資料２

サイバーセキュリティ政策に係る年次報告（2017 年度）（案）

資料２－１　サイバーセキュリティ政策に係る年次報告（2017 年度）（案）の概要

資料２－２　サイバーセキュリティ政策に係る年次報告（2017 年度）（案）

サイバーセキュリティ政策に係る年次報告(2017年度)(案)の概要

資料２－１

本年次報告の位置付け

- 現行の「サイバーセキュリティ戦略」（2015年9月4日閣議決定）に基づく三期目の年次報告。
- 2017年度のサイバーセキュリティに関する情勢、年次計画に掲げられた施策の実施状況・評価を取りまとめたもの。

政府機関等における情勢

- ウェブアプリケーションの脆弱性を悪用した攻撃等、依然として政府機関等を対象とした攻撃が頻発しているが、政府機関等の対策により、サイバー攻撃に係る件数は減少傾向。ただし、攻撃は巧妙化が図られるなど、予断を許さない状況。
- 2017年４月から、国による監視、監査、原因究明調査等の範囲を政府機関に加え、独立行政法人等へ拡大。

【第一GSOC※1における確認を要するイベント検知件数※2】

センサー監視等によるイベント検知件数のうち、対処の要否について確認を要するものの件数は昨年度より減少している。なお、既知の脆弱性に対する攻撃等が減少する一方、脆弱性が短時間のうちに攻撃に悪用されるなど攻撃の種類は昨年度より増加している。

※1　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
※2　既に攻撃手法に対応済みであるため攻撃としては失敗した通信、攻撃の前段階で行われる調査のための行為にとどまり明らかに対応不要と判断できる通信等を分析しノイズとして除去した上で、なお対処の要否について確認を要する事象の件数
※3　Denial of Serviceの略。サービス不能攻撃

【政府機関に対する攻撃の傾向】

センサー監視等による通報件数は133件、不審メール等の注意喚起件数は878件となり、どちらも2016年度から減少しているものの、脆弱性情報の公開直後の攻撃の増加、不審メールの巧妙化が確認されており、引き続き注意が必要。

【政府機関等に対する不審メールの傾向】

2017年度は、不審なファイルが添付されたメール（ファイル添付型）の比率が減少し、不審なURLが記載されたメール（URL型）の比率が増加。

サイバーセキュリティ政策に係る年次報告(2017年度)(案)の概要

主な政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

＜実績＞

- 「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」を基本とした国際標準化活動を推進。
- 「セキュリティマインドを持った企業経営WG」において、具体的な方策等の検討を実施し、報告書として取りまとめを実施。
- 中小企業投資促進税制において、セキュリティ製品等への税制措置を継続実施。

＜評価＞

意識醸成、個別分野への部分的な対策は一定程度進展。今後は、全産業分野における経営層の意識改革、業界横断的な対応や関連する環境整備等に向けて、関係省庁や関係機関における有機的・一体的な連携による取組等が必要。

2．国民が安全で安心して暮らせる社会の実現

＜実績＞

- 「サイバーセキュリティ月間」において、テレビアニメ『BEATLESS』とタイアップを行い、ポスターやバナーの作成、イベント「アナログハックを目撃せよ！2018」を開催。
- 重要インフラ事業者等を対象に情報共有・対処を行う「分野横断的演習」を継続実施。
- 各府省庁対抗による競技形式のサイバー攻撃対処訓練「NATIONAL 318(CYBER) EKIDEN 2018」を継続実施。

NATIONAL 318(CYBER) EKIDEN

＜評価＞

国民への意識啓発、重要インフラ防護の範囲の見直し、監視、監査、原因究明調査等の範囲拡大等、各層への取組は着実に進展。今後は、多様な国民のニーズに対するきめ細やかな対応、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく取組、新たな防護技術等を適時適切に活用し政府機関等のセキュリティ強化・充実に向けた取組等を推進

サイバーセキュリティ政策に係る年次報告(2017年度)(案)の概要

主な政策の取組実績と評価

3．国際社会の平和・安定及び我が国の安全保障

＜実績＞

- 国立研究開発法人相互の協力による自律的活動の向上に向けた取組として、国立研究開発法人協議会に情報セキュリティに関する枠組みを立ち上げ。
- 重要インフラ防護の国際連携を推進するMeridianカンファレンス等の国際会議において、我が国のサイバーセキュリティ戦略をはじめとする関係施策を積極的に発信。
- 国際サイバー演習への参加や二国間・多国間対話等を通じ、各国との連携を強化。

日・ASEAN情報セキュリティ政策会議

＜評価＞

高度なサイバー攻撃からの防護等に係る能力強化、サイバー空間における法の支配の推進や各国政府や地域の主体との間での連携強化等については着実に進展。今後は、引き続き取組を強化するとともに、サイバー空間における国際法の適用のあり方等についての議論、国際サイバー演習の範囲の拡大検討、各国との情報共有等の連携の深化のあり方の検討を進めることが必要。

4．横断的施策

＜実績＞

- 将来的な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示した「サイバーセキュリティ研究開発戦略」を策定。
- 「サイバーセキュリティ人材育成プログラム」を踏まえ、「サイバーセキュリティ人材の育成に関する施策間連携WG」において、各層別の人材像やキャリアパスの明確化、教材のR&D等について検討。

＜評価＞

「サイバーセキュリティ研究開発戦略」及び「サイバーセキュリティ人材育成プログラム」により、研究開発と人材育成に係る方向性を示すとともに、サイバー攻撃の検知・予測や防御力向上等に資する研究開発、各層別の人材育成施策を着実に推進。今後は、研究開発成果の社会実装の推進、人材育成に関する取組の「見える化」等、具体的な取組を推進することが必要。

サイバーセキュリティ政策に係る年次報告(2017年度)(案)の概要

主な政策の取組実績と評価

5．推進体制

＜実績＞

- 東京オリンピック競技大会・パラリンピック競技大会推進本部の下に設置されたセキュリティ幹事会、サイバーセキュリティワーキングチーム等において施策を検討するとともに、「2020年東京オリンピック競技大会・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)」に基づき対策を推進。
- 「サイバーセキュリティ対処調整センター」に関する検討を推進し、2018年度末目途に構築及び運用開始することを決定。
- 2018年平昌大会の直前及び期間中におけるサイバーセキュリティに係る状況について、試験的に運用しているサイバーセキュリティ関係機関等との情報共有体制を活用し、韓国政府が指定した窓口に対して定期的に情報提供を実施。
- リスクマネジメントについては、リスク評価に係る手順書を改訂し、東京圏（東京都、神奈川県、千葉県、埼玉県）の重要サービス事業者等を対象とする第２回目のリスク評価を依頼し、NISCにおいて131の事業者から実施結果を受領の上、同評価に基づく対策を促進。

＜評価＞

2020年東京大会のサイバーセキュリティの確保については、概ね当初の計画どおりに進捗。今後は、リスクマネジメントについては、３回目以降のリスク評価の対象を全国の大会会場がある自治体等に拡大するとともに、並行して横断的なリスク評価についても実施し、適切に対策の促進につなげていく等の取組が必要。

また、「サイバーセキュリティ対処調整センター」については、構築を2018年度内に完了し、限定的に運用を開始できるように運用要領等の検討・策定、要員の訓練等を行っていくことが必要。

資料２－２

サイバーセキュリティ政策に係る年次報告
（2017年度）（案）

2018年　月　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

Ⅰ　2017年度のサイバーセキュリティに関する情勢 2

１　我が国を取り巻くサイバーセキュリティに関する情勢 2

２　政府機関等におけるサイバーセキュリティに関する情勢 6

(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 6

(2)　2017 年度における政府機関等に対するサイバー攻撃等による情報セキュリティインシデントの傾向 8

Ⅱ　サイバーセキュリティ関連施策の取組実績 14

１　サイバーセキュリティ戦略について 14

２　主な政策の取組実績 16

(1)　経済社会の活力の向上及び持続的発展 16

(2)　国民が安全で安心して暮らせる社会の実現 17

(3)　国際社会の平和・安定及び我が国の安全保障 24

(4)　横断的施策 28

(5)　推進体制 30

Ⅲ　サイバーセキュリティ関連施策の評価 31

１　経済社会の活力の向上及び持続的発展 31

(1)　安全な IoT システムの創出 31

(2)　セキュリティマインドを持った企業経営の推進 31

(3)　セキュリティに係るビジネス環境の整備 32

２　国民が安全で安心して暮らせる社会の実現 32

(1)　国民・社会を守るための取組 32

(2)　重要インフラを守るための取組 33

(3)　政府機関を守るための取組 34

３　国際社会の平和・安定及び我が国の安全保障 35

(1)　我が国の安全の確保 35

(2)　国際社会の平和・安定 35

(3)　世界各国との協力・連携 36

４　横断的施策 37

(1)　研究開発の推進 37

(2)　人材の育成・確保 37

５　推進体制 38

別添１　各府省庁における情報セキュリティ対策に関する取組 39

別添２　「サイバーセキュリティ2017」に盛り込まれた施策の実施状況 65

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取組等 115

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 . 163

別添５　用語解説 229

はじめに

サイバー空間が経済社会の活動基盤となり人々の生活に恩恵をもたらす一方、サイバー空間がもたらす利益を損なう活動も増加してきている。2017年５月には、ランサムウェアによる被害が我が国を含め世界的規模で発生し、多くの企業や人々の活動に支障を与えた。さらに、国家の関与が疑われるような組織的かつ高度な攻撃手法の登場が、国民生活・経済社会活動に重大な被害を生じさせ、また影響を及ぼしており、我が国の安全保障に対する脅威も年々高まってきている。また、サイバー空間と実空間（フィジカル空間）の一体化の進展に伴い、脅威が更に深刻化・巧妙化することが予想される。

こうした状況の中、我が国においては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、2015年９月に「サイバーセキュリティ戦略」（以下「2015年戦略」という。）を閣議決定し、2015年戦略に基づく３期目の年次計画である「サイバーセキュリティ2017」によって施策を推進してきたところである。

本報告は、2017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2017」に掲げられた施策の実施状況等について取りまとめたものである。本編に記載のとおり、2017年度において特記すべき点としては、①セキュリティ研究開発のための取組の強化（サイバーセキュリティ研究開発戦略の策定等）、②次期サイバーセキュリティ戦略策定に向けた検討、③官民の多様な主体がサイバーセキュリティに資する情報を安心して共有できるようにするための仕組みに関する検討（サイバーセキュリティ基本法の一部を改正する法律案の閣議決定）などが挙げられる。

政府としては、我が国のサイバーセキュリティをより一層確固たるものにするため、本報告における施策評価等を踏まえ、サイバーセキュリティ関連施策の強化・加速を進めるとともに、次期サイバーセキュリティ戦略及び同戦略に基づく年次計画を策定し、これを着実に推進することとする。

Ⅰ　2017年度のサイバーセキュリティに関する情勢

1　我が国を取り巻くサイバーセキュリティに関する情勢

(1) サイバー攻撃はより深刻化・巧妙化し被害も拡散

2017年度は、ランサムウェアによる被害が世界中で発生した。また、新たな脆弱性を悪用したマルウェアや、様々な感染手法を用いたサイバー攻撃が確認された。サイバー攻撃以外にも、システムの不適切な管理や災害等に起因するIT障害が発生した。スマートフォンやIoTの普及及びFintechや仮想通貨の利用拡大もあり、サイバー空間の安全確保がますます国民生活にとって身近な課題となっている。

2017年３月、Javaのウェブアプリケーションフレームワーク「Apache Struts2」において任意のコードを実行できる脆弱性[1]が公表された。その後、当該脆弱性を悪用した不正アクセスにより、官公庁、重要インフラ事業者、通販サイト、テレビ局等、国民生活に密接に関係する様々なウェブサイトから個人情報等の漏えい事案が発生した。海外でも同様の被害が多数発生しており、米国の信用情報サービス会社のウェブサイトからは１億人を超える個人情報が漏えいした[2]。

2017年４月、「The Shadow Brokers」と名乗る集団により攻撃ツールセットが公開され、その中にはMicrosoft Windowsを標的とした「EternalBlue」、「DoublePulsar」が含まれていた。同年５月、当該攻撃ツールを悪用して作成されたランサムウェア「WannaCry」が世界的に大流行し、英国の病院では、医療行為に支障が発生する等の被害が発生したが、日本国内では人命や重要なサービスに影響を及ぼす被害は確認されなかった。同年６月、ランサムウェア「NotPetya」、同年10月、ランサムウェア「Bad Rabbit」によりウクライナの空港及び鉄道のシステム等に障害が発生したと報じられた。これらのランサムウェアは、ネットワーク接続したPCや制御装置等のIoT機器間で急速に感染が拡大することから、短時間で広範囲に被害が拡散した。同年12月20日、菅内閣官房長官は「WannaCry」の流行について、記者会見で「事案の背後に北朝鮮の関与があった」と述べた。

「WannaCry」の亜種はいまだに流行を続けており、内閣官房内閣サイバーセキュリティセンター（NISC）において亜種の一つを入手し動作を解析したところ、この亜種はファイルを暗号化し脅迫画面を表示するというランサムウェアとしての動作をせず、感染拡大のみを続けるというワームとしての動作をするものであった。セキュリティ対策が十分でない端末を、ファイアウォールを経由せずにインターネットに接続した結果このような亜種に感染した場合、脅迫画面を表示するといったランサムウェアとしての動作をしないために感染に気づかず、その端末を起点とした組織内部への感染拡大が懸念される。

2018年１月、国内の仮想通貨交換業者から多額の仮想通貨が不正に送信されたと見られる事案が発生した。他の仮想通貨等へ交換されたとみられる。また、他の仮想通貨交換業者に対して、金融庁は立入検査等を実施し、複数の仮想通貨交換業者へ行政処分を行った[3]。

---

[1] https://www.ipa.go.jp/security/announce/struts2_list.html
[2] https://equifaxsecurity2017.com
[3] https://www.fsa.go.jp/policy/virtual_currency02/index.html

仮想通貨を巡っては、流出のみではなく、感染したPCのCPU等の計算処理能力を利用して仮想通貨をマイニングするマルウェアの出現、仮想通貨がランサムウェアの身代金支払い手段として利用される等、サイバー攻撃者に悪用される事例が見受けられる。

2018年２月、2018年平昌オリンピック・パラリンピック競技大会（以下「2018年平昌大会」という。）において、大会運営用のシステムがサイバー攻撃の影響によって停止した等の報道があった。大規模な国際大会がサイバー攻撃の標的となる可能性を示した。

メールを用いてマルウェアを標的となる組織に送り付ける標的型攻撃については、2017年も引き続き増加している[4]。

その手口としては、金融機関等を装ったメールを送り、住所、氏名、銀行口座番号、クレジットカード番号等の個人情報を詐取したり、配送会社による再配達の連絡等を装い同様に個人情報を詐取したりする等、様々な手法が確認されている。

また、メールに添付されたファイルの形式については、圧縮ファイル、Word文書及びExcel文書が多数を占めた。これらの中には、DDE機能や数式エディタ等、現在ではあまり使用されずに残置された機能の脆弱性を悪用したものが確認されている。

スマートフォンアプリを狙ったサイバー攻撃も発生した。人気ゲームの攻略法を解説するガイドアプリに仕込まれたマルウェア、不正アプリをインストールすることで個人情報の漏えいやDDoS攻撃の踏み台となる等、スマートフォンにも様々な脅威が確認されている[5]。

2016年に出現したボットネット「Mirai」やその亜種により、ボット化したIoT機器等からDDoS攻撃が頻繁に行われるようになった。2017年のサイバー攻撃関連通信を宛先ポート番号・プロトコル別に集計した結果によれば、IoT機器が使用するポート番号が半数以上を占め、IoT機器を狙った攻撃であると推測される。

図表Ⅰ－１－１：宛先ポート番号別の年間観測パケット数割合[6]

ポート番号	攻撃対象
23/TCP	IoT機器（Webカメラ等）
22/TCP	IoT機器（モバイルルータ等） 認証サーバ（SSH）
445/TCP	Windows（サーバサービス）
2323/TCP	IoT機器（Webカメラ等）
5358/TCP	IoT機器（Webカメラ等）
7547/TCP	IoT機器（Webカメラ等）
1900/UDP	IoT機器（ホームルータ等）
1433/TCP	データベースサーバ（SQL）
443/TCP	Webサーバ（SSL/TLS）
80/TCP	Webサーバ（HTTP）

[4] https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf
[5] https://www.ipa.go.jp/files/000065376.pdf
[6] http://www.nict.go.jp/cyber/report/NICTER_report_2017.pdf

2018年２月、米国ソフトウェア開発者向けブログに対して、memcachedを悪用したDDoS攻撃[7]があり、過去最大の1.35Tbpsのトラフィックが確認された。さらに、2018年３月、米国サービスプロバイダーに対して、同様のDDoS攻撃により、最大1.7Tbpsのトラフィックが確認された。

我が国の政府機関、公共交通機関、水族館等のウェブサイトに閲覧障害が生じる事案が発生した。国際的ハッカー集団「アノニマス」を名乗る者が、65組織に関して、サイバー攻撃を実行したとする犯行声明とみられる投稿を、SNS上に掲載している状況が把握された[8]。

サイバー犯罪の低年齢化も問題視されている。例えば、2017年６月、14歳の少年がランサムウェアを作成した容疑で警察に逮捕された。また、マルウェア入手方法等の情報をフリーマーケットアプリに出品したとして13歳の少年が児童相談所に通告された。2017年に不正アクセス禁止法違反で検挙又は補導された者は、13歳から60歳まで幅広い年齢層にわたっている[9]。2017年12月、神奈川県では９歳から11歳の児童３人がマルウェアの作成等をしたとして児童相談所に通告された。

サイバー空間における事案の発生は、サイバー攻撃に限らない。例えば、2017年８月、日本国内の複数のインターネット接続サービスが相次いでつながりにくくなる大規模な通信障害が発生したが、原因は米国の大手インターネット関連事業者による経路制御情報の設定ミスによるものであった。また、2017年11月、複数の空港において通信施設に障害があり、航空便に多数の欠航等が発生したが、これは電源供給装置の不具合による電源供給ストップが原因であった[10]。こうしたトラブルは初動において原因がサイバー攻撃か否か判然とせず、大局的視点に立った合理的な判断や対応が可能となるよう、従前よりトレーニングやシミュレーションを重ねておく必要がある。

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「ビジネスメール詐欺」も発生した。2017年12月、大手航空会社が、偽の請求書メールにより、航空機リース料等の支払い要求に応じ、３億円を超える詐欺被害に遭った。

影響が懸念される新たな脆弱性や欠陥についての発見・公表も複数された。2017年10月、WPA2プロトコルの脆弱性を突く「KRACKs」と呼ばれる攻撃に関するアラートが公表された[11]。当該脆弱性が悪用された場合、無線LANの通信範囲に存在する第三者により、WPA2通信の盗聴が行われる可能性がある。2018年１月、CPUに起因する問題が公表[12]され、「Meltdown/Spectre」に対してCPUメーカーやソフトウェアメーカーが相次いで対応方針を発表する事態となった。

2017年度は一層深刻化・巧妙化したサイバー攻撃により、多くの被害が発生したが、他方、OS・ソフトウェアの更新やセキュリティソフトの導入、パスワードの適切な管理、適切なアクセス権の設定等、基本的な事項を遵守していれば防ぐことが可能であった事案も少なからず見受けられた。これらを踏まえれば、今一度基本に立ち返り、システム管理者や利用

[7] https://www.jpcert.or.jp/at/2018/at180009.html
[8] https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf
[9] https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf
[10] http://www.akita-airport.com/pages/news/p2023
[11] https://www.us-cert.gov/ncas/current-activity/2017/10/16/CERTCC-Reports-WPA2-Vulnerabilities
[12] https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

者が、それぞれの立場で、サイバー空間における様々な情報を正しく理解し、対策状況や影響・リスクを把握した上で、実施可能な対策を確実に実施することが重要である。

(2) 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。サイバー空間に関する国際的なルールや規範について、G7、GCSC[13]等閣僚によるハイレベル会合や、国連政府専門家会合その他の実務レベルにおける多国間協議・二国間サイバー協議等において議論が進められている。サイバー空間における国際法の適用の在り方、国際規範の形成、インターネットのガバナンスを巡っては、我が国と同様に情報の自由な流通、開放性、多様な主体の連携を求める立場がある一方で、サイバー空間の規制や国家による管理を強化する立場をとる動きも見られる。

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た。

欧州連合（EU）は、サイバー攻撃時の外交による対応を念頭にしたサイバー外交ツールボックス（2017年６月）、サイバーセキュリティ強化に向けた政策パッケージ、ENISA[14]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案（同年９月）、IoTセキュリティベースラインの勧告（同年10月）等を公表する等、サイバーセキュリティ関連の政策を強化している。また、2018年５月に、一般データ保護規則（GDPR）[15]が施行されるとともに、同月までに、NIS指令[16]を加盟国において国内法化することを義務づけている。

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[17]に署名した。関係米政府機関は、大統領令に基づいてサイバーセキュリティ強化施策等を報告することとされている[18]。

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、G7が2017年４月G7ルッカ外相会合の外相共同コミュニケ及び「サイバー空間における責任ある国家の行動に関するG7（ルッカ）宣言」において、国際違法行為を行った国家に対して均衡性のある対抗措置をとり得ることを確認した。他方、第５次国連政府専門家会合（GGE）[19]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。

---

[13] The Global Commission on the Stability of Cyberspace
[14] 欧州ネットワーク・情報セキュリティ機関（European Network and Information Security Agency）
[15] 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)
[16] 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
[17] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
[18] https://www.whitehouse.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/
[19] 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。

こうした情勢において、我が国は、自由、公正かつ安全なサイバー空間を堅持するため、米国、英国、豪州その他の国々との二国間協議のほか、「G7伊勢志摩サイバーグループ」等の多国間の会議に参加し、サイバー空間における法の支配の推進や国際連携に積極的に取り組んでいる。

2　政府機関等におけるサイバーセキュリティに関する情勢

(1) 政府機関等[20]におけるサイバーセキュリティに関する体制

政府機関におけるサイバーセキュリティ対策については、NISC及び各府省庁が、また、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。）におけるサイバーセキュリティ対策については、独立行政法人情報処理推進機構（IPA）[21]及び独立行政法人等が、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体制を構築して実施している。（図表Ⅰ－２－１）。

図表Ⅰ－２－１　政府機関等における情報集約・支援体制の枠組み

このような体制の下、政府機関等横断的な立場からサイバーセキュリティ対策を推進するため、2008年４月から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[22]）を、また、2017年４月から独立行政法人等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、24時間365日体制の下、サイバー攻撃等の不審な通信の

[20] 本章では、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並びにオブザーバ機関を総称して「政府機関等」という。

[21] 「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」（2016年１月のサイバーセキュリティ戦略本部決定）及び2016年４月に成立したサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成28年法律第31号）等を踏まえ、NISCの監督の下、独立行政法人情報処理推進機構（IPA）において、その有する技術的能力及び専門的な知識経験等の知見を活用し、独立行政法人等に対する監視体制を構築することとなった。

[22] GSOC（Government Security Operation Coordination team）

横断的な監視、分析、情報収集を実施するとともに、各組織への通報、情報提供などを行っている（図表Ⅰ－２－２）。

図表Ⅰ－２－２　GSOCの概要

また、NISCでは、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[23]）を派遣し、技術的な支援・助言を実施している。

一方、各府省庁や独立行政法人等においては組織内CSIRT[24]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。

[23] CYMAT（CYber incident Mobile Assistance Team）
[24] CSIRT（Computer Security Incident Response Team）

(2) 2017年度における政府機関等に対するサイバー攻撃等による情報セキュリティインシデントの傾向

政府機関等において発生した情報セキュリティインシデント[25]の主な要因は、「外部からの攻撃」によるものと「意図せぬ情報流出」によるものに大別される。

2017年度も、前年度と同様に職員の過失等によ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も散見されたが、年間を通してウェブアプリケーションの脆弱性を悪用した攻撃が頻発した。

以下に、2017年度の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について、情報セキュリティインシデントの主な要因ごとにその傾向を示す[26]。

①　外部からの攻撃に係る情報セキュリティインシデント

(ア)政府機関等への脅威動向について

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、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。

2017年度に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の件数（以下「確認を要するイベント検知件数」という。）[27]は、6,677件であった（図表Ⅰ－２－３）。2017年度の第一GSOCにおける確認を要するイベント検知件数の推移を見ると、既知の脆弱性に対する攻撃や調査段階の通信が減少し始めているのに対し、新たな脆弱性情報の悪用を含む様々な攻撃が行われており、引き続き十分な警戒を要する状況である[28]。

---

[25] 情報セキュリティに関する望まない又は予期しない事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（「別添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2017年度の情報セキュリティインシデント一覧」を参照。

[26] 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、これまで第２期GSOCシステムで検知・解析を行っていた件数とは比較できなくなっている。

[27] 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検知件数」を指標とすることとした。この「確認を要するイベント検知件数」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の件数である。

[28] 第二GSOCは、2017年度に運用を開始して間もないため、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調整中であることから、約27万件と高い値となっている。

図表Ⅰ－２－３　確認を要するイベント検知件数の推移

（イ）政府機関等に対する攻撃の傾向について

第一GSOCと第二GSOCにおけるセンサー等による監視活動において、不審な通信やWebサイトの障害等（疑いを含む）の事象を検知した際には、これを分析し、必要に応じ当該政府機関等への通報を行っており、2017年度においては、第一GSOCでは133件の通報を行っている[29]（図表Ⅰ－２－４）。

図表Ⅰ－２－４　GSOC センサー監視等による通報件数の推移

第一GSOCにおける外部からの攻撃に対する通報件数の内容について見ると、脆弱性を狙った攻撃としてウェブアプリケーションの脆弱性を悪用した攻撃に係る通報が多い。これは、脆弱性情報の公開直後に当該脆弱性を狙って攻撃されるケースが増えているためであり、脆弱性に対して迅速にパッチを適用して対処する等、対象システムの資産管理を確実に実施す

[29] GSOC では、センサー等の監視活動により検知された事象を分析した結果、攻撃が行われたと認識され、当該政府機関等において対応が推奨される事案について、通報を行っている。なお、第二 GSOC は、2017 年度に運用を開始して間もないため、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、2,618 件と通報件数が多くなっている。

ることが必要になってきている。また、メールによる標的型攻撃[30]の通報も多く、警戒が必要と考えられる（図表Ⅰ－２－５）。

図表Ⅰ－２－５　第一GSOCでの外部からの攻撃に対する通報件数における各種攻撃の割合（概要）

第二GSOCにおける外部からの攻撃に対する通報件数の内容については、対象機関の特性を踏まえた詳細な分析に基づき、通報の実施に係る判断基準を一層調整する必要がある状況ではあるが、SQLインジェクションの脆弱性を狙った攻撃に係る通報が多い。また、攻撃の特徴として、クロスサイトスクリプティングや、非公開のファイルを読み取るコマンドの実行といった複数の攻撃が同時に行われていることもあった。

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、2017年度においてはGSOCから878件の注意喚起を行った（図表Ⅰ－２－６）。

図表Ⅰ－２－６　不審メール等に関する注意喚起の件数の推移

[30] 不正プログラムが添付されていたり、不正プログラムが仕込まれた Web サイトへのリンクが記載されていたりする不審メール。

この注意喚起の件数は2016年度に比して2017年度は減少しているように見えるが、これは検体が同一である等の理由で既に注意喚起した不審メールと同種と考えられる不審メールに関しては注意喚起を行わない等、真に必要な注意喚起のみを行うこととしていることの結果と考えられ、必ずしも政府機関等に対する不審メールを送付するような攻撃が少ないことを意味しているものではない。むしろ真に必要な注意喚起のみを行っているにもかかわらず、依然として注意喚起の件数は一定数を維持しており、マルウェアの高度化が進む中、メール文面についても自然な日本語や実在する職員の名前が用いられるなど巧妙化してきている。一方で、暗号化通信の特性を悪用した攻撃もあることから留意しておく必要がある。

コラム　～不審メールの傾向～

○政府機関等に対する不審メールの傾向

図表Ⅰ－２－７は、GSOCに提供された政府機関等に対する不審メールの傾向を示したものである。2017年度は2016年度と比較して不審なファイルが添付されたメール（以下「ファイル添付型」という。）の比率が減少し、不審なURLが記載されたメール（以下「URL型」という。）の比率が増加した。URL型は、記載されたURLにアクセスすると不審なファイルがダウンロードされるものが多いが、メールに記載されたURLだけではセキュリティ機器が悪性と判断することが難しい。一方、ファイル添付型は、セキュリティ機器が添付ファイルをスキャンし悪性であると判断できれば、受信者に不審メールが届く前に検知される。こういったことから、URL型が増加したと考えられる。不審なURLへのアクセスに対して、メールをテキスト形式で表示する機能の活用を始めとした対策や、記載されたURLに受信者が不注意にアクセスしないよう周知することが重要である。

図表Ⅰ－２－７　不審メールの傾向

○政府機関等に対する不審メールで使用されたファイルの形式

GSOCで解析した不審なファイルの形式については、URL型でダウンロードされるものとファイル添付型を合わせると、2017年度は約半数がOffice形式のファイルであった。これらのOffice形式のファイルについては、利用者がマクロを有効化すると悪性のマクロが動作し、インターネットから更なるマルウェアをダウンロードするものが散見された。この手法は以前から存在するものであるが、2017年度には、マクロを有効化したタイミングではなく、フ

ファイルを閉じたタイミングで悪性の動作をするといった工夫をしたものも見られた。これは、セキュリティ製品による検知を妨害する目的があると考えられ、マクロを用いる手法は巧妙化している。また、マクロ以外についても、これまで危険性の面で注目されることが少なかったCSVファイルを開いた際に、Officeの各種の機能を用いてマルウェアに感染させる手法も登場している。このように、マクロを含むOfficeの各種の機能は攻撃者に悪用されることがあるため、不用意に有効化しないことについても注意が必要である。

(ウ)ソフトウェアの脆弱性情報の傾向について

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。2017年度においては、第一GSOCから161件（図表Ⅰ－２－８）、第二GSOCより116件の脆弱性情報等を配信した。

図表Ⅰ－２－８　第一 GSOC が配信したソフトウェアの脆弱性情報等の件数の推移

脆弱性を悪用した攻撃の代表的なものとしては、Webサイトの改ざんが挙げられる。GSOCにおける監視活動においても、Webサイトに対する脆弱性を悪用しようとする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。

(エ)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、依然として脅威は低下しておらず、むしろ攻撃が効率的に行われるようになっていると考えられる。また、センサー等で検知した政府機関等に対する不審な通信からは、脆弱性の公開に合わせた攻撃や、執拗な攻撃のほか、なりすましと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わかった。その結果、注意喚起を行った件数も決して少なくない状況であり、政府機関等に対する攻撃は深刻度を増していると言える。

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、深刻化が進む政府機関等へのサイバー攻撃に対し、引き続き迅速に対応していくこととしている。

②　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

2017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。

記憶媒体の紛失や、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、サーバのアクセス制限の設定ミスにより個人情報が外部から閲覧可能になっていた事案などが発生している。

Ⅱ　サイバーセキュリティ関連施策の取組実績

ますます深刻化・巧妙化しているサイバー攻撃に対応するなど、サイバーセキュリティに係る取組の推進は、安全保障・危機管理の観点から、また、我が国経済の成長を促進する観点からも、必要不可欠であることから、政府はサイバーセキュリティ基本法第12条に基づき、サイバーセキュリティ政策を俯瞰した中長期戦略である、「サイバーセキュリティ戦略」　（2015年９月４日閣議決定。以下「2015年戦略」という。）を策定した。

2015年戦略の期間は策定後３年とされており、2017年度においては、2015年戦略に基づく最終年度の年次計画である「サイバーセキュリティ2017」（2017年８月25日サイバーセキュリティ戦略本部決定）を策定し、これに沿ってサイバーセキュリティ政策を推進してきた。以下、2015年戦略及び今後閣議決定予定の「サイバーセキュリティ戦略（以下「2018年戦略」という。）」について概説した後、2017年度の主たる取組実績を概説する。

１　サイバーセキュリティ戦略について

2015年戦略は、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。）の開催、そしてその先の2020年代初頭までの将来を見据えつつ、策定から３年程度のサイバーセキュリティ政策の基本的な方向性を示すものであると同時に、関係者の共通の理解と行動の基礎となるものである。2015年戦略では、自由、公正かつ安全なサイバー空間を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与することを目的としている。これら３つを主要な政策分野とし、その基盤となる研究開発や人材育成を「横断的施策」として、経済や安全保障に係るものも含めた総合的なサイバーセキュリティ政策を推進する構造となっている。

また、2017年は2015年戦略の期間の終期や改正サイバーセキュリティ基本法の見直し期限（それぞれ2018年9月）まで1年余りを迎えることから、2020年東京大会に向けた抜本的対策を見据えた取組を行う必要がある。そこで、サイバー攻撃の複雑化といった脅威の動向の変化等を踏まえ、これまでの対策の延長線上での検討では必ずしも十分ではないことが考えられることから、サイバーセキュリティに関する様々な課題として更なる取組が必要と考えられる施策について、サイバーセキュリティ戦略本部において検討し、「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。）を策定した。

さらに、「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）を策定し、サイバーセキュリティ戦略本部において2018年戦略に係る検討を開始した。2018年戦略は、2015戦略策定後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である。

図表Ⅱ－１－１　2015年戦略中間レビューの概要

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（概要）
－サイバーセキュリティ戦略中間レビュー－(平成27年７月13日サイバーセキュリティ本部決定)

■ 現行戦略策定後の脅威動向等の認識を踏まえ、加速・強化すべき施策を取りまとめ、急ぎ対応が必要と考えられるものから実施（必要な制度面の見直し等を含む。）。
■ 今後は、本レビューを踏まえ、（必要な制度面の見直しも含め）可能な施策から段階的に実施（1年以内）

脅威等の変化

- IoT機器を踏み台にしたサイバー攻撃の顕在化
- 省庁・分野を越えた情報共有の必要性
- 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抜本的対策を見据えた取組の必要

ボット（注）撲滅の推進

■ 効率的かつ効果的な対策につなげるため、官民が連携し、実態の把握、対策の実施・周知、再発防止・環境改善を一体的に実施
- 政府内に体制を構築して継続的かつ広範な実態調査ができるよう、必要な法的整理
- 電気通信事業者等の協力を得た利用者等の特定・注意喚起等の対策の実施、周知（必要な技術的・制度的枠組の構築）
- 迅速な対処の協力の要請（製造事業者・販売事業者等）
- 諸外国との連携を促進し、協調した対策を実施。

情報共有・連携ネットワーク（仮称）の構築・運用

■ 官民が連携し、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により、サイバー攻撃の被害及び被害拡大を防止
- 効果的な情報連携体制を構築する制度整備。
  - ✓ 情報へアクセス権限を有する民間事業者の責務、官側の役割等
  - ✓ 情報提供を行う際の阻害要因に対処
- 情報提供者にとって提供しやすく、かつ利用者にとって対策しやすい情報の抽出及び環境の整備。
  - ✓ 事案に応じた提供内容をあらかじめ設定し、対策に効果的な内容を適切なタイミングで共有。

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体制の整備

■ 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）の構築（2018年度末目途）
- 組織委員会に対する適切な助言・支援が行えるよう、東京オリンピック競技大会・東京パラリンピック競技大会推進本部との連携等、制度的枠組の検討。
- 一定程度の専任要員（計画的に訓練）
- 200人以上の技術者等（重要サービス事業者、セキュリティ事業者等）との連携態勢。

■ セキュリティ情報センターの構築
- 安全に係る情報を集約、分析・評価を行い、関係機関等に対し必要な情報を随時提供

■ リスクマネジメントの促進
- 横断的リスク評価（2018年度までに全分野で実施）に基づくマネジメントを強力に推進
- 特に影響度が大きい重要サービス事業者について、鳥瞰図的な把握及び検証、リスクの確認及び対策を推進

経済社会の活力の向上及び持続的発展

- 安全なIoTシステムの創出による国際競争力の強化（国際標準化）［関係分野の用語・設計・開発等の概念を共通化する国際標準の策定］
- セキュリティに係るビジネス環境の整備［セキュリティ規格に関する要件の策定、セキュリティに係る損害保険の普及の支援］

国民が安全で安心して暮らせる社会の実現

- 深刻度判断基準の策定等によるサイバー攻撃対処態勢の強化［コンティンジェンシープラン策定の支援］
- 政府機関・独法等における効率的・効果的防護体制の再構築［検知精度・対処能力等の監視能力の向上、情報システムの侵入耐性診断時の自衛隊能力の活用］
- 地方公共団体におけるセキュリティ対策向上［セキュリティ人材・体制の確保充実の支援］
- 大学等における情報セキュリティ対策の向上［大学等の相互協力による取組、情報システムの侵入耐性診断実施支援］
- サイバー犯罪・サイバー攻撃対策の強化
- 普及啓発・情報発信［迅速な情報発信・相談対応のための取組強化］

国際社会の平和・安定及び我が国の安全保障

- 組織・分野 横断的な取組等による我が国の安全の確保
- 国立研究開発法人における先端技術の防護のための情報セキュリティ対策の強化
- 海外の多様な主体との多層的な連携の強化
- サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

- 経営層の意識改革や、橋渡し人材等幅広い階層における人材育成・確保の継続的な促進
- 研究開発等の推進

図表Ⅱ－１－２　2018年戦略の概要

「サイバーセキュリティ戦略（案）」の全体概要

中長期的

1　策定の趣旨・背景
1．1．　サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）
1．2．　2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2　サイバー空間に係る認識
2．1．　サイバー空間がもたらす恩恵
・人工知能（AI）、IoTなどサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。様々な分野で当然に利用され、人々に豊かさをもたらしている。
2．2．　サイバー空間における脅威の深刻化
・技術等を制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3　本戦略の目的
3．1．　基本的な立場の堅持
（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）
3．2．　目指すサイバーセキュリティの基本的な在り方
（1）目指す姿（持続的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）（2）主な観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）

戦略期間

4　目的達成のための施策

経済社会の活力の向上及び持続的発展
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
<施策例>・経営層の意識改革の促進（「費用」から「投資」へ）
・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）
・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化
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
<施策例>・中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定
3．安全なIoTシステムの構築
<施策例>・IoTシステムにおけるセキュリティの体系の整備と国際標準化
・IoT機器の脆弱性対策モデルの構築・国際発信
等

国民が安全で安心して暮らせる社会の実現
1．国民・社会を守るための取組
<施策例>・脅威に対する事前の防御（積極的サイバー防御）策の構築
・サイバー犯罪への対策
2．官民一体となった重要インフラの防護
<施策例>・安全基準等の改善・浸透（サイバーセキュリティ対策の関係法令等における保安規制としての位置付け）
・地方公共団体のセキュリティ強化・充実
3．政府機関等におけるセキュリティ強化・充実
<施策例>・情報システムの状態のリアルタイム監理の強化
・先端技術の活用による先取的対応への挑戦
4．大学等における安全・安心な教育・研究環境の確保
<施策例>・大学等の多様性を踏まえた対策の推進
5．2020年東京大会とその後を見据えた取組
<施策例>・サイバーセキュリティ対処調整センターの構築の推進
・成果のレガシーとしての活用
6．従来の枠を超えた情報共有・連携体制の構築
<施策例>・多様な主体の情報共有・連携の推進
7．大規模サイバー攻撃事態等への対処態勢の強化
<施策例>・実空間とサイバー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
等

国際社会の平和・安定及び我が国の安全保障
1．自由、公正かつ安全なサイバー空間の堅持
<施策例>・自由、公正かつ安全なサイバー空間の理念の発信
・サイバー空間における法の支配の推進
2．我が国の防御力・抑止力・状況把握力の強化
<施策例>・国家の強靭性の確保
（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する抑止力の向上
（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の状況把握の強化
（①関係機関の能力向上、②脅威情報連携）
3．国際協力・連携
<施策例>・知見の共有・政策調整
・事故対応等に係る国際連携の強化
・能力構築支援
等

横断的施策

人材育成・確保	<施策例>戦略マネジメント層の育成・定着、実務者層・技術者層の育成（高度人材含む）、人材育成基盤の整備、政府人材の確保・育成の強化、国際連携の推進
研究開発の推進	<施策例>実践的な研究開発の推進（検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備）、AI等中長期的な技術・社会の進化を視野に入れた対応
全員参加による協働	<施策例>サイバーセキュリティの普及啓発に向けたアクションプランの策定、国民への情報発信（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5　推進体制
本戦略の実現に向け、サイバーセキュリティ戦略本部の下、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、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。また、危機管理対応についても一層の強化　等

２　主な政策の取組実績

(1)　経済社会の活力の向上及び持続的発展

①　安全な IoT システムの創出

到来しつつある連接融合情報社会において、あらゆるモノがインターネットに接続されて新たなサービスが利用可能になるIoTシステムにおいては、高いレベルでのセキュリティ品質を確保することが必要となる。市場ニーズに応える安全なIoTシステムを実現し、我が国のIoTシステムの国際的評価を高めることを目指し、以下の取組等を実施した。

NISCにおいては、「サイバーセキュリティ関係施策に関する平成30年度予算重点化方針」（2017年8月25日サイバーセキュリティ戦略本部決定）にて、「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」[31]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。

さらに、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[32]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」を基本とした国際標準化活動を推進した。2017年11月のニューデリー会合にて日本提案を説明し、2018年2月より新規作業項目提案に向けたプロセスを進めている。

②　セキュリティマインドを持った企業経営の推進

NISCでは、企業におけるサイバーセキュリティに係る情報開示や人材配置等の実態について把握するための調査を行い、「企業のサイバーセキュリティ対策に関する調査報告書」[33]として公表した。

また、「企業経営のためのサイバーセキュリティの考え方」[34]（2016年８月２日）の見直しを念頭に、「セキュリティマインドを持った企業経営WG」において、①経営層が持つべき意識や果たすべき役割、②経営層がリスクマネジメントの一つとしてサイバーセキュリティの取組を進めていく上での具体的な方策、③中小企業を始めとする事業上のリソースの制約が大きい企業の対策、④産学官連携による取組について検討を実施し、報告書として取りまとめた。

③　セキュリティに係るビジネス環境の整備

我が国のIoT産業を含む情報通信技術を利活用した関連産業が国際競争力を有し、経済をけん引していくとともに、自立的にサイバーセキュリティの確保を行う能力を有していくためには、我が国においてサイバーセキュリティ関連産業が成長産業となるよう、必要な環境整備を行い、あらゆるビジネスの基盤となる公正な市場環境の整備を行う必要がある。このため、我が国の企業のセキュリティ確保及び国際競争力強化の基盤となるビジネス環境の整備に向けて、以下の取組等を実施した。

---

[31] https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
[32] Joint Technical Committee 1 Sub Committee 41 (Title:Internet of Things and related technologies)
[33] https://www.nisc.go.jp/inquiry/pdf/kigyoutaisaku_honbun.pdf
[34] https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

国際標準化の推進に関して、経済産業省では、専門機関と連携し、日本が主体となって、ISO/IEC JTC1 SC27/WG4[35] にIoTセキュリティガイドラインをベースとしたIoTセキュリティ規格を提案し、国際標準化を推進した。

また、IPAにおいても、SC27のWG2コンビーナ、WG3副コンビーナ（2017年４月ハミルトン会合、2017年10月ベルリン会合）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。さらにWG2については、日本技術の規格化作業を支援し、弱い秘密に基づく匿名エンティティ認証（ISO/IEC20009-4[36]）、公開鍵暗号(ISO/IEC18033-2/AMD1[37])、秘密分散メカニズム（ISO/IEC19592-2[38]）の規格を出版した。

財政投融資制度に関して、経済産業省では、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した。また、中小企業投資促進税制においては、セキュリティ製品等への税制措置を継続している。

文化審議会著作権分科会において、リバースエンジニアリングのための著作物の利用その他のニーズを踏まえた権利制限規定の在り方について、2017年4月に報告書を取りまとめた。これを踏まえ、リバースエンジニアリングのための著作物の利用を含む権利者の利益を不当に害しない一定の著作物の利用を許諾なく行えることとする権利制限規定等の整備を行う著作権法改正法案を、2018年2月に国会に提出した。

