資料１

サイバーセキュリティ政策に係る年次報告（2016 年度）（案）

資料１－１　サイバーセキュリティ政策に係る年次報告（2016 年度）（案）の概要

資料１－２　サイバーセキュリティ政策に係る年次報告（2016 年度）（案）

サイバーセキュリティ政策に係る年次報告(2016年度)(案)の概要

資料１－１

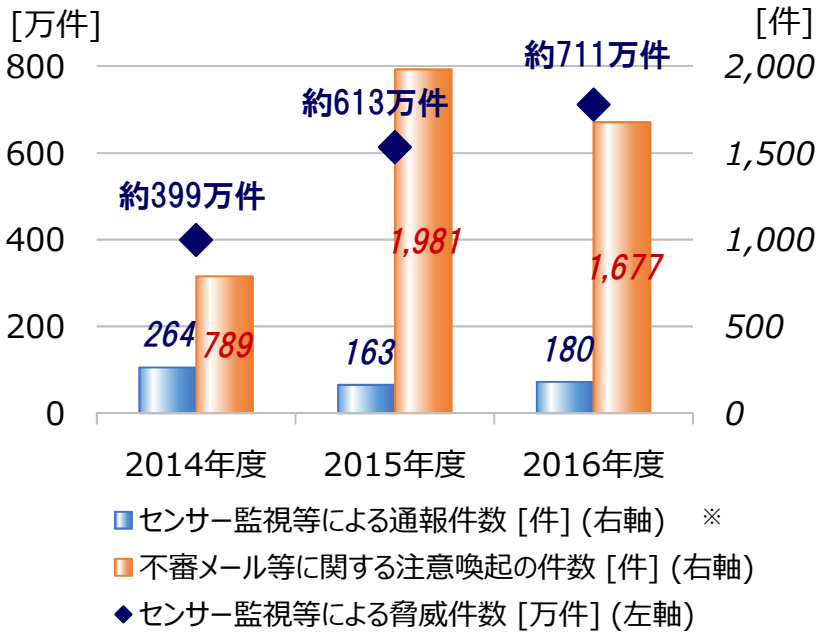
本年次報告の位置付け

- 「サイバーセキュリティ戦略」（2015年9月4日閣議決定）に基づく二期目の年次報告。
- 2016年度のサイバーセキュリティに関する情勢及び年次計画に掲げられた施策の実施状況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（Apache Struts等）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。
- 国による**監視、監査、原因究明調査等の範囲を拡大するための法改正を実施**（2016年４月成立、同年10月施行）。

【政府機関への脅威件数等】



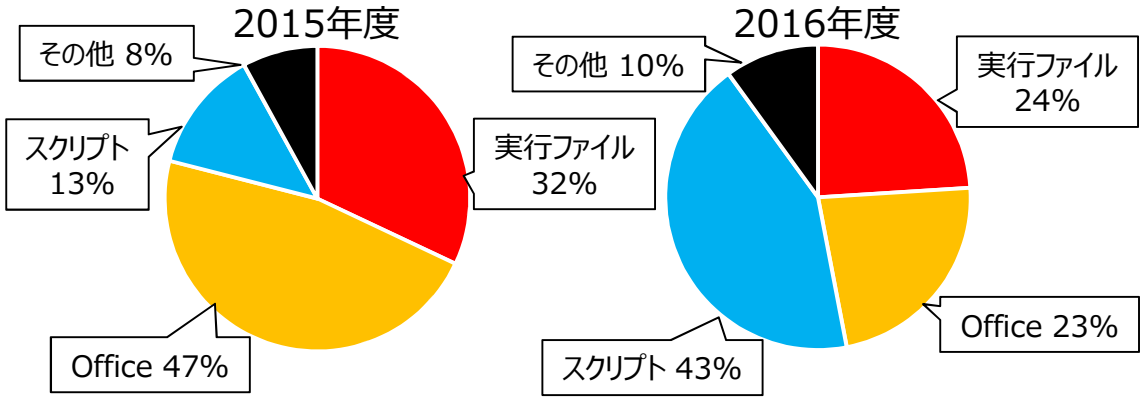
※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントを通知した件数。

【外部からの攻撃に係る2016年度の特徴】

- センサー監視等による脅威件数は約711万件となり、2015年度から約100万件増加。約4.4秒に１回、脅威を認知している。
- センサー監視等による通報件数は2015年度から増加（180件）。
- 不審メール等の注意喚起件数は急増した2015年度と同様1,500件を超えており高止まりしている状況（1,677件）。

【政府機関等に対する不審メールの添付ファイル形式の傾向】

実行ファイル及びOfficeファイルが依然として多くの割合を占める一方、スクリプト形式（JScript、VBScript等）の割合が**2016年度には43%と大きく増加**。



サイバーセキュリティ政策に係る年次報告(2016年度)(案)の概要

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化

- 「IoT推進コンソーシアム」において、IoT機器等の設計・製造・ネットワークへの接続等に係る**「IoTセキュリティガイドライン」を2016年７月に策定**。
- サイバーセキュリティをより積極的な経営への「投資」と位置づけ、企業の自発的な取組を促進するため、**「企業経営のためのサイバーセキュリティの考え方」を公表**。
- 我が国の企業のサイバー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た取組を実施。

2．国民が安全で安心して暮らせる社会の実現

- 「サイバーセキュリティ月間」（2017年２月１日～３月18日）において**「キックオフ・シンポジウム」を開催（２月１日）**。
- マルチメディアコンテンツ**『劇場版　ソードアート・オンライン　－オーディナル・スケール－』とタイアップ**を行い、ポスターやバナーの作成、イベント**「サイバー攻撃を目撃せよ！2017」を開催**。
- **「重要インフラの情報セキュリティ対策に係る第４次行動計画」を決定**。
- 重要インフラ13分野の事業者等が一堂に会して、相互に連携して情報共有・対処を行う**「分野横断的演習」**を継続実施。
- **「政府機関等の情報セキュリティ対策のための統一基準群」の改定。**
- **政府機関を対象とした監査を実施**し、全体として、統一基準が求める水準を満たすよう取組の実施を確認。助言への対応や技術的な対処・管理を含め、自律的な取組の継続が必要。
- 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 2017」**を継続実施。


サイバー攻撃を目撃せよ！2017


NATIONAL 318(CYBER) EKIDEN

サイバーセキュリティ政策に係る年次報告(2016年度)(案)の概要

主な政策の取組実績

3．国際社会の平和・安定及び我が国の安全保障

- G7伊勢志摩サミット（2016年５月）において立上げが決まった**G7のサイバーに関する新たな作業部会（伊勢志摩サイバーグループ）の第１回会合を開催**し、議長国として議論をリードし、G7各国との政策協調及び実務的な協力の強化に貢献。
- 日・ASEAN情報セキュリティ政策会議や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。
- **サイバーセキュリティ上の課題に国際的に連携して取組む「サイバーセキュリティ国際キャンペーン」を2016年10月に実施**。キャンペーン期間中のイベントの一つとして、在京米国大使館及び在日米国商工会議所と連携し、「サイバー・ハロウィン　キャリアトーク」を開催。


日・ASEAN情報セキュリティ政策会議

サイバー・ハロウィン　キャリアトーク

4．横断的施策

- 企業をはじ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**「サイバーセキュリティ人材育成プログラム」を2016年４月に策定**。
- サイバーセキュリティ対策を担う実践的な能力を有する人材不足への対応として、実践的な知識・技能を有する専門人材の育成・確保を目指して、2016年10月に情報処理安全確保支援士（通称：登録セキスペ）制度に必要な関係政省令の改正等を行い、2017年４月１日に**4,172人の情報処理安全確保支援士を登録**。
- 「ナショナルサイバートレーニングセンター」を組織し、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、若手のセキュリティエンジニアの育成をしているところ。

サイバーセキュリティ政策に係る年次報告(2016年度)(案)の概要

主な政策の取組実績

5．推進体制

- 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）の施行（2016年10月21日）により、**監視・監査・原因究明調査の対象を拡大**し、政府機関に加えて、独立行政法人及び一部の特殊法人等（９つの法人を指定）に対するセキュリティ対策の強化を図ったところ。
- 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のサイバーセキュリティワーキングチームにおいて、2020年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）のサイバーセキュリティの確保に資する具体的な施策について精力的に検討を推進。
- **リスク評価に基づく対策の促進**として、サービスの安全かつ持続的な提供の確保のためのリスク評価手順書を作成し、東京大会において開催・運営に影響を与える重要なサービスを提供する事業者等を選定。**2016年10月～12月の期間で第１回目のリスク評価を実施**し、約70組織から実施結果を受領。その取りまとめ及び次回に向けた改善の作業を実施。
- **対処体制の整備**として、東京大会のサイバーセキュリティ体制に関する体制検討会において、**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）の具体的な体制を検討**するとともに、**G7伊勢志摩サミット及びリオ大会開催期間等において、現地に連携要員を派遣し、情報共有手段として同検討に基づく情報共有体制の試験運用を実施**。

資料１－２

サイバーセキュリティ政策に係る年次報告
(2016年度)
(案)

2017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

サイバー空間が今や欠くことのできない経済社会の活動基盤となっている現代において、サイバーセキュリティの確保は国民生活や社会経済活動、我が国の安全保障の観点から極めて重要な課題となっている。2015年５月には、日本年金機構において約125万件の個人情報流出が発生するなど、政府機関や企業からの機密情報等の窃取を企図したサイバー攻撃は一層複雑化・巧妙化し、攻撃対象も拡大し続けている。また、海外においては、ウクライナでは2015年12月に多角的なサイバー攻撃によって大規模な停電が発生した旨報道されている。2017年５月には、ランサムウェア（いわゆる”WannaCry”）による我が国を含め世界規模でのサイバー攻撃が発生しており、サイバー攻撃は国民生活や社会経済活動に直接的かつ深刻な影響を及ぼす脅威となりつつある。

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「戦略」という。）を閣議決定し、戦略に基づく２期目の年次計画「サイバーセキュリティ2016」によって施策を推進してきたところである。

本報告は、2016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2016」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。本編記載のとおり、2016年度において特記すべき点としては、①サイバーセキュリティ基本法の一部改正法の施行及びそれに伴う政府機関等に対する対策の強化（指定法人の指定、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正等）、②セキュリティ人材育成のための取組の強化（サイバーセキュリティ人材育成プログラムの策定等）、③重要インフラ防護のための取組強化（重要インフラの情報セキュリティ対策に係る第４次行動計画の策定等）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、これを着実に推進することとする。

Ⅰ　2016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) サイバー空間は混沌とした状態

2016年度は、標的型攻撃も継続的に行われると同時にソフトウェアの脆弱性を悪用した従来型の攻撃が多発し、結果として大量の個人情報が窃取されるといった事案が散見された。また、マルウェアを用いずスクリプトを直接書き換えて情報を窃取するといった攻撃手法に加え、IoT機器に感染して大規模DDoS攻撃を仕掛ける新たなマルウェアが登場するなど高度化した攻撃手法も現れた。

2016年４月20日から同28日にかけて、ソフトウェアの脆弱性を突いたOSコマンドインジェクション攻撃[1]により、民間企業4社（日本テレビ、J-WAVE、栄光ゼミナール、エイベックス）から合計142万人分の個人情報が流出する事案が発生した[2]。2016年６月14日、旅行会社JTBのグループ会社のオペレーター端末において、取引先になりすました不正なメールの添付ファイルを開いたことによりPCがマルウェアに感染し、個人情報のあるサーバへ攻撃者が侵入する標的型攻撃により、約790万人分（後日重複分を除き679万人分に修正）の個人情報が流出した可能性がある事案が発生した[3]。

2016年12月2日には、化粧品会社資生堂の子会社の公式ウェブサイトに対し、不正アクセスの被害があり、氏名、住所、クレジットカード情報など約42万件が流出する可能性のある事案が発生した[4]。同社によると、公式サイトのECサイトにおけるウェブサーバにおいて、SSI[5]の脆弱性を突かれ、外部から不正アクセスを受けた結果、コンピュータ操作を可能にするバックドアプログラムを仕掛けられたことが原因としている[6]。

2017年２月５日以降は、ホームページの一部ページが改ざんされる事案が多発し、地方自治体、病院、教育機関等も被害を受けた。原因は、オープンソースのブログソフトウェアWordPressの脆弱性を悪用されたものであった。2017年３月10日には、トヨタファイナンス株式会社や住宅金融支援機構が事務を委託しているGMOペイメントゲートウェイ株式会社において、クレジットカード番号等の漏えい事案が発生した[7]。原因は、オープンソースのウェブアプリケーション開発ソフトウェアApache Struts ２の新たな脆弱性を悪用したものであった。３月10日以降も、日本貿易振興機構、日本郵便株式会社等において、Apache Struts ２の脆弱性を悪用した不正アクセスが発生した。

---

[1] OSコマンドとは、基本ソフトウェア（OS）を操作するための命令（コマンド）のことで、OSコマンドインジェクションとは、OSコマンドを挿入（インジェクション）してOSに不正に操作する攻撃手法のこと。

[2] 本項目における事案については、当該被害が公表されており、かつ、社会的影響が大きいと思われるものについて記載。
http://www.ntv.co.jp/info/pressrelease/20160421.html
https://www.j-wave.co.jp/topics/1604_info.htm
http://www.eikoh.co.jp/news/pdf/20160429.pdf
http://v4.eir-parts.net/v4Contents/View.aspx?template=announcement&sid=27850&code=7860

[3] http://www.jtbcorp.jp/jp/160614.html

[4] http://www.ipsa.co.jp/news/2/

[5] Server Side Includes。ウェブサーバの操作を正規に行うためのプログラム技術

[6] http://www.ipsa.co.jp/information/attention_161104.html

[7] https://corp.gmo-pg.com/news_em/20170310.html

こうした事態を避けるために、独立行政法人情報処理推進機構(IPA)等のセキュリティ関係機関による技術的対策等についての注意喚起やガイドラインを積極的に活用していくことや、公開された修正パッチを速やかに適用する等の対策が益々重要になってきている。加えて、各組織は自らが扱う情報の重要度に応じたセキュリティを構築する必要性を改めて認識させられたものであった。

海外においても、インターネット検索大手米Yahooから、億単位の個人情報流出が公表された。2016年９月、米Yahooは、2014年に約５億人の個人情報が盗み出されたことを、2016年12月には新たに、2013年８月に10億人超のユーザーアカウントが窃取されたことを明らかにしたものである[8]。2016年10月には、米Yahooの中核事業を48億ドルで買収することに合意した米通信大手Verizonが、買収金額の引き下げを求めて交渉中であることが報じられた。事案公表まで２年が経過していることを踏まえると、買収手続の最中であったころから、個人情報流出事案が企業買収に影響を与えたことに着目される。

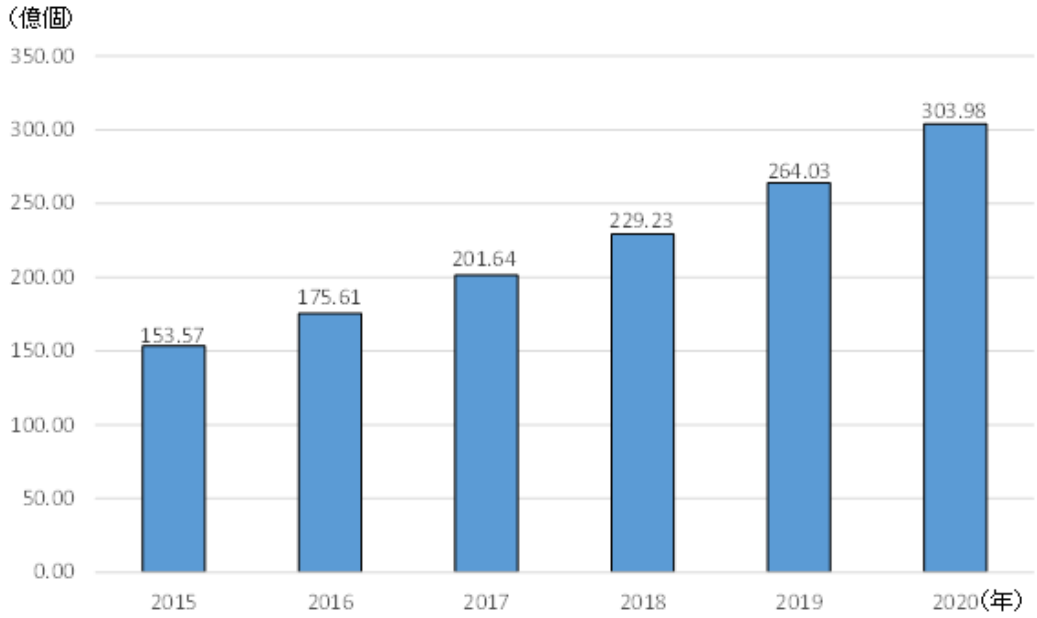
制御系システムを狙ったサイバー攻撃も引き続き発生しており、2016年12月にウクライナ・キエフで発生した停電について、ウクライナ国営電力会社は、サイバー攻撃によるものとの見方が示されている[9]。

2016年９月、IoT機器に感染し史上最大規模のDDoS攻撃を仕掛ける新型マルウェア（いわゆる”Mirai”）が登場した。2016年９月20日、米セキュリティ情報サイトKrebs on Securityが、ピーク時665GbpsのDDoS攻撃によって一時的にサイトが閉鎖に追い込まれ[10]、同22日には、フランスのインターネットサービスプロバイダーであるOVH社が、1.1TB[11]に達する大規模なDDoS攻撃を受けた[12]。Miraiのソースコードは、2016年10月１日、オンライン上に公開されたが、Miraiが攻撃対象としているIoT機器は、約49万3,000台に上るものと報じられた[13]。さらに、同21日には、米DNS[14]サービスプロバイダーであるDyn社が提供するサービスがDDoS攻撃を受け、その結果、処理に遅延が発生し、Twitter、Paypalなどのサービスの利用ができなくなった。従来のDDoS攻撃は、攻撃対象で処理するデータ量を多くする増幅が主流だった。例えば、DNS増幅攻撃(リフレクション攻撃)では、攻撃者がDNSに攻撃したい対象の名前を使って問い合わせをすることで、攻撃対象に問い合わせ結果が返る。問い合わせに必要な60byteの通信に対し、問い合わせ結果を4,000byteにも増幅することが可能である。一方、MiraiによるDDoS攻撃では、大量のIoT機器を操作してDDoS攻撃が行われる。それぞれにHTTP GETリクエストを大量に送信した場合は、正常な通信との区別がより難しいDDoS攻撃となる。正常なアクセスだけに、悪意ある通信だけを遮断することは難しいといった特徴がある。総務省によると、世界におけるIoTデバイスの数は、2020年で約300億個以上に達するとされている（図表Ⅰ－１－１）。IoTの進展に伴い、インターネット全体に影響を及ぼすような大規模なDDoS攻撃が増加する前に実効性のある対策に見直す必要があると言える。

---

[8] https://help.yahoo.com/kb/account/SLN27925.html
[9] http://en.interfax.com.ua/news/economic/391359.html
http://www.bbc.com/news/technology-38573074
[10] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[11] 記録上、過去最大規模の DDoS 攻撃
[12] https://twitter.com/olesovhcom/status/778830571677978624
[13] ITmedia,[マルウェア「Mirai」に感染した IoT 機器が急増、亜種も相次ぎ出現] (http://www.itmedia.co.jp/enterprise/articles/1610/20/news061.html)
[14] Domain Name System

図表Ⅰ－1－1　IoTデバイス数の2020年までの予測[15]



このほか、2016年５月15日、17都道府県のコンビニエンスストアに設置された現金自動支払機（ATM）約1,700台から、磁気ストライプカードを用いて偽造された南アフリカスタンダード銀行発行のデビットカードのキャッシング機能によって、現金約18億6,000万円が不正に引き出される事案が発生した。国内では、クレジットカードのショッピング機能とキャッシング機能に関して規定する法律を所管する官庁が異なっている。海外では、ICチップ対応がほぼ完了しているが、国内では、キャッシングに対して、ATMがICチップ対応済みであっても、ICチップ機能を使用しないことを悪用した事案であった。また、PC等のデータを暗号化し使用不能にした上で身代金を要求するランサムウェアについては、我が国においてもその感染被害が拡大傾向にあったと言える。IPAによれば、2016年中に検出したランサムウェア数は11,198であり、2015年（1,203）と比較し約9.3倍と急増している。ランサムウェアへの感染に備え、データのバックアップ等、適切な対策が必要となっている。

世論操作を意図していると疑われる攻撃も発生した。米国においては、2016年11月８日、一般有権者による2016年大統領選挙投開票が行われ、共和党のドナルド・トランプ氏が勝利したところ、同大統領選をめぐっては、2016年６月14日、ヒラリー・クリントン氏陣営の民主党全国委員会のコンピュータネットワークシステムに攻撃者グループが侵入し、内部の通信を閲覧したことが報じられたが、2016年12月29日、米連邦捜査局（FBI）及び国土安全保障省（DHS）は、ロシアの情報機関が過去2年にわたって民主党を標的とした電子メールのハッキングを行っていたとする報告書を発表した。また、同日、オバマ米大統領は、米大統領選を狙ったサイバー攻撃を仕掛けたとして、ロシアに対する制裁措置を発表した。英国においては、2016年６月23日実施のEU離脱の是非を問う国民投票において、2016年６月７日、インターネット経由で行われる国民投票の有権者登録サイトが機能しなくなった。この件に関し、英下院は、2017年４月12日、「外国によるDDoS攻撃による干渉の可能性を排除できない」とし、具体的な国には言及しなかったが、「ロシアや中国は大衆心理の把握や個人につけ込むため、こうした手段を講じる」と指摘する調査報告書を公表した[16]。こうした状況下

[15] 「平成28年版情報通信白書」（総務省）80頁より引用（データはIHS Technology作成）
[16] https://www.publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/496.pdf

において、欧州では、オランダ、フランス、ドイツといった2017年に国政選挙を控えた国において、集計を手作業で行う方針とするなど、サイバー攻撃を通じた選挙干渉に警戒する動きがみられる。

このように、2016年度は、従来型の攻撃が猛威を振るう中、個人情報窃取を企図した標的型攻撃も頻発し、さらに、マルウェアMiraiの登場など、サイバー攻撃の様態は、高度化、多様化しており、攻撃対象も、政府機関や重要インフラという分類に関係なく、ありとあらゆる対象が攻撃にさらされるなど、サイバー空間は混沌とした状態となっている。

(2) サイバー空間に係る国際的な動向

サイバー空間に関する国際的なルールや規範については、首脳や閣僚によるハイレベル会合や、国連政府専門家会合等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。このようなルールや規範を含む、サイバー空間の在り方については、国際法の適用や国際規範の在り方について様々な場を通じて議論がなされており、我が国と同様に情報の自由な流通や開放性を求める立場がある一方で、サイバー空間の規制や国家管理を強化する動きもみられる。

中国は、2016年11月７日に「サイバーセキュリティ法」を可決[17]、同年12月27日に「国家サイバー空間セキュリティ戦略」を策定・公表した。また、2017年３月１日、「中国サイバー空間国際協力戦略」を公表した。特に、サイバーセキュリティ法は、欧米諸国をはじめとする国際社会から、情報の自由な流通を制限するのではないかといった懸念も表明されている。ロシアは、2016年12月５日、「情報安全保障ドクトリン」を公表し、ロシアのサイバーセキュリティ政策の方向性を明示した。

欧州においては、2016年４月27日、EU域内の個人情報を保護することを目的とする一般データ保護規則[18]が、2016年７月19日、EU域内のネットワークと情報システムのセキュリティを確保するため、加盟国に各種取組を義務付ける、いわゆるNIS指令[19]が成立した。NIS指令では、加盟国政府機関の体制、インフラ事業者のセキュリティ確保のための要件が規定されているほか、インシデント発生時の情報提供の義務付けがなされている。他方、米国では、官民の情報共有に関して、「CISA（Cybersecurity Information Sharing Act of 2015）[20]」が策定されており、自主的な（ボランタリーな）情報共有を進めようとしている。また、米国は、オバマ政権からトランプ政権へ移行後、5か月近くたった2017年5月11日、サイバーセキュリティ政策に関する大統領令が署名されるなど、サイバーセキュリティを巡って不透明な状況が続いていた。引き続き、アメリカ第一主義を掲げるトランプ政権下におけるサイバーセキュリティ動向に注目が集まっている。

こうした情勢において、我が国では、「日米サイバー対話」や「日EUサイバー対話」をはじめとする二国間協議のほか、G7伊勢志摩サミット（2016年５月）において立上げが決まったG７のサイバーに関する新たな作業部会である「伊勢志摩サイバーグループ」や「国連政

[17] 2017年6月1日施行予定
[18] 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)
[19] 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
[20] 2015年12月18日成立

府専門家会合」等の多国間の会議に参加し、サイバー空間における国際的なルールや規範作り等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

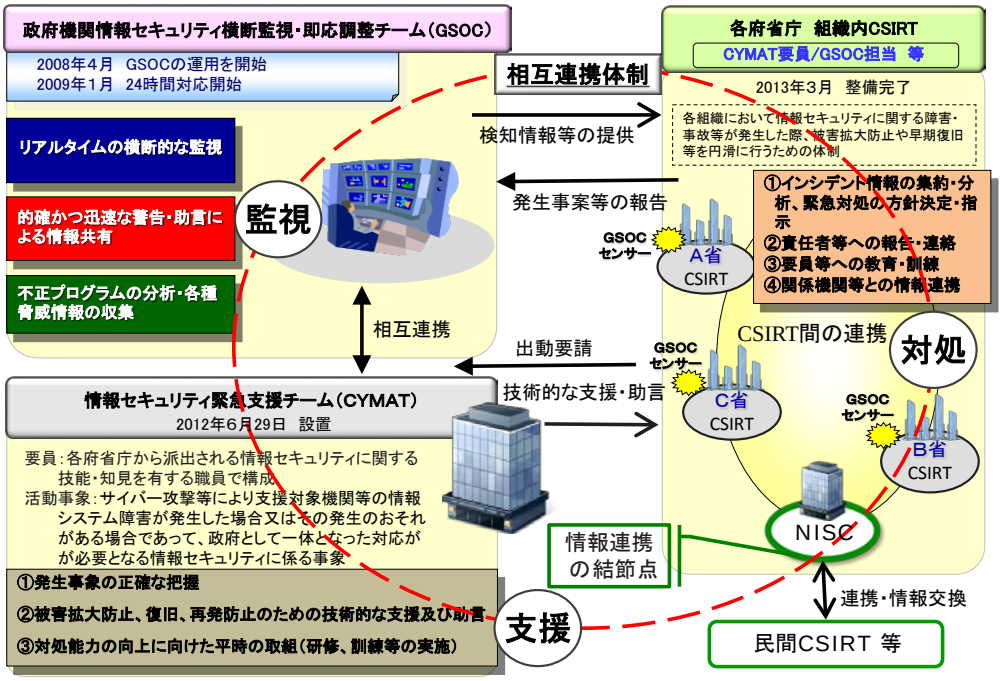
(1) 政府機関におけるサイバーセキュリティに関する体制

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、内閣官房内閣サイバーセキュリティセンター（NISC）及び各府省庁が適切な役割分担の下、相互に密接に連携しつつ、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）。

NISCにおいては、政府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、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC[21]）を設け、政府機関の情報システムに設置したGSOCセンサーを通じ、24時間365日体制の下、政府機関に対するサイバー攻撃等の不審な通信の横断的な監視、分析、情報収集を実施するとともに、各府省庁への通報、情報提供、助言などを行っている。また、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[22]）を派遣し、技術的な支援・助言を実施している。

一方、各府省庁においては組織内CSIRT[23]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する。

図表Ⅰ－2－1　政府機関における情報集約・支援体制の枠組み



[21] GSOC（Government Security Operation Coordination team）
[22] CYMAT（CYber incident Mobile Assistance Team）
[23] CSIRT（Computer Security Incident Response Team）

(2) 2016 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[24]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。

2016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Apache Struts等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。

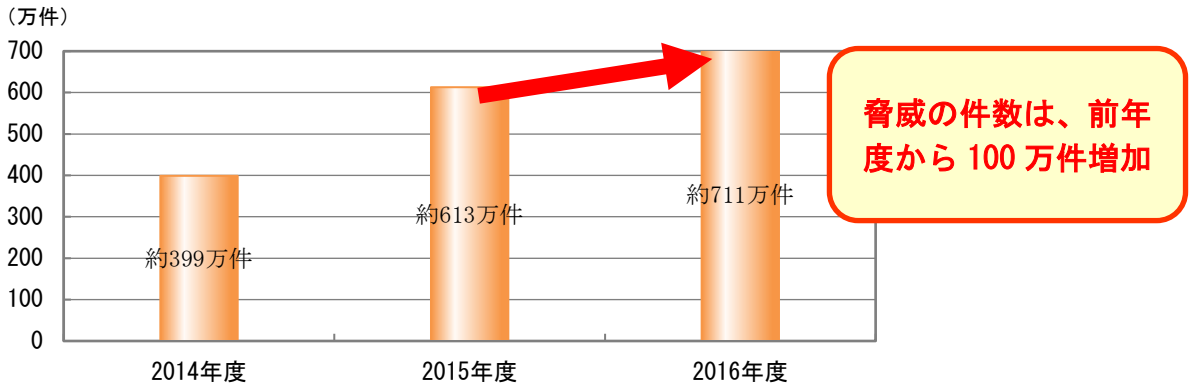
以下に、2016年度の政府機関等におけるサイバーセキュリティに関する情勢について、情報セキュリティインシデントの主な要因ごとにその傾向を示す。

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)政府機関への脅威動向について

NISCでは、GSOCにおいて、GSOCセンサーを政府機関に設置し政府横断的な情報収集・監視を行い、サイバー攻撃やその準備動作等の脅威を検知する業務を行っている。これは、外部から政府機関に対する不審な通信（不正アクセス等）や、標的型攻撃等によりもたらされた不正プログラムが行う外部との不審な通信等を検知し、攻撃を発見するもので、その検知は重要である。このGSOC センサーによる横断的な監視や政府機関のWebサイトの稼働状況の監視活動において、2016年度に政府機関への脅威と認知された件数は、約711万件であった（図表Ⅰ－２－２）。これは、約4.4秒に１回、脅威を認知している計算となり、2015年度の約613万件と比較して、約100万件増加している。2015年度も2014年度から脅威の認知件数が増加したが、2016年度は、2015年度を上回る脅威を認知しており、政府機関に対する攻撃が一層増加していることを示している。

図表Ⅰ－２－２　GSOC センサーで認知された政府機関への脅威の件数の推移

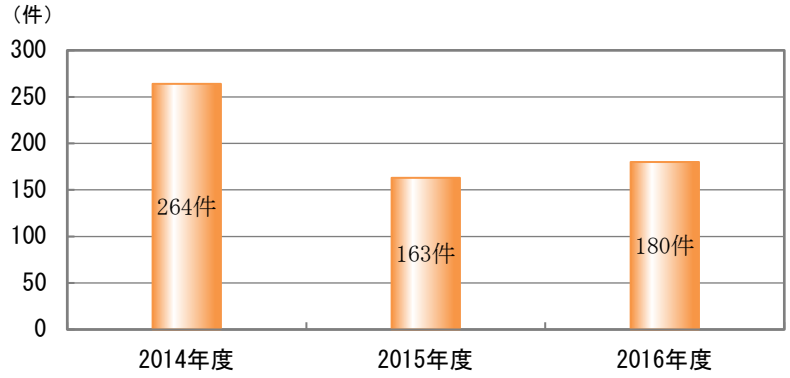


[24] 情報セキュリティに関する望まない又は予期しない事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（「別添５　用語解説」参照）。政府機関等において発生し公表又は報道された情報セキュリティインシデントの一覧については「別添３－10　政府機関等に係る 2016 年度の情報セキュリティインシデント一覧」を参照。

（イ）政府機関等に対する攻撃の傾向について

GSOCにおけるGSOC 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）を検知した際には当該政府機関等への通報[25]を行っており、2016年度においては、180件の通報を行った（図表Ⅰ－２－３）。2015年度の163件から増加しており、これは、政府機関等に深刻な被害をもたらし得る高い脅威となる攻撃が増大していることを示している。

図表Ⅰ－２－３　GSOC センサー監視等による通報件数の推移



通報件数の内容についてみると、2015年度は不審な通信の検知による通報件数が多く、全体の４割を占めていたが、2016年度はさらにその傾向に拍車がかかり、不審な通信の検知による通報件数は1.5倍に増加し、全体の７割を占めるに至った。特にApache Struts等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かった。脆弱性が発見された直後に攻撃されるケースが増えてきており、脆弱性に対するパッチの適用等の対応を迅速に実施することが必要になってきている。一方、標的型メールの検知[26]による通報件数は2015年度に比べて半分程度の件数に減少したが、依然無視できない件数となっており引き続き標的型メールへの警戒は必要と考えられる。

GSOCでは政府機関等のWebサイト等を定期的に監視しているが、DDoS攻撃などによるWebサイトの閲覧障害に関する通報が多い状況であり、件数は急増した2015年度と同水準であった。

このように、2015年度に大きな割合を占めた不審な通信の検知による通報が2016年度はさらに増加し、また、Webサイトの閲覧障害に関する通報が多いことから、標的型メールの検知による通報件数が2015年度に比べて減少したにも関わらず、全体の通報件数は増加する結果となっており、依然として政府機関等に対する攻撃は続いている。

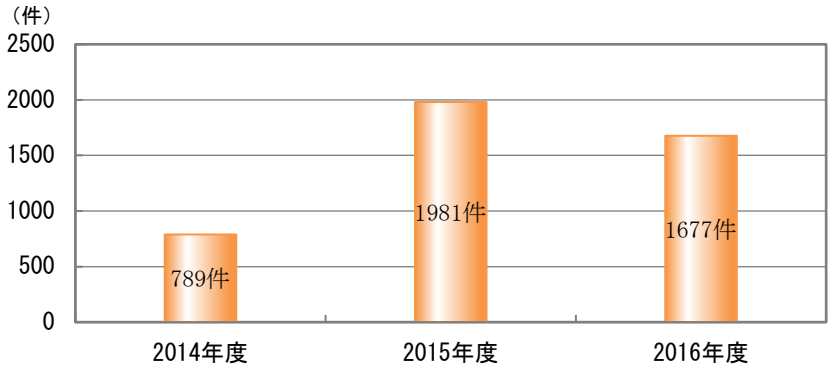
GSOCでは、政府機関等が受信する不審メール等の対応のため、情報を集約し注意喚起を行っている。この業務では、政府機関等が受信した不審なメールや添付ファイル、プログラムなどの検体の提供を受け、分析を行った結果、不正プログラムであることが確認できたものなどについて、政府機関等に対して一斉に注意喚起を行うもので、2016年度においては、1,677件の注意喚起文書を発出した（図表Ⅰ－２－４）。

---

[25] GSOC センサー等の監視活動により認知された脅威を分析した結果、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。

[26] 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付されていたりする、不審なメールの検知。

図表Ⅰ-2-4　不審メール等に関する注意喚起の件数の推移



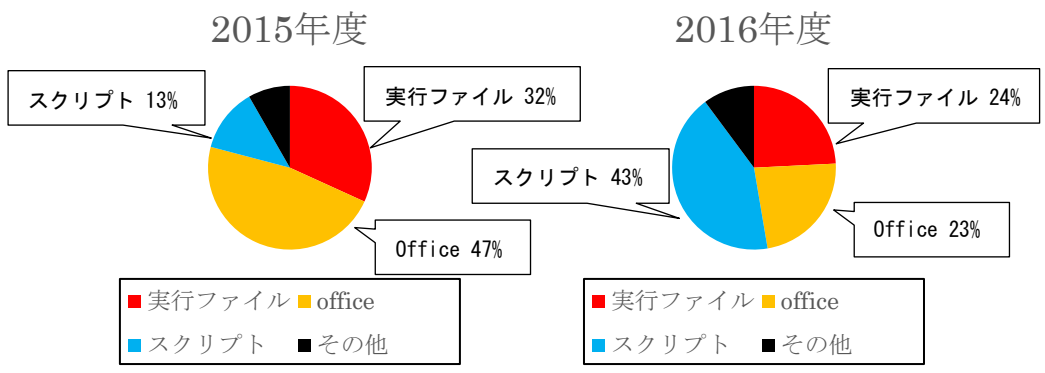
この注意喚起の件数は、2015年度は2014年度の789件に対して1,981件と2.5倍に急増し2,000件に迫る注意喚起を行ったが、2016年度は1,677件に減少した。これは、検体が同一である等の理由で既に注意喚起した不審メールと同種と考えられる不審メールに関しては注意喚起を実施しない等により真に必要な注意喚起のみを行うように見直しを実施した影響があると考えられ、必ずしも政府機関等に対し不審メールを送付するような攻撃が減少したことを意味しない。むしろ見直しを実施したにもかかわらず依然注意喚起件数は高い水準となっており、政府機関等に対する不審メールは多数送付されている状況が続いていると考えられる。

コラム　～不審メールの添付ファイルの形式～

GSOCにおいて解析した政府機関等に対する不審メールについて、その添付ファイルの形式で分類したものが図表Ⅰ-2-5である。2015年度から2016年度にかけて添付ファイルの傾向が大きく変わったことから、両年度を比較したところ、スクリプト形式（JScript、VBScript等）の割合が2016年度には43%と大きく増加した。また、2016年度には、実行すると外部から更なるマルウェアをダウンロードし、ファイルとして保存することなく実行する手口も確認されている。この場合、感染した端末を調査してもマルウェアの発見が難しいことに注意が必要である。

従来は、脆弱性を悪用し、マルウェアに感染させる手口が主流だったが、最近ではスクリプト形式に代表される正規の機能を悪用するものが増加しているため、各種ログ（proxyログ、Windowsイベントログ）の取得の強化や不要な機能は停止させるなどの対応が必要となる。

図表Ⅰ-2-5　不審メールの添付ファイルの形式の割合



(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、注意喚起を実施している。2016年度においては、GSOCより149件の脆弱性情報等を配信した（図表Ⅰ－２－６）。

図表Ⅰ－２－６　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

	2014年度	2015年度	2016年度
脆弱性情報等の配信	84 件	99 件	149 件

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

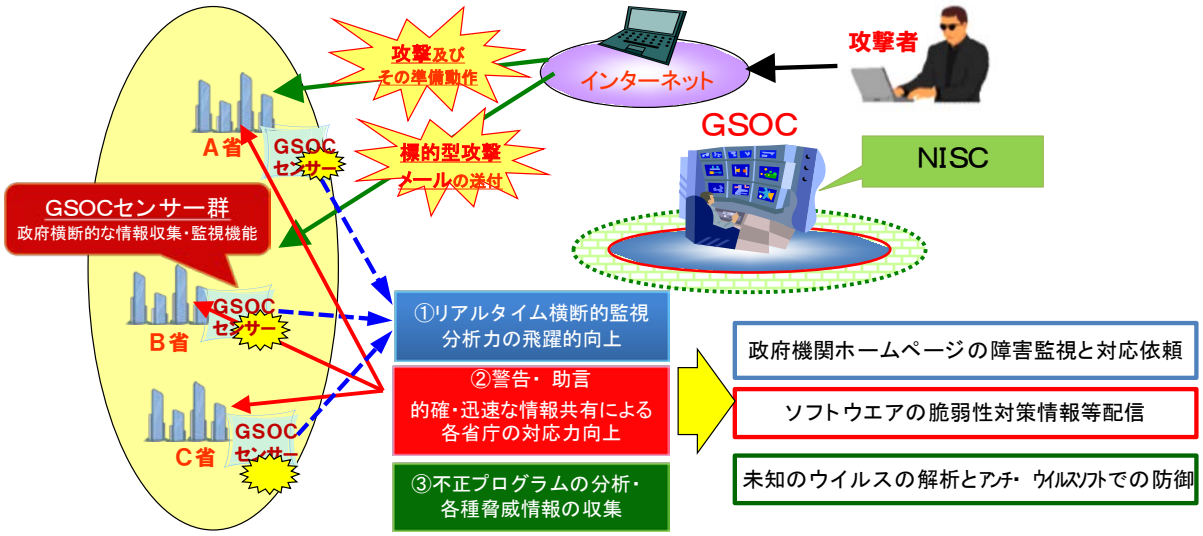
これまでに述べたとおり、注意喚起文書を発出した件数はやや減少したものの、脅威と認知した件数が2015年度の約613万件から約711万件と増加していること、GSOCセンサー等で検知した不審な通信を政府機関等に通報した件数が、2015年度の1.5倍に増加したことを併せ考えると、依然として、政府機関等に対する攻撃は深刻度を増しているといえる。

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においては、その検知・解析機能の強化、GSOCセンサーの増強等を図っている。また、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）を踏まえ、独立行政法人等に対する不正な通信の監視体制（第二GSOC）をIPAに構築し、2017年４月から運用を開始している。今後は、従前からの政府機関に対する監視体制（第一GSOC）と第二GSOCの間でも連携を図っていくことで、GSOCによる監視体制を強化していく予定である。

図表Ⅰ－2－7　GSOC の概要

【Government Security Operation Coordination team】（じーそっく）

- 2008年４月　第１期GSOCの運用開始（８時間運用）
- 2009年４月　24時間対応開始
- 2013年４月　第２期GSOCの運用開始
- 2017年４月　第３期GSOCの運用開始
  第二GSOCの運用開始



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

2016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

ますます複雑・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「戦略」という。）を策定した。

なお、この戦略の策定過程で、日本年金機構における不正アクセスによる情報流出事案が発生しており、政府としても本事案を重く受け止め、本事案等を踏まえて改めて見直しを行い、監査、原因究明調査等の対象の拡大等の所要の法改正を行うことを戦略に盛り込んだ。これを踏まえ、国による不正な通信の監視・監査・原因究明調査等の対象範囲を拡大するなど、政府機関等のサイバーセキュリティ対策の抜本的強化を図ることを目的と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案を第190回通常国会に提出した。同法案は2016年４月15日に成立し（平成28年法律第31号）、同年10月21日に施行された。

2016年度においては、戦略に基づく年次計画である「サイバーセキュリティ2016」（2016年８月31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、戦略について概説した後、2016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

戦略は、2020年東京オリンピック・パラリンピック競技大会の開催、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。サイバー空間は、「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」であり、人々の生活に恩恵をもたらす一方、国家の関与が疑われるような組織的かつ極めて高度なサイバー攻撃等による脅威の高まりも見られる状況にある。そのため、戦略は、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、まずは、現行の戦略の中間レビューとして、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を開始した。なお、同検討は、2017年夏までに方針を決定する予定である。

図表Ⅱ－１－１　サイバーセキュリティ戦略の全体構成

1 サイバー空間に係る認識
- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的
- 「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。

3 基本原則　① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

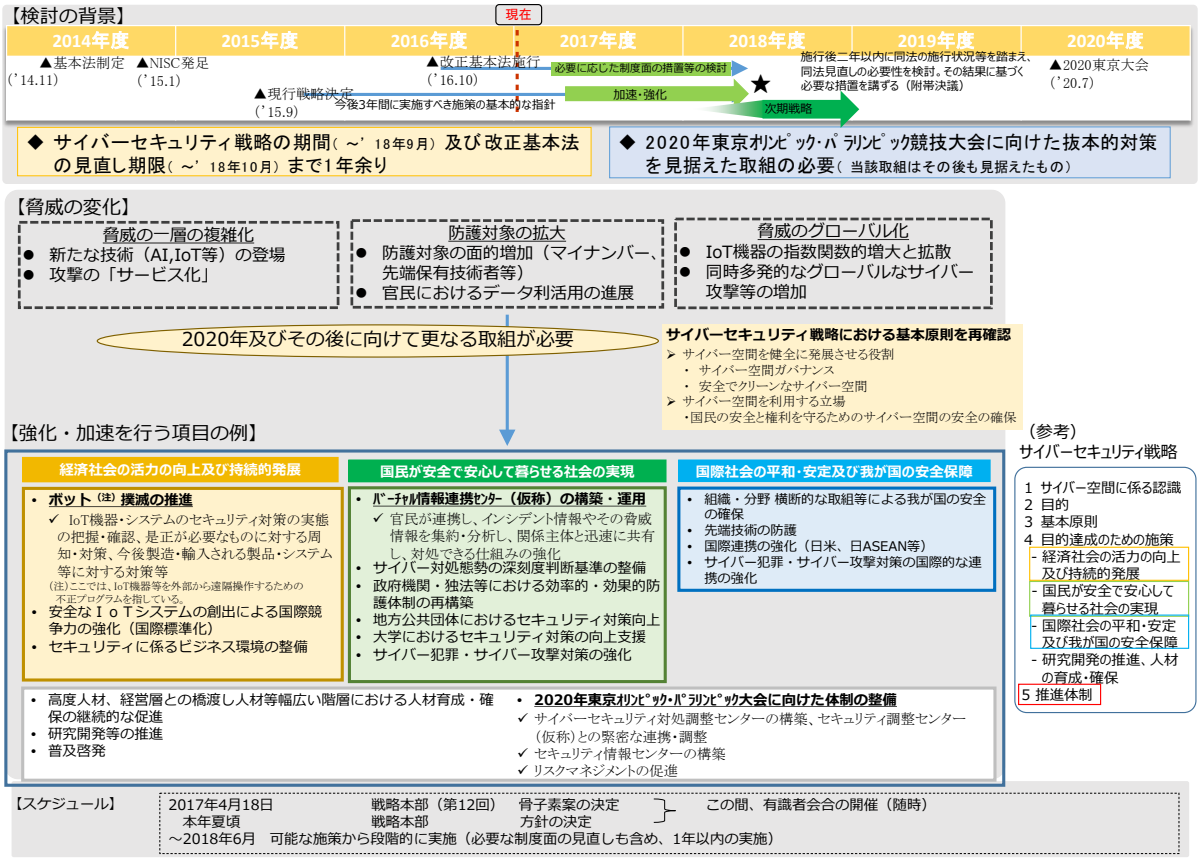
4 目的達成のための施策　①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

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
～ 費用から投資へ ～	～ 2020年・その後に向けた基盤形成 ～	～ サイバー空間における積極的平和主義 ～
■安全なIoTシステムの創出 安全なIoT活用による新産業創出	■国民・社会を守るための取組 事業者の取組促進、普及啓発、サイバー犯罪対策	■我が国の安全の確保 警察・自衛隊等のサイバー対処能力強化
■セキュリティマインドを持った企業経営の推進 経営層の意識改革、組織内体制の整備	■重要インフラを守るための取組 防護対象の継続的見直し、情報共有の活性化	■国際社会の平和・安定 国際的な「法の支配」確立、信頼醸成推進
■セキュリティに係るビジネス環境の整備 ファンドによるセキュリティ産業の振興	■政府機関を守るための取組 攻撃を前提とした防御力強化、監査を通じた徹底	■世界各国との協力・連携 米国・ASEANを始めとする諸国との協力・連携

横断的施策
- ■研究開発の推進　攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- ■人材の育成・確保　ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制　官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

図表Ⅱ－１－２　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



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、研究開発戦略専門調査会における議論等を通じ、2016年８月に安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにした、「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」[27]を策定した。

さらに、「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」（平成28年8月31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・デザインの考え方が前提として盛り込まれていることに留意することを示した。

総務省及び経済産業省においては、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、2016年7月に「IoTセキュリティガイドライン」を策定した。

さらに経済産業省は、IPAを通じて、「つながる世界の開発指針」[28]が産業間の情報連携においても有効であることを実証するため、ORiN協議会、一般社団法人エコーネットコンソーシアム及び神奈川工科大学と協力し、産業分野間（FA機器－HEMS）の情報連携に関する実証実験を実施した。「つながる世界の開発指針」を基に、４製品分野（車載機器、IoTゲートウェイ、金融端末（ATM)、決済端末（POS））においてセキュリティガイドラインが策定されるなど、普及展開にも努めた。

また、国立研究開発法人産業技術総合研究所（AIST）においては、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。ソフトウェア工学については、民間企業との共同研究において自動車やスマート工場を題材にした研究課題の洗い出しおよび実証実験環境の整備を行った。暗号技術においては、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解読に関する世界記録を更新し、得られた知見をもとに、格子暗号の実用化に向けた最大の障害である公開鍵サイズを90%削減する技術を開発した。

②　セキュリティマインドを持った企業経営の推進

ITの発展に伴って、経済・社会活動の大部分がインターネットに代表される、コンピュータ・ネットワークで処理されるようになり、ビジネスの変革がもたらされている。一方で、サイバー攻撃などによるリスクも増大するため、リスクをコントロールしつつ、企業としての挑戦を続けることが重要である。

---

[27] 「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」（http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf）

[28] 「つながる世界の開発指針」（http://www.ipa.go.jp/sec/reports/20160324.html）

こうした状況の下、2016年８月にNISCでは、企業の経営者を対象に、サイバーセキュリティをより積極的な経営への「投資」と位置づけ、企業の自発的な取組を促進するため、「企業経営のためのサイバーセキュリティの考え方」を示した。

また、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」として公表を予定している。

さらに、IPAでは、経営者が自らの責任で対応しなければならない事項を示した「経営者編」と、重要な情報に対する管理責任がある立場の方が実施する事項を示した「管理実践編」に分けて解説している、「中小企業の情報セキュリティ対策ガイドライン」[29]を公表し、中小企業に向けて、必要な情報セキュリティ対策を実施するよう促した。

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。

経済産業省においては、サイバーセキュリティ産業の活性化に向けた検討に着手、また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た特利制度を創設した。さらに、中小企業投資促進税制において、セキュリティ製品等の税制措置を継続している。

また、IPAにおいて、WG2コンビーナ、WG3副コンビーナ（2016年４月フロリダ会合、2016年10月アブダビ会合）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、日本から公開鍵暗号(1件）や軽量メッセージ認証方式（１件）が提案されており、規格化への支援を行っている。

文化庁の文化審議会著作権分科会においては、時代の変化に柔軟に対応できる権利制限規定の在り方について検討を行っているところであるが、当該検討の中で、セキュリティ目的も含めたリバースエンジニアリングのための著作物利用に係る課題についても検討を行っている。

(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

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。

[29] 「中小企業の情報セキュリティ対策ガイドライン」(https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

そこで、IPA及びJPCERT/CCでは、「ソフトウェア等脆弱性関連情報取扱基準」（平成26年経済産業省告示第110号）及び「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成29年経済産業省告示第19号）により、ソフトウェア製品及びウェブサイトの脆弱性についての届出を受け付け、ソフトウェア製品の脆弱性情報等を、JVN等を通じて利用者に提供した。さらには、IPAでは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」[30]とあわせて、基礎的な知識を実習形式で体系的に学べる「AppGoat」を公開して、脆弱性対策を促した。

また、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、国では２月１日から３月18日までの期間を「サイバーセキュリティ月間」として、産学官民の連携の下、集中的な普及啓発活動に取り組んでいる。NISCでは、2017年２月１日に開催したキックオフ・シンポジウムでは、『IoT時代のサイバーセキュリティー次世代のビジネスを支えるサイバーセキュリティー』というテーマで、企業にて直面しているサイバーセキュリティの課題やその対応について解説・議論した。

図表Ⅱ－２－１「2016年度サイバーセキュリティ月間 キックオフ・シンポジウム」の様子（2017年２月１日開催）

さらに、2017年３月４・５日には、サイバーセキュリティに関する理解を深めてもらうために、サイバー攻撃の実演や、近い将来実現し得る技術である、AR/VR機器の展示・体験などを交えたイベント「サイバー攻撃を目撃せよ！2017」を開催した。2016年度サイバーセキュリティ月間にて、NISCと『劇場版 ソードアート・オンライン －オーディナル・スケール

[30] 「安全なウェブサイトの作り方」（https://www.ipa.go.jp/security/vuln/websecurity.html）

ー』がタイアップを行っていることから、本イベントにおいてもタイアップコンテンツとして同作品のキャラクターが登場してサイバーセキュリティをわかりやすく啓発するマンガ冊子『ソードアート・オンライン サイバーセキュリティハンドブック』8,000部をIPAが作成して来場者に配布するなど、サイバーセキュリティをより身近なものとして捉えてもらえるような取組を行った。なお、本イベントでは、身近な話題からサイバーセキュリティに関する基本的な知識を、イラストを交えて紹介しているNISC作成の『情報セキュリティハンドブック』を冊子化して、家でもサイバーセキュリティを学べるよう、来場者に配布を行った。

図表Ⅱ－２－２「サイバー攻撃を目撃せよ！2017」の様子（2017年３月４・５日開催）

加えて、サイバー空間における悪意ある振る舞い等の脅威を無効化するため、事後追跡・再発防止及び今後生じうる犯罪・脅威への対策を積極的に強化していく必要がある。そのため、警察庁では、2016年８月31日に「警察庁サイバー人材確保・育成計画」を策定し、情報通信部門における高度な専門的知識・技能を有する人材及び情報通信技術に関する一定の専門性と所管行政に関する十分な知識、技能、経験を有し、高度専門人材と一般行政部門との橋渡しをする人材並びにサイバー空間の脅威への対処に係る警察官の確保・育成を図るため、サイバー空間を含めた治安の維持に万全を期すとともに、警察運営の更なる効率化を推進することとした。

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）を策定し、これに従って必要な施策を実施している。

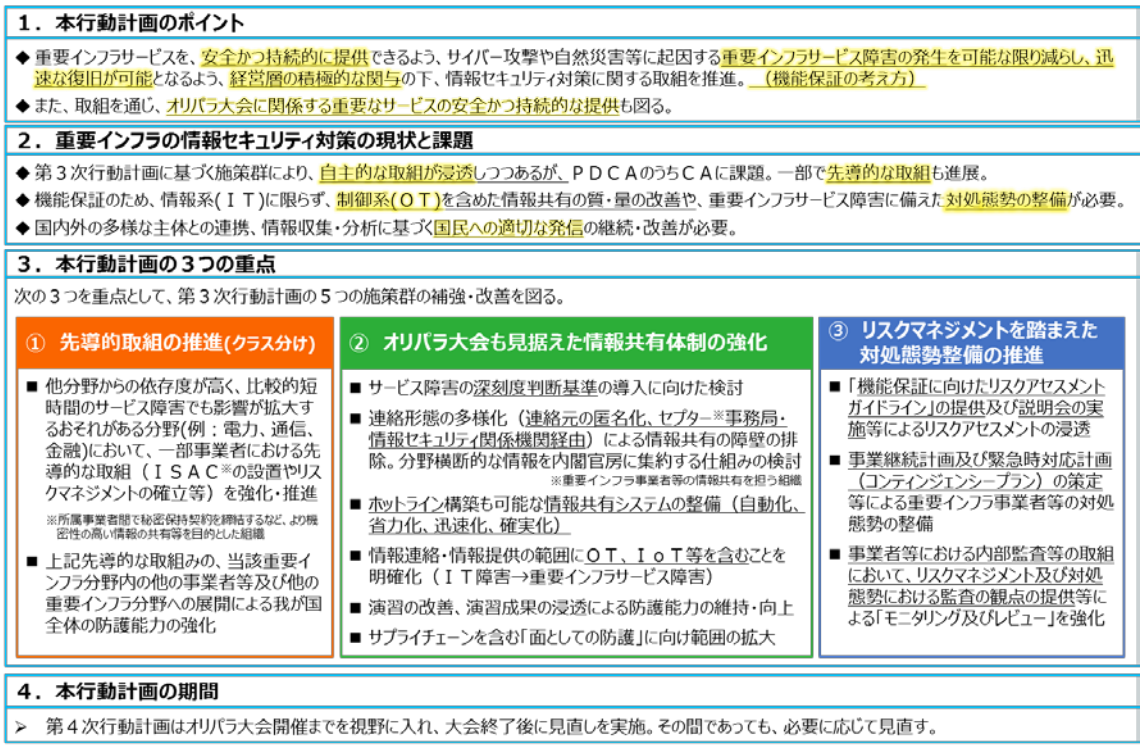
2016年度は、この第３次行動計画の最終年度に当たることから、各施策を着実に実施するとともに、2016年３月にサイバーセキュリティ戦略本部において決定した「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、第３次行動計画の成果と課題をとりまとめ、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（2017年４月18日サイバーセキュリティ戦略本部決定）を策定した。第４次行動計画の策定に当たっては、第３次行動計画の基本的な骨格（「安全基準等の整備及び浸

