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 23 年度）

平成 24 年5月 30 日

情報セキュリティ対策推進会議

目　　次

はじめに

情報セキュリティ対策推進会議（議長：竹歳誠内閣官房副長官）（以下「CISO 等連絡会議」という。）は、本日、平成 23 年度の政府機関における情報セキュリティに係る年次報告（以下「本報告」という。）を取りまとめ、情報セキュリティ政策会議（議長：藤村修官房長官）（以下「政策会議」という。）に報告することとなった。

本報告は、昨年度に引き続き二度目の報告となる。「情報セキュリティ２０１１」（平成 23 年７月８日、政策会議決定）において、「各府省庁の最高情報セキュリティ責任者（Chief Information Security Officer(CISO)）が中心となって能動的に改善を図っていく枠組み」とされている各府省庁の「情報セキュリティに係る年次報告書」が、本年度、初めて本格的に策定された。「情報セキュリティ２０１１」において、各府省庁の年次報告書等を通じて、各府省庁及び政府機関全体の情報セキュリティ対策の実施状況に係る評価を内閣官房が行い、本報告として取りまとめることとされている。

内閣官房は、以下の基準群に照らして、平成 23 年４月１日から平成 24 年３月 31 日までの期間に係る、府省庁（法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関若しくはこれらに置かれる機関 ）（除く復興庁）と政府機関全体を対象として、情報セキュリティ対策の実施状況について評価を行った。

参照した基準群（以下「統一基準群」という。）

- 政府機関のための情報セキュリティ対策のための統一規範（平成 23 年４月 21 日）
- 政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針（平成 23 年４月 21 日）
- 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（平成 23 年４月 21 日）
- 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 23 年４月 21 日）

対策実施状況の評価に当たり、まず、情報セキュリティ上のリスク評価を行わなければならない。

そのため、本報告書では、第一章で、平成 23 年度の内外の情報セキュリティの動向を概観する。次に第二章で、政府の取組について各府省庁の年次報告書に記載された対策実施状況報告、重点検査報告等に基づき検討し、最後に次年度に取り組むべき課題等について述べる。

本報告は、政府機関の情報セキュリティ対策の評価を行うことで政府機関の情報セキュリティ対策の向上を目指すことを主な目的としている。加えて、後述するように、平成 23 年度は、我が国の社会全体がこれまでにないほどの情報セキュリティ上の脅威にさらされていることが明らかになった一年でもあり、政府機関と地方公共団体・企業等の連携を強化するなどして我が国の情報セキュリティを向上させることが求められており、地方公共団体・企業等や家庭における情報セキュリティ対策のために、本報告書の政府機関の取組が参考となることを期待している。

第1章 平成 23 年度の情報セキュリティに関する動向と政府機関の取組

第１節 国内外における情報セキュリティに関する動向

平成 23 年度は、東日本大震災による影響への対応、並びに民間企業からの個人情報の大量流出に始まり、行政府や立法府を含む政府機関等（以下本章においては「政府機関等」という。）や企業等、広く社会への標的型攻撃が顕在化した年であった。

近年、サイバー攻撃を行う者の目的は多様化が進んでおり、愉快犯・技術力の誇示だけでなく、金銭詐取・高度技術等の企業の内部情報の窃取を目的とした攻撃も顕著であり、軍事的な情報収集活動も行われているといわれている。

また、攻撃対象も国民・企業から政府機関等まで幅広くなっており、攻撃手法もサービス不能攻撃（DoS 攻撃）やウェブサイト改ざん、単純なマルウェア感染、フィッシングだけでなく、複数のコンピュータからの DoS 攻撃（DDoS 攻撃）や高度ななりすまし、特定の組織・個人を狙う標的型攻撃のように複雑化・巧妙化が進んでいる。これらの事象について、確立した分類ではないが、一例として図　1－1 のように考えることができる。

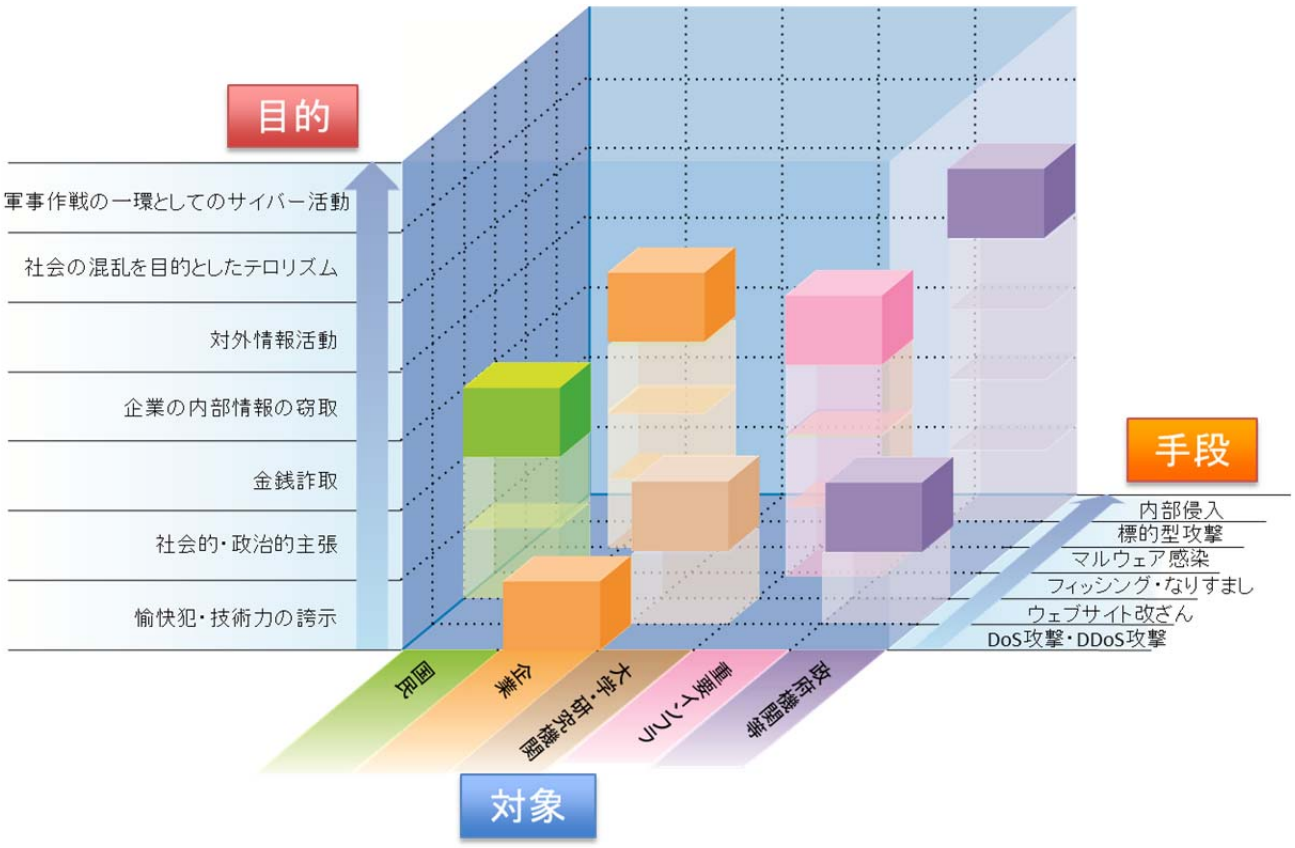


図　1-1サイバー攻撃に関する事象の整理例

以下に、平成 23 年度の我が国の内外における情報セキュリティに関する動向について、上記分類の観点で整理し、概観を述べる。また、東日本大震災による影響、海外の状況及びネットワーク環境の進化による新たな課題についても概観を述べる。

1 巧妙化する攻撃手法

A) 標的型攻撃の顕在化

ア）政府機関等への標的型攻撃

標的型攻撃（複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃）については、かねてから海外で発生事例が報告されていたが、平成 23 年度は、これらが我が国の政府機関等も標的になっていたことが顕在化した年となった。

現在、標的型攻撃の主な手法はメール（以下「標的型攻撃メール」という。）によるものであり、複数の府省庁から標的型攻撃メールが届いていると報告されている。そのうち、総務省及び外務省等では標的型攻撃メールに添付されたファイルを開封し、マルウェアに感染してしまうという事案も発生している。また、行政機関だけでなく、立法府である衆議院及び参議院の公務用メールアドレス宛にも標的型攻撃メールが送信され、院内のシステムがマルウェアに感染してしまうという事案も発生した。（標的型攻撃を含めた、政府機関等における情報セキュリティインシデントに関連する報道事例については、表 1-3 参照。）

今後、標的型攻撃メールの件数は増加することが予想され、また、電話によるフィッシングサイトへの誘導や USB メモリの利用といったメール以外の手法による標的型攻撃が発生する可能性も懸念される。

イ）民間企業への標的型攻撃

標的型攻撃は、政府機関等だけでなく、民間企業に対しても行われている。平成 23 年９月には三菱重工業(株)に対して標的型攻撃メールが送信され、マルウェアに感染し、同社はその事実を公表している。ただし、後日の調査で、防衛及び原子力の保護すべき情報の社外への流出は認められなかったことも同社は公表している。また、(株)IHI、川崎重工業(株)及び三菱電機(株)等でも、同様の攻撃を受けたと報道された。これらは、７月から９月にかけて、世界各国の化学工業や防衛関連企業を狙った標的型攻撃の一部との見方もある。

今後も、企業を狙う標的型攻撃は、大手企業に限らずに対象企業を拡大させながら、増加していくと考えられる。

ウ）時事情報を利用した攻撃（東日本大震災に関する情報を利用した標的型攻撃等）

標的型攻撃は、ソーシャルエンジニアリングの手法を用いるため、その時々で注目されている情報が利用されることも多い。

例えば、東日本大震災の発災後の平成 23 年４月から９月にかけて、震災や原発事故に関する情報の提供を装った標的型攻撃メールが我が国の民間企業等に合計約 540 件送付されたとの報告が警察庁[1]から発表された。

時事情報等を利用してメールの表題、文面を巧妙化させる手法は、今後も進化する

[1] http://www.npa.go.jp/keibi/biki7/231014kouhou.pdf
サイバーインテリジェンスに係る最近の情勢（平成 23 年４月～９月）（警察庁、平成 23 年 10 月 14 日）

と考えられる。

B) 内部ネットワークを経由した侵入（LANの深部、制御システムへの侵入）

標的型攻撃は、攻撃が成功すると情報システム内に潜伏し、更にネットワーク利用者が管理するサーバ（Microsoft社のActive Directoryサーバ、IBM社のNotesサーバ、その他LDAPサーバ等の認証サーバ）へ侵入を試みる事例が報告されている。また、ネットワーク内の他の情報システムへの侵入だけでなく、制御システムへの侵入を行うものもある。

平成20年に発見された「Conficker」は、ファイル共有機能やUSBメモリ等を経由して感染するマルウェアで、複数の亜種が現在も存在し、脅威であると報告されている。

また、平成22年には、特定の制御システムを狙って感染を拡大させるマルウェアとして「Stuxnet」が知られるようになった。Stuxnetは、特定の国の制御システムを狙ったものと考えられているが、平成23年度には、Stuxnetと類似のマルウェアとして「Duqu」が知られるようになった。

なお、インターネットに接続していない制御システムのデバイスや情報システムでも、メンテナンス等の理由によりUSBメモリ等をシステム上の端末に接続する必要がある。StuxnetやDuquは、そのような経路を狙って侵入を試みるため、インターネットに直接接続していない情報システムでもマルウェア感染のおそれがあることに注意が必要である。

C) なりすましの高度化（電子証明書の不正利用）

平成23年9月に、オランダの大手SSL認証局DigiNotar社からウェブサイト用の不正なSSL証明書が発行されるという事案が発生した。これにより、発行されたSSL証明書を利用して、Googleサービスとユーザ間の通信に割り込もうとする攻撃が発生したとの報道があった。なお、影響を受けたのは、イランのIPアドレスが99%以上であると報道されている。

また、平成23年11月には、マレーシアの政府機関が利用する電子証明書が盗まれ、マルウェアへの署名に使われるという事案も発生している。

これらのような事例は、日本国内では発生の報告はまだないが、今後発生する可能性も否定できないことから注意が必要である。

D) クラウドサービスへのDDoS攻撃

平成23年11月に、福岡県や鹿児島県など計約200の地方自治体が利用している電子認証サービスがDDoS攻撃を受ける事案が発生し、各地方自治体のウェブサイトで住民へ提供しているサービスに障害が発生した。これは、大手のクラウドサービス事業者が提供するクラウドサービスを共通的に使用していたものである。

東日本大震災以降、データセンタやクラウドサービスの利用が進んでいるが、情報システムが集約化されることによる、DoS攻撃・DDoS攻撃への脆弱性が露呈した事例と考えられる。

2 攻撃目的の多様化

A) 愉快犯・技術力の誇示、社会的・政治的主張

従来から、企業に対する攻撃は発生しているが、平成 23 年度は、より大規模になってきたと考えられる。代表的な事例は、平成 23 年４月から５月にかけて民間企業グループのウェブサイトからの数千万件を超える顧客情報の漏えいであるが、他にも多くの企業で顧客情報の漏えいを伴う攻撃の発生やウェブサイトの改ざん等が発生している。

攻撃を行う動機も愉快犯的なものや技術力の誇示だけでなく、社会的・政治的主張によるものもあり、多様化してきている。これらには、ハクティビストと呼ばれる、自分達の主義・主張を喧伝するために積極的にクラッキング行為を行う個人・組織等の関与が目立ってきている。

B) 金銭詐取

通信販売やクレジットカード会社等のウェブサイトからのクレジットカード情報等の情報漏えいは引き続き発生しており、実際にカード情報の不正利用が確認される事例も増えてきている。

また、メールの文面や差出人を金融機関等からであるように装うフィッシングメールの送付、個人の端末へのマルウェア感染、並びにセキュリティソフトや診断ソフトを装うが実際には機能しないソフトウェア（詐欺ソフト）をインストールさせる行為等により個人のクレジットカード情報や ID・パスワード等を盗み取ろうとする事例も依然として発生しており、各金融機関では、フィッシングメール等に対する注意を促している。

他にも、システムを使用不能にして、その復旧と引き換えに金銭を要求するソフトウェア（ランサムウェア）の発生事例も報告されている。加えて、海外の政府機関をかたって金銭を要求する事例が国内で発見されており、今後、国内の政府機関等をかたって金銭を要求する事例が発生することも考えられる。

C) 企業の内部情報の窃取、対外情報活動等

海外では企業・政府機関への機密情報の窃取を目的としたサイバー攻撃に関する報道が続いているが、日本国内においても民間企業からの個人情報を含む重要情報の漏えいに関する報道は続いている。

また、平成 24 年３月には大手工作機械製造会社にて、社員が退職間際に設計図データを複製し、持ち出した疑いで逮捕されるという報道もあり、内部犯行で重要情報が窃取される危険性も依然として存在している。

なお、このようなサイバー攻撃を行うのは、個人や犯罪組織だけでなく、国家的な組織の関与も示唆されることが海外にて報道されている。

D) 社会の混乱を目的としたテロリズム、軍事作戦の一環としてのサイバー活動

国民生活や社会経済活動に重大な影響を与えると考えられる重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させてしまうような大規模な被害を発生させるようなサイバーテロの脅威へ備えることが、ますます重要になってきている。

また、外国の軍事組織の作戦の一環としてサイバー攻撃が利用されることを前提に、

各国政府はその対策を検討している。

3 東日本大震災の影響

A) 地震による影響

地震自体の影響としては、首都圏においても事業所で火災が発生したり、一部の地域で液状化現象が発生したりした。また、鉄道の運行が停止したため、徒歩での帰宅を余儀なくされ、震災当日の首都圏では大量の帰宅困難者が発生するなど、交通も長期間、大規模に混乱した。

ただし、政府・行政サービスにおける情報システムに関しては、被災三県（岩手県、宮城県、 福島県）の内陸部で津波の被害を受けなかった地域を含め、耐震基準を満たした建屋の利用、サーバやラックを床に固定するなどしていたことで、倒壊による被害は全体的に少なかったとの報告もあり、地震自体によるものでは大きな被害を受けなかったとも考えられる。しかしながら、机や書庫の倒壊並びに天井板の落下等により、情報システムを利用できなかった事例も報告されている。

なお、建物自体には大きな被害が無かったものの一定期間退去命令が発令されたり、建物が倒壊するおそれから立入禁止とされることで、その間は避難のため業務ができない事例があった。

B) 津波による影響

被災三県の沿岸部を中心に、津波により甚大な被害を受けた。重要インフラにおける主なところでも、空港・鉄道等の施設が津波により被害を受け、情報通信・電力・ガス等の分野でも浸水により電気系統・電源設備等が使用できなくなり、サービスを供給できなくなるという事態になった。

なお、政府・行政サービスにおける情報システムに関しても、役場が津波により水没し壊滅的な被害を受け、戸籍データ等の行政サービスに必要な情報が破損・消失するなどの事態も発生した。また、バックアップデータの保管先も同時に被災してしまい、バックアップデータが利用できなくなった事例も発生した。

C) 停電・計画停電による影響

地震や津波によって発電所や発電設備に大きな被害が発生し、電力の供給不足が懸念されたことから、東京電力の管内において地域を区分して短時間の停電を行う計画停電が繰り返し行われた。

情報システムに関しては、震災発生後２日間程度の停電及び停電に起因するネットワークの停止が続いたり、交通機関の寸断や混乱により情報システムを操作できる者が現地に到着できず、その間は情報システムを運用することができない事例もあった。また、計画停電前に情報システムを停止させる作業が発生し、停止できない情報システムについても自家発電装置の燃料不足が懸念されるなど様々な影響を及ぼした。

