サイバーセキュリティ政策に係る年次報告
(2013年度)

2014年７月10日

情報セキュリティ政策会議

情報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。

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

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

＜目次＞

はじめに

サイバー空間と実空間の融合・一体化が進みITへの依存を深める現代社会において、サイバー空間を取り巻くリスクの深刻化は、国民生活や社会経済活動への影響はもとより、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。

あらゆるものがインターネットに繋がるIoT（Internet of Things）の時代を迎える中、サイバー攻撃は一層複雑・巧妙化し、攻撃対象も拡大してきている。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、国民生活や経済活動に直結する重要インフラ等の制御システムを狙った攻撃、急速に普及したスマートデバイス等を介した個人情報の窃取や不正な電子商取引の発生等は、我が国の国際競争力を揺るがしかねず、また国民一人ひとりにとってもITを安心して利用することが難しくなるといった課題を生じさせている。

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（NISC）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ところである。さらに昨年６月、情報セキュリティ政策会議は昨今のサイバー空間の情勢変化に対応すべく、新たな国家戦略となる「サイバーセキュリティ戦略」（以下「戦略」という。）及びその年次計画「サイバーセキュリティ2013」を策定した。

本報告は「サイバーセキュリティ立国」の実現を目標に掲げる戦略に基づく初年度の年次報告であり、2013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を俯瞰するとともに、従前は個別に報告されてきた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、各府省庁の関連施策の実施状況等について取りまとめ、報告するものである。

本編記載のとおり、NISCを結節点とした関係主体の連携体制の強化、「政府機関の情報セキュリティ対策のための統一基準群」、「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」、「サイバーセキュリティ国際連携取組方針」等の策定等のほか、年次計画に掲載された各府省庁の取組は着実に進捗している。

しかしながら、サイバーセキュリティを取り巻く環境は日々変化しており、2020年の東京オリンピック・パラリンピック開催に向けた対策強化も踏まえ、新たな課題への対応が常に求められている。政府としては、今後の環境変化に迅速かつ的確に対応すべく、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り継続的な改善を実践していくこととする。

（本ページは白紙です。）

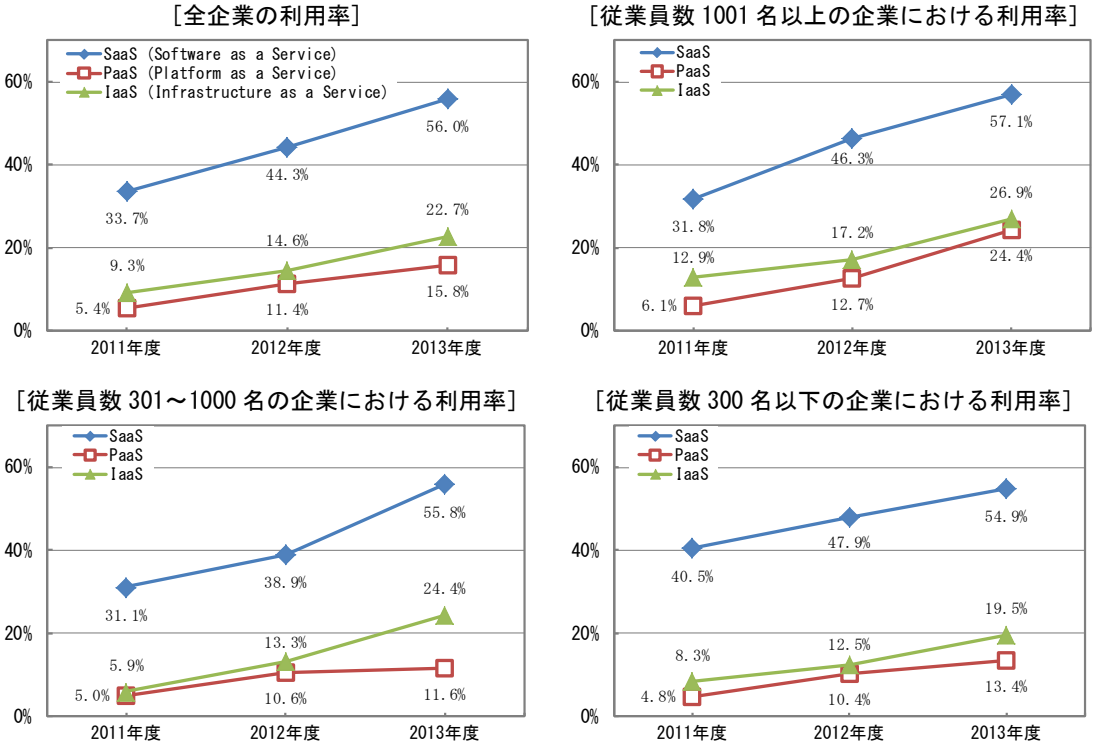
Ⅰ　2013 年度のサイバーセキュリティに関する情勢

1　我が国におけるサイバーセキュリティ全般の状況

今日のITの高度化の進展には、めざましいものがある。それに伴い、企業等の組織や個人などにおいて、クラウドコンピューティングやSNSなどのITを活用した多種多様なサービスが、ますます普及している状況にある。

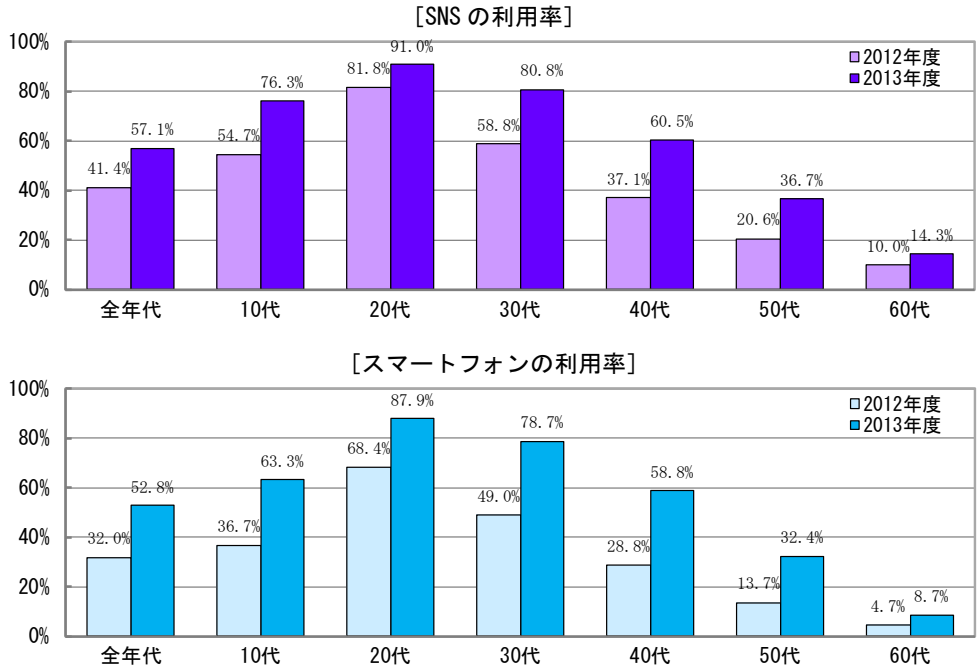
例えば、クラウドコンピューティング関連サービスの利用は、中小企業から大企業まで企業規模にかかかかわらず高まっており、企業活動がますますサイバー空間に依存していることの一例を示している（図表Ⅰ－1－1）。また、個人の活動面についてみれば、コミュニケーションなどにおけるSNSの利用率が、若年層以外の層でも高まっており、個人の社会的活動が大きくサイバー空間に依拠するようになりつつある（図表Ⅰ－1－2）。そして、地域の企業がインターネット等を通じて直接グローバルに事業活動でき、また、個人が携帯するスマートフォンやタブレットによってリアルタイムに地球上のあらゆる場所にいる人々と共通の体験ができるということは、人の活動能力や発展の可能性を飛躍的に高めることになる。

図表Ⅰ－1－1　クラウド関連サービスの利用動向[1]



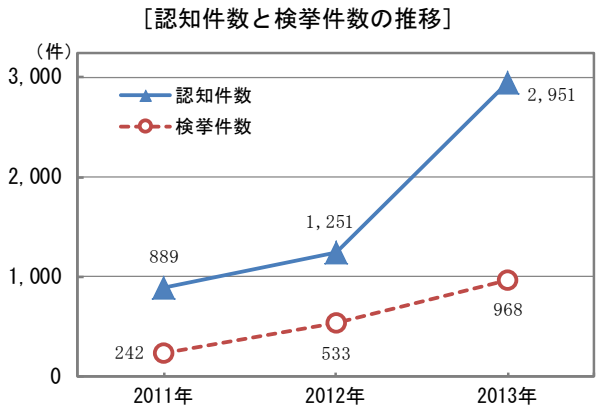
[1] 「IT 人材白書」（IPA）の各年度のデータ編「IT 人材動向調査結果（ユーザー企業向け）」から作成。

図表Ⅰ－1－2　SNS 及びスマートフォンの利用動向 [2]



これらのことは、ITの爆発的な普及についての積極的評価につながる側面である。一方、サイバー空間におけるリスクの深刻化も見逃すことはできない。例えば、2013年度に限ってみても、大手インターネットサービス事業者における不正アクセスによって100万件を超えるユーザー情報が漏えいした事案のほか、インターネットバンキングやSNSなどのサービスを利用する際のログインIDやパスワードを第三者がなんらかの手段によって入手し不正にアクセスする（不正ログイン）事案も発生しており、一般利用者も危険にさらされている状況にある。2013年における不正アクセス行為（認知件数）は、2012年に比して約2.4倍となっている。これら不正行為の目的としては、2012年はオンラインゲームなどの不正操作が中心であったが、2013年はインターネットバンキングやインターネットショッピングをターゲットとした金銭目的にウェイトが変化している（図表Ⅰ－1－3）。

図表Ⅰ－1－3　不正アクセス行為の発生状況 [3]



不正アクセス行為後の行為	2011年	2012年	2013年
インターネットバンキングの不正送金	188 件	95 件	1,325 件
インターネットショッピングの不正購入	172 件	223 件	911 件
オンラインゲーム、コミュニティサイトの不正操作	358 件	662 件	379 件
ホームページの改ざん・消去	28 件	42 件	107 件
情報の不正入手	74 件	99 件	92 件
インターネット・オークションの不正操作	22 件	29 件	36 件
不正ファイルの蔵置	4 件	1 件	20 件
その他	3 件	100 件	81 件

[2] 「平成 25 年情報通信メディアの利用時間と情報行動に関する調査＜速報＞」（情報通信政策研究所）のデータから作成。
[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、2014 年３月 27 日公表）のデータから作成。

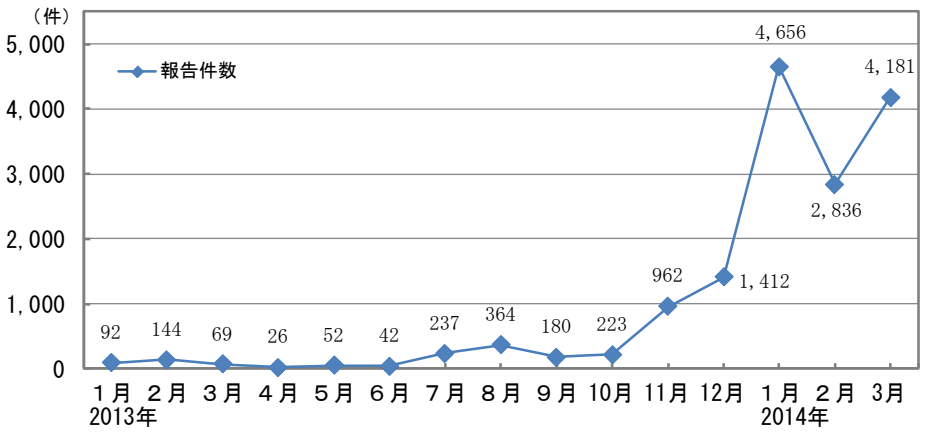
そして、不正アクセス行為の手口も巧妙化しており、ID・パスワードなどの識別符号を窃用した不正アクセス行為に係る検挙件数をみると、その入手手口は、2012年には「言葉巧みに利用権者から聞き出した又はのぞき見たもの」が最も多かったが、2013年には「利用者のパスワードの設定・管理の甘さにつけ込んだもの」が急増し大部分を占めるに至っている（図表Ⅰ－１－４）。

図表Ⅰ－１－４　不正アクセス行為に係る犯行の手口の内訳[4]

	2011年	2012年	2013年
識別符号窃用型の検挙件数	241 件	532 件	965 件
利用者のパスワードの設定・管理の甘さにつけ込んだもの	59 件	122 件	767 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	29 件	299 件	64 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	52 件	101 件	56 件
共犯者等から入手したもの	38 件	22 件	35 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	1 件	29 件	25 件
フィッシングサイトにより入手したもの	59 件	18 件	9 件
他人から購入したもの	0 件	0 件	7 件
その他	3 件	11 件	2 件
セキュリティ・ホール攻撃型の検挙件数	1 件	1 件	3 件

金銭目的の不正な行為の増大という傾向は、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、さらには住所、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行為であるフィッシングの急増にもみられる。例えば2014年３月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）」は、4,181件と年末から高い水準が続いている（図表Ⅰ－１－５）。そして、この件数のうち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（同月度の報告数の約97%）との報告[5]もあるほか、2013年度中に限ってみても、大手金融機関をかたるフィッシング事案が相次いで報道されるなど、こうした金銭目的とみられる不正アクセスがサイバーセキュリティに係る大きな脅威となっていることが分かる。

図表Ⅰ－１－５　フィッシング報告件数の推移[6]



[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、2014 年３月 27 日公表）のデータから作成。
[5] 「2014/03　フィッシング報告状況」（フィッシング対策協議会、2014 年４月１日公表）より。
[6] 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。

企業等の組織においては、通常、管理者がその情報システムの運用を行っている。不正アクセス行為の認知件数の内訳を、届け出た管理者別にみると、一般企業の被害が突出して増加している（図表Ⅰ－１－６）。その動機については、上述のように不正に経済的利益を得るためが顕著であるが、顧客データの収集等、情報を不正に入手するためというものも増加している点も注目される。

図表Ⅰ－１－６　届出管理者別の不正アクセス認知件数[7]

	2011年	2012年	2013年
一般企業	762 件	1,163 件	2,893 件
プロバイダ	115 件	22 件	9 件
大学、研究機関等	1 件	12 件	9 件
行政機関等	6 件	52 件	24 件
その他	5 件	2 件	16 件

また、標的型メール攻撃の傾向についてみると、2013年中に警察庁で把握した[8]標的型メール攻撃の件数は492件であり、前年から517件の減少（前年比51％減）がみられ、一見すると脅威が下火となったように見受けられる。しかし、同庁の分析では「ばらまき型」攻撃が減少した一方で、いわゆる「やりとり型」攻撃の増加や不正な外部接続の発覚を免れようとする手口の出現等、攻撃の手口が巧妙化したとされているなど、むしろ脅威は増大しているとの見方もある。

こうした標的型攻撃は、標的とされた組織の情報システム内に不正プログラムを侵入させ、企業の営業秘密等の重要な情報の窃取等を行うことを主目的とした攻撃である。昨今このような多様化・巧妙化した手口による攻撃が増加しており、攻撃により窃取された情報を用いた更なる標的型攻撃等の発生も懸念される。このような中、企業の管理レベルのアップを促進するべく、知的財産戦略本部において、営業秘密管理指針の記述における事例、ベストプラクティス等の反映なども議論されている[9]。

[7] 「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、2014 年３月 27 日公表）のデータから作成。
[8] 「平成 25 年中のサイバー攻撃の情勢及び対策の推進状況について」（警察庁、2014 年２月 27 日公表）より。情報窃取を企図したとみられる標的型メール攻撃として、「サイバーインテリジェンス情報共有ネットワーク」を通じて警察が把握したもの。
[9] 「営業秘密タスクフォース報告書」（知的財産戦略本部検証・評価・企画委員会営業秘密タスクフォース、2014 年４月 23 日公表）より。

２　政府機関等・重要インフラ企業におけるサイバーセキュリティに関する情勢

(1)　政府機関等におけるサイバーセキュリティに関する情勢

2013年度に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[10]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。

以下に、2013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。

ア　外部からの攻撃に係る情報セキュリティインシデント

前年度に引き続き、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使用等により、国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。

一般的に、サイバー攻撃の初期段階において多く使われる手段として、標的型メール攻撃がある。標的型メール攻撃とは、添付ファイルに不正プログラムが含まれていたり、本文中に不正プログラムが蔵置されているサーバのURLが記載されていたりする電子メールを標的に対して送付するものであり、メール受信者が添付ファイルを開いたり記載されているURLをクリックしたりすることにより、メール受信者の端末が不正プログラムに感染する。

NISCでは、GSOC[11]において、政府機関が受信する不審メールについて、情報の集約と注意喚起を行っており、2013年度においては、381件の注意喚起文書を発出した（図表Ⅰ－２－１）。2012年度は12月に大量の不審メールが政府機関に対して送付されたという特殊事情があるが、それを除くと全体的な傾向として、ここ数年漸増している。

図表Ⅰ－２－１　不審メールに関する注意喚起の件数の推移

	2011年度	2012年度	2013年度
不審メールに関する注意喚起の件数	209 件	415 件	381 件

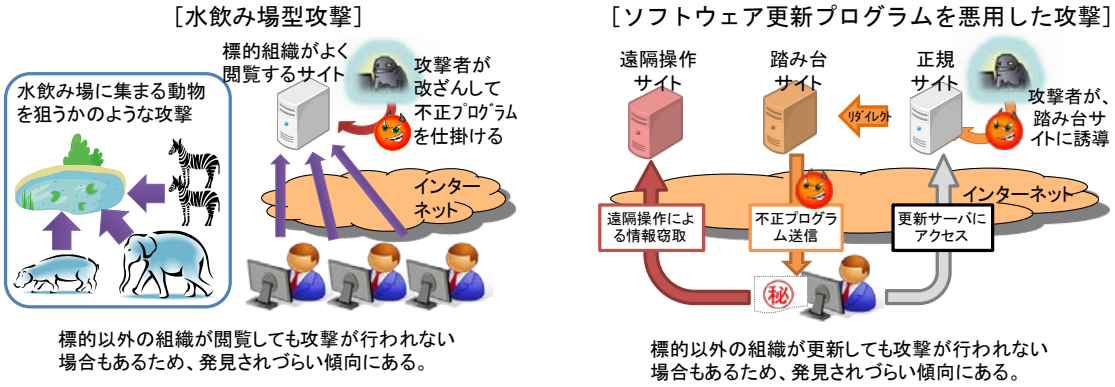
また、標的型攻撃に関しては標的型メール攻撃のほか、2013年には、いわゆる水飲み場型攻撃として、標的とする組織のIPアドレスからのサイト閲覧者のみが感染するタイプの攻撃も発生している。2013年10月に「中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃」として報道されたもので、政府においては７省庁の端末においてウイルスの自動的なダウンロードがあったが、情報流出については確認されなかった。

このほか、2014年２月に特定の動画再生ソフトをアップデートした際にウイルスに感染する情報セキュリティインシデントの発生も報じられている（独立行政法人において感染例あり）など、攻撃が巧妙化・多様化する傾向が見られた。なお、標的型攻撃においては、修正プログラムが公開される前の脆弱性を悪用するもの（いわゆるゼロデイ攻撃）もあり、

[10] 「別添３－９　政府機関等に係る2013年度の情報セキュリティインシデント一覧」を参照。
[11] Government Security Operation Coordination team。24時間365日、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等の業務を行っている。

不正プログラムの感染自体の防止は技術的に困難である。そのため、ネットワークの監視や連絡体制の強化等を含め、不正プログラム感染の情報システム内部への侵入拡大対策の重要性が高まっている。

図表Ⅰ－２－２　新たな脅威（標的型攻撃）の例[12]



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利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。2013年度においては、GSOCより78件の脆弱性情報等を配信した（図表Ⅰ－２－３）。

図表Ⅰ－２－３　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

	2011年度	2012年度	2013年度
脆弱性情報等の配信	68 件	74 件	78 件

脆弱性をつい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、2013年度は独立行政法人における被害が多くみられたことから、政府機関のみならず独立行政法人における対策の一層の強化促進が必要な状況にある。

政府機関へのサイバー攻撃への対応として、GSOCでは、GSOCセンサーと呼ぶ政府横断的な情報収集・監視機能を用いて、サイバー攻撃やその準備動作等を検知する業務を行っている。この業務において、政府機関への脅威と認知された件数は、2013年度は約508万件であった（図表Ⅰ－２－４）。2012年度と比較して件数がおよそ５倍に増加しており、約６秒に１回検知している計算となる。これは、政府機関等への脅威増とともに、年度途中に行ったセンサーの増強等による影響もあると考えられる。引き続きGSOCセンサーの増強等により、よりきめ細かく脅威を捕捉し解析することが重要である。

[12] 「別添５　最近の主な脅威の概要とその対策」を参照。

図表Ⅰ－２－４　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

	2011年度	2012年度	2013年度
政府機関への脅威の件数	約 66 万件	約 108 万件	約 508 万件

また、GSOCセンサー等による監視活動によって不正アクセス等（疑いを含む）を検知した際には当該政府機関への通報を行っており、2013年度においては、139件の通報を行った（図表Ⅰ－２－５）。

図表Ⅰ－２－５　GSOC センサー監視等による通報件数の推移

	2011年度	2012年度	2013年度
センサー監視等による通報件数	139 件	175 件	139 件

2012年度の通報件数が突出しているのは、先にも述べたが2012年12月に大量の不審メールの府省庁への送付があったためである。その結果、2012年度の通報は、半数以上が標的型メールの検知によるものであった。

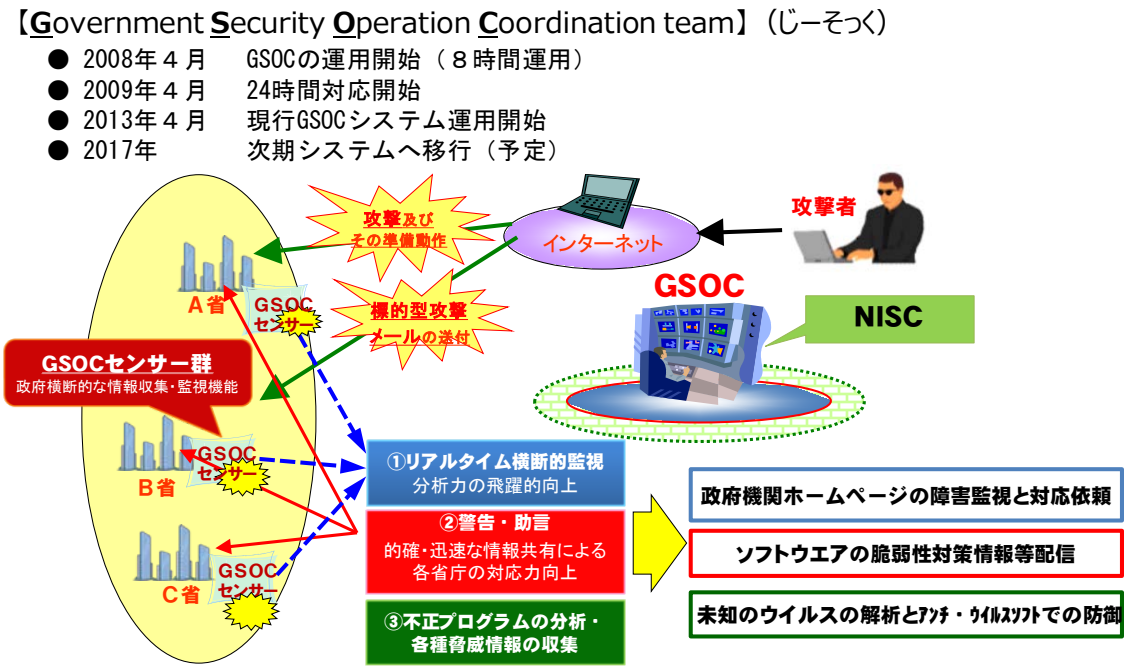
2013年度の場合には、標的型メールに関する通報は全体の約四分の一であった。2013年度の特徴的な点は、不審な通信[13]の検知である。このタイプは、2012年度まではほとんど存在していなかったが、2013年度は全体の３割に及んだ。不審な通信が検知される要因としては、標的型メールによる攻撃によるマルウェアへの感染や水飲み場型攻撃のように改ざんを受けたウェブサイトを閲覧することによるマルウェアのダウンロードの可能性が考えられる。

標的型メールについては、従来から脅威としては存在していたが、「ばらまき型」の攻撃がほとんどであり政府機関に対する成功率は低かった。しかし、2013年度から顕著にみられる、特定の組織、職員を対象とする、カスタマイズされた標的型メールによる攻撃の成功率が上がっているため、不審な通信の検知が増加していると考えられる。GSOCからの通報件数そのものは、大量の不審メールのような特殊要因を除くと例年と同じ程度ではあるが、前述のとおりGSOCから通報する不正アクセス等のタイプやその割合に変化があり、サイバー空間を巡るリスクがより深刻化している傾向がみられる。

標的型メールや水飲み場型攻撃はゼロデイ攻撃と組み合わせられる場合が多く、不正プログラムの侵入を完全に防ぐことは困難である。よって、GSOCの更なる強化が必要である。

[13] GSOC が各府省庁へ通報する「不審な通信」の全てが「不正な通信」というわけではない。例えば、ブラックリストに掲載されたウェブサイトへのテスト通信などは、事前の通報がない限り、GSOC からは不審な通信と見なされる可能性がある。

図表Ⅰ－2－6　GSOCの概要



イ　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

外部からの攻撃が増加する一方、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。

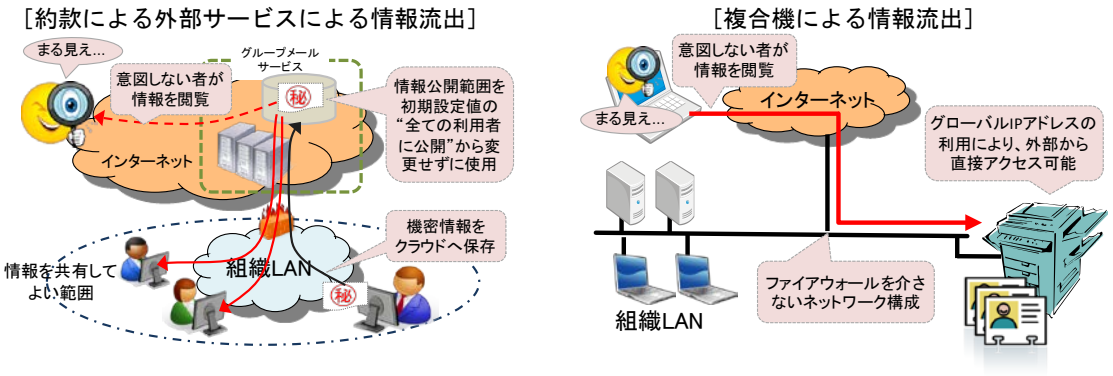
従来は、パソコンやUSBメモリの紛失、メールの誤送信といった人の不注意による偶発的なものが主であった。しかし、最近では、インターネットに繋がる機器やクラウドサービスの不適切な利用・利用時の不適切な設定に係る従来とは質の異なるものも発生している。

例えば、2013年７月に問題が表面化した、インターネット上でメールを共有できる無料のクラウドサービスで個人情報や中央官庁の内部情報が誰でも閲覧できる状態になっていた事案や、2013年11月に問題が表面化した、大学でファックスやスキャナーで読み取った学生らの個人情報がインターネット上で誰でも閲覧できる状態になっていた事案、2013年12月に問題が表面化した、入力した全ての文字情報がクラウドサービスのサーバに送信される日本語入力ソフトがインストールされていた事案等が発生している。

無料のクラウドサービスに係る事案について、同サービスは、インターネット上で電子メールを共有できるサービスであり、複数の府省庁において、職員が出張先において府省庁の者との内部情報の共有を図る目的や府省庁外の者との情報連絡を行う目的で同サービスが利用されてしまったことに起因するものである。

政府機関等においては、従来、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、保守的に対応してきた。しかし、業務現場においては、利便性の高いサービスのニーズは高まりつつある。上述の事案などは、そのニーズが情報セキュリティの観点から望ましくない結果を引き起こした事例とも考えられる。したがって、取扱いに注意を要する情報等について、業務現場のニーズに対応し、かつ、情報セキュリティが確保されたIT利活用環境の整備が求められている。

図表Ⅰ－2－7　新たな脅威（意図せぬ情報流出）の例[14]



(2)　重要インフラ企業におけるサイバーセキュリティに関する情勢

重要インフラ事業者等[15]におけるIT障害の発生時等において、重要インフラ所管省庁を経由してNISCに情報連絡のあった件数は、2013年度は153件と前年度（110件）の1.5倍に増加しており、情報連絡のうちサイバー攻撃に関するもの（意図的要因に係る件数）についても、133件と前年度（76件）より大きく増加している（図表Ⅰ－2－8）。なお、これらの増加はサイバー攻撃等によるIT障害等が増加していることを必ずしも示すものではなく、重要インフラ事業者等において情報共有の重要性が認識され、NISCとの情報共有体制がより積極的に行われるようになってきていることも大きく寄与しているものと考えられる。

図表Ⅰ－2－8　重要インフラ事業者等から NISC への情報連絡の件数

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡件数	43 件	110 件	153 件
サイバー攻撃に関するもの	15 件	76 件	133 件
不正アクセス、DoS 攻撃	12 件	55 件	121 件
コンピュータウイルスへの感染	2 件	6 件	7 件
その他の意図的要因（不審メール等）	1 件	15 件	5 件

サイバー攻撃の内訳としては、大多数が不正アクセス・DoS攻撃に分類されるものであり、この具体例としては次のようなものがあった[16]。

○事業者が管理する会員制サイトのサーバにおいて、当該サーバで利用しているミドルウェアにおける脆弱性を狙われ、当該サイトへログインするためのIDと暗号化されたパスワードが外部に漏えいした。

[14] 「別添５　最近の主な脅威の概要とその対策」を参照。
[15] 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」及び「物流」。）に属する事業を営む者等のうち重要インフラの情報セキュリティ対策に係る行動計画に指定された事業者等及び当該事業者等から構成される団体。2014 年度からは、第３次行動計画の策定に伴い、「化学」、「クレジット」及び「石油」分野が新たに重要インフラ分野に加わる。
[16] 「別添４－８　補完調査」を参照。

○ウェブサイトの管理システムに存在する脆弱性を狙われ、当該ウェブサイトが書き替えられ、ウェブサイト閲覧者に対し、外部の不正なウェブサイトへの誘導が行われた。

○DNSサーバに係る設定不備（オープンリゾルバ状態）が原因と推測される大量の接続要求が海外の複数地域からあり、その影響によりウェブサイトの表示が著しく遅くなった。

また、IPAが情報集約点となり、サイバー攻撃等に関する情報を参加組織間で共有する取組である「サイバー情報共有イニシアティブ（J-CSIP）」において、参加組織からIPAに対し、標的型攻撃メールと思われる不審なメール等の情報提供が行われた件数は385件であった。参加組織からの積極的な情報提供もあり、昨年度（246件）から約1.5倍に増加している。この情報をもとにするなどしてIPAから参加組織へ情報共有を実施した件数は180件であった。（図表Ⅰ－２－９）

図表Ⅰ－２－９　サイバー情報共有イニシアティブにおける情報提供等の件数

	2011年度	2013年度
IPA への情報提供件数	246 件	385 件
参加組織への情報共有実施件数	160 件	180 件

こうした状況を踏まえつつ、重要インフラ事業者等においても、引き続き情報セキュリティ対策を強化していくことが求められている。

3　2013 年度の政府の主な政策の取組実績

サイバー空間を巡るリスクの深刻化を受けて、新たな国家戦略として、2013年６月、内閣官房長官を議長とする情報セキュリティ政策会議は「サイバーセキュリティ戦略」を策定した。

2015年度までの３年間を対象とする同戦略は、①情報の自由な流通の確保、②深刻化するリスクへの新たな対応、③リスクベースによる対応の強化、④社会的責務を踏まえた行動と共助、を基本的な考え方とした上で、政府機関や重要インフラ事業者等の各主体がNISCを結節点として相互に連携しつつ、セキュリティ水準の向上やサイバー攻撃への対処能力の強化、人材育成や研究開発の推進等によるサイバーセキュリティ分野の基礎体力向上、国際連携の強化や政府組織体制の整備等に関する取組を推進することを通して、世界を率先する強靭で活力あるサイバー空間を構築し、もって「サイバーセキュリティ立国」を実現することを目標として掲げている（図表Ⅰ－３－１）。

図表Ⅰ－３－１　「サイバーセキュリティ戦略」の概要

同戦略には、政府機関・独立行政法人等、重要インフラ事業者等、企業・国民といった各主体に関し、強靭なサイバー空間を実現すべく守りを強化するための施策、人材の育成や技術力の強化・向上等、IT利活用の基礎体力となる情報セキュリティに係る基盤を強化することによる活力あるサイバー空間の実現に係る施策、そして、サイバー空間がグローバルなものであることから国際貢献等において世界を率先する施策などが盛り込まれている（図表Ⅰ－３－２）。

図表Ⅰ－３－２　「サイバーセキュリティ戦略」における主な取組（2013～2014 年度）

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靱な」サイバー空間（守り強化）	●機微情報を守るためのリスク評価手法の確立・統一基準の見直し ●GSOCの強化、CYMAT・CSIRTとの連携による的確・迅速な対応 ●対処訓練の実施、警察・自衛隊等の関係機関の役割整理 ●SNS・グループメールを含む新サービスに伴う新たな脅威への対応 ●サイバー(3.18)訓練	●重要インフラの範囲拡大や安全基準見直し等行動計画の見直し ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設 ●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂 ●税制など中小企業のセキュリティ投資の促進 ●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
「活力ある」サイバー空間（基礎体力）	●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂 ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し		
「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定	●日米 ●日英 ●日印 ●日露 ●日EU ●日ASEAN ●サイバー空間の国際規範づくり等に関する会議 ●IWWN[注1]	●MERIDIAN[注2]	（注１）サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加 （注２）重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。 等 ●共同意識啓発活動
組織体制	●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組：2015年度目途）		・GSOCの強化 ・GSOC保有情報の重要インフラ事業者との共有の仕組み ・必要な人材等の在り方　等

以下、同戦略に従って2013年度に推進した主な取組について概説する。

政府機関統一基準群については、新たな脅威及び技術への対応や実効性の向上を目的とした見直しを行い、2014年５月に改定を行った[17]。新たな脅威等への対応として、一つには、標的型攻撃の脅威への対応のための規定の整備を行っている。別に検討を行った統一基準に紐付くガイドライン[18]と合わせ、具体的には、標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずるというものである。また、情報システム等の外部委託先において不正機能の混入などを防止するための厳正な管理体制を求める、いわゆるサプライチェーン・リスク対策や、私物スマートフォン等の業務利用に係る管理の厳格化、府省庁におけるSNS等の利用時の機密情報の取り扱いの禁止、その他USBメモリや複合機に係る対策等について、近年の環境の変化を踏まえ、新たに規定を追加した。

なお、改定に当たっては、定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人ごとの遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく守られやすい基準となるよう配慮している（図表Ⅰ－３－３）。

図表Ⅰ－３－３　規定の見直しの例

（従来の統一基準における規定の例）

行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。

ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に報告することができない場合は、定められた　報告手順に従って、最高情報セキュリティ責任者に報告すること。

（見直し後）

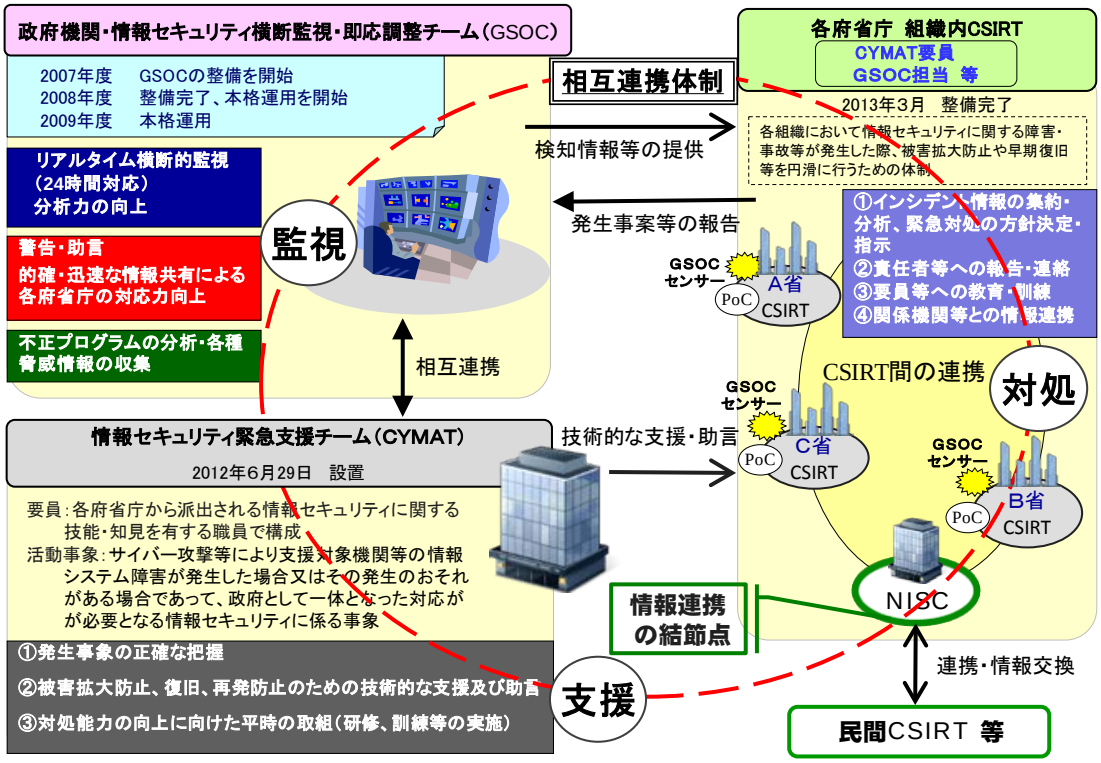
行政事務従事者は、情報セキュリティインシデントを認知した場合には、各府省庁の報告窓口に速やかに連絡し、指示に従うこと。

[17] 「別添３－１　「政府機関の情報セキュリティ対策のための統一基準群」の改定」を参照。
[18] 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。2013 年 10 月から試行を開始し、2014 年度より正式な運用を開始する予定である。「別添３－２　高度サイバー攻撃への対処」を参照。

その他、政府機関においては、GSOC・CYMAT・CSIRT連携の改善、３・18（サイバー）訓練の実施等により、サイバー攻撃対処態勢の充実・強化が進展した（図表Ⅰ－３－４・図表Ⅰ－３－５）。

図表Ⅰ－３－４　GSOC・CYMAT・CSIRT 間の連携強化

GSOC の機能強化とともに NISC を結節点とする GSOC、CYMAT 及び CSIRT の相互連携を深め、政府機関における情報集約・支援体制、サイバー攻撃に対する対処態勢を強化。



図表Ⅰ－３－５　３・18（サイバー）訓練

我が国に対するサイバー攻撃がより複雑・巧妙化しつつある状況を踏まえ、複数の政府機関を同時に狙うサイバー攻撃が発生した際の対処について、NISC と各府省庁及び重要インフラ事業者等との間の情報収集・共有訓練、並びに CYMAT 要員による緊急対処訓練を組み合わせて実施し、関係者間の連携習熟を行った。

［官房長官訓示］

［訓練全景］

重要インフラの情報セキュリティ対策については、従来の第２次行動計画により一定の成果を挙げているものの、第２次行動計画策定時に比べ社会面・技術面で様々な環境変化が生じていることから、サイバーセキュリティ戦略も踏まえ、新たな行動計画の検討を行った。

2014年５月に策定した第３次行動計画においては、第２次行動計画の基本的な骨格を維持しつつ、個別の施策に修正・補強が加えられている。具体的には、特に中小規模の事業者等が情報セキュリティ対策の水準を段階的に向上させることができるような指針の構築、平時の体制の延長線上にある大規模IT障害時の情報共有体制の構築、重要インフラの範囲を既存の10分野から、化学・クレジット・石油の３分野を加えた13分野への拡大等を行うこととした。また、情報セキュリティ対策の全体像を経営層にも把握してもらえるよう、行動計画の要点をまとめた章を設けるなど全体構成も工夫している。（図表Ⅰ－３－６）

図表Ⅰ－３－６　「重要インフラの情報セキュリティ対策に係る第３次行動計画」のポイント

施策群の構成と主要なポイント

1．安全基準等の整備及び浸透	対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求
2．情報共有体制の強化	平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化
3．障害対応体制の強化	関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化
4．リスクマネジメント	重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援
5．防護基盤の強化	関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　等

◆ 重要インフラ分野を既存の10分野から13分野に拡大（化学、クレジット及び石油の各分野を追加）
◆ 行動計画の要点として、「経営層に期待する在り方」等を示すとともに、PDCAサイクルに基づく事業者等の対策例とこれに関連する国の施策を一覧化
◆ 客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施

その他、重要インフラ分野においては、分野横断的演習の実施等の所要の取組を行っている[19]。

企業や個人における情報セキュリティ対策の促進については、他人に迷惑をかけず安全にIT利活用することについての認識醸成が重要である。情報セキュリティの普及啓発については、各府省庁・関係機関ホームページやセキュリティ関連行事における周知等のほか、引き続き国民の情報セキュリティに関する意識を向上させるための取組を推進した。

2009年度から毎年２月に実施している「情報セキュリティ月間」において、５回目となる2013年度は、情報セキュリティ月間の趣旨を広く国民に啓発することを企図し、月間の最初のワーキングデーを「サイバーセキュリティの日」に設定したほか、新たに策定した「情報セキュリティ普及啓発ロゴマーク」の活用やアニメ動画によるPR等を通し、身近で親しみやすい取組となるよう工夫している（図表Ⅰ－３－７）。

図表Ⅰ－３－７　情報セキュリティの普及啓発の取組

［情報セキュリティ月間ポスター］

［情報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）

［普及啓発アニメーション］

国民を守る情報セキュリティサイト
http://www.nisc.go.jp/security-site/

なお、「情報セキュリティ普及・啓発プログラム」（2011年７月策定）については、サイバー空間が国民のあらゆる世代・あらゆる場面・あらゆる活動に拡大・浸透している現状を踏まえ、

[19] 「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」を参照。

国及び国民全体の情報セキュリティへの関心・理解度・対応力の強化等を企図した見直しを行い、2014年７月、「新・情報セキュリティ普及啓発プログラム」を決定した（図表Ⅰ－３－８）。

図表Ⅰ－３－８　「新・情報セキュリティ普及啓発プログラム」のポイント

基本的な考え方　**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・増進を図る**

推進体制　産学官民の多様な主体で構成する協議会形式の場を設け、国民運動として普及啓発活動を推進していく体制を構築。
各主体が自律的に取り組める環境を整備し、国民1人1人に身近な地域との連携を推進。

主な取組

①総合的・集中的な普及啓発施策の更なる推進
・「情報セキュリティ月間」の期間を拡大(2月～3月18日＜サイバー訓練の日＞)し、広く国民に啓発。
・期間を問わず、ロゴマークやメディア等を活用し、国民に親しみやすい取組を推進し、取組の定着化を図る。
・国民1人1人が、サイバー空間の脅威から自ら身を守ることができるよう、国民運動として対策の実践や訓練等を促進。

②地域における取組の促進
・地域における各主体の活動や情報共有を促進。協議会形式の場を通じ、地域発産学官民連携による取組を全国的な動きに発展。

③特に注力が必要な層に対するきめ細やかな普及啓発活動の推進
・国民全体を対象とした活動に加え、特に注力が必要なターゲット（初等中等教育層、学ぶ機会が少ない層、関心が薄い層、中小企業を含めた企業等）に対し、協議会形式の場も活用してきめ細やかな普及啓発を推進。

同様に、人材育成についても「情報セキュリティ人材育成プログラム」（2011年７月策定）を見直し、2014年５月、「新・情報セキュリティ人材育成プログラム」を決定した。新しいプログラムにおいては、我が国の情報セキュリティ人材の「需要」と「供給」の好循環を形成することを目標として掲げ、情報セキュリティ人材の質的・量的不足の解消のための施策や、情報セキュリティを経営戦略として位置づけるよう経営層の意識改革を促すための施策等を盛り込んでいる（図表Ⅰ－３－９）。

図表Ⅰ－３－９　「新・情報セキュリティ人材育成プログラム」のポイント

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○組織の経営層
・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。
・製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

○実務者層のリーダー層
・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

【供給】人材の「量的拡大」と「質的向上」

○IT技術者等に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。

○高度な専門性及び突出した能力を有する人材の発掘・育成を推進するとともに、実社会での活躍を促進。

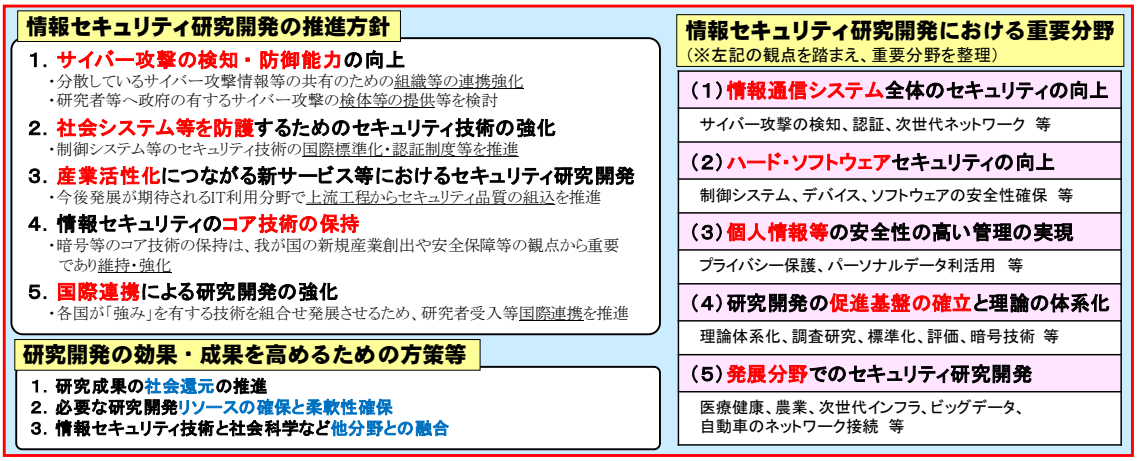
○グローバル水準の人材の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。

○政府機関は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。

○教育機関(初等中等教育機関を含む)の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。

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。改定にあたっては、単に研究開発の重点分野を見直すだけでなく、サイバー攻撃の検知・防御能力の向上、社会システム等を防御するためのセキュリティ技術の強化等を盛り込んでいる（図表Ⅰ－３－１０）。

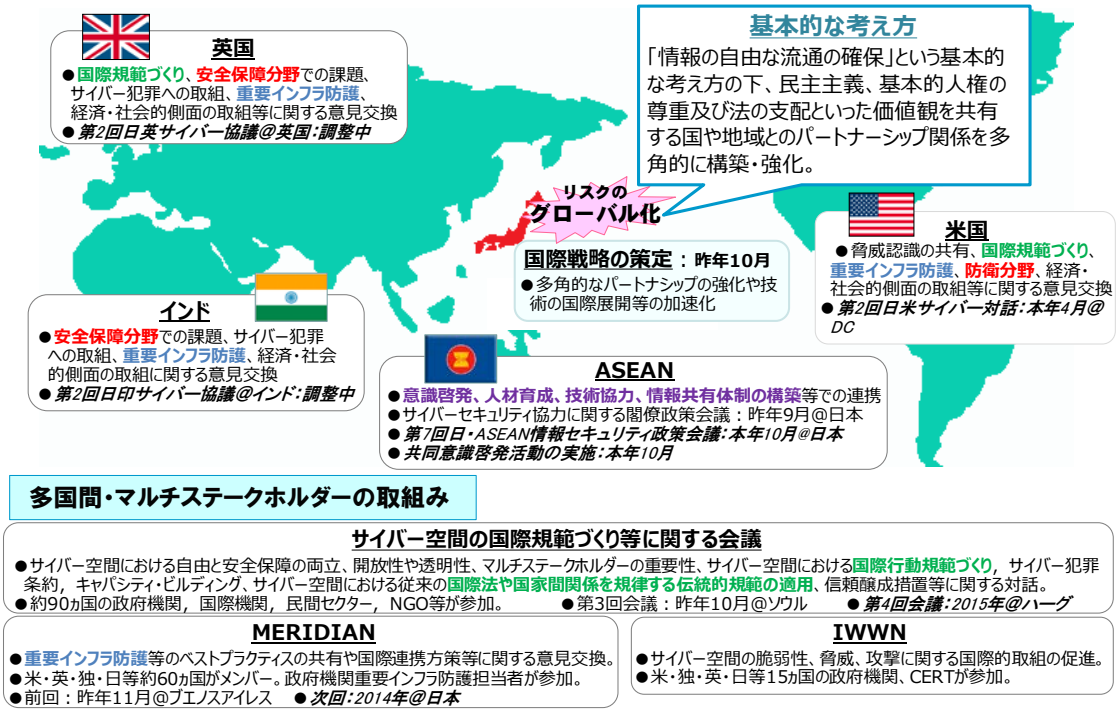
図表Ⅰ-3-10　「情報セキュリティ研究開発戦略」改定のポイント



国際連携の分野においては、従前の「日・ASEAN情報セキュリティ政策会議」や英国及びインドとの二国間サイバー協議に加え、2013年度には、米国との間でもサイバー対話を実施した。特に、ASEANについては、2013年９月に東京で「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催し、サイバーセキュリティの強化を含めた共同声明を発表した（図表Ⅰ-3-11）。こうした対話は、今後、ロシア、エストニア、豪州、フランス等との間にも拡大する予定であり、国際連携の輪を着実に広めてきている。

2013年10月には、「サイバーセキュリティ戦略」に則り、国際連携の強化に向けた日本の貢献の方向性を明確化した「サイバーセキュリティ国際連携取組方針」を策定した。これは、二国間、多国間、地域的枠組、国連会合その他あらゆる場を活用してサイバーセキュリティに関するグローバルな共通認識の醸成を図ることなどを明示しており、積極的に国際連携に取り組む日本の姿勢をアピールするものとなった（図表Ⅰ-3-12）。

図表Ⅰ-3-11　国際連携の取組実績



図表Ⅰ-3-12　「サイバーセキュリティ国際連携取組方針」のポイント

基本方針
① グローバルな共通認識の斬新的な醸成
② グローバルコミュニティへの我が国の貢献
③ 技術フロンティアのグローバルな拡大

重点取組分野
① サイバー事案への動的対応の実践
② 動的対応に備えた「基礎体力」の向上
③ サイバーセキュリティに関する国際的なルール作り

地域的取組
① アジア太平洋地域
② 欧米
③ その他の地域
④ 多国間枠組

なお、各国と協力・連携して情報セキュリティ上の課題に取り組むため、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」を実施している。

ASEAN各国との共同意識啓発活動、各省庁や関係団体等による国際関連イベントの開催、情報セキュリティ対策に関する情報提供等を集中的に実施することにより、ASEAN各国における情報セキュリティ対策の一層の普及を促している。2013年度は、ポスターやリーフレットのほか、スマートフォンの情報セキュリティにかかる意識啓発アニメーション（日本語版、英語版及びASEAN各国語字幕版）の作成や動画ポータルの開設等を行った（図表Ⅰ-3-13）。

図表Ⅰ-3-13　ASEAN 諸国との連携による意識啓発活動

各府省庁・関係団体等によるイベント開催又は後援名義

官房長官からのメッセージ　HP 掲載

国際連携による共同意識啓発活動
ASEAN 各国と 2012 年 10 月より共同の意識啓発（教材、共同ポスターの作成等）を実施

［共同シンポジウム開催］

［動画ポータル］

［情報セキュリティ Tips 配信］

［意識啓発ポスター］

［意識啓発リーフレット］

［意識啓発アニメーション］

［アニメーション DVD 贈呈式］

情報セキュリティ政策会議では、その下に設置される各専門委員会等において様々な課題が議論されているが、これら課題に対する実行計画をより実効性、持続性が高いものとするためには、様々な立場の専門家等が横断的に議論し、相互理解を深め、連携を強化することが求められている。また、社会経済活動がITへの依存度を増すほど、サイバーセキュリティ上のリスクも高まることから、「世界最高水準のIT利活用社会」の実現を目指すためには、IT利活用の促進とサイバーセキュリティ確保の双方バランスのとれた政策を総合的・戦略的に推進することが肝要である。このような観点から、IT総合戦略室とNISCとが連携し、IT政策担当大臣が主催する「IT利活用セキュリティ総合戦略推進部会」を新たに情報セキュリティ政策会議に設け、必要な取組について分野横断的に検討を進めている。

4　今後の取組

(1)　我が国のサイバーセキュリティ推進体制の強化

政府においては、情報セキュリティ政策会議の下、NISCが中心となって情報セキュリティ政策を推進してきたところであるが、サイバー空間をめぐるリスクの深刻化や、2020年に予定されているオリンピック・パラリンピック東京大会開催への対処能力強化のニーズを踏まえると、司令塔機能の一層の強化が求められている。そこで、「サイバーセキュリティ戦略」に盛り込まれた我が国のサイバーセキュリティ推進体制の強化(2015年度目途)を図るべく、2014年１月以降、情報セキュリティ政策会議等において討議を行った。本討議においては、次の３点が主な論点となった。

① サイバー脅威の甚大化に対応して能動的な対応能力を強化すべきであり、NISCの知見が各府省庁等に活用される仕組みを構築し、かつ、オリンピック・パラリンピック東京大会に備えて先行的に政府の体制強化の方向性が必要ではないかという点である。このため、GSOCの機能強化、重大なインシデントに関する原因究明など事後調査機能の強化、さらには、諸外国の政策やサイバーセキュリティを巡る情勢などの研究分析を行う専門的人材などの配備・育成を検討する必要があること。

② サイバー脅威の拡散に対応して、政府内における横串的機能を強化する必要があり、府省庁等のセキュリティ水準の向上に向けてNISCは積極的貢献をすべきであり、かつ、関係省庁のセキュリティ政策間の組織・分野横断的な実効性を確保の方向を目指すべきという点である。このため、政府機関統一基準等に照らして、各府省庁等の情報システムに関しセキュリティ監査機能を強化すること、そこで発見された事項への改善等に対処するためにも内閣情報通信政策監と連携しつつ、ITセキュリティ投資に関する評価機能を強化すべきであること、そして、セキュリティ政策についても総合調整機能を強化することについて検討する必要があること。

③ サイバー脅威のグローバル化に備えて、情報集約・国際連携機能の強化が必要であり、その観点から、政府機関間・重要インフラ事業者間でのサイバーセキュリティインシデント情報の集約機能の強化を図り、官民にまたがる複数の国際的窓口機能の在り方を整理するとともに、政府間連携のための人員強化といった点を検討する必要があること。

2013年度においては、国会においてもサイバーセキュリティ基本法を制定する動き[20]も高まってきたことから、その動きとも連携を図りながら体制強化の方向性について検討を進めた。そして、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）の下に設置された情報セキュリティ政策会議を、内閣に設置する本部に改組し、各府省庁等に対して情報セキュリティ監査・重大インシデントの原因究明等調査、行政機関からの資料提出義務、行政機関に対する勧告権等を備えるべきであること、その事務局等の機能を担う機関を整備すべきであることなどを検討した。

こうした討議を踏まえ、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」の決定に向けた検討を行うこととしている（図表Ⅰ－４－１）。

[20] サイバーセキュリティ基本法案は、本年６月 13 日に衆議院を通過し、６月 20 日に参議院において継続審査として決定された。

(2)　その他のサイバーセキュリティ施策の推進

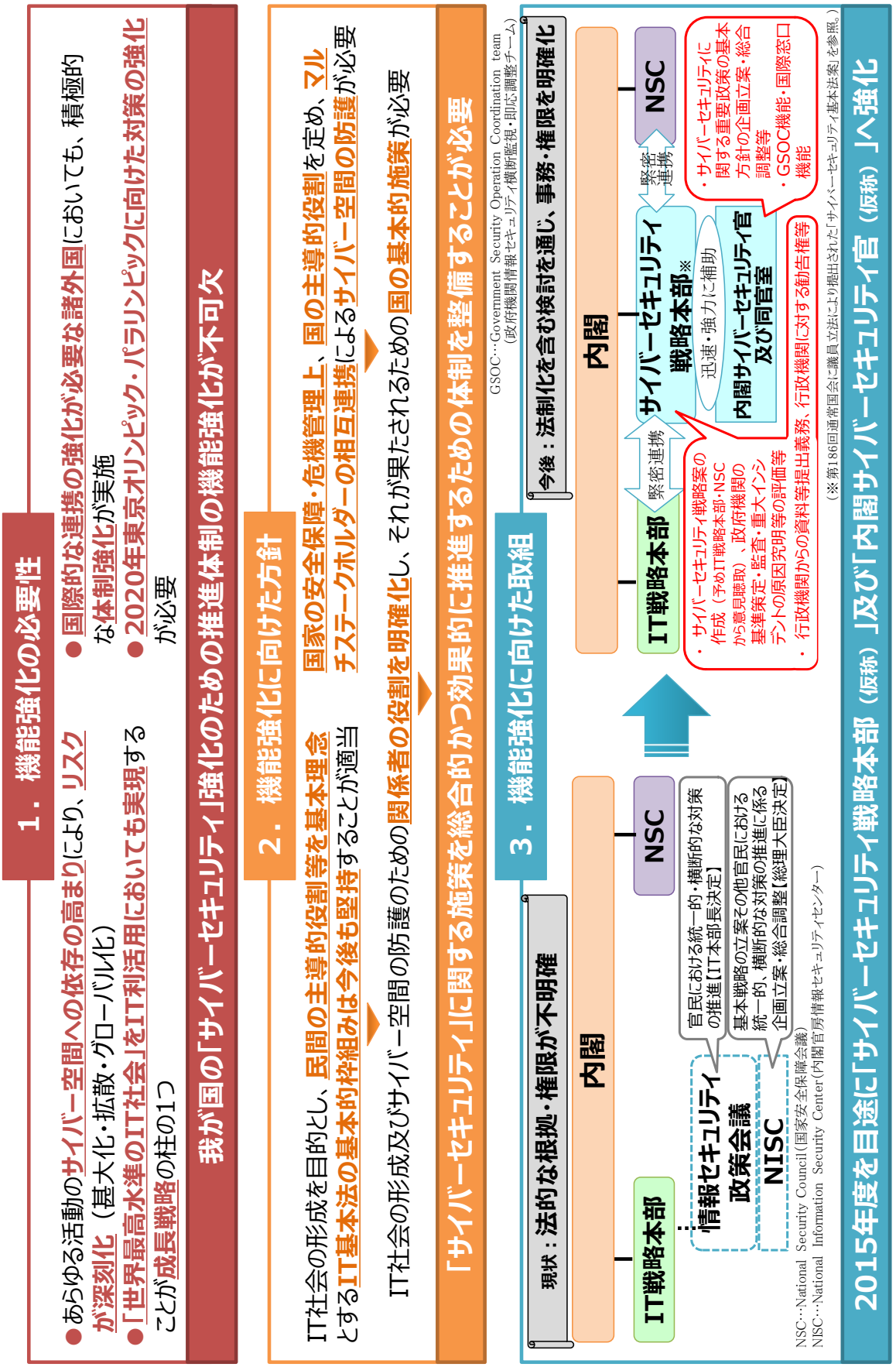
サイバーセキュリティ政策を体系的に推進すべく、約３か年を見据えた中期計画である「サイバーセキュリティ戦略」に基づき毎年度の計画を策定し、実施している。2014年度においても、2013年度に実施してきた各施策の成果等[21]を踏まえて、2014年７月に「サイバーセキュリティ2014」を決定したところであり、本計画を踏まえて、各府省庁が連携しつつ具体的施策を推進することとしている（図表Ⅰ－４－２）。

例えば、政府機関における対策に関して、従来から政府機関統一基準群ではクラウドサービスを外部委託の一形態として一括して扱っていたが、SaaS、PaaS、IaaS等多様化しているクラウドサービスの形態に即した使いやすい基準となっているとは言い難いとの懸念が提起された。また諸外国において政府調達におけるクラウドサービスの要件が定義されつつある動きも受け、多様化するクラウドサービスにおいて、セキュリティの観点から重要となる情報の所在や管理状況が利用者には捉えづらい面もあるとのサービスの特性も勘案した上で、当該サービスの利用に当たり必要となる情報セキュリティ要件等を検討するための取組を行っていくこととしている。

その他、重要インフラに関しては、新たに追加された石油・化学・クレジットという３分野における情報共有体制の整備等、また、人材育成に関しては、サイバーセキュリティ人材の採用等に大きな影響力を有する経営層の意識改革等に資する施策等を推進し、我が国の情報セキュリティ環境の強化を図っていくこととしている。

[21] 「別添２　「サイバーセキュリティ 2013」に盛り込まれた施策の実施状況」を参照。

図表Ⅰ－4－1　「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（案）」の概要



図表Ⅰ－4－2　「サイバーセキュリティ2014」の概要

▸「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、対象期間:2013～2015年度)に基づく年次計画の2期目。

	2013	2014	2015
戦　略	「サイバーセキュリティ戦略」(2013/06/10)		
年次計画	「サイバーセキュリティ2013」(2013/06/27) • 戦略に基づき、各分野で新たな方針／プログラム等を策定	「サイバーセキュリティ2014」(2014/07/10) • 新たな方針／プログラム等を踏まえ、個々の施策をより具体化して推進	
「強靭な」サイバー空間	「政府機関統一基準群」改定(2014/05/19) 「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」策定(2014/05/19) 「情報セキュリティ普及・啓発プログラム」改定(2014/07/10)	【主な施策】 • 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(内閣官房及び全府省庁) • 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(内閣官房及び総務省) • 調達時における対策の推進(内閣官房) • GSOCの抜本的強化(内閣官房及び全府省庁) • 重要インフラに関する、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、防護基盤の強化(内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁) • 新たな情報セキュリティ普及啓発プログラムの策定・推進(内閣官房及び関係府省庁) • 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) • 日本版NCFTAの創設に向けた検討(警察庁) • 防衛情報通信基盤(DII)の整備(防衛省) • 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、防衛省及び関係省庁)	
「活力ある」サイバー空間	「情報セキュリティ研究開発戦略」改定(2014/07/10) 「情報セキュリティ人材育成プログラム」改定(2014/05/19)	【主な施策】 • 情報セキュリティ研究開発戦略の研究開発の推進(内閣官房及び関係府省庁) • 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) • 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) • 情報セキュリティに係る競技会・演習等の実施(総務省及び経済産業省) • 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)	
「世界を率先する」サイバー空間	「サイバーセキュリティ国際連携取組方針」策定(2013/10/02)	【主な施策】 • サイバー空間に関する国際的な規範作りへの参画等(内閣官房、総務省、外務省、経済産業省及び関係府省庁) • 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、経済産業省及び関係府省庁) • 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、外務省及び関係府省庁) • サイバー攻撃に関する諸外国関係機関との連携の強化(警察庁及び法務省) • 諸外国とのCSIRT間連携の強化(経済産業省)	
推進体制等	「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」(討議中)	【主な施策】 • NISCの機能強化(内閣官房) • 官民の情報共有の更なる推進(内閣官房及び関係府省庁)	

