必要がある。

国際的な情報発信等については、国際的なイベントでの情報発信や、国際機関で中心的な役割を果たすなどの取組がなされており、引き続き、国際的な影響力向上に向けて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、今後は、「サイバーセキュリティ研究・技術開発取組方針」（令和元年５月サイバーセキュリティ戦略本部報告）に基づき、取組を推進していく。

4.3　全員参加による協働

【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、普及啓発・人材育成専門調査会等における議論を経て、2019年１月24日にサイバーセキュリティ戦略本部において「サイバーセキュリティ意識・行動強化プログラム」を決定した。

若年層への普及の観点では、全国各地で、児童・生徒、保護者・教職員等に対してe-ネットキャラバンやインターネット安全教室、講師へのトレーニングを実施した。また、各地域で情報教育を担う教員等を対象とした研修や、情報モラル教育に関するセミナーを実施した。さらに、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にも取り組んだ。

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。さらに、セミナー等への講師派遣や展示会への出展による情報の周知・提供を実施した。情報発信の一環として、内閣官房において、「インターネットの安全・安心ハンドブック」（旧称：ネットワークビギナーのための情報セキュリティハンドブック）の内容の見直しを行い、各種媒体にて無料で配信するとともに、都道府県警察と連携して普及活動を行った。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175件実施された。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を行った。特設サイトへの総アクセス数は12万超であった。

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、白書や各種調査報告書の公開、公衆無線LANに関するオンラインコンテンツを活用した啓発活動等を実施した。

図表３－４－１「約束のネバーランド×サイバーセキュリティ月間特別イベント「抗え。この世界（インターネット）の脅威に。」」の様子（2019年３月３日開催）

【評価】

「サイバーセキュリティ意識・行動強化プログラム」を2019年１月に策定するとともに、本プログラムに沿った取組を着実に進めた。特に、若年層を主な対象とした各地で行われる教室等において参加者が増加するなど、関心の高まりが見られており、継続的な取組を進めていくことが重要である。

情報発信や相談窓口に関しては、今後も内容の改善を検討しつつ、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のさらなる充実に関しては、各地域の関連行事は前年同程度開催され、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、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、前年度と比較して大きな反響が得られた。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。

また、事業者や関係団体等の取組が促進される環境整備等に関しては、各種調査報告書や白書等の公表等、今後も着実に取組を進めていくことが求められる。

5　推進体制

【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、内閣サイバーセキュリティ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、新戦略に基づく諸施策が着実に実施されるよう、新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、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推進するなど、内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図った。

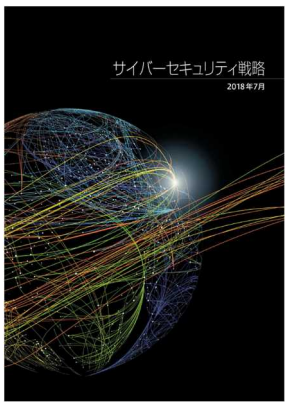
更に、新戦略の趣旨を、国内外の関係者に向け、効果的に発信し、十分な理解を得ること目的に、国内外の関係機関への配付や国際会議・普及啓発イベントにおける関係者への配布などにより広く国内外へ周知広報するため、新戦略のカラー冊子（日本語版及び英訳版、英訳版フライヤー）を制作した。

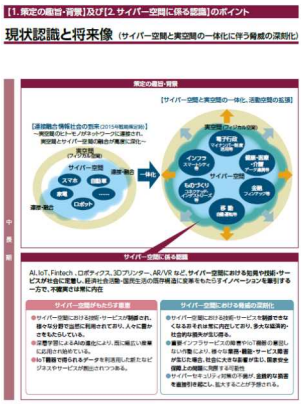
内閣官房及び関係省庁において、カラー冊子を活用するなどして、計79件のイベント等で、国内の関係者6,500名超、国外の関係者1,500名超に対して新戦略の発信を行い、周知を行った。また、カラー冊子については、第21回本部会合において、在外公館などを通じて発信すべきとの提案があったことを踏まえ、外務省を通じ、在外公館へ配布を行った。

【評価】

新戦略の発信や関係主体との連携強化を通じた推進体制については、パートナーシップに基づく取組や、新戦略のカラー冊子の制作・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る成果に関し、一定の評価ができる。一方で、新戦略で掲げたサイバーセキュリティエコシステムの推進には、その理解・浸透が広く行われることが必要不可欠であり、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である。その効果的な実施に向けて、十分な現状把握の上で進めることが重要であり、関係機関との一層の連携の強化を図り、被害実態の把握にも努め、新戦略の発信等に取り組むことが求められる。

図表３－５－１　新戦略カラー冊子





２部　年次計画（2019年度）

2部　年次計画（2019年度）

1章　2019年度のトピックとなる取組

本章では、新戦略の対処方針に関する国内外の関係者の理解・浸透を図るため、その方針別に、「トピックとなる取組」を抽出し、以下のとおり、その方向性と主な施策例を示す。

1　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～

1.1 サービス提供者関連

(1)　企業

【取組の方向性】

政府としては、民間企業のサイバーセキュリティの確保のため、「サイバーセキュリティ人材育成取組方針」（平成30年６月サイバーセキュリティ戦略本部報告）に基づき、引き続き一体となって取組を推進していく。

また、2019年４月には、Society 5.0の実現に必要なセキュリティ対策の全体像を示す「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を策定した。CPSFの全体枠組みに沿って対象者や具体的対象を整理することで、CPSFの具体化・実装を推進し、企業・組織におけるリスク源の洗い出し、対処すべきセキュリティ対策の検討を促進することで、各産業分野におけるサイバーセキュリティの確保を進めていく。

経営層に関しては、意識改革に向け、産業界とも連携した取組を引き続き進める。特に、サイバーセキュリティ対策の観点を含めたグループガバナンスの在り方に関するガイドラインの策定や、サイバーセキュリティ関係法令集に関するハンドブックの取りまとめに向けて、取組を進める。また、デジタルトランスフォーメーション（DX）の進展や、サイバー空間における脅威の高まりといった状況も踏まえ、DXとサイバーセキュリティを一体的に進める戦略マネジメント層の確保・育成に向け、2018年度に作成したモデルカリキュラムも活用した戦略マネジメント層の普及・育成の促進や、独立行政法人情報処理推進機構（IPA）を中心に、「産業サイバーセキュリティセンター」における短期プログラムや「戦略マネジメント系セミナー」、将来、戦略マネジメント層になることも見込まれる中核人材を育成する「中核人材育成プログラム」のカリキュラムのさらなる充実を目指す。実務者層・技術者層については、イノベーションを支える先端的な人材の育成に向け、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的とした「セキュリティ・キャンプ」の開催や「SecHack365」の実施等を進める。また、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。これらの人材育成施策を推進する際には、教える側の質の確保といった観点にも留意していく。

また、実務者層に向けては、サイバーセキュリティに関する投資の促進に向け、サイバーセキュリティ経営ガイドラインの実践のための「プラクティス集」の継続的な更新や可視化ツール作成に取り組む。さらに、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」の策定に取り組む。

加えて、中小企業・地域におけるサイバーセキュリティの取組は、日本の産業に対する世

界の信頼に直結する重要な課題であることを踏まえ、サイバーセキュリティ対策強化を中小企業・地域まで展開するため、中小企業・地域の更なる実態把握、徹底した中小企業の現場支援、地域を支えるコミュニティ形成を進めていく。

さらに、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向けては、我が国における検証等を通じてSociety 5.0を支える信頼の価値を創出するというコンセプト、“Proven in Japan”、を旗印として、新たなセキュリティ技術の有効性を検証・評価する仕組みを検討するとともに、IoT機器等の信頼を高度に検証するハイレベルな検証サービスの実証等を通じ、世界に貢献する高水準・高信頼の検証サービスを拡大するための包括的な検証基盤を構築する等の取組を進めていく。加えて、営業秘密の保護に関するハンドブック等の普及啓発や、今後さらに活用が進むと想定されるクラウドサービスに関するセキュリティ対策のガイドラインの普及に取り組む。

【関連する主な施策例】

・1.1(1)(ア)：サイバーセキュリティ人材育成取組方針の推進
・1.1(1)(イ)：グループ・ガバナンス・システムに関する実務指針の策定
・1.1(1)(オ)：サイバーセキュリティ関係法令集の策定
・1.1(2)(ア)：サイバーセキュリティ対策実施の目安となる可視化ツールの作成
・1.1(2)(イ)：サイバーセキュリティ対策情報開示の手引きの策定
・1.1(3)(ウ)：クラウドセキュリティ監査制度等の普及促進
・1.2(1)(ア)：Society 5.0の実現に向けたサイバー・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の推進
・1.2(3)(ウ)：サイバーセキュリティお助け隊に係る実証事業の全国実施
・1.2(3)(カ)：SECURITY ACTION制度の拡大及びニーズに応じた制度の見直し
・4.1(1)(ア)：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
・4.1(1)(エ)：モデルカリキュラムの活用等による戦略マネジメント層の普及促進

(2)　重要インフラ事業者等

【取組の方向性】

「サイバーセキュリティエコシステム」の実現に向け、重要インフラの防護については、「任務保証」の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現するため、サイバーセキュリティに関する全体的な底上げを行う必要があり、各々の主体が自主的な取組を進めつつ、国も積極的な支援を行うことで、官民一体でセキュリティ対策に取り組んでいくこととしている。

こうした取組を進める中、各地で複数の自然災害が発生し、重要インフラ事業者等においても、地震や台風によって多大な被害を受けたところである。また、災害による直接的な被害だけでなく、大規模停電に伴う間接的な被害を受ける事態も発生している。こうした状況から、「任務保証」の考え方を踏まえ、自然災害に起因する重要インフラサービス障害の発生を可能な限り減らすこともますます重要となっている。

また、新戦略にも記載したとおり、重要インフラ事業者等における適切な対応を促進するため、データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理の在り方を含め、安全基準等を改善する取組を継続的に推進する必要がある。

これらの社会動向の変化、新たな知見を踏まえ、「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）（平成30年４月４日サイバーセキュリティ戦略本部決定）」を改定する検討を進めてきた。

今後は、「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「データ管理の在り方」を同指針に追加するとともに所要の修正を行う改定を実施し、改定後の指針については、従来と同様、関係省庁等が連携し、各重要インフラ分野の「安全基準等」への反映を通じて事業者へ浸透させる取組を促進していく。

【関連する主な施策例】

・2.2(1)(ア)：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

1.2 全ての主体関連

(1)　意識・行動強化

【取組の方向性】

サイバー空間の脅威が広がる中、安全・安心なサイバー空間の利用を進めるため、サイバーセキュリティに対する国民一人一人の意識・理解を広く醸成し、自律的な活動が促進されることが不可欠である。政府としては、「サイバーセキュリティ意識・行動強化プログラム」（平成31年１月サイバーセキュリティ戦略本部決定）に基づき、産学官民の関係者の連携のもと、幅広く取組を推進していく。具体的には、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。また、同プログラムにおいて重点的な対象と位置付けた、中小企業、若年層、地域に向けた取組については、例えば中小企業にとって身近な知見者となる「セキュリティプレゼンター」を通じた情報の周知など、施策を一層強化し、それぞれの主体における取組の促進を図っていく。

【関連する主な施策例】

・4.1(イ)：人材育成や普及啓発に関するポータルサイトの構築

・4.3(ア)：サイバーセキュリティ意識・行動強化プログラムの推進

・4.3(キ)：セキュリティプレゼンター制度等を通じた企業等への意識啓発

・4.3(サ)：青少年や保護者等に向けたe-ネットキャラバン等啓発講座の推進

・4.3(タ)：一般のインターネット利用者を対象としたインターネット安全教室の推進

(2)　IoT関連

【取組の方向性】

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。また、セキュリティレベルや物理的安全性等の安全基

準が異なる様々なモノ（IoT機器）のつながりが拡大すると、新たな脅威を生む可能性があるため、一定の整合性・一貫性をもって戦略的に取り組む必要がある。

具体的には、我が国の安全・安心といった強みを活かしながらグローバルな規模での展開を進めることも見据え、ISO/IEC JTC 1/SC 27及びITU-T SG17において、引き続き、IoT推進コンソーシアムのIoTセキュリティワーキンググループにおいて策定された「IoTセキュリティガイドライン」の国際標準化に向けた取組を進めていく。

また、各IoT機器の特性や利用方法等を踏まえるとともに、サイバーセキュリティの確保に必要な要件を満たすIoT機器の利用を推奨するべく、改正省令やその運用方法・解釈等を定めるガイドラインの策定により、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を進めていく。さらに、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について、関連事業者との連携の下、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し、セキュリティ対策を推進していく。

【関連する主な施策例】

・1.3(1)(ウ)：IoTセキュリティガイドライン等をベースとした国際標準化の推進
・1.3(2)(イ)：IoT機器の技術基準へのセキュリティ対策の追加及びガイドラインの策定
・1.3(2)(イ)：家電など家庭で使われるIoT機器に関するサイバー・フィジカル・セキュリティ対策ガイドラインの策定
・1.3(2)(ウ)：サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び注意喚起

1.3 国際協力・連携関連

【取組の方向性】

サイバー攻撃は国境を越えるところ、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。2019年には、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 End Working Group)が立ち上がる予定であるところ、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。特に、2019年は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。

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、途上国のサイバーセキュリティ能力構築支援は、先進国の責務である。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によって培われた知見や経験の相互共有の促進、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を行うための講師育成に取り組む。この

ほか、JICA課題別研修等のスキームを用いて各種の能力構築支援を行う。このように、内閣官房が中心となって関係府省庁が効果的な連携、情報共有を行い、様々な政策手段を活用し、開発途上国における能力構築に貢献すると共に、同地域における実務的な協力活動を推進していく。

【関連する主な施策例】

・3.1(2)(ア)：多国のサイバー空間における国際的なルール・規定作り等への積極的関与

・3.3(1)(ウ)：アジア共通統一試験の定着及び講師育成の促進

・3.3(3)(ア)：関係府省庁・機関の連携による各国における効果的な能力構築支援

1.4 研究開発関連

【取組の方向性】

近年のサイバーセキュリティに関する脅威の拡大や、我が国の研究・技術開発の動向を踏まえ、顕在化する課題に対処していくため、「サイバーセキュリティ研究・技術開発取組方針」（令和元年５月サイバーセキュリティ戦略本部報告）に基づき、取組を進める。

具体的には、サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備を進める。また、サプライチェーン全体の信頼確保に向けた、ICT機器・サービスのセキュリティの技術検証を行うための推進体制の整備や、それを実施する上で必要となる、不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化に、関係機関の連携の下で取り組む。さらに、国内産業の育成・発展に向けた、製品・サービスを安心して利用するための検証基盤や中小企業のニーズに対応したビジネス創出等に向けた支援策の推進、AI等も活用した、サイバー攻撃の観測・把握・分析技術や情報共有基盤の強化、暗号等の基礎研究の促進等にも取り組む。加えて、サイバーセキュリティの研究・技術開発について、産学官の関係者が連携し、相互の取組の情報共有や研究活動における連携を図るためのコミュニティ形成についても、検討を開始する。

研究・技術開発の推進に当たっては、個別の研究・技術開発の成果の創出に留まらず、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。加えて、社会実装を促進する上では、サイバーセキュリティの重要性が社会において十分に認識されていることが前提となることから、国民社会におけるサイバーセキュリティに関する意識向上に向けた取組も併せて実施する。

【関連する主な施策例】

・1.2(2)(ウ)、4.2(1)(ア)：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

・4.1(5)(ア)、4.2(1)(ホ)：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の推進

・4.2(1)(コ)：IoTシステムにおける脅威に対応する先端的セキュリティ技術の研究開発

・4.2(1)(オ)：設計・製造におけるチップの脆弱性検知手法の研究開発

・4.2(1)(チ)：AI技術を駆使したマルウェアの挙動解析を自動化する技術の研究開発

2　積極的サイバー防御　～事前の能動的な取組～

2.1 政府関係者の取組

(1) 改定された統一基準群に基づく取組

【取組の方向性】

政府機関等においては、統一的な基準を踏まえた情報セキュリティ対策が講じられるところ、2018年7月に「政府機関等の情報セキュリティ対策のための統一基準群」の改定を行い、脅威に対して事前に積極的な防御策を講じる観点も踏まえ、未知の不正プログラムによる被害の未然防止／拡大防止、IT資産管理の自動化とそれによる脆弱性への迅速な対応、データ保護による情報漏えい対策等をコンセプトとした規定などによって、政府機関等における情報セキュリティ対策の強化・拡充の取組を行っている。今後は、脅威が深刻化するサイバー攻撃への対応及びクラウドサービス利用時における適切な情報セキュリティ対策等について、次期統一基準群の改定に際して、対策として盛り込むよう取組を進めていく。

また、政府機関等に対して、その基準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、独立行政法人等への監査は、IPAとの連携等により、2020年東京大会までに、全ての法人に対し行う計画とする。

あわせて、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収集・分析し、その結果を政府機関等に対して適宜提供しており、さらに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。

これらの取組などとともに、今後の政府機関等のIT投資の効率化を踏まえて、セキュリティ関連投資の充実を図るために必要な予算を確保するなどにより、政府機関等の情報セキュリティ対策を推進するものである。

【関連する主な施策例】

・2.3(1)(ア)：次期統一基準群改定に係るコンセプトの検討
・2.3(1)(キ)：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）の運用
・2.3(1)(セ)：政府機関等と次期GSOCにおける効果的かつ効率的な連携の推進
・2.3(4)(ア)：政府機関等における統一基準群等に基づく取組状況の監査の実施
・2.3(4)(イ)：政府機関等の情報システムに対するペネトレーションテストの実施
・2.3(4)(ウ)：独立行政法人等における統一基準群等に基づく取組状況の監査の実施
・2.3(4)(エ)：独立行政法人等の情報システムに対するペネトレーションテストの実施

(2) 政府調達におけるサプライチェーン・リスク対策

【取組の方向性】

サイバー攻撃は複雑化・巧妙化しており、今後発生し得るリスクに応じて事前に積極的に取り得る防御策が必要であるところ、サイバーセキュリティを確保する上では、情報の窃取、破壊、情報システムの停止等、悪意のある機能が組み込まれた機器をあらかじめ使用しない

ようにすることが極めて重要であり、こうしたサプライチェーン・リスク対策を強化するため、2018年7月に閣議決定した、新戦略において、サプライチェーン・リスク対策の重要性を盛り込むとともに、2018年12月には、各府省庁において特に防護すべきシステムとその調達手続について、「申合せ」を行った。

この「申合せ」は、2019年4月以降、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）総合戦略室や内閣サイバーセキュリティセンターの助言を得ることを示したものである。

【関連する主な施策例】

・2.3(1)(ス)：政府調達におけるサプライチェーン・リスク対策の強化
・2.3(2)(イ)：安心・安全なクラウドサービス利用に向けた安全性評価の方法に関する検討
・3.2(1)(キ)：防衛省の調達仕様書等に適用される調達に関する関連規則の整備
・3.2(1)(ケ)：防衛産業に適用される調達に関する情報セキュリティ基準の整備

(3) ボットネット対策

【取組の方向性】

IoT機器の生活への普及・浸透が進む中、2016年にはネットワーク上の脆弱なIoT機器が、ウイルス感染等により攻撃者の自由に操られる状態となった機器を束ねたネットワーク（ボットネット）を構築し、大規模なDDoS攻撃を仕掛ける事案が発生する等、IoT機器を悪用したサイバー攻撃の深刻化が進んでいる。

これに対し、2019年2月から開始した「NOTICE」では、国立研究開発法人情報通信研究機構（NICT）がパスワード設定等に不備のあるIoT機器を調査し、電気通信事業者が当該機器の利用者への注意喚起を行っている。サイバー攻撃を受けてから対応するのではなく、先手を打って悪用されるおそれのあるIoT機器を能動的に調査し利用者に対して適宜パスワード変更等を促すことにより、ネットワーク上の脆弱なIoT機器を減少させ、安全なIoTシステムの構築を目指していく。

今後も引き続き、産官学民及び民間企業相互間の連携と役割分担の下で進めるとともに、実効性の高い取組となるように適時見直しを行いながら、調査方法の高度化や実施体制の充実化等、取組を発展させていく。

【関連する主な施策例】

・1.3(2)(ウ)：サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び注意喚起

(4) 先行的防御を可能にするための取組

【取組の方向性】

サイバー空間の脅威の深刻化が進み、攻撃の種類も多種多様となっていることから、従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行い先行的な防御を進める必要がある。

具体的には、脅威情報の共有・活用の促進として、脆弱性情報の公表に係る制度の着実な

実施や脅威情報収集の自動化に関する支援、制御システムに係る公開情報の分析に基づく情報提供などの取組を進めるとともに、ウェブサイトへのサイバー攻撃の予兆を事前に検知するツールの利用拡大を目指して機能改善に向けた検討を行っていく。また、攻撃者の情報を集めるための攻撃誘引技術の活用として、官公庁・大企業のLAN環境を模擬した実証環境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進めていく。さらに、近年増加傾向にあるフィッシング詐欺に対してはサイト閉鎖等の対応を引き続き実施するとともに、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っていく。加えて、2019年から2020年にかけて予定されている複数の国際的なイベントに関連して、なりすましメールが増加することも想定され、国民の間で個人情報や金銭の詐取等の被害が生じる可能性は高いため、そのような被害を防止するためにもなりすましメールを防止する送信ドメイン認証技術を推進していく。

【関連する主な施策例】

- 2.1(1)(ア)：脆弱性情報公表に係る制度の実施等を通じた脆弱性関連情報の共有
- 2.1(1)(ウ)：ソフトウェア等の脆弱性に関する自動配信等による脆弱性マネジメント支援
- 2.1(1)(オ)：サイト閉鎖等によるフィッシング詐欺対策及び量的な対応力の向上
- 2.1(1)(キ)：ウェブサイトの攻撃兆候検出ツールの利用拡大
- 2.1(1)(サ)：なりすましメール対策となる送信ドメイン認証技術の周知・広報
- 2.2(1)(ケ)：大規模LAN環境を模擬した実証環境(STARDUST)を活用した標的型攻撃の解析及び事業者間での情報共有
- 2.2(1)(ト)：制御システムに係る脆弱性等の公開情報の分析・提供及び調査方法等の効率化の検討

2.2 従来の枠を超えた取組

(1) 情報共有連携体制（サイバーセキュリティ協議会）

【取組の方向性】

2018年12月に、サイバーセキュリティ基本法の一部を改正する法律が成立した。同法により改正された基本法第17条に基づき、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のサイバーセキュリティ協議会が組織された。

同協議会は、官民を問わず、また、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を目的としている。

サイバーセキュリティ協議会については、2019年４月に第一期の構成員の募集を行い、５月から暫定運用を開始する予定である。2019年度中に、第二期及び第三期の構成員の募集を行い、漸次拡大していくことを予定している。

運用面については、実際に情報共有活動を行う中で、構成員等の意見も踏まえつつ、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を迅速かつ確実に共有するとともに、より多くの主体が参加する重

厚な体制を構築するなど、さらなる情報共有の促進のために必要な施策を推進していく。

【関連する主な施策例】

・2.6(1)(ア)：サイバーセキュリティ協議会の運用ルールの見直し、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の迅速かつ確実な共有及び多くの主体が参加する重厚な体制の構築

(2) 暗号資産（仮想通貨）に関する取組

【取組の方向性】

インターネットを通じて電子的に取引されるいわゆる暗号資産（仮想通貨）において、暗号資産交換業者に対するサイバー攻撃により顧客の暗号資産（仮想通貨）が流出した事例が発生している。そのような状況を踏まえ、利用者保護の確保に向けて、サイバーセキュリティ対策を進めていく。

具体的には、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、自主規制機関における実効的な自主規制機能の発揮を促すとともに、自主規制機関と連携しながら、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っていく。また、引き続き、定期的な自主規制機関との意見交換等を通じて上記取組の推進を図っていく。

【関連する主な施策例】

・2.1(1)(セ)：暗号資産にかかる自主規制機能の発揮促進及び交換業者に対するモニタリングの強化

(3) 自動運転に関する取組

【取組の方向性】

自動運転の実現に向けては、外部からの通信が車両ネットワークにつながることも想定され、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おそれがあるため、かかる事態が生じないような対策が求められる。そのためには、車両機器や制御装置の脆弱性を設計・開発段階から取り除く視点などが必要となるが、自動車の安全基準については、国際場裡においてサイバーセキュリティ対策に係る国際基準策定の議論が進められており、議長国として議論を主導するとともに、国際基準の適合性に係る審査体制の構築に向け、検討の深化を図っていく。また、関係省庁との連携の下、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ことにより、自動運転に係る脅威を想定の上、先手を打って対策を進めていく。

【関連する主な施策例】

・2.1(1)(ソ)：自動車のサイバーセキュリティ対策に係る国際基準策定の主導及び基準適合性に係る審査体制の構築に向けた検討の深化

・2.1(1)(チ)：自動運転システムへの新たな攻撃手法及び対策技術等の調査

3　2020年東京大会とその後を見据えた対処態勢の強化

3.1 2020年東京大会に向けた対処態勢

【取組の方向性】

オリンピック・パラリンピック競技大会は、世界最大級のスポーツイベントであり、全世界から注目を集めることから、過去大会においてもサイバー攻撃の標的となっており、東京大会に向けて、国を挙げてサイバーセキュリティの確保に取り組んでいるところである。

大会のセキュリティ全般については、「2020 年東京オリンピック・パラリンピック競技大会関係府省庁連絡会議」の下で開催されている「セキュリティ幹事会」において、平成29 年３月、「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に向けたセキュリティ基本戦略（Ver.1）」を決定し対策を推進している。

サイバーセキュリティの確保については、基本法に基づく新戦略を平成 30 年７月に閣議決定し、この二つの戦略に基づき、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・事案情報の情報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ている。対処態勢の整備に当たっては、「セキュリティ幹事会」の下のサイバーセキュリティワーキングチームにおいて、関係府省庁、大会組織委員会、東京都等と協議を実施し、2018年度末にはサイバーセキュリティ対処調整センターの運用方針等を作成するとともに、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構築した。

2019 年度においては、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G20 大阪サミット等において運用するとともに各種演習・訓練を通じて、関係機関等との連携体制の強化や手順等の慣熟及び見直しを実施し、様々な事象への対応力、対処支援調整能力を高め、万全な対処態勢を確立させていく。また、これまでにも実施してきた「分野横断的演習」や「金融業界横断的なサイバーセキュリティ演習」等の官民の枠を超えた関係者間での演習・訓練についても、2020年東京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し、大会の開催を踏まえたシナリオを策定する等、より実効性の高いものとすることで障害対応体制の強化を一層推進していく。

大会のために準備した対処態勢やリスクマネジメントの取組によって得られた経験・ノウハウは、大会後もレガシーとして日本のサイバーセキュリティの確保に活用していく。

【関連する主な施策例】

- 2.2(1)(テ)：官民の枠を超えた関係者間での演習・訓練
- 2.5(1)(ア)：2020年東京大会に関する重要サービス事業者等のリスクマネジメントの促進
- 2.5(1)(ア)：サイバーセキュリティ対処調整センターの運用及び演習・訓練

3.2 大規模サイバー攻撃事態等への対処態勢

【取組の方向性】

海外での事例を踏まえると、我が国においてもサイバー攻撃によって国民生活に大きな影響を与えるような業務・機能・サービスの停止といった事態がいつ発生してもおかしくない状況にある。さらに、あらゆる分野で情報通信技術が不可欠となり、ネットワークを介してあらゆるものがつながっている昨今、複数の分野で一斉に被害を受け、その影響が実空間における混乱といった形で表面化することが考えられる。

こうしたことを踏まえ、政府においては内閣官房を中心として情報の集約・共有、初動対処に係る訓練・演習とその結果を踏まえた見直しを通じて対処態勢の強化を図り、各対処機関においてはサイバー空間における情報収集・分析能力の向上を図っていく。また、サイバー攻撃の対象となり得る事業者等においても、サイバー攻撃への対処活動を実施することから、この活動を支援する取組を充実・強化していく。

【関連する主な施策例】

・2.7(ア)：大規模サイバー攻撃事態等に対する訓練の実施

・2.7(イ)：初動対処態勢の整備や能力向上に必要な取組の実施

・2.7(カ)：個人情報漏えい等事案への適切な対応等

・2.7(キ)：国内における組織内CSIRT設立の支援

・2.7(ク)：金融分野における大規模インシデント等の発生に備えた官民連携の危機管理態勢の構築

2章　2019年度の各種施策一覧表

本章では、以下のとおり、新戦略の体系に沿って各目的・領域別に、新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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。
（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。

(2)サイバーセキュリティに対する投資の推進

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。

（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。
（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。

(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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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）	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。
（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。
（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。
（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。
（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（ア）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG 1（制度・技術・標準化）にて、策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、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。

(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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。

(3)中小企業の取組の促進

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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）
（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）
（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。
（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。

（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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、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。

(2) 脆弱性対策に係る体制の整備

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

（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。
（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

(1) 安全・安心なサイバー空間の利用環境の構築

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。
（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。
（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	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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(2)サイバー犯罪への対策

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。
（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、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。

（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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）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。
（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。
（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。

（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）	総務省 経済産業 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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。

(2)地方公共団体のセキュリティ強化・充実

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
(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。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。
(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。
(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。
(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。
(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。
(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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
(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。

（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。
（ウ）	経済産業省	経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPAを通じ、「IT製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを必要に応じて行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。
（エ）	経済産業省	経済産業省において、IPA を通じ、国際共通に政府調達等における情報セキュリティの確保に資するため、引き続きCCRAの会合などに積極的に参加するとともに、我が国に有益となるＨＣＤ（複合機）等の国際共通プロテクション・プロファイル（PP）の開発を推進する。
（オ）	経済産業省	経済産業省において、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。
（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。
（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。
（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。
（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。
（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。
（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。
（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。

(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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

(4)監査を通じたサイバーセキュリティの水準の向上

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。

(5)組織的な対応能力の充実

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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共に、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等を対象に、2018年度に改定した政府統一基準群の解説、マネジメント監査等の実施結果から得られた課題並びに昨今のサイバーセキュリティの動向等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の合同研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。

(2)大学等の連携協力による取組の推進

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。

(2)未来につながる成果の継承

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月の諸施策の目標と実施方針）より		
・2020年東京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
（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。
（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。
（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。

2.6　従来の枠を超えた情報共有・連携体制の構築

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）
（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。
（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、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。
（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。
（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、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。
（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。

(1) 多様な主体の情報共有・連携の推進

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

(2) 情報共有・連携の新たな段階へ

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

2.7　大規模サイバー攻撃事態等への対処態勢の強化

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。

（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。
（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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 End 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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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。
（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。

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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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）を実施していく。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（コ）	内閣官房	内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。
（サ）	警察庁 法務省	警察庁および法務省（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。

(2) サイバー攻撃に対する抑止力の向上

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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	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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。 ・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。
（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。
（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。
（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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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。

3.3　国際協力・連携

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、Blach 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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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。
（オ）	総務省 外務省	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	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。
（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。

（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。
（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、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。
（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。

(2) 事故対応等に係る国際連携の強化

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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。
（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。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

（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。

4　横断的施策

4.1　人材育成・確保

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）
（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。
（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。

(1)戦略マネジメント層の育成・定着

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。

(2)実務者層・技術者層の育成

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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、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。
（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。
（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、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	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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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・技術を有する人材の発掘・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	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。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

（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。
（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。
（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。
（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、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。
（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。

(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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。

4.2　研究開発の推進

(1)実践的な研究開発の推進

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）
（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。
（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）
（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。
（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。
（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。
（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）
（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）
（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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）
（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）
（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）
（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。
（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）

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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。
（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）
（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）

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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）
（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。
（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。
（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。
（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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。
（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。
（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）
（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。

(2) 中長期的な技術・社会の進化を視野に入れた対応

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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
(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。

4.3　全員参加による協働

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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
(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。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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
(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）
(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、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。
(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。
(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。
(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。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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
(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。

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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）	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。
（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。
（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。
（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）
（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）
（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。
（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）

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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
（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。
（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。

5　推進体制

新戦略（2018年7月27日閣議決定。2018年7月～2021年7月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、新戦略に基づく諸施策が着実に実施されるよう、新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** **・2020年東京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
（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。
（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。
（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）
（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。

別添１　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１－目次＞

内閣官房 108
内閣法制局 109
人事院 110
内閣府 111
宮内庁 112
公正取引委員会 113
警察庁 114
個人情報保護委員会 115
金融庁 116
消費者庁 117
復興庁 118
総務省 119
法務省 120
外務省 121
財務省 122
文部科学省 122
厚生労働省 124
農林水産省 125
経済産業省 126
国土交通省 127
環境省 128
防衛省 129

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2019年度当初までに定めた「対策推進計画」を基として、2018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2019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

2018 年度の総合評価・2019 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

2018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政府機関に対する攻撃、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、GSOCから提供された不審メール情報等を内閣官房において集計したところ、2018年は約350件と経年的には減少傾向にあるものの、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、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、情報の性格・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セキュリティ事案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、サイバー攻撃に対する防御についても同様であり、コンピュータ技術だけではなく、人を騙すテクニック、いわゆるソーシャルハッキングについても新たな手法が考案されていることから、広い意味での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、GSOCより発出されている不審メール情報等が多い状況が続いていることは、2020年東京オリンピック・パラリンピック競技大会を控え、関係者に対する警鐘として重く受け止めなければならない。

このような状況を踏まえ、内閣官房では2019年度においても、脅威に関する幅広い情報収集や実践的な職員教育を中心に情報セキュリティ対策を行っていくことが必要であり、さらに効果的な教育を実施する観点から、2017年度に導入したeラーニングを改善した上で引き続き実施するほか、従来の資料配布や、内閣官房内閣サイバーセキュリティセンター等が主催する研修会への参加を一層促進する。

情報収集については、CYMAT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

2018 年度の総合評価・2019 年度の全体方針

最高情報セキュリティ責任者
総務主幹　平川　薫

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。

2018 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 が実施するマネジメント監査の実施により、情報セキュリティ対策の助言を受けた。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。

2019 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、統一基準群の改定に伴う内閣法制局情報セキュリティポリシー関連規程の整備、NISC が実施したマネジメント監査における指摘事項に対する改善計画への対応、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

2018 年度の総合評価・2019 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　松尾　恵美子

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。

2018年度においては、「政府機関の情報セキュリティ対策のための統一基準」の改定や情勢の変化等を踏まえ、人事院情報セキュリティポリシーを改定し、その周知・徹底及び情報セキュリティ対策の遵守について再認識させるため、新任管理者を対象とした集合研修や新規採用職員研修における情報セキュリティに関する講義のほか、全職員を対象としたe-ラーニングによる情報セキュリティ教育を実施した。このほか、「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への報告を経験させた。

職員の情報セキュリティ対策の実施状況について、職員全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、課室ごとに結果を分析した。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。

2019年度においては、自宅におけるテレワークなど要管理対策区域外において情報処理を行う場合の情報セキュリティ対策を定め、テレワークを希望する職員に対する研修を実施し、情報セキュリティ対策の実施の徹底を図るとともに、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自己点検や監査を充実させ、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

2018 年度の総合評価・2019 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　井野　靖久

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日々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、不正なマルウェア等を検知する内部対策、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。

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。

こうした中、2019年1月には内閣府LANを更改し、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、セキュリティ対策を強化した。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した。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、2019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、政府ドメイン取得、運用方法の周知徹底等、職員に対する教育・訓練、啓発、自己点検等、人への対策を重点的に実施する。

宮内庁

2018 年度の総合評価・2019 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　野村　善史

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、2018年度においては、主に以下の取組を実施した。

〇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

〇重要な情報とインターネットの分離に係る実効的な対策の推進

〇宮内庁情報ネットワークシステムの更なる整備に向けた検討

2019年度においては、政府機関等の情報セキュリティ対策のための統一基準群の改定を踏まえ、宮内庁情報セキュリティポリシーや各種手順等の整備を行う。

また、宮内庁セキュリティ・ＩＴ人材確保・育成計画を推進し、お代替わりに伴う宮内庁の組織改正も踏まえ、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、宮内庁情報ネットワークシステムの更なる整備を円滑に実施し、情報セキュリティ対策の多層化・高度化を図る。

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

2018 年度の総合評価・2019 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　粕渕　功

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。

2018年度においては、標的型メール攻撃による情報漏えいの脅威が高まっていることから、公正取引委員会においても、同様の攻撃による情報漏えいを防ぐため、標的型メール攻撃に特化した全職員対象の訓練を実施するとともに、不審メールのURLをクリック等した場合にルールに則り報告・連絡を行うエスカレーション訓練も行うことでその対策に関する研修・周知を行った。また、公正取引委員会セキュリティ・ＩＴ人材確保・育成計画を改定し、当該計画に基づき情報セキュリティに対する更なる意識向上を図るため、情報セキュリティ全般に関する全職員を対象としたｅラーニング研修を実施したほか、管理職員並びに新規採用、中途採用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た。そのほか、引き続き、当該計画に基づき情報セキュリティ関係機関への出向を行うことにより、人材の育成を図った。さらに政府統一基準群の改定や内閣官房内閣サイバーセキュリティセンターによるマネジメント監査、自己点検・監査の結果を踏まえ、公正取引委員会における情報や機器の取扱いについての関係規程を見直し、情報セキュリティ水準の向上を図った。

2019年度においては、引き続き、情報セキュリティ全般に関する教育・訓練を実施し、情報セキュリティ対策に関する自己点検及び監査を実施する。また、標的型メール攻撃に特化した訓練については、今年度の訓練結果を踏まえ、内容等を見直すなどにより、実際の標的型メール攻撃に即した対応ができるようにする。そのほか、情報セキュリティインシデントが発生した際に、迅速かつ的確に対応できるよう、インシデント発生を想定した連絡訓練に加え、公正取引委員会の関係部局において初期対応訓練を行い、公正取引委員会として、情報セキュリティ対策の更なる向上を図る。

警察庁

2018 年度の総合評価・2019 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、警察情報セキュリティポリシーを策定するなどして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。

2018年度においては、2018年７月に「政府機関等の情報セキュリティ対策のための統一基準群」が改正されたことを受け、2018年９月に警察情報セキュリティポリシーを改正し、対策の強化等を図った。また、改正した警察情報セキュリティポリシーの浸透・徹底を図るとともに、教育教材について、昨今の情報セキュリティに係る脅威等を踏まえて内容を見直した上で、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も毎年度実施しており、監査の結果、情報セキュリティに関する教育の実施等、積極的な取組を確認した。一方で、端末のセキュリティ対策等の実施状況において改善を要する事項が認められたことから、改善措置の結果報告を求めるなどして確実に対策を講じた。

2019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を実施するとともに、「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」（平成30年12月10日関係省庁申合せ）に基づき必要な措置を講じる。また、職員が警察情報セキュリティポリシーの趣旨を理解し、適切に情報通信技術を活用できるよう情報リテラシーの向上を図っていく。

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

個人情報保護委員会

2018 年度の総合評価・2019 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、2016 年１月１日に設置された合議制の機関である。その使命は、独立した専門的見地から、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」（2019 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。

2019 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、2018 年度に改定した「個人情報保護委員会情報セキュリティポリシー」（2018 年 12 月 14 日最高情報セキュリティ責任者決定）の周知徹底を行うほか、委員会事務局の更なる体制拡充を踏まえて、新入・転入職員を含む全ての職員において的確な対応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・管理の徹底を図るものとする。

金融庁

2018 年度の総合評価・2019 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　中島　淳一

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（2018 年６月 15 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、ビックデータ利活用等の 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を継続していくことの必要性を強く認識しており、2018 年度においては、情報セキュリティに関する教育・訓練の実施、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・多層化等に取り組んだところである。

2019 年度においては、基本的にはこれまでの取組みを継続することとしつつ、2018 年度の取組み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みへの的確な対応を念頭におき、情報セキュリティに関する教育・訓練、情報システムに関する新たな技術的対策の導入に向けた検討、インシデント発生時における対応体制の見直しなどに引き続き取り組み、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

2018 年度の総合評価・2019 年度の全体方針

最高情報セキュリティ責任者
次長　井内　正敏

2018 年度は、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（以下「当庁ＬＡＮシステム」という。）の更改を通じて、技術的な面における情報セキュリティ対策の強化を行った。ネットワーク分離やログ統合監視機能等の導入により、庁外からの不正なアクセスに対する防御能力を向上させると同時に、シンクライアント端末や仮想デスクトップの採用により、行政端末からの情報漏えいのリスクを低減させた。

人的対策の強化についても継続して取り組んでいる。当庁ＬＡＮシステムの更改に合わせて、「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）」に準拠する形で、当庁情報セキュリティポリシー（以下「当庁ポリシー」という。）及び付随規程類を改定し、職員への周知を行った。また、年２回実施した不審メール訓練では、前年度の訓練よりも不審メールの開封率が大きく低下しており、継続的な取組によって職員の情報セキュリティ意識が向上していることが確認された。

2019 年度は、昨年度と同様に、ＰＤＣＡサイクルに従って情報セキュリティ対策を推進する。

対策のうち、情報セキュリティ教育に関しては、全職員を対象とした e ラーニングによる教育や不審メール訓練を継続して行い、情報セキュリティ意識の向上を目指す。なお、教育内容については必要に応じて見直しを行う。当庁ＬＡＮシステムを始めとする当庁が所管する情報システムに関しては、当庁ポリシー等や情報セキュリティ要件に従い適切に対策が行われるよう管理する。

上記の対策内容について、自己点検や情報セキュリティ監査によって遂行状況を確認し、問題点等があれば計画的な改善活動を行う。

復興庁

2018 年度の総合評価・2019 年度の全体方針

最高情報セキュリティ責任者
統括官　末宗　徹郎

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。

2018年度は、「政府機関等における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、復興庁情報セキュリティポリシー等の関係規定の改定を実施した。

また、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、2017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。

2019年度においては、2018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

2018 年度の総合評価・2019 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、行政組織、公務員制度、地方行財政、選挙、消防防災、情報通信、郵政事業など、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ており、国民生活の基盤に広く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。

○2018年度の総合評価

2018年度は、政府統一基準群の改定を受け、総務省情報セキュリティポリシー（以下、「ポリシー」という。）の改定を行い、引き続き、政府統一基準群に沿った対策が行えるよう配慮した。また、前年度の対策推進計画に基づく各種情報セキュリティ対策を実施したところ、自己点検や監査等の結果から、省内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。

○2019年度の計画

2019年度以降、国際的な大規模イベントが多数開催されることを踏まえ、引き続き、サイバーセキュリティに係る対策の実施を行う。特に、2018年度に実施した施策及びリスク評価の結果を踏まえ、以下の事項を重点的に実施する。

また、内閣サイバーセキュリティセンターによる重点検査、各種監査等に対しては、重要な取り組みとして随時対応を行う。

(ア)サイバー攻撃等に備えた教育・訓練の実施

省内の情報セキュリティ対策・職員のセキュリティ意識については、従来から教育を通じ向上に努めてきたところであるが、昨今の政府機関等へのサイバー攻撃等の増加・高度化も踏まえ、以下の教育・訓練を行う。

- 最新のサイバー攻撃動向に対応した教育
- 情報システム向けの情報セキュリティインシデント対応訓練

(イ)セキュリティ対策推進のための取組の実施

総務省においては、「大臣官房企画課サイバーセキュリティ・情報化推進室サイバーセキュリティ対策担当」及び最高情報セキュリティアドバイザーがCSIRTとして省内及び所管法人における情報セキュリティインシデントの対応を行うとともに、省内から寄せられる情報技術利活用時の情報セキュリティに係わる相談への対応を行ってきた。2019年度においても、引き続き以下の取組を実施する。

- 省内及び所管法人における情報セキュリティインシデントへの対応
- 最高情報セキュリティアドバイザーによる情報システム向け相談会の実施
- 利活用とのバランスを考慮した情報セキュリティ対策の推進
- 情報セキュリティに関する教育及び自己点検の実施
- 情報セキュリティ監査（ウェブサーバ監査、運用準拠性監査、ポリシー監査等）
- 不審メールへの適切な対応に関する訓練

法務省

2018 年度の総合評価・2019 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　川原　隆司

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、法務行政を司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において示された取組の方向性を踏まえ、2018 年度は、前年度に全面改定を行った当省の情報セキュリティの基本的枠組みを定める情報セキュリティポリシー（法務省における情報セキュリティ対策の基本方針等）について、確実な遵守のための浸透を図るとともに、あわせて、情報セキュリティマネジメントの実効性確保のための取組として，助言型の内部監査の試行を実施した。

また、情報セキュリティの様々な取組への適切な対応に必要な人材の確保のため、「法務省におけるセキュリティ・ＩＴ人材確保・育成計画」（2016 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。

これらの取組等を評価すると、情報セキュリティに係る教育、自己点検及び監査等の取組を通じて、新たな情報セキュリティポリシーの浸透は進んでいるものの、情報セキュリティ対策が組織全体で実行されるためには、各組織における情報セキュリティポリシーに基づく対策の実施状況を確認し、確実な遵守のための改善を図る必要がある。すなわち、組織及び情報システムの運用における情報セキュリティ対策が適切に行われているかを確認し、その結果に基づき情報セキュリティ対策の適切な改善に取り組むことが求められる。また、2018 年７月の政府統一基準群の改定を契機とした法務省ポリシーの改定を行ったことから、最新の情報セキュリティポリシーの浸透を効果的に進める必要がある。

さらに、サイバー空間における脅威の深刻化を踏まえて、新たな脅威の発生に適切に対応できるように継続的に改善を進めるとともに、事案発生時には迅速かつ適切に対処できるよう、組織としての対処能力の維持・向上を図る必要がある。

したがって、2019 年度は、最新の情報セキュリティポリシーに基づいた情報セキュリティ対策を浸透させつつ、組織及び情報システムの運用における情報セキュリティ対策の取組状況に関する監査を通じて情報セキュリティポリシーの遵守状況を確認するとともに、情報セキュリティインシデントに対処する要員等の知見及び技能の向上を通じたサイバーセキュリティ対処能力の向上に取り組むこととする。

外務省

2018 年度の総合評価・2019 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　下川　眞樹太

外務省は、安全保障をはじめとする外交機密情報に加え、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おり、情報セキュリティの確保は最重要課題の一つである。一方で、当省職員を標的とした不審メールが恒常的に送られており、またその技術や手口は日々巧妙化・高度化していることから、電子情報を含めた情報の適切な管理やセキュリティの確保のあり方について不断に見直していく必要がある。

＜外務省情報セキュリティポリシーの策定＞

2018 年度の取組としては、同年７月の政府統一基準群の決定を受け、当省におけるセキュリティ政策の土台となる「外務省情報セキュリティポリシー」の改定を行った。さらに職員の理解促進を目的として当該ポリシーをわかりやすく解説したマニュアル等も策定した。

＜セキュリティマインドの向上：サイバー訓練＞

標的型メールの模擬訓練を職員向けに複数回実施した。特に、当省ではＬＡＮをはじめ各種情報システムを在外公館でも共有していることから、一般の職員の他に現地採用の外国人職員も含めた同メール訓練を日本語及び英語で本省・在外公館双方において同時に実施した。

＜情報セキュリティ政策部門との協力や研修の充実化＞

刻々と進化するサイバー攻撃に対して実効性のある防御を行うためにも、その動向の把握が重要である。この観点から、セキュリティ専門家を外部から招いて省員向け研修を行う等して、セキュリティ分野における最新情報の共有を行っている。

また、省内のサイバー政策部門における意見交換を定期的に行ってきており、国際社会におけるサイバー問題への協力体制や各国の取組について把握するほか、当省が受けているサイバー攻撃の状況をシステム部門が政策部門に情報共有する等、多面的な取組を行っている。

＜インシデント発生への対処＞

実際に事案が発生した場合に備え、インシデント発生の際の情報共有フローを見直し、省内のサイバーセキュリティ・情報化参事官や所管する独立行政法人等との連絡が一層迅速に行われるよう体制を整備する等、即応力の強化を図っている。

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予定されている。これら行事が円滑に執り行われるよう、また、本格化する 2020 年東京オリンピック・パラリンピック競技大会の準備と並行して、引き続き外交業務が円滑に行われるよう、特に以下の事項について取り組み、外務省全体の情報セキュリティ水準のさらなる向上を図っていく。

（１）　改定した「外務省情報セキュリティポリシー」に則した教育資料の策定、ｅラーニングの実施
（２）情報システム保有課室のシステム担当者向け情報セキュリティ講習会の創設
（３）民間企業での取組事例や省員アンケート結果を参考にした効果的な啓発・教育方法の検討

財務省

2018 年度の総合評価・2019 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　矢野　康治

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。）とも連携し、情報セキュリティの確保に取り組んできた。

2018年度においては、政府機関としての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研修・標的型メール攻撃訓練を実施したほか、システム所管部局を対象とした研修や省内・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を実施
- システム統括部局（大臣官房文書課業務企画室）を中心に、CSIRT要員等のインシデント対処訓練やサイバー防御演習への参加
- 省内における情報セキュリティ上の課題把握のための内部監査や自己点検等を実施
- NISCによる独法への監査について、所管独法等連絡会議を開催して情報を共有
- 2018年7月に改正された政府統一基準群を踏まえた財務省情報セキュリティ対策基準の改定
- CIO補佐官４名を最高情報セキュリティアドバイザーとして指名

2019年度においては、着実に情報セキュリティ対策の強化を進めるため、新たに、「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」を踏まえた調達手続の実施（サプライチェーン・リスク対応）や、サイバーセキュリティ協議会構成員として求められる役割・取組みを進めていくとともに、引き続き、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）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や情報セキュリティインシデントの対処訓練等への参加を奨励（職員セキュリティ意識の向上を図る）
- 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する）
- 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

2018 年度の総合評価・2019 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　生川　浩史

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（2016 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。

リスク評価の結果、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。

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)　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

2018 年度の総合評価・2019 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　宮川　晃

近年の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及び情報通信技術の活用の進展に伴い、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の向上を図る必要がある一方で、世界的規模で生じているサイバーセキュリティに対する脅威も年々深刻化し、政府機関を標的とした様々なサイバー攻撃が増加している。

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、2018年度においては、次の取組を重点的に実施した。

- 高度な標的型攻撃に対する多層防御対策の強化
- インターネットからの重要情報に対する直接的なサイバー攻撃が及ばないようにするための内外環境の論理的な分離の実施
- 「政府機関等の情報セキュリティ対策のための統一基準群」の見直し等に基づく当省情報セキュリティポリシー（以下「ポリシー」という。）及び関係規程の改定
- 情報セキュリティ監査の実施

2019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、新たに以下の取組を実施することとする。

- 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
- 2018年度に改定した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

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、引き続き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

2018 年度の総合評価・2019 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　水田　正和

(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。

(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、2016 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、2019 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、2018 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、2019 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　2019 年度に発足する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推進体制の充実・強化

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

2018 年度の総合評価・2019 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、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）と連携しつつ、情報セキュリティ対策を実施してきているところ。

昨今、メールやウェブを経由し政府機関等を狙ったサイバー攻撃（標的型攻撃、ＤＤｏＳ攻撃、メールの大量送付、アプリケーションの脆弱性を悪用した攻撃等）は、対象や手法の多様化、規模の拡大の様相を呈しているところ。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。

2018 年度においては、2018 年７月に実施された統一基準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。

2019 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、2018 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、2018 年度に引き続きセキュリティ対策を維持・向上
(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) 人材・育成計画に基づく取組の継続によるセキュリティ・IT 人材の確保・育成
(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

国土交通省

2018 年度の総合評価・2019 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　栗田　卓也

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、2020年東京オリンピック・パラリンピック競技大会等に向けて、これらは、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、2018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「政府機関等の情報セキュリティ対策のための統一基準群」の改定を受け、国土交通省情報セキュリティポリシーを改定。また、情報セキュリティインシデント発生時の対処を適切に実施するため、「情報セキュリティインシデントの報告及び対処手順」を改定

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手続を設定

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）に参加

⑥国土交通省のメール・インターネット接続機能等に用いる情報システムの情報セキュリティ対策を強化

⑦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、鉄道、物流）の情報共有体制である交通ISAC（仮称）の創設の支援、空港分野の重要インフラ分野への追加、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配布等を実施

2019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セキュリティIT人材の確保・育成、②情報セキュリティに関する教育、③情報セキュリティ対策の自己点検、④情報セキュリティ監査、⑤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、⑥国土交通省情報セキュリティポリシーに基づく規程の改定等を推進する。

環境省

2018 年度の総合評価・2019 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　鎌形　浩史

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み、政府機関をはじめとする組織内部の情報窃取に対する脅威が継続している。また、2020年東京オリンピック・パラリンピック競技大会の開催に向け、今後さらなる攻撃の増加が懸念されるところ、サイバー攻撃は、行政事務従事者だけでなく外部委託先も含めて対象となることから、サプライチェーン全体における情報セキュリティ対策は重要な課題となっている。このような脅威に対し、環境省では、「侵入を前提とした多層防御」による『システム的対策』と、情報資産の紛失等の人為的なミスや外部委託先に対する管理の強化といった『人的対策』について、それぞれ取組を継続しているところである。

2018年度においては、「政府機関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日改定、サイバーセキュリティ戦略本部決定）に基づき、「環境省情報セキュリティポリシー」（以下、「ポリシー」という）の改定を行った。また、2018年度の情報セキュリティ教育では、e-ラーニングを通じて当該ポリシーの改定内容の浸透を図るとともに、集合研修や標的型メール訓練等によって、実践的な対策レベルの底上げを図った。さらに、自己点検における省内の情報システムの対策状況の調査や、各種監査における指摘事項への対応に加え、新たに省内でのクラウドサービスの利用実態を調査し、潜在するリスクの把握に努めた。

2019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。2018年度の取組の結果を踏まえて取組内容を見直しつつ、教育等の対策を効果的に推進するとともに、情報セキュリティ監査や自己点検の結果等に基づき、情報セキュリティ対策を総合的に改善、強化していく。

また、2018年度に検討を開始した次期システム更改に向け、働き方改革及び人材の多様化の支援等を推進するため、情報通信技術の活用、更にはAIやIoTを始めとする新技術の利活用の可能性を視野に入れ、業務効率化、柔軟性の確保と利便性の向上を図りつつ、十分なセキュリティを確保する等、時代の変化に合わせた新たな取組にも努めることとする。

防衛省

2018 年度の総合評価・2019 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・自衛隊としても、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、2018年度においては、サイバー防衛隊の体制強化、最新技術の研究、サプライチェーン・リスク対策等、様々な観点から能力を強化するため、主に以下の取組を行った。

○サイバー防衛隊の体制強化（約40名の増員）
○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の整備に関する研究
○人工知能のサイバーセキュリティへの応用に関する調査研究
○サプライチェーン・リスク対策として、調達仕様書に係る関連規則の整備

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、情報システムの利用環境等に関する重点検査及び職員に対する所持品検査等を実施し、情報セキュリティ対策が適切に取られていることを確認した。また、2019年２月の防衛省情報セキュリティ月間においては、重点テーマを「不審メールへの対処能力の向上～ 私はだまされない！ ～」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。

2019年度においては、2018年12月に策定された新たな防衛計画の大綱及び中期防衛力整備計画に基づき、①サイバー防衛隊等の拡充、②相手方によるサイバー空間の利用を妨げる能力の保持、③ 専門教育課程の拡充など優秀な人材の計画的な育成等、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、2018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２　2018 年度のサイバーセキュリティ関連施策の実施状況（一覧表）

＜別添２－目次＞

1. 経済社会の活力の向上及び持続的発展 133
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 133
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 136
1.3. 安全な IoT システムの構築 139
2. 国民が安全で安心して暮らせる社会の実現 141
2.1. 国民・社会を守るための取組 141
2.2. 官民一体となった重要インフラの防護 147
2.3. 政府機関等におけるセキュリティ強化・充実 156
2.4. 大学等における安全・安心な教育・研究環境の確保 161
2.5. 2020 年東京大会とその後を見据えた取組 162
2.6. 従来の枠を超えた情報共有・連携体制の構築 164
2.7. 大規模サイバー攻撃事態等への対処態勢の強化 166
3. 国際社会の平和・安定及び我が国の安全保障への寄与 168
3.1. 自由、公正かつ安全なサイバー空間の堅持 168
3.2. 我が国の防御力・抑止力・状況把握力の強化 171
3.3. 国際協力・連携 176
4. 横断的施策 181
4.1. 人材育成・確保 181
4.2. 研究開発の推進 187
4.3. 全員参加による協働 191
5. 推進体制 193

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、2016 年に決定した「企業経営のためのサイバーセキュリティの考え方」及び 2018 年に決定した「サイバーセキュリティ人材育成取組方針」を踏まえ、関係府省庁と協力し、サイバーセキュリティ対策の推進に関する以下の取組を行う。 ・サイバーセキュリティ対策について経営層が果たすべき役割、持つべき認識についての考え方の共有を図るため、「企業経営のためのサイバーセキュリティの考え方」の見直しを検討する。 ・サイバーセキュリティ対策の取組を分かりやすく表現・普及するため、マークやスローガンなどのツールについて検討を行う。 ・サイバーセキュリティ対策に関して、経営層が果たすべき役割・認識について、経営層の視点で、経営層自身に分かりやすく説明する人材、いわゆる伝道師の発掘と派遣や産業界と連携した経営層向けのセミナーについて検討を行う。	・内閣官房において、サイバーセキュリティに対する経営層の意識に関する調査を行うとともに、産業界による経営層向けのセミナー等の取組に積極的に協力を行った。
(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・システムに関する議論の中で、「守り」のリスク管理の一環として、サイバーセキュリティ対策を位置付け、コーポレート・ガバナンス・システムに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付けることを検討する。	・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・ガバナンス・システムに関する実務指針（仮称）にサイバーセキュリティ対策の在り方を盛り込む方向でドラフト版を作成した。なお、CGS 研究会（第２期）における議論を踏まえ、グループガバナンスの在り方に関するガイドラインを 2019 年６月に策定する予定。
(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の経営層の関与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、実効性評価の中にサイバーセキュリティへの経営層の関与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、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。	・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。
(オ)	内閣官房	内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。	・2018 年 10 月に、法律家を中心とした有識者から構成される「サイバーセキュリティ関連法令の調査検討等を目的としたサブワーキンググループ」を立ち上げた。本サブワーキンググループは、サイバーセキュリティ関係法令集の策定を目的の１つとしているものであり、2019 年２月に第一回会合を開催した。

(2) サイバーセキュリティに対する投資の推進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	経済産業省	経済産業省において、「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るために、具体的な対策事例や情報共有活動事例等を示すプラクティスを作成する。また、企業がどの程度サイバーセキュリティ対策を実施するかの目安として活用できる可視化ツールを作成する。	・経済産業省において、IPA に設置した、サイバーセキュリティ経営プラクティス検討会により、サイバーセキュリティ経営ガイドラインの具体的な実施事例等を示す、「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」をとりまとめ、公開した。また、本検討会において、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ための方向性について議論を行った。
（イ）	総務省	総務省において、ベストプラクティスも盛り込んだ「セキュリティ対策情報開示ガイドライン」（仮称）を策定、公表する。	・2017 年 12 月に、タスクフォースの下に「情報開示分科会」を設置し、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、その普及に必要な方策について検討を行い、その結果をとりまとめ、2018 年 6 月に情報開示分科会報告書として公表した。同報告書を踏まえ、2018 年度に企業のサイバーセキュリティ対策に関する情報開示を行うに当たって参照可能な手引きの策定に着手した。なお、手引きの策定・公表は 2019 年度早期を予定。
（ウ）	経済産業省	経済産業省において、一定のセキュリティ品質を有するセキュリティサービスを審査登録する体制を整備することにより競争力強化や活用促進を図るなど、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・向上するために実施すべき取組を定義した「情報セキュリティサービス基準」を策定した。本基準に適合するサービスの台帳を IPA より公表した（情報セキュリティサービス審査登録制度）。また、補助金や政府調達等から本台帳の利用を推奨することで、情報セキュリティサービスの活用促進を行った。
（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。	・説明会等を通じてコネクテッド・インダストリーズ税制の周知を行い、活用を促進した。
（オ）	経済産業省	経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。	・経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、2018 年度補正予算により、中小企業向けのサイバーセキュリティに関する相談窓口（サイバーセキュリティお助け隊）の構築に向け、全国で実証事業を行うこととした。実証により、中小企業の実態を明らかにした上で、中小企業が利用しやすいサイバーセキュリティ支援体制やサイバー保険について検討し、普及を図る。
（カ）	総務省	総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。	・総務省において、関係者間のサイバーセキュリティに関する情報開示・共有を促進するための仕組みの構築について検討を行った。

(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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、組織における内部不正防止のためのガイドラインや営業秘密保護ハンドブックの普及推進を図る。	・経済産業省において、IPA を通じて、 ・営業秘密保護に関する官民連携フォーラムにおける情報共有のため、フォーラム参加 29 組織（83 メールアドレス）に向けたメールマガジンを 2018 年度 12 回発行し、営業秘密保護に関する最新情報を提供したほか、セミナー等で４回講演し、普及促進を図った。 ・営業秘密保護ハンドブックの改訂を見据え、「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を実施し、2019 年４月に報告書を公開した。
（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～」及び「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～」についての普及啓発を図る。	・経済産業省において、「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～」を、HP や講演において周知した。
（ウ）	総務省 経済産業省	総務省及び経済産業省において、「クラウドサービス提供における情報セキュリティ対策ガイドライン」、クラウドセキュリティ監査制度等の普及促進を行う。	・総務省において、クラウド事業者が IoT サービスを提供する際のリスクへの対応方針を取りまとめ、2018 年７月 31 日、IoT サービスリスクへの対応方針等の掲載した「クラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）」を公表した。 ・また、経済産業省において、クラウド事業者の参加するセミナー、企業の経営者やセキュリティ担当者向けの講演において、JASA のクラウドセキュリティ・マーク（CS マーク）やクラウドセキュリティ認証の取得に向けて呼びかけを行うなど、普及・促進を図った。
（エ）	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）を設置する。	・経済産業省において、2018 年６月に IPA と連携して、コラボレーション・プラットフォームを立ち上げ、１～２か月に１度の頻度で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。
（オ）	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・サービスの有効性検証、レーティングを実施できる環境を整備するための検討を行う。	・経済産業省において、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、市場で流通させるための有効な施策についてサイバーセキュリティ分野への有識者ヒアリング等も含めた調査を行い、有効性検証やレーティング等の在り方について検討を行った。

（カ）	経済産業省	経済産業省において、IPA を通じ、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況などの実態と動向を把握するための調査・分析を行うとともに、組込みソフトウェアが組み込まれた製品やシステム開発の高信頼化を目的として、システムアプローチによる安全性解析手法の開発・セキュリティ分析手法の検討、コーディング規約策定及びそれらの普及を図る。	・経済産業省において、IPA を通じて、 ・IoT 機器、サービスを支える組込みソフトウェア産業の高度化に向けて、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況などの実態と動向を把握するための調査・分析を行い、結果を 2019 年３月に公開した。 ・組込みソフトウェア開発向けコーディング作法についてガイドをまとめるとともに、コーディング規約の重要性について普及展開を図った。また、安全性解析手法 STAMP の導入を容易にするモデリングツールを用いたハンズオンセミナーを行い、システムアプローチによる安全性解析手法の普及展開に努めた。
（キ）	経済産業省	経済産業省において、ASEAN をはじめとした新興国に対し、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。	・ベトナム、バングラデシュにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入のため、企画・計画段階から現地の電力企業への支援を実施した。また、カンボジア、ラオス、ミャンマーにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入に向けた理解を醸成するため、現地の電力企業向けに研修を実施した。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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に設置した WG1(制度・技術・標準化)において、Society5.0 の実現に必要なセキュリティ対策を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定する。また、産業分野毎に設置した SWG における検討を通じて、産業分野毎に守るべきもの・リスク・必要な対策について整理する。	・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に設置した WG１(制度・技術・標準化)を中心に、Society 5.0 の実現に必要なセキュリティ対策の全体像を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進め、2018 年４月と 2019 年１月の二度のパブリックコメントを実施した。本フレームワークは、パブリックコメントで寄せられた意見を踏まえて、2019 年度当初に公表する予定である。 また、ビル、電力、防衛、スマートホームの各分野について SWG を設置して、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を進めた。特に、ビル分野においては「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」を 2019 年３月に取りまとめ、パブリックコメントを実施した。
（イ）	経済産業省	経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、リスクの高い丸投げ下請や多様化するセキュリティ対策費用の増加に応じた適切な価格設定に向け、セミナー等を通した下請ガイドラインの更なる浸透を図るとともに、業界団体と連携したフォローアップなどを実施し、情報システム開発・運用に係る取引の適正化を図る。	・経済産業省において、 ・下請中小企業振興法の振興基準の改訂に伴い、下請ガイドラインについて業界団体と連携して、必要な見直しを実施。 ・セミナー等における周知や自主行動計画のフォローアップを行う等、取引適正化に向けた取組を実施。

(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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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 機器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、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。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。	・関係省庁と連携し、技術開発から実証実験、認証制度検討、グローバル協調にわたる総合的な研究開発計画を立案した。 ・研究開発計画に基づき公募により研究開発機関を決定し、概念設計を行う等研究開発を開始した。
（イ）	経済産業省	経済産業省において、業界横断的な指針及び産業ごとの対策を整理した上で、セキュリティ対策が講じられているかどうかを確認するための、認証を含む確認の仕組みを検討する。	・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に設置した WG１（制度・技術・標準化）を中心に、Society 5.0 の実現に必要なセキュリティ対策の全体像を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進め、2018 年４月と 2019 年１月の二度のパブリックコメントを実施した。本フレームワークは、パブリックコメントで寄せられた意見を踏まえて、2019 年度当初に公表する予定である。 また、ビル、電力、防衛、スマートホームの各分野について SWG を設置して、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を行うとともに、認証を含む確認の仕組みについて調査を行った。

(3) 中小企業の取組の促進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、中小企業における実態を踏まえつつ、IT やセキュリティの知識がなくとも理解できるような対策集の作成に向けた取組を行う。	・関係機関との連携の下、「小さな中小企業と NPO の情報セキュリティハンドブック」を取りまとめた。
（イ）	総務省	総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。（再掲）	・総務省において、関係者間のサイバーセキュリティに関する情報開示・共有を促進するための仕組みの構築について検討を行った。
（ウ）	経済産業省	経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。（再掲）	・経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、2018 年度補正予算により、中小企業向けのサイバーセキュリティに関する相談窓口（サイバーセキュリティお助け隊）の構築に向け、全国で実証事業を行うこととした。実証により、中小企業の実態を明らかにした上で、中小企業が利用しやすいサイバーセキュリティ支援体制やサイバー保険について検討し、普及を図る。

（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、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」の普及を図るとともに、「中小企業の情報セキュリティ対策ガイドライン」をより利用し易い内容に改訂を行い 2018 年度３月末に改訂版を公開した。
（オ）	経済産業省	中小企業における情報セキュリティ投資を促進するため、経済産業省において、以下の取組を実施する。 ・中小企業等の生産性向上に資する IT 導入の促進とあわせて、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。 ・認定された IT ベンターに対してサイバーセキュリティの情報提供などを実施するとともに、当該 IT ベンダーが取り組むセキュリティ対策に関する情報を中小企業向けに開示する仕組みの構築を進める。 ・財政投融資制度において、中小企業で導入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、特別利率による融資を実施する。	［経済産業省］ ・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 ベンダー等の「クラウドサービスの安全・信頼性に関する情報」、「セキュリティ対策状況」、「利用者のサポート体制」、「利用終了時のデータの取扱い」等を確認し、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当該情報を開示する仕組みを構築した。 ・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開始するなど支援策を強化した。 ［総務省］ ・説明会等を通じてコネクテッド・インダストリーズ税制の周知を行い、活用を促進した。
（カ）	経済産業省	経済産業省において、IPA を通じ、中小企業における情報セキュリティ教育担当者や中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ講習講師養成セミナー」を実施するとともに、中小企業団体、関係機関等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施する。さらに、IPA が 2017 年度に創設した、対策ガイドラインに基づき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「SECURITY ACTION」への登録を促すことで、中小企業のセキュリティレベルの向上、IPA 等の作成する啓発資料や情報セキュリティ対策支援サイト等のツール等の利用促進等を図る。	・経済産業省において、IPA を通じ、 ・「講習能力養成セミナー」を全国 21 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 1,150 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 63 箇所に講師を派遣し、3,801 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、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を紹介する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ー数が累計 81,400 名に増加した。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。さらに着実にこの考え方に基づく取組が行われているか適時確認をする。	・「サイバーセキュリティ関係施策に関する平成 31 年度予算重点化方針」（平成 30 年 7 月 25 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、自律的な IoT システムに係る関係省庁の取組を推進するとともに、各主体が協働できるよう情報共有等の取組を推進する。その際、各主体の間で共通認識や役割の明確化を図るため、「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」を踏また取組（IoT の分野個別の課題だけでなく、その範囲や定義、物理安全対策、責任分界点（既知の脆弱性への対応に関する製造者責任や運用者等の安全管理義務などインシデント発生時における関係者の責任を含む）やプライバシーの問題などの共通課題の検討を含む。）を推進する。	・「安全な IoT システムのためのセキュリティに関する一般的枠組」を踏まえ、2018 年４月に関係省庁との会合、2018 年８月にサイバーセキュリティ 第 192 委員会での講演を行うなど、各主体間での共通認識の醸成と情報共有を促進した。また、各省庁の 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、経産省　産業サイバーセキュリティ研究会など）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。 ・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 JTC1/SC27、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。 ・総務省及び経済産業省において、IoT 推進コンソーシアムを通じて、IPA 及び NICT と連携しつつ、「IoT セキュリティガイドライン」を様々な産業分野の標準仕様等に反映させるべく、普及展開に努めるとともに、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、「IoT セキュリティガイドライン」の考え方の基本となった「つながる世界の開発指針」、又はその他関連ガイド等を様々な産業分野や団体の標準仕様等に反映させるべく、引き続き提案活動を実施する。また「IoT セキュリティガイドライン」を基本とする考え方の国際標準化に向けた取り組みを進める。 ・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）の下に設置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）の場を活用して、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、JTC 1/SC 27 においては ISO/IEC 27030 の作業文書(WD)第二版が発行された。ITU-T SG17 においては、勧告案 X.sc-iot として 2018 年９月より勧告化の検討を開始した。 ・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 を通じて、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた取組を推薦するために、総務省、経産省及び業界団体でそれぞれ取り組むべき事項を、「IoT 機器のセキュリティ対策に関する検討の方向性」として取りまとめた。 ・経済産業省において、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下に設置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、機器製造業者、電力事業者、住設機器製造業者、建設事業者などの多岐に渡るステークホルダーと連携して、家庭で使用される IoT 機器のサイバーセキュリティの確保に求められるセキュリティ対策の方向性について検討を行った。 ・経済産業省において、IPA を通じて、「IoT セキュリティガイドライン」の考え方の基本となった「つながる世界の開発指針」及び関連ガイドを様々な産業分野の標準仕様等に反映させるべく、一般社団法人組込みシステム技術協会（JASA）、一般社団法人 IT 検証産業協会（IVIA）などの業界団体・組織が運営するシンポジウムや委員会等において普及展開を実施。さらに 2019 年２月には地域団体とも連携してセミナーを開催し、地域への普及を図った。

（エ）	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」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。	・IoT システムの設計・開発・運用等に係る概念について、国内において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、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。2018 年５月の独ベルリン会合、11 月の横浜会合にて作業原案を提案する等し、国際標準化に向けたプロセスを進めた。

(2) 脆弱性対策に係る体制の整備

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、サイバー環境をよりクリーンなものに保つため、官民が連携して「ボット撲滅」に向けた体制を構築し対策を推進するための検討を行う。	[NISC] ・内閣官房において、官民連携の枠組みとして、2018 年２月に開催した関係省庁及び民間も含めた関係者会合の結果を踏まえ、2019 年２月より同会合の関係者との意見交換を行い、実態を把握するとともに体制等についての検討を行った。 [警察庁] ・警察庁において、ボット対策を含むサイバー犯罪対策について講演を行った。 [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 を通じて、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた取組を推薦するために、総務省、経産省及び業界団体でそれぞれ取り組むべき事項を、「IoT 機器のセキュリティ対策に関する検討の方向性」として取りまとめた。
（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を通じて、IPA 及び NICT と連携しつつ、「IoT セキュリティガイドライン」を様々な産業分野の標準仕様等に反映させるべく、普及展開に努める。	・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 を通じて、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた取組を推薦するために、総務省、経産省及び業界団体でそれぞれ取り組むべき事項を、「IoT 機器のセキュリティ対策に関する検討の方向性」として取りまとめた。 ・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 2019 年３月に公布した。

（ウ）	総務省	総務省において、NICT を通じ、パスワード設定に不備のある機器の調査を行い、電気通信事業者の協力の下、当該機器の利用者を特定し、設定変更を促す取組を行う。また、「IoT セキュリティ総合対策」を踏まえ、2018 年度中に IoT 機器に対する脆弱性対策に関する実施体制を整備する。	・総務省において、IoT 機器等を悪用したサイバー攻撃の深刻化を踏まえ、2018 年５月に改正された国立研究開発法人情報通信研究機構法に基づき、2019 年２月より 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、電気通信事業者が用者への注意喚起を行う取組「NOTICE※」を実施。 ※ National Operation Towards IoT Clean Environment ・NOTICE の実施にあたっては、専用のサポートセンターを立ち上げ、ウェブサイトや電話による問合せ対応を通じて利用者に適切なセキュリティ対策等を案内。消費生活センター等とも連携して対応。 ・IoT 機器のセキュリティ対策の必要性、本取組の内容の広報のため、公共機関等でのポスター掲示に加え、新聞広告、交通広告等を実施。

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

(1) 安全・安心なサイバー空間の利用環境の構築

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、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。2018 年度においては、ソフトウェア製品の届出 325 件、ウェブアプリケーションの届出 223 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、202 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、2018 年度においては、脆弱性対策情報を 15,921 件（累計：97,444 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、情報システム等の国際的な安全性確保に寄与する。	・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 を通じて、ソフトウェア等の脆弱性に関する情報を、マネジメント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、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び脆弱性マネジメント支援を実施する。	・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 形式および 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および更新の通知を、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技術の普及・啓発活動を行う。	・経済産業省において、IPA を通じ、普及・啓発活動として、情報セキュリティ EXPO での講演及び「ファジング入門セミナー」の開催を実施した。

（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 を通じてフィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組等を実施する。	・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。2018 年度は、2019 年２月末現在で約５千(5174)のフィッシングサイト閉鎖の対応を行った。そのうち 69%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、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、IPA セミナー「脆弱性対策の効果的な進め方」、各種講演等で icat の紹介を行い、icat サービスの普及促進を図った。また、icat の利用サイト数は 1,161 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。	・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、2018 年度のダウンロード数は 3,361 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、「安全なウェブサイトの作り方」を引き続き公開するとともに、体験的かつ実践的に学ぶツール「AppGoat」について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」の継続公開および、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」の公開を実施した。また、AppGoat V3.0 を活用した脆弱性対策の普及方法について検討し、2019 年度に高等専門学校の教員向け講習を行い、授業を通じた普及啓発を推進することとした。
（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、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、2018 年度は、経済発展に伴いソフトウエア開発の分野でも存在感の増しているインドネシアでアンドロイドセキュアコーディングセミナーを実施した。
（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	総務省において、2018 年５月に成立した電気通信事業者間のサイバー攻撃に関する情報共有の促進のための制度整備を含む「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」を踏まえ、その施行に向けた省令等の整備を行う。	・総務省において、2018 年５月に成立したサイバー攻撃に関する電気通信事業者間の情報共有の促進のための制度整備を含む「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」を踏まえ、その施行に向けた省令等の整備を行った。具体的には、一般社団法人 ICT-ISAC から認定送信型対電気通信設備サイバー攻撃対処協会の認定申請を受け、同団体に対し、認定を行った。
（シ）	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。	・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（SPF、DMARC）の導入状況を公表している。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ス）	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、情報通信ネットワークの変化、新たなサービス提供に伴い社会・経済に生じ得るリスク源を評価するとともに、情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等について調査を行う。	・経済産業省において、IoT 製品の普及が進展する中で、IoT 製品が抱える脆弱性とその脅威を検知する手法について調査を行った。また、ソフトウェアを利用した製品・サービスの安全・安心を確保するために、OSS を含むソフトウェアを安心して利活用するための課題を明確にするための調査を行った。
（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	重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、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］ ・制度的な枠組みに関する状況の把握に努め、人的要因によるリスクに関しては、事業者等へのヒアリング等調査を実施した。 ・安全基準等の浸透状況調査を実施し、重要インフラ所管省庁や業界団体等が定める安全基準等が、重要インフラ事業者等にどの程度浸透しているかを把握し、その結果を 2019 年４月の重要インフラ専門調査会に報告した。 ・安全基準等の改善状況等の調査を行い、重要インフラ所管省庁及び重要インフラ事業者等が、本行動計画期間の指針改定やサイバー攻撃の動向、IT に係る環境変化の調査・分析結果等を受けて、安全基準等の継続的な改善に取り組んでいることを把握し、その結果を 2019 年４月の重要インフラ専門調査会に報告した。 ［金融庁］ ・金融庁においては、「サイバーセキュリティ戦略」の改訂（2018 年７月）等を踏まえ、2018 年 10 月、「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」をアップデートし、公表した。 ・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）」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「放送設備に関するサイバーセキュリティガイドライン」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。 ［厚生労働省］ ・水道分野については、2018 年度末に水道分野における安全基準である「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）を策定し、水道事業者等に通知した。 ・医療分野については、厚生労働省において、医療機関等におけるサイバーセキュリティ対策の現状について調査を行い、2018 年 10 月に医療情報システムの安全管理に関するガイドラインの周知徹底やサイバーセキュリティ事案発生時に医療法に基づき都道府県等が立ち入り検査を実施できること等に関して都道府県に対し通知した。 ［経済産業省］ ・ガス分野については、サイバーセキュリティ対策をガス事業法における保安規則として位置付けるべく、ガス事業法施行規則を改正した。 ［国土交通省］ ・国土交通省において、国土交通省所管の重要インフラ分野（航空、空港、鉄道、物流）における「情報セキュリティ確保に係る安全ガイドライン」の改訂を行い、事業者への周知・浸透を図るとともに、国土交通省のウェブサイトに掲載した。

（ソ）	金融庁	金融庁において、仮想通貨交換業者におけるサイバーセキュリティの強化に向け、認定された自主規制団体との意見交換等を通じて、実効性ある自主規制機能の確立を促していく。	・金融庁において、2018 年 10 月、一般社団法人日本仮想通貨交換業協会を資金決済法に基づく認定資金決済事業者協会として認定した。当協会においては、システムリスク管理の内容を含む自主規制規則を定めており、各暗号資産交換業者における規則の遵守態勢等について指導等を行っている。金融庁では、定期的な意見交換等を通じて、自主規制団体の上記のような取組による自主規制機能の確立を促している。
（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主導するとともに、基準適合性に係る審査体制の構築を図る。	・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下に参画し、2019 年１月の自動運転専門分科会に基準案を上程した。また、交通安全環境研究所において、国際基準に基づく審査の実施に必要な知見の収集を行う等、審査の円滑な実施に向けた検討を進めた。
（チ）	経済産業省 国土交通省	経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクへの対応に向けて、2018 年度中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、2019 年度以降、人材育成等に活用する。	・経済産業省及び国土交通省において、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）の構築に関して、予定通り終了した。
（ツ）	内閣府	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、2017 年度に作成したセキュリティ評価ガイドライン案を踏まえ、実証実験を実施する。	・2017 年度に作成したセキュリティ評価ガイドライン案に基づき、実機を用いたセキュリティ評価の実証実験を実施することにより、セキュリティ評価ガイドライン（案）を策定した。
（テ）	内閣官房	様々な用途への活用が進むドローンのサイバーセキュリティについて、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」等の場において、「空の産業革命に向けたロードマップ 2018～小型無人機の安全な利活用のための技術開発と環境整備～」（2018 年６月小型無人機に係る環境整備に向けた官民協議会決定）に基づき、空の産業革命に向けた総合的な検討の一環として論点整理を行う。	・ドローンのサイバーセキュリティについて、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」の場においては、「空の産業革命に向けたロードマップ 2018～小型無人機の安全な利活用のための技術開発と環境整備～」（2018 年６月小型無人機に係る環境整備に向けた官民協議会決定）に基づき、空の産業革命に向けた総合的な検討の一環として論点整理を行っているところ。