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。また、第４次行動計画に記載した事項のうち、特に必要なものについては、計画決定に先駆け2016年度中に着手している。

図表Ⅱ－２－３　「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



「安全基準等の整備及び浸透」については、2015年度の「重要インフラ分野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」の本編[31]・対策編[32]の改定、「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」[33]の策定に続き、2016年度は、これらを用いて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や所管省庁との関係法令に関する認識合わせ等を実施した。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。

[31] http://www.nisc.go.jp/active/infra/pdf/shishin4.pdf
[32] http://www.nisc.go.jp/active/infra/pdf/shishin4taisaku.pdf
[33] http://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf

「情報共有体制の強化」については、2016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結果、重要インフラ事業者等から所管省庁を通じて内閣官房へ情報連絡された件数が大幅に増加した。なお、第４次行動計画の策定過程において、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提言されたことを踏まえ、関係主体の理解を得た上で、計画策定を待たず情報連絡手順の整備に取り組んだ。また、重要インフラサービス障害に係る深刻度判断基準の具体化に向けた検討にも着手している。

図表Ⅱ－２－４　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
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
関係省庁・関係機関から内閣官房への情報共有件数	27件	52件	41件
内閣官房からの情報提供件数	38件	44件	80件

なお、警察においては、官民間の情報共有として、重要インフラ事業者等との間で構成するサイバーテロ対策協議会の枠組み等を通じ、犯罪捜査等により把握した新たなサイバー攻撃の手口等について注意喚起を行っている。

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ＩＴ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、相互に連携して情報共有・対処を行う「分野横断的演習」を毎年実施している。2016年度は、505組織2,084名が参加し、前年度の参加数（302組織1,168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。2016年度においては、多様な参加形態のモデルケースを提示するなど、演習環境・内容の充実を図っている。

図表Ⅱ－２－５　2016年度分野横断的演習の様子

演習の模様

丸川大臣による視察

なお、関係省庁においても、総務省における実践的サイバー防御演習（CYDER)、経産省における制御システムセキュリティセンター（CSSC）の模擬システム等を用いた実践的なサイバー演習、金融庁における金融業界横断的なサイバーセキュリティ演習（Delta Wall）を実

施したほか、警察においてサイバー攻撃を想定した官民合同の対処訓練を全国各地で開催した。

「リスクマネジメント」については、リスクマネジメントを行うことにより必要な対処態勢の整備を促進するという目的を確認するとともに、2020年東京オリンピック・パラリンピック競技大会を見据えた「機能保証に向けたリスクアセスメント・ガイドライン」[34]を作成し、関連事業者等による第１回目のリスクアセスメントの取組において活用した。これに当たっては、事業者向け説明会や意見交換会等を通じて詳細な説明を繰り返し行うことにより、機能保証のコンセプト、必要性及びその手法の所管省庁及び事業者等への浸透を促進した。なお、第４次行動計画の策定過程において、当該ガイドラインの一般の重要インフラに適用するための一般化、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むべき要点等に関する検討にも着手している。

「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設立（Telecom ISACの活動を移行）に当たっての一部放送事業者及びケーブルテレビ事業者の加盟、電力ISACの設立など、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。なお、第４次行動計画の決定に先駆け、内閣官房からの情報について、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開始した。

③ 政府機関を守るための取組

本節では、政府機関等全体としての対策水準の向上を推進するための取組について示す。

まず、統一基準群の改定を2016年８月のサイバーセキュリティ戦略本部において決定した。これにより、統一基準群の独立行政法人等への適用範囲の拡大、事案発生に備えた対処体制や対処・連絡手順等の整備に係る規定の強化、標的型攻撃等による不正プログラム感染の発生を前提とする情報システムの防御策の強化、情報及び情報システムへの不正アクセスの防止等を目的とする対策の見直し・強化、新たなIT製品・サービスの普及等に伴う対策事項の明確化等を行った。また、統一基準群の改定に伴い、政府機関等は、それぞれの組織において情報セキュリティポリシーの見直しを順次実施している。内閣官房では、勉強会の開催や情報セキュリティポリシーの改定に係る調査の実施を通じて、政府機関等における情報セキュリティポリシーの見直しについて、進捗状況の把握、支援等を行った。

【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、情報システムの調達においてセキュリティ・バ

[34] http://www.nisc.go.jp/active/infra/files/riskhyoka.ZIP

イ・デザインが強化されるよう統一基準群における所要の規定強化を行ったことから、政府機関等の職員に対する研修において、セキュリティ・バイ・デザイン及びサプライチェーン・リスク対応の必要性や具体的な対処方法を説明し、理解を促進した。さらに、府省庁の情報システムに対して、攻撃者が実際の攻撃で行う手法での疑似攻撃にて侵入試験（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システムを構築した。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、CSIRT体制や情報セキュリティインシデント発生時の対処の在り方に係る統一基準群の規定を強化したことを踏まえ、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インシデント・ハンドリングに関する事項の習得に重点を置いた研修を実施したほか、１府12省庁対抗による競技形式のサイバー攻撃対処訓練であるNATIONAL 318(CYBER) EKIDEN 2017を実施した。

図表Ⅱ－２－６「NATIONAL 318(CYBER) EKIDEN 2017」の様子

被害の低減のための主な取組としては、「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」[35]を改定し、府省庁に加え、独立行政法人及び指定法人に対しても、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。さらに、「情報セキュリティ監査実施手順の策定手引書」[36]の改定を行い、府省庁における情報セキュリティ監査の実効性の向上を図った。また、2015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。さらに、厚生労働省（日本年金機構を含む。）に対する施策の評価を行った。

[35] http://www.nisc.go.jp/active/general/risk.html
[36] http://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf

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。2016年には、指定法人についても独立行政法人と同様に、支援対象事象となり得る事象が発生した場合に、当該法人の要請を踏まえて所管府省庁がCYMATに事象対策の支援を要請できるよう、申合せを改定した。なお、2016年度には、CYMATが支援対象機関に対して具体的な支援及び助言を行う機会はなかった。

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2016年８月末までに「各府省庁セキュリティ・IT人材確保・育成計画」を策定し、同計画に基づく体制の整備として、2016年度における機構・定員要求の結果、府省庁全体で約80の定員増による体制強化を実現したほか、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、統一基準群の規定を強化したことに伴い、政府機関等の職員に対する研修においてクラウドサービス選定の際に考慮すべき点を説明し意識の向上を図ったほか、政府機関等における実際のクラウドサービスの利用や対策の状況について調査を実施した。

また、伊勢志摩サミット等の会合で準備するIT環境のセキュリティ対策について、事前に関係機関の協力を得て整理したことにより、会議開催に特化したIT環境の政府統一的なセキュリティ対策を共有し、推進した。

【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、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化を図っている。

2016年４月15日、国が行う不正な通信の監視、監査、原因究明調査等の対象範囲の拡大や、サイバーセキュリティ戦略本部の一部事務をIPA等に委託することを主な改正内容とする「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」が成立した。これを受け、特殊法人及び認可法人のうち９つの法人を指定法人としてサイバーセキュリティ戦略本部が指定した。また、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、サイバーセキュリティ戦略本部重大事象施策評価規則、サイバーセキュリティ戦略本部資料提供等規則等を改定した。

独立行政法人及び指定法人に対して、IPAと連携して監査を開始したほか、NISCの監督の下、IPAにおいて独立行政法人及び指定法人に対する不正な通信の監視体制を構築した。また、当該監視体制の構築を踏まえて、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、独立行政法人及び指定法人を所管する部局の管理職並びにこれらの法人の幹部職員に対する統一基準群や監査等に関する講義や、独立行政法人及び指定法人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、指定法人、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。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、海外においては、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指摘されている。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では、高度なサイバー攻撃からの防護及び脅威認識等に係る能力の強化のため、人材、技術、組織等の観点から、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整備に継続的に取り組んでいる。具体的には、警察庁が「インターネット・オシントセンター」（４月）、公安調査庁が「サイバー関連調査推進本部」（５月）を新たに設置したことを含め、対処機関自身の防護システムの機能拡充等を図るとともに、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り、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。この観点から、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、防衛省では、防衛産業との官民合同のサイバー演習や調達する情報システムに使用される部品等の製造元の追跡に関する調査研究を実施している。

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こととともに、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、内閣官房や警察において、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ほか、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していくこととしている。

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。国際社会の平和と安定を実現するためには、サイバーセキュリティを確保しつつ、サイバー空間における情報の自由な流通を確保す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、実空間と同様に法の支配が貫徹されるべきである。我が国は、国際的なルールや規範の形成と実現に向け、国際社会において、このための取組を積極的に進めている。首脳や閣僚によるハイレベルの多国間協議においては、参加各国との間で、サイバー空間に国際法が適用されることや、サイバー空間において国家が守るべき国際規範、重要インフラ分野におけるサイバーセキュリティの重要性等についての確認を行うことにより、サイバー空間に関する国際的な共通理解の促進に努めている。2016年度においては、G7伊勢志摩サミット（2016年５月）、同外相会合（2016年４月 広島）、同情報通信大臣会合（2016年４月 香川・高松）、同エネルギー大臣会合（2016年５月 北九州）、同交通大臣会合（2016年９月 軽井沢）、G20首脳会合（2016年９月 中国・杭州）において、関連する共同声明が採択されている。また、実務レベルでは、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作りに関する議論を進めつつ、第５会期国連政府専門家会合に外務省サイバー政策担当大使が参加し、国家によるICT[37]の利用に際しても既存の国際法上の義務が適用されること等のサイバー空間への国際法の適用や国際規範に関する議論に参画し、サイバー空間における法の支配の確立及び規範の深化に向け積極的に寄与してきた。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、社会活動や経済活動のみならず、軍事活動を含めたあらゆる活動が依拠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、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、我が国では、二国間等のサイバー協議やARF[38]等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戦略

[37] Information and Communications Technologyの略。情報通信技術のこと。
[38] 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。

に係る情報共有と相互理解を進めている。同時に、日・ASEAN情報セキュリティ政策会議やMeridian[39]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を主催したほか、IWWN[40]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を阻止する必要がある。このため、内閣情報官の下、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。警察庁で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。公安調査庁でも、サイバー空間上の国際テロ組織等に関する関連情報の収集・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。

国境を超えるサイバー空間の脅威に世界各国で連携して効果的に対処していくため、我が国は、世界各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、外務省、経済産業省、国際協力機構、JPCERT/CC等の各機関は、ASEAN各国をはじ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。さらに、内閣官房を中心とした関係省庁の緊密な連携の下、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強化すべく、「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）を策定した。

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。また、サイバーセキュリティ・コンテスト「SECCON CTF2016」等を通じ、我が国のサイバーセキュリティ人材が研鑽を積む場を提供した。

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。

[39] 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。
[40] 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。

G7伊勢志摩サミット（2016年５月）においては、「サイバーに関するG7の原則と行動」の合意を主導した。また、同サミットにおいて立上げが決まったＧ７のサイバーに関する新たな作業部会（伊勢志摩サイバーグループ）の第１回会合（2016年10月・東京）を開催し、サイバー空間の安全性及び安定性を高めるため、最近のサイバーセキュリティ環境に関する様々な議論を議長国としてリードし、Ｇ７各国との政策協調及び実務的な協力の強化に貢献した。

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９回日・ASEAN情報セキュリティ政策会議（2016年10月 東京）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、人材育成の面等で連携を強化していくことで合意した。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。また、隣国である中国及び韓国との間では、第３回日中韓サイバー協議（2017年２月 東京）を開催し、サイバー分野における各国の施策や戦略、国際的な規範等について協議を行った。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－２－７　「第９回日・ASEAN 情報セキュリティ政策会議」の様子

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の協力を進めている。また、同指針では、日本の安全に影響を与える深刻なものを含め、サイバー事案が発生した場合の日米両政府による連携と対処についても合意している。これに基づき、第４回目日米サイバー対話（2016年７月 米国・ワシントン）では、情勢認識、重要インフラ防護、能力構築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が行った。加えて、両国間では第５回日米サイバー防衛政策ワーキンググループ（2016年10月 東京）等を開催し、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日独サイバー協議（2016年９月 東京）、第３回日英サイバー協議（2016年10月 東京）、第２回日露サイバー協議（2016年11月 ロシア・モスクワ）、日ウクライナサイバー協議（2016年12月 ウクライナ・キエフ）、第３回日仏サイバー協議（2017年１月 フランス・パリ）、第２回日ＥＵサイバー対話（2017年1月 ベルギー・ブリュッセル）、第３回日・エストニアサイバー協議（2017年１月 エストニア・タリン）、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、ICTに関する研究開発等における連携について議論を行っている。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、防衛省では、北大西洋条約機構のサイバー防衛に関する研究や訓練などを行う機関である、サイバー防衛センター（NATO CCDCOE）が主催する国際サイバー演習への参加等を通じ、連携強化を図っている。

中南米、中東アフリカの両地域についても、第２回日イスラエル・サイバー協議（2016年６月 イスラエル・テルアビブ）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。

図表Ⅱ－２－８　「サイバーセキュリティ国際キャンペーン」で開催したイベントの様子

我が国では、サイバーセキュリティ上の課題に国際的に連携して取組む「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。キャンペーン期間中のイベントの一つとして、2016年度は、在京米国大使館及び在日米国商工会議所と連携し、「サイバー・ハロウィン　キャリアトーク」を開催した（図表Ⅱ－２－８）。

(4)　横断的施策

①　研究開発の推進

ネットワークへ接続するシステムや機器は、重要インフラ等での利活用を含めて大幅に拡大し、国や企業等は、これまで以上にサイバーセキュリティへの対策を講じていくことが必要になる。さらに、サイバー攻撃は日々進化し高度化・複雑化しており、その変化に対処していくため、創意と工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠であると言える。このため、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、将来的なサイバーセキュリティの考え方を含めた「サイバーセキュリティ研究開発戦略」の検討を開始した。

経済産業省においては、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。

また、経済産業省、総務省においてはIPA、NICT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、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等を引き続き実施した。 また、「CRYPTREC」において、暗号の利用者向けのセキュリティ対策等のニーズを踏まえ、暗号プロトコルも取組対象とし、ガイドライン策定に向けて検討を実施した。

文部科学省においては、新設した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、10年後を見据えた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る。

内閣府においては、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、制御ネットワークのセキュリティ対策として、設備全体の機器のソフトやデータについて、マルウェア等による改変を検知する技術を開発し、プロトタイプ実装によって基本機能（信頼の連鎖）が完成した。また、「情報共有システム」について、重要インフラ事業者のデモによる要件をフィードバックし、検証用プロトタイプの開発が完了した。

② 人材の育成・確保

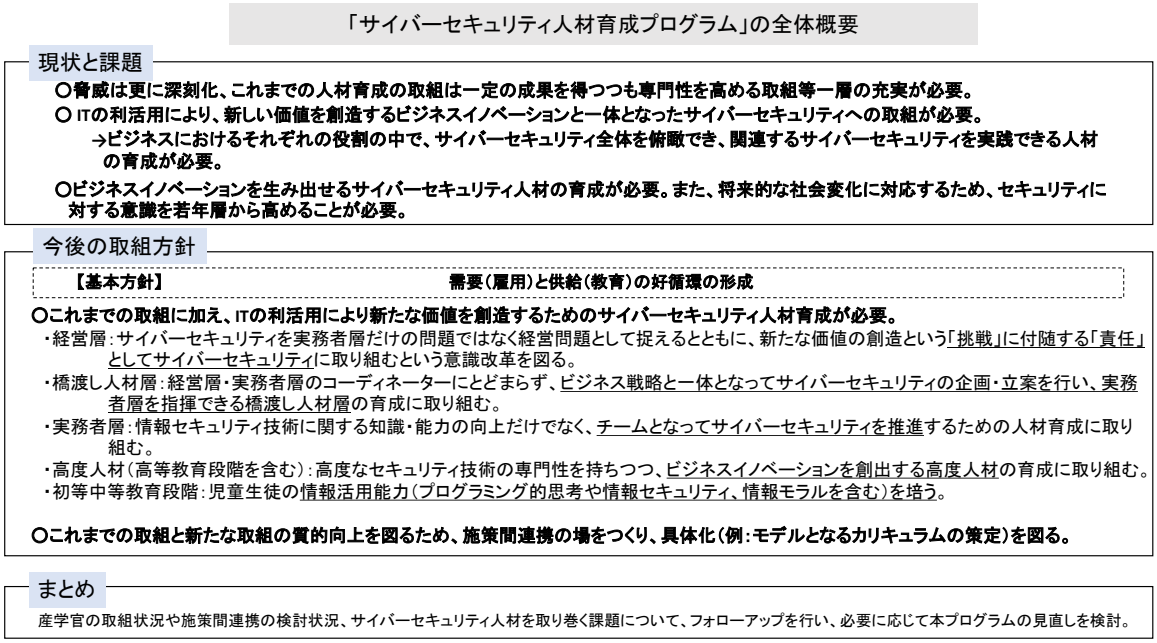
サイバー空間は、企業活動のグローバル化やデジタル化が進む中において、主に民間主体の投資や英知の集約により急速な拡大を遂げてきており、経済社会の活動基盤となっている。こうした中、サイバー攻撃は、情報等の窃取、社会システムの機能不全により、国民生活、さらには国際社会が危機にさらされる原因となりうる。このため、個人や組織を問わず、あらゆる主体がサイバーセキュリティに対する認識を深め、各主体の協力的かつ自発的な取組を通じて、その脅威に対処できる安全な空間としていかなければならない。

こうした環境整備に資するよう、2017年4月に、企業をはじ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「サイバーセキュリティ人材育成プログラム」を策定した。

また、具体的な施策として、経済産業省では、企業等におけるサイバーセキュリティ対策の重要性が高まる中、サイバーセキュリティ対策を担う実践的な能力を有する人材不足への対応として、実践的な知識・技能を有する専門人材の育成・確保を目指して、2016年10月に情報処理安全確保支援士（通称：登録セキスペ）制度に必要な関係政省令の改正等を行い、2017年４月１日に4,172人の情報処理安全確保支援士を登録した。また、総務省ではNICTに「ナショナルサイバートレーニングセンター」を組織し、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、若手のセキュリティエンジニアの育成を図ることとした。

図表Ⅱ－２－９「サイバーセキュリティ人材育成プログラム」の全体概要



(5)　推進体制

広く政府機関等における対策の強化を図る必要があるとの認識の下、更なる深刻化が進むサイバー攻撃に備え、2016年度においても、政府は、戦略に基づき、サイバーセキュリティ対策のための体制強化に取り組んだ。

まず、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）の施行（2016年10月21日）により、監視・監査・原因究明調査の対象を拡大し、政府機関に加えて、独立行政法人及び一部の特殊法人・認可法人（指定法人）に対するセキュリティ対策の強化を図った。

また、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のサイバーセキュリティワーキングチームにおいて、2020年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）のサイバーセキュリティの確保に資する具体的な施策について精力的に検討を推進した。また、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・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）にサイバーセキュリティ対策の強化を明記した。

NISCにおいては、リスク評価に基づく対策の促進として、サービスの安全かつ持続的な提供の確保のためのリスク評価手順書を作成し、東京大会において開催・運営に影響を与える重要なサービスを提供する事業者等を選定し、2016年10月～12月の期間で第１回目のリスク評価を実施した。約70組織から実施結果を受領し、取りまとめ及び次回に向けた改善の作業を実施した。また、対処体制の整備として、東京大会のサイバーセキュリティ体制に関する体制検討会において、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）の具体的な体制を検討するとともに、G7伊勢志摩サミット及びリオ大会開催期間等において、現地に連携要員を派遣し、同検討に基づく情報共有体制の試験運用を実施した。

Ⅲ　サイバーセキュリティ関連施策の評価

本章は、「サイバーセキュリティ戦略」に基づく年次計画である「サイバーセキュリティ2016」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2016」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しており、2020年の東京オリンピック・パラリンピック競技大会等に向けて、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。別途策定される2017年度の年次計画である「サイバーセキュリティ2017」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】

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。

【課　題】

「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、国際標準化等に取り組むことにより、安全、高品質を訴求できるIoTシステムを実現し、世界的な市場シェアの獲得を目指すことが必要である。

(2)　セキュリティマインドを持った企業経営の推進

【総　評】

2017年８月にNISCでは、企業の経営者を対象に、サイバーセキュリティをより積極的な経営への「投資」と位置づけ、企業の自発的な取組を促進するため、「企業経営のためのサイバーセキュリティの考え方」を示した。また、IPAでは、「中小企業の情報セキュリティ対策ガイドライン」を公表し、中小企業に向けて、必要な情報セキュリティ対策を実施するよう促した。

【課　題】

今後もITの発展に伴い、経営を取り巻く環境は大きく変化することが考えられ、それに合わせたサイバーセキュリティの対応が求められる。そのため、企業のサイバーセキュリティに係る取組について、経営層の認識、情報発信の状況や関連する制度面の課題等の把握に努め、経営層の認識を高めていくための推進方策等について検討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IoT産業を含む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、我が国企業の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。

【課　題】

我が国の政府機関や企業等のサイバーセキュリティの確保に向けて、サイバーセキュリティに係る投資を促進することで、サイバーセキュリティ関連産業における継続的な需要喚起を促す必要がある。

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】

サイバー空間の利用環境の整備のため、各種サイバー攻撃に関する情報収集や、未然にサイバー攻撃を防ぐための方策を実施した。また、「サイバーセキュリティ月間」では、一人でも多くの方にサイバーセキュリティに関する理解を深めていただくために、サイバー攻撃の実演や、近い将来実現し得る技術である、AR/VR機器の展示・体験などを交えたイベントを開催するなど、普及啓発活動を推進した。加えて、サイバー犯罪への対策についても警察庁を中心に強化を図った。

【課　題】

インターネットの利用に関し、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、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、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】

2016年度は、2014年度に策定した「重要インフラの情報セキュリティ対策に係る第３次行動計画」の最終年度に当たり、同計画における各施策を着実に推進した。また、2016年３月にサイバーセキュリティ戦略本部において決定した「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、第３次行動計画の成果と課題をとりまとめ、同計画の基本的な骨格を維持しつつ、機能保証の考え方を踏まえた「重要インフラの情報セキュリティ対策に係る第４次行動計画」を策定した。

【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。

(3)　政府機関を守るための取組

【総　評】

統一基準群を改定し、サイバーセキュリティ基本法に基づく国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準と位置付けられることを明確化するとともに、政府機関等がこれを踏まえた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行った。また、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ための検討をする上で有益な助言等を行った。さらに、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人材の育成を推進した。

【課　題】

「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」に基づき、独立行政法人及び指定法人に対する監査及び監視を実施するなど、引き続き、政府機関、独立行政法人及び指定法人におけるサイバーセキュリティ確保のための取組を総合的に強化する必要がある。

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】

各対処機関では、高度なサイバー攻撃からの防護及び脅威認識等に係る能力の強化のため、人材、技術、組織等の観点から、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、官民協力のもと取組を進めている。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。

【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、政府全体で取り組んでいく必要がある。

(2)　国際社会の平和・安定

【総　評】

G7伊勢志摩サミットを始めとする首脳・閣僚級のハイレベル協議の共同声明や、実務レベルにおける二国間サイバー協議や国連政府専門家会合等の多国間協議を通じ、責任ある国際社会の一員として、法の支配の確立に積極的に寄与しつつ、法執行面での各国との連携強化を進めてきた。また、重大な情報セキュリティインシデント発生時等における国外関係機関との連絡体制の確保と我が国の対処能力の向上のため、国際的なサイバー演習を行うとともに、信頼醸成を図る観点から、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、サイバー空間における国際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、内閣官房を中心とする関係省庁は、ASEAN各国等の開発途上国向け支援の取組を強化すべく、「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）を策定し、政府全体の取組としてキャパシティビルディングに積極的に協力している。

【課　題】

サイバー空間における法の支配の確立に向けては、首脳・閣僚によるハイレベルの協議や国連政府専門家会合等の場を通じ、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。

【課　題】

アジア大洋州においては、日ASEAN情報セキュリティ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、「情報セキュリティ研究開発戦略（改定版）」を踏まえ、各府省庁において、サイバー攻撃検知等、防御力向上等に資する研究開発施策が実施された。また、次期戦略として「サイバーセキュリティ研究開発戦略」の策定に着手した。

【課　題】

IoT技術、AI、AR/VR技術などによって、実空間とサイバー空間の融合が高度に深化し、新しい価値が創出されていく中で、単に情報システムへの脅威に対応するだけでなく、「人

間」や「人間が安心して暮らすことのできる社会システム」を守り、強くしていく方策の検討が必要である。こうした方策を含めた「サイバーセキュリティ研究開発戦略」を策定し、それに基づく具体的な研究開発の検討を促す必要がある。

(2)　人材の育成・確保

【総　評】

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、企業をはじ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。また、資格制度の整備や演習環境の強化等、セキュリティ人材の育成・確保に関する施策を推進した。

【課　題】

産学官の連携により、サイバーセキュリティ人材の「需要」と「供給」の好循環を形成することが求められており、経営層、橋渡し人材層、実務者層等、それぞれの人材層を対象にした施策間の連携等により、より効果的な人材育成の実施を図る必要がある。

５　推進体制

【総　評】

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）の施行（2016年10月21日）により、監視・監査・原因究明調査の対象を拡大し、政府機関に加えて、独立行政法人及び一部の特殊法人・認可法人（指定法人）に対するセキュリティ対策の強化を図った。

また、2016年度は、リスク評価手順書を作成し、東京都２３区内のオリパラの重要サービス事業者等を特定し、第１回目のリスク評価を実施した。また、G7伊勢志摩サミット及びリオ大会に連携要員を派遣して情報共有体制の試験運用をおこなうことにより、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）の検討を深化させた。

【課　題】

2017年度以降実施する第２回目以降のリスク評価について、評価結果のフィードバックと有識者等からのアドバイスを反映させ、逐次実施要領を改善するとともに、対象組織の地域的、業種的な拡大を図っていく必要がある。

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）の整備において、情報共有・対処支援の詳細な実施要領を策定し、演習や訓練等を通じて最適化するとともに、人員体制の検討・調整、情報共有システムやセンター設備の整備を具体的に実施していく必要がある。

（本ページは白紙です。）

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＞

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2017年度当初までに定めた「対策推進計画」を基として、2016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2017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

2016年度の総合評価・2017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　山﨑　重孝

2016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などその態様も多様化し、これらの攻撃への対応の重要性が一層増しているところである。

また、GSOCから発出された不審メール情報等を集計したところ、2016年度は約1,700件となっており、政府機関に対するサイバー攻撃の端緒となる攻撃が多い状況が続いているものと考えられる。

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

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

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

しかし、日々技術が進歩するとともに新たな脆弱性も発見される情報通信分野において、情報セキュリティ対策に終わりはない。また、サイバー攻撃に対する防御についても同様であり、コンピュータ技術だけではなく、人を騙すテクニック、いわゆるソーシャルハッキングについても新たな手法が考案されていることから、広い意味でのサイバー攻撃対策についても、絶えず見直す必要がある。

また、GSOCより発出されている不審メール情報等が多い状況が続いていることは、2020年東京オリンピック・パラリンピック競技大会を控え、関係者に対する警鐘として重く受け止めなければならない。

このような状況を踏まえ、内閣官房では2017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、NISC等が実施する研修会への参加を一層促進するほか、eラーニングを導入する。

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

2016年度の総合評価・2017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。

2016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におけるマネジメント監査の実施により、情報セキュリティ対策の助言を受けた。また、LANシステムの更改に伴い、セキュリティ対策強化を実施したほか、体制整備・人材拡充のために「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。）を策定した。

2017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、昨年度策定した人材育成計画に基づき、情報管理担当部門の職員はもとより、一般職員の情報リテラシーの向上を図ることにより、当局全体の体制を強化・整備する。また、統一基準群の改定に伴う内閣法制局情報セキュリティポリシー関連規程の整備、マネジメント監査における指摘事項に対する改善計画の策定等を通じ、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

2016年度の総合評価・2017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。

2016年度においては、4月にサイバーセキュリティ・情報化審議官を新設するなど、体制の強化を図るとともに各職員に人事院情報セキュリティポリシー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人事交流等により新たに人事院職員となった者を対象としたe-ラーニングによる情報セキュリティ教育を実施した。

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、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行い、訓練実施結果とその際の対処方法について周知するなどの対策を行った。

職員の情報セキュリティ対策の実施状況について、長期休業者等を除く職員全員が自己点検を行った。また、監査については、自己点検監査計画に基づき選定したサンプル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、セキュリティ対策の実施を確認した。

2017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他、NISC等が実施する研修への参加を一層促進し、情報セキュリティ対策へのより一層の理解を深めるとともに、情報セキュリティに対する意識を確実に向上させ、情報セキュリティ責任者等の役割に応じた情報セキュリティに対する一層の理解と意識の向上に取り組むこととする。

また、情報セキュリティ対策に係る自己点検や監査を充実させ、PDCAサイクルの実践の促進を図り、情報セキュリティ対策の一層の向上に努めることとする。

内閣府

2016年度の総合評価・2017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　河内　隆

内閣府では、情報システム対策として、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を実施している。

しかし、標的型メール攻撃等のソーシャルエンジニアリングを駆使した攻撃の脅威は、むしろ増大しており、更には、ソーシャルメディアサービス等の利用が進み、情報漏洩やプライバシー侵害等のリスクも増大している。

こうした状況の下で、情報システムの運用において、最も弱いのは人間であることから、内閣府では、情報システムのセキュリティ強化のために、人への対策にも積極的に取り組んでいる。

2016年度においては、上述のシステム面の対策とともに、人への対策として、職員の情報セキュリティ意識向上のために、標的型メール攻撃の訓練、情報セキュリティセミナー、ｅ-ラーニングを実施した。

2017年度においては、2016年度の反省及びセキュリティ脅威の動向を踏まえ、教育・訓練、セキュリティ脅威の啓発等を強化し、人への対策を中心に更なるセキュリティ強化を実施するとともに、2016年度に内閣サイバーセキリティセンターが実施した「サイバーセキュリティ対策を強化するための施策（監査)」による報告書で受けた助言の点検を行い、今後の情報セキュリティ対策の改善を図る。

宮内庁

2016年度の総合評価・2017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、2016年度においては、主に以下の対策を実施した。

〇宮内庁セキュリティ・IT人材確保・育成計画の作成・実施

〇CSIRT研修・訓練の成果を踏まえ、情報セキュリティインシデントの対処手順の充実化

〇情報の格付の決定・明示、パスワードの適切な管理に係る具体的手順の整備・周知

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検討（導入は2017年度を予定）

2017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改定を踏まえ、宮内庁情報セキュリティポリシーや各種手順等の整備を行う。

また、宮内庁セキュリティ・IT人材確保・育成計画を推進し、行政事務従事者の教育として、引き続き、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。

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

2016年度の総合評価・2017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。

2016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し、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・育成計画を作成し、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、職員における情報セキュリティ対策の実施状況を確認するため、情報セキュリティに関する自己点検を実施し情報セキュリティ対策の実施状況を確認した。さらに政府統一基準群の改定に伴い、公正取引委員会情報セキュリティポリシーを改定し、情報セキュリティ水準の向上を図った。

2017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、近年、危険性が増大している標的型メール攻撃に特化した訓練については、昨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、CSIRT体制を見直すとともにインシデント発生を想定した連絡訓練などを行い、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

2016年度の総合評価・2017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。

2016年度においては、2016年８月に「政府機関等の情報セキュリティ対策のための統一基準群」が改正されたことを受け、2017年１月に警察情報セキュリティポリシーを改正し、日本年金機構における情報流出事案等を踏まえた規定の強化を図った。

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。

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、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設定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。

2017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、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

2016年度の総合評価・2017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。

2017年度においては、改正個人情報保護法の全面施行といった制度・業務に係る大きな動向が予定されている。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、これまでの取組（「政府機関の情報セキュリティ対策のための統一基準群（2016年度版）」（2016年８月31日サイバーセキュリティ戦略本部決定）に積極的に応じた「個人情報保護委員会情報セキュリティポリシー」（2016年１月19日最高情報セキュリティ責任者決定）の早期改定、情報セキュリティ関係規程の整備及び運用、責任者等の体制の整備及び拡充、職員に対する教育及び訓練、情報セキュリティ対策に係る自己点検及び監査等）を継続的に実施し定着を図るほか、委員会事務局の更なる体制拡充及び委員会が整備・管理する情報システムの追加を踏まえて、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

2016年度の総合評価・2017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　森田　宗男

昨今、政府機関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・巧妙化し、攻撃対象も拡大し続けている。また、政府機関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極めて重要な課題となっている。

更に、ワークライフスタイルの変革の潮流を受け、在宅勤務を可能とするリモートアクセス環境の整備など、システムを活用した利便性向上が期待されている中で、情報セキュリティとの高いレベルでの両立の実現も求められているところである。

こうした状況にあって、金融庁としても、過去にサイバー攻撃を受けた教訓も踏まえ、サイバー攻撃に対応するための網羅的な対策を実施することの必要性を強く認識しており、2016年度においては、統一基準の改定に伴う金融庁情報セキュリティポリシーの見直し、技術的対策の多重化・多層化、訓練や教育の実施等に取り組んだところである。

2017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、各種監査結果のより一層の活用等、2016年度の取組みにより明らかになった課題や、サイバー攻撃の動向、ワークライフスタイル変革の潮流等への的確な対応を念頭におき、セキュリティ・IT人材の確保・育成、サイバー攻撃への対応能力の向上、サイバー攻撃に関する情報収集の強化や技術的対策の導入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

2016年度の総合評価・2017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年度は、昨年度の庁舎移転により他府省庁と執務環境の一部が共用となったことや、標的型攻撃をはじめとする外部環境からのサイバー攻撃リスクへの対策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や不審メール訓練の実施による啓蒙活動に取り組んだ。その結果、情報セキュリティインシデントは発生せず、消費者庁（以下「当庁」という。）の情報セキュリティマネジメントが相応に有効に機能しているものと判断するが、自己点検結果は実施率が98.96%となり、一部職員における電子メール転送禁止ルールの不認識が明らかとなったり、不審メール訓練において約２割の職員が訓練用の模擬メールを開封してしまったりと、改善すべき課題点も明らかとなった。

また、2016年度より運用が開始された新規システムについては、計画通りリスク評価ガイドラインに則ったサイバー攻撃対策のリスク評価と対策導入計画の策定を実施した。

2016年度対策推進計画において定めた重要情報を保管するための専用環境の運用開始については、重要情報の取扱いに係る規程を整備し、計画通り、専用環境の本格的な運用をすることが出来た。

2016年度はNISCによるマネジメント監査を初めて受審した。その結果、当庁の情報セキュリティ体制について、マネジメント面やシステム面、運用面に渡って対処すべき課題事項が明確となった。明らかとなった課題事項に対しては、計画的な改善に取り組み、情報セキュリティ体制の更なる向上を図る。

なお、2016年度対策推進計画において定めていた消費者庁LANシステム更改に向けた要件定義については、LANシステム更改予定が2018年度に変更となったことにより、次年度対応事項となったため、実施していない。

2017年度は、2016年度に初めて実施したNISCマネジメント監査や、情報セキュリティ監査において確認された課題事項への対策として、各課題に対する改善計画を策定し、計画的な改善活動による当庁情報セキュリティ体制の更なる向上を図る。また、職員への情報セキュリティ教育においては、情報セキュリティ教育管理徹底による確実な情報セキュリティ教育の実施や、継続的な不審メール訓練を実施し、入替り頻度が高い当庁の職員事情を考慮しながら、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、2017年度より、徳島県内に消費者行政新未来創造オフィスの開設が予定されていることを踏まえ、拠点間情報連携における情報セキュリティインシデントが発生することの無いよう、実施すべき情報セキュリティ対策の確実な実施や、情報セキュリティ監査等による対策実施状況の点検を行っていく。

復興庁

2016年度の総合評価・2017年度の全体方針

最高情報セキュリティ責任者
総括官　関　博之

復興庁は、復興に関する施策の企画、調整及び実施、地方公共団体への一元的な窓口と支援等を行う行政機関として、復興庁情報セキュリティポリシーの整備をはじめ、様々な情報セキュリティ対策の実施、情報セキュリティ対策のための体制整備、職員への情報セキュリティ教育の実施等を図ってきた。

2016年度は、「政府機関の情報セキュリティ対策のための統一基準（平成28年度版）」等を踏まえ、復興庁においても情報セキュリティ水準の適切な維持及び情報セキュリティ体制の強化を図ることを目的として、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実施した。

また、全職員を対象とした情報セキュリティ研修の実施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、2015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。

2017年度においては、復興庁情報セキュリティポリシー等の関係規程の改定内容及び2016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

2016年度の総合評価・2017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　山田　真貴子

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。

○　2016 年度の総合評価

2016 年度は、政府統一基準群の改定を受け、総務省情報セキュリティポリシー（以下、「ポリシー」という。）の改定を行い、引き続き政府統一基準群に沿った対策が行えるよう配慮した。

また、2016 年度においても、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、外部委託業者の情報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するなど、外部委託時等における情報セキュリティ管理に改善の余地が認められたため、対応する規定の改善等を実施した。

○　2017 年度の計画

2017 年度は、引き続き、サイバーセキュリティ・情報化審議官の下、サイバーセキュリティに係る対策の実施を行う。2016 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。2017 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

2016年度の総合評価・2017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　辻　裕教

法務省は、法秩序の維持や国民の権利擁護といった国民生活に密接に関連する広範な行政を任務としていることから、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、2016年度は、高度サイバー攻撃等への対応体制を整備することとして、特に重要な情報のインターネットからの分離及びインターネットの接続口の集約化を実現し、情報セキュリティインシデント対処体制（CSIRT）の抜本的な強化を行った。また、情報セキュリティマネジメントシステムの確立を図ることとして、情報セキュリティのリスク評価を行い、情報セキュリティの教育・自己点検・監査の有効性評価を実施した。さらに、当省が所管する情報システム及び情報をセキュリティ・リスクから保護し、かつ、効率的な行政運営の実現を図るために、セキュリティ・IT人材の確保・育成計画を策定した。

これらの取組等を総合的に評価すると、情報システムに関する技術的な対策や体制・制度の見直しなどにより、情報セキュリティの水準を多面的に向上することができたと認められる一方で、今後、情報セキュリティ対策のより一層の高度化を実現する上での課題も浮き彫りとなった。すなわち、地方支分部局等を含め組織の規模が大きく、かつ、本省部局等が所掌とする事務がそれぞれ高度の専門性・特殊性等を有し、独立性が高いという当省の特性に由来する課題である。

したがって、2017年度は、前年度に引き続き、高度サイバー攻撃等への対応体制を更に強化するとともに、情報セキュリティマネジメントシステムの改善を図り、セキュリティ・IT人材の確保・育成を着実に進めることに加えて、新たに、情報セキュリティ対策の基本的枠組みを当省の特性に適したものに刷新するための取組を行い、複雑かつ変化する環境下での組織的対応能力の向上に努めることとする。

外務省

2016年度の総合評価・2017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　山﨑　和之

2016年度、当省においては５月の伊勢志摩サミット、８月の第６回アフリカ開発会議（TICAD Ⅵ）及び12月の日ロ首脳会談などの国内外の大規模行事に際し、情報セキュリティ対策面についても、関係省庁や専門家の協力を得て万全の体制で臨み、いずれにおいても大事に至るような事案の発生は確認されなかった。

サイバー攻撃は、ますます多様化・深刻化しており、当省においてもランサムウェアや大規模なDDos攻撃、巧妙化する標的型メール攻撃への対策など、常に最新の脅威に立ち向かっている。

このような状況の中、当省においては2016年度情報セキュリティ対策として、以下の主要な取組を行った。

（１）「サイバーセキュリティ人材育成総合強化方針」に基づき、省内関係課室の横断的な議論を踏まえた人材育成計画の策定

（２）実在の攻撃手法を模した標的型メール攻撃訓練の実施や当省への攻撃事例を踏まえた新たな脅威に対する迅速な注意喚起等の発出

（３）第三者機関による外務省情報セキュリティポリシーの準拠性監査やNISCによるマネジメント監査を通じた情報セキュリティ制度や運用実態の再検証

2017年度においては、上記対策に加え、省内全ての情報システムに対する情報セキュリティ対策の底上げのため、情報セキュリティ支援部門の体制を強化し、情報システムを保有する全ての省内部局に対して外務省情報セキュリティポリシーで規定された安全・確実な情報セキュリティ確保のための対策支援及びチェック機能の強化を図る。

また、情報システムの開発・改修・運用管理に当たって、効果的な情報セキュリティ対策のための経費が予算要求時点で適切に盛り込まれるよう2018年度予算要求における助言・サポートを行うなど、情報セキュリティ対策のための側面支援を充実させる他、改正後の外務省情報セキュリティポリシーに基づき、一般職員のみならず、情報システムセキュリティ責任者や担当者向けの専門性の高いｅラーニングコンテンツの作成と教育の徹底を行い、当省全体の情報セキュリティリテラシー向上のための教育・啓発活動を継続する。

財務省

2016年度の総合評価・2017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　岡本 薫明

近年、政府機関等を狙ったサイバー攻撃が巧妙化・多様化し、サイバー攻撃の脅威は一層高まっている。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を取り巻く情勢を踏まえ、内閣サイバーセキュリティセンターとも連携をとりながら、情報セキュリティの確保等に取り組んできた。

2016年度においては、政府統一基準群の改定を踏まえたセキュリティポリシーの改定を行ったほか、最近の情報セキュリティインシデント事案等を踏まえ、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、職員が任意に参加する形式でCIO補佐官による講演を開催した。一般職員の情報リテラシー向上の観点からは、定期的に省内・地方支分部局の幹部職員等を対象に最近のセキュリティ情勢や留意点等について説明を行ったほか、全職員を対象に情報セキュリティ研修や標的型メール攻撃訓練を実施した。インシデント対応能力向上の観点からは、CSIRT要員等に対する情報セキュリティインシデント対処訓練を実施した。このほか、自己点検、情報セキュリティ監査、NISCによるマネジメント監査・ペネトレーションテスト等を行ったが、重大な問題は認められなかった。

2017年度においても、より一層のセキュリティ対策の強化を図っていく必要があることから、引き続き、「財務省セキュリティ・IT人材確保・育成計画」（28年８月末）に基づき、情報セキュリティに関する研修・説明会等を実施し、最新のセキュリティ情勢について省内における横串での情報共有を行うほか、より実効的な監査やセキュリティ対策の強化等を実施し、PDCAサイクルの推進を図る。また、所管する独立行政法人・指定法人等との連携も強化し、より強固な情報セキュリティ対策推進体制を構築していく。なお、2017年度に予定している基幹LANシステムの更改においては、業務の効率化と情報セキュリティ対策の双方の観点を踏まえたシステム整備を行う。

文部科学省

2016年度の総合評価・2017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　佐野　太

近年、新たな脆弱性や未知のマルウェアの出現により、深刻な被害につながる恐れのあるサイバー攻撃が数多く発生している。また、従来の情報窃取に加えて、重要な情報を暗号化して身代金を要求するといった攻撃等も確認され、その手法も多様化してきている。こうした外部からの攻撃に対する防御については、2016年度のシステム刷新により、一層の対策強化を実現しているところだが、更に新たな手法による攻撃に備えた対策強化への取組が必要となる。

他方、外部からの攻撃のみならず、情報セキュリティインシデントにつながる恐れのある過失を防止するため、組織内部に向けた取組も必要である。

こうした状況の中、本年１月の行政情報システム刷新（以下、「システム刷新」という。）による情報セキュリティ対策の抜本的強化を図ったところであり、また、CSIRT要員に対する研修を開催して省内職員の情報セキュリティにおけるリテラシー向上等にも努めてきたところである。これらを踏まえて、2017年度は主に以下の取組を行う。

(1) 情報セキュリティに関する教育について、情報セキュリティポリシーの改定及びシステム刷新を踏まえた教育コンテンツの改善など、内容の充実
(2) 情報セキュリティ対策の自己点検について、システム刷新による利用状況の確認と点検等の実施
(3) 情報セキュリティ監査について、リスクの高い情報システムを中心とした脆弱性診断等の実施
(4) 情報セキュリティに関する技術的な対策を推進するための取組について、セキュリティインシデント等に関する検知能力の強化
(5) その他、情報セキュリティポリシーの改定、システム刷新等を踏まえた関連規程の見直し。

厚生労働省

2016年度の総合評価・2017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　岡崎 淳一

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。

このような状況のなか、一昨年５月に日本年金機構（以下「機構」という。）における情報流出事案が発生し、当省においては「情報セキュリティ強化等に向けた組織・業務改革」（2015年９月18日）（以下「再発防止策」という。）を策定し、当省及び所管する独立行政法人等及び特殊法人（以下「所管法人等」という。）における情報セキュリティ対策の強化とともに、機構への指導監督強化に取り組んでいるところ。

2016年度においては、この再発防止策に基づく取組として、主に以下の対策に取り組んだ。

- 情報セキュリティ対策に関する司令塔機能強化のための組織再編
- CSIRTへの緊急・専門的支援等の業務委託
- 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（６月）の実施
- 当省及び所管法人等の個人情報等の重要情報を取り扱うシステムに係るリスク評価
- 当省及び所管法人等に対する情報セキュリティ監査
- 機構における再発防止に向けた取組を着実に進めるための機構に対する指導監督の強化

これまでの取組によって組織・業務的な改革については一定の成果を得たことから、2017年度においては、これまで実施した

- 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（６月）の実施
- 機構における再発防止に向けた取組を着実に進めるための機構に対する指導監督の強化について、対策を維持しつつ、
- 情報セキュリティ対策への支援強化（業務委託）
- 当省及び所管法人等の個人情報等の重要情報を取り扱うシステムに係るリスク評価
- 当省及び所管法人等に対する情報セキュリティ監査

については、内容や対象範囲を見直し、更なる対策の強化を図る。

農林水産省

2016年度の総合評価・2017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　荒川　隆

2016年度は、国内外において、パソコンに保存されているファイルを暗号化し、復号のための金銭を要求するランサムウェアが多く確認されたほか、国内においては、大手旅行会社、研究機関等を狙った標的型攻撃や、ソフトウェアの脆弱性を悪用した不正アクセスによる情報漏えいなど、依然として、官民問わずサイバー攻撃による被害が発生している状況である。

このような中、農林水産省においては、標的型攻撃、サービス妨害攻撃への対策強化や、仮想化技術による機微情報のインターネット分離等を講じたLANシステムの安定稼働を図るとともに、2016年４月１日付けで大臣官房に設置されたサイバーセキュリティ・情報化審議官の下、情報セキュリティに関する教育の実施や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、情報セキュリティインシデントへの迅速かつ適切な対処等に努めてきたところである。

2016年３月には、サイバーセキュリティ戦略本部において、サイバーセキュリティ人材育成総合強化方針が決定されたことを踏まえ、情報セキュリティ対策及び情報システムの適切な運用管理を行う体制を強化するため、2016年８月に農林水産省セキュリティ・IT人材確保・育成計画を策定したところである。

また、2016年８月に政府機関の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）が改定されたことから、2017年３月に農林水産省における情報セキュリティ関係規程についても統一基準群に準拠するよう必要な改正を行ったところである。

これらの状況を踏まえ、2017年度においては、2016年度に改正した情報セキュリティ関係規程に基づき、情報セキュリティの確保を図りつつ、情報セキュリティに関する教育やCSIRT構成員等に対する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の実施、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等に取り組むものとする。

また、インターネット分離の対象範囲を拡大し、霞が関の働き方改革を加速するための重点取組方針、統一基準群等を踏まえ、情報セキュリティの確保されたICT環境の整備に関する検討を進めるとともに、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、より一層の情報共有を行うほか、発生した情報セキュリティインシデントへの迅速かつ適切な対処等に努めるものとする。

経済産業省

2016年度の総合評価・2017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

2016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）は活発化し続け、対象や手法の多様化、規模の拡大の様相を呈した。
こうした中、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引き続き求められることから、2016年度には主に次の取組を実施した。

(1) 基幹OAシステムにおいて、インターネット分離の実現やウイルスメール対策機能の強化など、セキュリティ対策を実施
(2) 2017年度に予定している基幹OAシステムの更改に向け、サイバー攻撃対策等に関して現在以上の水準とするべくセキュリティ要件を決定
(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、体制の整備、有為な人材の確保、橋渡し人材向け研修受講の促進、一般職員のリテラシー向上のための研修、訓練等を実施
(4) 2016年８月の「政府機関の情報セキュリティ対策のための統一基準群」の改正を受け、経済産業省情報セキュリティ管理規程、経済産業省情報セキュリティ対策基準等を全面的に見直し、改正
(5) 省全体としてのインシデント・レスポンス体制・機能の更なる強化として、NISCの実施するCSIRT訓練、NATIONAL 318 EKIDEN、各種研修等に参加

2017年度においては、2018年２月に運用開始を予定している当省の次期基幹OAシステムについて、更なるセキュリティ向上を図るべく設計・構築等を進める。あわせて、従来からの取組も引き続き行い、当省全体の情報セキュリティ対策を継続的に強化していく。具体的には以下の通り。

(1) 基幹OAシステムの更改に伴うセキュリティ対策の強化
(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再確認と対策の更なる強化
(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) 監査や自己点検を通じた、各部局や職員一人一人の情報セキュリティに係る体制の強化、意識の向上
(5) セキュリティ水準を維持向上するための管理運用制度の見直し

国土交通省

2016年度の総合評価・2017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　藤田　耕三

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、その傾向は、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、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、内閣官房内閣サイバーセキュリティセンター（NISC）と連携して、政府機関の情報セキュリティ対策のための統一基準を踏まえた情報セキュリティ対策を実施している。

具体的には、2016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、サイバーセキュリティ・情報化審議官を新設

② 統一基準群の改定を踏まえ、国土交通省情報セキュリティポリシーを改正するとともに、サイバーセキュリティ人材育成総合強化方針を踏まえ、国土交通省セキュリティ・IT人材確保・育成計画を策定

③ 職員に対し、標的型メール攻撃訓練、情報セキュリティ対策の自己点検、研修を実施するとともに、職員が守るべき事項を記載した「国土交通省情報セキュリティハンドブック」を作成

④ NISCによる国土交通省に対するマネジメント監査及びペネトレーションテストに協力するとともに、NISCによるインシデント対処訓練及び情報通信研究機構（NICT）によるサイバー防御演習（CYDER）に参加

⑤ 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連絡会議の創設、航空及び鉄道分野のセプター事務局の国土交通省から民間団体への移行、所管する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

2017年度においては、サイバー攻撃の変化等の状況を踏まえ、情報管理の徹底などセキュリティポリシーの周知徹底を図るとともに、研修等を通じた職員への教育の充実等を推進する。

環境省

2016年度の総合評価・2017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　森本　英香

2015年５月に判明した日本年金機構に対する標的型メール攻撃による情報流出事案以降も、公開サーバに対するDDoS攻撃やWebサイトの改ざんなど国内の組織を標的としたサイバー攻撃が増加しているなか、安全な情報提供及び情報システムの利用をするために「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日改定　サイバーセキュリティ戦略本部決定）に基づき「環境省情報セキュリティポリシー」(以下「ポリシー」という）を改定した。また、当該ポリシーに基づき体制の強化、セキュリティ対策の充実、セキュリティに関わる教育を実施してきたところであるが、2016年度も環境省職員がWeb閲覧中に不審なサイトへ誘導される、独立行政法人に大量の不審なメールが送りつけられるなどのセキュリティ事案が発生している。

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「新システム」という）し、これまでのシステムにおける課題（サイバー攻撃への対処の迅速化、機微情報の安全性の向上等）を解決するために、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「多重防衛」を備えたシステムとして構築している。2017年度は新システムの機能・環境の有効利用を進める。

また、職員等に対する教育等を引き続き実施し、ポリシー等の理解度向上、サイバー攻撃の脅威と対策実践の徹底を図っていく。

更に、「政府機関の情報セキュリティ対策のための統一基準群」に基づくポリシーの改定に伴い、その適用範囲が独立行政法人等に拡大したことを踏まえ、環境省としても所管する独立行政法人等との連携並びに指導等を引き続き強化する。

防衛省

2016年度の総合評価・2017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　髙橋　憲一

2016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、2017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「サイバーは　一人ひとりが　最前線　～あなたの情報、狙われています～」とし、全職員に対して、自らが取り扱う情報の格付けや共有範囲の再認識、関連規則の再確認を行わせるとともに、標的型攻撃メールによる情報流出等の脅威の認識や対策の教育を行った。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。

2017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。2018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、脆弱性検査等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、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、官民連携の取り組みを引き続き実施する。

（本ページは白紙です。）

別添２　「サイバーセキュリティ 2016」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

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 2016	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 29 年度予算重点化方針」（平成 28 年 8 月 31 日サイバーセキュリティ戦略本部決定）において、「安全なＩｏＴシステムのためのセキュリティに関する一般的枠組」を踏まえることや、ＩＴ利活用等を目指す施策についても、セキュリティ・バイ・デザインの考え方を盛り込むことに留意することを示した。 ・また、セキュリティ・バイ・デザインの取組が行われていることの確認等を行う研究開発戦略専門調査会の委員を１名追加し、体制の強化を行った。

(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 2016	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。	・研究開発戦略専門調査会における議論等を通じ、2016 年８月に、安全な IoT システムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにした「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」を策定した。 ・また、「安全な IoT システム創出のためのセキュリティワーキンググループ」を発足し、具体的な取組の内容の検討を行うための体制を整えた。

(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 2016	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取りまとめ、普及に努める。また、総務省及び経済産業省において、当該ガイドラインを踏まえ、IoT セキュリティの確保に向けた総合的な対策を行うための実証事業を実施する。	・総務省及び経済産業省において、IoT 推進コンソーシアムを通じて、IPA 及び NICT と連携しつつ、2016 年 7 月に IoT セキュリティガイドラインを策定した。 ・総務省においては、2017 年 1 月から「サイバーセキュリティタスクフォース」を開催し、2017 年 4 月に IoT セキュリティ対策に関する提言として、「IoT セキュリティ対策の取組方針 ver1.0」を公表。 ・なお、経済産業省においては、IPA を通じて、同開発指針が産業間の情報連携においても有効であることを実証するため、ORiN 協議会、(一社)エコーネットコンソーシアム及び神奈川工科大学と協力し、産業分野間（FA 機器－HEMS）の情報連携に関する実証実験を実施した。「つながる世界の開発指針」を基に、４製品分野（車載機器、IoT ゲートウェイ、金融端末（ATM）、決済端末（POS））においてセキュリティガイドラインが策定されるなど、普及展開にも努めた。
(イ)	厚生労働省	厚生労働省において、医薬品医療機器法上の医療機器のサイバーセキュリティについて、今年度を目途にガイドラインを策定する。	・医療機器メーカ、医療機関、ICT の専門家などからなる医療機器のサイバーセキュリティに関する研究班を設け、サイバーリスクの分析、海外での対応状況の調査、国内医療機器産業へのサイバーセキュリティの考え方の普及方法等の検討を行い、医療機器のサイバーセキュリティ確保のためのガイダンスをとりまとめている。現在、完成に向けて最終調整をしている。