4 海外の状況

A) 各国政府の取組

米国 国防総省(DoD)は、平成 23 年 7 月に初のサイバー戦略を公表し、サイバー空間を陸、海、空、宇宙空間に次ぐ第 5 の新たな領域と宣言した。英国も 11 月に「サイバーセキュリティ戦略」を発表しており、各国では、サイバー空間に対する戦略を独自に定義するなどの取組が進められている。

他にも、オーストラリアにおいては、首相府のもとに情報セキュリティセンターを構築したり、法務省や国防省にて政府機関を横断して適用する情報セキュリティポリシーを策定したりする動きがある。また、国防省では、効果的な情報セキュリティ対策のランキングを公開するといった取組も行っている。

なお、情報セキュリティに関連する国際会議も開かれており、様々な議論が行われている。(表 1-1 参照)

表 1-1 平成 23 年度に開催された情報セキュリティに関連する主要な国際会議

年月	出来事	開催地
	主な議題・発表内容	
平成23年	6 月 21 日	日米「2＋2」共同発表	米国(ワシントン)
	Ⅲ. 日米同盟の安全保障及び防衛協力の強化 (1) 抑止及び緊急時の対処の強化 閣僚は，サイバー空間における増大する脅威によってもたらされる課題に日本及び米国が立ち向かうための新たな方法について協議することを決意し，サイバー・セキュリティに関する二国間の戦略的政策協議の設置を歓迎した。閣僚は，サイバー・セキュリティに関する効果的な二国間協力には，政府全体による解決及び民間部門との調整が必要であることを認識した。		
	11 月 1 ・2 日	サイバー空間に関するロンドン国際会議	英国（ロンドン）
	サイバー空間の経済的・社会的便益、サイバー・セキュリティの確保、サイバー空間における国際安全保障等について (サイバー空間の①経済成長と発展、②社会的便益、③サイバー犯罪、④安心・安全なアクセス、⑤国際安全保障について分科会で議論)		
	11 月 21･22 日	第 4 回 日・ASEAN 情報セキュリティ政策会議	マレーシア（クアラルンプール）
	①情報セキュリティ戦略の進捗状況 ②日・ASEAN における情報セキュリティ意識啓発に対する取組の推進 ③情報セキュリティにおける一層の連携強化		

B) ボットネットの閉鎖、容疑者の逮捕等

平成 22 年度は、新種のボットが増加し、それらの感染によるボットネットの拡大が報道されていたが、平成 23 年度は、各国の対処が進み、ボットネットの閉鎖（テイクダウン）や首謀者の逮捕も報道されるようになった。代表的な事例としては、平成 23 年 3 月の Rustock、 7 月の Kelihos といったボットネットの閉鎖が挙げられる。

ただし、今後はボットの潜伏方法やボットネットの構築方法が巧妙化することで、ボットネットが検知されにくくなることが懸念されている。

C) 情報交換の場の構築、情報セキュリティ人材の育成

海外では、情報セキュリティに関する情報交換等を目的としたカンファレンス（国際会議を含む）が多数開催されている。代表的な事例としては、米国で開催されるBlack HatやDEFCON、カナダのCanSecWest等があり、韓国やマレーシア、EU等でも多数のカンファレンスが開催されている。日本においても、PacSecカンファレンスが開催されたり、(独)情報通信研究機構(NICT)、(独)産業技術総合研究所(AIST)、(独)情報処理推進機構(IPA)、JPCERTコーディネーションセンター等の主催でカンファレンスが開催されたりしている。

また、海外では、カンファレンスに付属するイベントとして、情報セキュリティに関するコンテスト(CTF（Capture The Flag）等)も開催されている。日本国内では、若手の情報セキュリティ人材育成の場として、IPAが平成16年からセキュリティキャンプ（平成20年からセキュリティ&プログラミングキャンプに名称変更）を開催してきたほか、和歌山県白浜町で開催される「サイバー犯罪に関する白浜シンポジウム」において併設される情報セキュリティコンテストなど各地で様々な取組が行われていている。

そして、平成24年2月に、国内では初のCTFの全国的な大会となる第1回SecCon CTF(Security Contest Capture The Flag)福岡大会（九州地区）が開催された。今後、地区大会・全国大会が開催され、情報セキュリティ人材の発掘、育成の場の一つとなることが期待される。

5 技術の進歩や利用環境の変化による新たな課題

A) スマートフォン・タブレット端末の利用拡大

PCとほぼ同等の機能を持つスマートフォン･タブレット端末の利用が急拡大している。また、利用者が所有するスマートフォン・タブレット端末を業務に使用するBYOD（Bring Your Own Device）[2]も今後拡大すると予想される。

このような流れに伴い、平成23年5月に日本スマートフォンセキュリティフォーラム（JSSEC）[3]が設立され、12月に「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン(第一版)」[4]が発行された。

なお、スマートフォン・タブレット端末の利用拡大に伴い、取り扱うデータ量も増加しており、キャリアネットワークの通信帯域を圧迫させる一因になっている。また、マルウェアの作成者もスマートフォン・タブレット端末を標的にし始めていることから、マルウェア発見の報告も増加しており、注意が必要である。

他にも、スマートフォン・タブレット端末のアプリケーションのダウンロードサイトには、数十万件に及ぶアプリケーションが公開されているが、中には利用者に意識させ

[2] 「自分のデバイスを持ち込む」の略で、個人が私物の端末を企業内に持ち込んで業務に活用することを指す。
[3] 名称は当時。同組織は平成24年4月、任意団体から「一般社団法人 日本スマートフォンセキュリティ協会」（JSSEC）に改組した。
[4] http://www.jssec.org/dl/guidelines2011_v1.0.pdf
（日本スマートフォンセキュリティフォーラム（JSSEC）、平成23年12月1日）

ることなく、位置情報やアドレス帳情報、ウェブサイト上での行動履歴情報等を外部に送信するアプリケーションも登場してきている。これらの情報から個人の行動が追跡可能であり、プライバシーを守ることができない危険性が考えられる。

B) 暗号の危殆化

暗号アルゴリズム（ハッシュ関数 SHA-1（以下「SHA-1」という。）及び公開鍵暗号方式 RSA の 1024bit 鍵（以下「RSA1024」という。））の安全性低下（暗号の危殆化）について、現在のところ、SHA-1 及び RSA1024 が実運用に影響を及ぼす時間で解読されたとの報告はない。(現在の「暗号の危殆化」の判定は、危険度１。表 １-2 参照)

我が国の政府機関においては、「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 20 年４月 22 日情報セキュリティ政策会議決定)に基づいて、2013 年度末までに新しい暗号アルゴリズムを利用可能な状態に移行させるために準備を進めているところであり、引き続き動向を注視する必要がある。

なお、本移行指針は、コンピュータの計算性能の向上を主な危殆化の要因とした場合の予測(図 １－２参照)に基づいて策定されているが、現在報告されているコンピュータの計算性能の向上トレンド[5]も当時の予測に沿ったものである。また、平成 23 年８月に、CRYPTREC の電子政府推奨暗号リストに記載されている共通鍵暗号アルゴリズム Advanced Encryption Standard（AES）の効率的な攻撃方法が公表されたが、直ちに現実的な脅威につながることはなく、暗号の危殆化には至っていないと考えられる。

表 1-2 SHA-1 及び RSA1024 の安全性に関する危険度の定義

危険度	状態		危険度に応じた対処の例	現在の判定
0	安全	暗号として十分に利用できる状態	なし	
1	危険	理論的な暗号解読アルゴリズムが公開された状態	緊急対応計画の策定等体制を整備	○
2	一定年限後に危殆化	高性能計算機などの利用によって危殆化が実証された状態	状況判断、対策の周知、システム対応を実施	
3	危殆化	十分に短い時間で署名の偽造ができる状態	情報システムの利用停止若しくは別の業務を利用する	

[5] http://www.top500.org/ (www.Top500.org は、全世界で稼働しているスーパーコンピュータの上位 500 位までをリストアップするプロジェクトのウェブサイト。平成 23 年 11 月時点の性能第１位は日本の「京 (K Computer)」で、8.16 Petaflop/s（平成 23 年６月時点）と約 10 Petaflop/s レベルの計算性能を保持している)

表 1-2 は、SHA-1 及び RSA1024 の安全性に関する危険度を段階的に示したものである。
NISC は、危険度の判定に当たっては、
・総務省・経済産業省から提供される情報
・NISC で把握している各府省庁のシステムにおける暗号利用状況等から、
各府省庁のシステム及びシステムで取り扱う情報への影響の程度と範囲を踏まえ、総合的な観点でこれを実施する。

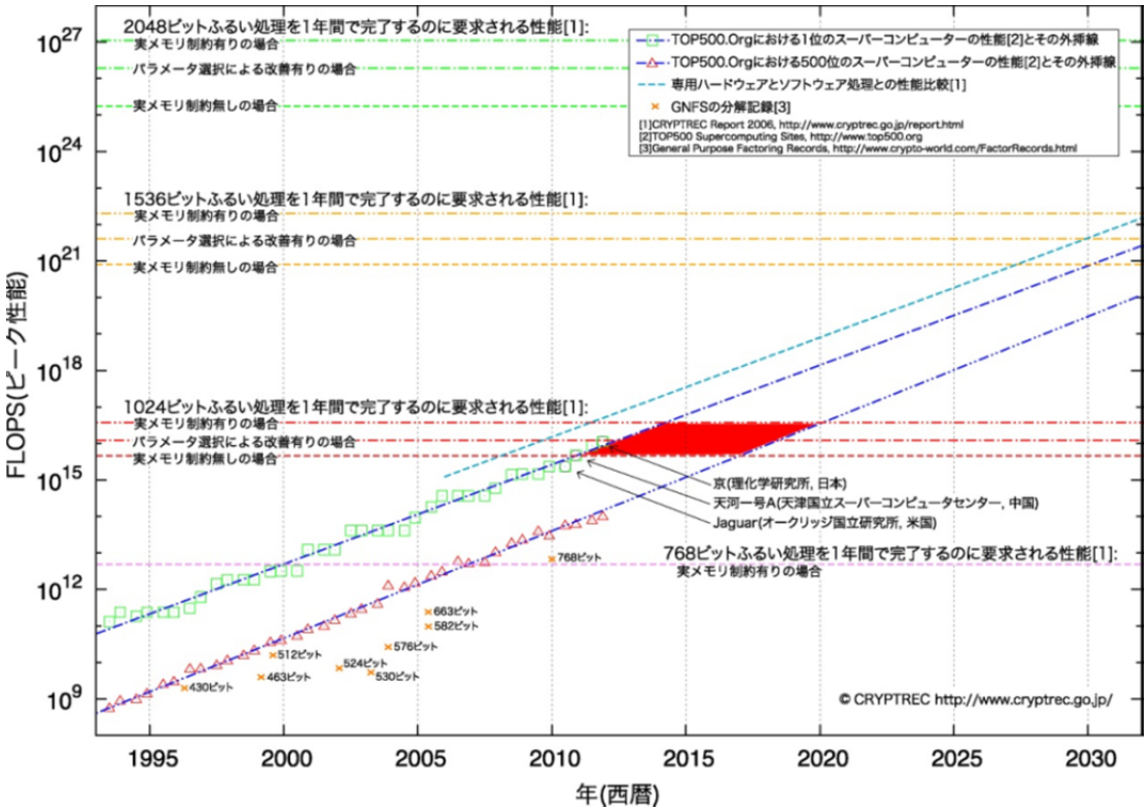


図 1-2 一年間でふるい処理を完了するのに要求される処理性能の予測(平成 23 年 12 月更新)[6]

図 1-2 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青（□）、500 位相当の計算機は紫（△）により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発達を示しており、今後も同様の発展が予想される。また、茶（×）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プロットしている。
2012 年現在、仮にメモリを無制限に利用できる環境を仮定する場合においては、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、京により達成されている。

[6] http://www.cryptrec.go.jp/report/c11_kentou_final.pdf
暗号技術検討会 2011 年度報告書 p32（CRYPTREC、平成 24 年 3 月）

表 1-3 平成 23 年度の政府機関等における情報セキュリティインシデントに関連する報道事例

報道年月		主な報道機関名	報道内容（府省庁・機関名）
平成23年	7月	朝日新聞、産経新聞 東京新聞、毎日新聞 日経新聞、読売新聞	ウェブサイトが大量アクセスにより一時閲覧困難に。（警察庁）
		朝日新聞、共同通信 日経新聞	四国地方整備局職員の端末がウイルス感染し、情報が流出したおそれがあることが判明。（国土交通省）
		産経新聞、読売新聞	５月中、標的型メールが警察庁職員に計 24 通届いていたと公表。分析の結果、不正プログラムによる強制接続先の半数が中国。（警察庁）
	9月	朝日新聞、産経新聞 東京新聞、毎日新聞 日経新聞、読売新聞	東京空港事務所の現役航空管制官が、個人ブログサイトに航空機のフライトプランの画像を掲載しているとの指摘を受け、本格調査開始。（国土交通省）
		朝日新聞、産経新聞 日経新聞、読売新聞	人事院、政府インターネットテレビ、政府広報オンラインの計３サイトが、一時閲覧しづらい状態に。（内閣府、人事院）
	10月	朝日新聞、産経新聞 東京新聞、毎日新聞 日経新聞、読売新聞	衆議院の公務用端末や衆議院内のサーバがマルウェアに感染していたことが判明。（衆議院）
		朝日新聞、東京新聞 毎日新聞、日経新聞 読売新聞	在外公館で運用するコンピュータが、夏以降、マルウェアに感染していたことが判明。（外務省）
		朝日新聞、産経新聞	平成 22 年 11 月に経済産業省職員を装った者から送られたウイルスメールを職員約 20 名が開封していたことを再度報道。（経済産業省）
		読売新聞	９月中旬に標的型攻撃メールが複数送りつけられ、うち１台がマルウェアに感染したことが判明。（内閣官房）
		朝日新聞、毎日新聞 日経新聞、読売新聞	国土地理院の測量用サーバにサイバー攻撃があり、不正に侵入された上で、外部への攻撃を中継する「踏み台」にされたことが判明したと発表。（国土交通省）
	11月	朝日新聞、東京新聞 毎日新聞、日経新聞 読売新聞	衆議院と同様に、参議院の公務用端末がマルウェアに感染していたことが判明。（参議院）
		朝日新聞、東京新聞 毎日新聞、日経新聞 読売新聞	職員用端末が新種のウイルスに感染していたことが判明。（総務省）
		読売新聞	労災などの業務管理を行う情報システムのサーバが、ウイルス対策ソフトを装ったウイルスに感染。（厚生労働省）

	12月	朝日新聞、東京新聞 毎日新聞、日経新聞 読売新聞	ウェブサイト「科学技術週間」の一部が不正に書き換えられたと発表。（文部科学省）
		朝日新聞、東京新聞 毎日新聞、日経新聞 読売新聞	国土地理院の研究開発の成果を公表するページが不正に書き換えられたと発表。（国土交通省）
平成24年	1月	読売新聞	東京電力福島原子力発電所における事故調査・検証委員会及び節電ポータルサイトのウェブサイトが不正に書き換えられていることが判明。（内閣官房）
		読売新聞	ネットアクション 2011 のウェブサイトが不正に書き換えられたと発表。（経済産業省）
	2月	毎日新聞、読売新聞	職員の業務用端末に、マルウェア付きの標的型メール攻撃を受けたと発表。（農林水産省）
		毎日新聞、日経新聞 読売新聞	庁内の端末３台がマルウェアに感染したと発表。（特許庁）
		朝日新聞	関東信越厚生局麻薬取締部は、横浜分室の男性麻薬取締官が、麻薬事件の容疑者１人の供述内容など捜査情報が入った USB メモリを紛失したと発表。（厚生労働省）
		読売新聞	奈良地検は、使用権限のない ID やパスワードを使って地検内の人事情報を閲覧したとして、男性検察事務官を戒告処分にしたと発表。（法務省）

第２節 政府機関に向けた NISC の取組

内閣官房情報セキュリティセンター（以下「NISC」という。）においては、政府機関全体の情報セキュリティ対策の向上及び職員一人ひとりの情報セキュリティ水準の向上を目的として、下記のような取組を進めてきた。

1 情報セキュリティ対策推進会議の開催

各府省庁の最高情報セキュリティ責任者（CISO：各府省庁官房長クラス）からなる情報セキュリティ対策推進会議（CISO 等連絡会議）を開催し、政府機関相互の緊密な連携を図るとともに、政府機関全体の情報セキュリティ水準向上のための取組を推進した。（第２回：平成 23 年５月 31 日、第３回：平成 23 年 10 月 14 日、第４回：平成 24 年１月 19 日、第５回：平成 24 年４月 18 日）

第２回会合においては、「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 22 年度）」が決定された。第３回会合においては、情報セキュリティ対策推進会議の下に「官民連携の強化のための分科会」を置くことが決定された。第４回会合においては、10 月以降３回開催された「官民連携の強化のための分科会」における検討結果が報告され、「情報セキュリティ対策に関する官民連携の在り方について」が決定された。

2 最高情報セキュリティアドバイザー等連絡会議の開催

各府省庁の最高情報セキュリティアドバイザー（民間非常勤等）からなる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、政府機関に共通する課題に対する情報セキュリティに係る専門的な知見からの助言やベストプラクティスの共有等を通じて、政府機関全体の情報セキュリティ対策に関する取組の高度化を推進した。（第２回：平成 23 年４月 28 日、第３回：平成 23 年６月 16 日、第４回：平成 23 年８月３日、第５回：平成 23 年 11 月４日、第６回：平成 24 年１月 26 日、第７回：平成 24 年４月３日、第８回：平成 24 年５月８日）