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

政府機関においては、Ⅰ章で述べた、政府機関統一基準群やリスク評価等に係る取組に加えて、情報セキュリティに関する各種取組を実施している[22]。本節では、各種取組のうちNISCを中心とした政府機関全体の取組の主なものについて示す。

(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が増大していることから、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実施する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・運用時から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「政府機関の情報システムの調達における情報セキュリティ要件策定マニュアル[23]」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、2013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。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、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実施しており、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[24]。

次に、近年多くみられる攻撃手口である標的型メール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なりすまし防止策の導入を推進[25]するとともに、府省庁の職員全般に対する標的型メールに対する教育訓練を行うなど、標的型メールによる不正プログラムへの感染を防ぐための対策を講じている[26]。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を実施し、対策の重点化による多重防御の実現に向けた取組を進めている[27]。

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、各府省庁CSIRT要員に対する研修を実施した[28]。今後は、標的型メールに対する教育訓練を各府省庁CSIRT要員に対する研修と併せて発展させ、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研修及び訓練を実施することを予定している。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

[22] 「別添２　「サイバーセキュリティ2013」に盛り込まれた施策の実施状況」の１①を参照。
[23] 「「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、2011年４月28日公表）http://www.nisc.go.jp/active/general/sbd_sakutei.html
[24] 「別添３－５　公開ウェブサーバの脆弱性検査結果の概要」を参照。
[25] 「別添３－４　なりすまし防止策の実施状況」を参照。
[26] 「別添３－３　教育・訓練に係る取組」を参照。
[27] 「別添３－２　高度サイバー攻撃への対処」を参照。
[28] 「別添３－３　教育・訓練に係る取組」を参照。

報セキュリティ緊急支援チーム（CYMAT：Cyber Incident Mobile Assistance Team）をNISCに設置しており、CYMAT要員の対処能力を向上させるための研修・訓練も実施している。

なお、2013年度におけるCYMATの活動として、６件の具体的な支援及び助言を行った。

2013年度においては、独立行政法人が標的となったサイバー攻撃事案が目立った[29]。その業務や扱う情報に鑑みれば、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必要である[30]。

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、政府機関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月に決定した[31]。

(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。

例えば、国立大学法人において複合機内部の情報がインターネット経由で外部から閲覧可能な状態となっていた事案が発生した際には、各府省庁の最高情報セキュリティ責任者等で構成される情報セキュリティ対策推進会議を開催し、複合機の利用実態及び対策状況の点検を実施するとともに、適切な対策を講ずることや所管法人等に対する指導を行うこと等について申し合わせるなど、政府機関全体として適切な対応に努めた[32]。

また、最高情報セキュリティアドバイザー等連絡会議においては、2013年度の情報セキュリティ対策状況を踏まえ政府機関の共通的な課題を抽出し、全府省庁での情報共有及び対策の検討を行った。当該会議においては、盗難・紛失による情報流出や不正プログラム感染につながるおそれのあるUSBメモリ等の外部電磁的記録媒体の利用に関して、漫然と技術的対策を講じるのでなく、明確な運用ルールを定め、それに応じた技術的対策を講ずることが重要であること、オンラインストレージ等の他の手段による情報の受渡しの仕組みを組織として整備するなど、外部電磁的記録媒体に依存しない運用についても検討する必要があること等を議論した。また、私物のスマートフォン等の業務利用に関して、単に一律に禁止するルールを定めるのみでは実効性が確保できないおそれがあることから、業務利用に係るニーズを踏まえたルールを明確とし、状況に合わせて技術的対策の導入も検討することが重要であることを確認した。

(3)　情報セキュリティ対策に係る教育

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重要である。

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自組織の職員に対して実施するとともに、NISCにおいては、上述の標的型メールに対する教育訓練、各府省庁CSIRT

[29] 「別添３－９　政府機関等に係る 2013 年度の情報セキュリティインシデント一覧」を参照。
[30] 「別添３－７　独立行政法人等の情報セキュリティ対策の現状について」を参照。
[31] 「別添３－８　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３－８　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。

要員に対する研修のほか、全府省庁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）を定例で開催している。

2013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、「安全なIT製品の調達に向けて」や「データベースにおける情報セキュリティ対策について」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[33]。また、独立行政法人職員を対象とした勉強会も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。

[33] 「別添３－３　教育・訓練に係る取組」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が確保される。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、2013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	対象項目
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

2013年度の本評価の対象者については、政府機関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、近年発生した事故・障害事案を踏まえつつ、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、これまでの点検の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

2013年７月から2014年３月まで
（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、政府機関統一基準群に基づく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、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、府省庁が把握した対策実施状況のうち、上述した実施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）　対策実施状況報告の結果

2013年度の政府機関全体の対策実施状況報告の結果は以下のとおり。

○　主体別の把握率の状況

主体別の把握率（報告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
98.8%	99.0%	99.4%	98.8%

※　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、点検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

	2011年度	2012年度	2013年度
責任者等	99.5%	99.6%	99.3%
システム責任者等	98.6%	97.9%	98.3%
行政事務従事者	95.9%	96.8%	96.8%
全主体平均	99.0%	98.9%	98.6%

図表Ⅱ－２－４　行政事務従事者の主な点検項目の実施率

点検項目	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	92.7%
情報の利用	98.2%
情報の保存	95.5%
情報の提供	95.4%
情報の消去	98.6%
主体認証情報の管理	97.3%
府省庁支給以外の情報システム	95.7%
不正プログラムの感染防止対策	98.6%

（イ）　所見

全主体平均の把握率は98.8%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を鑑みれば、全体的に高い水準を維持したと考えられる。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見受けられた。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・向上に不可欠であることから、今後更なる向上が望まれる。

責任者等の実施率は99.3％となっており、対策の浸透が認められ、引き続き、この水準を維持することが望まれる。特に課室情報セキュリティ責任者は、行政事務従事者に情報セキュリティ対策の教育を受講させる責務があるが、一部の組織においては、教育の実施率が低いところが見受けられた。組織全体の情報セキュリティ水準の向上のためには、行政事務従事者一人ひとりの情報セキュリティに対する意識の向上が重要であることから、着実に取組を進めていくことが望まれる。

システム責任者等の実施率は98.3％となっており、中でも、所管する情報システムの計画、構築・運用、移行・廃棄及び見直しの各段階において、情報セキュリティを確保するための措置を定めて適切に実施することを求める「情報システムのライフサイクル管理」については、前年度に比べて、全体的に実施率が向上するなど、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きている情報システムに関する対策については、万全を期すことが求められることから、更なる浸透が望まれる。

行政事務従事者の実施率は96.8％となっており、対策の浸透が認められる。点検項目のうち、「情報の作成と入手」については、前年度の実施率が相対的に低かった一部の組織において実施率の改善が見られたものの、政府機関全体としては他の項目と比べて低い数値となった。この数値が低いことは、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（どのように扱うべきと考えているのかを他人に認知させるための措置）が十分に実施されていないことを示しており、本対策が十分に実施できていない組織においては、速やかに改善措置を実施することが望まれる。

(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

2013年７月から2014年３月まで
（検査基準日：2013年11月１日）

ウ　主な検査内容

図表Ⅱ－２－５　重点検査の主な検査内容

対　象	検査項目	検査項目とした理由
公開ウェブサーバ	公開ウェブサイトが改ざんされる可能性についての確認状況	公開ウェブサイトが改ざんされると、改ざんされたウェブサイトの閲覧者のパソコンがウイルス感染するおそれがあるなどの影響を踏まえ、公開ウェブサイトの改ざんされる可能性の確認状況を把握するため。
	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について、対策の実施状況を把握するため。
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。
複合機	府省庁管理外のネットワークからの直接アクセスに係る複合機の対策状況	ネットワーク機能を持つ複合機を安全な状態で使用するための基本的な対策の実施状況を把握するため。

エ　主な検査結果

図表Ⅱ－２－６　重点検査の主な検査結果

対　象	検査項目	実施率
公開ウェブサーバ	公開ウェブサイトが改ざんされる可能性についての確認状況	97%
	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	95%
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	59%
複合機	府省庁管理外のネットワークからの直接アクセスに係る複合機の対策状況	100%

※小数点以下四捨五入

オ　所見

インターネット上で公開されているウェブサーバ（以下「公開ウェブサーバ」という。）において、そのウェブサイトが改ざんされる可能性があるか検査を実施した。併せて、公開ウェブサーバを管理する端末についても検査した。確認を行ったものは、公開ウェブサーバを持つ情報システム全数のうちの97%であり、その中にはウェブサイトが改ざんされる可能性があると判断された情報システムも把握されたが、それらについては、既に対策が完了した。

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。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95%であり、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、

また、公開ウェブサーバの脆弱性検査[34]の結果も踏まえると、今後も、SQLインジェクションの脆弱性への対策強化を推進していく必要がある。

電子メールの受信側における送信ドメイン認証技術の実施率は、電子メールを利用しているドメインの59%であり、各府省庁別にみると、ほとんどの府省庁において、電子メールを利用しているドメインの集約化と受信側における送信ドメイン認証技術の対策が進んでいることが確認されたが、一部の府省庁において、これらの取組が不十分であった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は、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する技術で、この結果を用いて受信した不審メールをフィルタリングするなどの対策を行うことができる。受信側における送信ドメイン認証技術を導入するためには、電子メールサーバへの機能追加が必要となることから、一定程度の予算措置が必要となるため、各府省庁で利用者の数が多いメールドメインを優先的に、かつ電子メールサーバの更新時期に合わせて措置することが求められる。

複合機については、複合機内部の情報がインターネット経由で外部から閲覧可能な状態となっていたものは無いことが確認され、基本的な対策は確実に実施されているものと認められるが、複合機は更に多機能化・高機能化することも想定されるため、最新の脅威に対抗できるよう、継続的に必要な対策を講じていくことが求められる。

このほか、サーバ集約化の観点から、各府省庁の公開ウェブサーバ及び電子メールサーバの台数を確認したところ、公開ウェブサーバは約600台（前年度約660台）、電子メールサーバは約770台（前年度約930台）であり、前年度と比較して更に集約化が進んでいる状況が確認された。また、第22回情報セキュリティ政策会議（2009年６月22日）で決定されたサーバ集約化計画の目標である2008年11月時点の政府機関の公開ウェブサーバ（約1,000台）及び電子メールサーバ（約1,900台）を、2013年度末までに政府機関全体として少なくとも半減することについては、達成が確認された。

ウィンドウズXP等のサポート対応終了（2014年４月９日（日本時間））に伴う対策状況については、検査時点において対策の目途がついていない府省庁も存在することが把握されたが、第14回情報セキュリティ対策推進会議（2013年12月12日）申し合わせのとおり、全府省庁において、サポート終了日までにソフトウェアを新しいものに入れ替えるなどの適切な措置を講じていることが確認された。今後とも、端末やサーバで使用するソフトウェアのサポート終了時期を念頭に置きつつ、計画的なシステム調達を行っていくことが求められる。

カ　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」及び「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・タブレット端末の府省庁における利用動向」に関して、主に電話や電子メール等の代表的な機能の利用のほか、ソーシャルネットワーキングサービスによる国民等に対する情報発信にも使用されていることが確認された。また、官支給

[34] 「別添３－５　公開ウェブサーバの脆弱性検査結果の概要」を参照。

品のスマートフォン・タブレット端末の情報セキュリティ対策の実施状況として、端末のセキュリティロック、OSの最新化等の基本的な対策はおおむね講じられていることが確認された。今後もスマートフォン・タブレット端末等の技術動向や利用環境における脅威の変化等を考慮し、対策を強化することが求められる。

なお、私物端末等の官支給品以外のスマートフォン、タブレット端末を業務に活用していくことも考えられるが、私物の端末を業務に使用する場合であっても官支給品と同等の対策水準を保つ必要があることから、その実施に当たっては、管理手順や安全管理措置等に係るマニュアルの整備についても検討する必要がある。

「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、主に外部への情報発信及び外部との情報共有のために利用されていることが確認された。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は、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の約60％が政府機関統一基準群で定める要機密情報を取り扱っておらず、残りの約40％も情報の保存場所を国内に限定するなどの対策が実施されていることが確認された。要機密情報のほか、完全性・可用性の確保が求められる情報を取り扱う場合は、業務データの適切な管理が重要であり、引き続き対策強化を進める必要がある。

さらに、パブリッククラウドサービスの利用において講じられている情報セキュリティ対策の実施傾向については、委託先による情報アクセス先の制限、情報の改ざんや消失等への対策に係る事業者との合意、契約満了後の情報の抹消等が確認されたほか、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）により要求しているものや、システムインテグレータによるセキュリティ運用の補完を行っているものなどが見受けられた。パブリッククラウドサービスの利用に当たっては、当該サービスの特性及び取り扱われる情報に応じた情報セキュリティ対策が必要であることから、適切な対策が講じられるよう、継続的に検討を進める必要がある。

Ⅲ　重要インフラ事業者等における対策状況の成果と課題

「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）」（以下「第２次行動計画」という。）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）」及び「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）」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、2009年度以降、当該行動計画に沿った施策の推進が図られてきた。

本章は、2013年度をもって第２次行動計画の期末を迎えるに当たり、諸施策の実施状況を点検し、成果と課題をとりまとめたものである[35]。

１　成果

今回、これら施策群の評価を行うに際し、第２次行動計画は2009年時点での重要インフラを取り巻く最新の知見を踏まえて策定されたものであることを考慮した。第２次行動計画における所期の目標については一定の成果を挙げたと評価できるものであった。

安全基準等の整備及び浸透については、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指した結果、指針と安全基準等の一体的・安定的な見直しサイクルを確立し、情報セキュリティ対策の啓発推進等を強化した。

情報共有体制の強化については、刻々と変化する重要インフラの情報セキュリティを取り巻く社会環境や技術環境及び複雑・巧妙化するサイバー攻撃等に対応することを目的に、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター及びセプター間における情報共有体制の整備及び重要インフラ事業者等における必要情報の享受・活用を実現した。

共通脅威分析については、重要インフラ全体の防護能力の維持・強化に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った結果、重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映した。

分野横断的演習については、IT障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じて相互の連絡・連携における仕組みの検証機会の提供に取り組んだ結果、演習参加組織数・人数は増加傾向にあり、演習で得られた知見に基づく重要インフラ事業者等のIT障害時の早期復旧手順及び事業継続計画等の検証を通じた情報セキュリティ対策に貢献した。

環境変化への対応のうち広報公聴活動については、重要インフラの情報セキュリティ施策の結果資料、重要インフラ専門委員会の会議資料等を内閣官房のウェブサイトに掲載し、公表するとともに、情報セキュリティ政策に係る講演等を行った。リスクコミュニケーションの充実については、情報セキュリティに係る関係機関との意見交換会の開催、セプターカウンシルにおける相互理解WGの開催を行った。国際連携の推進については、MERIDIAN会合、CyberStorm演習への参加等を通じて諸外国との連携を行った。こうした取組を通じて、環境変化に伴う脅威の察知能力の向上に努めた。

[35] 第２次行動計画は、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析」、「分野横断的演習」、「環境変化への対応」の５つの施策群から構成されており、各施策に係る詳細については別添４－１にて示す。

２　課題

各施策の実施を通じて、社会・技術面での環境変化を踏まえた改善・補強を要する課題も抽出された。各施策の主たる課題を以下に記載する。

安全基準等の整備及び浸透においては、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・強化にも効力が及ぶこと、重要インフラ事業者等から対策の実情を踏まえた段階的な（優先順位付けされた）指針の提示要望があること等から、各重要インフラ事業者等の情報セキュリティ対策に資することを目的に、重要インフラ事業者等のPDCAサイクルとの整合に基づく見直しが課題である。

情報共有体制の強化においては、実効性のある情報共有体制の構築を目的に、分野間における情報共有頻度の格差の解消、「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について、平時の体制の延長線上への構築、新たな関係主体との連携の在り方の整理等が課題である。

共通脅威分析においては、共通脅威分析の対象・位置付けや実施頻度の見直しに向けて、調査対象を全分野の共通脅威に限定せず、全分野に及ばずとも影響が大きな脅威を調査対象に加える運営に係る検討や、効果性を高めるため、時間的経過や環境変化の顕在化に応じた脅威等の詳細分析等が課題である。

分野横断的演習においては、区々である各組織のIT利用形態や情報管理態勢から演習環境の設定に限界があり、大幅な参加者拡大が望めない。このことから、重要インフラ事業者等における情報セキュリティ対策の課題抽出機会の提供を目的に、参加者拡大のみに依存せず、演習成果の更なる普及・浸透を重要インフラ分野全体に図ることが課題である。また、演習評価に基づく運営の質的改善、重要インフラのIT障害発生時の対応を踏まえた関係主体の在り方の検討、並びに重要インフラ所管省庁及び防災関係省庁が主催する演習・訓練との連携についての検討が課題である。

環境変化への対応のうち広報公聴活動においては、次期行動計画における本施策と他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しが課題である。リスクコミュニケーションの充実においては、国際標準と整合したリスクマネジメントの定義、機微情報の秘匿と情報の有用性のバランスを念頭に置いた情報共有の見直し、及び中長期的な実現・利用と脅威の影響の大きさが予想される新たな情報通信技術等を対象にした環境変化のテーマに係る中長期的な継続調査・検討が課題である。国際連携の推進においては、国境を越えて形成されたサイバー空間において深刻化・グローバル化するリスクへの迅速な対応に向けて、諸外国との連携推進を継続するとともに、ASEAN等のアジア太平洋地域や欧米等の二国間、多国間、地域的枠組みの積極的な活用を通じた国際連携の強化が課題である。

以上の第２次行動計画における成果・課題や、重要インフラの範囲の見直し等のサイバーセキュリティ戦略において検討を求められた課題などを踏まえ、第２次行動計画を策定してから５年の間に生じた、社会・技術面での環境変化等を加味した上で、サイバーセキュリティ戦略と整合する第２次行動計画の基本的骨格を維持しつつ、個別の施策やその実施体制を見直し、必要な補強・改善を行った次期行動計画として、2014年５月に、「重要インフラの情報セキュリティ対策に係る第３次行動計画」を策定した。

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最初の年次計画である「サイバーセキュリティ2013」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25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2013」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[36]。

しかしながら、今後とも、あらゆる活動の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、NISCの機能強化、2020年東京オリンピック・パラリンピック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、別途策定された2014年度の年次計画「サイバーセキュリティ2014」に沿って、戦略策定後に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】

新たな脅威・技術への対応及び規定内容の実効性向上を目的とした政府機関統一基準群の改定、高度化する標的型攻撃等に対応するためのリスク評価に係る取組等の各種施策の着実な実施（取組状況についてはⅡ章参照）のほか、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・啓発に係る取組等を推進した。また、「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」の改定等の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】

2014年度は、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、その進捗状況の把握や支援等を行うほか、リスク評価に係る取組については、引き続き、各府省庁のCISOがガバナンス機能を発揮し、標的型攻撃を始めとした高度サイバー攻撃の標的となる蓋然性が高い業務を特定してリスク評価を行い、限られた人員・予算の中で重要な業務・情報を守るために必要な情報セキュリティ対策を計画的・重点的に実施するための枠組みの構築を図る。

加えて、Ⅰ章で述べたクラウドサービスに関する検討、Ⅱ章で述べた独立行政法人における情報セキュリティ対策の推進、情報セキュリティインシデント発生時の連絡体制強化を行う。

[36] 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 2013」に盛り込まれた施策の実施状況」を参照。

②　重要インフラ事業者等における対策

【総　評】

2013年度は2009年に策定した「重要インフラの情報セキュリティ対策に係る第２次行動計画」の最終年度に当たり、第２次行動計画の施策を着実に実施し、第２次行動計画における所期の目標については一定の成果をあげたと評価できるものであった。

また、第２次行動計画の成果と課題をとりまとめ、第２次行動計画の基本的な骨格を維持しつつ、第２次行動計画の課題等を踏まえた修正・補強を行った「重要インフラの情報セキュリティ対策に係る第３次行動計画」を策定した。

【課　題】

新たに策定した第３次行動計画に基づき、内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁及び事案対処省庁の関係各主体において、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」及び「防護基盤の強化」に関する施策を実施する等により重要インフラ事業者等における情報セキュリティ確保に資する取組を実施していく必要がある。

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、政府機関や重要インフラ事業者等における情報セキュリティ対策のより一層の強化に取り組んだ。また、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支援、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、情報システム調達時における情報セキュリティの確保の支援、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着実に実施した。

【課　題】

我が国の国際競争力の源として重要な営業秘密等の企業秘密、知的財産情報や個人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、サイバー攻撃に関するインシデント等の認知・解析機能を引き続き強化していくことが求められる。また、サイバー攻撃がグローバル化する中、インシデント情報の共有促進や、企業等の海外進出先における情報セキュリティ対策を促進することは重要であり、今後も引き続き関係者間で協力し各種取組を引き続き推進していく。

④　サイバー空間の衛生

【総　評】

情報セキュリティ普及啓発については、各府省庁と連携し、毎年２月の「情報セキュリティ月間」における関連行事の開催、各府省庁・関係機関ホームページにおける周知等従来の取組に加え、「サイバーセキュリティの日」（２月の最初のワーキングデー）を新設したほか、「情報セキュリティ普及啓発ロゴマーク」を策定し、期間を問わず、各種メディア等を通じ

た情報発信をするなど、「情報セキュリティ普及・啓発プログラム」に基づき、普及啓発活動の充実・強化を進めた。

また、普及啓発に関する国際連携については、2013年10月に「サイバーセキュリティ国際連携取組方針」を策定し、その推進に取り組んでいるほか、毎年10月の「情報セキュリティ国際キャンペーン」の実施や、共同意識啓発教材の作成等を通じ、ASEAN、欧米諸国等と情報セキュリティ対策に関する連携を進めるなど、取組が進んでいる。

【課　題】

「情報セキュリティ普及・啓発プログラム」に基づく「情報セキュリティ月間」等を通じ、産学官民の連携構築が図られるなど、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は、全国的にみて未だ少数であることから、情報セキュリティに関する国民全体の機運をさらに向上させる具体的な取組方策について、新たに策定した「新・情報セキュリティ普及啓発プログラム」に基づく施策の推進の中で検討していく必要がある。

⑤　サイバー空間の犯罪対策

【総　評】

捜査機関におけるサイバー犯罪対策のための人材育成を強化するとともに、警察庁に「サイバー攻撃対策官」及び「サイバー攻撃分析センター」を、13都道府県警察に「サイバー攻撃特別捜査隊」を設置するなど、サイバー犯罪・サイバー攻撃に対する各種態勢が整備された。また、警察と民間事業者等の間で、不正プログラムの検体やサイバー空間に関する知見等の情報共有、サイバーテロ対処に関する共同訓練等、官民連携した取組が強化された。

【課　題】

2013年に入り急増しているインターネットバンキングに係る不正送金事犯等にみられるように、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）」等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】

サイバー防衛隊の新編、ネットワーク監視態勢の強化等を通じて、防衛省・自衛隊の対処態勢が強化されたほか、サイバー攻撃に関する関係機関の役割の整理・明確化を図るため、情報セキュリティ政策会議において、NISCの機能強化等に関する検討がなされるなど、所要の取組が進められている。

【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、関係府省庁個々の能力・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、海外市場において収集するサイバー攻撃等に関する動向を踏まえ、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、自動車に係る情報セキュリティの確保等が実施された。

【課　題】

高度な技術や製品等と、それらを創り出す先端的な研究者や技術者については、情報通信技術の普及・高度化と、その利活用の進展にとっての不可欠の基盤となるものである。このため、情報通信技術の利活用の裾野拡大による多様な分野におけるサービス革新・生産性の向上や、新ビジネスの創出において情報通信技術の利活用が重要となる中、これらと一体となって情報セキュリティ対策に関する高度な技術の研究開発、国際標準化や評価・認証を含んだ制度整備等を推進していく必要がある。

②　研究開発

【総　評】

サイバーセキュリティ戦略等を踏まえ、「情報セキュリティ研究開発戦略（改定版）」の策定に係る検討を情報セキュリティ政策会議の下の技術戦略専門委員会において実施した。

また、日々高度化・巧妙化するサイバー攻撃等に対応するため、標的型攻撃の対策技術に関する研究開発、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、制御システムセキュリティに関する研究開発等の各種研究開発が実施された。

【課　題】

サイバー攻撃の複雑・巧妙化に伴い、従来の情報セキュリティ対策のままでは、有効な対策の立案・実施に遅れが生じ、効果が急低下する可能性がある。このため、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。

このため、「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実施していく必要がある。具体的には、①サイバー攻撃の検知・防御能力の向上、②我が国の社会システム等を防護するためのセキュリティ技術の強化、③産業活性化につながる新サービス等におけるセキュリティ研究開発等に関する施策を推進していく。

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。

また、情報セキュリティ人材に係るキャリアパス・モデルの普及やスキル、資格、教育プログラムの整理、経営層向けのセミナーの開催等により、企業における人材育成の支援を行うとともに、複数大学や産学連携による高度で実践的な教育活動の支援や情報セキュリティに係る競技会の実施等により、優秀な人材の発掘及び更なる能力の向上が図られるなど、情報セキュリティ人材の育成に資する施策が着実に推進された。

【課　題】

サイバー空間の脅威の深刻化に対応するため、人材の育成は引き続き重要な課題となっている。現在、情報セキュリティ人材は、量的にも質的にも不足しているとされており、これまでも取り組んできた高度な人材の育成・発掘に加え、量的な対策として、組織の中で実務を担うボリュームゾーンである既存の情報通信技術に携わる技術者に情報セキュリティを必須能力として位置付ける取組や、訓練・演習教材等の作成、能力評価基準・資格のあり方等について検討し、人材の供給を推進することが求められる。

他方、そうした人材を雇用する側、すなわち組織経営層等の情報セキュリティに対する意識が未だ十分ではなく、脅威に見合った人材の需要が生まれていないのが現状である。我が国の情報セキュリティの水準向上に向けては、これらの問題を解決し、今後「人材の需要と供給の好循環」を生み出していくことが必要である。このため、人材の供給だけでなく、需要側に対するアプローチとして、例えば、情報セキュリティを事業継続に不可欠な経営戦略として経営層に認識させるための取組や、製品・サービスの調達における情報セキュリティの要件化を通じた提供側の意識改革に政府が率先して取り組むことが重要である。

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、「情報セキュリティ普及・啓発プログラム」に基づき、各種の普及啓発施策が着実に推進された。

具体的には、初等中等教育段階においては、各地域の指導主事に対する研修や教員向け指導手引書の作成等を通じ、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が図られた。また、高齢者等リテラシーの強化が必要とされる層に向けて、ウェブサイトやリーフレット等を通じた相談窓口の紹介や情報セキュリティ・サポーターを育成するための方策に関する調査が行われ、より効果的な普及啓発に向け検討が進められた。

また、スマートフォンやソーシャルメディア等の情報セキュリティの確保に向けては、利用実態の調査及び事業者への結果提供、留意すべき課題や注意点等をまとめたテキスト等の作成・配布、スマートフォンの特徴に適合したフィルタリングの開発支援等の取組が推進され、一定の進捗が図られた。

【課　題】

「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等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。一方、国民の中には、どこまで情報セキュリティ対策を行えばよいか不明である、情報セキュリティに関する脅威が難解で理解できないとする声も未だ多く、そうした国民一人一人に届き、自らの実践につながる普及啓発活動の推進が引き続き課題である。

このため、今後、国民に身近な地域が主体となった行事の活性化や、親しみやすいメディア等を活用した普及啓発活動が期待されるところであり、そのための環境整備について、新たに策定した「新・情報セキュリティ普及啓発プログラム」に基づく施策の推進の中で検討していく必要がある。

3　「世界を率先する」サイバー空間の構築

①　外交

【総　評】

米国、EUを始めとする各国との二国間協議の推進や国連、OECD、APEC、MERIDIAN等の場での国際的な規範作りに関する議論や国際対話への参画を通じ、サイバー空間に関する国際的なコンセンサス獲得や情報共有体制の構築、信頼醸成措置の促進に関して多角的な議論の進展に寄与している。また、2013年10月には、「サイバーセキュリティ国際連携取組方針」を策定し、こうした二国間又は多国間の協議に積極的に関与していくことを表明した。

【課　題】

サイバー攻撃の複雑・巧妙化に伴い、サイバー攻撃等のリスクの増大への対応は我が国一国だけでは困難なことから、連携の強化が推進されている米国、ASEANとの協力や国連やAPECといった国際的な場において、政府一体となった二国間連携や多国間連携の強化を深化させていくことが必要となっている。2014年に入り、我が国は、エストニア、豪州、フランス等との間で、二国間のサイバー対話等を立ち上げることに合意しており、こうした協議を通じ、グローバルな共通認識の醸成等に積極的かつ具体的に寄与していくことが重要となっている。

②　国際展開

【総　評】

ASEAN各国との間では、「日・ASEAN情報セキュリティ政策会議」の枠組みを通じた「日・ASEAN情報セキュリティ意識啓発イニシアチブ」の取組を継続し、情報セキュリティポスターやリーフレット、意識啓発アニメーションの作成、国際シンポジウムの開催などの取組を行うなど、協力関係の強化が進んだ。2013年においては、情報セキュリティに関する初の閣僚級の会議となる「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催し、技術協力や人材育成等における連携の推進等について合意するなど、国際連携の強化が進展した。また、海外CSIRTの構築、体制強化等の分野においても、第三国と連携し、アジア、アフリカでの研修を実施するなど、CSIRT間の連携が図られたほか、サイバー犯罪対策のための司法制度整備、捜査技術向上に関しても各種の会議、ワークショップを開催するなど国際的な連携に寄与している。

【課　題】

近年、サイバー空間を取り巻く脅威が複雑、巧妙化、さらにグルーバル化する状況を踏まえ、各国との連携を拡大・強化していくことが必要である。また、サイバー攻撃がグローバル化する中では、キャパシティビルディングの重要性も増してきており、「サイバーセキュリティ国際連携取組方針」に基づいて、更に情報セキュリティ対策を進めていくことが求められている。

③　国際連携

【総　評】

MERIDIAN、IWWN、FIRST等の各種の国際会議への参画や諸外国の関係機関との情報交換等を通じ、諸外国とのベストプラクティスの共有やCSIRT間の連携強化を図るとともに、我が国の「サイバーセキュリティ戦略」や「サイバーセキュリティ国際連携取組方針」等について情報発信を行うなど、国際的な窓口機能の強化に取り組んでいる。また、アジア大洋州地域サイバー犯罪捜査技術会議の開催等サイバー犯罪の取り締まりのための国際連携に向けた協力関係の構築や各種国際会議の場におけるサイバー犯罪条約の普及にも努めた。

【課　題】

国際会議への参画や外国関係機関との協力・連携を進めていく一方で、国際会議等を通じて把握した国際動向、海外のベストプラクティス等について、政府内で情報共有を進め、政府一体となった国際連携を効率的に進めていく必要がある。

4　推進体制等

【総　評】

サイバーセキュリティの強化を含む国家安全保障戦略が策定（国家安全保障会議決定及び閣議決定）されたことを踏まえ、第38回情報セキュリティ政策会議（2014年１月23日）において、NISCの機能強化等に関する検討を開始した。また、「サイバーセキュリティ戦略」に則り、情報セキュリティ政策会議を結節点としてIT総合戦略本部、総合科学技術会議、知的財産戦略本部などの関係機関及び関係府省庁、重要インフラ事業者等とのサイバーセキュリティに係る連携強化、情報共有の推進等に努めた。

【課　題】

我が国のサイバーセキュリティの推進体制については、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔としての位置付けを明確化し、政府機関の情報システムに関するセキュリティ監査機能の強化、専門的人材の配備・育成、脅威情報等の集約・共有化、国際的窓口機能の強化等、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の体制及び組織の強化を図っていく必要がある。

別添１　各府省庁における情報セキュリティ対策に関する取組

＜別添１－目次＞

内閣官房

平成25年度の総合評価及び平成26年度の全体方針

平成25年度にインターネットにおいて発生した情報セキュリティ事案を振り返ると、特定の利用者にのみウイルス感染を発生させるWebサイト改ざん事案や、ソフトウェアのアップデートプログラムをすり替えてウイルスに感染させる事案といった、高度な技術を用いて政府機関の情報の窃取を試みるといった事案が発生しております。

これらに対応するためには、サイバー攻撃に関する情報の収集・分析、ソフトウェアに関する脆弱性情報の入手及びシステムへの適用、職員に対する注意喚起や情報セキュリティ教育の充実などが重要となります。内閣官房においては、幸いにもウイルス感染や情報漏洩といった重大な事案は発生しておらず、これまで実施してきたこれらの情報セキュリティ対策が一定の効果をあげていると言えるでしょう。

しかし、日々技術が進歩する情報セキュリティ対策には、ここまでやれば良いといった終わりはありません。2012年に開催されたロンドンオリンピックでは２億件を超えるサイバー攻撃があったと言われていることを踏まえると、2020年に東京オリンピックの開催が予定される日本においては、今後、サイバー攻撃が一層増加していくことが容易に想像できます。内閣官房としてサイバー攻撃に対抗するためには、システムを用いた防御策を講じることはもちろんですが、職員一人ひとりが危機意識を高め、サイバー攻撃に備えることが重要です。

サイバー攻撃に対抗する職員の備えとは、何もコンピューター技術だけではありません。攻撃者が情報窃取を行うためには、マルウェアを組織内ネットワークで活動させる必要がありますが、そこには「どのようにすれば職員がマルウェアを実行するか」という視点、ソーシャル的要素が強い攻撃手法が使われます。マルウェアそのものは新しい技術を用いるのかもしれませんが、手口は古くからある「人を騙すテクニック」が用いられます。最近ではソーシャルハッキングと呼ばれていますが、要は人の心理的な隙を突いた詐欺のようなものです。これに対抗するためには、多くの経験を積むのが有効だと考えられますが、実際に被害にあっては困ることから、職員教育による擬似的で実践的な経験の積み重ねが重要になると思います。

そのような背景を踏まえ、平成26年度においては、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必要があると考えます。また、５月19日には、政府機関の情報セキュリティ対策の統一基準群が抜本的に見直され、改正されたことから、最新の情報セキュリティ情勢に対応すべく、内閣官房セキュリティポリシーについても、できるだけ早期に全面改正してまいりたいと考えます。

最高情報セキュリティ責任者
内閣総務官
河内　隆

内閣法制局

平成25年度の総合評価及び平成26年度の全体方針

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ります。

平成25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、内閣官房情報セキュリティセンター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、内閣官房情報セキュリティセンターが実施した標的型メール攻撃に対する教育訓練への参加、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、内閣官房情報セキュリティセンターからの情報セキュリティについての情報提供及びCISO等連絡会議での申し合わせ事項等に迅速かつ適切に対応しました。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ましたが、その結果については問題となるところはありませんでした。このような取組、対策等を実施した結果、平成25年度においても情報セキュリティインシデントの発生はなく、内閣法制局における情報セキュリティ対策は適切なものであったと評価しています。

平成26年度においては、平成25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、内閣官房情報セキュリティセンターからの情報提供やCISO等連絡会議での申し合わせ事項等に応じて、引き続き、適切な情報セキュリティ対策を実施します。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標的攻撃型メール訓練の実施等により、インシデントの発生防止を図ります。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、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います。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・向上に努めてまいります。

最高情報セキュリティ責任者
（内閣法制局総務主幹）
高橋　康文

人事院

平成25年度の総合評価及び平成26年度の全体方針

人事院では、政府における情報セキュリティ政策会議で決定する計画等に基づき、内閣官房情報セキュリティセンターと連携しつつ、情報セキュリティ対策を実施してきているところです。

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ます。

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と認識しています。

平成25年度は、人事院では、平成24年度に新しく整備したCSIRT体制の下で、サイバー攻撃を受けた場合に、CISOを中心に逸早く情報の集約が行われ、有効な対策が機動的に講じられるよう体制の充実を進めるとともに、USBの使用を「セキュリティUSB」に限ることで不正プログラムの侵入を未然に防ぐ対策を講じるなどの機械的な整備にも取り組み、組織とシステムの両面からセキュリティ対策の強化を進めてきたところです。

また、「人事院情報セキュリティポリシー」に基づき、情報セキュリティ対策の推進体制を整備するとともに、職員一人ひとりが情報セキュリティの重要性を認識できるよう、わかりやすい小冊子を作成して配付する等教育に力を入れました。これらの施策のほか、例年どおり自己点検及び監査により情報セキュリティ対策の評価を行いました。

平成26年度は、政府における統一基準の改訂が予定されているところ、それに準拠する人事院情報セキュリティポリシーの整備を進めるとともに、継続的に実効性のある情報セキュリティ対策を実施していきます。

最高情報セキュリティ責任者
（人事院事務総局総括審議官）
永長　正士

内閣府

平成25年度の総合評価及び平成26年度の全体方針

○平成25年度の総合評価

・教育・啓発に関する取組状況

内閣府本府情報セキュリティポリシー及び情報セキュリティポリシー技術基準（以下、内閣本府ポリシー・同技術基準）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ました。また、新規採用職員の研修においてもセキュリティ教育の概要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ました。

さらに、NISCとの協力により、全職員を対象とする標的型メール攻撃訓練を行い、結果と対処方法について各部局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いました。

・自己点検・監査の結果

職員の情報セキュリティ対策の実施状況を自己点検により行った結果、実施率99.9%を達成しました。また、監査については、平成25年度の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、自己点検どおりに完全実施していることを確認することが出来ました。

・NISCによる情報システムに関する重点検査の結果

今回の重点検査では、Microsoft Windows XPのサポート終了に対する基幹LAN上の状況の検査が追加されたが、内閣府LANに接続する端末機器のOSはWindows7であることを確認しました。また、ネットワークに接続する複合機の安全性に関する検査についても、問題が無いことを確認しています。

・平成25年度に発生した情報セキュリティインシデント

① 平成25年７月22日、交通安全総合ネットワーク「Cross Road」(内閣府ホームページに掲載)に対する断続的な不正アクセスが確認された事実を公表するとともに、サイトを利用する全登録者に対して説明を行いました。当該サイトは、一旦閉鎖し、動的サイトから静的サイトへの見直しを行った後、再開しました。

② 平成25年10月11日、内閣府職員のメールアドレスを詐称した電子メールが各方面に配信されているとの情報を受け、事実確認の後、内閣府ホームページ上で注意喚起を行うとともに、報道関係者にも連絡しました。

・CISO等連絡会議での申し合わせ事項等

平成25年７月11日、グループメールサービス利用に伴う情報漏出事案に関して杉田内閣官房副長官より指示された「再発防止策等の徹底について」に基づく内閣府情報セキュリティ責任者（大臣官房長）訓示を各部局情報セキュリティ責任者を集め行いました。

さらに、内閣府では「例外措置申請」手続の運用徹底を図るために「非政府ドメイン(Twitter, Facebook 等のSNS, 外部サービス）利用時の例外措置申請におけるチェックリストの利用について」を新たに定め、課室情報セキュリティ責任者に加え、大臣官房情報システム室長にも提出を義務付けるなど審査の厳格化を図りました。

○平成26年度の全体方針

内閣本府ポリシーの遵守徹底の為に、全職員に対して、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e-ラーニングを利用した職員への教育や、新人研修の場における周知徹底を図ります。

特に、SNSによる情報発信手段が政府関係機関でも広く利用されている現状を踏まえ、内閣府本府ポリシーにおける「例外措置申請」手続の運用徹底・周知に一層努めることにより、SNS利用にあたっての管理を適切に行い、障害事故防止に努めます。また、統一基準群の改定後は、速やかに内閣本府ポリシーの整備を実施するよう努めます。

最高情報セキュリティ責任者
（大臣官房長）
幸田　徳之

宮内庁

平成25年度の総合評価及び平成26年度の全体方針

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っています。

また，昨今は政府機関等に向けられた「標的型メール」等のサイバー攻撃が頻発しており，これに迅速かつ適切に対処するためには，当庁の職員一人ひとりが情報セキュリティ対策についての正しい知識を持ち，意識を一層高く保つことが求められます。

このことを踏まえ，平成25年度においては，これまでに引き続き，職員に対する情報セキュリティ教育の充実を図りました。

具体的には，当庁では，年度計画に基づく定期研修として，集合研修や自習教育を実施しており，集合研修については，初級及び中級の２つの段階に分けて，それぞれ年２回，対象者の業務上必要となる知識レベルに応じた教育を実施しています。また，定期研修のほかに，随時，新採用職員等に対する研修も行っています。

これらの研修で用いる教材については，情報のライフサイクルにおけるセキュリティ対策や日常的に使われるインターネットやメールにおける対策等について，国内で発生したセキュリティ事故の実例を紹介しながら，具体的かつ最新の動向を踏まえた説明を行うようにしています。

また，当庁では，これまでにも職員に対する「標的型メール」訓練を実施してきましたが，平成25年度においては，新たに，「やりとり型」の訓練を実施いたしました。

これらにより，情報セキュリティ上の脅威に対する職員の理解が深まったと考えられますが，情報セキュリティ対策実施状況の自己点検の結果では，到達率が100％に達していない事項も見られることから，なお改善の余地があるものと考えています。

平成25年度は，当庁において情報セキュリティインシデントは発生しませんでした。

平成26年度の全体方針としては，政府機関の情報セキュリティ対策のための統一基準群の改定に伴い，当庁の情報セキュリティポリシーの見直しを行い，職員への周知を図ります。また，巧妙化されるサイバー攻撃に対応できるよう，引き続き，教育・訓練を充実させるとともに，情報システムについても，リスク評価の結果を踏まえた対策の導入を推進していきます。

今後とも，様々な事態等を想定しつつ，引き続き情報セキュリティの維持・向上に努めてまいります。

最高情報セキュリティ責任者
宮内庁　審議官　和田裕生

公正取引委員会

平成25年度の総合評価及び平成26年度の全体方針

１　平成25年度の総合評価

公正取引委員会では，平成25年度において，NISCと連携を図りつつ，以下を始めとする対策を実施し，情報セキュリティを万全なものとするための対策を講じています。

その結果，いずれの取組についても，職員の意識向上が図られました。

(1) 教育・啓発に関する取組状況

情報セキュリティ対策に関し，e-ラーニング研修，集合研修やITパスポート取得を目指した研修を重点的に実施し，職員の情報セキュリティ対策への理解の向上を図りました。

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重点的に取り組んだ結果，平成24年度より職員の理解の向上及び意識の向上が図られました。

(2) 自己点検・監査の結果

平成24年度の自己点検結果を踏まえ，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，全職員の情報セキュリティ対策の実施率は，平成24年度と比較し改善しました。

(3) 情報システムに関する重点検査の結果

３項目について一部改善の余地があるとされたものの，その他の項目は問題なしとする結果となりました。

(4) 平成25年度に発生した情報セキュリティインシデント

情報セキュリティインシデントは発生しませんでした。

(5) CISO等連絡会議での申し合わせ事項等

「グループメールサービスの利用に関する事案の再発防止策（平成25年７月30日情報セキュリティ対策推進会議）」を受けて，①体制強化として，最高情報セキュリティ責任者を補佐し，最高情報セキュリティ責任者の指示を受けて情報セキュリティに係る事務を行う者を組織・体制に位置付ける，②全職員を対象に特別研修の実施，③情報セキュリティ強化週間を設け，集中的に職員のセキュリティ意識の向上を図るといった対策を実施しました。

２　平成26年度の全体方針

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っていきます。

(1) 職員に情報セキュリティ対策の実施を促すため，職員が実施すべき対策の周知，研修内容の見直し等を行います。

(2) 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，訓練等を行います。

(3) 平成25年度の情報システムの重点検査の結果に基づき，改善に取り組みます。

(4) 平成26年度改定予定の統一基準群に準拠した，新たな公正取引委員会情報セキュリティポリシー等の策定を行います。

最高情報セキュリティ責任者
（官房総括審議官）
山田　昭典

警察庁

平成25年度の総合評価及び平成26年度の全体方針

A）平成25年度の総合評価

ア）情報セキュリティ対策の実施状況

職員の情報セキュリティに対する理解の醸成を図るため、毎年度、情報セキュリティの維持の実施状況の自己点検を実施しているところ、平成25年度についても、警察情報セキュリティポリシーに規定されている事項が遵守されていることを確認しました。また、情報システムにおける情報セキュリティ対策の徹底のため、ウェブサーバ、電子メールサーバ、複合機等を対象に検査を実施したところ、必要な対策が実施されていることを確認しました。

イ）監査の状況

情報セキュリティ対策の実施状況を確認し、対策の徹底を図るとともに、その効果を高めていくために、毎年度、情報セキュリティ監査（以下「監査」という。）を実施しています。監査を実施した結果、情報セキュリティに関する教育の実施等、積極的な取組が見られた一方、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見られたことから、改善結果について報告を求めました。

ウ）教育・啓発に関する取組

警察庁においては、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、標的型メール対処訓練を実施しました。本訓練を通じて、メールを不用意に開封することでウイルス感染が起こり得ることを周知し、注意を呼び掛けました。また、職員に対する教育訓練等を行う機関において、情報セキュリティに関する講義を実施するなどし、職員の情報セキュリティに対する理解の醸成を図りました。

エ）情報セキュリティに関する障害・事故等への対処

警察庁においては、警察庁CSIRTを設置し、警察内部における情報セキュリティインシデントに対し、迅速かつ組織的に対処しています。平成25年度については、不正プログラムの感染の疑いのある検知事案への対処、情報セキュリティインシデントの未然防止活動等を実施しました。

B）平成26年度の全体方針

これまでも、情報セキュリティを確保するため、技術的対策に加え、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ところですが、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、標的型メール攻撃に関する訓練を始めとした対策を講じていくこととします。また、常に変化する情報セキュリティをめぐる状況や、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、警察情報セキュリティポリシーの改定についても検討していくこととします。

最高情報セキュリティ管理者
（警察庁情報通信局長）
佐野　淳

金融庁

平成25年度の総合評価及び平成26年度の全体方針

(1) 平成25年度の評価

金融庁においては、従来から情報セキュリティ対策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すが、平成25年度においては、昨今の情報セキュリティ事案を踏まえ、以下の情報セキュリティ対策を実施しました。

① 情報セキュリティ教育・啓発の取組状況

職員に情報セキュリティに関する知識を浸透させるため、情報セキュリティ研修を年度中に15回開催し、全職員が受講しました。研修では、近年頻発している標的型メール攻撃の概要、対応手順等についても説明しています。

また、平成26年３月18日（サイバー訓練の日）にNISCと協力してサイバー攻撃対処訓練を実施し、庁内CSIRTや重要インフラを含めた情報収集・共有態勢を確認しました。

② 情報セキュリティ自己点検の結果

全職員及び点検対象となる情報システムに対して、情報セキュリティ対策の実施状況に係る点検を行った結果、概ね適切に実施されていることを確認しました。

③ 情報セキュリティ監査の結果

政府統一基準及び金融庁情報セキュリティポリシーに基づき、情報セキュリティ監査を実施し、いくつかの指摘を受けております。指摘を受けた問題については、監査対象の情報システムを管理する部署が改善に取り組んでおります。

④ 情報システムに関する重点検査の結果

平成25年度において、情報システムに関する重点検査を実施し、概ね適切に対策が実施されていることが確認できました。今後も適切な情報セキュリティ対策の水準を維持するよう、努めてまいります。

⑤ 技術的な情報セキュリティ対策の取組状況

平成26年１月の金融庁行政情報化LANシステムの更改にあわせ、クライアントPCへの外部媒体の接続状況確認機能の追加等、技術的な情報セキュリティ対策を強化しました。

⑥ 平成25年度に発生した情報セキュリティインシデント

平成25年度は、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ません。

(2) 平成26年度の全体方針

平成26年度においても、以下の取組みを実施し、更なる情報セキュリティ対策の強化に努めます。

① 情報セキュリティ教育・啓発
② 情報セキュリティ自己点検の実施
③ 情報セキュリティ監査の実施
④ 過去に実施した情報セキュリティ監査結果のフォローアップ
⑤ 情報システムに関する重点検査の実施
⑥ 「政府機関の情報セキュリティ対策のための統一基準」の改定を踏まえた、金融庁情報セキュリティポリシーの改定
⑦ 脅威に応じた技術的セキュリティ対策の強化

最高情報セキュリティ責任者
（総括審議官）
三井　秀範

消費者庁

平成25年度の総合評価及び平成26年度の全体方針

消費者庁は、消費者からの個人情報を含めた事故情報や法執行前の機密情報等を取扱う行政機関として、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まいりました。平成25年度に当庁が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、以下の通り報告します。

■ 教育・啓発に関する取組状況

当庁では、ｅラーニングシステムを用いた情報セキュリティ教育環境を整備し、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ます。新たに当庁に配属される職員に対しては、転入時教育として、当庁の情報セキュリティポリシーの内容等の説明を実施しています。また、他府省庁における情報セキュリティ事故事例等、当庁においても注意を促す必要がある事項や、内閣官房情報セキュリティセンター（以下、「NISC」という。）において実施される情報セキュリティに係る勉強会の内容等について、都度全職員への周知を行い、職員に対する情報セキュリティ対策の教育・啓蒙に取り組んでいます。

平成25年度においては、行政機関を標的とした標的型攻撃の増加を受け、全職員を対象として疑似標的型メールによる対応訓練を実施したほか、CISO等連絡会議における申し合わせ事項を受けて、職員のソーシャルメディア利用に係る注意事項についての庁内教育を実施しました。

■ 自己点検・監査の結果

平成25年度は、継続的な情報セキュリティ対策の周知徹底に加え、自己点検実施に係る理解度向上のための職員教育を実施した結果、責任者を含む全ての当庁職員において、前年度に引き続き対策の実施率、到達率がいずれも100.0％であることが確認されました。

情報セキュリティ監査では、当庁の情報セキュリティに係る取り組みが問題なく遂行されていることが確認されましたが、課室間での業務依頼時の情報共有不足により、導入許可を得ていないソフトウェアについて、許可されたものであるとの誤認が生じ、特定の職員端末へ導入許可を得ずに当該ソフトウェアの導入を試みていたことが明らかとなりました。当該事象においては、職員端末における適切な権限管理により当該ソフトウェアの導入には至らず、情報漏えい等の情報セキュリティ事故は発生しませんでしたが、今後、情報セキュリティ教育等を通じ、情報セキュリティに係るルールについてさらなる周知徹底を図ります。

■ NISCによる情報システムに関する重点検査の結果

当庁が所管する消費者庁ネットワークシステム及び消費者庁ホームページシステムについて重点検査を行った結果、必要な情報セキュリティ対策が講じられていることが確認されました。

消費者庁ネットワークシステム及び消費者庁ホームページシステムは、平成26年度に更新を予定しており、更新後においても安全かつ安心な環境が実現できるよう、引き続き適切な情報セキュリティ対策の実施に取り組んでまいります。

■ 平成25年度に発生した情報セキュリティインシデント

平成25年度は、当庁及び当庁が所管する独立行政法人国民生活センターにおいて、情報セキュリティインシデントは発生しませんでした。

■ CISO等連絡会議での申し合わせ事項等

平成25年度は、他府省庁において民間企業が提供するグループメールサービスでの情報取扱いが不適切となっていた事象を受け、当庁におけるグループメールサービスの利用状況の一斉点検を行いました。点検の結果、当庁ではグループメールサービスの利用はあったものの、非公開情報の取り扱いは行っておらず、適切な情報取扱いのもとで利用されていることを確認しました。

なお、当該サービスについては、セキュリティの観点から利用を終了しております。また、第13回会合（平成25年９月26日開催）において決定された「高度サイバー攻撃対処のためのリスク評価等のガイドライン（試行版）」に基づいたリスク評価及び対策計画の立案については、対象となる消費者庁ネットワークシステム及び消費者庁ホームページシステムが平成26年度に更新を予定していることを踏まえ、リスク評価のみ実施しました。対象情報システムの更新完了後、速やかにリスク評価及び対策計画の立案に取り組む予定です。第16回会合（平成26年３月19日開催）において議題となった独立行政法人における情報セキュリティ対策推進については、当庁が所管する独立行政法人国民生活センターを対象に確認した結果、政府機関の情報セキュリティ対策のための統一基準に則った情報セキュリティポリシーの策定、当庁への情報セキュリティインシデント報告体制の整備等、適切な情報セキュリティ対策の推進について年度計画に盛り込まれていることを確認しました。

平成26年度は、職員の情報セキュリティに対するさらなる意識向上のため、職員教育の充実を図ります。平成25年度に実施した標的型メール対策訓練については、引き続き実施するとともに、定期的な実施運用のための環境を整備し、更なる職員における情報セキュリティレベルの向上を目指します。また、消費者庁ネットワークシステム及び消費者庁ホームページシステムが更新されることを踏まえ、サイバー攻撃対策に対するリスク評価や対策導入計画の策定など、適切な情報セキュリティ環境の実現に取り組んでまいります。

当庁情報セキュリティポリシーについては、平成26年度の政府機関の情報セキュリティ対策のための統一基準改訂を踏まえた見直しを実施し、情報セキュリティ動向の変化に応じた適切な情報セキュリティ対策の実現を目指します

最高情報セキュリティ責任者
消費者庁　次長
山崎　史郎

復興庁

平成25年度の総合評価及び平成26年度の全体方針

平成26年度以降の情報セキュリティ対策の実施に資するため、平成25年度に復興庁が講じた情報セキュリティ対策の具体的な取組状況や、職員に対する自己点検結果等について報告します。

当庁は比較的小規模であり、かつ時限の組織であることから、独自の情報システムを構築せず、内閣府の情報システムを活用しつつ、平成24年の発足以来、迅速かつ着実に様々な取組を進めてきました。

平成25年度においては、情報セキュリティに係る職員研修を本庁のみならず、地方局（各復興局）を含めて実施するなど、職員の意識啓発に努めました。また、情報セキュリティ対策の実施状況の自己点検、内部監査等を実施するなど、前年度に引き続き、情報セキュリティポリシー等に基づき必要となる措置を講じました。

一方で、情報セキュリティ対策も不断の見直しを行う必要があります。平成26年度以降も、情報セキュリティ関連規程の更なる整備、情報セキュリティ体制の強化、情報セキュリティ教育を充実するとともに、過去に講じた取組にとどまらず、新しく必要となる取組があれば速やかに実行に移すなど、スピード感を持ちつつ、より一層の情報セキュリティ水準の向上に努めてまいります。

最高情報セキュリティ責任者
復興庁統括官
岡本　全勝

総務省

平成25年度の総合評価及び平成26年度の全体方針

１．平成25年度の総合評価

平成25年度は、情報セキュリティインシデントを可能な限り未然に防止するとともに、情報セキュリティインシデントが発生した際に適切に対処できるよう、職員に対し、不審なメールへの適切な対応やホームページ閲覧によるウイルス感染についての注意喚起等を行ったほか、外部に公開しているウェブサーバについて、脆弱性の有無を確認する監査を実施し、脆弱性への対応がすべて完了するまでフォローアップを行うとともに、情報セキュリティインシデントが発生した場合を想定した訓練等を行いました。

２．平成26年度の全体方針

平成26年度は、以下の情報セキュリティ対策に重点的に取り組み、情報通信や行政の情報化等を所管する省として、情報セキュリティ専門家の助言も得て、情報通信技術の動向や最新のサイバー攻撃について情報収集に努め、新たな情報セキュリティ上の脅威にも適切に対応できるよう努めてまいります。

(1) 総務省情報セキュリティポリシー等の見直し

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、総務省情報セキュリティポリシーを改定するほか、各種手順書の見直しを行い、最新の脅威を踏まえた情報セキュリティ対策を実施します。

(2) 情報セキュリティに関する教育・啓発等

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や最新の攻撃手法を踏まえ、情報セキュリティに関する教育及び自己点検を実施し、職員による着実な情報セキュリティ対策の実施を図ります。

また、職員に対して、最新の攻撃手法を踏まえ、必要な注意喚起を行うとともに、最高情報セキュリティアドバイザー等による研修や相談会・イントラネットにおける情報セキュリティに関する情報発信を行い、一層の啓発に努めます。

さらに、職員が不審なメールへの適切な対応を身に付けられるよう、最新の脅威に即した訓練を行います。

(3) 情報システムの調達・運用における情報セキュリティ対策

情報システムの開発等を外部委託する際にも必要な情報セキュリティ水準が確保されるよう、上記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や最新の攻撃手法を踏まえ、調達に関する手順書を改定します。併せて、調達に当たり、最高情報セキュリティアドバイザー等への相談会を開催し、調達仕様書案等の妥当性確認を行います。さらに、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」に基づき、情報システムへの技術的な対策を進めます。

また、情報システム担当者に、情報システムに関する脆弱性情報及び注意喚起（ソフトウェアの更新指示等）等を速やかに周知し、情報セキュリティインシデントの未然防止を図ります。

(4) 最新の攻撃手法を踏まえた情報セキュリティ監査等

外部に公開しているウェブサーバについて、最新の攻撃手法を踏まえ、脆弱性の有無を確認する監査を実施し、脆弱性への対応がすべて完了するまでフォローアップを行います。また、情報セキュリティインシデントが発生した場合を想定し、総務省CSIRT（Computer Security Incident Response Team）、公開ウェブサーバ担当課室、運用業者といった関係者間の連絡、インシデントの現状把握、応急措置、復旧、原因調査、再発防止策の検討等を行う訓練を実施します。

最高情報セキュリティ責任者
（総務省大臣官房長）
戸塚　誠

法務省

平成25年度の総合評価及び平成26年度の全体方針

１　平成25年度の総合評価

(1) 標的型メール攻撃に対する対応

ア　職員が標的型メール攻撃への対応を経験することにより，不審なメールを受信した際の注意力及び適切な対処を身に付けるため，外部事業者に委託して，標的型メール攻撃の対応訓練を実施しました。

イ　電子メールのなりすまし対策を強化するため，電子署名方式の送信ドメイン認証技術を導入しました。

(2) 情報セキュリティに関する研修

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，情報セキュリティ月間に併せて，外部講師による情報セキュリティ研修を実施しました。

(3) 法務省CSIRTによる教育

平成25年２月に設置した法務省CSIRTにおける活動を円滑に行い，障害発生時における対応能力を強化するため，法務省CSIRTによる教育を実施しました。

２　平成26年度の全体方針

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，法務省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，技術的対策のみならず，職員一人一人がその脅威や障害が発生した際の影響を認識し，情報セキュリティに対する意識を維持・向上することが重要となります。

情報セキュリティ人材の育成及び確保に加えて，職員一人一人の情報セキュリティに対する意識の維持･向上を行うために，役割に応じた情報セキュリティ対策の教育を実施することや，訓練対象者を拡大して標的型メール攻撃対応訓練を実施するなど，より一層，職員に対する情報セキュリティ対策の教育及び訓練に取り組んでまいります。

また，平成26年度に政府機関の情報セキュリティ対策のための統一規範並びに政府機関の情報セキュリティ対策のための統一管理基準及び政府機関の情報セキュリティ対策のための統一技術基準が改定されることを踏まえ，法務省においても，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い，今後とも情報セキュリティ対策の向上に努めてまいります。

最高情報セキュリティ責任者
（法務省大臣官房長）
黒川　弘務

外務省

平成25年度の総合評価及び平成26年度の全体方針

○平成25年度の総合評価

平成25年５月に、外務大臣が情報セキュリティ政策会議の構成員となり、10月には同会議において「サイバーセキュリティ国際連携取組方針」が決定されました。当省においても、同方針に基づき、産学官等の関係者と協力して国際連携の取組を推進しています。

７月には、グループメールサービスの利用による政府機関からの情報流出事案が発表され、当省においては、同サービス等の業務利用方針を策定し職員への注意喚起を行いました。

平成25年度において、当省では、日本語入力補助ソフトBaidu IMEの事案、ウイルスチェックが不十分なコンテンツのホームページへの掲載の事案が発生しました。当省では、インストールするソフトウェアの厳格な管理、コンテンツのウイルス対策、多層化といった情報セキュリティ対策強化に努めています。

外務省全体の情報セキュリティ向上、全職員の情報セキュリティ意識の向上のため、情報セキュリティ対策自己点検、重点検査、NISC主催の標的型メール攻撃訓練、公開ウェブサーバ脆弱性検査、情報セキュリティ監査等に加え、外部から専門家を招き、実演を交えての職員向け情報セキュリティ説明会等を実施しました。また、高度サイバー攻撃への対処のためのリスク評価等の試行についても取り組んでいます。

○平成26年度の全体方針

平成26年度においては、政府機関における情報セキュリティ対策のための統一基準群の改定を踏まえ、外務省情報セキュリティポリシーの改定を予定しています。また、サイバー攻撃の脅威が急増していることから、平成26年度予算で情報セキュリティインシデント対応チームを新たに設置し、インシデント対応体制を強化するとともに、監視機器等を設置し、サイバー攻撃対策及び情報システム監査を強化していくことにより、さらなる情報セキュリティ対策向上に努めていく所存です。

最高情報セキュリティ責任者
外務省大臣官房長
越川　和彦

財務省

平成25年度の総合評価及び平成26年度の全体方針

１．平成25年度の総合評価

・財務省では、内閣官房情報セキュリティセンター（NISC）による重点検査や情報セキュリティ対策推進会議（CISO等連絡会議）での申し合わせ事項など、日々進化していく情報セキュリティ上の脅威に対する政府全体の取り組みを踏まえ、積極的なセキュリティ対策に取り組んでまいりました。

・一方で、水飲み場型攻撃によるウイルス感染事案のような巧妙な攻撃が顕在化し、情報漏えいなどのリスクがますます高まっている状況にあります。

・こうした事態も踏まえ、教育・啓発に一層力を入れるとともに、自己点検に取り組んだほか、未知のウイルスへの対応として、インターネットからの不正侵入防止やインターネットへの不正送信防止などのシステムによる対策を強化するとともに、監査にも力を入れてまいりました。特に教育・啓発及び自己点検、監査については以下の取り組みを行っております。

（教育・啓発及び自己点検に関する取組）

・財務省では、情報セキュリティ対策基準に基づき、職員が年間１回以上の情報セキュリティ研修を受講するよう、集合研修を実施している他、ｅラーニングによる自習環境を整備し、集合研修未受講者に対して自習を求めています。

・この他、全職員を対象に、無予告で標的型メール攻撃に対する訓練を実施し、職員の情報セキュリティに対する意識を高めました。

・また、情報セキュリティ対策基準の遵守事項の実施状況について、職員が自ら確認する「自己点検」を実施しています。平成25年度はすべての職員を対象として実施しました。点検の結果、概ね遵守事項が適正に実施されているものと確認しました。

（監査の結果）

・財務省が管理・運営している情報システムの一定数に対して、外部委託事業者による監査（外部監査）や情報セキュリティに関する専門的な知識及び経験を有した民間専門家である最高情報セキュリティアドバイザー（CIO補佐官）による監査（内部監査）を実施しました。監査の結果、各情報システムが概ね適正に管理・運営されていることが確認されましたが、一部対応が必要と指摘された事項については、速やかに改善を行うよう指示しております。

２．平成26年度の全体方針

・平成25年度の総合評価を踏まえ、引き続き、NISC等との連携を緊密に図りながら、新たな情報セキュリティ上の脅威に適切かつ柔軟に対応するよう努めます。情報セキュリティに関する教育・啓発及び自己点検、監査も平成25年度と同様に、しっかりと取り組んでまいります。