(2)　国民が安全で安心して暮らせる社会の実現

①　国民・社会を守るための取組

国民・社会がサイバー空間に起因する脅威にさらされないようにするためには、その利用環境が安全なものとなるよう、サイバー空間を構成する機器やサービスが安全かつ安定的に提供され続けることが不可欠である。

利用者たる個人や企業・団体が、自ら進んで意識・リテラシーを高めることも不可欠であり、２月１日～３月18日にNISCが中核となり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行う「サイバーセキュリティ月間」を実施した。「サイバーセキュリティは全員参加！」をキャッチフレーズに、普及啓発イベントやテレビアニメ「BEATLESS」とのタイアップ等を官民連携して実施した。

特に2018年は、NISCから全府省庁に改めて協力を呼びかけ、政府一体となって更に拡大して取り組み、全国で官民による計189件の関連行事を実施した。

NISC主催の取組では、2018年２月１日にキックオフサミットを開催し、各地域で活躍する普及啓発団体の取組紹介や啓発活動に関する課題について議論等を行った。本イベントの模様はインターネットで全国配信を行い、１万回以上のアクセス数を達成した。

---

[35] Joint Technical Committee 1 Sub Committee 27 Working Group 4 (Title:Security controls and services)
[36] Information technology-Security techniques-Anonymous entity authentication-Part 4:Mechanisms based on weak secrets
[37] Information technology-Security techniques-Encryption algorithms-Part 2:Asymmetric ciphers AMENDMENT 1
[38] Information technology-Security techniques-Secret sharing-Part 2:Fundamental mechanisms

図表Ⅱ－２－１「サイバーセキュリティ月間」キックオフサミットの様子（2018年２月１日開催）

2018年３月４日には、幅広く国民のサイバーセキュリティに関する意識向上を図るため、官民連携によるイベント「アナログハックを目撃せよ！2018」を実施した。本イベントにおいては、テレビアニメ「BEATLESS」とのタイアップコンテンツを中心としたステージやサイバー攻撃の実演、関係機関による展示ブース等を行い、2,000名以上の来場者があった。

図表Ⅱ－２－２　「アナログハックを目撃せよ！2018」の様子（2018年３月４日開催）

また、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て情報共有を図り、必要な対策等について協議を行うための協議会を創設する等の措置を講じるため、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第196回国会に提出した。

図表Ⅱ－２－３　「サイバーセキュリティ基本法の一部を改正する法律案」の概要

②　重要インフラを守るための取組

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。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次行動計画の策定に当たっては、「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19日情報セキュリティ政策会議決定、2015年５月25日サイバーセキュリティ戦略本部改訂）の基本的な骨格（「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」）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た上、

- 「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
- 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」に変更

など、重要インフラ防護における機能保証の考え方を踏まえたものとした。

図表Ⅱ－２－４　「重要インフラの情報セキュリティ対策に係る第４次行動計画」の概要

「重要インフラの情報セキュリティ対策に係る第４次行動計画」の概要

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、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
- 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
- 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。

「安全基準等の整備及び浸透」については、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（以下「指針」という。）の本編・対策編及び「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」を用いてPDCAサイクルに沿っ

た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ことを確認した。また、第４次行動計画を受けた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）」[39]（以下「指針（第５版）」という。）を取りまとめた。

「情報共有体制の強化」については、2017年度も前年度に引き続き、各種会合の場を通じて、いわゆる予兆・ヒヤリハットも含む情報共有を行う意義・必要性の周知等に取り組んだ。なお、第４次行動計画において、セプター事務局を経由した新たな情報連絡ルートの導入が明記されたところであり、セプター事務局経由で匿名化された情報が出てくるなど、一定の効果が出ている。また、サイバー攻撃による重要インフラサービス障害の深刻度評価基準の具体化に向けた検討のため、重要インフラ専門調査会の下にワーキンググループを設置し、議論を継続している。

図表Ⅱ－２－５　重要インフラ事業者等との情報共有件数の推移

年度	2014	2015	2016	2017
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
内閣官房からの情報提供件数	38件	44件	80件	54件

こうした官民間の情報共有に加え、民間同士でも、セプターカウンシルにおいて標的型攻撃が疑われるメールに関する情報共有体制としてC4TAP（CEPTOAR Council's Capability for Cyber Targeted Attack Protection）が整備・運用されているほか、IPAにおいてサイバー攻撃における情報共有を行う体制として「サイバー情報共有イニシアティブ（J-CSIP）」が整備・運用されている。

「障害対応体制の強化」については、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、NISCでは、重要インフラ13分野の事業者等が一堂に会して、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。2017年度は、2,647名が参加し、前年度の参加数（2,084名）に比べて大幅に増加しており、過去最大規模での開催となった。2017年度においては、2020年東京大会を見据えた情報共有体制の確認など、内容の充実を図っている。

図表Ⅱ－２－６　2017年度分野横断的演習の様子

演習の模様

鈴木大臣による挨拶

[39] https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf

「リスクマネジメント及び対処態勢の整備」については、2020年東京大会を見据えた、関連事業者等による継続的なリスクアセスメントの取組において利活用されている「機能保証のためのリスクアセスメント・ガイドライン」[40]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」[41]をとりまとめた。また、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、指針（第５版）に盛り込んだ。

「防護基盤の強化」においては、「情報共有体制の強化」とも関連する施策として、防護範囲の見直し及び情報共有範囲の拡充を推進した。具体的には、セプター事務局の民間主体への移行（医療セプター）、各セプターにおけるセプター構成員の拡大、標的型攻撃に関する情報共有体制であるC4TAPの運用改善などの成果や、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。さらに、内閣官房からの情報については、複数の重要インフラ分野におけるセプター構成員以外の事業者や、既存の重要インフラ分野以外の団体等への展開を実施した。

③　政府機関を守るための取組

本節では、政府機関等[42]における情報セキュリティに関する各種取組のうち、NISCを中心とした政府機関等全体の取組の主なものについて示す。

まず、政府機関等における統一的な基準の策定に関して、今後政府機関等が目指すべきサイバーセキュリティ対策の将来像、独立行政法人等の業務形態を踏まえ、「政府機関等の情報セキュリティ対策のための統一基準群」（以下「統一基準群」という。）の改定案を2017年度に検討した。主な改定概要は以下の図に示すとおりである[43]。

[40] https://www.nisc.go.jp/active/infra/files/riskhyoka2.ZIP
[41] https://www.nisc.go.jp/active/infra/files/tebikisho.zip
[42] 本章以降、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を総称して「政府機関等」という。
[43] 「別添3-1　政府機関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」参照。

図表Ⅱ－２－７　統一基準群の主な改定案概要

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の見直しについて（骨子）

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境界監視に加えプログラムが動作する内部（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データ保護により事案が発生した際にも被害を無効化す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、第1段階として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た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”を講じる時期。全ウェブサイト及び電子メール通信の暗号化対応の義務化。

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統一基準群にフィードバック。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。

※ PDCA:[Plan（計画）、Do（実行）、Check（評価）、Act（改善）]

4. 多様な業務形態への対応

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導入。どのような業務形態であっても、安全かつ円滑に情報システムを利用できるよう、安全対策等を整備。

【攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進】

情報の窃取・破壊・改ざんを企図したとみられる標的型攻撃を始めとしたサイバー攻撃に対処するため、全ての政府機関等において、攻撃に直面することを前提とした多層的な対策を講じている。

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は、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新たなサイバー攻撃の傾向等について、政府機関等に対し注意喚起等を行った。また、府省庁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ほか、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について重点検査を実施した。

被害の発生・拡大の防止のための主な取組としては、2020年東京大会も念頭に置きつつ、脅威の検知能力向上等を図った第３期GSOCシステムを2017年４月から運用している。また、GSOC連絡担当者やCSIRT要員の情報セキュリティ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形成して会合を継続的に開催し、情報セキュリティインシデント対処に関する課題の確認と、府省庁を超えた議論及び情報共有を実施した。さらに、府省庁の情報セキュリティインシデント対処に関わる要員（CSIRT要員）に対し、サイバー攻撃発生時におけるCISOを始めとした幹部による指揮の下での迅速かつ適切な情報セキュリティインシデントへの組織的対処及び確実な連携を目指し、近年のサイバー攻撃動向を踏まえたインシデント・ハンドリングを中心とした訓練や、府省庁に加えて、2017年度より独立行政法人等のCSIRT要員も対象とし、技術的事項の習得に重点を置いた研修を実施したほか、府省庁の職員を対象とし、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 2018を実施した。

図表Ⅱ－２－８「NATIONAL 318(CYBER) EKIDEN 2018」の様子

被害の低減のための主な取組としては、2016年度に改定した「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」[44]に基づき、府省庁及び独立行政法人等に対しても、標的型攻撃に対する多重防御の取組の推進を図った。

【しなやかな組織的対応能力の強化】

加速度的な変化への柔軟かつ迅速な対応を可能とする、しなやかな組織的対応能力の強化に取り組んでいる。

主な取組としては、政府機関への監査を実施し、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、2016年度に実施した政府機関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。

政府機関においては、サイバー攻撃等が発生した際に、府省庁の壁を越えて連携し、被害拡大防止等機動的な支援を行うため、情報セキュリティ緊急支援チーム（CYMAT ： CYber incident Mobile Assistance Team）をNISCに設置しており、CYMAT要員等の対処能力を向上させるための研修・訓練も実施している。2017年度におけるCYMATの活動としては、２件の具体的な支援及び助言を行った。

政府機関におけるセキュリティ・IT人材の確保・育成については、「サイバーセキュリティ人材育成総合強化方針」（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、各府省庁において2017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2017年度においては、同計画に基づく体制の整備として機構・定員要求を行い、府省庁全体で約50の定員増による体制強化を実現、適切な処遇の確保として、システム所管部局の府省重点プロジェクト相当官署に重点を置く要求方針の下、政府全体で約50のポストの要求が認められた。ほかにも、有為な人材を確保するための採用活動、研修の受講等の取組を推進した。

また、NISCにおいては、2016年度から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」等を対象とした研修を実施し、実際に発生した情報セキュリティインシデントを題材とした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

[44] http://www.nisc.go.jp/active/general/risk.html

人材を育成するため、新たに、全府省庁のセキュリティ担当者を対象としたeラーニング及び「CISSP入門講座」を実施した。

このほか、政府機関の情報セキュリティ担当者向け勉強会の開催、新任管理者向けの情報セキュリティをテーマとした講演の実施、近年のサイバーセキュリティに関する情勢を踏まえた初任者研修向け資料の提供、一般職員向けの教育資料の改定等、それぞれの対象者に応じた適切な教育施策を実施し、職員全体のサイバーセキュリティに関する素養の向上を確実なものとするよう取り組んだ。

【技術の進歩や業務遂行形態の変化への対応】

多機能化・多様化するIT製品・サービスの活用による行政事務の高度化・合理化や、ITの活用に係る時代の要請に応じた形態での行政事務の遂行に当たっては、サイバーセキュリティの確保に留意し、新たなIT製品・サービスの不適切な利用に起因する情報セキュリティインシデントの発生やセキュリティ水準の低下の防止を図っている。

主な取組としては、政府機関等において利活用が進むクラウドサービスについて、府省庁におけるクラウド利用状況の調査を実施し、更なる施策の検討を行った。

【監視対象の拡大等による総合的な対策強化】

政府機関等全体としてのサイバーセキュリティを強化するため、独立行政法人等における対策の総合的な強化を図っている。

独立行政法人等に対して、IPAとの連携により、2017年度から監査対象を大幅に拡大したほか、NISCの監督の下、IPAが運用を開始した当該法人に対する不正な通信の監視体制において、サイバー攻撃に関する注意喚起等を実施した。さらに、日本年金機構に対する施策の評価を行った。また、当該監視体制を踏まえて、政府関係機関における情報セキュリティインシデントに係る情報共有体制の見直しを行った。

このほか、独立行政法人等の情報セキュリティ担当者向け勉強会を開催した。また、独立行政法人等、国立大学法人及び大学共同利用機関法人についての情報セキュリティ対策の実施状況を把握、分析した。さらに、所管する府省庁との情報共有等を行い、情報セキュリティ対策強化に資する具体的な取組について検討を行った。

(3)　国際社会の平和・安定及び我が国の安全保障

自由、公正かつ安全なサイバー空間は、国際社会の平和と安定の礎であり、その安全な利用を確保することは、国際社会の平和と安定及び我が国の安全保障にとって重要な課題である。我が国は、この認識のもと、サイバー攻撃に対する国全体の対処能力の強化を進めるとともに、国際協調主義に基づく「積極的平和主義」の立場から、各国との連携・協力に取り組んでいる。

①　我が国の安全の確保

サイバー空間の脅威は、多様化・複雑化しており、中には、国家の関与や実空間における軍の活動との連動が疑われる高度なサイバー攻撃の事例もある。こうした増大するサイバー空間の脅威に適切に対処し、我が国の安全を確保するため、対処機関の能力強化、先端技術の活用や防護、政府機関・社会システムの防護に努めている。

内閣官房、警察庁、公安調査庁、防衛省の各対処機関は、高度なサイバー攻撃からの防護、脅威認識等に係る能力の強化のため、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。具体的には、対処機関自身の防護システムの機能拡充等を図ることは勿論のこと、サイバー脅威情報の収集・分析用機材の整備、職員に対するサイバーセキュリティ教育の充実やサイバー演習環境に関する調査研究、カウンターサイバーインテリジェンスに関する関係省庁への情報提供等による政府機関の対処能力の向上を進めている。

また、我が国の先端技術は、経済的優位性を保障するだけでなく、安全保障上も重要な国家的資産である。このため、関係する主体はサイバーセキュリティの確保に万全を期していく必要がある。特に先端技術が多く使用される防衛装備品に関するサイバーセキュリティの確保は重要であり、防衛省は、調達する情報システムについて、不正なプログラムやハードウェア機器等による情報セキュリティ上のリスク（サプライチェーンリスク）への対策として、調達仕様書に記載すべき事項を整理した。

内閣官房では、研究開発業務は一般的な行政事務とは異なるため、これに適したサイバーセキュリティのあり方が必要であることから、国立研究開発法人に関する所要の対策について検討を行った。マネジメント面においては、適切なガバナンス体制の確立に向けた支援を行い、技術面においては、国立研究開発法人の業務特性に応じた課題を検討し、ルール面への盛り込みを進めた。また、個々の法人については、上記を踏まえ、基本法に基づく監査により助言を行う活動を開始した。国立研究開発法人においては、国立研究開発法人相互の協力による自立的活動の向上に向けた取組として、国立研究開発法人協議会に情報セキュリティに関する枠組みが立ち上げられた。

さらに、重要インフラ事業者等の社会システムを担う事業者のサイバーセキュリティの確保は、我が国の安全保障に関係する政府機関の任務の遂行を保証するため、また、国民や社会に不可欠なサービスの持続的な提供を果たすため、極めて重要である。このため、内閣官房や警察は、重要インフラ事業者等との間でサイバー攻撃への対処を想定した官民合同の訓練を実施している。また、日米両政府は、「日米防衛協力のための指針」（2015年４月）に基づき、適切な場合に、民間との情報共有によるものを含め、自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力することとしている。

②　国際社会の平和・安定

サイバー空間は、社会・経済・文化等あらゆる活動の基盤となり、国境を超えた相互理解を促進している。無限の価値を生むサイバー空間の潜在能力を維持しながら、国際社会の平和と安定を実現するためには、サイバー空間における情報の自由な流通の確保と、サイバーセキュリティの確保を両立させることが必要である。このため、我が国は、以下のような場を通じ、責任ある国際社会の一員としての役割を積極的に果たしている。

国際社会の平和と安定のためには、サイバー空間においても、実空間と変わらず法の支配が徹底されなければならない。我が国は、二国間等のサイバー協議や多国間の枠組みにおいて、サイバー空間に対する既存の国際法の適用や国際的な規範づくりに関する議論を進め、サイバー空間における法の支配の推進及び規範の深化に向け積極的に寄与してきた。2017年度においては、国連政府専門家会合第５会期における議論に積極的に貢献した。また、G7伊勢志摩サイバーグループに参加し、サイバー空間における国際法の適用、規範や、サイバー

空間を巡る諸課題についての議論に積極的に関与した。2018年２月には、日英共催ASEAN向けサイバーワークショップを実施し，サイバー空間における国際法の適用、責任ある国家の行動規範、インターネットのガバナンスのあり方等について議論した。これに加え、サイバー犯罪条約の締結国の拡大や刑事共助条約・協定に基づく迅速な共助の実施、法執行機関間の連携強化によって、サイバー犯罪に対する法執行面での協力にも取り組んでいる。

サイバー空間が、社会活動、経済活動、そして軍事活動を含むあらゆる活動が利用し、依存する場となっている中では、サイバー攻撃を発端とした不測の事態の発生を防ぐため、国際社会において相互の理解と信頼醸成を進めることが重要である。このため、我が国は、二国間等のサイバー協議やARF[45]その他の多国間の枠組みを通じ、各国との間で相互の脅威認識の共有やサイバー政策に係る情報共有と相互理解を進めている。二国間協議としては、第５回日米サイバー対話（2017年７月 東京)、第２回日印サイバー協議（2017年８月 デリー)、第３回日イスラエル・サイバー協議（2017年11月 東京)、第３回日豪サイバー協議（2017年12月 東京)、第３回日ＥＵサイバー対話（2018年３月 東京)、第４回日英サイバー協議（2018年３月 ロンドン）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。また、ARFの枠組みの中に、我が国の主導により、サイバーセキュリティに関する会期間会合を設立した。2018年２月、第１回目の専門家会合を開催し、考え方を異にする国との間でも予測可能性を向上し、信頼醸成を進めるべく取組を始めた。同時に、日・ASEANサイバーセキュリティ政策会議（2017年10月）やMeridian[46]カンファレンス（2017年11月）等の国際会議において、我が国のサイバーセキュリティ戦略をはじめとする関係施策を積極的に発信するとともに、サイバー分野における各国との連携・協力の強化と信頼醸成を推進した。また、ASEAN各国との国際サイバー演習（2017年５月、７月）を主催したほか、IWWN[47]加盟国や各国CSIRT間で行われる国際サイバー演習に積極的に参加し、重大な情報セキュリティインシデント発生時における国外のサイバーセキュリティ関係機関との連絡体制の整備・維持に努めている。

サイバー空間が国際社会の平和と安定に寄与するものであり続けるためには、サイバー空間を悪用した国際テロ組織の活動等を阻止する必要がある。このため、内閣情報調査室は、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っている。警察庁は、インターネット上のテロ等関連情報を収集する「インターネット・オシントセンター」を通じ、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・分析の強化に努めている。公安調査庁もサイバー空間に流布する国際テロ組織等に関する情報の収集・分析を通じ、攻撃予兆等の早期把握のための体制強化や人的情報収集網の拡大など、サイバー攻撃に関する情報収集・分析を強化した。

サイバー空間の脅威は、容易に国境を超えるため、世界各国で連携して効果的に対処する必要がある。このため、我が国は、開発途上国におけるサイバーセキュリティに関する能力の向上（キャパシティビルディング）に積極的に協力している。内閣官房、警察庁、総務省、法務省、外務省、経済産業省、防衛省、国際協力機構（JICA)、JPCERT/CC等の各機関は、「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)」

[45] 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。
[46] 重要インフラ防護に関する国際連携を推進する場として、2005 年にイギリスで開始された会合。
[47] 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。

（2016年10月）に基づき、ASEAN各国を始めとするアジアやアフリカを対象に、サイバーセキュリティ人材の育成への支援、サイバーセキュリティ関連施策の立案に向けた協力、解析技術やサイバー犯罪捜査等に関する知識・知見の共有、各国におけるCSIRT構築支援等のキャパシティビルディングを行った。また、キャパシティビルディングの要望元国へは必要に応じて調査団を派遣し、今後のキャパシティビルディングに係る現地ニーズのきめ細かな把握と、各国の状況に応じた支援内容の立案に努めている。

また、我が国における国際的な人材育成も重要である。このため、サイバーセキュリティに関する国際会議や海外での研修機会に政府職員を派遣し、海外の様々な主体との間でコミュニケーションを深めるとともに、得られた知見や技術動向を国内関係者と共有することで、政府機関におけるサイバーセキュリティ分野における国際的な人材育成を図っている。

③　世界各国との協力・連携

サイバー空間における脅威は、容易に国境を越えるため、一国のみで対応することは容易ではない。我が国は世界各国との二国間・多国間の様々な枠組みを活用した協力・連携により、国際社会の平和・安定及び我が国の安全保障の実現に向けた取組を進めている。

アジア大洋州では、地域の責任ある国として、各国・地域との間で様々なチャネルを通じたサイバー分野での協力を進めている。40年以上にわたるパートナーであるASEANとの間では、内閣官房、総務省、経済産業省が中心となり、第10回日・ASEAN情報セキュリティ政策会議（2017年10月　シンガポール）を開催した。同会議では、引き続き、日ASEAN間の国際サイバー演習、重要インフラ防護、人材育成及び意識啓発の面等で連携を強化していくことで合意した[48]。この他、我が国と基本的な価値観を共有する地域の戦略的パートナーとの間では、随時の意見交換を通じて、サイバー空間における協力・連携を進めているところである。法執行面や安全保障面でも、アジア大洋州地域の法執行機関や刑事司法実務家、防衛当局関係者との間で、それぞれの分野に関する意見交換や技術面での交流を進めている。

図表Ⅱ－２－９　「第10回日・ASEAN情報セキュリティ政策会議」の様子

[48] 同会議は、2018 年から名称を「日・ASEAN サイバーセキュリティ政策会議」に改めることにも合意した。

米国とは、日米安保体制を基軸とし、サイバー分野においても緊密な連携を進めている。両国政府間の「日米防衛協力のための指針」（2015年４月）に基づき、サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切に共有するとともに、自衛隊及び米軍が任務を遂行する上で依拠する重要インフラ及びサービスを防護するために協力することとしている。また、同指針は、日本が武力攻撃を受けている場合に発生するものを含め、日本の安全に影響を与える深刻なサイバー事案が発生した場合、日米両政府は緊密に協議し、適切な協力行動をとり対処するとしている。第５回日米サイバー対話（2017年７月 東京）では、情報共有、重要インフラ防護、ボット対策、能力構築を含む国際場裡における協力等、サイバーセキュリティに関する幅広い日米協力について議論を行った。また、官民での日米連携強化を目的として、同対話の機会に官民会合も開催した。加えて、両国は、インターネットエコノミーに関する日米政策協力対話（第８回局長級会合）（2017年９月 ワシントン）等を開催している。経済面及び安全保障面からの意見交換と連携強化も進めている。

欧州諸国とは、政府横断的な二国間協議である第３回日ＥＵサイバー対話（2018年３月）、第４回日英サイバー協議（2018年３月）等を開催し、両国との間でサイバー空間に係る政策や国内動向の共有を進めるとともに、国際的規範や能力構築支援、脅威情報共有等における連携について議論を行った。また、英国とは、2017年８月の日英首脳会談において、サイバー分野を含む「安全保障協力に関する日英共同宣言」を発出した。また、仏国とは、2018年1月の第４回日仏外務・防衛閣僚会合において、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するため、日仏両国が協調した対応及び情報共有を強化することを確認した。この他にも、我が国と基本的価値観を共有する各国との間で、随時の意見交換を開催し、サイバー空間における協力・連携を進めている。また、防衛省は、北大西洋条約機構（NATO）が承認するサイバーに特化した研究機関である、サイバー防衛協力センター（NATO CCDCOE）への参加承認を取得する等、欧州各国との連携強化に努めた。

中南米、中東アフリカの両地域についても、第３回日イスラエル・サイバー協議（2017年11月 東京）を実施し、同国との連携強化に努める等、共通の価値観を持つ国々と随時の意見交換を進めるとともに、CSIRT間の連携やキャパシティビルディングに関する支援により、サイバー分野における幅広い協力関係を構築に努めている。

また、我が国では、サイバーセキュリティの課題に国際的に連携して取り組み、ASEANを中心とした開発途上国におけるサイバーセキュリティの普及啓発を進めるため、「サイバーセキュリティ国際キャンペーン」を毎年10月に実施している。

(4)　横断的施策

①　研究開発の推進

サイバーセキュリティの研究開発において、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、イノベーションを起こし、国際競争力の強化等を図っていくためには、近い将来と中長期的な社会・経済とITの利活用の進化を視野に入れることが重要である。

そしてITの極めて急速な進化に伴い、サイバー攻撃も日々進化し高度化・複雑化している。その変化に迅速に対処するため、さらに、近い将来のITの利活用を踏まえたサイバーセキュリティに関する研究開発を推進するため、以下の取組を実施した。

内閣官房においては、各府省庁と連携し、「情報セキュリティ研究開発戦略（改定版）」に基づき、情報セキュリティの研究開発を推進した。また、研究開発戦略専門調査会を通じ、社会・経済とITの利活用の進化を視野に入れ、かつ多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、将来的な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示す「サイバーセキュリティ研究開発戦略」を策定した。

図表Ⅱ－２－10　サイバーセキュリティ研究の広がり

（出典：サイバーセキュリティ研究開発戦略）

②　人材の育成・確保

サイバー空間は、企業活動のグローバル化やデジタル化が進む中において、主に民間主体の投資や英知の集約により急速な拡大を遂げてきており、経済社会の活動基盤となっている。こうした中、サイバー攻撃は、情報等の窃取、社会システムの機能不全により、国民生活、さらには国際社会が危機にさらされる原因となりうる。このため、個人や組織を問わず、あらゆる主体がサイバーセキュリティに対する認識を深め、各主体の協力的かつ自発的な取組を通じて、その脅威に対処できる安全な空間としていかなければならない。

こうした環境整備に資するよう、2017年４月に「サイバーセキュリティ人材育成プログラム」（2017年４月18日サイバーセキュリティ戦略本部決定）を策定した。これを踏まえ、「サイバーセキュリティ人材の育成に関する施策間連携WG」において、①各層別の人材像やキャリアパスの明確化、②ITの基本的知識と各層別のカリキュラムの方向性、③各省の人材育成施策に関する全体像整理と連携策の検討、④教材のR&D、⑤産学官連携の在り方・具体的方策について検討を実施した。並行して、内閣官房にて各層別の人材像、モデルとなるカリキュラムの方向性について調査を行い、「サイバーセキュリティ人材の育成に関する施策間連携WG」にて報告を行った。

また、「企業経営のためのサイバーセキュリティの考え方」の見直しを念頭に、「セキュリティマインドを持った企業経営WG」において、①経営層が持つべき意識や果たすべき役割、

②経営層がリスクマネジメントの一つとしてサイバーセキュリティの取組を進めていく上での具体的な方策、③中小企業を始めとする事業上のリソースの制約が大きい企業の対策、④産学官連携による取組について検討を実施し、報告書としてとりまとめた。

(5)　推進体制

2015年戦略は2018年に期限を迎えるが、国民生活・経済等のIT依存度はますます高まっていることに加えて、国内外において、ランサムウェア攻撃、IoTを踏み台にしたサイバー攻撃、重要インフラを標的にしたサイバー攻撃が発生していることから社会が質的に変化も感じられる。また、2020年東京大会におけるサイバーセキュリティ対策を万全なものにする必要がある。このような認識から、急ぎ加速・強化すべき施策を2015年戦略中間レビューとしてサイバーセキュリティ戦略本部で決定し諸施策を推進した。

2020年東京大会のサイバーセキュリティの確保については、引き続き2020年東京大会推進本部の下に設置されたセキュリティ幹事会、サイバーセキュリティワーキングチーム等において施策を検討するとともに、2020年東京大会のセキュリティの基本的な考え方、対策をまとめた「2020年東京オリンピック競技大会・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）に基づき対策を推進した。

対処体制の整備について、情報共有・対処体制に関する基本的な方針を関係府省庁、大会組織委員会、東京都等と協議の上、改正すると共に、サイバーセキュリティ対処調整センターの仕様の細部について検討を推進し、2017年12月のセキュリティ幹事会において、2018年度末目途に構築及び運用開始することを決定した。

また、2018年平昌大会の直前及び期間中におけるサイバーセキュリティに係る状況について、試験的に運用しているサイバーセキュリティ関係機関等との情報共有体制を活用し、韓国政府が指定した窓口に対して定期的に情報提供を実施した。加えて、2018年平昌大会期間中及び終了後、要員を派遣し、サイバーセキュリティの確保及びインシデント発生時の対応について情報収集を実施した。

リスクマネジメントについては、2016年度に東京23区の重要サービス事業者等を対象とした第１回目のリスク評価の実施結果及び2012年ロンドン大会のサイバーセキュリティ責任者らの助言を踏まえ、リスク評価に係る手順書を改訂し、東京圏（東京都、神奈川県、千葉県、埼玉県）の重要サービス事業者等を対象とする第２回目のリスク評価を依頼し、NISCにおいて131の事業者から実施結果を受領の上、同評価に基づく対策を促進した。また、スポーツ関連団体に対してサイバーセキュリティの確保についての勉強会を実施し、意識の高揚を図った。

加えて、大会全般にわたる横断的なリスク評価の実施に向け、2012年ロンドン大会のサイバーセキュリティ責任者らの助言を踏まえ、評価手法等の検討を実施した。

Ⅲ　サイバーセキュリティ関連施策の評価

本章は、2015年戦略に基づく年次計画である「サイバーセキュリティ2017」をはじめとする、過去３年間の年次計画に記載された諸施策について、「サイバーセキュリティ政策の評価に係る基本方針」（2015年９月25日サイバーセキュリティ戦略本部決定。2016年８月31日一部改定）に則り、取組状況を評価したものである。

「サイバーセキュリティ2017」に掲載された諸施策については、別添２に示すとおり各府省庁において具体的な取組が進められており、着実に進捗している。しかしながら、サイバー攻撃に伴うリスクは刻一刻と深刻化・巧妙化しており、2020年東京大会等に向けて、我が国のサイバーセキュリティを一層確固たるものにする必要がある。次期「サイバーセキュリティ戦略」に基づき、別途策定される2018年度の年次計画である「サイバーセキュリティ2018」については、本評価も踏まえて諸施策の改善を図るとともに、これを着実に推進することとする。

１　経済社会の活力の向上及び持続的発展

(1)　安全な IoT システムの創出

【総　評】

2016年１月より、総務省と経済産業省が共同して、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を立ち上げ、「IoTセキュリティガイドライン」の策定に向けた検討を開始。2016年７月に「IoTセキュリティガイドライン」を策定した。また、NISCにおいて2016年８月に「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」を策定する等安全なIoTシステムの創出に向けた取組を行った。さらに、安全なIoTシステムの創出に関し、国際的な貢献を図るため、2017年より「IoTセキュリティガイドライン」、「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」を基本とした国際標準化活動を推進している。これらの取組を通じ、IoTシステムのセキュリティに対する関心や個別分野における部分的な対策は一定程度、進んだと考えられるが、Society5.0の実現に向けて、さまざまな分野が横断的につながることによるリスクや、物理的な安全性に関わるリスクの問題への対処が必要となってくるため、関係主体間の相互信頼に基づく一層の連携が求められる。

【課　題】

Society5.0の実現に向け、官民が緊密に連携して安全なIoTシステムの創出に向けて取り組むべく、2018年戦略に基づき、関係府省庁や関係機関における有機的・一体的な連携を働きかけるとともに、関係する多様な主体の相互信頼に基づく体系的な体制の整備、各関係主体の任務の明確化等を促進していくことが必要である。

(2)　セキュリティマインドを持った企業経営の推進

【総　評】

企業経営層のリーダーシップにより、サイバーセキュリティ対策を推進するため、2015年12月に「サイバーセキュリティ経営ガイドライン」、2016年８月に「企業経営のためのサイバーセキュリティの考え方」を策定した。2017年11月には、国際的に事前対策だけではなく事後対策が要求されている状況を踏まえ、「サイバーセキュリティ経営ガイドライン」の改訂を行った。また、セキュリティマインドを持った企業経営WGにおいて、経営層によるリス

クマネジメントの一環としてのサイバーセキュリティ対策の推進等を含む「セキュリティマインドを持った企業経営ワーキンググループ報告書～事業継続と価値創出を支えるサイバーセキュリティ～」を取りまとめた。こうした取組を通じ、一部の大企業を中心にサイバーセキュリティ対策の意識は高まってきているが、業種・業態によって意識に違いがあることが明確となった。ITの利活用が事業継続、さらには、新たな価値創出において不可欠になりつつある中で、経営層がリスクマネジメントの一環として、サイバーセキュリティをとらえ、具体的な対策を講じていけるようにしていくことが求められる。

【課　題】

上記報告書の内容を踏まえて、経営層の理解と意識改革の推進や業種・業態別の差異を踏まえた基盤の整備等の具体的な取組を推進していく必要がある。

(3)　セキュリティに係るビジネス環境の整備

【総　評】

我が国の情報通信技術を利活用した関連産業の成長に伴い、サイバーセキュリティ関連産業に対する需要が一層増加することが見込まれる。こうした需要を捉えるため、各府省において、製品・サービスにおけるセキュリティ確保及び国際競争強化の基盤となるビジネス環境の整備に取り組んでいる。今後、Society5.0に向けて、IoTやAIなどに関する先端技術の利活用が期待されるところ、それに伴うサイバーセキュリティリスクへ対応を行うユーザー企業のニーズに対し、より適切かつ迅速に対応できるような仕組みが求められる。

【課　題】

新たな価値創出に向けた先端技術の利活用に伴うサイバーセキュリティに関連する課題に対応できる環境整備が必要である。特に、事業者が抱えるセキュリティ上の課題に対し、スムーズに対応するためのガイドラインや、サイバーセキュリティの製品・サービスを提供するサイバーセキュリティビジネスが、事業者を支えられるようなマッチングの仕組み等が必要である。

２　国民が安全で安心して暮らせる社会の実現

(1)　国民・社会を守るための取組

【総　評】

国民・社会がサイバー空間に起因する脅威にさらされないようにするため、その利用環境が安全なものとなるよう、関係府省庁による情報発信や環境整備の検討が進められている。サイバー空間の利用者たる国民一人一人がサイバーセキュリティについての関心を高め、問題に対応していくことを促すため、NISCにてSNSを活用した情報発信を積極的に行うとともに、「サイバーセキュリティ月間」では、政府一体となって、産学官が連携した活動を集中的に実施しており、その取組数は年々増加している。また、国民に親しみやすいメディアを活用し、イベントの開催やポスターによる広報活動等を実施するなど、新たな取組を行っている。これらの取組を通じ、国民の意識啓発は一定程度進んでいるが、リーチの届いていない層への効果的な訴求について引き続き検討し、取り組んでいくことが求められる。

【課　題】

セキュリティに対する意識や知識が国民全体に十分に浸透しているとは言い難く、地域・年齢層や所属、ライフスタイルが異なる多様な国民のニーズにきめ細やかに対応していけるよう、Webサイト等を利用し、着実に普及啓発活動を推進していくことが必要である。

(2)　重要インフラを守るための取組

【総　評】

「重要インフラ防護の範囲等の不断の見直し」については、セプター加入事業者の増加、ISACの対象事業者の拡大等により、多くの重要インフラ事業者等が情報共有の輪に加わり、面としての防護を強化することができた。また、核物質防護等の措置が要求される企業への情報提供を開始するなど、重要インフラ分野以外に事業者等についても情報共有体制の中に組み込むことができた。今後は、サイバー攻撃による脅威が深刻化・巧妙化する中、さらに防護範囲の見直しを進めていくことが求められる。

「効果的かつ迅速な情報共有の実現」については、第４次行動計画を策定し、情報連絡元の匿名化やホットラインの構築など、情報共有をより活発化するための環境整備に取り組んだ結果、情報共有件数は増加傾向にある。また、サイバー攻撃の手口に関する情報を受領し、その情報を踏まえ、必要に応じて注意喚起を行い、被害の防止に資することができた。ただし、情報共有の基盤となるプラットフォームの構築や、処理の自動化についてはまだ検討段階である。

「各分野の個別事情への支援」については、地方公共団体において、業務用ネットワークをインターネットから分離するなどのネットワーク分離や、都道府県ごとにインターネットの接続口を集約化するセキュリティクラウドの構築等により、セキュリティの全体的な底上げが行われ、一定レベルのセキュリティを確保することができたが、まだ取組が十分ではない地方公共団体もあると思われる。また、制御系については、セキュリティ向上に資する取組を行っているものの、IT系とは事情が異なり、まだ十分に制御系に対するセキュリティ意識が高まっているとは言えない状況である。

【課　題】

新たに策定した第４次行動計画に基づき、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、各関係主体において、「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」の各施策を推進する必要がある。

具体的には、「重要インフラ防護の範囲等の不断の見直し」については、今後もサイバー攻撃により、様々な分野のサービスに影響が及ぶおそれが想定されることから、社会情勢等に鑑み、必要に応じて、重要インフラ防護の範囲等を引き続き見直していく必要がある。

「効果的かつ迅速な情報共有の実現」については、情報を収集・分析・共有する基盤となるプラットフォームの構築や、処理の自動化について、まだ検討段階であるため、2020年東京大会に向けて、システムや体制の構築を進めるとともに、関係主体間の連携を高め、情報共有をより効果的かつ迅速に行っていく必要がある。

「各分野の個別事情への支援」については、地方公共団体について、今後も引き続き、高いレベルのセキュリティを確保できるように取組を進めていく必要がある。また、制御系については、今後も引き続き、情報収集・分析・展開を行って意識向上を図り、制御系システムのセキュリティを向上していく必要がある。

(3)　政府機関を守るための取組

【総　評】

2016年度に、政府機関等に対する攻撃動向を踏まえ、標的型攻撃等に対する防御策の更なる強化や、インシデント対処体制の強化等を盛り込んだ統一基準群の改定を行った。併せて、政府機関等がセキュリティポリシーの改定を速やかに行えるよう必要な支援等を実施した。2017年度には、政府機関等が目指すべきサイバーセキュリティ対策の将来像等を踏まえた統一基準群の改定に着手した。技術の進展、攻撃の動向に対して、迅速に基準の改定を行った。引き続き、政府機関等の情報セキュリティ水準の維持・向上のため、次期改定に向けて統一基準群の検討に資する技術の進展の把握等の取組を継続することが求められる。

また、監査においては、2015年度から府省庁に対してサイバーセキュリティ基本法に基づく監査として、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）を開始した。2016年度下半期には、サイバーセキュリティ基本法改正に伴い、独立行政法人等の監査を開始した。監査により政府機関等のセキュリティ対策の状況を把握し、各機関が今後のサイバーセキュリティ対策を強化する上での必要な助言等を行うとともに、監査を実施した機関に対してフォローアップを行った。監査の実施により、実施済みの機関の更なるセキュリティ対策の底上げが図られた。引き続き、監査を通じたサイバーセキュリティの強化が求められる。

さらに、府省庁のCSIRT要員に、情報セキュリティインシデントへの適切な対処に向けた訓練・研修を実施した。2017年度からは独立行政法人等のCSIRT要員も研修の対象とした。各機関での情報セキュリティインシデントへの対処能力の向上が図られた。引き続き、情報セキュリティインシデント対応能力向上のための取組が求められる。

そのほか、サイバーセキュリティ人材育成総合強化方針に基づき、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、一定の専門性を有する人材の育成、適切な処遇の確保を含む政府内部のセキュリティ・IT人材の充実に資する取組を行った。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。

【課　題】

新たな防御技術等を適時適切に活用し政府機関等のセキュリティを強化・充実するため、統一基準群の改定を2018年に予定するとともに、政府機関等においてもそれに準ずる情報セキュリティポリシー改定を速やかに行えるよう必要な支援等を行い、関連規程についても、引き続き、所要の改定作業に取り組んでいく必要がある。

また、監査においては、引き続き、政府機関等への監査及び監視の実施とともに、監査済の機関へのフォローアップを行う。特に独立行政法人等に対しては、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の監査を実施するとともに、IPAと連携して、フォ

ローアップを行い、サイバーセキュリティ確保のための取組を総合的に強化する必要がある。

さらに、府省庁のCSIRT要員に対しては、訓練・研修を引き続き行う。独立行政法人等のCSIRT要員に対しては、2017年度より研修の対象としたところであり、情報セキュリティインシデントへの対処能力の更なる向上のニーズに応えていく必要がある。

政府機関におけるセキュリティ・IT人材の確保・育成に関し、引き続き、サイバーセキュリティ人材育成総合強化方針に基づき、継続的に取組を推進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

(1)　我が国の安全の確保

【総　評】

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、防衛装備品に代表される安全保障上重要な先端技術のサイバーセキュリティの確保に向けても、官民協力の下、取組を進めている。さらに、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に必要な重要インフラ事業者等のサイバーセキュリティの確保に向け、米国との協力を含め、政府全体で取組を進めている。これにより対処機関の能力強化、先端技術の活用や防護、政府機関・社会システムの防護が進んでいるが、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、引き続き我が国の安全の確保のための取組を強化することが求められる。

【課　題】

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る。このためには、海外関係機関との情報共有等の連携が必須である。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、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、政府全体で重要インフラ事業者によるサイバーセキュリティの取組みを後押ししていく必要がある。

(2)　国際社会の平和・安定

【総　評】

首脳・閣僚級の共同声明や、実務レベルにおける二国間サイバー協議や多国間会議を通じ、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、法執行面においても各国との連携を強化してきた。また、重大な情報セキュリティインシデントが発生した際の国外関係機関との連絡体制を確保するとともに、我が国の対処能力の向上を図るため、国際的なサイバー演習を行っている。他にも、有志国との協力関係を深め、また我が国とサイバー空間における考え方を異にする国との間でも信頼醸成を図るため、我が国のサイバー分野における取組に係る情報共有と相互理解を進めている。

さらに、サイバー空間を利用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。加えて、国境を越えて起こるサイバー攻撃に世界各国で連携して効果的に対処していくため、「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）に基づき、内閣官房を中心とする関係省庁において開発途上国におけるキャパシティビルディングに積極的に協力している。

このように国際社会の平和と安定に寄与するための取組みを堅実に進めてきているところであるが、第５次国連政府専門家会合（GGE）がコンセンサス報告書を発出することがかなわなかったことは、サイバー空間における国際法の適用に関する合意形成の難しさを示している。今後、同盟国・有志国と連携してサイバー空間における国際法の適用のあり方等についてさらに議論を進めるとともに、各国との信頼醸成、開発途上国における能力構築支援を引き続き進めていくことが求められる。

【課　題】

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通じ、各国との連携のもと、サイバー空間における国際法の適用や国際規範について、より具体的に議論を進めるとともに、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。この際、サイバー空間を健全に発展させるため、サイバー空間における多様な参加主体による自律的なガバナンスを尊重する必要がある。国際的なサイバー演習についても、必要に応じ、演習の範囲の拡大を検討するとともに、内容の高度化を進めていく必要がある。キャパシティビルディングについては、対象国の現地ニーズのきめ細かな把握と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。

(3)　世界各国との協力・連携

【総　評】

アジア大洋州、北米、欧州、中南米、中東アフリカの各地域において、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、情報共有等、連携の深化のあり方を検討していく必要がある。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いるが、同地域のサイバーセキュリティ対策の底上げに向けて、更なる価値の共有・連携の強化を進めることが求められる。

【課　題】

アジア大洋州においては、日・ASEANサイバーセキュリティ政策会議による取組を継続・強化しつつ、ASEAN各国の状況に応じた連携・協力の強化を図る必要がある。あわせて地域における戦略的パートナーとの連携・協力も着実に進めていく。米国との間では、日米安保体制を基軸に、経済面や安全保障面を含むサイバーセキュリティに関するあらゆる面での協力を更に拡大・深化させていく。欧州との間でも、二国間協議等を通じた連携や国際場裡での協力強化を進める。中南米、中東アフリカにおいても、共通の価値観を持つ国々との連携を着実に進める。

４　横断的施策

(1)　研究開発の推進

【総　評】

日々進化しているサイバー攻撃に対応するため、国立研究開発法人等において、サイバー攻撃の検知・予測や防御力向上等に資する研究開発、SIPにおいて、重要インフラ分野における実用化を念頭に、産学官が連携した総合的な研究開発を推進した。また、情報通信技術（IT）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、将来的な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示す文書として、「近い将来」だけでなく、「中長期的」な社会・経済の変化とITの利活用の進化を視野に入れた「サイバーセキュリティ研究開発戦略」を策定した。一方で、研究開発成果の社会実装を推進していくとともに、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や、技術的な研究開発にとどまらない制度上の課題等に関する調査・研究を行うなどの取組の強化も必要である。