(2) サイバー犯罪への対策

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、スマートフォン等の情報端末や 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 等に関連した犯罪の被害防止を図るため、保護者向けのリーフレットを 2019 年１月に作成し、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、仮想通貨や 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！」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、警察庁における各種サイバーセキュリティ関連施策を広報した。 ・都道府県警察等において、教育機関関係者、地方公共団体職員、インターネットの一般利用者等を対象とした講演等を実施し、情報セキュリティに関する意識・知識の向上を図った。特に、2019 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、事業者団体に対する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の公表等を通じ、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！」を活用し、官民連携した広報啓発活動を推進した。 ・2018 年中の不正アクセス行為の発生状況等を 2019 年３月 22 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、2018 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、2018 年末現在の全国のサイバー防犯ボランティア数は、244 団体 9,022 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)	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・研修センターを通じ、サイバー犯罪等の取締りのための情報技術の解析に関する研究及びサイバー犯罪等の取締りに必要な専門的知識・技術に関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した。

（オ）	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強化、関係会合への参加、技術協力を通じた関係機関との協力、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。 ・高度情報技術解析センターを中心として、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、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、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した。（再掲） ・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。
（カ）	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・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。	・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。
（キ）	法務省 警察庁	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。
（ク）	総務省	総務省において、NICT を通じ、能動的・網羅的なサイバー攻撃観測技術の開発に取り組むとともに、運用するサイバー攻撃観測網（NICTER）における観測・分析結果を NISC をはじめとする政府機関等への情報提供等を通じた連携強化を図る。	・NICT を通じ、能動的・網羅的なサイバー攻撃観測技術の開発に取り組むとともに、運用するサイバー攻撃観測網（NICTER）における観測・分析結果を NISC をはじめとする政府機関等への情報提供等を通じた連携強化を行った。
（ケ）	経済産業省	経済産業省において、産業界及び関係省庁と連携し、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、「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。
（コ）	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、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を強化する。	・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。
（サ）	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政策会議等において官民連携による取組を推進する。	・都道府県警察において、JC3 を通じて企業等とサイバー空間の脅威への対処に関する情報を共有したほか、不正作成ＩＤの流通阻止に向けた官民連携による犯罪インフラ対策や、クレジットカードの不正利用に係る不正宿泊対策を実施した。 ・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。

(シ)	経済産業省	経済産業省において、フィッシング詐欺被害の抑制のため、フィッシング対策協議会を通じて、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を行う。	・経済産業省において、2018 年度は米国 APWG が５月に主催した APWG eCrime 2018 （サンディエゴ）に参加し、日本のフィッシング状況について発表するとともに、海外のフィッシング関連の状況や動向について情報収集を行った。 また、フィッシング対策協議会の技術・制度検討ワーキンググループにおいて、フィッシング対策ガイドラインやフィッシングレポートの改訂（2019 年度第１四半期中に公開予定）を進めた。
(ス)	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、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、必要な対策を行った。
(セ)	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

新戦略（2018 年７月 27 日閣議決定。2018 年７月～2021 年７月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	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	内閣官房	内閣官房及び重要インフラ所管省庁等において、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の５つの施策を実施する。 「安全基準等の整備及び浸透」については、重要インフラ各分野に横断的な指針の策定とそれに基づく、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、連絡形態の多様化や共有情報の明確化等による官民・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」については本項目、(ス)・(ソ)及び 2.1(1)（セ）、「情報共有体制の強化」については(コ)・(テ)、(2)(ア)及び 2.6(ア)、「障害対応体制の強化」については(ト)、「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」については本項目及び(ク)に取組の詳細を記載）。 ・「安全基準等」の整備を支援するため策定した「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）」について、2019 年１月の重要インフラ専門調査会において、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指針の改定について方向性の承認を得た。 ・広報広聴活動として、第４次行動計画について、重要インフラ事業者等を対象とした講演等を開催し、重要インフラ事業者等のセキュリティに対する意識向上を図った。

（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、地方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、2018 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27 か所を 2018 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の整備を目的とする「割賦販売法の一部を改正する法律（平成 28 年法律第 99 号）」の成立を受け、2017 年 12 月に改正政省令を公布し、2018 年６月に改正法を施行する。また、クレジットカード取引に関係する事業者等で構成されているクレジット取引セキュリティ対策協議会において、改正法の実務上の指針として、2018 年３月に改訂された「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-2018-」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）」が施行し、同法が実務上の指針と位置付けるクレジット取引セキュリティ対策協議会（事務局：一般社団法人日本クレジット協会）の「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」について 2019 年３月１日に改訂した。本実行計画に基づき、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、「未来投資戦略」等に基づき、保健医療記録共有サービスを 2020 年度から本格稼働させることを目指す中で、ネットワークや医療機関のセキュリティ対策強化について、コスト負担のあり方も含めて調査・検討する。	・厚生労働省において、「未来投資戦略」等に基づき、全国的な保健医療情報ネットワーク等のセキュリティ対策に関する調査事業を実施した。
（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・普及について一層推進していく。	・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。	・2018 年４月 24 日に医療セプターを代表し、公益社団法人日本医師会がセプターカウンシルに加盟した。 ・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）を発出し、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	スマートメーターシステムセキュリティガイドラインに基づき電力各社が取組を強化している中で、　経済産業省において、スマートメーターのセキュリティを含め電力会社を取り巻く情勢を分析し、課題の抽出及び必要な対策を検討すべく、新たに有識者が参画する専門の研究会(電力サブワーキング)を立ち上げる。	・経済産業省において、2018 年６月、電力分野のサイバーセキュリティに関する今後の取組について検討を行うため、有識者が参画する電力サブワーキンググループを設置し、2018 年度中に４回開催した。
（ク）	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次行動計画に基づく施策を、中小事業者へ拡大すると共に、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。	・重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大など、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を用いて標的型攻撃の解析を実施する。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構築及び関係事業者等での情報共有の取組を促進する。	・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の構築及び関係事業者等での情報共有の取組を促進した。

（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、重要インフラ事業者等への情報提供を行った。また、同機関が分析した情報の横展開を行った。さらに、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。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（サ）	内閣官房	内閣官房において、重要インフラサービスを安全かつ持続的に提供できるよう、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、オリパラ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」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」をとりまとめ、2018 年４月に公表した。 ・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（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズした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、諸外国における「脅威ベースのペネトレーションテスト」の手法や金融機関の活用状況を把握するための外部委託調査を実施し、2018 年５月に「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」を公表した。 また、大規模な金融機関との建設的な対話において「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、３メガバンクグループを中心に同テストの活用が進められた。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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	重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、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] ・制度的な枠組みに関する状況の把握に努め、人的要因によるリスクに関しては、事業者等へのヒアリング等調査を実施した。 ・安全基準等の浸透状況調査を実施し、重要インフラ所管省庁や業界団体等が定める安全基準等が、重要インフラ事業者等にどの程度浸透しているかを把握し、その結果を 2019 年４月の重要インフラ専門調査会に報告した。 ・安全基準等の改善状況等の調査を行い、重要インフラ所管省庁及び重要インフラ事業者等が、本行動計画期間の指針改定やサイバー攻撃の動向、IT に係る環境変化の調査・分析結果等を受けて、安全基準等の継続的な改善に取り組んでいることを把握し、その結果を 2019 年４月の重要インフラ専門調査会に報告した。 [金融庁] ・金融庁においては、「サイバーセキュリティ戦略」の改訂（2018 年７月）等を踏まえ、2018 年 10 月、「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」をアップデートし、公表した。 ・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）」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「放送設備に関するサイバーセキュリティガイドライン」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。 [厚生労働省] ・水道分野については、2018 年度末に水道分野における安全基準である「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）を策定し、水道事業者等に通知した。 ・医療分野については、厚生労働省において、医療機関等におけるサイバーセキュリティ対策の現状について調査を行い、2018 年 10 月に医療情報システムの安全管理に関するガイドラインの周知徹底やサイバーセキュリティ事案発生時に医療法に基づき都道府県等が立ち入り検査を実施できること等に関して都道府県に対し通知した。 [経済産業省] ・ガス分野については、サイバーセキュリティ対策をガス事業法における保安規則として位置付けるべく、ガス事業法施行規則を改正した。 [国土交通省] ・国土交通省において、国土交通省所管の重要インフラ分野（航空、空港、鉄道、物流）における「情報セキュリティ確保に係る安全ガイドライン」の改訂を行い、事業者への周知・浸透を図るとともに、国土交通省のウェブサイトに掲載した。

（セ）	総務省	総務省において、ネットワーク IP 化の進展に対応して、ICT サービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。	・2017 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、2018 年９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、「情報通信ネットワーク安全・信頼性基準」等について、2019 年に改正を行った。
（ソ）	総務省 経済産業省	総務省及び経済産業省において、重要インフラ事業者等が保有する重要データがクラウドサービス等において適切に保護される仕組みの在り方について本年度中に国内外の実態調査を踏まえ技術面・法制度面から検討を開始する。	・総務省及び経済産業省が中心となり、有識者からなる「クラウドサービスの安全性評価に関する検討会」において、適切なセキュリティを満たすクラウドサービスを政府が導入するために必要な評価方法について議論を開始した。 ・重要産業分野等において当該検討会の安全性評価制度の評価結果の活用を推奨することを前提として検討を進めている。 ・当該検討会を年度内に合計６回開催し、中間とりまとめを行った。 ・重要インフラ 14 分野に対するデータの管理に関するヒアリングを行った。 ・2019 年１月の重要インフラ専門調査会において、「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」を追加する改定について方向性の承認を得た。
（タ）	厚生労働省	厚生労働省において、医療機関におけるサイバーセキュリティの現状について調査を行うとともに、医療情報システムの安全管理ガイドラインの普及に取り組む。	・厚生労働省において、医療機関等におけるサイバーセキュリティ対策の現状について調査を行い、2018 年 10 月に医療情報システムの安全管理に関するガイドラインの周知徹底やサイバーセキュリティ事案発生時に医療法に基づき都道府県等が立ち入り検査を実施できること等に関して都道府県に対し通知した。
（チ）	厚生労働省	厚生労働省において、医療機器のサイバーセキュリティ対策ガイドラインの策定等により、医療機器のサイバーセキュリティ対策を推進していく。	・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）を発出し、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。
（ツ）	経済産業省	経済産業省において、「ガス事業法」により、ガス事業者に作成と遵守が課せられる保安規程の規定事項に「製造・供給に係る制御システムのサイバーセキュリティ対策」を追加することについて具体化を図る。	・経済産業省において、ガス事業者に作成と遵守が課せられる保安規程の規定事項に製造・供給に係る制御システムのサイバーセキュリティ対策を加えた「ガス事業法施行規則（昭和 45 年通商産業省令第 97 号）」の改正を行い、2019 年１月に公布した。

新戦略（2018 年７月 27 日閣議決定。2018 年７月～2021 年７月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（テ）	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。 ・ サービス障害の深刻度評価基準の導入に向けた検討を進める。 ・ 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、情報共有システム構築に係る検討を行う。	・サイバーセキュリティ戦略本部において、重要インフラ専門調査会における調査審議を踏まえ、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を決定した。 ・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を構築し、収集した情報を取りまとめた。 ・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実施した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ト）	内閣官房 金融庁 総務省	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 ・内閣官房において、重要インフラ事業者等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 に組織した「ナショナルサイバートレーニングセンター」を通じ、重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための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。 ・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、攻撃の実例分析を踏まえた金融業界横断的なサイバーセキュリティ演習について、必要に応じて対象業態を拡充の上、引き続き実施する。	［NISC］ ・内閣官房において、2018 年 12 月 13 日、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施した。 ［総務省］ ・実践的サイバー防御演習（CYDER）について、2018 年度、重要インフラ事業者向けの B-3 コースを開講し、重要インフラ事業者等から 397 名が受講。 ［経済産業省］ ・経済産業省において、2018 年 7 月から、「産業サイバーセキュリティセンター」において、約 80 名の受講生を受け入れ、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育成を目的とした第２期「中核人材育成プログラム」を開講した。 ［金融庁］ ・金融庁において、2018 年 10 月に、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として、今回から新たな業態として拡充した FX 業者、仮想通貨交換業者を含めた金融機関 105 社が参加し金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）を実施。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ナ）	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。	・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 47 件(2019 年２月末時点)について、その保有組織に対して情報提供した。
（ニ）	経済産業省	経済産業省において、制御システムのテスト環境を用いシステム全体の脅威分析、リスク評価を行う技術開発を行う。	・経済産業省において、ビルの制御システムを例に、建物全体に分布する制御システム全体についてのインシデント分析、リスク源整理、セキュリティ対策の検討を行い、ビルに係わるステークホルダーの検討会により、ガイドライン案として取りまとめた。また、CSSC と連携し、ビルの制御システムテスト環境に通じたレビューを行い、サイバー対策技術の整理とガイドライン案のブラッシュアップを実施した。

（ヌ）	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、非制御系の情報共有体制と整合性のとれた情報共有体制により、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、実際に運用を行っている事業者等にヒアリングを行い、現場での取組状況を把握するとともに、どのような情報が事業者等にとって有益なのか調査を行った。 [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、15 件(2019 年２月末時点)である。
（ネ）	経済産業省	経済産業省において、海外におけるルール化の動向も踏まえ、サプライチェーンにおける脅威を明確化し、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を策定するとともに、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、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)を中心に、Society 5.0 の実現に必要なセキュリティ対策の全体像を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進め、2018 年４月と 2019 年１月の二度のパブリックコメントを実施した。本フレームワークは、パブリックコメントで寄せられた意見を踏まえて、2019 年度当初に公表する予定である。 また、ビル、電力、防衛、スマートホームといった重要産業分野について SWG を設置して、各産業における守るべきものやリスクに基づいたセキュリティ対策の検討を進めた。特に、ビル分野においては「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」を 2019 年３月に取りまとめ、パブリックコメントを実施した。

(2) 地方公共団体のセキュリティ強化・充実

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、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。 ・セプター事務局や地方公共団体を含む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実施した。（自治体 CSIRT 協議会が 2018 年 10 月設立） [総務省] ・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、LGWAN メールでの送信や LGWAN 上の情報セキュリティ支援サイトにおいて、情報セキュリティに関する解説等を提供した。 また、2018 年９月に「地方公共団体における情報セキュリティポリシーガイドライン」の改定を行った。

（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。また、マイナンバー制度における情報連携の状況等を踏まえつつ、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。	【集合研修実施状況】 （１）情報セキュリティ監査セミナー　年二回実施　受講者数 95 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 142 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 2018 年 7 月 18 日～2019 年 1 月 31 日 受講者数 363,151 名
（ウ）	総務省	総務省において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。	・地方公共団体における情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、LGWAN メールでの送信や LGWAN 上の情報セキュリティ支援サイトにおいて、情報セキュリティに関する解説等を提供した。 （実績:緊急連絡等 78 件、ニュース・メルマガ 49 件） ・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の発生もあることから、行政専用ネットワークである LGWAN メール以外での提供媒体(インターネット)の拡充を図った。
（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 の連携組織を設立し、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。 ・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:11 県地域、165 団体が参加） ・2018 年 10 月に、自治体 CSIRT 協議会を立ち上げ、技術講習会や緊急時対応訓練を行った。 （実績） 技術講習会：88 団体 緊急時対応訓練：22 団体

（オ）	内閣官房 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、「自治体情報セキュリティ向上プラットフォーム」の利用を促進することにより、マイナンバー制度を含めたセキュリティ確保を徹底する。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、インターネットから独立する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］ ・総合行政ネットワーク（LGWAN）については、集中的にセキュリティ監視を行う LGWAN-SOC を 2017 年２月に構築し、政府共通ネットワークとの通信を監視している。また、2018 年度に LGWAN の更改を実施し、LGWAN 内の全ての通信について LGWAN-SOC による監視を開始したところ。 ・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ついては、総務省において毎年度実施している「地方自治管理概要」の調査項目として新たに追加して、調査を実施した。2018 年 10 月から、地方公共団体の LGWAN 端末に OS やウィルス対策ソフトの更新情報を提供した。 2018 年度「自治体情報セキュリティ向上プラットフォーム」利用団体数：420 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、2018 年度においても、安定的に運用を行った。 ［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、適切に監督を行った。
（カ）	総務省	総務省において、NICT に組織した「ナショナルサイバートレーニングセンター」を通じ、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。	・実践的サイバー防御演習（CYDER）について、2018 年度、地方公共団体からは 490 団体、計 1,664 名が受講。
（キ）	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、官民の認証連携をより一層推進していく。	・2017 年 11 月にマイナポータルの本格運用を開始し、これまでに国税庁の e-Tax、日本郵便の MyPost、野村総合研究所の e-私書箱、日本年金機構のねんきんネット及び総務省の総合無線局監理システム（PARTNER システム）との認証連携を開始した。
（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、2020 年度の導入を目指して準備を進めていく。	・厚生労働省において、マイナンバーカードを用いたオンライン資格確認を導入することとする、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提出した。

2.3. 政府機関等におけるセキュリティ強化・充実

(1) 情報システムのセキュリティ対策の高度化・可視化

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、統一基準群の改定に伴う各府省庁、独立行政法人及びサイバーセキュリティ基本法に基づく指定法人（以下「独立行政法人等」という。）の情報セキュリティポリシーの見直しについて、必要な支援を行う。また、新たに直面した脅威・課題への対応について、統一基準群の将来の改定に向けた知見の蓄積を行う。	・内閣官房において、統一基準群の改定案を策定し、サイバーセキュリティ戦略本部で決定した。また、本改定に伴う政府機関等の情報セキュリティポリシーの見直しが速やかに行われるよう、必要な支援を行った。 ・統一基準群の将来の改定に向け、情報セキュリティの動向等について情報収集を行った。
（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 が公表しているセキュリティ・バイ・デザインに関連するマニュアルの改定に着手する。	・内閣官房において、NISC が公表している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・デザインに関連するマニュアルの改定に向け、有識者や関連事業者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。
（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。	・経済産業省において、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。また、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を実施した。
（エ）	経済産業省	経済産業省において、IPA を通じ、CCRA などの海外連携、セキュリティ評価に係る国際基準の作成や各国の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。	・経済産業省において、IPA を通じ、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、安全な政府調達を推進するため、調達関係者に対する広報活動や勉強会、ヒアリングを実施するとともに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。	・経済産業省において、IPA を通じ、 ・統一基準（2018 年度版）において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室管理システムのセキュリティ要件について、政府機関等での調達・運用における確認すべきセキュリティ要件を明確にするため「入退室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」事業を実施。 ・認証の主流製品である複合機の暗号関連評価に関し、暗号モジュール試験及び認証制度(JCMVP)の活用を取り入れるとともに、業界団体から要望のあった暗号ツールの適用などの資料を公開し、申請者に対する利便性を向上。 ・分離されていた JISEC のハードウェア製品分野の規程・申請書様式を統一し、申請者がスムーズに申請手順の理解と手続が行える改善を図った。

（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。	・経済産業省において、IPA を通じ、IoT セキュリティフォーラム 2018 で「暗号モジュール試験及び認証制度」(JCMVP)の制度紹介を行うとともに、関連する動向として、欧米における情報の格付けとセキュリティ認証制度との対応関係の紹介を行った。 また、「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、デジタル複合機の中の暗号実装の正確性を確認することに貢献した。
（キ）	内閣官房	内閣官房において、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府機関情報システムの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、分析結果を各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、攻撃情報の共有等の連携を図る。	・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、巧妙化する情報セキュリティに関する脅威、動向等を踏まえ、各府省庁の情報システムにおける対策の実施状況の点検・改善を行うため、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の実施状況の調査を行う。調査結果は、マネジメント監査により確認された課題等も踏まえ、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ついて検討を行う。	・内閣官房において、昨今のサイバーセキュリティに関する状勢や動向を踏まえ、政府機関全体として分析、評価及び課題の把握、改善等が必要と考えられる項目として、2018 年度はリモートアクセスにおける情報セキュリティ対策、 サポートが切れる OS ソフトウェア対策及びソフトウェアに関する脆弱性対策対応を、それぞれ重点検査として実施した。調査結果は、統一基準群の改善等に向けた課題として検討を行った。
（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」の運用等を通じて標的型攻撃に対する多重防御の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、政府機関における IT-BCP の見直しにかかる調査等を実施するとともに、規程の改定に着手する。	・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、国内外の文献調査、専門家へのヒアリング及び政府機関等へのヒアリングを実施し、政府機関における IT-BCP のあるべき姿について規程の改定を含む検討を実施した。
（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。	・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。 また、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、耐量子計算機暗号の研究動向調査及び鍵管理ガイドラインの作成に向けた検討を行った。
（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のサイバーセキュリティ体制について、内閣官房等と緊密に連携し、迅速なサイバー攻撃からの防護の技術的な体制の強化に取り組む。	・社会保険診療報酬支払基金のサイバーセキュリティ体制について、内閣官房と連携し、体制強化に関する取組について検討を行った。
（ス）	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及びその後を見据えて、インシデント発生前及び発生時の情報提供の迅速化・高度化に資する GSOC システムの検知・解析機能を始めとした機能強化、GSOC センサーの増強等の検討を行うなど、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を踏まえつつ、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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、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の本格更改に向け、新たな政府のプライベート・クラウドとしての整備計画を策定する。	[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かかる調査を実施した。 [総務省] ・政府共通プラットフォームの本格更改に向け、政府共通プラットフォーム第二期整備計画(2019 年２月 25 日各府省情報化統括責任者（CIO）連絡会議決定）を策定した。
（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、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、2018 年度から検討を開始する。	・総務省及び経済産業省が中心となり、有識者からなる「クラウドサービスの安全性評価に関する検討会」において、適切なセキュリティを満たすクラウドサービスを政府が導入するために必要な評価方法について議論を開始した。 ・当該検討会を年度内に合計６回開催し、中間とりまとめを行った。
（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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、これらの情報技術を、政府機関等において活用できる可能性について検証する。	・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、次年度以降に行う調査の具体的な内容の策定を行った。

(4) 監査を通じたサイバーセキュリティの水準の向上

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、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ため、引き続き国の行政機関に対して監査を実施する。監査の実施に当たっては、２年間で全ての国の行政機関に対して監査を実施する計画とし、国の行政機関のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監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。2018 年度の監査については、前回までの監査の結果を踏まえるとともに前回対象としなかった部局やシステムを対象として実施する。	・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、2017 年度、2018 年度の２年間で全ての国の行政機関（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、2017 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、実際の攻撃　　手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを引き続き国の行政機関に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。なお、ペネトレーションテスト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。加えて、情報システムのペネトレーションテストを行うに当たり、自衛隊が有する知識・経験の活用を実施していく。	・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、全ての国の情報システムから調査対象システムを選定し、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、2017 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、改善状況のフォローアップを行った。
（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に基づく施策の取組について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、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ため、IPA との連携等により、引き続き独立行政法人等に対して監査を実施する。監査は、2020 年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う計画とし、独立行政法人等のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監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。2018 年度の監査については、独立行政法人等の業務内容の多様性を踏まえ選定した部署やシステムを対象として実施する。	・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、2018 年度に実施すべき独立行政法人等（以下「被監査主体」という。）への監査を実施し、被監査主体が今後のサイバーセキュリティ対策を強化するための検討をする上で有益な助言等を行った。また、2017 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、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを、IPA との連携等により、引き続き独立行政法人等に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。ペネトレーションテストは、2020 年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う。なお、ペネトレーションテストを実施した法人については、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、2018 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、2017 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

新戦略（2018 年７月 27 日閣議決定。2018 年７月～2021 年７月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	サイバーセキュリティ 2018	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。2018 年度は、政府機関等における実際のインシデント事案を題材とし、事案の関係者を交えた講義及びグループワークを実施した。また、CSIRT の能力を把握する手段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、2018 年度新任管理者セミナーにおいて、新任管理者向けに情報セキュリティをテーマとした講演を実施した。 ・内閣官房において、2019 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・演習を実施する。 ・内閣官房において、各府省庁における情報セキュリティ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、これまでの訓練や調査等により明らかになった課題や近年のサイバー攻撃動向等を踏まえた訓練を実施する。 また、府省庁及び独立行政法人等における情報セキュリティインシデント対処に関わる要員を対象として、研修を年間を通じて実施する。 さらに、政府機関等において自組織の環境に最適化した訓練を独自に実施できるようにするために必要な支援を行う。	・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 等の幹部も参加することで、組織的対処能力の向上も図った。また、2018 年度は訓練直後に 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。 ・内閣官房において、府省庁 CSIRT の対処能力の更なる強化のために必要な施策として、自組織においてインシデント対処訓練が実施できるよう支援するための資料及び手引書等を配布し、後日フォローアップを行った。
	内閣官房	内閣官房において、サイバー攻撃等により発生した支援対象機関等の情報システム障害又はその発生が予想される場合等、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。	・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。
	総務省	総務省において、NICT に組織した「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。 ・内閣官房及び総務省において、昨今のサイバー攻撃やこれまでの実施結果を踏まえつつ、NATIONAL 318(CYBER) EKIDEN を実施する。	・2018 年度については、実践的サイバー防御演習（CYDER）に国の行政機関から 386 名が受講。 ・１府 12 省庁が参加し、各府省庁のサイバー攻撃対処能力の向上を目的とした競技会である NATIONAL 318(CYBER) EKIDEN 2019 を実施した。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。また、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。	・文部科学省において、大学等における自律的な取組を促進するために、国立大学法人等が所有する情報システムの脆弱性診断（ペネトレーションテスト）を実施した。 ・文部科学省において、大学等の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、WG を設置し検討を行った。 ・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」の改訂のための見直しを行った。(改訂版の公表は 2019 年 6 月予定)
(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・演習の体系について検討し、試行的に実施する。	・文部科学省において、大学等の CISO、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、サイバー攻撃に係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に関する研修や実践的な演習を行った。
(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について必要に応じて支援する体制を整備する。	・文部科学省関係機関において、標的型サイバー攻撃により重大な被害が発生している（おそれを含む）場合、被害の最小化及び拡大防止のため、当該機関が迅速に民間セキュリティ事業者への移行を前提とした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を整備を開始し、一部については試行的に実施した。

(2) 大学等の連携協力による取組の推進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	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、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に、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施する。	・国立情報学研究所（NII）において、国立大学法人等のインシデント対応体制を高度化するために、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施した。
(イ)	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、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し、データ解析技術の開発を促進する。	・国立情報学研究所（NII）において、サイバー攻撃に関するデータ解析技術の開発を促進するため、国立大学法人等の通信データのうち、M2M を含めたサイバー攻撃に関するデータ等を収集し、共有するため、データのフォーマットや匿名化を含めた提供方法について検討し、国立大学法人等研究機関へ提供する準備を整えた。

（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手法を検討する。	・国立大学法人等における情報セキュリティ対策基本計画の進捗状況を把握し、その結果に基づき、対応すべき課題について文部科学省関係機関最高情報セキュリティ責任者会議を通じてフィードバックを行うことにより知見等の共有を図った。 ・学術系 CSIRT 情報交流会にオブザーバーとして参加し、大学等の CSIRT 間で情報共有の活性化を図った。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、「2020 年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」（2017 年３月 21 日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。 具体的には、オリパラ競技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て、リスク評価に基づく対策の促進と、情報の共有、インシデント発生時の調整役となるための組織であるサイバーセキュリティ対処調整センター(政府オリンピック・パラリンピック CSIRT）の整備を推進する。 2018 年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。 また、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピック CSIRT）については、2018 年度末を目途に構築し、2019 年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。	・引き続き、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象としたリスクマネジメントの促進や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進した。 ①　『リスクマネジメントの促進』 ・重要サービス事業者等（東京都、近郊県及び地方競技会場）を対象とする第３回リスクアセスメントの実施を依頼、各事業者等から提出された実施結果について、重要サービス分野内及び重要サービスを分野横断的に分析し、各事業者等へフィードバックを実施した。 ・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について、第１回として、電力、通信、水道、鉄道、放送分野等から５者を対象に実地検証、全重要サービス分野から 20 者を対象に書面検証を実施し、結果の取りまとめを行った。 ②　『対処態勢の整備』 ・サイバーセキュリティワーキングチーム等における検討を更に進め、大会に向けたサイバーセキュリティ体制の運用方針を関係府省庁、大会組織委員会、東京都等と協議の上、決定した。 ・サイバーセキュリティ対処調整センターを構築した。
（イ）	警察庁	警察庁に設置したセキュリティ情報センターにおいて、国の関係機関の協力を得て、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 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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月の諸施策の目標と実施方針）より			
・2020 年東京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	サイバーセキュリティ 2018	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に当たっては、整備した仕組み、その運用経験及びノウハウが、レガシーとして、2020 年東京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に活用できることを考慮し、構築した「サイバーセキュリティ対処調整センター」は、サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口となる組織（ナショナル CSIRT）へと成長・発展させ、サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう検討する。	・2020 年東京大会に向けた態勢の整備に当たっては、整備した仕組み、その運用経験及びノウハウが、2020 年東京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に活用できることを考慮し、「サイバーセキュリティ対処調整センター」の構築を実施した。整備する情報共有システムは、大会後に全国の重要インフラ事業者等までユーザーを拡大できるよう、特に専門的な知識がなくても使っていただけるよう考慮して設計を行った。 ・「リスクマネジメント」の手法についても、広く全国の事業者等に適用できるよう考慮し、米国のシンクタンクの支援及びリスクアセスメント結果の反映等により逐次改善を実施した。
（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図る。また、法務省において、人的情報収集・分析を行い、対応を推進する。	［警察庁］ ・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、体制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、2020 年東京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 に組織した「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に向けた大規模演習環境「サイバーコロッセオ」を活用し、同大会のサイバーセキュリティを守る高度な人材の育成を推進し、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図る。	・サイバーコロッセオについては、東京オリンピック・パラリンピック競技大会組織委員会のセキュリティ担当者等を対象に演習を実施し、2018 年度は延べ 137 名が受講。

2.6. 従来の枠を超えた情報共有・連携体制の構築

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、重要インフラ事業者等への情報提供を行った。また、同機関が分析した情報の横展開を行った。さらに、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。また、重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、IPA を通じ、障害事例等の情報を重要インフラ事業者等へ提供する。	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。また、一部、STIX 等の機械処理可能な形式での情報共有も試行した。 ・2018 年度は新たにエアポート業界 SIG と鉄鋼業界 SIG が運用開始した。また、既存の SIG と運用ルールの異なる新たな「情報連携体制」として、医療業界、水道業界での情報共有の取組を開始した。 ・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。 ・重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、2017 年度までに体制構築した 12 の情報共有体制に対して、情報処理システムの障害情報等を提供し、自律的な障害情報共有に向けた支援を実施した。また、障害事例から得られた経験やノウハウを「教訓」として取りまとめ、「情報処理システム高信頼化教訓集　IT サービス編」の書籍を 2019 年３月に発行するとともに、教訓を自組織内で実践するための対策方法や障害原因分析に用いられる分析手法をまとめた資料を web 公開した。
（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等の情報通信分野全体における情報共有を促進した。
（エ）	国土交通省	国土交通省において、2018 年４月から重要インフラ（航空、鉄道、物流分野）事業者による情報共有・分析及び対策を連携して行う体制である「交通 ISAC」（仮称）の仮運用が開始されたことから、事業者等が参加する検討会を開催し、交通 ISAC の本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論する。	・国土交通省において、2018 年４月から重要インフラ事業者（航空、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）の仮運用が開始されたことから、事業者が参加する検討会を開催し、交通 ISAC の本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論した。 また、2018 年７月に重要インフラ分野に追加された空港分野の事業者に対し、交通 ISAC への参加を促した。
（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、2019 年３月現在、「金融 ISAC」の加盟社は 382 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の ISAC について、必要な調査・情報収集を行うとともに、検討を進める。	・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・情報収集したところである。 ・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海外事例を中心に調査を行い、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、「金融 ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。	・経済産業省において、2018 年 11 月に金融 ISAC 事務局との間で意見交換を行い、金融 ISAC の活動目的・内容等について情報提供を受け、カード会社の参加状況等について確認した。また、この内容について、2018 年 11 月に開催したクレジットセプター運営会議で報告を行い、金融 ISAC の参加メンバーであるカード会社委員等との間で意見交換を行った。
（ク）	経済産業省	経済産業省において、自動車業界の事業者に対し、「J-Auto-ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。	・経済産業省において、自動車業界の「J-Auto-ISAC」等の情報共有機関等に対して、全自動車メーカーが参加し、同機関等を通じた情報共有網の拡充を進めた。
（ケ）	経済産業省	経済産業省において、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CC から重要インフラ事業者等へ提供する。	・経済産業省において、JPCERT/CC を通じ、 ・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情報セキュリティ上の脅威及びその対策について、46 件の「早期警戒情報」を発行した（2019 年 2 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　8,776 件：2019 年２月末現在）。また制御システムの関係者向けに 21 件の参考情報と 12 件の月次ニュースレター、57 件のニュースクリップなどの情報発信を行った。（全て 2019 年２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、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。	・都道府県警察において JC3 を通じて企業等とサイバー空間の脅威への対処に関する情報を共有したほか、不正作成ＩＤの流通阻止に向けた官民連携による犯罪インフラ対策や、クレジットカードの不正利用に係る不正宿泊対策を実施した。（再掲）

(1) 多様な主体の情報共有・連携の推進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	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協議会の創設に向けて検討を進める。	・2018 年 12 月に、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）が成立した。同法により改正されたサイバーセキュリティ基本法第 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を組織した。また、この協議会の規約等において、各主体の自主性を最大限に尊重するためのルール、各主体が安心して情報の共有を行うことを可能にするためのルール、既存の情報共有体制との円滑な連携等を可能にするためのルール等、様々な運用ルールを整備した。

(2) 情報共有・連携の新たな段階へ

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房が中心となり構築する情報共有体制において、積極的にサイバーセキュリティインシデント等に係る情報（例えば、リコールの要因となる情報など、国民の生命・身体を保護するために提供される情報を含む。）の共有に貢献する参加者が評価される環境を整備するための検討を進める。また、当該体制において情報の共有や分析を迅速に行うための処理の自動化に向けた検討を進める。	・2018 年 12 月に、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）が成立した。同法により改正されたサイバーセキュリティ基本法第 17 条に基づき、2019 年４月１日にサイバーセキュリティ協議会を組織した。この協議会の規約等において、サイバーセキュリティインシデント等に係る情報（リコールの要因となる情報等を含む。）を積極的に提供する構成員がより評価され、メリットを享受することを可能にするためのルールや、情報の共有・分析を迅速に行うための処理の自動化に対応したシステム等を整備した。
（イ）	内閣官房	内閣官房が中心となり構築する情報共有体制において、所管省庁を同じくする複数の業界が業界を跨いで情報共有の仕組みを構築する等新しい情報共有・連携を推進するための検討を進める。	・2018 年 12 月に、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）が成立した。同法により改正されたサイバーセキュリティ基本法第 17 条に基づき、2019 年４月１日にサイバーセキュリティ協議会を組織した。この協議会の規約等において、所管省庁を同じくする複数の業界が、業界を跨いで情報共有の仕組みを構築するといった様々な情報共有・連携の在り方に柔軟に対応できるようにするためのルール等を整備した。

2.7. 大規模サイバー攻撃事態等への対処態勢の強化

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、関係府省庁、重要インフラ事業者等と連携した初動対処訓練を実施する。	・内閣官房が、関係省庁及び重要インフラ事業者等とともに、重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、政府の初動対処態勢を整備するとともに、対処要員の能力強化を図った。
（イ）	内閣官房	内閣官房において、サイバー攻撃等の事象に関する政府としての一連の初動対処（検知、判断、対処、報告）を見直し、サイバーセキュリティに係る危機管理対応の一層の強化が図られるよう留意する。	・初動対処訓練を通じて、サイバー攻撃発生時における組織内の情報共有、関係府省庁、関係機関等との連携について確認した。そのうえで、サイバーセキュリティに係る危機管理対応の一層の強化を図るために見直すべき事項を洗い出し、環境整備等必要な措置の検討を行った。

（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図る。 ・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、官民の協働による対処態勢の強化を図る。 ・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。 ・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。また、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等の解析を推進する。	・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、JPCERT/CC を通じ、重要インフラ事業者等からの依頼に応じ、国際的な CSIRT 間連携の枠組みも利用しながら、攻撃元の国に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。	・経済産業省において、JPCERT/CC を通じ、 ・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情報セキュリティ上の脅威及びその対策について、46 件の「早期警戒情報」を発行した（2019 年 2 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 8,776 件：2019 年２月末現在）。また制御システムの関係者向けに 21 件の参考情報と 12 件の月次ニュースレター、57 件のニュースクリップなどの情報発信を行った。（全て 2019 年２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）」の活動を増強し、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 127 件行うとともに、うち 31 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、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、必要に応じて指導・助言等を行う。	・2018 年６月 11 日に第２回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ダークウェブの現状等について意見交換や、当委員会に報告された漏えい等事案について情報共有するなど、情報セキュリティ関係機関との連携を図った。 また、個人情報取扱事業者から個人データの漏えい等事案の報告を受けた際には、事実関係及び再発防止策の確認等を行うとともに、同種の事態が起きないよう必要に応じて指導等を行った。

（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 設立を促進・支援する。また、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およ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 2018 年３月末時点では 284 組織であったが、2019 年２月末現在で 329 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。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。	・2018 年５月の日イスラエル首脳会談で、両首脳は、サイバー面での協力を強化していくことを確認。両首脳は、イスラエルのベイルシェバにあるサイバーセキュリティーコンプレックスへ専門家を派遣することに合意し、本合意に基づき、2018 年６月、11 月に専門家を派遣した。 ・2019 年１月の日英首脳会談で、両首脳は、「日英共同声明」において、「自由で、開かれ、平和で、公正かつ安全なサイバー空間を促進することに対するコミットメントを改めて表明」するとともに、「サイバー攻撃を抑止し、対応し、緩和するために共に取り組み、国家の無責任な行動を非難」し、「サイバーにより可能となる知的財産の窃取その他の脅威から技術を保護するにあたり協力を強化すること」を表明した。 ・2019 年１月、櫻田大臣は、イスラエル、英国及びフランスに出張し、東京大会の成功に向けた協力関係の構築の確認、サイバーセキュリティの課題の共有や対応策に関する意見交換を実施した。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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とともに、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。	・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、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（「Forced Localization Measures」）を行う諸外国に対し、対話や意見交換を通じ、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、民間団体とも連携しつつ働きかけを行う。	・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、民間団体等との情報交換を行った。

(2) サイバー空間における法の支配の推進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、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。	・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。 ・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。 ・次会期国連政府専門家会合の方向性等を含め、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。また、各種国際会議等での議論やパネルディスカッション等を通じ、国際的なルール及び規範作りに積極的に関与している。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。今後は、更なる刑事共助条約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及び大韓民国との間では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、アジア大洋州地域サイバー犯罪捜査技術会議の主催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（2018 年 10 月、2019 年３月）、ASEAN サイバー犯罪対策対話（2019 年１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。 ・警察庁とアジア大洋州地域における法執行機関との間で、情報技術の解析に係る知識・経験等を共有し、情報技術解析能力の向上を図ることを目的として、2018 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。 ・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１月現在、85 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、引き続きアジア地域初の締約国として同条約の普及等に積極的に参画する。	・2018 年４月及び 2019 年３月にウィーンで開催された国連サイバー犯罪包括研究に関する政府間オープンエンド専門家会合や、2018 年７月及び 11 月にストラスブールで開催されたサイバー犯罪条約締約国会合のほか、2019 年１月にブルネイで開催された日 ASEAN サイバー犯罪対策対話等の場において、サイバー犯罪に関する有志国と連携しつつ、サイバー犯罪条約の有効性を発信するとともに、同条約に関心を持つアジア諸国に対して働きかけを行った。

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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、緊急対処能力の向上を図る。 ・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実施する。	・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とともに、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、2019 年３月までに各自衛隊の防護システム、防衛情報通信基盤（DII）のクローズ系、ネットワーク監視機材の機能拡充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する。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関係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の在り方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）について、実施に向けた所要の準備を進める。	・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）に向け、必要な訓練等を実施した。
（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研究を実施する。	・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のための試作品の設計を実施した。
（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、移動系サイバー演習環境構築技術に関する研究を開始した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行うとともに、引き続き調査研究等を通じて必要な関連規則等の整備を進める。	・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、調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達に係る関連規則を整備した。

(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、サイバー攻撃による当該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に対して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を検討し、これを盛り込んだ統一基準を公表した。 個々の法人については、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] ・国立大学法人等における情報セキュリティ対策基本計画の進捗状況を把握し、その結果に基づき、対応すべき課題について文部科学省関係機関最高情報セキュリティ責任者会議を通じてフィードバックを行った。 ・大学等の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、WG を設置し検討を行った。 ・国立情報学研究所（NII）が国立大学法人等と連携し、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 を運用した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。
(コ)	警察庁 法務省	警察庁及び法務省において、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図る。	[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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進する。	・関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進しているところ。
（イ）	防衛省	防衛省において、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を整備する。その際、悪意ある主体によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる。	・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。 また、悪意ある主体によるサイバー空間の利用を妨げる能力に関しては、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、当該能力を含むサイバー防衛能力の抜本的強化を図るため、2019 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。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（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、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平素から構築する。	・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、サイバーセキュリティに関する会期間会合を設立し、2019 年１月には第３回目となる専門家会合を開催したところ、考え方を異にする国との間でも予測可能性を向上し、信頼醸成を進めている。

（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、JPCERT/CC の FIRST、IWWN や APCERT 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行う。	・経済産業省において、JPCERT/CC を通じて、 ・2018 年度期限を迎えた MOU の更新を滞りなくすすめ、継続的な CSIRT 間連携関係の維持に努めた。日中韓 CSIRT MOU に基づき 2018 年 8 月に「第 6 回 日中韓サイバーセキュリティインシデント対応年次会合」を JPCERT/CC がホストし東京で開催した。 ・FIRST、APCERT 等の CSIRT コミュニティのイベントに積極的に参加し、CSIRT 間の連携の窓口として情報を取り入れる活動を継続して行った。 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等の活動等を通じて、各国 CSIRT とインシデント対応に関する連携を行った。 ・そのほか、コミュニティとも連携しインシデントハンドリング対応支援に生かし、得られた知見を外部への公開を行った。

(3) サイバー空間の状況把握の強化

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。また、政府機関が保有する機密情報が保護されるよう適切な措置を実施する。	・関係省庁との連携を密にし、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	警察庁及び法務省において、サイバーインテリジェンス対策に資する取組を実施する。	［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図る。 ・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図る。（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。また、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等の解析を推進する。	・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。（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情報収集を推進した。（再掲） ・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・育成を図る方策を検討する。	・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、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）の運用との連動等の有効活用やその高度化を進める。	・経済産業省において、JPCERT/CC を通じて、アフリカ地域の NationalCSIRT が加盟している AfricaCERT 加盟組織に対して、TSUBAME への参加の呼びかけを行い、当該組織からの問い合わせ等に対応することで、加盟に向けた取組を実施した。結果、ガーナの CSIRT（NCA CERT）が新たに TSUBAME に加わった。APCERT の中国での年次総会に合わせて、カンファレンスでの情報共有を実施した。 また、APCERT の Malware Mitigation WG に参加し TSUBAME との連携を模索中である。
（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。	・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。
（ク）	法務省	法務省において、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・育成を図る方策を検討する。	・法務省（公安調査庁）において、高度な専門性を有する人材の確保・育成に向けた方策の検討を実施した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ケ）	内閣官房	内閣官房及び外務省において、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・分析に努める。	・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。	［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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、日 ASEAN サイバーセキュリティ政策会議、二国間協議等の枠組みを通じ、アジア大洋州各国とのサイバー政策における相互理解と連携を強化する。また、総務省において、ワークショップの開催等を通じて、我が国と ASEAN 加盟国のネットワークオペレータ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、同地域の意識啓発を一層強化するため、セキュリティチェックシートを共同作成し、各国の言語に翻訳し希望国へ送付する等 ASEAN 加盟国の要望に応じた取組を行った。 ［総務省］ ・日本及び ASEAN の ISP 間の情報共有を促進する「第 9 回 ISP 向け日 ASEAN 情報セキュリティワークショップ」（2019 年 1 月、シンガポール）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、合同サイバー攻撃対応演習を実施した。
（イ）	警察庁 法務省 外務省	警察庁、法務省及び外務省において、国境を越えるサイバー犯罪の脅威に対抗するため、特にアジア太平洋地域諸国におけるサイバー犯罪対策に関する刑事司法制度の整備等が進むよう、二国間又は多国間の枠組みを活用した技術援助活動を積極的に推進する。	・警察庁とアジア大洋州地域における各法執行機関との間で、情報技術の解析に係る知識・経験等を共有し、情報技術解析能力の向上を図ることを目的として、2018 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。

（ウ）	防衛省	防衛省及び関係府省庁において、東南アジア各国との間で、防衛当局間の IT フォーラム等の取組を通じ、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。また、防衛省において、諸外国とのサイバー防衛協力を推進していく。	・防衛省において、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（2019 年３月）及び日越（ベトナム）ＩＴフォーラム（2019 年３月）等を実施した他、諸外国との連携を強化した。
（エ）	経済産業省	経済産業省において、アジアでの更なる情報セキュリティ人材の育成を図るため、アジア 11 か国・地域と相互・認証を行っている「情報処理技術者試験」について、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（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）が協力して試験を実施するための協議会である ITPEC がアジア統一試験を実施しているところ、ITPEC の更なる定着を図る。	・経済産業省において、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（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）が協力して試験を実施するための協議会である ITPEC がアジア統一試験を実施しているところ、ITPEC の更なる定着を図るため、2018 年８月に日本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、2019 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、アジアの優秀な IT 人材と日本の 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。
（オ）	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、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、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６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。
（カ）	総務省 外務省	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、日米の通信分野の ISAC 間の連携を推進する。	・「第３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２月、東京）を開催した。米国より DHS（国土安全保障省）、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・議論を行った。
（キ）	経済産業省	経済産業省において、国際協力体制を確立するという観点から、米 NIST 等の各国のサイバーセキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取組む。	・経済産業省において、IPA を通じ、2018 年４月に、米国立標準技術研究所（NIST）を訪問し、暗号モジュール試験・認証制度における連携や、現在 NIST が取り組んでいる暗号アルゴリズム確認やモジュール認証の自動化等に関する意見交換を実施した。
（ク）	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、新たな日米防衛協力のための指針や日米サイバー防衛政策ワーキンググループ（CDPWG）で示された方向性に基づき、2018 年９月に開催された CDPWG 第６回会合を含め、各種レベルで米国と協議を実施し、米国との連携を強化した。
（ケ）	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、二国間協議の枠組みを通じ、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回日仏サイバー協議（2018 年６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の共有を進めた。 ［防衛省］ ・防衛省において、2019 年３月より、NATO CCDCOE に防衛省職員を派遣する他、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 主催の演習のビジターデーへの参加等を通じ、欧州各国との連携強化に努めた。

（コ）	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、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強化する。	・Meridian 会合、CIP フォーラム、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、国際協調・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。
（サ）	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。	・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。（再掲） ・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。(再掲)
（シ）	経済産業省	経済産業省において、IPA 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ため、JIWG 及びその傘下の JHAS、JEDS と定期的に協議を行う。	・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、2018 年度の活動報告と 2019 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３回参加し、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。
（ス）	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、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、各国との協議及び脅威認識等の共有を図った。

(2) 事故対応等に係る国際連携の強化

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、二国間協議、IWWN、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、それぞれの取組において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・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で堅牢な定量評価の仕組み(サイバーグリーン)の検討や、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、サイバーグリーンインスティテュート(CGI)と連携し、インターネット上のリスクとなりうる要因となるデータを使用し、クリーンアップ活動につなげた。2017 年度にリリースした、インターネットリスク可視化サービス「Mejiro」は 2018 年８月に英語版を公開した。また、2019 年３月に新規データソース(CGI)の取込みと監視対象プロトコルを追加し機能の拡張を行った。
（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、APCERT の中国での年次総会（2018 年 10 月）に合わせて、WG 内で行っている情報共有の項目から主に IoT を対象とした攻撃の動向と各地域での影響について分析結果の共有を行った。また協調した対応を行うため、National CSIRT 間の情報共有、地域内でのセキュリティ機関との情報共有の重要性についての問題意識を共有した。TSUBAME 加盟組織拡大については、中東・アフリカ地域へのアプローチを継続して実施した。

（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、連携の支援。JPCERT/CC の経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習の実施。 ・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に関する技術セミナーを実施。	・経済産業省において、JPCERT/CC を通じ、2018 年度は、経済発展に伴いソフトウエア開発の分野でも存在感の増しているインドネシアにてアンドロイドセキュアセキュアコーディングセミナーを実施し、40 名程度が参加した。 アフリカ地域においては Africa Internet Summit 2018、Afrinic29 に参加し、OSINT トレーニング、インシデントハンドリングトレーニングを行った。 OSINT のトレーニングでは発生した脅威と、脅威因子に関する情報を収集したり、それらの情報の分析、フィルター処理を行い有用な情報を生成する手法についてレクチャーすることで、アフリカ地域におけるサイバーセキュリティ能力向上に貢献した。

(3) 能力構築支援

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、ASEAN 加盟国をはじめとする各国における能力構築支援に積極的に取り組む。取組に際しては、内閣官房を中心に、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2016 年 10 月）を踏まえ、政府及び関係機関が一体となって対応していく。 ・内閣官房において、日・ASEAN サイバーセキュリティ政策会議を通じたセキュリティ人材育成の取組や一般向け意識啓発の取組を通じて、ASEAN 加盟国の能力構築に貢献する。 ・警察庁において、アジア大洋州地域サイバー犯罪捜査技術会議や JICA 課題別研修（サイバー犯罪対処能力向上）、JICA 国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）の開催等を通じ、アジア大洋州地域をはじめとする各国における能力構築に貢献する。 ・総務省において、日 ASEAN 情報通信大臣会合を通じて、情報通信分野に関して ASEAN 域内各国・地域との間でのネットワークセキュリティ分野における能力構築等の連携を推進する。また、APT（アジア・太平洋電気通信共同体）における取組や ITU-D 等の取組を通じて、研修やセミナーを開催することにより、諸外国に対する意識啓発に取り組む。	[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。 ・2018 年において国際連携・協力の推進に資する取組として、セキュリティチェックシートを共同作成し、各国の言語に翻訳し希望国へ送付する等 ASEAN 加盟国の要望に応じた取組を行った。 [警察庁] ・警察庁とアジア大洋州地域における法執行機関との間で、情報技術の解析に係る知識・経験等を共有し、情報技術解析能力の向上を図ることを目的として、2018 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。（再掲） ・2018 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こと及び日本・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。 ・2019 年１～２月、警察庁とＪＩＣＡの連携の下、海外 20 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。 ・APT 加盟国を対象とした研修（2018 年 10 月、東京）や APT 幹部ワークショップ（2019 年３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。 ・ITU-D SG2 ラポータ会合（2018 年 10 月、ジュネーブ）におけるサイバーセキュリティワークショップにおいて、総務省のサイバーセキュリティ政策に関する講演及びパネルディスカッションを実施した。

	外務省 経済産業省	・外務省において、警察庁等とも協力しつつ、第３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。 ・経済産業省において、ASEAN 加盟国に対し、ISMS、CSMS に関する研修・セミナー等を通じて、我が国のセキュリティマネジメントに関するノウハウを共有することで、ASEAN 加盟国への能力構築支援へ貢献する。 ・経済産業省において、JPCERT/CC を通じ、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、連携の支援を行う。JPCERT/CC の経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習実施を行う。また、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、サイバー演習の実施等の活動等を行う。さらに、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先の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に関する技術セミナーを実施する。	・2018 年度予算として、東南アジアの国々の能力向上を支援する UNODC サイバー犯罪グローバル・プログラムに 10 万ドルを拠出し、また、UNODC による東南アジア向けのダークネットの調査等に関するプロジェクトに 50 万ドルを拠出した。また、2019 年１月にブルネイで第３回目 ASEAN サイバー犯罪対策対話を開催し、ASEAN 各国のサイバー犯罪対策の現状について意見交換を実施したほか、日 ASEAN 統合基金を活用して実施している ASEAN サイバー能力向上プロジェクトについて議論を行った。
（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）が米国土安全保障省及び同省傘下の ICS-CERT 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を通じた能力構築支援を開始する。	・経済産業省において、2018 年９月 10～14 日、米国・国土安全保障省（DHS）及び NCCIC ICS から専門家５名を招聘し、ASEAN 等向けに日米サイバー共同演習を実施し IPA 産業サイバーセキュリティセンター（ICSCoE）中核人事育成プログラムの研修生 83 名に加え、ASEAN 等の 15 の国・地域（ブルネイ、カンボジア、インドネシア、ラオス、マレーシア、ミャンマー、フィリピン、シンガポール、タイ、ベトナム）、オーストラリア、インド、韓国、ニュージーランド、台湾）からの参加者 36 名が参加した。

4. 横断的施策

4.1. 人材育成・確保

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、関係府省庁と連携しつつ、「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人材育成取組方針」に基づき、産学官の連携を図りつつ、関係施策を促進していく。	・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共に、施策間の連携を促進した。
（イ）	内閣官房	内閣官房において、「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人材育成取組方針」を踏まえ、さまざまな人材育成施策について、施策間の連携を強化するとともに、横断的かつ継続的に人材育成施策の全体像が把握できるよう、「見える化」の推進を図る。	・普及啓発・人材育成専門調査会において、人材育成に関する政府の取組を整理・更新し、「見える化」を進めた。

(1) 戦略マネジメント層の育成・定着

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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 に設置した「産業サイバーセキュリティセンター」において、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。	・経済産業省において、2018 年７月から、「産業サイバーセキュリティセンター」において、約 80 名の受講生を受け入れ、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育成を目的とした第２期「中核人材育成プログラム」を開講するとともに、各社の CISO 等の責任者やその補佐等を対象とした短期プログラムも計５回実施。また、制御システム等の安全性・信頼性を検証するリスク評価事業を１業種において実施。
(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、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 2018 年秋から開始する。	・経済産業省において、2018 年 11 月から同年 12 月までの間に週１回/全７回、「産業サイバーセキュリティセンター」において、約 20 名の受講生を受け入れ、企業におけるリスク管理に関わる責任者クラスを対象とした「戦略マネジメント系セミナー」を実施した。
(ウ)	経済産業省	経済産業省において、セキュリティ教育を提供するため、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、独立行政法人国立高等専門学校機構の情報担当教員向け研修に、JPCERT/CC から講師を派遣。
(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、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。
(オ)	内閣官房	内閣官房において、戦略マネジメント層を担う人材の育成に向けて、必要な知識・スキルを身に着けるための試行的取組について検討する。	・「戦略マネジメント層の育成手法に関する調査」を実施し、戦略マネジメント層を担う人材に必要な知識・スキル及びそれを学ぶカリキュラムを検討するとともに、実際に試行的取組を行い、成果を取りまとめた。

(2) 実務者層・技術者層の育成

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、官民の協働による対処態勢の強化を図る。（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。（再掲）

（ウ）	総務省	総務省において、NICT に組織した「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。	・実践的サイバー防御演習（CYDER）については、2018 年度、全国 47 都道府県で 107 回の演習を実施し、計 2,666 名が受講。
（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セキュリティ教育の強化のための施策として、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を進める。また、並行して、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）については、日々進歩しているサイバー攻撃技術に対応するため、定期的な環境更新（アップデート）を進めるなど、全国の高等専門学校生が共同で利用できるサイバーレンジ（実践的な演習環境）の提供に向けた取組を推進する。	・2018 年度予算において（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措置。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。また、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）では、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）に 2018 年度から取り組んでいる。あわせて、全国 10 カ所で「情報セキュリティ人材」の発掘・育成を実行。
（オ）	厚生労働省	厚生労働省において、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。（35 コース・受講者数 523 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。（2018 年 10 月 1 日時点の情報関係の指定講座数 332 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」の教育訓練を指定した。（2018 年 10 月 1 日時点の指定講座数 28 講座）
（カ）	経済産業省	経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として 2016 年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施と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。	・経済産業省において、2019 年４月時点の情報処理安全確保支援士（登録セキスペ）は 18,330 人（うち、男性 17,235 人、女性 1,095 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。
（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」の普及を図る。	・経済産業省において、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、IPA を通じて広報活動を実施した。
（ク）	内閣官房 経済産業省	内閣官房及び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一層の周知及び普及を図る。	・経済産業省において、IPA を通じ、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、広報活動を実施した。
（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 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、 ・全国各地域で、NPO 等の団体との連携により「インターネット安全教室」を合計 128 回開催し、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い、小中高校生からシニア層まで合計 12,252 名が参加した。 ・各地域団体による講習能力の向上を図る講師トレーニングを全国５箇所において開催し、合計 189 名が参加した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（コ）	経済産業省	経済産業省において、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 IPA と「一般社団法人セキュリティ・キャンプ協議会」にて共催しているセキュリティ・キャンプについて、サイバーセキュリティを取り巻く状況の変化への更なる対応を図る。	・経済産業省において、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、2018 年 8 月 14 日～18 日にかけて「セキュリティ・キャンプ全国大会」を東京都で実施。85 名が参加した。 また、2018 年５月から 2019 年 3 月にかけて、セキュリティ人材の裾野とコミュニティの拡大を目的に「セキュリティ・キャンプ地方大会」を全国 11 箇所で実施した。
（サ）	経済産業省	経済産業省において、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・技術を有する人材の発掘・育成に向け、「未踏 IT 人材発掘・育成事業」を実施する。	・経済産業省において、「未踏 IT 人材発掘・育成事業」は 21 テーマ 27 名のクリエータを採用し、着実に事業を実施した。また、2017 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、セキュリティ分野をテーマとした応募の促進を行った。
（シ）	経済産業省	経済産業省において、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」について、NPO 日本ネットワークセキュリティ協会及び企業が共同で開催地域拡大や競技内容の向上を図り、更なる人材候補者を増やすべく、大学等との連携や多様なコンテストの在り方を検討するとともに、同協会で実施するコンテスト（「SECCON 2018」）について普及・広報の支援を行う。	・経済産業省において、NPO 日本ネットワークセキュリティ協会が主催する「SECCON2018」に対して、経済産業省として後援するとともに、2018 年 12 月 22 日～23 日に実施された「SECCON2018 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。	・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。
（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を整備する。	・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具体的・実効的連携を深化するための取組を実施する。	・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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	経済産業省	経済産業省において、情報サービスの提供に必要な実務能力を明確化、体系化した共通指標である IT スキル標準の全面的な改訂に向け、第４次産業革命に伴い主流となる新技術に対応する IT 人材に焦点を当てたスキル標準の検討を引き続き行う。	・経済産業省において、第四次産業革命に向けて求められる新たな領域の“学び直し”の指針としてＩＴＳＳ＋を策定。主に、従来ＩＴスキル標準が対象としていた人材の新たな領域におけるスキル強化を想定していいる。2018 年４月に新たに「アジャイル領域」、「IoT ソリューション領域」を公表。

（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や、それに基づく指導方法・教材の利活用等について、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、「次世代の教育情報化推進事業」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や、それに基づく指導方法・教材の利活用等について、実践的な研究を実施し、成果を取りまとめている。
（ウ）	文部科学省	文部科学省において、2016 年 11 月の教育職員免許法改正及び 2017 年 11 月の同法施行規則改正に基づき、ICT を用いて効果的な授業を行ったり、適切なデジタル教材を開発・活用したりすることができる力を教師を志す学生に身に付けさせるため、各教科の指導法を学ぶ科目について、当該教科の特性に応じた情報機器や教材の効果的な活用方法を新たに内容に加えた教員養成課程の審査を行う。	・小学校・中学校・高等学校等の教員養成課程（合計 18,766 課程）について、ICT を活用した指導法等の内容を加えた授業科目や専任教員等の体制を審査の上、改めて文部科学大臣が認定した。新しい教員養成課程は、2019 年度入学生から適用される。
（エ）	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、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、2019 年１月 28 日～２月１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。
（オ）	文部科学省	文部科学省において、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、2019 年２月までに実施済。
（カ）	総務省	総務省において、NICT に組織した「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、若年層の ICT 人材を対象に、高度なセキュリティ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。	・若年層の ICT 人材を対象に、未来のサイバーセキュリティイノベーターの育成に取り組む「SecHack365」を実施。１年間を通じてセキュリティに関わる技術を本格的に指導し、2018 年度は、46 名がプログラムを修了した。修了生のうち、男性は 42 名、女性は４名。
（キ）	文部科学省	文部科学省において、複数の大学や産学の連携によるサイバーセキュリティに係る実践的な教育ネットワークの構築や PBL（課題解決型学習）の実施を支援する。	・「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」において、セキュリティ分野の人材育成にも取り組んでいる。当事業において、産学が連携した教育ネットワークを構築し、実際の課題に基づく課題解決型学習などの実践的な教育を行うことにより、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、学部 3～4 年生の学生を対象とした enPiTⅡにおいて外部有識者による中間評価を実施した。
（ク）	文部科学省	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。	・「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、学部 3～4 年生の学生を対象とした enPiTⅡ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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	内閣官房	各府省庁において、内閣官房の主導により 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。	・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。
(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、「各府省庁セキュリティ・IT 人材確保・育成計画」に沿って引き続き体制の整備と適切な処遇の確保に取り組む。	・各府省庁において、サイバーセキュリティ・情報化審議官が中心となって「各府省庁セキュリティ・IT 人材確保・育成計画」に沿って体制の整備と適切な処遇の確保に取り組み、それぞれフォローアップを行って確認したところ、いずれにも成果が見られた。
(ウ)	内閣官房 総務省	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とともに、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、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 2018 年度情報システム統一研修を実施したほか、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。また、府省庁を対象に、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を開催する。	・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４回開催し、実際に発生した事案を題材としたケーススタディや有識者による講義・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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、主要国における取組について調査の上、人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討を行う。	・国内外の大学や公的機関等における人材育成や研究開発の取組について、関係機関へのヒアリングや調査会での議論を行い、検討を進めた。
(イ)	経済産業省	経済産業省において、今後、ますますの経済連携が求められる ASEAN 各国において、我が国企業が安全に活動でき、また、我が国の持つノウハウを ASEAN 諸国と共有できるよう、セキュリティマネジメント導入のためのノウハウ支援等を行う。	・経済産業省において、ベトナム、バングラデシュにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入のため、企画・計画段階から現地の電力企業への支援を実施した。また、カンボジア、ラオス、ミャンマーにおいて、サイバー攻撃に強い電力制御システム（SCADA）の導入に向けた理解を醸成するため、現地の電力企業向けに研修を実施した。

4.2. 研究開発の推進

(1) 実戦的な研究開発の推進

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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			
項番	担当府省庁	サイバーセキュリティ 2018	取組の成果、進捗状況
(ア)	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、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、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。
(イ)	文部科学省	文部科学省において、サイバーセキュリティを含む経済・社会的な重要課題を解決につなげることが期待される、量子コンピュータをはじめとした量子科学技術に関する研究開発を推進する。	・経済・社会的な重要課題を解決につなげることを目指し、2018 年度より「光・量子飛躍フラッグシッププログラム（Q-LEAP）」を開始した。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次世代レーザーを対象とし、プログラムディレクターによるきめ細かな進捗管理によりプロトタイプによる実証を目指す研究開発を行う Flagship プロジェクトや、基礎基盤研究を推進している。
(ウ)	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と、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ていく。あわせて、JST の戦略的創造研究推進事業において、サイバーセキュリティを含めた研究課題を支援する。	・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。
(エ)	経済産業省	経済産業省において、AIST 等を通じ、IoT システムに付随する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、などを両立させるための革新的、先端的技術の基礎研究に取り組む。	・経済産業省において、AIST を通じ、ソフトウェア工学、暗号技術などを用いてシステムの品質、安全性、効率を向上、両立させるための革新的、先端的技術の基礎研究に取り組んだ。特筆すべき成果としては、入力を秘密にしたまま、あるクラスの計算を実行できる暗号技術の C++ライブラリでの実装において、世界最高速を達成したり、ウェブブラウザで１ミリ秒以下での計算を可能とした等、提案技術の実用性を実システム上で示すことができた。
(オ)	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コア技術の調査・研究開発・実証等を行う。	・経済産業省の「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 年度に、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実施。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月の諸施策の目標と実施方針）より			
・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** **・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**			
項番	担当府省庁	サイバーセキュリティ 2018	取組の成果、進捗状況
（カ）	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する研究を行う。	・経済産業省において、機器の信頼性創出や証明、トレーサビリティ確保、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の効率的な検出に関して高度な技術を持つ事業者と連携し、これらの課題についての国内外の動向調査、実際の市販製品を用いた試験的検証を実施し、これら課題への対応策の確立に向けた予備調査を実施した。
（キ）	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（機器やソフトウェアの真正性・完全性を確かめること）技術、動作監視・解析技術、異常検知時に制御システムの可用性を重視する防御技術等を開発する。	・技術開発を進めるとともに、真贋判定技術と動作監視解析技術を事業者環境で検証を行い、安全性と有効性の評価を実施した。 ・IoT 機器向け暗号実装技術では、当初性能目標を前倒しして達成し、最適化・高速化を行った。 ・2020 年東京オリンピック・パラリンピック競技大会に向けて、重要インフラ事業者への導入計画を着実に進めた。
（ク）	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 機器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、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。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）	・関係省庁と連携し、技術開発から実証実験、認証制度検討、グローバル協調にわたる総合的な研究開発計画を立案した。 ・研究開発計画に基づき公募により研究開発機関を決定し、概念設計を行う等研究開発を開始した。
（ケ）	総務省	総務省において、スマートシティにおけるプラットフォームに係るセキュリティ要件の具体化や所用の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を進める。	・「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発」については、上記公募に係る審査・採択を経て、2018 年度から取り組んでいる。
（コ）	総務省	総務省において、戦略的情報通信研究開発推進事業（SCOPE）のなかで、IoT 機器などのハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を実施する。	・2018 年度においては、IoT 部品・IoT 機器・IoT ネットワークについて階層を横断するセキュア化に向け、 IoT 部品のセキュア化のために AI 技術の利用によって未知の IoT 回路を比較的高い精度で不正回路か判定できる技術を、また、IoT 機器・ネットワークのセキュア化のために特定のモデル上で電力波形をはじめとする複数の外部特徴量から不正機能を検知する技術をそれぞれ開発した。
（サ）	内閣官房	内閣官房において、関係府省と連携しつつ、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、不正なプログラムや回路が仕込まれていないことの技術的検証等を行うための体制整備を図るとともに、そのために必要となる研究開発について関係施策を促進していく。	・研究開発戦略専門調査会において議論を実施し、技術検証体制の構築に向けた検討を進めた。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（シ）	総務省	総務省において、NICT を通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図り、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に向けて、試験運用を行った。
（ス）	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行う。	・総務省において、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技術を確立するため、周波数の利用状況の自動推定による広域ネットワークスキャン技術、広域ネットワークスキャンの無線通信量軽減技術に関する基礎技術の開発を行った。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月の諸施策の目標と実施方針）より			
・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 **・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・研究発**			
項番	担当府省庁	サイバーセキュリティ 2018	取組の成果、進捗状況
（セ）	内閣府	内閣府において、革新的研究開発推進プログラム（ImPACT）「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」により、機密情報を安全に伝送・保管できる通信ネットワークの構築を目指して量子暗号技術の研究開発を行う。	・量子暗号技術を応用したセキュアなデータ保存方法を開発し、模擬電子カルテデータを東京-名古屋-大阪-高知間（800km）で安全にデータ共有する実証実験に成功した。
（ソ）	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、研究開発を実施する。	・総務省において、量子鍵配送ネットワークの信頼性試験を継続した。鍵管理の高信頼性を実現し、ネットワークシステム全体の安全性向上に取り組んだ。Tokyo QKD Network 上に構築した情報理論的に安全な秘密分散ストレージシステムの技術と、量子鍵配送ネットワークの鍵管理システムの技術を活用し、JGN の広域ネットワーク上に模擬医療データの分散ストレージ機能を実装し、その動作実証を行った。光空間通信テストベッドに実装した物理レイヤ秘密鍵共有システムによる、見通し通信路における情報理論的に安全な鍵生成の高速化に取り組んだ。
（タ）	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、研究開発を実施する。	・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 2018 年度より開始（研究開発期間は 2018 年度～2022 年度）。
（チ）	内閣官房	内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。（再掲）	・2018 年 10 月に、法律家を中心とした有識者から構成される「サイバーセキュリティ関連法令の調査検討等を目的としたサブワーキンググループ」を立ち上げた。本サブワーキンググループは、サイバーセキュリティ関係法令集の策定を目的の 1 つとしているものであり、2019 年２月に第一回会合を開催した。

(ツ)	総務省 経済産業省	総務省及び経済産業省において、CRYPTREC 暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT 及び IPA を通じ、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。（再掲）	・総務省及び経済産業省において、CRYPTREC 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。 また、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、耐量子計算機暗号の研究動向調査及び鍵管理ガイドラインの作成に向けた検討を行った。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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、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			
項番	担当府省庁	サイバーセキュリティ 2018	取組の成果、進捗状況
(テ)	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 JTC1/SC27、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。（再掲）	・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た結果、ISO/IEC JTC 1/SC 27 においては ISO/IEC 27030 の作業文書(WD)第二版が発行され、ITU-T SG17 においては IoT セキュリティガイドラインをベースとした勧告案 X.sc-IoT の検討を 2018 年９月より開始した。
(ト)	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実施する。	・2019 年３月４日から８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、我が国初となるジャパン・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 42500 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。
(ナ)	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 JTC1/SC27 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。	・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（2018 年４月武漢会合、2018 年 10 月イェービク会合）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、特に 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いる。

(2) 中長期的な技術・社会の進化を視野に入れた対応

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、信頼性工学、心理学等の様々な社会科学的視点も含めて策定した「サイバーセキュリティ研究開発戦略」について、目下の課題を解決すべく、融合領域の研究動向についての調査等を検討する。	・研究開発戦略専門調査会において、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

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、「新・情報セキュリティ普及啓発プログラム」の改訂を行い、普及啓発施策の方向性と具体的な行動計画をとりまとめる。	・普及啓発・人材育成専門調査会等における議論を経て、2019 年 1 月のサイバーセキュリティ戦略本部において、「サイバーセキュリティ意識・行動強化プログラム」を決定した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（イ）	内閣官房	内閣官房において、家庭や教育現場、企業内等でのセキュリティ意識向上のため、緊急時における注意・警戒情報やサイバーセキュリティに関する役立ち情報等について、SNS 等を用いた発信を引き続き行うとともに、より効果的な手段について検討を行う。	・主に一般国民向けに、緊急時における注意・警戒情報やサイバーセキュリティに関する役立ち情報等について、媒体の特徴に合わせた情報発信を行った。
（ウ）	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。	・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にて、電話、メール、FAX 等で 13,185 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と情報受付を 413 件実施した。これを通じて、不審メールを 774 件入手した。入手した不審メール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。
（エ）	内閣官房	内閣官房において、主体的に普及啓発活動を行う動きが地域レベルでも促進されるよう、「情報セキュリティ社会推進協議会」等を活用しつつ、産学官民の連携・協力を通じて、必要な取組について検討を進める。	・普及啓発・人材育成専門調査会等における議論を経て、2019 年 1 月のサイバーセキュリティ戦略本部において、「地域における取組の支援」を重点的な対象の一つとした「サイバーセキュリティ意識・行動強化プログラム」を決定した。
（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。	・経済産業省において、電子署名の利活用に関するセミナー等を実施した。 総務省において、プラットフォームサービスに関する研究会の下にトラストサービス検討ワーキンググループを開催し、国際的な相互運用性の観点も踏まえつつ、トラストサービスの在り方について検討を行ったほか、トラストサービスワークショップの開催等を通じて、電子署名の普及促進を図った。
（カ）	経済産業省	経済産業省において、IPA、JPCERT/CC を通じて、情報漏えいの新たな手法や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、IPA を通じ、「緊急対策情報」を 13 件、「注意喚起情報」を 31 件、「安心相談窓口だより」を 9 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、セキュリティプレゼンター制度の運用などにより情報の周知を行い、セキュリティ啓発サイトや各種ツール類を用いて、対策情報の提供を行う。	・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、IPA において、セミナー等への講師派遣（150 件）や展示会への出展（26 件）等による情報の周知・提供を実施した。 ・セキュリティプレゼンター制度を運用し、登録したセキュリティプレゼンター（2018 年度新規登録 142 名）が活躍する地域で自主的に開催するセミナー等を支援することにより、自主的普及活動の拡大を図った。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	取組の成果、進捗状況
（ク）	内閣官房	内閣官房において、行動計画に基づき、NISC が中核的役割を担いつつ、各府省庁や民間の取組主体と協力して、「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催や情報発信等を通じ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。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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、引き続き内容の見直しを行うとともに、普及及び活用を促す取組を行う。	・「インターネットの安全・安心ハンドブック」（旧称：ネットワークビギナーのための情報セキュリティハンドブック）の内容見直しを行い、各種媒体にて無料で配信するとともに、都道府県警察と連携して普及活動を行った。
（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、10,065 件ダウンロードされた。
（サ）	総務省	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等を行う。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。	・子どもたちのインターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等に対する、学校等の現場での出前講座である e-ネットキャラバンを、情報通信分野等の企業・団体と総務省・文部科学省が協力して全国で開催した。2018 年度は、2018 年４月から 2019 年１月までの間、2,314 件の出前講座を実施した。また、2018 年 12 月に、自画撮り写真の交換に端を発した脅迫被害、SNS 上の知人による誘い出しに関する事例の追加等を行い、「インターネットトラブル事例集」　（2018 年度版）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。	・当初の予定通り、ネットモラルキャラバン隊による普及啓発活動を実施した。
（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、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、2019 年１月 28 日～２月１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、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、2019 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 14 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 55,524 点、ポスター5,421 点、４コマ漫画 7,292 点、書写（硬筆）2,395 点、合計 70,653 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 21 校の応募の中から「優秀活動事例賞」に５校、最も優れた活動に取り組んでいる１校に「文部科学大臣賞」を授与した。この取組を通じて、若年層の情報モラル/セキュリティの醸成と向上に寄与した。

（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、家庭や学校からインターネットを利用する一般の利用者を対象として情報セキュリティに関する啓発を行う安全教室について、全国各地の関係団体と連携し引き続き開催していく。	・経済産業省において、IPA を通じて、 ・全国各地域で、NPO 等の団体との連携により「インターネット安全教室」を合計 128 回開催し、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い、 小中高校生からシニア層まで合計約 12,252 名が参加した。 ・各地域団体による講習能力の向上を図る講師トレーニングを全国５箇所において開催し、合計約 189 名が参加した。

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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	サイバーセキュリティ 2018	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。特に、セキュアな公衆無線 LAN 環境の実現に向けて、各種ガイドラインの改定や教育コンテンツを活用した周知・啓発、データ利活用施策との連携、セキュアな公衆無線 LAN 環境の優良事例の調査・整理及びこれを踏まえた所要の政策支援等の取組を行う。	・総務省において、オンライン教育コンテンツ等を活用して公衆無線 LAN のセキュリティ対策に係る啓発を行った。
（ツ）	経済産業省	経済産業省において、IPA を通じて、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の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。	・経済産業省において、IPA を通じ、 ・国民全体に向けた活動として、2018 年 7 月に、「情報セキュリティ白書 2018」を発行した。 ・「情報セキュリティ脅威と倫理に関する意識調査（2018 年版）」を実施し、2018 年 12 月に報告書を公開した。 ・「IT システム・サービスの業務委託におけるセキュリティに係る責任範囲に関する調査」を実施し、2018 年３月に報告書を公開した。 ・「サイバーセキュリティ経営プラクティス」を 2019 年３月に公開した。 ・「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」を実施し、2019 年４月に報告書を公開した。

5. 推進体制

新戦略（2018 年 7 月 27 日閣議決定。2018 年 7 月～2021 年 7 月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、新戦略に基づく諸施策が着実に実施されるよう、新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** **・2020 年東京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	サイバーセキュリティ 2018	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推進した。また、情報共有のための環境については、継続して改善を実施している。

（イ）	内閣官房	内閣官房において、2018 年戦略に基づく諸施策が着実に実施されるようにするとともに、全ての主体によるサイバーセキュリティに関する自律的な取組を促進するため、各種イベント等における説明会の開催などを通じて、国内外の関係者への 2018 年戦略の発信を積極的に行い、周知を図る。	・内閣官房において、2018 年戦略について、国内外の関係機関への配付や国際会議・普及啓発イベントにおける関係者への配布などにより、広く国内外へ周知広報するため、カラー冊子を制作した。 ・内閣官房及び関係省庁において、カラー冊子を活用し、各種セミナーでの説明等を通じて、計 79 件のイベントで、国内の関係者 6,500 名超、国外の関係者 1,500 名超に対して、2018 年戦略の発信を行い、周知を図った。
（ウ）	内閣官房	内閣官房において、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）	・内閣官房が、関係省庁及び重要インフラ事業者とともに、重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、政府の初動対処態勢を整備するとともに、対処要員の能力強化を図った。
（エ）	内閣官房	内閣官房において、「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に向けたセキュリティ基本戦略（Ver.1）」（2017 年３月 21 日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。 具体的には、オリパラ競技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て、リスク評価に基づく対策の促進と、情報の共有、インシデント発生時の調整役となるための組織であるサイバーセキュリティ対処調整センター（政府オリンピック・パラリンピック CSIRT）の整備を推進する。 2018 年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。 また、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピック CSIRT）については、2018 年度末を目途に構築し、2019 年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。（再掲）	・引き続き、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象としたリスクマネジメントの促進や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進した。 ①　『リスクマネジメントの促進』 ・重要サービス事業者等（東京都、近郊県及び地方競技会場）を対象とする第３回リスクアセスメントの実施を依頼、各事業者等から提出された実施結果について、重要サービス分野内及び重要サービスを分野横断的に分析し、各事業者等へフィードバックを実施した。 ・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について、第１回として、電力、通信、水道、鉄道、放送分野等から５者を対象に実地検証、全重要サービス分野から 20 者を対象に書面検証を実施し、結果の取りまとめを行った。 ②　『対処態勢の整備』 ・サイバーセキュリティワーキングチーム等における検討を更に進め、大会に向けたサイバーセキュリティ体制の運用方針を関係府省庁、大会組織委員会、東京都等と協議の上、決定した。 ・サイバーセキュリティ対処調整センターを構築した。