3 「情報セキュリティ対策に関する官民連携の在り方について」の決定

重要な情報を扱う企業等における情報セキュリティ上の脅威が高まってきていることを踏まえ、情報セキュリティ対策推進会議（CISO 等連絡会議）の下に、情報セキュリティ対策推進会議幹事会の関係省庁構成員等からなる「官民連携の強化のための分科会」を設置し、情報セキュリティ対策における官民連携の強化のために取るべき方策等について検討を行った。分科会は計３回開催され、検討結果が「情報セキュリティ対策に関する官民連携の在り方について」として、情報セキュリティ対策推進会議において決定され、情報セキュリティ政策会議に報告された。分科会における検討結果の概要は、以下のとおり。

・国の安全に関する重要な情報を扱う契約に情報セキュリティ条項を定める。
・各府省庁が Computer Security Incident Response Team（以下「CSIRT」という。）の機能を保有するよう求める。また、企業等においても CSIRT の機能を保有する取組を

推進する。
・政府として一元的に脅威に対処するため、政府 CISO を新たに設置し、NISC センター長をもって充てる。
・大規模なインシデント等により政府として迅速かつ的確に対応すべき事態が発生した際に、他の府省庁への支援が可能となるよう、府省庁間協力のルール作りと NISC の調整機能の整備を検討する。
・官民のネットワーク関係者間の情報共有を NISC において実施する。
・情報セキュリティ人材を育成していく機運を醸成するため、啓発活動を実施する。

4 国の安全に関する重要な情報を取り扱う契約に関する情報セキュリティ要件の記載

国の安全に関する重要な情報を取り扱う契約について、情報処理に係る業務の外部委託にとどまらず、一般の調達等に際しても情報セキュリティ対策を契約で担保するため、「調達における情報セキュリティ要件について」（平成 24 年 1 月 24 日、内閣官房副長官から各府省庁大臣官房長等あて）を発出した。これにより、国の安全に関する重要な情報を国以外の者に扱わせることを内容とする契約を行う際には、情報セキュリティを確保するための整備、取り扱う府省庁の国の安全に関する重要な情報の秘密保持等、情報セキュリティが侵害された場合の対処、情報セキュリティ監査の実施等の情報セキュリティ要件を記載することとした。

5 各府省庁における「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）の作成及び公表

各府省庁の最高情報セキュリティ責任者が中心となり、自組織の情報セキュリティ対策の取組状況を国民へ公表し、各府省庁の参考となるベストプラクティスを共有するなどの取組を通じて、能動的に情報セキュリティ対策の改善を図ることを目的として、平成 22 年度の試行版に続き、平成 23 年度の「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）を作成した。情報セキュリティ報告書は、平成 24 年 5 月の情報セキュリティ対策推進会議の場で報告され、その後各府省庁から公表された。

また、平成 22 年度に引き続き、各府省庁の情報セキュリティ対策に係る推奨事例（ベストプラクティス）が政府機関において共有された。なお、平成 22 年度の推奨事例については、推奨事例とした意図を各府省庁が十分に把握し検討され、さらに多数の府省庁において採用されることで、各府省庁における情報セキュリティマネジメント水準の向上につながり、自律的な情報セキュリティ対策の改善が図られた。

6 「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

標的型攻撃の増加や新たなメディアの利用拡大、東日本大震災の教訓の反映などの昨今の情報セキュリティに係る情報技術、利用環境の変化に対応するため、「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、平成 24 年度版への改定を行った。本統一基準群の改定のポイントは、以下のとおり。

1．新たな脅威への対応・・・標的型攻撃の増加や、東日本大震災の発生の経験等を踏まえて、新たな脅威やリスクへの対応として、標的型攻撃に対する対策や管理者権限の適切な管理、障害・事故等の発生に備えた体制整備や他の組織との情報共有、省庁対策基準と情報システム運用継続計画との整合性確保等の規定を追加。
2．情報技術・利用環境の変化への対応・・・IPv6 技術の導入、共通基盤システムの適切な情報セキュリティマネジメント、情報を取り扱う区域のクラス区分毎の対策等、情報技術・利用環境の変化へ対応するための規定を追加。
3．実務に即した見直し・・・基準運用の実効性向上のため、情報システムの調達時における「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、「基本遵守事項」「強化遵守事項」の区分を廃止し、全ての遵守事項について確実なリスク分析を実施するための改定を実施。

本統一基準群は、「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」は平成 24 年４月 18 日の情報セキュリティ対策推進会議、「政府機関の情報セキュリティ対策のための統一規範」「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」及び「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」は同４月 26 日の情報セキュリティ政策会議において、それぞれ決定された。

7 NISC と関連する公的機関との協力覚書に基づく情報共有の実施

NISC と関連する公的機関((独)情報通信研究機構(NICT)、(独)産業技術総合研究所(AIST)及び(独)情報処理推進機構（IPA)) との間で締結されている協力覚書に基づき、定期的に意見交換を行うことで、逐次、情報セキュリティに係る専門的知見の共有を行った。また、一部の内容については最高情報セキュリティアドバイザー等連絡会議の場において報告、共有を行うなどにより、情報セキュリティに係る研究者・実務家の専門的知見の施策への反映を行った。

8 政府機関における標的型不審メール対処訓練の実施

各府省庁との協力の下、訓練を希望した内閣官房等 12 の政府機関約６万名の政府職員を対象として、標的型不審メール攻撃に関する模擬訓練を行った。訓練対象者に対して事前教育を実施した上で標的型不審メールを送付する模擬訓練を行い、参加府省庁には個別の訓練結果を通知した。訓練後、各府省庁内において適切な事後教育指導を実施している。

さらに、訓練の結果得られた知見については、NISC 主催の各府省庁勉強会において政府機関横断的に情報共有や意見交換を行うとともに、情報セキュリティ政策会議、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の場において報告し、成果を共有した。

9 公開ウェブサーバに対する脆弱性検査の実施

検査を希望した 11 省庁の公開ウェブサーバについて、約 330 画面をサンプル抽出し脆弱

性検査を実施した。検出された脆弱性のうち緊急性の高いものについては、当該府省庁に対し速報を発出し、対策を実施するとともに、検査結果については全府省庁に対して注意喚起及び情報共有を行った。さらに、検査結果は情報セキュリティ政策会議、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の場において報告し、成果を共有した。

10 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

政府機関（.go.jp）をかたるなりすましメールから、国民や政府機関自身を守るため、go.jp ドメインに対し、送信側 SPF 対策（DNS サーバへの SPF レコードの記録）の取組を推進した。その結果、以下のとおり、政府機関全体としての送信側 SPF 設定率の向上により、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が促進された。

（SPF 設定率（政府機関平均））

平成 23 年５月 30 日現在　35.8%　→　平成 24 年３月 31 日現在　97.4%

取組の結果は情報セキュリティ政策会議、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において報告し、成果を共有した。

11 政府職員に対する教育・意識啓発の推進

NISC において、政府機関等を対象とした勉強会の定期的な開催、情報セキュリティに係る教材の提供などの取組により、政府職員の情報セキュリティに対する教育・意識啓発の推進に努めた。特に、平成 24 年２月には政府機関の情報セキュリティ担当官を対象とした意見交換の場を設置し、情報セキュリティに関する課題の共有や、各府省庁の担当者間の交流等が行われた。

また、「官民連携の強化のための分科会」の報告結果を受けて、各府省庁の CSIRT 体制整備に係る取組を支援するため、NISC において、政府機関の CSIRT 体制の要員となる職員のインシデント対応に係る心得等を記載した、常時携帯可能な冊子の雛形を作成し、各府省庁への配布を行った。

12 「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析」の実施及び「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」の改定

平成 23 年３月 11 日に発生した東日本大震災を踏まえて、政府機関の情報システム運用継続の強化を目的として、「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析」を実施した。アンケート調査、現地ヒアリング、有識者検討会等からなる検討を行い、政府機関の情報システム運用継続計画に資する対策を「緊急対策」、「優先的に取り組むべき対策」及び「中長期的対策」として、取りまとめた。

成果については、情報セキュリティ政策会議、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の場へ報告を行い、各府省庁への共有を行った。さらに、調査結果については、政府機関統一基準群（平成 24 年度改定版）へ反映するとともに、本調査により得られた知見や教訓を踏まえて、平成 24 年５月に「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」[7]の改定を行った。

13 スマートフォンの業務利用に関するマニュアルの提供

今後、政府機関においてスマートフォンの業務利用の増加が想定されることを鑑みて、民間団体等で作成されているスマートフォン・タブレット端末に関する既存のマニュアル等を参考として、政府機関統一基準群適用個別マニュアル群として当センターで策定している「モバイル PC の利用手順雛形」を基に、「スマートフォン・タブレット端末の利用手順雛形」[8]の作成を行い、各府省庁に提供した。

14 暗号危殆化に関する緊急避難対応計画に係る発動要件の決定

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の急激な安全性の低下に備え、各府省庁において既に策定済みの緊急避難対応計画（コンティンジェンシープラン）に係る発動要件について検討を行い、最高情報セキュリティアドバイザー等連絡会議の場へ報告を行うとともに、平成 24 年 4 月 18 日の情報セキュリティ対策推進会議の場において決定した。

15 「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」に基づくリスク評価の運用

オンライン手続に応じたセキュリティ確保策として、適切な認証と電子署名を選択するための「ものさし」となる「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」に基づき、オンライン手続所管府省が平成 23 年度に実施したリスク評価の内容の適切さを確保するため、最高情報セキュリティアドバイザー等連絡会議の場において、専門的知見を有する者からの助言を行った。

16 「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」の普及・啓発

政府機関の情報システムについて、情報システムのライフサイクルにおける上流の企画・設計段階から情報セキュリティ対策を考慮し、調達仕様にセキュリティ要件を適切に組み込むために平成 23 年 3 月に NISC が策定した「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」について、各府省庁における活用を推進するため、NISC において、各府省庁に対する普及・啓発に係る支援を行った。

17 政府横断的な情報収集・分析システム（GSOC）による監視

[7] http://www.nisc.go.jp/active/general/itbcp-guideline.html
「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」の改定について（NISC、平成 24 年 5 月 11 日）
[8] http://www.nisc.go.jp/active/general/pdf/dm5-04-111_sample.pdf
スマートフォン・タブレット端末の使用手順雛形（NISC、平成 24 年 4 月）

政府機関の情報システムに対するサイバー攻撃等への対処を図るため、政府機関情報システムの 24 時間監視を行っている政府横断的な情報収集・分析システム（GSOC）の継続的な運用を行った。さらに、政府機関に対するサイバー攻撃等に関する情報収集を強化し、政府機関全体としての緊急対応能力の向上を図るため、分析・解析能力の強化や分析結果等の情報共有の推進を行った。また、訓練等を通じて緊急時の連絡体制を確認し、運用の実効性を確保した。

18 「情報セキュリティ人材育成プログラムを踏まえた 2012 年度以降の当面課題等について」の策定

「情報セキュリティ人材育成プログラム」(2011 年 7 月情報セキュリティ政策会議決定)を踏まえて情報セキュリティ政策会議の下に設置された「普及啓発・人材育成専門委員会」において、「情報セキュリティ人材育成プログラムを踏まえた 2012 年度以降の当面の課題等について」を取りまとめた。本報告書案において、以下のとおり、政府機関の情報セキュリティ担当者に係る人材育成に関する課題及び今後実施すべき施策が示されている。

① 組織内 CSIRT 等の設置、サイバーインシデント版の DMAT の育成
- CSIRT 要員の育成等
- サイバーインシデント版の DMAT の育成

② 情報セキュリティリスクに確実に対応できる職員の採用・育成
- 人事ローテーションの工夫
- 優秀な外部人材の活用
- 政府機関や独立行政法人等をハブとしたセキュリティ人材のネットワーク形成

③ 政府職員全体の情報セキュリティ意識の啓発と能力の底上げ
- 訓練・研修の充実
- 公務員採用時における情報セキュリティ関連素養の確認

19 「情報セキュリティ月間」における情報セキュリティ対策の普及・啓発

毎年２月の「情報セキュリティ月間」につき、平成 24 年２月においても、関連行事の開催、情報発信、官民連携の推進等の取組により、以下のとおり、政府、企業及び国民各層に対して、情報セキュリティ対策に係る普及・啓発を行った。

A) 情報発信

- 「国民を守る情報セキュリティサイト」の更新
- SNS（ソーシャルネットワーキングサービス）及びメールマガジンの活用
- インターネットテレビ番組の作成
- ポスター、インターネットバナー、ステッカーの作成、配布

B) 関連行事の開催

- 「国民を守る情報セキュリティシンポジウム」の開催
- 政府機関職員向け勉強会の開催
- 大規模サイバー攻撃事態等対処訓練の実施

・全国ブロック別イベントの開催

C) 官民連携の取組

・「国民を守る情報セキュリティサイト」リンク用インターネットバナー、民間企業等のバナーを相互のウェブサイトに掲示
・ソーシャルネットワーク、メールマガジン等の活用

（ステッカー）

（インターネットバナー(一例)）

（ポスター）

20 その他（NISC から各府省庁への注意喚起の事務連絡発出等）

平成 23 年度に発生した事象の内、NISC で緊急性が高いと判断した脆弱性等については、表 1-4 のとおり政府機関に対し事務連絡を発出し、迅速な注意喚起を行った。

表 1-4 平成 23 年度に発出した事務連絡

年月日		発出した事務連絡
平成 23 年	4 月 5 日	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
	9 月 13 日	電子政府推奨暗号の危殆化対応について（注意喚起）
	10 月 26 日	情報セキュリティ対策の推進について（要請）（※衆院・参院等のオブザーバ機関に向けた要請）
	10 月 27 日	「電子政府利用促進週間」における情報セキュリティ対策の周知について（依頼）
	11 月 22 日	政府情報システムに係る IPv6 対応時の注意事項について
	12 月 21 日	システム管理権限を狙った辞書攻撃、ブルートフォース攻撃への対処について
	12 月 21 日	ネットワーク管理者を管理するサーバのセキュリティ対策の徹底について

平成 24 年	1 月 19 日	公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について
	1 月 30 日	外部委託により構築・運用しているウェブサイトの情報セキュリティ対策について
	2 月 15 日	検索サイトを悪用した政府サイトを騙る事例に関する注意（注意喚起）

A) 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

震災対応の中で、国、地方公共団体等におけるソーシャルメディアの利用が増加していることから、当面留意が必要な事項について示したもの。

B) 電子政府推奨暗号の危殆化対応について（注意喚起）

電子政府暗号リストに記載されている共通鍵暗号 AES の安全性に関する見解が示されたことを受け、電子政府推奨暗号の危殆化に係る注意喚起を行うもの。

C) 情報セキュリティ対策の推進について（要請）

国会議員や政府機関への情報セキュリティ上のリスクが顕在化している状況を踏まえ、情報セキュリティ対策推進会議等オブザーバ機関に対して、NISC の取組も参考の上、情報セキュリティ対策の推進を要請するもの。

D) 「電子政府利用促進週間」における情報セキュリティ対策の周知について（依頼）

電子政府利用促進週間の実施に当たり、政府機関職員に対して、改めて情報セキュリティ対策の周知徹底を求めるもの。

E) 政府情報システムに係る IPv6 対応時の注意事項について

政府機関のウェブサイトや電子政府システムを始めとする外部と直接通信を行う情報システム等については、IPv6 移行に係るセキュリティ対応が喫緊に必要であることを鑑みて、政府情報システムの IPv6 対応時の注意事項を取りまとめたもの。

F) システム管理権限を狙った辞書攻撃、ブルートフォース攻撃への対処について

最近の標的型攻撃において、辞書攻撃、ブルートフォース攻撃と思われる手段で、組織内の各種サーバの管理者権限が奪取され、被害拡大する事例が見受けられることから、適切な管理者権限の設定を推奨するもの。

G) ネットワーク管理者を管理するサーバのセキュリティ対策の徹底について

最近の標的型攻撃において、組織内の各種サーバの管理者権限が奪取され、被害拡大する事例が見受けられることから、ネットワーク管理者を管理するサーバについて適切な設定を推奨するもの。

H) 公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について

NISC が 11 府省庁を対象に行った公開ウェブサーバ脆弱性検査において複数の府省庁で確認された脆弱性について注意喚起を行い、各府省庁の公開ウェブサーバの対策を推奨するもの。

I) 外部委託により構築・運用しているウェブサイトの情報セキュリティ対策について

政府機関から外部の事業者に構築・運用を委託したサイトが改ざんの被害に遭ったことを踏まえ、政府機関が外部委託等により構築・運用しているウェブサイトの情報セキュリティ対策について確認を求めるもの。

J) 検索サイトを悪用した政府サイトをかたる事例に関する注意（注意喚起）

政府機関になりすましたウェブサイトが検索サイトに表示される等、検索サイトを悪用した行為に対処する必要があることから、当該事例への対策、職員への注意喚起について示したもの。

第2章 政府機関の取組の評価

第１節 各府省庁における取組の概況

1 取組概況

本節では、各府省庁が作成した情報セキュリティ報告書を概観し、平成 23 年度に実施した情報セキュリティ対策についての概況を報告する。ここで紹介した各府省庁における取組の詳細については、各府省庁のホームページ又は NISC のホームページで公開している各情報セキュリティ報告書を参照していただきたい。