・平成26年度には統一基準群が改訂されることから、財務省において定める基準についても本基準を満たすように、改訂を行います。その際、規則が形骸化することのないよう実践的なものとなるように留意する他、職員に対して新基準の周知徹底を十分に行ってまいります。

最高情報セキュリティ責任者
（財務省大臣官房長）
佐藤　慎一

文部科学省

平成25年度の総合評価及び平成26年度の全体方針

文部科学省（以下「当省」という。）は、教育の振興及び生涯学習の推進を中核とした豊かな人間性を備えた創造的な人材の育成、学術、スポーツ及び文化の振興並びに科学技術の総合的な振興を図ることを任務としています。

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、中央省庁を標的とした水飲み場型攻撃の発生など、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、平成25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まいりました。

(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重点検査及びセキュリティ監査の実施
(4) 平成24年度のセキュリティ監査結果に対するフォローアップの実施
(5) 高度サイバー攻撃対処のためのリスク評価の実施
(6) WindowsXPのサポート終了にともなう対策の実施
(7) CYMAT要員登録による体制の強化

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)～(4)を実施し、政府全体の方針等に基づき、(5)～(7)の対策を実施しました。これらの取組みにより、平成25年度は、省内において重大な情報セキュリティインシデントは発生しませんでした。

平成26年度は、統一基準群の改定をふまえた文部科学省情報セキュリティポリシーの改定や、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・向上に努めてまいります。

情報セキュリティ最高責任者
（大臣官房長）
戸谷　一夫

厚生労働省

平成25年度の総合評価及び平成26年度の全体方針

１．平成25年度の総合評価

厚生労働省では、政府機関等に対するサイバー攻撃の脅威から国民生活に直結する重要な情報や情報システムを守るため、組織全体としての情報セキュリティ対策に積極的に取り組んでいます。平成25年度においては、以下の点を中心にその充実・強化に取り組みました。

(1) 教育・啓発に関する取組状況

情報セキュリティに対する意識の向上、普及啓発等を図るため、電子政府利用促進週間、情報セキュリティ月間をはじめ、政府機関等における情報セキュリティインシデント発生時などの様々な機会を捉え、職員に対する情報セキュリティ研修の受講勧奨等に取組み、受講率を大幅に向上させました。

また、標的型メール攻撃による被害を最小化するため、全職員をNISCが実施する標的型メール攻撃訓練の対象とするとともに、訓練結果を踏まえ、厚生労働省単独でも外部の専門業者による標的型メール攻撃訓練を実施し、注意喚起に努めました。

(2) 自己点検・監査の実施

全職員を対象に情報セキュリティ対策に係る実施状況の自己点検を行うとともに、情報システム等を対象にした情報セキュリティ監査を実施しました。その結果、早急に改善を要する脆弱性等の問題は検出されませんでしたが、見つかった課題については速やかに改善・対策を講じました。

(3) Windows XP等への対応

情報システムに関する重点検査において、Windows XP等の使用状況について確認を行い、サポート終了までに機器の更新等を行う、または、サポート終了後はインターネットへ接続しない等の適切な対応が図られることを確認しました。

また、サポート終了後においてインターネットへの接続はしないものの、当面の間Windows XPパソコンを使用する状況も確認されたことから、CISO等連絡会議での申し合わせ事項も踏まえ、再度、使用する際の注意事項について周知しました。

(4) 情報セキュリティインシデントへの対応

平成25年度においては、不正アクセス、メールの誤送信等の事案が発生したことから、関係機関への連絡、被害拡大防止等を行うとともに、職員に対する注意喚起等により再発防止に向けた周知を図りました。

２．平成26年度の全体方針

厚生労働省においては、施設等機関及び独立行政法人等が狙われる事案が増えてきたことを踏まえ、当該機関に対してもNISC等と連携し、適切な指導、要請等を行います。

また、サイバー攻撃の手法が高度化かつ多様化している状況に適切に対応するため、平成26年度においては、統一基準群の改定を踏まえた厚生労働省情報セキュリティポリシーの改定を行い、引き続き、情報セキュリティ対策の維持・強化に努めてまいります。

最高情報セキュリティ責任者
（厚生労働省大臣官房長）
二川　一男

農林水産省

平成25年度の総合評価及び平成26年度の全体方針

１　平成25年度の総合評価

農林水産省は、平成25年５月に取りまとめられた農林水産省へのサイバー攻撃に関する調査結果を真摯に受け止め、今後のサイバー攻撃への対応等を改善していくため、以下の取組をはじめとする情報セキュリティ対策の強化に努めてまいりました。

また、平成25年度においては、一部の部署が利用したグループメールが、機密情報を含むものではなかったものの、外部から閲覧可能な状態となっていたことから、同サービスを機密情報を扱う業務に利用しないこととしたほか、当省所管の独立行政法人において標的型メール事案が発生したこと等も踏まえ、独立行政法人等との速やかな連絡体制の構築、情報の共有等に取り組んでまいりました。

(1) 情報セキュリティ水準の向上

次世代ファイアウォールの導入や外部記録媒体の利用制限等の取組を実施。

(2) 教育・啓発に関する取組状況

全職員を対象に、標的型メール攻撃等に対する訓練を継続的に実施するとともに、ｅラーニングによる情報セキュリティ教育を新たに実施。

(3) 自己点検・監査の実施

全職員を対象に、業務上の情報セキュリティ対策の実施状況について自己点検を実施するとともに、情報システム等を対象とした情報セキュリティ監査を実施し、それらの結果を踏まえ、情報セキュリティの確保のための改善措置を実施。

(4) 最近の情報セキュリティ問題への対処

平成25年12月12日に開催された情報セキュリティ対策推進会議において申し合わされた「最近の情報セキュリティ問題への対処について」を踏まえ、ウィンドウズXP等のサポート終了に向けて計画的にパソコンの更新等を実施。また、複合機等のセキュリティ問題に対応するため、適切な機器設定等の措置を実施。

２　平成26年度の全体方針

農林水産省では、政府統一基準群の改定を踏まえ、速やかにセキュリティポリシーを改定することとしております。また、今後も、内閣官房等の関係機関と連携を取りながら、全職員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し、省全体の情報セキュリティレベルを向上させるため、情報セキュリティの強化・拡充に向けた取組を一層推進してまいります。

最高情報セキュリティ責任者
農林水産省大臣官房長
今井　敏

経済産業省

平成25年度の総合評価及び平成26年度の全体方針

平成25年度は、国内外において、標的型メール攻撃やホームページ改ざん等のサイバー攻撃が増加するとともに、その手口も巧妙化・高度化が著しいものでした。また、国内ではグループメールサービス等の約款による情報処理サービスの使い方を誤ったことによる情報漏えい事故も発生しました。

経済産業省において、平成25年度は、重要な情報システムのひとつである基盤情報システム更改後、年度を通して利用した１年であり、シンクライアントと無線LANの導入によって実現した、職場内・職場外を問わず業務を行いつつパソコン本体にデータを残さないといったセキュアな環境を浸透させるなど、セキュリティ対策の強化に努めました。

サイバー攻撃や情報処理サービス利用時の事故などは、攻撃等を早期に発見すること、情報漏えい等による悪影響を未然に防止することが重要です。このため、当省においては、入口対策に加えて出口対策等システム面での技術的対策の強化を実施するとともに、人的対策として、情報管理の徹底について改めて全職員に周知しました。さらに、教育面でも、標的型メール攻撃への対処訓練をはじめ、従来は個別に実施していた情報セキュリティ、行政文書管理、個人情報保護等について、これらを一体とした教材を準備し、e-Learningにより全職員に受講させるなど、効率的、かつ、効果的な取組を行いました。

平成26年度においては、引き続き情報セキュリティの強化のためのシステム対策、職員への教育を継続するとともに、業務改革を推進する観点から情報システムの更なる有効活用を目的とした改善検討を進める方針です。また、これらの検討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の改定を踏まえ、当省情報セキュリティポリシーや各種手順書等を改定する予定です。

具体的には、

・標的型メール等のサイバー攻撃への対処のためのシステム対策の強化として、リスク評価とその結果等を踏まえた新たな仕組みの導入
・全職員の情報管理、情報セキュリティに対する意識の更なる向上のための教育の継続と改定予定の当省情報セキュリティポリシーや各種手順書等の周知徹底

に向けた検討や取組を推進します。

最高情報セキュリティ責任者
（大臣官房長）
日下部　聡

国土交通省

平成25年度の総合評価及び平成26年度の全体方針

１．平成25年度の総合評価

平成24年度に引き続き、職員を対象とした教育訓練の実施、状況の変化に応じた継続的な取組等により、情報セキュリティ対策の徹底に努めています。

職員への教育訓練としては、中堅係長研修といった階層別の研修において情報セキュリティに関する講義を設けることにより、情報セキュリティに関する意識の向上や周知・徹底に向けた取組を実施しています。

また、平成25年度の新たな取り組みとして、国土交通省CSIRTのインシデント対応訓練を実施し、CSIRT要員の手順の習熟を図るとともに、手順の改善を行っています。

自己点検・監査、重点検査の結果としては、標的型攻撃等の外部からの脅威に対する情報セキュリティ対策やスマートフォン等の情報セキュリティ対策等について改善の余地が見られたほか、情報の取扱いに関するルール等について一部の職員の理解不足が見られたため、実施すべき措置の周知・徹底を継続していく必要があると考えています。

２．平成26年度の全体方針

平成25年度の総合評価を踏まえ、平成26年度の全体方針を以下の通り定め、引き続き情報セキュリティ対策の維持・強化に努めて参ります。

a）職員への情報セキュリティに関する教育訓練の強化

階層別研修等における職員への教育訓練の機会を増やし、情報の取扱いや新たな脅威に対する情報セキュリティ対策等の徹底を図ります。

b）国土交通省CSIRTのインシデント対応能力の強化

情報セキュリティインシデント発生時に迅速かつ的確な対応ができるように、インシデント対応訓練を実施し、職員の対応能力の向上、対応手順等の改善を図ります。

c）平成26年度の政府機関統一基準群の改定対応

政府機関統一基準群の改定を踏まえ、国土交通省情報セキュリティポリシー及び関連規程を改正するとともに、新たな遵守事項の周知・徹底を図ります。

d）サイバー攻撃に対する情報セキュリティ対策の徹底

重点検査等で明らかとなった外部からの脅威に対する情報セキュリティ対策の不足について改善を徹底するとともに、平成25年度に発生した情報セキュリティインシデントと類似の事案の発生を防止するための対策の徹底を図ります。

最高情報セキュリティ責任者
国土交通省総合政策局長
西脇　隆俊

環境省

平成25年度の総合評価及び平成26年度の全体方針

○平成25年度の総合評価

環境省は、廃棄物対策、公害規制、自然環境保全、野生動植物保護などを実施するとともに、地球温暖化、オゾン層保護、リサイクル、化学物質、海洋汚染防止、森林・緑地・河川・湖沼の保全、環境影響評価、放射性物質の監視測定などの対策を他の府省と共同して行うなど、幅広い分野を所管しています。特に東日本大震災後においては、原子力規制委員会の設立や除染や放射性廃棄物の処理等により業務が拡大し、これに伴い大幅に行政事務従事者が増加している状況にあります。

このような中、平成25年度においては、７月には政府間交渉に関する環境省関係者による情報のやりとりがインターネット上で閲覧可能となっていた問題が判明しました。当省においては、この事案を重大かつ全省的な問題と受け止め、大臣の指示の下、直ちに総点検を行い、類似事例の調査や今後の再発防止策を検討・実施いたしました。

本事案の背景としては、情報セキュリティ対策に対する当省職員の認識の甘さに原因があったことからこの点を厳しく反省し、機密情報を扱う業務に民間企業が提供する約款によるグループサービスを利用することを明確に禁止し、職員教育の徹底、情報セキュリティに関する組織体制の強化を進めました。

一方で、安全性と業務効率性を両立させる利用環境の確保の検討を行い、一部の機能の提供を開始するとともに、引き続き、安全な利用環境整備の検討を進めています。

また、昨今のますます巧妙化する標的型攻撃への技術的な対策を進めるとともに、業務で取り扱う情報や情報システムについては、内閣官房情報セキュリティセンターの指導の下、高度サイバー攻撃対処のためのリスク評価の試行に取り組みました。

○平成26年度の全体方針

平成26年度においては、政府機関の情報セキュリティ対策のための統一基準群の改訂に伴い環境省情報セキュリティポリシーの見直しを行うとともに、25年度に引き続き標的型攻撃への対策の強化や、適切な情報の取り扱いの徹底、サイバー攻撃への対策の充実を図ります。

技術面においては、従来から活用を進めているセキュアUSBやオンラインストレージシステムの活用を更に徹底するとともに、本格実施が予定される高度サイバー攻撃対処のためのリスク評価に取り組み、効果的・重点的な対策を計画的に推進するとともに、25年度の重点検査等で確認されたセキュリティ対策が不足している点を中心に、更に技術的な防御等の徹底を進めることで、全体の情報セキュリティ対策の底上げを目指します。

一方、情報の取り扱い等の面においては利用者の意識向上が重要と捉えており、25年度に発生した事案や最新のセキュリティ事情を踏まえ、e-learningの活用や職員採用時等の研修を中心に更に内容の充実を図ることにより、引き続き全省的な情報リテラシーの向上に努めてまいります。

環境省最高情報セキュリティ責任者
（大臣官房長）
鈴木　正規

防衛省

平成25年度の総合評価及び平成26年度の全体方針

○平成25年度の総合評価

・情報セキュリティ対策の実施状況に関する自己点検、近年のサイバー攻撃に関する脅威の高まりや、WindowsXPのサポート終了に伴う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、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ました。

・ウェブメール等のサービスの私的利用について情報流出等、セキュリティ面での危険性が懸念されることから職員に対して周知徹底を図りました。

○平成26年度の全体の方針

・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共に、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ります。

情報保証統括責任者
（防衛省運用企画局長）
中島 明彦

別添２　「サイバーセキュリティ 2013」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)業務で扱う情報の機密性の要求度等に応じた対策の重点実施のための枠組みの構築	内閣官房 関係府省庁	a) ・ 内閣官房において、高度サイバー攻撃対処のためのリスク評価等のガイドライン（試行版）を作成し、各府省庁における試行を実施するとともに、その結果を踏まえ、正式実施に向けた検討を行った。
		b) ・ 内閣官房において、新たな脅威・技術への対応及び規定内容の実効性向上を目的として、政府機関統一基準群の改定を実施した。改定に当たっては、対策推進計画に基づく PDCA サイクルの構築、標的型攻撃への対策、サプライチェーン・リスクへの対策、SNS、約款サービス等利用時の対策、アプリ・コンテンツ提供時の対策、複合機、私物端末、USB メモリへの対策等の内容を盛り込んだ。
(イ)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、政府情報システム管理データベースの利活用方法について、政府全体を通じたリスク管理、脆弱性の検出等の観点から検討を行った。また、府省庁におけるインシデントの調査において、政府情報システム管理データベースを活用した。
		b) ・ 総務省において、同データベースを引き続き維持・管理した。
(ウ)「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。
(エ)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。
(オ)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。
(カ)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、政府機関において私物のスマートフォン等を外出先やテレワーク等で業務利用する場合の対策として、私物端末の利用手順や管理責任者の明確化等を政府機関統一基準群の規定に盛り込んだ。 ・ また、各府省庁において実施手順等を整備するための手引きとして、府省庁対策基準策定のためのガイドラインにおいて、当該規定に準拠するための手順整備例等を基本対策事項として規定した。
(キ)重要な情報の提供における SNS の利用への対応	内閣官房	・ 内閣官房において、2013 年５月１日に各府省庁に対してソーシャルメディアを利用した国民への情報発信における留意事項に係る事務連絡を発出した。また、政府機関統一基準群の改定において、ソーシャルメディア利用に係る対策事項として、管理責任者を設置すること、重要な情報については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規定として整備した。
(ク)可搬記憶媒体(USB メモリ等)の情報セキュリティ対策の強化	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に当たり、USB メモリを始めとした外部電磁的記録媒体の利用に係る対策事項を規定した。 ・ また、府省庁対策基準策定のためのガイドラインにおいては、外部電磁的記録媒体の利用に係る脅威と対策を整理し、セキュア USB の導入を含め、各府省庁が外部電磁的記録媒体の利用に係る実施手順を整備する際の考え方を示した。
(ケ)複合機等のセキュリティ対策の強化	内閣官房 全府省庁	・ 内閣官房において、ネットワーク機能を持つ複合機等に求められる情報セキュリティ対策について検討するとともに、各府省庁における対策の徹底について、情報セキュリティ対策推進会議（2013 年 12 月）において申し合わせた。 ・ また、各府省庁で保有している複合機について、外部からの不正なアクセスを遮断する措置が講じられているかなどの検査を実施した。
(コ)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における情報セキュリティ対策に係る取組の検討を支援した。
(サ)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 関係府省庁	a)	・ 「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。
		b)	・ 内閣官房において、政府機関統一基準群の改定に当たり、政府共通プラットフォームを含む複数省庁で共通的に使用する政府情報システム基盤の利用に係る規定の見直し及び追加を実施した。
(シ)情報システムの共同利用や統合管理によるセキュリティ対策の強化に向けた取組	内閣官房		・ 内閣官房において、情報システムの共同利用や統合管理による情報セキュリティ対策の強化について検討を行った上で、省庁共同利用型メールサービスの仕様を決定し、同サービスを運用した。
(ス)政府機関の情報システムの効率的・継続的なセキュリティ向上	内閣官房 総務省 全府省庁	a)	・ 各府省庁において、「各政府機関の公開ウェブサーバ及び電子メールサーバの集約化計画の策定について」に基づき、保有する公開ウェブサーバ及びメールサーバの集約化を行い、計画どおり、約５割減少するなど、情報システムのスリム化や運用効率化を推進した。
		b)	・ 内閣官房において、各府省庁に対する重点検査により各府省庁のサーバ集約化計画の実施結果の取りまとめを行った。また、その結果について「サイバーセキュリティ戦略に係る年次報告」に記載し、情報セキュリティ政策会議に報告する予定である。
(セ)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		・ 情報提供ネットワークシステムの構築にあたっては、「サイバーセキュリティ 2013」にも掲載のあった、①個人情報を一元管理せず分散管理、②情報提供ネットワークシステムを用いた情報連携において個人番号ではなく符号を利用、③アクセス制御によりシステム内の特定個人情報にアクセスできる人を制限、④通信を暗号化、などの施策を講じることとした仕様書により調達手続を進め、落札事業者との契約を行った。
(ソ)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試行版の開設に当たり、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 を取得し、「情報セキュリティマネジメント実践のための規範」である ISO/IEC 27002 等の安全対策基準に準拠した運用を行っているデータセンター内にサーバを設置し、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を実施する等、情報公開システムとして必要なセキュリティ対策を実施した。
(タ)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、マニュアルの活用状況に関する各府省庁への確認等を実施した。
		c)	・ 各府省庁において、NISC からの調査を通じて、同マニュアルの活用等について報告を行った。
(チ)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)	・ 新たな政府機関統一基準群案においても、各府省庁における IT 製品の調達にあたっては、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定することを求めることとした。
		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効的かつ効率的に行えるようにするため、新たな政府機関統一基準群の見直しに合わせ、「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」を策定予定である。
(ツ)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)	・ 認証作業を実施し、2013 年度 40 件を越える認証を発行した。 ・ 認証取得製品については、IPA の Web サイトにて「CC v3.1 による認証製品リスト」、「CC v2.3 による認証製品リスト」及び「プロテクションファイルリスト」として公開している。
		b)	・ IPA より NISC への要員派遣を行い、各省庁のヒアリングを実施。そこで得られた要件に適切なプロテクション・プロファイルの情報を提供し、最新の「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」へ反映を行った。

		c) ・ IPA より NISC への要員派遣を行い、省庁に対する説明や勉強会を実施。調達者の要件を統一基準に反映し、より調達者が活用しやすいものとした。 ・ また、本要件の反映に当たり、製品ベンダにも広く説明を行い、パブリックコメント招請の実施により、製品提供側への制度浸透も図った。
		d) ・ 内閣官房において、サプライチェーン・リスクへの対応について、情報システム等の調達時に、委託先従業員等の情報を提供させることを選定条件にする規定を追加するなど、政府調達に関する協定の範囲内での政府機関統一基準群の見直しを行った。 ・ また、Common Criteria（ISO/IEC 15408）等の国際規格に基づく適合性評価の活用に関し、経済産業省が作成した「IT 製品の調達におけるセキュリティ要件リスト」の参照に係る規定を追加した。
(テ)政府調達の在り方の検討	内閣官房	・ 内閣官房において、サプライチェーン・リスクへの対応について、情報システム等の調達時に、委託先従業員等の情報を提供させることを選定条件にする規定を追加するなど、政府調達に関する協定の範囲内での政府機関統一基準群の見直しを行った。 ・ また、Common Criteria（ISO/IEC 15408）等の国際規格に基づく適合性評価の活用に関し、経済産業省が作成した「IT 製品の調達におけるセキュリティ要件リスト」の参照に係る規定を追加した。
(ト)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、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（試行版）を作成し、各府省庁における試行を実施するとともに、その結果を踏まえ、正式実施に向けた検討を行った。
(ナ)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 全府省庁	・ 各府省庁において、政府機関統一基準群及び個別マニュアル等を踏まえ、政府機関外の組織に運用・管理を委託している情報システムについて、情報セキュリティを確保するための取組を推進した。
(ニ)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「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」の対象となる各府省庁の情報システムについて、暗号アルゴリズムの移行状況を調査し、関係府省庁等と連携して円滑な移行を推進した。
		d) ・ 各府省庁において、同移行指針の対象となる情報システムについて、より安全な暗号アルゴリズムへの対応及び移行を着実に実施した。
		e) ・ 内閣官房において「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」の対象となる各府省庁の情報システムについて、暗号アルゴリズムの移行状況を調査し、関係府省庁等と連携して円滑な移行を推進した。
(ヌ)安全性・信頼性の高い暗号モジュールの利用推進	内閣官房 経済産業省 全府省庁	a) ・ 内閣官房において、政府機関統一基準群により「暗号モジュール試験及び認証制度」等の利用を求めるなどを規定し、暗号モジュール試験及び認証制度の利用を推進した。 ・ IT 製品の調達におけるセキュリティ要件リスト（案）の中の対象候補分野名 USB メモリに関して ISO/IEC 19790 に基づく JCMVP 認証の活用が記載され、今後の制度利用に貢献することが期待される。
		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。
(ネ)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。また、政府機関統一基準群において SPF、DKIM（Domain Keys Identified Mail）、S/MIME（Secure / Multipurpose Internet Mail Extensions）等の対策を行うよう規定し、これらの対策を推進した。
		b) ・ 引き続き、迷惑メール対策推進協議会と協力し、各種業界団体等に対して送信ドメイン認証技術等迷惑メール対策技術の導入を推進するための説明会を６回開催した。

(ノ)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	a)	・ 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に.go.jp で終わるものを使用するよう求めるとともに、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政府機関統一基準群によって規定した。
		b)	・ 各府省庁において、政府機関であることが保証される.go.jp で終わるドメイン名の利用を推進した。
(ハ)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、公開 PDF ファイルに関する政府認証基盤（GPKI：Government Public Key Infrastructure）を活用した電子署名の利用等により、政府機関において公開しているウェブサイト上の電子ファイルの正当性・安全性を担保するための取組を推進した。
(ヒ)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)	・ 警察庁の「サイバーインテリジェンス情報共有ネットワーク」及びセプターカウンシルの「標的型攻撃に関する情報共有体制（C⁴TAP）」と NISC との間における情報共有を行った。 ・ また、防衛省の「サイバーディフェンス連携協議会」との情報共有についても、2014 年度中の体制構築に向け、調整を行った。
(フ)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)	・ 関係府省庁において、独立行政法人に対して引き続き政府機関統一基準群を含む政府機関における一連の対策を踏まえ、情報セキュリティポリシーの策定・見直しを要請した。 ・ 内閣官房において、2014 年２月 28 日付けの事務連絡により、関係府省庁に対し、所管する独立行政法人等における情報セキュリティポリシーの整備を始めとした情報セキュリティ対策の状況について 2013 年度末時点で調査を依頼し、独立行政法人の現状を確認するとともに、独立行政法人に対して支援を行えるよう関係府省庁との間で情報の共有を図った。
		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。 ・ 内閣官房において、2014 年２月 28 日付けの事務連絡により、関係府省庁に対し、所管する独立行政法人等における情報セキュリティ対策の状況について 2013 年度末時点で調査を依頼し、実態を確認するとともに、調査結果に基づき、独立行政法人に対して支援等を行えるよう関係府省庁間との間で情報の共有を図った。
		c)	・ 関係府省庁において、所管する独立行政法人等に対して、独立行政法人から発信する電子メールについて、なりすまされることのないよう送信ドメイン認証技術の採用等を推進した。 ・ 内閣官房において、関係府省庁に対し、所管する独立行政法人等においても政府機関統一基準群を踏まえた対策を講ずるよう要請した。
		d)	・ 「政府におけるサイバー攻撃への迅速・的確な対処について」（2013 年６月 19 日情報セキュリティ対策推進会議決定）に基づき GSOC による情報収集・共有体制の独立行政法人等への拡大を検討した結果、所管府省庁との調整に基づき独立行政法人及び一部の特殊法人を枠組みに加えることとし、2013 年度中に情報共有等を開始した。
(ヘ)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)	・ 現地へ赴いて BCP（Business Continuity Planning）策定を支援する、BCP アドバイザーの紹介を、アドバイスを希望する２団体に対して実施した。 ・ 集合研修として「BCP 策定セミナー」及び「情報セキュリティ監査セミナー」「情報セキュリティ監査セミナー」を開催した。なお、各セミナーの参加者は 157 名（３回開催）、95 名（２回開催）、172 名（４回開催）である。 ・ また、情報セキュリティのマネジメントや情報資産の管理及びリスクへの対応並びに具体的な情報セキュリティ対策について習得する「入門 ISMS 概論コース」をｅラーニングで開催した。受講者数は 529 名である。
		b)	・ LGWAN（Local Government Wide Area Network）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、情報セキュリティ技術に関する解説、地方公共団体における事例紹介や、各種情報セキュリティ検討に資する資料の提供を行った。

		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 702 団体を対象に実施し、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 81 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 792 団体の約 45 万 URL を毎日巡回検査を行った。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。 ・ ウェブ感染型マルウェアに関する説明セミナーを、全国５箇所（仙台、東京、大阪、岡山、福岡）で開催し、対策強化を支援した。累計 444 名が参加した。
		e) ・ 地方公共団体における SPF（Shortest Path First）の導入率を調査するとともに、SPF 導入にあたってのセミナーを全国５箇所で開催した。（参加者数累計：444 名。ウェブ感染型マルウェアに関するセミナーと同時開催。）
		f) ・ e ラーニングによる情報セキュリティ関連研修においては、個人情報保護や、情報発信ツール利用におけるリスク管理ほか、地方公共団体の職員として必要な情報セキュリティに関する事項をテーマとした全６コースを実施した。延べ受講者数は、147,223 名である。
		g) ・ 総務省において、IPv4 と IPv6 が共存するネットワーク環境におけるセキュリティ課題の対応方策を確立するための実証実験を実施し、その成果をガイドラインとしてまとめ、講演会の形で広く展開した。講演会は全国 12 箇所で実施した。

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) ・ 2012 年度に引き続き、政府機関情報システムの 24 時間監視を実施し、情報共有、関係機関との連携を実施するとともに、2012 年度補正予算による GSOC の機能強化を行った。
		b) ・ 担当者の人事異動などの機会をとらえ、随時、緊急時の連絡体制を訓練により確認するとともに、3.18（サイバー）訓練実施時に、全府省庁一斉の連絡訓練を実施した。
		c) ・ GSOC の監視対象先を拡大するため、設置するセンサー数を増大した。その結果、収集される情報量が増加したため、必要とされる情報解析能力を満足するため GSOC の態勢強化を図ることとし、一部を先行して実施した。 ・ また、「サイバーセキュリティセンター」（仮称）における GSOC の在り方について検討を開始したが、一部については、2014 年度も引き続き検討を実施する。
		d) ・ GSOC で収集したインシデント情報や攻撃手法の分析結果等を標的型攻撃に関する情報共有体制（C⁴TAP）を通じて重要インフラ事業者等へ提供することとし、情報提供を開始した。
(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	a) ・ 「政府におけるサイバー攻撃への迅速・的確な対処について」（2013 年６月 19 日情報セキュリティ対策推進会議決定）において、「各府省庁の情報システムに対するサイバー攻撃に係る情報を可能な限り速やかに内閣官房情報セキュリティセンターに連絡する旨、各府省庁の情報セキュリティポリシーに記載すること」を求め、より一層迅速に情報共有を可能とする体制を構築した。
		b) ・ GSOC で収集した政府機関等に対するサイバー攻撃に関する全般的な傾向や情勢について分析を行い、各政府機関に対して当該分析結果を 2013 年度は２回提供した。
(ウ)政府 CISO による一元的態勢の構築	内閣官房 全府省庁	・ 内閣官房は、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うために政府 CISO を中心に設置された情報セキュリティ緊急支援チーム（CYMAT）に対して、定期的に研修を実施するなどして機能強化を図った。
(エ)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、2013 年 10 月～11 月にかけて内閣官房及び関係府省庁の担当者に対する実践的な訓練を実施した。
(オ)CSIRT 等の体制の整備及び連携の強化	内閣官房 全府省庁	a) ・ 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、情報セキュリティインシデント認知時における対応について研修を実施した。同研修では、事象判断、幹部報告、広報等の模擬訓練を行うとともに、グループディスカッションを通じて、CSIRT 要員の連携強化を図った。
		b) ・ 内閣官房において、PoC 会合を開催するなどにより、最新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・意見交換を図った。
(カ)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、2013 年 10 月～12 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。
(キ)標的型攻撃に係る教育訓練の実施及び連絡・報告訓練の訓練方法等の検討	内閣官房 関係府省庁	・ 内閣官房において、訓練を希望した 18 府省庁 19 万人に対して「標的型メール訓練」を行った。得られた知見を各府省庁にフィードバックするとともに、独自に標的型メール訓練を行う省庁に対して、支援を行った。 ・ また、2014 年度の「職員の連絡・報告にかかる訓練」に向けた訓練についても検討を行った。
(ク)「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	・ 新たなサイバー攻撃である標的型攻撃について、官公庁・大企業の LAN 環境を模擬した実証環境を用いて、標的型攻撃の解析及び防御モデルの実証実験を実施し、標的型攻撃の特徴情報について明らかにするとともに、求められるインシデントレスポンス等の検討を行った。 ・ また、官公庁・民間企業等を対象に大規模模擬環境を用いた実践的な防御演習を 2013 年度内に 10 回開催し、30 組織以上からのべ約 300 名が参加した。

(ケ)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の向上を図った。（2014 年３月）
(コ)政府機関における業務継続能力の強化	内閣官房 全府省庁	a) ・ 内閣官房において、各府省庁の情報システム運用継続計画の策定に寄与するため、「IT-BCP 策定モデル」、「個別対策事例」を 2013 年６月に提示した。重点検査を実施した結果、各府省庁の情報システム運用継続計画はおおむね策定されていること等を把握した。
		b) ・ 各府省庁において、業務継続計画を踏まえつつ、内閣官房において策定した「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」を活用し、情報システム運用継続計画の見直しの検討を行った。
(サ)平時からの情報共有体制の構築	内閣官房 全府省庁	・ 内閣官房において、各府省庁と協力し、民間の CSIRT や SOC 事業者の団体等と会合や意見交換を行い、官民による情報共有の推進を図った。
(シ)サイバー攻撃に係る脅威・手法分析の推進	内閣官房 関係府省庁	・ サイバー攻撃事態発生時における適切な対処態勢の構築を図るため、標的型メール攻撃に関する不正プログラムの解析を行うなど、サイバー攻撃に係る脅威・手法の分析を推進した。
(ス)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（2013 年７月、アメリカ）、CODE BLUE（2014 年２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。
(セ)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、警察庁、金融庁、経済産業省等で、採用時に情報セキュリティに係る資格の有無を確認する取組が実施された。 ・ また、そうした素養の確認を現状特に行っていない省庁においても、新規採用後早期に、情報セキュリティ教育を重視した研修を行われるなど、一定の進捗が図られている。 ・ なお、NISC において、そうした個別の事例について調査を実施するとともに、事例共有に資するよう各府省庁に対し調査結果のフィードバックを行った。
(ソ)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) ・ 内閣官房において、総務省が開催する情報システム統一研修について、教材に昨今の脅威を踏まえた対策を追記するなどの支援を行った。
		b) ・ 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、情報セキュリティインシデント認知時における対応について研修を実施した。同研修では、事象判断、幹部報告、広報等の模擬訓練を行うとともに、グループディスカッションを通じて、CSIRT 要員の連携強化を図った。
		c) ・ 人事院において、各府省庁の新規採用職員を対象とした合同研修において情報セキュリティの必要性に係る啓発を行い、内閣官房において、当該研修の教材について、昨今の脅威を踏まえた対策を追記するなど、教材作成の支援を行った。
		d) ・ 内閣官房において、情報セキュリティ対策上の役割に応じた教材の雛型について、昨今の脅威を踏まえた対策を追記するなど、必要な見直しを行い、各府省庁に配付した。
		e) ・ 各府省庁において、電子政府利用促進週間(2013 年 10 月 28 日～11 月３日)、情報セキュリティ月間（2014 年２月）等の機会において、情報セキュリティに係る直近の事例を踏まえ、情報の格付け・取扱制限、メールの適切な処理、情報の放置・安易な破棄の禁止等について意識啓発を行った。
(タ)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、内閣府、宮内庁、金融庁、財務省、環境省等において、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（通常の２年より長くしている）をはじめとした人事ローテーションに関する配慮が見られた。 ・ 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。 ・ NISC において、そうした個別の事例について調査を実施するとともに、事例共有に資するよう各府省庁に対し調査結果のフィードバックを行った。

(チ)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を推進した。 ・ また、NISC において、そうした個別の事例について調査を実施するとともに、事例共有に資するよう各府省庁に対し調査結果のフィードバックを行った。
(ツ)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を計７回開催し、政府機関における連携の強化を図った。また、同会議において、更なる情報セキュリティの確保のため、各府省庁において専任の対策官の設置や最高情報セキュリティアドバイザーの権限強化等、体制の充実強化を行うこと等を申し合わせた。
		b) ・ 内閣官房において、2013 年度に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」(情報セキュリティ報告書)に係る取組の推進	内閣官房 全府省庁	a) ・ 各府省庁において、自府省庁の情報セキュリティ報告書を作成し、内閣官房の作成する「政府機関における情報セキュリティに係る年次報告（平成 24 年度）」に掲載する形で、情報セキュリティ対策推進会議、情報セキュリティ政策会議に報告後、公表した。 ・ 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、各府省庁における情報セキュリティ報告書の比較・評価等を実施するとともに、優れた取組については、推奨事例候補として選出することにより、知見の共有やフィードバック等行った。 ・ また、政府機関統一基準群の改定に当たり、情報セキュリティ報告書に係る取組については各府省庁自らが達成目標や実施計画を策定する取組に刷新することとした。
		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、「政府機関における情報セキュリティに係る年次報告（平成 24 年度）」を作成し、情報セキュリティ対策推進会議で決定後、情報セキュリティ政策会議に報告し、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	・ 政府機関統一基準群の改定や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策定において、NICT、AIST 及び IPA の情報セキュリティに関する研究者・実務家の技術的・専門的な知見を活用した。
(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、関係省庁を通じて実施した独立行政法人に対する調査で、2013 年度末時点での情報セキュリティインシデントに備えた連絡訓練の実施状況を確認するとともに、独立行政法人を対象とした NISC 情報セキュリティ勉強会を開催し、情報セキュリティインシデントが発生した際の連絡体制をテーマとして取り上げることにより、その実効性の維持を図った。
(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)新たな「行動計画」の策定	内閣官房 重要インフラ所管省庁	・ 内閣官房において、重要インフラ所管省庁等と協力し、「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」（以下「第２次行動計画」という。）の施策の成果と課題をとりまとめ、第２次行動計画の基本的な骨格を維持しつつ、第２次行動計画の課題等を踏まえた修正・補強を行った「重要インフラの情報セキュリティ対策に係る第３次行動計画」（以下「第３次行動計画」という。）を策定した。
(イ)「安全基準等」策定方針及び重要インフラ分野における「安全基準等」の継続的改善	内閣官房 重要インフラ所管省庁	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）」及び同指針対策編の分析・検証を行い、分析・検証結果に基づき第３次行動計画において 2014 年度に指針（本編及び同対策編）を改訂することを明示した。
		b) ・ 重要インフラ所管省庁は、指針や各重要インフラ分野の特性を踏まえ、各重要インフラ分野における「安全基準等」の改善状況の分析・検証を行った。2013 年度は、２分野（医療、水道）で「安全基準等」の改定を実施した。
(ウ)「安全基準等」の整備浸透状況調査	内閣官房 重要インフラ所管省庁	・ ＜重要インフラ分野における調査＞ 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・検証及び改定等の実施状況並びに今後の実施予定等の把握及び検証を実施（2013 年 12 月）し、公表した。 ・ ＜重要インフラ事業者等に対する調査＞ 内閣官房において、重要インフラ所管省庁の協力を得て、各分野における安全基準等の整備状況、情報セキュリティ対策の実施状況等について調査を実施（2013 年４～９月）し、公表した。また、2014 年度の調査実施に向けて、重要インフラ所管省庁に対して調査内容の確認を行った。
(エ)共通脅威分析の実施	内閣官房	・ 内閣官房において、重要インフラ所管省庁及び重要インフラ事業者等の協力の下、重要インフラ分野における、情報セキュリティに係る設備等の実態を調査するとともに、将来想定される情報セキュリティに関する環境変化やそれに伴って発生する新たな脅威やリスクについて調査を行い、アンケート等の結果について各重要インフラ分野のセプターへ提供等を実施した。
(オ)リスク・コミュニケーションの充実	内閣官房 重要インフラ所管省庁	・ 内閣官房において、関係機関との意見交換会を実施した。 ・ 重要インフラ事業者等とリスク・コミュニケーションを行なう場として、分野横断的演習検討会を計５回実施するとともに、重要インフラ事業者、セプター及び重要インフラ所管省庁等とともに分野横断的演習を実施した。 ・ セプターカウンシルにおいて、重要インフラ事業分野の IT システムの利用現場や施設等の見学や紹介等の活動を３回行った。
(カ)「セプターカウンシル」の活動支援	内閣官房	・ 内閣官房において、セプターカウンシル事務局として、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 の企画・運営を通じて、カウンシル活動を支援した。2013 年度は、延べ 20 回の会合を開催し、分野横断的な情報共有の推進を図った。
(キ)共有すべき情報の整理	内閣官房	・ 第２次行動計画における情報共有の枠組みを通じて得た情報や環境変化を踏まえ、第３次行動計画の策定において、平時及び大規模 IT 障害時における共有すべき情報及びその共有方法について整理を実施した。
(ク)第２次行動計画の情報連絡・情報提供に関する実施細目に基づく情報共有の推進	内閣官房	a) ・ 実施細目に基づき、重要インフラ所管省庁等を通じ情報連絡を受け、内容に応じて関係省庁等への情報提供を着実に行った。（情報連絡 153 件、情報提供 49 件）
		b) ・ 第３次行動計画の策定等にあわせ、実施細目を見直し、改定を行った。
(ケ)実施細目に基づく情報共有に係るルールの改善等	重要インフラ所管省庁	a) ・ 各分野において、重要インフラ所管省庁から各セプターへの情報共有ルール及び重要インフラ事業者等から重要インフラ所管省庁への情報共有ルールについて、2013 年７月～10 月の間実施した情報共有の訓練（年１回実施）も活用し実施細目との整合性の確認等を実施した結果、情報共有ルールについては現行の通りとした。
		b) ・ 各分野において、セプター内における情報共有のルールについて、実施細目との整合性の確認、状況に応じた助言等を実施した。具体的には、情報共有ルールについては現行を維持しているが、情報共有の範囲等当該ルールの運用について適宜助言を実施した。
(コ)セプターの強化及び訓練	内閣官房 重要インフラ所管省庁	a) ・ 内閣官房において、重要インフラ所管省庁の協力を得て、2013 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。

		b)	・ 内閣官房において、重要インフラ所管省庁の協力を得て 2013 年７月～10 月にかけて 12 のセプターが参加し情報共有訓練を実施した。2014 年３月までに結果をとりまとめ、重要インフラ所管省庁及びセプターへ報告した。
(サ)「サイバー情報共有イニシアティブ」の強化	経済産業省		・ 2013 年６月、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（C⁴TAP）」との連携の実運用として脅威情報の相互共有を開始することで、情報流通先の産業分野を拡大した。さらに、2013 年度、ガス業界６組織、化学業界１組織が新たに参加し、参加組織数が 39 から 46 に拡大した。 ・ 各 SIG 内の活動においては、個別の事例を深く分析したり、複数の事例の相関情報を分析した結果の情報共有を行うなど、情報の充実、活動の活性化を行った。「標的型サイバー攻撃の特別相談窓口」と併せ、活動の中で得られた攻撃情報や検体などを「サイバー攻撃解析協議会」へ提供している。 ・ また、情報提供組織の意向に沿って JPCERT/CC に提供された情報をもとに、必要に応じて追跡調査や攻撃インフラとして悪用された設備の所有者や管理者への注意喚起を行った。
(シ)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。
(ス)分野横断的演習の実施	内閣官房 重要インフラ所管省庁		・ 有識者、重要インフラ事業者等及び重要インフラ所管省庁（オブザーバー）からなる「分野横断的演習検討会」を設置し、「情報セキュリティインシデントへの対応」をテーマに、検証課題や演習シナリオ等についての議論を進めるとともに、演習実施方法の改善や演習成果の普及に努め、2013 年 12 月に 61 組織 212 人の参加を得て（自職場からの３組織、10 人の演習参加者を含む。2012 年度より 64 人の増。）分野横断的演習（CIIREX2013：Critical Infrastructure Incident Response Exercise 2013）を実施した。 ・ また、演習当日及び後日に演習参加者による意見交換会を開催し情報共有の活性化と更なる気づきの創出を図った。 ・ 以上の 2013 年度演習の成果を整理、総括し、2014 年３月に結果を公表した。
(セ)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分野において、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、各分野における制御システムのセキュリティ評価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。
(ソ)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（インシデント件数 8,717 件：2013 年３月末現在）。そのうち、重要インフラ事業者を主な対象としたインシデント関する対応支援は 331 件、制御システムに関する対応支援は７件であった。
(タ)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)	・ 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）を設置し、検討会を計 25 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、「事例に基づく教訓集（仮称）」を取りまとめ、2014 年５月に公開し、業界団体等へ提供する予定。 ・ 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（34 号、36 号）に掲載した。
		b)	・ 制御システム・機器のセキュリティに関する規格である EDSA 規格に対して日本としての改訂要求を寄書し、IEC62443 への反映に貢献。EDSA 規格については IPA にて翻訳を行い、ウェブサイトを通じて公開され、IEC62443 規格のドラフト案を翻訳の上、標準化関係者へ展開。国内の製品認証制度の立ち上げにおいて、公益財団法人日本適合性認定協会（JAB）及び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、国内の認定及び認証制度確立を推進。

(チ)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、情報システム等の脆弱性情報の取扱いに関する研究会（脆弱性研究会、IPA）の下に、大学、制御システム製品開発者、制御システムユーザー、情報システム有識者、法律家等で構成するワーキンググループを立ち上げ、社会インフラの重要構成要素を制御するソフトウェアを含む制御システム製品への脆弱性関連情報の届出がなされた際の適切な対応を踏まえ、情報セキュリティ早期警戒パートナーシップガイドラインへの反映を行った。ガイドラインの改定案は 3 月 27 日に公開。 ・ JPCERT/CC において国内制御システムベンダの委員から構成される「制御ベンダにおける脆弱性取扱の社内体制整備促進検討会」を立ち上げ、脆弱性関連情報を受領した際のベンダにおける組織内取扱体制構築に必要と考えられる機能や要件を洗い出し、ベンダ社内の体制構築に資するモデルガイドラインを作成した。
		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、それぞれの関係者に対し 52 件の「早期警戒情報」を発行した。
		c) ・ JPCERT/CC において、ソフトウェア等の脆弱性に関する情報の発信を行っているサイト JVN（Japan Vulnerability Notes）を、より利用者に分かりやすいものとするため、所用の改善を行った。具体的には、脆弱性情報の案件ごと（海外案件か、国内案件かなど）に識別番号を設け、情報検索の利便性を向上、また脆弱性の分析結果について、国際標準に則った脅威のレベルを示すことにより、当該脆弱性の脅威に関する客観的な評価を利用者が認識することが可能となった。
(ツ)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に対しては、「制御ベンダにおける脆弱性取扱の社内体制整備促進検討会」において、脆弱性情報受領時の窓口機能の必要性に対する理解を促しつつ、連携のための環境整備を行った。また、制御システム保有組織関係者に対しては、インシデント発生時の対応に関する啓発活動や一部インシデント対応訓練への支援を通じて、連携体制の構築に取り組んだ。
(テ)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の認証制度を確立すべく、IPA が策定したパイロットプロジェクト計画に基づいて、JIPDEC により「制御システムセキュリティ認証基盤整備事業」を実施。本事業において、IPA より提案された認証スキーム及び認証基準案を基に、正式な認証制度の検討を開始し、本認証制度で用いる認証基準の定義や及びユーザーズガイドの策定等を実施。
(ト)制御機器等の評価・認証スキームの確立支援	経済産業省	・ 制御機器のセキュリティ評価・認証機関を 2014 年度までに設立できるよう、CSSC に対し必要な支援を実施した。 ・ 制御システムを所有する事業者のセキュリティマネジメントシステムの評価・認証事業を開始できるよう、一般財団法人日本情報経済社会推進協会（JIPDEC）に対し支援を実施した。
(ナ)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	・ 日本国内で制御機器のセキュリティ評価・認証が行えるよう、CSSC においてパイロット認証や評価・認証手法の技術開発を実施し、制御機器のセキュリティに関する評価・認証機関の設立ための準備を実施した。
(ニ)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	・ 制御機器の評価・認証において、制御機器のセキュリティ評価・認証制度について、日本の公益財団法人日本適合性認定協会（JAB）と米国国家規格協会（ANSI）との国際相互承認を合意した。
(ヌ)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、パイロット認証を２件実施し、評価・認証制度及びパイロット認証の成果を説明する約 150 人規模の会合を開催した。
(ネ)ソフトウェア、情報システムの信頼性向上	経済産業省	・ 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、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）を設置し、検討会を計 25 回開催。当該有識者の意見を踏まえながら、収集した情報を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、2014 年５月に公開予定。 ・ 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、高信頼設計・検証技術 WG、コンシューマデバイス安全標準化 WG）を設置し、検討会を計 14 回開催。また、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、2014 年５月に公開予定。さらに「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」を実施し、調査報告書を 2014 年７月に公開予定。
(ノ)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）-(ケ)

(ハ)重要インフラ事業者における人材育成の促進	内閣官房 重要インフラ所管省庁		・ 内閣官房が事務局を務めるセプターカウンシルにおいて、重要インフラ事業者等を対象としたワークショップ等を開催するなど、職員の情報セキュリティ意識の啓発と能力の底上げ等を実施した。
(ヒ)広報公聴活動の充実	内閣官房		・ NISC 重要インフラニュースレターを 22 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、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。 ・ 広報公聴に資するウェブサイトを充実させた。 ・ 行動計画に関する講演を１回行ったほか、第３次行動計画の策定に当たり、セプターや重要インフラ事業者等に対し、第３次行動計画やその施策について説明を行った。
(フ)重要インフラ分野での国際連携推進	内閣官房 総務省 経済産業省 重要インフラ所管省庁	a)	・ 重要インフラ政策に携わる政府機関が相互の連携について検討を行う MERIDIAN 会合に参加し、日本の情報セキュリティ政策等を紹介した。また、欧米や ASEAN 等の重要インフラ防護担当者との意見交換を通じて、情報セキュリティ政策の国際的な動向に関して情報収集を行った。
		b)	・ 重要インフラニュースレター等において、海外の関連動向やセキュリティ脅威に関する情報を紹介した。
(ヘ)電気通信システムの安全・信頼性確保	総務省		・ 2012 年度に発生した電気通信に関する事故の発生状況等の分析・評価等を行った結果を 2013 年９月２日に公表した。
(ホ)重要無線通信妨害対策の強化	総務省	a)	・ 重要無線通信妨害事案の発生時の対応強化のため、重要無線通信妨害申告受付について、夜間・休日の全国一元的受付を継続するとともに、地方総合通信局等における出動体制を見直し、また、携帯型電波監視機器の整備を進め、夜間・休日における迅速な出動体制の強化に努めた。
		b)	・ 電波利用秩序維持のため、遠隔操作による電波監視施設等の性能向上を図りつつ、同施設のセンサー42 か所を 2013 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に必要となる電波監視技術等について、調査研究等を実施した。
(マ)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		・ 日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議での検討を踏まえ、ASEAN 地域の情報セキュリティ強化支援政策の一環として、一般財団法人海外産業人材育成協会（HIDA）の要請に基づき、IPA より制御システムのマネジメントシステム（CSMS）に関する研修を実施。IEC62443-2-1 の解説に加え、国内外の制御システムのセキュリティの概況、課題、対応策等に関する教育を実施した。

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) ・ 中小企業の情報セキュリティ対策実施を促進するため、全国各地の商工会議所・商工会関係者・IT コーディネータ等に対して、中小企業情報セキュリティ対策指導者育成セミナーを全国 21 カ所で開催し、1,019 人が参加した。
		b) ・ 中小企業がコストをかけずに情報セキュリティ対策を行う「最低限の情報セキュリティ対策」及び「中小企業の情報セキュリティ対策ガイドライン」(小冊子) を Web で公開するとともに、イベント・セミナーでの配布及び本コンテンツを教材としたセミナーを全国で開催した。 ＜実績＞ ○イベント・セミナーでの配布　25,356 部 ○Web ダウンロード件数　32,729 件 ○セミナー実施回数　48 回
(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	・ 高度なセキュリティが確保されたソフトウェアへの投資を支援する中小企業投資促進税制について、業界団体等が主催する各種セミナーなどにおいて紹介・解説するなど、利用促進のための周知活動を行うとともに、更なる投資の促進を図る観点から、2014 年度税制改正において、措置内容の拡充及び適用期間の延長を行った。
(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	・ IPA において、中小企業・小規模事業者の新ビジネス創造促進のための IT 活用サービス提供者からの要請に応じて情報セキュリティ確保等の観点からの支援を行うための体制を構築した。
(エ)個人情報漏えい等防止のための対策	経済産業省	・ 個人情報取扱事業者が取り組むべき技術的安全管理措置に関しては、各技術的安全管理手法の有効性等を検証し、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の改定を検討した。
(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	内閣官房 経済産業省	・ 産業界と政府が一体となり営業秘密保護に関する情報共有・検討などを行なう体制の立ち上げのための検討を進めている。 ・ また、①産業界全体としての問題意識の喚起、②産業界全体の実態調査と課題の抽出、③漏えい事例やベストプラクティス等の事例情報の蓄積・共有、2014 年度は独立行政法人情報処理推進機構 (IPA) において事業を実施する予定。
(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開始の可否について提案が行われたことなども踏まえ、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	・ 企業・組織における情報セキュリティ被害状況調査の調査データを元に、IPA 及び (独) 経済産業研究所 (RIETI) の共同研究において、効果的な情報セキュリティ対策についての経済的観点からの分析を実施し、業種・企業規模別に有効な対策についての結果を学術的な観点で RIETI から DP(Discussion Paper) 、また一般企業向けには IPA から以下のように公表した。 RIETI「An Empirical Analysis of the Effectiveness of Information Security Measures」 (2013 年 10 月) IPA「企業における情報セキュリティ対策効果に関する検証」 (2014 年３月)
(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、「ユーザ企業におけるクラウドセキュリティ確保の検討」、「企業における情報セキュリティ活動の見える化」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。
(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) ・ 「2013 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/IEC 15408) 認証取得製品の導入状況について調査を実施した。
		b) ・ 監査企業台帳に関する規則の遵守徹底を図り監査企業台帳の品質を向上させるため、監査企業台帳の申告の案内の際に、監査企業台帳の申告内容に虚があり、監査の品質に疑義が生じた場合は、台帳からの登録抹消があり得る旨を追記した。

		c) ・ 情報セキュリティガバナンス協議会の会合において、情報セキュリティ報告書モデルをはじめとする企業の情報セキュリティ活動に関する情報発信の在り方について議論し、その効果や課題を共有した。
(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・モデル取引・契約書」を基に、一般社団法人コンピュータソフトウェア協会及び一般社団法人日本コンピュータシステム販売店協会が「情報システム取引者育成プログラム」を 2010 年より展開し、現在までに合計で約 2,350 名が受講している。
(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	・ 総務省、法務省及び経済産業省において、2012 年度に開催された「電子署名法の施行状況に係る調査研究会」の検討結果等を踏まえ、利用申込者の本人確認の見直しによる本人確認方法の多様化を図るため、「電子署名及び認証業務に関する法律施行規則」の一部改正案を検討したほか、総務省において「電子署名普及促進セミナー」を開催し、企業における電子署名の利活用の普及促進策を実施した。
(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、政府機関統一基準群の見直しに合わせ、「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」を策定予定である。
		b) ・ 制度で採用する国際標準を NIST と共同で開発し、暗号モジュールセキュリティ要件 ISO/IEC 19790 及び暗号モジュール試験要件 ISO/IEC 24759 の２件の国際標準化を完了させたことにより、制度開始に向けての環境整備を終えた。覚書の締結については、NIST における上記国際標準に基づく認証制度を立ち上げることの決定を待ち、実務者レベルで合意した内容を元に IPA で作成、提示済みの覚書に署名されることになる予定である。覚書締結に先立ち、共同認証の業務の運営主体となる法人組織について NIST で検討が開始されている。 ・ ハードウェア脆弱性評価に関する人材育成については、サイドチャネル解析ツール、パータベーション攻撃ツールを IPA で整備するとともに大学、評価機関、ハードウェアベンダへの啓発活動を展開している。
		c) ・ IPA を通じ、CCRA における複合機に関するコラボラティブ・プロテクション・プロファイル（cPP）の整備に向けた活動を実施した。
(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の会合において、我が国における CISO の在り方や問題点等について普及した。
(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	・ JPCERT/CC において、標的型攻撃を始めとする巧妙かつ執拗に行われる攻撃に対抗するため、そのような脅威を想定した組織内 CSIRT の構築・運用に関するマテリアルを作成し、２つの組織に対してそのマテリアルを基にした CSIRT 機能の強化策を試行しマテリアルの有効性を検証した。 ・ また、そのような脅威に対処するための演習に関するマテリアルを作成し、１つの組織に対してその演習を試行した。
(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	・ IPA のウェブサイトで継続的にサービスを提供している。利用件数も、月平均で 5,000 アクセスを記録するなど、年々増加してきている。
(タ)内部者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	・ 「内部不正ガイドライン」の英語版を作成し、国際会議や海外と協業する関連機関（JPCERT/CC など）へ配付をした。 ・ 国内では、NPO 日本ネットワークセキュリティ協会（JNSA）が本ガイドラインをベースにソリューションガイドを作成することに支援し、ガイドラインに製品等を対応付け、実際の対策に役立つ取組を実施した。 JNSA ソリューションガイド： http://www.jnsa.org/solguide/incident/2013/index.htm
(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	・ 情報セキュリティ月間の冒頭に、企業等の経営層をターゲットとしたシンポジウムを開催し、経営戦略として情報セキュリティを位置付けるための意識啓発を行った。
(ツ)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	・ 2013 年６月 20 日に「情報セキュリティ対策ベンチマーク バージョン 4.2」を公開。またベンチマーク利用を促進するため、A5 小冊子「情報セキュリティ対策ベンチマーク」をイベント・セミナー等で配布した。 ＜実績＞ ○システム利用件数　2,030 件 ○イベント・セミナーでの配布　7,913 部 ○Web ダウンロード件数　3,211 件

(テ)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（2013 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。 ・ 学校における情報セキュリティの確保について、各都道府県政令指定都市教育委員会に周知。（2013 年７月） ・ 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。（2013 年 11 月及び 2014 年１月）
(ト)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。
(ナ)個人情報保護法の見直し	消費者庁 関係府省庁	・ 消費者庁より、「平成 24 年度個人情報の保護に関する法律施行状況の概要」について、消費者委員会へ報告した（2013 年 10 月）。 ・ なお、2013 年 12 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見直し方針」が決定され、内閣官房をはじめ関係省庁と連携しつつ、2014 年６月までに法改正の内容を大綱として取りまとめるための検討を行っている。

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	・ 内閣官房において、各府省庁と協力し、「情報セキュリティ普及・啓発プログラム」の見直しを行い、2014 年度以降の具体的な取組について「新たな情報セキュリティ普及・啓発プログラム（仮称）」を策定するための検討・調整を実施し、その方向性を公表した。（2014 年６月末頃に策定予定）
(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 経済産業省 文部科学省 防衛省 関係省庁	・ 内閣官房において、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、防衛省と協力し、相互の連携強化を図るため、「情報セキュリティ普及啓発関係府省庁連絡会議」を定期的に開催（2013 年６月、７月、８月、10 月、11 月、2014 年３月）し、情報セキュリティ月間及び国際キャンペーンにおける取組の充実強化策の検討、サイバーセキュリティの日の新設並びに情報セキュリティ普及啓発ロゴマークの策定等を推進した。
(ウ)「サイバー衛生の日（サイバー･クリーン･デー）」(仮称)の新設	内閣官房 内閣府 警察庁 消費者庁 総務省 外務省 経済産業省 文部科学省 防衛省 関係省庁	・ 内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、経済産業省、文部科学省、防衛省及び関係省庁において、月間の趣旨を広く一般国民に啓発するとともに、特に、深刻化・高度化するサイバー空間の脅威やその対応策等について理解を深めることを目的として、月間の最初のワーキングデーを「サイバーセキュリティの日」として新設した。
(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、普及啓発を推進した。
(オ)表彰等の充実	総務省 経済産業省	a) ・ 2013 年度「情報通信月間」において、総務大臣表彰として８件の個人・団体を表彰した。 ・ 2013 年５月に開催された「第８回情報危機管理コンテスト」の優勝チームに対し、経済産業大臣賞を授与した。 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プロジェクトを 17 件（クリエータ数:22 人）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	・ 内閣官房において、各府省庁と協力し、関連行事の開催、各府省庁・関係機関ホームページにおける周知等の従来の取組に加え、「国民を守る情報セキュリティサイト」における情報セキュリティ有識者コラムの日替り掲載、情報セキュリティ普及啓発リーフレットやアニメーションの作成、サイバーセキュリティの日の新設等の新たな取組を実施し、「情報セキュリティ月間」の内容の充実とより一層の周知を図った。
(キ)国際連携を活用した普及・啓発活動の実施	内閣官房 関係府省庁	・ 2012 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、2013 年においては、国際連携・協力に係る取組により焦点を当てて、関連取組を支援するとともに、主に ASEAN と連携しながら、一般国民向けの意識啓発教材の作成・配布などに取り組んだ。
(ク)「情報セキュリティ国際キャンペーン」の実施	内閣官房 関係府省庁	・ 2012 年に引き続き、10 月に「情報セキュリティ国際キャンペーン」を実施し、国際連携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、ポスター等の周知用素材の作成・配布、動画等を活用した情報発信に努めた。また、特に、ASEAN 等と連携した共同意識啓発活動を進め、ASEAN の有識者が参加したシンポジウムを日本で開催した。
(ケ)「情報セキュリティ普及・啓発プログラム」の推進	内閣官房 関係府省庁	a) ・ 内閣官房において、各府省庁と協力し、「情報セキュリティ普及・啓発プログラム」に基づき、毎年２月に行う「情報セキュリティ月間」、10 月に行う「情報セキュリティ国際キャンペーン」を通じて集中的に普及啓発に取り組むとともに、「サイバーセキュリティの日」を新設するなど、本節に掲げる普及・啓発活動の充実・強化施策を推進した。

		b) ・内閣官房において、２月の情報セキュリティ月間等を通じ、自ら実施している対策がどのフェーズにあるのかを客観的に認識するためのツールである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するとともに、関係府省庁・業界団体等に対するメールを通じて周知させた。 ・同チェックリストについては、組織内の教育教材として活用しようと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、高齢者層を中心に幅広い層を対象としたリーフレットをリニューアル（2013 年 12 月）し、「国民を守る情報セキュリティサイト」に掲載したほか、各府省庁、関係企業等の協力の下、講習会等の場で資料を配布するなど周知させた。 ・また、「情報セキュリティを考えるグローバルシニアネットフォーラム」（2014 年２月）における講演等を通じて周知させた。
		d) ・情報セキュリティ月間（2014 年２月）において「情報セキュリティ月間キックオフ・シンポジウム」を開催し、企業等の経営層や管理職等をターゲットに情報セキュリティの重要性を訴求した。 ・また、全国８ブロックで情報セキュリティセミナーを開催し、企業の経営層を対象に含む講演等を実施した。
(コ)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 経済産業省 文部科学省	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」、メールマガジン、ソーシャルネットワーキングサービス等の活用を通じ、幅広い対象への情報提供を実施した。情報提供に当たっては、情報セキュリティ無関心層の関心を喚起しやすいよう、情報セキュリティに関わる多方面で活躍する有識者によるコラムの日替わり掲載や、川柳を用いたクイズなどを取り入れるなど工夫した。 ・内閣官房において、企業、一般国民等に対し、「情報セキュリティ月間キックオフ・シンポジウム」（2014 年２月）等講演を実施した。 ・「@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！」を活用した広報啓発活動を実施した。 ・総務省「国民のための情報セキュリティサイト」について、スマートフォンや SNS 等の新たな技術やサービスの登場等情報セキュリティ対策を取り巻く環境の変化を踏まえ、2013 年４月にサイトのリニューアルを実施するとともに、適宜最新のトピックを追加するなど国民への情報提供を行った。
		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、2013 年 10 月の情報セキュリティ国際キャンペーン及び 2014 年２月のサイバー空間の脅威に対する対処能力の強化のための広報月間の間は、全国各地で広報啓発活動を重点的に実施した。
		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、2014 年３月末までの間に延べ 8,428 件の講座を実施した。 ・2013 年度は、過去最多の実施件数（2014 年３月末時点で 2,073 件）となった。
		d) ・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 2013 年度に作成し、利用者及び事業者向けセミナー等を実施するなど普及啓発を推進した。
		e) ・全国約４万の小中高校・高等専門学校、教育委員会などによびかけ、標語・ポスター・四コマ漫画のコンクールを開催し、受賞作品を決定した。 ＜実績＞ ○作品数：33,335 点　※前年度比 19%増（27,946 点） （標語：26,198 点、ポスター：2,814 点、漫画：4,323 点） ○授賞式回数（全国、地域）　11 回 ○受賞作品のイベント展示数　40 回 ○小中高校への出前授業実施回数　39 回 ○マスコット着ぐるみ出演回数　13 回
		f) ・インターネット一般利用者の情報セキュリティ対策実施を促進するため、全国各地の小中学校や NPO 法人と協力し、インターネット安全教室を全国 120 カ所で開催、7,968 人が参加した。

		g) ・広く企業及び国民一般に情報セキュリティを普及させるため、地域の要請に応じた講師の派遣、イベントへの出展、印刷資料・映像コンテンツの配布、普及啓発を希望する方を登録して支援するセキュリティプレゼンター制度「iSupport」、官民情報セキュリティポータル「ここからセキュリティ！」の運営を実施した。 ＜実績＞ ○講師派遣数： 191 回 ○主催イベント開催数：４回（主な２件は下記） ①日韓情報セキュリティシンポジウム （2013 年 12 月 13 日@ベルサール飯田橋：200 名） ②IPA サイバーセキュリティシンポジウム （2014 年２月 19 日@イイノホール：434 名） ○イベント出展数：11 ヵ所 （内 情報セキュリティ EXPO：参加 7,423 名） ○資料・映像配布数： 資料　配布数：25 種、計 181,271 点 映像　YouTube 等再生： 158,235 回 研修用途の DVD 請求： 2,090 組織 ○プレゼンター登録数： 58 名 ○ここからセキュリティ！PV： 37 万件
		h) ・IPA において、安全なウェブサイト運営に根ざしたアプリケーション開発手法を学習する「脆弱性体験学習ツール AppGoat」を機能拡張し、３月に公開。また、脆弱性対策をテーマにした、IPA 主催セミナーを年６回開催するなど、脆弱性対策の普及啓発の推進に努めた。 ・JPCERT/CC において、開発者向け活動として、脆弱な製品開発を低減させるための活動として C/C++、Java、Android 開発に関する新たな情報発信をしたほか、セキュリティ対策が進まない制御開発者に向けたセキュアコーディング啓発情報発信についても 2013 年度に実施した。 ・運用者やエンドユーザー向けに脆弱性対策の促進のため対策判断に使われる JVN の分析結果に、表を用いる等よりわかりやすいデザインの CVSS を導入した情報発信を利用者に対して実施し正確な対策判断を支援する。このための作業は 2013 年度中に完了しており、2014 年４月より CVSS による発信を開始する。
		i) ・直近の情報セキュリティに関するトレンドやトピック等を取り上げて毎月公開している「今月の呼びかけ」や、年末年始・ゴールデンウィーク等の長期休暇前に留意すべき点を取りまとめた注意喚起に加え、届出・相談等の統計情報を四半期ごとに公開するなど、計 29 件の情報を発信した。
(サ)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、「情報セキュリティ月間キックオフ・シンポジウム」（2014 年２月）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を紹介するなど情報を共有化した。 ・共有化に当たり必要に応じて匿名化するなど、今後の情報収集の妨げとならないよう配慮した。
(シ)無線 LAN の情報セキュリティ確保の推進	総務省	・無線 LAN の利用における情報セキュリティ上の課題について、利用者及び事業者へのセミナーを全国 11 カ所で実施し、適切な無線 LAN の情報セキュリティ対策の普及・啓発を行った。
(ス)電波利用秩序維持のための周知啓発活動の強化	総務省	・毎年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、ポスター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。
(セ)情報漏えい対策への取組	経済産業省	a) ・家庭や企業・組織のパソコン等にインストールすることで、ファイル共有ソフトの実行を禁止することができ、またファイル共有ソフトがインストールされていないことを証明することにも利用が可能な「情報漏えい対策ツール」を引き続き公開。2013 年４月５日に Ver2.0 版の提供を開始し、例年よりも多い、計 11,527 件の提供を実施。※2013 年度総計値
		b) ・インターネットバンキング利用者を狙った不正送金の事例や文字入力を補助する IME の利用上の注意点、スマートフォンのワンクリック請求アプリ等、ユーザーの重要な情報や金銭を窃取する事例等を交え、その対策を IPA のウェブサイト等で公開し、国内のセキュリティ対策の促進。