別添３　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・注意喚起等）

＜別添３　目次＞

別添３－１　「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 197

別添３－２　サイバーセキュリティ基本法に基づく監査 200

別添３－３　重点検査 206

別添３－４　高度サイバー攻撃への対処 208

別添３－５　教育・訓練に係る取組 210

別添３－６　なりすまし防止策の実施状況 217

別添３－７　暗号移行 219

別添３－８　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 221

別添３－９　NISC 発出注意喚起文書及びサイバーセキュリティ対策推進会議決定等232

別添３－10　政府機関等に係る 2018 年度の情報セキュリティ インシデント一覧 234

別添３－11　政府のサイバーセキュリティ関係予算額の推移 238

別添３－１　「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

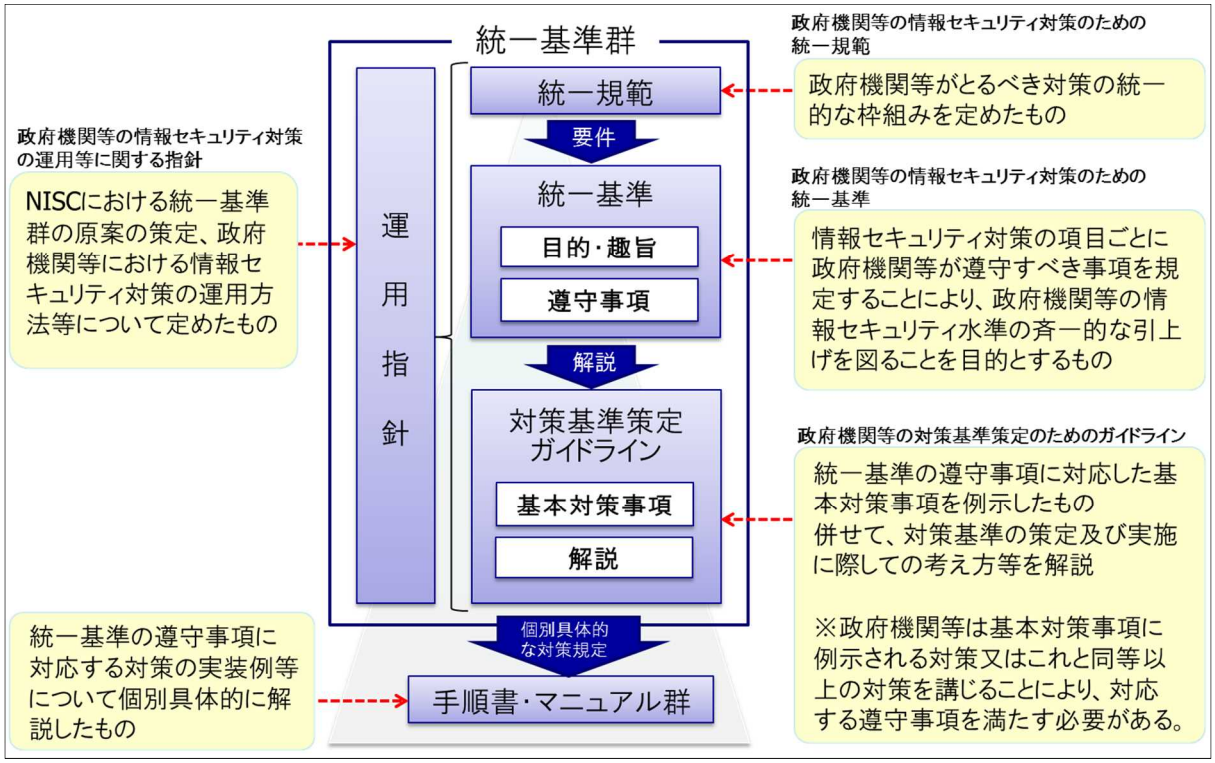
１　概要

「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、2018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。

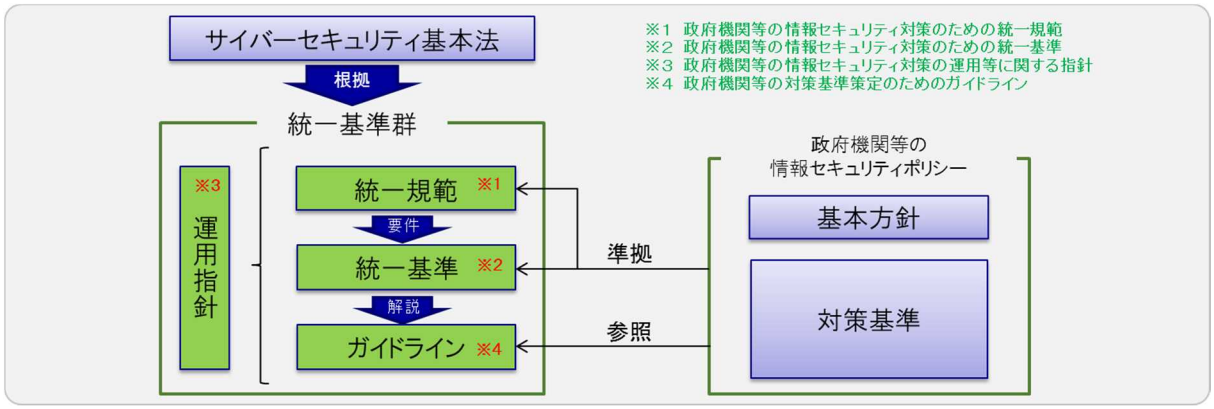
統一基準群（平成30年度版）の文書構成は、図表１のとおりである。

図表１　統一基準群の文書構成



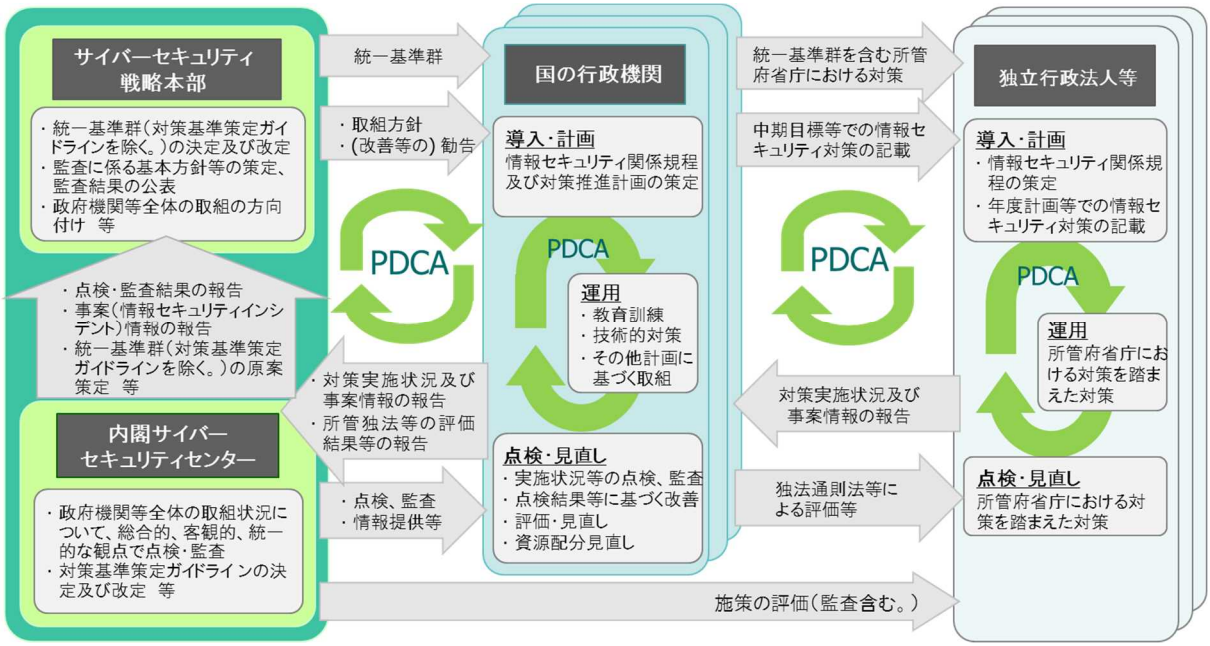
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等の情報セキュリティ対策のための統一基準（以下「統一基準」という。）」と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（図表２）。

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

最近のサイバー攻撃は、未知の不正プログラムの使用や脆弱性情報の公開直後の攻撃など、脅威が深刻化・巧妙化しており、国家の関与が疑われる大規模な事案も発生している。また、世界的規模でのランサムウェアによる被害は、標的型攻撃に加え、ばらまき型攻撃の危険性をあらためて認識させた。このようなサイバー攻撃から、行政サービスを守る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、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統一基準群（平成30年度版）が決定された。

統一基準群（平成30年度版）における主な改定内容を、以下に示す。

（１）将来像を見据えたサイバーセキュリティ対策の体系の進化

①情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止、②IT資産管理の自動化とそれによる脆弱性への迅速な対応、③データ保護による情報漏えい対策の導入を、今後政府機関等が目指すべき３本の柱とし、これらの対策の導入を推奨。

（２）政府機関等のサービスの利用者の側に立った対策

政府機関等は、自らの情報システムのサイバーセキュリティ対策に加え、国民が安心して安全にウェブサイト等を通じて行政サービスを利用できるよう、利用者側に立った追加的な対策を規定。

（３）政府機関等の自律的な能力向上への誘導（PDCA サイクルの効果的運用）

一巡した府省庁監査の結果から得られた知見を踏まえ、自らの対策状況を評価し、より効果的な改善に繋げるべく、政府機関等の自律的なPDCAサイクルの更なる循環を促す対策を規定。

（４）業務形態に対応した規定の整備

多様な業務形態が存在する独立行政法人等に目を向け、これらを踏まえたサイバーセキュリティ対策を規定。

別添３－２　サイバーセキュリティ基本法に基づく監査

１　2018 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、2018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。

なお、監査事務の一部をIPAに委託しているが、IPAはその技術力及び専門的な知識経験を活用して、監査事務をNISCとともに推進し、各法人の多様な業務内容を理解した上で、情報セキュリティ水準の向上に必要な助言をNISCに提示している。NISCは、IPAの監査内容を評価し、提示された助言が統一基準群のもとで、現実的かつ適切なものであるかの観点で確認し、各所轄府省庁を通じ各法人に通知している。各法人はこの助言に沿って、セキュリティ対策を実施し、情報セキュリティ水準の向上を図ることができている。

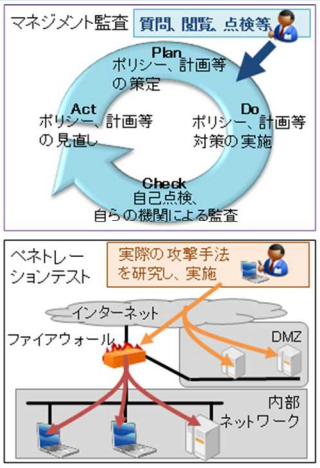
監査の実施内容

(1) マネジメント監査

- **国際規格において基本的な考え方である組織全体としてのPDCAサイクルが有効に機能しているかとの観点から検証する。**
- **対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。**

(2) ペネトレーションテスト

- **疑似的な攻撃を実施することによって、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。**



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

2018 年４月から 2019 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 22 府省庁）のうち、12 の府省庁を対象とした。

（３）マネジメント監査の実施内容

「政府機関等の情報セキュリティ対策のための統一基準群」等に基づく施策の取組状況について、各府省庁における組織・体制の整備状況、サイバーセキュリティ対策の実施状

況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかとの観点を中心に監査を実施した。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、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、2017 年度に被監査主体であった府省庁に対しては、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 2017 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

・行政事務従事者に遵守してほしい事項をまとめた「情報セキュリティハンドブック」を行政事務従事者に配布するなど、サイバーセキュリティの普及啓発に向けた取組を行っていた事例

・電磁的記録等からの不用意な情報漏えいを防止するための措置の一環として、PDF 作成時にプロパティ情報に作成者情報が入らないよう、端末のソフトウェアを制御していた事例

・行政事務従事者が業務にかかる脅威の可能性を認知した場合に、報告できる窓口を整備した上で、報告のあった脅威に対するリスク評価を行い、リスクを軽減する対策を実施していた事例

・システムのログイン時に、情報セキュリティに関する事項等について同意させてシステムの利用を可能とすることで、システムの情報セキュリティ水準の維持を徹底していた事例

② 主な助言等

2018 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 2017 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

2017 年度に監査を実施した 11 府省庁に対して、2017 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 2018 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、2017 年度から始まった各府省庁における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。2017 年度の監査においては、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も見られた。2018 年度の監査においては、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の、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。

フォローアップにおいて、各府省庁の 2017 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、計画に基づいて改善されており、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

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

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、使用されているパスワードについて、その保存方法

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。

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

2018 年４月から 2019 年３月までの間

今後、2020 年東京オリンピック・パラリンピック競技大会の前年度までの間に、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予定としている。

（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、30 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

・情報セキュリティ委員会を危機管理等の全組織的リスク管理態勢の枠組みの中に位置づけ、情報セキュリティリスクを全組織的リスクとして管理していた事例

・他の組織で発生した情報漏えい事案を参考として、対応訓練を実施していた事例

・情報の格付や情報を所持して外出する際の注意喚起等、周知徹底が必要な事項を目に

つきやすいところに適宜掲載していた事例
・委託先の情報セキュリティ対策の履行状況を確認する際に、委託先が独立監査法人等に依頼して実施した情報セキュリティ監査結果を、委託先から入手する等により、効率的に確認していた事例
・システムごとのライフサイクルに応じて、予算を考慮した運用計画を詳細に策定し、計画が完了するたびに具体的な導入を進めていた事例

② 主な助言等

2018 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 2017 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

2017 年度に監査を実施した独立行政法人等 33 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、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。

2018 年度は 30 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、2017 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、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

今後、2020 年東京オリンピック・パラリンピック競技大会の前年度までの間に、全ての独立行政法人及び指定法人に対しペネトレーションテストを実施する予定としている。

（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、30 の法人が運用するインターネットに接続する基幹 LAN システム及び重要な情報を取り扱う情報システムの中から選定した 31 の情報システムを対象とした。

（３）ペネトレーションテストの実施内容

攻撃者が実際に用いる手法での疑似的な攻撃による情報システムに対しての侵入可否調査を独立行政法人情報処理推進機構（IPA）に事務の一部を委託して実施した。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、使用されているパスワードについて、その保存方法が適切でない、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。

別添３－３　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
リモートアクセスにおける情報セキュリティ対策	リモートアクセスの利用状況及び情報漏えい対策の実施状況	リモートアクセス環境の導入が進んでいる状況を踏まえ、そのセキュリティ対策の実施状況を把握するため。
サポートが切れるOS・ソフトウェア対策	Windows　7のサポート終了に伴う対応状況	各政府機関においてサポート終了するOS・ソフトウェアに係る対応が、適切に検討・計画されていることを確認するため。
	Office 2010のサポート終了に伴う対応状況	
ソフトウェアに関する脆弱性対策	情報システムで利用しているソフトウェアの公開脆弱性への対策実施状況	各政府機関において、パッチ適用及びソフトウェアのアップデート等の対策が適切に行われていることを確認するため。

（１）リモートアクセスにおける情報セキュリティ対策

各府省庁における職員や委託事業者へのリモートアクセス環境の導入が進んでいる状況を踏まえ、利用状況及びセキュリティ対策状況について検査を実施した。

リモートアクセス環境の導入状況については、大多数の府省庁で導入されている状況である。また、今後新たにリモートアクセス環境の導入を検討しているとの回答も見られた。

リモートアクセス環境の安全な利用のための主な対策としては、通信内容の暗号化(VPNやhttps等のTLSプロトコルを用いたもの)、端末の盗難対策としてディスクの暗号化、端末自体に情報を持たないシンクライアント端末の利用やセキュアブラウザを活用するなどのセキュリティ対策があり、複数の対策を組み合わせた対策が取られていることが確認できた。

また、委託事業者が利用するためのリモートアクセス環境におけるセキュリティ対策については、事前申請内容に基づいたリモートアクセスポートの適切な管理や委託事業者が実施するセキュリティ対策要件の提示を求めるなどの対策が行われていることが確認できた。

以上のように、リモートアクセスにおける情報セキュリティ対策はおおむね良好に実施されていることが確認できた。今後は、更にセキュリティを高める対策として委託事業者への監査やリモートアクセスログの監査といった対策が考えられる。

（２）サポートが切れるOSソフトウェア対策

Windows 7・Windows Server 2008 及び 2008 R2延長サポート終了（2020年１月14日）、Microsoft Office 2010延長サポート終了（2020年10月13日）に伴うセキュリティ対応状況については、最新のOSやソフトウェアに更新される、若しくはシステム更改時にあわせ更新

する、当該ソフトウェアをアンインストールするなど、適切な対応が実施される予定であることが確認できた。

サポートが終了したOS、ミドルウェア、アプリケーション（以下、「各種ソフトウェア」と言う。）の利用は、情報セキュリティ関連の脆弱性を修正するための修正プログラムが原則としてベンダから提供されなくなり、これらの各種ソフトウェアを利用している情報システムにおいてウイルス対策ソフトウェアを導入するなどの対策を講じていたとしても、不正プログラム感染や不正アクセスによる情報漏えい等のリスクが高まることから、今後も、端末やサーバで使用する各種ソフトウェアについてはサポート期間を適時確認し、サポート終了までにソフトウェアを更改する等の必要な対応を徹底し、計画的にシステム調達や更新を行っていく必要がある。

（３）ソフトウェアに関する脆弱性対策

統一基準において、サーバ、通信回線装置、及び端末の設置又は運用開始時に、利用するソフトウェアの脆弱性対策を求めていること、また、日々発見される脆弱性に対して、適切なパッチの適用及びソフトウェアのバージョンアップは不可欠であることから、これらの実施状況について検査を実施した。

脆弱性対策の基本となる、情報システムで利用しているソフトウェアのバージョン管理については、おおむね全てのシステムにおいて何らかの方法で適切な管理がなされている状況である。管理方法としては、IT資産管理ソフトウェアの利用、電子化又台帳による一元管理などがあげられる。

脆弱性対策計画の策定及び実施状況については、おおむね全てのシステムにおいて自府省庁独自又は運用業者と連携するなどして、適切に行われている。クラウド利用の進展に伴い、クラウド事業者の責任において脆弱性対策計画が策定され、実施されるとの回答も一定数見られた。

ソフトウェアの脆弱性に関する情報源としては、NISC、IPA、JPCERT等の組織からの通知が最も多く利用されており、他にも当該ソフトウェアのWebサイトやセキュリティ関連ニュース、開発元や保守業者からの通知が多く利用されている状況である。数は少ないが、商用の脆弱性情報提供サービスを契約し、積極的に情報収集しているシステムも見られた。

脆弱性対策状況を確認する頻度としては、大半のシステムにおいて、脆弱性情報を入手するたびに、又は定期的に確認が行われている。

以上のように、ソフトウェアに関する脆弱性対策はおおむね良好に実施されていることが確認できた。今後は、IT資産管理ソフトウェアの活用等による省力化の推進や、クラウド利用時のクラウド事業者による脆弱性対策実施状況を定期的に把握するなどにより、脆弱性対策をより効率化、高度化していくことが適切と考えられる。

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。

別添３－４　高度サイバー攻撃への対処

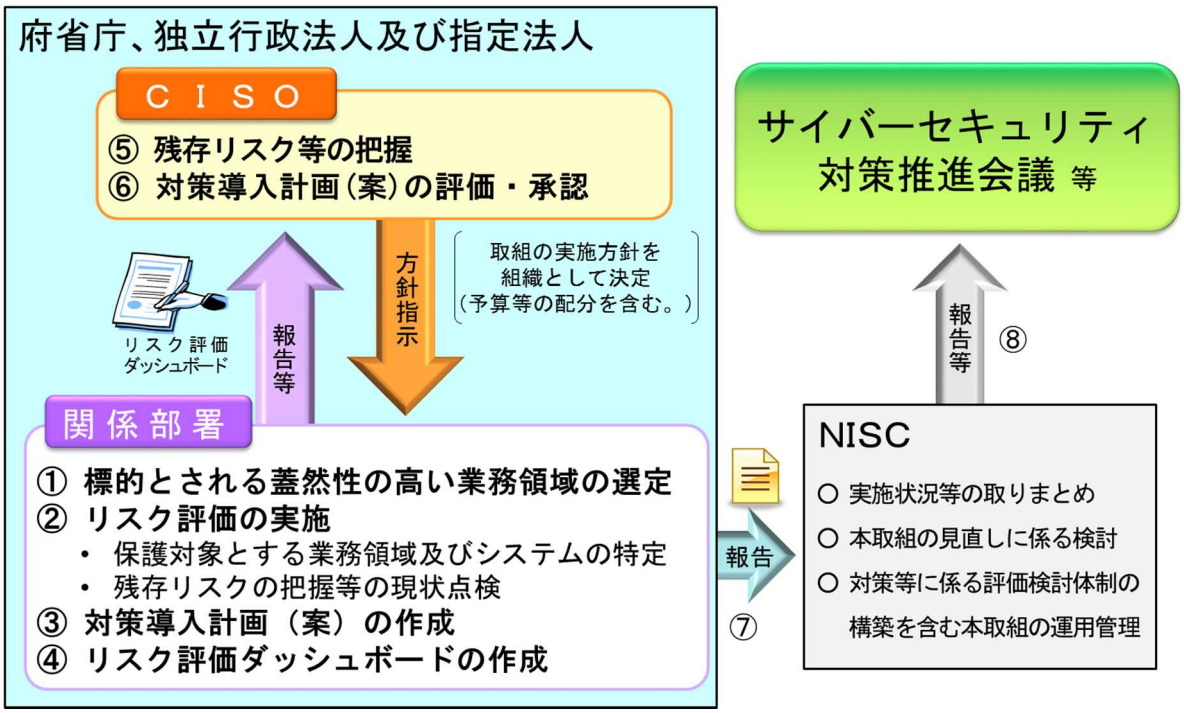
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

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。

2018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、2017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業務及び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130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ほぼ全て講じられており、標的型攻撃に対する対策が実施され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。

2018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は、2017年度と比較し、高度サイバー攻撃の標的とされる蓋然性の高いシステムは横ばいで推移しているが、対象となる業務が増加している状況である。高度サイバー攻撃への対策は、大きな改善まではいかないが、着実に対策の強化は進められている状況である。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300の業務領域に使用されるおよそ240の情報システムを対象として、各独立行政法人等のCISOの下で対策強化が実施された結果、ネットワークセグメントに対する対策やユーザ端末係る対策を中心に標的型攻撃に対する対策の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３－５　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。

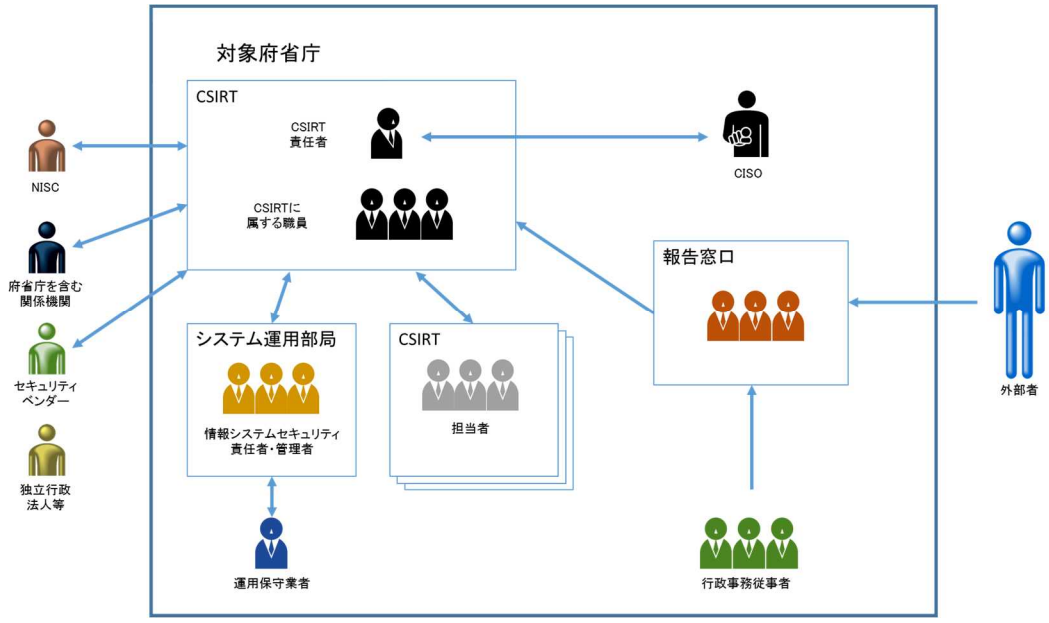
（２）概要

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。

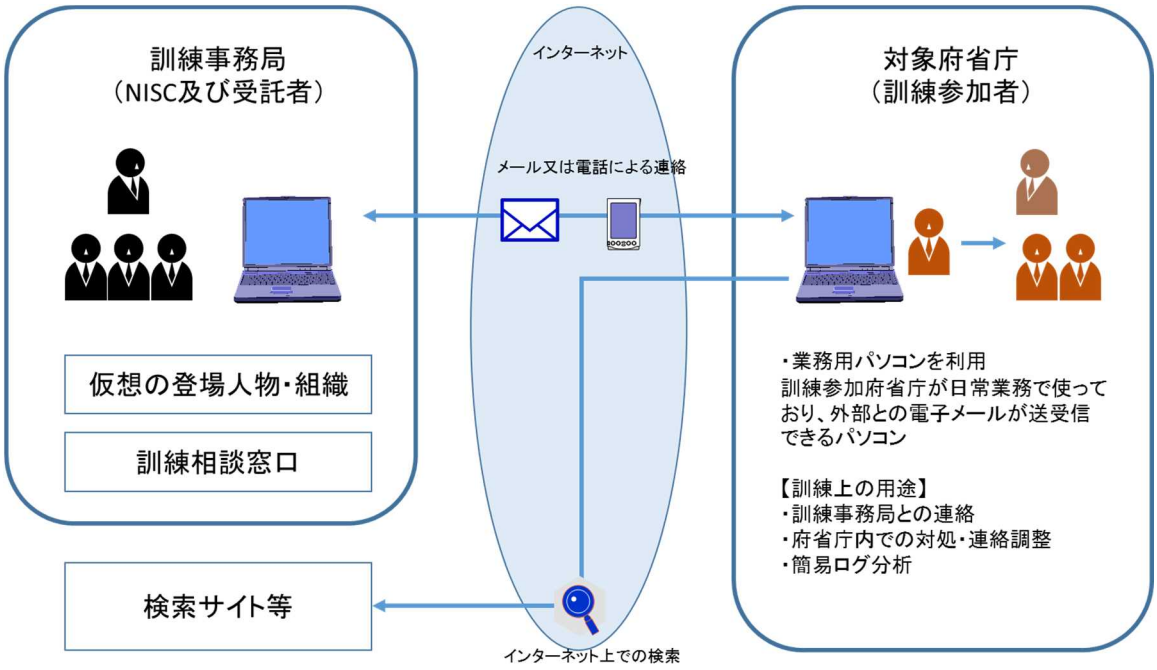
訓練参加者は、府省庁内外の様々な登場人物を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、通信ログ等の分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

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200人（全22府省庁参加）

（４）訓練時期

2019年１月～２月

（５）まとめ

多くの府省庁においてCISOが参加したことにより、より緊張感のある訓練が実施され、組織的対処能力の向上が図られた。今年度は訓練直後に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、2019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	2018 年 ６月～ 11 月	【CSIRT 会合】 ・SOC、CSIRT の成熟度の考え方と、現場で起きていること ・CSIRT 要員が身につけておくべき教養 ・不正アクセス事案に学ぶインシデント対処　ほか	NISC 職員、 外部講師	延べ約 90 名 （３回開催）
2	2018 年 ７月～ 2019 年 ３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 29・30 年度のトピック　ほか	外部講師	延べ約 200 名 （７回開催）
3	2019 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 ・サイバー攻撃の情勢 ・インシデント対処のプロセス ・ワークショップ　ほか	外部講師	延べ約 30 名 （３回開催）
4	2019 年 １月	【CSIRT 向け実機演習】 ・サイバー攻撃の手口 ・Web サイトへのサイバー攻撃 ・組織内部への侵入を狙った攻撃　ほか	外部講師	延べ約 40 名 （２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	2018年 ７月～ 2019年 ３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29・30年度のトピック　ほか	外部講師	延べ約790名 （７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	2018年 ９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の改定ポイントについて	NISC職員	延べ357名 （２回開催）
2	2018年 11月	統一基準群に基づく情報セキュリティ監査について ・基礎編　監査の基本知識、情報セキュリティ監査の解説 ・実践編　監査の実施、監査所見の演習	NISC職員	延べ239名 （２回開催）
3	2018年 12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	外部講師 NISC職員	延べ224名 （２回開催）

4	2019 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	延べ 265 名 （２回開催）

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に関する理解を深めるとともに、組織運営の在り方等について検討させるための研修を実施した。

（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

2018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座学や実機を用いた演習を４回実施した。

ケーススタディで学ぶインシデントハンドリングにおいては、７人の講師・アシスタントの指導の下、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少人数制のディスカッションを行ったほか、インシデント対応のため実機を用いた実習を行い、インシデントハンドリングを体験した。

No.	時期	テーマ
1	2018 年 ８月	【座学①】 1. サイバーセキュリティ戦略等について

		2.「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 3. 平成 31 年度機構・定員要求等について
2	2018 年 10 月	【座学②】 1. 脅威傾向と組織特性の分析 2. サイバーセキュリティ月間について
3	2019 年 １月	【座学③】 1. ケーススタディで学ぶインシデントハンドリング 2.「IT 調達に係る国の物品等又は役務の調達保身及び調達手続に関する関する申合せ」についての意見交換
4	2019 年 2 月	【座学（演習）④】 1. インシデント対応のためのサイバーセキュリティ実習

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ための研修を実施している。

（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)[1]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：2018 年８月～2018 年 12 月

受講者数：約 50 名

＜カリキュラム概要＞

①CISSP の概要	⑨セキュリティエンジニアリング(2)
②セキュリティとリスクマネジメント(1)	⑩通信とネットワークセキュリティ(1)

[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。

③セキュリティとリスクマネジメント(2)	⑪通信とネットワークセキュリティ(2)
④セキュリティの運用(1)	⑫セキュリティの評価とテスト
⑤セキュリティの運用(2)	⑬ソフトウェア開発セキュリティ(1)
⑥アイデンティティとアクセスの管理	⑭ソフトウェア開発セキュリティ(2)
⑦資産のセキュリティ	⑮まとめと学力考査
⑧セキュリティエンジニアリング(1)	

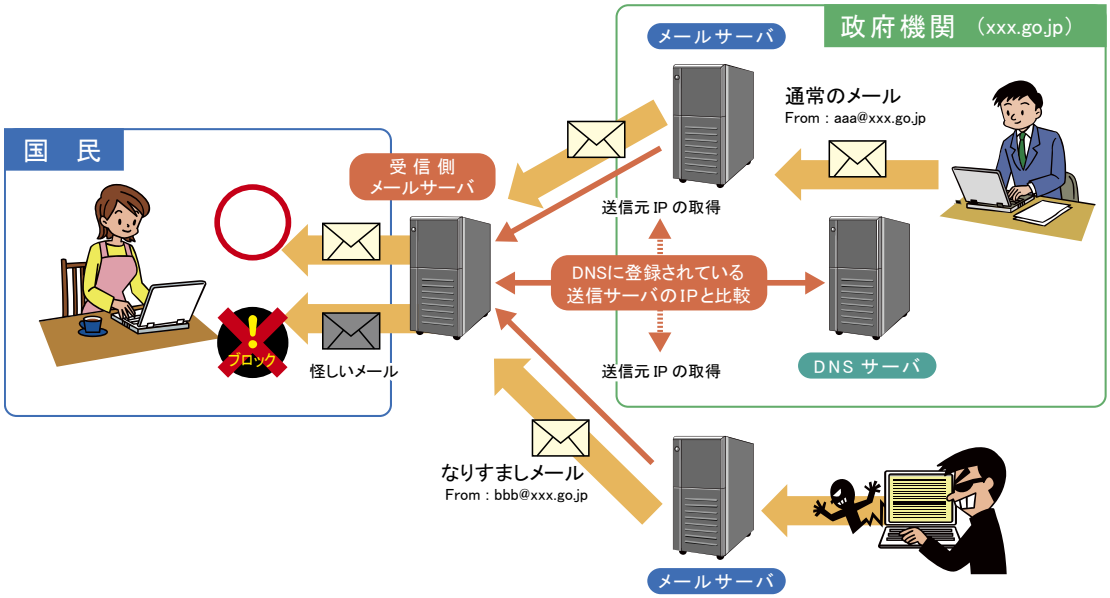
別添３－６　なりすまし防止策の実施状況

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
2018 年１月末	74.5%	11.7%	13.8%
2019 年１月末	69.7%	13.6%	16.7%

※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。主な原因として考えられるのは、この１年間で、政府機関のドメインの全体の１割程度が消滅し、ほぼ同数の新たなドメインが取得されており、総数は、横ばいで推移しているところ、新規に取得されたドメインの多くが適切な設定がなされてなかったことが挙げられる。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８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３－７　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ている。なお、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のうち、発行済み電子証明書の有効期間が残存し、やむを得ない場合については2019年度末まではその電子証明書を検証可としている。

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

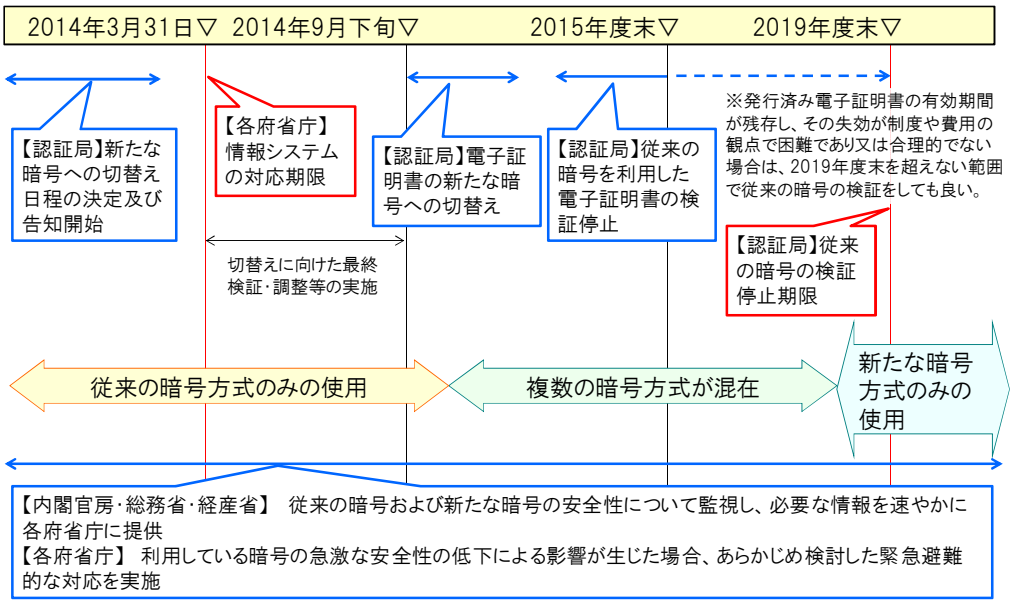
- 各府省庁が保有する情報システムの新たな暗号方式への対応時期　⇒「2013年度末まで」
- 新たな暗号方式による電子証明書の発行開始可能時期　⇒「2014年度早期」
- 従来の暗号方式による電子証明書の検証（有効性の確認）終了可能時期　⇒「2015年度早期」

（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



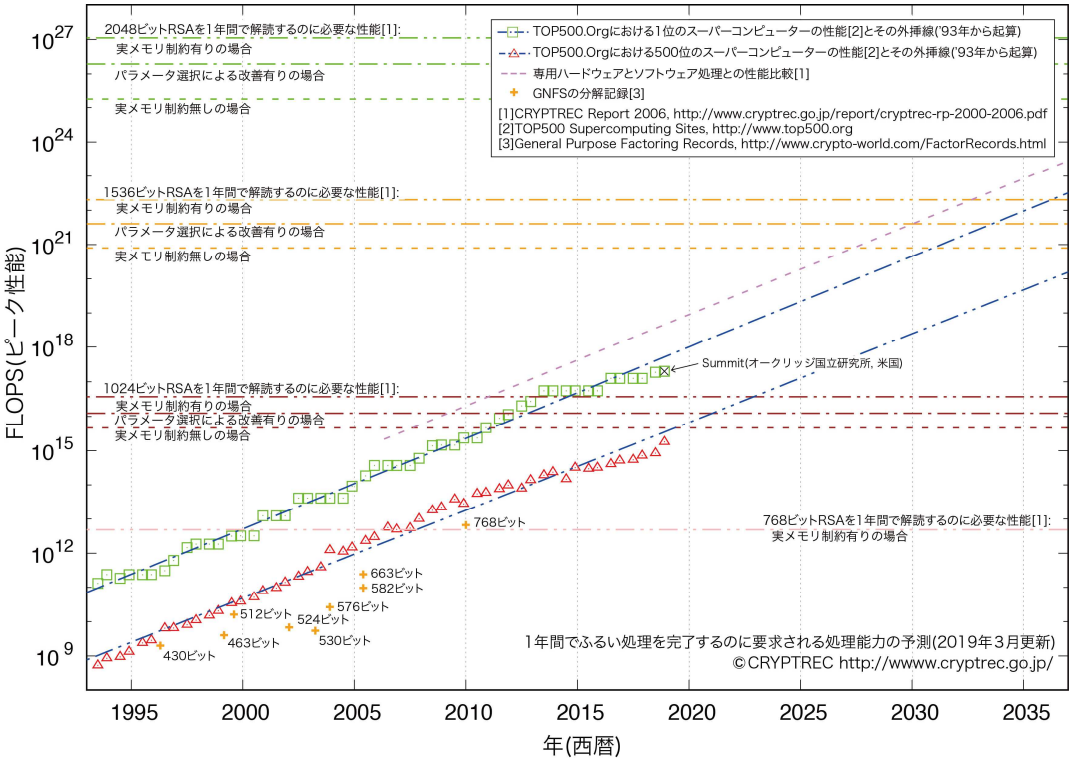
[4] https://www.nisc.go.jp/conference/suishin/index.html#2012_5
（第８回情報セキュリティ対策推進会議、2012 年 10 月 26 日）

（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３－８　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

１　調査目的

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[6]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

国立大学法人：86法人

大学共同利用機関法人：４法人

計　186法人（2019年３月末日現在）

（２）調査時点

独立行政法人、指定法人及び国立大学法人等　2018年12月末日

[6] 本調査では、国立大学法人及び大学共同利用機関法人を「国立大学法人等」という。

３　調査結果

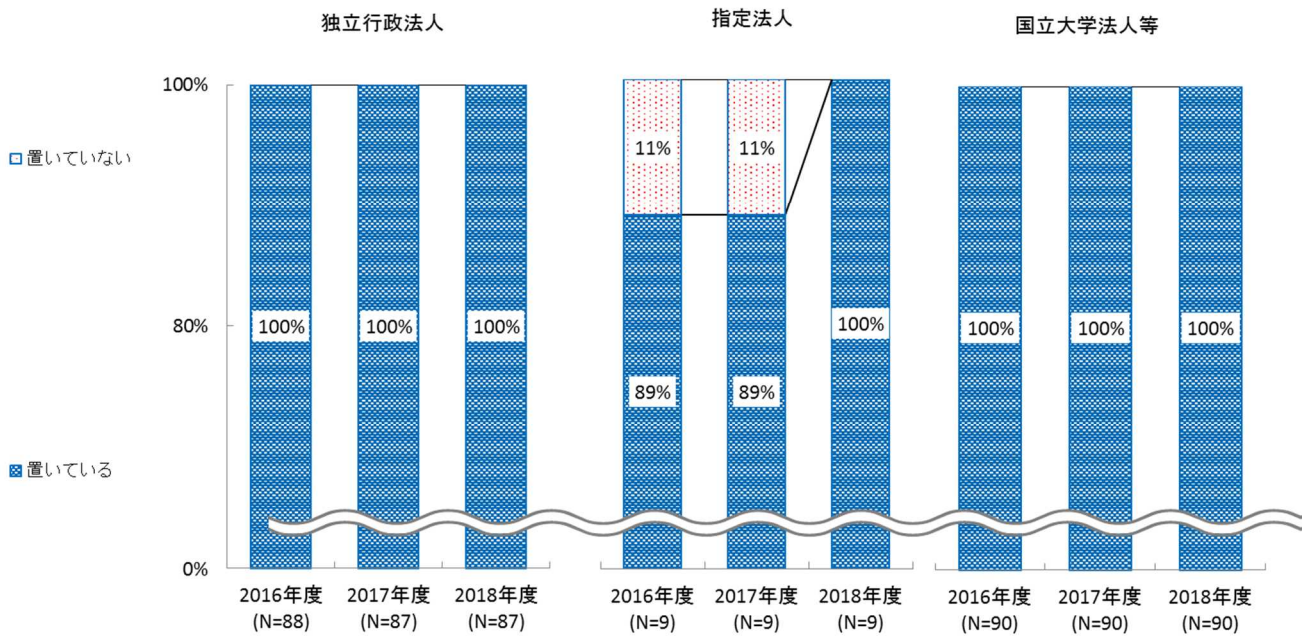
独立行政法人、指定法人及び国立大学法人等の調査結果については以下のとおりである。

また、構成比は小数点第１位を四捨五入しているため、合計しても必ずしも 100%となるとは限らない。

（１）情報セキュリティ対策の導入・計画

①　最高情報セキュリティ責任者（CISO）の設置状況

図表１　CISOの設置状況[7]



- 独立行政法人

  CISOを置いている法人は、87法人全てである。

- 指定法人

  CISOを置いている法人は、2017年度の8法人（89%）から9法人（100%）に増加している。

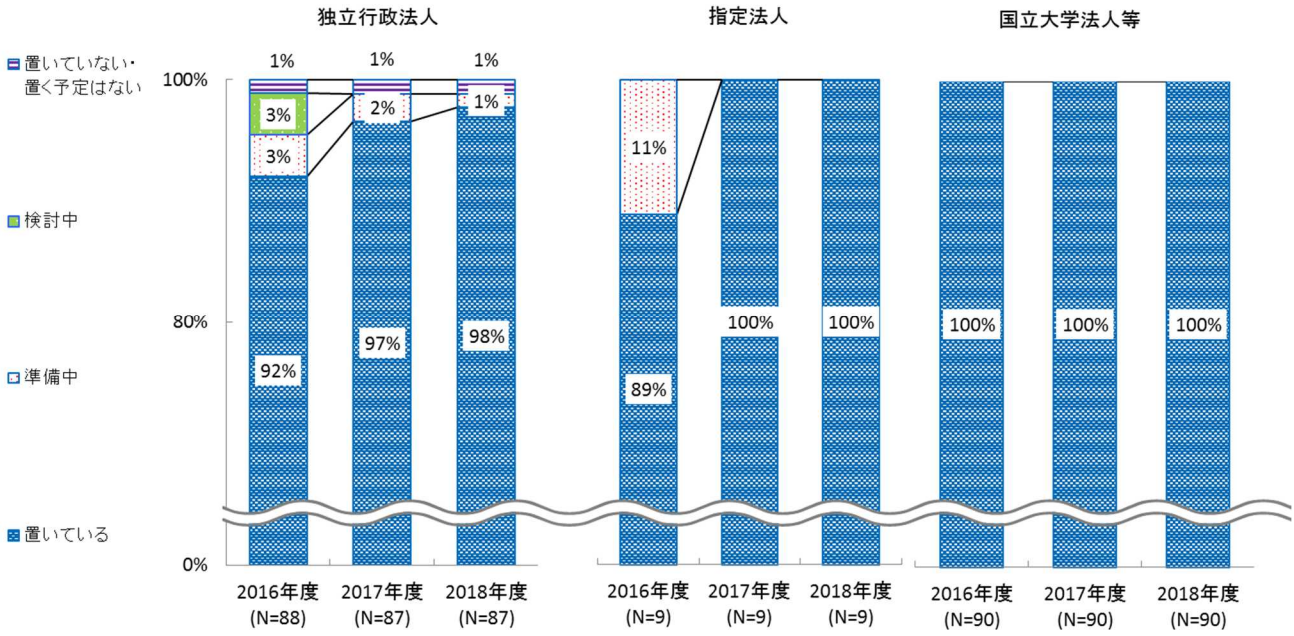
- 国立大学法人等

  CISOを置いている法人は、90法人全てである。

[7] 図表中における(N=)は、法人の数を表す。

② 情報セキュリティ委員会の設置状況

図表２　情報セキュリティ委員会の設置状況[8]



・ 独立行政法人

情報セキュリティ委員会を置いている法人は、2017年度の84法人（97%）から85法人（98%）に増加している。

・ 指定法人

情報セキュリティ委員会を置いている法人は、９法人全てである。

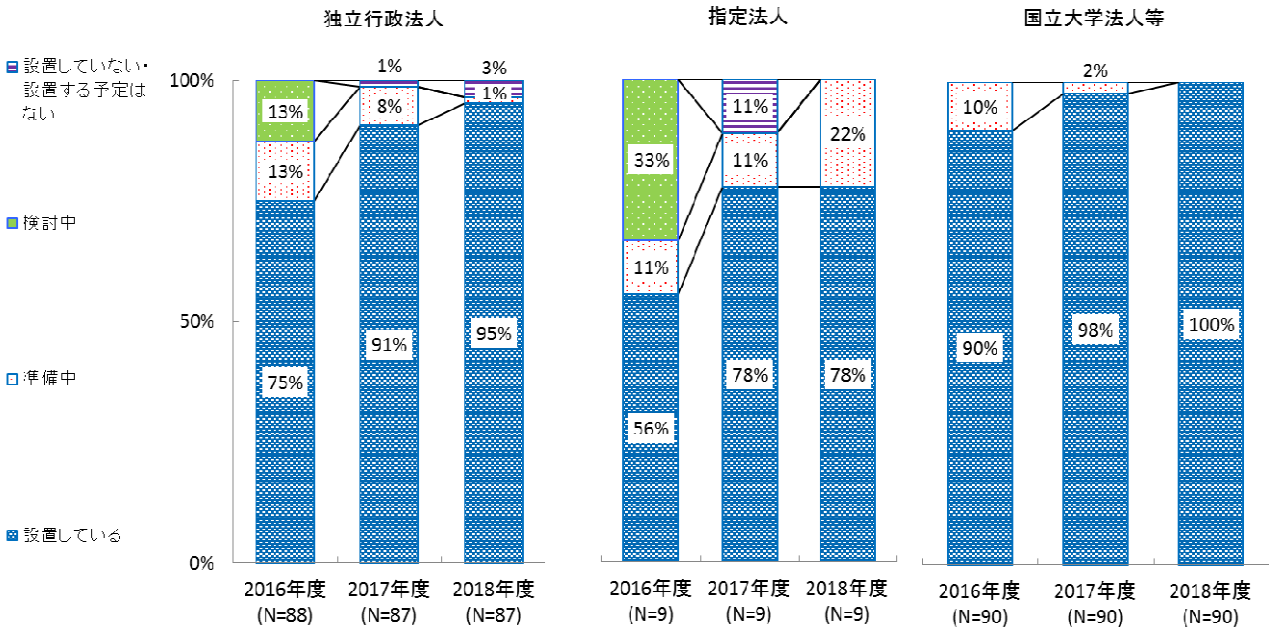
・ 国立大学法人等

情報セキュリティ委員会を置いている法人は、90法人全てである。

[8] 図表中の検討中について、「検討中」と「準備中」の違いが不明確との意見があったため、2017 年度からの調査の選択肢から「検討中」を削除した。以降の③ CSIRT の設置状況、④ 情報セキュリティポリシーの策定状況も同様である。

③　CSIRT（Computer Security Incident Response Team）の設置状況

図表３　CSIRTの設置状況



・独立行政法人

CSIRTを設置している法人は、2017年度の79法人（91%）から83法人（95%）に増加している。

・指定法人

CSIRTを設置している法人は、2017年度の7法人（78%）から変化していない。

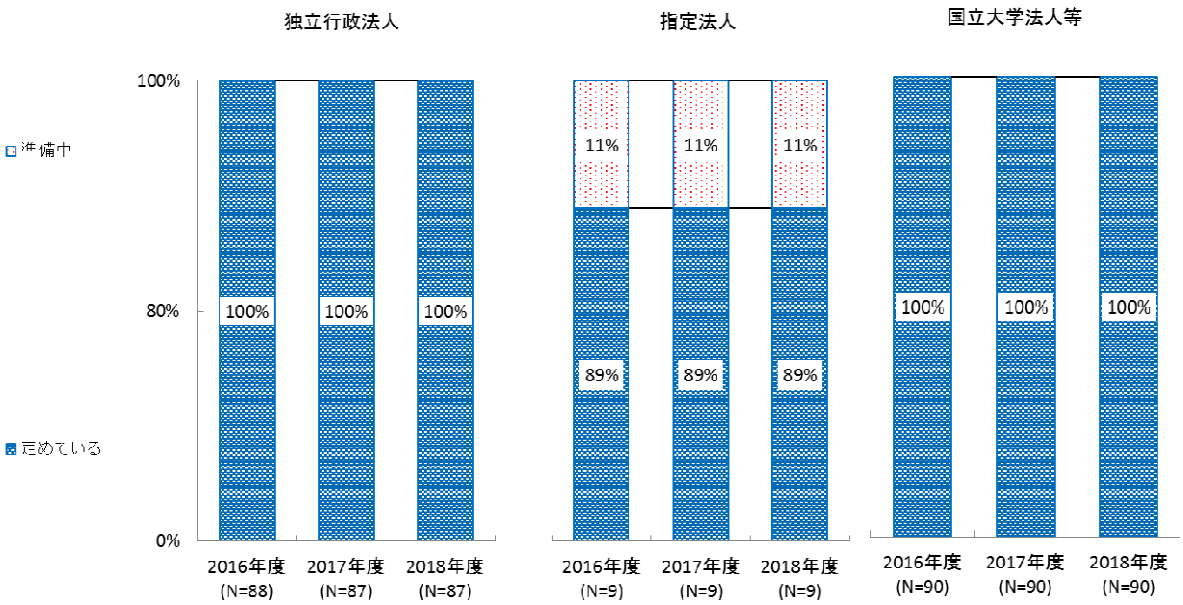
準備中が1法人（11%）から2法人（22%）に増加している。

・国立大学法人等

CSIRTを設置している法人は、2016年度の88法人（98%）から90法人（100%）に増加している。

④　情報セキュリティポリシーの策定状況

図表４　情報セキュリティポリシーの策定状況



・ 独立行政法人

情報セキュリティポリシーを定めている法人は、87法人全てである。

・ 指定法人

情報セキュリティポリシーを定めている法人は、８法人（89%）である。

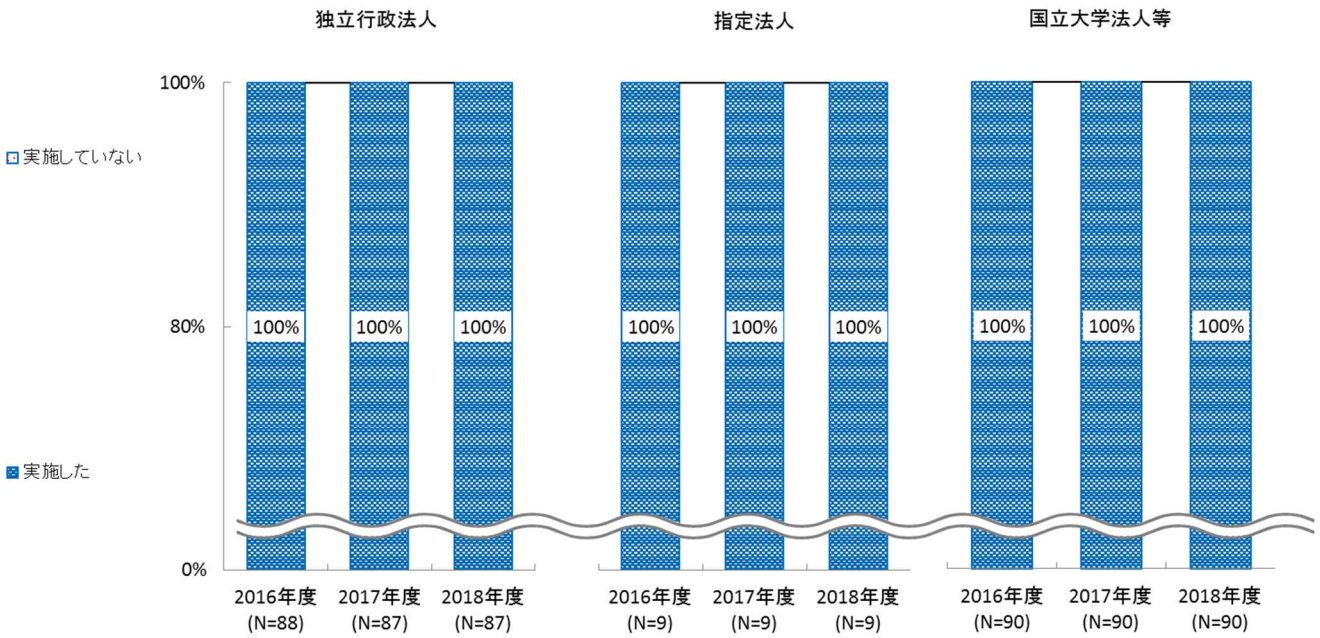
・ 国立大学法人等

情報セキュリティポリシーを定めている法人は、90法人全てである。

（２）情報セキュリティ対策の運用

①　教育・訓練[9]の実施状況

図表５　教育・訓練の実施状況



・ 独立行政法人

教育・訓練を実施している法人は、87法人全てである。

・ 指定法人

教育・訓練を実施している法人は、９法人全てである。

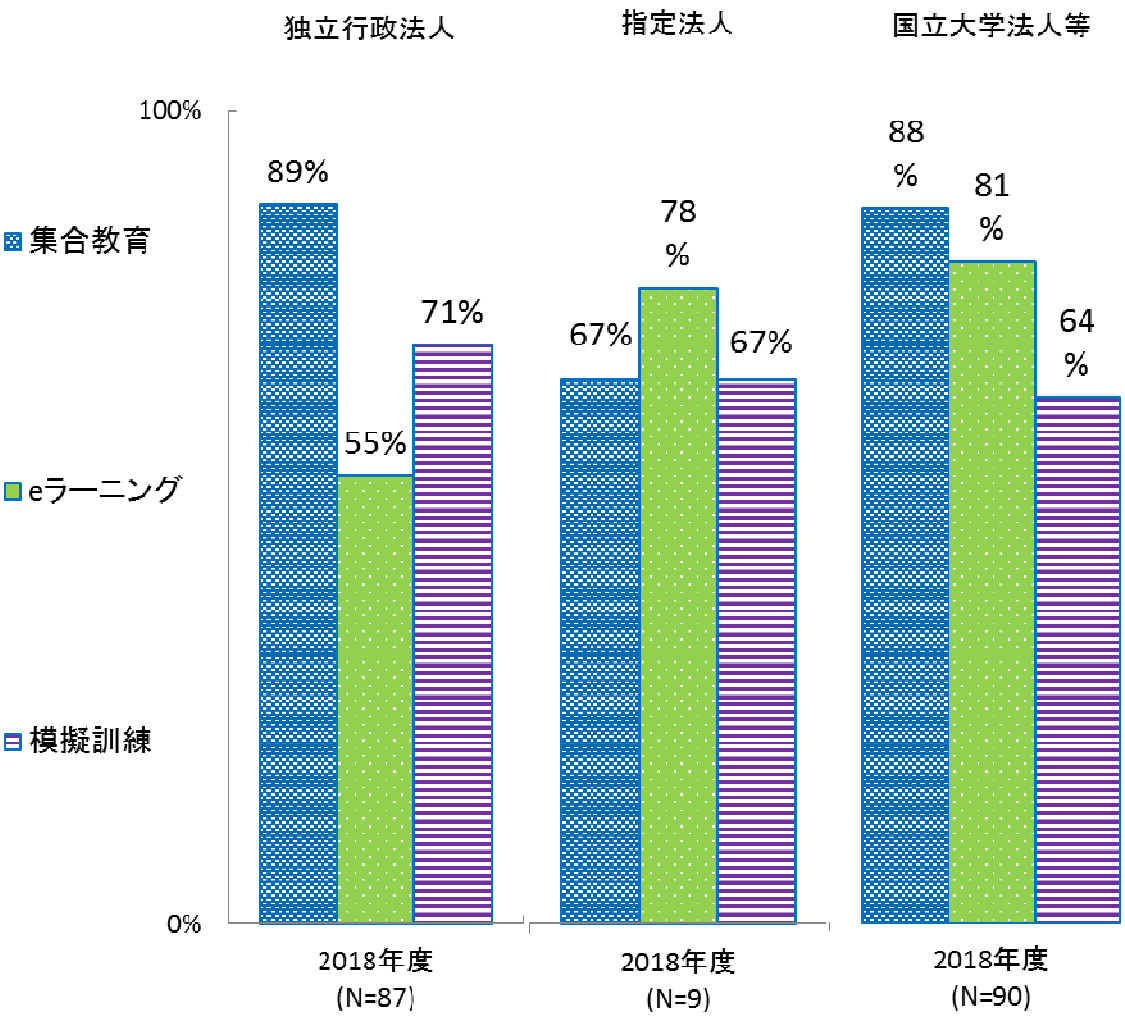
・ 国立大学法人等

教育・訓練を実施している法人は、90法人全てである。

[9] 教育・訓練とは、情報セキュリティ関係規定への理解を深めるために実施する取組のことである。

② 教育・訓練の実施内容

図表６　教育・訓練の実施内容



・ 独立行政法人

教育・訓練の実施内容について、集合教育を実施している法人は、77法人（89%）である。また、eラーニングを実施している法人は、48法人（55%）、標的型メール攻撃等の模擬訓練を実施している法人は、62法人（71%）である。

・ 指定法人

教育・訓練の実施内容について、集合教育を実施している法人は、６法人（67%）である。また、eラーニングを実施している法人は、7法人（78%）、標的型メール攻撃等の模擬訓練を実施している法人は、６法人（67%）である。

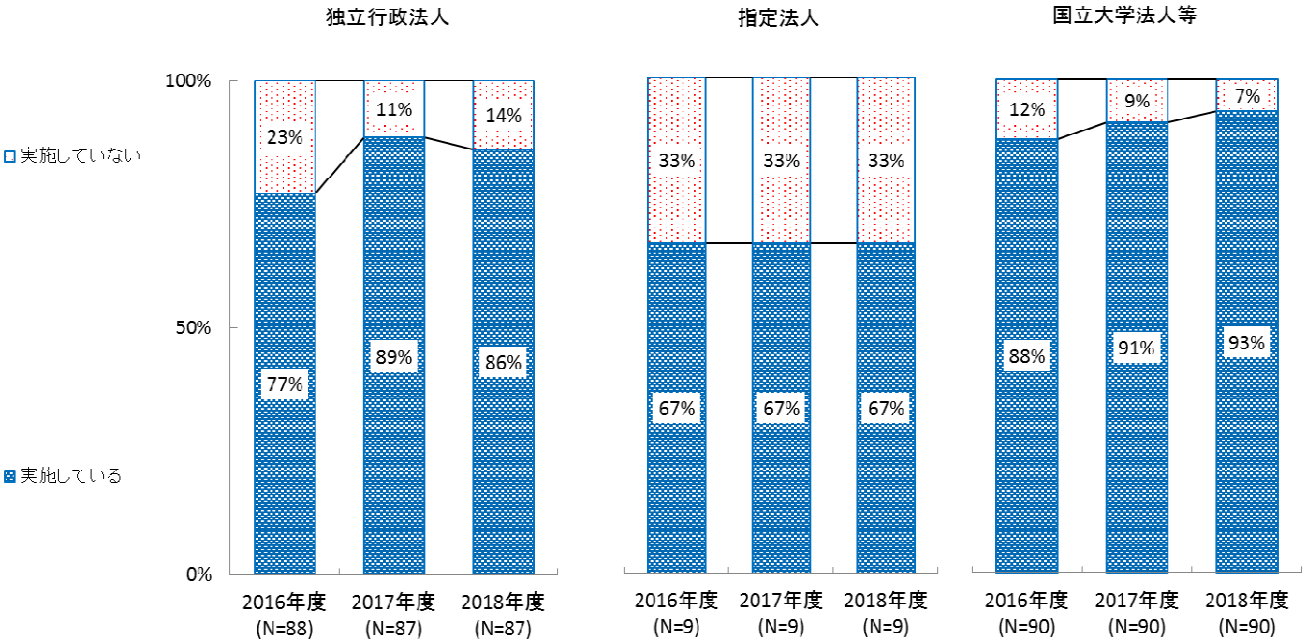
・ 国立大学法人等

教育・訓練の実施内容について、集合教育を実施している法人は、79法人（88%）である。また、eラーニングを実施している法人は、73法人（81%）、標的型メール攻撃等の模擬訓練を実施している法人は、58法人（64%）である。

（３）情報セキュリティ対策の点検

①　自己点検の実施状況

図表７　自己点検の実施状況



・独立行政法人

自己点検を実施している法人は、2017年度の77法人（89%）から76法人（86%）になっている。

・指定法人

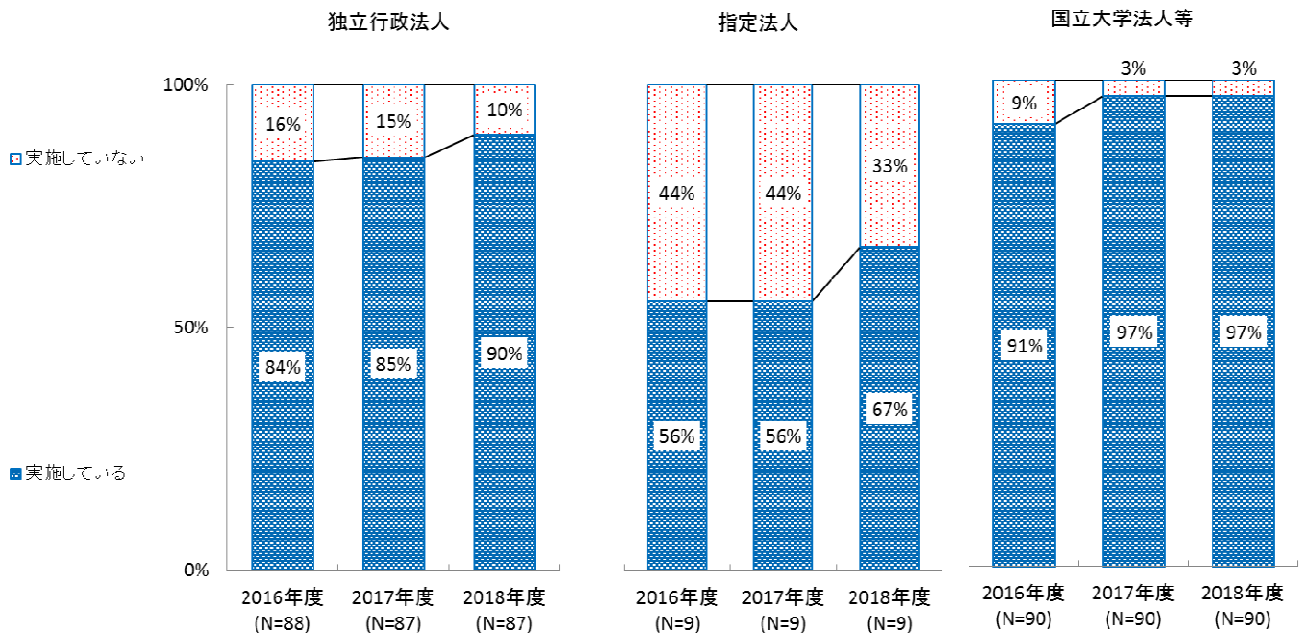
自己点検を実施している法人は、６法人（67%）である。

・国立大学法人等

自己点検を実施している法人は、2017年度の82法人（91%）から84法人（93%）に増加している。

② 情報セキュリティ監査の実施状況

図表８　情報セキュリティ監査の実施状況



・ 独立行政法人

情報セキュリティ監査を実施している法人は、2017年度の74法人（85%）から78法人（90%）に増加している。

・ 指定法人

情報セキュリティ監査を実施している法人は、2017年度の5法人（56%）から6法人（67%）に増加している。

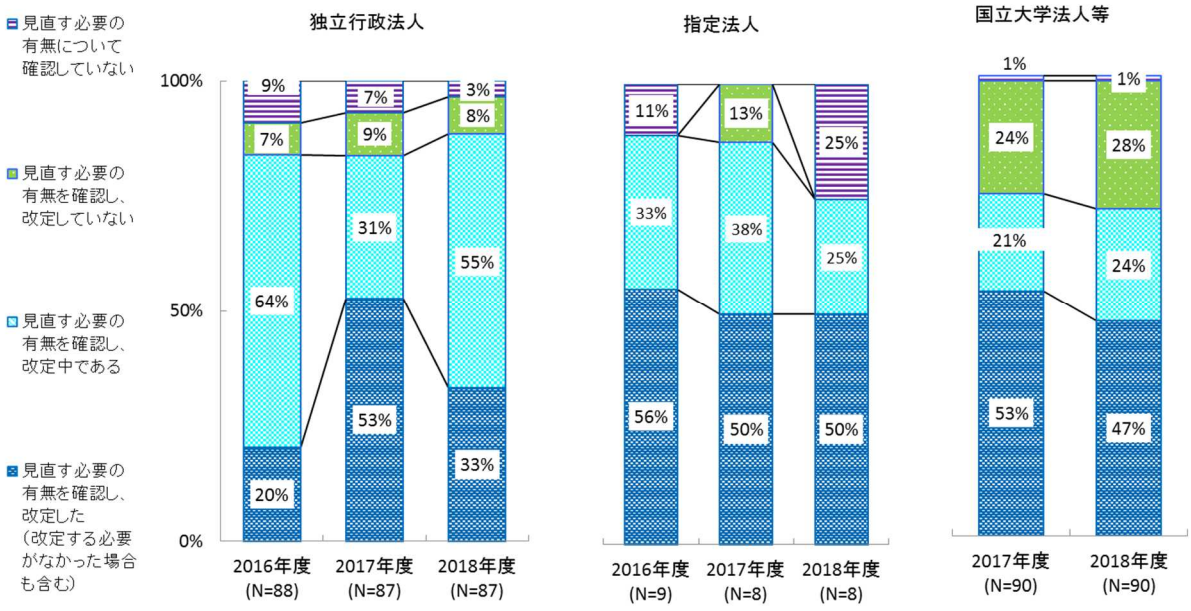
・ 国立大学法人等

情報セキュリティ監査を実施している法人は、87法人（97%）となっている。

（４）情報セキュリティ対策の見直し

①　情報セキュリティポリシー等の見直しの対応状況

図表９　情報セキュリティポリシー等の見直し等の対応状況



- 独立行政法人

  情報セキュリティポリシー等の規定類について、見直す必要の有無を確認した法人は、84法人（97%）である。

- 指定法人

  情報セキュリティポリシー等の規定類について、見直す必要の有無を確認した法人は、6法人（75%）である。

- 国立大学法人等

  情報セキュリティポリシー等の規定類について、見直す必要の有無を確認した法人は、89法人（99%）である。

４　各法人及び所管府省庁の対応

ほぼすべての法人において、CISO の設置、情報セキュリティ委員会の設置及び教育訓練が実施され、情報セキュリティの推進体制が年々整備されてきている。

一方、CSIRT の設置、自己点検、情報セキュリティ監査等を実施していない法人も散見されることから、当該法人は、速やかに対応することが必要である。

これらの結果を踏まえ、所管する府省庁は、上記の情報セキュリティ対策を実施していない独立行政法人等に対して、CSIRT の設置、自己点検、情報セキュリティ監査等を実施するように指導等を行うことが重要である。加えて、情報セキュリティ対策の取組が進んでいる法人に対しても、法人の情報セキュリティ対策の PDCA サイクルが継続的かつ有効に機能するよう、適宜その状況を把握し、必要に応じて助言することが望ましい。

別添３－９　NISC 発出注意喚起文書及びサイバーセキュリティ対策推進会議決定等

１「Twitter 利用におけるパスワード変更について（注意喚起）」（2018 年５月５日発出）

事　務　連　絡
平成 30 年５月５日

各府省庁等情報セキュリティ担当課室長　殿
各府省庁情報システム担当課室長　殿
サイバーセキュリティ対策推進会議オブザーバー機関情報セキュリティ担当課室長等 殿

内閣官房 内閣サイバーセキュリティセンター
内閣参事官（基本戦略担当）
内閣参事官（政府機関総合対策担当）
内閣参事官（重要インフラ担当）

Twitter 利用におけるパスワード変更について（注意喚起）

米 Twitter 社より、利用者のパスワードが米 Twitter 社のシステムの内部ログに暗号化されないまま保存されていたため、パスワードの変更を求める発表がなされました。

ついては、情報発信等のため業務上で Twitter を用いている場合には、以下の対策を講じるようお願いいたします。

①Twitter で利用しているパスワードを変更すること。

②Twitter で利用しているパスワードと同じパスワードを使用している他の全てのシステムやサービスのパスワードを変更すること。

上記については、独立行政法人その他の所管する法人に周知するとともに、業界団体を通じて連絡する等により所管する産業界（重要インフラ事業者を含む。）へも幅広く周知していただきますようお願いいたします。

（参考）
○米 Twitter 公式アカウント（ブログ）
https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

※　URL については廃止や変更されることがあります。最新のアドレスについては、御自身で御確認ください。

２　サイバーセキュリティ対策推進会議(CISO 等連絡会議)の開催状況

No.	開催日	主な議事
第 14 回	2018 年 ４月３日	・次期サイバーセキュリティ戦略骨子について ・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の見直しについて（骨子） ・2018 年サイバーセキュリティ月間について ・「各府省庁セキュリティ・IT 人材の確保・育成計画」の実施状況について ・「橋渡し人材のスキル認定の基準」について ・サイバーセキュリティ基本法の一部を改正する法律案について
第 15 回	2018 年 7 月 23 日	・次期サイバーセキュリティ戦略（案）について ・サイバーセキュリティ 2018（案）について ・サイバーセキュリティ政策に係る年次報告（2017 年度）（案）について ・サイバーセキュリティ関係施策に関する平成 31 年度予算重点化方針（案）について ・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の改定（案）について ・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 ・2018 年平昌オリンピック・パラリンピック競技大会における状況について
第 16 回	2018 年 12 月 10 日	・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きに関する申合せ（案）について ・サイバーセキュリティ基本法の改正について

別添３－10　政府機関等に係る 2018 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
2018 年	４月	【概要】原子力規制委員会は３日、Web サイトで３月 20 日に公開した東北電力女川原子力発電所の審査資料で、テロ等への悪用を避けるため空白とすべき構内図や写真を、４つのファイルで 57 ヶ所にわたってそのまま掲載するミスがあったと公表した。 【対応等】Web サイトに情報を掲載する際のマスキングの有無の確認等を徹底し、再発防止を図る。	意図せぬ情報流出
		【概要】厚生労働省千葉労働局は４日、柏労働基準監督署において、郵便物に同封されていた医療機関で撮影されたレントゲン写真等の画像データが保存されている DVD-RW１枚を誤廃棄したことを公表した。 【対応等】個人情報の重要性の再認識と管理の徹底を指示し、郵便物の作業手順等の再発防止策の注意喚起等を行った。	その他
		【概要】京都教育大学は６日、同大学が提供する WWW メールサービスにおいて、１件のアカウントに対して学外から不正アクセスが行われ、当該アカウントから学外の約 36 万件のアドレス向けに迷惑メールが発信されたことを公表した。	外部からの攻撃
		【概要】原子力規制委員会は 11 日、Web サイトに掲載した資料について、マスキングすべき情報が誤ってマスキング処理されないまま掲載されていたことと、当該資料を削除の上、改めてマスキング処理された資料を掲載したことを公表した。誤掲載した情報は、中部電力株式会社の印影及び担当者氏名（１名）であった。 【対応等】Web サイトに情報を掲載する際のマスキングの有無の確認等を徹底し、再発防止を図る。	意図せぬ情報流出
		【概要】地域医療機能推進機構相模野病院は 18 日、整形外科・泌尿器科手術の画像データを保存した外付けハードディスクを紛失したことを公表した。	その他
	６月	【概要】国立環境研究所は１日、国及び地方公共団体等職員の業務用メールアドレス（134 件）を誤って To 欄に入力してメールを送信したことを公表した。	意図せぬ情報流出
		【概要】国立病院機構小諸高原病院は 12 日、患者５名分の個人情報を保存した USB メモリを紛失したことを公表した。	その他
		【概要】島根大学は 22 日、教職員１名が、海外出張中に宅配業者を騙ったフィッシングメールを受信し、本文に記載された Web サイトにアクセスしたところ、同大学が利用しているメールサービスのサインインページに類似した偽サイトが表示され、そこに入力したパスワードが詐取されたことにより、教職員本人になりすまされ、外国から多量の迷惑メールの送信が行われたことを公表した。	外部からの攻撃
		【概要】弘前大学は 27 日、教職員に対して、同大学が利用しているメールサービスのサインインページに類似した偽サイトへ誘導しパスワードを入力させるフィッシングメールが届いたところ、教職員 12 名がパスワードを入力したことにより、これらのメールアドレスに届いた総計 3,151 通のメールが外部へ不正に転送され、メールアドレスを含む個人情報が漏えいしたことを公表した。	外部からの攻撃
		【概要】明石高専は６日、教員が誤って学生情報が保管されているリンク先を記載したメールを送信したと公表した。	意図せぬ情報流出
	７月	【概要】環境省は２日、（実在しない）同省職員のメールアドレスを詐称したメールが配信されており、当該メールにおけるマルウェアの検知・駆除の連絡を受けたことを公表した。 【対応等】環境省をかたった不審メールが送信されている状況と判断し、Web サイト上で注意喚起を実施した。	その他
		【概要】４日、経済産業省 Web サイトのコピーサイトが存在するとの情報が Twitter に掲載された。 【対応等】経済産業省は Web サイト上で注意喚起を実施した。	その他

年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】大阪大学は 27 日、基礎工学研究科・基礎工学部 Web サイトにおいて、Web サイトが改ざんされたことが判明したと公表した。	外部からの攻撃
		【概要】福島地方環境事務所は 30 日、入札を予定していた業務について、適切な入札の執行に支障を与える情報が当該事務所の Web サイトに誤って掲載されたことを公表した。 【対応等】同日、掲載されたファイルを削除し、同日 18 時頃、公告を一旦取り下げた。	意図せぬ情報流出
	８月	【概要】農畜産業振興機構は 17 日、元職員により、当機構が設置している委員会の委員数名の住所等の個人情報を含む、業務関連の内部情報が持ち出されたことを２日に確認したと公表した。	内部不正
	９月	【概要】福島地方環境事務所は 21 日、環境再生プラザが企画しているイベントの案内をスタッフが過去の同イベントに参加した者（64 アドレス、うち送信できたメールは 54 件）に対して BCC で送信する際、これらのアドレスが記載された Excel ファイルを誤って添付して送信したと公表した。 【対応等】所長より環境再生プラザを運営する事業者に対して、個人情報管理の徹底や本事案に関する問題点の抽出およびその解決策を早急に出すよう指示した。	意図せぬ情報流出
	11 月	【概要】気象庁は８日、気象庁発表の警報等を装った迷惑メールが一般国民宛てに届いたことを公表した。 【対応等】同日、気象庁 Web サイトに注意喚起を掲載した。	その他
		【概要】兵庫教育大学は 17 日、事務職員が、出張先や自宅においても業務用のメールを確認できるよう、2016 年４月 1 日から大学のメールアドレス宛てに届くメールをフリーメールへ自動転送しており、2018 年 10 月 26 日に当該職員のフリーメールに不正なアクセスを示すアラートが現れ、メールソフトのログイン履歴を確認したところ、第三者に閲覧されていた可能性があることが判明したと公表した。	意図せぬ情報流出
		【概要】森林研究・整備機構は 20 日、森林整備センター職員のメールアカウントが盗用され、英文の迷惑メールが大量に送信されたことが判明したと公表した。	外部からの攻撃
		【概要】日本貿易振興機構は 21 日、ジェトロ・バンコク事務所のサーバにおいて、不正アクセスによりバックドアとみられるプログラムが設置されていたことが判明したと公表した。	外部からの攻撃
		【概要】厚生労働省大分労働局は 29 日、「医療労務管理支援事業」の受託事業者が就業規則等について宛先を誤って送信したと公表した。 【対応等】受託事業者に対し、個人情報の重要性等を周知徹底するよう指示するとともに、個人情報保護管理規定及び実施体制を整備するよう指示した。	意図せぬ情報流出
		【概要】消費者庁は 30 日、所管法令に基づく調査対象の２事業者に対し、電子メールを送信した際、本来送付すべきファイルとは異なるファイルを誤って添付したことにより、当該２事業者とは異なる他の事業者の情報が漏えいしたと公表した。 【対応等】職員に対し、改めて情報の適切な管理について周知徹底を図るよう指導を行うとともに、再発防止に向け外部への情報発信に係る管理の改善を図った。	意図せぬ情報流出
		【概要】国立病院機構相模原病院は 30 日、患者 61 名分の個人情報が保存された外付けハードディスクを紛失したことを公表した。	その他
	12 月	【概要】環境省は４日、同省地球環境局地球温暖化対策課国民生活対策室が企画している２月に実施予定のイベントについて、委託事業者から再委託を受けた事業者が、案内の送付に先立ったテストメールを企業や団体 169 社（187 アドレス、うち送信できたメールは 183 件）に対して一斉送信する際、誤って BCC ではなく To で送信したと公表した。 【対応等】再委託者よりメール誤送信についてのお詫びとメールの削除をお願いする旨のメールを送信し、地球環境局地球温暖化対策課国民生活対策室長から委託事業者及び再委託を受けた事業者に対して、個人情報管理の徹底や本事案に関する原因の調査及びその解決策の提示を指示した。	意図せぬ情報流出
		【概要】新潟大学は６日、学生に対するフィッシングメールにより電子メールアカウントのパスワードが窃取され、不正アクセスを受けたと公表した。	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】国家公務員共済組合連合会は 12 日、舞鶴共済病院が、第三者からの不正アクセスを受けたことにより、Web サイトを停止したと公表した。	外部からの攻撃
		【概要】厚生労働省埼玉労働局は 18 日、平成 30 年度労働行政関係功労者表彰式の開催について同局 Web サイトで公開した際、誤って被表彰者の個人情報が掲載された資料を公開したと公表した。 【対応等】Web サイトへの掲載を行う際、資料に誤りがないか、掲載できない個人情報等が含まれていないかを複数人で確認すること等を再発防止策として周知徹底した。	意図せぬ情報流出
		【概要】環境省は 25 日、過去に実施していた実証事業サイトについて、検索エンジンにおいて、検索範囲を同サイトに限定して通販関係のキーワードを入力すると、検索結果の上位にインターネット通販情報が表示されることを公表した。 【対応等】同日中に実証事業サイトの運用管理者に対して閲覧停止及び原因調査を要請した。	外部からの攻撃
		【概要】厚生労働省広島労働局は 28 日、広島公共職業安定所において、求職者情報公開サービスにおける求職者情報を同局 Web サイトに掲載したところ、誤って求職者 97 名分の個人情報が記載された資料を掲載したことを公表した。 【対応等】Web サイトへの掲載を行う際、資料に誤りがないか、掲載できない個人情報等が含まれていないか等を複数人で確認すること等を再発防止策として周知徹底した。	意図せぬ情報流出
2019 年	１月	【概要】東京外国語大学は９日、職員に対して、メール保存制限の超過警告を装って偽のサインインページへ誘導しパスワードを入力させるフィッシングメールが 12 月 17 日に届き、同日職員１名が ID とパスワードを入力したところ、窃取された ID とパスワードを使用して本人になりすました不正なアクセスにより、12 月 18 日から 19 日にかけて約 24 万通の迷惑メールが送信されたこと、またその間、なりすましを行った者が個人情報を覗き見た可能性のあることが判明したことを公表した。	外部からの攻撃
		【概要】環境省は９日、COP24 会場内日本政府作業部屋に保管していた PC 及び USB メモリが無くなっており、盗難に遭ったと推測される旨を公表した。なお、情報流出の有無については確認されていない。 【対応等】物品及びデータの適切な管理について改めて周知徹底した。	その他
		【概要】厚生労働省島根労働局は 25 日、MRI 画像を保存した CD-R を紛失したことを公表した。 【対応等】個人情報の適正な管理の徹底について指導するとともに、CD-R 等の適正な管理を徹底した。	その他
		【概要】厚生労働省山梨労働局は 31 日、若年者地域連携事業において、ある企業の説明会参加申込書を、誤って別の企業に電子メールで送信したことを公表した。 【対応等】全ての委託事業の受託事業者に対して、本事案の事実経過を周知するとともに、個人情報の適正な管理の徹底について指導した。	意図せぬ情報流出
		【概要】造幣局は 31 日、造幣局オンラインショップにおいて、システムの保守の際の作業ミスにより、１月 23 日から１月 28 日まで 66 名の顧客の個人情報（氏名、住所、電話番号、FAX 番号、購入履歴）が別の顧客の注文履歴に混入し、各顧客の注文履歴画面で閲覧可能な状態になっていたことを公表した。	意図せぬ情報流出
	２月	【概要】環境省広報室は 15 日、九州地方環境事務所において、情報公開法第４条第１項に基づく行政文書の開示請求に基づき開示した文書について、非開示にすべき希少種の生息していた場所の情報や検討委員の電子メールアドレス等の個人情報が記載された形で文書を誤送付したことを公表した。 【対応等】情報開示文書を発送する際には、印刷された資料を担当部署及び公開担当部署のそれぞれで複数名により確認を行うとともに、封入時の最終確認をする等の体制の確保を行うこととした。	意図せぬ情報流出
	３月	【概要】国立精神・神経医療研究センターは６日、職員が約 25 名分の患者の個人情報を記録したタブレット型端末を紛失したことを公表した。	その他