A) 全体として

各府省庁の情報セキュリティ報告書については、「情報セキュリティ報告書専門委員会報告書～政府機関の能動的な情報セキュリティ対策のために～」[9]（※１）の報告書への記載事項として示された項目及び構成を踏まえて作成されている。内容については、各組織の取組が広く国民から適正に評価されることを目指すものとするため、適宜図や表を用いて分かりやすいものとなるよう工夫されている点も見られる。しかし、今回各府省庁の情報セキュリティ報告書が公表されることを踏まえ、自組織における報告書と他府省庁の報告書を比較することで、引き続き各府省庁において足らざるを補う取組を行う必要がある。各報告書に記載された取組の概況と主な取組事例については次の項目以降で紹介する。

B) 平成 23 年度における新たな取組

各府省庁の情報セキュリティ報告書より、平成 23 年度に行われた新たな取組の傾向として、首都直下型地震の発生等の不測の事態に備えた業務継続計画の策定や CSIRT 等インシデント対応体制の強化に関する取組が多く見られた。主な取組事例を以下に掲げる。

なお、主な取組事例において、府省庁名の後に記載したページ番号は、当該取組事項がその府省庁の情報セキュリティ報告書の中で記載されているページ番号を示す。

（主な取組事例）

- 首都直下型地震等の不測の事態に備え、業務継続計画を策定、情報システムに係る危機管理の強化（文部科学省 P7, 17）
- 首都直下地震を想定した「金融庁業務継続計画」については、東日本大震災の発生を踏まえ、平成 23 年 12 月に職員の参集体制の強化等、所要の改定を実施（金融庁 P15）
- 重要業務の継続を確保する観点から、災害時対応情報システムを沖縄県に設置（消費者庁 P10）

[9]平成 21 年 9 月 11 日情報セキュリティ政策会議情報セキュリティ報告書専門委員会決定

・ 情報システム運用継続計画の策定（農林水産省 P16）
・ 省内の CSIRT 体制の充実と関係職員への研修・演習の実施（外務省 P1,8）
・ 情報漏えいを防止する観点から、内部ネットワークについて、従来取得してきた外部記録媒体の証跡に加え、ファイル操作、印字等の証跡等新たに取得する項目を追加（警察庁 P6）

C) 従来からの取組の強化（教育・啓発／調達・外部委託）

「教育・啓発」

教育・啓発の関係では、多くの府省庁で e ラーニング研修が導入され、受講者管理を行うことで、未受講の職員に対するフォローまで適切に管理されている様子が見られた。さらに、教育の効果を高めるため、理解度確認テストを実施するなど、職員の理解度をチェックするといった取組も見られた。教育教材についても、多くの府省庁で職員の知識や役職別に複数種類準備することや、教材の一つとして NISC から随時提供される脆弱性情報が活用されている。また、それら教材については多くの場合、各府省庁のイントラネットの掲示板上に整備されている。主な取組事例を以下に掲げる。

（主な取組事例）

・ e ラーニングについては、受講の有無を定期的に確認し、実施時期の通知後の一定期間（１か月以上）e ラーニングを未受講のままである職員に対しては、受講促進メールを送信することにより、受講促進（内閣府 P12）
・ e ラーニングを利用した教育コンテンツについて、受講の有無、確認テストの成績等の受講状況を管理し、理解度の確認を実施（経済産業省 P26）
・ 職員をポリシーで規定する各役割に応じた教育コースの設定。職員のポリシーへの理解度を深めるため、平成 22 年度と比べテストの設問数を増やすとともに、その難易度の高度化。未受講者に対する督促を行うなど適正な受講者管理を実施（文部科学省 P10）
・ 職員の情報セキュリティ対策についての知識，経験及び理解度に応じ，初級用と中級用の教育教材を作成（宮内庁 P12）
・ 役割に応じた教育教材の整備、教育受講状況の管理（環境省 P16,17）
・ 情報セキュリティ関係の資料をワンストップ化し、職員がいつでも必要な資料を閲覧できるように、省内イントラネットのトップページにバナーを設け、情報セキュリティコーナーとして、適宜内容の追加・見直し（経済産業省 P19）
・ NISC から提供される「不審メール情報」の全職員に向けた情報発信や注意喚起、これに加えた不審なメールを受け取った場合の対処方法等についての周知（公正取引委員会 P9）
・ 新規採用者等向け研修、情報セキュリティに関する相談会の開催、最高情報セキュリティアドバイザーによる研修等の開催（総務省 P12）
・ 教育した内容の浸透度・理解度を確認するため，これまでのチェック形式による確認を本年度から質問形式に変更（法務省 P11）
・ 全職員に情報セキュリティに関する研修を浸透させるため、情報セキュリティ研修を年度中に12回開催し、最近頻発している標的型攻撃の概要、対応策も説明（金融

庁P2,13）
- NISCや情報システム管理運用委託業者等から提供される脆弱性情報、ウイルス情報、不審メール情報等を省内電子掲示板に掲載し、重要性又は緊急性の高い情報については適宜全職員向けにメールで注意喚起（文部科学省P11）
- 職員の情報セキュリティ意識の向上のため、①全ての職員を対象とした集合研修を18回にわたって実施、②常時自習が可能なeラーニングの研修教材を見直し、③課室長や情報システム管理課室向けの研修を実施するなどの取組を実施（財務省P10）
- 毎年２月を「防衛省情報セキュリティ月間」と定め、平成23年度においては年度末までに換装を行う情報システムの利用者に対する取り扱い教育時に、情報システムの特性に合せた情報セキュリティ教育を実施（防衛省P15）

「調達・外部委託」

NISC で策定した「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」の活用を促進するための研修を NISC と連携して行うことや、外部委託を実施する際の実施手順書等を作成するなどして委託先を適切に管理している取組が複数みられた。主な取組事例を以下に掲げる。

（主な取組事例）
- 「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」の活用を促進するための研修を、NISC との連携のもと、教育の一環として実施（厚生労働省 P10、国土交通省 P14）
- 委託先が受託業務を実施する際の情報セキュリティ対策に関して、契約時、実施時、納品時それぞれにおいて遵守すべき事項を記載した調達仕様書のひな型を整備しその適用を実施（経済産業省P27）
- 内閣法制局情報セキュリティポリシーに基づき、調達仕様書や契約書などの記載内容により、委託先の情報セキュリティ対策の実施状況を確認するなど、委託先の管理を実施（内閣法制局P9）
- 情報処理業務を外部委託によって行う際に課室情報セキュリティ責任者等が行う手続や，情報セキュリティの観点から調達仕様に含めるべき事項を示した手順書を作成（公正取引委員会P14）
- 調達に際し、CIO補佐官への相談会を開催し、調達仕様書案等の妥当性確認を行うとともに、情報セキュリティ要件についても確認を実施。（総務省P13）
- 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（法務省P13）
- 省内職員が情報システムのライフサイクルを通じ、要件定義、設計・開発、運用の各段階における調達において、適切なセキュリティ要件を策定するためのガイドラインを作成（文部科学省P11）
- 「外部委託における情報セキュリティ対策実施手順書」をまとめており、その中では、調達仕様書への記載例も掲載。調達担当者はこれをカスタマイズして活用し、これにより記載事項の標準化（厚生労働省P14）
- 昨年夏のサイバー攻撃事案の事実関係を踏まえ、防衛省の調達における情報セキュリティに関する特約条項等を平成23年12月に改正し、契約企業に対し、保護を要す

る情報の取扱いの厳格化、人的教育の徹底等を図り対策を強化（防衛省P16,17）

D) その他

上記のほか、各府省庁における以下のような取組が見られた。主な取組事例を以下に掲げる。

（主な取組事例）

- LAN 端末の電子メールソフト、文書作成ソフト等に、情報の格付及び取扱制限の表示フォームを自動付与する機能を導入（人事院 P2,文部科学省 P12）
- 統一管理基準で規定された組織以外に、情報セキュリティ対策をより推進するため、情報セキュリティ副責任者、情報セキュリティ連絡担当者を設置（宮内庁 P6）
- 外部に公開している全ての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、脆弱性の検出状況について推奨する対策等とともに担当者に通知し、脆弱性への対応が全て完了するまでフォローアップを実施（総務省 P1,10）
- 職員用端末へのセキュリティ対策シールの貼付（総務省 P13）
- 自己点検結果の正確性向上のため，自己点検に関する監査の対象を地方官署に勤務する職員まで拡大（法務省 P2,9）
- 毎年度、省内の情報システムの整備・運用状況の調査を行い、保有する情報システムに関する情報を把握。緊急時における連絡体制の整備やソフトウェアにおける脆弱性に係る技術的支援等、収集した情報を有効に活用するため、情報資産台帳の整備を実施（文部科学省 P6）
- 委託先における情報セキュリティ対策の履行状況についての監査等外務委託先の適正な管理（文部科学省 P9）
- ゴールデンウィーク、夏季休暇集中期及び年末年始の前や省内外の情報セキュリティ事案発生時等の機会をとらえ、緊急時連絡体制の再確認を行ったほか、最新の情報セキュリティを取り巻く状況を踏まえ、障害・事故等対処手順書を改訂（厚生労働省 P22）
- 職員が取り扱う行政情報をよりきめ細かく管理するという観点から、情報の機密性の格付区分において、政府機関統一基準で示された３段階の区分をさらに細分化して、「機密性２情報」を「機密性２Ａ情報」と「機密性２Ｂ情報」の区分に分割して、情報の機密性の格付を４段階の区分（農林水産省 P17）
- 情報漏えい防止サービス（PDF ファイルに対して細かくアクセス制限の設定を可能とする仕組み）の利用周知、暗号化機能付き USB メモリの導入、e ラーニングシステムの機能を活用した情報セキュリティ対策実施状況の自己点検の自動化（経済産業省 P28）
- セキュア USB メモリ、オンラインストレージシステムの導入（環境省 P18）
- システム構築時の技術者向けガイドラインの導入（環境省 P18）
- USB デバイス管理の導入や監査証跡の取得拡充等情報システムへのセキュリティ対策の強化、所持品検査等の特別検査の実施（防衛省 P18,19）

第２節 対策実施状況報告の評価

1 対策実施状況報告の目的

各府省庁は、「政府機関の情報セキュリティ対策のための統一規範」（平成 23 年４月 21 日情報セキュリティ政策会議決定）に基づく自府省庁の情報セキュリティ対策の実施状況を把握し、情報セキュリティ対策の改善に結びつける。

NISC は、各府省庁の情報セキュリティ対策の実施状況を取りまとめ、政府機関全体として分析・評価し、課題及びその改善に向けた今後の取組について報告する。

2 実施対象

対策実施状況報告は、「政府機関の情報セキュリティ対策のための統一規範」の第三条から第二十四条に定められた取組全般を対象範囲としている。

平成 23 年度は、従来の全取組項目を対象とした点検から、重要又は実施率が低い情報セキュリティ対策の取組項目を対象とした重点的な点検に変更することで、対策実施状況報告に係る点検者の意識改善及び作業の一層の効率化を図ることとした。そのため、当該報告の対象項目は、政府機関の情報セキュリティ対策のための統一規範の条項のうち NISC が指定した項目とした。具体的には、以下のとおり。

表 2-1 対策実施状況報告の実施対象

主体		対象職員	対象項目
最高情報セキュリティ責任者	責任者等	全て対象[10]	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
情報セキュリティ監査責任者・実施者			
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・管理者[11]	システム責任者等		
行政事務従事者	左記同様		

3 実施期間

平成 23 年７月から平成 24 年３月

（点検の実施時期については、各府省庁の実情に応じ、最適な時期を設定）

[10] 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。

[11] 「情報システムセキュリティ責任者・管理者」には、「権限管理を行う者」を含む。

4 実施方法

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遵守事項に定められた情報セキュリティ対策の実施主体が当該対策を適切に措置しているか否かを統計的に把握するために、主体ごとの対策実施状況について、各府省庁において把握・集計した上で NISC に報告し、NISC においてその結果を分析・評価した。

5 政府機関全体の評価

A) 対策実施状況報告の結果

平成 23 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。

ア) 把握率

把握率は、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表す。

表 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
平成 23 年度	99.6%	99.7%	99.8%	99.6%

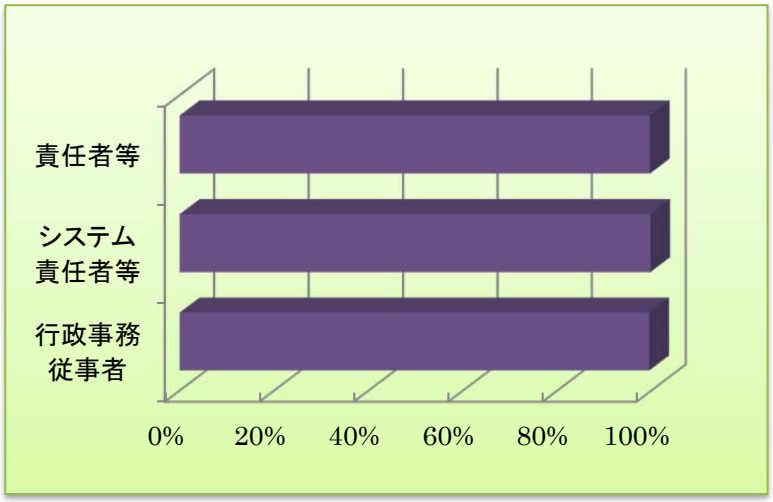


図 2-1 主体別の把握率

イ）実施率

実施率は、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を表す。

表 2-3 主体別の各点検項目の実施率の平均

	全主体平均	責任者等	システム責任者等	行政事務従事者
平成 23 年度	99.0%	99.5%	98.6%	95.9%

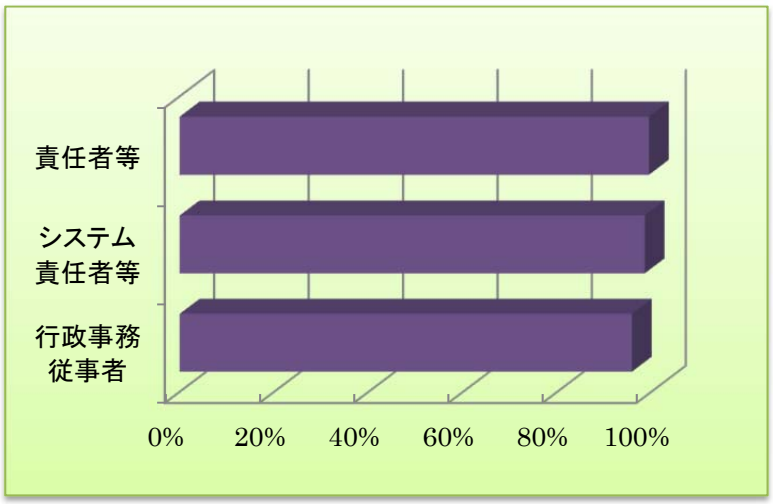


図 2-2 主体別の各点検項目の実施率の平均

ウ）到達率

到達率は、各主体の遵守事項のうち高水準の実施率（実施率 100%、同 95%以上、同 90%以上）を示す遵守事項の割合を表す。

表 2-4 主体別の到達率

		全主体平均	責任者等	システム責任者等	行政事務従事者
平成23年度	実施率100%の遵守事項の割合	86.4%	97.2%	79.6%	23.3%
	実施率95%以上の遵守事項の割合	93.7%	98.1%	89.0%	75.0%
	実施率90%以上の遵守事項の割合	96.7%	98.8%	95.0%	85.8%

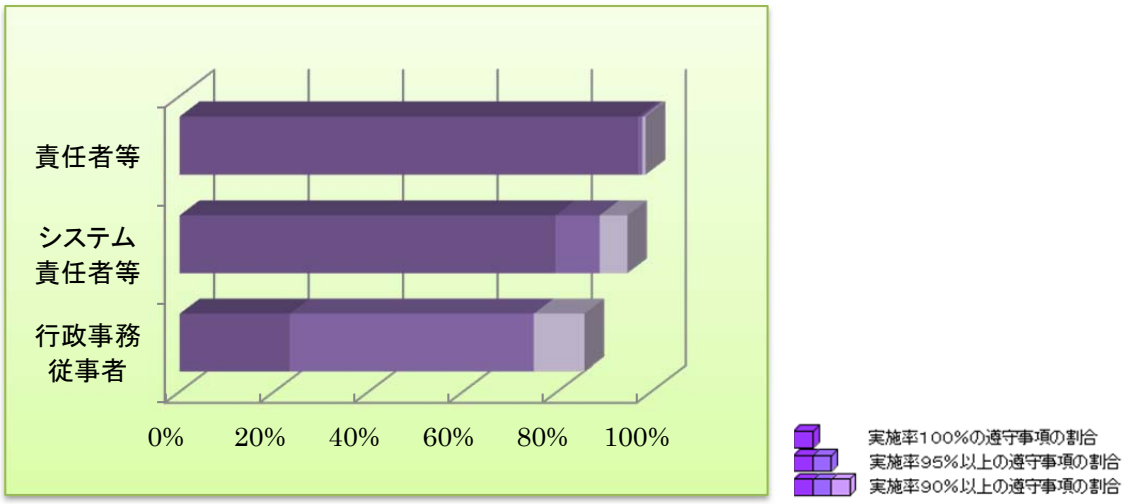


図 2-3 主体別の到達率

B) 所見

・全主体平均の把握率は 99.6%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かんがみれば、全体的に高い水準を達成したといえる。しかしながら、対策実施状況の把握は、PDCA サイクルにおける C（評価）のプロセスに相当し、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、政府機関全体で把握率 100%を達成すべく、今後更なる向上が望まれる。