【課　題】

今後は我が国のサイバーセキュリティに関連する研究開発の状況について把握し、その成果についての情報発信を促すとともに、これまでの技術研究にとどまらない基盤技術やサイバーセキュリティに関する制度上の課題に関する調査・研究を推進する。また、NISC及び関係府省庁の連携のもと、サイバーセキュリティ研究開発戦略に基づく新たなサイバーセキュリティの研究分野やテーマについて検討を促す必要がある。さらに、研究開発の取組について、その成果の社会実装を推進する必要がある。

(2)　人材の育成・確保

【総　評】

2016年３月に「サイバーセキュリティ人材育成総合強化方針」、2017年４月に「サイバーセキュリティ人材育成プログラム」を策定し、企業を始めとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示した。その後、2015年戦略中間レビューを踏まえ、サイバーセキュリティ人材の育成に関する施策間連携WG及びセキュリティマインドを持った企業経営WGにおいて、戦略マネジメント層の人材像や各人材層におけるモデルカリキュラム等について検討を行うとともに、セキュリティマインドを持った企業経営WGにおいて、経営層によるリスクマネジメントの一環としてのサイバーセキュリティ対策の推進等について検討を行い、その成果を報告書として取りまとめた。こうした取組は、今後のサイバーセキュリティ人材育成の取組方針について、産学官の共有が図られ、具体的な取組の充実につながるものであると考えられる。今後は、こうした取組を踏まえ、産学官の関係主体が、引き続き連携を図りつつ、戦略マネジメント層の定着・育成をはじめとした人材育成施策を推進していくことが求められる。

【課　題】

引き続き、人材規模・キャリアパス（需要）と、人材育成施策（供給）の好循環の形成に向けて、戦略マネジメント層の定着や人材育成に関する取組の「見える化」など、具体的な取組を推進するとともに、継続的にフォローアップを行う必要がある。

５　推進体制

【総　評】

サイバーセキュリティ戦略に基づいて各種施策を推進しているところ、国民生活・経済等の IT 依存度の高まり、国内外における複雑・巧妙化したサイバー攻撃の発生及び 2020 年東京大会におけるサイバーセキュリティ対策を万全なものにする必要があること等から 2017 年７月には 2015 年戦略中間レビューをサイバーセキュリティ戦略本部で決定し諸施策を加速・強化した。

また、2020 年東京大会のサイバーセキュリティの確保については、2020 年東京大会推進本部の下に設置されたセキュリティ幹事会、サイバーセキュリティワーキングチーム等において施策を検討するとともに、2020 年東京大会のセキュリティの基本的な考え方、対策をまとめた「2020 年東京オリンピック競技大会・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)に基づき対策を推進しており、2020 年東京大会のサイバーセキュリティの確保については、概ね当初の計画どおりに進捗している。

2018 年度中にサイバーセキュリティ対処調整センターを構築するべく準備を進めているところであり、合わせて具体的な準備についても進めている。

リスクマネジメントについては、計画どおり２回目のリスク評価を終了し、その教訓から、他のサービスに重大な影響を及ぼす重要サービス事業者に対して横断的なリスク評価を併せて実施することとし、具体的な作業に着手した。

【課　題】

2018 年度からは、３回目以降のリスク評価の対象を全国の大会会場がある自治体等に拡大するとともに、並行して横断的なリスク評価についても実施していかなければならず、計画的に２種類のリスク評価を実施するとともに、評価結果を個々の事業者にフィードバックさせ、適切に次回のリスク評価及び対策の促進につなげていく必要がある。

また、サイバーセキュリティ対処調整センターの構築を 2018 年度内に完了し、限定的に運用を開始できるように運用要領等の検討・策定、要員の訓練等を行っていく必要がある。

別添１　各府省庁における情報セキュリティ対策に関する取組

＜別添１－目次＞

内閣官房 42
内閣法制局 43
人事院 44
内閣府 45
宮内庁 46
公正取引委員会 47
警察庁 48
個人情報保護委員会 49
金融庁 50
消費者庁 51
復興庁 52
総務省 53
法務省 54
外務省 55
財務省 56
文部科学省 57
厚生労働省 58
農林水産省 59
経済産業省 60
国土交通省 61
環境省 62
防衛省 63

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2018年度当初までに定めた「対策推進計画」を基として、2017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2018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

2017 年度の総合評価・2018 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　土生　栄二

2017年度は、従来の標的型攻撃メールに加え、ランサムウェアなどを使用した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が取りまとめた不審メール情報等を集計したところ、2017年は約850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、いわゆるアナログハック（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2018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、これまでの資料配布を中心とした教育に加え、2017年度に導入したeラーニングを拡充した上で引き続き実施するほか、NISC等が主催する研修会への参加を一層促進する。

情報収集については、CYMAT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

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
総務主幹　木村　陽一

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。

2017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における助言についての改善計画を策定し、情報セキュリティ対策を実施した。また、体制整備・人材拡充のために策定した「内閣法制局セキュリティ・IT人材確保・育成計画」（以下「人材育成計画」という。）に基づき、リテラシー向上に努めた。

2018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、マルウエ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い、内閣法制局情報セキュリティポリシー関連規程の整備、NISCが実施するマネジメント監査、ペネトレーションテスト、CSIRT訓練等を通じ、情報セキュリティ対策に取り組むものとする。

このような取組、対策等を実施することによって、引き続き、情報システムの安全性を確保し、情報セキュリティ水準の維持・向上に努めていく。

人事院

2017 年度の総合評価・2018 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。

2017年度においては、５月施行の人事院情報セキュリティポリシーの周知・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情報システムセキュリティ責任者向けの説明会のほか、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、新規採用職員の研修においても情報セキュリティ教育に関する講義を設け、情報セキュリティ対策に対する理解の浸透に努めた。

さらに、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対処手順の一部を経験させた。

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。

2018年度においては、人事院が保有する情報及び情報システムをサイバー攻撃の脅威から保護するため、職員の更なるリテラシー向上対策として、これまで行ってきた人事院独自の教育の内容をより充実させ、情報セキュリティ対策への一層の理解を深めるとともに、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。

さらに、10月に予定されている基幹LANシステムの更改において、新たに適用されるべき情報セキュリティ対策の実施を確実に進める。

内閣府

2017 年度の総合評価・2018 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　北崎　秀一

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。

なお、こうした脅威を防ぐため単純に情報システムの利用制限で対応すると、日常の業務の遂行における生産性の低下を招きかねない。むしろ、「働き方改革」の実現等においては情報システムを積極的に活用することが期待されている。

以上の状況を踏まえ、2018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、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

2017 年度の総合評価・2018 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、2017年度においては、主に以下の対策を実施した。

〇政府機関の情報セキュリティ対策のための統一基準群の改定を踏まえた宮内庁情報セキュリティポリシーや各種実施手順等の整備
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導入
〇宮内庁情報ネットワークシステムにおける情報セキュリティ対策の強化

2018年度においては、引き続き、宮内庁セキュリティ・IT人材確保・育成計画を推進し、行政事務従事者の教育の充実を図る。具体的には、研修等の機会を通じて、新たに整備した宮内庁情報セキュリティポリシーや各種実施手順等の内容を周知するほか、全職員を対象とした標的型攻撃の訓練を実施して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、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、技術的措置としては、新たなサイバー攻撃の脅威や情報通信技術についての情報収集に努め、効果的な対策の検討・導入を進める。

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

2017 年度の総合評価・2018 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　南部　利之

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。

2017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、エスカレーションなどの組織としての対応についても訓練を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、当該計画に基づきシステム担当部署からの出向を増やし人材の育成を図った。さらに政府統一基準群の改定やNISC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。

2018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

2017 年度の総合評価・2018 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　村田　利見

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、情報システムに対する技術的対策に加え、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。

2017年度においては、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軽微な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。

2018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していくとともに、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

2017 年度の総合評価・2018 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、個人情報の利活用と保護のバランスを考慮したルールの策定、マイナンバーのセキュリティの確保、情報セキュリティ等の専門性を確保するための人材育成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」（2016年２月15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。

2018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年度に改定予定である「政府機関の情報セキュリティ対策のための統一基準群」に応じて「個人情報保護委員会情報セキュリティポリシー」（2017年３月31日最高情報セキュリティ責任者決定）の早期改定を行うほか、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

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
総務企画局総括審議官　佐々木　清隆

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IT国家創造宣言・官民データ活用推進基本計画（2017年５月30日閣議決定）」において、「官民データ利活用社会」の実現を目指していくことが表明され、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、2017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。

2018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、2017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、金融庁情報セキュリティポリシーの改定、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

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
次長　川口　康裕

2016年度に実施した内閣官房内閣サイバーセキュリティセンターマネジメント監査において確認された課題事項について、各課題事項への改善計画を定義し、計画的な課題改善推進ができた。

さらに、2017年度は、徳島県庁舎内に消費者行政新未来創造オフィスの開設に伴い、遠隔拠点での情報管理や拠点間での情報共有が必要となったことを踏まえ、拠点間での情報共有における情報セキュリティ対策の実現を重点課題と位置づけ、全職員を対象とした情報セキュリティ教育の実施による啓蒙活動に取り組んだ。その結果、遠隔地での情報管理や拠点間での情報共有を起因とした情報セキュリティインシデントは発生せず、当庁の情報セキュリティマネジメントは相応に有効に機能しているものと判断する。しかし、情報セキュリティ監査において情報管理面での課題が指摘され、改善すべき課題が明らかとなった。

年２回実施した不審メール訓練では、１回目の訓練で職員の４分の１が訓練用の模擬メールを開封したが、その後当該職員への再教育を実施し、不審メールに対する対策を再徹底することで、２回目の訓練では開封率を１割未満まで削減することが出来た。

また、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。）が2018年度に更改されることを踏まえ、当庁LANシステムの情報セキュリティ要件の定義についても今年度の重要な課題と位置づけ、要件定義策定作業に取り組んだ。

2018年度は、2017年度の情報セキュリティ監査における課題事項について改善計画を策定し、計画的な対応を図っていく。職員への情報セキュリティ教育においては、全職員を対象とした情報セキュリティ教育の実施を継続的に実施していくことに加え、不審メール訓練についても継続的に実施し、入替り頻度が高い当庁の職員事情や、東京と徳島の複数拠点で情報管理を行う必要がある当庁の特性を考慮しながら、個々の職員における情報セキュリティ意識の向上を目指す。

また、2018年度は当庁の情報システムの根幹となる当庁LANシステムの更改を控えており、計画に沿って情報セキュリティ対策が確実に実現されるよう、構築業務の管理徹底に取り組んでいく。

復興庁

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
統括官　加藤　久喜

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。

2017年度は、全職員を対象とした情報セキュリティ研修や標的型攻撃への対処訓練を実施するなど、職員の情報セキュリティ水準の更なる向上、多様化する標的型攻撃への適切な対処のための教育・訓練を実施した。

情報セキュリティ監査については、2016年度に改定した復興庁情報セキュリティポリシー等について、「政府機関の情報セキュリティ対策のための統一基準群」への準拠性監査を実施するとともに、2016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や課題等を把握することで、復興庁全体の情報セキュリティ水準の向上のための課題及び必要な対策を確認した。

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群」の見直しを踏まえ、復興庁情報セキュリティポリシー等の関係規程の改定を行うとともに、2017年度に実施した情報セキュリティに関する自己点検や情報セキュリティ監査で明らかとなった課題等を踏まえ、情報セキュリティ教育のための研修教材の見直しの実施など、復興庁職員の更なる情報セキュリティ対策に対する意識の向上を図ることにより、復興庁全体の情報セキュリティ水準の維持・向上に取り組んでいくこととする。

総務省

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
政策統括官（情報セキュリティ担当）　谷脇　康彦

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すべ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。

〇2017年度の総合評価

2017年度は、前年度の対策推進計画にもと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、省内は概ね適切な状態が保たれていると評価をしている。

一方、所管法人において、外部委託先管理を含む情報システムの運用保守における情報セキュリティ管理の不備によって情報セキュリティインシデントが発生したことを受け、情報システムに関する全省的な点検、追加の外部監査等を実施した。

〇2018年度の計画

2018年度は、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。2017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。

政府統一基準群の改定に伴うポリシーの改定や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。2018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）
・不審な電子メールへの適切な対応に関する訓練

法務省

2017 年度の総合評価・2018 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　小山　太士

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政府機関を守るための取組の方向性を踏まえ、2017年度は、前年度に引き続き、サイバー攻撃への対応体制を更に強化するため、サイバー攻撃によって情報システム内部に侵入を試みる脅威を早期に検知する仕組みの整備等を行った。また、情報セキュリティマネジメントシステムの推進を図るため、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）の全面改定を行い、あわせて、情報セキュリティの教育、自己点検及び監査等といった各プロセスの全面的な見直しを行った。さらに、情報セキュリティの様々な取組の基盤となるセキュリティ・IT人材の更なる確保・育成を図るため、「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、引き続きその確保・育成の取組を進めた。

これらの取組等を総合的に評価すると、複雑かつ変化する環境下での当省のサイバー攻撃に対する組織的対応能力の向上に向けて、継続的な情報セキュリティ対策の維持向上のための基本的な枠組みは整ったものと認められる。もっとも、情報セキュリティ対策の取組は、それが組織全体で実行されなければ、サイバー攻撃をはじめとする様々な脅威に対処しきれないおそれがあるため、枠組みを整えるだけでは足りず、それを組織全体に浸透させ、かつ、実効性を確保していく必要がある。

したがって、2018年度は、前年度に全面改定を行った情報セキュリティポリシーの浸透を図るとともに、あわせて、それに基づく情報セキュリティマネジメントの実効性を確保するための仕組みを構築していく。また、急速に変化するサイバーセキュリティの情勢に柔軟かつ継続的に対応していくとともに、人材育成計画に基づき、セキュリティ・IT人材の確保・育成を着実に進め、複雑かつ変化する環境下での更なる組織的対応能力の向上に努めることとする。

外務省

2017 年度の総合評価・2018 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

2017年５月、身代金要求型ウイルス（ランサムウェア）の被害が世界同時多発的に確認されたことを受け、情報セキュリティ対策の重要性が一段とクローズアップされている。また昨今では、インターネットへの接続機能を持つ監視カメラや家電などのIoT機器を踏み台とした大規模なサイバー攻撃が発生しており、政府機関としても常に最新の動向を見極めながら情報セキュリティ対策を適切に実施していく必要がある。

外務省では、取り扱う情報の性質上、外国諜報機関や内外の攻撃者（クラッカー）によるサイバー攻撃の標的となる蓋然性の高さを強く認識しており、最新の情報セキュリティを取り巻く情勢を踏まえつつ、当省保有の情報システムに対する技術的な対策及び職員に対する教育啓発等を実施してきている。

2017年度においては、11月のトランプ米国大統領の訪日といった大規模イベントや国内外における様々な外交行事に際して、重大な情報セキュリティインシデントの発生は確認されておらず、これまで持続的に取り組んできた各種対策が奏功しているものと考えている。

このような状況の中、2017年度においては、計画に大きな影響を及ぼすような情勢変化は生じていないとの認識のもと、当初計画の回数や内容について拡充するなどした上で、主に以下の取組を行った。

（１）外務省独自に整備している情報セキュリティ対策資料に基づいた職員向けｅラーニング教育の実施（ｅラーニングによる実施は初）
（２）新たな脅威への対応策に係る迅速な注意喚起の発出及び外部専門家による情報セキュリティ集合研修の開催
（３）本省職員及び在外職員を対象にした標的型メール攻撃への対処訓練の実施（実施回数を２回に増加）
（４）より効果的かつ教育的な「情報セキュリティ対策の自己点検」とするため、設問内容について大幅な改定を実施（設問内容及び回答群を一新）

2018年度においては、前述の対策を継続的に実施していくことに加え、情報セキュリティ対策を推進する役割にある大臣官房情報通信課のみならず、各課室の情報セキュリティ責任者による各職員への指導・監督を強化するため、責任者向けに特化した教育資料及びｅラーニングコンテンツを整備し、実施すべく作業を進める。情報セキュリティ責任者が負う責任の重さや担うべき役割を明確に認識させることによって、外務省全体の情報セキュリティ水準のより一層の向上を期する。

また、これまでに実施した標的型メール攻撃訓練結果を分析し、更に効果的な啓発・教育方法について検討していく。

財務省

2017 年度の総合評価・2018 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、内閣サイバーセキュリティセンター（NISC）とも連携し、情報セキュリティの確保に取り組んできた。

2017年度においては、2016年度のサイバーセキュリティ基本法改正の趣旨を踏まえ、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のほか、定期的に省内・地方支分部局の幹部職員等を対象にした説明会を実施
・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
・システム所管部局・会計担当部局職員を対象とした説明会や、CIO補佐官による講演の開催
・省内における情報セキュリティ上の課題把握の観点から内部監査・自己点検等の実施
・NISCによる独立行政法人監査結果について、所管独法・特殊法人連絡会議を開催のうえ情報共有を実施
・基幹LANシステムの更改に際し、情報セキュリティ対策を強化
・前年度に施行した政府統一基準群及び財務省情報セキュリティ対策基準の改定を踏まえ、財務省内の下位規則である各実施規則の改正・整備
・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

これらの取組と並行して、システム統括部局に総括係を新設することにより、同係において省内研修等の情報発信に関する企画・運営を一元的に担うこととし、統括部局として情報セキュリティ対応体制を強化した。また、システム所管部局等職員の一部をシステム統括部局の併任とすることにより、統括部局とシステム所管部局の情報共有を深めるなど、情報セキュリティに関連する部局横断的な体制強化もあわせて行ったところ。

2018年度においても、着実に情報セキュリティ対策の強化を進めていくため、引き続き「財務省セキュリティ・IT人材確保・育成計画」（2016年８月策定。以下「育成計画」）に基づき、

・研修・説明会等の開催や各種外部研修への参加奨励（職員セキュリティ意識の向上）
・より計画的な監査・自己点検等の実施と、同実施結果の研修など他の取組みへの反映（PDCAサイクルの推進）
・所管する独立行政法人・指定法人等との連携（財務省組織を挙げた情報セキュリティ体制の構築）

の取組みを進めていく。

文部科学省

2017 年度の総合評価・2018 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　藤原　誠

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。

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強化する必要がある。

更に、2018年度に行われる政府機関等の情報セキュリティ対策のための統一基準群の改定方針に沿って、情報セキュリティ対策の見直しを行うことも求められることとなる。

以上を踏まえ、2017年１月に行政情報システムの運用を通じて更なる情報システムの防御力の強化、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・ハンドリング能力の強化
(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

2017 年度の総合評価・2018 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　宮野　甚一

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、2017年度においては、情報セキュリティインシデントの対処等についての緊急・専門的支援等の業務委託や、職員の危機意識やリテラシー向上のための集中的取組期間の実施、当省と所管する独立行政法人及び特殊法人等に対する情報セキュリティ監査及びデータベースを保有するシステムのリスク評価などに取り組んできた。

2018年度においては、これまでの成果を踏まえ、取組内容を一部見直して継続実施するとともに、新たに、政府統一基準群の改定に伴う当省情報セキュリティポリシー、関係規程の見直しなどに取り組むことにより、更なる対策の強化を図るものとする。

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

2017 年度の総合評価・2018 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)　2017年度は、我が国を含む世界規模で、身代金要求型の不正プログラム「ランサムウェア」に感染する事案が多数発生し、システム障害やサービス停止の被害が発生するなど、サイバー攻撃は、より一層、巧妙化・深刻化が進んでいる。また、サイバー攻撃に悪用されるおそれのあるソフトウェアの脆弱性も増加傾向にあり、より迅速かつ適切な対応が求められている。

(2)　このような中、農林水産省においては、重大な情報セキュリティインシデントの発生を防止するため、ソフトウェアの脆弱性に関する注意喚起等を適時・的確に行うとともに、省内に設置した農林水産省CSIRTを中心に、迅速かつ的確な初動対応等に当たってきたところである。

(3)　2018年度は、政府機関等の情報セキュリティ対策のための統一基準群の見直しが夏頃に予定されている。また、農林水産省情報化統括責任者（CIO）補佐官と兼務されている農林水産省最高情報セキュリティアドバイザーについては、兼務を解消し、外部委託により確保することとしている。

(4)　これらの状況を踏まえ、2018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構成員等に対し、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　政府機関等の情報セキュリティ対策のための統一基準群の見直しを踏まえた農林水産省における情報セキュリティ関係規程の改正
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

2017 年度の総合評価・2018 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　髙橋　泰三

近年 2017 年度においても、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）は引き続き存在し、対象や手法の多様化、規模の拡大の様相を呈していた。

このようなサイバー攻撃から重要な情報を守り、業務サービスを維持することが求められることから、2017 年度には主に次の取組を実施した。

(1)　2018 年 2 月に基幹 OA システムを運用開始し、認証機能の強化等のセキュリティ対策を実施
(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再確認を行い、セキュリティに係る設定の見直しと変更を実施
(3)　「経済産業省におけるセキュリティ・IT 人材確保・育成計画」（以下「人材確保・育成計画」という。）に基づく、有為な人材の確保、橋渡し人材向け研修の受講、処遇の確保等を実施
(4)　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・意識の向上のため、監査や自己点検を実施
(5)　セキュリティ水準を維持向上するため、省内規程の新設・変更や管理運用制度等の見直しを実施

2018 年度は、従来からの取組に加えて、昨年度より運用開始した基幹 OA システムに対する更なるセキュリティ対策等、当省システムを利用する国民へのセキュリティを確保する対策を強化していくこととする。具体的には以下の通り。

(1)　基幹 OA システムについて、更なるセキュリティ対策を強化
(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)　人材確保・育成計画に基づく取組の継続によるセキュリティ・IT 人材の確保・育成
(4)　2018 年に予定されている NISC による統一基準の改正に伴う、当省関連規程の変更等
(5)　監査や自己点検を通じた、各部局や職員一人一人の情報セキュリティに係る体制の強化・意識の向上
(6)　当省のインシデント・レスポンス能力の更なる向上のため、NISCの実施するCSIRT訓練や各種研修等に参加

国土交通省

2017 年度の総合評価・2018 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　由木　文彦

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に向けて、これらは、より一層、高度化・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、2017年度においては、主なものとして、以下の対策を実施した。

①国土交通省の情報セキュリティ対策の推進体制を強化するため、「情報セキュリティ対策室」の体制を強化して「サイバーセキュリティ対策室」に改組するとともに、外部委託事業者によるインシデント発生時の支援体制を強化

②セキュリティ・IT人材の確保・育成の強化を図るため、「国土交通省セキュリティ・IT人材確保・育成計画」を改定

③職員に対し、標的型メール攻撃訓練、役職段階別等の研修を実施するとともに、新たに本省管理職級研修を新設。また、本省全職員に情報セキュリティハンドブックを配布。さらに、総務省等が実施する研修への職員の参加を奨励するとともに、省内イントラネットの情報セキュリティ関連ページを充実

④情報セキュリティ対策の持続的な向上を図るため、情報セキュリティ対策の自己点検及び情報セキュリティ監査を実施

⑤内閣官房内閣サイバーセキュリティセンター（NISC）が実施するインシデント対処訓練及び情報通信研究機構（NICT）が実施するサイバー防御演習（CYDER）に参加

⑥これらのほか、独立行政法人、重要インフラ分野、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、重要インフラ分野の情報共有等の体制である交通ISAC（仮称）の創設に向けた支援、空港分野の重要インフラ化の促進、所管事業者向けの情報セキュリティ対策のチェックリストの作成等を実施

2018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職員への教育、②情報セキュリティ対策の自己点検、③情報セキュリティ監査、④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、⑤国土交通省情報セキュリティポリシー等の改定等を推進する。

環境省

2017 年度の総合評価・2018 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

昨今のサイバー攻撃では、検知されにくい未知の不正プログラムやスクリプトの使用や、脆弱性情報の公開直後に攻撃が開始されるなど、攻撃の成功率向上を狙った巧妙化が進んでいる。また、公開サーバに対する攻撃だけでなく、組織内部を対象にマルウェアを侵入させ情報を窃取する「標的型攻撃」や、パソコン等に保存されているファイルを暗号化し身代金を要求する「ランサムウェア」、監視カメラや周辺機器の悪用と、攻撃の対象も拡大するなど複雑化している。

環境省では、2016年度に基幹システムであるネットワークシステムを更改（以下「現行システム」という）し、侵入を前提とし、その拡大や活動を阻止・検知する入口対策、内部対策及び出口対策などの「多層防御」を備えたシステムを構築し、サイバー攻撃の影響の極小化を実現した。これにより、昨今のサイバー攻撃の脅威に対する『システム的対策』は強化されたところである。しかしながら、メール誤送信や情報資産の紛失など人為的なミスによるインシデント事案が引き続き発生している状況から、『人的対策』について更なる強化が必要であると考えている。

2017年度においては、情報セキュリティ及びシステム利用に関する一般職員におけるリテラシー向上を図るため、現行システムの情報セキュリティ対策を前提としたサイバー攻撃へのより実践的な対処方法等についてケーススタディーを交えて学習するとともに、標的型メール攻撃に対する適切な対処方法等の理解を深めるための訓練を実施するなど、一般職員への教育を重点的に取り組んだところである。

2018年度においては、『人的対策』について引き続き強化を図ると共に、職員教育を通じてPDCAサイクルの安定的な運用による情報セキュリティ対策の改善維持に取り組む。また、昨今の働き方改革の推進におけるICT活用のニーズを踏まえ、「利便性の向上」と「情報セキュリティの確保」といった、相反する目的を実現するための『システム的対策』について次期システムを見据えた検討を行う。更には、2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティリスクの拡大に備えるべく、環境省ホームページなど外部に公開しているシステムにおけるセキュリティ対策の強化を図る。

防衛省

2017 年度の総合評価・2018 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　西田　安範

2017年度においては、防衛省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の特別検査を実施し、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、2018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「OSやソフトウェアは常に最新の状態に」とし、全職員に対して、脆弱性の脅威に際し留意すべき事項について教育を行うとともに、サイバー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。

2018年度においては、前年度に引き続き、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の特別検査を実施するほか、NISCのCSIRT訓練に併せて省内メール訓練を行う。2019年２月の防衛省情報セキュリティ月間においては、情報セキュリティに関する最新の動向を踏まえた教育、標的型攻撃メール訓練及び講習会を実施する。また、マネジメント監査を実施し、情報セキュリティに関する施策の取り組み状況を確認するほか、情報システムに対するペネトレーションテストを実施することによって、サイバーセキュリティの強化を図る。

更に、防衛省と防衛産業との間において、引き続きサイバー攻撃対処能力向上のための共同訓練等を実施し、官民連携の強化を図る。

（本ページは白紙です。）

別添２　「サイバーセキュリティ 2017」に盛り込まれた施策の実施状況

＜別添２－目次＞

1. 経済社会の活力の向上及び持続的発展 67
1.1. 安全な IoT システムの創出 67
1.2. セキュリティマインドを持った企業経営の推進 69
1.3. セキュリティに係るビジネス環境整備 72
2. 国民が安全で安心して暮らせる社会の実現 75
2.1. 国民・社会を守るための取組 75
2.2. 重要インフラを守るための取組 82
2.3. 政府機関を守るための取組 90
3. 国際社会の平和・安定及び我が国の安全保障 94
3.1. 我が国の安全の確保 94
3.2. 国際社会の平和・安定 97
3.3. 世界各国との協力・連携 102
4. 横断的施策 107
4.1. 研究開発の推進 107
4.2. 人材の育成・確保 109
5. 推進体制 112

1. 経済社会の活力の向上及び持続的発展

1.1. 安全な IoT システムの創出

(1) 安全な IoT システムを活用した新規事業の振興

項番	担当府省庁	サイバーセキュリティ 2017	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 30 年度予算重点化方針」（平成 29 年 8 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。

(2) IoT システムのセキュリティに係る体系及び体制の整備

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、IoT システムに係る大規模な事業のサイバーセキュリティ確保のための取組について、サイバーセキュリティ戦略本部の下で検討を進めるとともに、IT 総合戦略本部等においても現在検討が進められている IoT システムに係る大規模な事業について、関係省庁が適切に協働し、セキュリティ・バイ・デザインの考え方に基づいて必要な対策が整合的かつ遺漏なく実施されていくよう働きかけを行う。さらに、その確認を適時確認していく。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」を踏まえつつ、官民の連携の下、安全な IoT システムの創出に向けた取組を推進する。	・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」を基本とした国際標準化活動を推進。2017 年 11 月のニューデリー会合にて日本提案を説明し、2018 年 2 月より新規作業項目提案に向けたプロセスを進めている。
(イ)	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。	・内閣官房において、IoT セキュリティ強化の観点から、実態把握、対策の実施・周知等の取組を推進する官民連携の枠組みとして、関係省庁及び民間も含めた関係者会合を開催し、関係する施策の取組状況等の共有、今後取り組むべき課題等についての議論を実施した。 ・警察庁において、2017 年９月に、ボットネットについて取り上げたフォーラムに参加し、講演及びパネルディスカッションを行った。 ・総務省において、一般社団法人 ICT-ISAC、国立大学法人横浜国立大学等と連携し、重要 IoT 機器を中心に IoT 機器の実態調査を行い、脆弱な IoT 機器の所有者等に対して注意喚起を行う取組を行った。 ・経済産業省と総務省において、IoT 機器の製造・販売事業者と連携し、IoT セキュリティガイドラインを活用した IoT 機器のセキュリティ対策に向けた検討を実施。 ・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を開催し、IoT 機器の製造・販売事業者と連携し、IoT セキュリティガイドラインの普及啓発及び汎用的な IoT 機器のセキュリティ確保策等の検討に向けた議論を開始。

(3) IoT システムのセキュリティに係る制度整備

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	総務省 経済産業省	総務省及び経済産業省において、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、IoT セキュリティの確保に向けた総合的な対策及び 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。	・総務省及び経済産業省において、「IoT セキュリティガイドライン ver1.0」の英訳版を公表した。また、IoT 推進コンソーシアム IoT セキュリティ WG を開催し、「IoT セキュリティガイドライン ver1.0」の普及啓発や IoT 機器のセキュリティ確保策等の検討を行った。 ・経済産業省において、「IoT セキュリティガイドライン」を踏まえ 2017 年 4 月に「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver1.0」を資源エネルギー庁エネルギー・リソース・アグリゲーション・ビジネス検討会のサイバーセキュリティ WG で作成した。続いて、2017 年 11 月に対象範囲を拡大した「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver1.1」へ改訂した。2017 年 3 月に IPA を通じ公開した「つながる世界の利用時の品質」の考え方が、特定非営利活動法人人間中心設計推進機構（HCD-Net）から 2017 年 10 月に公開された「つながる世界の利用時の品質確保のための活用ガイド」に採用された。
(イ)	経済産業省	経済産業省において、IoT システムの構成要素である M2M 機器等の制御システム向けのセキュリティに係る認証制度である EDSA 認証（2014 年 4 月開始）について、普及・啓発を行うとともに、制御システム全体のセキュリティ評価・認証の仕組みを検討する。	・経済産業省において、技術研究組合制御システムセキュリティセンター（CSSC）を通じて、IoT システムの構成要素である制御機器の国際標準に基づく認証規格の個別システムへの適用及び新たな個別システムへの適用に向けた国際動向に関して、海外機関との情報共有を行った。
(ウ)	経済産業省	経済産業省において、JPCERT/CC を通じて、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 56 件について、その保有組織に対して情報提供した。また、SHODAN のデータの信頼性について調査した結果、データの信頼性が低いことが判明したため、独自のデータ収集方法、システム化などの有効性などの検討を行った。
(エ)	経済産業省	経済産業省において、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により、ソフトウェアに係る脆弱性について、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」などを通じて利用者に提供する。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 を通じて ・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。2017 年度においては、ソフトウェア製品の届出 422 件、ウェブアプリケーションの届出 178 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、197 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、2017 年度においては、脆弱性対策情報を約 14,000 件（累計：約 81,000 件）公開した。

(4) IoT システムのセキュリティに係る技術開発・実証

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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、量子コンピュータに対する耐性を持つと注目されている格子暗号の安全性の根拠となる格子問題を解読する大規模並列計算機向け格子問題求解アルゴリズムの高速性について、理論的な裏付けに初めて成功した。

（イ）	経済産業省	経済産業省において、IoT のセキュリティ対策等に関する研究開発を行う。	・経済産業省において、 「IoT 推進のための横断的な技術開発事業」において、「Sensor-to-Cloud Security ～ ビッグデータを守る革新的 IoT セキュリティ基盤技術の研究開発」、「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」、「次世代産業用ネットワークを守る IoT セキュリティ基盤技術の研究開発」、計３件のＩｏＴのセキュリティ対策等に関する研究開発を採択し、事業を実施している。
（ウ）	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、脅威分析やリスク評価を行うに際し、効率的なリスク分析を行うために、制御システムに対する典型的なサイバー攻撃シナリオを作成し、それに基づくシナリオベースアプローチの手法を検討した。
（エ）	内閣府 総務省 経済産業省	内閣府 SIP（戦略的イノベーション創造プログラム）を中心に、経済産業省、総務省をはじめとする関係省庁と連携し、自動車のセキュリティ上の課題について、車両レベル・コンポーネントレベル、制御システム等の研究開発を推進する。	・戦略的イノベーション創造プログラム（SIP）において、関係省庁が連携しつつ、自動走行におけるセキュリティ脅威の調査及び分析を行い、セキュリティ評価ガイドライン案を作成した。
（オ）	総務省	総務省において、「IoT セキュリティ対策の取組方針 ver1.0」を踏まえ、既に流通している脆弱性を有する IoT 機器のセキュリティ対策に取り組むとともに、今後製造する IoT 機器のセキュリティ対策について検討を行う。	・総務省にて開催されたサイバーセキュリティタスクフォースにおいて、2017 年 4 月「IoT セキュリティ対策の取組方針 ver1.0」に基づき具体的な施策展開の在り方について検討を進め、同年 10 月に、IoT システムのセキュリティ対策の総合的な推進に向けて取り組むべき課題を整理した「IoT セキュリティ総合対策」を取りまとめた。 ・2017 年９月から、一般社団法人 ICT-ISAC、国立大学法人横浜国立大学等と連携し、重要 IoT 機器を中心に IoT 機器の実態調査を行い、脆弱な IoT 機器を特定した場合には、所有者等に対して注意喚起を行う取組などを行った。 ・NICT の業務にパスワード設定に不備のある IoT 機器の調査等を追加する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案」を 2018 年３月に国会に提出した。

1.2. セキュリティマインドを持った企業経営の推進

(1) 経営層の意識改革

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	内閣官房 金融庁 経済産業省	内閣官房において、関係府省庁と協力して、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」を踏まえ、企業のサイバーセキュリティに係る取組について、現状の把握を行い、さらなるサイバーセキュリティ対策の推進に関する検討を行う。	・内閣官房において、「企業経営のためのサイバーセキュリティの考え方」（平成 28 年８月２日）の見直しを念頭に、「セキュリティマインドを持った企業経営 WG」において、①経営層が持つべき意識や果たすべき役割、②経営層がリスクマネジメントの一つとしてサイバーセキュリティの取組を進めていく上での具体的な方策、③中小企業をはじめとする事業上のリソースの制約が大きい企業の対策、④産学官連携による取組について検討を実施し、報告書としてとりまとめた。
（イ）	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、サイバーセキュリティ経営ガイドラインのさらなる普及を図るべく、昨今のサイバーセキュリティに関する状況を踏まえて当該ガイドラインを 2017 年 11 月に改訂した。さらに、説明会を通じて当該ガイドラインの普及促進を図った。

（ウ）	経済産業省	経済産業省において、企業のサイバーセキュリティ対策を推進するため、サイバーセキュリティ保険など、情報の保護が必要となる政府の補助事業や研究開発事業等の採択に際して、上記のサイバーセキュリティ経営ガイドラインや第三者認証取得など企業のサイバーセキュリティ対策への取組を、加点要素等として考慮する仕組みなどのインセンティブ策を検討する。	・経済産業省において、IPA を通じて、サイバーセキュリティ経営ガイドラインをベースとした中小企業向け情報セキュリティ対策ガイドラインに準拠する取組の実施を自己宣言した企業に対して、自己宣言マーク（SECURITY ACTION）の利用を認める活動を実施した。損保会社では、マーク取得事業者に対し、サイバー保険の保険料を割り引くなどの取組が行われた。

(2) 経営能力を高めるサイバーセキュリティ人材の育成

項番	担当府省庁	サイバーセキュリティ 2017	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人材育成プログラムを踏まえ、経営層、橋渡し人材層、実務者層など、それぞれの人材層向けのさまざまな施策について連携を強化することにより、より効果的かつ効率的に施策が進められるよう、施策間連携を図るためのワーキンググループを通じ、モデルとなる具体的な人材育成のカリキュラムの策定等を行う。	・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」（平成 29 年 4 月 18 日）を踏まえ、「サイバーセキュリティ人材の育成に関する施策間連携 WG」において、①各層別の人材像やキャリアパスの明確化、②IT の基本的知識と各層別のカリキュラムの方向性、③各省の人材育成施策に関する全体像整理と連携策の検討、④教材の R&D、⑤産学官連携の在り方・具体的方策について検討を実施し、報告書としてとりまとめた。 ・並行して、内閣官房にて各層別の人材像、モデルとなるカリキュラムの方向性について調査を行い、「サイバーセキュリティ人材の育成に関する施策間連携 WG」にて報告を行った。

(3) 組織能力の向上

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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、近年多くの届出を受けている Windows アプリケーションの DLL 読み込みの問題や Wordpress プラグインの脆弱性に関して、問題の解説や対策の考え方に関する講演を行った。
（イ）	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、サイバーセキュリティ経営ガイドラインのさらなる普及を図るべく、昨今のサイバーセキュリティに関する状況を踏まえて当該ガイドラインを 2017 年 11 月に改訂した。さらに、説明会を通じて当該ガイドラインの普及促進を図った。 ・経済産業省において、IPA を通じて、サイバーセキュリティ経営ガイドラインをベースとした中小企業向け情報セキュリティ対策ガイドラインに準拠する取組の実施を自己宣言した企業に対して、自己宣言マーク（SECURITY ACTION）の利用を認める活動を実施した。損保会社では、マーク取得事業者に対し、サイバー保険の保険料を割り引くなどの取組が行われた。
（ウ）	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、セキュリティリスクの増大につながる丸投げ防止やセキュリティ対策費用の増大を踏まえ、適切な価格設定などを反映させた改訂版下請ガイドライン（2017 年 3 月公表）の周知活動として、リーフレットを作成し 700 か所への配布、および全国主要都市 5 都市以上で 15 回下請取引適正化セミナーを開催した。

(エ)	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、JPCERT/CC を通じて、日本シーサート協議会の運営委員及び事務局業務を通じ、国内組織における CSIRT 構築や機能強化、CSIRT 間の連携の促進等を積極的に支援している。同協議会の加盟組織数は 2017 年 3 月末時点では 219 組織であったが、2018 年３月末現在で 284 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加した。 ・地方公共団体向けの研修や分野横断の演習への協力等標的型攻撃やその他のサイバーインシデント対応に関する普及啓発と体制整備を目的に、普及啓発資料や演習プログラムを作成し、実施した。
(オ)	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、サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）を実施する。また、2020 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する。	・実践的サイバー防御演習（CYDER）については、2017 年度、全国 47 都道府県で 100 回の演習を実施し、計 3009 名が受講。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、2017 年度は計 74 名が受講。
(カ)	経済産業省	経済産業省において、重要インフラ企業等に対するサイバー攻撃への対処能力向上のため、模擬システム等を用いた実践的なサイバー演習を行う。	・経済産業省において、CSSC を通じて、電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等の関係者が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性を検証することを目的に、模擬システム等を用いた実践的なサイバーセキュリティ演習を行った。 ・上記 4 分野において、演習を計 5 回に分けて実施。計 128 名が参加した。
(キ)	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 を通じて、2017 年度、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 144 件行うとともに、うち 27 件に対してオンサイトでレスキュー活動を実施した。また、標的型攻撃に係る情報セキュリティ対策ベンダへの情報提供を 10 件行った。
(ク)	金融庁	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を引き続き実施する。	・金融庁において、2017 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、金融機関 101 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 Ⅱ）を実施。
(ケ)	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 を通じて、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、2017 年度のダウンロード数は 3,475 件と、利用拡大を図った。 ・解析対象ログの拡張については引き続き検討を実施した。
(コ)	経済産業省	経済産業省において、最新の脅威情報やインシデント情報等の共有のため IPA を通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう参加組織の拡大、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。	・経済産業省において、IPA を通じて、J-CSIP の情報共有活動については、着実な運用を継続した。2017 年度は 3,456 件の情報提供を受け、そのうち 274 件を標的型攻撃メールと判定した。情報の集約と分析を行い、242 件の情報共有を実施した。 ・IPA において、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、2016 年度までに体制構築した９産業分野（政府・行政サービス、情報通信（２団体）、電力、航空、金融、クレジット、重要インフラ事業者の地域団体・組織（２団体））に加えて、2017 年度に新たに体制構築した３産業分野（金融、鉄道、政府・行政サービス（２団体））に対して、情報処理システムの障害情報等を提供するとともに、積極的、かつ継続的な意見交換を実施して、自律的な障害情報共有に向けた支援を実施した。 ・STIX/TAXII による脅威情報の表現形式について、調査・検討を実施した。

(サ)	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。また、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案」を 2018 年 3 月に国会に提出した。
(シ)	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、2018 年３月現在、「金融 ISAC」の加盟社は 331 社（正会員）まで増加。

1.3. セキュリティに係るビジネス環境整備

(1) サイバーセキュリティ関連産業の振興

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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認定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、セキュリティ監査サービス、脆弱性診断サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準を定めた情報セキュリティサービス基準を策定した。当該基準に準拠するセキュリティサービスの流通状況について IPA に調査を依頼した。
(イ)	総務省 経済産業省	総務省及び経済産業省において、クラウドセキュリティガイドライン、クラウドセキュリティ監査制度等の普及促進を行う。	・総務省において、「クラウドサービス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の追加等を行っているところ。 ・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、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。
(ウ)	経済産業省	経済産業省において、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の施策を推進する。	・経済産業省において、 ・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した。また、中小企業投資促進税制においては、セキュリティ製品等への税制措置を継続した。 ・データ利活用の推進に必要なサイバーセキュリティ投資や IT 投資を支援する税制の特例等を含む生産性向上特別措置法案を閣議決定した。 ・ＩＴベンダー等を「情報処理支援機関」として認定し、その機関に対して、ＩＰＡによる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、IT ツールやベンダーの見える化により、安全で使いやすいＩＴツールの利用を促す仕組みの構築等を含む、中小企業等経営強化法の改正案を閣議決定した。
(エ)	文部科学省	文部科学省において、著作権法におけるセキュリティ目的のリバースエンジニアリングに関する適法性の明確化に関する措置を速やかに講ずる。	・文化審議会著作権分科会において、リバースエンジニアリングのための著作物の利用その他のニーズを踏まえた権利制限規定の在り方について検討を行い、2017 年 4 月に報告書を取りまとめた。これを踏まえ、リバースエンジニアリングのための著作物の利用を含む権利者の利益を不当に害しない一定の著作物の利用を許諾なく行えることとする権利制限規定等の整備を行う著作権法改正法案を、2018 年 2 月に国会に提出した。

(2) 公正な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 2017	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。	・経済産業省において、2017 年 6 月 14 日に第 3 回「営業秘密官民フォーラム」を開催し、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による企業情報の漏えいに関して産業界及び関係省庁と連携し、最新の手口や対応策に関する情報共有を行うと共に、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」を毎月配信し、判例分析や逮捕情報等に関する情報共有を行った。
(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、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～企業価値向上に向けて～」及びそのパンフレット「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～」について普及啓発を図った。
(ウ)	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の普及促進を図る。	・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 メーリングリスト）に向けたメールマガジンを 2017 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 6 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、「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」を実施し、2018 年 3 月に報告書を公開した。 ・「データ利活用における重要情報共有管理に関する調査」を実施し、2018 年 3 月に報告書を公開した。
(エ)	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。	・経済産業省において、セキュリティ確保を理由とした過度なセキュリティ規制への対応は、海外事業者にとって貿易制限的な措置となり得るため、当該規制の実施や導入を計画する諸外国に対して懸念を表明するとともに、規制改善のための意見交換と改善要請を図った。また、当該取組をＧ７外相会合や首脳会合の成果文書として反映させるべく検討を進めた。