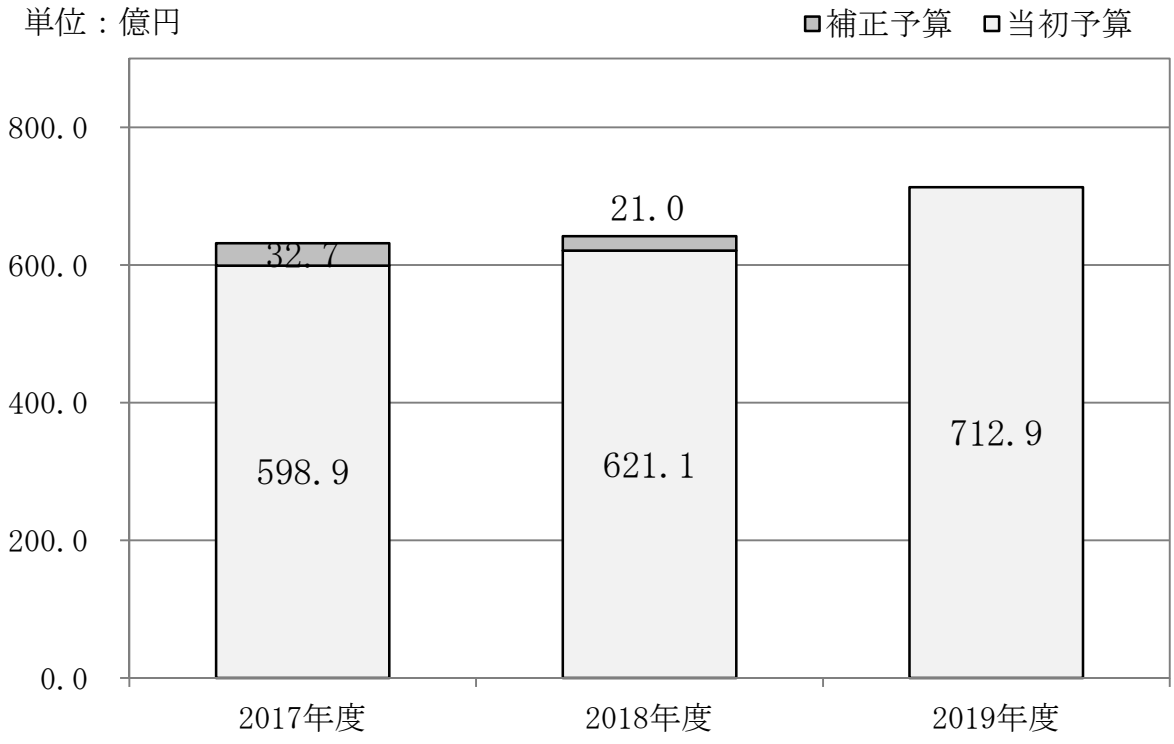
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】厚生労働省長野労働局は 14 日、長野公共職業安定所において、「地方人材還流促進事業」の利用者に対してメールを送信する際、１名のメールアドレスを誤って BCC ではなく To で送信したことを公表した。 【対応等】メール送信時に宛先の確認を徹底する等メールによる誤送信の防止策の再確認の指示を行った。	意図せぬ情報流出
		【概要】広島大学高等教育研究開発センターは 19 日、第三者からの不正アクセスにより Web サイトが改ざんされ、特定の検索サイトの検索結果画面から情報調査室の Web サイトにアクセスした場合、外部の問題がある商業サイトに転送される不正コードが組み込まれていたことを公表した。	外部からの攻撃
		【概要】地域医療機能推進機構うつのみや病院は 29 日、約 700 名の氏名、年齢及び生年月日を含む健診データが保存された USB メモリを紛失したことを公表した。	その他

※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３－11　政府のサイバーセキュリティ関係予算額の推移

	2017 年度	2018 年度	2019 年度
当初予算額	598.9 億円	621.1 億円	712.9 億円
補正予算額	32.7 億円	21.0 億円	－

※サイバーセキュリティに関する予算として切り分けられないものは計上していない。
※補正には減額補正を含む。



別添４　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４－目次＞

別添４－１　第４次行動計画の概要 241
別添４－２　重要インフラにおける取組の進捗状況 246
別添４－３　安全基準等の継続的改善状況等の把握及び検証 263
別添４－４　安全基準等の浸透状況等に関する調査（アンケート調査） 271
別添４－５　安全基準等の浸透状況等に関する調査（往訪調査） 309
別添４－６　情報共有件数 313
別添４－７　セプター概要 314
別添４－８　分野横断的演習 315
別添４－９　セプター訓練 318
別添４－10　補完調査 319

別添４－１　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

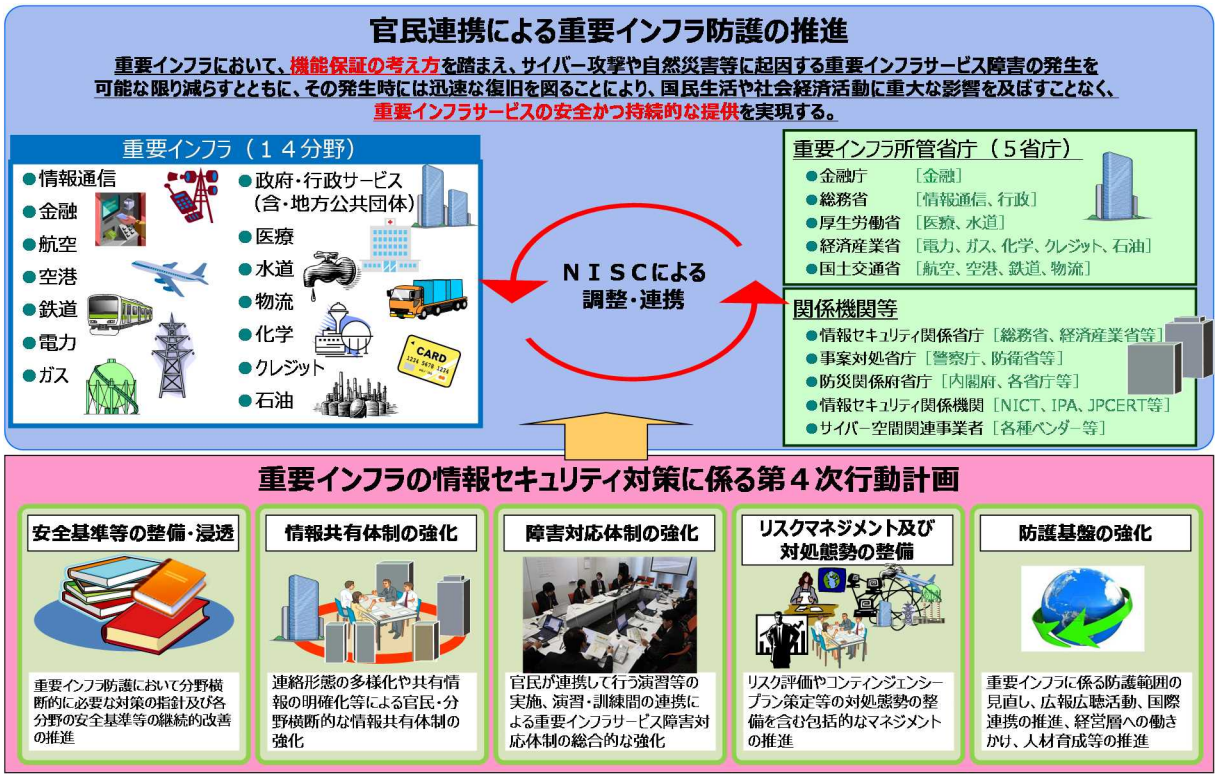
■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 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

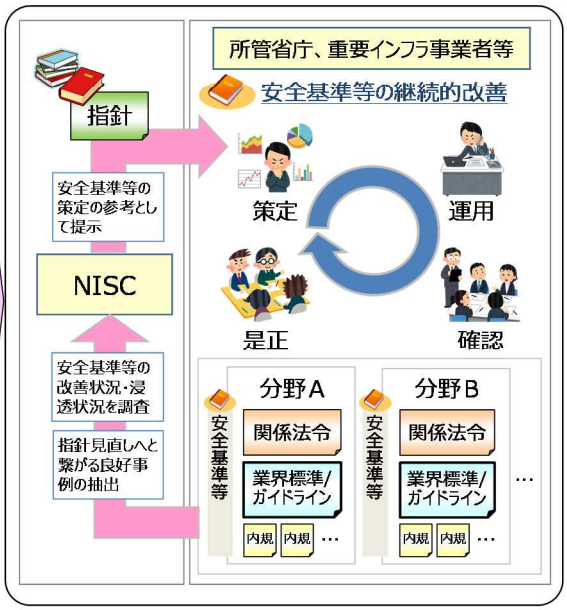
行動計画期間中の施策

（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

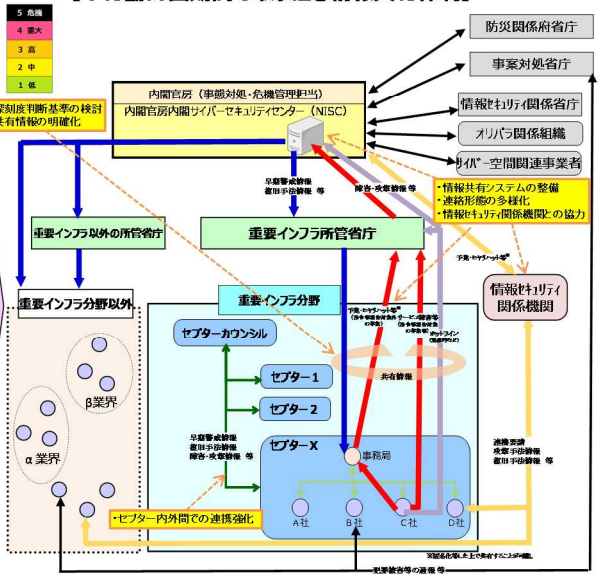
（１）情報共有体制の充実
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（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

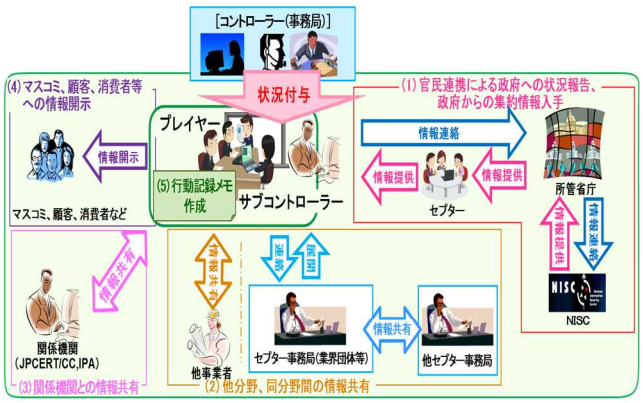
行動計画期間中の施策

（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。

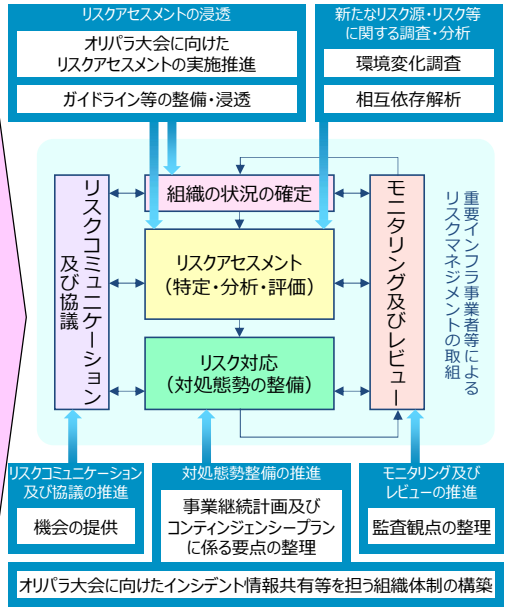
行動計画期間中の施策

（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

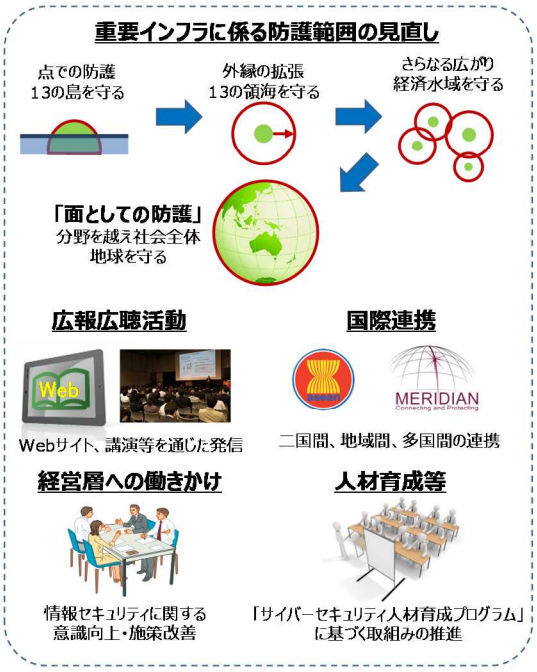
（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

（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

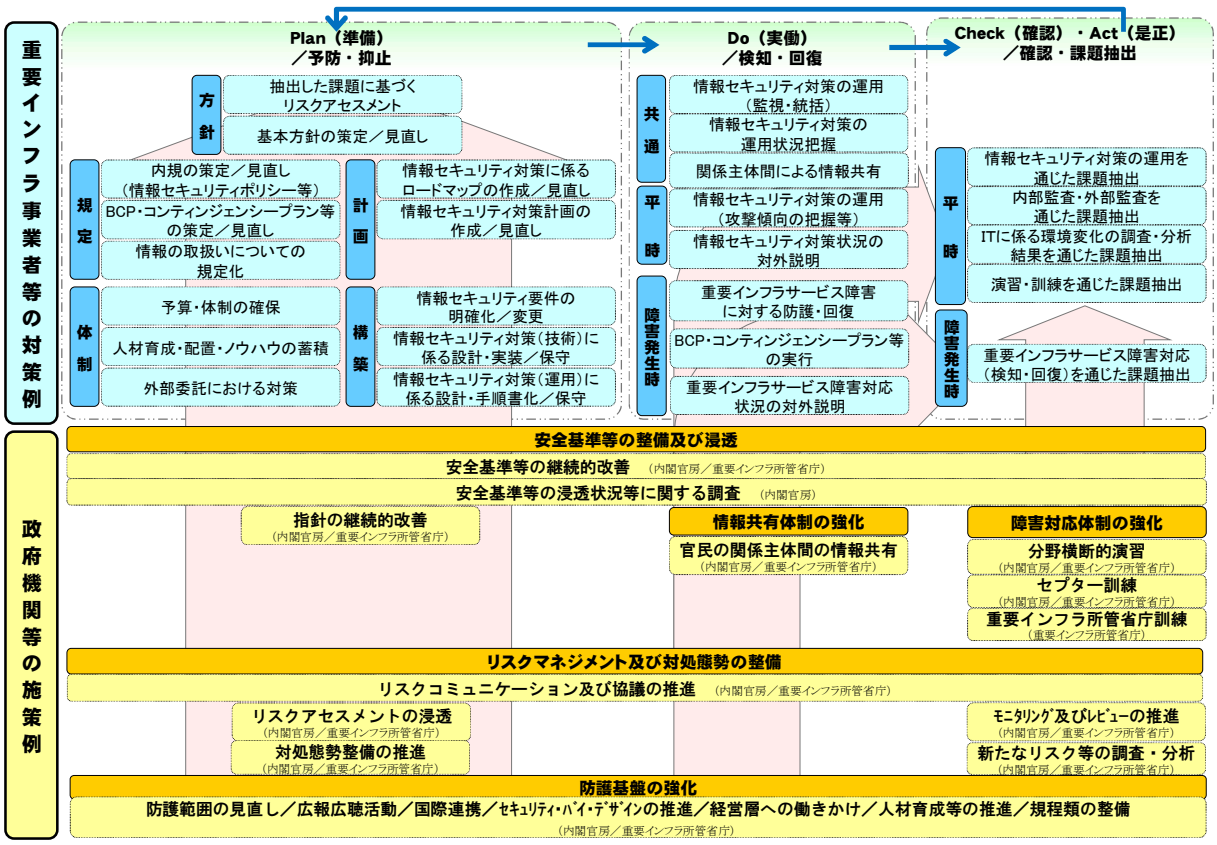
（４）経営層への働きかけ
- 情報セキュリティに関する経営層の意識向上のための働きかけ

（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４－２　重要インフラにおける取組の進捗状況

本章では、「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」（以下「第４次行動計画」という。）に基づく取組について、2018年度の進捗状況の確認・検証結果を報告する。

１　重要インフラと第４次行動計画全体に関する取組

(1)　第４次行動計画の概要

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月改定）」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たものであり、2017年４月にサイバーセキュリティ戦略本部で決定した。その後、2018年７月に、重要インフラ分野として「空港分野」を追加する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つの施策を掲げており、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである（参考：別添４－１）。施策ごとの取組の進捗状況については次節に示す。

(2)　取組の進捗状況

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の中で明確化したほか、重要インフラサービスに重点を置き、これまで「IT障害」としていた表記を「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た。

2018年度は、2017年度に引き続き、同計画に従って機能保証の考え方に基づき、５つの施策それぞれについて取組を進めた。各施策の取組等の詳細は次節以降に示すが、過去最大規模での分野横断的演習の開催、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の決定など、各種取組の着実な成果を得た。なお、第４次行動計画における施策の枠外の取組として、2017年度に引き続き、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実施した（参考：別添４－10）。

(3)　今後の取組

引き続き、内閣官房と重要インフラ所管省庁等が一体となり、第４次行動計画に基づく取組を推進し、重要インフラ事業者等に対して必要な支援を実施する。

２　第４次行動計画の各施策における取組

本節においては、第４次行動計画における施策ごとの取組の進捗状況について示す。なお、進捗状況の確認・検証は、第４次行動計画のⅤ.1.3及びⅤ.2.3に記載される各施策における目標及び具体的な指標を踏まえたものである。

(1)　安全基準等の整備及び浸透

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜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関して、以下の取組を実施した。本取組の中で、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PDCAサイクルとの整合性の確保、第４次行動計画の他施策との連携強化を図ることにより、情報セキュリティ対策の重要性を重要インフラ事業者等に訴求する仕組みを構築した。

○安全基準等策定指針の改定等

第４次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、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方針等を定める際に考慮すべき事項を整理することなどを柱とする指針の改定作業を進め、「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）」をとりまとめ、2018年４月のサイバーセキュリティ戦略本部において決定、公表を行った。

また、2019年１月の重要インフラ専門調査会において、自然災害の多発やサイバーセキュリティ戦略の改定、重要インフラ分野への空港分野の追加等、指針第５版とりまとめ後の環境変化を踏まえた指針の改定について方向性が承認された。

○安全基準等の改善状況調査

各重要インフラ分野における安全基準等の継続的な改善状況について調査した（参考：別添４－３）。各分野において安全基準等の改善の必要性について検討・確認し、2017年度より４分野増加した８つの分野において安全基準等の改善を行ったほか、７の分野において改善に向けた分析・検証に着手している。なお、各分野における制度的な枠組みについては、経済産業省においてガス事業法施行規則を改定し、「ガス工作物の運転又は操作を管理する電子計算機に係るサイバーセキュリティの確保に関すること」をガス事業法上の保安規制の一部として位置付ける取組があった。

○安全基準等の浸透状況等調査

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状況について調査を実施した。アンケート調査（参考：別添４－４）では、2,050件の回答が得られ、分析の結果、重要インフラ事業者等が「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割合」は2017年度と同様の約５割であった。また、重要インフラ事業者等が「先導的な情報セキュリティ対策に取り組んでいる割合」は2017年度の約２割から2018年度には約３割となった。良好な点として、ほぼ全ての事業者等で何らかの情報セキュリティ対策が取られていることから、セキュリティマインドが醸成されていること等が認められた。

また、往訪調査を実施し、情報セキュリティに係る体制や規程等について意見交換を行うとともに、政府への意見・要望の収集を実施し、良好事例及び課題を整理した（参考：別添４－５）。

イ　今後の取組

2018年度の取組結果を活用しつつ、第４次行動計画に基づき、重要インフラ防護において分野横断的に必要な対策の指針及び各重要インフラ分野の安全基準等の継続的改善を推進するとともに、重要インフラ事業者等への安全基準等の浸透を図る。具体的には、「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（第５版）」を改定した上で、同指針の普及・浸透を図るとともに、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。また、浸透状況等調査については、アン

ケートの回答が事業者等に資する内容となるよう、取組の充実を図る。

(2)　情報共有体制の強化

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜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。こうした取組により、官民の各関係主体が協力する情報共有体制の維持・強化を推進するとともに、重要インフラ事業者等による情報共有活動の活性化を図った。

〇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、2017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。その結果、重要インフラ事業者等から内閣官房に対して223件の情報連絡が行われ、内閣官房からは43件の情報提供を行っている（参考：別添４－６）。

表１：重要インフラ事業者等との情報共有件数

年度	2014	2015	2016	2017	2018
重要インフラ事業者等から内閣官房への情報連絡件数	124件	401件	856件	388件	223件
内閣官房からの情報提供件数	38件	44件	80件	54件	43件

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、情報連絡の件数は前年度に比べ減少しているものの、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参加し、内閣官房や関係省庁との連携要領、関係主体の役割の在り方及び同手順の実効性に関する検証を実施した。

〇セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、空港分野が追加となり、14分野で19セプターが設置されている（参考：別添４－７）。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（仮称）の創設に向けた取組や、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、2018年４月の総会で決定した活動方針に基づき、2018年度に、運営委員会（４回）、相互理解WG（４

回)、情報収集WG（４回)、総会準備WG（３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において、重要インフラ専門調査会における調査審議を踏まえ、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を決定した。

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、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）や共有情報の理解浸透（共有範囲の明確化）等、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

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜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。こうした取組により、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等の検証や、関係主体間における情報共有の有効性の検証を可能にするとともに、技術面での対処能力の向上等を図った。

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「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」及び「情報共有体制の実効性の向上」に取り組んだ（参考：別添４－８)。

2018年度からは、空港分野を加えた全14分野が演習に参加し、参加者数は3,077名に増加した。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	2015	2016	2017	2018
参加者数	1,168名	2,084名	2,647名	3,077名

2018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、募集の際に自職場参加について丁寧に説明したテキストブック等を添付することで、昨年度と比較し、自職場参加者が増加した（2017年度：63%→2018年度：75%)。

また、演習当日における経営層参加については、参加者募集時や事前説明会における資料に加え、ベースシナリオの中でも経営層の参加を促したものの、その参加率は28%に留まっている。

なお、2017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82%となっている。一方で、安全基準等の浸透状況等調査の結果から、組織内外で実施する演習・訓練への参加状況について、分野横断的演習を含む組織外で実施される演習・訓練への参加割合は61%、組織内で演習・訓練を実施している割合は29%に留まっている。

○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４－９）。

表３：参加セプター・参加事業者等数の推移

年度	2015	2016	2017	2018
参加セプター	18	18	18	19
参加事業者等	1,658	2,020	2,106	2,005

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（受信確認）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。

○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 Ⅲ）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、2020年東京オリンピック・パラリンピック競技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。

(4)　リスクマネジメント及び対処態勢の整備

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜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の推進に係る取組を以下のとおり実施した。これらの取組を通じて、重要インフラ事業者等におけるサイバー攻撃を想定したリスクマネジメント及び対処態勢整備に必要となる考え方や観点、具体的な作業手順等を整理するとともに、重要インフラ事業者等への浸透を図った。

○リスクマネジメントに対する支援

内閣官房は、2020年東京オリンピック・パラリンピック競技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った。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た「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」をとりまとめ、2018年４月に公表した。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や、ISACにおける勉強会、分野横断的演習の説明会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。

なお、「機能保証のためのリスクアセスメント・ガイドライン」の配付数について、掲載されているWebサイトの閲覧数は257件、第３回説明会の参加者数は504人、第４回説明会の参加者数は515人となっている。

○対処態勢整備に対する支援

内閣官房は、個々の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「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」について、「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）」に盛り込んだ。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及びコンティンジェンシープラン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構築したほか、サイバーセキュリティ対処調整センターを含む、大会に向けたサイバーセキュリティ体制の運用方針等について、大会組織委員会、東京都等と協議の上、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サイバーセキュリティWTにおいて決定した。

○リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動（運営委員会（４回）、相互理解WG（４回）、情報収集WG（４回）、総会準備WG（３回））を支援したほか、分野横断的

演習に関しても、説明会、意見交換会、各重要インフラ分野が検討に参加する検討会（２回）及び拡大作業部会（１回）をそれぞれ開催した。また、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参加事業者等を対象に、説明会(25回）や情報交換会（６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

2018年度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。

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

第４次行動計画における本施策の目標及び具体的な指標は次のとおりである。

＜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

防護基盤の強化として、以下の取組を実施した。こうした取組により、第４次行動計画の全体を支える共通基盤の強化が図られた。

○防護範囲の見直し

重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大、民間事業者におけるICT-ISAC、金融ISAC及び電力ISACの活発な活動、交通ISAC（仮称）の創設に向けた取組など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上に着実な成果があったと認められる。

○広報広聴活動

内閣官房は、NISCのWebサイトにおいて、分野横断的演習やセプターカウンシルの開催について広報を行うとともに、重要インフラ専門調査会の会議資料等の掲載を通じ、第４次行動計画の進捗状況等を随時公表したほか、重要インフラ事業者等に対して、情報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、海外機関等の公表情報の紹介等を記載した重要インフラニュースレターを24回発行した。

また、重要インフラ防護に関する講演を14回実施し、第４次行動計画の考え方や取組状況について重要インフラ事業者等や海外等への周知を図った。

さらに、情報通信、航空、鉄道、物流、ガス及びクレジット分野の合計16事業者等を対象とした往訪調査の機会を活用し、第４次行動計画やその施策等について説明し、第４次行動計画への意見や内閣官房への要望についてヒアリング等を行った。

〇国際連携

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。

多国間では、2018年10月に韓国で開催されたMeridian会合において、日本のサイバー演習や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。また、2018年12月に開催した分野横断的演習当日に合わせて海外機関を対象とした演習見学会を開催し、演習概要の説明及び各国のサイバー演習の取組に関する情報交換を実施した。加えて、国際的な情報共有の枠組みであるIWWNを利用して、サイバー攻撃や脆弱性対応についての情報を継続的に共有している。

地域間では、2019年１月にASEAN研修員向けの「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」研修において、日本における重要インフラ防護の取組について講演した。

二国間では、日仏サイバー協議における意見交換や、日米間や日豪間における政府間協議等を行った。また、2018年４月に開催された米国サイバー演習の視察に合わせ、サイバー演習について米国と意見交換を実施したほか、2019年１月には仏国サイバー演習を視察するとともに、サイバー演習や重要インフラ防護施策について意見交換を実施した。

〇経営層への働きかけ

内閣官房において、「記述情報の開示に関する原則」の公表（金融庁）、「経営ガイドライン」の普及活動、産業サイバーセキュリティ研究会の活動（経済産業省）のほか、IPA（中小企業向けのサービス）等の取組について、第４次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、関連施策を通して経営層への働きかけを実施した。

〇人材育成等の推進

内閣官房は、「サイバーセキュリティ人材育成取組方針」（2018 年６月サイバーセキュリティ戦略本部報告）に基づく取組を推進した。重要インフラ事業者等については、情報セキュリティ人材の育成カリキュラム等による組織内の人材教育について、各関連施策を通じて普及啓発を行った。

〇規格・標準及び参照すべき規程類の整備

内閣官房は、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するとともに、「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）」を作成するに当たって関連する規格を整理し、指針に反映した。

また、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サイバーセキュリティ戦略、第４次行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を更新し、配布した。

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、引き続き見直しの取組及びそれぞれの事業者等の状況に合わせた取組の推進を実施する。

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及び講演等を通じ、行動計画の取組を広く認識・理解し得るよう引き続き努めるとともに、より効果的な広報チャネルについても検討を進める。また、往訪調査や勉強会・セミナー等を通じた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て、欧米・ASEANやMeridian等の二国間・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、引き続き、各関連文書を合本し、「重要インフラ防護に係る規程集」として発行する。また、重要インフラ防護に係る関連規格について、適切な版を必要なときに参照できるようにするため、他の関係主体との協力の下、国内外で策定される関連規格について調査を行った上で整理し、その結果を明示する。

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次行動計画を踏まえて考慮すべき情報セキュリティ対策の対策項目を例示することや、経営層の積極的な関与が期待される場面や関わり方等を明確化すること、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定める際の考慮すべき事項を整理すること等を柱とする指針の改定を行い、2018 年４月のサイバーセキュリティ戦略本部において決定、公表を行った。
②必要に応じて社会動向の変化及び新たに得た知見に係る検討を実施し、その結果を公表。	・2019 年１月の重要インフラ専門調査会において、自然災害の多発やサイバーセキュリティ戦略の改定、重要インフラ分野への空港分野の追加等の環境変化を踏まえた指針の改定について、方向性が承認された。
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。	・2018 年４月に決定した指針（第５版）の説明を重要インフラ所管省庁やセプター等に対して行うとともに、指針の更なる改定に関して重要インフラ所管省庁やセプター等に背景や方針の説明を行うことなどを通じて、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・検証及び改訂等の実施状況並びに今後の実施予定等の把握を実施（2018 年 12 月～2019 年３月）し、「2018 年度　重要インフラにおける安全基準等の継続的改善状況等の調査」を 2019 年４月に公表した。 ・各重要インフラ分野における制度的枠組みの現状の把握に努めた。
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の協力を得て、各重要インフラ分野における安全基準等の整備状況、情報セキュリティ対策の実施状況等についての調査（2018 年６月～12 月）及び事業者等への往訪による調査（2018 年１月～12 月）を実施し、「2018 年度　重要インフラにおける『安全基準等の浸透状況等に関する調査』について」を 2019 年４月に公表した。
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をもとに、各施策の改善事項の検討を実施した。
(2)「情報共有体制の強化」に関する施策	
① 平時及び大規模重要インフラサービス障害対応時における情報共有体制の運営及び必要に応じた見直し。	・平時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、第４次行動計画に基づいた手順を確認し、訓練により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。（2018 年度　情報連絡 230 件、情報提供 43 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、重要インフラ事業者等への情報提供を行った。また、同機関が分析した情報の横展開を行った。さらに、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を構築し、収集した情報をとりまとめた。
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、2018 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者等への支援の実施。	・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実施した。

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。（2018 年度のセプターカウンシル会合の回数は延べ 16 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・訓練について、相互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、より実態に即した訓練を 14 分野 19 セプターを対象に実施した。
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。2018 年度は、3,077 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、2020 年東京オリンピック・パラリンピック競技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、個別シナリオ作成における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ついて説明を実施するとともに、経営層による演習参加の重要性を明確にするよう、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。	・ 2017 年度分野横断的演習の事後調査により、演習に参加して得られた気づきを踏まえた改善状況等（リスク分析の成果の検証状況、復旧手順及び IT-BCP 等の検討の状況）を把握し、その分析結果を踏まえた 2018 年度分野横断的演習の企画・運営について検討した。また、効果的な取組を進めていると評価される参加事業者等について、ヒアリング等を通じて具体的な取組内容を把握し、グッドプラクティスとしてまとめ、他の演習参加者等に提供した。 ・ 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。また、演習参加により抽出された課題・問題点等を明確にした。 ・ 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。 ・ 個別の重要インフラ事業者等による演習実施の支援に資することを目的に、仮想的な演習環境の構築を進めた。
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。	・ 2020 年東京オリンピック・パラリンピック競技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。 ・ 2018 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 (25 回) 及び情報交換会 (６回) を開催するなど、2020 年東京オリンピック・パラリンピック競技大会の開催・運営を支える重要サービスを提供する事業者等 (268 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。	・ 2020 年東京オリンピック・パラリンピック競技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、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」をとりまとめ、2018 年４月に公表している。なお「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」は本手引書に統合する形となっている。
③ 本施策における調査・分析の結果を重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に反映する参考資料として提供。	・ 安全基準の整備等に関わる新たなリスク源について、安全基準等策定指針等の改定に向けて整理したほか、新たなリスク源に関するヒアリング等を実施することで、社会状況を反映したより実態に近い各重要インフラ分野におけるサービス維持に関する状況等の把握を行った。
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。	・ 新たなリスク源に関するヒアリング等を実施することで、社会状況を反映したより実態に近い各分野におけるサービス維持に関する状況等の把握を行い、他施策の内容検討に繋げた。
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。	・ 2018 年４月に公表した「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）」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」の中で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記載を行い、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た。 ・ 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参加事業者等を対象に、説明会や情報交換会等を開催し、有識者による講演や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）及び拡大作業部会（１回）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。	・ 個々の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、「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」について、「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）」に盛り込み、2018 年４月に公表している。 ・ 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。

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構築した。また、サイバーセキュリティ対処調整センターを含む、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サイバーセキュリティ体制の運用方針等について、大会組織委員会、東京都等と協議の上、決定した。
⑨ リスクマネジメント及び対処態勢における監査の観点の整理及び重要インフラ事業者等への提供。	・ リスクマネジメントにおける内部監査の観点を、「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」に記載し、2018 年４月に公表している。
(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。	・ 防護範囲見直し及び情報共有範囲の拡充を推進した。これにより、重要インフラ分野の追加（空港分野）、各セプターにおける中小事業者を含めたセプター構成員の拡大、民間事業者における ISAC の活発な活動など、情報共有の輪を拡大・充実化する動きが生じており、情報共有等の活動に関する主体性・積極性の向上が図られた。
② Web 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。第４次行動計画の実行に当たり、セプターや重要インフラ事業者等に加え海外の重要インフラ関係者に対し、第４次行動計画やその施策等について計 14 回講演を行った。
③ 往訪調査や勉強会・セミナー等を通じた広聴を実施。	・ 往訪調査等を通じて、第４次行動計画やその施策等について説明を行うとともに、第４次行動計画への意見や NISC への要望についてヒアリング等を行った。
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、ASEAN 研究員向け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における講演、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て、相互理解の基盤を強化した。
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。	・ 米国サイバー演習の視察及び意見交換を通じて得た知見を踏まえ、国内での有識者・業界関係者等との議論・検討を行い、分野横断的演習内容の改善を行った。
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。	・ 「記述情報の開示に関する原則」の公表（金融庁）、「経営ガイドライン」の普及活動、産業サイバーセキュリティ研究会の活動（経済産業省）のほか、IPA（中小企業向けのサービス）等の取組について、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、関連施策を通して経営層への働きかけを実施した。
⑦ 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行。	・ 重要インフラ関係者が共通に参照する関連文書について、サイバーセキュリティ戦略、行動計画等の各関連文書を合本した「重要インフラ防護に係る規程集」を更新、配布した。
⑧ 関連規格を整理、可視化。	・ 国内外で策定される重要インフラ防護に関係する規格について情報を収集するとともに、「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）」を作成するに当たって関連する規格を整理し、指針に反映した。
⑨ 重要インフラ事業者等に対する第三者認証制度の認証を受けた製品活用の働きかけ。	・ 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、「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、委託先の組織としての活用の把握等の留意点が記載されている「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、「自治体情報セキュリティ対策検討チームの報告（2015年11月）」を踏まえた地方公共団体におけるセキュリティ対策の抜本的強化への取組や、「政府機関の情報セキュリティ対策のための統一基準」の改定等を踏まえ、2018年９月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」等を改定した。また、2017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、その結果や有識者からの意見を踏まえ、「情報通信ネットワーク安全・信頼性基準」等について、2019年３月に改定した。 ・ 厚生労働省において、2019年３月に「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）」を策定した。 ・ 国土交通省において、国土交通省所管の重要インフラ分野（航空、空港、鉄道、物流）における「情報セキュリティ確保に係る安全ガイドライン」の改訂を行い、事業者への周知・浸透を図るとともに、国土交通省のウェブサイトに掲載した。 ・ 金融庁及び経済産業省については、自らが安全基準等の策定主体とはなっていない。 ・ 制度的枠組みを適切に改善する取組として、経済産業省においてガス事業法施行規則を改定し、「ガス工作物の運転又は操作を管理する電子計算機に係るサイバーセキュリティの確保に関すること」をガス事業法上の保安規制の一部として位置付けた。
③ 重要インフラ分野ごとの安全基準等の分析・検証を支援。	・ 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。	・ 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」及び「水道分野における情報セキュリティガイドライン」について、ツイッター等を活用した普及活動を実施した。また、2018年10月に「医療情報システムの安全管理に関するガイドライン」の周知徹底等に関して都道府県等に対し通知した。
⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・ 重要インフラ所管省庁は、内閣官房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。
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、内閣官房が実施した安全基準等の浸透状況等の調査について、所管の各重要インフラ分野に協力を求め、2,050者から回答を得た。なお、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、所管の各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。 ・ 厚生労働省においては、2018年10月に「医療情報システムの安全管理に関するガイドライン」の周知徹底等に関して都道府県等に対して通知した。また、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等を行った。 ・ 国土交通省において、2018年４月から重要インフラ事業者（航空、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）の仮運用が開始されたことから、事業者が参加する検討会を開催し、交通ISACの本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論した。また、2018年７月に重要インフラ分野に追加された空港分野の事業者に対し、交通ISACへの参加を促した。
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、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際に、事案の大小や重要インフラサービスの事案であるか否かに関わらず、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た。 ・ 2018 年４月 24 日に医療セプターを代表し、公益社団法人日本医師会がセプターカウンシルに加入した。 ・ 国土交通省において、2018 年７月に重要インフラ分野に追加された空港分野がセプターカウンシルに加入するよう、事業者と調整中である。
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	・ 厚生労働省において、医療分野におけるセプター構成員の拡充に関して支援を行った。また、IPA の情報収集・分析・共有の仕組み（J-CSIP）に加入するよう調整を行い、医療分野は、2018 年５月、水道分野は 2018 年 11 月に加入した。 ・ 国土交通省において、2018 年７月に重要インフラ分野に追加された空港分野が IPA の情報収集・分析・共有の仕組み（J-CSIP）に加入するよう、事業者と調整し、2018 年 11 月に加入した。
(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、2018 年８月から 10 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、2018 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、2018 年 12 月に実施された分野横断的演習に参加した。
④ セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。	・ 重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2018 年度分野横断的演習への参加を促し、全体で過去最多の 3,077 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、2018 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。	・ 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、金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）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、オリパラ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において、内閣官房が作成した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の浸透状況を把握するための調査に協力した。
③ 本施策における調査・分析に関し、当該調査・分析の対象に関する情報及び当該調査・分析に必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査・分析が本施策における調査分析と関連する場合には、必要に応じて内閣官房と連携。	・ 重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・ 「ＥＵ諸国及び米国における情報共有体制に関する調査」については、重要インフラ所管省庁において、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。

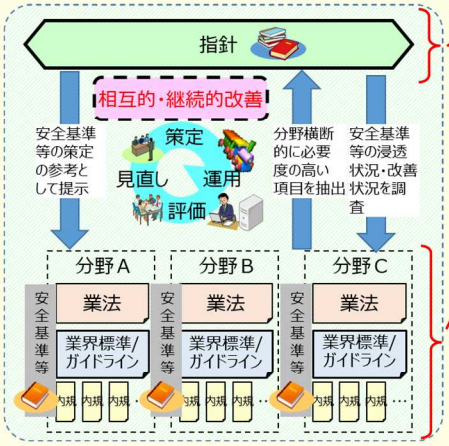
⑤ 重要インフラ事業者等のリスクコミュニケーション及び協議の支援。	・ 重要インフラ所管省庁において、重要インフラ事業者等の情報セキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象とした説明会、意見交換会等の開催に協力することにより、重要インフラ事業者等間のリスクコミュニケーション及び協議を支援した。
⑥ 重要インフラ事業者等が実施する対処態勢の整備並びにモニタリング及びレビューの必要に応じた支援。	・ 金融庁において、諸外国における「脅威ベースのペネトレーションテスト」の手法や海外金融機関の活用状況を把握するための外部委託調査を実施し、2018 年５月に「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」を公表した。また、大規模な金融機関に対し、サイバーセキュリティ対策の一層の高度化を図るため、「脅威ベースのペネトレーションテスト」の活用を促した。 ・ 厚生労働省において、2018 年度に策定した「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）」において、コンティンジェンシープランを位置付けた。
(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。	・ 厚生労働省において、2018 年度に策定した「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）」において、経営層が果たすべき役割を位置付けた。
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。	・ 厚生労働省において、医療分野におけるセプター構成員の拡充に関して支援を行った。 ・ 国土交通省において、重要インフラ分野に空港分野が追加となるよう調整する（2018 年７月 25 日に重要インフラ分野に追加）とともに、空港セプターに新たに参加する事業者についてセプター事務局と検討・調整を行った。
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。
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。	・ 重要インフラ所管省庁において、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。	・ 2018 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訓練に参加し、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ウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
(2)「障害対応体制の強化」に関する施策	
① 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。	・ 事案対処省庁は、2018 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、2018 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。	・ 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ウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

別添４－３　安全基準等の継続的改善状況等の把握及び検証

調査の目的

○重要インフラ防護能力の維持・向上を目的に、情報セキュリティ対策のＰＤＣＡサイクルを踏まえた「指針」及び「安全基準等」の相互的・継続的改善を目指す。このことから「安全基準等」の改善状況を年度ごとに調査し、重要インフラ専門調査会に報告するもの。



<指針>
「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」の略称

<安全基準等とは>
以下の総称
- 業法に基づき国が定める「強制基準」
- 業法に準じて国が定める「推奨基準」及び「ガイドライン」
- 業法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」
- 業法や国民・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

＊指針は含まない

【調査ポイント】
①ＰＤＣＡサイクルに基づく安全基準等の改善要否を判断するための分析・検証作業の取組状況の把握
②分析・検証の結果に基づく安全基準等の改定状況の把握
③指針の継続的改善に繋がる安全基準等の具体的な改定事例の抽出

調査対象一覧

分野		安全基準等名称
情報通信	電気通信	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） 電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則
	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	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 第9版 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		航空運送事業者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）
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１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３版）
電力		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 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 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		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
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
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３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

調査対象数：24件

調査結果一覧

分野		安全基準等名称	2018年度内の取組状況	
			分析・検証	改定
情報通信	電気通信	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） 電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則	実施した 実施した 実施中	実施した 実施した 実施していない
	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	実施していない 実施していない	実施していない 実施していない
	ケーブル	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＞	実施した	実施していない
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 第9版 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	実施していない 実施した 実施していない	実施していない 実施していない 実施していない
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）	実施した	実施した
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）	実施した	実施した
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）	実施した	実施した
電力		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 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 スマートメーターシステムセキュリティガイドライン	実施中 実施していない 実施していない 実施中	実施していない 実施していない 実施していない 実施していない
ガス		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	実施中	実施していない
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	実施した	実施した
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）	実施していない	実施していない
水道		水道分野における情報セキュリティガイドライン	実施した	実施した
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）	実施した	実施した
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	実施した	実施中
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	実施した	実施した
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	実施した	実施中

調査対象数：24件

安全基準等の継続的改善状況（概要）

○安全基準等の継続的改善における2018年度の取組状況及び改定状況については以下のとおり。

分析・検証後、改定を実施済：9件　　分析・検証後、改定を実施中：2件　　分析・検証を実施中：5件

（上記以外に昨年度に改定不要と判断したため、今年度は分析・検証を実施しなかった等が8件）

○安全基準等の分析・検証を行うに至った主な契機は以下のとおり。

- 指針の改定
- ITに係る環境変化の調査・分析からの課題発見
- 定期的に検証することとしている

（上記以外にも、 ユーザからの要望やIoTの普及や仮想化技術の進展などネットワークの環境変化に対応等もあった。）

○重要インフラの情報セキュリティ対策に係る第４次行動計画と指針に記載されている「機能保証の考え方」、「経営層の在り方」、「制御系セキュリティ」について、下記のことが考えられる。

- 指針の改訂に伴い、第5版で新たに記載された「機能保証の考え方」等の内容を踏まえた安全基準等の改善が見受けられ、リスクアセスメントの取組が一歩進んだ。
- 経営層の積極的関与や在り方についての記載が充実化されている安全基準等も存在し、経営層に対するアプローチの重要性が認識されてきていることが認められる。
- OT（制御系）とIT（情報系）を含めた内容の記載のある安全基準等もあることから、制御系を含めた意識醸成がされ始めていることが確認できる。

安全基準等の継続的改善状況（詳細 1/12）

分野		情報通信（電気通信）	情報通信（電気通信）
名称		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）
発行主体等		総務省	一般社団法人電気通信事業者協会
最新改定／新規作成年月		2015年4月	2018年10月
分析・検証状況	分析検証の実施状況	2018年度中に実施済	2018年度に実施済
	分析検証の実施契機	その他状況の変化等（平成29年８月にGoogleを起因とする大規模なインターネット障害が発生したことを踏まえ、その対象について分析・検証を実施。）	安全基準等策定指針の改定（第5版への改定） / ITに係る環境変化の調査・分析からの課題発見 / サイバー攻撃動向を受けて
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2017年12月～2018年９月 （２）情報通信審議会 情報通信技術分科会 IPネットワーク設備委員会 （３）同委員会は、近年のIoTの普及に伴う通信ネットワークの高度化や利用形態の多様化を踏まえ、「IoTの普及に対応した電気通信設備に係る技術的条件」について検討（合計８回）。同委員会の検討結果について、情報通信審議会情報通信技術分科会で審議が行われ、一部答申を受けたため、改定を行うことが正式決定。	（１）2018年4月～2019年3月 （２）一般社団法人電気通信事業者協会　安全・信頼性協議会　安全基準検討ワーキンググループ （３）同ワーキンググループで分析・検証し、改定が必要な場合は同WGで改定案を作成・検討し、策定する。
改定状況	改定の実施状況	2018年度中に実施済	2018年度に実施済
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2019年３月 （２）総務省総合通信基盤局電気通信事業部電気通信技術システム課安全・信頼性対策室 （３）2018年12月下旬から１か月間、改定案について意見募集を実施し、その結果に基づき、2019年３月末までに改定を実施する予定。	（１）2018年10月 （２）一般社団法人電気通信事業者協会　安全・信頼性協議会　安全基準検討ワーキンググループ （３）同ワーキンググループで改定案を作成・検討し、策定。
	改定内容	大規模インターネット障害に関し、事業者等に推奨する対策の追加	主として、NISC指針第5版で記載されたリスクアセスメントのうち、「機能保証の考え方」を踏まえた継続的な改善に取り組む必要性、経営層の積極的な関与・在り方についての記載充実化・明確化、「サイバー攻撃リスクの特性」「対策の考慮事項」の整理、OT(制御系)含めたCSIRTの構築や人材育成、の4点を反映した。
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目、第4版の記載項目）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目		なし	ISO/IEC27001:・27002:2013の要素を取り入れるとともに、ISO/IEC27017:2015（クラウドサービスのための実践規範）を取り入れた。

安全基準等の継続的改善状況（詳細 2/12）

分野		情報通信（電気通信）	情報通信（放送）
名称		事業用電気通信設備規則 ※電気通信事業法、電気通信事業法施行規則は改定なし	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
発行主体等		総務省	放送セプター（日本放送協会（NHK）、一般社団法人日本民間放送連盟）
最新改定／新規作成年月		2015年11月27日	2016年10月
分析・検証状況	分析検証の実施状況	実施中	2018年度に実施予定なし (理由：放送設備サイバー攻撃対策ガイドラインの現場への浸透を進めているため、本ガイドラインの分析・検証は2019年度以降に実施予定)
	分析検証の実施契機	その他状況の変化等（IoTの普及や仮想化技術の進展などネットワークの環境変化に対応して、設備の維持・管理に求められる知識、能力の確保の在り方や将来にわたっての人材の確保・育成の方策等について検討する必要があるため。）	－
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年10月～ （２）情報通信審議会（情報通信技術分科会ＩＰネットワーク設備委員会） （３）2019年5～6月頃に一部答申を予定。	－
改定状況	改定の実施状況	－	－
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	－
	改定内容	－	－
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		いいえ（本件は、事業用電気通信設備の技術基準に特化した内容であるため）	はい（第4版の記載項目）
独自記載項目		なし	なし

安全基準等の継続的改善状況（詳細 3/12）

分野		情報通信（放送）	情報通信（ケーブルテレビ）
名称		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＞
発行主体等		一般社団法人ICT-ISAC放送設備サイバー攻撃対策ＷＧ	一般社団法人日本ケーブルテレビ連盟（通信・放送制度委員会）
最新改定／新規作成年月		2018年6月	2012年11月
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2018年6月に作成）	2018年度に実施済
	分析検証の実施契機	―	定期的に検証することとしている
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	（１）毎年4～5月 （２）通信・放送制度委員会 （３）通信・放送制度委員会配下のセキュリティWGにて改訂の必要性を検討→通信・放送制度委員会で承認を行う。
改定状況	改定の実施状況	―	実施不要と判断（理由：既存内容を確認した結果、大きな変更は必要ないと判断し、次回は2019年度に検討を行うと判断した。
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	―
	改定内容	―	―
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		いいえ（本ドキュメントは、放送設備のサイバー攻撃の対策に特化しており、該当部分のみを参照した）	いいえ（各ケーブルテレビ事業者に対して災害や事業環境変化による経営危機に備えるために経営戦略と連動したBCPの策定を促進させている。本ガイドラインは業界におけるセキュリティ対策の留意点をまとめたものであり、BCPの一部として位置付けている。）
独自記載項目		なし	なし

安全基準等の継続的改善状況（詳細 4/12）

分野		金融	金融
名称		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 第9版
発行主体等		公益財団法人　金融情報システムセンター（FISC）	公益財団法人　金融情報システムセンター（FISC）
最新改定／新規作成年月		2008年６月	2018年3月
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：次年度以降に改訂の要否含め検討予定）	2018年度中に実施済
	分析検証の実施契機	―	ITに係る環境変化の調査・分析からの課題発見
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	（１）2018年7月～2019年3月 （２）安全対策専門委員会、安全対策に関する検討部会 （３）金融機関、ＩＴベンダー等から構成される安全対策専門委員会等を2018年12月から開催し、会員意見を踏まえ 2019年3月までに改訂内容を決定する予定。
改定状況	改定の実施状況	―	―
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	―
	改定内容	―	―
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目）	はい（第5版の記載項目）
独自記載項目		金融機関における固有業務や設備設置に係る基準等	金融機関における固有業務や設備設置に係る基準等

安全基準等の継続的改善状況（詳細 5/12）

分野		金融	航空
名称		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
発行主体等		公益財団法人　金融情報システムセンター（FISC）	国土交通省
最新改定／新規作成年月		2017年５月	2019年（平成31年）3月29日
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2016年度に分析・検証実施済）	2018年度に実施済
	分析検証の実施契機	－	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	（１）2018年（平成29年）4月～2018年（平成30年）12月 （２）国土交通省、航空運送事業者、定期航空協会 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考。
改定状況	改定の実施状況	2019年度以降に先送り（理由：2017年度にサイバー攻撃対応に係る改訂を実施し、2017年５月に第３版追補３を発刊したため）	2018年度に実施済
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	（１）2018年4月～2019年3月末 （２）国土交通省 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）（以下「策定指針」という。）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。
	改定内容	－	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・ガイドライン名称の見直し　　・全体構成や表現の見直し
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目		金融機関における固有業務や設備設置に係る基準等	政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。

安全基準等の継続的改善状況（詳細 6/12）

分野		空港	鉄道
名称		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
発行主体等		国土交通省	国土交通省
最新改定／新規作成年月		2019年（平成31年）3月29日	2019年（平成31年）3月29日
分析・検証状況	分析検証の実施状況	2018年度に実施済	2018年度に実施済
	分析検証の実施契機	安全基準等策定指針の改定（第5版への改定）	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年（平成29年）4月～2018年（平成30年）12月 （２）国土交通省、主要な空港・空港ビル事業者 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考。	（１）2018年（平成29年）4月～2018年（平成30年）12月 （２）国土交通省、重要インフラ事業者等 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考。
改定状況	改定の実施状況	2018年度に実施済	2018年度に実施済
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年4月～2019年3月末 （２）国土交通省 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）（以下「策定指針」という。）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。	（１）2018年4月～2019年3月末 （２）国土交通省 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）（以下「策定指針」という。）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。
	改定内容	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・全体構成や表現の見直し	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・全体構成や表現の見直し
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目、第4版の記載項目）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目		政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。	政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。

安全基準等の継続的改善状況（詳細 7/12）

分野		電力	電力
名称		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
発行主体等		一般社団法人　日本電気協会	経済産業省
最新改定／新規作成年月		2016年5月	2018年10月
分析・検証状況	分析検証の実施状況	実施中	2018年度に実施予定なし（理由：引用している民間規格が改定手続き中で、改定が次年度になるため）
	分析検証の実施契機	その他状況の変化等（ユーザーからの要望による）	―
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）２０１８年１２月～２０１９年１０月 （２）情報専門部会 （３）電気事業者主体の分科会・作業会で、分析・検証を実施。改定案も含めて検討し、上位の会議体で審議。	―
改定状況	改定の実施状況	―	―
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	―
	改定内容	―	―
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目）	はい（第5版の記載項目）
独自記載項目		電力制御システムに特化する内容は安全基準等策定指針には含まれていないことがある。	電力制御システムやスマートメーターに特化する内容は安全基準等策定指針には含まれていないことがある。

安全基準等の継続的改善状況（詳細 8/12）

分野		電力	電力
名称		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	スマートメーターシステムセキュリティガイドライン
発行主体等		経済産業省	一般社団法人　日本電気協会
最新改定／新規作成年月		2016年9月	2016年3月
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2016年度に改定されたところであり、環境変化がないため。）	実施中
	分析検証の実施契機	―	安全基準等策定指針の改定（第5版への改定）/その他状況の変化等（ユーザーからの要望による）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	（１）２０１８年１２月～２０１９年１０月 （２）情報専門部会 （３）電気事業者主体の分科会・作業会で、分析・検証を実施。改定案も含めて検討し、上位の会議体で審議。
改定状況	改定の実施状況	―	―
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	―	―
	改定内容	―	―
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		いいえ（本ドキュメントは保安規程の記載事項に特化した内容のため、該当部分のみを参照。）	はい（第5版の記載項目）
独自記載項目		なし	スマートメーターシステムに特化している内容は安全基準等策定指針に含まれていないことがある

安全基準等の継続的改善状況（詳細 9/12）

分野		ガス	政府・行政サービス
名称		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	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
発行主体等		一般社団法人　日本ガス協会	総務省自治行政局地域情報政策室
最新改定／新規作成年月		2016年7月	2018年9月
分析・検証状況	分析検証の実施状況	実施中	2018年度に実施予定なし（理由：2017年以前に分析・検証実施済）
	分析検証の実施契機	その他状況の変化等（2018年3月METIガス安全小委員会を踏まえ、都市ガス業界におけるサイバーセキュリティ保安規程化が決定したため）	ー
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年4月～2019年3月（予定） （２）JGAシステムセキュリティWG （３）保安規程化の決定を踏まえ、要領改訂内容についてシステムセキュリティWGにて検討中。その結果を、上位組織の保安対策小委員会に報告し、改訂を行うことを正式決定予定。	ー
改定状況	改定の実施状況	ー	2018年度に実施済
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	ー	（１）平成29年12月～平成30年9月 （２）総務省自治行政局地域情報政策室（調査研究受託事業者：日本電気株式会社） （３）①改定項目の整理→②有識者へのヒアリング→③改定案の作成→④有識者検討会議の開催→⑤パブコメ→⑥改定
	改定内容	ー	「政府機関の情報セキュリティ対策の統一基準」等の反映
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目、第4版の記載項目）	はい（第4版の記載項目）
独自記載項目		なし	なし

安全基準等の継続的改善状況（詳細 10/12）

分野		医療	水道
名称		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）	水道分野における情報セキュリティガイドライン
発行主体等		厚生労働省	厚生労働省　医薬・生活衛生局水道課
最新改定／新規作成年月		2017年５月	2019年３月
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2017年以前に分析・検証実施済のため）	2018年度に実施済
	分析検証の実施契機	ー	安全基準等策定指針の改定（第5版への改定、第4版への改定）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	ー	（１）2018年4月～2019年3月 （２）厚生労働省医薬・生活衛生局水道課 （３）第4次行動計画等に基づき、安全基準等の改定を行った。
改定状況	改定の実施状況	実施不要と判断（理由： 2017年度に改定実施済みのため）	2018年度に実施済
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	ー	（１）2018年4月～2019年3月 （２）厚生労働省医薬・生活衛生局水道課 （３）第4次行動計画等に基づき、安全基準等の改定を行った。
	改定内容	ー	指針等を参考にして、PDCAサイクルによる情報セキュリティ対策の実施と見直しの考え方の充実、情報セキュリティの取組における経営層の役割の追加、最高情報セキュリティ責任者の役割の充実、インシデント発生時における対応の追加、平時及びインシデント発生時における関係機関との連携体制の追加等を行った。
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		いいえ（安全基準等策定指針よりも国内の法令や現場の実態に沿った要件を重視したため）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目		なし	なし

安全基準等の継続的改善状況（詳細 11/12）

分野		物流	化学
名称		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	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
発行主体等		国土交通省	石油化学工業協会
最新改定／新規作成年月		2019年（平成31年）3月29日	2015年3月
分析・検証状況	分析検証の実施状況	2018年度に実施済	2018年度に実施済
	分析検証の実施契機	安全基準等策定指針の改定（第5版への改定）	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年（平成29年）4月～2018年（平成30年）12月 （２）国土交通省総合政策局物流政策課、重要インフラ事業者及び業界団体（１７社６団体） （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考。	（１）2018年4月～2018年7月 （２）石油化学工業協会 情報通信委員会 情報セキュリティWG （３）WGで第5版に則り分析・検証し、安全基準の改定が必要と判断
改定状況	改定の実施状況	2018年度に実施済	実施中
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年4月～2019年3月末 （２）国土交通省 （３）「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月改定）（以下「策定指針」という。）を踏まえるとともに「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。	（１）2018年7月～2019年5月 （２）石油化学工業協会 情報通信委員会 情報セキュリティWG （３）WGで改定案を作成し、情報通信委員会で承認を得る予定
	改定内容	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・全体構成や表現の見直し	リーダーシップの観点、リスクアセスメント、リスク対応などを追加、充実
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目、第4版の記載項目）	いいえ（この点も含めて、安全基準等の継続的改善のために分析・検証を実施しているところである。）
独自記載項目		政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。	なし

安全基準等の継続的改善状況（詳細 12/12）

分野		クレジット	石油
名称		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
発行主体等		一般社団法人　日本クレジット協会	石油連盟
最新改定／新規作成年月		2018年4月（最新改定）/2014年12月（新規）	2017年5月26日
分析・検証状況	分析検証の実施状況	2018年度に実施済	2018年度に実施済
	分析検証の実施契機	ITに係る環境変化の調査・分析からの課題発見	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年4月に、日本クレジット協会クレジットCEOTOAR運営会議において協議	（１） （２）石油連盟　サイバーセキュリティ専門委員会 （３）指針第5版の改定内容や各社の取り組み状況を踏まえ、ITセキュリティ連絡会にて改定することを決定
改定状況	改定の実施状況	2018年度に実施済	実施中
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	（１）2018年4月に、日本クレジット協会クレジットCEOTOAR運営会議において協議	（１）未定 （２）石油連盟　サイバーセキュリティ専門委員会、危機管理委員会 （３）サイバーセキュリティ専門委員会にて改定原案作成済。今後、上部組織である危機管理委員会を得て、正式改定となる
	改定内容	障害発生時に重要インフラ事業者が報告を行う際の「インシデント報告書（重要インフラサービス障害）」のフォーマットの変更	『指針第4版』の以下の新たな要請項目について「実施が望ましい項目」として追記 ①経営層の果たすべき役割、経営層による情報セキュリティ対策の運用状況把握 ②抽出した課題に基づくリスク評価の実施 ③基本方針の策定・見直しの実施 ④情報セキュリティ対策に係るロードマップの作成・見直しの実施
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか		はい（第5版の記載項目） ※「クレジットCEPTOARにおける情報セキュリティガイドライン」には記載していないが、重要インフラについては、割賦法のもと、PCIDSS準拠が義務付けられている。PCIDSSでは、「安全基準等策定指針」の記載項目をカバーしていることを包括的に確認している。	はい（第5版の記載項目）
独自記載項目		なし	なし

別添４－４　安全基準等の浸透状況等に関する調査（アンケート調査）

アンケート調査の目的、概要及び内容

◆アンケート調査の目的

アンケート調査は、重要インフラ所管省庁（以降、所管省庁）や業界団体等が定める「安全基準等」※1が、重要インフラ事業者等（以下、事業者等）にどの程度浸透しているかを把握することを目的として、毎年、事業者等の情報セキュリティに関する取組状況を確認し、その分析結果を公表するものです。

アンケート調査への回答を通じて、事業者等が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できることを目指すと共に、アンケート調査で得られた知見や課題は重要インフラ防護能力のための各施策へと展開します。

◆アンケート調査の概要

・アンケート調査対象範囲　　：所管省庁にて調査対象の事業者等を決定
・アンケート調査方法と調査基準日：以下の方法のいずれかを所管省庁が選択
　① NISCが準備する調査票（アンケート）を活用　　（基準日：2018年3月末日）
　② 関連組織が独自に行う調査の結果をNISCで読み替え（基準日：各調査で設定した基準日）

注）今年度より政府・行政サービス分野は、NISCが準備する調査票（アンケート）を利用して回答を実施しているため、一部の設問で回答の傾向が大幅に変化している。

◆アンケート調査の内容

・安全基準等の整備・浸透に係る事項：① 行動計画※2や指針※3、リスクアセスメント手引書※4等の認知状況
　② 事業者等が定める内規の策定・見直しの状況　等
・情報セキュリティ対策の実施に係る事項：　PDCAサイクルに沿った具体的な情報セキュリティ対策の取組状況
・意見、要望

※1 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。

※2 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　（サイバーセキュリティ戦略本部決定）
昨今のサイバー攻撃による急速な脅威の高まりや、2020東京オリンピック・パラリンピック競技大会も見据え、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。

※3 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決定）
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。

※4 重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第1版）　（サイバーセキュリティ戦略本部決定）
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。

重要インフラ分野のアンケート調査状況

NISC独自アンケートの配布は重要インフラ13分野(*1)の2,610事業者等。回答は1,381事業者等。
（昨年度比　配布数：284%　回答数：200%　回答率：-22.1ﾎﾟｲﾝﾄ*1 ）(*2)

重要インフラ分野		調査対象範囲	アンケート配布数	アンケート回収数	調査方法
情報通信	電気通信	T-CEPTOAR構成各社、電気通信事業者協会正会員各社	72	23	NISC調査
情報通信	ケーブルテレビ	ケーブルテレビセプターに加盟する事業者	334	125	NISC調査
情報通信	放送	日本放送協会（ＮＨＫ）、地上系民間基幹放送事業者（多重単営社及びコミュニティ放送事業者を除く）	196	191	NISC調査
金融		銀行等、証券会社、生命保険会社、損害保険会社	(799)	(669)	独自調査(*3)
航空		航空運送事業者	2	1	NISC調査
鉄道		鉄道CEPTOAR構成員事業者	22	19	NISC調査
電力		一般送配電事業者、主要な発電事業者	12	12	NISC調査
ガス		ガスセプターを構成する主要ガス事業者	11	11	NISC調査
政府・行政サービス		地方公共団体	1,788	866	NISC調査
医療		電子カルテ等の医療情報システムを導入している医療機関の中からランダムで選定した事業者	31	18	NISC調査
水道		現在給水人口30万人以上の水道事業者又は水道用水供給事業者	79	70	NISC調査
物流		物流CEPTOAR構成員事業者	17	11	NISC調査
化学		石油化学工業協会に加盟する事業者のうち主にエチレンセンターを運営する企業	13	9	NISC調査
クレジット		リスクアセスメント対象会社（自社でオーソリゼーションシステムを保有しているクレジットセプター構成員）	21	18	NISC調査
石油		石油精製企業	12	7	NISC調査
全分野合計		－－－	2,610 (3,409)	1,381 (2,050)	－－－

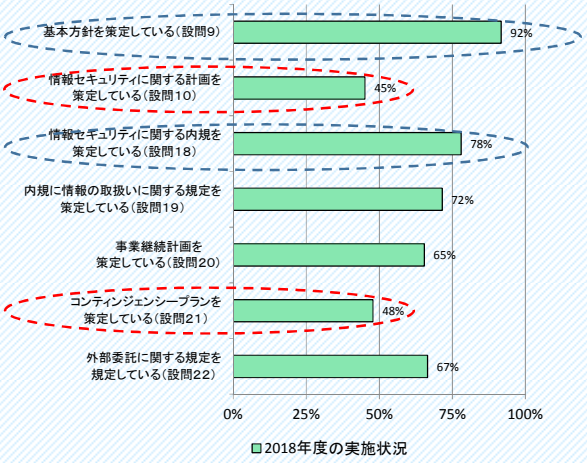
＊１：2018年3月末日基準のアンケート調査のため、2018年7月に重要インフラ分野として追加された「空港分野」は対象外である。
＊２：政府・行政サービス分野が、今年度からNISC独自アンケートを利用して、回答を実施したため。
＊３：金融機関等のシステムに関する動向及び安全対策実施状況調査（調査基準日：2018年3月31日）

アンケート調査の要約（１/５）

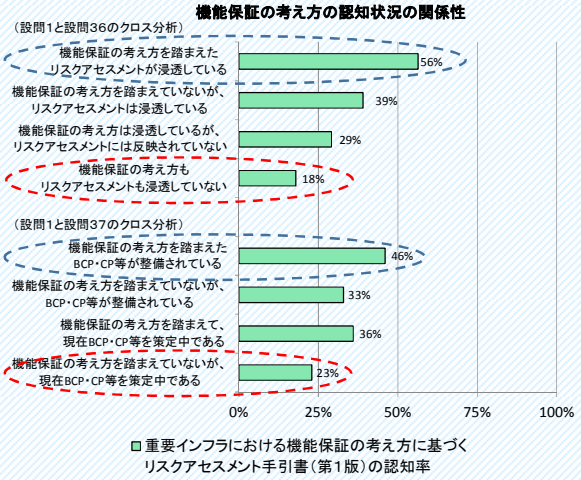
(1) 規定類の整備状況と機能保証の考え方についての状況

- 基本方針や情報セキュリティに関する内規が策定されている（グラフ① 青枠内）。一方で、情報セキュリティに関する計画・コンティンジェンシープランが策定されていない（グラフ① 赤枠内）。
  新たなリスクに対応し続けていくための計画である情報セキュリティリスク対応計画や初動対応（緊急時対応）の方針を定めたコンティンジェンシープランを策定する事業者を増やし、対処態勢整備を強化することが重要である。
- リスクアセスメント手引書を認知している事業者等は、「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及びBCP・CPの整備が進んでいる（グラフ② 青枠内）。一方で、認知していない事業者等は取組が遅れている（グラフ② 赤枠内）。
  サイバーセキュリティ戦略にも記載されている、「任務保証」の考え方を踏まえたリスクアセスメント、BCP・CPの策定が重要であるため、見直し等により「機能保証」の考え方が盛り込まれるよう、リスクアセスメント手引書を普及・啓発が重要である。

グラフ① 各種規程類の整備状況（複数回答）



グラフ② リスクアセスメント手引書の認知状況と機能保証の考え方の認知状況の関係性

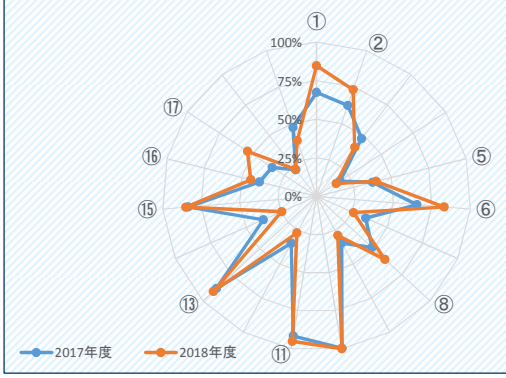


アンケート調査の要約（２/５）

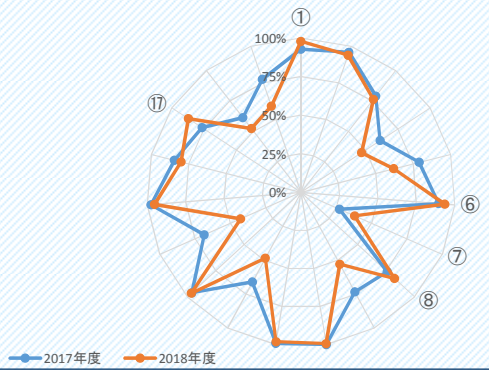
(2) 対策状況

- 従業員1,000人以下の企業（グラフ①）は、昨年からの各対策の強化による影響により以下の良化ポイントが見られる。
  ①情報セキュリティ対策に関する基本方針の策定　②情報セキュリティに関する内規の策定状況
  ⑤情報セキュリティ対策に関する計画策定状況　⑥情報セキュリティ対策の実施に向けた予算の確保状況
  ⑧全従業員向けセキュリティ研修の実施状況　⑪責任者へのセキュリティ対策の運用報告
  ⑬障害発生時における連絡体制の整備状況　⑮脅威や脆弱性等の情報収集
  ⑯情報セキュリティに関する監査実施状況　⑰外部の演習等への参加状況
- 従業員1,001人以上の企業（グラフ②）は、昨年からの各対策の強化による影響により以下の良化ポイントが見られる。
  ①情報セキュリティ対策に関する基本方針の策定　⑥情報セキュリティ対策の実施に向けた予算の確保状況
  ⑦セキュリティ人材の確保状況　⑧全従業員向けセキュリティ研修の実施状況
  ⑰外部の演習等への参加状況
- PDCAサイクルにおいて、取組が進んでいない（グラフ①,②上凹んでいる）項目については、取組が進んでいる事業者等に往訪調査等で確認し、全体を真円に近づけられるよう、得られた結果を展開する必要がある。

グラフ① 行動計画テーマ別グラフ（従業員1,000名以下）



グラフ② 行動計画テーマ別グラフ（従業員1,001名以上）

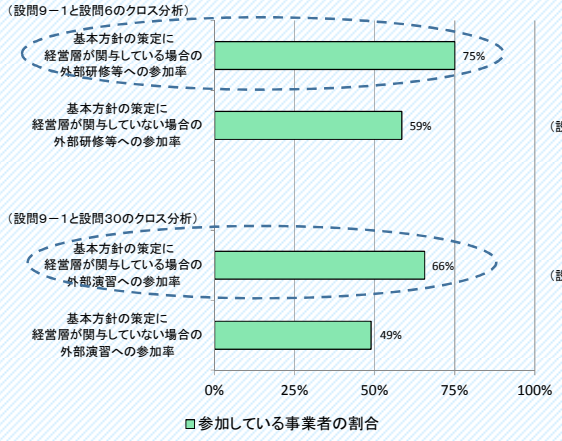


アンケート調査の要約（３/５）

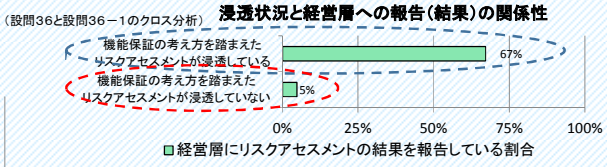
(3) 経営層の関与状況

- 基本方針の策定に経営層が関与している事業者等は、他事業者等の取組事例や外部研修等で推奨されている内容を把握するために、外部での研修や演習等に参加している傾向があるため、他事業者動向を認識する意義も含めて、分野横断的演習の参加を推奨していく必要がある（グラフ①）。
- 機能保証の考え方を踏まえてリスクアセスメントを実施している事業者は、経営層までリスクアセスメントの報告を行っている傾向があるため、機能保証の考え方を普及・啓発していくことが重要である（グラフ②）。
- リスク対応において経営層が積極的に関与している事業者等は、情報資産管理や管理している資産の格付けを実施している傾向があるため、リスク対応に関して、経営層に働きかけていく必要性が認められる（グラフ③）。

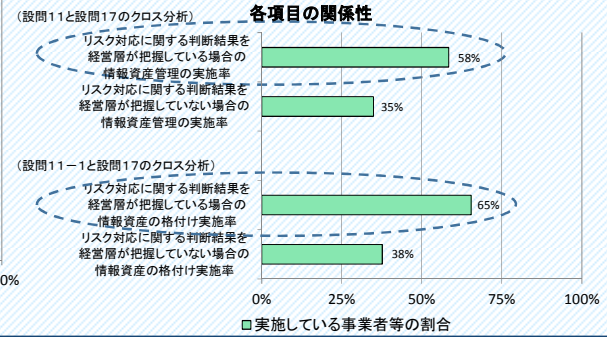
グラフ① 基本方針策定時の経営層の関与と各項目の関係性



グラフ② 機能保証の考え方（リスクアセスメント）の浸透状況と経営層への報告（結果）の関係性



グラフ③ リスク対応における経営層の関与と各項目の関係性

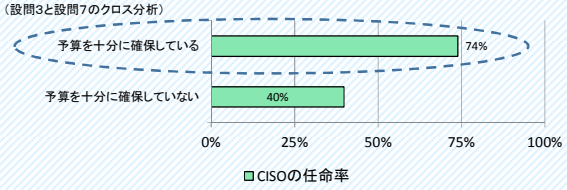


アンケート調査の要約（４/５）

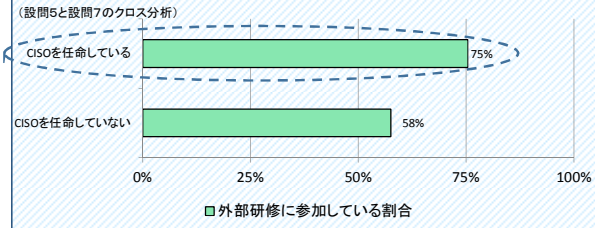
(4) CISOの任命状況

- 情報セキュリティ対策の実施を取り組む上で十分な予算が確保されている事業者等は、CISOを任命している割合が高く、経営層の働きかけにより、確保されていると考えられる（グラフ①）。
- CISOを任命している事業者等は、セキュリティ人材を育てるために、積極的に外部への研修に参加している（グラフ②）。
- 内規等を策定する際の参考文献として、所管省庁が発行しているガイドライン・指針等を参考にしている事業者等は、CISOを任命している傾向がある。NISCが定めている安全基準等策定指針にもCISOの任命を求めていることが、所管省庁発行のガイドライン・指針等に反映されているためであると考えられる（グラフ③）。

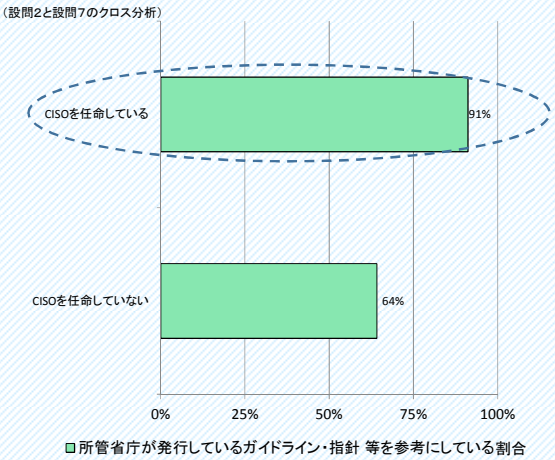
グラフ① 予算の確保状況とCISOの任命状況の関係性



グラフ② CISOの任命状況と外部研修の参加状況の関係性



グラフ③ CISOの任命状況と内規等を策定する際の参考文献の関係性



アンケート調査の要約（５／５）

(5) 自由意見

【安全基準等に関する意見・要望等】

- 事業規模を考慮した基準等や費用対効果の高い対策等の例示の要望があった。
  （備考：事業規模の小さい事業者の人材育成、費用を抑える仕組み等）
  ＜参考例＞ 中小企業の情報セキュリティ対策ガイドライン第３版　等　（IPA）
  サイバーセキュリティ経営ガイドラインVer 2.0実践のためのプラクティス集　等（IPA）

【安全基準等策定指針（第5版）に関する意見・要望等】

- 指針を活用したガイドラインにおいて、一部分野で参考資料としてチェックシートが作成されているが、多くの分野で対策例を示してほしいという要望があった。
  ＜参考例＞対策例：補完調査報告書（NISC）等

【情報共有体制に関する意見・要望等】

- 情報共有方法（メール、システム、電話等）の統一化してほしい。
- 最新の重要インシデント（ヒヤリハット含む）を早期に情報、評価結果、対策を情報共有できる体制。
- 報告ルート一本化による事業者負担を軽減してほしい。
- 情報システム部とセキュリティベンダーの月例会を実施し、サイバーセキュリティインシデントに関する情報交換を行っている。