・責任者等の実施率は 99.5%となっており、対策の浸透が認められる。ただし、これらの者が実施すべき対策は、職員の行動の基礎となる規程の整備などといったものであり、その重要性にかんがみれば、本来、全ての対策が実施されているべきであり、更なる浸透が望まれる。

特に、課室情報セキュリティ責任者は、行政事務従事者に対して情報セキュリティに関する教育を行わなくてはならないとされているが、当該項目の実施率が低い府省庁が散見された。行政事務従事者に適切な情報セキュリティ対策を日々実施させるためには、情報セキュリティ対策に関する教育を通して、自らの責務を自覚させることが不可欠であることから、なお一層の取組が必要と考えられる。

・システム責任者等の実施率は、98.6%となっており、対策の浸透が認められる。ただし、行政事務で取り扱うほとんどの情報は情報システムを活用しており、情報システムには万全の情報セキュリティ対策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、95.9%となっており、対策の浸透が認められる。ただし、一部の項目には十分といえない項目がみられる。「情報の取扱い」に関する項目のうち、特に「情報の作成と入手」については、まだ取組が不十分な省庁が多く、課題が認められる。このため、取組が進んでいる府省庁においてはこれを維持・向上し、遅れている府省庁においては改善措置の速やかな実施が求められる。

・全主体平均の到達率は「実施率 100%の遵守事項の割合」が 86.4%となった。特に、行政事務従事者においては、「実施率 100%の遵守事項の割合」が 23.3%、「実施率 90%以上の遵守事項の割合」が 85.8%となった。行政事務従事者の到達率が他の主体と比較して低い値になった理由は、従来特に実施率が低かった「情報の取扱い」に関する項目を重点的に点検したためである。また、自己点検票のひな型に自己点検時の事前教育教材を追加し、点検実施者が点検項目を理解しやすいように改善したことにより、より実態に即した精度の高い点検が実施できたためであると考えられる。

今後も引き続き自己点検票の改善を図り、より正確に実態を把握し、取組が十分でない項目についての情報セキュリティ対策を行うことで、政府機関全体の情報セキュリティレベルの向上を推進していく。

6 府省庁別の評価

A) 評価方法

各府省庁の把握率及び実施率について、NISC で ABCD 評価を行った。ABCD 評価の見方は、図　2－4のとおり。

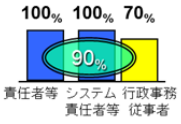
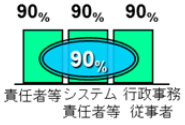
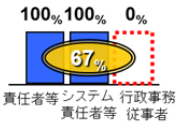
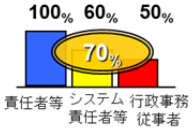
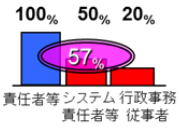
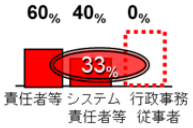
評価基準	把握率及び実施率	概要	評価パターン例
A	100%	適切に実施すべき対策について、全ての項目で統一基準群に準拠した対策が実施されている。	
B	80%≦x＜100%	適切に実施すべき対策について、概ね全ての項目で統一基準群に準拠した対策が実施されているが、一部の項目で不十分なものが含まれている。	 
C	60%≦x＜80%	適切に実施すべき対策について、不備の項目が一部に見られるなど、対策が遅れている。	 
D	60%未満	適切に実施すべき対策について、不備の項目が相当数見られるなど、対策が著しく遅れている。	 

図 2-4 対策実施状況報告の ABCD 評価

B) 把握率及び実施率の評価結果

平成 23 年度の把握率及び実施率（府省庁別）の評価は表　2-5 のとおり。

表　2-5　把握率及び実施率の評価結果（府省庁別）

府省庁名	把握率の評価	実施率の評価
内閣官房	A	B
内閣法制局	A	B
人事院	A	B
内閣府	A	A
宮内庁	A	B
公正取引委員会	A	B
警察庁	A	A
金融庁	A	B
消費者庁	A	B
総務省	B	B
法務省	A	A
外務省	A	B
財務省	A	B
文部科学省	A	B
厚生労働省	A	B
農林水産省	B	B
経済産業省	B	B
国土交通省	A	B
環境省	B	B
防衛省	A	A

（参考）各府省庁の対策実施状況報告の集計結果

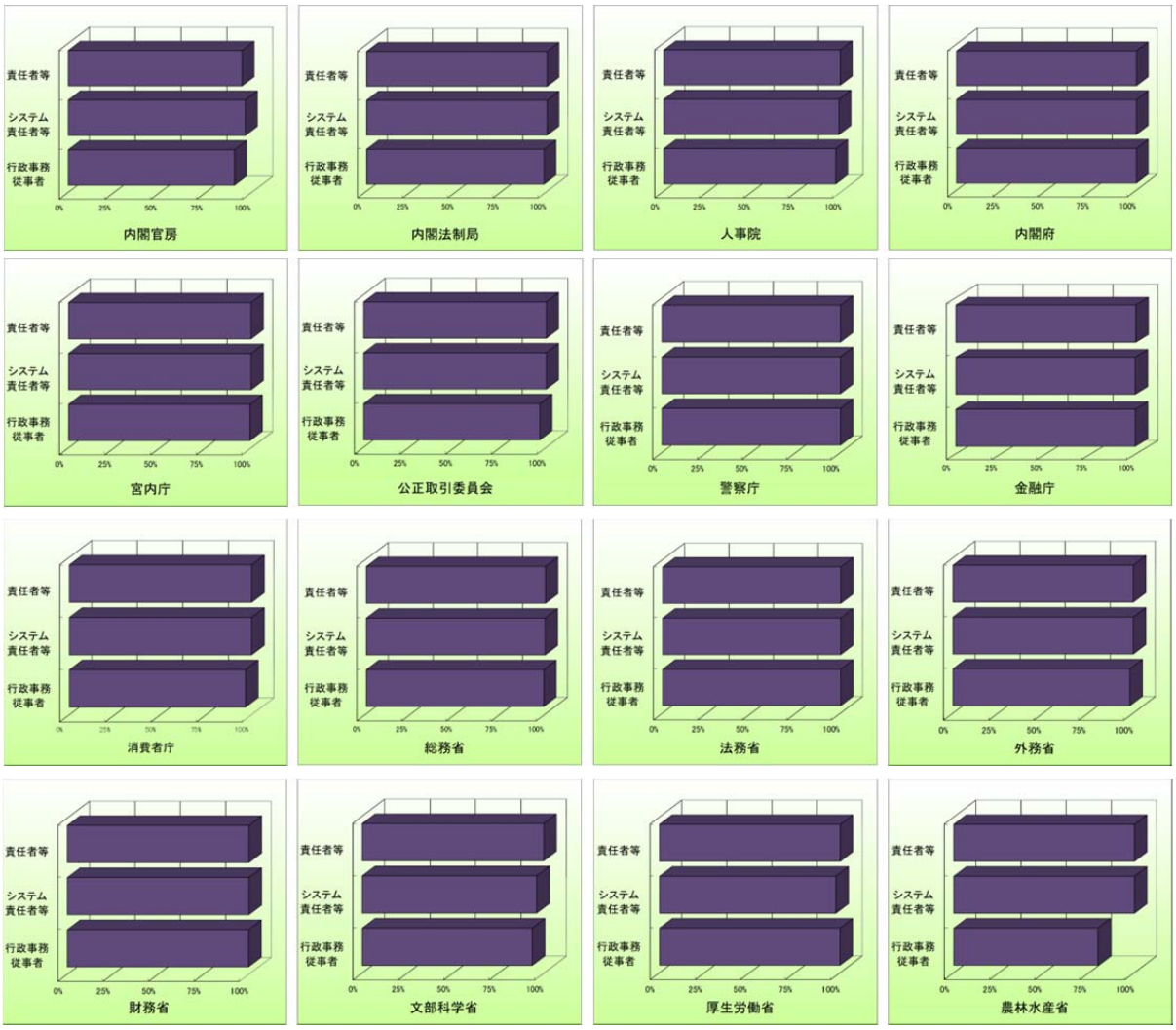


図 2-5 主体別の各点検項目の実施率の平均

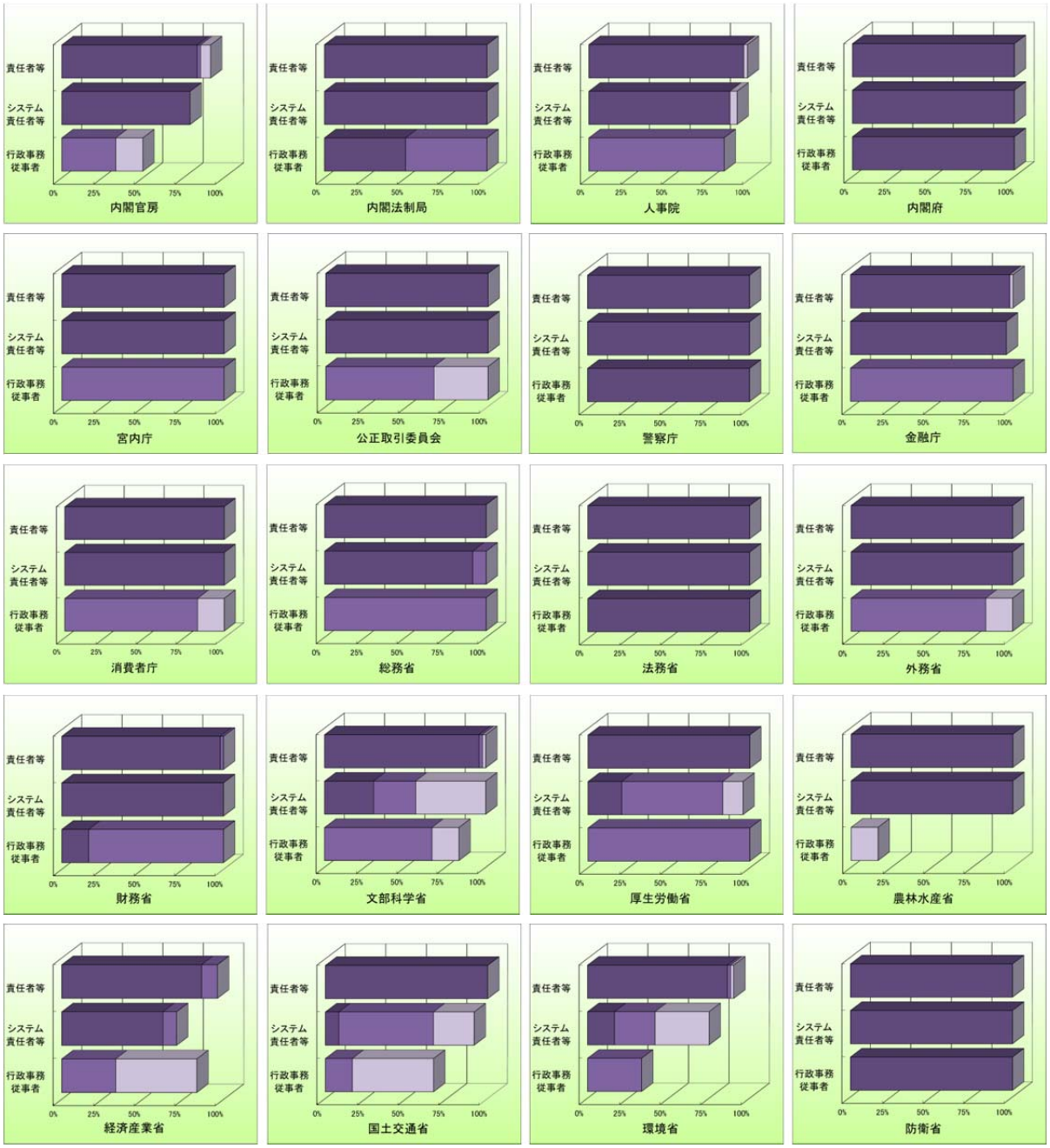
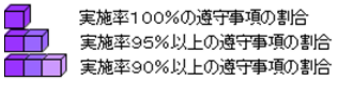

責任者等
システム責任者等
行政事務従事者
0%
25%
50%
75%
100%
内閣官房
内閣法制局
人事院
内閣府
宮内庁
公正取引委員会
警察庁
金融庁
消費者庁
総務省
法務省
外務省
財務省
文部科学省
厚生労働省
農林水産省
経済産業省
国土交通省
環境省
防衛省

図 2-6 主体別の到達率


実施率100%の遵守事項の割合
実施率95%以上の遵守事項の割合
実施率90%以上の遵守事項の割合

第３節　重点検査の評価

1 重点検査の目的

情報セキュリティの確保のためには、各府省庁において、政府統一基準群に準拠した対策が適切に講じられることが重要である。このため、各府省庁のウェブサーバ及び電子メールサーバに対する具体的な情報セキュリティ対策の実施状況を把握することを目的に、重点検査を実施した。

また、検査項目については、平成 22 年度の公開ウェブサーバ脆弱性検査の結果や、昨今の情報セキュリティに関する動向等を踏まえ選定した。

2 検査対象機関・システム等

下記 20 府省庁（本省及び地方支分部局）の情報システムにおいて重点検査を行った。

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、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

※：内閣官房のウェブサーバについては、内閣府との共有システムを除く

◆：内閣法制局及び人事院のウェブサーバについては、ホスティング又は e-gov 移行済みのため対象なし

3 検査期間

平成 23 年 7 月から平成 24 年 3 月

（検査基準日：平成 23 年 10 月 1 日）

4 検査方法

NISC が配布した調査票に基づき、各府省庁がウェブサーバ及び電子メールサーバについて内部調査を行い回答。両者間で回答内容の確認作業等を行った。

表 2-6 重点検査の実施対象・検査内容

	ウェブサーバ	電子メールサーバ
対象数	796 台	973 台
平成 22 年度「公開ウェブサーバの脆弱性検査」結果を基に各府省庁の実態を検査する必要があると判断した事項	・SSL バージョン２の無効化 ・強度の弱い暗号方式の無効化	―
昨今の情報セキュリティに関する動向から検査する必要があると判断した事項	要安定情報を取り扱うウェブサーバにおける大量パケット送信型の DoS 攻撃対策 （電子計算機及び通信回線が装備している機能を使用した対応状況、影響最小化への対応状況、監視対象の特定と監視方法及び監視記録の保存期間策定への対応状況、対処手順や連絡体制の整備状況）	―
対策実施状況報告との関連で検査する事項	OS 及びサーバアプリケーションのセキュリティアップデートの状況	

5 評価

A) 評価方法

各検査項目について、表 2-7 の評価基準に基づき、府省庁全体の対策の実施率の評価を行った。

表 2-7 評価基準

評価基準	実施率	概要
A	100%	全てのサーバで対策が実施されている。
B	80%≦x＜100%	概ね全てのサーバで対策が実施されているが、ごく一部のサーバで対策未実施である。
C	60%≦x＜80%	一部のサーバで対策未実施である。
D	60%未満	多くのサーバで対策が未実施である。

B) 評価結果

ウェブサーバにおける SSL バージョン２の無効化等や、ウェブサーバ及び電子メール

サーバにおける OS 及びサーバアプリケーションのセキュリティアップデートの府省庁全体の実施率は表 2-8 のとおりである。

表 2-8 各種対応状況の府省庁全体の実施率評価

対応状況		府省庁全体の実施率評価	
		ウェブサーバ	電子メールサーバ
SSL バージョン２の無効化		B	ー
強度の弱い暗号方式の無効化		B	ー
DoS 攻撃対策状況	電子計算機及び通信回線が装備している機能を使用した対応状況	B	ー
	影響最小化への対応状況	B	ー
	監視対象の特定と監視方法及び監視記録の保存期間策定への対応状況	B	ー
	対処手順や連絡体制の整備状況	B	ー
OS のセキュリティアップデートを適切に実施している状況		A	A
サーバアプリケーションのセキュリティアップデートを適切に実施している状況		A	A

C) 所見

ウェブサーバにおける「SSL バージョン２の無効化」及び「強度の弱い暗号方式の無効化」の対応状況については、府省庁全体では、それぞれ 95%以上のサーバに対して対策が実施されていた。府省庁別では、大半の府省庁において全てのサーバに対して対策が実施されていたものの、一部の府省庁では、未実施や 70%～95%の実施率にとどまった。

また、大量パケット送信型の DoS 攻撃への対応状況については、電子計算機及び通信回線が装備している機能の使用や影響最小化等の各項目において、それぞれ府省庁全体で 90%～96%の実施率であった。府省庁別では、ほとんどの府省庁では、全てのサーバに対してこれらの対策が実施されていたものの、70%～80%の実施率にとどまった府省庁もあった。

ウェブサーバにおいてこれらの対策がとられていないと、ウェブページの改ざんや通信の盗聴ほか、DoS 攻撃によって利用者にサービスを提供できなくおそれがあることから、対策が不十分な府省庁においては、対策を着実に実施することが求められる。

ウェブサーバ及び電子メールサーバにおける OS 及びサーバアプリケーションのセキュリティアップデートについては、それぞれ府省庁全体で 100%の実施率であった。これらは基本的な対策であることから、引き続き、適切に実施する必要がある。

