資料２

サイバーセキュリティ政策に係る年次報告（2014 年度）（案）

資料２－１　サイバーセキュリティ政策に係る年次報告
（2014 年度）（案）の概要

※資料２－２　サイバーセキュリティ政策に係る年次報告
（2014 年度）（案）

※は、サイバーセキュリティ戦略本部決定案。

サイバーセキュリティ政策に係る年次報告(2014年度)(案)の概要

資料２－１

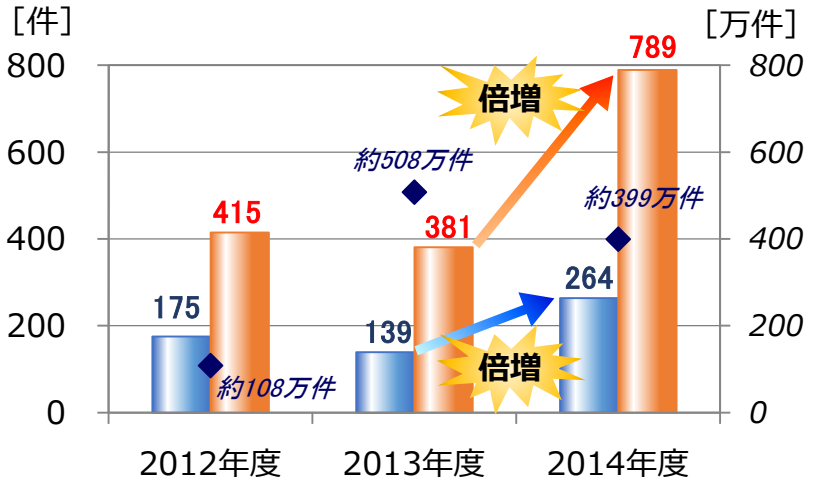
本年次報告の位置付け

- 現行の「サイバーセキュリティ戦略」（2013年6月10日情報セキュリティ政策会議決定）に基づく２期目の年次報告。
- 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を踏まえ、同法に基づく取組も報告。

政府機関等における情勢

- **標的型攻撃の脅威が深刻化**しており、最近では日本年金機構が個人情報の流出を発表（2015年６月）。
- 日本年金機構の原因究明調査結果を踏まえ、情報システムに対する横断監視の対象拡大等、**対策の強化を実施予定**。

【政府機関への脅威件数等】



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

【外部からの攻撃に係る2014年度の特徴】

以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、標的型メールによる脅威が一層深刻化。

- センサー監視等による**通報件数は前年度から倍増**（264件）、そのうち**約４割は標的型メール**（標的型メールの通報件数は前年度比約３倍に増加）。
- 不審メール等の**注意喚起件数**は**前年度から倍増**（789件）。
- センサー監視等による**脅威件数は約399万件**。
  （約８秒毎に１回脅威を認知。前年度より減少したのは、GSOCシステムの能力向上によって、軽微なものの判別対象からの除外を含め、脅威の識別精度が向上したことによるもの。脅威そのものは一層深刻化。）
- 文書作成ソフト等の**未知の脆弱性を利用した攻撃**や、不正通信の接続先にクラウド上のサーバが利用される等、**認知・防御が困難に**。

【2014年度の主なサイバー攻撃事案】

2014.9	［法務省］ サーバに対する外部からの不正アクセスが発覚。
2014.10	［国土地理院］ パソコンがウイルスに感染、情報流出の可能性を発表。
2015.2	［日本貿易振興機構］ 標的型メールによるパソコンのウイルス感染が発覚。
（参考）	
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。

サイバーセキュリティ政策に係る年次報告(2014年度)(案)の概要

2014年度の主な取組実績

■ サイバーセキュリティ推進体制の強化 ―「サイバーセキュリティ基本法」（2015年１月全面施行）に基づく機能強化

- 2014年11月、サイバーセキュリティに関する基本理念等を定めたサイバーセキュリティ基本法が成立。
- サイバーセキュリティ基本法に基づき、我が国のサイバーセキュリティ推進体制を強化するため、2015年１月、**サイバーセキュリティ戦略本部を内閣に設置**。また、その事務局機能を担う**内閣サイバーセキュリティセンターを内閣官房に設置**。
- NISCと関係機関（JPCERT/CC、IPA、NICT、AIST）との協力関係を強化するための**パートナーシップを構築**。

■ 政府機関等における取組 ―「政府統一基準群」（2014年5月改定）に基づく対策の推進 等

- 各府省庁において、**政府統一基準群（2014年５月改定）を踏まえ、セキュリティポリシーの改定を進め対策の強化**を図るとともに、**標的型攻撃に対応するため、リスク評価に係る取組を本格実施**。NISCにおいて、マニュアルを整備し、**サプライチェーン・リスクに対応するための調達要件を強化**。
- NISCにおいて、府省庁CSIRTやCYMAT※の要員を対象とした研修・訓練に加え、３月18日（サイバーの日）には総務省と共催で競技形式の「**サイバー攻撃対処訓練（NATIONAL ３１８ （CYBER） EKIDEN）**」を実施し、**サイバー攻撃対処態勢を強化**。


NATIONAL ３１８ (CYBER) EKIDEN

- 各府省庁において、独立行政法人について、政府統一基準群等を踏まえた対策を講じることによりセキュリティの強化を進める旨の会議決定（2014年6月）を踏まえて対策を推進。
- NISCにおいて、クラウドサービスに関して、調達や運用の観点からセキュリティ対策を検討。
- 戦略本部による**各府省庁等に対する監査について、基本方針を策定（2015年５月）**。マネジメント監査及びペネトレーションテスト（システムへの侵入検査）の実施を決定。

※ CYber incident Mobile Assistance Team　（府省庁横断的な情報セキュリティ緊急支援チーム）

サイバーセキュリティ政策に係る年次報告(2014年度)(案)の概要

2014年度の主な取組実績

■ 重要インフラ事業者等における取組 ―「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）の推進

- 各重要インフラ分野の安全基準等を策定するための**指針を改定**（2015年５月）。
- 重要インフラから124件の情報連絡を受け、38件の情報提供（注意喚起等）を実施。
- 重要インフラ全13分野が参加する**分野横断的演習を実施**（2014年12月）。

年度	2012	2013	2014
参加機関数	42	61	94
参加者数	148	212	348

分野横断的演習の参加機関数・参加者数

■ 国民への普及啓発 ―「新・情報セキュリティ普及啓発プログラム」（2014年７月）の推進

- 国民への普及啓発に関する取組については、「知る・守る・続ける」をキャッチフレーズとしたサイバーセキュリティ月間（2015年２月１日～３月18日）において、普及啓発に関する行事や関連キャンペーンなどを、今年度も実施。
- 加えて、参加者との双方向型のセミナー「**サイバーセキュリティカフェ**」を学生向け及び一般向けの２回開催。

サイバーセキュリティカフェ

■ 国際連携 ―「サイバーセキュリティ国際連携取組方針」（2013年10月）の推進

- 米国との間において、日米サイバー対話（2014年４月）等の枠組みの中で緊密に連携。また、首脳会談等を端緒として、**新たに欧州連合、イスラエル、仏、エストニア、豪等との協議を立ち上げ**。
- 日・ASEAN情報セキュリティ政策会議の枠組みにおいて、「**日ASEANにおける重要インフラ防護に関するガイドライン**」を策定。また、**Meridian会合を日本において開催**、各国の重要インフラ防護に関するベストプラクティスや政策動向などに関する情報共有を実施。

Meridian会合

（参考）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。

資料２－２

サイバーセキュリティ政策に係る年次報告
（2014年度）（案）

2015年〇月〇日

サイバーセキュリティ戦略本部

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

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

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

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

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

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

＜目次＞

はじめに

情報通信技術に大きく依存している現代社会において、サイバーセキュリティの確保は、国民生活や社会経済活動はもとより、国家の安全保障・危機管理においても極めて重要な課題となっている。2015年６月には、日本年金機構が標的型攻撃を受けて約125万件の個人情報流出を発表したが、政府機関や企業からの機密情報等の窃取を企図した標的型攻撃は一層複雑・巧妙化し、攻撃対象も拡大し続けている。また、インターネットバンキングにおける不正送金事案等、不正な電子商取引の発生件数も依然として増加傾向にあることや、重要インフラ等の制御システムを狙った攻撃なども増加傾向にある。このように、サイバー攻撃の脅威は一層拡大してきており、国民の安全・安心に直接的かつ重大な影響を及ぼし、また、我が国の国際競争力を揺るがしかねない課題を生じさせている。

こうした状況の中、我が国においては、2005年４月に内閣官房情報セキュリティセンターが設置されるとともに、同年５月に内閣官房長官を議長とする情報セキュリティ政策会議が高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）の下に設置され、我が国におけるサイバーセキュリティ政策の司令塔の役割を担ってきた。2014年度においては、2013年６月に策定された「サイバーセキュリティ戦略」に基づく２期目の年次計画「サイバーセキュリティ2014」によって施策を推進した。さらに、2014年11月にサイバーセキュリティ基本法が成立し、2015年１月には我が国の司令塔の役割を担うサイバーセキュリティ戦略本部及び内閣サイバーセキュリティセンター（NISC）が設置され、新しい法的枠組みに基づく活動を開始したところである。

本報告は2014年度の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政府機関等における取組、重要インフラ事業者等における取組、「サイバーセキュリティ2014」に掲げられた各府省庁の関連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、2014年度において特記すべき点としては、サイバーセキュリティ基本法の成立に加え、サイバーセキュリティ戦略本部の設置、NISCの法制化措置を実施するなど、我が国のサイバーセキュリティ推進体制の強化を行ってきたことが挙げられる。しかしながら、サイバー攻撃によるリスクが一層拡大・深刻化していることや、社会保障・税番号（マイナンバー）制度の導入、2020年のオリンピック・パラリンピック東京大会開催に向けた対策強化等、新たな課題への対応も求められている。

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、本報告における施策評価等を踏まえ、サイバーセキュリティ関連施策に関して適切なPDCAサイクルを回すことによって継続的な改善を実践するとともに、新たなサイバーセキュリティ戦略及び同戦略に基づく年次計画を策定し、これを着実に推進することとする。

Ⅰ　2014 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

近年、企業において情報システムの新規構築や再構築の取り組みが増加してきている（2010年度を底に増加傾向）[1]。また、個人においても、スマートフォンの世帯保有率は2013年末には約60%となっており、2010年末の10%に比較すると６倍に急増している[2]など、情報通信技術の利活用は一層高まっている。

こうした状況の中、2014年度はインターネットバンキングやフィッシング等による被害が増加した。2014年の不正アクセス行為の認知件数は3,545件であり、昨年（2013年）の2,951件から約20%増加している。これら不正行為の目的としては、インターネットバンキングの不正送金が昨年度からさらに増加しており、他の目的に比して突出していることが特徴的である（図表Ⅰ－１－１）。また、2014年はインターネットショッピングの不正購入を目的としているものは2013年から減少しているものの、インターネットバンキングの不正送金と合わせて、引き続き金銭目的の不正アクセス行為が増加している。

図表Ⅰ－１－１　不正アクセス行為の認知件数とその後の行為[3]

不正アクセス行為後の行為	2013年	2014年
インターネットバンキングの不正送金	1,325 件	1,944 件
他人へのなりすまし	26 件	1,009 件
インターネットショッピングの不正購入	911 件	209 件
情報の不正入手	92 件	177 件
オンラインゲーム、コミュニティサイトの不正操作	379 件	130 件
ホームページの改ざん・消去	107 件	40 件
インターネット・オークションの不正操作	36 件	13 件
不正ファイルの蔵置	20 件	1 件
その他	55 件	22 件
合　計	2,951 件	3,545 件

不正アクセス行為の手口は、ID・パスワードなどの識別符号を窃用した不正アクセス行為に係る検挙件数をみると、その入手手口は、2013年では「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が大部分を占めていたが、2014年は「フィッシングサイトにより入手したもの」が急増しており、不正アクセス行為の手口が巧妙化している（図表Ⅰ－１－２）。さらに、正規のサービス提供企業を装ったメールを送り、IDやパスワードなどのログイン情報のほか、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を不正に窃取するフィッシングはサイバー空間における脅威を拡大している要因である。例えば、2015年度にフィッシング対策協議会に寄せられた「フィッシング報告件数（海外含む）」によれば、2014年度の報告件数は14,085件であり、2013年度に引き続き高水準で維持されている（図表Ⅰ－１－３）。また、フィッシング対策協議会の月次報告によると、この件数のうちの多くがオンラインゲームや金融機関をかたるフィッシングとの報告もあることなどを踏まえると、金銭目的とみられる不正アクセスはサイバーセキュリティに係る大きな脅威であるといえる。

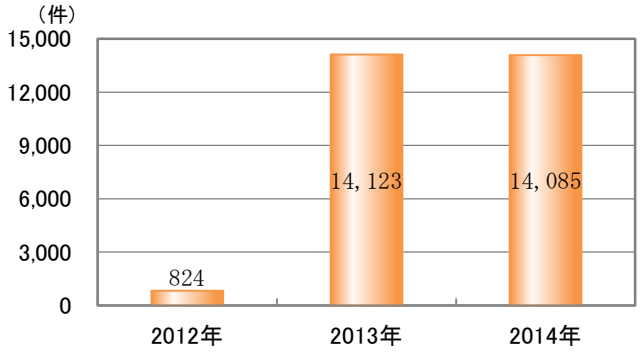
---

[1] 平成 26 年度我が国情報経済社会における基盤整備調査報告書 p9-10（2015 年３月経済産業省）。
[2] 総務省「平成 26 年版情報通信白書」。
[3] 「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技術の研究開発の状況」（警察庁、総務省及び経済産業省、2015 年３月 19 日公表）のデータから作成。

図表Ⅰ－1－2　不正アクセス行為に係る犯行の手口の内訳[4]

	2013年	2014年
識別符号窃用型の検挙件数	965件	336件
利用権者のパスワードの設定・管理の甘さにつけ込んだもの	767件	84件
フィッシングサイトにより入手したもの	9件	71件
言葉巧みに利用権者から聞き出した又はのぞき見たもの	64件	53件
識別符号を知り得る立場にあった元従業員や知人等によるもの	56件	47件
インターネット上に流出・公開されていた識別符号を入手したもの	9件	34件
他人から入手したもの	33件	25件
スパイウェア等のプログラムを使用して識別符号を入手したもの	25件	6件
その他	2件	16件
セキュリティ・ホール攻撃型の検挙件数	3件	2件

図表Ⅰ－1－3　フィッシング報告件数の推移[5]



金銭目的とみられる不正アクセスに加え、2014年度は、大規模な情報流出を伴う事案が海外のみならず日本国内においても確認され、一般企業等においても不正アクセスは脅威となっている（図表Ⅰ－1－4）。2014年７月には、教育関連企業で、我が国において最大規模の顧客漏えいが発覚し、約2,900万件の顧客情報が漏えいしたとされている[6]。また、米国においては、2014年10月に、米国大手金融機関がサイバー攻撃を受けた結果、顧客の個人情報や同社の内部情報が流出し、これにより約7,600万件の世帯及び約700万件の小規模企業の口座に影響があることを公表した[7]。また、2014年12月には、米国映画会社が北朝鮮の政治体制を扱った映画の全米公開を中止するとの声明を発表したが、米国政府は同社へのサイバー攻撃について、攻撃の手口などから北朝鮮政府に責任があると結論付ける十分な情報があると指摘したうえで、米国企業に重大な損害を与え、表現の自由を抑圧しようとする破壊的な攻撃であり、国家の行動として許容できる範囲を逸脱していると非難し[8]、北朝鮮政府に対する追加的な経済制裁を行

[4] 「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技術の研究開発の状況」（警察庁、総務省及び経済産業省、2015年３月19日公表）のデータから作成。
[5] フィッシング対策協議会　月次フィッシング報告状況より作成。
[6] http://www.benesse.co.jp/customer/bcinfo/01.html
[7] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, Washington, D.C. 20549, FORM 8-K, CURRENT REPORT, Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934, Date of Report (date of earliest event reported): October 2, 2014, JPMorgan Chase & Co., (http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm)
[8] Update on Sony Investigation, FBI National Press Office, December 19, 2014, (https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation)

うに至った[9]。2015年２月には、米国大手保険会社においても、サイバー攻撃により、氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報等の個人情報が大規模に流出する事案が発生した[10]。このように、米国においては、複数の企業が、サイバー攻撃によって大規模な情報流出という事態に陥っており、多大な被害が生じている。この他にも、国家の関与が疑われる事案や国際テロ組織等の関与が疑われる事案も発生してきている。

図表Ⅰ－１－４　届出管理者別の不正アクセス認知件数[11]

	2012年	2013年	2014年
一般企業	1,163 件	2,893 件	3,468 件
大学、研究機関等	12 件	9 件	56 件
プロバイダ	22 件	9 件	16 件
その他	54 件	40 件	5 件
うち行政機関	52 件	24 件	3 件

標的型攻撃の脅威も引き続き急速に増大しており、警察庁によれば同庁で2014年中に把握した標的型メール攻撃は1,732件と前年（2013年）の492件に比して約3.5倍に増加している[12]。同庁の分析では、英文による「ばらまき型」攻撃の増加のほか、日本の制度を踏まえた内容のメールや特定の分野の研究会等を装ったメールも確認されており、攻撃の手口が巧妙化・多様化していることが指摘されている。2015年６月には、日本年金機構において約125万件に上る個人情報の流出が発表されたところであり[13]、その原因究明を速やかに図るとともに早急な対処策を講じることが求められている。また、海外においても、フランス国際放送（2015年４月）[14]やドイツ連邦議会（2015年５月）[15]に対するサイバー攻撃事案が報道されているほか、最近では米国連邦人事管理局の情報システムがサイバー攻撃を受け、2,000万人を超える連邦職員等の個人情報が流出した旨が公表されるなど[16]、サイバー攻撃によって機能停止や大量の個人情報が流出する事案が相次いでおり、サイバー攻撃は一層複雑化・巧妙化しているとともに、その被害が飛躍的に増大している状況にある。

このように、情報通信技術の普及等によって国民生活の利便性の向上や社会経済活動の効率化、さらに新市場の創出が図られている一方、国民の資産を狙ったサイバー攻撃が深刻度を深めているほか、標的型攻撃による大量の個人情報流出事案などが相次いで発生している。政府はもとより関係するステークホルダーの連携・協力によりサイバーセキュリティの強化を図ることは我が国にとって喫緊の課題であり、政府としても最重要課題の一つとして取り組んでいくことが求められている。

---

[9] Executive Order-Imposing Additional Sanctions with Respect to North Korea (https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea)
[10] How to access & sign up for identity theft repair & credit monitoring services(https://www.anthemfacts.com/)
[11] 「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技術の研究開発の状況」（警察庁、総務省及び経済産業省、2015 年３月 19 日公表）のデータから作成。
[12] 「平成 26 年中のサイバー空間をめぐる脅威の情勢について」（警察庁、2015 年３月 12 日）。
[13] http://www.nenkin.go.jp/n/data/service/0000150601ndjIleouIi.pdf
[14] http://www.ssi.gouv.fr/actualite/attaque-informatique-contre-tv5-monde-lanssi-mobilisee/
[15] http://www.bundestag.de/presse/pressemitteilungen/2015/pm_15061112/378140
[16] https://www.opm.gov/cybersecurity/

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については、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いる。

NISCにおいては、府省庁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[17]）を設け、府省庁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、各府省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[18]）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。

(2) 2014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[19]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。

2014年度は、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、外部からの攻撃、特に標的型メール攻撃数が前年度比で約３倍、不審な通信数が前年度比で約２倍となるなど、深刻な被害をもたらし得る脅威が急速に高まった年度となった。主な情報セキュリティインシデントとして、2014年９月に公表された「法務省民事局及び法務局のサーバ等への不正アクセスを確認した件」及び同年10月に公表された「国土交通省国土地理院におけるウイルス感染事案」では、情報が外部に送信された可能性があると公表され、更に2015年２月に公表された日本貿易振興機構の「PCのマルウェア感染と個人情報の流出」では、標的型メール攻撃により不正プログラムに感染し遠隔操作が行われ、個人情報が外部に流出したと公表された。その後も外部からの攻撃は収まることはなく、政府機関に対する執拗な攻撃の中、2015年６月、日本年金機構からの情報流出事案が公表されることとなった。例えば標的型メール攻撃は、標的となった組織内のわずか１人が不審メールの添付ファイルを開封し、又はリンクをクリックすることで不正プログラムに感染し、場合によっては、大規模な情報流出や情報システムの破壊をもたらすこともある。このようなサイバー攻撃の特性にかんがみれば、攻撃数の多さよりも、攻撃の成功の可能性がより高い標的型メール攻撃などの巧妙な攻撃に対してより大きな注力が必要である。

以下に、2014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。

---

[17] GSOC（Government Security Operation Coordination team）。
[18] CYMAT（Cyber Incident Mobile Assistance Team）。
[19] 「別添３－１１　政府機関等に係る2014年度の情報セキュリティインシデント一覧」を参照。

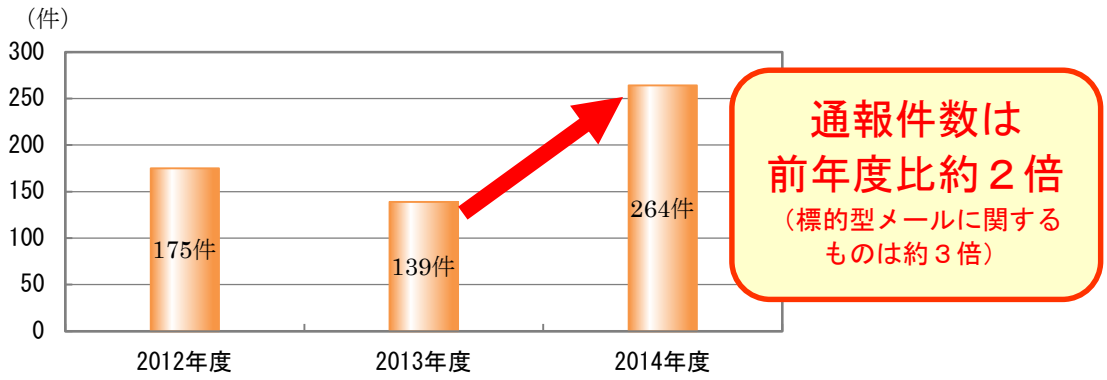
①　外部からの攻撃に係る情報セキュリティインシデント

（ア）政府機関に対する攻撃の傾向について

ここ数年、政府機関や独立行政法人等において、不正アクセスや不正プログラムの攻撃等により、政府機関等の重要な情報の窃取を企図したものとみられる情報セキュリティインシデントが多数発生している。

NISCでは、GSOCにおいて、政府機関に対するサイバー攻撃へ対応するために、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正な通信等を検知し、攻撃を発見するものである。一般的に、標的型攻撃はサイバー攻撃の初期段階において多く使われる手段であり、その検知は極めて重要である。このGSOCセンサー等による監視活動によって不正アクセスや不審な通信等（疑いを含む）を検知した際には当該政府機関への通報[20]を行っており、2014年度においては、264件の通報を行った（図表Ⅰ－２－１）。2013年度の139件と比較してほぼ倍増しており、これは、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急激に増大していることを示している。

図表Ⅰ－２－１　GSOC センサー監視等による通報件数の推移



2012年度の通報は、半数以上が標的型メールの検知[21]によるものであった。2013年度には、標的型メールに関する通報は全体の約四分の一と減少したが、不審な通信の検知[22]が全体の３割に及んだ。

2014年度については、前年度から引き続き不審な通信の検知が多くみられ、全体の３割以上を占める一方で、標的型メールに関する通報も増加に転じ、４割を占めている。不審な通信が検知される要因としては、標的型メール攻撃による不正プログラムへの感染等も大きな要因と考えられることから、2014年度はまさに標的型メール攻撃の脅威が高まったと考えられる。

[20] 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。
[21] 不正プログラムが添付されていたり、不正リンクが付されていたりする不審メールの検知。
[22] 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。

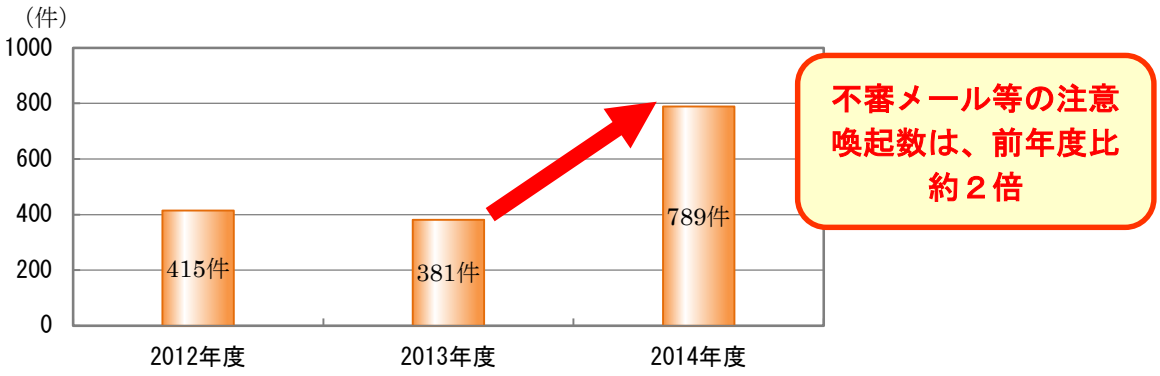
標的型メール攻撃とは、不正な情報窃取等を目的として実行型ファイル（不正プログラム）が添付されていたり、本文中に特定のサイトに誘導するリンクが付されたりする不審メールを、標的とする組織の職員等に送付する攻撃である。従来は、「ばらまき型」攻撃と呼ばれる標的とする複数の対象に対して同一のメールを送信するタイプの攻撃が多くみられたが、最近では、特定の組織を標的に選び重要な情報を盗むこと等を目的として、その組織の特定の職員等に向けて作成された偽のメールを送付するタイプの攻撃も多くみられるようになった。これらの標的型メールは、実在する企業名や政府機関名をかたり、その本文等が巧妙に作られているものや、別途入手した本物のメールを流用したと思われるものがみられ、一見しただけでは本物と偽のメールの識別が困難で、メール受信者が業務に関係するメールと信じてしまうように巧みに偽装されている。このように、標的型メール攻撃の手法がより巧妙化することで、深刻な被害をもたらし得る攻撃が成功する可能性が高まっていると考えられる。

標的型メール攻撃では、メール受信者が添付されたファイルを開くことや、記載されているリンクをクリックすることで不正プログラムがダウンロードされ、メール受信者の端末で不正プログラムが実行される。一旦、不正プログラムが実行されると、C&Cサーバ[23]と通信を行い、新しい不正プログラムをダウンロードしたり、不正に入手した情報を外部へ送信したりする。そのやりとりは通常のWebアクセス等の正常な通信と識別が困難となるよう設計され、更にC&Cサーバがクラウドサーバの中にある場合には、同じサーバ上にはほかに多くのウェブサイトも存在するため、不正な通信を識別・検知し遮断を行うような防御が難しいという大きな問題がある。GSOCで検知した不正プログラムの通信先を国別にみると、2013年度まではほとんどが海外であったのに対し、2014年度は日本国内を通信先とするものが増加した。国内のサーバ上には通常業務において高い頻度で参照する必要のあるウェブサイトが多いが、このような国内のサーバ上にC&Cサーバが巣くい、更に防御が難しいクラウドサーバ上にC&Cサーバが巣くったことが、不正プログラムとC&Cサーバの通信を遮断するような防御を一層困難にさせたと考えられる。

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正体の怪しい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、不審メールや不正プログラムであることが確認できたものについて、政府機関に対して一斉に注意喚起を行うもので、2014年度においては、789件の注意喚起文書を発出した（図表Ⅰ－２－２）。

[23] Command and Control Server。不正プログラムに感染した端末に指令（Command）を送り、制御（Control）を行うサーバ。感染した端末を遠隔操作し、情報搾取や破壊活動を指令する。

図表Ⅰ－２－２　不審メール等に関する注意喚起の件数の推移



特に2014年度は、2013年度の381件に対して789件と倍増しており、以前にも増して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急増している。このような高い脅威となる攻撃は、政府機関に対してのみならず、我が国全体についても高まっていると考えられる。このことは、例えば、独立行政法人情報処理推進機構（IPA）による、「情報セキュリティ10大脅威」の第３位に「標的型攻撃による諜報活動」が挙げられていることが示している。「情報セキュリティ10大脅威」によれば、2014年は、やり取り型攻撃[24]が国内で確認されたことや、日本語文書作成ソフトの脆弱性を悪用しウイルス感染させる等、さらに巧妙化した手口が確認された[25]としているが、国内のC&Cサーバが増加したことを合わせて考えれば、政府機関のみならず我が国全体を標的とした攻撃が増加していると考えられる。

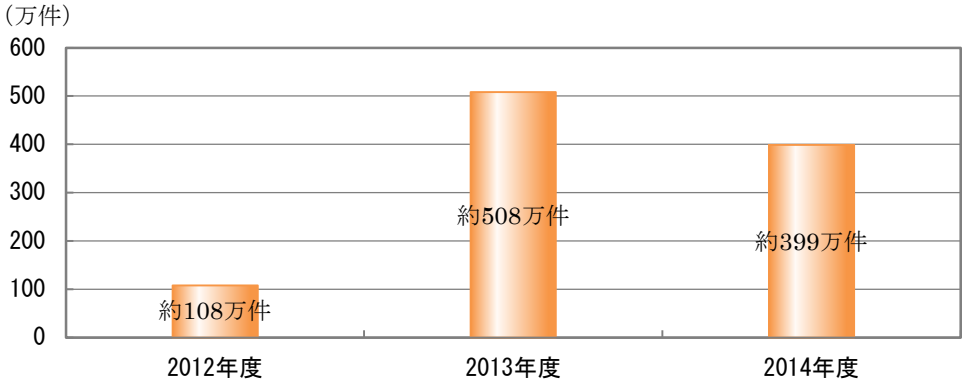
（イ）政府機関への脅威動向について

GSOCにおけるGSOC センサー等による監視活動において、2014年度に政府機関への脅威と認知された件数[26]は、約399万件であった（図表Ⅰ－２－３）。これは、約８秒に１回、脅威を認知している計算となる。2013年度に約508万件あった脅威の認知件数は、2014年度には約399万件と数としては減少している。これは、GSOCシステムの能力向上によって、軽微なものの判別対象からの除外を含め、脅威の識別精度が向上したことによるものである。このような能力向上により、より効果的なサイバー攻撃の分析を効率的に行えるようになり、標的型攻撃がもたらすような、より高い脅威を初期段階で効果的に捉えることができるようになった。

脅威の認知件数が数としては減少したにも関わらず、政府機関に対する通報を行った件数は、2014年度は264件と、2013年度と比較してほぼ倍増したことは、政府機関に対する攻撃は減少しておらず、むしろ高い脅威となる攻撃が急増していることを示している。

[24] やり取り型攻撃：いきなり不正プログラムを送り付けるのではなく、標的とメールのやり取りを行い信用させた後に、不正プログラムが添付されたメールを送信する攻撃手法。
[25] 情報処理推進機構「情報セキュリティ 10 大脅威 2015」。
[26] GSOC センサー等の監視活動により、政府機関に対する脅威であると認知されたもの。

図表Ⅰ－２－３　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



（ウ）ソフトウェアの脆弱性情報の傾向について

GSOCでは、ウェブ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。2014年度においては、GSOCより84件の脆弱性情報等を配信した（図表Ⅰ－２－４）[27]。

図表Ⅰ－２－４　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

	2012年度	2013年度	2014年度
脆弱性情報等の配信	74 件	78 件	84 件

脆弱性を悪用した攻撃の代表的なものとしては、ウェブサイトの改ざんが挙げられる。これまで政府機関における対策を重点的に推進してきたが、2014年度も2013年度から引き続き政府機関のみならず、大学や研究所等においてもウェブサイト改ざんがみられたことから、独立行政法人等においても対策の一層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264件と2013年度から倍増し、その内訳は標的型メールの検知が４割、不審な通信の検知が３割を占めること、また、政府機関から提供があった検体のうち、不審メール及び不正プログラムと確認され、注意喚起文書を発出した件数も789件と前年度から倍増したことを合わせ考えると、2014年度は標的型メール攻撃のような外部からの攻撃の脅威が高まったといえる。

このような標的型メール等による外部からの執拗かつ巧妙な攻撃により、現実に情報流出の事実が確認された重大な事案として、先に述べた日本年金機構からの情報流出事案がある（図表Ⅰ－２－５）。本事案において、GSOCでは厚生労働省から外部に対する不審な通信を検知し、直ちに厚生労働省に対し通報を行ったが、結果として、厚生労働省のネット

[27] 2014 年度は、OpenSSL、bash、Apache Struts 2 等の広く用いられているサーバーソフトウェアの脆弱性が公開され、その脆弱性を悪用した攻撃が発生した。またクライアントソフトウェア Internet Explorer のゼロデイの脆弱性が公表され、修正プログラムが提供されるまでの数日間、ユーザーの不安を招くこととなった（情報処理推進機構「情報セキュリティ 10 大脅威 2015」）。

ワークに接続されている日本年金機構の端末から、極めて大量の個人情報が流出するという情報セキュリティインシデントになった。攻撃手法がますます巧妙化する中、不正プログラムの侵入を完全に防ぐことは困難であるが、侵入を検知した場合には、直ちに必要な対策を講じることが重要であり、重要な情報を扱う独立行政法人等を含め、防御する側の迅速かつ適切な対応が求められる。

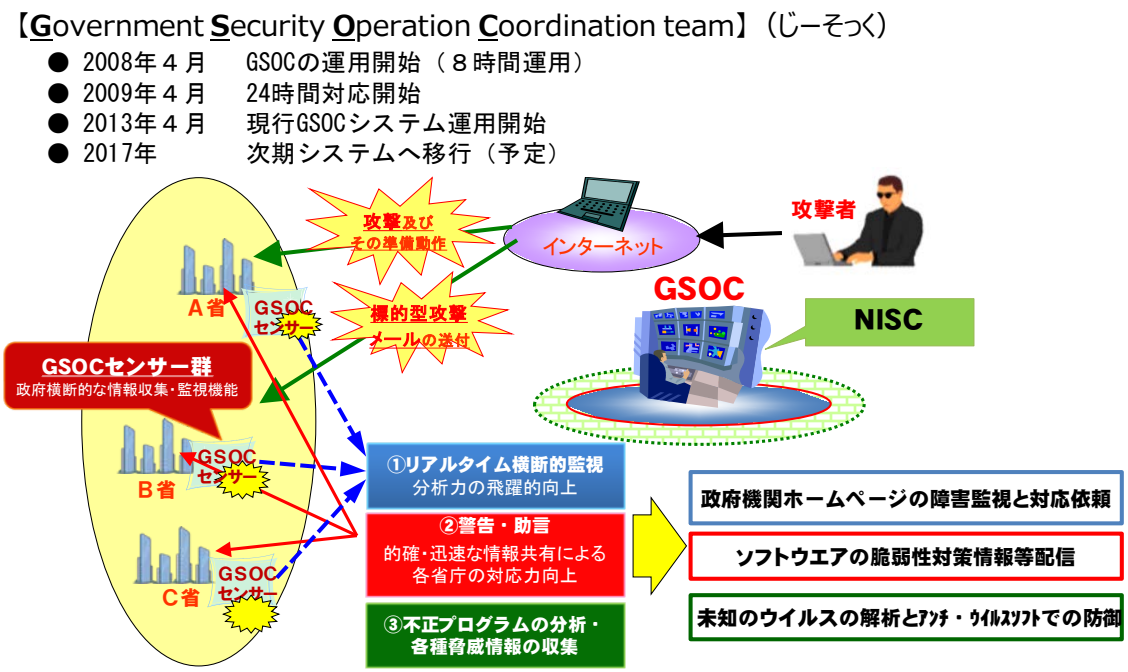
このため、「日本再興戦略」改訂2015（2015年６月30日閣議決定）においても、「まず、内閣サイバーセキュリティセンター（NISC）における政府機関等の情報システムに対する横断監視について、中央省庁に加え、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等についても、公平な受益者負担に留意しつつ段階的に監視対象に追加するとともに、監視手法についても高度化を図る。」とされており、今後、サイバーセキュリティ対策の見直し強化を行っていくことが政府の方針となっている。

図表Ⅰ－２－５　日本年金機構からの情報流出事案（2015 年６月）

2015 年６月、日本年金機構において約 125 万件の個人情報が流出していたことについて公表された。当該事案は、機構の職員が標的型メールの添付ファイルを開封してしまったことにより、機構内の端末がマルウェアに感染、一時的にファイル共有サーバに保存していた個人情報が流出してしまったものである。

巧妙化する標的型攻撃を完全に防ぐことは困難であるものの、本事案では、機構内の個人情報管理が適切でなかったことや、不審な通信が検出された後の対処が適切であったのかなどについて議論となっているが、NISC における原因究明調査や、厚生労働省が立ち上げた「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検証委員会」における原因究明の結果を踏まえ、サイバーセキュリティ対策の見直し強化を行っていくことになる。

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

2014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。

従来からみられる、記憶媒体の紛失やメールの誤送信といった人の不注意による偶発的なインシデントは2014年度も発生している。

また、近年見られるようになった、インターネットに繋がる機器やクラウドサービスの不適切な利用・利用時の不適切な設定に係るインシデントも発生しており、2014年度は、政府機関、独立行政法人等で、本来、関係者だけが閲覧し得る個人情報や内部情報が、インターネット上のホームページやクラウドサービス上で誰でも閲覧できる状態になっていた事案などが発生している。

政府機関等においては、政府外部のクラウドサービスの利活用については、情報セキュリティを確保する観点から、慎重に対応してきた。業務現場においては、利便性の高いサービスに対するニーズは高まる一方であるが、上述の事案のように、不適切な利用や不適切な設定が原因で、情報セキュリティインシデントを引き起こすことも考えられる。したがって、取扱いに注意を要する情報等について、業務現場のニーズをふまえつつ、情報セキュリティが確保されたIT利活用環境を整備することが必要である。

3　2014 年度の政府の主な政策の取組実績

深刻化し拡散するサイバーセキュリティに係る諸課題に適切に取り組むため、政府は、サイバーセキュリティ政策を俯瞰した中長期戦略として「サイバーセキュリティ戦略」（2013年６月10日情報セキュリティ政策会議決定。以下「従来戦略」という。）に基づき、官民における統一的・横断的な情報セキュリティ対策を推進してきた。2014年度の主な取組実績としては、従来戦略を受け、情報セキュリティ政策会議（以下「政策会議」という。）において、2014年１月から継続して我が国のサイバーセキュリティ推進体制の機能強化の検討を行った。また、国会においてもサイバーセキュリティに係る初の法律としてサイバーセキュリティ基本法についての審議が進められた。以下、サイバーセキュリティ基本法、サイバーセキュリティ推進体制の機能強化の検討結果等について概説する。

(1)　サイバーセキュリティ基本法

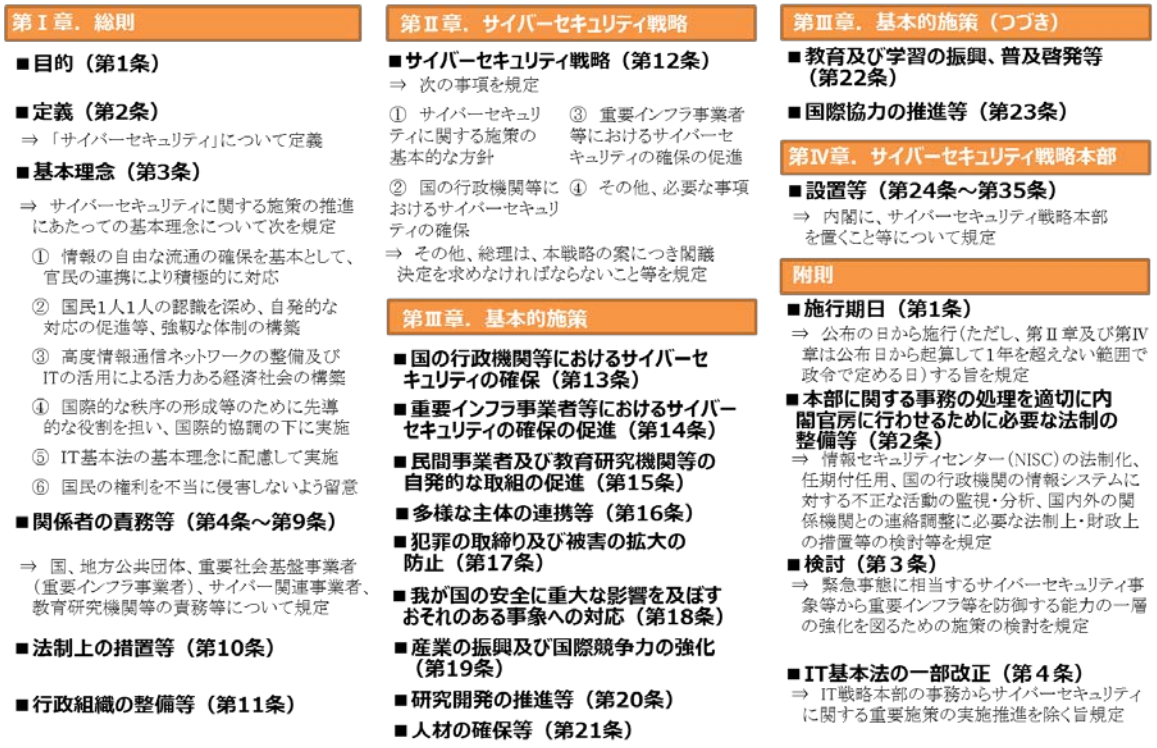
2014年11月12日に公布・一部施行されたサイバーセキュリティ基本法（完全施行は2015年１月９日。以下「基本法」という。）は、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項を定めるとともに、戦略本部を設置する等の措置を講じるものである。

主な内容としては、第一に、サイバーセキュリティについて定義するほか、我が国のサイバーセキュリティに関する施策について基本理念を規定している。第二に、国をはじめ、地方公共団体、重要社会基盤事業者（注：重要インフラ事業者のこと。）、サイバー関連事業者等の責務等を規定している。第三に、サイバーセキュリティ戦略を策定しなければならないこととし、その実施に必要な資金等の確保を図るため、政府は必要な措置を講ずるよう努めることなどを規定している。第四に、国が講ずるものとする基本的施策として、国の行政機関等や重要社会基盤事業者等における取組について規定している。第五に、我が国における司令塔となるサイバーセキュリティ戦略本部を内閣に設置すること等を規定している。そのほか、附則において、サイバーセキュリティ戦略本部に関する事務の処理を適切に内閣官房に行わせるため、内閣官房情報セキュリティセンターの法制化を含む必要な法制の整備を行うこと等を規定している（図表Ⅰ－３－１）。

基本法において特に注目すべき点は、まず、「サイバーセキュリティ」という言葉を法律上の用語として定義したことである。これは、サイバー空間が実社会と一体となった現代において、サイバー攻撃への対応が重要であることを強く意識したものであり、「サイバーセキュリティ」という言葉が広く国民、企業、政府、自治体等の中で浸透することによって、意識が高まることを期待している。

また、国や地方公共団体、重要社会基盤事業者のほか、国民一人一人の努力についても規定するなど、関係する主体それぞれの役割が明確にされたことも注目すべき点である。とりわけサイバーセキュリティは国家の安全保障、危機管理にも関わる分野でもあることから、官民の役割を明確化した上で、国が主導的な立場を果たしながら、官民の緊密な連携により取組を進めていくことが重要である。

図表Ⅰ-3-1　サイバーセキュリティ基本法の概要

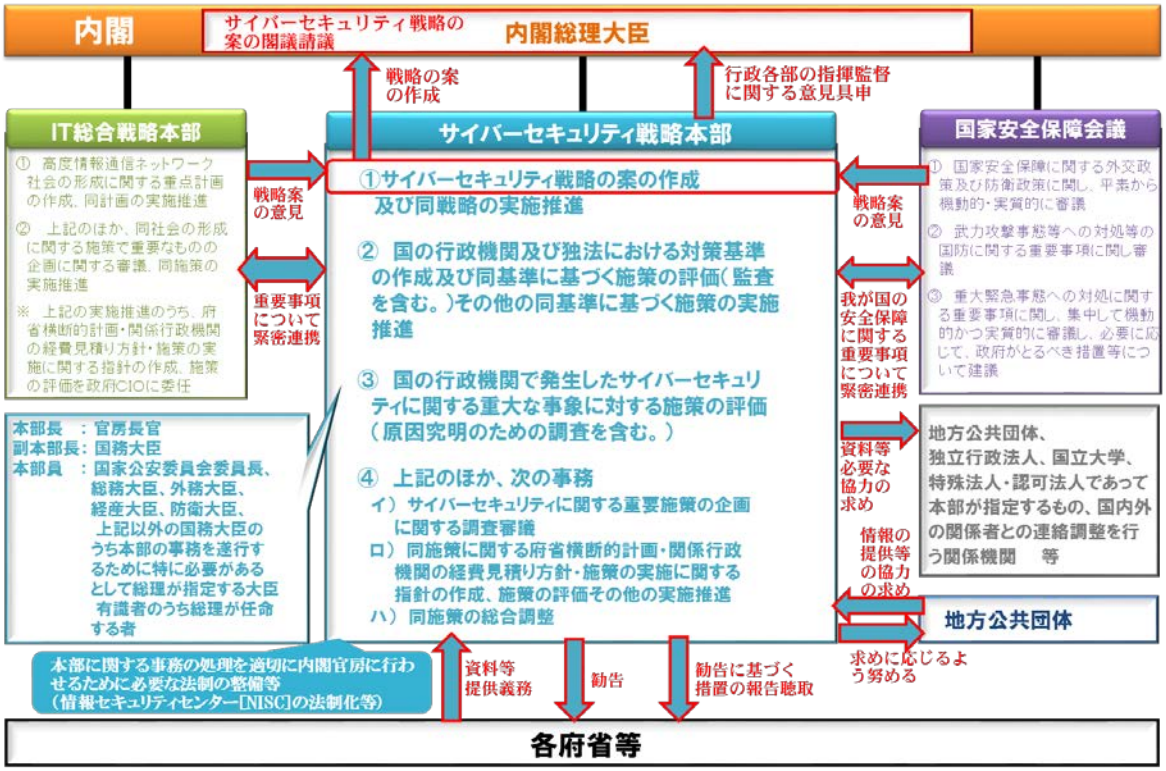


(2)　サイバーセキュリティ戦略本部

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、基本法が完全施行された2015年１月９日、我が国における司令塔となるサイバーセキュリティ戦略本部（本部長：内閣官房長官。以下「戦略本部」という。）が内閣に設置された（図表Ⅰ-3-2）。戦略本部の事務としては、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のほか、高度情報通信ネットワーク社会推進戦略本部（以下「IT総合戦略本部」という。）及び国家安全保障会議と緊密に連携することや、関係行政機関からの同本部への資料提供義務等が基本法に規定されている。このため、戦略本部は所掌事務の遂行に資する資料又は情報を提出義務に基づき集約することができ、情報のハブとして、関係機関のスムーズな連携を促進する調整役となることができる。さらに、基本法において、戦略本部を中心に、関係府省の情報共有体制の強化を図ることとしており、これによって国としての対処能力の向上を図ることが可能となる。

なお、基本法において、戦略本部はIT総合戦略本部や国家安全保障会議と緊密に連携することが規定されており（基本法第25条）、例えば、戦略本部がサイバー攻撃の情報等を把握し、その分析等を行った結果、外国政府等が関与している可能性が高いと判断する場合等については、国家安全保障会議に対しその情報を提供する等、適切に対処していくことなどが想定される。また、戦略本部がサイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、IT総合戦略本部及び国家安全保障会議の意見を聴取しなければならないとされている。

図表Ⅰ－3－2　サイバーセキュリティ戦略本部の機能・権限（イメージ）

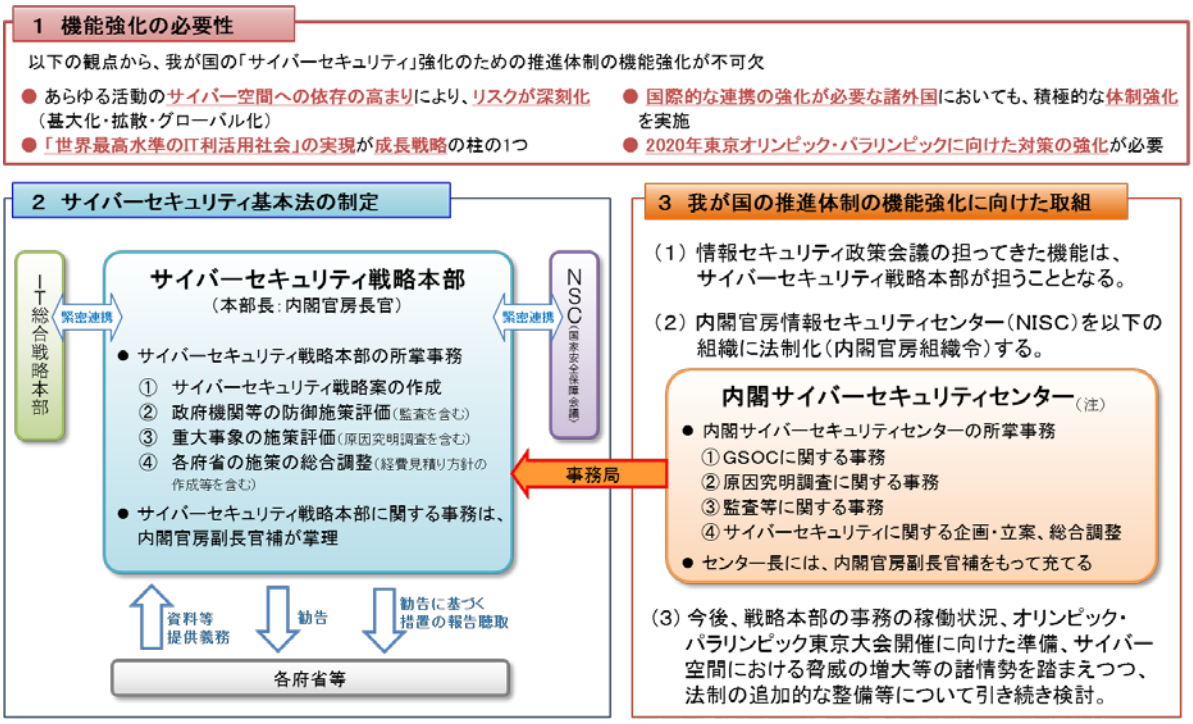


図表Ⅰ－3－3　第１回サイバーセキュリティ戦略本部会合（2015 年２月 10 日）の様子

(3)　内閣官房におけるサイバーセキュリティ推進体制の強化（政府取組方針）

前述のとおり、基本法附則第２条において、政府は所要の法令を整備し、内閣官房に置かれる情報セキュリティセンターを法制化することとされた。これを踏まえ、2014年11月25日、情報セキュリティ政策会議は、「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」を決定した（図表Ⅰ－3－4）。具体的には、新たに内閣サイバーセキュリティセンターを内閣官房に設置し、内閣サイバーセキュリティセンター長には、平素から事態対処・危機管理や安全保障までの連続的に対応できる体制を確保するため、事態対処・危機管理を担当し、かつ、安全保障局次長に充てられている内閣官房副長官補をもって充てることとされた。

図表Ⅰ－3－4　「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」概要

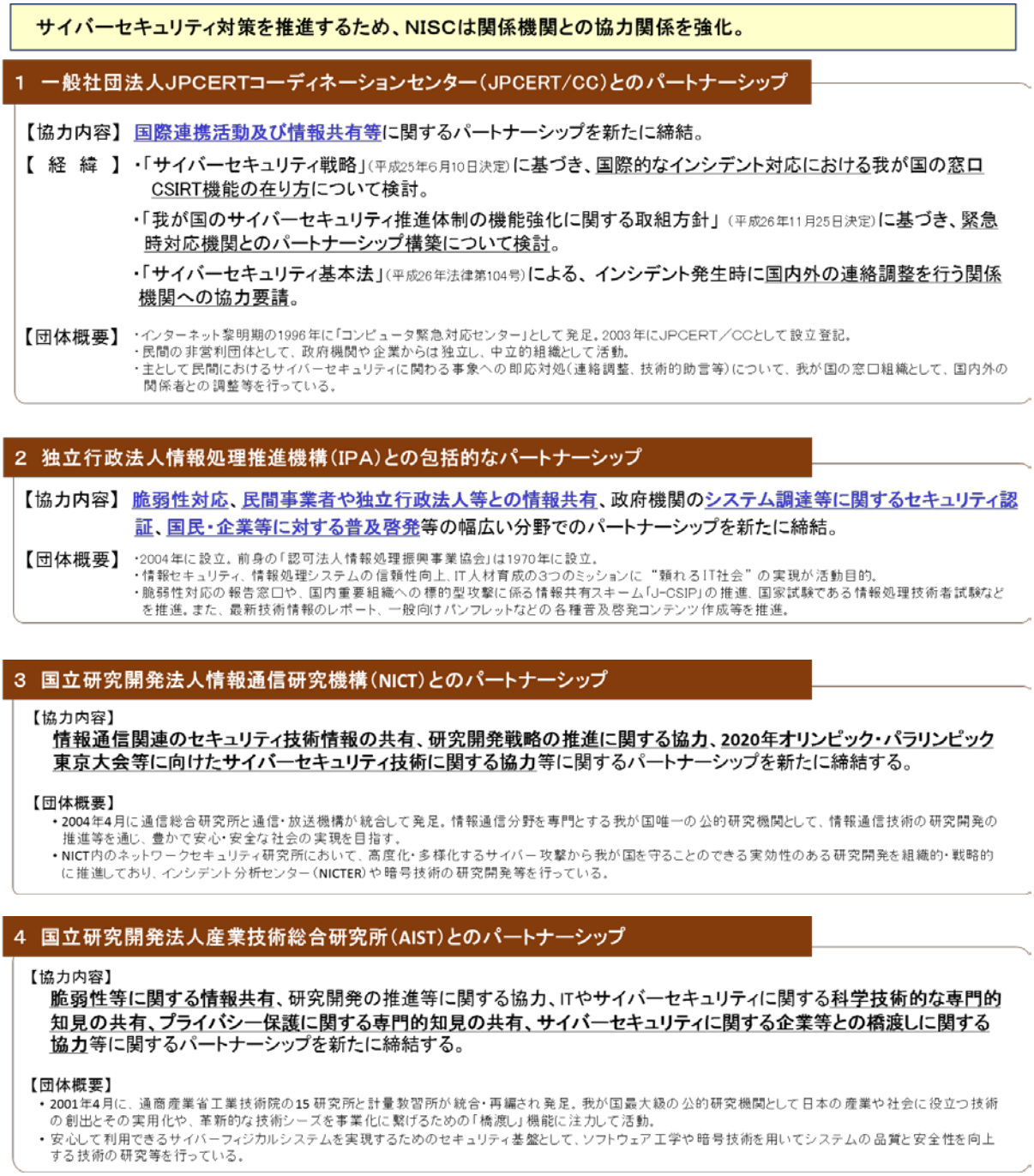


図表Ⅰ－3－5　内閣サイバーセキュリティセンター発足式の様子

また、内閣サイバーセキュリティセンターに関し、①政府機関等における情報システムに対する情報通信ネットワーク等を通じた不正な活動の監視及び分析を行うGSOC機能の強化、②諸外国の政策、サイバーセキュリティ上の脅威に関する情勢、サイバー攻撃に使用された技術等の統合的な分析機能の強化、③政府機関等や重要インフラ事業者等におけるインシデント情報等、国内外の情報集約機能の強化、④国際連携の強化、⑤政府内の人材育成機能の整備や任期付職員等による人材の確保について、2020年オリンピック・パラリンピック東京大会も見据えつつ、必要な措置について可及的速やかに検討することとした。

本取組方針に基づき、基本法が完全施行された2015年１月９日、戦略本部の設置と同時に、政府は内閣官房に内閣サイバーセキュリティセンターを設置し、統合的な分析等に必要な人材の確保を進め、サイバーセキュリティに係る緊急時対応関係機関とのパートナーシップを2015年２月及び2015年５月に構築するなど、具体的な機能強化の取組を実施した（図表Ⅰ－3－6）。

図表Ⅰ-3-6　関係機関とのパートナーシップ構築



(4)　新たなサイバーセキュリティ戦略の策定に向けて

政府は、基本法第12条に基づき、サイバーセキュリティに関する施策の総合的かつ効率的な推進を図るためにサイバーセキュリティ戦略を策定、閣議決定し、国会報告・公表をすることとなっている。これを受け、2015年２月10日に開催された第１回戦略本部会合において、安倍総理から、新たなサイバーセキュリティ戦略案（以下、「新戦略案」という。）の策定に向けた検討を開始すべき旨の指示があった。そして、2015年５月25日に開催された第２回戦略本部会合において、新戦略案をパブリックコメントに付した。しかしながら、日本年金機構の情報流出事案が発生したことから、この原因究明調査の結果を踏まえ必要な見直しを行った上で閣議決定する予定である。

第２回戦略本部会合においてパブリックコメントに付したこの新戦略案は、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り、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、新戦略案は、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。

図表Ⅰ－３－７　パブリックコメントに付した新たなサイバーセキュリティ戦略案の全体構成

(5)　その他主な政策の取組実績

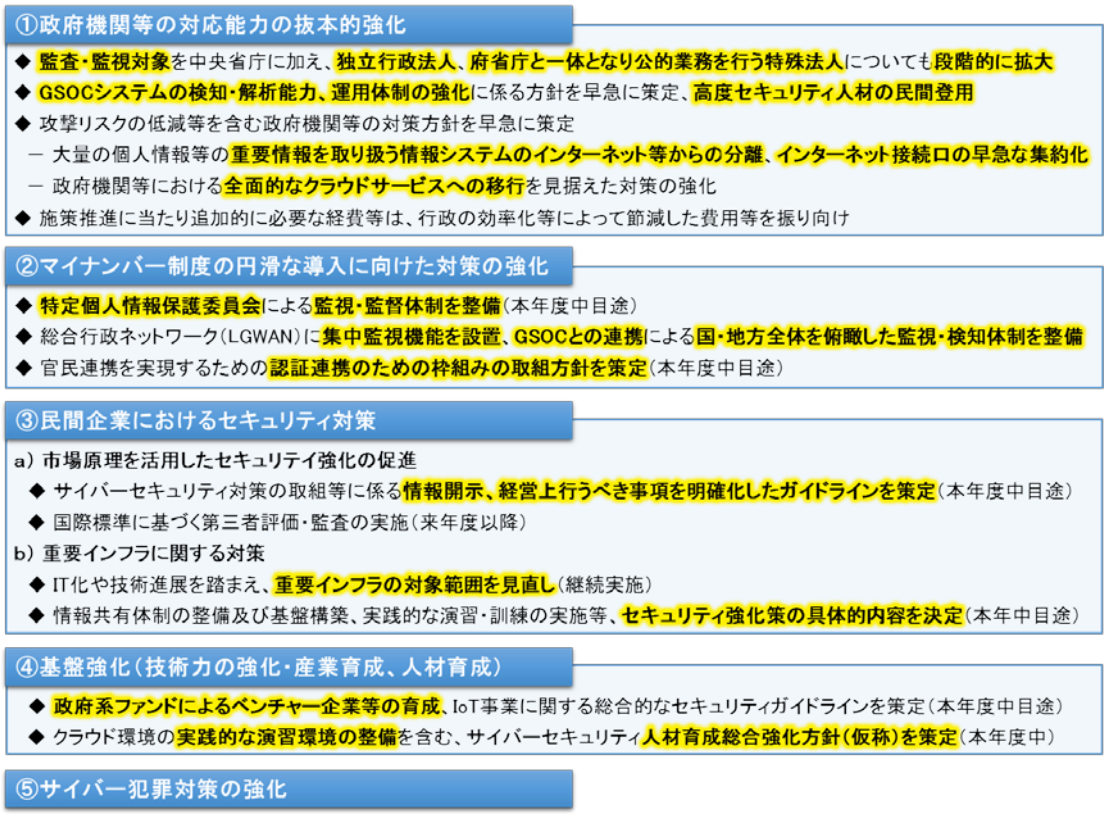
その他、主な取組について概説する。

ア　サイバーセキュリティ戦略以外の国家戦略

新たなサイバーセキュリティ戦略の検討と並行して、世界最高水準のIT社会を実現するためにもサイバーセキュリティの確保が必要であることから、2015年６月に閣議決定された「『日本再興戦略』改訂2015」及び「世界最先端IT国家創造宣言」においてもサイバーセキュリティに関する施策を掲げている。

具体的には、監査・監視対象を拡大することなどによる「政府機関等の対応能力の抜本的強化」や、総合行政ネットワーク（LGWAN）に集中監視機能を設置することなどの「マイナンバー制度の円滑な導入に向けた対策の強化」、経営上行うべき事項を明確化する等の「民間企業におけるセキュリティ対策」、政府系ファンドの活用等による「サイバーセキュリティの確保に向けた基盤強化（技術力の強化・産業育成、人材育成）」のほか、「サイバー犯罪対策の強化」といった施策が盛り込まれた（図表Ⅰ－３－８）。

図表Ⅰ－３－８　「『日本再興戦略』改訂 2015」におけるセキュリティ施策の概要



図表Ⅰ-3-9　民間企業のサイバーセキュリティリスク開示に係る動向

民間企業のサイバーセキュリティに関する情報開示の現状を把握するため、上場企業 225 社（日経 225）の有価証券報告書について、「事業等のリスク」へのサイバーセキュリティリスクの記載状況の調査を NISC において実施した（2014 年度委託調査「企業の情報セキュリティリスク開示に関する調査」。調査範囲は 2009 年度から 2013 年度までの５年間）。

調査の結果、サイバーセキュリティリスクを開示している企業数は、2009 年度の 116 社（52%）から 2013 年度の 136 社（60%）へと増加していることが確認された。また、業種によって開示率に大きくバラつきがあることや、サイバーセキュリティリスクについて記載しているものの、記載文書が５年間同一の企業が約半数（65 社）あること等の現状も明らかとなった。

調査対象企業のうち、個別にヒアリングを行った企業からは、情報開示について、経営者や各事業責任者等のリスク認識を高め、具体的なリスク及び対策を共有するうえで大きな効果があったとの意見があった。一方で、国等に対し、サイバーセキュリティリスクの開示に係るガイドラインの作成、開示を促進する指導、サイバー攻撃に関する情報やサイバー攻撃対策ガイド等の提供を要望する声もあった。

こうした結果を踏まえた所要の取組について、2015 年度以降進めていく予定である。

［2013 年度 日経 225 社 ― 業種別報開示状況］

日経業種分類				開示	開示企業%	
大分野	（社数）	中分野	（社数）	企業数	中分類	大分類
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	**100.0%**	
B 金融	21	**06 銀行**	11	11	**100.0%**	100.0%
		07 その他金融	1	1	**100.0%**	
		08 証券	3	3	**100.0%**	
		09 保険	6	6	**100.0%**	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	**100.0%**	
		13 サービス	7	5	71.4%	
D 素材	64	14 鉱業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	**100.0%**	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	**100.0%**	
		27 その他製造	3	3	**100.0%**	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	**100.0%**	
		31 海運	3	1	33.3%	
		32 空運	1	1	**100.0%**	
		33 倉庫	1	1	**100.0%**	
		34 電力	3	3	**100.0%**	
		35 ガス	2	2	**100.0%**	
合計	225		225	136		

イ　政府機関におけるサイバー攻撃対処訓練

2015年３月18日の「サイバーの日」に、サイバー攻撃対処を行う政府各機関の現場における実践的な能力向上に向け、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」が初めて実施された。

本訓練は、お互いに切磋琢磨する共通の場を新たに設けることで、現場力の向上をより一層加速させることを目的としており、総務省の実践的サイバー防御演習（CYDER）をベースとして、複数のマイルストーン（４区間）を設置し、タイムトライアル方式で競技が実施された。

参加省庁は12省庁（警察庁、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省及び防衛省）であったが、うち最速タイムの総合優勝として警察庁には官房長官表彰が、また、最もチームワークに秀でた金融庁には総務大臣表彰が授与された。

図表Ⅰ-3-10　NATIONAL ３１８（CYBER） EKIDEN の様子

［当日の様子］

［官房長官表彰］

ウ　サイバーセキュリティの普及啓発に関する取組

NISCは、その役割の一環として、広く国民のサイバーセキュリティに対する理解を深め、関心を高めるための普及啓発を推進している。特に、毎年、産学官民が連携して普及啓発活動を集中的に展開するキャンペーン期間を設けている。これまで２月を「情報セキュリティ月間」として取り組んできたが、2015年から、期間を２月１日から３月18日（「サイバーの日」）までに拡大するとともに、名称を「サイバーセキュリティ月間」に変更して取り組むこととした。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、政府のみならず、全国の自治体や公的機関、関連事業者・団体などにより、普及啓発に関する行事や関連キャンペーンなどの取組が多数開催された。

図表Ⅰ-3-11　「サイバーセキュリティ月間」ポスター

また、NISCが運営する「国民を守る情報セキュリティサイト」において、月間の特設ページを設け、都道府県別のイベント一覧や「情報セキュリティ９か条」リーフレット、スマートフォンやSNS の安全な利用に関するアニメーション動画など、各種コンテンツを掲載した。さらに、同サイトでは、多様な業種・地域でサイバーセキュリティに関する活動を行っている方々からのメッセージをコラムとして発信し、より一層多様な観点からの情報発信の場となった。

加えて、街中のカフェ等を活用してサイバーセキュリティについて学ぶ双方向型のセミナー「サイバーセキュリティカフェ」として、学生向けセミナーほか、日本学術会議が推進する「サイエンスカフェ」の枠組も活用した一般向けセミナーを開催し、いずれも講師と会場の活発なやりとりが展開された。

図表Ⅰ-3-12　サイバーセキュリティカフェの様子

このほか、大手ニュースサイトと連携した国民の意識調査を実施し、多くの回答を頂いた。国民のリテラシーを多様な手法で高めていくとともに、こうした調査によりその動向を定量的に把握していくことも今後の課題である。

エ　国際連携に関する取組

サイバー空間における脅威は、容易に国境を越え、もはや一国のみで対応することは極めて困難である。このため、我が国は、「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）に基づき、世界各国と協力関係を構築し、情報の自由な流通が確保された安全で信頼できるサイバー空間の構築に取り組んできた。

2014年度のサイバー分野における政府横断的な二国間協議では、前年度までに開催実績のある米国、英国との協議実施に加え、首脳会談等を端緒として、新たに、欧州連合、中韓（三カ国協議）、イスラエル、仏、エストニア、豪、露との協議を立ち上げた。これらの二国間協議では、サイバーセキュリティ戦略、重要インフラ防護、安全保障等、サイバー空間に関する幅広い議題を議論し、各国との連携・協力の強化や対話を通じた信頼醸成を進めている。また、特に米国との間では、インターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ、日米エネルギー戦略対話などの様々な枠組みの中でも、サイバーセキュリティ分野における緊密な連携を進めている。

ASEANとの関係では、2014年10月、第７回目となる日・ASEAN情報セキュリティ政策会議を主催し、共同意識啓発活動やサイバーセキュリティに関する研修、サイバー演習等の既存の取組を充実・高度化させるとともに、サイバーセキュリティに関する共同の政策文書である「日ASEANにおける重要インフラ防護に関するガイドライン」を策定した。同会議では、今後、これらの取組を継続しつつ、サイバーセキュリティ人材の育成等、日ASEAN間の連携を更に強化していくことで合意している。また、11月には、重要インフラ防護の多国間の枠組みであるMeridian会合を日本において開催し、各国の政府関係者とベストプ

ラクティスや政策動向等に関する情報共有を進めた。このほかにも、国連やOECD等におけるサイバー分野の国際会議に積極的に参加し、多国間での国際連携の強化に努めた。

図表Ⅰ-3-13　国際会合の様子

［第７回 日・ASEAN 情報セキュリティ政策会議］

［Meridian 会合］

我が国では情報セキュリティ上の課題に国際的に協力・連携して取り組む「情報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。本年度はASEANと共同での意識啓発グッズの作成や日ASEANの国際シンポジウムの開催といった既存の取組に加え、政府広報（政府インターネットテレビやFM番組、Web広告等）やSNS（日ASEAN共同で情報セキュリティに関する標語・電子ポスターを各国言語で作成・SNSを活用して配信）などのメディアをより積極的に活用し、効果的な広報に努めた。また、日米の連携により、学生や若手エンジニアをターゲットとしたシンポジウムを開催し、サイバーセキュリティ産業への将来世代の関心と理解の向上に努めた。

図表Ⅰ-3-14　2014 年度情報セキュリティ国際キャンペーンの活動について

政府広報予算を活用したメディアでの情報発信

- 政府インターネットTVによる動画制作・配信

政府インターネットテレビ

- FMラジオ番組の制作・放送・配信
（10月19日JFN系で全国放送，Webサイトから番組配信中）

Weekly ニッポン!!