【その他の意見・要望等】

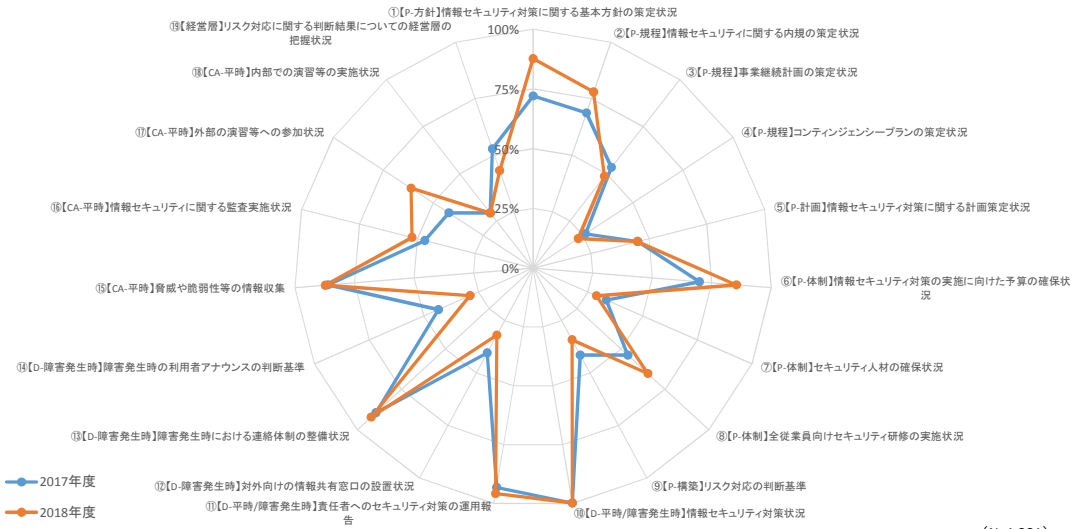
- 初心者でもわかりやすい解説がほしい。
  ＜参考例＞　関連JIS　Q 27001の解説書　等
- 担当者が少ない事業者向けの良好事例を紹介してほしい。
  ＜参考例＞　中小企業における情報セキュリティ対策の実態調査（IPA）　等
- 国の演習や人材育成等の紹介してほしい。
  ＜参考例＞　CYDER（NICT）、分野横断的演習（NISC）等

アンケート調査結果概要　－　PDCA サイクルに沿った対策状況（１／４）　－

(1) 全分野の重要インフラ事業者

※2018年度は金融分野を、
2017年度は金融・自治分野を除く

行動計画のテーマ別グラフ（レーダーチャート（全分野集計））



（N=1,381）

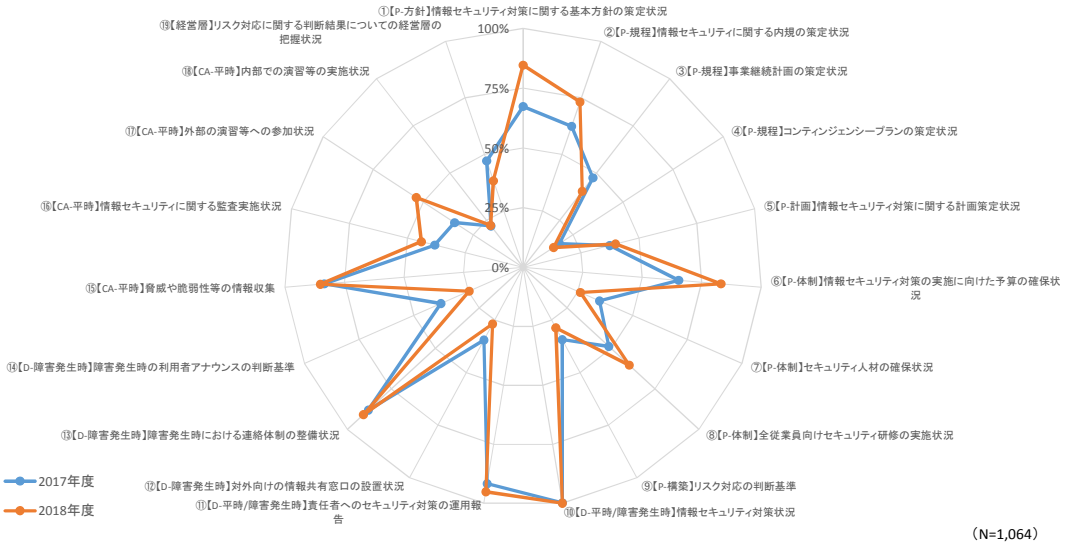
	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	72.0%	68.6%	53.4%	26.2%	45.1%	69.9%	33.4%	53.9%	41.5%	99.9%	93.1%	40.4%	89.5%	43.3%	86.1%	46.8%	42.2%	29.3%	52.8%
2018年度	87.6%	77.9%	48.6%	22.5%	45.0%	85.4%	28.9%	65.3%	34.2%	99.7%	95.7%	31.9%	92.1%	28.8%	87.4%	52.3%	61.0%	29.2%	43.2%
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

アンケート調査結果概要　－　PDCA サイクルに沿った対策状況（２／４）　－

(2) 従業員1000名以下の重要インフラ事業者

※2018年度は金融分野を、2017年度は金融・自治分野を除く

行動計画のテーマ別グラフ（レーダーチャート（1,000名以下の事業者等））



（N=1,064）

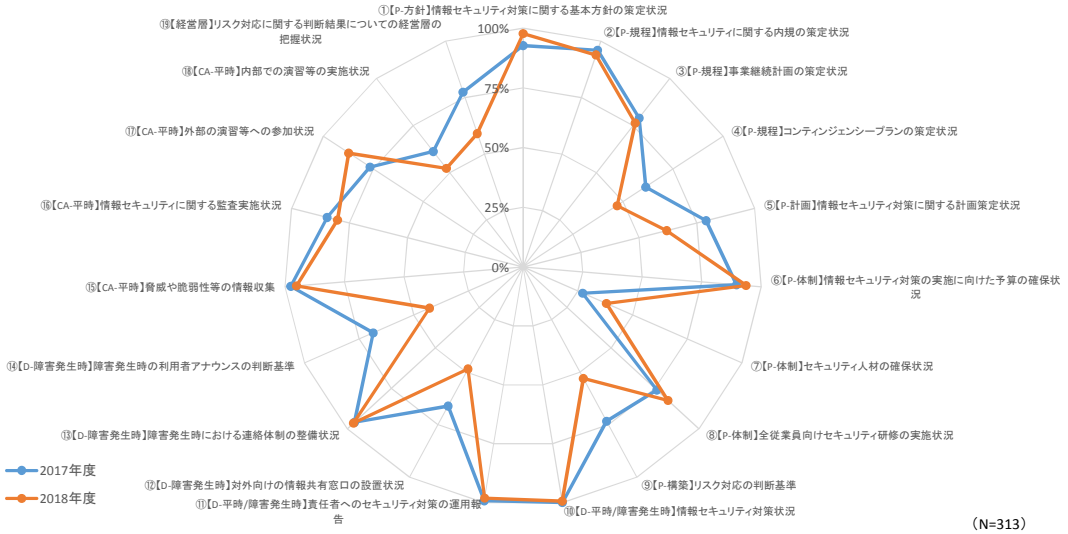
	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	67.3%	62.4%	47.5%	18.2%	37.4%	65.3%	34.9%	48.8%	34.3%	99.8%	91.7%	34.5%	88.1%	37.6%	83.5%	38.2%	34.3%	22.0%	47.2%
2018年度	84.7%	73.2%	40.3%	15.2%	39.9%	83.1%	26.1%	60.3%	28.8%	100%	95.1%	26.9%	90.9%	24.6%	85.2%	44.0%	53.5%	22.3%	38.3%
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

アンケート調査結果概要　－　PDCA サイクルに沿った対策状況（３／４）　－

(3) 従業員1,001名以上の重要インフラ事業者

※2018年度は金融分野を、2017年度は金融・自治分野を除く

行動計画のテーマ別グラフ（レーダーチャート（1,001名以上の事業者等））

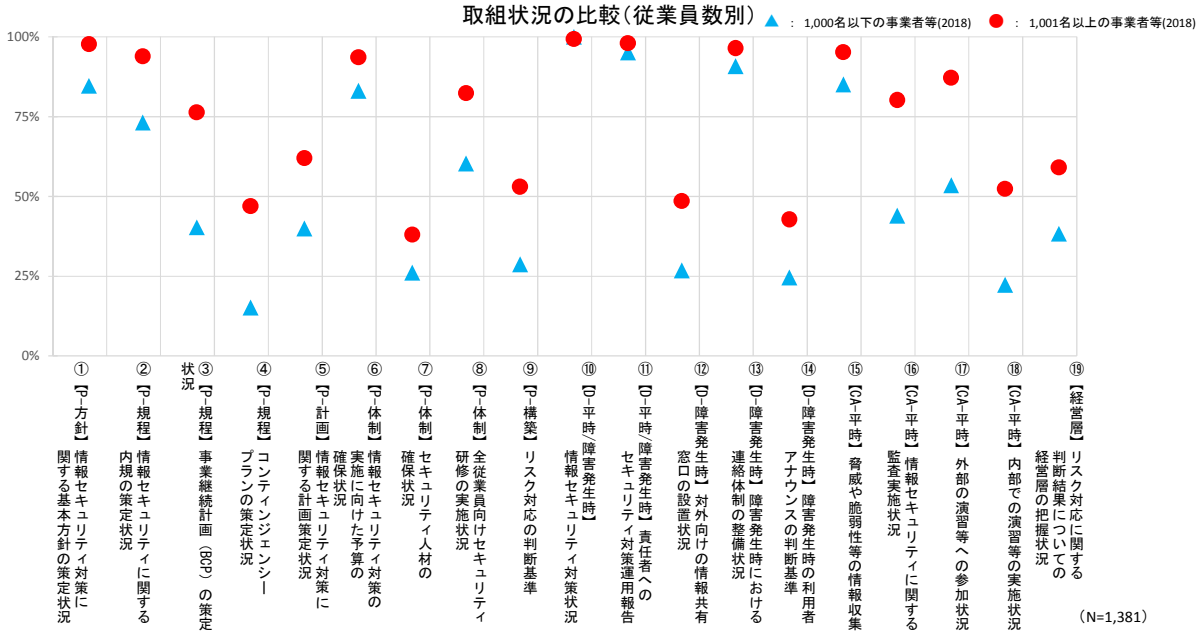


（N=313）

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲
2017年度	92.7%	96.0%	79.0%	61.3%	79.0%	89.6%	27.2%	76.0%	73.4%	100.0%	99.2%	66.1%	96.0%	68.5%	97.6%	84.7%	76.6%	61.3%	77.4%
2018年度	97.8%	93.9%	76.4%	47.0%	62.0%	93.6%	38.0%	82.4%	53.0%	99.4%	98.1%	48.6%	96.5%	42.8%	95.2%	80.2%	87.2%	52.4%	59.1%
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

アンケート調査結果概要　－　PDCA サイクルに沿った対策状況（４／４）　－

(4) 従業員1,000名以下と1,001名以上の重要インフラ事業者の対策状況の比較（2018年度）

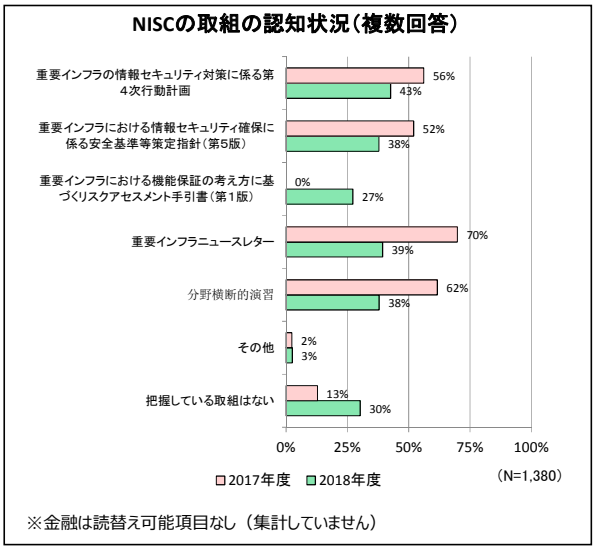


	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪		⑫		⑬		⑭		⑮		⑯		⑰		⑱		⑲	
	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●
2017年度	67.3%	92.7%	62.4%	96.0%	47.5%	79.0%	18.2%	61.3%	37.4%	79.0%	65.3%	89.6%	34.9%	27.2%	48.8%	76.0%	34.3%	73.4%	99.8%	100.0%	91.7%	99.2%	34.5%	66.1%	88.1%	96.0%	37.6%	68.5%	83.5%	97.6%	38.2%	84.7%	34.3%	76.6%	22.0%	61.3%	47.2%	77.4%
2018年度	84.7%	97.8%	73.2%	93.9%	40.3%	76.4%	15.2%	47.0%	39.9%	62.0%	83.1%	93.6%	26.1%	38.0%	60.3%	82.4%	28.8%	53.0%	100.0%	99.4%	95.1%	98.1%	26.9%	48.6%	90.9%	96.5%	24.6%	42.8%	85.2%	95.2%	44.0%	80.2%	53.5%	87.2%	22.3%	52.4%	38.3%	59.1%
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

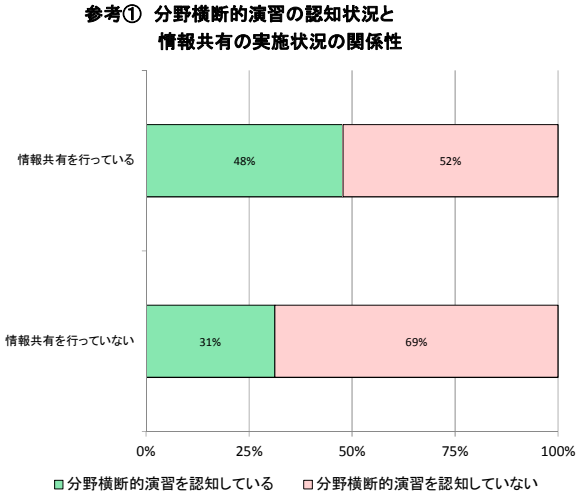
アンケート調査結果詳細　－　（１／５８）　－

設問1　NISCの取組の認知状況

・行動計画や指針、リスクアセスメント手引書を認知している事業者等は、セキュリティ対策が進んでいる傾向がある。分野横断的演習を認知している事業者等は、情報共有を行っている傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

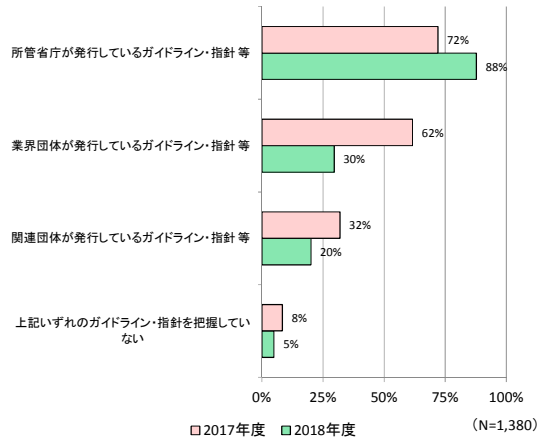


アンケート調査結果詳細　－　（２/５８）　－

設問2　自分野の安全基準等の認知状況

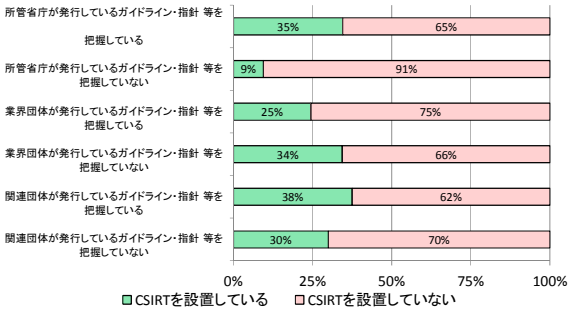
・CSIRTを設置している事業者は所管省庁が発行しているガイドライン・指針等を認知している傾向がある（参考①）。また、基本方針、計画、内規等の作成、外部演習への参加も同じ傾向がある。
・業界団体や関連団体が発行しているガイドラインや指針を確認している事業者等は、事業継続計画（BCP）やコンティンジェンシープラン（CP）を策定している傾向がある（参考②）。

自分野の安全基準等の認知状況（複数回答）

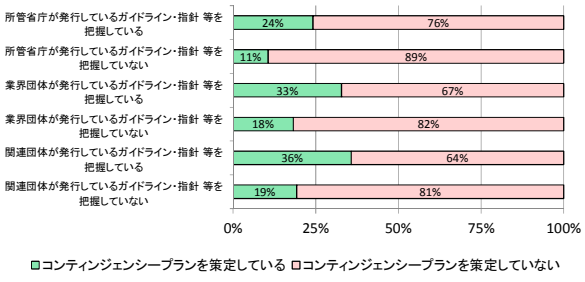


※金融は読替え可能項目なし（集計していません）

参考①　自分野の安全基準等の認知状況とCSIRTの設置状況の関係性



参考②　自分野の安全基準等の認知状況とコンティンジェンシープラン（CP）策定状況の関係性

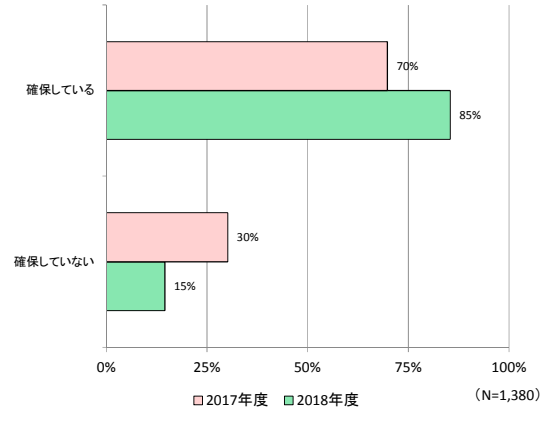


アンケート調査結果詳細　－　（３/５８）　－

設問3　情報セキュリティ対策の実施に向けた予算の確保状況

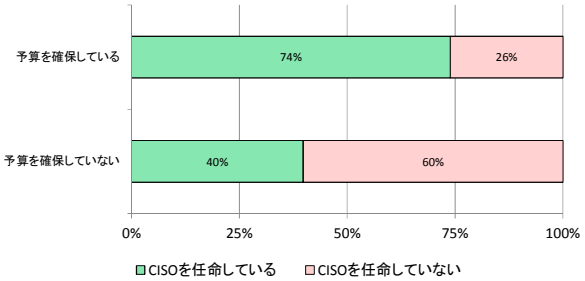
・情報セキュリティ対策の実施を取り組む上で十分な予算が確保されている事業者等は、CISOを任命している割合が高く、経営層の働きかけにより、確保されていると考えられる（参考①）。
・予算の確保ができている事業者等は、情報セキュリティ対策に関する計画等が実施されている事業者等が多い傾向がある（参考②）。

情報セキュリティ対策の実施に向けた予算の確保状況（単一回答）

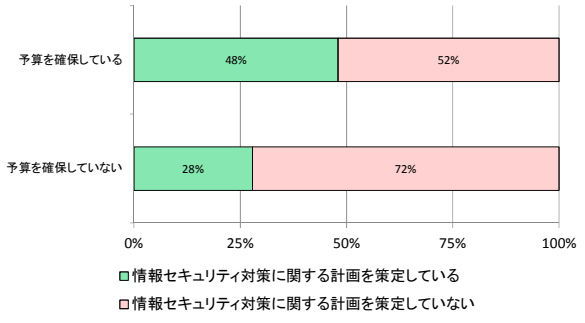


※金融は読替え可能項目なし（集計していません）

参考①　予算の確保状況とCISOの任命状況の関係性



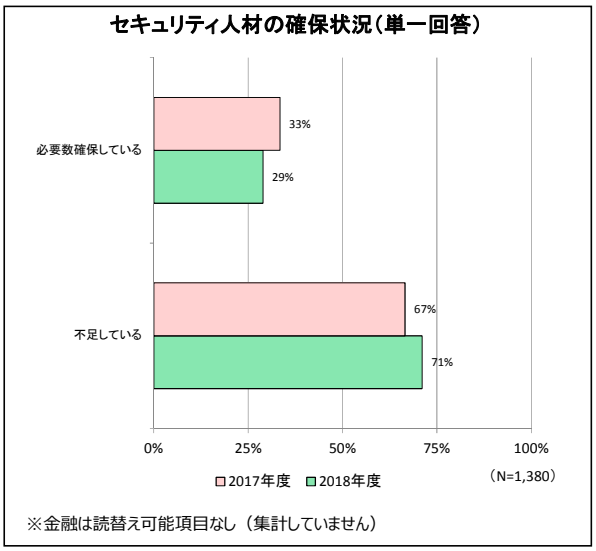
参考②　予算の確保状況と情報セキュリティ対策に関する計画状況の関係性



アンケート調査結果詳細　－　（４／５８）　－

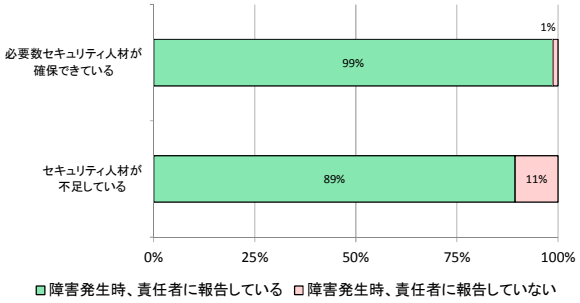
設問4　セキュリティ人材の確保状況

・セキュリティ人材が必要数確保できている事業者等は、障害発生時に経営層に報告し、情報セキュリティを経営リスクの一つとしてとらえていると考えられる（参考①）。
・セキュリティ人材が必要数確保できている事業者等は、社員に対する情報セキュリティの研修に力を入れる傾向が見られ、セキュリティ対策体制の構築が進められていると考えられる（参考②）。

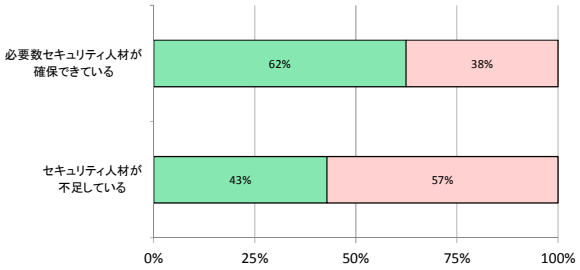


※金融は読替え可能項目なし（集計していません）

参考①　セキュリティ人材の確保状況と事業者等の責任者への報告状況の関係性



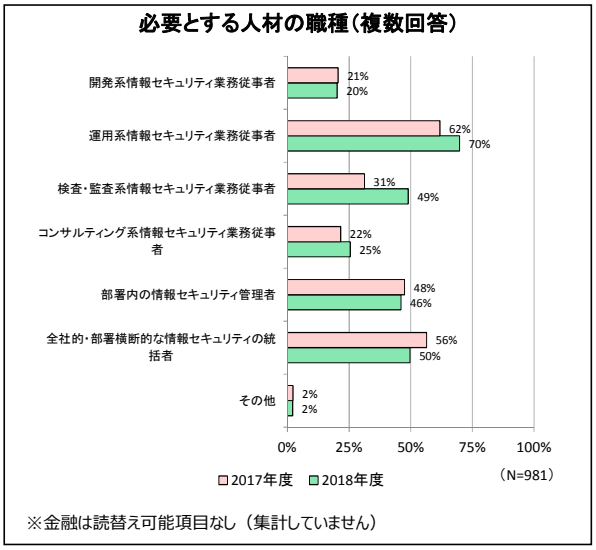
参考②　セキュリティ人材の確保状況と自社研修の実施状況の関係性



アンケート調査結果詳細　－　（５／５８）　－

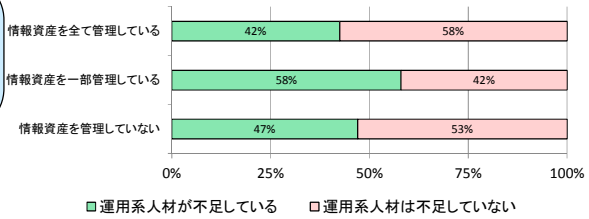
設問4-1　必要とする人材の職種

・運用系の人材が足りていない事業者等は、足りている事業者と比較して、情報資産の洗い出しを行い、台帳で管理している資産が一部にとどまっている傾向がある（参考①）。
・また、セキュリティ対策の統括者がいない事業者等は、情報資産の洗い出しができていないだけではなく、専門部署の設置や情報セキュリティ対策に関する計画、外部委託の規程ができていない傾向がある（参考②）。

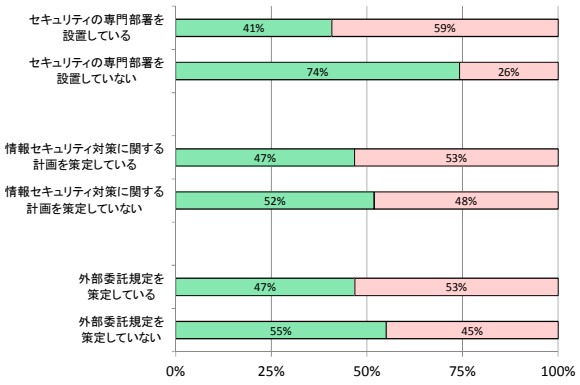


※金融は読替え可能項目なし（集計していません）

参考①　運用系人材の充足状況と情報資産管理状況の関係性



参考②　セキュリティ統括者の充足状況と各項目の関係性

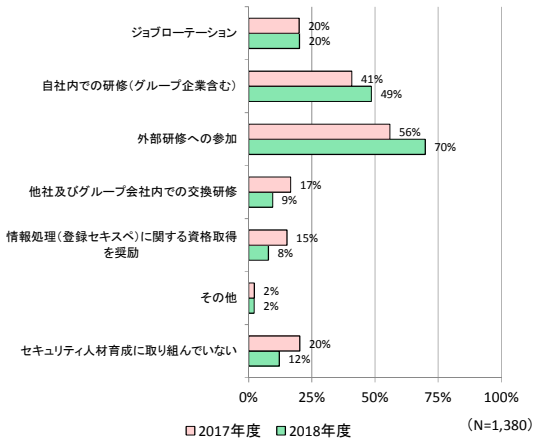


アンケート調査結果詳細　－　（６／５８）　－

設問5　セキュリティ人材育成の取組状況

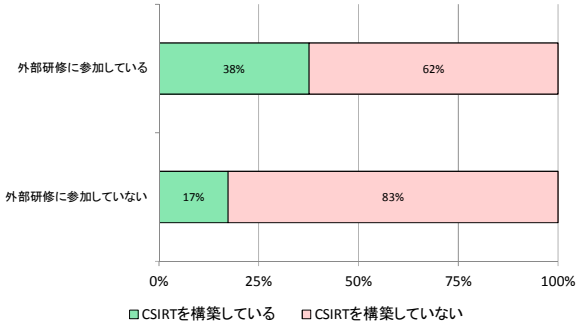
・セキュリティ人材育成のために外部研修に参加している事業者等は、社員のセキュリティ研修を実施している。また、外部研修に参加している事業者等はCSIRTの設置率が2倍を超えている（参考①）。
・セキュリティ人材を育成していない事業者等は、予算も確保されていない傾向がある（参考②）。

セキュリティ人材育成の取組状況（複数回答）

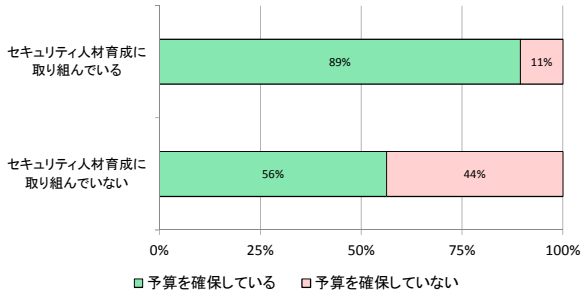


※金融は読替え可能項目なし（集計していません）

参考①　外部研修の参加状況とCSIRTの構築状況の関係性



参考②　セキュリティ人材の育成状況と予算の確保状況の関係性

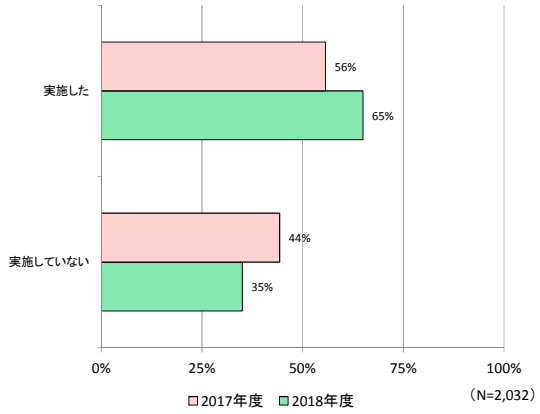


アンケート調査結果詳細　－　（７／５８）　－

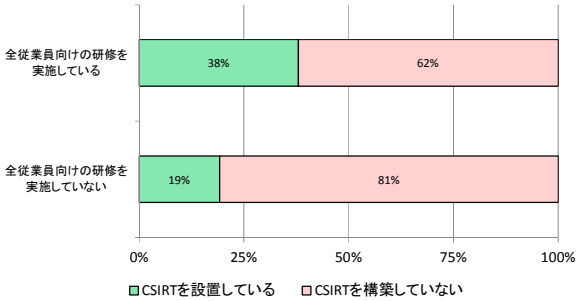
設問6　全従業員向けセキュリティ研修の実施状況

・全従業員向けのセキュリティ研修を実施している事業者等は、CSIRTの設置率が２倍である（参考①）。
・全従業員向けのセキュリティ研修を実施している事業者等は、情報セキュリティ基本方針を策定しており、セキュリティに関する規程類も策定している傾向がある（参考②）。

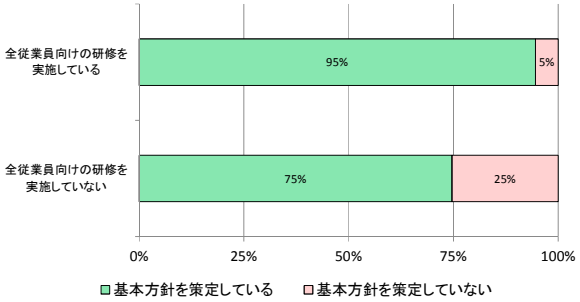
全従業員向けセキュリティ研修の実施状況（単一回答）



参考①　従業員向け研修の実施状況とCSIRTの設置状況の関係性



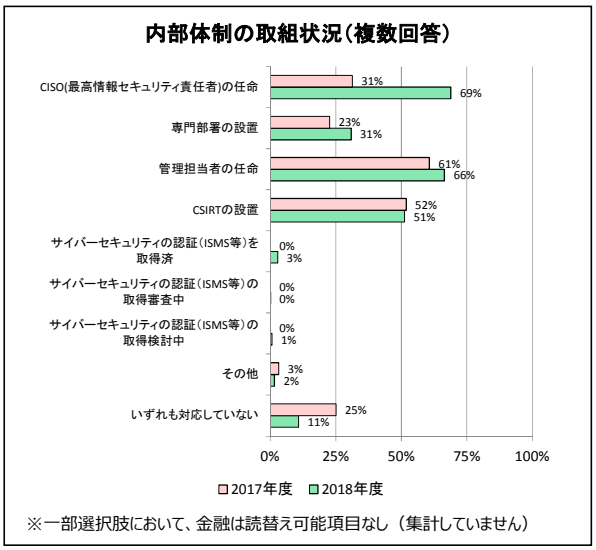
参考②　全従業員向け研修の実施状況と情報セキュリティ基本方針策定の関係性



アンケート調査結果詳細　－　（８／５８）　－

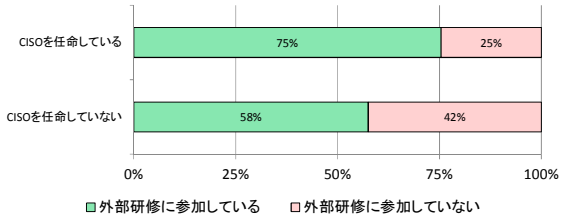
設問7　内部体制の取組状況

・CISOを任命している事業者等は、セキュリティ人材を育てるために、積極的に外部への研修に参加している。また、全従業員向けのセキュリティ研修を実施している（参考①）。
・CSIRTが設置されている事業者等は、分野横断的演習を認知している傾向がある（参考②）。
・ CISOを任命している事業者等は、CSIRTが設置されている傾向がある（参考③）。

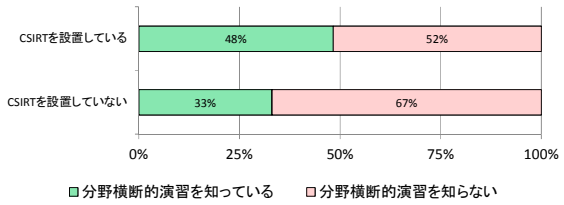


※一部選択肢において、金融は読替え可能項目なし（集計していません）

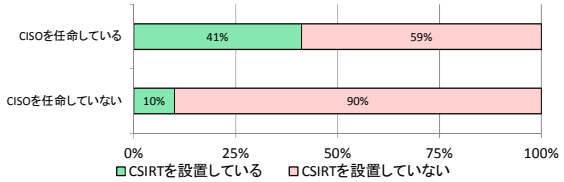
参考①　CISOの任命状況と外部研修の参加状況の関係性



参考②　CSIRTの設置状況と分野横断的演習の認知状況の関係性



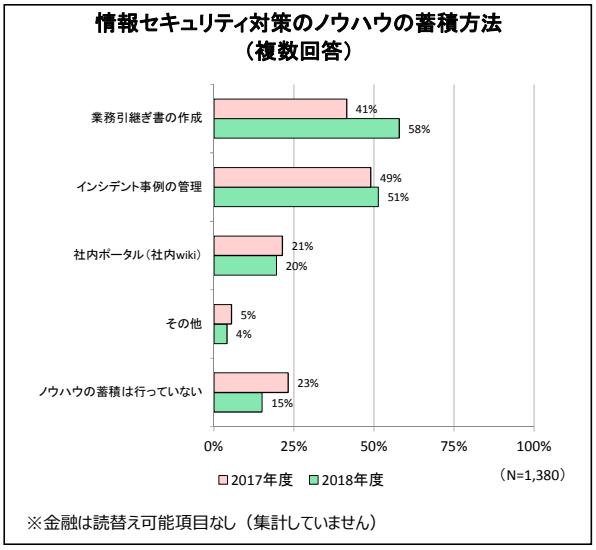
参考③　CISOの任命状況とCSIRTの設置状況の関係性



アンケート調査結果詳細　－　（９／５８）　－

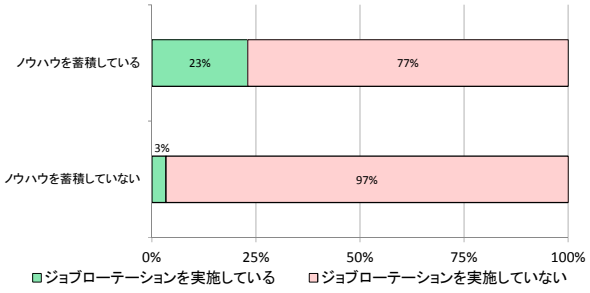
設問8　情報セキュリティ対策のノウハウの蓄積方法

・人材育成の手法として、ジョブローテーションを実施している事業者等は、ノウハウの蓄積を行っている。セキュリティ人材の育成手法として、ジョブローテーションは有効であることが確認できる（参考①）。
・ノウハウの蓄積方法としては、予算が少ない事業者等も業務引継ぎ書の作成やインシデント事例の管理で実施している（参考②）。

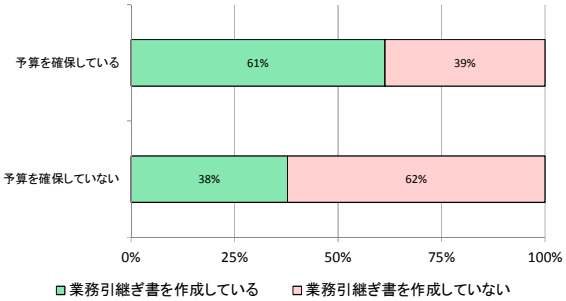


※金融は読替え可能項目なし（集計していません）

参考①　ノウハウの蓄積状況とジョブローテーションの実施状況の関係性



参考②　予算の確保状況とノウハウ蓄積方法の関係性

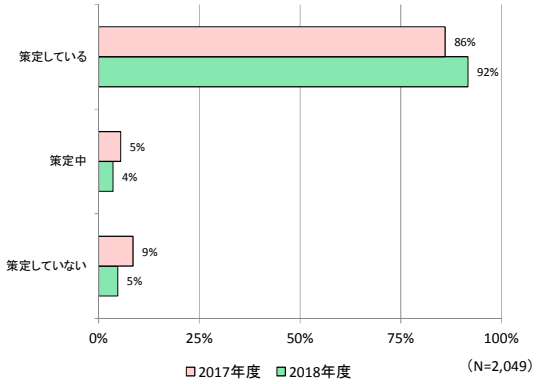


アンケート調査結果詳細　－　（１０／５８）　－

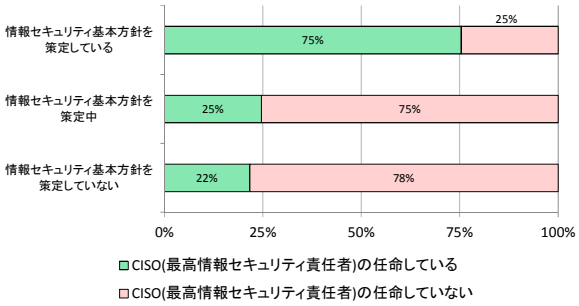
設問9　情報セキュリティ対策に関する基本方針の策定状況

・CISOが任命されている事業者等は、情報セキュリティ基本方針が策定されている（参考①）。
・情報セキュリティ基本方針が策定できていない事業者等は、内規等の策定も進んでいない傾向がある（参考②）。

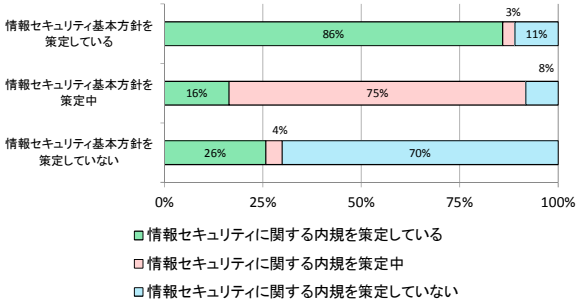
情報セキュリティ対策に関する情報セキュリティ基本方針の策定状況（単一回答）



参考①　情報セキュリティ基本方針策定状況とCISOの任命状況の関係性



参考②　情報セキュリティ基本方針の策定状況と内規の策定状況の関係性

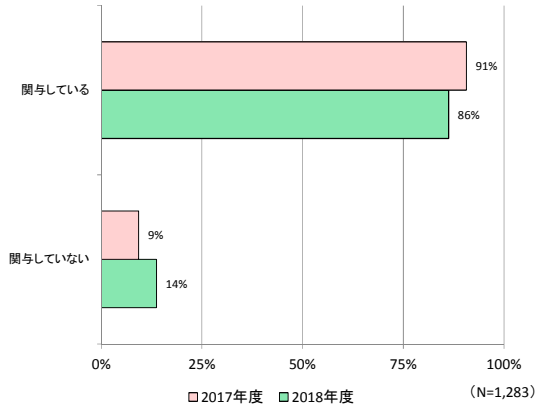


アンケート調査結果詳細　－　（１１／５８）　－

設問9-1　情報セキュリティ基本方針の策定に関する経営層の関与状況

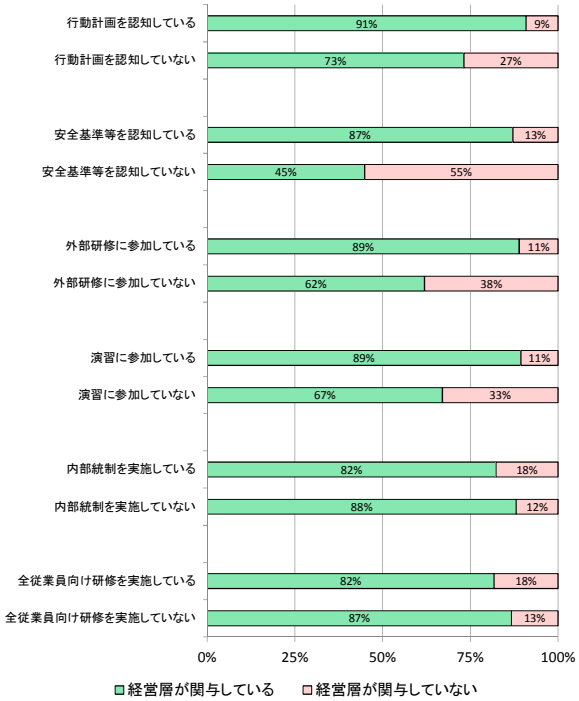
・行動計画やガイドライン等を認知し、外部への研修や演習等に参加しているような情報収集に積極的な事業者等は、経営層が関与している傾向がある（参考①）。

情報セキュリティ基本方針の策定に関する経営層の関与状況（単一回答）



※金融は読替え可能項目なし（集計していません）

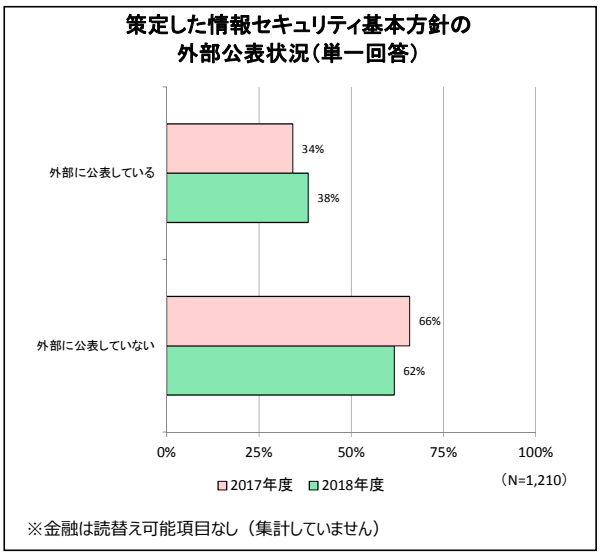
参考①　経営層の関与状況と各項目との関係性



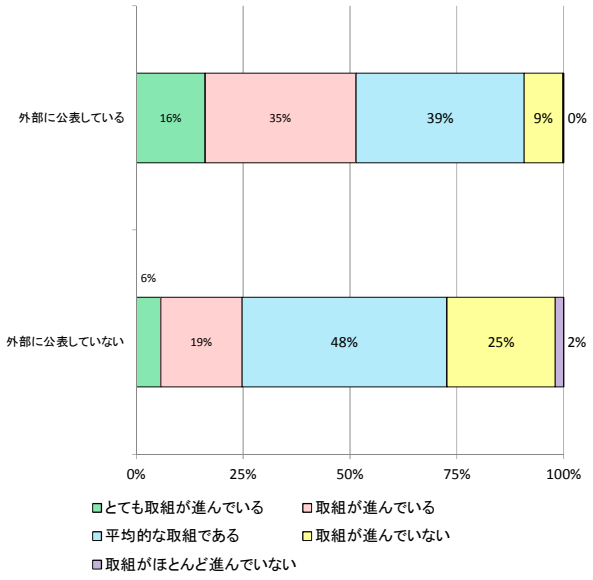
アンケート調査結果詳細　－　（１２／５８）　－

設問9-2　策定した情報セキュリティ基本方針の外部公表状況

・情報セキュリティ基本方針を外部に公表している事業者等は、外部に公表していない事業者等に比べ、情報セキュリティの取り組みが進んでいる傾向が見られる。これは、外部への見せる安全や攻撃者への抑止効果を目指しているのではないかと感じる。また、外部に公表している事業者等は、情報セキュリティを経営リスクの一つととらえ、投資家からの評価も意識していると考えられる（参考①）。



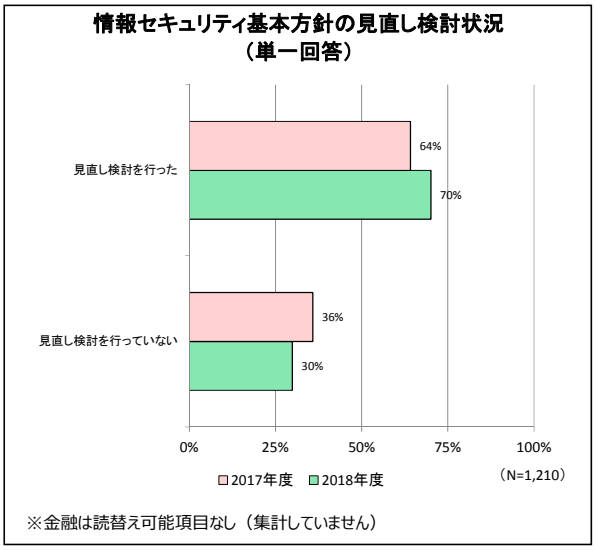
参考①　情報セキュリティ基本方針の外部公表状況と
情報セキュリティへの取組進捗状況の関係性



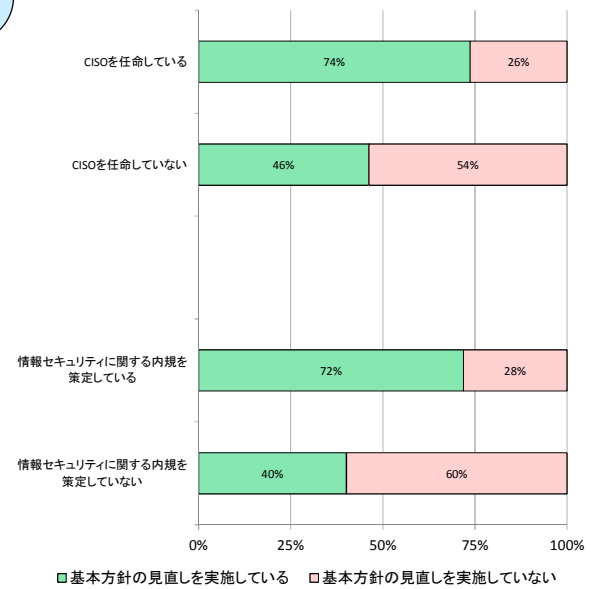
アンケート調査結果詳細　－　（１３／５８）　－

設問9-3　情報セキュリティ基本方針の見直し検討状況

・CISOを任命している事業者等は、情報セキュリティ基本方針の見直し検討を行っている傾向がある。経営層が意識をもって実施している結果であると考えられる 。情報セキュリティ基本方針の見直し検討を行っている事業者等は、情報セキュリティに関する内規や外部委託の規程の策定が実施されている傾向もある。規程を策定することから意識改革ができると考えられる（参考①）。



参考①　情報セキュリティ基本方針の見直し状況と
各項目の関係性

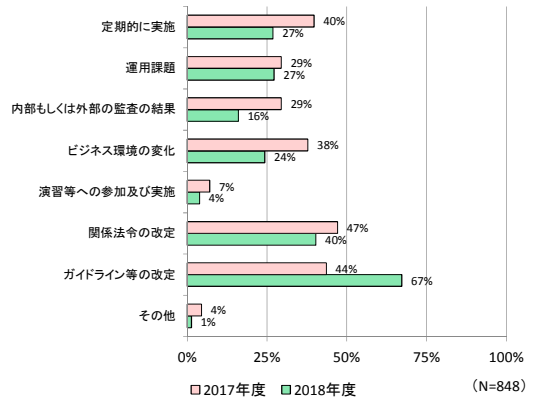


アンケート調査結果詳細　－　（１４／５８）　－

設問9-4　情報セキュリティ基本方針の見直し検討の契機

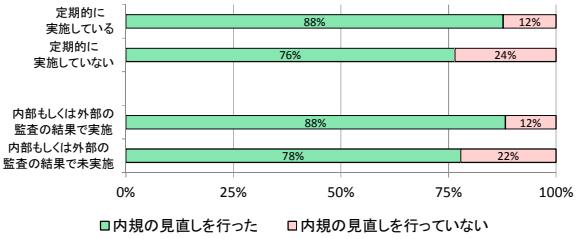
・情報セキュリティ基本方針を定期的もしくは監査の度に見直している事業者等は、基本方針だけではなく、内規の見直しも実施している傾向がある（参考①）。
・情報セキュリティ基本方針を運用課題として検討している事業者等は、インシデント事例の管理でノウハウの蓄積をしている傾向がある（参考②）。
・情報セキュリティ基本方針をビジネス環境の変化を契機にして見直している事業者等は、リスク対応要否に係る判断基準を定めている傾向がある（参考③）。

情報セキュリティ基本方針の見直し検討の契機（複数回答）

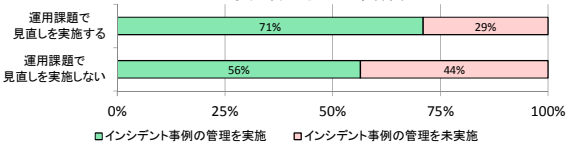


※金融は読替え可能項目なし（集計していません）

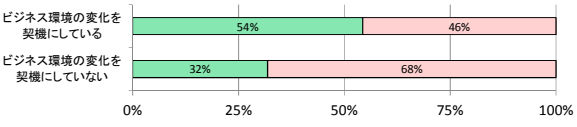
参考①　情報セキュリティ基本方針の見直し事由と内規の見直し状況の関係性



参考②　情報セキュリティ基本方針の見直し事由とインシデント事例管理状況の関係性



参考③　情報セキュリティ基本方針の見直し事由とリスク要否の判断基準の決定状況の関係性

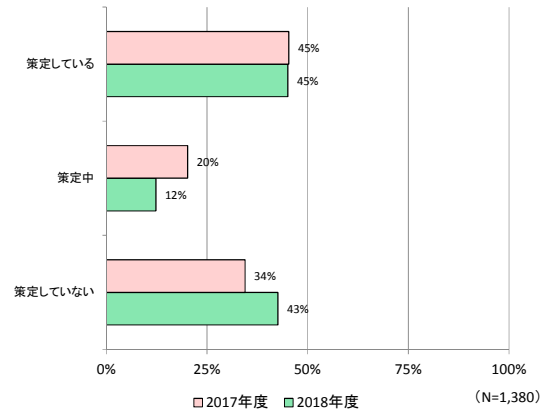


アンケート調査結果詳細　－　（１５／５８）　－

設問10　情報セキュリティ対策に関する計画策定状況

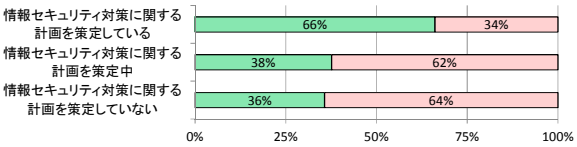
・情報セキュリティ対策に関する計画を策定している事業者等は、情報資産の格付けを実施しており、リスクの特定、対応要否の判断基準、対応優先順位づけ等を実施している傾向がある（参考①,②）。
・策定中になっている事業者等は、リスク対応に関しては未着手となっている傾向がある（参考②）。

情報セキュリティ対策に関する計画策定状況（単一回答）

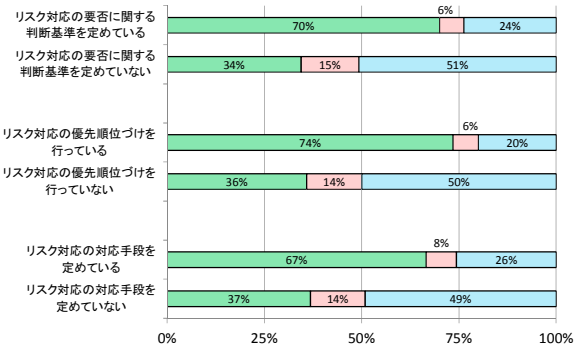


※金融は読替え可能項目なし（集計していません）

参考①　情報セキュリティ対策に関する計画策定状況と情報資産の格付け状況の関係性



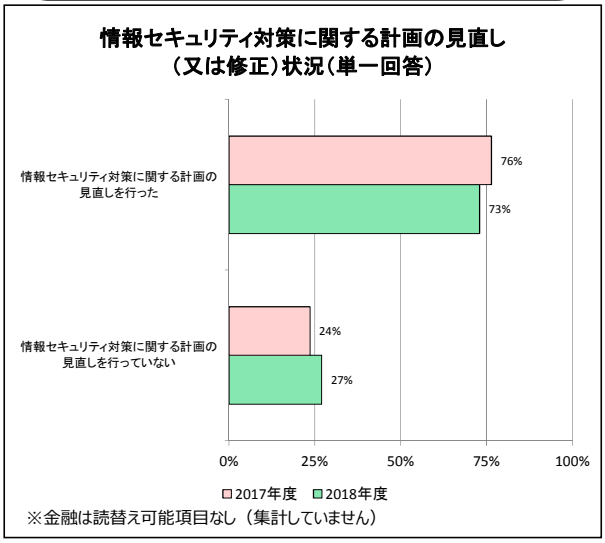
参考②　情報セキュリティ対策に関する計画策定状況と各項目の関係性



アンケート調査結果詳細　－　（１６／５８）　－

設問10-1　情報セキュリティ対策に関する計画の見直し（又は修正）状況

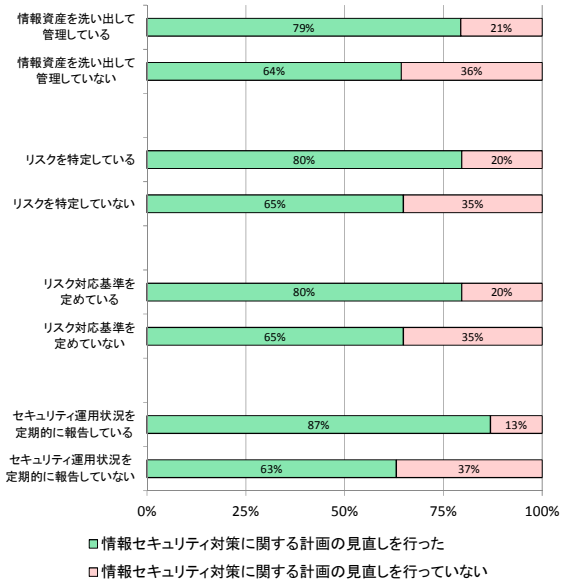
・情報セキュリティ対策に関する計画の見直しを行った事業者等は、情報資産の洗い出しやリスク特定、リスク対応基準の策定だけではなく、運用面において、セキュリティ対策状況を定期的に責任者と共有している傾向がある（参考①）。
・事業者等の内部で情報セキュリティ対策の計画を定め、計画に則り、PDCAを回せる事業者等は、多くの項目で良好な傾向がある。



情報セキュリティ対策に関する計画の見直し（又は修正）状況（単一回答）

※金融は読替え可能項目なし（集計していません）

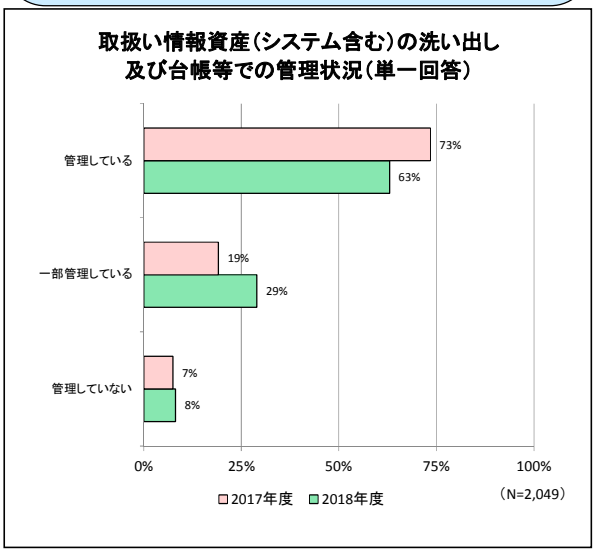
参考①　情報セキュリティ対策に関する計画の見直し状況と各種実施状況の関係性



アンケート調査結果詳細　－　（１７／５８）　－

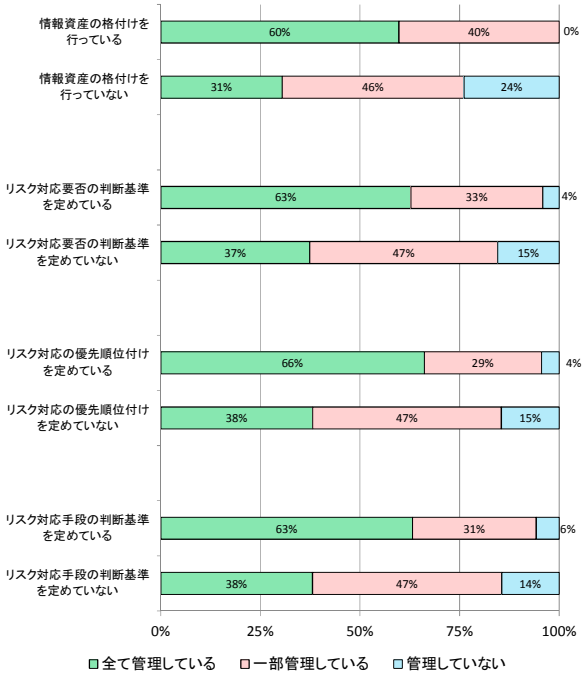
設問11　取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況

・取扱い情報資産の管理をしている事業者等は、情報資産の格付けまで実施している傾向やリスクの判断基準等が定められている傾向がある（参考①）。
・情報資産と重要度に応じた格付けを定めると共に、障害発生時に正しい判断や行動ができるように、リスク判断基準も明確になっており、管理と運用の両面で必要事項が定められている傾向がある。



取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況（単一回答）

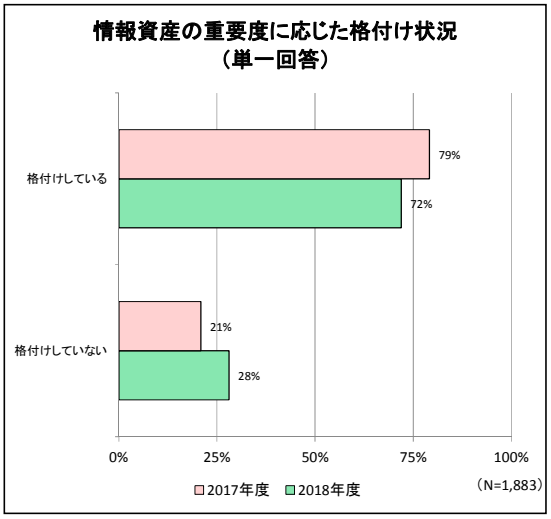
参考①　情報資産の管理状況と各項目の関係性



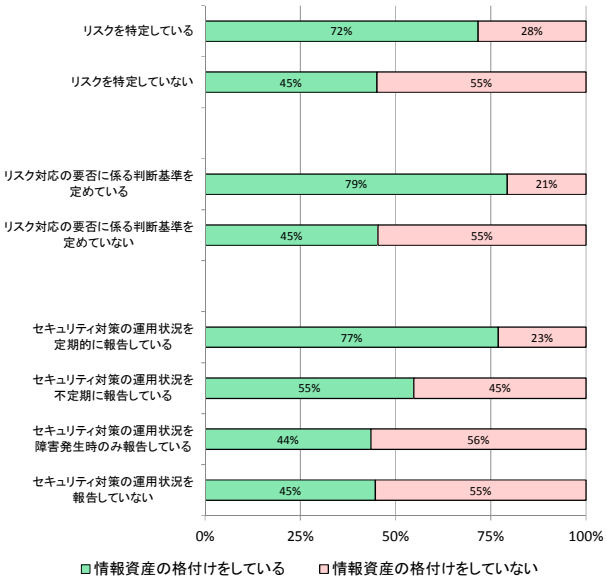
アンケート調査結果詳細　－　（１８/５８）　－

設問11-1　情報資産の重要度に応じた格付け状況

・情報資産の重要度に応じた格付けを実施している事業者等は、リスク特定、リスク対応基準等を定めている傾向がある。また、情報セキュリティに関する運用状況を定期的に報告している事業者等は、情報資産の重要度に応じた格付けもできている（参考①）。



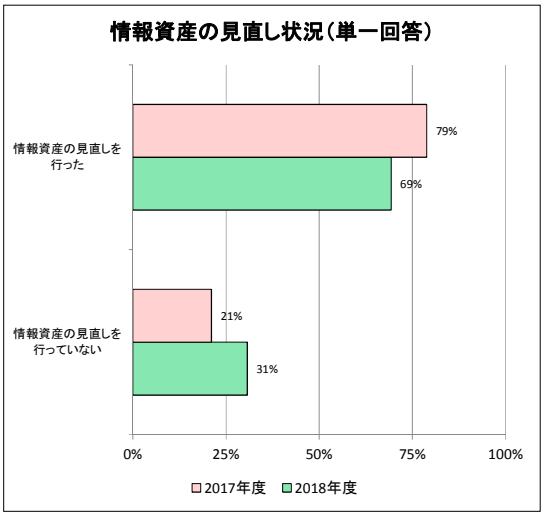
参考①　情報資産の格付け状況と各項目の関係性



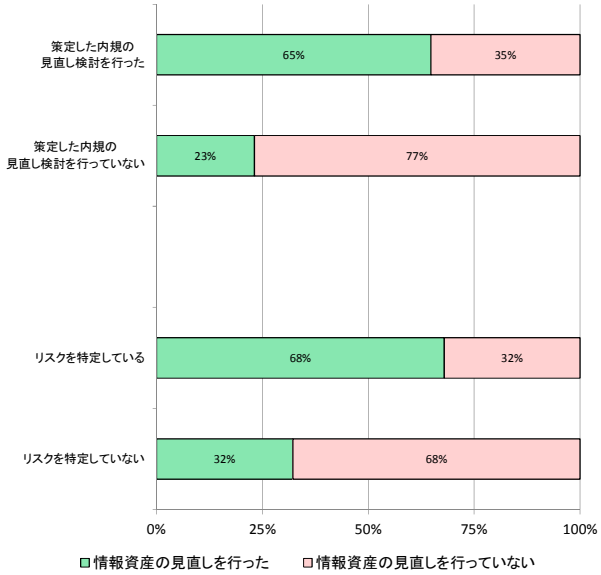
アンケート調査結果詳細　－　（１９/５８）　－

設問11-2　情報資産の見直し状況

・情報資産の見直しを行っている事業者等は、内規等の見直しを実施し、リスクの特定も実施している傾向がある（参考①）。内規等の見直しを契機に情報資産とリスクを適正に管理していることが推察できる。



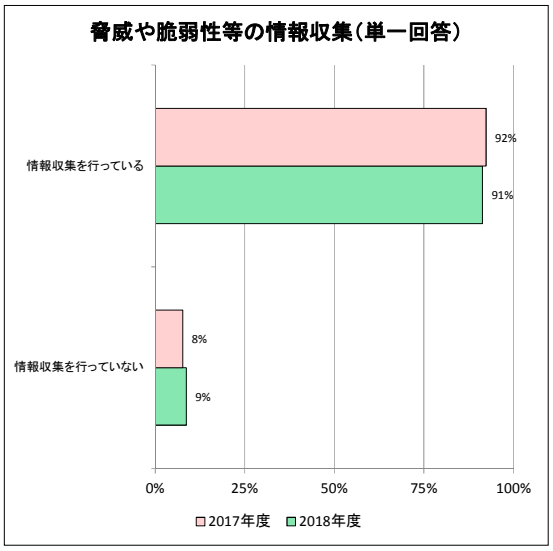
参考①　情報資産の見直し状況と各項目の関係性



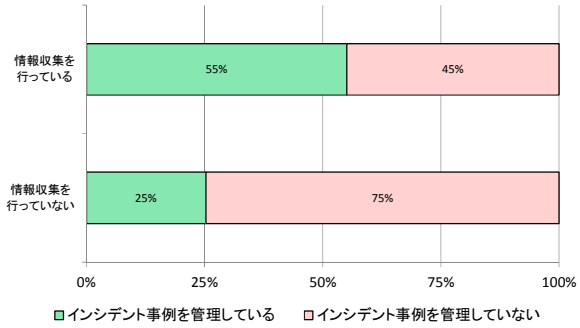
アンケート調査結果詳細　－　（２０/５８）　－

設問12　脅威や脆弱性等の情報収集

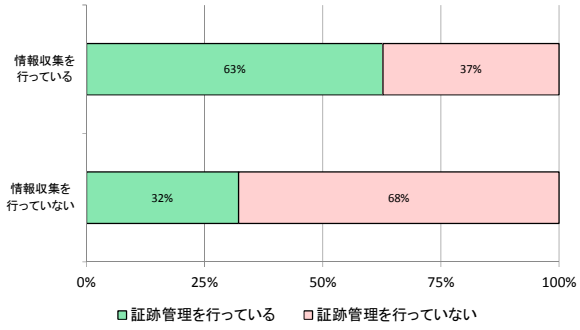
・情報収集を行っている事業者等は、自社内のインシデント管理を実施している傾向があり、セキュリティ対策としても証跡管理を行っていることが多い（参考①、参考②）。セキュリティ情報の収集を行っている事業者等は、収集したセキュリティ情報をもとに対策まで実施していると推察できる。



参考①　情報収集とインシデント事例管理状況の関係性



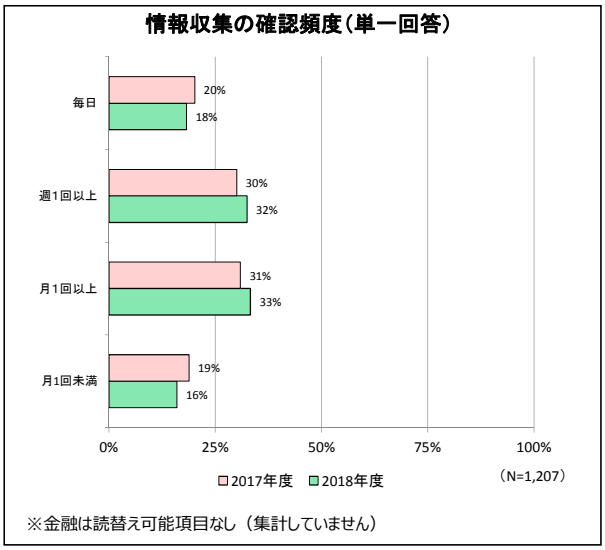
参考②　情報収集と証跡管理の関係性



アンケート調査結果詳細　－　（２１/５８）　－

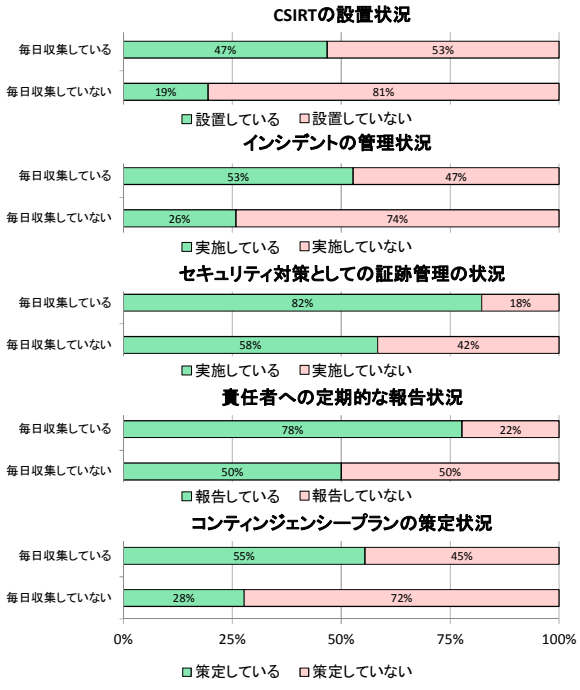
設問12-1　情報収集の確認頻度

・情報収集を毎日行っている事業者等は、CSIRTの設置、インシデント管理、証跡管理、責任者との情報連携、コンティンジェンシープラン（CP）の策定等、様々な取り組みが進んでいる傾向がある（参考①）。
・政府の動向やインシデント情報を収集し、事業者等のセキュリティ対策を実施していると推察できる。



※金融は読替え可能項目なし（集計していません）

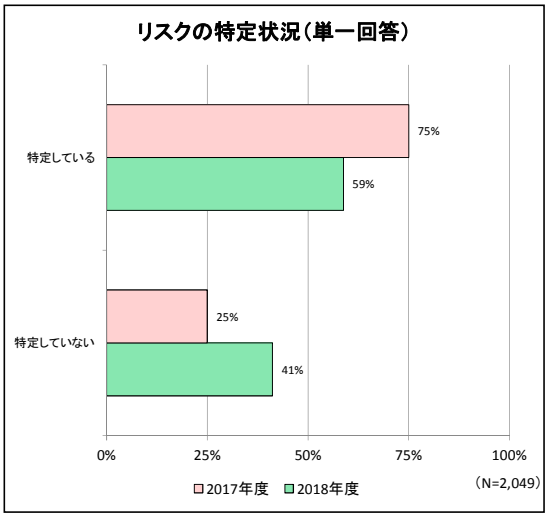
参考①　情報収集の頻度と各項目の関係性



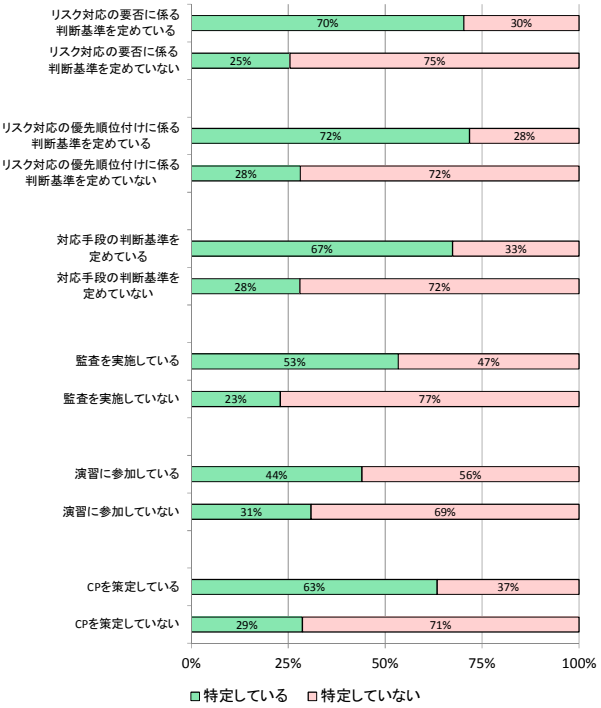
アンケート調査結果詳細　－　（２２/５８）　－

設問13　リスクの特定状況

・リスクの特定を行っている事業者等は、リスク対応要否の判断基準やリスク対応の優先順位づけ、リスク対応手段の判断基準等を策定していることから有事の際の対応を想定し、リスクの特定を行っている（参考①）。
・リスクの特定を行っている事業者等は、監査の実施や演習の参加割合が高いため、改善活動を進める上でリスクを特定することは、優先事項として取り組んでいると推察できる。



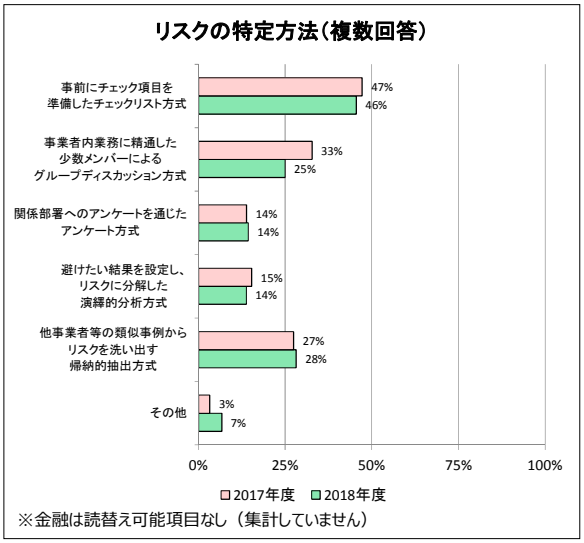
参考①　リスクの特定状況と各項目の関係性



アンケート調査結果詳細　－　（２３/５８）　－

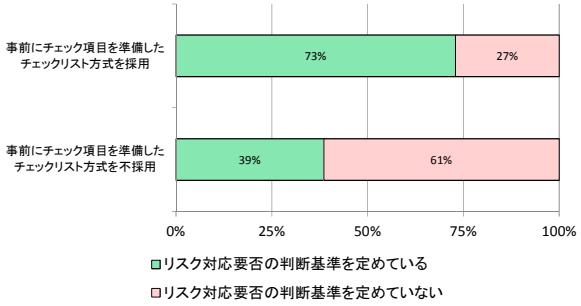
設問13-1　リスクの特定方法

・リスクの特定方法としてチェック項目の方式を用いる場合は、リスク対応要否の判断基準が定められている傾向があるため、リスク対応を強化したい場合は、チェックリスト方式を採用することが推奨される（参考①）。
・リスクの特定方法として、他事業者等の類似事例からの帰納的抽出方式を用いた場合は、セプター事務局からの情報をしっかりと受け取っている傾向があるため、情報共有を強化したい場合は、演繹的分析方式を採用することが推奨される（参考②）。

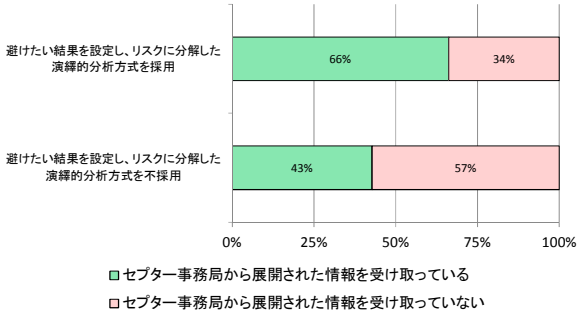


※金融は読替え可能項目なし（集計していません）

参考①　リスクの特定方法と
リスク対応要否の判断基準の関係性



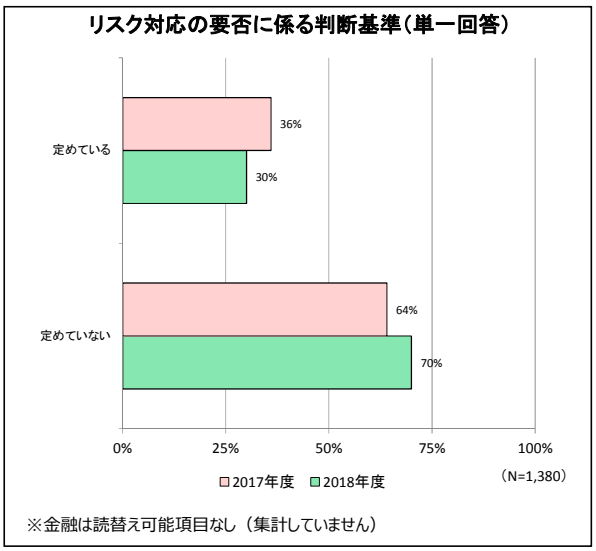
参考②　リスクの特定方法と情報共有の関係性



アンケート調査結果詳細　－　（２４／５８）　－

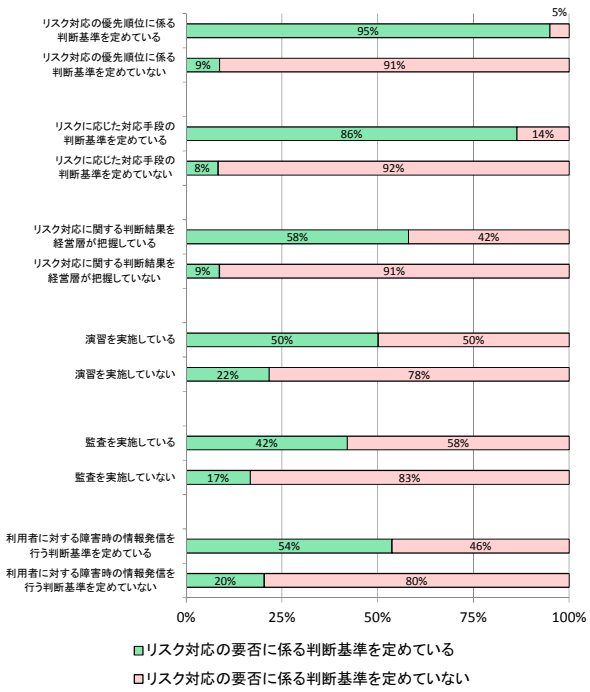
設問14　リスク対応の要否に係る判断基準

・リスク対応の要否に係る判断基準が決定している事業者等は、多くの項目において良好な傾向が見られた。特に、リスク対応の要否だけではなく、優先順位に係る判断基準も定められ、対応手順に至るまで決定している傾向がある。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。



※金融は読替え可能項目なし（集計していません）

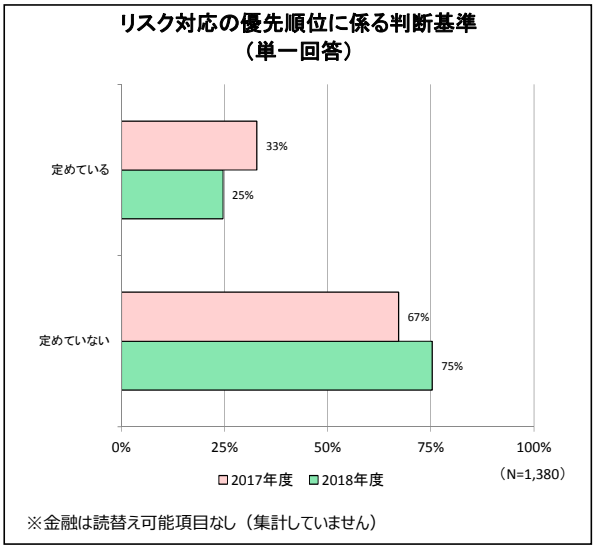
参考①　リスク対応の要否に係る判断基準の決定状況と各項目の関係性



アンケート調査結果詳細　－　（２５／５８）　－

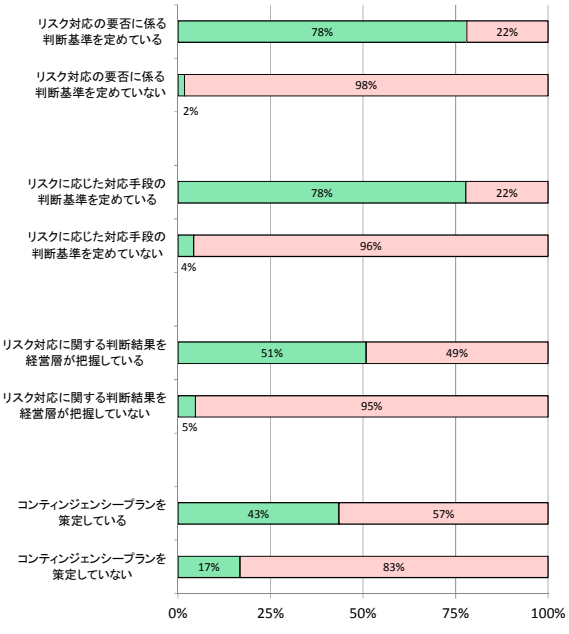
設問15　リスク対応の優先順位に係る判断基準

・リスク対応の優先順位が決定している事業者等は、多くの項目において良好な傾向が見られた。特に、対応手順に至るまで決定している傾向がある。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。