(3) 我が国企業の国際展開のための環境整備

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	総務省 経済産業省	総務省及び経済産業省において、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。	・総務省において、国内関係機関と連携し、ITU-T SG17 会合（2017 年９月、2018 年３月）に我が国から IoT や ITS セキュリティに関する勧告策定に向けた寄与文書を入力するなど、国際標準化の議論に参加・貢献した。 ・経済産業省においては、専門機関と連携し、我が国が主体となって、ISO/IEC JTC1 SC27/WG4（2017 年 10 月）に IoT セキュリティガイドラインをベースとした IoT セキュリティ規格を提案し、国際標準化を推進した。

（イ）	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 を通じて、WG2 コンビーナ、WG3 副コンビーナ（2017 年４月ハミルトン会合、2017 年 10 月ベルリン会合）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。 ・WG2 については、日本技術の規格化作業を支援し、弱い秘密に基づく匿名エンティティ認証（ISO/IEC20009-4）、公開鍵暗号(ISO/IEC18033-2/AMD1)、秘密分散メカニズム（ISO/IEC19592-2）の規格を出版した。 ・WG3 については、副コンビーナ（2017 年４月ハミルトン会合、2017 年 10 月ベルリン会合）として、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。
（ウ）	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 を通じて ・NIST 脆弱性対策データベース NVD と JVNiPedia との連携、CVSS バージョン 3 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。
（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 を通じて、IEEE 策定のプロテクション・プロファイル（PP）に適合した認証を 2017 年度で 44 製品（保証継続を含む）に発行した。 ・米国と共同で開発した MFP のプロテクション・プロファイルを補完する eratta を作成し 2017 年６月に発表するとともに、当該 PP に適合した認証を 2017 年度 4 製品に発行した。
（オ）	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 12 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、マレーシア、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、IPA を通じて、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）が試験を実施するための協議会である ITPEC と協力し、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、2017 年８月にタイ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、経済産業省は、2018 年２月には、ITPEC 試験合格者で特に優秀な者として選出したアジアトップガン人材を日本に招き、日本企業と IT ビジネスや研究開発等に係るワークショップを実施するなど、アジアの優秀な IT 人材と日本の IT 企業との交流を図った。
（カ）	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、ASEAN10 か国の政府関係者に対して、「日 ASEAN 情報セキュリティ政策会議」の下で実施されたワーキンググループの開催（７月、２月）に際して、日本の取組事例について紹介したほか、「日英共催 ASEAN 諸国向けサイバーワークショップ」（２月）の開催に際してサイバーセキュリティと自由貿易の両立の重要性を訴求。また、AOTS 研修を活用し、2017 年度に専門家派遣２回（８月、２－３月）と訪日受け入れ研修１回(12 月)を実施。ベトナム電力公社の関係者に対し、電力分野のサイバーセキュリティについて日本が持つ知見を提供した。
（キ）	経済産業省	経済産業省において、JPCERT/CC を通じて、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。	・経済産業省において、JPCERT/CC を通じ、2017 年度にオフショア開発で大きなシェアを占めるインドにおいてセキュアコーディングセミナーを実施し、デリー、バンガロールの二か所で 100 名を超える受講者が集まった。
（ク）	経済産業省	経済産業省において、IoT システムセキュリティの国際標準規格を視野に入れた認証制度にかかる評価・検討を行う。	・経済産業省において、CSSC を通じて、IoT システムの構成要素である制御機器の国際標準に基づく認証規格の個別システムへの適用及び新たな個別システムへの適用に向けた国際動向に関して、海外機関との情報共有を行った。

2. 国民が安全で安心して暮らせる社会の実現

2.1. 国民・社会を守るための取組

(1) 安全・安心なサイバー空間の利用環境の構築

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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、2017 年度にオフショア開発で大きなシェアを占めるインドにおいてセキュアコーディングセミナーを実施し、デリー、バンガロールの二か所で 100 名を超える受講者が集まった。
(イ)	経済産業省	経済産業省において、IPA を通じ、IoT 機器、サービスを支える組込み産業の高度化に向け、産業動向の把握・分析を行うとともに、「セキュリティ・バイ・デザイン」の産業展開の観点から、セキュリティとセーフティ設計プロセスの整合化やシステムアプローチによるセキュリティ分析手法の検討を進め、組込みコーディングスタンダードの整備普及を図る。	・経済産業省において、IPA を通じて、2018 年 2 月に、「組込みソフトウェア開発向けコーディング作法ガイド［C 言語版］（ESCR_C 言語版）Ver.3.0」を Web 公開するとともに、同ガイドの英訳版についても 2018 年 3 月に Web 公開した。また、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 2018 年 3 月に Web 公開した。
(ウ)	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、AppGoat V3.0 を活用して集合教育を行う上で必要な段取りや注意点をまとめた以下の資料を公開した。また、これら資料を基にした 2018 年度セミナーを計画した。 ・脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き ・AppGoat を利用した集合学習補助資料 -SQL インジェクション編/クロスサイトスクリプティング編/クロスサイトリクエストフォージェリ編
(エ)	経済産業省	経済産業省において、IPA を通じ、情報処理システムや組込みシステム等におけるソフトウェアの不具合や脆弱性が社会に与える混乱や被害を防止する観点から、企画・設計段階からセキュリティ配慮が行われるよう IoT セキュリティガイドラインの普及・国際標準化の取り組みを進めるとともに、ソフトウェアによって中核機能が実現される製品、システム及びサービスについて第三者がその安全性・信頼性等を利用者に対し十分に説明できるよう、設計プロセス・利用時体験・流通するデータ等多面的な観点から利用者への品質説明力を強化する。	・経済産業省において、IPA を通じ、「IoT セキュリティガイドライン」を基本とする考え方を国際標準化するべく、一般社団法人情報処理学会情報規格調査会と連携して「IoT セキュリティガイドライン国際標準化専門委員会」を設置し、国内の検討体制を構築した。また、同専門委員会傘下に「ISO/IEC JTC 1/SC 27/WG 4」に対応する国内小委員会「SC 27/WG 4 小委員会」を設置し、新規規格提案のための原案を作成した。さらに、2017 年 10 月にドイツ・ベルリンで開催された「ISO/IEC JTC 1/SC 27」の会合にて、作成した新規規格提案の原案を新規検討項目（New Work Item）にすべく説明を行った。 ・IPA において、今後の普及に活かすため、製品・サービス等の異なる 27 の業界団体・機関等に対し、情報処理システムの信頼性向上に関する利用者や業界等のニーズや課題の把握を行った。
(オ)	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、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」の運用などにより、脆弱性関連情報をより確実に利用者に提供する。	・経済産業省において、IPA 及び JPCERT/CC を通じて、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。2017 年度においては、ソフトウェア製品の届出 422 件、ウェブアプリケーションの届出 178 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、197 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、2017 年度においては、脆弱性対策情報を約 14,000 件（累計：約 81,000 件）公開した。
(カ)	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。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。

(キ)	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、セキュリティキャンプ、専門学校等での講演及び「ファジング入門セミナー」の開催を実施した。
(ク)	総務省	総務省において、NICT を通じ、運用するサイバー攻撃観測網（NICTER）について、センサーの高度化等による観測機能の強化を図るとともに、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、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継続的に実施した。また、IoT 機器からの応答データを自動分類して IoT 機器の判定を機械学習により行う手法を開発し有効性を実証した。
(ケ)	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、マルウェアに感染したユーザーを検知し、マルウェアの除去を促す取組（感染駆除）及び閲覧することでマルウェアに感染する悪性サイトへアクセスする利用者に注意喚起を行う取組（感染防止）等を行う実証（ACTIVE）を引き続き実施する。	・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、閲覧することでマルウェアに感染する悪性サイトへアクセスする利用者に注意喚起を行う取組（感染防止の取組）及びマルウェアに感染した端末が C&C 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取組（被害未然防止の取組）等を行う実証を実施した。
(コ)	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、中東・アフリカ地域の NationalCSIRT が加盟している OIC-CERT 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。また、APCERT の日本での年次総会に合わせて、主に TSUBAME 参加組織に対してワークショップを実施し、香港の 2 つの CSIRT に対しトレーニングを行い、現場のエンジニア向けに、TSUBAME のデータを使った分析手法を共有した。TSUBAME の Web サイト内に加盟組織間で情報共有をするための機能を追加中である。
(サ)	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 と連携し、フィッシング対策協議会が届出を受けたフィッシングサイトについてサイト閉鎖を依頼している。 また、JPCERT/CC は国内外からフィッシングサイトの情報提供をうけ 、2017 年度は、約 3.5 千(3,523)のフィッシングサイト閉鎖の対応を行った。そのうち 75%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ている。
(シ)	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。 ・icat の利用サイト数は約 1,200 サイトとなった。
(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。	・公衆無線 LAN のセキュリティ対策の推進状況を把握するため、全国調査を実施した。
(セ)	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、利用者及びアクセスポイント設置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、利用者及びアクセスポイント設置者に対する周知啓発を実施する。	・普及啓発のためのセミナーを６都市で６回開催し、261 名が聴講した。また、総務省において、2017 年 11 月から「公衆無線 LAN セキュリティ分科会」を開催し、公衆無線 LAN におけるセキュリティ上の課題を整理し、必要な対策について、検討を行った結果を報告書及び行動計画として取りまとめた。
(ソ)	内閣官房	内閣官房及び関係省庁において、サイバー空間を安全に利用でき、また安全に発展させるよう、サイバーインシデント情報やその脅威情報を分析し、民間等の関係主体と共有することで着実にそのインシデント等への対応に繋げるため、情報共有・連携ネットワーク（仮称）の構築・運用に向けた検討を進める。	・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を創設する等の措置を講じるため、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第１９６回国会に提出した。

(2) サイバー空間利用者の取組の促進

項番	担当府省庁	サイバーセキュリティ 2017	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」の改訂を行うとともに、同プログラムに基づき、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を通じ普及啓発活動を進める。	・内閣官房において、「普及啓発・人材育成専門調査会」にてサイバーセキュリティ普及啓発に関する施策の今後の方針の検討を行った。 ・２月１日～３月 18 日に、NISC が中核となり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行う「サイバーセキュリティ月間」を実施した。 ・「サイバーセキュリティは全員参加！」をキャッチフレーズに、普及啓発イベントやテレビアニメ「BEATLESS」とのタイアップ等、官民連携して実施した。 ・特に、NISC から全府省庁に改めて協力を呼びかけ、政府一体となって更に拡大して取り組み、全国で官民による計 189 件の関連行事を実施した。
(イ)	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ほか、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。	・出会い系サイト等に関連した犯罪の被害防止を図るため、中学生・高校生向けのリーフレットを 2017 年６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、各種ソフトウェアに係るぜい弱性情報、サイバー攻撃の観測状況等のサイバーセキュリティ関連情報を広く一般に提供した。 ・ＪＣ３に対してサイバーセキュリティ関係情報の提供を実施した。 ・情報セキュリティ・ポータルサイト「ここからセキュリティ！」を活用し、官民連携した広報啓発活動を実施した。 ・警察庁の統合ウェブサイトとして、サイバーポリスエージェンシーを 2017 年６月に開設した。 ・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、2017 年 10 月のサイバーセキュリティ国際キャンペーン及び 2018 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。
(ウ)	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、電子署名の利活用に関するセミナーの開催及び HP を活用した電子署名の利活用策に関する情報提供を行うことで、国民による安全なサイバー空間の利用をサポートするとともに、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、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。
(エ)	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。	・児童生徒・保護者・教職員等を対象とした子どもたちのインターネットの安心・安全利用のための啓発講座である e-ネットキャラバン(e-ネット安心講座)を 2,309 件実施。 ・また、2017 年は、神奈川県座間市での事件を踏まえ、例年春に実施している「春のあんしんネット・新学期一斉行動」の名称を「あんしんネット　冬休み・新学期緊急一斉行動」として、12 月から前倒し実施し,集中的な取組を展開した。

（オ）	文部科学省	文部科学省において、2015 年度に作成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、指導主事、教員等を対象としたセミナー及びフォーラムを実施する。	・教員等を対象とした情報モラル教育指導者セミナー・フォーラムについて、2018 年２月までに実施済。
（カ）	文部科学省	文部科学省において、全国の学校へ配布する普及啓発資料の作成や、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、全国の小中高等学校等への啓発資料の作成・配付と、ネットモラルキャラバン隊などによる普及啓発活動を実施した。
（キ）	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、2017 年度、8,652 件ダウンロードされた。
（ク）	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、情報モラル・セキュリティコンクールを開催。2017 年度は、学校単位での情報モラル・情報セキュリティを促進させるため、他校の参考となる優れた活動に取り組んでいる学校を称える「優秀活動事例賞」を新設、授与した。また、最も優れた活動に取り組んでいる学校に対して 2016 年度に引き続き文部科学大臣賞を授与した。 ・全国の小中高生から、標語 55,744 点、ポスター5,493 点、4 コマ漫画 6,720 点、書写（硬筆）2,292 点、合計 70,249 点の応募があった。この取り組みを通じて、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。
（ケ）	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。	・2017 年６月に「情報セキュリティ社会推進協議会総会」を開催し、地域を含む会員全体の取組の報告と普及啓発活動に関する意見交換を行った。 ・また、2017 年 12 月に「情報セキュリティ社会推進協議会運営委員会」を開催し、全国各地での取組を行っている団体等の参加の下、普及啓発活動の在り方に関して議論を行うとともに、2018 年「サイバーセキュリティ月間」に向けた意見交換を行った。
（コ）	経済産業省	経済産業省において、IPA を通じ、各府省庁と協力し、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、全国各地域で、NPO 等の団体と連携により「インターネット安全教室」を合計 91 回開催し、小中高校生からシニア層まで合計約 7,100 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 4 箇所において開催し、合計約 100 名が参加した。また、座間市において発生した事件に関連し SNS の適正な利用促進のための研修等に向けた講師トレーニング用資料を作成し、NPO 等の団体関係者約 40 名に対しトレーニングを試行した。
（サ）	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 を通じて、広く企業及び国民一般に情報セキュリティ対策を普及するため、セミナー等への講師派遣（196 件）や展示会への出展等による情報の周知・提供を実施した。

(シ)	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30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1,564名が参加した。 ・また、中小企業団体との連携により2017年2月に公表した中小企業における情報セキュリティ対策の普及促進に資する中小企業共同宣言の枠組の下、IPAは、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」を創設し、その普及と登録促進を図るため、共同宣言参加団体等関連各団体及び地域経済産業局との連携により全国9か所で「中小企業情報セキュリティセミナー」を開催、約500名が参加した。これらの開催等を通じて、IPAが作成する情報セキュリティ啓発資料や情報セキュリティ対策支援サイト等のツールを紹介し、利用促進を図った。
(ス)	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14件、「注意喚起情報」を37件、「安心相談窓口だより」を11件(うち2件は更新)公表した。 ・経済産業省において、JPCERT/CCを通じ、情報セキュリティに関する脅威情報やそれらの分析・対策情報を「早期警戒情報」を47件、「注意喚起情報」65件を発信した。
(セ)	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おいて、電話、メール、FAX等で10,374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412件実施した。これを通じて、不審メールを799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。
(ソ)	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、2017年7月に、情報セキュリティ白書を発行した。 ・「情報セキュリティ脅威と倫理に関する意識調査（2017 年版）」を実施し、2017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インシデント及びマネジメントに関する調査」を実施し、2018年3月に報告書を公開した。 ・「CISO等の役割事例調査」を実施し、2018年3月に報告書を公開した。 ・上記に関連する普及啓発のための講演を11回行った。
(タ)	文部科学省	文部科学省において、大学等における多岐にわたる情報資産や多様なシステムの利用実態といった特性を踏まえ、大学等のマネジメント面・技術面の取組の強化を促進するとともに、大学等の自律的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る枠組みを整備し、これら取組を支援する。	・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等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。 ・国立大学法人等の監査担当者等に対して、情報セキュリティ監査の基礎知識等に関する研修を実施し、自律的な監査の実施に向けた支援を行った。 ・国立大学法人等のセキュリティ担当者を対象とし、インシデント対応などの実践的な研修を実施した。 ・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、国立情報学研究所による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。

(チ)	内閣府	個人情報保護委員会において、関係省庁と協力し、2017年5月30日に全面施行された改正個人情報保護法を踏まえ、個人情報取扱事業者における、外部からの不正アクセス等による個人データの漏えい等にかかる対応が適切に実施されるよう、情報セキュリティ関係機関と連携して取り組む。	・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について、事案の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・助言等を行った。また、情報セキュリティ関係機関との連携を図るため、個人情報サイバーセキュリティ連携会議を設置・開催するとともに、個人データに係る漏えい等の事案の状況や最近の情報セキュリティインシデントについて情報共有を行った。

(3) サイバー犯罪への対策

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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。
(イ)	警察庁	警察庁において、サイバー空間の脅威に対処するため、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、総合セキュリティ対策会議等において官民連携による取組を推進する。	・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、インターネットショッピングに係る詐欺サイト対策等を実施した。 ・「新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進について」をテーマに2017年度サイバーセキュリティ政策会議を開催し、報告書を取りまとめた。 ・都道府県警察において、インターネットカフェ連絡協議会等を通じ、利用者の追跡可能性の確保の要請や犯罪情報の提供等を行い、事業者の自主的な取組に関する指導・支援を実施した。 ・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。
(ウ)	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。 ・2017年中の不正アクセス行為の発生状況等を2018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。

(エ)	警察庁	警察庁において、サイバー空間における犯罪被害防止のための教育等のボランティア活動の促進を図るため、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。	・警察庁において、サイバー防犯ボランティア団体を集めて、好事例となる取組について情報共有を行うなど、活動の支援を行った。 ・都道府県警察において、2017 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、2017 年末現在の全国のサイバー防犯ボランティア数は、221 団体 8,294 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。
(オ)	警察庁	警察庁において、スマートフォン利用者等を狙ったサイバー犯罪に関し、情報セキュリティ関連事業者等との連携強化による情報集約等に努め、取締りの強化を図る。また、取締りにより判明した実態等を踏まえ、一般利用者等の情報セキュリティ対策の向上に資する情報発信等を推進する。	・警察庁において、スマートフォンにおける被害も確認されているランサムウェアについて、その被害防止対策等を盛り込んだ情報セキュリティ対策 DVD の活用、警察庁ウェブサイトにおける注意喚起等の広報啓発を実施した。 ・都道府県警察において、スマートフォン利用者等を狙ったサイバー犯罪の取締りに努めるとともに、学校等教育機関、一般国民に対し、スマートフォンを利用する際の情報セキュリティに関する広報啓発を実施した。
(カ)	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、最新のサイバー犯罪情勢に応じた課程の見直しを行うとともに、サイバー犯罪対策・サイバー攻撃対策に専従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、サイバー空間における警察全体の対処能力向上に資する研修を実施した。
(キ)	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、JPCERT/CC を通じ、米国 APWG が 4 月に主催した APWG eCrime 2017 (スコッツデール) 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、協議会の各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の改定 (2018 年度初頭に公開予定) を進めるとともに、「STOP THINK CONNECT」の啓発イベントを開催するなど、フィッシング対策の啓発活動に取り組んだ。
(ク)	警察庁	警察庁において、全国の情報技術解析部門で効果的かつ効率的な解析を推進することにより、多様化・複雑化が著しいサイバー犯罪に的確に対処する。また、家電、電気メーター、自動車等の日常生活に近い機器に係るオンライン化等の新たな技術やサービスの開発が次々に進められている背景を踏まえ、デジタルフォレンジックに係る対処能力をより一層強化する。	・デジタルフォレンジック用資機材の更新を行い、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、関係機関との協力を推進した。 ・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、最新のサイバー犯罪情勢に応じた課程の見直しを行うとともに、サイバー犯罪対策・サイバー攻撃対策に専従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、サイバー空間における警察全体の対処能力向上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。
(ケ)	法務省	法務省において、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査能力の充実を図る。	・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。
(コ)	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。

（サ）	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、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」の解説の改正を踏まえ、関係事業者への周知を図り、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. 重要インフラを守るための取組

項番	担当府省庁	サイバーセキュリティ 2017	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、（イ）、「情報共有体制の強化」については(1)(ア)、(2)(ア)・(エ)、(3)(ア)・(キ)、「障害対応体制の強化」については(カ)、「リスクマネジメント及び対処態勢の整備」については(ウ)、「防護基盤の強化」については本項目、(1)(ア)に取組の詳細を記載）。 ・「安全基準等」の整備を支援するため、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）(案)」を策定した。また、「安全基準」等の浸透については、「安全基準等の浸透状況等に関する調査」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 2018 年３月の重要インフラ専門調査会に報告した。 ・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セミナーや講演会等を開催し、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）	内閣官房	重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。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］ ・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、所管事業者の対策状況調査結果等を受けて、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 2018 年３月の重要インフラ専門調査会に報告した。 ・制度的な枠組みに関する現状の把握に努めた。 ［金融庁］ ・FISC において、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」を開催し、リスクベースアプローチの導入、外部委託に関するリスク管理、FinTech に関するリスク管理に関する考え方を反映し、「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 2018 年３月に改訂。 ・FISC において、昨今のサイバー攻撃動向等を踏まえ、「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」を 2017 年５月に改訂。 ［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３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、ICT-ISAC 放送設備サイバー攻撃対策 WG において「放送設備に関するサイバーセキュリティガイドライン」を作成している。 ・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］ ・医療分野については、2017 年５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」の改定を行い、第５版の公表を行った。 ・水道分野については、「水道分野における情報セキュリティガイドライン（第３版）」（2013 年６月）を改定中である。 ［経済産業省］ ・石油・化学・クレジット分野において、2017 年度に安全基準（ガイドライン）の分析・検証を実施した。うち、石油・クレジット分野においては、その結果を受け、安全基準（ガイドライン）の改訂を実施した。 ［国土交通省］ ・2018 年４月から、主要な空港ビル事業者等が「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく各種取組みを開始することから、事業者自らが情報セキュリティ対策を実施するにあたっての参考となるように、国土交通省において 2018 年３月に「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」を作成した。

（ウ）	内閣官房	内閣官房において、重要インフラサービスを安全かつ持続的に提供できるよう、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、情報セキュリティ対策に関する取組を推進。また、この取組を通じ、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。 ・迅速かつ効率的な情報共有に資するため、情報共有システム構築に係る調査検討を行う。 ・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」の一般化を行う。 ・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等を整理する。 ・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整理等を行う。	・新たに構築する情報共有システム及びホットラインを含む新たに設置した情報連絡ルートの効果的運用の定着に向けた検討を開始した。 ・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「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」を作成し、2018 年 3 月 20 日の専門調査会にて承認された。安全基準等策定指針の関連文書として、2018 年 4 月に公表予定である。 ・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「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」を整理し、安全基準等策定指針の別紙として掲載した。同指針は 2018 年 4 月に公表予定である。 ・事業者等における内部監査等の取組について、リスクアセスメント手引書の参考項目として「リスクマネジメントの取組に対する内部監査」の項目を作成し、機能保証の考え方を踏まえ、リスクに適切に対処できているかという視点からの考慮を推奨する観点を記載した。
（エ）	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、申告受付の夜間・休日の全国一元化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研究を実施する。	・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、2017 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次世代化を進め、また、同施設のセンサ 19 か所を 2017 年度内に更改した。 ・高い周波数帯や低い出力の無線局に対する電波監視を強化するための小型モニタリングセンサを設置した。
（オ）	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。	・2016 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、2017 年 7 月に公表した。 ・2017 年 8 月に発生した大規模なインターネット障害について分析・検証を行い、その結果を 2017 年 12 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、見直す検討を 2018 年 3 月から開始した。

(カ)	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 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、重要インフラにおけるサイバー攻撃への対処能力を向上させ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、重要インフラ等企業におけるサイバー攻撃に対する対応能力を向上させるため、模擬システムを活用した実践的なサイバー演習を実施する。 ・金融庁において、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。	・内閣官房において、2017 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。 ・総務省において、2017 年度は、実践的サイバー防御演習（CYDER）に重要インフラ事業者から 553 名受講。 ・金融庁において、2017 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、金融機関 101 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 Ⅱ）を実施。（再掲） ・経済産業省において、CSSC を通じ、電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等の関係者が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性を検証することを目的に、模擬システム等を用いた実践的なサイバーセキュリティ演習を行った。上記 4 分野において、演習を計 5 回に分けて実施。計 128 名が参加した。
(キ)	経済産業省	経済産業省において、IPA に、2017 年４月に「産業サイバーセキュリティセンター」を設立し、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向けて、7 月に教育カリキュラムを開始する。さらに、センターにおいて、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、2017 年４月に IPA に「産業サイバーセキュリティセンター」を設立した。同年７月から、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材を育成する「中核人材育成プログラム」を開始し、約 80 名の受講生を受け入れ、１年間のカリキュラムを実施。また、各社の CISO およびその補佐等を対象とした、短期プログラムも計６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２業種において実施。

(1) 重要インフラ防護の範囲等の不断の見直し

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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。	・重要インフラの４分野でセプター構成員が増加し、また、医療セプターがセプターカウンシルに参加するなど、セキュリティの取組の輪が広がっている。

(2) 効果的かつ迅速な情報共有の実現

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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判断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。 ・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）の検討を進める。	・サービス障害の深刻度を評価する基準について、専門調査会の下に設置されたワーキンググループにおいて検討を実施。2018 年３月末の重要インフラ専門調査会においてパブコメ案が了承され、今後、パブコメの手続きに付す予定。 ・分野横断的演習やセプター訓練において、予兆・ヒヤリハットに関する情報も共有すべき情報の対象である旨を喚起した。 ・迅速かつ効率的な情報共有に資するため、情報共有システム構築に係る設計に着手した。

（イ）	経済産業省	経済産業省において、官民における最新の脅威情報やインシデント情報等の共有のため、IPAが情報ハブとなり実施している「サイバー情報共有イニシアティブ」（J-CSIP）について参加組織の拡大、共有情報の充実を行う。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、障害事例や提供情報の分析結果等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を通じて、J-CSIPの情報共有活動の着実な運用を継続した。2017 年度は 3,456 件の情報提供を受け、うち 274 件を標的型攻撃メールと判定した。情報の集約と分析を行い、242 件の情報共有を実施した。 ・J-CSIP の参加組織は 228 組織（複数業界に関係する組織が複数の SIG に所属するケースがあるため延べ数）へと一層拡大した。 ・IPA において、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、2016 年度までに体制構築した９産業分野（政府・行政サービス、情報通信（２団体）、電力、航空、金融、クレジット、重要インフラ事業者の地域団体・組織（２団体））に加えて、2017 年度に新たに体制構築した３産業分野（金融、鉄道、政府・行政サービス（２団体））に対して、情報処理システムの障害情報等を提供するとともに、積極的、かつ継続的な意見交換を実施して、自律的な障害情報共有に向けた支援を実施した。
（ウ）	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。また、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、47 件の「早期警戒情報」を発行した（2018 年３月末現在）。 ・被害の発生及び拡大抑止のための関係者間調整を実施した（調整件数 8,891 件：2018 年３月末現在）。そのうち、重要インフラ事業者を主な対象としたインシデント関する対応支援は 220 件であった。また制御システムに関する対応支援は、３件のインシデント報告を受領し、計 14 件のインシデント通知を行うとともに、制御システムの関係者向けに 22 件の参考情報と 12 件の月次ニュースレター、103 件のニュースクリップなどの情報発信を行った。
（エ）	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から情報を受領し、重要インフラ事業者等への情報提供を行った（54 件）。また、同機関が分析した情報の横展開を行った。 ・第４次行動計画においては、情報連絡元を秘匿化するルートの新設（セプター事務局等経由）やホットラインの導入とともに、情報共有システムも活用して分野横断的に情報の集約・分析・共有する仕組みを構築する旨を明記したが、セプター事務局経由で匿名化された情報が出てくるなど、一定の効果が出ている。
（オ）	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、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整備・構築に向けた検討を行う。	・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した。また、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整備・構築に向けて、試行環境を構築しての実証実験を実施した。

（カ）	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、関係省庁との情報共有等を通じて、サイバー攻撃事案の攻撃者や手口の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とともに、重要インフラ事業者等の意向を尊重し、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。	・「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とともに、サイバー攻撃の実態解明を図っている。 ・各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。 ・警察庁において、サイバー攻撃事案の攻撃者や手口の実態解明を推進するため、サイバー攻撃に係る情報の集約・分析等のための体制を強化した。
（キ）	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、2018年6月までの円滑な施行に向けて、政省令等の整備を進める。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、2017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-2017-」に基づく関係事業者等の取組を更に推進するとともに、進捗状況等を踏まえて、必要な見直しを行う。	・経済産業省において、「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月の施行が決定した。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月に改訂を行い、「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-」を策定した。

(3) 各分野の個別事情への支援

項番	担当府省庁	サイバーセキュリティ2017	取組の成果、進捗状況
（ア）	内閣官房	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。	・内閣官房において、サイバーセキュリティ基本法に基づき、地方公共団体がサイバーセキュリティ戦略本部に協力を求められるよう、連絡先窓口を整備し、周知している。 ・重要インフラの情報セキュリティ対策に係る第4次行動計画等に基づき、地方公共団体で発生した重要インフラサービス障害等の事案について、内閣官房に情報連絡してもらうとともに、内閣官房において集約した情報セキュリティに関する情報について、総務省を経由して地方公共団体への情報提供を行っている。

（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。	J-LIS における研修実施結果 ・集合研修、ｅラーニング共、予定どおり実施した。実施結果は、以下のとおり。 ・集合研修 ・情報セキュリティ最新動向セミナー等 ・10 回開催、受講者数：678 人 ・情報セキュリティ監査セミナー ・２回開催、受講者数：93 人 ・情報セキュリティマネジメントセミナー ・２回開催、受講者数：105 人 ・ICT-BCP セミナー ・２回開催、受講者数：88 人 ・ｅラーニングによる情報セキュリティ研修 ・情報セキュリティ研修 ・８コース、受講者数：399,973 人 ・情報セキュリティ対策等研修支援 ・13 道府県が主催する情報セキュリティ研修に 406 団体が受講 ・「情報セキュリティ最新動向セミナー」の動画撮影及び提供 ・地方公共団体職員が情報セキュリティ研修用に活用できるテキストの提供
（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 上のセキュリティ支援ポータルサイトにおいて、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 68 件、ニュース・メルマガ 51 件） ・地方公共団体の外郭団体での情報セキュリテイ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。(実績:2017 年 12 月より開始)
（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。2016 年度に作成・提供した訓練ツールを活用し、地方公共団体のインシデント即応体制の強化を図る。	・公開サーバや内部のサーバ、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セルフ診断ツールを作成し、提供した。新たな脆弱性にも対応できるようツールの保守・運用も行った。（実績:ヘルプデスクへの問合せ 48 件） ・2016 年度に作成・提供した訓練ツールを活用し、地方公共団体が緊急時対応訓練を実施する場合、訓練のコントローラーや評価者を派遣した。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:10 府県、164 団体が参加)

(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・検知を行うとともに、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構築に係るフォローアップ及び、2017 年度予算を活用し、地方公共団体の情報セキュリティ対策に係る LGWAN 環境の健全性を補完する新たなプラットフォームの構築により、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。また、情報提供ネットワークシステム等のマイナンバー関係システムについて、インターネットから独立する等の高いセキュリティ対策が講じられたものとなるよう、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。	・個人情報保護委員会と関係省庁等との間における特定個人情報の情報セキュリティに関する連携、関連システムへのサイバー攻撃等の兆候を検知した場合の連絡・対応を円滑に行う場として設置した「特定個人情報セキュリティ関係省庁等連絡協議会」を開催し、特定個人情報の情報セキュリティに関して、関係機関と情報共有を行った。 ・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について運用を開始した。 ・加えて、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セキュリティ・ＩＴ関係の講座を有する大学での講座受講等の専門的知識の会得に重点を置いた研修の実施に注力した。 ・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構築に係るフォローアップを実施するとともに、2017 年度予算を活用し、地方公共団体の情報セキュリティ対策に係る LGWAN 環境の健全性を補完する「自治体情報セキュリティ向上プラットフォーム」を構築し、運用を開始した。 ・総務省において、2017 年 5 月に個人情報保護委員会と協議のうえ、情報提供ネットワークシステムの設置を行い、7 月より情報連携の試行運用、11 月より本格運用を開始した。また、2017 年度当初予算において、情報提供ネットワークシステムにおけるログの分析機能等のセキュリティ対策事業費を確保・実施した。
(カ)	内閣官房 内閣府	内閣府において、2017 年 7 月に試行運用を開始し、2017 年秋頃に本格運用を開始する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 との認証連携を開始した。
(キ)	内閣官房 経済産業省	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、経済産業省において、IPA と JPCERT/CC と連携し、制御システムに係る脆弱性情報の提供収集・分析・展開にも取り組む。	［NISC］ ・IPA や JPCERT/CC といった情報セキュリティ関係機関との意見交換や、重要インフラ事業者及び機器ベンダー等との意見交換・設備の視察等を行い、さらに、制御機器・システムのセキュリティに関する情報収集を行い、今後の取組の方向性等を検討した。 ・第４次行動計画においては、共有すべき情報として制御系システムや IoT システムの不具合等に関する情報も含まれることを明確化するとともに、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旨を記載しており、分野横断的演習の場などにおいてその位置付けの浸透を図った。 ［経済産業省］ ・JPCERT/CC を通じて、米国 ICS-CERT などからの連絡を受けて、14 件の制御システム関連の脆弱性調整を行った。 ・そのほか、制御システムに関する３件のインシデント報告を受領し、計 14 件のインシデント通知を行うとともに、制御システムの関係者向けに 22 件の参考情報と 12 件の月次ニュースレター、103 件のニュースクリップなどの情報発信を行った。 ・IPA において、制御システム関連の脆弱性情報の届出を３件受け付けた。 ・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、JPCERT/CC は、脆弱性情報の受け付け、制御システム関連の脆弱性 14 件の調整を行った。

（ク）	経済産業省	経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、セキュリティ対策に関する知見を収集し、それに基づいた実践的な演習を実施する。	・経済産業省において、CSSC を通じ、電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等の関係者が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性を検証することを目的に、模擬システム等を用いた実践的なサイバーセキュリティ演習を行った。 ・上記 4 分野において、演習を計 5 回に分けて実施。計 128 名が参加した。
（ケ）	経済産業省	経済産業省において、制御機器のセキュリティ評価・認証の利用促進を図るとともに、制御システムのセキュリティに関する評価・認証制度の検討を行う。	・経済産業省において、CSSC を通じ、IoT システムの構成要素である制御機器の国際標準に基づく認証規格の個別システムへの適用及び新たな個別システムへの適用に向けた国際動向に関して、海外機関との情報共有を行った。

2.3. 政府機関を守るための取組

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、新たに直面した脅威・課題への対応について、統一基準群を始めとした規程に適時反映するため、統一基準群の次期改定に向けた検討を進める。	・内閣官房において、今後政府機関等が目指すべきサイバーセキュリティ対策の将来像、統一基準群の直接の適用対象となった独立行政法人等の業務形態を踏まえたサイバーセキュリティ対策、及びその他次期統一基準群に係る所要の改定内容について検討を行った。それら検討結果を踏まえ、2018 年夏頃の決定を目指し、統一基準群の改定案をまとめた。

(1) 攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進

項番	担当府省庁	サイバーセキュリティ 2017	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。	・GSOC におけるセンサー監視等により政府機関等に対する新たなサイバー攻撃の傾向等を含め、政府機関等に対し適切に注意喚起等を行った。
（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、GSOC 連絡担当者、府省庁 CSIRT 要員、CYMAT 要員等を対象としたコミュニティを形成して会合を継続的に開催し、情報セキュリティインシデント対処に関して、府省庁における課題を確認するとともに、府省庁を超えた議論や情報共有を実施した。
（ウ）	内閣官房	内閣官房において、2016 年度に改定した統一基準群に基づき、クラウドを利用する際の意識向上を図るとともに、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、情報システムの調達仕様書の策定段階において適切に定めるべきセキュリティ対策要件について検討を行い、各府省庁におけるセキュリティバイデザインの取組を促進する。また、各府省庁共通的に取り組むべき事項については、規程への反映に向けた検討を行う。	・内閣官房において、NISC が公表しているセキュリティ・バイ・デザイン関連マニュアルの各府省庁での活用状況についての調査結果の分析を行い、当該マニュアルの改定方針に係る検討を行った。また、情報システムの調達管理に関する研修に講師を派遣し、セキュリティ・バイ・デザインの取組について講演を行った。

（エ）	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、政府調達等におけるセキュリティの確保に資するため、「IT 製品の調達におけるセキュリティ要件リスト」について IPA と共同で技術の発展に応じた更新を行うために改定案を策定し、公表した（2018 年 2 月）。 ・IPA において、「IT 製品の調達におけるセキュリティ要件リスト」の効果的活用を促すためのガイドブックの改訂を行い、公表した（2018 年 2 月）。 ・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。
（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、政府調達を推進するため、調達関係者に対する勉強会やヒアリングを実施するとともに必要に応じて手順等の見直しを実施する。	・経済産業省において、IPA を通じて、統一基準（2016 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、その形態が多様なネットワークカメラについて、政府機関での調達・運用においてどのようなセキュリティ要件を確認すべきかについて「ネットワークカメラシステムにおける情報セキュリティ要件に関する調査」事業を実施し、その結果を「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」として公開した。 ・認証の主流製品である複合機に対し、申請時における技術的な提出資料の提出及び認証機関による指摘事項の DB 化等の手続きの見直しにより、認証期間の短縮（４か月）を実現した。
（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 を通じて、電子情報通信学会ハードウェアセキュリティ研究会(2017 年 7 月）、JEITA ハードウェアセキュリティ分科会(2017 年 7 月)及び日仏サイバーセキュリティセミナー（2017 年 12 月）において、JCMVP 制度の紹介を実施した。この中で、暗号製品のセキュリティに関する最新動向の紹介、制度の最新状況の解説及び利用促進の普及活動を行い、それぞれ 50 名、10 名、65 名が聴講した。
（キ）	内閣官房	内閣官房において、各府省庁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行い、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。	・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、国の行政機関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、助言等を行った。
（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、2017 年度は電子メールの送受信時におけるなりすまし対策並びに Windows OS 及び Microsoft Office の旧バージョンのサポート切れに伴う対応を、それぞれ重点検査として実施した。また、マネジメント監査により確認された課題等も踏まえ、統一基準群の改定等に反映した。
（ケ）	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とともに、将来の GSOC システムにおける監視の在り方を検討する。	・2020 年東京オリンピック・パラリンピック競技大会も念頭に置きつつ、脅威の検知能力向上等を図った第 3 期 GSOC システムの運用を開始した。 ・GSOC による監視業務の対象範囲について、独立行政法人等へ拡大し、GSOC センサー設置等の措置を講じるとともに、IPA において監視体制の運用を開始した。 ・2020 年及びその後を見据えて、政府機関等における更なるセキュリティ対策の向上に向けて、端末等での新たな監視手法の導入や脆弱性の適切な把握が可能となるような仕組み等について検討した。

(コ)	内閣官房	内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能の強化を図るため、情報システムにおけるログの取得や活用の在り方について、サイバー攻撃を受けた際の影響範囲の特定、原因究明等の観点から更なる検討を行う。	・内閣官房において、サイバー攻撃の把握・対処のためにログ管理を適切に実施するための要件について検討を行い、次期統一基準群の改定案の策定を行った。
(サ)	内閣官房	内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能が強化されるよう、CSIRT 体制の強化やインシデント対処の改善に関する各府省庁の取組状況及び課題を把握し、府省庁 CSIRT の対処能力の更なる強化のために必要な施策を検討する。	・内閣官房において、府省庁 CSIRT 要員を対象としたコミュニティを通じて、CSIRT 体制の強化やインシデント対処の改善に関する各府省庁の取組状況及び課題を把握し、インシデント対処チェックリスト及び CSIRT 要員に求めるスキルセットの共有を図った。
(シ)	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・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、独立行政法人及び指定法人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の実施を検討する。 ・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) 要員等に対する訓練等を実施する。 ・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、政府機関におけるサイバー攻撃への対処能力の向上に向け、新たなシナリオによる実践的なサイバー防御演習 (CYDER) を実施する。 ・内閣官房及び総務省において、政府機関のインシデント対処能力の向上のため、府省間の競技形式による演習 (NATIONAL 318(CYBER) EKIDEN) 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、サイバー攻撃発生時における CISO を始めとした幹部による指揮の下での迅速かつ適切なインシデントへの組織的対処及び確実な連携を目指した訓練を実施した。 ・府省庁、独立行政法人及び指定法人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、技術的事項の習得に重点を置いた研修を実施した。 ・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、自組織おいてインシデント対処訓練実施できるよう支援するためツールの説明会を実施した。 ・内閣官房において、サイバー攻撃等の発生時における対処能力の向上を図るため、インシデント発生時の対応等について、情報セキュリティ緊急支援チーム (CYMAT) 要員等に対して、技術的事項の習得に重点を置いた研修を年間を通じて実施した。また、サイバーセキュリティに関連するシンポジウム等へ参加し、CYMAT における対処能力の向上に関する情報収集に努めた。 ・2017 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 316 名受講。 ・2017 年度も府省間の競技形式による演習 (NATIONAL 318(CYBER) EKIDEN) を実施し、対処能力の向上を図った。
(ス)	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、国立情報学研究所による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。
(セ)	内閣官房	内閣官房において、政府職員のインシデント対処能力等を向上させていくため、サイバー攻撃対処能力を競う NATIONAL 318(CYBER) EKIDEN を、さらに発展させていくべく取り組む。	・NATIONAL 318(CYBER) EKIDEN について、昨今のサイバー攻撃やこれまでの実施結果を踏まえ、2017 年度は内容を高度化して実施した。
(ソ)	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。	・内閣官房において、国際的なセキュリティカンファレンスへの参加等を通じて、フォレンジック調査、マルウェア解析、最新のサイバー攻撃手法等に関する技術情報を収集し、フォレンジック調査に当たる職員の技術力の向上を図った。

（タ）	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、2016 年に改定した「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。

(2) しなやかな組織的対応能力の強化

項番	担当府省庁	サイバーセキュリティ 2017	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、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年間で全府省庁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。2017 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・システムを対象とした内容とした監査テーマで実施する。	・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、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、2016 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	内閣官房及び各府省庁において、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、「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」の推進を始めとし、体制の整備、有意な人材の確保、一定の専門性を有する人材の育成、適切な処遇の確保を含む政府内部のセキュリティ人材の充実に係る諸施策を推進する。	・内閣官房及び各府省庁において、「サイバーセキュリティ人材育成総合強化方針」に基づき、「各府省庁セキュリティ・IT 人材確保・育成計画」を策定した。 ・同計画に基づき、体制の整備、有意な人材の確保、一定の専門性を有する人材の育成、適切な処遇の確保を含む政府内部のセキュリティ人材の充実に係る諸施策を推進し、それぞれフォローアップを行って結果を確認したところ、全体に成果が見られた。
（ウ）	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。	・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 6 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。
（エ）	内閣官房	内閣官房において、引き続き、府省庁、独立行政法人及び指定法人を対象に、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、統一基準群や情報セキュリティ監査、及び府省庁マネジメント監査・ペネトレーションテストの実施結果から得られた問題の傾向と対策等をテーマとした NISC 勉強会を開催した。 ・2017 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、2018 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。
（オ）	内閣官房 総務省	内閣官房及び総務省において、各府省庁のセキュリティ・IT 人材の育成・確保のため、現行の研修体系の抜本的整理を進めるとともに、研修修了者にスキル認定を行う枠組みを構築し、研修修了者等に対するスキル認定の実施に向けて取り組む。	・現行の研修体系の抜本的整理が 2017 年内に完了した。また、2018 年 1 月 31 日に、研修修了者等に対してスキル認定を行うための全府省庁共通の基準である「橋渡し人材のスキル認定の基準」を決定した（サイバーセキュリティ対策推進専任審議官等会議・各府省情報化専任審議官等連絡会議合同会議決定）。