- 新聞広告 / インターネット広告
（ニュースサイトへのWeb広告，70の全国紙・地方紙への新聞広告の実施）

国際連携による共同意識啓発活動

- 情報セキュリティTips及び電子ポスター(日英及びASEAN各国語)をASEAN各国と共同制作。SNS等で配信(我が国では10月の平日，毎日異なる画像をNISC Twitterアカウントから配信)

例）左：日本語版，右：タイ語版

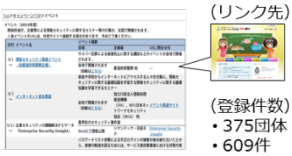
- 3回目となる日ASEAN情報セキュリティ国際シンポジウムに加え，新たに若手向けの日米サイバーセキュリティシンポジウムを開催

日米

日ASEAN

関係団体・各省庁等によるイベント開催・ウェブ上での協力

- 関連イベント開催と情報の登録



（リンク先）

（登録件数）
・375団体
・609件

- リンクバナーの掲載

関連団体・各省庁等のウェブサイトでのNISC「国民を守る情報セキュリティサイト」へのリンクバナー掲載

（バナー掲載先）
・官公庁：23機関，
・公益法人等：9団体
・一般企業：12社
・海外：3団体

オ　オリンピック・パラリンピック東京大会に関する取組

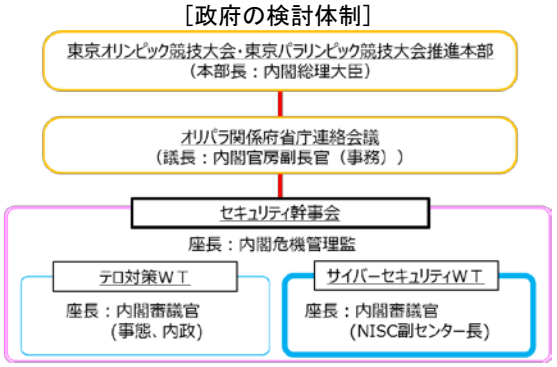
2020年オリンピック・パラリンピック東京大会の開催に向けて、2014年４月には全閣僚を構成員とする2020年オリンピック・パラリンピック東京大会等に関する閣僚会議が設置された。サイバーセキュリティについて万全の態勢で臨むことは我が国の重要な責務であるとの認識の下、同会議の下に関係省庁による「セキュリティ幹事会」及びNISC副センター長を座長とする「サイバーセキュリティワーキングチーム（WT）」を設置し、検討を進めている。

なお、2015年６月には「平成三十二年東京オリンピック競技大会・東京パラリンピック競技大会特別措置法」が施行され、専任の担当大臣が新設されるとともに、総理大臣を本部長とする東京オリンピック競技大会・東京パラリンピック競技大会推進本部及び同事務局が設置された。

図表Ⅰ-３-15　2020 年オリンピック・パラリンピック東京大会に向けた検討

［推進本部事務局設置の様子］

［政府の検討体制］



Ⅱ　政府機関における取組と評価

1　政府機関全体における情報セキュリティ対策に関する取組

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[28]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。

(1)　外部からの攻撃等の情報セキュリティインシデントへの対処等に係る取組

Ⅰ章で述べたとおり、標的型攻撃を始めとする外部からの攻撃に係る脅威は深刻であることから、政府機関においては重層的な防御策に加え、情報セキュリティインシデントへの対処等のための様々な取組を総合的に深化させていくことがより重要となっている。

外部からの攻撃においては、情報システムの脆弱性が悪用される場合が多いことから、まず、構築時から運用時に至るまで情報システムの脆弱性を極力排除し、情報セキュリティを確保することが重要といえる。このためNISCでは、情報セキュリティを企画・設計段階から確保するための方策（SBD：Security By Design）として「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[29]」を策定するとともに、同マニュアルの利用を推奨しており、2014年度は、引き続き、それらに係る勉強会を各府省庁において開催し、その普及促進を図ったほか、政府統一基準群の改定を踏まえ、同マニュアルについても改定を行い、サプライチェーン・リスクに対応するための調達要件の強化等を行った。また、情報システムの運用時における脆弱性対策の徹底を図るため、各府省庁がインターネット上で公開しているウェブサーバを対象とした脆弱性検査を継続しており、各府省庁においては、当該検査により検出された問題を踏まえ、必要な対策を実施した[30]。加えて、NISCから各府省庁に「情報システムで利用しているソフトウェアのサポート終了に伴う対応について（注意喚起）」[31]を発出し、情報システムで利用しているソフトウェアについて、脆弱性を残したまま運用することのないよう、各府省庁に適切な運用の徹底を求めた。

次に、近年多くみられる攻撃手口である標的型攻撃に対応するため、未然防止に関する取組として、一般的な不正プログラム対策に加え、電子メールサーバについて送信ドメイン認証技術を用いた、不審メールのなりすまし防止策の導入を推進[32]している。また、高度化する標的型攻撃に対応するため、その標的とされる蓋然性が高い業務・情報に係るリスク評価に基づく対策の重点化による多重防御の実現に向けた取組を本格実施した[33]。他方、この取組は費用を要することから、適切なリソースの配分を含め最高情報セキュリティ責任者の主体的な関与が重要となる。このため、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（議長：杉田内閣官房副長官））において、標的型攻撃の実演を行い、サイバー攻撃による情報窃取の脅威や対策の重要性・必要性について改めて認識の共有を図った。

---

[28] 「別添２　「サイバーセキュリティ 2014」に盛り込まれた施策の実施状況」の１①を参照。
[29] 「「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について」（NISC、2015 年５月 22 日公表）http://www.nisc.go.jp/active/general/sbd_sakutei.html
[30] 「別添３－７　公開ウェブサーバの脆弱性検査結果の概要」を参照。
[31] 「別添３－１０　NISC 発出注意喚起文書及び情報セキュリティ対策推進会議決定等」を参照。
[32] 「別添３－６　なりすまし防止策の実施状況」を参照。
[33] 「別添３－４　高度サイバー攻撃への対処」を参照。

さらに、サイバー攻撃等により情報セキュリティインシデントが発生した場合への備えとして、各府省庁のCSIRTの対処能力の向上に資するため、情報セキュリティインシデントの発生時における連絡・報告等の対処に係る訓練を実施した[34]。また、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）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。

2013年度と同様に、2014年度においても独立行政法人が標的となったサイバー攻撃事案が発生している[35]こと、また独立行政法人では政府機関と同様に重要な情報を取り扱っている場合があること、独立行政法人等への攻撃は政府機関に対する標的型攻撃を行うための情報収集を目的とした準備行動である可能性があること等から、独立行政法人においても情報セキュリティ対策の強化を図ることが重要である[36]。このため、独立行政法人制度の改革も踏まえつつ、独立行政法人においても、政府統一基準群を含む政府機関における情報セキュリティ対策を踏まえた対策を講じることによりセキュリティの強化を進めることを2014年６月に決定し[37]、これを踏まえた対策を推進した。

(2)　IT の利用動向の変化に伴う新たな課題等への対応に係る取組

昨今、利用者が意図しない形で情報が流出するといった問題が発生するなど、ITの利用動向の変化に伴う新たな課題等が浮上しており、これら課題について政府機関全体として対応を進めている。

2014年５月に改定した政府統一基準群（平成26年度版）においては、私物を含めたスマートフォンの利用に関する対策やソーシャルメディアサービス、グループメールサービスの利用に関する対策、複合機等のネットワーク接続機器に関する対策の強化を行ったところであり、各府省庁においては、改定内容を踏まえて、それぞれの府省庁ポリシーの見直しを行い、2015年度の早い時期から新ポリシーに基づいた運用を開始できるよう、準備を進めた。NISCにおいては、各府省庁が新たな政府統一基準群に準拠した府省庁対策基準等の情報セキュリティ関係規程が適切に定められるよう、スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書を始めとするマニュアルの整備等の支援を行った[38]。

また、政府機関から外部に送信されたメールについて、外部の受信者側において民間のオンライン翻訳サイトを利用したことに伴い当該メールの内容が閲覧可能な状態になっていた事例を踏まえ、「ネット上の外部サービス利用による情報漏出の危険性について（注意喚起）」[39]を発出し、ネット上で無料提供されているサービスの利用に当たって、意図しない形での情報流出が生じないよう、各府省庁に対し注意喚起を行うなど、政府機関全体として適切な対応に努めた。

政府機関において利活用が進むクラウドサービスに関しては、政府機関が利用する際に心得るべきセキュリティ上の観点を整理するために研究会を立ち上げ、将来的な政府統一基準

[34] 「別添３－５　教育・訓練に係る取組」を参照。
[35] 「別添３－１１　政府機関等に係る 2014 年度の情報セキュリティインシデント一覧」を参照。
[36] 「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」を参照。
[37] 「別添３－１０　NISC 発出注意喚起文書及び情報セキュリティ対策推進会議決定等」を参照。
[38] 「別添３－１　政府統一基準群による対策の推進」
[39] 「別添３－１０　NISC 発出注意喚起文書及び情報セキュリティ対策推進会議決定等」を参照。

群への反映を念頭に置きつつ、適切にセキュリティを確保した上でクラウドサービスを利活用するための対策要件の検討を進めている[40]。

(3)　情報セキュリティ対策に係る教育

組織の情報セキュリティ水準の維持・向上には、情報や情報システムを取り扱う職員一人ひとりの情報セキュリティに対する意識の向上が欠かせない。

各府省庁において、情報セキュリティポリシー浸透のための教育を原則として自組織の全職員に対して実施するとともに、NISCにおいては、上述の各府省庁CSIRT要員に対する訓練のほか、全府省庁や独立行政法人の情報セキュリティ担当職員等を対象とする勉強会（NISC情報セキュリティ勉強会[41]）を定例で開催している。

2014年度のNISC情報セキュリティ勉強会においては、外部の有識者を講師として招き、「情報システムに係るサプライチェーン・リスクの事例と問題点」や「行政機関におけるスマホアプリ開発の注意点」をテーマとして開催するなど、最近の脅威やその対策等に関する教育・意識啓発を行った。また、独立行政法人職員を対象とした勉強会も引き続き実施することにより、独立行政法人職員への知識普及・意識啓発も行った。これら勉強会への参加者数は増加を続けており、各組織の関心の高さがうかがえる。

(4)　サイバーセキュリティ基本法の施行等に伴う取組

ア　サイバーセキュリティ基本法の施行に伴う取組

サイバーセキュリティ基本法により、「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の作成及び当該基準に基づく施策の評価（監査を含む。）」がサイバーセキュリティ戦略本部の事務と規定された。監査は、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対策を強化するため、マネジメント監査やペネトレーションテストを通じて、これら機関における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を目的としている。

2014年度から各府省庁に対して監査の前提となる実地調査等を開始しているところ、2015年度には監査の基本方針策定、試行監査の実施、制度設計等を行い（監査の基本方針については、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）、各府省庁との情報交換を通じて、必要に応じ改善策の助言も行っていくこととしている[42]。

また、政府機関における情報セキュリティ対策の推進を図るため各府省庁最高情報セキュリティ責任者等から構成される「情報セキュリティ対策推進会議」（議長：杉田内閣官房副長官）は、同法の施行に伴いサイバーセキュリティ戦略本部令（平成26年政令第400号）第４条の規定に基づき、第１回サイバーセキュリティ戦略本部会合での審議を経てサイバーセキュリティ戦略本部長により「サイバーセキュリティ対策推進会議」（議長：杉田内閣官房副長官）として改組された。

---

[40] 「別添３－３　クラウドサービスの利用に係る対策」を参照。
[41] 「別添３－５　教育・訓練に係る取組」を参照。
[42] 「別添３－２　サイバーセキュリティ基本法に基づく監査」を参照。

イ　「行政文書の管理に関するガイドライン」の改正に伴う取組

秘密文書について、従前の「秘密文書等の取扱いについて」（昭和40年４月15日事務次官等会議申合せ）を廃止し、改めて秘密文書の管理のルールを公文書管理法の下で整理することとされ、2015年１月、「行政文書の管理に関するガイドライン」（内閣総理大臣決定）の改正が行われた。これに伴い、政府統一基準群における「機密性３情報」の分類の基準における「秘密文書」を同ガイドラインの定めによる「秘密文書」とすることや、同ガイドラインで規定する秘密文書の表示や保存等との扱いと政府統一基準群との関係が整合性のあるものとして整理された。それらを解説するため、「行政文書の管理に関するガイドラインの一部改正に伴う政府機関の情報セキュリティ対策のための統一基準の扱いについて」（2015年１月23日内閣官房副長官）[43]を発出し、情報セキュリティポリシーの運用について周知を図った。

[43] 「別添３－１０　NISC 発出注意喚起文書及び情報セキュリティ対策推進会議決定等」を参照。

2　政府機関全体としての対策状況の評価

各府省庁においては、自らが取り扱う情報のオーナーとしてその管理に責任を持ち、それぞれの業務や取り扱う情報、情報システムの特性に応じて、職員の教育や情報システムに関する技術的な対策等を講ずることにより情報セキュリティを確保することが基本原則である。NISCではこれら対策状況を把握し、政府機関全体として情報セキュリティを確保し、その改善を図ることを目的として、各府省庁の取組について評価を行っている。

本節では、2014年度における各府省庁の取組についての評価結果を報告する。

(1)　対策実施状況に係る評価

ア　目的

対策実施状況に係る評価は、各府省庁における情報セキュリティ対策が適切に実施されているかについて把握し、取組が不十分なものについて改善を図るなどするため、政府機関全体としてその実施状況を分析・評価することを目的とするものである。

イ　評価の対象

対策実施状況に係る評価の対象を、図表Ⅱ－２－１に示す。

図表Ⅱ－２－１　対策実施状況に係る評価の対象

主体	対象者	評価項目
最高情報セキュリティ責任者 統括情報セキュリティ責任者 情報セキュリティ責任者 課室情報セキュリティ責任者 情報システムセキュリティ責任者 情報システムセキュリティ管理者 行政事務従事者	左記に掲げる主体の全員※ ※長期休暇中等の理由により、各府省庁が設定した自己点検の期間内に、責務が発生しなかった者は、対象には含まない。	政府機関の情報セキュリティ対策のための統一規範のうちNISCが指定した項目

2014年度の本評価の対象者については、政府統一基準群に定める役割を担う主体のうち、主たるものを指定し、それらの主体の全員としている。対象項目については、近年発生したインシデントを踏まえつつ、情報の取扱い等の日常的に実施が求められる基本的な対策や、情報システムにおいて特に実施が求められる対策、これまでの対策実施状況の評価結果において実施率が低い対策等を考慮して指定した。

ウ　実施期間

2014年８月から2015年２月まで
（自己点検の実施時期については、各府省庁において設定）

エ　実施方法

各府省庁は、政府統一基準群に基づく府省庁対策基準に規定される自己点検・監査等を実施することにより、府省庁対策基準に基づき情報セキュリティ対策が適切に実施されているかについて把握する。

NISCは、各府省庁が把握した対策実施状況のうち、上述した対象に関するものを集計し、その集計結果を分析・評価した。

オ　政府機関全体の評価

（ア）　対策実施状況

2014年度の政府機関全体の対策実施状況は以下のとおり。

○　主体別の把握率の状況

主体別の把握率（評価の対象とした者のうち、対策実施状況が把握できた者の割合）を図表Ⅱ－２－２に示す。

図表Ⅱ－２－２　主体別の把握率

全主体平均	責任者等	システム責任者等	行政事務従事者
98.4%	99.4%	99.4%	98.4%

※　把握率の集計においては、最高情報セキュリティ責任者・統括情報セキュリティ責任者・情報セキュリティ責任者・課室情報セキュリティ責任者を合わせて「責任者等」として、情報システムセキュリティ責任者・情報システムセキュリティ管理者を合わせて「システム責任者等」として扱う。実施率についても同じ。
※　政府機関全体での平均値を算出しているため、人数比を考慮した平均値とは一致しない。

○　主体別の実施率の状況

主体別の実施率（把握した者のうち、責務が生じた者に占める対策を実施した者の割合）及びその推移、評価項目別の実施率のうち行政事務従事者に係る主な項目の結果をそれぞれ図表Ⅱ－２－３及び図表Ⅱ－２－４に示す。

図表Ⅱ－２－３　主体別の実施率及びその推移

	2012年度	2013年度	2014年度
責任者等	99.6%	99.3%	99.7%
システム責任者等	97.9%	98.3%	97.8%
行政事務従事者	96.8%	96.8%	97.1%
全主体平均	98.9%	98.6%	98.7%

図表Ⅱ－２－４　行政事務従事者の主な評価項目の実施率

評価項目	実施率
情報の作成と入手 ※情報の格付・取扱制限の決定・明示等	91.8%
情報の利用	99.0%
主体認証情報の管理	97.4%
府省庁支給以外の情報システム	96.2%
不正プログラムの感染防止対策	98.4%

（イ）　所見

全主体平均の把握率は98.4%となっており、今回の報告対象が政府機関の全ての行政事務従事者であることに鑑みれば、前年度に引き続いて、全体的に高い水準を維持していると考えられる。しかしながら、中には前年度に引き続いて、把握率が十分でない組織もみられた。自組織の対策の実施状況を把握することは、PDCAサイクルのC（Check）のプロセスに該当し、情報セキュリティ水準の維持・向上に不可欠な取組であることか

ら、該当する組織においては全ての行政事務従事者に対して自己点検の実施徹底を図るなど、自組織の対策の実施状況を十分に把握するための改善を図る必要がある。

責任者等の実施率は99.7%となっており、対策の浸透が認められる。しかしながら、一部の組織においては、責任者等による、対策実施状況の結果の分析・評価の実施率が低いところがみられた。情報セキュリティ関係規定の遵守状況等を点検・分析・評価した上で適時改善を図らなければ、情報セキュリティ対策の実効性を継続的に担保することは困難であることから、着実に実施していく必要がある。

システム責任者等の実施率は97.8%となっており、対策の浸透が認められる。ただし、行政事務を遂行するに当たって活用することが必要不可欠となっている情報システムに関する対策については、情報システムのライフサイクル全般（計画、構築・運用、移行・廃棄及び見直しの各段階）にわたって適切に実施されなければ十分とはいえないことから、更なる浸透に努める必要がある。

行政事務従事者の実施率は97.1%となっており、対策の浸透が認められる。全体としては、高い水準を維持しているが、評価項目のうち、「情報の作成と入手」については、前年度の実施率よりも下がっている組織が複数みられた。情報の作成及び入手はあらゆる行政事務の様々な場面に関係するものであることから、その際における対策が不十分な組織については、速やかに改善を図る必要がある。

各府省庁が自己点検等により把握した対策実施状況からは、全体として一定の対策の浸透がみられると評価できる。一方で、上述したように対策が十分には実施されていないとみられる点もあることに加え、全体として一定の対策の浸透がみられると評価できる状況は前年度以前から続いており、自己による点検を基に評価を行っていることを勘案すると、点検が場合によっては形式的になることにより継続的改善の停滞が生じている可能性や、対策や点検項目の内容に対する行政事務従事者の理解不足等の影響を受けている可能性も排除できないと考えられる。

したがって今後は、現状として把握されている課題のみならず、これまで把握されていない課題も存在し得るとの認識の下、サイバーセキュリティ戦略本部による第三者的な視点からの各府省庁に対する監査[44]等を実施し、セキュリティ対策の一層の推進を図っていくこととする。

[44] 「別添３－２　サイバーセキュリティ基本法に基づく監査」を参照。

(2)　重点検査による評価

ア　重点検査の目的

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。

イ　検査期間

2014年８月から2015年２月まで
（検査基準日：2014年10月１日）

ウ　主な検査内容と結果

図表Ⅱ－２－５　重点検査の主な検査内容と結果

対　象	検査項目	検査項目とした理由	実施率※
公開ウェブサーバ等	インターネットからアクセスされる情報システムの脆弱性対策の確認状況	ウェブサーバ、メールサーバ等で使用する基本的なソフトウェアにおいて、近年重大な脆弱性が発見されており、インターネットからアクセスされる情報システムを対象に、脆弱性対策の確認状況を把握するため。	99%
	SQL インジェクション脆弱性がある可能性についての確認状況	NISC が実施した政府機関の公開ウェブサーバに対する脆弱性検査において、過去に検出された SQL インジェクション脆弱性対策の実施状況を把握するため。	94%
電子メール	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。	65%

※小数点以下四捨五入

エ　所見

インターネットからアクセスされる情報システム全数のうちの99%について、2014年度中に、脆弱性対策が講じられたソフトウェア（バージョン）を使用しているか確認することや検査業者等による脆弱性診断を実施するなどにより、脆弱性対策状況の確認が行われた、又は確認を行う計画があることを把握した。比較的高水準で実施されているといえるが、本来は100%実施されるべきものであり、残る１%の情報システムについても、重点検査の実施後に改善を図った。

情報の漏えいや改ざんの被害につながる危険性の高いSQLインジェクション脆弱性について、前年度に引き続き検査を実施した。検査基準日の時点において、確認を行ったのは、SQLインジェクション脆弱性が技術的に存在し得るウェブサイトを持つ情報システム全数のうちの94%であったが、残る６%の情報システムについても、重点検査の実施後に確認状況の改善を図った。また、当該確認の結果、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、迅速に対処を完了した。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検出されたことから、今後も、SQLインジェクション脆弱性への対策を強化していく必要がある。

インターネットから電子メールを受信する電子メールシステムについて、受信側における送信ドメイン認証技術の実施率は65％であり、昨年度と比較してわずかではあるが改善がみられた。これは、各府省庁において、電子メールシステムの集約化が大きく進んだこと等が影響しているものと推測される。受信側における送信ドメイン認証技術の導入には電子メールシステムへの機能追加が必要となるため、一定程度の予算措置が必要ではあるものの、自組織が受信した電子メールが送信元をなりすました不審メールであるかを検知し、不審メールのフィルタリング等に活用できる技術であることから、着実に導入を進めることが重要である。

オ　その他の課題

今般の重点検査では、その他の課題として官支給品、私物のスマートフォン・タブレット端末の府省庁における利用動向、ソーシャルメディアサービスの利用動向及びパブリッククラウド[45]サービスの府省庁における利用動向についても調査を行った。

官支給品のスマートフォン・タブレット端末の利用動向について、スマートフォン・タブレット端末の利用目的を調査したところ、出張先や外出先等での業務利用に加えて、特定の情報システムの専用端末として利用されていることやペーパーレス会議を行うために導入されていることなどが把握された。また、セキュリティ対策の実施状況については、ソフトウェアの最新化、ウイルス対策ソフトウェアの導入、セキュリティロックの設定等の基本的な対策は、前年度と同様、おおむね実施されていることが確認された。今後も政府機関においてスマートフォン・タブレット端末が様々な業務で利活用されることが予想されることから、組織や取り扱う情報の特性等に応じて適切なセキュリティ対策を実施していくことが重要である。

また、官支給品に加えて私物のスマートフォン・タブレット端末の利用動向について調査した。その結果、大半の府省庁で私物端末の利用可否を組織としてポリシー等に定めていることが確認されたが、明確な規定が無い府省庁も少数ながら確認された。私物端末を業務利用するに当たっては、官支給品と同等の対策水準を保つ必要があることから、組織として私物端末の利用可否をポリシーとして明確化することが重要であり、業務利用を許可する場合、禁止する場合いずれにおいても適切な運用管理体制の下でセキュリティ水準が確保されるよう、引き続き対策を推進する必要がある。

ソーシャルメディアサービスの利用動向については、政府機関の情報発信等を目的に府省庁が組織的に利用しているソーシャルメディアサービスのアカウントを対象にセキュリティ対策の実施状況等について調査した。なりすまし対策として有効な認証アカウントの利用状況については、認証アカウントが利用できるにもかかわらず利用していないアカウントが多数確認されたことから、改善を進める必要がある。また、運用ルールの整備状況について調査した結果、書き込み内容の事前チェックや端末及び担当者を限定するなどのセキュリティに係る運用ルールがおおむね考慮されているが、一部のアカウントで運用ルールを定めず利用されている状況が確認された。今後、明確な運用ルールの下でソーシャルメディアサービスが利用されるよう、継続的に対策強化する必要がある。

[45] 仮想化技術等を用い、インターネット等を経由し不特定多数の契約者（組織）が物理的なIT資源（サーバ、ストレージ、OS、アプリケーション等）を共用して利用するもの。

パブリッククラウドサービスの府省庁における利用動向については、前年度同様、外部への情報発信及び情報共有といった用途が主流である一方で、行政サービスの提供等といったほかの使い方もみられるなど、パブリッククラウドの利用目的に関し、多様化の兆しが見え始めていることが把握された。

また、パブリッククラウドサービスを利用して実施する行政事務における情報の取扱い状況についても、パブリッククラウドサービスを利用する情報システム全数のうち、政府統一基準群で定める要機密情報を取り扱わない割合が前年度と比べて増加したことや、要機密情報を取り扱う全てのシステムがその情報の保存場所を国内に限定していることが確認された。

パブリッククラウドサービスの利用における情報セキュリティ対策については、前年度と比較して、一システム当たりにおいて講じられている対策数が平均で約1.4倍となり、各府省庁における委託先による情報へのアクセスの制限、情報の改ざんや消失等への対策、情報システムに障害が発生した場合等の復旧対策に加えて、公的認定資格を有する第三者によるセキュリティの評価を受けることをSLA（Service Level Agreement）により要求するなど、情報システムの特性に応じた多様な対策が実施されている状況がみられた。

なお、パブリッククラウドサービスの利用に当たっては、調達や運用の観点からのセキュリティ対策を検討する研究会[46]を実施しており、今後は当該研究会の結果を踏まえ、さらに適切な対策が講じられるよう、検討を進めていく。

[46] 「別添３－３　クラウドサービスの利用に係る対策」を参照。

Ⅲ　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、2014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。

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

2014年度は、第３次行動計画の期初年度に当たるため、広報広聴活動（防護基盤の強化）を中心として、分野横断的演習の検討会（障害対応体制の強化）やセプターカウンシル（情報共有体制の強化）等の幅広い機会を捉えて、第３次行動計画の考え方や施策内容について周知を図った。

また、第３次行動計画策定の際に重要インフラ分野として新たに追加した３分野（化学・クレジット・石油の各分野）については、内閣官房において重要インフラ所管省庁と連携しながらIT依存度調査（リスクマネジメント）を実施して分野の特性把握の支援を行った。更に新規３分野における防護対象範囲の確定や、緊急連絡体制の整備等についても、内閣官房と重要インフラ所管省庁に加え既存分野のセプター（情報共有体制の強化）が必要な助言を行うことで、年度内にその整備等を実施した。防護対象範囲や緊急連絡体制等については、第３次行動計画の記載事項であることから、2015年５月には当該部分を追記するための第３次行動計画の改訂をサイバーセキュリティ戦略本部において実施した。

第３次行動計画の各施策については、その他詳細は次節に示すものの、安全基準等策定指針の改訂（安全基準等の整備及び浸透）や、過去最大規模の分野横断的演習の開催（障害対応体制の強化）などを実施したほか、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４－８）。

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変化としては、サイバーセキュリティ基本法が、2014年11月に成立・一部施行した。同法における重要社会基盤事業者（いわゆる重要インフラ事業者）の責務として、サービスの安定的かつ適切な提供や、自主的・積極的な取組が求められており（法第６条）、これは第３次行動計画における重要インフラ防護の目的や基本的な考え方と符合するものである。国の施策としては、基準の策定、演習及び訓練、情報の共有そ

の他の自主的な取組の促進等が謳われており（法第14条）、それについても第３次行動計画の施策と合致する。よって、サイバーセキュリティ基本法は第３次行動計画における強力な推進役となるものである。

2015年１月に、同法は全面施行され、新たにサイバーセキュリティ戦略本部が設置された。これにより、これまで我が国全体の重要インフラ防護について議論を行ってきた情報セキュリティ政策会議の重要インフラ専門委員会は、サイバーセキュリティ戦略本部令第４条の規定に基づき、第１回サイバーセキュリティ戦略本部会合での審議を経て、同本部の重要インフラ専門調査会として改組された。よって、同専門調査会で審議し、同本部決定となる第３次行動計画についても、その位置付けが明確になり訴求力が向上している。

ところで、同法においては、重要インフラの一つである地方公共団体について、その位置付けの特殊性から、他の重要インフラ事業者等より一段高い対応や国との連携を求めている。これに対応するため、内閣官房と総務省が連携しながら、必要な情報提供等の協力を行っているところである。

(3)　今後の取組

第３次行動計画に基づく取組については、2015年度以降も引き続き推進し、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。

一方で、政府機関のみならず、重要インフラ事業者等においても、サイバー攻撃はますます高度化・複雑化しており、標的型攻撃を始めとする外部からの攻撃に係る脅威は益々深刻化している。加えて、地方公共団体におけるマイナンバー制度の導入や、制御系機器のオープン化などの環境変化も急激に進んでいる。

そうした状況を踏まえ、また、サイバーセキュリティ基本法の規定により、新たなサイバーセキュリティ戦略を策定しているところである。同戦略の策定後は、必要に応じて第３次行動計画の改定を行いながら、既存の第３次行動計画を補完するものとして、同戦略に謳われる事項を実現するための取組を行っていく。

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通りである。

＜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、同指針の改訂と合わせ、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。

○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４－２）。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、新規３分野において新たに安全基準等を定めた。

○安全基準等の浸透状況等調査

重要インフラ事業者等における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４－３）。

今年度の調査においては、アンケート方式により具体的な対策状況の確認を可能とすることに加え、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に調査項目の見直しを行った。加えて、アンケート調査を補完するため、新たに往訪による調査を実施して、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、第３次行動計画が目指す経営層の在り方等についての現状を明示するとともに、収集した課題及び良好事例を掲載できるように構成を見直した。なお、アンケート調査は3,228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

2014年度の取組結果を活用し、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より充実させる。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通りである。

＜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等を取り決めた上で、情報共有体制を構築・運営した。2014年度は、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151件の情報連絡が行われ、内閣官房からは38件の情報提供を行った（参考：別添４－４）。

図表Ⅲ－２－１　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
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
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
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

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、内閣官房（事態対処・危機管理担当）及び関係省庁と連携し、2015年３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関係主体における対応の検証を実施した。

○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、新たに追加した３分野（化学・クレジット・石油の各分野）を含めて13分野で18セプターが設置されている（参考：別添４－５）。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における会議体であり、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、2014年４月の総会で決定した活動方針に基づき、2014年度に、企画運営WG（10回）、相互理解WG（３回）、情報共有WG（４回）、情報収集WG（５回）、総会準備WG（５回）及び幹事会（６回）を開催し、セプター間の情報共有の一層の充実や、自律的な運営体制確保のための検討等を図った。加えて、セプターカウンシルの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反映が必要であることを踏まえ、サイバー空間関連事業者等との連携強化も含め、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ため、自律的な運営体制とそれによる活性化を目指すため、企画・運営の在り方等に係る検討を支援していく。

(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通りである。

＜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・連絡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「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４－６）。

新たに追加した３分野を含む全13分野が演習に参加し、2012年度分野横断的演習と比較すると、参加機関数は約2.2倍（42組織→94組織）、参加者数は約2.4倍（148名→348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・交換の機会の充実を図った。

図表Ⅲ－２－２　過去３年間の分野横断的演習参加機関・参加者数

年度	2012	2013	2014
参加機関数	42組織	61組織	94組織
内、大阪会場参加			（10組織）
内、自職場参加	（３組織）	（３組織）	（15組織）
参加者数	148名	212名	348名
内、大阪会場参加			（32名）
内、自職場参加	（15名）	（10名）	（59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100％（有意義だった：55.6％、概ね有意義だった：44.4％）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61.9％、今後実施予定が6.3％であった。また、組織外で実施する演習への参加率は58.7％、今後参加予定は6.3％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４－７）。

図表Ⅲ-２-３　過去３年間のセプター訓練参加セプター・参加事業者数

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

実施に当たっては、2013年度までのセプター訓練が「片道」訓練（内閣官房からの情報提供のみ）であったのに対し、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」訓練とした。また、各セプターからの要望も取り込み、抜き打ち実施や通知情報の具体化等の訓練内容の充実も図った。

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。

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、事業者等の内規の策定・見直しや対策の実施・改善に資する運営の見直し・追加に係る検討、参加対象の裾野拡大に資する会場新設・既存会場等の改善に係る検討、情報共有体制の実効性の向上に係る検討・運用見直しへの支援について取り組む。

セプター訓練については、これまで実施してきた標準フォーマットに基づく訓練に加え、各セプターの課題意識等、実情に合った訓練メニューを提示することで、各セプターの実情及び要望をより踏まえた「カスタマイズ型訓練」を実施し、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。

(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通りである。

＜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

新たに追加した３分野である、化学分野、クレジット分野及び石油分野を対象に、相互依存性解析と密接に関連するITへの依存度に関する調査１件を行った。調査結果は当該３分野に個別に提供するとともに、それ以外の重要インフラ事業者等に対しても2015

年３月にその概要を公表[47]・共有している。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IT依存に関する考え方や、類似の情報システムを利用する際の情報セキュリティ上の注意点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（２回）をそれぞれ開催した。また、重要インフラ専門委員会及び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。

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、2014年度においては実施しておらず、実施の必要性も含め、環境変化を踏まえて引き続き検討する。また、重要インフラ事業者等は、各自がリスクマネジメントを実施しており、各関係主体間における共通的なリスクマネジメントの考え方や用語による情報共有や議論がなされておらず、第３次行動計画の各種取組が各重要インフラ事業者等のリスクマネジメントにおいて効果的に活かされない可能性がある。そのため、各自のリスクマネジメントにおいて共通的に利活用することができる手引書等の提供についても検討する。

(5)　防護基盤の強化

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

＜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。

[47] 重要インフラ分野の変化に基づく IT 依存度に関する調査報告書
http://www.nisc.go.jp/conference/cs/ciip/dai01/pdf/01sankoushiryou02.pdf

NISCのWebサイトについて、第３次行動計画の策定やサイバーセキュリティ基本法の施行に伴った修正を行うとともに、重要インフラ専門委員会及び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。

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に広く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[48]。

そのほか、前述の安全基準等策定指針の改訂に係る意見公募等を2015年２月に実施して、広く一般からの意見を集めた。

○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、Meridian会合を2014年11月に日本で開催し、重要インフラ防護等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するとともに、2015年４月のサイバー空間に関するハーグ会議（Global Conference on CyberSpace 2015）において、その成果を報告した。また、Meridian会合の開催に合わせて、各国の重要インフラ防護担当者に対し制御システムセキュリティセンター（CSSC）を紹介し、制御システムセキュリティの重要性について共有した。加えて、IWWN総会を2014年５月に日本で開催し、国際的なサイバー攻撃や脆弱性対応についての情報を共有した。

日・ASEANにおいては、重要インフラ防護専門家パネル会合（2014年１月に東京、同年２月にクアラルンプール、同年５月にタイ）を開催し、重要インフラ防護に関するベストプラクティスや日・ASEANにおける重要インフラ防護について議論するとともに、2014年10月の日・ASEAN情報セキュリティ政策会議において、日・ASEANにおける重要インフラ防護に関するガイドラインを策定した。また、2015年２月にジャカルタにおいて、日・ASEAN重要インフラ防護ワーキンググループ（重要インフラ防護専門家パネル会合から改称）を実施、重要インフラ防護に関する国際協力について協議を継続している。加えて、日・ASEANセキュリティシンポジウムを2014年10月に日本で開催し、国際連携の取組等を公表した。

二国間協議については、米、EU、イスラエル、仏、英、エストニア、豪、露等と、重要インフラ防護における我が国及び相手各国の取組等について情報交換を実施した。

そのほか、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）、海外の重要インフラ防護担当者向けの研修（１回）、重要インフラ防護に関する海外講演（１回）をそれぞれ実施した。

[48] https://youtu.be/jZk47olgy8U

〇規格・標準及び参照すべき規程類の整備

関係主体が重要インフラにおける情報セキュリティ対策を検討する上で、関連文書や関連規定を必要なときに参照できるようにすること等を実現するため、重要インフラ防護に関する諸国の枠組み等に関する調査報告書をまとめ、その概要版を2015年３月に公表した[49]。同調査において、我が国の重要インフラ防護に適用する場合の手引書等の整備（2015年度予定）のため、欧米の重要インフラ防護に関する情報セキュリティの関連規定・国際標準等の抽出を実施したほか、欧米の重要インフラ防護の政策的・実効的枠組みを整理した。

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、国際的標準化機関であるIECやCAB（IECの下部組織。適合性評価評議会。）への提案調整を継続して実施している。また、相互認証の拡大に向け、国際認証推進組織であるISCIと、制御システム全体の認証制度（SSA認証）の効果的な実施手順に関して継続的に協議している。

イ　今後の取組

広報広聴活動については、WebサイトやNISC重要インフラニュースレターを通じて、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行うとともに、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等について、2014年度に抽出した情報セキュリティの関連規定・国際標準等を参考に、検討を進める。また、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も、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。

[49] 重要インフラ防護に関する諸国の枠組み等に関する調査報告書
http://www.nisc.go.jp/conference/cs/ciip/dai01/pdf/01sankoushiryou03.pdf

Ⅳ　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」に基づき策定された２期目の年次計画である「サイバーセキュリティ2014」に掲載された諸施策について、「サイバーセキュリティ政策の評価等の基本方針」及び「平成26年度サイバーセキュリティ政策の評価等の実施方針」に則り、その成果や進捗状況等を取りまとめたものである。

「サイバーセキュリティ2014」においては、戦略の体系に沿って各府省庁のサイバーセキュリティ政策に関係する具体的な取組が掲載されており、これらの取組は以下に示すとおり着実に進捗しており、おおむね所期の成果を挙げたと判断される[50]。

しかしながら、今後もあらゆる活動においてサイバー空間への依存が高まり、サイバー空間を取り巻くリスクの深刻化が一段と進むと想定され、マイナンバーや2020年オリンピック・パラリンピック東京大会に向けた検討の進展によっては、新たな課題への対応が必要となることも予想される。このような中で、我が国の成長戦略の柱の一つとして掲げられた「世界最高水準のIT利活用社会」を実現するためには、本評価も踏まえて、別途策定される2015年度の年次計画「サイバーセキュリティ2015」に沿って、各分野で策定等された政府機関統一基準群、重要インフラにおける第３次行動計画、国際連携取組方針等に基づき、個々の施策について、具体化・深化させて推進していくとともに、引き続き適切なPDCAサイクルを回していくことが必要である。

１　「強靭な」サイバー空間の構築

①　政府機関等における対策

【総　評】

2014年５月の政府統一基準群の改定の内容を踏まえて、各府省庁において府省庁対策基準の見直しを行い、対策を強化するとともに、高度化する標的型攻撃に対応するため、その標的とされる蓋然性が高い業務・情報に係るリスク評価による対策の重点化を行ったほか、クラウドサービスの利用に係る対策の検討や独立行政法人の情報セキュリティ対策の推進、政府機関全体で情報セキュリティインシデントの発生時における連絡・報告等の対処に係る訓練を実施するなど、各種施策を実施した。（取組の状況については、Ⅱ章参照。）

加えて、地方公共団体の情報セキュリティ対策水準向上のための普及・啓発の推進、「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」の改定等による政府調達における情報セキュリティの確保に係る取組を実施した。

【課　題】

標的型攻撃を始めとするサイバー攻撃の高度化・深刻化を踏まえ、サイバー攻撃を前提とした情報システムの防御力を、攻撃側に勝る速度で強化することに加え、政府機関全体としてのサイバーセキュリティに関する情報共有及び政府機関内外における連携に関する体制強化も求められる。また、サイバーセキュリティ基本法を踏まえ、サイバーセキュリティ戦略本部による各府省庁等に対する監査に係る制度の早急な立ち上げを図り、これら組織におけるサイバーセキュリティ対策の状況及びPDCAサイクルが有効に機能しているかとの観点から

[50] 個別施策の進捗状況等については、「別添２　「サイバーセキュリティ 2014」に盛り込まれた施策の実施状況」を参照。

検証し、改善を図ることも必要である。また、これらを含む必要な措置について、新たに策定されるサイバーセキュリティ戦略に盛り込み取組を加速する。

②　重要インフラ事業者等における対策

【総　評】

2014年度は、第３次行動計画の期初年度に当たるため、広報広聴活動等により第３次行動計画の考え方や施策内容について周知を図ったほか、新たに追加した重要インフラ３分野について、重要インフラ分野として活動するために必要な支援・助言を行った。また、第３次行動計画の各施策である、「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」についても着実な取組を行った。

【課　題】

政府機関のみならず、重要インフラ事業者等においても、サイバー攻撃はますます高度化・複雑化しており、標的型攻撃を始めとする外部からの攻撃に係る脅威は依然として深刻である。加えて、地方公共団体におけるマイナンバー制度の導入や、制御系機器のオープン化などの環境変化も急激に進んでいる。このような中で、第３次行動計画の各施策を引き続き推進するとともに、新たに策定されるサイバーセキュリティ戦略に基づき各種取組を行っていく必要がある。

③　企業・研究機関等における対策

【総　評】

強靭なサイバー空間の構築に向け、企業・研究機関等においても情報セキュリティ対策の強化が推進されるよう、政府として支援を行った。

具体的には、情報セキュリティに関する指導者育成セミナーや対策ガイドライン等を通じた中小企業における情報セキュリティ対策の推進、情報セキュリティ対策に資する各種ツール・分析等の提供、個人情報保護制度やガイドラインの見直し、経営層向けセミナーの開催、大学に対する情報セキュリティに関する最新情報の提供等の取組を実施した。

【課　題】

個人情報や営業秘密、知的財産情報等の重要な情報を取り扱う企業や教育・研究機関において、セキュリティ対策の向上、経営層の意識改革、組織能力の向上や、サイバーセキュリティ関連産業の振興、公正なビジネス環境の整備、我が国企業の国際展開のための環境整備などが必要となってくる。そのために必要な取り組みを推進していく必要がある。

④　サイバー空間の衛生

【総　評】

国民全体の情報セキュリティに関する関心・理解度の向上に向け、2014年７月に情報セキュリティ政策会議において「新・情報セキュリティ普及啓発プログラム」を決定した。2015年２月の「情報セキュリティ月間」については、新たに「サイバーセキュリティ月間」として、期間を２月１日から３月18日までに拡大展開し、街中のカフェを活用した双方向型のセミナー「サイバーセキュリティカフェ」のほか、大手ニュースサイトと連携した国民の意識

調査、全国の関連行事の都道府県別掲載による情報発信など、国民一人一人に訴求するための新たな取り組みを実施した。そのほか、2014年10月の「情報セキュリティ国際キャンペーン」については、国際連携・協力の推進に資する取り組みとして、ASEAN諸国と共作したTipsのTwitterでの日次配信および日ASEAN共作ポスターのほか、新聞広告、ラジオ放送、動画などの周知用素材による情報発信に努めた。また、ASEAN諸国と連携した意識啓発をテーマとしたシンポジウム、および米国と連携した若手層のサイバーセキュリティへの関心喚起を目的としたシンポジウムをそれぞれ日本で開催した。

【課　題】

「新・情報セキュリティ普及・啓発プログラム」に基づく「サイバーセキュリティ月間」等を通じ、産学官民が連携した取組が行われるなど、一定の成果が見られた。他方、こうした産学官民各主体が連携した普及啓発活動について、その活動の成果として国民の関心・理解度がどの程度向上したのか、取組の効果を測定できる意識指標等についても検討を進める必要がある。

⑤　サイバー空間の犯罪対策

【総　評】

警察庁にサイバーセキュリティ対策を担当する長官官房審議官及び長官官房参事官が新設され、司令塔機能が強化されるとともに、警察大学校に捜査員に対する専門的な研修等を行う「サイバーセキュリティ研究・研修センター」が新設されるなど、サイバー空間の脅威に対し、警察全体の対処能力向上のための基盤強化が図られている。また、日本版NCFTA（一般財団法人日本サイバー犯罪対策センター（JC3））が創設されるなど、サイバー犯罪対策に係る産学官の連携が強化された。

【課　題】

インターネットバンキングに係る不正送金事犯による被害が拡大し続け、2014年には過去最悪になるなど、サイバー空間における脅威はますます深刻化しており、「「世界一安全な日本」創造戦略（2013年12月）」などに掲げられた施策を着実に推進し、サイバー空間における様々な事態への対処能力の強化に不断に取り組む必要がある。

⑥　サイバー空間の防衛

【総　評】

サイバー攻撃の未然防止に資するよう情報収集機能を強化するとともに、サイバー攻撃発生時に重要通信の経路を確保し被害拡大を防止するための取組やサイバー演習環境の構築に向けた取組を着実に進めているほか、米国をはじめとする諸外国との連携強化に向けた取組を実施した。また、防衛省・自衛隊と防衛産業との間でサイバー攻撃関連情報に関する情報共有や共同訓練の実施により官民の連携に向けた取組が強化された。

【課　題】

国全体として対応能力の一層の強化を図るためには、内閣サイバーセキュリティセンターにおいて、GSOC 機能の強化、総合的分析機能の強化、国内外の情報集約機能の強化、国際連携の強化、人材の育成及び登用を取り組むとともに、関係府省庁の個々の能力・態勢強化

に向けた取組の推進に加え、「国家安全保障戦略（2013 年 12 月）」等に基づいた組織・分野横断的な取組を総合的に推進していく必要がある。

２　「活力ある」サイバー空間の構築

①　産業活性化

【総　評】

新たな成長市場を取り込み、新たなリスクに対し、より的確かつ迅速に対応していくためには、海外の技術、サービスや製品への依存度が高い我が国のサイバーセキュリティ産業について、国際競争力を強化することが必要である。

産業活性化の具体的取組として、M2Mにおける情報セキュリティの確保に関する検討及び研究開発の推進、新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発、クラウドコンピューティングの国際標準化に向けた取組等が実施された。

【課　題】

様々なモノがネットワークに接続されるIoTシステムが今後広がっていくことを踏まえ、安全なIoTシステムを活用した新規事業の振興、IoTシステムのセキュリティに係る制度整備、必要な技術開発・実証事業を進めていく必要がある。

また、セキュリティマインドを持った企業経営の推進を促すとともに、セキュリティに係るビジネス環境の整備に向け、サイバーセキュリティに関連する制度の見直し、サイバーセキュリティ関連産業の育成支援、国際的な標準規格や評価・認証制度等の我が国企業の国際展開のための環境整備を進めていく必要がある。

②　研究開発

【総　評】

サイバーセキュリティ戦略や昨今のサイバーセキュリティを取り巻く環境変化、技術戦略専門委員会での議論なども踏まえ、2014年７月に「情報セキュリティ研究開発戦略（改定版）」を策定のうえ、総務省、経済産業省などの関係省庁やNICT、AISTなどの国立研究開発法人、制御システムセキュリティセンター等でセキュリティの研究開発を推進した。

また、サイバーセキュリティ戦略本部の下に、「研究開発戦略専門調査会」を2015年２月に設置した。同会合にて、IoTセキュリティに関する議論などを行った。

【課　題】

サイバー攻撃の複雑・巧妙化に伴い、変化の激しい情勢に適切に対応できる、創意と工夫に満ちた情報セキュリティ技術を生み出していくことが重要である。

そのための研究開発を引き続き実施していく必要があり、「情報セキュリティ研究開発戦略（改定版）」に基づき、サイバー攻撃の検知・防御能力の向上、情報セキュリティのコア技術の保持等の各種研究開発を引き続き推進していく。

③　人材育成

【総　評】

サイバーセキュリティ戦略等を踏まえ、「新・情報セキュリティ人材育成プログラム」の策定に係る検討を情報セキュリティ政策会議の下の普及啓発・人材育成専門委員会において実施し、2014年５月、情報セキュリティ政策会議において同プログラムを決定した。本プログラムも踏まえ、複数大学や産学連携による高度で実践的な教育活動が引き続き推進されるとともに、国立高等専門学校におけるサイバーセキュリティに関する教育プログラムの開発が開始された。また、情報セキュリティに係る競技会では、海外からの参加者も初めて対象とするなど、情報セキュリティ人材の育成に資する施策が着実に展開された。

また、企業向けセミナーの開催等を通じ、経営層に対し、セキュリティを組織の経営戦略の一環として認識させ、人材も含め積極的な投資を促すとともに、経済団体との連携を強化し、人材確保の重要性を訴求した。

【課　題】

サイバー空間の脅威がさらに深刻化する中、人材不足は引き続き重要な課題となっており、人材の需要と供給の好循環の実現に向け、これまで以上に力を入れて取り組んでいく必要がある。具体的には、サイバーセキュリティに関する人材の育成や発掘だけでなく、育成された人材の登用、その後のキャリアパス構築までを総合的に見据えた取組を、産学官がそれぞれの立場で役割を発揮し、一体となって推進していくことが求められる。また、実践的な演習環境の整備や教材の産学官共同開発、人材の実践的な能力を適時適切に評価できる試験制度の充実も今後の課題である。

④　リテラシー向上

【総　評】

国民全体の情報セキュリティに関するリテラシー向上に向け、2014年７月に決定した「新・情報セキュリティ普及・啓発プログラム」に沿って、各種の普及啓発施策を着実に推進した。具体的には、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、高齢者等リテラシーの強化が必要とされる層に向けたウェブサイトやリーフレットなどを通じた啓発、相談窓口の紹介等を通じた普及啓発活動が展開された。また、国民一人一人に身近な活動が国及び地域でさらに促進されるよう、事業者や各種団体、学識経験者等により構成する「情報セキュリティ社会推進協議会」を、NISCが事務局となり新たに設置した。

【課　題】

「新・情報セキュリティ普及・啓発プログラム」に基づき、特にスマートフォンなどを取り巻く情報セキュリティ上の問題やその対策について、国民の様々な層を対象とした普及啓発施策が推進された。今後、国民に身近な地域における普及啓発活動のより一層の活性化や、一人一人の確実な実践につながる普及啓発活動の推進が課題である。また、そうした活動の成果として国民のリテラシーがどの程度向上したのか、取組の効果を測定できる意識指標等についても検討を進める必要がある。

3　「世界を率先する」サイバー空間の構築

①　外交

【総　評】

2013年10月に策定した「サイバーセキュリティ国際連携取組方針」に基づき、前年度までに開催実績のある米国、英国との協議実施に加え、首脳会談等を端緒に、新たに欧州連合、中韓（三カ国）、イスラエル、仏、エストニア、豪、露との協議を立ち上げ、サイバーセキュリティ戦略、重要インフラ防護、安全保障等、サイバー空間に関する幅広い議題を議論し、各国との連携協力の強化や対話を通じた信頼醸成を推進した。特に米国との間では、日米サイバー対話に加え、インターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ、日米エネルギー戦略対話などの様々な枠組も活用し、サイバーセキュリティ分野における緊密な連携を推進した。また、「国際安全保障の文脈における情報及び電気通信分野の進展」に関する政府専門家会合（国連サイバーGGE）の第４回期会合に政府専門家を派遣し、サイバー空間における国際法の適用の検討などに貢献した。加えて、サイバーセキュリティに関する国際会議であるMeridian会合やIWWN年次会合を我が国で開催し、各国の関係機関とのベストプラクティスや政策動向に関する情報共有等を進め、国際連携の強化に努めた。

【課　題】

複雑化・巧妙化するサイバー空間の脅威に対応するため、今後、海外連携先との情報共有や人材育成等における協力を強化していく必要がある。また、国連サイバーGGEの議論を踏まえ、サイバー空間における国際的な法の支配を確立に向け貢献していく必要がある。加えて、多国間の場や各国との協議において、サイバー空間に関する国際的な信頼醸成を進めていく必要がある。

②　国際展開

【総　評】

ASEAN諸国との間で、日・ASEAN情報セキュリティ政策会議の枠組みの下、サイバーセキュリティに関する研修や共同での意識啓発活動、サイバー事案発生時における情報連絡演習等の取組を継続しつつ、日ASEANにおける重要インフラ防護に関するガイドラインを共同で策定するなど、新たな取組を推進した。これらに加え、日ASEANサイバー犯罪対策対話等の国際会議や、JPCERT/CCを通じたアジア地域やアフリカ地域におけるCSIRT構築支援の活動等、海外におけるキャパシティビルディングに率先して貢献し、ASEAN地域等と共に成長できる関係の構築に努めた。

産業面では、評価・認証を含むサイバーセキュリティに関連する国際標準化活動の支援や海外主要国との共同研究開発等により、我が国サイバーセキュリティ産業の国際展開に向けたビジネス環境の整備を推進した。

【課　題】

昨今の複雑化、高度化、そしてグローバル化しているサイバー空間の脅威に対処するにあたっては我が国自身の対処能力の強化のみならず、諸外国のキャパシティビルディング支援

と連携を強化していく必要がある。また、国際標準化活動や先端的技術分野における国際的な共同プロジェクトなどを引き続き推進していく必要がある。

③　国際連携

【総　評】

アジア大洋州地域サイバー犯罪捜査技術会議などの様々な国際的な枠組を通じ、サイバー犯罪捜査技術力の向上や諸外国の法執行機関等との連携を強化した。また、日・ASEAN情報セキュリティ政策会議、Meridian、IWWN、FIRSTなどの各種国際会議への参加や諸外国関係機関との情報交換を通じ、我が国のサイバーセキュリティ基本法や重要インフラ防護における取組の発信や、サイバー攻撃対策を推進するための情報交換を行った。加えてサイバー犯罪条約の普及に向けた活動の推進や各国との国際捜査共助を推進した。

【課　題】

昨今のサイバー空間は、経済活動のみならず、安全保障やインテリジェンス活動の舞台ともなっており、これらに対応するため、外国政府機関との情報共有を含む情報収集・情勢分析機能の強化を図る必要がある。また、非政府主体によるサイバー空間の悪用に対し、対策を講じていく必要がある。加えて、国境を越えるサイバー犯罪への対策に向け、サイバー犯罪条約の加盟国の拡大や二国間の国際捜査共助の取組を強化していく必要がある。

4　推進体制等

【総　評】

2014年11月にサイバーセキュリティ基本法が成立したことを踏まえ、情報セキュリティ政策会議において「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」を決定した。また、本取組方針に基づき、2015年１月、内閣に「サイバーセキュリティ戦略本部」を、内閣官房にサイバーセキュリティ戦略本部の事務局となる「内閣サイバーセキュリティセンター」を設置した。

【課　題】

「政府機関等における情報システムに対する情報通信ネットワーク等を通じた不正な活動の監視及び分析を行うGSOC機能の強化」、「諸外国の政策、サイバーセキュリティ上の脅威に関する情勢、サイバー攻撃に使用された技術等の統合的な分析機能の強化」、「政府機関等や重要インフラ事業者等におけるインシデント情報等、国内外の情報集約機能の強化」、「国際連携の強化」、「政府内の人材育成機能の整備や任期付職員等による人材の確保」については今後の課題であり、必要な措置について継続して検討する必要がある。

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2015年度当初までに定めた「対策推進計画」を基として、2014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2015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