※金融は読替え可能項目なし（集計していません）

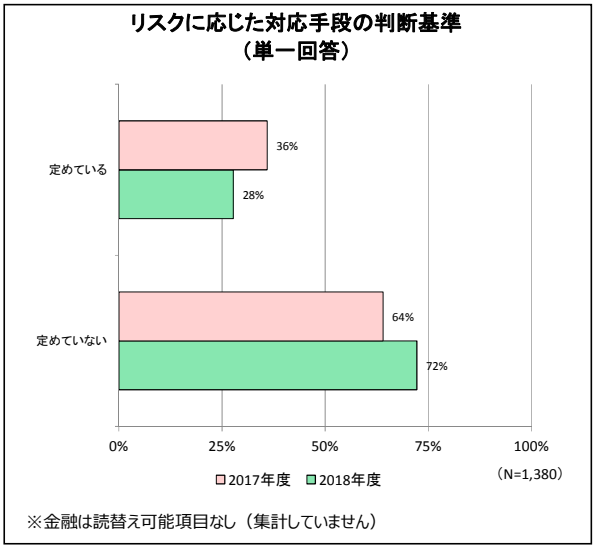
参考①　リスク対応の優先順位に係る判断基準の決定状況と各項目の関係性



アンケート調査結果詳細　－　（２６/５８）　－

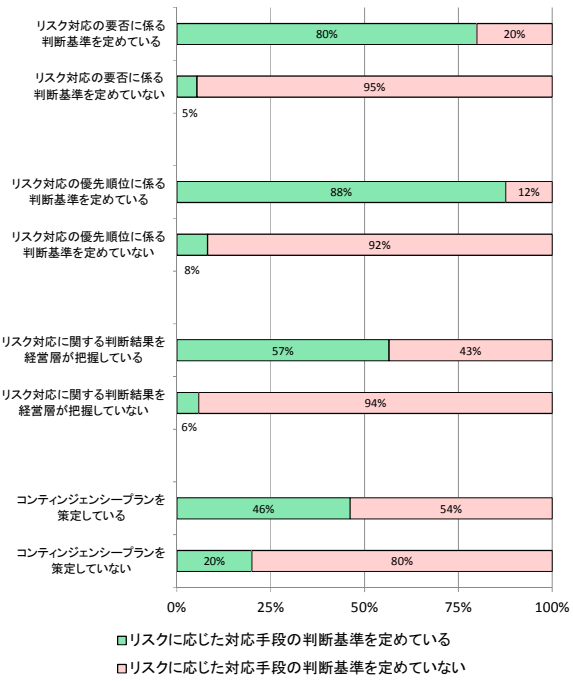
設問16　リスクに応じた対応手段の判断基準

・リスクに応じた対応手順の判断基準が決定している事業者等は、多くの項目において良好な傾向が見られた。さらに、経営層の積極的な関わりも確認できることから、演習や監査の機会を通じて、情報セキュリティ体制の改善活動がされていると推察できる（参考①）。



※金融は読替え可能項目なし（集計していません）

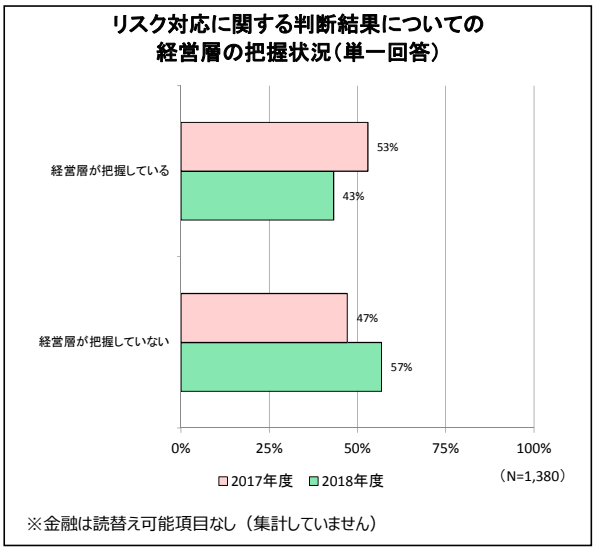
参考①　リスクに応じた対応手段の判断基準の決定状況と各項目の関係性



アンケート調査結果詳細　－　（２７/５８）　－

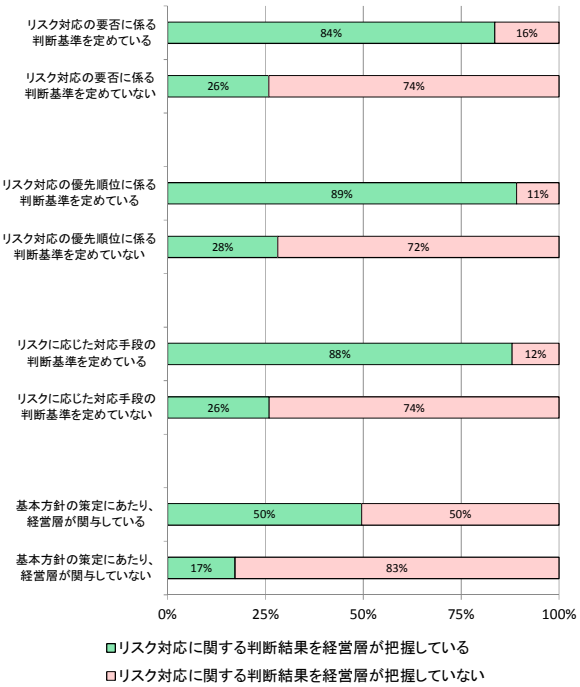
設問17　リスク対応に関する判断結果についての経営層の把握状況

・リスク対応に関する判断結果を経営層が把握していない事業者等は、演習を実施しておらず、監査も実施していない傾向がある。また、障害発生時に利用者に対して情報発信を行う判断基準も策定されていない。さらに、経営層が把握している事業者等は、情報セキュリティ基本方針にも関与している傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

参考①　リスク対応の判断結果の経営層の認知状況と各項目の関係性

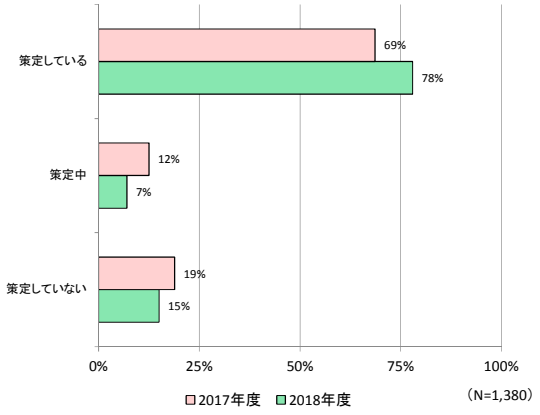


アンケート調査結果詳細　－　（２８／５８）　－

設問18　情報セキュリティに関する内規の策定状況

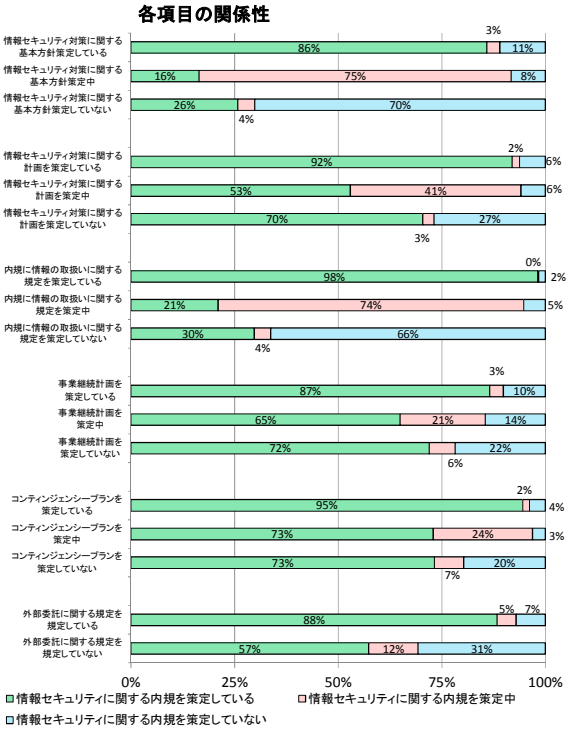
・情報セキュリティに関する内規まで策定している事業者等は、規定類が策定されている傾向がある（参考①）。ただし、事業継続計画（BCP）やコンティンジェンシープラン（CP）は、それほど大きな差は見られないことから、これらの策定については、規定類の整備とは異なるアプローチでの啓発活動が必要であると推察できる。

情報セキュリティに関する内規の策定状況（単一回答）



※金融は読替え可能項目なし（集計していません）

参考①　情報セキュリティに関する内規の策定状況と各項目の関係性

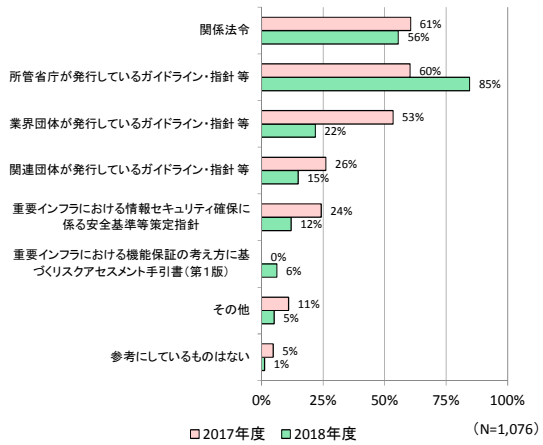


アンケート調査結果詳細　－　（２９／５８）　－

設問18-1　内規等を策定する際の参考文献

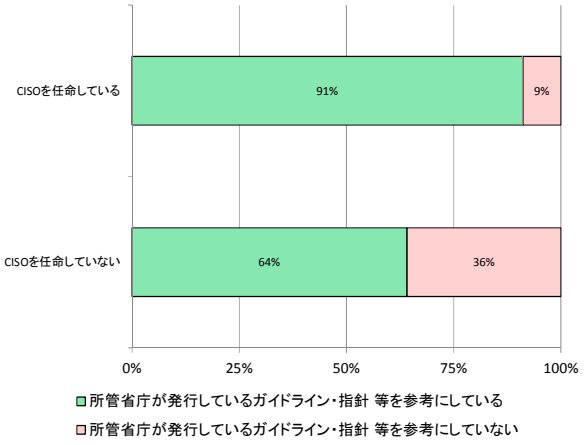
・内規等を策定する際の参考文献として、所管省庁が発行しているガイドライン・指針等を参考にしている事業者等は、CISOを任命している傾向がある。政府が指針等で、CISOの任命を求めていることが反映されているためであると考えられる（参考①）。

内規等を策定する際の参考文献（複数回答）



※金融は読替え可能項目なし（集計していません）
※リスクアセスメント手引書は、2018年度から調査開始

参考①　CISOの任命状況と内規等を策定する際の参考文献の関係性

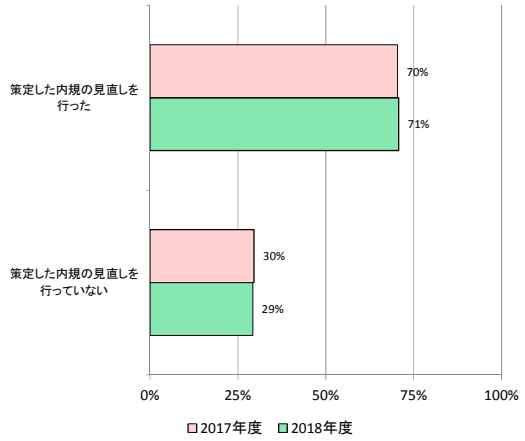


アンケート調査結果詳細　－　（３０/５８）　－

設問18-2　策定した内規の見直し検討状況

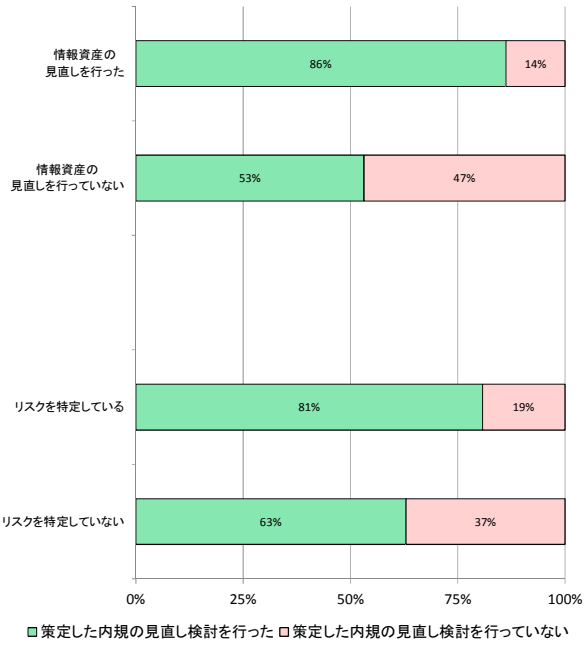
・策定した内規等の見直しを実施している事業者等は、情報資産の見直しも実施している傾向がある。また、リスクの特定も実施している傾向がある（参考①）。
・そのため、内規等の見直しに合わせて、情報資産の見直しがされる仕組みが循環していることが推察される。

策定した内規の見直し検討状況（単一回答）



※金融は読替え可能項目なし（集計していません）

参考①　策定した内規の見直し検討状況と各項目の関係性

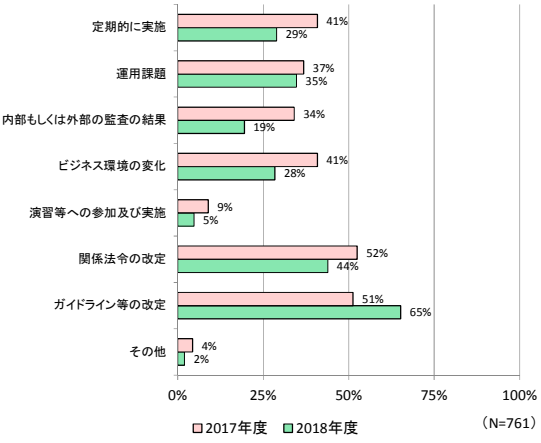


アンケート調査結果詳細　－　（３１/５８）　－

設問18-3　内規の見直し検討の契機

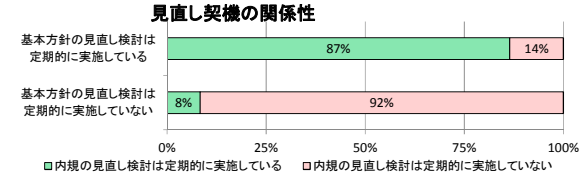
・内規の見直し検討の契機と情報セキュリティ基本方針の見直しの契機は、同じく定期的に見直し検討を行っていることが確認できる（参考①）。
・定期的もしくは運用課題を見つけて自発的に見直し検討を行っている事業者等よりも、ガイドラインや関係法令の改定といった外的要因により、見直しをしている割合が多い傾向がある。

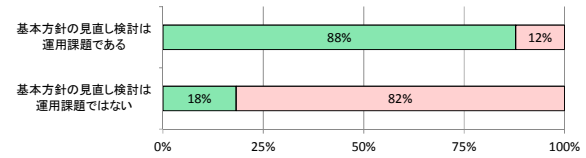
内規の見直し検討の契機（複数回答）

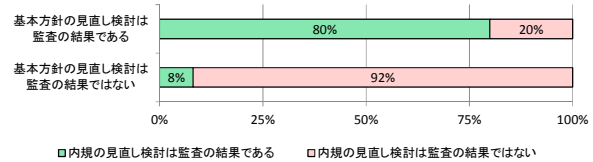


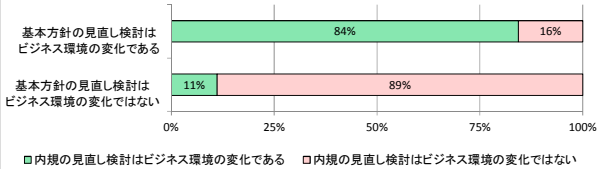
※金融は読替え可能項目なし（集計していません）

参考①　内規の見直し検討の契機と基本方針の見直し契機の関係性





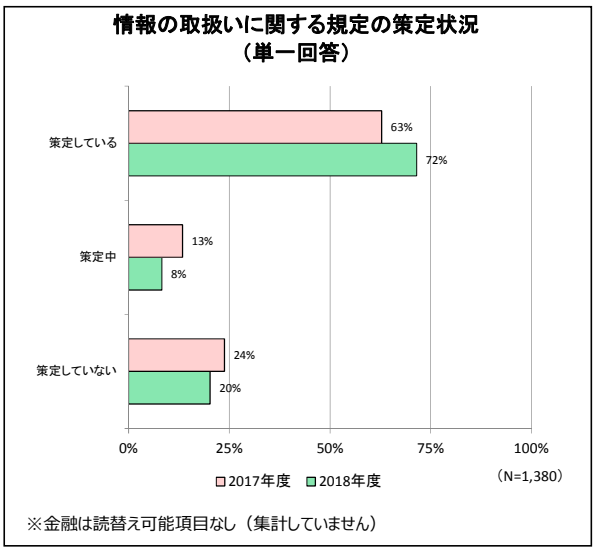




アンケート調査結果詳細　－　（３２／５８）　－

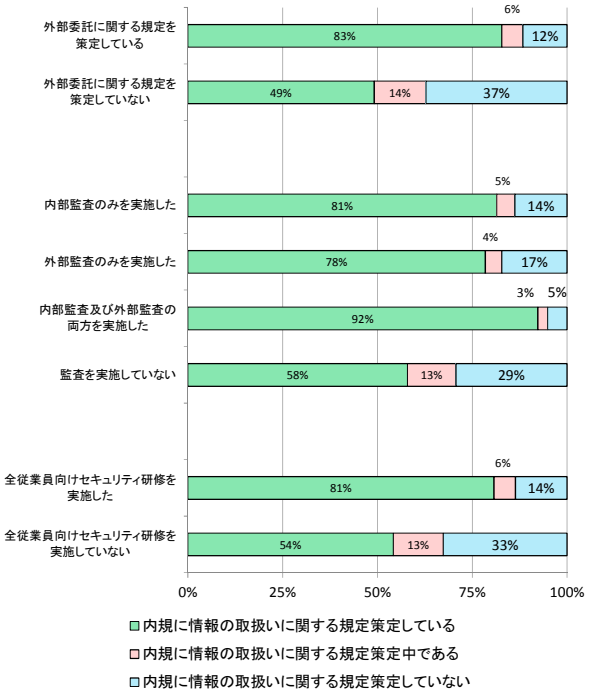
設問19　情報の取扱いに関する規定の策定状況

・情報の取扱いに関する規程を策定している事業者等は、外部委託に関する規程を策定している傾向がある。また、策定中の事業者等は、監査や従業員向けのセキュリティ研修（演習等）を実施していない傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

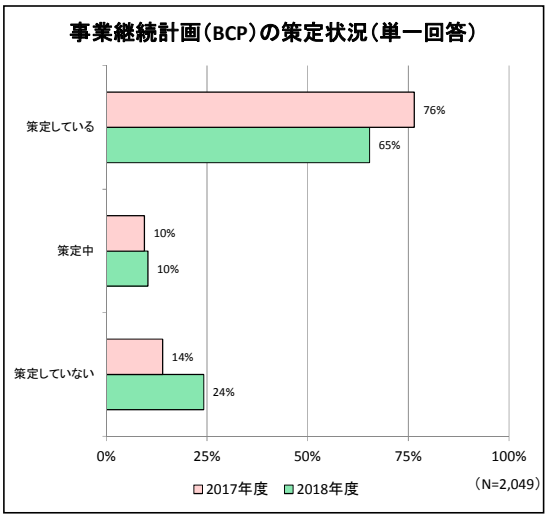
参考①　情報の取扱いに関する規定策定状況と各項目の関係性



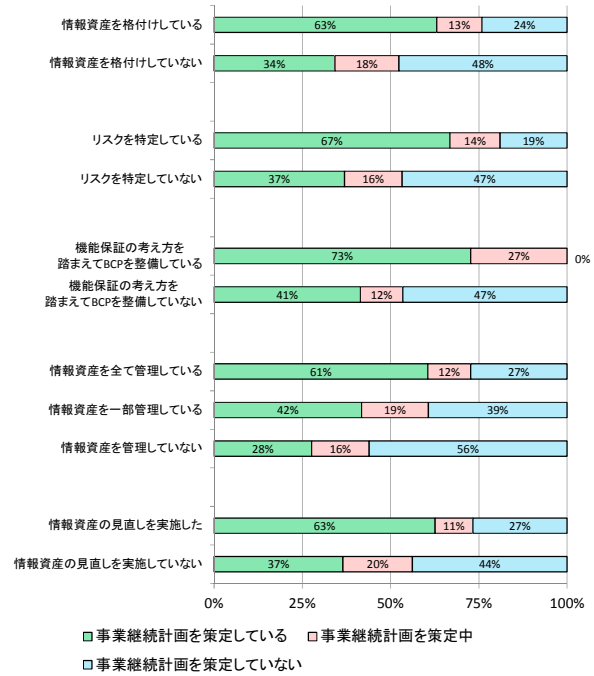
アンケート調査結果詳細　－　（３３／５８）　－

設問20　事業継続計画（BCP）の策定状況

・策定している事業者等は、情報資産の格付けやリスクの特定を実施している傾向がある。また、機能保証の考え方を踏まえて策定されている傾向がある（参考①）。



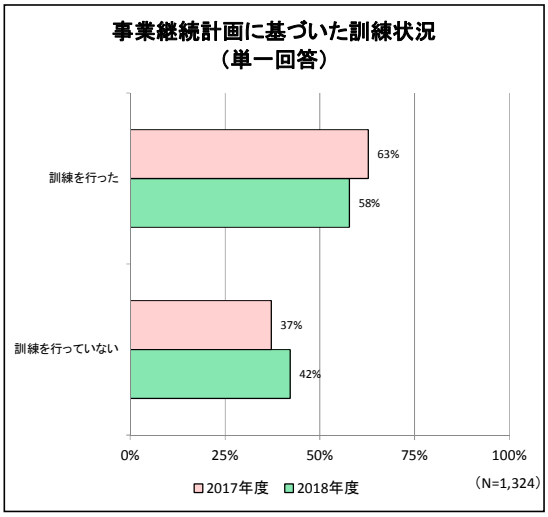
参考①　事業継続計画（BCP）の策定状況と各項目の関係性



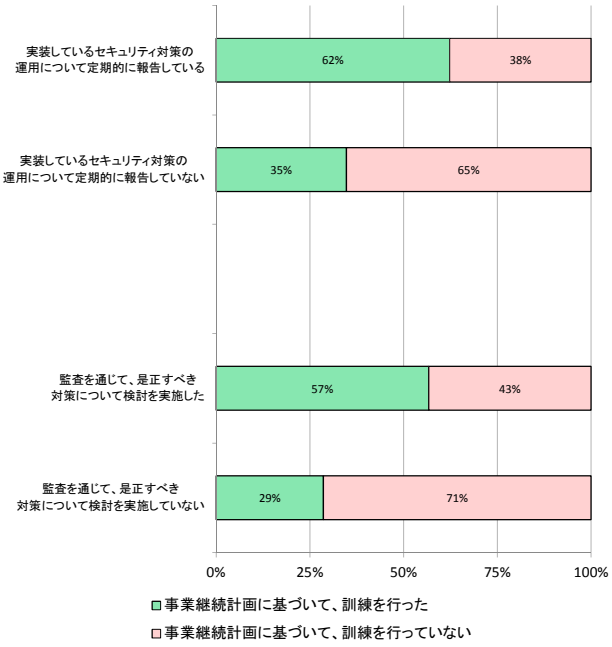
アンケート調査結果詳細　－　（３４／５８）　－

設問20-1　事業継続計画（BCP）に基づいた訓練状況

・訓練を行った事業者等は、運用状況を責任者に定期的に報告している傾向がある。また、監査を通じて是正すべき対策について検討している傾向がある（参考①）。



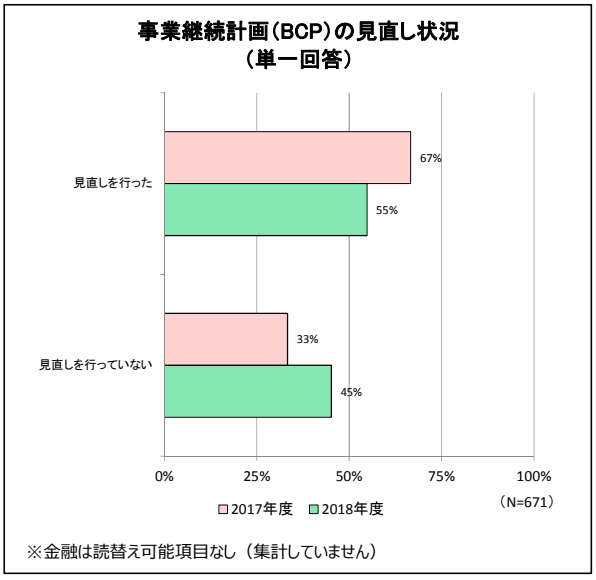
参考①　事業継続計画（BCP）に基づいた訓練状況と各項目の関係性



アンケート調査結果詳細　－　（３５／５８）　－

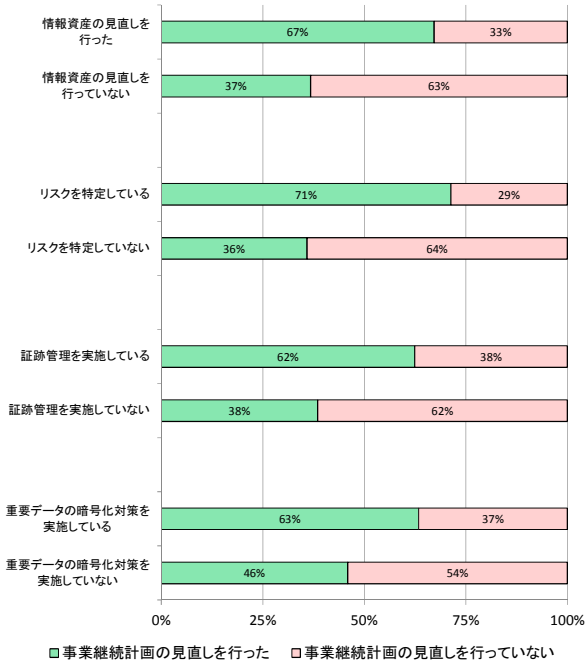
設問20-2　事業継続計画（BCP）の見直し状況

・事業継続計画（BCP）の見直しを行った事業者等は、情報資産の見直しを行っており、リスクの特定を実施している傾向がある。また、セキュリティ対策として、証跡管理や重要データの暗号化等の取組みがされている（参考①）。



※金融は読替え可能項目なし（集計していません）

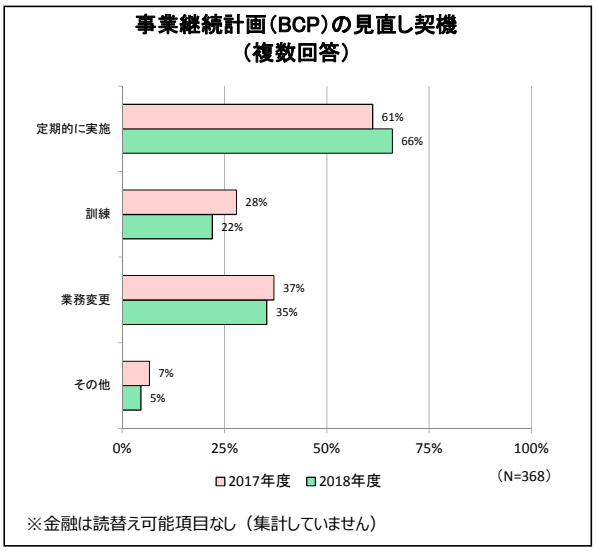
参考①　事業継続計画（BCP）の見直し状況と各項目の関係



アンケート調査結果詳細　－　（３６／５８）　－

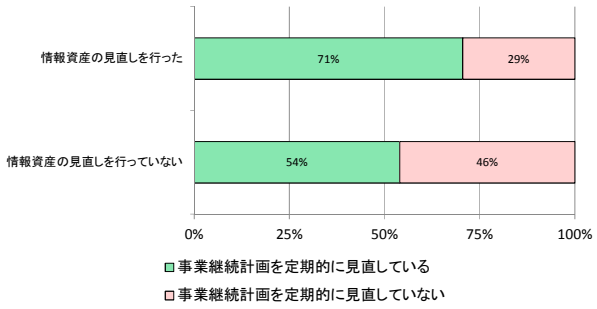
設問20-3　事業継続計画（BCP）の見直し契機

・定期的に事業継続計画（BCP）を見直しを実施している事業者等は、情報資産の見直しやリスクの特定を実施している傾向がある（参考①）。
・訓練を契機に事業継続計画（BCP）を見直している事業者等は、経営層にリスクアセスメントの結果を報告している傾向がある（参考②）。

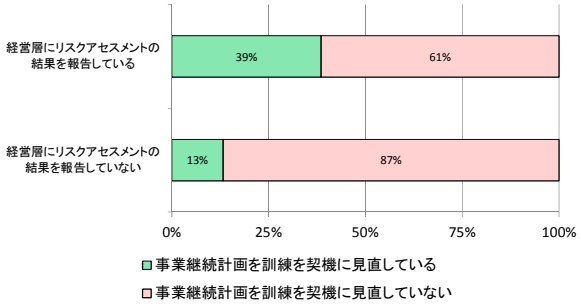


※金融は読替え可能項目なし（集計していません）

参考①　事業継続計画（BCP）の定期見直しと情報資産の見直しの関係



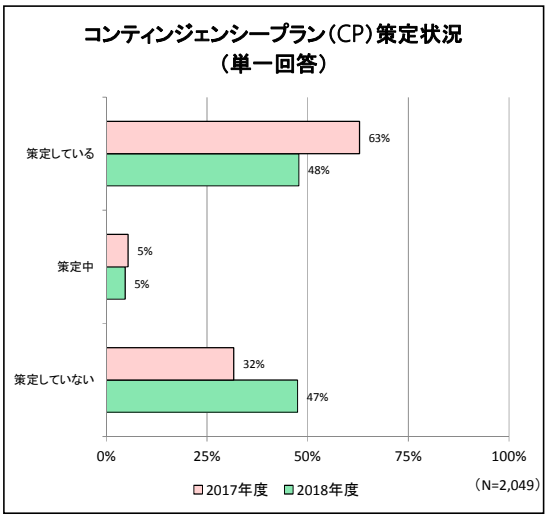
参考②　事業継続計画（BCP）の訓練ごとの見直しと経営層への報告の関係性



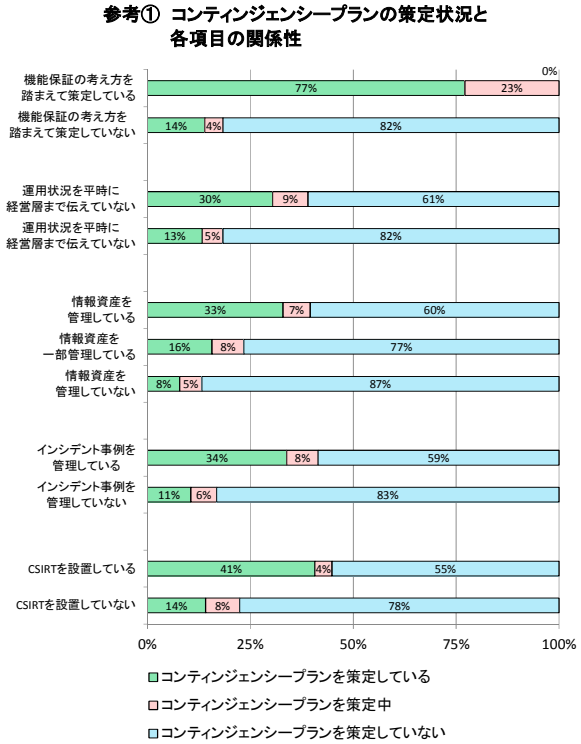
アンケート調査結果詳細　－　（３７／５８）　－

設問21　コンティンジェンシープラン（CP）策定状況

・コンティンジェンシープラン（CP）を策定している事業者等は、機能保証の考え方を踏まえた上で策定されている事業者等が多い。さらに、経営層まで状況報告されている事業者等も多い。また、コンティンジェンシープラン（CP）を策定している事業者等は、情報資産・インシデントを管理し、CSIRTが設置されている傾向がある（参考①）。



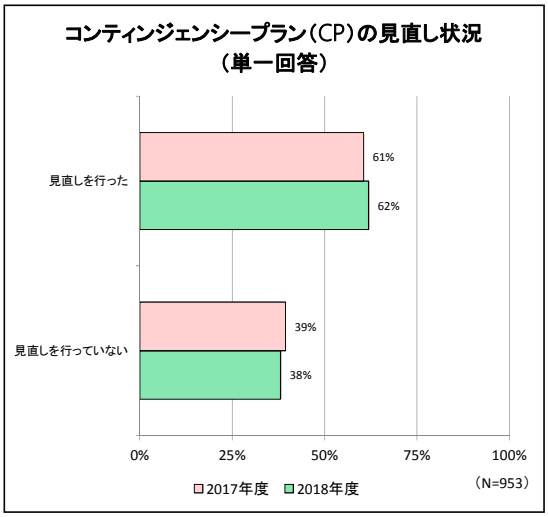
参考①　コンティンジェンシープランの策定状況と各項目の関係性



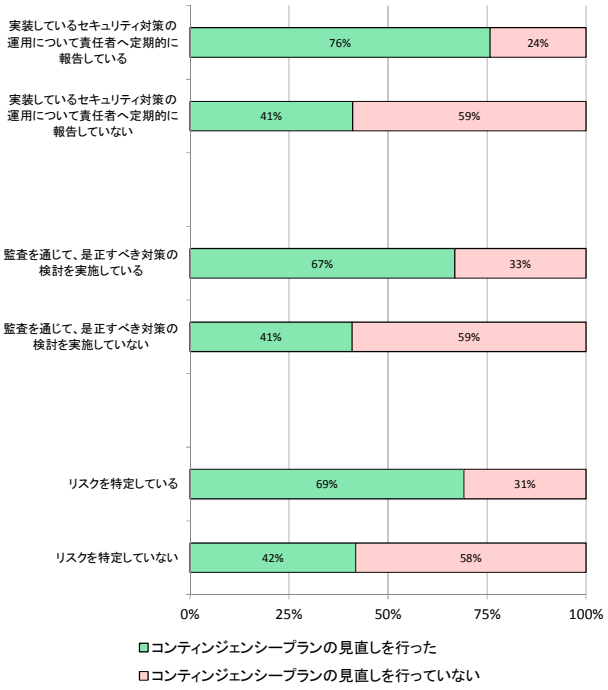
アンケート調査結果詳細　－　（３８／５８）　－

設問21-1　コンティンジェンシープラン（CP）の見直し状況

・コンティンジェンシープラン（CP）の見直しを行っている事業者等は、責任者に定期的に報告を行い、監査を通じて是正すべき対策を検討している傾向がある。また、コンティンジェンシープラン（CP）の見直すべき項目を検討するために、リスクの特定を実施していることが多い（参考①）。



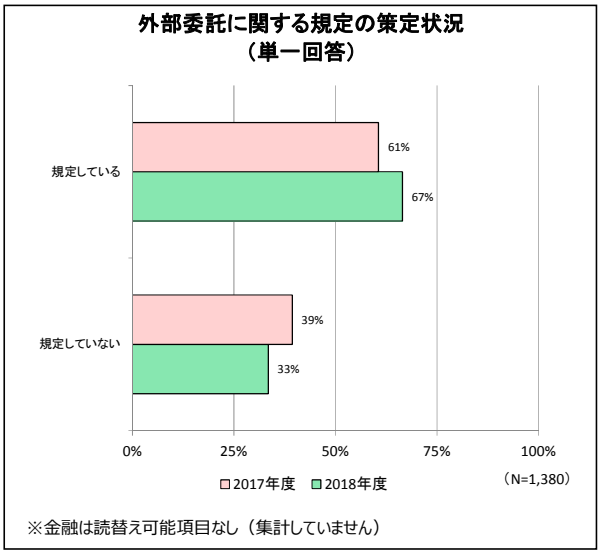
参考①　コンティンジェンシープラン（CP）の見直し状況と各項目の関係性



アンケート調査結果詳細　－　（３９／５８）　－

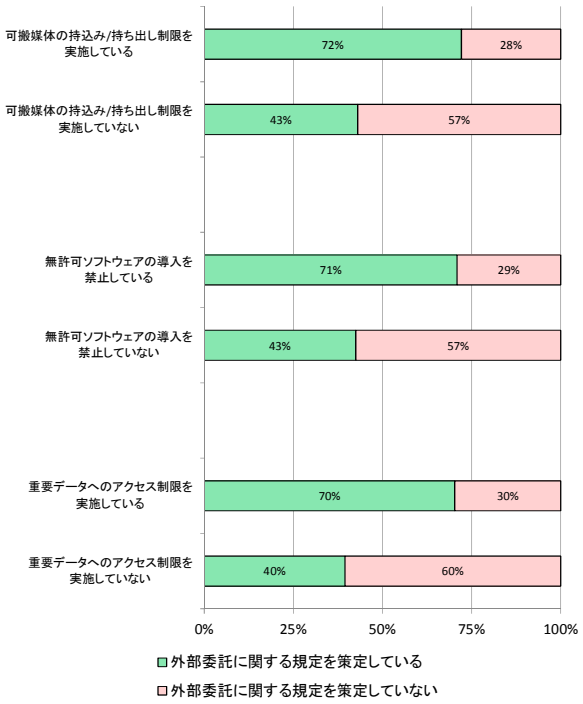
設問22　外部委託に関する規定の策定状況

・外部委託に関する規程を策定している事業者等は、可搬媒体の持込持ち出し制限を実施していたり、無許可ソフトウェアの導入を禁止していたり、重要データのアクセス制限を行っている傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

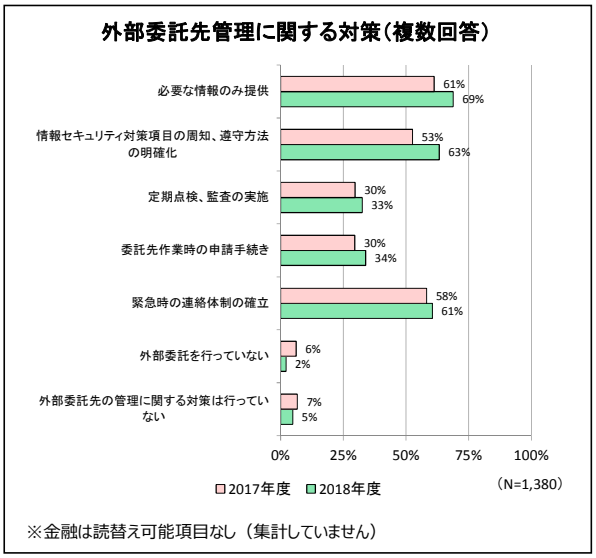
参考①　外部委託に関する規定の策定状況と各項目の関係性



アンケート調査結果詳細　－　（４０／５８）　－

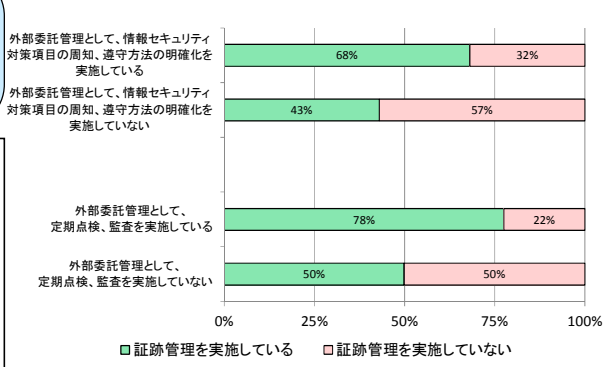
設問23　外部委託先管理に関する対策

・証跡管理を行っている事業者は「対策項目の周知や定期点検・監査」を実施している傾向がある（参考①）。
・自事業者等も内部及び外部監査を実施している事業者は、外部委託先事業者等の定期点検・監査も実施している傾向がある（参考②）。

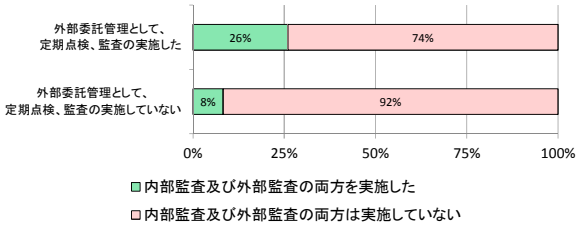


※金融は読替え可能項目なし（集計していません）

参考①　外部委託先管理に関する対策と証跡管理実施の関係性



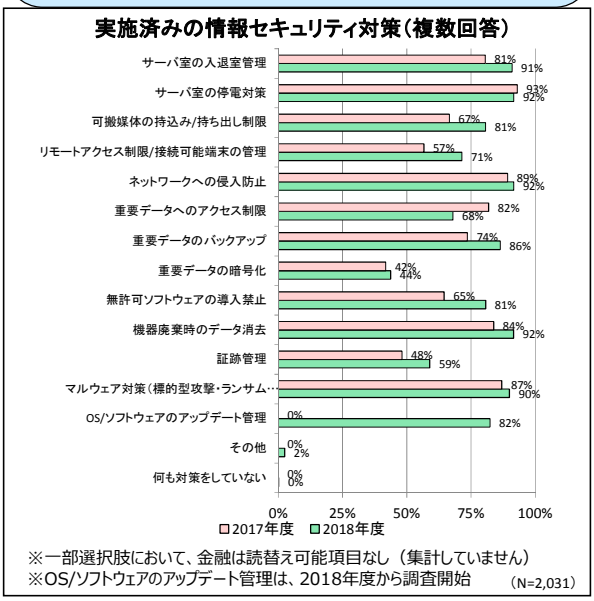
参考②　外部委託先管理に関する対策と監査実施の関係性



アンケート調査結果詳細　－　（４１／５８）　－

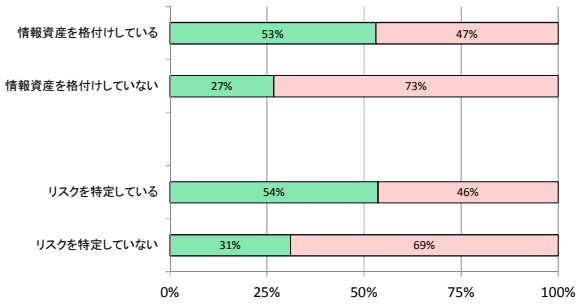
設問24　実施済みの情報セキュリティ対策

・重要データの暗号化を実施している事業者等は、情報資産の格付けを実施し、リスクの特定を行っている傾向がある（参考①）。
・証跡管理を行っている事業者等は、コンティンジェンシープラン（CP）を策定している傾向がある（参考②）。

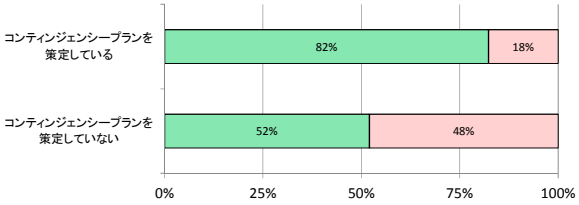


※一部選択肢において、金融は読替え可能項目なし（集計していません）
※OS/ソフトウェアのアップデート管理は、2018年度から調査開始　（N=2,031）

参考①　情報セキュリティ対策の実施状況と重要データ暗号化実施の関係性



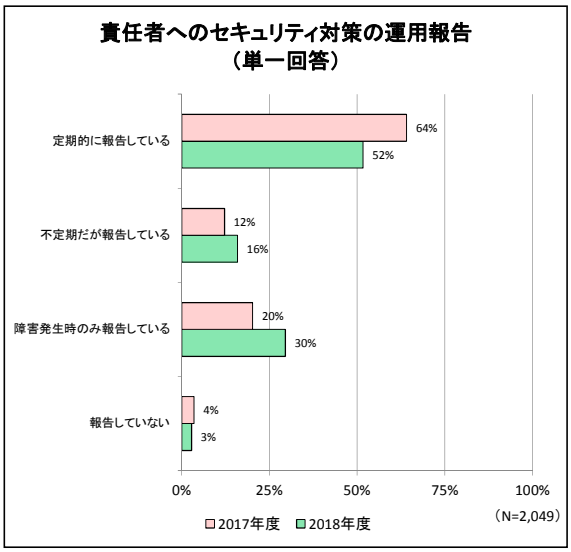
参考②　コンテンジェンシープラン（CP）策定状況と証跡管理実施の関係性



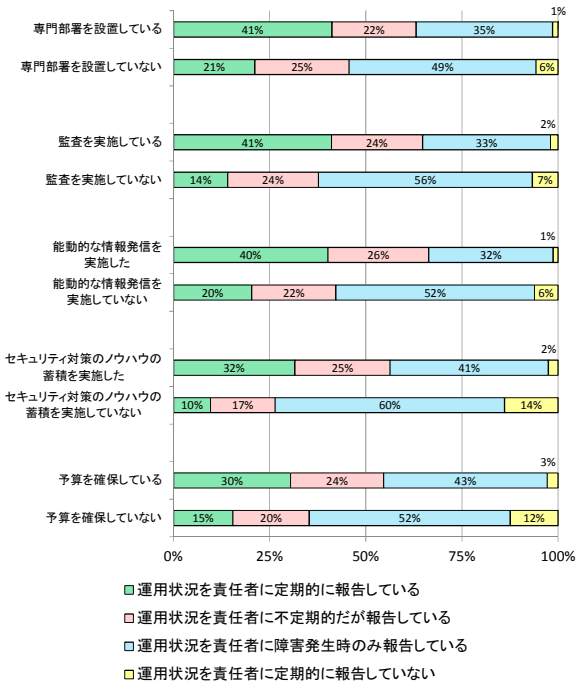
アンケート調査結果詳細　－　（４２／５８）　－

設問25　責任者へのセキュリティ対策の運用報告

・セキュリティ対策を実施する専門部署を設置している事業者等は、定期的に運用報告を行っている傾向がある（参考①）。
・障害発生時のみ責任者へ報告している事業者等は、監査を実施しておらず、能動的な情報提供を行っていない傾向がある（参考②）。



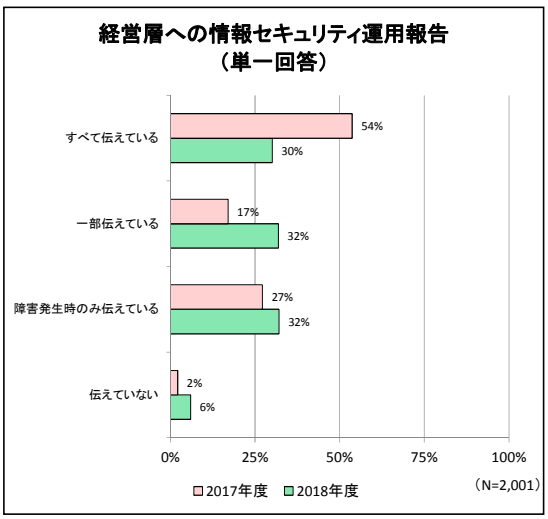
参考①　責任者へのセキュリティ対策の運用報告と各項目との関係性



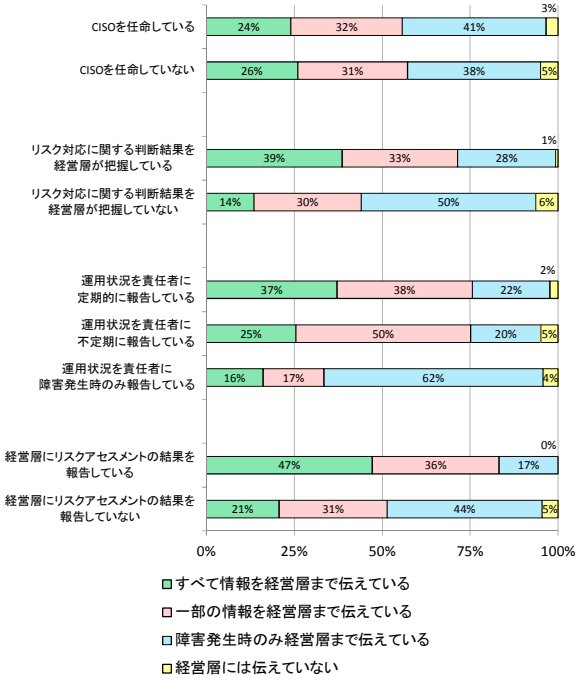
アンケート調査結果詳細　－　（４３／５８）　－

設問25-1　経営層への情報セキュリティ運用報告

・責任者に定期的に情報セキュリティ報告を行っている事業者等は、経営層にも定期的に情報を報告している傾向がある（参考①）。
・経営層に報告している事業者等はリスクアセスメントの結果についても、経営層に報告を行っている傾向がある（参考②）。



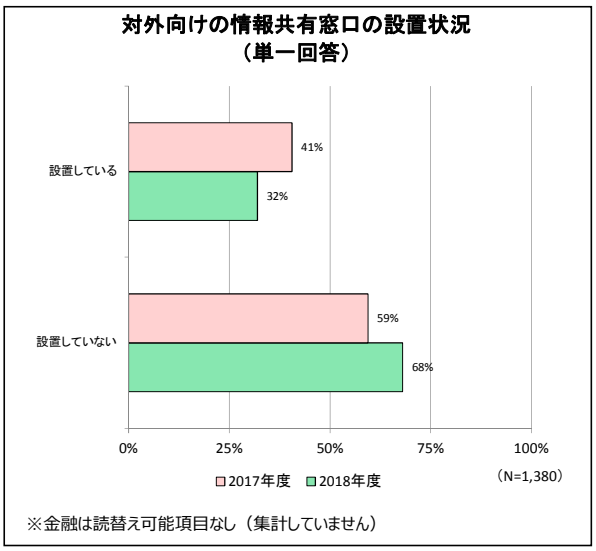
参考①　経営層への報告状況と各項目の関係性



アンケート調査結果詳細　－　（４４／５８）　－

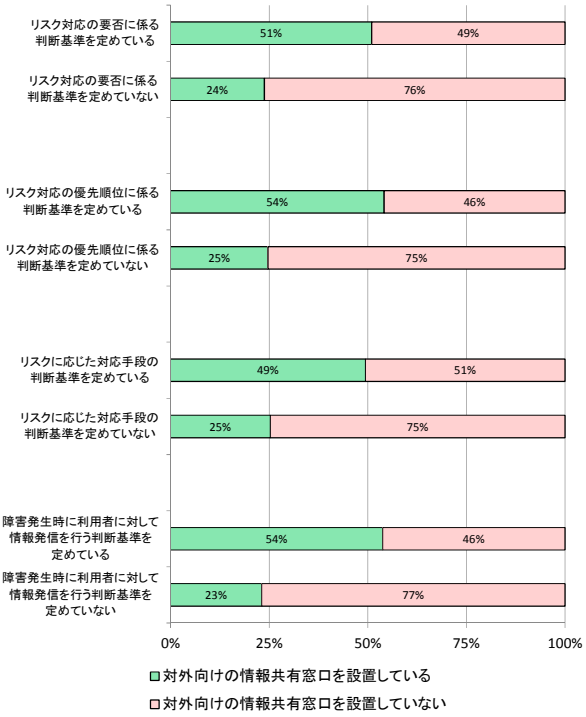
設問26　対外向けの情報共有窓口の設置状況

・対外向けの情報共有窓口を設置している事業者等は、リスク対応の優先順位に係る判断基準、対応要否に係る判断基準、リスクに応じた対応手段の判断基準が決められているだけではなく、障害発生時のサービス利用者への情報発信に関する基準も定めている傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

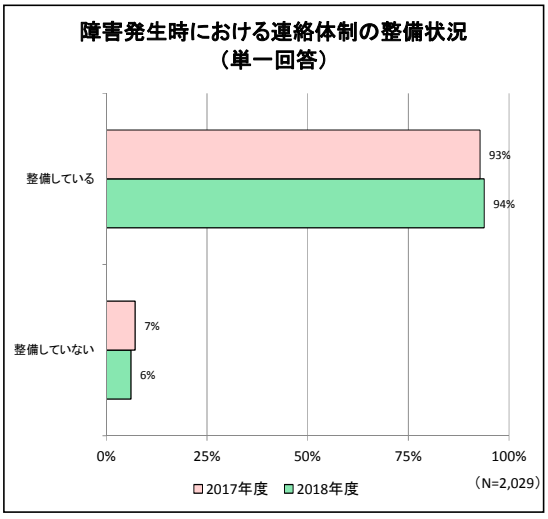
参考①　対外向け情報窓口の設置状況と各項目の関係性



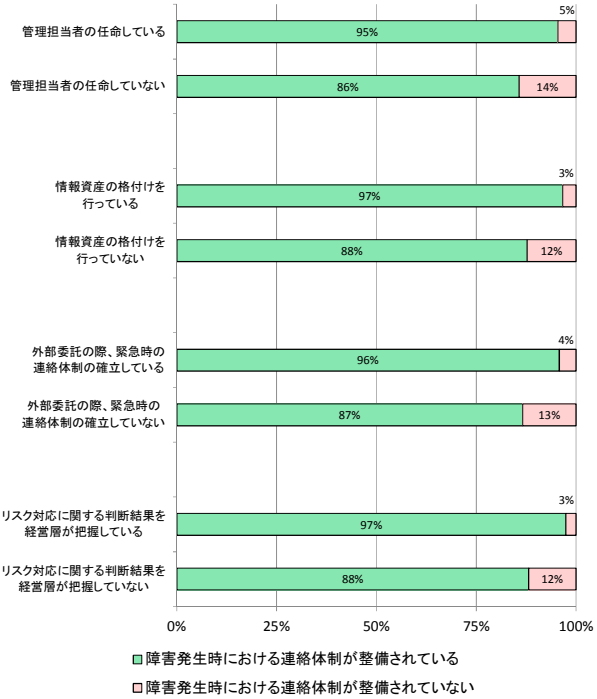
アンケート調査結果詳細　－　（４５／５８）　－

設問27　障害発生時における連絡体制の整備状況

・障害発生時における連絡体制を整備している事業者等は、情報セキュリティの管理担当者を任命しており、情報資産の格付けを実施し、外部委託の際に緊急連絡の体制を整備して、経営層にリスク対応に関する判断結果が共有されている傾向がある（参考①）。



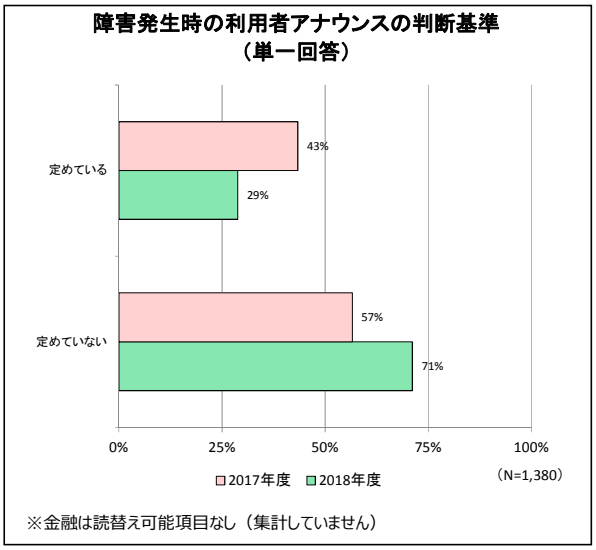
参考①　障害発生時の連絡体制整備状況と各項目の関係性



アンケート調査結果詳細　－　（４６/５８）　－

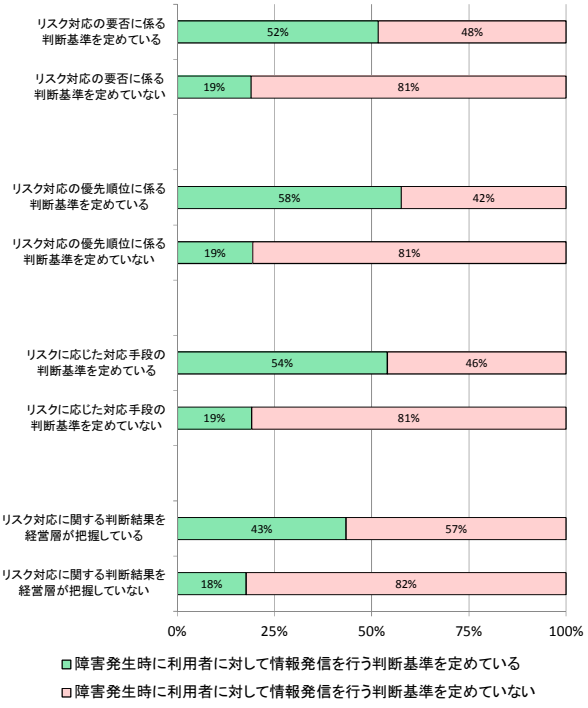
設問28　障害発生時の利用者アナウンスの判断基準

・アナウンスの判断基準を定めている事業者等は、リスクに対して判断基準もそれぞれ明確化されており、その基準および判断結果を経営層が把握している傾向がある（参考①）。



※金融は読替え可能項目なし（集計していません）

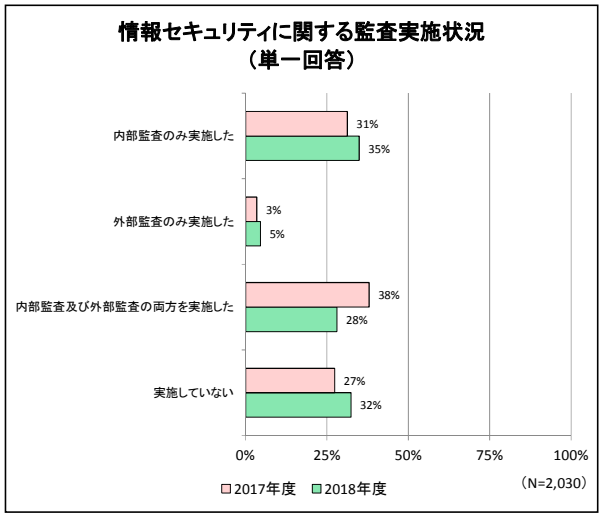
参考①　障害発生時の判断基準策定と各項目の関係性



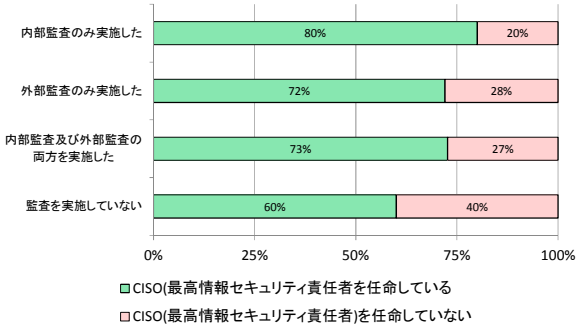
アンケート調査結果詳細　－　（４７/５８）　－

設問29　情報セキュリティに関する監査実施状況

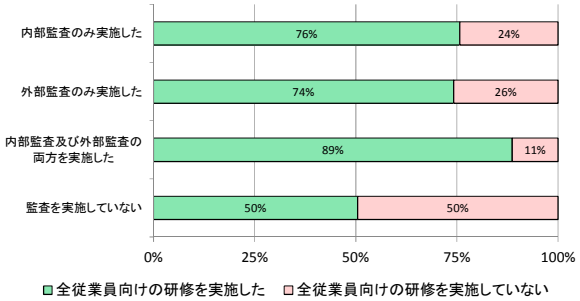
・CISOを任命している事業者は、内外監査を実施し、全従業員向けの研修を実施している傾向がある（参考①、参考②）。また、内部と外部の監査の両方を実施している９割の事業者等では、全社員向けの研修が行われている（参考②）。



参考①　監査の実施状況とCISOの設置状況の関係



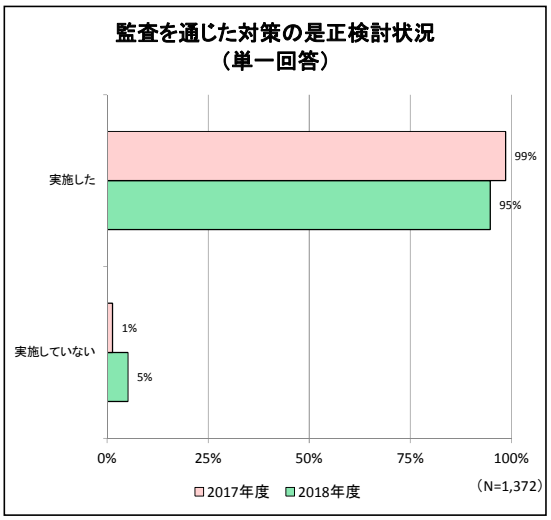
参考②　監査の実施状況と全従業員向けの研修実施状況の関係



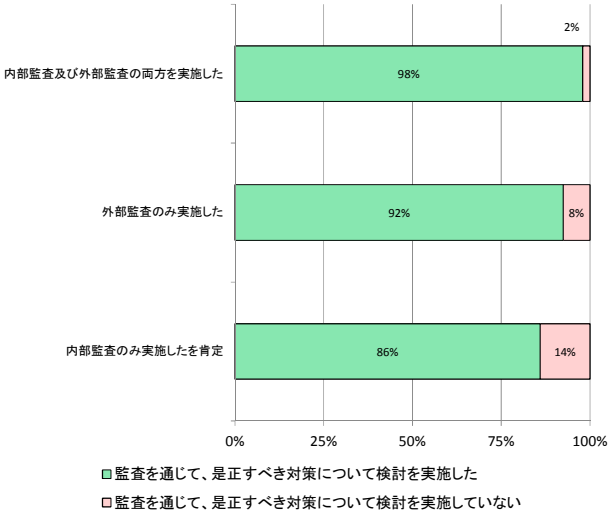
アンケート調査結果詳細　－　（４８／５８）　－

設問29-1　監査を通じた対策の是正検討状況

・監査を通じて対策の是正を実施している事業者等は、監査を、「内部・外部」＞「外部のみ」＞「内部のみ」の順で実施している。是正まで実施している事業者等は、全体的に取組が進んでいる傾向がある（参考①）。



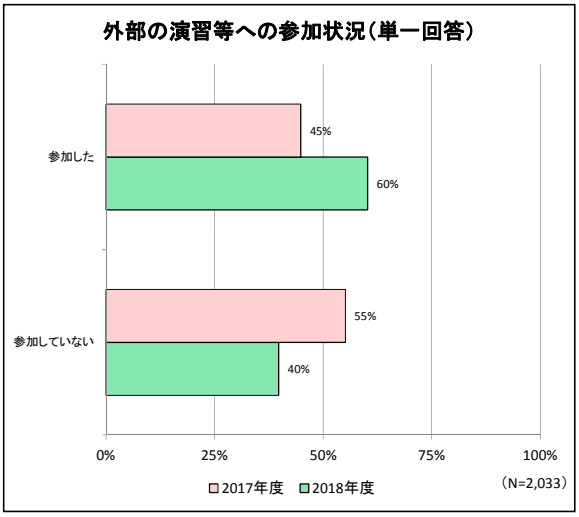
参考①　内部監査と外部監査の実施状況と対策の是正状況の関係性



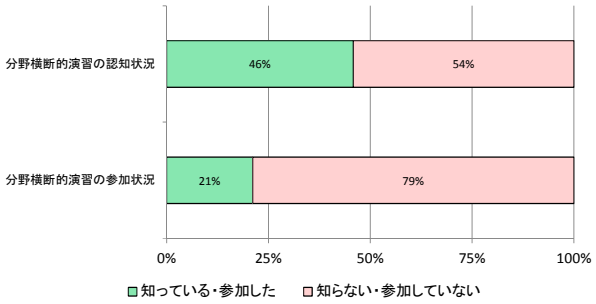
アンケート調査結果詳細　－　（４９／５８）　－

設問30　外部の演習等への参加状況

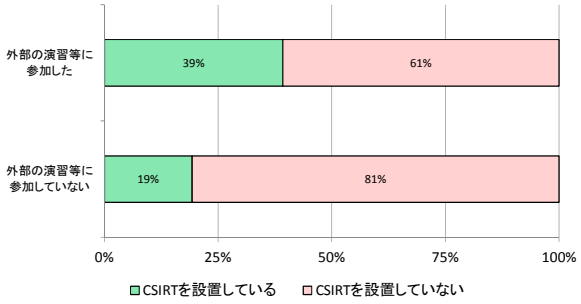
・外部の演習等に参加している事業者等のうち、５割弱が分野横断的演習を認知しており、約2割が分野横断的演習に参加した（参考①）。外部の演習等に参加するような演習に対して積極的な事業者等に対する分野横断的演習のPRは一定の効果が出ている。
・CSIRTが設置されている事業者等は「外部の演習等に参加している」傾向がある（参考②）。外部の演習等を通じて、他社の状況に刺激を受け、改善活動が進んでいると推察できる。



参考①　外部の演習等に参加している事業者等における分野横断的演習認知度と参加状況の関係性



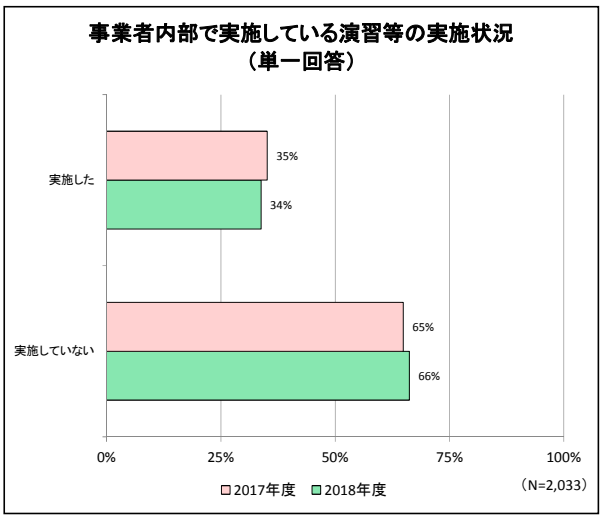
参考②　外部の演習等に参加している事業者等とCSIRT設置状況の関係性



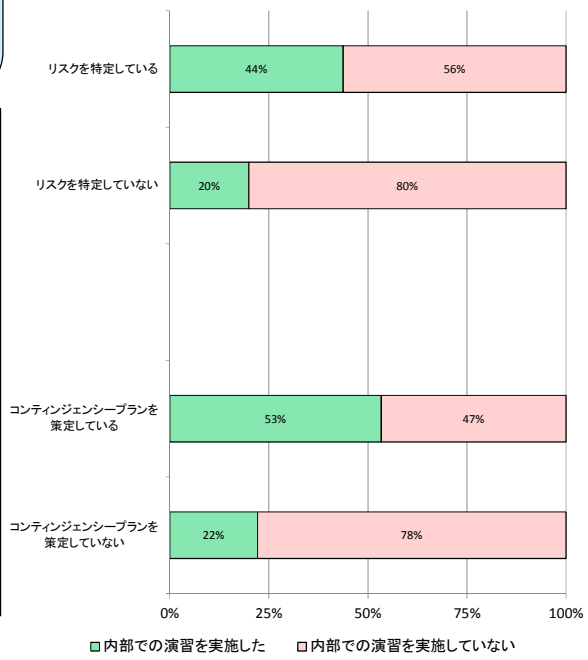
アンケート調査結果詳細　－　（５０／５８）　－

設問31　事業者等の内部で実施している演習等の実施状況

・事業者等ごとに演習を実施している事業者等では、リスクの特定やコンティンジェンシープラン（CP）の策定もできている傾向がある（参考①）。
・リスクの特定やコンティンジェンシープラン（CP）の策定ができている事業者等は、演習の機会を通じて、改善項目の洗い出しをしていると推察できる。



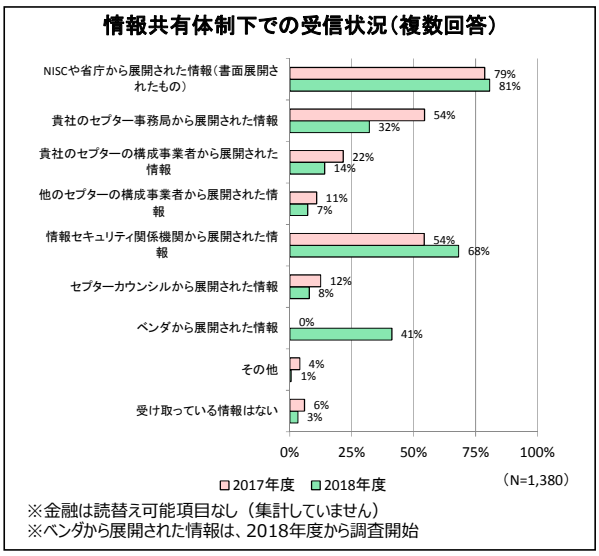
参考①　内部で実施している演習内容と各項目の関係性



アンケート調査結果詳細　－　（５１／５８）　－

設問32　情報共有体制下での受信状況

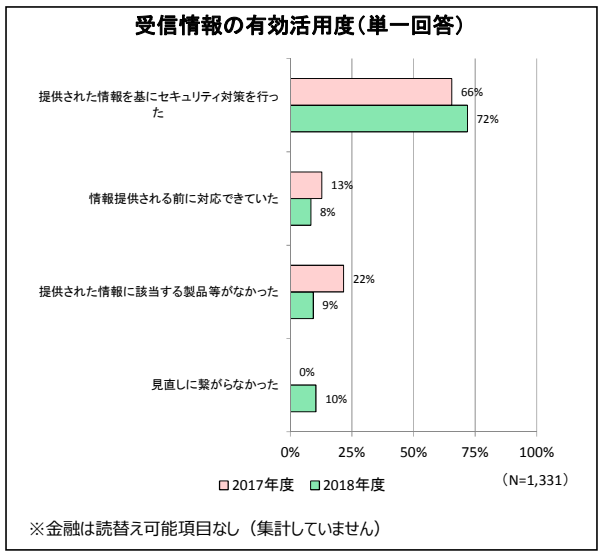
・NISCや省庁、情報セキュリティ機関といった外部から展開された情報の受信については増加傾向があるが、セプター内、セプター間の情報共有が低調でありセプターの活動の活性化を図る必要がある。



※金融は読替え可能項目なし（集計していません）
※ベンダから展開された情報は、2018年度から調査開始

設問32-1　受信情報の有効活用度

・提供された情報を基に対策を行っている事業者が増加しており、引き続き情報提供を着実に行うことが必要であると考えられる。

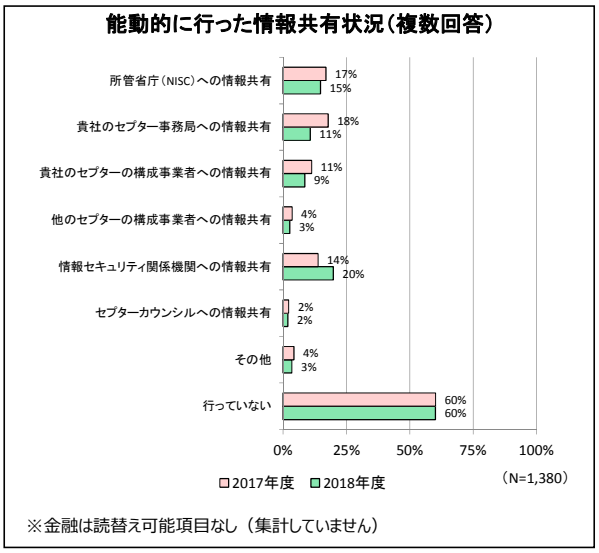


※金融は読替え可能項目なし（集計していません）

アンケート調査結果詳細　－　（５２／５８）　－

設問33　能動的に行った情報共有状況

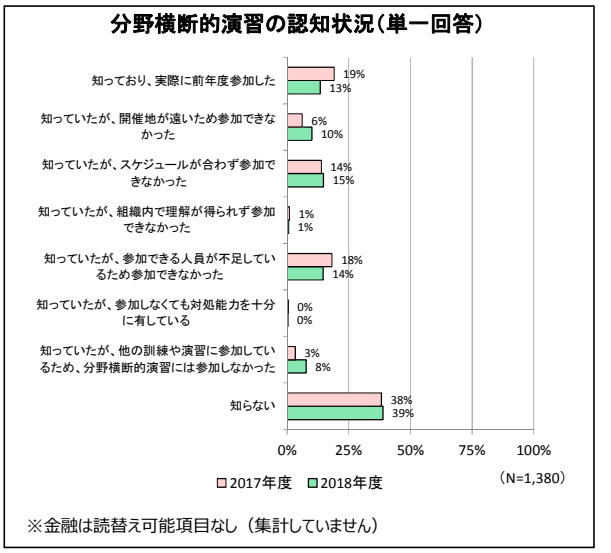
・能動的に情報共有を行っていない事業者が依然として半数以上となっている。また、情報セキュリティ機関への情報共有は増加している一方で所管省庁やセプターへの情報共有は低下しており、その状況も依然として低調である。情報共有の必要性の周知や、情報共有することによるメリットを示すなど、情報共有の活発化に向けた取組を行う必要がある。



※金融は読替え可能項目なし（集計していません）

設問34　分野横断的演習の認知状況

・「知っているが参加していない」事業者に向け、自職場参加の推奨等にて参加を促し、分野横断的演習に可能な限り参加できるよう継続的な取り組みが望まれる。
また、「知らない」事業者に対しては、所管省庁等を通して広報活動を行う必要がある。

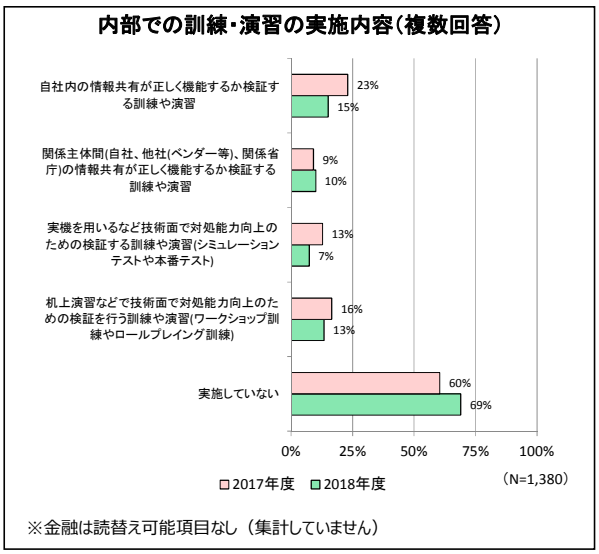


※金融は読替え可能項目なし（集計していません）

アンケート調査結果詳細　－　（５３／５８）　－

設問35　内部での訓練・演習の実施内容

・「実施していない」事業者については、まずは分野横断的演習等の演習に参加することが有効であると考えられるため、継続して演習開催の取り組みを行う必要がある。



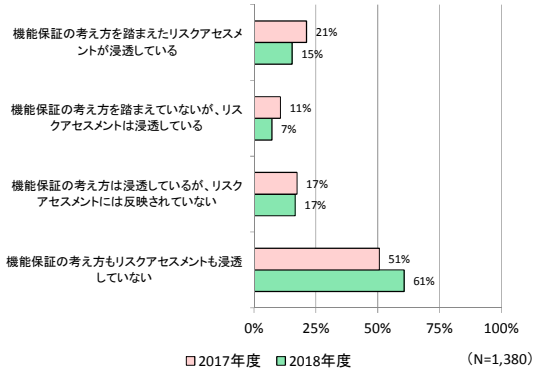
※金融は読替え可能項目なし（集計していません）

アンケート調査結果詳細　－　（５４／５８）　－

設問36　機能保証の考え方を踏まえたリスクアセスメントの認知状況

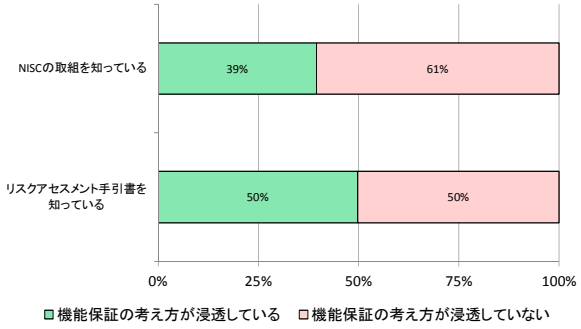
・何らかのNISCの取組を把握している事業者等のうち、６割の事業者で機能保証の考え方が浸透していない。また、リスクアセスメント手引書を把握している事業者等は５割である。そのため、一層の周知・啓発の必要性が認められる（参考①）。
・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者等であっても、うち4割がリスク対応の優先順位に係る判断基準を定めていないため、一層の実践が期待される。（参考②）

機能保証の考え方を踏まえた
リスクアセスメントの認知状況（単一回答）

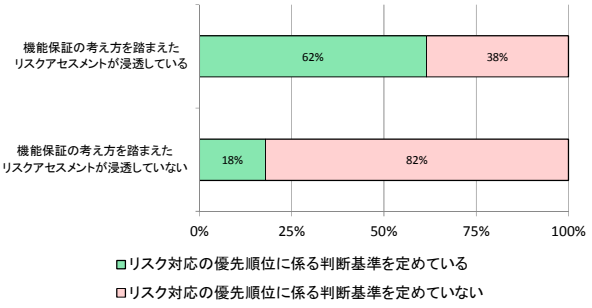


※金融は読替え可能項目なし（集計していません）

参考①　機能保証の考え方とNISCの取組認知度の関係性



参考②　リスクアセスメントの浸透とリスク対応の判断基準（優先順位）の関係性

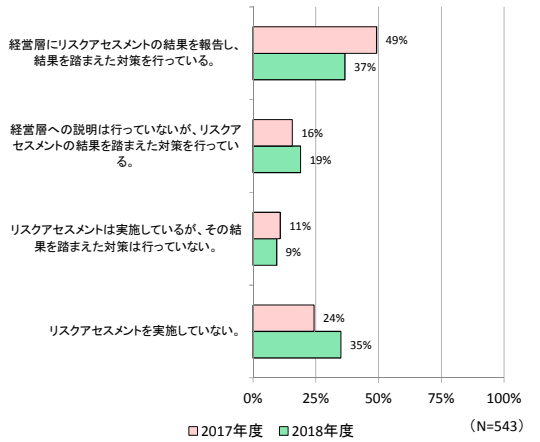


アンケート調査結果詳細　－　（５５／５８）　－

設問36-1　結果を踏まえた対策の実施状況

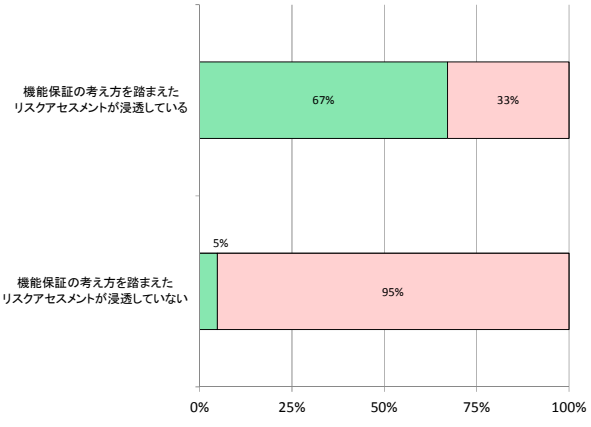
・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者等のうち7割の事業者等が、リスクアセスメントの結果を経営層へ報告していることが分かる（参考①）。一方で、全体ではリスクアセスメント自体の認知率・実施率ともに昨年より悪化している。リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じることは経営者の責務であるため、機能保証の考え方の浸透も含め、経営層への更なる働きかけが必要である。

結果を踏まえた対策の実施有無（単一回答）



※金融は読替え可能項目なし（集計していません）

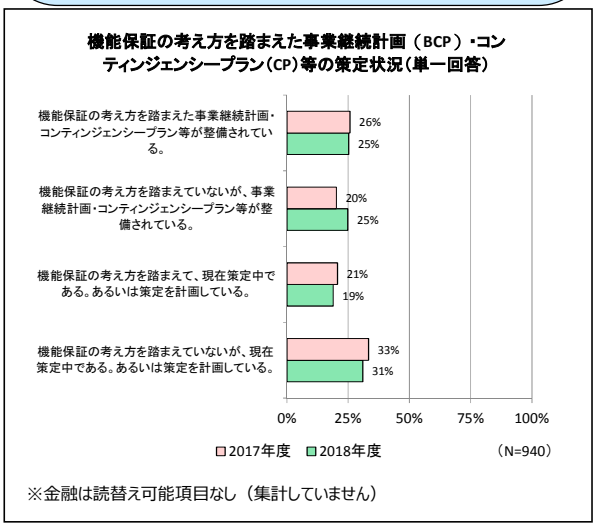
参考①　機能保証の考え方（リスクアセスメント）の浸透状況と経営層への報告（結果）の関係性



