資料１

サイバーセキュリティ政策に係る年次報告（2015 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（2015 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（2015 年度）（案）

サイバーセキュリティ政策に係る年次報告(2015年度)(案)の概要

資料１－１

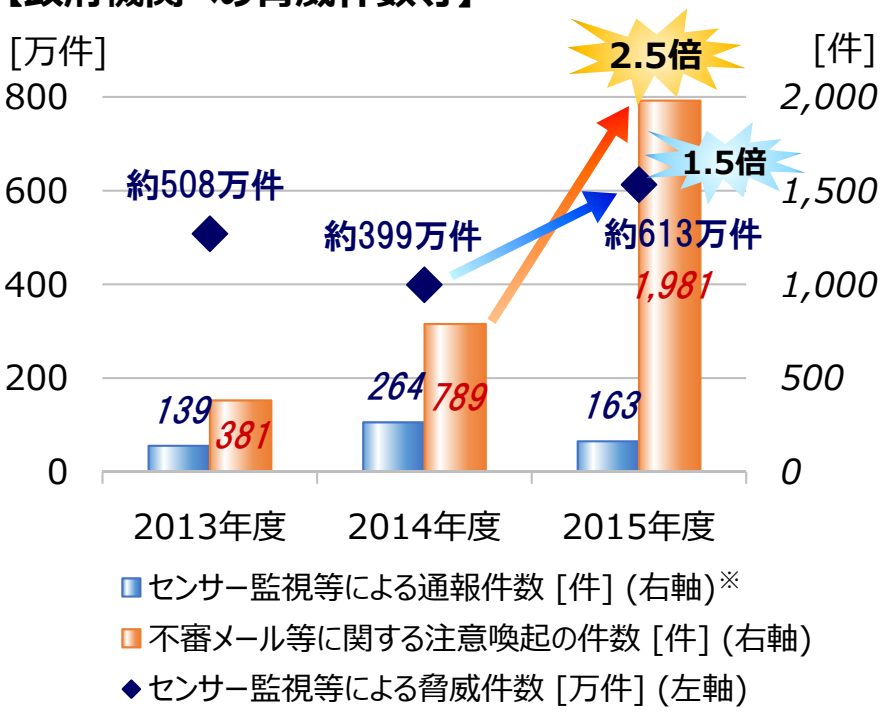
本年次報告の位置付け

- 「サイバーセキュリティ戦略」（2015年9月4日閣議決定）に基づく最初の年次報告。
- 2015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

- 日本年金機構において、**標的型メール攻撃によって大量の個人情報が流出する国内初の事案が発生**（2015年５月）。
- 当該事案等を踏まえ、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）。

【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、当該政府機関へ通報した件数。

【外部からの攻撃に係る2015年度の特徴】

上半期には標的型メール攻撃が頻発し、下半期には政府機関のWebサイトを閲覧困難にする攻撃が頻発。脅威件数は前年度よりも増加しており、脅威は一層深刻化。

- センサー監視等による**脅威件数は約613万件**となり、**前年度比で約1.5倍**。約５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前年度から減少（163件）。また、標的型メールに関する通報件数が全体に占める割合は３割程度に減少。
- 不審メール等の**注意喚起件数**は**前年度比約2.5倍**に増加（1,981件）。

【2015年度の主なサイバー攻撃事案】

2015.6	［日本年金機構］ パソコンがウイルスに感染、約125万件の情報流出を公表。
	［法務省］ パソコンがウイルスに感染した疑いがあると公表。
2015.7	［環境省］ パソコンがウイルスに感染した疑いがあると公表。
	［厚生労働省］ ハローワークのパソコンがウイルスに感染したと公表。
2015.11	［厚生労働省］ ホームページが閲覧困難。
2016.2	［金融庁、国税庁］ ホームページが閲覧困難。

サイバーセキュリティ政策に係る年次報告(2015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

- 2015年10月に設立された「IoT推進コンソーシアム」において、2016年１月に**「IoTセキュリティワーキンググループ」を設置**。IoT機器等の設計・製造・ネットワークへの接続等に係るセキュリティガイドラインについて検討、2016年６月を目途に公表予定。
- セキュリティマインドを持った企業経営の浸透を目的として、**「サイバーセキュリティ経営ガイドライン」を2015年12月に公表**。
- サイバーセキュリティ対策の研究開発に取り組む企業への出資。

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」（2016年２月１日～３月18日）のキックオフイベントとして、**「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**「攻殻機動隊S.A.C.」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！秋葉原0305」を開催**。
- セキュリティ対策の基本的な知識を学べる**「情報セキュリティハンドブック」を作成**。
- **「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」を決定**。
- 「政府機関の情報セキュリティ対策のための統一基準群」の改定案について検討。2016年夏頃の決定を目指して改定作業中。
- 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 2016」**、政府機関、重要インフラ事業者等の対処能力向上のための**実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）等を継続実施**。
- 監査制度の設計及び当該制度の有効性の検証を目的とした**試行的な監査を10府省庁に対して実施**。

サイバー攻撃を目撃せよ！秋葉原0305

情報セキュリティハンドブック

サイバーセキュリティ政策に係る年次報告(2015年度)(案)の概要

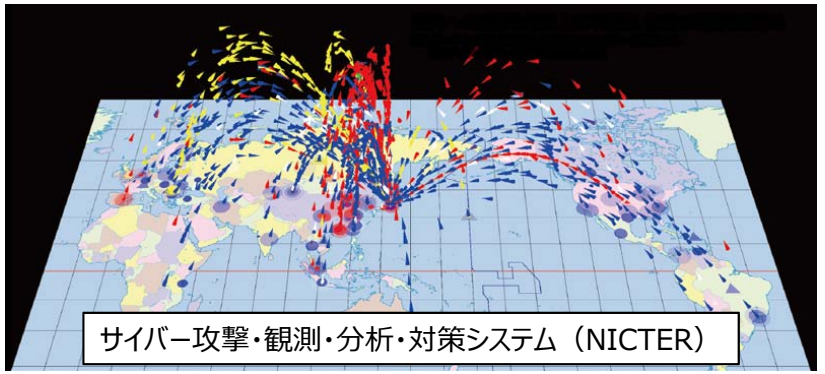
主な政策の取組実績

3．国際社会の平和・安定及び我が国の安全保障


日・ASEAN情報セキュリティ政策会議

- 2015年4月、日米両国政府によるサイバー空間の安全かつ安定的な利用の確保に資するための協力を含む**新たな「日米防衛協力のための指針」に合意**。
- 首脳・閣僚のハイレベル国際協議や国連政府専門家会合、法執行機関間の連携強化により、**サイバー空間における法の支配の確立に積極的に寄与**。
- **国際サイバー演習の主催や積極的な参加**を通じ、重大な情報セキュリティ事案発生時における国外関係機関との連絡体制の整備を推進。
- 多国間や二国間の国際会議を通じ、**我が国のサイバーセキュリティ関係施策や考え方等を積極的に発信・連携を具体化**。

4．横断的施策


サイバー攻撃・観測・分析・対策システム（NICTER）

- 人材育成に係る施策を総合的かつ強力に推進するための方針である**「サイバーセキュリティ人材育成総合強化方針」を2016年３月に決定**。
- 国家試験である**「情報処理技術者試験」に新たな試験を追加**したほか、企業等のセキュリティ対策を担う専門人材の国家資格として、新たに「情報処理安全確保支援士」の創設に係る取組を推進中。
- 国立研究開発法人情報通信研究機構（NICT）を通じて、サイバーセキュリティ研究の一環として、**「サイバー攻撃・観測・分析・対策システム（NICTER）」を活用し、IoT機器を標的としたサイバー攻撃を観測**。
- 戦略的イノベーション創造プログラム（SIP）に**「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加**し、府省庁の枠や旧来の分野の枠を超えた研究開発を推進中。

サイバーセキュリティ政策に係る年次報告(2015年度)(案)の概要

主な政策の取組実績

5．推進体制

- **国による監視、監査、原因究明調査の対象**を、**独立行政法人、サイバーセキュリティ戦略本部が指定する特殊法人・認可法人に拡大**し、戦略本部の事務の一部をIPAに委託することを主な内容とする「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案」を2016年２月２日に閣議決定、第190回国会に提出した。
  同法案は2016年４月15日に成立し、同月22日に公布。
- 各府省庁において最高情報セキュリティ責任者（CISO）・情報化統括責任者（CIO）の補佐等を行う**「サイバーセキュリティ・情報化審議官」等を新設**。
- 2016年のG7伊勢志摩サミット、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、継続的なリスク評価を実施。
  2019年ラグビーワールドカップ開催時においてオリンピック・パラリンピックCSIRT（Computer Security Incident Response Team）の稼働を目指し、関係者間の調整を実施。
- **サイバーセキュリティに係る演習の質的向上や継続的・安定的な運用に向け、NICTを演習の実施主体とする**ための「国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律案」を2016年３月１日に閣議決定し、第190回国会に提出。2016年４月20日に成立、５月31日に施行。


G7伊勢志摩サミット　第２セッション


G7伊勢志摩サミット　議長記者会見

資料１－２

サイバーセキュリティ政策に係る年次報告
（2015年度）（案）

2016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。

内閣官房内閣サイバーセキュリティセンター

ホームページ： http://www.nisc.go.jp/

Twitter：@cas_nisc、https://twitter.com/cas_nisc

Facebook： https://facebook.com/nisc.jp

＜目次＞

はじめに

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、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。その一方、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が見られる状況にあり、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・巧妙化し、攻撃対象も拡大し続けている。このため、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・危機管理の観点から極めて重要な課題となっている。

こうした中、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１月に全面施行されたサイバーセキュリティ基本法の規定に基づき、サイバーセキュリティ政策に関する新たな国家戦略である「サイバーセキュリティ戦略」（以下「戦略」という。）を2015年９月４日に閣議決定した。戦略は2020年代初頭までの将来を見据えつつ、サイバーセキュリティ政策の基本的な方向性を示したものであり、政府としては、戦略に基づく最初の年次計画「サイバーセキュリティ2015」に具体的な施策を示し、これを推進してきたところである。

本報告は、2015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2015」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、2015年度において特記すべき点としては、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等を受けて、政府や民間企業等の意識が大きく変化したことが挙げられる。政府においては、同事案を踏まえサイバーセキュリティ基本法を改正し、不正な通信の監視や監査等の対象を独立行政法人等へ拡大するための準備を進めるとともに、各府省庁におけるサイバーセキュリティ対策を指揮監督する「サイバーセキュリティ・情報化審議官」等を設置するなど、対策の更なる強化が進められている。また、民間企業等においても、サイバー攻撃を受けた場合の初動対応の体制整備や、関係機関における情報共有体制の整備が加速している。

一方、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、今後更なる対策の強化が求められている。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、本編記載のサイバーセキュリティ関連施策の評価結果等を踏まえ、サイバーセキュリティ政策に対して継続的な改善を施すとともに、これを着実に推進することとする。

Ⅰ　2015 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) 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の発生

サイバーセキュリティは、安全保障・危機管理の上からも、また、我が国経済の成長を促進する上からも、必要不可欠であることから、政府は、2014年11月に成立したサイバーセキュリティ基本法に基づき、新たな国家戦略である「サイバーセキュリティ戦略[1]」（以下「戦略」という。）の閣議決定に向けて作業を進めていた。その過程の最中、2015年６月１日、日本年金機構（以下「機構」という。）において、職員の端末に対する外部からの不正プログラムが添付されたメールによる不正アクセスにより、機構が保有している個人情報の一部である約125万件が外部に流出したことが公表された（Ⅰ－２－(3)参照）。

我が国では、2011年の衆議院事務局、重工業等に対するサイバー攻撃に端を発して、特定の政府機関、企業を狙ったいわゆる標的型攻撃が広く社会的に課題として認識された。その後も事案について公表されるケースは年々増加傾向にあり、こうした状況の中、今般の機構における事案は、サイバー攻撃による個人情報の大量流出が国内において現実に確認された初めてのものとなった。

本事案について、同年８月20日、サイバーセキュリティ戦略本部（以下「戦略本部」という。）は、「日本年金機構における個人情報流出事案に関する原因究明調査結果」[2]を公表したが、この原因究明調査で明らかとなったことは、不正プログラム感染後、数時間以内に複数の端末から不審な通信が発生しており、攻撃成功後、数日で情報が流出したことである。一般的に、標的型攻撃については、先端技術等の機微な情報の窃取等をもくろみ長期間の潜伏期間を経て情報が流出すると言われていたが、こうした前提が通用しない攻撃への対応が求められるという課題が明確に認識された。

本事案で大量の個人情報が流出する要因となった不正プログラムの亜種は、その当時、機構以外の政府関係機関に対する「標的型攻撃」においても使用されており、本事案発生後も、政府関係機関や国立大学を標的としたサイバー攻撃は続いた。その手口としては、一般によく見られる圧縮した不正プログラムをメールに添付して送付するもののほか、閲覧すると感染するウェブサイトへのリンクをメールに貼り付けて送付するものなども見られている。

一般社団法人JPCERTコーディネーションセンターの資料等[3]によると、類似の標的型攻撃は2012年頃から国内の多数の組織において観測されていた。そして、2014年秋頃からは、本事案と同様の偽装方法を用いた不正プログラムの添付等をした標的型攻撃が増加していたと報告されており、標的となった対象組織で一旦不正プログラムが動作すると、国内外の複数のサイトとの間で通信を行うものとなっていた。

---

[1] サイバーセキュリティ戦略（http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf）

[2] 日本年金機構における個人情報流出事案に関する原因究明調査結果（http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf）

[3] 日本の組織をターゲットにした攻撃キャンペーンの詳細（https://www.jpcert.or.jp/present/2015/20151028_codeblue_ja.pdf）
標的型への対応-JPCERT/CC-（https://www.jpcert.or.jp/present/2015/JNSAWG20150625-apt.pdf）

なお、ほぼ同時期の2015年６月４日には、米国連邦政府人事管理局（OPM[4]）において、システムへの不正アクセスにより、約420万人分もの大量の個人情報が流出したことが公表[5]（同年７月９日には、調査の結果、流出した個人情報が約2,150万人分であったことが追加公表[6]）されており、国内外において個人情報が標的となっていることが明らかとなった。

(2) 政府機関、重要インフラ等におけるサイバーセキュリティ上の脅威

国民が安全・安心に暮らせる社会を実現するためには、政府機関や重要インフラ事業者等が機能及びサービスの持続的な提供を行い、かつ障害の発生減少、早期検知及び障害発生時の迅速な対応・復旧が求められる。

2015年度における我が国の当該分野におけるサイバーセキュリティの状況を概観すると、上半期は日本年金機構を含め我が国政府機関等への標的型攻撃が多く確認された。一方、下半期には、政府機関、重要インフラ事業者等へのDDoS[7]攻撃が多数みられ、Webサイトの閲覧障害が相次いだ。また、インターネットバンキングに係る不正送金についても、被害額がますます悪化している。

国外の事例をみると、重要インフラに関しては、2015年４月にフランスの国際放送局に対するサイバー攻撃によって番組の視聴障害が発生している。また、2015年12月にはウクライナにおいてサイバー攻撃に起因する大規模停電が発生[8]、2016年１月にはイスラエルの電力公社において、電力供給への影響はなかったものの、サイバー攻撃を受けたと報道される[9]など、重要インフラ等に対するサイバー攻撃に顕著なものがみられる。特に、ウクライナにおける停電事案については、米国国土安全保障省（DHS[10]）の調査によると、外部からの標的型攻撃が停電の原因としている旨報じられている[11]。攻撃者は、インターネットに接続されたコンピュータから制御系に入り込んで停電させるとともに、復旧を妨害するために顧客電話窓口の妨害、無停電電源装置の妨害といった極めて高度で執拗な攻撃を行ったとしている[12]。

また、下半期はランサムウェアについての被害が相次いでおり、国外では、病院等でランサムウェアに感染したことから、重要インフラサービスの提供に支障が生じた事例がみられた[13]。我が国においても、2016年２月以降、ランサムウェアの被害報告が増加傾向にあり、注意喚起がなされている[14]。

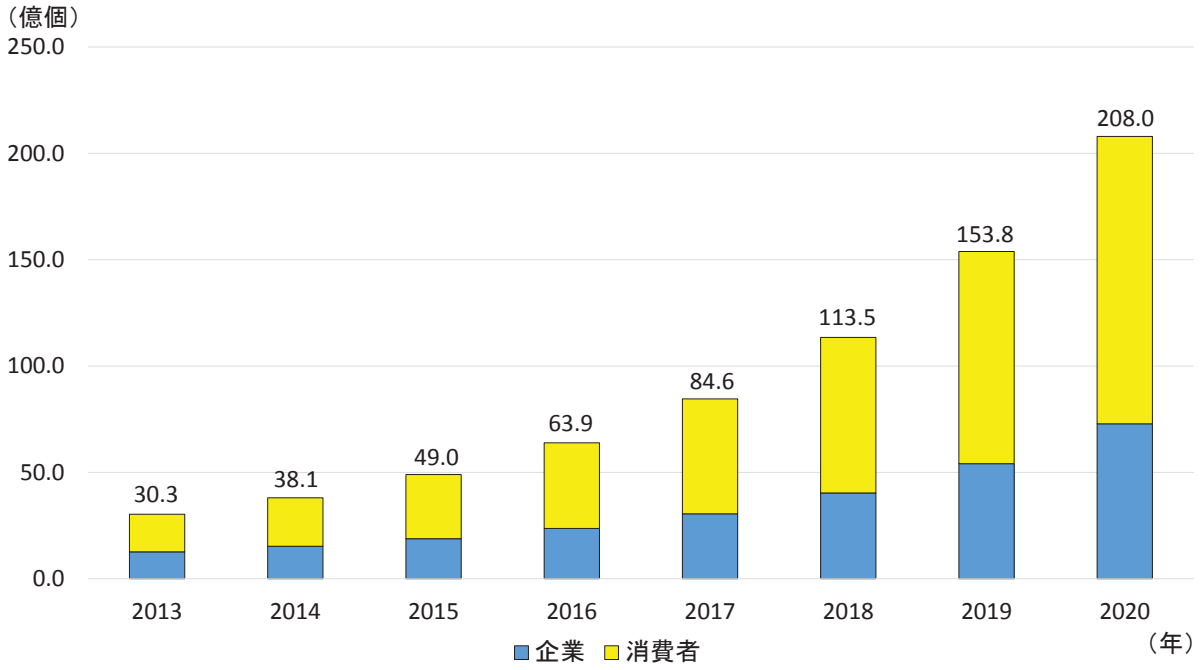
---

[4] Office of Personnel Management
[5] Announcements “Information About the Recent Cybersecurity Incident”, June 4, 2015, (http://www.opm.gov/news/latest-news/announcements/)
[6] https://www.opm.gov/cybersecurity/cybersecurity-incidents/
[7] Destributed Denial of Service（「別添５　用語解説」参照）
[8] Ukraine to probe suspected Russian cyber attack on grid (http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231)、ウクライナ電力供給会社発表（http://www.koe.vsei.ua/koe/index.php?page=50&novost=208)、(http://oe.if.ua/showarticle.php?id=3413)
[9] Israel’s Power Grid Hit with Ransomware (http://news.softpedia.com/news/israel-s-power-grid-targeted-by-ransomware-499488.shtml)
[10] Department of Homeland Security
[11] U.S. government concludes cyber attack caused Ukraine power outage (http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K)
[12] https://www.rsaconference.com/writable/presentations/file_upload/exp-t09r_the_seven_most_dangerous_new_attack_techniques-final2.pdf
[13] Hollywood Presbyterian Medical Center (http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf)
[14] 【注意喚起】ランサムウェア感染を狙った攻撃に注意（https://www.ipa.go.jp/security/topics/alert280413.html)

(3) IoT の普及とセキュリティ対策の重要性の認識

企業の調査によると、世界におけるIoT[15]デバイスの数は、2020年で約200億個以上に達するとされている（図表Ⅰ－1－1）。我が国においては、2020年までに、市場ニーズに応える安全なIoTシステムを実現し、経済社会への影響が大きな事業について、官民が連携し、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ている。

図表Ⅰ－1－1　IoT デバイス数の 2020 年までの予測[16]



他方で、国内においては、IoT機器の普及に伴い、IoT機器が攻撃の標的となることが懸念されるとして、2015年12月、警察庁が注意喚起を行っている[17]。警察庁によると、IoT機器を標的とした攻撃が観測されており、ルータやWebカメラ等のIoT機器が攻撃者に乗っ取られ、踏み台として悪用されていると考えられるとしている。

自動車分野においても同様にIoT化が進んでいる中、2015年７月には、米国の自動車会社がハッキング対策のため約140万台の自動車をリコールしたとの報道[18]もあり、自動車のセキュリティにも注目が集まっている。このように、様々なモノがインターネットにつながるようになったことで、セキュリティ対策の重要性がますます認識されるようになっている。

[15] Internet of Things（「別添５　用語解説」参照）
[16] 図表はガートナー・リサーチに基づき NISC が作成。Gartner “Forecast: Internet of Things- Endpoints and Associated Services, Worldwid, 2015” 29 October 2015
[17] IoT 機器を標的とした攻撃の観測について（https://www.npa.go.jp/cyberpolice/topics/?seq=17323）
[18] Chrysler Recalls 1.4 Million Vehicles After Jeep Hacking Demo（http://www.darkreading.com/vulnerabilities---threats/chrysler-recalls-14-million-vehicles-after-jeep-hacking-demo-/d/d-id/1321463）

こうした状況を踏まえ、我が国では、安全なIoT環境の創出のため、内閣府の戦略的イノベーション創造プログラム（SIP）[19]や民間主導の「IoT推進コンソーシアム[20]」におけるIoTセキュリティガイドライン[21]の策定など各種対策が進められている。

(4) サイバー空間対策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。

加えて、注目すべき動きとして、2015年９月25日の米中首脳会談においては、商業的利得のために企業秘密や機密情報を含む知的財産を窃取しないことなどを内容とするサイバー空間における二国間合意がなされた[22]。その後、米国では、中国からの政府、防衛産業等へのサイバー攻撃は続いているといった見解[23]が示されている一方、同年12月１日にワシントンで開催された米中間のサイバー犯罪取締りの実務者会議の際、中国政府は、米国政府へのサイバー攻撃は中国政府が関与したものではなく、個人の犯罪行為であることを示し[24]、双方のサイバー犯罪取締りの協力などについて表明する[25]動きがみられた。

こうした情勢において、我が国では、「日米サイバー対話」や「インターネットエコノミーに関する日米政策協力対話」をはじめとする二国間協議のほか、国連政府専門家会合や「サイバー空間に関する国際会議」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。

---

[19] 戦略的イノベーション創造プログラム（http://www8.cao.go.jp/cstp/gaiyo/sip/）（Ⅱ-2-(4)-①参照）
[20] IoT推進コンソーシアム（http://www.iotac.jp/）
[21] IoTセキュリティガイドラインについて（http://www.iotac.jp/wp-content/uploads/2016/01/資料2_IoTセキュリティガイドラインについて.pdf）
[22] Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference（https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint）
[23] STATEMENT OF ADMIRAL MICHAEL S. ROGERS COMMANDER UNITED STATES CYBER COMMAND BEFORE THE SENATE ARMED SERVICES COMMITTEE（http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf）
[24] First China-U.S. cyber security ministerial dialogue yields positive outcomes（http://news.xinhuanet.com/english/2015-12/02/c_134874733.htm）
[25] http://news.xinhuanet.com/world/2015-12/04/c_128500279.htm

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

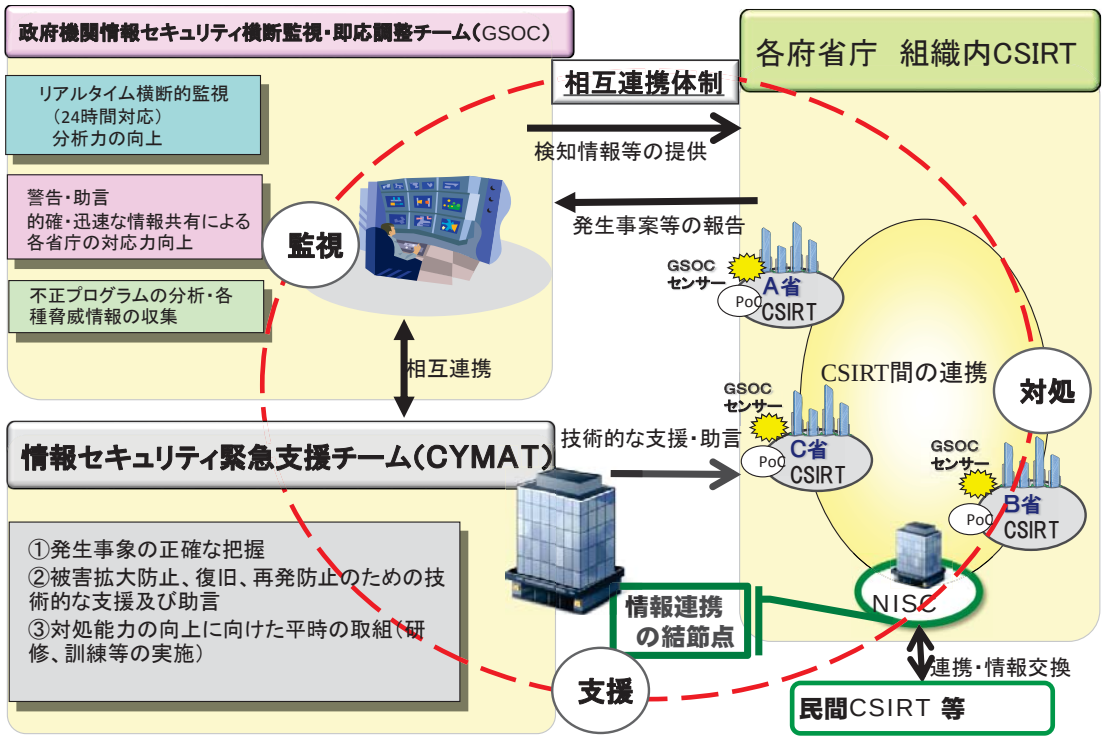
(1) 政府機関におけるサイバーセキュリティに関する体制

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・即応チーム（GSOC[26]）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[27]）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[28]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



[26] GSOC (Government Security Operetion Cordination team)
[27] CYMAT (CYber incident Mobile Assistance Team)
[28] CSIRT (Computer Security Incident Response Team)

(2) 2015 年度における政府機関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[29]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。

2015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、上半期は、2014年度から引き続き、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にみられるような外部からの攻撃、特に標的型攻撃が多く発生し、下半期には、政府機関のWebサイトを閲覧困難にするような攻撃が頻発した。

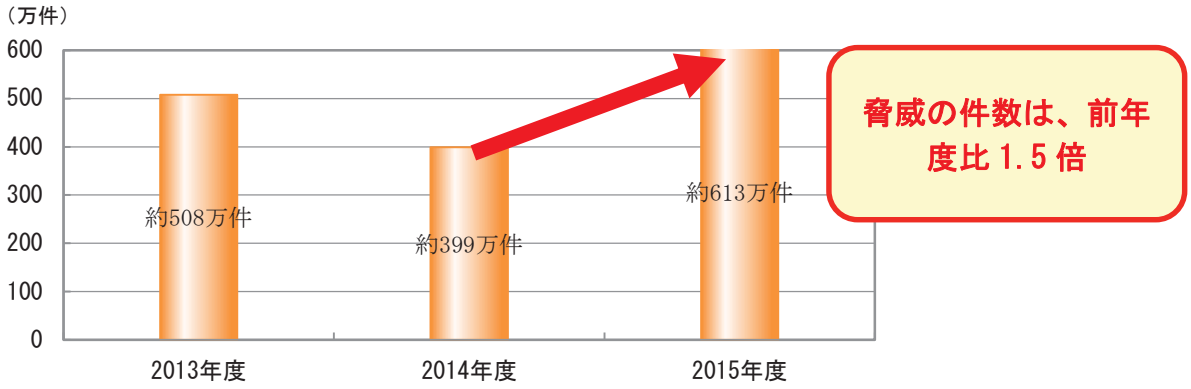
以下に、2015年度の政府機関等におけるサイバーセキュリティに関する情勢について、情報セキュリティインシデントの主な要因ごとにその傾向を示す。

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、2015年度に政府機関への脅威と認知された件数は、約613万件であった（図表Ⅰ-2-2）。これは、約５秒に１回、脅威を認知している計算となり、2014年度の約399万件と比較して、約1.5倍に増加している。2014年度は2013年度よりも脅威の認知件数が減少した[30]が、2015年度は、2014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



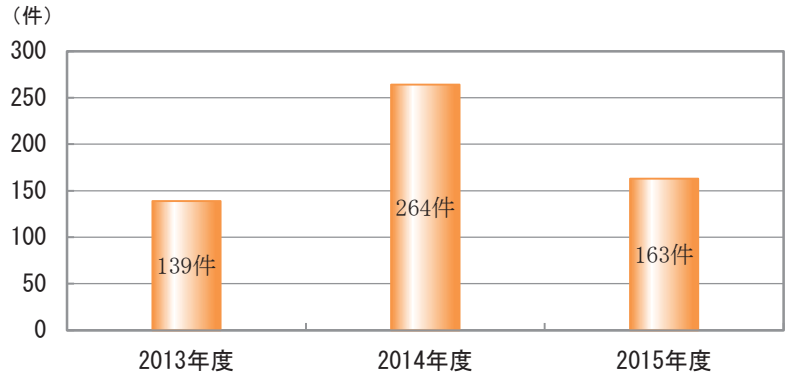
[29] 情報セキュリティに関する望まない又は予期しない事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（「別添５　用語解説」参照）。政府機関等において発生した情報セキュリティインシデントの一覧については「別添３－１１　政府機関等に係る 2015 年度の情報セキュリティインシデント一覧」を参照。

[30] GSOC システムの能力向上に伴って脅威の識別精度が向上したことにり、軽微なものを判別対象から除外したものを含む。

（イ）政府機関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への通報[31]を行っており、2015年度においては、163件の通報を行った（図表Ⅰ－２－３）。2014年度の264件と比較すると約2/3に減少しているが、これは、2015年５月の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に係る通報などを含んでおり、政府機関に深刻な被害をもたらし得る高い脅威となる攻撃が減少したことを示しているとは考えられない。こうした中、サイバーセキュリティ戦略本部は、2015年８月20日に公表した「日本年金機構における個人情報流出事案に関する原因究明調査結果」[32]において、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を踏まえ、早期に着手すべき政府機関における標的型攻撃に対する情報システムの防御策を示したところであり、政府機関による防御策の取組の結果、一定の効果が得られていると考えられる。

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、2014年度は標的型メールの検知[33]に関する通報件数が突出して多く[34]、まさに標的型メール攻撃の脅威が急速に高まった年であったが、2015年度は一転し、前年の半分以下の件数に減少し、通報件数全体の約３割であった。一方、不審な通信の検知[35]による通報件数は、依然高い割合を占めている状況に変化はみられず、2015年度は、全体の通報件数の約４割であった。

GSOCでは政府機関のWebサイト等を定期的に監視しているが、2015年10月以降、DDoS攻撃などによるWebサイトの閲覧障害に関する通報が急増した。2014年度には数件しかなかったWebサイトの閲覧障害に関する通報は、2015年度はその件数が約６倍に増加したが、そのうち約９割は2016年１月から２月に集中している。

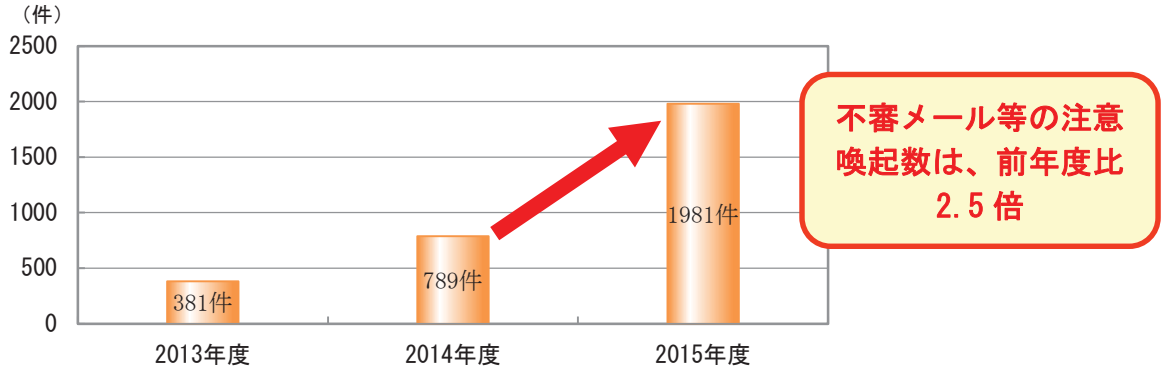
---

[31] 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。
[32] 日本年金機構における個人情報流出事案に関する原因究明調査結果　４．２ 標的型攻撃に対する情報システム防御策等の考え方（http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf）
[33] 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。
[34] 2014 年度は標的型メールの検知に関する通報が前年度の約３倍であった。
[35] 外部から政府機関に対する不正アクセスや政府機関内部から外部に対する不正な通信の検知。

このように、2014年度に急増した標的型メール検知に関する通報等が2015年度は減少したことから、全体の通報件数も減少したが、依然として政府機関に対する攻撃は続いている。

GSOCでは、政府機関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、政府機関に対して一斉に注意喚起を行うもので、2015年度においては、1,981件の注意喚起文書を発出した（図表Ⅰ－２－４）。

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、2014年度は2013年度の381件に対して789件と倍増したが、2015年度はさらに倍増し2,000件に迫る注意喚起を行った。これは、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を踏まえ、政府機関の防御能力を高めたことなどの結果として、不審メールや不正プログラムの検知能力が向上し、政府機関から提供される検体数が増加したため、それに応じてGSOCによる注意喚起数が増加したことが考えられる。また、2013年度以降の状況を見ると、検体提供数及び注意喚起の件数ともに年々伸びている状況から、以前にも増して政府機関に対し不審メールを送付するような攻撃は増加していると考えられる。

（ウ）ソフトウェアの脆弱性情報の傾向について

GSOCでは、Webサイト等への攻撃を始めとする各種のサイバー攻撃に悪用される可能性があるソフトウェアについての脆弱性対策情報等を政府機関等に配信し、注意喚起を実施している。2015年度においては、GSOCより99件の脆弱性情報等を配信した（図表Ⅰ－２－５）。

図表Ⅰ－２－５　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

	2013年度	2014年度	2015年度
脆弱性情報等の配信	78件	84件	99件

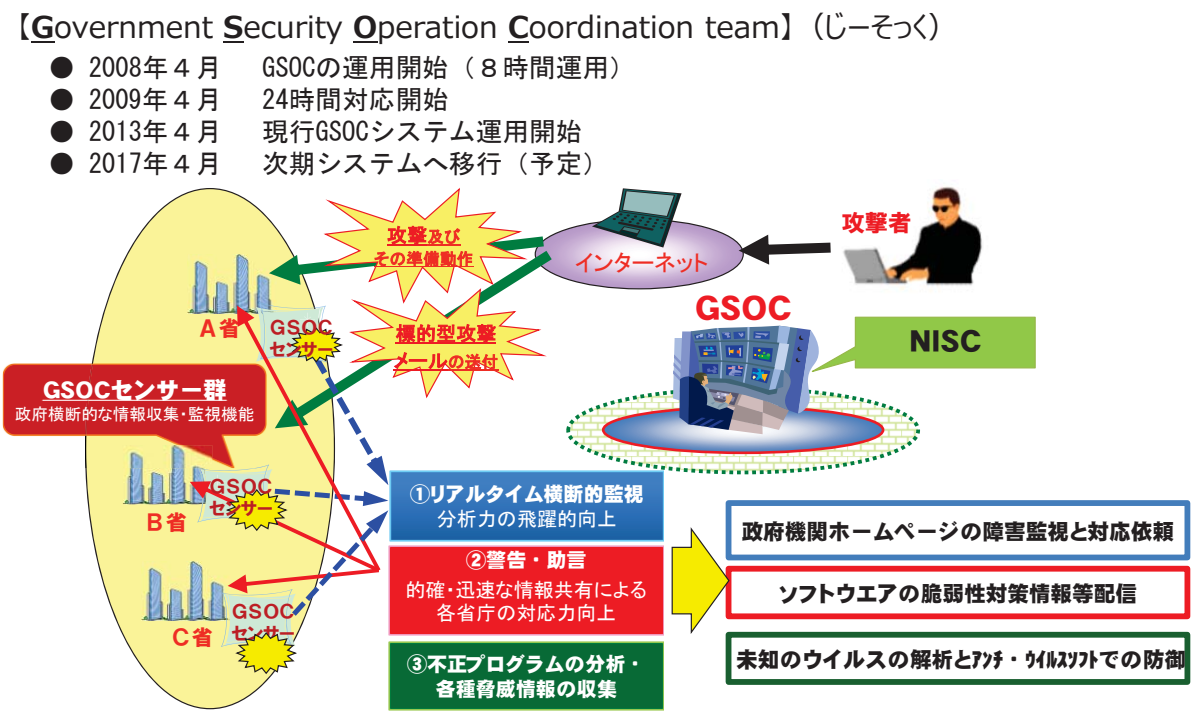
脆弱性を悪用した攻撃の代表的なものとしては、Webサイトの改ざんが挙げられる。GSOCにおける監視活動においても、Webサイトに対する脆弱性を悪用しようとする攻撃を検知しており、今後も対策の強化促進が必要である。

(エ)今後の対応

これまでに述べたとおり、GSOCセンサー等による監視活動による政府機関への通報件数は、標的型メール攻撃が猛威を振るった2014年度から減少したものの、脅威と認知した件数は2014年度の約399万件から約613万件と増加していること、政府機関から提供があった検体のうち、不正プログラムなどと確認され、注意喚起文書を発出した件数も、2014年度の789件から1,981件と急増したことを併せ考えると、依然として、政府機関に対する攻撃は深刻度を増している。

こうした状況を踏まえ、2017年４月の運用開始を目指す次期GSOCシステムにおいては、その検知・解析機能の強化、GSOCセンサーの増強等を図ることとしている。

図表Ⅰ－２－６　GSOC の概要



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

2015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。

従来から見られる記憶媒体の紛失のほかに、電子データを公開した際に、本来は不開示とすべき事項の処理が不十分で、一定の操作を行うことで黒塗り処理が外れる状態であったような事案が発生している。また、インターネットとつながる複合機やプリンタのセキュリティ対策がきちんととられず、機器内部のデータが外部から見えていた大学などが多数あることが判明し、政府機関においては既に取組が進められているところであるが、改めて注意喚起を行ったところである。

(3) 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の概要

2015年６月１日、日本年金機構（以下「機構」という。）は、外部から送付された不審メールに起因する不正アクセスにより、機構が保有している個人情報の一部（約125万件）が外部に流出したことが５月28日に判明したとして、報道発表を行った。

NISCにおいては、本件事案について、100万件を超える国民の個人情報が流出したことを踏まえ、国民生活に重大な影響を与える「特定重大事象」として政府を挙げて対応するようにとの官房長官（サイバーセキュリティ戦略本部長）からの指示を受け、客観的・専門的立場から事案の原因究明を実施するため、サイバーセキュリティ基本法第25条第１項第３号に規定された「国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）」に基づき、６月１日に原因究明調査チームを設置し、調査を行った。そして、サイバーセキュリティ戦略本部（以下「戦略本部」という。）は、同年８月20日、「日本年金機構における個人情報流出事案に関する原因究明調査結果」を決定し、公表した[36]。

その概要は次のとおりである。本事案は、攻撃者が機構に送付した不審メールにあるリンク先や添付ファイルに係る不正プログラムに感染したことが原因で、外部との不審な通信が発生したと考えられる。攻撃者は、件名を「厚生年金制度の見直しについて（試案）に関する意見」等として機構の業務への関連を偽装したメールを執拗に送信し、ついには遠隔操作下においた端末を起点に感染拡大活動及び情報窃取活動を行った。これら悪質極まりないサイバー攻撃の結果、約125万件もの大量の個人情報が流出したと認められる。NISCでは、これら不審メールに係る不正プログラムの接続先に関する情報を含む解析結果や、検知した不審な通信に関する情報を厚生労働省に提供・通知し、厚生労働省において接続先のURLの遮断を実施したが、情報流出を防ぐことが出来なかった。

「政府機関の情報セキュリティ対策のための統一基準」（2014年５月19日情報セキュリティ政策会議決定）（以下「政府統一基準」という。）においては、情報セキュリティインシデントに対応するための体制の整備や、情報セキュリティインシデントを認知した際の報告・対処手順を整備するよう求めている。今回の情報セキュリティインシデントにおいて、厚生労働省では、政府統一基準に準拠したセキュリティポリシーに基づく手順書に基づいた必要

[36] 日本年金機構における個人情報流出事案に関する原因究明調査結果（http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf）

な措置は一応とられていたが、責任者への報告はなされていなかったとしている。なお、機構のセキュリティポリシーにおいては、情報セキュリティインシデントに対処するための体制の必要性を規定し、その具体化はシステム障害対応を主たる目的としたリスク管理一般の規定等に委ねていたが、サイバー攻撃を想定した具体的な対応について、明確化されていなかった。またいずれの規程類においてもCSIRT体制についての定めがなかった。

政府統一基準において、多重防御の情報セキュリティ対策体系によって標的型攻撃に備える必要が示され、その具体的な対策を示すものとして、「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」（2014年６月25日情報セキュリティ対策推進会議決定）があるが、その適用範囲は、国の行政機関と記述している。厚生労働省においては、標的型攻撃に対する多重防御の取組を進めていたが、機構は、同ガイドラインの取組の対象とされておらず、その取組が十分でなかった。

さらに、標的型攻撃からの有効な遮断機能を有すると考えられるインターネットに接続していない業務系から、インターネットに接続している情報系に個人情報を移して取り扱っていたため、標的型攻撃を受けるリスクに当該個人情報をさらす結果となった。

そして、一連の調査結果を踏まえ、各府省庁への情報提供が有効に機能するための対策、情報セキュリティインシデントに備えた体制の強化、標的型攻撃のリスクを踏まえたシステムの構築、維持運用の強化対策等の再発防止対策が必要である旨記載している。これを踏まえ、サイバーセキュリティ戦略本部長から厚生労働大臣に対して勧告を行っており、厚生労働省では勧告等を踏まえて、2015年９月18 日に再発防止策として「情報セキュリティ強化等に向けた組織・業務改革－日本年金機構への不正アクセスによる情報流出事案を踏まえて－」を策定し、公表した[37]。また、2016年４月28日に勧告の改善状況をサイバーセキュリティ戦略本部長に報告し、公表した[38]。

NISCでは、政府機関のサイバーセキュリティに関して「予防」、「検知」、「対処」の側面から指針を示す等の取組を行ってきたが、これまでの取組を一層加速・強化することが必要である。サイバーセキュリティを取り巻く環境は年々変化していることを踏まえ、府省庁間の緊密な連携を通じて、政府全体としてのサイバーセキュリティの強靭化の取組について、継続的かつ速やかに推進していく必要がある。

[37] 情報セキュリティ強化等に向けた組織・業務改革－日本年金機構への不正アクセスによる情報流出事案を踏まえて－（http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150918-02.pdf）
[38] http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_160428-01.pdf

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、新たな「サイバーセキュリティ戦略」[39]（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、既にパブリックコメントに付した戦略案の内容について、本事案等を踏まえて改めて見直しを行うこととし、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み、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が2016年４月15日に成立した[40]。

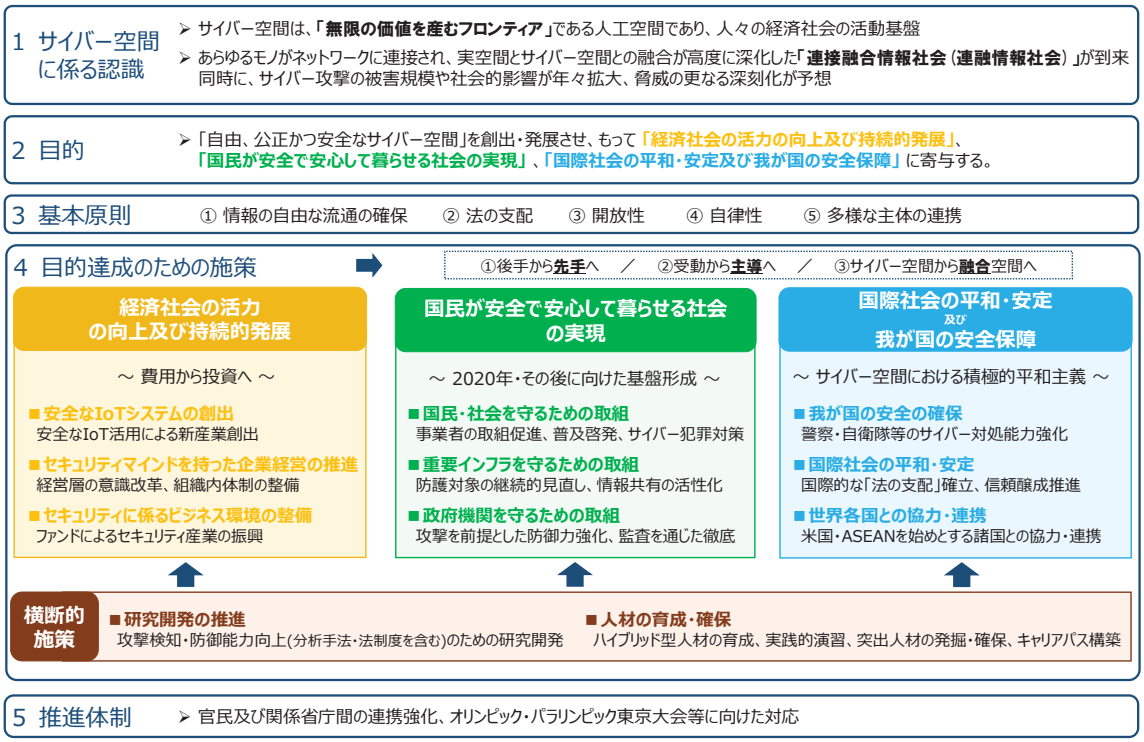
2015年度においては、戦略に基づく最初の年次計画である「サイバーセキュリティ2015」（2015年９月25日サイバーセキュリティ戦略本部決定）を策定し、これに沿ってサイバーセキュリティ政策を推進してきた。以下、戦略について概説した後、2015年度の主たる取組実績を概説する。

１　新たなサイバーセキュリティ戦略について

戦略は、2020年オリンピック・パラリンピック東京大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後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。そのため、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。

[39] サイバーセキュリティ戦略（http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf）
[40] 本法等の施行は、公布の日から６ヶ月以内の政令で定める日とされている。

図表Ⅱ－１－１　新たなサイバーセキュリティ戦略の全体構成



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

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進化した「連接融合情報社会（連融情報社会）」の進展に伴い、様々な機器がネットワークに接続され利活用されるようになってきている。一方で、こういったIoT機器の設計・製造・管理・運用や、それらをネットワークに接続する際にセキュリティを確保していくことは、IoTを活用した革新的なビジネスモデルを創出していくとともに、国民が安全で安心して暮らせる社会を実現するために必要不可欠である。

戦略においても、IoTシステムのセキュリティが確保された形での新規事業の振興やガイドラインの策定などの制度整備、技術開発などを進めることとされている。

これらを踏まえ、2015年10月に設立された「IoT推進コンソーシアム」において、2016年１月に「IoTセキュリティワーキンググループ」が設けられ、IoTシステム特有の性質に着目し、IoT機器等の設計・製造・ネットワークへの接続等に係るセキュリティガイドラインについて検討を行っているところであり、同年６月を目途に、当該ガイドラインを公表する予定である。

②　セキュリティマインドを持った企業経営の推進

連接融合情報社会における企業経営に当たって、これまで以上に、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進や組織能力の向上等を図ることが必要であり、セキュリティマインドを持った企業経営を浸透させることが重要である。こうした中、2015年12月に経済産業省と独立行政法人情報処理推進機構（IPA）が「サイバーセキュリティ経営ガイドライン」を公表した。

同ガイドラインは、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO（最高情報セキュリティ責任者：企業内で情報セキュリティを統括する担当役員）等）に指示すべき「重要10項目」をまとめている。

図表Ⅱ－２－１　サイバーセキュリティ経営ガイドラインの概要

１．経営者が認識すべき３原則
（１）経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、対応に係る**情報の開示**など、関係者との適切なコミュニケーションが必要

２．経営者がＣＩＳＯ等に指示をすべき１０の重要事項

リーダーシップの表明・体制構築	（１）組織全体での対策方針を策定すること
	（２）方針を実装するための体制を構築すること
ＰＤＣＡ策定	（３）リスクを洗い出し、計画を策定すること
	（４）ＰＤＣＡを実施し、状況報告をすること
	（５）ビジネスパートナーを含めＰＤＣＡを実施すること
攻撃を防ぐ事前対策	（６）予算・人材などリソースを確保すること
	（７）ＩＴシステムの委託先対策も確認すること
	（８）最新状況を対策に反映し、被害拡大を防ぐため、情報収集・共有活動に参加すること
攻撃を受けた場合に備えた準備	（９）迅速な初動対応を行うため、ＣＳＩＲＴ整備や訓練を実施すること
	（10）情報開示や経営者がスムーズな説明が出来るよう事前に準備すること

サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

③　セキュリティに係るビジネス環境の整備

IoT産業等の関連産業の成長に伴い、今後、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。このため、我が国において、サイバーセキュリティ産業がこうした需要を捉え、成長産業となるよう、国内外で大規模に活躍できる企業やベンチャー企業の育成等によりこれを振興していくことが重要である。

こうした中、株式会社産業革新機構による、サイバーセキュリティ対策の研究開発に取り組む企業への出資の実績も出てきており、引き続き、独立行政法人における研究開発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んでいくことが重要である。

また、我が国のサイバーセキュリティ関連産業が、国際競争力を有し、もって成長産業として我が国経済をけん引していくためには、国際的なルール等に我が国の立場を十分に盛り込んでいくことが重要である。こうした中、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つつ国際標準化を推進している。

(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。そのため、IPAと一般社団法人JPCERTコーディネーションセンターでは、「ソフトウエ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）[41]により、ソフトウェア製品及びWeb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関連情報を、脆弱性対策情報ポータルサイト（JVN）等を通じて利用者に提供した。Webサイトについては、IPAにおいて、届出を受けた脆弱性関連情報を基に、届出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げた「安全なウェブサイトの作り方」を公開し、Webサイト開発者や運営者が適切なセキュリティを考慮したWebサイトを作成するための情報を提供した。また、情報処理システムの信頼性の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うなど、サイバー空間の利用環境の安全性向上に向けた取組を行った。

また、利用者たる個人や企業・団体の意識・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。2015年度は、まずキックオフイベントとして、例年同様「キックオフ・シンポジウム」を2016年２月１日に開催した。2015年度のテーマは、『サイバーセキュリティを駆使する人材育成―連接融合情報社会で活躍できる人材とは―』として、サイバーセキュリティを駆使する人材が将来にわたって活躍し続けるための環境整備等について解説・議論した。

[41] 情報処理の促進に関する法律（昭和 45 年法律第 90 号）を改正し（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））、法令に基づく適切な方法・手続に則り、その社会的影響に応じ、開発者の同意がない場合であっても脆弱性の情報を公表できる制度とした。

図表Ⅱ－２－２　「2015 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

さらに、2015年度からの新たな取組として、NISCが運営する普及啓発のWebサイト「みんなでしっかりサイバーセキュリティ」[42]をリニューアルし、コンテンツの充実を図った。例えば、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「情報セキュリティハンドブック」を本Webサイトに掲載し、無料でダウンロードができるようになっている。次に、ソーシャルメディアを活用し、サイバーセキュリティの重要性を継続的に訴求していくため、セキュリティ関連情報（アップデート情報など）やセキュリティ関連の読み物を情報発信する「サイバー天気予報」（Twitter、LINE）を立ち上げた。加えて、「新・情報セキュリティ普及啓発プログラム」（2014年７月10日情報セキュリティ政策会議決定）に基づき、国民に親しみやすいメディアの影響力に着目し、マルチメディアコンテンツ「攻殻機動隊S.A.C.」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！秋葉原0305」の開催など、国民一人一人に、「サイバーセキュリティ月間」の趣旨が広く浸透し、サイバーセキュリティへの意識が高まるよう、官民一体となって新たな取組を実施した。

図表Ⅱ－２－３　セキュリティ対策の基本的な知識を学べる「情報セキュリティハンドブック」

[42] 「みんなでしっかりサイバーセキュリティ」（http://www.nisc.go.jp/security-site/）

図表Ⅱ－２－４　「サイバー攻撃を目撃せよ！秋葉原 0305」の様子

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得る犯罪・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、戦略に基づき、「警察におけるサイバーセキュリティ戦略」を制定し、警察組織の総合力を発揮した効果的な対策を推進していくこととした。特に、サイバー空間の脅威への対処に係る組織基盤の強化のため、2015年12月には、「サイバー空間の脅威への対処に係る人材育成方針」を策定し、職員の採用・登用、教養・研修、キャリアパスの管理等を部門横断的かつ体系的に実施することで、サイバー空間の脅威への対処に係る人材の裾野の拡大及び能力の向上を図ることとしている。

②　重要インフラを守るための取組

国民生活・経済社会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。

具体的には、各重要インフラ分野における安全基準等を策定するための指針を改訂し、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）」を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した。また、当該改訂に合わせ、具体化例を記載した同指針対策編の改訂を行うとともに、新たな試みとして、対策途上や中小規模の重要インフラ事業者等も取り組みやすいよう、対策の段階的な実現に資することを目的に、対応の優先順位付けの考え方を例示した手引書を策定した。

重要インフラ防護においては、迅速かつ的確な情報共有が有効であり、重要インフラ事業者等におけるIT障害発生時等においては、重要インフラ所管省庁を経由して内閣官房（NISC）に情報連絡が行われる。2015年度は401件の情報連絡が行われ、前年度（124件）の約３倍に増加している。また、脆弱性情報や注意喚起等のNISCから重要インフラ所管省庁を経由して重要インフラ事業者等に情報提供を行った件数は、2015年度は44件で、これも前年度（38件）より増加している。なお、これらの増加は、サイバー攻撃等によるIT障害等が増加していることを必ずしも示すものではなく、日本年金機構における不正アクセスによる情

報流出事案等を踏まえ、情報共有の重要性が認識され、NISCとの情報共有体制がより積極的に行われるようになってきているという側面もあると考えられる。

図表Ⅱ－２－５　重要インフラ事業者等との情報共有件数の推移

年度	2009	2010	2011	2012	2013	2014	2015
重要インフラ事業者等から内閣官房への情報連絡件数	128件	169件	43件	110件	153件	124件	401件
関係省庁・関係機関から内閣官房への情報共有件数	294件	137件	400件	50件	55件	27件	52件
内閣官房からの情報提供件数	13件	48件	34件	38件	49件	38件	44件

こうした官民間の情報共有に加え、民民間でも、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ついて情報共有体制としてC⁴TAP[43]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。J-CSIPにおいては、自動車業界を対象とした、「自動車業界SIG」を新たに設立するなどにより、参加組織を59組織から72組織に拡大している。

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同に会して、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。2015年度は302組織1,168名が参加し、過去最大規模での開催となった。

図表Ⅱ－２－６　2015 年度分野横断的演習の様子

遠藤大臣による演習視察

全体振り返りの模様

なお、重要インフラの情報セキュリティ対策に係る第３次行動計画については、2016年度が見直し時期とされていることから、見直しに向けた検討を開始しており、2016年３月にはサイバーセキュリティ戦略本部において、同計画の見直しに向けたロードマップを決定した。同ロードマップに従い検討を進め、同計画の見直しについては2016年度末を目途に結論を得、早急に対処すべき事項については同計画の見直しを待たずに対処していくこととなる。

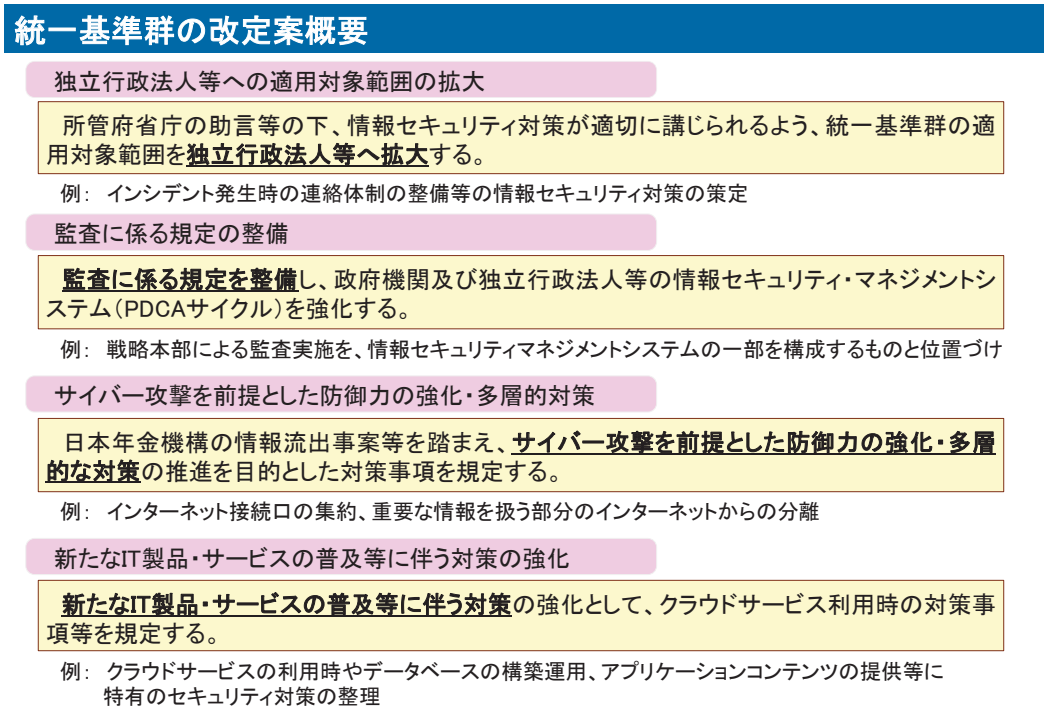
[43] CEPTOAR Councils Capability for Cyber Targeted Attack Protection

③ 政府機関を守るための取組

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

まず、政府機関における統一的な基準の策定に関して、本節で後に述べる政府機関における取組や脅威等の動向を踏まえ、「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。）の改定案を2015年度に検討した。主な改定概要は以下の図に示すとおりである。2016年夏頃に開催されるサイバーセキュリティ戦略本部において決定されることを目指して、現在、改定作業を進めているところである[44]。

図表Ⅱ－２－７　統一基準群の主な改定案概要



【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、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、政府機関等において適切に注意喚起等を行ったほか、GSOCが有するべき機能、政府機関等の連携体制等について検討を行い、次期GSOCシステムの仕様に反映させることで、情報の収集・分析機能等の強化を進めている。また、サプライチェーン・リスク対応のための仕様書策定手引書を整備し公表したほか、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」へのサプライチェーン・リスク対応の追加、情報システムの調達においてセキュリテ

[44] 「別添 3-1　政府機関の情報セキュリティ対策のための統一基準群による対策の推進」参照。

ィ・バイ・デザイン[45]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。さらに、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[46]ほか、各府省庁の基幹LANシステム等を対象として侵入試験（ペネトレーションテスト）を実施し、その結果を踏まえ、セキュリティ対策水準の向上を図るための助言等を行った[47]。

被害の発生・拡大の防止のための主な取組としては、政府機関全体における検知・解析機能の強化のため、前述したように次期GSOCに関する検討を進めている。また、各府省庁におけるCSIRT体制・連携体制等の強化の指示を行うとともに、昨今のサイバーセキュリティについての情勢等を踏まえ、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を検討し、統一基準群における所要の規定強化を行ったほか、近年のサイバー攻撃動向を踏まえた情報セキュリティインシデント発生時の対処を中心とした訓練[48]や、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 2016を始めとした政府機関、重要インフラ事業者等のLAN管理者の対処能力向上のための実践的サイバー防御演習（CYDER : CYber Defense Exercise with Recurrence）を実施した。さらに、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の再発防止策として、業務効率等を考慮しつつ可能な限りインターネットの接続口を集約するよう仕様書に明記すること等の反映を行うことを検討した。加えて、デジタルフォレンジック調査に係る最新動向を把握しつつ重大な情報セキュリティインシデント発生時に専門事業者と連携して速やかに調査を行うことができるようにした。

図表Ⅱ－２－８　「National 318(CYBER) EKIDEN 2016」の様子

被害の低減のための主な取組としては、リスクや影響度に応じた情報システムの対策強化について、「「日本再興戦略」改訂2015」等に基づいて検討を行い、前述したインターネットの接続口の集約、情報セキュリティインシデント発生時の対処手順における意思決定の判断基準等の策定、行政事務の特性や取り扱う情報の性質及び量を考慮した情報システムの分離、機密性・完全性の高い情報を管理するデータベースにおける情報漏えいや改ざん等への対策等を検討し、統一基準群における所要の規定強化を行った。また、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」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推進している[49]。

---

45 システム等の企画・設計段階からセキュリティの取組を織り込んでいくこと。「別添５　用語解説」参照。
46 「別添 3-3　重点検査による評価」参照。
47 「別添 3-2　サイバーセキュリティ基本法に基づく監査」参照。
48 「別添 3-6　教育・訓練に係る取組」参照。
49 「別添 3-5　高度サイバー攻撃への対処」参照。

【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を行っている。主な取組としては、監査制度の設計及び当該制度の有効性の検証を目的とした試行的な監査を10府省庁に対して実施し、本格的な監査を実施するために必要な監査制度の枠組みを確立したほか、被監査対象組織に対しては、改善のために必要な助言等を行った[50]。また、府省庁における情報セキュリティインシデント発生時に、緊急度に応じて、情報システムへの緊急措置等を迅速に行えるようにするための意思決定プロセスについて検討するとともに、情報システムの運用継続計画の整備及び整合的運用を確保するための施策について見直しを行い、統一基準群の改定案をまとめた。

政府機関においては、サイバー攻撃等が発生した際に、府省庁の壁を越えて連携し、被害拡大防止等機動的な支援を行うため、情報セキュリティ緊急支援チーム（CYMAT ： Cyber Incident Mobile Assistance Team）をNISCに設置しており、CYMAT要員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。2015年度におけるCYMATの活動としては、７件の具体的な支援及び助言を行った。

また、セキュリティ・IT人材の不足という政府機関における共通的な課題に対応するため、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、「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）において取りまとめた。当該方針では、2016年度から新設された「サイバーセキュリティ・情報化審議官」等の主導の下、各府省庁において「セキュリティ・IT人材確保・育成計画（仮称）」を作成することや、当該人材の研修受講者を今後４年で1,000人を超える規模とすること等を目指すこととしている。

さらに、政府機関等における対処能力向上や情報共有の推進のため、勉強会の開催、セミナーにおける講演、教養資料の作成、情報セキュリティインシデント発生時の対処訓練の実施等を行った[51]。

【技術の進歩や業務遂行形態の変化への対応】

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

主な取組としては、政府機関等において利活用が進むクラウドサービスについて、クラウド事業者及びクラウドに係る有識者から構成される「政府機関がクラウド利用の際に留意すべきセキュリティに関する研究会」を開催し、クラウドサービス選定の際に考慮すべき点について整理・検討を行い、その結果を踏まえて統一基準群における所要の規定強化を行った[52]。また、サービス不能攻撃への対処や、サポート切れソフトウェアの使用回避及びインターネットに接続された機器のセキュリティ問題等について注意喚起を行った[53]。