(ソ)サイバー攻撃高度解析機能の整備	総務省 経済産業省	・ サイバー攻撃解析協議会のオフラインでの実務者会合を２回開催し、脅威の傾向についての共有や取組の検討を行った。 ・ 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立ち上げと運用を行った。 ・ Web 改ざん攻撃への対応についてサイバー攻撃解析協議会で協議した上で研究者を交えた意見交換を実施し、データ提供を行った。
(タ)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-(ソ)
(チ)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	・ 警察庁において、全国警察による捜査、情報収集、分析等の司令塔として、警察庁警備局警備企画課に同課の「サイバー攻撃対策官」を長とする「サイバー攻撃分析センター」を設置することにより、サイバー攻撃に係る情報の早期把握及び被害の拡大防止に資する情報収集を推進するとともに、13 都道府県警察において「サイバー攻撃特別捜査隊」を設置することによりサイバー攻撃への対処体制を強化した。 ・ また、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。 ・ 警察庁において、サイバー攻撃手法に関する知識・技能の習得を目的とした民間委託研修を実施するなど、サイバー空間におけるサイバー攻撃の予兆の早期把握を可能とする態勢を整備した。 ・ 政府のサイバーテロ・サイバーインテリジェンスに関する対策に資する関連情報の収集・分析に努めるとともに、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。
(ツ)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) ・ 警察庁において、全国警察による捜査、情報収集、分析等の司令塔として、警察庁警備局警備企画課に同課の「サイバー攻撃対策官」を長とする「サイバー攻撃分析センター」を設置することにより、サイバー攻撃に係る情報の早期把握及び被害の拡大防止に資する情報収集を推進するとともに、13 都道府県警察において「サイバー攻撃特別捜査隊」を設置することによりサイバー攻撃への対処体制を強化した。 ・ また、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、分析し、また、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通じて、サイバー攻撃の実態解明を図っている。 b) ・ サイバー攻撃事案の実態解明に資するため、インターネット観測技術に関する調査研究を行った。
(テ)新しい脅威・攻撃の分析・共有	経済産業省	・ 定期的に研究会を開催し、成果物として「標的型メール攻撃におけるシステム設計ガイド」を 2013 年８月に公開した。システム設計ガイドの作成に当たっては、NISC 協力の下で、攻撃を受けた省庁をヒアリングし、想定脅威に応じた対策を立案している。
(ト)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) ・ JPCERT/CC において、インシデント報告の受付、攻撃手法の解析及び被害の発生・拡大の抑止のためのインシデント発生源等への連絡調整、脅威情報の収集・分析、注意喚起等の情報発信、脆弱性関連情報に関する製品開発者間の調整、製品開発者への情報提供から対策情報公開に至るまでの調整を迅速に行うための製品開発者連絡網の拡充等の活動を継続して行うとともに、国内金融機関を狙うフィッシング詐欺や情報窃取型マルウェアの増加に対応するため「フィッシング対策協議会」との間の情報連携を一層強化し、マルウェア等の分析及びフィッシングサイトの閉鎖のための調整を行った。2013 年度（2014 年３月末現在）のインシデント報告件数は、29,191 件。 ・ 攻撃手法や脅威動向に関する情報共有・連携を目的とする、情報セキュリティに関する専門家や事業者、関係機関との間で年間 30 回を超える会合を開催した。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組を進めた。 ・ 制御システムセキュリティ情報共有コミュニティの活動として、制御システムに関するセキュリティインシデントに関わる事例その他の技術動向に関する情報共有のための月刊のニュースレターを、２月末現在 353 名の登録者にメール配付した。また、コミュニティを通じて、自己評価ツール等の普及を進めた。自己評価ツールの直接配布人数は累計 343 名であり、再配布を許諾して普及を促している。

		b) ・ JPCERT/CC において、APCERT（Asia Pacific Computer Emergency Response Team）のメーリングリスト、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）の情報共有を進めている。 ・ 10 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２月に実施された APCERT のメンバーを中心とする「APCERT Drill 2014」において、各国チームがマルウェアや攻撃手法の解析を行い結果を共有した。 ・ 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、2012 年度から継続して共有を行なっている海外組織に加え、IWWN の加盟組織との共有も開始した。
		c) ・ 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。また、執拗な標的型攻撃への対応を効果的に行うためのオンサイトでの情報収集、対処、調整支援を実施。2013 年度のインシデント報告件数は、29,191 件。
		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。法改正や技術動向の変化を踏まえたガイドラインを作成し、公開した。
(ナ)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	・ 年間 40 回の注意喚起を発信し、エンドユーザー及びシステム管理者へのセキュリティ対策の啓発に努めた。
(ニ)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) ・ 米国国土安全保障省が管轄するサイバー攻撃対策向けの研究データを入手し、NICT で取得している研究データとの突合分析によりサイバー攻撃対策の研究に活用するとともに、研究者間で連携に向けた議論を行った。また、この進捗は第５回の「インターネットエコノミーに関する日米政策協力対話」（2014 年３月、東京）にて当該進捗状況を米国と確認した。
		c) ・ 「日 EU・ICT セキュリティワークショップ」（2013 年 12 月、ベルギー）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、EU 加盟国との共同研究を開始すべく意見交換を実施した。
		d) ・ 新たにフィリピン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」（2013 年８月、東京）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」の開始を「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、東京）にて確認するなど、ASEAN 諸国との連携を推進した。
(ヌ)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	・ 高度化・巧妙化するマルウェアの被害を防止するため、ネットワーク型のボットウイルスに感染したユーザーを検知し、マルウェアの除去を当該ユーザーに促すほか、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、2013 年 11 月から ISP 等により実施し、マルウェア感染を防止するための仕組みを構築した。
(ネ)革新的な情報セキュリティ技術の研究開発基盤の構築	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及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プロトタイプ開発を行った。 ・ また、組織内ネットワークを流れる通信及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 改の開発に着手した。
(ノ)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	・ 2013 年 11 月から「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」を開催し、サイバー攻撃が巧妙化、複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能になるよう、サイバー攻撃への適正な対処の在り方について検討を行い、2014 年４月にとりまとめを実施。

(ハ)脆弱性に関する情報収集・提供	経済産業省	・ 従来の届出の受付による脆弱性関連情報以外に、自ら海外からの情報等を基にした、国内ではインシデントに至っていない脆弱性を利用したマルウェア等の収集を行い、分析の上、関係者への通知等提供を行った。2013 年度は 250 件以上の収集を実施。
(ヒ)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、継続的に「JVN iPedia」及び「MyJVN」のサービスをエンドユーザーに提供している。JVN iPedia の登録件数は、４万件を超過し、海外からの脆弱性対策情報を１営業日以内に日本語翻訳して公開している。 ・ 連絡が不能となった脆弱性情報届出案件を公表することを主とし告示改正に関し、実運用上の問題点や解決案などについて検討を行い、併せて IPA が提供する情報セキュリティ早期警戒パートナーシップガイドラインの同期を図った。 ・ 脆弱性研究会の下に、制御システム脆弱性取扱検討ワーキンググループを設け、制御システム製品への脆弱性関連情報の届出がなされた際の適切な対応をまとめ、情報セキュリティ早期警戒パートナーシップガイドラインへの反映を行った。 ・ JPCERT/CC において、「脆弱性関連情報届出受付制度」における調整機関業務を着実に実施するとともに、海外からの脆弱性情報連絡窓口としての活動を並行して行い、日本の製品開発者にはシームレスな調整を継続して実現し続けている。また、連絡不能開発者に関する告示の改正や制御システムの脆弱性の取扱いに関する協議にも参加し、現場の経験に基づく制度策定にも貢献した。
(フ)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）について、IPA が運用する MyJVN API 及び NIST（National Institute of Standards and Technology）の NVD（National Vulnerability Database）を外部データソースとして利用する方式への切り替えを 2010 年度に実施した。これによる 2013 年度の配信件数は 10,820 件であった（2014 年３月 10 日現在）。
		b) ・ 継続的に IPA のウェブサイトで継続的に icat を提供している。現在、約 700 のウェブサイトで icat を掲載していただいており、注意喚起情報のタイムリーな提供を行っている。
(ヘ)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) ・ 2013 年の１年間だけで、過去最多となる 127 のソフトウェア製品の脆弱性対策情報を一般に公開した。また、ウェブサイトにおいても、手紙や電話による運営者への説明を行い、759 のウェブサイトで脆弱性が解消された。
		b) ・ 「ソフトウエア等脆弱性関連情報取扱基準」（経済産業省告示）に基づいて運用している脆弱性ハンドリング体制について、滞留案件対策として 2011 年度より開始された連絡不能開発者リストの公表により、滞留案件数は著しい改善がみられたが、そのような活動によっても、引続き開発者と連絡が取れない案件の公表是非について、当事者ではない第三者の判断を仰ぐべく、公表判定委員会の発足が脆研で議論されてきた。その実現に当たり、告示の改正が必要であるとの判断が経済産業省によってなされ、2014 年１月末から１カ月かけてパブリックコメントが募集された。正式な告示は、その結果を反映させて今後公表される予定である。この告示改訂版に連動して公表される「早期警戒パートナーシップガイドライン」では、制御システムの届出をハンドリングする際の配慮も加えられ、状況に応じたより適切な運用の実現が可能となる。製品開発者向けの活動では、既に発行済みの C/C++セキュアコーディングスタンダードへの更新の反映、Android に作り込まれる脆弱性対策の情報発信のほか、遅々として進まない制御開発者向けに、セキュアコーディング導入の敷居を下げるための発信情報を準備中である。
		c) ・ IPA では、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［C 言語版］」を改訂し、新たに Ver.2.0 として３月７日に書籍を発行。 ・ 最新 JIS 規格「C99」に対応し、旧版（Ver.1.1）からのルールを継承しつつ、C99 から新たに追加・変更された機能等に対応し、また ESCR と相互に内容を引用している関係にあり、同じく近年改訂が行われた、欧州組込み業界標準規格の「MISRA C」（MISRA C:2012）に対応した内容。
		d) ・ 「TCP/IP に係る既知の脆弱性検証ツール」及び「SIP に係る既知の脆弱性検証ツール」を引き続き提供した。
		e) ・ AppGoat を題材にしたセミナーを年４回実施し、ウェブアプリケーションの脆弱性対策を広く普及した。
		f) ・ IPA から公開した「自動車の情報セキュリティへの取組みガイド」を基に、国内外において展示・講演を行うなど、自動車の情報セキュリティ対策の普及を実施した。

		g) ・ 脆弱性を検出する技術（ファジング）を普及・啓発するための活動として、以下を実施した。 ○ファジング支援ツールの公開 ○普及啓発資料の公開（４種類）、講演（４回） ○脆弱性の検出 ○ファジング入門セミナー実施（２回）
(ホ)ソフトウェアの脆弱性への対応に関する制度の在り方	経済産業省	・ 情報システム等の脆弱性情報の取扱いに関する研究会（脆弱性研究会）において、大学、制御システム製品開発者、制御システムユーザー、情報システム有識者、法律家等で構成するワーキンググループを立ち上げた。本 WG にて４回の会合を実施し、制御システム関係者への 10 回のヒアリングを経て、社会インフラの重要構成要素を制御するソフトウェアを含む制御システム製品への脆弱性関連情報の届出がなされた際の適切な対応をまとめ、情報セキュリティ早期警戒パートナーシップガイドラインへの反映を行った。ガイドライン（案）は３月末に公開予定。
(マ)脆弱性ハンドリングの国際調整	経済産業省	・ 2013 年６月に全世界で公開されている脆弱性情報の識別に関する WG が FIRST で立ち上がり JPCERT/CC は事務局として運営に参加している。定期的にテレカンを実施する等仕組みの構築の可能性について検討を重ね、関連情報を保有する組織に対して保有情報の分類につながる調査を実施し現在回答を集約している。 ・ JPCERT/CC において、過去数年にわたって策定に協力してきた脆弱性情報ハンドリングプロセスの国際標準化は、最終的には２つの標準に分かれ、ISO/IEC 29147（脆弱性の開示に関する標準）と ISO/IEC 30111（脆弱性ハンドリングプロセスに関する標準）として、それぞれ 2014 年２月５日、及び 2013 年 10 月 22 日に発効された。内容的には、国内の制度と大きな乖離はないものとなっている。
(ミ)組込み機器の脆弱性対策の推進	経済産業省	・ 今後ネットワークに繋いだ利活用が見込まれる医療機器についての脆弱性を含むインシデントや情報セキュリティ施策の現状を調査し、セキュリティ上の脅威を整理するとともに、将来に向けた課題等の提言を行った。
(ム)制御システムに係る脆弱性ハンドリング体制の改善	経済産業省	・ JPCERT/CC において国内制御システムベンダからの委員によりなる「制御ベンダにおける脆弱性取扱の社内体制整備促進検討会」を立ち上げ、脆弱性関連情報を受領した際のベンダにおける組織内取扱体制構築に必要と考えられる機能や要件を洗い出し、ベンダ社内の体制構築に資するモデルガイドラインを作成した。
(メ)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	・ 一般社団法人 TERAS が、ソフトウェアシステム・サービスの安全性・信頼性を利用者に第三者が説明できるよう品質説明力を強化するオープンなソフトウェアツールキット TERAS をオープンソースソフトウェアとして 2014 年４月に公開予定。110 社の企業がこのツールキットを活用実証している。 ・ IPA において、組込みソフトウェアメーカ、システムインテグレータ、第三者検証事業者等有識者の意見を踏まえながら、2013 年６月 12 日に「製品・システムにおけるソフトウェアの信頼性・安全性等に関する品質説明力強化のための制度構築ガイドライン」を策定し、公表。 ・ 利用者への品質説明力の強化については、パッケージソフトウェアの分野から取組を開始し、一般社団法人コンピュータソフトウェア協会(略称「CSAJ」)が同制度ガイドラインに準拠したパッケージソフトウェア品質認証制度（PSQ 認証制度）を正式に運用開始（事業化）。
(モ)SOC 事業者間等における情報共有の促進	内閣官房 総務省 経済産業省	・ 内閣官房、総務省及び経済産業省において、民間の CSIRT や SOC 事業者の団体等と会合や意見交換を行い、官民による情報共有の推進を図った。
(ヤ)スパムメール対策の強化	内閣官房 総務省 消費者庁	a) ・ 総務省及び消費者庁において、2013 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。
		b) ・ 引き続き、迷惑メール対策推進協議会と協力し、各種業界団体等に対して送信ドメイン認証技術等迷惑メール対策技術の導入を推進するための説明会を５回開催した。
		c) ・ 外国執行当局との連携を強化するため、ロンドンアクションプラン第９回会合（2013 年 10 月）のようなマルチラテラルの場や、個々の国との間におけるバイラテラルな場で、スパム対策に関する情報交換や国際的な協力関係の構築に向けた意見交換等を実施した。 ・ 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、2013 年５月から、ベトナム当局（VNCERT）との間で、新たに開始した。
		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。

(ユ)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７月に暗号プロトコル評価ポータルサイトを開設し、安全性に関する評価結果の公開を開始した。さらに、2013 年 12 月には複数の暗号プロトコル評価ツールを用いて多角的な評価を自動的に行う評価システムを開発し、公開した。また、2013 年 12 月、国際的な連携体制として「暗号プロトコル評価技術コンソーシアム」を設立した。 ・ 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。
(ヨ)IPv4 アドレスの枯渇に伴う諸課題への対応推進	総務省	・ 総務省において、IPv4 アドレスを共同利用する環境における通信の安全性・信頼性の確保のため、情報セキュリティ等に係る技術的諸課題を解決するための実証実験を実施し、その成果をガイドラインとしてまとめ講演会で周知した。
(ラ)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もに、ITU-T SG17 において X.1037 として勧告化を実施した。
(リ)IPv6 環境における脆弱性検証ツールの貸出し	経済産業省	・ 継続してツールの貸出を実施した。
(ル)インターネット利用環境の変化に伴う情報セキュリティ対応推進	総務省	・ 再掲：１-①-１）-(へ) g)

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体制等の強化	警察庁	a) ・ 13 都道府県警察に「サイバー攻撃特別捜査隊」を設置し、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。
		b) ・ 警察庁に「サイバー攻撃対策官」及び「サイバー攻撃分析センター」を設置し、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。
		c) ・ サイバー攻撃に係る体制等を強化するため、リアルタイム検知ネットワークシステムを更新し、サイバー空間の観測機能の強化をし、サイバーフォースセンターの技術力向上等を行った。
		d) ・ 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。
(イ)悪質・巧妙化するサイバー犯罪の取締りのための態勢の強化	警察庁	・ 警察のサイバー犯罪捜査指揮を担当する警察職員を対象とした専科教養を実施した。 ・ 都道府県警察のサイバー犯罪捜査官を対象とした民間委託教養による専科教養を実施した。 ・ 都道府県警察のサイバー犯罪捜査用資機材の増強を実施 ・ 2013 年４月に、都道府県警察に対して、民間事業者等の知見の活用を指示した。
(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の設置を推進し、匿名性排除のための会員制導入の働き掛けや防犯情報の提供等の情報共有を行うなど、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、児童ポルノ流通防止対策専門委員会への参加や、アドレスリスト作成管理団体等に対し、必要な情報提供や助言を行うなどの支援を実施した。
(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	・ 総合セキュリティ対策会議については、「サイバー空間の脅威に対処するための産学官連携の在り方～日本版 NCFTA の創設に向けて～」をテーマに、2013 年７月以降、７回にわたって会議が開催され、2014 年１月、「サイバー空間の脅威に対処するための新たな産学官連携の在り方～日本版 NCFTA の創設に向けて～」とする報告書が取りまとめられた。
(オ)サイバー犯罪の被害防止対策の推進	警察庁	・ 2014 年２月のサイバー空間の脅威に対する対処能力の強化のための広報月間において、サイバー犯罪の被害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を実施した。 ・ 出会い系サイト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 2013 年６月に作成し、各都道府県警察において配布するとともに、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おいて取りまとめられた「不正アクセス防止対策に関する行動計画に関する行動計画」に基づいた取組を推進した。 ・ 同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！」を活用した広報啓発活動を実施した。 ・ 2013 年中の不正アクセス行為の発生状況等を、2014 年３月 27 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	・ 2013 年４月 23 日～25 日、アルゼンチン、ブエノスアイレスにて APWG 主催の Counter-eCrime Operations Summit 2013 (CeCOS VII) が開催された。本会議には、世界各地のサイバー犯罪対策の専門家約 200 名が結集しサイバー犯罪やフィッシングに関する、情報交換、共有が行われた。フィッシング対策協議会からは「Finding the Banking Trojan in Eastern Asia（極東地域におけるオンライン銀行詐欺ツール関する所見）」の発表を行った。また、本会議への参加報告書及び会議で発表した資料をフィッシング対策協議会の Web サイトに公開した。 https://www.antiphishing.jp/report/wg/2013cecosvii.html
(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、サイバーテロ対策協議会に参画している重要インフラ事業者等への個別訪問等を通じてサイバー攻撃情勢に関する情報提供を行うとともに、警察庁において、サイバー攻撃のデモンストレーションを含むセミナーを民間事業者に委託して全国で開催し、サイバーテロに対する危機意識の醸成を図るとともに、警察と重要インフラ事業者等の共同訓練等を通じて官民の連携強化を推進することで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 6,020（2014 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、2013 年中に 492 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官房情報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関連企業と共有し、官民連携した対策の向上を図った。
(コ)諸外国におけるサイバー攻撃等の調査研究	警察庁	・ 諸外国におけるサイバー攻撃事案及びサイバーディフェンス施策並びにサイバー犯罪捜査手法に関して調査を行った。
(サ)ログの保存の在り方の検討	警察庁 総務省	・ 現在、警察庁と総務省で情報交換を含め、協議を行っている。
(シ)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。
		b) ・ 不正プログラムの解析のための体制等を強化し、2013 年においては、1,063 件（2012 年比 821 件増）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。
(ス)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。
(セ)サイバー防犯ボランティア育成の推進	警察庁	・ 各種会議において、「サイバー防犯ボランティア活動のためのマニュアル（モデル）」、「サイバー防犯ボランティア育成のための研修カリキュラム（モデル）」の活用などによるサイバー防犯ボランティアの育成・支援等の強化について全国警察に指示した。
(ソ)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、携帯電話販売事業者等に対して、児童の保護者へのフィルタリングサービス等の説明の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、児童や保護者に対する啓発活動の強化、携帯電話事業者等に対する要請の徹底等を推進した。
(タ)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。

⑥ サイバー空間の防衛

施策名	関係府省庁	進捗状況
(ア)サイバー防衛隊（仮称）の新編	防衛省	・ 防衛省において、日々高度化・複雑化するサイバー攻撃の脅威に適切に対処するため、2014 年３月 26 日にサイバー防衛隊を新編した。
(イ)サイバー攻撃等対処に係る企画機能の強化	防衛省	・ 防衛省において、サイバー攻撃等の脅威の増大に対応するため、2013 年５月 16 日運用企画局情報通信・研究課に「サイバー攻撃対処・情報保証企画室」及び統合幕僚監部指揮通信システム企画課に「サイバー企画室」を新設し、サイバー企画機能を強化した。
(ウ)ネットワーク監視態勢の強化	防衛省	・ 防衛省において、防衛情報通信基盤（DII）について、サイバー攻撃等に関する状況把握能力を向上させるとともに、サイバー攻撃等発生時における被害局限化、早期復旧等の対処能力を強化するため、2014 年３月１日に「防衛情報通信基盤（DII）用のネットワーク監視器材」を整備した。
(エ)サイバー演習環境構築技術に関する研究	防衛省	・ 防衛省において、指揮系システムについて、サイバー攻撃時においても部隊運用を継続するとともに、被害の拡大を防止するなどの事後対処能力の練度向上を目的としたサイバー演習環境の構築技術に関する研究試作を 2014 年３月 18 日に開始した。
(オ)陸自電算機防護システムの整備等	防衛省	・ 陸上自衛隊の指揮系システムを防護対象とした陸自電算機防護システムについて、インターネットからのサイバー攻撃を受けやすい業務系のシステムについても防護対象とした新たな陸自電算機防護システムを整備し、2012 年度から引き続き運用している。
(カ)サイバー防護分析装置の機能強化	防衛省	・ 防衛省において、サイバー攻撃等に関する技術は日々進歩していることを踏まえ、2014 年３月１日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整備した。
(キ)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、2014 年度以降、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・分析体制を強化・向上させる。
(ク)情報保証に係る最新技術動向等の調査研究	防衛省	・ 2012 年度に引き続き、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、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。
(ケ)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 フォーラムを実施する（2013 年１月）など米国等との連携を強化した。
(コ)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	・ 2013 年 12 月には国家安全保障会議が設置されるとともに、サイバーセキュリティの強化を含む国家安全保障戦略が策定（国家安全保障会議決定及び閣議決定）された。 ・ 以上も踏まえつつ、引き続き関係機関の役割の整理・明確化を行うため、現在、第 38 回情報セキュリティ政策会議（2014 年１月 23 日）において、NISC の機能強化等に関する検討を開始し、NISC の機能強化に関する取組方針の決定に向けた討議を進めている。 ・ なお、「政府機関の情報セキュリティ対策のための統一基準」（2014 年６月）に関する「府省庁対策基準策定のためのガイドライン」（2014 年６月）において、各府省庁 CSIRT がインシデントを認知した場合の報告・対処について、大規模サイバー攻撃事態等の場合の報告等を記載するとともに、「重要インフラの情報セキュリティ対策に係る第３次行動計画」（2014 年６月）において、大規模 IT 障害対応時の情報共有体制等における各関係主体の役割の整理・明確化を行った。

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討及び研究開発の推進	総務省 経済産業省	・ M2M 機器間認証用モジュールに実装されるシステム LSI チップのセキュリティ仕様を標準化するため、これまでのスマートカードの世界で培われてきたセキュリティ技術を基礎に、M2M 用モジュールのセキュリティ要求仕様の研究開発を実施した。
(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	・ 制御システムを高セキュア化する技術の研究開発を実施した。具体的には、制御システムのサーバや制御端末の脆弱性検証を行う技術を研究し、実機の脆弱性検査を行うことでその有効性を確認した。
(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、文書自体の部分秘匿や匿名化を行いながら文書の非改ざんや作成者の属性を認証可能な電子署名技術、及び情報の内容を秘匿しながら集計を行う秘匿集計技術を開発し、ソフトウェア実装にて機能検証を実施した。 ・ ネットワーク利用者の所属などの属性のみを認証することでプライバシー保護を図るための匿名認証方式を開発し、ソフトウェア実装にて機能検証を行った。ISO における匿名認証方式の国際標準化に寄与した。 ・ クラウドコンピューティング等でのプライバシー保護機能が期待されている次世代暗号「ペアリング暗号」の安全性評価や楕円曲線上の離散対数問題の高速化手法について研究を実施した。また、離散対数問題に基づく暗号方式の最新の解読法の進展状況等を調査し、CRYPTREC を通じて電子政府システムの安全性維持の活動に貢献した。
(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	・ スマートメータやセンサー等に実装可能な軽量暗号を、クラウド上で高速に並列復号処理する実装法を世界で初めて開発した。軽量暗号が省リソースデバイスにおける小型ハードウェア実装での優位性のみならず、ハイエンドプラットフォームでの高速ソフトウェア実装でも AES に対して優位性を持つことを示した。また、軽量暗号の分類や安全性・実装性能に関する要件を定めた国際標準 ISO/IEC 29192-1 の規格化をエディタとして主導し、2012 年に出版。開発した軽量暗号は、省リソースデバイスにおける小型ハードウェア実装での優位性のみならず、ハイエンドプラットフォームでの高速ソフトウェア実装でも AES に対して優位性を持つことが示された。 ・ 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認証を行う物理的複製困難関数（PUF）技術に必要とされるセキュリティ及びプライバシー要件を取りまとめた。また、プライバシーを保護しながら RFID タグにおける認証を行う方式の１チップ実装にて有効性を確認した。 ・ 大規模ノードにおける機器認証処理のオーバーヘッドを log オーダーで削減する認証方式を開発し、ソフトウェア実装にて有効性を確認した。
(オ)社会基盤としてのクラウドコンピューティングの情報セキュリティ確保の推進	総務省	・ 総務省において、ITU-T SG13 及び SG17 並びに ISO/IEC 等の国際標準化機関における議論の動向を踏まえ、クラウドサービス提供事業者が利用者との間で取り決めるべき合意（責任の分担設定など）を含めた「クラウドサービス提供における情報セキュリティ対策ガイドライン」（2014 年４月公表）の策定を行った。
(カ)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	・ 現在は、民間主導により、クラウドコンピューティングにおけるサービス内容・範囲・品質等に関する保証基準に関して、ISO/IEC 19667 Information Technology - Cloud Computing - Service Level Agreement (SLA) Framework and Terminology として、国際標準化の議論が進められている。なお、本標準については 2014 年度夏にも成立する予定。
(キ)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 が主催するソフィア会合（2013 年４月）、インチョン会合（2013 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積極的に参画した。 ・ ITU-T におけるセキュリティ分野の研究委員会 SG17 の会合（2013 年４月及び８月、2014 年１月）に参加し、我が国の研究開発成果等を踏まえ、クラウドコンピューティングのセキュリティに関する勧告策定に貢献した。 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、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。

(ク)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-(ナ)
(ケ)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-(ニ)
(コ)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	・ 評価・認証の国際的な相互承認枠組みである CCRA の会議に参加（2013 年５月・９月、2014 年３月）。各国調達の状況の情報を収集、また USB メモリや MFP の分野で国際的な調達要件作成への参加を表明し、相互承認の推進に努めた。
(サ)自動車に係る情報セキュリティの確保	経済産業省	・ 2013 年３月に IPA が公開した「自動車の情報セキュリティへの取組ガイド」に基づき、大学関係者から、自動車セキュリティに関する提言が公開された。この提言を受け、自動車業界において、自動車に係る情報セキュリティを検討する環境が整備された。
(シ)政府調達の在り方の検討	内閣官房	・ 再掲：１-①-１）-(テ)
(ス)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	・ 現在まで、リバースエンジニアリングの適法性を明確化する法改正に至っていないが、適法性の明確化を図るべく、引き続き次の改正の機会に向けて努力を続けることとする。

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	・ 2013 年６月の「サイバーセキュリティ戦略」を踏まえ「情報セキュリティ研究開発戦略」の進捗状況を確認し、次期の研究開発戦略のための見直し方針を策定する技術戦略専門委員会を実施した。 ・ なお、「情報セキュリティ研究開発戦略」の見直しを 2014 年６月までに行う予定である。
(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及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プロトタイプ開発を行った。 ・ また、組織内ネットワークを流れる通信及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 改の開発に着手した。
(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	・ 2013 年度において実施した「ビッグデータ利活用のためのデータ連携技術に関するフィージビリティスタディ及び予備研究」において、今後のビッグデータ利活用技術の研究開発に向け、個人のプライバシー保護に関する研究開発動向を調査。
(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	・ 2012 年度に開発した認証技術の部分実証システムの構築を進め、セキュアな認証機能の追加を目的として、大規模認証・プライバシー保護機構の詳細設計を行うとともにテストベッドへの展開を図った。
(カ)量子情報通信ネットワーク技術の研究開発	総務省	・ 都市圏敷設ファイバ等のフィールド環境での量子暗号による量子鍵配送のデータを蓄積し、量子鍵の安全性や量子暗号システムの故障率の定量化を行った。 ・ また、量子暗号のアプリケーション拡張に向け、量子鍵を通常のネットワーク機器での暗号化機能に利用するため、アプリケーションインターフェース技術の研究開発を実施した。
(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設計及びプロトタイム開発を実施した。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開始した。 ・ 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、スマートフォン利用時におけるリスク評価、暗号プロトコルの脆弱性に基づくリスク評価を行うためのセキュリティ知識ベースと分析エンジンを改良し、リスクの可視化を行うためのシステム化を行った。 ・ 多様なセンサー群で収集したビックデータをクラウド等の解析するシステムにおけるプライバー、セキュリティの確保に向けて、軽量暗号の評価基盤の構築に着手した。また、今後の利用が拡大が期待されるペアリング暗号や格子暗号等の安全性評価に取り組んだ。
(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、Scyther をベースにして、プロトコルの安全性を GUI を通じて自動的に検証し、その検証結果を蓄積可能なシステムを構築した。
(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）の情報蓄積機能及び管理機能を強化するとともに、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 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	・ セキュリティ評価と最適構成の導出を行うために必要な、ICT システムに必要なセキュリティ要件、ソフトウェアの脆弱性、セキュリティ対策技術の DB を拡張し、ネットワーク製品、暗号プロトコルの安全性情報に加え、スマートフォンに関する安全性情報を加味したリスク評価を実施可能とする技術開発を行った。
(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	・ ３件の補助事業を行い、より安全でエネルギー効率のよいクラウドコンピューティングシステムの研究開発を行った。結果の多くは学会等での発表及びプログラムのオープン化によって、広く一般に裨益するものとなっている。

(シ)スマートフォンにおけるリスクの可視化	総務省	・ スマートフォンのアプリケーションの解析手法を検討し、静的解析を自動的に行い、結果を安全性情報として知識ベースに格納するとともに、利用者端末にリスクを可視化するシステムを試作した。
(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	・ 2013 年度において、IT システムの耐災害性強化等を推進するため、スピントロニクス材料・デバイス基盤技術や高機能高可用性ストレージ基盤技術の研究開発を実施。
(セ)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	総務省 経済産業省	・ 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心理特性及び利用者環境の分析、組織内の通信状況を把握することでマルウェアの活動を検知するためのセンサーの試作等、標的型攻撃を検知する技術について調査及び研究開発を実施。 ・ 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ネットワーク制御技術について基礎的な研究開発を実施。
(ツ)革新的な情報セキュリティ技術の研究開発基盤の構築	総務省	・ 再掲：１-④-(ネ)
(テ)サイバーセキュリティ研究開発拠点の構築	総務省	・ NICT において「サイバー攻撃対策総合研究センター（CYREC）」を立ち上げ、官民の英知を集めたオールジャパンの研究開発体制を構築し、サイバー攻撃の観測・解析の高度化に向けた研究開発・実証実験を開始した。 ・ また、産官学連携の一環として、セキュリティコンテスト SECCON2013 全国大会のサイバー攻防戦をリアルタイムに可視化する、NIRVANA 改 SECCON カスタムの導入・稼働を行い、高度情報セキュリティ人材の育成に資する活動を実施した。
(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	・ 日本国内で制御機器のセキュリティ評価・認証が行えるよう、CSSC においてパイロット認証や評価・認証手法の技術開発を実施し、制御機器のセキュリティに関する評価・認証機関の設立ための準備を実施した。
(ナ)産業技術総合研究所における研究開発の促進	経済産業省	・ ユーザーの属性に応じて柔軟なアクセス制御を可能とする、通信効率の良い暗号の構成法を提案した。プライバシーや企業機密の保護を実現する技術として、暗号化データベースのままで検索処理を可能とする技術を開発し実装した。スマートフォンアプリケーションでのパーソナルデータの取扱状況を確認するため、国内外のアプリケーションについて、プライバシーポリシーの掲載状況を調査、比較し発表した。

③ 人材育成

施策名	関係府省庁	進捗状況
(ア)情報セキュリティ人材育成プログラムの改訂	内閣官房	・ サイバーセキュリティ戦略（2013 年６月情報セキュリティ政策会議決定）、国家安全保障戦略（2013 年 12 月閣議決定）、創造的 IT 人材育成方針（2013 年 12 月 IT 総合戦略本部決定）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普及啓発・人材育成専門委員会において実施し、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。
(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」を実施し、当該事業のうち、主に情報セキュリティ分野の実践教育を実施する大学における社会人学生の受け入れを支援した。
(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」において、大学や産業界による全国的なネットワークを形成し、参加する大学の拡大を図るとともに、実際の課題に基づく PBL（課題解決型学習）等の実践的な教育を推進した。
		b) ・ 複数の教育機関と複数の企業での実践的インターンシップを実施する際のマッチング運用モデルについて、IPA の公開データベース（IT 人材育成 iPedia）において公開した。
		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」において、各大学で作成された授業や教材を、教材共有のためのポータルサイトに掲載し、その利用促進を図った。
(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」において、大学や産業界による全国的なネットワークを形成し、参加する大学の拡大を図るとともに、実際の課題に基づく PBL（課題解決型学習）等の実践的な教育を推進した。
		b) ・ 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、情報セキュリティに関する研究科等の設置の重要性について記載し、そうした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、今後具体的な検討を進めることとした。
(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) ・ 2013 年８月 13 日～17 日の期間で 41 名の受講者が参加し、セキュリティ・キャンプ実施協議会と共催で成功裡にセキュリティ・キャンプ中央大会 2013 を実施した。当該中央大会では、最近注目度が高まる組込み機器の脆弱性発見を講義に取り入れたり、セキュリティ関連企業への訪問などを実施し充実を図った。 ・ また、９月（福岡）と 12 月（沖縄）にはセキュリティ・キャンプを地方に展開するためにセキュリティ・キャンプ地方大会を開催し 36 名の受講者があった。 ・ さらに、セキュリティ・キャンプ実施協議会とともにキャンプ卒業生と会員企業間のインターンシップを実施（２企業）し、卒業生の社会における採用・活用の促進に努めた。
		b) ・ NPO 法人日本ネットワークセキュリティ協会主催、経済作業省を始めとする関係省庁等が後援として、「SECCON CTF 2013」を開催した。経済産業省としても、地域のセキュリティ人材育成推進体制の在り方検討及び普及活動を行った。
		c) ・ 総務省において、官公庁・民間企業等を対象に大規模模擬環境を用いた実践的な防御演習を 2013 年度内に 10 回開催し、30 組織以上からのべ約 300 名が参加した。 ・ 経済産業省において、電力、ガス、化学、ビルの４分野において、各事業者が実際にサイバー攻撃が発生した際の現象及びその障害への対策を体験できるサイバーセキュリティ演習を実施した。
(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	・ 情報セキュリティ関連分野で活躍する総勢 61 名の情報セキュリティスペシャリストについてキャリアパス事例集として 2012 年４月に IPA セキュリティセンターより公開。また、セキュリティ・キャンプへの参加募集活動に併せて大学、高等専門学校等に配布するなどの普及を実施。
(キ)スキル、資格、教育プログラム等の整理	経済産業省	・ 「情報セキュリティ人材育成指標策定事業」にて、2012 年３月に情報セキュリティ関連業務で求められるスキルと関連する資格、教育プログラムを整理した。その内容を踏まえ 2012 年９月に IPA より「共通キャリア・スキルフレームワーク」を拡充し公開した。

(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) ・「新・情報セキュリティ人材育成プログラム」において、情報処理技術者試験等を通じた人材の能力の見える化について記載した。また、各府省庁における資格の活用状況等について調査を行い、事例共有に資するよう調査結果のフィードバックを行った。
		b) ・情報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	・情報処理技術者試験は、昨今の情報セキュリティの重要性の一層の高まりや情報セキュリティ人材が不足している状況を踏まえ、情報セキュリティスペシャリスト試験を含む全試験区分を対象に、情報セキュリティに関する出題を強化・拡充する方針を決定し、2013 年 10 月 29 日に公表した。
(コ)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	・「情報セキュリティ人材育成指標策定事業」にて情報セキュリティ人材に求められるタスクとスキルを 2012 年３月に整理した。その内容を踏まえ 2012 年９月に IPA より共通キャリア・スキルフレームワークを拡充し公開した。
(サ)先端的な研究者等の国際会議への参加支援等	内閣官房 関係府省庁	・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（2013 年 11 月）や、情報共有やインシデント対応に関する国際連携を議題とする FIRST（2013 年６月）などに、内閣官房や各省庁より職員を派遣するとともに、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）等を国内で開催し、サイバーセキュリティにおける国際連携の推進に関する議論に積極的に参画した。これらを通じ、情報セキュリティ分野の国際協力等を担当する人材の経験、能力の涵養に努めた。 ・また、CODE BLUE（2014 年２月）等、海外の専門家等を招へいして民間が主催する行事の開催を支援するとともに、内閣官房からも職員を派遣し講演等を実施した。
(シ)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-(ト)
(ス)情報セキュリティに詳しい法律家の育成	内閣官房 関係府省庁	・法律家の育成に関し、関係府省庁の取組状況を調査し、事例共有に資するよう調査結果のフィードバックを行うとともに、「新・情報セキュリティ人材育成プログラム」策定の検討にあたっての参考とした。
(セ)情報セキュリティ専門家等の育成の促進	内閣官房 経済産業省	・「新・情報セキュリティプログラム」中で、情報セキュリティ監査・格付けの必要性を強調し、それらを担う人材の育成、資格制度の適切な活用等の具体策について記載した。
(ソ)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) ・高等教育機関において産学連携により自立的に実践的 IT 教育講座を開設・運営するためのノウハウやコンテンツを、「産学連携 IT 人材育成プラットフォーム」として IPA の公開データベース（IT 人材育成 iPedia）において公開した。
		b) ・高校生向けに IT に関連する職業に携わる若者の具体的な仕事内容を紹介した広報誌を IPA を通じて公開した。
		c) ・「情報セキュリティ人材育成指標策定事業」にて情報セキュリティ人材に求められるタスクとスキルを 2012 年３月に整理した。その内容を踏まえ 2012 年９月に IPA より共通キャリア・スキルフレームワークを拡充し公開した。
		d) ・ITPEC は継続的にアジア共通統一試験を実施。2013 年 10 月の試験からはバングラデシュでトライアル試験を実施し、ITPEC への加盟支援を開始した。さらには、我が国の IT スキル標準の普及拡大を図るため、タイへの普及に取り組み始めた。
(タ)制御システムセキュリティに係る人材育成	経済産業省	・経済産業省において、制御システムユーザーや ASEAN 諸国の電力分野関係者に対し、制御システムセキュリティに係る人材育成のため、CSSC のテストベッド施設を活用した、サイバーセキュリティ演習や研修を実施した。
(チ)内閣官房情報セキュリティセンターや独立行政法人等を活用した人材育成	内閣官房 総務省 経済産業省	・「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。
(ツ)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	・CYMAT 要員研修等を通じ情報セキュリティ確保体制を整備するとともに、各府省庁間の人的ネットワークを構築した。また、内閣官房ほか各府省庁において、情報セキュリティ関係企業との意見交換会や、独立行政法人を活用した情報セキュリティ人材のネットワーク形成等の取組が推進され、政府として一定の進捗が図られた。
(テ)優秀な外部人材の活用	内閣官房 関係府省庁	・再掲：１-①-２）-(チ)

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) ・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。（2013 年 11 月及び 2014 年１月） ・情報モラルに関する教育の充実を図るため、教員向け指導手引書を作成した。
		b) ・地方自治体の情報教育担当を集めて実施した会議（2013 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。（2013 年 11 月及び 2014 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	・2013 年度において、情報セキュリティ・サポーターの育成方策に関する調査を実施し、活動を支援した。
(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	・内閣官房の「国民を守る情報セキュリティサイト」において、各府省庁が既に設置している情報セキュリティに関する相談窓口を紹介する連携を強化した。消費者に対する窓口相談対応力の強化については、消費者庁及び関係府省庁の連携にまでは至っていない。
(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	・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 2013 年度に作成し、利用者及び事業者向けセミナー等を実施するなど普及展開を図った。
(オ)官民連携・国際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 2013 年度に作成し、利用者及び事業者向けセミナー等を実施するなど普及展開を図った。
		b) ・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 2013 年度に作成し、利用者及び事業者向けセミナー等を実施するなど情報発信を行った。
(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	・利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会提言「青少年が安全に安心してインターネットを利用できる環境の整備に関する提言」（2011 年 10 月）、安心ネットづくり促進協議会スマートフォンにおける無線 LAN 及びアプリ経由のインターネット利用に関する作業部会報告書（2012 年６月）を受け、無線 LAN 経由の通信やアプリケーションといったスマートフォンの特徴に適合したフィルタリングの開発を支援し、各携帯事業者等より対応したフィルタリングが整ってきている。さらに 2013 年９月に同研究会より「スマートフォン安心安全強化戦略」が提言され、携帯事業者等に更なる要請を行っている。 ・望ましいフィルタリング提供の在り方についての判断基準の検討に活用するべく、携帯型ゲーム機やインターネット接続テレビ、携帯多機能プレイヤー、PC 等の機器について、青少年による機器の利用実態調査を実施し、調査結果を事業者に提供している。
(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	・「スマートフォン　プライバシー　イニシアティブ」（SPI）に基づき、業界団体等とも緊密に連携をしつつ、その推進を図った結果、業界団体における自主ガイドラインの策定・公表について一定の進捗が見られたほか、アプリケーションのプライバシーポリシーの作成状況も前年に比べ改善が見られた。 ・2013 年９月には、アプリケーションのおける利用者情報の取扱いが適切かどうか第三者が検証する仕組みを推進する SPIⅡをとりまとめ。同年 12 月には、SPI、SPIⅡに係る諸課題を検討するタスクフォースを設置した。
(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	内閣官房 総務省 経済産業省	・内閣官房において、2013 年５月１日に各府省庁に対してソーシャルメディアを利用した国民への情報発信における留意事項に係る事務連絡を発出した。また、政府機関統一基準群の改定において、ソーシャルメディア利用に係る対策事項として、管理責任者を設置すること、重要な情報については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規定として整備した。

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	・ 二国間や多国間におけるサイバー協議を通じ、我が国の基本的な価値観（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等）が最大限に反映されるよう、国際的な規範作りにあっては、ハイレベルによる働きかけを通じ、米・英等の有志国と連携して、積極的に議論に参画した。
(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」や「サイバー空間に関するソウル会議」等への参画を通じ、サイバー空間を利用した行為に対する従来の国際法の適用や、国際的な規範作り等に関する我が国の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歩」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３次国連サイバーGGE」に政府専門家（サイバー政策担当大使）を派遣し、サイバーセキュリティ分野における行動規範作りなどに積極的に寄与するとともに、同会合における議論のとりまとめに貢献した。引き続き、第４次会合等における国際的な規範作りに積極的に関与する。
(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 外務省 総務省 経済産業省 関係府省庁	・ 米国との二国間対話については、「日米サイバー対話」（2013 年５月）、「インターネットエコノミーに関する日米政策協力対話」（2014 年３月）を通じ、両国のサイバー戦略等の共有をはじめ、脅威情報の共有、意識啓発、研究開発等における連携強化に取り組んだ。 ・ また、日 EU インターネット・セキュリティフォーラムを通じ、英国を含む欧州諸国ともサイバーセキュリティ分野での連携・協力を進めたほか、日露「２＋２」における日露サイバー安全保障協議の立ち上げ合意、日・EU 定期首脳会議における日・EU サイバー協議の立ち上げ検討のための専門家協議の実施が合意されるとともに、エストニアとの間でサイバー協議立ち上げの合意が行われた。 ・ このほか、インドとも次回の日印サイバー協議の開催に向けて具体的な日程調整を進めているところであり、各国との情報交換、協議等に積極的に取り組んだ。
(オ)海外情報セキュリティ機関との情報交換	経済産業省	・ NIST との第 10 回定期会合を 2013 年 12 月２日に NIST にて開催。NIST・経済産業省・AIST・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。また情報セキュリティ人材育成と暗号の個別テーマについては、NIST 担当者とディスカッションを実施した。 ・ KISA とは年間３回の会合を実施（①KISA 院長交替に伴う実務者会合：2013 年７月８日、②IPA・KISA トップ会談：2013 年８月 27 日、③実務者定期会合：2014 年３月 10 日）。さらに新たな取組として IPA と KISA 共催による「日韓情報セキュリティシンポジウム」を今後継続的に開催することとし、2013 年 12 月 13 日にベルサール飯田橋にて両国のサイバーセキュリティ政策やサイバー攻撃事例等をテーマに第１回を開催し、約 200 名が参加。
(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	・ MERIDIAN をはじめ、APEC、OECD、IWWN、FIRST、ARF、ITU、ACF 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情報共有、ベストプラクティス共有、信頼醸成措置の促進等を進めたほか、Meridian については、2014 年会合の日本招致を表明し、我が国のプレゼンス向上に取り組んだ。 ・ 2013 年 10 月に開催された「サイバー空間に関するソウル会議」に参画し、「サイバーセキュリティ国際連携取組方針」を踏まえ、国際的なルールづくりや二国間又は多国間等の協議に積極的に寄与することを表明するなど、多国間の枠組みによる国際連携・協力を推進した。 ・ 2013 年４月の国連犯罪防止刑事司法委員会並びに 2013 年３月及び 10 月の G8 ローマ・リヨン・グループ会合に参加し、サイバー犯罪対策に関する国際協力に積極的に寄与した。
(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	・ サイバーに関する脅威情報の交換、国際的なサイバー政策についての連携、重要インフラ保護のための情報共有、防衛・安全保障戦略に関するサイバー防衛の取組・議論等を通じ、日米同盟の強化を推進するため、各分野での連携を進めているところである。

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 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た連携・協力を推進しており、2013 年については、初めて閣僚級の会議を開催し、技術協力や人材育成等の推進に合意したほか、専門家パネルの開催による具体的な協力事項の検討、専門家派遣による人材育成支援等を新たに開始した。
		a) ・ 2012 年 10 月に開催された第５回会合の決定事項に基づき、各国の連絡窓口の確認を行うとともに、共同意識啓発、サイバー攻撃予知・即応技術に関する研究開発、CSIRT 構築・連携等における日・ASEAN 協力に取り組んだ。
		b) ・ ASEAN 各国の情報通信所管の閣僚級が来日して、「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、東京）を開催し、共同声明を採択した。
		c) ・ 2013 年 10 月に開催された第６回会合では、同年９月の「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」で合意された技術協力や人材育成等における連携の具体化や、共同意識啓発及びサイバー連絡演習に関する成果の確認と 2014 年以降の継続等に合意した。また、サイバーセキュリティに関する特定のテーマについて、関心を有する国の政府機関等が参加し、課題の洗い出し及び協力の方向性等について議論するための「専門家パネル」の設置・開催に合意し、2014 年２月に、重要インフラ防護を議題とする会合をマレーシアで開催した。
		d) ・ 2013 年５月に開催された第５回政府ネットワークセキュリティワークショップでは、共同意識啓発活動の継続や、情報共有体制を強化するためサイバー連絡演習を共同で実施すること等に合意した。これらについては、2013 年中に着実に取組を進め、第６回政策会議において、日・ASEAN 間でその成果確認も行った。
		e) ・ ASEAN 諸国との情報セキュリティ意識啓発活動については、2012 年にも作成したポスターに加え、新たに意識啓発リーフレット（ASEAN 各国語版も作成）やステッカー、スマートフォンや SNS を題材とする新作の意識啓発アニメを作成した。サイバー演習については、第５回政府ネットワークセキュリティワークショップにおける実施合意を踏まえ、2013 年８月に日・ASEAN の政府間で初めて連絡演習を実施した。
		f) ・ インドネシア情報通信省の情報セキュリティ対策実施能力の向上を図るため、技術協力プロジェクトを実施予定。 ・ 同プロジェクトに係る専門家派遣については、2013 年度中の派遣開始を目指していたが、インドネシア政府からの専門家派遣の要請書の接到が遅延。2013 年 12 月 RD 署名、2014 年３月調査団派遣、2014 年６月専門家派遣開始予定。実施期間は２年６ヶ月を予定。
		g) ・ 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」（2013 年８月、東京）を総務省が主催し、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。
		h) ・ 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」（2013 年 11 月、マレーシア）を活用し、日本から 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。
(イ)国際連携を活用した普及・啓発活動の実施	内閣官房 関係府省庁	・ 再掲：１-④-(キ)
(ウ)「情報セキュリティ国際キャンペーン」の実施	内閣官房 関係府省庁	・ 再掲：１-④-(ク)
(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) ・ 「APEC 電気通信・情報作業部会」（2013 年４月、インドネシア）に参加し、国際連携に基づくサイバー攻撃対策の研究開発などの取組を紹介し、各国と意見交換を実施した。 ・ また、「APEC 電気通信・情報作業部会」（2013 年９月、ハワイ）では、日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議の結果を報告した。

		b) ・ JPCERT/CC は、６月と 11 月にアフリカ諸国に対し、それぞれザンビアとコートジボワールにて、CSIRT 構築・運用強化のための研修を行った。９月にはモンゴルの MonCIRT 及び MNDC に、10 月にはラオスの LaoCERT 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。研修実施に際しては、FIRST や APCERT に協力を呼びかけ、アフリカ諸国への支援に関しては、FIRST 及び韓国の KrCERT/CC との、またラオスの LaoCERT への研修に関してはタイの ThaiCERT との連携をとるなど国際連携を図りつつ実施した。
(オ)海外の組織内 CSIRT の構築・運用支援	経済産業省	・ JPCERT/CC では８月にモンゴルの MonCIRT 及び MNDC に、10 月にはラオスの LaoCERT 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 では TSUBAME プロジェクトメンバーに対して、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。 ・ C/C++セキュアコーディングセミナーを５月にインドネシア（バリ）にて開催した。
(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 は、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等の開発し、大洋州諸国をカバーする CSIRT である PacCERT（在フィジー）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）を英語化し、タイの ThaiCERT に実施ノウハウとともに提供した。
		b) ・ ＜FIRST＞ JPCERT/CC の理事が FIRST の Steering Committee（SC）のメンバーを務め、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ている。また６月にバンコクで開催された第 25 回 FIRST 年次会合や９月にインドネシアのジョグジャカルタで開催された FIRST Technical Colloquium（FIRST TC）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 は、IWWN で定期的に開催される電話会議やメーリングリストを通して情報共有を行い、メンバー間の連携を進めた。 ・ ＜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＞ 10 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２月に実施された APCERT のメンバーを中心とする「APCERT Drill 2014」に参加し、JPCERT/CC としてのインシデント対応能力の向上を図った。「APCERT Drill 2014」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	・ ASEAN７カ国の官民関係者を招聘し、「ASEAN 地域の重要インフラ関係者に対する情報セキュリティ強化支援」研修を本邦にて実施。（2013 年１月） ・ JICA の電子政府推進のための研修を通じ、アジア各国の政府関係者に情報セキュリティ対策ベンチマークの講演を実施。（計２回：2013 年５月 28 日、11 月 18 日） ・ 「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 12 日～13 日@ホテルオークラ東京）にて自動車の情報セキュリティに関するパネル展示、及び情報セキュリティ白書の CD-ROM、内部不正に関する報告書等を配布。 ・ ASEAN 各国において日本企業が安全に活動できるよう、ベトナム・マレーシアの情報セキュリティの現状をレポートしたドキュメンタリー映像「東南アジアの情報セキュリティ～現状と対策について～」を YouTube 上に公開（再生回数：2,000 回）。また映像 DVD を JETRO の ASEAN８ヵ国（10 拠点）に送り、計 2,000 枚を展示・配布。
(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	・ 再掲：１-④-(ニ)

(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)	・＜共同解析やマルウェア解析連携との連動等＞ 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、及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。 ・＜アジア太平洋地域以外への観測点の拡大に向けた調整＞ イスラム協力機構（OIC）に加盟する国々の CSIRT から成る OIC-CERT に対して TSUBAME プロジェクトを紹介した。既に複数のチームが関心を持ち、プロジェクト参加に向けて具体的な協議を進めているところである。
		b)	・サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組みを、OECD 等の関係組織とともに検討を進めた。
(コ)途上国向け研修・セミナー等の開催	総務省		・APT 研修「ブロードバンド通信のためのサイバーセキュリティ政策・技術」（2014 年２～３月）において、APT（アジア・太平洋電気通信共同体）加盟国を対象とした情報セキュリティ研修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。
(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係る知識・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、2013 年 12 月、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。 ・2013 年５月、外務省において、「サイバー犯罪の捜査・訴追における効果的な国際協力に関するワークショップ」を開催し、アジア・太平洋諸国 16 か国及び３国際機関が参加した。2013 年 12 月に開催された「サイバー犯罪対策協力に関する欧州評議会オクトパス会合」の開催経費を支援し、同会合において「アジア・太平洋地域におけるサイバー犯罪法制」に関するワークショップを開催した。2013 年度、国連薬物犯罪事務所（UNODC）の東南アジア諸国向けサイバー犯罪対策能力構築支援プロジェクトの実施を支援した。 ・国連アジア極東犯罪防止研修所の実施した国際研修及び汚職防止刑事司法支援研修において、アジア太平洋地域諸国を含む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。（2013 年８月、同年 10 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		・C/C++セキュアコーディングセミナーを５月にインドネシア（バリ）にてセミナーを約 100 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 の会合（ジュネーブ：2013 年４月、８～９月）に参加し、IPv6 に関するセキュリティガイドラインの国際標準化を推進し、X.1037 として勧告化を完了した。 ・ISO/IEC JTC1/SC27 の会合（ニース：2013 年４月、仁川：2013 年 10 月）に参加し、侵入検知・防止システム（IDPS）やセキュリティ情報・イベント管理（SIEM）等に関する国際標準化に貢献した。 ・ISO/IEC SC27/WG2 において、匿名認証プロトコルの規格である ISO/IEC 20009-2 の標準化をエディタとして主導し、2013 年 12 月に IS として出版した。 ・軽量暗号の国際標準 ISO/IEC 29192 について、軽量ハッシュ関数に関する新パートを開始し、エディタとして規格化に貢献した。 ・IETF Meeting（ベルリン：2013 年７月～９月、ロンドン：2014 年３月）に参加し、ネットワーク機器のリスク評価と対策提示技術の標準化を推進した。
		b)	・ISO/IEC JTC1/SC27 が主催する春秋年２回の国際会合に IPA が参加し、情報セキュリティマネジメントシステム（WG1）、暗号とセキュリティメカニズム（WG2）、セキュリティ評価技術（WG3）の３分野において日本の代表として意見をまとめた。中でも WG2 はコンピーナ（主査）として、また WG3 はバイスコンピーナ（副主査）として会議の運営をまとめる役も担った。 （2013 年４月仏ソフィアアンティポリス：、2013 年 10 月：韓国仁川） 2013 年度は日本技術が含まれた規格１件（ISO/IEC 20008-2）が発行。 ・また、暗号モジュールの非侵襲攻撃への対処に関する試験方法 ISO/IEC 17825、暗号アルゴリズムの適合性試験 ISO/IEC 18367 のドラフト作成、審議に参加した。

(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	・ 標的型攻撃などのサイバー攻撃の定常化により、グローバル化した情報システムへの脆弱性対策とインシデント対応が必要不可欠になっていることを踏まえ、Cybersecurity Innovation Forum 会議、FIRST の CVSS ワーキンググループ、FIRST カンファレンス、ISO/IEC JTC1/SC27 の活動等に参画した。
(ソ)Common Criteria (ISO/IEC 15408)における国際協調	経済産業省	・ CCRA を通じ、国際共通プロテクション・プロファイル (PP) 等の情報を国内の統一基準の政府調達要件作成にフィードバックを行った。 ・ また、日本の強みである MFP 分野のプロテクション・プロファイルを IPA がとりまとめ、政府及び MFP ベンダと調整をし開発を行っている。
(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	・ JIWG との会合に２回 (2013 年９月及び 2014 年２月) 出席し、欧州 SOG-IS との EAL7 までの相互承認に関する議論を開始した。JHAS 会合に４回参加し、最新のスマートカード攻撃技術関連の情報収集に努めた。また JTEMS 会合に４回参加し、カード端末攻撃技術関連の情報収集を行った。
(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、オランダ、スペイン、イギリス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 MOU を締結し、制御システムセキュリティに係る協力関係を構築した。
(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、テストベッド施設の運用及び訓練の実施を含む人材育成のための情報共有など連携を強化するための MOC を締結した。 ・ また、CSSC において、我が国の研究成果を積極的に国際標準に反映するため、国際認証推進組織 (ISCI) に加入し、制御システムセキュリティ分野での国際的な連携を強化した。
(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-(コ)
(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２月)、OECD/ICCP/WPISP (Organisation for Economic Co-operation and Development / Committee for Information, Computer and Communications Policy / Working Party on Information Security and Privacy、2013 年４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。 ・ 関係省庁連絡会議等を活用し、各省庁と連携しつつ、越境プライバシールールシステム (CBPR) への 2013 年６月の参加申請に向け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（2013 年６月、バンコク）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。 ・ 政府のサイバーテロ・サイバーインテリジェンスに関する対策に資する関連情報を収集する態勢の強化に向け、外国関係機関との連携、情報交換を緊密に行うなど、関係機関との協力体制の強化に努めた。
(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	・ 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（2013 年４月、2013 年 10 月）、ICPO サイバー犯罪に関するユーラシア地域作業部会（2013 年 11 月）等に参加し、外国捜査機関職員との情報交換や協力関係の確立等を積極的に推進した。 ・ 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（2013 年 12 月）し、アジア大洋州地域における各捜査機関との協力関係の構築を推進した。 ・ 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するため、派遣先国の検討や必要経費の要求を実施した。 ・ 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（2014 年１月末現在、66 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	・ 刑事共助条約を締結済みの米国、大韓民国及び EU との間で、中央当局間実務者協議を実施した。
(エ)サイバー犯罪条約普及への参画	外務省	・ アジア初のサイバー犯罪条約締約国として、我が国は 2013 年６月にサイバー犯罪条約のビューロー（運営委員会）メンバーに選出された。2013 年６月、９月及び 12 月の条約委員会及び関連会合に出席し、ビューローメンバーとして積極的に議論に参加した。 ・ 2013 年 12 月に開催された「サイバー犯罪対策協力に関する欧州評議会オクトパス会合」の開催経費を支援し、同会合において「アジア・太平洋地域におけるサイバー犯罪法制」に関するワークショップを開催した。 ・ また、各種国際会議において、サイバー犯罪条約の普及に努めた。
(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等を図るため、IWWN、FIRST、Meridian 等の国際会議や電話会議に積極的に参加し、我が国からの情報発信を行いつつ、各国の政府機関との連携強化を図るとともに、JPCERT/CC による FIRST 等への参加を通じ、各国の CERT 間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	・ 2013 年度、JPCERT/CC は新たに４チームと MOU/NDA を更新又は新規に締結した（2014 年３月末現在で 22 の経済地域の 27 組織との間に効力を発揮）。また、2011 年に日中韓の National CSIRT の間で締結した MOU に基づき、2013 年７月、三者による第１回年次会合を上海で開催し、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) ・ 2013 年に策定した「サイバーセキュリティ戦略」や「サイバーセキュリティ国際連携取組方針」をはじめ、「情報セキュリティ国際キャンペーン」の取組等について、NISC ホームページに英語版を公開するなど、ホームページを通じた国際的な広報、情報発信を行った。 ・ また、サイバーセキュリティ分野における国際連携・共助に関する基本方針等をまとめた「サイバーセキュリティ国際連携取組方針」について、2013 年 10 月の策定後、各国際会議や二国間対話等の場を通じ、積極的な広報・発信に努めた。 b) ・ 国際会議や電話会議等を通じて把握した国際動向、海外のベストプラクティス等について、NISC が開催する関係省庁連絡会議等を通じて共有又は報告するとともに、脅威・脆弱性に関する情報等の共有を通じ、JPCERT/CC 等の関係機関と連携して対策強化に努めた。
(ク)重要インフラ分野での国際連携推進	内閣官房 総務省 経済産業省 重要インフラ所管省庁	・ 再掲：１-②-(フ)