アンケート調査結果詳細　－　（５６／５８）　－

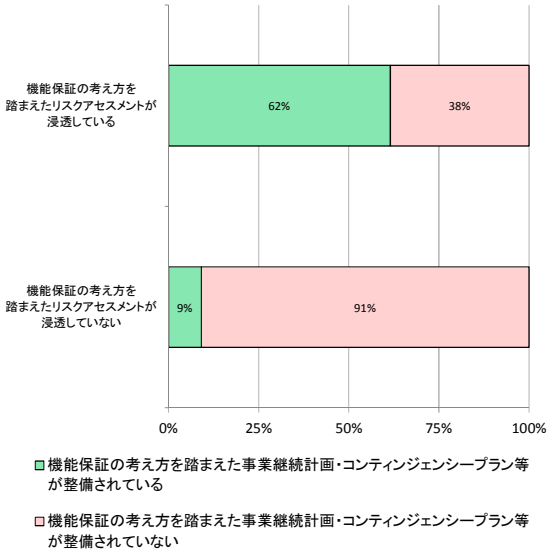
設問37　機能保証の考え方を踏まえた事業継続計画（BCP）やコンティンジェンシープラン（CP）等の策定状況

・機能保証の考え方を踏まえたリスクアセスメントが浸透している事業者のうち、機能保証の考え方を踏まえた事業継続計画（BCP）・コンティンジェンシープラン（CP）等が整備されている事業者は6割に留まっており、一層の実践が期待される（参考①）。
・策定中・計画中の事業者も合わせると８割になるため、それらの事業者への支援も有効と考えられる。
・全体では機能保証の考え方そのものの浸透に課題があり、まずはその普及・啓発が必要と考えられる。



※金融は読替え可能項目なし（集計していません）

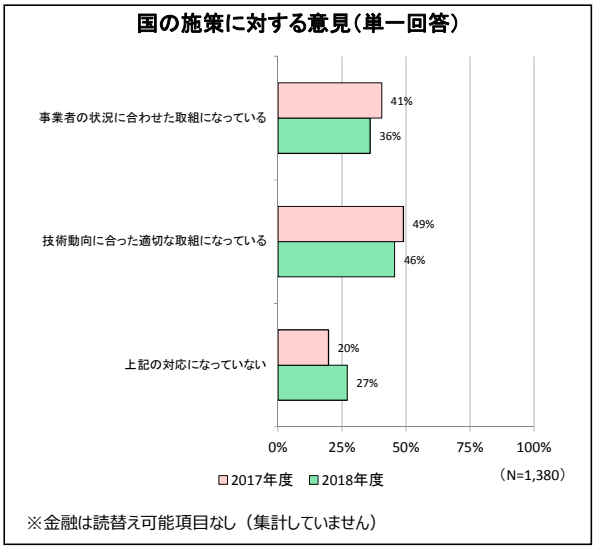
参考①　機能保証の考え方の浸透状況と事業継続計画/コンティンジェンシープラン整備状況の関係性



アンケート調査結果詳細　－　（５７／５８）　－

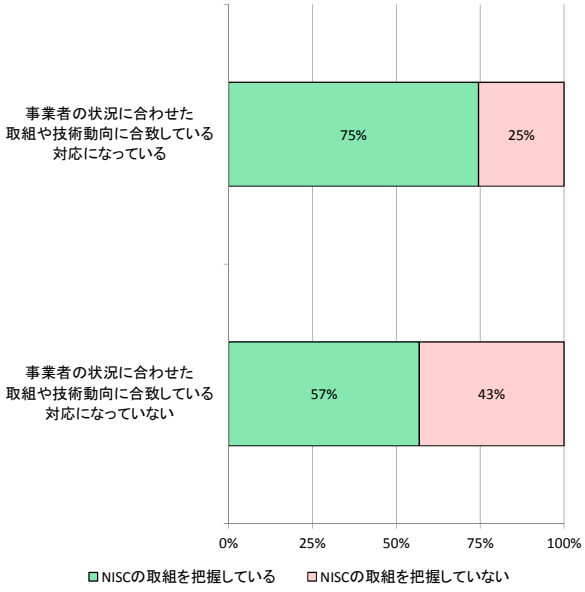
設問38　国の施策に対する意見

・事業者の状況に合わせた取組や技術動向に合致していると回答した者は、NISCの取組や自分野のガイドラインを把握している傾向があり、国の施策を理解した上でセキュリティ対策に取り組んでいるものと考えられる（参考①）。



※金融は読替え可能項目なし（集計していません）

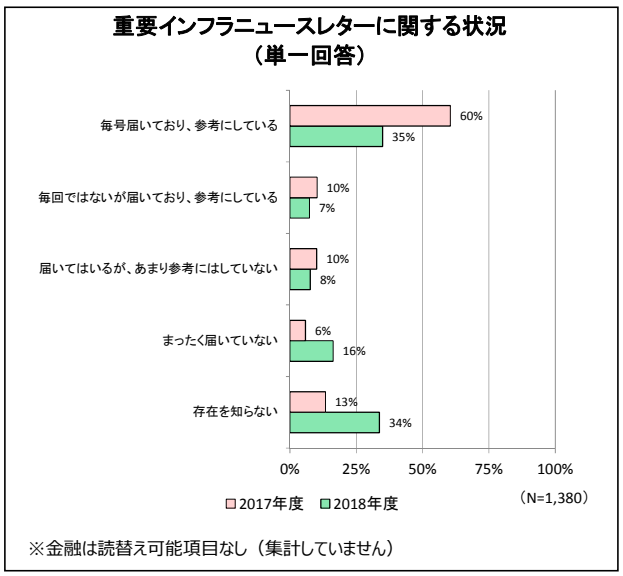
参考①　NISC等の取組把握状況と事業者等のセキュリティ対策の取組の関係性



アンケート調査結果詳細　－　（５８/５８）　－

設問39　重要インフラニュースレターに関する状況

・重要インフラニュースレターが届いていない、あるいはその存在すら知らないという事業者が増加しており、その結果参考にしている事業者についても減少してしまっている。事業者が求める内容を調べるとともに、周知活動や配信先の確認等を行う必要がある。



アンケート項目

調査に用いたｱﾝｹｰﾄ項目は以下の通り。なお、各項目のｸﾞﾗﾌについては「5.調査結果詳細」の該当設問を参照のこと

【Ⅰ．前提条件】

分野の選択
従業員数（規模）の選択

【Ⅱ．浸透状況等調査項目】

設問1　NISCの取組の認知状況
設問2　自分野の安全基準等の認知状況
設問3　情報セキュリティ対策の実施に向けた予算の確保状況
設問4　セキュリティ人材の確保状況
設問4-1　必要とする人材の職種
設問5　セキュリティ人材育成の取組状況
設問6　全従業員向けセキュリティ研修の実施状況
設問7　内部体制の取組状況
設問8　情報セキュリティ対策のノウハウの蓄積方法
設問9　情報セキュリティ対策に関する基本方針の策定状況
設問9-1　基本方針の策定に関する経営層の関与状況
設問9-2　策定した基本方針の外部公表状況
設問9-3　基本方針の見直し検討状況
設問9-4　基本方針の見直し検討の契機
設問10　情報セキュリティ対策に関する計画策定状況
設問10-1　計画の見直し（又は修正）状況
設問11　取扱い情報資産（システム含む）の洗い出し及び台帳等での管理状況
設問11-1　情報資産の重要度に応じた格付け状況
設問11-2　情報資産の見直し状況
設問12　脅威や脆弱性等の情報収集
設問12-1　情報収集の確認頻度
設問13　リスクの特定状況
設問13-1　リスクの特定方法
設問14　リスク対応の要否に係る判断基準

【Ⅱ．浸透状況等調査項目】（続き）

設問15　リスク対応の優先順位に係る判断基準
設問16　リスクに応じた対応手段の判断基準
設問17　リスク対応に関する判断結果についての経営層の把握状況
設問18　情報セキュリティに関する内規の策定状況
設問18-1　内規等を策定する際の参考文献
設問18-2　策定した内規の見直し検討状況
設問18-3　内規の見直し検討の契機
設問19　情報の取扱いに関する規定の策定状況
設問20　事業継続計画（BCP）の策定状況
設問20-1　事業継続計画（BCP）に基づいた訓練状況
設問20-2　事業継続計画（BCP）の見直し状況
設問20-3　事業継続計画（BCP）の見直し契機
設問21　コンティンジェンシープラン（CP）策定状況
設問21-1　コンティンジェンシープラン（CP）の見直し状況
設問22　外部委託に関する規定の策定状況
設問23　外部委託先管理に関する対策
設問24　実施済みの情報セキュリティ対策
設問25　責任者へのセキュリティ対策の運用報告
設問25-1　経営層への情報セキュリティ運用報告
設問26　対外向けの情報共有窓口の設置状況
設問27　障害発生時における連絡体制の整備状況
設問28　障害発生時の利用者アナウンスの判断基準
設問29　情報セキュリティに関する監査実施状況
設問29-1　監査を通じた対策の是正検討状況
設問30　外部の演習等への参加状況
設問31　内部での演習等の実施状況

【Ⅲ．国の施策の取組状況調査】

設問32　情報共有体制下での受信状況
設問32-1　受信情報の有効活用度
設問33　能動的に行った情報共有状況
設問34　分野横断的演習の認知状況
設問35　内部での訓練・演習の実施内容
設問36　機能保証の考え方を踏まえたリスクアセスメントの認知状況
設問36-1　結果を踏まえた対策の実施状況
設問37　機能保証の考え方を踏まえた事業継続計画（BCP）・コンティンジェンシープラン（CP）等の策定状況
設問38　国の施策に対する意見
設問39　重要インフラニュースレターに関する状況

【Ⅳ．　自由記述】

a.　本編及び対策編に対する意見（自由意見を記載）
b.　安全基準等に対する意見（自由意見を記載）
c.　その他の意見（自由意見を記載）
d.　NISCの取組についての意見（自由意見を記載）
e.　セキュリティ人材についての意見（自由意見を記載）
f.　人材育成についての意見（自由意見を記載）
g.　内部統制強化についての意見（自由意見を記載）
h.　ノウハウの蓄積方法についての意見（自由意見を記載）
i.　基本方針の見直し契機についての意見（自由意見を記載）
j.　リスクの特定方法についての意見（自由意見を記載）
k.　内規の策定する際の参考文献に関する意見（自由意見を記載）
l.　内規の見直し契機についての意見（自由意見を記載）
m.　事業継続計画（BCP）の見直し契機についての意見（自由意見を記載）
n.　セキュリティ対策の実施手法に関する意見（自由意見を記載）
o.　情報共有（受信側）に関する意見（自由意見を記載）
p.　情報共有（送信側）に関する意見（自由意見を記載）

アンケート調査の自由意見

【安全基準等に関する意見・要望等】

- 情報セキュリティポリシーを策定する際には、安全基準等や関連組織が発行しているガイドブック等を参考にしている。
- 販売されている情報システムの製品については、購入時点で情報セキュリティのガイドライン等に準拠することができるよう、政府として動いていただきたい。
- 分野特有のシステムに汎用的なOSの採用やバックアップの回線にインターネットVPNの採用等の新たなリスクが増加していることから、安全基準等を改正する際には、事業者の現状を把握する必要がある。
- 安全基準等は、策定する所管省庁ごとに事業者に求める対策水準が異なるため、設備によっては対策水準が異なる。分野によらない一律の対策水準を策定していただきたい。
- 安全基準等を策定する際は、最終目標だけでなく、各事業者等の事情を踏まえ、状況に応じた段階的な対応策及び業務支援の拡充を考慮したうえで、円滑な対応ができるよう検討いただきたい。
- 安全基準等の内容が抽象的である。安全基準等として、どの程度の対策水準を求めているのか、またどの対策の水準を満たせば十分なのか具体的かつ明確に示していただきたい。
- 事業規模が小さい事業者では、人材面や資金面が十分ではないため、政府や情報セキュリティ関連団体が要求する事項を実施することは難しい。対策を実施するのに障壁が高いセキュリティ対策を要求するのであれば、実現可能な手立ても併せて提示していただきたい。事業規模に合わせた対策内容や優先順位、ロードマップ等を示していただきたい。
- 事業規模が小さい事業者は人材や資金が乏しいため、安全基準等の対策をすべて講じることは難しい。事業規模を考慮した安全基準等を策定していただきたい。
- 安全基準等の充足度が事業者でも確認できるチェックリストがほしい。
- 安全基準等の改訂があった場合は、わかりやすい新旧対照表をいただきたい。
- 一部の安全基準等は、難しい専門的用語やカタカナ英語を用いているので、わかりにくい。初心者でも理解し、読み手全員が共通の認識を得られるように、解説や例示を設ける等の配慮をいただきたい。
- 安全基準等に基づき規則・基準・内規等を整備したとしても、その実効性に疑問がある。また、訓練や演習、監査も人材面や資金面の負担が大きい。そのため、費用対効果の高い対策等を示していただきたい。
- 重要サービスの提供に関わる重要な施設は広大であり、様々な職種の方が作業に関わるため、入退管理制限対策を行い、部外者の侵入を完全に塞ぐことは難しい。

【指針に関する意見・要望等】

- 一部の分野では、指針を参考にガイドラインが策定され、チェックシート等が整備された。
- 具体的にどのような対策を進めていくべきか、明示的に示してほしい。
- 「機能保証」は重要であるが、これを前提すると情報セキュリティ以外も考慮する必要が発生してしまう。

【情報共有体制の推進に関する意見・要望等】

- 一部の分野では、業法に基づいて報告する事案でないヒヤリハット等を情報共有できるルートが設定されている。
- 第４次行動計画の情報共有体制では、業法に関わる事案やヒヤリハットで匿名化の処置が必要な事案によって、報告ルートが異なっている。インシデント対応は対応事項が多いので、報告ルートを統一化し、事業者負担の軽減してほしい。
- 政府やセプター事務局、セキュリティ関係機関は、脅威の大きさに関わらず注意喚起を行っているため、その件数が多い。結果、事業者が情報の確認や評価する負荷が増加したため、脅威情報の検知等が遅くなるリスクが増加している。情報提供元が情報を集約し、評価していただきたい。
- 報告先により、情報共有方法（メール、システム、電話等）が統一されていない。この部分も、統一化していただきたい。
- 情報共有の手法が、情報共有ツールを用いたシステム化が進んでいるが、一部の事業者ではセキュリティ上の思想により、情報共有ツールが遮断されているケースもあり、情報の共有にタイムラグが生じている。
- 政府の施策が改善され、事業者まで周知が必要な事項の場合は、連絡していただきたい。
- 情報システム部とセキュリティベンダーの月例会を実施し、サイバーセキュリティインシデントに関する情報交換を行っている。
- 情報セキュリティのインシデント事例の提供は有難い。必要に応じて、関係部署と共有し、セキュリティ強化を図っている。
- セキュリティ情報は積極的に収集しているが、情報報告や社内展開には消極的である。
- セキュリティベンダーの担当者から定期的にセキュリティパッチ配信や情報セキュリティの助言をいただいている。
- 地域的に近い事業者や同じ分野の事業者、ITユーザ会の参加事業者と情報システム部会を開催し、意見交換している。
- 技術の進展やソフトウエアの開発によって、リスクや脅威の変化するので、最新の状況を連携していただきたい。
- 情報システムや情報セキュリティの発展速度が著しく早いため、習得したノウハウがすぐに過去のものになってしまう。また、情報セキュリティの情報は公開されにくいため、最新情報が簡単には得にくい。

【国・政府に対する意見・要望等】

- NISCが発行している重要インフラニュースレターは、必要な情報がまとめられており、対策検討や注意喚起に役立っている。
- 重要インフラニュースレターの情報は、専門性が高く、送られてくる情報が理解できない部分がある。
- 政府や情報セキュリティ関係機関から早期警戒情報や脆弱性情報等の情報が届くが、提供元ルートを一元化してほしい。
- 分野的横断演習のインデント対応の中で、自社の対応における問題点や課題が明確になった。
- 「重要インフラ事業者等」に該当する事業者等の定義を明確にしていただきたい。
- ランサムウェア等によるシステム不全に陥るようなサイバー攻撃が目立ってきているが、現状では、マルウェアの対策はソフトウェア業界任せになっており、表面化していない脅威に積極的に取り組んでいるとは言い難い。そのような脅威を未然に防ぐためにも、政府の研究機関等が、マルウェア対策に取り組んでいただきたい。
- 情報セキュリティに関わる「人材育成」を重要課題と捉え、積極的な支援や方策等について取り組んでいただきたい。
- 情報セキュリティ対策に関わる補助金などを準備いただきたい。
- 情報セキュリティの担当者が少ない事業者でも取り組めるセキュリティ対策良好事例を紹介いただききたい。
- ネットワークを含めたセキュリティの基礎から習得する必要があるため、Cyderだけでなく、ベンダーが実施している有償の技術研修にも参加している。セキュリティ対策への理解が得られなければ、予算の確保もできないため、Cyder等の研修において、ネットワークを含めたセキュリティの基礎から習得する研修を設定してほしい。
- CSIRT構築など情報セキュリティ対策として求められる要件を鑑みて、最低限義務付ける人員・業務項目を提示いただくとともに、ハードルの高いセキュリティ対策を要求するなら、実現可能な手立てや態勢整備のための支援・補助を期待する。
- 情報セキュリティや情報システムを保守する技術職の人材不足で、十分な対応ができない。また、次世代の育成にも問題を抱えている。政府として、事業規模の小さい事業者でも、情報セキュリティや情報システムを保守する技術職の従業員が十分確保できるような施策を行っていただきたい。
- IoT機器やSNSの普及により、インターネット環境が必要不可欠となってきている。利便性を高めつつ、セキュリティ強化をする必要があり、設備費用や運用費用も高額になっている。政府として、費用を抑える仕組みを検討していただきたい。

【アンケートに関する意見・要望等】

- アンケート後に表示される事業者に向けた「アドバイス」があり、大変参考になった。
- 情報セキュリティ対策のノウハウを蓄積するという考えそのものがなく、大変参考になった。
- 情報セキュリティの専門知識を有する従業員が少ない事業者等もいるため、情報セキュリティ用語の説明や推奨される取り組み等のURLを増やして頂けると他部署の従業員等への情報の共有や浸透に、より一層利用しやすくなる。
- 重要インフラサービス提供に最も大きく影響するシステムに対する設問への回答が、実態とそぐわない場合がある。そのシステムについて回答を求める場合は、実態に合った設問に修正していただきたい。
- 重要システムの運用管理部門と全体統制を行う部門が異なるため、各設問項目において、回答すべき部門や回答を想定しているシステム等を明記していただきたい。（「システム運用部門への問い」「全社的なリスク統括部門への問い」 等）
- 「アンケート設問に対する注釈の内容が読めない」「解説文のアドレスをコピーできない」「表示されるURLがリンク切れしている」等があるため、必要に応じて改善していただきたい。また、シートの保護を解除する件について、ご検討いただきたい。

【その他の意見】

- 情報セキュリティは社内を横断した対策を求められることから様々な知見が必要だが、情報セキュリティを一括して相談できる窓口がない。コンサルタントに相談することも考えられるが、資金が必要となるため、事業規模の小さい事業者では、現実的な選択肢ではなく、対策の取り組みが滞ってしまう。

別添４－５　安全基準等の浸透状況等に関する調査（往訪調査）

往訪調査の目的等

1.本調査の目的

- アンケート調査結果から得られた仮説の検証及び良好事例の収集
- 各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

※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）

2.調査方法

安全基準等の浸透状況等調査の結果を基にした現地ヒアリング（2時間程度）

3.主な調査内容

① 経営層の関わり方について
② 演習や訓練について
③ 情報共有体制について
④ 内部・外部犯行対策について
⑤ システムの出入り口対策について

4.調査対象

重要インフラ事業者等　16者
情報通信分野・航空分野・鉄道分野・物流分野・ガス分野・クレジット分野
※アンケート調査結果・地域特性・事業規模を踏まえ、選定
※所管省庁や関係セプター事務局と調整の上、対象事業者を選定

5.調査期間

2018年1月～2018年12月

6.調査結果

往訪先事業者等から得られた検証結果と良好事例を取りまとめた。

※調査対象を公表することにより事業者に不利益が生ずる可能性があるため、個社名は非公表

往訪調査で収集した良好事例のトピック

往訪調査を通じて収集した良好事例の中から、特に紹介したい良好な事例は下記である。

■新システムの導入を見据えたインシデント対応訓練

重要インフラ事業者等は、標的型攻撃メール訓練や自社ルールに基づく訓練を、e-lerningや分野横断的演習などを通じて防護能力の維持・向上を図るべきである。

新システム導入による初動対応の変更点を訓練を通じて、定着化させている事業者等がある。具体的には、新システム導入により想定されるサイバー攻撃やシステム不具合の挙動を周知し、挙動を確認している。

訓練の時期：システム導入前
訓練対象者：重要システム関係者（運用者・保守員・設計者）

■社内の情報共有（社内CSIRT）

重要インフラ事業者等は、情報セキュリティ部門を中心に、情報共有体制を構築するべきである。

情報セキュリティ部門だけでなく**制御部門に対して、国内外の最新インシデント情報やCSMS認証等の紹介を行い、情報セキュリティへの取り組み意識を醸成**させている事業者等がある。

■外部委託事業者との外部委託契約での内部犯行の抑制

昨今のサプライチェーンリスクを鑑み、外部委託事業者やその再委託先等が重要インフラ事業者の資産にアクセスするリスクを低減する取組を行うべきである。

内部犯行対策として有効な事項を外部委託契約書に明記し、発注事業者と外部委託事業者の双方で内部犯行を防止している事業者等がある。

（犯行対策の例）
申請外作業の禁止、単独作業禁止、作業前セキュリティ更新プログラム（パッチ）の適用、セキュリティ教育受講　等

往訪調査結果（1/5）　経営層の関わり方について

【経営層の働きかけ（トップダウン）】 経営層が情報セキュリティの積極的な取り組みを従業員に働きかけている。

- 東京オリンピック・パラリンピック競技大会や主要国首脳会議等のような国際的イベントに目標を合わせて、従業員の士気を上げながら情報セキュリティへの取り組みを加速させている。国際的イベントを見据え構築した情報セキュリティ体制を社内のレガシーとして定着化させることも視野に体制を整えている。
- 経営層が率先して情報セキュリティの取り組みは将来への投資であると説明し、情報セキュリティの取り組みを先導している。

■経営層の働きかけ

- 国際的イベントを万全な設備・組織体制で迎えられるように、重要システムに対するリスクアセスメントを実施し、改善活動をしている。また、過去の国際的イベントで発生したサイバー攻撃の事例を洗い出し、社員への情報共有及び対策状況の確認・対策の実施を指示している。
- 国際的イベントに向けて構築している情報共有体制やインシデント対応の規則・基準等をレガシーとして、定着化させている。
- 経営層が情報セキュリティの改善活動を統括する立場になり、セキュリティ連絡部会を発足し、平時からの情報共有やPDCAに沿った改善活動を行い、組織的な情報セキュリティ体制を構築している。また、毎月セキュリティ連絡部会を開催し、経営層が直接進捗を確認している。さらに、サイバーセキュリティの資金はコストではなく、投資であると経営層自ら社員に説明し、活発な取り組みを経営層が先導している。

リスクアセスメント手順

【経営層への働きかけ（ボトムアップ）】 従業員が経営層に、情報セキュリティの動向を報告し、経営層の積極的な関与を促している。

- 情報セキュリティのインシデント情報や政府の動向等の最新情報を経営層に定期的に報告し、経営層の積極的な働きかけを促している。

■経営層への働きかけ

- 流行しているサイバー攻撃やマルウェアの傾向等の情報を収集し、自社の重要システムが被害を受けた場合に想定される重要サービス支障の大きさを分析し、経営層に報告している。また、リスクを除去するために必要な設備対策や人材配置等の意見具申を行い、経営層を巻き込んだ取り組みを活性化させている。
- 政府が求める取り組みや同業他社の取り組み等を経営層に説明して、情報セキュリティの取組みにおける自社の状況と自社が取り組むべき事項を報告し、経営層と改善活動を行っている。

報告内容（例）
■最新動向
・インシデントの動向
・政府や同業他社の動向（取り組み状況）
■世間のインシデント状況
・流行しているサイバー攻撃の事例
・マルウェアに感染した場合の想定される被害
■その他
・リスクアセスメントの結果
・必要な設備・人的対策　等

往訪調査結果（2/5）　演習や訓練について

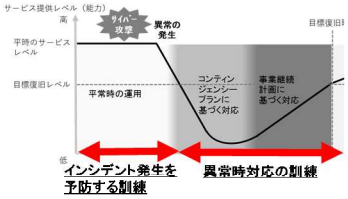
【インシデント発生を予防する訓練】 サイバー攻撃の被害を受けないための訓練・演習を実施している。

- 標的型攻撃やマルウェア感染等のサイバー攻撃を受けないように、平時から全従業員に対して、訓練や演習を行い、危機意識を高めている。

■ 標的型攻撃メール訓練

- 業務関係者を模した巧妙なメールを送り、標的型攻撃メール攻撃を体験し、情報セキュリティの危機意識を高めている

✓ 訓練の頻度：年間３回程度
✓ 訓練対象者：全従業員（契約社員含む）
✓ 訓練の手段：事前告知なしで標的型攻撃メールを模した訓練メールを送付



【異常時対応の訓練】 重要インフラサービスの提供に支障が発生した場合を想定した訓練・演習を実施している。

- 自社や政府の演習・訓練を活用して、コンティンジェンシープラン（CP）と事業継続計画（BCP）の機能とインシデント対応力の確認・改善を行っている。
- 新システム導入によって生じる初動対応の変更点等を周知し、訓練を通じてインシデント対応の流れを定着させ、インシデント対応力の強化を図っている。

■ CPとBCPの発動を想定した訓練実施（自社訓練）

- サイバー攻撃の被害を受けている想定の下、規則・基準・対応マニュアルに則り、正しい判断・行動や社内連携ができるかを検証している。

✓ 訓練の頻度：年間１回程度
✓ 訓練対象者：従業員（契約社員含む）、ベンダ、メーカ
サービスを提供する上で関係する事業者　等

■ NISC主催の分野横断的演習の活用

- 分野横断的演習で、自社のリスクに合わせたシナリオを作成し、政府への情報連絡や社内連携、CPやBCPが発動した場合のインシデントの対応等を検証し、PDCAサイクルに沿った改善活動を行っている。

✓ 訓練の頻度：年間１回
✓ 訓練対象者：情報システム部門、制御部門、広報部門、ベンダ　等

■ e-learningを用いた訓練

- e-learningを用いて、マルウェア感染や標的型攻撃を受けた場合の被害を体験している。さらに、被害を受けた後の初動対応や報告等の一連のインシデント対応の流れをe-learningを用いて訓練している。

✓ 訓練の頻度：年間１回程度
✓ 訓練対象者：従業員（契約社員含む）

■ 新システムの導入を見据えたインシデント対応訓練

- 新システム導入により想定されるサイバー攻撃やシステム不具合の挙動を周知し、挙動を確認した場合の初動対応を確認している。また、新システム導入による初動対応の変更点を訓練を通じて、定着化させている。

✓ 訓練の時期：システム導入前
✓ 訓練対象者：重要システム関係者（運用者・保守員・設計者）

往訪調査結果（3/5）　情報共有体制について

【情報共有体制の構築】 情報セキュリティに関わる情報を担当者に早急に伝えるため、十分な情報共有体制を構築している。

- 社内では部署を跨いだ情報共有の仕組みを構築し、収集した情報を担当部署に適切に展開する体制を構築している。
- 社外からの情報収集窓口を複数設け、最新のインシデント情報を確実に収集できる体制を構築している。

■社内の情報共有（社内CSIRT）

- 重要システムを保守している制御部門が情報セキュリティに関わる対策を適切に行うため、情報システム部門や制御部門等で構成する社内CSIRTを結成すると共に、情報交換する連絡会を設けている。
- 情報セキュリティの取り組みが遅れがちである制御部門に対して、国内外の最新インシデント情報やCSMS認証等の紹介を行い、情報セキュリティへの取り組み意識を醸成させている。
- 情報セキュリティのインシデントが発生した場合、経営層や様々な部署がインシデント対応に関わることが想定されるため、対応に関わるメンバーで訓練に参加し、対応の流れの確認や課題の洗い出しを行い、体制の強化を図っている。

■グループ（親会社・子会社）内で情報共有

- 情報セキュリティのリソース（作業者、資金等）が不足している子会社も情報セキュリティの取組みを進めるため、親会社から子会社に情報セキュリティの情報提供を行い、協力して情報セキュリティに取り組んでいる。
  （情報共有の例）
  ・国内外の最新インシデント情報や政府の動向等の最新情報
  ・セキュリティポリシー,BCP,CP,対応マニュアル等の規則や内規類　等
- グループ外からの情報セキュリティに関わる情報は、リソースが豊富な親会社が統括的に管理し、必要な情報を担当者に直接展開している。

■日本CSIRT協議会との連携や地域的な取り組み

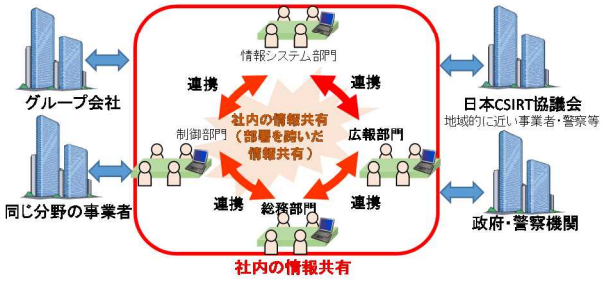
- 日本CSIRT協議会に加盟した事業者内でサイバーセキュリティの情報を共有している。
- 地域におけるセキュリティを守ることを目的に、最新情報を地域的に近い事業者や警察等と共有をしている。

■警察機関との連携

- サイバー攻撃を受けた場合、警察機関との早急な対応が求められることから、日頃から、警察機関と情報共有を行い、「顔の見える関係」を構築している。また、警察機関から情報セキュリティの情報を収集している。
- 警察機関が開催している訓練に参加し、警察機関との連携体制や情報共有すべき情報の再確認を行っている。

■同じ分野内での情報共有

- 分野内の事業者等が情報共有できる環境を設け、情報セキュリティに関する情報を共有している。
- 日頃の業務を通じて、担当者間の「顔の見える関係」が構築されている。その結果、見ず知らずの人と情報共有をするという障壁が少なく、意見交換が活発に行われていると共に、インシデント発生時に利害関係なく、相談・協力がされている。



往訪調査結果（4/5）　内部・外部犯行対策について

【内部犯行対策（人的リスク対策）】 悪意のある従業員や外部委託事業者の作業者から重要システムを守っている。

- 適切な情報資産の管理や閲覧・使用権限の設定を行い、従業員が不正な作業ができない環境を構築している。
- 外部委託事業者の不正な作業を防止するため、外部委託契約内容に対策事項を明記し、発注事業者と外部委託事業者の双方で管理している。

■情報資産の管理

- 情報セキュリティとして管理すべき情報資産（電子データや情報システム等）を洗い出し、経営上の影響度合いや関係法令上の規則に応じて、情報資産の重要度を明文化している。さらに、情報資産の重要度に準じて、閲覧権限や使用権限を設けている。その結果、従業員による内部犯行や目的外使用等を抑止する環境を構築されている。
- 運用上、最低限の従業員に特権IDを付与すると共に、特権IDの取得者同士で定期的に相互監視を行い、特権者の不正を防止している。
- 定期的に情報資産や使用・閲覧権限、特権ID等の棚卸を行い、情報資産を管理する上で、漏れがないか確認する体制が規則化されている。

■重要システムに関わる作業ログの監視

- 事前に申請（計画）した作業以外の作業がされていないか、作業終了後に、作業内容や権限変更等の作業ログを確認している。

■外部委託事業者との外部委託契約

- 内部犯行対策として有効な事項を外部委託契約書に明記し、発注事業者と外部委託事業者の双方で内部犯行を防止している。
  （外部委託契約書に明記した内部犯行対策の例）
  ・重要システムに関わる申請外作業の禁止
  ・重要システムに関わる作業の単独作業禁止
  ・PCや外部記憶媒体の作業前セキュリティ更新プログラム（パッチ）の適用
  ・作業者の条件に情報セキュリティ教育受講を追加　等

■単独作業の禁止（作業監視者の配置）

- 重要システムに関する作業は、単独作業を禁止し、監視者を設けている。また、作業内容の事前確認を行い、悪意を持った作業の抑止や誤った作業を防止する体制が構築されている。
- 外部委託事業者のみの作業を禁止し、発注事業者が作業監視を行っている。

【外部犯行対策（物理的侵入防止策）】 重要インフラサービスの提供に係る重要な施設への物理的な侵入を防止している。

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）への施設出入り口に、監視カメラや侵入アラームを設置する対策や２要素認証対策の入退出管理システム等を設ける等の物理的侵入防止対策を設けている。

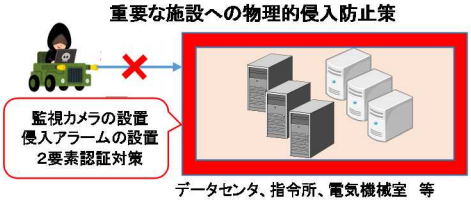
■監視カメラや侵入アラームの設置

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）の出入り口に監視カメラや侵入アラームを設置し、部外者の侵入防止と侵入された場合の早期発見ができる環境を設けている。

■　２要素認証対策の導入

- 重要インフラサービスの提供に係る重要な施設（データセンタ、指令所、電気機械室　等）への入退室には、記憶・所持・生体情報のいずれか２つ以上を用いた２要素認証を設け、部外者の侵入を防止している。

重要な施設への物理的侵入防止策



データセンタ、指令所、電気機械室　等

往訪調査結果（5/5）　システムの出入り口対策について

【ネットワーク侵入対策（出入り口対策）】 重要システムへの侵入防止対策や侵入検知対策を行っている。

- 重要システムのリスクアセスメントを実施し、外部から重要システムにサイバー攻撃ができる経路を洗い出し、その侵入経路に必要な対策を実施している。
- 重要システムにマルウェアや不正なアクセスが発生した場合に、早期に異常を検知するため、ネットワーク侵入検知対策を実施している。

■保守用PCや外部記憶媒体（USBメモリ等）

- 保守用PCや外部記憶媒体（USBメモリ等）の正規の目的使用以外の使用を禁止し、マルウェア感染等のリスクを低減させている。
- 保守用PCや外部記憶媒体の正規な目的使用は、管理者の承認を得てから使用するという運用を規則化し、万が一、マルウェア感染が発生した場合に感染経路を特定し、迅速な処置がされている。
- 保守用PCや外部記憶媒体の管理者および重要システムの管理者は、定期的かつ作業前に、セキュリティ更新プログラム（パッチ）を適用することを規則化させ、マルウェア感染等のリスクを低減させている。

■インターネット

- 従来、制御システムはクローズドな環境で運用してきたが、一部の制御システムの情報（発電情報、運行情報　等）をインターネット経由で公開する運用が求められるようになった。そこで、境界に片方向のゲートウェイ（データダイオード）を導入し、外部からの不正なアクセスを防止している。
- 不正なアプリケーションの実行や不審なウェブサイトへのアクセス制限させるため、ホワイトリストまたはブラックリスト型のFWを設けている。また、最新情報の収集を行い、必要に応じてFWの設定を更新している。

■メンテナンス回線

- メンテナンス（保守）用の回線は、一貫して自社で敷設・管理した信頼性の高い専用回線を用いている。
- 平時は、専用回線を接続しておらず、メンテナンスや異常時対応等の場合に限り接続するという運用ルールを用いている。インシデント発生時等のメンテナンス回線を接続する場合は、作業終了後に作業ログを確認し、不正な作業をおこなっていないか確認している。

■メールやファイルのダウンロード

- 外部から不審なメールを受信させないように、送信元や添付ファイル等を確認するシステムを導入している。
- 不審なデータやファイルをダウンロードしないように、ダウンロードするデータやファイル等に規制を設けている。

■ USBポートやLANポート

- 未使用のUSBポートやLANポートから情報の窃取やサイバー攻撃等を防ぐ対策を導入している。
  （未使用のUSBポートやLANポート対策の例）
  - ・空きポートを物理的に塞ぐ
  - ・承認されていない機器が接続されても検知させない
  - ・承認されていない機器が接続された場合、アラームを鳴動させる　等

■ IPSやIDS等のネットワーク監視機器の導入

- 不正なアクセスや挙動が発生した場合に、早期に不具合を発見するため、IPS※1やIDS※2等のネットワーク監視機器を導入している。また、24時間365日の体制で機器の監視を行うと共に異常時の連絡体制を整備し、十分な初動対応体制を構築している。

※1 IPS（Intrusion Prevention System）：侵入防止システム
※2 IDS（Intrusion Detection System）：侵入検知システム

別添４－６　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	FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
重要インフラ事業者等からNISCへの情報連絡(※)	401	856	388	69	50	60	44	223
関係省庁・関係機関からのNISCへの情報共有	52	41	19	0	1	3	3	7
NISCからの情報提供	44	80	54	7	17	8	11	43

※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			FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
未発生の事象		予兆・ヒヤリハット	75	330	80	7	8	8	4	27
発生した事象	機密性を脅かす事象	情報の漏えい	15	30	15	4	4	2	3	13
	完全性を脅かす事象	情報の破壊	52	47	20	5	7	3	2	17
	可用性を脅かす事象	システム等の利用困難	86	80	143	21	20	29	27	97
	上記につながる事象	マルウェア等の感染	111	289	65	9	2	4	2	17
		不正コード等の実行	11	10	13	2	1	0	1	4
		システム等への侵入	27	26	17	6	1	3	4	14
		その他	24	44	35	15	7	11	1	34

※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		FY27 計	FY28 計	FY29 計	FY30 1Q	FY30 2Q	FY30 3Q	FY30 4Q	FY30 計
意図的な原因	不審メール等の受信	83	546	89	16	5	9	6	36
	ユーザＩＤ等の偽り	8	1	4	2	1	0	0	3
	DoS攻撃等の大量アクセス	47	23	31	6	4	5	2	17
	情報の不正取得	8	14	16	2	5	1	2	10
	内部不正	2	0	4	1	0	0	0	1
	適切なシステム等運用の未実施	10	19	15	4	1	7	2	14
偶発的な原因	ユーザの操作ミス	10	15	23	4	1	4	1	10
	ユーザの管理ミス	5	8	13	5	0	1	0	6
	不審なファイルの実行	51	243	42	10	5	1	0	16
	不審なサイトの閲覧	49	29	20	1	1	1	1	4
	外部委託先の管理ミス	12	20	41	11	9	5	4	29
	機器等の故障	17	22	32	8	8	7	4	27
	システムの脆弱性	29	56	36	7	6	5	1	19
	他分野の障害からの波及	5	0	10	2	0	1	3	6
環境的な原因	災害や疾病等	0	0	0	0	0	1	0	1
その他の原因	その他	22	34	29	6	7	8	8	29
	不明	105	92	57	10	9	14	13	46

別添４－７　セプター概要

セプター及びセプターカウンシルの概要

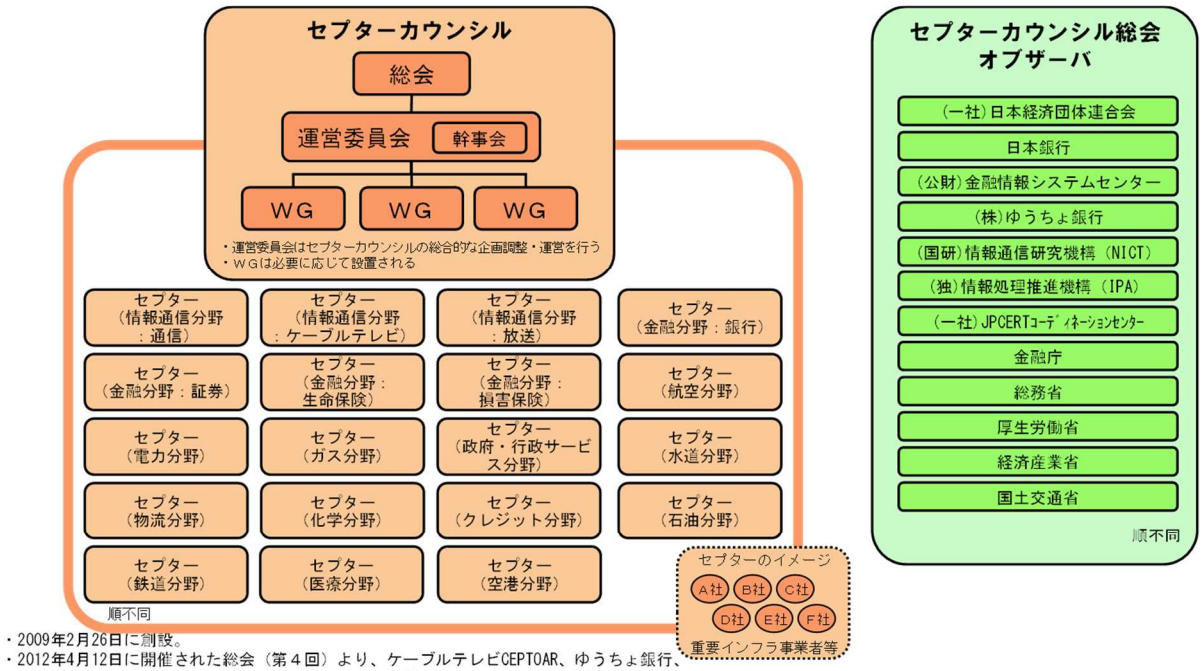
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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（2019 年４月 23 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

2019年3月末日現在

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信	放送		銀行等	証券	生命保険	損害保険		航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会 銀行等CEPTOAR	金融CEPTOAR連絡協議会 証券CEPTOAR	金融CEPTOAR連絡協議会 生命保険CEPTOAR	金融CEPTOAR連絡協議会 損害保険CEPTOAR		航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 IT統括部	(一社)生命保険協会 総務部経営企画・法務グループ	(一社)日本損害保険協会 IT推進部品質管理グループ		定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術ユニット	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^数）	23社1団体	335社1団体	197社・団体	1,386社	269社7機関	41社	46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18機関	8水道事業体	6団体17社	13社	51社	12社
NISCからの情報の展開先（構成員以外）	407社・団体	411社	12社	3社・団体	—	—	—		—	—	—	14社・機関	182社・団体	—	379社	内容に応じ1,343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））

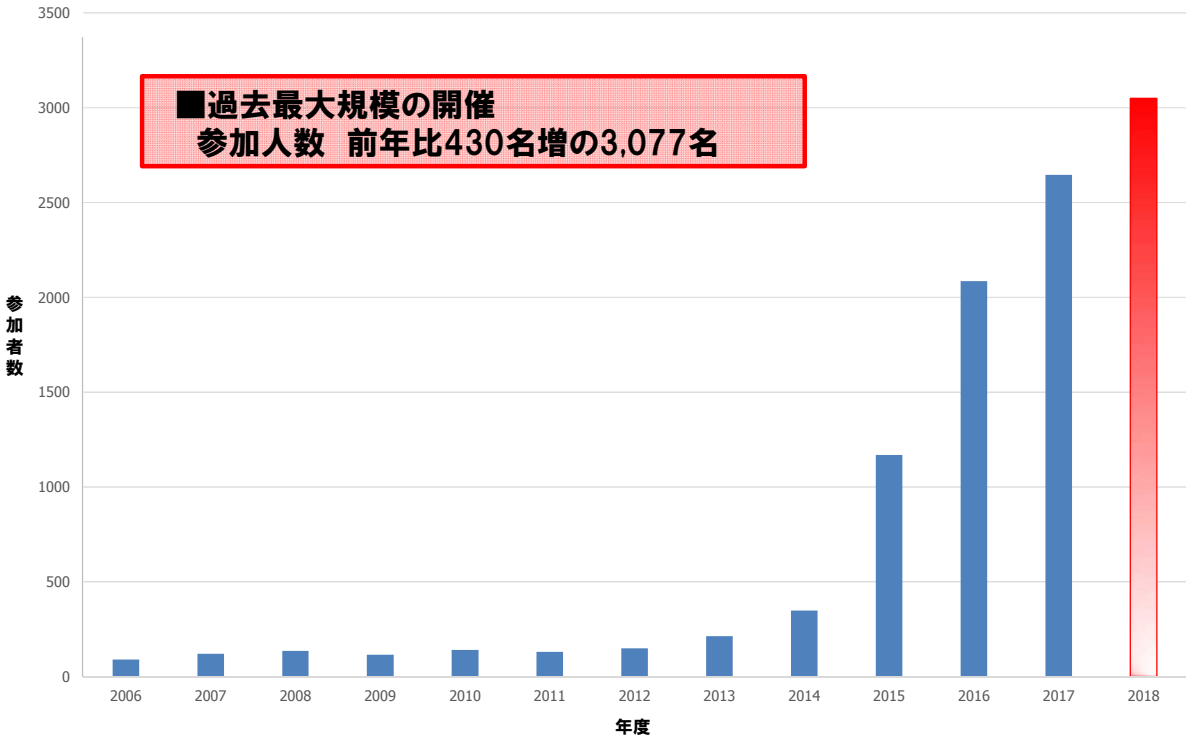
■ その他

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への拡張）、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４－８　分野横断的演習

分野横断的演習の参加者数の推移



2018 年度の取り組み

- より実践的な演習機会の提供
  - 実時間に近い時間軸の検討
  - 実環境に即した個別シナリオの検討
    （サブコントローラーへの支援の充実）
  - オリパラへの対応
  - 国際・地域的な視点の考慮
- 自職場参加の推進
  - 自職場参加者への説明の充実
  - 自職場参加者を意識したシナリオの準備
  - 経営層への理解浸透
- 重要インフラ全体での防護能力の底上げ
  - 参加が少ない業界の参加推進
    （場所、実施日程等の検討）
  - セプター事務局向け説明の充実
  - 第4次行動計画に基づく情報共有体制に関する理解の増進
  - ベンチマークの作成
- 情報共有体制の実効性の向上
  - 「普段やっていることを検証する」だけでなく「(必ずしも普段できていなくても)やるべきことをしっかり実行するための契機となる」演習へ
  - 事業者等が常用するツール等を意識した演習の検討

2018 年度分野横断的演習　開催実績

＜事前説明会＞
日　程　：２０１８年１０月２３日（火）、２５日（木）、２６日（金）、３０日（火）
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：２０１８年１２月１３日（木）１３：００～１７：００
場　所：東京会場、大阪会場、福岡会場、自職場
参 加 者：３，０７７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】

演習の模様

櫻田大臣による挨拶

演習内容：
【第1部】インシデント初動対応に重点を置く（重要インフラサービスに影響なし）
犯行声明からのサイバー攻撃情報共有体制、レピュテーションリスクへの対応を重点とする
【第2部】インシデント初動対応に加え、重要インフラサービス障害等への対応（重要インフラサービスに影響あり）
サイバー攻撃による重要インフラサービスへの影響障害対応体制、内部的な判断、意思決定、インシデントの本格対応を重点とする。

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1月２２日（火）１３：３０～１６：３０
場　所：東京会場、大阪会場、福岡会場
内　容：①組織間での情報共有（テーマに応じたグループディスカッション）
②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

2019 年度の主な取組方針

【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
・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

【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】

・NISCおよ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、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）
・さらなる自職場参加の推進

別添４－９　セプター訓練

セプター訓練（第 13 回）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」で、内閣官房が定期的及びセプターの求めに応じてセプターの情報疎通機能の確認等の機会を提供する取組として位置付けられている。

他の演習・訓練との関連性に留意しつつ、各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の情報共有体制を強化し、官民連携による重要インフラ防護の維持・向上を図る。

＜目的＞

✓ 関係主体間における情報疎通機能の確認を通じた 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、2,005者

＜実施期間＞

2018年8月から10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、自社への被害状況（≒受信確認）をセプター事務局又は所管省庁へ報告
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

セプター訓練（第 13 回）の特徴

1．多数の事業者による参画

✓ 全てのセプターが参画し、2,005者が訓練に参加（2017年度参加実績2,106者）

2．実施結果及び訓練により得られた気づき等

✓ 2017年度の結果と比較し訓練情報の受信確認の割合が低下（全体94%→89%）
- 9セプターにて、2017年度より受信確認割合が低下した。
- 受信確認割合100%は、2017年度12セプターに対して、2018年度は8セプターであった。

✓ 訓練を通じて新たな課題や気付き等を認識
- 連絡先の複数登録や、メール・FAX・電話等による伝達手段の多様化。
- 事業者-セプター事務局間の連絡フォーマットの周知・浸透および改良。
- 定期的な登録状況点検（メール送達確認）の実施等による、連絡先担当者の確実な最新化。

受診確認割合が低下したセプターには、特に課題や気付きを基にした対策を図る必要がある。

別添４－10　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）

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、2018年1月1日～2018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

2018 年度　調査対象事例　概要

- **“外部事業者のサービス障害に起因した重要インフラサービス障害”**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2018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
外部事業者のサービス障害に起因した重要インフラサービス障害			
1	インターネットサービス利用時の認証の障害	インターネットを通じて提供される重要インフラサービスで、利用者を認証する機能に障害が発生し、一部サービスが使用できなくなった。	外部サービス（クラウド型認証サービス）の障害
2	重要インフラ事業者間での映像データ送受信の中断	重要インフラサービスとして提供する予定の映像を予定時刻に送受信できず、利用者に提供できなくなった。	外部サービス（通信回線）の障害
3	重要インフラサービスの受付業務の遅延	利用者の受付業務に支障が発生し、重要インフラサービスの提供が遅延した。	外部サービス（顧客受付システムを共同利用するための共通ネットワーク）の障害
外部からのサイバー攻撃			
4	IoTデバイスへの不正侵入及び改ざん	第三者にネットワークカメラ等に不正に侵入・改ざんされ、施設等の監視に支障が発生した。	第三者が類推可能な認証情報（ID/パスワード）の悪用
5	脆弱性を悪用した攻撃	クラウド基盤のネットワーク機器が機能停止し、基盤上の業務システムが使用できなくなった。	ネットワーク機器の脆弱性を悪用した攻撃
6	広域DoS攻撃によるWebサイト閲覧障害	ある分野の複数の重要インフラ事業者等のWebサイトが閲覧できなくなった。	Webサイトに対するDoS攻撃
重要インフラ事業者内でのインシデント			
7	商用ネットワークの高負荷による通信障害	商用ネットワーク全体が高負荷となり、特にDNSサーバからの応答が滞ったことで、顧客のインターネット接続に支障が発生した。	商用ネットワーク内のネットワーク機器の不具合によるトラフィックの異常増加
8	他人の認証情報の悪用による情報の不正取得	本来、閲覧権限のない機微情報を不正に利用された。	従業員による他人の認証情報（ID/パスワード）の不正利用

得られた気付き・教訓　概要（各事案に共通する事項）

外部事業者に起因した重要インフラサービス障害事例（No. 1, 2, 3）から

- セキュリティ対策やリスクマネジメントに日々積極的に取り組んでいる先導的な重要インフラ事業者であっても、外部事業者のサービス障害に起因したサービス障害への対応を経て、**重要インフラ設備の一部を外部事業者に依存してサービスを提供する際のリスク**が再認識されている。重要インフラ事業者側で取り得る対策としては以下が挙げられる。他事業者においても参考とすることが期待される。
  - 外部事業者のサービスが中断した場合の、自組織への影響を再度評価する。
  - 特定の外部事業者のみに依存しない、多様性のある設備を自組織側で確保する。
  - （事業上の制約で多様性のある設備が確保できない場合、）重要な業務については、外部事業者のサービスの復旧までの間、自組織側で実行可能なコンティンジェンシープランの整備や更なる効率化を図る。
  - 外部事業者との緊急連絡体制の整備は必須であるが、外部事業者側の現場の対応状況を直接確認できる連絡体制がより望まれる。緊急時の連絡の場合は、中継のみのために介在する組織/担当者をできる限り減らすなど、連絡体制を効率化する。
  - 自組織内の各部署/各担当者が有事における自身の役割を理解し、能動的に動けるレベルを目指して訓練を行う。

外部からのサイバー攻撃への対応事例（No. 4, 5, 6）から

- 情報セキュリティの専任の担当者がいない/少ない事業者においては、担当者の稼働やスキルの不足、予算の不足等により、既知のリスクへの対策が十分に行うことができず、事案への対応の進め方にも窮する場合がある。この際、**事業上の関係がある組織や情報セキュリティ関係機関等からの助言により事態が好転したケース**が複数の重要インフラ事業者で確認されている。しかしながら、事案に対応した多くの担当者によれば、「緊急時には、平時から関係のある信頼できる組織や担当者に対してでなければ、そもそも相談しようという発想が出てこない」という。情報共有の体制や訓練への参加は重要であるが、参加するだけでなく、**平時からの実体のあるコミュニケーション**が有事の際に重要となる。

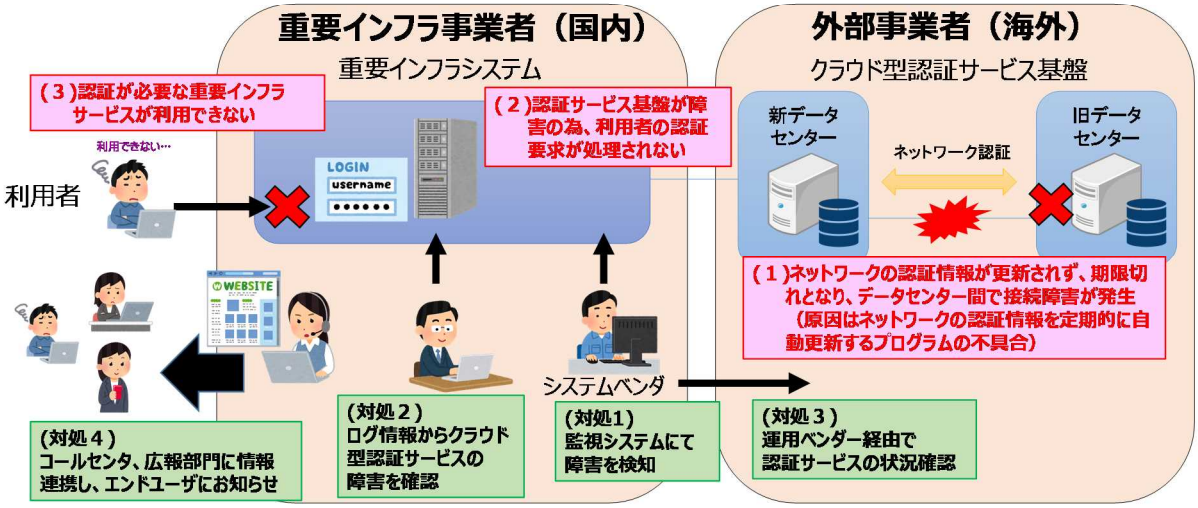
重要インフラ事業者内で発生した事案への対応事例（No. 7, 8）から

- 機器の故障等、偶発的な要因で発生する障害は、完全に防止することは困難であるが、事業上重要なシステム/サービスについては、各分野の安全指針等を参考に、迅速に対処・復旧するための対策を**設計段階から検討する**必要がある。
- 従業員による不正等、人為的に発生する要因は、自組織で扱う情報の重要性等も考慮し、セキュリティリスクについて、システム面、運用面のアプローチで低減するとともに、**実行動機の抑止に繋がる対策**についても従業員への研修等、教育面のアプローチを検討する必要がある。

※　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　インターネットサービス利用時の認証の障害

- インターネットを通じて提供される重要インフラサービスにおいて、利用時に認証が必要な一部のサービスが利用できなくなる事象が発生。
- 原因は、利用者の認証に使用している外部事業者のクラウド型認証サービスの障害。当該外部事業者では、データセンターの移行のために新旧データセンターを暫定のネットワークで接続しており、そのセキュリティ強化のためにネットワーク認証を導入していたが、認証情報の有効期限が切れたことにより、通信断が発生。
- 恒久対策として、特定の外部事業者１社のサービスに依存しないよう、複数の認証方法の導入を検討。



【１　背景】

- インターネットを通じて提供される重要インフラサービスにおいて、利用者の認証に外部事業者（海外）のクラウド型認証サービスを採用していた。
- 外部事業者では、クラウド認証サービスの基盤があるデータセンターの移行を進めており、新旧データセンター間を暫定ネットワークで接続し、セキュリティ強化の為にネットワーク認証を導入していた。

【２　検知】

- 監視システムにてクラウド型認証サービスの異常を検知。
- 障害発生直後からコールセンターに多数の問い合わせ。

【３　対処】

- 重要インフラシステム側のログのエラー情報から、クラウド型認証サービスでの障害であることを特定。
- システムベンダ経由で、外部事業者から障害に関する調査・対応状況を収集し、テレビ会議で利用者対応部門（広報、コールセンター等）にリアルタイムに共有。
- 外部事業者による復旧までの間、ホームページとコールセンターを通じて、復旧状況を利用者に逐一提供。

【４　原因】

- ネットワーク認証の認証情報の有効期限切れにより、新旧データセンター間の接続に障害が発生した結果、旧データセンター側のシステムに登録されていた利用者情報との照合ができなくなった。
- ネットワーク認証の認証情報は自動で更新される仕組みであったがプログラムの不具合により更新されなかった。

【５　再発に備えた対策】

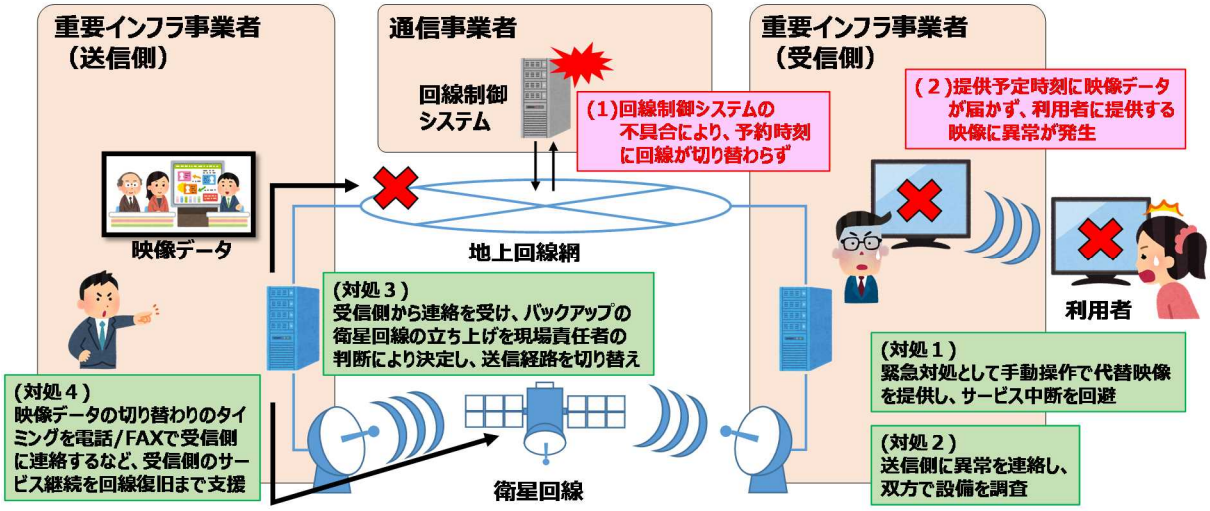
- 重要インフラサービス側の認証機能の多様化や代替手段の導入を検討し、特定１社への依存を解消。
- 外部事業者の現地の運用者とのホットラインを構築し、日本法人を経由する連絡体制で生じる時間ロスを解消。

【６　得られた気付き・教訓】

- **自力でのサービス継続のための代替手段の必要性**
  外部事業者による利用者認証サービスを利用していたが、その障害時に自組織側で発動できる代替手段がなく、外部事業者による復旧を待たざるを得なかった。自力でのサービス継続のため、利用者への代替の認証手段を用意しておくべきであった。
- **有事を想定した利用者対応訓練の効果**
  重要インフラサービスの障害では利用者からの問い合わせが急増するが、有事の情報公開についてシステム部門と利用者対応部門で定期的に訓練を実施しており、混乱なく対応できた。
- **外部事業者との緊急時の連絡体制整備**
  海外の外部事業者という事もあり、連絡ルートにシステムベンダや日本法人が介在しているため、復旧状況の把握に時間がかかった。本件を受け、経営幹部が主体的に交渉に動き、現地の運用者と直接連絡が取れるホットラインを構築した。
- **海外サービス利用時の現地時差**
  海外のサービスを利用する場合、メンテナンス等が相手国の深夜時間帯に実施されると日本時間で業務時間帯にあたることもあることから、サービス提供側の国と利用者側の国との時差によるリスクの見直しを行った。

事例２　重要インフラ事業者間での映像データ送受信の中断

- 重要インフラ事業者間で映像データの送受信に使用している回線が、予約日時に切り替わらず、接続障害が発生し、受信側の重要インフラ事業者では予定の映像を利用者に提供できなくなった。
- 回線が切り替わらなかった原因は、回線を提供している通信事業者の回線制御システムの不具合。
- 通信事業者の回線網は冗長化されているため、回線起因の障害は当該重要インフラ事業者では前例が無かったが、「サービス（映像の提供）の継続を最優先に行動」という共通の対応方針の下、衛星回線経由のルートに切り替え、迅速に復旧。



【１　背景】

- 重要インフラ事業者間で、サービスに使用する映像データを送受信する際、通信事業者の回線を利用している。
- 回線は、通信事業者の回線制御システムに使用時間帯を予約設定することで時間帯毎に切り替わる仕組み。

【２　検知】

- 受信側の重要インフラ事業者のオペレーターが、映像提供予定時刻に映像データが届いていないことを発見。同時に、受信側の重要インフラ事業者では利用者に提供する映像に異常が発生。
- 送信側の重要インフラ事業者は、受信側からの連絡により、映像データが正常に届いていないことを認識。

【３　対処】

- 回線制御システムの予約含め、重要インフラ事業者側の操作ミスや設備不具合を調査したが、該当無し。
- 重要インフラ事業者から通信事業者に問い合わせたが、原因・復旧共に不明との回答。
- 送信側で、別の通信事業者が提供するバックアップ用の衛星回線への切り替えを決定し、送信のタイミング等を連絡。
- 受信側は、通信事業者の回線の復旧までの約30分間、手動操作によりサービスを継続。

【４　原因】

- 通信事業者の回線制御システムのソフトウェア不具合。（通信事業者内でも回線は冗長化されていたが、制御するソフトウェア側の不具合のため機能せず）

【５　再発に備えた対策】

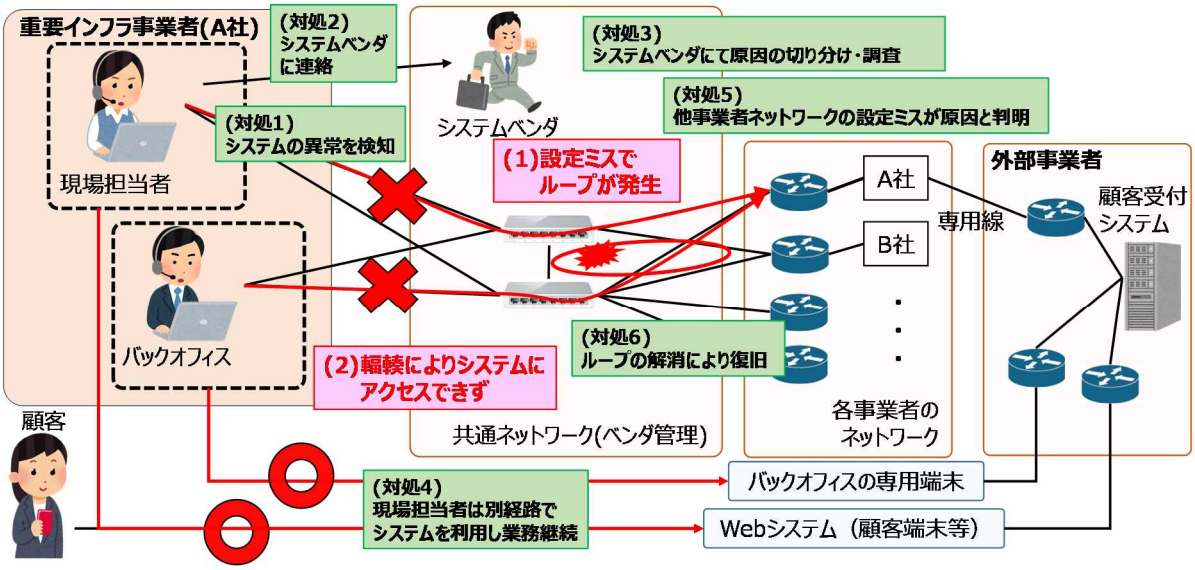
- 回線制御システムの不具合の解消（通信事業者にて実施）。
- 通信事業者に対する、異常発生時の迅速な情報提供の依頼。
- 緊急時対応プロセスの更なる効率化による有事の切り替え時間短縮、及びオペレーター全員への定期訓練等による手順の浸透。
- 自組織全体、及び同じ分野の重要インフラ事業者への事例共有による、分野内での類似事案への対処能力の強化。

【６　得られた気付き・教訓】

- **事業継続を最優先として動く組織のマインド**
  事業継続のために優先すべき対応がオペレーションの現場まで浸透し、かつ判断の権限を持っていることが、迷いのない迅速な対処に繋がった。
- **日常的な障害対応訓練**
  コンティンジェンシープラン等を整備するだけでなく、日常的に障害対応訓練を行っており、誰が対応することになっても判断し対応できるレベルまで緊急時のオペレーションが成熟していた。
- **依存度の高い外部サービスの障害に備えた対策**
  経営上重要な事業に使用している外部事業者のサービスで障害が発生する事態に備え、代替の外部サービスを確保していたことが、復旧時間の短縮に大きく寄与した。
- **他事業者任せにしない再発防止**
  障害の直接原因は他事業者であったが、そのような場合に備えた自組織側の対応プロセスについても見直した。

事例３　重要インフラサービスの受付業務の遅延

- 複数の事業者が利用する顧客受付システムを接続する共通ネットワークにおいて、ある事業者の設定ミスによりループが発生。ネットワーク全体が輻輳し、複数の事業者が当該システムを利用できなくなった。
- 現場担当者は、別の経路を利用して顧客受付システムに接続し、業務を継続。
- 恒久対策として、システムベンダでネットワーク機器の交換および障害検知のためのログ監視ツールを導入。



【１　背景】

- 複数事業者が利用する顧客受付システムのネットワークに、個々の重要インフラ事業者が管理する部分と、複数事業者が利用する部分（共通ネットワーク）がある。
- 共通ネットワークについては、システムベンダに保守を委託している。

【２　検知】

- 重要インフラ事業者の現場担当者が、当該システムが利用できなくなっている状態を検知した。

【３　対処】

- 現場担当者は、まずシステムベンダに連絡し、ネットワークベンダにて原因の切り分け作業を行った。
- 切り分け作業の結果を元に、システムベンダにて調査を開始した。
- 経路のループの箇所を特定し、設定を修正することでネットワークを正常化した。
- 顧客受付システムは別のネットワーク上に設置されていたため、現場担当者はインターネット経由、もしくはバックオフィスの専用端末で当該システムに接続することで顧客の受付業務を継続した。

【４　原因】

- 共通ネットワークに接続する他事業者の作業ミスで、当該事業者と共通ネットワークとの間でループが発生した。
- 共通ネットワークが輻輳し、接続された複数の事業者において、顧客受付システムが利用不可となった。

【５　再発に備えた対策】

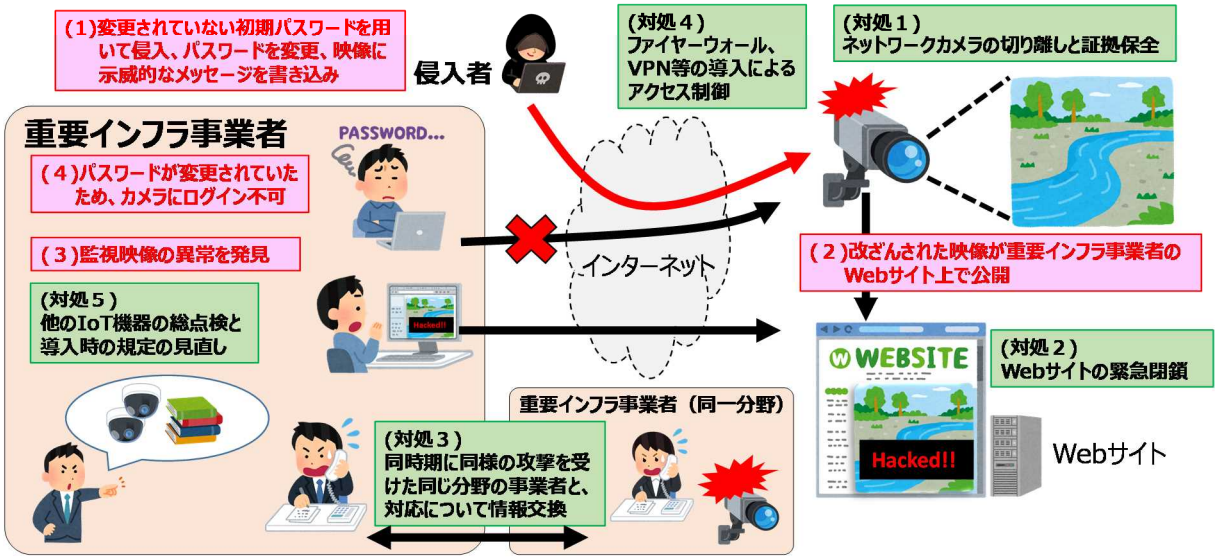
- システムベンダにおいてループが発生しないネットワーク機器および障害検知のためのログ監視ツールを導入。
- 対処に時間がかかったことへの対策として、委託先のシステムベンダの保守体制（緊急時の情報伝達経路等）の見直しを依頼。
- 顧客受付システムを利用する事業者間で事例を共有。

【６　得られた気付き・教訓】

- **外部サービスでの障害に備えた自組織側での対応訓練**
  SLAを厳しくする、抜け漏れがないようにRFPに記載する等の対策を行っていても、外部サービスの障害を完全に防ぐことは困難である。外部サービスが利用不可となったことを想定し、日頃から訓練を行っていると、システムが利用できなくても業務を継続できると考えられる。
- **委託先との連絡体制整備**
  対処に時間がかかった原因の一つとして、「委託先の情報伝達がしっかりしていなかった」、「対処方針を示す指示役（旗振り役）がいなかった」といった点が挙げられる。緊急時における委託先との情報伝達経路を整備するとともに、委託先における体制についても把握しておくことが重要である。
- **同一システムを利用する間での事例の共有**
  本事案は、ある事業者の設定ミスが他事業者に波及したという事例であり、利用者側でシステムや対応の改善のみで完全に防ぐことは困難である。同様の事案を起こさないように、関係する事業者間で事例の共有を行うと良い。

事例４　IoT デバイスへの不正侵入及び改ざん

- 重要インフラ事業者が管理する施設情報の監視に使用していたネットワークカメラが外部から侵入され、管理ログインができなくなる、映像が改ざんされる、などの被害が複数の分野で発生した。
- 侵入された原因は、第三者が容易に類推できるパスワードや、アクセス制御の不備。
- 今回の件を受け、ネットワークに接続するIoT機器のパスワード設定やファイヤーウォール等でのアクセス制御の総点検を行ったほか、導入時のセキュリティ上の考慮事項を内規に盛り込んだ。



【１　背景】

- 重要インフラ事業者の施設情報の監視・公開を目的として、ネットワークカメラを設置し、映像をWebサイトで公開。

【２　検知】

- 施設の映像を確認するためにアクセスした従業員が、複数のカメラの映像内に不審なメッセージを発見。
- ネットワークカメラのパスワードが侵入者により変更され、管理画面にログインできなくなっていた。
- 他の事業者でもネットワークカメラに対し、同様の不正侵入が確認され、メーカーから注意喚起が発出された。

【３　対処】

- Webサイトでの監視映像の公開を停止し、当該カメラに対する外部からの直接アクセスも制限。
- 当該重要インフラ事業者が保有している全てのIoT機器の状況を調査。念のためパスワードを全て変更。
- 対応方針について、同時期に同様の攻撃を受けた同じ分野の事業者と情報交換、外部の調査機関にも相談。
- 侵入された機器をネットワークから切り離したうえで、ログ等の痕跡を保全するため電源は維持し、外部の調査機関立ち合いのもと、調査。１日分のログしか残らない設定となっていたため、侵入元特定には至らず。
- Webサイト閉鎖中の代替措置として、従業員による目視で施設の監視を行い、状況をWebサイトやTwitterを通じて利用者に逐一伝達。
- 代替機器を手配し、監視映像の公開を再開。

【４　原因】

- ネットワークカメラのパスワード設定は、導入時、事業者と機器設置業者のいずれでも検討されず、初期設定のまま運用されていた。
- ネットワークカメラへの直接アクセスによる閲覧は許可する予定はなかったが、特にアクセス制限を行っていなかった。

【５　再発に備えた対策】

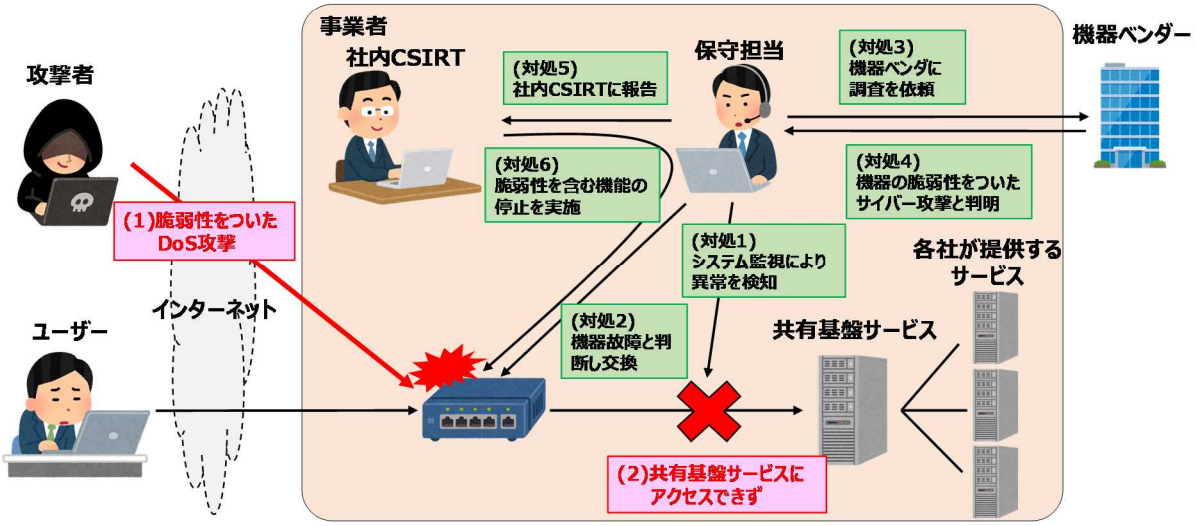
- IoT機器のセキュリティ設定やログの取得・保存期間に関して、導入時および運用時の手順を見直し、利用部門への研修も企画。
- IoT機器を調達する際の検討事項として、認証やアクセス制御等のセキュリティ機能の観点を追加。
- ネットワークカメラへのアクセスはVPN経由のもののみ許可するようにし、外部からアクセスできないようにネットワークを構成変更。

【６　得られた気付き・教訓】

- **IoT機器を悪用されるリスクの認識**
  IoT機器の初期パスワードは、公開されているマニュアル等を通じて誰でも容易に知り得ることを認識し、悪用されないように導入時に必ずパスワードを変更する。メーカーが発信する脅威情報にも注意し、注意喚起等が行われた場合は、自組織の利用形態におけるリスクを点検し対応の要否を検討する。
- **同様の攻撃を受けた事業者との情報交換の有用性**
  同時期に他の事業者でも同様の攻撃を受けたことを知っていたため、攻撃手口や対応方法等について当該事業者と情報交換しながら対応を進めることができ、平時から互いに相談できる関係作りの重要性を認識した。

事例５　脆弱性を悪用した攻撃

- ネットワーク機器の脆弱性をついたDoS攻撃により、複数のWeb上のサービスが停止した。
- 当初はシステム障害として対応したが、ベンダに調査を依頼したところ、ネットワーク機器の特定の機能に含まれる脆弱性をついたサイバー攻撃が原因だと判明し、社内CSIRT部門に報告した。
- 脆弱性を含む機能の停止、及びファームウェアのバージョンアップを実施した。



【１　背景】

- 事案発生の数日前、当該脆弱性を利用した攻撃があったという情報をつかんだ。
- 該当機器には、情報をつかんだ10日後の、月次メンテナンスの日にパッチを適用する予定であった。

【２　検知】

- システム監視にて検知し、保守担当にて確認した。
- ネットワーク機器のステータスランプが点滅状態（正常時は点灯）になっていたため、ハード故障と判断し対応した。

【３　対処】

- ネットワークから該当機器を切り離しバックアップ用の機器で運用し、翌日には該当機器を交換した。
- ベンダーにて該当機器のログ等を調査したところ、ネットワーク機器の特定の機能の脆弱性をついたサイバー攻撃が原因と報告があり、社内CSIRTに報告した。
- 脆弱性を含む機能を停止し、ファームウェアをバージョンアップした。

【４　原因】

- ネットワーク機器の特定の機能の脆弱性をついた攻撃が原因であった。
- 該当機器では、アクセス制限を使用機能に応じたプロトコルとIPアドレスで実施していたが、本脆弱性がある機能に気がつかず、アクセスが可能な状態になっていた。

【５　再発に備えた対策】

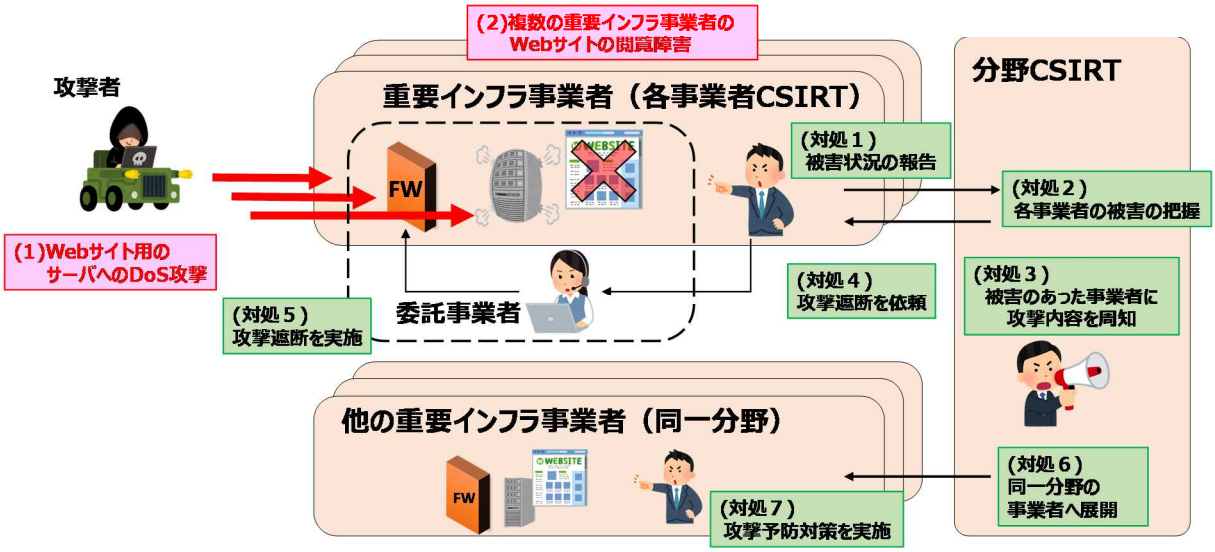
- 本内容を社内、グループ会社で共有した。
- 普段使用しない機能の脆弱性をついた攻撃であったことから、他にも各ネットワーク機器で動作中の機能を確認し、不要な機能を停止した。
- ネットワーク機器への脆弱性が出た場合は、検証環境にて対象かどうかの確認を行う、診断ツールが利用できる場合は使用する等、社内ルールを変更した。
- サイバー攻撃に関する勉強会を定期的に実施することとした。