第3章 平成 23 年度における重点取組事項

第１節　　標的型不審メール対処訓練

1 不審メール対処訓練の目的･経緯

以前から政府機関に対するスパムメールやウイルス付メールが送られて来ており、迷惑メールフィルタリング機能の強化やウイルス対策ソフトの導入など、これまでも情報システム面からの対応は行ってきた。しかし、情報システムの対応だけでは防ぎ切れないような明らかに政府機関を攻撃対象とする意図を持ったメール攻撃が顕在化している。メール文面や送信元などを巧妙に作り込み、受け手の心の隙を突くようなメールが情報システムによる防御をくぐり抜けて日常的に政府機関の職員宛に届くようになった。当然情報システム面からの対策も強化しなければならないが、受け手自身が知性をもって判断し対応することも求められることから、職員の意識啓発・訓練の実施が重要であるとの認識に至った。

そこで、対応の強化を図る一つの施策として、一部の府省庁で行われ情報セキュリティ報告書に記載されていた標的型メール攻撃への対処訓練を平成 22 年度の推奨事例として取り上げた。

しかしながら、単独で訓練を実施することが困難な府省庁もあり、また、訓練結果の知見を個別の府省庁に止めることなく、全府省庁等で共有することが重要であるとの認識の下、NISC が主導し政府機関全体の取組としてこの対処訓練を実施することとした。

また、「情報セキュリティ２０１１」では、希望府省庁に対して標的型メール攻撃に係る教育訓練を実施した結果を当該府省庁にフィードバックし、さらに得られた知見についても全府省庁等で共有するとともに公表することとされている。

2 訓練概要

A) 訓練期間

平成 23 年 10 月～12 月

B) 訓練対象

内閣官房等 12 の政府機関約６万名

- 訓練への参加を希望した府省庁の職員を対象。
- 訓練対象者は、各府省庁の事情により、職員全員、本省の職員のみ、一部地方支分部局を含むなど様々。

C) 訓練実施方法

本件訓練業務については、外部事業者への委託により実施

D) 訓練内容

ア）NISC において訓練実施計画書を作成

・訓練概要、訓練スケジュール、注意点、参加府省庁へのお願い事項などについて説明。
・事前教育コンテンツ、事後教育(Web)コンテンツ、10 パターンの模擬メール案文、ヘルプデスクの対応マニュアルなどを提示し、各府省庁の事情に応じてカスタマイズ。

イ）訓練対象者に対して各府省庁を通じて事前教育の実施

≪教育コンテンツの主な内容≫
○標的型メールとは（基本的な対応、被害例）
・適切な対応
・想定される被害
・実際の被害事例
○見極めるポイント
・差出人欄に注意！！
・件名に注意！！
・本文末の署名に注意！！
○不審なメールが送られてきた場合の対処方法
・ヘルプデスク若しくは情報システムセキュリティ管理者に連絡
○開封してしまった場合の対処方法
・LAN ケーブルを抜き、ヘルプデスク若しくは情報システムセキュリティ管理者に連絡

ウ）訓練対象者に対して標的型不審メールを模擬したメールを２回送付

・【１回目】－　実行型ファイルを添付したメールを送付
・【２回目】－　本文中にＵＲＬを埋め込んだメールを送付

エ）模擬メール中の添付ファイルを開封若しくは、ＵＲＬをクリックするなど不適切な扱いをした場合は、フィッシングサイトを模擬した Web サイトに誘導

○模擬メールを開封した者に対して、
・メールを取り扱う上での注意点（不審なメールの被害例、見分け方のポイント、不審なメールを開封してしまった場合の対応等）をまとめた教育コンテンツを表示する Web サイトに誘導。

・教育コンテンツの後に、なぜ、このメールを開封してしまったのか等のアンケートを設け、回答を要請。

オ）参加府省庁には、個人を特定する情報を除き、訓練結果をフィードバックし、各府省庁内において適切な事後教育指導を実施

（・訓練結果については、参加府省庁の希望により、部局別、官職別の集計・分析を行った上で、参加府省庁にフィードバック。）

カ）作業スケジュール

平成 23 年５月下旬～６月初旬　各府省庁訓練概要説明、参加意向確認
８月下旬～９月初旬　業者選定（請負契約）
９月初旬～９月下旬　実施計画書、スケジュール等作成
10 月初旬　各府省庁一斉説明会
- ・訓練の概要説明
- ・メール案文、事前、事後教育コンテンツのひな形の提示等
- ・ヘルプデスク対応要領

10 月初旬～10 月下旬　各府省庁個別説明会
- ・訓練日程調整
- ・メール案文、事後教育コンテンツのカスタマイズ
- ・メール設定変更等の個別調整

10 月下旬～12 月中旬　訓練実施
- ・確認テストメール送信（受信確認）
- ・訓練対象者のアドレス受渡し
- ・訓練メールの送信（添付メール、リンクメール）
- ・エスカレーションの実施

平成 24 年１月中旬～１月下旬　CISO 等連絡会議、政策会議、アドバイザー会議に訓練結果の中間報告
１月中旬～２月上旬　各府省庁個別報告会
- ・訓練結果の報告（開封率、アンケート結果等）
- ・訓練実施した感想、想定外の事象や気づきの点についてヒアリング
- ・来年度の訓練の実施について

４月上旬～４月中旬　CISO 等連絡会議、アドバイザー会議に訓練結果の最終報告

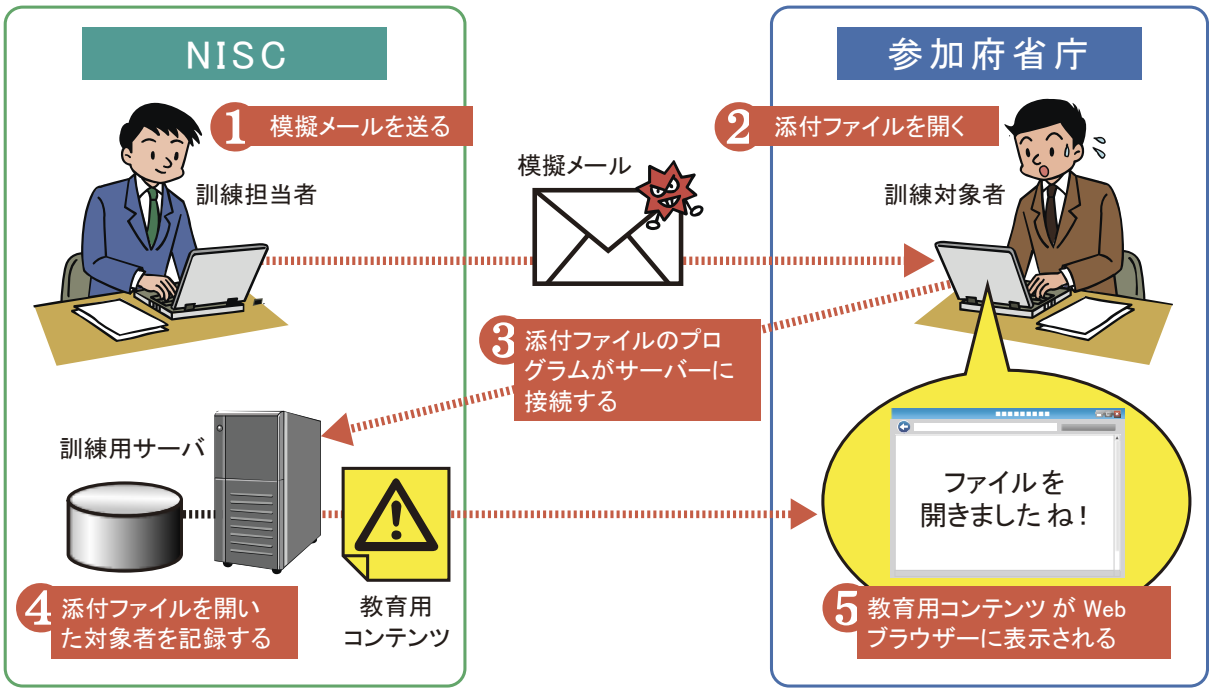


図 3-1　標的型不審メール教育訓練の流れ

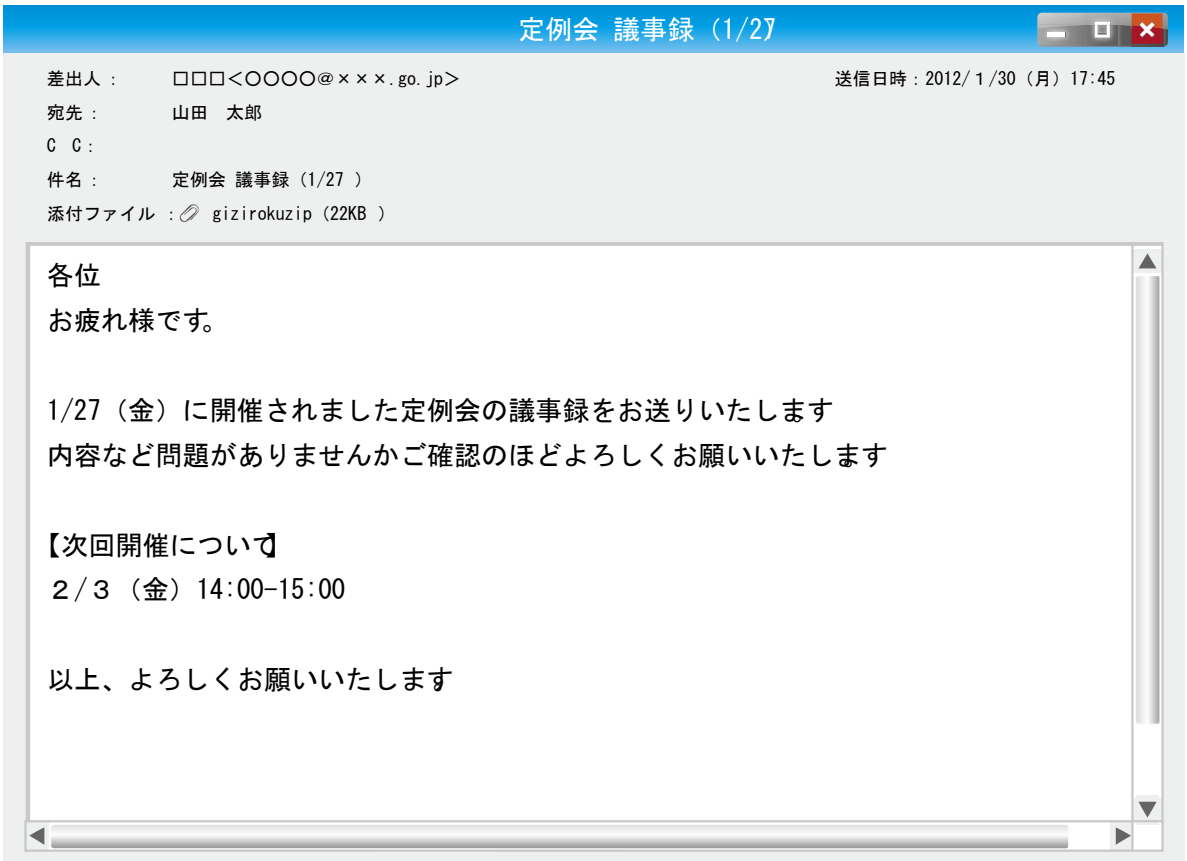


図 3-2　標的型不審メールを模擬したメールのイメージ

これはメール取扱訓練です。

政府職員を対象に、情報セキュリティ教育の一環として実施しています。
あなたはウイルスメール、迷惑メール、詐欺メールの可能性のある不審なメールを開封してしまいました。
不審なメールを正しく取り扱わないと、あなたが今お使いのパソコンだけでなく、ネットワークに繋がっている他のコンピュータにまで悪影響を及ぼしてしまう場合があります。
当省は、毎日多数のウイルス付電子メールを受けており、その中にはウイルス対策ソフトでは検出不能な最新型ウイルスが含まれている場合があります。
不審なメールは開かず削除してください。当省を守るのは、職員一人ひとりの心がけです。
下の説明文をよくお読み頂き、今後は正しいメールの取扱い方を日々実践して下さい。
****
本メールは訓練用メールです。ウイルス感染、情報漏えい等の実害はありません。
この教材をよくお読みいただきますよう、お願いします。
****
本文書の最後に、本訓練に対する設問があります。回答にご協力をお願いいたします。

図 3-3 開封者用の教育コンテンツのイメージ

3 訓練結果

(1) 今回の訓練における不審メールの開封率
（添付ファイルを開封若しくはＵＲＬをクリックした割合 ）

- １回目（添付ファイルを開封）　平均　10.1%（最低 1.1%～最高 23.8%）
- ２回目（ＵＲＬリンクをクリック）　平均　3.1%（最低 0.4%～最高 6.1%）
- １回目、２回目ともに開封しなかった者　87.5%
- １回目のみ開封した者　9.4%
- ２回目のみ開封した者　2.4%
- ２回とも開封した者　0.7%

		2回目		
		URL をクリックしなかった	URL をクリックしてしまった	
1回目	添付ファイルを開かなかった	87.5%	2.4%	89.9%
	添付ファイルを開いてしまった	9.4%	0.7%	10.1%（１回目開封率）
		96.9%	3.1%（２回目開封率）	

図 3-4　1回目、2回目の開封者・非開封者の割合

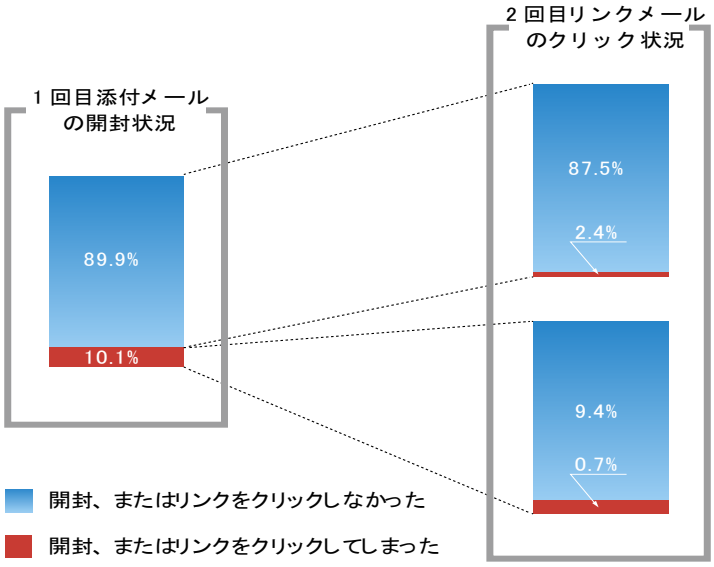


図 3-5　1 回目、2 回目の開封者・非開封者の割合

(2)不審メールを開封した者によるアンケートの回答結果

ア）１回目（添付メール）

訓練用メールを開封した 5,766 名から 2,291 件のアンケート回答があった。

・添付メール訓練の開封者のうち、習慣で開封したという者が約１／３。不審な点はないと判断して開封した者を含め、約半数の者は、普段から不審なメールについて全く注意しておらず、何の疑いも無く開封したと推測される。

・また、残りの約半数の者は、注意はしていたが、業務に関係するメールであると判断し、開封したと推測される。（図　3-6、図　3-7 を参照）

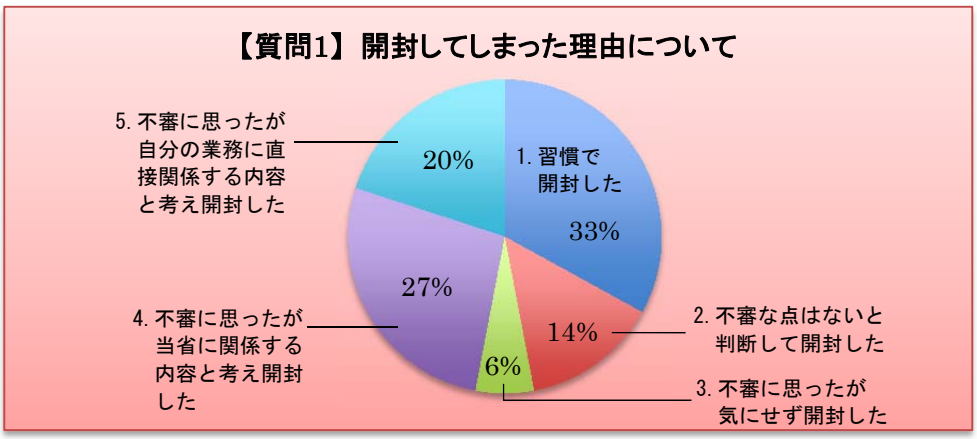


図 3-6　開封してしまった理由（添付メール）

○訓練用メールを開封してしまった理由

・「1. 習慣で開封した」　→757 件（33.0%）

・「4. 当省（庁、府）に関係する内容と考え、開封した」→622 件（27.1%）
・「5. 自分の業務に直接関係する内容と考え、開封した」→451 件（19.7%）
・「2. 不審な点はないと判断して開封した」　→328 件（14.3%）

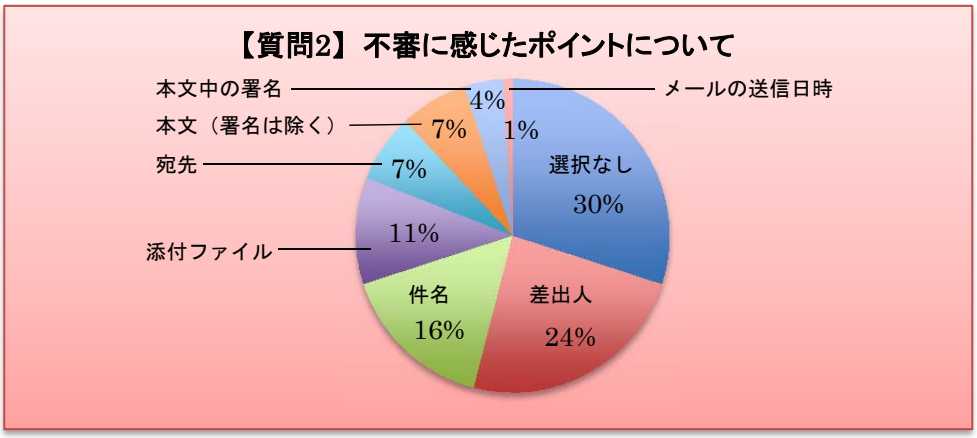


図　3-7不審に感じたポイント（添付メール）

○訓練用メールで不審に感じたポイント
・「選択なし」　→　1,032 件（29.1%）
・「差出人」　→　857 件（24.2%）
・「件名」　→　577 件（16.3%）
・「添付ファイル」　→　404 件（11.4%）