(ケ)インターネット国際接続の冗長化の推進	総務省	・ 2013 年９月に通信事業者にヒアリングを行い、国際情報通信インフラの分散化、冗長化の現状等を把握した。 ・ 現状、一部の地方公共団体が国際海底ケーブルの敷設に向けた調査研究を開始したほか、通信事業者等が中心となって新たな国際通信ルートの構築に向けた研究会を開催する等、自主的な取組が進んでいるところ。

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	a) ・ 2013 年 12 月には国家安全保障会議が設置されるとともに、サイバーセキュリティの強化を含む国家安全保障戦略が策定（国家安全保障会議決定及び閣議決定）された。 ・ 以上も踏まえ、第 38 回情報セキュリティ政策会議（2014 年１月 23 日）において、NISC の機能強化等に関する検討を開始し、NISC の機能強化に関する取組方針の決定に向けた討議を進めている。
		b) ・ 2013 年 12 月には国家安全保障会議が設置されるとともに、サイバーセキュリティの強化を含む国家安全保障戦略が策定（国家安全保障会議決定及び閣議決定）された。 ・ 以上も踏まえ、第 38 回情報セキュリティ政策会議（2014 年１月 23 日）において、NISC の機能強化等に関する検討を開始し、NISC の機能強化に関する取組方針の決定に向けた討議を進めている。
(イ)各府省庁の情報セキュリティ対策推進のための情報セキュリティ・コンサルティング機能の充実	内閣官房	・ 内閣官房（NISC）において、情報セキュリティに関する課題等について各府省庁からの意見を集め、個別に打合せを行うなどして取組に係る実効性の向上を図った。
(ウ)関係機関等との連携強化	内閣官房 内閣府	・ IT 総合戦略本部については、世界最先端 IT 国家創造宣言等を着実に実行するための情報通信技術（IT）関係施策に関する 2014 年度戦略的予算重点方針に基づき、概算要求の調整等について連携した。 ・ 総合科学技術会議については、科学技術イノベーション総合戦略　第２章 Ⅲ．世界に先駆けた次世代インフラの整備を着実に実行するための 2014 年度アクションプランの検討、レビュー等について連携した。 ・ 知的財産戦略本部については、技術・営業秘密保護のための取組の促進において連携している。 ・ また、国家安全保障会議については、2013 年 12 月に策定された、サイバーセキュリティの強化を含む国家安全保障戦略（国家安全保障会議決定及び閣議決定）も踏まえ、NISC の機能強化等に関する検討において連携している。 ・ なお、「重要インフラの情報セキュリティ対策に係る第３次行動計画」（2014 年６月）において、大規模 IT 障害対応時の情報共有体制等における防災関係府省庁等の関係主体の役割の整理・明確化を行っている。
(エ)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、「情報セキュリティ対策・プライバシーに関する状況の調査分析を行い、「パーソナルデータを活用したオンラインサービスに有効な個人情報保護対策」を 2014 年３月に公開した。 ・ また、情報セキュリティに関連した事象、対策状況、制度や基盤情報などを俯瞰的にまとめた「情報セキュリティ白書 2013」を９月２日に発行した。さらに英訳版を 12 月に作成し、国内外の関連機関へ配付している。
(オ)官民の情報共有の更なる推進	内閣官房 関係府省庁	・ 既に運用を開始している、警察庁の「サイバーインテリジェンス情報共有ネットワーク」及びセプターカウンシルの「標的型攻撃に関する情報共有体制（C⁴TAP）」との間における情報共有を行った。
(カ)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	・ 政府機関においては、内閣官房は警察庁の「サイバーインテリジェンス情報共有ネットワーク」との間で相互に情報共有を進めている。重要インフラ事業者等においては、情報共有の在り方を含め、「重要インフラの情報セキュリティ対策に係る第３次行動計画」を策定した。
(キ)サイバーセキュリティに関する国際戦略の策定	内閣官房	・ サイバーセキュリティ分野における国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理し、これらを一体のものとして取りまとめた「サイバーセキュリティ国際連携取組方針」を、2013 年 10 月の情報セキュリティ政策会議において策定した。

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

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「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、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１）。

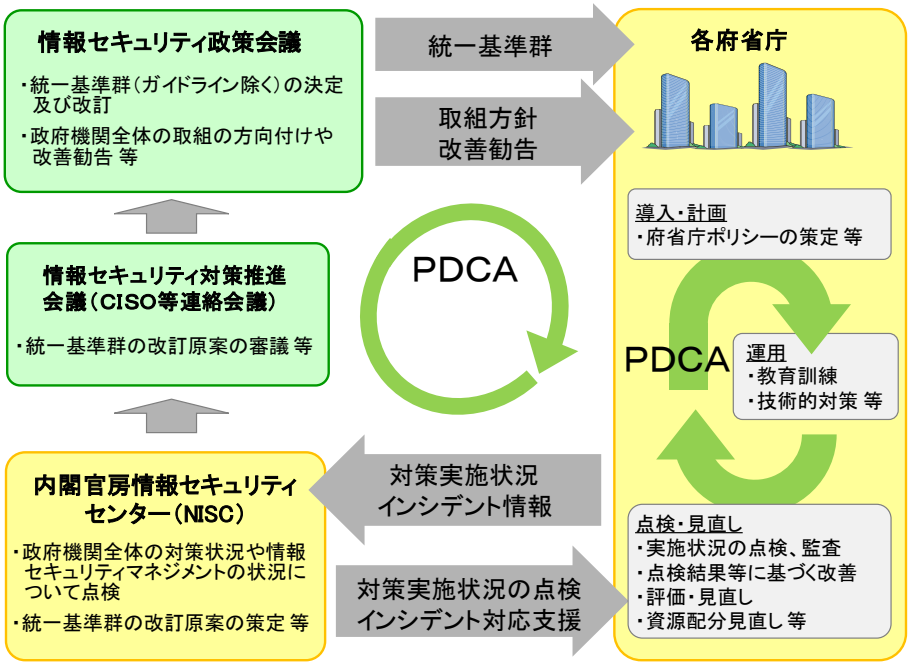


図１　政府機関における情報セキュリティ対策

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、及び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。

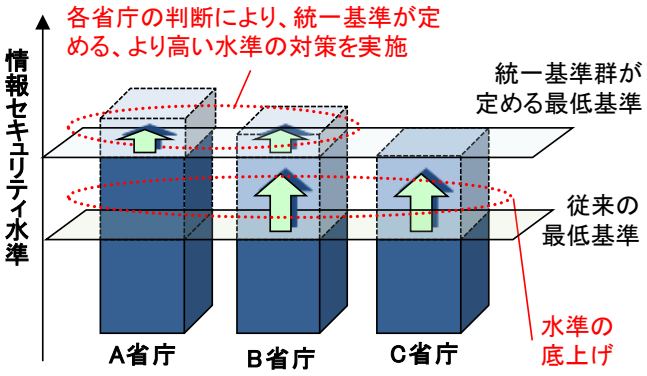


図２　統一基準群の効果（イメージ）

このような状況を踏まえ、今般、サイバーセキュリティ2013（2013年６月27日情報セキュリティ政策会議決定）の「Ⅱ 具体的な取組」に記載されている、「標的型攻撃等の脅威の顕在化や、スマートフォン及びクラウドコンピューティング技術の普及等、新たな技術や環境の変化に対応して、各府省庁が達成目標や実施計画を策定し、PDCAサイクルの適正性やガバナンス機能の有効性を確認するための枠組みの構築等に係る政府機関統一基準群の見直しを行う」のとおり、文書体系の変更も含めた抜本的な見直しを行った。

改定に当たっては、従来の統一基準群における課題を踏まえ、①統一基準群の実効性の向上、②新たな脅威・技術への対応、の二つの観点から改定方針を検討した。2013年10月２日情報セキュリティ政策会議において改定の方向性を決定し、2014年１月23日情報セキュリティ政策会議においてパブリックコメントに付す案を決定、2014年１月24日から２月14日までNISCのホームページにおいてパブリックコメントを実施し、必要な修正を行った上で、2014年５月19日情報セキュリティ政策会議において、「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）」が決定された（図３）。

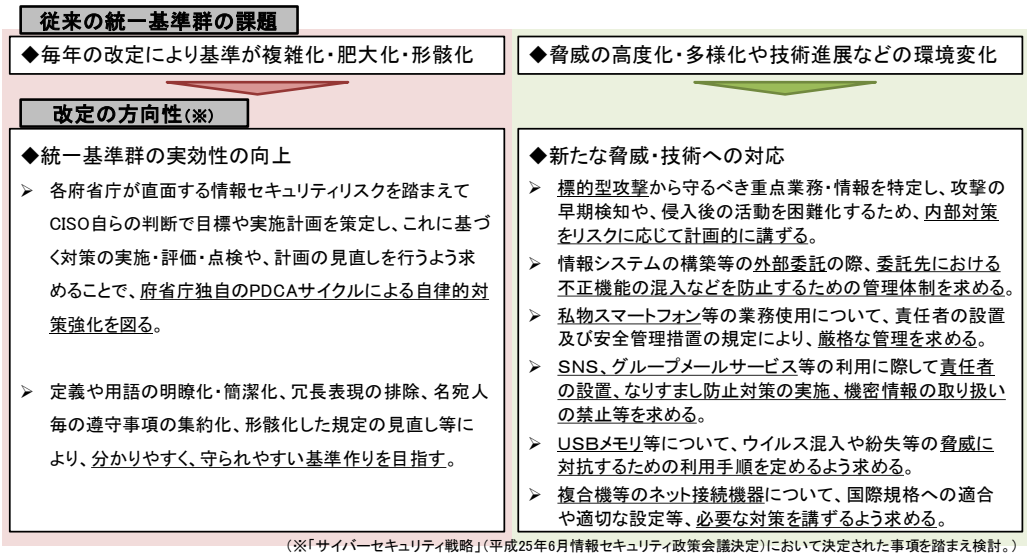


図３　統一基準群の改定の方向性[1]

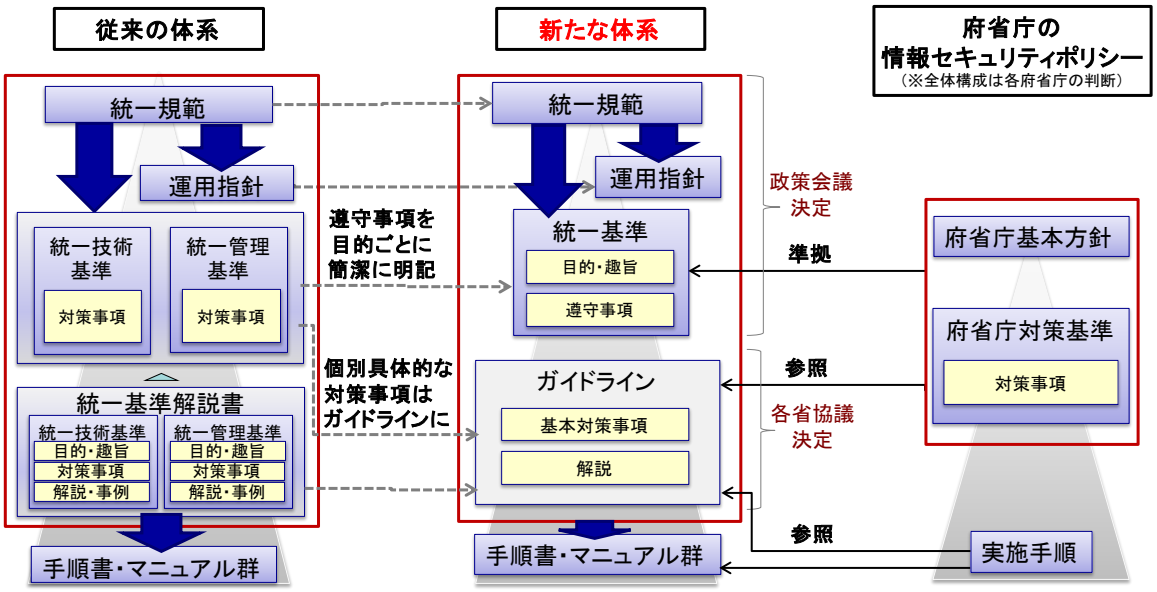
[1] http://www.nisc.go.jp/conference/seisaku/dai38/pdf/38shiryou0401.pdf［PDF］
第 38 回情報セキュリティ政策会議（2014 年 1 月 23 日）資料より一部抜粋

２　統一基準群の実効性向上のための見直し

統一基準群の実効性向上に向けては、主に、①府省庁独自のPDCAサイクルによる自律的対策強化、②分かりやすく、守られやすい基準作り、の二つの観点から見直しを行った。

(1) 府省庁独自のPDCAサイクルによる自律的対策強化

上述のとおり、統一基準群はこれまで政府機関全体の情報セキュリティ対策の水準向上に貢献してきたが、急速に変化する脅威・技術に対応するためには、各府省庁が画一的な対策を行うのみでは必ずしも十分ではなくなってきている現状を踏まえ、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府省庁ポリシーを策定できるよう、政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）において、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、府省庁対策基準策定のためのガイドライン（以下「ガイドライン」という。）において、府省庁ポリシーの策定手順や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、考え方等の解説を行った（図４）。



＜統一基準群（平成 26 年度版）における各文書の概要＞

【政府機関の情報セキュリティ対策のための統一規範（統一規範）】
政府機関の取るべき対策の統一的な枠組みを定めるもの。

【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（運用指針）】
統一基準の策定及びその運用等のために必要な事項について示すもの。

【政府機関の情報セキュリティ対策のための統一基準（統一基準）】
各府省庁が情報セキュリティ確保のために採るべき対策、及びその水準をさらに高めるための対策の基準を定めたもの。

【府省庁対策基準策定のためのガイドライン（ガイドライン）】
統一基準に準拠して府省庁対策基準を策定する際に参照するものであり、府省庁対策基準の策定手順や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、考え方等を解説したもの。

図４　統一基準群の体系

また、従来の府省庁における情報セキュリティ対策のPDCAサイクルは、情報セキュリティ関係規程の見直しに主眼が置かれていたが、本改定においては、各府省庁が直面する情報セキュリティリスクを踏まえ、最高情報セキュリティ責任者（CISO）が自らの判断で目標や実施計画を策定し、これに基づく対策の実施・評価・点検や計画の見直しを行うよう求めることにより、職員教育や設備投資まで網羅した府省庁独自のPDCAサイクルによる自律的対策強化を図った（図５）。

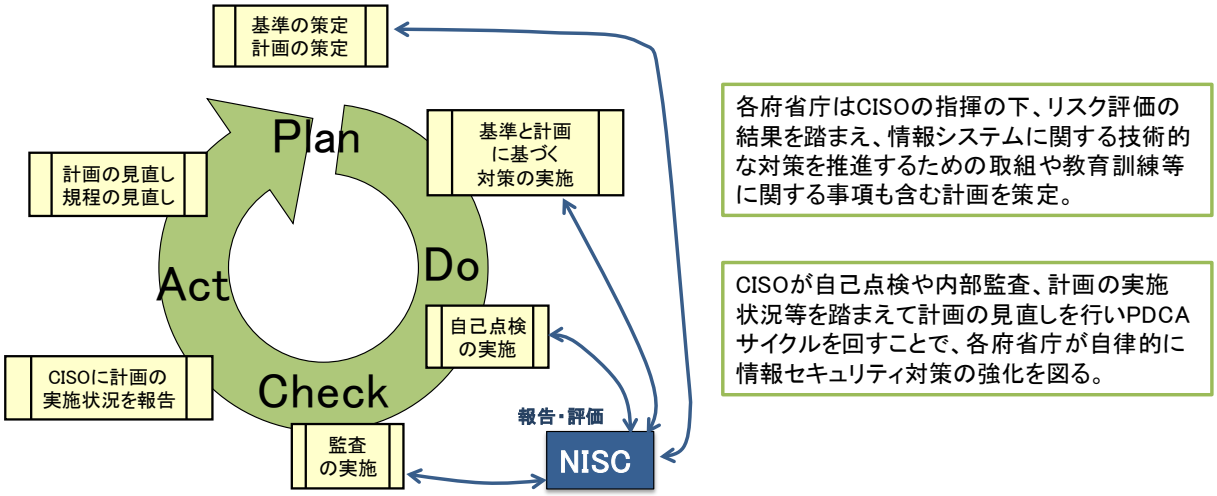


図５　府省庁における情報セキュリティ対策の PDCA サイクル

(2) 分かりやすく、守られやすい基準作り

定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人ごとの遵守事項の集約化により、分かりやすく、守られやすい基準作りを行った（図６）。

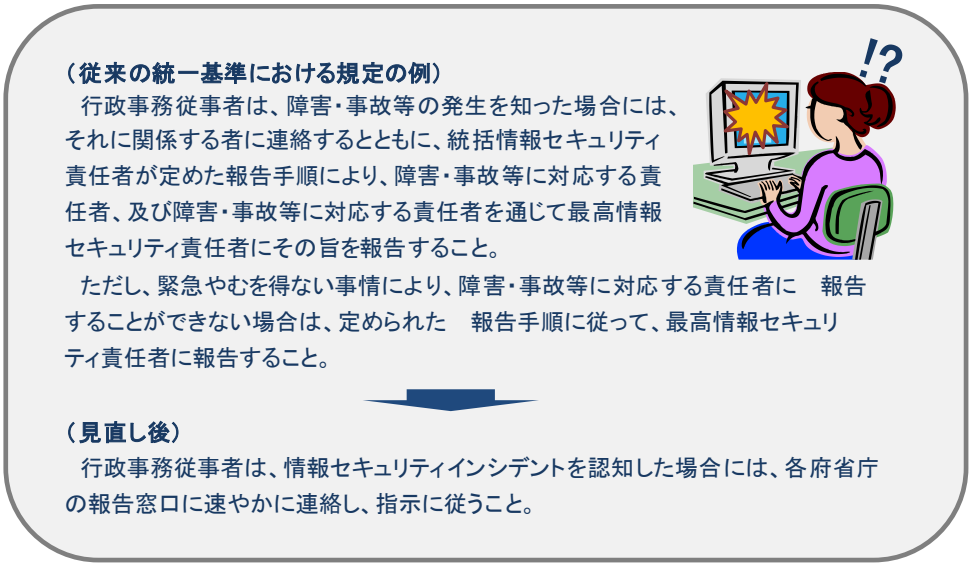


図６　規定の見直しの例 [2]

[2] http://www.nisc.go.jp/conference/seisaku/dai39/pdf/39shiryou0201.pdf［PDF］
第 39 回情報セキュリティ政策会議（2014 年５月 19 日）資料より一部抜粋

また、細分化・肥大化した基準の規定を整理・統合するとともに、名宛人ごとの遵守事項の集約化を行うことにより、ユーザビリティの向上を図った（図７）。

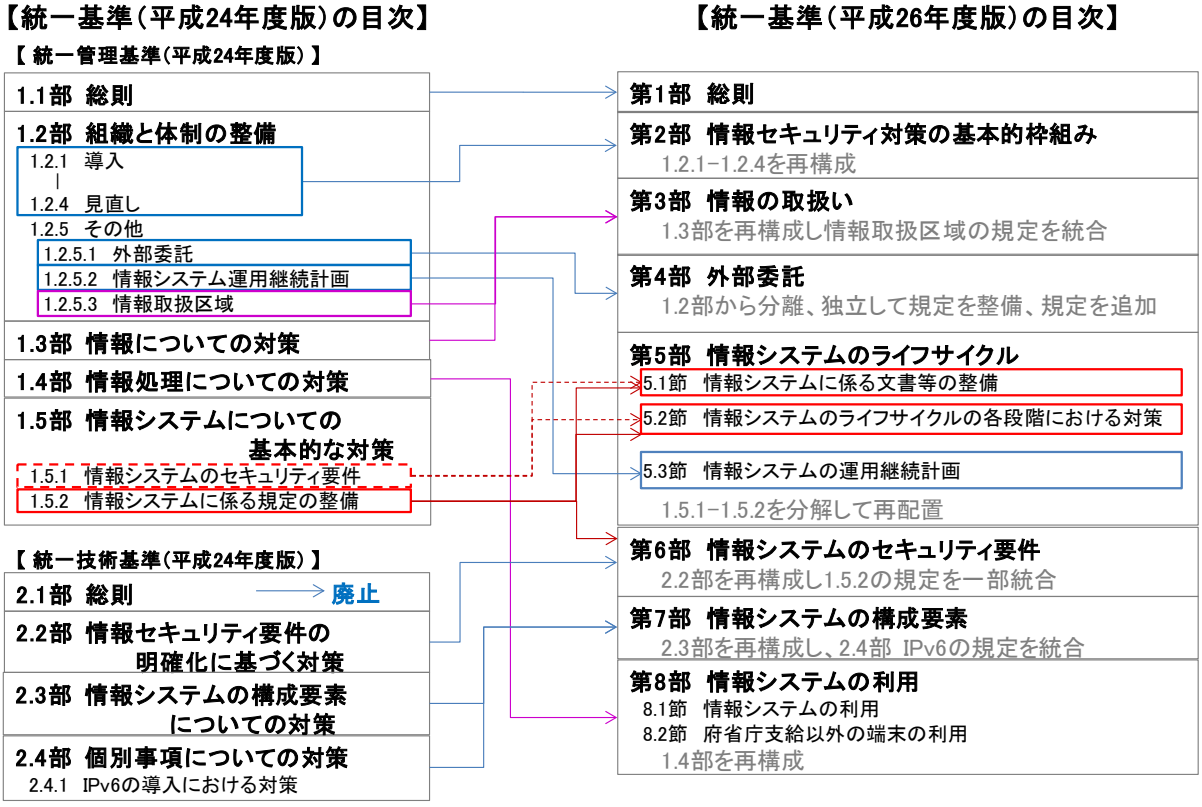


図７　部構成の変更

３　新たな脅威・技術への対応のための規定の見直し

(1) 標的型攻撃対策

外部から行われる情報の窃取・破壊等の攻撃は、政府機関にとって極めて大きな脅威であり、特に組織的・持続的な意図を持って行われる標的型攻撃への対策強化が喫緊の課題となっている。

標的型攻撃への対策は、外部からの侵入の防止に加え、内部に侵入されることを前提とする必要があるが、最新の攻撃傾向を考慮したシステム設計及び運用管理に係る対策項目の明確化及び重点的・計画的な対策の実施が必要であったことから、「高度サイバー攻撃対処のためのリスク評価等ガイドライン」に係る取組と併せて、統一基準の規定の見直しを行った。

＜追加・見直しをした規定＞

- ✧ 「標的型攻撃による組織内部への侵入を防御する対策（入口対策）」の実施＜遵守事項 6.2.4(1)(a)＞
- ✧ 「内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）」の実施＜遵守事項 6.2.4(1)(b)＞

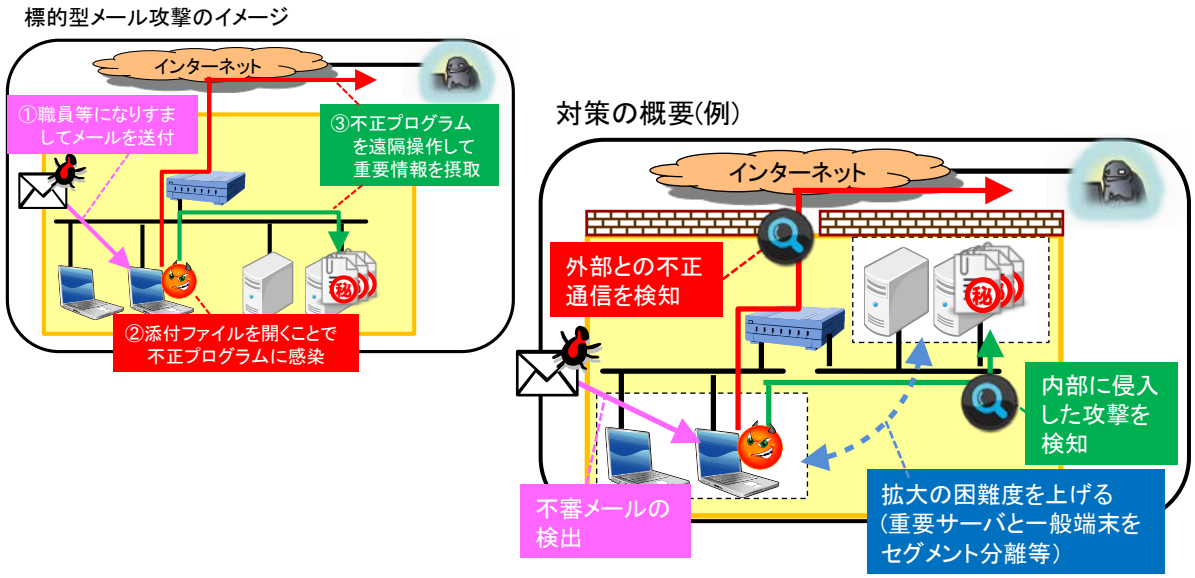


図８　標的型メール攻撃（イメージ）とその対策例

(2) サプライチェーン・リスク対策

海外では、機密情報の窃取を目的とした標的型攻撃に外国政府が関与していることも指摘されている。このような組織的なサイバー攻撃の可能性の一つとして、マルウェアやバックドアといった政府機関が意図しない機能が情報システムに埋め込まれるなどの情報セキュリティ上のサプライチェーン・リスクが想定されており、政府機関においても、対策の強化が求められている。

こういった動向を踏まえて、情報システム構築等の外部委託の際、委託先において不正な機能が混入されるなどのサプライチェーン・リスクを低減するために、委託先に厳正な管理体制を求めるなどの対策の見直しを行った。

＜追加・見直しをした規定＞

- ✧ 調達時に、外部委託に係る契約に関して資本関係・役員等の情報や委託事業従事者の国籍等に関する情報の提供を求める＜遵守事項 4.1.1(2)(a)＞
- ✧ 機器等の調達に係る規定の整備に関して必要な場合には、機器等の開発等のライフサイクルで不正な変更が加えられない管理がされているかを府省庁が確認する＜遵守事項 5.1.2(1)(a)＞

図９　サプライチェーン・リスク

(3) 私物端末利用に係る対策

近年のスマートフォンやタブレット端末等の小型軽量で高機能な端末の普及や、モバイル通信インフラの進展等により、出張先や外出先においても事務処理が容易に行える環境が整ってきており、今後、政府機関においても、スマートフォンやタブレット端末を業務に活用していくことも考えられる。

一方で、本来、行政事務は官支給の端末を用いて遂行すべきところ、私物のスマートフォンやタブレット端末を業務に利用することによる新たな情報セキュリティインシデントの発生が懸念される。

こうしたモバイル端末の利用環境の変化を受け、今般の統一基準群の改定において、府省庁の管理責任者による厳格な管理の下で私物端末が利用されるよう、規定の見直しを行った。

＜追加・見直しをした規定＞

- ✧ 私物端末利用の許可等の手続及び安全管理措置に関する規定整備＜遵守事項 8.2.1(1)(a)(b)＞
- ✧ 端末利用による行政事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者の設置＜遵守事項 8.2.1(1)(c)＞
- ✧ 要機密情報を取り扱う場合の安全管理措置の実施に係る管理責任＜遵守事項 8.2.1(1)(d)＞

なお、統一基準群の改定に当たっては、総務省のスマートフォン・クラウドセキュリティ研究会の取組結果や、2013年度各府省庁情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告「私物端末の業務利用におけるセキュリティ要件の考え方」等も参考に、具体的な安全管理措置の実施手順や申請手続き方法等をガイドラインにおいて整理した。

(4) クラウドサービスの利用に係る対策

2013年７月、インターネット上でメールを共有できるクラウドサービスで個人情報や中央官庁の内部情報が誰でも閲覧できる状態になっていた事案が発生したことを受け、このようなインターネット上で提供され、アカウント登録及び利用規約等への同意のみで利用できる無料の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の強化が必要となった。

従来の統一基準では、このようなサービスについて、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が明確にされていなかったことから、今般の改定において、対象となるサービスの範囲を「約款による外部サービス」として改めて定義した上で、以下の規定を追加した。

＜追加・見直しをした規定＞

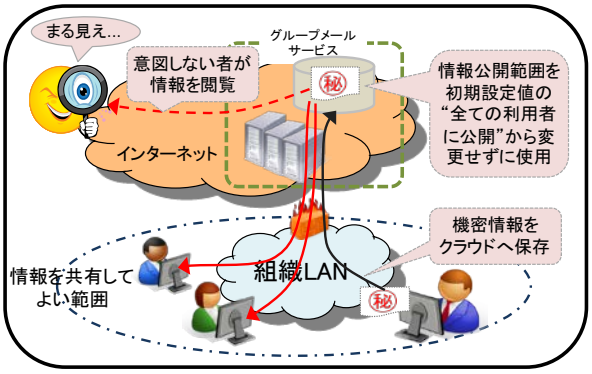
- ✧ 利用可能な約款による外部サービスの明確化及び要機密情報の取扱いの禁止＜遵守事項 4.1.2(1)(a)＞
- ✧ 利用手順等の整備、利用サービスごとに責任者の設置＜遵守事項 4.1.2(1)(b)＞

※「約款による外部サービス」とは

民間事業者等の府省庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

約款・利用規約等のサービス利用条件のみで、情報セキュリティ対策として求める水準に達しているものは「約款による外部サービス」から除外し、通常の「外部委託」と同等に扱ってよいとしている。

グループメールサービスの不適切な利用（イメージ）



グループメールサービスの適切な利用（例）

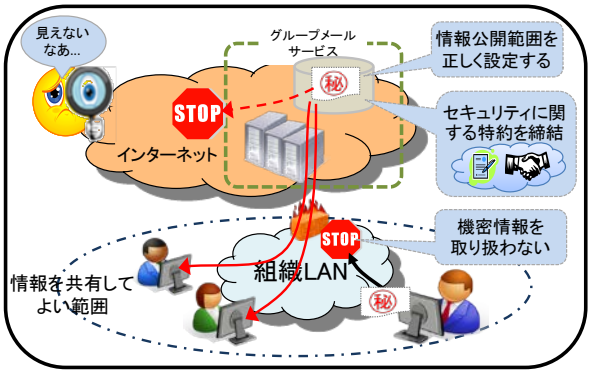


図１０　グループメールサービスの利用

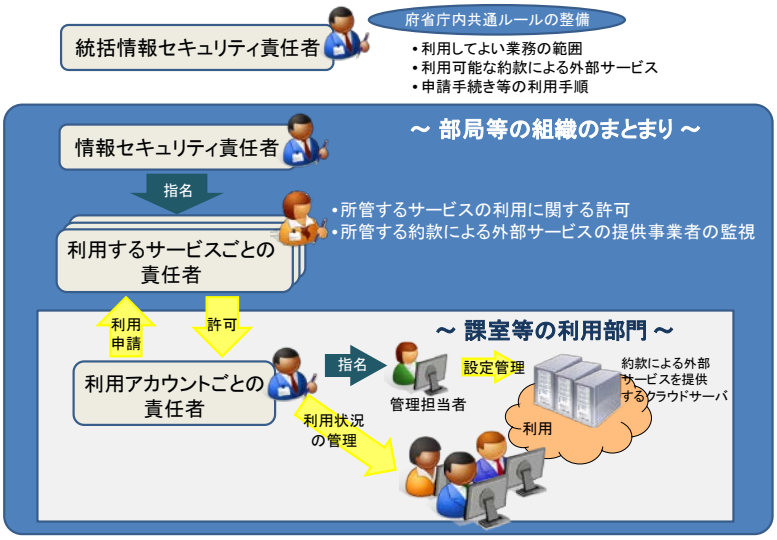


図１１　約款サービスの利用の流れ（イメージ）

(5) ソーシャルメディアサービスの利用に係る対策

2013年４月に米国の通信社が利用するソーシャルメディアサービスの公式アカウントが乗っ取られ、虚偽の情報が発信される事案が発生するなど、ソーシャルメディアサービスが標的となる攻撃が顕在化している。近年、我が国の政府機関においてもソーシャルメディアサービスを利用した情報発信が行われるようになっているが、従来の統一基準では、ソーシャルメディアサービスを利用した情報発信に係る対策事項が明確に規定されていなかった。

このため、政府機関の情報発信の手段としてソーシャルメディアサービスを利用する場合は、府省庁のアカウントを利用することを前提として、以下の規定を追加した。

＜追加・見直しをした規定＞

- ソーシャルメディアサービスの利用に係る運用手順の整備、府省庁が運用するアカウントへのなりすまし等への対策の実施＜遵守事項 4.1.3(1)(a)＞
- ソーシャルメディアサービスごとの責任者の設置＜遵守事項 4.1.3(1)(b)＞
- 可用性が求められる情報を発信する場合は府省庁の自己管理ウェブサイトに情報を掲載した上で従たる情報発信の手段としてソーシャルメディアサービスを利用＜遵守事項 4.1.2(1)(c)＞

(6) USBメモリ等の外部電磁的記録媒体の利用に係る対策

USBメモリを始めとする外部電磁的記録媒体は、技術の進歩に伴い大容量化・低価格化が進んでいる。中でもUSBメモリは、持ち運びが手軽であるなど、その利便性の高さから、一般に広く普及している。一方、コンピュータウイルス等の不正プログラムがUSBメモリに混入し、そのUSBメモリを接続した端末が不正プログラムに感染したり、USBメモリを紛失したりすると、重大な情報の漏えいにつながるおそれがある。さらには、インターネット等外部との接続を持たないクローズなシステムに対する攻撃の手段としてUSBメモリが用いられた事例が確認されている。

このため、USBメモリ等の外部電磁的記録媒体の業務利用において、ウイルス混入や紛失等の脅威に対抗するために、以下の規定を追加した。

＜追加・見直しをした規定＞

✧ USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順の整備＜遵守事項 8.1.1(1)(c)＞

(7) 複合機・特定用途機器の利用に係る対策

プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機は、通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用されるシステム特有の機器（特定用途機器）についても、その特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

一方で、複合機や特定用途機器は単なる事務機器として取り扱われて、十分な情報セキュリティ対策が講じられていない場合も想定され、実際に近年、複合機に関係する情報セキュリティインシデントが発生している。

そこで、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずるよう規定を追加した。

＜追加・見直しをした規定＞

✧ 複合機の調達時における、適切なセキュリティ要件の策定＜遵守事項 7.1.3(1)(a)＞
✧ 複合機の運用時における、情報セキュリティインシデントへの対策＜遵守事項 7.1.3(1)(b)＞
✧ 複合機の運用終了時（リース返却・廃棄時）における、内部に保存した情報の抹消＜遵守事項 7.1.3(1)(c)＞
✧ 特定用途機器についての対策＜遵守事項 7.1.3(2)(a)＞

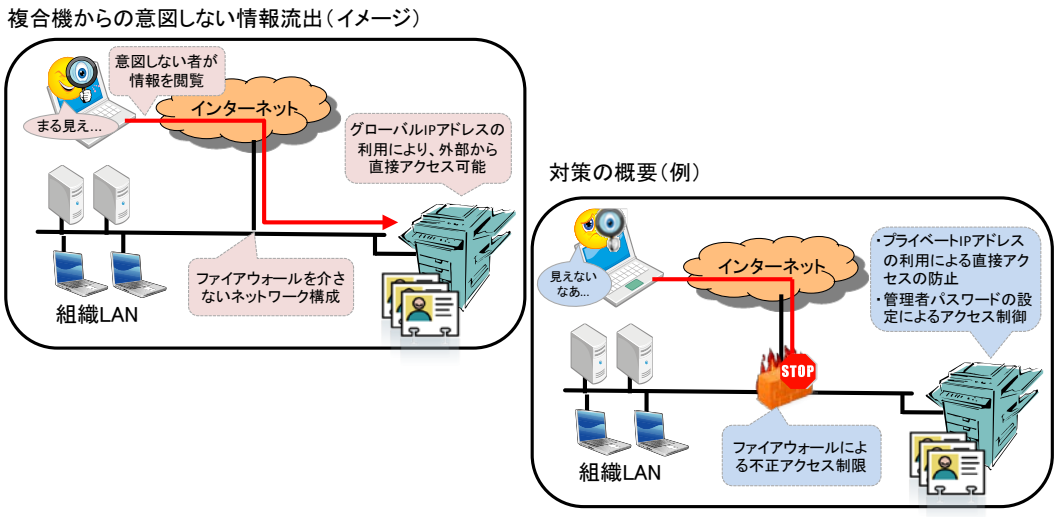


図１２　複合機の利用における脅威と対策例

別添３－２　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。

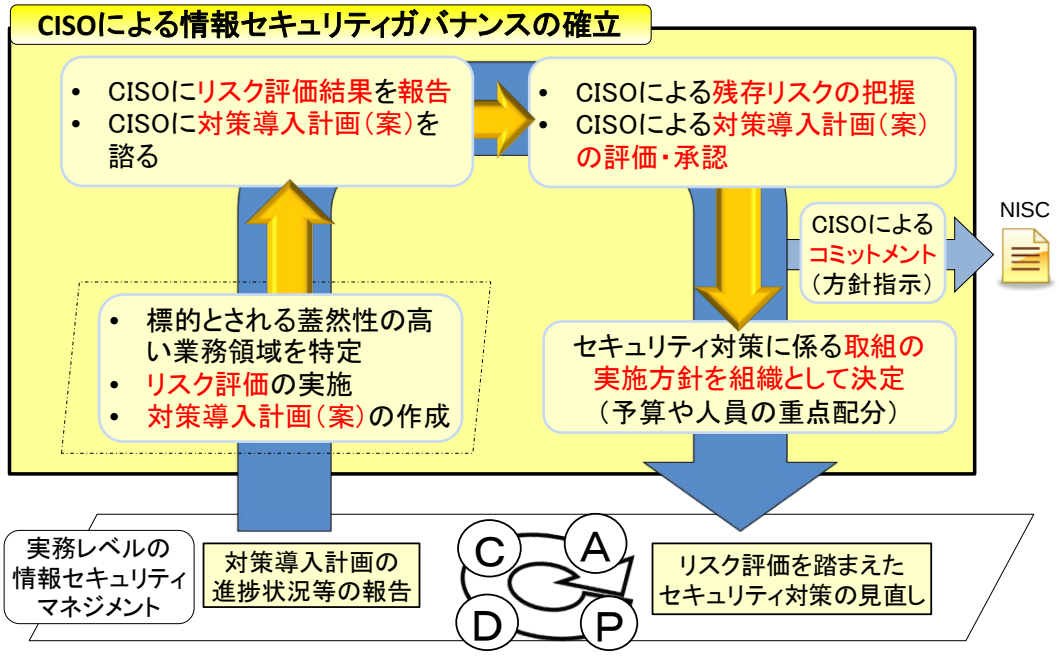


図　最高情報セキュリティ責任者による情報セキュリティガバナンスの概要

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（試行版）」（2013年９月26日情報セキュリティ対策推進会議）を策定し、全府省庁において本ガイドラインに基づく試行を実施したところである。また、試行の結果を踏まえた必要な見直しを行った上で、2014年度より正式な運用を開始する予定である。

表　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	内閣官房情報セキュリティセンター	

また、標的型攻撃等の高度サイバー攻撃は、時間の経過とともに新たな攻撃手法が出現したり、既存の攻撃方法に変化が生じたりすることが想定されることから、高度サイバー攻撃に対する効果的な防御を中長期的に実現していくためには、本取組の運用管理を適切に実施していく必要がある。中でもガイドラインに掲げる技術的対策については、技術動向や攻撃手法の進歩・変化に応じた継続的な見直しを行うことが特に重要である。そこで、NISCにおいて、府省庁等との情報共有を行い、これらの攻撃を監視・把握するとともに、現有の検討会を発展させ、新たな対策の採否に係る客観的な評価及び対策内容の見直しに係る検討を行うための体制を構築する予定である。

別添３－３　教育・訓練に係る取組

１　標的型メールに対する教育訓練の実施結果の概要

(1) 訓練の目的・特徴

NISCが実施する本教育訓練の目的は、標的型メール攻撃に関する教育・意識啓発のため標的型メールを通じて“ヒヤリハット”を経験することで、今後の電子メールの取り扱いにおいて注意を深め、同攻撃に対し適切な対処を身につけることである。

昨今ますます巧妙化する標的型メール攻撃の実態も踏まえ、より多くの職員に訓練メールを開封させ、“ヒヤリハット”体験をさせることを狙い、前年度よりもさらに巧妙に作成した訓練メール（本文、差出人、メールアドレス、添付ファイルなど）を使用した。

(2) 訓練の概要

○実施期間：2013年８月から12月まで

○実施規模：18府省庁　約18万人
（２回実施。２回目はより実践的な訓練をする目的から訓練対象者の１割を対象）

○実施方法：図に訓練メール送信から開封の記録までの流れを示す
（希望する府省庁には、２回目の訓練実施と併せて、府省庁の窓口に対するやり取り型メール訓練を実施した。）

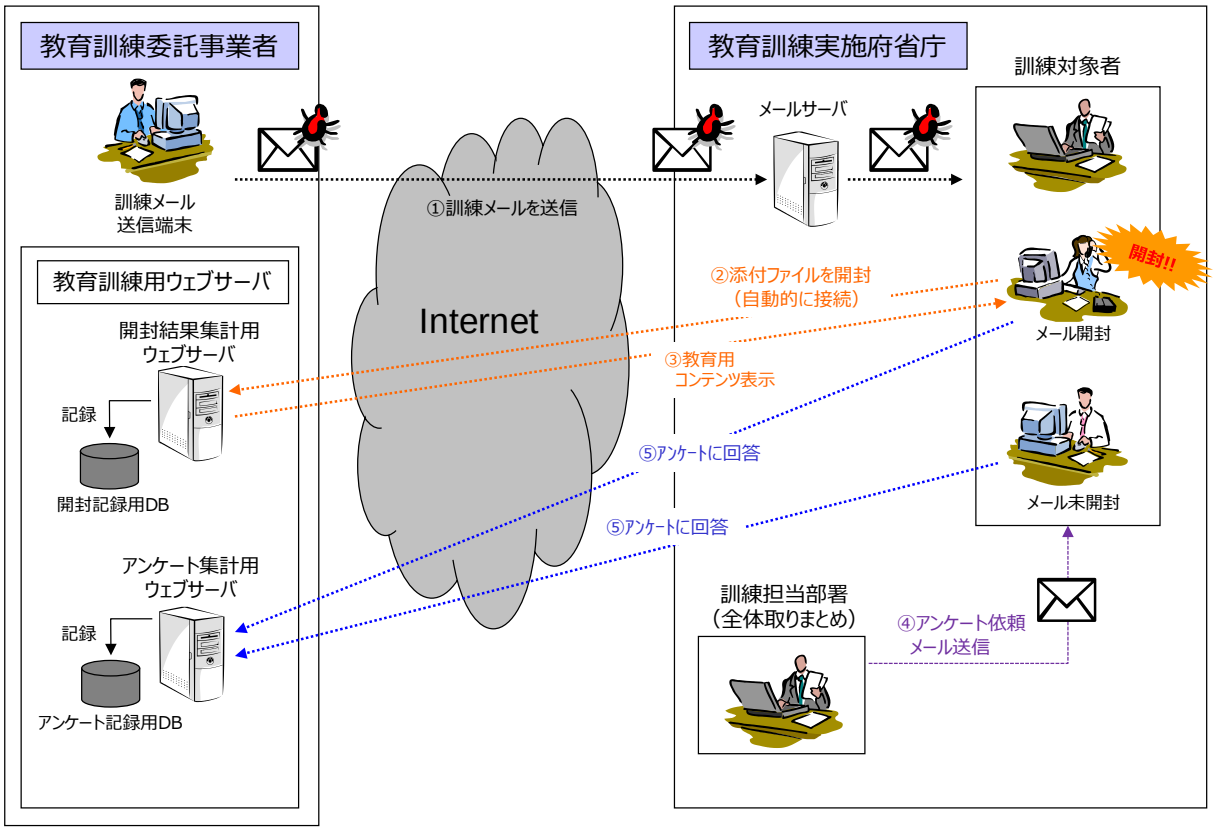


図　訓練メール送信から開封の記録までの流れ

(3) 訓練の結果

○１回目訓練：開封率　10.1%

○２回目訓練：開封率　16.3%

(4) 結果の分析

○訓練メールをさらに巧妙化したことにより、開封率は前年度より上昇する結果となった。

○これにより、訓練メールを開封した際に前年度よりも多くの職員が“ヒヤリハット”を体験することができたと考えられる。

○２回目の訓練では、１回目の訓練と比較して開封率が上昇した。２回目はより実践的な訓練をする目的から訓練対象者を絞って１割を対象としたことによる影響も考えられるが、本訓練は、組織の実情や業務内容等により各府省庁において訓練メールを作成しているため、訓練メールの難易度は様々であり、開封率は各府省庁によってばらつきがあった。

(5) まとめ

本訓練は、ある程度のレベルの標的型メール攻撃への対処に一定の効果があったと考えられる。訓練により得られた知見を各府省庁にフィードバックするとともに、独自に標的型メール訓練を行う府省庁に対して、支援を行っていく。

一方、巧妙な標的型メール攻撃について開封せずに対処することを全ての職員が常に行うことは困難であるため、どの職員でも標的型メールを開封することがありうることを前提とした、不審なメールを開封した際のエスカレーションを含めた連絡・報告等の対処も重要となる。

２　各府省庁CSIRT要員に対する研修

(1) 研修目的

各府省庁において情報セキュリティインシデントが発生した場合、被害拡大防止や早期復旧等を円滑に実施する必要がある。本研修は、各府省庁のCSIRT要員に対し、情報セキュリティに関する実践的な知識の習得や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) 研修概要

ア　講習

標的型攻撃とウェブサイト改ざん等の情報セキュリティインシデントへの対処に係る全般的な知識の習得を行った。

イ　演習

標的型攻撃とウェブサイト改ざんの仮想シナリオを用いて、状況把握、発生現場への指示、報道発表用資料の作成を行うなど、情報セキュリティインシデント対処等に係る基本的な行動を模擬体験した。

ウ　グループ討議

上述の講習や演習を通じて得た知見を踏まえ、自組織のCSIRT体制に関する課題を共有するとともに、今後の取組の方向性等についてグループ討議を行った。

(3) 参加人数

約50人（16府省庁参加）

(4) 研修時期

2014年２月

(5) まとめ

本研修は、各府省庁のCSIRT体制が整備されてから（2013年３月に全府省庁において整備完了）初めての取組となったが、アンケート結果で「情報セキュリティインシデントへの対処準備や組織内連携の重要性を実感できた」など有効性を認める意見が多数見受けられた。

グループ討議においては、各府省庁CSIRT要員の間での情報共有を行うことにより、情報セキュリティインシデントへの対処に関する意識啓発が図られるとともに、共通的な課題等が把握された。

今後は、本研修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の取組の充実を図る。

３　NISC情報セキュリティ勉強会

(1) 目的

情報セキュリティに関連する研究機関や情報セキュリティベンダ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

各府省庁及び情報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	2013年 ４月	安全なIT製品の調達に向けて －潜在する脅威とセキュリティ要件の実例－	独立行政法人・情報処理推進機構研究員	約100人 （計１回開催）
2	2013年 ７月	データベースにおける情報セキュリティ対策について	日本オラクル株式会社社員	約90人 （計１回開催）
3	2013年 10月	高度サイバー攻撃対処のためのリスク評価等の取組について	内閣官房情報セキュリティセンター職員、独立行政法人・情報処理推進機構研究員	約100人 （計１回開催）
4	2014年 ２月	情報セキュリティの重大脅威とその対策について（情報セキュリティ月間）	独立行政法人・情報処理推進機構研究員	約220人 （計２回開催）

別添３－４　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、重要な情報を摂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。2013年度は、「サイバーセキュリティ2013」及び「政府機関の情報セキュリティ対策のための統一技術基準」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。

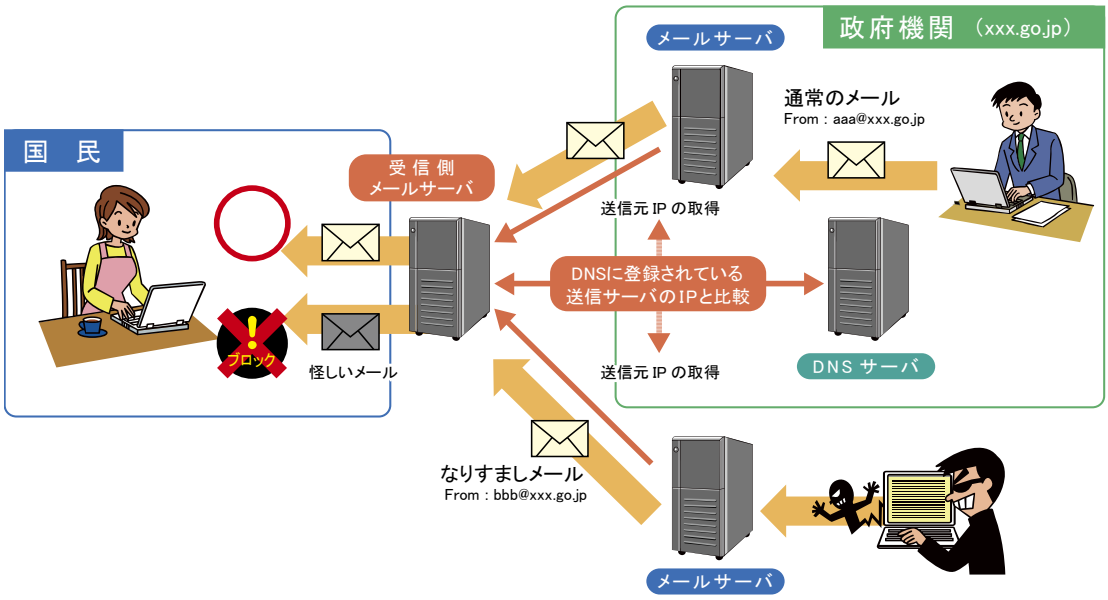


図　SPF を活用したなりすまし対策の概要

図に、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。

２　取組の結果及び今後の課題

2014年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の設定状況は以下のとおり。

[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。

ドメインレベル	-all※1	~all※2	設定なし
第３レベル（xxx.go.jp）ドメイン	81.1%	11.8%	7.1%
第４レベル（yyy.xxx.go.jp）以上のドメイン	48.3%	3.5%	48.2%

※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。

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、例えば、第３レベルドメインでは前年度と比較して1.2%減少しているものの、いまだに一定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。

また、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３－５　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

2013年10月から12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（CVSS基本値：7.0～10.0）としてSQLインジェクション脆弱性等が検出されたが、既に対応を終えている。また、危険性が比較的高い脆弱性（CVSS基本値:4.0～6.9）として、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、これらについては計画的に対応を進めている。

[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３－６　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

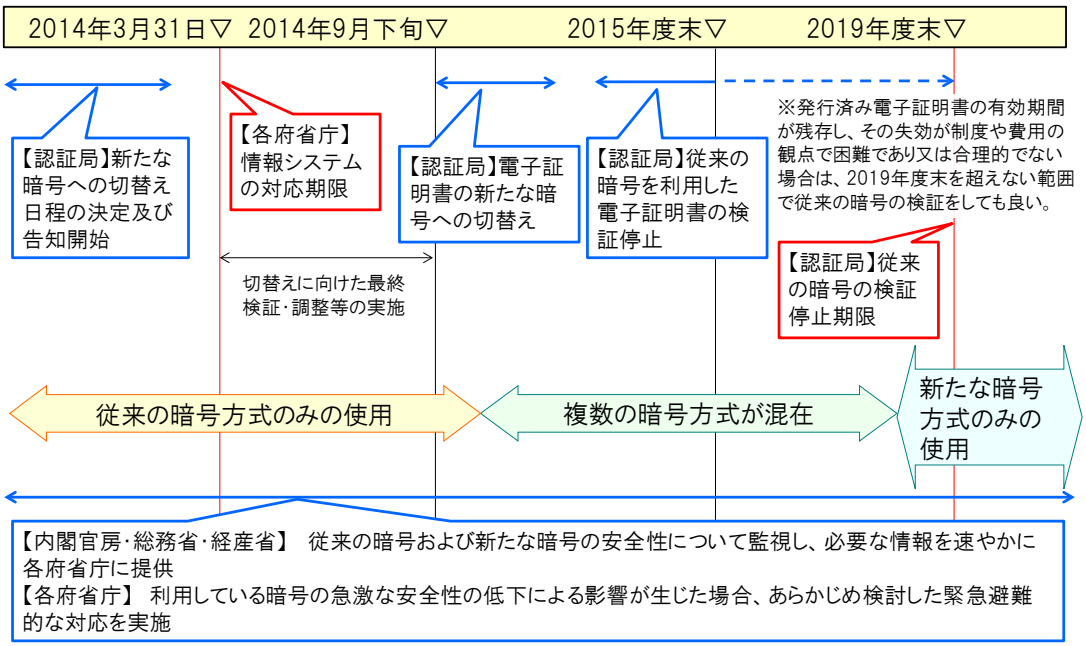
  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  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。

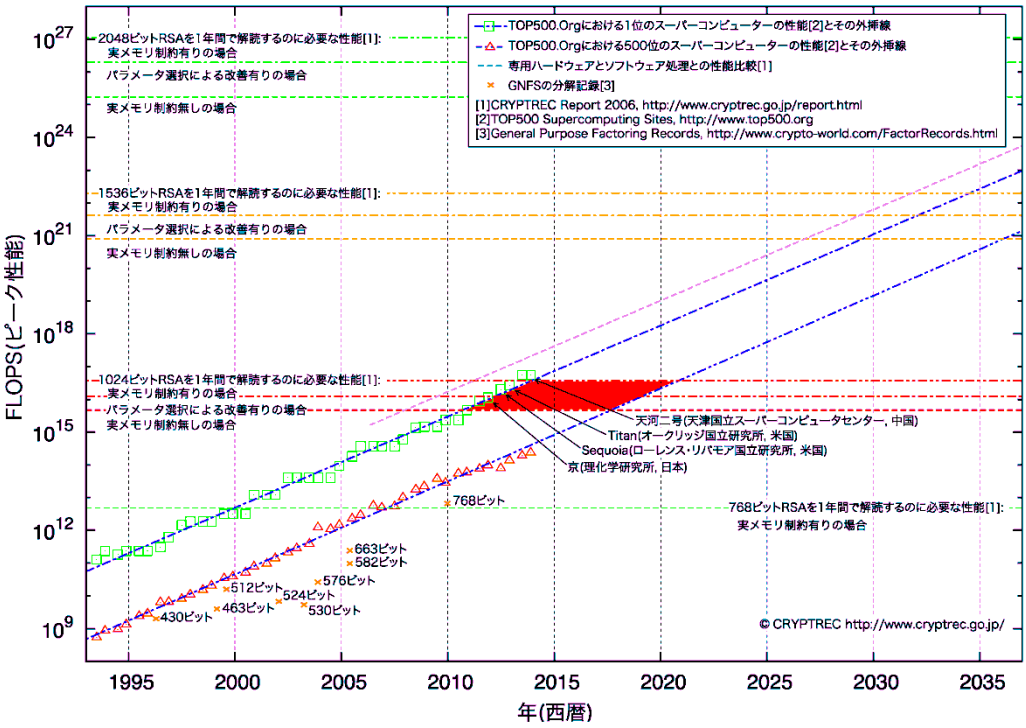


図　１年間でふるい処理を完了するのに必要な処理性能の予測（2014 年２月更新）[6]

[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）

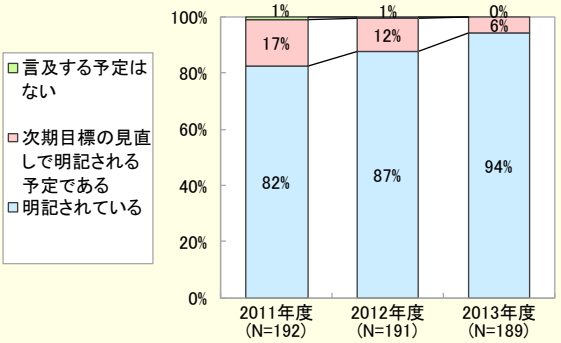
別添３－７　独立行政法人等の情報セキュリティ対策の現状について

対象機関：独立行政法人、国立大学法人及び大学共同利用機関法人（189法人）
調査時点：2014年3月末時点　（参考）前回調査：2013年3月末時点 191法人

サイバーセキュリティ2013（2013年6月27日 情報セキュリティ政策会議決定）

Ⅱ 具体的な取組
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
【独立行政法人、地方公共団体等における対策の強化】
（フ）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及び関係府省庁）
a） 関係府省庁において、所管する独立行政法人等に対して、政府機関統一基準群を含む政府機関における一連の対策を踏まえ、情報セキュリティポリシーの策定・見直しを要請するとともに、必要な支援等を行う。
b）関係府省庁において、独立行政法人等の業務特性及び対策の実施状況に応じて、自らの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する。

情報セキュリティ対策に係る中期目標への明記



情報セキュリティ対策に係るPDCAサイクルの構築

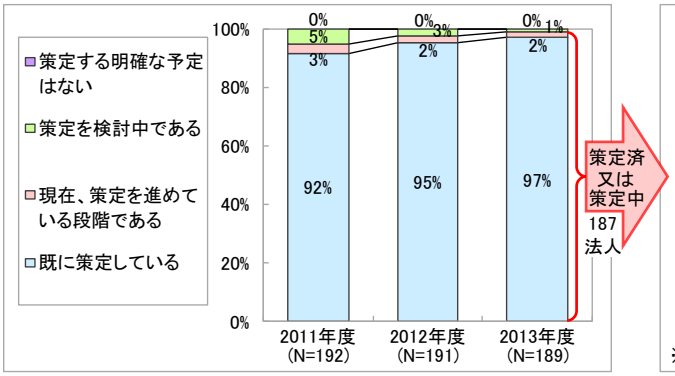
対策内容	状況	2013年度（率）
情報セキュリティポリシーの策定	実施している	97%
情報セキュリティポリシーの教育・訓練	実施している	90%
情報セキュリティポリシーの遵守状況の把握	実施している	74%
情報セキュリティポリシーの見直し	実施している	95%

- 全ての法人で中期目標への明記又は明記予定となっており、明記した法人の割合も年々増加している。
- 情報セキュリティ対策に係るPDCAサイクルについては、ポリシーの遵守状況の把握（C：Check）が十分とは言い切れない状況であり、情報セキュリティ対策が徹底されるよう、所管する府省庁への要請と必要な支援を行う。

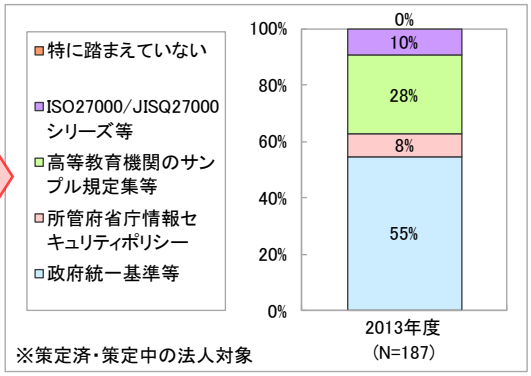
＜情報セキュリティポリシーの策定状況＞

- 全ての法人で情報セキュリティポリシーを策定する方向であり、既に策定した法人も年々増加している。
- ポリシー策定中又は策定を検討中の法人については、確実に結論を得るよう各府省庁が指導していくことが必要である。

情報セキュリティポリシーの策定



他の情報セキュリティポリシーの参照状況

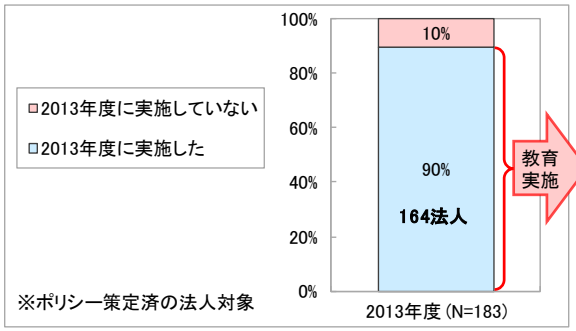


※策定済・策定中の法人対象

＜情報セキュリティポリシーの運用状況（教育・訓練）＞

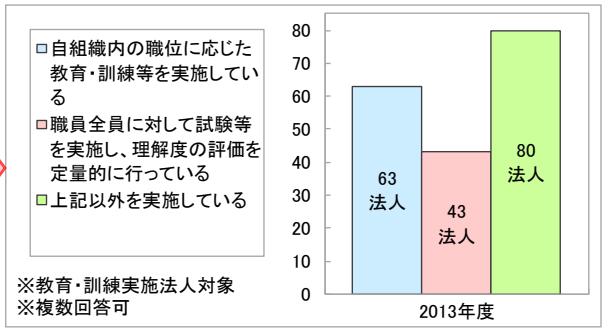
- 情報セキュリティポリシー策定済の法人において、2013年度に教育・訓練を実施した法人は90%に及ぶが、法人の中には、不定期に実施（当該年度は計画外やポリシー改定時に実施）とする法人も存在するため、毎年の教育・訓練が行われるよう、一層の対応強化が必要である。