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
河内　隆

2014年度においては、暗号化技術の一つとして幅広く利用されているプロトコルや、UNIXで幅広く用いられている基本ソフトウェアに脆弱性が発見されるなど、従来、何も問題がないと考えられてきた部分に脆弱性が発見され、影響度が大きい情報セキュリティ事案が発生した。一方、公開Webサイトにおいては、大手企業各社が外国の代替アクセスサービスを経由するアクセスを、模倣Webサイトが存在するものと誤認し、「模倣サイトに注意」といった注意喚起を自社のWebサイト利用者に対し行うような事案も発生している。

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、2013年度の約380件に対し2014年度は約780件と、前年比において２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、世の中で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2015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

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
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。

2014年度においては、全職員を対象とした情報セキュリティ研修、NISCから送付される不審メール情報の全職員への周知及び注意喚起、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の実施、当局独自の全職員を対象とした標的型メール攻撃に係る訓練並びにCSIRT構成員を対象としたインシデント訓練などによって教育・啓発を行ったほか、NISCからの情報セキュリティについての情報提供及び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）での決定事項等に迅速かつ適切に対応した。また、職員の情報セキュリティ対策に係る自己点検・監査及び政府統一基準群に係る重点的検査を実施したが、その結果については問題となるところはなかった。このような取組、対策等を実施した結果、内閣法制局における情報セキュリティ対策は、堅牢性を強化することができたと評価している。

2015年度においては、2014年度に実施した取組等への評価結果及び新たな脅威の出現、技術の進歩等への対応を踏まえ、また、NISCからの情報提供やサイバーセキュリティ対策推進会議での決定事項等に応じて、引き続き、適切な情報セキュリティ対策を実施する。特に、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、他府省との電子メールの送受信における情報セキュリティ対策に注意することが重要と考えられるため、昨年度に引き続き、全職員に対し、情報セキュリティ教育、不審メール情報の周知、標的型攻撃メールに対処するための教育や訓練の実施等により、インシデントの発生防止を図る。また、CSIRT構成員に対するインシデント発生時の対応訓練を実施するほか、政府統一基準群の改定を踏まえた内閣法制局情報セキュリティポリシーの改定を行う。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

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
千葉　恭裕

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、NISC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。

近年の情報通信技術の急速な進歩により、システムの利便性が高まってきている一方で、不正アクセスや新しい形のサイバー攻撃による情報漏えいのリスクや脅威は増大するなど、情報セキュリティをめぐる状況は、日々変化するとともに情報セキュリティ対策の重要性はますます高まってきている。

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利用するためには、組織として積極的に情報セキュリティ対策に取り組む必要がある。

2014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を徹底させるために、全職員にe-ラーニング等による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、全職員を対象とする標的型メール攻撃に対する訓練を行い、結果と対処方法について情報セキュリティ責任者を通じて全職員に周知するなど、改めて情報セキュリティ対策の徹底を行った。

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。

2015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高度化・巧妙化しているところ、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、技術的対策に加え、職員の的確な対応が求められることから、情報セキュリティに対する意識を更に向上させることが重要となる。行政事務従事者としてだけでなく、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意識の向上に取り組むこととする。

内閣府

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
幸田　徳之

内閣府においては、昨年度抜本的に改定された「政府機関の情報セキュリティ対策のための統一基準群」（2014年５月19日 情報セキュリティ政策会議決定ほか。以下「政府統一基準群」という。）を踏まえ、当該政府統一基準群に準拠した新たな「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。）を策定したところである。

今年度においては、情報セキュリティの基本であるポリシーの理解・遵守の徹底のため、全ての職員に対し、情報セキュリティ対策の重要性について、報道等で取りざたされている情報セキュリティインシデント等を事例として紹介しながら、引き続き情報セキュリティ教育システム（e-ラーニング）を活用した教育や、新採用職員研修における講義などにより周知徹底を図ることとする。

近年より増加傾向にあり、攻撃手法が複雑化・巧妙化している標的型攻撃や、政府関係機関において普及啓発活動、広報活動などの情報発信のための利用が増加したソーシャルネットワーキングサービスを含むソーシャルメディアサービス（以下「SMS」という。）など、情報セキュリティを取り巻く情勢の変化に対応するため、政府統一基準群に新たに標的型攻撃対策、SMSによる情報発信等の項目が追加されたことにより、次の二点について重点を置くこととする。

① 標的型攻撃対策については、日々高度化する攻撃手法に対応するため、高度サイバー攻撃対処のためのリスク評価による独立行政法人情報処理推進機構（IPA）の対策セットを可能な限り実装し、攻撃事例やその対処法に関する情報を常に注視するとともに、標的型メール攻撃の対処法に関する教育など、実例を踏まえた対処情報、基本的対処を職員に周知する。

② SMSによる情報発信については、政府統一基準群で示されていることを基にしたSMS等を利用する為のルールによる手続きの周知徹底を図り、SMS利用にあたっての管理を適切に行うとともに、障害事故防止に努めることとする。

今後の情報セキュリティに関する情勢及び技術動向、新たに策定されるサイバーセキュリティ戦略などを踏まえ、NISCとの更なる連携強化を図ると共に、個別の取組による効果的な情報セキュリティ対策を講じていくこととする。

宮内庁

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
和田　裕生

宮内庁は、内閣総理大臣の管理の下にあって、皇室関係の国家事務を担い、業務で取り扱う情報や情報システムも多岐にわたる。

昨今は、政府機関等を対象としたサイバー攻撃が頻発しており、また、攻撃の手法も巧妙化・複雑化している状況にあるが、そのような中で、宮内庁としてもサイバー攻撃に迅速かつ適切に対処し、高い情報セキュリティ水準を維持していくためには、人的な対策と技術的な対策の両方を継続的に実施していくことが重要となる。

2014年度においては、主に以下の対策を実施した。

○　外部電磁的記録媒体の利用制限

使用可能な外部電磁的記録媒体は官給のセキュアUSBメモリ等に限定する旨をルール化し、使用承認のない外部電磁的記録媒体については、端末に接続しても使用できなくなるシステム上の措置を実施した。

○　宮内庁ネットワークシステムにおける技術的対策の強化

宮内庁ネットワークシステムの更新に際し、運用管理セグメントと他のセグメントの分離を行うとともに、アクセスログの収集・分析を行うためのソフトウェアを導入した。

○　ネットワークを介したバックアップシステムの導入

災害・事故等における情報システムの運用継続を確保するため、ネットワークを介して遠隔地にバックアップを行うシステムを導入した。

○　宮内庁情報セキュリティポリシー等の整備

政府機関の情報セキュリティ対策のための統一基準群の改定を踏まえ、宮内庁情報セキュリティポリシーや各種手順書等の整備を行った。

なお、2014年度は、宮内庁において情報セキュリティインシデントは発生していない。

2015年度においては、行政事務従事者の教育の充実を図り、更なるレベルの向上を目指す。具体的には、研修等の機会を通じて、新たに整備した宮内庁情報セキュリティポリシーや各種手順書の内容を周知するほか、標的型攻撃を想定した対処訓練を実施し、訓練結果に応じて指導・研修を実施するなどのPDCAサイクルの推進を図る。

また、引き続き、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、必要な対策については速やかに措置を行い、より一層の情報セキュリティ対策の向上に努めていく。

公正取引委員会

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
山本　佐和子

１　2014年度の総合評価

(1) 全体方針の取組実績

職員に対する情報セキュリティ対策を促すために、実施すべき対策の周知や研修を実施し、不審メールによる攻撃への対策として、職員への不審メール情報の発信、教育及び訓練を実施した。また、2014年度に改定された政府統一基準に準拠した、公正取引委員会情報セキュリティポリシー等を策定した。

(2) 教育・啓発に関する取組状況

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、これに加えて集合研修も実施しており、職員の情報セキュリティ対策の理解向上に寄与した。

また、政府機関等に対して、標的型メール攻撃が増大していることを受け、職員への不審メールによる攻撃に係る教育に取り組み、その結果を踏まえて、全職員に対し、巧妙化する標的型メール攻撃への意識向上を図った。

(3) 自己点検・監査の結果

2013年度の自己点検結果を踏まえ、2014年度の職員の情報セキュリティ対策の実施状況の改善に取り組んだ結果、ほとんどの点検項目について実施していることが確認できており、相当程度高い情報セキュリティ対策の実施が確認された。

(4) NISCによる重点検査や脆弱性検査の結果

情報システムに関するNISCによる重点検査では、いずれの調査項目においても、特段の問題がないことを確認した。

また、当委員会の情報システムのうち、インターネットに公開しているウェブサイトについての脆弱性検査を行ったところ、特段の問題のないことを確認した。

(5) 2014年度に発生した情報セキュリティインシデント

当委員会を装ったなりすましメールが発生したため、当委員会のホームページにおいて、注意喚起等を行った。

２　総合評価を踏まえた方針

以下の目標に重点的に取り組むことによって、情報セキュリティレベルの更なる向上を図る。

○　職員に情報セキュリティ対策の実施を促すため、自己点検結果等を踏まえて、職員が実施すべき対策の周知、研修内容の見直し等を行う。

○　不審メールによる攻撃への対策として、職員への不審メール情報の発信、教育、訓練等を行う。特に、標的型メール攻撃による情報流出を防止するため、全職員を対象とした標的型メール攻撃訓練を実施する。

○　情報セキュリティ対策上の役割別に、情報セキュリティ対策のために遵守すべき事項の実施状況について確認するため、自己点検等を行う。

○　2014年度に改定された政府統一基準に準拠した、新たな公正取引委員会情報セキュリティポリシー等を策定したことから、政府統一基準と公正取引委員会情報セキュリティポリシー等の整合性について監査する。

警察庁

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ管理者
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。

2014年度においては、標的型メール攻撃の手口が巧妙化している情勢等に鑑み、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脆弱性検査を実施し、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。

2015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を実施していく。また、従前の情報セキュリティ対策に加えて、サイバー攻撃の標的とされる可能性の高い業務やそこで取り扱う情報の重要度を踏まえ、組織として特に守るべきシステムを選定し、重点的に対策を講じていくこととする。

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。

金融庁

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
小野　尚

近年、情報通信技術の進歩により情報システムの利便性が高まる一方、標的型メール攻撃に象徴されるようにウィルス感染や不正アクセスにより情報漏えい等のリスクが増大している。特に、ここ数年、政府機関に対するサイバー攻撃は、攻撃手口が高度化・巧妙化している中、攻撃件数が大幅に増加し、攻撃主体が多様化する等、その脅威が増大している。

このような状況を踏まえ、2014年度、政府においては、「サイバーセキュリティ戦略」に基づく年次計画である「サイバーセキュリティ2014」が制定され、また、「サイバーセキュリティ基本法」等に基づき「サイバーセキュリティ戦略本部」や「内閣サイバーセキュリティセンター」(以下「NISC」という。）が設置される等、情報セキュリティに係る一層の態勢強化が図られている。

金融庁としても、従来から情報セキュリティの重要性を強く認識し、積極的に取組を進めているところであるが、当庁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、更なる技術的対策を実施するとともに、職員一人一人がその脅威や攻撃が発生した場合の社会的影響を認識し、情報セキュリティに対する意識を維持・向上させていくことが重要と考えている。

以上を踏まえ、2015年度においては、NISC等の関係機関との連携を緊密に図りながら、職員の教育、自己点検、情報セキュリティ監査、技術的対策の実施等の取組を推進するとともに、PDCAサイクルの実施を徹底することにより一層の情報セキュリティの強化に努めていく。

消費者庁

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
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。

2014年度は「政府機関の情報セキュリティ対策のための統一基準群」の改定を受け、情報セキュリティポリシーの見直しを実施した。また当庁情報システムの根幹となる消費者庁ネットワークシステムを更改し、行政事務遂行の利便性を向上させるとともに、システム的な情報セキュリティ対策の強化を図った。

2014年度の評価として、自己点検の実施率、到達率を前年度から継続して100.0%を達成したこと及び情報セキュリティインシデントが発生しなかったことから、当庁の情報セキュリティマネジメントは有効に機能しているものと考えられるが、引き続き緊張感を持って対応していくことが必要である。

そこで2015年度は、職員の情報セキュリティ対策に対する更なる意識向上を目的として、今年度改定した情報セキュリティポリシーの周知徹底に取り組む。また技術面において「高度サイバー攻撃対処のためのリスク評価等のガイドライン」に基づく当庁情報システムにおける対策導入計画に基づく対策を確実に遂行する。

2015年度末には、消費者庁において庁舎移転が予定されており、これらを踏まえ、移転後にも遅滞なく情報セキュリティ対策を実施するための対応策の検討を実施する。

復興庁

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
吉田　光市

復興庁は、復興に関する国の施策の企画、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、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に取り組んできた。2014年度に実施した情報セキュリティ対策の具体的取組や自己点検結果等について、以下のとおり報告する。

①　情報セキュリティインシデント

情報セキュリティに関する重大なインシデントは発生していない。

②　教育・啓発に関する取組状況

庁内電子掲示板に研修資料や情報セキュリティポリシー資料等を掲載し、全職員が常時参照可能とすることで、職員が理解すべき情報セキュリティ対策を適宜確認できる環境を整備している。また、全職員に対して、情報セキュリティポリシーの内容、標的型メール攻撃に対する対策、職員のソーシャルメディア利用に係る注意事項等について、年２回庁内教育を実施し、職員に対する情報セキュリティ対策の教育・啓発に取り組んでいる。

③　自己点検・監査の結果

自己点検を行った結果、昨年度に比べ実施率は向上しているものの改善の余地が残った。具体的には、職員が情報を作成及び入手した段階で当該情報に格付及び取扱制限を明示するなどの対策が不十分だったため、2015年度に改善を図る。

④　NISCによる重点検査や脆弱性検査の結果

当庁が所管するウェブシステムについて脆弱性検査を行った結果、実害に結びつく脆弱性は見られなかった。また、指摘された軽微な項目についても対策を完了している。

⑤　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）における決定事項等

政府統一基準群の改定を踏まえた当庁の情報セキュリティポリシーの改定を行った。

2015年度は改定した情報セキュリティポリシーを踏まえ、引き続き上記の取組、対策等を実施することによって、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。

総務省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
福岡　徹

サイバー空間を取り巻くリスクが深刻化する中、国民生活の基盤に広く関わる行政機能を担う総務省としても、情報セキュリティ対策の強化が求められている。

本計画は、総務省のすべての職員及び所管する情報システムを対象として、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年度は、昨年度に実施した情報セキュリティ対策及びリスク評価の結果等を踏まえ、以下の対策を重点的に実施する。

１　標的型サイバー攻撃等に備えた教育・訓練の実施

かねてより、省内の情報セキュリティ対策強化や職員の意識向上に向けた取組を行ってきたところであるが、近年、政府機関への標的型サイバー攻撃等が増加・高度化していることを踏まえ、従前の教育・訓練に加え、以下の取組を行う。

(1)　改定後のポリシーに基づく教育・研修

2015年３月26日に改定された「総務省情報セキュリティポリシー」の周知・徹底のため、e-ラーニングや最高情報セキュリティアドバイザー等による教育・研修を実施する。

(2)　不審メールへの適切な対応に関する訓練

2015年度においては、これまで実施してきた不審メール訓練により得られた知見を踏まえ、やり取り型で行われる手法等に重点を置くなど、訓練の内容・対象を見直した上で実施し、不審メールへの対応能力の向上を図る。

(3)　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

標的型サイバー攻撃等は完全に阻止することが難しいことを踏まえ、セキュリティインシデントの発生を想定した情報システム担当職員・運用事業者等向けの訓練を実施する。

２　セキュリティ対策推進のための支援の実施

総務省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。）は、最高情報セキュリティアドバイザーの助言の下、CSIRTとして省内における情報セキュリティインシデントへの対処を行うとともに、省内から寄せられる情報セキュリティに関する相談への対応を行ってきたところ。

近年、政府機関への標的型サイバー攻撃等が増加・高度化していることに加え、省内から情報技術利活用時の情報セキュリティに係る相談が多く寄せられている実態等を踏まえ、情報システム室は2015年度における省内のセキュリティ対策推進のため、以下の支援を行う。

(1)　情報システム向け相談会の実施

情報システムにおいて、情報システムの構想段階から網羅的なセキュリティ対策が行われるよう、最高情報セキュリティアドバイザー、情報システム室による相談会を実施する。

(2)　情報技術の利活用拡大を見据えた情報セキュリティ対策の推進

今後、ソーシャルメディアサービス及び約款による外部サービスを含む情報技術の利活用が拡大することが予想されることから、情報システム室は、企画構想段階から導入予定部局の相談を受け付け、運用及び利用時における情報セキュリティ対策が確実に実装されるよう、適切な助言を実施する。

また、2015年度においても引き続き以下の取組を実施する。

○　機微度の高い情報の管理対策の強化
○　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

法務省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
黒川　弘務

2014年度に、政府機関の情報セキュリティ対策のための統一基準群が改定されたことに伴い、法務省においても情報セキュリティを確保するために講じるべき対策の水準を高めるため、法務省における情報セキュリティ対策の基本方針及び各種対策基準の改定を行った。

情報セキュリティに関する教育については、企画担当情報セキュリティ責任者が企画・立案した「年度教育計画」に基づく研修のほか、専門的な知識を有する外部講師による研修として、課室等情報セキュリティ責任者を対象とした、情報セキュリティを取り巻く環境の変化に対応した情報セキュリティに関する知識を習得するための研修、本省部局課等における情報セキュリティ担当者を対象とした、インシデント発生時における対応要領に関する知識を習得するための研修等を実施した。

また、高度化・巧妙化する政府機関を標的とする標的型攻撃の実情を踏まえ、不審なメールを受信した際の注意力及び適切な対処を職員に身に付けさせるため、外部から受信可能なメールアドレスを対象に、標的型メール攻撃の対応訓練を外部委託事業者に委託して２回実施した。

2015年度は、政府機関等において発生した情報セキュリティインシデント等も踏まえ、日々変化するサイバー攻撃に対する脅威を認識し、障害が発生した際には迅速かつ的確な対応を実施できるよう、職員に対する情報セキュリティ教育をさらに充実させるほか、標的型メール攻撃を経験できる実践的な訓練を継続し、職員の情報セキュリティに対する意識を維持・向上できるよう、積極的に取り組む。

外務省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
上月　豊久

外務省においては、本省に加え通信事情の異なる200公館以上の在外公館がネットワークで接続され、日本人職員に加え、現地採用の職員が同一ネットワーク上の端末を使用し業務を行っており、そういった事情を踏まえたきめの細かい情報セキュリティ対策の実施が必要であると認識している。

こうした中、当省では、年間約900万通に及ぶ標的型メールを含む不審メールを受信しており、ネットワークの監視システムを強化するとともに、これらサイバー攻撃に対する対策強化のため、昨年４月に情報セキュリティインシデント対応チーム（※1）を発足させた。同チームでは、日々の監視・対処・分析業務を実施すると共に、本省・在外公館職員を対象とした標的型メール攻撃に対する訓練を実施し、すべての職員が実際に脅威を体験することなどによる啓発を行っており、今年度も引き続き訓練の拡充や対策の強化など同チームが中心となって各種セキュリティ対策を進めている。

最近は、ソフトウェアの脆弱性をついたゼロデイ攻撃や未知のウイルスなど、もはやシステムだけでサイバー攻撃を防御することは困難となっており、職員に対する情報セキュリティ教育はますます重要となっている。昨年度は、「外務省員のための情報セキュリティ対策１０＋１箇条」、「現地職員のための情報セキュリティ対策８箇条」（13カ国語）を新たに策定し、加えて、職員への情報セキュリティ啓発のための「外務省情報セキュリティナレッジ」ページ（※2）を立ち上げた。その他に、情報セキュリティに関するeラーニング講座の開設、情報セキュリティ責任者及び一般職員向けの集合研修の実施、専門家を招いてのCSIRT（GISIRT（※3）と呼称）研修の実施等、情報セキュリティ対策にかかる啓発・教育を充実させた。

脅威や攻撃手法がますます巧妙化していく中、モバイル端末の導入などにより、守るべき対象が広がっているという現状も踏まえ、引き続き対象や目的を明確にした効果的な情報セキュリティ対策の実施に努めていく。

（※１）インシデント対応チーム：サイバーセキュリティ対策のためのシステムの管理・情報分析全体を総括する担当官の下、セキュリティベンダー、システム運用業者、及びセキュリティ監視運用者から構成され、通信監視、検知情報の分析・管理、不審プログラムの解析影響範囲の特定、インシデント発生原因の研究及びその対策の検討、検討内容を踏まえた再発防止のための設定・運用方法の見直し及び職員への情報セキュリティ啓発を行うチーム。特に、在外公館を含めた全ての端末の通信状況を監視し、インシデント発生時に速やかに対処することを目的としている。

（※２）外務省情報セキュリティナレッジ:省内LAN上に構築した情報セキュリティ普及啓発に特化したホームページ。過去に発出した注意喚起情報や、各種教材等が掲載されており、職員がいつでもアクセス可能。

（※３）GISIRT:Gaimusho Information Security Incident Response Team

財務省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
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、件数も増加しているとされる等、サイバー攻撃の脅威は一層高まっている。2014年度には、サイバーセキュリティ基本法が成立し、サイバーセキュリティ戦略本部が設置される等、政府における情報セキュリティの体制が強化されたところである。

財務省においては、従来から情報セキュリティの重要性を強く認識し、業務遂行にあたり情報セキュリティの確保等に取り組んできた。2015年度も引き続き、政府の方針に沿い、NISC等と緊密に連携をとりながら、新たな情報セキュリティ上の脅威にも適切かつ迅速に対応する等、情報セキュリティの確保等に適切に取り組んでいく。

具体的には、2014年度に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）に準拠し改定した財務省の情報セキュリティポリシーに基づき、情報セキュリティに関する教育、自己点検、監査及び情報システムの技術的な対策等について、組織特有のリスク等も踏まえつつ着実に取り組んでいく。

文部科学省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
戸谷　一夫

当省では、情報通信技術の急速な進歩に伴う取り巻く状況の変化や、政府機関に対する標的型攻撃の発生など、ますます高度化・巧妙化するサイバー攻撃に対処するため、2014年度においては、以下の点を中心に情報セキュリティ対策に取り組んできた。

①　情報セキュリティ研修の全職員受講の徹底
②　標的型メール攻撃に対する訓練の実施による職員の意識啓発
③　省内情報システムに対する情報セキュリティ監査の実施
④　自己点検及び重点検査の実施
⑤　高度サイバー攻撃対処のためのリスク評価結果に基づく対策の実施
⑥　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）における決定事項等に基づく対策の実施
⑦　CSIRT要員のインシデント対処能力向上のための訓練受講

文部科学省情報セキュリティポリシーに基づく対策として、上記①～③を実施し、政府全体の方針等に基づき、④～⑦の対策を実施した。

2015年度は、政府全体のセキュリティ対策を着実に実施するとともに、文部科学省情報セキュリティポリシーの改定をふまえた実施手順書の改定や、高度サイバー攻撃対処のためのリスク評価の取組をふまえた対策を引き続き推進するとともに、セキュリティ監査や脆弱性診断結果のフォローアップを行うなど、情報セキュリティ対策の不断の見直しを行い、PDCAサイクルの実施を徹底することで、より一層の情報セキュリティの維持・向上に努めていく。

厚生労働省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
蒲原　基道

近年のインターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴い、これら技術を行政事務に積極的に活用することにより、国民の利便性や業務の効率化の向上を図る必要がある一方で、世界的規模で生じているサイバーセキュリティに対する脅威も年々深刻化し、政府機関を標的とした様々なサイバー攻撃が増加している。医療や年金、雇用対策など、国民生活に直結する政策を担っている当省においては、業務で取り扱う情報資産を適切な運用管理の下、あらゆる脅威から守ることが重要であり、そのためには、必要な情報セキュリティの確保とその継続的な強化・拡充に取り組むことが不可欠である。

2014年度においては、「サイバーセキュリティ戦略」の基本的な考え方を踏まえ、本戦略の年次計画である「サイバーセキュリティ2014」に基づき、「厚生労働省情報セキュリティポリシー」の見直しなどに取り組み、情報セキュリティの維持・強化を図ってきたところである。

2015年度においては、教育・研修、監査等の従前の取組を継続して実施するとともに、新たな脅威であるサプライチェーンリスク等への対応についても所要の措置を講じることとする。

また、2015年５月に日本年金機構において、職員のパソコン端末に対する外部からのウイルスメールによる不正アクセスにより、日本年金機構が保有している個人情報の一部が外部に流出するという事態が発生した。

本事案を受け、厚生労働省としては、日本年金機構の業務全般に対する指導監督体制の見直し等を図るほか、昨今の高度化した攻撃に対応できるよう、より高度かつ強固なセキュリティ体制の整備や対処手順の見直し、職員の意識やリテラシー向上のための情報セキュリティ教育の一層の充実など、改善・強化していく。

また、本事案については、原因究明と再発防止対策の検討を行うため「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検証委員会」を開催しており、検証委員会の検討も踏まえ、厚生労働省として再発防止に取り組むこととしている。

農林水産省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
佐藤　一雄

あらゆる活動のサイバー空間への依存の高まりにより、サイバーセキュリティに対するリスクが深刻化（甚大化・拡散・グローバル化）する中で、農林水産省においては、前年度の自己点検や情報セキュリティ監査の結果等も踏まえ、よりセキュリティ水準の高い方式の導入等を行うとともに、情報セキュリティインシデントへの対処態勢の充実・強化や行政事務従事者の情報リテラシーの向上に努めてきた。

また、NISCからのWindows XPのサポート終了に伴う注意喚起を踏まえたソフトウェアの更新等も実施してきたところである。

このような取組を通じ、行政事務従事者の意識も含め、情報セキュリティレベルについて一定の向上は図られたものの、機密情報の窃取を目的とする標的型攻撃等は複雑化・巧妙化、また対象が分散化しており、本省のみならず、地方組織等も含めて、より迅速かつ適切な対応が求められる状況になっている。

こうした中、2014年５月には、脅威の高度化・多様化や技術の進展等の環境変化への対応等を踏まえ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（2014年５月19日情報セキュリティ政策会議決定ほか。以下「政府統一基準群」という。）が改定され、また、11月には、我が国のサイバーセキュリティに関する施策の基本理念、基本的施策、国及び地方公共団体の責務等を定めた「サイバーセキュリティ基本法」（平成26年法律第104号）が成立した。

農林水産省としては、サイバーセキュリティ基本法、政府統一基準群の改定を踏まえ改定した農林水産省の情報セキュリティ関係規程（2015年４月１日施行。）等に基づき、情報セキュリティの確保を図ることとする。このため、引き続き内閣官房等の関係機関と連携を取りつつ、全ての行政事務従事者が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、情報の取扱いをはじめとする情報セキュリティに関する教育を実施するとともに、情報システムに関する技術的な対策を推進するなどにより、情報セキュリティレベルの向上を図ることとする。

経済産業省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
日下部　聡

2014年度は、国内外で大規模な個人情報の漏えいやサイバー攻撃が発生するとともに、我が国政府機関を狙う標的型攻撃ついても更なる巧妙化・高度化が進んだ。

2014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」（2014年５月19日　情報セキュリティ政策会議決定ほか。以下「政府統一基準群」という。）の改正を踏まえ、当省情報セキュリティポリシーの改正作業を行った。また、巧妙化・高度化する標的型攻撃への対応として、職員に対する教育・訓練の実施、基幹情報システムの対策強化を実施するとともに、特に国民に直接影響のある情報システムとして、ウェブサイト等インターネット上で運用する情報システムのセキュリティ対策の状況を確認、改善する取組を行った。

さらに、組織単位、職員単位で情報セキュリティ対策の実施状況について確認した結果、高いレベルで実施されていることが確認できた。

2015年度においては、以下の３点をポイントとしつつ、これまで以上に適切な情報管理、情報セキュリティ対策の実施に努める。

○　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
○　政府統一基準群の改正を踏まえて改正した経済産業省情報セキュリティポリシーに基づく新たなルールの全職員への徹底
○　省内各部局がインターネット上で運用する情報システムのセキュリティ対策の強化

国土交通省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
瀧口　敬二

最近の状況をみると、標的型メール攻撃や不正アクセス等、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、その手口が巧妙になっている。

このような中、国土交通省では、NISC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、2014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。また、組織面では、情報セキュリティ対策を専門的に実施する「情報セキュリティ対策室」の設置（2015年４月～)、政府統一基準改正を踏まえた国土交通省情報セキュリティポリシー改正の周知徹底や研修教育の充実等を行った。

2015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、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、情報システムに関する技術的なセキュリティ対策を一層強化する。

環境省

2014年度の総合評価・2015年度の全体方針

最高情報セキュリティ責任者
森本　英香

近年益々高度化、多様化するサイバー攻撃に対応するため、サイバーセキュリティ基本法（平成26年法律第104号）に基づきサイバーセキュリティ戦略本部が設置され、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ところ、環境省においても環境省情報セキュリティポリシー及びその実施手順書となる情報セキュリティマニュアルに基づき各種セキュリティ対策を講じているところであるが、2014年度も複数のセキュリティインシデントが発生している。

これらの原因は、各セキュリティ責任者のポリシー遵守の不徹底による脆弱性対策の不備及び行政事務従事者の不注意によるところが大きい。

これを是正するため、ポリシー遵守の徹底を最重要課題と位置づけ、各種セキュリティ対策を行うこととする。

また、高度サイバー攻撃対処のためのリスク評価の結果を踏まえ、2016年度に予定されているシステム更改に向け更なる対策強化のための要件の整理を実施する。

防衛省

2014年度の総合評価・2015年度の全体方針

情報保証統括責任者
深山　延暁

2014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た結果、情報セキュリティ対策が適切にとられていることが確認された。また、標的型攻撃メールによる情報流出等の認識や、可搬記憶媒体の取り扱い等について強化した規則の遵守事項等について、個々の職員に対し教育するとともに、不審メールを模擬したメール送付に対する訓練等を実施し、情報セキュリティ意識の向上を図った。

2015年度においては、2014年度に引き続き、自己点検、重点検査、監査等を実施し、情報セキュリティの確保に着実に取り組んでいく。職員への教育訓練としては、情報システムで取り扱うデータに対するリスクの認識や、可搬記憶媒体の取り扱い上の遵守事項について教育するとともに、不審メール対処訓練を実施する。さらに、情報セキュリティ担当者に対しては、インシデント対処訓練を実施し、対処能力の維持・向上を図る。また、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、演習等を実施し、官民連携の取組を本格化させる。

別添２　「サイバーセキュリティ 2014」に盛り込まれた施策の実施状況

＜別添２－目次＞

１　「強靭な」サイバー空間の構築

① 政府機関等における対策

１）情報及び情報システムに係る情報セキュリティ水準の一層の向上

施策名	担当府省庁	進捗状況
(ア)業務・情報の特性に応じた対策の重点実施のための枠組みの構築・運用	内閣官房 関係府省庁	a)・内閣官房において、各府省庁における試行の実施結果を踏まえて「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」の正式版を作成し、各府省庁において、本ガイドラインに基づく取組の正式実施を開始するとともに、2014 年度における運用状況を確認し、サイバーセキュリティ対策推進会議において報告した。
		b)・内閣官房において、対策推進計画の策定に係るマニュアルを作成し、各府省庁において、CISO のガバナンスの下で PDCA サイクルが適切に機能する計画が策定されるよう、支援した。また、各府省庁において作成された対策推進計画を確認し、各府省庁の全体方針や取組の重点を把握した。
(イ)政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し	内閣官房 全府省庁	・内閣官房において、政府機関統一基準群の改定を受けた各府省庁の情報セキュリティポリシーの見直しについて、2015 年度当初から改定後の統一基準に準拠したポリシーの運用が開始できるよう、個別の問合せ・相談に対応するとともに、情報セキュリティポリシーの見直し状況に係るアンケートを実施するなど、その進捗状況の把握や支援等を行った。
(ウ)政府情報システム管理データベースの利活用	内閣官房 総務省 関係府省庁	a)・内閣官房において、ODB を活用して直近にベンダーサポート終了が予定されているソフトウェアの利用状況、サプライチェーン・リスク観点での製品利用動向等の把握を行った。
		b)・総務省において、各府省の利用に支障がないよう、同データベースを引き続き維持・管理した。
(エ)「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の推進	内閣官房 関係府省庁	・内閣官房において、最高情報セキュリティアドバイザー等連絡会議を開催し、専門的知見を有する者（最高情報セキュリティアドバイザー等）から「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の対象となるオンライン手続を所掌する各府省庁に対し、当該府省庁が認証方式を決定するに当たっての助言等を行った。
(オ)特定秘密を取り扱うシステムに係る情報セキュリティ対策	内閣官房 関係府省庁	・内閣官房及び関係府省庁において、特定秘密の保護措置の実施に関する規程を新たに策定し、同規程の中で、各省庁の最新の情報セキュリティポリシーを厳格に運用するほか、特定秘密である情報を記録する電磁的記録を取り扱う際の端末・利用者の制限、電磁的記録の書き出しログ・印刷ログの保存、特定秘密である情報を取り扱う場所への機器持ち込み制限等、特定秘密を取り扱うシステムに係る情報セキュリティ対策を盛り込み、実施している。
(カ)特別管理秘密を取り扱うシステムに係る情報セキュリティ対策	内閣官房 関係府省庁	・内閣官房及び関係府省庁において、「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」に基づく特別管理秘密に係る基準を踏まえた対策の実施状況の重層的なチェックを実施した。
(キ)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に向けた取組の推進	内閣官房 関係府省庁	・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取組を推進した。
(ク)政府機関におけるスマートフォン等の情報セキュリティ対策の強化	内閣官房	・内閣官房において、官給品及び私物のスマートフォン等を業務利用する際に情報セキュリティ対策が適切に実施されるよう、各府省庁におけるスマートフォン等の管理体制や実施手順書の整備の支援を目的とした手引書を策定し、各府省庁へ展開した。また、新たにスマートフォン等の業務利用を計画している府省庁に対して、情報セキュリティ対策要件の検討支援を行った。
(ケ)政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化	内閣官房 総務省	a)・政府共通プラットフォームの円滑な運用・保守作業を実施しており、対象システムに影響のある障害は発生していない。
		b)・内閣官房において、政府共通プラットフォームが提供する個別サービス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。
(コ)複数の府省庁で共通的に使用する政府情報システム基盤の運用管理に関する体制等の整備	内閣官房 総務省 全府省庁	・「政府共通プラットフォーム運用管理基本規程」（2013 年３月 15 日各府省情報化統括責任者（CIO）連絡会議幹事会決定）に定めた運用管理体制の下、政府共通プラットフォームの安定的な運用を継続するとともに、対象システムへの連絡・調整を適切に実施している。
(サ)社会保障・税番号制度に対応した情報セキュリティ対策	内閣官房 関係府省庁	・2013 年度から設計・開発工程に着手済み。2017 年１月の情報連携の開始に向け、設計・開発作業を進捗中である。

(シ)オープンデータ推進における情報セキュリティの確保	内閣官房 関係府省庁	・データカタログサイト本格版の運用開始にあたり、国際標準化機構（ISO/IEC）の「情報セキュリティ・マネジメント・システム要求事項」である ISO/IEC 27001 や「個人情報保護マネジメントシステム―要求事項」に適合した JIS Q 15001 のプライバシーマークを取得したデータセンターにサーバを設置した。具体的なセキュリティの確保として、不正アクセス対策として、ファイアウォールの設置、サイトにおける入力項目に関して脆弱性診断テスト等を実施した。
(ス)情報システムに企画・設計段階から情報セキュリティ対策が適切に組み込まれるための方策	内閣官房 総務省 全府省庁	a) ・各府省庁において、情報システムに係る調達仕様書に必要なセキュリティ対策を確実に記載するため、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の活用を行った。
		b) ・内閣官房において、「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」が情報システムに係る政府調達の一環として広く活用されるよう、各府省庁に講師を派遣して講習会を行うなど、その普及・利用促進のための取組を行った。また、改定された政府機関統一基準群や講習会で出た意見等を踏まえ、マニュアルの改定を行い、府省庁への通知を実施した。
(セ)調達時における対策の推進	内閣官房	・内閣官房において、各府省庁が外部委託する際に、仕様書等へサプライチェーン・リスクに対応した対策の要件を適切に盛り込むことを支援するための仕様書策定手引書を整備し、各府省庁へ展開した。また、各府省庁の個別の情報システム調達等におけるサプライチェーン・対策を講じるための要件の盛り込みに係る助言を行うなどの支援を行った。
(ソ)安全性・信頼性の高い IT 製品等の利用推進	経済産業省 全府省庁	a) ・IT 製品の調達時において、利用環境における脅威を分析した上でその要件を満たした機器を調達できるよう、2014 年５月に「IT 製品の調達におけるセキュリティ要件リスト」を改正するとともに、当該リストを参照した上で IT 製品を調達するよう政府機関統一基準群を改正した。
		b) ・各府省庁が情報セキュリティに配慮した IT システムの調達を実行的かつ効率的に行えるようにするため、2014 年５月に、「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」（2011 年４月策定）を改定した「IT 製品の調達におけるセキュリティ要件リスト」を策定した。
(タ)政府調達における情報セキュリティの確保	内閣官房 経済産業省	a) ・政府調達等における情報セキュリティの確保に資するため、IPA を通じ、「IT 製品の調達におけるセキュリティリスト」に関する政府及び独立行政法人の調達担当者向けの説明会（６回）や、一般向けのシンポジウムにおいて、当該リストの普及啓発や情報提供を行った。また、政府等における本リストの有効活用のために必要な情報をまとめ、2014 年５月に「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」を策定した。
		b) ・「IT 製品の調達におけるセキュリティ要件リスト検討委員会」を半年に一度（６月、12 月）開催し、cPP（collaborative Protection Profile)策定状況の情報を提供するとともに、要件リストの改定イメージについて検討した。また、ネットワークデバイス、モバイルデバイス、アプリケーション、セキュリティ管理、その他分野の計８つのプロテクションプロファイル（翻訳版）を公開した。
		c) ・評価認証手続きの改善に向け、規定の見直しを実施するとともに、調達者・開発者・評価者等向けに、評価認証制度及び ST 作成、CC 評価のセキュリティアーキテクチャに関する説明会を計４回実施するなど広報活動を行った。政府調達を推進するため、政府機関及びベンダーに対してヒアリングを計 16 回行い「IT 製品の調達におけるセキュリティ要件リスト」の改定案に反映した。また、要件リストの活用に向け、政府機関や独法等のシステム担当者及び調達担当者に対して、計 11 回勉強会や説明会を実施した。
(チ)情報システムの設計等の段階における情報セキュリティの技術基準の整備等	内閣官房 全府省庁	・内閣官房において、各府省庁における試行の実施結果を踏まえて「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」の正式版を作成し、各府省庁において、本ガイドラインに基づく取組の正式実施を開始するとともに、2014 年度における運用状況を確認し、サイバーセキュリティ対策推進会議において報告した。
(ツ)運用・管理を委託している情報システムの情報セキュリティ対策の強化	内閣官房	・内閣官房において、府省庁によるクラウド調達・運用の際のセキュリティ対策・推進に係る検討の場として、NISC サイバーセキュリティ補佐官主催のクラウドセキュリティ研究会を設置するとともに、これまでに３回（2014 年 11 月、2015 年１月及び４月）開催し、検討を行った。
(テ)政府機関における安全な暗号利用の推進	内閣官房 総務省 経済産業省 全府省庁	a) ・総務省及び経済産業省において暗号技術検討会を開催し、CRYPTREC 暗号リストに掲載された暗号技術の監視、当該暗号の安全性及び信頼性確保のための調査等を実施した。

		b) ・ 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。
		c) ・ 内閣官房において、各府省庁が「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」に基づき、政府認証基盤及び電子認証登記所において電子証明書の発行等に使用される暗号アルゴリズムと、各府省庁の情報システムにおいて電子署名の検証に使用される暗号アルゴリズムとを、より安全な暗号アルゴリズムに移行する対応がおおむね完了したことを確認した。
(ト)安全性・信頼性の高い暗号モジュールの利用推進	経済産業省 全府省庁	a) ・ 経済産業省が策定した「IT 製品の調達におけるセキュリティ要件リスト」の対象候補「USB メモリ」のセキュリティ要件として、JCMVP で採用している国際標準を加えることで、安全性の高い暗号モジュールの製品カテゴリとして提示した。国際標準の改定に伴い、一致規格の JIS 原案を作成し、３月に公示した。
		b) ・ 各府省庁において、暗号モジュールを調達する際には、必要に応じて、同制度により認証された製品等を優先的に取り扱った。
(ナ)政府機関から発信する電子メールに係るなりすましの防止	内閣官房 総務省 全府省庁	a) ・ 内閣官房において、.go.jp ドメインにおける SPF(Sender Policy Framework)を用いた送信側の送信ドメイン認証技術の採用状況及び設定内容を定期的に確認し、問題がある場合は改善を図るよう府省庁に求めた。
		b) ・ 2014 年 10 月、迷惑メール対策に関する国際連携の枠組みであるロンドン・アクション・プラン（LAP）の第 10 回目の定期会合(LAP 10 Tokyo)がアジア地域において初めて我が国で開催され、日本の送信ドメイン認証技術等の技術的対策の取組状況等について説明を行ったほか、各国の迷惑メールに関する技術的対策について情報交換を行った。 ・ 2014 年 10 月、LAP 10 Tokyo と併催する形で第 11 回迷惑メール対策カンファレンスが開催され、送信ドメイン認証技術等迷惑メール対策技術の導入推進を含む議論が行われた。
(ニ)政府機関のドメイン名であることが保証されるドメイン名の使用の推進	内閣官房 総務省 全府省庁	・ 内閣官房において、各府省庁が国民等に対して情報発信を行う際に使用するドメイン名は原則として.go.jp で終わるものとし、必要によりソーシャルメディアを利用する場合においても情報の発信元が政府機関であることが保証されるよう、府省庁の自己管理ウェブサイトにおいて当該情報を掲載した上で発信すること等を引き続き求めた。
(ヌ)政府認証基盤を活用した電子署名の利用等の推進	内閣官房 全府省庁	・ 内閣官房において、総務省と連携し、政府認証基盤(GPKI:Government Public Key Infrastructure）によるドキュメント署名証明書の提供を推進するとともに、各府省庁におけるドキュメント署名証明書活用について周知を行った。
(ネ)国の重要な情報を扱う企業等の情報セキュリティ対策の推進	内閣官房 全府省庁	a) ・ 各府省庁において「調達におけるセキュリティ要件の記載について」を踏まえ、国の安全に関する重要な情報を国以外の者に取り扱わせる契約を締結する際には、情報セキュリティ要件を定め、これに遵守するよう求める措置を実施した。
		b) ・ 内閣官房において、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）と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新たに締結するとともに、独立行政法人情報処理推進機構（IPA）と脆弱性対応、民間事業者や独立行政法人等との情報共有、政府機関のシステム調達等に関するセキュリティ認証、国民・企業等に対する普及啓発等の幅広い分野でのパートナーシップを新たに締結した。
(ノ)独立行政法人等における情報セキュリティ対策の推進	内閣官房 独立行政法人等所管府省庁 関係府省庁	a) ・ 内閣官房において、独立行政法人の毎年の年度計画等に政府機関統一基準群を含む情報セキュリティ対策を踏まえ、情報セキュリティポリシーの策定及びこれに基づく対策の実施を行うことを盛り込むよう、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）で申し合わせた。
		b) ・ 関係府省庁において、引き続き独立行政法人に対して情報セキュリティ対策に係る PDCA サイクルを構築するための取組を推進することを要請するとともに、中期目標に情報セキュリティ対策に係る事項を明記することを推進した。また、内閣官房において、独立行政法人の情報セキュリティ対策について確認するとともに、関係府省庁との間で情報の共有を図った。

(ハ)地方公共団体の情報セキュリティ対策水準向上のための普及・啓発	総務省	a) ・ J-LIS において実施した研修 ＜集合研修（実績）＞ ○ICT-BCP 策定セミナー ３回開催、受講団体数:111 団体、受講者数:121 人 ○情報セキュリティ監査セミナー ２回開催、受講団体数:92 団体、受講者数:95 人 ○情報セキュリティマネジメントセミナー ３回開催、受講団体数:125 団体、受講者数:145 人 ＜ｅラーニング（実績）＞ ○情報セキュリティ研修 12 コース、受講団体数:818 団体、受講者数:175,313 人
		b) ・ 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。
		c) ・ Web サーバ等公開サーバや、ネットワーク機器等における脆弱性診断について、診断実施を希望する 806 団体（2015 年３月現在）を対象に実施し、脆弱性対策支援を行った。 ・ ・全国２箇所（東京・大阪）において、脆弱性の本質を理解し、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開催し、脆弱性対策強化を支援した。なお、講習会には 69 名が参加した。
		d) ・ ウェブサイトを閲覧しただけで感染するタイプのマルウェア検知について、検知を希望する 853 団体（2015 年３月現在）の約 51 万 URL を毎日巡回検査した。その結果、一部団体（関連団体含む）において発生したウェブ感染型マルウェア（ウェブ改ざん）を検知し、その対処方法等を当該団体に対して通知した。 ・ 標的型攻撃等、いわゆるマルウェアの検知について、検知を希望する 217 団体に提供し、標的型攻撃検知を支援した。 ・ 情報セキュリティ対策に関する事例等を紹介するセミナーを、全国５箇所（東京、名古屋、広島、大阪、新潟、熊本）で開催し、対策強化を支援した。累計 547 名が参加した。
		e) ・ 2014 年度は国際的なスパムメール対策の連携推進を重点的に行ったため、地方公共団体への送信ドメイン認証技術の採用等の推進に関する具体的活動は十分には行えなかった。

２）サイバー攻撃への対処態勢の充実・強化

施策名	担当府省庁	進捗状況
(ア)政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用による緊急対応能力の向上	内閣官房 全府省庁	a) ・ 内閣官房において、2014 年度にセンサー監視等による脅威件数は、約 399 万件であり、脆弱性対策情報等の配信を 84 件、不審メールに関する注意喚起を 789 件実施した。
		b) ・ ３月 18 日に NATIONAL318（CYBER）EKIDEN を実施し、サイバー攻撃対処を行う政府各機関の現場における実践的な能力に向け、各府省庁対抗による、競技形式のサイバー攻撃対処訓練を初めて実施した。
		c) ・ GSOC システムの具備すべき機能等を含む基本設計を作成するに当たり参考とするために必要な、諸外国の状況及び今後の技術動向等の調査等を実施し、2015 年７月末までに中間とりまとめ予定。
(イ)サイバー攻撃事態への対処に資する情報の集約・共有の充実	内閣官房 全府省庁	・ 内閣官房において、2014 年度にセンサー監視等による脅威件数は、約 399 万件であり、脆弱性対策情報等の配信を 84 件、不審メールに関する注意喚起を 789 件実施した。
(ウ)情報セキュリティ緊急支援チーム(CYMAT)要員等への訓練による対処能力の向上	内閣官房 全府省庁	・ 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）要員に対する教育訓練を年間を通じて実施したほか、2014 年９月、10 月、2015 年１月の各２日間に内閣官房及び関係府省庁の担当者に対する実践的な演習を行った。
(エ)CSIRT 等の体制の整備及び連携の強化	内閣官房 全府省庁	・ 内閣官房において、各府省庁の CSIRT 等の機能を維持・向上させるため、各府省庁の CSIRT 要員に対し、情報セキュリティインシデント発生を想定した対処訓練を実施した。同訓練では、並行で発生する複数のインシデントについて、事象把握、優先度付け、初動対処、被害拡大防止、幹部報告、関係機関への連絡、技術的な調査、広報準備等の模擬訓練を行った。また、PoC 会合を開催するなどにより、最近の情報セキュリティに関する脅威や技術の動向等について各府省庁の CSIRT 間における情報共有等を行った。
(オ)公開ウェブサーバに対する脆弱性検査の実施	内閣官房 関係府省庁	・ 内閣官房において、検査を希望する府省庁について、公開ウェブサイトの画面をサンプル抽出し、2014 年９月から 2015 年２月の間に脆弱性検査を実施し、その結果を当該府省庁等にフィードバックした。次年度における重点検査の検査項目への反映についても検討を行った。
(カ)「新たなサイバー攻撃に対する情報セキュリティ防御モデル」の検討及び演習の実施	総務省	・ 標的型攻撃への対処能力の向上に向けて、2013 年度に引き続き官公庁・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、防御モデルの検討、実践的防御演習を実施。2014 年度における成果として、解析は実際に組織に送付された標的型攻撃の検体を実証環境にて実行し、攻撃者の挙動を観測。防御モデルは標的型攻撃の予防・検知手法を整理。実践的防御演習は７回開催し、62 組織のべ 215 名が参加。また、演習で得られた知見を活用し、３月に内閣官房と共催で NATIONAL CYBER EKIDEN を実施。
(キ)大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等	内閣官房 関係府省庁	・ 内閣官房及び関係府省庁が相互に連携し、重要インフラ事業者がサイバー攻撃を受けたとの想定に基づく大規模サイバー攻撃事態等対処訓練を実施するとともに、当該訓練の結果を踏まえ、訓練参加者等による検討を行い、大規模サイバー攻撃事態等が発生した際に政府及び関係機関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。（2015 年３月）
(ク)政府機関における業務継続能力の強化	内閣官房	a) ・ 内閣官房において、各府省庁の監査担当者等に対し、情報システム運用継続計画に関連して、サーバ装置の運用時に必要な措置を講じているかどうかを確認するための監査手法等の情報提供を行うなどして、各府省庁の計画の運用及び維持・改善を図った。
		b) ・ 各府省庁において、内閣官房が策定した「中央省庁における情報システム運用継続計画ガイドライン」に基づき、災害や障害発生時における行政の継続性を確保するため、バックアップシステムの構築の検討等を行った。
(ケ)平時からの情報共有体制の構築	内閣官房 総務省 経済産業省 全府省庁	・ 内閣官房において、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）と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新たに締結するとともに、独立行政法人情報処理推進機構（IPA）と脆弱性対応、民間事業者や独立行政法人等との情報共有、政府機関のシステム調達等に関するセキュリティ認証、国民・企業等に対する普及啓発等の幅広い分野でのパートナーシップを新たに締結した。
(コ)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た対処能力の向上	内閣官房	・ BlackHat Briefings（2014 年８月、アメリカ）、CODE BLUE（2014 年 12 月、東京）等の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、最先端のサイバー攻撃の手法及びこれへの対処に関する情報収集を行った。

(サ)情報セキュリティに関する政府人材の育成	内閣官房 関係府省庁	・ サイバーセキュリティ基本法を踏まえ、内閣サイバーセキュリティセンターの体制強化の１つとして、サイバー攻撃に関するインシデントの情報等の集約、国内外の情勢の分析、技術動向の分析等の業務を行う任期付職員の採用を行った。
(シ)採用時における情報セキュリティ関連素養の確認	内閣官房 関係府省庁	・ 内閣官房副長官から各府省庁官房長宛に発出された、新規採用の際に情報セキュリティに関する素養の確認を要請する文書（2012 年６月）を受け、関係省庁等に対し、採用時に情報セキュリティに係る資格をはじめとした素養の確認に努めるよう啓発を行った。 ・ また、新規採用した職員に対し、早期に情報セキュリティに関する研修を行うなど、一定の進捗が図られている。
(ス)政府職員に対する教育・意識啓発の推進	内閣官房 人事院 総務省 全府省庁	a) ・ 総務省において開催する情報システム統一研修にて、内閣官房からの教材作成に関する支援等を受け、情報セキュリティ確保・維持管理等に関する集合研修及びｅラーニングを実施した。
		b) ・ 内閣官房において、2014 年６月から 2015 年２月にかけて、政府機関統一基準やサプライチェーン・リスク及び最近のサイバーセキュリティの現状と対策等をテーマに、政府職員等を対象に情報セキュリティ勉強会を計５回実施した。また、情報セキュリティ対策上の役割等に応じた政府機関統一基準の教材等を各府省庁に提供した。
		c) ・ 内閣官房において、近年、多発している「職員の不注意」や「サイバー攻撃」に起因する情報流出事案等を踏まえた教材の見直しを行い、人事院において、政府職員に対する採用時の合同研修で当該教材を活用し、情報セキュリティに関する教育を実施した。
		d) ・ 各府省庁において、内閣官房が開催した各府省庁の CSIRT 要員に対する情報セキュリティインシデント対処訓練に参加し、技術や知見等の向上を図った。また、各府省庁において、電子政府利用促進週間（2014 年 10 月 27 日～11 月２日）、サイバーセキュリティ月間（2015 年２月１日～３月 18 日）等の機会において、サイバーセキュリティに関する最近の脅威等を踏まえ、職員が遵守すべき情報の取り扱いや留意事項等について意識啓発を行った。
(セ)人事ローテーションの工夫	内閣官房 関係府省庁	・ 内閣官房副長官から各府省庁官房長宛に発出された、情報セキュリティ担当者に係る人事ローテーションの工夫を要請する文書（2012 年６月）を受け、関係省庁等に対し、情報セキュリティ担当者に係る人事異動の期間の長期化をはじめとした人事ローテーションへの配慮に関し一層の周知を図った。 ・ また、情報セキュリティ担当者に対し、NISC との人事交流や、CYMAT 要員としての配置、大学・大学院に留学させての専門教育受講等の取組が推進され、一定の進捗が図られている。
(ソ)優秀な外部人材の活用	内閣官房 関係府省庁	・ 内閣官房副長官から各府省庁官房長宛に発出された、情報セキュリティに係る外部人材の活用を要請する文書（2012 年６月）を受け、一部を除いた各府省庁において民間企業等の外部人材を CIO 補佐官等として任期付きで採用しているほか、情報システム運用・管理の委託等を通じて民間の人材の受け入れ・活用を推進した。
(タ)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・共有に係る取組の推進	内閣官房 関係府省庁	・ 内閣官房において、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を集約するとともに当該情報について分析し、その結果を各府省庁に提供し、共有を図った。

３）その他

施策名	関係府省庁	進捗状況
(ア)情報セキュリティガバナンスの機能強化に向けた取組	内閣官房 全府省庁	a) ・ 内閣官房において、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２回（2014 年６月及び９月）、サイバーセキュリティ対策推進会議を４回（2015 年２月、５月、６月及び７月）の計６回開催し、情報セキュリティ対策を推進するための取組を決定するなど政府機関における連携の強化を図った。
		b) ・ 内閣官房において、最高情報セキュリティアドバイザー等連絡会議を計３回開催し、各府省庁の最高情報セキュリティアドバイザーの専門的知見に基づく議論等を経て、各府省庁の取組の高度化のための助言等を実施した。
(イ)「情報セキュリティに係る年次報告書(仮)」に係る取組の推進	内閣官房 全府省庁	a) ・ 内閣官房において、対策推進計画の策定に係るマニュアルを作成し、各府省庁において、CISO のガバナンスの下で PDCA サイクルが適切に機能する計画が策定されるよう、支援した。また、各府省庁において作成された対策推進計画を確認し、各府省庁の全体方針や取組の重点を把握した。
		b) ・ 内閣官房において、対策実施状況報告及び重点検査を基に客観的に比較可能な形で評価し、必要な対策の実施を求めた。
		c) ・ 内閣官房において、政府機関を取り巻く情報セキュリティに関する脅威とその分析等を行い、その結果を「サイバーセキュリティ政策に係る年次報告（2013 年度）」に盛り込み、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）において決定後、公表した。
(ウ)情報セキュリティ対策に関連する独立行政法人等との連携の強化	内閣官房 総務省 経済産業省	・ 内閣官房において、独立行政法人との間で締結した協力覚書に基づき、脆弱性関連情報の政府機関内での共有を図るなど、政府機関における情報セキュリティ施策を推進した。
(エ)独立行政法人等との緊急時等の連絡体制の整備	内閣官房 独立行政法人等所管府省庁	・ 内閣官房において、所管府省庁管理職と独立行政法人役員レベルとの間でインシデント情報及び対応状況が周知されるなど、実効性のあるインシデント情報共有体制を構築することを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）で申し合わせた。
(オ)行政機関以外の国の機関との連携	内閣官房	・ 内閣官房において、衆議院、参議院、国立国会図書館、最高裁判所、会計検査院及び日本銀行にオブザーバー機関として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）及び最高情報セキュリティアドバイザー等連絡会議等への参画を求め、共通する情報セキュリティ上の課題について情報共有・交換を行い、連携を行った。

② 重要インフラ事業者等における対策

施策名	関係府省庁	進捗状況
（ア）「安全基準等の整備及び浸透」に関する内閣官房の施策	内閣官房	a）・内閣官房において、「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（第３版）改定版」及び「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』策定にあたっての指針（第３版）対策編改定版」を、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再構成し、「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）」及び「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」の改訂を実施するとともに、「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）」を新設した。2015 年３月にはサイバーセキュリティ戦略本部への付議案を策定し、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、公表した。
		b）・社会動向の変化及び新たに得た知見については、第３次行動計画の記載内容に含まれていることを確認した上で、上記 a)の再構成において併せて実施した。また、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。
		c）・内閣官房において、指針改訂の方針・原案等に関し、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訴求した。また、第３次行動計画から新たに重要インフラ分野となった３分野による安全基準等新設への支援を実施した。
		d）・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１月～３月）し、「2014 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 2015 年３月に公表した。
		e）・内閣官房において、従来の調査項目を第３次行動計画の記載内容に照らして見直しを実施し、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（2014 年７月～９月）及び事業者等への往訪による調査（2014 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するとともに、今後の改善状況を測るための基準を作成し、「2014 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 2015 年３月に公表した。
（イ）「安全基準等の整備及び浸透」に関する重要インフラ所管省庁の施策	重要インフラ所管省庁	a）・経済産業省において、第３次行動計画において新規追加した３つの重要インフラ分野に関して、当該分野の安全基準等の策定状況等を内閣官房に提供した。
		b）・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を行ったほか、地方公共団体に関し、「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の改定を実施し、公表した。 ・厚生労働省及び国土交通省については、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。
		c）・総務省について、「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」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の改定を実施し、公表するとともに、情報セキュリティ対策の実施状況について調査を実施し、公表した。 ・経済産業省について、日本電気協会において策定作業中の「電力制御システムセキュリティガイドライン（仮称）」の策定作業に必要な支援を行ったほか、日本ガス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」改訂が必要かどうか内容を確認した。
		d）・総務省について、「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」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の改定を実施し、公表するとともに、情報セキュリティ対策の実施状況について調査を実施し、公表した。 ・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電気設備自然災害等対策ＷＧにおいて、電気事業者が今後取り組むべきセキュリティ対策について提言を行ったほか、ガス分野においては全国でセキュリティに関する説明会を全８か所で実施し、セキュリティの重要性を訴えた。

		e）・ 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。
		f）・ 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、事業者からの回答率向上に努め、3,228 者（昨年度は 3,160 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。
（ウ）「情報共有体制の強化」に関する内閣官房の施策	内閣官房	a）・ 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た。
		b）・ 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。（2014 年度情報連絡 151 件、情報提供 38 件）
		c）・ 重要インフラ所管省庁の協力を得て、2014 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。
		d）・ 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。
		e）・ 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。（2014 年度のセプターカウンシル会合の回数は延べ 34 回）
		f）・ 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て、新規に設置した二つの WG を通じ、カウンシルの現状と課題を整理し、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るとともに、総会準備のノウハウや資料の整理、継承等を図った。
		g）・ 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整理を行った。
（エ）「情報共有体制の強化」に関する重要インフラ所管省庁の施策	重要インフラ所管省庁	a）・ 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。
		b）・ 重要インフラ所管省庁において、a)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。
		c）・ 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。
		d）・ 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やセプターを対象にした IT 依存度調査や、安全基準等の浸透状況調査のうちの往訪調査など多くの調査・ヒアリングに協力した。
		e）・ 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。 ・ また、国土交通省において、セプターの機能充実の支援のため、担当者不在時の対応など、情報共有体制の強化を検討中。
		f）・ 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。
		g）・ 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。
（オ）「情報共有体制の強化」に関する情報セキュリティ関係省庁の施策	情報セキュリティ関係省庁	a）・ 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。
		b）・ 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。
		c）・ 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。