(3) 技術の進歩や業務遂行形態の変化への対応

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、各府省庁におけるクラウドサービス等の利用や対策の状況について調査するとともに、各府省庁と共有し、統一的な対策の必要性が把握された場合は統一基準群等への反映に向けた検討を行う。	・内閣官房において、利活用が進むクラウドサービスについて、府省庁におけるクラウド利用状況の調査を実施し、更なる施策の検討を行った。
(イ)	内閣官房	内閣官房において、IT を活用した政府機関全体としての行政事務について、関係機関と連携し、サイバーセキュリティの確保が前提となった遂行形態の実現を図る。	・内閣官房において、マイナンバー制度関連システム等に関するセキュリティ要件の助言等、必要な支援を行った。

(4) 監視対象の拡大等による総合的な対策強化

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、IPA との連携等により、引き続き、日本年金機構を含む独立行政法人・指定法人に対して監査を行う。監査の実施に当たっては、2020 年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し監査を行う計画とする。また、IPA の実施する、独立行政法人・指定法人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。	・内閣官房において、2017 年度に実施すべき法人に対し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)を実施し監査結果報告書を所管府省へ通知した。 ・IPA による独立行政法人・指定法人に係る監視業務を監督するとともに、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った。

3. 国際社会の平和・安定及び我が国の安全保障

3.1. 我が国の安全の確保

項番	担当府省庁	サイバーセキュリティ 2017	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)	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、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。

(1) 対処機関の能力強化

項番	担当府省庁	サイバーセキュリティ 2017	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。	・関係府省庁との連携を推進し、情報収集能力を強化するため、情報共有実務の見直し作業を実施。また、会議開催や資料発出を通じ、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・分析を強化するとともに、分析結果の共有を推進。 ・2017 年 12 月から 2018 年２月にかけて、各行政機関における特定秘密の保護状況について調査を実施し、各行政機関の保護規程に基づく保護措置が適確に講じられている状況を確認することができた。 ・「特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について 」（2011 年７月１日　情報保全システムに関する有識者会議）における決定事項に基づいて、情報セキュリティ対策の進捗状況の確認を実施している。
(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。	・各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図っている。 ・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（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、情報を適時・適切に関係機関に提供した。
(ウ)	警察庁	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及び当該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、大規模産業型制御システムに対するサイバー攻撃対策に係る訓練を実施する。さらに、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。 ・サイバー空間に関する観測機能の強化を図るとともに、サイバーフォースセンターの技術力向上等を通じて、サイバー攻撃対策に係る体制等を強化した。
(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)	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、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、2018 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、ネットワーク監視器材等の機能拡充の検討等を実施した。
(カ)	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開始した。
(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り組みとして、2018 年２月に CSIRT 要員及び職員に対する不審メール訓練を実施した。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）	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、次年度の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）について、体制を整備した。
（ケ）	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研究における試作を開始した。

(2) 我が国の先進技術の活用・防護

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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、調達する情報システムについて、不正なプログラムやハードウェア機器等による情報の漏洩・改竄やシステムの運用停止等の情報セキュリティ上のリスク（サプライチェーンリスク）への対策として、調達仕様書に記載すべき事項を整理した。
（イ）	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について、当該法人のマネジメント・技術面の取組を促進するとともに、これら法人相互の協力による自立的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る支援を本格化させる。 ・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。	・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強化した。 ・マネジメント面においては、適切なガバナンス体制の確立に向けた支援を行うとともに、技術面においては、国立研究開発法人の業務特性に応じた課題を検討し、統一基準に盛り込んだ。 ・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、国立研究開発法人相互の協力による自立的活動の向上に向けた取組を促進し、国立研究開発法人において、国立研究開発法人協議会が立ち上げられた。 ・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等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。 ・国立情報学研究所が、国立大学法人及び大学共同利用機関法人と連携し、SINET におけるサイバー攻撃検知システムを構築し、2017 年 7 月以降運用を開始。

(3) 政府機関・社会システムの防護

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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・実効的連携要領の確立等に向けた取組を実施する。また、任務保証の観点から、任務遂行上依拠する社会インフラへのサイバー攻撃の影響に関する知見を向上し、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実施した。

3.2. 国際社会の平和・安定

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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 のインドでの年次総会に合わせて、主に TSUBAME プロジェクト加盟組織に対してワークショップを実施し、Wannacry のパケットの特徴を使用した攻撃の推定や、IoT 機器への攻撃の状況や、マルウエアに感染した機器の挙動について情報共有を行い、問題意識を共有した。また、台湾の３つの CSIRT に対しトレーニングを行い、TSUBAME のデータを使った分析手法を共有した。TSUBAME プロジェクト加盟組織の拡大については、中東・アフリカ地域へのアプローチを継続して実施した。

(1) サイバー空間における国際的な法の支配の確立

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	内閣官房 警察庁 総務省 外務省 経済産業省、防衛省	内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、各二国間協議や国連政府専門家会合、APEC、OECD 会合等の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、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。	・バイ・マルチの枠組みで、米国その他関係国との協議を実施し、国際的なルールや規範、能力構築支援等のサイバーに関する諸課題について議論を行い、相互の理解を深めている。 ・国連政府専門家会合第５会期における議論に積極的に貢献した。また、各種国際会議やワークショップ等への参加を通じ、国際的なルールや規範作りに積極的に関与している。 ・2018 年２月には、日英共催 ASEAN 向けサイバーワークショップを実施し、サイバー空間における国際法の適用、責任ある国家の行動規範、サイバー犯罪条約、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ついて議論を行った。
(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/G8、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（2017 年４月、10 月、2018 年３月）、ICPO が主催した第３回サイバー犯罪国際専門家会合（2017 年７月）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ている。 ・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、2017 年 11 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（2018 年１月現在、74 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共助要請を実施した。 ・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 及び日・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、中央当局を設置していることから、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米国及び韓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。（再掲）
（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。	・2017 年４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、2017 年６月及び 11 月に開催されたサイバー犯罪条約締約国会合等において、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。

(2) 国際的な信頼醸成措置

項番	担当府省庁	サイバーセキュリティ 2017	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、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、国連の場を活用したルール作りに携わるとともに、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。これらの取組に当たっては、関係府省庁が共同して対外的な情報発信を強化すると共に、把握したサイバーセキュリティに関する情報を国内の関係機関と共有する。	・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諸国と二国間協議を実施し、国際的なルールや規範、能力構築支援等のサイバーに関する諸課題について議論を行い、相互の理解をさらに深めている。 ・二国間協議、ARF 等の枠組み等を通じ、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、引き続き信頼醸成に努めている。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、第１回目の専門家会合を開催し、考え方を異にする国との間でも予測可能性を向上し、信頼醸成を進めることができた。

（イ）	内閣官房	内閣官房及び関係府省庁において、各二国間協議や IWWN 等のサイバー空間に関する多国間の国際会議等に参画し、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、各国との情報共有や国際連携、信頼醸成を推進し、インシデント発生時の国外との情報連絡体制を整備する。	・IWWN、FIRST 等への国際会議や電話会議に参画し、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連携に努めた。 ・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。 ・ASEAN 加盟国とのサイバー演習に関しては、2013 年から実施している遠隔演習に加え、対面で行う机上演習も実施し、アジア地域における政策担当者レベルでの連絡体制の強化を図った。 ・有志国政府の視察団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信頼関係構築の一助とした。 ・エストニア情報セキュリティ庁（RIA）傘下の CERT-EE が主催する CERT-EE シンポジウム及び NATO CCDCOE が主催するサイバーカンフェレンス CyCon に参加し、国家政策立案者、CERT 関係者、セキュリティベンダーから最新のセキュリティ傾向や技術について習得しつつ、関係者との交流を行った。
（ウ）	経済産業省	経済産業省において、JPCERT/CC を通じて、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、今年度期限を迎えた 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「第５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」が開催され、これに参加した（2017 年９月、韓国）。 ・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。特に、FIRST の Board of Directors として FIRST と各地域の CSIRT との連携促進に注力した。 ・シンガポールが主催する ASEAN CERT Incident Drill(ACID)や、APCERT Drill に参加し、主に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、CSIRT 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公開した。

(3) サイバー空間を悪用した国際テロ組織の活動への対策

項番	担当府省庁	サイバーセキュリティ 2017	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。
（イ）	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国際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、人的情報収集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。	・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（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、情報を適時・適切に関係機関に提供した。

(4) サイバー分野における能力構築（キャパシティビルディング）への協力

項番	担当府省庁	サイバーセキュリティ 2017	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 情報セキュリティ政策会議を通じた人材育成の取組や ASEAN 加盟国と連携したサイバーセキュリティに関する国際キャンペーンの取組を通じて、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）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、APEC 電気通信・情報産業大臣会合を通じて、情報通信分野に関して APEC 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意識啓発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。 ・外務省において、警察庁等とも協力しつつ、第２回日・ASEAN サイバー犯罪対策対話や 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。	［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みを行った。 （日・ASEAN） ・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。 ・2017 年においても「サイバーセキュリティ国際キャンペーン」において国際連携・協力の推進に資する取組として、共同ポスター、意識啓発マンガを共同作成した。共同ポスターについては我が国において印刷のうえ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、2017 年 11 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） ・2017 年 10 月、警察庁と JICA の連携の下、ベトナム公安省からサイバー犯罪対策等に従事する職員を招聘し、日本の法制度、捜査手法及びサイバー犯罪対策に取り組むための民間との協力に関する知識や経験を習得させるとともに日本・ベトナム両国の関係強化を目的として、JICA 国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）を実施した。 ・2018 年１～２月、警察庁と JICA の連携の下、海外 15 か国の捜査機関等からサイバー犯罪対策等に従事する職員を招へいし、サイバー空間の脅威への対処に関する知識・技術を習得させるとともに、外国捜査機関等との協力関係を強化することを目的とした JICA 課題別研修（サイバー犯罪対処能力向上）を実施した。 ［総務省］ ・ASEAN とのサイバーセキュリティ分野での人材育成協力の強化を目指すプロジェクト「日 ASEAN サイバーセキュリティ能力構築センター（旧称：日 ASEAN サイバーセキュリティ協力ハブ）」をタイで 4 年間実施することについて、2017 年 12 月開催の第 12 回日 ASEAN 情報通信大臣会合において合意した。 ・APEC 電気通信・情報作業部会（2017 年 12 月、バンコク）のセキュリティ繁栄分科会に参加し、我が国の能力構築の取組について情報を共有した。 ・APT の加盟国を対象とした研修（2017 年 11 月、東京）を開催し、我が国のサイバーセキュリティに関する取組について情報を共有した。 ［外務省］ ・サイバー犯罪対策として、ベトナム国別研修「サイバーセキュリティ及びサイバー犯罪対処能力強化」において、ベトナム公安省職員 10 名に対して本邦研修を実施。警察庁によるサイバー犯罪にかかる講義等に加え、民間委託によるサイバー解析技術の実践を通じた人材育成を行った。 ・課題別研修「サイバー犯罪対処能力向上」（受入機関：警察庁）において、15 か国 17 人を受入。

			・インドネシアでは、2014年から2017年にインドネシア通信情報省に対して情報セキュリティ能力対策実施の能力向上を目的として、技術協力案件（情報セキュリティ能力向上プロジェクト）を実施し、ISMS（Information Security Management System）認定機関の設立や、CSIRT（Computer Security Incident Response Team）の地方行政機関での設置といった成果があった。しかし、重要情報インフラに対するサイバーセキュリティ対策はまだ十分ではなく、また、サイバーセキュリティ人材も慢性的に不足していることから、セキュリティ人材教育システムに関する支援をインドネシア政府から要請された。JICA は同技術協力案件（サイバーセキュリティ人材育成プロジェクト）の実施に向けて、2018 年１月から２月にかけて詳細計画策定調査を実施した。本プロジェクトにより、企業や政府に対してサイバーセキュリティ人材を持続的に供給し、重要情報インフラをはじめとする国家中枢へのサイバー攻撃の予防・防止に貢献することが期待される。 ・ベトナムでは、2016 年にベトナム政府から要請を受けた技術協力案件（サイバーセキュリティに関する能力向上プロジェクト）の実施に向けて、JICA は 2017 年 10 月から 11 月にかけて詳細計画策定調査を実施した。本プロジェクトにより、ベトナム政府のサイバーセキュリティに関する政策策定能力や対策が強化されることが期待される。 ・ミャンマーでは、技術協力案件（サイバーセキュリティに関する能力向上プロジェクト）の実施に向けて JICA とミャンマー政府で調整を続ける中、個別専門家「通信政策アドバイザー」（2015 年から 2017 年まで実施）がサイバーセキュリティ政策に関する助言やワークショップ等を実施した。 ・ASEAN 地域（カンボジア、ラオス、マレーシア、ミャンマー、フィリピン、タイ、ベトナム）に対して、サイバーセキュリティ対策におけるインシデントレスポンス（被害の早期発見・検知ならびに対処）能力の向上を目的として、JICA 課題別研修「サイバー攻撃防御演習」（2016 年度から 2018 年度で実施中）が 2018 年２月に実施された。また同研修は、本邦研修の活動のフォローアップ活動を、毎年２か国選定して実施することとしており、2016 年度のフォローアップ活動として、インドネシア、ミャンマー当地にて、研修員所属組織を中心に、実践的防護演習の短縮版を実施した。 ・ASEAN 地域（カンボジア、インドネシア、ミャンマー、フィリピン、タイ、ベトナム）に対して、サイバーセキュリティに関する政策能力向上を目的として、JICA 課題別研修「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」（2017 年度から 2019 年度で実施中）が 2018 年１月に実施された。 ・29 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、ASEAN 向けの、テロリストの ICT 利用対策及びサイバー犯罪対策の強化のためのプロジェクトに 50 万ドルを拠出した。

(5) 国際的な人材育成

項番	担当府省庁	サイバーセキュリティ 2017	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、国際会議への参加や留学の支援、我が国での国際会議の開催、現在国内で開催されている競技イベントを国際レベルで行うこと等を通じ、我が国の情報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。

3.3. 世界各国との協力・連携

項番	担当府省庁	サイバーセキュリティ 2017	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 1 月の日・エストニア首脳会談で、両首脳は、サイバー協議等の機会を活用し、引き続き両国の協力を進めていくことで一致した。 ・2017 年 4 月の日英首脳会談において、英国の招きに応じ、設立まもない NCSC を訪問した。また、2020 年東京オリンピック・パラリンピックに向けたサイバーセキュリティ分野における日英協力のさらなる進展、並びに連携を図って行くことで意見が一致した。 ・2017 年 8 月の日英首脳会談において、東南アジア、南アジア、及びアフリカの途上国のサイバーに関する能力構築支援の連携を推進することを含む「安全保障協力に関する日英共同宣言」を発出した。 ・2018 年 1 月の第４回日仏外務・防衛閣僚会合において、四大臣は、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するため、日仏両国が協調した対応及び情報共有を強化することを確認した。 ・2017 年 5 月にて、丸川東京オリンピック競技大会・東京パラリンピック競技大会担当大臣は、イスラエルのマタニアサイバーセキュリティ総局長官と会談。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協力について意見交換した。
(イ)	内閣官房 外務省	内閣官房及び外務省において、サイバー空間の安全及び安定を促進するため、「Ｇ７伊勢志摩サイバーグループ」を含め、Ｇ７各国との政策協調及び実務的な協力の強化に向け、Ｇ７各国と連携のうえ我が国も引き続きイニシアチブを発揮していく	・Ｇ７伊勢志摩サイバーグループに参加し、サイバー空間における国際法の適用、規範や、サイバー空間を巡る諸課題についての議論に積極的に関与した。 ・Ｇ７各国と、マルチ会議、二国間協議の場も活用し、緊密な連携を継続しつつ、各国との政策協調及び実務的な協力を強化している。

（ウ）	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、経済産業省及び関係府省庁において、これまで二国間対話等を実施してきた各国との枠組を継続するとともに、合意された連携を推進する。また、更なる連携の対象を検討し、必要があれば新たな二国間対話等の立ち上げを図り、国際協力体制を確立する。	［NISC］ ・米国との二国間対話については、「第５回日米サイバー対話」（2017 年７月）等を実施し、両国のサイバーセキュリティ政策や脅威情報の共有等に取り組み、日米協力・官民連携の推進・深化に努めた。 ・その他の国との協議については、「日印サイバー協議」（2017 年８月）、「日イスラエルサイバー協議」（2017 年 11 月）、「日豪サイバー協議」（2017 年 12 月）、「日仏外務・防衛閣僚会合」（2018 年１月）、「日 EU サイバー対話」（2018 年３月）、「日英サイバー協議」（2018 年３月）等を実施した。 ・2017 年９月、NISC が、シンガポールの CSA とサイバーセキュリティ対策で協力する覚書を交わした。 ［総務省］ ・二国間協議として「第５回日星 ICT 政策対話」（2017 年５月、シンガポール）、「第２回日独 ICT 政策対話」（2017 年９月、東京）、「第 23 回日 EU ICT 政策対話」（2017 年 10 月、東京）、「第 20 回日仏 ICT 政策対話」（2018 年３月、パリ）を開催し、各国とサイバーセキュリティ政策の共有等を実施し、関係強化及び信頼醸成に取り組んだ。
（エ）	内閣官房 外務省	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・分析に努めることができた。
（オ）	内閣官房	内閣官房及び関係府省庁において、「サイバーセキュリティ国際キャンペーン」を実施し、サイバーセキュリティに関する国際的なイベントの開催や各国と連携した意識啓発活動を行うことで、幅広い範囲での国際協力体制を確立し、サイバー空間の安全を確保していく。	・2017 年 10 月に「サイバーセキュリティ国際キャンペーン」を実施し、国際連携・協力の推進に資する取組（各省庁・関係団体等によるシンポジウム、セミナー開催等）のほか、関係省庁の協力を得て、ポスター、SNS 等の周知用素材による情報発信に努めた。
（カ）	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（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。
（キ）	経済産業省	経済産業省において、攻撃者が悪用する、グローバルに広がっている脅威や攻撃基盤等の問題に、各国の CSIRT が連携して対応・対策を実施するために必要となる、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 を通じて、サイバーグリーンインスティテュート(CGI)と連携しながら、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収集・共有し、クリーンアップ活動につなげた。また、JPCERT/CC でも複数のデータを集め、DDoS 等の要因となる要素を集計し、独自の評価指標として、インターネットリスク可視化サービス「Mejiro」として JPCERT/CC Web にて公開を行った。
（ク）	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 等の各国の情報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１月に、米国立標準技術研究所（NIST）との定期会合を NIST にて開催し、NIST、IPA がそれぞれの活動に関する情報共有を実施した。具体的には企業の CISO、セキュリティ人材育成、サイバーセキュリティフレームワーク、SP800-171 対応、IoT 普及対策、脆弱性流通自動化（SCAP)に関する意見交換を実施した。

（ケ）	経済産業省	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等を行う。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。	・経済産業省において、JPCERT/CC を通じ、2017 年度にオフショア開発で大きなシェアを占めるインドにおいてセキュアコーディングセミナーを実施し、デリー、バンガロールの二か所で 100 名を超える受講者が集まった。 ・アフリカ地域においては Africa Internet Summit 2017 に参加し、JPCERT/CC からログ分析ハンズオンと APT 対応ログ分析ハンズオントレーニングを行い、Web サーバのログファイルの読み方や高度サイバー攻撃による横断的侵害の証跡の発見で使用されることが多い、Active Directory と Proxy サーバのログから追跡を行う手法についてレクチャーし、アフリカ地域におけるサイバーセキュリティ分野への貢献を行った。アジア地域においてはセキュリティコーディングセミナーをインドの２都市で実施し、Android アプリケーションにおいて、日本での脆弱性情報の届出対応の仕組みと届け出された脆弱性のトレンドの紹介、脆弱性を作りこまないソースコードレビューのトレーニングを行った。
（コ）	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・運用面の協力に関する企画・立案機能を強化する。	・防衛省において、サイバーセキュリティに係る諸外国との技術面・運用面の協力等に関する企画・立案要員の機構・定員要求を行い、体制強化を図った。

(1) アジア大洋州

項番	担当府省庁	サイバーセキュリティ 2017	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 情報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分野における連携を強化する。また、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。さらに、ARF を中心とした地域の枠組みによる信頼醸成を進める。	[NISC] ・日本と ASEAN 加盟各国は、2009 年以降、「情報セキュリティ分野における日・ASEAN の連携枠組み」に基づき、日・ASEAN 情報セキュリティ政策会議（2018 年度からは、日・ASEAN サイバーセキュリティ政策会議に改名）を通じて、次のような連携・協力を推進している。 ・2017 年 10 月に第 10 回日・ASEAN 情報セキュリティ政策会議をシンガポールにおいて開催し、「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」（2013 年９月）における共同閣僚声明の合意事項についての取組状況の確認、情報共有体制の更なる強化について議論した。また意識啓発活動、重要インフラ防護に関するガイドラインの改定等を実施するとともに、引き続き、日・ASEAN 共同の意識啓発活動、サイバー演習、重要インフラ防護や人材育成等で連携を継続・強化していくことで合意した。個別の検討事項については WG において議論を進めた。 ・重要インフラ防護 WG では、2014 年に策定された「日・ASEAN 情報セキュリティ政策会議における重要インフラ防護に関するガイドライン」の発行とともに、このガイドラインに基づく ASEAN 各国における重要インフラ防護政策の導入・実施に向けた、今後の協力について議論を進めた。また、第 10 回日・ASEAN 情報セキュリティ政策会議に合わせ、重要インフラ防護に係るワークショップを開催し、海外政府関係者、国際機関及び我が国の専門家を講師に招き、ASEAN 各国が自国に適した政策の検討に資する取組やベストプラクティスの共有を図った。 ・サイバー演習 WG では、情報連絡体制の更なる強化に向け、各国間におけるサイバー演習手順（SOP）の改善を行うとともに、情報連絡演習及び机上演習に係る演習シナリオや各国の政策担当者の役割等について検討を重ね、5 月と 7 月に演習を行った。なお、SOP については、ASEAN 事務局のサイトに公開された。 ・人材育成 WG では、日・ASEAN における人材育成の方策について、短期研修及び、長期研修に関する検討を行った。 [総務省] ・日本及び ASEAN の ISP 間の情報共有を促進する「第 8 回日 ASEAN ISP 向け情報セキュリティワークショップ」（2018 年 2 月、東京）を総務省が主催し、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、日 ASEAN 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、2017 年 11 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）
(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、オーストラリア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（2017 年 12 月）及び日越（ベトナム）ＩＴフォーラム（2018 年 3 月）等を実施し、諸外国との連携を強化した。

(2) 北米

項番	担当府省庁	サイバーセキュリティ 2017	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、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。	[NISC] ・第５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、重要インフラ防護、ボット対策、能力構築、官民連携の強化を含む国際場裡における協力等、サイバーに関する幅広い日米協力について議論を行った。 [総務省] ・第８回インターネットエコノミーに関する日米政策協力対話（2017 年９月、ワシントン D.C.）を開催し、両国は、インターネットエコノミーの成功のためのサイバーセキュリティの重要性を確認し、人材育成等、サイバーセキュリティ対策のための両国の能力を強化するための特定の国家のイニシアティブに関する情報を共有した。 [外務省] ・第５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、両国における取組み、国際場裡における協力、能力構築支援等、サイバーに関する幅広い日米協力について議論を行い、共同プレスリリースを発出した。
(イ)	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。	・内閣官房において、2017 年 9 月の第８回日米インターネットエコノミー政策協力対話において、サイバーセキュリティを含む幅広い課題について議論を行い、今後の協力の強化について確認した。 ・総務省において、第 2 回 ISAC 間連携国際ワークショップ（東京）を 2017 年 11 月に開催し、日本の ICT-ISAC、米国の Comm-ISAC、IT-ISAC 及び Auto-ISAC 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。
(ウ)	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、新ガイドライン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、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。

(3) 欧州

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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、二国間協議の枠組みを通じ、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。	・防衛省において、NATO CCDCOE への参加承認を取得する等、欧州各国との連携強化に努めた。
(イ)	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、JTEMS、JEDS と定期的に協議を行う。	・経済産業省において、IPA を通じて、JIWG プレナリ会合に 1 回参加し、2017 年度の活動報告と 2018 年度の活動計画を協議した。また、JHAS 会合に 3 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。

(4) 中南米、中東アフリカ

項番	担当府省庁	サイバーセキュリティ 2017	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、国際的な会議の場等を活用し、二国間協議を実施していない国との関係も強化する。	・国連政府専門家会合や ARF をはじめとする国際的な会議の場等を活用し、各国との対話を継続している。

4. 横断的施策

4.1. 研究開発の推進

項番	担当府省庁	サイバーセキュリティ 2017	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た「サイバーセキュリティ研究開発戦略」を策定する。	・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た「サイバーセキュリティ研究開発戦略」を決定した（サイバーセキュリティ戦略本部第 14 回会合決定）。
(イ)	総務省	総務省において、NICT を通じ、情報通信ネットワークの安全性を確保する上で、さまざまなシステムで利用されている暗号方式・プロトコル等の安全性評価を行い、システムの安全性維持に向けた研究開発を実施する。	・総務省において、NICT を通じ、暗号技術の安全性に係る監視及び評価を行い、安全性の低下が認められた暗号技術について、 CRYPTREC 統一 WEB サイト上で注意喚起及び適切な運用方法の周知を実施した。

(1) サイバー攻撃の検知・防御能力の向上

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	総務省	総務省において、NICT を通じ、政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術の研究開発を行う。また、サイバーセキュリティ関連情報の大規模集約を行うとともに、セキュリティ検証プラットフォームを構築し、サイバーセキュリティ研究の基盤となる環境整備を行う。	・総務省において、NICT を通じ、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継続的に実施した。また、IoT 機器からの応答データを自動分類して IoT 機器の判定を機械学習により行う手法を開発し有効性を実証した。
(イ)	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、CSSC を通じて、制御システムにおけるサイバー攻撃を検知・予測する技術や、ダウンタイムを大幅に削減するための、高可用性技術に関する調査・研究を行った。
(ウ)	総務省	総務省において、NICT を通じ、サイバーセキュリティの研究開発を促進するため、攻撃トラフィック、マルウェア検体等のデータセットについて、大学等の外部の研究機関の安全な利用を可能にする研究基盤（NONSTOP）を運用する。	・総務省において、NICT を通じ、サイバーセキュリティ・ユニバーサル・リポジトリ「CURE（Cybersecurity Universal Repository）」の実現に向けて、各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等の集約をさらに進めるとともに、CURE の WEB の API と WebUI を整備し異種 DB の統合を実施した。 ・また、複数情報源の紐づけ等を通じて攻撃キャンペーンの解明を行い、攻撃発生時における対応策を、セキュリティ関連組織やユーザに対して自動的に展開できるようにするための自動対策技術の基礎検討を実施した。
(エ)	文部科学省	文部科学省において、NII を通じ、サイバー攻撃耐性を向上させるため、大学等の関係機関において、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。	・国立大学法人及び大学共同利用機関法人において、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ために、M2M を含めたサイバー攻撃に関する通信データ等を収集し、共有するための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を行い、H30 年度に試験的に公開するための通信データ処理プログラム、および、公開用ポータルサイトのシステム開発を実施。

(2) サイバーセキュリティと他分野の融合領域の研究

項番	担当府省庁	サイバーセキュリティ 2017	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た「サイバーセキュリティ研究開発戦略」を策定する。	・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た「サイバーセキュリティ研究開発戦略」を決定した（サイバーセキュリティ戦略本部第 14 回会合決定）。
(イ)	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。	・経済産業省において、NEDO を通じて、「IoT 推進のための横断的な技術開発事業」の公募を 2016 年度、2017 年度に実施。データの収集、蓄積、解析、セキュリティの 4 つの技術領域において、16 件の研究開発テーマを実施するとともに、2030 年の IoT 社会の共通基盤技術となりうる先進的かつ分野横断的な技術の開発を産学官の連携体制で実施。
(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。	・理化学研究所革新的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、人工知能に必要なセキュリティ・プライバシーの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推進した。

(3) サイバーセキュリティのコア技術の保持

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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。	・量子鍵配送ネットワークの信頼性試験を継続。またネットワークシステム全体及び装置の各コンポーネントの安全性向上に取り組み、送信機内の信号変調器の不完全性による安全性劣化の可能性を明らかにすると共に、その対策方法の開発に成功した。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に、分散データの秘匿性更新技術を実装した。光空間通信テストベッドにおいて、物理レイヤ秘密鍵共有システムを実装し、見通し通信路における情報理論的安全な鍵生成の原理実証実験に成功した。
(イ)	総務省 経済産業省	総務省及び経済産業省において、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、暗号プロトコル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、セキュリティ産業の競争力強化に係る検討、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、暗号技術検討会を開催し、暗号技術の安全性に係る監視及び評価を踏まえた CRYPTREC 暗号リストの改定と、CRYPTREC 成果文書の参照性向上のための文書番号の整理を実施した。また、NICT 及び IPA を通じ、暗号技術評価委員会及び暗号技術活用委員会を開催し、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等を引き続き実施した。
(ウ)	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 を通じて、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、量子コンピュータに対する耐性を持つと注目されている格子暗号の安全性の根拠となる格子問題を解読する大規模並列計算機向け格子問題求解アルゴリズムの高速性について、理論的な裏付けに初めて成功した。

(4) 国際連携による研究開発の強化

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	総務省	総務省において、情報セキュリティ分野の国際標準化活動である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、国際規格への反映が行われるよう積極的に参画する。	・総務省において、ITU-T SG17会合（2017年9月、2018年3月）に我が国から寄与文書を入力するなど、国際標準化の議論に参加・貢献した。

(5) 関係機関との連携

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	内閣府	内閣府において、戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」により真贋判定技術（機器やソフトウェアの真正性・完全性を確認する技術）を含めた動作監視・解析技術と防御技術の研究開発を行う。	・大規模システムの真贋判定技術に関して、実システムで評価するための運用機能の開発を完了、基本機能を完成した。 ・IoT向けの暗号実装技術として「セキュア暗号ユニット（SCU）」を試作し、低電力、小面積・低コスト、超高速動作の単体性能目標を達成した。

4.2. 人材の育成・確保

項番	担当府省庁	サイバーセキュリティ 2017	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」に基づき、施策間連携を図りつつ、関係施策を促進していく。	・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」（2017年4月18日）を踏まえ、「サイバーセキュリティ人材の育成に関する施策間連携WG」において、①各層別の人材像やキャリアパスの明確化、②ITの基本的知識と各層別のカリキュラムの方向性、③各省の人材育成施策に関する全体像整理と連携策の検討、④教材のR&D、⑤産学官連携の在り方・具体的方策について検討を実施し、報告書としてとりまとめた。（再掲） ・並行して、内閣官房にて各層別の人材像、モデルとなるカリキュラムの方向性について調査を行い、「サイバーセキュリティ人材の育成に関する施策間連携WG」にて報告を行った。（再掲）

(1) 高等教育段階や職業能力開発における社会ニーズに合った人材の育成

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
(ア)	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演習を推進する体制の構築や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。

（イ）	内閣官房	内閣官房において、産業界や大学、関係省庁等、産学官の連携体制の下、情報共有を行いつつ、モデルとなるカリキュラムの策定をはじめとした施策間連携を推進する。	・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」（平成29年4月18日）を踏まえ、「サイバーセキュリティ人材の育成に関する施策間連携WG」において、①各層別の人材像やキャリアパスの明確化、②IT の基本的知識と各層別のカリキュラムの方向性、③各省の人材育成施策に関する全体像整理と連携策の検討、④教材の R&D、⑤産学官連携の在り方・具体的方策について検討を実施し、報告書としてとりまとめた。（再掲） ・並行して、内閣官房にて各層別の人材像、モデルとなるカリキュラムの方向性について調査を行い、「サイバーセキュリティ人材の育成に関する施策間連携WG」にて報告を行った。（再掲）
（ウ）	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。	・「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。
（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、情報セキュリティ教育の演習拠点を整備（2016年：５拠点、2017年：５拠点（予定）、合計10拠点整備予定）設置し、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。	・2017 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は、引き続き教育実践・検証を進めるとともに、先行５拠点（一関、木更津、石川、高知、佐世保）に加えて、後発５拠点（旭川、小山、岐阜、松江、熊本）にサイバーレンジ（実践的な演習環境）を設置。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）	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。
（カ）	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。（24コース・受講者数447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３月末時点の情報関係の指定講座数363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３月末時点の指定講座数12講座）

(2) 初等中等教育段階における教育の充実

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	文部科学省	文部科学省において、次期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。	・「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。

（イ）	文部科学省	″文部科学省において、教員研修センターと連携し、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。	・教職員支援機構と連携し、2018年1月29日～2月2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。教員等を対象とした情報モラル教育指導者セミナー・フォーラムについて、2018年2月までに実施済。

(3) 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

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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「セキュリティ・キャンプ実施協議会」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、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、2017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。82名が受講した。 ・また、2017年6月から2018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10箇所で実施した。
（イ）	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用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 CTF 2017」）について経済産業省において普及・広報の支援を行う。	・NPO日本ネットワークセキュリティ協会が主催する「SECCON2017」において、経済産業省として後援するとともに、2018年2月17日～19日に実施された「SECCON2017 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。
（ウ）	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、IPAを通じ、「未踏IT人材発掘・育成事業」は20テーマ28名のクリエータを採用し、着実に事業を実施した。また、2016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。

(4) 人材が将来にわたって活躍し続けるための環境整備

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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、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、IPAを通じて広報活動を実施した。
（イ）	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、普及を図るべくIPAを通じて広報活動を実施した。
（ウ）	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、IPAを通じ、新たなスキル標準を策定する一環として、主に従来ITSSが対象としている既存のIT人材が「セキュリティ領域」や「データサイエンス領域」のスキル強化を図るための”学び直し”をするための指針として”ITSS＋（プラス）”を2017年4月7日に公開した。また、新たな開発手法や、新技術に対応できるIT人材に焦点を当てた新たなスキル標準を引き続き検討する。
（エ）	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。	・2017年4月及び10月の登録により、6,994名の情報処理安全確保支援士（登録セキスペ）が誕生した。また、2018年4月15日に実施予定の情報処理安全確保支援士試験には、23,180名の応募があった。登録セキスペの更なる活用のため、IPAのHPで登録状況を公表するとともに、支援士制度の普及のため、企業や団体への周知等を行った。

（オ）	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、未来のサイバーセキュリティ研究者・起業家の育成に取り組む。	・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」を実施し、1 年間を通じて高度なセキュリティ技術を本格的に指導。2017 年度は、39 名がプログラムを修了した。

(5) 組織力を高めるための人材育成

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	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り組みとして、2018 年 2 月に CSIRT 要員及び職員に対する不審メール訓練を実施した。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。
（イ）	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、独立行政法人、重要インフラ事業者及び地方公共団体等におけるサイバー攻撃への対処能力の向上に向け、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、2017 年度、全国 47 都道府県で 100 回の演習を実施し、計 3009 名が受講。
（ウ）	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開始した。
（エ）	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・実効的連携要領の確立等に向けた取組を実施する。また、任務保証の観点から、任務遂行上依拠する社会インフラへのサイバー攻撃の影響に関する知見を向上し、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実施した。

5. 推進体制

項番	担当府省庁	サイバーセキュリティ 2017	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、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進化を図るため、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。中期的には、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、NISC 内に専従の CSIRT 組織を整備する。また、サイバーセキュリティに関し、司令塔機能を果たすため、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情報及びサイバー攻撃に関わる情報の共有を推進した。 ・JPCERT/CC 及び NICT を含む、日本の情報セキュリティ関係組織等で検知した攻撃予見情報・観測/分析結果情報を、韓国 POC（Point of Contact）に提供。また、大会期間中に職員２名を派遣し、韓国のサイバーセキュリティ対策・サイバー脅威情勢について情報収集を実施。 ・総合的分析機能の強化を図り、司令塔機能の強化に資するよう努めた。 ・NISC と NICT との包括協定に基づき、NICT は、NICTER で観測したサイバー攻撃に関する情報等を NISC に情報共有しているところ。
（イ）	警察庁	警察庁において、「セキュリティ情報センターについて」（2015 年８月３日セキュリティ幹事会決定）等に基づき、セキュリティ情報センターを設置する。同センターにおいては、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。	・警察庁にセキュリティ情報センターを設置し、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。

（ウ）	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のため、運営に大きな影響を及ぼし得る重要サービス事業者等におけるサイバーセキュリティに係るリスク評価について、大会の詳細や情勢の変化に応じた手順書の見直しを実施するとともに、地方における会場等を勘案し、対象となる事業者の地理的、分野的な拡大を図る。更に、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していく。また、これら重要サービス事業者等に対するサイバー攻撃への対応に係る関係主体との情報共有の中核的役割を果たすサイバーセキュリティ対処調整センター（オリンピック・パラリンピックCSIRT）の2018年度中の構築に向け、情報共有システムの構築を推進するとともに、2018年２月から３月にかけて開催される平昌冬期オリンピック・パラリンピック競技大会等の機会をとらえ関係組織間のさらなる連携の深化を図る。	・サイバーセキュリティ体制に関する検討会において、2016年度までに検討し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）の設置時期や機能・役割についてセキュリティ幹事会において決定するとともに、脅威情報や、発生が想定されるインシデントの種類・規模に応じた対処の具体的な内容について重点的に検討した。2018年度末の構築に向け、仕様の細部について検討を実施すると共に、情報共有・対処体制に関する基本的な方針を関係府省庁、大会組織委員会、東京都等と協議の上、改正した。 ・関係する所管省庁及び地方公共団体の協力を得て、リスクアセスメントを促進した。2016年度に作成したリスク評価手順書を第１回目（2016年度、対象：東京23区）のリスク評価の教訓及びロンドン大会のサイバーセキュリティ責任者の支援を得て改訂し、７～10月の間に第２回目のリスク評価を東京、千葉、埼玉、神奈川に対象を拡大して実施した。また、重要サービス事業者等における大会に係るリスクを確認しその対策を進めるため、大会の安全・円滑な準備及び運営並びに継続性の確保の観点から、特に影響が重大なサービスを分野を横断して抽出し、当該サービスに係るサイバーセキュリティ上のリスクについて、重要サービス事業者等における対策の状況等を把握する、横断的リスク評価を開始した。2017年度は重要サービスの継続性確保SGと連携し、大会組織委員会、所管省庁、関係事業者等から横断的リスク評価に必要な情報収集を実施した。
（エ）	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。	・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の在り方を改善するため、GSOCと関係組織間でインシデント発生時の連絡体制等について適宜調整した。

（本ページは白紙です。）

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取組等

＜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 117
別添３－２　サイバーセキュリティ基本法に基づく監査 121
別添３－３　重点検査 127
別添３－４　高度サイバー攻撃への対処 129
別添３－５　教育・訓練に係る取組 131
別添３－６　なりすまし防止策の実施状況 138
別添３－７　暗号移行 140
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 142
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 153
別添３－10　政府機関等に係る 2017 年度の情報セキュリティインシデント一覧 . 158
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 161

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や、より高い水準のセキュリティを確保するための対策事項を定めている。統一基準群の運用により、個々の機関のサイバーセキュリティ対策が強化され、それに伴い政府機関等全体のセキュリティ対策水準も底上げされている（図表１）。

図表１　統一基準群の効果（イメージ）

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、2017年度時点では、2016年８月31日のサイバーセキュリティ戦略本部決定により改定された統一基準群（平成28年度版）が運用されている。

統一基準群（平成28年度版）の文書構成は、図表２のとおりである。

図表２　統一基準群の文書構成

府省庁は、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、「府省庁対策基準策定のためのガイドライン（以下「ガイドライン」という。）」を参照した上で、「政府機関の情報セキュリティ対策のための統一規範（以下「統一規範」という。）」及びその細則である「政府機関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。）」に準拠した情報セキュリティポリシーをそれぞれ策定し、当該ポリシーに基づく情報セキュリティ対策を適切に講じることとされている。また、独立行政法人及び指定法人（以下「独立行政法人等」という。）は、「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（以下「運用指針」という。）」に基づき、統一基準群及び所管府省庁の情報セキュリティポリシーを参照の上、組織及び取り扱う情報の特性等を踏まえた情報セキュリティポリシーを策定することとされている（図表３）。

図表３　統一基準群と政府機関等の情報セキュリティポリシーの関係

政府機関等の情報セキュリティ対策は、運用指針において、①政府機関等の個々の組織のPDCA、②政府機関等全体としてのPDCAの２つのマネジメントサイクルにより、継続的に強化することとされている（図表４）。

図表４　政府機関等における情報セキュリティのマネジメントサイクル

２　統一基準群の改定に係る検討

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、統一基準群の改定に向けた検討を行い、2017度末に改定の素案を策定した。今般の改定において、今後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を見据え、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について規定し、対策の強化を図ることとしている。

その他、主な改定は、図表５に示すとおりである。

図表５　統一基準群の主な改定内容

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の見直しについて

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境界監視に加えプログラムが動作する内部（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データ保護により事案が発生した際にも被害を無効化す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、第1段階として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た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”を講じる時期。全ウェブサイト及び電子メール通信の暗号化対応の義務化。

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統一基準群にフィードバック。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。

※ PDCA:[Plan（計画）、Do（実行）、Check（評価）、Act（改善）]

4. 多様な業務形態への対応

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導入。どのような業務形態であっても、安全かつ円滑に情報システムを利用できるよう、安全対策等を整備。

別添３－２　サイバーセキュリティ基本法に基づく監査

１　2017 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、2017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。

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

2017 年４月から 2018 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、11 の府省庁を対象とした。

（３）マネジメント監査の実施内容

「政府機関等の情報セキュリティ対策のための統一基準群」等に基づく施策の取組状況について、各府省庁における組織・体制の整備状況、サイバーセキュリティ対策の実施状況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかとの観点を中心に監査を実施した。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、2016 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 2016 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

- 行政事務従事者の自己点検結果を分析するに当たり、情報セキュリティ責任者による部局単位の分析の前に、各課室単位での早期改善が図れるよう課室を所管する情報セキュリティ担当者単位で分析・改善を実施していた事例
- 対策推進計画に係る詳細計画について、ある項目の実施時期の見直しによる計画全体への影響を把握し、情報セキュリティに係る各取組による効果を高めるため、当該計画における情報セキュリティ監査や教育等の各取組内容の関連性を可視化した事例
- セキュリティ強化月間において、自己点検の結果を踏まえ、要保護情報の適切な管理策としてクリアデスクを推進し、統括情報セキュリティ責任者が現場を視察していたほか、最高情報セキュリティ責任者からの各種指示について、毎週の幹部会議において周知するなど、リーダーシップを発揮し、組織全体の情報セキュリティ対策を推進するための取組が図られていた事例
- 情報セキュリティに係る集合教育、各所属セキュリティ事務担当者への教育、システム管理担当者への教育等、多種の教育を実施しているほか、セキュリティニュースとして、昨今の情報セキュリティに係る動向や、直近の内部監査結果等を踏まえた留意事項及び良い取組事例等を配付し、職員の情報セキュリティに係る意識を高める取組を実施していた事例

② 主な助言等

2017 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 2016 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

2016 年度に監査を実施した 12 府省庁に対して、2017 年度に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。その結果、監査における全ての助言に対して、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、改善策が実施済となっていた。

これまでの監査で得られた知見を、統一基準群の改定作業に反映した。具体的には、情報セキュリティ対策の運用について、責任者への報告を通じ、自らの課題の認識と、これに対する対応方針の検討を誘発し、PDCA サイクルをより効果的に機能させるなどの規定を盛り込んだ。

2017 年度の監査においては、監査対象とした政府機関全体として、2015 年度から開始した監査で把握した状況と比較して、情報セキュリティ対策の水準の底上げが図られていることを確認できた。また、サイバーセキュリティ推進部局が直接に対策を講じる部分については着実に取り組まれている一方、当該部局以外の部局が対策を講じる部分については、その対策水準の向上が求められる場合も見られた。府省庁は、継続的にサイバー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 サイクルを適切に構築・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

2017 年４月から 2018 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、主体認証情報（ID・パスワード等）について、パスワード解析に十分な耐性を有するものとなっていないなどの不備であった。調査中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

2017 年４月から 2018 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、33 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

- 組織全体として情報セキュリティ活動としての取り組みが行われていた事例
  - ➢ 情報セキュリティリスクを確実にとらえて適切な対応をとることを目的として、リスク委員会及び情報セキュリティ分科会を設け、組織全体のリスクマネジメントの活動の中で、情報セキュリティリスクを低減させる取り組みを行っていた事例
  - ➢ 部等の各代表者で構成される情報システム委員会を設け、情報セキュリティポリシーの改訂内容や守るべき情報資産と情報セキュリティ対策、リスク等