（ウ）	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。	・CSSC において、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に関して、海外機関との情報共有を行った。
（エ）	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。	・JPCERT/CC において、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 74 件について、その保有組織に対して情報提供した。
（オ）	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関連情報届出受付に係る制度により、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、利用者に提供し、脆弱性が届出されたものの連絡がつかない案件については、経済産業省告示に基づき、引き続き公表を行う。また、これまで対象としていなかった案件の取扱いについては、法令に基づき、検討を進める。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。	・ソフトウェア製品開発者との間の調整が整わず公表に至らなかった脆弱性情報に関する案件も一定の要件のもとで公表を行うため、経済産業省において、2017 年２月に、「ソフトウェア等脆弱性関連情報取扱基準」を廃止し、「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」を制定した。2016 年度は、IPA においてソフトウェア製品について 1,032 件、ウェブアプリケーションについて 341 件の届出を受理し、IPA 及び JPCERT/CC において、197 件の脆弱性情報を公表した。また、JPCERT/CC において、海外研究者からの国内開発者との調整依頼や、事案で悪用された検体分析の結果発見したゼロデイ脆弱性の調整・公表を行った。

(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 2016	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。	・AIST において、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。ソフトウェア工学については、民間企業との共同研究において自動車やスマート工場を題材にした研究課題の洗い出しおよび実証実験環境の整備を行った。暗号技術においては、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解読に関する世界記録を更新し、得られた知見をもとに、格子暗号の実用化に向けた最大の障害である公開鍵サイズを 90%削減する技術を開発した。
（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。	・「IoT 推進のための横断技術開発プロジェクト」の事業で、セキュリティ対策等に関する研究開発を採択し、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を開発し、評価・認証制度やサイバー演習へと活用する。	・CSSC において、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行った。
（エ）	経済産業省	経済産業省において、自動車のセキュリティ確立に向けて、自動車業界関係者等と制御システム等に関するセキュリティ上の課題と対策について情報交換を行い、解決に向けた方向性を得るとともに研究開発を推進する。	・経済産業省において、内閣府 SIP（戦略的イノベーション創造プログラム）と連携しつつ、自動車のセキュリティに関して、脅威分析ツールの仕様を策定するとともに、車両や車内ネットワーク、部品に対する評価手法、および評価基準の検討を行った。また狭域通信における署名検証の簡略化手法を開発した。
（オ）	総務省	総務省において、脆弱性を有するブロードバンドルータ等の IoT 製品について、ISP 事業者等 を通じ利用者に対策を促す仕組みの構築に向けた取組を進める。	・総務省においては、2017 年 1 月から「サイバーセキュリティタスクフォース」を開催し、2017 年 4 月に IoT セキュリティ対策に関する提言として、「IoT セキュリティ対策の取組方針 ver1.0」を公表。また、2016 年度に脆弱性を有する IoT 製品の調査を実施するとともに、特に脆弱性を有するブロードバンドルータに関しては実態調査及び利用者への注意喚起を実施した。

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 2016	取組の成果、進捗状況
(ア)	内閣官房 金融庁	内閣官房及び金融庁において、上場企業におけるサイバー攻撃によるインシデントの可能性等について、米国の証券取引委員会（SEC）における取組等を参考にしつつ、事業等のリスクとして投資家に開示することの可能性を検討し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。	・普及啓発・人材育成専門調査会の下に設置されている、セキュリティマインドを持った企業経営 WG を通じて、情報発信のあり方を含め、企業経営のためのサイバーセキュリティに係る基本的な考え方を検討。内閣官房において、その議論を踏まえて、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」のとりまとめを行った。 ・さらには、内閣官房において、経営層の認識、情報発信の状況や関連する制度面の課題等の把握を務めるため、企業のサイバーセキュリティに関する調査を行った。
(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。	・説明会にて経営者がリーダーシップをとってセキュリティ対策を行うことの重要性について説明を行うことで、サイバーセキュリティ経営ガイドラインの普及促進を図った。 ・また、IPA を通じて、サイバーセキュリティ経営ガイドラインの解説書を公開（2016 年 12 月）し、サイバーセキュリティ経営ガイドラインの内容を実施する上でのポイントとなる情報を提示することによって、より一層の企業への定着を図った。
(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。	・攻めの IT 経営銘柄の評価項目の中にもサイバーセキュリティ経営ガイドラインで要求している項目を組み込むことで、セキュリティへ取り組む企業へのインセンティブ策を講じた。 ・また、サイバーセキュリティ保険を提供している損保会社が中小企業への割引を適用できるよう IPA、損保会社等の関係者とセキュリティアクションの枠組を構築した。

(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 2016	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、経営層と実務者層の間をつなぐ「橋渡し人材層」が活躍できるよう、経営層の示す経営方針を踏まえたサイバーセキュリティに係るビジョンの策定能力や、こうしたビジョンを経営層及び実務者層に提案したり、意思疎通を図る能力の向上を推進するための方法の開発等を実施する。	・企業の経営層に対し、2016 年 8 月に策定した「企業経営のためのサイバーセキュリティに係る基本的な考え方」を各セミナー等で説明したほか、内閣官房主催のシンポジウムにて、ＩＴの利活用による新しい価値の創造における経営層、橋渡し人材層、実務者層の役割や人材育成等、企業が直面しているサイバーセキュリティの課題やその対応について解説・議論した。

(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 2016	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。	・JPCERT/CC において、アプリケーションセキュリティに関する業界ベストプラクティス文書を多数公開している団体 OWASP のセキュア開発に関するドキュメントのうち, OWASP Cheat Sheet 集および OWASP ASVS（アプリケーションセキュリティ検証標準）の翻訳・公開を行った。

（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。	・説明会にて経営者がリーダーシップをとってセキュリティ対策を行うことの重要性について説明を行うことで、サイバーセキュリティ経営ガイドラインの普及促進を図った。 ・また、IPA を通じて、サイバーセキュリティ経営ガイドラインの解説書を公開（2016 年 12 月）し、サイバーセキュリティ経営ガイドラインの内容を実施する上でのポイントとなる情報を提示することによって、より一層の企業への定着を図った。中小企業においても経営者が自らの責任で対応すべき事項を示した「経営者編」と、重要な情報を管理する責任者が実施すべき事項を示した「管理実践編」に分けて解説している、「中小企業の情報セキュリティ対策ガイドライン」を公表し普及促進を図った。
（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発注者が把握できない多重の再委託などを防止し、情報システム開発・運用に係る取引の適正化を図るための制度整備を行う。	・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た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を 2017 年 3 月に公表した。
（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。	・JPCERT/CC は、日本シーサート協議会の運営委員および事務局業務を通じ、協議会加盟組織数の拡大を図り、国内組織における CSIRT の活動を促進・支援している。同協議会の加盟組織数は 2016 年度当初の 137 組織から 219 組織に拡大した。 ・また、早期警戒情報の受信対象組織の拡大を図ることにより情報提供による国内組織の CSIRT の活動に対する促進・支援をおこなった。早期警戒情報の受信組織数は 2016 年度は 234 組織から 343 組織に拡大した。さらに、早期警戒情報の受信組織を対象に、脅威や攻撃に関する分析情報や各組織の取組み事例等の情報交換を行う目的で、情報交換会を 2016 年度に 4 回実施している。
（オ）	総務省	総務省において、NICT 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 年東京オリンピック・パラリンピック競技大会に向けた大規模演習環境「サイバーコロッセオ」を活用し、同大会のサイバーセキュリティを守る高度な人材の育成を推進する。	・実践的サイバー防御演習（CYDER）について、2016 年度より、地方公共団体等を演習の主たる対象として追加するとともに、技術的知見を有する NICT を実施主体として、約 1500 名に対し演習を実施した。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、大会開催時を想定した模擬環境で攻撃・防御双方の実践的な演習（サイバーコロッセオ）を実施した。
（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標的型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。	・ＣＳＳＣにて、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 138 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。	・IPA において、2016 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 120 件行うとともに、うち 17 件に対してオンサイトでレスキュー活動を実施した。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 132 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実施する。	・金融庁において、2016 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、金融業界横断的なサイバーセキュリティ演習（Delta Wall）を実施し、金融機関 77 社が参加。
（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。	・IPA において、企業に対し広く iLogScanner の紹介を行い、2016 年度のダウンロード数は 4,561 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 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）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。	・IPA における J-CSIP の情報共有活動については、着実に運用を継続。2016 年度は 2,000 件を超える情報提供を受け、うち 200 件程度を標的型攻撃メールと判定。情報の集約と分析を行い、100 件程度の情報共有を実施。また、一部、STIX 等の機械処理可能な形式での情報共有も試行した。 ・J-CSIP の参加組織は 2015 年度末時点の 72 組織から、86 組織へと一層拡大した。
（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、サイバー攻撃に関する情報共有網の拡充を進める。	・2016 年 7 月に正式に活動を開始した「ICT-ISAC」は、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。
（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・提供及びこれを踏まえた取組みの高度化（脆弱性情報の迅速な把握・防御技術の導入等）の意義について、周知すること等により、2017 年３月末現在、「金融 ISAC」の加盟社は 271 社（正会員）まで増加した。

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 2016	取組の成果、進捗状況
（ア）	経済産業省	経済産業省において、NEDO 等の支援事業や政府系ファンドによるベンチャー企業や国内外で大規模に活躍できる企業の育成など、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、サイバーセキュリティ産業の活性化に向けた検討に着手。
（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の普及促進を行う。	・クラウド事業者の参加するセミナーにおいて、CS マークの一層の取得に向けて呼びかけを行うなど、普及・促進を図った。また、JIPDEC において開始した、ISMS クラウドセキュリティ認証においても、認証の要求事項に内部監査についての内容が盛り込まれており、実質的な促進が図られている。
（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。	・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た特利制度を創設した。また、引き続き、中小企業投資促進税制において、セキュリティ製品等の税制措置を継続した。
（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、時代の変化に柔軟に対応できる権利制限規定の在り方について検討を行っているところであるが、当該検討の中で、セキュリティ目的も含めたリバースエンジニアリングのための著作物利用に係る課題についても検討を行っている。

(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 2016	取組の成果、進捗状況
（ア）	経済産業省	経済産業省において、産業界と協力し、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、関係省庁とも連携し「営業秘密官民フォーラム」を開催する。	・2016 年６月 15 日第２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～」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～企業の価値向上に向けて～」についての普及啓発を図った。また、2016 年 12 月にハンドブックを活用してもらえるようにまとめたパンフレット「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～」を策定した。
（ウ）	経済産業省	経済産業省において、IPA を通じて、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。	・2017 年 1 月に、内部不正防止ガイドライン第３版を改訂し、第３版公開以降になされた法改正、策定されたガイドラインの内容とも整合させた第４版を公開した。 ・企業の営業秘密保護に関する実態調査を実施し、2017 年３月に報告書を公開した。 ・営業秘密保護に関する官民連携フォーラムにおける情報共有推進のため、フォーラム参加 24 組織（79 メーリングリスト）に向けたメールマガジンを９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、セミナー等において普及促進を図った。
（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。	・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計画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 2016	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、ITU-T SG17 会合（2016 年８月、2017 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。 ・経済産業省において、ISO/IEC JTC1/SC27、ITU-T SG17 等が主催する国際会合での議論を参考とし、総務省・経済産業省・IoT 推進コンソーシアムで作成した「IoT セキュリティガイドライン」の国際標準化提案を視野に入れた検討を行った。
（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。	・IPA において、WG2 コンビーナ、WG3 副コンビーナ（2016 年４月フロリダ会合、2016 年 10 月アブダビ会合）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、日本から公開鍵暗号（1 件）や軽量メッセージ認証方式（１件）が提案されており、規格化への支援を行っている。公開鍵暗号は、2017 年度に規格化見込みである。
（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。	・IPA において、脆弱性対策に関しては、NIST 脆弱性対策データベース NVD と JVN iPedia との連携、CVSS バージョン 3 への対応など、持続的に、脆弱性対策情報の発信と共に、対策基盤の整備を推進した。 ・インシデント対応との連携強化を図るため、脅威情報構造化記述形式 STIX の普及啓発を推進した。 ・国際的な標準化活動等に関しては、ISO/IEC 29147 脆弱性情報の開示、ISO/IEC 30111 脆弱性対応手順の改訂への対応、ISO/IEC 19770-2 ソフトウェア識別子の JIS 化対応などを推進した。

（エ）	経済産業省	経済産業省において、IPA による CCRA などの海外連携を通じ、セキュリティ評価に係る国際基準の作成や各国の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。	・IPA において、IEEE 策定の PP に準拠した認証を 2016 年度で 26 件発行した。 ・米国と共同で開発した MFP の PP（ Protection Profile for Hardcopy Devices）の JISEC における PP 認証申請及び当該 PP に適合する MFP の製品認証申請受付を実施した。
（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。	・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ため、2016 年８月にモンゴル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、2017 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。	・HIDA 研修を活用し、2017 年２月 14 日～23 日に ASEAN ８か国（シンガポール、ブルネイ除く）を対象とした訪日研修「地域の重要インフラ関係者に対する情報セキュリティ強化支援研修コース」を実施。ASEAN 諸国の官民関係者に対し、重要インフラ防護の実際について最新動向等について知見を提供した。
（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。	・ミャンマーにおいて海外セキュアコーディングセミナーを実施すべくミャンマーmmCERT と調整中。
（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。	・CSSC において、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に関して、海外認証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 2016	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。	・JPCERT/CC において、アプリケーションセキュリティに関する業界ベストプラクティス文書を多数公開している団体 OWASP のセキュア開発に関するドキュメントのうち, OWASP Cheat Sheet 集および OWASP ASVS（アプリケーションセキュリティ検証標準）の翻訳・公開を行った。
(イ)	経済産業省	経済産業省において、IPA を通じて流通後の修正が容易でないとされる組込みソフトウェア及びスマートフォン等のアプリケーションにおいて多用される言語に関し、IPA において整備したコーディングスタンダードについて、更なる開発の高信頼化を図るための取組等を行う。	・IPA において、2016 年 10 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++版）Ver2.0 を出版し、PDF ファイルを Web 公開するとともに、同ガイドの英訳版の PDF ファイルについても Web 公開した。
(ウ)	経済産業省	経済産業省において、IPA を通じて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」について集合教育用の機能拡張を行うことで更なる普及啓発を図る。	・IPA において、既存の個人学習向け機能の拡張と新規に集合学習向け機能をサポートした AppGoat の開発を行い、2017 年 2 月に公開した。公開後一ヶ月で 200 件以上の利用申請があった。
(エ)	経済産業省	経済産業省において、IPA を通じて、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が社会に与える混乱や被害を防止する観点から、更なる開発・検証技術の高度化を図りつつ、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、利用者への品質説明力を強化する。	・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 26 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。 ・ソフトウェアの品質について説明力の強化を図るため、26 団体・機関に 2016 年度までに発行した関連するガイドライン等を紹介するとともに、現場への適用を依頼した。
(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関連情報届出受付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。	・脆弱性情報公表に係る制度については、着実に運用を継続して実施した。2016 年度は、IPA においてソフトウェア製品について 1,032 件、ウェブアプリケーションについて 341 件の届出を受理し、IPA 及び JPCERT/CC において、197 件の脆弱性情報を公表した。 ・「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、2016 年度においては、脆弱性対策情報を約 7,900 件（累計：約 67,000 件）公開した。また、IPA において、脆弱性対策情報の公開件数増加や CVSSv3 などに対応するため、ハードウェア増強を含めたソフトウェア開発に着手した。
(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。	・JPCERT/CC において、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。	・IPA において、普及・啓発活動として、情報セキュリティ EXPO 等での講演、および、「ファジング活用の手引き」「ファジング実践資料」の改訂版の公表、「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。	・リフレクション型 DDos 攻撃観測センサなどの、新たな攻撃観測用センサを用いた観測技術を開発した。 ・また、地方自治体の DAEDALUS への加入を進め、約６００の自治体へアラート提供を実施した。

(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（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。	・JPCERT/CC において、インターネット定点観測情報共有システム（TSUBAME）を運用しており、2016 年度は香港の政府系 CSIRT である GovCERT.HK が新規に加盟した。 ・また、日本で開催した APCERT の年次総会において、主に TSUBAME 参加組織に対してワークショップを実施するとともに、香港の 2 つの CSIRT に対してトレーニングを行い、エンジニア向けに TSUBAME データを用いた分析手法を共有した。 ・さらに、中東・アフリカ地域の National CSIRT が加盟する OIC-CERT に対して TSUBAME 加盟に向けた取組を実施した。 ・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。
(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。	・フィッシング対策協議会において、2016 年度は 249 ブランド、3559 件の URL について、6656 件の報告を受けた。これら届出を受けたフィッシングサイトについて JPCERT/CC と連携しサイト閉鎖を依頼している。JPCERT/CC では、国内外からフィッシングサイトの情報提供をうけ 、2016 年度は、2,337 件のフィッシングサイト閉鎖の対応を行った。そのうち 80%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。 ・またフィッシング対策協議会では、サービス事業者および消費者に向けフィッシング対策の普及と啓発を図るため、フィッシング対策ガイドラインの改定版およびフィッシングレポート 2016 を 2016 年 5 月にそれぞれ公開した。
(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。	・IPA において、「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 1,000 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。	・警察庁において、「Wi-Fi 提供者向けセキュリティ対策の手引き」の改訂等を踏まえ、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の考え方について都道府県警察へ通知した。
(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。	・2016 年８月に Wi-Fi アクセスポイント設置者向けの手引きの改定を実施。また、普及啓発セミナー及び総務省 HP「国民のためのセキュリティサイト」における周知啓発を実施。

(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 2016	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」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。	・例年通り２月１日～３月 18 日をサイバーセキュリティ月間として、イベントの開催をはじめとした様々な取組を実施した。 ・２月１日に、キックオフシンポジウム「ＩｏＴ時代のサイバーセキュリティ―次世代のビジネスを支えるサイバーセキュリティ―」を開催し、企業が直面するサイバーセキュリティの課題やその対応について解説・議論を行った。 ・「新・情報セキュリティ普及啓発プログラム」（2014 年７月 10 日）において、「情報セキュリティ対策の重要性を広く国民一人一人に訴求していく手法として、国民に親しみやすいメディア（コミック、ソング等）の影響力に着目し、これらを取り扱う事業者やクリエイター等と連携した取組も効果的であると期待」とあり、本月間において「劇場版 ソードアート・オンライン －オーディナル・スケール－」とタイアップを行うことで、国民に対して広くサイバーセキュリティに関する普及啓発強化を図った。
(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 2016 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。 ・セキュリティ・ポータルサイト「@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。 ・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、2016 年 10 月のサイバーセキュリティ国際キャンペーン及び 2017 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。	・総務省及び経済産業省において、電子署名の利用促進に関するセミナーの開催等を通じて、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 1,755 件実施。また、2016 年度より低年齢のネット利用に対応して対象学年の引き下げ及びフィルタリングについての説明に特化した講座である e-ネットキャラバン Plus を新設。

（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。	・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を全国で 10 か所及びフォーラムを全国 2 か所で実施した。
（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（全国７か所：東京での全国フォーラムを含む）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、全国 7 か所において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。	・IPA が提供している「情報漏えい対策ツール」は、民間のダウンロードサイトを活用して、2016 年度においては 9,352 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、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。	・IPA において、情報モラル・セキュリティコンクールを開催。2016 年度は、学校単位で情報モラル・情報セキュリティを促進させるため、従来からの賞に加えて文部科学大臣賞を設け、授与した。 ・全国の小中高生から、標語 52,022 作品、ポスター 4,925 作品、４コマ漫画 8,849 作品の応募があった。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。	・2016 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、会員団体の取組を報告と、普及営発活動に関する意見交換を行った。 ・また、2016 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、サイバーセキュリティ月間 2017 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。	・IPA において、全国各地域で、NPO 等の団体との連携により「インターネット安全教室」を合計 84 回開催し、小中高校生からシニア層まで合計約 4,800 名が参加した。 ・各地域団体による講習能力の向上を図る講師トレーニングを全国 5 箇所において開催し、合計約 120 名が参加した。
（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。	・広く企業及び国民一般に情報セキュリティ対策を普及するため、IPA において、セミナー等への講師派遣（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（仮称）」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「iSupport」等のツール等の利用促進等を図る。	・「講習能力養成セミナー」を全国 29 箇所において開催し、中小企業の経営者、社内教育担当者等合計約 1,550 名が参加した。 ・また、中小企業団体との連携により、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を構築するとともに、「中小企業の情報セキュリティ対策推進シンポジウム」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 iSupport 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。	・IPA 及び JPCERT/CC において、一般国民や中小企業者等に対し、脆弱性対策情報の公表や注意喚起等を行った。 ・IPA においては、具体的に、「緊急対策情報」を 17 件、「注意喚起情報」を 27 件、「安心相談窓口だより」を 17 件公表した。

（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。	・情報セキュリティ安心相談窓口では、電話、メール、FAX 等で 15,629 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情報提供と相談を 519 件実施した。これを通じて、不審メールを 1229 種類入手した。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。	・IPA において、国民全体に向けた活動として、2016 年７月に、情報セキュリティ白書を発行した。 ・また、2016 年 12 月に「情報セキュリティ脅威と倫理に関する意識調査、（2016 年版）、2017 年３月に「サイバーサプライチェーンリスク管理に関する課題抽出調査」を実施し、報告書を公開した。 ・民間事業者に向けた活動として、2016 年 12 月にサイバーセキュリティ経営ガイドライン解説書を作成、公開し、普及啓発を行った。

(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 2016	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、JC3 と連携して、ウイルス感染を目的とした改ざんサイトの対策等を実施した。 ・「コミュニティサイトに起因する児童被害防止のための官民連携の在り方」をテーマに平成 28 年度総合セキュリティ対策会議を開催し、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、ウイルス対策ソフト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。特に、平成 28 年７月からは、ウェブブラウザ事業者等が加盟する国際的な団体である APWG への情報提供も開始した。

（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。 ・2016 年中の不正アクセス行為の発生状況等を 2017 年３月 23 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、平成 28 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、2016 年末現在の全国のサイバー防犯ボランティア数は、202 団体 8,598 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 を監修し、ホームページで公開するとともに、都道府県警察で活用するなど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。	・フィッシング対策協議会において、米国 APWG と連携し、同組織およびその会員との情報交換を継続的に実施するとともに 2016 年度は、APWG が主催するカンファレンスである APWG eCrime 2016 （2016 年６月１日−３日 トロントにて開催）に参加し、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。 ・これらの活動で収集した情報を踏まえ、フィッシング対策ガイドラインの改定に着手した。

（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、2016 年においては、1,520 件（2015 年比約 60%増）の不正プログラムを解析した。 ・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）が施行されたことを踏まえ、そ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 2016	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３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。また、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い検討を進め、行動計画の見直しについて 2016 年度内を目途に結論を得るとともに、早急に対処すべき事項については、行動計画の見直しを待たずに対処する。	・第３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（イ）、「情報共有体制の強化」については本項目、(1)(ア)、(2)(ア)・(エ)、(3)(ア)・(キ)、「障害対応体制の強化」については(オ)、「リスクマネジメント」については本項目、「防護基盤の強化」については(1)(ア)に取組の詳細を記載）。 ・行動計画の見直しについて、ロードマップに従って検討を進め、2017 年３月の重要インフラ専門調査会において結論を得た。 ・具体的には、第３次行動計画の５つの施策群ごとの分析的な評価、第３次行動計画全体としての総合的な評価を行った。 ・上記の評価を踏まえ、第４次行動計画においては、機能保証の考え方を盛り込み、情報系（IT）に限らず制御系（OT）を含めた取組が必要であることから「IT 障害」という用語を「重要インフラサービス障害」に改め、取り組むべき施策として、オリパラ大会も見据えた情報共有体制の強化等を盛り込んだ。 ・早急に対処すべき事項として、情報共有範囲の拡大（(1)(ア)参照）を行ったほか、重要インフラサービス障害の深刻度判断基準、「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、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むべき要点等に関して、それぞれ検討を開始するなど、第４次行動計画の決定前に対応している。
（イ）	内閣官房	内閣官房において、各重要インフラ分野における安全基準等について、強制基準やガイドライン等の体系を明らかにする調査を引き続き実施し、当該調査結果を踏まえ、安全基準等の体系を明示した調査項目を加えた安全基準等の改善状況調査を実施し、継続的に課題の抽出を行う。	・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 2017 年３月の重要インフラ専門調査会に報告した。 ・重要インフラ分野ごとの関係法令の解釈に関する所管省庁との認識合わせを通じて、関係法令による義務的な報告が着実に行われていることや、ガイドラインによる補完的な報告が行われていることを確認した。 ・これらを踏まえ、所管省庁と業法・ガイドラインによる報告のレベル感を確認しつつ、今後の方針について検討を行い、第４次行動計画においては、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定として位置付けることや、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旨を記載した。
（ウ）	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、申告受付の夜間・休日の全国一元化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、2016 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行い、また、同施設のセンサ 21 か所を 2016 年度内に更改した。 ・競技施設等の比較的狭いエリアの電波監視に適した電波監視技術について、実証試験を実施した。

（エ）	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。	・2015 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、2016 年７月に公表した。 ・「情報通信ネットワーク安全・信頼性基準 」等について、上記の事故の発生状況の分析結果や、有識者からの意見を踏まえ、2016 年度の見直しは不要であるとの結論を得た。
（オ）	内閣官房 総務省 経済産業省 金融庁	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 ・ 内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施する。 ・ 総務省において、NICT 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実施する。	・内閣官房が主体となり、分野横断的演習を実施（2016.12.7）し、約 500 組織、約 2,000 名が参加。東京会場、地方会場、自職場の参加形態を用意して参加機会の拡大を図るとともに、最新の攻撃トレンドを加味しつつ多様な参加者への適合と CSIRT アクションを盛り込んだシナリオを用意。サブコントローラーの活用による自社環境に即したインシデントハンドリングを実現するなど、演習環境・内容の改善に取り組んだ。 ・総務省において、NICT を通じ、重要インフラ事業者等に対するサイバー攻撃について実践的な演習を実施した。 ・経済産業省において、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、CSSC を通じて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 138 名が参加した。 ・金融庁において、2016 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た、金融業界横断的なサイバーセキュリティ演習（Delta Wall）を実施し、金融機関 77 社が参加。
（カ）	経済産業省	経済産業省において、我が国の重要インフラのサイバーセキュリティ対策を抜本的に強化するため、重要インフラのサイバー攻撃に対する防御力を確認し、事業者の意識を喚起するとともに、今後重要インフラ対策の中核を担う人材育成や技術開発を行う体制を強化する。	・IPA を通じて、重要インフラ事業者のサイバー攻撃に対する防護力の確認等の取り組みを推進。 ・IPA において、重要インフラにおけるサイバーセキュリティ中核人材を育成する機関「産業サイバーセキュリティセンター」の設立に向けた体制整備や、センターで提供するカリキュラムについて調整を行った。

(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 2016	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３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、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、重要インフラに係る防護範囲の見直しについて検討を進め、行動計画の見直しについて 2016 年度内を目途に結論を得るとともに、早急に対処すべき事項については、行動計画の見直しを待たずに対処する。	・セプター構成員の拡充及び中小事業者を含めたセプター構成員以外への NISC からの情報提供を複数分野において開始した。さらに、核物質防護等の措置が要求される企業を含め、重要インフラ分野に属さない事業者等への内閣官房からの情報提供も開始した。 ・また、第４次行動計画においては、「面としての防護」を実現するための防護範囲見直しの取組を継続していく旨を記載した。

(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 2016	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、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、サイバー攻撃に対する体制強化のため、情報共有の強化について検討を進め、行動計画の見直しについて 2016 年度内を目途に結論を得るとともに、早急に対処すべき事項については、行動計画の見直しを待たずに対処する。	・情報連絡手順の整備や情報連絡様式の改良等、円滑な情報共有のための環境整備に取り組むとともに、各種会合の場を通じて小規模事象も含む情報共有の必要性を周知した結果、情報連絡件数が増加した。 ・情報連絡事例集を作成（2016.7）し、所管省庁・重要インフラ事業者に展開するとともに、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。 ・第４次行動計画においては、共有すべき情報として「予兆・ヒヤリハットに関する情報」が含まれること等その考え方をあらためて明確化するとともに、サービス障害に係る深刻度判断基準の具体化に向けた検討に取り組む旨を明記した。
(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。	・IPA における J-CSIP の情報共有活動については、着実に運用を継続。2016 年度は 2,000 件を超える情報提供を受け、うち 200 件弱程度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、100 件弱程度の情報共有を実施した。また、一部、STIX 等の機械処理可能な形式での情報共有も試行した。 ・J-CSIP の参加組織は 2015 年度末時点の 72 組織から、86 組織へと一層拡大した。 ・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、2015 年度までに体制構築した 6 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）に加えて、2016 年度に新たに体制構築した 3 産業分野（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。	・JPCERT/CC において、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、55 件の「早期警戒情報」を発行した。 ・JPCERT/CC において、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 10641 件：2017 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 247 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 43 件のインシデント通知を行いつつ、制御システムの関係者向けに 12 件の参考情報と 12 件の月次ニュースレター、147 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、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。	・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（78 件）。また、同機関が分析した情報の横展開を行った。 ・柳条湖事件が起こった９月 18 日前後は、中国を送信元としたサイバー攻撃が多くなることから、情報セキュリティ関係機関から各機関の取組状況や最近の攻撃トレンド等の情報を受領し、重要インフラ所管省庁への情報共有を行った。 ・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。
（オ）	総務省	総務省において、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。	・総務省において、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・重要インフラ事業者等の 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に係る情報収集・分析を継続的に実施する。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ための体制を強化し、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、サイバー攻撃への対処、官民連携及び国際連携に係る体制を強化した。
（キ）	経済産業省	経済産業省において、「クレジット取引セキュリティ対策協議会（官民の約 40 事業者等で構成）」で策定された「実行計画」を踏まえ、2020 年までに、カード情報を保有する事業者における情報漏えい防止対策の徹底やクレジット決済端末の IC 対応化 100％の実現を含めた不正使用被害の最小化を目指し、割賦販売法の見直しにより、加盟店を含めた関係事業者におけるセキュリティ対策を義務付ける等、クレジットカードを安全に利用できる環境整備を推進する。	・2016 年 12 月に、第 192 回臨時国会にて、クレジットカード決済端末のＩＣ対応化等による不正使用対策、クレジットカード会社に対するクレジット加盟店管理の強化等を措置した、割賦販売法の一部を改正する法律が可決・成立し、同月に公布された（公布から１年６ヶ月以内に施行）。改正割賦販売法の円滑な施行に向けて、本年２月より産業構造審議会割賦販売小委員会を再開し、政省令等の整備に係る検討を進めているところ。 ・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、2016 年 2 月に策定された「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」について、関係事業者等の取組を更に推進するため、2017 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-2017-」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 2016	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対して情報の提供など、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３次行動計画等に基づき、地方公共団体で発生した IT 障害等の事案について、総務省を経由し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。 ・地方公共団体の情報セキュリティの向上に資するよう、講演を行った。
(イ)	総務省	総務省において、関係機関と協力の上、地方公共団体職員が ICT-BCP 策定の必要性と基本事項を理解・習得することを支援するため、ICT-BCP 策定セミナーを実施する。また、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。	・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 ICT-BCP 策定の重要性を理解し、見直しの時期や留意事項及び評価並びに改善方法等の基本事項について修得することを支援するため、ICT-BCP セミナーを実施した。また、情報セキュリティに係る PDCA サイクルを運用できる人材の育成等を図るため、新任の担当者・管理職に必要な知識、運用する際のノウハウ及び情報セキュリティインシデント対応に関する研修を開催した。また、情報セキュリティマネジメントセミナー及び情報セキュリティ監査セミナーも実施した。 ・加えて、地方公共団体における一般職員向けの情報セキュリティに関する意識の向上や個人情報の取扱いに関する一般知識の向上等を図るため、情報セキュリティや個人情報保護の基礎的な事項の修得を目的とした e ラーニングによる情報セキュリティ研修を実施した。
(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。	・不審メール情報や脆弱性などの早期警戒情報を関係機関から収集し、また地方公共団体から提供される不審メール情報も含めて LGWAN メールで送信した。(年間 125 回) ・特に不審メールは過去のものも含め、新たに、不審メール一覧を LGWAN 上のセキュリティ支援ポータルサイトに掲示し、随時更新も行い、全地方公共団体で共有できるようにした。 ・地方公共団体や公的機関における情報セキュリティ事故の報道、地方公共団体のインシデント報告から考えられる共有すべき情報について、メールマガジンとして毎週全地方公共団体に LGWAN メールで送信した。
(エ)	総務省	総務省において、関係機関と協力の上、公開サーバやネットワーク機器等における脆弱性診断、Web 感染型マルウェアによる改ざん検知を地方公共団体に対して実施する。また、地方公共団体における緊急時の対応について、訓練ツールを提供する等支援する。	・公開サーバやネットワーク機器等における脆弱性診断、Web 感染型マルウェアによる改ざん検知を実施した。なお都道府県ごとに、高度なセキュリティ対策を施した自治体情報セキュリティクラウドが構築されたことに伴い、2016 年度でこれらの診断事業を終了した。 ・地方公共団体における緊急時の対応について、訓練のシナリオやマニュアル、評価書等から構成される訓練ツールを作成し、LGWAN 上のセキュリティ支援ポータルサイトで提供した。

（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）について集中的にセキュリティ監視を行う機能を設けるなどして、GSOC との情報連携を通じた、国・地方全体を俯瞰した監視・検知体制を整備するとともに、地方公共団体のセキュリティ強化対策を推進するため、情報システムの強靱性の向上や、自治体情報セキュリティクラウドの構築について、フォローアップを行う等により、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・監督機能を強化する。	・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、2016 年５月及び 2017 年１月に開催し、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、2017 年７月以降の本格運用に向けて、運用・保守等の体制を整備した。 ・さらに、情報セキュリティやＩＴに係る専門知識を持った職員を採用するなど、セキュリティ・ＩＴ人材の確保を重視した体制整備を図った。 ・加えて、多様な人材の活用と育成のため、外部講師による研修を自ら実施したほか、他の行政機関等が実施する研修に積極的に参加する等、個人情報保護委員会内外の様々な機会を通じて、職員の能力向上のための取組を行った。特にサイバーセキュリティ分野における対応能力の向上や、セキュリティ・ＩＴ人材の確保・育成を図ることを目的に、職員の専門的知識の習得に重点を置いた研修に注力した。 ・総務省において、地方公共団体における情報セキュリティ対策の抜本的強化策を検討するために、2015 年度に設置した「自治体情報セキュリティ対策検討チーム」の報告を踏まえ、情報セキュリティ対策の強化を行う団体を支援するため 2015 年度補正予算において、255 億円を計上するとともに、2016 年度地方財政計画に所要の歳出を計上した。 ・さらに、総合行政ネットワーク（LGWAN）については、集中的にセキュリティ監視を行う LGWAN-SOC を構築し、2017 年２月から運用を開始した。 ・加えて、2016 年度当初予算において、情報連携に用いる情報提供ネットワークシステムに関するセキュリティ対策事業費を確保した。また、2015 年 11 月に、情報提供ネットワークシステムを使用した円滑かつ安定的な情報連携の実施や、情報セキュリティの確保のため、「電気通信回線を通じた送信又は電磁的記録媒体の送付の方法及び情報提供ネットワークシステムを使用した送信の方法に関する技術的基準」（平成 27 年総務省告示第 401 号）を制定した。
（カ）	内閣官房 内閣府	内閣府等の関係省庁において、本人確認の連携による官民のオンラインサービスのシームレスな連携について、2017 年１月以降、順次、実施する。データやお知らせ情報をマイナポータルにおいて確認可能とするなど利用者が望むワンストップサービス、マイナンバーカード等の活用による ID の入力を要しないオンラインサービスの検討などについては、データの重要性に応じた二経路又は二要素認証や、行政機関発行 ID と民間発行 ID との連携による認証の導入などにより、重要情報の適正な管理のためのセキュリティ対策を講じつつ、進める。	・官民のオンラインサービスのシームレスな連携については、2017 年１月より内閣府のマイナポータルと国税庁の e-Tax システムの間でシングルサインオンによる認証連携を実現した。 ・マイナポータルを通じた自己情報やお知らせ情報の確認、子育てワンストップサービスの提供については、2017 年度中から順次実現すべく準備中。 ・2017 年 1 月からアカウント開設等のサービスを開始したマイナポータルにおいては、マイナンバーカードを活用し、ID の入力を要しないオンラインサービスを実現した。

（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、経済産業省告示に基づき、IPA とJPCERT/CC により運用され、制御システムの脆弱性情報の届出も受け付ける脆弱性関連情報届出受付に係る制度を運用する。	[NISC] ・関係省庁や情報セキュリティ関係機関との意見交換等（重要インフラ専門調査会（2016 年９月）において、JPCERT/CC が制御系システムに係る情報共有の取組状況を説明するなど）を継続的に行い、今後の取組方針を検討し、第４次行動計画に反映した。 ・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た。 [経産省] ・JPCERT/CC において、米国 ICS-CERT などからの連絡を受けて、5 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 1 件のインシデント報告を受領し、計 41 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 12 件の参考情報と 12 件の月次ニュースレター、214 件のニュースクリップなどの情報発信を行った。
（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、CSSC を通じて、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 138 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行った。
（コ）	経済産業省	経済産業省において、策定されたスマートメーターシステム及び電力制御システムに係るセキュリティガイドラインを電気事業法の保安規制に位置付ける。	・2016 年９月 23 日公布、９月 24 日施行にて、省令等の改正を行い、日本電気技術規格委員会（ＪＥＳＣ）により定められたガイドラインを引用し、電気事業者が行うべきサイバーセキュリティ対策と保安規程に具体的に記載すべき事項を規定した。

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 2016	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、統一基準群の改定を行い、その改定による府省庁及び独立行政法人等の情報セキュリティポリシーの見直しについて、進捗状況を把握し、必要な支援を行う。また、新たに直面した脅威・課題への対応について、情報システムにおける対策の迅速・柔軟な見直しを推進する。	・内閣官房において、府省庁と協議の上統一基準群の改定案を策定し、サイバーセキュリティ戦略本部決定した。本改定に伴う府省庁及び独立行政法人等の情報セキュリティポリシーの見直しに際し、速やかに改定作業ができるよう、勉強会の開催、個別の問合せ、相談に対応するとともに、情報セキュリティポリシーの改定に係る調査を実施するなど、その進捗状況の把握や支援等を行った。 ・また、緊急対応が必要な事案や新たな脅威・課題が生じた際は、情報システム等に対する対策を講ずるよう、府省庁（独立行政法人等へは所管府省庁を経由）に対し、注意喚起等を発出した。

(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 2016	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、GSOC、CYMAT、各府省庁 CSIRT 等のインシデント対処に関わる要員による情報共有及び連携の促進に資するコミュニティを形成する。	・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、政府機関におけるセキュリティ・バイ・デザインを推進するため、サプライチェーン・リスクへの対応を含むセキュリティ・バイ・デザインの観点から情報システムの調達仕様書に確実に記載すべき事項について、各府省庁の取組状況を調査する。また、見直しが必要となる事項については、統一基準群等に適切に反映されるよう検討を行う。	・内閣官房において、統一基準勉強会等の政府機関職員及び独法等の職員に対する研修において、セキュリティ・バイ・デザイン及びサプライチェーン・リスク対応の必要性や具体的な対処方法を説明し、理解を促進した。 ・また、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活用状況について、各府省庁の調査を実施し、セキュリティ・バイ・デザインのさらなる推進に必要な取組事項の検討を行っている
（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。	・IPA において、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容の見直しのため、①既存対象製品分野に対応する新規プロテクション・プロファイルの採用の検討、②新規製品分野の追加等について検討を行った。また、日米の認証機関が共同で開発したデジタル複合機のプロテクション・プロファイル（HCDpp）を CCRA の国際相互承認の対象とするため、現在日本において認証を行っている。 ・モバイルデバイス、アプリケーション、IDS/IPS、オペレーティングシステム及び暗号化ストレージの 5 技術分野の 8 つのプロテクションプロファイル（翻訳版）を WEB 公開した。
（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。	・IPA において、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」事業に着手した。

（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。	・IPA において、JCMVP 制度紹介セミナーを 1 回開催し、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、27 社 28 名が参加した。加えて、ハードウェアセキュリティフォーラム(2016 年 12 月)において、発表及びパネル展示を通じて、JCMVP 制度の紹介を行った。
（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、全府省庁の情報システムから調査対象システムを選定し、攻撃者が実際の攻撃で行う手法での疑似攻撃にて侵入調査を実施した。実施結果から問題点を改善するための対応策について、問題点の改善及びセキュリティ対策の維持・向上への助言等を行った。
（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、マネジメント監査の 2015 年度試行により確認された課題等も踏まえ、統一基準群をはじ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、電子メールの送受信時におけるなりすまし対策、ウェブブラウザのサポートポリシー変更に伴う対策、Web アプリケーションフレームワークのセキュリティ対策、DNS サーバのセキュリティ対策の４つについての重点検査を実施した。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ついて検討を行っている。
（ケ）	総務省	総務省において、システムのログに基づいて標的型攻撃を検知し、被害を未然に防止等するための防御モデルの検討を行う。	・システムのログに基づいて標的型攻撃を検知し、被害を未然に防止等するための防御モデルについて検討を行い、ガイドラインを作成した。
（コ）	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も念頭に置きつつ、インシデント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・解析機能をはじめとした機能強化、GSOC センサーの増強等の検討を行う。	・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次期 GSOC システムを構築した。 ・GSOC による監視業務の対象範囲について、独立行政法人等に拡大するため、独立行政法人等に GSOC センサー設置等の措置を講じるとともに、IPA において監視体制を構築した。
（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、近年のサイバー攻撃動向やログ管理・監視に関する国内外の関連文書等を調査して情報収集を行い、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強化すべき対象を検討している。
（シ）	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、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した。

(ス)	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。 ・ 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 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、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を実施した。また、インシデント・ハンドリングに関する事項の習得に重点を置いた研修を年間を通じて実施した。 ・内閣官房において、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、インシデント・ハンドリングに関する事項の習得に重点を置いた研修を年間を通じて実施した。また、サイバーセキュリティに関連するシンポジウム等へ参加し、CYMAT における対処能力の向上に関する情報収集に努めた。 ・総務省において、NICT を通じ、官公庁、地方公共団体、独立行政法人等に対するサイバー攻撃について実践的な演習を実施した。
(セ)	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開始した。
(ソ)	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、2014 年度に初めて開催し、2015 年度も規模を拡大して開催した、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。	・2014 年度、及び 2015 年度の NATIONAL 318(CYBER) EKIDEN の結果等を踏まえ、訓練の内容・対象とする組織の範囲・形態等の検討を行い、2016 年度は訓練内容を複雑・高度化して訓練を実施した。
(タ)	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。
(チ)	内閣官房	内閣官房において、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用等を通じて標的型攻撃に対する多重防御の取組を引き続き推進する。	・内閣官房において、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を改定し、府省庁に加え、独立行政法人及び指定法人に対しても、標的型攻撃に対する多重防御の取組の推進を図った。また、政府全体としての本取組の実施状況について、サイバーセキュリティ対策推進会議に報告した。

(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 2016	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、2015 年度に実施した試行的な監査の結果を踏まえ、各府省庁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、2016 年度の監査については、各府省庁が実施しているセキュリティ監査の評価を監査テーマとして実施するとともに各府省庁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ことに加え、2015 年度に実施した監査に係るフォローアップを実施する。また、厚生労働省（日本年金機構を含む。）に対する施策の評価を実施する。	・内閣官房において、「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年 5 月 25 日 サイバーセキュリティ戦略本部決定）に基づき、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、2015 年度に実施した政府機関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（日本年金機構を含む。）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、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。	・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、2016 年 8 月末までに「各府省庁セキュリティ・IT 人材確保・育成計画」を策定した。 ・同計画に基づく体制の整備として、2017 年度においては政府全体で約 80 名の定員増を実現。また、有為な人材を確保するための取組として、人事院が主催する人材確保活動等に参加するなど、政府一体となった採用活動を実施した。 ・一定の専門性を有する人材を育成するため、内閣官房において、2016 年度において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。
(ウ)	内閣官房	内閣官房において、政府機関全体での事例の共有、意見交換等の継続的な実施を促進するため、サイバーセキュリティ・情報化審議官等の研修等を通じたコミュニティの形成を図る。	・内閣官房において、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セキュリティ関係の研修を 8 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、各府省庁の審議官等が情報共有や意見交換を行う機会を提供した。
(エ)	内閣官房	内閣官房において、幹部職員や独立行政法人を所管する部局の担当者を対象に、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、各府省庁によるサイバーセキュリティに関する職員教育を支援するため、資料のひな形の提供等を行うとともに、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、独立行政法人及び指定法人を所管する部局の管理職及びこれらの法人の幹部職員に対し、統一基準や監査に関する講義を行うとともに、改正サイバーセキュリティ基本法に基づき監査の事務の一部を委託された独立行政法人情報処理推進機構から、最近のサイバーセキュリティの動向について講義を行った。 ・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、また改正サイバーセキュリティ基本法の施行を受けた独法等向けの新たな施策をテーマとした NISC 勉強会を開催した。 ・2016 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、一般職員が普段の業務を行うに当たり、情報セキュリティ対策を適切に遵守するための主要事項を整理した教育資料である「情報セキュリティ小冊子」を、2016 年度改定の統一基準群を踏まえて修正した。 ・・内閣官房において、2017 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、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の構築に取り組む。	・「サイバーセキュリティ人材育成総合強化方針」に基づき、各府省庁において確保・育成すべき人材に求められるスキルを整理した上で総務省が実施する「情報システム統一研修」のコース内容の見直し等、研修体系の抜本整理に取り組むとともに、研修修了者にスキル認定を行う枠組みについて検討を進めた。

(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 2016	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、新たな IT 製品・サービスの普及等に伴う政府統一的な対策の必要性を検討するため、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、各府省庁と共有する。	・内閣官房において、政府機関等の職員に対する研修においてクラウドサービス選定の際に考慮すべき点を説明し意識の向上を図ったほか、政府機関等における実際のクラウドサービスの利用や対策の状況について調査を実施した。
（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、伊勢志摩サミット等会合で準備する IT 環境のセキュリティ対策について、事前に関係機関の協力を得て整理したことにより会議開催に特化した IT 環境の政府統一的なセキュリティ対策を共有し推進した。さらに、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確認等、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 2016	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、情報システムへの不正な活動に対する国による監視、監査及び原因究明調査等の対象範囲を国の行政機関から独立行政法人及び戦略本部が指定する特殊法人・認可法人に拡大することとしたサイバーセキュリティ基本法の一部改正法の成立を踏まえ、その施行の準備及び改正法の適切な運用体制を構築する。具体的には、統一基準群を改定し、独立行政法人・指定法人の情報セキュリティ対策の策定、運用方法等を規定するとともに、IPA と連携した上で、独立行政法人・指定法人に対してマネジメント監査を始める。また、独立行政法人・指定法人に係る監視業務を行う IPA に対し、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、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。また、所管する府省庁との情報共有等を行った。また、独立行政法人については、2015 年度の主務大臣の業務実績評価を分析し、情報セキュリティ対策の課題を把握するとともに、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。 ・内閣官房において、サイバーセキュリティ基本法の一部改正法の成立を踏まえ、IPA と連携し、独立行政法人・指定法人に対して監査を開始した。 ・IPA の実施する、2017 年度からの独立行政法人・指定法人に係る監視体制の構築について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ため、インシデント発生時及び平時における IPA 及び関係組織との情報共有体制の検討を行った。

3. 国際社会の平和・安定及び我が国の安全保障

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 2016	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、参画機関、重要インフラ事業者等の連絡体制を確認するとともに、政府及び関係省庁が迅速かつ適切な初動対処を行うための態勢を整備した。
（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、2016 年９月より国内外におけるサイバー攻撃関連情報の収集・分析を開始し、サイバー攻撃対処部隊及び関係機関と情報共有を図った。

(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 2016	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。	・関係府省庁の CI 担当者と連携し、サイバー空間におけるカウンターインテリジェンスに関する情報を集約するとともに当該情報について分析し、各種会議や資料発出を通じて、分析結果を関係府省庁に提供し、共有を図った。 ・2016 年 12 月から 2017 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等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、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。 ・法務省において、「公安調査庁サイバー関連調査推進本部」を設置し、人的情報収集を強化したほか、得られた情報・分析結果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、サイバーテロ対策の強化のため、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・育成を図る方策を検討し、警察庁サイバー人材確保・育成計画を策定した。
（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、2017 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を実施した。
（カ）	防衛省	防衛省において、指揮系システムについて、サイバー攻撃時においても部隊運用を継続するとともに、被害の拡大を防止するなどの事後対処能力の練度向上を目的としたサイバー演習環境の構築技術に関する研究を継続して実施する。また、その研究成果を受け、自衛隊のサイバー攻撃対処部隊の事後対処能力の練度を向上させるため、一般的な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演習環境を整備する。	・防衛省において、サイバー演習環境の構築技術に関する研究の試験評価を実施した。また、その研究成果を受け、2017 年３月に一般的なシステムを模擬したサイバー演習環境を構築した。
（キ）	防衛省	防衛省において、サイバー攻撃生起時における重要通信の優先的な経路確保を可能とするための最新技術の取得に向けた調査研究を実施する。	・防衛省において、サイバー攻撃生起時における重要通信の優先的な経路確保を可能とするための最新技術の取得に向けた調査研究を実施し、2017 年 3 月までに重要通信の経路確保と被害拡大防止を行うサイバー攻撃対処等に関する技術資料を得た。
（ク）	防衛省	防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT 要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。	・防衛省において、サイバー攻撃等対処に向けた人材育成の取組として、2017 年２月に CSIRT 要員に対するインシデント対処訓練を実施した。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。
（ケ）	防衛省	防衛省において、サイバーセキュリティの更なる向上のため、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）の実施について検討する。	・防衛省において、ペネトレーションテストの実施体制の整備に向け、機構・定員要求を実施し、所要の態勢整備を行った。

(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 2016	取組の成果、進捗状況
（ア）	防衛省	防衛省において、更なるサイバーセキュリティの確保のため、防衛省が調達する情報システムに係る防衛装備品等について、意図的に不正改造されたハードウェア機器や不正プログラムが埋め込まれたソフトウェア等によるサイバー攻撃の脅威に適切に対応する必要がある。このため、構成品等のサプライチェーンへの対策として、そのトレーサビリティに関する調査研究等を通じて、調達段階での対策（調達方法、契約方法等）など、関連規則等の整備・導入に向けた検討を進める。	・防衛省において、サイバーセキュリティの更なる確保のため、調達する情報システムについて、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。

(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 2016	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を 2017 年２月に実施した。また、任務保証に関する専門的、具体的な意見交換を行った。

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 2016	取組の成果、進捗状況
(ア)	経済産業省	経済産業省において、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。	・JPCERT/CC において、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、現在問題となっている IoT 機器への攻撃の状況や、マルウェアに感染した機器の挙動について情報共有を行った。また、感染した機器などを使った DDoS 攻撃の手法について共有し、問題意識を共有した。また、香港の 2 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 加盟組織拡大については、中東・アフリカ地域へのアプローチを継続して実施した。

(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 2016	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。	・「日米サイバー対話」その他の二国間協議並びに日中韓協議、日 EU 協議及び G7 の枠組みの下の協議を実施し、国際的なルール、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、相互の理解を深める取組を進めた。 ・2016 年８月から始まった第５会期国連政府専門家会合に政府専門家（外務省サイバー政策担当大使）を派遣し、サイバーセキュリティ分野における既存の国際法の適用、国際的な規範の形成等に関する議論に積極的に貢献している。また、様々な国際会議に参画し、サイバーセキュリティ分野における我が国の取組に関する情報発信にも努めた。
(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・協定を締結済みのアメリカ合衆国、大韓民国及び EU 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/G8 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（2016 年 10 月）、ICPO 及び Europol が共催したサイバー犯罪会議（2016 年９月）等に参加し、外国捜査機関職員との情報交換を積極的に推進するとともに、協力関係の醸成に努めている。 ・アジア大洋州地域における各捜査機関の間で、解析技術やサイバー犯罪捜査における知識・経験等を共有することにより、サイバー犯罪捜査技術力の向上を図ることを目的として、2016 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。 ・外国捜査機関等との連携強化を目的として、サイバー犯罪に係るリエゾンを派遣した。 ・サイバー犯罪捜査において、外国捜査機関からの協力を得る必要がある場合には、刑事共助条約（協定）や ICPO、サイバー犯罪に関する 24 時間コンタクトポイント（2017 年３月末現在、73 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、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。
（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。	・2016 年 11 月，ストラスブールで開催されたオクトパス会合において、サイバー犯罪条約委員会との共催で「アジア太平洋地域におけるサイバー犯罪に関する法整備及び能力構築」と題するワークショップを実施し、我が国及びサイバー犯罪条約未締約国を含むアジア太平洋 13 か国が自国のサイバー犯罪法制等について報告し、参加国からは有意義な意見交換の場であったとして高評価を得た。

(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 2016	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。	・米国、英国、オーストラリア等の友好国との間で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、認識を共有するとともに、更なる関係強化を図った。 ・日露、日ウクライナ、日中韓サイバー協議を実施し、相互のサイバー政策及び立場に関する議論を行うことにより、信頼醸成に努めた。
（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、各国政府機関との連携に努めた。 ・MERIDIAN 会合、CIP フォーラム等に参加し、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。

（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。	・JPCERT/CC において、2016 年 10 月に東京で行われた APCERT 年次総会 2016 で、TSUBAME やサイバーグリーンのワークショップを実施し、アジア太平洋地域におけるリーダーシップとプレゼンスの維持・向上に資するイベントを行った。また、継続して FIRST と各地域の CSIRT との連携促進に注力するとともに、日中韓 CSIRT MOU に基づき 2016 年８月に中国で開催された「第 4 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」に参加し、日中韓 CSIRT 間協力について報告した。

(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 2016	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。	・警察庁において「インターネット・オシントセンター」を設置するなど、各省庁において、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・分析の強化に取り組んでいる。 ・また、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っている。
（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。	・警察庁において、インターネット・オシントセンターを設置し、インターネット上に公開されたテロ等関連情報の収集・分析を強化した。 ・法務省において、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・分析を強化したほか、人的情報源を活用したサイバー空間上におけるテロ関連情報の収集・分析態勢を強化した。

(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 2016	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、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、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］ ・内閣官房を中心とした関係省庁の緊密な連携の下、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強化すべく、「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）を策定した。 ・日・ASEAN 情報セキュリティ政策会議人材育成 WG を開催し、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。 ・2016 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。 ・ベトナム政府に対し、サイバーセキュリティの意識啓発に係るセミナーを開催し、同国の意識啓発施策の強化に向けた支援を行った。 ［警察庁］ ・アジア大洋州地域における各捜査機関の間で、解析技術やサイバー犯罪捜査における知識・経験等を共有することにより、サイバー犯罪捜査技術力の向上を図ることを目的として、2016 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。（再掲） ［総務省］ ・APEC 電気通信・情報作業部会（2016 年 10 月、京都）のセキュリティ繁栄分科会に参加し、我が国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（2016 年 11 月、東京）を開催し、我が国の取組について情報を共有した。 ・第７回 APT サイバーセキュリティフォーラム（2016 年 10 月、カンボジア）に参加し、我が国のサイバーセキュリティ政策及び取組について説明した。 ・ITU-D SG2 ラポータ会合中に ITU サイバーセキュリティワークショップ（2017 年１月、ジュネーブ）を日本主導により開催し、我が国のサイバーセキュリティ政策及び取組について説明した。 ［外務省］ ・2016 年 10 月、オールジャパンでの各国への支援の方針となる、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」を策定。これを踏まえ、日本政府としては、政府開発援助（ODA）及びその他の政府資金（OOF）等を活用し、①脅威への対処能力の向上支援、②サイバー犯罪対策支援、及び③サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有、の各分野について、当面は ASEAN 諸国を主な対象として、日本の強みを生かした支援を行っていくこととなった。 ・インドネシアでは、インドネシア通信情報省の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、同局の機能強化や、政府内各部局の IT 利用サポート体制の導入支援、情報セキュリティの啓発活動改善を行うための技術協力案件（情報セキュリティ能力向上プロジェクト）を 2016 年度においても継続的に実施した。同事業は 2017 年１月に完了し、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。