（カ）「情報共有体制の強化」に関する事案対処省庁の施策	事案対処省庁	a）・ 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。
		b）・ サイバー攻撃の予兆を把握するため、「サイバー攻撃特別捜査隊」を中心として、全国の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を推進したほか、サイバーテロ対策協議会を通じた事業者間の情報共有を実施した。
		c）・ 内閣官房と必要に応じて情報共有を実施した。
		d）・ 都道府県警察において、重要インフラ事業者等への個別訪問を行い、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、重要インフラ事業者等の意向を尊重し、IT 障害対応能力の向上を図った。
（キ）「障害対応体制の強化」に関する内閣官房の施策	内閣官房	a）・ 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。
		b）・ 13 分野 18 セプター中、14 セプターに対しセプター訓練を実施した（１分野は独自に訓練を実施。２分野は新規参入分野のため今年度未実施）。
		c）・ 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、94 事業者 348 名が演習に参加した。
		d）・ 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導入等）を検討・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（大阪会場の新設、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。
		e）・ 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。
		f）・ 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。
		g）・ 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。
（ク）「障害対応体制の強化」に関する重要インフラ所管省庁の施策	重要インフラ所管省庁	a）・ 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、2014 年８月から 10 月までの間に、セプター訓練を実施し、14 セプターと 1,644 団体が参加した。
		b）・ 重要インフラ所管省庁は、2014 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。
		c）・ 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、2014 年 12 月に実施された分野横断的演習に参加した。
		d）・ 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 2014 年度分野横断的演習への参加を促し、全体で 94 組織 348 名の参加者を得た。うち、今年度より新設された大阪会場には、10 組織 32 名の参加を得た。
		e）・ 重要インフラ所管省庁は、2014 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。

		f）・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。 ・また、総務省において、分野横断的演習の成果を情報セキュリティポリシーガイドラインの改定の参考資料として活用した。
		g）・総務省において、分野横断的演習及び総務省が実施する訓練等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２月に開催された 2014 年度電力分野サイバーセキュリティ演習について、同一事業者が双方の訓練に参加することを働きかけることによって、分野横断的演習と相互連携への協力を図った。
（ケ）「障害対応体制の強化」に関する事案対処省庁の施策	事案対処省庁	・都道府県警察において、重要インフラ事業者等への個別訪問を行い、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、重要インフラ事業者等の意向を尊重し、IT 障害対応能力の向上を図った。
（コ）「リスクマネジメント」に関する内閣官房の施策	内閣官房	a）・「重要インフラ防護に関する諸国の枠組み等に関する調査」を行い、その中で重要インフラ防護における情報セキュリティの関連規定・国際標準等 797 件を抽出、リスト化することで手引書等の素材を準備した。
		b）・相互依存性解析の一部として、新たに重要インフラ分野として加わった化学、クレジット及び石油の３分野を対象に「重要インフラ分野の変化に基づく IT 依存度に関する調査」を行い、当該３分野の IT 依存度等の結果を各重要インフラ分野のセプターへ共有することで、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。
		c）・相互依存性解析の一部として、新たに重要インフラ分野として加わった化学、クレジット及び石油の３分野を対象に「重要インフラ分野の変化に基づく IT 依存度に関する調査」を行い、業法からの要請と情報セキュリティの関係性について改めて課題を洗い出し、安全基準等に反映する基礎資料を提供した。
		d）・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、分野横断的演習の検討会等を計６回行うとともに、セプターカウンシルにおける計８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）の支援を行った。
（サ）「リスクマネジメント」に関する重要インフラ所管省庁の施策	重要インフラ所管省庁	a）・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、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。
		b）・総務省において、「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」の改定を実施し、公表した。 ・経済産業省において、2013 年度に行ったサイバーセキュリティに関する調査結果を反映する形で、産業構造審議会保安分科会電力安全小委員会電気設備自然災害等対策ＷＧにて、電気事業者が今後取り組むべきセキュリティ対策について提言を行った。
		c）・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。
（シ）「防護基盤の強化」に関する内閣官房の施策	内閣官房	a）・NISC 重要インフラニュースレターを 21 回発行し、注意喚起情報の掲載のほか、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の広報を行った。
		b）・第３次行動計画の策定、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 23 回説明を行った。
		c）・二国間・地域間・多国間での会合、シンポジウム、意見交換等に積極的に参加し、相互理解の基盤を強化した。また、Meridian 会合を東京に招へいし、2014 年 11 月、重要インフラ防護等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行った。
		d）・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。
		e）・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、規程集の発行を行うべく、収録すべき文書の確認・収集等を行った。
		f）・国際標準化機関・団体等 10 組織における情報セキュリティの国際標準、関連規定、報告書等をリスト化し、関連性について資料化し、可視化を行った。

		g）・欧米の重要インフラ防護に係わる枠組みを整理、関連付けをした調査報告書をまとめ、その概要版を公表した。
		h）・国際電気標準会議（IEC）等において我が国における検討課題をセキュリティ認証等の基準及び規格に反映すべく関係省庁、関係機関との協議を開始した。
(ス)「防護基盤の強化」に関する重要インフラ所管省庁の施策	重要インフラ所管省庁	a）・総務省及び経済産業省を中心として、内閣官房が行う Meridian 会合の開催等の国際連携に対して協力を行った。
		b）・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。
		c）・総務省及び経済産業省を中心として、内閣官房が行う手引き書の整備に関し、情報収集・共有などの協力を行った。
		d）・総務省及び経済産業省を中心として、内閣官房が行う手引き書の整備に関し、情報収集・共有などの協力を行った。
		e）・経済産業省において、国内の製品認証制度の立ち上げにおいて技術研究組合制御システムセキュリティセンター（CSSC）への支援を行い、2014 年４月に国内の EDSA に係る認定及び認証制度（制御機器のセキュリティに係る認定及び認証制度）を確立した。
(セ)大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等	内閣官房 関係府省庁	・再掲：１-①-２）-(キ)
(ソ)情報通信分野における事業者との官民連携の推進	総務省	・総務省において、情報セキュリティ上の事案について、ISP 事業者団体の「テレコム・アイザック推進会議」（Telecom-ISAC Japan）と随時情報共有を行い、情報通信分野における事業者との官民連携を推進した。
(タ)個別分野におけるサイバー演習	総務省 経済産業省	a）・巧妙化・複雑化するサイバー攻撃に対応するため、Telecom-ISAC Japan において、電気通信事業者等によるサイバー攻撃演習を実施し、事業者間連携等を促進した。
		b）・経済産業省において、電力、ガス、化学、ビルの４分野で、実際にサイバー攻撃が発生することを前提としたサイバー演習を実施した。前年度と比して各分野の参加者層の拡大を図ることにより、各分野における制御システムのセキュリティ検証とセキュリティ対策に関する知見の蓄積を促し、今後の制御システムのセキュリティ対策に繋げた。
(チ)電気通信システムの安全・信頼性確保	総務省	・総務省において、2013 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、2014 年９月に公表した。 ・総務省において、2014 年６月に公布・施行された改正電気通信事業法の内容を踏まえ、「情報通信ネットワーク安全・信頼性基準」の改正を実施した。
(ツ)重要無線通信妨害対策の強化	総務省	a）・総務省において、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・休日の全国一元的受付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。
		b）・総務省において、電波利用秩序維持のため、耐災害性能が向上する電波監視施設の次世代化を開始しつつ、同施設のセンサー29 か所を 2014 年度内に更改した。
		c）・将来の多様な無線システムに対応するため、高密度化技術等を用いて構成装置を汎用化する等の電波監視技術について、調査研究等を実施した。
(テ)「サイバー情報共有イニシアティブ」の強化	経済産業省	・J-CSIP において、前年度に引き続き標的型サイバー攻撃に関する情報共有を継続しつつ、産業分野・参加メンバーを拡大した。さらにやり取り型攻撃など、特殊な攻撃事案に関してはその特徴を分析し、一般に公表した。 ・2014 年度に石油業界１組織、化学業界７組織と NDA を新たに締結。2014 年度では、J-CSIP 参加組織より 626 件の情報提供を受け、うち 505 件を標的型攻撃メールと判断。IPA が独自の経路で入手した情報の展開も含め、195 件の情報共有を実施した。 ・標的型サイバー攻撃の特別相談窓口の運営を通じ、情報提供者へ調査結果及びこれに基づく対応策、初動対応の方針等をアドバイスすることにより、被害の拡大と感染予防（未然の発生防止）に貢献するとともに、解析協議会の活動の一環として、JPCERT/CC、NICT と連携し、ウイルス解析の多様化による感染時痕跡発見の迅速化と網羅性向上を図る等の施策を実施した。
(ト)サイバー攻撃(インシデント)対応調整支援	経済産業省	・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 9,684 件：2015 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に関する対応支援は 276 件、制御システムに関する対応支援は 29 件（2015 年３月末）であった。

(ナ)重要インフラで利用される情報システムのセキュリティ・信頼性向上のための支援体制の整備	経済産業省	a) ・ 昨年度に引き続き、重要インフラ事業者の情報処理システム等の信頼性向上のため、IPA において、重要インフラ等の IT サービス事業者、製品・制御システム事業者等有識者からなる委員会（重要インフラ IT サービス高信頼化部会、製品・制御システム高信頼化部会等）を計 75 回開催。当該有識者から自主的に提供のあった障害情報や意見を踏まえながら、障害事例集の整備・共有に関わる検討を行い、追加事例 28 件を「情報処理システム高信頼化教訓集」へ追加、2015 年３月に公開した。成果物は重要インフラ事業者や業界団体等へ提供する予定。 ・ ３つの産業分野（情報通信、行政、電力）において障害情報収集・共有体制を構築した。 ・ また、IPA において、「情報システムの障害状況データ」を継続してまとめ、SEC ジャーナル（36 号、38 号）に掲載した。
		b) ・ 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、2014 年４月に、国内の EDSA に係る認定及び認証制度（制御機器のセキュリティに係る認定及び認証制度）を確立。SSA（制御システムに係る認定及び認証制度）に関しては、評価認証に係る実施手順を検討し、次年度以降のパイロット認証実施につなげた。IEC62443 の標準化に積極的に参画し、国際標準化機関である IEC および ISCI と今後のスキームにあり方に向けた話し合いを実施した。
(ニ)重要インフラ事業者に対するソフトウェアや制御システム等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等	経済産業省	a) ・ IPA において、制御システムのセキュリティに対して、制御システムの利用者（特に準大手・中堅企業の利用者）がどのように対応すべきかを解説した資料を、制御システム分野の有識者・事業者・運用保守事業者へのヒアリング及び制御システム業界の専門家による査読を経て公開した。 ・ JPCERT/CC において、2014 年５月改訂の早期警戒パートナーシップにおいて、製品開発者が必要と判断した場合に、JPCERT/CC と協議のうえで、製品開発者自身が製品利用者、あるいはシステム構築事業者に対して、一般公表前に情報提供出来るようになった。これが、制御システムにおける事情を鑑みた内容となっており、これまでの重要インフラ限定の制度から改善され、運用が開始されている。国内届出案件および海外届出案件でそれぞれ公表実績があり、製品利用者との事前調整が必要と申告を受け、その要望に応じた調整を実施した。
		b) ・ 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、当該対策が必要と判断できる組織を任意に選定し、それぞれの関係者に対し 26 件の「早期警戒情報」を発行した（2015 年３月末現在）。
		c) ・ IPA において、継続して JVN iPedia への脆弱性対策情報の登録・公開作業を実施。NIST の NVD（National Vulnerability Database：米国 NIST が管理している脆弱性情報データベース。）で公開された脆弱性対策情報を、１営業日以内に、翻訳して JVN iPedia に登録・公開した。2014 年度に登録した脆弱性対策情報は、合計 8,074 件（累計 53,235 件）であった。脆弱性対策に広く利用され、登録データへのアクセス数は、前年度比約 1.9 倍であった。 ・ JPCERT/CC において、JVN 掲載情報の RSS フィード、Twitter 投稿、VRDA フィードなどの提供により、利用者が入手しやすい形式での情報提供を実施した。
(ヌ)制御システムに関するインシデントや脆弱性への対応のための連携体制の構築	経済産業省	・ 国内制御システムベンダーに対する脆弱性情報受領時の窓口機能新規構築支援や、脆弱性の低減のための調査に加え、業界団体と合同でのセキュリティカンファレンスや JPCERT/CC 主催のカンファレンスの開催等を通じた業界関係者への普及啓発、情報収集・分析を通じた脅威情報・参考情報の提供といった支援活動を行った。

(ネ)制御システムにおける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確立支援	経済産業省	・ 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は、2013 年度に前倒しで達成しており、2014 年度は説明会等により制度の普及に協力した。 ＜実績＞ ○「情報セキュリティ EXPO：認証制度の実現」（５月 14 日、５月 15、５月 26 日） ○「資源開発関連組織（業界団体）との会合」にて CSMS の制度紹介を実施（10 月９日） ○「重要インフラ関連組織との会合」にて CSMS の制度紹介を実施（12 月８日） ○「ガス関連組織（業界団体）との会合」にて CSMS の制度紹介を実施（12 月９日） ○「CSMS 適合性評価制度に関する説明会」（２月 17 日、２月 26 日） ○「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」研修コース策定支援[講義資料提供]（２月 16 日～２月 25 日）
(ノ)制御機器等の評価・認証スキームの確立支援	経済産業省	・ 国内の製品認証制度の立ち上げにおいて技術研究組合制御システムセキュリティセンター（CSSC）への支援を行い、2014 年４月に国内の EDSA に係る認定及び認証制度（制御機器のセキュリティに係る認定及び認証制度）を確立した。
(ハ)制御システムセキュリティの国際標準に基づく評価・認証機関設立	経済産業省	・ SSA（制御システムに係る認定及び認証制度）に関しては、評価認証に係る実施手順を検討し、次年度以降のパイロット認証実施につなげた。EDSA（制御機器に係る認証制度）に関しては、パイロット認証を経て４月１日から認証を開始し、３件の制御機器に対し認証を発行した。
(ヒ)制御システムセキュリティ評価・認証の国際相互承認	経済産業省	・ EDSA（制御機器に係るセキュリティ認証制度）認証に関して、国際的標準化機関である IEC の下部組織である CAB（適合性評価評議会）において、IEC への提案準備に関して協議した。また、相互認証の拡大に向け、ISCI と SSA 認証（制御システム全体の認証制度）の効果的な実施手順に関して協議を行った。
(フ)制御システムセキュリティ評価・認証の利活用に向けた検討	経済産業省	・ 制御機器のセキュリティ評価・認証について、評価・認証制度及びパイロット認証の成果に関する説明を 150 人規模で実施した。また、認証のコスト分散及び認証期間短縮になるような提案を認証スキームオーナーに行い協議した。
(ヘ)ソフトウェア、情報システムの信頼性向上	経済産業省	・ 昨年度に引き続き、重要インフラ分野の情報システムに係るソフトウェア情報の収集・分析及び対策について、IPA において、重要インフラ等の IT サービス事業者、製品・制御システム事業者等有識者からなる委員会（重要インフラ IT サービス高信頼化部会、製品・制御システム高信頼化部会等）計 75 回開催。当該有識者の意見を踏まえながら、収集した情報の分析を行い、対策を検討し、分析手法集・対策手法集として取りまとめ、2015 年３月に公開した。 ・ 昨年度に引き続き、ソフトウェアの信頼性の見える化の促進を図るために、IPA に産学の有識者からなる委員会（サプライチェーンにおけるソフトウェアの高信頼化 WG、サプライチェーンにおける品質の見える化 WG、ソフトウェア品質説明力向上・普及ＷＧ、開発手法適用のための分析 WG）を設置し、検討会を計 25 回開催。また、「ソフトウェア開発の取引構造（サプライチェーン）の実態に関わる課題の調査報告書」を 2014 年７月に公開した。 ・ 委員会活動等を通じて収集した信頼性検証手法や設計方法適用事例を報告書として取りまとめ、2015 年 11 月に公開予定。 ・ 相互に接続される製品・サービスの信頼性を確認する仕組み、事業者等が取り組むべき事項を整理し、セーフティ・セキュリティ設計と見える化のガイドブック「つながる世界のセーフティ&セキュリティ設計入門」として取りまとめ、啓発用の小冊子を 2015 年７月に公開予定。2015 年９月に書籍として発行予定。
(ホ)社会的に重要な情報システムについての情報セキュリティ強化	経済産業省	・ 制御システムのセキュリティに対して、制御システムの利用者（特に準大手・中堅企業の利用者）がどのように対応すべきかを解説した資料を、制御システム分野の有識者・事業者・運用保守事業者へのヒアリング及び制御システム業界の専門家による査読を経て作成。
(マ)我が国の重大なセキュリティ事案に対する対応支援	経済産業省	・ 新たに立ち上げたサイバーレスキュー隊（J-CRAT）において、標的型サイバー攻撃特別相談窓口への相談を契機として、状況などから対応が必要と判断した相談組織に対し、メールや電話を使ったヒアリングや、相談者自身による調査対応の支援を 38 組織実施。うち、支援対象組織の現場において、複数関係者による対応が必要と判断した 11 組織に対して、オンサイトでレスキュー活動を実施した。

③ 企業・研究機関等における対策

施策名	関係府省庁	進捗状況
(ア)中小企業における情報セキュリティ対策の推進	経済産業省	a) ・「中小企業情報セキュリティ指導者育成セミナー」を全国で 20 回開催した。さらに、全国の商工会議所・商工会等の中小企業団体等が主催する情報セキュリティセミナーに IPA が講師を 21 回派遣した。 ・また、上記２つのセミナーや中小企業向けのイベント等において、IPA が制作した「映像で知る情報セキュリティ（DVD）」、「企業（組織）における最低限の情報セキュリティ対策のしおり（冊子）」、「2014 年度版情報セキュリティ 10 大脅威（冊子）」等の啓発資料を配布し、利用促進を図った。
		b) ・「中小企業情報セキュリティ指導者育成セミナー」および IPA が講師を務める企業向けの情報セキュリティセミナーにおいて、中小企業の情報セキュリティ対策ガイドラインをより見やすくした「中小企業における情報セキュリティ対策ガイドライン事例集・チェック項目（冊子）」を配布し、普及啓発に努めた。
(イ)中小企業における情報セキュリティ対策の底上げ	総務省 経済産業省	・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を延長した。また、中小企業におけるパソコン、経理事務ソフトウェアなど少額減価償却資産の投資の促進等を図るため、2013 年度末とされていた適用期限を２年間延長。WindowsXP のサポート期限が切れることに伴う中小企業のパソコン、ソフトウェア等の入替えニーズにも対応した。
(ウ)中小企業・小規模事業者の IT 活用における情報セキュリティの確保	経済産業省	・中小企業の情報セキュリティ対策水準の底上げのため、中小企業向けセキュリティ診断・学習及び支援ツール「iSupport」において、情報セキュリティ対策を推進するための自社診断ツールや、社内教育を行うための各種オンラインツールを提供した。
(エ)個人情報漏えい等防止のための対策	経済産業省	・2014 年 12 月 12 日付けで「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を改正し、サイバー攻撃対策に関する安全管理措置についての項目を追記した。改正後、全国主要都市８カ所にて説明会を開催した。
(オ)技術・営業秘密保護に関する官民フォーラムなどの場の準備	経済産業省	・2015 年１月、我が国企業の重要技術等の国内外への流出を断固として許さない社会を創出するため、官民の代表者が参画する「技術情報等の流出防止に向けた官民戦略会議」を開催し、官民の今後の取組を「行動宣言」として取りまとめた。
(カ)上場企業における事業等のリスクとしての開示の検討	金融庁	・上場企業におけるサイバー攻撃によるインシデントについて、事業等のリスクとしての開示を行うことの可能性について、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、検討を行っている。 ・その際、米国での開示の実態や、米国 SEC が「詳細な開示はかえって攻撃者に攻撃のヒントを与えるおそれがある」としていることのほか、証券監督者の国際機関（IOSCO）においてサイバーリスク等に係る情報開示の検討が続いていることなども踏まえ、その状況も見定めつつ、分析を行っていく。
(キ)セキュリティエコノミクスに関する対応	経済産業省	・国内の企業を対象とした「2014 年度情報セキュリティ事象被害状況調査」を実施し、2015 年１月に公表した。サイバー攻撃等による被害状況や復旧に要した費用（被害額）、セキュリティ対策の実施状況等を明らかにした。セキュリティパッチの適用率の向上は見られたものの、サイバー攻撃の遭遇率（被害あり＋発見のみ）が 19.3%と前回より 5.5 ポイント増加と本調査での過去最悪を記録した。 ・組織において、情報セキュリティに関連する脅威に対していかなるリスクが事業経営に影響するかを分析するリスク分析が重要である。一般的にリスク分析の結果の対処の一つとして、リスク移転（保険）の考えがあるが、海外に比較し国内での知名度が低い状況である。国内の実態を明らかにするため、国内の情報セキュリティに関連したリスク対応と保険に関する実態を調査した。調査の結果、経営者のセキュリティリスクへの認知が高いほど、IT 関連保険に加入していることが明らかになった。これにより、リスク対策のためには経営者への意識向上の働きかけが有効であることが明らかになった。本調査の結果は、経済産業省と IPA 共同で開催している「サイバーセキュリティリスクと企業経営に関する研究会」で議論したものである。
(ク)情報セキュリティガバナンス確立の促進	経済産業省	・情報セキュリティガバナンス協議会において、情報リスクの管理に関する参加企業内での知見の共有を図った。具体的には、「企業における情報セキュリティ活動の見える化」及び「内部犯行問題」をテーマとする WG を発足し、国内外の状況や事例を踏まえたレポートを作成・共有した（いずれも WG を８回実施し、全体会合も５回実施するとともに、「http://isga.jp/wg/index.html」において、2014 年度の活動報告書の概要を公開する予定）。

(ケ)企業における情報セキュリティ対策の支援	経済産業省	a) ・「2014 年情報処理実態調査」により、企業における情報セキュリティ監査制度の活用・企業における情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況、取引（委託、外注を含む）相手における情報セキュリティ対策実施状況の確認状況、Common Criteria（ISO/IEC15408）認証取得製品の導入状況について調査を実施した。
		b) ・ 情報セキュリティ監査制度の基盤となる JIS Q27001 及び 27002 が 2014 年に改正されたことを踏まえ、当省の所管する情報セキュリティ管理基準の改正に向けて、有識者の意見も踏まえて、JIS の変更点や監査実務上の課題等の検討を行うため、調査事業を実施した。当該事業の成果を踏まえて、2015 年度に当該基準を改正する予定である。
		c) ・ 企業が適切に情報セキュリティ報告書を作成することができるようにするために、情報セキュリティガバナンス協議会において、経営目標や事業方針等に必要な情報セキュリティの取組をテーマとする WG を発足し、国内外の状況や事例を踏まえたレポートを作成・共有した（WG を８回実施し、全体会合も５回実施するとともに、「http://isga.jp/wg/index.html」において、2014 年度の活動報告書の概要を公開する予定）。
(コ)「情報システム・モデル取引・契約書」の活用・普及	経済産業省	・ 情報システムの信頼性向上の観点から、ユーザー・ベンダー間の取引の可視化・役割分担の明確化を進めるため経済産業省において策定・公表した、「情報システム・モデル取引・契約書（第一版）」、「情報システム・モデル取引・契約書（追補版）」等について、ユーザー・ベンダー双方の関係業界団体と連携し普及活動を実施。
(サ)企業における電子署名利活用の普及促進	総務省 法務省 経済産業省	・ 電子署名の安全な利用方法等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行った。
(シ)情報システム調達時等における情報セキュリティの確保の支援	経済産業省	a) ・ IPA が実施する JISEC の運用を推進するとともに、情報システム調達時の同制度の利用拡充を図るため、2014 年５月に改定された政府機関統一基準群の見直しに合わせて、2014 年５月に「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」を改定した「IT 製品の調達におけるセキュリティ要件リスト」を策定した。
		b) ・ 2015 年１月に NIST を訪問し暗号モジュールの共同認証に関する覚書の進捗フォローを実施した。そこで、暗号モジュールの NIST 及び IPA による共同認証で用いる国際標準をベースにしたセキュリティ要件の制定に関する Federal Register Notice（米国連邦政府官報公示）を 2015 年に検討していること、また NIST より共同認証を運営するための第三者機関について非営利機関の MITRE を候補としてへの委託を検討していることの説明があり、意見交換を行った。
		c) ・ 複合機ベンダー12 社及び経済産業省 CIO 補佐官を含む cPP 検討委員による検討会を３回、具体的な評価手法検討のため、評価機関を含む評価検討 WG 委員による検討会を５回開催し、cPP のドラフト版を作成した。さらに米国 NIAP と電話会議による定期的な要件に関する確認を行い、cPP ドラフト版に反映した。
(ス)CISO 等の設置促進	経済産業省	・ 情報セキュリティガバナンス協議会において、CISO 等に報告する情報の集約・可視化をテーマとする WG を発足し、国内外の状況や事例を踏まえたレポートを作成・共有した（WG を８回実施し、全体会合も５回実施するとともに、「http://isga.jp/wg/index.html」において、2014 年度の活動報告書の概要を公開する予定）。
(セ)組織の緊急対応チームの普及、連携体制の強化	経済産業省	・ 国内組織内 CSIRT 機能構築支援先組織数としては 2015 年３月末時点で 256 組織に拡大。また組織内 CSIRT 向け標的型攻撃への対応ガイドとして、「APT への備えと対応ガイド 第２版」を作成。
(ソ)企業の運営するウェブサイトの安全性向上	経済産業省	・ ウェブサーバのアクセスログから攻撃と思われる痕跡を検出するためのツールとして 2008 年４月より IPA のウェブサイトでの公開している「ウェブサイト攻撃の検出ツール」（iLogScanner）について、昨今のウェブサイトの脅威・インシデントの傾向や利用者らの要望を踏まえ、以下の機能を追加し、2014 年 10 月９日より提供開始。 （ⅰ）認証ログ解析機能 （ⅱ）最新版ログフォーマットへの対応 （ⅲ）オフライン版 iLogScanner の追加
(タ)内部の不正行為によるセキュリティインシデント防止の検討	経済産業省	・ ガイドライン普及を念頭としたセミナーシンポジウム（共催を含む）を計 15 回（3,081 名）、講師派遣依頼での講師を 16 か所にて実施し、普及に努めた。内部者による大規模情報漏えい事案が発生したため、９月にその対策を強化した第２版、３月には最新の動向等を考慮した第３版を発行した。

(チ)経営層向けセミナーの開催等	内閣官房 総務省 経済産業省	・ 企業の経営層に対し経営戦略としてサイバーセキュリティを位置づけることの重要性について、経団連の委員会で内閣官房より説明したほか、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。
(ツ)実務者層のリーダー層に対する組織内部におけるコミュニケーション能力の強化	内閣官房 総務省 経済産業省	・ サイバーセキュリティ月間の冒頭に、企業等の経営層や実務者層をターゲットとしたシンポジウムを開催し、経営戦略としてサイバーセキュリティを位置づけるための意識啓発を行った。
(テ)情報セキュリティ対策に資する各種ツール・分析等の提供	経済産業省	・ IPA のウェブサイトで「情報セキュリティ対策ベンチマーク」を公開し、2014 年度は 3,189 回の診断利用があった。
(ト)地方公共団体の教育関係部門における情報セキュリティに関する取組の推進	文部科学省	・ 地方自治体の情報教育担当を集めて実施した会議（2014 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（2014 年 10 月及び 2015 年１月）。
(ナ)大学に対する情報セキュリティに関する最新情報の提供	内閣官房 総務省 文部科学省 経済産業省	・ 文部科学省が主催する国立大学等の最高情報セキュリティ責任者等を集めたセミナーを通じ、内閣官房からも最近の脅威や政府の取組状況等について、大学等への情報提供を行った。 ・ また、「新・情報セキュリティ人材育成プログラム」において、情報セキュリティを専門としつつ様々な専門分野の知見や組織経営等に必要な知識を併せ持つ人材育成の重要性について記載し、今後その方策等について具体的な検討を進めることとした。
(ニ)個人情報保護法の見直し	内閣官房 消費者庁 関係府省庁	・ 2014 年６月に、IT 総合戦略本部において「パーソナルデータの利活用に関する制度大綱」を決定し、2015 年３月 10 日に、「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」を閣議決定し、国会へ提出した。

④ サイバー空間の衛生

施策名	関係府省庁	進捗状況
(ア)新たな情報セキュリティ普及啓発プログラムの策定	内閣官房 関係府省庁	・ 国及び国民全体の情報セキュリティへの関心・理解度・対応力の強化・増進を図り、我が国の情報セキュリティ水準の向上を図るため、2014 年度以降の情報セキュリティ普及啓発に関する新たな計画として、2014 年７月に、「新・情報セキュリティ普及啓発プログラム」を策定し、公表した。
(イ)各府省庁と連携した普及啓発活動の推進	内閣官房 内閣府 警察庁 消費者庁 総務省 外務省 文部科学省 経済産業省 防衛省 関係省庁	・ 「サイバーセキュリティ月間（２月１日から３月 18 日に期間を拡大し、「情報セキュリティ月間」から名称変更）」を中心とし、関係府省庁と連携した普及啓発を実施した。また、関係省庁連絡会を２回開催して政府としての情報共有を図ったほか、官民で構成する「情報セキュリティ社会推進協議会」を立ち上げ、特に地域の活動活性化に向け、多様な主体との連携強化を図った。今後は、内閣府が推進する青少年のインターネット利用環境整備に係る取組や文部科学省の情報モラル教育とより一層歩調を合わせつつ、さらなる情報連絡を図っていく予定。
(ウ)「サイバーセキュリティの日」の取組の推進	内閣官房 内閣府 警察庁 消費者庁 総務省 外務省 文部科学省 経済産業省 防衛省 関係省庁	・ 「サイバーセキュリティの日」に当たる２月２日にサイバーセキュリティ月間キックオフシンポジウムを開催し、272 名の来場者に対し、活力ある経営を支えるサイバーセキュリティをテーマに有識者を集めて講演を行った。冒頭、内閣官房副長官から参加者に対し、経営戦略としてのサイバーセキュリティの重要性を訴求する挨拶があったほか、官房長官からのビデオメッセージにより国民一人一人の主体的なサイバーセキュリティ確保の取組の必要性について呼びかけた。
(エ)ソフトウェア教育との連携	内閣官房 文部科学省	・ 放送大学「情報コース」内の教育科目で、プライバシーやデータ保護の在り方等を含めた ICT に関する講義を引き続き配信し、普及啓発を促進した。
(オ)表彰等の充実	総務省 経済産業省	a) ・ 情報セキュリティも含めた情報化の促進に貢献した個人・企業等を表彰する情報化貢献表彰を情報化月間記念式典（2016 年 10 月開催）において実施。なお、2014 年度は、セキュリティ・キャンプ実施協議会の委員長を務め、若年層のセキュリティ人材育成等に多大な貢献をされた、S&J コンサルティング株式会社の三輪代表取締役社長等が受賞された。 b) ・ 我が国における情報技術（IT）関連分野の発展に不可欠な突出した IT 人材の発掘・育成のため、未踏 IT 人材発掘・育成事業を実施し、情報セキュリティ分野を含めたソフトウェア関連分野の開発支援プロジェクト 14 件（クリエータ数：25 人）を採択し、クリエータを支援した。
(カ)「情報セキュリティ月間」の充実	内閣官房 関係府省庁	・ 2014 年度より月間の名称を「サイバーセキュリティ月間」に改め、期間を２月１日から３月 18 日までに拡充して取り組んだ。全国約 150 の関係機関にポスターを配布し、ウェブサイト上に全国のイベント約 1,200 件の一覧を掲載したほか、多様な業種から 52 名に執筆いただいた日替わりコラムを掲載し、それらをツイッター等により国民に広く周知した。また、新たな取組として民間のニュースポータルサイトと連携した国民の意識調査、サイエンスカフェの枠組を活用した双方向型の啓発活動セミナーなど新たな取組も実施した。
(キ)国際連携を活用した国内外における普及・啓発活動の実施	内閣官房 関係府省庁	・ 2010 年 10 月に開始した「情報セキュリティ国際キャンペーン」について、2014 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、新聞広告、ラジオ放送、動画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及び ASEAN 諸国と連携したシンポジウムをそれぞれ日本で開催した。
(ク)「新たな情報セキュリティ普及・啓発プログラム」(仮称)の推進	内閣官房 関係府省庁	a) ・ サイバーセキュリティ月間の取組をはじめ、産学官民が連携した各種の普及啓発活動を推進した。また、関係する機関で構成する「情報セキュリティ社会推進協議会」を、NISC が事務局となり設置した。 b) ・ 内閣官房において、サイバーセキュリティ月間等を通じ、自己診断チェックリストの活用を進めるため、「国民を守る情報セキュリティサイト」上での情報発信を継続した。また、IPA と共同で「情報セキュリティ対策９か条」のリーフレットを新たに作成し、全国の学校・図書館等に広く配布した。これらの教材について、組織内の教育教材として活用を希望する民間企業も見られるなど、一定の進捗が図られた。

		c) ・内閣官房において、IPA と連携し、高齢者層に対しても訴求しやすい「情報セキュリティ９か条」リーフレットを作成し、「国民を守る情報セキュリティサイト」に掲載したほか、「サイバーセキュリティ月間」関連行事で資料を配布する等により周知を図った。また、高齢者向けのイベント「スマートエイジングフォーラム」での講演を通じ、普及啓発を行った。
		d) ・内閣官房において、サイバーセキュリティ月間の開始に当たり、「“費用”から“投資”へ－経営の活力を支えるサイバーセキュリティー」と題したシンポジウムを開催し、企業等の経営層や管理職層をターゲットに情報セキュリティの重要性を訴求した。
(ケ)各種メディア等を通じた普及・啓発の推進	内閣官房 警察庁 総務省 文部科学省 経済産業省	a) ・内閣官房において、「国民を守る情報セキュリティサイト」等のウェブサイトやツイッター等の活用を通じ、幅広い対象への情報提供を実施した。また、サイバーセキュリティ月間期間中には、サイバーセキュリティに関する専門家と一般国民の対話形式のセミナーを初めて開催した。また、インターネット上では、民間のニュースポータルサイトと連携した意識調査を実施したほか、様々な分野や業種でセキュリティの素養を活かして活躍する経営者、職員、ブロガー等によるコラムを日替わり掲載した。 ・「@police」において、各種ソフトウェアに係るぜい弱性情報やインターネット定点観測情報等の情報セキュリティ関連情報を適宜提供した。 ・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。
		b) ・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、2014 年 10 月の情報セキュリティ国際キャンペーン及び 2015 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重点的に推進した。
		c) ・2006 年４月から、子どもたちのインターネットの安全・安心利用に向けた啓発のための講座「e-ネットキャラバン」を全国規模で開始し、2015 年３月末迄の間にのべ 11,217 件の講座を実施した。2014 年度は、過去最多の実施件数(2015 年３月末時点で 2,789 件)となった。
		d) ・2014 年度においてはスマートフォンで無線 LAN を利用する際の情報セキュリティ上の課題や注意点等についてまとめたテキストを総務省「国民のための情報セキュリティサイト」において公表したほか、我が国の Wi-Fi 利用における情報セキュリティ意識等に関する調査結果を公表するなどして、国民の意識啓発を実施。
		e) ・第 10 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2014 を実施した。応募点数は、標語作品 33,299 点、ポスター作品 4,427 点、４コマ漫画作品 4,571 点、そして、新企画の「書写（硬筆）」5,468 点、「行動宣言」3,012 点、合計 50,777 点と過去最多となった。
		f) ・全国各地にて、地元の NPO 等と協力して「インターネット安全教室」を 95 回開催した。
		g) ・2014 年度の IPA からの情報セキュリティセミナー外部講師派遣については 197 件実施し、また 25 件のイベントの主催・出展を行った。その際に普及啓発用の資料（冊子、パンフレット、DVD 等）として 22 種・合計約 10 万５千部を配布した。 ・第 10 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2014 は全国から応募が集まり、合計 50,777 点の応募点数となった。 ・指導者育成セミナー等での普及を進め、情報セキュリティ対策支援ポータルサイト（iSupport）に登録された 2014 年度のプレゼンターは 53 名、一般ユーザは 1,371 名となった。
		h) ・IPA において、継続して JVN iPedia への脆弱性対策情報の登録・公開作業を実施。NIST の NVD で公開された脆弱性対策情報を、１営業日以内に、翻訳して JVN iPedia に登録・公開。2014 年度に登録した脆弱性対策情報は、合計 8,074 件（累計 53,235 件）。脆弱性対策に広く利用され、登録データへのアクセス数は、前年度比約 1.9 倍。 ・JPCERT/CC において、脆弱性情報ハンドリングで運用中のベンダーポータルサイトは、登録された製品開発者が PGP メールを使えない場合でも、SSL で暗号化された通信によって、安全な情報提供手段を提供した。また、JVN に掲載するベンダーステータスは、ポータルサイト経由でベンダー自身が更新するため、多くの公表案件で活用されている。

		i) ・ 2014 年度のウイルス届出件数は年間 4,537 件。このうち、実際に被害があったものは１件。また、2014 年度の不正アクセス届出件数は年間 126 件であり、実際に被害のあったものが 105 件と、全体の８割以上。ウイルス・不正アクセス情報の届出状況をレポートとして四半期毎に公開。「情報セキュリティ安心相談窓口」にて、国民一般及び企業からマルウェア及び不正アクセスに関する相談への対応を実施。2014 年度の相談受付件数は、年間 15,324 件であり、うち 8,658 件を 24 時間対応の自動応答システムで対応。
(コ)情報セキュリティに関する事故事例等に関する普及啓発の推進	内閣官房 経済産業省 関係府省庁	・ 内閣官房及び経済産業省において、各府省庁と協力し、「サイバーセキュリティ月間キックオフシンポジウム」等の講演や「国民を守る情報セキュリティサイト」等を通じ、既存の公開されている事例やインシデントに関する統計を紹介するなど情報を共有化した。
(サ)無線 LAN の情報セキュリティ確保の推進	総務省	・ 2015 年度においては地方公共団体の情報システム担当者を対象に無線 LAN の情報セキュリティ対策に関するセミナーを全国６箇所で行い、547 名が参加。あわせて、周知啓発テキストの公開、公衆無線 LAN 利用における情報セキュリティ意識等に関する調査結果の公表等を通じて、国民の意識啓発を実施。
(シ)電波利用秩序維持のための周知啓発活動の強化	総務省	・ 年間を通じた周知啓発に加え、特に 2014 年６月の電波利用環境保護周知啓発強化期間において、新聞、電車の中吊り広告、ホームページ、広報誌等の各種メディアにより電波利用のルールに関する周知啓発を実施した。
(ス)情報漏えい対策への取組	経済産業省	a) ・ 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」を継続して提供。
		b) ・ IPA が月に一度発信する「今月の呼びかけ」において、直近で悪用されている手口や事例に加え、セキュリティ対策を紹介。
(セ)サイバー攻撃高度解析機能の整備	総務省 経済産業省	・ JPCERT/CC において、サイバー攻撃解析協議会の実務者間で脅威情報を共有可能にするポータルサーバの運用を行った。 ・ 個別のサイバー攻撃について、手口や対応策などを関係組織間で情報共有し、連携した対応などを行った。
(ソ)サイバー攻撃(インシデント)対応調整支援	経済産業省	・ 再掲：１-②-(ト)
(タ)サイバー攻撃の予兆の早期把握と情報収集・分析の強化	警察庁 法務省	・ 警察庁にサイバー空間上の情報を収集する機能を持つ資機材を整備することで、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た。 ・ 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。 ・ 法務省は、政府のサイバー攻撃への対策に資する関連情報の収集・分析のため、人的情報収集等を通じたサイバー攻撃の予兆情報、特に攻撃主体に関する情報の収集・分析態勢の強化に努めるとともに、得られた情報や分析結果を適宜適切に関係機関に提供した。
(チ)サイバー攻撃事案の実態解明に係る情報収集・分析等	警察庁	a) ・ 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。 ・ 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ため、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等を行った。
		b) ・ 警察庁において、サイバー攻撃事案の実態解明に資するよう、インターネット観測技術に関する調査研究を行った。
(ツ)新しい脅威・攻撃の分析・共有	経済産業省	・ 「脅威と対策研究会」において、近年攻撃による被害が顕著になってきた標的型攻撃について、攻撃詳細と対策概要をまとめたガイドを作成し、「『高度標的型攻撃』対策に向けたシステム設計ガイド」として公開（2014 年９月）。
(テ)コンピュータセキュリティ早期警戒体制の強化	経済産業省	a) ・ 攻撃手法や脅威動向、分析手法等に関する情報共有・連携を目的とする会合を、専門家との間で、年間 10 回以上開催した。また前年度から引き続き、標的型攻撃等の手法に対して、個別のインシデントや検体の調査・解析を行うとともに、それらを含めた複数の攻撃関連情報から攻撃を分析してその結果を共有する取り組みを進めた。脆弱性情報ハンドリングは、告示に基づく調整業務だけでなく、分析用に入手したゼロデイ検体への対応を速やかに行った。2014 年度においても、様々な亜種が確認されたマルウェアで確認されたゼロデイの脆弱性について、JPCERT/CC が入手した情報を速やかに製品開発者に提供し、密な連携によって短期間での対策情報の公表に結びつけた。

		b) ・ 海外の関係機関と共有している攻撃手法の分析レポートについては、昨年度から継続しているアジアパシフィックの複数の海外組織との共有に加え、IWWN の加盟組織との共有するレポートの一部として組み入れ、定期的な共有を行なった。
		c) ・ 執拗に行われる標的型攻撃への対応支援に際して約 40 件の案件を取り扱い、必要に応じてオンサイトでの情報収集、対処、調整支援を実施するとともに、セキュリティ事業者やシステム運用事業者等との情報交換や対応支援も行なった。また、制御システムに関する不正アクセス行為等のインシデントに関して、①国内外からのインシデント報告の受付と調整対応、②国内外関連組織との連携体制強化及び普及啓発等を実施した。
		d) ・ JPCERT/CC において、国内外に設置されたフィッシングサイトに関して、一般消費者からの報告を元に、閉鎖依頼や Web サイトなどを通じた注意喚起活動を行った。また脅威の現状や新しい対策技術の反映を踏まえてガイドラインの改訂を行い公開した。
(ト)注意喚起等による情報セキュリティリスクの低減	経済産業省	・ 情報セキュリティ上の最新情報を適宜収集しつつ、特に必要とされる場合には注意喚起等による対策情報等の公表を実施。 ・ 緊急度の高い脆弱性対策情報や攻撃情報、影響度の大きなインシデントに対して、以下の注意喚起を発信し、情報セキュリティリスクの低減に貢献。 - 脆弱性対策情報：63 件（内、攻撃情報有り：32 件） - 影響度の大きなインシデント：９件 - 夏休み、年末年始等の注意喚起：３件 - その他：３件 ・ 「脅威と対策研究会」（2014 年４月、５月、６月、７月）において、近年攻撃による被害が顕著になってきた標的型攻撃について、攻撃詳細と対策概要を纏めたガイドを作成し、「『高度標的型攻撃』対策に向けたシステム設計ガイド」として公開。（2014 年９月）
(ナ)サイバー攻撃事前防止・早期対策に向けた取組の推進	総務省	a) ・ 研究開発においては、連携国を拡大するとともに、サイバー攻撃の予兆を検知する基礎技術を開発した。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試行し、ISP 連携による対応体制の確立に向けた活動を行った。
		b) ・ 2013 年に実施した、サイバー攻撃の情報に関する米国国土安全保障省との情報共有を踏まえ、日米サイバー対話（2014 年４月ワシントン）、インターネットエコノミーに関する日米政策協力対話（2014 年９月ワシントン）等の場において、さらなる研究に向けた議論を行った。
		c) ・ 日 EU サイバー対話（2014 年 10 月東京）、日仏サイバー対話（2014 年 12 月パリ）にて、サイバー攻撃事前防止・早期対策の研究状況を共有するとともに、フランス・オランダと個別に交渉し、新たに共同研究に合意することができた。また、第 21 回日 EU･ICT 政策対話（2015 年３月）においても双方のサイバー攻撃防止の取組に関する情報等の共有が行われた。
		d) ・ 新たにシンガポールとサイバー攻撃観測データの共有を開始するとともに、「日 ASEAN 情報セキュリティワークショップ（2014 年 10 月フィリピン）」にてサイバー攻撃事前防止・早期対策の研究状況を共有し、意見交換を実施した。また、サイバー攻撃事前防止・早期対策に加え、マルウェア感染防止を含めた ASEAN との総合的な技術協力「JASPER」の実施など、ASEAN 諸国との連携を推進した。
(ニ)高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築	総務省	・ 2013 年度に引き続き、一般のインターネット利用者のマルウェア感染を予防し、マルウェアの駆除を行うプロジェクトを実施。 ・ 2014 年度の成果として感染予防については、国民がよく利用するサイトに対してマルウェアが埋め込まれた場合に検知するシステムのプロトタイプを構築。また、感染駆除については、NICT の観測網と連携することで感染端末の捕捉手法を高度化するとともに、６月から実施された米国連邦捜査局（FBI）、欧州刑事警察機構（ユーロポール）が中心となった国際的なマルウェア駆除作戦において本取組を活用。
(ヌ)情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用の在り方の検討	総務省	・ 総務省において、「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」のとりまとめを行い、それを踏まえた、ISP など電気通信事業者等における関係ガイドラインの改定等を支援した。

(ネ)脆弱性に関する情報収集・提供	経済産業省		・ IPA において、2014 年度も昨年度に継続して、組込み製品（スマートデバイス１製品）に対してファジングを実践して脆弱性を検出し、検出した脆弱性は情報セキュリティ早期警戒パートナーシップへの届出を実施。ファジングが脆弱性検出に有効であることを普及啓発するため、IPA セミナーを２度実施し、51 名の技術者が参画。 ・ JPCERT/CC において、2014 年度の活動では、自ら見つけた脆弱性を届出制度に届けて調整したほか、影響範囲が大きな脆弱性については、解析チームの分析のもと、CERT/CC の公表に先駆けて JVN 公表を行う活動を実施した。
(ノ)脆弱性関連情報届出受付制度の運営及び脆弱性関連情報の提供	経済産業省		・ IPA において、継続して JVN iPedia への脆弱性対策情報の登録・公開作業を実施。NIST の NVD で公開された脆弱性対策情報を、１営業日以内に、翻訳して JVN iPedia に登録・公開。2014 年度に登録した脆弱性対策情報は、合計 8,074 件（累計 53,235 件）。脆弱性対策に広く利用され、登録データへのアクセス数は、前年度比約 1.9 倍。また、脆弱性対策情報の登録状況をレポートとして四半期毎に公開（2014 年４月、７月、10 月、2015 年１月）。 ・ JPCERT/CC における今年度の制度に基づく IPA との活動、および海外の関係機関との連携等による JVN 公表件数は 293 件（３月末時点）となった。
(ハ)ソフトウェア等の脆弱性に係るマネジメントの支援等	経済産業省	a)	・ 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サービス（VRDA フィードの配信）を運用している。また、ツイッターによる JVN 公表情報の配信も始めており、対策が必要な管理者に対する「気付き」の機会提供のサービスも拡大させている。
		b)	・ IPA から発信する注意喚起情報を外部のウェブページの一部に組入れるツール icat を継続提供中。2014 年度から経済産業省のウェブページでも利用されており、761 のウェブサイトで利用。
(ヒ)ソフトウェアや情報システムの安全な利用の推進及び脆弱性の発生を縮減するための対策の推進	経済産業省	a)	・ 脆弱性関連情報の届出受付を行いつつ、四半期毎に届出の受付状況を公開。2014 年のソフトウェア製品の届出件数は、2013 年より減少し 209 件。また、ウェブサイトの脆弱性関連情報については、2009 年以降最多の 1,118 件の届出を受付。JPCERT/CC など関係機関と協力し、ウェブサイト運営者、ソフトウェア製品開発者などに届出内容の確認・検証・通知を実施した結果、2014 年は、過去最高となるソフトウェア製品 140 件の修正が完了。また、ウェブサイトにおいては、2013 年より減少したが 633 件の修正が完了し、脆弱性対策の促進に貢献。脆弱性対策が未実施である製品のうち、開発者と連絡がとれない案件について、連絡不能開発者一覧として製品開発者名 33 件（累計 185 件）、及び製品情報 27 件（累計 155 件）を公表し、関係者からの連絡を要請。この結果、製品開発者と連絡がとれ対応が可能となった案件が４件（累計 25 件）、製品の取扱いが終了となった案件が７件（累計 15 件）。2014 年度末時点で製品開発者名を 160 件、製品情報を 148 件公表中。また、連絡不能となった案件について、脆弱性情報を公表するかを判定する公表判定委員会を開催（2014 年 11 月 26 日）。届出により脆弱性が発見されたウェブサイトの中で、対策が未実施であるウェブサイトに対し、ウェブサイト運営者への繰り返しの連絡（メール、電話による状況確認）及び催促の通知書の送付などを実施。その結果、211 件の修正を完了。
		b)	・ 今年度の活動では、Java 技術者の祭典である JavaOne での講演を CERT/CC と共同で行ったほか、セキュアコーディング導入に踏み切れない制御システム開発者に向けた厳選ルール資料の公表、制御システムイベントとして注目を集める S4 での講演など、実施している。
		c)	・ IPA では、昨年度改訂した、組込みソフトウェア開発におけるコーディングの際の注意事項やノウハウをルール集としてまとめた「組込みソフトウェア向けコーディング作法ガイド ESCR(*1)［C 言語版 ver.2.0］」のルールにセキュリティ対応の検討結果を踏まえ、CERT-C、CWE それぞれとの対応整理。対応表を 2015 年４月に公開した。また、「組込みソフトウェア向けコーディング作法ガイド ESCR［C 言語版 ver.2.0］の電子書籍版を Amazon から販売開始（2015 年２月２日発行）。 ・ さらに、ESCR[C++言語版]の改訂作業に着手。改訂に当たっては MISRA(*2)と相互に情報交換を行いながら実施。ESCR[C++言語版]の改訂版は 2016 年３月発行予定。 (*1) ESCR：Embedded System development Coding Reference (*2)MISRA（The Motor Industry Software Reliability Association）：MISRA は自動車メーカー、部品メーカー、研究者からなる欧州の自動車業界団体。MISRA が作成した C 言語のためのソフトウェア開発標準規格は世界的なコーディング作法の標準。

		d) ・ 脆弱性体験学習ツール「AppGoat」を開発経験の浅い初心者から上級者まで、脆弱性の発見方法、対策について実習形式で体系的に学べるツールとしてIPA のウェブサイトで公開中。年間 6,493 件のダウンロードを記録。 ・ 「脆弱性体験学習ツール AppGoat ハンズオンセミナー」を年間２回実施。
		e) ・ これまで調査を行ってきた情報家電や自動車、医療機器の情報セキュリティや 2012 年度に公開した「自動車の情報セキュリティへの取組みガイド」を基に、組込みシステムの情報セキュリティの普及啓発活動を実施(第 11 回情報セキュリティ EXPO[春]、2014 年５月 14～16 日)。
		f) ・ 「セキュリティテスト「ファジング」入門セミナー」を２回実施した。また、ファジングに関する講演を３回実施した。
(フ)脆弱性ハンドリングの国際調整	経済産業省	・ 2015 年８月リリースを当初からの目標として、現時点で把握できる公共の脆弱性情報データベース（CVE、NVD、ODVDB、JVN iPedia、CERT/CC VDB j 、CNVD）情報の集約を実現する計画を遂行中。
(ヘ)組込み機器の脆弱性対策の推進	経済産業省	・ 2013 年度に実施した「医療機器における情報セキュリティに関する調査」について IPA としての今後の医療機器セキュリティの向上に向けた提言をまとめ、IPA の Web サイトで公表（2014 年４月 13 日）。 ・ 2014 年度においては、組込み製品（スマートデバイス１製品）に対してファジングを実践したことにより、１件の脆弱性を検出し、ファジングが脆弱性検出に有効であることを実証。また、検出された脆弱性は、情報セキュリティ早期警戒パートナーシップへの届出を実施。
(ホ)情報システム等の安全性・信頼性等に関する利用者への品質説明力の強化	経済産業省	・ 利用者への品質説明力の強化については、品質説明力強化の課題となっている、品質基準の定義、審査方法等に関して、品質基準に関する国際規格および取組み事例を整理し、啓発書、解説書とのダイジェスト版として「つながる世界のソフトウェア品質ガイド（ダイジェスト版）」を IPA が 2015 年３月に公開した。また、昨年度に引き続き、品質に関する制度構築を目指す（継続を含め）４団体(*)について支援（一般社団法人コンピュータソフトウェア協会（CSAJ）がクラウド向けパッケージソフトウェア品質認証制度を開始した（2014 年９月））。 (*)一般社団法人コンピュータソフトウェア協会（CSAJ）、一般社団法人ディペンダビリティ技術推進協会（DEOS）、一般社団法人 IIOT、ワイヤレススマートユーティリティネットワーク利用促進協議会。
(マ)スパムメール対策の強化	消費者庁 総務省	a) ・ 総務省及び消費者庁において、2014 年度は特定電子メール法に基づき、計７件の行政処分を実施した。 ・ 2014 年９月には、同法の措置命令違反による初の逮捕者が出た。
		b) ・ 2014 年 10 月、迷惑メール対策に関する国際連携の枠組みであるロンドン・アクション・プラン（LAP）の第 10 回目の定期会合(LAP 10 Tokyo)がアジア地域において初めて我が国で開催され、日本の送信ドメイン認証技術等の技術的対策の取組状況等について説明を行ったほか、各国の迷惑メールに関する技術的対策について情報交換を行った。 ・ 2014 年 10 月、LAP 10 Tokyo と併催する形で第 11 回迷惑メール対策カンファレンスが開催され、送信ドメイン認証技術等迷惑メール対策技術の導入推進を含む議論が行われた。
		c) ・ 2014 年 10 月、迷惑メール対策に関する国際連携の枠組みであるロンドン・アクション・プラン（LAP）の第 10 回目の定期会合(LAP 10 Tokyo)がアジア地域において初めて我が国で開催され、日本の送信ドメイン認証技術等の技術的対策の取組状況等について説明を行ったほか、各国の迷惑メールに関する技術的対策について情報交換を行った。 ・ 引き続き、総務省・民間団体の取組として中国、ブラジル等と迷惑メールの送信元 IP アドレスの交換を実施しており、インドやカナダとも同取組を行うべく調整を継続している。
		d) ・ 「迷惑メール追放支援プロジェクト」としてインターネット接続サービス事業者への違法スパムメールに関する情報提供を引き続き実施した。
(ミ)暗号・認証技術等を用いた通信プロトコルの利用による安全な通信環境の実現	総務省	・ 2013 年に設立した「暗号プロトコル評価技術コンソーシアム」と連携し、SSLv3 に対する POODLE attack 等、通信プロトコルの脆弱性に対する安全性評価を実施し、評価結果を集約して早期に情報提供した。 ・ 広く普及している暗号・認証プロトコルである SSL/TLS についての推奨利用ガイドラインを作成し、CRYPTREC を通じて公開した。さらに最新攻撃状況を踏まえて 2014 年度改訂版を作成した。

(ム)IPv6 ネットワークのための情報セキュリティ検証環境の構築	総務省	・ IPv6 技術検証協議会において、IPv6 環境における脅威シナリオの検証作業と対策手法の検討を行った。また、協議会での議論を元に NICT において対策手法の実装と有効性の検証を行った。検証結果は協議会の最終報告として一般公開するとともに、ITU-T SG17 において勧告化を実施した。 ・ さらに IPv6 の脅威に関する対策手法として NDP Guard と呼ばれるシステムを開発し、その評価結果を国内研究会において公開した。また IPv6 におけるセキュリティマネジメント手法についてまとめ、ITU-T SG17 において勧告化を実現した。

⑤ サイバー空間の犯罪対策

施策名	関係府省庁	進捗状況
(ア)サイバー攻撃対策に係る態勢等の強化	警察庁	・ サイバー犯罪・サイバー攻撃手法の高度化等に対応するため、以下のとおり施策を実施して、警察におけるサイバーセキュリティ対策に係る態勢等の強化を推進した。
		a) ・ 2014 年４月、警察庁にサイバーセキュリティ対策を担当する長官官房審議官及び長官官房参事官を設置して司令塔機能を強化した。 ・ 新組織の下、2014 年９月に、今後重点的に取り組むべき「サイバーセキュリティ重点施策 2014-2015」を策定し、同施策の下で、サイバー空間の脅威への警察全体の対処能力を強化した。
		b) ・ 2014 年４月、警察大学校にサイバーセキュリティ研究・研修センターを設置し、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。
		c) ・ 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を実施した。 ・ 都道府県警察にサイバー犯罪の取締りを行うための資機材を整備した。
		d) ・ サイバー攻撃の予兆を把握するため、サイバー空間上の情報を収集する機能を持つ資機材を整備するとともに、「サイバー攻撃特別捜査隊」を中心として、全国の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した。
		e) ・ 警察庁に設置した「サイバー攻撃分析センター」にサイバー攻撃に関する捜査情報、不正プログラムの解析情報等を集約し、その実態を解明するために必要な分析機能を持つ資機材を整備することでその態勢を拡充し、情報の収集・分析や広域捜査・国際捜査を推進するための体制を強化した。
		f) ・ セキュリティ関連事業者が保有しているインターネット上の脅威に関する技術情報及びその分析結果に係る情報の提供を受けるなどし、サイバー攻撃対策に係る体制等を強化した。
		g) ・ 警察庁において各都道府県警察のサイバー攻撃対策要員の事案対処能力・技術力の維持・向上のため、民間企業への委託研修を実施した。 ・ 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。
		h) ・ 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するために必要な経費を要求した。
(イ)日本版 NCFTA の創設に向けた検討	警察庁	・ 企業等と共に業務開始に向けた準備を進めた結果、2014 年 11 月、日本版 NCFTA である一般財団日本サイバー犯罪対策センター（JC3）が業務を開始した。 ・ 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。
(ウ)サイバー空間の安全と秩序を維持するための民間との連携強化	警察庁	・ 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、利用者の事後追跡可能性の確保のための取組や防犯情報の提供を行うなど、事業者との連携強化を推進した。 ・ 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。
(エ)犯罪に強い IT 社会構築のための官民連携に向けた取組の推進	警察庁	・ 「官民連携を通じたサイバー犯罪に対処するための人材育成等」をテーマに平成 26 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。

(オ)サイバー犯罪の被害防止対策の推進	警察庁	・ 私事性的画像記録の提供等による被害の防止に関する法律の成立を受け、警察庁ウェブサイトに広報啓発用のページを追加した。 ・ 2014 年 10 月の情報セキュリティ国際キャンペーン及び 2015 年２月のサイバーセキュリティ月間において、サイバー犯罪の被害の防止のための対応策等を警察庁ウェブサイトに掲載するなどの広報啓発活動を実施した。 ・ 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 2014 年 10 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。
(カ)不正アクセス禁止法の適正な運用を始めとした不正アクセス防止対策の推進	警察庁 総務省 経済産業省	・ 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。 ・ 2014 年中の不正アクセス行為の発生状況等を、2015 年３月 19 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。
(キ)フィッシング対策協議会	経済産業省	・ ２回の APWG（Anti-Phishing Working Group）主催の国際会議に参加し、国内外関係者と情報交換を行った。そのうち１回は JPCERT/CC が「Phishing Trends in Japan and the Counteraction as the Council of Anti-Phishing Japan」と題した講演を行い、海外関係者も含む参加者に対して、日本のフィッシング動向とフィッシング対策協議会の取り組みについて発表を行った。これら海外から得られた知見は、フィッシング対策協議会の WG 会等を通じて共有されている。
(ク)重要インフラに対するサイバーテロ対策に係る官民の連携強化	警察庁	・ 都道府県警察において、重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供を行うことにより、昨今の我が国政府機関等に対するサイバー攻撃事案の発生等を踏まえた、サイバーテロに対する危機意識の醸成を図るとともに、事案発生を想定した共同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、重要インフラ事業者等の意向を尊重し、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。
(ケ)サイバーインテリジェンス対策に係る官民の連携強化	警察庁	・ 警察庁において、情報窃取の標的となるおそれのある先端技術を有する民間事業者等と構築した「サイバーインテリジェンス情報共有ネットワーク」について、その参画事業者数を 6,833（2015 年１月）まで拡大した。 ・ 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、2014 年中に 1,723 件の標的型メール攻撃を把握し、その分析結果について、同ネットワーク参画事業者等及び内閣サイバーセキュリティセンターと共有した。また、警察庁で把握した攻撃に使用された不正プログラムの検体及び不正接続先アドレスについて、民間の情報セキュリティ企業と共有し、官民連携した対策の向上を図った。
(コ)ログの保存の在り方の検討	警察庁 総務省	・ 警察庁と総務省で情報交換を含め、協議を行ったほか、総務省の研究会において、検討を行った。
(サ)デジタルフォレンジックに係る取組の推進	警察庁	a) ・ サイバー犯罪捜査に従事する警察職員に対し、電磁的記録の解析等に係る研修を実施した。 ・ 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。 ・ 新設した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。 b) ・ 高度情報技術解析センターを中心として、不正プログラムの解析のための体制等を強化し、2014 年においては、1,122 件（2013 年比約６％増）の不正プログラムを解析した。 c) ・ デジタルフォレンジックを取り巻く課題とその対応方策に関する調査研究を行った。
(シ)サイバー犯罪対策のための人材育成の強化	法務省	・ 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。
(ス)サイバー防犯ボランティア育成の推進	警察庁	・ 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、2014 年末現在の全国のサイバー防犯ボランティア数は、199 団体 7,474 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。

(セ)スマートフォンの安全利用のための環境整備	警察庁	・ 警察庁において、スマートフォンを利用した児童の犯罪被害が急増していることにを踏まえ、携帯電話販売店に対するフィルタリング推奨状況等実態調査を実施するとともに、その結果について携帯電話事業者に説明した上、保護者に対するフィルタリングの説明強化等について要請した。 ・ 都道府県警察において、スマートフォン等を利用して児童が犯罪の被害に遭うことを防止するため、関係機関・団体と連携した児童や保護者に対する啓発活動を推進した。
(ソ)スマートフォン利用者等を狙ったサイバー犯罪への対処	警察庁	・ 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。

⑥ サイバー空間の防衛

施策名	関係府省庁	進捗状況
(ア)サイバー情報収集装置の整備	防衛省	・ サイバー空間における脅威が複雑化・巧妙化している状況の中で、サイバー攻撃の兆候を早期に察知し、未然防止に資する情報収集装置について、2015年３月に整備し、運用を開始した。
(イ)次期サイバー防護分析装置のシステム設計等	防衛省	・ サイバー防護分析装置の換装に向けて、防衛省に対するサイバー攻撃への対処を統合的に実施するためのシステム設計等を 2015 年３月までに実施した。
(ウ)サイバー防護分析装置の機能強化	防衛省	・ 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、2015 年３月にサイバー防護分析装置の情報収集機能や分析機能、演習機能の強化等、技術の進化に対応した機能向上等を実施した。
(エ)防衛情報通信基盤(DII)の整備	防衛省	・ 防衛省・自衛隊の各部隊等間における確実な指揮命令の伝達と迅速な情報共有を行うために不可欠な防衛情報通信基盤（DII）のクローズ系に最新技術を適用し、セキュリティの向上を図りつつ、2015 年３月までに情報共有機能を強化した。
(オ)ネットワークサイバー攻撃対処技術の研究	防衛省	・ サイバー攻撃の生起時に、ネットワーク内において迅速に経路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実施に向け、2015 年３月までに契約を完了した。
(カ)サイバー演習環境構築技術に関する研究	防衛省	・ サイバー演習環境の構築技術に関する研究について、2015 年３月までに基本設計を完了し、細部設計を開始した。
(キ)ネットワーク監視態勢の強化	防衛省	・ 2015 年３月に防衛情報通信基盤（DII）用のネットワーク監視器材の機能強化を行った。
(ク)陸自電算機防護システムの整備等	防衛省	・ 陸上自衛隊の情報システムを対象とした陸自電算機防護システム等、各自衛隊の情報システムを監視、防護するための機材を 2015 年３月に整備し、運用を開始した。
(ケ)国外におけるサイバー攻撃関連情報に関する情報収集・分析機能強化	防衛省	・ 防衛省において、情報本部等による国外におけるサイバー攻撃関連情報の収集・分析態勢の強化・向上のため、検討を実施している。
(コ)情報保証に係る最新技術動向等の調査研究	防衛省	・ 情報システムの情報保証を確保するため、サイバー攻撃及びサイバー攻撃対処に係る最新技術動向並びにサイバー攻撃等対処要員の確保のための施策等について調査を実施し、2015 年３月に防衛省におけるサイバー攻撃等対処の資とする内容を含む報告書に取りまとめた。
(サ)人材育成及び外国との連携強化	防衛省	・ 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。また、日米 IT フォーラム（2015 年１月）、日越ＩＴフォーラム（2015 年３月）等を実施し、米国及び諸外国との連携を強化した。
(シ)民間企業等との連携強化	防衛省	・ 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 2015 年２月に実施し、また、防衛省と防衛産業によるサイバー攻撃対処に係る情報を、情報の保全性を確保しつつ、迅速かつ効率的・効果的に共有するための新たな官民情報共有システムを 2015 年２月に導入した。
(ス)国家レベルのサイバー攻撃への対応の強化	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省 関係府省庁	・ 2014 年 11 月に成立したサイバーセキュリティ基本法を受け、情報セキュリティ政策会議において、「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（2014 年 11 月 26 日決定）を策定した。同方針に基づき、政府機関等へのサイバー攻撃の常時監視を行う GSOC の機能強化や、政府機関、独立行政法人や重要インフラ事業者等におけるインシデント情報の集約機能や助言機能等の強化に向けた、官民連携のスキームの強化・構築等について検討を行い、可及的速やかに結論を得ることとしている。