【６　得られた気付き・教訓】

- **脆弱性へのパッチ適用の判断**
  月次メンテナンスでパッチを適用するまでの間に攻撃を受けた。ネットワーク機器の脆弱性が公表された場合に、対応要否を迅速に見極めるために、検証環境にて影響有無の確認を行う、診断ツールが利用できる場合は利用するなど、運用を見直した。
- **報告用フォーマットの改善**
  最初からサイバー攻撃である可能性も視野に入れて対応できるよう、責任者への報告用フォーマットにサイバー攻撃が疑われる場合のチェックポイントを組み込んだ。
- **セキュリティリテラシーの底上げ**
  一部のセクションでは診断ツールでチェックができていたなど、部署ごとの対応にばらつきがあった。サイバー攻撃に関する勉強会等によりセキュリティリテラシーの底上げを図った。

事例６　広域 DoS 攻撃による Web サイト閲覧障害

- ある分野の広範囲の重要インフラ事業者にDoS攻撃があり、運営しているWebサイトが閲覧できなくなった。
- 異常を察知した重要インフラ事業者が、当該分野の全体調整を行っている分野CSIRTに報告した。
- 報告により得られた内容から原因を特定し、被害を受けている事業者に攻撃元等の情報を展開することで、事態の収束を図った。また、被害を受けていなかった同一分野の重要インフラ事業者にも攻撃元等の情報を共有し、セキュリティインシデントの抑止に繋げた。



【１　背景】

- 複数の重要インフラ事業者において、Webサイトの運用を同一の事業者に委託していた。

【２　検知】

- Webサイト運用担当者が、Webサイトの表示が不安定であることに気づいた。
- 外部機関からも「攻撃を受けているのではないか」、という指摘があった。

【３　対処】

- インシデントハンドリングを実施することとなっている事業者に状況を報告し、関係する事業者全体の被害状況を把握した。
- 取りまとめられた状況から、攻撃元IPアドレス等の詳細な攻撃情報を関係事業者全体に周知した。
- 委託事業者にWebサイト運用サーバへの攻撃を遮断するよう指示した。

【４　原因】

- 委託先運用のサーバへのDoS攻撃

【５　再発に備えた対策】

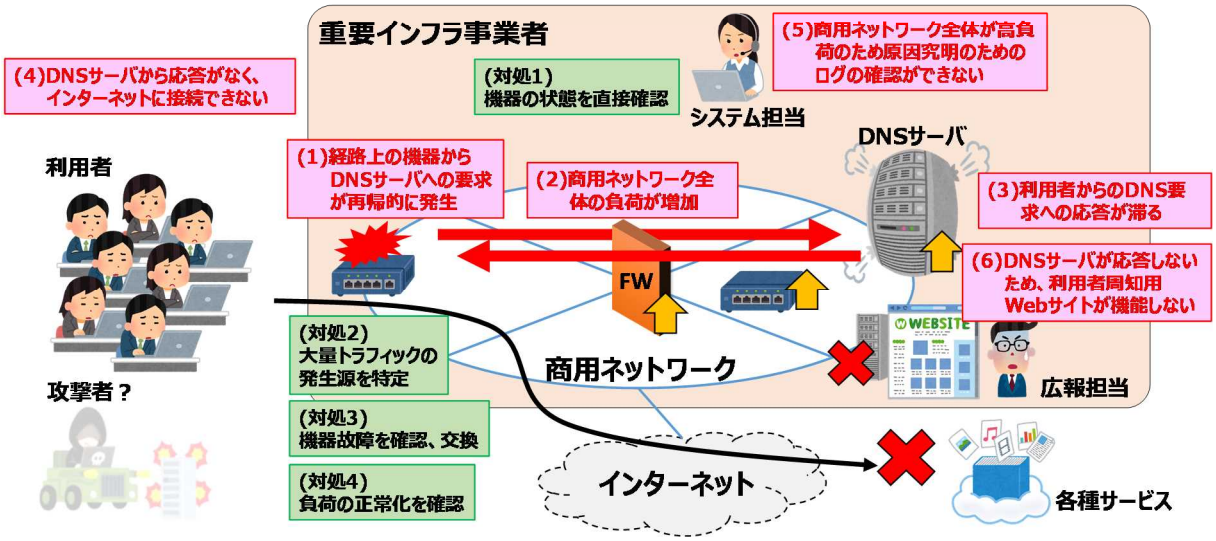
- 委託先事業者に指示し、関係事業者を防護しているファイアウォールに攻撃元と考えられるIPアドレスをリスト登録した。
- 早期に情報共有できる体制を構築し、サイバー攻撃があった際、関係する事業者に素早く展開できるよう、共有体制の見直しを行った。

【６　得られた気付き・教訓】

- **組織間の情報共有体制の構築**
  平時から関係する組織間で情報を共有し、連絡先を認識(顔の見える関係の構築)しておくことで、広範囲にわたるサイバー攻撃が発生した際に、スムーズな情報連携が確立でき、早期に事態を収束することが可能となると考えられる。
- **自組織でのサイバーセキュリティの専門人材の登用・育成**
  システムやセキュリティの運用を外部委託している場合でも、有事の際に状況の正確な認識、事態への円滑な対処等を統制しながら進めることのできるサイバーセキュリティの専門人材は、自組織側でも確保する必要があることを認識した。専門人材の採用や自組織内での育成を、費用面等の制約条件も考慮して検討する。また、希望すれば専門人材としてのキャリアパスが選択できるような仕組みも検討する。
- **サイバー攻撃への対応ノウハウの定着**
  今回のサイバー攻撃への対応において、専用のマニュアルは存在していなかったが、攻撃を受けたシステムの運用監視を長期間行っていた、スキルのある担当者により、苦慮しつつも対応を行うことができた。今後はこの対応を組織として形式知化し他の担当者にも展開し、組織的に対応できるよう対策を行う。
- **DoS攻撃への対策**
  自組織の事業上、重要なサーバについては、ある程度の瞬発的なアクセス増加に耐え得るサーバリソースの設計や、通信量のモニタリング、特定IPからのアクセスの制限方法の導入等の対策を講じる。

事例７　商用ネットワークの高負荷による通信障害

- DNSサーバに通常の数十倍以上の大量のアクセスがあり、DNSサーバからの応答ができなくなったことで、利用者がインターネットに接続できなくなった。DNSサーバへのDoS攻撃の可能性も視野に入れ、調査を実施。
- 原因は、経路上のネットワーク機器とDNSサーバ間で大量のトラフィックが発生し、DNSサーバにアクセスしづらいなどの影響が発生したことによるもの。当該DNSサーバと同一セグメントにあるメールサーバ等への接続にも影響が出たほか、機器監視も同一セグメントで行っていたため、ログが追えない状態となった。
- 今後に備えた対策として、監視用の専用ネットワークの整備や帯域制御などの設計の見直しを行った。



【１　背景】

- 利用者にインターネット接続サービスを提供していた。
- 機器の監視は、商用ネットワークで実施していた。
- 商用ネットワークは帯域制御しておらず、異常トラフィックを考慮した設計となっていなかった。

【２　検知】

- 利用者から、「インターネットに接続できない」という問い合わせがあった。
- 商用ネットワークの状況を確認するために、機器にアクセスしたが、輻輳が発生しており、確認できなかった。

【３　対処】

- 現地で直接各ネットワーク機器の通信状況を確認した。
- 通信内容から、特定の機器間で通信が再送され続けていることを確認。サイバー攻撃の可能性も考慮し、対応を実施した。
- 当該機器を再起動し、輻輳が正常化したことを確認後、機器を交換した。

【４　原因】

- 当該機器の一部ポートにおけるソフトウェアエラーにより、再帰的にリクエストが発生した。

【５　再発に備えた対策】

- 輻輳によるネットワーク機器のリソース逼迫も誘発していたため、帯域制御を実施した。
- 商用ネットワークの障害時にも状態把握が可能となるよう、監視専用のネットワークを別途構築し、監視方法を変更した。
- 利用者への周知方法として、自組織のWebサイトを利用する以外に、SNSの公式アカウントを取得し、周知方法を増やした。

【６　得られた気付き・教訓】

- **障害に強いネットワーク設計の重要性**
  ネットワーク機器の監視用のネットワークと、商用ネットワークを分離して整備することで、商用ネットワークで障害が発生してもネットワーク機器の状態をリアルタイムに確認でき、原因の切り分けがより迅速になる。監視用ネットワークと商用ネットワークを分けておくことが重要である。
  DNSサーバ等、サービス提供上重要なサーバは、経路の異なる別セグメントに分散して配置するなどを設計段階で検討しておくことで、サービス提供の強靭性を向上できる。設計段階からの障害対策が重要である。
- **通信帯域の制限**
  通信帯域の制限により、ネットワーク機器のリソース逼迫を回避できることに加え、閾値超過時の早期異常検知にも役立つ。
- **周知方法の多様化**
  オンプレミスのみでWebサイトを構築している際、自組織のネットワークに異常があった場合、利用者への広報手段として機能しなくなる場合がある。外部のSNSで公式アカウントを運用する等、周知方法の多様化を考慮する必要がある。

事例８　他人の認証情報の悪用による情報の不正取得

- ある重要インフラ事業者では、業務用データは部署ごとにアクセスを制限しており、他部署の従業員のIDによるアクセスは、通常であれば利用できない状態であった。
- 不正を行った従業員は、他部署の従業員（被害者）のIDからパスワードを類推し、本来アクセス権の無い他部署の業務用データにアクセスし、機密情報を印刷した上、 私的利用していた。
- 複合機の印刷ログから不正を行った従業員を特定するとともに、全システムのパスワードを、より複雑性を高めた上で変更を行った。また、全従業員向けに研修を行うことで内部不正の抑止に関する意識向上を図った。

【１　背景】

- 重要データ（顧客の個人情報等）と業務用データ（その他の情報）が別のシステムで管理されていた。
- 業務用データを取り扱うシステムへのログインは、部署ごとにアクセス制御を実施しており、関係する従業員のみ利用可能となっていた。

【２　検知】

- 該当部署で閲覧不可能な業務用データの資料が印刷され、プリンターに放置されていた。

【３　対処】

- プリンターのログを確認し、印刷した端末を特定した。
- 該当する端末を利用している職員に聞き込みを実施し、職員の特定に至った。
- サーバのアクセスログから、業務用データへの不正なアクセスを開始した時期を特定した。

【４　原因】

- 業務用データへのアクセスに使用するID・パスワードは、使用頻度が高いことから、類推しやすい平易なものになっていた。

【５　再発に備えた対策】

- パスワードの桁数を増やし、ランダムなものに設定しなおした。また、類推しやすい平易なものを設定不可とした。
- アクセスログを取得していることを含めて、全従業員向けに研修を実施し、内部不正の抑止に関して意識向上を図った。

【６　得られた気付き・教訓】

- **組織内での意識醸成と抑止**
  組織内で内部不正・不正アクセスに関する周知・教育を研修等を通じて徹底しておく必要がある。それと同時に、万が一不正アクセスが行われた際には、早期に検知できるよう、各システムのアクセスログを収集し、定期的に不審な点が無いか確認しておくことが肝要であると考えられる。
- **生体認証を含めた二要素認証の採用**
  重要なデータへのアクセスについては、ID・パスワードのような、代替しやすい手段だけではなく、第三者が不正利用しにくい生体情報を含めた二要素認証を採用することが望まれる。
- **（参考）パスワード設定の重要性**
  パスワードの定期的な変更の要否については、議論の残すところではあるが、システムログインにおけるパスワードは、英数・記号・大文字小文字を含めた推察されにくいランダムな文字列で10桁以上で設定しておくことが望まれる。

  NISCとしての見解は、パスワードの定期変更は基本は必要なしと考えている。ただし、万が一パスワードが流出した場合は速やかに変更すべきであると考えている。また、ZIPファイルのようなものの暗号キーである場合は、英数・記号・大文字小文字を含めた推察されにくいランダムな文字列で15桁以上で設定することが望まれる。

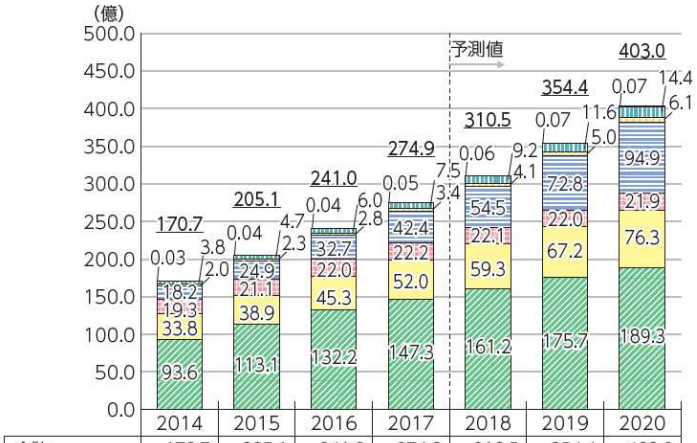
  ※参考資料：インターネットの安全・安心ハンドブックVer.4.00（NISC）
  （https://www.nisc.go.jp/security-site/files/handbook-all.pdf）

別添５　サイバーセキュリティ関連データ集

＜別添５－目次＞

データ 1 世界の IoT デバイス数の推移及び予測..... 331
データ 2 NICTER 観測結果..... 331
データ 3 平成 30 年インターネット観測結果..... 332
データ 4 「Security Action」制度　登録事業者数..... 348
データ 5 情報処理安全確保支援士　登録者数 349
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 . 349

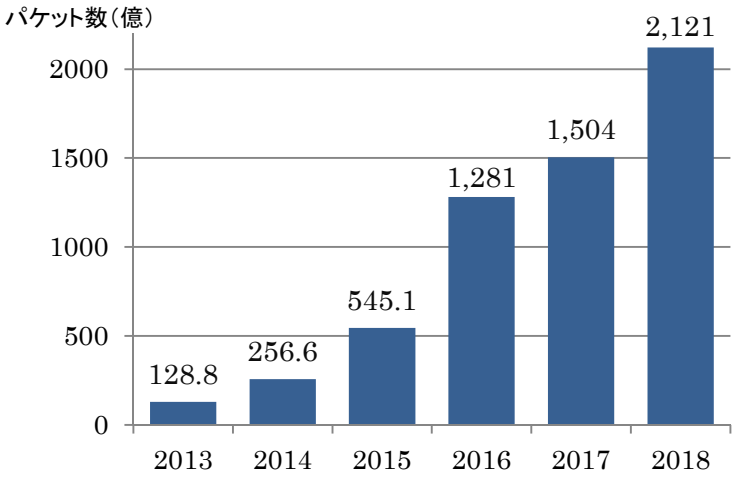
データ 1 世界の IoT デバイス[1]数の推移及び予測



	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

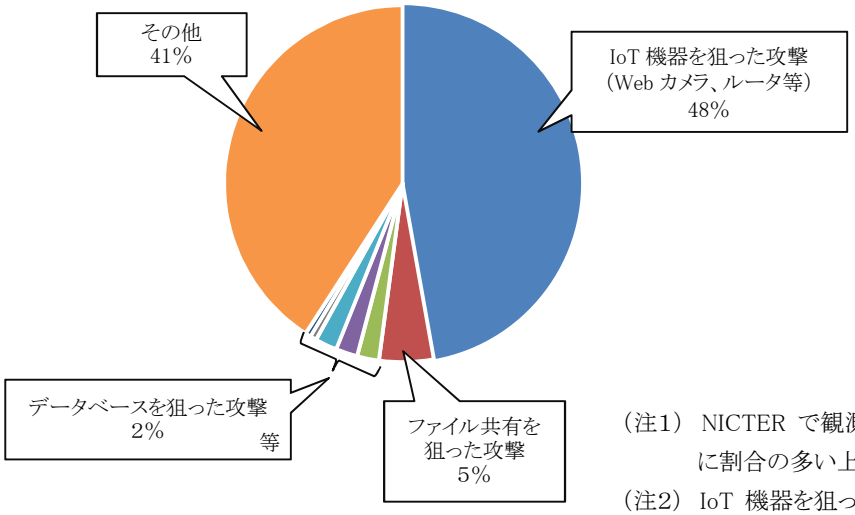
データ 2 NICTER 観測結果

データ 2.1 ダークネットセンサによる攻撃の観測数



[1] 各カテゴリの範囲は以下のとおり。
「通信」:固定通信インフラ・ネットワーク機器、2G、3G、4G 各種バンドのセルラー通信及び Wifi・WIMAX などの無線通信インフラ及び端末。
「コンシューマー」:家電(白物・デジタル)、プリンターなどの PC 周辺機器、ポータブルオーディオ、スマートトイ、スポーツ・フィットネス、その他。
「コンピューター」:ノートパソコン、デスクトップパソコン、サーバー、ワークステーション、メインフレーム・スパコンなどコンピューティング機器。
「産業用途」:オートメーション(IA/BA)、照明、エネルギー関連、セキュリティ、検査・計測機器などオートメーション以外の工業・産業用途の機器。
「医療」:画像診断装置ほか医療向け機器、コンシューマーヘルスケア機器。
「自動車・輸送機器」:自動車(乗用車、商用車)の制御系及び情報系において、インターネットと接続が可能な機器。
「軍事・宇宙・航空」:軍事・宇宙・航空向け機器(例:航空機コックピット向け電装・計装機器、旅客システム用機器、軍用監視システムなど)。

データ 2.2 ダークネットセンサによる攻撃の観測結果の内訳(2018 年)

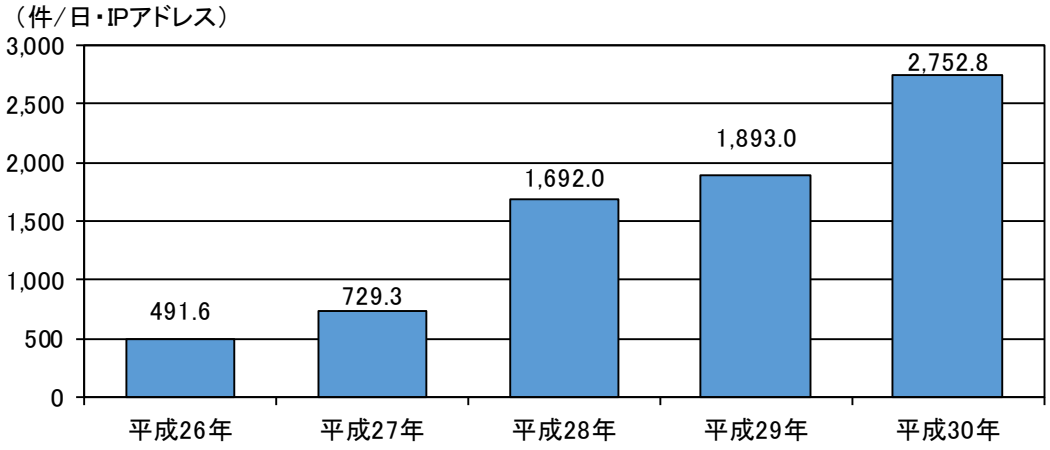


（注1） NICTER で観測されたパケットのうち、サービスの種類(ポート番号)ごとに割合の多い上位から 30 位までを分析したもの。

（注2） 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。

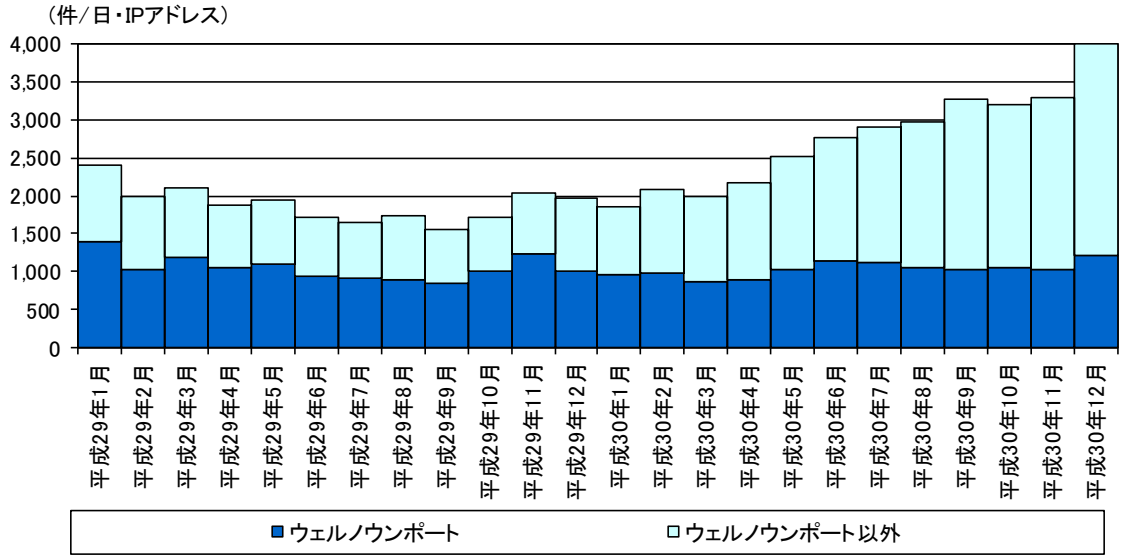
データ 3 平成 30 年インターネット観測結果[2]

データ 3.1 センサーにおいて検知したアクセス件数の推移

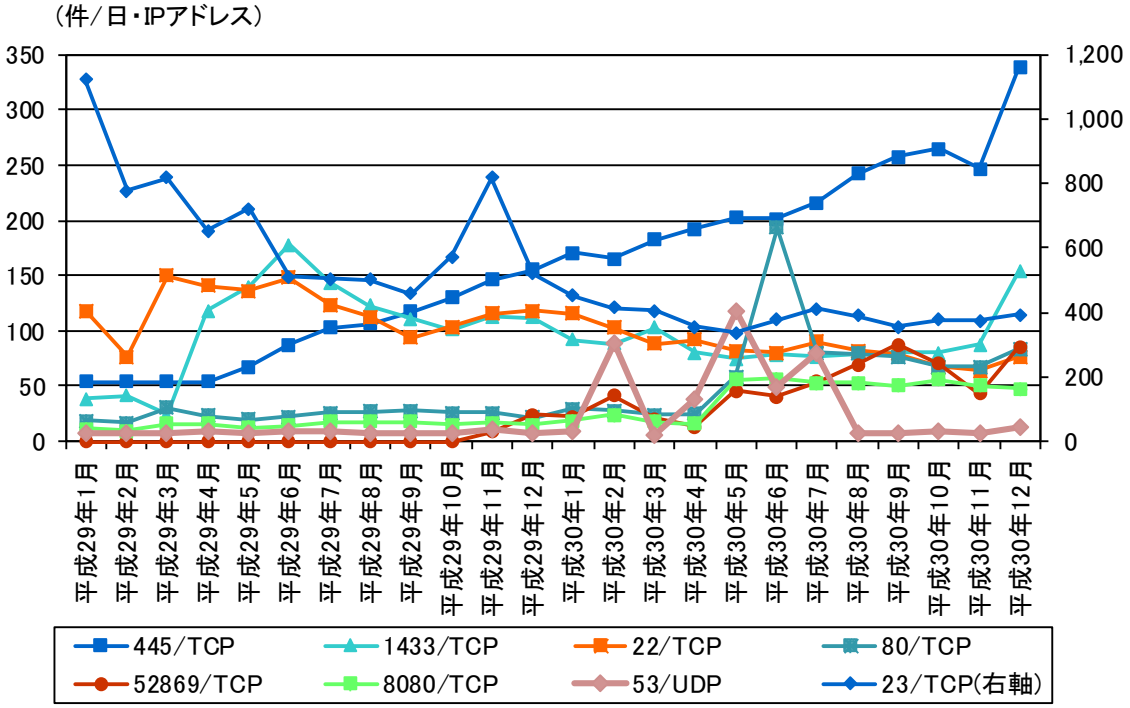


[2] 警察庁にて、全国の警察施設のインターネット接続点にセンサーを設置し、インターネット定点観測システムを構築してアクセス情報等を集約・分析した結果。「@police」 https://www.npa.go.jp/cyberpolice/ で公開。

データ 3.2 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[平成 29 年（以下「前期」）及び平成 30 年（以下「今期」）]



データ 3.3 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 3.4 センサーにおけるアクセス検知の観測結果

宛先ポート別アクセス検知件数（今期順位）

今期順位	前期順位	ポート	今期件数[3]	前期比[3]
1 位	1 位	23/TCP	387.08 件	－41.7%　（－277.20 件）
2 位	4 位	445/TCP	223.83 件	＋137.0%　（＋129.39 件）
3 位	3 位	1433/TCP	89.74 件	－13.7%　（－14.21 件）
4 位	2 位	22/TCP	84.94 件	－29.3%　（－35.26 件）
5 位	11 位	80/TCP	67.90 件	＋182.5%　（＋43.87 件）

宛先ポート別検知件数（増加順位）

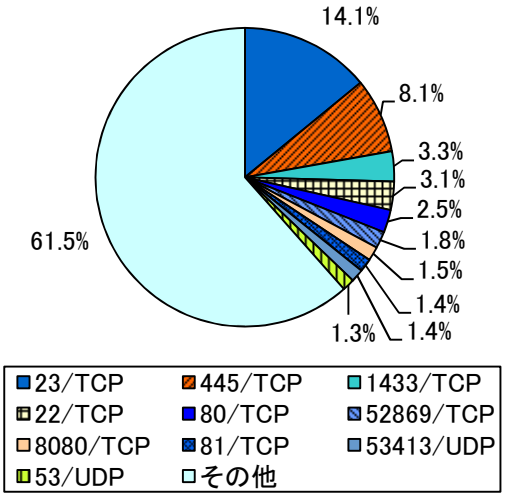
増加順位	ポート	今期件数[3]	前期比[3]	今期順位	前期順位
1 位	445/TCP	223.83 件	＋137.0%　（＋129.39 件）	2 位	4 位
2 位	52869/TCP	49.71 件	＋1,671.0%　（＋46.91 件）	6 位	34 位
3 位	80/TCP	67.90 件	＋182.5%　（＋43.87 件）	5 位	11 位
4 位	53/UDP	35.82 件	＋342.3%　（＋27.72 件）	10 位	24 位
5 位	8080/TCP	41.91 件	＋177.5%　（＋26.81 件）	7 位	15 位

宛先ポート別検知件数（減少順位）

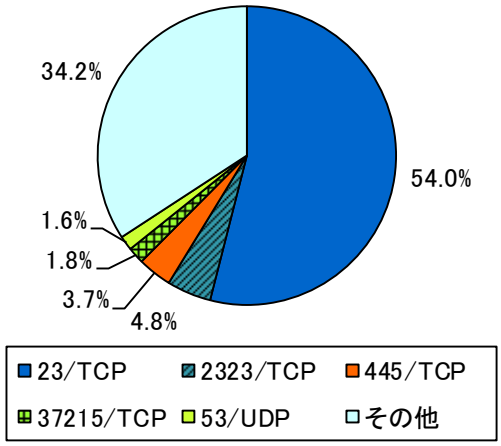
減少順位	ポート	今期件数[3]	前期比[3]	今期順位	前期順位
1 位	23/TCP	387.08 件	－41.7%　（－277.20 件）	1 位	1 位
2 位	5358/TCP	1.19 件	－97.4%　（－44.94 件）	128 位	6 位
3 位	22/TCP	84.94 件	－29.3%　（－35.26 件）	4 位	2 位
4 位	2323/TCP	28.02 件	－46.2%　（－24.09 件）	13 位	5 位
5 位	1900/UDP	11.45 件	－64.4%　（－20.73 件）	22 位	9 位

[3] 一日・1IP アドレス当たり。

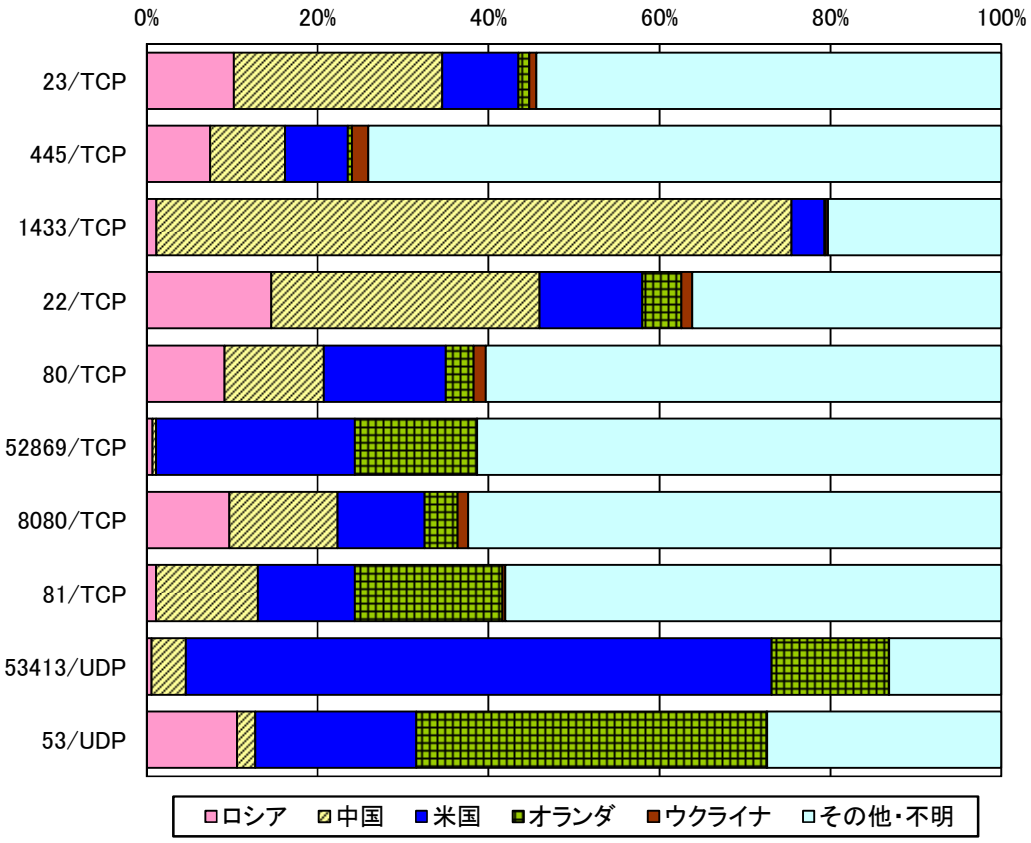
宛先ポート別比率（全て）



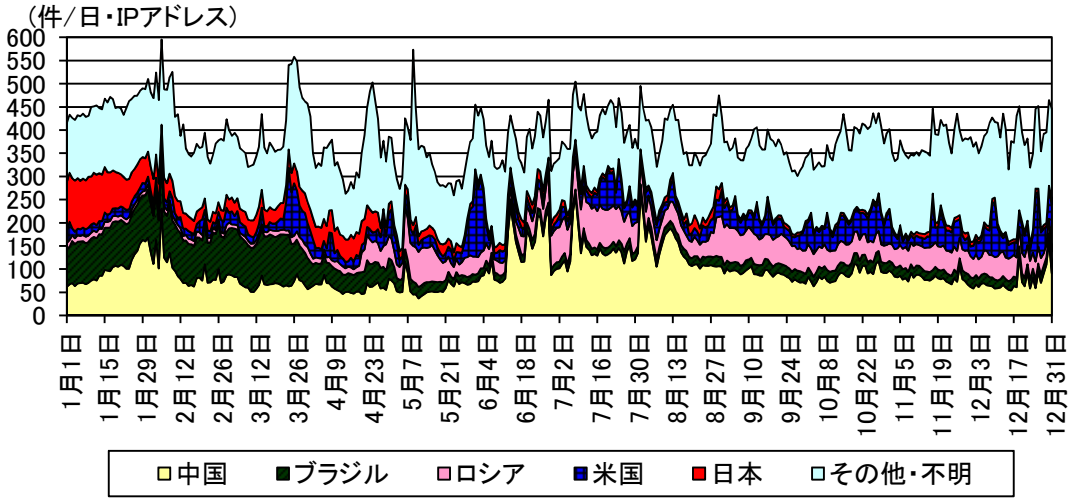
宛先ポート別比率（日本国内）



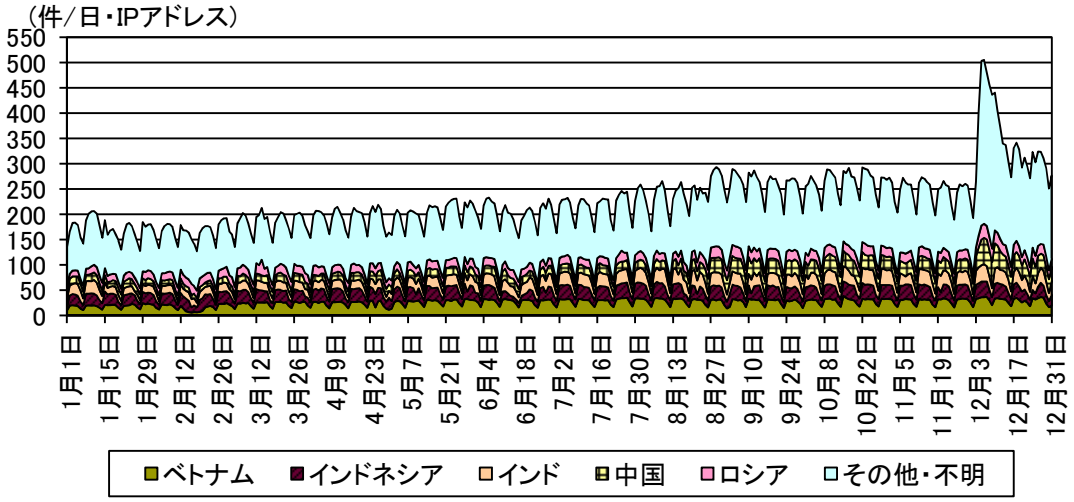
宛先ポート別上位の着信元国・地域別比率



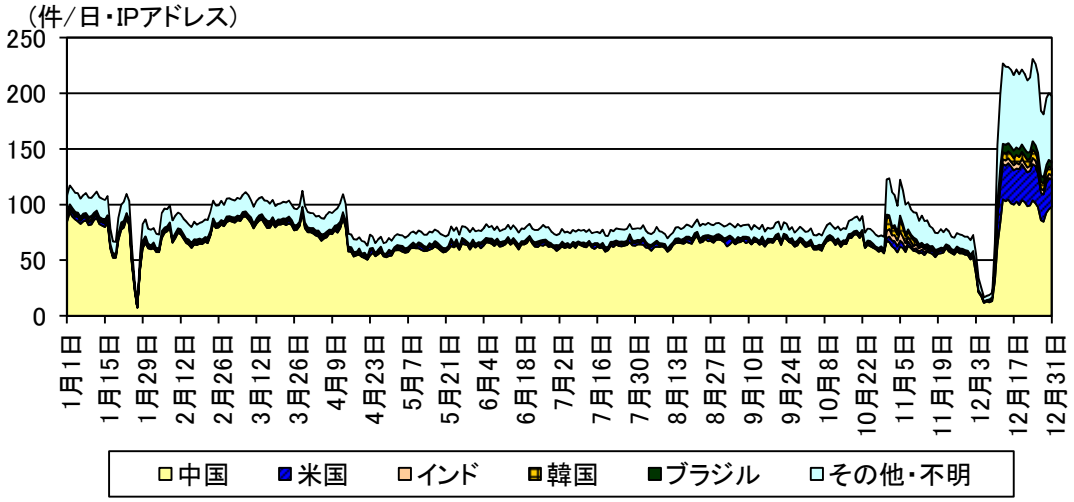
宛先ポート 23/TCP に対するアクセス件数の推移



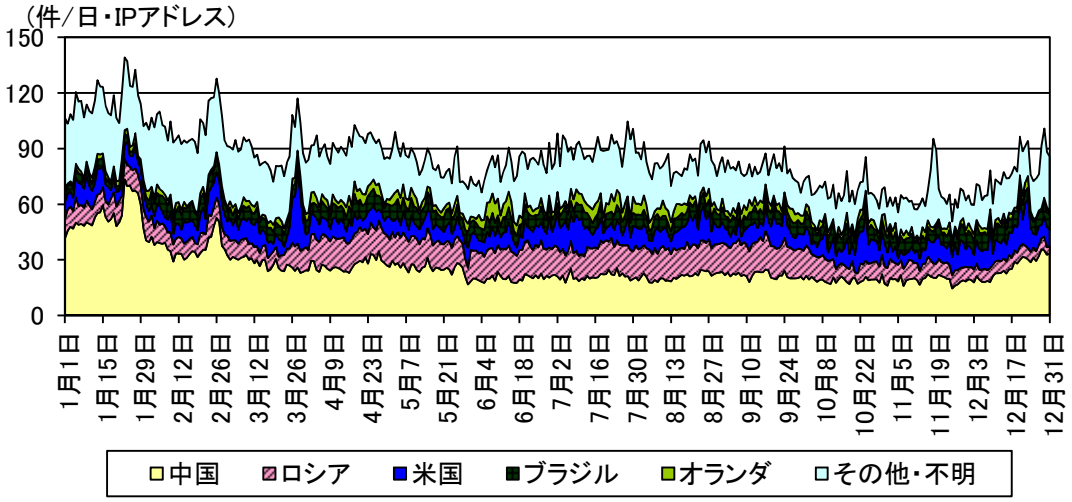
宛先ポート 445/TCP に対するアクセス件数の推移



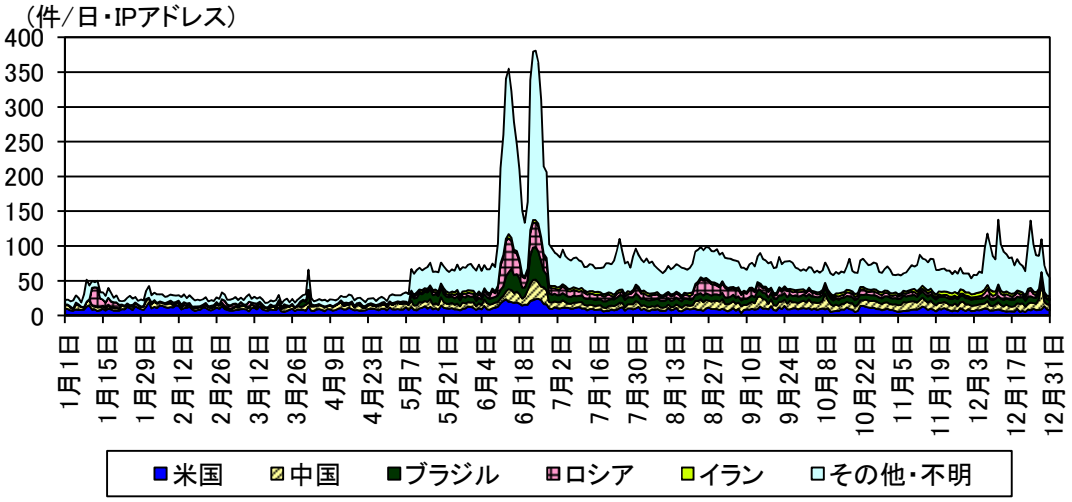
宛先ポート 1433/TCP に対するアクセス件数の推移



宛先ポート 22/TCP に対するアクセス件数の推移



宛先ポート 80/TCP に対するアクセス件数の推移



データ 3.5 着信元国・地域別アクセス検知件数

着信元国・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 [4]	前期比 [4]
1 位	3 位	ロシア	573.44 件	＋327.7%　（＋439.37 件）
2 位	1 位	中国	387.68 件	－16.7%　（－77.47 件）
3 位	2 位	米国	346.02 件	＋37.8%　（＋94.85 件）
4 位	7 位	オランダ	164.50 件	＋159.6%　（＋101.13 件）
5 位	13 位	ウクライナ	140.83 件	＋335.5%　（＋108.49 件）

着信元国・地域別検知件数（増加順位）

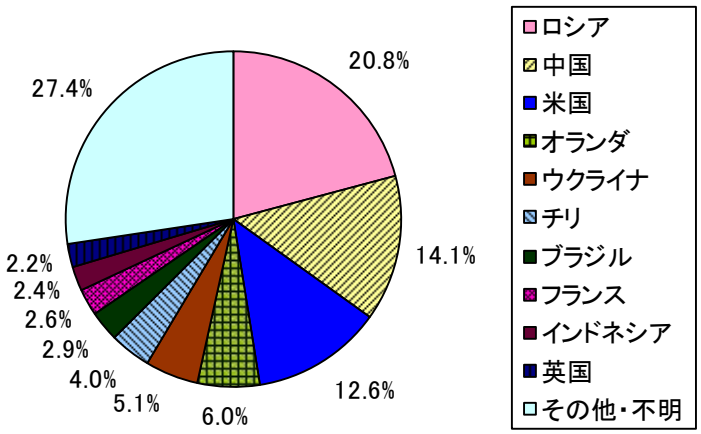
増加順位	国・地域	今期件数 [4]	前期比 [4]	今期順位	前期順位
1 位	ロシア	573.44 件	＋327.7%　（＋439.37 件）	1 位	3 位
2 位	ウクライナ	140.83 件	＋335.5%　（＋108.49 件）	5 位	13 位
3 位	オランダ	164.50 件	＋159.6%　（＋101.13 件）	4 位	7 位
4 位	米国	346.02 件	＋37.8%　（＋94.85 件）	3 位	2 位
5 位	チリ	109.35 件	＋248.7%　（＋78.00 件）	6 位	15 位

着信元国・地域別検知件数（減少順位）

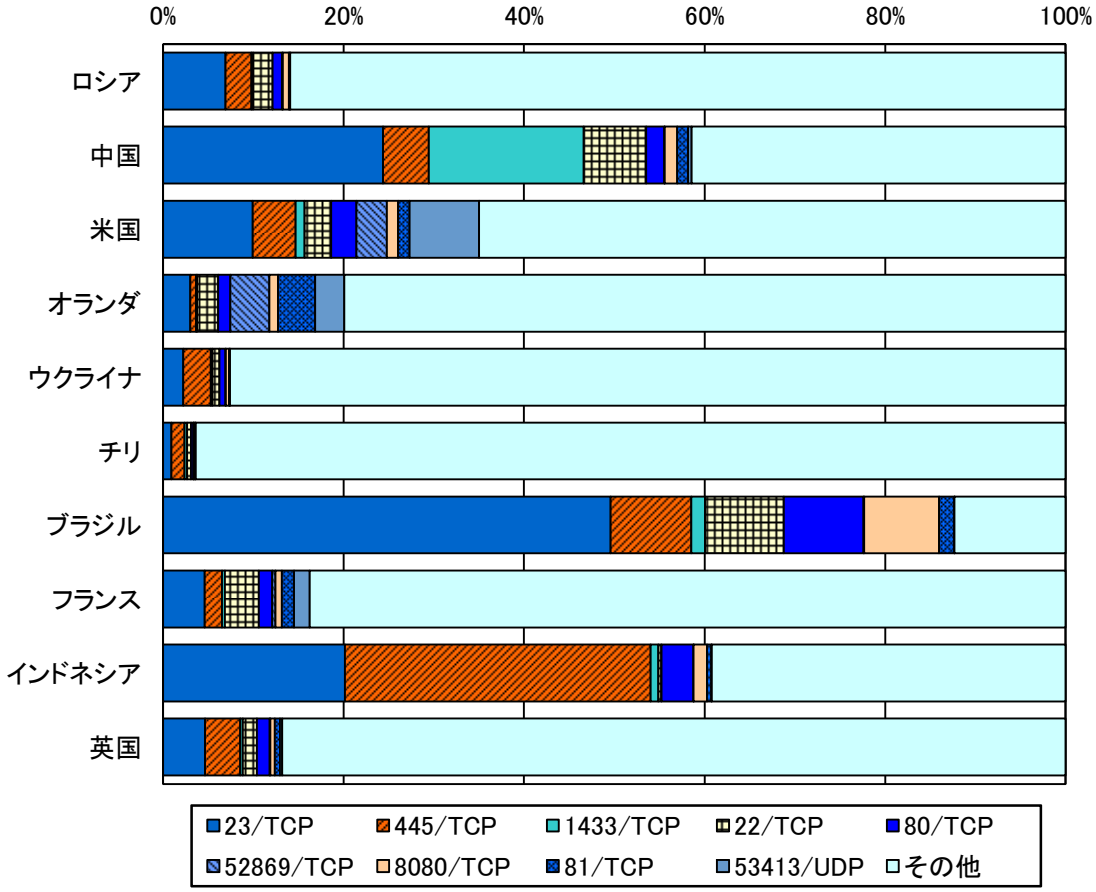
減少順位	国・地域	今期件数 [4]	前期比 [4]	今期順位	前期順位
1 位	中国	387.68 件	－16.7%　（－77.47 件）	2 位	1 位
2 位	韓国	35.02 件	－54.4%　（－41.72 件）	17 位	5 位
3 位	インド	39.32 件	－46.9%　（－34.71 件）	15 位	6 位
4 位	アルゼンチン	9.83 件	－74.3%　（－28.48 件）	34 位	11 位
5 位	台湾	28.31 件	－47.5%　（－25.64 件）	19 位	9 位

[4] 一日・1IP アドレス当たり。

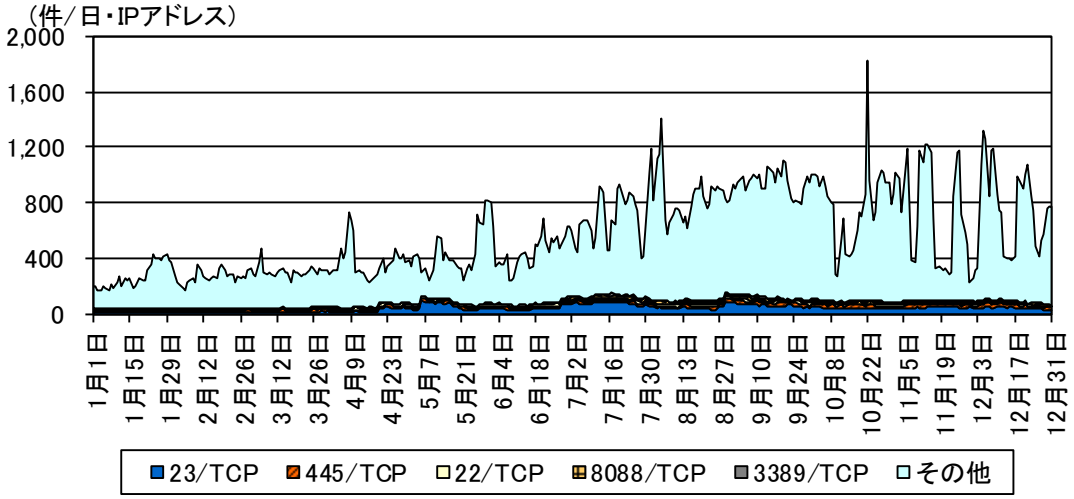
着信元国・地域別比率



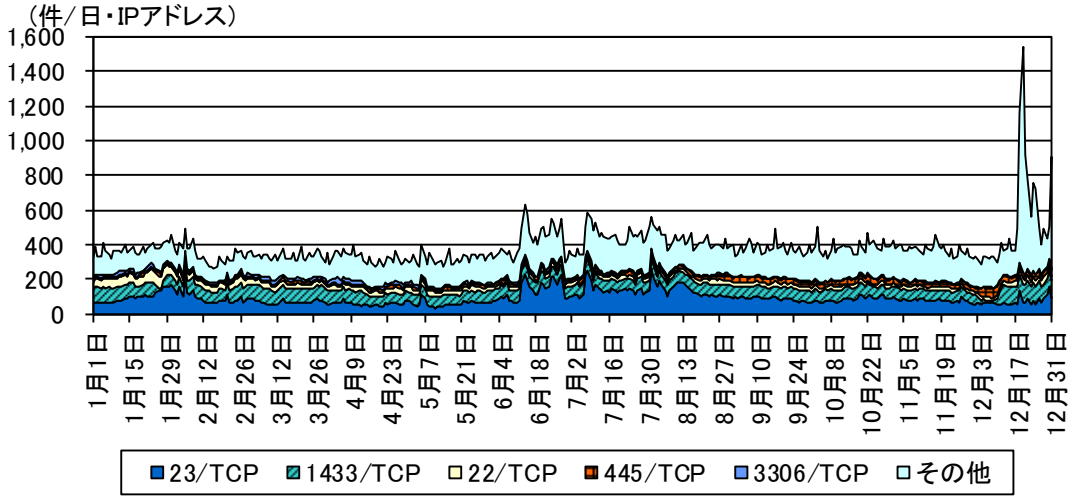
着信元国・地域別上位の宛先ポート別比率



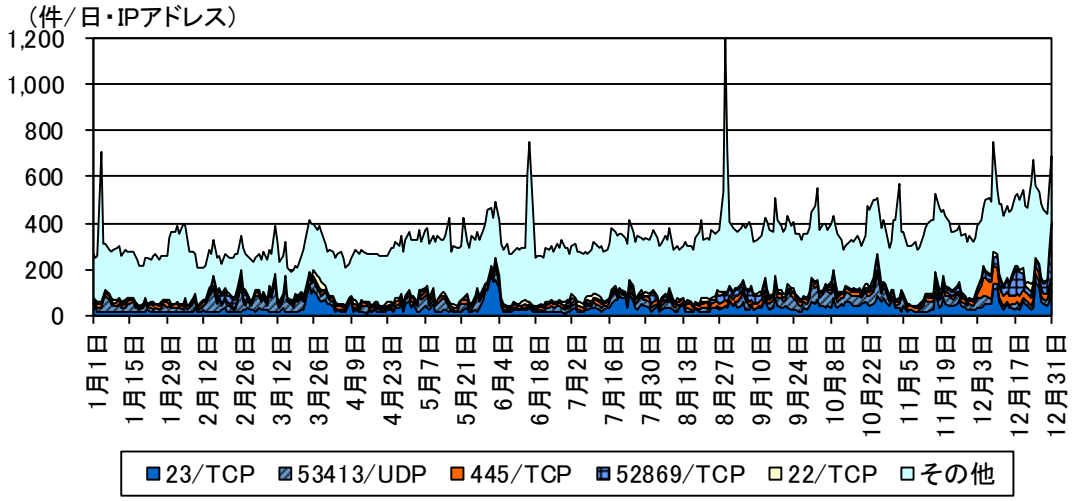
ロシアからのアクセス件数の推移



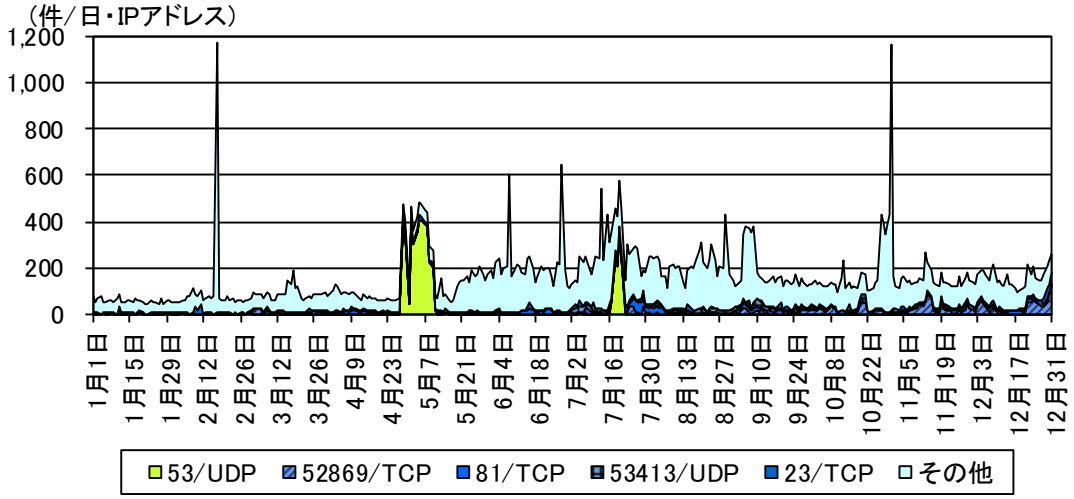
中国からのアクセス件数の推移



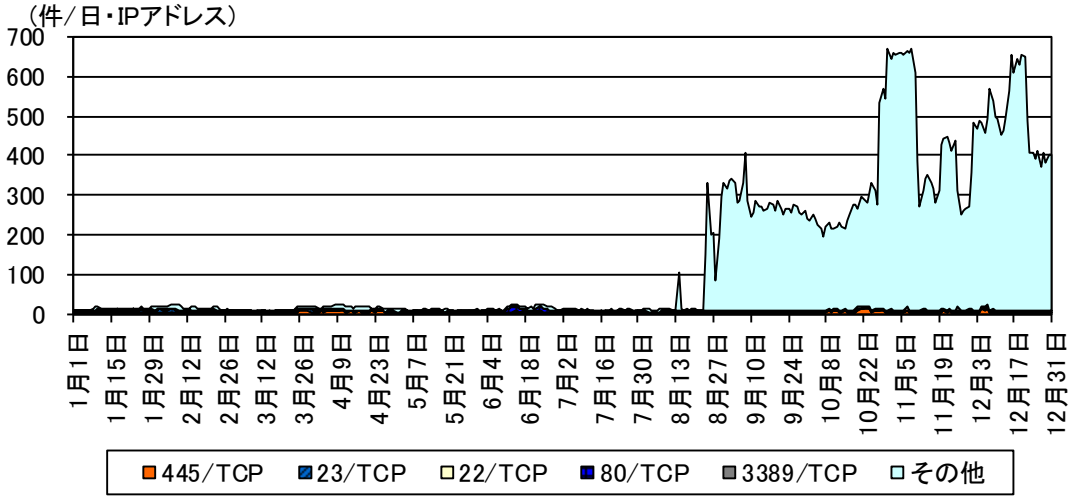
米国からのアクセス件数の推移



オランダからのアクセス件数の推移



ウクライナからのアクセス件数の推移

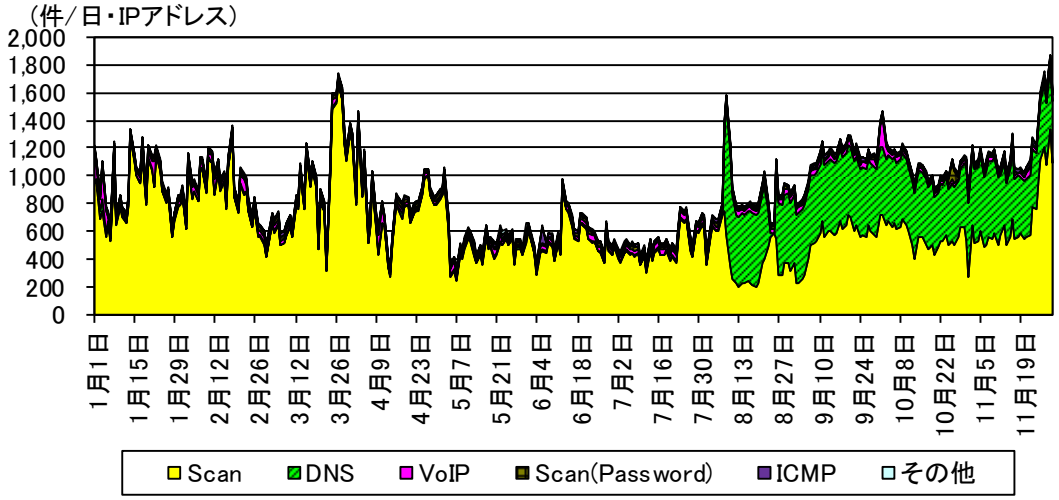


データ 3.6 不正侵入等の観測結果

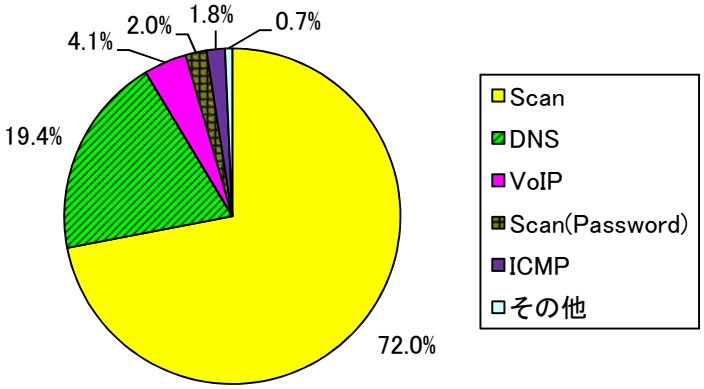
不正侵入等の攻撃手法別検知件数

今期順位	前期順位	攻撃手法	今期件数[5]	前期比[5]	増加順位	減少順位
1 位	1 位	Scan	638.59 件	－42.6%　（－474.49 件）		1 位
2 位	3 位	DNS	172.26 件	＋557.5%　（＋146.06 件）	1 位	
3 位	2 位	VoIP	36.56 件	＋17.2%　（＋5.37 件）	2 位	
4 位	4 位	Scan(Password)	18.04 件	－29.4%　（－7.52 件）		2 位
5 位	5 位	ICMP	15.64 件	＋45.2%　（＋4.87 件）	3 位	

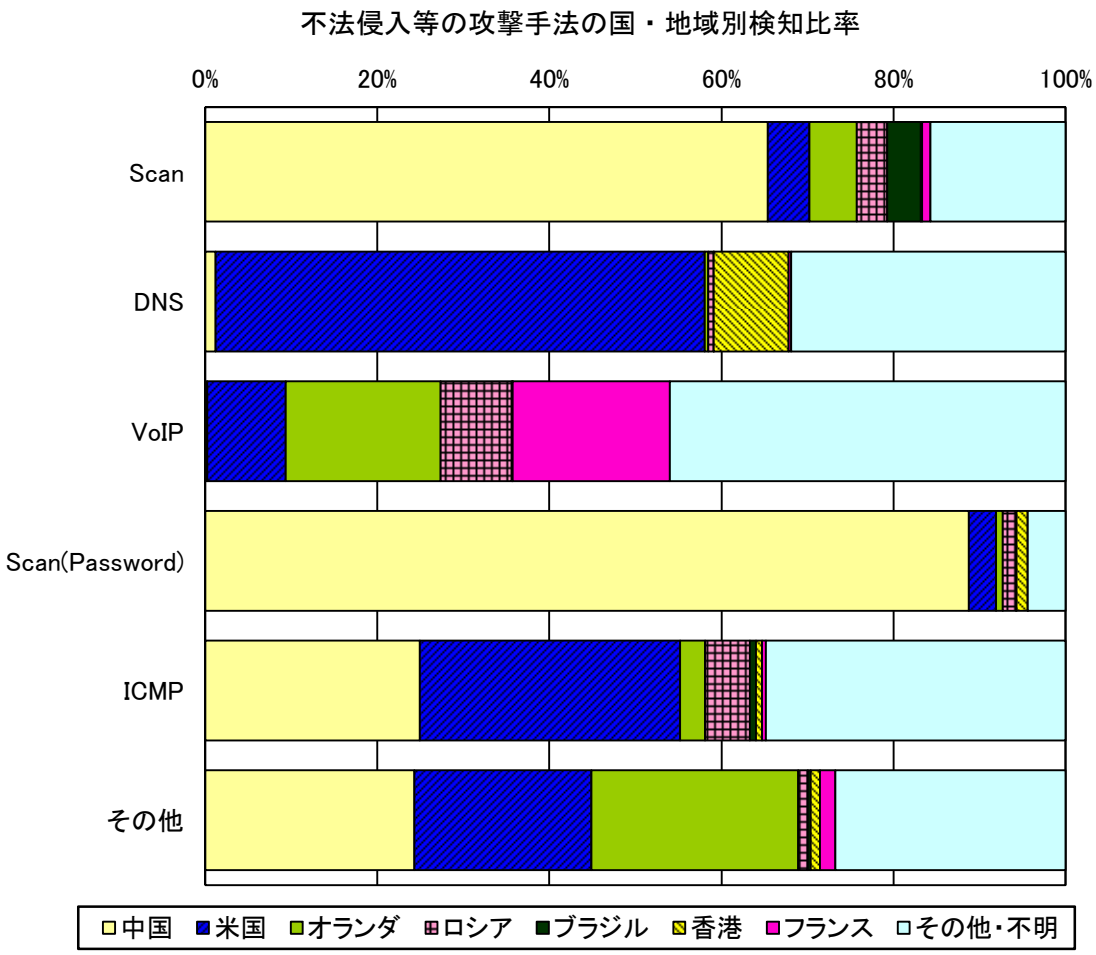
不正侵入等の攻撃手法別検知件数の推移



不正侵入等の攻撃手法別検知比率



[5] 一日・1IP アドレス当たり。


不法侵入等の攻撃手法の国・地域別検知比率
0%
20%
40%
60%
80%
100%
Scan
DNS
VoIP
Scan(Password)
ICMP
その他
中国
米国
オランダ
ロシア
ブラジル
香港
フランス
その他・不明

データ 3.7 着信元国・地域別アクセス検知件数

不正侵入等の着信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[6]	前期比[6]
1 位	1 位	中国	441.22 件	－57.7%　（－601.87 件）
2 位	3 位	米国	138.57 件	＋304.4%　（＋104.31 件）
3 位	2 位	オランダ	44.64 件	＋5.6%　（＋2.36 件）
4 位	7 位	ロシア	27.81 件	＋249.3%　（＋19.85 件）
5 位	9 位	ブラジル	24.99 件	＋471.6%　（＋20.62 件）

不正侵入等の着信元国・地域別検知件数（増加順位）

増加順位	国・地域	今期件数[6]	前期比[6]	今期順位	前期順位
1 位	米国	138.57 件	＋304.4%　（＋104.31 件）	2 位	3 位
2 位	ブラジル	24.99 件	＋471.6%　（＋20.62 件）	5 位	9 位
3 位	ロシア	27.81 件	＋249.3%　（＋19.85 件）	4 位	7 位
4 位	マカオ	13.42 件	－[7]　（＋13.39 件）	8 位	－[7]
5 位	香港	16.37 件	＋419.8%　（＋13.22 件）	6 位	11 位

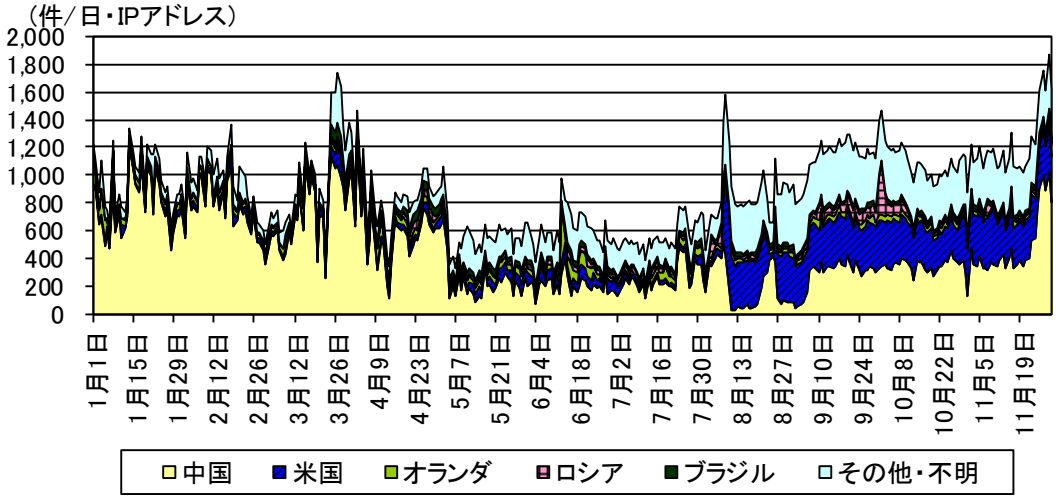
不正侵入等の着信元国・地域別検知件数（減少順位）

減少順位	国・地域	今期件数[6]	前期比[6]	今期順位	前期順位
1 位	中国	441.22 件	－57.7%　（－601.87 件）	1 位	1 位
2 位	ポーランド	2.07 件	－51.5%　（－2.21 件）	29 位	10 位
3 位	スイス	0.81 件	－66.1%　（－1.58 件）	41 位	15 位
4 位	チリ	1.29 件	－33.3%　（－0.64 件）	34 位	16 位
5 位	リトアニア	1.09 件	－23.5%　（－0.34 件）	36 位	22 位

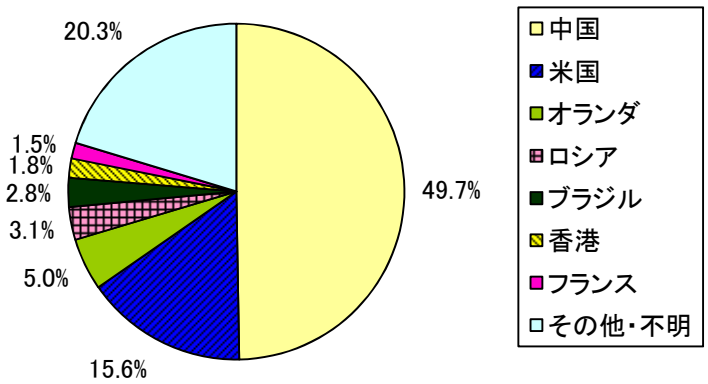
[6] 一日・1IP アドレス当たり。

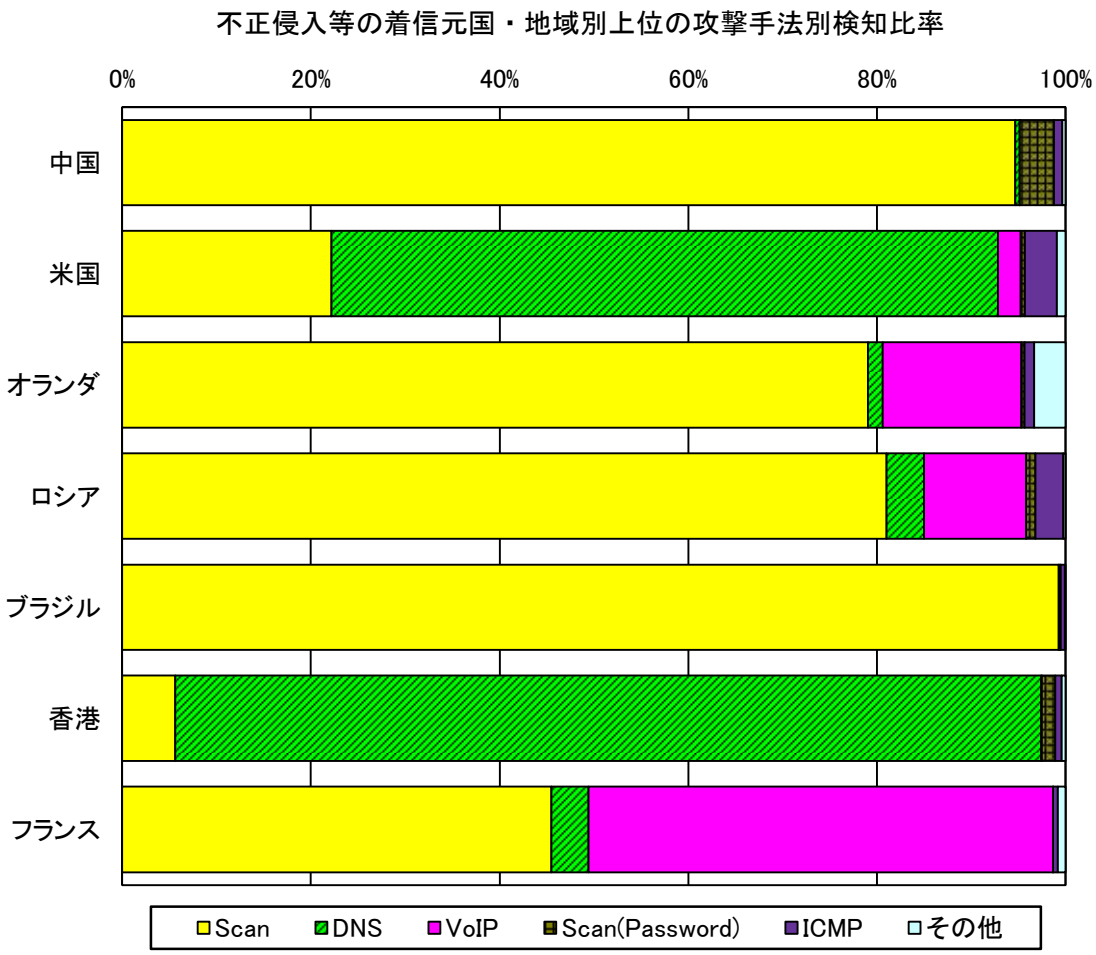
[7] 前期の検知件数が僅かなため、前期比及び前期順位は記載していません。

不正侵入等の着信元国・地域別検知件数の推移



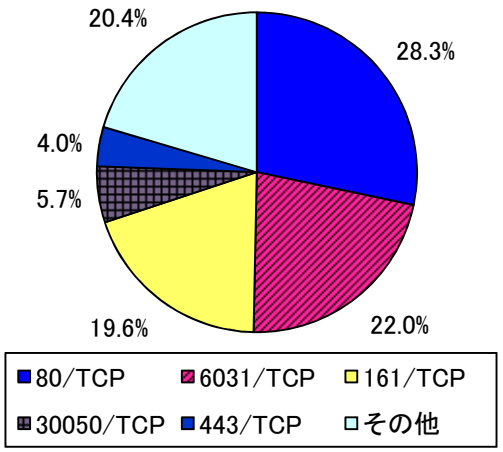
不正侵入等の着信元国・地域別検知比率



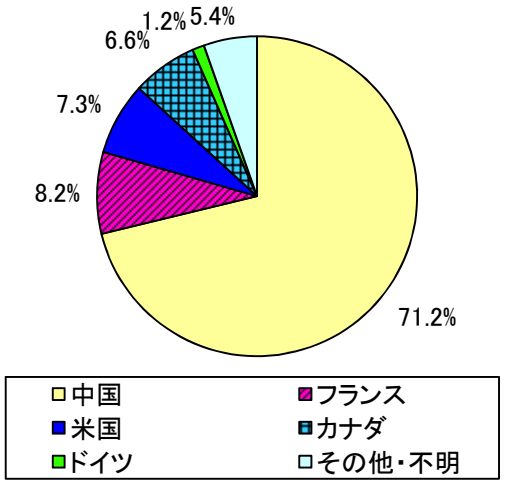

不正侵入等の着信元国・地域別上位の攻撃手法別検知比率
0%
20%
40%
60%
80%
100%
中国
米国
オランダ
ロシア
ブラジル
香港
フランス
Scan
DNS
VoIP
Scan(Password)
ICMP
その他

データ 3.8 DoS 攻撃被害の観測結果

跳ね返りパケット着信元ポート別比率



跳ね返りパケット着信元国・地域別比率



跳ね返りパケットの着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 [8]	前期比 [8]
1 位	1 位	80/tcp	5,417.49 件	−54.5%　(−6,485.81 件)
2 位	— [9]	6031/tcp	4,218.42 件	— [9]　(+4,218.41 件)
3 位	— [9]	161/tcp	3,753.56 件	— [9]　(+3,753.54 件)
4 位	— [9]	30050/tcp	1,086.68 件	— [9]　(+1,086.67 件)
5 位	3 位	443/tcp	756.93 件	+90.8%　(+360.3 件)

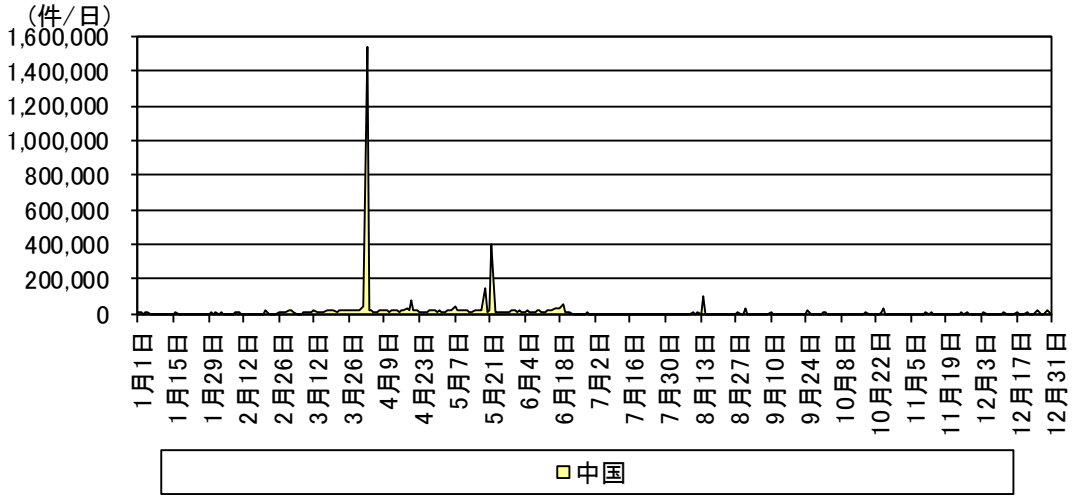
跳ね返りパケットの着信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [8]	前期比 [8]
1 位	1 位	中国	13,636.8 件	+56%　(+4,893.53 件)
2 位	4 位	フランス	1,577.39 件	+47.6%　(+508.45 件)
3 位	2 位	米国	1,406.21 件	−76%　(−4,459.63 件)
4 位	3 位	カナダ	1,265.77 件	+6.4%　(+76.46 件)
5 位	5 位	ドイツ	227.45 件	−68.9%　(−503.61 件)

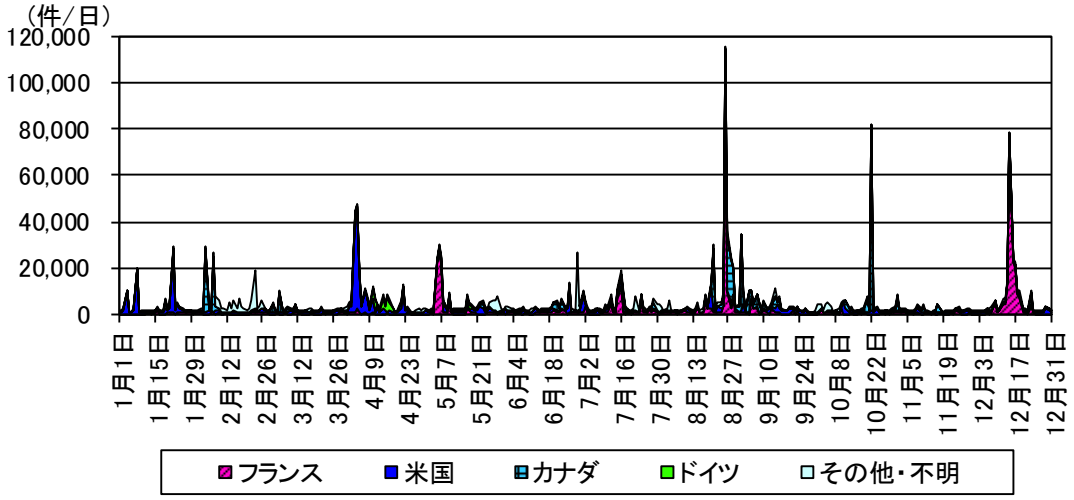
[8] 一日当たり。

[9] 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着信元国・地域別検知件数の推移（中国のみ）



跳ね返りパケットの着信元国・地域別検知件数の推移（中国以外）



データ４　「Security Action」制度　登録事業者数

平成29年度		平成30年度			合計			累計登録者数
一つ星	二つ星	一つ星	二つ星	登録のみ	一つ星	二つ星	登録のみ	
213	271	52,955	8,626	5,497	53,168	8,897	5,497	67,562

データ 5 情報処理安全確保支援士　登録者数

平成29年度		平成30年度		平成31年度	累計 登録者数	平成31年4月1日時点 登録者数(※)
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	18,466	18,330

(※)累計登録者数から登録消除等 136 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

年度＼試験区分		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(※)	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

(※)平成28年度までは情報セキュリティスペシャリスト試験、平成29年度からは、情報処理安全確保支援士試験を示す。

別添６　担当府省庁一覧（2019 年度計画）

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、文部科学省、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	◎：経済産業省
(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	◎：内閣府、経済産業省 〇：総務省 ※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	
(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（◎）：内閣官房副長官補（国土交通、海上保安担当） ※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 ○：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、警察庁
(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 ○：法務省
(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、経済産業省
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）

別添７　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。
	APEC	Asia-Pacific Economic Cooperationの略（エイペック）。アジア太平洋地域の21の国と地域が参加する枠組み。
	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、2019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。
	CSMS	Cyber Security Management Systemの略。制御システムのセキュリティマネジメントシステム。
	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。
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、2017年５月現在、世界80ヶ国の官・民・大学等369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。
	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カ国）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。
	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	NATIONAL 318(CYBER) EKIDEN	府省庁職員を対象とした、１府12省庁対抗による競技形式のサイバー攻撃対処訓練のこと。
	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実施するとともに、民間や大学が実施する情報通信分野の研究開発の支援の実施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。
	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	Organization 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 2018	SECCON：SECurity CONtest 2018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2018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。
	Slow HTTP DoS	DoS攻撃の一種で、対象Webサーバへ比較的少ないパケット数をTCPセッションが継続するように長時間に渡って送り続け、正規の閲覧者がアクセスできないようにする攻撃。
	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。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	暗号アルゴリズム	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。
	クロスサイトスクリプティング	閲覧者が入力したデータがページ内容に反映されるような動的Webページにおける、当該ページに不正なスクリプトを埋め込むことができる脆弱性、もしくはその脆弱性を利用した攻撃手法。
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	2020年東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織。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戦略本部令（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もの会議体であり、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	2018年４月４日サイバーセキュリティ戦略本部決定。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	2017年４月18日サイバーセキュリティ戦略本部決定。昨今のサイバー攻撃による急速な脅威の高まりや、2020東京オリンピック・パラリンピック競技大会も見据え、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。2018年７月25日に、重要インフラ分野として「空港分野」を追加する改定を実施している。
	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	2020年東京大会の開催・運営に影響を与える可能性のあるサービスのうち重要なもので、会場に供給する電力や、競技を中継する通信等のサービスを提供する事業者のこと。

	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
	情報セキュリティ政策会議	2005年５月、IT総合戦略本部の下に設置された会議。内閣官房長官を議長とし、我が国の情報セキュリティに関する諸問題に係る対策等を決定する。サイバーセキュリティ戦略本部に業務が引き継がれ、2015年６月に廃止。
	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。
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。
	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。
つ	つながる世界の開発指針	IPAにおいて、2016年３月に策定、2017年６月に第２版へ改訂。様々なモノがつながって新たな価値を創出していく『つながる世界』ならではの機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項をとりまとめたもの。
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。
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）。
	特定秘密	行政機関の長が、当該行政機関の所掌事務に係る特定秘密保護法別表に掲げる事項に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるものとして指定したものをいう（特定秘密保護法第3条第1項）。
	匿名エンティティ認証（ISO/IEC20009-4）	本人を特定させることなくプライバシーを保護して、相手（エンティティ）の認証を行うことができる技術。
	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）
	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	ハクティビスト	ハッカー（hacker）と活動家（activist）を合わせた造語。政治的な動機でハッキング活動を行う人やグループを指す。その思想は「ハクティビズム（hacktivism）」と言われる。例えば、国際的ハッカー集団「アノニマス」があたるとされる。
	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。
	秘密分散メカニズム（ISO/IEC19592-2)	データに特殊な符号化を施して複数の断片に分割することで、個々の断片からは情報が漏れず、幾つかの断片が消失しても復元が可能な技術。
	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。たとえば、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	政府が運営するオンラインサービス。子育てに関する行政手続きがワンストップでできたり、行政機関からのお知らせを確認できたりするポータルサイトのこと。

	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。