			・2017 年３月、マレーシアにおいて第２回目となる日ＡＳＥＡＮサイバー犯罪対策対話を実施し、我が国としてASEANにおけるサイバー犯罪条約の普及・拡大に向けたプレゼンを行うとともに、参加国の取組につき情報交換を行った。 ・28 年度予算として、東南アジアにおけるサイバー犯罪対策を含む、法執行当局に対する刑事司法面の対処能力向上プロジェクト実施のため、UNODC に 30 万ドルを、また、東南アジアにおける、テロリストによるサイバーを用いた攻撃の防止と影響緩和のための国家の能力強化のため、国連テロ対策センター(UNCCT.)に 40 万ドル強を拠出した。 ・サイバー犯罪対策の分野における協力として、日 ASEAN 統合基金（JAIF）を活用した「ASEAN サイバー能力向上プロジェクト」の実施を承認。 ［経済産業省］ ・経済産業省において、HIDA 研修を活用し、2017 年２月 14 日～23 日に ASEAN８か国（シンガポール、ブルネイ除く）を対象とした訪日研修「地域の重要インフラ関係者に対する情報セキュリティ強化支援研修コース」を実施。ASEAN 諸国の官民関係者に対し、重要インフ防護の実際について最新動向等について知見を提供した。

(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 2016	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 2016	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。	・G7 伊勢志摩サミットを主催し、「サイバーに関する G7 の原則と行動」の合意を主導した。 ・2017 年２月の日米首脳会談において、サイバー空間の分野における二国間の安全保障協力を拡大する旨を含む共同声明を発出。
(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 伊勢志摩サミットにおいて立ち上げが決定された「サイバーに関する G7 作業部会」を通じ、G7 各国との政策協調及び実務的な協力を強化する。	・G７伊勢志摩サミットにおいて立ち上げが決定された G７のサイバーに関する新たな作業部会（伊勢志摩サイバーグループ）の第１回会合を 2016 年 10 月に東京で開催し、サイバー空間の安全性及び安定性を高めるため、最近のサイバーセキュリティ環境に関する議論及び国際法、規範、信頼醸成、能力構築支援等の取組に関する議論を議長国としてリードし、G７各国との政策協調及び実務的な協力の強化に貢献した。
(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。	・米国との二国間対話については、「第４回日米サイバー対話」（2016 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、日米協力の推進・深化に努めた。 ・その他の国との協議については、「第２回日イスラエル・サイバー協議」（2016 年６月）、「第２回日豪サイバー政策協議」（2016 年８月）、「第３回日英サイバー協議」（2016 年 10 月）、「第２回日露サイバー協議」（2016 年 11 月）、「第３回日仏サイバー協議」（2017 年１月）、「第２回日 EU サイバー対話」（2017 年１月）、「第３回日・エストニアサイバー協議」（2017 年１月）及び「第３回日中韓サイバー協議」（2017 年２月）等を実施した。さらに、新たな枠組みとして、「日独サイバー協議」（2016 年９月）、「第１回日韓サイバー協議」（2016 年 10 月）、「重要インフラのサイバーセキュリティに関する日米韓専門家会合」（2016 年 12 月）及び「日ウクライナサイバー協議」（2016 年 12 月）を立上げ、各国との連携強化や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。	・2016 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。 ・また、在京米国大使館及び在日米国商工会議所と連携したイベント「サイバー・ハロウィン　キャリアトーク」を日本で開催した。これを通じ、主に学生を対象に、サイバーセキュリティにおけるキャリアの魅力の周知を図った。

（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。 ・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、サイバー攻撃への対処、官民連携及び国際連携に係る体制を強化した。（再掲） ・また、FIRST 会合に参加し、情報交換等国際的な連携を通じて、サイバー攻撃手法等に関する情報収集を実施している。 ・法務省において、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。	・JPCERT/CC において、米国関係組織と協力してサイバーグリーンのポータルサイトをリニューアルし、公開した。また、AS（オートノマス・システム）毎の統計・指標を提供した。さらに、G7 香川・高松情報通信大臣会合（2016 年４月）、APCERT 年次総会 2016 のサイバーグリーンワークショップ（2016 年 10 月）等においてサイバーグリーンに係る取組を紹介し、普及啓発を行った。
（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。	・2017 年２月に、IPA が、米国立標準技術研究所（NIST）との定期会合を NIST にて開催した。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 CMVP、サプライチェーンセキュリティ、ソフトウェア ID タグ、NVD/JVN、CVSS、暗号、生体認証 CC 評価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。	・JPCERT/CC において、JICA、HIDA 等外部機関による研修を通して、重要インフラ防護や制御システムセキュリティに関する JPCERT/CC の取組について講義するとともに、ボツワナ、エジプト、モーリシャス、モンゴルや中東においても CSIRT 能力構築支援を推進した。 ・ミャンマーにおいて海外セキュアコーディングセミナーを実施すべくミャンマーmmCERT と調整中。
（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、体制強化を行った。

(1) アジア大洋州

項番	担当府省庁	サイバーセキュリティ 2016	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。	・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を通じて、次のような連携・協力を推進している。 ・2016 年 10 月に第９回日・ASEAN 情報セキュリティ政策会議を東京において開催し、「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」の改定案の検討とともに、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９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、各国間における情報共有の手順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。 ・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。第９回日・ASEAN 情報セキュリティ政策会議では、従来の検討に加え、各国が人材育成に持続的に取り組むための考察・検討を行っていくことを確認した。
(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。	・アジア大洋州地域における各捜査機関の間で、解析技術やサイバー犯罪捜査における知識・経験等を共有することにより、サイバー犯罪捜査技術力の向上を図ることを目的として、2016 年 12 月に、アジア大洋州地域サイバー犯罪捜査技術会議を開催した。（再掲）
(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。	・防衛省において、日尼（インドネシア）ＩＴフォーラム（2016 年６月）、日越（ベトナム）ＩＴフォーラム（2017 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 2016	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。	・第４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、能力構築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。
(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。	・総務省において、ISAC 間連携国際ワークショップ（東京）を 2016 年 11 月に開催し、日本の ICT-ISAC、米国の Comm-ISAC、IT-ISAC 及びドイツの eco（インターネット産業協会）との間で、情報共有に関する議論・意見交換を行った。また、2017 年 3 月 19 日に国際情報通信技術見本市「CeBIT」（ドイツ）において「ハノーバー宣言」が署名され、同宣言に 2016 年 11 月に開催された ISAC 間連携国際ワークショップを歓迎する記載が盛り込まれた。
(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、日米サイバー防衛政策ワーキンググループ（CDPWG）を 2016 年 10 月に開催し、情報共有や訓練・人材育成等、様々な協力分野に関する専門的、具体的な意見交換を行った。

(3) 欧州

項番	担当府省庁	サイバーセキュリティ 2016	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 CCD COE における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。	・仏、独、英、エストニア、ウクライナ、EU 等とのサイバー協議を通じて、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 と定期的に協議を行う。	・IPA において、JIWG プレナリ会合に 1 回参加し、2016 年度の活動報告と 2017 年度の活動計画を協議した。また、JHAS 会合に 6 回、JTEMS 会合に 2 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 2016	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、二国間協議等の枠組みを通じ、各国との連携を強化する。	・2016 年６月、第２回日イスラエルサイバー協議を実施し、同国との連携強化に努めた。 ・国連政府専門家会合等の多国間協議の場等を利用し、各国との意見交換を実施している。

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 2016	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、各省庁と協力し、「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する。	・「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、次期戦略である「サイバーセキュリティ研究開発戦略」の検討を開始した。
(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。	・電子政府システムをはじめ国民生活を支える様々なシステムで利用されている暗号方式(SHA-1)への新たな攻撃(脅威)が発見されたことを受け、CRYPTREC より速報を発信した。また、その他の暗号技術に関する新たな脅威に対する調査を実施し、調査結果を CRYPTREC を通じて公開した。また、IoT 時代に軽量暗号の利用促進を図るため、軽量暗号を選択・利用する際の技術的判断に資する「軽量暗号ガイドライン」を作成した。

(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 2016	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。	・サイバー攻撃統合分析プラットフォーム NIRVANA 改のアラート管理機能、可視化機能の強化を図った。 ・また、各種サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする CURE システムの基本設計の実施や、実組織ネットワーク環境を模擬するシステム構築技術の開発を行った。
(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。	・昨年に引き続き、サイバーセキュリティ研究基盤である NONSTOP を運用し、国内複数大学等がユーザとして活用した。
(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。	・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提供方法について検討を実施した。

(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 2016	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、法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進する。	・次期戦略である「サイバーセキュリティ研究開発戦略」の検討の際に、信頼性工学、心理学等の様々な社会科学的視点も含めた。
(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。	・経済産業省は、NEDO を通じて世界に先駆けて大量のデータの効率的かつ高度な利活用を実現するため、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、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、ビッグデータや AI（人工知能）といった社会・技術の変化を先取りした調査・研究・開発についての検討を行っていく。	・理化学研究所に新設した革新知能統合研究センター（ＡＩＰセンター）において、10 年後を見据えた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るところ。

(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 2016	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し、安全性評価基準の策定に向けた文書化を実施した。また、Tokyo QKD Network 上に秘密分散ストレージ機能を実装し、そのネットワーク実証に世界で初めて成功した。光空間通信テストベッドの空間伝送特性の計測・評価を実施するとともに、その結果に基づく実証実験系の設計を実施した。
(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、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、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等を引き続き実施した。 また、「CRYPTREC」において、暗号の利用者向けのセキュリティ対策等のニーズを踏まえ、暗号プロトコルも取組対象とし、ガイドライン策定に向けて検討を実施した。
(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。	・AIST において、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。ソフトウェア工学については、民間企業との共同研究において自動車やスマート工場を題材にした研究課題の洗い出しおよび実証実験環境の整備を行った。暗号技術においては、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解読に関する世界記録を更新し、得られた知見をもとに、格子暗号の実用化に向けた最大の障害である公開鍵サイズを 90%削減する技術を開発した。
(エ)	文部科学省	文部科学省において、科学技術基盤としてイノベーションを支える情報基盤に係る耐災害性強化（分散システム導入や自己修復機能の付加等）等、課題達成に貢献する機能の強化等をより一層推進するため、研究開発を実施する。	・不揮発性ワーキングメモリを活用した耐災害性に優れた情報システムを実現するスピントロニクス材料・デバイス基盤技術の研究開発や、大規模災害時にも情報を安全に保存し、継続した情報サービスを提供できる高機能・高可用性情報ストレージ基盤技術の開発を行った。

(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 2016	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。	・ITU-T SG17 会合（2016 年８月、2017 年３月）において、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 2016	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」により制御・通信機器の真正性／完全性確認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。	・制御ネットワークのセキュリティ対策として、設備全体の機器のソフトやデータについて、マルウェア等による改変を検知する技術を開発し、プロトタイプ実装によって基本機能（信頼の連鎖）が完成した。 ・「情報共有システム」について、重要インフラ事業者のデモによる要件をフィードバックし、検証用プロトタイプの開発が完了した。

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 2016	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、「新・情報セキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成総合強化方針」に基づき関係施策を促進していく。	・2017 年３月に開催した普及啓発・人材育成専門調査会にて「サイバーセキュリティ人材育成プログラム（案）」を決定したのち、国民からの意見募集を行った。 ・「サイバーセキュリティ人材育成プログラム」の決定に向けて、引き続き検討を進める。

(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 2016	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事業」の１分野としてセキュリティ分野の人材育成に取り組んでいる。当事業において、大学院修士課程及び学部 3～4 年生の学生を対象（社会人学生も含む）とした PBL（課題解決型学習）等の産学協同による実践的教育プログラムの実施や、産学の実践的教育のネットワークの拡充等を支援した。
(イ)	内閣官房	内閣官房において、関係府省庁と連携しつつ、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、実践的なサイバー演習環境の整備に向けた検討を行う。	・2017 年１月に産学官の有識者を集めた、情報セキュリティ社会推進協議会 産学官人材育成 WG を開催し、産業間、大学、各府省庁との間の情報共有、取組についての議論を行った。 ・また、「サイバーセキュリティ人材育成プログラム（案）」にもその結果を反映した。
(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事業」の１分野としてセキュリティ分野の人材育成に取り組んでいる。当事業において、大学院修士課程及び学部 3～4 年生の学生を対象（社会人学生も含む）とした PBL（課題解決型学習）等の産学協同による実践的教育プログラムの実施や、産学の実践的教育のネットワークの拡充等を支援した。

（エ）	文部科学省	文部科学省において、高等専門学校における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に着手する。	・2016 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、パイロット校 5 か所（一関、木更津、石川、高知、佐世保）に演習拠点を設置し、サイバーレンジ（実践的な演習環境）の提供に向けた取組に着手した。
（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事業」の 1 分野としてセキュリティ分野の人材育成に取り組んでいる。当事業において、大学院修士課程及び学部 3～4 年生の学生を対象（社会人学生も含む）とした PBL（課題解決型学習）等の産学協同による実践的教育プログラムの実施や、産学の実践的教育のネットワークの拡充等を支援した。
（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について、実施した。（20 コース・受講者数 376 人） ・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情報関係分野の教育訓練を指定した。（情報関係の指定講座数　486 講座） ・2016 年 10 月指定講座より、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」の課程を専門実践教育訓練給付の対象講座に加え、2017 年４月指定までに４講座を指定。
（キ）	内閣官房	内閣官房において、行政機関等が入手したサイバーセキュリティに係る事案情報、不正プログラム情報や、行政機関自らが感知した事案情報等について、情報提供者の秘密保持等に配慮し、関係者の同意を得た上で、学習教材として教育・訓練等に活用される方法の検討を進める。	・内閣官房において、2016 年 8 月に、サイバーセキュリティに係る事案情報等を踏まえつつ、企業のサイバーセキュリティ対策の実装のためのツールを含めた「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。

(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 2016	取組の成果、進捗状況
（ア）	文部科学省	文部科学省において、学習指導要領を踏まえながら、児童生徒の発達段階に応じた情報活用能力（情報活用の実践力、情報の科学的な理解、情報社会に参画する態度）を培う教育を一層推進する。特に、指導の改善が図られるよう、小中高等学校におけるプログラミングや情報セキュリティ、情報モラル等を含め、情報活用能力を各教科等の学習と効果的に関連づけて育成するためのカリキュラム・マネジメントの在り方に関する調査研究を実施する。	・推進校を指定し、学習指導要領の改訂に関する議論を踏まえながら、児童生徒の発達の段階に応じ、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、各教科等の学習と効果的に関連付けて育成するためのカリキュラム・マネジメントの在り方に関する調査研究を実施した。今年度の成果を踏まえ、引き続き 2017 年度において調査研究を実施予定。
（イ）	文部科学省	文部科学省において、初等中等教育に携わる全ての教員並びに教育委員会及び学校の全ての管理職等の情報セキュリティに関する基本的な知識を含む情報通信技術や情報モラルに関する指導力の向上を目指した取組が地方公共団体等において進められるよう、各地域で中核的な役割を担う指導主事、リーダー的教員等を対象とした研修や指導方法等に関する情報交換の機会の提供等を行う。	・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とともに、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等を全国で 10 か所及びフォーラムを全国 2 か所で実施した。

(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 2016	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。	・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、2016 年８月９日～13 日にかけて「セキュリティ・キャンプ全国大会」を千葉県で実施。51 名が受講した。 ・また、2016 年５月から 2017 年２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９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 法人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 2016」）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「SECCON2016」において、経済産業省として後援するとともに、2017 年１月 28 日、29 日に実施された「SECCON2016 決勝大会」において、最も優秀な成績を収めた社会人チームを対象として経済産業大臣賞を新規創設した。
(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。	・「未踏 IT 人材発掘・育成事業」は 16 テーマ 31 名のクリエータを採用し、着実に事業を実施した。また、2016 年度より、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 2016	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。	・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。	・2016 年４月の春期情報処理技術者試験から情報セキュリティマネジメント試験を開始し、１年間で 45,089 人の応募があった。
(ウ)	経済産業省	経済産業省において、情報セキュリティ人材を含めた高度 IT 人材育成のため、IT サービス産業において求められる次世代の高度 IT 人材像を発信するとともに、学生や若手技術者が将来のキャリアパスをイメージできるように、新たな IT サービスビジネスの創造事例をとりまとめ、広報・普及する。	・第４次産業革命に対応する能力・スキルを明確化するため、IT スキル標準について全面的な改訂に着手。2017 年３月の人材育成推進会議における中間取りまとめではデータサイエンティスト、セキュリティに関連する人材類型の拡充を行った。
(エ)	経済産業省	経済産業省において、情報処理の促進に関する法律を改正し、情報セキュリティ人材の国家資格として新たに創設した情報処理安全確保支援士制度の実施に向けて必要な措置をとる。加えて、行政機関等における人材登用で当該制度を積極的に活用する方策を検討する。	・経済産業省において、情報処理の促進に関する法律の改正に伴い、情報処理安全確保支援士（通称：登録セキスペ）制度の実施（試験、登録等）に必要な関係政省令の改正等を 2016 年 10 月に行った。 ・また、IPA において、第１回登録（2017 年４月１日付）に向けて 4,175 人の登録申請を受け付け、4,172 人を登録した。また、2017 年４月 16 日に実施の第１回目の情報処理安全確保支援士試験には 25,130 人の応募があった。 ・登録セキスペの更なる活用のため、IPA の HP で登録状況を公表できるよう準備を行っている。

(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 2016	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組として、2017 年２月に CSIRT 要員に対するインシデント対処訓練を実施した。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、国立研究開発法人情報通信研究機構法の改正（2016 年４月 20 日成立、同年５月 31 日施行）を踏まえ、NICT 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。	・総務省において、国立研究開発法人情報通信研究機構法の改正（2016 年４月 20 日成立、同年５月 31 日施行）を踏まえ、NICT 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）を実施し、2016 年度には約 1500 名が受講した。
(ウ)	防衛省	防衛省において、指揮系システムについて、サイバー攻撃時においても部隊運用を継続するとともに、被害の拡大を防止するなどの事後対処能力の練度向上を目的としたサイバー演習環境の構築技術に関する研究を継続して実施する。また、その研究成果を受け、自衛隊のサイバー攻撃対処部隊の事後対処能力の練度を向上させるため、一般的な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演習環境を整備する。	・防衛省において、サイバー演習環境の構築技術に関する研究の試験評価を実施した。また、その研究成果を受け、2017 年３月に一般的なシステムを模擬したサイバー演習環境を構築した。
(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に係る連携の強化を図るため、情報共有の深化に資するワークショップ等を行うとともに、事案発生を想定した共同訓練を実施する。	・防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処に係る連携の強化を図るため、事案発生を想定した共同訓練を 2017 年２月に実施した。また、任務保証に関する専門的、具体的な意見交換を行った。

5. 推進体制

項番	担当府省庁	サイバーセキュリティ 2016	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を進化させるため体制を整備するとともに情報共有システムの構築を行う。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の運用を通じた国内外のインシデント情報の情報共有を推進した。また、同環境の機能の改善により情報提供体制の充実を図るとともに、セプターカウンシル運営のための支援等、重要インフラ事業者等に関する取り組みのための協力体制の整備を実施した。 ・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。
(イ)	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をはじめとする国際的なビッグイベントにおけるサイバーセキュリティを確実に確保するため、その運営に大きな影響を及ぼし得る重要システム・サービスを洗い出し、それらに対するリスク評価を実施する（2016 年度以降本格実施）ために必要な評価手順等の整理を関連組織と連携して推進する。また、これら重要システム・サービス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オリンピック・パラリンピック CSIRT の構築に向け、調査研究や関係主体との連携を通じて検討を行う。	・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のサイバーセキュリティワーキングチームにおいて、2020 年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）のサイバーセキュリティの確保に資する具体的な施策について精力的に検討を推進した。また、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・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）にサイバーセキュリティ対策の強化を明記した。 ・サービスの安全かつ持続的な提供の確保のためのリスク評価手順書を作成するとともに、東京大会において開催・運営に影響を与える重要なサービスを提供する事業者等を選定し、リスク評価の実施を依頼した。各事業者等は、2016 年 10 月～12 月の期間で第１回目のリスク評価を実施。約 70 組織から実施結果を受領し、取りまとめ及び次回に向けた改善の作業を実施した。各事業者等には、第１回のリスク評価により明らかになったリスクへの対策実施を依頼した。2017 年８月～10 月の期間で第２回のリスク評価の実施を予定している。 ・東京大会のサイバーセキュリティ体制に関する体制検討会において、具体的な対処体制（オリンピック・パラリンピック CSIRT）を検討し、脅威情報等の共有する情報の種類やポリシー、関係する組織の役割等、情報共有に関する基本的な方針及び関係組織とその役割、インシデント対処のポリシーと対処支援の内容等、インシデント対処に関する基本的な方針について決定した。 ・G7 伊勢志摩サミット及びリオ大会開催期間等において、現地に連携要員を派遣するとともに、情報共有手段として同合意に基づく情報共有体制の試験運用を実施した。引き続き関係省庁・関係者間のより円滑な情報共有のためのシステムの整備に向けた検討を実施する。

（ウ）	内閣官房	内閣官房において、2016 年に開催される G7 伊勢志摩サミット及び関連大臣会議におけるサイバーセキュリティの確保のため、一時的に会議場に設置される情報システムを含む政府機関情報システムにおける対策の徹底を図る。また、サミット等各会議の円滑な開催に不可欠な重要サービスを提供する重要インフラ事業者等におけるサイバーセキュリティの確保のため、重要インフラ所管省庁をはじめとする関係省庁と連携し、必要な対策を推進する。各会議開催期間における実践的な対処体制として、サイバーセキュリティ関係機関を含む関係主体間の迅速かつ的確な情報共有を可能とする体制を確立し、実践的な事案対処訓練を実施する。	・G7 伊勢志摩サミット及び関係大臣会合の開催に際しては、「伊勢志摩サミットにおける警備対策の基本方針」（2015 年９月 15 日付伊勢志摩サミット準備会議警備対策部会決定）を踏まえ、全ての関係府省庁の緊密な連携の下、サイバーセキュリティ確保のための取組を推進。 ・NISC はインシデント発生を想定した連絡訓練を実施するとともに、全サミット等会議会場事務局及び三重、広島、宮城の各県警本部に連携要員を派遣し、会合開催当日にあっては、前項の情報共有体制の着実な運用を行い、関係するインシデント等について的確な対応を行った。
（エ）	内閣官房	内閣官房において、検知、判断、対処、報告といった一連の初動対処を見直し、政府全体での実践的訓練などを通じ、危機管理対応の一層の強化を図る。	・情報システムへの不正な活動に対する国による監視の対象範囲を、国の行政機関から独立行政法人及び戦略本部が指定する特殊法人及び認可法人（指定法人）に拡大することとしたサイバーセキュリティ基本法の一部改正法の成立を踏まえ、府省庁、独立行政法人及び指定法人等の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ついて初動対処に係る関係組織間の情報共有体制を見直した。

（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

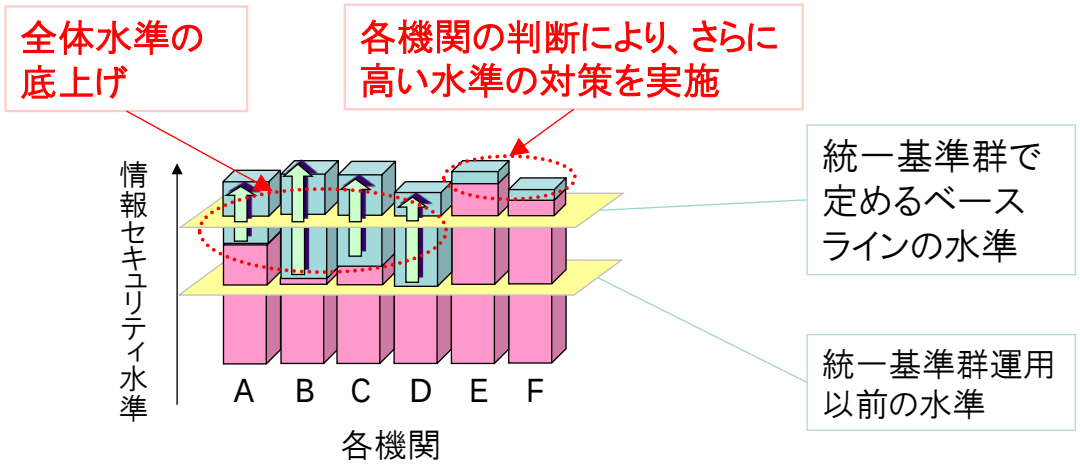
＜別添３　目次＞

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

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）。

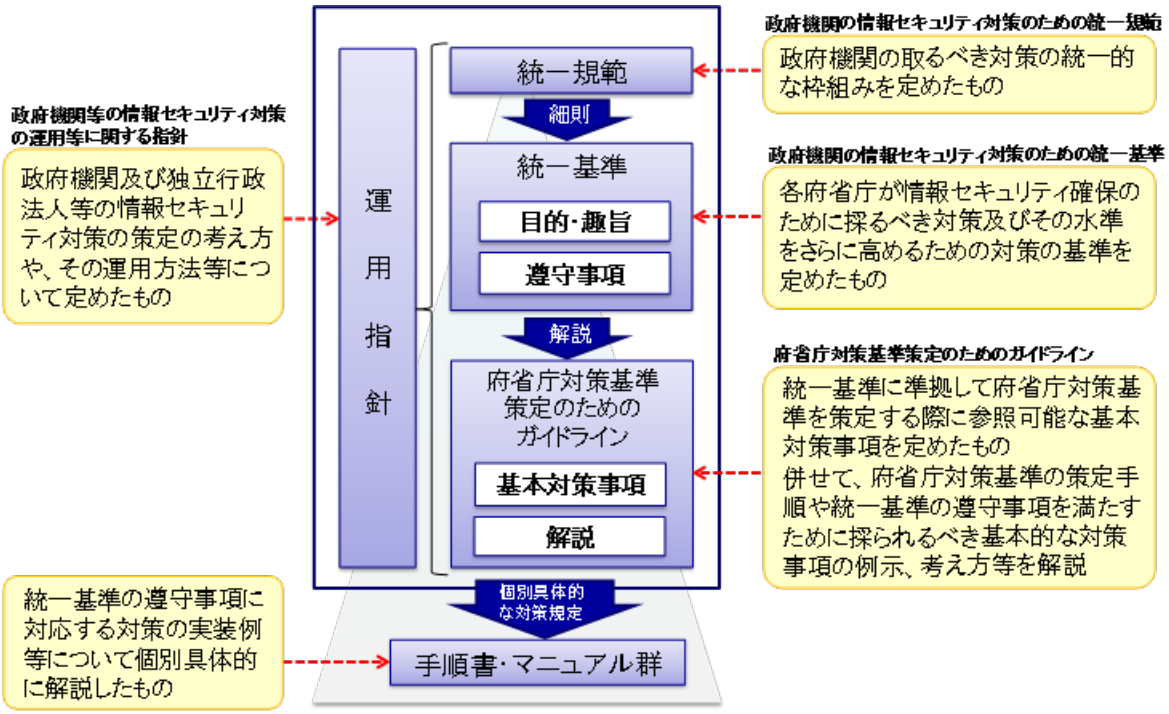
図表１　統一基準群の効果（イメージ）



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、現在は、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。

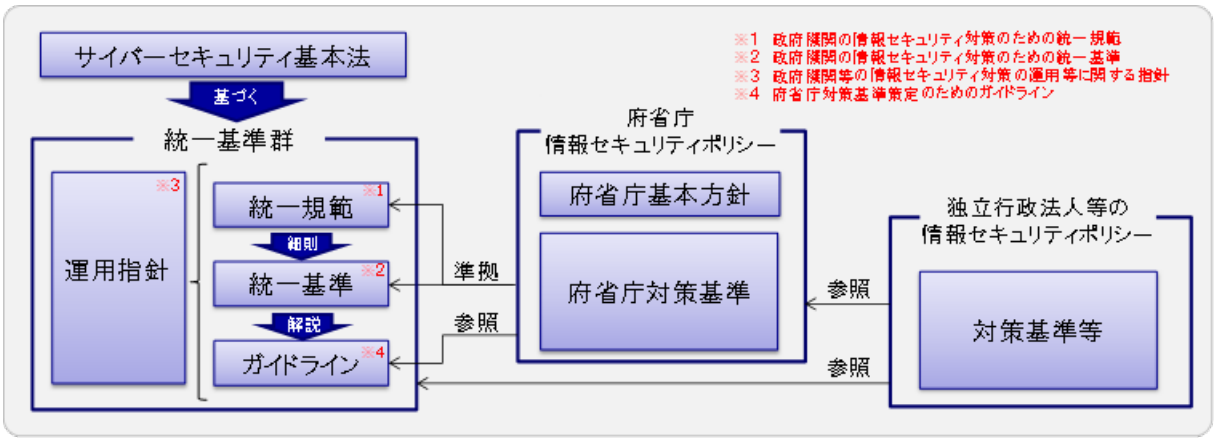
統一基準群（平成28年度版）の文書構成は、図表２のとおりである。

図表２　統一基準群の文書構成



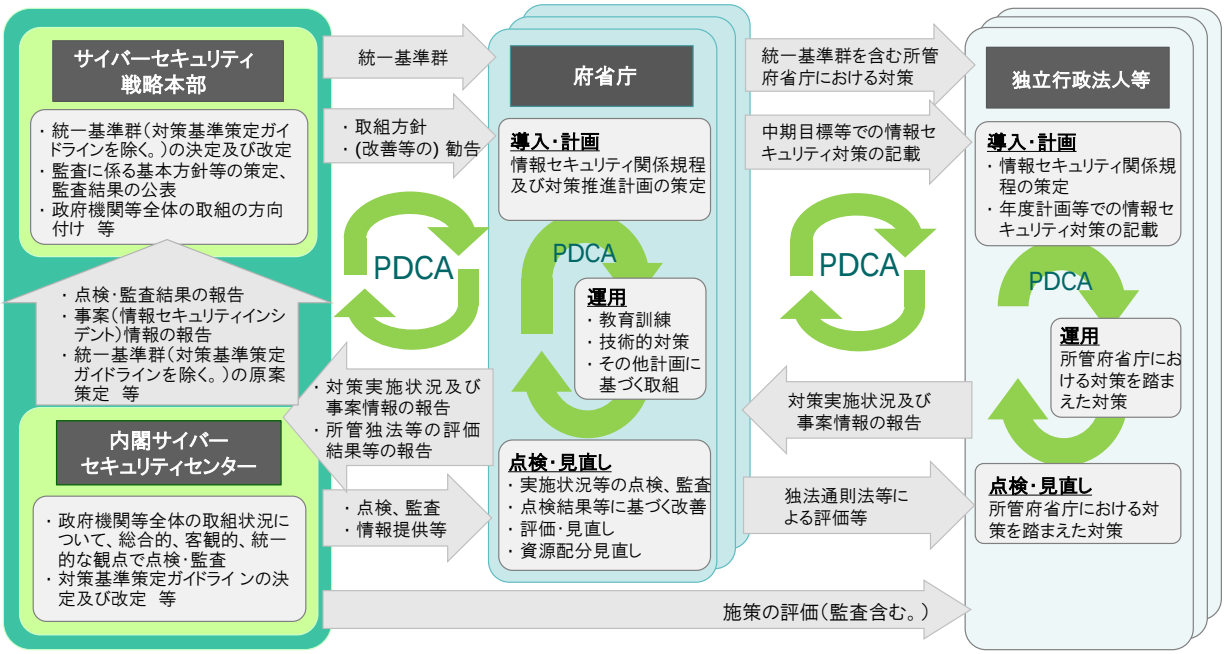
府省庁は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「府省庁対策基準策定のためのガイドライン（以下「ガイドライン」という。）」を参照した上で、「政府機関の情報セキュリティ対策のための統一規範（以下「統一規範」という。）」及びその細則である「政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）」に準拠した情報セキュリティポリシーをそれぞれ策定し、当該ポリシーに基づく情報セキュリティ対策を適切に講じることとされている。また、独立行政法人及び指定法人（以下「独立行政法人等」という。）は、「政府機関等の情報セキュリティ対策の運用等に関する指針（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

2015年１月９日のサイバーセキュリティ基本法の全面施行及び2015年９月４日の新たなサイバーセキュリティ戦略の閣議決定を受け、サイバーセキュリティ戦略本部による監査を始めとした政府機関等のサイバーセキュリティの確保に係る様々な取組が進められている。また、2015年５月に発生した日本年金機構における情報流出事案を教訓として、重要な情報を扱う情報システムのインターネットからの分離や実効的なCSIRT体制の確立等の対策を促進するとともに、2016年10月21日の改正サイバーセキュリティ基本法の施行により、サイバーセキュリティ戦略本部による監査の対象範囲を指定法人に、原因究明調査、監視等の対象範囲を独立行政法人及び指定法人にそれぞれ拡大した。

一方、クラウドサービスの利用等、ITを利活用した政府機関等における業務形態は日々多様化しており、これらに対する適切な情報セキュリティ確保のための取組も必要となっている。

このような政府機関等におけるセキュリティ対策の取組やサイバー脅威の動向等を踏まえ、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統一基準群（平成28年度版）が改定された。

統一基準群（平成28年度版）における主要な改定内容を、以下に示す。

（１）　サイバーセキュリティ基本法と統一基準群の関係の明確化

統一基準群がサイバーセキュリティ基本法の第13条及び第25条に掲げられている「国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する統一的な基

準」として位置づけられることを明確化するため、統一規範及び運用指針に所要の規定を追加した（図表３）。

（２） サイバーセキュリティ戦略本部が実施する監査に係る規定の追加

独立行政法人等を含む政府機関等全体の情報セキュリティマネジメントサイクルを明確化し、サイバーセキュリティ基本法第25条第１項第２号に基づくサイバーセキュリティ戦略本部が実施する監査に係る規定を運用指針に追加した（図表４）。

（３） インシデント対処に係る規定の見直し及び強化

日本年金機構における情報流出事案によって得た教訓、その他の情報セキュリティインシデントの発生状況やサイバー攻撃の動向等を踏まえ、各組織のCSIRTが事案発生時に実働する体制となるよう、以下のとおり規定の見直し及び規定の強化を行った。

① 関連部局との役割分担を含むCSIRTの役割を明確化し、外部の専門家による必要な支援を速やかに受けられる体制の構築等のCSIRT設置に係る要件を明確化（図表５）。

図表５　CSIRTの役割として規定すべき事項の例

CSIRTの役割として規定すべき事項

情報セキュリティインシデント発生時の対処の一元管理

- 組織全体における情報セキュリティインシデント対処の管理
- 情報セキュリティインシデントの可能性の報告受付
- 組織における情報セキュリティインシデントに関する情報の集約
- 情報セキュリティインシデントの幹部への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化
- 所管する独法等における情報セキュリティインシデントに関する情報の集約

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

- 情報セキュリティインシデントであるかの評価及び対処全般に関する指示等
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- NISCへの連絡
- 情報セキュリティインシデントに係る情報の共有
- 情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

② 情報セキュリティインシデント対処として想定されるプロセスを更に具体化するとともに、CSIRTが対処状況全般を把握することや対処手順が適切に機能することを訓練等により確認すること、インシデント対処の意思決定の判断基準・決定方法等をあらかじめ明確化すること等を追加規定（図表６）。

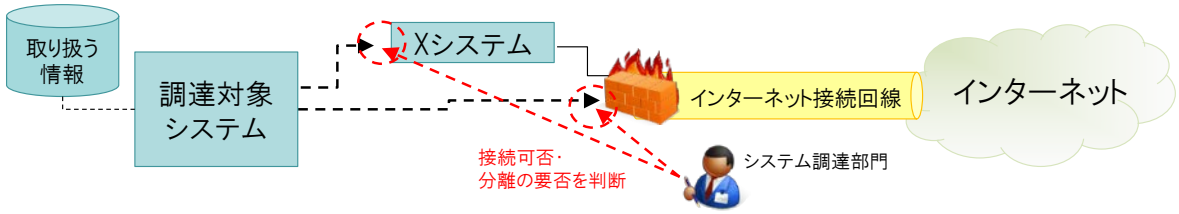
図表６　インシデント対処プロセスの例

検知／連絡受付	－　情報セキュリティインシデントの可能性の報告受付
トリアージ	－　報告された情報セキュリティインシデントの可能性に関する状況確認 －　状況確認結果に基づく情報セキュリティインシデントであるか否かの評価 －　対処する情報セキュリティインシデントの優先順位付け（事案が多発している場合等）
インシデント レスポンス	－　応急措置の実施 －　被害規模･範囲等の特定を含む状況分析 －　関係部局、セキュリティベンダ等の外部組織、CYMAT等への支援要請 －　復旧対応の実施 －　情報セキュリティインシデントの原因調査と原因が生じた理由の究明 －　再発防止策の検討
報告／情報公開	－　最高情報セキュリティ責任者への報告 －　NISCへの連絡 －　警察等の関係組織への通報･連絡･報告等 －　報道発表等の対外対応

（４）　標的型攻撃等による不正プログラム感染の発生を前提とする情報システムの防御策の強化

日本年金機構における情報流出事案によって得た教訓を踏まえ、業務や取り扱う情報の性質等に応じて、重要な情報に攻撃が到達しないよう、情報システムの調達時にインターネットやインターネットと接点を有する情報システムから分離することの要否の判断を求めるなどの規定を追加した（図表７）。

図表７　情報システムの分離判断のイメージ



また、電子メールに添付された実行プログラム形式ファイルを不用意に実行することで不正プログラム感染することを回避するための方策として、電子メールに添付された実行プログラム形式ファイルを削除等するなどの防御策の強化を図った。

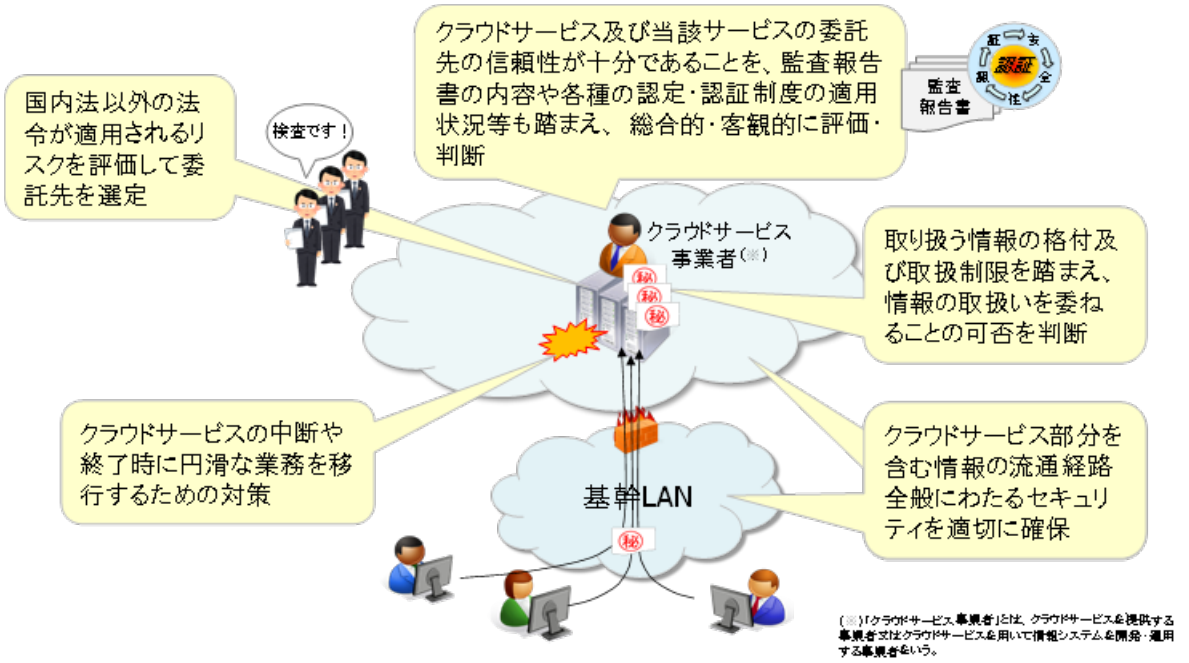
（５）　新たなIT技術・サービスの普及等に伴う対策の強化

近年、政府機関等において利活用が進められているクラウドサービスを利用する際のセキュリティ対策として、クラウドサービスを利用する際に考慮すべき規定を追加した。

また、適正なクラウドサービス事業者を選定するために考慮すべき要件として、クラウドサービスの利用におけるリスクを例示し、当該リスクを踏まえた上で、情報の取扱いを委ねることの可否を判断するよう求める規定を追加した。

さらに、具体的な対策として、クラウドサービスを利用するに当たって、調達仕様書等に記載すべきセキュリティ要件を例示するなど、新たなIT技術・サービスの普及等に伴う対策の強化を図った（図表８）。

図表８　クラウドサービスを利用する際に考慮すべき事項・リスク・要件の例



クラウドサービスを利用するに当たって考慮すべきリスクの例

① クラウドサービスは、詳細な仕組みを利用者が知ることがなくても手軽に利用できる半面、運用詳細はブラックボックスとなっている

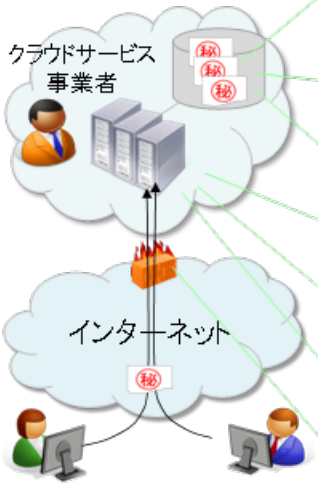
② オンプレミスとクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス事業者との間の責任分界点やサービスレベルの合意が容易ではない。

③ 不特定多数の利用者の情報やプログラムを一つのクラウド基盤で共用することとなるため、情報が漏えいするリスクが存在する。

④ クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。

⑤ サーバ装置等機器の整備環境がクラウドサービス事業者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

クラウドサービスを調達する際に考慮すべきセキュリティ要件の例示



クラウドサービス上で取り扱う情報の暗号化
クラウドサービス上で取り扱う情報の確実な削除・廃棄

クラウド事業者による情報の管理・保管の実施内容の確認

クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標

クラウドサービス上の脆弱性対策の実施内容の確認

クラウドサービスに係るアクセスログ等の証跡の保存及び提供

利用者が求める情報開示請求に対する開示項目や範囲の明記

インターネット回線とクラウド基盤の接続点の通信の監視

別添３－２　サイバーセキュリティ基本法に基づく監査

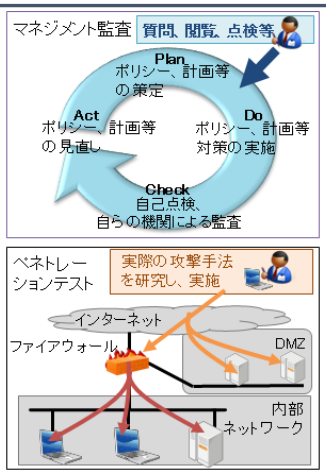
１　2016 年度における監査の概要

サイバーセキュリティ基本法に基づく監査について、2016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、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、政府機関等において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

2016 年４月から 2017 年３月までの間

（２）マネジメント監査の実施対象

政府機関（全 22 府省庁）のうち、12 の府省庁（厚生労働省については、日本年金機構を含む。）を対象とした。

（３）マネジメント監査の実施内容

「政府機関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、2015 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 2015 年度に実施した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

- 最高情報セキュリティ責任者、最高情報セキュリティアドバイザー、情報セキュリティの推進部署及び関連部署等において定例会合や臨時会合を開くなど、密接に連携する仕組みを構築するとともに、新たなリスクに対する調査・評価等を適時に実施し、訓練内容を変更するなど、新たなリスクへの対応を積極的に実施していた事例
- リスク評価に係る取組みについて、リスクの分析・評価を単に実施するだけではなく、①新たな情報資産に対する詳細なリスクの分析や、②リスクとなる可能性のある事象の調査により把握された事象の横展開及び要因整理に取り組むなど、リスク評価の仕組み自体の改善を図り PDCA サイクルを機能させていた事例
- 要機密情報の運搬・送信等に当たっては決裁を必須とする運用とし、要機密情報の消去に当たっては機密性に応じて収集場所を分別して施錠可能な場所に保管する運用としていた事例
- 情報システムの更改に際し、外部委託事業者に対して、要件定義書や基本設計書等に加えて、セキュリティポリシーへの準拠や脅威分析等を記載した「情報セキュリティ設計書」の作成及び「情報セキュリティ設計書」に基づく機器等の設計・導入を調達仕様書で要求していた事例

② 主な助言等

2016 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定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定の整備及び運用状況
- 情報システムの構成要素に係る規定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 2015 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

2015 年度に監査を実施した 10 府省庁に対して、2016 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、改善策を実施済みであるか又は改善策に取り組んでいる状況であった。

2015 年度及び 2016 年度の監査において、府省庁全体として「政府機関の情報セキュリティ対策のための統一基準」及び「府省庁対策基準」が求める必要な水準を満たすようサイバーセキュリティに係る取組が実施されていた。助言への対応を含め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、府省庁は対策状況を評価して改善を行う自律的な取組を実施し、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

2016 年４月から 2017 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。厚生労働省については、日本年金機構を含む。）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 44 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ウイルス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）が容易に推測・特定できるという、設定・管理における不備であった。また、一部の情報システムにおいて、インターネットから情報システムに侵入できる脆弱性が発見された。調査中において侵入に利用できる脆弱性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。

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

2016 年 10 月から 2017 年５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

独立行政法人及び指定法人（全 97 法人）のうち、６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

- 最高情報セキュリティ責任者の指示の下、情報システムの脆弱性を明らかにするため脆弱性診断やペネトレーションテストの技術的診断を実施するとともに、法人内外のリスクを考慮した情報システム対策が講じられるよう、外部から情報セキュリティアドバイザーを採用し組織内のマネジメントシステムの確立に努めた。
- 法人内の情報セキュリティ管理体制の強化のため、最高情報セキュリティ責任者及び情報セキュリティ委員会のメンバーにより PDCA サイクルの推進を図るとともに、統一基準の遵守事項等について、分かりやすいガイドラインや解説書を作成し職員への理解度の向上・定着に努めた。

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定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

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

2016 年 10 月から 2017 年５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

独立行政法人及び指定法人（全 97 法人）のうち、６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６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、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ウイルス感染したと想定して当該端末（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は発見されなかった。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）が容易に推測・特定できるという、設定・管理における不備であった。調査中において侵入に利用できる脆弱性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	Internet Explorer	NISC が注意喚起した事項について、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。
	Apache Struts2	
	BIND	

インターネットから電子メールを受信する情報システムについて、受信側における送信ドメイン認証技術等を用いた対策の実施状況を確認したところ、対策の約７割がSPF（Sender Policy Framework）を利用したものであった。

受信側における送信ドメイン認証技術の導入には、一定程度の予算措置による情報システムへの機能追加が必要となり、電子メールによる標的型攻撃に係るリスクの低減を図るためにも、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、着実に対策の導入を推進することが重要である。

2016年度の重点検査では、送信側における送信ドメイン認証技術等を用いた対策の実施状況についても調査しており、対策の９割以上がSPFを利用したものであった。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。

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を利用する割合が最も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、送信側における送信ドメイン認証技術を用いた対策も合わせて実施することが必要である。

Internet Explorerサポートポリシー変更（2016年１月12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、その後の追跡調査においてInternet Explorer11への更新計画など適切な対応が実施されていることを確認できた。今後とも、端末やサーバで使用するソフトウェアのサポート終了時期を念頭に置きつつ、計画的なシステム調達を行っていく必要がある。

Apache Struts2の脆弱性対応状況について、脆弱性の有無の確認を行った。確認により対応が完了していないことが判明した情報システムについては、迅速な対応を促した。

なお、本検査実施後にもApache Struts2の別の脆弱性が明らかになっており、同ソフトウェアを使用している情報システムにおいては引き続き脆弱性情報に注意していくことが重要である。また、情報システムを使用する業務や利用環境等の事情で、ソフトウェアの脆弱性への即時の対応が困難な場合であっても、システム構成、運用方法等を改善する等により暫定的なリスク低減を図り、可能な限り速やかに恒久的な対策が実施できるようにすることが重要である。

DNSサーバ用ソフトウェアであるBINDの脆弱性対応状況について、脆弱性の有無の確認を実施し、BINDを使用している全てのDNSサーバで適切な対応が実施されていることを確認できた。今後とも、脆弱性対策のほか、統一基準群で求めているDNSのセキュリティ対策を実施することが重要である。

別添３－４　高度サイバー攻撃への対処

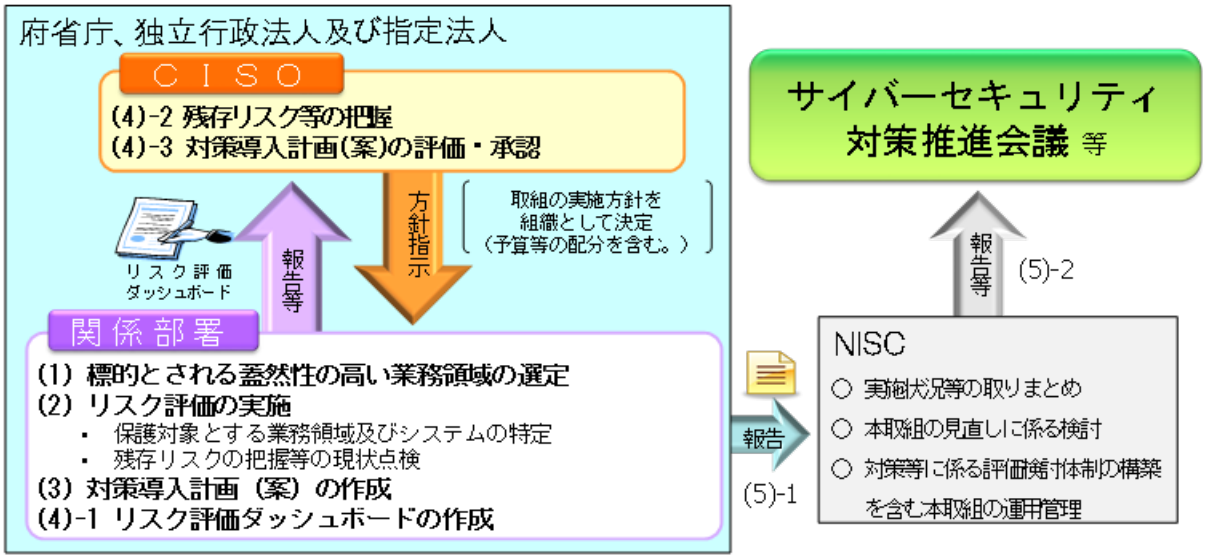
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

高度サイバー攻撃のうち、昨今、特に大きな脅威となっている標的型攻撃の主目的は、情報システム内の端末を不正プログラムに感染させることではなく、情報システム内部に侵入基盤を構築し、更に侵入範囲を拡大して重要な情報の窃取・破壊等を行うことであり、そのために組織力を動員した攻撃が行われることから、内部統制的な手法だけでは十分な防御を行うことは困難であり、情報システムにおける適切な対策の実施及び運用・監視の強化を伴う計画的で持続可能な情報セキュリティ投資が必要となる。

このため、各府省庁において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みを実現することが不可欠である。

そこで、NISCでは、その実現に向けたリスク評価手法及び標的型攻撃を始めとした高度サイバー攻撃への対策について、産学官の専門家による検討会を開催して検討を進め、2013年度後半より試行としての取組を開始し、2014年に「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（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



正式な運用を開始した初年度である2014年度においては、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システムを選定した結果、政府機関全体でおよそ40の情報システムが特定され、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、およそ５割の対象システムにおいて、各府省庁のCISOによる方針決定の下で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。

2016年度の対策実施状況の総論としては、2015年度に引き続き、全体として順調に対策強化が行われた。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110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特に重点的に取組が実施された結果、ほぼ全てのシステム及びガイドラインに掲載されている標的型攻撃手法に対して、ガイドラインに掲載されている対策又は各府省庁独自の対策が講じられており、いくつかのシステムについては2015年度から更に対策が強化されている。また、残るわずかな対策についても、今後のシステム更改等に合わせて計画的に対策を強化することとしており、2018年度までには、ガイドラインに掲載されている対策が全てのシステム・標的型攻撃手法に対して完了する計画となっている。

対象システムの中でも防御の優先度が高いシステムについては一層対策が進んでおり、2015年度末の時点で、全てのシステム及び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既に講じられており、いくつかのシステムについては2016年度には更に対策が強化されている。

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。）を適用範囲に加えた。これを受け、2016年度から、独立行政法人等においても、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システムを選定し、システムごとに対策実施状況の現状点検及び対策強化を図るための複数年にわたる計画を、予算要求等を踏まえつつ策定しているところである。

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、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、CSIRT要員の情報セキュリティインシデント対応における判断能力及び対処能力を向上させるとともに、情報セキュリティインシデントの対処が、各府省庁が定めた手順書に沿って対処できるか、その実効性を確認することを目的としたものである。