２　「活力ある」サイバー空間の構築

① 産業活性化

施策名	関係府省庁	進捗状況
(ア)M2M における情報セキュリティの確保に関する検証等の推進	総務省	・ M2M における情報セキュリティの確保が課題になっていることを踏まえ、M2M の情報セキュリティ技術の確立のための実証事業について検討を実施した。
(イ)スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進	経済産業省	・ エネルギー設備導入等に伴うサイバーセキュリティ確保に向けて、CSSC を通じて、ホワイトリスト、サイバー攻撃の早期認識技術、ログ蓄積分析技術の研究開発を実施した。
(ウ)新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発	総務省	・ クラウド等の新たな情報流通形態に対応するため、暗号化したままセキュリティレベルの更新と演算ができる準同型暗号方式を世界で初めて開発、暗号化することでプライバシーを保護したままデータマイニングの一手法である線形回帰演算が効率よく計算できることを示した。 ・ NICT で開発した代理再暗号化技術を活用してクラウド上でセキュアに情報共有を行えるセキュアストレージシステムを提案した。2014 年度はこれを応用し、クラウドを介したセキュアな自動情報共有システムを試作した。
(エ)省リソースデバイスにおける情報セキュリティ技術の研究開発	総務省	・ RFID タグを応用した暗号プロトコルとして、高速に複数のタグへの読込が行なわれたことに対しての証拠を残すプロトコルの研究開発を行った。 ・ リソースの少ない M2M デバイスにおいて、チップの物理的特性を利用した物理的複製困難関数（PUF）を活用した理論的な安全性モデルを提案した。
(オ)クラウドサービスレベルのチェックリスト等の普及・促進	経済産業省	・ 経済産業省ホームページにて該当のチェックリストを公表するとともに、講演等においてクラウドを安全に使うための仕組みとして紹介を行った。
(カ)クラウドコンピューティングの国際標準化に向けた取組	総務省 経済産業省	a) ・ 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 が主催する香港会合（2014 年４月）、メキシコ会合（2014 年 10 月）に参加し、我が国の 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事案の提案を行った。 b) ・ 2011 年に策定した「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」の改訂を行い、2014 年３月に、当該ガイドライン改訂版とともにクラウドセキュリティガイドライン活用ガイドブックを 2014 年３月に公開した。本ガイドラインを国際標準化するために、英訳したものを JTC1/SC27 の主催する会合に提案しており、関係各国の意見も踏まえた形で本ガイドラインをベースにした国際標準が 2015 年度中に発表される見通しである。
(キ)制御システムセキュリティの国際標準に基づく評価・認証機関設立	経済産業省	・ 再掲：１-②-(ハ)
(ク)制御システムセキュリティ評価・認証の国際相互承認	経済産業省	・ 再掲：１-②-(ヒ)
(ケ)国際的なルールに基づくセキュリティ製品の貿易の推進	経済産業省	・ デジタル複合機のためのセキュリティ要件（PP:Protection Profile）を米国と共同で開発している。（完成目標：2015 年７月末） ・ USB メモリ、ND/FW（ネットワークデバイス/ファイアウォール）、FDE（ディスク全体暗号化）等の共通セキュリティ要件（cPP）の開発に参画し、ND/FW と FDE の cPP の完成に貢献した。
(コ)自動車に係る情報セキュリティの確保	経済産業省	・ 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セキュリティに係る課題と対策について情報交換を図るとともに、戦略的イノベーション創造プログラム（SIP）において、欧米等海外におけるセキュリティの標準化等の動向を詳細に分析した。
(サ)安全性確保のためのソフトウェア等のリバースエンジニアリングの適法性の明確化	文部科学省	・ 法制的に難しい論点を含むものであるため、現時点において措置を講ずるには至っていないが、引き続き、文化庁としても法制的な検討を行っていくところである。

② 研究開発

施策名	関係府省庁	進捗状況
(ア)「情報セキュリティ研究開発戦略」の研究開発の推進	内閣官房 関係府省庁	・ 研究開発については、昨今のサイバーセキュリティを取り巻く環境変化を分析した上で、技術戦略専門委員会の意見も踏まえ、2014 年７月、「情報セキュリティ研究開発戦略」（2011 年７月）の改定を行った。各府省庁と協力し、「情報セキュリティ研究開発戦略（改定版）」を踏まえ、施策を推進している。
(イ)スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進	経済産業省	・ 再掲：２-①-(イ)
(ウ)標的型攻撃の対策技術に関する研究開発	総務省	・ 標的型攻撃によって組織内部に侵入したマルウェアが、組織内外のネットワークとの間で行う異常な通信を検出するため、組織内ネットワークを流れる通信のリアルタイム分析環境および大規模蓄積環境を NICT において整備するとともに、いくつかの異常通信検知エンジンの開発を行った。また、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 改の実用化に向けた開発を実施した。
(エ)情報セキュリティ強化を含むビッグデータ利活用のための研究開発	文部科学省	・ 他の研究開発課題に重点化している中で、予算措置をしていないため本施策に取組めていない。
(オ)新世代ネットワーク基盤技術に関する研究開発	総務省	・ 2013 年度に実施した、複合サービス収容ネットワーク基盤技術の部分実証システム構築に必要な大規模認証・プライバシー保護機構の詳細設計に基づいた開発と実装を進めた。
(カ)量子情報通信ネットワーク技術の研究開発	総務省	・ フィールド環境での量子鍵配送装置の動作試験を継続した。また、伝送光パルスの強度揺らぎの評価と安定化、および安全性への影響の解析を行った。さらに、量子鍵配送ネットワーク上での効率的な鍵管理アーキテクチャの検討とプログラム実装を行った。
(キ)ネットワーク等の安全性・信頼性確保に資する情報セキュリティ技術に関する研究開発	総務省	・ サイバー攻撃観測技術の高度化に向けて、能動的観測システムの開発と小規模実証実験を実施した。また、国際的な技術連携を進めるとともに、研究成果展開の一環として、2013 年 11 月から地方自治体へのサイバー攻撃アラート情報の提供を実施中。また、2014 年 12 月より総務省の ACTIVE プロジェクトへの観測データの提供を開始し、ISP 経由で感染ユーザへの注意喚起のバックデータとして活用された。 ・ セキュアネットワークの設計・評価と最適構成技術として、Android スマートフォンのアプリケーション利用時におけるリスクの評価、可視化を行うためのシステムを構築し、従来法に比べて高精度でリスク評価できる結果を得た。 ・ 次世代暗号として期待されるペアリング暗号や格子暗号等の安全性評価を行い、CRYPTREC を通じて公開した。 ・ SSL/TLS サーバ認証等で利用されている公開鍵の検証ツールを開発、JIPDEC に技術移転し、我が国の電子入札、電子申請、電子契約等を支える認定認証業務の安全性検証に貢献した。
(ク)情報通信構成要素の安全性検証技術の高度化に関する研究開発	総務省	・ 通信プロトコルの安全性を理論的かつ網羅的に検証するツールである ProVerif を使用する際、安全性検証を確実に進めることを目的として検証過程を確認しながら進めることが可能な手法を構築した。
(ケ)サイバーセキュリティ研究基盤の構築	総務省	・ 攻撃トラフィックやマルウェア検体等のセキュリティデータセットの安全な外部利用を可能にする研究基盤（NONSTOP）を構築し、国内複数大学との連携の下、NONSTOP を運用した。また、マルウェア対策研究人材育成ワークショップ 2013 および 2014 向けに、NONSTOP 経由で攻撃データセットの安全な提供を行い、国内 14 組織が研究に利活用した。
(コ)システムにおける適切な情報セキュリティ設定を自動的に導出する技術の研究開発の推進	総務省	・ 企業内ネットワークに対して、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を行う技術の研究開発に着手した。
(サ)セキュアでグリーンなクラウドコンピューティング環境の整備	経済産業省	・ 予算事業「中小企業等省エネルギー型クラウド利用実証支援事業」において、クラウド基盤ソフトウェアが抱える課題を解消し、その成果を世の中に公表する実証を、６件実施した。この実証にて、省エネ性・信頼性・運用性の向上を実現している。
(シ)スマートフォンにおけるリスクの可視化	総務省	・ Android スマートフォンのアプリケーション約 10 万件のリスク分析結果を有する知識ベースを作成し、当該知識ベースを活用した Android アプリケーションに対するリスク分析・可視化システムを構築した。

(ス)イノベーション創出を支える情報基盤強化のための新技術開発	文部科学省	・ 耐災害性強化に向けて、分散システムについては、基盤システムを構築し、シミュレータによる計測分析により、50%の機器喪失下においても災害直後に 90%の情報にアクセスできることの確認、自己修復機能については、シミュレートするためのモデルを構築する等、各機能の高度化に向けた取組を実施した。 ・ 2014 年６月、2015 年３月に東北大学においてワークショップ、シンポジウムを開催した。
(セ)M2M における情報セキュリティの確保に関する検証等の推進	総務省	・ 再掲：２-①-(ア)
(ソ)省リソースデバイスにおける情報セキュリティ技術の研究開発	総務省	・ 再掲：２-①-(エ)
(タ)新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発	総務省	・ 再掲：２-①-(ウ)
(チ)サイバー攻撃事前防止・早期対策に向けた取組の推進	総務省	a) ・ 再掲：１-④-(ナ)、３-②-(ク)
		b) ・ 再掲：１-④-(ナ)、３-②-(ク)
		c) ・ 再掲：１-④-(ナ)、３-②-(ク)
		d) ・ 再掲：１-④-(ナ)、３-②-(ク)
(ツ)サイバー攻撃の解析・検知に関する研究開発	総務省	・ サイバー攻撃に遭いやすい利用者の行動特性、組織内の通信状況等を把握することで標的型攻撃を検知する技術について、複数のセンサーを統合的に管理する技術、行動特性からサイバー攻撃に遭いやすい利用者を抽出する技術等の研究開発を実施。 ・ また、ネットワーク構成や端末間のアクセス制御を素早く変更することで標的型攻撃の被害軽減及び感染端末の検知を行うための技術について、処理能力の向上等、実用化に向けた研究開発を実施。
(テ)サイバーセキュリティ研究開発拠点の構築	総務省	・ 「サイバー攻撃対策総合研究センター（CYREC）」を構築し、サイバー攻撃のモニタリング（観測）・解析の高度化に向け、官民の英知を集めたオールジャパン体制での研究開発・実証実験を進めた。また、同センターにおいては、産業界との連携を強化するとともに、高度情報セキュリティ人材の育成に貢献するため、日本最大の CTF 大会 SECCON に可視化エンジン NIRVANA 改を導入した。
(ト)制御システムセキュリティに関する研究開発	経済産業省	・ 前年度までの研究成果に基づき、制御機器のセキュリティ認証技術基盤を確立し、世界共通の制御機器の認証制度を日本において 2014 年４月に開始するとともに、セキュリティ検証のための技術開発として、ホワイトリスト、サイバー攻撃の早期認識技術、ログ蓄積分析技術の研究開発を実施した。
(ナ)産業技術総合研究所（AIST）における研究開発の促進	経済産業省	・ デバイス I/O やシステム下位層から、マルウェアやサイバー攻撃などを監視したり、USB メモリ、通信デバイスなど不要なデバイスやデータへのアクセスを制限したりするための仕組みに関する先端的な研究開発を行った。成果を CODEBLUE、制御システムセキュリティカンファレンス、Black Hat SanPaulo、Industrial Control Systems Joint Working Group などで発表すると共に、一部の機能については CSSC においても試作を行った。

③ 人材育成

施策名	関係府省庁	進捗状況
(ア)「新・情報セキュリティ人材育成プログラム」の推進	内閣官房	・ 情報セキュリティ政策会議普及啓発・人材育成専門委員会での議論を経て、2014 年５月 19 日に「新・情報セキュリティ人材育成プログラム」を情報セキュリティ政策会議決定した。その後、プログラムに基づく施策を各省において実施している。
(イ)リカレント教育の促進	文部科学省	・ 「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いる。当該事業において、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）等の産学協働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。（事業全体のネットワーク形成状況（2015 年３月時点）：大学のべ 96 校、企業のべ 107 社）
(ウ)情報セキュリティに関する教育における産学連携の促進	文部科学省 経済産業省	a) ・ 「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いる。当該事業において、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）等の産学協働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。（事業全体のネットワーク形成状況（2015 年３月時点）：大学のべ 96 校、企業のべ 107 社） b) ・ 産業団体と教育機関の情報共有の場を継続的に運営した。また、実践教育の有識者によるＷｅｂコミュニティを開設し、テーマ別の情報共有・意見交換を開始した。 c) ・ 「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いる。当該事業において、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）等の産学協働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。（事業全体のネットワーク形成状況（2015 年３月時点）：大学のべ 96 校、企業のべ 107 社）
(エ)大学等における情報セキュリティに関する教育	内閣官房 総務省 文部科学省 経済産業省	a) ・ 「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いる。当該事業において、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）等の産学協働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。（事業全体のネットワーク形成状況（2015 年３月時点）：大学のべ 96 校、企業のべ 107 社） b) ・ 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、「新・情報セキュリティ人材育成プログラム」において、情報セキュリティに関する研究科等の設置の重要性について記載し、高等教育機関に対し、国や産業界等が求める人材像を提示していくことについて、具体的な検討を行っている。
(オ)情報セキュリティに係る競技会・演習等の実施	総務省 経済産業省	a) ・ 夏のセキュリティ・キャンプ全国大会及び日本各地でセキュリティ・ミニキャンプを開催した。全国大会においては 42 名の修了生を輩出した。また、ミニキャンプについては、今年は全国５か所で実施し、昨年度２か所から大きく数を増やした。 b) ・ セキュリティ・キャンプ全国大会において半日の CTF を実施した。また、SECCON CTF 2014 を後援するとともに SECCON CTF の講師や参加者としてセキュリティ・キャンプ修了生が協力した。 c) ・ 夏のセキュリティ・キャンプ全国大会及び日本各地でセキュリティ・ミニキャンプ（５箇所）を開催した。また、SECCON CTF 2014 を後援するとともに、SECCON CTF の講師や参加者としてセキュリティ・キャンプ修了生が協力した。
(カ)横断的キャリアパス・モデルの普及、人材育成計画の策定促進	経済産業省 関係府省庁	・ 情報セキュリティ人材育成の必要性を経営者に訴えることを目的のひとつとして、IPA において「情報セキュリティ上の脅威から企業を護るための人材育成ガイド」を 2014 年８月に発行。
(キ)スキル、資格、教育プログラム等の整理	経済産業省	・ IPA において、IT スキル標準等の各種スキル標準と共通キャリア・スキルフレームワーク(CCSF)を統合し、「i コンピテンシディクショナリ(以下「iCD」」（試用版）として 2014 年７月に公開。また、高度化・多様化している情報セキュリティの脅威に対応する情報セキュリティ人材の役割をモデル的に定義し、iCD の構造に合わせ、「情報セキュリティ強化対応スキル指標」として 2014 年８月に公開し、各種セミナーや教育事業者との協業による説明会等で普及を促進。

(ク)情報セキュリティ資格の周知及び普及	内閣官房 総務省 経済産業省	a) ・ 情報処理技術者試験を周知し、更なる普及・定着化を図るため、企業や業界団体、教育機関及び全国の書店等へ試験のパンフレット等を配布。また、企業や教育機関等への個別訪問を実施し、訪問先での試験の活用の依頼と活用事例の収集を実施。
		b) ・ サイバーセキュリティ月間を中心に、各地での講演会等を通じて資格及び教育プログラムを含めた人材育成施策についての啓発活動を行った。また、NISC ホームページや「国民を守る情報セキュリティサイト」等により、関連する情報発信を行った。
(ケ)情報セキュリティに関する国家試験の改善	経済産業省	・ 情報セキュリティに関する出題の強化・拡充については、IT パスポート試験は 2014 年５月７日から、情報セキュリティスペシャリスト試験を含むその他の試験区分は 2014 度春期試験から実施済み。
(コ)情報処理技術者試験制度に関する在り方についての検討	経済産業省	・ 2015 年１月に創設された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において検討し、情報セキュリティマネジメントに関する新たな試験区分を創設する予定。（2016 年目途）
(サ)IT スキル標準の活用（公共機関での活用を含む）	経済産業省	・ IT スキル標準等の各種スキル標準と共通キャリア・スキルフレームワーク（CCSF）を統合し、「i コンピテンシディクショナリ（以下「iCD」」（試用版）として 2014 年７月に公開した。 ・ 2013 年度に実施した大学や社会人の有識者による「IT 人材における情報セキュリティの育成ニーズ・課題調査」の結果を踏まえ、2014 年８月に「情報セキュリティ強化対応スキル指標」を公開するとともに、スキル指標の活用や情報セキュリティを担う人材の育成をわかりやすく解説した冊子「情報セキュリティ上の脅威から企業を護るための人材育成ガイド」を発行した。
(シ)グローバル水準の人材の育成	内閣官房 関係府省庁	・ インシデント対応に関する国際連携を議題とする FIRST 会合（2014 年６月）や情報技術世界会議（WCIT）2014（2014 年９月）、日米重要インフラ防護（CIP）フォーラム（2014 年 12 月）などの国際会議等に職員や有識者を派遣するなど、グローバルレベルでの見識の拡大に努めた。 ・ 重要情報インフラ防護に関する国際連携を議題とする Meridian 会議等の国際会議や米国、ASEAN 諸国と連携した国際シンポジウム等を国内で開催し、サイバーセキュリティ分野における人材の能力の涵養に努めた。特に米国とのシンポジウムは若手人材育成をテーマの中心に据えた。
(ス)大学に対する情報セキュリティに関する最新情報の提供	内閣官房 総務省 文部科学省 経済産業省	・ 再掲：１-③-(ナ)
(セ)サイバー攻撃の事例共有、ケースを基にした教材等の開発	内閣官房 関係省庁	・ 「新・情報セキュリティ人材育成プログラム」において、情報セキュリティのスキル向上のための実践的取組の１つとして、サイバー攻撃の事例共有、ケースを基にした教材等の開発について記載し、関係機関にその実施を依頼しているところ。
(ソ)情報セキュリティに関する教員の養成	内閣官房 総務省 文部科学省 経済産業省	・ 「新・情報セキュリティ人材育成プログラム」において、情報セキュリティに関する教員の養成について記載したところであり、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ところ。
(タ)情報セキュリティ監査知識を有する人材の育成等の促進	内閣官房 経済産業省	・ 「新・情報セキュリティ人材育成プログラム」において、情報セキュリティ対策を組織の内部及び外部から客観的かつ公正に評価できる情報セキュリティ監査知識を有する人材の育成について記載したところであり、引き続き関係省庁、団体等と検討していく。
(チ)情報セキュリティ人材育成に係る枠組みの検討	経済産業省	a) ・ IPA の公開 Web「IT 人材育成 iPedia」において、産学連携 IT 人材育成プラットフォームを運用し、講座の自立的な継続改善や地域連携団体の活動に関する情報提供・共有を行った。
		b) ・ 高等教育機関の情報系学科学生に IT 業務の魅力を紹介する広報誌の制作・配布を行った。全国の 330 学科に 35,000 部を配布し、IT が支え・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。
		c) ・ IT スキル標準等の各種スキル標準と共通キャリア・スキルフレームワーク（CCSF）を統合し、「i コンピテンシディクショナリ（以下「iCD」」（試用版）として 2014 年７月に公開した。 ・ iCD においては、前述（47 頁、（キ））の「情報セキュリティ強化対応スキル指標」に加え、IT 人材が担う役割（タスク）や保有すべきスキルを最新化し、参照モデルとして公開した。

		d) ・ ITPEC は継続的にアジア共通統一試験を実施。バングラデシュが 2014 年９月に日本と相互認証協定を締結し、ITPEC に加盟した。この結果、日本との相互認証協定の締結国が 11 か国から 12 か国に拡大した。さらには、我が国の IT スキル標準の普及を図るため、タイでの導入企業を選定し、トレーニングを実施した。
(ツ)制御システムセキュリティに係る人材育成	経済産業省	・ 制御システムユーザ等に対し、電力、ガス、化学、ビルの４分野において、実際にサイバー攻撃が発生することを体感することができるサイバー演習を CSSC のテストベッドを活用して実施し、合計 80 名以上が参加した。
(テ)政府機関等による民間セキュリティ人材の一時的受入れ	内閣官房 関係府省庁	・ 「情報セキュリティ人材育成プログラム」及び「情報セキュリティ研究開発戦略」の改定等に係る検討に際し、NICT、AIST、IPA 等人材育成、研究開発等の諸課題についての連絡会、意見交換等を実施した。
(ト)優秀な外部人材の活用	内閣官房 関係府省庁	・ 再掲：１-①-2）-(ソ)

④ リテラシー向上

施策名	関係府省庁	進捗状況
(ア)初等中等教育段階における情報に関する教育	文部科学省	a) ・ 2006 年４月から、子どもたちのインターネットの安全・安心利用に向けた啓発のための講座「e-ネットキャラバン」を全国規模で開始し、2015 年３月末迄の間にのべ 11,217 件の講座を実施した。2014 年度は、過去最多の実施件数（2015 年３月末時点で 2,789 件）となった。 ・ 現行の学習指導要領を踏まえ、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ため、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た（2014 年 10 月及び 2015 年１月）。
		b) ・ 地方自治体の情報教育担当を集めて実施した会議（2014 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（2014 年 10 月及び 2015 年１月）。
(イ)情報セキュリティ・サポーターの育成・活用	総務省	・ 情報セキュリティ・サポーターによる普及・啓発活動に対して後援を行うなど必要な支援を実施した。
(ウ)情報セキュリティ相談窓口の充実	内閣官房 関係府省庁	・ 「国民を守る情報セキュリティサイト」において、各府省庁及び関係機関が設置している情報セキュリティに関する相談窓口を紹介する取組を行った。 ・ また、民間のニュースポータルサイトと連携し、サイバーセキュリティに関する公的な相談窓口に関する認知度の調査を行うとともに、設問に付した解説によるサイト訪問者への啓発を実施した。
(エ)スマートフォン等による安心・安全な無線 LAN の利用の推進	総務省	・ 利用者の無線 LAN へのオフロードを推進するため、2014 年度においては無線 LAN を利用する際の情報セキュリティ上の課題や注意点等についてまとめた利用者向けテキストを総務省「国民のための情報セキュリティサイト」において公表したほか、我が国の WiFi 利用における情報セキュリティ意識等に関する調査結果を公表するなどして、利用者の意識啓発を実施した。
(オ)官民連携によるスマートフォン等の情報セキュリティ確保の推進	総務省 経済産業省	a) ・ スマートフォン等の普及に伴い発生する情報セキュリティ上の課題の１つである無線 LAN のセキュリティについて、2014 年度においては利用の際の情報セキュリティ上の技術的課題等についてまとめたテキストを総務省「国民のための情報セキュリティサイト」において公表する等必要な周知啓発を実施した。
		b) ・ スマートフォンの利用に当たり課題となる無線 LAN のセキュリティについて、2014 年度においては関連技術やサービス、普及の動向等を踏まえたテキストを総務省「国民のための情報セキュリティサイト」において公表するなど、必要な情報を発信した。
(カ)スマートフォン等におけるフィルタリングの在り方の検討	総務省 経済産業省	・ 2014 年７月に、総務省の ICT サービス安心・安全研究会において「青少年インターネットセッション　議長レポート」が公表され、今後のフィルタリングの推進に必要な取組について取りまとめられた。 ・ また、2015 年２月から「春のあんしんネット・新学期一斉行動」を実施しており、総務省から各携帯電話事業者に対し、店頭でのフィルタリングの説明の徹底等を改めて依頼し、各携帯電話事業者において、必要な取組が進められている。
(キ)スマートフォン時代における利用者情報保護に関する取り組みの推進	総務省	・ 2013 年９月公表の SPI Ⅱを踏まえ、アプリケーションの第三者検証を推進するにあたっての諸課題を検討するタスクフォース（TF）を同年 12 月に設置し、2014 年３月には利用者情報の取扱いの現況及び TF での検討結果を「スマートフォン プライバシー アウトルック」（SPO）としてとりまとめ、同年５月に公表した。同報告書により、アプリマーケットでのプライバシーポリシーの作成・公表状況は 2013 年時に比べて改善傾向にあることが示された。 ・ 2015 年２月以降、第三者検証の技術的課題等について実証実験を開始させており、2015 年度予算案においても、当該実験を継続して実施するための所要の予算を計上している。SPO についても 2014 年度版を年度末にとりまとめ、2015 年度初めに公表する予定である。
(ク)ソーシャルメディアの利用に係る情報セキュリティ確保方策	総務省 経済産業省	・ 総務省「国民のための情報セキュリティサイト」において、ソーシャルメディアの利用上の注意点について周知を行った。 ・ IPA が月に一度発信する「今月の呼びかけ」において、ソーシャルメディアで悪用されている手口や事例に加え、セキュリティ対策を紹介し、広く注意を呼びかけた。

３　「世界を率先する」サイバー空間の構築

① 外交

施策名	関係府省庁	進捗状況
(ア)ハイレベルによる戦略的な取組の強化	内閣官房 外務省 関係府省庁	・ イスラエル、オーストラリア、フランス、EU との首脳会談において、二国間のサイバー協議の立ち上げに合意した。また、ハイレベル会合等においてサイバー空間に関する規範やルール等を議題に意見交換を行い、我が国の価値観の各国への展開に努めた。
(イ)サイバー空間に関する国際規範作りへの参画等	内閣官房 総務省 外務省 経済産業省 関係府省庁	・ 「日米サイバー対話」、「日 EU サイバー対話」、「日中韓サイバー協議」、「日イスラエルサイバー協議」、「日仏サイバー協議」、「日英サイバー協議」、「日エストニアサイバー協議」、「日豪サイバー協議」、「日露サイバー協議」の各二国間協議等及び経済開発協力機構（OECD）のセキュリティガイドライン見直しの協議等の多国間協議への参画を通じ、サイバー空間を利用した行為に対する国際法の適用や国際的なルール・規範作り等に関する我が国の意見表明や情報発信に努め、当該議論に積極的に関与した。
(ウ)「国際安全保障の文脈における情報及び電気通信分野の進展」に関する政府専門家会合への政府専門家の派遣等による安全保障分野での国際議論への参画	内閣官房 外務省 関係府省庁	・ 第４次国連サイバーGGE 会合に政府専門家（外務省サイバー政策担当大使）を派遣し、サイバー空間における国際法の適用や、サイバーセキュリティ分野における行動規範作り、信頼醸成措置の促進、能力構築支援等に積極的に寄与した。
(エ)サイバーセキュリティ政策に関する二国間対話の強化	内閣官房 総務省 外務省 経済産業省 関係府省庁	・ 米国との二国間対話については、「第２回日米サイバー対話」（2014 年４月）、「第６回インターネットエコノミーに関する日米政策協力対話局長級会合」（2014 年９月）等を通じ、両国のサイバーセキュリティ政策や脅威情報の共有をはじめ、重要インフラ防護における協力、意識啓発における連携強化に取り組んだ。 ・ EU との対話については、「第 21 回日 EU･ICT 政策対話」（2015 年３月）、「第１回日 EU サイバー対話」（2014 年 10 月）等を通じ、日 EU 間のサイバーセキュリティ政策に関する情報等の共有が行われた。 ・ 第２回目となる日英サイバー協議（2014 年 12 月開催）に加え、EU、中韓、イスラエル、フランス、エストニア、オーストラリア、ロシアとの間で、新たにサイバー協議を立ち上げるなど、二国間の連携強化や信頼醸成に取り組んだ。
(オ)海外情報セキュリティ機関との情報交換	経済産業省	・ 米国立標準技術研究所（NIST）との定期会合を 2014 年 12 月２日に、NIST にて開催。NIST、産業技術総合研究所、JPCERT/CC、IPA の各機関がそれぞれの活動に関する情報共有を実施。IPA からは早期警戒パートナーシップ、ソフトウェア識別タグに関する取組み、J-CSIP、J-CRAT の活動紹介に加え、これらの将来的な計画について紹介。その他、我が国におけるサイバーセキュリティ基本法の制定についても報告。NIST からは、情報共有に関連する NIST-SP シリーズの「Guide to Cyber Threat Information Sharing」（NIST-SP800-150）のドラフトの状況やサイバーセキュリティフレームワークに関する内容について紹介があった。 ・ 韓国インターネット振興院（KISA）とは 2014 年 11 月 18 日に、IPA においてトップ会合を実施。IPA、KISA 双方より、IoT 及びサイバーセキュリティに関する、自国における取組み、最新動向についての情報交換及び意見交換を実施。
(カ)多国間の枠組み等における国際連携・協力の推進	内閣官房 外務省 関係府省庁	・ OECD、APEC、OECD、IWWN、FIRST、Meridian 等の国際会合への参画を通じ、重要インフラ防護、インシデント対応等に関する取組みやベストプラクティスの共有を推進した。Meridian 会合については、本年度、我が国として主催し、我が国のプレゼンスの向上、国際協調・協力の推進に努めた。
(キ)サイバー空間における米国との協力の深化	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省 関係府省庁	・ 米国との間で、「第２回日米サイバー対話」（2014 年４月）、「第６回インターネットエコノミーに関する日米政策協力対話局長級会合」（2014 年９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を始め、重要インフラ防護における協力、意識啓発における連携強化に取り組んだほか、米国の映画配給会社に対するサイバー攻撃等の事案の発生に際しては、迅速な情報共有を行うなど、日米協力の推進・深化に努めた。

② 国際展開

施策名	関係府省庁	進捗状況
(ア)日・ASEAN 情報セキュリティ政策会議の推進による日 ASEAN 関係の連携強化	内閣官房 総務省 外務省 経済産業省	・ 日本と ASEAN 諸国は、2009 年以降、「情報セキュリティ分野における日・ASEAN の連携枠組み」に基づき、日・ASEAN 情報セキュリティ政策会議を通じ、以下のような連携・協力を推進している。
		a) ・ 2013 年 10 月にフィリピンで開催された第６回日・ASEAN 情報セキュリティ政策会議において合意された共同意識啓発活動及びサイバー連絡演習を ASEAN 各国と連携して着実に実施するとともに、重要インフラ防護の共同での取組として「日・ASEAN における重要インフラ防護に関するガイドライン」を策定した。
		b) ・ 2014 年 10 月に第７回日・ASEAN 情報セキュリティ政策会議を東京において開催し、「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」(2013 年９月）における共同閣僚声明の合意事項についての取組状況の確認、情報共有体制の更なる強化について議論した。また意識啓発活動、日・ASEAN 重要インフラ防護に関するガイドライン策定、サイバー連絡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の連携を強化していくことで合意した。
		c) ・ 2014 年８月、第６回日・ASEAN 政府ネットワークセキュリティワークショップをシンガポールにおいて開催し、共同意識啓発活動、重要インフラ防護、サイバー連絡演習の報告・検討したほか、事業継続計画（IT-BCP）等について議論した。
		d) ・ 第７回日・ASEAN 情報セキュリティ政策会議において、「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、取組状況の確認を行い、日 ASEAN 間の情報共有体制の更なる強化について検討した。また、今後も、意識啓発活動、日・ASEAN 重要インフラ防護に関するガイドライン策定、サイバー連絡演習等を実施するとともに、重要インフラ防護や人材育成の面等での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、ベストプラクティスやガイドラインの策定に向けた検討を重ね、日 ASEAN の共同ガイドライン及びベストプラクティス集を策定した。 ・ サイバー演習 WG で、演習シナリオや各国の政策担当者の役割などにつて検討を重ねた。 ・ 人材育成 WG を立ち上げ、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。
		e) ・ 独立行政法人国際協力機構（JICA）による、インドネシアに対する技術協力プロジェクト「情報セキュリティ能力向上プロジェクト」を 2014 年７月に開始した（協力期間は 2017 年１月までを予定）。
		f) ・ 総務省において、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 情報セキュリティワークショップ（2014 年 10 月、フィリピン）」を主催し、サイバー攻撃対策や人材育成の ASEAN との連携方策の議論を実施した。
		g) ・ ASEAN 各国の研究者が参加するアジア地域の情報セキュリティ研究者の会合「RAISE（2014 年８月、タイ）」を活用し、独立行政法人情報通信研究機構（NICT）が中心となって、情報セキュリティに関する対策技術、標準化動向の共有等を通じ、研究者間の連携強化を推進した。 ・ 経済産業省において、2015 年２月に ASEAN 加盟国のうち８カ国に対する第３回目となる情報セキュリティマネジメントシステム（ISMS）及び制御システムセキュリティに関する研修を実施した。
(イ)日・ASEAN のサイバー犯罪対策協力の促進	警察庁 外務省 法務省	・ 2014 年５月 28 日、シンガポールにおいて、第１回日・ASEAN サイバー犯罪対策対話を開催した。対話では、日本側からサイバー犯罪対策の現状や日・ASEAN 統合基金（JAIF）について紹介したほか、ASEAN 各国からもサイバー犯罪対策の現状と今後の課題が紹介され、特にサイバー犯罪対策のための能力構築支援の必要性について幅広い意見交換を実施した。また、日・ASEAN サイバー犯罪対策対話を定例開催することで一致した。加えて、サイバー犯罪分野能力構築支援について、国連アジア極東犯罪防止研修所で実施したサイバー犯罪対策及びデジタルフォレンジックに関する国際研修を紹介した。
(ウ)国際連携を活用した国内外における普及・啓発活動の実施	内閣官房 関係府省庁	・ 再掲：１-④-(キ)

(エ)APEC における情報セキュリティ分野の連携推進	総務省 経済産業省	a) ・ 2014 年 10 月にオーストラリアで開催された「APEC 電気通信・情報作業部会」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、我が国からプライバシー及びスパムメール対策等を観点としたネットワークセキュリティ分野の意識啓発を目的としたワークショップの開催を提案。2015 年５月の同作業部会を次回会合期間中に開催することが合意された。
		b) ・ JPCERT/CC を通じ、2014 年５月と 11 月にアフリカ諸国に対し、それぞれジブチとモーリシャスにて、FIRST と連携しながら CSIRT 構築・運用強化のための研修を行った。2014 年５月にはタイの ThaiCERT に、同９月にはモンゴルの MNCERT/CC、2015 年３月にはミャンマーの mmCERT/CC の技術者に対して CSIRT 構築・運用強化支援のための現地研修を行った。
(オ)海外の組織内 CSIRT の構築・運用支援	経済産業省	・ JPCERT/CC において、５月にはタイの ThaiCERT に、９月にはモンゴルの MNCERT/CC 等に、３月にはミャンマーの mmCERT/CC 等の技術者に対して CSIRT 構築・運用強化支援のための現地研修を行った。 ・ JPCERT/CC において、５月にラオスの LaoCERT に、９月と 10 月にスリランカの Sri Lanka CERT|CC 及び TechCERT に対して TSUBAME 分析ノウハウの共有や教育などのトレーニングを実施し、分析者の増加と技術向上に取り組んだ。 ・ JPCERT/CC において、インドの CERT-In をカウンターパートとし、９月にデリー及びバンガロールで Android のセキュアコーディングセミナーを開催した。 ・ JPCERT/CC において、タイの ThaiCERT が 10 月に主催したバンコクでの現地の大学生を対象としたマルウェア解析競技会における講義を行った。
(カ)各国における対外・対内調整を担う CSIRT の体制強化の支援及び連携の強化	経済産業省	a) ・ JPCERT/CC において、海外 National-CSIRT の構築・運用支援の効率化及び支援成果の持続のためのツールをミャンマーの mmCERT/CC に提供した。また、メールによる標的型攻撃に対する演習用ツールセット（IT セキュリティ予防接種ツールセット）の英語版を、ルーマニアの CERT-Ro に実施ノウハウとともに提供した。
		b) ・ ＜FIRST＞ JPCERT/CC の職員が FIRST の Board of Directors のメンバーとなり、FIRST 加盟チーム間の連携を一層強化する基盤づくりに寄与した。また 2014 年６月にボストンで開催された FIRST 会合に参加し、各国のインシデント対応状況の情報共有を通じて、参加した CSIRT 間の連携を進めた。 ・ ＜IWWN＞ JPCERT/CC において、内閣官房と連携のうえ、IWWN 年次会合を 2014 年５月に東京にて開催した。また、内閣官房及び JPCERT/CC において、定期的に開催される IWWN の電話会議やメーリングリストを通して情報共有を行うとともに、ワーキンググループの活動にも積極的に参画し、メンバー国間の連携を進めた。 ・ ＜APCERT＞ JPCERT/CC は APCERT の議長チーム、事務局を務め、メーリングリスト、ワークショップの開催、年次会合を通じて、各種情報（ボット感染 IP 情報、マルウェア分析結果、ソフトウェアの脆弱性関連情報、攻撃動向及び対応手法等）の情報共有を行い、APCERT 加盟チーム間の連携を先導的に進める等 APCERT 加盟チーム間の連携を一層強化する基盤づくりに寄与している。 ・ ＜演習＞ JPCERT/CC は 2014 年９月に実施された ASEAN の CSIRT を中心とする「ASEAN サイバーセキュリティ演習」及び 2015 年３月に実施された APCERT のメンバーを中心とする「APCERT Drill 2015」に参加し、インシデント対応能力の向上を図った。「APCERT Drill 2015」については運営側の立場でも関与し、アジア太平洋地域の CSIRT のインシデント対応能力の向上に寄与した。
(キ)ASEAN のビジネス環境整備（ISMS 等）	経済産業省	・ IPA のウェブサイトにて「情報セキュリティ対策ベンチマーク」の英語版診断システムをバージョン 4.3 にアップデートするとともに、関連する英語ドキュメント類のアップデート版公開により最新版を提供し、ASEAN 各国における情報セキュリティ対策の普及に寄与した。
(ク)サイバー攻撃事前防止・早期対策に向けた取組の推進	総務省	a) ・ 再掲：1-④-(ナ)、２-②-(チ)
		b) ・ 再掲：1-④-(ナ)、２-②-(チ)
		c) ・ 再掲：1-④-(ナ)、２-②-(チ)
		d) ・ 再掲：1-④-(ナ)、２-②-(チ)

(ケ)アジア太平洋地域等での早期警戒情報の共有促進	経済産業省	a) ・ TSUBAME プロジェクトメンバー間で観測したデータの詳細分析を行い、攻撃に使用された可能性のあるシステムやマルウェアの特定、およびインシデント通知を行った。プロジェクトメンバーには分析ノウハウの共有や教育などのトレーニングを実施し、分析者の増加と技術向上にも取り組んだ。また、アジア太平洋地域以外への観測点の拡大に向けて、プロジェクト規約の見直しを進めた。
		b) ・ 健全なサイバー空間を実現することを目的とするイニシアティブ（サイバーグリーン）とその実現のための調査・実証運用プロジェクトを実施した。 ・ インターネット全体の健全性とリスクを各国／地域間で比較可能にする指標を設定し、その指標を用いて、各国の CSIRT、ISP やセキュリティベンダーなどの技術パートナーと連携し、より効率的に健全なサイバー空間を実現することを目的とするイニシアティブを「サイバーグリーン」と名付け、そのコンセプトの有効性を検証する活動を進めた。2014 年度はサイバーグリーンを実現するための調査および実証運用（「サイバーグリーンプロジェクト」）として、指標作成エンジンの開発や、環境改善の取り組みを行うポータルサイトの準備を行った。また、コミュニティメンバ（リスク環境データを提供するデータプロバイダーやセキュリティベンダー、海外 CSIRT）と連携し、小規模な試験運用を実施し、コンセプトの実証実験を行った。
(コ)途上国向け研修・セミナー等の開催	総務省	・ APT（アジア・太平洋電気通信共同体）加盟国を対象とした研修「ブロードバンド通信のための情報セキュリティ構築」（2014 年 12 月）及び同「デジタルデバイドを解消するための ICT サービスと e-アプリケーションの活用」（2015 年３月）において、情報セキュリティに関する講義を実施することにより、情報共有を進めるとともに連携を強化した。 ・ 第５回 APT サイバーセキュリティフォーラム（2014 年５月、モンゴル）に参加し、我が国のサイバーセキュリティ政策及び取り組みについて説明を行った。
(サ)途上国に対する技術援助の推進（サイバー犯罪対策のための刑事司法制度整備）	警察庁 法務省 外務省	・ 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、2014 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。 ・ 国連アジア極東犯罪防止研修所の実施した汚職防止刑事司法支援研修及び仏語圏アフリカ刑事司法研修において、開発途上国から参加した刑事司法実務家（警察官、検察官及び裁判官等）に対し、日本におけるサイバー関連犯罪やデジタル・フォレンジックによる解析技術の現状に詳しい専門家による講義を実施した上で、各国におけるサイバー犯罪及びこれに対する捜査の現状について意見交換を行った（2014 年 10 月、2015 年２月）。
(シ)ソフトウェア開発のアウトソーシング先国等におけるセキュアコーディングセミナーの実施	経済産業省	・ Android セキュアコーディングセミナーを 2014 年９月にインド（デリー及びバンガロール）にて計約 45 名を対象として開催した。
(ス)情報セキュリティ分野での国際標準化への参画	総務省 経済産業省	a) ・ ITU-T SG17 第４回会合（2014 年９月）を通じて、サイバー脅威情報をやり取りする際に用いるプロトコルを定める X.1582 など、日本が開発した技術について国際標準化を積極的に推進した。
		b) ・ ISO/IEC JTC1/SC27/WG2（暗号）のコンビーナ（国際主査）として、国際の議論を牽引。日本技術の提案も支援。また、暗号モジュール関連の ISO/IEC CD18367、ISO/IEC DIS17825、ISO/IEC19790 欠陥レポートの作成を行った。
(セ)脆弱性対策に関する国際標準化活動等への参画	経済産業省	・ 米 DHS 主催の Software and Supply Chain Assurance Working Group 会議への参画や米 NIST、米 MITRE との打合せを通して SCAP、ソフトウェア識別タグの利活用についてすり合わせを実施。 ・ 電話会議及び FIRST 会合にて CVSS V3 の仕様検討 WG に参加。2014 年 12 月、CVSS ワーキンググループから CVSS V3 プレビュー第２版をリリース。また、CVSS V2 計算ソフトウェア多国語版については、計 11 言語に対応。次期バージョンである CVSS V3 計算ソフトウェア多国語版については、英語、日本語のサポートを完了。 ・ FIRST に設置した「脆弱性情報のグローバルな取り扱い」を検討するためのグループ（VRDX-SIG: Vulnerability Reporting and Data eXchange SIG）に参画。FIRST 会合にて第２回会合を主催し、脆弱性データベースのカタログ化の検討を実施。 ・ ISO/IEC JTC1 SC7 の活動に参加し、ソフトウェア識別タグの技術仕様規格（ISO19770-2）の DIS 化が完了（2014 年 10 月）。 ・ SCAP の国内への普及セミナーを実施（２回）。 ・ インシデント対応の自動化の技術仕様として、STIX の概説を公開（2015 年１月）。

(ソ)Common Criteria (ISO/IEC 15408)における国際協調	経済産業省	・ CCRA で開発中の USB やネットワークデバイス等の国際的な政府調達セキュリティ要件の策定に参加。 ・ 2014 年９月に開催された CCRA 会議及び CC の国際コンファレンス（ICCC）に参加、日本の状況の発表と各国の認証制度・評価技術の情報を入手し、これらの情報をセミナーを通じ国内のベンダー等に提供した。
(タ)ハードウェア CC 評価・認証制度における欧州との協調関係の構築	経済産業省	・ JHAS 会合に６回、JTEMS 会合に３回参加し、最新動向情報を収集すると共に日本からの情報発信も行った。また JIWG と 2014 年９月及び 2015 年２月に打ち合わせを行い情報交換を実施した。
(チ)制御システムセキュリティに関する国際支援	経済産業省	・ CSSC において、ENCS（The European Network for Cyber Security：欧州の制御システムセキュリティを取り組んでいる研究機関等）と LOI（Letter of Intent、検討することを同意した覚書）を締結した。また、英国研究者と研究情報交換を行い、制御システムセキュリティに係る協力関係を構築した。ASEAN の制御システムセキュリティ関係者に対して研修を実施。ISCI との会合や IEC CAB での議論に参加し、制御機器におけるセキュリティ認証基準の国際標準化に係る事項を積極的に提案した。
(ツ)制御システムのセキュリティに係る米国との連携推進	経済産業省	・ 米国国土安全保障省と経済産業省、関係組織（CSSC、IPA、JPCERT/CC、AIST）との間で、制御システム関連研究開発等の情報の共有を行った。また、米国の制御システムセキュリティ認証制度団体である ISCI と SSA 認証における認証のコスト分散及び認証期間短縮等、効果的な認証実施手順に関する検討を行った。
(テ)国際的なルールに基づくセキュリティ製品の貿易の推進	経済産業省	・ 再掲：２-①-(ケ)
(ト)個人情報の保護に関する国際的な取組への対応	消費者庁	・ APEC/ECSG/DPS（Asia-Pacific Economic Cooperation/Electronic Commerce Steering Group/Data Privacy Sub-Group、2014 年８月及び 2015 年１～２月）、OECD/ICCP/WPSPDE（Organisation for Economic Co-operation and Development/Committee for Information, Computer and Communications Policy/Working Party on Security and Privacy in the Digital Economy、2014 年６月及び 12 月）等の国際的な会合への出席等を通じ、国際的な取組を把握するとともに、我が国の個人情報保護法制についての説明等を行うことにより、国際的な理解を求めた。 ・ 関係省庁連絡会議幹事会を活用し、越境プライバシールールシステム（ＣＢＰＲ）におけるアカウンタビリティ・エージェント（認証機関）の審査基準について確認するなど、各省庁と連携しつつ、CBPR の運用開始に向けて必要な対応を行った。

③ 国際連携

施策名	関係府省庁	進捗状況
(ア)サイバー攻撃に関する諸外国関係機関との連携の強化	警察庁 法務省	・ 諸外国関係機関との情報交換を行うなど、サイバー攻撃の主体・方法等に関する情報収集・分析を継続的に実施している。 ・ FIRST 会合に参加し、情報交換等国際的な連携を通じて、諸外国関係機関との連携強化を推進した。
(イ)サイバー犯罪の取締りのための国際連携の推進	警察庁	・ 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（2014 年 11 月、2015 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（2014 年５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、アジア大洋州地域サイバー犯罪捜査技術会議を開催（2014 年 12 月）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（2015 年２月末現在、67 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。
(ウ)中央当局制度を活用した国際捜査共助の迅速化	警察庁 法務省	・ 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。
(エ)サイバー犯罪条約普及への参画	外務省	・ 多国間協議、二国間協議の場等を活用し、各国に対し、同条約への加盟を懇懇。 ・ 新たに 2014 年９月にトルコ、同 10 月にルクセンブルク、2015 年２月にポーランドが、それぞれ同条約を締結した。また、欧州評議会を通じて、６月に行われたサイバー犯罪条約の関連会議に財政支援を行うとともに専門家を派遣した。
(オ)国際会議等への参加を通じた連携の強化	内閣官房 警察庁 総務省 経済産業省 関係府省庁	・ 諸外国との情報共有、ベストプラクティスの共有を図るため、IWWN、FIRST、Meridian 等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。
(カ)諸外国との CSIRT 間連携の強化	経済産業省	・ 2014 年度、JPCERT/CC は既存の MOU/NDA の更新手続きを進め、2015 年３月末現在で 23 の経済地域における 27 組織との間の MOU が効力を発揮している。2011 年に JPCERT/CC 及び中韓の National CSIRT 間で締結した MOU にもとづき、８月に三者による第２回年次会合をソウルで開催し、迅速かつ効果的なインシデントへの対処を確認した。
(キ)国際的な窓口機能の強化を通じた各国との連携	内閣官房	a) ・ 2014 年 11 月に制定された「サイバーセキュリティ基本法」について国内外で積極的に概要説明を行ったことをはじめ、NISC ホームページで「情報セキュリティ国際キャンペーン」の取組や英語翻訳資料を公開するなど、国際的な広報、情報発信を行った。 ・ 我が国の重要インフラ防護分野や地域協力等におけるベストプラクティスについて、日・ASEAN 情報セキュリティ政策会議や、Meridian 会合において情報共有し、諸外国との連携の強化に努めた。
		b) ・ 国際会議への参加や関係機関との協議を通じて把握した国際動向や脅威情報等について、関係省庁との間で情報の共有化を図るなど、関係機関との連携に努めた。

４　推進体制等

施策名	関係府省庁	進捗状況
(ア)NISC の機能強化	内閣官房	・ 2014 年 11 月に成立したサイバーセキュリティ基本法を受け、情報セキュリティ政策会議において「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（2014 年 11 月 26 日決定）を策定した。また、内閣官房において内閣官房組織令を改正し、2015 年１月に「内閣サイバーセキュリティセンター」へ改組した。
(イ)関係機関等との連携強化	内閣官房 内閣府	・ 内閣官房及び内閣府において、IT 総合戦略本部の他、総合科学技術・イノベーション会議、中央防災会議、知的財産戦略本部等、関係する本部・会議において互いに会合への出席、必要な情報交換等を行い、政府全体としてサイバーセキュリティ政策の一体的推進に努めた。
(ウ)情報セキュリティ対策に資する各種ツール・分析等の提供	経済産業省	・ IPA において、2014 年７月 15 日に情報セキュリティ白書 2014 を出版した。また、８月には電子書籍版も発行している。さらに、英訳版を作成することで海外への日本のセキュリティの状況について発信している。
(エ)官民の情報共有の更なる推進	内閣官房 関係府省庁	・ 内閣官房において、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）と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新たに締結するとともに、独立行政法人情報処理推進機構（IPA）と脆弱性対応、民間事業者や独立行政法人等との情報共有、政府機関のシステム調達等に関するセキュリティ認証、国民・企業等に対する普及啓発等の幅広い分野でのパートナーシップを新たに締結した。
(オ)サイバー攻撃に関するインシデント情報等の政府機関や重要インフラ事業者等の関係機関間における共有の促進	内閣官房	・ 内閣官房において、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）と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新たに締結するとともに、パートナーシップに基づく情報管理協定を締結した。また、IPA とも脆弱性対応や標的型攻撃等に関する情報共有、政府機関等のシステム調達等に関するセキュリティ認証、国民・企業等に対する普及啓発に関する分野等において包括的なパートナーシップを新たに締結した。

別添３　政府機関等における情報セキュリティ対策に関する取組等

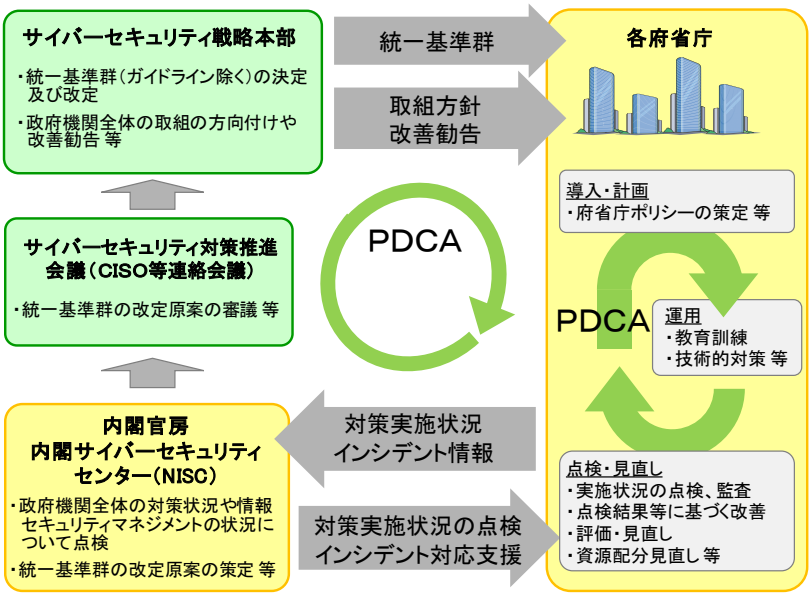
＜別添３－目次＞

別添３－１　政府統一基準群による対策の推進

１　概要

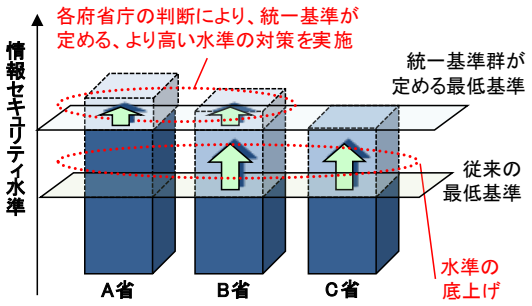
政府機関における情報セキュリティ対策は、情報セキュリティ政策会議（現サイバーセキュリティ戦略本部）等の定める「政府機関の情報セキュリティ対策のための統一基準群（以下「政府統一基準群」という。）」と、それに準拠した各府省庁の情報セキュリティポリシー（以下「府省庁ポリシー」という。）に基づき実施されている。また、政府統一基準群及び府省庁ポリシーの改定を含む対策の見直しについては、①各府省庁におけるPDCAサイクル、②政府機関全体としてのPDCAサイクルの二つのメカニズムで推進されている（図表１）。

図表１　政府機関における情報セキュリティ対策



政府統一基準群は、政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策や、その水準をさらに高めるための対策の基準等を定めたものであり、2005年12月13日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て毎年改定を行ってきた。これまで、各府省庁でばらつきのあった情報セキュリティ対策水準の底上げへの貢献など、一定の効果が得られてはいるが（図表２）、毎年の改定による基準の複雑化・肥大化・形骸化や、脅威の高度化・多様化及び技術進展等の環境変化への対応といった改善すべき点も明らかになってきた。

図表２　政府統一基準群の効果（イメージ）

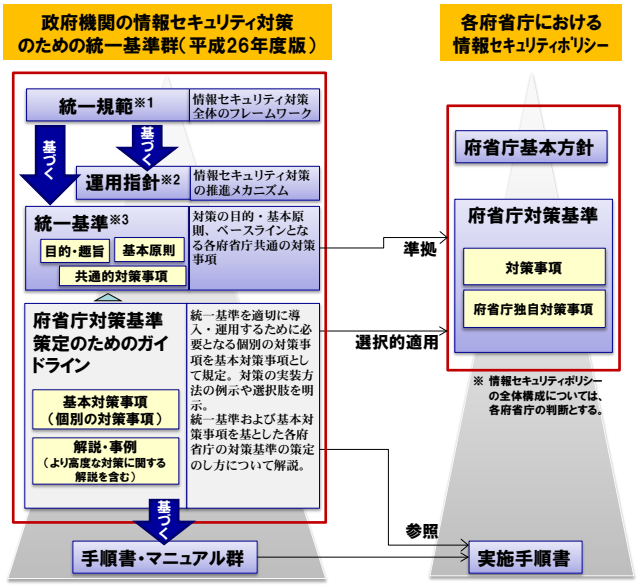


このような状況を踏まえ、2013年度より政府統一基準群の実効性の向上及びサプライチェーン・リスクやクラウドコンピューティング等の新たな脅威・技術への対応の二つの観点から、文書体系の変更も含めた抜本的な見直しをすすめ、第39回情報セキュリティ政策会議（現サイバーセキュリティ戦略本部）（2014年５月19日）において、政府統一基準群（平成26年度版）を決定した。

２　府省庁ポリシーの策定支援

今般決定した政府統一基準群（平成26年度版）は、府省庁が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て対策基準を策定できるよう、各府省庁が必ず実施すべき対策事項を遵守事項として目的ごとに簡潔に明記するとともに、ガイドラインにおいて、府省庁ポリシーの策定手順や政府統一基準の遵守事項を満たすために採られるべき基本的な対策事項の例示、考え方等を解説している（図表３）。

図表３　政府統一基準群と府省庁ポリシーの関係



※１　統一規範：政府機関の情報セキュリティ対策のための統一規範
※２　運用指針：政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針
※３　統一基準：政府機関の情報セキュリティ対策のための統一基準

政府統一基準群（平成26年度版）の改定内容を踏まえて、各府省庁はそれぞれの府省庁ポリシーの見直しを行い、2015年度の早い時期から新ポリシーに基づいた運用を開始できるよう、準備を進めた。NISCは、各府省庁が新たな政府統一基準群に準拠した府省庁対策基準等の情報セキュリティ関係規程が適切に定められるよう、外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書、スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書[1]といったマニュアルの整備やひな形の提供等の支援を行った。

[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（平成 26 年度版）」について」
http://www.nisc.go.jp/active/general/kijun26.html

別添３－２　サイバーセキュリティ基本法に基づく監査

2015年１月に完全施行されたサイバーセキュリティ基本法において、サイバーセキュリティに関する対策基準に基づく施策の評価（監査）が本部事務とされた。これを受け、各府省庁における自己点検や監査等の取組に加え、サイバーセキュリティ戦略本部が各府省庁に対して第三者的な視点から監査を実施し、改善策の助言を行う方針の下、監査制度の確立に取り組んでいる（図表１）。

具体的には、政府統一基準群等に基づく各府省庁の施策の取組状況について、組織全体としてのPDCAサイクルが有効に機能しているかとの観点から検証するマネジメント監査と、インターネットに接続されている情報システムの対策状況について、擬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検証を行うペネトレーションテストの二本立てで監査を行う。こうした取組を通じて、他の政府機関においても参考とすべきような良い事例を見出していくとともに、サイバーセキュリティ対策の継続的な強化や、発見されたシステムの脆弱性について、改善のための助言をしていく（図表１）。

図表１　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[2]

１ 監査の目的

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、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サイクルが継続的かつ有効に機能するよう助言し、対策の効果的な強化を図る。

２ 監査の対象

国の行政機関　※独立行政法人については、当面、特に必要があると認める場合に監査の対象とする。

３ 監査の基本的な方向性

(1) 助言型監査
- 有益な助言を行う。
- グッドプラクティスを共有。

(2) 第三者的視点からの監査
- 内部監査とは独立した監査を実施。

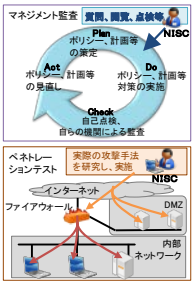
(3) 各機関の状況を踏まえた監査
- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定
- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

４ 監査の実施内容

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

(2) ペネトレーションテスト
- 疑似的な攻撃を実施することによって、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。



５ 監査の進め方　※監査事務については、内閣サイバーセキュリティセンターが実施する。

(1) 監査方針の策定
- 年度ごとの監査の基本的な考え方を含む年度監査方針を、年次計画の一部として策定。

(2) 監査の実施
- 必要に応じて外部専門家が協力。
- 過年度の監査実施結果のうち重要な事項については、改善状況を継続的にフォローアップ。

(3) 個別の監査実施結果の通知
- 監査実施結果を、各機関の最高情報セキュリティ責任者（CISO）へ通知。
- 各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は計画を報告。

(4) 監査実施結果の取りまとめ・報告
- サイバーセキュリティの特性を踏まえ、攻撃者を利することのないよう配慮しつつ、当該年度に実施した監査の結果を取りまとめ。
- サイバーセキュリティ戦略本部に報告。

今後、マネジメント監査については2015年度から試行等を通した制度設計を行い、2016年度から本格実施する予定である。またペネトレーションテストについては準備が整い次第、2015年度から調査対象府省庁について速やかに実施する予定である。

[2] サイバーセキュリティ戦略本部第二回会合（2015 年５月 25 日）資料を基に作成

別添３－３　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（平成26年度版）」（以下「政府統一基準」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」として規定化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、調達や運用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べく、クラウドサービスに係る関係者・有識者による研究会を実施した。