---

50 「別添 3-2　サイバーセキュリティ基本法に基づく監査」参照。
51 「別添 3-6　教育・訓練に係る取組」参照。
52 「別添 3-4　クラウドサービスの利用に係る対策」参照。
53 「別添 3-10　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」参照。

【監視対象の拡大等による総合的な対策強化】

政府機関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。

主な取組としては、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の教訓やⅡ－２－(5)で述べるサイバーセキュリティ基本法の改正を踏まえ、統一基準群の対象範囲を独立行政法人や指定法人まで拡大することを検討し、文書体系の見直し等を行ったほか、GSOCの監視対象やマネジメント監査の方針等についても検討を進めている。また、独立行政法人、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を把握、分析[54]し、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、法務省公安調査庁、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、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

[54] 「別添 3-9　独立行政法人等における情報セキュリティ対策の調査結果の概要」参照。

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。2015年度においては、G7外相会合（2015年４月　ドイツ・リューベック）、同エネルギー大臣会合（2015年５月　ドイツ・ハンブルク）、G20首脳会合（2015年11月　トルコ・アンタルヤ）、東アジア首脳会議（2015年11月　マレーシア・クアラルンプール）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４次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[55]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内容を含む報告書の策定に貢献し、サイバー空間における法の支配の確立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・協定に基づく協力、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ところである。

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[56]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[57]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

[55] Information and Communications Technology の略。情報通信技術のこと。「別添５　用語解説」参照。
[56] 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。「別添５　用語解説」参照。
[57] 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。「別添５　用語解説」参照。

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[58]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を進めている。

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、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」を設置し、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。法務省でも、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等の各機関において、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。

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、我が国関係機関の協力のもとASEAN各国を対象に開催されたサイバーセキュリティ・コンテスト「Cyber SEA Game 2015」と、我が国におけるサイバーセキュリティ・コンテスト「SECCON CTF2015」との間で連携を図り、我が国のサイバーセキュリティ人材が、海外の優秀な人材との間で相互に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ものであり、一国のみで対応することは困難である。我が国は世界各国との二国間・多国間の様々な枠組みを活用した協力・連携により、国際社会の平和・安定及び我が国の安全保障の実現に向けた取組を進めている。

アジア大洋州では、地域の責任ある国として、各国・地域との間で様々なチャネルを通じたサイバー分野での協力を進めている。40年以上にわたるパートナーであるASEANとの間では、内閣官房、総務省、経済産業省が中心となり、第８回日・ASEAN情報セキュリティ政策会議(2015

[58] 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。「別添５　用語解説」参照。

年10月 インドネシア・ジャカルタ）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２回日中韓サイバー協議（2015年10月 韓国・ソウル）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－２－９　「第８回日・ASEAN 情報セキュリティ政策会議」の様子

米国との間では、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。2015年度においては、両国政府間において新たな「日米防衛協力のための指針」（2015年４月）を策定し、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ることとしている。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。第３回目となる日米サイバー対話（2015年７月 東京）では、情勢認識、重要インフラ防護、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ている。加えて、両国間ではインターネットエコノミーに関する日米政策協力対話（第７回局長級会合）（2016年２月 東京）、第３回及び第４回の日米サイバー防衛政策ワーキンググループ（それぞれ2015年４月 東京、2016年１月 米国・ワシントンDC）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。

欧州諸国との間では、政府横断的な二国間協議である第２回日エストニアサイバー協議（2015年12月 東京）及び第２回日仏サイバー協議（2016年１月 東京）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との間でも、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－２－10　「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。写真左は、キャンペーンのイベントとしてASEAN各国との連携により開催した「サイバーセキュリティカフェ」、写真右は、同じく在京米国大使館及び在日米国商工会議所との連携により開催した「サイバー・ハロウィンキャリアトーク」の様子。

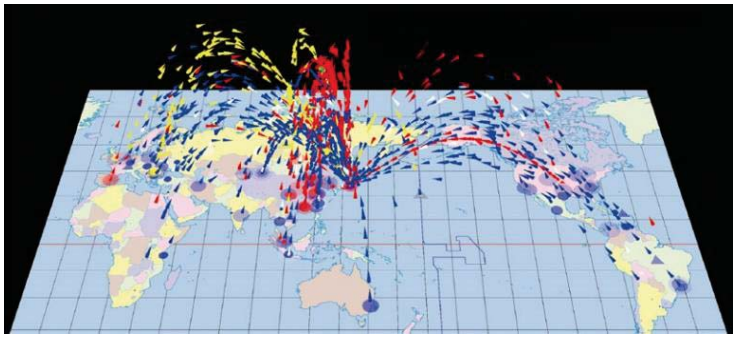
(4)　横断的施策

①　研究開発の推進

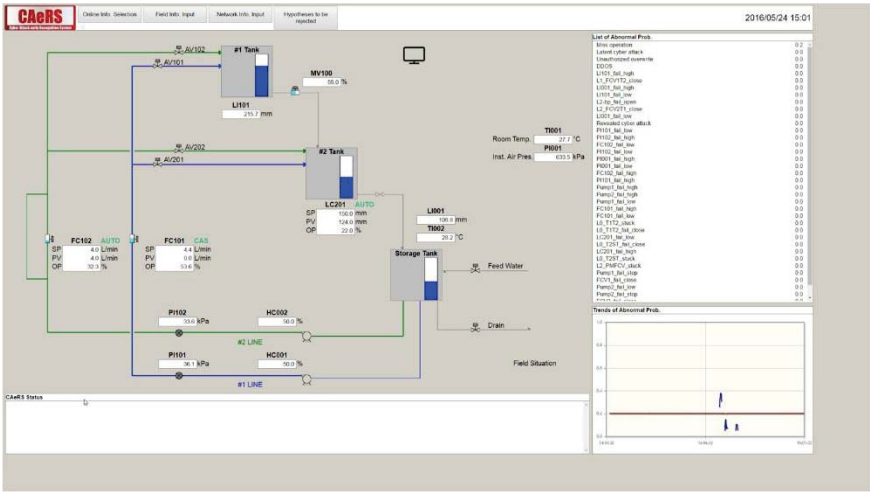
サイバー攻撃は、日々進化し、高度化・複雑化しており、その変化に対処していくため、幅広い分野において、創意・工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠である。さらに、2016年１月には、「第５期科学技術基本計画」を閣議決定し、国及び国民の安全・安心の確保と豊かで質の高い生活の実現のための重要政策課題の一つとして、サイバーセキュリティの確保が設定されている。

まず、IoTシステム等が普及した連接融合情報社会においては、実態に応じた検知・防御能力の一層の向上が求められる。例えば、総務省では、国立研究開発法人情報通信研究機構（NICT）を通じて、サイバーセキュリティ研究の一環として、「サイバー攻撃・観測・分析・対策システム（NICTER）」を活用し、IoT機器を標的とした新たなサイバー攻撃を多数観測するとともに、次世代暗号基盤技術などのネットワークセキュリティ技術の研究開発を推進している。また、経済産業省では、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開発を推進している。

図表Ⅱ－２－11　サイバー攻撃・観測・分析・対策システム（NICTER）



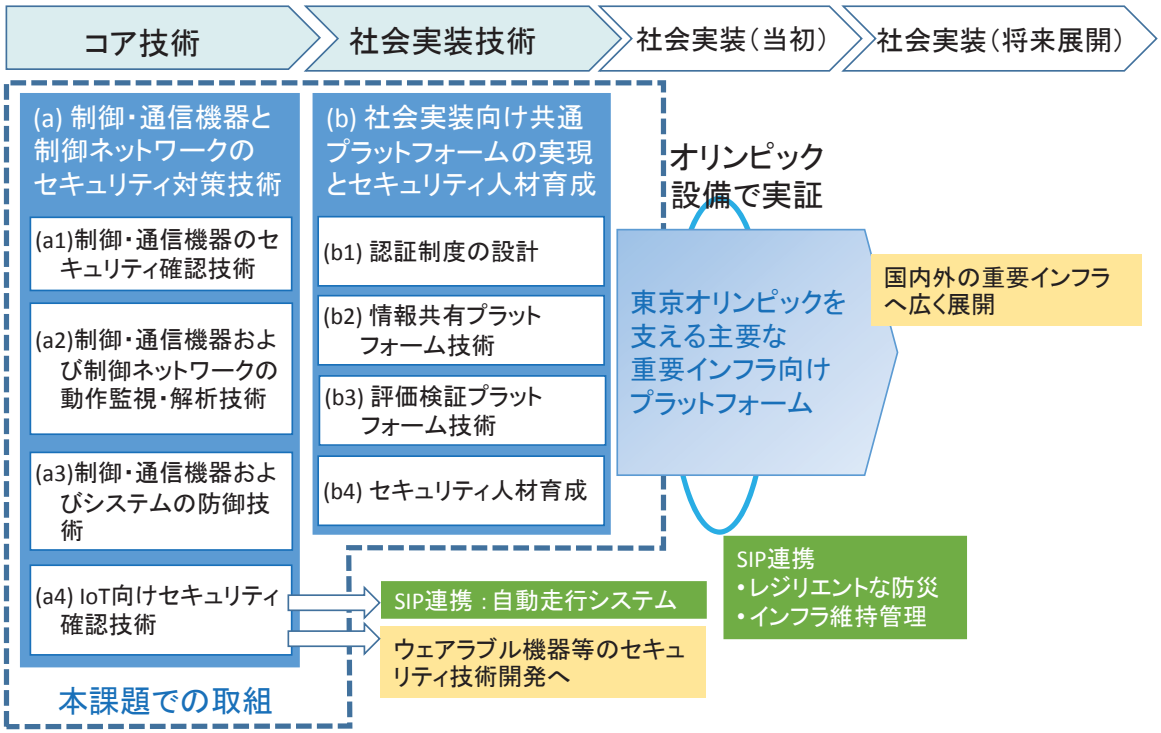
図表Ⅱ－２－12　CSSC による制御システムのサイバー攻撃検知技術



また、サイバー空間は実空間と融合し、法令等の研究や政策、情勢、技術といった様々な分野における分析手法の研究が必要である。例えば、文部科学省では、ビッグデータや人工知能（AI）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開始し、研究開発拠点の立ち上げの準備に入った。

さらに、研究開発は短期間で成果が出るものではなく、長期的に取り組むべき課題であり、関連機関との連携が必要である。例えば、内閣府（総合科学技術・イノベーション会議）では、戦略的イノベーション創造プログラム（SIP）に「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加し、府省庁の枠や旧来の分野の枠を超えた研究開発を推進しているところである。

図表Ⅱ－２－13　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」



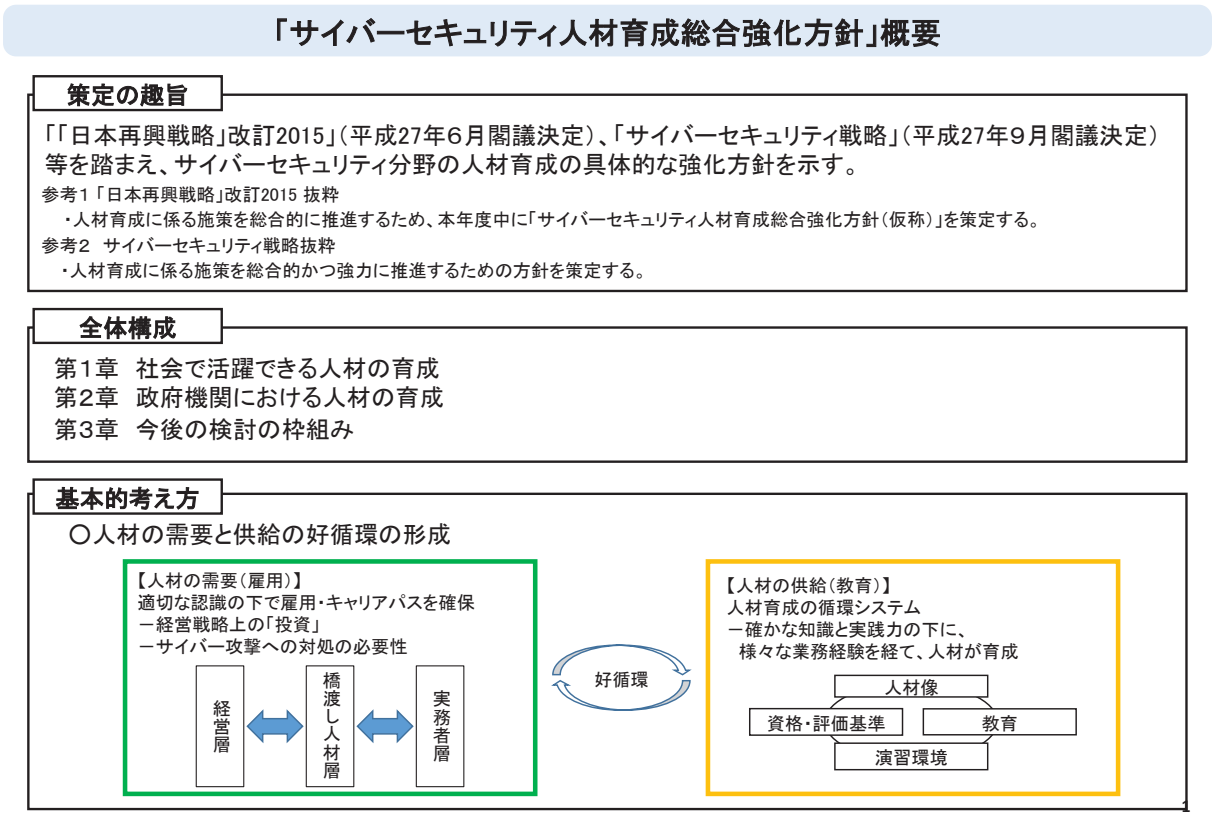
②　人材の育成・確保

連接情報融合社会においては、サイバーセキュリティは、同分野の専門家はもちろん、一般的な情報通信技術者、ひいてはIoTシステムの利用者に至るまで、程度に差はあるものの様々な層の人材に必須の素養である。そこで、人材育成に係る施策を総合的かつ強力に推進するための方針である「サイバーセキュリティ人材育成総合強化方針」を2016年３月に決定し、民間人材の育成と政府機関における人材育成について、人材の需要と供給の好循環を形成するための必要な施策を講じることを基本的な考え方とした方針を示した。

また、サイバーセキュリティ人材が将来にわたって活躍し続けるための環境整備の一環として、経済産業省では、能力の可視化を図るため、国家試験である「情報処理技術者試験」を実施するほか、企業等のセキュリティ対策を担う専門人材の国家資格として、新たに「情報処理安全確保支援士」の創設に係る取組を進めた。加えて、総務省では、本年４月の国立研究開発法人情報通信研究機構法の改正を踏まえ、技術的知見を有するNICTをサイバーセキュリティに関する演習の実施主体とし、演習の質の向上や継続的・安定的な運用を実現するとともに、演習の主な対象を地方自治体等に拡大する。

さらに、突出した能力を有した人材の発掘・確保に向けて、「セキュリティキャンプ」等の事業を行うとともに、SECCON等の世界各国から集まり能力を競うコンテストの支援を行った。

図表Ⅱ－２－14　「サイバーセキュリティ人材育成総合強化方針」概要



図表Ⅱ－２－15　「SECCON 2015 決勝大会」遠藤大臣ご視察の様子

(5)　推進体制

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を踏まえ、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、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、政府によるサイバーセキュリティ対策の抜本的強化を図るため、サイバーセキュリティ基本法の改正を行うこととした。具体的には、国による監視、監査、原因究明調査の対

象をそれぞれ拡大し、国の行政機関、独立行政法人、特殊法人及び認可法人のうちサイバーセキュリティ戦略本部が指定するものを対象とすることとした。特殊法人・認可法人の指定に当たっては、戦略本部は、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動に及ぼす影響を勘案することとされており、その対象としては、日本年金機構等を想定している。また、戦略本部の事務の一部をIPAに委託することを可能としており、委託に当たっては秘密保持義務等を規定し、適切に事務が行われるようにしている。これらを内容とする「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案」を2016年２月２日に閣議決定し、第190回国会に提出した[59]。

これに加えて、「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」（2016年１月25日サイバーセキュリティ戦略本部決定。以下「機能強化方針」という。）を策定した。方針は、上述の法改正を含む、政府機関等におけるサイバーセキュリティ推進体制の更なる強化に向けた具体的な方向性を定めたものであり、サイバーセキュリティに係る政府人材等の強化、大規模なサイバー攻撃に備えた官民の連携体制等の構築、重要インフラ事業者等に関する取組支援の強化、マイナンバー事業の円滑な導入及び推進及び東京オリンピック・パラリンピック競技大会等に向けた取組の加速化を盛り込んでおり、関係省庁において、同方針を踏まえた施策を講じた。

まず、各府省庁においては、CISO・CIOの補佐等を行う「サイバーセキュリティ・情報化審議官」等を新設しており、「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日戦略本部決定）には、これらを含めた、政府機関における人材育成のための施策が盛り込まれた。

また、安定的・継続的なサイバー防御演習の実施体制の確保に向け、NICTにおいてサイバーセキュリティに係る演習等が実施できるよう、「国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律案」を2016年３月１日に閣議決定し、第190回国会に提出した[60]。JPCERT/CCとの協力関係については、2015年２月に合意したパートナーシップに基づき、情報共有システムの整備や定期的な会合の開催を含めた情報共有体制を構築し、日常的に活発な情報共有や関係組織への連絡等の対処を行った。

さらに、2016年のG7伊勢志摩サミット、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、継続的なリスク評価を実施するとともに、2019年ラグビーワールドカップ開催時においてオリンピック・パラリンピックCSIRTの稼働を目指し、関係者間の調整を行った。

図表Ⅱ－２－16　G7伊勢志摩サミットの様子


[59] 同法律は2016年４月15日に成立し、同月22日に公布された。
[60] 同法律は2016年４月20日に成立し、同月27日に公布。同年５月31日に施行。

図表Ⅱ－２－17　「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」の概要

１．更なる機能強化の必要性

平成27年5月に発生した日本年金機構における個人情報流出事案等を踏まえ、「『日本再興戦略』改訂2015」や「サイバーセキュリティ戦略」を閣議決定し着実に推進している。本文書は、深刻化が進むサイバー攻撃に備え、**政府機関等をはじめとしたサイバーセキュリティ推進体制の更なる機能強化に向けた具体的な方向性**を定めるもの。

２．更なる取組強化策

(1) 国が行う不正な通信の監視等の対象の拡大

- 監視・監査・原因究明調査の対象範囲を独立行政法人及び指定法人（本部が指定する特殊法人及び認可法人）まで拡大し、同業務の一部をIPAへ委託（今国会にてサイバーセキュリティ基本法改正を審議）
- 平成28年夏を目途に統一基準群を改定

(2) サイバーセキュリティに係る政府人材等の強化

- NISC要員の増強を図り、監視・監査業務を含む体制を強化
- マイナンバー等のセキュリティ確保のため個人情報保護委等の体制を整備
- 各府省庁にCISO・CIO（官房長等）を補佐する「情報セキュリティ・情報化推進審議官(仮称)」等を設置
- 「サイバーセキュリティ人材育成総合強化方針(仮称)」を策定（今年度末目途）

(3) 大規模なサイバー攻撃に備えた官民の連携体制等の構築

- 独立行政法人及び指定法人におけるCYMATと同様の取組を促進（平成29年度上半期を目途に体制を整備し、運用を開始）
- NICTにおいてサイバーセキュリティに係る演習・訓練・教育コンテンツ制作等が実施できるよう必要な法整備を速やかに実施

(4) 重要インフラ事業者等に関する取組支援の強化

- 重要インフラ事業者等の迅速かつ自主的な取組を促進（基本法に基づいた関係行政機関の長への勧告についても必要に応じ運用）
- 重要インフラ全体の面的防護等のため、平成28年度末を予定する行動計画の見直しに向け、検討ロードマップを取りまとめ（今年度末目途）

(5) マイナンバー事業の円滑な導入及び推進

- 各地方自治体において、自治体情報セキュリティクラウドを構築する等、情報セキュリティ対策を抜本的に強化
- 年金関連業務について、勧告に対する措置状況報告等を踏まえた厚生労働省に対する追加的監査実施などを通じ、年金関連業務におけるマイナンバー利用の早期開始に努める。

(6) 東京オリンピック・パラリンピック競技大会等に向けた取組の加速化

- 伊勢志摩サミット等の国際的なイベントにおけるサイバーセキュリティ確保のための取組を着実に推進
- 2020年に向け継続的なリスク評価を実施
- 2019年ラグビーワールドカップ開催時においてオリパラCSIRTを稼働

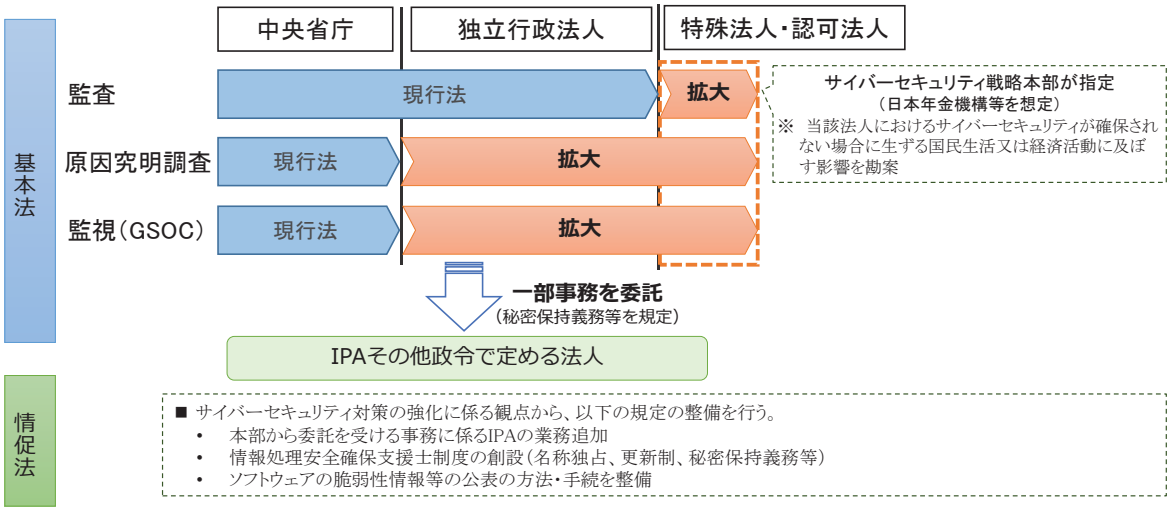
３．今後の取組

本方針に基づく取組は、可及的速やかに実施。また、サイバー空間における脅威の増大・深刻化や東京オリンピック・パラリンピック競技大会に向けた準備状況等時々刻々と変化する諸情勢を踏まえつつ、法制の追加的な整備等についても引き続き検討。

図表Ⅱ－２－18　「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」の概要

日本年金機構の情報流出事案等を踏まえ、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ため、サイバーセキュリティ基本法等の改正を行う必要。

■ 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を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）等に委託



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」に基づく最初の年次計画である「サイバーセキュリティ2015」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）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2015」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2016年度の年次計画である「サイバーセキュリティ2016」については、本評価も踏まえて諸施策の改善を図るとともに、これを着実に推進することとする。

１　経済社会の活力の向上及び持続的発展

(1)　安全な IoT システムの創出

【総　評】

2016年１月より、総務省と経済産業省が共同して、IoT推進コンソーシアム　IoTセキュリティワーキンググループを立ち上げ、IoTセキュリティガイドラインの策定に向けた検討を開始した。また、スマートメーターのセキュリティガイドラインを策定する等、各分野のガイドラインについても検討が進められている等、安全なIoTシステムの創出に向けた取組が行われている。

【課　題】

IoTセキュリティガイドライン（2016年６月策定予定）を普及させるとともに、同ガイドラインを踏まえて、IoT機器の脆弱性等に関する情報が、それに対する対策とともに利用者に着実に行き届くような仕組み等、IoTに対する総合的なセキュリティ対策を関係省庁が連携して実施していく必要がある。

(2) セキュリティマインドを持った企業経営の推進

【総　評】

経済産業省において2015年12月に「サイバーセキュリティ経営ガイドライン」が取りまとめられ、説明会等によりガイドラインの普及が進められた。また、情報セキュリティインシデントの情報共有については、各業界団体を中心に情報を共有する枠組みが進みつつある。また、政府機関や重要インフラ事業者等の担当者のサイバー攻撃への対処能力向上のための演習が実施される等組織能力向上のための取組が行われた。

【課　題】

利害関係者からサイバーセキュリティに関する取組が正当に評価され企業価値の向上につながるための仕組み等について、更なる検討が必要である。また、経営層の意識改革を促していくとともに、経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う「橋渡し人材層」の育成が重要

である。社会で活躍できる人材の育成に向けて、産学官連携による人材供給を進めるなどにより、人材の需要と供給の好循環を形成するための取組を一層強化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】

我が国のセキュリティ産業育成に向け、独立行政法人と連携し、セキュリティ技術研究のための先進的な研究開発を進めるための支援事業を開始した他、産業革新機構と連携し、先端的なセキュリティ技術への投資案件が実現する等の進展が見られた。また、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している。

【課　題】

我が国のサイバーセキュリティ関連産業が成長産業となるよう、引き続き先進的な研究開発を行っているベンチャー企業に対する支援事業を実施させるとともに、国際会合等に参加し、積極的に我が国の意向を国際標準等に盛り込んでいく必要がある。また、著作権法におけるリバースエンジニアリングに関する適法性の明確化についても速やかに措置を講ずる必要がある。

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の検討を推進した。また、「サイバーセキュリティ月間」では、ソーシャルメディアの活用や国民に親しみやすいメディアの活用など新たな取組を実施するなど、普及啓発活動を推進した。さらに、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】

産学官民の様々な立場の主体が有機的に連携し、一体となって行う普及啓発活動が地域レベルでも促進されるよう、各地で実施されている草の根的な活動に対し、積極的に支援等を行うことが望まれる。また、サイバー犯罪の捜査や未然防止に向け、官民の人事交流などの官民連携の強化が必要である。

(2)　重要インフラを守るための取組

【総　評】

第３次行動計画の２年目に当たり、同計画における各施策の着実な取組を行った。また、サイバー攻撃の深刻化や、サイバーセキュリティ戦略等を踏まえ、重要インフラ防護に関する検討課題を整理し、2016年３月にサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」を決定した。

【課　題】

第３次行動計画の各施策を引き続き推進する一方で、上記ロードマップに従い検討を進めていき、第３次行動計画の見直しを行う必要がある。また、深刻化するサイバー攻撃に対応するため、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必要がある。

(3)　政府機関を守るための取組

【総　評】

サイバーセキュリティ基本法の制定・施行を踏まえた統一基準群の位置付けの明確化や、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の教訓、外部環境変化等を踏まえた規定の強化を内容とする統一基準群の改定案をまとめた。また、セキュリティ・IT人材の不足という政府機関における共通的な課題に対応するため、政府機関におけるセキュリティ・IT人材の育成についての施策を「サイバーセキュリティ人材育成総合強化方針」に盛り込んだ。

【課　題】

統一基準群については、2015年度に示した改正の方向性に加え、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」に基づき、政府機関、独立行政法人に加え、戦略本部が指定する特殊法人、認可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。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、司令塔機能の抜本的強化やセキュリティ・IT人材（部内育成の専門人材）の確保・育成等、政府機関におけるセキュリティ・IT人材の育成を推進する必要がある。

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】

首脳・閣僚による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。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、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次期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。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キャパシティビルディングを中心としつつ、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、各府省庁において、サイバー攻撃検知や防御力向上等に資する研究開発施策が実施された。また、内閣府（総合科学技術・イノベー

ション会議）では、SIPに「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加し、産学官が連携した総合的な研究開発を推進した。

【課　題】

日々高度化・巧妙化するサイバー攻撃を予測して対応するため、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た領域の研究との連携を深め、融合領域における研究を一層促進していく必要がある。また、暗号研究等の基礎研究についても引き続き取り組むとともに、SIPにおける「重要インフラ等におけるサイバーセキュリティの確保」にについても着実に取組を進めていく必要がある。

(2)　人材の育成・確保

【総　評】

「サイバーセキュリティ人材育成総合強化方針」を決定し、各府省庁にまたがる人材育成に係る施策を総合的かつ強力に推進するための方針を示した。また、新しい資格制度の検討や、演習環境の整備等、人材の需要と供給の好循環に向けた施策を推進した。

【課　題】

「サイバーセキュリティ人材育成総合強化方針」の下、引き続き人材の需要と供給の好循環に向けた施策を推進していくとともに、実践的な能力を適時適切に評価できるスキル基準の整備や、キャリアパスの構築等について取り組む必要がある。また、「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」の成立を踏まえ、情報処理安全確保支援士制度の実施に向けて取り組む必要がある。

5　推進体制

【総　評】

NISCにおいて、特定任期付職員等の採用による高度セキュリティ人材の民間登用等を行い、総合的分析機能の強化を図ることができた。また、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を踏まえ、監視、監査、原因究明調査の対象範囲を独立行政法人等にも拡大するとともに、戦略本部の事務の一部をIPA等に委託すること等を内容とする「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案」を2016年２月に閣議決定し、国会に提出した。また、総務省において、NICTの業務の範囲にサイバーセキュリティに関する演習を追加すること等を内容とした「国立研究開発法人情報通信研究機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する等の法律案」を2016年３月に閣議決定し、国会に提出（同年４月20日成立）。政府全体として、大規模なサイバー攻撃に対処するための体制整備が着実に進められている。

【課　題】

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」を踏まえて、特殊法人、認可法人の指定等の所要の準備を進める必要がある。また、NICTが速やかにサイバーセキュリティに関する演習を行うことができるよう所要の準備を進める必要がある。さらに、今年度の検討結果を踏まえて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専従CSIRTを整備するとともに、2016年３月に策定

したサイバーセキュリティ人材育成総合強化方針に基づき高度専門人材を外部から受け入れる等、NISCの対処能力を更に強化していく必要がある。

別添１　各府省庁における情報セキュリティ対策に関する取組

＜別添１－目次＞

政府統一基準において、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2016年度当初までに定めた「対策推進計画」を基として、2015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2016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

2015年度の総合評価・2016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

2015年度は、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するなど、政府機関に対する標的型攻撃やDoS攻撃等、的を絞った執拗な攻撃が相次いで発覚し、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、2014年度の約780件に対し2015年度は約2,000件と、前年比において２．５倍以上に増加している。これはサイバー攻撃の端緒となる攻撃が増加したものと考えられる。

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の増加は、2020年オリンピック・パラリンピック東京大会を控え、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2016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ラーニングの導入を進める。

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

2015年度の総合評価・2016年度の全体方針

最高情報セキュリティ責任者
総務主幹　岩尾　信行

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。

2015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。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。）からの不審メール情報等の周知及び注意喚起等に迅速かつ適切に対応した。また、Webサイトにおけるセキュリティ対策強化及び標的型攻撃対策を実施しするとともに、USBメモリの利用制限を行うことにより情報セキュリティ強化を実施した。

2016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、2015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、CSIRT構成員を対象としたインシデント発生時の対応訓練等を実施するほか、NISCからの不審メール等の情報提供について迅速かつ適切に対応することでインシデントの発生防止を図る。内閣法制局LANシステムの更改に伴い、サイバー攻撃に対するセキュリティ対策を強化する。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改定を行う。

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

2015年度の総合評価・2016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　江畑　賢治

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増加しており、情報漏えいのリスクや脅威は増大してきている。

このような環境の中、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。

2015年度においては、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に、最高情報セキュリティアドバイザーによる情報セキュリティ責任者、情報システム責任者を対象とした集合研修を行うとともに、全職員を対象としたe-ラーニングによる情報セキュリティ教育を実施した。

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、各課の情報セキュリティ責任者を通じ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し、自己点検どおりに実施していることを確認した。

2016年度においては、政府機関等に対するサイバー攻撃手法が巧妙化・悪質化しているところ、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には、サイバーセキュリティ・情報化審議官の新設等により強化されたセキュリティ体制のもと、更なる技術的対策の実施に加え、職員一人一人の的確な対応が求められることから、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ていくことが重要となる。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。

内閣府

2015年度の総合評価・2016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（平成26年5月19日情報セキュリティ政策会議決定)」を踏まえ、「内閣府本府情報セキュリティポリシー」（以下「ポリシー」という。）を策定し運用を行っている。

ポリシーは、実情と情勢を踏まえ、CISO補佐官の助言や準拠性監査に基づき、運用実態に合うように改定することとしている。

2015年度は、情報セキュリティの強化対策として、①情報セキュリティの確保に対する職員の意識改革に向けた取り組みと、②部局のソーシャルメディアサービス運用者による事故を防止する対策の2点に重点を置いて実施した。

2016年度においては、引き続き上記①と②の強化対策に重点を置き、サイバー攻撃の変化等の状況を踏まえつつ、効果的な対策を講じて、情報システムの安全性の確保と職員のリテラシーの向上を図ることとする。

宮内庁

2015年度の総合評価・2016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　和田　裕生

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、2015年度においては、主に以下の対策を実施した。

○　情報セキュリティ責任者向けの個別研修
○　全職員を対象とした標的型攻撃を想定した対処訓練
○　システム上、実行形式ファイルについて、Webサイトからのダウンロードや電子メールによる送受信を遮断
○　不正な通信ブロックの強化

2016年度においては、引き続き、全職員を対象に標的型攻撃を想定した対処訓練を実施して意識の向上を図るとともに、マルウェアに感染した場合にも被害を最小化できるよう、初動対応の在り方、日常的な情報の保存管理について、重点的な教育を行う。また、技術的な対策については、新たなサイバー攻撃の脅威や情報通信技術についての情報収集に努め、より効果的な対策の検討・導入を進める。

さらに、情報セキュリティ対策に係る自己点検や監査を充実させることにより、PDCAサイクルの推進を図り、一層の情報セキュリティ対策の向上に努めることとする。

公正取引委員会

2015年度の総合評価・2016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　山本　佐和子

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。

2015年度は、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たことから、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、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（年２回）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に対しては、集合研修も実施した。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た（当該点検では、ほとんどの項目について必要な対策が行われており、相当程度高い情報セキュリティ対策が実施されていることを確認している。）。

2016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、2015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体制に関する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

2015年度の総合評価・2016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　川邉　俊一

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。

2015年度においては、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を受け、類似の手口による攻撃を受けていないかの点検を行うとともに、重要情報の取扱いに配意するよう注意喚起を行うなど、情報の適切な管理について一層の徹底を図った。

標的型メール攻撃の手口が巧妙化している情勢を踏まえ、2015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。このほか、情報システムにおける情報セキュリティ対策に関する重点検査やぜい弱性検査を実施し、必要な対策が講じられていることを確認した。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、情報流出事案防止対策等の実施状況において軽微な改善を要する事項が認められたことから、改善措置の結果報告を求めるなどして確実に対策を講じた。

2016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関する対策を実施していく。さらに、2016年度からは新たにサイバーセキュリティ・情報化審議官及び情報セキュリティ対策官が設置されることや2015年度のNISCによるマネジメント監査の受監結果を踏まえ、情報セキュリティ対策についてのPDCAサイクルをより強力に回して一層の推進を図る。

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

2015年度の総合評価・2016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」を決定したところである（2016年２月15日）。

委員会は、このような組織の使命及び業務内容を踏まえて、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。

2015年度においては、情報セキュリティ政策会議（2014年５月19日）における「政府機関の情報セキュリティ対策のための統一基準群」（以下「統一基準群」という。）の改定を踏まえ、統一基準群に準拠した「個人情報保護委員会情報セキュリティポリシー」（以下「ポリシー」という。）の策定及び責任者等の体制を整備し、職員に対する情報セキュリティ教育、情報セキュリティ対策に係る自己点検及び監査、インシデント発生を想定した訓練等を実施し、情報セキュリティ水準の維持・向上に努めるものとする。

また、2016年度においては、サイバー攻撃手法が高度化・巧妙化している状況の下、委員会事務局の体制拡充及び委員会が整備又は管理する情報システムの増加が見込まれることから、全ての職員において的確な対応を可能とするため、ポリシーその他の内部規程の整備及び着実な運用、教育及び訓練の徹底を図るものとする。

金融庁

2015年度の総合評価・2016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　小野　尚

近年、情報技術の高度化とその普及の進展に伴い、業務の効率化や対外的な情報発信等の観点から情報システムの活用が進む一方で、標的型メール攻撃やDDoS攻撃等に見られるように、情報の搾取や業務の遂行を脅かすことなどを企図したサイバー攻撃の脅威が高まっており、その手法は高度化・巧妙化してきている。

こうした状況を背景に、2014年11月、「サイバーセキュリティ基本法」が制定され、同法に基づき、サイバーセキュリティ政策に係る政府の司令塔として「サイバーセキュリティ戦略本部」が位置付けられたほか、2015年9月には、今後の基本的な施策の方向性を示すものとして、「サイバーセキュリティ戦略」が策定されている。

金融庁としては、サイバー攻撃による情報漏洩や重要システム稼動停止による社会的な影響を鑑み、保有する情報や情報システムの保護やシステムの可用性向上のための対策に重点を置いて取り組んできた。

しかしながら、2016年初めには、当庁のウェブサイトがDDoS攻撃を受けて閲覧できない状況が発生しており、改めて、多様なサイバー攻撃に応じた対応を網羅的に実施していくことの必要性を認識した。

この様な点に鑑み、2016年度においては、内閣サイバーセキュリティセンター等と緊密に連携を図りながら、サイバーセキュリティに関する情報を収集・分析の上、当庁におけるセキュリティに係るリスクを網羅的に評価・把握し、必要な取組みをできるものから速やかに実施して、PDCAサイクルの実践の徹底により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

2015年度の総合評価・2016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

消費者・生活者の視点に立ち様々な消費者行政を行う機関である消費者庁にとって情報セキュリティの確保は極めて重要である。特に国民から寄せられる情報や法執行前の機密情報等の意図せぬ情報漏えいなどの情報セキュリティ上の脅威が現実のものとなれば国民からの消費者行政への信頼が失墜する。以上の認識に基づき当庁における情報セキュリティ確保を確実なものとするため、情報セキュリティポリシーの整備をはじめ、そのための組織・体制の整備、職員への情報セキュリティ教育などの様々な情報セキュリティ対策の実施に取り組んできた。

2015年度は、2015年度対策推進計画に基づき、2014年度に見直した情報セキュリティポリシーに関わる周知徹底を行い、情報セキュリティ対応能力の向上を図った。また、平成27年度末に実施した中央合同庁舎４号館への庁舎移転に伴う物理的環境の変化に伴い見直すべき情報セキュリティ対策事項を整理し、情報セキュリティポリシーの見直しを実施しており、平成27年度対策推進計画は適切に実行された。当庁の情報セキュリティマネジメントの実効性については、自己点検において不審メール対策に係る点検事項について一部不備が確認されたが、情報セキュリティインシデントに繋がる事象は発生しておらず、当庁の情報セキュリティマネジメントは相応に有効に機能しているものと判断する。

2016年度は、中央合同庁舎４号館への庁舎移転に伴い変化した情報セキュリティ対策内容の他、増加するサイバー攻撃による情報漏えい事案を踏まえた情報セキュリティインシデント発生時の対応手順について、職員への周知徹底に取り組む。また、2015年度情報セキュリティ監査において指摘された課題事項や、新たなシステムの運用開始、次期消費者庁LANの要件定義の開始を踏まえ、情報セキュリティ管理についてのレベルアップに取り組むとともに、サイバーセキュリティ対策推進会議（CISO等連絡会議）の議長指示において指示された標的型攻撃等のサイバー攻撃を踏まえた技術的な対策を実施し、当庁が所管する情報システムの技術面・管理面での情報セキュリティ能力の向上を図る。

復興庁

2015年度の総合評価・2016年度の全体方針

最高情報セキュリティ責任者
総括官　吉田　光市

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。

2015年度は、全職員に対象として実施している情報セキュリティ研修に加え、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を踏まえ情報の管理等に関する留意事項の周知や標的型攻撃への対処訓練の実施など、情報セキュリティに対する職員の更なる意識の向上を図った。

また、情報セキュリティ監査については、2014年度に改正した復興庁情報セキュリティポリシーについて、政府機関の情報セキュリティ対策のための統一基準群に対する準拠性監査を実施するとともに、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遵守状況や課題等を把握することで、復興庁全体に対する情報セキュリティ対策の強化の方向性について確認を行った。

2016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にあわせて、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行うとともに、2015年度の情報セキュリティ監査の結果等を踏まえた情報セキュリティ教育のための教材の見直しなど、更なる情報セキュリティ強化のための取組、対策等を実施することにより、職員のセキュリティ意識の向上を図るとともに、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

2015年度の総合評価・2016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　黒田　武一郎

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。

○　2015年度の総合評価

2015年度は、情報システム向けセキュリティインシデント対応訓練を除き、対策推進計画に従った情報セキュリティ対策を実施した。特に全職員に対する取組として、2014年度末に改定を行った情報セキュリティポリシー（以下、「ポリシー」という。）に基づく教育を行い、新しいポリシーの周知・徹底に努めた。教育後に行った自己点検では、職員のポリシーへの認識度の向上、ポリシー遵守に関する良好な結果が得られ、省全体のセキュリティレベルの向上が図れたと評価している。

情報システム向けセキュリティインシデント対応訓練については実施計画を変更し、総務省CSIRTに対してマルウェア感染による情報流出を想定した模擬訓練を実施した。これは、2015年６月に発表された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を受け、CSIRTにおける情報セキュリティインシデントへの即応体制を強化する必要性が高いと判断したためである。

○　2016年度の計画

2016年度は、４月に新設された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体制及び対策の強化をはかる。特に、「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、内閣サイバーセキュリティセンター及び内閣官房情報通信技術総合戦略室と連携しながら、可能な限り早期に「セキュリティ・IT人材確保・育成計画（仮称）」及び「セキュリティ・IT人材育成支援プログラム（仮称）」を作成し、可能なものから順次必要な措置を講ずる。

また、2015度に実施した施策及びリスク評価の結果を踏まえ、以下の事項を重点的に実施する。また、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)標的型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、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標的型サイバー攻撃等の増加・高度化に伴い従来の教育では対応できない事例も見られることから、平成28年度は、最新のサイバー攻撃等の動向も踏まえ、従来の教育に加え、以下の教育・訓練を行う。

・ サイバー攻撃動向に対応した教育
・ 情報システム向けの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支援の実施

総務省においては、大臣官房企画課情報システム室（以下、「情報システム室」という。）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。2016年度においても、引き続き以下の支援を実施する。

・ 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

また、昨今の政府機関へのサイバー攻撃等の増加・高度化を踏まえ、情報システム室は、所管する独立行政法人において実施した各種監査結果の確認等の支援を行う。

法務省

2015年度の総合評価・2016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　黒川　弘務

法務省においては、従来から情報セキュリティ対策を推進してきたところであるが、2015年度は、政府機関等に対するサイバー攻撃等の脅威がより鮮明に顕在化したことから、対策推進計画に基づいた教育・監査等の取組のほか、サイバーセキュリティ対策推進会議議長指示等を踏まえたサイバーセキュリティ対策を適切に実施し、技術的な対策についても一層の充実を図った。

しかしながら、法務行政が果たすべき使命はますますその重要性を増しており、観光立国実現に向けた出入国手続の迅速化・円滑化及びテロリスト等に対する水際対策、国民が安全で安心して暮らせる社会の実現のための再犯防止対策やヘイトスピーチ対策、あるいは、震災復興支援や社会保障・税に関わる番号制度への対応等のための登記インフラの充実などの主要な施策が、深刻化し続けるサイバー攻撃等によって妨げられることはあってはならないことである。

そのため、社会環境の変容が一層加速することに伴う脅威の急速な増大や予見困難な新たな課題に直面することを想定し、中長期にわたる継続的な取組により、法務省におけるセキュリティ対策の総合的な強化を図る必要がある。

2016年度は、中長期的な取組の基礎となるセキュリティ対策の推進基盤を構築するために、改めて法務省全体のリスク評価を実施し、必要となる対策を洗い出した上で具体的な取組の計画を策定するほか、情報セキュリティインシデントへの対応体制であるCSIRTを含め、情報セキュリティ体制全体を最適化した上、情報セキュリティポリシー及び教育・自己点検・監査実施計画の抜本的な見直しを行い、これらの取組が後年度においても持続可能となる情報セキュリティマネジメント体制を確立することを目指す。

外務省

2015年度の総合評価・2016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

2015年度の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発生以降も、政府関係機関や重要インフラ事業者等におけるサイバー攻撃による情報漏えいの疑い、ウェブサイトの改ざん、DDoS攻撃等の事案が複数報道されている。更に国際社会においても、身代金要求型の新種のマルウェアによる攻撃やウクライナの重要インフラシステムに対するサイバー攻撃等も発生しており、情報セキュリティ強化のための情報システムやネットワーク構成の見直し、不正通信等の早期検知・監視体制強化、ソフトウェアの脆弱性への迅速な対応、専門人材の育成と一般職員教育など多層的に情報セキュリティ対策を講じていく必要性を認識している。

かかる状況下、2016年度は５月にG7伊勢志摩サミット、８月にはケニアで開催されるTICADという大規模国際会議が予定されているところ、各種構築システムに対する情報セキュリティ対策や情報管理の他、事前演習の実施、連絡体制整備において、NISC、関係省庁、その他関係機関と連携を密にするとともに、専門家の意見も取り入れつつ、万全の体制で対応に当たる。

当省においては、2015年度の外務省情報セキュリティポリシーの改正において、昨今の高度化する攻撃や対象機器の多様化への対応を盛り込んだ。2016年度は、新ポリシーに基づき、各種システムの情報セキュリティ対策強化や本省・在外公館職員への情報セキュリティポリシー遵守のための啓発を推進する。

また、本省基幹LANシステムの更新が行われたところ、ポリシー及び累次のサイバーセキュリティ対策推進会議議長指示を踏まえ、引き続き適正な運用・管理を継続していく。

更に、2016年度は政府全体の取組の一環として、2015年度実施されたシステムに対するペネトレーションテストに加え、省全体の情報セキュリティの管理体制に対するNISCによるマネジメント監査の実施が予定されている。当省としては、このNISCによる監査に全面的に協力すると共に、監査結果に基づいてPDCAサイクルを回し、更なる情報セキュリティ対策の改善を図る。

2016年度、新たに設置されるサイバーセキュリティ・情報化参事官に加え、CIO補佐官、CISO補佐官の増員を図り、情報セキュリティ体制を更に強化する。この新体制のもと、上記取組を計画的に実施し、効果的な情報セキュリティ対策の実施に努めていく。

財務省

2015年度の総合評価・2016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、件数も増加するなど、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。

2015年度においては、一般職員のセキュリティ意識の向上の観点からは、全職員を対象とした情報セキュリティ研修や標的型メール攻撃に対する訓練等を実施したほか、幹部職員も参加するセキュリティ勉強会を開催した。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等を実施した。また、システム面においては、サイバーセキュリティ対策推進会議議長指示に基づく対策を実施したほか、自己点検、情報セキュリティ監査、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。

2016年度においては、G7仙台財務大臣・中央銀行総裁会議の開催も予定しており、昨今の情報セキュリティ情勢を鑑みれば、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。そのため、引き続き、情報セキュリティに関する研修・訓練や、実効的な監査、システム面でのセキュリティ対策の強化等を実施していく。また、所管する独立行政法人・特殊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、業務の効率化を更に推進し、情報セキュリティ対策の強化を踏まえた基幹LANの構築を行う。

文部科学省

2015年度の総合評価・2016年度の全体方針

最高情報セキュリティ責任者
大臣官房長　藤原　誠

2015年度においては、近年益々、高度化・巧妙化する政府機関を狙った標的型メール攻撃等に対抗するため、以下の点を中心として情報セキュリティ対策に取り組み、技術的なセキュリティ対策の実施や研修を通じて、職員に対する情報セキュリティ意識の向上を図り、文部科学省における情報セキュリティの維持と向上に努めてきた。

(1) 情報セキュリティ研修の実施と全職員への受講徹底
(2) 情報セキュリティ自己点検による情報漏えい防止策の実施
(3) マネジメント監査対応と省内情報システムに対する脆弱性診断の実施
(4) 標的型攻撃に対応したマルウェア検知システム導入によるセキュリティ防御力の向上
(5) 情報セキュリティ関係規程の整備
(6) インシデント対応体制の強化と訓練の実施
(7) 次期行政情報システム調達における情報セキュリティ強化策の検討

2016年度においては、政府全体のセキュリティ対策方針に従って省内における情報セキュリティレベルの向上を図るとともに、2015年度に実施した脆弱性診断のフォローアップや情報セキュリティ教育の充実等を通じてPDCAサイクルの実施を徹底する。

また、2015年度に国立大学法人等において不正アクセスや情報漏えい等の情報セキュリティインシデントが多く発生している状況に鑑み、文部科学省における検討を踏まえ、文部科学省関係機関に対して必要な情報セキュリティ対策の強化を求めていくこととし、関係機関における各種取組が推進されるよう一層の支援を行うこととする。

厚生労働省

2015年度の総合評価・2016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

2015年度においては、年度当初の2015年４月15日に策定した対策推進計画において、2014年度の情報セキュリティ対策の実施状況の点検結果を踏まえ、情報セキュリティインシデント発生時の報告遅延について周知徹底を図ることとしていたところ、５月に日本年金機構（以下「機構」という。）における不正アクセスによる情報流出事案が発生した。

本事案を受け、厚生労働省（以下「厚労省」という。）は、第三者からなる検証委員会の報告（８月21日）、サイバーセキュリティ戦略本部）の原因究明調査結果（８月20日）、同戦略本部長である内閣官房長官から厚生労働大臣に対してなされた勧告（９月11日）等を踏まえ、９月18日に、本事案を踏まえた再発防止策として、「情報セキュリティ強化等に向けた組織・業務改革」を取りまとめ、公表した。

この再発防止策では、厚労省、機構ともに標的型攻撃に対する危機意識やインシデントに対処する体制、技術的対応が不十分であったこと等を反省点としつつ、厚労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、厚労省と機構の関係の強化に取り組むこととしている。

厚労省は、この再発防止策を、事実上の2015年度対策推進計画の改訂版として、2015年10月１日に大臣を本部長として設置した「情報セキュリティ強化等に向けた組織・業務改革推進本部」を中心に、

・外部専門人材の確保を含むCSIRT等の体制強化
・インシデント発生時におけるCSIRTと対処・復旧部局の役割の明確化や、CSIRT、幹部等への速やかな報告、連絡体制の構築等を内容とする情報セキュリティポリシー等の改定
・職員の危機意識やリテラシー向上のための教育・訓練の充実
・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

などに取り組んできた。

2016年度においては、引き続き、再発防止策の着実な実施に取り組むとともに、その中で新たに、CSIRT支援機能の強化、個人情報等の重要情報を取り扱う厚労省及び所管法人等のシステムに係るリスク評価、所管法人等に対する情報セキュリティ監査等に取り組むこととする。

また、2016年４月15日に成立した「サイバーセキュリティ基本法」改正法や、2016年夏を目途に予定されている「政府機関等の情報セキュリティ対策のための統一基準群」の見直しへの対応、「サイバーセキュリティ人材育成総合強化方針」（サイバーセキュリティ戦略本部決定）に基づくセキュリティ・IT人材の育成・確保についても所要の措置を講じることとする。

農林水産省

2015年度の総合評価・2016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

サイバー空間において、政府機関等が保有する機密情報等の窃取を企図した標的型攻撃が一層複雑・巧妙化する中で、農林水産省においては、情報セキュリティレベルの向上を図るため、採用者、一般職員及び部局庁等連絡員を対象とした業務内容や職責に応じた教育を実施するとともに、農林水産省情報セキュリティインシデント対応チーム（以下「CSIRT」という。）構成員等を対象とした勉強会や情報セキュリティインシデントの発生を想定した実践的演習等に努めてきたところである。

また、情報システムの脆（ぜい）弱性を突いた攻撃に備えるため、ソフトウェアの更新等の脆（ぜい）弱性対策を速やかに講じてきたところである。

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を踏まえ、職員の一層の情報リテラシーの向上を図るとともに、更なる情報システムの防御策を講ずることが必要となった。このため、最高情報セキュリティ責任者を中心に、職員に対する個人情報を含む要機密情報の管理の徹底に向け、注意喚起等を実施するとともに、省内の情報システムの点検を実施し、情報セキュリティの向上に努めたところである。

さらに、2016年１月には、「世界最先端IT国家創造宣言」（平成25年６月14日閣議決定）に基づき、省内にある18のLANシステムのうち、９のLANシステムの統合（第１次統合）を行い、この中でシンクライアントの導入等、情報システムの効率化や情報セキュリティの向上に向けた技術的な対策を実施してきたところである。

このような状況を踏まえ、農林水産省としては、2015年度に改定した農林水産省の情報セキュリティ関係規程等に基づき、情報セキュリティの確保を図ることとする。

また、内閣官房等の関係機関と連携を取りつつ、引き続き全ての職員に対し、情報セキュリティや危機管理の重要性について十分に認識するよう、情報の取扱い及び標的型メール攻撃への対応をはじめとする情報セキュリティに関する教育の実施や、標的型メール攻撃等のサイバー攻撃に対する注意喚起の徹底を行うとともに、CSIRT構成員等に対しては、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や、情報システムに関する技術的な対策等の推進を図ることとする。

経済産業省

2015年度の総合評価・2016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　嶋田　隆

2015年度においても、政府機関等を狙った標的型攻撃やDDoS攻撃などのサイバー攻撃は活発化し続け、こうした攻撃から重要な情報や業務サービス等を保護するための総合的な情報セキュリティ対策の更なる強化が迫られた。

こうした中、2015年度に当省で実施した主な取り組みは以下のとおりである。

(1) 2014年度に改正した当省情報セキュリティポリシーに基づく、各課室毎に策定している情報の管理と取扱いのルールの再整備と点検
(2) 独自に規定されていた特許庁の情報セキュリティポリシーを廃止・統合し、省全体において一元的に情報セキュリティ対策を推進
(3) 高度化する標的型メール攻撃への対処方法等に関する訓練や動画コンテンツ等を含む分かり易い教材を用いた職員教育の徹底
(4) 職員、組織、情報システムを対象とした監査・点検による情報セキュリティ対策実施状況の評価と改善
(5) 活発化・多様化するサイバー攻撃等への対処として、重要な情報システムにおけるセキュリティ強化策の技術的検討及び実施

今後、2020年の東京オリンピック・パラリンピックに向け、政府機関を含め我が国全体での情報セキュリティ対策を今まで以上に強化していくことが求められている。

このため、当省では、2016年度において、以下の方針の下、取組を実施する。

(1) 標的型攻撃に対するソフト・ハード両面での対策の更なる強化
(2) 基幹となる情報システムにおけるネットワークセキュリティの更なる強化
(3) 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
(4) サイバーセキュリティ人材育成総合強化方針に基づく環境整備と人材の育成
(5) 政府機関の情報セキュリティ対策のための統一基準群の改定を踏まえた新たな情報セキュリティポリシー等の整備

国土交通省

2015年度の総合評価・2016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　毛利　信二

最近の状況をみると、標的型メール攻撃、不正アクセスやDDOS攻撃等、政府機関等に対するサイバー攻撃は、増加・多様化・高度化の傾向にあり、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、内閣サイバーセキュリティセンターと連携して、政府統一基準を踏まえた情報セキュリティ対策を実施しており、2015年度には、高度化・多様化する攻撃に対する多重防御等の観点からシステム対策の強化を行った。

2016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、職員への研修・教育を推進する。また、５月に開催される伊勢志摩サミットや９月に開催される交通大臣会合に向けてサイバーセキュリティ対策を一層強化する。

環境省

2015年度の総合評価・2016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おける不正アクセスによる情報流出事案を発端に、益々高度化・巧妙化するサイバー攻撃に対応するため、各府省のサイバーセキュリティ対策も一層の強化が求められている。環境省においても、環境省情報セキュリティポリシー等（以下「ポリシー等」という。）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、平成27年度も環境省及び特殊会社のパソコンがサイバー攻撃によりマルウェアに感染するなどのセキュリティインシデントが発生している。

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の更改を予定しており、現状における課題（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、本システムの更改においては、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する。

また、引き続き職員等に対する教育等を実施し、ポリシー等の理解度向上と対策実践の徹底を図っていく。

更に、2016年度に予定されている「政府機関の情報セキュリティ対策のための統一基準群」の見直しに伴い、その統一基準群の適用範囲が独立行政法人等に拡大することを踏まえ、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強化する。

防衛省

2015年度の総合評価・2016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　真部　朗

2015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、2016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「自らが取り扱う情報は自らが守る。」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、職員に対して、ｅ－ラーニングを活用した情報セキュリティ教育の試行を行った。

2016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、2017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及び標的型攻撃メール訓練を実施する。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 2015」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 2015	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。	・ 2015 年３月に研究開発戦略専門調査会を開催し、外部有識者からのヒアリングを行うとともに、IoT セキュリティについての議論を行った。 ・ 2016 年３月に研究開発戦略専門調査会を開催し、各省から IoT に係る取組について意見聴取を行うとともに、IoT コンソーシアム等各府省庁連携で進めるべき案件についての進め方の検討を行った。

(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 2015	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とともに、その確認を適時確認していく。	・ 2015 年３月に研究開発戦略専門調査会を開催し、外部有識者からのヒアリングを行うとともに、IoT セキュリティについての議論を行った。 ・ 2016 年３月に研究開発戦略専門調査会を開催し、各省から IoT に係る取組について意見聴取を行うとともに、IoT コンソーシアム等各府省庁連携で進めるべき案件についての進め方の検討を行った。

(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 2015	取組の成果、進捗状況
(ア)	経済産業省	経済産業省において、IPA を通じて、IoT システムに含まれる機器等に関して、攻撃事例や利用形態を基に整理を行い、総合的なガイドラインや基準の確立に向け、脅威分析とセキュリティ対策の明確化を図る。	・ IPA において、IoT 分野の全体像の整理と具体事例に対する脅威とその対策を明確化した報告書を作成。また、IoT 機器が満たすべきセキュリティ・セーフティ等の要件について、指針として取りまとめた。
(イ)	総務省	総務省において、国際的な動向も踏まえ、IoT システムに関する横断的な取組の１つとして、M2M 機器の運用の実装上のセキュリティに係る横断的なガイドライン策定の検討を実施する。	・ 2016 年１月より、IoT 推進コンソーシアム　IoT セキュリティワーキンググループを立ち上げ、IoT セキュリティガイドラインの策定に向けた検討を開始したところ。
(ウ)	経済産業省	経済産業省において、エネルギー分野における IoT のセキュリティガイドラインとして、スマートメーターのセキュリティの評価技術・手順の実証を行う。	・ スマートメーターシステムにおけるセキュリティ評価実証を行い、有効な評価技術・評価方法を構築した。さらに、スマートメーター制度検討会セキュリティ検討ワーキンググループの報告書を基に、日本電気技術規格委員会（JESC）において、スマートメーターシステムに係るセキュリティガイドラインを策定した。
(エ)	厚生労働省 経済産業省	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検討を進める。	・ 厚生労働省において、医療機器サイバーセキュリティ確保に関するガイダンスを策定すべく、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について検討を行った。 ・ 経済産業省において、産学官で連携し、医療機器に係る情報セキュリティに関する情報（リスク・対応事例、関連ガイドライン等）の収集・分析・周知を進めた。

（オ）	総務省	総務省において、自動車分野における IoT のセキュリティガイドラインとして、「700MHz 帯安全運転支援システムのセキュリティガイドライン」を策定する。	・ 700MHz 帯安全運転支援システムを構築するための指針について、総務省に設置した「情報セキュリティアドバイザリーボード　ITS ワーキンググループ」での検討結果を基に、平成 27 年７月９日、「700MHz 帯安全運転支援システム構築のためのセキュリティガイドライン」を策定した。
（カ）	経済産業省	経済産業省において、CSSC を通じ、IoT システムの構成要素である 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認証制度を確立する。	・ EDSA 認証（2014 年４月開始）について、説明会の開催や HP での普及・啓発を行い、2015 年度は１製品の認証を行った。また、制御システム全体のセキュリティ評価・認証に向けて、制御システムセキュリティ国際標準 IEC 62443 の規格要求事項を整理した。
（キ）	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 を通じて、SHODAN などのインターネット上の公開情報を分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステム 51 件(複合機含む）について、その保有組織に対して情報提供した。
（ク）	経済産業省	経済産業省において、経済産業省告示により指定された 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制度」により、IoT システムを作動させるソフトウェアに係る脆弱性について、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」などを通じて、利用者に提供する。また、IPA（受付機関）と JPCERT/CC（調整機関）は、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、経済産業省告示に基づいた手続きの上、公表を行う。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。	・ 2015 年度は、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、ソフトウェア製品の脆弱性について 431 件、ウェブサイトの脆弱性について 413 件の届出を受け付け、調整が整った案件など 171 件のソフトウェア製品にかかる脆弱性に関する情報を、JVN 等を通じて利用者に提供した。IoT システムを作動させるソフトウェアに係る脆弱性は４件を公表。 ・ JPCERT/CC では、ISC BIND/DHCP、NTP、Apache、OpenSSL 等脆弱性の影響範囲が広い製品について、製品開発者が公表したアドバイザリ情報を日本語化し、公表している。2015 年度は 142 件を公表し、そのうち IoT システムを作動させるソフトウェアに係る脆弱性の情報は 30 件。
（ケ）	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検討を実施する。	・ 2016 年１月より、IoT 推進コンソーシアム　IoT セキュリティワーキンググループを立ち上げ、IoT セキュリティガイドラインの策定に向けた検討を開始したところ。

(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 2015	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品質、安全性、効率を向上、両立させるための革新的、先端的技術の基礎研究に取り組む。	・ 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、大規模ソフトウェアの解析ツールを開発し、自動車等組込みシステムを題材に有効性を検証した。暗号技術においては、暗号化したままデータ処理や認証・認可を実現する高機能暗号技術について、高速処理を可能とする新方式や暗号文サイズが世界最小値となる技術を開発した。
（イ）	総務省	総務省において、IoT システムの構成要素の特徴を加味したセキュリティ技術の確立に向けた調査・実証を実施する。	・ 「M2M セキュリティ実証事業」においてウェアラブル機器やセンサー機器のような IoT 機器における適切な暗号機能の実装手法や運用上の課題について実証事業を実施。
（ウ）	経済産業省	経済産業省において、CSSC における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、制御システムのテスト環境を用いたシステムの脅威と対策に関する技術開発を行い、制御システムセキュリティ国際標準 IEC 62443 の規格要求事項の整理や、サイバー演習でのシナリオ作成に活用した。
（エ）	総務省	総務省において、IoT システムにおけるセキュリティ技術の確立に向け、IoT 機器及びその運用基盤に対する脅威分析及びリスク評価を行う。	・ 「M2M セキュリティ実証事業」においてウェアラブル機器やセンサー機器のような IoT 機器における適切な暗号機能の実装手法や運用上の課題について実証事業を実施。