に関して議論した後、情報セキュリティ委員会で審議していた事例

・ 情報セキュリティインシデントに対処するための体制（CSIRT）が中心となり、インシデントの事例を法人内に共有、対処訓練を実施するなど、法人全体のインシデント対処能力向上に努めた事例
・ 各所に散らばっている拠点、部署に対して、計画的に内部監査が実施されていたうえ、チェックリストの整備、フォローアップなど細部に配慮の行き届いた情報セキュリティ監査（内部監査）を実施していた事例
・ トップマネジメント（理事長、CISO）の判断により、情報セキュリティ対策にかかる予算的、人的な資源の投入が迅速に行われていた事例
・ 運用保守作業の委託先との連絡を密にし、委託先の判断のみに頼ることなく、申請された保守作業結果について日次、月次または四半期の報告により担当部署が確認していた事例

② 主な助言等

監査においては、以下に示す主な監査項目について、法人におけるサイバーセキュリティ対策に関連する規程の整備状況及びその運用状況に係る監査を実施し、情報システムにおける技術的な対策を含めて、改善のために必要な助言等を行った。

【主な監査項目】

・ 情報セキュリティ対策の基本的枠組みに係る規程の整備及び運用状況
・ 情報の取扱いに係る規程の整備及び運用状況
・ 外部委託に係る規程の整備及び運用状況
・ 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

2017 年度は、33 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の取組は府省庁に比較し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。今後、各法人において、助言等を踏まえつつ、引き続き、取組を促進する必要がある。

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

2017 年４月から 2018 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、33 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 34 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、主体認証情報（ID・パスワード等）について、パスワード解析に十分な耐性を有するものとなっていないなどの不備であった。調査中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
電子メールのなりすまし対策	電子メールの受信側における送信ドメイン認証技術の導入状況	政府機関等に対する標的型攻撃の脅威等を踏まえ、電子メールの送信ドメインのなりすまし防止に係る対策等の実施状況を把握するため。
	電子メールの送信側における送信ドメイン認証技術の導入状況	
技術的な情報セキュリティ対策	Windows Vista	サポート切れの OS 及びソフトウェアについて、各政府機関において適切に対応しているかどうかを確認するため。
	MS Office 2007	

（１）電子メールのなりすまし対策について

電子メールのなりすまし対策の一つに、送信ドメイン認証技術があり、SPF (Sender Policy Framework)、DKIM(Domainkeys Identified Mail)が挙げられる。これらは、送信する電子メールのドメインを管理するDNSサーバに登録・公開された送信側メールサーバの情報や電子署名で使用する公開鍵を利用することで実現するものである。また、これらの送信ドメイン認証技術を補強する仕組みとしてDMARC(Domain-based Message Authentication, Reporting & Conformance)がある。送信ドメイン認証技術による電子メールのなりすましを防止するには、送信したメールの正当性を受信側が確認できるような送信側の対策と、受信した電子メールの正当性を判定して、なりすまされた電子メールから受信者を保護するための受信側の対策があり、両方の実施が求められるところである。

政府機関に対する標的型攻撃の脅威等を踏まえ、2017年度も引き続き電子メールのなりすまし対策状況について検査を実施した。

電子メールのなりすまし対策の実施状況を確認したところ、電子メールの受信側の情報システムと送信側の情報システムで、共に約９割が対策を実施していることを確認できた。対策のうち、送信ドメイン認証技術を用いた対策は年々強化されており、受信側の対策では約７割、送信側の対策では約９割の情報システムにおいてSPFを利用している。更に、DKIMやDMARCを併せた複合的な対策も進んでいる。なお、別の方法により調査した政府機関のドメイン名における送信側のSPFの設定状況は別添３－６に掲載している。

政府機関において、標的型攻撃の脅威等によるリスクを低減するためにも、各府省庁で利用者の数が多いメールドメインを優先的に、かつサーバの更新時期に合わせるなどして、送信ドメイン認証技術等の対策を着実に導入し、なりすまし対策を推進することが重要である。

また、既に実施している対策についても、適宜、設定等の見直しや対策の強化を検討し、継続的に対策を推進することが重要である。

（２）サポート切れＯＳ・ソフトウェアについて

Windows Vista延長サポート終了（2017年４月11日（米国時間））及びMicrosoft Office 2007延長サポート終了（2017年10月10日（米国時間））に伴うセキュリティ対応状況については、検査時点において対応を検討中の府省庁が存在することを把握したが、それらはその後の追跡調査において、最新のOSやソフトウェアに更新される、若しくは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」という。）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。

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。

2017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、2016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増えているが、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た。具体的には、政府機関全体で、ガイドラインに基づき保護対象に選定されたおよそ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。

2017年度が運用の初年度となる独立行政法人等においては、ガイドラインに基づく業務や情報に関するリスク評価等のプロセスを通じて、計画的・重点的な対策導入を行う対象を選定した結果、およそ230の業務領域に使用されているおよそ220の情報システムが特定された。また、システムごとに対策実施状況の現状点検を実施した上で、「多重防御」の観点から対策強化の要否を検討した結果、各独立行政法人等のCISOによる方針決定の下で、およそ５割の対象システムにおいて更なる対策強化を図るための複数年にわたる計画が策定された。

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、各府省庁における情報セキュリティ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要員の情報セキュリティ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180人（全22府省庁参加）

（４）訓練時期

2018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となった。

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、情報セキュリティ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情報セキュリティ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、2018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

情報セキュリティ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・情報セキュリティ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	2017 年 ５月～ 11 月	【CSIRT 会合】 ・府省庁 CSIRT におけるインシデント対処に関する課題整理 ・セキュリティ情報分析 勘ドコロ 2017 ・府省庁 CSIRT 要員に求められるスキルセット案について ・最新の攻撃事例と対策のあり方 ・平時の CSIRT 業務、CSIRT 要員の役割について、必要性分析　ほか	NISC 職員 外部講師	延べ約 100 名 （３回開催）
2	2017 年 ７月～ 2018 年 ３月	【CSIRT 研修】 ・攻撃手法 ・デジタル・フォレンジック ・インシデント・レスポンス　ほか	外部講師	延べ約 190 名 （７回開催）
3	2017 年 ９月～ 10 月	【CSIRT 向け講習会】 インシデント対処に必要な基礎知識 ・サイバー攻撃の動向と脅威 ・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 50 名 （３回開催）
4	2017 年 10 月～ 11 月	【CSIRT 向け実機演習】 インシデント対処に関する技術的知識 ・標的型攻撃に関する解説 ・標的型攻撃の脅威の検出方法 ・標的型攻撃における簡易ログ分析 ・フォレンジックに関する解説　ほか	外部講師	延べ約 50 名 （３回開催）

３　独立行政法人等 CSIRT 要員に対する研修

（１）目的

情報セキュリティ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・情報セキュリティ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	2017 年 ７月～ 2018 年 ３月	【CSIRT 研修】 ・攻撃手法 ・デジタル・フォレンジック ・インシデント・レスポンス　ほか	外部講師	延べ約 990 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	2017 年 ７月	政府機関等の情報セキュリティ対策のための統一基準群について	NISC 職員	延べ 330 名 （２回開催）

2	2017 年 10 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 250 名 （２回開催）
3	2018 年 ３月	府省庁マネジメント監査・ペネトレーションテスト実施結果から得られた問題点の傾向と対策	NISC 職員	延べ 270 名 （２回開催）

図表３　NISC勉強会におけるワークショップの様子

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

2017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５回実施した。

サイバーセキュリティ机上演習においては、４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疑似体験を通じた少人数制のディスカッションを行った。

No.	時期	テーマ
1	2017 年 ４月	【座学①】 ・　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）について ・　重要インフラ防護とオリパラに向けた取組
2	2017 年 ８月	【座学（演習）②】 インシデント・ハンドリング
3	2017 年 ９月	【座学③】 １．サイバーセキュリティ戦略の概要と取組 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
4	2017 年 12 月	【座学（演習）④】 サイバーセキュリティ机上演習
5	2018 年 １月	【座学⑤】 １．ISO/IEC27001 と情報セキュリティマネジメントシステムについて ２．次期サイバーセキュリティ戦略の検討等について

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

①情報セキュリティに関するｅラーニング

IPA（独立行政法人情報処理推進機構）が実施している国家試験「セキュリティマネジメント試験」、または同機構が定義している ITSS（IT スキル標準）レベル２に相当する程

度のセキュリティに関する知識の習得等を目的としたｅラーニング[1]を実施。

実施時期：2017 年５月～８月及び９月～11 月

＜カリキュラム概要＞

①情報セキュリティ基礎知識
②情報セキュリティマネジメントのフレームワーク
③情報セキュリティを支える暗号技術の基礎と応用
④情報セキュリティのリスクマネジメントとリスクコントロール
⑤ネットワークを守る認証技術とシステム技術
⑥情報セキュリティに関わる法律の基礎知識
⑦企業の情報ネットワークシステムのセキュリティ/ソフトウェアのセキュリティ課題と対策
⑧Web・データベース・クラウドのセキュリティと CSIRT

②「CISSP」入門講座

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

実施時期：2017 年８月～2017 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)
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)	

[1] 株式会社ドコモ gacco が提供する「情報セキュリティ初級」講座。

[2]学校法人東京電機大学が開講している「国際化サイバーセキュリティ学特別コース」(CySec) における「サイバーセキュリティ基盤」科目を「CISSP 入門講座」として実施。

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、政府機関全体として取組を推進しており、「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推進している。

図表１　SPFを活用したなりすまし対策の概要

図表１に、政府機関において取り組んでいるSPFを活用したなりすまし対策の概要を示す。SPFを利用する場合、電子メールの送信側であらかじめ電子メールを送信する可能性のある電子メールサーバのIPアドレスをSPFレコード[3]に設定して公開する。受信側では、電子メールの受信時に、SPFレコードに公開されたIPアドレスと実際に送信元となっている電子メールサーバのIPアドレスが一致するかどうかを確認する。このような手順により、受信者が受け取った電子メールについて、送信者情報が詐称されているかどうかの確認が可能となる。

[3] SPF において、そのドメイン名が使用する送信メールサーバの IP アドレス等の情報が記載され、DNS サーバに設定してインターネット上に公開されるもの。

２　取組の結果及び今後の課題

2017年及び2018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
2017 年１月末	71.4%	15.3%	13.3%
2018 年１月末	74.5%	11.7%	13.8%

※１　設定された以外のIPアドレスは当該ドメイン名の電子メールを送信する電子メールサーバとして認証しない。

※２　認証情報を公開しているが、正当な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、「-all」の設定に改善が見られるものの、SPFの設定の有無という点では、１年前と比較してほとんど横ばいであることがわかった。SPFの設定がなされていないドメイン名について分析したところ、約７割が、電子メールに関係する設定が記載されていないドメイン名[4]であることが判明した。このようなドメイン名では、外部との電子メールの送受信を目的としていないことが考えられる。電子メールを利用していないドメイン名についても、その情報を、当該ドメイン名を管理するDNSサーバのSPFレコードに設定することで、当該ドメイン名になりすました電子メールについて受信者が正当性を確認できるようになる。別添３－３に記載したとおり、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。

また、政府機関においては、電子メールを送信する電子メールサーバのIPアドレスを明確に宣言するため、SPFレコードの末尾に「-all」を設定するよう推進している。この設定が「~all」となっているドメイン名は減少しており、「-all」が増えている状況にあることから、今後も継続して「-all」を設定するよう取り組んでいく。

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)やDAMRCといったSPF以外の送信ドメイン認証技術の導入についても、技術動向等を踏まえて必要な取組を推進する。

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

別添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」[5]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

[5] http://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。現在報告されている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、今後数年の間に危殆化する可能性があることが指摘されている。

図は、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おり、今後も同様の傾向が予想される。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（2018 年２月更新）[6, 7]

[6] スーパーコンピュータの性能の伸びに関する外挿線は僅かではあるが鈍化してきている。

[7] http://www.cryptrec.go.jp/report/cryptrec-rp-2000-2017.pdf ［PDF］
「CRYPTREC Report 2017(暗号技術評価委員会報告)」(CRYPTREC、2018 年６月)

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[8]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（2018年３月末日現在）

（２）調査時点

独立行政法人及び指定法人　2017年12月末日

国立大学法人等　2018年３月末日

[8] 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[2]

- 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、８法人（89%）である。

- 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。

[9] 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[3]

・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、2016年度の81法人（92%）から84法人（97%）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。

[10] 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、2016年度の66法人（75%）から79法人（91%）に増加している。

・指定法人

CSIRTを設置している法人は、2016年度の５法人（56%）から７法人（78%）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81法人（90%）から88法人（98%）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[11]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。

[11] 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、75法人（84%）である。また、eラーニングを実施している法人は、46法人（53%）、標的型メール攻撃等の模擬訓練を実施している法人は、65法人（75%）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、５法人（56%）、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、80法人（89%）である。また、eラーニングを実施している法人は、70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、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、2016年度の68法人（77%）から77法人（89%）に増加している。

・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、2016年度の79法人（88%）から82法人（91%）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、74法人（85%）である。

・ 指定法人

情報セキュリティ監査を実施している法人は、５法人（56%）である。

・ 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、2016年度の82法人（91%）から87法人（97%）に増加している。

（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、81法人（93%）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、８法人である。

- 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　「府省庁が提供しているソフトウェアの脆弱性に関する情報提供及び脆弱性を含むソフトウェアに関する対策実施の必要性について（注意喚起）」（2017 年６月２日発出）

事　務　連　絡
平成 29 年６月２日

各府省庁情報セキュリティ担当課室長 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（政府機関総合対策担当）

府省庁が提供しているソフトウェアの脆弱性に関する情報提供及び脆弱性を含むソフトウェアに関する対策実施の必要性について（注意喚起）

統一基準群においては、ソフトウェアに関する脆弱性対策として、

・利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること
・アプリケーション・コンテンツの作成時の対策として、府省庁外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること
・セキュリティ要件の策定の際、提供するアプリケーションが脆弱性を含まないこと等を仕様の内容に含めること

を求めています（遵守事項 6.2.1 並びに 6.3.1(1)及び(2)）。

先般、府省庁が利用者にソフトウェアを提供する場合の脆弱性対策について平成 28 年 10 月 18 日付事務連絡にて注意喚起を実施したところですが、平成 29 年５月 25 日以降、JPCERT/CC 及び IPA が共同で運営している脆弱性対策情報ポータルサイト（JVN）において、複数の府省庁が提供するソフトウェアのインストーラにおける DLL 読み込みに関する脆弱性が発見されたと報告されています。

また、上記に関連し、インストーラ作成ソフトウェアを使用して作成されたインストーラや圧縮解凍ツールで作成された自己解凍書庫ファイルなど、Windows アプリケーションによる DLL 読み込みやコマンド実行に関する脆弱性が多数報告されていると、JVN より情報発信されています。

つきましては、これら状況を踏まえ、広く一般にソフトウェアを提供し行政サービスを行っている又は今後提供する予定がある府省庁においては、ソフトウェア開発時に使用したツール等を把握し、該当するツール等の脆弱性を修正するための修正プログラムが提供されたときに適切に対応するなど、貴機関の情報セキュリティポリシー及びその運用に万全を期されるようお願いいたします。

なお、所管する独立行政法人及び指定法人に対しても、本注意喚起について周知願います。

＜参考＞

・Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題
　https://jvn.jp/ta/JVNTA91240916/index.html（平成 29 年５月 25 日付け）

・府省庁が提供するソフトウェアにおける脆弱性に関する情報
　https://jvn.jp/jp/JVN75514460/index.html（平成 29 年５月 25 日付け）
　https://jvn.jp/jp/JVN41185163/index.html（平成 29 年５月 25 日付け）
　https://jvn.jp/jp/JVN92422409/index.html（平成 29 年５月 26 日付け）

２　「ＤＮＳの世界的な運用変更に伴うキャッシュＤＮＳサーバーの設定更新の必要性について」（2017 年７月 18 日発出）

事　務　連　絡
平成 29 年７月 18 日

各府省庁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

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（重要インフラ担当）
内閣参事官（政府機関総合対策担当）
内閣官房 情報通信技術(IT)総合戦略室
内閣参事官

ＤＮＳの世界的な運用変更に伴うキャッシュＤＮＳサーバーの
設定更新の必要性について

この度、インターネットの重要資源の世界的な管理・調整業務を行う団体ＩＣＡＮＮ（Internet Corporation for Assigned Names and Numbers）から、ＤＮＳ（ドメインネームシステム）において電子署名の正当性を検証するために使う暗号鍵の中で最上位となる鍵（ルートゾーンＫＳＫ）を更新することが発表されました。

これに伴い、キャッシュＤＮＳサーバーを運用する者においては、速やかに事前公開されているルートゾーンＫＳＫの公開鍵の情報を更新する等の措置を講じる必要があります。本年９月１９日までに必要な措置が講じられない場合、ウェブサイトへのアクセスやメールの送信ができない利用者が生じる可能性があります。

上記内容について総務省から内閣サイバーセキュリティセンター及び情報通信技術(IT)総合戦略室に対し周知依頼がありましたので、別紙の内容をご確認のうえ対策を講じるようお願いいたします。また、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。

別紙

インターネットの重要資源の世界的な管理・調整業務を行う団体ＩＣＡＮＮ（Internet Corporation for Assigned Names and Numbers）がDNS(ドメインネーム・システム)で利用されているDNSSECに必要な電子署名鍵を初めて交換することが発表されました。

DNSSECの電子署名正当性を確認するために使う鍵の中で、最上位となる鍵「ルートゾーンKSK」について、信頼性維持のため本年7月～来年3月に更改作業が行われ、本年9月から新旧の鍵の併用が開始されます。

キャッシュDNSサーバーを運用されている事業者等については、別紙詳細を確認いただき、「鍵更改への追従」「鍵の移行期間中のデータ量(UDPメッセージサイズ)増大」への対応を確実に実施していただきますようお願いします。

なお本年9月19日までに必要な処置が講じられない場合、Webアクセスやメール送信などができない利用者が生じる可能性があります。

対象者

DNSを用いた検索を実際に行う「キャッシュDNSサーバー」の運用者全て

例：契約者向けに提供するインターネットサービスプロバイダ、LAN利用者向けに提供する官庁・独法・学校・企業など

※DNSSECを無効にしている方も下記影響・対応の②についてご確認ください。

影響

① 検索結果の正当性が確認できなくなり利用者のネット利用に不具合が生じる。
② 検索結果の受信データ量(UDPメッセージサイズ)が増大することから、利用者のネット利用に不具合が生じる可能性がある。

対応

① 「鍵の更改」に追従する。
・キャッシュDNSサーバーのソフトウェアを最新版に更新する。
・キャッシュDNSサーバーにおいてDNSSECのトラストアンカーの自動更新の設定を行う。

② 「鍵の移行期間」のデータ量(UDPメッセージサイズ)増大に対応する。
・キャッシュDNSサーバーにおいてUDP受信サイズを4096オクテットの検索結果が受信できる設定を行う。
・キャッシュDNSサーバーにおいて4096オクテットの検索結果が受信できるか確認する。

<使用しているDNSサーバーが4096オクテットの検索結果を受信できるか確認例>
・WEBでの確認例　http://keysizetest.verisignlabs.com/
・コマンドラインでの確認例　dig +bufsize=4096 +short rs.dns-oarc.net txt
【JPRS】ルートゾーンKSKロールオーバーによる影響とその確認方法について
・https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.html
【ICANN】Root Zone KSK Rollover
・https://www.icann.org/resources/pages/ksk-rollover

３　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 13 回	2017 年 7 月 19 日	・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 ・「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」について ・サイバーセキュリティ基本法第 25 条第 1 項第 2 号に基づく監査の報告について ・DNS の世界的な運用変更に伴い必要となる対策について

別添３－10　政府機関等に係る 2017 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
2017年	４月	【概要】公正取引委員会は７日、「審決等データベース」を運用するサーバが不正利用され、３日からデータベースの使用を止めていることを公表した。その後の調査の結果、①当該サーバに使用されているソフトウェアの脆弱性により外部から不正に操作され、②不正プログラムを含むファイルのダウンロード、③不正プログラムの実行による不正なメール送信が行われていたことが判明した。 【対応等】セキュリティを更に確保する観点から新たにシステムを構築する必要があると判断し、2018 年度から政府共通プラットフォームでの公開をもってサービスを再開するとした。	外部からの攻撃
		【概要】厚生労働省福島労働局は 11 日、ハローワークインターネットサービス上の「障害者求職情報」に誤って求職者の母親の携帯電話番号を掲載したことを公表した。 【対応等】ハローワークインターネットサービス上で個人情報その他不必要な情報がないか点検した。また、個人情報を扱う業務について、漏えい防止のための基本動作を徹底するよう注意喚起した。	意図せぬ情報流出
		【概要】総務省は 13 日、政府統計の総合窓口（e-Stat）の一つの機能である「地図による小地域分析（jSTAT MAP)」という地理情報システムに不正アクセスがあり、約２万３千人分の個人情報が流出した可能性があることと、流出による被害は確認されていないことを公表した。 【対応等】該当システムの脆弱性の解消及び構成しているシステム全てについて脆弱生がないことを確認した上で、サービス提供を再開した。 更に再発防止に向け、e-Stat 全システムの監視を強化するとともに、サーバ脆弱性検査を複数回実施するなどの対策を行った。	外部からの攻撃
		【概要】徳山工業高等専門学校は 21 日、機械電気工学科ウェブサイトのトップページが外部からの不正アクセスにより改ざんされ、状況調査のため当該サーバを一時停止したことを公表した。	外部からの攻撃
		【概要】最高裁判所は 23 日、22 日に裁判所ウェブサイトが一時的に閲覧しにくくなる障害が発生したことを公表した。	ウェブサイトの閲覧障害
		【概要】独立行政法人医薬品医療機器総合機構は 28 日、新医薬品の承認申請に用いる申請電子データの一部（治験データ）が記録された USB メモリ１個を、機構内で紛失したことを公表した。	その他
		【概要】国立国会図書館は 27 日、ウェブサイトが 18～26 日の間、３回にわたり、ほぼ閲覧できない状態なったことを公表した。	ウェブサイトの閲覧障害
		【概要】参議院のウェブサイトは、28 日の午前中約６時間にわたり、ほとんど閲覧できない状態になった。	ウェブサイトの閲覧障害
	５月	【概要】情報通信研究機構は２日、Apache Struts2 の脆弱性を悪用した不正アクセスを受けたサーバ中に、利用者（378 件）の ID、メールアドレス、暗号化されたパスワードの情報が含まれていると判明したことを公表した。	外部からの攻撃
		【概要】教職員支援機構は 17 日、同機構のポータルサイト「つくばの森・Ｔネット」において、３月 28 日から５月 12 日までの間、登録ユーザーの個人情報が他の登録ユーザーにより閲覧できる状態になっていたことを公表した。	意図せぬ情報流出
		【概要】環境省は 26 日、ウェブサイトに掲載していた報告書作成支援ツール v3.02 のインストーラに脆弱性があることが判明したため、19 日より公開を中止していることを公表した。また 29 日には、それ以前に掲載していた ver2.0 以降の報告書作成支援ツールのインストーラにも同様の脆弱性があると判明したことを公表した。 【対応等】インストーラを作成するソフトウェアのバージョンを上げ、脆弱性対策を施したインストーラを公開した。	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】厚生労働省長崎労働局は 29 日、「地域若者サポートステーション事業」の受託者が事業利用者への連絡用携帯電話を紛失したことを公表した。 【対応等】受託事業者に対し、個人情報の管理を徹底させるとともに、業務で使用している携帯電話について、セキュリティ機能や画面ロック機能等を活用して、紛失・盗難の際に個人情報が漏えいしないような対策を講じることを指示した。	意図せぬ情報流出
	６月	【概要】国立環境研究所は５日、同研究所が運用する出張対応用の Web メールサーバにおいて、職員１名のメールアカウントが不正ログインされ、スパムメールが送信されたことを公表した。	意図せぬ情報流出
		【概要】国土交通省は６日、同省の「土地総合情報システム」に不正アクセスがあり、不動産取引価格アンケートの回答情報等が流出した可能性があると公表した。14 日には、個人情報の流出は確認されていないという調査結果を公表した。 【対応等】今般の不正アクセスの要因となった脆弱性を解消するとともに、システム監視の強化、再発防止を徹底することとした。	外部からの攻撃
		【概要】農林水産省は９日、ウェブサイトより提供している「電子納品チェックシステム(農林水産省農業農村整備事業版)平成 26 年３月版(Ver.8.0.001.001)」のインストーラに脆弱性が発見されたため、同日中に脆弱性対応を行い、インストーラの公開を再開したことを公表した。 【対応等】脆弱性対応を行い、インストーラの公開を再開した。	その他
	７月	【概要】外務省は７月４日及び 11 月２日、外務省職員をかたるウイルス付きファイルが添付されたメールや、不審なサイトへのリンク先が書かれたメールを確認したため、ウェブサイトに注意喚起を掲載した。 【対応等】不審メールの添付ファイルやメール本文内の URL をクリックしないように依頼する注意喚起文をウェブサイトへ掲載した。	その他
		【概要】外務省は５日、日本政府または日本大使館を装って、ビザ申請手数料を徴収しようとする詐欺サイト、ソーシャルメディア、E メールの存在を確認したため、ウェブサイトに注意喚起を掲載した。 【対応等】査証申請の確認方法等について、ウェブサイトにて注意喚起を行った。	その他
		【概要】12 日、各省庁の入札関連情報をまとめた総務省のウェブサイトで、宮内庁等が作成した入札資料に通信ネットワークで使っている機器の型番やソフトウェア名などの情報が記載され、そのまま公開されていた。 【対応等】宮内庁等は詳細情報を削除し、総務省は公開資料を差し替えた。	意図せぬ情報流出
		【概要】国立研究開発法人建築研究所は 20 日、調達情報メールサービスを装ったウイルス付きメールが配信されていることを公表した。	その他
		【概要】農林水産省は 21 日、ウェブサイトより提供している「電子納品チェックシステム（農林水産省農業農村整備事業版）平成 26 年３月版(Ver.9.0.001.001)」のインストーラに脆弱性が発見されたため、12 日に公開を中止していたが、脆弱性対応を行い、インストーラの公開を再開したことを公表した。 【対応等】脆弱性対応を行い、インストーラの公開を再開した。	その他
		【概要】厚生労働省九州厚生局は 26 日、九州厚生局麻薬取締部の職員が、覚せい剤取締法違反被疑事件の捜査において捜索現場等を撮影したデジタルカメラを一時紛失し、その後、当該デジタルカメラ本体は回収したが、撮影した記録が残っている SD カードを紛失したことを公表した。 【対応等】デジタルカメラはネックホルダーで常に身体に装着させるとともに、管理責任者を定め、現場でデジタルカメラの所在について複数人で、複数回確認することとした。	その他
	８月	【概要】勤労者退職金共済機構は 17 日、機構ドメインの不審メールが送信されている情報が機構に寄せられたことを公表した。	その他
		【概要】消防庁は 29 日、東京・霞ヶ関の消防防災・危機管理センターに置いていた災害時用のノートパソコン１台を紛失したことと、保存していた情報の不正使用は確認されていないことを公表した。持ち出した職員はおらず、盗難の疑いもあるとみて警視庁麹町署に相談した。 【対応等】施錠を強化して入出者を制限し、パソコンに入っていた公用の携帯電話番号などを変更した。	意図せぬ情報流出

年月 (※1)		情報セキュリティインシデントの概要・対応等 (※2)	種別
	９月	【概要】厚生労働省静岡労働局は 12 日、「障害者就業・生活支援センター事業」の受託事業者が事業利用者への連絡用携帯電話を紛失したことを公表した。 【対応等】受託事業者に対し、個人情報の管理を徹底させるとともに、個人情報漏えい防止策の実施状況を報告するよう指示した。	意図せぬ情報流出
		【概要】25 日、ハッキングによって SNS などから漏えいしたとみられるアカウント（ID、パスワード）の中に、日本政府や独立行政法人の使うドメイン「go. jp」のメールアドレス１万 4720 件が見つかったと報道された。 【対応等】内閣サイバーセキュリティセンターは、国の統一基準でメールアドレス等の私的使用を禁じている旨、関係省庁に改めて注意喚起した。	意図せぬ情報流出
	10 月	【概要】厚生労働省石川労働局は２日、受託事業者の担当者２名に対してメールを送信する際、受託事業者ではない者にも送信したことを公表した。 【対応等】メール送信時の点検･確認と個人情報漏えい防止対策徹底を指示した。	意図せぬ情報流出
		【概要】環境保全再生機構は 13 日、環境保全活動を行う助成団体の連絡先として登録しているメールアドレス（292 件）宛てにメールを 11 日に一括送信した際、誤ってメールアドレスを To 欄に入力し送信したことを公表した。	意図せぬ情報流出
		【概要】独立行政法人国立重度知的障害者総合施設のぞみの園は 18 日、当該法人のメールサーバにおいて不正中継が行われていたことを公表した。	その他
	11 月	【概要】厚生労働省大分労働局は２日、「訓練受講希望者等に対するジョブ・カード作成支援推進事業」の受託事業者が、求職者に対してジョブ・カードをメールで送信する際､別の求職者に係る職業能力証明シートを誤って送信したことを公表した。 【対応等】受託事業者に対し、メール送信時の点検・確認と個人情報漏えい防止対策の徹底を指示した。	意図せぬ情報流出
		【概要】厚生労働省群馬労働局は 14 日、高崎労働基準監督署において、患者のレントゲン写真等の画像データが保存されている CD-R１枚を紛失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、個人情報が保存された記録媒体の処理手順の見直しを行った。	その他
	12 月	【概要】放送大学は 13 日、11 月８日に放送大学から大量のメールが送信された事象があり、調査した結果、放送大学のアカウントが第三者に不正に利用され、不特定多数のメールアドレスに迷惑メールが送信されていたことを公表した。	その他
2018 年	１月	【概要】新潟大学は９日、同学医歯学総合病院のウェブサイトが第三者による不正アクセスにより改ざんされたことと､個人情報の流出は確認されていないことを公表した。	外部からの攻撃
	２月	【概要】産業技術総合研究所は 13 日、所内で使用している業務システムに外部からの不正アクセスがあったことを公表した。	外部からの攻撃
	３月	【概要】情報処理推進機構は 13 日、IT パスポート試験の団体申込者が利用するシステムに不具合があり、計 137 件の個人情報が漏えいしたことを公表した。	意図せぬ情報流出
		【概要】30 日、中央省庁職員の公用メールアドレス計 2000 件余りがインターネット上に流出し、匿名化ソフトを使って利用者情報を秘匿できるダークウェブ（闇サイト）の取引サイトで売りに出されていたことが報道された。 【対応等】内閣サイバーセキュリティセンターは、国の統一基準でメールアドレス等の私的使用を禁じている旨、関係省庁に再度改めて注意喚起した。	意図せぬ情報流出

※1 初めて報道又は公表された年月。
※2 情報セキュリティインシデントの概要については、報道内容・公表内容を元に記載。また、政府機関における情報セキュリティインシデントについては、公表内容を元に対応等を記載。

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

	2016 年度	2017 年度	2018 年度
当初予算額	498.3 億円	598.9 億円	621.1 億円
補正予算額	72.2 億円	32.7 億円	－

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

（本ページは白紙です。）

別添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 165
別添４－２　重要インフラにおける取組の進捗状況 170
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 185
別添４－４　安全基準等の浸透状況等に関する調査 192
別添４－５　往訪調査 207
別添４－６　情報共有件数 212
別添４－７　セプター概要 213
別添４－８　分野横断的演習 215
別添４－９　セプター訓練 217
別添４－10　補完調査 218

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 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、2017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）」に続く、我が国の重要インフラの情報セキュリティ対策として位置付けられたものであり、2017年４月にサイバーセキュリティ戦略本部で策定された。

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つの施策が掲げられており、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。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。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。

2017年度は、第４次行動計画の初年度に当たり、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、「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」のとりまとめなど、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、2016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

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

2015年５月にサイバーセキュリティ戦略本部において決定され、497の対策項目を採録している「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４版）」（以下「指針」という。）に関し、往訪調査等の各種機会を通じて、重要インフラ事業者等へ説明を行い、周知を図った。

また、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、４つの分野において安全基準等の改善を行ったほか、11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現状の把握に努めた。

○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（参考：別添４－４）。アンケート調査では、3,142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約２割であった。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。一方、CSIRTを設置している事業者がほとんど増えていないことから、CSIRTの設置等について呼びかけていく必要がある。

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

2017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）」を策定した上で、同指針の普及・浸透を図るともに、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。

○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て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。2017年度も前年度に引き続き、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388件の情報連絡が行われ、内閣官房からは54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
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
内閣官房からの情報提供件数	38件	44件	80件	54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。なお、第４次行動計画において、セプター事務局を経由した新たな情報連絡ルートの導入が明記されたところであり、セプター事務局経由で匿名化された情報が出てくるなど、一定の効果が出ている。

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、内閣官房（事態対処・危機管理担当）及び関係省庁と連携し、大規模サイバー攻撃事態等対処訓練に参加し、関係主体の役割の在り方及び当該手順の実効性に関する検証を実施した。

○セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、13分野で18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、一部の分野については、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。

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、NISC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、2017年４月の総会で決定した活動方針に基づき、2017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）、企画運営WG（４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、並

びに、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）」の運営を通じて、情報共有活動の更なる充実を図っている。

○深刻度評価基準の策定に向けた取組

専門調査会の下に設置した重要インフラサービス障害に係る対処態勢検討ワーキンググループにおいて議論を行い、取組の第一段階として、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』評価するための評価基準の試案を策定した。

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、情報共有をしやすくする環境整備（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（深刻度評価基準の策定、OT・IoT等を含む共有範囲の明確化）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、NISCは運営及び活動に対する支援を継続していく。

なお、深刻度評価基準については、パブリックコメントの結果も踏まえ、議論を継続する。

(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、そのために必要な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。

○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「セキュリティ意識とニーズに応える演習企画」、「セキュリティ対策のPDCAサイクルの強化に資する運営」、「情報共有体制の実効性向上」、「演習運営ノウハウや知識等の還元」に取り組んだ（参考：別添４－８）。

全13分野が演習に参加し、2014年度分野横断的演習と比較すると、参加者数は約7.6倍（348名→2,647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の機会をもうけた。

表２　分野横断的演習参加者数の推移

年度	2014	2015	2016	2017
参加者数	348名	1,168名	2,084名	2,647名

2017年度において、事業継続計画（BCP）を関係部署と協議し的確に発動できている事業者は、2016年度から大きな変化はなく、いずれも70%以上である。また、経営層の参加率については、事前の説明会において、その重要性に言及したこと等から2016年度は23%、2017年度は29%となり、若干の増加がみられた。

○セプター訓練

各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	2014	2015	2016	2017
参加セプター	14	18	18	18
参加事業者	1,644	1,658	2,020	2,106

実施に当たっては、重要インフラ事業者等に情報が届いているかを確認（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など、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、本訓練の有用性があらためて確認された。

○重要インフラ所管省庁等との連携

NISC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）を実施したほか、経済産業省では制御システムセキュリティセンター（CSSC）における模擬システム等を用いて、制御システムを有する電力・ガス・ビル・化学の４分野において、実践的なサイバー演習を行った。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 Ⅱ）を実施した。

イ　今後の取組

第４次行動計画に基づき、「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」について取り組む。

セプター訓練については、最近、参加事業者数が増加していることから、その機会を有効に活用し、各分野の特性や最新の攻撃トレンドを踏まえた模擬情報のカスタマイズ化、全セプターにおける日程を定めない抜き打ち訓練や（セプター事務局を経由する）新たな報告形態の導入を念頭に置いた訓練の実施等、内容の充実に取り組む。

(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、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」をとりまとめた。さらに、重要インフラ事業者等への浸透を図るべく、セプターカウンシルにおいて、当該手引書に関する説明を実施した。

○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、セプターカウンシルにおいて、当該指針に関する説明を実施した。

○リスクコミュニケーション及び協議に対する支援

内閣官房は、重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても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、オリパラ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、説明会や意見交換会等を開催し、オリパラ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

2017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必要に応じた支援を実施する。

(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。

なお、「情報共有体制の強化」とも関連する施策として、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、セプター事務局の民間主体への移行（医療セプター）、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、標的型攻撃に関する情報共有体制であるC4TAPの運用改善などの成果や、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

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公表した。

重要インフラ事業者等に対しては、政府機関、関係機関、セプター、海外機関の情報セキュリティに関する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16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国民への周知を図った。

○国際連携

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、2017年10月にノルウェーで開催されたMeridian会合において、日本における重要インフラ防護のための各施策や取組等の事例紹介や、各国の取組等に関する意見交換を実施した。また、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、2017年７月に日・ASEANワークショップを開催し、海外政府関係者、国際機関及び我が国の専門家を講師に招き、ASEAN各国が自国に適した政策の検討に資する取組やベストプラクティスの共有を図った。

二国間では、日米間の重要インフラ防護をテーマとする会合における講演・意見交換や、日英サイバー協議をはじめとする政府間協議等を行った。

○規格・標準及び参照すべき規程類の整備

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案をとりまとめた。さらに、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、EDSA認証取得のために必要な機器開発・設計・検証等に関するセミナーを実施するとともに、制御システムのセキュリティ評価・認証に関する検討を実施した。

イ　今後の取組

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。

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詳細

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案を 2018 年３月にとりまとめた。
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。	・他施策との連携強化として、安全基準等策定指針対策編の対策項目に基づいて、分野横断的演習の検証課題の設定を実施した。
③上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。	・内閣官房において、四半期毎に開催した重要インフラ所管省庁との連絡会議等の機会を通じて、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。	・内閣官房において、重要インフラ所管省庁の協力を得て、各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（2017 年 12 月～2018 年３月）し、「2017 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 2018 年３月に公表した。 ・各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。	・内閣官房において、重要インフラ所管省庁の協力を得て、各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（2017 年６月～12 月）及び事業者等への往訪による調査（2017 年１月～12 月）を実施し、「2017 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」及び「2017 年度 重要インフラ事業者等 往訪調査 調査報告書」を 2018 年３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。	・内閣官房において、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。（2017 年度　情報連絡 407 件、情報提供 54 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から情報を受領し、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。
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、考え方の整理を実施した。
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集約するための情報共有システムの構築に向けた検討を実施した。
⑥ 重要インフラ所管省庁の協力を得つつ、各セプターの機能、活動状況等を把握するための定期的な調査・ヒアリング等の実施、先導的なセプター活動の紹介。	・重要インフラ所管省庁の協力を得て、2017 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
⑦ 情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。	・セプター事務局や重要インフラ事業等への支援に向け、情報共有に必要となる情報共有システムの構築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幹事会及び運営委員会、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。（2017 年度のセプターカウンシル会合の回数は延べ 20 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する秘密保持契約の締結に向けた検討を行った。
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所管省庁へ報告を行うなど、より実態に即した訓練を 13 分野 18 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、「セキュリティ意識とニーズに応える演習企画」「セキュリティ対策の PDCA サイクルの強化に資する運営」「情報共有体制の実効性向上」「演習運営ノウハウや知識等の還元」に重点をおきつつ、分野横断的演習を実施した。2017 年度は、2,647 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 年のオリパラ大会を見据えた情報共有体制の確認や横連携（事業者間の情報共有）における視点にも留意した。 ・ 経営層向けの内容を含む講演を実施するとともに、経営層による演習参加の意義・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。	・ 演習実施前に、演習の検証課題を例示することにより、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。 ・ 事後の意見交換会における討議事項に「事業継続計画」などに関する事項に加え、セキュリティに関する対策や課題等に関する意見交換を行う機会を提供した。
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、目的等を整理した「テキストブック」を作成し、参加事業者に提供した。また、昨年度の演習後の取組みで他の事業者にも十分に参考となる事例を「グッドプラクティス」として提示した。 ・ 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、参加事業者に、これを分かりやすく提示した。
⑦ 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開。	・ 重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、対外的に明確化した資料を作成し展開した。
⑧ 職務・役職横断的な全社的に行う演習シナリオの実施による人材育成の推進。	・ 複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者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。 ・ 2017 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（７回）及び情報交換会（３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（141 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、2018 年４月に公表した。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した。
③ 本施策における調査・分析の結果を重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に反映する参考資料として提供。	・ 環境変化調査として、リスクアセスメントの実施における、限られた資産を有効に使うための優先順位を判断するために必要となるサービス維持レベルの検討に資するため、各重要インフラ分野の事業者が、サービス提供に当たり設定している約款などを調査し、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傾向等の把握を行った。
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。	・ 環境変化調査として、各重要インフラ分野の事業者が、サービス提供に当たり設定している約款などを調査し、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傾向等の把握を行った。これが、重要インフラサービスの安全かつ持続的な提供に関する継続的な議論の深化に資するものとなることも期待している。
⑤ 重要インフラ事業者等が取り組む内部ステークホルダー相互間のリスクコミュニケーション及び協議の推進への必要に応じた支援。	・ 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、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。	・ サイバーセキュリティ対処調整センターについて、2018 年度末の構築に向け、仕様の細部について検討を実施すると共に、情報共有・対処体制に関する基本的な方針を関係府省庁、大会組織委員会、東京都等と協議の上、改正した。また、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」の中で、2018 年度末を目途に構築及び運用開始することを決定した。
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月に公表した。
(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、セプターカウンシル事務局の民間主体への移行、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、標的型攻撃に関する情報共有体制である C4TAP の運用改善などの成果や、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 23 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 19 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、日・ASEAN CIIP ワークショップや Meridian 会合及び IWWN 等の地域間・多国間における取組に参加し、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。	・アメリカ DHS との会合等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、国際整合性も考慮した上で深刻度評価基準の素案を策定した。
⑥ 重要インフラ所管省庁と連携し、重要インフラ事業者等の経営層に対し働きかけを行うとともに、知見を得て、本行動計画の各施策の改善に活用。	・経営層に関する取組は、基本Ｇをフォローしつつ、各省庁の経営ガイドライン等の調査を行った。
⑦ 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行。	・重要インフラ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、リスクマネジメントに関する手順書を作成するに当たって関連する規格を整理し、手順書に反映した。
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た。
2. 重要インフラ所管省庁の施策　金融庁、総務省、厚生労働省、経済産業省、国土交通省	
(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、2017 年 11 月に「サイバーセキュリティ経営ガイドライン」の改訂を行い、「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」の追加や、委託先の組織としての活用の把握等の留意点の追記等を行った。
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。	・2018 年４月から、主要な空港ビル事業者等が「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく各種取組みを開始することから、事業者自らが情報セキュリティ対策を実施するにあたっての参考となるように、国土交通省において 2018 年３月に「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」を作成した。 ・厚生労働省については、サイバー攻撃の手法の多様化・巧妙化を含めた医療情報システムを取り巻く環境の変化に対応するため、「医療情報の安全管理に関するガイドライン」の改定を行い、2017 年５月に第５版を公表した。また、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業に着手した。 ・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。
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、2017 年５月に行った「医療情報システムの安全管理に関するガイドライン」の改定に併せて、「医療情報システムを安全に管理するために－－『医療情報システムの安全管理に関するガイドライン』全ての医療機関等の管理者向け読本」についても、第２版として改定を行った。
⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各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、所管の各分野に協力を求め、3,144 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」、総務省では「地方自治情報管理概要」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。 ・ 国土交通省については、航空、鉄道、物流分野における、有事の情報共有・平時の知見共有を通じた集団防御を図るため、重要インフラ事業者（航空、鉄道、物流）が情報の共有・分析や対策を連携して行う体制である「交通 ISAC（Information Sharing and Analysis Center）」（仮称）の創設に向けた支援を行っている。 ・ 平成 30 年３月 17 日に医療セプター事務局を厚生労働省から公益社団法人日本医師会に移管するとともに、日本歯科医師会、日本薬剤師会、日本看護協会及び四病院団体協議会についても構成員とすることとした。
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において、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において、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。 ・ 平成 30 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。
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。
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は、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った。
(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、2017 年７月から 10 月までの間に、全 18 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、2017 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、2017 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 2017 年度分野横断的演習への参加を促し、全体で過去最多の 2,647 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、2017 年度分野横断的演習の事後アンケートに回答するとともに、演習における対応記録を作成し来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、来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」を実施したほか、経済産業省では制御システムセキュリティセンター（CSSC）における模擬システム等を用いて、制御システムを有する電力・ガス・ビル・化学の４分野において、実践的なサイバー演習を行った。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 Ⅱ）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。	・ 厚生労働省においては、NISC 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は、NISC が作成したリスクアセスメント・ガイドラインや手引書等の浸透状況を把握するための調査に協力した。
③ 本施策における調査・分析に関し、当該調査・分析の対象に関する情報及び当該調査・分析に必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査・分析が本施策における調査分析と関連する場合には、必要に応じて内閣官房と連携。	・ 重要インフラ所管省庁から、重要インフラ分野に関するＩＴ障害等の情報提供や環境変化などの動向など、必要な情報を内閣官房に提供した。
④ 本施策における調査・分析の施策へ活用。	・ 「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今後、情報共有体制の強化に係る施策を検討するに当たっての基礎資料として活用が予定されている。 ・ 厚生労働省においては、平成 29 年度は海外における医療分野のサイバーセキュリティに関する基礎調査を行った。平成 30 年度は海外における情報連携機能（ISAC 等）について調査する予定。
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。	・ 厚生労働省では、医療分野においては、平成 29 年５月に改定を行った「医療情報の安全管理に関するガイドライン（第５版）」の中で、非常時の事前・事後の対応について、サイバー攻撃に関して記載を追加した。また、水道分野においては、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業を進め、コンティンジェンシープランを位置付ける予定。
(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 情報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は、「水道分野における情報セキュリティガイドライン（第３版）」の改定作業を進め、経営層が果たすべき役割を位置付ける予定。
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及び内閣官房において、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は、医療セプターの構成員について、セプター事務局において検討・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。	・ 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。2017 年度は、重要インフラ事業者から、553 名受講した。 ・ 分野横断的演習等に参加した。