別添３－４　高度サイバー攻撃への対処

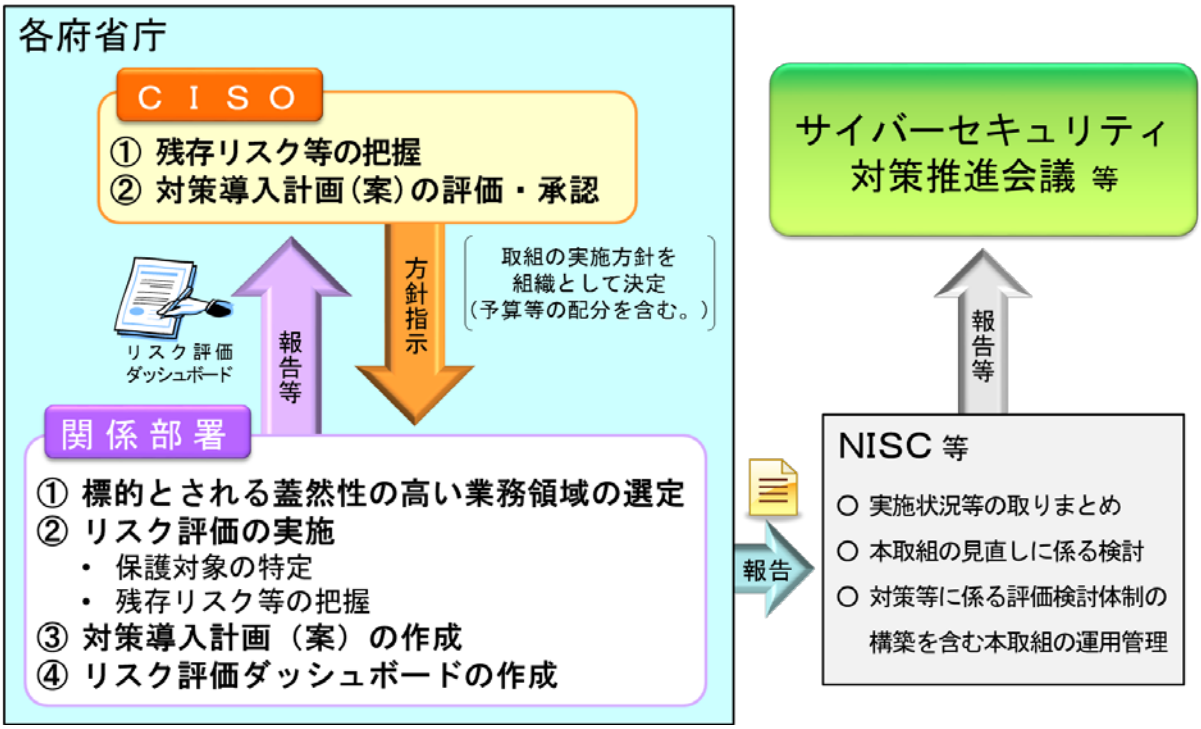
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

高度サイバー攻撃のうち、昨今、特に大きな脅威となっている標的型攻撃の主目的は、情報システム内の端末を不正プログラムに感染させることではなく、情報システム内部に侵入基盤を構築し、さら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、「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、全府省庁において2014年度より正式な運用を開始した（図表１、図表２）。

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



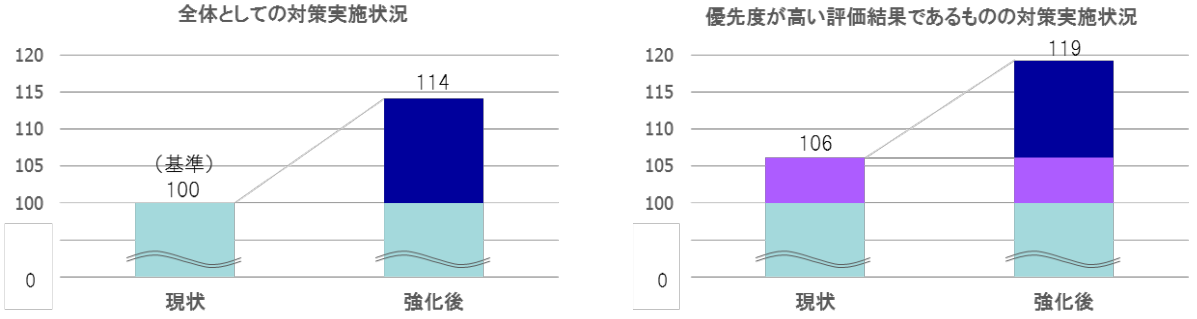
図表２　検討会の構成員一覧

委員長	佐々木　良一	東京電機大学教授／内閣官房情報セキュリティ補佐官
委　員	有村　浩一	一般社団法人 JPCERT　コーディネーションセンター 常務理事
	上原　哲太郎	立命館大学　情報理工学部　情報システム学科教授
	岡谷　貢	独立行政法人情報処理推進機構　セキュリティセンター 情報セキュリティ技術ラボラトリー　研究員
	佳山　こうせつ	富士通株式会社　クラウドビジネスサポート本部 クラウド CERT 室　アシスタントマネージャー
	齋藤　衛	株式会社インターネットイニシアティブ サービスオペレーション本部　セキュリティ情報統括室長
	高倉　弘喜	名古屋大学情報基盤センター教授
	谷川　哲司	日本電気株式会社　経営システム本部 （セキュリティ技術センター）シニアエキスパート
	松尾　真一郎	独立行政法人情報通信研究機構　ネットワークセキュリティ 研究所　セキュリティアーキテクチャ室長
	松川　博英	トレンドマイクロ株式会社 フォワードルッキングスレットリサーチシニアリサーチャー
	満塩　尚史	経済産業省　CIO 補佐官／最高情報セキュリティアドバイザー
	本川　祐治	株式会社日立システムズ　ICT 基盤事業グループ ネットワークサービス事業部　主管技師長
事務局	NISC	

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。

さらに、対象システムにおける現状点検時点と計画に基づく強化後の対策実施状況としては、現状の全体平均を基準として100と置くと、強化後は114に向上する見込みであり、また、対象システムの中でも防御の優先度が高い評価結果であるものについては、同様に、現状が106、強化後が119となっており、いずれも全体と比較して高い水準となった（図表３）。

図表３　2015 年度における本取組の政府機関全体としての状況



別添３－５　教育・訓練に係る取組

１　各府省庁CSIRT要員に対する訓練

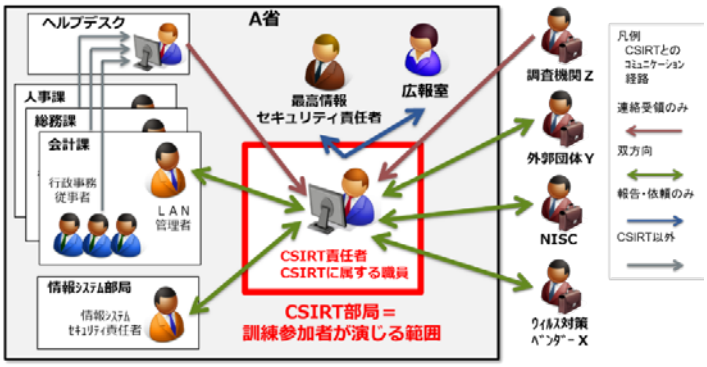
(1) 訓練の目的

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場合、初動対処、被害拡大防止、早期復旧等に取り組むに当たり、府省庁関係者への報告やNISCへの連絡等を円滑に実施する必要がある。本訓練は、各府省庁のCSIRT要員に対し、情報セキュリティインシデント発生を想定した対処訓練等を実施することで、情報セキュリティインシデントへの対処能力の向上を図ることを目的としたものである。

(2) 訓練の概要

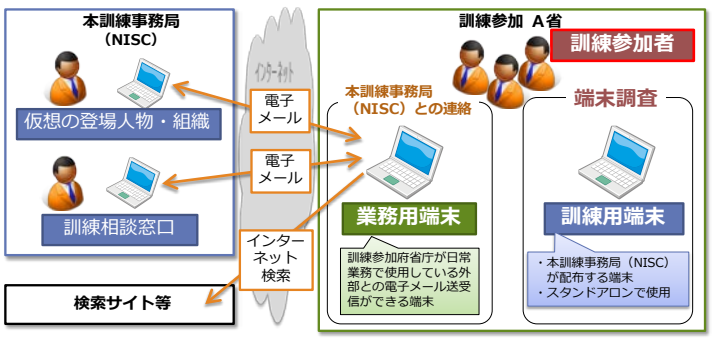
訓練参加者は、仮想の政府機関Ａ省CSIRT部局の職員として、時間差で発生する標的型攻撃を模した複数の情報セキュリティインシデントに対し、府省庁関係者への報告・指示、NISCへの連絡、端末の簡易解析等を行った。図表１に本訓練で登場する仮想の政府機関Ａ省CSIRT部局等を示す。

図表１　本訓練で登場する仮想の政府機関Ａ省 CSIRT 部局等



具体的に、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、CSIRT部局以外の登場人物を演じる事務局（NISC）と連絡を行い、本訓練を進行した。その他、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端末で調査等を実施した。図表２に本訓練の物理的環境を示す。

図表２　本訓練の物理的環境



(3) 参加人数

約50人（全21府省庁参加）

(4) 訓練時期

2015年１月～２月

(5) まとめ

訓練参加者のアンケートでは、訓練全体の感想として、「情報セキュリティインシデントを認知した際の関係者との連携の重要性が再認識できた」、「実践的な内容で非常に良い訓練だった」、「CSIRT要員の対応能力が向上したと思う」などの肯定的な感想が６割以上あったほか、訓練結果を受けて、基本的な対処方法や役割分担等に課題を把握し、情報セキュリティインシデントの対処手順の改善を検討する府省庁が一部あったことから、一定の成果が得られたと考えられる。

今後は、前年度の研修と本訓練を通じて明らかとなった課題等を踏まえ、CSIRT要員の情報セキュリティインシデントへの対処能力の向上のため、情報セキュリティインシデントに関する情報交換やディスカッション、訓練等の取組を充実化する。

２　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等からの専門的知見の提供により、情報セキュリティ関係職員の知見を向上し、政府機関等における対策の参考とする。

(2) 対象

各府省庁及びサイバー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）オブザーバー機関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	2014年 ６月	政府機関に今後求められうる情報セキュリティ対策について ・バイオメトリクスの安全性と個人認証の信頼性確保 ・Man-in-the-Browserの脅威と根本的な解決策 ・行政機関におけるスマホアプリ開発の注意点	独立行政法人・産業技術総合研究所研究員	約110人 （計１回開催）
2	2014年 ７月	政府機関統一基準について	NISC職員	約130人 （計１回開催）
3	2014年 10月	情報システムに係るサプライチェーン・リスクの事例と問題点	株式会社サイバーディフェンス研究所社員	約160人 （計１回開催）
4	2014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	NISC指導専門官等	約110人 （計１回開催）
5	2015年 ２月	最近のサイバー攻撃の現状と対策について（サイバーセキュリティ月間） ・サイバー攻撃の現状と対策 ・効果的な情報セキュリティの職員教育とは ・「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」の紹介	NISC職員 株式会社ラック社員 独立行政法人・情報処理推進機構研究員	約240人 （計２回開催）

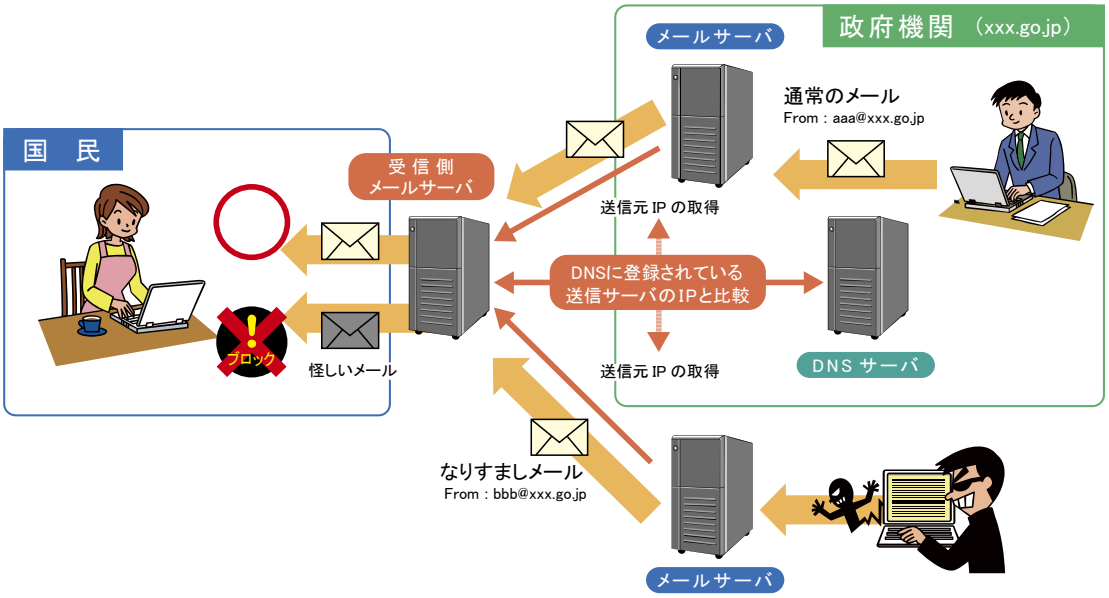
別添３－６　なりすまし防止策の実施状況

１　取組の概要

政府機関になりすました電子メールを一般国民や民間企業等に送信し、電子メールに添付したファイルを実行させて不正プログラムに感染させることで、重要な情報を窃取するなどの攻撃が発生している。なりすましの手段として、悪意ある第三者が、電子メールアドレスのドメイン（@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きた。2014年度は、「サイバーセキュリティ2014」及び「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[3]に設定して公開する。受信側では、電子メールの受信時に、SPFレコードに公開されたIPアドレスと実際に送信元となっている電子メールサーバのIPアドレスが一致するかどうかを確認する。このような手順により、受信者が受け取った電子メールについて、送信者情報が詐称されているかどうかの確認が可能となる。

[3] SPF において、そのドメイン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

2014年及び2015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
2014 年１月末	81.1%	11.8%	7.1%
2015 年１月末	80.8%	11.7%	7.5%

※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年前とほとんど変化が無かったが、新規に取得した政府機関のドメインのうち、４割以上がSPFを設定していない状況が見られるため、ドメインを新規に取得する際に適切な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、前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、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３－７　公開ウェブサーバの脆弱性検査結果の概要

１　検査の目的

NISCが実施する本検査の目的は、サンプルとして抽出した府省庁の公開ウェブサーバを対象に脆弱性検査を行い、脆弱性が見つかった場合には改善を指導するとともに、その結果のうち、必要な事項を各府省庁で共有することで、政府機関の公開ウェブサーバにおける情報セキュリティ対策の向上を図ることである。

２　検査概要

本検査は、検査対象の公開ウェブサーバに対してインターネットからの擬似的な攻撃による検査手法を用いることで、公開ウェブサーバの脆弱性の有無を確認し、インターネットからの攻撃に対する安全性を客観的に検査した。

(1) 検査期間

2014年９月から2015年２月まで

(2) 検査対象

サンプルとして抽出した政府機関の公開ウェブサーバ[4]（約300画面）

(3) 検査方法

検査対象の公開ウェブサーバにインターネットからアクセスし、検査ツール及び手動により既知の脆弱性の有無及び既知の攻撃手法に対する対策状況を確認した。

(4) 検査内容

ウェブサーバ及びウェブアプリケーションの動的な画面に対して、情報セキュリティ上の問題がないかを検査した。

３　検査結果の概要

検査の結果、危険性の高い脆弱性としてSQLインジェクション脆弱性やクロスサイトスクリプティング脆弱性等が検出されたが、既に対応を終えている。

[4] 各府省庁が独自に実施している脆弱性検査の検査対象は含まれない。

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」[5]に基づき、移行が進められた。

政府機関の暗号アルゴリズムに係る移行指針の改定概要

1　経緯

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

（H20年4月22日　情報セキュリティ政策会議決定）

2　政府機関における移行に向けた準備スケジュール

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

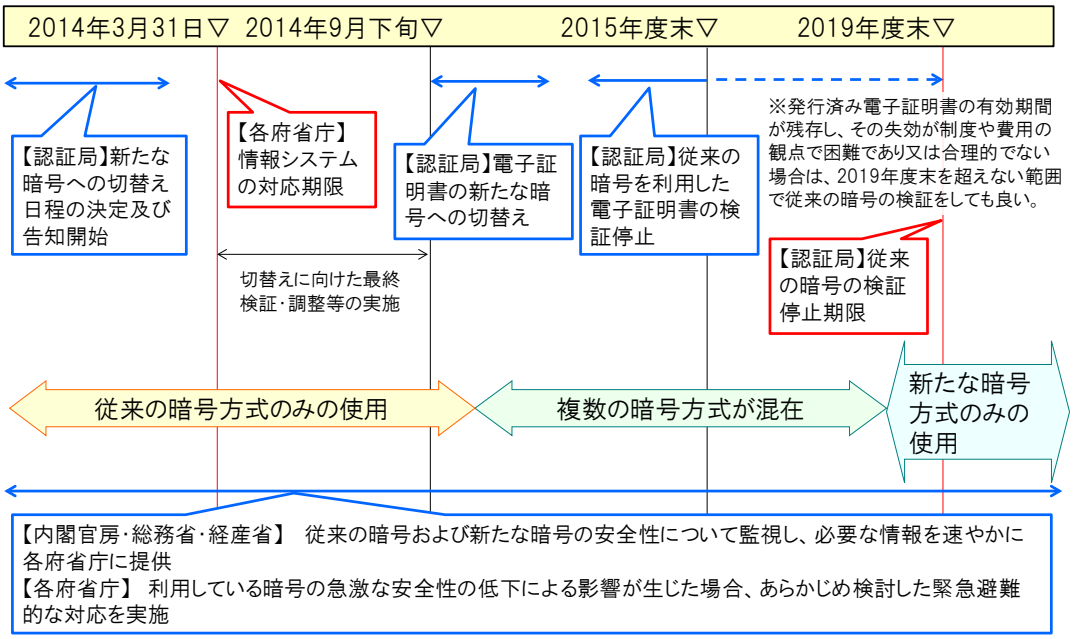
（H21年2月3日　情報セキュリティ政策会議決定）

3　移行指針の改定概要

- 切替時期について各認証基盤との調整結果を踏まえ、以下のとおり改定

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

（参考）政府機関における暗号移行スケジュール



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

（参考１）「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」（平成24年10月26日改定）

平成 20 年 4 月 22 日
情報セキュリティ政策会議決定
平成 24 年 10 月 26 日改定
情報セキュリティ対策推進会議決定

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

１　はじめに

近年、政府機関の情報システムにおいて使用されている一部の暗号アルゴリズム（ハッシュ関数[1]SHA-1 [2]（以下「SHA-1」という。）及び公開鍵暗号方式[3]RSA 1024 [4]（以下「RSA1024」という。））の安全性低下が指摘されている。一般的に、暗号アルゴリズムは、電子計算機の能力の向上などにより、安全性が時間の経過とともに低下するものであるが、暗号技術検討会[5]などにおいては、それら暗号アルゴリズムの安全性の低下により、近い将来に現実的な問題が生じる可能性について指摘しているところである。

SHA-1 及び RSA1024 は、電子申請、電子入札等を行うための政府機関の情報システムにおいて、その安全性及び信頼性を確保するための技術の一要素として広く使用されている暗号アルゴリズムである。政府機関の情報システムの安全性及び信頼性を確保するためには、これらの暗号アルゴリズムについて、情報システムのライフサイクル等を踏まえつつ、適時により安全なものに移行する必要がある。その際、関係する情報システム間における相互運用性を確保する観点や政府機関全体の情報セキュリティ向上の観点から、政府統一的な対応が必要である。

そこで、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 について、より安全な暗号アルゴリズムに移行するための指針を、以下のとおりとりまとめることとした。

２　対象機関

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁、復興庁、総務省、法務省、外務省、

---

[1] 与えられたデータから固定ビット長の値を生成する関数。本指針では、一方向性（当該関数の演算の非可逆性）及び衝突困難性（同一の数列を生成する異なるデータの発見困難性）の両性質を持つものとする。
[2] ハッシュ関数 SHA の一つ。与えられたデータから 160 ビットの値を生成する。
[3] 関連した２つの鍵（公開鍵と秘密鍵）を使用する暗号方式であり、一方の鍵（公開鍵又は秘密鍵）で暗号化したデータは他方の鍵（秘密鍵又は公開鍵）でのみ復号できるようになっている。２つの鍵は、公開鍵が与えられても、秘密鍵を導き出すことが計算上困難な特性を持っている。
[4] 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 1024 ビットとしたもの。
[5] 総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長の私的研究会として毎年度開催。

財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省とする。

３　内容

(1)　情報システムの設計要件

情報システムにおける暗号アルゴリズムの用途を踏まえつつ、それぞれの情報システムにおいて、以下のように設計を行う。

ア　政府認証基盤（GPKI）[6]及び電子認証登記所（商業登記認証局）[7]

(ｱ)　電子証明書[8]の発行に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、使用する暗号アルゴリズムを特定の時期に切替可能とする。

(ｲ)　電子証明書の検証に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、それぞれの暗号アルゴリズムごとに、検証を行う期間の開始及び終了時期を設定可能とする。

(ｳ)　(ｱ)及び(ｲ)においては、以下の暗号アルゴリズムを含める。

a.電子証明書の発行及び検証に使用する暗号アルゴリズムについては、ハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA2048 [9]（以下「RSA2048」という。）の組合せ並びにハッシュ関数 SHA-256 [10]（以下「SHA-256」という。）及び RSA2048 の組合せ。

b.電子証明書の発行対象者[11]の鍵ペア[12]に使用される暗号アルゴリズムについては、RSA1024 及び RSA2048。

イ　政府認証基盤に依存する情報システム

(ｱ)　文書ファイルへの電子署名及びその検証に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、暗号アルゴリズムごとに電子署名及び検証を行う期間の開始及び終了時期を設定可能とする。

(ｲ)　(ｱ)においては、以下の暗号アルゴリズムを含める。

a.ハッシュ関数については、SHA-1 及び SHA-256。

b.公開鍵暗号方式については、RSA1024 及び RSA2048。

---

[6] Government Public Key Infrastructure：国民等と行政機関との間でやり取りされる文書ファイルについて、内容が改ざんされていないことや、その文書ファイルが真にその名義人によって作成されたかを確認できるようにするための仕組み。

[7] 商業登記に基づく電子認証制度に係る電子証明書を発行する認証局。

[8] 認証局により発行された電子署名の検証用公開鍵が真正であることを証明するデータ。

[9] 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 2048 ビットとしたもの。

[10] ハッシュ関数 SHA の一つ。与えられたデータから 256 ビットの値を生成する。

[11] 電子証明書を利用する実体（個人、組織等）をいう。いわゆる「エンドエンティティ」。

[12] 公開鍵暗号方式で使用する「秘密鍵」と「公開鍵」の対となる２つの鍵のこと。

ウ　ア及びイ以外の情報システム

(ｱ)　SHA-1 又は RSA1024 に対して現実的な脅威となる攻撃手法が示された時点で、速やかに別の暗号アルゴリズムに変更する等の対応措置を可能とする。

（例）

・　暗号モジュール[13]を、交換できるようにコンポーネント化して構成する。

・　複数の暗号アルゴリズムを選択可能とする。

(ｲ)　複数の暗号アルゴリズムを導入する場合は、以下のものを含める。

a.ハッシュ関数に SHA-1 以外を導入する場合には、SHA-256 相当以上の暗号強度を持つもの

b.公開鍵暗号方式に RSA1024 以外を導入する場合には、RSA1152 [14]相当以上の暗号強度を持つもの。

(ｳ)　SHA-1 及び RSA1024 以外の暗号アルゴリズムを導入した後は、新たなアルゴリズムで電子署名を行うこととし、検証等暗号アルゴリズムの移行が完了するまでの間に必要となる場合においてのみ SHA-1 及び RSA1024 を使用することが可能な構造とする。

エ　その他

新たな暗号アルゴリズムへの移行が完了する以前に、SHA-1 又は RSA1024 の安全性の低下による影響が発生する状況（発生が予測された場合を含む。以下同じ。）に備え、緊急避難的に、電子証明書の失効、再発行等を積極的に活用し、情報システムが提供する業務が継続して運用できる構造とする。

(2)　計画等の策定

ア　各府省庁は、(1)に定める暗号アルゴリズムの安全性向上に必要な対応について、情報システム全体の更改前の部分的な実施も検討した上で、情報システムごとの移行時期を踏まえ、必要となる対応を 2008 年度中にとりまとめる。

イ　既に発行済みの電子署名付き文書ファイル及び電子証明書について、暗号アルゴリズムの移行に伴い、失効、再発行等の対応が必要となる場合に備え、それぞれの手続きごとに、当該対応に係る手順書の整備等必要な措置を講ずる。

ウ　新たな暗号アルゴリズムへの移行が完了する以前に、SHA-1 又は

[13] ハードウェア、ファームウェア及びソフトウェアにおいて、暗号化、復号、電子署名等の暗号化機能を実装した構成要素のこと。
[14] 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さは 1152 ビットとしたもの。

RSA1024 の安全性の低下による影響が発生する状況に備え、情報システムの停止等に伴う国民への影響を最小限とするために必要な措置を講ずる。

(3)　スケジュール

ア　各府省庁は、(2)アにおいて取りまとめた内容の概要について、 2008 年度中に内閣官房に報告する。

イ　内閣官房、総務省、法務省、経済産業省及び関係府省庁は、アの報告等を基に、新たな暗号アルゴリズムへの切替時期並びに SHA-1 及び RSA1024 の使用停止時期について、2008 年度中に検討する。

ウ　内閣官房、総務省及び関係府省庁は、政府認証基盤と他の認証局との相互接続に必要となる技術要件及び新たな暗号アルゴリズムへの移行が完了する以前に安全性の低下による影響が発生する状況に備えた官民共同の電子証明書の失効等の仕組みについて、2008 年度当初に検討に着手する。

エ　内閣官房、総務省及び関係府省庁は、新たな暗号アルゴリズムに対応した情報システムの相互運用性の検証を可能とする環境の整備について 2008 年度当初に検討に着手し、2009 年度の構築を目指す。

オ　各府省庁は、上述の検討結果を踏まえ、原則として、2010 年度に新規に構築（更改を含む。以下同じ。）する情報システムから３(1)の設計要件を組み入れ、2013 年度までに各情報システムを当該要件に適合させるものとする。ただし、2009 年度に構築する情報システムについては、３(1)ウの仕様を適用する。

カ　総務省及び経済産業省は、現在使用されている SHA-1 及び RSA1024 並びに新たに使用する SHA-256 及び RSA2048 の安全性について監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

キ　総務省及び法務省は、2014 年 9 月下旬以降の早期に、政府認証基盤及び電子認証登記所（商業登記認証局）において、電子証明書の発行に使用する暗号アルゴリズムを SHA-256 及び RSA2048 の組合せに変更するとともに、電子証明書の発行対象者の鍵ペアに使用される暗号アルゴリズムを RSA2048 に切り替える。

ク　総務省及び法務省は、2015 年度までに、政府認証基盤及び電子認証登記所（商業登記認証局）において、暗号アルゴリズム SHA-1 又は RSA1024 を用いた電子証明書の検証を終了する。ただし、発行済み電子証明書の有効期間が 2015 年度末を超え、その検証の終了が制度や費用の観点で困難であり又は合理的でない場合は、2019 年度を超えない範囲で SHA-1 又は RSA1024 を用いた電子証明書の検証を行うことも可能とする。

４　本指針の見直し

本指針は、暗号技術検討会及び電子署名及び認証業務に関する法律の施行状況に係る検討会[15]の検討状況のほか、各府省庁の対応状況等を踏まえ、必要に応じて見直しを行う。

[15] 総務省政策統括官（情報通信担当）、法務省民事局長及び経済産業省商務情報政策局長の私的検討会として開催。

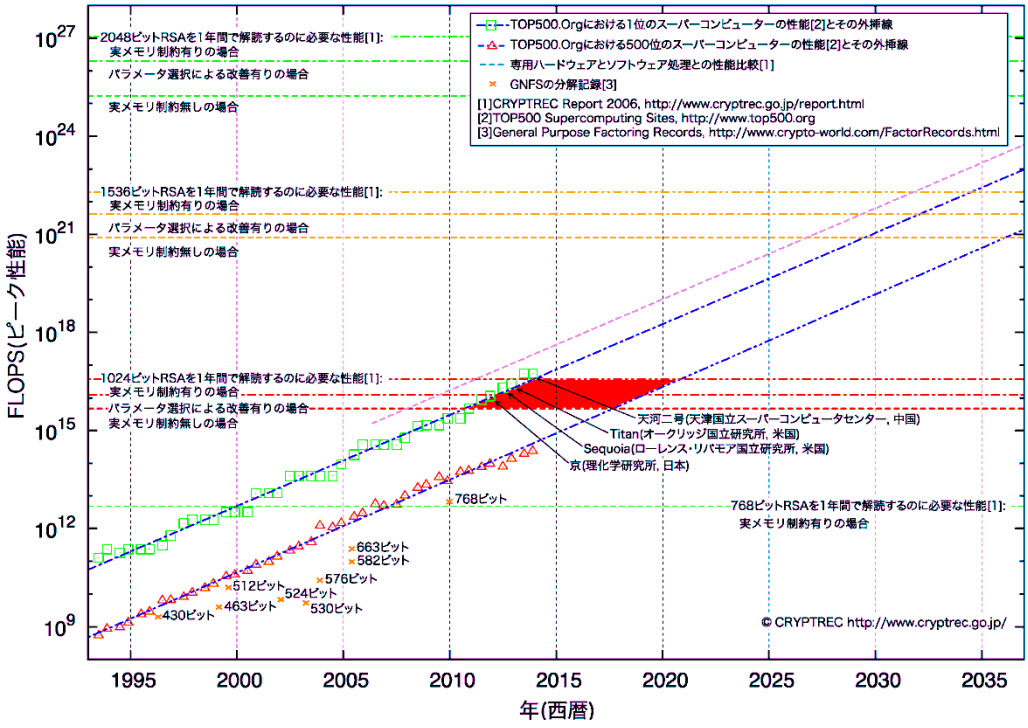
（参考２）暗号の危殆化

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（2014 年２月更新）[6]



[6] http://www.cryptrec.go.jp/report/c13_kentou_giji02_01-1.pdf［PDF］
2013 年度暗号技術調査 WG（暗号解析評価）活動報告（CRYPTREC、2014 年３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

政府機関と同様、重要な情報を取り扱う独立行政法人等もサイバー空間を巡るリスクは深刻な問題であり、昨今のサイバー攻撃事案において独立行政法人が標的となっている事例が複数判明している。

このような背景から、「サイバーセキュリティ戦略」（2013年６月10日　情報セキュリティ政策会議決定）及び同戦略の達成に向けた具体的な年度計画である「サイバーセキュリティ2014」（2014年７月10日　情報セキュリティ政策会議決定）において、政府統一基準を含む政府機関における一連の対策を踏まえ、独立行政法人等の情報セキュリティ対策を推進することを定めている。

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。

本調査の実施を通して、独立行政法人等における情報セキュリティ対策の現状を調査し、その結果を共有するとともに、情報セキュリティ対策強化への意識向上を図ることを目的とした。

２　調査概要

(1) 調査対象

独立行政法人通則法第２条第１項に定める独立行政法人並びに国立大学法人法第２条第１項に定める国立大学法人及び同法同条第３項に定める大学共同利用機関法人（以下「国立大学法人等」という。）

なお、2015年３月末日現在、独立行政法人及び国立大学法人等（以下これらを総称して「独立行政法人等」という。）の数は188法人である。

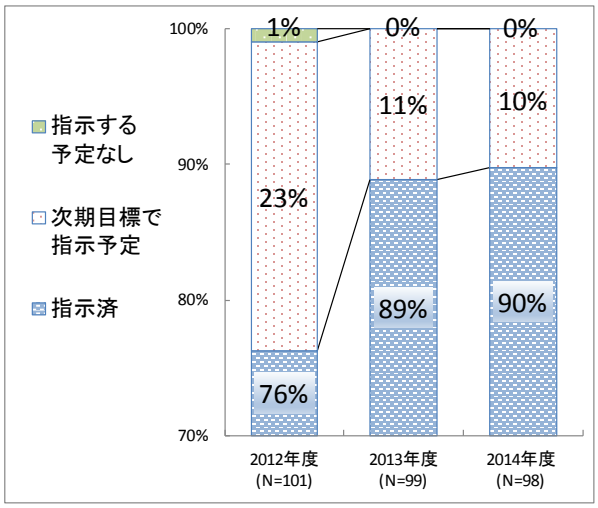
(2) 調査時期

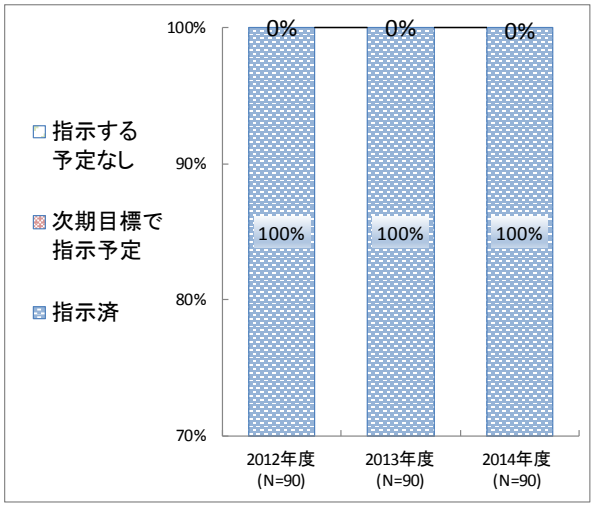
2015年３月末時点

３　調査結果の概要

(1) 中期目標での指示状況

主務大臣による中期目標（中長期目標又は年度目標を含む。以下同じ）での情報セキュリティ対策に関する事項の指示状況は、以下のとおりである。





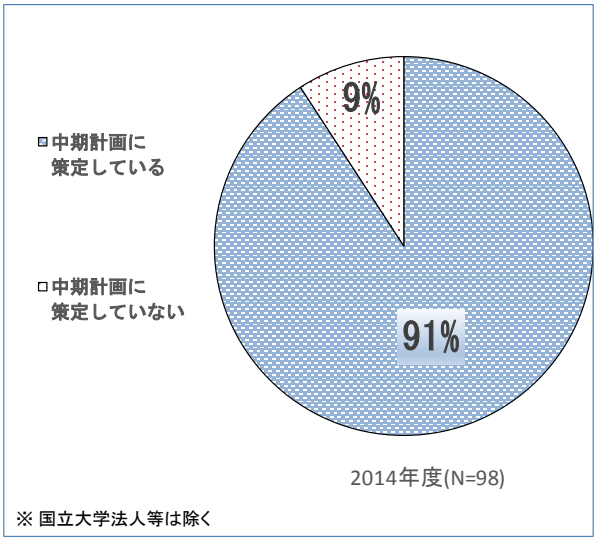
中期目標での指示状況（左：独立行政法人、右：国立大学法人等）

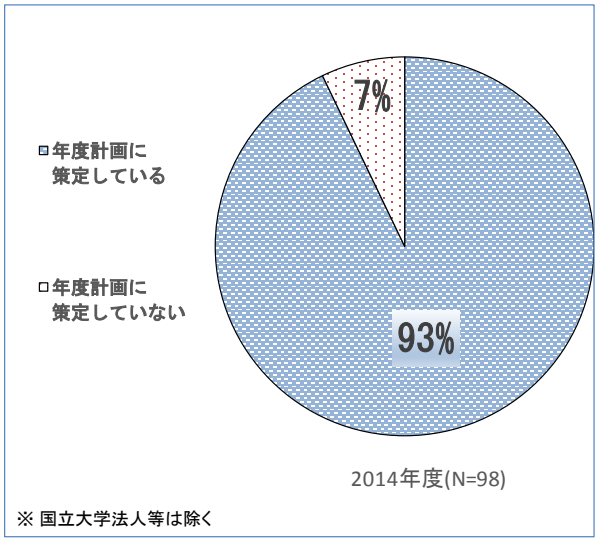
・独立行政法人98法人のうち、88法人（90%）については中期目標において指示済であり、10法人（10%）については、次期中期目標の見直し時に指示する予定である。

・国立大学法人等については、90法人全てについて、中期目標において指示済である。

(2) 独立行政法人における中期計画・年度計画への策定状況

独立行政法人における、中期計画・年度計画への情報セキュリティ対策に関する事項の策定状況は、以下のとおりである。





独立行政法人における各計画への策定状況（左：中期計画、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定められている。

・残る７法人（７%）について、前年度における情報セキュリティ対策の実施状況は次のとおりである。

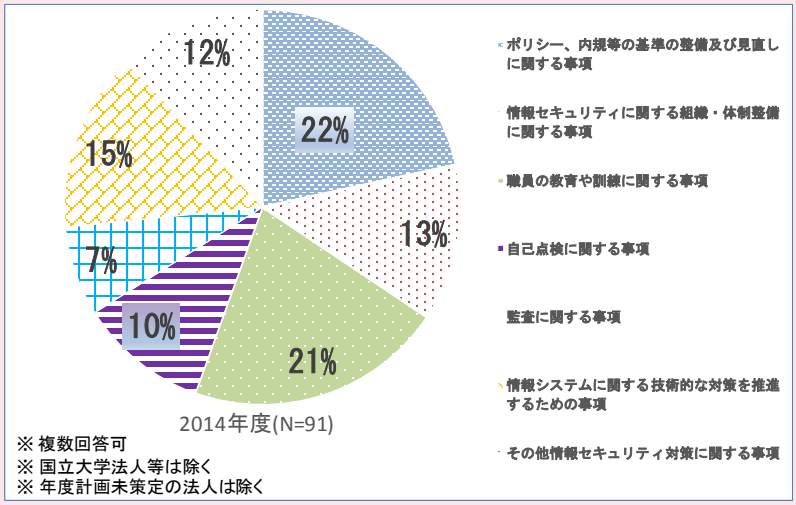
年度計画の策定と情報セキュリティ対策の実施状況	法人数
組織内の教育等、情報セキュリティ対策が行われていない法人	4
情報セキュリティポリシーの策定、組織内の教育・点検・見直し等を実施している法人	3

・残る７法人のうち、３法人は、年度計画に情報セキュリティに関する事項が定められていないが、一定の情報セキュリティ対策を進めていることがうかがえる。一方、その他の４法人は、十分な情報セキュリティ対策が実施されていないため、所管府省庁は、速やかに情報セキュリティ対策が実施されるよう、当該独立行政法人に対し指導、支援、フォローする必要がある。

・また、所管府省庁は、独立行政法人の情報セキュリティ対策の実施状況を十分認識し、独立行政制度の枠組みを活用して情報セキュリティ対策が着実に進むよう、継続的に指導、支援する必要がある。

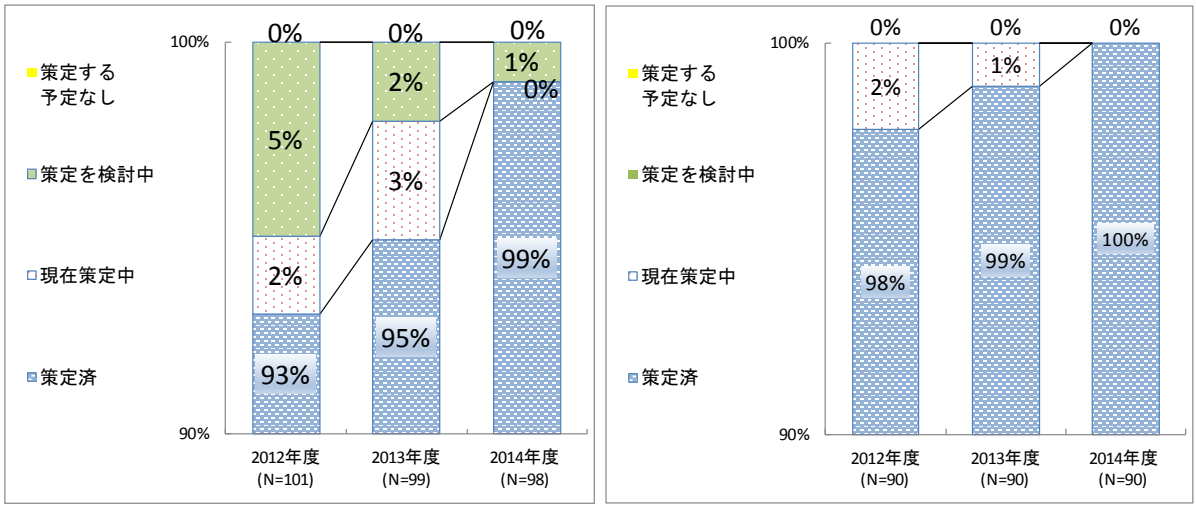
・なお、独立行政法人における年度計画に定めた情報セキュリティ対策に関する事項は、以下のとおりである。

年度計画に定めた情報セキュリティ対策に関する事項（分類状況）



(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。



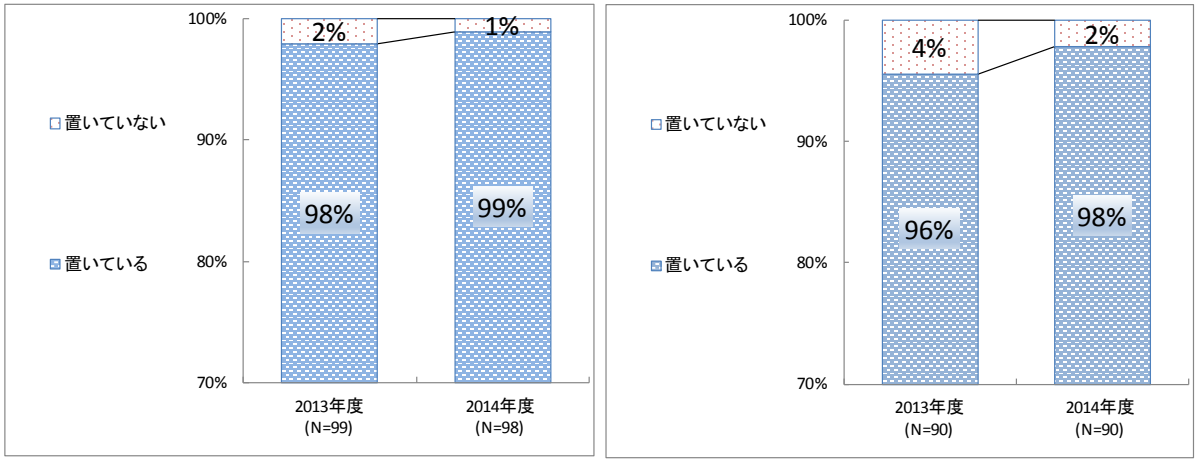
ポリシーの策定状況（左：独立行政法人、右：国立大学法人等）

・独立行政法人98法人のうち、97法人（99%）については「策定済」であり、１法人（１%）が「現在検討中」である。

・国立大学法人等については、90法人全てでポリシー策定済である。

(4) 情報セキュリティ対策推進体制

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）の設置状況は、以下のとおりである。



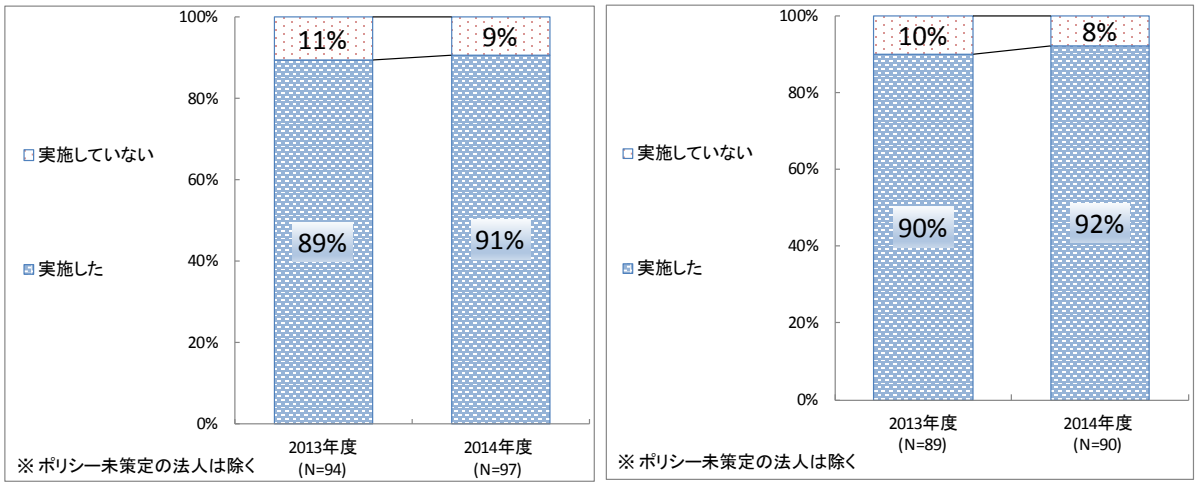
CISOの設置状況（左：独立行政法人、右：国立大学法人等）

・CISO未設置の法人は、独立行政法人で１法人（１%）、国立大学法人等では２法人（２%）と前年度よりも減少している。CISO未設置の主な理由として「適切な人材確保が難しい」が挙げられており、当該法人の情報セキュリティ対策推進体制の構築に向けて、所管府省庁による指導を通じて、組織業務全般を理解し資源配分についてリーダシップを発揮するとのCISOの本来の役割についての理解を図り、早急に設置することが必要である。

(5) ポリシーの運用状況

独立行政法人等における職員等への教育・訓練の実施状況は、以下のとおりである。

①　教育・訓練の実施状況



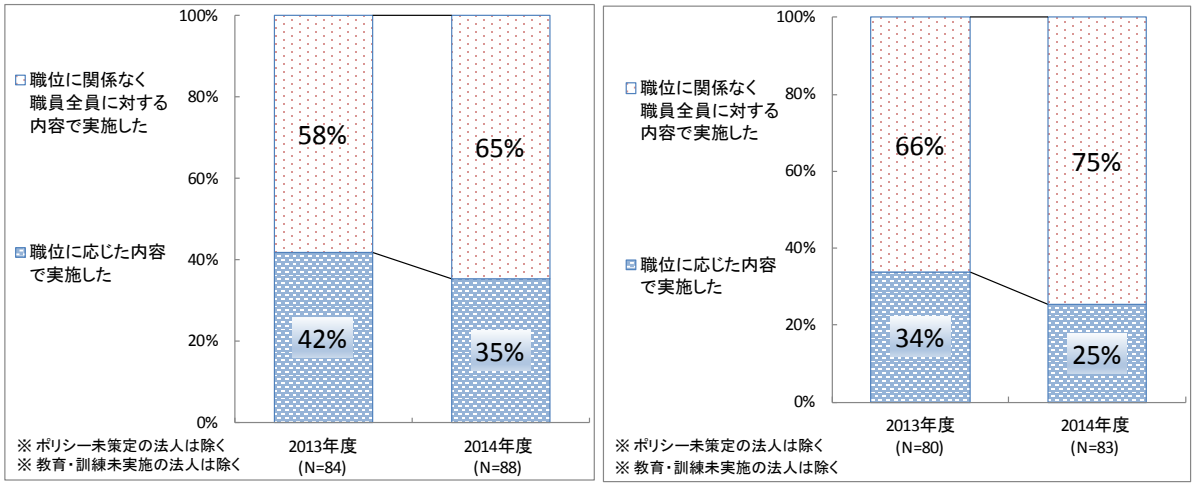
教育・訓練の実施状況（左：独立行政法人、右：国立大学法人等）

・ポリシー策定済の独立行政法人及び国立大学法人等において、教育・訓練を実施した法人は、いずれも前年度より増加している。

・未実施の独立行政法人等においては、「ポリシーや規程類の見直し中」「教育計画の未立案」「教育・訓練環境の未整備」「IT専門家のアドバイスをもらえるから教育不要」などを理由として、組織内の教育・訓練を実施していない。

・政府統一基準では、毎年度最低１回の教育・訓練を行うことを遵守事項としている。定期的に教育・訓練を行うことで情報セキュリティ対策に対する意識向上を図れるため、教育制度の確立、教育計画の立案、環境整備が推進されるよう、所管府省庁による指導・支援が必要である。

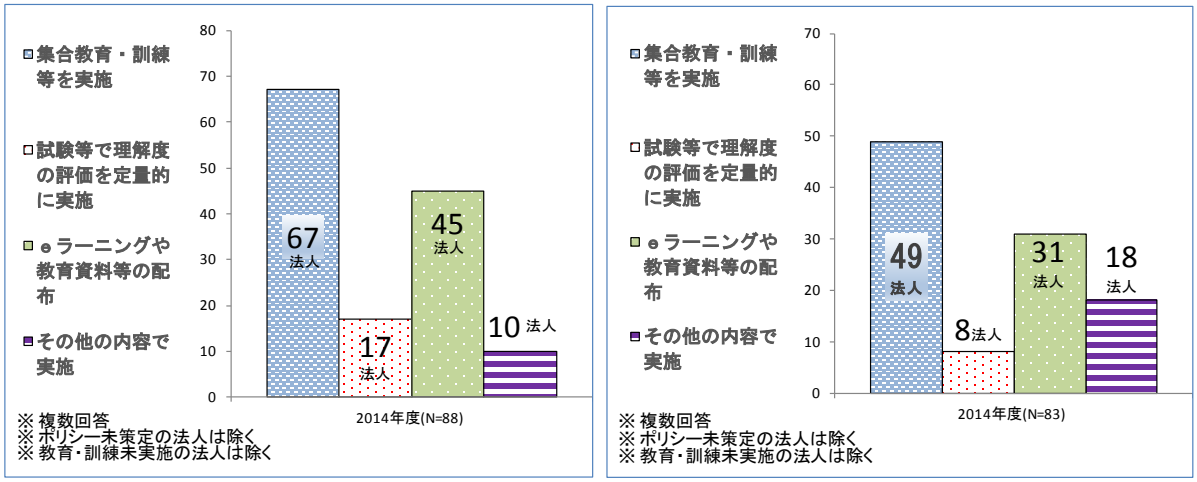
②　教育・訓練の対象



教育・訓練の対象（左：独立行政法人、右：国立大学法人等）

・独立行政法人等における教育・訓練については、約30%の法人が職員等の職位に応じた内容で実施しており、約70%の法人は職位に関係なく職員全員に対する内容で実施している。

③　教育・訓練の手段



教育・訓練の手段（左：独立行政法人、右：国立大学法人等）

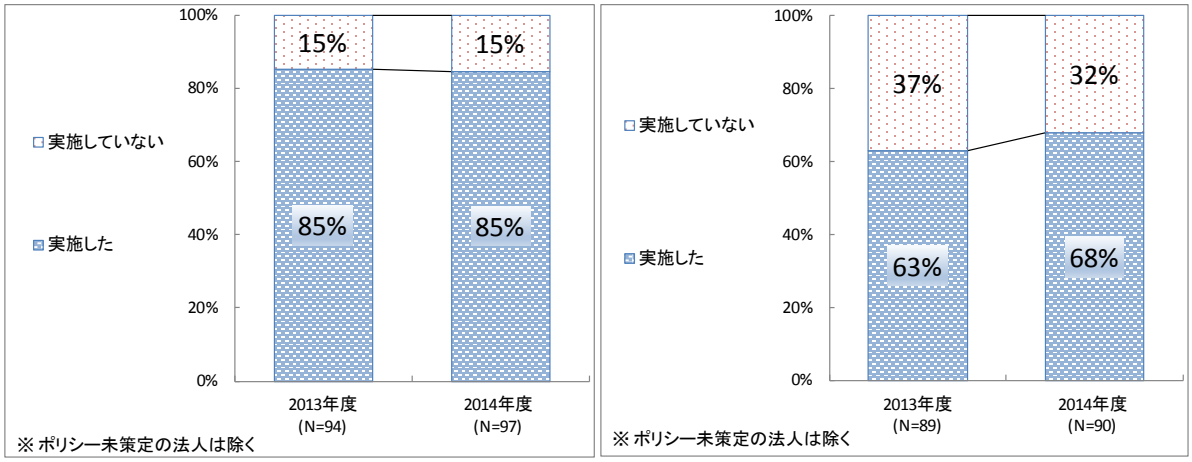
・ポリシー策定済で教育・訓練を実施した独立行政法人等では、半数以上の法人にて集合教育・訓練等を実施している。

・標的型攻撃等への対策のためにも、模擬訓練の実施や教育内容の理解度を試験等で定量的に評価するなど、他法人の取組を参考にさらなる教育内容の充実を図る必要がある。

(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の遵守状況等を把握するための取組は、以下のとおりである。

①　自己点検・監査等の実施状況



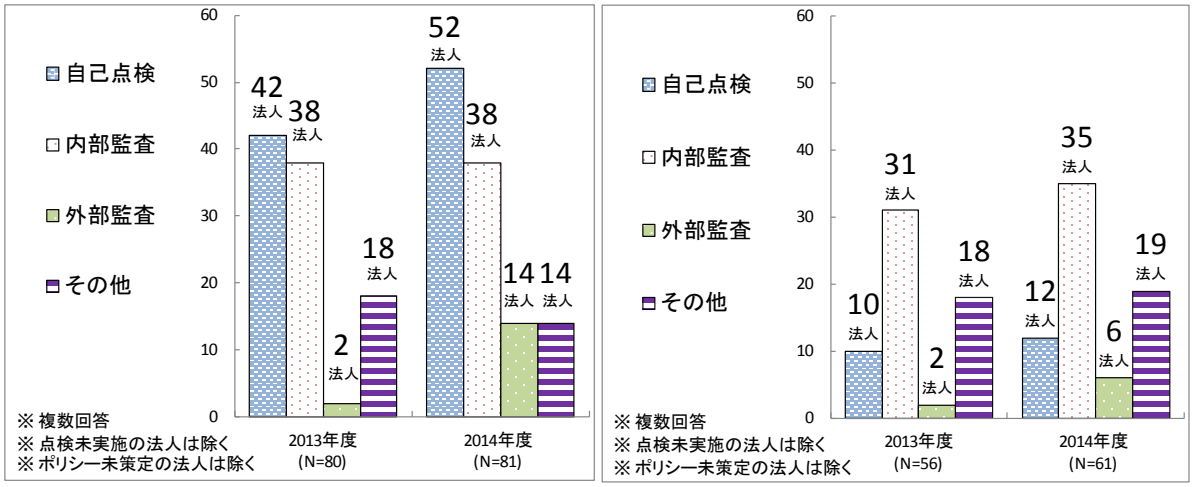
自己点検・監査等の実施状況（左：独立行政法人、右：国立大学法人等）

・ポリシー策定済の独立行政法人等で、自己点検・監査等を実施している独立行政法人は、前年度からほぼ横ばいである。一方、国立大学法人等については、前年度より増加しているものの７割未満にとどまる。

・未実施の独立行政法人等においては、「ポリシーや規程類の見直し中」「点検方法の検討中」「点検計画を立案してない」などを理由として、自己点検・監査等を実施していない。

・政府統一基準では、自己点検・監査等を行うことを遵守事項としている。定期的に自己点検・監査等を行うことで情報セキュリティ対策の実効性を確保できるため、自己点検・監査等の制度構築や計画立案が行われるよう、所管府省庁による指導・支援が必要である。

② 自己点検・監査等の実施内容



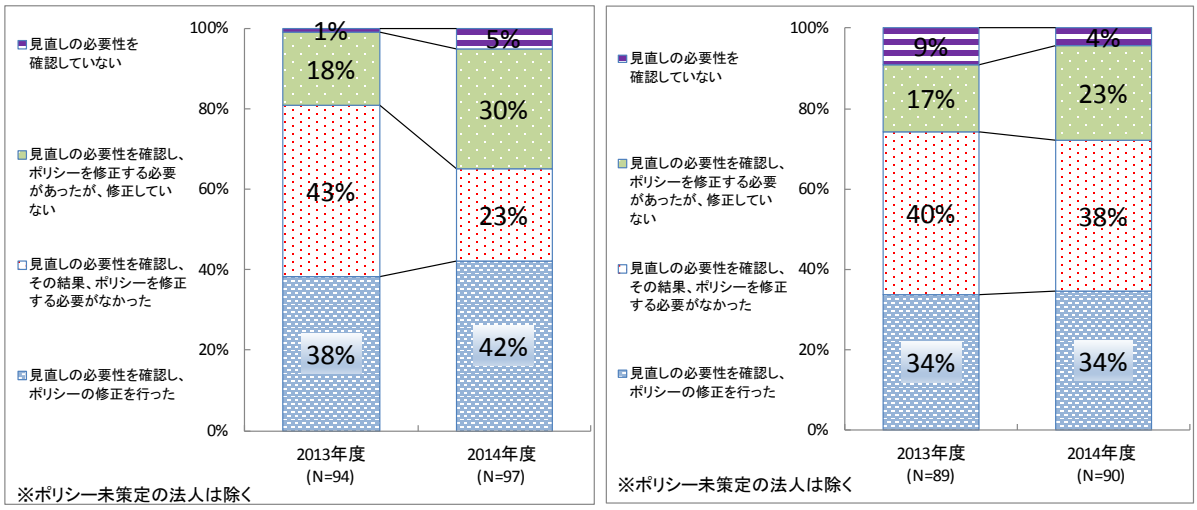
自己点検・監査等の実施内容（左：独立行政法人、右：国立大学法人等）

・国立大学法人等は内部監査のみ実施することが多いが、独立行政法人は自己点検および内部監査の両方を実施していることがうかがえる。

・外部監査の実施は、独立行政法人で前年度の２法人から14法人に、国立大学法人等で前年度の２法人から６法人に増加している。

(7) ポリシーの見直し

独立行政法人等における定期的なポリシーの見直し状況は、以下のとおりである。



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）

・ポリシー策定済の独立行政法人等において、ポリシー見直しの必要性を確認しなかった独立行政法人は、前年度の１法人（１％）から５法人（５％）に増加している一方、国立大学法人等については、前年度の８法人（９％）から４法人（４％）に減少している。

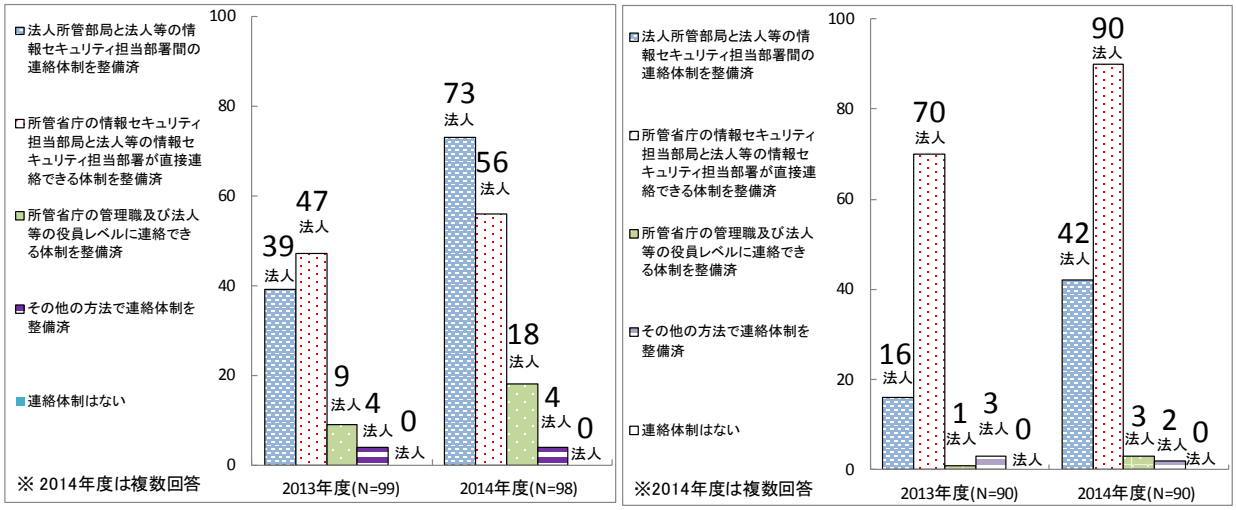
・未実施の独立行政法人等においては、「2015年度に見直す予定」などを理由としている。

・ポリシー見直しの必要性を確認し、その結果、修正が必要であったが、ポリシーを修正しなかった独立行政法人等は、前年度から大幅に増加している。

・修正が必要なのに修正しなかった独立行政法人等は、その主な理由として「現在、実施手順書や細則等含めた修正作業中（2014年度末時点で作業完了していない）」を挙げている。

(8) インシデント情報の共有体制

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所管府省庁との情報共有体制の整備状況は、以下のとおりである。



インシデント情報の共有体制（左：独立行政法人、右：国立大学法人等）

・全ての独立行政法人において、所管府省庁との連絡体制が整備されている。

・独立行政法人の情報セキュリティ担当部署における、「所管府省庁の情報セキュリティ担当部局と直接連絡できる体制」は、前年度から２割ほど増加し、「所管府省庁の法人所管部局との連絡体制」については、前年度から大幅に増加していることから、複数の連絡体制が整備されつつあることがうかがえる。

・国立大学法人等の情報セキュリティ担当部署における、「所管府省庁の情報セキュリティ担当部局と直接連絡できる体制」は、全ての国立大学法人等で整備されており、「所管府省庁の法人所管部局との連絡体制」については、前年度から大幅に増加していることから、連携体制を強めていることがうかがえる。

・インシデント情報の迅速かつ有効活用の観点から、「所管府省庁の管理職及び法人の役員レベルにも連絡できる体制」を整備した法人は、前年度から増加しているが、独立行政法人全体では約18法人、国立大学法人全体では約３法人にとどまる。インシデント対応の際には経営判断が求められる場合もあることから、実務者レベルと並行してインシデント情報及び対応状況が高職位者にも周知されるよう、早急な体制整備が必要である。

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、対応できていない独立行政法人等に対して対策実施を行うよう指導を行っており、各独立行政法人等においても改善が講じられている。

別添３－１０ NISC発出注意喚起文書及び情報セキュリティ対策推進会議決定等

１　「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）

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

平成 26 年 6 月 25 日
情報セキュリティ対策推進会議

独立行政法人においても政府機関と同様、国の重要な情報に相当する情報が取り扱われているところ、昨今のサイバー攻撃事案において、独立行政法人が標的となっている事例が複数判明している。係る状況に鑑みると、独立行政法人においても、政府統一基準群を含む政府機関における情報セキュリティ対策を踏まえた対策を講じるべきであり、以下１．～３．の措置を通じてセキュリティ対策の強化を図っていくこととする。なお、第 186 回国会（常会）において「独立行政法人通則法の一部を改正する法律」が可決されたことに伴い、実施されることとなる独立行政法人制度の改革も踏まえつつ、速やかな対策の実施が求められる。