（オ）	総務省 経済産業省	総務省及び経済産業省において、IoT 機器へのバックドア対策のためのログ検知技術の開発に関する研究や、高信頼な暗号の実装を実現する技術やハードウェアトロージャン検知の技術等ハードウェアの真正性の向上に係る技術の開発に関する研究、IoT システムに対応したセキュリティ評価認証制度の確立に向けた検討を行う。	・ 多様な機器が接続される IoT システムにおいて、制御機器向けのビッグデータ I 等を用いたサイバー攻撃の予測技術と自動更新技術や、末端のセンサー等の IoT 機器に搭載でき、膨大なデータを低消費電力で暗号化する技術を開発するための予算化を行った。また、内閣府と連携して、ログ検知技術や、小型で強固な暗号処理とハードウェアトロージャン対策が講じられたセキュアチップの開発等を実現するための研究プログラム（SIP）立ち上げに協力を行った。
（カ）	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。	・ 自動走行システムの共通モデル構築に向けて調査を実施しモデル案を作成した。また、車両に対する攻撃への対策技術の評価方法を検討するため、他業界での攻撃事例を収集した。

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 2015	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。	・ サイバーセキュリティを事業戦略の一つとした企業経営について検討するため、普及啓発・人材育成専門調査会の下に、セキュリティマインドを持った企業経営ワーキンググループを設置し、検討を行っているところ。
（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、サイバーセキュリティ対策の在り方、CISO の設置を含めた組織体制の在り方、技術的対策、情報開示の在り方等を含めたサイバーセキュリティ経営ガイドラインを年内のできるだけ早期に策定する。また、当該ガイドラインも含めた企業の取り組みについて、第三者認証等によりステークホルダー等から評価される仕組みを検討する。さらに、経済産業省において、実効性を高めるため、同ガイドラインの内容や利活用の在り方も含めた指針の法制度化を、中小企業向けも含めて検討する。	・ 2015 年 12 月、経済産業省と IPA にて、「サイバーセキュリティ経営ガイドライン」を策定、公表した。また、経済団体や企業に説明を行うなど、普及活動を行った。
（ウ）	経済産業省	経済産業省において、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り組みを、加点要素等として考慮する仕組みを検討する。	・ 補助事業等の採択に際して、企業のサイバーセキュリティ対策への取り組みを加点要素等として考慮する仕組みを検討した。

(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 2015	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、実務者層のリーダー層が「橋渡し人材層」として活躍できるよう、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伝えていくコミュニケーション能力の向上を図るためのセミナー等を実施する。	・ 企業の経営層に対し経営戦略としてセキュリティ・バイ・デザインを位置づけることの重要性について、内閣官房から、経済団体の委員会等で説明したほか、業界団体等が主催する行事等の機会を捉えて経営層に対する意識啓発を行った。

(3) 組織能力の向上

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、企業における製品・サービスの関係者を対象に、セキュリティ・バイ・デザインを共通の価値として認識させることを目指したセミナーの開催等の普及啓発活動を行う。	・ 企業の経営層に対し経営戦略としてセキュリティ・バイ・デザインを位置づけることの重要性について、内閣官房から、経済団体の委員会等で説明したほか、業界団体等が主催する行事等の機会を捉えて経営層に対する意識啓発を行った。
(イ)	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 は、開発者啓発を目的としたセミナー、大学、カンファレンスで計 9 回講演等を実施（2015 年度）し、そのうち 1 回は海外での開催である。また、開発者向けセキュアコーディング関連の資料の公開を計 5 回実施し、うち一つは査読付き論文として採択されたものもある。主なものとして、2015 年 6 月 JASPAR　セキュアコーディング概論、2015 年 10 月 JavaOne 2015 ″Case Studies and Lessons Learned from Certificate Validation Vulnerabilities″ などがある。
(ウ)	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、最新のサイバー攻撃の手口を踏まえたサイバーセキュリティ対策の在り方、組織体制の在り方、最新の攻撃に対する技術的対策、情報開示の在り方等を含めたサイバーセキュリティ経営ガイドラインを年内のできるだけ早期に策定し、企業に対して発信していく。また、当該ガイドラインも含めた企業の取り組みについて、第三者認証等によりステークホルダー等から客観的に評価される仕組みを検討する。	・ 2015 年 12 月、経済産業省と IPA にて、「サイバーセキュリティ経営ガイドライン」を策定、公表した。また、経済団体や企業に説明を行うなど、普及活動を行った。
(エ)	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。	・ 2015 年 12 月、経済産業省と IPA にて策定した「サイバーセキュリティ経営ガイドライン」において、IT システム管理を外部委託する場合、当該委託先にもサイバーセキュリティの確保をさせることが必要であることを明記。
(オ)	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計ることにより、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 2015 年度当初の 83 組織から 137 組織（2016 年３月末時点）に拡大した。さらに、早期警戒情報の受信対象組織の拡大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・支援した。早期警戒情報の受信組織数は、2015 年度は 177 組織から 233 組織（2016 年３月末時点）に拡大した。また、広く国内の企業組織における CSIRT の設立と、高度サイバー攻撃対策の促進のため、CSIRT マテリアルの改訂版（2015 年 11 月）、および高度サイバー攻撃への備えと対応ガイド（2016 年 3 月末予定）を一般公開した。
(カ)	総務省	総務省において、企業における標的型攻撃への対処能力の向上に向けた実践的な防御演習（CYDER）を実施する。	・ 2015 年 10 月より、官公庁・重要インフラ事業者等の LAN 管理者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）を計７回実施。（含：National 318 EKIDEN 2016）
(キ)	経済産業省	経済産業省において、企業への標的型攻撃への対処能力向上のため、CSSC における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。
(ク)	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 のサイバーレスキュー隊（J-CRAT）内に併設された「標的型サイバー攻撃の特別相談窓口」の運営を通して情報収集に努め、標的型サイバー攻撃の情報提供、相談を通じレスキュー活動 160 件（内オンサイト：39 件）を実施。 ・ 2015 年にレスキュー活動を効率化、高度化する設備を整備し、運用を開始（2015/10）。

（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。	・「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を IPA のウェブサイトで継続公開。 － オンラインでの利用件数：1,582 件 － オフライン版のダウンロード数：4,357 件
（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 が運営する「サイバー情報共有イニシアティブ」（J-CSIP）を通じて、サイバー攻撃に関する情報共有を着実に実施。 ・2012 年から 2015 年の 3 年間の情報共有活動における情報の集約・分析の成果として、国内組織を執拗に狙う攻撃の実態を明らかにし、「攻撃者 X の分析」として公開（2015/5）。 ・日本の基幹産業の 1 つである自動車業界を対象とした、「自動車業界 SIG」（10 組織）を新たに設立（2016/1）。 ・化学業界 SIG へも 3 組織が新たに参加。これにより、J-CSIP の参加組織数は 59 組織から 72 組織に拡大。
（サ）	総務省	総務省において、ISP 事業者を中心に構成されている「Telecom-ISAC Japan（一般財団法人データ通信協会テレコム・アイザック推進会議）」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。	・関係者による情報共有を促進・円滑化し、ICT 分野全体にわたる情報共有機能を強化するため、「Telecom-ISAC Japan」を核としたサイバー攻撃に関する情報共有網の拡充を進めるべく、平成 28 年３月に「ICT-ISAC」が設立されたところ。
（シ）	金融庁	金融庁において、金融機関に対し、2014 年 11 月から本格的に活動を開始した「金融 ISAC」を含む情報共有機関等を通じた情報収集・共有体制の構築を促していく。	・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、機会を捉えて周知すること等により、2016 年３月末現在、「金融 ISAC」の加盟社は 172 社まで増加した。

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 2015	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 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。	・NEDO と連携し、セキュリティ技術研究のための先導的な研究開発を進めるための支援事業を開始し、我が国のセキュリティ産業育成のための基盤構築に貢献。また、産革機構と連携し、先端的なセキュリティ技術への投資案件 1 件の形成が実現。
（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。	・JASA において、いわゆる「見える化」の一環として、CS マーク（クラウドセキュリティガイドラインに基づく情報セキュリティ対策を実施している旨の言明の内容がクラウド情報セキュリティ監査により確認されたことを示す標章）の発行を本格的に開始。当該マークを取得した企業は JASA のホームページにおいても公開されている。 ・総務省において、JASA と連携し、クラウドセキュリティガイドラインの普及・促進を行った。
（ウ）	総務省 経済産業省	総務省及び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関連税制の利用促進等、中小企業の情報セキュリティ対策の底上げを支援する施策を推進する。	・中小企業者等の少額減価償却資産の取得価額の損金算入の特例及び中小企業投資促進税制について、説明会の開催等、中小企業の利用促進のための取組を実施した。
（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。	・法制的に難しい論点を含むものであるため、現時点で措置を講ずるには至っていないが、引き続き、文化庁において法制的な検討を行っている他、文化審議会著作権分科会においても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、現在検討を行っているところである。

(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 2015	取組の成果、進捗状況
(ア)	経済産業省	経済産業省において、関係省庁及び産業界の協力の下、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、「営業秘密官民フォーラム」を設置する。	・ 官民の実務者間において、営業秘密の漏えいに関する最新手口やその対応策に係る情報交換を行う場として、関係省庁、及び 17 の関係団体・法人からなる「営業秘密官民フォーラム」を設立。平成 27 年７月７日に第１回を開催し、関係省庁から最新の手口やその対応策を報告すると共に、独立行政法人情報処理推進機構（IPA）からサイバーセキュリティ対策について最新状況の紹介を行った。
(イ)	経済産業省	経済産業省において、企業の重要情報である営業秘密の管理手法等の一層の高度化に資するため、人事・労務面、情報セキュリティなど多面的な対策について、最新の技術開発や内外の不正な営業秘密侵害事例を踏まえ、「営業秘密保護マニュアル（仮称）」として策定し、公表する。	・ 営業秘密として法的保護を受けられる水準を越え、秘密情報の漏えいを未然に防止するための様々な対策を「秘密情報の保護ハンドブック～企業価値向上に向けて～」として策定し、平成 28 年２月８日に公表した。
(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。	・ IPA において、内部不正防止のためのガイドライン普及のためのセミナー・シンポジウム（共催を含む）を計４回（1,245 名）、講師派遣依頼での講師を 20 箇所にて実施し、普及に努めた。また、内部不正の防止に向けた環境整備を促進するため、内部不正の実態調査を実施し、３月に公表した。
(エ)	経済産業省 外務省	経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（「Forced Localization Measures」）を行う諸外国に対し、対話や意見交換を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう，民間団体とも連携しつつ働きかけを行う。	・ 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サミット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 2015	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、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（2015 年９月、2016 年３月）に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積極的に参加・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等に参加し、制御システムセキュリティに関わる国際標準化を推進した。

（イ）	経済産業省	経済産業省において、IPA を通じ情報セキュリティ分野と関連の深い国際標準化活動である ISO/IEC JTC1/SC27 が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。	・ IPA の事業における成果等を国際標準に適用し、国内の情報セキュリティ活動において円滑な対策の実施等を行うことができるように、SC27 国際会合に出席し、ISO 国際標準に対する改善案や新規の標準作成等に関して提案を実施（平成 26 年 4 月、10 月）。IPA より、WG2（暗号とセキュリティメカニズム）や WG3（セキュリティの評価・試験・仕様）を中心に、関係する会議全体をカバーできる人員を派遣し、日本の代表としての意見を国際会議に反映。 ・ WG2 では、コンビーナ（主査）として国際的に暗号技術の標準化に大きく貢献。日本発の技術の規格 3 件を発行。 ・ WG3 では、副コンビーナとして、議論を牽引。国内主査として各種提案活動の支援。暗号モジュールの認証に用いられる国際標準 ISO/IEC 19790 及び ISO/IEC 24759 について、JIS 原案作成を通じて得られた知見を反映した正誤表を作成し、国際会合での議論を経て訂正再発行を行った。また、ISO/IEC 19790 と組み合わせて使用される国際標準 ISO/IEC 18367 について意見をとりまとめ、標準化を完了した。
（ウ）	経済産業省	経済産業省において、2014 年に改訂した「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」を新たな国際標準（ISO/IEC27017）のベースとして組み入れるべく、国際標準化を推進する。	・ 2015 年 12 月 15 日付けで、ISO27017 は発行された。
（エ）	経済産業省	経済産業省において、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ脆弱性対策に関する SCAP、CVSS 等の国際的な標準化活動等に参画し、情報システム等の国際的な安全性確保に寄与する。	・ 経済産業省において、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。
（オ）	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に貢献するとともに、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、我が国のベンダーが国際的な市場をもつ複合機分野において、最大の供給相手国である米国の認証機関及び複合機ベンダーと協力し、複合機のセキュリティ要件（PP)を開発。当 PP はすでに米国の調達のための PP として指定されている。
（カ）	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 ヶ国・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。	・ ITPEC は継続的にアジア統一試験を実施(2015 年度：２回開催）。 ・ 2015 年度はトップガンプログラムを通じ、ITPEC 試験合格者で特に優秀な者をアジアトップガン人材として 13 名選出し、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。
（キ）	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、日本企業が安全に活動でき、また、日本の持つノウハウを 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、「ASEAN 地域の重要インフラ関係者等に対する情報セキュリティ強化支援」研修を実施し、ASEAN 諸国の官民関係者に対し情報セキュリティマネジメントシステム（ISMS）の構築・運用方法や制御システムセキュリティの最新動向、IPA が運用する IT セキュリティの認証制度（JISEC）等について知見を提供した。
（ク）	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。	・ JPCERT/CC では、ASEAN 加盟国であるタイのバンコクにおいて、2015 年 7 月 16 日、17 日の二日間にわたり Java および Android アプリ開発者を対象としたセキュアコーディングセミナーを実施した。初日は Java プログラミングに関する講義とハンズオンを、2 日目は Android アプリ開発のセキュアコーディングとして、脆弱性事例ベースの座学と脆弱性検証のハンズオン、セキュリティコードレビューを実施した。

（ケ）	経済産業省	経済産業省において、CSSC が実施している制御システムセキュリティにかかる認証制度について、国際標準化の推進とそれをベースにした国際的な相互承認の対象制度の拡大を推進する。	・ IEC62443 に基づく制御システムセキュリティに関わる国際標準化を推進すると共に、制御システムの国際的な相互承認の対象制度の拡大も念頭に、制御システムの評価技術・手法の検討を行った。

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 2015	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、事業者のセキュリティ・バイ・デザインに対する取組を促すとともに、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行う。	・ 企業の経営層に対し経営戦略としてセキュリティ・バイ・デザインを位置づけることの重要性について、内閣官房から、経済団体の委員会等で説明したほか、業界団体等が主催する行事等の機会を捉えて経営層に対する意識啓発を行った。 ・ 各府省庁とは、サイバーセキュリティを事業戦略の一つとした企業経営について検討するため、普及啓発・人材育成専門調査会の下に、セキュリティマインドを持った企業経営ワーキンググループを設置し、検討を行っているところ。
(イ)	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 は製品開発者啓発を目的としたセミナー、大学、カンファレンスで計９回講演等を実施（2015 年度）し、そのうち１回は海外での開催である。また、開発者向けセキュアコーディング関連の資料の公開を計５回実施し、うち一つは査読付き論文として採択されたものもある。主なものとして、2015 年６月 JASPAR　セキュアコーディング概論、2015 年 10 月 JavaOne 2015 ″Case Studies and Lessons Learned from Certificate Validation Vulnerabilities″ などがある。
(ウ)	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、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）については、改訂作業（セキュリティ含む）を実施し、2016 年３月に原稿案を作成した。当該案については、2016 年５月までにパブリックコメントを募り、完成版として 2016 年６月に出版する予定。
(エ)	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」と体験的かつ実践的に学ぶツール「AppGoat」について IPA を通じて普及啓発を図る。	・ IPA において、「安全なウェブサイトの作り方 改訂第７版」をウェブ上で継続して公開。 ・ 脆弱性体験学習ツール「AppGoat」を IPA のウェブサイトで公開。 － ダウンロード数：5,921
(オ)	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、製品・サービス等の異なる 20 の業界団体・機関等（具体的には 27 団体・機関）に対し、情報処理システムの信頼性の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い、2016 度の計画に反映した。さらに、「ソフトウェア品質説明のための制度ガイドライン」に基づいた、品質関連の制度の構築を目指す一般社団法人ディペンダビリティ技術推進協会に対して、認証制度の開始（2015 年６月）に向けた支援等を行った。また、品質説明力強化に向けて、2015 年６月に出版した「つながる世界の品質ガイド」については、関連セミナーを実施するとともに、430 部以上を販売。普及啓発を推進した。

（カ）	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。また、連絡不能案件について、経済産業省告示に基づいた手続きのうえ、公表を行う。	・ 2015 年度は、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、ソフトウェア製品の脆弱性について 431 件、ウェブサイトの脆弱性について 413 件の届出を受け付け、171 件のソフトウェア製品にかかる脆弱性に関する情報を、JVN 等を通じて利用者に提供した。このうち２件は、公表判定委員会による公表判定を受けて公開された連絡不能開発者が提供するソフトウェア製品に関するものである。また、JPCERT/CC では、ISC BIND/DHCP、NTP、Apache、OpenSSL 等脆弱性の影響範囲が広い製品について、製品開発者が公表したアドバイザリ情報を日本語化し、公表しており、2015 年度は 142 件を公表した。
（キ）	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 フィードの配信において、安定した情報発信を継続するために情報発信基盤を再構築した。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。
（ク）	経済産業省	経済産業省において、IPA を通じ、情報システムの脆弱性に対して、プロアクティブに脆弱性を検出する技術の普及・啓発活動を行う。	・ 経済産業省において、IPA を通じ、情報システムの脆弱性に対して、「ファジングセミナー」を開催する等、プロアクティブに脆弱性を検出する技術の普及・啓発活動を実施。 － セキュリティテスト「ファジング」セミナーを開催（2016/10/8、2016/3/14）。 － その他、セキュリティキャンプ全国大会（2015/08/10-15）でセミナーを開催。
（ケ）	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。	・ ダークネット観測センサーを 30 万アドレスへ拡張、海外へのセンサー設置を実現、また、高機能センサー「Ghost Sensor」を開発し長期運用試験を実施した。地方自治体へ DAEDALUS への加入を進め 500 以上の自治体へアラート提供を実施した。
（コ）	総務省	総務省において、高度化・巧妙化するマルウェアの被害を防止するため、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）を引き続き実施する。	・ 関係機関等と連携しながら、引き続き利用者のマルウェア感染駆除及び感染防止の取組を実施しているところ。2015 年度においては、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」を踏まえ、マルウェアと C&C サーバ間の通信を抑止するとともに、マルウェアに感染した端末の利用者への注意喚起を行うことで被害を軽減する取組を新たに実施。
（サ）	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情報共有システム（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、2015 年度は、モンゴルとモロッコの CSIRT が新たに TSUBAME に加盟した。また、ラオスの CSIRT へのトレーニングや多くの TSUBAME 参加組織が集まる APCERT 年次会合にあわせて Workshop を開催した。また、APCERT 年次会合が OIC-CERT の年次会合と合同開催であったため、TSUBAME について OIC-CERT メンバーに説明を行い加盟に向けた活動を行った。この中で技術的な内容の発表等を通じて、既存のメンバーに対してセンサーの安定稼働を維持する取り組みを計った。

（シ）	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2015年度は207ブランド、3,111件の URL について、14,393 件の報告を受けた（2016 年３月末時点）。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３月末現在で約 2,000 のフィッシングサイト閉鎖の対応を行った。そのうち 85% 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を 2015 年７月に、またフィッシングレポート 2015 を 2015 年９月にそれぞれ公開した。
（ス）	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。	・ サイバーセキュリティ注意喚起サービス「icat」を IPA のウェブサイトで継続提供。 -利用中のウェブサイト数：739 ・ Adobe Flash Player の利用を前提としない「icat for JSON」を 2016 年２月に公開。 -利用中のウェブサイト数：288
（セ）	警察庁	警察庁において、公衆無線 LAN を悪用したサイバー犯罪に対する事後追跡可能性の確保に必要な対策について検討する。	・ 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について検討した。
（ソ）	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。	・ 無線 LAN のセキュリティに関する周知啓発セミナーを５回実施。また、無線 LAN におけるセキュリティ対策の検討を実施。

(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 2015	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に関する普及啓発活動を推進する。特に、「サイバーセキュリティ月間」を中心とし、シンポジウムやサイバーセキュリティカフェ等の活動を通じ普及啓発活動を進めるとともに、児童生徒やその保護者ならびに学校の教職員を対象とした啓発活動や、サイバー空間の脅威や対策について学ぶ機会の少ない者に対する取組も推進する。	・ 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、様々な取組を実施した。 ・ 「新・情報セキュリティ普及啓発プログラム」（平成 26 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、本月間においてマルチメディアコンテンツ「攻殻機動隊 S.A.C.」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 2015 年８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。 ・ 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、2015 年 10 月のサイバーセキュリティ国際キャンペーン及び 2016 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	総務省において、「サイバーセキュリティ月間」に合わせて、全国でサイバーセキュリティ関連セミナーを実施するとともに、総務省「国民のための情報セキュリティサイト」を通じて最新のセキュリティトピックに関する普及啓発を実施する。	・ 無線 LAN のセキュリティに関する周知啓発セミナーを５回実施。
（エ）	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。	・ 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。
（オ）	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」の実施や「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、関係者と連携して周知啓発のための取組を行う。	・ 「春のあんしんネット・新学期一斉行動」として、総合通信局等や関係省庁、関係事業者・団体等と協力し、各地域において、スマートフォン利用における注意点に関する啓発活動や、「e-ネットキャラバン」を含む青少年のインターネットリテラシー向上のための啓発講座等を集中的に実施した。また「e-ネットキャラバン」については、総合通信局等の職員を講師として派遣する、新規協力団体・講師の獲得に協力する等、推進体制の強化を支援した。
（カ）	文部科学省	文部科学省において、児童生徒への指導に役立つ教員用動画教材及び指導手引書や子供たちがインターネット上で遭遇する課題について保護者向けの普及啓発教材を作成・普及する。	・ 文部科学省において、児童生徒への指導に役立つ教員用動画教材及び指導手引書や保護者向けの普及啓発教材を作成した。
（キ）	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、フォーラム（東京で１回）、ネットモラルキャラバン隊(全国７カ所)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。	・ 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、フォーラム（東京で１回）、ネットモラルキャラバン隊（全国７カ所）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した。
（ク）	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」を一般国民に提供する。	引き続き、IPA のウェブサイトにおいて、「情報漏えい対策ツール」を提供。ダウンロード件数：9,177 件。
（ケ）	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／セキュリティ意識の醸成と向上を図るため、標語・ポスター・４コマ漫画等のコンクールを主催。全国の小中高校にコンクール作品募集を呼掛け、応募作品 66,858 作品（標語 46,444／ポスター4,574／4 コマ 7,763／書写：3,781／行動宣言 4,296）を得た。

（コ）	内閣官房	内閣官房において、関係省庁と協力し、関係府省庁が既に設置している情報セキュリティに関する相談窓口について、国民・利用者の視点に立ち、連携を強化するなど、相談体制を充実させる。	・ サイバーセキュリティの普及啓発活動を促進するため、「みんなでしっかりサイバーセキュリティ」サイトのリニューアルオープンをして、関係省庁及び関係機関が設置した相談窓口や届け出窓口に関する情報を集約した。
（サ）	内閣官房	内閣官房において、産学官民が協議会等の形で連携し、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」等を活用しつつ必要な取組について検討を進める。	・ 2015 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、普及啓発活動に関する意見交換を行った。
（シ）	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 78 ヵ所にてインターネット安全教室を開催（内、新規開催５ヵ所、参加者 4,373 名）。
（ス）	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（250 件実施）やイベント（第 12 回情報セキュリティ EXPO[春]等）への出展等による情報の周知・提供を行った。 ■イベントの主催・出展（主なもの） 第 12 回情報セキュリティ EXPO[春]の出展(5/13-5/15) 来場者 10,639 名 サイバーセキュリティイニシアティブ 2015(7/2) 参加者約 150 名 ITpro EXPO オープンシアターの出展(9/30-10/2) 来場者約 400 名 その他、広報主管の IPA シンポジウムや SEC 主管の CEATEC など含め 14 のイベントに主催・出展 ■全国の団体等からの要請による講師派遣 250 件実施
（セ）	総務省	総務省において、関係機関と協力のうえ、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。	・ J-LIS において研修を実施。 ■集合研修(実績) －ICT-BCP セミナー ２回開催、受講団体数：82 団体、受講者数：87 人 －情報セキュリティ監査セミナー ３回開催（うち１回は追加開催）、受講団体数：124 団体、受講者数：137 人 －情報セキュリティマネジメントセミナー ３回開催（うち１回は追加開催）、受講団体数：125 団体、受講者数：141 人 －トピックスセミナー １回開催、受講団体数：142 団体、受講者数：174 人 ■ｅラーニング －情報セキュリティ研修(実績) ９コース、受講団体数：802 団体、受講者数：230,628 人
（ソ）	総務省	総務省において、関係機関と協力のうえ、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。また、地方公共団体における緊急時の対応について、マニュアルを提供する等支援する。	・ 総合行政ネットワーク（LGWAN）内のポータルサイトにおいて、情報セキュリティ事件事故事例の紹介、地方公共団体における情報セキュリティ対策の取組事例のほか、情報セキュリティ技術に関する解説等の資料提供を行った。 ・ 地方公共団体における緊急時の対応について、情報セキュリティインシデント対応ハンドブックを作成し全地方公共団体に対し提供した。

（タ）	総務省	総務省において、関係機関と協力のうえ、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、脆弱性対策の知識向上を目的に実技形式の講習会等を全国２カ所で開催する。	・ 公開サーバやネットワーク機器等における脆弱性診断を 400 以上の地方公共団体に対し実施するとともに、Web 感染型マルウェアによる改ざん検知を、全都道府県及び全市区町村のホームページ等を対象に毎日巡回して実施した。 ・ 脆弱性対策の知識向上を目的とした実技形式の講習会を２か所（東京、大阪）で開催した。
（チ）	総務省	総務省において、実践的な防御演習（CYDER）を、ものづくりの源泉としてサプライチェーンの一端を担う中小企業にも積極展開し、標的型攻撃への対処能力の向上を図る。	・ 2015 年 10 月より、官公庁・重要インフラ事業者等の LAN 管理者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）を計７回実施（含：National 318 EKIDEN 2016）。
（ツ）	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。	・ IPA において、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講習能力養成セミナーを全国 30 か所で開催 （参加者 1,782 名）するとともに、経営指導員向け研修会（58 回）や税理士向け研修会(13 回)への講師派遣を行い、啓発資料等の利用促進を図った。また、情報セキュリティ対策支援サイト「iSupport」への登録は、プレゼンターが累計 570 名、一般ユーザーが累計 9,560 名に増加。
（テ）	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 において、「今月の呼びかけ」や長期休暇前の注意喚起、突発的に明るみになった脅威に対する注意喚起など、21 件の情報を発信。 ・ 脆弱性や攻撃に対する「緊急対策情報」、「注意喚起情報」の発信。 － 緊急対策情報：17 件 － 注意喚起情報：11 件
（ト）	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相談窓口」を通じ、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り組みを支援する。	・ IPA の「情報セキュリティ安心相談窓口」では、15,143 の相談を受け付け、対応を実施。また、「標的型サイバー攻撃の特別相談窓口」では、537 件の相談を受け付け、対応を実施。
（ナ）	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、2014 年度のサイバーセキュリティの脅威・対策・政策に関する動向をまとめた「情報セキュリティ白書 2015」を 2015 年７月１日に出版した。また、同年７月 23 日には電子書籍版も発行した。 ・ IPA において、インターネット利用者を対象に、情報セキュリティの脅威・倫理に対する意識調査を実施し、結果を 12 月 24 日に公開した。調査によれば、悪意の投稿経験がある利用者は 24.7%で、昨年比で約 3%増加した。 ・ IPA において、企業の経営者やリスク管理責任者等を対象に、サイバーリスクに対する体制整備の状況やリスク移転の手段であるサイバー保険の活用実態を把握する調査を実施し、結果を６月 30 日に公開した。

(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 2015	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、各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。 ・ 「サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進」をテーマに平成 27 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。
(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。 ・ 2015 年中の不正アクセス行為の発生状況等を 2016 年３月 24 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。	・ 都道府県警察において、平成 26 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、2015 年末現在の全国のサイバー防犯ボランティア数は、224 団体 9,406 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。	・ 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研究・研修センターにおいて、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初めとする全部門の捜査員を対象に、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は米国 APWG と連携し、同組織およびその会員との情報交換を行っている。2015 年度は、APWG が主催するカンファレンスである APWG eCrime 2015 （2015 年 5 月 26-29 日 バルセロナにて開催）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は、協議会内のワーキンググループ活動を通じてフィッシング対策ガイドラインの改定内容に反映された。改定版のガイドラインは 2016 年度初頭に公開の予定である。
（ク）	警察庁	警察庁において、多様化・複雑化するサイバー犯罪に適切に対処するため、高度情報技術解析センターを中心に不正プログラムの効率的な解析を推進するとともに、サイバー犯罪捜査に従事する警察職員に対する研修の実施、資機材の増強、関係機関との協力等を通じ、デジタルフォレンジックに係る体制を強化する。	・ デジタルフォレンジック用資機材を増強した。 ・ 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、2015 年においては、948 件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研究・研修センターにおいて、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初めとする全部門の捜査員を対象に、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）
（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案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」の解説の改正を踏まえ、関係事業者における適切な取組を推進するなど必要な対応を行う。	・ 警察庁及び総務省において、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」の解説の改正を踏まえ、関係事業者への周知を図り、関係事業者における適切な取組を推進するなど必要な対応を行った。

2.2. 重要インフラを守るための取組

項番	担当府省庁	サイバーセキュリティ 2015	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、本年度内を目途に、更なるセキュリティ強化等の具体的内容について取りまとめる。	・ 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つの施策を着実に実施した。 ・ サイバー攻撃の深刻化や、サイバーセキュリティ戦略等を踏まえ、重要インフラ防護に関する検討課題を整理し、2016 年３月にサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」を決定した。

（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実施する。その調査結果を踏まえ、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、課題の抽出を行う。	・ 内閣官房において、重要インフラ所管省庁の協力も得た上で、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に関する調査を実施するとともに、具体的な今後の取組方針を「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」においてとりまとめた。 ・ 経済産業省において、電力分野に関して、スマートメーターシステム、制御系システムの安全基準を策定し、電気事業法における保安規制に位置付けることについて検討している。
（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、2015 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、同施設のセンサー17 か所を 2015 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、シミュレーション等を実施した。
（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。	・ 2014 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、2015 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、2015 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	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、重要インフラにおける標的型攻撃への対処能力を向上させ、重要インフラの持続的なサービス提供に向けた実践的な防御演習（CYDER）を実施する。 ・ 経済産業省において、CSSC を通じて、重要インフラ等企業における標的型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。	・ 内閣官房において、2015 年 12 月に、情報セキュリティインシデント発生時の組織内外との情報共有体制の構築・改善、事業継続計画（BCP）等の策定・改訂の検証を図ることを目的として、全 13 重要インフラ分野や所管省庁等の 302 組織 1,168 名の参加を得て分野横断的演習を実施した。 ・ 総務省において、2015 年 10 月より、官公庁・重要インフラ事業者等の LAN 管理者のサイバー攻撃への対処能力向上のため、National 318 EKIDEN 2016 を含め、実践的サイバー防御演習（CYDER）を計７回実施。 ・ 経済産業省において、2016 年１月から２月までにかけて、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。

(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 2015	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等との連携の下、2020 年の東京オリンピック・パラリンピック競技大会をテストケースとして、情報システムの障害が当該大会の開催に重大な影響を与えるサービス、それを提供する事業者及びその分野の候補を選定すると共に、所管省庁や事業者が行うリスク評価を支援するための手順を整備する。前記取組により得られた知見も活用し、新たな重要インフラ分野や事業者の候補を選定する。	・ 内閣官房において、重要インフラ所管省庁等と連携し、大会運営に係る重要システム・サービスの候補を抽出するとともに、一部の事業者に対して NISC で作成したリスク評価手順案のトライアル実施を依頼し内容の充実を図った。

（イ）	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、取組を拡大する対象として、重要インフラ事業者等が提供するサービスに間接的に関わる外部委託先や主要関係先の洗い出しを行う。	・ 内閣官房において、第３次行動計画に基づいて、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の範囲を拡大するとともに、障害対応体制の強化としての分野横断的演習においても参加事業者の範囲を拡大し、中小事業者への取組の拡大を図った。 ・ 内閣官房において、重要インフラ事業者等が重要インフラサービスを提供するために利用する外部サービスの依存性に関する調査を実施し、既存の情報共有体制の範囲と比較して重要な外部委託先や主要関係先の抽出を行った。 ・ 重要インフラに係る防護範囲の見直し等に関する検討課題を整理し、2016 年３月にサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」を決定した。
（ウ）	内閣官房	内閣官房において、重要インフラ分野以外の民間企業をサイバー攻撃から保護するために、既存の重要インフラ分野いかんに関わらず情報共有等の取組の対象とすべき企業の範囲について検討を行う。	・ 内閣官房において、重要インフラ事業者等が重要インフラサービスを提供するために利用する外部サービスの依存性に関する調査を実施し、既存の情報共有体制の範囲と比較して重要な外部委託先や主要関係先の抽出を行った。 ・ 情報共有等の取組の対象とすべき範囲等を含め、重要インフラ防護に関する関する検討課題を整理し、2016 年３月にサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」を決定した。

(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 2015	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、サイバー攻撃に対するより効果的な情報を迅速に共有するための在り方を検討すると共に、小規模な障害情報や予兆情報（ヒヤリハット等）の情報共有について政府機関内での連携強化を図る。	・ 内閣官房において、より効果的かつ迅速な情報共有に資するため、重要インフラ所管省庁との情報共有様式の改良等を行ったほか、重要インフラ所管省庁や重要インフラ事業者等が集まる会合等において、小規模な障害情報や予兆情報（ヒヤリハット等）も含めて情報共有を積極的に行うことの必要性について周知を図った。 ・ 重要インフラ防護に係る情報共有に関する検討課題を整理し、2016 年３月にサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」を決定した。
（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 が運営する「サイバー情報共有イニシアティブ」（J-CSIP）を通じて、サイバー攻撃に関する情報共有を着実に実施。 ・ 2012 年から 2015 年の３年間の情報共有活動における情報の集約・分析の成果として、国内組織を執拗に狙う攻撃の実態を明らかにし、「攻撃者 X の分析」として公開（2015/5）。 ・ 日本の基幹産業の１つである自動車業界を対象とした、「自動車業界 SIG」（10 組織）を新たに設立（2016/1）。また、化学業界 SIG へも３組織が新たに参加。これにより、J-CSIP の参加組織数は 59 組織から 72 組織に拡大。 ・ IPA を通じ、情報処理システムに係る障害事例情報の分析に基づく教訓やガイド等を提供し、新たな産業分野（具体的には、航空運行分野、生命保険分野、ケーブルテレビ分野）において、自律的な障害情報収集・共有の体制を構築した。 ・ 「情報システムの障害状況データ」を継続してまとめ、IPA が発行する「SEC ジャーナル」（42 号、44 号）に掲載した。

（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、57 件の「早期警戒情報」を発行した（2016 年３月 31 日現在）。 ・ 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 9659 件：2016 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 629 件であった。また制御システムに関する対応支援は、７件のインシデント報告を受領し、計 21 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６件の参考情報と 12 件の月次ニュースレター、231 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次行動計画等に基づき、情報セキュリティ関係機関等から 2015 年度に 52 件の情報提供を受け、必要に応じて重要インフラ事業者等と情報提供を行っている。 ・ 内閣官房と JPCERT/CC、IPA 等との間で締結したパートナーシップに基づき、サイバーセキュリティ動向及びインシデント対応方法等の意見交換をはじめ緊密な連携を行っている。
（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・構築に向けた検討を行った。
（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を行う。 ・ 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。 ・ 「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事案発生時に、被害者等から提出を受けたウェブサーバ等に保存されている大量の通信記録の分析等、迅速な初動捜査を実施するために必要な資機材に係る予算を措置した。 ・ 警察庁において官民一体となったサイバー攻撃対策を推進し、また、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・分析のための体制を強化した。

(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 2015	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 障害等の事案を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サイバーセキュリティに関する情報を、総務省を経由して地方公共団体に情報提供を行っている。 ・ 総務省において、平成 27 年７月から 11 月まで、地方公共団体における情報セキュリティに係る抜本的な対策を検討するため、自治体情報セキュリティ対策検討チームを開催するとともに、内閣官房等もオブザーバとして参加した。

（イ）	内閣官房 内閣府 総務省	内閣官房及び総務省において、総合行政ネットワーク（LGWAN）に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対策に関する支援の強化を図ること等により、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、特定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立ち上げるとともに、監視・監督方針を速やかに策定するなど、本年度中を目途に、監視・監督体制を整備する。	・ 個人情報保護委員会（2015 年 12 月末までは特定個人情報保護委員会）において、特定個人情報の適正な取扱いの確保を図るため、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」を改正し、個人番号利用事務で使用する情報システムについて、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を踏まえたシステム構築及び運用体制整備を行うこと等を盛り込むとともに、「平成 27 年度監視・監督方針」を定めたほか、関係機関と連携し、専門的・技術的知見を有する監視・監督体制の整備を行った。 ・ 総務省において、自治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自治体情報セキュリティ対策検討チームを立ち上げ検討を行った。また、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平成 27 年度補正予算において、255 億円を計上し、３月に第１回の交付決定を行った。さらに、平成 28 年度当初予算において、情報連携に用いる総合行政ネットワーク（LGWAN）及び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、平成 27 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。
（ウ）	内閣官房	内閣官房において、マイナンバー制度の下で認証連携を行うに当たって、利便性の向上とセキュリティの確保がバランスの取れたものとなるよう、政府内及び官民での認証連携について、多要素認証等の認証方式や連携条件についての検討を行い、本年中を目途に取組方針を策定する。	・ 内閣官房及び内閣府を中心として、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検討を行い、施策と工程の具体化を行った。
（エ）	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制度」を運用する。	・ 内閣サイバーセキュリティセンターから発行される「NISC 重要インフラニュースレター」の制作において、IPA と JPCERT が運用する JVN での公開情報に関し情報提供を実施（毎月実施、年 12 回）。 ・ JPCERT/CC では、米国 ICS-CERT からの依頼を受けて、2015 年度は 17 件の制御システム関連の脆弱性について製品開発者と調整を行った。
（オ）	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、それに基づいたセミナー及びより実践的な演習を実施する。	・ 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い、得られた知見を各分野に展開した。
（カ）	経済産業省	経済産業省において、CSSC が実施する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、制御システム全体のセキュリティに関する評価・認証制度の構築を行う。また、制御システムのセキュリティマネジメントシステム適合性評価スキームの普及について、JIPDEC 等関係機関に対して支援を行う。さらに、CSSC の制御システムセキュリティテストベッド施設を利用した研究開発成果の展開を図り、その成果を用いて制御システムセキュリティに係る国際標準化の推進を図るとともに、それに基づいた国際的な相互承認制度の拡大を推進する。	・ EDSA 認証（2014 年４月開始）について、説明会の開催や HP での普及・啓発を行い、2015 年度は１製品の認証を行った。また、制御システム全体のセキュリティ評価・認証に向けて、制御システムセキュリティ国際標準 IEC 62443 の規格要求事項を整理した。IEC62443 に基づく制御システムセキュリティに関わる国際標準化を推進すると共に、制御システムの国際的な相互承認の対象制度の拡大も念頭に、制御システムの評価技術・手法の検討を行った。

2.3. 政府機関を守るための取組

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、新たに直面した脅威・課題への対応について、政府統一基準を始めとした規程に適時反映するため、政府統一基準等の次期改定に向けた検討を順次進める。	・ 内閣官房において、統一基準群とサイバーセキュリティ基本法の関係を明確化し、独法等が適用対象となる様、文書体系の見直し等を行うとともに、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の教訓として、重要な情報を取り扱う部分のインターネットからの分離や CSIRT の整備等に係る規定を強化した。その他に、外部環境変化等に従い、クラウドサービス利用、データベース管理、文書管理ガイドラインの一部改正に伴う規定についても強化した。2016 年夏頃の決定を目指し、統一基準群の改定案をまとめた。

(1) 攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進

項番	担当府省庁	サイバーセキュリティ 2015	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。また、諸外国における SOC 事例の調査を行い、その結果を踏まえ、GSOC が有するべき機能、政府機関等の連携体制等について、検討を行う。	・ 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。 ・ 諸外国における SOC 事例の調査を行い、その結果を踏まえ、GSOC が有するべき機能、政府機関等の連携体制等について検討を行い、次期 GSOC システムの仕様に反映させた。
（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、府省庁 CSIRT 要員（GSOC 連絡担当者を含む）を対象とした勉強会を開催し、情報セキュリティインシデントに係る情報共有を実施した。 ・ 内閣官房において、情報セキュリティインシデント対処に関わる CSIRT 要員間の情報共有、連携促進のための取組に関して、各府省庁に対するアンケート等を実施し、その結果を踏まえて今後の取組についての検討を行った。
（ウ）	内閣官房	内閣官房において、政府機関における情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組（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、各府省庁における事例を調査し、各府省庁と共有する。また、情勢変化に応じた運用中の情報システムにおける対策の迅速・柔軟な見直しの在り方について検討を行う。さらに、それらについて、政府機関全体として取り組むべき事項が把握された際には、政府統一基準を始めとした規程への反映に向けた検討を行う。	・ 内閣官房において、府省庁における仕様書記載内容の事例を参考に、サプライチェーン・リスク対応のための仕様書策定手引書を整備し公表した。また、各府省庁における実効的な取組が可能となるよう、サプライチェーン・リスク対策の考え方について研修を行った。さらに、各府省庁におけるサプライチェーン・リスク対応の取組状況を把握するために調達仕様書へのサプライチェーン・リスク対応の考慮状況について実態調査を行った。 ・ 内閣官房において、SBD マニュアルへサプライチェーン・リスク対応を追加するとともに、総務省統一研修等にて職員への周知を行った。また、情報システムの調達においてセキュリティ・バイ・デザインが強化されるよう、所要の規定強化を内容とする統一基準群の改定案をまとめた。

（エ）	経済産業省	経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPA を通じ、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。	・ 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、JISEC 運営審議委員会を開催し、①対象候補「ルータ／レイヤー３スイッチ」の検討、②既存分野への新規 PP の適用の検討、③CC 承認アレンジメント及び加盟国における cPP 開発状況の確認を実施するとともに、必要な調査を実施した。 ・ 最新のプロテクション・プロファイル（翻訳版）の情報提供について、モバイルデバイス、ハードコピーデバイス（デジタル複合機）、ネットワークデバイス、暗号化ストレージ、オペレーティングシステム及びデータベース管理システムの６技術分野の計８つのプロテクションプロファイル（翻訳版）を公開した。特にハードコピーデバイスのプロテクション・プロファイルについては、ベンダー説明会を 2015/10/6、12/17 に開催し普及啓発した。
（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見直しを実施する。	・ IPA において、JISEC（IT セキュリティ評価及び認証制度）の制度紹介の開催の他、業界団体（JEITA、IVIA）や国際人材関係（JICA、HIDA）での説明会を実施。また、ベンダーや運営審議委員へのヒアリングを実施し、評価の長期化や申請事業者の妥当性に関する懸念について対応すべく規程改正を実施した。
（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、暗号モジュール試験及び認証制度で採用している国際標準の改定に伴い、一致規格の JIS 原案を作成した。国際標準に基づく制度の利用促進のため、説明会を通じて、国際標準の解説を行うと共に、原案作成作業を通じて得られた解釈などについても解説を行った。
（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対策の実施状況の点検・改善を行うため、ペネトレーションテストを実施することにより、攻撃者が用いる手法で実際に侵入できるかどうかの観点から防御策の状況を検証し、改善のための必要な助言等を行う。	・ 内閣官房において、「サイバーセキュリティ対策を強化するための監査に係る基本方針」（平成 27 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、ペネトレーションテストを各府省庁の基幹 LAN システム等を対象として実施し、その結果を踏まえ、セキュリティ対策水準の向上を図るための助言等を行った。
（ク）	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を調査し、各府省庁と共有するとともに、調査結果に応じて、政府統一基準を始めとした規程への反映や改善に向けた取組について検討を行う。	・ 内閣官房において、昨今のサイバーセキュリティに関する状勢や動向を踏まえ、政府機関全体として分析、評価及び課題の把握、改善等が必要と考えられる項目として、公開ウェブサイトのウェブアプリケーションへの既知の攻撃手法に対する対策状況、電子メールのなりすまし対策状況及び技術的なセキュリティ対策状況の３つについての検査を実施した。また、2015 年度までに実施した重点検査の結果を踏まえ、統一基準群の改定案をまとめた。
（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予防・検知するモデルについて検討するとともに、標的型攻撃発生時において被害の拡大防止と被害の最小化を図る暫定対処のモデルについて検討を実施。
（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・解析機能を始めとした機能強化、GSOC センサーの増強、設置対象の法人等の段階的追加を含む監視対象の拡大を行うための具体的方策の検討を行う。	・ 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など、GSOC システムに求められる機能の検討を行い、次期システムの仕様を決定した。 ・ 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、独立行政法人情報処理推進機構において監視体制を構築することにより、体制整備を図ることとした。
（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検討を行う。	・ 内閣官房において、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、府省庁における標的型攻撃の発生時の検知及び初期対処のために取得すべきログや保管期間に関する内容を検討し、統一基準群の改定案をまとめた。

(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・対処機能及び要員間の連携の強化を図るため、各府省庁の CSIRT 体制やインシデント対処に係る現状の課題等について、CISO を始めとした幹部による指揮の下での組織的対処の観点も含めて調査し、各府省庁と共有するとともに、調査結果に応じて、要員のキャリアパスの構築等にも配慮しつつ、CSIRT の体制の拡充や実効性の向上に取り組むとともに、政府統一基準を始めとした規程への反映について検討を行う。また、調査結果については、各府省庁と共有を図る。	・ サイバーセキュリティ対策推進会議議長による指示の下、各府省庁における CSIRT 体制、対処手順等に係る課題等を調査し、その結果を踏まえ、各府省庁に対して CSIRT 体制・連携体制等の強化の指示を行った。 ・ CISO を交えて実施した CSIRT 訓練の自己評価、アンケート、訓練結果等の分析を通じて、各府省庁の CSIRT 体制や情報セキュリティインシデント対処に関する課題等を調査し、各府省庁にその結果を共有するためにとりまとめを行った。 ・ 上記の取組や昨今のサイバーセキュリティについての情勢等を踏まえ、CSIRT 体制やインシデント対処の在り方を検討し、その内容を統一基準群の改定案にまとめた。 ・ 各府省庁においては、セキュリティ人材を念頭とした人事ルート例（イメージ）を設定することとしている。
(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、各府省庁における対処要員を対象として、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（独立行政法人等を所管する部局との連携等を含む。）の実現を目指し、インシデント・ハンドリングを中心として近年のサイバー攻撃動向を踏まえた訓練を平素から実施する。 ・ 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技術的事項の習得に重点を置いて実施する。 ・ 総務省において、政府機関における標的型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防御演習（CYDER）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（独立行政法人等を所管する部局との連携等を含む。）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。 ・ 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）要員に対する技術的事項の習得に重点を置いた研修を年間を通じて実施したほか、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。 ・ 2015 年 10 月より、官公庁・重要インフラ事業者等の LAN 管理者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）を計７回実施。（含：National 318 EKIDEN 2016）
(セ)	内閣官房	内閣官房において、政府職員のインシデント・ハンドリング能力等を向上させていくため、2014 年度に初め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、2015 年度は規模を拡大し訓練を実施した。
(ソ)	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、各府省庁の CSIRT 等が、サイバー攻撃発生時に外部の専門家等による必要な支援をより迅速に得られるようにするための体制・制度の構築に取り組むとともに、政府統一基準を始めとした規程への反映に向けた検討を行う。	・ 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、情報セキュリティインシデントが発生した際に、その対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制の構築について検討し、統一基準群の改定案をまとめた。
(タ)	内閣官房	内閣官房において、GSOC システム等による監視効率の向上等によりリスクを低減させるため、業務効率にも留意しつつ、各府省庁の情報システムの集約化に合わせたインターネット接続口の早急な集約化を行うことによる攻撃リスクの低減等を含む政府機関等の対策方針を早急に取りまとめるとともに、政府統一基準を始めとした規程への反映に向けた検討を行う。	・ 内閣官房において、業務効率等考慮しつつ可能な限りインターネットの接続口を集約するよう仕様書に明記すること等の反映を行うことを検討し、統一基準群の改定案をまとめた。

（チ）	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適切に始動させるため、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。 ・ 内閣官房において、サイバー攻撃で被害を受けた端末等のフォレンジック調査及び技術動向調査を専門事業者に委託し、フォレンジック調査に係る最新動向を把握しつつ重大インシデント発生時に専門事業者と連携して速やかにフォレンジック調査を行うことができるようにした。
（ツ）	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の加速を図るとともに、個人情報や機微な情報を始めとした機密性・完全性の高い情報に焦点を当てた政府機関における情報管理の更なる強化に向けて、取り扱う情報の性質や量に応じた情報システムの分離、機密性・完全性の高い情報を管理するデータベースに対する不正なアクセス等による情報漏えいや改ざん等への対策について政府統一基準を始めとした規程への反映に向けた検討を行う。	・ 「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」の運用等を通じた標的型攻撃に対する多重防御の取組について、各府省庁における実施結果を取りまとめ、政府全体としての本取組の実施状況等について、サイバーセキュリティ対策推進会議に報告した。 ・ 行政事務の特性や取り扱う情報の性質や量を考慮した情報システムの分離等の対策を反映することについて検討し、統一基準群の改定案をまとめた。 ・ 機密性・完全性の高い情報を管理するデータベースに対する不正なアクセス等による情報漏えいや改ざん等への対策について検討し、統一基準群の改定案をまとめた。
（テ）	内閣官房	内閣官房において、リスク評価に基づく重点的な対策実施を推進するとともに、リスクや影響度に応じたインシデント対処や情報システムの対策強化に関する優先度の評価方法について、その在り方に関する検討を行う。	・ 内閣官房において、リスクや影響度に応じた情報システムの対策強化について、「「日本再興戦略」改訂 2015」等に基づいて検討を行い、業務効率等を考慮した可能な限りのインターネット接続口の集約、行政事務の特性や取り扱う情報の性質や量を考慮した情報システムの分離等の対策や、情報セキュリティインシデント発生時の対処手順における意思決定の判断基準等の策定を内容とする統一基準群の改定案をまとめた。 ・ 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」の運用等を通じた標的型攻撃に対する多重防御の取組について、各府省庁における実施結果を取りまとめ、政府全体としての本取組の実施状況等について、サイバーセキュリティ対策推進会議に報告した。【再掲】

(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 2015	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、政府機関における政府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、点検を目的とした従来の施策等の統合も視野に入れた監査制度を設計するとともに、当該制度の有効性の検証を目的として、試行的な監査を実施する。試行的な監査については、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、次年度以降の本格的な監査制度の運用に資することを考慮し、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体制の整備及び運用状況に係る現状を把握し、改善に資する対応策について助言等を行う。また、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を内閣官房が実施する監査及び原因究明調査の対象とすることを検討した上で、当該法人の業務等の性質やセキュリティ対策の緊急性等に応じて監査等を実施する。さらに、当該法人を所管する府省庁と協力し、当該法人に対する監査等の在り方について検討を行う。	・ マネジメント監査については、「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」（平成 27 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、監査制度の設計及び当該制度の有効性の検証を目的とした試行的な監査を実施した。試行的な監査においては、2016 年度以降の本格的な監査制度の運用に資することを考慮するとともに、被監査主体に対しては、改善のために必要な助言等を行った。また、本格的な監査を実施するために必要な監査制度の枠組みを確立し、監査要領をサイバーセキュリティ対策推進会議に報告した。 ・ 独立行政法人等に対する監査等の在り方に関しては、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に係る勧告を受け、同機構を内閣官房が実施する監査の対象とすることとし、2016 年度に実施する監査支援に関する必要な予算要求や執行準備を実施した。
(イ)	内閣官房	内閣官房において、リスク評価に基づく組織的な情報システムの対策・管理を推進するため、情報システムにおけるリスク対処方針、対策水準、事態の緊急度に応じた意思決定プロセス等を情報システムのユーザー側と管理側との双方の合意に基づき、CIO 補佐官や最高情報セキュリティアドバイザー等の外部から起用する人材の積極的な活用を図りつつ、組織的に設定する制度について、その在り方に関する検討を行う。	・ 内閣官房において、府省庁における情報セキュリティインシデント発生時に緊急度に応じて、情報システムへの緊急措置等を迅速に行えるようにするための意思決定プロセスについて検討するとともに、情報システムの運用継続計画の整備及び整合的運用を確保するための施策について見直しを行い、統一基準群の改定案をまとめた。
(ウ)	内閣官房	内閣官房において、政府機関における共通的な課題や未知の脅威等の顕在化に備えた対応に関するプラクティスの共有や意見交換を促進するためのコミュニティを形成する。	・ 内閣官房において、府省庁情報セキュリティ担当者を対象とした勉強会を開催し、政府機関における共通的な課題や未知の脅威等の顕在化に係る情報共有を実施した。
(エ)	内閣官房	内閣官房において、各府省庁におけるけん引役となるセキュリティ人材の育成に資するため、各府省庁のセキュリティ担当者に加え、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平素から開催する。また、各府省庁におけるサイバーセキュリティに関する職員教育を推進するため、教育資料のひな形の提供等による支援を行う。	・ 政府機関や独法等の職員向けに、統一基準群やマネジメント監査、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の解説、サイバーセキュリティに関する最新の動向等をテーマとした NISC 情報セキュリティ勉強会を実施した。 ・ 独法所管部局の管理職及び独法の役員を対象とした出前講座を開催し、年金事案を教訓とした標的型攻撃等について解説した。 ・ 2015 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。 ・ 教育資料のひな形として、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について、テーマおよびユースケースごとに整理した「情報セキュリティ小冊子」を作成する等の支援を行った。 ・ セキュリティ・IT 人材の不足という政府機関における共通的な課題に対応するため、政府機関におけるセキュリティ・IT 人材の育成について、CISO 等連絡会議／CIO 連絡会議合同会議における討議を踏まえ、「サイバーセキュリティ人材育成総合強化方針」において取りまとめた。

（オ）	内閣官房	内閣官房において、各府省庁による新規採用時の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、教育資料のひな形として、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について、テーマおよびユースケースごとに整理した「情報セキュリティ小冊子」を作成する等の支援を行った。【再掲】 ・ 内閣官房において、2016 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。

(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 2015	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、クラウド事業者及びクラウドに係る有識者等から構成される「政府機関がクラウド利用の際に留意すべきセキュリティに関する研究会」を開催し、クラウド調達の際のセキュリティ対策推進のために、調達者が如何なる視点をクラウドサービス選定の際に考慮すべきかについて整理・検討を行った。 ・ 上記研究会での検討結果を統一基準群に追記・反映するべく、当該基準への追記案を府省庁等に提示して意見交換を行うとともに、それを通じ、府省庁における実際のクラウドサービス等の利用や対策の状況について調査を実施し、共有を図った。
（イ）	内閣官房	内閣官房において、IT を活用した政府機関全体としての行政事務について、関係機関と連携し、サイバーセキュリティの確保が前提となった遂行形態の実現を図る。	・ 内閣官房において、マイナンバー制度関連システム等に関するセキュリティ要件の確認等、必要な支援を行った。また、各府省庁に対して、以下に関する注意喚起を行った。 –「サービス不能攻撃への対処について」（2015 年 11 月 25 日発出） –「情報セキュリティ問題への対処について」（2016 年１月７日発出） –「分散型サービス不能攻撃への対処について」（2016 年２月２日発出）

(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 2015	取組の成果、進捗状況
（ア）	内閣官房	内閣官房において、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政府機関の取組を踏まえた取組を総合的に強化するため、当該法人を所管する府省庁と協力し、当該法人における対策の実施状況を確認し、当該法人の対策強化を図る。また、当該法人において統一的に取り組むべき事項が把握された際には、当該法人の性質等を踏まえつつ、政府統一基準を始めとした規程への反映に向けた検討を行う。	・ サイバーセキュリティ対策推進会議において、独立行政法人及び特殊法人等を所管する府省庁は、各法人に対し政府機関における取組を踏まえた取組に加え、継続的なセキュリティ対策強化のための取組を講じるよう指導することを申し合わせた。これを受け、内閣官房においては、独立行政法人、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、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、2014 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。 ・ 平成 28 年２月２日に閣議決定・国会提出され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において、サイバーセキュリティ戦略本部が作成するサイバーセキュリティに関する対策の基準の対象範囲が指定法人にも拡大されたことを踏まえ、統一基準群の対象範囲についても指定法人まで拡大することを検討し、統一基準群の改定案をまとめた。

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 2015	取組の成果、進捗状況
（ア）	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・分析する体制の確立及び強化を実施するとともに、必要な機材の整備を行う。	・ 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 2015 年 10 月に整備するとともに、サイバー情報収集装置の機能拡充を実施した。
（イ）	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、関係府省庁等と連携した初動対処訓練を実施する。	・ 内閣官房及び関係省庁と新たに重要インフラ事業者を加え、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。

(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 2015	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。 ・ 2015 年７月、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の強化を図るため、「第２回政府における情報保全に関する検討委員会」（2011 年７月）における決定事項に基づいて、関係府省庁のシステムにおける情報セキュリティ対策の進捗状況の確認を実施した。
（イ）	警察庁 法務省	警察庁及び法務省において、サイバーインテリジェンス対策に資する取組を実施する。	・ 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、政府のサイバーインテリジェンス対策に資する関連情報の収集・分析のため、人的情報収集を強化し、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、サイバー攻撃対策に係る体制等を強化するため、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。	・ インターネット観測技術に関する調査研究を行い、観測に必要な機能等について成果物に取りまとめた。今後これらの成果物を用いてサイバー空間に関する観測機能の高度化を図る。 ・ 大規模産業型制御システムの構成、セキュリティの考え方、サイバー攻撃の可能性、攻撃発生時の影響等についての調査研究を実施するとともに、調査研究結果に基づき、実際の対処の任に付く警察職員が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実施できるようにするための訓練を実施した。 ・ DoS 攻撃や Web サイト改ざん等に係る観測機能強化を見据えた検討、開発及び試験運用を実施した。 ・ 民間事業者等との協力関係構築に取り組み、収集するインターネット上の脅威に係る技術情報の範囲拡大を図り、サイバー攻撃対策に係る体制等を強化した。
（エ）	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、防衛省情報通信基盤（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。	・ 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、2016 年３月までに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、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の機能拡充を実施した。
（オ）	防衛省	防衛省において、サイバー攻撃時においても、被害の拡大防止等対処能力を向上し継続的な部隊運用を確保するため、指揮系システムに係るサイバー演習環境の構築技術に関する研究の実施及び当該成果を踏まえて演習環境の構築を行う。また、将来の技術動向等を踏まえたサイバー攻撃対処能力の向上を目的として、相手方のサイバー空間の利用を妨げる能力に関する調査研究を行い、攻撃・防御機能及び統裁・評価機能等を備えた演習環境を整備する。	・ サイバー演習環境の構築技術に関する研究試作を実施した。また、その研究成果を受け、実戦的なサイバー演習環境の整備を開始した。
（カ）	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、サイバー攻撃の生起時に、ネットワーク内において迅速変更等を行うことにより、重要通信の経路を確保し、被害拡大を防止するための研究を実施し、2016 年 3 月までに装置を試作した。
（キ）	防衛省	防衛省において、実践的な教育を実施し、巧妙化するサイバー攻撃に適切に対応していくため、体験学習型の手法を用いた e ラーニングコンテンツに関する調査研究を実施するとともに、国内外の大学院等への留学等も引き続き行い、人材育成への取り組みを実施する。	・ 体験学習型の手法を用いた e ラーニングコンテンツに関する調査研究を実施し、サイバーセキュリティ教育の検討を開始した。また、サイバー攻撃等対処要員に関する人材育成の取組として、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。

(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 2015	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を目的として、防衛省において調達する情報システムに使用される、部品等のトレーサビリティ（製造元の追跡）に関する調査研究を行う。	・ 防衛省において、更なるサイバーセキュリティの確保を目的として、防衛省において調達する情報システムに使用される、部品等のトレーサビリティ（製造元の追跡）に関する調査研究を実施し、2016 年 3 月に報告書に取りまとめた。
（イ）	経済産業省	経済産業省において、我が国の先端技術の活用・防護を図るため、CSSC を通じて、システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を行う。	・ CSSC において、制御システムのログを分析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究・検証を行った。

(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 2015	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、任務遂行上依存する部外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 2016 年 2 月に実施した。また、日米サイバー防衛政策ワーキンググループ共同声明を 2015 年 5 月に発出し、任務保証のためのサイバーセキュリティに係る重要インフラ防護に関する協力を進めていくことで一致した。

3.2. 国際社会の平和・安定

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
(ア)	総務省	総務省において、近年、被害が拡大しているサイバー攻撃（DDoS 攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外の ISP、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するセンサーを設置し、諸外国と連携してサイバー攻撃の予兆を検知し迅速に対応することを可能とする技術について、その研究開発及び実証実験を実施する。本件技術開発にあたり、欧米、ASEAN 諸国等との連携を進める。	・ 研究開発においては、欧米、ASEAN 諸国等と連携し、サイバー攻撃の予兆を検知する技術を開発した。実証実験においては、国内の ISP 団体とともにサイバー攻撃の予兆に関する情報の早期共有を行い、ISP 連携による対応体制を確立した。
(イ)	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情報共有システム（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。	・ 2015 年度は、JPCERT/CC が運用するインターネット定点観測情報共有システム（TSUBAME）にモンゴルとモロッコの CSIRT が新たに加盟した。また、ラオスの CSIRT に対するトレーニングや、APCERT 年次総会に合わせた Workshop の開催により、攻撃方法の共有等、各国関係機関との連携を図った。そのほか、TSUBAME ML 等での事象や解析結果の共有や、個別事案について該当地域の CSIRT に対し、情報共有を行った。

(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 2015	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、防衛省において、各二国間協議や国連サイバーGGE、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」をはじめとする二国間協議を開催するとともに、４月にハーグで開催された「サイバー空間に関する会議」等への参画を通じ、サイバー空間を利用した行為に対する既存の国際法の適用や、国際的な規範作り等に関する我が国の取組に関する情報発信に努め、当該議論に積極的に関与した。 ・ 第４次国連政府専門家会合に政府専門家（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ルール作りなどに積極的に寄与するとともに、同会合における議論のとりまとめに貢献した。
(イ)	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。	・ 第 13 回（６月）及び第 14 回（12 月）サイバー犯罪条約委員会（於：仏ストラスブール）に出席し、議論に積極的に参加。11 月には、ゼーゲル欧州評議会サイバー犯罪条約委員会事務局長が来日し、サイバー政策担当大使とサイバー犯罪条約締約国拡大等について意見交換を行った。

（ウ）	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 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大韓民国との間では中央当局間実務者協議を実施し、共助の迅速化を図った。
（エ）	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、外国法執行機関との連携を強化するため、職員を派遣する。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（2015 年 11 月、2016 年３月）、ICPO サイバー犯罪に関するユーラシア地域作業部会（2015 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、2015 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（2016 年３月末現在、70 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、ロシア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。