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、CSSC に委託したサイバーセキュリティ演習にて制御システムのセキュリティ評価・認証を取り上げ、演習参加者である重要インフラ事業者等の意識向上を図った。
3. 情報セキュリティ関係省庁の施策	**警察庁、総務省、外務省、経済産業省、原子力規制庁、防衛省**
(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	**内閣府（防災担当）、警察庁、防衛省**
(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。	・ 2017 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、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。	・ 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、2017 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、2017 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

安全基準等の継続的改善状況（概要）

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3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
	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
金融	銀行等 生命保険 損害保険 証券	金融機関等におけるセキュリティポリシー策定のための手引書 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空		航空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）
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：22件

○安全基準等の継続的改善における2017年度の取組状況については以下のとおり。

分析・検証後、改定を実施済：4件　　分析・検証後、改定を実施中：2件　　分析・検証を実施中：9件

（上記以外にも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7件）

○分析・検証を行うに至った主な契機は以下のとおり。

・安全基準等策定指針の改定
・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、「政府機関の情報セキュリティ対策の統一基準」改定や改正個人情報保護法への対応等もあった。）

○指針の継続的改善に繋がる具体的な改定事例として以下が挙げられた。

リスクベースアプローチの導入、外部委託に関するリスク管理、FinTechに関するリスク管理に関する考え方を反映

（金融機関等コンピュータシステムの安全対策基準・解説書より）

【考察】

調査結果より、下記のことが考えられる。

- 安全基準等策定指針の改定に伴い、PDCAサイクルに基づいた構成とするなど、安全基準等の改善が見受けられる。
- 抽出した課題に基づいたリスク評価を実施するなど、リスクアセスメントの考え方が安全基準等に取り込まれていることが認められる。
- 医療分野では、多様化・巧妙化しているサイバー攻撃や、IoT等の新技術及びそれを利用したサービスの普及等に対応すべく、項目の追加・改定を実施し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 1/11）

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3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	2016年5月
分析・検証状況	分析検証の実施状況	実施中	実施中
	分析検証の実施契機	・定期的に検証することとしている	・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4月～2018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）電気通信事故検証会議及びネットワークの安全・信頼性対策に関する調査にて得られた提言等を踏まえて改定の検証を実施する。	（１）2017年4月～2018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 （３）同協議会内の安全基準検討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で改定案を作成し、安全・信頼性協議会で承認する。
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	－	－

安全基準等の継続的改善状況（詳細 2/11）

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	2017年度実施予定なし （理由：現在、ICT-ISAC放送設備サイバー攻撃対策WGにて放送設備に関するサイバーセキュリティガイドラインを作成中のため）
	分析検証の実施契機	その他状況の変化等 （具体的に：近年、IoT等のネットワークの新たな利用形態の広がりやネットワークのソフトウェア化等の技術進展により、通信サービスの多様化・高度化が進展したため。）	－
	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）2017年12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）2018年７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	－	－

安全基準等の継続的改善状況（詳細 3/11）

分野		情報通信（ケーブルテレビ）	金融
名称		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	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
発行主体等		一般社団法人日本ケーブルテレビ連盟	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		2012年11月	2008年６月
分析・検証状況	分析検証の実施状況	実施中	2017年度実施予定なし （理由：セキュリティポリシーに関する課題が無いことから、改訂のための分析・検討予定なし。）
	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）2017年4月～2018年3月 （２）日本ケーブルテレビ連盟 （３）日本ケーブルテレビ連盟事務局において分析・検証を実施し、必要に応じて通信・放送制度委員会において議論する	－
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	－	－

安全基準等の継続的改善状況（詳細 4/11）

分野		金融	金融
名称		金融機関等コンピュータシステムの安全対策基準・解説書	金融機関等におけるコンティンジェンシープラン策定のための手引書
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		2018年3月	2017年5月
分析・検証状況	分析検証の実施状況	2017年度に実施済	2017年度実施予定なし （理由：2016年以前に分析・検証実施済。）
	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）2016年7月～2017年4月 （２）公益財団法人金融情報システムセンター（FISC）監査安全部（以下、当センターという） （３）当センターにて2016年6月まで開催された「金融機関における外部委託に関する有識者検討会」及び、2017年6月までに開催された「金融機関におけるFinTechに関する有識者検討会」における検討内容を踏まえ、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を行う。	－
改定状況	改定の実施状況	2017年度に実施済	2017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）2017年5月～2018年3月 （２）公益財団法人金融情報システムセンター（FISC）監査安全部（以下、当センターという） （３）当センターにて金融機関、ＩＴベンダー等から構成される安全対策専門委員会を開催し、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂に係る検討を行った（計9回開催）。 改訂原案は、2018年2月に開催された安全対策専門委員会にて最終承認を受け、2018年3月にPDF版を当センターのＨＰにてリリース、2018年5月には冊子版を発刊。	（１）2016年9月～2017年5月 （２）公益財団法人　金融情報システムセンター（FISC）監査安全部 （３）サイバー攻撃動向等を踏まえ、「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」のサイバー攻撃対応に係る改訂を実施した。2017年3月に安全対策専門委員会にて改訂内容が承認され、2017年5月に第3版追補3を発刊した。
	改定内容	リスクベースアプローチの導入、外部委託に関するリスク管理、FinTechに関するリスク管理に関する考え方を反映	昨今のサイバー攻撃動向等を踏まえ、サイバー攻撃リスクの特性やサイバー攻撃対応の考慮事項（態勢整備、平時の運用、インシデントレスポンス等）について記載。

安全基準等の継続的改善状況（詳細 5/11）

分野		航空	鉄道
名称		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）	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）
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		2016年4月1日	2016年4月1日
分析・検証状況	分析検証の実施状況	実施中	実施中
	分析検証の実施契機	・安全基準等策定指針の改定	・安全基準等策定指針の改定
	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）2017年（平成29年）4月～2018年（平成30年）3月 （２）航空運送事業者・定期航空協会・国土交通省 （３）当該ガイドラインについては、最終改定が2016年（平成28年）4月1日付けであることから、 ①それ以降に改定された「政府機関の情報セキュリティ対策のための統一基準群」を初めとした、ガイドラインの参照規程の改定内容 ②今後行われる予定と聞いている、「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」の改定内容 の２点を踏まえたガイドラインの改定について、作業方針及び改定内容の検討中である。	（１）2017年（平成29年）4月～2018年（平成30年）3月 （２）国土交通省・重要インフラ関係事業者等 （３）当該ガイドラインについては、最終改定が2016年（平成28年）4月1日付けであることから、 ①それ以降に改定された「政府機関の情報セキュリティ対策のための統一基準群」を初めとした、ガイドラインの参照規程の改定内容 ②今後行われる予定と聞いている、「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」の改定内容 の２点を踏まえたガイドラインの改定について、作業方針及び改定内容の検討中である。
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	－	－

安全基準等の継続的改善状況（詳細 6/11）

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	2016年9月
分析・検証状況	分析検証の実施状況	2017年度実施予定なし （理由：2016年に策定されたところであり、環境変化がないため）	2017年度実施予定なし （理由：2016年に改定されたところであり、環境変化がないため。）
	分析検証の実施契機	－	－
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	－
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	－	－

安全基準等の継続的改善状況（詳細 7/11）

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	2017年度実施予定なし （理由：2016年に改定されたところであり、環境変化がないため。）	2017年度実施予定なし （理由：　2016年に策定されたところであり、環境変化がないため）
	分析検証の実施契機	－	－
	分析・検証プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	－
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	－	－

安全基準等の継続的改善状況（詳細 8/11）

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	2015年3月
分析・検証状況	分析検証の実施状況	2017年度実施予定なし （理由：「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版の発行を踏まえて2018年度に実施予定のため）	2017年度に実施済
	分析検証の実施契機	－	・その他状況の変化等 （具体的に：「政府機関の情報セキュリティ対策の統一基準」改定を受けて）
	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）平成28年12月～平成29年3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最近のセキュリティ事案の動向調査→②地方公共団体における情報セキュリティポリシー運用状況の調査→③平成29年度改訂に向けての課題整理及び改正の方向性
改定状況	改定の実施状況	－	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）平成29年12月～平成30年3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
	改定内容	－	「政府機関の情報セキュリティ対策の統一基準」等の反映

安全基準等の継続的改善状況（詳細 9/11）

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	2013年6月
分析・検証状況	分析検証の実施状況	2017年度に実施済	実施中
	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 ・その他状況の変化等 （具体的に：改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等への対応）	・安全基準等策定指針の改定
	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）2016年6月～2016年12月 （２）医療情報ネットワーク基盤検討作業班（医療情報ネットワーク基盤検討会の下に設置される作業班） （３）現状調査等の結果を踏まえ、当該作業班において改定案を作成し、医療情報ネットワーク基盤検討会に諮る。	（１）2017年12月～2018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うこととしている。
改定状況	改定の実施状況	2017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）2016年12月～2017年5月 （２）医療情報ネットワーク基盤検討会 （３）医療情報ネットワーク基盤検討作業班において作成した改定案について、パブリックコメントを実施した上で、医療情報ネットワーク基盤検討会で決定した。	－
	改定内容	サイバー攻撃の手法の多様化・巧妙化、IoT等の新技術やサービス等の普及等、医療情報システムを取り巻く環境の変化及び改正個人情報保護法に対応するため、項目の追加、改定を実施するとともに、第4.2版の公表以降に追加された標準規格等への対応等を行った。	－

安全基準等の継続的改善状況（詳細 10/11）

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３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		2016年4月1日	2015年3月
分析・検証状況	分析検証の実施状況	実施中	実施中
	分析検証の実施契機	・安全基準等策定指針の改定	・安全基準等策定指針の改定
	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）2017年（平成29年）4月～2018年（平成30年）3月 （２）国土交通省総合政策局物流政策課、物流事業者及び業界団体（17社6団体） （３）当該ガイドラインについては、最終改定が2016年（平成28年）4月1日付けであることから、 ①それ以降に改定された「政府機関の情報セキュリティ対策のための統一基準群」を初めとした、ガイドラインの参照規程の改定内容 ②今後行われる予定と聞いている、「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」の改定内容 の２点を踏まえたガイドラインの改定について、作業方針及び改定内容の検討中である。	（１）現在分析・検証を実施中（改定時期については未定） （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）指針改定内容を分析・検証の上、安全基準の改定が必要と判断されれば改定作業を実施
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	－	

安全基準等の継続的改善状況（詳細 11/11）

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		2017年11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	2017年度に実施済	2017年度に実施済
	分析検証の実施契機	・その他状況の変化等 （具体的に：2017年度新規構成員追加に伴う改定。）	・安全基準等策定指針の改定
	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）2017年4月から11月にかけて、日本クレジット協会クレジットCEPTOAR運営会議において協議 （２） （３）	（１）2017年4月～2017年5月 （２）石油連盟　サイバーセキュリティ専門委員会（当時はITセキュリティ連絡会） （３）指針第4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	2017年度に実施済	2017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）2017年4月から11月にかけて、日本クレジット協会クレジットCEPTOAR運営会議において協議 （２） （３）	（１）2017年4月～5月 （２）石油連盟　サイバーセキュリティ専門委員会（当時はITセキュリティ連絡会）、危機管理委員会 （３）ITセキュリティ連絡会にて改定原案を作成、上部組織である危機管理委員会を得て、2017年5月26日に正式に策定
	改定内容	これまで、本ガイドライン内記載の「対象となる重要インフラ事業者（構成員）」を今年度新規23社の追加に伴い、別紙記載に改定。	指針第4版に基づき、以下の点について改定 （1）PDCAサイクルに基づく構成に変更 （2）新たに取り組むべき事項として以下を追加 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

別添４－４　安全基準等の浸透状況等に関する調査

調査の目的、概要及び内容

◆調査目的

本調査は、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※1」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することを目的として、毎年、重要インフラ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。

本調査への回答を通じて、重要インフラ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、本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。

※1 安全基準等
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」等の総称を指す。

◆調査概要

調査対象範囲　：　重要インフラ分野の所管省庁（以降、所管省庁）にて調査対象の重要インフラ事業者等を決定
調査方法　：　以下の方法のいずれかを所管省庁が選択
①NISCが準備する調査票（アンケート）を活用
②各所管省庁、関連組織が独自に行う調査の結果をNISCで読み替え
調査基準日　：　調査方法①の場合、2017年3月末日
調査方法②の場合、各調査で設定した基準日

◆調査内容

①安全基準等の整備・浸透に係る事項　：　指針※2の認知、内規の策定・見直しの状況
②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
③意見、要望

※2　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進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。次の各書で構成され、サイバーセキュリティ戦略本部で決定。
・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４版）
・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４版）対策編
・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（第１版）

調査結果の要約

(1) 良好な点
- 事業継続計画は、9割弱の事業者等で策定されている（策定中も含む）ことから、計画策定の重要性が浸透していることがうかがえる。（設問20）
- 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がうかがえる。（設問24）
- 監査を実施したほぼ全ての事業者等が対策の是正検討を行っていることから、監査の有効性がうかがえる。（設問29-1）
- 国の施策については、事業者や技術動向に則した取組となっている評価を8割程度の事業者等からいただけている。（設問38）

(2) 問題点
- 7割弱の事業者等がセキュリティ人材を確保できていない状況から、セキュリティ人材育成方法等を関係主体間で共有していく仕組みが必要である。（設問4）
- 継続して調査が行われた分野においては、CSIRTを設置した事業者等がほとんど増えていないことから、CSIRT設置を呼びかける必要性がある。（設問7）
- 基本方針策定に関しては、9割以上の事業者等において経営層が関与している状況である。しかし、リスク対応に関しては、半数の事業者等において経営層が関与していない。経営層の積極的な関与が期待される。（設問9-1、設問17）
- 機能保証の考え方を踏まえたリスクアセスメントは、十分に浸透しているとはいい難い状況である。（設問36）

(3) 今後の対応
- 機能保証の考え方を踏まえたリスクアセスメントを実施するため、公表を予定している「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）」等を普及していく。
- 政府の取組に関して一定の評価をいただけているため、今後も事業者等の状況や技術動向を踏まえた上で、適切な取組を実施していく。

各重要インフラ分野の調査状況

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セプターもしくはTCAに加盟する電気通信事業者	85	36	NISC調査
	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	371	227	
	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）	195	195	
金融		銀行等、証券会社、生命保険会社、損害保険会社	828	665	独自調査 (*1)
航空		航空運送事業者	7	2	NISC調査
鉄道		鉄道事業者（ＪＲ，大手民鉄）	22	22	
電力		一般送配電事業者、主要な発電事業者	12	12	
ガス		大手ガス事業者	10	10	
政府・行政サービス		地方公共団体	(1,788)	(1,788)	独自調査 (*2,*3)
医療		医療情報システム導入病院	66	35	NISC調査
水道		給水人口30 万人以上の水道事業者及び同事業者に対して、その用水を供給している水道用水供給事業者	85	85	
物流		物流事業者	17	16	
化学		石油化学工業協会会員企業のうち、協会の情報セキュリティＷＧに所属している石油化学事業者	13	13	
クレジット		クレジットセプター加盟業者	28	28	
石油		石油精製企業	8	8	
全分野合計		－－－	3535	3142	－－－

＊１：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：2017年3月31日）
＊２：地方自治情報管理概要　－電子自治体の推進状況－（調査基準日：2016年4月1日）URL:http://www.soumu.go.jp/main_content/000474755.pdf
＊３：本資料では集計されておりません。

調査結果概要 － ＰＤＣＡサイクルに沿った対策状況（1/2）－

(1) 全体集計

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))※政府・行政サービス除く

	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	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

調査結果概要 － ＰＤＣＡサイクルに沿った対策状況（2/2）－

(2) 従業員1,000名以下の重要インフラ事業者

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））※金融、自治除く

	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	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

(3) 従業員1,001名以上の重要インフラ事業者

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））※金融、自治除く

	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	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

(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

取組状況の比較（従業員数別）

	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	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2019年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
2020年度	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－

調査結果詳細（1/6）

設問1　NISCの取組の認知状況

・NISCの取組を認知している事業者等は半数程度にとどまっており、更なる周知活動が必要と考えられる。
・事業者規模別に分析した結果、規模が小さくなるほど認知率が低くなる傾向がみられた。

NISCの取組の認知状況（複数回答）

※金融は読替え可能項目なし（集計していません）

設問2　自分野の安全基準等の認知状況

・所管省庁または業界団体が発行しているガイドライン・指針等の認知率は６～７割程度となっている。発行団体からの周知や、事業者等が関心を持って情報を収集することが望まれる。

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）

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

・近年、情報漏えいやデータ等の不正利用等により、経営や事業が大きなダメージを受ける事象が発生している。このように、サイバー攻撃は経営にも大きな影響を与える可能性があるので、より多くの事業者等が経営層を巻き込んで予算を確保することが望まれる。

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）

設問4　セキュリティ人材の確保状況

・セキュリティ人材に関して、7割程度の事業者等が不足していると考えていることが浮き彫りとなった。

セキュリティ人材の確保状況（単一回答）

※金融は読替え可能項目なし（集計していません）

設問4-1　必要とする人材の職種

・「運用系情報セキュリティ業務従事者」、「部署内の情報セキュリティ管理者」及び「全社的・部署横断的な情報セキュリティの統括者」のニーズが高い。

必要とする人材の職種（複数回答）

設問5　セキュリティ人材育成の取組状況

・人材育成の手段として、自社内（グループ企業含む）や外部の研修への参加が主なものとなっている。
・2割程度の事業者等が人材育成に取り組んでいないため、本設問の選択肢を参考とし、取り組むことが望まれる。

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）

設問6　全従業員向けセキュリティ研修の実施状況

・「サイバーセキュリティは全員参加」であるため、より多くの事業者等が、全社的にセキュリティ意識の水準を向上させる施策を実施することが望まれる。
・事業者規模別に分析した結果、特に小規模事業者等では、実施率が低いため、全従業員向けのセキュリティ研修を実施することが望まれる。

全従業員向けセキュリティ研修の実施状況
（単一回答）

設問7　内部体制の取組状況

・「CSIRTの設置」について、「インシデントの一元管理」、「インシデント対応の統一的窓口」、「外部とのインシデント共有関係の構築」といった様々なメリットがあるが、今年度のCSIRT設置は2割程度となっており、CSIRTの設置が望まれる。

内部体制の取組状況（複数回答）

設問8　情報セキュリティ対策のノウハウの蓄積方法

・「情報セキュリティは一日にしてならず」、であるため、本設問の選択肢を参考とし、ノウハウの蓄積を行っていくことが望まれる。

情報セキュリティ対策のノウハウの蓄積方法
（複数回答）

※金融は読替え可能項目なし（集計していません）

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

・1割程度の事業者等が情報セキュリティ対策に関する基本方針を策定していない。基本方針は、情報セキュリティマネジメントシステムを構築する上で一番の基本となるため、策定されていることが強く望まれる。

情報セキュリティ対策に関する
基本方針の策定状況（単一回答）

設問9-1　基本方針の策定に関する経営層の関与状況

・基本方針の策定に関与している経営層は9割程度であるが、より実効的な基本方針とするため、経営層の積極的な関与が望まれる。

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）

設問9-2　策定した基本方針の外部公表状況

・策定した基本方針については、3割程度の事業者等が外部に公表している。

策定した基本方針の外部公表状況
（単一回答）

※金融は読替え可能項目なし（集計していません）

設問9-3　基本方針の見直し検討状況

・基本方針の見直し検討を行った事業者等は、6割程度であった。

基本方針の見直し検討状況（単一回答）

※金融は読替え可能項目なし（集計していません）

設問9-4　基本方針の見直し検討の契機

・基本方針の見直しについては、本設問の選択肢の契機を参考とし、必要に応じて実施することが望まれる。

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）

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ない3割程度の事業者等においては、計画を策定することが望まれる。

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）

設問10-1　計画の見直し（又は修正）状況

・計画を策定している事業者等の内、8割程度は計画の見直しを実施している。

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）

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

・ISMSにおいても、情報資産の洗い出しは、保護すべき資産を認識する第一歩となっている。しかし、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を行っていない事業者等は1割弱おり、資産の洗い出し及び管理を行うことが望まれる。

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）

設問11-1　情報資産の重要度に応じた格付け状況

・多くの事業者等では、情報資産の重要度に応じた格付けを行っている。
　情報資産は、格付けを行うことにより、脅威やリスクに対して必要なアクセス制御等の対策が明確となるため、格付けの導入について検討することが望まれる。

情報資産の重要度に応じた格付け状況（単一回答）

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ない事業者等が2割程度あるが、情報資産には生成から廃棄までのライフサイクルがあるため、定期的な見直しを実施することが望まれる。情報資産が多い場合には、運用負担が大きくなることが想定されるが、工夫して見直しを実施することが望まれる。

情報資産の見直し状況（単一回答）

設問12　脅威や脆弱性等の情報収集

・脅威や脆弱性等の情報収集を行っている事業者等は9割程度あるが、このような情報については、今後とも積極的に収集することが望まれる。

脅威や脆弱性等の情報収集（単一回答）

設問12-1　情報収集の確認頻度

・8割程度の事業者等が月に一回以上情報収集を行っている。
・脆弱性情報の公表から攻撃発生までの時間が短くなってきているため、情報収集の頻度を高めることが望まれる。

情報収集の確認頻度（単一回答）

※金融は読替え可能項目なし（集計していません）

設問13　リスクの特定状況

・リスクの特定については8割程度の事業者等が実施している。ただし、中小規模の事業者等では、リスク特定の実施率が半数を切っているため、実施することが望まれる。

リスクの特定状況（単一回答）

設問13-1　リスクの特定方法

・リスクの特定方法については、選択肢の方法を参考とし、自組織に適した手法を見つけ、実施することが望まれる。
・その他具体的な方法として、自組織の業務フローを整理し、その間に発生しうるリスクの洗い出しを実施している等の例もあった。

リスクの特定方法（複数回答）

※金融は読替え可能項目なし（集計していません）

設問14　リスク対応の要否に係る判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスク対応の要否に係る判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、要否に係る判断基準を明文化しておくことが望まれる。

リスク対応の要否に係る判断基準（単一回答）

※金融は読替え可能項目なし（集計していません）

設問15 リスク対応の優先順位に係る判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスク対応の優先順位に係る判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、優先順位に係る判断基準を明文化しておくことが望まれる。

リスク対応の優先順位に係る判断基準（単一回答）

※金融は読替え可能項目なし（集計していません）

設問16 リスクに応じた対応手段の判断基準

・事業者規模別に分析した結果、規模が小さくなるほど、リスクに応じた対応手段の判断基準を定めている事業者等が少なくなっているが、リスク対応を属人化せずに進めるために、リスクに応じた対応手段の判断基準を明文化しておくことが望まれる。

リスクに応じた対応手段の判断基準（単一回答）

※金融は読替え可能項目なし（集計していません）

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については、5割程度の経営層が把握しているが、判断結果については、経営層が把握しておくことが望まれる。

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（単一回答）

※金融は読替え可能項目なし（集計していません）

設問18 情報セキュリティに関する内規の策定状況

・事業者規模別に分析した結果、規模が小さくなるほど、情報セキュリティに関する内規を策定している事業者等の数が少なくなっているが、情報セキュリティに関する内規は策定されていることが強く望まれる。

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）

設問18-1 内規等を策定する際の参考文献

・内規等の策定・見直しの際には、選択肢にある文書を参考にすることが望まれる。
・その他の具体的内容として、ISO27001やJIS Q15001、J-CLICSチェックリスト(JPCERT)、情報セキュリティポリシーサンプル(JNSA)、重要インフラのサイバーセキュリティを向上させるためのフレームワーク(NIST)等が挙げられていた。

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）

設問18-2 策定した内規の見直し検討状況

・内規の見直し検討を行った事業者等は7割程度であった。

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）

設問18-3　内規の見直し検討の契機

・選択肢の項目を参考とし、必要に応じて内規を見直すことが望まれる。
・その他の例として、自然災害や情報漏えい事案が起こった際などの例が挙げられていた。

※金融は読替え可能項目なし（集計していません）

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定を「策定している」または「策定中」の事業者等は8割程度であった。

※金融は読替え可能項目なし（集計していません）

設問20　事業継続計画の策定状況

・1割強の事業者等は事業継続計画を策定していないため、事業継続計画の策定が望まれる。

設問20-1　事業継続計画に基づいた訓練状況

・事業継続計画を策定している事業者等のうち、事業継続計画に基づいた訓練を行った事業者等は6割程度であった。

設問20-2　事業継続計画の見直し状況

・事業継続計画を策定している事業者等のうち、見直しを行った事業者等は7割程度であった。

※金融は読替え可能項目なし（集計していません）

設問20-3　事業継続計画の見直し契機

・選択肢の項目に該当した場合、必要に応じて事業継続計画を見直すことを推奨したい。
・その他の例として、組織体制の変更があった際等が挙げられていた。

※金融は読替え可能項目なし（集計していません）

設問21　コンティンジェンシープラン策定状況

・コンティンジェンシープランについて、6割程度の事業者等で策定されている。

コンティンジェンシープラン策定状況
（単一回答）

設問21-1　コンティンジェンシープランの見直し状況

・約6割の事業者等がコンティンジェンシープランを見直しており、今後も必要に応じて見直しを行うことが望まれる。

コンティンジェンシープランの見直し状況
（単一回答）

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定については、6割程度の事業者等が策定していることが認められる。

外部委託に関する規定の策定状況
（単一回答）

※金融は読替え可能項目なし（集計していません）

設問23　外部委託先管理に関する対策

・外部委託を実施している9割程度の事業者等が、外部委託先管理の対策を実施しているが、外部委託先管理に関する対策は、今後も継続していくことが望まれる。

外部委託先管理に関する対策（複数回答）

※金融は読替え可能項目なし（集計していません）

設問24　実施済みの情報セキュリティ対策

・おおよその対策は取られているが、「証跡管理」や「重要データの暗号化」に関しては、実施率が低いため、未実施の事業者等においては、必要に応じて実施することが望まれる。

実施済みの情報セキュリティ対策（複数回答）

設問25　責任者へのセキュリティ対策の運用報告

・ほぼ全ての事業者等が責任者へ報告を実施しているが、今後も必要に応じて、報告を上げることが望まれる。

責任者へのセキュリティ対策の運用報告
（単一回答）

設問25-1　経営層への情報セキュリティ運用報告

・ほぼ全ての事業者等が、経営層まで適切に報告を行っている。

経営層への情報セキュリティ運用報告
（単一回答）

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については、4割程度の事業者等が設置している。

対外向けの情報共有窓口の設置状況
（単一回答）

※金融は読替え可能項目なし（集計していません）

設問27　障害発生時における連絡体制の整備状況

・9割程度の事業者等において、障害発生時の連絡体制が整備されているが、一歩進んで連絡体制がきちんと機能するか確認を行うことが望まれる。

障害発生時における連絡体制の整備状況
（単一回答）

設問28　障害発生時の利用者アナウンスの判断基準

・全ての障害に対して判断基準を策定することは難しいと思われる。しかしながら、想定される障害については素早い意思決定ができるよう、判断基準を定めておくことが望まれる。

障害発生時の利用者アナウンスの判断基準
（単一回答）

※金融は読替え可能項目なし（集計していません）

設問29　情報セキュリティに関する監査実施状況

・監査の実施率について、昨年度と比較して多少伸びてはいるが、実施していない事業者等においては実施することが望まれる。

情報セキュリティに関する監査実施状況
（単一状況）

設問29-1　監査を通じた対策の是正検討状況

・ほぼ全ての事業者等が監査を通じて是正検討を行っていることから、監査の有効性が認められる。

監査を通じた対策の是正検討状況
（単一回答）

※政府・行政サービスは読替え可能項目なし（集計していません）

設問30　外部の演習等への参加状況

・外部演習等への参加が半数以下にとどまっている。演習に参加することで、セキュリティ対策の重要性や自組織内での課題を認識する機会が得られるため、参加していない事業者等においては、機会を見つけて参加することが望まれる。

外部の演習等への参加状況（単一回答）

設問31　内部での演習等の実施状況

・内部での演習を実施する事業者等は3割程度にとどまっている。セキュリティ対策に関する意識の向上を図るため、事業者内での実施が困難な場合は、外部の演習等への参加を検討することが望まれる。

内部での演習等の実施状況（単一回答）

設問32　情報共有体制下での受信状況

・NISCや省庁経由から展開された情報の受信状況は8割程度の事業者等ではあるが、セプター事務局・セプター構成員からの情報共有はまだ多くはなく、セプター内における情報共有をより活性化することが望まれる。

情報共有体制下での受信状況（複数回答）

※金融は読替え可能項目なし（集計していません）

設問32-1　受信情報の有効活用度

・6割以上の事業者等において、提供された情報を有効活用している。

受信情報の有効活用度（単一回答）

※金融は読替え可能項目なし（集計していません）

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」事業者等は6割程度になっている。「重要インフラの情報セキュリティ対策に係る第４次行動計画」等を参照し、情報共有体制の強化に向けた取組を進めることが望まれる。

能動的に行った情報共有状況（複数回答）

※金融は読替え可能項目なし（集計していません）

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」、「知らない」事業者等は8割程度になっている。「知っている」にとどまっている事業者等においては、自職場参加という形態もあるため、分野横断的演習に可能な限り参加し、セキュリティ対策の重要性に気づく機会を得ることが望まれる。また、知らない事業者等に対しては、これまで以上の広報活動も検討する。

分野横断的演習の認知状況（単一回答）

※金融は読替え可能項目なし（集計していません）

設問35　内部での訓練・演習の実施内容

・内部での訓練・演習を実施していない事業者等は6割程度になっている。内部での訓練・演習が難しい場合、分野横断的演習等、外部の訓練・演習に参加することが望まれる。

内部での訓練・演習の実施内容（複数回答）

※金融は読替え可能項目なし（集計していません）

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

・機能保証の考え方を踏まえたリスクアセスメントは、まだ十分には浸透していない。今後公表予定の、「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（第5版）」や、関連文書である「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」等を参照し、機能保証の考え方を踏まえたリスクアセスメントの取組を進めてほしい。

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）

設問36-1　結果を踏まえた対策の実施状況

・リスクアセスメントの結果を経営層へ報告している事業者が半数にとどまっている。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、経営層への更なる働きかけが必要である。NISCでは、経営層が果たすべき役割を盛り込んだ「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）」等を、今後公表予定である。

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）

設問37　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策定状況

・事業継続計画やコンティンジェンシープランの策定は一定浸透しているが、機能保証の考え方はまだ一部にしか浸透していない。今後公表予定の「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（第5版）」等を参考に、機能保証の考え方を取り入れることが望まれる。

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）

設問38　国の施策に対する意見

・多くの事業者等が、国の施策について「事業者の状況に合わせた取組になっている」又は「技術動向に合った適切な取組になっている」と考えており、今後も事業者の状況や技術動向を踏まえ、適切な取組を行っていきたい。

国の施策に対する意見（複数回答）

※金融は読替え可能項目なし（集計していません）

設問39　重要インフラニュースレターに関する状況

・7割程度の事業者等が重要インフラニュースレターを参考にしており、今後もより多くの事業者等にとって有益なものとなるよう、内容の充実や周知をさらに進めていきたい。

重要インフラニュースレターに関する状況（単一回答）

※金融は読替え可能項目なし（集計していません）

調査結果詳細 － 自由意見 －

【安全基準等、指針に関する意見】

- 規模の大きい事業者等を前提としているように感じるため、小規模事業者等用など規模ごとに分類されていれば参考になるのではないか。
- 改定があった場合は、新旧比較表を出してほしい。
- 安全基準等は、複数あってもよいのではないか。（ex.経営層向け、運用者向け、オペレータ向け、ユーザー向け 等）
- セキュリティ対策を実施しなければいけないことは十分承知しているが、中小規模の事業者等では、人員や予算の関係上、なかなか対策に踏み出しきれないのが現状。

【情報共有体制の推進に関する意見・要望等】

- 共有されている情報が多岐にわたり詳細に記載されているため非常に参考になっている。しかし、同一情報源の重複する情報も多く共有されているため、閲覧に時間が取られてしまうのが現状。
- 各所から様々な情報が提供されているが、分かりにくい。情報提供も同一組織からまとめて提供されるような体制があると、各事業者等も情報を管理しやすくなるのではないか。
- 関係省庁や関連団体、NISC等から情報発信されることで、そのリスクや対応方法を知ることができるだけではなく、内規の見直しの契機にもなる。今後とも積極的に情報提供いただきたい。
- 情報の入手については積極的に行っているが、情報発信（報告）については消極的であるのが現状。

【アンケートに関する意見】

- 本アンケート調査は専門用語が多く、回答が難しい。より多くの理解を得るためにも、分かりやすく丁寧な説明が必要。
- こういったアンケート調査に回答することで、自組織の対策状況が把握できるため、非常に役立っている。
- 業界団体経由での依頼だが、その団体がセプター事務局であっても業界団体経由での提出は情報セキュリティ上問題があると考える。業界団体・事務局スタッフは、同業他社のスタッフでもあり得るためである。アンケート回答が守秘されるよう検討いただきたい。
- WEBアンケート等を利用し、もう少し簡単にアンケートに回答できるようにしてほしい。

【国・政府に対する意見・要望等】

- セキュリティ対策の項目等は専門用語をできるだけ避け、図やチャートで説明するような取組が必要ではないか。
- 分野によっては、インセンティブが働かない限り、セキュリティ関連の対策（システム導入、人材育成、教育等）は取られないのではないか考える。
- これまで報告している安全関係の報告以外にも、セキュリティに関するインシデントの報告意識の醸成が必要。
- 中小事業者等向けの情報セキュリティ対策に関わる補助金等を整備いただきたい。
- IT人材育成に向けた支援を重視していただきたい。

【その他の意見】

- 社内や外部でのCTFを実施するのもよいのではないか。

（参考）アンケート項目

【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
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　事業継続計画の策定状況
設問20-1　事業継続計画に基づいた訓練状況
設問20-2　事業継続計画の見直し状況
設問20-3　事業継続計画の見直し契機
設問21　コンティンジェンシープラン策定状況
設問21-1　コンティンジェンシープランの見直し状況
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・コンティンジェンシープラン等の策定状況
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）

別添４－５　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

システム構成図及び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

【主な調査項目】

① システム概要　② セキュリティ対策の規程・体制等
③ 平時の対応について　④ 障害発生時の対応について
⑤ 人材育成の考え方　⑥ 経営層の関与状況　⑦ その他

4.調査対象

重要インフラ事業者等8社
（医療・水道・クレジット・鉄道　うち 中小事業者等5社）
※所管省庁や関係セプターと調整の上、対象事業者を選定
※中小事業者とは、従業員数1000名未満を指す

5.調査期間

2017年1月～2017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

調査のポイントと良好事例

今年度の主な調査のポイントと往訪調査で得られた良好事例は、以下の通り。

調査のポイント	良好事例
➢ 事業者内で、円滑にセキュリティ対策を実施するには、事業者内部の体制づくりや経営層の役割が重要ではないか。	《CSIRT》 CSIRTを設置し、社外窓口を明確化したことで、関係省庁や関係機関、セプター窓口、NISC等との情報共有が円滑になり、知りえた情報を社内に共有したことで、全社員のセキュリティ意識の向上につながったという良好事例があった。 《経営層》 経営層にシステムに熟知・精通し、セキュリティ意識をもった人材を確保することで、サイバーセキュリティ対策がなされた企業体制の構築ができていた。
➢ 制御系システムを安全かつ持続的に稼働させるためには、人材が重要な要素ではないか。	制御系システムでは、そのシステムを熟知した人材を中心に、セキュリティ対策を実施することで、安全かつ持続的なシステム稼働がなされていた。

課題と取るべき施策の例

今年度の往訪調査で得られた主な課題とNISCが取るべき施策の例は、以下の通り。

課題	NISCが取るべき施策の例
前年度は比較的大規模な事業者等との意見交換が多く、今年度は中小規模（総従業員1,000名未満）の事業者等を中心に意見交換をさせていただいた。 比較的大規模な事業者等と比較して、今年度に意見交換を実施した事業者等の多くは、比較的安価に実行が可能なセキュリティ対策でさえ実施されていない実態がうかがわれた。 以上から、対策が実施されていないのは、予算だけの問題ではなく、セキュリティマインドの低さも原因となっていると考えられる。	事業者等内で**セキュリティマインドを醸成するため**に、2018年上半期に改訂を予定している**「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」**を普及させるべく、業界団体・関係団体等に働きかける。 また、その傘下の事業者等にNISCが実施している**分野横断的演習**に参加してもらう等、中小事業者向けの普及啓発活動を推進する。
制御系システムは、巨大なシステムになりがちであり、更新費用は巨額で、更新頻度は15年～20年に1度となる場合が多い。 そのため、継続的なメンテナンスが必要であるが、外部媒体の対策が取られていないことが多い。	常に高いセキュリティ状態が保てるように、まずは**構築時から「セキュリティ・バイ・デザイン」の考え方を取り入れておく**必要があるため、「セキュリティ・バイ・デザイン」の考え方の普及を行う。 また、メンテナンスで必要となる外部媒体のセキュリティ対策の在り方についても、普及啓発していく必要がある。

（参考）往訪調査結果　①システム概要（1/7）

（問題点）

- USBポートを物理的に使用不可にする対策は取られていない。
- 保有しているシステムのサイバーセキュリティ対策に対する関心が低い。
- クローズドな環境で利用されているPCはアップデートが行われておらず、古いバージョンで稼働している。

（良好事例）

- USBポートの使用を禁止する等の規程が作成されている。
- 上位事業者等がサイバーセキュリティに関する規程を明確に定め、グループ事業者等に展開している場合、下位事象者等も同様に順守する必要がある。そのため、下位事業者等のサイバーセキュリティ対策が充実している。
- リモート接続が可能なシステムは、常時外部に接続されておらず、必要に応じて接続される規則が徹底されている。
- 重要インフラサービスのシステムは、クローズドな環境で利用されていることが多く、外部接続しているシステムと接続しないように指示が徹底されている。
- システムへのアクセスは、特定の権限・認証システムが必要である。

（考察）

- 制御系システムは、巨大なシステムになりがちであり、更新費用は巨額で、更新頻度は15年～20年に１度となる場合が多い。それゆえ、制御系システムのサイバーセキュリティ対策は、システム構築時から将来を見据えて考慮することが望まれる。
- USBポートを特殊なシールなどで物理的にふさぐ方法は、低コストで実施可能である。このような小さな対策でも、できる対策から実践することが望まれる。

（参考）往訪調査結果　②セキュリティ対策の規程・体制等（2/7）

（問題点）
- 業務委託先からのサイバーセキュリティ対策に関する向上提案が乏しい。
- 事業者内部の報告体制等が内規や基本方針等に明記されていない。
- 制御系システムのサイバーセキュリティ対策に関する規程がない。

（良好事例）
- 所管省庁、セキュリティ関係機関、NISC等が発信するサイバーセキュリティ情報を事業者内部に展開している。
- ステークホルダ全体で、サイバーセキュリティ対策に関するインシデントの訓練を実施している。
- 年に一回以上、サイバーセキュリティ研修を実施している。
- サイバーセキュリティ担当者が、サイバーセキュリティ対策の規程の必要性を感じて、規程の策定を働きかけている。
- 職層ごと（全社員向けやシステム管理者向けなど）にサイバーセキュリティの規程が存在する。

（考察）
- 各事業者の制御系システム構築や保守ができる事業者は限られ、マンネリ化した業務委託となっている可能性がある。早急に現状を把握し、厳格な業務契約により、緊張感を持ったシステム構築や保守ができる体制に改善することが望まれる。
- サイバー攻撃の手段・種類が多様化しており、年々規程の見直しが必要になっている。規程を定期的に見直す仕組み作りを検討し、定着させることが望まれる。

（参考）往訪調査結果　③平時の対応について（3/7）

（問題点）
- 制御系システムへのサイバー攻撃に対する警戒心・危機感が希薄である。
- インシデント発生を考慮した訓練を実施していない。インシデント対応経験がある人材も少ない。
- 分野内でサイバーセキュリティ対策に関する情報交換が行われていない。

（良好事例）
- ICT-BCPを策定しており、毎年外部監査を受け、正当性を担保している。
- 外部からはVPNを利用した接続を徹底している。
- 二要素認証（ID/Password、USBキー等）を利用して、高いセキュリティレベルを維持している。
- USBメモリ等への書出しは、専用のソフトウェアを必要としている。
- 内部ネットワーク上の不正利用端末対策としてMAC認証を実施している。
- 内部ネットワークに接続している全端末にアンチウィルスソフトを導入している。
- 最近発生したサイバーインシデント事例等を題材にしたサイバー訓練を実施している。
- 重要データはクラウドではなく、オンプレミスで運用され、他サービスとは別の専用回線を使用している。
- 物理的なアクセス権の制限等、従業員の出入りを徹底管理している。

（考察）
- サイバーセキュリティ対策関係は、優先順位が低く、対策検討の段階で落されがちである。サイバーセキュリティ対策の重要性を認識していただき、重要インフラサービスを堅守することが望まれる。
- 事業者間で活発な情報交換を実施し、重要インフラ全体の防護能力を向上することが望まれる。

（参考）往訪調査結果　④障害発生時の対応について（4/7）

（問題点）
- コンティンジェンシープランが策定されていない。
- コンティンジェンシープランを策定している事業においても、コンティンジェンシープランを発動する訓練は実施されていない。

（良好事例）
- 初動対応マニュアルが存在している。
- 小規模のサイバー攻撃に対しても、関連グループ内で情報共有し、連携を深めている。
- 全従業員向けの連絡手段を構築している。
- サイバーセキュリティ対策の訓練は、全国拠点で実施し、実機にて行っている。

（考察）
- システムに関わるインシデント発生時には、システムを総括する責任者に報告し、対応することになる。普段から障害発生時を想定した訓練を行い、その連絡系統が実際に機能するのか、責任者から有効な指示が出せるのか、等を検証することが望まれる。

（参考）往訪調査結果　⑤人材育成の考え方（5/7）

（問題点）
- サイバーセキュリティ人材が不足している。

（良好事例）
- サイバーセキュリティ知識向上のため、外部研修等の機会を設けている。
- サイバーセキュリティの専門講師を招聘し、全社員のセキュリティ意識向上に役立てている。
- セキュリティポリシーに基づき、セルフチェックを実施している。
- 全従業員が複数年に一度は参加できるよう、サイバーセキュリティの訓練を実施している。
- サイバーセキュリティ人材育成に特化した取り組みとして、資格取得を奨励している。
- サイバーセキュリティ対策向けの業者に委託し、全従業員向けの訓練を実施している。
- セキュリティ関係団体が貸与しているDVD等を利用した視聴教材で人材育成を実施している。