１．独立行政法人の業務計画の一つとして情報セキュリティ対策の位置付け

独立行政法人の毎年の年度計画（法人の分類によっては、事業計画）に、政府統一基準群を含む政府機関における情報セキュリティ対策を踏まえ、独立行政法人において情報セキュリティ・ポリシーを定めるとともに、これに基づき情報セキュリティ対策を講ずる旨、盛り込むこととする。また年度計画（法人の分類によっては、事業計画）の基として、通則法に基づいて主務大臣から所管の独立行政法人に指示される中期目標（法人の分類によっては、中長期目標又は年度目標）にも、同様に情報セキュリティ対策を講ずる旨、盛り込むこととする。

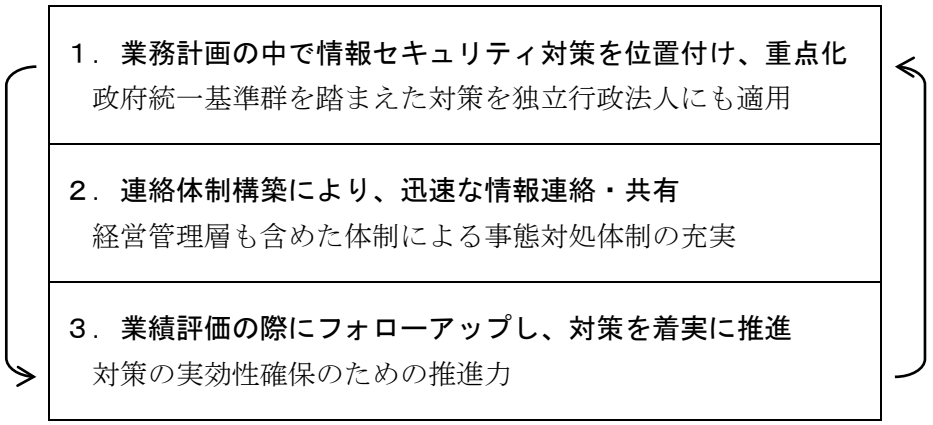
２．実効性のあるインシデント情報共有体制の構築

被害の拡大防止等の観点から、インシデント情報を各独立行政法人において迅速かつ有効活用するため、所管府省庁を通じた情報連絡体制を構築する。インシデント対応の際には経営判断が求められる場合もあることから、実務者レベルと並行して、所管府省庁管理職、独立行政法人役員レベルにもインシデント情報及び対応状況が周知される体制とする。情報共有体制を通じて、インシデント発覚時のＮＩＳＣへの情報提供、ＮＩＳＣからの注意喚起の双方向の円滑な情報連絡を図る。

３．業務実績評価時における情報セキュリティ対策の確認

各独立行政法人は、事業年度ごとに通則法に基づき主務大臣による業務の実績等に関する評価を受ける。その際に、主務大臣は情報セキュリティ対策の実施状況に関しても評価を行い、評価結果を公表する。係る評価結果に関しては、ＮＩＳＣにおいても確認し、必要に応じて所管府省庁に対して助言等を行うものとする。

（参考）対策のイメージ



２　「情報システムで利用しているソフトウェアのサポート終了に伴う対応について（注意喚起）」（2014年７月10日NISC発出）[7]

事　務　連　絡
平成 26 年 7 月 10 日

各府省庁等情報セキュリティ担当課室長　殿
情報セキュリティ対策推進会議オブザーバー機関情報セキュリティ担当課室長等 殿

内閣官房情報セキュリティセンター
内閣参事官（政府機関総合対策促進担当）

情報システムで利用しているソフトウェアのサポート終了に伴う対応について（注意喚起）

ソフトウェアベンダによるサポートを受けているソフトウェアについては、当該サポートの終了に伴い、情報セキュリティ関連の脆弱性を修正するための修正プログラムがソフトウェアベンダから原則として提供されなくなり、これらのソフトウェアを利用している情報システムに関しては、ウイルス対策ソフトウェアを導入するなどの対策を講じていたとしても、不正プログラム感染や不正アクセスによる情報漏えい等のリスクが高くなります。

最近の例では、Windows Server 2003※1については、約１年後の 2015 年７月 15 日にサポートの終了が予定されており、独立行政法人情報処理推進機構から当該ソフトウェアを利用している企業・組織に対して、当該ソフトウェアサポートが継続している OS へのバージョンアップ実施を呼びかける内容の注意喚起が発表されているところであり、利用しているソフトウェアのサポート終了に備え、所要の対応を講ずる必要があります。

つきましては、各府省庁の情報システムを構成するサーバや端末等の機器で利用している OS、ミドルウェア、アプリケーション等の各種ソフトウェアのソフトウェアベンダによるサポート期間を適時確認し、サポート終了までにソフトウェア更改等の必要な対応を徹底するようお願いいたします。

また、現在運用している情報システムに限らず、情報システムの新規調達又は更改の際には、サポート期間を考慮した上で導入するソフトウェアを決定するようお願いいたします。

[7] http://www.nisc.go.jp/active/general/pdf/soft_140710.pdf［PDF］

(参考)

○「府省庁対策基準策定のためのガイドライン」(NISC、平成 26 年５月 19 日)の「6.2.1 ソフトウェアに関する脆弱性対策」
http://www.nisc.go.jp/active/general/pdf/guide26.pdf

○「サポートが終了する Windows Server 2003 を利用している企業・組織への注意喚起」　(独立行政法人情報処理推進機構)
http://www.ipa.go.jp/about/press/20140708.html

○「Windows Server 2003 のサポートが終了します」　(マイクロソフト社)
http://www.microsoft.com/ja-jp/server-cloud/local/products/windows-server-2012-r2/migration/campaign.aspx ※2

○マイクロソフト　プロダクト　サポート　ライフサイクル　(マイクロソフト社) http://support.microsoft.com/lifecycle/?C2=1163 ※2

※1　マイクロソフト社のソフトウェア製品。ウェブサーバやファイルサーバ等の各種サーバで使用されることが多い。

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

３　「行政文書の管理に関するガイドラインの一部改正に伴う政府機関の情報セキュリティ対策のための統一基準の扱いについて」（2015年１月23日内閣官房副長官）[8]

閣サ第 19 号
平成 27 年１月 23 日

（別紙１）あて

内閣官房副長官
（情報セキュリティ対策推進会議議長）

行政文書の管理に関するガイドラインの一部改正に伴う
政府機関の情報セキュリティ対策のための統一基準の扱いについて

今般、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）が一部改正されたところですが、それに伴う「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推進会議決定）（以下「統一基準」という。）の扱いについては下記のとおりとしますので、各府省庁の情報セキュリティポリシーの運用に際して御留意をお願いします。

記

1.　統一基準の「1.2 情報の格付の区分・取扱制限」の「機密性についての格付の定義」については、それぞれ下表のとおり解釈をしていただくようお願いします。また、機密性３情報」の分類の基準における「秘密文書」は、従前は『「秘密文書等の取扱いについて」（昭和40年４月15日事務次官等会議申合せ）の定めによる「秘密文書」を指す』ものでしたが、行政文書の管理に関するガイドラインの一部改正に伴い、『「行政文書の管理に関するガイドライン」の定めによる「秘密文書」を指す』ものとします。

格付の区分	分類の基準（統一基準）	分類の基準の解釈
機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報	行政事務で取り扱う情報のうち、「行政文書の管理に関するガイドライン」に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当	行政事務で取り扱う情報のうち、行政機関の保有する情報の公開に関

[8] http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai01/pdf/01shiryou07.pdf［PDF］

	する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報	する法律（平成 11 年法律第 42 号）（以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	公表済みの情報、公表しても差し支えない情報等、機密性２情報又は機密性３情報以外の情報	情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

2.　「行政文書の管理に関するガイドライン」の第 10「公表しないこととされている情報が記録された行政文書の管理」においては、秘密文書の管理について、秘密文書の指定区分（「極秘文書」又は「秘文書」）ごとに適正な管理を求めています。秘密文書の管理に関しては、「行政文書の管理に関するガイドライン」の規定を優先的に適用し、当該ガイドラインに定めが無い事項については、統一基準の定めるところによるものとします。

　情報セキュリティポリシーの運用に際しての留意事項について、別紙２に示します。

４　「ネット上の外部サービス利用による情報漏出の危険性について(注意喚起)」(2015年２月20日NISC発出) [9]

事　務　連　絡
平成 27 年 2 月 20 日

各府省庁情報セキュリティ担当課室長　殿
オブザーバー機関情報セキュリティ担当課室長等 殿

内閣官房　内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）

ネット上の外部サービス利用による情報漏出の危険性について（注意喚起）

一部で報道されているとおり、政府機関から外部に送信されたメールについて、民間のオンライン翻訳サイトを利用したことに伴い、当該メールが閲覧可能な状態になっていました。

オンライン翻訳サイトをはじめ、主に一般消費者向けにネット上で無料提供されている、ウェブメールサービス、グループサービス、検索サービス、オンラインストレージ、データ転送、ソーシャルメディア、日本語文字入力補助（ＩＭＥ）等のサービスについては、利用の際の情報管理について保証がないことが一般的です。これまでにも、こうしたサービスの不用意な利用により、政府機関の情報が意図せず外部に漏出した例があります。

「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版)」では約款による外部サービスの利用において要機密情報を取り扱わないよう求めております。職員が業務上、特に要機密情報に関してこうしたサービスを利用することのないよう、不要なサービスへの接続を遮断する等の技術的措置を含め、改めて徹底をお願いいたします。

また要機密情報はもちろん、メールも含め、情報をいったん外部に送信してしまうと、その後は情報の管理が及ばず、第三者に見られるリスクがあるものと十分認識し、送信内容や方法（暗号化など）について細心の注意を払うことが必要です。

以上の旨、各職員向けへの注意喚起方、お願いいたします。

（参考）独立行政法人情報処理推進機構「今月の呼びかけ」
http://www.ipa.go.jp/security/txt/2014/02outline.html

[9] http://www.nisc.go.jp/active/general/pdf/gaibuservice_150220.pdf [PDF]

５　「ウェブサイト等の利用者に使用を求めているソフトウェアのサポート終了に伴う対応について（注意喚起）」（2015年３月３日NISC発出）[10]

事　務　連　絡
平成 27 年３月３日

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

内閣官房　内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）

ウェブサイト等の利用者に使用を求めているソフトウェアのサポート終了に伴う対応について（注意喚起）

府省庁が運営しているウェブサイト等において利用者の動作環境として特定の汎用ソフトウェア（バージョン）の使用を求めている場合がありますが、当該ソフトウェア（バージョン）のサポート終了後にも継続して使用を求めることは、利用者を危険にさらすことにつながるものであり、政府機関統一基準の遵守事項 6.3.1 においては、このようなことも含む「府省庁外の情報セキュリティ水準の低下を招く行為」の防止を規定しているところです。

最近の例では、オラクル社からは Java SE 7 について 2015 年４月にサポートを終了することが、マイクロソフト社からは Internet Explorer について 2016 年１月以降 OS に紐づく特定のバージョンのみをサポートすることがそれぞれ発表されています。

インターネット上で国民等に向けて公開しているウェブサイトや政府機関内で共通的に利用している情報システム等において、利用者の動作環境としてサポートが終了しているソフトウェア（バージョン）の使用を求めることのないよう、必要な対応をお願いいたします。

（対応の例）

○サポートが継続されるバージョンでの動作検証を行い、正常動作を確認後、利用者に当該バージョンで動作する旨を周知

○サポートが継続されるバージョンでの動作検証を行い、動作に異常がある場合にはサポートが継続されるバージョンで動作するようプログラムを修正し、利用者に当該バージョンで動作する旨を周知

[10] http://www.nisc.go.jp/active/general/pdf/soft_150303.pdf［PDF］

○当該ソフトウェアを利用者が使用しないでもよいようプログラムの構造を修正

○利用者の情報セキュリティ水準を低下させない利用方法を利用者に周知（例：ソフトウェアが備える互換表示機能等の利用を推奨する）

また、ウェブサイト等の新規構築、更改等の際には、利用者に使用を求めることとなるソフトウェアのサポート期間を考慮した上で導入するソフトウェアを決定する、利用者に使用を求めるソフトウェアのサポート終了時における動作検証等を保守契約の内容に含めるなどの措置を講じてください。

なお、府省庁の情報システムにおける自らの利用者環境についても、「情報システムで利用しているソフトウェアのサポート終了に伴う対応について（注意喚起）」（平成 26 年７月 10 日　内閣官房情報セキュリティセンター）のとおり、必要な対応を徹底するようお願いいたします。

（参考）

○「府省庁対策基準策定のためのガイドライン」（平成 26 年５月 19 日　内閣官房情報セキュリティセンター）の「6.3.1 アプリケーション・コンテンツの作成時の対策」
http://www.nisc.go.jp/active/general/pdf/guide26.pdf

○情報システムで利用しているソフトウェアのサポート終了に伴う対応について（注意喚起）（平成 26 年７月 10 日　内閣官房情報セキュリティセンター）
http://www.nisc.go.jp/active/general/pdf/soft_140710.pdf

○Java 7 のパブリック・アップデートの終了（オラクル社）
https://www.java.com/ja/download/faq/java_7.xml※1

○Oracle Java SE サポート・ロードマップ（オラクル社）
http://www.oracle.com/technetwork/jp/java/eol-135779-ja.html※1

○Internet Explorer のサポート ライフサイクル ポリシーに関する FAQ（マイクロソフト社）
https://support2.microsoft.com/gp/microsoft-internet-explorer※1

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

別添３－１１ 政府機関等に係る2014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
2014年	４月	【概要】大阪労働局において、休職者支援訓練実施施設に対して、申込手続きに係る事務連絡をメールで送信した際、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、「宛先」で一斉送信したため、全員のメールアドレスが表示されて送信される個人情報漏えい事案が発生。 【対応等】全職員に対し、本事案の経過を説明し、複数の外部の宛先にメール送信する場合には、複数人による確認の徹底を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・取扱いについての徹底を図るよう指示。	意図せぬ情報流出
		【概要】中国労災病院は、同院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。	外部からの攻撃
		【概要】国立感染症研究所は、ウェブメールサーバへの不正アクセスにより、職員のメールアドレスから約2000件の迷惑メールが送信されたと発表。 【対応等】迷惑メール発信元のアカウントを抹消し、パスワード奪取に関わった不正なウェブサイトをアクセス禁止に設定するとともに、全職員に対して注意喚起のメールを送信する等により、周知徹底を図った。	外部からの攻撃
		【概要】千葉大学は、当該大学教授のハードディスクに保存されていた学生等に関する個人情報が、インターネット経由で閲覧できる状態になっていたと発表。	意図せぬ情報流出
	５月	【概要】国会図書館は、国立国会図書館内ネットワークシステムの運用管理業務の委託先事業者の社員が、同業務の遂行のため与えられた権限を利用し、国立国会図書館の内部情報を不正に閲覧・複写し取得したと発表。 【対応等】国立国会図書館内における情報セキュリティ対策を強化し、運営管理者の不正行為を抑止する再発防止策を早急に講じた。	内部不正
		【概要】神戸大学は、留学生３人が大学から付与されている神戸大学ネットワークのID・パスワードを外部に漏らし、海外から不正アクセスされた事案があったと発表。	内部不正
	６月	【概要】大阪大学は、理学研究科・理学部ウェブサイトが改ざんされていると大学ホームページで発表し、６月25日に、外部からの不正アクセスがあった旨の報告を発表。	外部からの攻撃
		【概要】国土地理院は、６月18日にアンケート調査への協力依頼メールをBccで発信した際、その後のウイルス検査結果メール（自動配信）がシステム設定不備により、メールアドレスが見える状態で発信されてしまったと発表。 【対応等】送信先に、直ちに連絡し、謝罪するとともにメールの削除を依頼。また、ウイルスチェックサーバの設定の修正を行い、通知メールが送信される場合に不必要な情報が表示されないような措置を講じた。	意図せぬ情報流出
	７月	【概要】情報・システム研究機構は、Webサイトへの第三者による不正アクセスがありスクリプトを埋め込まれたが、同日中に完全除去したと発表。	外部からの攻撃
	８月	【概要】防災科学技術研究所は、同研究所の一部のサイトに意図しないフィッシングサイトが８月９日に作成されていたと発表。	外部からの攻撃
		【概要】厚生労働省は、障害者関連団体の代表ら少なくとも22人の氏名、住所、電話番号などを外部業者に伝え、この業者のホームページで2013年１月～2014年６月５日の間、閲覧可能な状態になっていたと発表。情報の悪用などは報告されていないという。 【対応等】このような事案が二度と発生することがないよう、発送業務等の調達を行う際には、複数の職員による仕様書のダブルチェックを行うことにより、個人情報の漏洩防止を徹底するよう措置。	意図せぬ情報流出
		【概要】国立長寿医療研究センターは、個人情報を含むUSBメモリを３月４日にセンター内で紛失したと発表。個人情報は１件（１家族）で、当該者には説明済。	その他
	９月	【概要】交通安全環境研究所は、ホームページ上にて講演会等に申込を行った人の個人情報が８月15日～26日の間、閲覧可能な状態であったと発表。	意図せぬ情報流出
		【概要】中部労災病院は、９月７日～10日にかけて同院の職員のメールアドレスが不正利用され、迷惑メールが発信される事象が発生したと発表。	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】法務省は、同省民事局と法務局のサーバーに不正アクセスがあり、法務局の情報の一部が外部に送信された可能性があると発表。 【対応等】直ちに情報流出を防止する措置をとった。	外部からの攻撃
	10月	【概要】国土地理院は、職員の業務用パソコンがウイルスに感染し、情報が外部に送信された可能性があると発表。 【対応等】原因及び外部に送信された可能性のある情報等について、調査を実施。	外部からの攻撃
		【概要】環境省国際サンゴ礁研究・モニタリングセンターは、ウェブサイトが８月27日～９月16日の間、不正アクセスされていたことが判明したと発表。 【対応等】当該サイトについては環境省ホームページへの統合を予定しており、それまでの間その運用を休止。また、情報セキュリティ対策の見直し等再発防止に向けて鋭意取り組みを実施。	外部からの攻撃
	11月	【概要】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、不正な発信に利用されたメールアドレスを抹消した。	外部からの攻撃
		【概要】国際交流基金の日中交流センターは、同センターのメールアカウントが不正に利用され、大量の迷惑メールが送信されていたことが確認されたと発表。	外部からの攻撃
		【概要】厚生労働省において、入札説明会に参加した業者から送付依頼のあった文書をメールで送信した際、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、「宛先」で一斉送信したため、全員のメールアドレスが表示されて送信される個人情報漏えい事案が発生。 【対応等】電子メールを複数の個人のメールアドレス宛に送信する場合には、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、個人情報の漏えい防止の徹底を図るよう指示。	意図せぬ情報流出
	12月	【概要】国土交通省中国地方整備局は、情報公開Webサイト「瀬戸内海環境情報センター」の一部が不正アクセスされ、改ざんされていたため、当該サイトを一時閉鎖し原因調査を進めたと発表。 【対応等】再発防止のために必要な対策を講じるまでの間、本Webサイトは一時閉鎖。今後、更に情報セキュリティの強化に向けて取り組みを実施。	外部からの攻撃
2015年	１月	【概要】慶応大や産業技術総合研究所など５つの研究機関がサイバー攻撃の被害に遭っていたことが関係者への取材で分かった。いずれもサーバーに侵入され、サイトの一部を改ざんされるなどした。被害に遭ったのは、他に城西国際大、愛知工業大、国立障害者リハビリテーションセンター。 【対応等】国立障害者リハビリテーションセンターでは、直ちに必要なアップデート等の対策を講じ、今回と同様の手法のサイバー攻撃があったとしても被害を受けないことを確認。	外部からの攻撃
	２月	【概要】東京労働局は、高校生就職面接会への参加申込みをした企業に対し、その可否をメールにより通知した際、通知先の担当者等のメールアドレスを「BCC」に設定して送信すべきところを誤って「宛先」で一斉送信したため、参加申込企業の担当者等のメールアドレスが表示されて送信される個人情報漏洩事案が発生。 【対応等】２月４日に労働局各部室長、管下公共職業安定所長及び管下労働基準監督署長に対し、本事案の経過を通知し、メール誤送信の防止をはじめとした基本的な作業手順の徹底を図るよう指示。	意図せぬ情報流出
		【概要】大阪国税局は、調査で得た情報が保存された外付けHDDを紛失したと発表。当該HDDには、納税者の会計データなどの個人情報が記録されていた。 なお、外部への流出は確認されていない。 【対応等】媒体の管理方法として、媒体や書類などを所持して庁舎内を移動する際には、書類との混同を避けるため、専用の箱に入れて移動することとし、専用の収納庫に常時施錠して保管することを徹底するなどの改善を図った。	その他
		【概要】日本貿易振興機構は、海外事務所職員のPC１台が昨年９月に外部からの標的型メールの送付を受け、不正なプログラムに感染していたことが調査により判明したと発表。	外部からの攻撃

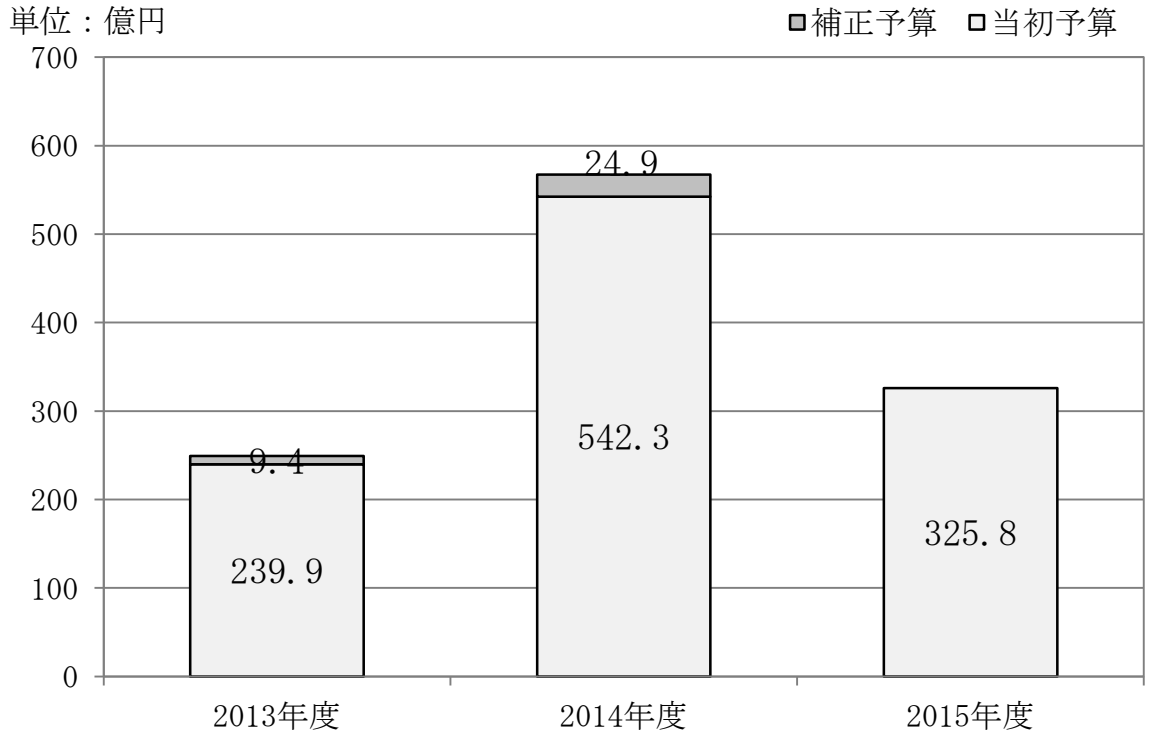
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
	３月	【概要】原子力規制委員会は、原子力に関する内部の研修資料の電子データが、クラウドソーシングサイト上で誰でも見られる形で公開されていると明らかにした。 【対応等】原子力規制庁は契約先に対し、工事請負契約等に係る指名停止等措置要領（環境省大臣官房会計課長通知）第10条に基づき文書にて注意喚起を実施するとともに、原子力規制庁職員に対しては、環境省情報セキュリティポリシー（第７版）（平成26年10月27日環境省情報セキュリティ委員会）に基づき、委託先における情報セキュリティ対策の履行状況の確認や、委託先への情報の提供等において遵守すべき事項等について、再度周知を実施。	その他

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

別添３－１２ 政府のサイバーセキュリティ関係予算額の推移

	2013 年度	2014 年度	2015 年度
当初予算額	239.9 億円	542.3 億円	325.8 億円
補正予算額	9.4 億円	24.9 億円	－

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

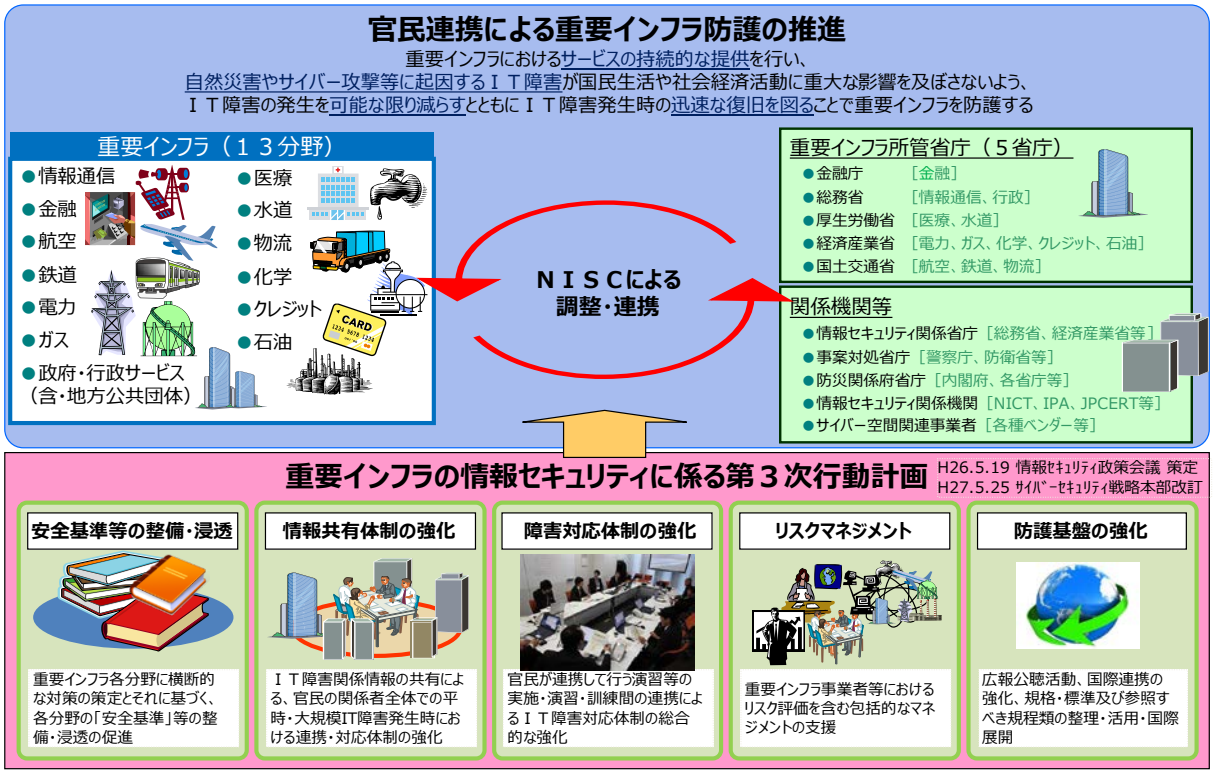


別添４　重要インフラ事業者等における情報セキュリティ対策に関する取組等

＜別添４－目次＞

別添４－１　第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

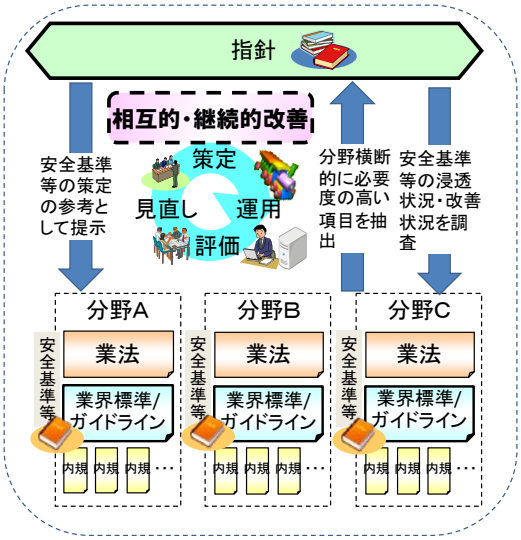
行動計画期間中の施策

（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

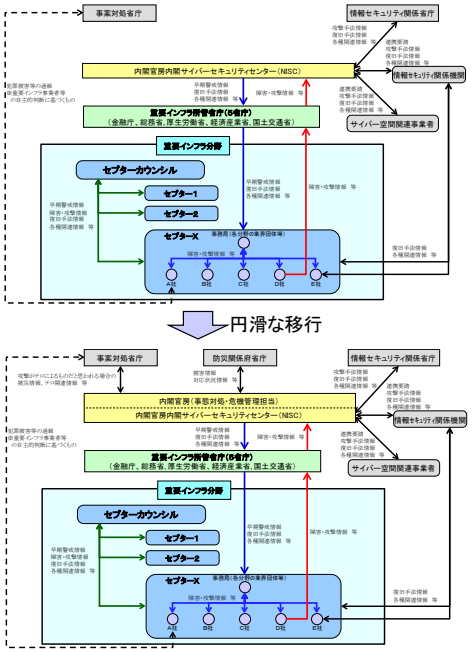
（３）　関係主体の役割の明確化
- 多様な関係主体の役割を平時・大規模IT障害発生時に分類して明確化

第３次行動計画に基づく取組

平時

平時の延長線上の体制

大規模IT障害発生時



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

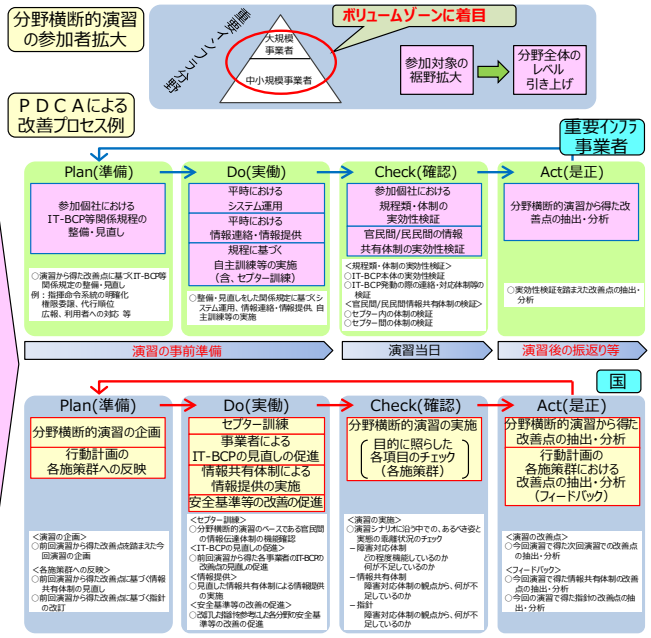
- 横断的演習の成果の重要インフラ全体への普及・浸透
- IT障害発生時の対応を踏まえた関係主体の在り方
- 重要インフラ所管省庁等による演習・訓練との連携　　等

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

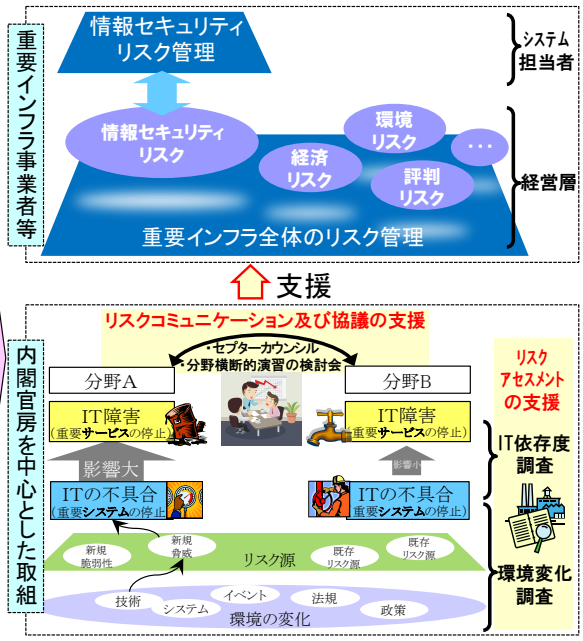
行動計画期間中の施策

（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

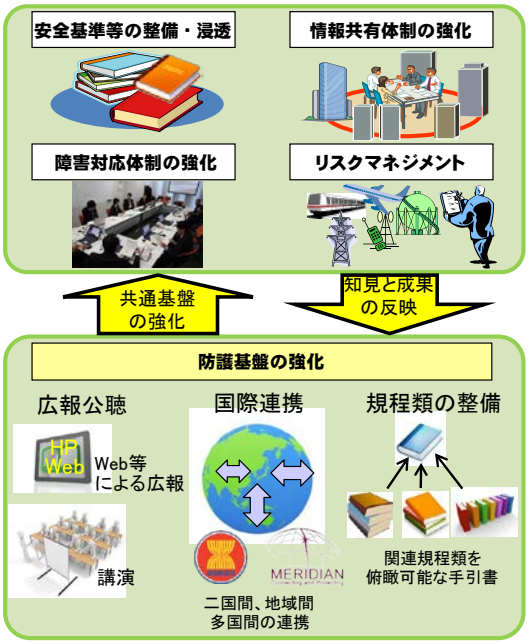
行動計画期間中の施策

（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

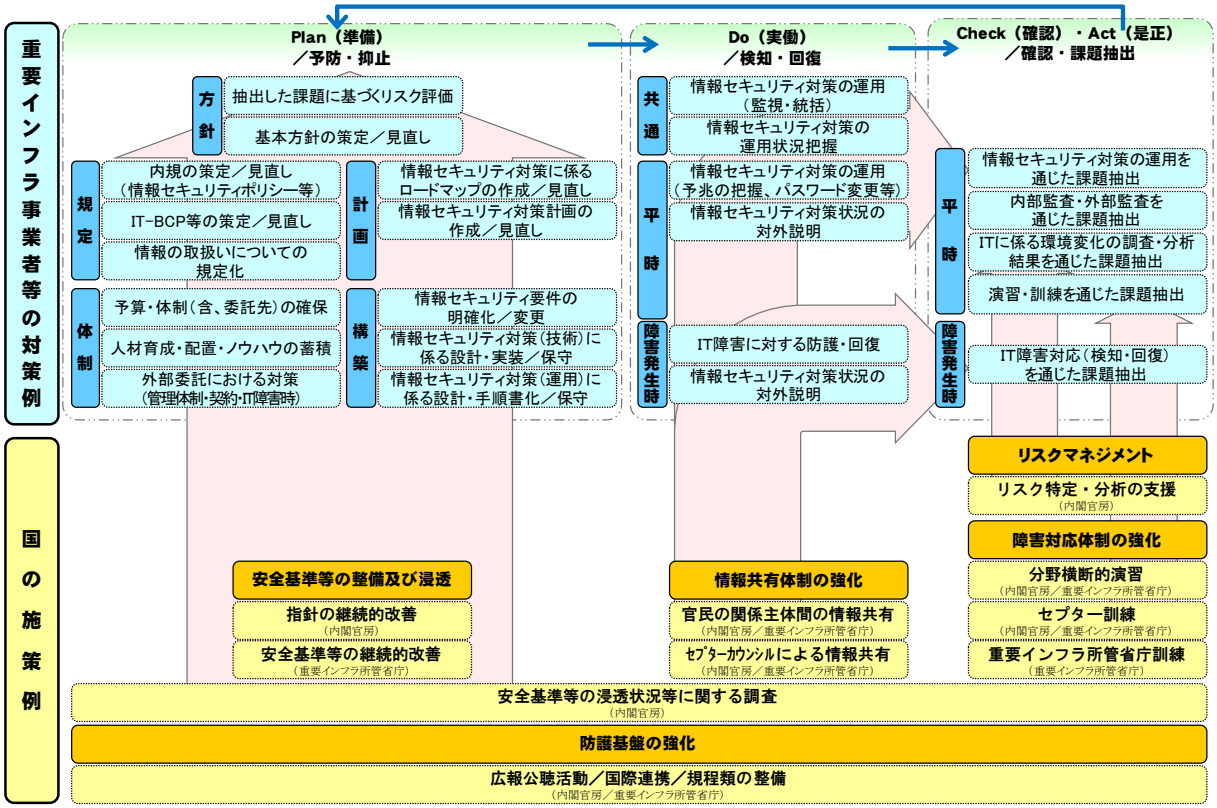
（２）　国際連携
- 欧米、ＡＳＥＡＮ、Meridian等二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携

（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」



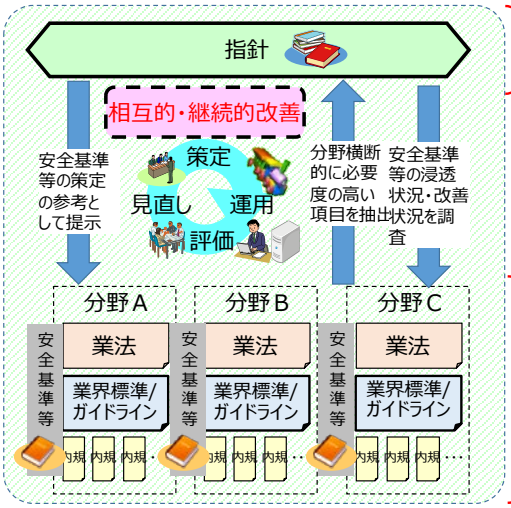
別添４－２　安全基準等の継続的改善状況等の把握及び検証

重要インフラ専門調査会第１回会合（平成27年３月26日）資料５（2014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】

◆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
◆サイバーセキュリティ2014　：　重要インフラ所管省庁の協力を得つつ、各重要インフラ分野における安全基準等の継続的改善状況を把握するための調査を実施し、結果を公表する

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】

○新規３分野を含む全ての重要インフラ分野（13分野）の以下について、2015年１月～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３版改訂版（2012年度末改定）等を契機とした各分野の「安全基準等」の改善状況(2013年度～2014年度)については、以下のとおり。

2014年度までに改善済	：	４分野（電気通信、ケーブル、医療、水道）
2014年度末までに改善予定	：	２分野（金融、政府・行政）
既に適合済であるため改善不要と判断	：	１分野（電力）
指針第４版の対応と合わせて改善予定	：	６分野（放送、航空運送、航空管制、鉄道、ガス、物流）
分野新設に伴う「安全基準等」新設（予定）	：	３分野（化学、クレジット、石油）
	・化学	： 2014年度末策定に向け対応中
	・クレジット	： 2014年12月に新規策定
	・石油	： 2014年度末策定に向け対応中

○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	①：2013年３月／－／2014 年６月 ②：2013年３月 ③：2013年12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。 ②：電気通信事業法の改正を踏まえた改訂。 ③：実施予定なし。（2013年度に指針（第３版）改定を受けた検討を行い、実施済み）
	２．継続的改善（分析・検証）プロセス ①：2013年４月より2013年10月／－／2014年10月より2014年12月にかけ実施。 ②：2014年７月より2015年３月にかけ実施中。 ③：－
	３．継続的改善（分析・検証）の結果 ①：適用対象ではなかった電気通信事業者のうち、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事業者に対し、新たに適用する技術基準を規定。 ②：－ ③：－
	４．その他

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** 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 会員事業者の情報セキュリティポリシー導入支援を推進中。

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** 指針改定を受けて実施。
	２．継続的改善（分析・検証）のプロセス 現在のガイドラインの改善を実施中。
	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（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 ②：2013年3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：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：実施予定なし。
	２．継続的改善（分析・検証）のプロセス ①：－ ②：2013年６月より2015年３月を目処に実施。(業態別化の検討は2015年３月以降も継続する予定。) ③：－
	３．継続的改善（分析・検証）の結果 ①：－ ②：－ ③：－
	４．その他

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** 定期的な改善、指針改定を受け実施。
	２．継続的改善（分析・検証）のプロセス 2012年11月より航空運送事業者・定期航空協会・国土交通省において実施。
	３．継続的改善（分析・検証）の結果 緊急に改定を実施する必要はないと判断し、2014年度の改定は見送った。
	４．その他 指針（第４版）本編、対策編改定、並びに新たに策定される手引書を踏まえ改定方針等について検討中。

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** 定期的な改善、指針改定を受け実施。
	２．継続的改善（分析・検証）のプロセス 2012年11月より国土交通省において実施。
	３．継続的改善（分析・検証）の結果 緊急に改定を実施する必要はないと判断し、2014年度の改定は見送った。
	４．その他 指針（第４版）本編、対策編改定、並びに新に策定される手引書を踏まえ改定方針等について検討中。

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** 定期的な改善、指針改定を受け実施。
	２．継続的改善（分析・検証）のプロセス 2012年11月より重要インフラ関係事業者、国土交通省において実施。
	３．継続的改善（分析・検証）の結果 緊急に改定を実施する必要はないと判断し、2014年度の改定は見送った。
	４．その他

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、その他（電力システムのサイバーセキュリティ対策に関する提言事項への対応）を受け実施。
	２．継続的改善（分析・検証）のプロセス 2014年6月より2014年12月にかけ実施。
	３．継続的改善（分析・検証）の結果 提言事項の内容がガイドラインの定義事項に包含されていることを確認。
	４．その他 各事業者の提言事項への対応を支援するためガイドラインの定義事項をベースに、取り組むべき具体的事項を各事業者に通知した。

安全基準等の継続的改善状況（ガス分野、自治分野）

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** 指針改定を受け実施。
	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 指針（第４版）改定後実作業を開始予定（2015年４月より）。

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	2010年11月
状況	**１．継続的改善（分析・検証）状況・理由** 指針改定、 情報セキュリティ対策の運用を通じた課題抽出、 ＩＴに係る環境変化の調査・分析結果を通じた課題抽出を受け実施。
	２．継続的改善（分析・検証）のプロセス 2014年2月より2015年3月にかけ実施中。
	３．継続的改善（分析・検証）の結果 －
	４．その他

（注）自治分野の「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」は、2015年３月27日に改定済。

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** 指針（第３版）改定を受け実施。
	２．継続的改善（分析・検証）のプロセス 2014年11月より2014年12月にかけ実施。
	３．継続的改善（分析・検証）の結果 現在のガイドラインの改定は不要と判断。
	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** 実施予定なし。 （2013年度指針改定を受け実施済）
	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 指針（第４版）改訂を受け実施予定。

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** 定期的な改善、指針改訂を受け実施。
	２．継続的改善（分析・検証）のプロセス 2012年11月より改定方針等について検討を実施。
	３．継続的改善（分析・検証）の結果 緊急に改定を実施する必要はないと判断し、2014年度の改定は見送った。
	４．その他 指針（第４版）本編、対策編改定、並びに新に策定される手引書を踏まえ改定方針等について検討中。

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（仮称）
発行主体	石油化学工業協会
最新改定年月	策定中
状況	**１．継続的改善（分析・検証）の状況・理由** －
	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 新規重要インフラ分野 2014年度末安全基準等の策定を予定。

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** －
	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 新規重要インフラ分野

名称	石油分野における安全基準等（作成中）
発行主体	石油連盟
最新改定年月	策定中
状況	**１．継続的改善（分析・検証）の状況・理由** －
	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 新規重要インフラ分野 2014年度末安全基準等の策定を予定。

（参考）調査対象とした安全基準等一覧

分野		調査対象とする安全基準等の名称
情報通信	電気通信	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） 情報通信ネットワーク安全・信頼性基準 電気通信分野における情報セキュリティ確保に係る安全基準（第２版）
	ケーブル	ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン
	放送	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
金融		金融機関等におけるセキュリティポリシー策定のための手引書 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空	航空運送	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン（第３版）
	航空管制	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン（第３版）
鉄道		鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第２版）
電力		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
ガス		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
政府・行政		地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		医療情報システムの安全管理に関するガイドライン第4.2版
水道		水道分野における情報セキュリティガイドライン
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン（第２版）
化学(新規)		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（仮称）（作成中）
クレジット(新規)		クレジットCEPTOARにおける情報セキュリティガイドライン
石油(新規)		石油分野における安全基準等（作成中）

別添４－３　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１回会合（平成27年３月26日）資料６（2014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　：　2014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　：　2014年 7月～2014年11月

とりまとめ　：　2014年12月～2015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」策定にあたっての指針（第3版）および対策編

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３，３９１事業者等に、その回答は３，２２８事業者等から（回収率：95.2% 前年度比：+1.1%）

重要インフラ分野		活用する独自調査				浸透状況等調査		
		活用	名称	調査基準日	調査周期	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）
情報通信	電気通信	無	－－－	－－－	－	電気通信事業者（一部抽出）	97 (76)	73 (20)
	ケーブルテレビ	無	－－－	－－－	－	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	237 (241)	237 (221)
	放送	無	－－－	－－－	－	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		有	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	3月31日	1年毎	銀行等、証券会社、生命保険会社、損害保険会社	855 (892)	737 (796)
航空	航空運送	無	－－－	－－－	－	航空運送事業者	2 (2)	2 (2)
	航空管制	無	－－－	－－－	－	官庁	2 (1)	2 (1)
鉄道		無	－－－	－－－	－	ＪＲ、大手民鉄	22 (22)	22 (22)
電力		無	－－－	－－－	－	一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)
ガス		無	－－－	－－－	－	大手ガス事業者	12 (10)	12 (10)
政府・行政サービス		有	地方自治情報管理概要 －電子自治体の推進状況－	4月1日	1年毎	地方公共団体	1,789 (1,789)	1,789 (1,789)
医療		無	－－－	－－－	－	病院情報システムを導入する病院	60 (50)	53 (38)
水道		無	－－－	－－－	－	給水人口30万人以上の水道事業者、水道用水供給事業者	88 (45)	88 (45)
物流		無	－－－	－－－	－	物流事業者、業界団体（一部抽出）	21 (22)	7 (10)
全分野合計		－	－－－	－－－	－	－－－	**３，３９１ (3,356)**	**３，２２８ (3,160)**

調査結果の総括

(1) 総括に当たっての前提

今回の調査実施期間（2014年７月～11月）は、第３次行動計画策定（2014.5.19）の直後であり、また適用する指針は第２次行動計画に基づく第３版である。

このことから今回の調査結果は、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と位置付けられるとともに、今後の改善状況を測るための基準となるものである。

(2) 調査結果の概要

①PDCAサイクルに沿った継続的な対策

- ✓ 「初期対応」（PDCAのうちP（規定、体制、構築）の一部が該当）は概ね実施されている（ほぼ８割超）。
- ✓ 「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））の実施率はほぼ３割以下に留まる。

②経営層の在り方

- ✓ 「重点化対策の合意」は約８割で経営層が関与している一方、「運用状況の把握」では約５割に留まる。
- ✓ 経営資源の継続的な確保に関連して、「人員不足による対策の遅れ」（往訪調査でも同様の意見あり。）、「IT人材育成のための支援」や「対策費用補助の制度化」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

- ✓ 「企業体力に応じた評価指標や水準別の対策の提示」、「対策費用が利益、資産へ与える影響に関する指標の提示」等を国の支援として求める意見があった。

④情報共有体制

- ✓ 「重要インフラ事業者間でのリスク情報の共有」（往訪調査でも同様の意見あり。）、「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・啓発に役立つ資料の作成やセミナーの開催を求める意見があった。

(3) 課題

◆ 第３次行動計画の策定に際して第２次行動計画における改善点として抽出した項目が、今回の調査結果においても今後改善すべき課題であることを改めて確認することができた。具体的には以下のとおり。

①PDCAサイクルに沿った継続的な対策の改善

- ✓ PDCAサイクルに沿った継続的な対策の改善に関しては、「初期対応」の実施状況には向上の余地があり、「継続的改善」については実施の定着が課題と認められる。

②経営層の関与の強化

- ✓ 経営層においては、対策の必要性への認知はあるものの、予算・体制・人材等の経営資源の継続的な確保や運用状況の理解・把握には認知度の向上が課題と認められる。
  また、予算・人材等において国の支援を求める声があるが、自らの責任における実施は第３次行動計画が期待するところであり、自助・共助・公助の精神も踏まえつつ、国がどの程度まで支援を行うべきかについては今後の課題として慎重な検討が必要と考えられる。

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

- ✓ 事業者等による自らの責任における実施状況に関しては、新設する指針_手引書が例示する優先順位付けに基づき、情報セキュリティ対策がどの程度進展するかについて今後の調査が必要と考えられる。

④情報共有体制の推進

- ✓ 情報共有体制の推進に関しては、適切に運営できているかについて調査の必要性が認められる。

⑤広報公聴活動の強化

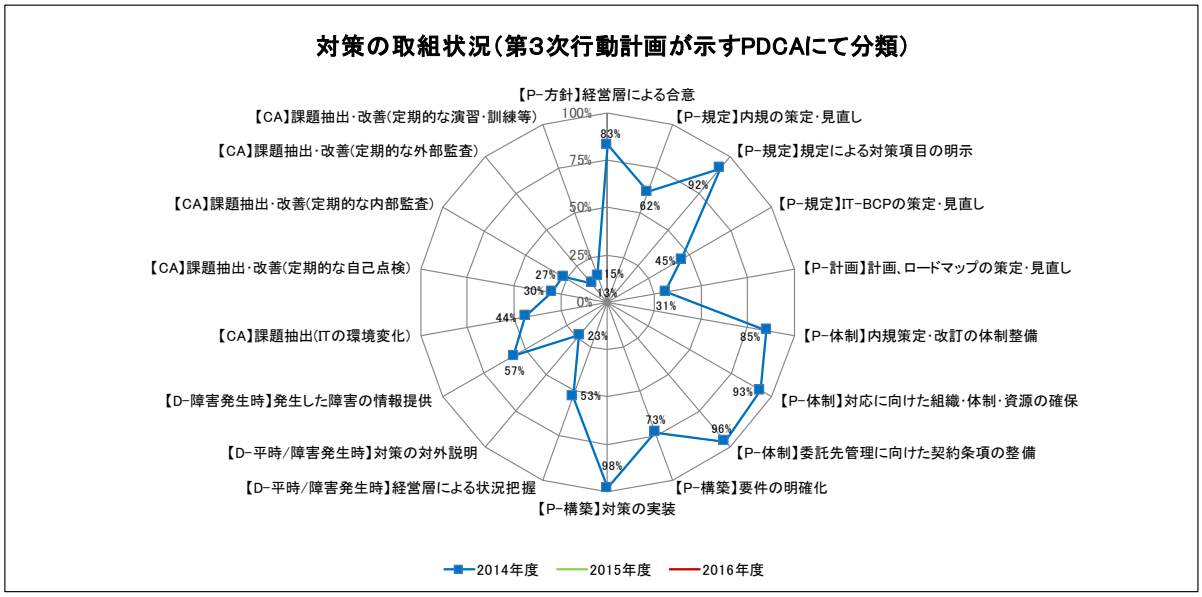
- ✓ 防護基盤の強化（広報公聴活動）に関しては、第３次行動計画や改訂後の指針に関し、周知・啓発を進める必要が認められる。

(4) 今後の対応

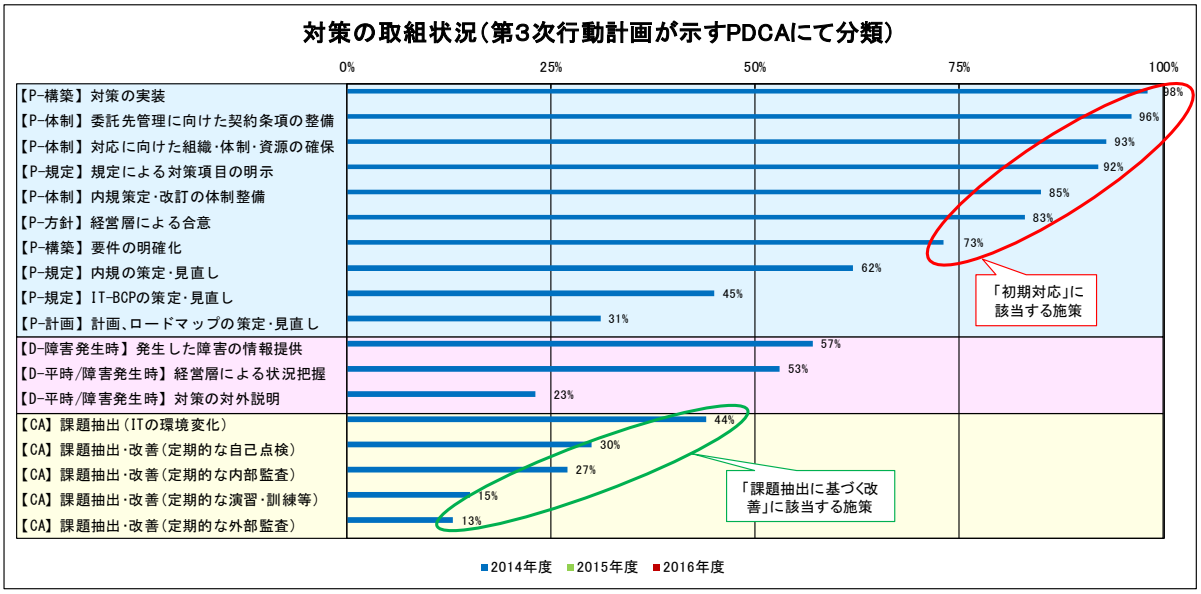
- ✓ 第３次行動計画が目指す「重要インフラにおけるサービスの持続的な提供」に向け、「情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するもの」との考えに基づき、「経営層の在り方」の浸透を中心に情報セキュリティ対策の継続的改善が行われるよう、取り組んでいく必要がある。
- ✓ 具体的には、本調査及びこれを補う往訪調査、分野横断的演習、NISCが活動を支援するセプターカウンシル等、重要インフラ事業者等との意見交換の場等を通じて、行動計画や指針の目的や考え方、各施策の成果を説明し浸透を図るとともに、国の支援に対する各事業者等からの要望等を把握する取組を、より充実させることとしたい。

調査結果：主要な基礎データ(1/2)

(1) PDCAに沿った情報セキュリティ対策の取組（その１：対策毎の実施状況）

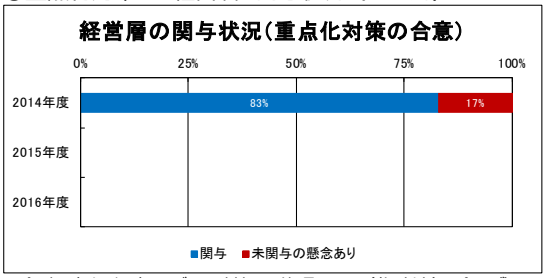


(1) PDCAに沿った情報セキュリティ対策の取組（その２：PDCA別の取組状況（実施率順に再配置））



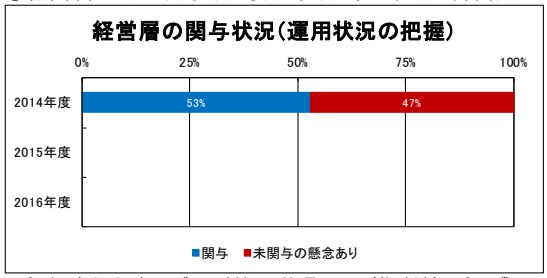
(2) 経営層の関与状況

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え可能項目なし（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）

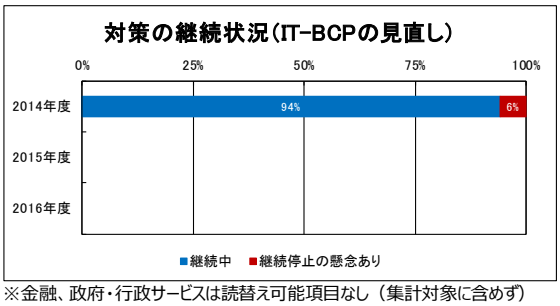


※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

調査結果：主要な基礎データ(2/2)

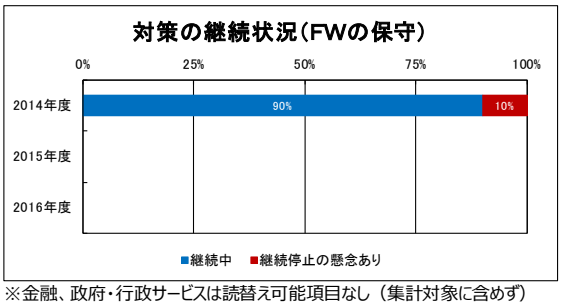
(3) 対策の継続状況

①IT-BCP策定、見直しの継続状況（P-規定）



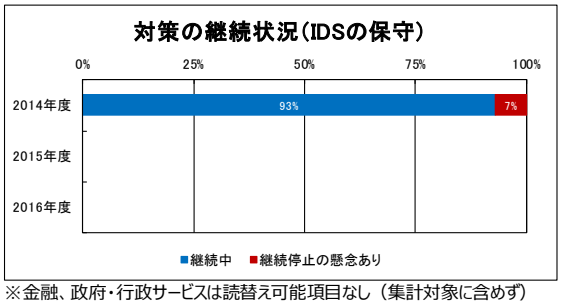
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

②ファイアウォールの保守継続状況（P-構築）



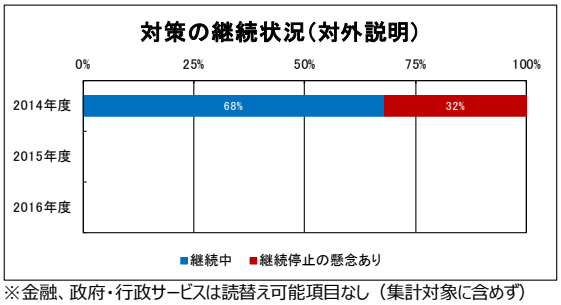
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

③侵入検知システムの保守継続状況（P-構築）



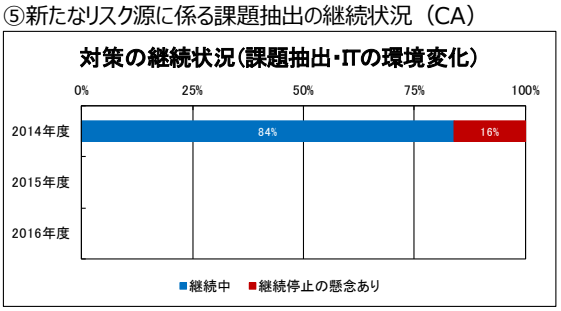
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

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）



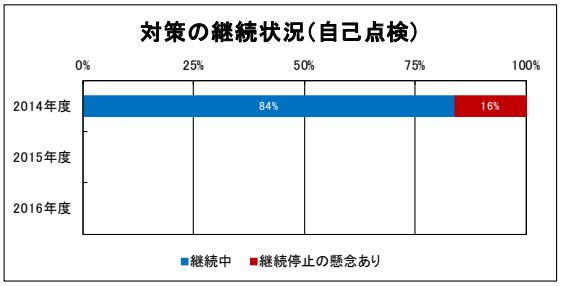
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑤新たなリスク源に係る課題抽出の継続状況（CA）



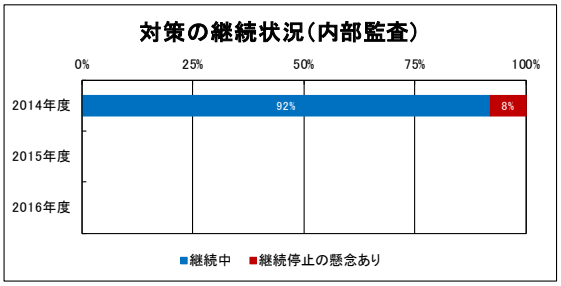
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑥自己点検による課題抽出・改善の継続状況（CA）



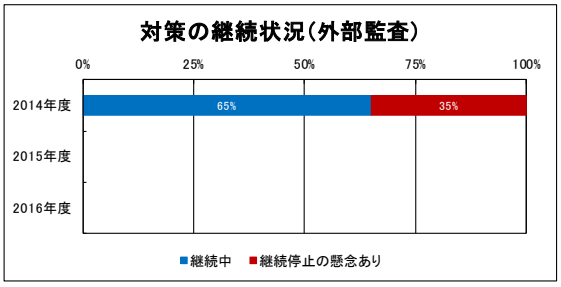
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑦内部監査による課題抽出・改善の継続状況（CA）



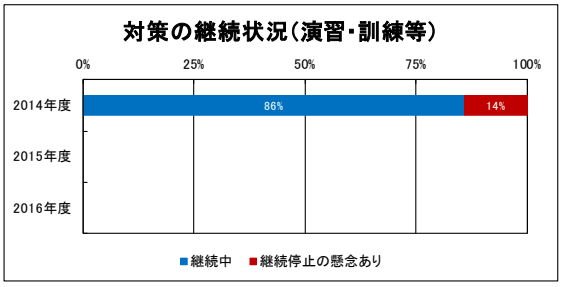
※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑧外部監査による課題抽出・改善の継続状況（CA）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

⑨演習・訓練等による課題抽出・改善の継続状況（CA）



※金融、政府・行政サービスは読替え可能項目なし（集計対象に含めず）

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（本編及び対策編）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）

指針の本編及び対策編の双方を認知している事業者は6割強。2割強は双方とも認知していない状況。

（年度）	2014	2015	2016
両方とも知っている	63%	－	－
本編のみ知っている	13%	－	－
対策編のみ知っている	1%	－	－
両方とも知らない	23%	－	－

(b)　指針（本編及び対策編）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）

指針を認知した契機は、NISC、所管省庁、業界団体が同程度。この他、web検索が契機との回答も多い。

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

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）

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

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

(b)　内規における対策の規定状況（複数回答）

情報の取扱い制限、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%	－	－
情報システムの格付け	39%	－	－
情報の格付け	49%	－	－
情報の取扱制限	89%	－	－
ソフトウェアの導入制限	74%	－	－
不審メールへの対処	65%	－	－
可搬媒体の利用制限	77%	－	－
リモートアクセスの利用制限	55%	－	－
スマートデバイスの利用ルール	40%	－	－
外部委託先に求めるｾｷｭﾘﾃｨ対応	49%	－	－
内規違反に対する罰則規定	44%	－	－
上記はいずれも未策定	2%	－	－