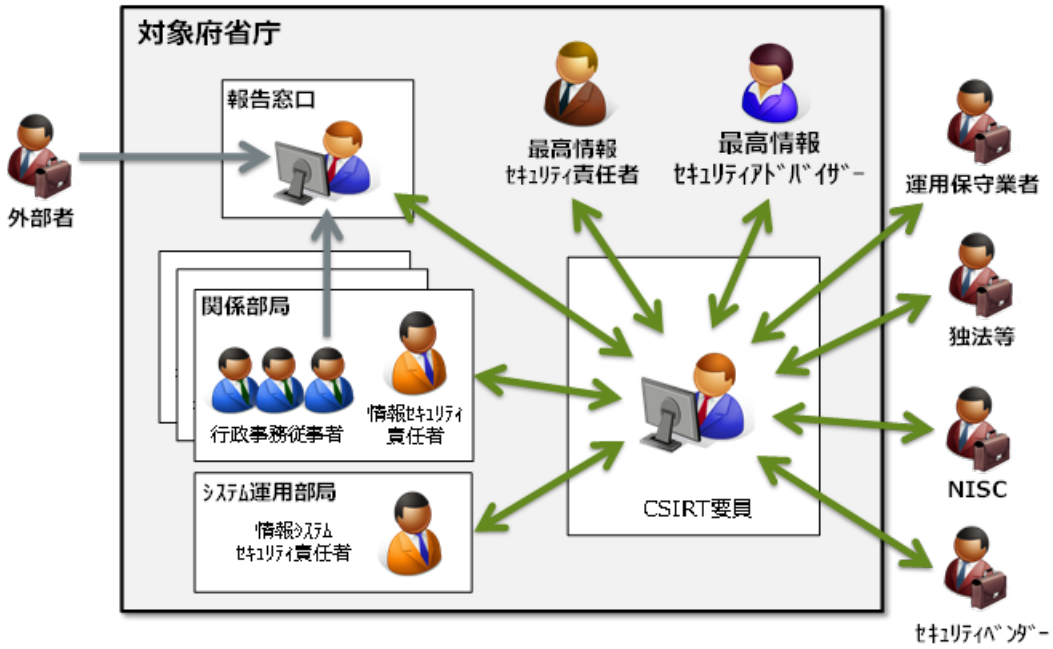
（２）概要

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。

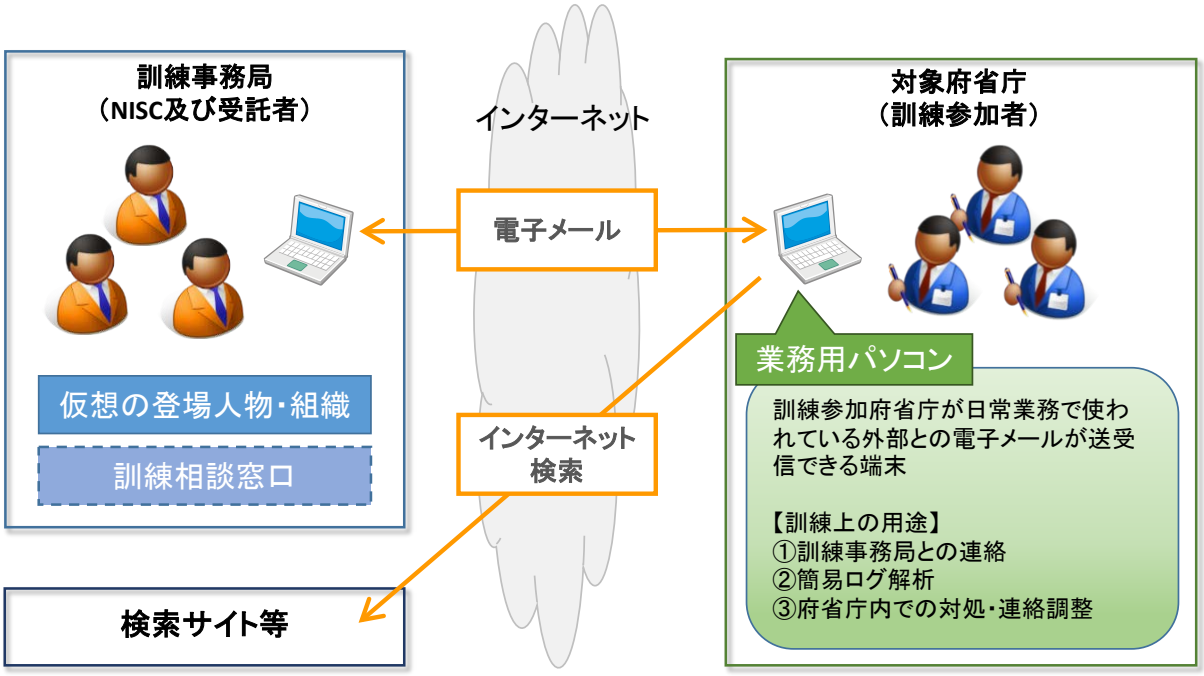
訓練参加者は、府省庁内外の様々な登場人物を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、通信ログ等の分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

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130人（全22府省庁参加）

（４）訓練時期

2016年10月～11月

（５）まとめ

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、2017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	2016年 ７月	【CSIRT会合】 ・政府機関統一基準のCSIRT関連の改正内容	NISC職員	約40名 （計１回開催）
2	2016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 ・昨今のサイバー攻撃の概要 ・情報セキュリティインシデント対処 ・代表的な攻撃 ・組織として求められる対応 ・ログの活用	外部講師	約60名 （計３回開催）
3	2016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 ・実機演習の概要 ・実機演習①～③	外部講師	約50名 （計３回開催）
4	2017年 ２月	【CSIRT会合】 ・CSIRT内の役割と人材定義 ～CSIRT活動に必要なスキルとインシデント対応の勘所～	外部講師	約30名 （計１回開催）
5	2016年 ６月～ 2017年 ２月	【CSIRT研修】 ・インシデントとハンドリングの概要 ・CSIRT等との連携について ・発生源の調査及び対応方法 ・インシデント対応実施報告の評価 ・再発防止策の策定と実施 ・最新のセキュリティ動向と対策	外部講師	延べ約200名 （７回開催）

３　NISC 勉強会

（１）目的

NISC職員による統一基準群の解説や外部有識者による最新のサイバーセキュリティに関する動向の情報等の提供により、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	2016 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	335 名 （計２回開催）
2	2016 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、監査の実施手順等の解説 ・実践編　自己点検票を利用した監査の実施	NISC 職員	324 名 （計２回開催）
3	2016 年 10 月	・独立行政法人及び指定法人に対する監査について ・独立行政法人及び指定法人におけるリスク評価の実施について ・独立行政法人及び指定法人に求められるインシデント対処について	NISC 職員	254 名 （計２回開催）
4	2017 年 １月	・サイバー攻撃が疑われる事象への初動対処及び他組織との"現実的な"情報共有 ・独法等に対するマネジメント監査における調査票及び監査の進め方について	・NISC 職員 ・外部講師	349 名 （計２回開催）

４　NISC 情報セキュリティマネジメントセミナー

（１）目的

政府機関等に対するサイバー攻撃の深刻度が増している状況やサイバーセキュリティ基本法の一部改正法の施行を踏まえ、各府省庁の独立行政法人等を所管する部署の幹部職員並びに独立行政法人等の役員及び情報セキュリティを担当する幹部職員を主な対象に、これらの法人の情報セキュリティ対策の状況及び取り組むべきセキュリティ対策につい

て解説し、情報セキュリティ対策の強化・拡充について更なる理解を促すこととする。

（２）対象

各府省庁の独立行政法人及び指定法人を所管する部署の管理職、独立行政法人及び指定法人の役員等

（３）内容

独立行政法人及び指定法人におけるサイバーセキュリティ対策の状況、最近のサイバーセキュリティの動向を踏まえた組織として取り組むべきサイバーセキュリティ対策について解説した。

実施時期：2016年12月～2017年１月

講師　　：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）、独立行政法人情報処理推進機構セキュリティセンター長等

開催回数：５回

参加人数：約260名

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

2016年度においては、2015年に発生した日本年金機構における個人情報流出事案を題材として作成した教材を用いて行うケーススタディを３回、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・演習を４回実施した。

ケーススタディにおいては、３名の講師の指導の下、インシデント発生時等における組織としての対応等についてそれぞれの専門領域をテーマとした少人数制のディスカッションを行った。

回	時期	テーマ
1	2016年 ６月	【座学①】 ・　サイバーセキュリティ・情報化審議官等の役割等について ・　政府機関等の情報セキュリティ対策のための統一基準群について

2	2016 年 ７月	【ケーススタディ①】 組織管理者としての留意点 １．組織管理者としてのインシデント対応の留意点 ２．日本年金機構事案のケーススタディ
3	2016 年 ９月	【座学②】 サイバーセキュリティ最新動向等
4	2016 年 10 月	【ケーススタディ②】 リスクマネジメントと危機管理 １．リスクマネジメントと危機管理の関係 ２．リスクマネジメントの視点 ３．危機管理の視点
5	2016 年 11 月	【座学（演習）③】 標的型攻撃体験ワークショップ
6	2017 年 ２月	【ケーススタディ③】 インシデント対応の実務
7	2017 年 ３月	【座学④】 組織における CSIRT の役割～インシデントレディネスのすすめ～

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新たに実施した。

（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：2016 年 8 月～11 月

＜カリキュラム概要＞

①情報セキュティ基礎知識
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：2016 年 11 月～2017 年３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ソフトウェア開発セキュリティ(1)
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(2)
⑥アイデンティティとアクセスの管理	⑭セキュリティの評価とテスト
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。

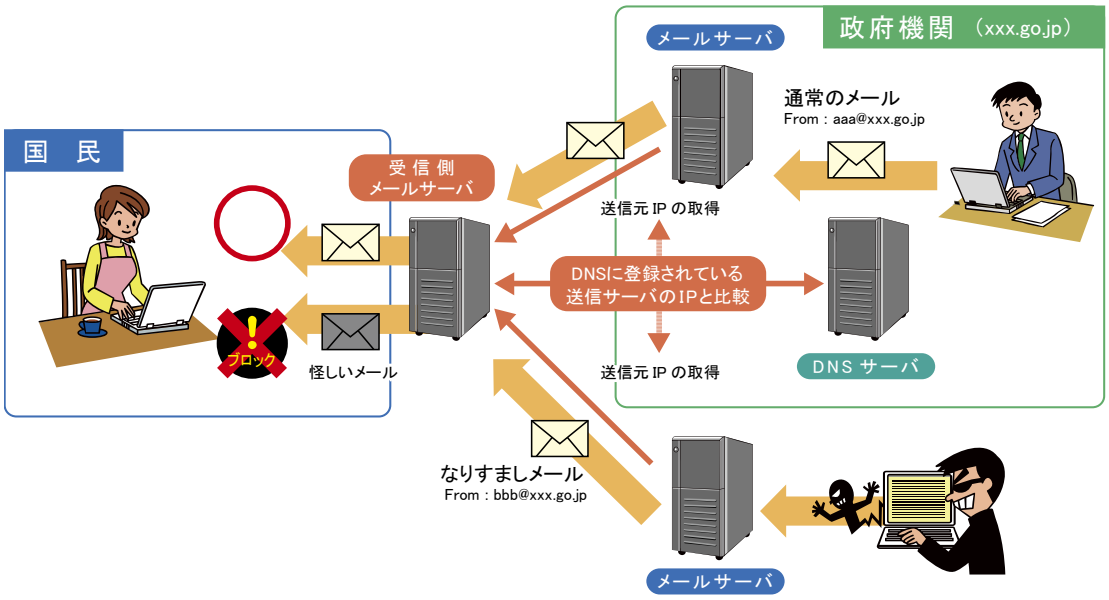
別添３－６　なりすまし防止策の実施状況

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

2016年及び2017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
2016 年１月末	71.7%	13.2%	15.1%
2017 年１月末	71.4%	15.3%	13.3%

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

※２　認証情報を公開しているが、正当な電子メールであっても認証が失敗する可能性もある。

調査の結果、SPFの設定状況は１年前と比較して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について、2015年度と同程度の割合で存在するため、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)等のSPF以外の送信ドメイン認証技術の導入についても、技術動向等を踏まえて必要な取組を推進する。

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

別添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、移行が進められた。

政府機関の暗号アルゴリズムに係る移行指針の改定概要

1　経緯

①電子政府システム（入札・申請等）において電子署名等のために広く使用されているSHA-1及びRSA1024と呼ばれる暗号方式の安全性の低下が指摘

②より安全な暗号方式（SHA-256及びRSA2048）への移行が必要であることから、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を策定

（H20年4月22日　情報セキュリティ政策会議決定）

2　政府機関における移行に向けた準備スケジュール

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

（H21年2月3日　情報セキュリティ政策会議決定）

3　移行指針の改定概要

- 切替時期について各認証基盤との調整結果を踏まえ、以下のとおり改定

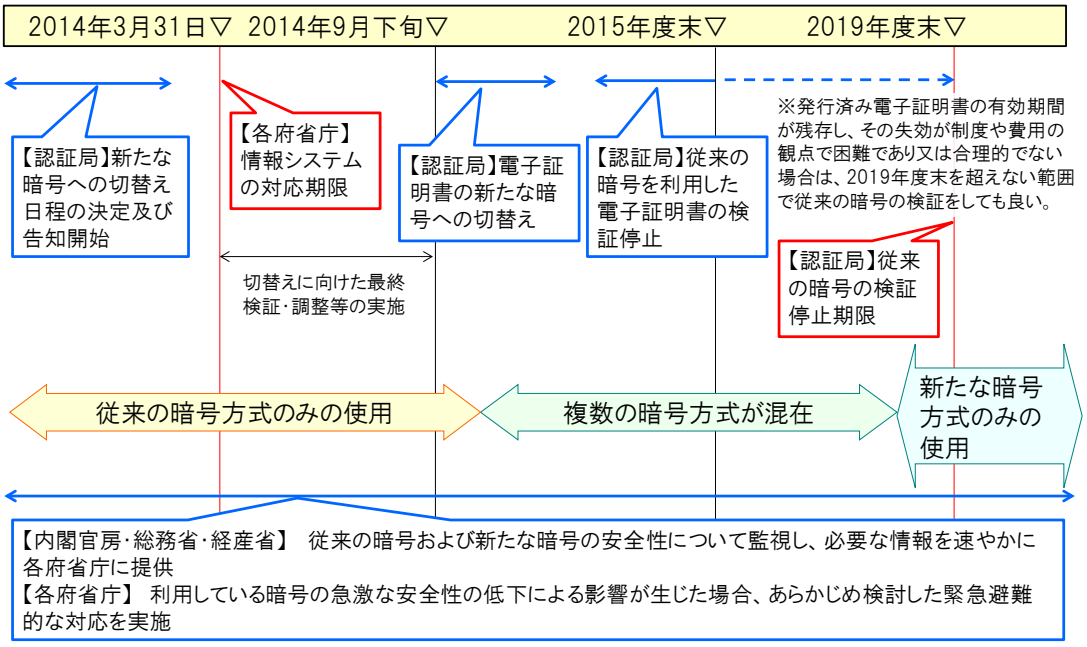
  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  a.「2014年9月下旬以降、早期に」新たな暗号方式に切替

  b.「2015年度末までに」従来の暗号方式によって発行された証明書の検証を終了

  ただし、発行済み電子証明書の有効期間が残存し、やむを得ない場合は、「2019年度末まで」検証可

（参考）政府機関における暗号移行スケジュール



[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）

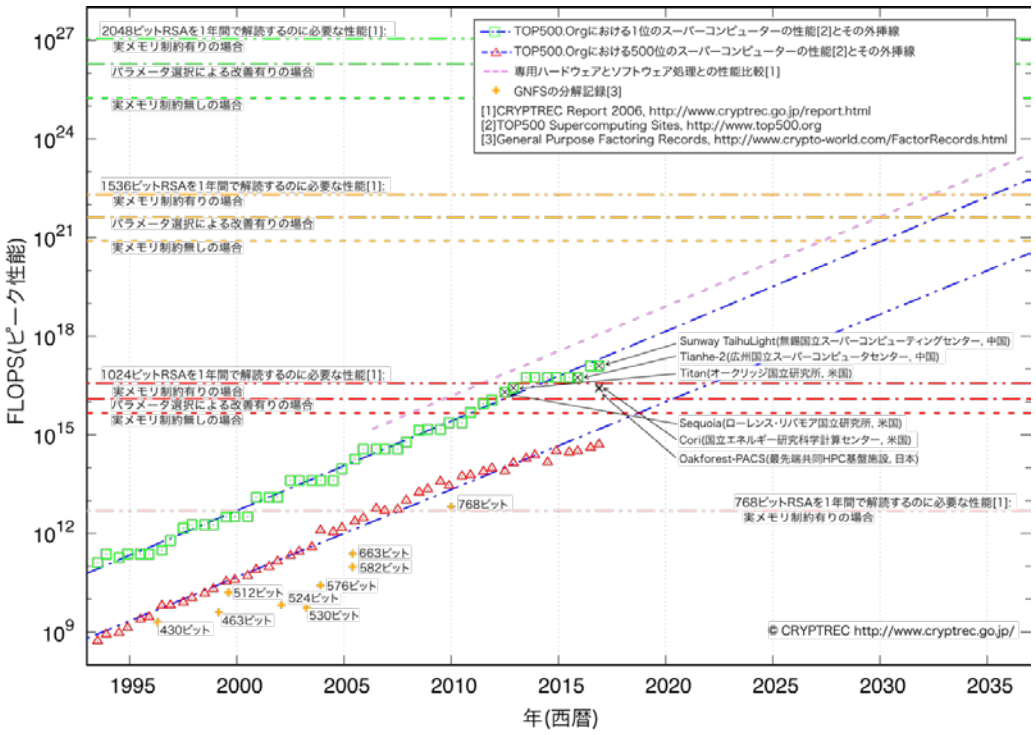
（参考）暗号の危殆化

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。

2013年度現在、実メモリの使用に係る制約を仮定する場合においても、既知のアルゴリズム（一般数対ふるい法）を用いて1024ビット素因数分解を１年間で実行するのに匹敵する演算性能が、スーパーコンピュータの「天河二号」により達成されている。

図表１　１年間でふるい処理を完了するのに必要な処理能力の予測（17 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/cryptrecrp-0002-2016.pdf［PDF］
「CRYPTREC Report 2016(暗号技術評価委員会報告)」（CRYPTREC、17 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：88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　187法人（2017年３月末日現在）

（２）調査時点

独立行政法人及び指定法人　2016年12月末日

国立大学法人等　2017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

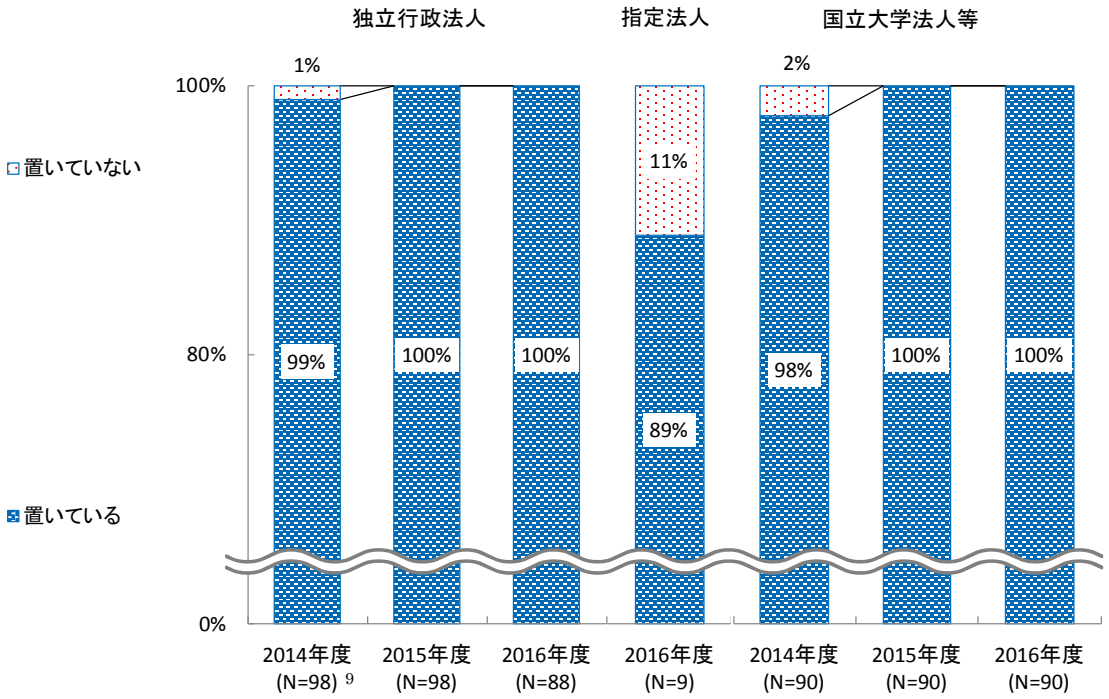
独立行政法人、指定法人及び国立大学法人等の調査結果については以下のとおりである。

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



- 独立行政法人

  CISOを置いている法人は、88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。

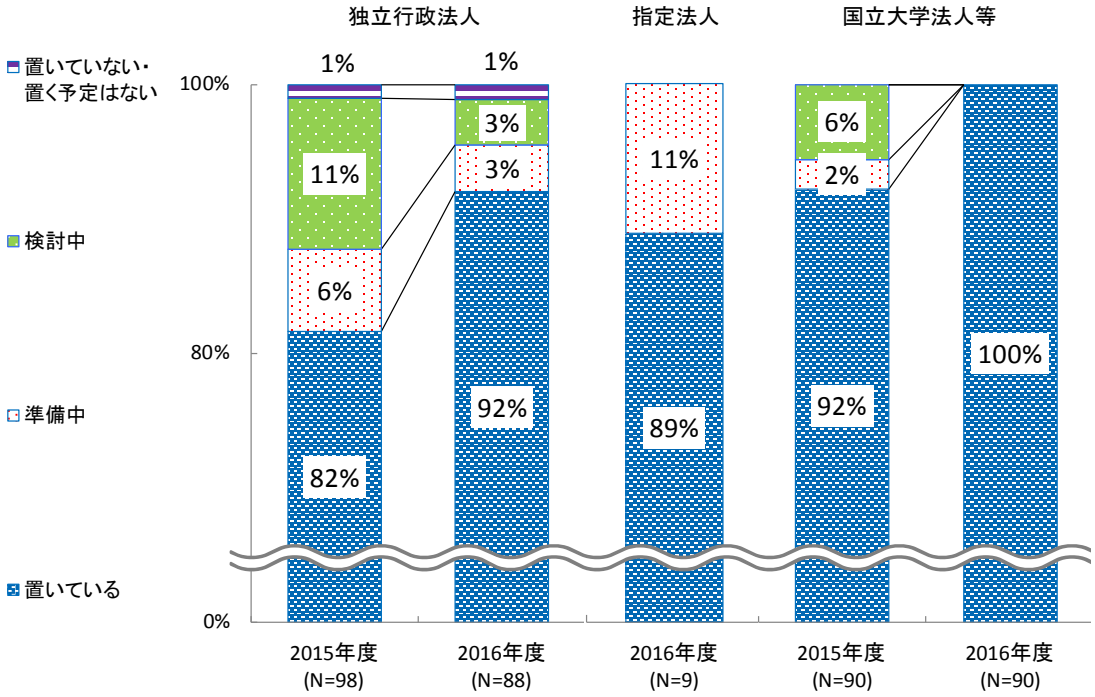
- 国立大学法人等

  CISOを置いている法人は、90法人全てである。

[9] (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



・ 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、2015年度の80法人（82%）から81法人（92%）に増加しており、準備中・検討中の法人を合わせると87法人（98%）である。

・ 指定法人

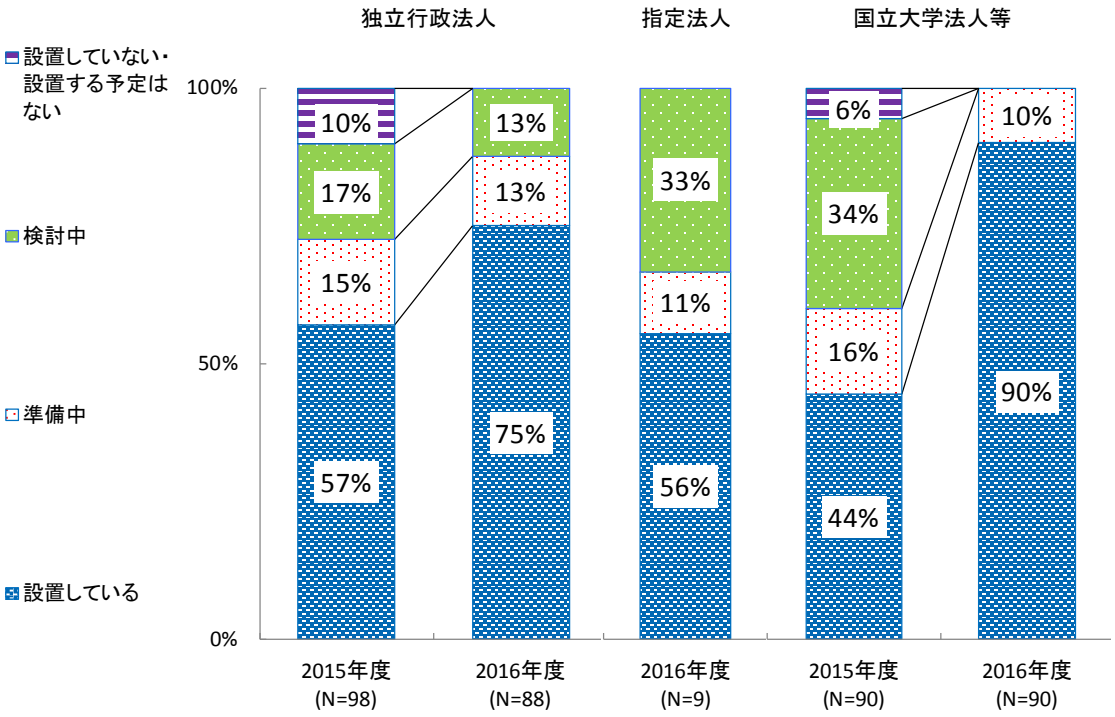
情報セキュリティ委員会を置いている法人は、８法人（89%）である。準備中の法人を合わせると、９法人全てである。

・ 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。

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、2015年度の56法人（57%）から66法人（75%）に増加している。準備中・検討中の法人と合わせると88法人全てである。

・指定法人

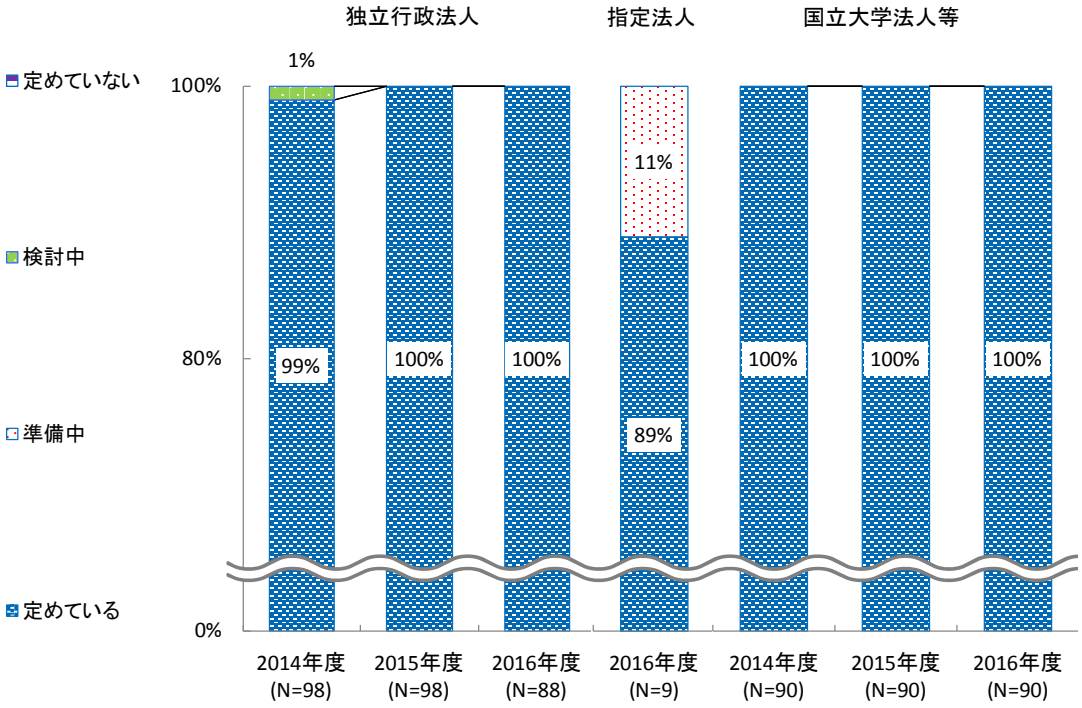
CSIRTを設置している法人は、５法人（56%）である。準備中・検討中の法人と合わせると、９法人全てである。

・国立大学法人等

CSIRTを設置している法人は、2015年度の40法人（44%）から81法人（90%）に増加している。準備中・検討中の法人と合わせると90法人全てである。

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、88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。準備中の法人と合わせると、９法人全てである。

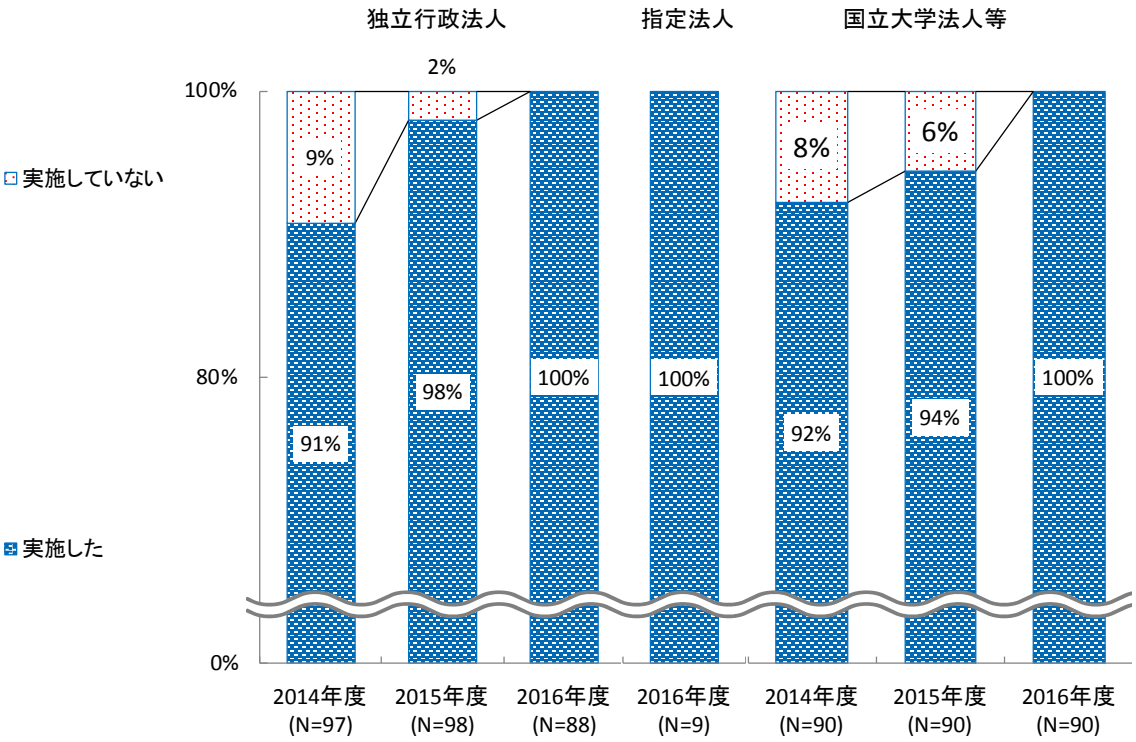
・ 国立大学法人等

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[10]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、2015年度の96法人（98%）から88法人（100%）となり、全ての法人で実施している。

・ 指定法人

教育・訓練を実施している法人は、９法人全てで実施している。

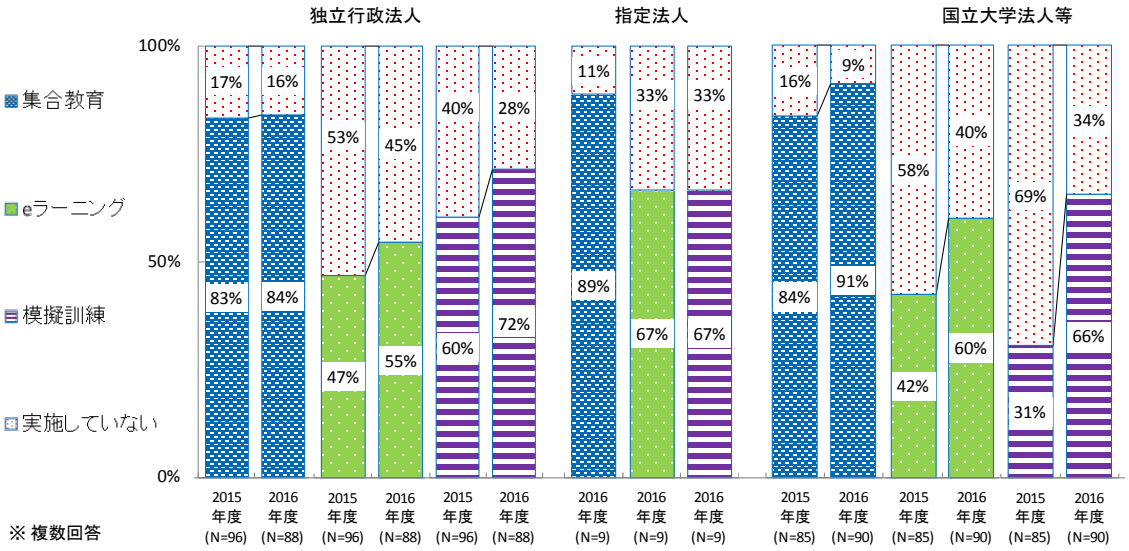
・ 国立大学法人等

教育・訓練を実施している法人は、2015年度の85法人（94%）から90法人（100%）となり、全ての法人で実施している。

[10] 教育・訓練とは、職員が情報セキュリティ関係規定への理解を深められるよう実施する、情報セキュリティに係る教育及び訓練である。

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、2015年度の80法人（83%）から74法人（84%）となっている。また、eラーニングを実施している法人は、2015年度の45法人（47%）から48法人（55%）、標的型メール攻撃等の模擬訓練を実施している法人は、2015年度の58法人（60%）から63法人（72%）といずれも増加している。

・ 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８法人（89%）である。eラーニング、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。

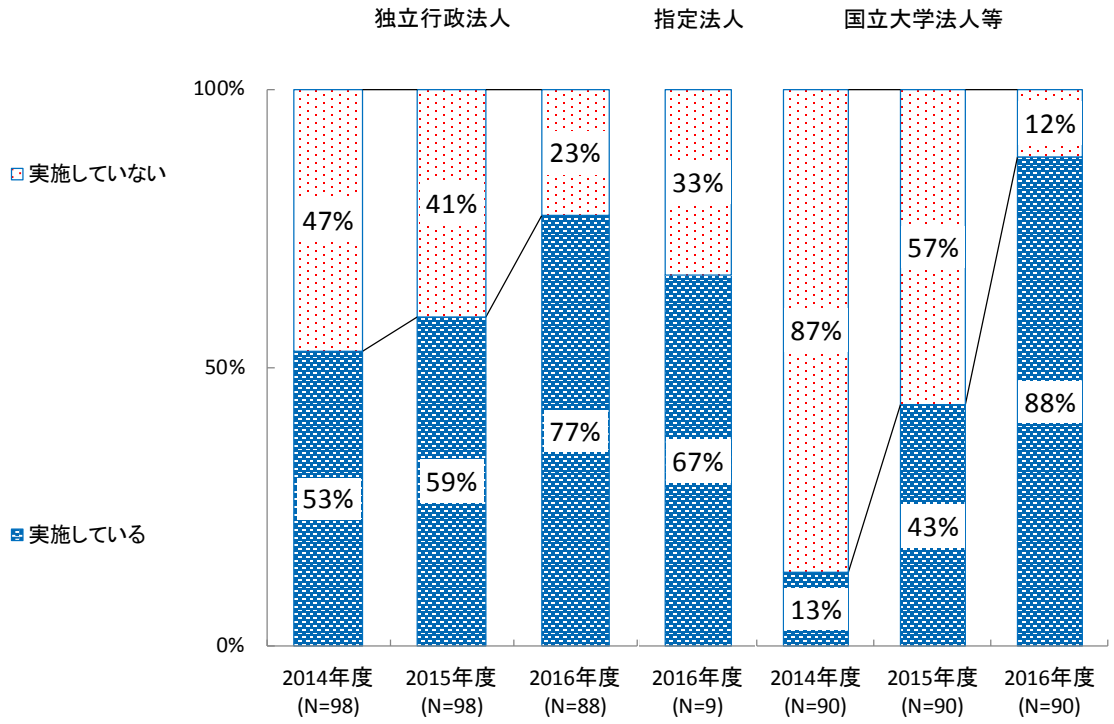
・ 国立大学法人等

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、2015年度の71法人（84%）から82法人（91%）、eラーニングを実施している法人は、2015年度の36法人（42%）から54法人（60%）、標的型メール攻撃等の模擬訓練を実施している法人は2015年度の26法人（31%）から59法人（66%）といずれも増加している。

（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、2015年度の58法人（59%）から68法人（77%）に増加している。

・指定法人

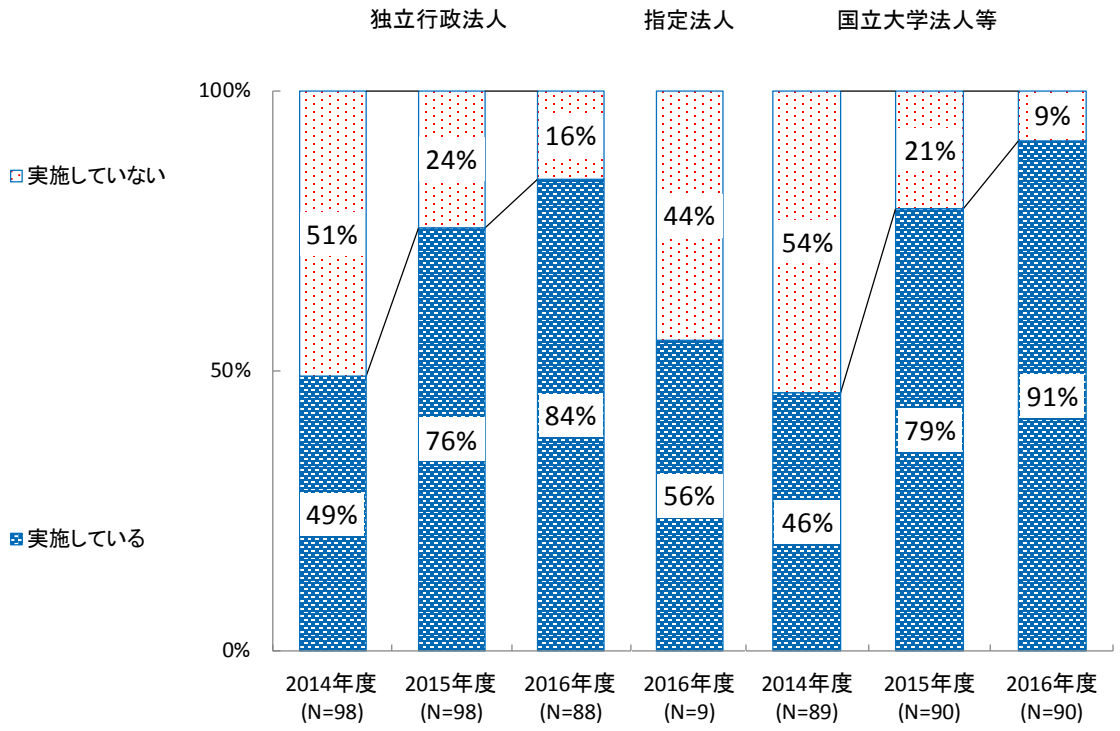
自己点検を実施している法人は、６法人（67%）である。

・国立大学法人等

自己点検を実施している法人は、2015年度の39法人（43%）から79法人（88%）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（84%）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。

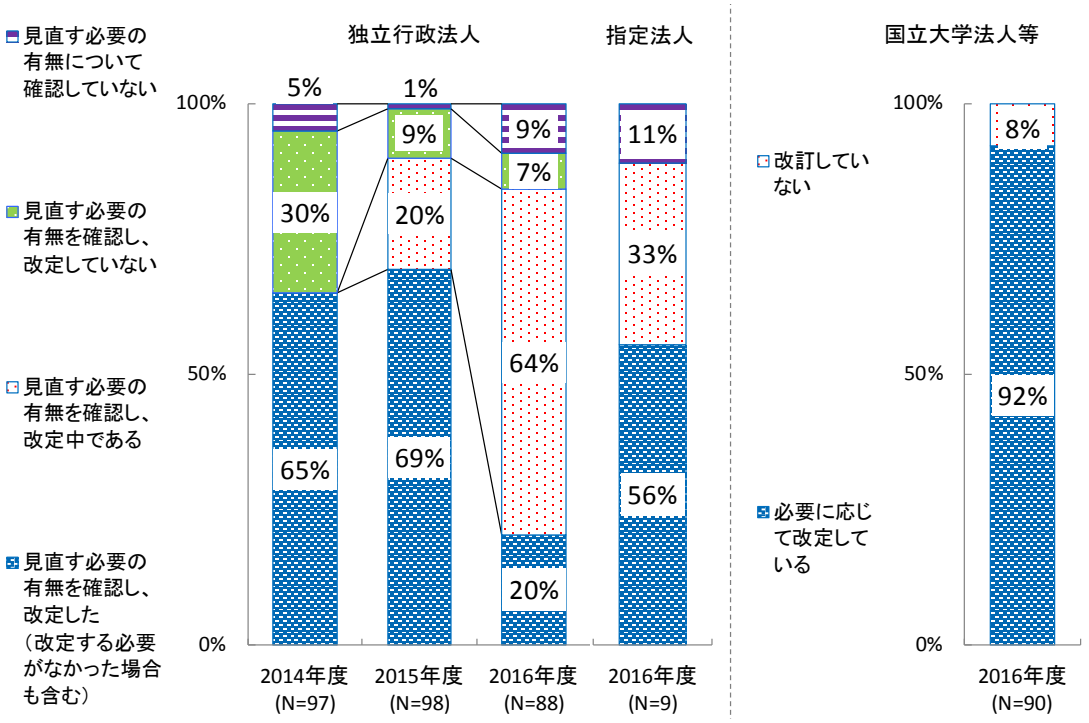
・ 国立大学法人等

情報セキュリティ監査を実施している法人は、2015年度の71法人（79%）から82法人（91%）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等の対応状況

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、74法人（84%）である。うち、56法人（64%）については、改定中である。これは政府機関の情報セキュリティ対策のための統一基準（平成28年度版）による改定と推測される。

・ 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（89%）である。

・ 国立大学法人等

情報セキュリティポリシー等を必要に応じて改定している法人は、83法人（92%）である。

４　所管する府省庁の対応

ほぼ全ての法人においてCISOが設置されるとともに、教育・訓練が実施されるなど、情報セキュリティの推進体制は年々改善されている。一方、自己点検や監査を実施している法人等は増加しているものの、まだ実施していない法人も散見される。

これらの結果を踏まえ、所管する府省庁は、情報セキュリティ対策の重要性について、意識の向上を図る取組を引き続き促進するとともに、より一層情報セキュリティ対策を講ずるよう指導等を行うことが重要である。

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　「ランサムウエアへの対処について（注意喚起）」（2016 年４月 21 日発出）

事　務　連　絡
平成 28 年４月 21 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）

ランサムウエアへの対処について（注意喚起）

最近、ランサムウエアと呼ばれる不正プログラムが、メールや不正サイト等によって広範に送り付けられているとの分析があります（※１）。

この不正プログラムに感染した場合の挙動としては、感染端末や接続されているサーバのファイルを暗号化して読み取れないようにしてしまい、その上で攻撃元からは情報を取り戻したければ身代金（ランサム）を払え、場合によっては身代金を払わなければ暗号化して人質に取った情報を勝手に公開する、などとして脅すのが主なものです。未知の脆弱性を利用し、セキュリティ製品等では検知・駆除不可なものも存在します。もちろん、身代金を払ったとしても攻撃元が情報を正常な状態に戻す、又は外部に公表しないといった行為をとる確証は全くありません。

これら不正プログラムによる被害を最小化するためには、

・OS やソフトウェアを常に最新版に保つこと
・多量のデータが格納されているサーバ等の被害を抑えるために、定期的にバックアップをとり、バックアップデータはインターネットから隔離しておくこと

その他のいわゆる標的型攻撃への対策が有効です。

なお、政府機関等の端末がこの不正プログラムに感染する場合、業務継続が不能となる、内部情報が窃取される、攻撃を受けたことが外部に知られ容易に攻撃が成功する組織として認知されるといった悪影響が主に考えられます。

各府省庁におかれましては、職員にこうした脅威の顕在化についてお知らせの上、基本的な注意や動作（不審なメールの添付ファイルを開いたりリンクをクリックしたりしない、業務に関係ないサイトの閲覧をしない、不審に気づいた際は府省庁内連絡窓口に報告する）を改めて促していただくとともに、最近のランサムウエアによる感染についても脅威として想定した上で対策を再検証し、不測の事態に備えるようお願いいたします。

＜参考＞

・独立行政法人情報処理推進機構(IPA)
　https://www.ipa.go.jp/security/txt/2016/01outline.html
※１　https://www.ipa.go.jp/security/topics/alert280413.html
・JPCERT コーディネーションセンター
　https://www.jpcert.or.jp/pr/2016/pr160002.html

２　「情報セキュリティ対策の徹底と見直しについて」（2017 年２月 21 日発出）

事　務　連　絡
平成 29 年２月 21 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）

情報セキュリティ対策の徹底と見直しについて

ソフトウェアのサポート切れや、複合機等インターネットに接続された機器等への対応については、政府機関の情報セキュリティ対策のための統一基準（平成 28 年８月 31 日サイバーセキュリティ戦略本部決定）6.2 及び 7.1.3 に規定されており、また、平成 25 年 12 月 12 日に開催した情報セキュリティ対策推進会議(CISO 等連絡会議)における申し合わせ事項「最近の情報セキュリティ問題への対処について」(別紙)に基づき、対応して頂いてきたところです。

毎年２月１日～３月 18 日までは、サイバーセキュリティ月間として、各機関において様々な取組がなされていることと思いますが、その取組の一環として、改めて別紙申し合わせの内容をご確認いただき、①ソフトウェアのサポート終了問題、及び②複合機等のインターネットに接続された機器のセキュリティ問題について、貴機関及び所管法人に対する指導等を再度徹底するとともに、所要の対策の見直しをしていただきますようお願いいたします。

なお、平成 29 年４月 11 日に Windows Vista のサポートが、同年 10 月 10 日には Office 2007 のサポートが終了する予定となっておりますので十分ご留意ください。

（参考）
○ご存じですか? OS にはサポート期限があります! - Microsoft atLife（マイクロソフト社）
https://www.microsoft.com/ja-jp/atlife/article/windows10-portal/eos.aspx
○サポート終了の重要なお知らせ - Office 2007、Exchange Server 2007、SharePoint Server 2007、Visio 2007、Project 2007（マイクロソフト社）
https://www.microsoft.com/ja-jp/office/2007/end-of-support/default.aspx
○2017 年にサポートが終了する製品（マイクロソフト社）
https://support.microsoft.com/ja-jp/help/4001737/products-reaching-end-of-support-for-2017

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

	開催日	主な議事
第 10 回	2016 年 6 月 9 日	・サイバーセキュリティ政策に係る年次報告(案)について ・サイバーセキュリティ 2016(案)について ・政府機関等の情報セキュリティ対策のための統一基準群の改定(案)について
第 11 回	2016 年 8 月 9 日	・サイバーセキュリティ 2016(案)について ・政府機関等の情報セキュリティ対策のための統一基準群の改定(案)について ・サイバーセキュリティ政策の評価に係る基本方針等の改定(案)について ・標的型攻撃等の脅威について
第 12 回	2016 年 10 月 7 日	・サイバーセキュリティ基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人について(案) ・サイバーセキュリティ基本法の一部改正に伴う関係規則等の整備(案)について ・「各府省庁セキュリティ IT 人材確保・育成計画」の作成状況等について

別添３－10　政府機関等に係る 2016 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
2016 年	４月	【概要】国立保健医療科学院は 11 日、同院をかたる大量の不審メールを確認したため、当該不審メールに対する注意喚起を HP へ掲載した。 【対応等】不審メールに関する情報とメール本文内の URL をクリックしないように依頼する注意喚起文を HP へ掲載した。	その他
		【概要】国立研究開発法人産業技術総合研究所は 13 日、北海道センターが 11 日にメールマガジンを配信した際、誤って登録者の電子メールアドレス計約 1,600 件が他の登録者の間に流出したことを公表した。	意図せぬ情報流出
	５月	【概要】日本貿易振興機構は 17 日、ジェトロ北京事務所知的財産権部ウェブサイトにおいて、一部ページが改ざんされ、対象サイトを閲覧した場合、パソコンにウィルス感染や不正プログラム侵入の恐れがあるため、公開を停止したことを公表した。	ホームページの閲覧障害
	６月	【概要】日本スポーツ振興センターは２日、toto 、BIG の当せんをかたり、メール内リンク先を開くことを求めて手数料をだまし取る等のメールが発信されており、これまでに４件の被害相談が寄せられていることを HP で公表した。	その他
		【概要】電気通信大学は３日、同大学の研究室が管理するパソコンが不正アクセスされ、学外約 280 万のメールアドレス向けに、海外銀行のインターネットバンキングのログイン ID とパスワードを窃取する目的のフィッシングメールを送信されたことを公表した。	外部からの攻撃
		【概要】山口大学は 23 日、業務用パソコンがウイルス感染し、外部との通信の事実があることから、当該パソコンに保存された延べ 20,998 名分の個人情報が流出した可能性があることを公表した。その後、８月 17 日には、当該事案を調査委託したセキュリティ調査専門会社から個人情報の流出は確認されなかったという調査結果を公表した。	外部からの攻撃
		【概要】情報通信研究機構(NICT)は６月 28 日、委託研究を受託している会社において、委託研究で利用している実験システムに関する情報が格納された外付けハードディスクドライブ（HDD）の紛失が発生したことを公表した。	意図せぬ情報流出
	７月	【概要】環境省生物多様性センターは 12 日、当該センターから 2010 年度までシステムの構築や保守運用業務を請け負っていた会社の再委託先において、業務に関する情報が格納された可能性のある外付けハードディスクドライブ（HDD）が紛失したことを公表した。 【対応等】14 日、調査の結果、すでにシステム変更が行われており、当時のシステム設計内容は現行システムに一切引き継いでいないことから、仮に情報が漏えいした場合でもインシデントに発展する可能性はないと判断した。 請負会社に対して、口頭による厳重注意を行うとともに、引き続き、紛失した HDD の捜索を実施するとともに、紛失の原因を明らかにし、当省へ報告するよう指示し、業務発注先に対し情報管理の徹底を求めるとともに、一層の情報管理の徹底をするとした。	意図せぬ情報流出
		【概要】厚生労働省は 15 日、少量新規化学物質確認通知書を e-gov 電子申請システムを介して送信処理を行ったところ、誤って別の事業者に送信するという事案が発生したことを公表した。 【対応等】関係者へ説明と謝罪を行い了承を得た。また、e-gov 電子申請システム上の送信処理を改善することとし、それまでは、印刷した通知書を事業者宛に郵送することとした。郵送に当たっては、別事業者の通知書の混入がないこと及び封筒の宛先と内容物の宛先が同一であることについて、ダブルチェックを徹底することとした。	意図せぬ情報流出
		【概要】長崎大学は 20 日、業務用パソコン１台がコンピュータウイルスに感染し、歯学部の職員及び元職員 627 名分の個人情報を含む職員名簿等のデータが漏洩した可能性があることを公表した。 現在のところ，本件による個人情報の不正使用等の被害は確認されていない。	外部からの攻撃
	８月	【概要】広島大学は５日、同大学大学院社会科学研究科で使用している 437 名分の個人情報が保存されたパソコンから、マルウェア感染が原因と思われる外部への暗号化された通信が行われていたことについて公表した。 現時点で、本件の個人情報が第三者に流出したという情報や、不正に使用された事実は確認されていない。	外部からの攻撃

年月 (※1)		情報セキュリティインシデントの概要・対応等 (※2)	種別
	９月	【概要】茨城労働局は１日、「若年者地域連携事業」（委託事業）において、受託事業者が開催するセミナーのインターネット上の申し込みフォーム確認画面に既申込者の 17 名の個人情報が表示される事案について公表した。 【対応等】当該事業者に個人情報の厳格な管理を指示するとともに、すべての委託事業の受託者に個人情報の緊急点検の指示と報告を求めた。	意図せぬ情報流出
		【概要】佐賀大学は５日、同大学海洋エネルギー研究センターで、学生と教職員 138 名分の個人情報が保存された業務用パソコンがマルウェア感染したことを公表した。	外部からの攻撃
		【概要】神戸大学は７日、業務用パソコン２台がマルウェアに感染、うち１台がランサムウェアに感染し、端末やネットワークストレージ上のファイルが暗号化された。もう１台は卒業生等の個人情報が格納されていたが、情報の流出は確認されていない事を公表した。	外部からの攻撃
		【概要】環境省は 15 日、生物多様性センターのホームページが閲覧できない状況になったことを公表した。 【対応等】原因調査と復旧に向けた作業を実施するとともに、センターホームページでは個人情報や希少種に関する機微な情報は扱っておらず、情報の流失はないとした。外部から攻撃の可能性もあったが、攻撃による閲覧障害かどうかは不明であった。	ホームページの閲覧障害
		【概要】日本政府観光局（JNTO)は 21 日、同日午前２時、米国向けホームページ内の一部のコンテンツにおいてプレスリリースタイトル及びリンク先ページの改ざんを確認し、当該ページを閉鎖したことを公表した。	ホームページの閲覧障害
		【概要】国立高等専門学校機構は 28 日、９月 23 日未明から昼過ぎにかけてサービス不能攻撃を受けたため、当サイトがアクセスしにくい状態になっていたことを公表した。	ホームページの閲覧障害
	10 月	【概要】住宅金融支援機構は６日、同機構が業務委託している企業のメールサーバが不正アクセスを受け、同機構のお客様の情報が流出した可能性があることを公表した。	外部からの攻撃
		【概要】富山大学は 10 日、水素同位体などについて研究している施設がサイバー攻撃を受け、研究者のパソコンから個人情報や公知の研究成果が流出した可能性があることを公表した。	外部からの攻撃
		【概要】京都労働局は 20 日、京都西陣公共職業安定所園部出張所において、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」に誤って求職者の携帯電話番号を掲載するという事案が発生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求職情報を公開している求職者について、個人情報その他不必要な情報の掲載がないか、至急点検するとともに、個人情報の取扱いに関する研修を実施することなど、個人情報の厳格な取扱いの徹底を指示した。	意図せぬ情報流出
		【概要】埼玉労働局は 31 日、受託事業者の担当者が、127 件の個人情報が登録された業務用携帯電話を帰宅途中に紛失し、後日、交通機関より回収したことを公表した。 【対応等】紛失期間中に通話記録がないこと及び現在までに利用者に対して実害がないことを確認し、関係者全員に謝罪文を送付し、受託事業者へ携帯電話の管理、個人情報の重要性の周知徹底を実施した。	意図せぬ情報流出
	11 月	【概要】外務省は４日，外務省職員をかたるウィ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，当該不審メールに対する注意喚起を HP へ掲載した。 【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 HP へ掲載した。	その他
		【概要】情報通信研究機構（NICT）は 11 月４日、業務に関係するファイルが保存されたノート PC の紛失が判明し、警察署に紛失届けを提出したが、現時点で発見に至っていないことを公表した。	意図せぬ情報流出
	12 月	【概要】公正取引委員会は 12 月 16 日に，同委員会を装った「なりすましメール」が不正に発信されていると発表。 【対応等】公正取引委員会は，公正取引委員会とは無関係の者が同委員会を詐称して「なりすましメール」を不正に発信されているとホームページに公表し，注意喚起するとともに，「なりすましメール」の不正発信について，関係省庁に連絡した。	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】石川労働局は 22 日、金沢公共職業安定所の付属施設である金沢新卒応援ハローワークにおいて、来春の大学等卒業予定者で当該ハローワークを利用して求職活動中の学生に対し、就職面接会の案内に係るメールを送信する際に、複数のメールアドレスを「ＢＣＣ」に入力の上、送信するべきところを、「宛先」に入力して送信したため、宛先となった 235 件のメールアドレスが他の受信者に漏えいしたことを公表した。 【対応等】管内全公共職業安定所長に対して、本件について情報提供するとともに、同様の事案が発生しうる状況にないか早急な確認を行うよう注意喚起を行った。	意図せぬ情報流出
2017 年	１月	【概要】文部科学省は 10 日、４日に中堅幹部や若手職員ら約 30 人の人事異動案を担当者が誤って全職員にメールで一斉送信していたと発表。 【対応等】全職員に対し、謝罪と当該メールの削除依頼をメール送信により行った。また、誤送信の再発防止のため、メール送信の際の宛名設定の操作方法の改善を図るとともに、全職員に対し注意喚起を行った。	その他
		【概要】厚生労働省は 12 日、同省労働基準局で 12 月 27 日に外部の公益社団法人へメールを送信する際にファイルを取り違え、誤って個人情報を含む別文書を添付する事案が発生したことを公表した。 【対応等】関係者へ説明と謝罪を行い了承を得た。また、再発防止策として、個人情報等を含む資料をスキャナで読み取り、メールでファイルを送信する場合には、添付後に当該ファイルを開いて正しいファイルが添付されているか確認することを徹底することとした。	意図せぬ情報流出
		【概要】埼玉労働局は 12 日、職業安定部地方訓練受講者支援室が担当する受託事業の受託事業者において、利用者 27 名に対しセミナー案内メールを送信する際に「BCC」で送信すべきところを誤って「CC」で送信したため、全受信者のメールアドレスが表示された事案について公表した。 【対応等】本事案を管内関係機関に周知し、メールアドレス誤送信を含む個人情報漏えいの防止について、再徹底の指示などを実施した。	意図せぬ情報流出
		【概要】国立研究開発法人産業技術総合研究所は 13 日、12 日に中国センターにおいてメール誤送信が発生し、外部の関係者 28 人を含む 77 人のメールアドレスが流出したことを公表した。	意図せぬ情報流出
		【概要】独立行政法人製品評価技術基盤機構は 26 日、当該機構認定センターの認定審査業務において、事業者の担当者氏名 21 名分及び審査に関する情報の一部が記録された USB メモリが 2017 年１月 17 日に盗難された事を公表した。	意図せぬ情報流出
	２月	【概要】独立行政法人勤労者退職金共済機構は３日、同機構のメールアドレスを装ったいわゆる「なりすましメール」が不正に発信されるという事案が確認されたことを公表した。	その他
		【概要】公正取引委員会は２月７日に，同委員会を装った「なりすましメール」が不正に発信されていると発表。 【対応等】公正取引委員会は，公正取引委員会とは無関係の者が同委員会を詐称して「なりすましメール」を不正に発信されているとホームページに公表し，注意喚起するとともに，「なりすましメール」の不正発信について，関係省庁に連絡した。	その他
		【概要】外務省は９日，「最新海外安全情報メールサービス」をかたる不審メールを確認したため，当該不審メールに対する注意喚起を HP へ掲載した。 【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 HP へ掲載した。 なお，「最新海外安全情報メールサービス」は 2016 年 12 月 31 日をもって終了していることを付記。	外部からの攻撃
	３月	【概要】独立行政法人地域医療機能推進機構神戸中央病院は８日、同院の医師が、附属看護専門学校の講義に使用するため、同院で検査した患者様 10 名の個人情報を保存した私物 USB メモリを紛失していたことが、2017 年２月３日に拾得された方が同院宛に匿名にて郵送頂いたことにより判明し公表した。	意図せぬ情報流出
		【概要】独立行政法人住宅金融支援機構は 10 日、同機構の団体信用生命保険特約制度のクレジットカード払いに係る事務を委託している会社より、同社の機構団体信用生命保険特約料クレジットカード支払いサイトに対して Apache Struts2 の脆弱性を悪用した不正アクセスがあり、同機構の顧客の個人情報が流出した可能性があるとの報告を受け公表した。	外部からの攻撃