(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 2015	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、内閣サイバーセキュリティセンターをサイバーセキュリティに関する我が国の国際的な窓口（コンタクトポイント）とし、外務省及び関係府省庁と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、エストニア、仏等の友好国とのサイバー協議を実施し、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、脅威認識やサイバーセキュリティ戦略等との政策について共有した。 ・ 日中韓サイバー協議を実施し、サイバーセキュリティ分野における情報交換、信頼醸成を推進した。 ・ ARF サイバー関連ワークショップに参加し、サイバー攻撃を受けた際の対応要領について意見交換及び情報共有を実施した。

（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、それぞれの取り組み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積極的に参画し、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強化に努めた。 ・ IWWN における合同サイバー演習に参画し、有志国を中心とする国外機関との情報連絡体制について確認をするとともに、重大インシデント発生時への体制整備に努めた。 ・ MERIDIAN 会合に参加し、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連絡演習を実施し、アジア地域における政策担当者レベルでの連絡体制の整備・推進に努めた。
（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、MOU に基づき「日中韓サイバーセキュリティインシデント対応年次会合」を主催した（2015 年８月）。FIRST、IWWN とアジア・アフリカ地域の CSIRT との連携促進に注力するとともに、APCERT2015 年次会合における TSUBAME Workshop 開催（2015 年９月）等 APCERT の活動支援に取組み、各国 CSIRT との継続的な連携関係の維持を図った。

(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 2015	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」（仮称）設置に伴う情報収集・分析等の強化のための予算を措置するなど、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、国際テロ組織等による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（仮称）」の設置に伴う情報収集・分析等の強化のための予算を措置するなどし、サイバー空間上の攻撃主体・方法等に関する情報収集・分析の強化に取り組んでいる。 ・ 法務省において、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・分析を通じた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強化に努めた。また、人的情報収集網の拡大に努めるなどして、サイバー攻撃に関する情報収集・分析を強化した。

(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 2015	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、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。	・ 2015 年度は、JPCERT/CC において、「セキュアコーディングセミナー」(2015 年 7 月、タイ)、「インシデントハンドリングトレーニング」(2015 年 11～12 月、コンゴ共和国)を実施した。また、アジア太平洋地域における CSIRT 構築支援として、JICA 等外部機関と協力しつつ、技術研修や CSIRT マネージャ向け研修等を行った。

（イ）	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省	内閣官房、警察庁、総務省、外務省、経済産業省、防衛省、その他関係府省庁において、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り組みや 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り組みを通じて、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始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）における取り組みや ITU-D 等の取り組みを通じて、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 プロジェクトの枠組みを通じて、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、日本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。	［NISC］ （日・ASEAN） ・ 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。 ・ 2015 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、意識啓発標語、意識啓発マンガの共同作成を行った。共同ポスターおよび意識啓発マンガについては我が国において印刷し、ASEAN 加盟国へ配布を行ったほか、独立行政法人情報処理推進機構（IPA）が作成したパスワード啓発ポスターを、ASEAN 加盟国で主に使用される各言語に翻訳し、展開した。また、意識啓発と国際交流をテーマにサイバーセキュリティカフェを日本で開催した。 ［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、2015 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」（2015 年５月、フィリピン）に参加し、同作業部会のセキュリティ繁栄分科会において、我が国からサイバーセキュリティ基本法、政府全体の体制及び取組について説明した。APT の加盟国を対象とした研修（2015 年 11 月、2016 年３月、東京）を開催し、我が国の取り組みについて情報を共有した。第６回 APT サイバーセキュリティフォーラム（2015 年 10 月、タイ）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 サイバーセキュリティワークショップ（2015 年９月、スイス）に参加し、サイバーセキュリティ基本法及びサイバーセキュリティ戦略について説明した。 ［外務省］ （能力構築支援） ・ 2015 年７月、サイバーセキュリティ分野について、ベトナム側の能力構築支援のニーズの把握、及び日本側として効果的な支援の方向性を見極めることを目的として、ベトナムに政府調査団を派遣。現在、更なる調査のため、2015 年 12 月より、JICA において情報収集・確認調査を実施中。 （サイバー犯罪） ・ 第２回日 ASEAN サイバー犯罪対策対話については、開催予定国であるマレーシア側の事情により、開催を 2016 年９月に延期。 ・ UNODC を通じた ASEAN 諸国に対するサイバー犯罪技術援助プロジェクトについては、2016 年３月より、マレーシア、インドネシア、ラオス、カンボジア、ベトナム、ミャンマーにおいて、各種研修・ワークショップを順次実施中。 ・ JAIF の枠組みを通じた ASEAN サイバー犯罪能力プロジェクトについては、ASEAN 事務局より提出されたプロポーザルを承認。

(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 2015	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、わ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 等への会議に参加したほか、米国国務省主催「インターナショナル・ビジター・リーダーシップ・プログラム」に参加し、得られた知見・技術動向に関する情報を関係各所に共有し、関係者のスキル向上を図った。 ・ インドネシア・ジャカルタにおいて ASEAN サイバーセキュリティ・コンテストである加盟国を対象とした「サイバーSEA ゲーム」を開催し、優勝チームおよび準優勝チームを日本での SECCON CTF2015 に招待することを通じ、我が国の情報セキュリティ人材が海外の優秀な技術者との研鑽を積む場を提供した。

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 2015	取組の成果、進捗状況
(ア)	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、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 2015 年 10 月に整備した。
(イ)	内閣官房 外務省	内閣官房、外務省及び関係府省庁において、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。	・ ４月末の日米首脳会談の際、共同声明のファクトシートの中で、サイバーセキュリティに関する協力について盛り込まれた。１２月には、サイバーセキュリティを担当する遠藤国務大臣が訪米し、政府・議会のサイバーセキュリティ関係者と会談を行った。
(ウ)	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。	・ 2010 年 10 月より開始した「情報セキュリティ国際キャンペーン」を「サイバーセキュリティ国際キャンペーン」に名称を改め、2015 年 10 月に実施した。2015 年においても国際連携・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、インターネット広告、ラジオ放送、SNS 等の周知用素材による情報発信に努めた。また、意識啓発等をテーマに米国および ASEAN 諸国と連携したイベントをそれぞれ日本で開催した。
(エ)	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３回日米サイバー対話」(2015 年７月)、「インターネットエコノミーに関する日米政策協力対話（第７回局長級会合）」(2016 年２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。 ・ 2014 年度に引き続き「第２回日中韓サイバー協議」(2015 年 10 月)、「第２回日エストニアサイバー協議」(2015 年 12 月)、「第２回日仏サイバー協議」(2016 年１月)を開催し、二国間等の連携強化や信頼醸成に取り組んだ。
(オ)	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、攻撃主体・方法等に関する情報収集・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。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。

（カ）	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、サイバーグリーンについて基礎システムの調査、開発、今後の自走化の検討を行った。ポータルサイトについては、予定されていた機能追加を行い、プロジェクト（実証実験）の理解を促進させるための手段として機能している。実証運用の運用については、評価指標の改善に向けた検討を重ねると共に、TSUBAME データをフィードし、指標に適切に反映すべく取組んでいる。また、各種イベントの機会を捉えてサイバーグリーンの普及活動を積極的に行った。主なイベント・活動として、APCERT および OIC-CERT による同時開催の年次総会（2015 年９月、クアラルンプール）におけるワークショップの開催、Global Conference on CyberSpace 2015（ハーグ会議）における講演、TF-CSIRT（欧州の CSIRT コミュニティ）会合における講演等が挙げられる。
（キ）	経済産業省	経済産業省において、国際協力体制を確立するという観点より、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。	・ IPA が、米国立標準技術研究所（NIST）との定期会合を 2015 年 12 月３日に、NIST にて開催。NIST、産業技術総合研究所、IPA の各機関がそれぞれの活動に関する情報共有を実施。具体的には暗号、ソフトウェア ID タグ、J-CSIP、内部不正防止、CMVP、サイバーセキュリティフレームワークに関する意見交換を実施。 ・ 韓国インターネット振興院（KISA）との定期会合を 2016 年３月 25 日に、KISA にて開催。IPA、KISA 双方より、IoT セキュリティ、サイバーセキュリティに関するガイドライン等についての意見交換を実施。
（ク）	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。	・ 2015 年度は、JPCERT/CC において、「セキュアコーディングセミナー」（2015 年７月、タイ）、「インシデントハンドリングトレーニング」（2015 年 11～12 月、コンゴ共和国）を実施した。また、アジア太平洋地域における CSIRT 構築支援として、JICA 等外部機関と協力しつつ、技術研修や CSIRT マネージャ向け研修等を行った。
（ケ）	内閣官房	内閣官房において、外国関係機関との情報交換等を緊密に行い、主要国のサイバー攻撃対処や国家の関与が疑われるようなサイバー攻撃の動向等の情報収集・分析に努める。	・ 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。

(1) アジア大洋州

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
（ア）	防衛省	防衛省及び関係府省庁において、東南アジア各国防衛当局との間の IT フォーラム等の取組を通じ、サイバー分野での国際連携や能力構築への協力、情報の収集や発信を推進していく。	・ 防衛省において、日星（シンガポール）ＩＴフォーラム（2015 年７月）、日越（ベトナム）ＩＴフォーラム（2016 年２月）等を実施し、諸外国との連携を強化した。

（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、2015 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） ・ 国連アジア極東犯罪防止研修所の実施した第 160 回国際研修において、参加した国内外の刑事司法実務家（警察官、検察官及び裁判官等）に対し、サイバー犯罪の現状及び対策等に詳しい専門家の講義等を実施した上で、各国におけるサイバー犯罪対策法制、捜査公判実務の現状及び課題についての意見交換を行った（2015 年５月から６月）。
（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の枠組みを通じ、ASEAN 加盟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。	［NISC］ ・ 日本と ASEAN 加盟各国では、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、以下のような連携・協力を推進している。 ・ 2015 年 10 月に第８回日・ASEAN 情報セキュリティ政策会議をインドネシア・ジャカルタにおいて開催し、「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およびアクションプランの策定、サイバー演習等を実施するとともに、今後も重要インフラ防護や人材育成の面等で連携を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」に基づき、日本及び ASEAN 加盟各国における重要インフラ防護、インシデント対応におけるベストプラクティスの共有を推進するとともに、ガイドラインの改定およびアクションプランの策定に向けた検討を重ねた。 ・ サイバー演習 WG では、演習シナリオや各国の政策担当者の役割などについて検討を重ねた。 ・ 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、長期研修および我が国への留学生受け入れ等を中心に議論を進めた。 ［総務省］ ・ 日本及び ASEAN のネットワークオペレータ間の情報共有を促進する「日 ASEAN ISP 情報セキュリティワークショップ」（2015 年 12 月、東京）を総務省が主催し、日 ASEAN の取組の共有及びさらなる連携方策の議論を行うとともに、日 ASEAN 合同サイバー攻撃対応演習を実施した。 ［経産省］ ・ 2015 年 11 月にインドネシアにて、2016 年２月に日本にて、「ASEAN 地域の重要インフラ関係者等に対する情報セキュリティ強化支援」研修コースを実施し、ASEAN 地域の貿易投資環境を整備した。

(2) 北米

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
(ア)	総務省	総務省において、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、サイバー攻撃に関するデータを共有及び研究開発の分野での協力関係の加速化という考えに基づき、データの共有などの米国との情報共有を強化する。	・「インターネットエコノミーに関する日米政策協力対話（第７回局長級会合）」（2016 年２月）において、最近のサイバーセキュリティ政策のアップデート事項について議論し、産業界や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を共有し、自由、安全、相互運用可能かつ信頼できるサイバー空間を追求し続けることを確認した。
(イ)	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、技術分野での協力において、包括的な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。	・日米サイバー防衛政策ワーキンググループ（CDPWG）を 2015 年４月及び 2016 年１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。
(ウ)	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。	・2015 年７月、日米両国の関係省庁の出席を得て、第３回日米サイバー対話を開催した。日米両国のサイバーセキュリティに関する取組の現状、サイバー分野における日米防衛協力及び国際場裡における日米協力等の課題について議論を行い、所要の成果を得た。

(3) 欧州

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
(ア)	防衛省	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。	・防衛省において、NATO CCD COE における演習への参加(2015 年４月)等を通じて、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 が JIWG に１回、JHAS に６回、JTEMS に３回参加し、最新技術動向を日本のコンソーシアム(ICSS-JC)と共有した。

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 2015	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）」（2014年７月 政策会議決定）を踏まえ、施策を推進している。また、2016年３月に研究開発戦略専門調査会を開催し、各府省庁の取組について意見聴取を行うとともに、今後の取組について検討を行った。
（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保証する上で、ルータ等のネットワーク機器に実装されている通信プロトコル等が安全性の高いものであるかを検証するための評価手法の確立に向けた研究開発を実施する。	・認証プロトコルを始めとする 50 個以上の標準化プロトコルの評価結果（脆弱性の有無）を集約し、問題点を洗い出し、技術的に信頼性のある情報の参照をつけた「AKE Protocol Zoo」を整備し公開した。
（ウ）	総務省	総務省において、NICTを通じ、ネットワークの各構成要素（ノード）における最適な情報セキュリティ設定を自動的に導出することを目指し、利用者環境のプライバシーを保護しつつネットワーク全体におけるリスク評価・検証技術の研究開発を実施する。	・「知識ベース」を情報連携の核とすることで、必要な情報が必要な時に入手できる土台を確立した。独自の情報だけでなく、外部機関の知識ベースとも連携し、記述フォーマットの異なる各種セキュリティ情報の横断検索機能を実現した。
（エ）	総務省	総務省において、NICTを通じ、2020年頃の実現を視野に、ユーザーからの要求に応じた最適な品質やセキュリティ・耐災害性等に優れた新世代ネットワークの基盤技術の研究開発を推進する。	・ネットワーク仮想化技術を用いた新世代ネットワークテストベッドや、P2P エージェントプラットフォーム（PIAX）と分散クラウド、ネットワーク仮想化を組合せた複合サービス収容ネットワーク基盤を構築し、ユーザーのエンドツーエンド要求品質にあわせかつ安全なネットワークの構築検証や、ゲリラ豪雨発生時の周辺データ（気象、交通、SNS 等）を収集統合する災害時通信技術検証など、さまざまな新世代ネットワーク技術を検証した。

(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 2015	取組の成果、進捗状況
（ア）	総務省	総務省において、NICTを通じ、標的型攻撃の対策技術として、マルウェアに感染したコンピュータからの情報流出に対処する技術の研究開発を行う。	・標的型攻撃研究の基盤となる組織内ネットワークのリアルタイム分析環境および大規模蓄積環境を整備した。組織内ネットワークを流れる通信および各種分析エンジンからのアラートを統合的に分析・可視化するプラットフォーム NIRVANA 改を開発・実用化し技術移転を実施した。
（イ）	総務省	総務省において、NICTを通じ、世界最先端のサイバー攻撃観測・分析・対策・予防技術、セキュアネットワークの設計・評価と最適構成技術、次世代暗号基盤技術等、ネットワークセキュリティ技術の研究開発を実施する。	・サイバー攻撃観測技術を高度化するための能動的観測システムの開発及び実証実験を実施し、国際的な技術連携の推進、観測データやアラート情報の外部利活用を推進した。 ・Android スマートフォンのアプリケーションのリスク分析を行うアルゴリズムとして、機械学習を用いた手法の提案及び新規の脆弱性検知アルゴリズムを構築し、両方式を Android アプリのリスク分析プラットフォームに装着し、評価結果をリアルタイムに知識ベースに蓄積することで、Android アプリのリスクを統合的かつタイムリーに判定するソフトウェアを構築した。 ・暗号化したままセキュリティレベルの更新と加算と乗算が可能な格子理論ベースの準同型暗号方式 SPHERE（スフィア）を高度化し、実用的な時間で暗号化したままデータを分類できるビッグデータ向け解析技術（ロジスティック回帰分析）を開発した。 ・今後のプライバシーに関する諸問題の検討の場として有識者を交えたプライバシー検討 WG を立ち上げ、データ収集時の適切な同意取得やプライバシーリスク評価に関する議論を開始した。

（ウ）	総務省	総務省において、利用者の行動特性等を利用した、標的型攻撃等の新たなサイバー攻撃への対策技術に関する研究開発を実施する。	・ 総務省において、利用者の行動特性等を利用した、標的型攻撃等の新たなサイバー攻撃への対策技術に関する研究開発を実施。
（エ）	経済産業省	経済産業省において、CSSC を通じて、システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト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、システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を行った。
（オ）	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。	・ サイバーセキュリティ研究基盤(NONSTOP)を構築し、ダークネット観測結果やマルウェア等の安全な情報遠隔利用システムを構築し国内複数大学等をユーザーとした運用を行った。また、マルウェア対策研究人材育成ワークショップでも NONSTOP 経由でのデータセット提供し人材育成に貢献した。
（カ）	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、共有する体制の構築を開始した。
（キ）	総務省 経済産業省	総務省及び経済産業省において、IoT 機器へのバックドア対策のためのログ検知技術の開発に関する研究や、高信頼な暗号の実装を実現する技術やハードウェアトロージャン検知の技術等ハードウェアの真正性の向上に係る技術の開発に関する研究、IoT システムに対応したセキュリティ評価認証制度の確立に向けた検討を行う。	・ 多様な機器が接続される IoT システムにおいて、制御機器向けのビッグデータ I 等を用いたサイバー攻撃の予測技術と自動更新技術や、末端のセンサー等の IoT 機器に搭載でき、膨大なデータを低消費電力で暗号化する技術を開発するための予算化を図った。また、内閣府と連携して、ログ検知技術や、小型で強固な暗号処理とハードウェアトロージャン対策が講じられたセキュアチップの開発等を実現するための研究プログラム（SIP）立ち上げに協力を行った。

(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 2015	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。	・ 研究開発戦略専門調査会にて、心理的側面など、技術以外の観点も含めた議論を行った。
(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。	・ 2030 年の IoT 社会の深化に向けて分野横断で不可欠な、高度なデータの利活用を可能とする次世代のデータ収集・蓄積・解析技術及びセキュリティ技術の研究開発テーマ等研究開発の基本計画の策定に向け、企業や大学等(30 者程度)にヒアリング等を NEDO とも連携して実施。
(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。	・ 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開始するとともに、研究開発拠点を理化学研究所に新年度から立ち上げるための準備を行った。

(3) サイバーセキュリティのコア技術の保持

項番	担当府省庁	サイバーセキュリティ 2015	取組の成果、進捗状況
(ア)	総務省	総務省において、NICT を通じ、情報の円滑な利用を妨げず、必要な情報秘匿及び認証を両立するための研究開発を行う。	・ 暗号化したままセキュリティレベルの更新と加算と乗算が可能な格子理論ベースの準同型暗号方式 SPHERE（スフィア）を高度化し、実用的な時間で暗号化したままデータを分類できるビッグデータ向け解析技術（ロジスティック回帰分析）を開発した。今後のプライバシーに関する諸問題の検討の場として有識者を交えたプライバシー検討 WG を立ち上げ、データ収集時の適切な同意取得やプライバシーリスク評価に関する議論を開始した。
(イ)	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。	・ デコイ BB84 方式について、フィールド環境で長期動作し、かつ最新理論に則った安全性を保証する装置の開発をした。また、実際の量子鍵配送システムにおける統一的な安全性評価基準項目の選定・文書化を実施した。さらに、量子鍵配送により供給された鍵を、効率的に上位アプリケーションへと供給するシステムを開発した。
(ウ)	総務省 経済産業省	総務省及び経済産業省において、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、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。	・ 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て検討を実施することとした。
(エ)	経済産業省	経済産業省において、AIST 等を通じ、IoT システムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムの品質、安全性、効率を向上、両立させるための革新的、先端的技術の基礎研究に取り組む。	・ 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、大規模ソフトウェアの解析ツールを開発し、自動車等組込みシステムを題材に有効性を検証した。暗号技術においては、暗号化したままデータ処理や認証・認可を実現する高機能暗号技術について、高速処理を可能とする新方式や暗号文サイズが世界最小値となる技術を開発した。
(オ)	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。	・ 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。

(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 2015	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（2015 年９月、2016 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積極的に参加・貢献した。
(イ)	総務省	総務省において、近年、被害が拡大しているサイバー攻撃（DDoS 攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外の ISP、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するセンサーを設置し、諸外国と連携してサイバー攻撃の予兆を検知し迅速に対応することを可能とする技術について、その研究開発及び実証実験を実施する。	・ 我が国におけるサイバー攻撃のリスクを軽減するため、国内外の ISP、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するセンサーを設置し、諸外国と連携してサイバー攻撃の予兆を検知し迅速に対応することを可能とする技術について、その研究開発及び実証実験を実施。

(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 2015	取組の成果、進捗状況
(ア)	内閣府	内閣府において、2015 年６月 18 日の総合科学技術・イノベーション会議で追加が決定された、戦略的イノベーション創造プログラム（SIP）新規課題候補「重要インフラ等におけるサイバーセキュリティの確保」に対し、研究開発に向けた取組を推進する。	・ 第 12 回 CSTI（2015 年 11 月 10 日）での実施方針決定を受け、速やかに推進委員会を立上げ。2016 年１月末に委託先を決定、研究開発体制を整備し、研究開発に着手。

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 2015	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」に基づき関係施策を推進していく。	・ 普及啓発・人材育成専門調査会を開催し、各府省庁における施策について意見聴取等を実施した。現在の状況や社会的ニーズも踏まえ、2016 年度以降の人材育成に係る各施策を強化することを目的とした「サイバーセキュリティ人材育成総合強化方針」を３月 31 日にサイバーセキュリティ戦略本部で決定した。
(イ)	内閣官房	内閣官房において、人材育成に係る施策を総合的に推進するため、「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。	・ 普及啓発・人材育成専門調査会を開催し、各府省庁における施策について意見聴取等を実施した。現在の状況や社会的ニーズも踏まえ、2016 年度以降の人材育成に係る各施策を強化することを目的とした「サイバーセキュリティ人材育成総合強化方針」を３月 31 日にサイバーセキュリティ戦略本部で決定した。
(ウ)	経済産業省	経済産業省において、中長期スパンでの情報セキュリティを含めた IT 人材育成の在り方について、引き続き検討を進める。	・ セキュリティ人材の確保に関する研究会を開催し、産業構造審議会商務流通情報分科会情報経済小委員会 IT 人材ワーキンググループで提示された、今後必要な３つの情報セキュリティ人材（①ホワイトハッカーのような高度セキュリティ技術者、②ユーザー企業において社内情報セキュリティ技術者と連携して情報セキュリティ確保を確保する人材、③安全な情報システムを設計、開発、運用するために必要な情報セキュリティに関する知識・技能を身に付けた人材）の育成等の在り方を取りまとめた。

(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 2015	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。	・「情報技術人材育成のための実践教育ネットワーク形成事業」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きた。当事業において、主に大学院修士課程の学生を対象（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。	・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、産業界、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総合強化方針」（2016 年３月 サイバーセキュリティ戦略本部決定）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。	・「情報技術人材育成のための実践教育ネットワーク形成事業」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きた。当事業において、主に大学院修士課程の学生を対象（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。	・平成 27 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プログラム開発に係る予算を措置。高知高専が事業実施の中心となり、各国立高専におけるセキュリティ教育の現状について把握したうえで、高専共通の情報セキュリティのスキルセット及びカリキュラムの検討、教材の開発に着手した。
(オ)	内閣官房	内閣官房において、シンポジウムやセミナー等の啓発の場や情報共有の場を活用し、大学におけるサイバーセキュリティに関する教育の実施に資するような情報セキュリティに関する最新情報を提供する。	・・大学等における講演・セミナー等を通じ、サイバー空間における脅威の動向や我が国の政策等について情報提供を実施した。また、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、産業界、大学、各省との間の情報共有を行った。
(カ)	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。	・「情報技術人材育成のための実践教育ネットワーク形成事業」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きた。当事業において、主に大学院修士課程の学生を対象（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。
(キ)	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。（26 コース・受講者数 452 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　548 講座（2016 年３月末時点））
(ク)	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。	・サイバーセキュリティのスキル向上のための実践的取組の一つとして、実際に起きたサイバー攻撃の事例を基にした教材等の開発について検討している。

(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 2015	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、論理的思考力の育成等に関しては、教員の指導の参考となるよう、発達段階に応じたプログラミングの指導手引書を作成する。また、情報モラルについては、教員の指導に役立つ動画教材及び指導手引書を作成・普及し、情報セキュリティを含む情報モラルに関する教育の充実を図る。	・ 学習指導要領に基づく情報活用能力育成の推進を図るため、平成 27 年度において、教員の指導の参考となるよう、発達段階に応じたプログラミングに関する授業の事例を収集するとともに、情報モラルに関する動画教材や指導手引書を作成した。
（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。	・ 地方自治体の情報教育担当を集めて実施した会議（2015 年９月）において、情報セキュリティの取組に関する普及・啓発を実施した。 ・ 独立行政法人教員研修センターにおいて、各地域で情報教育を推進する中核的な役割を担う指導主事等を対象とした研修を実施し、教員の指導力の向上を図った（2015 年 10 月及び 2016 年１月）。
（ウ）	内閣官房	内閣官房において、教育機関で育成する人材のレベルの明確化と併せて、そうした人材を育成する教員にとって必要となるスキル育成の場や教員向けの教材等について、民間の能力の活用や、一線を退いた技術者等が活躍できる環境整備も含め、産学官が相互に連携しながら検討を進める。	・ 「サイバーセキュリティ戦略」に記載した「教員の情報通信技術を活用した指導力向上を目指した研修等の改善・充実を進める」について、教員の指導力向上を担う文部科学省に今後の対応等を相談している。

(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 2015	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。	・ セキュリティ・キャンプについて参加人数を 50 名として実施。専門講義の枠組みを変更し、高レイヤー・低レイヤー・検知・解析の４トラックから選択受講する枠組みとし、巧妙化するサイバー脅威に対応するため、幅広い分野のセキュリティ知識・技術を身につけることを可能とした。
（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 2015」）について経済産業省において普及・広報の支援を行う。	・ SECCON CTF 2015 について経済産業省からの後援名義による広報の支援を行うとともに、決勝大会（国際大会）において、日本チーム参加者全員に経済産業大臣名による激励文を発出し、日本における今後の活躍を期待することで、更なるスキル、知識醸成の意識高揚を行った。
（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・育成事業として 23 名のクリエイターを発掘・育成。また、セキュリティを専門分野とするプロジェクトマネージャーの追加を検討し、2016 年度の事業から選任の見込み。

(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 2015	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。	・ 企業や大学・高専など約 200 件を訪問し、IT に関する唯一の国家試験である情報処理技術者試験の普及を図った。

（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（仮称）」の創設を検討する。	・「情報セキュリティマネジメント試験」の 2016 年 4 月からの実施に向けて、情報処理技術者試験規則等の関係省令を改正。
（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。	・・高等教育機関の情報系学科の学生等に IT 業務の魅力を紹介する広報誌 30,000 部を配布し、IT が支える・変える未来イメージ、産業界で活躍する人物像の紹介やスキルアップの必要性を伝えた。
（エ）	経済産業省	経済産業省において、情報処理技術者試験にサイバーセキュリティに従事する者の実践的な能力を適時適切に評価するための更新制度を導入するため必要な措置をとる。加えて、行政機関等における人材登用でこれらの能力評価制度を積極的に活用する方策を検討する。	・最新のセキュリティに関する知識・技能を備えた、高度かつ実践的な人材に関する国家資格である「情報処理安全確保支援士」制度の創設に向けて、産業構造審議会商務流通情報分科会情報経済小委員会試験ワーキンググループを設置し、本制度に係る資格登録・更新制度の具体的な設計方針を取りまとめた。 ・「サイバーセキュリティ人材育成総合強化方針」において、民間企業等における能力評価制度の活用促進策を盛り込んだ。

(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 2015	取組の成果、進捗状況
（ア）	防衛省	防衛省において、高度化するサイバー攻撃等への適切な対処態勢を維持するため、人材育成の取組として、国内外の大学院等への留学等を推進する。	・サイバー攻撃等対処に向けた人材育成の取組として、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す人材の育成を実施した。
（イ）	総務省	総務省において、官公庁や企業等組織における実践的サイバー防御演習（CYDER）の基盤の強化及び拡充を通じた実践的なサイバーセキュリティ人材の育成について検討を行う。	・2015 年 10 月より、官公庁・重要インフラ事業者等の LAN 管理者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）を計 7 回実施（含：National 318 EKIDEN 2016）。
（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。	・サイバー演習環境の構築技術に関する研究試作を実施した。また、その研究成果を受け、実践的なサイバー演習環境の整備を開始した。
（エ）	防衛省	防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための具体的・実効的連携要領の確立等に向けた共同訓練を実施する。	・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共同訓練を 2016 年 2 月に実施した。

5. 推進体制

項番	担当府省庁	サイバーセキュリティ 2015	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、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則り 2015 年度当初からリエゾンを配置するとともに情報共有のための枠組み（運用要領）を整備して既存のシステムを活用して暫定的に情報共有を開始した。 ・ NISC の情報システムの換装に合わせて新たに JPCERT/CC 情報共有のためのシステムを構築し 2016 年３月より運用を開始した。 ・ 専従の CSIRT 組織を整備すべく、その中核となる要員の定員要求を実施した。 ・ 総合的分析機能の強化を図り、司令塔機能の強化促進に努めた。
(イ)	内閣官房	内閣官房において、東京オリンピック・パラリンピック競技大会を始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。	・ 大会運営に係る重要システム・サービスの候補を抽出するとともに、所管省庁を通じて一部の事業者に対して NISC で作成したリスク評価手順案のトライアル実施を依頼し内容の充実を図った。 ・ 国内外の CSIRT に関する調査研究を実施し情報収集をするとともに関係府省庁、オリパラ組織委員会及び情報セキュリティ関係組織で構成するサイバーセキュリティ体制に関する検討会を立ち上げ検討を推進した。2015 年度は主に情報共有体制について検討した。
(ウ)	内閣官房	内閣官房において、2016 年に開催される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。	・ 会議開催府省連絡会合を開催し、準備状況の確認を実施するとともにセキュリティ対策についての情報共有を実施した。 ・ サミット等会議へリエゾンを派遣しインシデント発生時の情報共有を行うためにリエゾンプロジェクトチームを立ち上げ、各府省の準備段階から情報共有を実施した。 ・ サミット等会議に関連するシステムのインシデント発生時の情報共有体制の確認を実施するとともに、情報伝達訓練を実施した。
(エ)	内閣官房	内閣官房において、IPA との連携をはじめ、高度セキュリティ人材の民間登用等により NISC の対処能力の一層の強化を図り、インシデント発生時に適切に NISC へ情報が集約されるよう関係省庁（幹部クラスを含む）との迅速な情報共有体制を構築する。	・ 内閣官房において、任期付職員の採用等を行い、NISC の更なる要員強化を行った。また、「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）」を策定し、その中において、政府における人材確保・育成の一環として、即戦力となる高度専門人材を外部から受け入れることとした。また、インシデント発生時の NISC への情報集約については、サイバーセキュリティ戦略本部重大事象施策評価規則（平成 27 年２月 10 日サイバーセキュリティ戦略本部決定）及びサイバーセキュリティ戦略本部資料提供等規則（平成 27 年２月 10 日サイバーセキュリティ戦略本部決定）等を適切に運用することにより、情報共有体制の構築及び適切な運用を行っている。
(オ)	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、幹部も含めた組織的対応体制の構築や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。	・ サイバーセキュリティ対策推進会議議長による指示の下、各府省庁における CSIRT 体制、対処手順等に係る課題等を調査し、その結果を踏まえ、各府省庁に対して CSIRT 体制・連携体制等の強化の指示を行った。【再掲】 ・ 上記の取組や昨今のサイバーセキュリティについての情勢等を踏まえ、CSIRT 体制やインシデント対処の在り方を検討し、その内容を統一基準群にの改定案にまとめた。【再掲】

（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

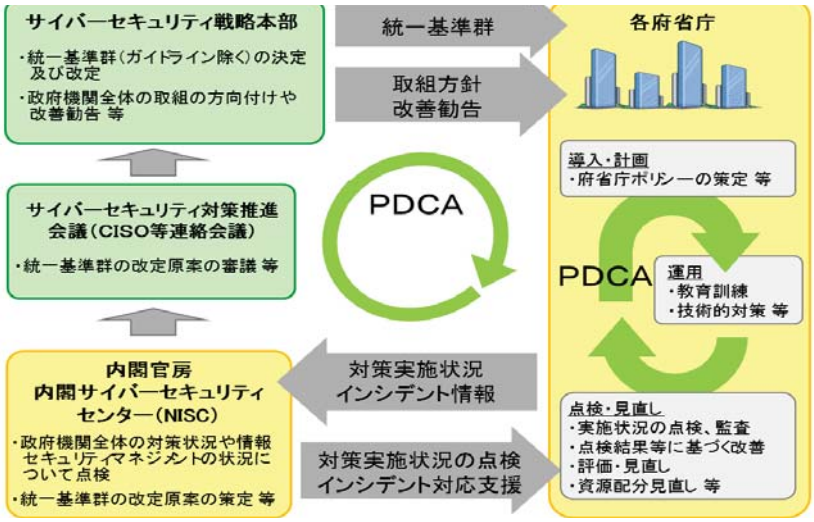
１　概要

「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、府省庁が講ずるべき情報セキュリティ対策のベースラインを定めたものであり、2005年12月の情報セキュリティ政策会議（現サイバーセキュリティ戦略本部）において初版が決定されて以来、情報セキュリティを取り巻く情勢の変化等に応じた改定を重ね、現在は、2014年５月19日に決定された統一基準群（平成26年度版）が運用されている。

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た上で、統一基準群に準拠した府省庁の情報セキュリティポリシー（以下「府省庁ポリシー」という。）を定め、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。

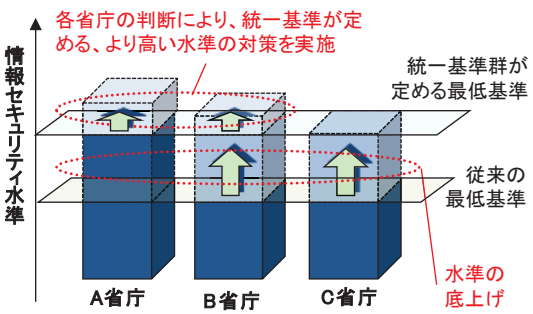
政府機関の情報セキュリティ対策は、統一基準群及び府省庁ポリシーの策定・見直しを含む、①各府省庁におけるPDCAサイクル、②政府機関全体としてのPDCAサイクルの２つのメカニズムにより、継続的に取り組まれている。（図表１）

図表１　政府機関における情報セキュリティのマネジメントサイクル



統一基準群の運用開始以来10年が経過したが、その間の取組や都度の見直し等によって、府省庁の情報セキュリティ対策の強化が図られるとともに、政府機関全体の情報セキュリティ対策水準が底上げされるなど、一定の効果が得られている（図表２）。

図表２　統一基準群の効果（イメージ）



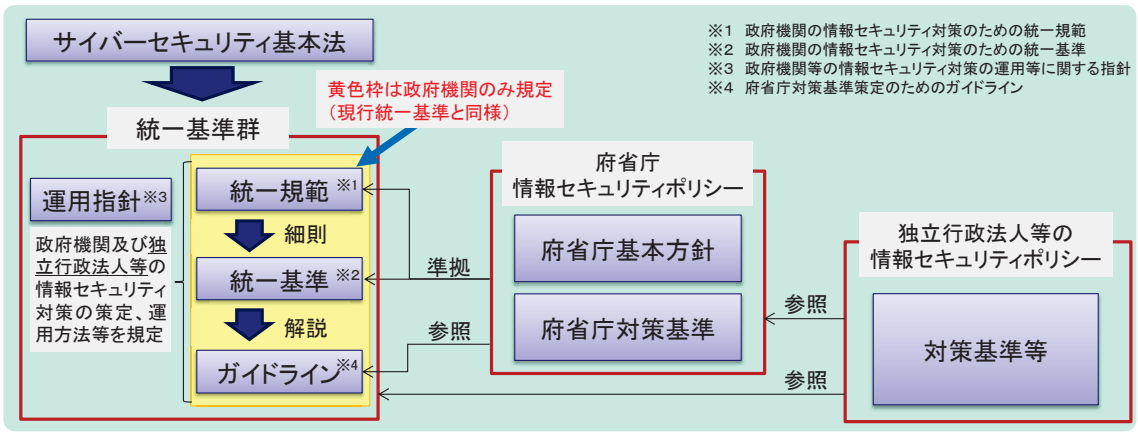
２　統一基準群の改定に係る検討

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、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等を受け、サイバーセキュリティ戦略本部による監査の実施や独立行政法人等への対策範囲の拡大等、政府機関等におけるサイバーセキュリティの確保に係る様々な取組が行われている。また、2015年５月の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を踏まえ、情報システムの重要な情報を扱う部分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が進められるなど、政府機関等を標的とした様々なサイバー攻撃に対抗するための対策が実施されている。加えて、クラウドサービスやテレワーク環境の利用が促進されるなど、政府機関等におけるITを利活用した業務形態を取り巻く環境も継続的に変化している。

このような政府機関における取組や脅威等の動向を踏まえ、2015年より統一基準群の改定に向けた検討を開始し、2015年度末までに改定の素案を策定した。各府省庁との調整及びパブリックコメント募集等を経て、今夏までに改定案を決定すべく検討を進めている。

今般の改定においては、まず、サイバーセキュリティ基本法と統一基準群との関係性の整理及び統一基準群の独立行政法人等への適用範囲の拡大を図るべく、サイバーセキュリティ基本法第25条に掲げられている「国の行政機関及び独立行政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」として統一基準群を位置づけることとし（図表３）、ドキュメント構成の見直し及び所要の規定の追加を検討した。

図表３　統一基準群改定内容①　サイバーセキュリティ基本法との関係



その他の主要な改定内容については、図表４に示すとおりである。2016年夏までに改定案を決定し、その後、府省庁ポリシーへの速やかな反映を促進し、各府省庁において新ポリシーの下で情報セキュリティ対策が更に強化されるよう、改定版統一基準群の理解度向上のための講習の実施や、各種マニュアル・ひな形の提供等を検討し、政府機関等におけるサイバーセキュリティが適切に確保されるよう、取組を進める。

図表４　統一基準群改定内容②　主な改定内容

統一基準群の改定概要

独立行政法人等への適用対象範囲の拡大

所管府省庁の助言等の下、情報セキュリティ対策が適切に講じられるよう、統一基準群の適用対象範囲を**独立行政法人等へ拡大**する。

例：インシデント発生時の連絡体制の整備等の情報セキュリティ対策の策定

監査に係る規定の整備

監査に係る規定を整備し、政府機関及び独立行政法人等の情報セキュリティ・マネジメントシステム（PDCAサイクル）を強化する。

例：戦略本部による監査実施を、情報セキュリティマネジメントシステムの一部を構成するものと位置づけ

サイバー攻撃を前提とした防御力の強化・多層的対策

日本年金機構の情報流出事案等を踏まえ、**サイバー攻撃を前提とした防御力の強化・多層的な対策**の推進を目的とした対策事項を規定する。

例：インターネット接続口の集約、重要な情報を扱う部分のインターネットからの分離

新たなIT製品・サービスの普及等に伴う対策の強化

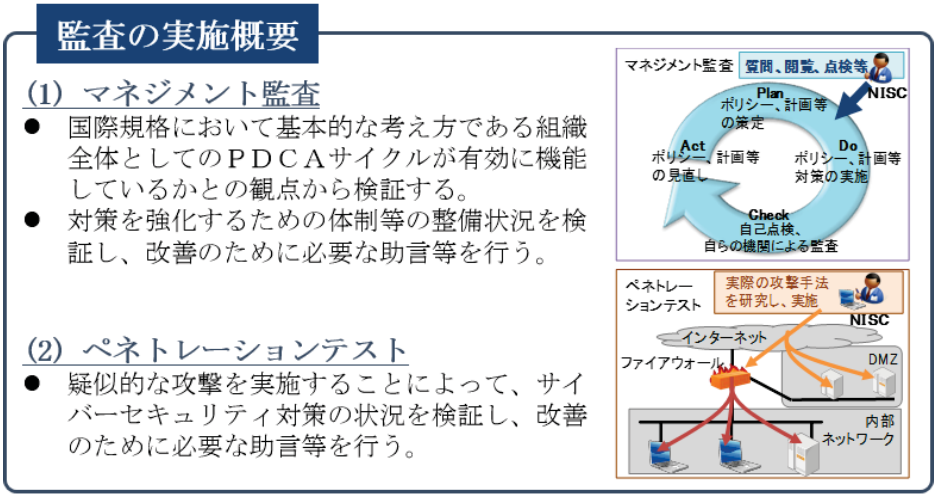
新たなIT製品・サービスの普及等に伴う対策の強化として、クラウドサービス利用時の対策事項等を規定する。

例：クラウドサービスの利用時やデータベースの構築運用、アプリケーションコンテンツの提供等に特有のセキュリティ対策の整理

別添３－２　サイバーセキュリティ基本法に基づく監査

１　2015 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の実施初年度である2015年度は、政府機関を対象として、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。



２　2015 年度における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

2015 年４月から 2016 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、10 の府省庁を対象とした。

（３）マネジメント監査の実施内容

「政府機関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、サイバー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、自律的なサイバーセキュリティ対策の水準の向上を促す仕組みを確立するため、点検を目的とした従来の施策等の統合も視野に入れた監査制度を設計するとともに、当該制度の有効性の検証を目的として、試行的な監査を実施することとした。試行的な監査については、各府省庁が実施している情報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、2016 年度以降の本格的な監査制度の運用に資することを考慮し、各府省庁のサイバーセキュリティ対策の実施状況を把握した上で、その維持改善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とした。

（４）マネジメント監査の実施結果

マネジメント監査制度の設計及び当該制度の有効性の検証を目的とした試行的な監査を実施した。試行的な監査においては、2016 年度以降の本格的な監査制度の運用に資することを考慮するとともに、被監査主体に対しては、改善のために必要な助言等を行った。

また、本格的な監査を実施するために必要な監査制度の枠組みを確立するとともに、「サイバーセキュリティ対策を強化するための監査（マネジメント監査）に係る実施要領」として 2016 年３月 29 日開催のサイバーセキュリティ対策推進会議にて各府省庁と申し合わせた。

なお、試行的な監査におけるグッドプラクティスの事例と主な助言等は以下のとおりである。

① グッドプラクティスの事例

- 「新・情報セキュリティ人材育成プログラム」（2014 年５月 19 日 情報セキュリティ政策会議決定） の「３．（５）①　サイバー空間を取り巻くリスクに対応できる職員の採用・育成」にある「一定の専門的知見を持った職員」配置の必要性を踏まえ、民間企業や大学院への派遣により IT 専門知識を有する職員の育成に係る取組を継続的に行い、かつ、この取組で得た知識を生かすことが可能なポストへの配置等が行われていた事例
- 内部監査において、監査計画の立案、計画的かつ全国的な監査の実施、チェックシートを使った監査の品質管理、監査結果の報告及び被監査主体に改善を求め、対処結果を報告する仕組みを整備・運用して PDCA サイクルを適切に回し、さらに、毎年度、情報セキュリティニュースにおいて、主な指摘事項毎にとりまとめて解説し、監査結果の組織内への浸透を図っていた事例

② 主な助言等

2015 年度の試行的な監査においては、以下に示す主な監査項目について、被監査主体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
- 情報セキュリティの脅威に対する対策の適切性
- 情報の取扱いに係る整備及び運用状況
- 外部委託に係る整備及び運用状況
- CSIRT に係る整備及び運用状況
- 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整備及び運用状況
- 情報システムの構成要素に係る整備及び運用状況
- 情報システムの利用に係る整備及び運用状況

３　2015 年度における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

2015 年４月から 2016 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（2015 年４月１日時点で 21 の府省庁）が運用するインターネットに接続する基幹 LAN システム及び重要な情報を取り扱う情報システムの中から、希望のあった 52 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及び情報システム内部の端末がウイルス感染したとの想定での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では、侵入できる脆弱性がいくつかの情報システムで発見された。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た脆弱性を認知した場合には、当該府省庁に速やかに対処を求めるとともに、対処計画の策定又は対処結果の報告を求めた。その結果、調査中において侵入に利用できた脆弱性については、全て対策が施された。

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も視野に入れた助言等を行った。

別添３－３　重点検査による評価

１　目的

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　検査基準日

2015年10月１日

３　検査項目と結果

検査項目		検査項目とした理由	実施率※
ウェブアプリケーションへの既知の攻撃手法に対する対策	SQL インジェクション攻撃への対策実施に関する確認状況	公開ウェブサーバに対する脆弱性検査において過去に数多く検出されたSQLインジェクション脆弱性、クロスサイトスクリプティング脆弱性について、対策の実施状況を把握するため。	96%
	クロスサイトスクリプティング攻撃への対策実施に関する確認状況		95%
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。	61%
技術的な情報セキュリティ対策	Adobe Flash Player の脆弱性への対応状況	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。	96%
	一太郎 Government 7 の不正なアップデートモジュールへの対応状況		100%

※小数点以下四捨五入

４　所見

情報の漏えいや改ざんの被害につながる危険性の高い脆弱性のうち、2014年度に引き続きSQLインジェクション及び2013年度の検査にて危険性の高かったクロスサイトスクリプティングの脆弱性について検査を実施した。

検査基準日において、各脆弱性が存在し得るウェブサイトを持つ情報システムの確認を行ったのは、情報システム全数のうち、SQLインジェクションが96%、クロスサイトスクリプティングが95%であった。未確認の情報システムについては、未確認の理由及び当該理由の妥当性を確認し、必要に応じて更なる確認を促した。また、確認の結果、当該脆弱性が存在する可能性があると判断された情報システムについては、迅速な対策の実施を促し、代替等の対策を既に実施している情報システムを除いて、対策の実施は完了した。

本検査により、複数の情報システムにおいて当該脆弱性が存在する可能性があることが判明したことから、今後も、各府省庁においては、当該脆弱性に係る情報を随時収集するとともに、定期的な検査を実施するなどして当該脆弱性への対策を強化していくことが重要である。

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を用いた対策の実施率は61％であり、2014年度と比較して若干下回る結果となった。これは、情報システム自体を自府省庁内における設置・運用から民間の外部サービスを利用するケースが増加したものの、当該外部サービスにおいて、送信ドメイン認証技術が導入されていなかったこと等が影響しているものと考えられる。

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。併せて、2016年度以降においても、重点検査等の機会を通じて、当該対策の導入の推進を促してくことが必要である。

また、認証結果にかかわらずメールを受信している情報システムにおいては、当該府省庁が取り扱う情報の重要性、情報システムの特性等を踏まえ、なりすましメールを受信することによるリスクを評価した上で、送信ドメイン認証結果の活用の要否を検討することが望まれる。

技術的な情報セキュリティ対策について、ソフトウェアの重大な脆弱性への対策状況について検査を実施した。Adobe Flash Playerの重大な脆弱性については、検査基準日時点で、対策の実施率は96％であった。対策の実施が完了していない情報システムについては、迅速な対応の実施を促した。

なお、インターネットとの通信を遮断するなど別途の対策を実施している情報システムを除いて、対策の実施は完了している。

また、一太郎Government 7の不正なアップデートモジュールへの対応については、検査基準日時点で、対策の実施は完了している。

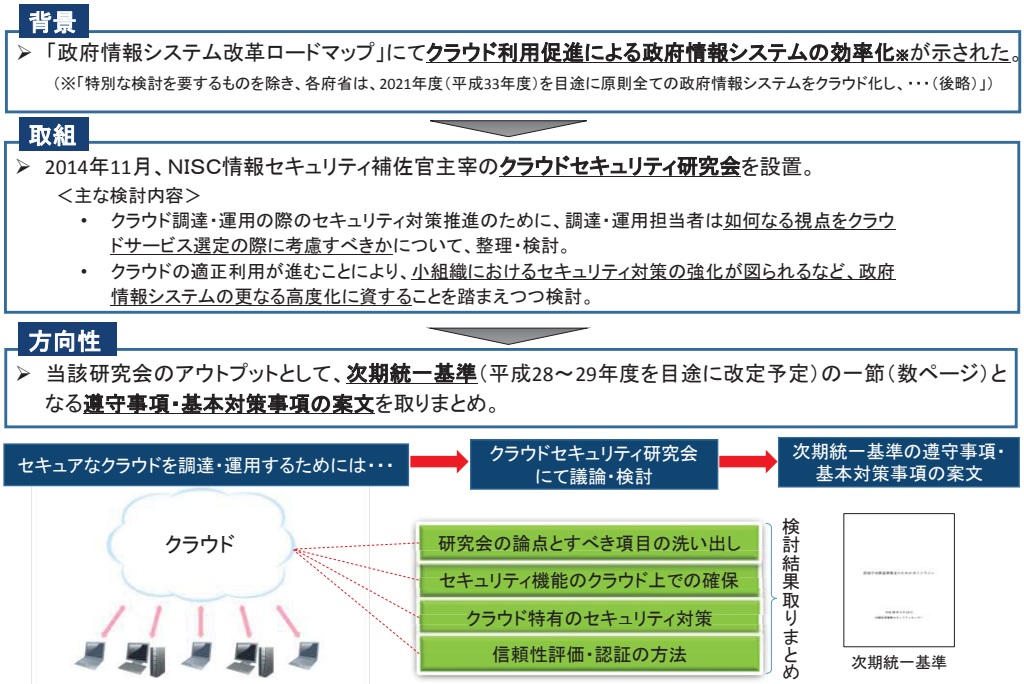
今後も、各府省庁においては、ソフトウェアの脆弱性に係る情報を随時収集の上、必要な対策を適宜実施していくことが重要である。また、情報システムの特性等に鑑みて、ソフトウェアの脆弱性への即時の対策の実施が困難な場合であっても、暫定的に当該脆弱性が悪用されるリスクの低減を図るとともに、システム構成、運用方法等を改善し、可能な限り速やかに恒久的な対策が実施できるようにすることが重要である。

別添３－４　クラウドサービスの利用に係る対策

2014年５月に改定された「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）」（以下「統一基準群」という。）において、クラウドサービスを含む種々の約款への同意によって利用可能となる不特定利用者向けの外部サービスの利用について、「約款による外部サービスの利用」として規定したところであるが、これは府省庁におけるクラウドサービスの利用に特化して、業務への利用可否の判断や利用の際の安全管理措置等に関する基準を明確にするものとはなっていなかった。

一方、各府省情報化統括責任者（CIO）連絡会議において2015年３月に改定された「政府情報システム改革ロードマップ」には、政府情報システムの効率化のために、「業務の見直しも踏まえた大規模な刷新が必要な情報システム等の特別な検討を要するものを除き、各府省は、2021年度（平成33年度）を目途に原則全ての政府情報システムをクラウド化し、（後略）」という旨が盛り込まれている。

これまでにもクラウドサービスの調達・提供側それぞれ向けに、「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（2014年３月、経済産業省）」や、「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（2014年４月、総務省）」といった文書が策定されているところ、今後政府機関におけるクラウドサービスの利用が更に拡大していくことが見込まれる中、クラウドサービス調達の際のセキュリティ対策を検討するに当たり、政府担当者として考慮すべき視点や基本的な考え方について整理するため、クラウドサービスに係る事業者・有識者等から構成される研究会を開催した。また、研究会で整理した結果を統一基準群に反映するため、原案を府省庁等に提示して意見交換を行うとともに、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を実施した。



別添３－５　高度サイバー攻撃への対処

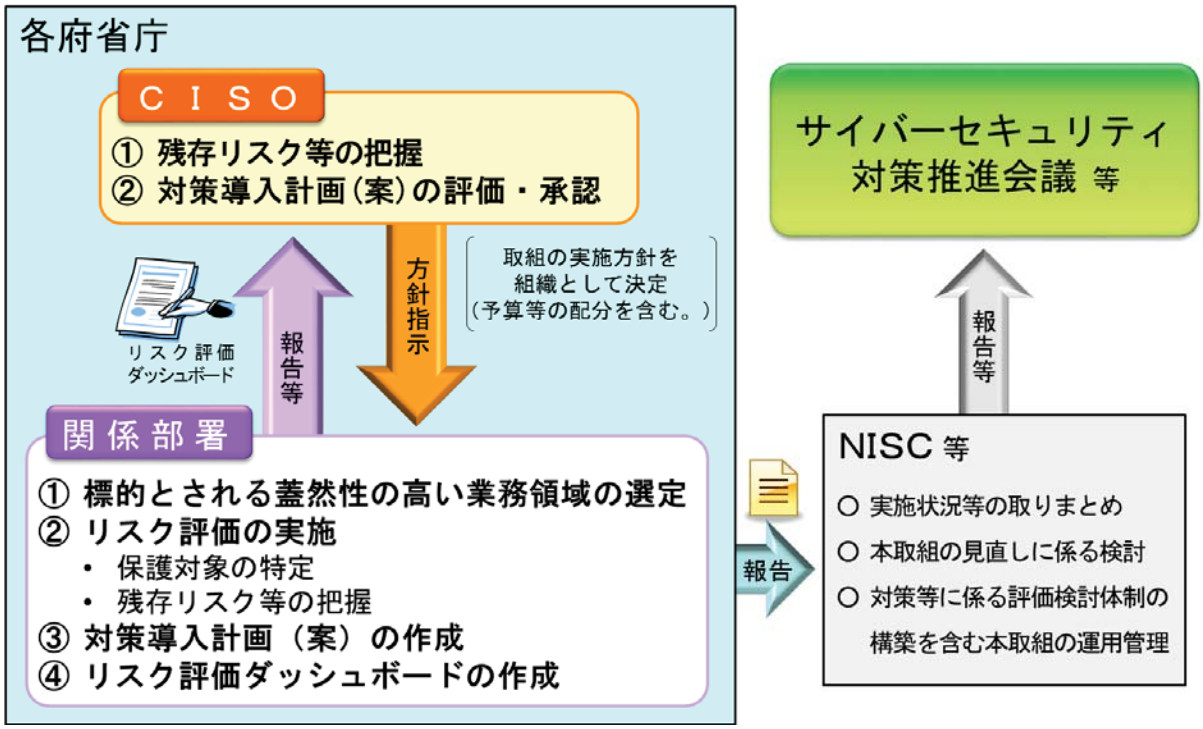
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

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。

2015年度の対策実施状況の総論としては、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100の業務領域に使用されているおよそ40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た。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いる。

今後も、計画に基づき着実に対象システムの標的型攻撃対策を強化していくとともに、2015年６月に明らかとなった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の教訓等を踏まえ、重要なシステムのインターネットからの分離、インターネット接続口の統合・集約、情報システムにおける電子メールに添付された実行プログラム形式のファイルに係る取扱の制限、ガイドラインに掲載されている標的型攻撃手法や対策の見直し、標的型攻撃発生時に適切に対応する体制の整備・強化等を推進することで、高度サイバー攻撃への更なる対処を推進していく。

別添３－６　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。

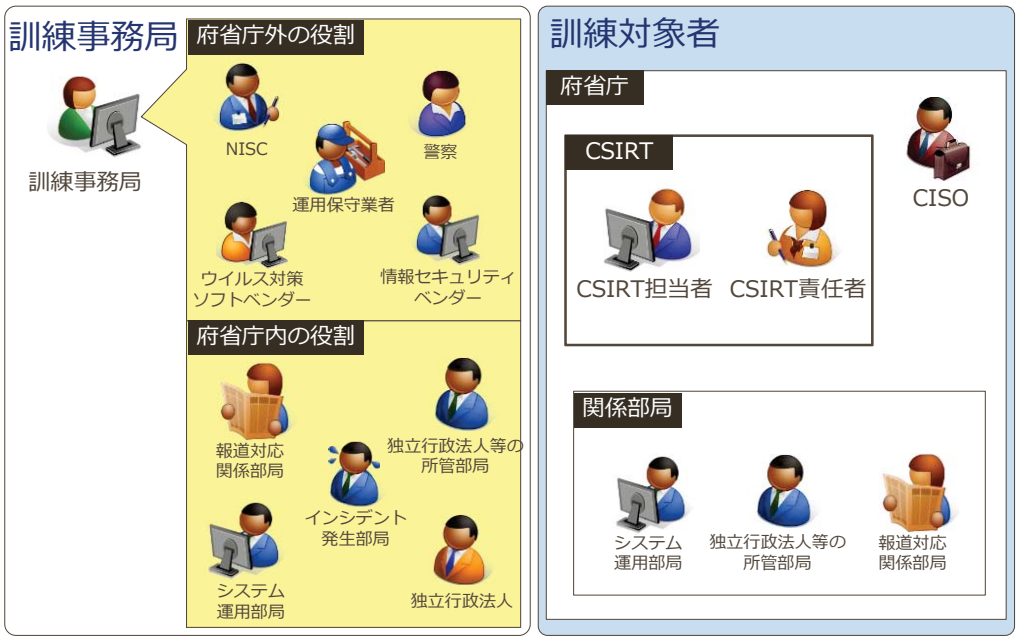
（２）概要

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）とのやりとりを通じて訓練を進行した。

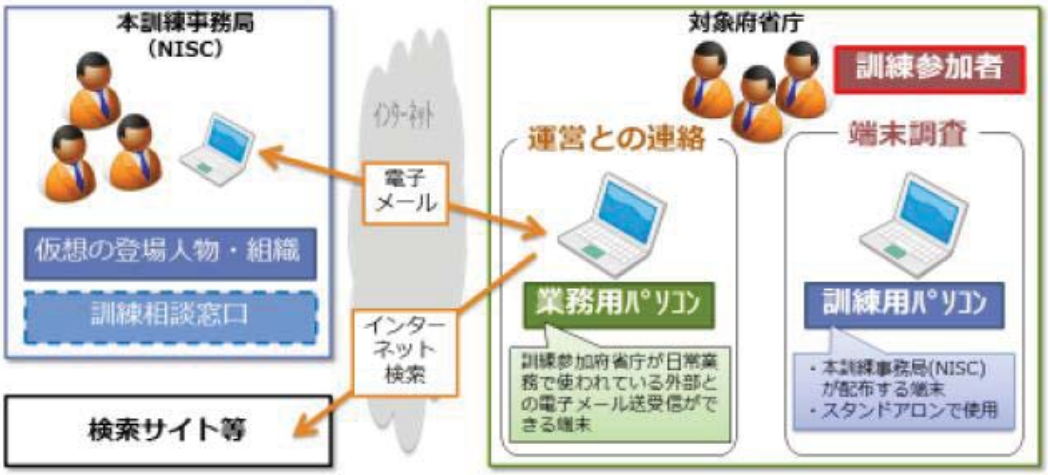
訓練参加者は、府省庁内外の様々な登場人物を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、訓練用のツールや解析対象となるデータを保存した訓練用パソコンを操作することにより、保全したハードディスクイメージや通信ログの分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

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100人（全22府省庁参加）

（４）訓練時期

2016年２月～３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、情報セキュリティインシデントであるかの評価、CISOやNISC等への報告・連絡に関する課題、改善点等を見出すことができたことが確認された。

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、2016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。

（２）対象

各府省庁のCSIRT要員等

（３）内容

回	時期	テーマ	講師	参加人数
1	2015年 ８月	・サイバー攻撃事例 ・サイバー攻撃の発生に備えた事前確認と対処事項	NISC 職員	約 50 人 （計１回開催）
2	2015年 10 月	・最近のサイバー攻撃手口 ・ログを活用したサイバー攻撃の早期発見と分析 ・民間企業における CSIRT に関する取組の工夫	NISC 職員 一般社団法人職員 民間企業社員	約 50 人 （計１回開催）
3	2016年 ２月～ ３月	情報セキュリティインシデント発生時の対処に必要な基礎知識 ・情報セキュリティインシデント対処概論 ・ケーススタディで学ぶインシデント対処 ・ハードディスクの分析手法 ・ログ分析手法	民間企業社員	約 60 人 （計３回開催）

３　NISC 情報セキュリティ勉強会

（１）目的

情報セキュリティに関連する研究機関や情報セキュリティベンダー等からの知見の提供により、情報セキュリティ関係職員の基本的知見を向上し、政府機関等における対策の参考とする。

（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、独立行政法人等の情報セキュリティ担当職員等

（３）内容

回	時期	テーマ	講師	参加人数
1	2015 年 9月	・情報セキュリティ上のサプライチェーン・リスク対応について ・標的型攻撃対策について	NISC 職員	第一部：123 名 第二部：179 名 （計2回開催）

2	2015 年 11 月	統一基準群に基づく情報セキュリティ監査について ・基礎編　監査の基本知識、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 ・NISC 情報セキュリティ指導専門官	第一部【基礎編】 （独法等対象） 141 名参加 第二部【基礎編、実践編】 （府省庁対象） 113 名参加 （各 1 回開催）
3	2016 年 1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（案）の検討状況について ・社会的出来事（安全保障や外交）と連動した「サイバー攻撃」 ・拡大する「攻撃側と防御側の格差」の状況理解と最近の手口	・NISC 職員 ・株式会社サイバーディフェンス研究所社員	173 人 （計 1 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

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対象に、NISC職員が各府省庁等に出向いて、情報セキュリティインシデント対応に係る基礎的な講義を行うことにより、情報セキュリティ対策の重要性やインシデント発生時の初動対応等について認識させる。

（２）対象

各府省庁の独立行政法人等を所管する部署の管理職や独立行政法人の役員等

（３）内容

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を踏まえ、標的型メールを事例として、サイバー攻撃の実情やリスクを紹介し、標的型攻撃対策として各組織の責任者がどのような対応を平素から取っておくべきか、また、インシデントが発生した際の対応において留意すべき点等について具体的に紹介した。

実施時期：平成27年10月～12月

開催回数：計７回

参加人数：約420名

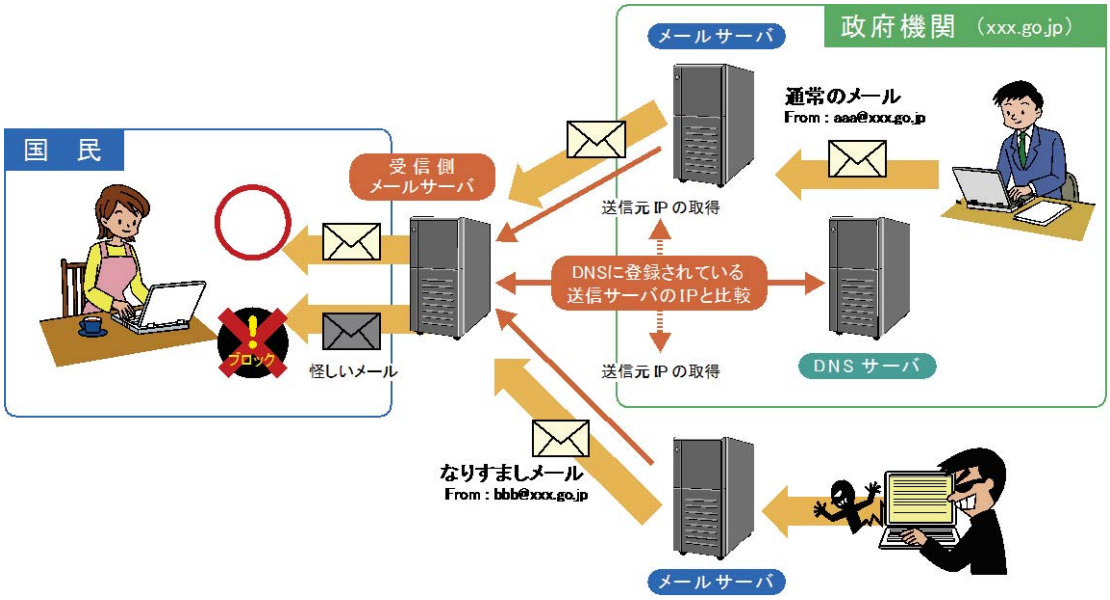
別添３－７　なりすまし防止策の実施状況

１　取組の概要

政府機関になりすました電子メールを一般国民や民間企業等に送信し、電子メールに添付したファイルを実行させて不正プログラムに感染させることで、重要な情報を窃取するなどの攻撃が発生している。なりすましの手段として、悪意ある第三者が、電子メールアドレスのドメイン（@マーク以降）を、政府機関のドメイン（xxx.go.jp）に詐称するものがある。