職員の教育・訓練



※ポリシー策定済の法人対象

実施内容



※教育・訓練実施法人対象
※複数回答可

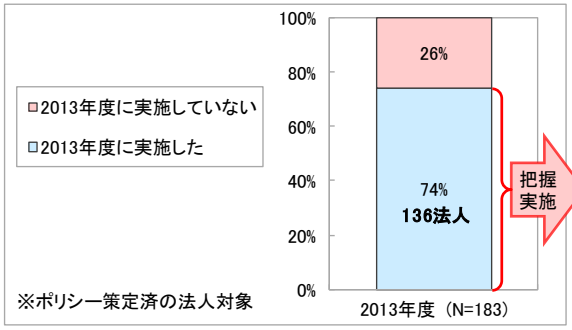
教育・訓練の実施内容『上記以外を実施している』 の主なもの：

- 情報管理マニュアル（冊子）を作成し、配布、周知した
- 職員全体を対象とした個人情報保護研修（情報セキュリティ含む）を実施した
- Web形式の情報セキュリティポリシー認識度調査を実施した
- 情報セキュリティ関連セミナー実施時に周知及び情報セキュリティ監査時の指導等
- 個人情報保護の全体研修および異動時研修に合わせて実施
- 情報統括本部ISMS内部監査員養成研修
- 全員に対して講習会を実施し、機器やソフトウェア等の不正使用に係わる確認書を受領した
- 新規採用者説明会で説明し、また全職員に対してポリシーの周知を行っている
- 情報システム復旧訓練、情報セキュリティパトロールを実施した
- フィッシングメール模擬訓練の実施

＜情報セキュリティポリシーの運用状況（遵守状況の把握、ポリシーの見直し）＞

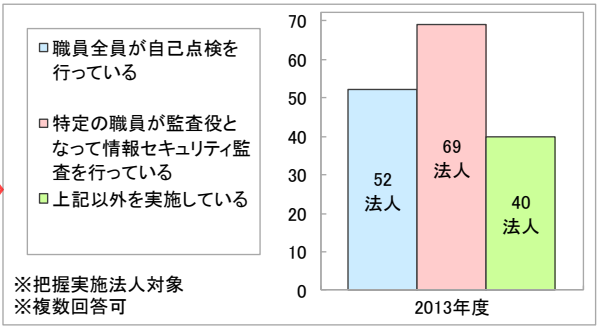
- 情報セキュリティポリシー策定済の法人において、2013年度に遵守状況を把握した法人は74%である。
- 把握していない法人には、実施規程、体制や手順を検討中とする法人が多く、対策が十分とは言い切れない。
- 遵守状況を毎年把握していくよう、一層の対応強化が必要である。
- ポリシーの見直しについては、95%の法人にて必要性を確認しており、着実に対策が進められている。

遵守状況の把握



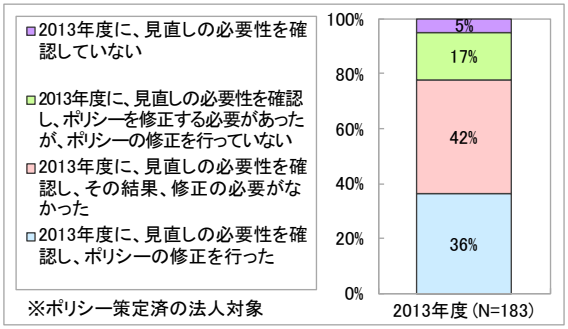
※ポリシー策定済の法人対象

実施内容



※把握実施法人対象
※複数回答可

ポリシーの見直し



※ポリシー策定済の法人対象

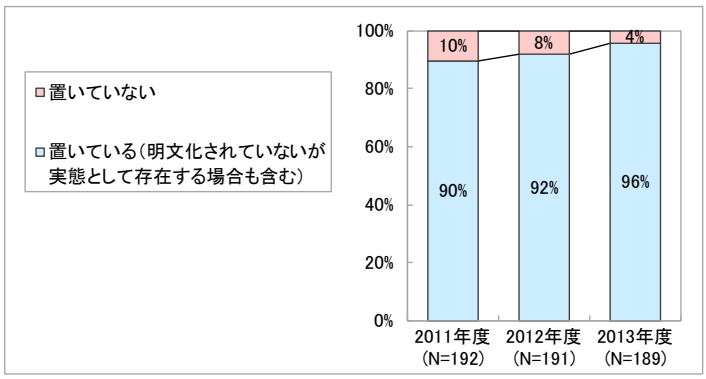
遵守状況を把握するための実施内容『上記以外を実施している』の主なもの：

- 各情報システムの管理者を対象に遵守状況の確認を行った
- 情報システムを利用する者を対象に自己点検を実施
- 業者に委託し、状況把握を行った
- WEB学習ソフトによる学習を試験的に実施した
- コンプライアンスへの対応状況として内部監査を行った
- 内部監査の際、現在の情報セキュリティに対する意識について聞き取りをした
- 情報セキュリティ委員会で運用状況について確認を行った
- 任意参加の情報セキュリティテストで、情報セキュリティポリシーの遵守状況を確認した
- 定期的に外部専門機関にシステム監査を委託実施
- 年度初めに全職員に情報セキュリティの状況調査を行っている

＜情報セキュリティ対策推進体制の整備状況＞

- 最高情報セキュリティ責任者（CISO）については、4%の法人で未設置だが、現在設置検討中とする法人も複数存在しており、着実に対応が進められている。
- 情報セキュリティ対策推進体制の構築に向けて、確実な設置が必要である。

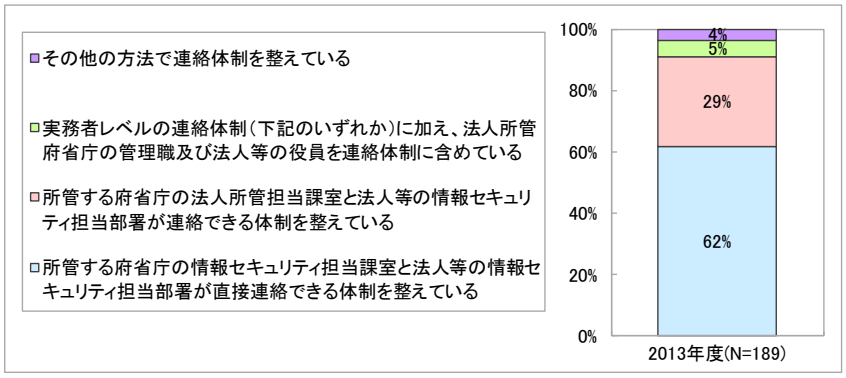
最高情報セキュリティ責任者（CISO）の設置



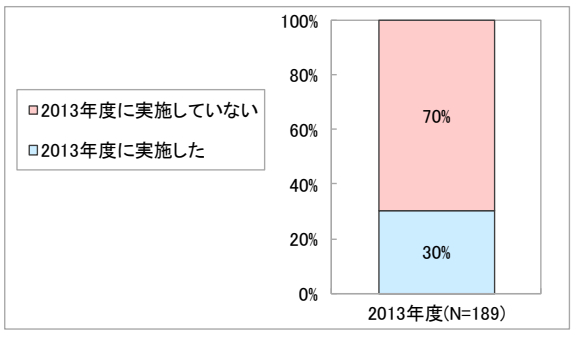
＜情報セキュリティ事案が発生した際の体制の整備状況＞

- 緊急時の体制構築については、全ての法人で整備されているが、所管府省庁の管理職及び法人等の役員を連絡体制に含めている法人はわずか5%と少ないため、迅速な意志決定に資する連絡体制を整備できるよう、一層の対応強化が必要である。

所管省庁への連絡体制



連絡体制に係る訓練の実施状況



連絡体制に係る訓練未実施の理由　の主なもの：

- 通常連絡を取り合っている部署であるため
- 情報セキュリティ担当部署が一元化され、事案発生時の連絡窓口が明確になっているため
- 組織が小さく、訓練を行う規模にないため
- 日常的に運用しており、緊急対応に当たっているため
- 通常の緊急連絡体制に含まれるため

別添３－８　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　「政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）」（2013年５月１日NISC発出）[7]

事　務　連　絡
平成２５年５月１日

各府省庁情報セキュリティ担当課室長　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）

政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）

近年、インターネット上の様々なソーシャルメディアサービス（以下、「ソーシャルメディア」という。）の普及に伴い、政府機関においても、情報発信等を目的に、こうしたサービスの利用が増えています。一方で、先般、米国の通信社の公式ツイッターアカウントが乗っ取られ、虚偽の情報が発信される事案が発生するなど、ソーシャルメディアを狙った攻撃も顕在化しています。

万一、政府機関のソーシャルメディアのアカウントが攻撃者に乗っ取られ、虚偽の情報が発信された場合、国民生活等に大きな影響を及ぼすことが懸念されます。

こうした状況を踏まえ、内閣官房情報セキュリティセンターでは、ソーシャルメディア利用におけるなりすましやアカウント乗っ取りの防止等のために留意すべき事項を取りまとめましたので、各府省庁におかれては、これらの事項に十分留意し、ソーシャルメディアを利用するようお願いします。

なお、本事務連絡は、平成 23 年 4 月 5 日付け「国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針」（内閣官房情報セキュリティセンター、内閣官房情報通信技術（IT）担当室、総務省、経済産業省連名）をベースに、情報セキュリティの確保の観点から、新たに留意すべき事項を追加したものです。

記

[7] http://www.nisc.go.jp/active/general/pdf/social_media_130501.pdf [PDF]

（１） ソーシャルメディアの特性を踏まえた利用

① ソーシャルメディアを情報公開の主たる手段として利用しない

ソーシャルメディアは、以下のような特性があることから、原則として、国民に広く公開すべき情報の主たる公開手段としては利用せず、二次的・補助的な情報公開の手段として利用してください。

- 情報の閲覧がそのソーシャルディアの利用者に限られる場合があります。
- ソーシャルメディアを提供する民間事業者の都合で、サービスが一時的に中断又は廃止されたり、扱っている情報の取扱い方法が変更されたりする場合があります。

② 組織が管理するアカウントでの運用

ソーシャルメディアは、政府機関のような組織によるアカウントと、個人利用者のアカウントで同じ環境を利用することが多いため、情報発信が組織として行われていることを明確にする必要があります。また、後述する各種セキュリティ対策も、組織として対処する必要があります。このため、ソーシャルメディアの利用時は、組織が管理するアカウントで運用し、職員個人が私的に取得したアカウントは、組織としての情報発信には利用しないでください。

③ 意図しないコミュニケーションが発生することを前提とした利用

ソーシャルメディアは、利用者間の相互コミュニケーションを促進するために、利用者の意見を表明しやすい環境となっています。このため、政府機関に対して、批判、苦情又は誹謗中傷が殺到してしまう、いわゆる「炎上」が発生したりする場合があります。

（２） なりすましの防止

① アカウントの運用組織の明示

政府機関からの情報発信であるかを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、公的機関が運用していることを国民に明示することが必要です。

② 自己管理ウェブサイトとの相互リンク

政府機関からの情報発信であるかを明らかにするために、政府機関が自身で管理しているウェブサイト（.go.jpドメインが望ましい。以下、「自己管理ウェブサイト」という。）内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けるようにしてください。また、運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている自己管理ウェブサイト上のページのURLを記載してください。

③ 認証アカウント（公式アカウント）の利用

ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、政府機関が利用するアカウントと、なりすまされたアカウントを区別する参考となるため、可能な限りこれを取得してください。

（３）アカウント乗っ取りの防止

第三者が何らかの方法で不正にログインを行い、偽の情報を発信する等の不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法については次のような適切な管理を行ってください。

① パスワードの適切な管理

以下に例示するような、パスワードの適切な管理を行ってください。

- ログインパスワードは十分な長さと複雑さを持たせる
- パスワードを知る担当者を限定する
- パスワードの使い回しはしない

② アカウント認証の強化策の利用

二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り、利用してください。

③ ログインに利用する端末の紛失・盗難の防止

ソーシャルメディアへのログインに利用する端末を紛失したり盗難されたりした場合に、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理は厳重に行ってください。

④ 使用する端末のセキュリティ確保

ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性があります。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用やアンチウイルスソフトウェアを導入するなど、適切なセキュリティ対策を実施してください。

（４）なりすましや不正アクセスを確認した場合の対処

① なりすましが発生していることを発見した場合

自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していない等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行ってください。

② アカウント乗っ取りを確認した場合

アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織のCSIRTやNISCに報告するなど、適切な対処を行ってください。

（５）　発信又は公開する情報に関する留意事項

① 要機密情報の発信の禁止

要機密情報（機密性２以上に相当する情報）は発信しないでください。

② URL短縮サービスは使用しない

URL短縮サービスにより短縮したURLは、リンク先の本来のドメイン名が表示されず、利用者がドメイン名を判断材料にしてリンク先の安全性を確認することができなくなるため、URL短縮サービスは、原則使用しないでください。

③ リンク先の内容への留意

政府機関のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するページへのリンクを掲載することは、当該の投稿やページの内容を信頼性のあるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やページの内容が変更される可能性があることを考慮した上で、慎重に行うようにしてください。

④ 発信する情報の再確認

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまいますので、完全に削除することは不可能です。このため、当該情報が機密情報の漏えい等に繋がる可能性がないか等、情報発信する前にその影響を十分に再確認してください。

（６） 情報発信を円滑に行うための利用者への配慮

① アカウント運用ポリシーの策定と明示

- アカウント運用ポリシー(ソーシャルメディアポリシー)として策定してください。その際、以下の参考資料や他の公共機関・民間企業が公表しているものを参考にしてください。
- ソーシャルメディアのアカウント設定における自由記述欄、又は、ソーシャルメディアアカウントの運用を行っている旨の表示をしている自己管理ウェブサイト上のページに、アカウント運用ポリシーを掲載してください。（自組織内にも周知しておくことが望ましい。）
- 特に、専ら情報発信用途に用いる場合には、その旨をアカウント運用ポリシーに明示してください。

（参考資料）

・法人における SNS 利用に伴うリスクと対策　（JPCERT コーディネーションセンター）
http://www.jpcert.or.jp/research/sns2012.html
・SNS の安全な歩き方　（日本ネットワークセキュリティ協会）
http://www.jnsa.org/result/2012/sns.html

以　上

２　「政府におけるサイバー攻撃への迅速・的確な対処について」（2013年６月19日情報セキュリティ対策推進会議決定）[8]

平成25年6月19日
情報セキュリティ対策推進会議決定

政府におけるサイバー攻撃への迅速・的確な対処について

近年、ますます高度化・巧妙化するサイバー攻撃に政府として迅速かつ的確に対処するため、 各府省庁において下記の取組を徹底する。

記

１　各府省庁等の情報セキュリティポリシーについて

各府省庁の情報システムに対するサイバー攻撃に係る情報を可能な限り速やかに内閣官房情報セキュリティセンターに連絡する旨、各府省庁の情報セキュリティポリシーに記載すること。また、各府省庁から所管する独立行政法人等に対して、当該独立行政法人等の情報システムに対するサイバー攻撃に係る情報を可能な限り速やかに所管府省庁に連絡する旨、当該独立行政法人等の情報セキュリティポリシーに記載するよう要請すること。

２　各府省庁等におけるサイバー攻撃に係る情報連絡体制について

各府省庁は、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成22年12月27日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）等を踏まえ、サイバー攻撃による事案が発生した際の所要の連絡体制を確認・構築すること。また、各府省庁から所管する独立行政法人等に対して、同様の確認・構築を実施するよう要請すること。

３　各府省庁等の国民への説明責任の履行について

各府省庁は、各府省庁の情報システムに対するサイバー攻撃により、国民の権利が侵害され又は行政事務の遂行に重大な支障を及ぼすおそれがある情報の漏えいや破損等の可能性がある事案が発生した場合には、必要に応じ、国民への説明責任を果たすこと。また、各府省庁から所管する独立行政法人等に対して、同様の対応をとるよう要請すること。

[8] http://www.nisc.go.jp/press/pdf/ciso_10_press.pdf［PDF］

３　「再発防止策等の徹底について」（2013年７月11日情報セキュリティ対策推進会議議長指示）[9]

再発防止策等の徹底について

平成25年7月11日
情報セキュリティ対策推進会議議長指示

1. 民間企業が提供する約款によるグループメールサービスを業務に利用していないかどうかの実態を早急に調査すること。

2. かかるメールサービスを業務に利用した結果、情報漏出が生じていないか、遺漏なく点検すること。

3. 点検の結果、情報漏出のおそれがある事案がある場合には、直ちに漏出防止措置を講ずること

4. 以上の結果は迅速にNISCに報告すること。

5. 民間企業の提供する約款によるグループメールサービスを、機密情報を扱う業務に利用することのないよう、各府省庁の情報セキュリティポリシーを職員に徹底すること。

[9] http://www.nisc.go.jp/conference/suishin/ciso/dai11/pdf/2.pdf [PDF]

４　「Windows XP等のサポート終了に係る注意喚起並びに重点検査項目の追加について」（2013年７月23日NISC発出）[10]

事　務　連　絡
平成 25 年７月２３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）

Windows XP 等のサポート終了に係る注意喚起
並びに重点検査項目の追加について

日本マイクロソフト株式会社が提供するソフトウェア製品 Windows XP、Office 2003、Internet Explorer6（いずれも同社の登録商標）は、2014 年 4 月 9 日のサポート終了に伴い、同日以降はセキュリティ関連の脆弱性などを修正するための修正プログラムの提供は行われなくなる予定です（参考参照)。

サポート終了後に、Windows XP、Office 2003、Internet Explorer6 を使用することは、不正プログラム感染や不正アクセスによる情報漏洩などのリスクが高くなります。「政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版)」（2.2.2.1 セキュリティホール対策）においても、政府機関の情報システムは、公開されたセキュリティホールへの対策を求めており、Windows XP、Office 2003、Internet Explorer6 を利用する情報システムは、上記サポート終了後はこれを満たすことができません。

各府省庁においては、サポート終了に伴うご対応を順次進めていただいていると存じますが、改めて自府省庁の情報システムについて、Windows XP、Office 2003、Internet Explorer6 の利用状況と、サポート終了に向けた対応計画を確認し、サポート終了までにソフトウェア更改等の適切な対応をお願いいたします。

また、本件に係る対応状況については、平成 25 年 7 月 16 日付事務連絡別添２「重点検査結果の報告要領」に定める「情報セキュリティ上のトピックのうち重要性が見込まれる事項」に該当するため追加の検査項目として報告を頂きますようお願いします。なお、回答様式は他の重点検査項目と併せて別途配布する予定です。

（参考）
Windows XP/Office 2003 をご利用のお客様へ　（日本マイクロソフト株式会社）
http://www.microsoft.com/ja-jp/windows/lifecycle/xp_eos.aspx

[10] http://www.nisc.go.jp/active/general/pdf/winxp_130723.pdf [PDF]

５　「グループメールサービスの利用に関する事案の再発防止策について」（2013年７月30日情報セキュリティ対策推進会議）[11]

グループメールサービスの利用に関する事案の
再発防止策について

平 成 ２ ５ 年 ７ 月 ３ ０ 日
情報セキュリティ対策推進会議

政府におけるグループメールサービスの利用に関する事案の再発防止策についてまとめたところ、以下の通り。

１．策定機関
２１政府機関

２．対策の内容

《NISCからの対策情報発出》
・ 各府省庁向けに対策情報を発出し、グループメールの利用やアプリケーションの開発など、外部委託を利用する際における情報セキュリティ対策について注意喚起を図る

《各組織における職員向けの対策》
・ 各府省庁において、研修や教育の拡充、セキュリティ事案に関する状況に応じた注意喚起発出、閲覧制限などの技術的対策等を通して、各職員に情報セキュリティポリシーを徹底

《各組織における体制強化》
・ 各組織におけるさらなる情報セキュリティ確保のため、専任の対策官の設置、統括情報セキュリティ責任者や情報セキュリティアドバイザーの権限強化といった体制強化を検討

《政府全体での業務手段の確保》
・ 関係機関連携の下、業務情報の安全かつ円滑なやり取りを確保すべく、各省庁で共用できるグループメールサービス等を政府で構築することを早急に検討

[11] http://www.nisc.go.jp/conference/suishin/ciso/dai12/pdf/2.pdf [PDF]

６　「外部委託に係る情報セキュリティ対策等について（注意喚起）」（2013年７月30日NISC発出）[12]

事　務　連　絡
平成 25 年 7 月 30 日

各府省庁情報セキュリティ担当課室長　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）

外部委託に係る情報セキュリティ対策等について（注意喚起）

先般、政府機関において民間企業が提供するグループメールサービスを業務利用した結果、必要な情報セキュリティが確保されなかった事案が発生しました。本事案は、統一管理基準で定める府省庁外情報システムの利用及び外部委託における重要な情報の取扱い並びに情報セキュリティ上必要な措置について十分理解されていないことが原因の一つと考えられますが、民間企業が提供する外部の情報処理サービスの利用に際して注意すべき事項を十分認識していないことも考えられます。

このような状況を踏まえ、下記のとおり民間企業による役務の提供を受ける場合の情報セキュリティ上の注意事項について改めて取りまとめましたので、適切な対応をとっていただくようお願いいたします。

記

（１）約款による情報処理サービスを業務で利用する際の注意事項

①　機密情報を扱う業務におけるグループメールサービス等の利用の禁止

平成25年７月11日開催の情報セキュリティ対策推進会議（CISO等連絡会議）における議長指示「民間企業の提供する約款によるグループメールサービスを、機密情報を扱う業務に利用することのないよう、各府省庁の情報セキュリティポリシーを職員に徹底すること。」のとおりですが、グループメールサービス以外についても、約款が用意されており、情報セキュリティに関する事項について利用者による条件選択の余地が限られている情報処理サービス（以下「約款による情報処理サービス」という。）では、情報セキュリティに関する特約を個別に締結できない等の問題があるため、機密性を要する情報を扱う業務での利用は原則認められませんので、各府省庁における情報セキュリティポリシーの徹底を図るようお願いします。なお、国民への情報提供等の目的で公開情報を扱う場合については、約款による情報処理サービスの利用を妨げるものではありません。

[12] http://www.nisc.go.jp/active/general/pdf/gaibuitaku_130730.pdf [PDF]

・再発防止策等の徹底について（平成25年７月11日情報セキュリティ対策推進会議）
http://www.nisc.go.jp/conference/suishin/ciso/dai11/pdf/2.pdf

② レンタルサーバ利用時のバックアップの実施

約款による情報処理サービスでは、一般的に、データのバックアップまでは保証されておらず、利用者側の責任となっている場合がありますので、約款の内容を踏まえた上で適切なバックアップの実施の必要性を検討する必要があります。

・レンタルサーバ業者におけるデータ消失事象について（注意喚起）（平成24年６月29日）
http://www.nisc.go.jp/active/general/pdf/rentalsv_kanki_120702.pdf

（２）ソーシャルメディアを利用する際の注意事項

政府機関においてソーシャルメディアを業務で利用する場合、ソーシャルメディアの特性を踏まえた利用が求められます。

ソーシャルメディアは拡散性が高いという特徴がある一方で、その過程で誤った情報が付加されたり、一部の情報のみが切り取られたりすることで、本来の意図とは異なる形で情報が伝搬する可能性があります。また、ソーシャルメディアを運営する民間事業者の都合でサービスが一時的に中断又は廃止されたり、扱っている情報の取扱い方法が変更されたりすることもあります。これらの理由から、重要な公開情報については、自己管理のウェブサイトに主たる情報として掲載した上でソーシャルメディアの投稿を活用する等の対応が必要です。

また、ソーシャルメディアの利用時は、組織が管理するアカウントで運用し、職員個人が私的に取得したアカウントは、組織としての情報発信には利用しないよう注意が必要です。さらに、なりすましやアカウント乗っ取りについても対策が必要です。

政府機関においてソーシャルメディアを業務で利用する場合について、平成25年５月１日に「政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）」にて、情報セキュリティ対策等に関する注意事項を示していますので、再度徹底をお願いします。

・政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）（平成25年５月１日）
http://www.nisc.go.jp/active/general/pdf/social_media_130501.pdf

（３）アプリケーション及びウェブコンテンツ等を作成する際の注意事項

政府機関がアプリケーションやウェブコンテンツ等を作成し国民に提供する際には、情報システムの情報セキュリティ対策措置及び機密情報の取扱い等について、安全性に注意した取扱い措置が求められます。

以下に、政府機関が提供するアプリケーションやウェブコンテンツ等（以下「政府機関提供コンテンツ」という。）の作成を外部に委託する際、近年の新しい情報通信技術の利用形態の発展を踏まえ、特に注意すべき事項について示します。

① 利用者個人の行動を追跡する機能の組込みに関する注意

民間企業が提供するアプリケーションやウェブコンテンツ等においては、広告を提供する等の目的で利用者個人の行動を追跡するトラッキングという手法がよく用いられています。トラッキングに際してはクッキーや端末識別番号、URL短縮サービス等が利用されますが、トラッキングは、行動履歴という利用者のプライバシーに係る情報（以下「利用者情報」という。）の第三者提供につながりますので、政府機関提供コンテンツにおいては、国民のプライバシーを不当に侵害することのないよう注意する必要があります。

政府機関提供コンテンツの作成を民間企業に業務委託する場合、委託先がこの点に留意せず不用意に利用者情報を収集又は第三者提供するトラッキング機能を組込んでしまう事態が想定されます。政府機関提供コンテンツとして不適切なサービスが国民に提供されてしまうことがないよう、業務委託時の契約において、利用者個人の行動を追跡する機能を不用意に組込まないよう、発注仕様を明確にする等の措置が必要です。

② 政府機関提供コンテンツへの広告表示に関する注意

民間企業が提供するアプリケーションやウェブコンテンツ等では一般的に広告を表示させることが多いため、政府機関提供コンテンツの作成を民間企業に業務委託した場合に、委託先が故意又は不用意に政府機関提供コンテンツ内に広告を表示させる機能を埋め込む可能性があります。政府機関提供コンテンツにおいて広告を表示させる場合には、「国のウェブサイトへのバナー広告掲載要領」（関係省庁申合せ 平成24年6月25日改定。以下「掲載要領」という。）の規定に従う必要がありますが、民間企業においては、掲載要領に適合しない広告を用いることもあることから、委託先が不用意に広告を表示させる機能を埋め込むと、掲載要領に違反するコンテンツが表示されたり、前記①のトラッキング手法が用いられたりするおそれがありますので、注意が必要です。

政府機関提供コンテンツの作成を民間企業に業務委託する場合、広告を表示させる機能の埋め込みを業務委託時の契約において禁止する、又は、掲載要領に適合する広告のみが表示されるよう、発注仕様を明確にする等の措置が必要です。

③ 委託先に係る詳細の確認に関する注意

外部にアプリケーション等の開発を委託するにあたり、委託先や再委託先が、悪意のある不正プログラムを含む不適切なプログラムを故意又は不用意に組込むリスクについて注意する必要があります。

こういった不適切なプログラムの組込みについては、委託先事業者の所在地や、委託先で設計・開発に係る者の所属、専門性（資格等）、実績及び国籍等を確認する等の対応を行うことが重要です。また、委託先が再委託する場合においても、再委託先の会社名、代表者名、所在地、及び主な出資者等について確認することを推奨します。

以　上

７　「最近の情報セキュリティ問題への対処について」(2013年12月12日 情報セキュリティ対策推進会議申し合わせ）[13]

最近の情報セキュリティ問題への対処について

平成２５年１２月１２日
情報セキュリティ対策推進会議申し合わせ

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

１．ウィンドウズ XP 等のサポート終了問題

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

２．複合機等のインターネットに接続された機器のセキュリティ問題

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

記

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

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

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

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

[13] http://www.nisc.go.jp/conference/suishin/ciso/dai14/pdf/2.pdf [PDF]

８　「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。

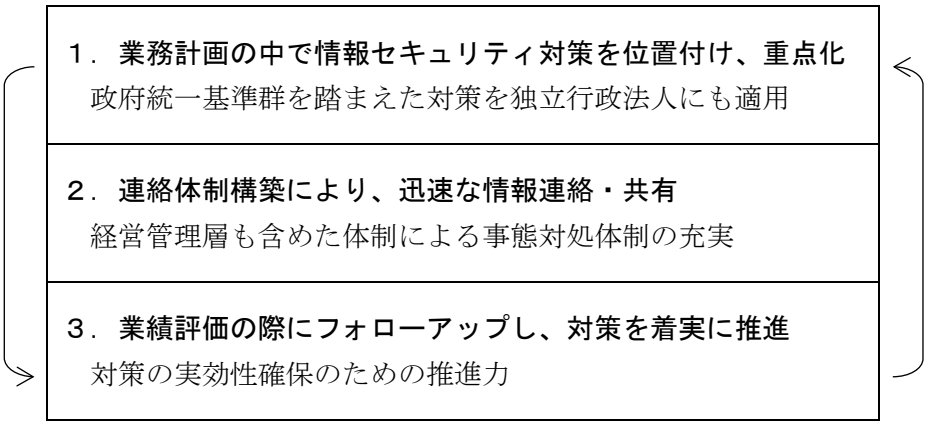
２．実効性のあるインシデント情報共有体制の構築

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



別添３－９　政府機関等に係る2013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
2013年	４月	【概要】原子力規制庁は、環境省が関係省庁向けに作った環境大臣の「会見録」を、メールアドレス登録している報道関係者約250人に誤送信したと発表。 【対応等】誤送信した報道関係者には担当者が専用のメーリングリストを作成し、毎回、使用していたところ、本事案が起きた時は、本来の担当者と違う職員がメールアドレスを直接入力し、送信したため誤送信を招いた。本事案後は担当者を決めて、報道関係者への送信者、メーリングリストの管理を一人で行うこととした。	意図せぬ情報流出
		【概要】宇宙航空研究開発機構は、サーバへ外部から不正なアクセスがあり、国際宇宙ステーション日本実験棟「きぼう」の運用準備に使われる参考情報等が流出した可能性があると発表。その後、宇宙航空研究開発機構は同事案について、サイバー攻撃を受け、国際宇宙ステーション日本実験練「きぼう」、宇宙ステーション補給機「こうのとり」の運用準備に係る技術情報等が流出したと発表。	外部からの攻撃
	５月	【概要】住宅金融支援機構は、同機構のメールアドレスを詐称したメールが送信された可能性があることを発表。	その他
		【概要】日本貿易振興機構は、サーバが何らかの理由により意図せざる外部との通信を行っていた可能性があると発表。	外部からの攻撃
		【概要】国土交通省は、北陸地方整備局湯沢砂防事務所に設置している外部委託者用メールサーバーが、外部から不正アクセスを受けたことが判明し、当該メールサーバーが踏み台となり、大量のスパムメールが送信された可能性がある旨、発表。 【対応等】大量のスパムメールが不正中継されていた。ウイルスの感染や情報の漏洩はなかった。当該メールサーバの回線は切断し、利用を停止した。	外部からの攻撃
	６月	【概要】科学技術振興機構は、同機構のウェブサイトにおいて、第三者の不正アクセスにより一部ページが改ざんされたと発表。	外部からの攻撃
		【概要】東京大学医学部付属病院は、同病院サイトのトップページに他の悪質なホームページに誘導する不正なデータが埋め込まれる事案が発生したと発表。	外部からの攻撃
		【概要】海洋研究開発機構高知コア研究所は、同研究所のウェブサイトにおいて、第三者の不正アクセスにより一部のページが改ざんされたと発表。	外部からの攻撃
		【概要】鹿児島大学は、同大学共同獣医学部付属病院のホームページが第三者に改ざんされたと発表。	外部からの攻撃
	７月	【概要】インターネット上でメールを共有できる米グーグルの無料サービス「グーグルグループ」で個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた。 【対応等】内部情報等が誰でも閲覧できる状態になっていることが確認された府省庁（復興庁、農林水産省、国土交通省、環境省）においてサービスの利用を停止するなどの措置を講じたほか、NISCにおいて全府省庁を対象とした調査を実施するとともに、各府省庁の情報セキュリティポリシーの徹底を図った。調査の結果、その他の府省庁における同様の事態は確認されなかった。	意図せぬ情報流出
		【概要】国土交通省は、同省九州地方整備局港湾空港部のコンピューターサーバーから不正通信の可能性のある外部への通信があったことを確認し、何らかの情報が流出した可能性があると発表。 【対応等】情報流出の可能性を把握した直後からサーバや端末等の詳細な調査を実施した結果、不正通信が確認されたが、流出した情報の特定及び情報流出の原因の究明には至らなかった。県警等の関係機関と連携しつつ、再発防止のために通信の監視体制強化等の対策を実施している。これらの状況について12月25日に発表した。	外部からの攻撃
		【概要】科学技術振興機構は、外部からの攻撃を受けたことから、安全策を講じるため、一時「J-STAGE」サービスを停止していたと発表。	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】内閣府は、交通安全総合ネットワーク「Cross Road」（内閣府ホームページに掲載）に対する不正アクセスが確認されたが、現時点で内容の改ざん等の被害は確認されていないと発表。 【対応等】当該サイトに対する断続的な不正アクセスが確認された事実を公表するとともに、サイトを利用する全登録者に対して説明を行った。当該サイトを一端閉鎖し、動的サイトから静的サイトへの見直しを行った後、再開した。	外部からの攻撃
		【概要】科学技術振興機構は、大学などの研究者に交付する競争的資金の申請書類計27課題分のデータが、検索サイト経由で閲覧できる状態になっていたと発表。	その他
		【概要】厚生労働省は、成田空港検疫所の職員１人のメールのアカウントとパスワードが不正に使用され、検疫所のメールサーバに不正アクセスされ、メールが大量に送信されたと発表。 【対応等】不正なアクセスを、７月23日に確認し調査を行ったところ、７月21日から23日まで不正アクセスが行われていたが、23日中にアカウント等の変更を行い、それ以降不正アクセスは停止されている。また、他の職員のメールアカウントへの不正アクセスの形跡はなかった。なお、メールサーバへの不正アクセスはあったが、検疫所に関する情報の漏えい等の実害は確認されていない。その後、不正アクセスを防止するための対策も講じている。	外部からの攻撃
	８月	【概要】東京海洋大学は、同大学産学・地域連携推進機構ウェブサイトにて、第三者の不正アクセスにより一部ページが改ざんされていたと発表。	外部からの攻撃
		【概要】佐賀大学総合情報基盤センターは、教育用メールサービスが学外から大量メール送信の攻撃を受けたと発表。	外部からの攻撃
		【概要】厚生労働省は、労働基準局安全衛生部化学物質対策課が事務局である会議に関し、傍聴が可能である旨のメールを送信した際、個人メールアドレスを「CC」で送信したため、外部の傍聴希望者に全員のメールアドレスが表示されたまま送信されるという個人情報漏えい事案が発生したと発表。 【対応等】宛先の各者に対し、漏えいに関するお詫びと、問題のメールを削除するよう依頼するメールを送付した。	意図せぬ情報流出
		【概要】神戸大学は、「グーグル・グループ」に保存していた同大学留学生センターに所属する学生の成績評価案等の個人情報がインターネット上で閲覧可能な状態となっていたと発表。	意図せぬ情報流出
		【概要】森林総合研究所は、職員が不審なメールを開いてアカウントが盗用され、大量のメールが送信されたと発表。	外部からの攻撃
		【概要】理化学研究所は、同研究所北京事務所のウェブサイトがウイルス感染したことが８月14日に判明し、15日から同サイトを閉鎖していると発表。	外部からの攻撃
	９月	【概要】国土交通省淀川河川事務所は、淀川河川公園の施設利用ホームページに外部から不正侵入された可能性があったことから、閉鎖していること、現時点で個人情報が流出した形跡はないことを発表。 【対応等】施設利用ホームページは2014年５月28日現在閉鎖している。予約システムの停止が長期間続いているため、「調査を行ったこと、その結果情報漏洩の可能性は極めて低いこと、ホームページの会員にお詫びしていること」を４月11日に発表した。今回の問題点を解消した新システムを構築し、2014年年度末を目処にホームページによる予約を再開予定。	外部からの攻撃
		【概要】国土交通省は、国営武蔵丘陵森林公園ホームページのサーバー内に不正プログラムが発見されたため、公開を一時中止し、原因を調査していると発表。 【対応等】ソフトウェアのバージョンが古いことによる脆弱性をつかれたものと推測されるファイルが見つかったが、詳細は不明。現在はソフトウェアの更新、更新端末の制限などを行い公開を再開している。なお、当該ホームページは個人情報を取り扱っていない。	外部からの攻撃
		【概要】日本銀行金融市場局企画課市場整備Ｇは、同整備Ｇから金融機関の担当者に対して、電子メールを送信した際、宛先を「To」で一斉送信したことにより、送信先308件のメールアドレスが他の受信者に見える状態になっていたことを発表。 【対応等】電子メールの送信時、宛先に外部のアドレスを含む場合において、あらかじめ設定した宛先形式、宛先数を超えた際は、送信者に注意喚起するシステム対策を講じた。	意図せぬ情報流出
		【概要】東京工業高等専門学校は、インターネットを利用したファイル管理システムに保存されているファイルについて、学生の成績情報等の個人情報を含むものが学校関係者以外からアクセスできる状態となっていたと発表。	意図せぬ情報流出

年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】琉球大学は、同大学教育学部付属小学校の児童を管理するサーバが不正アクセスを受け、児童のデータ770人分が流出したと発表。	外部からの攻撃
		【概要】科学技術振興機構は、同機構の中国総合研究交流センターが運用するウェブサイト「客観日本」の一部が不正アクセスにより改ざんされていたと発表。	外部からの攻撃
		【概要】国立青少年教育振興機構は、同機構のホームページで第三者の不正アクセスにより一部ページ改ざんが発生したため、ホームページを一時停止したと発表。	外部からの攻撃
	10月	【概要】国立遺伝子学研究所は、同研究所研究用ウェブサイトの一部が不正アクセスにより改ざんされたため、サービスを停止したと発表。	外部からの攻撃
		【概要】国土交通省は、同省自動車局審査・リコール課が運営する「自動車の不具合・リコール情報」のサイトにおいて利用しているソフトウェアに情報セキュリティ上の脆弱性が確認されたことから、一時的に機能を制限すると発表。 【対応等】脆弱性が確認されたソフトウェアを使用しないシステムに改修を行い、2014年３月31日に全機能の利用を再開した。	その他
		【概要】中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃（標的組織のIPアドレスからのサイト閲覧者だけが感染するもの）が８月から９月にかけて発生。 【対応等】NISCを中心として情報共有等することで各府省庁で早期に攻撃の把握、注意喚起、調査等の対応を実施した。その結果、複数（７省庁）の省庁において端末等のウイルス感染が確認されたが、本事案による情報流出は確認されなかった。	外部からの攻撃
		【概要】厚生労働省は、「公益通報相談窓口」を通じて内部告発してきた通報者の電子メールについて、労働基準局監督課職員が内容を確認する返信メールを送信する際に、別の案件の通報者に誤送信したと発表。 【対応等】関係者に速やかに連絡を取り、経過の説明及び謝罪をし、御了解いただいた。併せて、別の案件の通報者に対しては、誤送信したメールの破棄を依頼し、メールを破棄していただいたことを確認した。	意図せぬ情報流出
	11月	【概要】東京外国語大学は、同大学国際社会学部学生が学務情報システムに偽装したフィッシングサイトを作成し、不正に入手したユーザIDとパスワードを用いて、学務情報システムに不正にアクセスしたと発表。	内部不正
		【概要】東京大学医科学研究所、東北大学、琉球大学の３大学で、ファックスやスキャナーで読み取った、学生らの個人情報がインターネット上で誰でも閲覧できる状態になっていた。	意図せぬ情報流出
		【概要】国土交通省海事局船員政策課は、各船社の船舶保安統括者に対し、送信先全て(136件)のメールアドレスが表示された形式で事務連絡を送信したと発表。 【対応等】外部に一斉電子メールで情報を送信する際には、個人情報保護に留意し、BCC形式で送信を行うこと、送信先や送信方法の確認、送信時のダブルチェック等の徹底を図った。	意図せぬ情報流出
		【概要】筑波大学計算科学研究センターは、同センターにあるスーパーコンピューターログインサーバへの不正アクセスにより、全ユーザの暗号化されたssh公開鍵認証情報が取得された可能性があると発表。	外部からの攻撃
		【概要】京都大学基礎物理学研究所は、外部からのコンピュータ不正アクセスのため、スーパーコンピュータを含む計算機サービスを一部停止していたと発表。	外部からの攻撃
		【概要】高エネルギー加速器研究機構は、同機構が運用するスーパーコンピューターシステムログインサーバに対する外部からの不正アクセスが発見されたと発表。その後、調査の結果、システムおよびユーザー領域における改ざん、ならびに個人情報の漏えい等の被害が無いことを確認したと発表。	外部からの攻撃
		【概要】国土交通省は、関東地方整備局国営昭和記念公園事務所が使用している外部ホスティングサーバへの不正アクセスがあり、当該サーバを経由した外部サーバへのアクセスが行われていたことを発表。 【対応等】アプリケーションのバージョンが古いことによる脆弱性をつかれたものであり、海外からの複数のアクセスを確認できたが詳細は不明。事件発生後すぐに運用を停止し、改修の検討を行っている。なお、当該サーバは、個人情報及び機密性を有する情報は保存しておらず、データ管理用のサーバであり一般の方向けのホームページとの関連はない。	外部からの攻撃

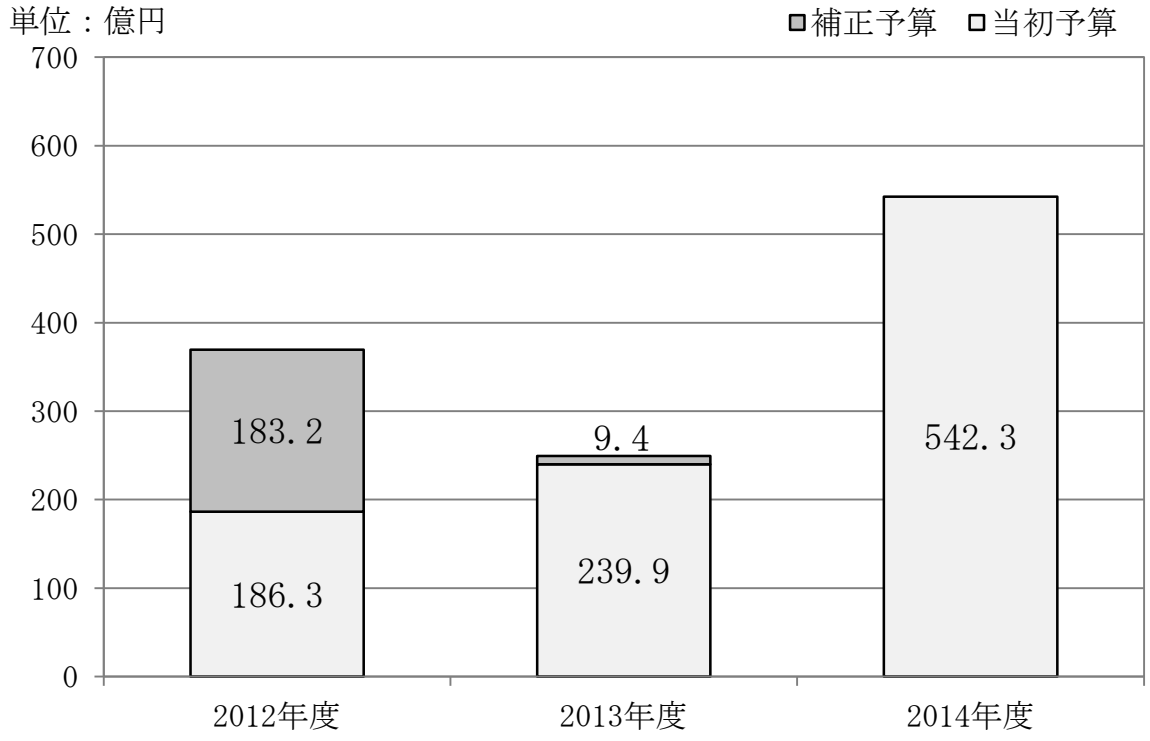
年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		【概要】国土交通省四国山地砂防事務所は、同事務所に設置している地すべり自動観測システムのメールサーバが外部から不正アクセスを受けたと発表。 【対応等】調査の結果、情報の漏洩、ウイルスの感染についてはなかった。 認証パスワードの強度の不足により、アカウントを不正利用されたのが原因でありパスワードをより強度の高いものに変更した。また、事務所独自のインターネット接続は廃止し、局経由でインターネット接続を行う方針とする。	外部からの攻撃
	12月	【概要】信州大学は、学内の教員免許更新支援センターのサーバーが不正アクセスを受け、免許状更新講習の受講申込者7,822人分の個人情報が流出した可能性があると発表。	外部からの攻撃
		【概要】国立がん研究センターは、同センター職員ががん検診を受けた9,121人の氏名や判定結果など個人情報の入ったUSBメモリーを紛失したと発表。	意図せぬ情報流出
		【概要】労働者健康福祉機構福井及び熊本産業保健推進連絡事務所は、両事務所のメールアドレスを不正に使用したメールが送信されたと発表。	外部からの攻撃
		【概要】外務省や東京大学などの一部のパソコンにおいて、入力した全ての文字情報が「百度（バイドゥ）」のサーバに送信される日本語入力ソフト（Baidu IME）がインストールされていた。	意図せぬ情報流出／その他
2014年	１月	【概要】日本原子力研究開発機構は、高速増殖炉もんじゅで、職員用のパソコン１台がウイルス感染し、メールなどの情報が外部に漏れた可能性があると発表。その後、調査の結果、動画再生ソフトの更新の際にウイルス感染した可能性があるが、当該パソコン以外のパソコンへのコンピュータウイルス感染の拡大は確認されず、メールアドレス等の個人情報、プラント情報、核不拡散・核セキュリティ上重要な情報は含まれていなかったと発表。	外部からの攻撃
		【概要】外務省は、同省が運営する日本留学総合ガイドホームページの一部にウイルスのチェックが不十分なままコンテンツが一時期掲載され,場合によって閲覧者のパソコンがウイルスに感染している可能性があったと発表。 【対応等】速やかにコンテンツを差し替え、ホームページ上で注意喚起を行ったが、閲覧者のウイルス感染等の被害は確認されなかった。再発防止に向け,多層的にウイルス対策を実施するなど、一層の情報セキュリティ対策強化に努めている。	外部からの攻撃
		【概要】農業・食品産業技術総合研究機構と農業生物資源研究所は、フィッシングメールにより、メールの送受信に必要なID等が盗まれ、研究員らのメールアカウントを使って大量の不審なメールが発信されたと発表。	外部からの攻撃
	２月	【概要】東京大学カブリ数物連携宇宙研究機構は、観測データ解析用の計算機に不正アクセスがあり、ユーザ認証情報が取得された可能性があると発表。	外部からの攻撃
		【概要】国立天文台は、東京大学カブリ数物連携宇宙研究機構から奪取された認証情報を用いた不正アクセスが発生したが、個人情報や研究データの喪失は確認されていないと発表。	外部からの攻撃
		【概要】国立がん研究センター東病院のパソコン２台が動画再生ソフト「GOMプレーヤー」をアップデートした際にウイルスに感染していたことが判明。	外部からの攻撃
		【概要】筑波大学計算科学研究センターは、同センター計算機システム T2K-Tsukubaログインサーバーにおいて、外部から不正アクセスがあったと発表。	外部からの攻撃
		【概要】筑波大学は、同大学内のハードディスクに記録された学生や教職員ら約450人の個人情報が、一定期間検索サイトで閲覧可能になっていたと発表。	意図せぬ情報流出
		【概要】名古屋大学は、同大学院医学系研究科が使用するサーバ内の研究のために集積した検査データ356人分及び学生の名簿42人分等の個人情報が、外部から閲覧可能になっていたと発表。	意図せぬ情報流出
	３月	【概要】浜松医科大学は、同大学院生が同大学付属病院の患者の個人情報を含むファイルを個人所有のコンピューターに入れて無断で学外に持ち出し、電子メールで誤送信したと発表。	その他
		【概要】鳥取大学は、附属病院の医師が患者の個人情報の入ったUSBメモリーを紛失したと発表。	意図せぬ情報流出
		【概要】建築研究所は、同研究所国際地震工学センターのサーバーからシステムの利用登録者情報の内330件の電子メールアドレス等が漏えいしたと発表。	外部からの攻撃

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

別添３－１０ 政府のサイバーセキュリティ関係予算額の推移

	2012 年度	2013 年度	2014 年度
当初予算額	186.3 億円	239.9 億円	542.3 億円
補正予算額	183.2 億円	9.4 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２次行動計画の各施策の成果と課題

１　安全基準等の整備及び浸透

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- ✓ 「安全基準等の整備及び浸透」に期待される成果は、重要インフラ事業者等における各種の対策の更なる充実と、その着実な実践である。
- ✓ そのため、指針と安全基準等の項目の充実と、個別事業者等の安全基準等に基づいた取組みの確実な実施に着目した指標を設定する。
- ✓ 具体的な指標は、指針及び参考資料に採録した対策項目数、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数、指針の重要インフラ事業者等による評価とする。

(1) 実施状況

情報セキュリティ対策に取り組む関係主体が、自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指し、安全基準等の整備及び浸透に取り組んだ。

具体的には、サイバー攻撃の高度化等の環境変化、東日本大震災にて生じた複合的システム障害やデータ滅失等への対応にて得た教訓等を踏まえ、「指針の継続的改善」として2010年度及び2012年度に指針本編の改定及び対策編の新設・改定を行った。

加えて、「安全基準等の継続的改善」として重要インフラ所管省庁による同改善状況を、「安全基準等の浸透」として重要インフラ事業者等による情報セキュリティの対策状況を年度ごとに調査・報告を行った。

(2) 成果

指針において、対策項目を「要検討事項」と「参考事項」に分類し、335項目の具体例を採録した。また、浸透状況等の調査によると、調査対象の約50%の重要インフラ事業者等が定期的な自己検証を、約70%が自己検証を行っているとの結果を得た。

このことから、指針と安全基準等の一体的・安定的な見直しサイクルを確立するともに、情報セキュリティ対策の啓発推進を強化する等、重要インフラ防護に向けて一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(3) 課題

サイバー攻撃についてはますます複雑･巧妙化しており、例えば他事業者等を経由した侵入、他事業者等から窃取した可能性がある情報による侵入及びユーザー情報窃取、他事業者等になりすました上でのDoS攻撃等が見受けられる状況にある。

このことを各重要インフラ事業者等の情報セキュリティ対策に照らした場合、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・強化にも効力が及ぶ等、その重要性が従来より増加している状況にあると言える。

加えて、重要インフラ事業者等からは、指針に対して「対策について、段階的な（優先順位付けされた）指針にするとわかりやすい」、「対策編で更なる具体的内容を提示してほしい」等との意見がある。

これらに鑑み、各重要インフラ事業者等の情報セキュリティ対策に資することを目的とした重要インフラ事業者等のPDCAサイクルとの整合に基づく本項の施策見直しを課題とする。

２　情報共有体制の強化

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- ✓ 「情報共有体制の強化」により期待される成果は、関係主体間で共有する情報についての整理がなされ、情報提供、情報連絡等に必要な環境整備等が進展し、各セプター、セプターカウンシルの自主的な活動が充実強化された結果として、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である。
- ✓ そのため、整備された情報共有体制と共有された情報の充実に着目した指標を設定する。
- ✓ 具体的な指標は、内閣官房が発信した情報件数、セプター等で共有された情報件数、共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数とする。

(1) 実施状況

重要インフラの情報セキュリティを取り巻く社会環境や技術環境の変化、複雑・巧妙化するサイバー攻撃等に応じた情報セキュリティ対策への反映を通じた重要インフラ全体の防護能力の維持・強化に資することを目的に、官民の各主体が協力する情報共有体制の維持・向上に取り組んだ。

具体的には、「共有すべき情報の整理」及び「情報提供、情報連絡の充実」として、2009年３月に「第２次行動計画の情報連絡・情報提供に関する実施細目」（以下「実施細目」という。）を改定し、以降、関係主体間における具体的な情報連絡・情報提供方法の一層の充実、共有すべき情報項目の定期的な評価を行いつつ、情報共有を行った。

なお、共有すべき情報の整理については、「ＩＴ障害の未然防止」、「ＩＴ障害の拡大防止・迅速な復旧」及び「ＩＴ障害の原因等の分析・検証」による再発防止の３つの観点から、政府機関、関係機関、重要インフラ所管省庁、重要インフラ事業者等の各関係主体に応じた共有すべき情報の抽出と整理を行った。

加えて、内閣官房、重要インフラ所管省庁、重要インフラ事業者等との間でセプター訓練を行った。

「セプターの強化」としては、情報通信分野においてケーブルテレビ業界が2012年12月に「ケーブルテレビCEPTOAR」を発足し、2013年４月に正式に活動を開始した。

「セプターカウンシル」の取組としては、全セプターから構成される幹事会を定期的に開催するとともに、情報共有活動の強化に向けた「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)」が創設され、情報共有活動の充実を図ってきた。また、東日本大震災ではセプターカウンシルで培われた人的ネットワークを活用し、回線負荷の少ないファイル形式での情報提供及びアクセス集中回避に向けたボランティアミラーサイトの利活用を推奨する等、多発するＩＴ障害や輻輳においても円滑な情報提供がなされた。

(2) 成果

第２次行動計画期間中において、実施細目に基づき、重要インフラ所管省庁を経由して重要インフラ事業者等から603件の情報連絡を、内閣官房から182件の情報提供をそれぞれ行うとともに（2014年３月末時点)、毎年行っているセプター訓練には延べ58セプターが参加した。

なお、ＩＴ障害発生時の連絡共有体制については、当該体制が有効に機能した結果として、図表１に示すとおり、件数が増加している状況にある。

図表１　情報連絡のうちサイバー攻撃に関するものの推移

サイバー攻撃に関する情報連絡	2009 年度	2010 年度	2011 年度	2012 年度	2013 年度
不正アクセス、DoS 攻撃	３件	４件	12 件	55 件	121 件
コンピュータウイルスへの感染	０件	１件	２件	６件	７件
その他の意図的要因（不審メール等）	０件	０件	１件	15 件	５件
合計	３件	５件	15 件	76 件	133 件

また、セプターカウンシルについては、「ケーブルテレビCEPTOAR」の活動開始に伴い、参加セプター数は13となった。

このことから、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター・セプター間における情報共有体制の整備及び重要インフラ事業者等における必要情報の享受・活用の実現において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(3) 課題

サイバー攻撃に係る情報連絡件数が増加傾向にある一方、大規模ＩＴ障害の発生に関する連絡はなく、重要インフラ所管省庁、情報セキュリティ関係省庁及び関係機関と内閣官房との間で情報連絡・情報提供が完結した。

また、情報共有体制の運用にて以下の課題が見受けられた。

・分野間における情報共有頻度に格差が生じつつあり、情報連絡の対象に該当するものの対象と認識されない情報がある。
・攻撃手法の複雑・巧妙化に伴い、定義する「脅威の類型」では十分な情報連絡に至らない場合が生じつつある。加えて現行の関係主体だけでは十分な連携に至らない可能性が生じつつある。

これらに鑑み、実効性のある情報共有体制の構築を目的とした情報共有頻度の格差を解消すること、「脅威の類型」を細分化すること、大規模ＩＴ障害対応時の情報共有体制を平時の体制の延長線上に構築すること、情報共有体制の更なる強化に向けた共有すべき情報項目の見直しをすること及び既存の関係主体とサイバー空間関連事業者や防災関係府省庁等の新たな関係主体との連携の在り方を整理することを課題とする。

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。

３　共通脅威分析

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- ✓ 「共通脅威分析」に期待される成果は、指針の継続的改善及び重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供することである。
- ✓ そのため、毎年度当初に、重要インフラ事業者等の必要性を勘案して策定する共通脅威分析の検討項目に対する年度末時点の達成度に着目した指標を設定する。
- ✓ 具体的な指標は、実施した検討項目件数、各検討結果の重要インフラ事業者等による評価とする。

(1) 実施状況

重要インフラ全体の防護能力の維持・強化に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った。

具体的には、各分野におけるＩＴ利用の進展に応じて、図表２に示すとおり、様々な視点でＩＴに係る技術、環境等を対象とした各分野共通に起こり得る脅威を把握するための分析を毎年度行った。

図表２　共通脅威分析の各年度の分析内容

2009 年度	重要インフラにおける共通脅威の分類（環境変化調査と共同実施） （重要インフラ分野共通のＩＴに関する技術、システム、環境等、広い範囲を対象として、脅威の候補を抽出し、「重要インフラ分野共通に起こり得る脅威とは何か」という視点で絞り込み、優先度付けによって分析対象を明確化）
2010 年度	重要インフラ分野におけるクラウドコンピューティング環境 （重要インフラにおけるクラウドの範囲、導入に際しての脅威と対応方策、導入の可能性と形態、諸外国との比較等を調査・分析）
2011 年度	重要システム等の堅ろう性 （制御システムを含む国内外のサイバー攻撃事例や対策動向等に着目した調査・分析を行い、堅ろう化手法を提示）
2012 年度	重要インフラ分野における同時多発型ＩＴ障害発生時の復旧対応について （外部依存性、特にシステムベンダのリソース集中の脅威に焦点をあてた課題とベストプラクティスの提示及び過去の相互依存性解析の再確認調査の実施）
2013 年度	次期行動計画策定のための今後の脅威候補対象（環境変化調査と共同実施） （クラウド、スマートフォン・タブレット端末、BYOD 及びリモートメンテナンスの４つのトピックに対する環境変化調査と、M2M、ビッグデータ、スマートコミュニティ等の将来の新たな社会インフラ構造変化を見据えた長期的な環境変化調査を実施）

「相互依存性解析の継続」については、第２次行動計画において共通脅威分析の中で継続的に取り組むこととされたことから、図表２のとおり2012年度に当該調査も行った。

「共通脅威分析の検討」については、共通脅威分析のテーマを各重要インフラ事業者等にとって優先度の高いものとするため、ＩＴ技術等に係る環境変化調査や東日本大震災からの「気付き」に基づくものを選定した。また、効果的な情報共有の実現に向け、重要インフラ事業者等、重要インフラ所管省庁、関係機関及び有識者が参加する検討会にてリスクコミュニケーションを図りながら分析を進めた。

(2) 成果

図表２に示すとおり、本施策にて実施の検討項目数は十分であると考えられる。

また、分野横断的演習の参加事業者等へのアンケートによると、各年度平均で80％以上の重要インフラ事業者等から、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の

評価を得た（2009年度：82％、2010年度：80％、2011年度：66％、2012年度：86％、2013年度：98％）。

このことに加え、本施策によって重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映したことから、重要インフラサービスの維持、復旧への活用への貢献において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(3) 課題

重要インフラ分野が有する重要システムにおいては、ＩＴ依存度、事業規模、運用体制、他分野との独立性等が分野において区々であることから、環境変化等により生じる新たな脅威が必ずしも全分野の共通脅威とはなり得ない。一方、新たな脅威が全分野の共通脅威ではない場合であっても、複数分野における脅威の影響の大きさから分析を必要とする場合があり得る。このことから、重要インフラ防護の維持・向上に資することを目的として、複数分野における脅威であってもその影響の大きさに応じて調査対象に加えることが必要である。

また、共通脅威分析は、時間的経過や環境変化の顕在化に応じて、その変化に潜む重要インフラに共通的な脅威等を詳細に分析することで効果性の高い結果が得られる。このことから、共通脅威分析の位置付けや実施頻度の見直しが必要である。

さらに、分析結果の指針反映に止まっている施策間の連携については、他施策が抽出した脅威等を本施策の検討項目に取り上げる等、施策間における成果の相互利活用についての検討が必要である。

これらの検討・見直しを課題とする。

４　分野横断的演習

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- ✓ 「分野横断的演習」に期待される成果は、重要インフラ事業者等のＩＴ障害発生時の早期復旧手順、事業継続計画の検証などに対する貢献である。演習で得られた知見を現実のＩＴ障害発生時の事業継続、早期復旧活動に効果的に活用できるものとするためには、より現実の状況に近い演習の実施が重要であり、それぞれの役割を担当する多くのプレイヤーの参加が望ましい。
- ✓ そのため、演習参加者の拡大と演習で得られた知見が、重要インフラ事業者等の取組みに貢献したかどうかに着目した指標を設定する。
- ✓ 具体的な指標は、演習の延べ参加者数と、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重要インフラ事業者等の数とする。

(1) 実施状況

重要インフラ分野におけるＩＴ依存度の進展及びＩＴを巡る様々な脅威の顕在化が見られる中、ＩＴ障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じた相互の連絡・連携における仕組みの検証はますます重要になっていることから、その機会の提供に取り組んだ。

内閣官房主催の分野横断的演習はこれら仕組みを検証する我が国唯一の取組であり、第１次行動計画期間中の2006年度より毎年行ってきた。具体的には、第２次行動計画期間において、相互依存性解析から得た各分野の依存度が高い電力・通信・水道の途絶想定に基づく影響の波及に係る検証を分野横断的演習の３か年計画として設定し、詳細は環境や参加者のニーズ等を踏まえ、各実施年度の検討会にて決定した。

2010年度以降、日常使用するインフラ環境の利用、柔軟な演習参加者の設定等、より効果的、実践的な演習とするために、参加事業者等による自職場演習を導入した。

2011年度は、2011年発災の東日本大震災の経験を踏まえた複合障害（電力・通信・水道・ガス）を想定した演習テーマとするとともに、希望する分野が独自で設定したシナリオを「サブシナリオ」として状況に付加し、分野固有の課題検証を可能とした。

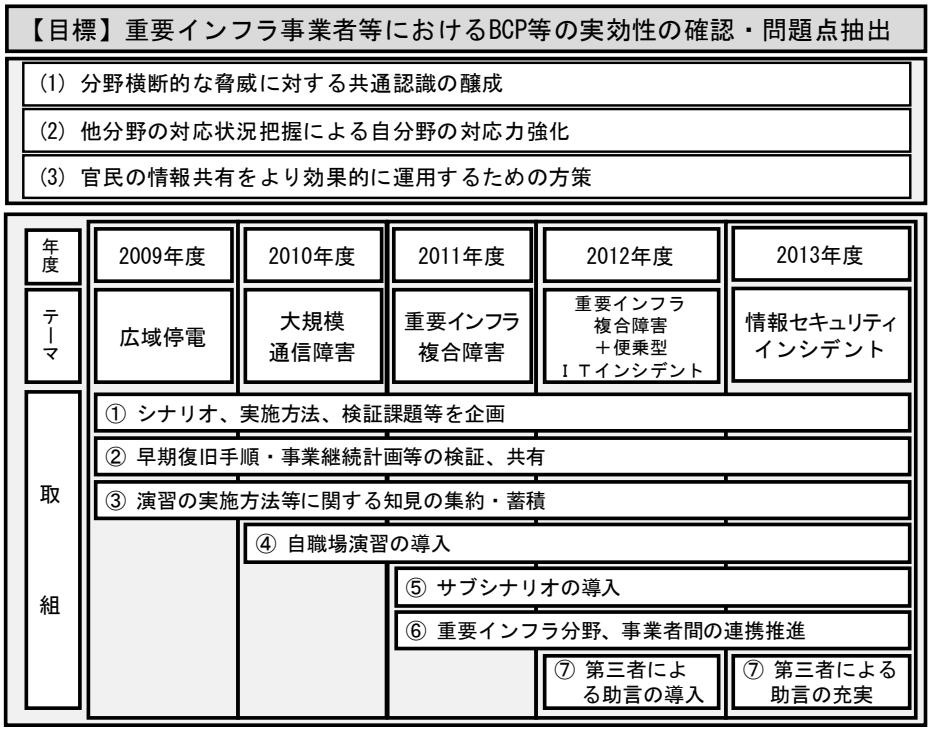
2012年度は複合障害の復旧段階への対応に加え、サイバー攻撃等近年の環境変化をテーマとするとともに、演習時のプレイヤー（参加事業者等）の判断・行動等への有識者等による助言制度を採用し、第三者視点に基づくＩＴ障害発生時の早期復旧手順及び事業継続計画等への検証における新たな気付きを提供し得る機会を提供した。