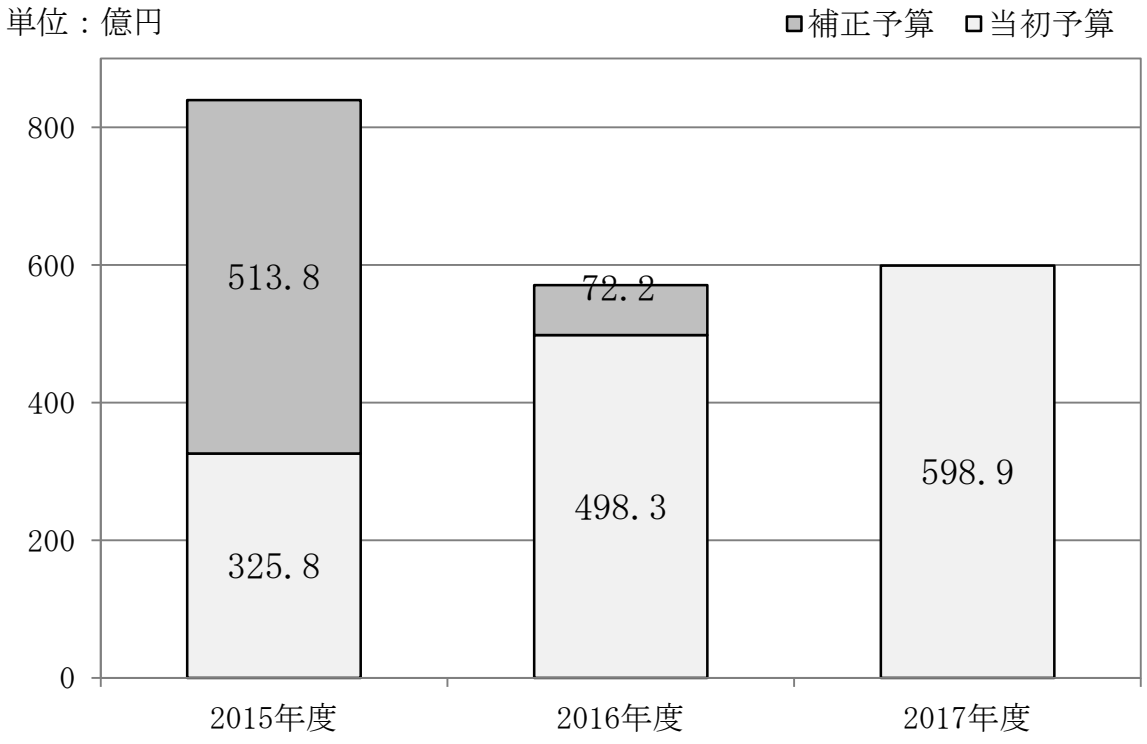
年月 (※1)		情報セキュリティインシデントの概要・対応等 (※2)	種別
		【概要】独立行政法人日本貿易振興機構は 10 日、同機構のウェブサイトの相談利用者様登録ページが外部からサイバー攻撃を受け、一部の情報が消去され、過去に利用者様登録ページ利用の 26,708 件のメールアドレスが窃取された可能性があることを公表した。	外部からの攻撃
		【概要】国立研究開発法人科学技術振興機構は 10 日、科学技術情報発信・流通総合システム（J-STAGE）が、３月８日に外部からの攻撃を検知したため、現在サービスを停止し、セキュリティ対応のための緊急メンテナンスを行っていることを公表した。	外部からの攻撃
		【概要】独立行政法人工業所有権・情報研修館（INPIT）は９日、特許情報プラットフォーム（J-PlatPat）サービスが、外部からの攻撃を検知したため、現在サービスを停止し、セキュリティ対策を行っていると公表した。	外部からの攻撃
		【概要】岡山大学病院は 24 日、15 日に当該病院においてログ解析用ソフトにより医療用端末を解析したところ患者個人情報２名分が保存された医療用端末２台がウイルスに感染し、外部との通信を行っていたことが判明、電子カルテなどの医療情報システム、基幹システムへの不正アクセスは確認されていないことを公表した。	外部からの攻撃

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

別添３－11　政府のサイバーセキュリティ関係予算額の推移

	2015 年度	2016 年度	2017 年度
当初予算額	325.8 億円	498.3 億円	598.9 億円
補正予算額	513.8 億円	72.2 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

「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、サイバー攻撃や自然災害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

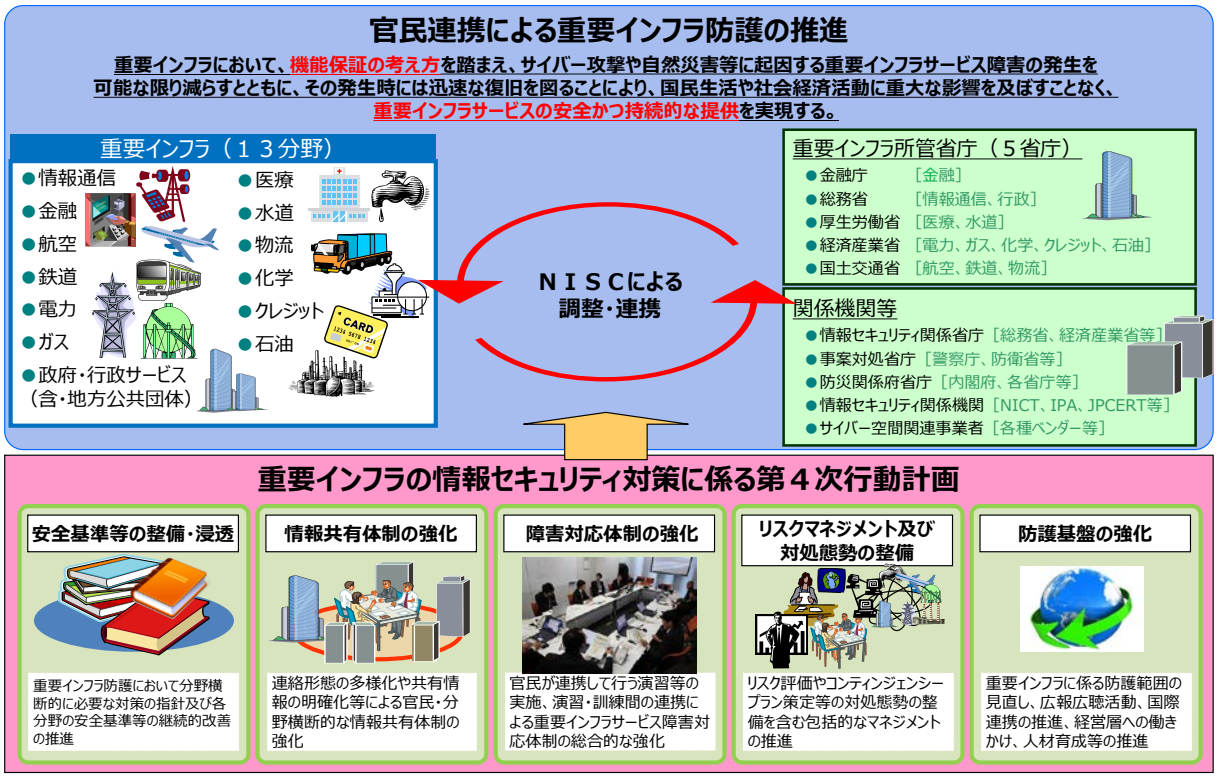
■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 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、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

「基本的な考え方」

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。
重要インフラ全体の機能保証の観点から、官民が一丸となった重要インフラ防護の取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

第４次行動計画　施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的として、セキュリティ対策のPDCAに沿って「指針」及び「安全基準等」の継続的改善を推進する。

※安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称
※指針・・・・・・安全基準等の策定・改定に資するため、分野横断的に必要度の高い対策項目を収録したもの

現状の課題

- 自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である

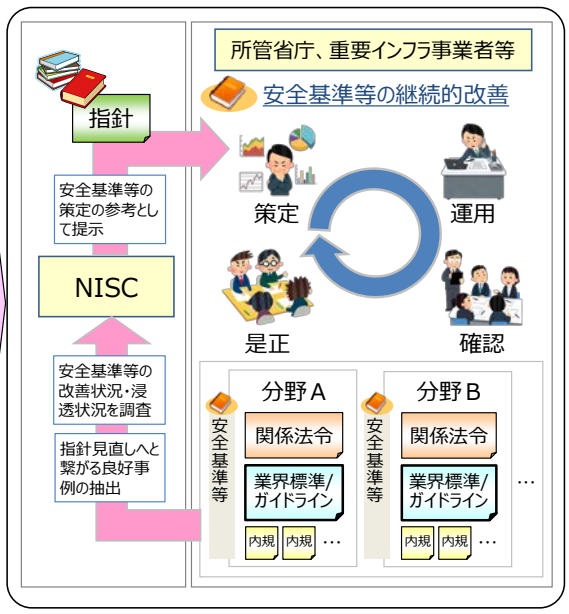
行動計画期間中の施策

（１）　指針の継続的改善
- 情報セキュリティ文化の醸成やPDCAサイクルの実行に責任を持つ経営層が認識すべき事項及び行動を指針改定時に詳細化
- 機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の対処態勢整備の必要性を指針改定時に明記

（２）　安全基準等の継続的改善
- セキュリティ対策のPDCAサイクルに沿った業界標準/ガイドラインの改善プロセスの推進
- 情報セキュリティの取組の保安規制への位置付けや、関係法令等におけるサービス維持レベルの具体化等、制度的枠組みを適切に改善する取組の継続的な実施

（３）　安全基準等の浸透
- 重要インフラ事業者等への毎年のアンケート調査により、セキュリティ対策状況を把握するとともに、アンケートへの回答を通じ、事業者等が対策の課題、解決策等を認識可能となるよう支援

第４次行動計画に基づく取組



第３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

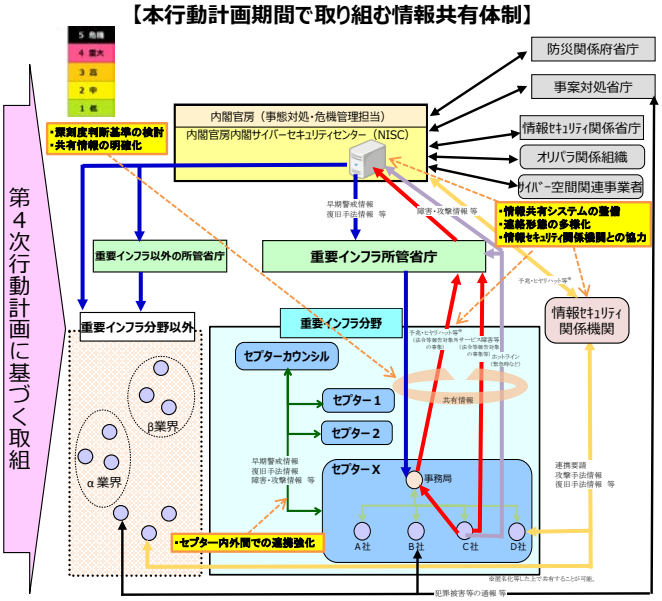
（１）情報共有体制の充実
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（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３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

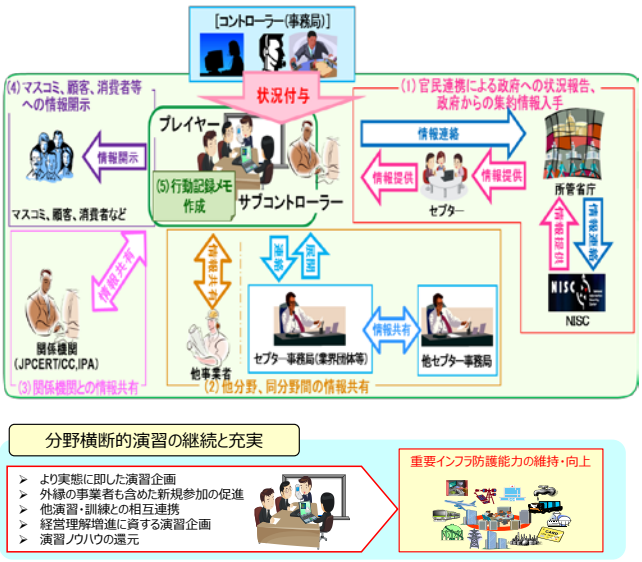
行動計画期間中の施策

（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

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上

第３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

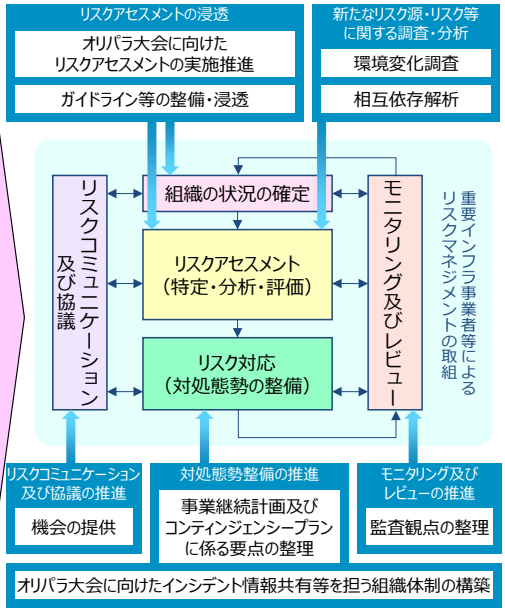
（１）リスクマネジメントの標準的な考え方

（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３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

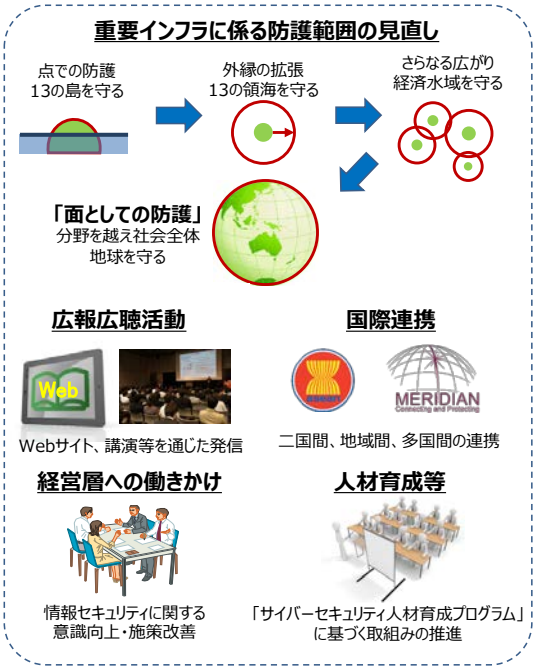
（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

（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

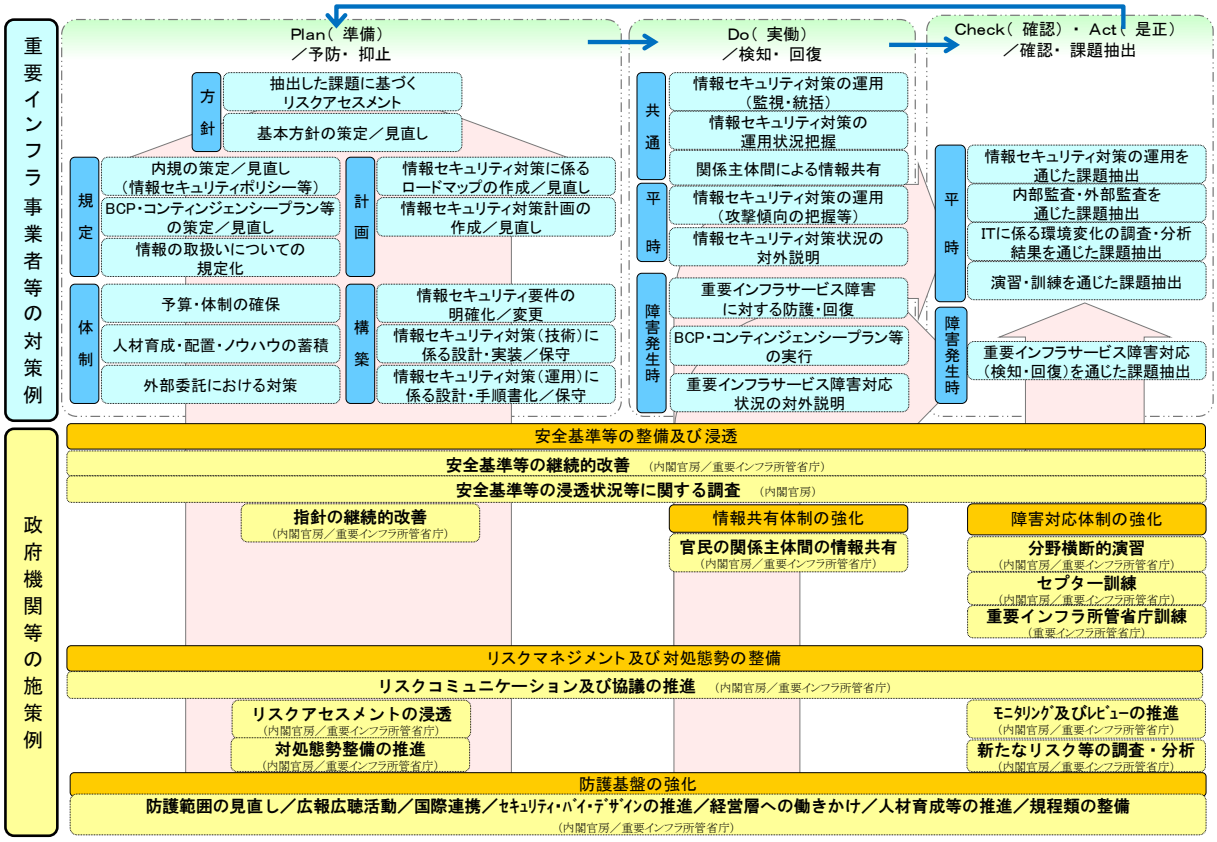
（４）経営層への働きかけ
- 情報セキュリティに関する経営層の意識向上のための働きかけ

（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３次行動計画」（以下「第３次行動計画」という。）に基づく取組について、2016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３次行動計画全体に関する取組

(1)　第３次行動計画の概要

第３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）」及び「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）」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、2014年５月に情報セキュリティ政策会議で策定された。また、重要インフラ分野として新たに追加した３分野に関する記載の追記、及びサイバーセキュリティ基本法の施行を受けた組織体制の変更に伴い、2015年５月には、サイバーセキュリティ戦略本部で第３次行動計画の一部改訂が行われている。

第３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「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

2016年度は、第３次行動計画の最終年度に当たり、引き続き第３次行動計画に従って５つの施策それぞれについて取組を進めた。各施策の取組等の詳細は次節以降に示すが、重要インフラ事業者等から内閣官房への情報連絡が前年度比約２倍と活発に行われたほか、過去最大規模での分野横断的演習の開催、2020東京オリンピック・パラリンピック競技大会（以下、「オリパラ大会」という。）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」の整備・公表など、各種取組の着実な成果を得た。なお、第３次行動計画における施策の枠外の取組として、2015年度に引き続き、ＩＴ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４－９）。

また、2016年３月にサイバーセキュリティ戦略本部において決定した「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、第３次行動計画の成果と課題をとりまとめ、同計画の基本的骨格（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た「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下、「第４次行動計画」という。）を策定した。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。なお、第４次行動計画に記載した事項のうち、特に必要なものについては、同計画の決定に先駆け2016年度中に着手している。

(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３次行動計画の各施策における取組

本節においては、第３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３次行動計画のV.3.2に記載される各施策において期待される成果

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３次行動計画における本施策の期待される成果及び具体的な指標は次のとおりである。

＜期待される成果＞
・情報セキュリティ対策に取り組む関係主体が、必要な取組を定期的な自己検証の下で行うことの実現に向けた、重要インフラ事業者等における各種対策の更なる充実とその着実な実践
＜具体的な指標＞
・指針に採録した対策項目数
・安全基準等の浸透状況等の調査にて把握した、安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の割合
・重要インフラ事業者等による指針への意見・要望

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３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、次回の指針の改定に向け、安全基準等の改善状況調査及び安全基準等の浸透状況等調査を通じて、指針の見直しにつながる良好事例等を収集したほか、行動計画の見直しを通じて、指針改定の方向性をまとめた。

○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、10の分野において安全基準等の改善を行ったほか、３つの分野において改善に向けた分析・検証に着手している。

○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、3,144件の回答が得られ、分析の結果、重要インフラ事業者等の定期的な自己検証への取組は７割強の実施率であった。良好な点として、標的型攻撃等のリスクへの関心が高まり、対策が進んでいること等が認められた。一方、事業継続計画の策定状況等については更なる調査が必要である。

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、良好事例及び課題、指針への意見・要望の収集を行った。指針への意見・要望としては、指針の内容に関する説明の充実等があった。

イ　今後の取組

2016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、指針に関して、第４次行動計画に記載されている方針に基づき改定するとともに、重要インフラ所管省庁と連携し、制度的枠組みを適切に改善する取組の継続的な推進を図る。また、浸透状況等調査の充実を図る。

(2)　情報共有体制の強化

第３次行動計画における本施策の期待される成果及び具体的な指標は次のとおりである。

＜期待される成果＞
・最新の情報共有体制及び情報連絡・情報提供に基づく情報共有、並びに各セプター及びセプターカウンシル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、活用できるようになっていること。
＜具体的な指標＞
・内閣官房による情報連絡・情報提供の件数
・セプターカウンシルや分野横断的演習等の関係主体間の情報交換の開催回数
・セプターカウンシルにおける情報共有の件数

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３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。2016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や情報セキュリティ関係機関等から内閣官房に対して897件の情報連絡が行われ、内閣官房からは80件の情報提供を行っている（参考：別添４－５）。

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
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
関係省庁・関係機関から内閣官房への情報共有件数	27件	52件	41件
内閣官房からの情報提供件数	38件	44件	80件

なお、第４次行動計画の策定過程において、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提言されたことを踏まえ、関係主体の理解を得た上で、情報連絡手順の整備に取り組んだ。

また、重要インフラサービス障害に係る深刻度判断基準の具体化に向けた検討にも着手している。

大規模ＩＴ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ＩＴ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、2017年２月の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４－６）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど重要インフラ防護の関係主体間における情報連携の結節点としても機能している。また、一部の分野についてはISACが設立、または拡大されるなど自主的な分野内情報共有体制が確立された。

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、2016年４月の総会で決定した活動方針に基づき、2016年度に、運営委員会（４回）、相互理解WG（４回）、情報収集WG（４回）、総会準備WG（３回）を開催し、セプター間の情報共有や事例紹

介等、情報セキュリティ対策の強化に資する情報収集や知見の共有を行った。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。

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（深刻度判断基準の策定、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。

(3)　障害対応体制の強化

第３次行動計画における本施策の期待される成果及び具体的な指標は次のとおりである。

＜期待される成果＞
・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、重要インフラ事業者等のＩＴ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に対する貢献
＜具体的な指標＞
・分野横断的演習の参加者数
・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、重要インフラ事業者等における、ＩＴ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に貢献するとともに、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３次行動計画に基づく基本方針として、前年度に引き続き「事業者等による障害対応能力の向上」、「重要インフラ全体の対策水準の底上げ」、「関係主体間の連携・維持の強化」、「国は事業者等の自律的かつ継続的な取組を支援」を掲げ、具体的な取組の方向性として「課題抽出を通じた改善の促進」、「参加対象の裾野拡大」、「情報共有体制の検証」、「ＮＩＳＣの施策への活用」を決定し、実施した（参考：別添４－７）。

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、参加機関数は約5.4倍（94組織→505組織)、参加者数は約6.0倍（348名→2,084名）にそれぞれ増加した。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の充実を図った。

表２　分野横断的演習参加機関・参加者数の推移

年度	2014	2015	2016
参加機関数	94組織	302組織	505組織
内、地方会場参加	(10組織)	(66組織)	(153組織)
内、自職場参加	(15組織)	(36組織)	(109組織)
参加者数	348名	1,168名	2,084名
内、地方会場参加	(32名)	(149名)	(378名)
内、自職場参加	(59名)	(315名)	(989名)

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は、「有意義だった」が66.7%、「概ね有意義だった」が33.3%であった。分野横断的演習を含め組織内外で実施する演習・訓練への参加状況については、「自社で実施している」と回答した事業者が68.2%、「今後実施予定」が13.0%であった。また、「組織外で実施する演習」への参加率は69.3%、「今後参加予定」は7.3%となっている。

○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４－８）。

表３：参加セプター・参加事業者等数の推移

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

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検証、情報提供における脆弱性情報として分野固有のシステムの例示など、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、金融業界横断的なサイバーセキュリティ演習（Delta Wall）を実施した。

イ　今後の取組

第３次行動計画策定当初の2014年度に決定した分野横断的演習の基本方針及び取組の方向性を維持しつつ、第４次行動計画に基づき、セキュリティ意識の高まりと旺盛なニーズに応える演習企画の検討、各事業者のセキュリティ対策のＰＤＣＡに資する演習運営の検討、情報共有体制の実効性向上に係る施策の検討、演習運営ノウハウや知識等の還元の検討について取り組む。

セプター訓練については、例年多くの事業者等の参加実績を有した本件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踏まえた訓練の実施等、訓練内容の充実に取り組む。

(4)　リスクマネジメント

第３次行動計画における本施策の期待される成果及び具体的な指標は次のとおりである。

＜期待される成果＞
・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
＜具体的な指標＞
・内閣官房が実施した環境変化調査や相互依存性解析の件数
・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できる機会の開催回数

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。これにより、重要インフラ事業者等が主体的にリスクマネジメントを実施し、官と民、民と民における双方向のコミュニケーション及び協議が促進された。

なお、第４次行動計画の策定過程において、その重要性が改めて確認された当該ガイドラインの一般の重要インフラに適用するための一般化、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むべき要点等に関する検討にも着手している。

〇リスクアセスメントに対する支援

内閣官房は、第３次行動計画に記載されている環境変化調査の関連調査として、EU諸国及び米国における情報共有体制に関する調査を行い、その調査結果を重要インフラ事業者等に対して公表[1]した。これは、EU諸国及び米国における情報共有体制の状況及びその背景にある法制度等を含む環境の変化について把握し、情報共有体制の強化に係る施策に活用するとともに、各重要インフラ事業者等が実施するリスクアセスメントの参考情報として利活用できるようにしたものである。

〇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。

〇リスクマネジメントに利活用できる手引書等の整備

内閣官房は、個々の重要インフラ事業者等のリスクマネジメントにおいて利活用できる手引書等の整備について、オリパラ大会をテストケースと定め、関連事業者等が行うリスクアセスメントのガイドラインとして、「機能保証に向けたリスクアセスメント・ガイドライン」を整備し、公表[2]した。さらに、大会に係る重要サービスを提供する事業者等によるリスクアセスメントを、当該ガイドラインに基づいて実施し、その結果報告等から更なる改善に向けた課題を抽出した。

イ　今後の取組

これまでの「リスクアセスメント」、「リスクコミュニケーション及び協議」等の推進に係る施策の充実を図るとともに、第４次行動計画に基づき、各重要インフラ事業者等がリスクアセスメント結果に基づく適切な意思決定を行うための内部統制の強化や、各重要インフラ事業者等が主体的かつ自律的に行う事業継続のための対処態勢の整備の推進に係る施策を新たに実施する。

(5)　防護基盤の強化

第３次行動計画における本施策の期待される成果及び具体的な指標は次のとおりである。

[1] EU 諸国及び米国における情報共有体制に関する調査報告書
https://www.nisc.go.jp/inquiry/pdf/kyoyutaisei_gaiyou.pdf

[2] 2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価資料一式
https://www.nisc.go.jp/active/infra/files/riskhyoka.ZIP

＜期待される成果＞
・「広報公聴活動」については、行動計画の枠組みについて広く国民の理解を得ることと及び本行動計画への協力者の関係主体以外への拡大
・「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
・「規格・標準及び参照すべき規程類の整備」については、整備した規程類についての重要インフラ事業者等における利活用
＜具体的な指標＞
・ニュースレター等による情報の発信回数
・行動計画に関連した講演等の回数
・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３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ICT-ISAC設立（Telecom ISACの活動を移行）に当たっての一部放送事業者及びケーブルテレビ事業者の加盟、電力ISACの設立など、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。なお、第４次行動計画の決定に先駆け、内閣官房からの情報について、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開始した。

○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３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23回発行した。

また、重要インフラ防護に関する講演を18回実施し、第３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。

なお、第４次行動計画の策定に当たっては、重要インフラ専門調査会における重要インフラ分野に関わる各業界や情報セキュリティ関係機関を含めた有識者、重要インフラ所管省庁等との議論の過程をＮＩＳＣのWebサイトに公表するとともに、意見公募（2017年１月26日～２月16日）の手続きにより、一般からの意見を広く聴取した。

○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、2016年11月にメキシコで開催されたMeridian会合において、重要インフラ防護のための官民連携等の政策面でのベストプラクティスの共有や、国際連携方策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、2016年10月に日・ASEAN情報セキュリティ政策会議を開催し、「日・ASEANにおける重要インフラ防護に関するガイドライン」の改定とともに、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、同会議に合わせ、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。以上のほか、JICAやHIDAと連携し、ASEAN向けの重要インフラ防護に関する研修を３件実施した。

二国間では、「日米サイバー対話」をはじめとした政府間協議を実施したほか、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・意見交換等を行った。

○規格・標準及び参照すべき規程類の整備

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、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。

また、国際基準等を重要インフラ防護に適用する場合のガイドラインとして、「機能保証に向けたリスクアセスメント・ガイドライン」を作成、公表した。なお、その作成に当たり、国内外で策定されている重要インフラ防護に活用できるリスクマネジメント関係規格について、情報を収集するとともに、規格間の相違などを踏まえて規格を整理し、活用した。

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３次行動計画における各施策の取組詳細

第3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 本行動計画の初年度及び必要に応じた指針の改定に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表。	・ ・ 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４版）」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。
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、他施策との連携を強化した上で実施し、これらの結果を公表。	・ 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。 ・ 安全基準等の改善状況調査及び安全基準等の浸透状況等調査を通じて得た知見を用いて、行動計画の見直しに役立てた。
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。また、安全基準等に係る関係法令等について、重要インフラ所管省庁と認識合わせを行った。
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を状況把握するための調査を実施し、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（2016 年 12 月～2017 年３月）し、「2016 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 2017 年３月に公表した。
⑤ 重要インフラ所管省庁の協力を得つつ、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（2016 年７月～11 月）及び事業者等への往訪による調査（2016 年４月～12 月）を実施し、「2016 年度　重要インフラにおける『安全基準等の浸透状況等に関する調査』について」を 2017 年３月に公表した。
(2)「情報共有体制の強化」に関する施策	
① 平時及び大規模IT障害対応時の情報共有体制の運営を通じた更なる促進及び必要に応じた見直し。	・ 平時から大規模 IT 障害対応時への情報共有体制の切替えについて、第３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。（2016 年度　情報連絡 897 件、情報提供 80 件）
③ 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。	・ 重要インフラ所管省庁の協力を得て、2016 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を 2017 年３月に公表した。
④ 先進的なセプターの機能や活動の紹介。	・ セプターからの求めに応じ、先進的なセプターにおけるセプター機能の実装状況、組織化手法及び講演会等の意識啓発に関する取組状況等を紹介した。
⑤ セプターカウンシルに参加するセプターと連携しつつ、セプターカウンシルの運営及び活動に対する支援の実施。	・ セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会、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。（2016 年度のセプターカウンシル会合の回数は延べ 16 回）
⑥ 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。	・ 2016 年４月開催のセプターカウンシル総会において、セプターカウンシルの構成メンバーによる自律的な運営体制と、情報共有の活性化に向けた各種規程を改定した。各会合を自主的に開催するための準備作業や資料等の整理を行い、各担当者へノウハウの継承を図った。
⑦ 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。
(3)「障害対応体制の強化」に関する施策	
① 他省庁のIT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ＩＴ障害対応の演習・訓練情報を把握するとともに、当該情報を重要インフラ分野の分野委員が出席する検討会等の場において紹介した。また、各演習・訓練における目的や特徴を共有し、演習参加者にとって有益となるような演習運営を行った。
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。	・ 13 分野 18 セプター全てに対してセプター訓練を実施した。

③ 分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。	・ 重要インフラ全体の防護能力の維持・向上を図る観点から、「事業者等による障害対応能力の向上」「重要インフラ全体の対策水準の底上げ」「関係主体間の連携・維持の強化」「事業者等の自律的かつ継続的な取組について国が支援」との基本方針に基づき分野横断的演習を実施した。2016 年度は、505 組織、2,084 名が演習に参加した。
④ 分野横断的演習の改善策検討。	・ 多様な参加者に対して適合するようシナリオ整備を行った。また、CSIRT アクションも盛り込んだシナリオ内容とした。 ・ 重要インフラ全体の対策水準の底上げのために、多様な参加形態のモデルケースを提示（会場参加、自職場参加等）するとともに、中堅・中小規模の事業者等へも参加勧奨を実施した。 ・ 経営層に対する見学参加の呼びかけや、経営層向けの内容を含む講演を行った。
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IT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。	・ 演習事前説明会において、事前に検証課題を説明することにより、関係する規程の確認などを重要インフラ事業者等に実施してもらうことにより、演習への参加効果を高める取組を実施した。また、演習参加により抽出された課題等について、演習参加事業者内での改善に繋げる様に促した。 ・ 事後の意見交換会において、分野横断的に編成されたグループにおいてディスカッションを実施し、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った。
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。	・ 演習参加者のサブコン配置状況を集約した上で、参考となるようなサブコン配置事例を説明会で紹介することで、サブコン活用による演習効果向上を図った。
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。	・ 分野横断的演習の成果を、演習に参加できない者に対しても広く浸透させ、重要インフラ全体の防護能力の維持・向上に資するべく、成果展開用資料を作成した。また、演習事前説明会や講演等を通じて、普及啓発用動画の紹介を行った。
(4)「リスクマネジメント」に関する施策	
① リスクマネジメントの標準的な考え方や定義等の利活用や国際標準等を読み替えた手引書等の提示による関係主体間の共通認識の醸成。	・ 個々の重要インフラ事業者等のリスクマネジメントにおいて利活用できる手引書等の整備について、2020 年東京オリンピック・パラリンピック競技大会をテストケースと定め、関連事業者等が行うリスクアセスメントのガイドラインとして、「機能保証のリスクアセスメント・ガイドライン」を整備し、公表した。さらに、大会に係る重要サービスを提供する事業者等によるリスクアセスメントを、当該ガイドラインに基づいて実施し、その結果報告等から更なる改善に向けた課題を抽出した。
② 本施策における調査・分析による重要インフラ事業者等におけるリスクマネジメントの支援。	・ 第３次行動計画に記載されている環境変化調査の関連調査として、EU 諸国及び米国における情報共有体制に関する調査を行い、その調査結果を重要インフラ事業者等に対して公表した。これは、EU 諸国及び米国における情報共有体制の状況及びその背景にある法制度等を含む環境の変化について把握し、情報共有体制の強化に係る施策に活用するとともに、各重要インフラ事業者等が実施するリスクアセスメントの参考情報として利活用できるようにしたものである。
③ 本施策における調査・分析の結果を安全基準等に反映する基礎資料として提供。	・ 環境変化調査の一部として、EU 諸国及び米国における情報共有体制の状況及びその背景にある法制度等を含む環境の変化について把握する目的で「EU 諸国及び米国における情報共有体制に関する調査」を行い、第４次行動計画における情報共有体制の強化に係る施策を検討する際の基礎資料として提供した。
④ 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を支援。	・ 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。また、2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの参加事業者等を対象に、説明会、意見交換会等を開催し、大会に係るリスクコミュニケーション及び協議を支援した。
(5)「防護基盤の強化」に関する施策	
① Web サイトやニュースレター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。
② 講演等を通じた公聴活動を実施。	・ 第３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３次行動計画やその施策等について計 18 回講演を行った。
③ 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 情報セキュリティ政策会議や 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。

④ 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。	・ EU 諸国及び米国における情報共有体制等に関する調査を実施し、調査報告書を 2017 年３月に公表した。
⑤ 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。
⑥ 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。
⑦ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、必要に応じて、手引書等を整備。	・ 個々の重要インフラ事業者等のリスクマネジメントにおいて利活用できる手引書等の整備について、オリパラ大会をテストケースと定め、関連事業者等が行うリスクアセスメントのガイドラインとして、「機能保証に向けたリスクアセスメント・ガイドライン」を整備し、2017 年１月に公表した。
⑧ 制御系機器・システムの第三者認証制度の拡充を支援。	・ 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	
(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、日本電気技術規格委員会が策定した「スマートメータシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」を、法体系（電気設備に関する技術基準を定める省令及び保安規程）に位置づけた。
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。	・ 国土交通省については、対策項目をＰＤＣＡサイクルに沿って再構成するとともに、各事業者の対策状況や課題を反映させた形でガイドラインの改定を実施した。 ・ 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、現行のガイドラインの改定作業を実施した。 ・ 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。	・ 経済産業省において、日本電気技術規格委員会が策定した「スマートメータシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」を、法体系（電気設備に関する技術基準を定める省令及び保安規程）に位置づけた。
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を実施。	・ 経済産業省において、日本電気技術規格委員会が策定した「スマートメータシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」を、法体系（電気設備に関する技術基準を定める省令及び保安規程）に位置づけた。
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 内閣官房と連携しつつ、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。	・ 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、平成 28 年６月に「国土交通省 IT 政策検討会」で取りまとめた報告書において、「システムやリスク管理等の情報共有、未確認情報等の相談といった現場レベルでの機動的な情報共有体制を早急に構築するため、「ISAC」の創設を目指す」と述べるとともに、所管する重要インフラ事業者に対し、平成 29 年度から実施する ISAC 創設に向けた検討会への参加に係る説明会を行った。

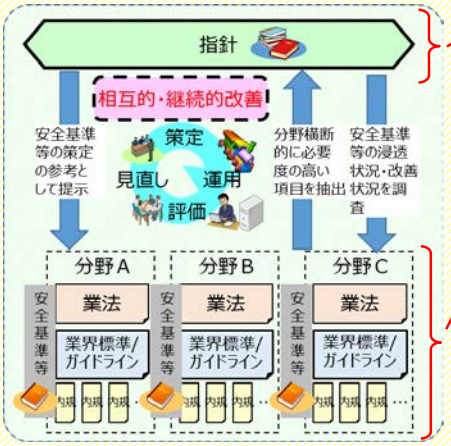
③ 重要インフラ事業者等からのIT障害に係る報告の内閣官房への情報連絡。	・ 重要インフラ所管省庁において、重要インフラ事業者等からのＩＴ障害等に係る報告があった際に、事案の大小や重要インフラサービスの事案であるか否かに関わらず、速やかに内閣官房へ情報連絡を行った。
④ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。	・ 重要インフラ所管省庁において、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤ セプターの機能充実への支援。	・ 重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要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運営委員会にオブザーバーとして出席した。
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運営委員会にオブザーバーとして出席した。
(3)「障害対応体制の強化」に関する施策	
① 内閣官房が情報疎通機能の確認（セプター訓練）等の機会を提供する場合の協力。	・ 重要インフラ所管省庁を通じた情報共有体制の確認として、2016 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、2016 年度分野横断的演習検討会、作業部会等にオブザーバーとして出席し、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担当職員などが、2016 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 2016 年度分野横断的演習への参加を促し、全体で 505 組織 2,084 名の過去最大の参加者を得た。
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、2016 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、事後の検討会及び作業部会等にオブザーバーとして出席した。
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、分野横断的演習の成果により、重要インフラ所管省庁と重要インフラ事業者等及びセプターとの間の情報共有体制が、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）を実施した。 ・
(4)「リスクマネジメント」に関する施策	
① 本施策における調査・分析を必要とする対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供。	・ 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。
② 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。
③ 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を支援。	・ 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。
(5)「防護基盤の強化」に関する施策	
① 内閣官房と連携して、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 内閣官房と連携して、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 内閣官房と協力し、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。
④ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備。	・ 重要インフラ所管省庁において、内閣官房が策定するリスクマネジメントに関する手引書の作成のため、協力先となる個別の重要インフラ事業者等の紹介などの協力を行った。
⑤ 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援。	・ 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行った。
3. 情報セキュリティ関係省庁の施策	
(1)「情報共有体制の強化」に関する施策	
① 内閣官房と連携しつつ、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運営委員会にオブザーバーとして出席した。
4. 事案対処省庁の施策	
(1)「情報共有体制の強化」に関する施策	
① 内閣官房と連携しつつ、大規模IT障害対応時における情報共有体制の運用。	・ 2016 年度において大規模ＩＴ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。 ・ 警察庁において、インターネット・オシントセンターを設置し、インターネット上に公開されたテロ等関連情報の収集・分析を強化した。
③ 内閣官房に対して、必要に応じ情報連絡の実施。	・ 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、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、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 重要インフラ事業者等からの要望があった場合、IT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、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、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。

別添４－３　安全基準等の継続的改善状況等の把握及び検証

調査の目的

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



<指針>
「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針」の略称

<安全基準等とは>
以下の総称
- 業法に基づき国が定める「強制基準」
- 業法に準じて国が定める「推奨基準」及び「ガイドライン」
- 業法や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
- 業法や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

＊指針は含まない

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

調査対象一覧

分野		安全基準等名称
情報通信	電気通信	情報通信ネットワーク安全・信頼性基準 電気通信分野における情報セキュリティ確保に係る安全基準（第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	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）
	航空管制	航空管制システム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		電力制御システム等における技術的水準・運用技術に関するガイドライン 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 スマートメータシステムセキュリティガイドライン 電力制御システムセキュリティガイドライン
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4.2版)
水道		水道分野における情報セキュリティガイドライン
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン(第３版)
化学		石油化学分野における情報セキュリティ確保に係る安全基準
クレジット		クレジットCEPTOARにおける情報セキュリティガイドライン
石油		石油分野における情報セキュリティ確保に係る安全ガイドライン

調査対象数：24件

安全基準等の継続的改善状況（概要）

○安全基準等の継続的改善における2016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：９件　　分析・検証後、改定を実施中：３件　　分析・検証を実施中：６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６件）

○分析・検証を行うに至った主な契機は以下のとおり。
・指針が改定されたため（平成27年５月25日 サイバーセキュリティ戦略本部 決定）
・「重要インフラの情報セキュリティ対策に第３次行動計画の見直しに向けたロードマップについて」（平成28年３月31日 サイバーセキュリティ戦略本部 決定）に基づく2016年度の検討状況を踏まえて
・定期的に検証することとしている

○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。
「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。」（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より）
【指針改善の方向性】
サイバー攻撃の高度化等により重要インフラで不測の事態が発生する可能性は一層高まっていることから、経営層や職員等が行うべき初動対応(緊急時対応)の方針、手順、態勢等を定めた「コンティンジェンシープラン」の必要性に関して指針に記載する。

【考察】
下記の考察結果より、ＰＤＣＡサイクルを踏まえた安全基準等の継続的改善が着実に進んだ１年であったと考えられる。
・多くの重要インフラ分野で分析・検証が行われていることから、安全基準等の継続的な改善を目的とする分析・検証の推進体制が確立され、着実に機能していると認められる。
・改定が行われた分野(年度内予定含む)は、昨年度の２分野から10分野に拡大しており、重要インフラ防護能力の維持・向上へと繋がったと認められる。
・電力分野では、サイバーセキュリティ確保に関する強制基準を盛り込んだ法令改正が行われ、また、これに合わせて既存の安全基準等の見直しや新たな安全基準等が整備されるなど、重要インフラ分野における先導的な取組が確認できた。
・安全基準等の見直し過程における重要インフラ事業者に対する意見照会や、改定後に全国規模の説明会を実施するなど、重要インフラ事業者の実状を考慮した安全基準等の改定等に努めている分野が確認できた。

安全基準等の継続的改善状況（詳細 1/12）

分野		情報通信（電気通信）	情報通信（電気通信）
名称		情報通信ネットワーク安全･信頼性基準	電気通信分野における情報セキュリティ確保に係る安全基準（第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	2016年度実施予定なし （理由：2015年度に分析・検証実施済）
	分析検証の実施契機	・定期的に実施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）2016年4月～2017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。	－
改定状況	改定の実施状況	－	2016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5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）安全基準検討ワーキンググループで改定案を作成し、安全・信頼性協議会で承認
	改定内容	－	「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」の改定に伴い、PDCAサイクルの考え方（持続的な改善）、経営層のあり方（自主的な取組み）等を盛り込んだ。

安全基準等の継続的改善状況（詳細 2/12）

分野		情報通信（電気通信）	情報通信（放送）
名称		事業用電気通信設備規則 ※電気通信事業法、電気通信事業法施行規則は改定なし	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
発行主体等		総務省	放送セプター（日本放送協会（NHK）、一般社団法人日本民間放送連盟）
最新改定／新規作成年月		2015年11月27日	2016年10月
分析・検証状況	分析検証の実施状況	実施中	2016年度実施予定なし （理由：2015年度実施済み。放送セプターコアメンバーにて以前より改定の必要性を議論していたが、指針の改定を受けて改定作業に入ることを決定。）
	分析検証の実施契機	・その他状況の変化等 （具体的に：2025年頃までに固定電話網が公衆交換電話網（PSTN）からIP網に移行する見込みとなったため。また、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）2016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及び同技術検討作業班） （３）2017年７月頃に一部答申を予定	－
改定状況	改定の実施状況	－	2016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）2015年7月～2016年9月 （２）放送セプターコアメンバー（NHK担当者、民放連・総務委員会・情報セキュリティ対策WG委員） （３）放送セプターコアメンバーで改定案を作成し、NHKおよび民放連・総務委員会で承認を得て、10月に改定。
	改定内容	－	旧ガイドラインを、直近の指針に従いPDCAサイクルに沿った構成に改めるとともに、最近のサイバー攻撃の動向と放送事業者の現状を踏まえて、大幅に改定した。

安全基準等の継続的改善状況（詳細 3/12）

分野		情報通信（ケーブル）	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	2016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）2016年4月～2017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 4/12）

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		2016年３月	2013年３月
分析・検証状況	分析検証の実施状況	実施中	2016年度に実施済
	分析検証の実施契機	・安全基準等策定指針の改定 ・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）2016年7月～2017年４月（予定） （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）公益財団法人金融情報システムセンターにて、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」及び現在開催中の「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、監査安全部で「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」の改訂原案を検討中。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改訂原案を検討中。また今後、「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」に関する改訂について、分析・検証を行う予定。それら検討結果について、公益財団法人金融情報システムセンター（FISC）監査安全部が事務局となる「安全対策専門委員会」に報告し、改訂を行うことが正式決定となる予定。（2016年５月より、公益財団法人金融情報システムセンター（FISC）監査安全部が事務局となる「安全対策専門委員会」およびその下部組織である「安全対策基準改訂に関する検討部会」にて、改訂の検討を行う予定）	（１）2016年１月～2016年８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て、「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について監査安全部で検討を実施。その結果を監査安全部が事務局となる「安全対策専門委員会」に報告し、改訂を行うことを正式決定。
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）2016年９月～2017年３月（予定） （２）公益財団法人　金融情報システムセンター（FISC）監査安全部が事務局となる「安全対策専門委員会」（以下、「専門委員会」）及びその下部組織である「コンティンジェンシープラン改訂に関する検討部会」（以下、「検討部会」） （３）サイバー攻撃動向等を踏まえて、「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について「検討部会」で検討を実施（合計３回開催）。現在FISC会員から意見を募集中であり、今後、会員意見の反映を「検討部会」にて検討、上位組織の「専門委員会」で改訂について正式決定の予定。
	改定内容	－	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 5/12）

分野		航空（航空運送）	航空（航空管制）
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）	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン（第４版）
発行主体等		国土交通省	国土交通省
最新改定／新規作成年月		2016年4月	2016年4月
分析・検証状況	分析検証の実施状況	実施中	2016年度実施予定なし （理由：2016年４月１日に改定されたところであり、その後、大きな環境変化がないため）
	分析検証の実施契機	・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4月～2017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、2016年4月1日付けで改訂したばかりであることから、重要インフラの情報セキュリティ対策に係る第３次行動計画の見直し～第４次行動計画案策定の動向を注視しつつ、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の指針の改訂を踏まえた改定について、その必要性を含めて検討中である。	－
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 6/12）

分野		鉄道	電力
名称		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）	電力制御システム等における技術的水準・運用技術に関するガイドライン
発行主体等		国土交通省	電気事業連合会
最新改定／新規作成年月		2016年4月	2016年８月
分析・検証状況	分析検証の実施状況	実施中	2016年度に実施済
	分析検証の実施契機	・安全基準等策定指針の改定	・定期的に検証することとしている ・その他状況の変化等 （具体的に：「制御システムセキュリティガイドライン」、「スマートメーターシステムセキュリティガイドライン」が策定されたことにより、実施。）
	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4月～2017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、2016年4月1日付けで改訂したばかりであることから、重要インフラの情報セキュリティ対策に係る第３次行動計画の見直し～第４次行動計画案策定の動向を注視しつつ、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の指針の改訂を踏まえた改定について、その必要性を含めて検討中である。	（１）2016年４月　～　2016年５月 （２）電気事業連合会 （３）「制御システムセキュリティガイドライン」、「スマートメーターシステムセキュリティガイドライン」が策定されたことにより、本ガイドラインを改定することが決定した。
改定状況	改定の実施状況	－	2016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６月　～　2016年８月 （２）電気事業連合会 （３）電事連会員企業に意見照会を実施し意見を取りまとめた後，８月下旬に決裁を行い，各社へ通知した。
	改定内容	－	「制御システムセキュリティガイドライン」、「スマートメーターシステムセキュリティガイドライン」の民間規格が策定されたことから，サイバー攻撃に対する技術的水準・運用基準についての記載を削除した。

安全基準等の継続的改善状況（詳細 7/12）

分野		電力	電力
名称		電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
発行主体等		経済産業省	経済産業省
最新改定／新規作成年月		2016年９月	2016年９月
分析・検証状況	分析検証の実施状況	2016年度実施予定なし （理由：2015年以前に分析・検証実施済）	2016年度実施予定なし （理由：2015年以前に分析・検証実施済）
	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	2016年度に実施済	2016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９月 （２）経済産業省 （３）2016年７月、産業構造審議会保安分科会電力安全小委員会（第１３回）に改正方針を報告し、パブリックコメントを実施後、改定を行った。	（１）2016年９月 （２）経済産業省 （３）2016年７月、産業構造審議会保安分科会電力安全小委員会（第１３回）に改定方針を報告し、パブリックコメントを実施後、改定を行った。
	改定内容	事業者に適合維持を義務付けている電気設備に関する技術基準を定める省令に、サイバーセキュリティの確保を規定。省令に定める技術的要件に適合する具体的な内容を例示した「電気設備の技術基準の解釈」で、「サイバーセキュリティの確保は、日本電気技術規格委員会規格である『スマートメーターシステムセキュリティガイドライン』、『電力制御システムセキュリティガイドライン』によること」とした。	自主保安活動を行う上での基本的なルールとして、事業者自らが定める保安規程に、日本電気技術規格委員会規格「スマートメーターシステムセキュリティガイドライン」、「電力制御システムセキュリティガイドライン」によるサイバーセキュリティ対策に関する事項を記載し、国へ届出ることを規定した。

安全基準等の継続的改善状況（詳細 8/12）

分野		電力	電力
名称		スマートメーターシステムセキュリティガイドライン	電力制御システムセキュリティガイドライン
発行主体等		一般社団法人日本電気協会	一般社団法人日本電気協会
最新改定／新規作成年月		2016年３月	2016年５月
分析・検証状況	分析検証の実施状況	2016年度実施予定なし （理由：本ガイドラインは昨年度末に策定されたところであり、環境変化がないため。）	2016年度実施予定なし （理由：本ガイドラインは今年度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 9/12）

分野		ガス	政府・行政サービス
名称		製造・供給に係る制御系システムのセキュリティ対策ガイドライン	地方公共団体における情報セキュリティポリシーに関するガイドライン
発行主体等		一般社団法人　日本ガス協会	総務省自治行政局地域情報政策室
最新改定／新規作成年月		2016年７月	2015年3月
分析・検証状況	分析検証の実施状況	2016年度に実施済	2016年度中に実施予定
	分析検証の実施契機	・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	・サイバー攻撃動向を受けて ・その他状況の変化等 （具体的に：2016年の政府統一基準群の改訂や、年金機構の個人情報流出事案を踏まえた2015年度補正予算による自治体の情報セキュリティ対策の抜本的強化の実施等。）
	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）2015年11月～2016年４月 （２）日本ガス協会　　システムセキュリティWG （３）直近の指針改定や所管省庁による事業者調査結果を受け、安全基準等の改定要否を分析・検証し、改定を実施することとした。	（１）2017年１月～３月 （２）総務省自治行政局地域情報政策室 （３）政府統一基準群の改訂による「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改正点の洗い出し等
改定状況	改定の実施状況	2016年度に実施済	2017年度以降に実施予定 （理由：当初から2016年度は調査を行い、その翌年度に改正を行う予定だったため。）
	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４月～2016年７月 （２）日本ガス協会　　システムセキュリティWG （３）WGメンバーで改定案の検討を行い、７月に改訂版を発行した。会員事業者２０３者に通知すると共に、９月から１０月にかけて全国８会場で改訂版に関する説明会を開催し、業界内における安全基準の浸透を図った。	－
	改定内容	直近の指針改定や所管省庁による事業者調査結果を踏まえて、観点・構成の見直しを行った。	－