これまで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、「政府機関の情報セキュリティ対策のための統一基準」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た。

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[1]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。

[1] SPFにおいて、そのドメイン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

2015年及び2016年の１月末時点での、政府機関のドメインにおける送信側の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における送信側のSPFの設定状況

ドメインリスト取得日	-all※1	~all※2	設定なし
2015 年１月末	80.8%	11.7%	7.5%
2016 年１月末	71.7%	13.2%	15.1%

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

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

調査の結果、SPFの設定状況は１年前と比較して、適切な設定がなされている割合がやや低下していることがわかった。主な原因として考えられるのは、この１年の間に消滅した政府機関のドメインが全体の約８％あり、その中で適切なSPF設定をしていたものが９割を超えていた反面、新規に取得したドメインは全体の約７％あるうち、それらの半数近くが適切な設定がなされていなかったことが挙げられる。今後は新規のドメインに対し、然るべき設定がなされるよう、必要な取組を推進する。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について、2014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。

別添３－８　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」[2]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

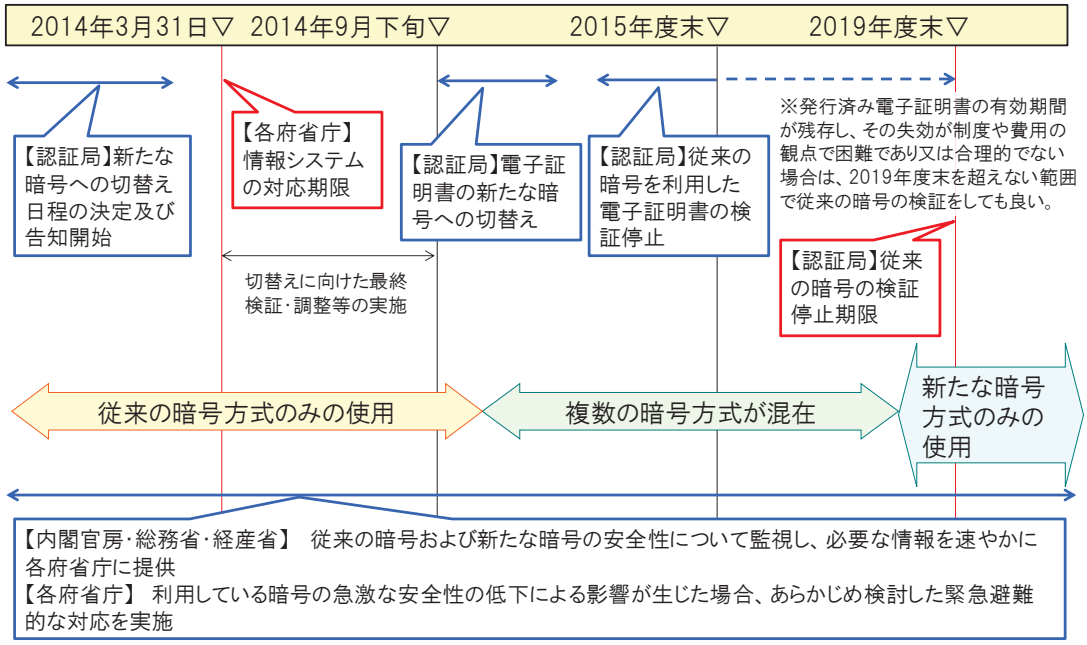
  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  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



[2] 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）

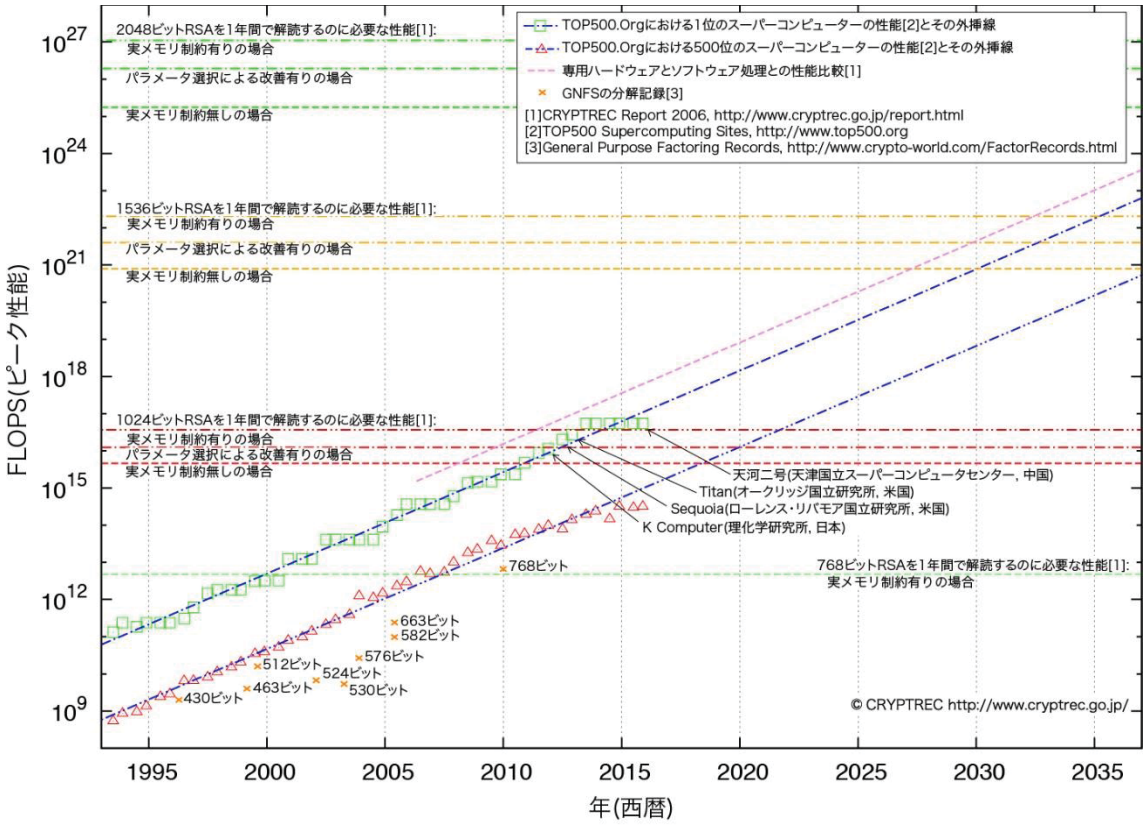
（参考）暗号の危殆化

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年間でふるい処理を完了するのに必要な処理性能の予測（2016年２月更新）[3]



[3] http://www.cryptrec.go.jp/report.html

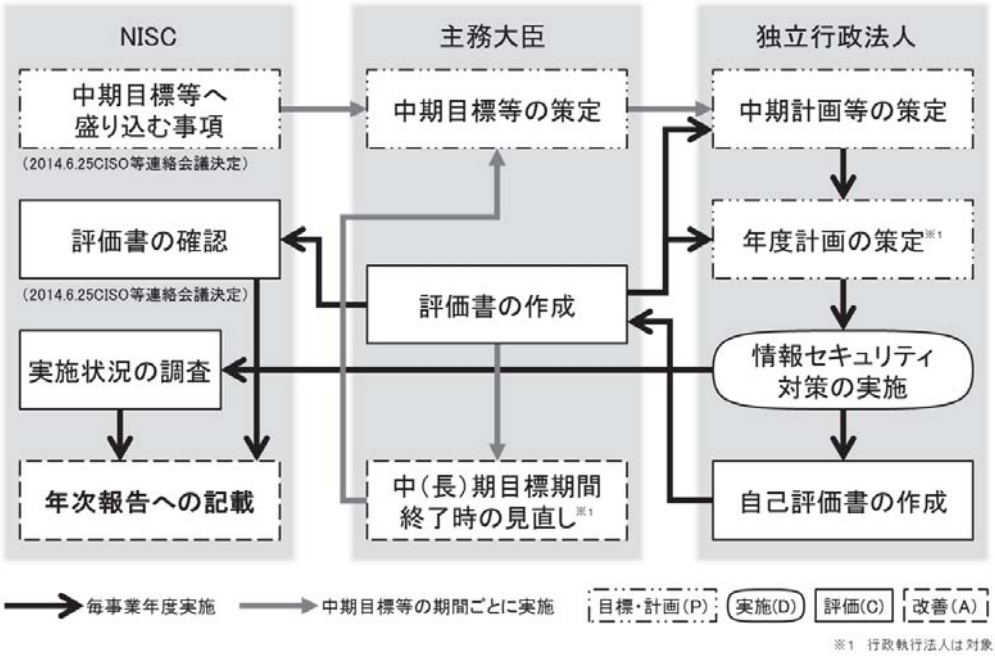
CRYPTREC Report 2015 暗号技術評価委員会報告（CRYPTREC、2016 年６月）

別添３－９　独立行政法人等における情報セキュリティ対策の調査結果の概要

１　調査目的

独立行政法人における情報セキュリティに係る取組は、サイバーセキュリティ戦略（2015年９月４日　閣議決定）において、法人の特性等を踏まえつつ、政府機関の取組に準じて対策を推進することとされている。また、独立行政法人における情報セキュリティ対策の推進について（2014年６月25日　情報セキュリティ対策推進会議決定）において、政府機関における情報セキュリティ対策を踏まえ、独立行政法人の年度計画、中期目標等に情報セキュリティ対策を講じる旨を盛り込むことや、主務大臣による業務実績評価時における情報セキュリティ対策の確認等を通じて情報セキュリティ対策の強化を図ることとされている。

図表１　独立行政法人の情報セキュリティ対策に係る取組の概要



このような背景から、独立行政法人並びに国立大学法人及び大学共同利用機関法人[4]における情報セキュリティ対策の実施状況を明らかにし、その結果を共有するとともに、情報セキュリティ対策の強化を図るため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：98法人 ／ 国立大学法人等：90法人

計　188法人（2016年３月末日現在）

（２）調査時点

2016年３月末日

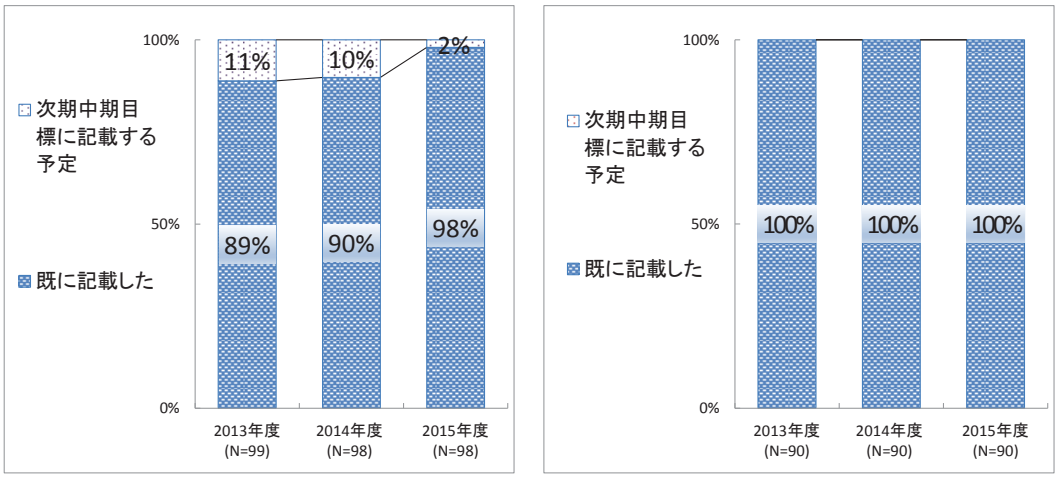
[4] 本調査では、国立大学法人及び大学共同利用機関法人を「国立大学法人等」という。また、独立行政法人及び国立大学法人等を「独立行政法人等」という。

３　調査結果

（１）中期目標等における記載状況

中期目標等における情報セキュリティ対策の記載状況は以下のとおりである。

図表２　中期目標等での記載状況（左：独立行政法人、右：国立大学法人等）

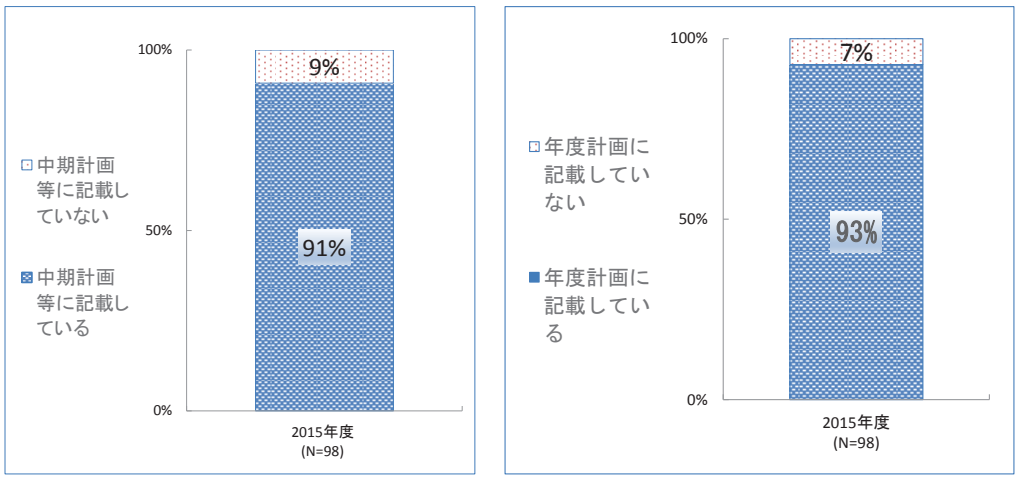


- 独立行政法人98法人のうち、96法人（98%）については中期目標等において記載したが、２法人（２%）については、次期中期目標等の見直し時に記載する予定である。
- 国立大学法人等については、90法人全てが記載した。

（２）独立行政法人の中期計画等及び年度計画における記載状況

独立行政法人の中期計画等及び年度計画における情報セキュリティ対策の記載状況は、以下のとおりである。

図表３　独立行政法人の各計画における記載状況(左：中期計画等、右：年度計画)

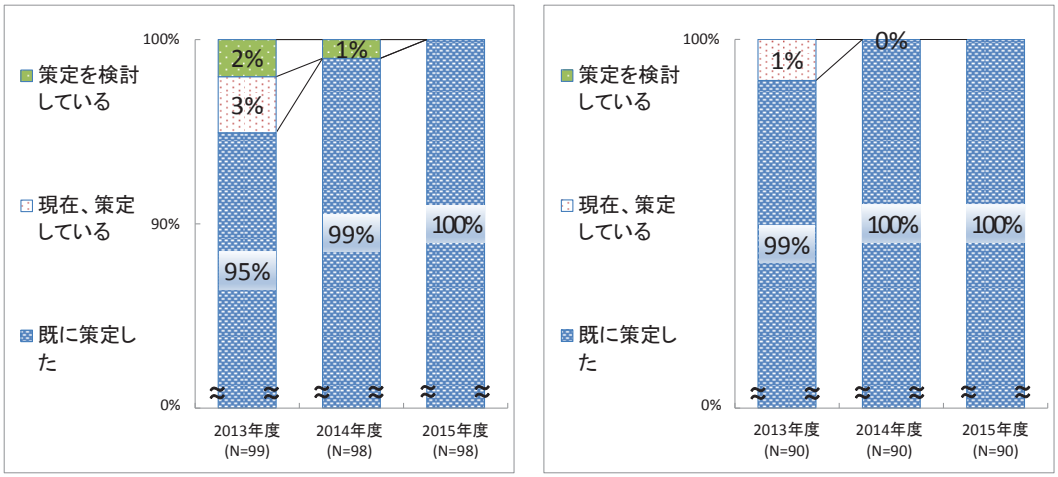


・ 独立行政法人98法人のうち、91法人(93%)は年度計画において情報セキュリティに関する事項が記載されている。

（３）情報セキュリティポリシーの策定状況

独立行政法人等における情報セキュリティポリシー（以下「ポリシー」という。）の策定状況は以下のとおりである。

図表４　ポリシーの策定状況（左：独立行政法人、右：国立大学法人等）

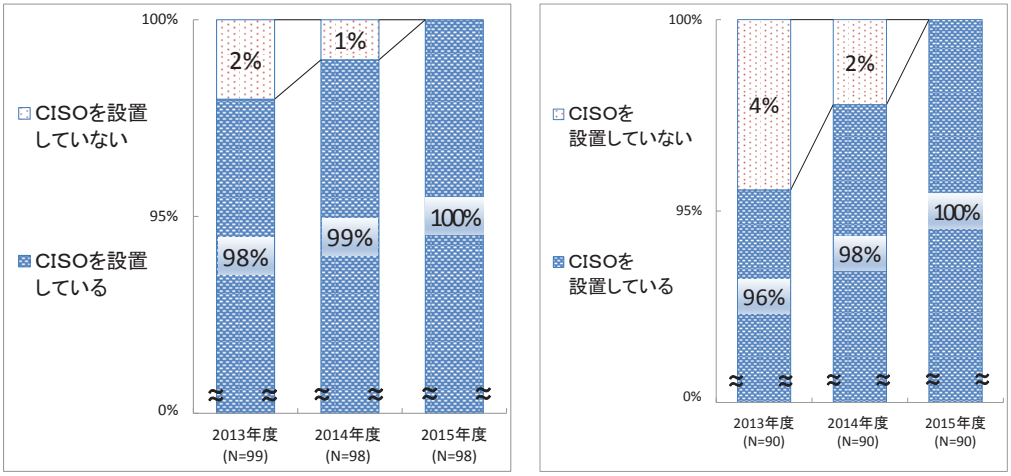


・ 全ての法人がポリシーを策定した。

（４）情報セキュリティ対策の推進体制

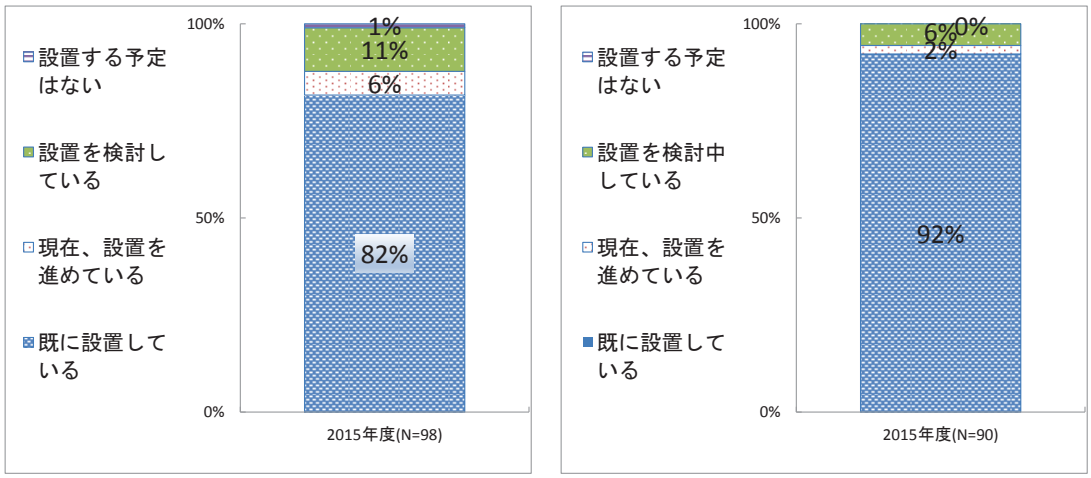
独立行政法人等における最高情報セキュリティ責任者（CISO）や情報セキュリティ委員会の設置状況は以下のとおりである。

図表５　CISOの設置状況（左：独立行政法人、右：国立大学法人等）



・ 全ての法人が最高情報セキュリティ責任者（CISO）を設置した。

図表６　情報セキュリティ委員会の設置状況（左：独立行政法人、右：国立大学法人等）



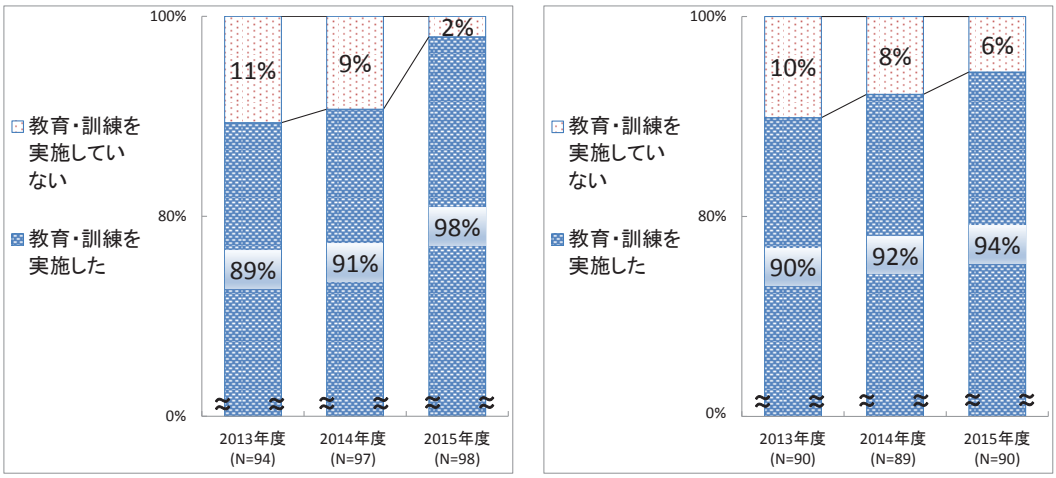
・ 情報セキュリティ委員会を設置済みの法人は、独立行政法人で80法人（82%）、国立大学法人等で83法人（92%）であり、設置を進めている・検討中の法人も独立行政法人で17法人（17%）、国立大学法人等で７法人（８%）である。

・ 設置する予定がない法人は、独立行政法人の１法人のみであり、未設置の理由は「各担当・所属が適切な対応をし、CISOまでの連絡体制が整備済」としている。しかしながら、情報セキュリティ委員会は、CISOまでの連絡をする場ではなく、ポリシーや対策推進計画等を組織横断的に審議する場であり、これらを審議・決定する会議体の設置が望まれる。

（５）ポリシーの運用状況

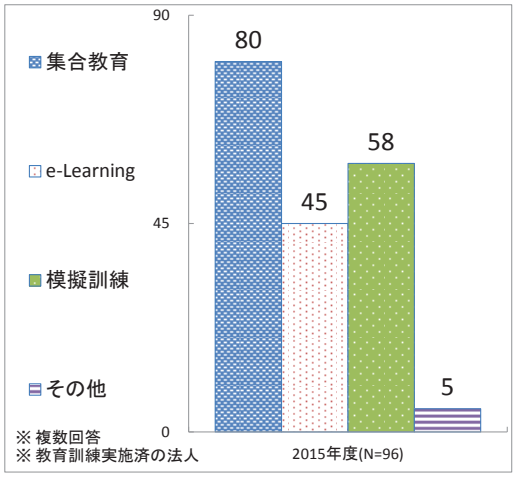
独立行政法人等における教育・訓練の運用状況は以下のとおりである。

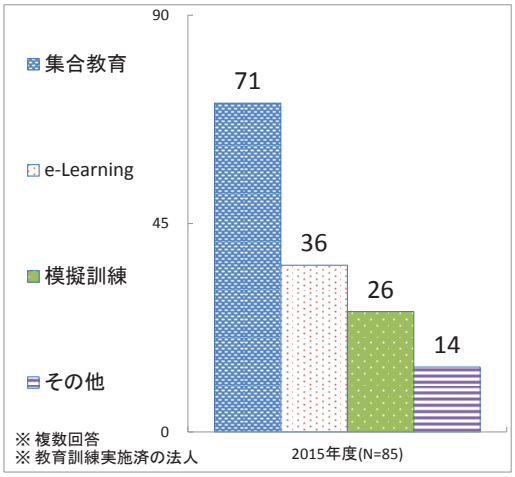
図表７　教育・訓練の実施状況（左：独立行政法人、右：国立大学法人等）



・教育・訓練を実施した独立行政法人は96法人（98%）、国立大学法人等は85法人（94%）であり、いずれも2014年度より増加している。
・未実施の法人については、「教育計画を策定していない」、「規程類の整備中」、「ポリシーに具体的記載がない」等を理由に組織内の教育・訓練を実施していないが、規程や計画がないことが実施しない理由とはならないため、教育の実施は必要である。
・昨今の政府機関に対する標的型攻撃などの脅威が増大している状況を鑑み、独立行政法人等においても、情報セキュリティインシデントを未然に防止するための取組が不可欠である。情報セキュリティ対策に関するルールへの理解を深め、対策を適切に実施するためにも、定期的に教育・訓練を行うことが望まれる。

図表８　教育・訓練の実施方法（左：独立行政法人、右：国立大学法人等）



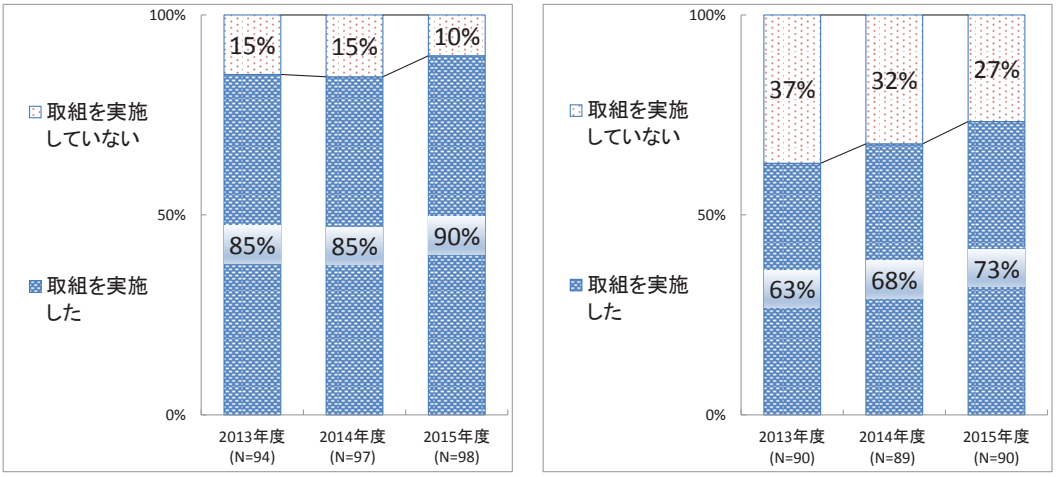


・教育・訓練を実施した法人のうち、集合教育を実施した独立行政法人は2014年度の67法人（76%）から80法人（83%）、国立大学法人等は2014年度の49法人（59%）から71法人（84%）といずれも増加している。
・標的型メール攻撃等の模擬訓練は、独立行政法人では58法人（60%）と過半数が実施している。

（６）ポリシーの遵守状況

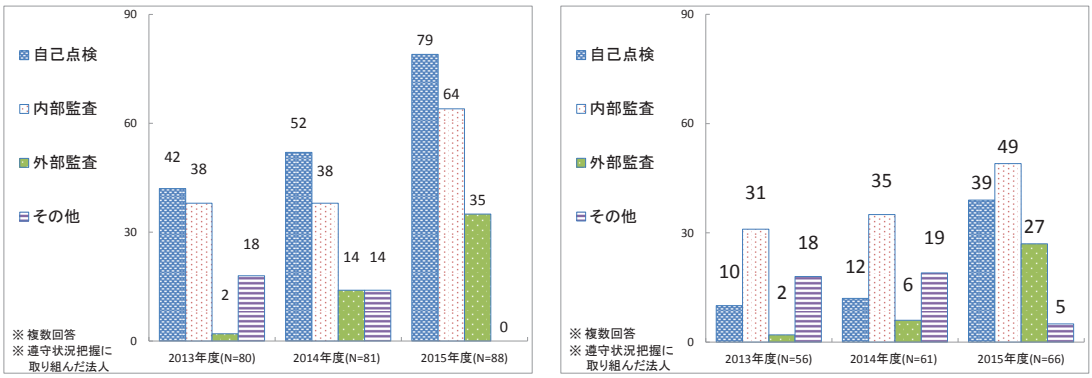
独立行政法人等におけるポリシー遵守状況を把握するための取組の実施状況は以下のとおりである。

図表９　遵守事項把握のための取組の実施状況（左：独立行政法人、右：国立大学法人等）



・遵守状況把握のための取組を行っている独立行政法人は88法人(90%)、国立大学法人等においても66法人(73%)と年々増加している。
・未実施の法人については、「年度後半にポリシー改正したばかり」、「ポリシー・手順の改訂中」、「遵守状況把握のための手順未整備」、「把握のための手順作成中」を理由としている。遵守状況把握はPDCAサイクルを回すためには必要なため、取組の実施が望まれる。

図表10　遵守事項把握のための取組の実施内容（左：独立行政法人、右：国立大学法人等）

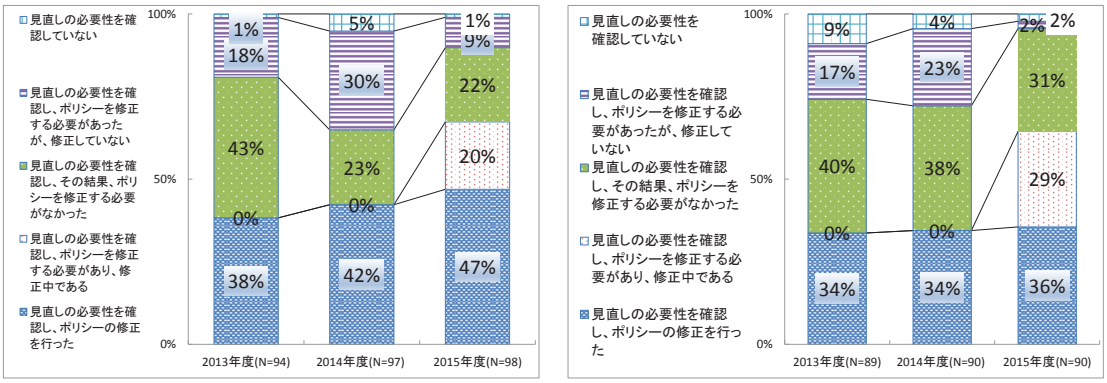


・実施した取組内容は自己点検・内部監査・外部監査のいずれも増加している。特に外部監査を実施している法人が大幅に増加している。

（７）ポリシーの見直し

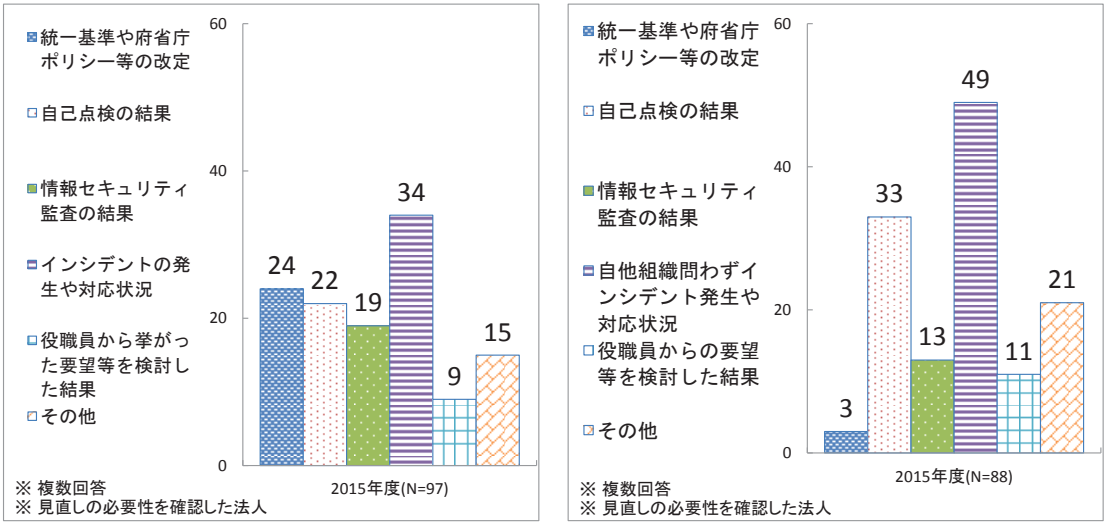
独立行政法人等におけるポリシーの見直し状況は以下のとおりである。

図表11　ポリシーの見直し状況（左：独立行政法人、右：国立大学法人等）



- 2015年度より項目を細分化し、「修正中」の選択肢を追加した結果、ポリシーの見直しを確認し修正を行った・修正中の独立行政法人は68法人（67%）、国立大学法人等は58法人（65%）である。
- ポリシーの見直しの必要性を確認した独立行政法人は97法人(99%)、国立大学法人等は88法人(98%）である。
- 必要性の見直しを確認していない法人は、「リソースが足りなかった」、「インシデントの発生がなかった」などを理由に挙げている。

図表12　ポリシー見直しを確認するに至った契機（左：独立行政法人、右：国立大学法人等）



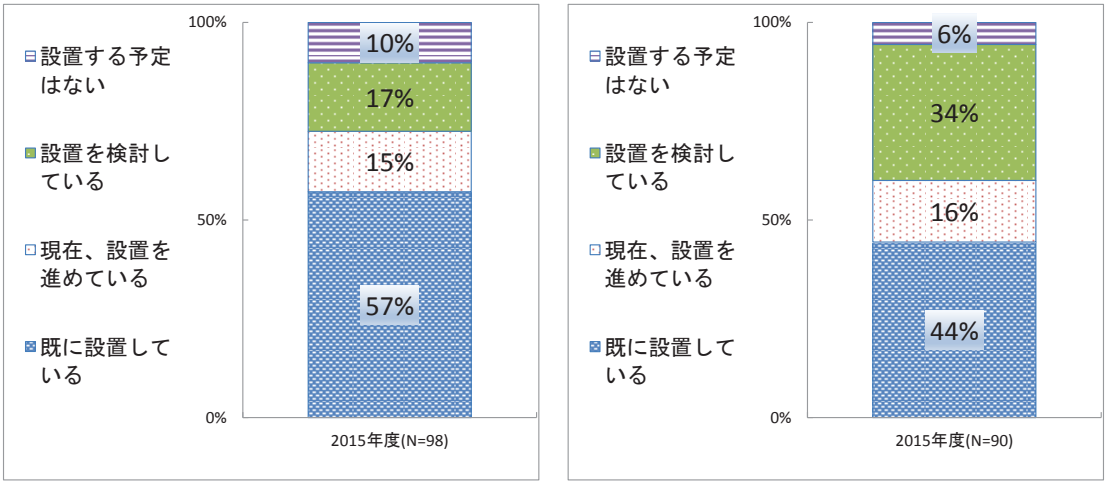
- ポリシーの見直しを確認した法人は、インシデント発生や対応状況を契機として挙げている。
- 次いで契機となっているのは、独立行政法人では統一基準や府省庁ポリシー等の改定、大学法人等では自己点検が挙げられる。

（８）情報セキュリティインシデント対処の体制

独立行政法人等における情報セキュリティインシデント発生時の対処体制については以下のとおりである。

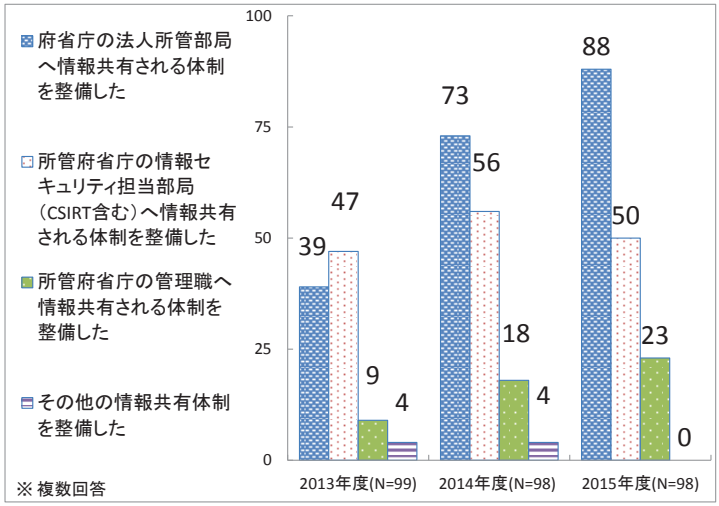
図表12　CSIRT（Computer Security Incident Response Team）の設置状況

（左：独立行政法人、右：国立大学法人等）



- 独立行政法人については56法人（57%）で既に設置済みであり、設置を準備・検討中の法人と合わせると88法人（90%）となる。国立大学法人等においても、設置済みは40法人（44%）だが、設置を準備・検討中の法人と合わせると85法人（94%）となり、インシデント対処体制の整備が進んでいえることが伺える。
- 設置する予定はない法人は、「情報セキュリティ部局等で対応」、「適応人材の不足」等を理由に挙げている。
- インシデント発生時に情報を一元的に管理し、組織的な対応を行うため、早期のCSIRT機能の整備が望まれる。

図表13　独立行政法人における所管府省庁との情報セキュリティインシデント情報の共有体制



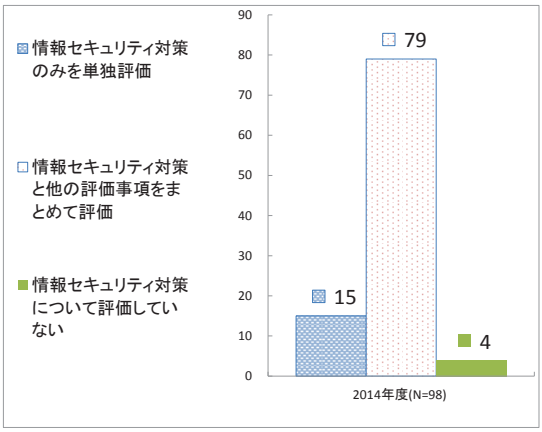
・所管府省庁の法人所管課との連絡体制を整備した法人は増加しているが、所管府省庁の情報セキュリティ担当部局との連絡体制が減少している。法人所管課への連絡体制の徹底が図られたことがうかがえる。

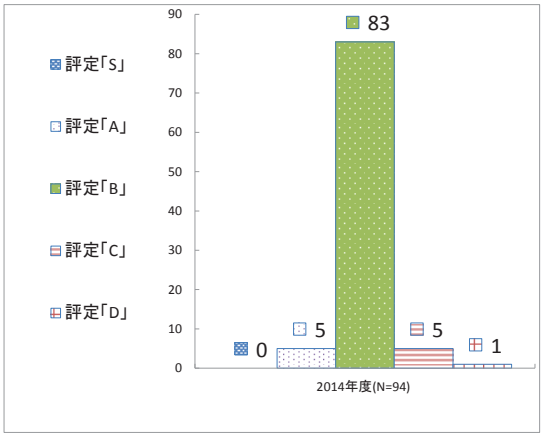
（９）情報セキュリティ対策に係る業務実績の評価書への記載状況

独立行政法人の業務の実績等に関する評価における情報セキュリティ対策の記載状況は以下のとおりである。（注：2015年度の主務大臣による評価は、2014年度における独立行政法人等の取組内容となる。）

図表14　独立行政法人の業務の実績等に関する評価における情報セキュリティ対策の記載状況

（左：年度計画の策定状況、右：年度実績評価での評価状況）





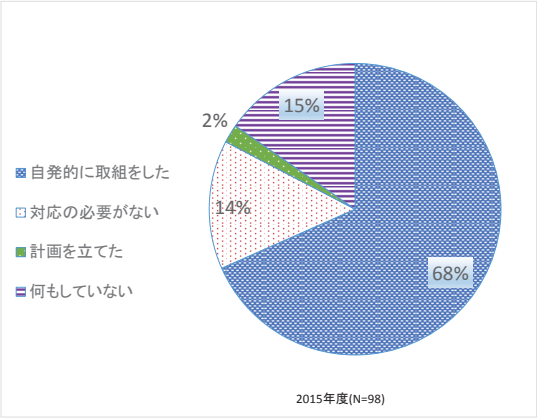
・主務大臣が情報セキュリティ対策に係る業務に関する評価を実施している法人は、94法人（96%）である。
・情報セキュリティ対策を評価した94法人のうち、当該対策のみを評価単位としているのは15法人（16%）のみであり、残り79法人（84%）は他の業務実績とまとめた評価単位で評価を行っている。
・評価単位ごとに付す項目別評定については、標準の「B」が83法人（88%）に及ぶ。なお、評定「A」である５法人ではいずれも情報セキュリティ対策に関する言及はなかった。
・他の業務実績とまとめた評価単位の法人は、情報セキュリティ対策以外の業務実績の影響により、標準未満の評定である「C」や「D」となったと考えられる法人が多く見受けられた。
・独立行政法人の評価に関する指針（平成 26 年９月２日　総務大臣決定）によると、評価単位は、原則、中（長）期目標を定めた項目とすることとされているが、より的確な評価を実施するため、この評価単位をより細分化した単位で項目別評定を行うことは妨げないとされている。従って今後は、情報セキュリティを一つの評価単位とすることにより、情報セキュリティ対策が一層強化されることが望まれる。

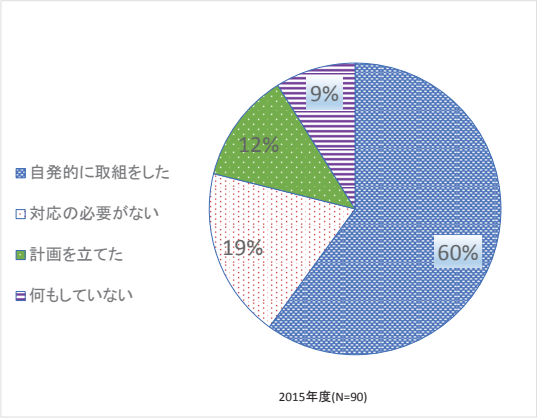
（10）サイバーセキュリティ基本法の施行に伴う対策状況

サイバーセキュリティ基本法の施行に伴い、独立行政法人及び国立大学法人等において、どのような対応を行ったか調査した。

図表15　サイバーセキュリティ基本法の施行に伴う対策状況

（左：独立行政法人、右：国立大学法人）





- 独立行政法人98法人のうち83法人(85%)、国立大学法人等90法人のうち82法人(91%)は、対応必要性を確認し、自組織における対応について検討を行っている。
- 独立行政法人の67法人(68%)は自発的に取組を行っている。そのうち20法人は、CSIRTや連絡体制の整備・確認など、組織の体制にかかわるものであった。
- 国立大学法人等の54法人(60%)は自発的な取組を行っている。そのうち27法人は、標的型攻撃メール訓練や講習会など、法人内の教育や訓練にかかわるものであった。

４　所管府省庁及び独立行政法人等の対応

上記調査結果を踏まえ、所管府省庁においては、情報セキュリティ対策が十分とはいえない独立行政法人等に対し、対策を講じるよう指導等を行うことが望まれる。

また、サイバーセキュリティ基本法の施行に伴い、独立行政法人も統一基準群に従って対策を実施するとともに、監査により取組を改善することが求められるようになるなど、独立行政法人等を取り巻く情報セキュリティ対策に関する情勢に大きな変化があった。これに即応し、多くの法人が何らかの問題意識を持ち、検討・取組を行っている一方で、取組が十分とは言いがたい法人も見受けられる。

所管府省庁は独立行政法人等に対し、情報セキュリティ対策を講ずるよう指導等を行うことはもとより、情報セキュリティ対策の重要性を認識させるなどの意識啓発に取り組むことも重要である。

別添３－10　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　「サービス不能攻撃への対処について（注意喚起）」（2015 年 11 月 25 日発出）

事　務　連　絡
平成27年11月25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）

サービス不能攻撃への対処について（注意喚起）

昨今、公的機関や重要インフラ関係事業者等を標的としたサービス不能攻撃（DoS 攻撃及び DDoS 攻撃）の発生が多数報道されています。

「政府機関の情報セキュリティ対策のための統一基準」6.2.3 においては、システムの可用性を維持するため、「サービス不能攻撃対策」について規定しており、各府省庁におかれましては各種対策を講じていることと思いますが、改めて最近のサービス不能攻撃を想定した対策を検証するとともに、夜間及び休業日での対応を含む対処手順・連絡体制を再確認し、不測の事態に備えるようお願いいたします。

また、攻撃に伴い、ホームページの閲覧障害が発生することが想定されますが、府省庁ホームページは国民に対する情報発信の重要なツールであり、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力回避すべきです。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼしうるような重要情報については、広報担当とも協力の上、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなど、必要な措置について準備するようお願いいたします。

２　「情報セキュリティ問題への対処について（注意喚起）」（2016 年１月７日発出）

事　務　連　絡
平成28年１月７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）

情報セキュリティ問題への対処について（注意再喚起）

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)における標記申し合わせ(別添参照)に基づき、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といった影響範囲の広い問題について取組が進められてきました。他方で今般、同取組に関連し、大学等において複合機で読み取られた内部の情報が、インターネット上で誰でも閲覧できる状態になっていた旨の報道があったところです。

また、平成 24 年８月に、マイクロソフト社から「Internet Explorer のサポートポリシーについて、重要なお知らせ」が発表され、動作するオペレーティングシステムのライフサイクルに準拠していた Internet Explorer（以下、IE）のサポートポリシーが、平成 28 年１月 12 日（米国時間）を過ぎると、各オペレーションシステムの最新版の IE のみがサポート対象となることとなりました。

つきましては、改めて上記申し合わせの注意内容をご確認いただき、①サポート切れソフトウェア（特に IE）の使用回避、及び②複合機等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、所管の法人に対する指導等を再度徹底するとともに、所要の対策を講じられるようお願いいたします。

(参考)
○Internet Explorer のサポートポリシーが変わります(マイクロソフト社)
https://www.microsoft.com/japan/msbc/Express/ie_support/

○ 【注意喚起】Internet Explorer のサポートポリシーが変更、バージョンアップが急務に
(平成 27 年 12 月 15 日　(独)情報処理推進機構)
https://www.ipa.go.jp/security/ciadr/vul/20151215-IEsupport.html

別添

最近の情報セキュリティ問題への対処について

平成２５年１２月１２日
情報セキュリティ対策推進会議申し合わせ

本日の情報セキュリティ対策推進会議において、以下の情報セキュリティ問題について議論し、各府省庁により下記の対応を行っていくことを確認した。

１．ウィンドウズ XP 等のサポート終了問題

平成２６年４月９日をもって、ウィンドウズ XP やオフィス 2003 等のソフトウェアに関して、マイクロソフト社による脆弱性へのサポート対応が終了するため、その後十分な情報セキュリティの確保が困難となる。関係ソフトウェアを新しいものに入れ替えるか、機器ごと更新するか、機器をインターネットに接続しないといった措置を、サポート終了時点までに適切に講ずる。

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

複合機をはじめとして、テレビ会議システムや防犯カメラ等、ネットに接続可能な機器が増えつつあるが、これらについて適切な設定を怠る場合、情報が流出したり、ウィルス感染や攻撃の道具として利用されるなどのセキュリティ上の問題が発生するおそれがある。適切な機器設定を行うなど、外部からの不正なアクセスを遮断する措置を手当てする。

記

上述の問題については、政府機関のみならず、関係公共機関や、広く各界各層に影響しうる問題であることに鑑み、各府省庁は以下の対応を行う。

イ．自府省庁が管理する情報システムに関し、地方支分部局までも含め、必要な情報セキュリティ対策を点検の上、徹底すること。

ロ．各府省庁の所管法人等に対し、必要に応じて政府機関と同様の措置を講じるよう、指導すること。

ハ．各府省庁関係の各界各層に対し、情報セキュリティに関する注意喚起を発し、情報セキュリティ対策の必要性について周知すること。

３　「情報セキュリティ問題への対処について（注意喚起）」（2016 年１月７日発出）

事　務　連　絡
平成 28 年２月２日

各府省庁情報セキュリティ担当課室長 殿

内閣官房 内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）
内閣参事官（情報統括担当）
内閣参事官（事案対処分析担当）

分散型サービス不能攻撃への対処について（注意再喚起）

平成 27 年 11 月 25 日付文書でも注意喚起をしましたが、政府機関や重要インフラ関係事業者(以下「政府機関等」という。)を標的とした分散型サービス不能（ＤＤｏＳ）攻撃とみられる攻撃により、ホームページの閲覧が不能となる事案が多発しています。ＮＩＳＣで把握している限りにおいても、回線容量を超過させる手法や、異常な通信によりサーバの処理容量を超過させる手法など、様々な手法が用いられていることが判明しています。また分散型サービス不能攻撃は昨今では、インターネット上に存在する地下組織が安価に提供しており、大規模な攻撃を試みることがより容易となっている背景事情も影響しているものと考えられます。
各府省庁におかれましては、「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 26 年 5 月 19 日情報セキュリティ政策会議決定）に基づき、分散型を含むサービス不能攻撃への対策を講じていることと存じます。他方で、本年は伊勢志摩サミット及び関連大臣会合の開催を控え、我が国への国際的な関心が高まることから、この種の攻撃がさらに活発化することも予想されます。

こうした最近の分散型サービス不能攻撃を回避する対策は、以下を例とするいくつかの手法が回線事業者やウェブホスティング事業者等により提供されており、比較的短期間で導入が可能とのことです。

・攻撃元となっているＩＰアドレスからの通信を遮断する
・攻撃と判断される異常なパケットの通信を破棄する
・ウェブサーバを仮想的に多数配置し、攻撃による大量の通信を分散させて処理する

各府省庁におかれましては、以上の状況も踏まえつつ、引き続き攻撃動向に注意するとともに、開設しているウェブサイトの重要度等にも鑑み、分散型サービス不能攻撃対策の強化について速やかに御検討をお願いします。

また、攻撃を受けた府省庁にあっては、『我が国におけるサイバー攻撃に係る情報収集・集約体制等の整備について』（平成 22 年 12 月 27 日情報セキュリティ対策推進会議申合せ）３（１）に基づき、関係機器のログ等の情報をＮＩＳＣに提供いただきますようお願いします。具体的には、攻撃と思われる通信を認知した際は、初動にて実施した対策等を記入し、インシデント連絡様式を初報として速やかにご提出ください。加えて、府省庁にて把握されているログ情報、フロー情報、トラフィック情報等についても併せてご提出をお願いします。

４　「政府機関におけるセキュリティ・IT 人材育成総合強化方針」（2016 年３月 29 日 CISO 等連絡会議・CIO 連絡会議合同会議）

政府機関におけるセキュリティ・ＩＴ人材の育成

政府機関においても、近年のサイバーセキュリティ事案の増加等に鑑み、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等に取り組み、セキュリティを確保しつつ効率的な行政運営の実現を図ることが必要である。

一方、政府機関における課題として、セキュリティに係る人材が圧倒的に不足しているとともに、システム管理や業務改革に関する知識・経験を有する人材も不足していること、加えて、一般職員の情報リテラシーも不十分であること、また、自組織におけるセキュリティ対策等の司令塔機能も弱体であること等が挙げられる。このため、これらの課題解決に向け、①司令塔機能の抜本的強化、②高度専門人材と一般行政部門との橋渡しとなるセキュリティ・ＩＴ人材（橋渡し人材）の確保・育成、③即戦力人材としての民間の高度専門人材の確保、④一般職員の情報リテラシー向上の実現を図ることが必要である。

各府省庁におけるセキュリティ・ＩＴに係る体制・人材に関しては、近年急速な進展が見られ、かつ、今後も目まぐるしく変化が生ずることが想定される分野であるため、各府省庁の所管業務ではあるものの、こうした進展や変化に応じた適切な対応が困難な面があること、また、インシデント対応、システム管理など、業務としての共通点が認められることに加え、育成すべき人材なども共通している面が大きいため、各府省庁それぞれで対応するのではなく、政府全体で目指すべき方向性を共有し、横断的な連携を図りながら、方策を進めていくことが効果的であると考えられることから、政府機関において取り組むべき方針として以下を示す。なお、方針に基づく取組は適宜見直していくものとする。

１．各府省庁における司令塔機能の抜本的強化

各府省庁においては、平成 28 年度から、サイバーセキュリティ・情報化審議官の新設等により、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等について、最高情報セキュリティ責任者（ＣＩＳＯ）と情報化統括責任者（ＣＩＯ）を補佐し、府省庁内を指揮監督できる強力な体制を構築する。

また、サイバーセキュリティ・情報化審議官等の主導の下、組織規模や所管するシステム等の実情を踏まえつつ、人材の着実な確保・育成を図るため、速やかに、採用、人材育成、将来像等にわたる具体的な取組方策を定めた「セキュリティ・ＩＴ人材確保・育成計画（仮称）」を作成し、各府省庁のサイバーセキュリティ・情報化審議官等で構成する会議において共有の上、フォローアップを実施する。当該計画の下で、有為な人材を確保するとともに、「セキュリティ・ＩＴ人材育成支援プログラム（仮称）」を設け、当該プログラムを通じ、セキュリティ・ＩＴに係る業務に充てるべき人材を育成する。内閣官房等においては、当該計画及びプログラムの作成、当該人材の確保・育成を支援する。

各府省庁の取組状況については、サイバーセキュリティ対策推進会議（ＣＩＳＯ等連絡会議）、各府省情報化統括責任者（ＣＩＯ）連絡会議や次官連絡会議においても共有を図る。

２．橋渡し人材（部内育成の専門人材）の確保・育成

セキュリティに関して対応が求められる事案の急増、システムによる更なる業務効率化の推進など、セキュリティ・ＩＴに係る業務の増加、複雑困難化がみられる中で、各府省庁に

おける現在のセキュリティ・ＩＴに係る体制は脆弱であり、各府省庁を中心に橋渡し人材を確保・育成することが喫緊の課題であることから、体制や人材に係る実態を把握した上で、「セキュリティ・ＩＴ人材（橋渡し人材)」として、「セキュリティ・ＩＴに関する一定の専門性と、所管行政に関する十分な知識・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」を相当数確保・育成する必要がある。ついては、以下のとおり、(1)体制の整備・人材の拡充、(2)有為な人材の確保、(3)一定の専門性を有する人材の育成、(4)研修体系の抜本的整理、(5)適切な処遇の確保に係る取組を実施することとする。

（１）　体制の整備・人材の拡充

・各府省庁の統括部局の体制の整備及び人材の拡充を行う
・併せて、各府省庁の一定のシステム所管部局の体制の整備及び人材の拡充を行う。（統括部局の体制整備等も踏まえつつ段階的に実施）

各府省庁のセキュリティ・ＩＴに係る統括部局の体制の整備及び人材の拡充を実施する。また、当該整備及び拡充と併せて、各府省庁の社会的な影響の大きいシステムを所管する部局についても体制の整備及び人材の拡充を実施する。

（２）　有為な人材の確保

・政府一体となって、各府省庁参加の合同説明会、内閣人事局による各種広報等における積極的な広報を実施する。
・将来的に、大学等での「出張講義」、職場での業務体験イベントやインターンシップの実施などを検討する。（可能なものは平成 29 年度から実施）
・各府省庁において有為な人材を確保する。（平成 29 年度から順次実施）

政府機関におけるセキュリティ・ＩＴ人材の確保・育成に向けた取組に対する学生等の関心を高めることで、当該人材の志望者の拡大を図るため、府省庁横断的な人材のニーズを踏まえ、政府一体となって、各府省庁参加の合同説明会、内閣人事局による各種広報等の中央の採用活動における積極的な広報を実施する。

将来的に、産学官が連携した教育の充実に併せて、情報系の大学・学部等を対象にした「出張講義」の実施、学生等を対象とした職場での業務体験イベント（事案対応シミュレーション等）やインターンシップの実施などのほか、有為な人材の確保に向けた更なる方策を検討する。

各府省庁において、セキュリティ・ＩＴに係る素養の把握に努め、セキュリティ・ＩＴ人材に求められる資質を十分に考慮し、適性が認められる者を採用（新卒採用のほか、実務経験者の選考による中途採用も可能）するなどにより、有為な人材を確保する。

（３）一定の専門性を有する人材の育成

・各府省庁において、「セキュリティ・IT 人材育成支援プログラム(仮称)」を設け、一定の専門性を有する人材を育成する。（平成 29 年度から順次実施）
・将来的に、一部の人材を総務省行政管理極東で採用・一括管理し、各府省庁等に派遣する枠組みを検討する。（各府省庁の人材育成に目途が立った段階での実施に向け検討）

各府省庁において、適切な人材育成を図るための「セキュリティ・ＩＴ人材育成支援プログラム（仮称)」を設け、橋渡し人材にとっても魅力あるものとなるよう、当該プログラムの中で、各府省庁における一般行政事務従事等により、所掌事務に関する十分な知

識・経験を習得させつつ、セキュリティ・ＩＴに係るスキルレベルの確保や能力向上を図るため、各府省庁のシステムのライフサイクル経験とともに、セキュリティについては、事案対処、保安、事故対応、危機管理、安全保障等の業務に従事させるほか、橋渡し人材に共通した取組として、役職段階ごとの研修受講（原則必須化）、内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）・内閣官房情報通信技術（ＩＴ）総合戦略室（ＩＴ室）・総務省行政管理局・個人情報保護委員会への出向（原則必須化）、国内外の大学院・民間企業への派遣、ＮＩＣＴが整備する人材育成施設の活用などを通じ、一定の専門性を有する人材を育成する。

また、将来的に、一部の人材を総務省行政管理局等で採用して一括で管理し、各府省庁等への派遣を可能とする枠組みについても検討を行う

（４）研修体系の抜本的整理

・現行の研修体系の抜本的整理、研修修了者にスキル認定を行う枠組みの構築等を行う。（可能なものは平成 28 年度から実施）
・管理職に実践的な演習等に係る研修を実施する。（可能なものは平成 28 年度から実施）
・CSIRT 要員への研修・訓練を活用する（平成 28 年度から実施）

ＮＩＳＣ及び総務省行政管理局等において、橋渡し人材のセキュリティ・ＩＴに係る能力の向上を図るため、橋渡し人材としての研修受講者数を今後 4 年間で 1000 人を超える規模とすることを目指して、役職段階別（係員、係長など）のスキルレベルのモデルを設定し、これに応じた現行の研修体系の抜本的整理を行うとともに、研修修了者にスキル認定を行う枠組みを構築するほか、研修の受講履歴を体系的に整理して各府省庁の人事担当者と情報共有を行う枠組みを検討する。

また、管理職向けに、ＮＩＳＣ及び総務省行政管理局等において、基本的なセキュリティ・ＩＴについての素養を身につけるための研修、業務・システム改革やサイバーセキュリティのケーススタディなどの実践的な演習等に係る研修を実施する。

また、ＣＳＩＲＴ要員への研修や訓練についても活用していく。

（５）適切な処遇の確保

・業務の専門性・特殊性を踏まえ、手当等を新たに支給することによる一定の給与上の評価を行う（平成 29 年度から順次実施）
・「セキュリティ・ＩＴ人材確保・育成計画（仮称）」の中で、出向等の機会を捉えた昇任等も含め、高位のポストまでを見据えた人事ルート例（イメージ）を設定する。（平成 28 年度に速やかに実施）

セキュリティ・ＩＴに係る業務の専門性・特殊性等とともに、適切な育成がなされた人材が充てられることを踏まえ、手当等を新たに支給することによる一定の給与上の評価を行う。

各府省庁のセキュリティ・ＩＴ人材は、「セキュリティ・ＩＴ人材育成支援プログラム（仮称）」を通じて、所掌事務に関する十分な知識・経験を得つつ、セキュリティ・ＩＴに係る能力も向上させることにより、的確な育成が図られる人材であることから、有為な人材には、適切な時期にセキュリティ・ＩＴに係る枢要なポストへ昇任させるなど、これに相応しい処遇が確保されることが必要である。そのため、各府省庁において、「セキュリティ・

ＩＴ人材確保・育成計画（仮称）」の中で、出向等の機会を捉えた昇任等も含め、高位のポストまでを見据えた人事ルート例（イメージ）を設定する。

３．外部人材（即戦力の高度専門人材）の確保

セキュリティ人材については、ＮＩＳＣ等において、平成 28 年度から民間の特に高度なセキュリティ人材を特定任期付職員等の制度を活用して採用し、必要に応じて監査等を通じ各府省庁に派遣する。

ＩＴ人材については、ＩＴ室において、一元的に採用・管理（プール制）している政府ＣＩＯ補佐官を積極的に活用し、引き続き必要な人材を各府省庁に派遣する。

また、政府において必要な即戦力となる外部人材を確保していくため、我が国に実践的な能力を有するセキュリティ人材の層の充実を積極的に図るための施策を推進する。具体的には、enPiT の枠組みを活用した産学のネットワークの構築、産学官が連携した教育の充実、ＮＩＣＴ等の演習基盤を活用した実践的演習の強化、「情報処理安全確保支援士」等サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる資格制度等の整備等を推進する。

４．一般職員の情報リテラシー向上

各府省庁の新人研修等において、セキュリティ・ＩＴに関する各種研修を実施する。なお、当該研修に利用可能な研修教材として、ＮＩＳＣや総務省行政管理局から各府省庁にコンテンツを提供する。その際、e-learning 等による実施や、そのためのセキュリティ・ＩＴ教材の共通化なども併せて検討する。さらに、採用予定者に対して研修教材を提供することについても併せて検討する。これらについて、可能なものは平成 29 年度から実施していく。

内閣人事局が行う新任の管理職を対象とした研修において、管理職に必要な基礎的能力の向上の一環として、セキュリティ・ＩＴに関する基礎的知識を得る機会を引き続き提供する。

内閣人事局が作成する「人事評価マニュアル」を改訂し、セキュリティ、危機管理、ＩＴ利活用等について取られた行動に関する評価の着眼点を明示する。また、内閣人事局が実施する評価者訓練においても周知する。これらについて、可能なものは平成 28 年度から実施していく。

〔参考資料省略〕

５　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 2 回	5 月 21 日	・サイバーセキュリティ戦略(案)について ・サイバーセキュリティ対策を強化するための監査に係る基本方針(案)について
第 3 回	6 月 1 日	・日本年金機構からの情報流出事案について
第 4 回	7 月 22 日	・2014 年度の政府機関における情報セキュリティ対策に関する取組と評価等について ・議長指示事項の対応状況について
第 5 回	8 月 19 日	・サイバーセキュリティ戦略(案)について ・サイバーセキュリティ 2015(案)について ・日本年金機構事案を踏まえた議長指示について ・情報セキュリティ緊急支援チーム(CYMAT)への参加について
第 6 回	9 月 24 日	・サイバーセキュリティ 2015(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(案)について ・標的型攻撃の脅威について(実演)
第 7 回※	10 月 30 日	・政府情報セキュリティ・IT 人材対策について
第 8 回	1 月 22 日	・我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針(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見直しについて ・2016 年サイバーセキュリティ月間について ・「NATIONAL318(CYBER)EKIDEN2016」の開催について ・インターネットに接続されている機器のセキュリティについて
第 9 回※	3 月 29 日	・政府情報セキュリティ・IT 人材対策について ・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実施要領について ・2016 年サイバーセキュリティ月間について ・政府関係機関を取り巻く最近の話題