イ）２回目（リンクメール）

訓練用メールを開封した 1,778 名から 582 件のアンケート回答があった。
・リンクメール訓練についても、添付メール訓練とほぼ同様の結果となった。
・今回の訓練においては、開封者からのアンケートのみ実施したが、今後の訓練の継続に当たり、未開封者が何を不審に思い開封を止まったのかなどについても意見を聞きたいという課題が残った。（図　3－8 図　3－9 を参照）

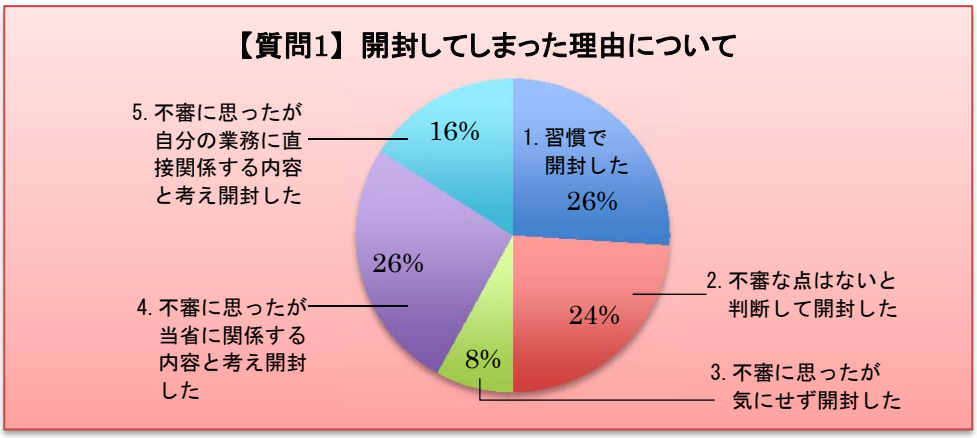


図　3-8開封してしまった理由（リンクメール）

○訓練用メールを開封してしまった理由

・「4. 当省（庁、府）に関係する内容と考え、開封した」→154 件（26.5%）
・「1. 習慣で開封した」　→149 件（25.6%）
・「2. 不審な点はないと判断して開封した」　→138 件（23.7%）
・「5. 自分の業務に直接関係する内容と考え、開封した」→ 93 件（16.0%）

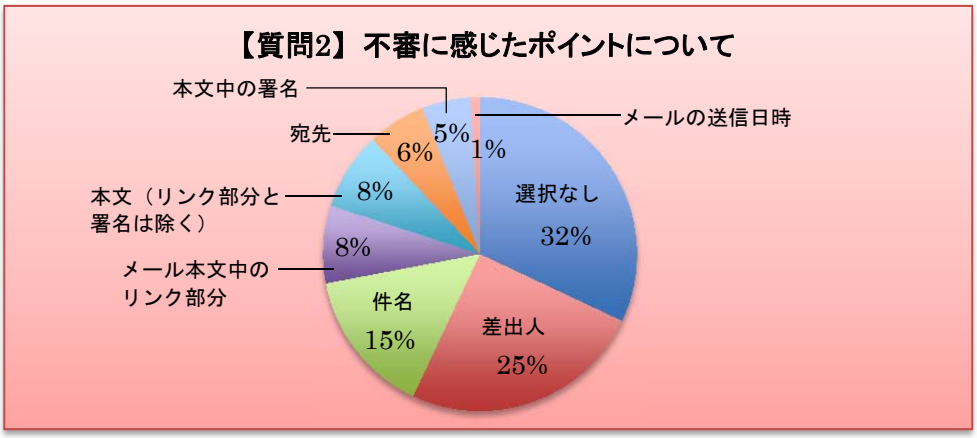


図 3-9不審に感じたポイント（リンクメール）

○訓練用メールで不審に感じたポイント

・「選択なし」　→　273 件（32.0%）
・「差出人」　→　209 件（24.5%）
・「件名」　→　129 件（15.1%）
・「リンク部分」　→　69 件（ 8.1%）

ウ）アンケート結果（自由記述欄）

アンケート回答者のうち、自由記入欄の記載は約 700 件。（アンケート回答者の約 24%）

○自由記入欄の記載の大半が、「今回は反省し今後注意する」、「訓練をまたやってほしい」等の前向きなものであった。
このほか、主な記載事例について類型別に整理すると以下のとおりであった。

≪開封理由≫

【不注意型】
・自分も関係するタイムリーな内容、件名等に反応して開いてしまった。
・休暇明け、出張戻り後、会議で戻った後など、たまったメールを無意識に開いた。

【親切型】
・誤送信と思い、送信者に教えてあげるために開封した。（多数）

【誤解型】
・差出人が不審であると思いながらも、件名で関係があると思い開封した。
・差出人に心当たりがあった。（名字のみしか見ずに判断）

【お手上げ型】
・今回の訓練メールで注意すべき箇所はどこであったのか？わからないので教えてほしい。
・業務上、外部の見知らぬ人からもメールは多く届く。判断が難しい。

【負け惜しみ型】
・訓練とわかっていて開封した。（開封したらどうなるか興味があった）
・わざと開けてあげた。
・手が滑った。

【不運型】
・電話中に相手から「いまメール送りました」と言われ、そのときに訓練メールがちょうど届いて無意識にあけてしまった。

【優柔不断型】
・同僚・上司から「開けてみろ」といわれたから。

≪対策等への意見≫

【問題提起】
・開封感染は防げない、事後措置が重要ではないか。
・危険なメールかどうかの見分け方、もっと分かりやすい指標が必要。
・「至急」が件名についていれば、普通は開けるだろう。本当に至急の要件のときにはどう判断したらいいのか。
・表題を見てすぐに判断すべきもの、省庁外からのメールも多くある、どう見分けるか？
・訓練をし過ぎるとエスカレーションもしなくなるのではないか。

【対策の提案（システム対応）】
・システム上の不審メールのスクリーニングの精度向上が必要。
・外部からもよくメールが来るので、メールソフト側で省内以外から来たメールということが一目で分かるようにしてはどうか。
・省庁外からのメールは、受信トレイに送信者名やアドレス等、色分けや点滅等をする注意喚起補助機能が欲しい。
・添付ファイルを開く際には、チェックリストが立ち上がってチェックしないと開けない機能を設けるのはどうか。
・go. jp 以外から届くメールには自動的に警告文を挿入する。

≪その他≫

【クレーム等】
・紛らわしいメールを送るな。
・腹立たしい訓練である。
・不快。
・いたずらをやめろ。
・業務時間中に送るな。
・訓練はムダ。

4 課題･反省点

○参加府省庁からのアンケート、意見交換の結果から得られた課題・反省点

- 訓練後、ヘルプデスクへの連絡・相談や不審メール対応のコンテンツへのアクセス数が増大するなどの現象がみられ、訓練効果はあったと感じた。
- 実質１か月余りの間に２回の送信を行ったため、１回目と２回目の間隔が短くなり、訓練として有効に機能したか疑問。一時的な効果となった可能性がある。
- 実施時期が繁忙期と重なる府省庁が多かった。
- ２回とも差出人メールアドレス、ドメインが同じであったため、訓練メールであると容易に判断された場合があった（迷惑メールの自動フィルタリング機能等も含めて）。
- 普段は html ファイルをそのまま添付することはあまりなく、不審メールとしての巧妙さに欠け、すぐに不審メールと判ってしまった。
- 開封者が見る教育コンテンツが長文すぎて、最後まで読んでもらえないため、アンケートまでたどりつかない場合も多かったと思われる。
- 開封者のアンケートは取得できるが、未開封者がなぜ開封に至らなかったかなどの意見収集が出来ていない。
- 各府省庁においては、開封者の個人特定ができないため、個別の事後教育につながらない。
- エスカレーションの訓練としては十分な結果を出せたとは言えない。
- 訓練結果については、速報値だけでも早く欲しい。報告書もできるだけ早く欲しい。

5 平成 24 年度の訓練実施方針

○本訓練は、政府機関において大規模に実施する初めての取組であったが、実施府省庁の担当者へのヒアリングの結果、「有効であった」との回答が大半を占めており、一定の有効性はあったと認められる。この成果を一過性のものとすることなく、訓練手法を改善しつつ継続することが重要であることから、平成 23 年度に実施した標的型不審メール攻撃訓練の結果、判明した課題や反省点を踏まえ、平成 24 年度においても訓練を継続すべく内容の検討を行う。

第２節　なりすまし防止策の実施状況

1 取組の概要

近年、なりすましと呼ばれる不審メールにより、一般国民や民間企業等に偽の情報やウイルスが含まれるファイルを送信する等の犯罪行為が横行している。その手段として、悪意の第三者が、政府機関又は政府機関の職員であると誤認させる目的で、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）に詐称することが見受けられる。

これまで政府機関でのなりすましの防止策については、「第２次情報セキュリティ基本計画」[12]にその対策を掲げる等して政府機関全体として取組を推進してきた。平成 23 年度については、「情報セキュリティ２０１１」[13]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」[14]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メールにより、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、この防止策である SPF（Sender Policy Framework）等の送信ドメイン認証技術（コラム参照）の採用を推進した。

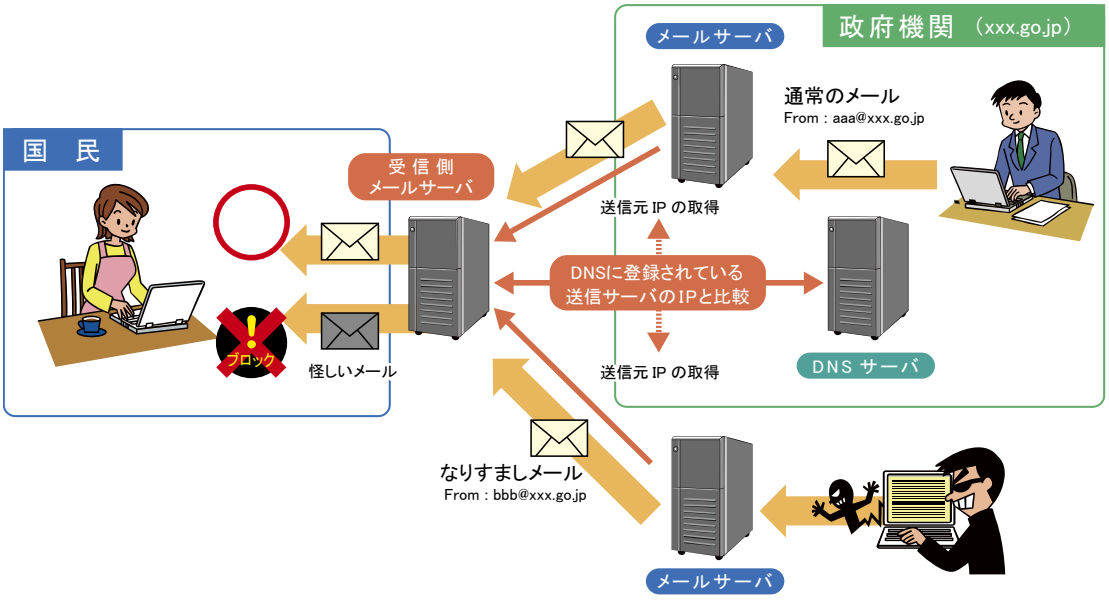


図 3-10　SPF を活用したなりすまし対策の概要

図　３－１０は、今年度政府機関において取り組んだ 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、メールの送信側であらかじめメールを送信する可能性のあるメールサーバの IP アドレスを SPF レコード[15]に公開する。受信側では、メールの受信

[12] 平成 21 年２月３日情報セキュリティ政策会議決定
[13] 平成 23 年７月８日情報セキュリティ政策会議決定
[14] 平成 23 年４月 21 日情報セキュリティ政策会議決定
[15] SPF レコードとは、SPF/SenderID 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、インターネット上に公開されているもの。

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。

今年度の取組では、特に、送信側における対策である政府ドメインの DNS サーバに、SPF レコードとして利用する送信メールサーバの IP アドレスの公開を行う取組を最優先で推進した。

＜コラム：送信ドメイン認証技術＞

送信ドメイン認証技術は、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術。本技術には２つの方式があり、１つがネットワーク方式と呼ばれている SPF 及び Sender ID、もう１つが電子署名方式と呼ばれている Domain Keys Identified Mail(DKIM)という方式である。いずれの方式も既存のメールシステムの仕組みに大きな変更を加えなくても導入できるように考慮されているが、一般的に SPF 及び Sender ID の方が DKIM と比べてコストの面で導入しやすいとされている。そのため、政府機関では、それぞれの方式の導入コストと効果を勘案し、平成 23 年度は特に SPF の導入を推進した。

2 送信側における SPF 対策に関する取組結果

グラフ（図　3－１１）に、政府ドメイン[16]（サードレベルドメイン）における、送信側における SPF 対策（送信側 SPF 対策）の導入状況の推移を示す。送信側 SPF 対策導入率は、平成 23 年度当初が 36.5%であったのに対し、年度末には 97.4%まで向上した。

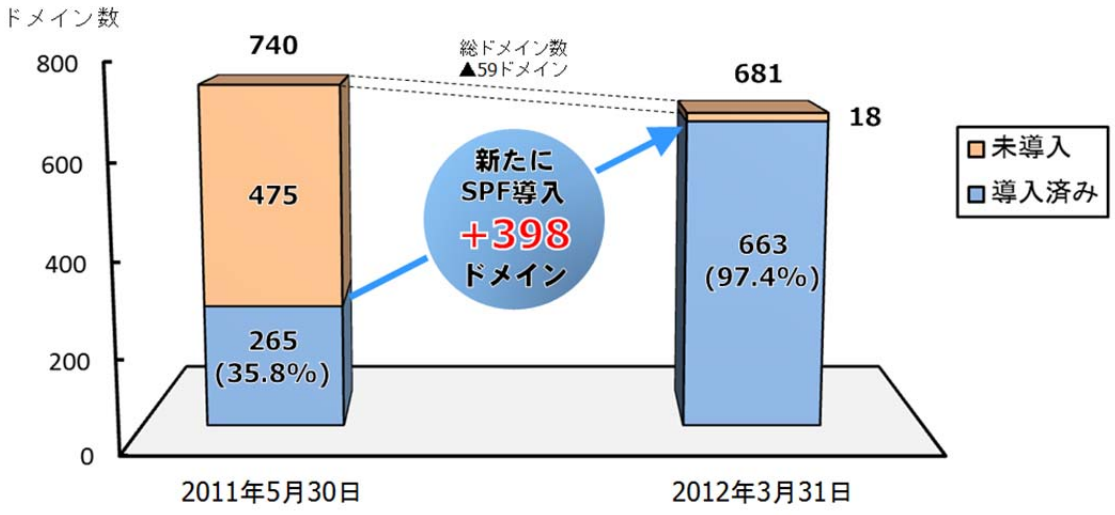
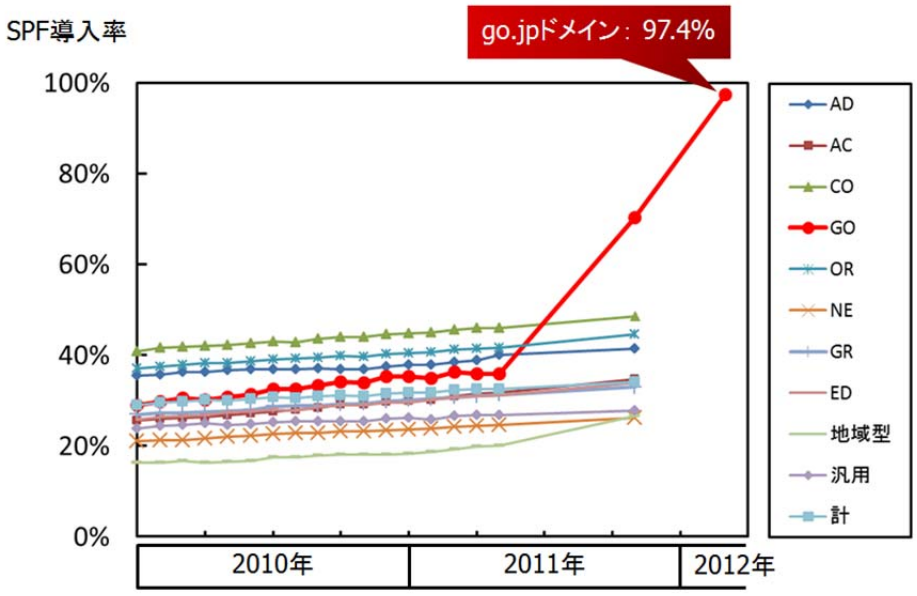


図 3-11　SPF 導入実施状況の推移(政府ドメイン)

[16] ここでいう政府ドメインとは、ドメイン名の末尾が.go.jp で終わるドメインのうち、立法機関、司法機関及び特殊法人等が管理しているものを除いたドメインを示す。