安全基準等の継続的改善状況（詳細 10/12）

分野		医療	水道
名称		医療情報システムの安全管理に関するガイドライン（第４．３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	厚生労働省健康局水道課
最新改定／新規作成年月		2016年3月	2013年6月
分析・検証状況	分析検証の実施状況	実施中	2016年度実施予定なし （理由：安全基準等指針の改定を受け、2017年度に実施する予定になっているため）
	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5月～2017年3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置かれる作業班） （３）現状調査等の結果を踏まえ、上記作業班において改定案を策定し、上記検討会の場で改定案の承認を図る。	－
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 11/12）

分野		物流	化学
名称		物流分野における情報セキュリティ確保に係る安全ガイドライン（第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	2015年3月（新規作成）
分析・検証状況	分析検証の実施状況	実施中	2016年度実施予定なし （理由：2015年度に分析・検証実施済）
	分析検証の実施契機	・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4月～2017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（１６社６団体） （３）当該ガイドラインについては、2016年4月1日付けで改訂したばかりであることから、重要インフラの情報セキュリティ対策に係る第３次行動計画の見直し～第４次行動計画案策定の動向を注視しつつ、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の指針の改訂を踏まえた改定について、その必要性を含めて検討中である。	－
改定状況	改定の実施状況	－	実施不要と判断 （理由：指針改定、情報セキュリティ対策の運用を通じた課題抽出を受け分析・検証の結果、改定が必要な箇所は特に無かった）
	改定プロセス （１）実施時期 （２）実施主体 （３）実施の流れ	－	－
	改定内容	－	－

安全基準等の継続的改善状況（詳細 12/12）

分野		クレジット	石油
名称		クレジットCEPTOARにおける情報セキュリティガイドライン	石油分野における情報セキュリティ確保に係る安全ガイドライン
発行主体等		一般社団法人日本クレジット協会	石油連盟
最新改定／新規作成年月		2014年12月（新規策定）	2016年３月24日
分析・検証状況	分析検証の実施状況	2016年度に実施済	実施中
	分析検証の実施契機	その他状況の変化等 （具体的に：構成員の拡大（本年度から中小カード会社にも対象範囲を拡大し、今後も順次拡大する予定））	・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）2016年9月から12月 （２）日本クレジット協会クレジットCEPTOAR運営会議 （３）上記会議で協議	（１）現在分析・検証を実施中（改訂時期については未定） （２）石油連盟　ITセキュリティ連絡会 （３）指針改訂内容を分析・検証の上、安全基準の改訂が必要と判断されれば改訂作業を実施
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）2016年9月から2017年１月 （２）日本クレジット協会クレジットCEPTOAR運営会議 （３）上記会議において改定予定	―
	改定内容	・対象サービスを「クレジットカード決済サービス」とし、これにあわせて防護すべき重要システム、サービス維持レベル、対象となる重要インフラ事業者について改定 ・環境整備について、主な着眼点を追記 ・障害発生時の対応及び所管省庁等への報告を追記	―

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、2016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）

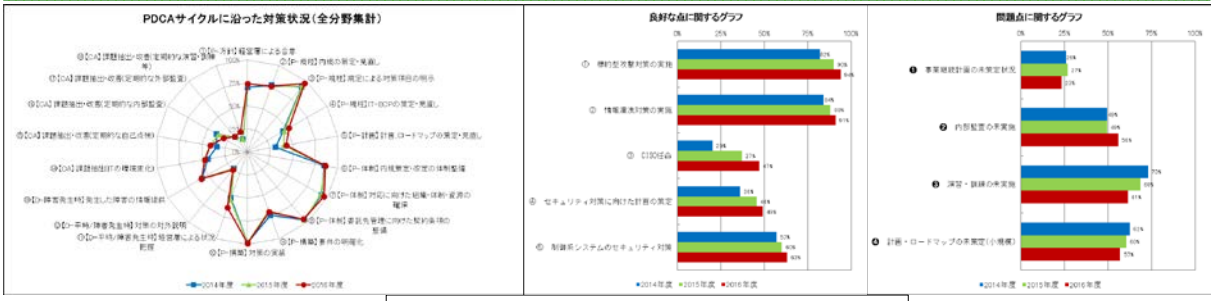
調査結果の要約

(1) 良好な点

- 社会問題となっている標的型攻撃、情報漏えい等のリスクへの関心が高く、対策も進んでいる様子がうかがえる。(下中図①,②)
- 経営層の関与が高まるとともに、計画的に情報セキュリティ対策に取り組む事業者の数が増加している。(下中図③,④)
※往訪調査（参考）でも同様の意見あり
- 情報系システムだけでなく、制御系システムに対するセキュリティ対策の意識が高まっている。(下中図⑤)

(2) 問題点

- 事業継続計画の必要性や、課題抽出における演習・訓練や監査の有効性に関し、事業者の理解を促進する必要がある。(下右図❶,❷,❸)
※往訪調査（参考）でも同様の意見あり
- 小規模な事業者(概ね100名以下)の多くが、情報セキュリティ対策の推進に係る内規や計画・ロードマップを策定していない。(下右図❹)
- サイバーセキュリティ戦略等でCSIRT設置の必要性が指摘されているが、設置している事業者は20%程度に留まっている。(2016年度から調査)



アンケート配布は3,302事業者等。回答は3,144事業者等。

(3) 今後の対応

- 事業継続計画の必要性や演習・訓練及び監査の有効性等について、事業者の理解を促進する（指針の改定等）。
- 事業者への往訪調査等を通じて、CSIRT設置の詳細状況の把握や、小規模事業者の課題に関する原因分析を進める。
- 指針や安全基準等に関する意見を踏まえ、指針の改定を実施する。また、調査票の見直しを行うことにより、アンケート回答の負担を軽減しつつ、情報セキュリティ対策の取組状況を詳細に、かつ効率的に確認し、重要インフラ防護施策への更なる活用を図る。

◆調査内容
①安全基準等の整備・浸透に係る事項：指針※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

◆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、2016年3月末日
調査方法②の場合、各調査で設定した基準日

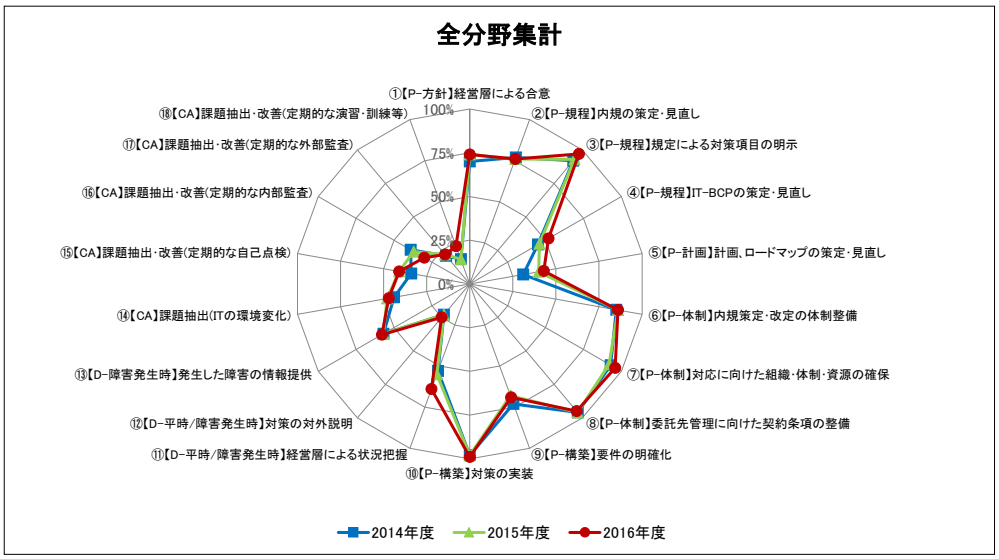
各重要インフラ分野の調査状況

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	電気通信事業者（一部抽出）	85	69	NISC調査
	ケーブルテレビ	一般社団法人日本ケーブルテレビ連盟加盟事業者のうち一定要件を満たすケーブルテレビ事業者	334	294	
	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）、一般社団法人日本民間放送連盟	194	191	
金融		銀行等、証券会社、生命保険会社、損害保険会社	650	566	独自調査(*1)
航空	航空運送	航空運送事業者	2	2	NISC調査
	航空管制	官庁	2	2	
鉄道		ＪＲ、大手民鉄	22	22	
電力		一般電気事業者、日本原電(株)、電源開発(株)	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)
医療		病院情報システムを導入する病院	60	45	NISC調査
水道		給水人口30万人以上の水道事業者、水道用水供給事業者	87	87	
物流		物流事業者、業界団体（一部抽出）	16	16	
化学		石油化学事業者	13	13	
クレジット		クレジットカード会社等	18	18	
石油		石油精製・元売事業者	9	9	
全分野合計		－－－	**3,302**	**3,144**	－－－

＊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：2016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：2015年4月1日）

調査結果概要 - ＰＤＣＡサイクルに沿った対策状況（1/2）-

(1) 全分野の重要インフラ事業者

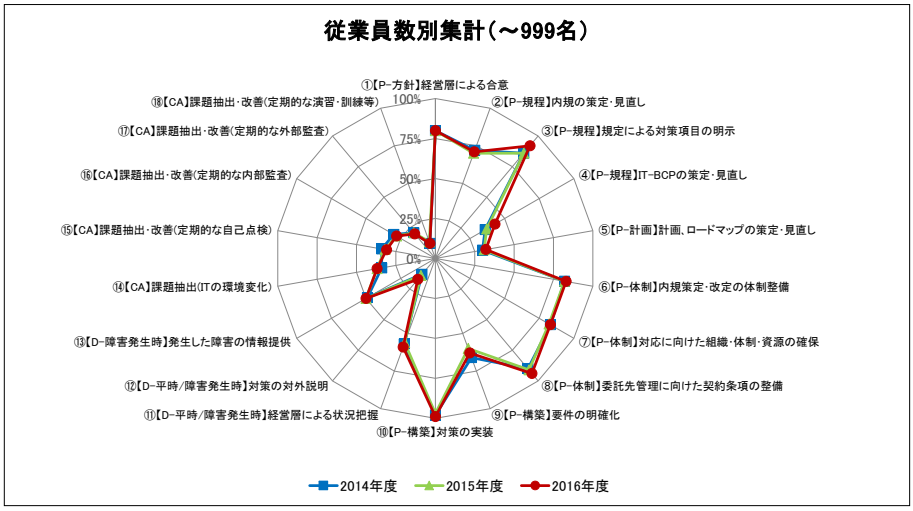


項目	2014年度	2015年度	2016年度
①	70%	74%	74%
②	77%	76%	76%
③	92%	93%	97%
④	45%	46%	52%
⑤	31%	40%	43%
⑥	85%	86%	86%
⑦	93%	92%	96%
⑧	96%	96%	95%
⑨	73%	68%	69%
⑩	98%	98%	99%
⑪	53%	55%	64%
⑫	23%	23%	25%
⑬	57%	57%	58%
⑭	44%	48%	47%
⑮	34%	41%	41%
⑯	39%	37%	30%
⑰	21%	22%	22%
⑱	15%	15%	23%

※ ①、③、⑫については、政府・行政サービス分野における独自調査結果の読替を実施している。

調査結果概要 - ＰＤＣＡサイクルに沿った対策状況（2/2）-

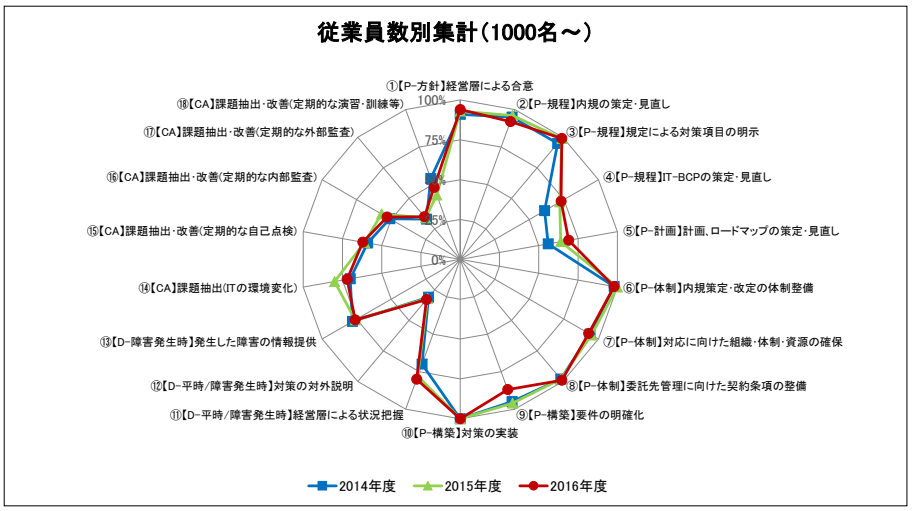
(2) 従業員1000名未満の重要インフラ事業者



項目	2014年度	2015年度	2016年度
①	80%	80%	80%
②	72%	70%	71%
③	86%	86%	92%
④	36%	37%	43%
⑤	30%	31%	32%
⑥	82%	82%	83%
⑦	83%	82%	83%
⑧	90%	91%	94%
⑨	66%	60%	63%
⑩	98%	97%	99%
⑪	57%	56%	59%
⑫	13%	14%	17%
⑬	49%	50%	50%
⑭	34%	37%	37%
⑮	34%	32%	31%
⑯	30%	28%	28%
⑰	21%	21%	20%
⑱	10%	11%	10%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

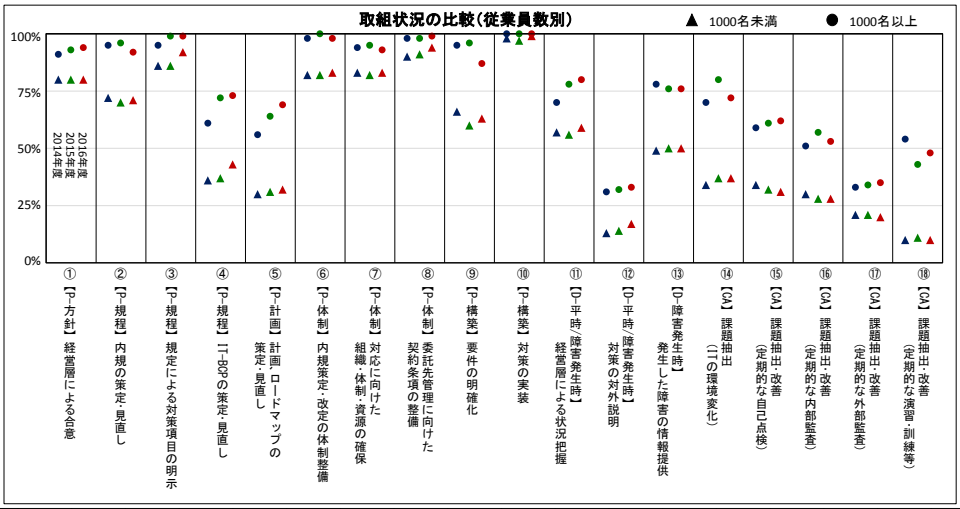
(3) 従業員1000名以上の重要インフラ事業者



項目	2014年度	2015年度	2016年度
①	91%	93%	94%
②	95%	96%	92%
③	95%	99%	99%
④	61%	72%	73%
⑤	56%	64%	69%
⑥	98%	100%	98%
⑦	94%	95%	93%
⑧	98%	98%	99%
⑨	95%	96%	87%
⑩	100%	100%	100%
⑪	70%	78%	80%
⑫	31%	32%	33%
⑬	78%	76%	76%
⑭	70%	80%	72%
⑮	59%	61%	62%
⑯	51%	57%	53%
⑰	33%	34%	35%
⑱	54%	43%	48%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

(4) 従業員1000名未満と1000名以上の重要インフラ事業者の対策状況の比較



	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪		⑫		⑬		⑭		⑮		⑯		⑰		⑱	
	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●	▲	●
2014年度	80%	91%	72%	95%	86%	95%	36%	61%	30%	56%	82%	98%	83%	94%	90%	98%	66%	95%	98%	100%	57%	70%	13%	31%	49%	78%	34%	70%	34%	59%	30%	51%	21%	33%	10%	54%
2015年度	80%	93%	70%	96%	86%	99%	37%	72%	31%	64%	82%	100%	82%	95%	91%	98%	60%	96%	97%	100%	56%	78%	14%	32%	50%	76%	37%	80%	32%	61%	28%	57%	21%	34%	11%	43%
2016年度	80%	94%	71%	92%	92%	99%	43%	73%	32%	69%	83%	98%	83%	93%	94%	99%	63%	87%	99%	100%	59%	80%	17%	33%	50%	76%	37%	72%	31%	62%	28%	53%	20%	35%	10%	48%

※従業員数が不明な回答（独自調査を読み替える金融、政府・行政サービス分等）は、集計していません。

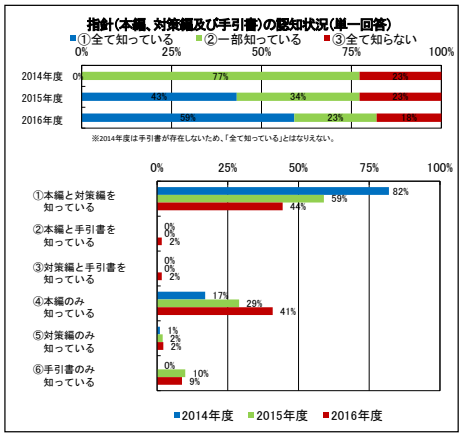
調査結果詳細（1/6）

(1) 安全基準等の整備状況

① 指針の認知

(a) 指針（本編、対策編及び手引書）の認知状況

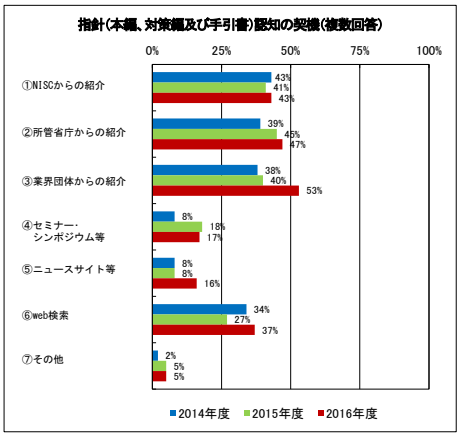
・指針本編、対策編、手引書の全てを知っている事業者は着実に増えてきていると認められる。
・2割弱の事業者は指針を全く知らないため、引き続き認知度向上に向けた取組を行う必要がある。



※金融、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）
※2015年度に手引書を新たに作成したことに伴い、集計方法を変更

(b) 指針（本編、対策編及び手引書）認知の契機

・業界団体からの紹介が増えていることから、情報セキュリティ対策の水準の向上、サイバー攻撃への対応能力の向上に必要不可欠である、各業界の情報共有が進んでいることが認められる。

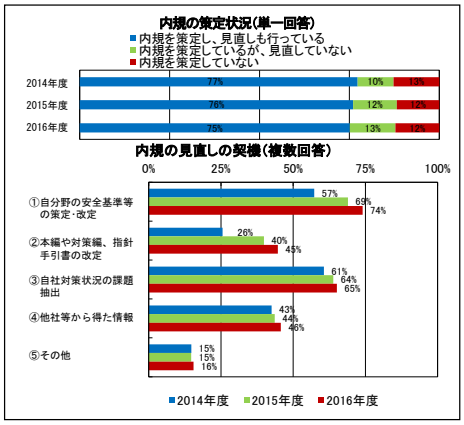


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

② 内規の策定・見直し

(a) 内規策定・見直しの契機

・内規を策定していない事業者の約80%は100名未満の規模であり、今後も継続してアプローチする必要がある。
・安全基準等や指針の改定に合わせて内規を見直すといった、見直しの機会が着実に増えていることが認められる。

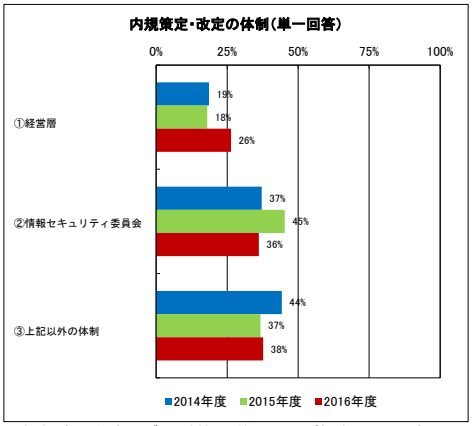


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

③ 内規改定のプロセス

(a) 内規策定・改定の体制

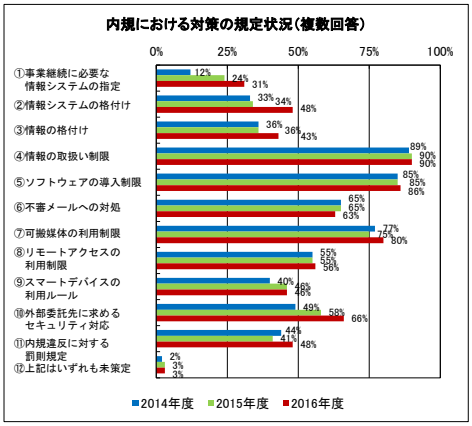
・情報セキュリティ対策には経営層の関与が必要不可欠であるが、内規の策定・改定の体制に「経営層にて実施」の回答が増えていることから、経営層の意識が醸成されつつあると認められる。



※金融、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）

(b) 内規における対策の規定状況

・直近数年間で委託先に起因するセキュリティインシデントが増えていること等を背景として、委託先に求めるセキュリティ対応が伸びたと推察される。



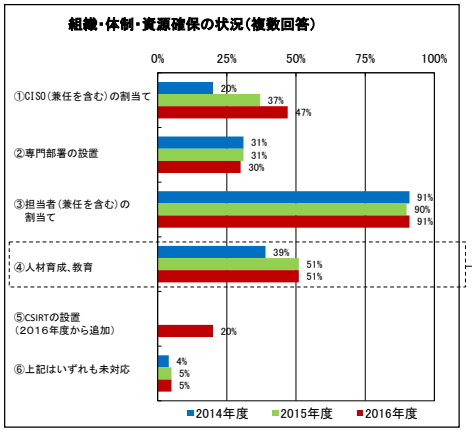
調査結果詳細（2/6）

(2) 情報セキュリティ対策の実施状況

① 体制・資源の確保

(a) 組織・体制・資源確保の状況

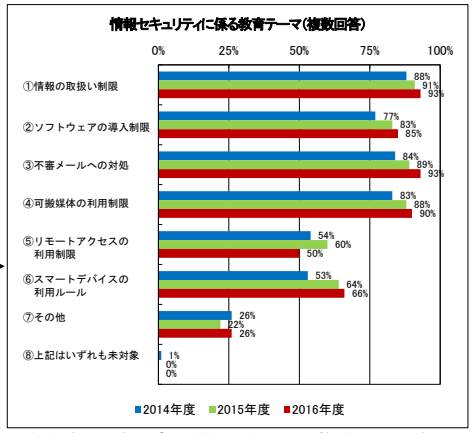
・CISOの割り当てが伸びていることから、情報セキュリティ対策に対する経営層の関与が増えたと認められる。
・CSIRTに関する一般の認知度は高まっているものの、設置している割合は多くない。



※金融は読替え可能項目なし（集計していません）

(b) 情報セキュリティに係る教育テーマ

・標的型攻撃メールの増加に伴い、不審メールに対する教育テーマが増えたと推察される。

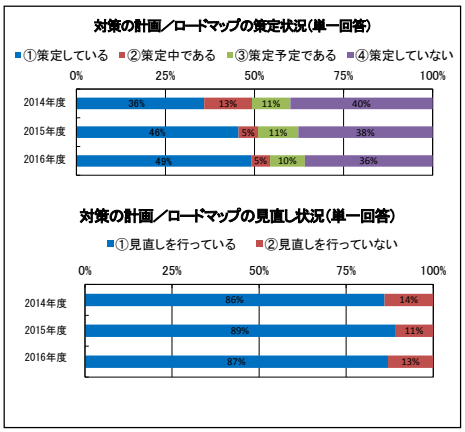


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

② 情報に係る対策

(a) 対策の計画／ロードマップの策定・見直し状況

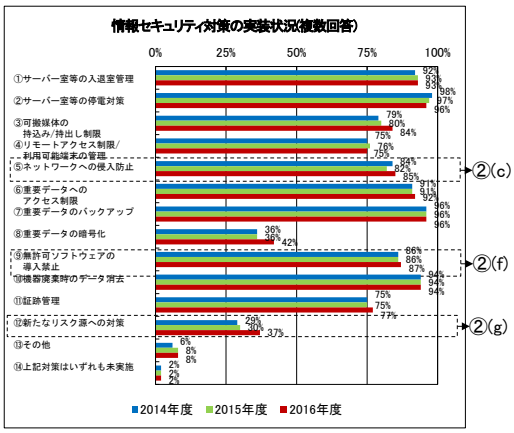
・セキュリティ対策を計画的に実施する事業者が増えている。
・100名未満の事業者においては、計画/ロードマップの策定が行われおらず、原因分析が求められる。



※金融、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）

(b) 情報セキュリティ対策の実装状況

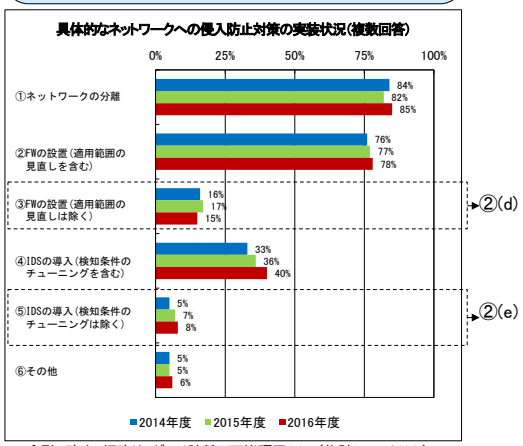
・近年ランサムウェアによる被害が増えていることから、新たなリスク源への対策が増えていると推察される。



※金融、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）

(c) 具体的なネットワークへの侵入防止対策の実装状況

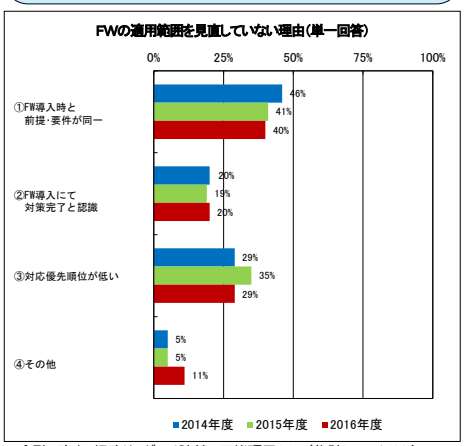
・FWやIDSの導入効果を維持・向上させるには、定期的な見直し作業が必要不可欠であるという点について、指針等で啓発していく必要がある。



※金融、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）
※前設問(2)②(b)選択肢⑤選択事業者のみの回答

(d) FWの適用範囲を見直していない理由

・FWの導入効果の維持・向上には、見直し作業が必要不可欠であること、また、その重要性・効果が組織内で理解され、取組につながるよう啓発していく必要がある。



※金融、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）
※前設問(2)②(c)選択肢③選択事業者のみの回答

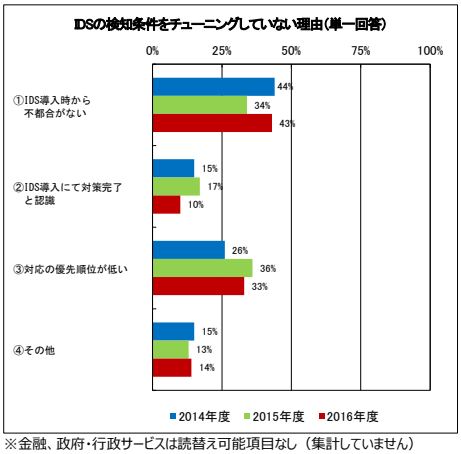
調査結果詳細（3/6）

(2) 情報セキュリティ対策の実施状況（続き）

② 情報に係る対策（続き）

(e) IDSの検知条件をチューニングしていない理由

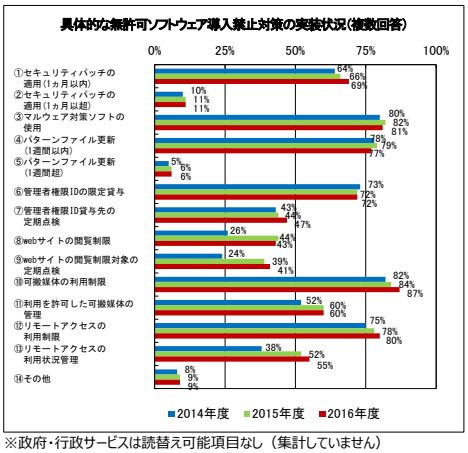
・IDSの導入効果の維持・向上には、見直し作業が必要不可欠であること、また、その重要性・効果が組織内で理解され、取組につながるよう啓発していく必要がある。



※金融、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）
※前設問(2)②(c)選択肢⑤選択事業者のみの回答

(f) PCにおける情報セキュリティ対策の実装状況

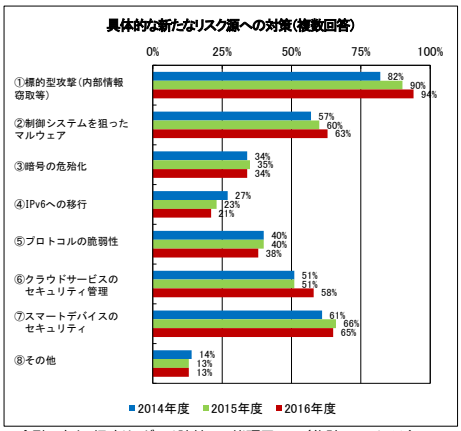
・可搬媒体の利用制限が伸びているが、昨今のスマートフォン等を利用した情報漏えい事例に対する対策のためと認められる。



※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）
※前設問(2)②(b)選択肢⑨選択事業者のみの回答

(g) 具体的な新たなリスク源への対策

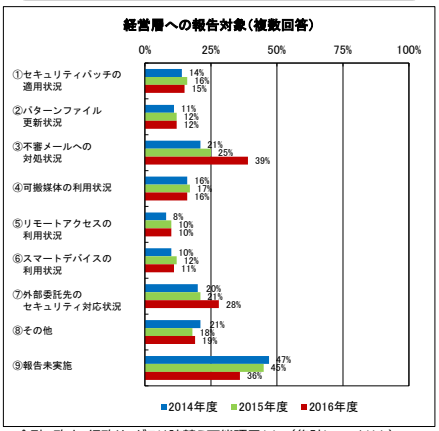
・標的型攻撃の脅威が依然として高まっていることから標的型攻撃の対策が着実に伸びていると認められる。
・制御システムを狙ったマルウェアが伸びていることから、制御システムに対するセキュリティ意識が高まっていることが認められる。



※金融、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）
※前設問(2)②(b)選択肢⑫選択事業者のみの回答

(h) 経営層への報告対象

・標的型攻撃メールは経営層を狙ったものが多いことから、不審メールへの対処状況に対する関心は高いと考えられる。
・昨今の情報漏えい事件を背景として、外部委託先のセキュリティ対策状況にも関心が高いと推察される。

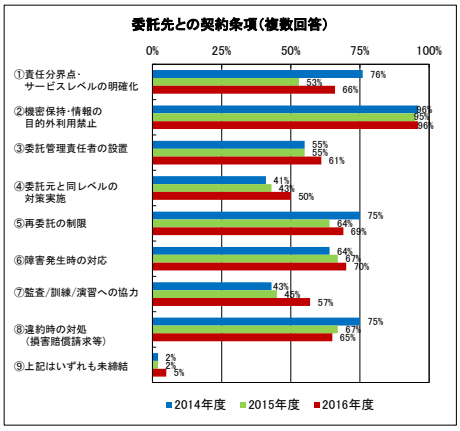


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

③ 要件の明確化

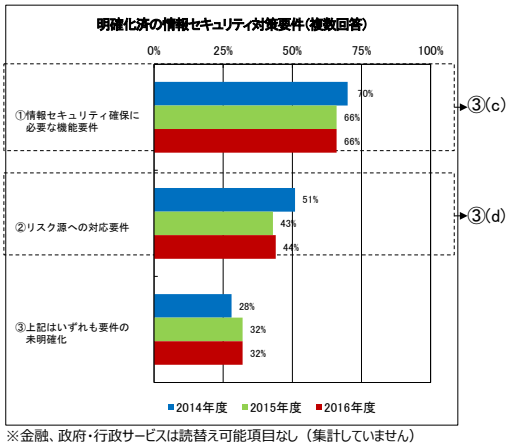
(a) 委託先との契約条項

・委託先も含めたセキュリティ対策が必要だと叫ばれる中、委託先との契約の中で監査/訓練/演習への協力を求める事業者が増加したと認められる。



(b) 明確化済の情報セキュリティ対策要件

・要件の明確化に関する大きな変化はない。



※金融、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）

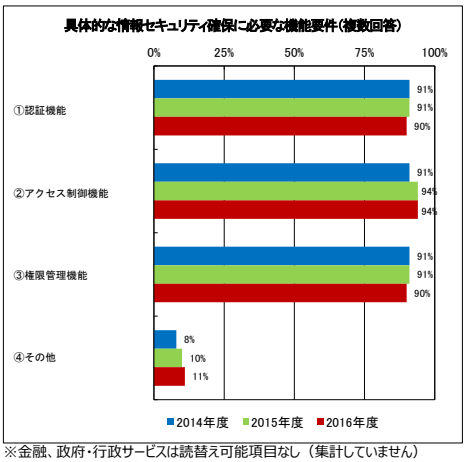
調査結果詳細（4/6）

(2) 情報セキュリティ対策の実施状況（続き）

③ 要件の明確化（続き）

(c) 具体的な情報セキュリティ確保に必要な機能要件

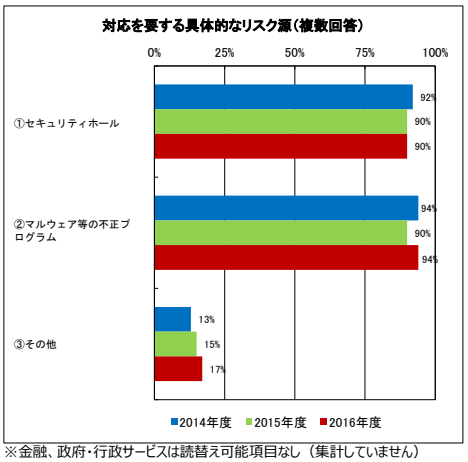
・認証、アクセス制御といった基本的な機能要件に関しては、これまで同様に実施できていると認められる。



※金融、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）
※前設問(2)③(b)選択肢①選択事業者のみの回答

(d) 対応を要する具体的なリスク源

・セキュリティホールやマルウェア等の不正プログラムといったリスク源に関しては、これまで同様に対応を要するリスク源として認識されていると認められる。

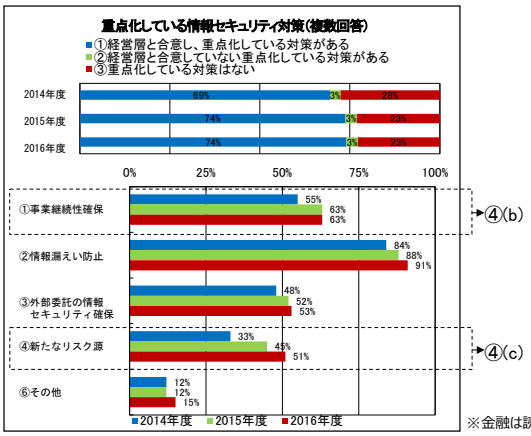


※金融、政府・行政サービスは読替え可能項目なし（集計していません）
※前設問(2)③(b)選択肢②選択事業者のみの回答

④ 重点化対策と対象とする脅威

(a) 重点化している情報セキュリティ対策

・経営層の関与の伸びに加えて、重点化している情報セキュリティ対策が全体的に伸びていることから、重要インフラ防護に対する意識が醸成されつつあると認められる。

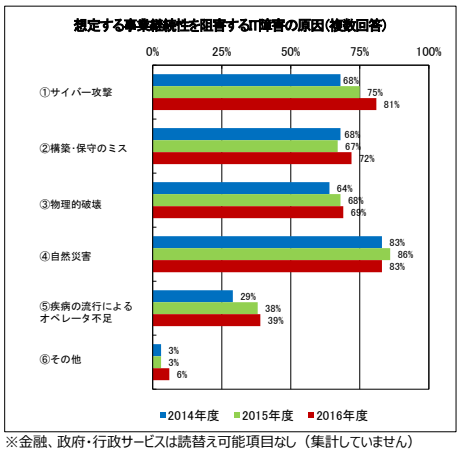


④(b)
④(c)

※金融は読替え可能項目なし（集計していません）

(b) 想定する事業継続性を阻害するIT障害の原因

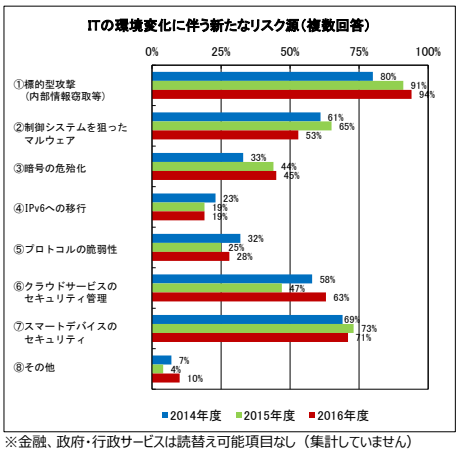
・サイバー攻撃により事業継続が阻害されるという事が認知されつつあると推察される。



※金融、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）
※前設問(2)④(a)選択肢①選択事業者のみの回答

(c) ITの環境変化に伴う新たなリスク源

・標的型攻撃の脅威は依然として高く、その対策が着実に伸びていると認められる。



※金融、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）
※前設問(2)④(a)選択肢④選択事業者のみの回答

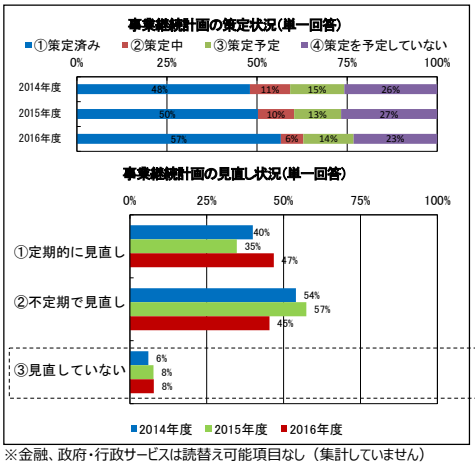
調査結果詳細（5/6）

(2) 情報セキュリティ対策の実施状況（続き）

⑤ 事業継続計画の策定・改定

(a) 事業継続計画の策定・見直し状況

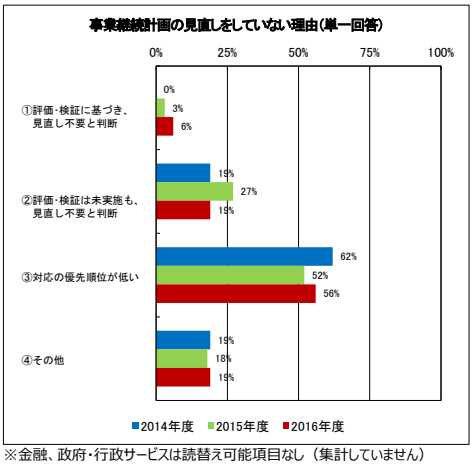
・事業継続計画が必要であるという意識が年々醸成されつつあると推察される。



※金融、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）

(b) 事業継続計画の見直しをしていない理由

・事業継続計画の見直しを実施していない事業者の大半においては、見直しの必要性・重要性が組織内で理解されていないと認められることから、指針等で啓発していく必要がある。



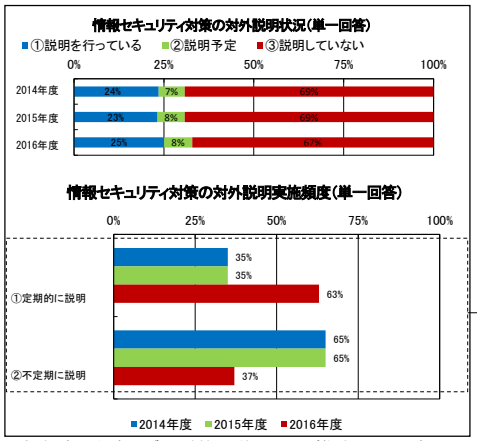
※金融、政府・行政サービスは読替え可能項目なし（集計していません）

⑥ 対策の対外説明

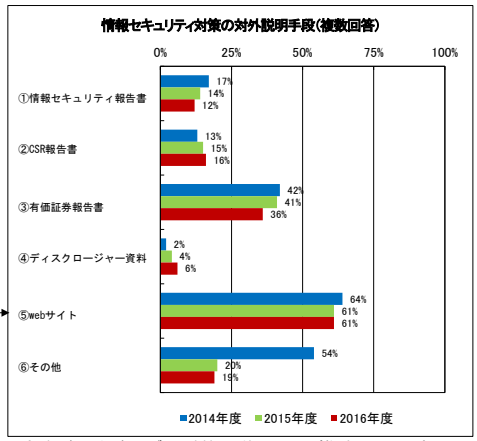
(a) 情報セキュリティ対策の対外説明状況

(b) 情報セキュリティ対策の対外説明手段

・国民の安心感を醸成させるべく、情報セキュリティ対策状況について、Webサイト、有価証券報告書等を通じて、定期的に説明するようになっていると推察される。



※金融、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）



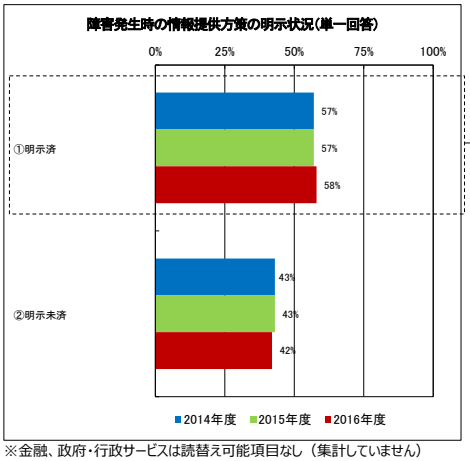
※金融、政府・行政サービスは読替え可能項目なし（集計していません）

⑦ IT障害発生時の情報提供

(a) 障害発生時の情報提供方策の明示状況

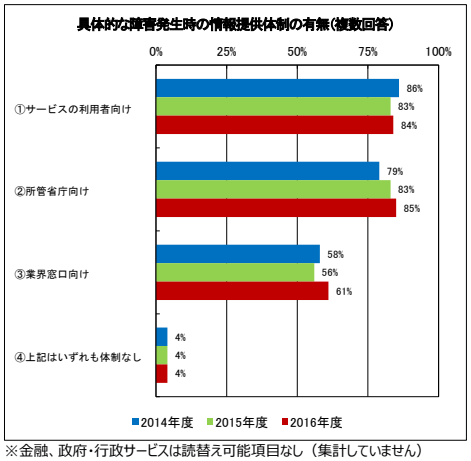
(b) 具体的な障害発生時の情報提供体制の有無

・障害発生時に即応できるような対策を取っている事業者等は6割弱をキープできていると認められる。



※金融、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）

・サービスの利用者向けだけではなく、所管省庁や業界窓口に向けての情報共有体制の構築が伸びており、障害発生時の対応強化に寄与していると認められる。



※金融、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）

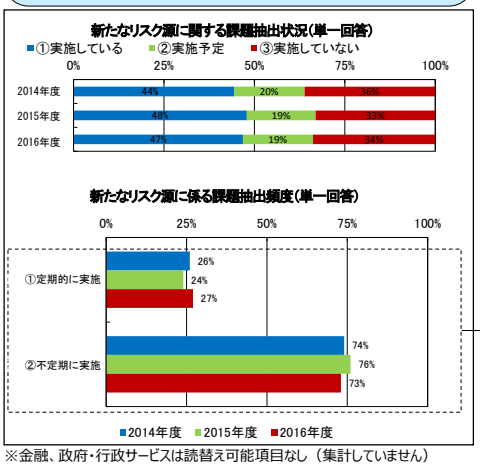
調査結果詳細（6/6）

(2) 情報セキュリティ対策の実施状況（続き）

⑧ ITの環境変化に伴い想定する脅威

(a) 新たなリスク源に係る課題抽出状況

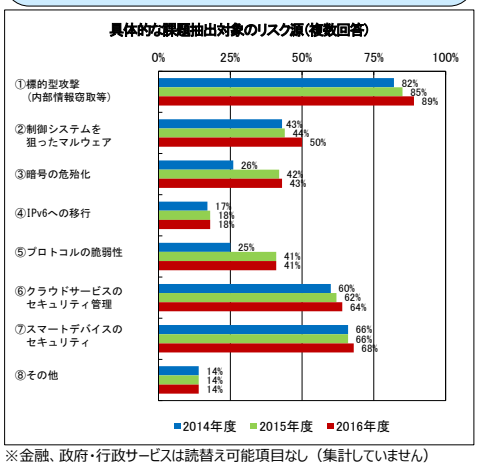
・新たなリスク源の発生は不定期であることから、課題抽出を定期的に実施する事業者等が増えていないと推察される。



※金融、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）

(b) 具体的な課題抽出対象のリスク源

・標的型攻撃の脅威が依然として高いことから、その対策が着実に伸びていると認められる。
・制御システムを狙ったマルウェアの事例が増えていることから、制御システムに対するセキュリティ意識が高まっていることが認められる。



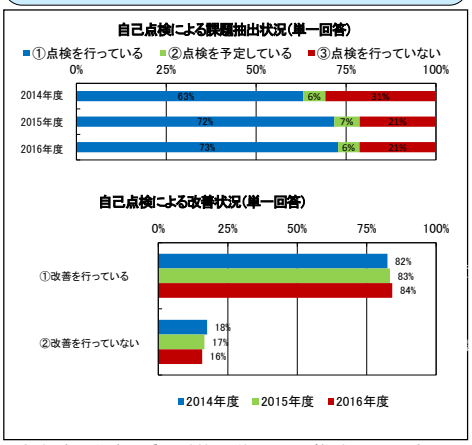
※金融、政府・行政サービスは読替え可能項目なし（集計していません）

(3) 安全基準等の準拠状況

① 内規に基づく自己点検の実施

(a) 自己点検による課題抽出・改善状況

・自己点検を行う事業者が増えていることから、情報セキュリティ対策のＰＤＣＡの重要性が認識されつつあると推察される。

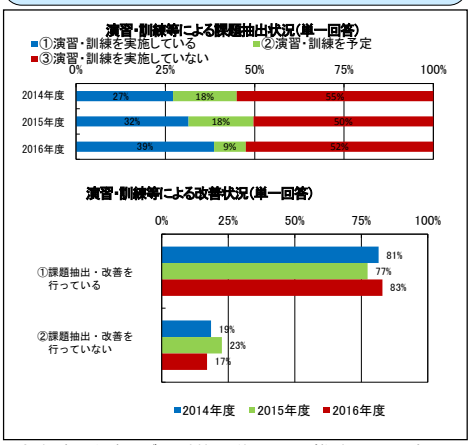


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

② 演習・訓練等の実施

(a) 演習・訓練等による課題抽出・改善状況

・実施している事業者は着実に増加しており、課題抽出・改善を行っている事業者も伸びていることから、演習・訓練の有用性が浸透していると認められる。

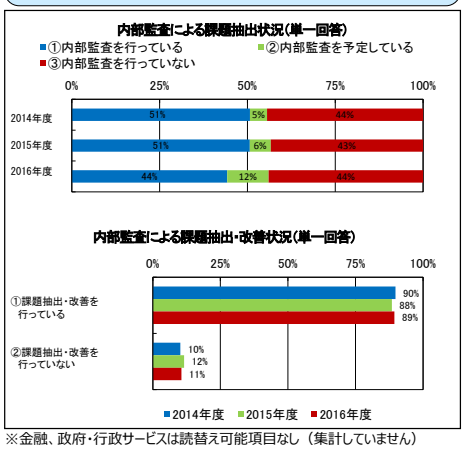


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

③ 内部監査の実施

(a) 内部監査による課題抽出・改善状況

・内部監査の実施事業者等については、大きな伸びが認められない。

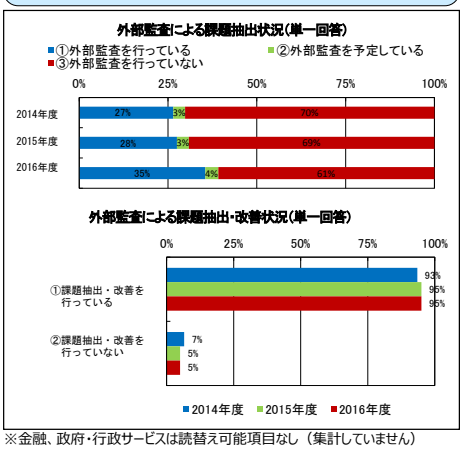


※金融、政府・行政サービスは読替え可能項目なし（集計していません）

④ 外部監査の実施

(a) 外部監査による課題抽出・改善状況

・外部監査を実施している事業者等が伸びているため、外部監査の有用性が認知されつつあると認められる。



※金融、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）

調査結果詳細 - 自由意見 -

【安全基準等に関する意見】

- 業界団体や所管省庁等が発行するガイドライン等において、分野特有の組織特性や慣習等を考慮した内容にしてほしい。
- 情報セキュリティ対策の強化の必要性は理解をしているが、対策の導入においては、企業規模に応じて事業性・採算性を含め検討していくため、全事業者に共通した強制基準にならないようにしてほしい。
- 事業者の規模に応じた規模別対策や、規模別のセキュリティ対策に向けたロードマップなどがあると、目標としやすいのではないか。

【指針に関する意見】

- 政府が主導して、情報セキュリティ対策における有効な手段を示してほしい。
- 指針に関する説明会や情報セキュリティ対策の講習会を開催してほしい。
- リスク対策における表記について、指針と ISO31000 シリーズの表記を統一してほしい。
- 記載されている用語は、専門的知識なしでも理解できるようにしてほしい。

【情報共有体制の推進に関する意見・要望等】

- インシデント事例や他社の情報セキュリティ対策への取組事例等の情報がほしい。
- 匿名で情報提供や共有する仕組みが必要。
- 各社間の交流の活発化を進めてほしい。

【アンケートに関する意見】

- WEB 上のアンケート等で、簡潔なアンケートにしてほしい。
- アンケート項目が多すぎる。

【国・政府に対する意見・要望等】

- 助成金や減税措置を導入してほしい。
- 将来を考えた人材育成の支援を重視してほしい。
- 事業者単独でセキュリティ人材を育成することは困難。
- オリンピック・パラリンピックに向けたセキュリティ対策の整備を進めてほしい。

【その他の意見】

- 制御システム系に対する情報セキュリティ対策の重要性は認識している。
- 予算が許すなら、全ての情報セキュリティ対策を導入したい。
- 少人数、特に兼任のみで管理していくのは、すでに限界となっている。

（参考）アンケート項目

【Ⅰ．基礎的事項】
貴社（又は貴団体）の従業員数を選んでください。

【Ⅱ．指針の認知状況に係る事項】
(1)　指針_本編、指針_対策編及び指針_手引き書をご存知ですか。［(1)①(a)］
(2)　指針_本編、指針_対策編及び指針_手引き書を何で知りましたか。［(1)①(b)］
(3)　今後の周知方法の検討に活かしたいと思いますので、効果的に周知する手段について良いと思われるものがありましたらご紹介ください。

【Ⅲ．情報セキュリティ対策の実施状況に係る事項】
(1)　情報セキュリティ対策にあたって、経営層と合意の上、重点化しているものをお知らせください。［(2)④(a)］
(2)（ＩＴ障害防止等の観点から見た事業継続性確保のための対策を重点化している場合）
事業継続性を阻害する具体的な想定原因をお知らせ下さい。［(2)④(b)］
(3)（ＩＴの環境変化に伴う新たなリスク源への対策を重点化している場合）対象とするリスク源等をお知らせください。［(2)④(c)］
(4)　内規の策定・見直しの契機をお知らせ下さい。　［(1)②(a)］
(5)　内規策定・改定を行う際の体制をお知らせ下さい。［(1)③(a)］
(6)　内規改定に要するおおよその期間をお知らせ下さい。
(7)　内規において規定済のものをお知らせ下さい。［(1)③(b)］
(8)　対策に係る計画またはロードマップの策定・見直し状況をお知らせ下さい。［(2)②(a)］
(9)　事業継続計画の策定・見直し状況をお知らせ下さい。［(2)⑤(a)］
(10)（事業継続計画の策定・見直しを行ったことはあるが、現在は見直しを行っていない場合）現在は見直しをしていない理由をお知らせ下さい。［(2)⑤(b)］
(11)　組織・体制及び資源の確保として行っているものをお知らせ下さい。［(2)①(a)］
(12)（情報セキュリティに係る人材育成、教育を行っている場合）教育テーマの対象としているものをお知らせ下さい。［(2)①(b)］
(13)　委託先との契約において締結されているものをお知らせ下さい。［(2)③(a)］
(14)　情報セキュリティ要件を明確にしているものをお知らせ下さい。［(2)③(b)］
(15)（情報セキュリティ確保のために求められる機能の観点から、情報システムに導入すべきセキュリティ要件を明確化している場合）明確化した情報セキュリティ要件をお知らせ下さい。［(2)③(c)］
(16)（情報セキュリティについてのリスク源に対して、情報システムに導入すべきセキュリティ要件を明確化している場合）明確化した情報セキュリティ要件にて対象とするリスク源をお知らせ下さい。［(2)③(d)］
(17)　明確化した情報セキュリティ要件への対応として、対策を行っているものをお知らせ下さい。［(2)②(b)］
(18)（明確化した情報セキュリティ要件への対策として「ネットワークへの侵入防止」を行っている場合）具体的に対応しているものをお知らせ下さい。［(2)②(c)］
(19)（明確化した情報セキュリティ要件への対策として「ファイアウォールの導入」を行っているが、適用範囲の妥当性評価・必要に応じた見直しは行っていない場合）適用範囲の妥当性評価・必要に応じた見直しを行っていない理由をお知らせ下さい。［(2)②(d)］
(20)　（明確化した情報セキュリティ要件への対策として「侵入検知システムの導入」を行っているが、検知条件の妥当性評価・必要に応じたチューニングは行っていない場合）検知条件の妥当性評価・必要に応じたチューニングを行っていない理由をお知らせ下さい。［(2)②(e)］
(21)（情報セキュリティ要件への対策として無許可ソフトウェアの導入禁止を行っている場合）具体的に対応しているものをお知らせ下さい。［(2)②(f)］
(22)（ＩＴの環境変化に伴う新たなリスク源への対策を行っている場合）対象としているリスク源をお知らせ下さい。［(2)②(g)］
(23)　経営層への報告対象としているものをお知らせ下さい。［(2)②(h)］
(24)　情報セキュリティ対策についての対外的な説明状況をお知らせ下さい。［(2)⑥(a)］
(25)　（情報セキュリティ対策についての対外的な説明を行っている場合）その説明方法をお知らせ下さい。［(2)⑥(b)］
(26)　重要インフラサービスに障害が発生した場合に、障害の状況や復旧等の情報提供の方策が明示されていますか。［(2)⑦(a)］
(27)（重要インフラサービスに障害が発生した場合における情報提供の方策が明示されている場合）提供先において情報提供に向けた体制がありますか。［(2)⑦(b)］
(28)　ＩＴの環境変化に伴う新たなリスク源について、リスクの特定・分析等を通じた確認・課題抽出を行っていますか。［(2)⑧(a)］
(29)（ＩＴの環境変化に伴う新たなリスク源について確認・課題抽出を行っている場合）現時点で対象とする新たなリスク源等をお知らせ下さい。［(2)⑧(b)］
(30)　安全基準等や内規等に基づく情報セキュリティ対策の実施状況の自己点検を行い、同対策の改善につなげていますか。［(3)①(a)］
(31)　情報セキュリティ対策の実施状況に係る内部監査を行い、同対策の改善につなげていますか。［(3)③(a)］
(32)　情報セキュリティ対策の実施状況に係る外部監査を行い、同対策の改善につなげていますか。［(3)④(a)］
(33)　ＩＴ障害発生を想定した演習・訓練等を実施し、情報セキュリティ対策の改善につなげていますか。［(3)②(a)］