※各府省情報化統括責任者(CIO)連絡会議との合同開催

別添３－11　政府機関等に係る 2015 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
2015年	4月	【概要】宮崎労働局は 24 日、都城公共職業安定所において職員及び非常勤職員の勤務状況報告書を宮崎労働局にメールで報告した際、誤って法人等を送信先に入れ送信したため、報告書内の個人情報及び誤って送信先に含めた法人等のメールアドレスが漏えいしたと発表。 【対応等】誤送信した関係者等に対し、経過説明、謝罪をし、各々了承を得た。また、メール誤送信を防止するための研修を実施し、個人情報の適切な取扱いについて徹底を図るよう指示した。	意図せぬ情報流出
	5月	【概要】長崎労働局は 18 日、職員 A がメール署名欄を職員 B の署名欄を転用かつ修正して使用していたが、その際、署名欄のメールアドレスの修正を行わず、職員 B のアドレスが記載されたまま事業団体にメールを送信したため、無関係である職員 B のメールアドレスが事業団に漏洩したと発表。 【対応等】関係者にメールの削除を依頼し、事実経過と謝罪を行い了承を得た。また、全職員に対してメールアドレスに関する注意喚起を行うとともに、各自で作成しているメール署名欄の再確認等を指示した。	意図せぬ情報流出
		【概要】文部科学省は、平成 27 年２月、行政文書開示請求に応じて、個人情報を不開示とした上で文書を開示したが、不開示とした個人情報の一部 111 人分が電子的操作により読み取れることが判明したと発表。 【対応等】行政文書開示請求者に対し、電子データの返還並びに消去及び廃棄を依頼し、個人情報の漏えいが確認された方に謝罪した。以後、不開示処理をした電子データを紙に出力し、スキャナーで再度電子化する等確実な不開示処理を徹底するとともに、不開示処理方法を定めたマニュアル及びチェックリストを整備する等の再発防止策を講じた。	意図せぬ情報流出
		【概要】東京国税局は 27 日、強制調査先から押収した USB メモリなどが所在不明になっていることを明らかにした。紛失したのは調査先のデータなどが入った USB メモリ 10 本とブルーレイディスク１枚。 【対応等】所在不明が判明した後、調査先に謝罪した。 また、調査先から押収した物品の収納庫への入退室確認及び収納箱の持出し確認について、複数名で実施するなどの再発防止策を講じた。	その他
	6月	【概要】日本年金機構は１日、職員のパソコンにウイルスメールによる不正アクセスがあり、年金加入者と受給者の個人情報、約 125 万件が外部に流出したと発表。	外部からの攻撃
		【概要】富山大学で２月、工学部のサーバが海外からの攻撃で乗っ取られ、中国・米国への新たな攻撃に利用されていたことがわかった。サーバの管理パスワードが簡易なものであったことが原因としている。	外部からの攻撃
		【概要】北海道労働局は９日、担当職員が厚生労働省担当者へ重大災害報告書をメール送信するため、宛先を設定する際、１名の厚生労働省担当者について、誤って同姓同名の別人(民間会社)のアドレスを設定して送信したため、重大災害報告書に記載された個人情報等が漏洩したと発表。 【対応等】関係者にメールの削除を依頼し、事実経過と謝罪を行い了承を得た。また、メールの誤送信を防止するための研修を実施し、個人情報の適切な取り扱いについて改めて基本的な作業手順の徹底を図るよう指示した。	意図せぬ情報流出
		【概要】国立医薬品食品衛生研究所は 13 日、職員のパソコン１台がマルウェア感染したと発表。 【対応等】感染が疑われた時点で速やかに外部とのネットワークを遮断した。なお、調査の結果、外部との不審な通信や情報漏洩は確認されなかった。	その他
		【概要】国際協力機構において、情報システムの点検を実施したところ、１台の PC において標的型攻撃メールの添付ファイルを開封したことによるウイルス感染が確認され、さらに PC 及びサーバへの感染が確認され、外部の不審なサイトとの通信を行っていたことが判明したと発表。情報流出は確認されていない。	外部からの攻撃
		【概要】香川大学は 18 日、医学部附属病院の PC が、外部から送られたメールによってコンピュータウイルスに感染したと発表。 同パソコンからの不審な通信があったが、情報流出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
		【概要】福島労働局は 23 日、厚生労働省の担当官に放射線作業届の定期報告をメールで送信するに当たり、送信先アドレスの設定を誤り、民間の放射線管理担当者宛てに誤送信した。なお、メールに添付されていた報告には放射線作業に係る事業場担当者の個人名等が記載されていたと発表。 【対応等】関係者に対し、メールの削除を依頼するとともに、経過説明と謝罪を行い了承を得た。また、全職員に対してメール送信時の情報漏えい防止対策の確実な実施の徹底を指示した。	意図せぬ情報流出
		【概要】法務省は 25 日、本省内でファイル共有やメールなどの一般事務を処理するためのネットワークシステムに接続された端末が、不正プログラムに感染した疑いがあると発表。 【対応等】不審な通信が確認された後、ネットワークを遮断した。調査の結果、不正プログラムに感染したことが判明した。情報流出やシステムへの影響は確認されていない。	外部からの攻撃
	7 月	【概要】環境省は 10 日、省内のネットワークにつながれた PC が、サイバー攻撃を受けてウイルスに感染した疑いがあるとして、ネットワークから遮断したと発表。外部への情報流出は確認されていない。 【対応等】外部からの指摘を受け調査を行ったところ、不正通信の痕跡を確認したため、ネットワークから遮断を行った。	外部からの攻撃
		【概要】愛媛大や福岡大など国私立 5 大学のウェブサイトがサイバー攻撃を受け，メールアドレスやコンテンツを管理するための ID，パスワードが流出する被害が発生したことがわかった。	外部からの攻撃
		【概要】東京大学は 16 日、メールを管理する PC が不正なプログラムに感染し、学生の氏名や学生証番号等約３万 6300 件がサーバから流出した可能性があると発表。	外部からの攻撃
		【概要】厚生労働省は 17 日、ハローワーク職員の PC１台がウイルスに感染したことを発表。 【対応等】不審な通信が確認された日のうちに、感染した PC が置かれていたハローワーク内の全端末をネットワークから抜線し、調査を行った結果、ウイルス感染が判明した。なお、情報流出は確認されていない。	外部からの攻撃
	８月	【概要】内閣府は７月 31 日、NPO 法人に関する情報を提供する「内閣府 NPO ホームページ」で、NPO 法人等からの問い合わせを受け付けるメールのアカウントが乗っ取られたと発表。このアカウントを使用し、メール約２万件が送信された。メールアカウントのパスワードが短く推測されやすいものだったという。 【対応等】乗っ取られたメールアカウントに問い合わせをした 63 の個人や法人に、問い合わせ内容が流出したおそれがあるとして、謝罪をした。 その後の調査にて個人情報の流出はないことが判明した。 また契約相手先名にて警察に被害について届け出た。 内閣府は契約相手先に対し、「内閣府本府における物品等の契約に係る指名停止等措置要領」（内閣府大臣官房会計課長決定）第６に基づき文書にて警告するとともに、再発防止策として運用方法の見直しを行い、メールを使用しないでサポートデスクを運用する方式に契約を変更した。	外部からの攻撃
		【概要】富山大学は５日、担当教員の PC１台がウイルスに感染していることが確認され、そのパソコンには環境省が実施している「子どもの健康と環境に関する全国調査」に関する個人情報が、調査の実施手順に反したかたちで保管されていたと発表。当該個人情報の外部への流出は確認されていない。	その他
		【概要】科学技術振興機構は７月 15 日から 17 日までの間、業務用 PC 数台がウイルスに感染し、最大 215 人分の事業関係者の名前や住所、電話番号などが流出した可能性があると発表。職員が改ざんされたウェブサイトを業務で閲覧したことで、ウイルスに感染したという。	外部からの攻撃
		【概要】大阪労働局は 10 日、国家公務員一般職試験の受験生に対し、ハローワーク見学の実施勧奨に係るメールを送信した際、「BCC」に宛先を入力の上、送信すべきところを「宛先」に入力して送信したため、宛先となったメールアドレスが受信者全員に表示されたと発表。 【対応等】受験生に対して、謝罪と当該メールの削除依頼をメール送信するとともに、電話による再度の謝罪及び削除依頼を行い、了承を得た。また、複数の宛先にメール送信する際に、複数人での確認を徹底するよう指示するとともに、個人情報の取り扱いに関する研修を行い、個人情報の適切な管理・取り扱いについて徹底を図った。	意図せぬ情報流出

年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
	9 月	【概要】厚生労働省は 1 日、他省庁作成の注意喚起文書を、事業主団体にメールで送信した際に、個人メールアドレスを「BCC」に設定して送信すべきところを誤って、「TO」で一斉送信したため、全員のメールアドレスが表示されるという個人情報漏えい事案が発生したと発表。 【対応等】電子メールを複数の個人メールアドレスあてに送信する場合には、BCC で送信することを再度周知・徹底のうえ、複数の職員によるダブルチェックを徹底することにより、個人情報漏洩防止の徹底を図るよう指示。	意図せぬ情報流出
		【概要】関東信越厚生局は 21 日、職員が帰宅途中の電車内で、麻薬取締部が保有する PC、情報を記録した USB メモリ（個人情報を記録）及び会議資料等の入った鞄を網棚に置き忘れたと発表。 【対応等】関東信越厚生局は 24 日、紛失した PC 等が発見され、情報流出は認められなかった。	意図せぬ情報流出
	10 月	【概要】国立ハンセン病療養所は 7 日、職員が個人情報の入った USB メモリを紛失したと発表。 【対応等】個人所有の USB メモリの使用を一切禁止するとともに、パスワードをかけることを徹底するなど管理体制の整備に努めた。	意図せぬ情報流出
		【概要】日本政府観光局のホームページが 10 日から 11 日にかけて約 5 時間、ホームページの閲覧がしづらい状態となった。	ホームページの閲覧障害
		【概要】京都労働局は 16 日、A事業場に係る電子申請の電子公文書が誤ってB事業場を担当する別の社会保険労務士に送信されたと発表。 【対応等】関係者に対し、事情を説明し謝罪し、了解を得た。また、各所属長から全職員に対し、注意喚起文書を手交することを指示した。	意図せぬ情報流出
	11 月	【概要】厚生労働省は 11 日、再生医療等安全性確保法に関する各種申請書作成支援サイトのホームページに、プログラム上の不具合が確認され、サイト URL に特定の数字を入力することにより、他の申請者の作成情報が閲覧可能な状態であったと発表。 【対応等】改ざんや情報漏えいの有無を確認し、原因を調査し、プログラムを修正する等により復旧に努めた。なお、今回の事案で情報の漏えい、改ざん等の被害は確認されなかった。	その他
		【概要】厚生労働省は 23 日、ホームページに外部からの大量通信が発生したため、21 日未明から 23 日午後まで、ホームページの閲覧を停止したと発表。 【対応等】ホームページに外部からの大量通信が発生したため、原因調査を行いホームページ閲覧の提供を攻撃が止むまで停止し、復旧に努めた。 併せて、改ざんや情報流出の有無を確認した。なお、今回の事案で改ざんや情報流出は確認されなかった。	ホームページの閲覧障害
	12 月	【概要】日本スポーツ振興センター（JSC）は 16 日、14 日にホームページ上に公開した新国立競技場整備事業技術提案書の公表方法に不備があり、一定の特殊操作を行えば不開示とした情報が判読可能となること、また、当該不具合については、公表ファイルを差し替え、解消したことを明らかにした。	意図せぬ情報流出
		【概要】国立病院機構岩国医療センターのホームページが、23 日に不正アクセスを受け、改ざんされていることが判明した。ホームページの閲覧を停止し、情報流出の有無を確認し、原因を調査し、復旧に努めた。情報流出やウイルス感染などの被害はない。	ホームページの閲覧障害
2016 年	1 月	【概要】インターネットとつながる複合機やプリンタのセキュリティ対策がとられず、内部データが外部から見えていた大学などが多数あることがわかった。大学等 26 校の計 140 台に蓄積された文書や画像が外部から見えている状態にあったという。	意図せぬ情報流出
		【概要】厚生労働省は 6 日、業関係団体に送付した文書に個人情報が含まれていたと発表。 【対応等】メール送信先へ、外部送信しないよう伝達するとともに、送付先に伺いメールの削除を確認、個人情報漏えいの当事者に説明及び謝罪した。	その他
		【概要】北海道大学は、13 日、学内のサーバが不正アクセスの被害に遭い、約 11 万人分の個人情報が流出した疑いがあると発表した。 その後、２月 18 日、個人情報等の流出は確認されなかったとする調査結果を発表した。	外部からの攻撃

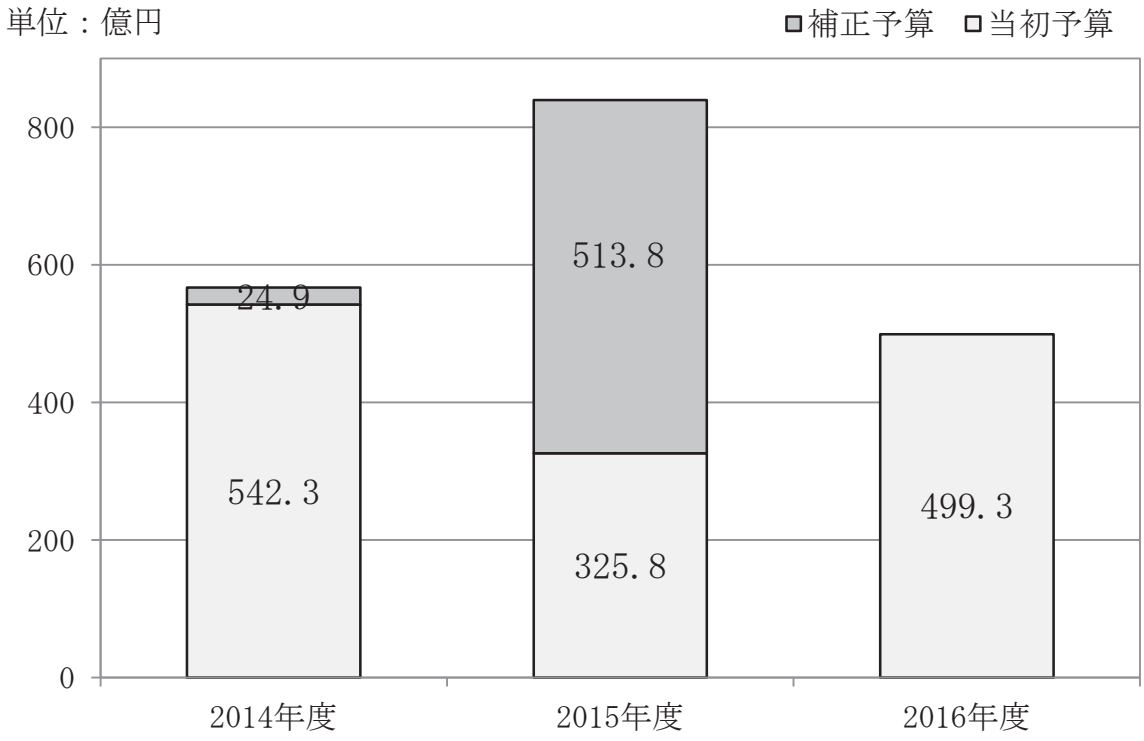
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】金融庁は、ホームページに外部から大量通信が発生したため、18 日早朝からホームページの閲覧がしづらい状態となったと発表。 【対応等】改ざんや情報流出の有無を確認し、原因を調査し、復旧に努めた。	ホームページの閲覧障害
		【概要】関東信越厚生局は 22 日、ホームページに掲載した関東信越年金記録訂正審議会の答申書（東京部会審議に係る平成２７年１２月分）について、本来、匿名化して掲載すべき個人情報等を誤ってそのまま掲載したと発表。 【対応等】誤掲載されたファイルを削除し、誤って個人情報等を掲載した 55 人及び関連事業所に対し、事態を説明し、謝罪を行った。 また、地方厚生局を含む本省全部局及び関係団体に今回の事案を周知するとともに、個人情報の匿名化等の内容の確認を確実に行うよう改めて徹底することとした。	意図せぬ情報流出
		【概要】厚生労働省は、ホームページが 25 日夜から閲覧がしづらい状態となったと発表。25 日夜から 15 時間にわたり閲覧がしづらい状態となり、26 日昼にいったん復旧したが、その夜に再び閲覧がしづらい状態となった。 【対応等】ホームページに外部からの大量通信が発生したため、原因調査を行いホームページ閲覧の提供を攻撃が止むまで停止し、復旧に努めた。なお、今回の事案で改ざんや情報流出は確認されなかった。	ホームページの閲覧障害
		【概要】警察庁は 27 日、ホームページが同日夜に一時的に閲覧がしづらい状態となったと発表。 【対応等】改ざんや情報流出の有無を確認し、原因を調査し、復旧に努め、再発防止対策を講じた。	ホームページの閲覧障害
	２月	【概要】財務省は１日、ホームページが１月 31 日深夜から閲覧がしづらい状態となったと発表。 【対応等】改ざんや情報流出の有無を確認し、原因を調査し、復旧に努めた。	ホームページの閲覧障害
		【概要】金融庁は２日、ホームページが１月 31 日深夜から閲覧がしづらい状態となったと発表。 【対応等】改ざんや情報流出の有無を確認し、原因を調査し、復旧に努めた。	ホームページの閲覧障害
		【概要】厚生労働省は２日、ホームページが１月 31 日深夜から閲覧がしづらい状態となったと発表。１時間半ほどで復旧した。 【対応等】ホームページに外部からの大量通信が発生したため、原因調査を行いホームページ閲覧の提供を攻撃が止むまで停止し、復旧に努めた。なお、今回の事案で改ざんや情報流出は確認されなかった。	ホームページの閲覧障害
		【概要】国税庁は 10 日、ホームページが閲覧ができない状態となり、その後も断続的に閲覧がしづらい状況が続いていると発表。 【対応等】改ざんや情報流出の有無を確認し、原因を調査し、復旧に努めた。	ホームページの閲覧障害
		【概要】公正取引委員会は 18 日に，同委員会のメールアドレスを不正に利用した「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，同委員会のメールアドレスを不正に利用した「なりすましメール」が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，受信者に対し「なりすましメール」であることを連絡した。	その他
		【概要】国際協力機構は 19 日，一時的にホームページが閲覧ができない状態であったと発表。	ホームページの閲覧障害

※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３－12　政府のサイバーセキュリティ関係予算額の推移

	2014 年度	2015 年度	2016 年度
当初予算額	542.3 億円	325.8 億円	499.3 億円
補正予算額	24.9 億円	513.8 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。



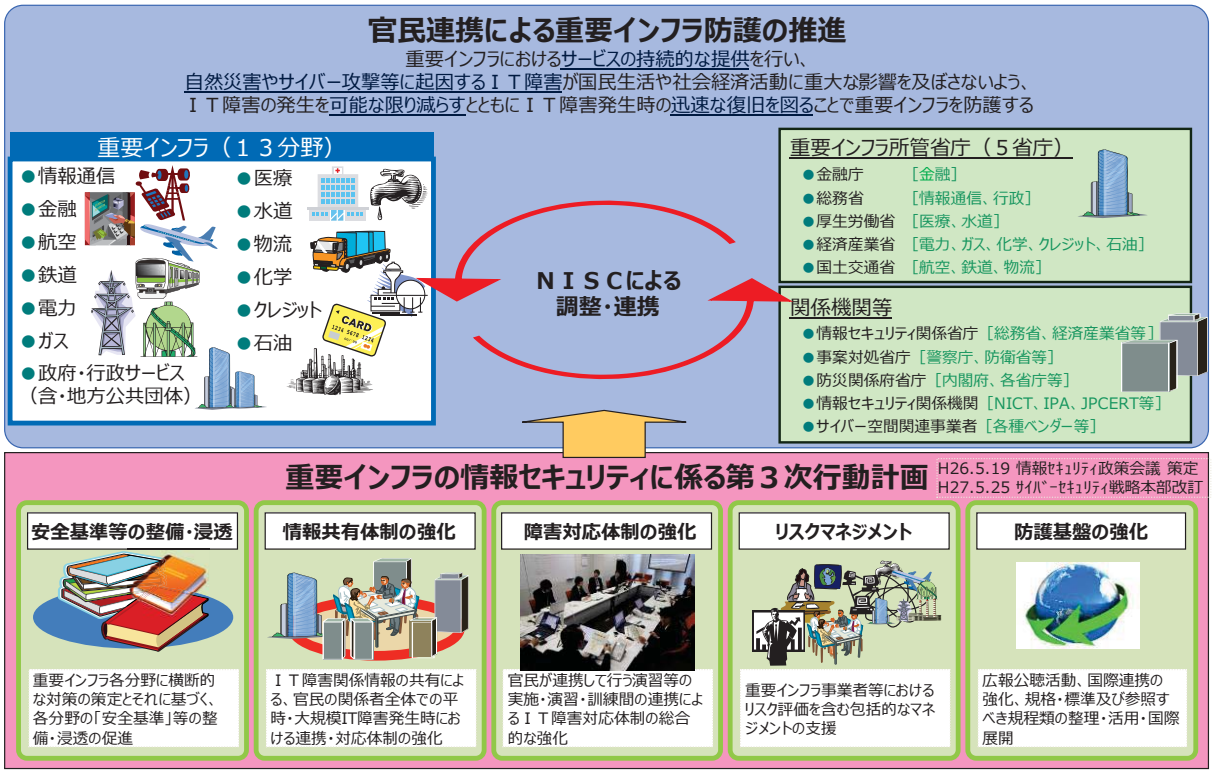
（本ページは白紙です。）

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３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３次行動計画



第３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

重要インフラにおける**サービスの持続的な提供**を行い、**自然災害やサイバー攻撃等に起因するＩＴ障害**が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を**可能な限り減らす**とともにＩＴ障害発生時の**迅速な復旧を図る**ことで重要インフラを防護する。

「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。
また、重要インフラ防護における官民が一丸となった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**。

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

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。
- ＩＴ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、ＩＴ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

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とする**リスク源の認識**。
- 上記のリスク源の評価及びそれに基づく**優先順位を含む方針の策定**。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営**資源の継続的な確保**。
- システムの運用状況の把握等を通じた当該方針の**実行の有無の検証**。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の**検証及び改善策の有無の検証**。

第３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・向上を目的に、PDCAサイクルの下、「指針」及び「安全基準等」の相互的・継続的改善を目指す。

※安全基準等・・・業法、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・改訂に資するため、分野横断的に必要度の高い対策項目を収録したもの

行動計画期間当初の課題

- 優先順位付けされた指針の提示要望（事業者等から）
- 事業者等のPDCAサイクルに沿った指針の見直し

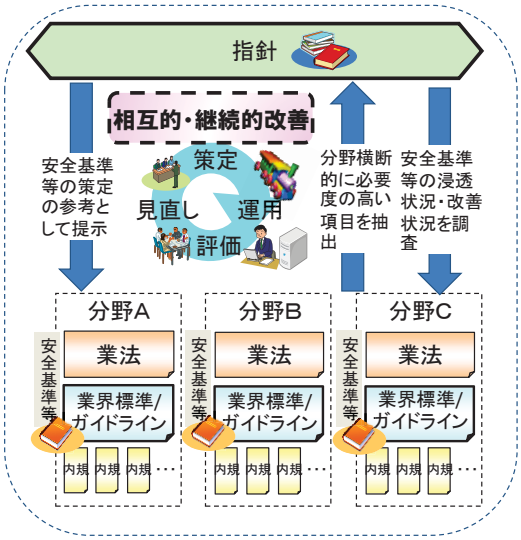
行動計画期間中の施策

（１）　指針の継続的改善
- 指針本編・対策編のPDCAサイクルに沿った見直し
- セキュリティ対策の優先順位付け等（成長モデル）の考え方の例示

（２）　安全基準等の継続的改善
- 各分野の安全基準等を対策等から得た知見を基に改善

（３）　安全基準等の浸透
- 毎年の調査（重要インフラ事業者等への往訪を含む）により、対策状況を客観的に把握
- 中小規模事業者等調査対象の拡大と対策プロセスに沿った項目整理により、強化対象等を明確化

第３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

多様な脅威に対応するため、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に加え、分野内、分野間あるいは官民間の情報共有を一層強化する。

行動計画期間当初の課題

- 情報共有頻度の分野間格差の解消
- 「脅威の類型」の細分化
- 大規模ＩＴ障害対応時の情報共有体制の構築
- 新たな関係主体との連携の在り方の整理　　等

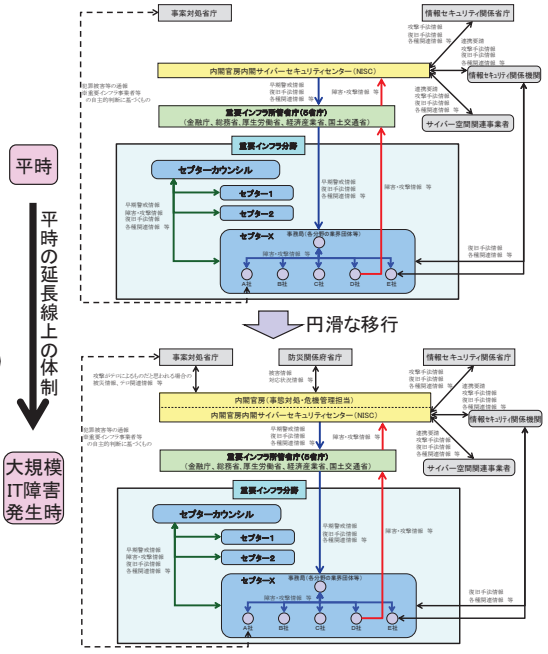
行動計画期間中の施策

（１）　情報共有体制の発展
- 新たな関係主体※の追加
  ※防災関係府省庁、サイバー空間関連事業者
- 平時とその延長線上の大規模IT障害対応体制の構築

（２）　情報共有の更なる促進
- 迅速・正確な状況把握のための情報連絡・提供時の詳細項目の見直し
- セプターカウンシルを始めとするセプター間の情報共有の更なる充実

（３）　関係主体の役割の明確化
- 多様な関係主体の役割を平時・大規模IT障害発生時に分類して明確化

第３次行動計画に基づく取組



第３次行動計画 施策③：障害対応体制の強化

分野横断的演習の更なる充実に加え、IT障害対応に関する他の演習・訓練との連携・役割分担を行うことで、重要インフラ事業者等のIT障害対応能力を高める。

行動計画期間当初の課題

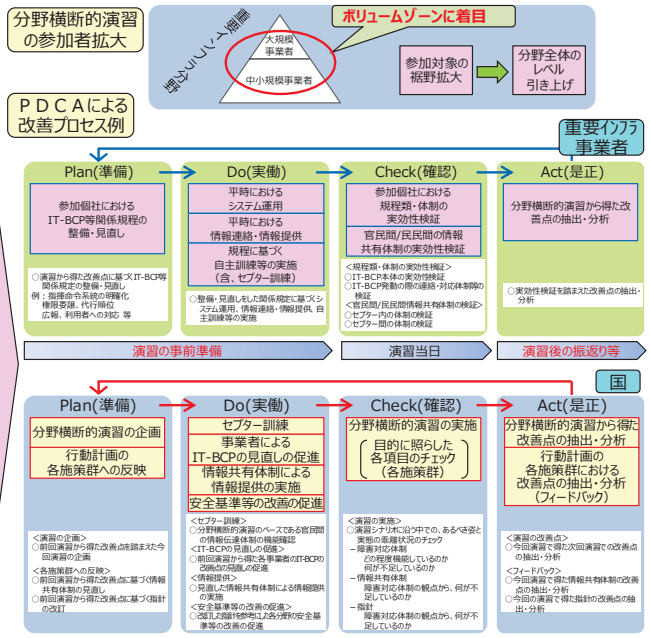
- 横断的演習の成果の重要インフラ全体への普及・浸透
- IT障害発生時の対応を踏まえた関係主体の在り方
- 重要インフラ所管省庁等による演習・訓練との連携　　等

行動計画期間中の施策

（１）　分野横断的演習の改善
- 他施策等との連携強化による横断的演習自身の改善
  ※他施策で得られた知見、最新動向のシナリオへの反映
  ※演習成果の他施策への反映
- 成果の浸透
- 参加対象の裾野拡大

（２）　関係演習・訓練との連携による相乗効果
- セプター訓練・重要インフラ所管省庁による他演習・訓練と相互に連携・補完

第３次行動計画に基づく取組



第３次行動計画 施策④：リスクマネジメント

重要インフラ事業者等がその事業目的であるサービスの持続的提供を実現するために実施するリスクマネジメントを支援する。

行動計画期間当初の課題

- 重要インフラ事業者等において、事業目標達成に向け必要なリスクマネジメントの訴求
- 環境変化等に応じて生じ得るリスク源、多大な影響が生じうる環境変化の中長期的な調査

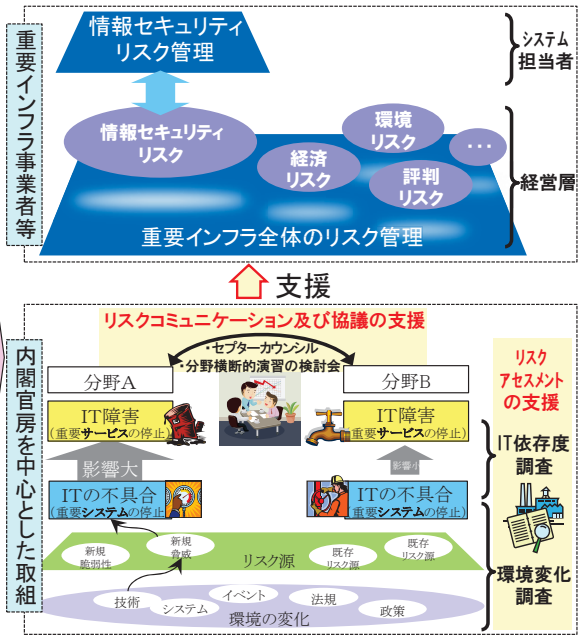
行動計画期間中の施策

（１）　リスクマネジメントの標準的な考え方
- リスクマネジメントは自らの状況把握をし、各重要インフラ事業者等がそれぞれにおいて主体的に実施
- 防護基盤強化のため作成する手引書等の利活用
  ※国際標準への準拠を求めるものではなく、自組織のリスクマネジメントの更なる最適化等が目的。

（２）　リスクマネジメントの内閣官房による支援
- リスクアセスメントの支援
  ・環境変化調査
  ・相互依存性解析（ＩＴ依存度調査含む）
- リスクコミュニケーション及び協議の支援

（３）　他施策との相互反映プロセスの確立
- 環境変化調査、相互依存性解析の結果 ⇒ 他施策
- 他施策で顕在化したリスク等 ⇒ 調査・解析対象

第３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

広報公聴、国際連携、関係規程類、国際基準等の手引書作成等、重要インフラ防護の全体を支える共通基盤的な取組を強化する。

行動計画期間当初の課題

- 広報公聴の一層の充実
- 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
- 参照すべき規程類の整備・活用　　等

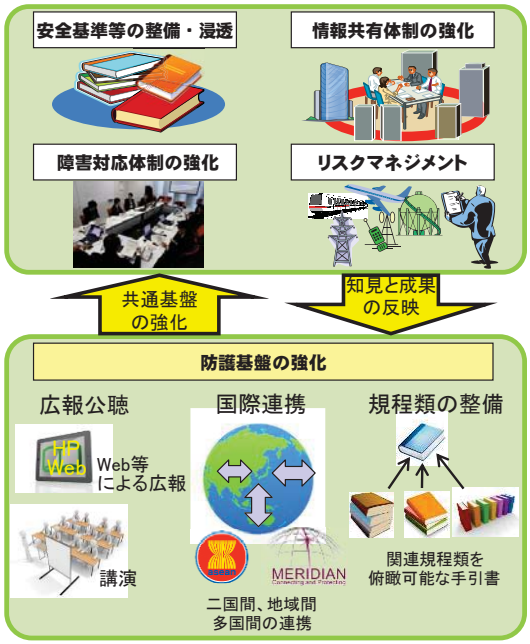
行動計画期間中の施策

（１）　広報公聴
- 行動計画及びその取組について、広く認識・理解を得るための公報広聴活動の充実

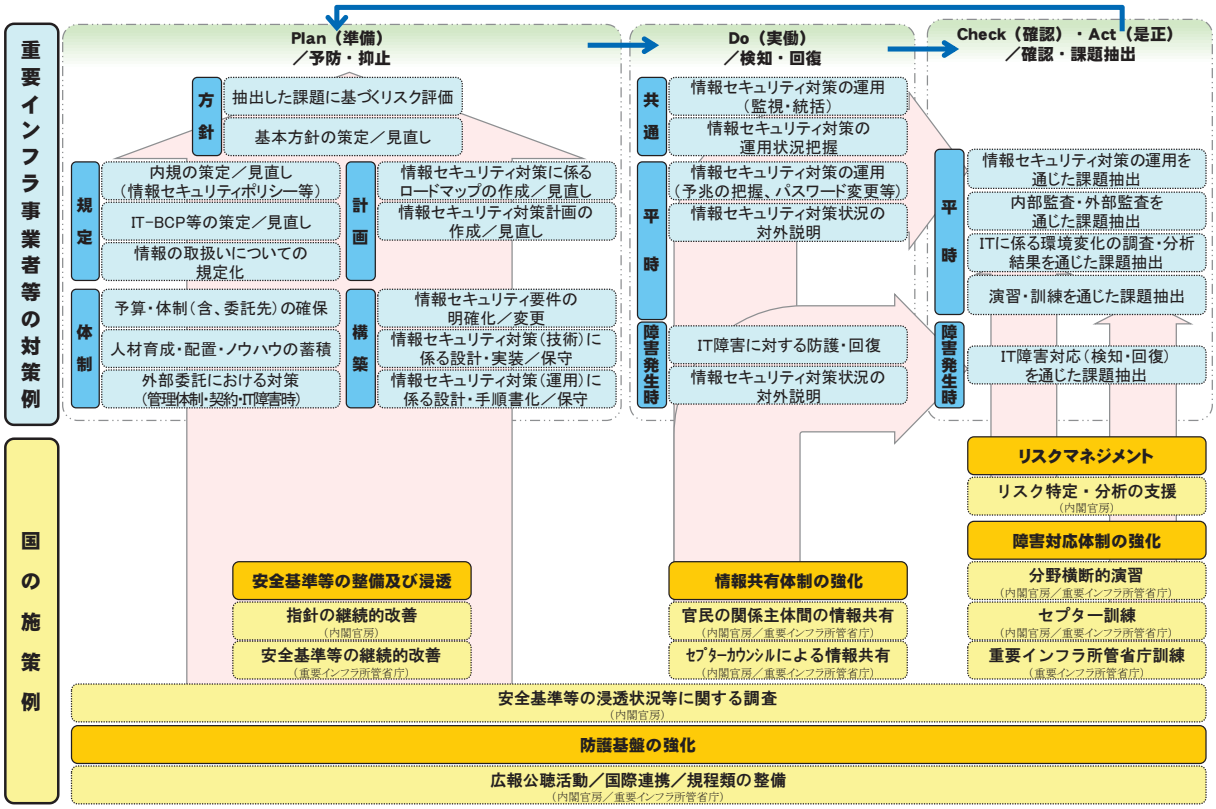
（２）　国際連携
- 欧米、ＡＳＥＡＮ、Meridian等二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携

（３）　規程類の整備
- 重要インフラ防護に係る関連規程集の発行
- 国際基準等の適用の際の手引書等の整備
- 情報セキュリティに関する評価・認証制度の拡充の支援

第３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「国の施策例」



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、2015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

2015年度は、第３次行動計画の２年目に当たり、2014年度に引き続き第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ている。各施策の取組等の詳細は次節以降に示すものの、2015年５月にはサイバーセキュリティ戦略本部において安全基準等策定指針の改訂が行われたほか、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３倍と活発に行われ、また、分野横断的演習も過去最大規模での開催となるなど、各種取組を行っているほか、第３次行動計画における施策の枠外の取組として、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）。

このように、第３次行動計画における取組は着実に進展しているものと評価できる。

第３次行動計画を取り巻く環境としては、2016年度末で第３次行動計画の期間が終了することから、対策強化に向けた検討課題を整理した、「第３次行動計画の見直しに向けたロードマップ」をとりまとめ、サイバーセキュリティ戦略本部において2016年３月に決定した。同ロードマップにおいては、IoTの浸透に伴う制御技術と情報通信技術の相互依存性の高まり、面的防護に向けた情報共有等の連携体制強化の必要性等、及び諸外国における重要インフラへの取組の加速化の３点を考慮すべき環境変化とした上で、サイバー攻撃に対する体制強化、重要インフラに係る防護範囲の見直し、及び多用な関係者間の連携強化の３本柱からなる強化すべき取組の方向性を示している。

(3)　今後の取組

第３次行動計画に基づく取組については、2016年度も引き続き推進し、内閣官房と重要インフラ所管省庁等が一体となって、重要インフラ事業者等に対して必要な支援を実施することが原則である。

また、第３次行動計画そのものについても、前述のロードマップに従って各種課題について検討を進め、2017年３月末を目途にその見直しについて結論を得るとともに、早急に対処すべき事項については、第３次行動計画の見直しを待たずに対処していく。

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のPDCAサイクルとの整合及び第３次行動計画の他施策との連携強化を図るとともに、その重要性を重要インフラ事業者等、とりわけ経営層に訴求する仕組みを構築した。

○安全基準等策定指針の改訂等

各重要インフラ分野における安全基準等を策定するための指針を改訂し、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）」を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した。同指針は従来の内容を踏まえつつ、第３次行動計画の記載内容に照らして、情報セキュリティの対策項目を重要インフラ事業者等のPDCAサイクルに沿って整理する等の再構成を行ったもので、採録した対策項目数は、PDCAの各プロセスに応じて整理した結果、497項目となった。

また、同指針の改訂と併せ、重要インフラ専門調査会において、具体化例を記載した同指針対策編の改訂を行うとともに、新たな試みとして、対策途上や中小規模の重要インフラ事業者等も取り組みやすいよう、重要インフラ事業者等による対策項目の段階的な実現に資することを目的に、対応の優先順位付けの考え方を例示した手引書を策定した。同手引書については、重要インフラ事業者等への周知広報に努め、具体的には、分野横断的演習の検討会、重要インフラ事業者等に往訪した際などに説明を行った。

○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は継続的に改善していくことが重要であることから、各分野横断的な安全基準等についての改善状況調査を実施した（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、２つの分野において安全基準等の改善を行ったほか、12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安全基準等の浸透状況を把握するため、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）。

今年度の調査においては、昨年度に引き続き、回答を通じて重要インフラ事業者等による対策状況のセルフチェックが可能となるよう調査項目を配置するとともに、アンケート調査を補完するため、往訪による調査を実施し、より掘り下げた対策状況のヒアリングを通じ課題及び良好事例を収集した。

また、報告のとりまとめに当たっては、新たに従業員数別の集計結果を追加し、従業員数の大小による取組状況の違いについても明らかにした。なお、アンケート調査は

3,281事業者等からの回答があり、重要インフラ事業者等における安全基準等に基づく自己検証への取組は７割強、定期的な自己検証への取組は５割弱、定期的な自己検証に基づく課題抽出・改善への取組は３割強の実施率であった。加えて、重要インフラ事業者等からセミナー等の開催を通じた指針の更なる理解を求める声があった。

イ　今後の取組

2015年度の取組結果を活用し、引き続き、重要インフラ事業者等に対して第３次行動計画や安全基準等策定指針の目的・考え方の浸透を目指す。

具体的には調査の継続に加え、重要インフラ事業者等との意見交換の場等での説明を通じて上記目的・考え方の浸透をより一層図るとともに、国の支援に対する各事業者等からの要望等を把握する取組を更に充実させる。また、重要インフラ所管省庁と連携し、強制基準やガイドライン等の体系を明確にし、安全基準等の改善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。2015年度は、より効果的かつ迅速な情報共有に資するため、重要インフラ所管省庁との間の情報共有様式の改良に取り組んだほか、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場等を通じて、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を図った。なお、重要インフラ事業者等や情報セキュリティ関係機関から内閣官房に対して453件の情報連絡が行われ、内閣官房からは44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	2009	2010	2011	2012	2013	2014	2015
重要インフラ事業者等から内閣官房への情報連絡件数	128件	169件	43件	110件	153件	124件	401件
関係省庁・関係機関から内閣官房への情報共有件数	294件	137件	400件	50件	55件	27件	52件
内閣官房からの情報提供件数	13件	48件	34件	38件	49件	38件	44件

また、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検討を進めるとともに、内閣官房（事態対処・危機管理担当）及び関係省庁と連携し、2016年１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。

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、2015年４月の総会で決定した活動方針に基づき、2015年度に、企画運営WG（６回）、相互理解WG（４回）、情報収集WG（４回）、総会準備WG（３回）及び幹事会（４回）を開催し、セプター間の情報共有や事例紹介等、情報セキュリティ対策の強化に資する情報収集や知見の共有を行った。また、セプターカウンシルの自律的な運営体制と更なる活性化に向けた組織の在り方を検討し関係規程の改正を行った。具体的には、運営委員会及び新たな幹事会を設置し、これまでNISCが務めた事務局機能を移管することで、各セプターが積極的にセプターカウンシルの運営を行う体制を構築するとともに、NISCは引き続きセプターカウンシルの運営及び活動に対する支援を行うこととした。なお、セプターカウンシルにおいて、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や、米国を始めとした諸外国の情報共有に係る取組の進展を踏まえ、情報共有をしやすくする環境整備や共有情報の拡充・共有体制の強化等、引き続き情報連絡・情報提供の取組を継続・強化していく。また、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、検証結果等を踏まえた手順の整理を実施する。

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、2013年度分野横断的演習と比較すると、参加機関数は約5.0倍（61組織→302組織）、参加者数は約5.5倍（212名→1,168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	2012	2013	2014	2015
参加機関数	42組織	61組織	94組織	302組織
内、大阪会場参加			（10組織）	（66組織）
内、自職場参加	（３組織）	（３組織）	（15組織）	（36組織）
参加者数	148名	212名	348名	1,168名
内、大阪会場参加			（32名）	（149名）
内、自職場参加	（15名）	（10名）	（59名）	（315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99.1％（有意義だった：75.7％、概ね有意義だった：23.4％）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63.1％、今後実施予定が16.2％であった。また、組織外で実施する演習への参加率は55.9％、今後参加予定は17.1％となっている。

○セプター訓練

各分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、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　セプター訓練参加セプター・参加事業者数の推移

年度	2012	2013	2014	2015
参加セプター	11セプター	12セプター	14セプター	18セプター
参加事業者	1,570者	1,561者	1,644者	1,658者

実施に当たっては、2014年度のセプター訓練から取り入れた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（それまでは内閣官房からの情報提供のみである「片道」訓練）をベースに実施した。また、各セプターの実情及び要望も考慮し、日時を予め通知せず抜き打ちによる訓練の実施、メール等が使えないことを想定した訓練の実施、通知情報の具体化等の訓練内容充実など、「カスタマイズ型訓練」の実施に取り組んだ。

また、セプター訓練を分野横断的演習に先んじて実施することで、各分野内の「縦」の情報共有と、分野横断的演習における各分野間の「横」の情報共有とを連携・補完させ、相乗効果を発揮できるよう取り組んだ。結果、課題の抽出や、新たな気付きを得たセプターもあり、訓練の有用性が改めて確認された。

○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、LAN管理者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）を実施するとともに、その拡大に向けた法整備を行ったほか、経済産業省では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。

イ　今後の取組

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、セキュリティ意識の高まりと旺盛な演習ニーズに応える会場新設や参加モデルに係る検討、各事

業者のセキュリティ対策・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、分野横断的演習の運営ノウハウや知識等の還元に関する検討について取り組む。

セプター訓練については、2015年度から実施した「カスタマイズ型訓練」を継続して実施し、各分野における「縦」の情報共有体制の更なる強化を図っていく。

また、分野横断的演習等と、重要インフラ所管省庁等が実施する演習等とが相互に補完し、効率的・効果的な重要インフラ防護能力の維持・向上が図られるよう連携を図っていく。

(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が主体的に実施するリスクマネジメントを推進するとともに、官と民、民と民における双方向のコミュニケーションが促進され、重要インフラ事業者等が実施するリスクコミュニケーション及び協議の強化が図られた。

○リスクアセスメントに対する支援

第３次行動計画に記載されている相互依存解析の関連調査として、重要インフラ事業者等の外部サービスへの依存性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、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際に、調査結果に含まれる外部サービスの概念やその評価に向けた考え方等を利活用できるようにしたものである。

○リスクコミュニケーション及び協議に対する支援

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、前述のとおりセプターカウンシルの活動を支援したほか、分野横断的演習につい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、重要インフラ専門調査会についても４回開催し、重要インフラ防護施策に関する意見交換を行った。

○リスクマネジメントに利活用できる手引書等の整備

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、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手法について国際標準等を参考に手順書として整備し、一部の事業者等の協力を得て当該手順書を用いたリスクアセスメントのトライアルを実施した。

イ　今後の取組

第３次行動計画に記載されている環境変化調査及び相互依存性解析については、第３次行動計画の見直しにも資するよう、外部委託による実施の必要性も含めて調査内容の検討を行う。

また、リスクマネジメントに利活用できる手引書等の整備については、2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの手法の整備作業やトラ

[1] 重要インフラ事業者等の外部サービスへの依存性に関する調査報告書
http://www.nisc.go.jp/inquiry/pdf/itizon2016_gaiyou.pdf

イアルを通じて得られた知見を基にして、重要インフラ事業者等に対する平時のリスクアセスメントを支援するガイドラインを整備するとともに、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可能な手引書等についても検討を行う。

(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。

＜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。

○広報広聴活動

第３次行動計画に基づく取組に関する国民への周知や重要インフラ事業者等への広範な協力・支援を得るための広報広聴活動を実施した。

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の周知・広報を実施した。また、分野横断的演習についてはその結果について、NISC公式twitter（@cas_nisc）等を通じても広報を実施した。

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NISC重要インフラニュースレターを22回発行した。

また、重要インフラ防護に関する講演を23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るとともに、分野横断的演習について説明・周知用の映像資料を作成し、動画共有サイトにおいて広く公開した。

○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。

多国間の会合としては、2015年10月にスペインで開催されたMeridian会合において、重要インフラ防護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、多国間でサイバー攻撃や脆弱性対応についての情報を共有している。

日・ASEANにおいては、2015年10月に日・ASEAN情報セキュリティ政策会議を開催し、2014年に策定された「日・ASEANにおける重要インフラ防護に関するガイドライン」に基づき、日本及びASEAN加盟各国における重要インフラ防護、インシデント対応におけるベストプラクティスの共有を推進した。また、2015年２月に日本国内において、JICAやHIDAと連携しASEAN向け重要インフラ防護研修（２回）を実施した。

二国間協議についても、「日米サイバー対話」をはじめとして実施しているほか、日米間の重要インフラ防護をテーマとする会合に出席するなどの取組を行っている。

〇規格・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水準を向上させるため、内閣官房及び重要インフラ所管省庁等を対象として重要インフラ防護に関する規程集の作成・配布を実施した。

また、国際基準等を重要インフラ防護に適用する場合の手引書として、リスクマネジメントに関する手引書を作成することとし、国内外で策定され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、手引書の作成に活用した。

加えて、制御機器に係るセキュリティ認証制度（EDSA認証）について、経済産業省及びCSSCを中心として説明会の開催やWebサイトでの普及・啓発を実施。2015年度は１製品の認証が行われている。また、制御システム全体のセキュリティ評価・認証に向けて、制御システムセキュリティ国際標準IEC 62443の規格要求事項を整理するとともに、IEC62443に基づく制御システムセキュリティに関わる国際標準化を推進している。

イ　今後の取組

広報広聴活動については、Webサイトの内容の見直しを随時行っていくとともに、NISC重要インフラニュースレターと併せて、国民や重要インフラ事業者等に対する情報の展開と収集を引き続き実施する。また、講演等の機会を積極的に活用し、重要インフラ防護の取組の周知をより一層図っていく。

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、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、キャパシティビルディングへ積極的に寄与するとともに、各国の取組の共有などを通じ、相互の重要情報インフラ防護能力の向上と連携の強化を図る。

規格・標準及び参照すべき規程類の整備については、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水準を向上させるため、重要インフラ防護に関する規程集の作成を引き続き行い、重要インフラ事業者等を含めた配布範囲の拡大や、収録対象の文書の拡大等を図っていく。また、国際基準等を重要インフラ防護に適用する場合の手引書については、リスクマネジメントの施策における取組と連携して、手引書の精査を行っていく。さらに、制御系機器・システム等に関する評価・認証の導入の在り方については、経済産業省及びCSSC等の関係主体との協力の下、制御系機器・システムの第三者認証制度の拡充を支援する。

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「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）」を決定・公表するとともに、併せて「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）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（第１版）」を公表した。
② 必要に応じて社会動向の変化及び新たに得た知見に係る検討を、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。
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、四半期毎に実施した重要インフラ所管省庁との検討を通じて安全基準等の継続的改善を支援した。
④ 重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善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（2015 年 12 月～2016 年３月）し、「2015 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把握及び検証』について」を 2016 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（2015 年７月～11 月）及び事業者等への往訪による調査（2015 年４月～12 月）を通じて第３次行動計画策定時に認識した課題の妥当性に関する検証を実施し、「2015 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 2016 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り替えについて、第３次行動計画に基づいた手順の整備に向けた検討を実施し、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。（2015 年度　情報連絡 453 件、情報提供 44 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、2015 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幹事会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。（2015 年度のセプターカウンシル会合の回数は延べ 21 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。	・ 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それによる活性化に向けた組織の在り方を検討し関係規程の改正を図った。また構成委員による自主的な運営への段階的かつ円滑な移行について検討を進め、各会合の開催準備に関し資料整理の上、ノウハウの継承等を図った。
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、分野横断的演習等の場において紹介した。また、各演習・訓練における検証課題や得られる成果の違い等について周知を実施した。
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。結果、302 事業者 1,168 名が演習に参加した。
④ 分野横断的演習の改善策検討。	・ 事業者等による課題抽出を通じた改善を促進する観点から、改善策として、演習当日及び前後の説明会・意見交換会等の充実（説明会での第３次行動計画施策の説明、「安全基準等」策定指針を基にした検証課題の設定、サブコントローラーの選出必須化等）を実施した。 ・ また、重要インフラ全体の対策水準の底上げのため、参加形態を多様化（大阪会場の規模拡充、自職場参加の拡充等）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。
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等を重要インフラ事業者等に実施して貰うこと等により、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すのはもちろんのこと、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、成果展開用資料及び普及啓発用動画を作成した。
⑥ 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供。	・ 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、成果展開用資料及び普及啓発用動画を作成した。
⑦ 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開。	・ 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、成果展開用資料及び普及啓発用動画を作成した。
(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。	・ 2020 年の東京オリンピック・パラリンピック競技大会に向けたリスクマネジメントに関する検討と協同して、重要インフラ事業者等によるリスクマネジメントに利活用できる手引書等について、国際標準等を参考に手順書として整備を進めるとともに、一部事業者の協力を得てトライアルを実施した。
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。	・ 相互依存性解析の一部として、重要インフラサービスを支える外部サービスについて把握する目的で「重要インフラ事業者等の外部サービスへの依存性に関する調査」を行い、重要インフラ事業者等へ提供・公表することで、重要インフラ事業者等が自ら実施するリスクマネジメントに資する情報を提供した。
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。	・ 相互依存性解析の一部として、重要インフラサービスを支える外部サービスについて把握する目的で「重要インフラ事業者等の外部サービスへの依存性に関する調査」を行い、各事業者等における安全基準等において、外部委託事業者等の関係事業者を含めたサービス継続体制の確保に資する基礎資料として、重要インフラ事業者等へ提供・公表した。
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がリスクコミュニケーション及び協議を行う場として、セプターカウンシルにおける計 12 回の活動（環境変化を踏まえた各重要インフラ分野の取組事例の共有及び IT システムの利用現場や施設等の見学等）の支援を行うとともに、分野横断的演習につい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、重要インフラ専門調査会についても４回開催し、重要インフラ防護施策に関する審議に資する意見交換を行った。
(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 22 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について計 17 回説明を行った。
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 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。	・ 現在の国際連携の取り組み等を日・ASEAN セキュリティシンポジウム（10 月９日開催）で公表し NISC ホームページで公開した。

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、規程集の発行を実施し、重要インフラ所管省庁等に配布を行った。
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。	・ リスクマネジメントに関する手引書の整備を進めた。
⑧ 制御系機器・システムの第三者認証制度の拡充を支援。	・ 経済産業省が中心となって実施している制御系機器・システムの第三者認証制度の拡充について、国際電気標準会議（IEC）等における情報等の意見交換を行った。
2.重要インフラ所管省庁の施策	
(1)「安全基準等の整備及び浸透」に関する施策	
① 指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。	・ 重要インフラ所管省庁において、指針として新たに位置付けることが可能な安全基準等がないことから、新たな情報提供は行っていない。
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。	・ 総務省については、電気通信事業法の技術基準の適用範囲を拡大する改正等を行った。 ・ 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作業を実施した。 ・ 厚生労働省については、安全基準等の分析・検証を実施したが、安全基準等は現時点では、現行のガイドラインの改定は不要と判断した。 ・ 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」や策定作業中の「電力制御システムセキュリティガイドライン（仮称）」の検討作業に必要な支援を行ったほか、経済産業省が行った都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業の結果を日本ガス協会と共有し、同協会が作成している「製造・供給に係る制御システムの情報セキュリティ対策ガイドライン」改訂作業に必要な支援を行った。
④ 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透を実施。	・ 経済産業省については、産業構造審議会保安分科会電力安全小委員会において、電気事業法体系下でのサイバーセキュリティ対策のあり方を検討し、同法省令に根拠規定を追加することにより、日本電気技術規格委員会策定のガイドラインを保安規制に位置付けることとなった。
⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の継続的改善状況等の調査について、所管の各分野における現状を把握した上で、調査の回答を行った。
⑥ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。	・ 重要インフラ所管省庁は、内閣官房が実施した安全基準等の浸透状況等の調査について、所管の各分野に協力を求め、事業者からの回答数増加に努め、3,281 者（2014 年度は 3,228 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。
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の他、重要インフラ事業者等の外部サービスへの依存性に関する調査など多くの調査・ヒアリングに協力した。

⑤ セプターの機能充実への支援。	・ 重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥ セプターカウンシルへの支援。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
(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、2015 年８月から 11 月までの間に、セプター訓練を実施し、18 セプターと 1,658 団体が参加した。
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、2015 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、2015 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 2015 年度分野横断的演習への参加を促し、全体で 302 組織 1,168 名の参加者を得た。うち、2014 年度より新設された大阪会場には、66 組織 149 名の参加を、自職場からは 36 組織 315 名の参加をそれぞれ得るとともに、208 組織の初参加者を得た。
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、2015 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。	・ 総務省において、分野横断的演習及び総務省の実践的サイバー防御演習との相互の連携について検討している。 ・ 経済産業省において、2015 年に開催されたサイバーセキュリティ演習におけるシナリオについて、分野横断的演習におけるシナリオの内容との連携を検討するなど相互連携への協力を図った。
(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の伝達のほか、重要インフラ事業者等の外部サービスへの依存性に関する調査に関して調査先となる個別の重要インフラ事業者等の紹介など、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。	・ 重要インフラを支える外部サービスに関する調査につちえは、重要インフラ所管省庁において今後、重要インフラの範囲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。
(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、2014 年４月に開始した EDSA 認証について、説明会の開催や Web サイトでの普及・啓発を行い、2015 年度には、１製品の認証を行った。
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の一部において、ブラックリスト情報等について内閣官房に情報連絡を実施した。
③ セプターカウンシル等からの要望があった場合、意見交換等を実施。	・ 重要インフラ所管省庁において、セプターカウンシル総会及び幹事会にオブザーバーとして出席した。
4. 事案対処省庁の施策	
(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。	・ 2014 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。
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。また、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に係る情報収集・分析のための体制を強化した。
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。	・ 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。
(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。	・ 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。

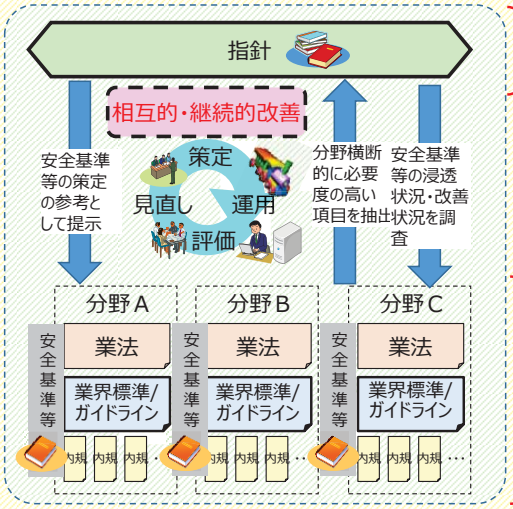
別添４－３　安全基準等の継続的改善状況等の把握及び検証

重要インフラ専門調査会第５回会合（平成28年３月25日）資料２（2015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把握及び検証」について）より

本調査の目的

【目的】

○重要インフラ防護能力の維持・向上を目的に、ＰＤＣＡサイクルの下、「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。



<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

【実施根拠】

◆サイバーセキュリティ2015　：　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、（中略）の５つの施策を実施する

◆第３次行動計画　：　重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表

本調査のポイント及び結果概要

【把握及び検証のポイント】

○重要インフラ分野の以下について、2015年12月～2016年３月にて調査。（再調査期間を含む）

項　目	ポイント
実施状況等	・各分野のPDCAサイクルに基づく継続的改善の実施状況と今後の予定 ・安全基準等の分析・検証方法及び分析検証の観点・背景
指針の改訂要件	・指針の継続的改善に繋がる安全基準等における具体的な対策項目や事例の有無確認

【結果概要】

○指針第４版（2015年度改訂）等を契機とした各分野の「安全基準等」の改善に向けた取組状況については、以下のとおり。

2015年度末までに改善済	：	２分野（電気通信、金融）
2015年度末までに分析・検証済	：	５分野（航空運送、航空管制、鉄道、自治、物流）
分析・検証中	：	７分野（放送、電力、ガス、医療、水道、化学、石油）
2015年度は実施予定なし	：	２分野（ケーブル、クレジット） ＊両分野とも構成員の拡大に向けた取組を優先するため

○今回の調査結果からは、指針への反映を要する分野横断的に必要度の高い項目はなかった。

安全基準等の継続的改善状況（情報通信分野：電気通信）

名称	①：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等（関連する告示を含む） ②：情報通信ネットワーク安全・信頼性基準 ③：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２版）
発行主体	①：総務省、②：総務省、③：一般社団法人電気通信事業者協会　安全・信頼性協議会
最新改定年月	①：2014年６月／2015年８月／2015 年11月、②：2015年４月、③：2013年３月
状況	**１．継続的改善（分析・検証）状況・理由** ①：これまで技術基準の適用対象ではなかった電気通信事業者（回線非設置事業者）における電気通信事故の多発。情報通信技術の発展に伴い可能となったベストエフォート方式での一定の通信品質の担保 ②：定期的な改善 ③：指針改訂を受けた改善
	２．継続的改善（分析・検証）プロセス ①：－／2013年４月～2013年10月、2015年５月～2015年７月／2013年12月から2014年12月、2015年４月から2015年11月にかけて、実施 ②：2015年５月から2016年３月にかけて、実施中 ③：2015年６月から2015年12月にかけて、実施
	３．継続的改善（分析・検証）の結果 ①：これまで技術基準の適用対象ではなかった電気通信設備のうち、国民生活に重要な役割を果たす役務を提供する電気通信設備を、技術基準の適用対象とする旨を規定。 0AB-J IP電話の品質要件の緩和、ベストエフォート方式で0AB-J IP電話を提供する際の品質要件の規定 ②：－ ③：改定不要と判断
	４．その他 ①：技術基準の新規適用対象範囲について2013年４月から同年10月に検討し、情報通信行政・郵政行政審議会の審議や意見募集を2015年５月から同年７月に実施。 0AB-J IP電話の品質要件を2013年12月から2014年12月に検討し、情報通信審議会及び情報通信行政・郵政行政審議会の審議や意見募集を2015年９月から同年10月に実施

安全基準等の継続的改善状況（情報通信分野：ケーブルテレビ・放送）

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
発行主体	一般社団法人日本ケーブルテレビ連盟
最新改定年月	2012年11月
状況	**１．継続的改善（分析・検証）の状況・理由** 2015年度は新規の重要インフラ事業者向け施策を優先したため、実施予定なし
	２．継続的改善（分析・検証）のプロセス －
	３．継続的改善（分析・検証）の結果 －
	４．その他 －

名称	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	日本放送協会（NHK）、一般社団法人日本民間放送連盟
最新改定年月	2007年11月
状況	**１．継続的改善（分析・検証）の状況・理由** 指針改訂を受け、実施中
	２．継続的改善（分析・検証）のプロセス 2015年７月から、NHKと民放連・情報セキュリティ対策ワーキンググループにて実施中
	３．継続的改善（分析・検証）の結果 －
	４．その他 指針（第４版）に合わせて改定作業中

安全基準等の継続的改善状況（金融分野）

名称	①：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 ②：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 ③：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	公益財団法人金融情報システムセンター（FISC）
最新改定年月	①：2008年6月、②：2015年6月、③：2013年３月
状況	**１．継続的改善（分析・検証）の状況・理由** ①：実施予定なし ②：指針改訂、情報セキュリティ対策の運用を通じた課題抽出、ＩＴに係る環境変化の調査・分析結果を通じた課題抽出、サイバー攻撃動向を受け、実施 ③：サイバー攻撃動向を受け、実施中
	２．継続的改善（分析・検証）のプロセス ①：－ ②：2014年６月から2015年6月にかけて、ＦＩＳＣ監査安全部が事務局となる安全対策専門委員会及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実施 ③：2014年11月から、ＦＩＳＣ監査安全部が事務局となる安全対策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にて実施中
	３．継続的改善（分析・検証）の結果 ①：－ ②：部分的な改訂及び新たな安全基準等の追加として、「金融機関等コンピュータシステムの安全対策基準・解説書（第８版追補改訂版）を2015年６月に発刊。主な改訂内容としては、サイバー攻撃に関する対応、クラウドサービス利用に関する対応、外部委託先による不正な引出し事例への対応 ③：－
	４．その他 ②ＦＩＳＣ安全対策基準の業態別化については、継続検討中

安全基準等の継続的改善状況（航空分野：航空運送・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３版）
発行主体	国土交通省
最新改定年月	2012年10月
状況	**１．継続的改善（分析・検証）状況・理由** 指針改訂、サイバー攻撃動向、所管事業者に対するセキュリティ対策の実施状況と課題に係るアンケート結果を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年4月から、航空運送事業者・定期航空協会・国土交通省にて実施
	３．継続的改善（分析・検証）の結果 全面改訂を実施することで対応
	４．その他 改訂の方向性については、指針（第４版）改訂を受けたPDCAサイクルに沿った対策項目の再配置、最新のセキュリティ動向を踏まえた対策項目の追加が軸。そこに各事業者等へのアンケート結果を反映

名称	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３版）
発行主体	国土交通省
最新改定年月	2012年10月
状況	**１．継続的改善（分析・検証）状況・理由** 指針改訂、サイバー攻撃動向を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年4月から、国土交通省にて実施
	３．継続的改善（分析・検証）の結果 全面改訂を実施することで対応
	４．その他 改訂の方向性については、指針（第４版）改訂を受けたPDCAサイクルに沿った対策項目の再配置、最新のセキュリティ動向を踏まえた対策項目の追加が軸