2013年度は政府機関や主要企業に対して頻発するサイバー攻撃等の現状や参加者からの要望を踏まえた情報セキュリティインシデントをそれぞれテーマとして設定した。

これら取組を図表３に示す。

なお、第２次行動計画以外にも、図表４に示すとおり、重要インフラ所管省庁においても個別の重要インフラ分野でのサイバー関連の対処能力向上を目指した演習・訓練を主催した。

図表３　第２次行動計画期間中の分野横断的演習の取組



図表４　重要インフラ所管省庁が主催する演習・訓練

省庁	名称	概要	対象者	実施期間	備考
総務省	電気通信事業分野におけるサイバー攻撃対応演習	サイバー攻撃等によるインターネットの機能不全に対応するために、複数の電気通信事業者等が参加し演習を行うことにより、高度なＩＴスキルを有する人材を育成し、電気通信事業者間の緊急対応体制を強化	電気通信事業者	2006 ～2008 年度	国の施策としては終了（テレコムアイザック推進会議にて継続中）
経済産業省	情報セキュリティ対策推進事業	制御システムに対するサイバー攻撃の脅威を認識し、セキュリティインシデント発生の検知手順・障害対応手順の妥当性について検証	2012 年度は、電力・ガス・ビル分野	2012 ～2016 年度	
	電力卸取引市場におけるサイバー演習	卸売電気業界における経済的損失を最小限にとどめるためのインシデントレスポンスに係る対応体制、連絡体制等の確認検証	電力卸売	2006 年度	机上演習終了済
国土交通省	重要インフラの情報セキュリティ対策に係る机上演習	高度化・煩雑化するＩＴ障害からの防御を目的とした重要インフラ分野におけるセキュリティ対策評価・検証、関係者の熟度及び対応能力の検証	物流分野（航空・鉄道）	2007 ～2009 年度	机上演習終了済

(2) 成果

ＩＴ障害発生時の事業継続・早期復旧活動において演習で得た知見を効果的に活用するためには、より現状に近い演習の実施が不可欠であり、前述の時宜に応じた演習テーマ設定やサブシナリオの導入等は現状に近づけた演習の実現に寄与したと考えられる。

また、各年度の演習参加規模や参加事業者等へのアンケートにて得た、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重要インフラ事業者等は図表５に示すとおり推移している。

図表５　各年度の演習参加規模及びアンケート回答結果

年度	演習参加規模	有意義と回答した参加事業者等の割合
2009 年度	30 組織、116 名	82%
2010 年度	38 組織、141 名	80%
2011 年度	37 組織、131 名	66%
2012 年度	42 組織、148 名	86%
2013 年度	61 組織、212 名	98%

官民あるいは他事業者等との情報連携が不可欠であるＩＴ障害発生時の早期復旧に向けて、より多くのプレイヤー参加が演習効果を高めることに資することから、上表のとおりプレイヤーである演習参加組織数・人数は増加傾向にあり、その効果も増していると考えられる。

このことから、演習で得られた知見に基づく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事業継続計画等の検証を通じた情報セキュリティ対策への貢献において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(3) 課題

区々である各組織のＩＴ利用形態・情報管理態勢に対応し得る演習環境の設定は大規模化するほど困難であり、大幅な参加者拡大が望めない中、結果として演習成果を直接享受できるのは重要インフラ事業者等の一部に限定されている。このことから重要インフラ事業者等における情報セキュリティ対策の課題抽出機会の提供を目的として、参加者の拡大に依存することなく、重要インフラ分野全体に演習成果の更なる普及・浸透を図ることが必要である。

また、演習の評価に基づいて、次年度演習のテーマ設定、運営改善、他施策へ展開する等、演習運営の質的な改善を目指すことが必要である。

さらには、重要インフラのＩＴ障害発生時の対応には、重要システムを構成する製品、プラットフォーム等の提供サービス、重要システムを支える技術等の提供者の協力を要する可能性を踏まえ、演習における関係主体の在り方を改めて検討することが必要である。

なお、重要インフラ所管省庁が独自に主催する重要インフラ事業者等を対象とする演習・訓練に加え、防災関係省庁が主催するＩＴに係る物理的障害発生を想定した政府機関内での対処を検証する訓練も実施されていることから、各機関との連携について検討することを要する。

これらの検討・見直しを課題とする。

５　環境変化への対応

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- ✓ 「環境変化への対応」に挙げた施策のうち、「広報公聴活動」に期待される成果は、行動計画の枠組みついて広く国民の理解を得ることと、第２次行動計画への協力者を関係主体以外にも拡大することである。
- ✓ そのため、第２次行動計画の周知機会の充実に着目した指標を設定する。
- ✓ 具体的な指標は、Webサイトのコンテンツの充実度、行動計画を紹介したセミナー等の回数とする。
- ✓ 「環境変化への対応」に挙げた施策のうち、「リスクコミュニケーション」に期待される成果は、関係主体間で互いの活動への理解の向上と、連携を図りやすい環境の醸成である。
- ✓ そのため、関係主体間のコミュニケーション機会の充実に着目した指標を設定する。
- ✓ 具体的な指標は、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コミュニケーションの機会の開催回数とする。

(1) 実施状況

ア　広報公聴活動

国民に対する説明責任を果たすことを目的として広報公聴活動を行った。

具体的には、広報活動として、第２次行動計画に基づき行った重要インフラの情報セキュリティ施策の結果である、指針、環境変化調査及び共通脅威分析の調査報告書、分野横断的演習の成果展開資料、重要インフラ専門委員会の会議資料等について、内閣官房のWebサイトに掲載し、公表した。

公聴活動として、各種セミナーやフォーラム等の場を活用し、情報セキュリティ政策に係る講演等を四半期に１回程度の頻度で行った。加えて、国内外の情報セキュリティに関する情報を「NISC重要インフラニュースレター」として関係省庁や重要インフラ事業者等に月に２件程度の頻度でメール配信を行った。

また、指針の改定に際しては、Webサイトにてパブリックコメントにより意見聴取を行った。

イ　リスクコミュニケーションの充実

リスクや情報セキュリティ対策の方法に係る認識の共有及び情報セキュリティ対策の連携効果の向上を目的として、関係機関等との意見交換を行った。

具体的には、内閣官房は情報セキュリティに係る関係機関との意見交換会を四半期ごとに開催し、情報セキュリティに係る取組や共通脅威等に係る意見交換を行った。また、セプターカウンシルにおいては、2010年６月に情報共有活動の推進を目的とした相互理解ＷＧを設置し、各重要インフラ事業分野が有する重要システムの利用現場や施設等の見学・紹介を行った。

さらに、2009年度から2010年度までにかけて関係主体間にて行うリスクコミュニケーションのテーマの提供を目的として、環境変化に伴う脅威についての調査・抽出をした上で、以下の詳細調査を行った。

・サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化
・情報システムのサプライチェーンにおける情報セキュリティ
・スマートグリッドの普及とその重要インフラの情報セキュリティにもたらす影響
・制御システムのオープン化が重要インフラの情報セキュリティに与える影響
・東日本大震災における重要インフラの情報システムに係る対応状況等
・重要インフラ分野におけるＩＴ依存度調査（水道分野及び医療分野）
・期行動計画の策定に向けた重要インフラ分野におけるＩＴ環境変化及び実態の調査

これらの調査結果については、セプターカウンシルへの情報共有やリスクコミュニケーシ

ョンの充実に活用した。

ウ　国際連携の推進

国際会合への参加や他国機関等との連携を通じて重要インフラ防護のためのベストプラクティス等に係る最新動向の把握・情報共有を行った。

具体的には、重要インフラ政策に携わる政府機関が相互連携について検討を行うメリディアン会合に毎年参加し、日本の情報セキュリティ政策等を紹介するとともに、欧米やアジア各国の重要インフラ防護担当者との意見交換を通じて、情報セキュリティ政策の国際的な動向に係る情報収集を行った。

また、2010年９月及び2013年３月に開催された世界的規模のサイバー演習であるサイバーストームにIWWN(International Watch and Warning Network)の一員として参加し、重要インフラ分野における国際的な連携を深めた。

さらに、「NISC重要インフラニュースレター」等による海外の関連動向や情報セキュリティ上の脅威に係る情報提供及びセプターカウンシル等における各国動向等についての情報共有を行った。

(2) 成果

ア　広報公聴活動

重要インフラの情報セキュリティ施策の結果、重要インフラ専門委員会の会議資料等については速やかに掲載を行った。

また、情報セキュリティ政策に係る講演等については、第２次行動計画期間において、25回行った（2009年度：６回、2010年度：６回、2011年度：５回、2012年度：４回、2013年度：４回)。さらに、「NISC重要インフラニュースレター」については113件を配信した。

加えて、2010年度及び2012年度に行った指針改定に際し、改定の都度、パブリックコメントによる意見聴取を行った。

このことから、充実したコンテンツの提供を通じて第２次行動計画の枠組み等に係る広報公聴活動について一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

イ　リスクコミュニケーションの充実

関係機関との意見交換会については、各年度とも四半期ごとに開催するとともに、重要インフラ事業者等とのリスクコミュニケーションとして、共通脅威分析及び分野横断的演習の検討会を計25回開催した（2009年度：５回、2010年度：５回、2011年度：５回、2012年度：５回、2013年度：５回)。

また、相互理解ＷＧを計18回開催した。

環境変化の変化に伴う情報共有等への調査結果の活用も含め、このことから、官と民、民と民における双方向のリスクコミュニケーションの促進、重要インフラ事業者等間の直接的なコミュニケーション機会の拡大、信頼関係の強化、環境変化に伴う脅威の察知能力の向上を通じて、リスクや情報セキュリティ対策の方法に係る認識の共有及び情報セキュリティ対策の連携効果の向上に向けて一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

ウ　国際連携の推進

メリディアン会合への参加にて情報セキュリティ対策に係るベストプラクティスの共有を図るとともに、サイバーストームへの参加にて共同演習等の国際的な連携を図る等、重要インフラ防護に係る国際的な取組に参画していくことで、諸外国との連携が実現できた。

このことから、重要インフラ防護のためのベストプラクティスに係る最新動向の把握・情報共有について一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定

の成果を挙げたと評価できる。

(3) 課題

ア　広報公聴活動

これまでの取組は、主に重要インフラ事業者等を対象としており、国民に対する冷静な対応を取る上で必要な情報の提供と理解促進に資する情報公開には及んでいない。一方、第２次行動計画に基づく取組の多くが国民の理解・活用に直結した内容ではない。

これらに鑑み、次期行動計画における本施策と他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しを課題とする。

イ　リスクコミュニケーションの充実

リスクコミュニケーションにおける有用な情報には機微情報を含み、開示制約から参加者を限定せざるを得ない状況にある。また、リスクコミュニケーションの前提となるリスクマネジメントの定義については、国際標準との整合をとることに留意する必要がある。

これに鑑み、機微情報の秘匿と情報の有用性の相反性を踏まえつつ、より多くの関係主体による情報共有・連携の実現に向けた情報の共有範囲の確認や共有手段の多様化等の見直しを課題とする。

また、ビッグデータ、M2M、スマートコミュニティ等の新たなＩＴ技術革新については中長期的な実現･利用が見込まれる状況にあり、新たなＩＴ技術革新に付随する脅威については、重要インフラサービスに大きな影響を与えることが予想される。

これに鑑み、将来的な脅威の影響の大きさが予想される環境変化のテーマについては、中長期的に継続した調査の実施に係る検討を課題とする。

ウ　国際連携の推進

サイバー空間は国境を越えてグローバルに形成されており、サイバー空間に存在するリスクについては深刻化・グローバル化している。

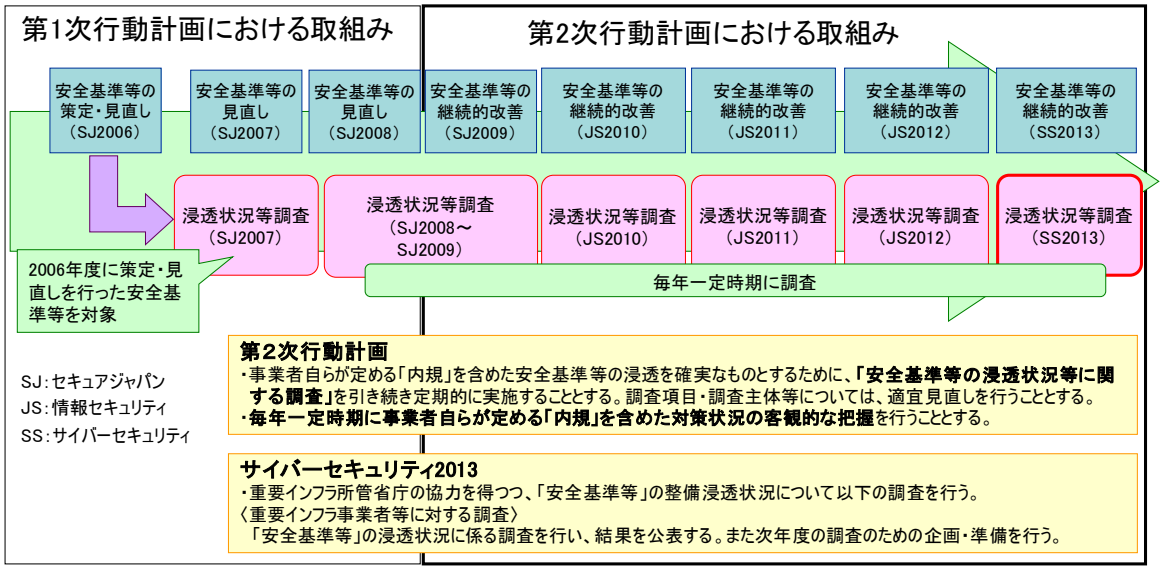
これに鑑み、求められるリスクへの迅速な対応に向けて、引き続き諸外国との連携を推進するとともに、国際的な枠組みに限定せず、ASEAN等のアジア太平洋地域や欧米等の二国間、多国間、地域的枠組みの積極的な活用を通じた国際連携の強化を課題とする。

別添４－２　安全基準等の浸透状況等に関する調査

「2013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」（重要インフラ専門委員会第34回会合（平成25年11月29日）資料３）より

「安全基準等の浸透状況等に関する調査」の概要（1/2）

「重要インフラの情報セキュリティに係る第２次行動計画」及び「サイバーセキュリティ2013」に基づき、各重要インフラ分野における安全基準等について、重要インフラ事業者等にどの程度浸透しているか、また重要インフラ事業者等が安全基準等に対して準拠しているかを把握するために、**毎年一定時期（定点）に**行う調査。
　安全基準等は随時見直しがなされるものであり、また着実にその浸透を図るべきものであることから、定期的な本調査を通じて継続的に浸透状況等を把握し、施策の成果検証に活用する。



「安全基準等の浸透状況等に関する調査」の概要（2/2）

◆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	：	以下方法のいずれかを重要インフラ所管省庁が選択 ①重要インフラ分野が独自で行う調査を活用し、NISCが提供する調査項目に読替え ②NISCが提供する調査資料を活用
調査基準日	：	2013年3月末日（「①独自調査を活用」する場合は、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担当（発出・回収方法は重要インフラ所管省庁が決定）
分野毎の集計	：	集計担当については、以下のいずれかを重要インフラ所管省庁が選択 ① 重要インフラ所管省庁にて集計 ② NISCにて集計
全体集計・とりまとめ	：	NISCにて集計・とりまとめ

◆実施時期（NISC提供の調査資料活用の場合）
調査期間　：　2013年4月～2013年9月（再調査期間を含む）
とりまとめ　：　2013年10月～2013年11月

◆主な調査内容（NISC提供の調査項目）
①安全基準等の整備状況に係る事項
　指針・対策編の認知に係る状況及び手段
　内規策定・見直しの契機及び参考とする安全基準等の諸規格
②情報セキュリティ対策状況に係る事項
　組織・体制及び資源の確保に係る対策状況
　情報保護に係る対策状況
③安全基準等への準拠状況に係る事項
　自己点検、演習、訓練等に係る実施状況
④情報セキュリティ対策に係る提言、要望等

調査結果　アンケート回収状況と留意点

- **調査への協力を求めた3,356事業者等に対し、3,160事業者等からアンケートを回収　（回収率：94.1%　前年比：+0.9%）**
- **全体集計においては、分野に共通の重み付け（正規化）をした上で実施**

分野		既存調査活用	アンケート回収状況　＊カッコ内は昨年度の数値		
			調査対象範囲	配布数	回収数
情報通信	電気通信	しない	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	76 (79)	20 (28)
	ｹｰﾌﾞﾙﾃﾚﾋﾞ	しない	ケーブルテレビセプター参加事業者	241 (---)	221 (---)
	放送	しない	日本放送協会及び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）	194 (193)	194 (184)
金融		する	金融機関等	892 (921)	796 (789)
航空	航空運送	しない	航空運送事業者	2 (2)	2 (2)
	航空管制	しない	官庁	1 (1)	1 (1)
鉄道		しない	鉄道事業者22社	22 (22)	22 (22)
電力		しない	一般電気事業者、日本原電(株)、電源開発(株)	12 (12)	12 (12)
ガス		しない	政令指定都市8社、同等の事業者2社	10 (10)	10 (10)
政府・行政ｻｰﾋﾞｽ		する	地方公共団体	1,789 (1,784)	1,789 (1,784)
医療		しない	医療機関（病院抽出）	50 (50)	38 (43)
水道		しない	水道事業体（事業者抽出）	45 (45)	45 (45)
物流		しない	物流事業者及び業界団体	22 (21)	10 (9)
全分野合計				**3,356 (3,140)**	**3,160 (2,928)**

留意点

留意点1：類似調査との重複回避
⇒既存調査の活用にて調査運営を効率化

留意点2：調査対象の範囲
⇒調査可能な範囲から取組み。調査対象の拡大は追って検討（範囲は重要インフラ所管省庁が決定）
（第23回重要インフラ専門委員会資料より）

分野にて回収数が異なるため、分野に共通の重み付け（正規化）をした上で集計を実施

＜集計式＞

$$A=\frac{\left(a_1/\alpha_1\right)+\left(a_2/\alpha_2\right)+\cdots+\left(a_n/\alpha_n\right)}{n}$$

A：回答Ａに対する全体集計（%）
a_n：分野ｎにおける回答Ａの数
α_n：分野ｎにおける回収数

※安全基準等の範囲にあわせて、情報通信を3つ、航空を2つに分けて集計するため、原則 n=13
（既存調査を活用する場合に読み替え可能な項目がない場合を除く）

＜参考＞既存調査と浸透状況等調査の関係整理（2013年度実績）

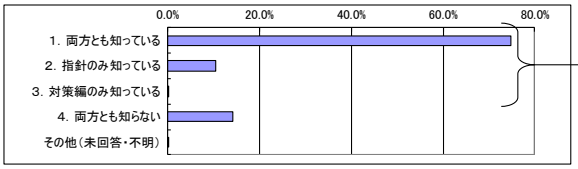
分野		既存調査				浸透状況等調査		
		有無	名称	調査基準日	調査周期	既存調査活用	調査対象範囲 ※既存調査活用する場合は、既存調査の範囲・数	ｱﾝｹｰﾄ配布数
情報通信	電気通信	なし				しない	固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等	76
	ケーブルテレビ	なし				しない	ケーブルテレビセプター参加事業者	241
	放送	なし				しない	日本放送協会及び地上系民間基幹放送事業者（多重単営社及びｺﾐｭﾆﾃｨ放送事業者を除く）	194
金融		あり	金融機関等のコンピュータシステムに関する安全対策実施状況調査書	3月31日	1年毎	する	金融機関等	892
航空	航空運送	なし				しない	航空運送事業者	2
	航空管制	なし				しない	官庁	1
鉄道		なし				しない	鉄道事業者22社	22
電力		なし				しない	一般電気事業者、日本原電(株)、電源開発(株)	12
ガス		なし				しない	政令指定都市8社、同等の事業者2社	10
政府・行政サービス		あり	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	する	地方公共団体	1,789
医療		なし				しない	医療機関（病院抽出）	50
水道		なし				しない	水道事業体（事業者抽出）	45
物流		なし				しない	物流事業者及び業界団体	22

※既存調査の活用項目は、主な調査内容の①安全基準等の整備状況に係る事項、②情報セキュリティ対策状況に係る事項、③安全基準等への準拠状況に係る事項、が対象

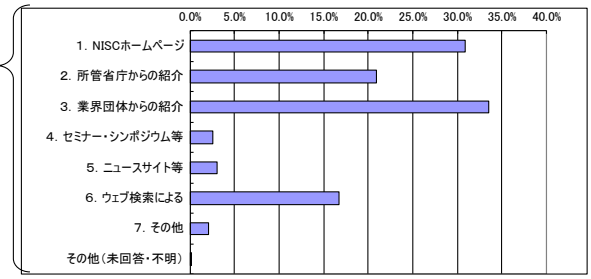
調査結果　①安全基準等の整備の状況に関する事項

- **指針について、認知している事業者等は8割強であると推定。**
- **指針・対策編を認知している事業者のうち、それらを知った手段は、業界団体からの紹介が一番多く、NISCホームページ、所管省庁からの紹介が続く。**

(1)指針・対策編の認知度
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



(2)指針・対策編を知った手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

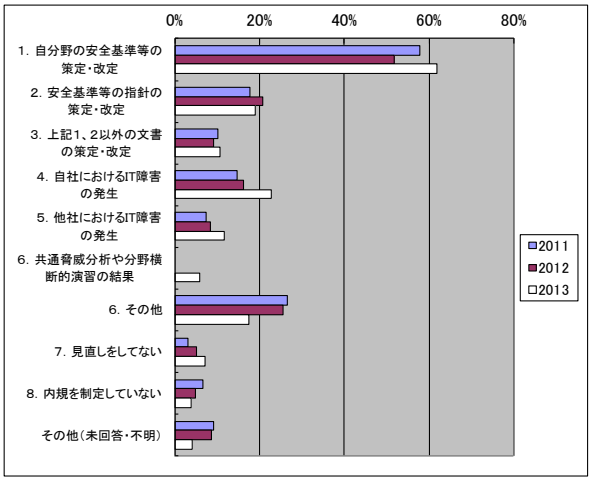


3)効果的に周知する手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

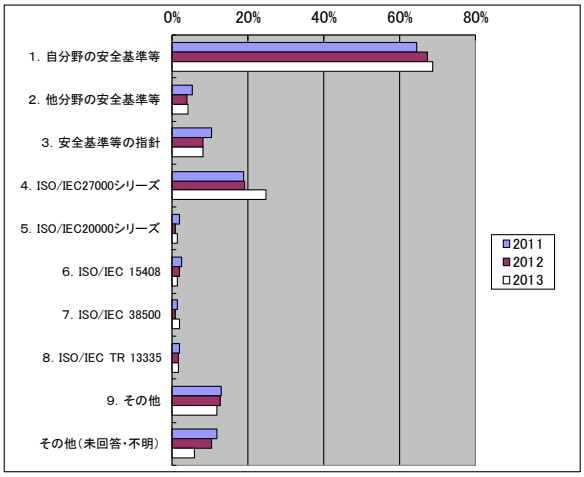
・業界団体からの定期的な紹介
・所管省庁からの情報提供
・担当者宛メール通知
・セミナーやシンポジウムの開催
・マスメディアを通じた広報

- **内規策定・見直しの契機としては、自分野の安全基準等が約6割を占める。**
- **参考とする安全基準、規格等も、自分野の安全基準等が約7割を占める。**

(1) 内規策定・見直しの契機

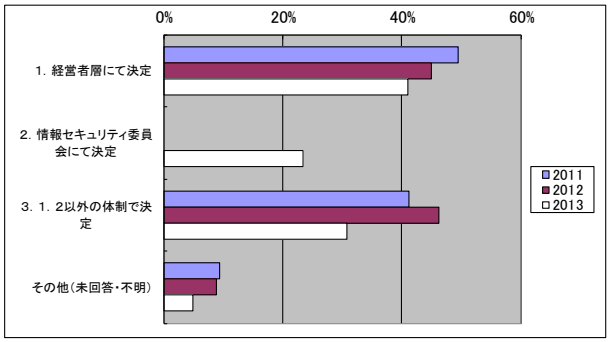


(2) 内規策定・見直しにあたり参考とする安全基準、規格等

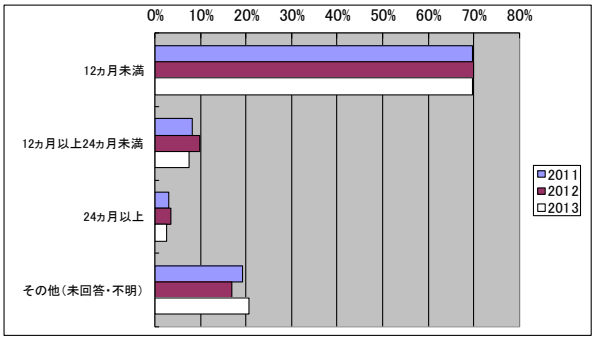


- **内規改定を行う際の体制は、経営者層での決定が減少し、経営者層以外の体制での決定が増加。**
  経営者層以外の体制での決定は、情報セキュリティ委員会によるものが大半。
- **内規の改定は、概ね1年未満で実施されている。**

(3) 内規改定を行う際の体制
項目2は2013年度に追加



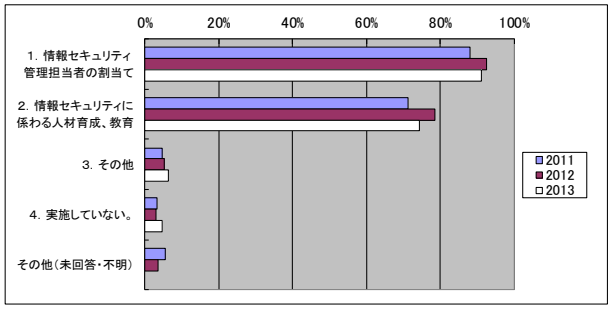
(4) 内規改定に要する期間
金融は読み替え可能項目なし（集計対象に含めず）



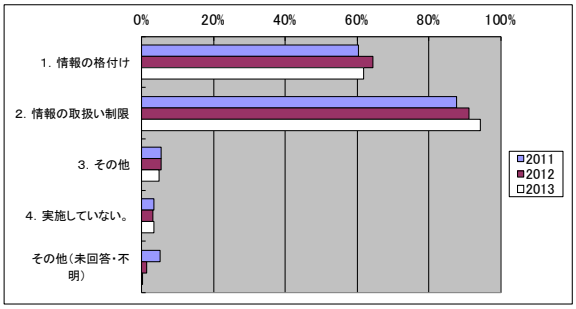
調査結果　②情報セキュリティ対策の実施状況に関する事項（1/2）

- **今回からケーブルセプターが新たに調査対象となった。**
- **経年変化（除、ケーブルセプター回答）については、(1)－(4)の各対策状況とも、ほぼ昨年度と同様の結果。**

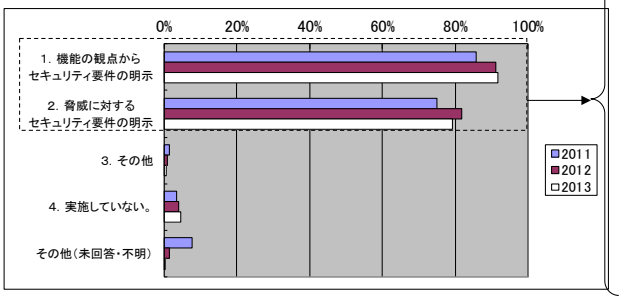
(1) 組織・体制及び資源の確保に関する対策



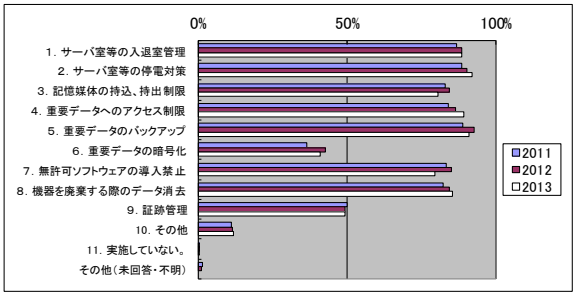
(2) 情報についての対策



(3) 情報セキュリティ要件の明確化
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

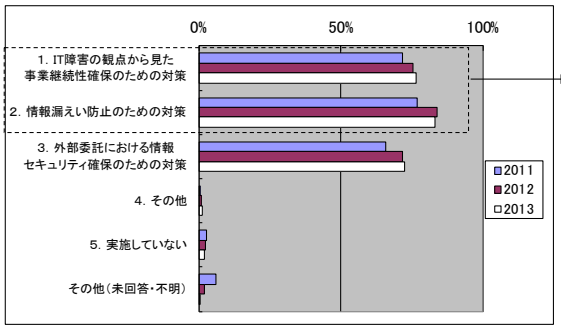


(4) 情報セキュリティ要件に対応した情報システムの対策

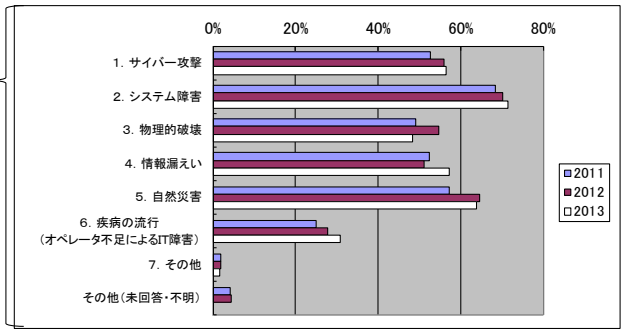


- **(5)－(6)の各対策状況とも、ほぼ昨年度と同様の結果。**
- **事業継続計画の策定状況については、策定予定なしが暫時減少傾向にあり、策定予定を含めて策定が進んでいる傾向にある。一方、策定済みであるものの定期的な見直しについては減少した。**

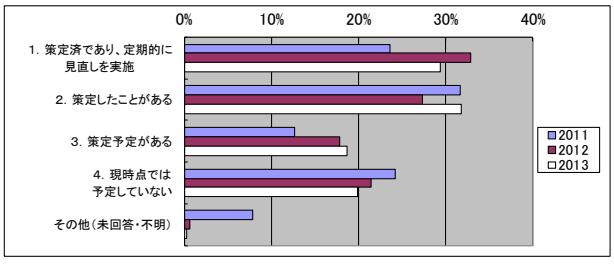
(5) 情報セキュリティ対策の運用に関する対策



(6)運用に関する情報セキュリティ対策において対象とする脅威



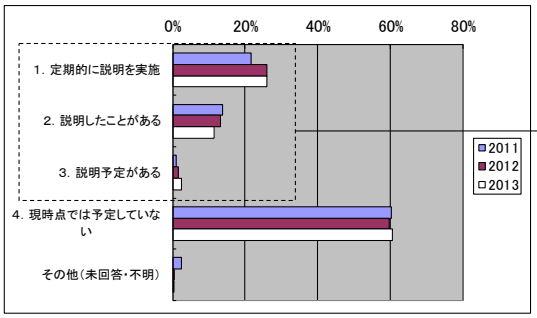
(7) 事業継続計画の策定状況



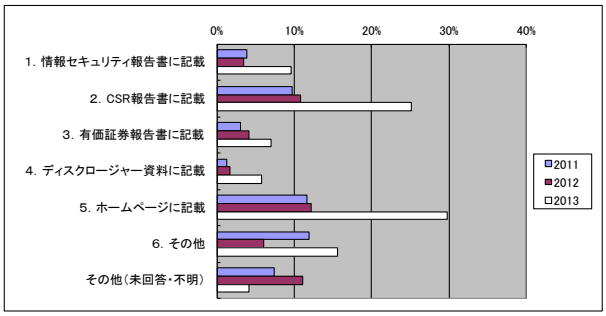
調査結果　②情報セキュリティ対策の実施状況に関する事項（2/2）

- **情報セキュリティ対策の対外的な説明を定期的に実施している事業者等は昨年度同様約3割。また、説明方法については、ホームページ、CSR報告書を用いている事業者等が多い。**
- **昨年度同様6割強の事業者等で、IT障害時の情報提供に関する方策を内規等に明示している。**

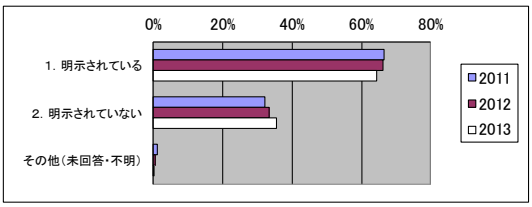
(8) 情報セキュリティ対策の対外的な説明の状況
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



(9) 情報セキュリティ対策の対外的な説明の方法
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）

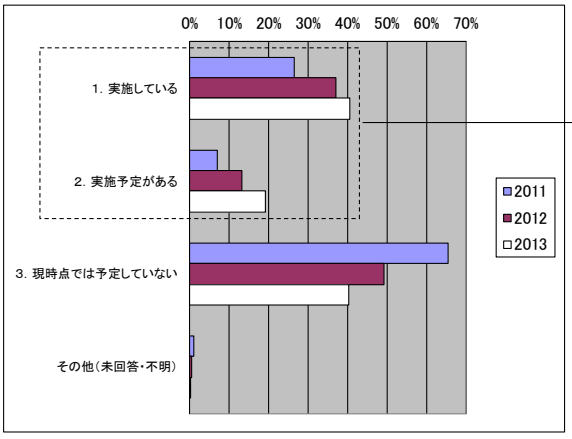


(10) IT障害時のユーザへの情報提供の方策
金融、政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）

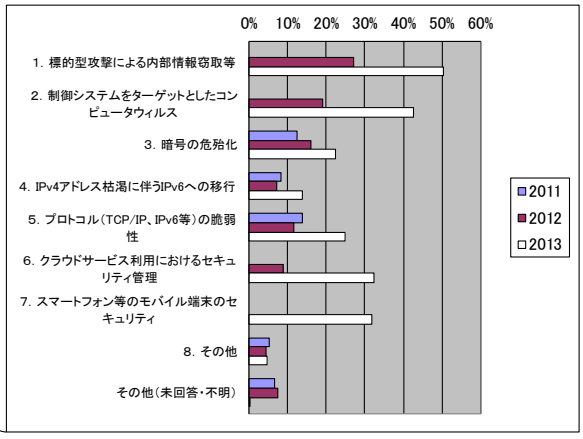


- **ITに係る環境変化に伴う脅威に対して、対策を実施、または予定している事業者等は昨年度同様、６割程度と推定。**
- **想定する脅威に関しては、標的型攻撃による内部情報窃取等、制御システムをターゲットとしたコンピュータウィルスが引き続き上位。続いてクラウドサービス利用におけるセキュリティ管理、スマートフォン等のモバイル端末のセキュリティといった新技術の脅威想定が伸長。**

(11) ITに係る環境変化に伴う脅威に対する対策
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）



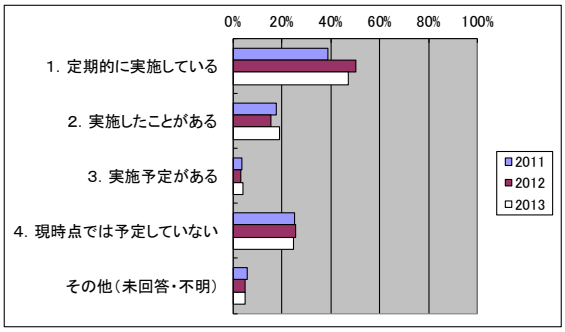
(12) 想定する脅威
政府・行政サービスは 読み替え可能項目なし（集計対象に含めず）
※項目1、2、6は2012年度に、7は2013年度に追加



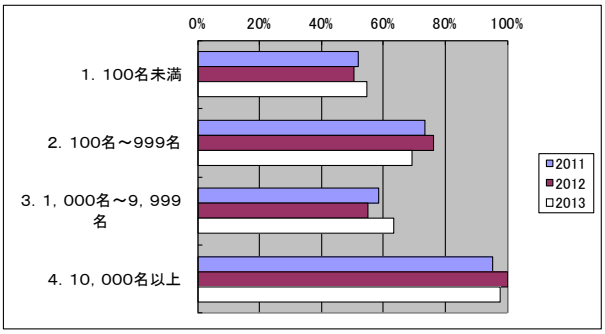
調査結果　③安全基準等に対する準拠状況に関する事項

・ 昨年度同様、自己点検を定期的に実施している事業者等が約5割、予定を含む実施割合が約7割と推定。

(1) 自己点検の実施

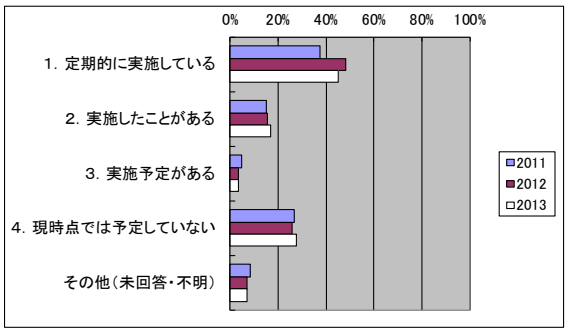


自己点検の事業規模ごとの実施割合（予定含む）

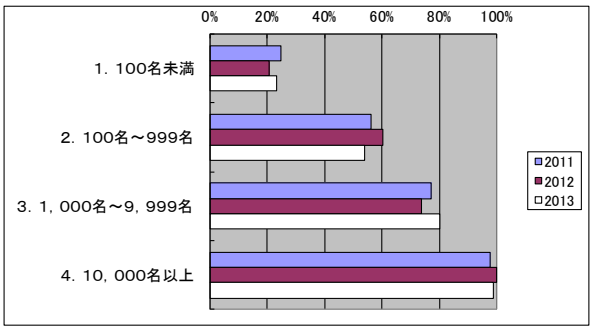


・ 演習・訓練の実施状況については、総じてほぼ昨年度水準。

(2)演習・訓練の実施

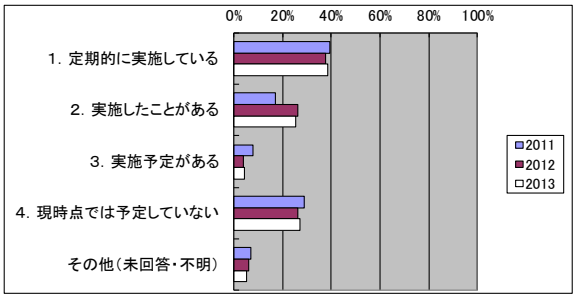


演習・訓練の事業規模ごとの実施割合（予定含む）

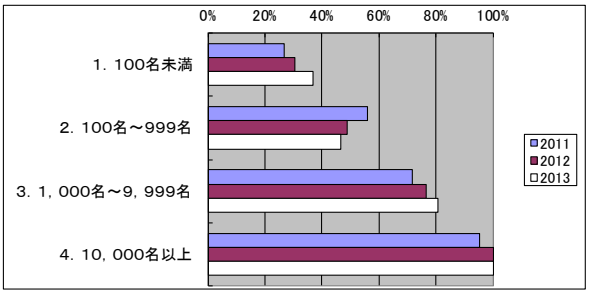


・ 内部監査の実施状況については、総じてほぼ昨年度水準。

(3) 内部監査の実施

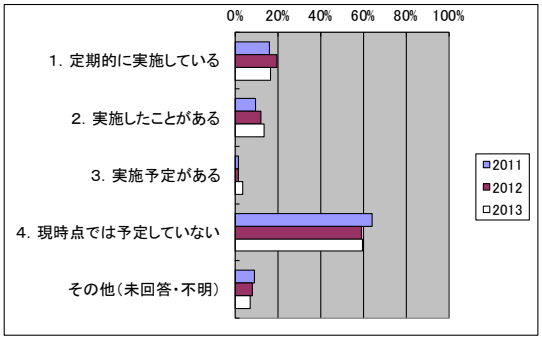


内部監査の事業規模ごとの実施割合（予定含む）

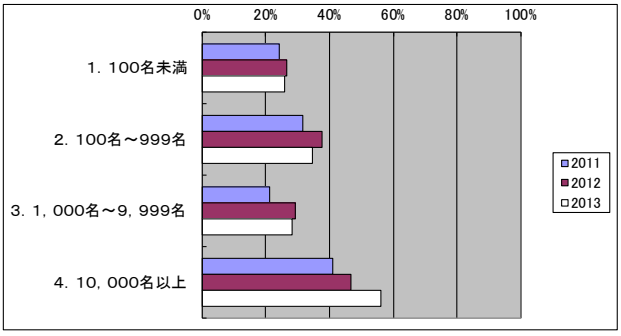


・ 外部監査の実施状況については、総じてほぼ昨年度水準。
・ 費用のかかる外部の監査機関の利用は大規模事業者では増加傾向だが、他事業者ではやや微減。

(4) 外部監査の実施
金融は読み替え可能項目なし（集計対象に含めず）



外部監査の事業規模ごとの実施割合（予定含む）



調査結果　④安全基準等への提言、要望等

・ 安全基準等の指針に対する意見としては、対策の段階化（最低限必要なレベル、望ましいレベル、理想レベル）等による企業規模に見合った指針化、取り組み易い具体策の提示等、より実効性を求める要望があった。

・ 安全基準等に対する意見としては、事例提供・分野内共通の留意点の提示・セミナー開催等の情報提供、事業者としての必要最低限の対応の担保に向けた法制化を視野に見直しを進めることの検討着手について意見があった。

1．安全基準等の指針に対して
① 最低限必要な対策、望ましい対策、理想とする対策など段階的な指針にするとわかりやすい
② 情報セキュリティ政策会議で策定している指針や対策編は参考になるが、次元がハイレベルのように感じる
③ 対策編で更なる具体的な内容を示してほしい
④ チェックシートなどがあるとさらに有意義になるのではないか

2．安全基準等に対して
① ガイドライン適用の参考としたく、出来るだけ多くの事例を提供いただきたい
② 内規案があるとより理解、対策が可能となる
③ 一般論ではなく、規模・コスト別の対策例を提示いただきたい
④ 必要最低限にすべき。過度に基準を設定しても、実行できなければ意味を呈さない
⑤ 安全基準等は参考するも、見直しが追いついていないように感じる。ITが専門ではない事業分野においては、対策を最新に保つのが難しいので、事業分野に共通する留意点を専門的な立場から提示して頂きたい
⑥ 日々発見される脅威への対応が充分なのか不安な面が多々ある。多くの安全基準等のセミナー開催を希望
⑦ 営利企業においては、情報セキュリティの重要性は理解できても、それに要するコストは常にメリットとの見合い。その意味で政府等が示すガイドラインは、強制力がなく、状況に応じた事業者判断を可能としている形態は適切と考えられる。
一方で昨今の情報セキュリティを巡る情勢から、各事業者が足並みをそろえた対応すべき点も生じることが想定される。事業者の必要最低限な対応の担保に向け、法制化も視野に対策見直しを進めることも要検討だと考えられる

※金融、政府・行政サービスは、調査対象外

・ 自由意見としては、IT人材育成支援・情報セキュリティ相談窓口、セキュリティ対策費用の助成等の支援、政府レベルでのOS不具合・ウイルスソフト等の情報公開・対策、セキュリティ対策の一定水準の義務付け、サイバーテロ等に対する取り締まりと法的措置の強化といった意見があった。

3．その他（自由意見を記載）
① IT人材育成のための支援を重視して頂きたい
② 情報セキュリティの相談窓口の設置をお願いしたい
③ 対策実施には多額の設備投資を要する箇所もある。支援して頂けるような枠組みがあれば助かる
④ 情報セキュリティに関して、一定の水準を保つよう義務付けるとともに、セキュリティ費用等における助成の検討をお願いしたい
⑤ セキュリティ全般に対するOSの不具合、ウイルスソフト等を政府として迅速に公開してほしい
⑥ 現在、コンピュータウイルスの対策はソフトウエア業界任せであり、真の脅威に積極的に取り組んでいるとは言い難いとの思いがある。真の脅威を未然に防ぐためにも国の研究機関等が、重要なコンピュータウイルス対策を行うべきではないか
⑦ サイバーテロ、不正アクセス、ウイルス散布、スパムメール等に対する取り締まりと法的措置の強化を実施して頂きたい

※金融、政府・行政サービスは、調査対象外

まとめ

・ 重要インフラ事業者等における情報セキュリティ対策の実施状況を分野横断的に把握

- 回答選択の傾向は総じて昨年とほぼ同様であった。また、回収率は94．1%（対前年度＋0．9%）であった。
- 想定する脅威として、「クラウドサービス利用におけるセキュリティ管理」、「スマートフォン等のモバイル端末のセキュリティ」といった環境変化を挙げる事業者が増加している。
- 一部項目において見られた対策状況の率の減少（対前年比）については回答者の追加・入替え等に起因するものであり、追加・入替え等を除く対策状況については横ばいから微増であった。
  このことから、現調査対象範囲における安全基準等の対策状況は、対策途上期から成熟期に移行しつつあることが推定される。

≪さらなる情報セキュリティ対策の拡充に向けて≫

- 環境変化、とりわけ新技術に係る重要インフラ事業者等によるリスク分析への支援について検討を要する。
- 現調査対象範囲からの対象拡張及び具体的な対策状況確認を通じて、本調査結果（特に課題）を国の施策にフィードバックする機能の実現に向けた検討を要する。

- 今後の重要インフラ事業者等における情報セキュリティ対策の実施状況の把握については、本調査による以下の実現を目指し、一部調査運営を見直した上で継続して実施する。

  ✓ 調査対象範囲の拡張にて、より広範な重要インフラ全体の状況確認
  ✓ より具体的な対策状況の確認を通じたより深化した課題抽出
  ✓ 成熟期への移行推定に基づく率の減少（対策退化傾向）の検知

＜参考＞　アンケート項目

・ 以下のアンケート項目にて調査を実施（「NISCアンケート項目に準じて実施」の場合）
・「既存調査を活用」する場合は、全体集計に際して、可能な範囲でアンケート項目との読み替えを実施

【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。

【① 安全基準等の整備の状況に関する事項】
（1） 指針及び対策編をご存知ですか。
（2） 指針及び対策編を何で知りましたか。
（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。
（4） 内規の策定・見直しの契機を以下からお知らせ下さい。
（5） 参考とする安全基準等や諸規格をお知らせ下さい。
（6） 内規改定を行う際の体制をお知らせ下さい。
（7） 内規改定に要する大体の期間をお知らせ下さい。

【② 情報セキュリティ対策の実施状況に関する事項】
（1） 組織・体制及び資源の確保に関する対策を実施していますか。
（2） 情報についての対策を実施していますか。
（3） 情報セキュリティ要件の明確化を実施していますか。
（4） 明確化した情報セキュリティ要件に対応した情報システムの対策を実施していますか。
（5） 情報セキュリティ対策の運用に関する対策を実施していますか。
（6） 事業継続計画の策定状況をお知らせ下さい。
（7） 事業継続計画の対象とする脅威をお知らせ下さい。
（8） 貴社（又は貴団体）における情報セキュリティ対策の対外的な説明状況をお知らせ下さい。
（9） 情報セキュリティ対策の対外的な説明の方法をお知らせ下さい。
（10）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、復旧等の情報提供の方策が明示されていますか。
（11）環境変化に伴う脅威に対する対策を実施していますか。
（12）対象とする脅威をお知らせ下さい。

【③ 安全基準等に対する準拠状況に関する事項】
（1） 安全基準等や貴社（又は貴団体）の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っていますか（予定を含む）。
（2） IT障害発生を想定した演習、訓練等を実施していますか（予定を含む）。
（3） 情報セキュリティ対策の実施状況に関する内部監査を実施していますか（予定を含む）。
（4） 情報セキュリティ対策の実施状況に関する外部監査を実施していますか（予定を含む）。

【④ 政府への提言、要望等】
（1） 安全基準等の指針に対して（自由意見を記載）
（2） 安全基準等に対して（自由意見を記載）
（3） その他（自由意見を記載）

（参考）安全基準等の浸透状況等に関する調査：数値データ

①安全基準等の整備の状況に関する事項

指針・対策編の認知度
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2013
両方とも知っている	74.9%
指針のみ知っている	10.6%
対策編のみ知っている	0.2%
両方とも知らない	14.3%
その他（未回答・不明）	0.0%

指針・対策編を知った手段
金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2013
NISCホームページ	30.8%
所管省庁からの紹介	20.9%
業界団体からの紹介	33.5%
セミナー・シンポジウム等	2.5%
ニュースサイト等	3.1%
ウェブ検索による	16.8%
その他	2.1%
その他（未回答・不明）	0.1%

内規策定・見直しの契機

（年度）	2011	2012	2013
自分野の安全基準等の策定・改定	57.7%	51.9%	61.7%
安全基準等の指針の策定・改定	17.7%	20.8%	19.0%
上記以外の文書の策定・改定	10.2%	9.2%	10.8%
自社におけるIT障害の発生	14.8%	16.1%	22.8%
他社におけるIT障害の発生	7.3%	8.4%	11.6%
共通脅威分析や分野横断的演習の結果	－	－	6.0%
その他	26.5%	25.6%	17.5%
見直しをしてない	3.2%	5.2%	7.0%
内規を制定していない	6.7%	4.8%	3.8%
その他（未回答・不明）	9.1%	8.6%	4.2%

内規策定・見直しにあたり参考とする安全基準、規格等

（年度）	2011	2012	2013
自分野の安全基準等	64.3%	67.3%	68.6%
他分野の安全基準等	5.3%	4.0%	4.2%
安全基準等の指針	10.2%	8.0%	8.1%
ISO/IEC27000シリーズ	18.6%	19.1%	24.6%
ISO/IEC20000シリーズ	2.0%	0.8%	1.2%
ISO/IEC 15408	2.3%	2.0%	1.4%
ISO/IEC 38500	1.2%	0.9%	1.9%
ISO/IEC TR 13335	2.0%	1.5%	1.5%
その他	12.8%	12.6%	11.7%
その他（未回答・不明）	11.7%	10.2%	5.8%

内規改定を行う際の体制

（年度）	2011	2012	2013
経営者層にて決定	49.4%	44.9%	41.0%
情報セキュリティ委員会にて決定	－	－	23.4%
上記以外の体制で決定	41.2%	46.2%	30.8%
その他（未回答・不明）	9.4%	8.9%	4.8%

内規改定に要する期間
金融は読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
12ヵ月未満	69.7%	69.9%	69.7%
12ヵ月以上24ヵ月未満	8.3%	9.7%	7.4%
24ヵ月以上	2.9%	3.5%	2.4%
その他（未回答・不明）	19.1%	16.8%	20.5%

②情報セキュリティ対策の実施状況に関する事項

組織・体制及び資源の確保に関する対策

（年度）	2011	2012	2013
情報セキュリティ管理担当者の割当て	88.2%	92.7%	91.3%
情報セキュリティに係わる人材育成、教育	71.4%	78.4%	74.5%
その他	4.8%	5.2%	6.3%
実施していない。	3.3%	2.9%	4.8%
その他（未回答・不明）	5.5%	3.5%	0.0%

情報についての対策

（年度）	2011	2012	2013
情報の格付け	60.4%	64.3%	61.9%
情報の取扱い制限	87.8%	91.3%	94.3%
その他	5.4%	5.4%	4.9%
実施していない。	3.4%	3.2%	3.3%
その他（未回答・不明）	5.1%	1.4%	0.1%

情報セキュリティ要件の明確化

政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
機能の観点からセキュリティ要件の明示	85.6%	91.1%	91.7%
脅威に対するセキュリティ要件の明示	75.1%	81.7%	79.3%
その他	1.4%	1.0%	0.5%
実施していない。	3.4%	3.9%	4.5%
その他（未回答・不明）	7.8%	1.6%	0.1%

情報セキュリティ要件に対応した情報システムの対策

（年度）	2011	2012	2013
サーバ室等の入退室管理	86.8%	88.3%	88.3%
サーバ室等の停電対策	88.5%	90.2%	92.0%
記憶媒体の持込、持出制限	82.9%	84.4%	80.4%
重要データへのアクセス制限	84.1%	86.2%	89.1%
重要データのバックアップ	88.9%	92.7%	90.7%
重要データの暗号化	36.4%	42.7%	41.0%
無許可ソフトウェアの導入禁止	83.2%	85.1%	79.6%
機器を廃棄する際のデータ消去	82.4%	84.2%	85.3%
証跡管理	50.0%	49.2%	49.4%
その他	11.4%	11.5%	11.9%
実施していない。	0.4%	0.3%	0.2%
その他（未回答・不明）	1.6%	1.3%	0.0%

情報セキュリティ対策の運用に関する対策

（年度）	2011	2012	2013
IT障害の観点から見た事業継続性確保のための対策	71.4%	75.2%	76.2%
情報漏えい防止のための対策	76.9%	83.9%	83.0%
外部委託における情報セキュリティ確保のための対策	65.5%	71.7%	72.4%
その他	0.4%	0.8%	1.2%
実施していない	2.9%	2.4%	1.9%
その他（未回答・不明）	6.1%	2.1%	0.0%

運用に関する情報セキュリティ対策において対象とする脅威

（年度）	2011	2012	2013
サイバー攻撃	52.6%	56.0%	56.6%
システム障害	68.4%	70.1%	71.4%
物理的破壊	49.2%	54.7%	48.5%
情報漏えい	52.5%	51.2%	57.2%
自然災害	57.3%	64.7%	63.9%
疾病の流行（オペレータ不足によるIT障害）	24.9%	27.8%	30.7%
その他	1.8%	1.9%	1.7%
その他（未回答・不明）	4.1%	4.3%	0.0%

事業継続計画の策定状況

（年度）	2011	2012	2013
策定済であり、定期的に見直しを実施	23.6%	32.8%	29.4%
策定したことがある	31.7%	27.3%	31.8%
策定予定がある	12.7%	17.8%	18.7%
現時点では予定していない	24.2%	21.4%	19.8%
その他（未回答・不明）	7.8%	0.6%	0.3%

情報セキュリティ対策の対外的な説明の状況

政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
定期的に説明を実施	21.6%	25.8%	25.9%
説明したことがある	13.9%	13.3%	11.3%
説明予定がある	0.9%	1.7%	2.3%
現時点では予定していない	60.2%	59.7%	60.4%
その他（未回答・不明）	2.4%	0.1%	0.0%

情報セキュリティ対策の対外的な説明の方法

金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
情報セキュリティ報告書に記載	3.8%	3.5%	9.6%
CSR報告書に記載	9.7%	10.8%	25.1%
有価証券報告書に記載	3.0%	4.2%	7.1%
ディスクロージャー資料に記載	1.3%	1.7%	5.8%
ホームページに記載	11.6%	12.2%	29.8%
その他	11.9%	6.0%	15.6%
その他（未回答・不明）	7.4%	11.0%	4.1%

IT障害時のユーザへの情報提供の方策

金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
明示されている	66.5%	66.4%	64.5%
明示されていない	32.3%	33.2%	35.5%
その他（未回答・不明）	1.2%	0.4%	0.0%

ITに係る環境変化に伴う脅威に対する対策
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
実施している	26.6%	37.1%	40.6%
実施予定がある	6.9%	13.1%	19.1%
現時点では予定していない	65.5%	49.3%	40.2%
その他（未回答・不明）	1.0%	0.5%	0.1%

想定する脅威
政府・行政サービスは読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
標的型攻撃による内部情報窃取等	－	27.0%	50.4%
制御システムをターゲットとしたコンピュータウィルス	－	19.2%	42.6%
暗号の危殆化	12.3%	15.9%	22.3%
IPv4アドレス枯渇に伴うIPv6への移行	8.2%	7.1%	13.7%
プロトコル（TCP/IP、IPv6等）の脆弱性	13.7%	11.5%	24.8%
クラウドサービス利用におけるセキュリティ管理	－	8.9%	32.4%
スマートフォン等のモバイル端末のセキュリティ	－	－	32.0%
その他	5.2%	4.4%	4.8%
その他（未回答・不明）	6.5%	7.5%	0.2%

③安全基準等に対する準拠状況に関する事項

自己点検の実施

（年度）	2011	2012	2013
定期的に実施している	39.0%	50.1%	47.1%
実施したことがある	17.6%	15.7%	19.3%
実施予定がある	3.8%	3.4%	4.1%
現時点では予定していない	25.3%	25.7%	24.6%
その他（未回答・不明）	6.0%	5.1%	4.9%

自己点検の事業規模ごとの実施割合（予定含む）

（年度）	2011	2012	2013
100名未満	51.8%	50.4%	54.7%
100名～999名	73.6%	76.3%	69.4%
1,000名～9,999名	58.6%	54.9%	63.4%
10,000名以上	95.4%	100%	97.8%

演習・訓練の実施

（年度）	2011	2012	2013
定期的に実施している	37.3%	47.9%	45.2%
実施したことがある	15.0%	15.6%	16.9%
実施予定がある	4.6%	3.6%	3.5%
現時点では予定していない	26.5%	25.8%	27.4%
その他（未回答・不明）	8.2%	7.1%	7.1%

演習・訓練の事業規模ごとの実施割合（予定含む）

（年度）	2011	2012	2013
100名未満	24.8%	20.6%	23.4%
100名～999名	56.2%	60.1%	53.8%
1,000名～9,999名	77.0%	73.7%	80.1%
10,000名以上	97.9%	100%	98.7%

内部監査の実施

（年度）	2011	2012	2013
定期的に実施している	39.3%	37.4%	38.6%
実施したことがある	17.1%	26.3%	25.1%
実施予定がある	8.0%	4.0%	4.3%
現時点では予定していない	28.7%	26.4%	26.9%
その他（未回答・不明）	6.8%	5.9%	5.1%

内部監査の事業規模ごとの実施割合（予定含む）

（年度）	2011	2012	2013
100名未満	26.7%	30.6%	36.8%
100名～999名	55.8%	48.7%	46.7%
1,000名～9,999名	71.6%	76.6%	80.8%
10,000名以上	95.4%	100%	100%

外部監査の実施
金融は読み替え可能項目なし（集計対象に含めず）

（年度）	2011	2012	2013
定期的に実施している	16.2%	19.5%	16.4%
実施したことがある	9.6%	12.0%	13.6%
実施予定がある	1.3%	1.3%	3.5%
現時点では予定していない	63.9%	59.0%	59.4%
その他（未回答・不明）	8.9%	8.2%	7.1%

外部監査の事業規模ごとの実施割合（予定含む）

（年度）	2011	2012	2013
100名未満	24.1%	26.6%	25.8%
100名～999名	31.7%	37.6%	34.6%
1,000名～9,999名	21.2%	29.3%	28.4%
10,000名以上	41.0%	46.8%	56.1%

別添４－３　安全基準等の継続的改善状況等に把握及び検証

「2013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」（重要インフラ専門委員会第35回会合（平成26年１月10日）資料２）より

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、②総務省 ③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、②2013年3月、③2010年12月
状況	１．継続的改善（分析・検証）状況・理由 ①：スマートフォンの急激な普及による通信事故等の多発を受け、分析・検証を実施中。 ②：省内研究会の結果を受け、２０１３年４月から２０１４年３月を目処に、情報通信審議会、総務省電気通信技術システム課において、分析・検証を実施予定。 ③：定期的な改善及び指針改訂を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）プロセス ①：－ ②：－ ③：2013年４月から、電気通信事業者協会 安全・信頼性協議会 安全基準検討WGにおいて、実施中。 ３．継続的改善（分析・検証）の結果 ①：－ ②：－ ③：－

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 改定すべき内容が特にないため、実施予定なし。 ただし、諸所の状況に鑑みて、分析・検証の実施可否について検討。 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 －

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 一部の事業者において自局の安全基準の分析・検証を実施中。分野での検討体制に関し、今後調整を予定。 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 －

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	①2008年6月、　②2013年3月、　③2013年3月
状況	１．継続的改善（分析・検証）の状況・理由 ①③：改定すべき内容が特にないため、実施予定なし。 ②：昨今のサイバー攻撃動向を受けた改善、クラウド利活用に係る対応及び構成見直し（業態別化）として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス ②：2013年4月から2015年6月を目処に、公益財団法人金融情報システムセンター（FISC）監査安全部が事務局となる「安全対策基準改訂に関する専門委員会」において実施。また、以下の取組を実施中。 ■サイバー攻撃対応として、サイバー攻撃対応に関する有識者検討会を設置し、原則月１回の検討。 ■金融機関等におけるクラウドサービスの利用に係る対応として、海外動向を含め、クラウドサービス利活用に係る調査研究。 ■構成見直し（業態別化）の検討として、安全対策基準を業態別に再編する検討（今年度は証券会社編の検討）。なお、本件の取組期間は２０１５年６月以降も継続検討予定。 ３．継続的改善（分析・検証）の結果 －

安全基準等の継続的改善状況（航空分野（航空管制、航空運送））

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 定期的な改善及び指針改訂を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス 2012年11月から、国土交通省において、分析・検証を実施中。 ３．継続的改善（分析・検証）の結果 －

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 定期的な改善及び指針改訂を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス 2012年11月から、空運送事業者・定期航空協会・国土交通省において、分析・検証を実施中。 ３．継続的改善（分析・検証）の結果 －

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 定期的な改善及び指針改訂を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス 2012年11月から、鉄道局・重要インフラ関係事業者等において、分析・検証を実施中。 ３．継続的改善（分析・検証）の結果 －

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 昨今のサイバー攻撃動向を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス 2013年8月から2014年3月を目処に、経済産業省の委託事業の中の専門家による委員会において、分析・検証を実施中。 ３．継続的改善（分析・検証）の結果 －

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 標的型サイバー攻撃等の環境変化への対応については、都度、別途の正会員通知で対応済であることから、本安全基準の改定については必要性なしと判断し、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．その他の取組 ①標的型メールの情報共有体制として、Ｃ４ＴＡＰ、Ｊ－ＣＳＩＰに参画 ②業界内でのサイバー攻撃を想定した対応訓練を実施 ③全国の事業者に情報セキュリティ説明会を実施

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 指針改訂を受けた改善として、平成２６年度以降の改定を予定。 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 －

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 定期的な改善として、分析・検証を実施済。 ２．継続的改善（分析・検証）のプロセス ２０１０年2月から２０１３年１０月にかけて、医療情報ネットワーク基盤検討会において、分析・検証を実施済。 ３．継続的改善（分析・検証）の結果 「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」において、「診療録等の保存を行う場所について」の一部改正及び最新の技術等への対応を踏まえ、部分的な改訂を実施済。 ４．その他の取組 上記改訂後も、引き続き医療情報ネットワーク基盤検討会において、分析・検証を実施中。

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 指針改訂を受けた改善として、分析・検証を実施済。 ２．継続的改善（分析・検証）のプロセス ２０１２年１２月から２０１３年６月にかけて、厚生労働省健康局水道課において、分析・検証を実施済。 ３．継続的改善（分析・検証）の結果 「水道分野における情報セキュリティガイドライン」において、新たな脅威、情報通信技術の利用形態の変化及び指針改定の視点を踏まえ、全面的な改訂を実施済。