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3割強、それ以外の体制が関わる割合は4割弱。
内規が未策定の事業者も15%存在。

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

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・資源確保については、9割強の事業者が担当者（兼任を含む）を割当。
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	63%	－	－
専門部署の設置	31%	－	－
担当者（兼任を含む）の割当て	91%	－	－
人材育成、教育	65%	－	－
上記はいずれも未対応	4%	－	－

※(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）

(1)③(b)で内規の規定割合が相対的に低い、リモートアクセスの利用制限、スマートデバイスの利用ルールについては、教育についても他テーマより実施割合が低い。

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

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）

65%程度の事業者が対策の計画／ロードマップの策定を行っていない。また、4割弱の事業者は、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%	－	－
策定のみ行っている	5%	－	－
現時点では行っていない	2%	－	－
策定中	13%	－	－
策定予定がある	11%	－	－
現時点では予定なし	38%	－	－

(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割以上の実施割合なのに対し、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割合は3～5割程度と、相対的に低い。

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

具体的なネットワークへの侵入防止対策としては、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割程度と、他の対策より相対的に高い。

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

ファイアウォールの適用範囲を見直していない理由としては、導入前と前提・要件が同じとの回答が最多。これに、対応優先順位が低いとの回答が続く。

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

侵入検知システムの検知条件をチューニングしていない理由としては、導入時から不都合がないとの回答が最多。これに、対応の優先順位が低いとの回答が続く。

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

※(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）

具体的な新たなリスク源への対応としては、標的型攻撃が最多。これに、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、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%	－	－
制御システムを狙ったマルウェア	57%	－	－
暗号の危殆化	34%	－	－
IPv6への移行	27%	－	－
プロトコルの脆弱性	40%	－	－
クラウドサービスのセキュリティ管理	51%	－	－
スマートデバイスのセキュリティ	61%	－	－
その他	14%	－	－

(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、報告対象としている割合は概ね1～2割の範囲。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%	－	－
パターンファイル更新状況	11%	－	－
不審メールへの対処状況	21%	－	－
可搬媒体の利用状況	16%	－	－
リモートアクセスの利用状況	8%	－	－
スマートデバイスの利用状況	10%	－	－
外部委託先のセキュリティ対応状況	20%	－	－
その他	21%	－	－
報告未実施	47%	－	－

※(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）

具体的な無許可ソフトウェア導入禁止対策の実施状況としては、マルウェア対策ソフトの使用が最多。これに、可搬媒体の利用制限、パターンファイル更新（1週間以内）、リモートアクセスの利用制限が続く。

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

③　要件の明確化

(a)　委託先との契約条項（複数回答）

ほとんどの契約で機密保持・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/演習への協力の項目を設けている割合は4割強。

（年度）	2014	2015	2016
責任分界点・サービスレベルの明確化	76%	－	－
機密保持・情報の目的外利用禁止	96%	－	－
委託管理責任者の設置	55%	－	－
委託元と同レベルの対策実施	41%	－	－
再委託の制限	75%	－	－
障害発生時の対応	64%	－	－
監査/訓練/演習への協力	43%	－	－
違約時の対処（損害賠償請求等）	75%	－	－
上記はいずれも未締結	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としては、事業者の7割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%	－	－
リスク源への対応要件	51%	－	－
上記はいずれも要件の未明確化	28%	－	－

※(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同程度の割合。

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

※(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）

想定する事業継続性を阻害するIT障害の原因としては、8割強の事業者が自然災害を挙げ、これにサイバー攻撃、構築・保守のミス、物理的破壊が続く。

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

事業継続計画は、55%程度の事業者が現在未策定の状況。

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

※(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は、認証機能、アクセス制限機能、権限管理機能のいずれも同程度の割合。

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

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）

重点化している情報セキュリティ対策としては、情報漏えい防止が8割以上と最も多く、これに事業継続性確保が続く。

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

※(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）

ITの環境変化に伴う新たなリスク源としては8割の事業者が標的型攻撃を挙げ、これに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、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）	80%	－	－
制御システムを狙ったマルウェア	61%	－	－
暗号の危殆化	33%	－	－
IPv6への移行	23%	－	－
プロトコルの脆弱性	32%	－	－
クラウドサービスのセキュリティ管理	58%	－	－
スマートデバイスのセキュリティ	69%	－	－
その他	7%	－	－

※(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ためとの回答が6割強で最多。

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

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現状実施している事業者は2割強である一方、予定していない事業者は6割弱で最多。

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

情報セキュリティ対策の対外説明を実施している事業者が用いる手段としては、webサイトが65%程度と最多。これに、その他の手段、有価証券報告書が続く。

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

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）

約6割の事業者が、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%	－	－
明示未済	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）

障害発生時の情報提供体制としては、サービスの利用者向けが8割強と最多。これに、所管省庁向け、業界窓口向けが続く。

（年度）	2014	2015	2016
サービスの利用者向け	86%	－	－
所管省庁向け	79%	－	－
業界窓口向け	58%	－	－
上記はいずれも体制なし	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現状実施している事業者は5割弱、実施予定なしの事業者は3割弱。

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

※(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）

課題抽出を実施している事業者の具体的な課題抽出対象のリスク源は標的型攻撃が8割強で最多。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%	－	－
制御システムを狙ったマルウェア	43%	－	－
暗号の危殆化	26%	－	－
IPv6への移行	17%	－	－
プロトコルの脆弱性	25%	－	－
クラウドサービスのセキュリティ管理	60%	－	－
スマートデバイスのセキュリティ	66%	－	－
その他	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%	－	－
１度以上/２年以内の点検にて課題抽出・改善を実施	2%	－	－
１度以上/２年超の点検にて課題抽出・改善を実施	19%	－	－
定期的な点検のみ実施	17%	－	－
不定期に実施の点検にて課題抽出・改善を実施	18%	－	－
不定期な点検のみ実施	8%	－	－
点検未実施	12%	－	－
点検実施予定あり	6%	－	－
点検実施予定なし	5%	－	－

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・改善の実施状況も同程度。
一方、5割の事業者は実施予定なしと回答。

（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%	－	－
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度以上/２年超の演習・訓練等にて課題抽出・改善を実施	1%	－	－
定期的な演習・訓練等のみ実施	1%	－	－
不定期に実施の演習・訓練等にて課題抽出・改善を実施	7%	－	－
不定期な演習・訓練等のみ実施	4%	－	－
現在演習・訓練等未実施	5%	－	－
演習・訓練等実施予定あり	18%	－	－
演習・訓練等実施予定なし	50%	－	－

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5割弱。定期的な内部監査に基づく課題抽出・改善の実施状況は35%程度。

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

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割強。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%。

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

調査結果詳細：自由意見

【経営層の在り方に関する意見】

- 人員が少なく、なかなか対策に手が回らない。（往訪調査でも同様の意見あり。）
- 小規模の事業体では、セキュリティ対策の必要性を理解していても、対策の策定や見直しには人的時間的に制約があり、実施できない状況がある。
- ＩＴ人材育成のための支援を重視して頂きたい。
- 一企業の立場で情報セキュリティ対策を講じようとすると、それなりの費用がかかる。これに対して一定額の補助を国として制度化していただけるなら、もっと良い対策を講じることができると考える。

【事業者等による自らの責任における実施状況に関する意見】

- 企業の体力に応じた評価指標などがより充実すると、効果的なセキュリティ対策ができると考える。
- 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やすいのではないか。
- セキュリティ対策（現状では主にサイバー攻撃対策）はどれだけ強化しても利益を生み出すわけではなく、一般的にその重要性は理解されても、必要性は軽視されがちであり、特に費用面ではある意味軽減を図りやすい一面がある。こういった問題点を広くかつ分かりやすく知らしめる観点からも、対策を怠ることによる影響額（被害額＋投資コスト）がどれだけの利益、資産等の損失に至るかの指標的なものを示してほしい。

【情報共有体制の推進に関する意見】

- 現実のリスクの公開と情報共有が必要。セキュリティベンダー間では実現しているが、ユーザー間ではリスクの共有がなされていない。
- 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対応をお願いしたい。
- 引き続きNISCメール等による情報提供をお願いする。
- 国からの脆弱性情報等が届いていない。（往訪調査時の意見）

【防護基盤の強化（広報公聴活動）に関する意見】

- 指針の重要部分を抜粋した概要資料があれば、周知・理解に役立つと考える。
- セミナー等を開いていただければ内容がより理解できると思う。
- 公的機関での広報活動をもっと積極的に行ってほしい。

【その他の意見】

- 本編、対策編の策定は大変ありがたい。欲を言えば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と思う。
- ＩＴ関連の危険性を学校教育の場で教えておいた方がよいのではないか。
- 今回の質問について、社内セキュリティの観点から答えにくい点があった。
- 本アンケートについて、用語の意味合いや問いの位置付けが難解であった。
- 情報セキュリティの相談窓口の設置をお願いしたい。
- 現在、コンピュータウィルスの対策はソフトウェア業界任せであり、真の脅威に積極的に取り組んでいるとは言い難いと思う。真の脅威を未然に防ぐために国の研究機関が重要なコンピュータウィルス対策を行うべきではないか。
- ISMS認証やプライバシーマークの取得が、継続的なセキュリティ対策の改善につながっている。（往訪調査時の意見）
- 自社のセキュリティ対策の水準が、どの程度なのかを知りたい。（往訪調査時の意見）
- 同業他社との意見交換の場を設け、自社のセキュリティ対策の水準や最新動向等を把握するように努めている。（往訪調査時の意見）

（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)　本編及び対策編をご存知ですか。[(1)①(a)]
(2)　本編及び対策編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４－４　情報共有件数

重要インフラ専門調査会第２回会合（平成27年７月23日）参考資料２（2014年度の情報連絡等について）より

「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年度～2013年度分）及び「重要インフラの情報セキュリティ対策に係る第３次行動計画」（以下「行動計画」という。）（2014年度分）に基づき内閣官房（NISC）と重要インフラ事業者等及び関係省庁・関係機関との間で行われた情報共有の件数は次のとおりである。

年度	2009	2010	2011	2012	2013	2014
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
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
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

重要インフラ事業者等から内閣官房（NISC）への情報連絡件数（2014年度は**124**件）の事象※別の内訳は次のとおりである。

※行動計画の別紙３によるもの。なお、行動計画の策定の際、分類方法を大きく見直したため、2013年度以前との比較はできない。

事象の類型		事象の例	2014年度
未発生の事象		予兆・ヒヤリハット	９件
発生した事象	機密性を脅かす事象	情報の漏えい	９件
	完全性を脅かす事象	情報の破壊	14件
	可用性を脅かす事象	システム等の利用困難	38件
	上記につながる事象	マルウェア等の感染	27件
		不正コード等の実行	３件
		システム等への侵入	12件
		その他	12件

（単一選択式）

同様に、原因※別の内訳は次のとおりである。

※行動計画の別紙３によるもの。なお、行動計画の策定の際、分類方法を大きく見直したため、2013年度以前との比較はできない。

原因の類型	原　因	2014年度
意図的な原因		55件
	不審メール等の受信	６件
	ユーザＩＤ等の偽り	７件
	DoS攻撃等の大量アクセス	25件
	情報の不正取得	13件
	内部不正	０件
	適切なシステム等運用の未実施	４件
偶発的な原因		31件
	ユーザの操作ミス	０件
	ユーザの管理ミス	２件
	不審なファイルの実行	１件
	不審なサイトの閲覧	１件
	外部委託先の管理ミス	10件
	機器等の故障	７件
	システムの脆弱性	９件
	他分野の障害からの波及	１件
環境的な原因	災害や疾病	０件
その他の原因		52件
	その他	９件
	不明	43件

（重複選択式）

別添４－５　セプター概要

セプターカウンシル総会第７回会合（平成27年４月23日）公表資料、重要インフラ専門調査会第１回会合（平成27年３月26日）資料７（2014年度 セプターの活動状況の把握について）等より

セプター及びセプターカウンシルの概要

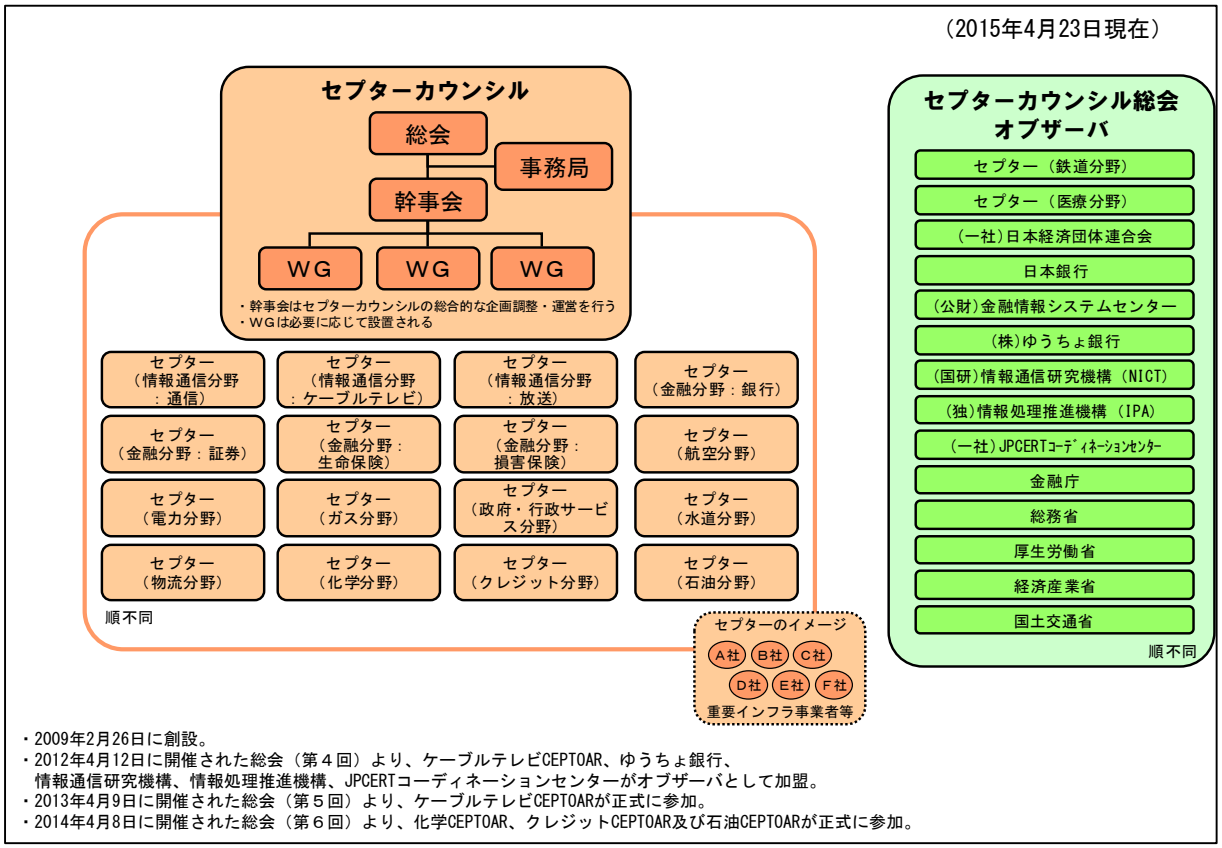
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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



・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

2015年3月末現在

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	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTAOR	電力CEPTOAR	GASCEPTOAR	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）	２６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）	310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・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）	1,487社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	254社７機関 （証券会社、取引所等証券関係機関）	42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（1,356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）	８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）	15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	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	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４－６　分野横断的演習

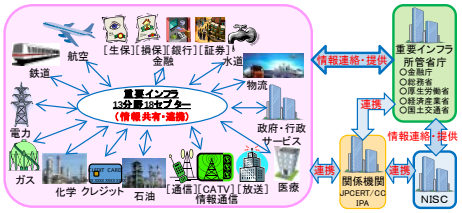
重要インフラ専門調査会第１回会合（平成27年３月26日）資料８（2014年度 分野横断的演習について）より

2014 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>
日　時：２０１４年１１月７日（金）１４：００～１７：００
内　容：①NISC各施策の概要説明（第３次行動計画・「安全基準等」策定指針・情報共有体制）
②分野横断的演習の事前説明

規程類の事前確認、個別検証課題の確認・調整

<演習当日>
日　時：２０１４年１２月８日（月）１２：１５～１８：１５
場　所：東京会場、大阪会場、自職場
参 加 者：９４組織３４８名（うち、１０組織３２名が大阪会場、１５組織５９名が自職場より参加。初参加事業者等　３６組織）
【重要インフラ事業者等：１３分野　合計７０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】



演習内容：２部構成で実施（それぞれの検証課題に対する参加事業者等の理解を深める効果を狙ったもの）
○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。
○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。

演習を通じた内規・体制等の課題抽出

<意見交換会>
日　時：２０１５年２月５日（木）１４：００～１６：００
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分野横断的演習の中間報告

他事業者等との情報共有を通じた改善の促進

2014 年度分野横断的演習　報告概要

取組に当たって

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

2014年度の取組と今後の取組方針

2014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・中小規模事業者等の参加
- ✓ 演習シナリオを通じた情報共有体制の実効性の検証

取組実績等を通じて得た気付き等
- ✓ 演習当日後の改善実施に向けた訴求不足
- ✓ 大阪会場新設への高評価
- ✓ 情報共有体制の誤認を思わせる意見の存在

今後の取組の観点

基本方針・取組の方向性を踏襲しつつ、以下観点の改善についても検討

演習運営
- ✓ 事業者等の内規の策定・見直しや対策の実施・改善に資する運営の見直し・追加に係る検討
- ✓ 参加対象の裾野拡大に資する会場新設・既存会場等の改善に係る検討

他施策との連携
- ✓ 情報共有体制の実効性の向上に係る検討・運用見直しへの支援

第３次行動計画に基づく分野横断的演習の基本方針

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

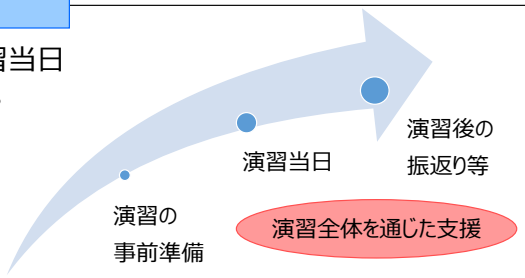
○ 重要インフラ全体の防護能力の維持・向上を図るため、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指す。

○ 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

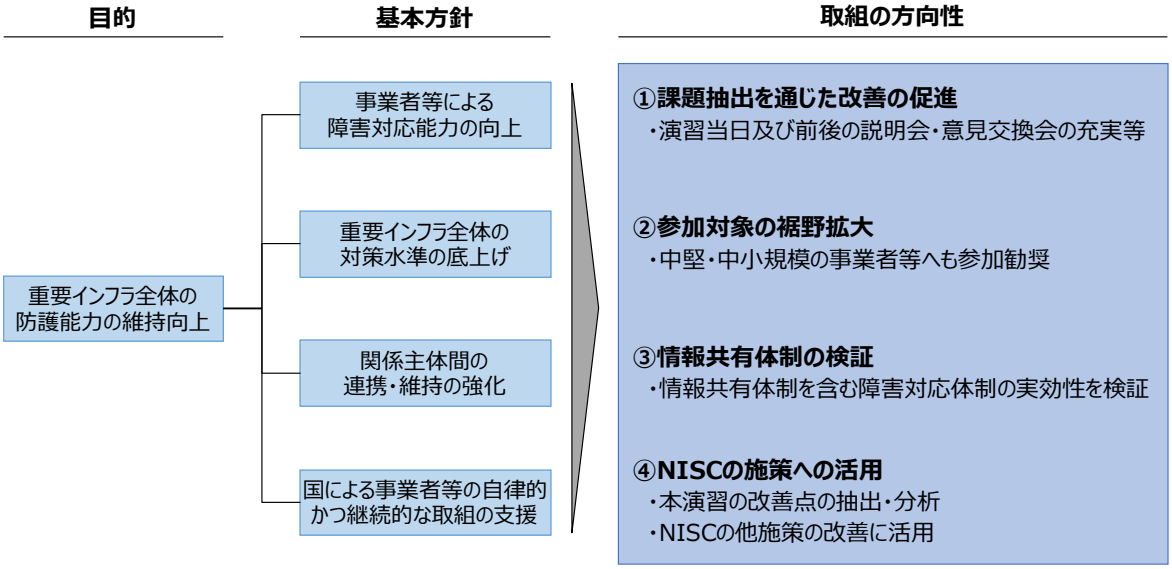
○ 事業者等による実効性確認の機会としての演習当日に加え、事前準備及び事後の振り返りにて構成。

- 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する。



分野横断的演習の取組の方向性

NISCは方向性①・②・③に基づいて実施した今年度の取組に対して、方向性④の観点から振返りを行う。



2014 年度の取組実績(1/2)

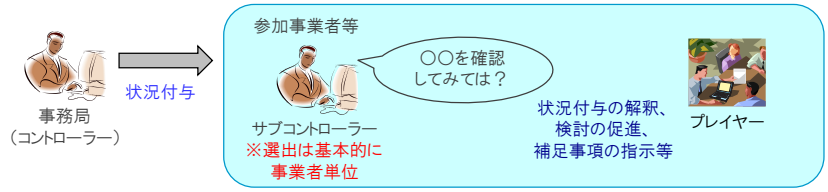
取組実績１：演習当日及び前後の説明会･意見交換会等の充実

事前準備

- 事前説明会にて以下を実施
  - ✓ 第３次行動計画、「安全基準等」策定指針、情報共有体制について説明を実施
  - ✓ 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
- 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

- 指針対策編のIT-BCPに関する項目を検証課題に設定
- 演習当日の時間配分の見直し、振り返りの時間を確保
- 自己評価の促進やサブシナリオの作成等を目的に、サブコントローラーを導入



事後の振返り

- 分野間の情報共有を促進するため、意見交換会でグループディスカッションを実施

取組実績２：中堅･中小規模事業者等の参加

- 参加形態の多様化
  - ✓ 大阪会場の新設　（首都圏以外の事業者等の参加促進）
  - ✓ より実践的で効果の高い演習環境を実現する自職場参加を拡充（演習経験者へ推奨）
- セプター事務局等に対して、演習の基本方針を説明
  - ✓ セプター事務局等を通じた中堅･中小規模の事業者等への参加勧奨
  - ✓ 参加者層を考慮したシナリオ設定
    （高度なシナリオを希望する場合はサブシナリオを事業者等にて作成）
- 参加勧奨用の映像を作成
- 参加実績（過去３年間）は右記のとおり

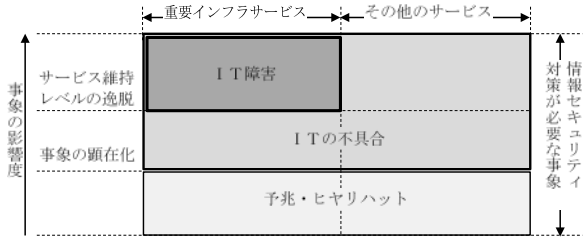
	２０１２年度	２０１３年度	２０１４年度
参加機関	42組織 (21事業者等)	61組織 (38事業者等)	94組織 (70事業者等)
参加者	148名	212名	348名
（大阪会場）	–	–	10組織32名
（自職場参加）	3組織15名	3組織10名	15組織59名

※今年度、本演習に初めて参加した事業者等は36組織

2014 年度の取組実績(2/2)

取組実績３：演習シナリオを通じた情報共有体制の実効性の検証

■ IT-BCP等に基づく対応に加え、官民間の情報共有体制を検証課題とした演習シナリオを作成
　✓ 情報共有の対象範囲を従来のＩＴ障害からＩＴの不具合や予兆・ヒヤリハットに拡大したことの実効性の検証



情報共有の対象範囲（第３次行動計画 P45）

（参考）検証課題と事業者等が得た気付き

＜ＩＴ障害等における対外的な情報共有＞
○ 官民間の情報共有体制の枠組みについて、再確認が必要。
○ 所管省庁へ情報連絡する基準が不明確。
○ 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・ルールの整備が必要。

＜ＩＴ障害等の対応における内部的な判断や意思決定＞
○ BCP・IT-BCP等の発動条件が地震等を前提としており、情報セキュリティインシデントの発生を前提としていない。
○ BCP・IT-BCP等のドキュメント作成後の運用（経営層・組織内への定着、定期的な見直し等）について改善が必要。これに加え、判断力等の人的スキル向上が課題。
○ これらの課題解決には、演習・訓練が重要。

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) 取組実績等を通じて得られた気付き等

■ アンケート等による評価
　✓ 本演習を有意義と評価した参加事業者等の割合は100%。
　✓ 自組織で演習を行うにあたって本演習が参考になったという意見の存在。
　　（自組織でＩＴ障害に関する演習・訓練を実施していると回答した参加事業者等は約６割。）
　✓ 大阪会場の新設については、演習に参加しやすくなったという意見が多く、好評価。

■ 改善点
　✓ サブコントローラーの導入により事業者等の自律的な改善に資する演習を実現できたものの、今回選出した事業者等は全体の約４割。
　✓ 演習当日後の改善実施（内規の整備・見直し等）に向けた訴求不足。
　✓ 官民間の情報共有体制について、誤認を思わせる意見の存在。

(2) 今後の取組の観点

基本方針・取組の方向性を踏襲しつつ、以下の観点からの改善についても検討

■ 演習運営
　✓ 事業者等の内規の策定・見直しや対策の実施・改善に資する運営の見直し・追加に係る検討
　✓ 参加対象の裾野拡大に資する会場新設・既存会場等の改善に係る検討

■ 他施策との連携
　✓ 情報共有体制の実効性の向上に係る検討・運用見直しへの支援

別添４－６　セプター訓練

重要インフラ専門調査会第１回会合（平成27年３月26日）資料９（2014年度 セプター訓練について）より

セプター訓練（第９回）のまとめ

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、証券）、航空分野、鉄道分野、電力分野、ガス分野、医療分野、水道分野、物流分野、クレジット分野の計１４セプター
参加事業者等（参加事業者等数：1,644団体）（訓練参加の事業者等は各セプターにおいて選定）
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

2014年８月から10月まで（実施日時はセプターごとに決定）

④実施内容

(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。
（セプターの希望に応じ実施方法のカスタマイズ（時間抜き打ち、模擬情報の具体化）を実施。）
(3)訓練実施後、得られた気付き等を調査票（アンケート）に記載し提出。

セプター訓練（第９回）のアンケート結果（1/3）

１．情報共有体制の整備・維持に関して（１／２）

(1) 情報伝達を確実に実施するための工夫（連絡先の整備・維持）に関する気付き等

【セプター独自の取組・前回の訓練からの改善点】

○年1回は、登録されている連絡先へ**メールの到達確認を実施し、連絡先を整備している**。

○連絡先未届けの事業者がないことを事前に確認し、また、人事異動等に伴う**変更届出を行っていない事業者が存在した際には、変更手続き等の依頼**を実施している。

○メールが不達にならないように、**日頃からメールアドレスの整備**に努めている。

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○**人事異動時等に連絡先の変更を速やかに申請**するよう、参加事業者への**指導を強化した**。

○**定期的に実施することで、社内連絡先を最新に維持**できるメリットがある。

○「担当者や**連絡先の変更に伴う変更手続き**（変更届出書の提出）の周知徹底」の**注意喚起**を実施した。

分野・事業者によって、連絡先を更新するタイミング（①年１回の訓練時、②人事異動時、③担当者・連絡先変更時）が違っている。

情報伝達を確実に実施するためには、連絡先の更新は担当者・連絡先が変更したタイミングにより、速やかに実施したほうが望ましいことから、そのための各分野・事業者内における仕組み・ルール作りが検討されることを期待します。

セプター訓練（第９回）のアンケート結果（2/3）

１．情報共有体制の整備・維持に関して（２／２）

(2) 情報伝達を確実に実施するための工夫（連携ルートの複線化・代替手段の考慮）に関する気付き等

【セプター独自の取組・前回の訓練からの改善点】

○情報連携ルートの更なる複線化を目的に、要望がある事業者については、**通常の社内メールアドレスに加え、携帯のメールアドレス等を複数登録**できるようにした。

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○情報提供に使用しているファイル配信ツールの不具合発生を踏まえ、今後、**情報提供ルート（手段）の代替手段を明確化**するとともに、当該手段についてセプター構成員に十分な周知を行う。

○**担当者不在時等に備えた情報受信者の複数登録**（担当者の追加や関連部署への転送等）の対応等の注意喚起を実施した。

情報伝達を確実に実施するためには、担当者不在時のための情報連携ルートの複線化は重要であるとともに、情報伝達手段としても、不測の事態に陥った場合の手段の代替を考慮したほうが望ましいことから、未整備の分野・事業者においては検討されることを期待します。

(3) 情報伝達を迅速に実施するための工夫（メーリングリスト等の活用）に関する気付き等

【セプター独自の取組・前回の訓練からの改善点】

○セキュリティ関係者の情報共有を迅速に行うため、**メーリングリストを活用**している。

○メールでの情報発信をスムーズに行うために、**一斉送信用のアドレスリストを用意**している。

○NISC等から提供される脅威情報等を**情報共有する掲示板をイントラネットに設置**し、受信した情報に対し対応すべき内容を追記し、**当該掲示板を通じて社内関係者へ情報提供**を実施している。

情報伝達を迅速に実施するためには、メーリングリストや掲示板などの情報伝達システムを活用することは有効であることから、構成員の多い分野・事業者においては検討されることを期待します。

２．より実践に近い状況の訓練の実施に関して

(1) 突発的な事態への対応の訓練（日時の抜き打ち）に関する気付き等

【セプター独自の取組・前回の訓練からの改善点】

○各事業者に対し、**実施する期間（数日間）のみを伝え、具体的な訓練日時を通知せず**実施している。

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○**訓練時間等を決めずに行うことで問題点などが明らかになるのではないか。**

(2) 事業者を起点とした事態への対応の訓練に関する気付き等

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○事前の周知は行っているが、メールは受信していても受信確認の連絡が来なかった例が散見された。**事業者からの情報発信に慣れてもらうため**、事業者が起点となるような訓練ができないか。

(3) 模擬情報の具体的な記載に関する気付き等

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○模擬情報を具体的内容とすることで、**自社内での訓練に展開しやすくなる**のではないか。

○模擬情報について、具体的な内容を記載していただけると、その**情報に即した社内対応ができ、より現実味のある訓練になる**ので、次回の訓練では改善していただきたい。

より実践に近い訓練を実施することにより、情報共有体制の新たな気付きを得ることは重要である。

各分野・事業者の実情を踏まえつつ、実践的な訓練内容を取り入れるための検討が行われ、段階的に実態に即した情報共有訓練が実施されることを期待します。

セプター訓練（第９回）のアンケート結果（3/3）

３．その他

緊急性と秘匿情報との関係に関する気付き等

【今回の訓練を踏まえた今後の改善点、意見、感想等】

○訓練において、情報連携を添付文書ではなく、メール本文に記載する方法でも連携いただくなど、**緊急度が高い情報は、メール本文による情報連携が有効であるので検討いただきたい**。

○情報セキュリティ上、パスワード付きのメール送信が原則であろうが、**緊急かつ広範に情報伝達が必要な場合、情報の秘匿性確保よりも容易に内容確認出来ることを優先**し、パスワードを設定せずに情報提供を行っても良いのではないか。

«NISCコメント»

情報共有で取り扱われる情報は機微情報を含むことから、原則パスワードを付した電子メールにて情報提供を行う事により、外部への情報漏えいを防止することが必要である。

一方、機密性を確保することよりも緊急性を優先させるべき事態が発生した場合においては、原則によらず電話等の他の情報連絡手段を含め、最適な手法等により情報提供を実施することとしたい。

総括・今後の方向性と NISC からの要望

◆セプター訓練の総括

① 訓練の結果、**課題の抽出**ができたセプターや、**新たな気付き**を得たセプターもあり、**セプター訓練の有用性が改めて確認**された。

② 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。

◆今後のセプター訓練の方向性とNISCからの要望

今年度のセプター訓練の結果を踏まえ、**IT障害対応を念頭においたより実態に即した情報共有訓練**となるよう、次回のセプター訓練の実施前までに、**訓練方法の多様化や実施形態の見直し（例：カスタマイズ項目の充実）等の所要の検討**を進めていく。

また、第３次行動計画において、NISCは「定期的及びセプターの求めに応じて機会を提供」することとしており、具体的な訓練内容を検討する際は、**各分野の情報共有体制等の諸事情を踏まえつつ、今回のセプター訓練で得られた気付き事項の反映の確認、かつ検証できるような効果的な訓練内容**となるよう、各セプターからも積極的な提案を期待する。

別添４－８　補完調査

重要インフラ専門調査会第１回会合（平成27年３月26日）資料10（2014年度 重要インフラにおける補完調査結果について）より

補完調査の目的・観点

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26年5月19日 情報セキュリティ政策会議決定）

調査の実施方法

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。

調査対象の選定

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　Webサイト（トップページ）の改ざん
事例２　会員制サービスの不正ログイン
事例３　端末へのマルウェア感染　※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１　Web サイト（トップページ）の改ざん（1/2）

【発生事象の概要】

- Webサイトに対する不正アクセスにより、トップページが改ざんされた。
- 閲覧すると、攻撃者の主義主張を表す画像が表示され、更に別のWebサイトに誘導される。
- Webサイトを一時閉鎖後、改ざん箇所の修正と他への影響有無確認を実施して復旧。

【背景】

- Webサーバは外部の共用サーバ（ホスティングサービス）を利用。
- Webサイト自体の運用は事業者の広報担当者（IT担当部署ではない）が実施。
  （Webサイトの構築は外部委託したが、日々の運用・保守は外部委託せずに広報担当者が実施。）

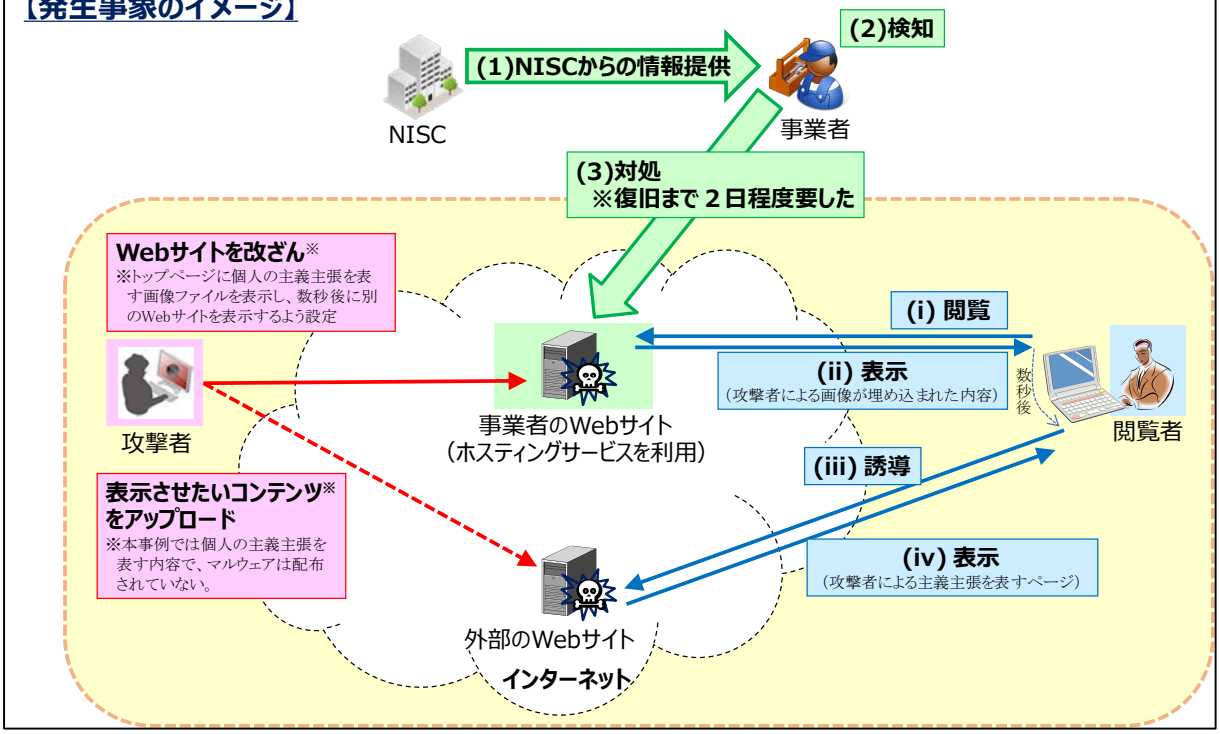
【検知】

- NISCからの所管省庁を通じた情報提供により、IT担当部署の担当者がWebサイトの改ざんを認知。

【対処】

- 検知が深夜であり、また、ホスティングサービスの業者の応対時間外だったため、IT担当部署の担当者判断により、翌朝から対処を行った。
- 広報担当者がWebサイトの一時閉鎖作業に着手したが、トップページのみではなく、Webサイト全体を閉鎖する方法が容易に判明せず、作業に時間を要した（約半日）。
- 危機管理の責任者の指示により、Webサイトの一時閉鎖について報道発表を閉鎖当日中に実施。
- 危機管理の責任者の指示により、費用発生の如何に関わらず早期復旧すべき方針が示され、Webサイト構築時の業者と協力して復旧作業（作業用に一時閉鎖を部分解除／改ざん箇所を修正）を実施。
- その後、トップページ以外の全ページを目視により検査・確認し、Webサイトを再公開。

【発生事象のイメージ】



事例１　Web サイト（トップページ）の改ざん（2/2）

【原因】

- ホスティングサービスの契約内容にログ採取が含まれておらず、改ざん原因は特定できなかった。
- なお、状況から推測される原因は次のとおり。
  - ✓ 使用していたCMS※について、数年間更新しておらず、脆弱性があるバージョンを使用していた。
    ※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。
  - ✓ Webサイトを更新するためのソフトウェア（FTPクライアント）に脆弱性があるバージョンを使用していた。（パスワードを保持する設定としていたが、パスワード漏えいの脆弱性があった。）
  - ✓ パスワード（FTPパスワード）を運用開始以来、一度も変更していなかった。

【再発防止策】

- FTPパスワードを変更（推測されにくいようランダムな文字列を使用。）。
- 使用しているソフトウェアについては、パッチ適用等の脆弱性対策を実施。
- 専門知識を持った外部業者への運用委託を含めた、Webサイトの全面更改を検討・計画。
- Webサイト更改に当たり、情報セキュリティ対策の検討などに外部専門家（コンサルティング会社）を活用。

【得られた気づき・教訓】

- 夜間・休日対応のため、組織内外との連絡ルール、連絡手段及び役割分担の整理が重要。
  （担当者自身がどこまで判断してよいかを明確にしておく必要。）
- ホスティングサービス等の外部サービス利用時は、夜間・休日を含めた対応体制や、ログの取得といった障害発生時の対応の可否について確認が必要。
  （事業者自身が提供するサービスに照らして、それが十分であるかを併せて確認する。）
- Webサイトの改ざんに備えた、閉鎖のための判断基準や操作手順の整備が必要。
  （マルウェアが埋め込まれていた場合、閲覧者へのマルウェア感染拡大を防止する必要。）
- 復旧・稼働を優先する重要な業務・システムを整理し、それを組織内に定着しておくことが重要。
  （時間外勤務や外部委託等の費用発生をしてでも迅速に対応すべきものを確認。）
- 環境変化や時間経過に応じ、適切な予算措置や人材確保により情報セキュリティ対策を継続的に実施していくことが必要。
  （Webサイトの構築時だけではなく、維持するためにも、専門知識を持つ人材や費用が必要であり、IT担当部署だけでなく、経営層を含めた共通認識とする必要。）
- 情報セキュリティ事象について、報道発表を行う基準やその判断者を事前に決めておくことが必要。
  （不特定多数に影響のある事象については、迅速かつ正確な情報発信が重要。）

事例２　会員制サービスの不正ログイン（1/2）

【発生事象の概要】

- 複数の会員制サービスのサーバに対し、大量のログイン試行が行われた。
- 一部のログイン試行が成功し、個人情報を含む会員情報が閲覧された。
- サービスを一時停止し、不正ログインされたアカウントの凍結や監視強化等を措置。

【背景】

- 攻撃を受けた事業者は会員制サービスを複数運用。
- 各会員制サービスは、各担当部署（IT担当部署ではない）が原則として管理。
- 会員制サービスのログイン状況の監視は、一定時間ごとのログ監視により実施。

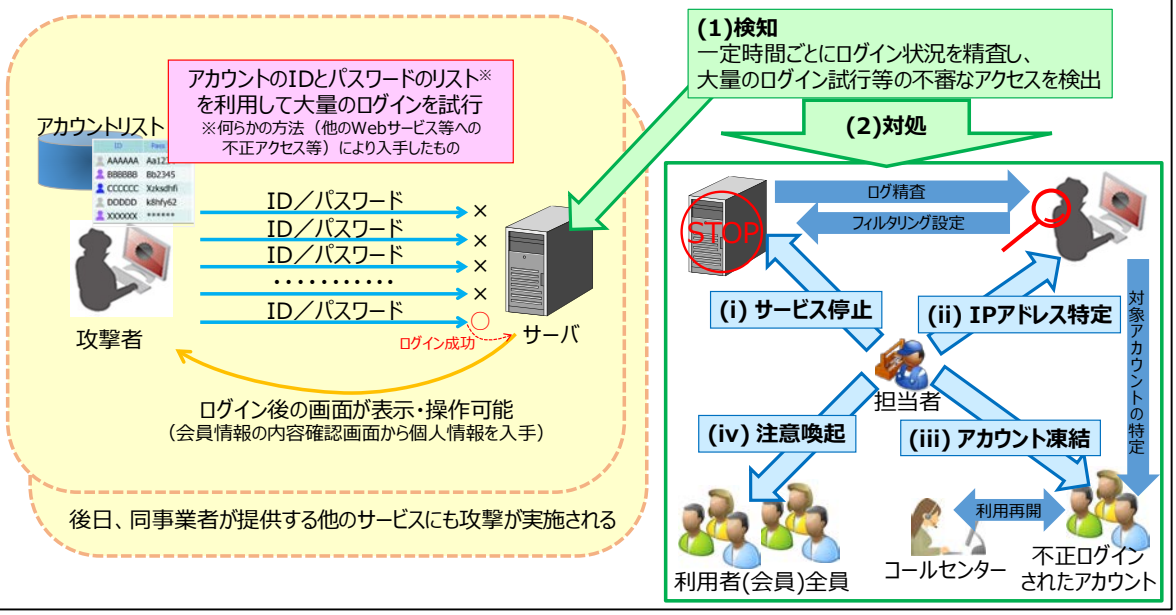
【検知】

- 短時間に大量のログイン試行が行われたことが、ログ監視により検出され、担当部署へ通知。
- その後も、大量のログイン試行が、同一サービスだけでなく、他のサービスにおいても行われたことを確認。
  （管理状況の異なる他のサービスの監視体制を強化する前にログイン試行を受けた。）

【対処】

- 会員制サービスを一時停止。深夜であり担当者が駆けつけるまでに数時間を要した。
  （その後、24時間対応を実施している別の部署に停止作業を移管することで改善。）
- 一時停止中に、不審なIPアドレスを特定。通信の遮断（フィルタリング）等を実施後、サービス再開。
- 不正ログインされたアカウントを凍結し、電子メールにて連絡。再開手続きはコールセンターにより実施。
- サービスの会員全員に対して、電子メールでパスワード管理に関する注意喚起を行った。

【発生事象のイメージ】



事例２　会員制サービスの不正ログイン（2/2）

【原因】

- 第三者によるアカウントリスト攻撃※と推定される

※アカウントリスト攻撃･･･IDとパスワードがセットになった「アカウントリスト」を元に不正ログインを試行する攻撃。アカウントリストは、何らかの方法（例：他のオンラインサービスへの不正アクセス）により事前に入手しておく。利用者がIDとパスワードをオンラインサービス間で使い回していると、攻撃が成功してしまう。

【再発防止策】

＜早期対策＞

- 大量アクセスに対する監視間隔の短縮による早期検知。　（例：日時→毎時、毎時→15分ごと）
- 大量ログイン試行の検知後、通信を遮断するまでのプロセスを自動化。

＜中長期対策＞

- ログイン画面に画像認証（CAPTCHA※）を追加。
  ※歪んだり崩れた文字列を表示させ、それを利用者に入力させることで、機械的な自動アクセスを防ぐ方法。
- ログイン後の画面や会員情報照会画面に個人情報を表示させず、閲覧・変更時は二重認証※を実施。
  ※本事例の場合においては、ID・パスワード以外に、個人情報の一部を認証項目として入力させることとしている。
- リスクベース認証※を実施。
  ※利用者のログイン環境（IPアドレス、使用パソコン、使用ブラウザ等）を総合的に分析し、普段と異なる環境からのアクセスと判断した場合に、追加的な認証を要求する方式。

【得られた気づき・教訓】

- 提供サービスのログを定期的に確認するとともに、異常となる閾値を決めておくことが重要。
  （確認するスキームがなければそもそも不正アクセスに気付くことすらできない。）
- 他事業者で発生した攻撃について、自サービスでの発生に備えた対応を実施することが重要。
  （アカウントリスト攻撃が発生しているのであれば、監視間隔を短くする等の措置が有効。）
- 攻撃情報や情報セキュリティ対策について、部署間やグループ会社間での情報共有が必要。
  （利用者から見れば一つの事業者として捉えられ、再発防止を全社的に取り組む必要。）
- 不正ログインの疑いがある場合の、サービス停止の判断基準の整備が必要。
  （不正ログインが続けば、個人情報の漏えいが拡大してしまうため迅速な対応が必要。）
- 夜間・休日における迅速なサービス停止のため、事業者内連携も含めた体制の確認が必要。
  （担当者が駆けつけるだけでなく、停止作業を他部署の担当者に移管する方法も有効。）

【得られた気づき・教訓（事業者による取組以外のもの）】

- 攻撃元の通信遮断に資するため、被攻撃事業者とISP事業者との情報共有枠組みが必要。
- 攻撃手法の事業者間での情報共有について、既存の各種法令の整理が必要。
  （アカウントリスト攻撃のアカウントリストの個人情報への該当性に留意が必要。）
- 利用者自身が、IDやパスワードを使いまわさないように心掛けることも必要。

事例３　端末へのマルウェア感染（1/2）

【発生事象の概要】

- マルウェア感染によるものと疑われる通信について、NISCから該当事業者へ情報提供を行った。
- 情報提供した内容を元に、事業者のIT管理部署が調査を実施。
- 感染の疑いがある端末を特定し、端末の初期化を行うとともに、部署内で情報共有を行った。

【背景】

- 部署ごとに別の業務システムを有しており、それぞれ別のファイヤーウォールを通してインターネットに接続。
- マルウェア感染が疑われた業務システムは、複数の下部組織が使用。下部組織ごとに管理者がおり、独立した管理が行われている。また、外部から下部組織内への接続は行えない設定※となっている。
  ※NAT変換（ネットワークアドレス変換）を行い下部組織内のネットワークが当該下部組織の外からは隠蔽されている。

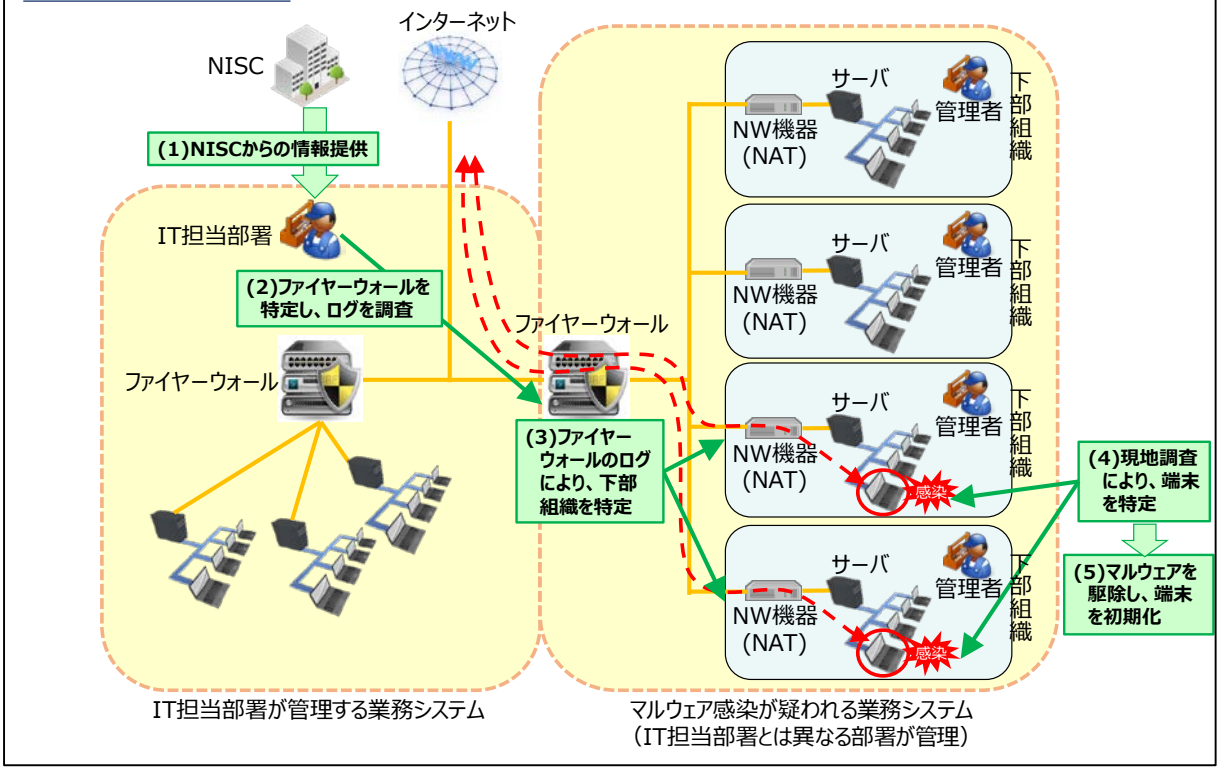
【検知】

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

【対処】

- 情報提供の内容（IPアドレス）から、該当のファイヤーウォールを特定し、該当部署に連絡を実施。
- IT担当部署でファイアウォールのログを調査し、マルウェア感染の疑いのある複数の下部組織を特定した。
- 該当の下部組織に対してそれぞれ連絡を行い、現地にて端末の調査を実施。
- マルウェア駆除ツールを使用し、マルウェアによるものと疑われる通信の停止を確認。端末の初期化も実施。
- 各部署の責任者間、各下部組織の責任者間、及び各下部組織の管理者間において、情報を共有した。

【発生事象のイメージ】



事例３　端末へのマルウェア感染（2/2）

【原因】

- ウィルス対策ソフトの設定について、調達時の仕様書に十分な内容が記載されていない等の理由により、定義ファイルの更新や定期的なスキャンが行われていない端末が存在した。
- マルウェア感染が疑われた業務システムは、下部組織ごとの管理者が管理しているものの、業務システム全体としての管理状況の把握が十分に行われていなかった。
- 端末利用者に対して情報セキュリティ研修を行っていないなど、情報セキュリティ意識が不十分であった。

【再発防止策】

＜早期対策＞

- 該当業務システム配下の全端末について、定義ファイルの更新と定期的なスキャンの設定※を実施。
  ※定期スキャンの設定時刻経過後に電源を入れた場合には、電源投入時に定期スキャンを実施するよう確実な設定を実施。
- ウィルス対策ソフトがマルウェアを検知した場合、IT担当部署の管理者に、電子メールで通知するよう設定。

＜中長期対策＞

- 業務システム内のネットワーク管理については、下部組織ごとではなく、部署として統一的な管理を実施。
- 調達仕様書のひな形の作成や運用手順等の明確化を行い、部署内での調達・運用管理を統一化。
- 情報セキュリティに関する従業員・職員研修を定期的に実施。
- IT担当部署（情報セキュリティ担当）の増強を実施。

【得られた気づき・教訓】

- 事業者全体の情報セキュリティ意識の向上のためには、経営層から意識付けを始める必要。
- 情報セキュリティ対策を、事業者内、部署内で統一することが重要。
  （下部組織ごとに責任者が管理している場合でも横串を通して管理することが重要。）
- 運用ルールの統一には、調達仕様書のひな形作成や、運用手順のマニュアル化が有効。
- 統一的な管理には、情報セキュリティ教育を受けた者を管理者とし、上位の組織から横串を通して行うことが必要。
  （情報セキュリティを確保するためには一定の専門知識が必要で、人数も限られる。）、
- 端末利用者の情報セキュリティ意識向上のために、定期的な情報セキュリティ教育が必要。
- 事後的な原因調査のため、ファイヤーウォール等のネットワーク機器でのログ取得が重要。

（本ページは白紙です。）

別添５　用語解説

	用　　語	解　　説
A	ACF	Asia-Pacific Telecommunity Cybersecurity Forumの略。アジア太平洋電気通信共同体（APT）のサイバーセキュリティフォーラム。
	AIST	national institute of Advanced Industrial Science and Technologyの略。独立行政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。
	ANSI	American National Standards Instituteの略。米国国家規格協会。
	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。
	BlackHat Briefings	サイバーセキュリティの現状や最先端の技術を知ることができる国際カンファレンス。1997年から開催されている。
C	C^4TAP	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。
	CODE BLUE	日本発の情報セキュリティ国際会議。2014年２月及び12月に開催。
	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。
	CYREC	Cybersecurity Research Centerの略。標的型攻撃等の新たなサイバー攻撃の抜本的な解決を目指し、2013年４月、NICTが主導的な役割を担って構築した、オール・ジャパンの英知を結集したサイバーセキュリティ研究開発拠点。
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。
	DKIM	DomainKeys Identified Mailの略。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールにおける送信元のなりすまし等を防ぐ。
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。
	GPKI	Government Public Key Infrastructureの略。国民等から行政機関に対する申請・届出等や、行政機関から国民等への申請・届出等に対する結果の通知等を、インターネットを利用しペーパーレスで行うことを目的として、申請・届出等やその結果の通知等が、真にその名義人（申請者や行政機関の処分権者）によって作成されたものか、申請書や通知文書の内容が改ざんされていないかを確認する行政機関側の仕組みとして整備された公開鍵暗号方式によるデジタル署名を用いた認証システム。
	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。
	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。
	IPv4	Internet Protocol version 4の略。現在広く使用されているInternetの通信のプロトコル。
	IPv6	Internet Protocol version 6の略。IPv4の次期規格であり、アドレス数の大幅な増加、セキュリティ強化及び各種設定の簡素化等が実現可能。
	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。
	ISO/IEC 27000シリーズ	情報セキュリティの管理・リスク・制御に関するベストプラクティスを提供する国際規格。
	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人材育成iPedia	高度IT人材の早期育成を図る上で重要となる教育機関における実践的なIT教育の拡充・普及を支援するための情報提供サイト。IPAが運営。
	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	JAB	Japan Accreditation Boardの略。公益財団法人日本適合性認定協会。
	JASPER	Japan-ASEAN Security PartnERshipの略。ASEAN各国向けのセキュリティ対策に関する総合的な技術協力プロジェクト。
	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。
	JNSA	Japan Network Security Associationの略。NPO日本ネットワークセキュリティ協会。
	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	National CSIRT	特定の国や地域に関連したサイバーセキュリティインシデントに関連する各種問い合わせの窓口として、他のCSIRTとの情報連携、調整等を担う国際連携CSIRTのこと。
	NCFTA	National Cyber-Forensics and Training Allianceの略。FBI、民間企業、学術機関を構成員として米国に設立された米国の非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。
	NICT	National Institute of Information and Communications Technologyの略。国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を実施するとともに、民間や大学が実施する情報通信分野の研究開発の支援の実施等を行う独立行政法人。

	NII	National Institute of Informaticsの略。国立情報学研究所。大学共同利用機関法人情報・システム研究機構の一員。情報学という新しい学問分野での「未来価値創成」を目指すわが国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	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。
	NVD	National Vulnerability Databaseの略。NISTが管理している脆弱性情報データベース。
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。
	PDF	Portable Document Formatの略。アドビシステムズ社によって開発された電子文書フォーマット。全ての環境でほぼ共通の文書表示ができる仕様から、2008年７月にISO32000-1として標準化された。
	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。
R	RIETI	the Research Institute of Economy, Trade and Industryの略。独立行政法人経済産業研究所。2001年に設立された経済産業省所管の政策シンクタンク。
S	S/MIME	Secure / Multipurpose Internet Mail Extensionsの略。電子署名を利用した、電子メールの送信者認証技術の一つ。RSA Data Security社によって提案され、IETFによって標準化された。RSA公開鍵暗号方式を用いてメッセージを暗号化して送受信する。この方式で暗号化メールをやり取りするには、受信者側もS/MIMEに対応している必要がある。
	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。
	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。
お	オープンデータ	行政機関が保有する統計・行政などのデータを広く利用しやすい形で公開すること。Data.gov（米国）やData.gov.uk（英国）などの取組が各国政府によって行われており、我が国でも電子行政オープンデータ戦略が策定され、取組が進んでいる。
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）。
	共通キャリア・スキルフレームワーク	IPAにおいて、2008年10月策定、2012年３月追補。我が国が目指すべき高度IT人材像に即したキャリアと求められるスキルを示したフレームワーク。
	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	2013年６月10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立国」の実現を目指し、2015年度までの３年間の国家戦略をとりまとめたもの。なお、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、新しい法的枠組みに基づく新たなサイバーセキュリティ戦略案をとりまとめているところであり、2015年５月25日の第２回サイバーセキュリティ戦略本部会合においてパブリックコメント案が示された。
	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。
	情報セキュリティガバナンス協議会	企業組織が適切な情報セキュリティガバナンスを確立することを促進するため、経営陣が情報リスクについて正しく理解し、組織として適切なリスク管理と情報セキュリティ対策を実施することを目指し、情報リスクの管理に関する知見の共有や情報セキュリティガバナンスに関する普及啓発等を実施することを目的に2012年５月21日に設立された協議会。
	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。
	情報セキュリティスペシャリスト試験	情報処理技術者試験の一区分であり、セキュリティにおける専門性を有することを認定する国家試験。
	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。
	スパイウエア	利用者のコンピュータから、個人情報やコンピュータの情報などを情報収集者に送信するソフトウェアのこと。一般的には、そのようなソフトウェアがインストールされていることや動作していることに利用者が気付いていない状態で、自動的に情報を送信するソフトウェアをスパイウェアと呼ぶ。
	スパムメール	迷惑メールのこと。
	スマートコミュニティ	様々な需要家が参加する一定規模のコミュニティの中で、再生可能エネルギーやコージェネレーション等の分散型エネルギーを用いつつ、ＩＴや蓄電池等の技術を活用したエネルギーマネジメントシステムを通じて、分散型エネルギーシステムにおけるエネルギー需給を総合的に管理し、エネルギーの利活用を最適化するとともに、高齢者の見守りなど他の生活支援サービスも取り込んだ新たな社会システムを構築したもの。
	スマートデバイス	情報処理端末のうち、単なる計算処理だけではなく、多用途に使用可能な多機能端末のこと。スマートフォンやタブレット端末の総称として使われることが多い。
	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	脆弱性関連情報届出受付制度	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。
	政府機関統一基準群	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。
	世界最先端IT国家創造宣言	2013年６月14日閣議決定（2014年６月24日、2015年６月30日改定）。今後５年程度の期間に、我が国が国民一人ひとりがITの恩恵を実感できる世界最高水準のIT国家となるために必要となる政府の取組等を取りまとめたもの。
	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	総合科学技術・イノベーション会議	内閣総理大臣及び国務大臣と有識者の議場として、日本全体の科学技術を俯瞰し、各省より一段高い立場から、総合的・基本的な科学技術政策の企画立案及び総合調整を行うことを目的として、2001年１月に内閣府に総合科学技術会議が設置された。2014年５月、単なる研究開発の促進のみならず、その成果を産業化等の出口へ繋げてゆくことの明確化を企図し、総合科学技術・イノベーション会議に改称。
	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	知的財産戦略本部	内外の社会経済情勢の変化に伴い、我が国産業の国際競争力の強化を図ることの必要性が増大している状況に鑑み、知的財産の創造、保護及び活用に関する施策を集中的かつ計画的に推進するため、2003年３月、内閣に設置された本部。
	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 Japan）。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。
	特別管理秘密	国の行政機関が保有する国の安全、外交上の秘密その他の国の重大な利益に関する事項であって、公になっていないもののうち、特に秘匿することが必要なものとして当該機関の長が指定したもの。
	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）
	認証局	電子証明書の発行などを行う第三者認証機関のこと。
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	コンピュータウイルス、ワーム、スパイウェア等の、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。
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。
	ボットウィルス	コンピュータを外部から遠隔操作するためのプログラムの一種。ボットウィルスに感染してしまうと、外部からの指示を待ち、インターネットを通じて、攻撃者にコンピュータを遠隔操作されてしまう。外部から遠隔操作するという動作から、ロボット（Robot）をもじってボット（BOT）と呼んでいる。
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。
め	迷惑メール対策推進協議会	電気通信事業者、メール送信事業者、広告事業者、配信ASP事業者、セキュリティベンダー、各関係団体、消費者、学識経験者、関係省庁など迷惑メール対策に関わる関係者が幅広く集まり、関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などにより、関係者による効果的な迷惑メール対策の推進に資することを目的として、2008年11月27日に設立された協議会。
	迷惑メール追放支援プロジェクト	民間事業者による自主的な迷惑メール対策を促すことを目的とした取組。2005年２月から開始。
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。
り	リカレント教育	職業人を中心とした社会人に対して、学校教育の修了後、いったん社会に出てから行われる教育であり、職場から離れて行われるフルタイムの再教育のみならず、職業に就きながら行われるパートタイムの教育も含む。
	リスクコミュニケーション	リスクに関する正確な情報をステークホルダーである関係主体間で共有し、相互に意思疎通を図ること。
	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、共用、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	量子力学の理論を用いた暗号技術。原理的に盗聴の有無を検知できる特性を持つ。