安全基準等の継続的改善状況（鉄道分野、電力分野）

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２版）
発行主体	鉄道事業者等
最新改定年月	2012年10月
状況	**１．継続的改善（分析・検証）の状況・理由** 指針改訂、サイバー攻撃動向、所管事業者に対するセキュリティ対策の実施状況と課題に係るアンケート結果を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年4月から、国土交通省鉄道局・重要インフラ関係事業者等にて実施
	３．継続的改善（分析・検証）の結果 全面改訂を実施することで対応
	４．その他 改訂の方向性については、指針（第４版）改訂を受けたPDCAサイクルに沿った対策項目の再配置、最新のセキュリティ動向を踏まえた対策項目の追加が軸。そこに各事業者等へのアンケート結果を反映

名称	電力制御システム等における技術的水準・運用基準に関するガイドライン
発行主体	電気事業連合会情報通信部
最新改定年月	2010年3月
状況	**１．継続的改善（分析・検証）状況・理由** 定期的な改善、産業構造審議会保安分科会電力安全小委員会での議論を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年6月から2016年度にかけて実施中
	３．継続的改善（分析・検証）の結果 民間規格を策定することで対応
	４．その他 電力安全小委員会(第10回)での議論を踏まえ、サイバーセキュリティ対策を電気事業法の保安規制上、位置づけることを検討中。現在、日本電気技術規格委員会にて民間規格の審査中

安全基準等の継続的改善状況（ガス分野）

名称	製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン
発行主体	一般社団法人日本ガス協会
最新改定年月	2012年1月
状況	**１．継続的改善（分析・検証）状況・理由** 指針改訂を受け、実施中
	２．継続的改善（分析・検証）のプロセス 2015年６月から2016年６月の期間にかけて、日本ガス協会システムセキュリティワーキンググループにて実施中
	３．継続的改善（分析・検証）の結果 部分的な改定実施の方向で対応中
	４．その他 －

安全基準等の継続的改善状況（自治分野）

名称	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	総務省
最新改定年月	2015年3月
状況	**１．継続的改善（分析・検証）状況・理由** サイバー攻撃動向を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年3月と2015年6月から2015年12月にかけて、総務省自治行政局地域情報政策室にて実施
	３．継続的改善（分析・検証）の結果 改定不要と判断
	４．その他 2015年3月の主な改定(追記)内容 ・標的型攻撃への対策(入口対策・内部対策等)、情報漏洩対策（支給品以外の端末・ＵＳＢメモリ等の取扱い、暗号化等）、組織体制の整備(地方公共団体におけるＣＳＩＲＴ機能として統一的な窓口機能の整備) 日本年金機構の事案を踏まえた2015年6月以降の対応 ・標的型攻撃に係るインシデント初動マニュアルの策定、インシデント発生時のNISCまでの連絡ルート強化、自治体の緊急時対応計画の見直し・訓練の徹底、自治体情報セキュリティ支援プラットフォームの構築 ・大臣通知により、次の三層からなる対策を講じて情報セキュリティ対策の抜本的強化の取組を自治体に要請 －マイナンバー利用事務系では、端末からの情報持出し不可設定等を図り、住民情報流出を徹底して防止 －LGWAN環境のセキュリティ確保に資するため、LGWAN接続系とインターネット接続系の分割 －都道府県と市区町村が協力して自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を講じる

安全基準等の継続的改善状況（医療分野、水道分野）

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4.2版)
発行主体	厚生労働省
最新改定年月	2013年10月
状況	**１．継続的改善（分析・検証）状況・理由** 情報セキュリティ対策の運用を通じた課題抽出を受け、実施中
	２．継続的改善（分析・検証）のプロセス 2015年10月から2016年３月にかけて、医療情報ネットワーク基盤検討作業班にて実施中
	３．継続的改善（分析・検証）の結果 －
	４．その他 －

名称	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	厚生労働省
最新改定年月	2013年6月
状況	**１．継続的改善（分析・検証）の状況・理由** 2015年度指針改訂を受け、実施中
	２．継続的改善（分析・検証）のプロセス 2015年５月から2016年５月にかけて、厚生労働省医薬・生活衛生局生活衛生・食品安全部水道課にて実施中
	３．継続的改善（分析・検証）の結果 －
	４．その他 －

安全基準等の継続的改善状況（物流分野、化学分野）

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２版）
発行主体	国土交通省
最新改定年月	2012年10月
状況	**１．継続的改善（分析・検証）の状況・理由** 指針改訂、サイバー攻撃動向、所管事業者に対するセキュリティ対策の実施状況と課題に係るアンケート結果を受け、実施
	２．継続的改善（分析・検証）のプロセス 2015年4月から、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)にて実施
	３．継続的改善（分析・検証）の結果 全面改訂を実施することで対応
	４．その他 改訂の方向性については、指針（第４版）改訂を受けたPDCAサイクルに沿った対策項目の再配置、最新のセキュリティ動向を踏まえた対策項目の追加が軸。そこに各事業者等へのアンケート結果を反映

名称	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	石油化学工業協会
最新改定年月	2015年３月(新規策定)
状況	**１．継続的改善（分析・検証）の状況・理由** 指針改訂、情報セキュリティ対策の運用を通じた課題抽出を受け、実施中
	２．継続的改善（分析・検証）のプロセス 2015年６月から2016年５月にかけて、石油化学工業協会 情報通信委員会 情報セキュリティＷＧにて実施中
	３．継続的改善（分析・検証）の結果 －
	４．その他 －

安全基準等の継続的改善状況（クレジット分野、石油分野）

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
発行主体	一般社団法人日本クレジット協会
最新改定年月	2014年12月（新規策定）
状況	**１．継続的改善（分析・検証）の状況・理由** ＩＴ障害対応(検知・回復)を通じた課題抽出を受け、実施予定
	２．継続的改善（分析・検証）のプロセス 未定
	３．継続的改善（分析・検証）の結果 －
	４．その他 2015年度は構成員の拡大を検討しているため、構成員拡大が完了した後の2016年度中に見直しの予定としている

名称	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	石油連盟
最新改定年月	2015年3月（新規策定）
状況	**１．継続的改善（分析・検証）の状況・理由** 定期的な改善として、実施中
	２．継続的改善（分析・検証）のプロセス 2016年１月から2016年３月にかけて、石油連盟 危機管理委員会 ITセキュリティ連絡会にて実施中
	３．継続的改善（分析・検証）の結果 －
	４．その他 －

別添４－４　安全基準等の浸透状況等に関する調査

重要インフラ専門調査会第５回会合（平成28年３月25日）資料３（2015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）より

本調査運営の概要

◆調査概要

調査対象範囲　：　事業者等の範囲を重要インフラ所管省庁が決定
調査方法　：　以下のいずれかを重要インフラ所管省庁が選択
①NISCが提供する調査項目の活用
②重要インフラ分野による独自調査結果をNISCが提供する調査項目に読替（回答負荷の軽減）
調査基準日　：　2015年3月末日（調査方法②の場合はその調査基準日）
調査資料の発出・回収　：　重要インフラ所管省庁が送付・回収方法を決定し、実施
分野毎の集計　：　送付・回収した重要インフラ所管省庁が集計（所管する各分野の状況把握の観点）
全体集計・とりまとめ　：　NISCが集計・とりまとめ

◆実施時期　（NISC提供の調査項目を活用する場合）

調査期間　：　2015年　7月～2015年11月
とりまとめ　：　2015年12月～2016年　2月

◆主な調査内容（NISC提供の調査項目）

①指針(*)の認知状況に係る事項　：　指針の認知に係る状況及び周知手段
*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）、同対策編、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）
②情報セキュリティ対策の実施状況に係る事項：　Plan（方針、規定、計画、体制及び構築）、Do（平時、障害発生時の運用）、Check・Act（確認・課題抽出）の各状況
③情報セキュリティ対策に係る意見、要望等

回答状況

アンケートを配布は3,507事業者等。回答は3,281事業者等。（昨年度比　配布数：+3.4%　回答数：+1.6%　回答率：▲1.6%）

重要インフラ分野		調査対象範囲	アンケート配布数（括弧内は昨年度）	アンケート回収数（括弧内は昨年度）	調査方法
情報通信	電気通信	電気通信事業者（一部抽出）	88 (97)	75 (73)	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	332 (237)	307 (237)	
	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 (194)	194 (194)	
金融		銀行等、証券会社、生命保険会社、損害保険会社	851 (855)	683 (737)	独自調査(*1)
航空	航空運送	航空運送事業者	2 (2)	2 (2)	NISC調査
	航空管制	官庁	2 (2)	2 (2)	
鉄道		ＪＲ、大手民鉄	22 (22)	22 (22)	
電力		一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)	
ガス		大手ガス事業者	12 (12)	12 (12)	
政府・行政サービス		地方公共団体	1,789 (1,789)	1,789 (1,789)	独自調査(*2)
医療		病院情報システムを導入する病院	60 (60)	46 (53)	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	91 (88)	91 (88)	
物流		物流事業者、業界団体（一部抽出）	16 (21)	10 (7)	
化学		石油化学事業者	9(-)	9(-)	
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		－－－	**3,507（3,391）**	**3,281(3,228)**	－－－

＊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：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：4月1日）

調査結果の総括

(1) 調査結果の概要

◆ 昨年度と比して回答数が増加したが、各項目の調査結果は概ね昨年度結果と同等の傾向であった。
◆ 従業員数1,000名を境に行った各集計の結果からは、相対的に取組が進んでいる対策項目は従業員数の多寡を問わず概ね同様であること、各項目とも従業員数1,000名以上の事業者等の取組状況の方が進んでいることがうかがえた。

①PDCAサイクルに沿った継続的な対策

✓ 全回答の集計結果における「初期対応」（PDCAのうちP（規定、体制、構築）の一部が該当）の実施率は概ね85%超。「継続的改善の起点となる課題抽出に基づく改善」（PDCAのうちCA（課題抽出・改善））の実施率は概ね５割程度の項目と概ね３割以下の項目に2分化されている。
✓ 従業員数別の集計結果における「初期対応」の実施率については、1,000名以上の事業者では95%程度、1,000名未満の事業者では８割程度。また、「継続的改善の起点となる課題抽出に基づく改善」の実施率については、1,000名以上の事業者では一部項目が３割程度も総じて概ね７割程度、1,000名未満の事業者では一部項目が５割程度も総じて概ね３割程度。

②経営層の在り方

✓ 全回答の集計結果における「経営層の関与」状況は、「重点化対策の合意」が約８割、「運用状況の把握」が約５割。
✓ 2015年度調査での「運用状況の把握」においては、1,000名以上の事業者では８割弱、1,000名未満の事業者では55%程度。
✓ 経営資源の継続的な確保に関連して、「対策費用補助の制度化」、「IT人材育成のための支援」、「最小限の負担で対応できるような支援」等の国に対する要望等の意見があった。

③事業者等による自らの責任における実施状況

✓ 昨年度調査にて指針_本編・対策編を両方知っていた事業者のうち、約1/3の事業者が指針_手引書を認知していない。
✓ 「企業の水準に合わせた、水準別対策などがあると、目標とし易いのではないか」との意見があった。

④情報共有体制

✓ 重要インフラサービスでの障害発生時の情報提供体制は、サービス利用者や所管省庁向けが８割超で存在、業界窓口向けは55%程度で存在。
✓ 「大規模なサイバー攻撃、セキュリティインシデント発生時の迅速な情報提供」を求める意見があった。

⑤広報公聴活動

✓ 指針等に関して「周知・広報活動、内容の説明がある定期的なセミナー開催」を求める意見、要点のみが明確に記載されたパンフレット的な簡略版の作成等の意見があった。

(2) 課題

①PDCAサイクルに沿った継続的な対策の改善
✓ 継続的改善に向けた「現状の把握」、「課題抽出」の実施・定着が課題と認められる。

②経営層の関与の強化
✓ 「運用状況の把握」、「対策の対外説明」の実施・定着が課題と認められる。
✓ 予算・人材等に係る国の支援への要望を受け、国が行い得る支援についての検討が課題と認められる。

③事業者等による自らの責任における情報セキュリティ対策の推進
✓ 優先順位付けを例示する指針_手引書の認知度の向上を通じた掲題の対策の推進が課題と認められる。

④情報共有体制の推進
✓ 共有すべき情報の範囲の見直しや情報共有の活性化が課題と認められる。

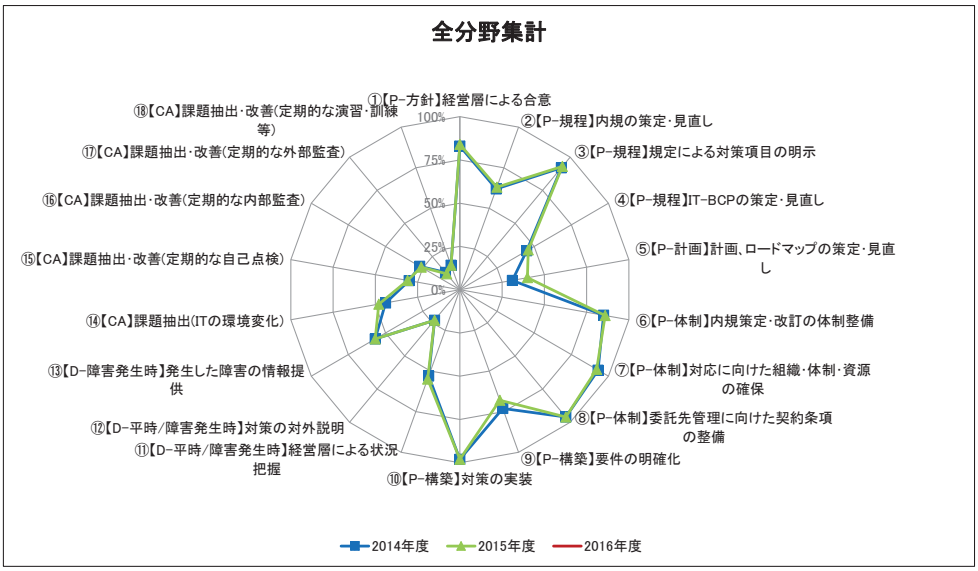
⑤広報公聴活動の強化
✓ 第３次行動計画や改訂後の指針に関し、周知・啓発を進める必要が認められる。

(3) 今後の対応

✓ 第３次行動計画が目指す「重要インフラにおけるサービスの持続的な提供」に向け、経営層の総合的判断の下、「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」との考えに基づき、情報セキュリティ対策の継続的改善が行われるよう、取り組んでいく必要がある。
✓ 引き続き、重要インフラ事業者等との意見交換の場等を通じて、行動計画や指針が示す目的や考え方等の浸透を推進するとともに、国による支援の改善に資する情報や意見の収集に係る取組を、より充実させることとしたい。

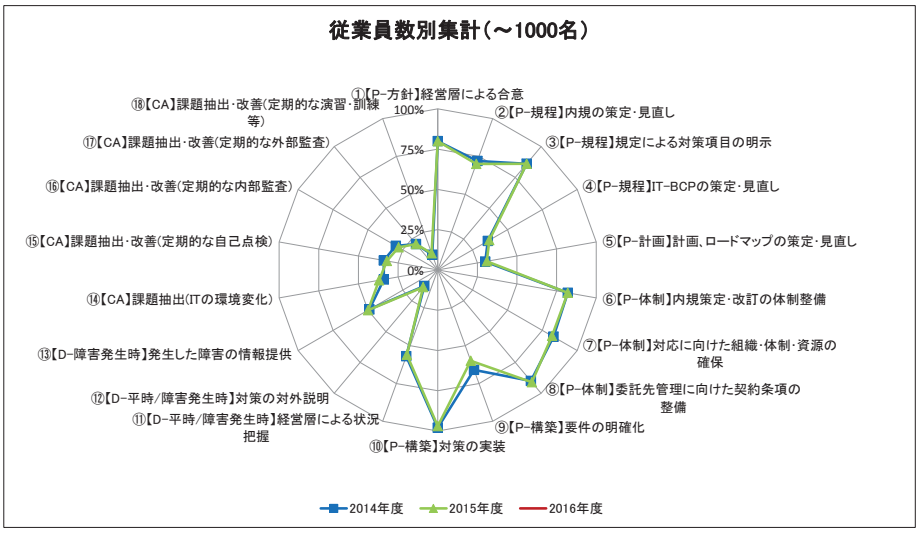
調査結果　－　主要な基礎データ①

(1) PDCAに沿った情報セキュリティ対策の取組（その１：全体）



項目	2014年度	2015年度
①	83%	84%
②	62%	63%
③	92%	93%
④	45%	46%
⑤	31%	40%
⑥	85%	86%
⑦	93%	92%
⑧	96%	96%
⑨	73%	68%
⑩	98%	98%
⑪	53%	55%
⑫	23%	23%
⑬	57%	57%
⑭	44%	48%
⑮	30%	31%
⑯	27%	26%
⑰	13%	12%
⑱	15%	15%

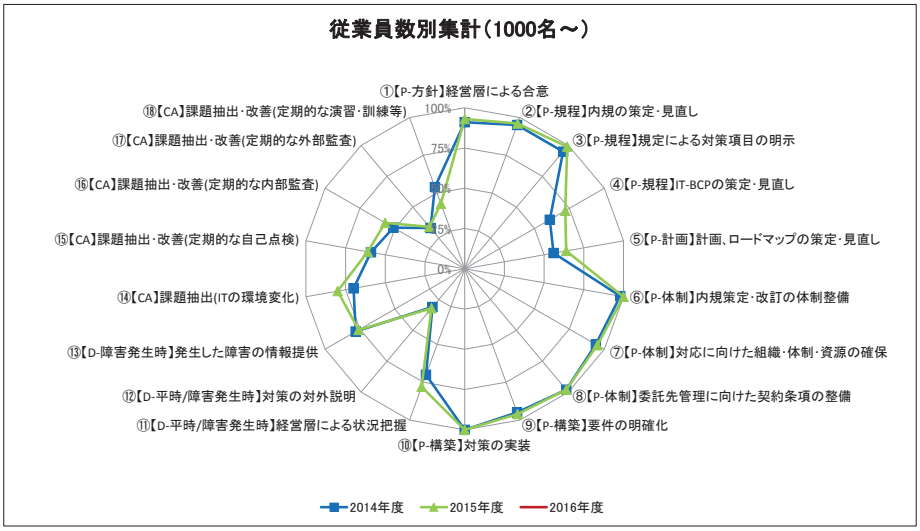
(1) PDCAに沿った情報セキュリティ対策の取組（その２：従業員数別（1000名未満））



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

※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、集計対象に含めず

(1) PDCAに沿った情報セキュリティ対策の取組（その３：従業員数別（1000名以上））

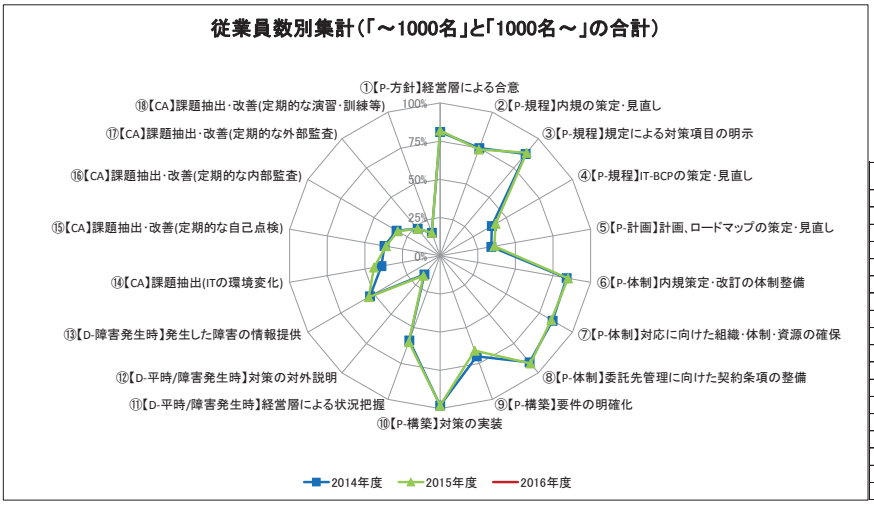


項目	2014年度	2015年度
①	91%	93%
②	95%	96%
③	95%	99%
④	61%	72%
⑤	56%	64%
⑥	98%	100%
⑦	94%	95%
⑧	98%	98%
⑨	95%	96%
⑩	100%	100%
⑪	70%	78%
⑫	31%	32%
⑬	78%	76%
⑭	70%	80%
⑮	59%	61%
⑯	51%	57%
⑰	33%	34%
⑱	54%	43%

※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、集計対象に含めず

調査結果　－　主要な基礎データ②

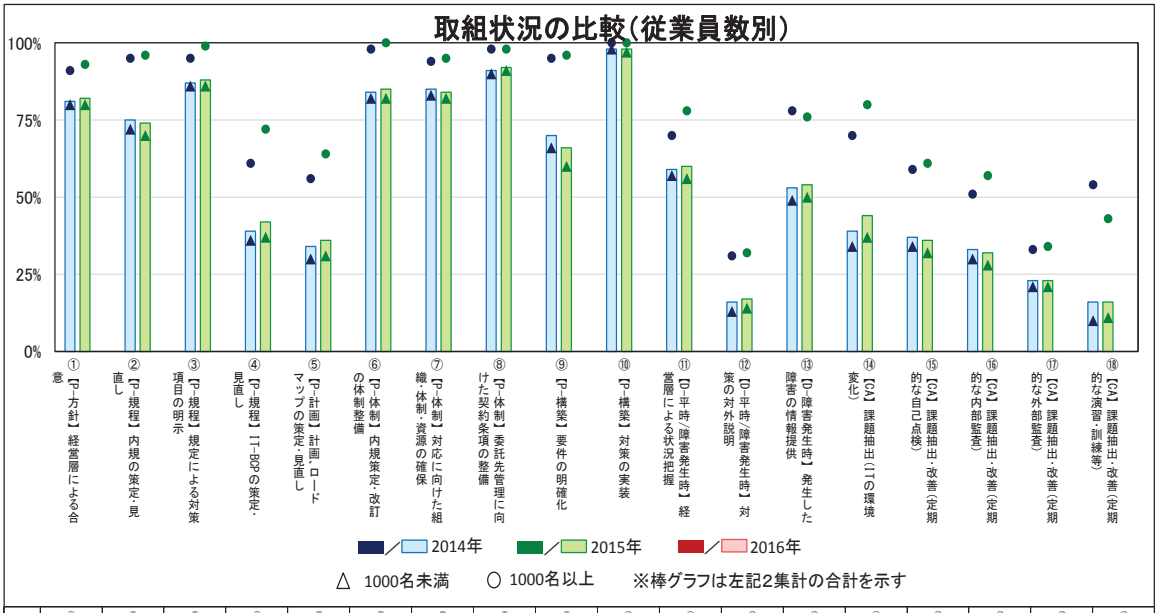
(1)　PDCAに沿った情報セキュリティ対策の取組（その4：従業員数別（1,000名未満と1,000名以上の合計））



項目	2014年度	2015年度
①	81%	82%
②	75%	74%
③	87%	88%
④	39%	42%
⑤	34%	36%
⑥	84%	85%
⑦	85%	84%
⑧	91%	92%
⑨	70%	66%
⑩	98%	98%
⑪	59%	60%
⑫	16%	17%
⑬	53%	54%
⑭	39%	44%
⑮	37%	36%
⑯	33%	32%
⑰	23%	23%
⑱	16%	16%

※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、集計対象に含めず

(1)　PDCAに沿った情報セキュリティ対策の取組（その５：従業員数別取組状況の比較）

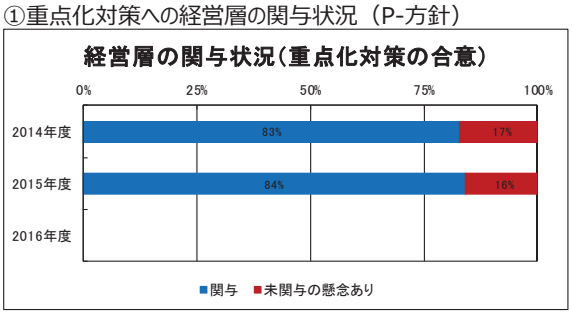


	①			②			③			④			⑤			⑥			⑦			⑧			⑨			⑩			⑪			⑫			⑬			⑭			⑮			⑯			⑰			⑱		
	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□	▲	●	□
2014年度	80%	91%	81%	72%	95%	75%	86%	95%	87%	36%	61%	39%	30%	56%	34%	82%	98%	84%	83%	94%	85%	90%	98%	91%	66%	95%	70%	98%	100%	98%	57%	70%	59%	13%	31%	16%	49%	78%	53%	34%	70%	39%	34%	59%	37%	30%	51%	33%	21%	33%	23%	10%	54%	16%
2015年度	80%	93%	82%	70%	96%	74%	86%	99%	88%	37%	72%	42%	31%	64%	36%	82%	100%	85%	82%	95%	84%	91%	98%	92%	60%	96%	66%	97%	100%	98%	56%	78%	60%	14%	32%	17%	50%	76%	54%	37%	80%	44%	32%	61%	36%	28%	57%	32%	21%	34%	23%	11%	43%	16%

※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、集計対象に含めず

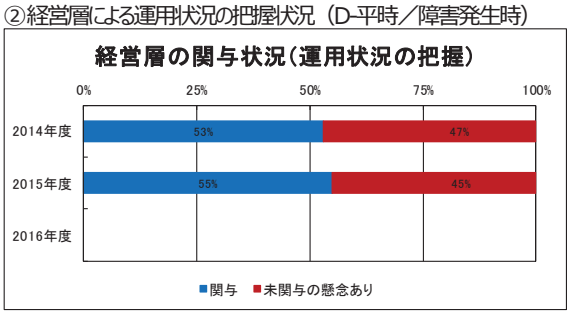
(2)　経営層の関与状況

①重点化対策への経営層の関与状況（P-方針）



※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

②経営層による運用状況の把握状況（D-平時／障害発生時）

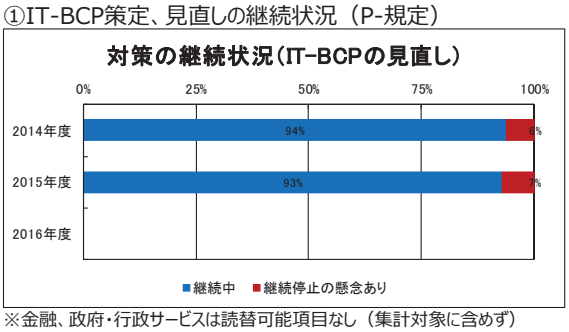


※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

調査結果　－　主要な基礎データ③

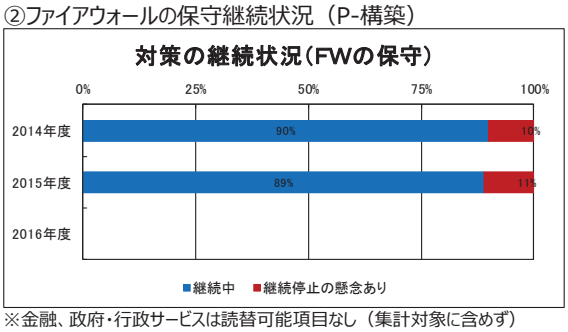
(3) 対策の継続状況

①IT-BCP策定、見直しの継続状況（P-規定）



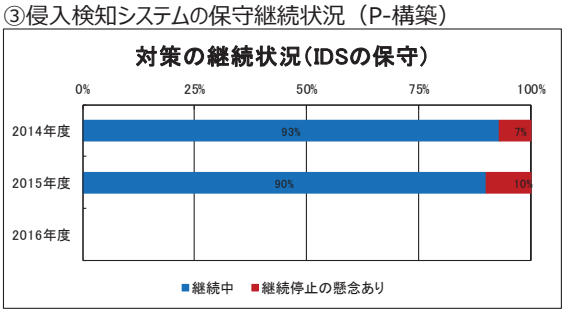
※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

②ファイアウォールの保守継続状況（P-構築）

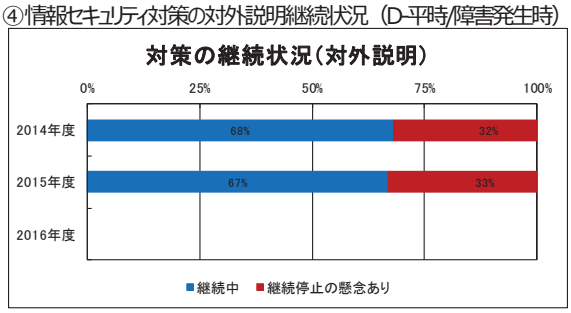


※金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

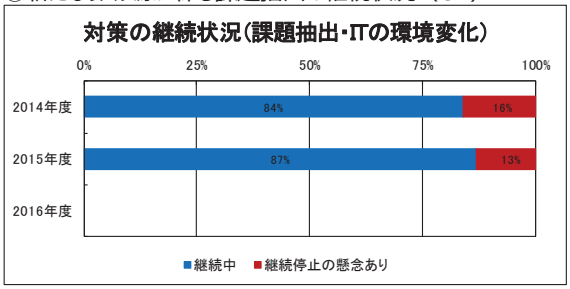
③侵入検知システムの保守継続状況（P-構築）



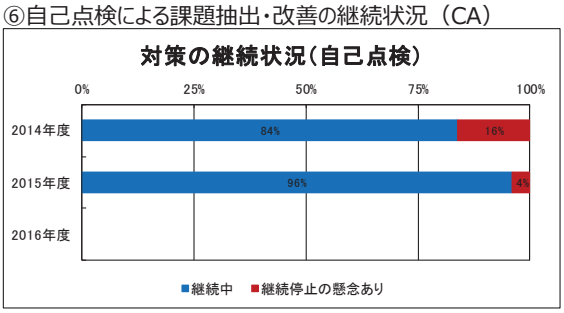
④情報セキュリティ対策の対外説明継続状況（D-平時/障害発生時）



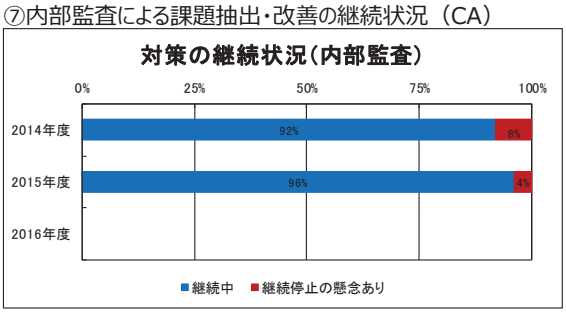
⑤新たなリスク源に係る課題抽出の継続状況（CA）



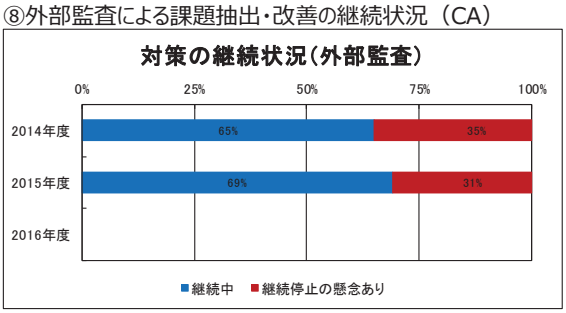
⑥自己点検による課題抽出・改善の継続状況（CA）



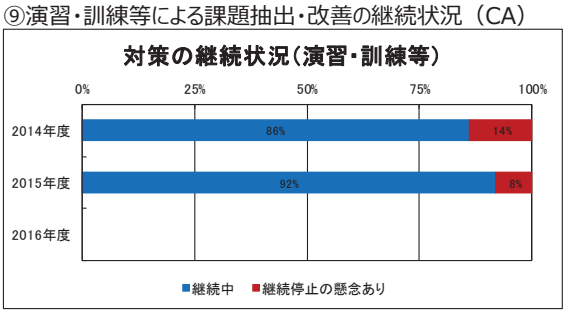
⑦内部監査による課題抽出・改善の継続状況（CA）



⑧外部監査による課題抽出・改善の継続状況（CA）



⑨演習・訓練等による課題抽出・改善の継続状況（CA）



調査結果詳細：(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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

指針_手引書新設後の初回調査。全て認知している事業者は4割強。2割強は全て認知していない状況。

（年度）	2014	2015	2016
全て知っている	－	43%	－
本編と対策編を知っている	63%	20%	－
本編と手引書を知っている	－	0%	
対策編と手引書を知っている	－	0%	
本編のみ知っている	13%	10%	－
対策編のみ知っている	1%	1%	－
手引書のみ知っている	－	3%	
両方とも知らない	23%	23%	－

(b)　指針（本編、対策編及び手引書）認知の契機（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

NISC、所管省庁、業界団体からの各紹介が同程度(4割程度)。この他には、Web検索が契機との回答が続く。

（年度）	2014	2015	2016
NISCからの紹介	43%	41%	－
所管省庁からの紹介	39%	45%	－
業界団体からの紹介	38%	40%	－
セミナー・シンポジウム等	8%	18%	－
ニュースサイト等	8%	8%	－
Web検索	34%	27%	－
その他	2%	5%	－

②　内規の策定・見直し

(a)　内規策定・見直しの契機（複数回答）

金融は読替可能項目なし（集計対象に含めず）

内規策定・見直しの契機は、自分野の安全基準等の策定・改訂、指針_本編・対策編の改訂、自社対策状況の課題抽出、他社から得た情報が同程度(5割程度)。
内規策定後に見直しを行っていない事業者も35%程度存在。

（年度）	2014	2015	2016
自分野の安全基準等の策定・改訂	52%	55%	－
本編や対策編の改訂	46%	48%	－
自社対策状況の課題抽出	53%	54%	－
他社等から得た情報	49%	49%	－
その他	11%	11%	－
見直しを行っていない	35%	34%	－
内規が未策定	4%	4%	－

(b)　内規における対策の規定状況（複数回答）

情報の取扱制限、可搬媒体の利用制限、不審メールへの対処など情報漏えい防止につながる対策を規定している割合が相対的に高い。

（年度）	2014	2015	2016
事業継続に必要な情報ｼｽﾃﾑの指定	44%	44%	－
情報システムの格付け	39%	38%	－
情報の格付け	49%	42%	－
情報の取扱制限	89%	90%	－
ソフトウェアの導入制限	74%	74%	－
不審メールへの対処	65%	65%	－
可搬媒体の利用制限	77%	71%	－
リモートアクセスの利用制限	55%	55%	－
スマートデバイスの利用ルール	40%	57%	－
外部委託先に求めるｾｷｭﾘﾃｨ対応	49%	58%	－
内規違反に対する罰則規定	44%	41%	－
上記はいずれも未策定	2%	3%	－

③　内規改定のプロセス

(a)　内規策定・改訂の体制（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

経営層が関わる割合は15%程度、情報セキュリティ委員会が関わる割合は4割弱、それ以外の体制が関わる割合が4割弱。
内規が未策定の事業者も15%程度存在。

（年度）	2014	2015	2016
経営層	16%	15%	－
情報セキュリティ委員会	32%	39%	－
上位以外の体制	38%	32%	－
内規が未策定	15%	14%	－

調査結果詳細：(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（複数回答）

金融は読替可能項目なし（集計対象に含めず）

**組織・体制・資源確保として、9割程度の事業者が担当者（兼任を含む）を割り当てている。
一方、専門部署を設置している事業者は3割強。**

（年度）	2014	2015	2016
CISO（兼任を含む）の割当て	20%	37%	－
専門部署の設置	31%	31%	－
担当者（兼任を含む）の割当て	91%	90%	－
人材育成、教育	65%	68%	－
上記はいずれも未対応	4%	5%	－

※(a)で「人材育成、教育」を選択した場合

(b)　情報セキュリティに係る教育テーマ（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

教育テーマの採用率については、各テーマとも昨年度と比して上昇。

（年度）	2014	2015	2016
情報の取扱制限	88%	91%	－
ソフトウェアの導入制限	77%	83%	－
不審メールへの対処	84%	89%	－
可搬媒体の利用制限	83%	88%	－
リモートアクセスの利用制限	54%	60%	－
スマートデバイスの利用ルール	53%	64%	－
その他	26%	22%	－
上記はいずれも未対象	1%	0%	－

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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

対策の計画／ロードマップの策定は45%程度の事業者が行っている。一方、35%程度の事業者は現時点で策定の予定もない。

（年度）	2014	2015	2016
両方とも行っている	31%	40%	－
策定のみ行っている	5%	5%	－
現時点では策定していない	2%	2%	－
策定中	13%	5%	－
策定予定がある	11%	11%	－
現時点では予定なし	38%	36%	－

(b)　情報セキュリティ対策の実装状況（複数回答）

多くの対策が7割以上の実施率ではあるが、重要データの暗号化、証跡管理、新たなリスク源への対策の実施率は3～5割程度。

（年度）	2014	2015	2016
サーバー室等の入退室管理	92%	93%	－
サーバー室等の停電対策	98%	97%	－
可搬媒体の持込み／持出し制限	79%	80%	－
リモートアクセス制限／利用可能端末の管理	75%	76%	－
ネットワークへの侵入防止	84%	82%	－
重要データへのアクセス制限	91%	91%	－
重要データのバックアップ	87%	96%	－
重要データの暗号化	36%	36%	－
無許可ソフトウェアの導入禁止	86%	86%	－
機器廃棄時のデータ消去	85%	94%	－
証跡管理	51%	52%	－
新たなリスク源への対策	29%	30%	－
その他	6%	8%	－
上記対策はいずれも未実施	2%	2%	－

※(b)で「ネットワークへの侵入防止」を選択した場合

(c)　具体的なネットワークへの侵入防止対策の実装状況（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

ネットワークの分離、ファイアウォールの設置（適用範囲の見直しを含む）の実施率が7～8割程度。

（年度）	2014	2015	2016
ネットワークの分離	84%	82%	－
FWの設置（適用範囲の見直しを含む）	76%	77%	－
FWの設置（適用範囲の見直しは除く）	16%	17%	－
IDSの導入（検知条件のチューニングを含む）	33%	36%	－
IDSの導入（検知条件のチューニングは除く）	5%	7%	－
その他	5%	5%	－

※(c)で「FWの設置（適用範囲の見直しは除く）」を選択した場合

(d)　FWの適用範囲を見直していない理由（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

ファイアウォール導入前と前提・要件が同一との回答が4割強。対応優先順位が低いとの回答が35%程度。

（年度）	2014	2015	2016
FW導入時と前提・要件が同一	46%	41%	－
FW導入にて対策完了と認識	20%	19%	－
対応優先順位が低い	29%	35%	－
その他	5%	5%	－

※(c)で「IDSの導入（検知条件のチューニングは除く）」を選択した場合

(e)　IDSの検知条件をチューニングしていない理由（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

導入時から不都合がないとの回答と対応の優先順位が低いとの回答が共に35%程度。

（年度）	2014	2015	2016
IDS導入時から不都合がない	44%	34%	-
IDS導入にて対策完了と認識	15%	17%	-
対応の優先順位が低い	26%	36%	-
その他	15%	13%	-

※(b)で「新たなリスク源への対策」を選択した場合

(g)　具体的な新たなリスク源への対策（複数回答）

政府・行政サービスは読替可能項目なし（集計対象に含めず）

新たなリスク源として対策が行われているのは、標的型攻撃が9割で最多。以降、スマートデバイスのセキュリティ、制御システムを狙ったマルウェアが6割程度。

（年度）	2014	2015	2016
標的型攻撃（内部情報窃取等）	82%	90%	-
制御システムを狙ったマルウェア	57%	60%	-
暗号の危殆化	34%	35%	-
IPv6への移行	27%	23%	-
プロトコルの脆弱性	40%	40%	-
クラウドサービスのセキュリティ管理	51%	51%	-
スマートデバイスのセキュリティ	61%	66%	-
その他	14%	13%	-

(h)　経営層への報告対象（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

各状況とも、報告対象となっているのは概ね1～2割程度。また報告未実施の事業者が半数近くを占める。

（年度）	2014	2015	2016
セキュリティパッチの適用状況	14%	16%	-
パターンファイル更新状況	11%	12%	-
不審メールへの対処状況	21%	25%	-
可搬媒体の利用状況	16%	17%	-
リモートアクセスの利用状況	8%	10%	-
スマートデバイスの利用状況	10%	12%	-
外部委託先のセキュリティ対応状況	20%	21%	-
その他	21%	18%	-
報告未実施	47%	45%	-

※(b)で「無許可ソフトウェアの導入禁止」を選択した場合

(f)　具体的な無許可ソフトウェア導入禁止対策の実施状況（複数回答）

マルウェア対策ソフトの使用が95%程度で最多。これに可搬媒体の利用制限、リモートアクセスの利用制限が8割程度で続く。

（年度）	2014	2015	2016
セキュリティパッチの適用（1ヵ月以内）	64%	66%	-
セキュリティパッチの適用（1ヵ月超）	10%	11%	-
マルウェア対策ソフトの使用	96%	96%	-
パターンファイル更新（1週間以内）	78%	79%	-
パターンファイル更新（1週間超）	5%	6%	-
管理者権限IDの限定貸与	73%	72%	-
管理者権限ID貸与先の定期点検	43%	44%	-
Webサイトの閲覧制限	26%	44%	-
Webサイトの閲覧制限対象の定期点検	24%	39%	-
可搬媒体の利用制限	82%	84%	-
利用を許可した可搬媒体の管理	52%	60%	-
リモートアクセスの利用制限	75%	78%	-
リモートアクセスの利用状況管理	38%	52%	-
その他	8%	9%	-

③　要件の明確化

(a)　委託先との契約条項（複数回答）

95%程度の契約で機密保持・情報の目的外利用禁止の条項が設けられている。
一方、委託元と同レベルの対策実施、監査／訓練／演習への協力の条項が設けられているのは45%程度。

（年度）	2014	2015	2016
責任分界点・サービスレベルの明確化	76%	53%	-
機密保持・情報の目的外利用禁止	96%	95%	-
委託管理責任者の設置	55%	55%	-
委託元と同レベルの対策実施	41%	43%	-
再委託の制限	75%	64%	-
障害発生時の対応	64%	67%	-
監査/訓練/演習への協力	43%	45%	-
違約時の対処（損害賠償請求等）	75%	67%	-
上記はいずれも未締結	2%	2%	-

(b)　明確化済の情報セキュリティ対策要件（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

明確化済の情報セキュリティ対策要件については、事業者の65%程度が情報セキュリティ確保に必要な機能要件、5割強がリスク源への対応要件を挙げている。

（年度）	2014	2015	2016
情報セキュリティ確保に必要な機能要件	70%	66%	－
リスク源への対応要件	51%	43%	－
上記はいずれも要件の未明確化	28%	32%	－

※(b)で「リスク対応への要件」を選択した場合
(d)　対応を要する具体的なリスク源（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

対応を要する具体的なリスク源としては、セキュリティホール、マルウェア等の不正プログラムがいずれも9割程度で挙げられている。

（年度）	2014	2015	2016
セキュリティホール	92%	90%	－
マルウェア等の不正プログラム	94%	90%	－
その他	13%	15%	－

※(a)で「事業継続性確保」を選択した場合
(b)　想定する事業継続性を阻害するIT障害の原因（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

85%程度の事業者が自然災害を挙げ、以降75%程度の事業者がサイバー攻撃を、7割弱の事業者が物理的破壊、構築・保守のミスを挙げている。

（年度）	2014	2015	2016
サイバー攻撃	68%	75%	－
構築・保守のミス	68%	67%	－
物理的破壊	64%	68%	－
自然災害	83%	86%	－
疾病の流行によるオペレータ不足	29%	38%	－
その他	3%	3%	－

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（単一回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

45%程度の事業者が、事業継続計画を策定し、見直しを行っている。

（年度）	2014	2015	2016
策定済・定期的に見直し中	19%	17%	－
策定済・不定期に見直し中	26%	29%	－
策定済・現在は見直しをしていない	3%	4%	－
策定中	11%	10%	－
策定予定がある	15%	13%	－
策定を予定していない	26%	27%	－

※(b)で「情報セキュリティ確保に必要な機能要件」を選択した場合
(c)　具体的な情報セキュリティ確保に必要な機能要件（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

情報セキュリティ確保に必要な機能要件として、認証機能、アクセス制限機能、権限管理機能のいずれもが9割強で挙げられている。

（年度）	2014	2015	2016
認証機能	91%	91%	－
アクセス制御機能	91%	94%	－
権限管理機能	91%	91%	－
その他	8%	10%	－

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（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

情報漏えい防止対策が9割弱と最多。以降、事業継続性確保が75%程度で続く。

（年度）	2014	2015	2016
事業継続性確保	65%	75%	－
情報漏えい防止	84%	88%	－
外部委託の情報セキュリティ確保	57%	59%	－
新たなリスク源	33%	45%	－
その他	12%	12%	－
特になし	7%	6%	－

※(a)で「新たなリスク源」を選択した場合
(c)　ITの環境変化に伴う新たなリスク源（複数回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

9割強の事業者が標的型攻撃を挙げ、以降7割強の事業者がスマートデバイスのセキュリティ、65%程度の事業者が制御システムを狙ったマルウェアを挙げている。

（年度）	2014	2015	2016
標的型攻撃（内部情報窃取等）	80%	91%	－
制御システムを狙ったマルウェア	61%	65%	－
暗号の危殆化	33%	44%	－
IPv6への移行	23%	19%	－
プロトコルの脆弱性	32%	25%	－
クラウドサービスのセキュリティ管理	58%	47%	－
スマートデバイスのセキュリティ	69%	73%	－
その他	7%	4%	－

※(a)で「策定済・現在は見直しをしていない」を選択した場合
(b)　事業継続計画の見直しをしていない理由（単一回答）
金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

事業継続計画を策定したものの現在は見直しを行っていない理由としては、対応の優先順位が低いとの回答が約半数で最多。

（年度）	2014	2015	2016
評価・検証に基づき、見直し不要と判断	0%	3%	－
評価・検証は未実施も、見直し不要と判断	19%	27%	－
対応の優先順位が低い	62%	52%	－
その他	19%	18%	－

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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

情報セキュリティ対策の対外説明を行っている事業者は2割強。
説明予定のない事業者が6割弱。

（年度）	2014	2015	2016
定期的に説明	8%	8%	-
不定期に説明	15%	15%	-
現在は説明を未実施	11%	12%	-
説明予定	7%	7%	-
説明予定なし	58%	58%	-

※(a)で「定期的に説明」又は「不定期に説明」を選択した場合

(b)　情報セキュリティ対策の対外説明手段（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

対外説明手段としては、Webサイトが6割強。これに有価証券報告書が4割強で続く。

（年度）	2014	2015	2016
情報セキュリティ報告書	17%	14%	-
CSR報告書	13%	15%	-
有価証券報告書	42%	41%	-
ディスクロージャー資料	2%	4%	-
Webサイト	64%	61%	-
その他	54%	20%	-

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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

6割弱の事業者が、障害発生時の情報提供方策を明示済。

（年度）	2014	2015	2016
明示済	57%	57%	-
明示未済	43%	43%	-

※(a)で「明示済」を選択した場合

(b)　具体的な障害発生時の情報提供体制の有無（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

情報提供体制として、サービスの利用者向けと所管省庁向けが共に8割強、業界窓口向けが55%程度。

（年度）	2014	2015	2016
サービスの利用者向け	86%	83%	-
所管省庁向け	79%	83%	-
業界窓口向け	58%	56%	-
上記はいずれも体制なし	4%	4%	-

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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

新たなリスク源に係る課題抽出を行っている事業者は5割弱。
実施予定なしの事業者は25%程度。

（年度）	2014	2015	2016
定期的に実施	12%	12%	-
不定期に実施	33%	36%	-
現在は未実施	9%	7%	-
実施予定あり	20%	19%	-
実施予定なし	27%	26%	-

※(a)で「定期的に実施」又は「不定期に実施」を選択した場合

(b)　具体的な課題抽出対象のリスク源（複数回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

課題抽出対象とするリスク源は、標的型攻撃が85%程度。これにスマートデバイスのセキュリティ、クラウドサービスのセキュリティ管理が続く。

（年度）	2014	2015	2016
標的型攻撃（内部情報窃取等）	82%	85%	-
制御システムを狙ったマルウェア	43%	44%	-
暗号の危殆化	26%	42%	-
IPv6への移行	17%	18%	-
プロトコルの脆弱性	25%	41%	-
クラウドサービスのセキュリティ管理	60%	62%	-
スマートデバイスのセキュリティ	66%	66%	-
その他	14%	14%	-

調査結果詳細：(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（単一回答）

金融は読替可能項目なし（集計対象に含めず）

定期的な点検の実施状況は5割弱。定期的な点検に基づく課題抽出・改善の実施状況は3割強。

（年度）	2014	2015	2016
１度以上/１年以内の点検にて課題抽出・改善を実施	10%	14%	-
１度以上/２年以内の点検にて課題抽出・改善を実施	2%	2%	-
１度以上/２年超の点検にて課題抽出・改善を実施	19%	16%	-
定期的な点検のみ実施	17%	15%	-
不定期に実施の点検にて課題抽出・改善を実施	18%	19%	-
不定期な点検のみ実施	8%	8%	-
点検未実施	12%	3%	-
点検実施予定あり	6%	7%	-
点検実施予定なし	5%	6%	-

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（単一回答）

金融、政府・行政サービスは読替可能項目なし（集計対象に含めず）

定期的な演習・訓練等の実施状況は2割弱。定期的な実施に基づく課題抽出・改善の実施状況は15%程度。

（年度）	2014	2015	2016
１度以上/１年以内の演習・訓練等にて課題抽出・改善を実施	13%	14%	-
１度以上/２年以内の演習・訓練等にて課題抽出・改善を実施	2%	1%	-
１度以上/２年超の演習・訓練等にて課題抽出・改善を実施	1%	0%	-
定期的な演習・訓練等のみ実施	1%	3%	-
不定期に実施の演習・訓練等にて課題抽出・改善を実施	7%	9%	-
不定期な演習・訓練等のみ実施	4%	4%	-
現在演習・訓練等未実施	5%	3%	-
演習・訓練等実施予定あり	18%	18%	-
演習・訓練等実施予定なし	50%	48%	-

③　内部監査の実施

(a)　内部監査による課題抽出・改善状況（単一回答）

金融は読替可能項目なし（集計対象に含めず）

定期的な内部監査の実施状況は45%程度。定期的な内部監査に基づく課題抽出・改善の実施状況は3割強。

（年度）	2014	2015	2016
１度以上/１年以内の内部監査にて課題抽出・改善を実施	8%	9%	-
１度以上/２年以内の内部監査にて課題抽出・改善を実施	11%	10%	-
１度以上/２年超の内部監査にて課題抽出・改善を実施	16%	13%	-
定期的な内部監査のみ実施	13%	12%	-
不定期に実施の内部監査にて課題抽出・改善を実施	6%	8%	-
不定期な内部監査のみ実施	4%	3%	-
現在内部監査未実施	4%	2%	-
内部監査実施予定あり	5%	6%	-
内部監査実施予定なし	11%	13%	-

④　外部監査の実施

(a)　外部監査による課題抽出・改善状況（単一回答）

金融は読替可能項目なし（集計対象に含めず）

定期的な外部監査の実施状況は2割弱。定期的な外部監査に基づく課題抽出・改善の実施状況は15%程度。

（年度）	2014	2015	2016
１度以上/１年以内の外部監査にて課題抽出・改善を実施	5%	6%	-
１度以上/２年以内の外部監査にて課題抽出・改善を実施	3%	3%	-
１度以上/２年超の外部監査にて課題抽出・改善を実施	7%	5%	-
定期的な外部監査のみ実施	6%	5%	-
不定期に実施の外部監査にて課題抽出・改善を実施	4%	4%	-
不定期な外部監査のみ実施	1%	1%	-
現在外部監査未実施	14%	12%	-
外部監査実施予定あり	3%	3%	-
外部監査実施予定なし	16%	18%	-

調査結果詳細：自由意見

【国・政府に対する意見・要望等】

- 過去の事例をもとに必要性と効果について分かり易く説明することが必要と感じる
- 情報セキュリティ対策の向上に対しては、国の助成をお願いしたい。
- 情報セキュリティの相談窓口の設置をお願いしたい。
- セキュリティ対策の裏口をつくようなコンピュータウイルスが目立ってきたように思います。現在、コンピュータウイルスの対策はソフトウエア業界任せであり、真の脅威に積極的に取り組んでいるとは言い難いとの思いがいたします。真の脅威を未然に防ぐためにも国の研究機関なりが、重要なコンピュータウイルス対策を行うべきではないでしょうか。
- 政府が行っている情報セキュリティ対策の推進については理解しておりますが、一般企業（重要インフラであっても）でこれに追随できる対策を行えている所は少ないのではないかと思います。それぞれの企業の水準に合わせた、水準別対策などがあると、目標とし易いのではないかと思います。
- 情報セキュリティの分野は利益を生まないので、優先順位が低くなりがちです。いろんな意味での「負担」をできる限り少なく対応できるようサポートしてもらえることを望みます。
- 他の企業（団体）が講じている具体的なセキュリティ対策の情報を収集するための意見交換会を開催していただきたい。システム開発やセキュリティ対策などについては開発ベンダーとの協議でほぼ確定しますが、常にセキュリティ対策のレベル（金額面も含めて。）が課題となっています。既存システムも含めて様々な情報を収集できれば大変参考になります。
- 情報セキュリティ対策の重要性について広く認識されているかについて疑問がある。担当セクションが無い社もある。
- IT人材育成のための支援を重視して頂きたい。

【情報共有体制の推進に関する意見・要望等】

- 大規模なサイバー攻撃、セキュリティインシデント発生時の迅速な情報提供をお願いしたい。
- 緊急性が高いセキュリティ事故が発生した場合、即座に対策が出来るように早急な連絡（メール等）をお願いしたい。

【指針に関する意見】

- 所管省庁や業界団体による周知、広報活動、内容の説明がある定期的なセミナー開催を希望
- 経営層にも見ていただける様、また、手軽に見れる様、冊子での配布が効果的ではないか
- より普及や周知に向け要点のみが明確に記載された一般用のさらなる簡略版（パンフレット的なもの）を作ってみてはどうか
- 具体的な対策の例示、チェックシートなどがあるとさらに有意義なものになる
- 指針としては理解できるが、それを実現場に落としこむ作業が非常に大変。内容をより具体化する、個別の案件に対してのQ&A窓口を設置するなどの対応を希望
- 安全基準等は参考にしているが、日々変化する環境に対して見直しが追いついていないように感じる。ITが専門ではない事業分野においては、対策を最新に保つのが難しいので、事業分野に共通する留意点を専門的な立場から提示して頂きたい
- 各社にて自社システムの状況を考慮したセキュリティ対策等を講じているため、指針等による画一的なセキュリティ基準等は経済的にも負担が大きく、２重投資になる可能性も高い
- 監督官庁毎に明示される指針が異なる可能性も否定できないため、省庁間での連携をお願いしたい
- 今回のアンケートにて初めて内容を再確認した。今後の改訂においては変更箇所を知らせて欲しい
- 重要インフラ活動の担当者には、直接周知してほしい。今回の指針等は全く知らなかった

【安全基準等に関する意見】

- 事業者規模に分別した安全基準の基本要綱（雛形）を希望する
- 安全基準に則り対策を講じる必要性は非常に感じているが、そこまでなかなか実施できていないのが現状です。最低限取り組むべきものなどの具体例があれば示すことができないでしょうか

（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・改訂を行う際の体制をお知らせ下さい。[(1)③(a)]
(6)　内規改訂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。

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 計	FY27				
		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件	51件	97件	118件	135件	401件
関係省庁・関係機関からのNISCへの情報共有	27件	2件	10件	21件	19件	52件
NISCからの情報提供	38件	9件	14件	11件	10件	44件

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		事象の例	FY26 計	FY27				
				1Q	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	9件	4件	21件	28件	22件	75件
発生した事象	機密性を脅かす事象	情報の漏えい	9件	2件	7件	3件	3件	15件
	完全性を脅かす事象	情報の破壊	14件	8件	8件	17件	19件	52件
	可用性を脅かす事象	システム等の利用困難	38件	12件	19件	28件	27件	86件
	上記につながる事象	マルウェア等の感染	27件	14件	30件	23件	44件	111件
		不正コード等の実行	3件	1件	1件	2件	7件	11件
		システム等への侵入	12件	7件	6件	9件	5件	27件
		その他	12件	3件	5件	8件	8件	24件

上記事象における原因別類型は以下のとおり。（複数選択）

原因の類型	原　因	FY26 計	FY27				
			1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	6件	2件	19件	22件	40件	83件
	ユーザＩＤ等の偽り	7件	1件	3件	3件	1件	8件
	DoS攻撃等の大量アクセス	25件	3件	9件	20件	15件	47件
	情報の不正取得	13件	0件	4件	4件	0件	8件
	内部不正	0件	1件	1件	0件	0件	2件
	適切なシステム等運用の未実施	4件	5件	2件	1件	2件	10件
偶発的な原因	ユーザの操作ミス	0件	4件	2件	2件	2件	10件
	ユーザの管理ミス	2件	2件	2件	1件	0件	5件
	不審なファイルの実行	1件	3件	7件	9件	32件	51件
	不審なサイトの閲覧	1件	7件	16件	11件	15件	49件
	外部委託先の管理ミス	10件	2件	2件	7件	1件	12件
	機器等の故障	7件	4件	6件	5件	2件	17件
	システムの脆弱性	9件	6件	8件	10件	5件	29件
	他分野の障害からの波及	1件	0件	2件	0件	3件	5件
環境的な原因	災害や疾病等	0件	0件	0件	0件	0件	0件
その他の原因	その他	9件	3件	9件	5件	5件	22件
	不明	43件	14件	19件	29件	43件	105件

別添４－６　セプター概要

セプターカウンシル総会第８回会合（平成28年４月26日）公表資料、重要インフラ専門調査会第５回会合（平成28年３月25日）資料４（2015年度 セプターの活動状況について）等より

セプター及びセプターカウンシルの概要

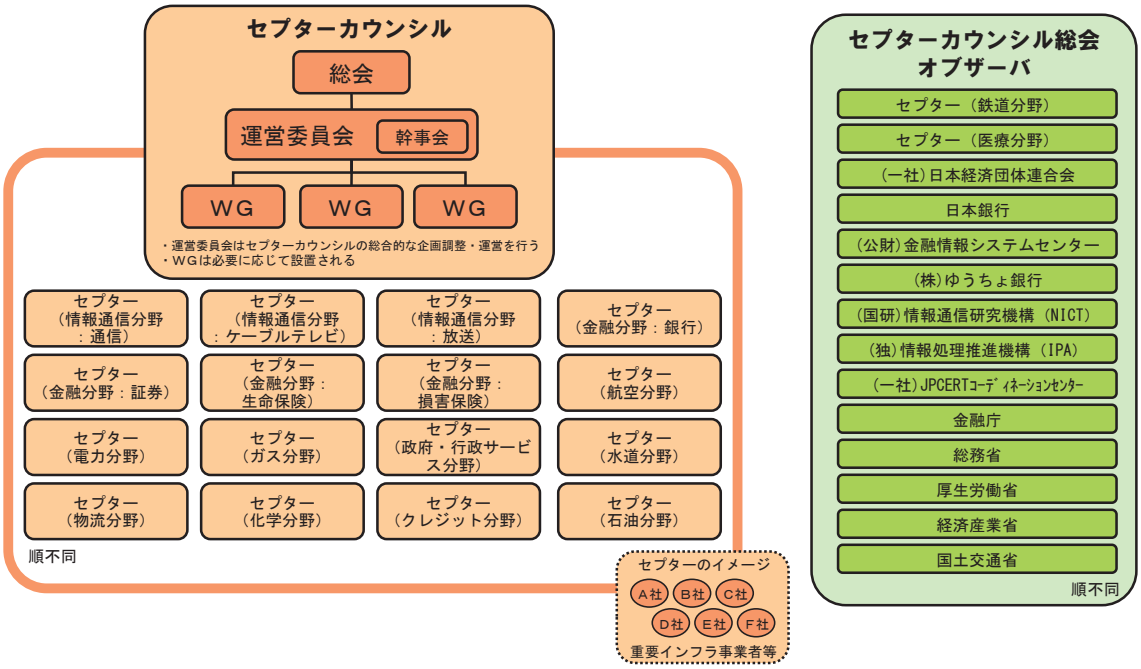
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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。
- IT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（2016 年４月 26 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。

セプター特性把握マップ

2016年3月末日現在

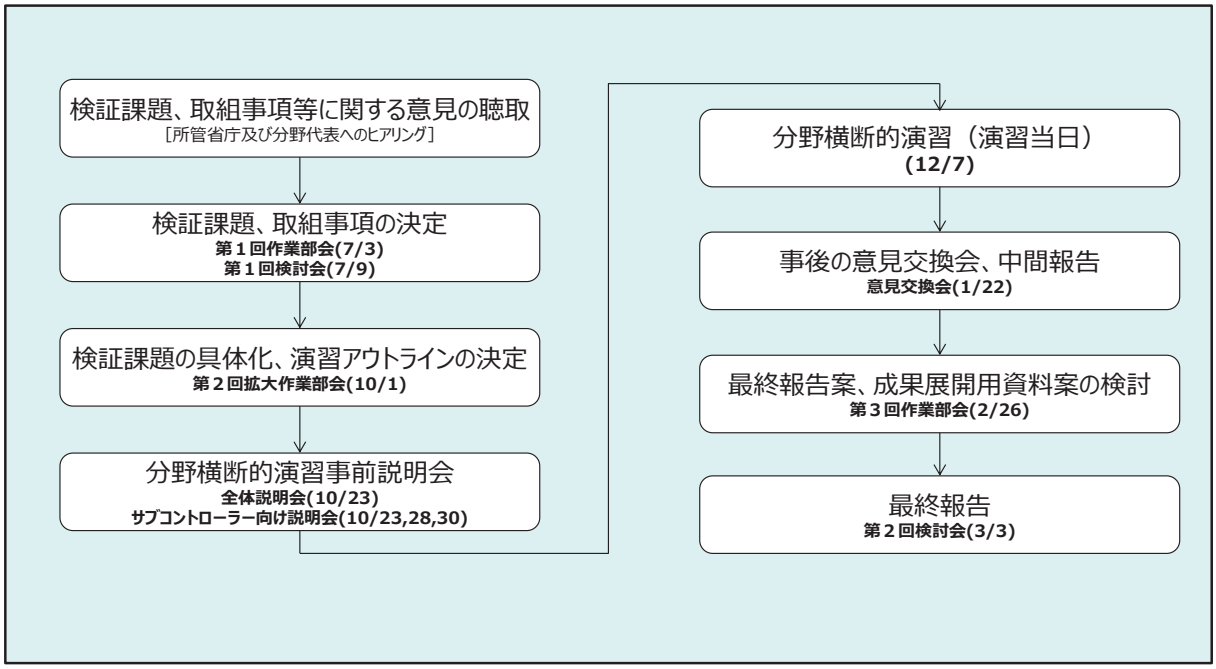
重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会 銀行等CEPTOAR	金融CEPTOAR連絡協議会 証券CEPTOAR	金融CEPTOAR連絡協議会 生命保険CEPTOAR	金融CEPTOAR連絡協議会 損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTAOR	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	(一財)日本データ通信協会 テレコム・アイザック推進会議	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務システム部	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推進部共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 総務課 危機管理室	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（内訳）	24社・団体 （固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等）	332社 （(一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者）	194社 1団体 （日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟）	1,446社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	256社 ７機関 （金融商品取引業者、取引所等証券関係機関）	41社 （(一社)生命保険協会の定款に定める社員および特別会員）	29社 （オブザーバ３社含む） （(一社)日本損害保険協会 情報システム委員会参加会社）	2グループ 3機関 （航空運送事業者、定期航空協会、官庁［航空局、気象庁］）	22社 1団体 1機関 （鉄道事業者22社、1団体、官庁［鉄道局］）	12社 2機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	10社 （主要な一般ガス事業者10社）	47 都道府県 1,741 市区町村	1グループ 6機関 （医療機関、(公社)日本医師会、四病院団体協議会（(一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会）、保健医療福祉情報システム工業会）	8水道 事業体 （会員水道事業体のうち会長都市並びに地方支部長都市） [補足]障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,361事業体)へ情報を提供	6団体 16社 （日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社）	11社 （主要な石油化学事業者）	18社 （主要なクレジットカード会社等）	14社 ・グループ （主要な石油精製・元売会社）
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年４月制定	2014年１２月制定
情報と連絡手段	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、ＷＥＢ	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、携帯、WEB	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	脆弱性に関する情報等 メール、電話携帯、FAX、電子会議室TV会議、会議体	障害事例 情報等 メール、電話、携帯、AX	障害事例 情報等 メール、電話、WEB	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話、携帯、FAX	障害事例 情報等 メール、電話、携帯電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話