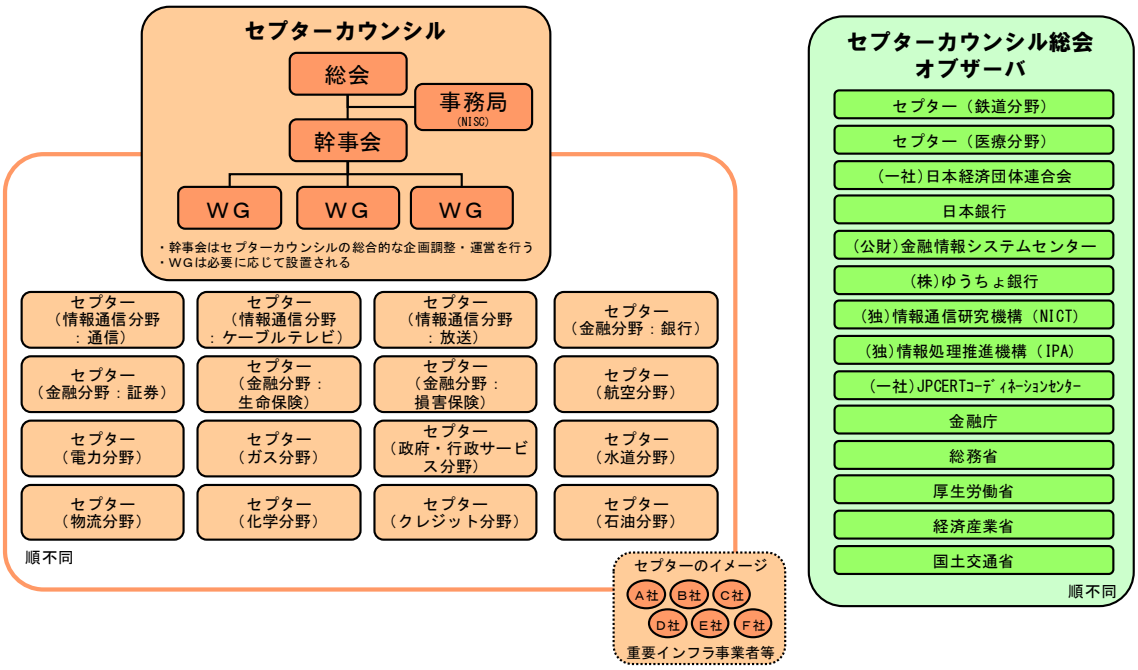
安全基準等の継続的改善状況（物流分野）

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 定期的な改善及び指針改訂を受けた改善として、分析・検証を実施中。 ２．継続的改善（分析・検証）のプロセス 2012年11月から、（一般社団）日本物流団体連合会において、分析・検証を実施中。 ３．継続的改善（分析・検証）の結果 －

別添４－４　セプター概要

セプターカウンシル総会第６回会合（平成26年４月８日）公表資料より

セプターカウンシルの概要



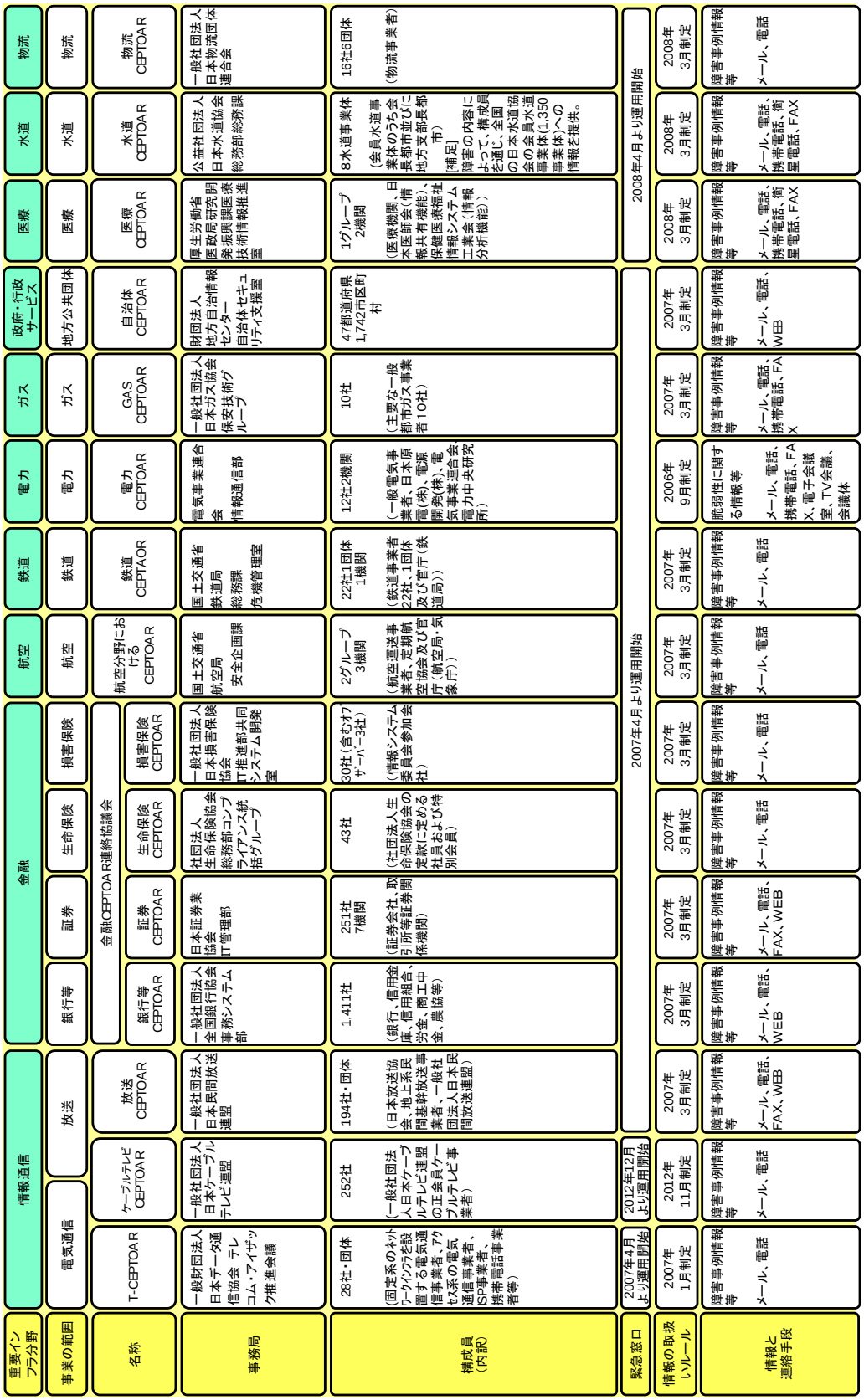
・2009年２月26日に創設。
・2012年４月12日に開催された総会（第４回）より、ケーブルテレビCEPTOAR、ゆうちょ銀行、
情報通信研究機構、情報処理推進機構、JPCERTコーディネーションセンターがオブザーバとして加盟。
・2013年４月９日に開催された総会（第５回）より、ケーブルテレビCEPTOARが正式に参加。
・2014年４月８日に開催された総会（第６回）より、化学CEPTOAR、クレジットCEPTOAR及び石油CEPTOARが正式に参加。

セプターの概要

セプター名		事務局	構成員数（2014年３月末現在）
情報通信	T-CEPTOAR	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	２８社・団体
	ケーブルテレビCEPTOAR	一般社団法人日本ケーブルテレビ連盟	２５２社
	放送CEPTOAR	一般社団法人日本民間放送連盟	１９４社・団体
金融	銀行等CEPTOAR	一般社団法人全国銀行協会	１，４１１社
	証券CEPTOAR	日本証券業協会	２５１社、７機関
	生命保険CEPTOAR	一般社団法人生命保険協会	４３社
	損害保険CEPTOAR	一般社団法人日本損害保険協会	３０社（含むオブザーバ3社）
航空分野におけるCEPTOAR		国土交通省　航空局安全企画課	２グループ、３機関
電力CEPTOAR		電気事業連合会	１２社、２機関
GAS CEPTOAR		一般社団法人日本ガス協会	１０社
自治体CEPTOAR		地方公共団体情報システム機構	47都道府県、1,742市町村区
水道CEPTOAR		公益社団法人日本水道協会	８水道事業者
物流CEPTOAR		一般社団法人日本物流団体連合会	１６社、６団体
化学CEPTOAR		石油化学工業協会	（調整中）
クレジットCEPTOAR		一般社団法人日本クレジット協会	（調整中）
石油CEPTOAR		石油連盟	（調整中）
鉄道CEPTOAR ※		国土交通省　鉄道局総務課危機管理室	２２社、１団体、１機関
医療CEPTOAR ※		厚生労働省　医政局研究開発振興課医療技術情報推進室	１グループ、２機関

別添４－５　セプターマップ

「セプターの活動状況の把握について」（重要インフラ専門委員会第36回会合（平成26年３月11日）資料３）より



別添４－６　セプター訓練

「2013年度のセプター訓練について」（重要インフラ専門委員会第36回会合（平成26年３月11日）資料２）より

訓練の概要
セプター訓練は、実施細目に基づく情報共有体制の維持・向上のため、NISCが定期的に情報疎通機能の確認等の機会を提供することとして、「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」に記載されているものです。

①目的：
(1)セプター、NISC、重要インフラ所管省庁による、情報共有体制の維持、向上
（連絡網の保守、手順の習熟）
(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
※実際の情報提供においては実施してしない事項の確認等（例えば到達確認、個社の意見の吸上げなど）、情報共有体制の点検の機会としての活用。

②参加者： 情報通信分野（電気通信、ケーブルテレビ、放送）、金融分野（銀行等、証券、生命保険）、航空分野、鉄道分野、電力分野、ガス分野、水道分野、物流分野の１２セプター及び参加事業者
（訓練に参加する事業者等については、各セプターにて選定）
金融庁、総務省、厚生労働省、経済産業省、国土交通省の担当者およびリエゾン、NISCの担当者

③実施日時：２０１３年7月から１０月（実施日時はセプターごとに決定）

④実施方法：実施細目に基づき、NISCから電子メールにてリエゾン経由で各セプターに発出し、
各セプターから参加事業者に対して情報の連絡を実施
希望するセプターについては実施方法のカスタマイズを実施。
実施後に参加したセプター等に調査票（アンケート）を依頼。

⑤使用した情報：NISCが作成した模擬情報を使用（情報共有レベル：Green）。
希望するセプターについては模擬情報のカスタマイズを実施。

⑥改善点：
・訓練手順、訓練日時、模擬情報の内容について、セプターの要望に応じて変更できるよう、具体的な変更案を追加するとともに、過去の変更例を提示。
・昨年度の実施手順に関する要望を実施案内に記載。その他、訓練内容が解りやすくなるよう実施案内を改善。

◆12のセプターにご参加いただき、訓練を実施した。

・訓練により情報共有体制の維持、向上を図ることができた。また、訓練内容のカスタマイズにも積極的に取り組むセプターが増えつつある。

- 各セプターの多くの事業者等（約1561団体）に参加いただいた。
- 昨年度の課題を踏まえた、連絡方法・ルートの改善、連絡先担当者の更新、電話による着信確認など、各セプターにて情報伝達能力の維持・向上が確認できた。
- 到達までの時間を測定いただいたセプターでは、大半の事業者等で2時間以内に受信していることが確認できた。
- 3セプターが実施内容のカスタマイズを行った。詳細は次ページ参照。

・訓練の機会を活用し、セプターや個社において独自の取り組みが行われた。

- 受領した情報に、各部署で対応すべき内容等の情報を付加して展開した。
- セプター訓練に合わせて、社内の情報共有に関する訓練を実施した。
- 前回に引き続き、到達時間を正確に把握するため、電子メールで情報を閲覧した時刻を報告してもらった。
- 訓練の事前周知を複数回行った。
- モバイル環境を想定した提供情報の加工を行って、事業者に展開した。

・NISCは情報共有体制の強化に通じた重要インフラ防護能力の維持・向上のために、引き続き定期的に訓練の機会を提供することが重要と考えます。
・ご意見を踏まえ、今後も訓練方法の多様化や訓練の実施形態を見直しを検討します。
・各セプターにおける独自の取組みが広がりつつあり、今後も訓練の機会を有効に活用することを期待します。
・今後は、障害対応体制強化の一環として、訓練の機会を提供していきます。

◆今回行われた実施内容のカスタマイズ事例（３セプターがカスタマイズを実施）

- 提供する模擬情報に具体的な内容を記載し、双方向でのやり取りを実施した。一往復（NISCからの第１報の後、セプター（事業者）から所管省庁を通じて情報連絡）を実施したセプターがあった。
- 提供する模擬情報に具体的な内容を記載した上で、緊急性を重視し、NISCからの第１報をメール本文で受信してセプター内の情報共有を行ったセプターがあった。
- 時間を抜き打ちで実施した。

・今後もセプターの要望に対応できるよう、様々なカスタマイズについて訓練に盛り込んでいきます。
・調査票の結果でも、双方向や模擬情報の中身を記載することを望む事業者の回答があるため、セプターにおいても、次回以降、引き続き訓練手順のカスタマイズをご検討していただくことを期待します。

別添４－７　分野横断的演習

「「2013年度重要インフラの分野横断的演習に関する調査」の結果について」（重要インフラ専門委員会第36回会合（平成26年３月11日）資料５）より

分野横断的演習の要点

・IT障害に適切に対応するには、連絡体制や対応手順などを含むBCP等の整備が必要です。
・BCP等の実効性の確保には**演習や訓練により、その検証と改善**を重ねることが不可欠です。

分野横断的演習とは

①官民の重要インフラ関係者が一堂に会する演習

重要インフラ事業者・セプター（10分野・15セプター）
情報通信（通信、ケーブルテレビ、放送）、金融（生保、損保、銀行、証券）、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

NISC
情報共有体制の検証
所管省庁
金融庁、総務省、厚労省、経産省、国交省

※2013年度は61組織・212名が参加

②官民／事業者間連携の検証が可能
・外部組織との情報共有体制等について検証が可能です。
・多く企業・団体が参加するため実践的な検証が可能です。

③他事業者との意見交換により新たな気づきが期待できる
・演習実施後には意見交換会を行い、相互の情報共有を図ります。
・他事業者の取組みや専門家（有識者）のアドバイスなど、自社の参考になる情報が得られます。

2013年度の分野横断的演習

テーマ
情報セキュリティインシデントの対応

検証課題
（1）情報セキュリティインシデントに関する情報共有体制
（2）情報セキュリティインシデントへの対応
（3）BCP等※の発動・解除方法

※BCP等：BCPそのものだけではなく、情報システムに関するIT-BCPや障害対応手順、システム操作マニュアル等の関係する文書を含む

得られた気づきの例
・社内の総務・企画部門との情報連携に課題を感じた。
・複数のシステムに障害が発生した際に、復旧の優先順位が課題となった。

⇒演習で得られた気づきや知見を「**情報セキュリティインシデント対応のためのチェックリスト**」としてまとめました。（本資料に添付）

演習の経緯－第２次行動計画における分野横断的演習の取組み

第1次行動計画（2006～2008年度）

【目標】官民連携の充実

＜2006年度＞ 官民連携の仕組みづくり
- 研究的演習：演習実施概念、演習課題設定、演習手法の理解等を主眼として実施。
- 机上演習：脅威として災害を設定し、会議形式の演習を実施。

＜2007年度＞ 官民連携体制の機能向上
- 機能演習：脅威としてDDoS攻撃を設定し、チーム毎に個室に分かれ、メールのみを利用した演習を実施。

＜2008年度＞ 官民連携体制の実効性向上
- 機能演習：参加者にIT障害の発生原因を知らせない等より現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧や事業継続等を行っていく演習を実施。

分野横断的な演習手法に関する知見

第2次行動計画（2009～2013年度）

【目標】重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出

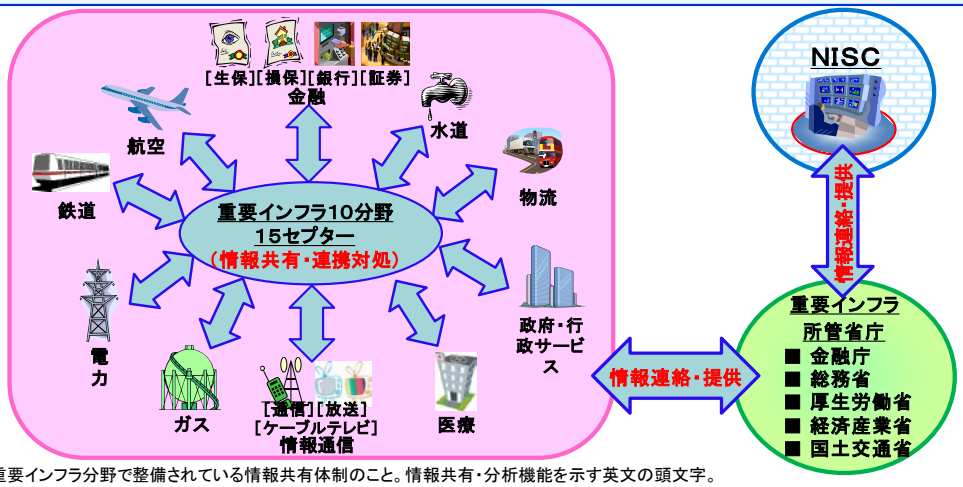
①分野横断的な脅威に対する共通認識の醸成
②他分野の対応状況把握による自分野の対応力強化
③官民の情報共有をより効果的に運用するための方策

年度	2009年度	2010年度	2011年度	2012年度	2013年度
テーマ	広域停電	大規模通信障害	重要インフラ複合障害	重要インフラ複合障害＋便乗型ITインシデント	情報セキュリティインシデント
取組み	① シナリオ、実施方法、検証課題等を企画				
	② 早期復旧手順・事業継続計画等の検証、共有				
	③ 演習の実施方法等に関する知見の集約・蓄積				
		④ 自職場演習の導入			
			⑤ サブシナリオの導入		
			⑥ 重要インフラ分野、事業者間の連携推進		
				⑦ 第三者による助言の導入	⑦ 第三者による助言の充実

分野横断的演習の目的と参加機関、メリットについて

[目的]
IT障害の要因となり得る事態に際し、重要インフラ各分野が的確に情報共有・連携し、IT障害の未然防止やIT障害に係る被害の最小化・早期復旧に関する検証を行なうことを目的とし、内閣官房情報セキュリティセンターの施策として、2006年度より継続実施（計8回）。

[参加機関]
重要インフラ事業者等：　10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）
セプター※1：　10分野の15セプター
政府：　重要インフラ所管省庁（金融庁、総務省、厚労省、経産省、国交省）及び内閣官房情報セキュリティセンター（NISC）



※1　セプター：　各重要インフラ分野で整備されている情報共有体制のこと。情報共有・分析機能を示す英文の頭文字。

[分野横断的演習のメリット]
（1）分野横断的な脅威や各分野への波及（障害状況・対応など）の把握と、対応力の検証ができる
（2）官民間に加え、他分野、同業他社、関係機関等との情報共有や連携による対応力の向上を図ることができる
（3）他分野の対応方法や気づきを共有することで、新たな対応・改善方針を得ることができる

2013年度分野横断的演習実施概要

1. 日時：　2013年12月9日（月）　12:00　～　18:30
※　10:40～11:50　受付
※　10:45～11:45　ツール試用　（参加自由）

2. 場所：　株式会社三菱総合研究所（東京都千代田区永田町2－10－3）　4階会議室
一部事業者等における自職場

3. 参加者（プレイヤー、コントローラーを含む）：
61組織212名が参加（内3組織10名が自職場参加）

（重要インフラ事業者等：10分野）
情報通信（通信、ケーブルテレビ、放送）、金融（銀行、生命保険、損害保険、証券）、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流
※　証券事業者（1社）及び物流事業者（1社）が自職場演習

（セプター：10分野　15セプター）
※　証券セプターが自職場演習、ガスセプターがサブシナリオ策定

（関係機関）　IPA、JPCERT／CC

（分野横断的演習検討会　有識者委員）
慶應義塾大学大学院　大林教授（座長）、名古屋工業大学大学院　渡辺教授（副座長）　他

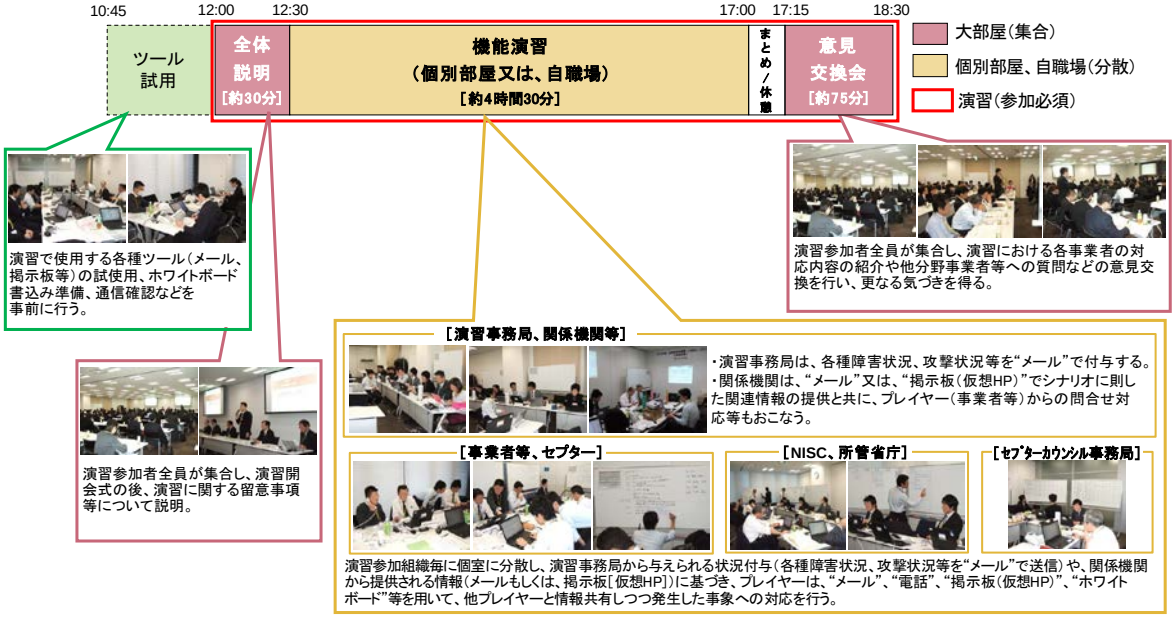
（政府）
重要インフラ所管省庁、内閣官房情報セキュリティセンター

4. シナリオ概要
複数の情報セキュリティインシデント予兆が検知される中、大規模な情報セキュリティインシデントが発生し、複数分野においてサービスへの影響が発生した。一部分野におけるサービスへの影響が他分野にも波及し、多くの重要インフラ事業者等において、インシデントの防止や被害最小化、あるいは事業継続のための、原因調査・復旧対応が求められた。

分野横断的演習の様子

事務局からの状況付与（各種障害状況、攻撃状況等）に従い、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”等を用いて、他プレイヤーと情報共有しつつ発生した事象への対応を行う。
また演習後の意見交換会において、演習で得られた気づきを参加者間で共有する。

［演習当日のタイムスケジュール］



演習において得られた主な気づき

■ 演習の事前説明会での講演や演習終了後の意見交換会等、分野横断的演習の取組み全体を通じて、各重要インフラ事業者等において、情報セキュリティインシデントの予兆検知時・障害発生時の情報共有・対処を効果的に行うための気づきを得ることができた。

演習において得られた主な気づき

●情報セキュリティインシデントに関する情報共有体制に関する気づき
- ・予兆をとらえるための情報収集先や収集内容の事前整理の必要性
- ・予兆を捉えた際やインシデント発生時における報告基準の明確化の必要性
- ・情報共有に関わる社内連携や対応フローの整備の必要性
- ・収集した情報の共有範囲の策定の必要性（予兆、インシデント）
- ・インシデント対処における情報収集の重要性
- ・インシデント発生時の情報収集先や収集内容の事前整理の必要性
- ・社内のインシデント対応状況集約に関する仕組み構築の有用性
- ・ネットワーク利用不可時の代替通信手段の確保
- ・インシデントに関する所管省庁への報告の判断基準の必要性
- ・外部への情報発信の有無、タイミングの判断基準の必要性
- ・HP利用不可時の代替情報開示手段の確保の必要性
- ・適時、適切に情報発信するための事前準備の有効性（フォーマットの作成等）
- ・メール利用不可時の分野内の情報共有手段確保の必要性
- ・他事業者や同業他社との情報共有方法に関する検討の重要性

●情報セキュリティインシデントへの対応に関する気づき
- ・インシデントへの対応手順策定、体制整備の必要性
- ・被害想定の困難さや影響範囲が不明な中での対応の必要性
- ・想定される影響を踏まえた前広な対応の有効性
- ・既存の災害対応体制を活用したインシデント対応の有効性
- ・分野横断的・複合的な事象への対応検討の必要性
- ・イントラへの大規模インシデントを想定した対応検討の重要性
- ・制御システムへのインシデントを想定した対応検討の重要性

●BCP等の発動・解除方法に関する気づき
- ・情報セキュリティの観点を含めたBCP等策定の必要性
- ・BCP等を踏まえたシステム復旧順位の策定の必要性
- ・BCP等を踏まえたサービス継続と対応体制の検証の必要性

演習内容の総括

○検証課題の設定について	
・ほぼ全ての参加者が今年度の演習は有益だったと評価しており、検証課題の設定は概ね適切だったと言える。	
○検証課題ごとの評価	
情報セキュリティインシデントに関する情報共有体制	・予兆段階での社内外との情報共有についての検証ができ、不確実な予兆情報に基づく情報共有（判断基準や手順等）の改善に資する気づきが得られた。 ・インシデント発生時の情報共有についての検証ができ、共有すべき相手（政府、セプター、事業者等）や手段等、平時から点検しておくべき点に関する気づきが得られた。 ・他分野との情報共有のあり方について気づきが得られた。 ・情報開示は積極的になされ、複数の手段を用いての情報開示や顧客への影響に配慮した注意喚起等に関する気づきが得られた。
情報セキュリティインシデントへの対応	・インシデントの予防措置や対処についての検証ができ、複合的な障害における対応の優先順位付けや対応のルール・文書の改善に資する気づきが得られた。
BCP等の発動・解除方法	・情報セキュリティインシデントに対応するBCP等の内容や判断基準および対応内容についての検証ができ、これらの改善に資する気づきが得られた。

演習運営面の総括

○演習運営面の評価

・事前説明会を通じて参加者へ演習本番前に関係文書や体制の確認を促した結果、一部の参加者では、文書が最新の内容に更新されていない等の修正すべき点の発見につながった。一方で、シナリオの詳細が非開示だったため、文書や体制の事前確認を十分に行うことができなかったとの意見もあり、事前説明会を含めた演習実施方法の更なる検討が必要である。
・演習当日の意見交換会に加え、作業報告メモ、アンケート等の分析を踏まえた後日の意見交換会を開催することで、他事業者の取組みや気づきを共有できた。
・自職場から演習に参加した事業者では、実際の環境でより実践的に情報共有体制等の検証ができた。
・一部の分野では、セプターが事業者の検討を深める役割を果たし、より多くの気づきの創出を図る独自の取組みが行われた。
・第三者による助言は有益だとの意見が多かったが、演習参加者の増加に伴い助言の体制や実施方法のあり方について更なる検討が必要である。

○課題と今後の方向性

（1）参加者の特性や取組み等の多様性を踏まえた演習
・全分野共通の検証課題と、参加者の特性に応じて個別に設定する検証課題の整理
・個別に設定する検証課題に配慮した、シナリオ作成方法および演習実施方法の改善
・演習の自職場参加も活用し、より多くの参加者に対応できる演習実施形態を検討

（2）各参加者が効率的に演習の振り返りを行うための支援
・当日の時間配分を見直し振り返りの時間を確保
・効果的な振り返りを実現する仕組みづくり

（3）新規参加者の受け入れ拡大（重要インフラ防護施策の普及）
・新規参加事業者も取組みやすい難易度を下げた演習を一部取り入れることを検討
・新規参加がしやすい仕組みづくり（第三者助言の活用等）

別添４－８　補完調査

「2013年度 重要インフラにおける「補完調査」について」（重要インフラ専門委員会第36回会合（平成26年３月11日）資料４）より

補完調査の目的・観点

目的・スタンス

○第２次行動計画で期待される結果（アウトカム）の評価をより実態に即すようにするためには、指標では捉えられない側面を補完的に調査することが必要であり、IT障害等の事例を調査し、評価の材料を得る。

○検証にあたり、所管省庁及び重要インフラ事業者等の協力（情報提供・ヒアリングの実施等）を得るに当たっては、検証に協力した事業者等に不利益が生じないよう必要な配慮を行う。

検証の観点

○目的・スタンスに照らして、以下の点について検証を行う。なお、重要インフラ事業者等が「安全基準等」により具体的に対応することが望まれる課題については、「指針及び対策編」見直しの取り組みに反映させる。

・ＩＴ障害の未然防止、拡大防止、早期復旧のために実際にどのような対処が行われたか
・安全基準等は、被害の発生防止、拡大防止に関し、十分なものであったか
・官民の情報共有体制、セプター等による事業者間での情報共有が、具体的にどのように機能したか
・他の事業者等から受けた影響、あるいは他の事業者等へ与えた影響はあったか
・その他、被害の未然防止、拡大防止、早期復旧の観点から得られた教訓はあるか

補完調査対象事例

検証の対象とする事例

実際に発生した「ＩＴ障害」及びＩＴ障害の要因となり得る「脅威」について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさを考慮して以下の事例を選定した。

No.	事　例	脅　威
事例１	認証ＩＤ・パスワードの外部漏えい	サイバー攻撃をはじめとする意図的要因
事例２	複数Ｗｅｂサイトの改ざん	サイバー攻撃をはじめとする意図的要因
事例３	複数回にわたるＷｅｂサイト遅延障害	サイバー攻撃をはじめとする意図的要因

事例１（認証ＩＤ・パスワードの外部漏えい）　１／２

【概　要】

- 事業者が管理する会員制サイトのサーバに対する不正アクセスにより、当該サイトへログインするための認証ＩＤと暗号化されたパスワードが外部に漏えいした。
- 監視強化中に再び不正アクセスを検知したため、関連する全システムの稼働を停止するとともに当該会員制サイトのサービス提供を停止。サーバを再構築したうえでサービスを再開した。

＜１回目の不正アクセス＞

当該サーバで利用しているミドルウェアにおける脆弱性について、情報セキュリティ関係機関が注意喚起を実施。

それを受けた当該事業者は、パッチの適用について検討を開始するとともに、暫定的なセキュリティ対策を実施したうえで、当該対策を実施するまでの間に不正アクセス等がなかったかについてログ等の確認作業を実施。

確認作業の結果、不正アクセスにより認証ＩＤと暗号化されたパスワードが収集された痕跡を確認。

＜２回目の不正アクセス＞

数日後、セキュリティ監視を強化しているなかで、新たな不正アクセスを検知。

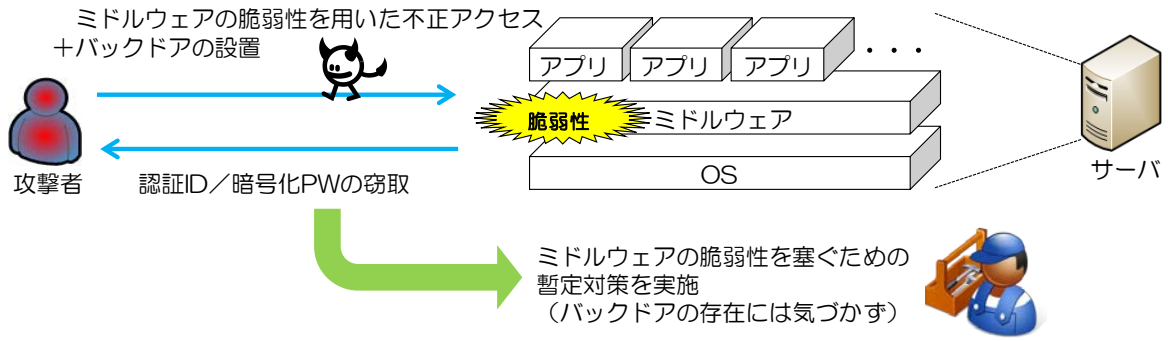
当該不正アクセスは、１回目の不正アクセス時に設置されたバックドアプログラムに起因する不正アクセスと判明。

関連する全てのシステムの稼働を直ちに停止させ、新たな情報漏えいを未然に防止。

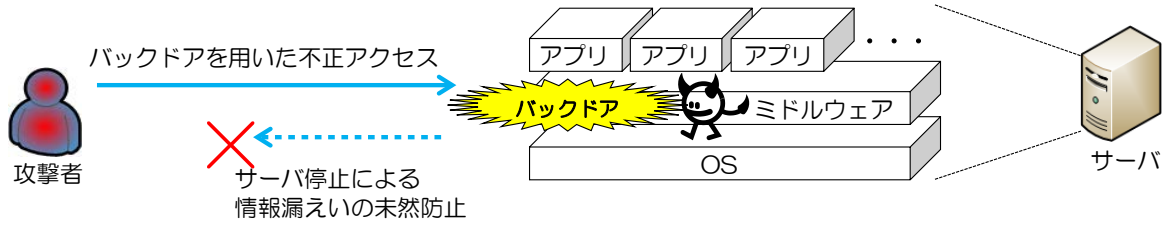
その後、サーバを再構築（当該ミドルウェアのパッチは適用済）し、新たなセキュリティ監視装置（WAF）を導入したうえでサービスを再開。

【事象のイメージ】

＜１回目の不正アクセス＞



＜２回目の不正アクセス＞



事例１（認証ＩＤ・パスワードの外部漏えい）　２／２

【原　因】

＜１回目の不正アクセス＞

- 当該サーバで利用しているミドルウェアにおける脆弱性を悪用した不正アクセスであったが、開発元が当該脆弱性のパッチを公開し、情報セキュリティ関係機関が注意喚起を行うまでの間に攻撃が発生した。
- 脆弱性に対するパッチについて、当該ミドルウェア上で動作する各種アプリケーションの動作を確認する必要があるため、直ちにパッチを適用できない状況であった。

＜２回目の不正アクセス＞

- １回目の不正アクセスの際に、サーバ上の、通常では発見しづらい箇所にバックドアプログラムが設置されていた。

【再発防止】

- 高度な攻撃を検知・自動ブロックするためのセキュリティ監視装置を導入。
- ユーザに対し、認証パスワードの再設定の必要性を周知。
- 社内のシステムを洗い出し、脆弱性対応を一元化できる仕組みを導入。
- 脆弱性の重要度に対する対応目安日数を設定し、対応状況をシステムで管理。
- 情報セキュリティ事案に対する全社的な緊急対応体制※を新たに整備し、その体制に基づく訓練を実施。

※ＩＴ障害発生時に、社内の対策本部を立ち上げる基準や手順等

【得られた気づき・教訓】

- パッチ適用など根本対処が直ちにできない場合は、不正アクセスの監視強化などの暫定対処を行う。
- 脆弱性への対応を迅速に行うために、平時からシステムで利用されているソフトウェアを把握する。
- 脆弱性情報を重要度に応じて、その対応状況を含めて管理し組織内で迅速に情報共有を行う。
- 情報セキュリティ事案に対する緊急対応体制を平時から準備し、その対応を訓練する。
- 不正アクセスされた場合は、情報漏えいの可能性だけでなく、2次被害としてバックドアプログラムの設置の可能性を想定し、隠しファイルの確認を含めた対応を行う。

事例２（複数Ｗｅｂサイトの改ざん）　１／２

【概　要】

- 本事業者は複数のWebサイトを有しており、その一部はIT担当部署以外の担当部署が管理をしている。
- ある担当部署が管理する一部のWebサイトに対する不正アクセスにより、当該Webサイトが書き替えられ外部のWebサイトへの不正な誘導（リダイレクト）が発生。
- さらに、上記のインシデント対応中に別の担当部署が管理するWebサイトに対しても不正アクセスにより、当該Webサイトが書き替えられるインシデントが発生した。

＜１件目のインシデント案件＞

事業者の職員が利用している端末に導入されているウィルス対策ソフトがウィルスを検知。ウィルスについて調査したところ、IT担当部署以外の担当部署で管理しているWebサイトにアクセスしたことによるものと特定。

報道発表を行うとともに、当該Webサイトを閉鎖し、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

その後、コンテンツの見直しを行い、メインのWebサイトに統合済。

＜２件目のインシデント案件＞

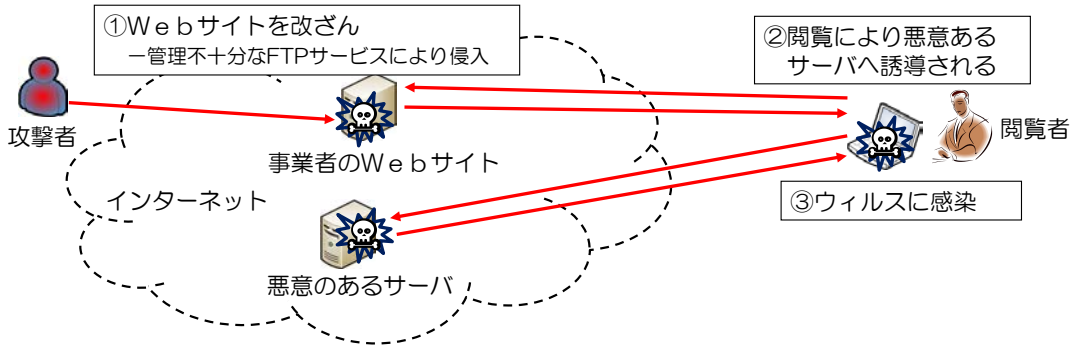
１件目のインシデント案件と同じ週に、別の担当部署が管理するWebサイトの一部を閲覧出来ない事象を職員が発見。当該Webサイトの保守業者に連絡を取り調査を行ったが、ウィルス対策ソフトでは検知されず、原因の特定に至らなかった。

しかし、不正アクセスによる改ざんを疑い担当部署の判断で当該Webサイトを閉鎖。ウィルス対策ベンダに調査を依頼したところ新種のウィルスであり、 Webサイトへの不正アクセスによりウィルスを混入されていたことが確認できたため、報道発表を行うともに、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

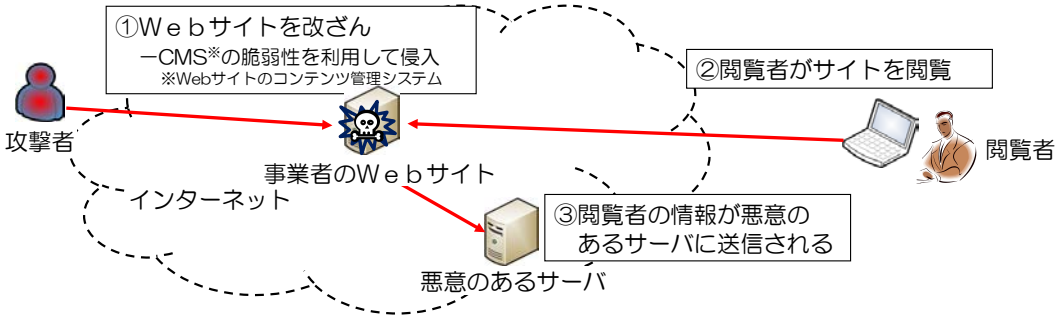
その後、Webサイトの脆弱性調査を行い、多数の脆弱性を確認し、対応後にWebサイトを再開。

【事象のイメージ】

＜１件目のインシデント案件＞



＜２件目のインシデント案件＞



事例２（複数Ｗｅｂサイトの改ざん）　２／２

【原　因】

＜１件目のインシデント案件＞

- 初期構築時にのみFTPを利用し、その後はCMSを利用した更新を行っていた。現在の担当者がFTPサービスが提供されている事を知らなかったため、FTPのID・パスワードは初期構築時より変更されていなかった。
- 不正なFTP接続によって、外部のWebサイトよりウィルスをダウンロードさせるプログラムがWebサイトに挿入された。

＜２件目のインシデント案件＞

- 同一Webサイト上にバージョンが異なる（脆弱性を有するバージョンを含む）CMSが存在していた。脆弱性の存在を認識していたものの運用中のWebサイトへの影響を考慮し、更新及び統一化が出来ていなかった。また、担当部署に加え外部事業者等の複数者がWebサイトの内容変更が可能な権限を有していた。
- 改ざんの約1ヶ月前に当該Webサイトに対して総当たり攻撃が行われていた。

【再発防止・課題等】

- Webサイトの必要性の見直しを行い、可能な限りIT担当部署が管理するWebサイト等に統合することにより管理の効率化等を図った。
- ファイアウォール等の設定を見直し、Webサイト利用における最小限の通信のみとした。
- 管理ページを含めたWebサイトのログを取得し、適切な期間（例えば1年間）保存するとともに、定期的に確認を行うこととした。
- CMSを1つに統合し一元的に管理すると共に、Webサイトの内容変更ができる権限を持つ者を限定した。
- 事業者内のWeb管理者向け研修において、事例を共有することにより他の担当部署が管理するWebサイトで同様の事象が起こらないように注意を促した。
- 幹部会議において事例を紹介し、担当者任せにせず幹部主導の下、組織として改善を行って欲しい旨の周知を行った。

【得られた気づき・教訓】

- ２件目の案件において、担当部署の判断により詳細が判明する前にWebサイトを停止することにより被害の拡大が防止された。現場で素早い判断を行うための体制や運用ルールの明確化または、現場で判断が出来ない場合であっても、速やかに判断できる者に報告できる体制構築が望ましい。
- Webサイトのアクセスログについて、事業者全体のルールでは保存期間を決めていなかったため、今回の2件ともに1ヶ月の保存期間であった。そのためログの解析が十分に出来なかった。今回の教訓を踏まえ、全体ルールとして適切な期間のログの保存を義務付けた。
- Webサイトの担当部署が複数に分かれるためITに詳しくない担当者もいる。ITに詳しくない担当者に対してもインシデント内容の重大性を理解してもらうための分かりやすい説明が必要である。また、何か不明な点があればIT担当部署に問い合わせを行うべきである。
- 普段からWebサイトの挙動に気を配り、通常と違う挙動が見られた場合に調査を行う、いわゆる予兆を見逃さない心構えが重要である。

事例３（複数回にわたるＷｅｂサイト遅延障害）　１／２

【概　要】

- 事業者が管理するWebサイトに複数回にわたり、海外の複数地域より大量の接続要求があり、表示が著しく遅くなった。
- ４回目の事象発生時に、DNSサーバへの接続要求も多数確認した。当該事象を情報共有した結果、DNSサーバがオープンリゾルバ状態※1であることが判明したため、対策を実施した。

※1 応答する必要のない外部からの問い合わせに応答する状態。攻撃の踏み台として利用される危険が高い。

＜１～３回目のインシデント案件＞

最初の２回については、Webサイトの表示が著しく遅くなったものの、短時間で通常状態となったため、監視強化を行った上で様子見とした。

３回目については、それまでに２回発生していたこと、比較的影響が長時間続いたこともあり、ファイアウォールにて発信元IPの遮断を実施した。しかしながら遮断後においても、IPアドレスを変えて引き続きアクセスされる状況であったため、Webサーバの処理能力に余裕があったことから、厳しめに設定していたファイアウォール側での同時接続数を増加させることで対応した。

＜４回目のインシデント案件＞

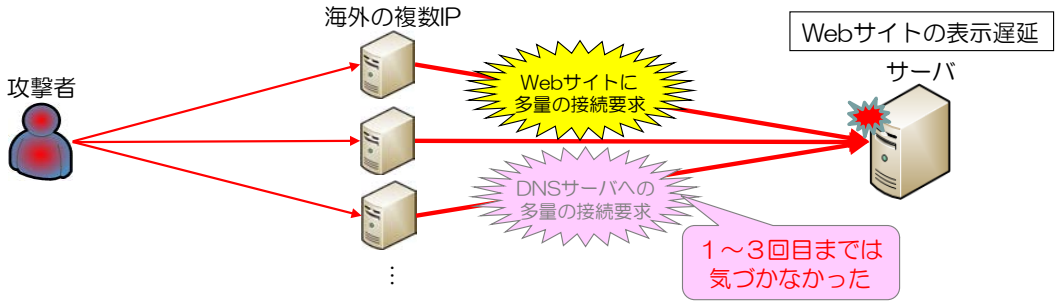
３回目と同様の措置を実施して対処した。またDNSサーバへの接続要求も多数確認※2した。

本事案を情報連絡により情報共有したところ、NISCより、DNSサーバがオープンリゾルバ状態である旨の指摘を受け、対策を行い解消した。その後は、同様の事象は発生していない。

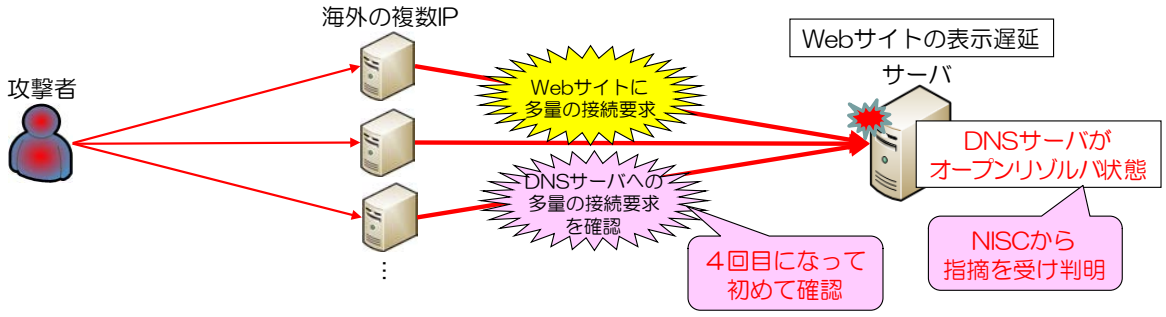
※2 DNSサーバへの接続要求は１回目からあったが、Webサイトの遅延のみに注意を向けていたため、４回目になって初めて気づいた。

【事象のイメージ】

＜１～３回目のインシデント案件＞



＜４回目のインシデント案件＞



事例３（複数回にわたるＷｅｂサイト遅延障害）　２／２

【原　因】

＜１～３回目のインシデント案件＞

- 根本原因については不明。
- 他事業者で同様の事象が発生していないかどうかの確認を行い、他事業者で発生していないことを確認。

＜４回目のインシデント案件＞

- 根本原因については不明だが、DNSサーバがオープンリゾルバ状態であったことが判明。
- 運用保守は業務委託し、常駐保守となっていることもあり、セキュリティ対策は十分に実施しているとの思い込みがあった。
- 公開サーバ系を中心としたパッチ適用等は実施していたため、脆弱性は問題ないとの認識があった。
- セキュリティ監査については、予算の関係もありしばらく実施できていない状態であった。

【再発防止】

- 監視強化の一環として、ログ確認を毎日定期的に実施。
- 不正アクセス対策として、高度な攻撃を検知・自動ブロックするためのIPS装置※1を導入。
- セキュリティ注意喚起に関する連絡を確実に実施※2。
- ファイアウォール等（IPS含む）のログは、アクセス数が多いと一杯になってしまうため、ログサーバで保存する等の管理を徹底。

※1　不正侵入防止システム
※2　ネットワーク構成が２つに分かれており端末も別々のため、セキュリティ注意喚起に関する連絡については、確認が十分に行えていない状態であった。

【得られた気づき・教訓】

- 障害等が発生した場合には、把握をしている範囲で関係機関に情報連絡を行うとともに、関係機関から提供された情報について、適切に対応する。
- 公開サーバ系については、パッチ適用等の脆弱性対策を行うだけでなく、設定情報等のチェックを含めたセキュリティ監査についても、定期的に実施する。
- 運用保守を委託先に全て任せるのではなく、セキュリティ対策は事業者自身が責任を負うということを再度認識するとともに、連絡体制を整えておく。
- 障害発生時は、事業者内だけでなく、他事業者とも連携をとるとともに、Webサイト応答時間計測システム※3等の仕組みについても活用することにより、横の情報共有を行う。

※３　DDoS攻撃やアクセス集中時等のWebサイトのレスポンス変化を観測し、情報共有を行うセプターカウンシルにおける取組み。

（本ページは白紙です。）

別添５　最近の主な脅威の概要とその対策

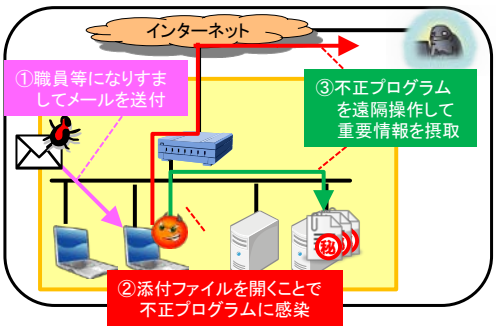
①　標的型攻撃（メールによる攻撃）

脅威の概要

- 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

＜最近の事例＞
- 2012年11月　一部の独立行政法人が「なりすましメール」による不正プログラムに感染し、情報漏えいした可能性があることが判明

標的型メール攻撃のイメージ

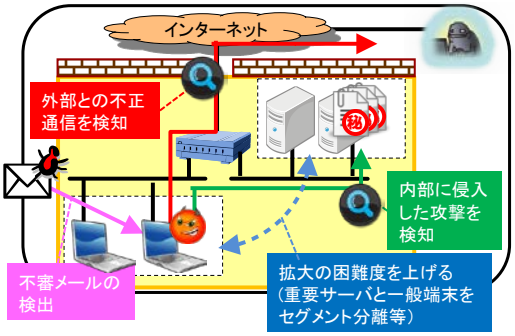


主な対策

- 不審なメールを検出する仕組みの整備、対応能力を向上する（SPFの検証、教育・訓練、等）。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

＜統一基準群（平成26年度版）における対策事項＞
- 6.2.4項 標的型攻撃対策
- 6.2.1項 ソフトウェアに関する脆弱性対策
- 7.2.1項 電子メール　等

対策の概要(例)



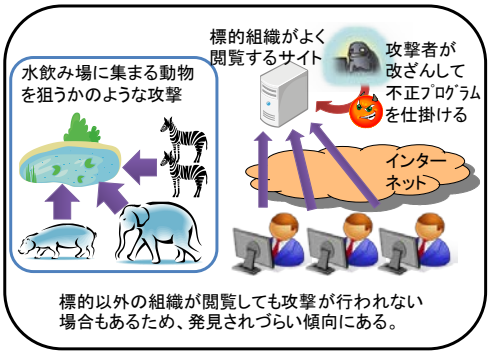
②　標的型攻撃（水飲み場型攻撃）

脅威の概要

- 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ブラウザの未知の脆弱性を悪用した攻撃（ゼロデイ攻撃）の場合もあり、未然防止は困難。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

＜最近の事例＞
- 2013年８月～９月　中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃（標的組織のIPアドレスからのサイト閲覧者だけが感染するもの）が発生

水飲み場型攻撃（イメージ）

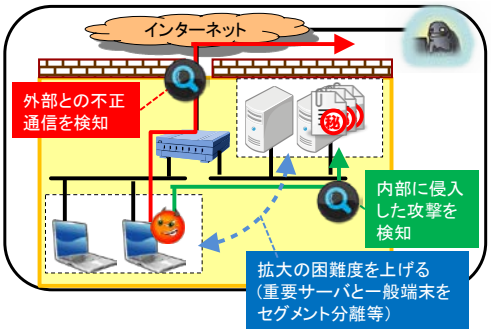


主な対策

- 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
- 内部対策としては、以下が挙げられる。
  - 内部に侵入した攻撃を早期検知して対処
  - 侵入範囲の拡大の困難度を上げる
  - 外部との不正通信を検知して対処

＜統一基準群（平成26年度版）における対策事項＞
- 6.2.4項　標的型攻撃対策　等

対策の概要(例)



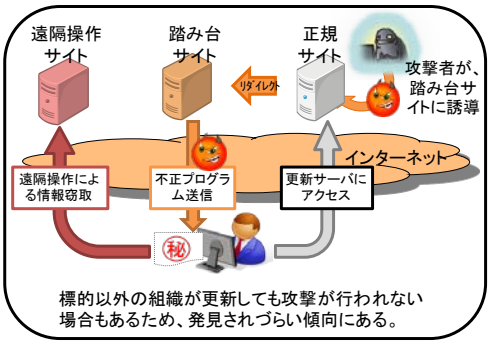
③　標的型攻撃（ソフトウェアの更新プログラムを悪用した攻撃）

脅威の概要

- 広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行った端末を不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

＜最近の事例＞
- 2014年1月　一部の独立行政法人において、無料動画再生ソフトをアップデートした際に不正プログラムに感染したことが判明

ソフトウェアの更新プログラムを悪用した攻撃（イメージ）

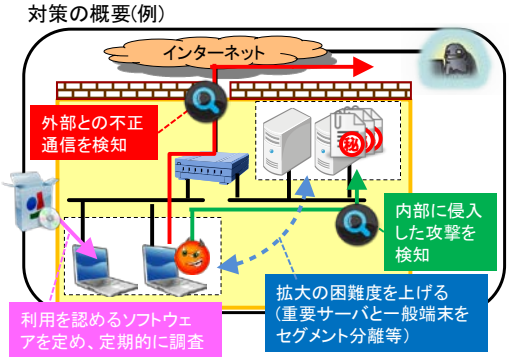


必要な対策

- 端末で利用を認めるソフトウェアを定め、利用されているソフトウェアの状態を定期的に調査する。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

＜統一基準群（平成26年度版）における対策事項＞
- 6.2.4項　標的型攻撃対策
- 7.1.1項　端末　等

対策の概要(例)



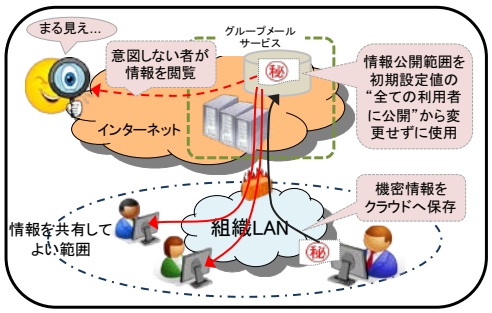
④　意図しない外部への情報流出（約款による外部サービス）

脅威の概要

- 約款に同意して利用する一般消費者向けのサービス（グループメールサービス等）には、情報セキュリティに関する十分な条件設定が行えないものも多く、当該サービスの利用が機密情報の流出につながるおそれがある。

＜最近の事例＞
- 2013年7月　インターネット上でメールを共有できる民間企業の無料サービスで個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた

グループメールサービスの不適切な利用（イメージ）

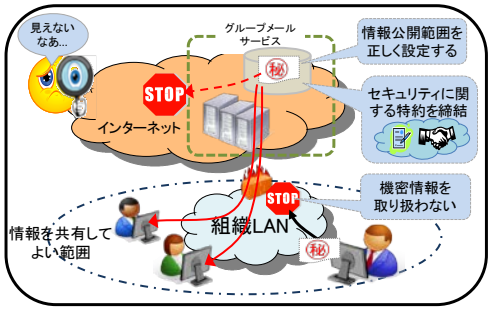


主な対策

- 約款による外部サービスの利用に係る責任者を設置し、アクセス権設定等の安全管理措置を含む利用手順を整備する。
- セキュリティ水準を十分確保するための特約等を締結する、又は機密性の高い情報を取り扱わない。

＜統一基準群（平成26年度版）における対策事項＞
- 4.1.2項　約款による外部サービスの利用　等

グループメールサービスの適切な利用（例）



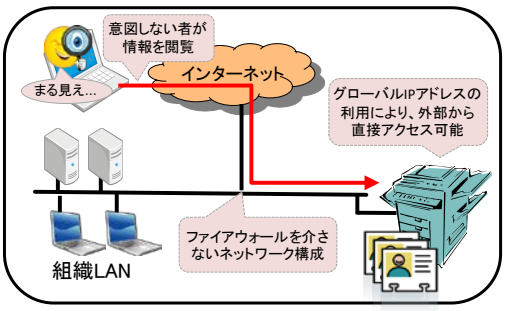
⑤　意図しない外部への情報流出（複合機）

脅威の概要

- 機密情報を内部に蓄積し、ネットワークに接続された複合機は、サーバ装置等と同様の脅威が想定される。
- 運用管理が不十分な場合、外部からアクセスされるなどのおそれがある。

＜最近の事例＞
- 2013年11月　一部の国立大学において、ファックスやスキャナーで読み取った、学生らの個人情報がインターネット上で誰でも閲覧できる状態になっていた

複合機からの意図しない情報流出（イメージ）

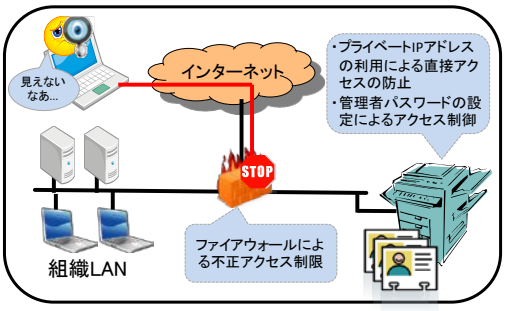


主な対策

- ネットワーク構成の見直しやファイアウォールの利用によるインターネットを介したアクセスの制限を行う。
- 管理者パスワードの設定、リモートメンテナンスに関する設定等を適切に行う。

＜統一基準群（平成26年度版）における対策事項＞
- 7.1.3項　複合機・特定用途機器
- 7.3.1項　通信回線　等

対策の概要（例）



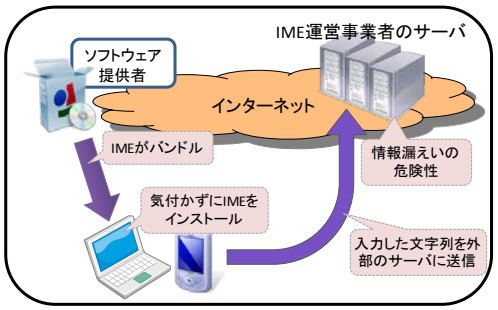
⑥　意図しない外部への情報流出（日本語 IME）

脅威の概要

- 特定の日本語文字入力補助ソフト（日本語IME）が動作している状態でキーボードから入力した内容が、外部のサーバに送信されることによる情報流出。
- 別のソフトウェアにバンドルされるなど、意図せず当該IMEをインストールするおそれがある。

＜最近の事例＞
- 2013年12月　府省庁や国立大学の一部の端末において、当該IMEがインストールされていた

日本語IMEによる意図しない情報流出（イメージ）

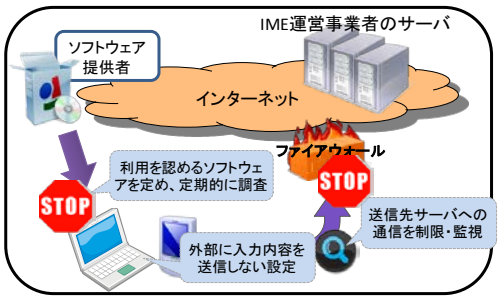


主な対策

- 端末で利用を認めるソフトウェアを定め、利用されているソフトウェアの状態を定期的に調査する。
- 入力内容を送信しないようにIMEを設定する。
- 送信先サーバへの通信を制限・監視する。

＜統一基準群（平成26年度版）における対策事項＞
- 5.2.1項　情報システムの企画・要件定義
- 7.1.1項　端末
- 8.1.1項　情報システムの利用　等

対策の概要(例)



別添６　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	C⁴TAP	Ceptoar Council's Capability for Cyber Targeted Attack Protectionの略（シータップ）。セプターカウンシルにおける標的型攻撃に関する情報共有体制。重要インフラサービスへの攻撃の未然防止、もしくは被害低減、サービスの維持、早期復旧を容易にすることを目的として、2012年12月に運用を開始した。
	CC	Common Criteriaの略。ISO/IEC 15408のこと。情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
	CCRA	Common Criteria Recognition Arrangementの略。CCに基づいたセキュリティ評価・認証の相互承認に関する協定。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
	CERT/CC	Computer Emergency Response Team/Coordination Centerの略（サートシーシー）。サイバー攻撃情報やシステムの脆弱性関連情報を収集・分析し、関係機関に情報提供等を行っている非営利団体の一般的な名称。複数の国で設立されており、日本にはJPCERT/CCが設置されている。
	CIO	Chief Information Officerの略。情報化統括責任者。企業や行政機関等の組織において情報化戦略を立案、実行する責任者のこと。なお、「政府CIO」は内閣情報通信政策監である。
	CISO	Chief Information Security Officerの略。最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣官房情報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、第１回を開催。
	Common Criteria	CCを参照。
	cPP	Collaborative Protection Profileの略。調達に際して考慮すべきセキュリティ要件。
	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、2014年５月現在、世界64ヶ国の官・民・大学等298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。内閣官房情報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、また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。
	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情報データベース。
	JVNiPedia	IPAが運営する脆弱性対策情報提供サイト。
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 で配布されている個人向けの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。独立行政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。
	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 Information Security Centerの略。内閣官房情報セキュリティセンター。2005年に情報セキュリティ政策に係る基本戦略の立案その他官民における統一的、横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行うために設置。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。セキュリティ設計仕様書のひな型のこと。
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。
	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	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、緊急事態又は機器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	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（試行版）	政府機関において、内部規律違反による情報漏えい、標的型攻撃等による情報窃取等に備えるべく、各府省庁の業務・情報に係る機密度等に応じたリスク評価を行うためのガイドライン。2013年９月より試行、その結果を踏まえて2014年度から正式導入。
	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	情報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、サイバー攻撃に関する情報を共有すべく、警察庁と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	サイバー攻撃対策の強化のため、2013年４月、13都道府県警察において設置された特別捜査隊。
	サイバー攻撃分析センター	サイバー攻撃の実態を把握し、被害を未然防止・拡大防止するため、サイバー攻撃に係る都道府県警の操作の指導調整、情報収集及び総合的な分析を行うため、2013年５月、警察庁警備局へ設置したセンター。
	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。
	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	サイバーテロやハイテク犯罪に対し,警察と企業の協力体制を強化するため設立された協議会。
	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」策定にあたっての指針（第３版）	2010年５月11日情報セキュリティ政策会議決定、2013年２月22日改定。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。2014年度に改訂予定。

	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。重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画。「重要インフラの情報セキュリティ対策に係る第２次行動計画」（2009年２月３日情報セキュリティ政策会議決定、2012年４月26日改定）の基本的な骨格を維持しつつ、課題等を踏まえた修正・補強を行ったもの。
	重要インフラ分野	情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油。重要インフラの情報セキュリティ対策に係る第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。
	情報セキュリティ月間	情報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月に実施しており、情報セキュリティについて様々なイベントの開催等を行っている。
	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。
	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。
	情報の格付	情報の重要性や価値等を主体的にランク付けすること。情報を作成又は入手し管理を監視する前に、機密性、完全性、可用性の観点から決定する。
	情報の取扱制限	情報を取り扱う際の制限事項。機密性、完全性、可用性の観点から複製禁止、持出禁止、再配布禁止、暗号化、読後破棄などを決定する。
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。
	スマートメーター	通信機能を備え、電力使用量などを自動送信したり、家電製品等を制御可能な次世代の電力メーター。
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。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、2013年末現在、10分野で15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、また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（Telecom Information Sharing and Analysis Center Japan）。通信事業者等が中心となって設立した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	内閣官房情報セキュリティセンター	2005年に情報セキュリティ政策に係る基本戦略の立案その他官民における統一的、横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行うために設置。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 Information Security Center）。
	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またはハードウェア。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	最初から標的型メールを送付するのではなく、業務との関連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標的型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、損失などの回避または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。