（考察）
- 各事業者等には、サイバーセキュリティの専門人材がいないことが多く、担当者は他業務（主にシステム関係）と併任になっている体制が主立っている。今後サイバーセキュリティ対策の重要度はますます増加することが予想されるため、セキュリティ対応体制の強化を検討することが望まれる。

（参考）往訪調査結果　⑥経営層の関与状況（6/7）

（問題点）
- 一部の経営層は、サイバーセキュリティ対策を軽視している。

（良好事例）
- 経営層がITに関する講演を外部で行うなど、IT全般に知見がある。
- 経営層とシステム関係者が直接意見交換できる場を設けている。
- 経営層が、サイバーセキュリティ意識の醸成が必要であると強く感じている。

（考察）
- サイバーセキュリティ対策の強化は、年々重要度が増し、意識の醸成が必要不可欠である。経営層の方々には、従業員に対して、サイバーセキュリティの重要性を気付かせる機会を提供するなど、積極的な働きかけを行っていくことが望まれる。また、サイバーセキュリティ対策の専門人材の配置や内規・基本方針等の整備等、インシデント発生時に早急に的確な対応ができる仕組みを作り上げていくことが望まれる。

（参考）往訪調査結果　⑦その他（7/7）

（問題点）
- 制御系システムのある事業者等では、内部でコンセンサスを取る部署が明確になっていない。
- CSIRTを十分に理解していない従業員が多い。
- データの開示範囲やアクセス権などの分類ができておらず、全てのデータを守っている状態である。

（良好事例）
- 情報系の人材と制御系の人材間の情報交換が活性化され、分野横断的演習などの訓練に部署間を跨いで参加するようになり、相互協力体制が強化されている。
- セキュリティ対策の観点から、外部委託は一切実施していない。
- CSIRTの設置により、事業者内部でのセキュリティ意識が向上した。
- 新規システム構築時には、セキュリティ審査を行う委員会に稟議を掛けてから実施している。
- リスクアセスメントを実施している。

（考察）
- Miraiのように、IoT機器を利用したマルウェアも存在する。各組織のIoTについても管理体制を強化することが望まれる。

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３次行動計画」及び「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	FY26	FY27	FY28	FY29				
	計	計	計	1Q	2Q	3Q	4Q	計
重要インフラ事業者等から NISC への情報連絡(※)	124	401	856	148	101	73	66	388
関係省庁・関係機関からの NISC への情報共有	27	52	41	13	1	1	4	19
NISC からの情報提供	38	44	80	26	9	14	5	54

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			FY26	FY27	FY28	FY29				
			計	計	計	1Q	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	9	75	330	41	21	15	3	80
発生した事象	機密性を脅かす事象	情報の漏えい	9	15	30	3	4	3	5	15
	完全性を脅かす事象	情報の破壊	14	52	47	8	4	3	5	20
	可用性を脅かす事象	システム等の利用困難	38	86	80	37	43	36	27	143
	上記につながる事象	マルウェア等の感染	27	111	289	42	9	5	9	65
		不正コード等の実行	3	11	10	4	4	2	3	13
		システム等への侵入	12	27	26	5	5	4	3	17
		その他	12	24	44	8	11	5	11	35

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		FY26	FY27	FY28	FY29				
		計	計	計	1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	6	83	546	54	28	1	6	89
	ユーザＩＤ等の偽り	7	8	1	3	1	0	0	4
	DoS 攻撃等の大量アクセス	25	47	23	12	14	5	0	31
	情報の不正取得	13	8	14	3	7	3	3	16
	内部不正	0	2	0	0	1	0	3	4
	適切なシステム等運用の未実施	4	10	19	4	5	5	1	15
偶発的な原因	ユーザの操作ミス	0	10	15	6	10	4	3	23
	ユーザの管理ミス	2	5	8	7	3	1	2	13
	不審なファイルの実行	1	51	243	28	11	1	2	42
	不審なサイトの閲覧	1	49	29	3	1	11	5	20
	外部委託先の管理ミス	10	12	20	11	8	12	10	41
	機器等の故障	7	17	22	6	8	12	6	32
	システムの脆弱性	9	29	56	22	5	6	3	36
	他分野の障害からの波及	1	5	0	0	4	5	1	10
環境的な原因	災害や疾病等	0	0	0	0	0	0	0	0
その他の原因	その他	9	22	34	5	6	7	11	29
	不明	43	105	92	23	11	7	16	57

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（2018 年４月 24 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。

セプター特性把握マップ

2018年3月末日現在

重要インフラ分野	情報通信			金融				航空	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	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				航空分野における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
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険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 総務部組織法務グループ	(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	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	24社 1団体	335社 1団体	196社・団体	1,416社	266社 ７機関	41社	46社	14社 1団体	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 ９機関 （日本病院団体協議会の加盟団体にも参加依頼中）	8水道事業体	6団体 17社	13社	51社	12社
2014年4月時点	27社 1団体	250社 1団体	194社 1団体	1,411社	251社 ７機関	43社	30社（オブザーバ３社含む）	2ｸﾞﾙｰﾌﾟ 3機関	22社 1団体 1機関	12社 2機関	10社・団体	47 都道府県 1,742 市区町村	1グループ ２機関	8水道事業体	6団体 16社	―	―	―
NISCからの情報の展開先（構成員以外）	406社・団体	406社	12社	3社・団体	―	―	―	―	―	13社・機関	153社・団体	―	381社	内容に応じ1,359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（内容に応じ展開先を選定）、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））																	
事務局の民間移行	2018年3月　医療分野（厚生労働省医政局 →　（公社）日本医師会）																	
その他	空港について2018年4月1日以降取組を開始。																	

■　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を設立、2017年４月より運用開始）、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）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報WAISE（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

2017 年度分野横断的演習　開催概要

＜事前説明会＞
日　程　：２０１７年１０月１６日（月）、１０月１８日（水）、１９日（木）
場　所　：東京会場、大阪会場、福岡会場（説明会の模様について、演習当日まで動画配信）
内　容　：①分野横断的演習の背景説明（第４次行動計画、情報共有体制）
②分野横断的演習の事前説明
③最新動向等についての有識者講演　等

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：２０１７年１２月１３日（水）１２：３０～１７：００
場　所：東京会場、大阪会場、福岡会場、自職場
参 加 者：２，６４７名
【重要インフラ事業者等：１３分野】
【セプター：１３分野１８セプター】
【政府機関　等】
演習内容：
○第１部　各分野においてサービスへの影響が小さい重要インフラサービス障害が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証。（ランサムウェアによる攻撃）
○第２部　サービスへ影響が生じる重要インフラサービス障害が発生し、事業継続が脅かされる事態を想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。（ＤＤｏＳ攻撃、ネットワーク機器のマルウェア感染、制御システムのマルウェア感染）

演習の模様

鈴木大臣による挨拶

演習を通じた内規・体制等の課題抽出

＜意見交換会＞
日　時：２０１８年１月２４日（水）１４：００～１７：３０
場　所：東京会場、大阪会場、福岡会場
内　容：①組織間での情報交換（テーマに応じたグループディスカッション）
②最新動向等についての有識者講演　等

他事業者等との情報共有を通じた改善の促進

2017 年度における取組実績（概要）

事前準備

<参加募集>
- ✓ 事業者の参加拡大（初参加者の会場枠の確保）

<シナリオ作成>
- ✓ 最新動向の把握、シナリオのレビュー

<事前説明会>
- ✓ サブコントローラーへの説明充実
  （サブシナリオ作成事例、プレイヤーに期待される行動例の提示）

<演習参加者の理解の増進>
- ✓ テキストブックの作成（分野横断的演習の全体像、グッドプラクティスの提示）

演習当日

<演習当日の取組み>
- ✓ 演習シナリオのより一層の充実による実践的な演習
- ✓ 情報伝達の有効性の検証（事業者間における情報の横連携）
- ✓ セプター事務局、所管省庁の課題設定（情報提供・連絡・共有に関する課題設定）
- ✓ 国際対応（海外機関に対する演習視察機会の提供）
- ✓ 他組織（金融ISAC、日本シーサート協議会）との相互連携

事後の振返り

<振返りシートおよびアンケート分析>
- ✓ ２０１７年度の新たな取組への評価（情報の横連携、テキストブック、プレイヤーの行動評価）
- ✓ 演習運営全般への評価（演習環境、状況付与のタイミング）

<意見交換会>
- ✓ 東京、大阪、福岡会場において開催（福岡会場は今年度より実施）

2018 年度に向けた取組

➢ 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
- ◻ 実環境に即したサブシナリオの検討
  （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次行動計画に基く情報共有体制に関する理解の増進

➢ 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)やるべきことをキチンと実行するためのきっかけづくりとなる」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

別添４－９　セプター訓練

セプター訓練（第 12 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、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18セプター、2,106者

＜実施期間＞

2017年7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 12 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、昨年度を上回る2,106者が訓練に参加

２．実施結果及び訓練により得られた気づき等

✓ 昨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96%→94%）
- 5セプターで昨年度より受信確認割合が低下（訓練参加者大幅増によるものを含む）
- 一方、昨年度受信確認割合が100%だった12セプターは引き続き100%を維持

✓ 前回（第11回）のセプター訓練で得られた気付き・課題等への対策の有効性を確認
- 主たる担当の不在時等も想定した確実な情報共有体制の構築が有効に機能
- 情報共有ルールの理解を深めるための対策（セプターから事業者への説明実施、連絡フォーマットの準備等）が有効であることを検証

✓ 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

別添４－10　補完調査

補完調査とは

補完調査の目的

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とら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

補完調査として、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（ヒアリング等）を行い、調査結果については、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、事例の概要・原因とともに、得られた気付き・教訓等をとりまとめ、公表するものです。

調査対象

調査対象は、実際に発生した重要インフラサービス障害等について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさ、及び得られる気付き・教訓の有用性等を考慮して、以下の事例を選定しました。

事例１　WannaCryによるサイバー攻撃
事例２　認証の脆弱なIoT機器への第三者アクセス
事例３　コインマイナー
事例４　SNSアカウント乗っ取り
事例５　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃
事例６　送信元詐称メールに対する備え
事例７　DDoS攻撃
事例８　リスト型の不正ログイン攻撃
事例９　SQLインジェクションによる個人情報流出

事例１　WannaCry によるサイバー攻撃

【事例の概要】

- シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいたが、該当するファイルは開くことができなかった。
- 保守ベンダにて、ファイルサーバのLANケーブルを抜線してネットワークから隔離し、ファイルサーバがランサムウェアに感染していることをウイルス対策ソフトにて確認した。
- ランサムウェア感染していると考えられるファイルをすべて消去し、バックアップデータから復元した。
- 再度、感染がないことを確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。

【１　背景】

- 業務都合上、シンクライアント端末上でUSBメモリを利用していたが、許可されたUSBメモリのみ使用可としていた。
- インターネットからダウンロードするものは全てウイルスチェックを徹底していた。
- シンクライアント端末は環境復元ソフトが入っており、再起動の度に設定された状態に復元される仕様になっていた。

【２　検知】

- シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいた。
- 関係省庁から、WannaCryに関する注意喚起があり、内容が酷似していることを確認した。

【３　対処】

- ファイルが開けない状態であったため、上司に報告し、システム担当が保守ベンダに対処を依頼した。
- 保守ベンダがランサムウェアの感染を確認し、インターネット接続用のLANケーブルを抜線した。さらにファイルサーバ内の感染していると考えられるファイルを削除した。
- 保守ベンダにより、システム担当が事前に取得し、ローカルに保存していたバックアップデータから、ファイルを復元した。
- 再度感染がないか確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。
- 状況を上司に報告し、関係省庁等と連携をとった。

【４　原因】

- 感染原因は特定できておらず、おそらくUSBメモリ経由ではないかと思われる。

【５　再発に備えた対策】

- シンクライアント端末は、環境復元ソフトにより、セキュリティアップデートも無効化されてしまうため、セキュリティアップデートが有効化されるよう検討した。
- USBメモリの使用方法に関しては、再度周知徹底を行った。
- ローカルへのバックアップの定期的な取得を検討した。
- システム担当の一時対応強化のため、外部のセキュリティ研修に参加した。

【６　得られた気付き・教訓】

- **重要データの定期的なバックアップ取得**
  システム担当者が定期的にバックアップを取得していたため、復号できないファイルに対しても、バックアップデータから復元することができた。ランサムウェア対策においては、定期的なバックアップを取ることが重要である。
- **関係省庁・団体との情報共有**
  今回の初動対応時、ウイルス対策ソフトでは感染が検知できない状況ではあったが、情報提供を受けていた内容と酷似していたことから状況を把握できたものであり、日頃からシステム担当者まで情報共有されていたことが役立った。

事例２　認証の脆弱な IoT 機器への第三者アクセス

【事例の概要】

- 水圧監視用のIoT機器（以下、水圧センサ）数十台が、インターネット経由で第三者が容易にログインでき、監視情報を閲覧できる状態になっていることが、外部からの指摘により発覚した。
- 水圧センサに内蔵された監視用Webの認証が不要又はマニュアルから入手できるID/初期パスワードが使われており、接続可能なIPアドレスや端末も制限されていなかった。
- 情報セキュリティ担当とIoT機器所管の事業部門（水道設備部門）で連携して設置場所を特定し、機器設置業者の協力の下、対象の全てのIoT機器のパスワードを複雑なものに変更した。

【１　背景】

- 水道施設の水圧監視のため、水圧データを閲覧できる簡易Webサーバ機能（パスワード認証）を持つIoT機器（水圧センサ）を水道施設 約20か所に設置した。
- 導入は、各種設定の検討も含め、機器設置業者に委託していた。
- 当該IoT機器以外にも水圧監視の手段を有していた。

【２　検知】

- 事業者の情報セキュリティ担当が、第三者から、「脆弱なIoT機器を発見した」との連絡があり、対象の機器のIPアドレス、大まかな地理情報、問題点等を受領した。

【３　対処】

- 情報セキュリティ担当にて、受領したIPアドレスが割り当てられた機器の所管の事業部門を特定するため、調査を開始した。IoTデバイスは資産管理台帳の対象に含めていなかったため難航したが、最終的に水圧センサであることを特定し、事業部門（水道設備部門）に連絡した。
- 水道設備部門から機器設置業者に対して、該当機器のパスワードを複雑なものに変更するよう指示した。
- 機器設置業者にて、全ての水圧センサのパスワードを複雑なものに変更した。また、水圧センサの不正操作の痕跡、機微情報の漏えい、他の設定不備及び水圧の制御システムへの影響がないことも確認した。
- 情報セキュリティ担当にて、他の事業部門に対して、IoT機器が脆弱な状態で運用されていないか、確認を依頼した。結果、他に問題のある機器は発見されなかった。

【４　原因】

- 事業部門及び機器設置業者において、IoT機器のセキュリティ対策の必要性の認識が浅く、認証の設定についても導入時の検討事項に挙がらず、初期パスワードのまま導入されていた。
- 業務上、モバイル端末でのアクセスが必要であるため、インターネット経由でアクセスできる環境に水圧センサを接続していたが、水圧センサ及びルータへのアクセス元のIPアドレスや端末の制限は行っておらず、誰でもアクセス可能な状態で稼働していた。

【５　再発に備えた対策】

- IoT機器の設置に関して、資産管理やセキュリティ対策のルールを策定し、事業部門及び機器設置業者に展開した。

【６　得られた気付き・教訓】

- **IoT機器の管理とセキュリティ対策のルール化**
  IoT機器は、組織によっては事業部門が導入し、情報システム部門の管理外であるケースもあり、資産管理方法やセキュリティ対策、有事の際の対応について、双方協議の上、ルール化することが望ましい。
- **セキュリティ対策機能を備えたIoT機器の選定**
  IoT機器を選定する際、セキュリティ対策機能についても仕様を調べ、IoT機器で扱う情報や用途に相応であるかを確認すると良い。
- **IoT機器のセキュリティ対策についての当事者意識**
  IoT機器への被害が進行すると、ボット化して外部への攻撃に使用されるおそれもあるため、セキュリティ対策は事業者がその必要性を理解して要件を定めることが望ましい。また、ベンダに導入を委託する場合も、どのような対策が必要かを事業者自身が理解し、チェックすると良い。

事例３　コインマイナー

【事例の概要】

- 攻撃者は、アプリケーションサーバ（APサーバ）の脆弱性をつき、仮想通貨をマイニングする不正なプログラムを埋め込み、マイニングさせた（結果は通信遮断により、攻撃者に届かず）。
- 大量のトラフィック（UDPパケット）の発生により、利用者がサービスにアクセスしづらいなどの影響が発生した。
- 大量のトラフィックの発生をネットワーク監視により検知し、調査後、本事案が発覚した。
- APサーバの脆弱性対応を行った上で、不正プログラムを削除し、検知する仕組みを導入した。

【１　背景】

- CSIRT部門は、関係機関等を通じて、日々脆弱性情報等を収集し、サーバに保有する情報の重要度に応じて対策を行っていた。
- CSIRT部門からシステム部門に対して脆弱性対策を指示していたが、長期間対応を行っていなかった。

【２　検知】

- ネットワーク監視により、海外のIPアドレスへの大量トラフィック（UDPパケット）を検知（通常の３倍程度まで徐々に増大。CPU負荷も上昇）。

【３　対処】

- システム部門は、脆弱性対応を行った上、不正プログラムを削除した（任意のコード実行が可能な状態であり、他のサイバー攻撃を受けるおそれがあったが、コインマイニング以外の形跡がないことを確認した）。
- 不正プログラム（cronの改ざん）を検知する仕組みを導入した。
- インシデント内容について、関係機関と情報共有を行った。

【４　原因】

- 任意のコード実行が可能な緊急度の高い脆弱性を突かれ、不正プログラムを埋め込まれた。
- 過度にCPU負荷を与えないようなマイニングにより、検知するまでに時間を要した。

【５　再発に備えた対策】

- 事業者内で、脆弱性情報の重要度・緊急度の認識を統一し、CSIRT部門は、システム部門から定期的に対応状況の報告を受けることとした。
- 任意のコード実行が可能な脆弱性等が、マイニングに利用されたため、脆弱性対応に漏れがないよう、情報システムの構成管理方法を検討した。

【６　得られた気付き・教訓】

仮想通貨のマイニングを目的とした攻撃が増加しており、HPへのアクセスが困難になるなど、サービス提供に影響が発生するおそれがあることから、攻撃手法を認識し、事前に対策をとることが重要である。

- **コインマイニングの早期検知**

  ①　コインマイニングの検知に時間を要したことから、トラフィック量やCPU使用率（特に、Webサーバ等の権限によるプロセス起動）の上昇などシステム監視を徹底する。

  ②　さらに、システム監視では検知できない場合、不正な外部通信（マイニング結果の送信）や改ざん（cronの改ざん）を検知することが効果的である。

- **コインマイニングに関する情報共有**

  攻撃元IPアドレス等に加え、コインマイナー特有の情報（ウォレットアドレス、仮想通貨名等）の共有を行い、対策に活用することが重要である。

事例４　SNS アカウント乗っ取り（1/2）

【事例の概要】

- 海外へのPRのため、５年以上前から海外の短文投稿サイトを使用して情報発信を実施していた。
- 短文投稿サイト(SNS)のアカウントが乗っ取られ、パスワードが変更されるとともに、過去の投稿がほとんど削除され、政治的な発言が投稿された。
- SNS運営会社を通じてパスワードをリセットするとともに、SNSアカウント管理について見直し、周知を行った。

【１　背景】

- 事業者は、海外へのPRを積極的に行うために、海外の短文投稿サイト(SNS)にアカウントを作成し、定期的に情報を発信していた。
- 事業者は、SNS担当者として現地出身の人を1年ごとに雇用し、現地文化を踏まえた表現を用いて、現地の言葉で発信していた。フォロワー数は順調に伸びており、クレーム等は発生していなかった。

【２　検知】

- SNS担当者が情報発信しようとしたところ、短文投稿サイトのログインができないことから本事案が判明した。
- 攻撃者にパスワードが変更されていたこと、及び本人認証コードの送信先が退職した前任者の携帯電話となっていたことから、パスワードリセットも不可であった。
- 投稿内容を見ると、ほとんどの投稿が削除されており、政治的な発言が投稿されていた。

【３　対処】

- 短文投稿サイトのSNS運営会社に連絡し、本人確認後、パスワードリセットが認められた。しかし、これ以上の対応(過去の投稿の復元、ログの解析や提供)はできないとの回答があった。

  ※やり取りはすべて現地の言葉で行われた

- 短文投稿サイトは、アカウントを退会(削除)できない仕様となっていたため、投稿内容及び登録していた画像をすべて削除した。
- 警察とも相談して対応したが、過去の投稿が削除されているため、被害を証明することが難しいことに加え、SNS運営会社が日本にはないため、対応が難しい案件となった。
- SNS運営会社の日本の代理店を通じて、有料の公式アカウントを申請した。新しいアカウントができ次第、新アカウントへ旧ユーザーを誘導する予定。

【４　原因】

- 攻撃者がID/パスワードの認証を突破し、短文投稿サイトのアカウントを乗っ取ったものと思われる。

【５　再発に備えた対策】

- ２段階認証を有効化し、不審なログイン試行(通常と異なる環境からのログインや連続パスワード試行等)が発生した際に、認証コードを入力させるようにする。
- 担当者の異動等によりアカウントを引き継ぐ際には、
  ・ログインパスワードの変更
  ・2段階認証に用いるメールアドレス(携帯電話番号等)の変更
  を確実に実施する。

事例４　SNS アカウント乗っ取り（2/2）

【6 得られた気付き・教訓】

・SNSアカウントの管理における対策

①不正アクセスの検知（2段階認証/不審なログインへのアラート設定）

不審なログイン試行が発生した際に、普段利用しているものとは異なる端末や環境からのログイン試行に早期に気付けるようにするため、あらかじめ登録した通知先にアラートを送信するように設定しておく。また、SNS担当者の異動の際は、２段階認証に用いるメールアドレス及び携帯電話番号の変更を着実に実施する必要がある。

②公式アカウントの作成における有料アカウントの検討

一般アカウントと有料アカウントでは、公式マークの表示や提供される機能など、サービス内容も異なる。リスクと得られるメリットを検討し、状況によっては有料アカウントも検討すると良い。

・SNSへのコンテンツ投稿における留意事項

①標的となるリスクの軽減

目的、発信方針(内容・表現)等を定めたソーシャルメディアポリシー(※)を策定し、SNS担当者と理解を共有しておくと良い。特に、海外の利用者を対象として情報発信する場合は、今回のように現地の文化的・政治的な背景をよく理解した上で、内容・表現に留意して発信することが望ましい。

※参考例　NISC　SNS運用ポリシー(https://www.nisc.go.jp/security-site/SNSpolicy.html)

②投稿コンテンツのバックアップ

SNSで発信される情報は、その手軽さや重要度の低さなどからバックアップの考慮対象外となることが多い。しかし、投稿コンテンツが削除されてしまった場合、SNS運営会社側でも復元対応が困難なケースがある。被害の証明や復元のために、投稿内容のバックアップを取っておくと良い。

事例５　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃

【事例の概要】

- 保守ベンダから、マルウェアに感染したフリーソフトウェアに由来する不正通信が検出されたとの報告があった。
- システム担当が導入していた端末運用管理ソフトウェアにより、フリーソフトウェアをインストールした端末を特定し、早急に端末をネットワーク（インターネットに接続）から切り離した。
- 不正通信は、正規のフリーソフトウェアに埋め込まれたマルウェアによるものであり、フリーソフトウェアを利用していた感染端末以外からの不正通信等はないことを確認した。

【１　背景】

- インターネット接続用にファイアウォールを構築していた。
- 端末へのソフトウェアのインストールは許可制(要申請)になっており、その旨は定期的な研修等で伝えていた。

【２　検知】

- 所管省庁から、広く利用されているフリーソフトウェアのマルウェア感染の可能性について注意喚起があった。
- 保守ベンダからシステム担当に対して、不正通信を行っている端末があることが報告された。

【３　対処】

- システム担当が端末運用管理ソフトウェアを利用し、当該ソフトウェアを使用している端末を探り当て、当該端末がマルウェアに感染して不正通信が行われていたことを確認した。
- ネットワークケーブルの抜線により、不正通信が停止したことを確認した。
- 保守ベンダに調査を依頼し、感染端末以外から不正通信が行われていないことを確認した。
- 状況を上司に報告し、関係省庁等と連携をとった。
- 保守ベンダの調査報告後に、該当端末のOSの再インストールを実施した。

【４　原因】

- 信頼できると考えられるフリーソフトウェアの正規インストーラにマルウェアが埋め込まれていた。
- 許可を取らずにフリーソフトウェアをインストールした。
  ※ただし、今回の場合は申請しても許可されていた可能性あり

【５　再発に備えた対策】

サプライチェーン攻撃に対して、決定的な対策を取ることは困難ではあるが、効果があるものと考え、以下の対策を実施した。

- インストールするソフトウェアの管理・把握を強化した。
- マルウェア感染事例として注意喚起を実施した。
- 全従業員向けに研修を実施し、セキュリティ意識の高揚を図った。
- サイバー攻撃に起因した事業継続計画（ICT-BCP）が策定されていないため、策定を検討した。

【６　得られた気付き・教訓】

- **資産管理の重要性（端末運用管理ソフトウェアの導入等）**
  本事案では、ファイアウォールを導入していたが、セキュリティポリシーが適用される前は不正通信が行われていた。感染端末の検索や許可されていないソフトウェアの検索のために、端末運用管理ソフトウェアを導入していたことが感染端末の早期発見に役立った。
- **ネットワーク監視の重要性**
  保守ベンダが早期に不正通信を検出したことが、本事案での被害抑止につながった。平時から、事業者内の端末からの通信を監視しておくことで、サプライチェーン攻撃のような予期せぬ感染の拡大防止に役立つと考えられる。
- **保守ベンダとの日常的な情報交換の大切さ**
  保守ベンダと良好な関係が構築できていたため、対応を必要とする情報が得られ、対応などについての相談もできたため、早期に原状回復することができた。

事例６　送信元詐称メールに対する備え

【事例の概要】

- 近年、知名度の高い事業者名を使用した不審メールが出回る事例が多く、送信元を詐称された事業者はどのような対応を行っているのか好事例を調査した。
- 送信元詐称メールの情報は、複数のチャネルから寄せられていた。
- 情報はインシデント対応部門に集約され、迅速な対応がなされていた。

【１　背景】

- 知名度の高い金融機関や物流事業者、テーマパーク等の事業者名を送信元に詐称する不審メールが増えている。
- 特に、重要インフラ事業者は、顧客からの信頼も厚いため、攻撃者に社名が利用されやすいと考えられる。
- 利用者からの信頼を維持するために、どのような対応が望ましいのか好事例を調査した。

【２　検知】

- 送信元詐称メールを認知する経路は、複数のチャネルにわたっていた。具体的には、利用者からの問合せ(コールセンター)、SNSによる投稿、セキュリティ関係機関やセキュリティベンダーからの報告、同業他社からの連絡等により、本事案を把握した。
- 大規模なものだと、コールセンターへの問合せ量が通常時の15倍近くになることもあった。

【３　対処】

- 複数の検知経路から受領した情報について、最終的にはインシデント対応部門に集約していた。
- インシデント対応部門は、HPに迷惑メールの文面等を掲載して注意喚起を行い、さらにコールセンターへの情報提供及び対応の指示を行うなど、対応を迅速に行うための連絡ルートを確立していた。

【４　得られた気付き・教訓】

- **巧妙に詐称されたメール文面やWebページの特徴**
  送信元詐称メールの文面は、普段事業者が定型的に送信する文章がほぼそのまま利用されているケースが多い。また、リンク先のURLについても、実際のWebページを模倣しているものもあるため、気付きにくい。
  しかし、事業者が送信するメールはテキスト形式であったが、送信元詐称メールはURLを隠すためHTMLメールになっていたり、ファイルが添付されていたり、ショートメッセージサービス(SMS)を利用していたりするなど、多少異なる点があった。
- **どの事業者にも存在するリスク**
  Webシステム等を堅牢に構築していたとしても、攻撃者が送信元を詐称してばらまくメールは防ぎようがない。そのため、どの事業者にも発生しうるインシデントであると言える。
  利用者からの信頼を失わないためにも、このようなリスクがあることを認識して対応できるよう、情報収集・情報集約・周知に関する連絡ルートを確認しておく必要がある。
- **顧客への注意喚起方法**

①広報方法
詐称メールへの注意を促すために、自社のHPは良い広報ツールとなる。トップページのお知らせ欄や、アクセス数が多いページの上部等に表示することが効果的である。

②広報内容
不審メールの文面が入手できる場合は、その文面をHP等に掲載すると効果的である(ただし、個人情報を掲載しないように注意する必要がある)。

事例７　DDoS 攻撃

【事例の概要】

- DDoS攻撃の数日前から、HPへの軽微なDoS攻撃が行われていた（攻撃者による偵察の可能性あり）。
- その後、匿名の脅迫メールを受信し、ほぼ同時に海外からのDDoS攻撃が発生し、HPにアクセスしづらくなった。（同日中に複数回（グループ会社にも攻撃）、数日後にもDDoS攻撃が発生した）
- 当該HPの代替用サイトを開設するとともに、Webサーバの移設等を行い、影響を緩和した。
- HPにアクセスしづらくなっている事象について、メールやSNSにより顧客に周知した。

【１　背景】

- 事業者は、メインとなるサービスをHPで提供しており、当該サービスを継続的に提供することが最も重要であると位置づけていた。
- DDoS攻撃が発生する数日前から、HPへの軽微なDoS攻撃が行われていた(攻撃者による偵察の可能性あり)。また、関係機関からも同様の情報を得ていた。

【２　検知】

- 匿名の脅迫メールを受信し(DDoS攻撃解除のためにビットコインを要求するもの)、ほぼ同時に、海外からのDDoS攻撃が発生し、HPへアクセスがしづらくなった。
  ※同日中に複数回（グループ会社にも攻撃）、数日後にもDDoS攻撃が発生した。
- 脅迫メールの受信とほぼ同時にDDoS攻撃が行われたため、攻撃を事前に気づくことはできなかった。

【３　対処】

- 代替用サイトを開設するとともに、攻撃対象となったグループのWebサイトのサーバー分離等の対応を行った。
- 顧客対応については、HPで対応することができなかったため、メール及びSNSにより顧客に周知した。

【４　原因】

- 事業者は、これまでDDoS攻撃を受けたことがなく、特段の技術的対策や対応マニュアル等が整備されていなかった。

【５　再発に備えた対策】

- 早期検知や未然防止の観点から、クラウド型のDDoS攻撃対策サービスを速やかに導入した。
- 不審メールの受信時やサイバー攻撃を受けた際における情報連絡体制を整備した。
- DDoS攻撃等のサイバー攻撃を踏まえたBCPを策定し、業務継続体制を構築することを検討した。

【６　得られた気付き・教訓】

- **事業継続計画(BCP)の整備**

  DDoS攻撃への技術的な対策の準備がない場合は、即時対応が困難であるため、サービスの継続性が求められるものは、技術的対策やBCPを検討しておくことが重要（本事案では、代替用サイトを開設した）。

- **連絡体制の整備**

  同時多発的にサイバー攻撃が行われる可能性があることから、自社だけではなくグループ会社やサプライヤーなど内外の関係者を含めた複数の連絡体制の備えが重要である。

- **事後の検討**

  目的を達成するまで執拗なサイバー攻撃が行われる可能性があることから、復旧をもって対応を完了するのではなく、事後に攻撃内容を検証し、対策を検討することが重要である。

事例８　リスト型の不正ログイン攻撃

【事例の概要】

- 事業者が運営している会員サイトに、ログインエラーが急増した。
- 保守ベンダがWAFを用いて、攻撃元のIPアドレスからの通信を遮断した。
- 攻撃者が別のIPアドレスから攻撃を行うことによって、サービスへの影響が出ることを懸念し、会員サイトを一時閉鎖した。
- 攻撃があった時間帯にログインのあったユーザに対して、パスワードを強制変更した。

【１　背景】

- 会員サイトのセキュリティ対策として、WAF (Web Application Firewall)を構築していた。
- 会員サイトへのログインにはID/パスワードが必要であり、同一IDによるログイン試行が複数回失敗した場合、一定時間アクセスができなくなる設定としていた。

【２　検知】

- WAFにより、会員サイトへのログイン試行が増えていることを検知し、保守ベンダが攻撃元IPアドレスからの通信を遮断した後、事業者に報告した。
- ログの状況から、第三者によるリスト型攻撃と判断した。(数件の不正ログインが成功した形跡があり、氏名やメールアドレス等の情報が盗み見られた可能性がある)

【３　対処】

- 保守ベンダが、大量のログイン試行を行ったIPアドレスを特定し、WAFにて当該IPアドレスからの通信を遮断した。
- 上司に相談し、攻撃者が別のIPアドレスから攻撃するおそれがあったため、会員サイトを一時閉鎖した。
- 攻撃時間帯にログインのあったユーザのパスワードを強制変更した。
- パスワードを強制変更したIDのユーザに対して、メールや電話等により、パスワードの変更を通知した上で、会員サイトを再開した。

【４　原因】

- WAFによる不正ログインの検知は行っていたが、自動遮断機能は設定していなかった。
- ユーザが他サイトと同じパスワードを利用していた。

【５　再発に備えた対策】

- 大量のログイン試行による攻撃を検知した際、WAFにて自動的にアクセスを遮断する設定を行った。
- 他サイトと同じパスワードを利用しないこと、パスワードを定期的に変更することをユーザに周知（メール、ログイン画面）した。

【６　得られた気付き・教訓】

- **システムログの分析**
  システムログの傾向分析を定期的に実施することで、平常時とは異なる状況にいち早く気づくことが大切である。また、分析した結果を踏まえ、WAFの自動遮断設定に生かすことが可能となる。
- **サイバー攻撃を考慮したサービスの継続や停止の判断の明確化**
  意思決定するためのルール（サービス継続・停止判断基準）を明確化・明示しておくことで、いざという時の判断や対応を迅速に行うことが可能となる。
- **ユーザへの継続的な注意喚起**
  他サイトと同じパスワードを利用しない等、ユーザに注意喚起し続けることが重要である。

事例９　SQL インジェクションによる個人情報流出

【事例の概要】

- 業務部門は、個人情報を含むHPのコンテンツのサービス終了に伴い、管理しなくなった。
- 攻撃者は、SQLインジェクションにより、サービス終了済みで管理していないHPから顧客情報を取得した。
- HPの高負荷状態の検知により、本事案が発覚した。さらにセキュリティベンダーの調査により、過去の類似の事案も発覚した。
- 攻撃対象となった不要なHPを削除し、不正アクセスの検知機能を強化した。

【１　背景】

- 業務部門は、個人情報を含むHPのコンテンツを管理していたが、システム部門で一括管理することとなった。
- 一部のサービス終了済みHPのコンテンツは、業務部門からシステム部門に引き継がれないまま、管理されない状態となっていた。
- システム部門で管理しているHP等については、脆弱性アセスメントやペネトレ―ションテスト等を実施し、適切に対応していた。

【２　検知】

- HPの高負荷状態を検知し、SQLインジェクションによる顧客情報の漏えいが発覚した。
- セキュリティベンダーの調査により、過去にもSQLインジェクションによって顧客情報が漏えいしていたことも発覚した。

【３　対処】

- 攻撃対象となった、管理していない不要なHPを削除した。
- SQLインジェクション等の不正アクセスの検知機能を強化した。

【４　原因】

- 攻撃対象となったHPは、既に存在自体が認識されておらず、管理や対策が行われていなかった。
- 資産管理台帳が整備されていないことから、担当者がコンテンツを作成・削除・更新した場合に、管理者が認識できる仕組みになっておらず、オリジナルデータのコピー等も複数箇所に散在していた。

【５　再発に備えた対策】

- 業務部門の情報資産管理が不十分であったため、システム部門は、必要な情報資産以外を削除し、Webサーバを再構築した。
- 検知機能の強化の観点から、導入が容易なWAFのクラウドサービスの利用を開始した。
- 情報共有強化の観点から、経営層が関与するリスク管理委員会を設置した。
- 対策の実効性の観点から、各種関連規程・マニュアルを策定した。

【６　得られた気付き・教訓】

- **情報資産管理の徹底**

  情報資産を洗い出した上で、管理台帳への登録を適切に行い、情報資産を網羅的に管理・対策することが重要である。（特に、使用しなくなった情報資産を放置しないことが重要）

- **SQLインジェクション等の未然防止**

  脆弱性アセスメント等の結果を踏まえ、攻撃対象とならないよう、セキュアプログラミングによる安全なウェブサイトを作ることが重要である。（ただし、認識していない情報資産がある場合は、脆弱性が残存している可能性があるため、注意が必要）

別添５　用語解説

	用　　語	解　　説
A	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。
	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、2017年３月末現在、13分野で18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。
	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。
	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	DDE機能	DDEはDynamic Data Exchangeの略。Microsoft Officeの機能の一つであり、officeファイル間でデータを動的に取得するため、例えば、Wordファイル内でExcelファイルを参照している場合、Excelファイルに変更があればWordファイル内にも反映される。
	DDoS攻撃	Distributed Denial of Serviceの略。分散型サービス不能攻撃。大量のコンピュータが一斉に特定のサーバにデータを送出し、通信路やサーバの処理能力をあふれさせて機能を停止させてしまうサイバー攻撃。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。
	DoublePulsar	Microsoft Windowsの脆弱性を利用するバックドアツール。「WannaCry」をコンピュータに感染させるためのバックドアとして利用された。
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。
	EternalBlue	Microsoft Windowsの脆弱性を利用する攻撃ツール。Server Message Block1.0（SMBv1）サーバが特定のリクエストを処理する際のセキュリティ上の欠陥を利用するものであり、攻撃者は任意のコードを実行できる。
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/G8	Group of Seven（主要７か国首脳会議）、Group of Eight（主要８か国首脳会議）の略。
	GSOC	Government Security Operation Coordination teamの略（ジーソック）。政府機関情報セキュリティ横断監視・即応調整チーム。政府機関等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、各政府機関への助言、各政府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。内閣官房内閣サイバーセキュリティセンターにおいて、2008年４月から運用開始。 近年のサイバー攻撃の複雑・巧妙化を踏まえ、2017年４月に運用開始した第３期GSOCでは、検知・解析機能の強化、センサーの増強等を図っている。また、2017年４月からは、独立行政法人等に対する監視体制（第二GSOC）の運用を開始し、従前からの政府機関に対する監視体制（第一GSOC）と連携を図り、監視体制を強化している。
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。従来のパソコン、サーバ、携帯電話、スマートフォンのほか、ICタグ、ユビキタス、組込システム、各種センサーや送受信装置等が相互に情報をやり取りできるようになり、新たなネットワーク社会が実現すると期待されている。
	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。
	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。
	ISP	Internet Service Providerの略。インターネット接続事業者。
	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。
	ISO/IEC JTC1 SC27/WG4	セキュリティコントロールとサービスの分野を対象に、国際規格を策定するISO/IEC JTC1 SC27配下の作業グループ。
	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-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る用語で、「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。
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。
	Meltdown/Spectre	Googleのセキュリティチームが公開した、処理性能を向上させる仕組みを悪用するCPUの脆弱性。
	memcached	分散型メモリキャッシュシステム。データベースへの問い合わせ結果を一時的にキャッシュすることで、データベースへのアクセス回数を減らし、ウェブアプリケーションの高速化等を行う。
	MOU/NDA	Memorandum Of Understanding/Non-Disclosure Agreementの略。覚書及び秘密保持契約。
	MyJVN	JVNiPedia で配布されている脆弱性チェックツール。PCのソフトウェアが最新か、セキュリティ設定に問題がないか等を確認し、対策が必要な場合は情報へのリンクを提供する。
N	NCFTA	National Cyber-Forensics and Training Allianceの略。FBI、民間企業、学術機関を構成員として米国に設立された米国の非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。
	NICT	National Institute of Information and Communications Technologyの略。国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を実施するとともに、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。
	NONSTOP	NICTER Open Network SecurityTest-Out Platformの略。NICTER（NICTが開発するインターネットで発生する様々なセキュリティ上の脅威を迅速に把握し、有効な対策を導出するための複合的なシステム。）が保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤。
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 CTF2017	SECCON CTF：SECurity CONtest Capture The Flag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。競技を通じた実践的情報セキュリティ人材の発掘・育成、技術実践の場の提供を目的とする。
	SIP	cross-ministerial Strategic Innovation promotion Programの略。戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS	Social Networking Serviceの略。社会的ネットワークをインターネット上で構築するサービスのこと。友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、「友人の友人」といったつながりを通じて新たな人間関係を構築したりする場を提供する。
	SOC	Security Operation Centerの略。セキュリティ・サービス及びセキュリティ監視を提供するセンター。
	Society5.0	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。
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。
	WPA2	Wi－Fi Protected Access 2の略であり、無線LANの通信規格の一つ。暗号化にAESを採用しており、WEP、WPAといった無線LANの規格よりも安全性が高い。
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。
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。
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。
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月間	サイバーセキュリティについて国民に広く普及啓発するため、2009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（「サイバーの日」）までに期間を拡大したもの。月間の期間中、サイバーセキュリティについて、「知る・守る・続ける」をキャッチフレーズに、普及啓発に関する行事や関連キャンペーン等を行っている。
	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。
	サイバーセキュリティ国際キャンペーン	2012年より毎年10月にサイバーセキュリティ国際キャンペーンを実施し、アジア、欧米をはじめとする諸国と国際連携を活用した行事やサイバーセキュリティ対策に関する情報提供を実施し、国際連携の推進と国内におけるサイバーセキュリティ対策の一層の普及を図っている。
	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（2015年戦略）	2015年９月４日、閣議決定。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、2020年代初頭までの将来を見据えつつ、今後３年程度の基本的な施策の方向性を示したもの。2015年１月にサイバーセキュリティ基本法が全面施行されたことに伴い、新たな法的枠組みに基づき策定された。
	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。
	サイバー犯罪条約	サイバー犯罪に関しての対応を取り決めた国際条約。通称ブダペスト条約。日本においては2012年11月に効力が発生した。
	サイバーフォースセンター	サイバー攻撃対策の技術的基盤として、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	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。
し	事業継続計画	BCPを参照。
	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	重要インフラの情報セキュリティ対策に係る第４次行動計画において新設した用語。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３次行動計画及び同第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10日情報セキュリティ政策会議決定。2015年５月25日サイバーセキュリティ戦略本部改訂。重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画。
	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。
	重要インフラ分野	情報通信、金融、航空、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次行動計画において記載。
	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３次行動計画及び同第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３次行動計画 及び同第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
	情報セキュリティ研究開発戦略	2011年７月８日情報セキュリティ政策会議決定、2014年７月10日情報セキュリティ政策会議改定。

	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。
	情報セキュリティ普及啓発プログラム	今後推進すべき新たな普及啓発の進め方についてまとめたプログラム。2011年７月８日情報セキュリティ政策会議決定。改定版である新・情報セキュリティ普及啓発プログラムは2014年７月10日情報セキュリティ政策会議改定。
す	数式エディタ	コンピュータ上で数式を組み付けて表示するためのソフトウェア。
	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。
	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	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	国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態。
て	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	技術や機器の検証・評価のための実証実験、又はそれを行う実験機器や条件整備された環境のこと。
	電子署名	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」、「政府機関の情報セキュリティ対策のための統一基準」（2016年８月31日サイバーセキュリティ戦略本部決定）及び「府省庁対策基準策定のためのガイドライン」（2016年８月31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。
	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EU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ＥＵ両政府による包括対話。（第１回：2014年10月、第２回：2017年１月、第３回：2018年３月）
	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）
は	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
	バックドア	外部からコンピュータに侵入しやすいように、“裏口”を開ける行為やその裏口のこと。バックドアがしかけられてしまうと、インターネットからコンピュータを操作されてしまうなどの可能性がある。
ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	秘密分散メカニズム（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。
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	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。
り	リスクマネジメント	リスクを組織的に管理し、損失などの回避・低減等を図るプロセスのこと。
	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。

（本ページは白紙です。）