【Ⅳ．　その他一般的事項】
(1)　本編、対策編に対してのご意見がありますか。（自由意見を記載）
(2)　安全基準等に対してのご意見がありますか。（自由意見を記載）
(3)　その他、ご意見がありますか。（自由意見を記載）

※［ ］の部分は、調査結果詳細における該当箇所。

（参考）往訪調査（1/2）

1.往訪調査の位置付け

安全基準等の浸透状況調査の補完として、アンケート形式による安全基準等の浸透状況調査以外に、直接重要インフラ事業者等に意見を聞き、具体的な対策状況に係る課題抽出及び良好事例の収集を行う。
※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（平成27年５月25日サイバーセキュリティ戦略本部改訂）

2.調査方法

事前に往訪先事業者からいただいたシステム構成図及び事前アンケートに対する回答を基にした現地ヒアリング

3.主な調査内容

【主な調査項目】

① 経営層の関与状況　② 規程類や契約類の遵守状況
③ 人材育成の考え方　④ 障害対応体制　⑤ その他

※その他、情報共有や最近のサイバー攻撃及び分野内のセキュリティ動向などについて意見交換を実施

4.調査対象

重要インフラ事業者１０社（医療・金融・物流・化学・石油）
※所管省庁や関係セプターと調整の上、対象事業者を選定

5.調査期間

2016年1月～2016年10月

(1) 良好な点

1. 経営層の関与

- 内部の障害対応訓練に役員が参加することが通例となっており、他業務よりも優先すべきという意識が醸成されている。
- 経営層が委員長となっているリスクマネジメント会議を設けており、情報セキュリティについてもその場で共有している。
- IT系部署と制御系部署の管理権限の一部を特定の部門に一本化することで、情報共有できる体制を構築している。

2. 規定類や契約類の遵守状況

- 規定類やセキュリティガイドライン等は、国内及び海外事業所で統一したものを運用している。
- 規定類は、内部監査や外部監査の結果を受けて、適時改正している。

3. 人材育成

- 人事異動が発生するごとにセキュリティ教育を実施しているほか、一部の事業者では月に1度、全社員を対象に情報セキュリティに関するe-learningを実施している。

4. 障害対応体制

- システム障害が発生しても、手作業によりサービスを継続することができるように準備しており、ステークホルダーを含めた全職員で訓練を実施しており、同訓練を年に一回程度実施している事業者も存在する。
- インシデント発生時は、CSIRTに連絡し、深刻度に応じて社長の指示により対応する運用としている。

※上記記載内容は、一部事業者の意見を記載しているだけであり、往訪調査を行った全事業者の意見を総括しているわけではありません。

（参考）往訪調査（2/2）

(2) 問題点

1. 経営層の関与

- 一部の事業者では、経営層から情報セキュリティに関する指示が出てくることがほとんどない。
- 担当役員の情報セキュリティに対する理解の度合いにより、投資への意識が大きく異なっている。

2. 規定類や契約類の遵守状況

- 一部の事業者では、IT-BCPは策定しているものの、改定作業を行っていない。
- BCPは策定しているが、ITに特化したものは策定していない。

3. 人材育成

- 一部の事業者では、情報セキュリティに特化した教育は行っていない。
- 情報セキュリティ人材については、社会全体として不足していると感じる。
- 事業者単独でセキュリティ人材を育成することは困難である。

4. その他

- 一部の事業者では、NISC発行の重要インフラニュースレター以外の情報源がない。
- 一部の事業者では、社員個人のセキュリティ意識やITリテラシーが低いと感じられる。
- 上位役職者へのセキュリティ教育をどのように行えば効果的か思案している。

※上記記載内容は、一部事業者の意見を記載しているだけであり、往訪調査を行った全事業者の意見を総括しているわけではありません。

(3) 考察

- 経営層の情報セキュリティに対する理解度が高い事業者では、経営層が障害対応訓練や情報共有を主導的に行っているが、経営層の理解度が低い事業者では、サイバー攻撃対策への投資が推進されていない傾向にあるため、経営層の情報セキュリティに対する理解度を高める必要がある。
- 一部の従業員数1000名未満規模の事業者では、IT-BCPを策定していない、もしくは策定しているが、定期的な見直しを実施できていない事業者が見受けられる。また、情報セキュリティ教育を実施していない事業者では、社員の情報セキュリティに対する意識の低くなっている。このことから、従業員数1000名未満規模の事業者の取組支援を強化する必要がある。
- 往訪先事業者の多くは、情報セキュリティ人材が不足していると感じていることから、情報セキュリティ人材の育成を支援する必要がある。
- 制御系部署とIT系部署の管理権限の一部を組織的に統合し、円滑な情報共有の実施、および障害対応体制を確立している事業者があるが、制御系・IT系に精通した人材の有無により、取り組みの度合いに違いがあると考えられる。制御系部署、IT系部署ともに人材が固定化される傾向が見受けられたことから、ローテーションによる人材育成が重要である。
- システム障害対応訓練をステークホルダーと合同で行っている事業者があり、情報セキュリティに関する意識が醸成されている。このことから、常日頃から関係組織との意思統一および情報共有が重要であると考えられる。

別添４－５　情報共有件数

「重要インフラの情報セキュリティ対策に係る第３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				
	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	313	256	155	132	856
関係省庁・関係機関からのNISCへの情報共有	27	52	4	24	12	1	41
NISCからの情報提供	38	44	16	9	26	29	80

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				
			計	計	1Q	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	9	75	130	108	57	35	330
発生した事象	機密性を脅かす事象	情報の漏えい	9	15	8	11	5	6	30
	完全性を脅かす事象	情報の破壊	14	52	12	10	11	14	47
	可用性を脅かす事象	システム等の利用困難	38	86	13	22	29	16	80
	上記につながる事象	マルウェア等の感染	27	111	122	89	42	36	289
		不正コード等の実行	3	11	4	1	1	4	10
		システム等への侵入	12	27	7	7	6	6	26
		その他	12	24	17	8	4	15	44

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				
		計	計	1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	6	83	224	190	90	42	546
	ユーザＩＤ等の偽り	7	8	0	0	1	0	1
	DoS攻撃等の大量アクセス	25	47	6	5	9	3	23
	情報の不正取得	13	8	7	3	3	1	14
	内部不正	0	2	0	0	0	0	0
	適切なシステム等運用の未実施	4	10	2	1	5	11	19
偶発的な原因	ユーザの操作ミス	0	10	8	2	3	2	15
	ユーザの管理ミス	2	5	3	1	0	4	8
	不審なファイルの実行	1	51	97	93	37	16	243
	不審なサイトの閲覧	1	49	16	4	6	3	29
	外部委託先の管理ミス	10	12	4	5	1	10	20
	機器等の故障	7	17	5	8	3	6	22
	システムの脆弱性	9	29	10	8	18	20	56
	他分野の障害からの波及	1	5	0	0	0	0	0
環境的な原因	災害や疾病等	0	0	0	0	0	0	0
その他の原因	その他	9	22	7	8	7	12	34
	不明	43	105	32	18	14	28	92

別添４－６　セプター概要

セプター及びセプターカウンシルの概要

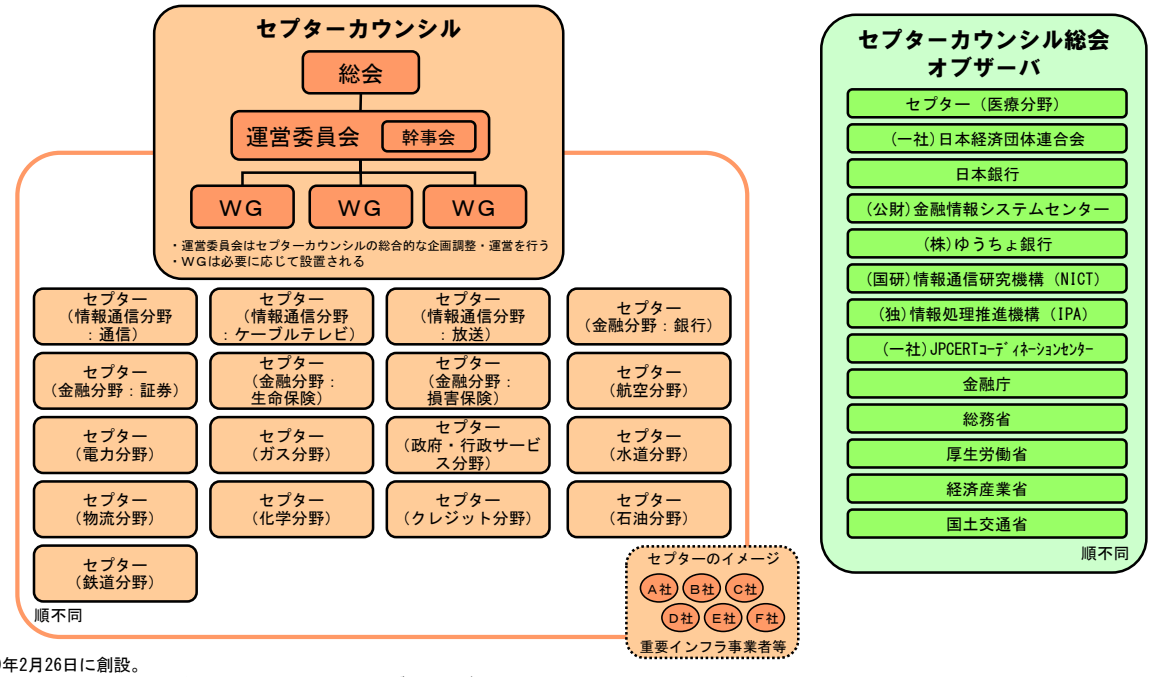
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、２００９年２月２６日に創設。

セプターカウンシルの概要（2017 年４月 25 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。

セプター特性把握マップ

2017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 銀行等CEPTOAR	金融CEPTOAR連絡協議会 証券CEPTOAR	金融CEPTOAR連絡協議会 生命保険CEPTOAR	金融CEPTOAR連絡協議会 損害保険CEPTOAR	航空分野における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
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 品質グループ	定期航空協会	(一社)日本鉄道電気技術協会	電気事業連合会 情報通信部	(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	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	23社 1団体	335社 1団体	195社 1団体	1,428社	261社 ７機関	41社	29社 (オブザーバ３社含む)	14社 1団体	22社 1団体	12社 2機関	10社	47 都道府県 1,741 市区町村	1グループ 6機関	8水道事業体	6団体 16社	13社	28社	13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	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）	376社・団体	438社	―	3社・団体	―	―	―	―	―	―	38社	―	377社・機関	内容に応じ1,351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	2016年7月 航空分野（国土交通省航空局 → 定期航空協会）、鉄道分野（国土交通省鉄道局 →（一社）日本鉄道電気技術協会）																	

■ その他

既存事業領域を越える連携等	情報通信（Telecom-ISACの活動を新たに設立されたICT-ISACに移行し一部の放送事業者及びケーブルテレビ事業者が加盟）、電力（電力ISACを設立、４月より運用開始予定）、 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４－７　分野横断的演習

分野横断的演習の実施経緯

第１次行動計画（2006～2008年度）

【目標】官民連携の充実

	官民連携の仕組みづくり	官民連携体制の機能向上	官民連携体制の実効性向上
年度	2006年度	2007年度	2008年度
人数	90名	120名	136名
テーマ	災害 災害に伴うIT障害の発生	意図的要因 サイバー攻撃に伴うIT障害の発生	意図的要因 IT障害の発生原因を関係者間の情報共有で特定

第2次行動計画（2009～2013年度）

【目標】重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出

① 分野横断的な脅威に対する共通認識の醸成
② 他分野の対応状況把握による自分野の対応力強化
③ 官民の情報共有をより効果的に運用するための方策

2009年度	2010年度	2011年度	2012年度	2013年度
116名	141名	131名	148名	212名
広域停電	大規模通信障害	電力・ガス等の重要インフラ複合障害	電力・通信等の重要インフラ複合障害＋便乗型ITインシデント	大規模な情報セキュリティインシデント

第3次行動計画（2014年度～2016年度）

【目標】事業者等による情報セキュリティ対策の実施及び実効性の確認等を通じ重要インフラ全体の防護能力の向上を図る。

✓ 事業者等による障害対応能力の向上
✓ 重要インフラ全体の対策水準の底上げ
✓ 関係主体間の連携・維持の強化
✓ 国は事業者等の自律的かつ継続的な取組を支援

年度	2014年度	2015年度	2016年度
人数	348名	1,168名	2,084名
テーマ	IT障害発生時の対応に関する事項を軸とし、情報共有を含む障害対応体制の実効性を検証		

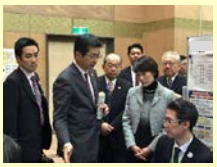
2016 年度分野横断的演習　開催概要

＜事前説明会＞
日　　程　：２０１６年１０月２８日（金）、１１月１日（火）、２日（水）
場　　所　：東京会場、地方会場（説明会の模様について、演習当日まで動画配信）
内　　容　：①重要インフラ防護施策の概要説明
②分野横断的演習の事前説明
③有識者による講演（「情報セキュリティの現状と課題」（金野委員））

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：２０１６年１２月７日（水）１２：１５～１７：００
場　　所：東京会場、地方会場、自職場
参 加 者：５０５組織２，０８４名
【重要インフラ事業者等：１３分野　合計４４６機関】
【セプター：１３分野１８セプター】
【政府機関　等】


演習の模様


丸川大臣による視察

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ＩＴ障害が発生したケースを想定し、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）
○第２部　サービスへ影響が生じるＩＴ障害が発生し、事業継続が脅かされるケースを想定し、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、ＯＳ脆弱性、制御システム）

演習を通じた内規・体制等の課題抽出

＜意見交換会＞
日　　時：２０１７年１月２４日（火）１４：００～１７：３０
場　　所：東京会場、大阪会場
内　　容：①分野を超えた事業者間でのグループディスカッション
②有識者による講演（「最近のサイバー攻撃の傾向と情報連携の促進」（真鍋委員））

他事業者等との情報共有を通じた改善の促進

2016 年度における取組実績（概要）

- セキュリティ意識の高まりと多様なニーズに応える演習の企画
- 各事業者のセキュリティ対策に資する演習の運営

事前準備

＜参加募集＞
- ✓ 複数の参加形態を活用した柔軟な参加モデルを提示
  （例：会場参加、自職場参加　等）
- ✓ 参加するプレイヤー選定に応じた社内の検証課題を例示

＜事前説明会／サブコン説明会＞
- ✓ 東京会場、地方会場にて説明会を実施
- ✓ サブコンの配置のあり方について事例紹介し、サブコンの活用による演習効果の向上を促進
  （例：仮想1社、複数社に共通するサブコンの配置　など）

＜セプター訓練の実施＞
- ✓ セプター訓練を本演習の前に実施し、分野内の情報共有体制における課題・改善事項を抽出

演習当日

＜演習取組み＞
- ✓ 東京会場、地方会場、自職場間で相互に連携可能な演習環境を設営
- ✓ 多様な参加者への適合と、CSIRTアクションを盛り込んだシナリオ整備

＜見学会＞
- ✓ 多数の見学参加を可能とする会場設営、時間割の設定
- ✓ 経営層向けの見学参加の呼びかけ、経営層向けの内容を含む講演の実施

事後の振返り

＜意見交換会＞
- ✓ 東京会場、大阪会場にて分野横断的に編成されたグループをベースとしたディスカッションを実施
- ✓ セキュリティに関する対策や課題等に関する意見交換や人脈形成を促進

分野横断的演習の取組の経緯

演習を踏まえた気づき（取組の視点）

- 演習参加を踏まえたPDCAの日常的な実践
- 組織内におけるセキュリティ対策の改善や必要なリソースの確保に関する経営層による理解の促進
- セキュリティ対策レベル、サービス内容等を異にする事業者が有する多様な演習ニーズへの対応
- 情報共有すべき具体的な内容の再確認・徹底

2017年度に向けた諸課題

- セキュリティ意識の高まりと旺盛なニーズに応える演習企画
  （例）
  - 地方会場（九州）の内容充実
  - 重要インフラ事業者の裾野拡大に加え、密接に関連する外縁の事業者の参加拡大
  - 他関係機関や他演習／訓練との相互連携

- 各事業者のセキュリティ対策のPDCAに資する演習運営
  （例）
  - 経営者の理解／直接参加の増進
  - 見学会スタイルの在り方検討
  - 最新の攻撃手法対策やCSIRT能力向上を目指したシナリオ整備

- 情報共有体制の実効性向上に係る施策
  （例）
  - 情報伝達ルートの有効性に関わる検証
  - プレイヤー以外の各主体に対する演習テーマの設定（NISC／所管省庁／セプター事務局など）

- 演習運営ノウハウや知識等の還元
  （例）
  - 自社演習実施に資する演習ノウハウの還元（E-learning等の仮想演習環境の検討）
  - 国際対応（海外組織への施策紹介）

別添４－８　セプター訓練

セプター訓練（第 11 回）の概要

1. 概要

○「セプター訓練」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」を踏まえ、セプターにおける情報疎通機能の確認等を行うために、内閣官房の主催により実施している訓練。

○「セプター訓練」と「分野横断的演習」を相互に連携・補完させることを通じて、各々の重要インフラ分野内部における「縦」と分野間における「横」の情報共有体制を強化し、重要インフラ防護の維持・向上を図ることが可能。

2. 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セプターより、合計2,020者

3. 実施期間

2016年7月から10月まで（セプター毎に異なる日時に実施）

4. 訓練内容

(1) NISCが所管省庁経由でセプター事務局に情報提供を発出。
(2) セプター事務局は参加事業者に対し情報提供及び受信確認を実施し、所管省庁経由でNISCへ報告。
→関係主体における情報共有体制の実効性の検証、既存の手順等の改善、解決すべき課題の抽出。

セプター訓練（第 11 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2,020者が訓練に参加。

2. 実態に即した訓練内容

○多くのセプターにおいて実施日時を指定せずに実施（15セプター）

○最新のトレンド、分野固有の内容を織り込んだ情報提供を実施（12セプター）

○通常の連絡手段が使用不可能との想定の下、代替的な連絡手段の実効性を検証（5セプター）

3. 訓練の成果等

○昨年度と比較し、多くのセプターにおいて訓練情報の受信確認の割合が向上（15セプター）

○主担当の不在時、夜間・休日等における体制構築の必要性をはじめ、多くの課題について認識

○その後実施された「分野横断的演習」（12月7日）において、参加者の約8割が「セプター訓練で確認した情報共有の手順を、演習の際に確実に実践できた。」旨を回答

別添４－９　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※の枠組みの評価に当たって、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3次行動計画（平成27年5月25日サイバーセキュリティ戦略本部改訂）

調査の運営

補完調査として、IT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ＩＴ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。

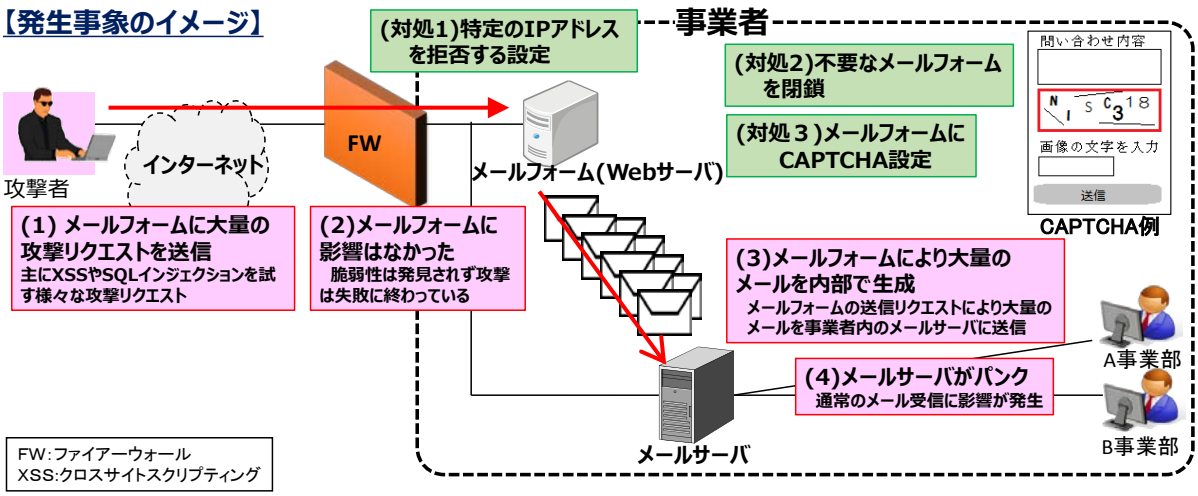
事例１　メールフォームへの攻撃
事例２　アクセス制限の不備
事例３　ランサムウェア被害
事例４　管理サーバへの不正アクセス
事例５　ソフトウェアの継続的なセキュリティ対策
事例６　システムの不具合によるサービス障害

事例１　メールフォームへの攻撃（1/2）

【事例の概要】

- Webサイトに設置した複数のメールフォームに、脆弱性を狙った大量のリクエストがあった。
- メールフォームに脆弱性はなく、メールフォームやWebサイトに影響はなかった。
- メールフォームから大量のメールが事業者内に送信され、事業者内のメールが約1日受信できない状態になった。
- メールを利用した一部の業務について、手順を変更して実施した。

【発生事象のイメージ】



事例１　メールフォームへの攻撃（2/2）

【１　背景】

- アンケートや各種イベントの申込受付のために、Webサイトに20か所程度メールフォームを設置していた。
- メールフォームに入力されたメッセージは、事業者内の特定のメールアドレス宛に送信される仕組みだった。
- メールフォームは定期的にメンテナンスされており、未対応の脆弱性などはなかった。

【２　検知】

- 他事業部の担当者からシステム担当者へメールが届いていないとの連絡があった。

【３　対処】

- 攻撃元IPアドレスを特定し、該当IPアドレスからの接続を拒否した。
- 現在使用されていないメールフォームを閉鎖した。
- メールフォームにCAPTCHAを設定した。

【４　原因】

- 攻撃者が、複数のメールフォームに対してWebサイトの脆弱性を探る多数の攻撃リクエストを送信したため。

※WebサイトにXSSやSQLインジェクションなどの脆弱性はなく、攻撃者の意図は失敗に終わったと思われる。

【５　再発防止策】

＜システム面＞

- 特定の送信元IPアドレスをFWで接続拒否する設定を追加。
- 特定の送信元IPアドレスをメールフォームのプログラムで拒否する設定を追加。
- すべてのメールフォームにCAPTCHAを設定し、自動化された大量アクセスへの対策を実施。

＜運用面＞

- 大量アクセスがあった場合に、送信元IPアドレスを特定する方法の共有。
- 特定の送信元IPアドレスを拒否する設定方法の共有。
- 利用していないメールフォームの閉鎖。

※今回は単一IPアドレスからの大量アクセスだったが、今後、不特定多数のIPアドレスからアクセスされた場合の対応体制については。継続して検討を進めている。

【６　得られた気付き・教訓】

・メールフォーム運用時に考慮する点

① 大量のメールが生成・送信される可能性がある。

WEBサイトの負荷以外にも、送信先のメールサーバの負荷も考慮に入れる必要がある。

② CAPTCHAを利用することにより、自動化された大量のリクエストを軽減できる。

大量のリクエストは自動化されたものが多いため、CAPTCHAを利用することにより軽減を図ることができる。ただし、解析技術の進歩などにより、CAPTCHAの有効性については定期的な見直しが必要。

③ 使用していないメールフォームは閉鎖する。

入力フォームがあるページは攻撃の対象になりやすい。

④ 定期的な脆弱性チェック・ソフトウェアのアップデート対応が必要。

今回の攻撃は、主にXSSやSQLインジェクションを狙った内容であったため、日常的な情報収集・対応がなければ、業務への深刻な影響が出た可能性がある。

⑤ メールフォームから送信されるメールは、メールサーバからも社外発信できない設定にする。

メールフォームに未知の脆弱性があったとしても、外部へメール送信の踏み台として利用されるリスクを減らせるため、多層防御の観点から有効な設計であった。

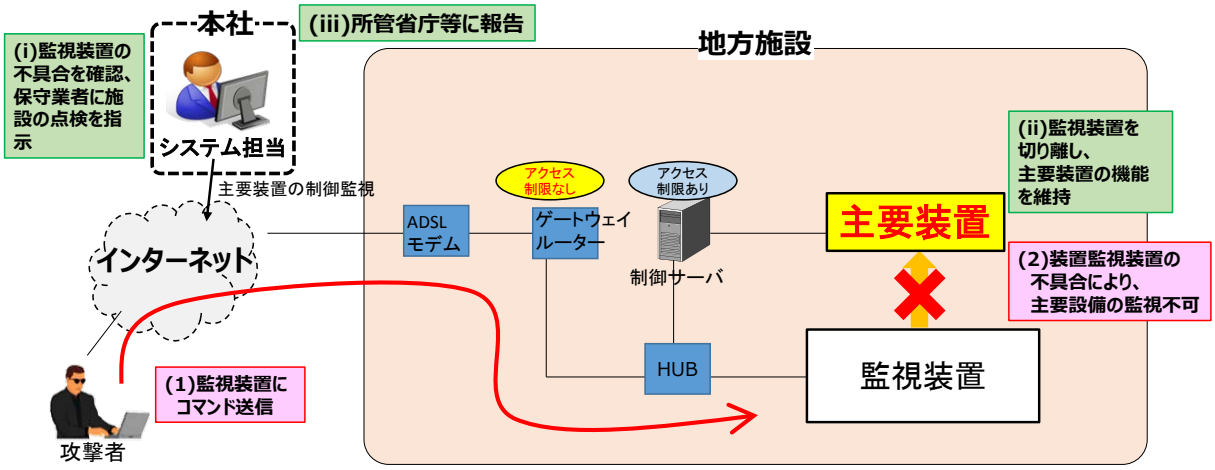
⑥ 必要に応じて、迷惑メール対策を実施する。

意図に反した内容も送られてくるため、頻繁に送られてくるようなら対応が必要になる場合もある。

事例２　アクセス制限の不備

【事例の概要】

- 主要装置へのアクセス制限には対応していたものの、監視装置へのアクセス制限に不備があった。
- 監視装置への不正アクセスにより、機能が停止された。なお、主要装置の基本的な動作には影響はなく、重要インフラサービス自体への影響はなかった。
- 監視装置を切り離し、主要装置の機能を維持した。



【１　背景】

- インターネットを経由して、アクセス制限をしていないゲートウェイルータを介して、監視装置をつないでいた。
- 地方施設のシステムの保守・点検については、保守ベンダーに委託していた。

【２　検知】

- 本社では、毎日定時に監視装置の管理画面にアクセスし、機器が正常に動作しているか確認していたが、その日は監視ができなかった。また同日、システムの保守ベンダーから、当該施設で使用していたものと同型の機器で構成されている他の施設で、監視装置に不具合が発生しているとの連絡があり、発覚した。

【３　対処】

- 現地でサービス提供が維持できているかを現地業者に確認。
- 保守ベンダーに施設の対応を依頼。
- 監視装置へのアクセスに問題があることが分かったため、同装置をシステムから切り離した。
- 所管省庁等へ連絡。

【４　原因】

- ゲートウェイルーターの設定で、ポートにアクセス制限がかけられておらず、また、監視装置で不要なポートが開いていたため、悪意を持った第三者から送信されたコマンドが送られてしまったもの

【５　再発防止策】

- ゲートウェイルーターのポート制限を実施（通常操作は可能）
- 悪意あるコマンドを受け付けないよう、プログラムを改修

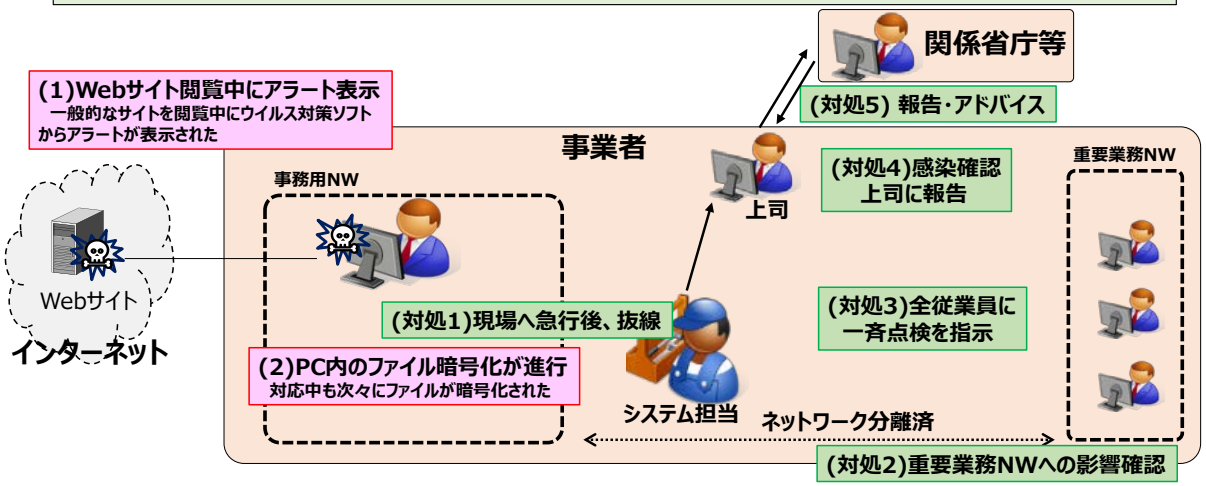
【６　得られた気付き・教訓】

- **積極的な情報共有**
  当該事業者は、同型の機器を使用している他事業者への参考になるだろう、との考えで所管省庁へ自主的に報告を上げた。このように積極的に情報共有していただくことにより、他事業者の参考となり、重要インフラサービスの面的な防護にもつながる。
- **機器の設定確認**
  機器の設定がほぼ初期設定だったことが不正アクセスを受けた要因になったので、本当に必要なポート以外は閉じるなどして、攻撃を受ける可能性を最小限に抑える努力が必要。
- **保守ベンダーとの情報共有等**
  インターネットに接続している機器については、サイバーセキュリティ対策がどのように行われているか保守ベンダーと情報を共有するとともに、必要に応じてセキュリティ対策を第三者に監査してもらうなど検討すると良い。

事例３　ランサムウェア被害

【事例の概要】

- Webサイトの閲覧中に、ウイルス対策ソフトからアラートが表示された。
- システム担当に連絡し、早急にPCをネットワーク（インターネットに接続）から切り離した。
- ランサムウェアに感染したものであり、インシデント対応中もPC内で次々にファイルが暗号化され、最終的には数百のファイルが暗号化されていた。
- 重要業務ネットワークは、事務用ネットワークとは切り離されていたため、重要業務ネットワークへの感染はなかった。



【１　背景】

- 重要業務ネットワーク(クローズドなネットワーク)と事務用ネットワーク(インターネットに接続されているネットワーク) を分けて構築していた。
- 事務用PCの管理は利用者各自に任せられており、セキュリティアップデートがなされていないものもあった。

【２　検知】

- Webサイトの閲覧中にウイルス対策ソフトのアラートが表示され、利用者がシステム担当へ連絡した。

【３　対処】

- システム担当が現場に急行し、ネットワークケーブルを抜線した。
- 当該PCがランサムウェアに感染していること、及び重要業務ネットワークへの影響がないことを確認した。
- 全従業員にウイルスチェックを依頼し、報告させた。
- 状況を上司に報告し、関係省庁等と連携をとった。
- 関係省庁等から助言をもらい、復号ツール(ウイルス対策ベンダー提供)を試した。

【４　原因】

- Webブラウザやソフトウェアの脆弱性を悪用したドライブバイダウンロード攻撃によるランサムウェア感染

【５　再発防止策】

- OSのセキュリティパッチやソフトウェアのバージョンを管理する仕組みの検討を始めた。
- ウイルス対策ソフトの管理サーバを導入し、定期的なパターンファイルの更新管理を検討した。
- 個人が作成したデータを保存するファイルサーバの導入を進めていたが、ランサムウェア対策として、
  ・世代管理できること
  ・PCから書込みができないドライブにバックアップが取れること
  をファイルサーバーの要件に加えた。

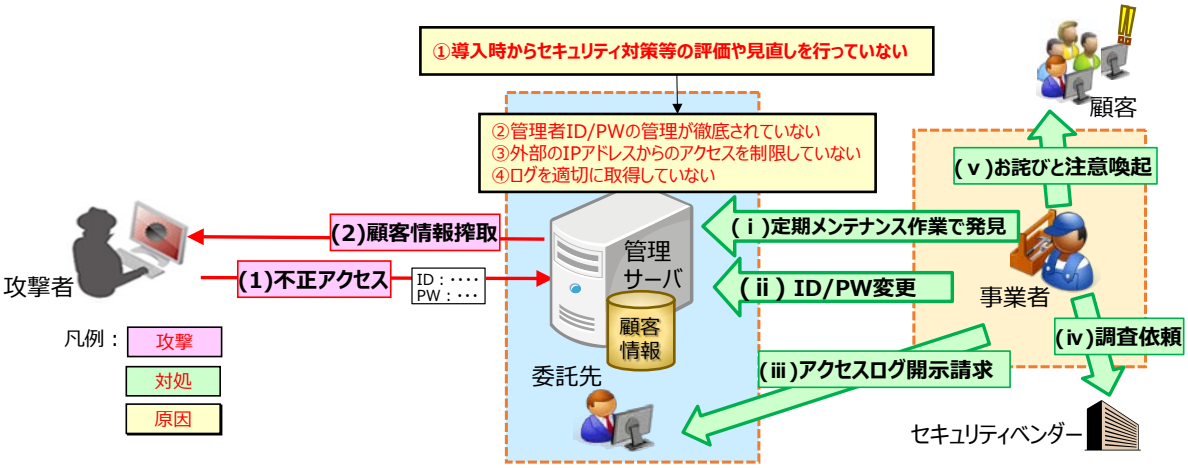
【６　得られた気付き・教訓】

- 日常的に連絡体制を周知することの大切さ
  （社内）システム担当への連絡先が周知され、各利用者もきちんと認識しており、日ごろから活用されていた
  （社外）関係する組織のシステム担当者と定期的に情報交換をしており、事例を共有でき、助言をもらうことができた。
- ファイルバックアップの重要性
  ウイルス対策ベンダーが提供している復号ツールをいくつか試してみたが、処理にかなりの時間がかかり、今回のケースでは最終的には復号できなかった。バックアップ等の事前の対策が有効である。
- ネットワーク分離の大切さ
  重要業務ネットワークを事務用ネットワークと分離していたため、重要業務ネットワークへの影響はなかった。

事例４　管理サーバへの不正アクセス

【事例の概要】

- 攻撃者は、管理者ID/PWを取得し（経緯不明）、当該ID/PWで管理サーバへ不正アクセスを行った。
- 事業者は、管理サーバへの不正アクセスを定期メンテナンスで発見、顧客情報漏えいが判明。
- 委託先でログを取得する契約となっていないものの、委託先へ開示請求を行い、アクセスログを入手。
- アクセスログを基に、セキュリティベンダーに調査を依頼し、HPで顧客へお詫びと注意喚起。
- 継続的な評価・改善、ID/PWの管理徹底、アクセスの制限、ログによる早期検知などの対策を講じた。



【１　背景】

- 委託先のサーバを利用し、顧客情報のやり取りを行っており、外部のIPアドレスからのアクセスが可能。更に、アクセスログを取得する契約となっていない。
- 管理者ID/PWを定期的に変更していない。

【２　検知】

- 管理サーバへの不正アクセスを定期メンテナンスで発見し、委託先へログの開示請求を行った。
- セキュリティベンダーによる調査を行ったものの、管理者ID/PW漏えいの原因特定に至らず。

【３　対処】

- 管理者ID/PWを変更。
- HPで顧客情報漏えいについてお詫びと注意喚起。

【４　原因】

① 導入時からセキュリティ対策等の評価や見直しを行っていない。
② 管理者ID/PWの管理が徹底されていない。
③ 外部のIPアドレスからのアクセスを制限していない。
④ ログを適切に取得していない。

【５　再発防止策】

① 定期的にシステムの安全性を評価・改善するため、情報セキュリティ委員会（社長が委員長）を設置。
② 社内システム全てのID/PWを変更し、ID管理規程を整備し、PW変更管理を徹底。
③ 管理サーバへのアクセスを事業者のIPアドレスに制限。
④ ログ管理に関する規程を定め、ログを適切に取得。

【６　得られた気付き・教訓】

- **不正アクセスの未然防止**

① システム導入時から情報セキュリティ対策等の評価や見直しを行っていないことから、環境変化に伴う継続的な評価・改善を経営者主導で、全社的に取り組むことが重要。

② ID/PWの漏えいにより不正アクセスされたことから、ID/PWの変更を定期的に行い、漏えい防止の対策を講じるなど、適切に管理することが重要。

③ 外部から不正アクセスされたことから、外部のIPアドレスからのアクセスを制限することが重要。

- **不正アクセスの早期検知**

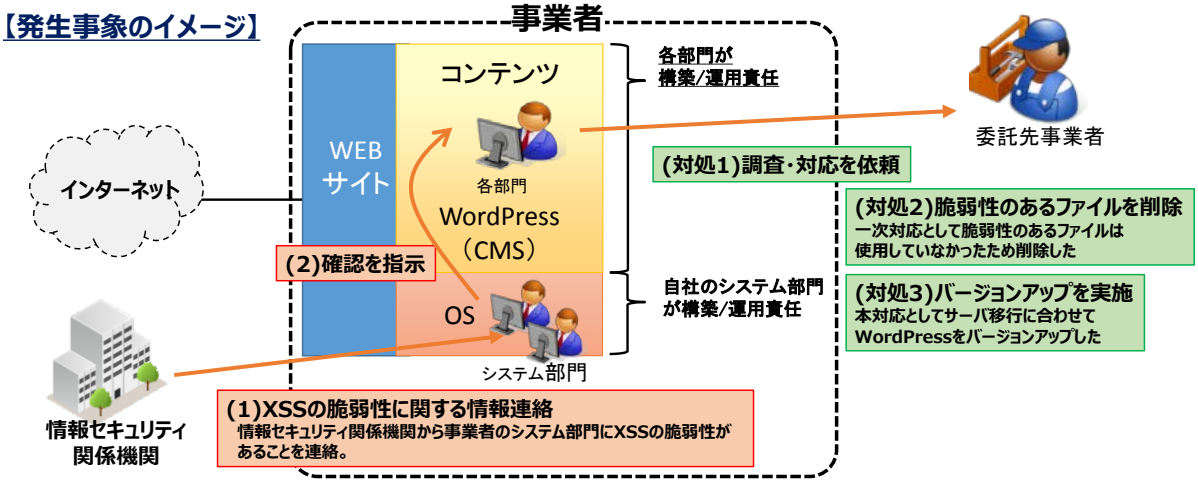
不正アクセスに気付くのに時間を要したことから、ログの取得を委託先との契約で明確化し、早期に検知することが重要。

事例５　ソフトウェアの継続的なセキュリティ対策（1/2）

【事例の概要】

- WordPressにXSS(クロスサイトスクリプティング)の脆弱性が発見され、セキュリティアップデートが公式HPにおいて公開された。
- 該当Webサイトはメンテナンス契約などを結んでおらず、担当者が脆弱性に気づかないままだった。
- 情報セキュリティ関係機関から、XSSの脆弱性に関する連絡を受け、委託先事業者に調査・対応を依頼した。

【発生事象のイメージ】



【１　背景】

- 自部門のプロジェクトに関するWebサイトの構築を外部に委託し、システム部門が運用する共用サーバに配置した。
- 共用サーバにおけるOSのセキュリティ対策は、自社のシステム部門で一括して行われるが、CMS(コンテンツマネジメントシステム)等のセキュリティ対策は、各部門において管理する運用となっている。
- 該当WebサイトはCMS(コンテンツマネジメントシステム)のWordPressを用いて構築している。

【２　検知】

- 情報セキュリティ関係機関からWebサイトにXSSの脆弱性がある旨、システム部門に情報連絡があった。
- WordPressに関する脆弱性であり、セキュリティアップデートが10カ月前にリリースされていた。
- 調査の結果、脆弱性を利用したサイバー攻撃を受けた形跡はなかった。

【３　対処】

- 委託先事業者に連絡し、調査・対応を依頼した。
- 一次対応：脆弱性のあるファイルは、当該Webサイトでは使用していなかったため、削除した。
- 本対応：サーバ移行にあわせて、WordPressを最新のセキュリティアップデートにバージョンアップした。

【４　原因】

- 継続的に脆弱性情報をチェックする体制が定められておらず、該当Webサイトが脆弱性のある状態で放置されてしまった。

当時の体制

委託先事業者	･･･Webサイト構築までの契約(保守契約等なし)
自社システム部門	･･･共用サーバのOSのセキュリティ対策
各部門	･･･CMS等のセキュリティ対策

※各部門は当時セキュリティアップデートを確認しなければいけない認識がなかった

【５　再発防止策】

＜短期的対策＞

- 担当部門がWebサイトに関する定期的な脆弱性に関する情報を収集することとした。
- 保守契約があり、保守期間が残っているWebサイトについて、委託先事業者と脆弱性対応に関する取決めの確認を実施した。

＜中長期的対策＞

- システム部門にて、運用保守契約の中に、定型的に盛り込むべき継続的な脆弱性対応に関する項目を検討している。

事例５　ソフトウェアの継続的なセキュリティ対策（2/2）

【６　得られた気付き・教訓】

- **各部門の役割の明確化**

① 「システム部門」と「各部門」それぞれが実施するセキュリティ対策の明確化

Webサイトの運用について、複数の部門が関係する組織体制の場合、どのような運用をする必要があるか留意点をまとめた社内共通の規程があると良い。

② メンテナンス契約の必要性

各部門に専門的な知識を持つ人が少なく、日常的にセキュリティに関する情報収集が難しい場合は、メンテナンス契約などにより運用を委託する方法もある。

- **脆弱性に関する情報収集の必要性**

① WordPressをはじめとするCMSソフトについても、オフィスのPCで使用しているソフトと同様に脆弱性の情報収集やセキュリティアップデートが必要

サーバで使用するソフトについても、脆弱性が発見され、修正プログラムが配布される。契約によっては、バージョンアップなどを行う場合は有償になるケースもある。

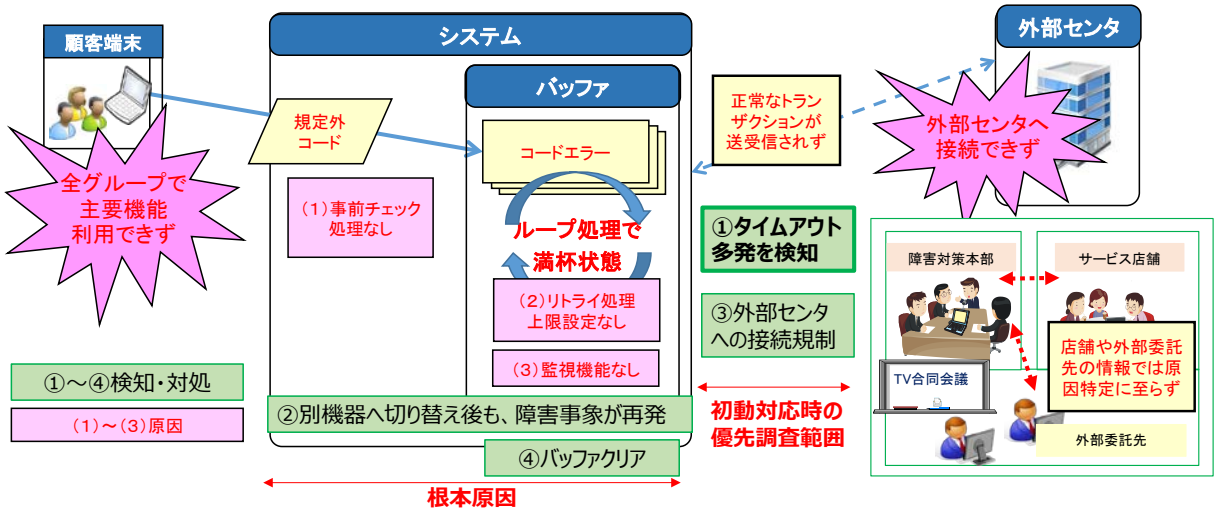
② 定期的な情報収集

情報収集先として、該当ソフトウェアの公式ホームページ、IPA、JPCERT/CC、NISCからのニュースレター等がある。事業者によっては、ISACやセプターに加入している場合があり、そこから得られる情報も有効である。

事例６　システムの不具合によるサービス障害

【事例の概要】

- 顧客が、端末にデータに異常があるカードを挿して操作を行ったところ、全グループ会社において、端末で他社との取引ができなくなった（複数の外部センタ間の接続も不可）。
- 過去に例のない障害のため、障害範囲の切り分けに手間取り、原因究明や復旧に時間を要した。
- 障害原因となったプログラムを改修。他の類似ロジックの総点検を実施した。
- システム監視設計強化、組織間情報共有の円滑化、想定外事態への対処を迅速化する対策を講じた。



【１　背景】

- グループ会社とともにシステム運用を外部委託（システムは複数の外部センタと接続してサービスを提供）。
- 機器の切り替えなどのシステム障害対応訓練を、外部委託ベンダやグループ会社と定期的に実施。
- カードの不良によって、偶発的に、端末から規定外コードがシステムに送信。

【２　検知】

- システムと外部センタとの連携を要する特定の処理でタイムアウトを検知。
- 外部委託先から全グループ会社に自動通報。

【３　対処】

- 店舗や外部委託先のサービス影響情報では原因特定に至らず、タイムアウト多発したことを受け、過去障害事例を参考にネットワークの障害状況を確認・解析。
- 機器の切り替えや外部センタとの接続規制を実施するも同事象が再発。
- 共通バッファ領域※が枯渇していることを究明し、該当機器の再立ち上げ（バッファクリア）を実施し、復旧。

※バッファ領域は、外部センタとの共通バッファ領域であったため、関連する全ての外部センタで障害が発生。

【４　原因】

- 特定業務においてカードの事前チェック処理が一部漏れており、規定外コードがシステムに送信され、特定の処理が異常終了。
- 規定外コードのエラー処理がループ化されており、共通バッファ領域が枯渇し、当該領域を使用する処理にも影響が波及。
- バッファ領域の異常をリアルタイムに検知する仕組の不備。

【５　再発防止策】

- エラー処理ロジックの適正化（事前チェック処理の実装、リトライ処理の上限設定など）
- その他の業務に関連する類似ロジックの総点検を実施
- 現状把握・対処の迅速化に向けた手順の見直し及びマニュアル・ツール類の整備。
- 早期検知を可能とする監視設計の見直し（バッファ領域の状態の常時監視など）

【６　得られた気付き・教訓】

早期復旧体制の整備

① 重要リソースの異常をリアルタイムに検知していなかったことから、システム監視設計を強化し、障害を未然に防止することが重要。

② 想定外事態への原因究明に時間を要したことから、業務部門や外部委託先との間で、情報共有の更なる円滑化が重要。

③ 機器の切り替えでは復旧できなかったことから、想定外の事態を前提とした関係組織全てを巻き込んだ訓練が重要。

（本ページは白紙です。）

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。
	ARF	ASEAN Regional Forumの略。政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラム。
	ASEAN	Association of South East Asian Nationsの略。東南アジア諸国連合。
B	BCP	Business Continuity Planの略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCPのうち情報（通信）システムについて記載を詳細化したものがIT-BCP（ICT-BCP）である。
C	C4TAP	Ceptoar Council's Capability for Cyber Targeted Attack Protectionの略（シータップ）。セプターカウンシルにおける標的型攻撃に関する情報共有体制。重要インフラサービスへの攻撃の未然防止、もしくは被害低減、サービスの維持、早期復旧を容易にすることを目的として、2012年12月に運用を開始した。
	CC	Common Criteriaの略。ISO/IEC 15408のこと。情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
	CCRA	Common Criteria Recognition Arrangementの略。CCに基づいたセキュリティ評価・認証の相互承認に関する協定。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005年以降順次構築が進められ、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。
	Common Criteria	CCを参照。
	cPP	Collaborative Protection Profileの略。CCRAにおいて各国の政府調達に用いるPPとして承認されたもの。
	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	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。
	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。
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。
	ECサイト	ECはElectronic Commerce（電子商取引）の略。商品やサービスをインターネット上のWebサイトで販売するサイトのこと。
F	FA機器	FAはFactory Automationの略。コンピュータ制御技術を用いて工場を自動化するために使われる機器のこと。
	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	G8	Group of Eightの略。主要８か国首脳会議。
	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。政府機関に設置したセンサー（GSOC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。
H	HEMS	Home Energy Management Systemの略。家庭で使うエネルギーを管理するシステム。
	HIDA	The Overseas Human Resources and Industry Development Associationの略。一般財団法人海外産業人材育成協会。
	HTTP GETリクエスト	インターネット上でウェブサーバーとクライアントが相互に通信するための仕組みにおいて、指定したURLアドレスからファイルの送信を要求するリスクエスト。
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。
	ISO/IEC 15408	CC（Common Criteria）を参照。
	ISP	Internet Service Providerの略。インターネット接続事業者。
	ITPEC	IT Professionals Examination Councilの略。アジア統一共通試験実施委員会。我が国の情報処理技術者試験制度を移入して試験制度を創設した国（６カ国）が協力して試験を実施するための協議会。
	ITU	International Telecommunication Unionの略。国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-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。
	IWWN	International Watch and Warning Networkの略。2004年に、米国・ドイツの主導により創設された会合で、サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組の促進を目的としている。先進15ヶ国の政府機関が参加している。
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。
	JIPDEC	Japan Institute for Promotion of Digital Economy and Communityの略。一般財団法人日本情報経済社会推進協会。電子情報を高度かつ安全安心に利活用するための基盤整備や諸課題の解決を通じて情報経済社会の推進を図り、もって我が国の国民生活の向上及び経済社会の発展に寄与することを目的とする。
	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。我が国において各国関係機関と連携して、サイバー攻撃情報やシステムの脆弱性関連情報等を収集・分析し、関係機関に情報提供するとともに、サイバー攻撃発生時には、関係者間の連絡調整や、攻撃の脅威分析、対策の検討に関する支援活動等を実施している機関。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。
	Meridian	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。欧米諸国やアジア各国等の政府機関（重要インフラ防護担当）が参加し、ベストプラクティスの交換や国際連携の方策などについて議論している。
	MOU/NDA	Memorandum Of Understanding/Non-Disclosure Agreementの略。覚書及び秘密保持契約。
	MyJVN	JVN iPedia 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。
	NIRVANA改	NICTが開発したネットワークリアルタイム可視化システムNIRVANA（NIcter Real-network Visual ANAlyzer）を改良し、組織内ネットワークにおける通信状況とサイバー攻撃の警告とを、総合的かつ視覚的に分析可能なプラットフォーム。
	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。

	ORiN協議会	Open Resource interface for the Network協議会の略。異なるアーキテクチャの産業機器を相互に接続する技術であるORiNの普及、維持・発展を目的とした協議会。
	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	SBD	Security By Designの略。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。
	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。
	SEC	Securities and Exchange Commissionの略。米国証券取引委員会。
	SECCON CTF2016	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。
	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。
V	VR/AR	Virtual Reality（仮想現実）/Augmented Reality（拡張現実）の略。VRはコンピュータ上に人工的な環境を作り出し、あたかもそこにいるような感覚を体験できる技術、ARは現実空間に付加情報を表示させ、現実世界を拡張する技術のこと。
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 JTC 1）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 JTC 1/SC 27）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 JTC 1/SC27のワーキンググループ3（WG3：セキュリティ評価基準）の副コンビーナ（副議長）を務めている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	暗号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。
	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	経済産業省において、2011年４月策定、2014年３月改訂。経済産業省が策定した、クラウドサービス利用者及び事業者が対処すべきセキュリティマネジメントのガイドライン。
	クラウドセキュリティガイドライン活用ガイドブック	経済産業省において、2014年３月に、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」改訂版と併せて公表した、同ガイドラインの解説書。
こ	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	最高情報セキュリティアドバイザー等連絡会議	サイバーセキュリティ対策推進会議（CISO等連絡会議）に対して、専門的な見地から審議、検討、助言等を行い、各府省庁における知識・経験の共有を図ることを目的とした有識者で構成される会議。
	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	2013年４月、サイバー攻撃対策の強化のため、13都道府県警察に設置された。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）	2015年５月25日サイバーセキュリティ戦略本部決定。安全基準等（国・業界団体・各事業者等が定める各種の基準やガイドライン）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。同時に、同文書を補完するものとして、同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の２つの文書が策定されている。
	重要インフラの情報セキュリティ対策に係る第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。
	情報セキュリティ人材育成プログラム	政府や公的研究機関等での研究開発を推進するとともに、大学や企業等においても産学官の連携の下で推進し、情報セキュリティ研究開発の総合力を高めることを目的として定められた。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・情報セキュリティ人材育成プログラムは2014年５月19日情報セキュリティ政策会議決定。
	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	スクリプト	コンピュータプログラムの種類の一つ。コンピュータが解釈できる機械語への変換や実行可能なファイルの作成などの過程を省略または自動化し、ソースコードを記述したら即座に実行できるようなプログラムのこと。
	ステークホルダー	利害関係者のこと。
	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的。
	スマートメーター	通信機能を有し、遠隔での検針等を行うことが可能となる新しい電力量計。
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。
	脆弱性関連情報届出受付に係る制度	2004年７月、経済産業省が「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）を公示し、脆弱性関連情報の届出の受付機関としてIPA、脆弱性関連情報に関して製品開発者への連絡及び公表に係る調整機関としてJPCERT/CCが指定されている。
	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。
	セキュリティ・バイ・デザイン	SBD（Security By Design）を参照。
	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）。
	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。
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）
	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）
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。
	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。この攻撃では、標的の組織がよくやり取りをする形式や内容の電子メールを送りつけ、その電子メールの添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する手口がよく使われている。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。
	標的型メール	標的型攻撃を参照。
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。
	フィルタリング	インターネットのウェブページ等を一定の基準で評価判別し、違法・有害なウェブページ等の選択的な排除等を行う機能のこと。
	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	ポータルサイト	インターネットにアクセスする際の入口となるウェブサイト。
	ポート	ポート番号。コンピュータが通信する際に通信先のプログラムを識別するための番号で、通常利用されるTCP/IPでは、65535番までである。通常、プロトコルに応じてポートが割り当てられている。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。
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。）