（注）　本マップは、各セプターの自主的な整備状況を把握し、マップとして取り纏めたもの。

別添４－７　分野横断的演習

重要インフラ専門調査会第５回会合（平成28年３月25日）資料５（２０１５年度　分野横断的演習について）より

2015 年度分野横断的演習検討会　全体の流れ



2015 年度分野横断的演習　開催概要　～2006 年度より実施～

＜事前説明会＞
全体向け　：　２０１５年１０月２３日（金）
サブコン向け　：　２０１５年１０月２３日（金）、２８日（水）、３０日（金）
場　所　：　東京会場（全体向け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（第３次行動計画、情報共有体制）
②分野横断的演習の事前説明
③最新動向等についての有識者講演　等

規程類の事前確認、個別検証課題の確認・調整

＜演習当日＞
日　時　：２０１５年１２月７日（月）１２：１５～１８：１５
場　所　：東京会場、大阪会場、自職場
参加者　：３０２組織１，１６８名（うち、６６組織１４９名が大阪会場、
３６組織３１５名が自職場より参加。初参加事業者２０８組織）
【重要インフラ事業者等：１３分野　合計２７７機関】
【セプター：１３分野１８セプター】
【関係機関、分野横断的演習検討会有識者、政府機関　等】


演習の模様(遠藤大臣による視察)


全体振り返りの模様

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障害が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証。（標的型攻撃）
○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事態を想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。（ＤＤｏＳ攻撃、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

＜事後の意見交換会＞
日　時：２０１６年1月２２日（金）１４：００～１７：３０
場　所：東京会場、大阪会場
内　容：①分野をまたいだ事業者等間での情報共有（グループディスカッション）
②最新動向等についての有識者講演　等

他事業者等との情報共有を通じた改善の促進

2015 年度分野横断的演習　報告概要

取組にあたって

第３次行動計画　✓ 重要インフラ全体の防護能力の維持・向上を図る

分野横断的演習の基本方針

- ✓ 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

分野横断的演習の取組の方向性

- ✓ 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

2015年度の取組と今後の取組方針

2015年度の取組実績

- ✓ 演習当日及び前後の説明会・意見交換会等の充実
- ✓ 中堅・中小規模事業者の参加拡大と初心者向け見学会開催
- ✓ 情報共有体制やインシデント対応能力の実効性検証

取組実績等を通じて得た気づき等

- ✓ 年々高まるセキュリティ意識と対策とのギャップ認識の存在
- ✓ ＰＤＣＡサイクルを通じた継続的な訴求の必要性
- ✓ 演習取組全体に対するニーズと有益性の声
- ✓ 情報共有体制の誤認や課題の存在

今後の取組の観点

2015年度の基本方針・取組・演習運営を踏襲しつつ、以下観点の改善についても検討

- ✓ セキュリティ意識の高まりと旺盛な演習ニーズに応える会場新設や参加モデルに係る検討
- ✓ 各事業者のセキュリティ対策・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
- ✓ 分野横断的演習の運営ノウハウや知識等の還元に関する検討

分野横断的演習の取組の経緯

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 【机上演習】	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	重要インフラ複合障害	重要インフラ複合障害 ＋ 便乗型ＩＴインシデント	情報セキュリティインシデント

第３次行動計画　（2014年度～）

【目標】 重要インフラ全体の防護能力の維持向上を図る為、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確認等を通じた障害対応能力の向上を目指す

- ✓ 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**
人数	348名	**1168名**
テーマ	IT障害発生時の対応に関する事項を軸とし、情報共有体制を含む障害対応体制の実効性を検証	

分野横断的演習の基本方針とその骨格

第３次行動計画が目指す方向性

○ 分野内外の重要インフラ事業者等やサイバー空間関連事業者との依存関係が強くなる中、重要インフラ全体の防護には、全体の対策水準の底上げや関係主体間の連携の維持・強化が重要。

第３次行動計画において分野横断的演習で目指すこと

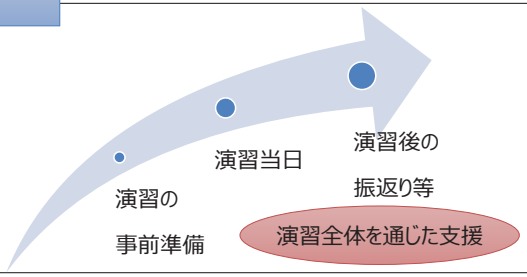
○ 重要インフラ全体の防護能力の維持・向上を図るため、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指す。
○ 国は、この取組が事業者等によって自律的かつ継続的に行われるよう支援。

分野横断的演習の骨格

○ 事業者等による実効性確認の機会としての演習当日に加え、事前準備及び事後の振り返りにて構成。

・演習当日は、日々の情報セキュリティに関する取組の実効性を確認するための１日でしかない。

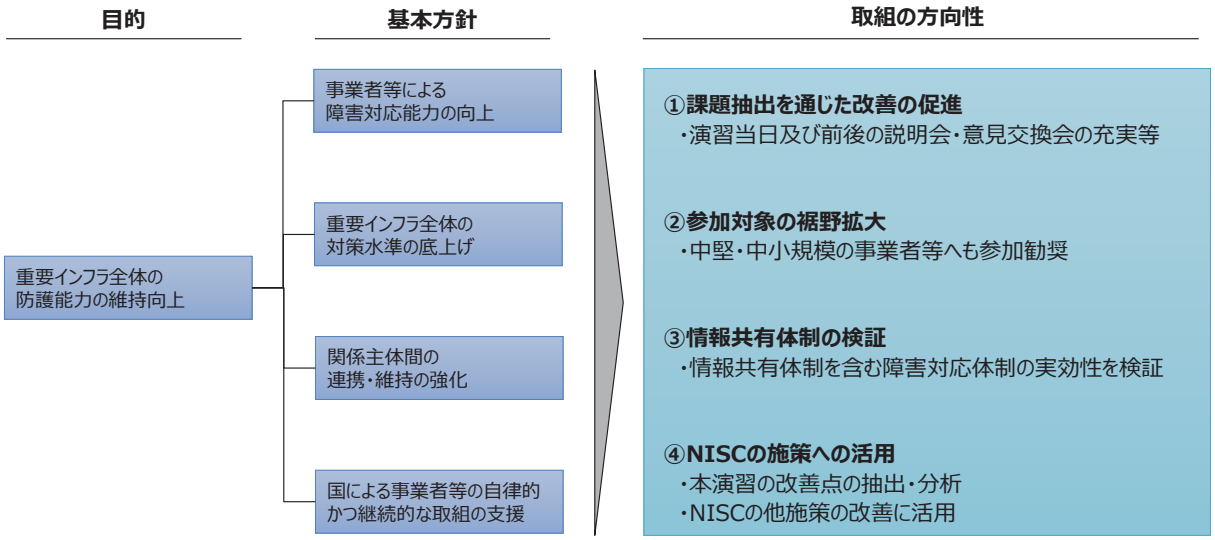
・演習の事前準備と事後の振返り等を通じて、事業者等が365日、対策を進めていくことを支援。



演習当日に参加することが重要ではなく、演習当日の気づきを基に、内規や体制をいかに改善できるかが重要。

分野横断的演習の基本方針に基づく取組の方向性

◆ ２０１４年度第１回検討会において、「基本方針」とそれに基づく４つの「取組の方向性」を決定。
◆ NISCは方向性①・②・③に基づいて実施した取組に対して、方向性④の観点から振返りを実施。



2015 年度の取組実績①

取組実績１：演習当日及び前後の説明会・意見交換会等の充実

事前準備

＜事前説明会＞
- ✓ 演習の検証課題を事前に示し、関連する規程の有無や対策状況の確認を促進
- ✓ 第３次行動計画、情報共有体制について説明を実施

＜サブコン説明会＞
- ✓ サブコンの目的/役割/作業タスクについて個別説明を実施
- ✓ 各事業者の実態に即した演習シナリオの策定や組織の現状把握を推進

＜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改善点を抽出

演習当日

＜演習取組＞
- ✓ 東京会場、大阪会場、自職場間で相互連携可能な演習実施環境を設営
- ✓ 演習時間、振り返り時間等を鑑みたタイムラインを確保
- ✓ サブコン中心による演習推進や振り返りリードを実施

＜見学会＞
- ✓ 演習参加を検討している事業者向けの見学会を実施

事後の振返り

＜意見交換会＞
- ✓ 東京会場、大阪会場にて事業者間のグループ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の意見交換や人脈形成を促進
- ✓ 「安全基準等」策定指針について説明を実施

2015 年度の取組実績②

取組実績２：中堅・中小規模事業者の参加拡大と初心者向け見学会開催

参加者裾野拡大を目指した参加勧奨

- ✓ 参加勧奨用のＤＶＤ動画の配布やYouTubeによる演習施策の報知
- ✓ 所管省庁、セプター事務局等を通じた中堅・小規模事業者への参加勧奨
- ✓ 演習結果や課題抽出をネガティブ化しないステークホルダー全体の演習意識の定着

	２０１３年度	２０１４年度	２０１５年度
参加機関	61組織 (38事業者等)	94組織 (70事業者等)	302組織 (277事業者等)
参加者	212名	348名	1,168名
（大阪会場）	－	10組織32名	66組織149名
（自職場参加）	3組織10名	15組織59名	36組織315名

※今年度演習初参加の事業者等は２０８組織

参加者層を意識した演習シナリオ設計

- ✓ 全参加者のレベルを意識したベースシナリオを策定
- ✓ 事業者のサービス実現方式を鑑みた複数シナリオを整備し、選択方式を採用
- ✓ シナリオの高度化や多様化の要素は、サブコンにてカスタマイズを行い柔軟に実現

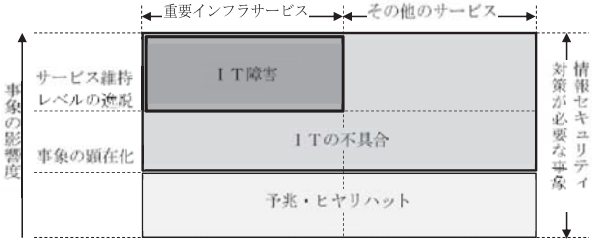
初心者向け見学会開催

- ✓ 演習参加にハードルを感じる事業者向けに演習会場を解放し見学会を開催
- ✓ 演習会場の雰囲気の把握や演習施策内容の理解浸透を促進
- ✓ 来年度の参加検討に向けた土台を形成

2015 年度の取組実績③

取組実績３：情報共有体制やインシデント対応能力の実効性検証

■ ２０１５年度の検証課題
- ✓ ＩＴ障害時の対応を軸とし、情報共有体制を含む障害対応体制の実効性を検証
- ✓ 情報共有の対象範囲が、ＩＴ障害だけでなく、ITの不具合や予兆・ヒヤリハットも含まれる点について実効性を検証



（上図）情報共有の対象範囲（第３次行動計画 P45）

＜振返りシートから抽出した気付き・課題＞

◆ ＩＴ障害等における対外的な情報共有
- ✓ 所管省庁への情報連絡の内容、タイミング、基準が曖昧であり今後整備が必要
- ✓ 官民間の情報共有は、ＩＴ障害の未然防止、拡大防止、迅速な原因究明などに効果がある
- ✓ 自組織外からの情報収集や対外的な情報発信については、体制・ルールに一部課題がある

◆ ＩＴ障害等の対応における内部的な判断や意思決定
- ✓ ＢＣＰは策定しているが、セキュリティインシデントを対象としたＢＣＰは策定出来ていない
- ✓ 緊急時に迅速に判断出来るよう、社内へ対応ルールを周知徹底する必要がある
- ✓ 緊急時における判断や対応は、継続的な訓練や演習が重要

実績まとめ

１．事前の取組

①スケジュール設計

サブコントローラの役割が正しく機能する事前準備が演習の肝となっていたが、準備期間/説明イベントを充実したことや、各事業者の演習理解度や前向きな姿勢により、予定通りの演習が推進された。

②検証課題の設計

演習で検証出来なかった課題として、「他事業者等（分野内・分野間）との情報共有」が挙げられた。（回答の２３％）

「情報共有アクション」が、検証出来なかった主な理由は以下が推測される。

○個社毎のシナリオ作成により、「官民の情報共有体制の検証」と、「事業者内部の対応」に重点が置かれた為。

○他事業者等（分野内・分野間）の情報共有ルール、体制が不十分な為。

○業法等の定めが無い事象に関する官民間の情報共有について基準不明確とする意見や誤認が存在する為。

⇒ 縦／横の情報共有体制の実効性検証について継続的な取組が必要。

２．演習当日

演習会場、自職場のそれぞれのメリット/デメリットに関する意見が寄せられた。

⇒ 演習参加者のそれぞれ異なるニーズにマッチする柔軟な参加モデルが必要。

３．事後の意見交換会

事後の意見交換会では、自由に意見交換できる環境づくりを行うことで、活発に情報共有・意見交換が行われ、事業者間のネットワーク形成に資することができた。

⇒ 他事業者のセキュリティ対策に関する考え方、ルール、設計等の情報を得られる場は、参加者にとって非常に貴重であり、継続的な取組が必要。

取組実績等を通じて得られた気付きと今後の取組の観点①

アンケート、振り返りシート等による得られた内容	取組実績等を通じて得た気づき等
✓ 2014年フォローアップアンケートの結果、約90.2%の事業者が、演習により課題抽出出来たと回答。 ✓ 19.1%の事業者が、「リソース不足」等を理由に改善に取組めていない。 ✓ 23.5%の事業者がセキュリティインシデントを経験	◆ 各参加事業者においてセキュリティ意識は、年々高まっているが、現状の対策については課題が残存。その対策に対しては、リソース等の問題により、ギャップが存在。
	◆ 事業者へのＰＤＣＡサイクルを通じた継続的な訴求の必要性
✓ アンケートの結果、99%の事業者が演習が有益であったと回答。 ✓ サブコントローラ施策により39%の事業者が演習が円滑に進行したという意見 ✓ 緊急時の対応には継続的な演習が必要という振り返りシートの声 ✓ 2015年度演習では、重要インフラ事業者以外からの演習参加希望や見学希望の声があり、個別に対応	◆ 本演習の有益性や必要性については、参加者から高評価を得ている。さらなる演習ニーズに対し応える必要がある。
✓ アンケートの結果、検証出来なかった項目の23.1%が他事業者（分野内や分野間）との情報共有を挙げている。 ✓ 行動記録メモ／メール内容の分析の結果、縦の情報共有のルート誤りが存在	◆ 官民間の情報共有体制について誤認が存在する。また、横の情報共有に関する課題が存在する。

取組実績等を通じて得られた気付きと今後の取組の観点②

取組実績等を通じて得た気づき等

- ■ 年々高まるセキュリティ意識と対策とのギャップ認識の存在
- ■ ＰＤＣＡサイクルを通じた継続的な訴求の必要性
- ■ 演習取組全体に対するニーズと有益性の声
- ■ 情報共有体制の誤認や課題の存在

今後の取組の観点

２０１５年度の基本方針／取組／演習運営を踏襲しつつ、さらなる改善について検討を行う。

- ➢ セキュリティ意識の高まりと旺盛なニーズに応える会場新設や参加モデルに係る検討
  - （例） □ 九州会場の新設
  - □ 会場/自職場/両立等の参加モデル
  - □ 他サイバー演習の運営ノウハウの取り込み
- ➢ 各事業者のセキュリティ対策・ＰＤＣＡに資する演習運営の検討
  - （例） □ サブコン施策による教育、スキル継承
  - □ 経営理解の増進
  - □ CSIRT能力向上
- ➢ 情報共有体制の実効性向上に係る施策の検討
  - （例） □ 金融ＩＳＡＣ、Telecom-ISAC等との演習連携強化
  - □ 分野内外の情報共有を促すシナリオ設計
- ➢ 分野横断的演習の運営ノウハウや知識等の還元に関する検討
  - （例） □ E-learning等の仮想演習環境の導入
  - □ 国際連携（海外組織との連携強化）

別添４－８　セプター訓練

重要インフラ専門調査会第５回会合（平成28年３月25日）資料６（2015年度 セプター訓練について）より

セプター訓練（第 10 回）の概要

訓練の概要

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』において、内閣官房（NISC）が、定期的及びセプターの求めに応じ、セプターの情報疎通機能の確認等の機会を提供するものとして位置付け。

また、各重要インフラ分野内における『縦』の情報共有体制の確認・強化を図るセプター訓練と、重要インフラ分野間の『横』の情報共有体制の確認・強化を図る分野横断的演習とが相互に連携・補完することで、『縦』方向と『横』方向双方の情報共有体制を強化し、官民連携による重要インフラ防護の推進を図るもの。

①目的

(1) 関係主体間の情報疎通機能確認を通じた情報共有体制の実効性検証と、重要インフラ防護能力の維持・向上
(2) 各主体、各経路における既存の手順等の改善、解決すべき課題の抽出

②参加者

情報通信分野（電気通信、放送、ケーブルテレビ）、金融分野（銀行等、生命保険、損害保険、証券）、航空分野、鉄道分野、電力分野、ガス分野、政府・行政サービス分野、医療分野、水道分野、物流分野、化学分野、クレジット分野、石油分野の計１８セプター
参加事業者等（参加事業者等数：1,658団体）
金融庁、総務省、厚生労働省、経済産業省、国土交通省、NISC

③実施期間

2015年８月から11月まで（実施日時はセプターごとに決定）

④実施内容（基本的な訓練の流れ）

(1)電子メールにて、NISCから所管省庁経由で各セプターに情報提供を発出。
(2)各セプターは、参加事業者等に対し情報提供及び参加事業者等の受信確認を実施し、所管省庁経由でNISCへ報告。
(3)訓練実施後、得られた気付き・課題等を調査票（アンケート）に記載し提出。

今年度のセプター訓練（第 10 回）の特徴

１．全てのセプター(18セプター)における訓練の実施

※２０１４年度セプター訓練は、１４セプターのみ実施。

２．IT障害対応を念頭においた実態に即した訓練の実施

①抜き打ちによる訓練の実施

(1)実施日時を指定しない訓練（５セプター）
(2)実施日のみ指定し、時刻は指定しない訓練（６セプター）
※２０１４年度、抜き打ちによる訓練は、１セプター（実施日のみ指定し、時刻は指定しない訓練）のみ実施。

②各分野の個別課題や要望等を踏まえた訓練の実施

(1)電話及びFAXのみの訓練（電子メールが使用できないことを想定）
(2)仮想事業者からの情報連絡を踏まえたNISCからの情報提供訓練（情報連絡への習熟を意図）　等

３．昨年度の訓練結果により得られた気付き等の検証及び分野横断的演習との連携

①昨年度の訓練結果により得られた気付き等の検証

情報伝達ツール（共有システム）に支障が発生した場合の代替手段の検証　等
※２０１４年度訓練では、訓練実施中に情報伝達ツールのIT障害が発生。その結果得られた気付き（代替手段の検討・整備等を実施）

②分野横断的演習との連携

NISCから訓練の模擬情報を展開する際、添付資料として情報共有体制の理解・浸透のための参考資料を送付
※２０１４年度分野横断的演習にて得られた気付き（情報共有体制の誤認を思わせる意見多数有り）

セプターの情報共有体制の状況（事前アンケート調査結果より）

1. 夜間・休日において情報提供できる体制になっているか。

① 情報提供できる（6セプター）
② 情報提供できない（9セプター）
③ その他（4セプター）

主なコメント等
・個人所有の携帯電話の情報をリスト化して共有している
・できる事業者とできない事業者がある
・連絡体制上は夜間・休日の対応が可能だが、訓練は不可　等

2. セプター事務局とセプター構成員との間、情報共有に係る取り決めを定めた文書（情報共有するための様式や重要度による情報共有範囲の設定等）等を整備していますか。

① 整備している（11セプター）
② 整備していない（6セプター）
③ その他（1セプター）

主なコメント等
・情報提供の様式は原則、NISCの様式を使用している　等

3. セプター構成員に対する情報共有への理解・浸透策について、実施しているものはありますか。

①特に実施していない （9セプター）
②定期的に説明会を実施 （1セプター）
③人事異動の際、新任者に対し取り決め文書等を配布 （1セプター）
④定期的に関係者に対し取り決め文書等を配布 （3セプター）
⑤その他（6セプター）

主なコメント等
・会員事業者向けHPにより関連文書の掲載・情報提供を実施
・定期的に意見交換会を実施
・制度改正時等に関連文書を送付　等

4. セプター訓練以外に、セプター内において、独自の情報疎通確認訓練を実施していますか。

①特に実施していない （15セプター）
②年1回実施している （2セプター）
③年2回以上実施している（0セプター）
④その他（1セプター）

主なコメント等
・地震等により応急支援が必要な場合に備え、衛星電話による連絡網を設置しており、毎月、伝達訓練を実施している　等

セプター訓練の結果①（情報受信確認状況等（総括））

参加者全てに受信確認できた	12 セプター	全ての参加者には確認できなかった	6 セプター
内訳（到達状況）		内訳（受信確認率）	
セプターから送信後～30分	1セプター	91%以上	1セプター
セプターから送信後～1時間	1セプター	81%以上90%以下	2セプター
セプターから送信後～3時間	3セプター	71%以上80%以下	1セプター
セプターから送信後～当日	3セプター	61%以上70%以下	2セプター
セプターから送信後～二日目	3セプター		
セプターから送信後～三日目	1セプター		

セプター訓練の結果②（訓練実施後のアンケート調査結果より）

1．前回（第9回）の訓練で得られた気付き・課題等について、今回の訓練で検証することが出来たか。

① **検証することが出来た**（8セプター）
主な内容
・ 代替手段による情報提供
・ 登録連絡先の複数線化（モバイルメールアドレス） 等

② **検証することが出来なかった**（6セプター）
主な内容
・ 前回の訓練で、気付き・課題なし
・ 連絡体制が課題であったが、組織変更により体制変更になったため 等

③ **前回の訓練に参加していない**（4セプター）

2．今回のセプター訓練の結果を踏まえ、どのような気付き・課題等があったか。

① **連絡手段（メール・電話等）**（7セプター）
主な内容
・ モバイルメールアドレスへの配信の必要性
・ メール・FAXによる連絡の他、電話による受信確認の必要性
・ 高負荷に耐えられる新たな配信ツールへの移行 等

② **連絡先の整備**（5セプター）
主な内容
・ 人事異動等の際の連絡先の確認
・ 各部署3名以上選任し、人事異動の都度見直しを実施 等

③ **代替手段及び連携ルート**（5セプター）
主な内容
・ 電話・FAXの必要性 等

④ **情報提供の迅速性**（4セプター）
主な内容
・ 緊急用携帯アドレスを含めることの必要性
・ 常に受信を意識してもらえるよう配慮 等

⑤ **情報共有の取り決め及び周知・浸透**（2セプター）

⑥ **その他、訓練全般**（5セプター）
主な内容
・ 訓練参加事業者の拡大
・ 情報伝達の中継点が多く正しく情報が伝達しているか 等

⑦ **特になし**（3セプター）

セプター訓練の結果③（訓練実施後のアンケート調査結果より）

3．現状の情報共有の課題を感じている点はあるか。あれば検討の方向性について聞かせてください。

① **突発的な対応が発生した際、事業者が情報を迅速かつ確実には受信できない可能性がある。**
・特に課題と感じている点はない（11セプター）
・中長期的な課題として検討（7セプター）
主な内容
・ 平時用と緊急時用の配信リストの設定及び別の伝達手段の設定
・ 迅速な登録情報の変更手続の周知徹底
・ 勤務時間外の体制の検討及びモバイル配信手段の検討 等

② **主たる担当が不在の際、事業者が情報を確実には受信できない可能性がある。**
・特に課題と感じている点はない（12セプター）
・分野横断的演習までに検討（1セプター）
・中長期的な課題として検討（5セプター）
主な内容
・ 受信者の複数設定の検討 等

③ **情報の重要度により、事業者が共有範囲の違いを理解していない可能性がある。**
・特に課題と感じている点はない（14セプター）
・中長期的な課題として検討（4セプター）
主な内容
・ 基本的に「特定分野・関係者限り」の情報の扱いとなるが、案件毎に事業者のプレス発表のタイミングと兼ね合いの検討が必要 等

④ **夜間・休日において、事業者が情報を確実には受信できない可能性がある。**
・特に課題と感じている点はない（7セプター）
・中長期的な課題として検討（11セプター）
主な内容
・ 確実に受信確認を行えるのが平日の日中に限られるため、緊急時の体制・手法等の検討 等

⑤ **事業者が、情報共有のルール等に習熟していない可能性がある。**
・特に課題と感じている点はない（12セプター）
・分野横断的演習までに検討（1セプター）
主な内容
・ セプター事務局にて内規を見直し、事業者へ再周知 等

・中長期的な課題として検討（5セプター）
主な内容
・ 情報セキュリティ対策に関する意識の徹底 等

セプター訓練の結果④（訓練実施後のアンケート調査結果より）

4. 訓練の感想及び意見等（セプター）

〇情報連絡の流れを確認でき、有益。

〇訓練を繰り返していくことが必要。

〇訓練実施日を明示しないことで、適切に情報把握が可能かどうかを検証できた。

〇訓練実施日時を明示しないことで実践的な訓練となり、改めて連絡体制を見直す良い機会となった。

〇緊急度が「緊急」の場合の情報共有ルートとして考えていたモバイル端末向けのメーリングリストは、情報の伝達に制約があることが浮き彫りになるなど、問題点の洗い出しができた。

〇緊急度が非常に高い情報を連携するのであれば、各セプターが個別に、メーリングリストや掲示板などの情報伝達システムを構築するのではなく、NISCにおいて情報伝達システムを構築し、直接事業者を登録するのがよいのではないか。

等

5. 訓練の感想及び意見等（所管省庁）

〇全事業者からの受信確認ができるよう、情報共有体制を見直しつつ、訓練を継続して実施していきたい。

〇セプター加盟事業者が大幅に増加しているので、情報セキュリティに対する意識向上に係る取組を一層進めていく必要性が感じられた。

〇訓練実施日を明示しなかったことで、各事業者が主担当者の不在時や夜間・休日時にいかに対応すべきか検討する良い機会となった。

〇より実践的な訓練を行うとの観点から、時間のみでなく、実施日も含めて、抜き打ちで実施する方向性が適当。

〇各関係者の協力が得られればの話であるが、訓練を業務時間外や休日に実施することも検討すべき。

〇連絡体制は、2団体を通して事業者に到達する体制となっており、伝達の寸断や遅れの原因になっていると推察するため、体制の見直しを検討する必要がある。

〇毎年行われるセプター訓練の結果について、評価をしていただき、他分野との比較などをしていただければ各分野の情報共有体制の改善につながるのではないか。

等

セプター訓練の総括及び今後の方向性

◆訓練の総括

① 各セプターにおいて、これまでの訓練参加実績、情報共有体制（構成員数、手段、伝達ルート等）状況及び訓練要望等を踏まえた訓練を実施することにより、**多くの気付きや課題等を得られたことで、訓練の有用性をあらためて確認**できた。

② アンケート調査の結果、**緊急時における情報共有の体制や手法等に課題を感じている**セプターが多く、各セプターにおいて中長期的な課題として検討すべきものと思料。

◆今後の方向性

① 重要インフラ防護能力の維持・向上のため、**定期的に訓練を実施することは重要**であり、NISCは引き続きその機会を提供。

② 今後のセプター訓練においても、**IT障害対応を念頭においた実態に即した情報共有訓練**となるよう、今回の訓練結果やセプターの情報共有体制の現状を考慮し、**セプター毎に、具体的な訓練内容を検討**していく。

別添４－９　補完調査

重要インフラ専門調査会第５回会合（平成28年３月25日）資料７（2015年度 重要インフラにおける補完調査について）より

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　DDoS攻撃によるサービス障害
事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い
事例３　USBメモリを介したマルウェア感染　※マルウェア･･･コンピュータウィルスなどの不正・悪質なソフトウェアの総称
事例４　Webサイトへの不正アクセス

事例１　DDoS 攻撃によるサービス障害①

【事例の概要】

- サービス提供WebサイトがDDoS攻撃を受け利用者がアクセスできない状態となった。
- データセンター事業者にてトラフィック制限を行う等の対応を実施した。
- 分野内での情報共有を行うとともに、利用者への周知を実施した。

【背景】

- サービス提供Webサイトを外部のクラウドサービスを利用して構築。
- 告知用Webサイトは災害対応等を考慮し、別のデータセンターでも運用していた。

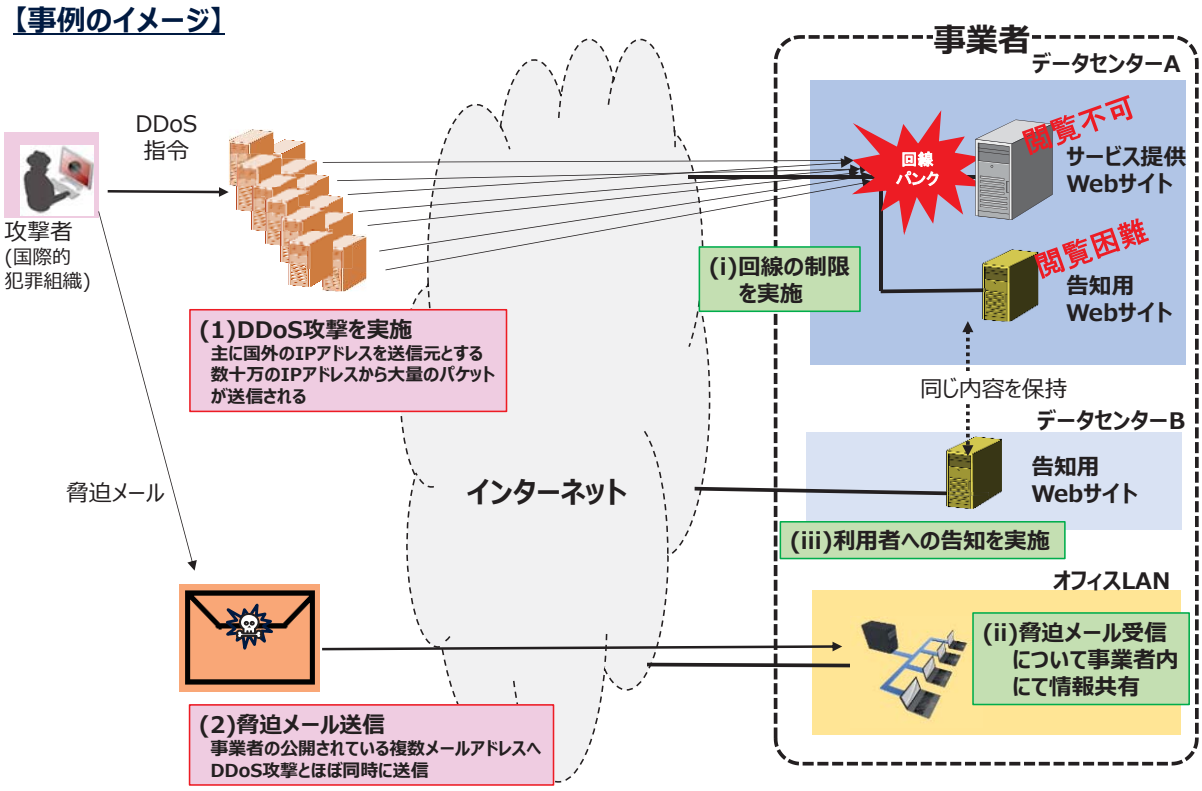
【検知】

- 監視担当部署でサービス提供Webサイトの異常を検知しDDoS攻撃と判断。
- 同時にインターネット上に公開されているメールアドレス宛に金銭を要求する脅迫メールが届き、その情報が事業者内で共有された。

【対処】

- データセンター事業者側にてアクセス制限を実施した。
- 告知用Webサイトには影響がなかったため、そちらを通じて利用者にサービス利用不可の状況と代替サービスの提供方法の案内を実施した。
- 分野内での情報共有を実施。同じような攻撃を受けたケースを参考に対応を検討した。

【事例のイメージ】



事例１　DDoS 攻撃によるサービス障害②

【原因】

- 国際的な犯罪組織によるDDoS攻撃により、平時の1000倍以上もの通信がありデータセンターの回線がパンクした。

（DDoS攻撃解除のために金銭を要求※。）
※要求通り金銭を支払っても攻撃がやまない場合が多い。

【再発防止策】

＜短期的対策＞

- データセンター事業者にてサービス提供に用いていない通信を遮断※した。
※攻撃に利用された通信がUDPパケットのみだったため、UDPパケットがサービス提供に利用されていないことを確認の上、データセンター事業者側でUDPパケットをカットすることにより通信を維持させた。

＜中長期的対策＞

- CDN※サービスを利用することにより大量の通信を処理できる環境を検討。
※ Contents Delivery Network:ウェブコンテンツの大量配信に最適化されたネットワーク。負荷分散以外にも不要な通信を遮断し、必要な通信のみを正規サイトに流すオプションメニューもある。
- DDoS攻撃対策を含むセキュリティに関する社内規程を追加準備中。
- 今後不審な通信を遮断できるよう、送信元の国単位やIPアドレスの範囲を指定した遮断など柔軟な通信遮断手順を検討。

【得られた気付き・教訓】

- データセンター事業者と連絡が取れるような体制の構築
（DDoS攻撃ではサーバーの負荷上昇に止まらず、データセンター事業者の回線をパンクさせる場合もあるため、データセンター事業者との連携体制を構築しておくことが重要。）
- 外部との積極的な情報共有
  - ✓ 外部との情報共有窓口の明確化
（分野内の情報共有により、攻撃者の傾向を知り迅速に対策を打つことができた。）
  - ✓ 周囲から情報を得るため、まずは自らの情報を発信
（事象発生時の情報発信について、予め経営層を含めたコンセンサスを得ておく。）
- サービス利用者への周知方法の確保
  - ✓ 告知手段の冗長化
（告知用Webサイトを複数データセンターで構築していたため、事象発生時も告知手段を確保できた。この他、電子メールやtwitter等も検討されていた。）
  - ✓ インシデント対応における広報担当者との連携
（対応チーム内に広報担当がいたおかげで、状況に応じ適切な告知手段を選択するなど、対外的な対応もスムースに行うことができた。）

事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い①

【事例の概要】

- 改ざんされたWebサイトにアクセスした事業者に対して、NISCから注意喚起を実施。
- 端末を特定し隔離するとともに、事業者全体のインターネット接続を遮断。
- 事業者のIT担当部署が調べたところ、Adobe Flash Playerが最新だったため感染はなかった。

【背景】

- 事業者内LAN及びインターネット接続の管理をIT担当部署が実施。
- 職員が業務上よく利用するWebサイトが改ざんされた。

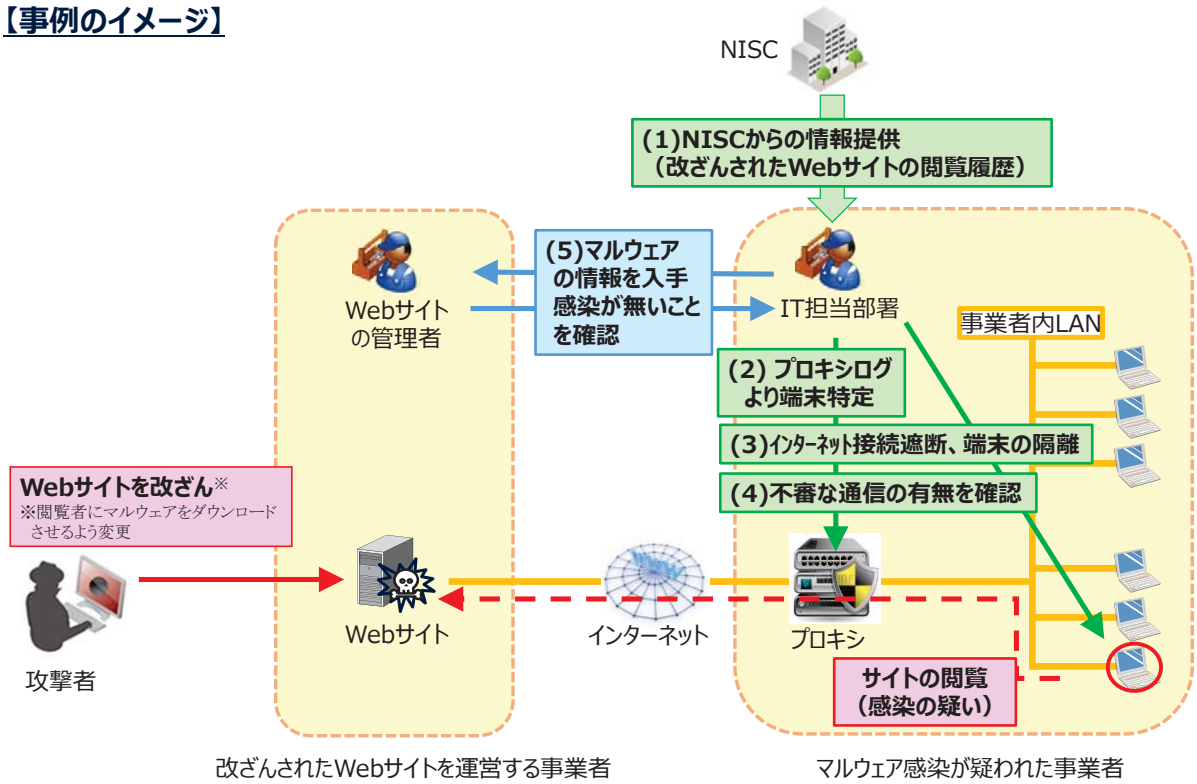
【検知】

- NISCからの所管省庁を通じた情報提供により、IT担当部署がマルウェア感染の疑いを認知。

【対処】

- 保守ベンダー※と連携し、情報提供の内容を元にプロキシログから感染の疑いがある端末を特定。
  ※事業者内LAN管理業務の委託先。契約時間外であったが、緊急時対応として対処。
- 該当端末を隔離するとともに、プロキシの停止によりインターネット接続を遮断※。
  ※インターネット接続の遮断についての権限はIT担当部署にあることが、規程に定められていた。
- プロキシログから該当端末が外部へ不審な通信をしていないことを確認。
- 改ざんされたWebサイトの管理者からマルウェアに関する情報※を入手し、マルウェア感染がないことを確認。
  ※マルウェアのファイル名、保存先、通信先情報等

【事例のイメージ】



事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い②

【原因】

- 事業者内LANに接続された端末が、改ざん※されたWebサイトにアクセスした。
  ※ブラウザのプラグイン（Adobe Flash Player）の脆弱性を利用しマルウェアに感染させる仕掛けが埋め込まれた。
- 端末のブラウザのプラグインは更新済みであったため、マルウェア感染はなかった。

【再発防止策】

＜短期的対策＞

- 業務上必要な場合を除き、該当のプラグインを原則使用禁止とした。
- やむを得ず使用する場合は常に最新版にアップデートするよう注意喚起を実施。

＜中長期的対策＞

- ネットワーク機器のログ監視・分析能力の強化策を検討。

【得られた気付き・教訓】

- 不要なブラウザのプラグインの使用禁止
  （一律禁止できない場合は、実行を制限するブラウザ設定等の導入も検討すべき。）
- 緊急時を考慮した規程類や判断基準等の事前確認・見直し
  （社内規程に従いIT担当部署の判断でインターネットを遮断できた。）
- 緊急時を考慮した保守体制の整備
  （事象発生直後から保守ベンダーと連携し迅速に対応できた。）
- プロキシログ等の調査手順の確認
  （プロキシログの調査手順を知っていたため、端末を迅速に特定できた。）
- インターネット接続の遮断等についての具体的手順の確認
  （プロキシを停止したことにより必要な通信も遮断されてしまった。）
- 能動的な情報収集と対策への活用
  （配信されたマルウェアの情報を入手することで、感染がないことを確認できた。）

事例３　USB メモリを介したマルウェア感染①

【事例の概要】

- スタンドアローン※で運用中のPCにおけるマルウェア感染が発覚。
- PC間のデータ交換のために、USBメモリを日常的に使用しており、それを介して感染が拡大した。
- USBメモリを使用した全PCを特定し、ウイルス対策ソフトを用いて駆除。

※LAN等のネットワークに接続していない状態をいう。

【背景】

- 事業所内のほとんどのPCがスタンドアローンによる運用で、外部の事業者とのデータ交換、PC間のデータ交換、PCのソフトウェア更新に、それぞれ特定のUSBメモリを使用。
- USBメモリの使用は管理され、許可されていないUSBメモリの使用は許されていない。
- 業務要件によりウイルス対策ソフト等が導入できないPCも存在。

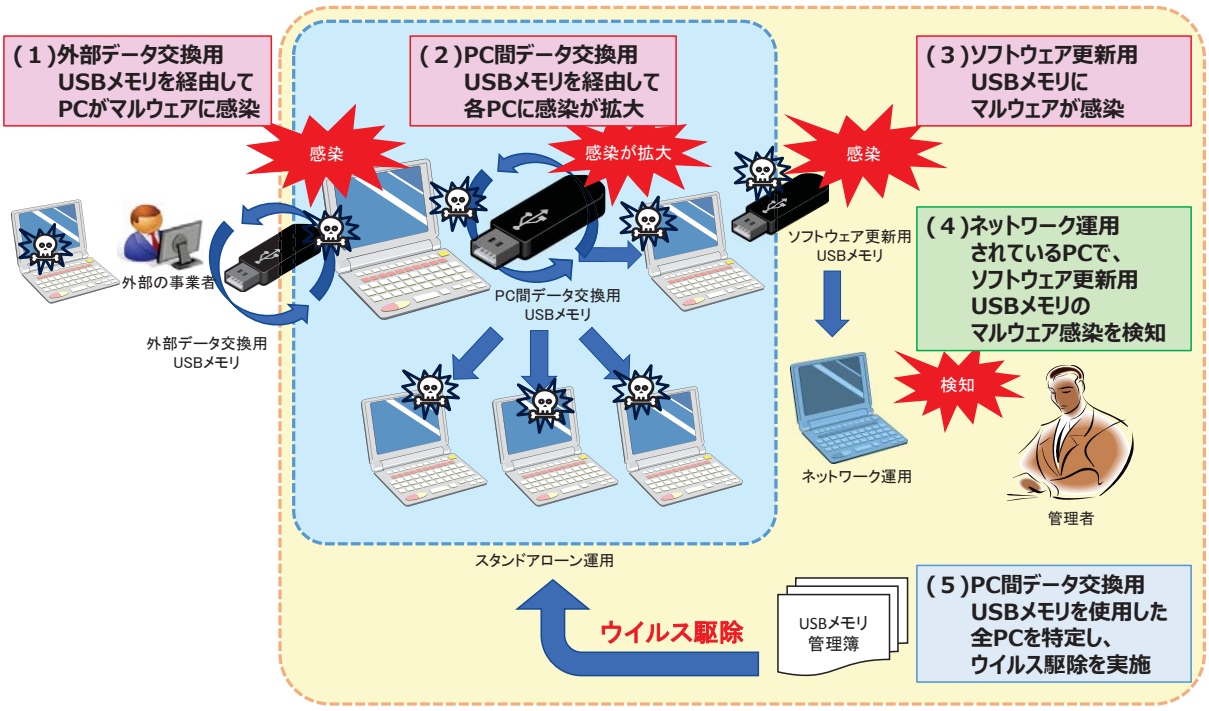
【検知】

- ソフトウェアの更新に用いていたUSBメモリをネットワーク運用されているPCに挿入した際、マルウェアを検知。

【対処】

- PC間のデータ交換用USBメモリを使用した全てのPCを特定。
- ウイルス対策ソフトが導入できるPCは、ウイルス対策ソフトを最新の状態にし、ウイルス駆除を実施。
- ウイルス対策ソフトが導入できないPCは、USBメモリ型のウイルス対策ソフトでウイルス駆除を実施。

【事例のイメージ】



事例３　USB メモリを介したマルウェア感染②

【原因】

- 過去に外部の事業者とUSBメモリを用いてデータ交換していたことから、そのUSBメモリを介してPCがマルウェア感染していたものと思われる。
- 上記PCから、組織内PC間のデータ交換に用いるUSBメモリを介して、他のPCへ更に感染が拡大したものと考えられる。

【再発防止策】

＜短期的対策＞

- ウイルス対策ソフトを導入できるPC

  USBメモリ等を用いて、定期的にウイルス定義ファイル等の更新を実施する。
- ウイルス対策ソフトを導入できないPC

  USBメモリ型のウイルス対策ソフトを用いて、定期的にウイルスチェックを実施する。

  USBメモリを用いて外部とデータ交換をする際は、事前に別のPCでウイルスチェックを実施する。

＜中長期的対策＞

- PCのネットワーク化及び管理サーバーの導入による手動更新の負担軽減などを検討している。

【得られた気付き・教訓】

- スタンドアローンで運用しているPCの把握と適切なセキュリティ対策の実施
  （スタンドアローンのPCもUSBメモリ等を介して、マルウェアに感染する可能性がある。）
- スタンドアローンで運用しているPCにおけるウイルス対策ソフト等のソフトウェアの最新化
  - ✓ ソフトウェア更新作業の組織的な運用計画の整備
    （人手を介した更新作業は運用負担が大きいため、場当たり的な対応では、作業の実施漏れや引継ぎ漏れ等により、更新されない状態が長く続いてしまう可能性がある。）
  - ✓ 業務要件によりウイルス対策ソフト等をインストールできないPCへの対策
    （USBメモリ型のウイルス対策ソフトを用いた対応も可能だが、運用負担軽減のための対策を別途検討する必要がある。）
- USBメモリ等外部記憶媒体の使用履歴の保持
  （履歴を元に感染の疑いのあるPCを特定し、調査対象範囲を絞ることができる。）

事例４　Web サイトへの不正アクセス①

【事例の概要】

- Webサイトへの不正アクセスにより、Web管理者情報の窃取やWebサイトの改ざんが発生。
- 事案の発生がNISC等から事業者に対して速やかに伝達され、被害を最小限に。
- Webサイトを一時閉鎖後、CMS※やレンタルサーバの脆弱性対策等を実施。

※Content Management System：Webサイト上のコンテンツを管理・編集するためのソフトウェア。

【背景】

- Webサイトのコンテンツ制作は外部業者に委託。
- Webサーバは外部のレンタルサーバを利用するが、日々の保守・運用は事業者自らが対応。

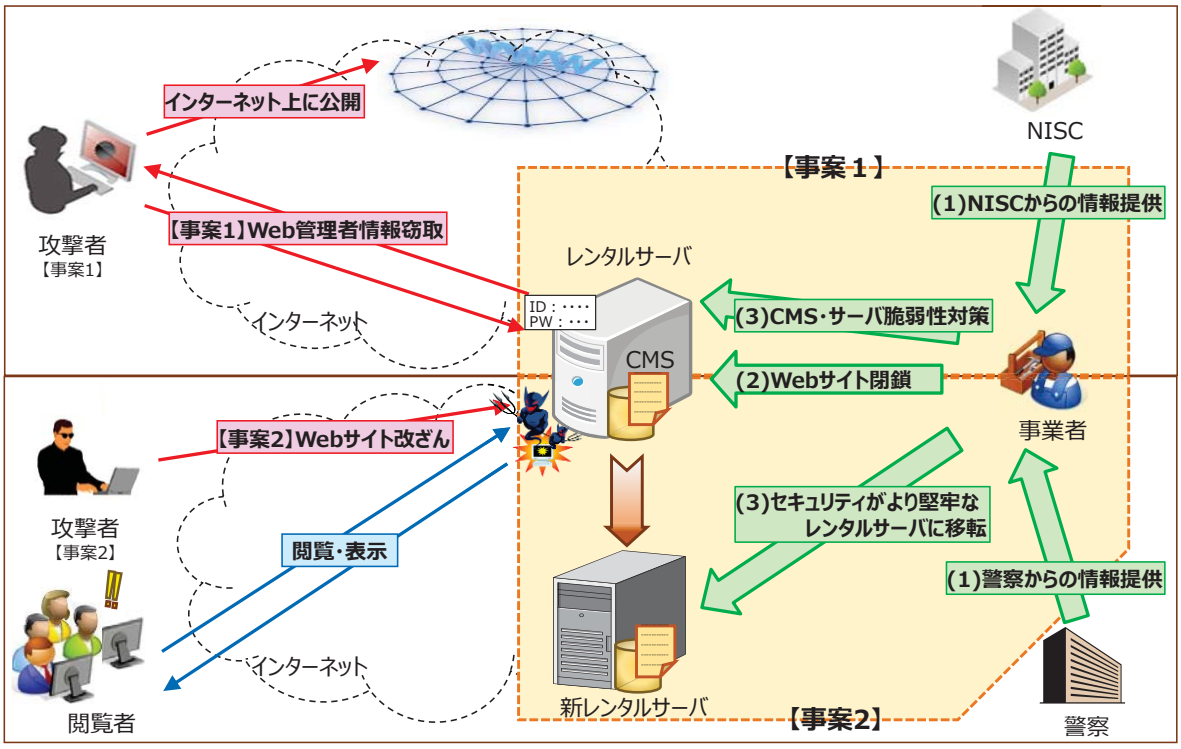
【検知】（事案2は事案1から約半年後に発生）

- 【事案１】NISC等からの情報提供により、IT担当部署の担当者がWeb管理者情報の窃取を認知。
- 【事案２】NISC等からの情報提供により、IT担当部署の担当者がWebサイトの改ざんを認知。

【対処】

- 【事案１/２】不正アクセスを認知後、事業者内セキュリティポリシーを踏まえ速やかに責任者に報告し、当日中にWebサイトを閉鎖。
- 【事案１】Web管理者情報を変更した上で、CMSやレンタルサーバの脆弱性対策を実施。
- 【事案２】Web管理者情報を変更した上で、セキュリティ向上を図るため別会社のレンタルサーバに移転。
- 【事案１/２】事案発生１週間以内にWebサイトを再開。

【事例のイメージ】



事例４　Web サイトへの不正アクセス②

【原因】

- 【事案１】使用していたCMSが汎用的なものでなく独自仕様なので安全といった誤解もあり、脆弱性対策が不十分であった。
- 【事案２】CMS管理外のWebサイトが改ざんされており、レンタルサーバのセキュリティに問題ありと推定。
- 【事案１/２】IT担当部署の職員数の不足もあり事案対応に追われ、対外機関との間での情報共有が必ずしも十分でなかった。

【再発防止策】

＜短期的対策＞

- 【事案１】CMSやレンタルサーバの脆弱性情報を常に把握し、速やかに更新。
- 【事案１】レンタルサーバのアクセスログを定期的に確認し、不正アクセスを速やかに検知。
  ※（独）情報処理推進機構が提供するWebサイトの攻撃兆候検出ツール”iLogScanner”を使用。
- 【事案２】Webサイトの更新作業に際して、送信元を特定のIPアドレスに限定するなどセキュリティ対策を柔軟に適用できるレンタルサーバを利用。

＜中長期的対策＞

- 【事案１/２】事業者単独では対応できない事案も想定して、事案発生時におけるグループ会社のセキュリティ担当者間での連携を強化。
- 【事案１/２】平時から対外機関との間のセキュリティ情報に係る共有体制を把握。

【得られた気付き・教訓】

- 外部委託契約におけるセキュリティ対策についての責任分界の確認
  （外部業者が対策してくれるという思い込みはせず、あらかじめ契約内容等を確認すべき。）
- 不正アクセス検出を目的としたサーバアクセスログ調査手順の確認
  （情報セキュリティ関係機関から検出ツールが公開されている。）
- Webサイト閉鎖を想定したサービス利用者向け情報伝達手段の確保
  （Webサイトの閉鎖期間が長期間に及ぶ場合、サービス利用者に対してどのように事業者発の情報を伝達するか、代替手段をあらかじめ決めておくことも有効。）
- 対外機関との情報共有体制の確認
  （平時から対外機関との間での情報共有体制を理解しておくことで、事案発生時における初動対応でも慌てずに連携を図ることができる。）
- 事業者内のIT担当部署におけるセキュリティ人材の育成・確保
  （平時から事業者内全体のセキュリティ意識の向上を図り、事案発生時に対応可能な人材の育成に努めるとともに、必要に応じ、例えばグループ会社のセキュリティ担当者間で相互協力が図れるよう取り決め等を結んでおくことも有効。）

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。
	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、業務（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。
	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。
	CIO	Chief Information Officerの略。情報化統括責任者。企業や行政機関等の組織において情報化戦略を立案、実行する責任者のこと。なお、「政府CIO」は内閣情報通信政策監である。
	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。
	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。
	CSAJ	Computer Software Association of Japanの略。一般社団法人コンピュータソフトウェア協会。
	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。
E	eラーニング	electronic learningの略。情報通信技術を用いた教育、学習のこと。
F	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、2015年７月現在、世界70ヶ国の官・民・大学等321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）。政府横断的な情報収集、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	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。
I	IaaS	Infrastructure as a Serviceの略（イアース、アイアース）。ネットワーク経由で、サーバ仮想化やデスクトップ仮想化、共有ディスクなど、ハードウェアやインフラ機能の提供を行うクラウドサービスのこと。
	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。
	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	経済産業省から、各府省庁の調達時に活用することを目的に、コモンクライテリア（CC）認証を取得するべきセキュリティ機能及び評価保証レベル（EAL）を製品分野ごとに明確化したリスト。
	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。
K	KISA	Korea Internet & Security Agencyの略。韓国インターネット振興院。
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。
	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	PaaS	Platform as a Serviceの略（パース）。ネットワーク経由で、仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うクラウドサービスのこと。
	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。
	PoC	Point of Contactの略。連絡窓口。
	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	SaaS	Software as a Serviceの略（サーズ、サース）。ネットワーク経由で、電子メール、グループウェア、顧客管理などのソフトウェア機能の提供を行うクラウドサービス。以前は、ASP（Application Service Provider）などと呼ばれていた。
	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。
	SLA	Service Level Agreementの略。サービス水準保証のこと。
	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。
	SSL/TLS	Secure Socket Layer / Transport Layer Securityの略。インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルのこと。ショッピングサイトやインターネットバンキングなど、個人情報や機密情報をやり取りする際に広く使われている。現在は、SSL3.0をもとに改良が加えられたTLS1.2が標準的なプロトコルとして利用されている。
T	TCP/IP	Internet等で標準的に用いられる通信プロトコルで、TCP（Transmission Control Protocol）とIP（Internet Protocol）を組み合わせたもの。
	TLS	Transport Layer Securityの略。インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルで、SSLを元にして標準化された。
	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。
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。
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。
	科学技術イノベーション総合戦略	2013年６月閣議決定。日本経済の再生に向けて、科学技術イノベーションの潜在力を集中して発揮し、未来を切り拓くための科学技術政策の全体像を示す。
	各府省情報化統括責任者（CIO）連絡会議	政府全体として情報化推進体制を確立し、行政の情報化等を一層推進することにより国民の利便性の向上を図るとともに、行政運営の簡素化、効率化、信頼性及び透明性の向上に資するため、2002年９月、IT総合戦略本部に設置された会議。政府CIOを議長とする。

	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）。
	業務継続計画	BCPを参照。
く	クラウドコンピューティング	データサービス等が、ネットワーク上にあるサーバ群（クラウド（雲））にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」利用することができるコンピュータ・ネットワークの利用形態。
	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	国民を守る情報セキュリティサイト	NISCが開設したサイバーセキュリティに関する普及・啓発のためのポータルサイト。http://www.nisc.go.jp/security-site/
	国連サイバーGGE	GGE:the Group of Government Expertsの略。国連総会第一委員会のサイバーセキュリティに関する政府専門家会合。
	国家安全保障会議	国家の安全保障に関する重要事項及び重大緊急事態への対処を審議する目的で、内閣におかれる。英語略称は、NSC（National Security Council）。
	国家安全保障戦略	2013年12月17日、国家安全保障会議及び閣議決定。我が国における国家安全保障に関する基本方針。
	コンプライアンス	法令遵守。企業が経営・活動を行う上で、法令や各種規則などのルール、さらには社会的規範などを守ること。
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。
	サイバー攻撃解析協議会	サイバー攻撃の実態を把握し、その結果を関係省庁、重要インフラ事業者等に提供することを目的に、総務省、経済産業省、NICT、IPA、テレコム・アイザック推進会議、JPCERT/CCにより2012年７月に発足した協議会。
	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。
	サイバー攻撃分析センター	2013年５月、サイバー攻撃に係る情報集約・分析機能の強化のため、警察庁に設置された。都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換を実施している。
	サイバーストーム演習	CyberStorm演習。米国土安全保障省、米国防総省などが2006年からおおよそ隔年で実施している官民連携のサイバー演習。
	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国際連携取組方針	2013年10月２日、情報セキュリティ政策会議決定。サイバーセキュリティ戦略に基づき策定した、我が国のサイバーセキュリティ分野における国際連携についての基本方針。
	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。
	サイバーセキュリティの日	毎年２月（情報セキュリティ月間）の最初の平日。従前の「情報セキュリティの日」（２月２日）に代わって2014年に新設。
	サイバーディフェンス連携協議会	サイバー攻撃について官民一体で情報共有を図ることを目的とする、防衛省と防衛産業の協議会。2013年７月発足。
	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	事案対処省庁	重要インフラの情報セキュリティ対策に係る第３次行動計画における関係主体の一つ。警察庁、消防庁、海上保安庁及び防衛省。
	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・改訂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。
	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３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、経済産業省及び防衛省。

	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。
	情報セキュリティ国際キャンペーン	2012年より毎年10月に情報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情報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情報セキュリティ対策の一層の普及を図っている。
	情報セキュリティ人材育成プログラム	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。
	情報セキュリティ事象	情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。（JIS Q 27000:2014）
	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	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。
	政府統一基準群	政府機関の情報セキュリティを確保するため、政府機関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情報セキュリティ政策会議決定文書等のこと。「政府機関の情報セキュリティ対策のための統一規範」（2011年４月21日情報セキュリティ政策会議決定、2014年５月19日改定）、「政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針」（2005年９月15日同会議決定、2014年５月19日改定）、「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26年度版）」（2005年９月15日同会議決定、2014年５月19日改定）等。
	政府共通プラットフォーム	各府省が別々に整備・運用している政府情報システムを可能なものから順次統合・集約化し、政府情報システム全体の運用コストの削減、セキュリティの強化等を図るための基盤。2013年３月から運用開始。
	政府情報システム管理データベース	ITガバナンスの強化、情報システムの合理化、情報システムの経費節減、脆弱な情報システムへの対処等を容易にするため、国が保有する情報システムについて、情報システムのライフイベント毎に作成される資料や情報資産等を統一かつ網羅的に管理し、データを蓄積するデータベース。
	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の略）。重要インフラ分野における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、2014年末現在、13分野で18セプターが活動。
	セプターカウンシル	CEPTOAR-Council。各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。

そ	ソーシャルメディア	ブログ、ソーシャルネットワーキングサービス（SNS）、動画共有サイトなど、利用者が情報を発信し、形成していくメディア。利用者同士のつながりを促進する様々なしかけが用意されており、互いの関係を視覚的に把握しやすいのが特徴。
た	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。
ち	中央当局制度	特定の当局を中央当局として指定し、外交ルートを経由せずに中央当局間で共助の授受を行う制度。
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。
	テレコム・アイザック推進会議	一般財団法人日本データ通信協会 テレコム・アイザック推進会議（Telecom-ISAC Japan、ISAC：Information Sharing and Analysis Center）。国内の主要ISP等が中心となって2002年に設立された、通信サービスの安全な運用のためにサイバー攻撃関連情報の共有及び分析等を行う民間組織。
	テレワーク	ICTを活用して、場所と時間にとらわれない柔軟な働き方。企業等に勤務する被雇用者が行う雇用型テレワーク（例：住宅勤務、モバイルワーク、サテライトオフィス等での勤務）と、個人事業者・小規模事業者等が行う自営型テレワーク（例：SOHO、住宅ワーク）に大別される。
	電子商取引	インターネット等を用いて財やサービスの受発注を行う商取引等の総体のこと。
	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	特定電子メール法	特定電子メールの送信の適正化等に関する法律。平成14年４月17日法律第26号。いわゆる「迷惑メール防止法」のこと。
	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	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。略称はNISC（National center of Incident readiness and Strategy for Cybersecurity）。
	なりすまし	他の利用者のふりをすること。または、中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話。（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月）
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。
	パッケージソフトウェア品質認証制度	PSQ（Packaged Software Quality）認証制度。CSAJ（一般社団法人コンピュータソフトウェア協会）によるパッケージソフトウェアの品質認証制度で、国際規格であるISO/IEC 25051:2006に準拠している。
	パブリッククラウド	クラウドサービスのうち、広く一般の利用者を対象に提供されるもの。対して、企業・団体の社員等の内部の利用者に向けて提供するものは「プライベートクラウド」と呼ばれる。

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	ファイアウォール	ネットワークの境界に設置し、ネットワーク内外の情報のやり取りを制御するために用いるソフトウェア又はハードウェア。外部から内部のネットワークへの侵入や、内部から外部への不要な通信の防止等を目的とする。
	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。
	復号	暗号化されたデータに定められた演算を施し、元のデータに戻すこと。
	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。
	踏み台	悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されているコンピュータ等のこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。
	プライバシーポリシー	インターネット上のサービスにおいて、サービス提供者が明らかにするサービスを受ける者の個人情報取扱方針のこと。メールアドレスや通信記録の管理方法等を明らかにする。
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	水飲み場型攻撃	対象組織の職員が通常閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータにマルウェアを自動的に導入させる攻撃手法。
	未踏IT人材発掘・育成事業	2000年度から「未踏ソフトウェア創造事業」として開始し、2008年度により若い人材の発掘・育成に重点化すべく「未踏IT人材発掘・育成事業」として再編したもの。
む	無停電電源装置	二次電池など電力を蓄積する装置を内蔵し、外部からの電力供給が途絶えても一定時間決められた出力で外部に電力を供給することができる装置。

や	やり取り型攻撃	最初から攻撃メールを送付するのではなく、業務との関連等を装った通常のメールのやりとりを何通か行い、より自然な状況を装った後に攻撃メールを送付する手口。
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。