また、グラフ（図　3-１２）に、日本の各ドメインにおける送信側 SPF 対策実施率の推移を示す。政府ドメインは、他のドメインと比較し、送信側 SPF 対策実施率が急激に上昇していることが分かる。



（WIDE プロジェクトにて調査・公開しているデータ[17]に、NISC で年度末に
測定した政府ドメインの結果を加え、グラフを作成。）

図　3-12　SPF 導入実施状況の推移（ドメイン別の比較）

このように、ほとんどの政府ドメインで送信側 SPF 対策が実施されており、受信側のメールサーバに SPF レコードを確認する機能を導入していれば、政府機関をなりすますメールが検知でき、メールを破棄することやメールヘッダ情報で注意を促すなどの適切な対処ができる状態となった。

3 その他の取組

送信側 SPF 対策の取組にあわせ、下記についても実施した。

A）利用していないドメインの登録廃止

過去に利用していたが、現在は利用していないドメインについては、なりすましの温床となる可能性があることから、そのような可能性をできる限り排除することを目的としてドメイン登録の廃止を推進した。

[17] http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

B) SPF レコードの限定子及び機構を”-all”と記述

SPF レコードには、限定子及び機構と呼ばれる記述方法により、「登録されてない IP アドレスのメールサーバからも送信される可能性がある」ということを示す”~all” という記述も可能となっている。

そのため、SPF レコードを公開していたとしても、その内容が”~all”となっている場合、そのような記述をしているドメインで詐称したメールについては、受信側でなりすましメールと明確に判断することは不可能である。この結果、なりすましメールであるかどうかが分からずに、受信者が添付ファイルを開きウイルスに感染するというリスクが高まるものと考えられる。

この問題の対策として、限定子及び機構は「登録されてない IP アドレスのメールサーバからは送信される可能性はない」ということを明確に示す ”-all” という記述にすることを推進した。

C) ベストプラクティス等の共有

最高情報セキュリティアドバイザー等連絡会議にて、取組推進におけるベストプラクティス、各種課題及び各府省庁における送信側 SPF 対策実施率の進捗を共有し、取組が円滑に行われるよう促した。

（ベストプラクティスの例）

・SPF レコードのよくある記述間違いの紹介と記述内容の確認方法について
・ドメイン管理をアウトソーシングしている場合の対応方法について
・利用していないドメインの登録廃止に係る手続方法について

D) 受信側における SPF 対策の推進

なりすまし電子メールにより政府機関自身に害が及ぶことの無いよう、政府機関における受信側 SPF 対策についても実施を推進した。本府省庁の 20 ドメインについては、平成 23 年度末で 17 府省庁が受信側 SPF 対策を完了し、平成 24 年度末には 18 府省庁が対策を完了する見込みである。

E) その他

NISC に対し、ある政府機関をかたったなりすましメールを受信した府省庁から、SPF レコードの記述方法に誤りを示すエラー(DNS への参照回数が規定の 10 回を越えている)が出ている旨の連絡があり、そのエラーの原因調査と修正を実施した。原因究明の過程では、IPv6 アドレスに係る別の問題（ある大手プロバイダの受信メールサーバにおける IPv6 アドレスの処理の不具合）も新たに発見したが、直ちに修正を依頼するなど SPF レコードに係る不具合に随時対応した。

参考文献

・送信ドメイン認証技術導入マニュアル

第３節 公開ウェブサーバの脆弱性検査

1 検査の目的

従前より重点検査においてウェブサーバの台数やパッチの適用状況等、ウェブサーバの運用状況について検査を行ってきた。これを実践的に一歩進め、公開ウェブサーバに対する脆弱性検査（インターネットからの侵入検査）を実施した。その結果、複数の府省庁で共通的に検出される脆弱性を把握し、その内容を全省庁と共有することで政府機関全体の情報セキュリティ対策の向上につなげている。検査結果については以下のとおりである。

2 検査概要

A) 検査期間

平成 23 年９月～12 月

B) 検査対象

希望府省庁における公開ウェブサーバ（11 省庁、約 330 画面[18] ）

C) 検査方法

対象とする公開ウェブサーバにインターネット経由でアクセスし、ツール及び手動により検査を実施

図 3-13 検査方法イメージ図

D) 検査内容

・サーバ OS 部分に関する検査
・ウェブアプリケーション部分に関する検査

[18] NISC で実施した脆弱性検査の検査対象であり、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ていない。

3 検査内容詳細

A) サーバ OS 部分に関する検査

	検査内容
(1)	ポートスキャン
(2)	提供サービスの情報取得及び挙動確認
(3)	ツールによる検査
(4)	DoS 検査
(5)	手動による侵入検査

B) ウェブアプリケーション部分に関する検査

	検査内容
(1)	クロスサイトスクリプティング検査
(2)	SQL インジェクション検査
(3)	セッション管理検査
(4)	認証検査
(5)	ファイル拡張子検査
(6)	コマンドインジェクション検査
(7)	ディレクトリトラバーサル検査
(8)	権限昇格検査
(9)	パラメータ書き換え検査
(10)	ウェブアプリケーション固有の問題についての検査

4 検査結果概要

ウェブアプリケーションに関する検査では、SQL インジェクションといった個別のアプリケーションに見られる危険度の高い脆弱性を検知し、プラットフォームに関する検査では、Apache の Range ヘッダにおけるサービス運用妨害などの危険度の高い脆弱性を検知した。検出した府省庁に対しては即日速報を発出し、該当府省庁においては速やかに対処を実施した。

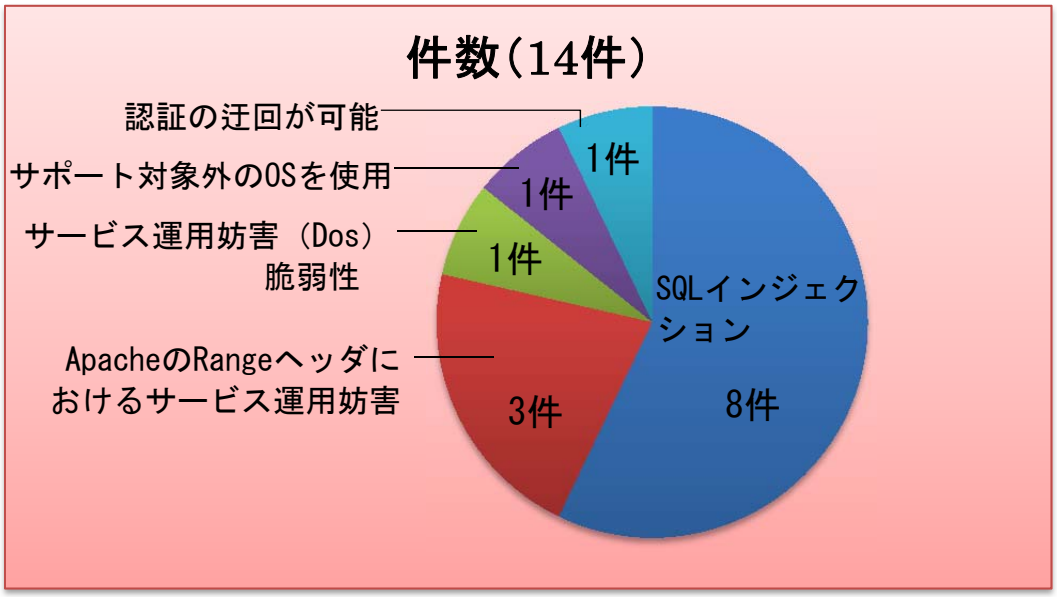


図 3-14　危険度の高い脆弱性の内訳

危険度の高い脆弱性については検出した府省庁において対処済みである。

また上記危険度の高い脆弱性のうち、複数府省庁で検出された「SQL インジェクション」と「Apache の Range ヘッダにおけるサービス運用妨害」については、脆弱性の内容に加え対処方法を全府省庁と共有し、政府機関全体の情報セキュリティ対策の向上に活用した。

公開ウェブサーバの脆弱性は日々発見されるものであり、継続的に検査することが重要であると考えている。この状況を踏まえ、来年度も希望府省庁に対し公開ウェブサーバに対する脆弱性検査を実施し、政府機関全体の情報セキュリティ対策の向上に努めてまいりたい。

具体的な取組として、以下のような注意喚起を全府省庁に発出し情報共有を図った。

（全府省庁に発出した注意喚起）

事　務　連　絡
平成２４年１月 18 日

各府省庁情報セキュリティ担当課室長あて（注意喚起）
情報ｾｷｭﾘﾃｨ対策推進会議ｵﾌﾞｻﾞｰﾊﾞｰ機関情報セキュリティ担当課室長あて（情報提供）

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）

公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について（注意喚起）

内閣官房情報セキュリティセンターでは、平成 23 年 9 月から 12 月までの間、希望した 11 府省庁の公開ウェブサーバを対象とする脆弱性検査を実施しました。

その結果、危険度高（CVSS（注）基本値 7.0～9.9）に相当する SQL インジェクションやサービス運用妨害（DoS）の脆弱性が複数の省庁で確認されました。特に、SQL インジェクションについては、同手法を用いて政府機関のウェブサイトが改ざんされる事案も発生しています。

脆弱性が確認されたウェブサーバについては各府省庁において既に適切に措置が講じられたところですが、全ての府省庁において、本事務連絡に記載の SQL インジェクション及びサービス運用妨害（DoS）の脆弱性の確認方法等を参考に、管理している公開ウェブサーバについて確認し、脆弱性の存在が疑われる場合には、保守業者又は専門の検査会社に相談することを推奨します。特に、公開ウェブサーバを構築中の場合は、検収時に確認することを強く推奨します。

注　CVSS（共通脆弱性評価システム：Common Vulnerability Scoring System）は、米国家インフラストラクチャ諮問委員会（NIAC）のプロジェクトで 2004 年 10 月に原案が作成。特定のベンダーに依存しない共通の評価方法として、多数の組織で採用（参考 URL：http://www.first.org/cvss/eadopters.html）。

1　SQL インジェクション

(1)　概要

SQLインジェクションの脆弱性が存在すると、攻撃者が用意したSQL文をデータベース上で実行することが可能となるため、データベースに格納されている情報の漏えいや改ざんが発生する可能性があります。ウェブアプリケーションでは、実行されるべきでない悪意のあるSQL文が攻撃者から入力された場合、データベースで実行される前にSQL文として処理されないよう無効化する必要がありますが（図 ①）、無効化されずにデータベースで実行された場合、データベースの操作が可能となります（図 ②）。本脆弱性を悪用するとデータベース接続ユーザの権限の範囲で登録されている情報の取得や改ざん等が可能となります。

この中でも、今回確認されたSQLインジェクションの脆弱性は、

・攻撃を実施するに当たって攻撃が困難（複雑）となる要因が存在しなかった

・認証を必要としない箇所において検出されたことから、危険度の高いものであるといえます。

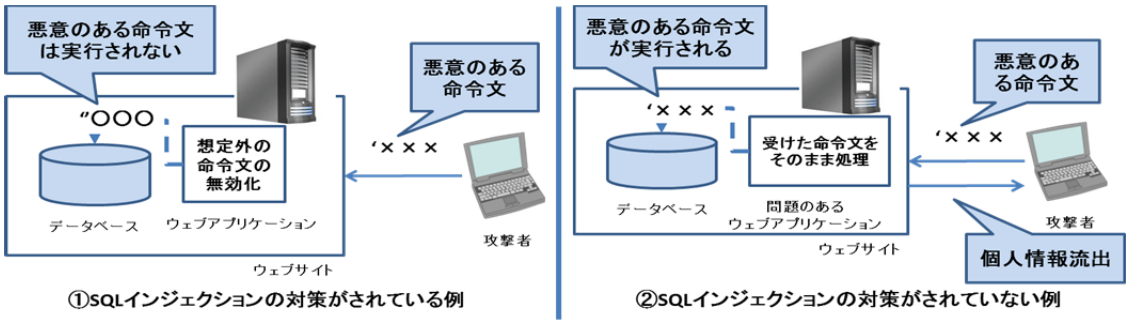


図 SQL インジェクションの概要

(2)　確認方法

本確認方法では、ブラウザの入力欄に SQL 文の特殊文字である「’」を含む文字列を入力し、その応答から SQL インジェクションの脆弱性が存在する可能性の有無を判断します。

例えば、ブラウザの入力欄に「テスト’」と入力し、検索ボタンを押下します。

その際、以下のような応答が返された場合には SQL インジェクションの脆弱性が存在する可能性が高いといえます。

- データベースのソフトウェア名（Oracle, SQL Server, MySQL, DB2, PostgreSQL）を含むエラーメッセージが表示される。
- SQL 文の一部が表示される。
- SQL 文の構文エラーに関するメッセージが表示される。
- 「ORA-01756」などユーザ向けではないメッセージが表示される。

また、SQL インジェクションの脆弱性が存在する可能性が高い場合「テスト’’」（シングルクォート 2 つ）を入力すると上記のような応答は返されません。

なお、上記の確認方法は「SQL インジェクションの脆弱性が存在する可能性」を判別するものであり、実際に SQL インジェクションの脆弱性の有無を保証するものではありません。独立行政法人情報処理推進機構(IPA)の「安全なウェブサイトの作り方 改訂第 5 版」（2011 年 4 月、http://www.ipa.go.jp/security/vuln/websecurity.html）チェックリスト等を参考に確認することを推奨します。

上記確認の結果、SQL インジェクションの脆弱性が存在する可能性が高いと判断した場合は、保守業者や専門の業者に相談するなどの対応を検討願います。

(3)　対策例

- 入力値チェック処理の徹底

想定外の文字の入力を拒否する必要があります。例えば「値段」を入力するテキストボックスからの入力の場合には、入力値として数字以外の文字を受け付ける必要はないと考えられることから、数字以外の文字が入力された場合には、エラー処理を行うようにアプリケーションを修正します。数字に限らず、入力文字種や文字

列の長さが制限できる場合には、指定した制限規則外の文字列を受け付けないようにすることでWebアプリケーションの安全性が高まります。

- エスケープ処理の徹底

  SQL文で使用されている特殊文字をエスケープ処理する必要があります。エスケープが必要な文字種に関しては、データベースサーバの種類やアプリケーション環境に依存します。

【参考情報】

- IPAセキュア・プログラミング講座 第6章 入力対策 SQL注入:#1 実装における対策

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web06.html

2　サービス運用妨害（DoS）

(1)　概要

Apache 2.0.64以下及び2.2.19以下のバージョンには、Rangeヘッダ及びRequest-Rangeヘッダの処理に問題があり、サービス運用妨害（DoS）の脆弱性が存在します。脆弱性が悪用されると遠隔の第三者によって、サービス運用妨害（DoS）攻撃を受ける可能性があります。また、「Apache Killer」と呼ばれる攻撃ツールが公開されており注意が必要です。

なお、この脆弱性については、Apacheが組み込まれている、又はApacheをベースとして使用するソフトウェア製品においても脆弱性の影響を受ける可能性があります。

また、動作しているApacheのバージョンが1.3系の場合には本脆弱性の影響は受けません。ただし、1.3系は開発が終了しているバージョンであり、今後発見される脆弱性への対応が行われないため、最新の2.2系へのバージョンアップを検討することが望まれます。

(2)　対策例

脆弱性の影響を受けるバージョンを使用している場合には、ベンダーから提供されているセキュリティパッチの適用又は脆弱性の改修された最新バージョンへのバージョンアップを行います。

- Apacheプロジェクト提供の2.2系における最新バージョン（2011年11月時点）

  Apache HTTP Server 2.2.21

  http://www.apache.org/dist/httpd/

パッチ適用又はバージョンアップができない場合及びApache2.0系を使用している場合には、回避策として以下のいずれかの設定を行います。設定方法の詳細について

は、参考情報を参照してください。

＜回避策＞

（ｉ）大量のRangeヘッダを含むリクエスト及びRequest-Rangeヘッダの無視又は拒否

使用されているApacheのバージョンに応じて、以下のどちらかを設定してください。

設定１：Apacheの設定ファイルに以下の設定を追加（※Apache 2.2系で有効）

【設定例】

```
SetEnvIf Range (?:,.*?){5,5} bad-range=1
RequestHeader unset Range env=bad-range
RequestHeader unset Request-Range
```

設定２：Apacheの設定ファイルに以下の設定を追加※Apache 2.0系及び2.2系で有効

【設定例】

```
RewriteEngine on
RewriteCond %{HTTP:range} !(^bytes=[^,]+(,[^,]+){0,4}$|^$) [NC]
RewriteRule .* - [F]
```

（ii）Rangeヘッダを完全に無効化

Apacheの設定ファイルに以下の設定を追加

【設定例】

```
RequestHeader unset Range
RequestHeader unset Request-Range
```

（iii）一時的な対策として、Rangeヘッダカウントモジュールを適用

以下のリンクから入手可能。

http://people.apache.org/~fuankg/httpd/mod_rangecnt-improved/

http://people.apache.org/~dirkx/mod_rangecnt.c

【参考情報】

- Apache HTTPD Security ADVISORY（開発元のセキュリティアドバイザリ）

  http://httpd.apache.org/security/CVE-2011-3192.txt
- Apache HTTP Server 2.2.21 Released

  https://www.apache.org/dist/httpd/Announcement2.2.html
- JPCERT/CC Apache HTTP Server のサービス運用妨害の脆弱性に関する注意喚起

  https://www.jpcert.or.jp/at/2011/at110023.html
- 情報処理推進機構（IPA） ウェブサーバ「Apache HTTP Server」の脆弱性（CVE-2011-3192）について

  http://www.ipa.go.jp/security/ciadr/vul/20110831-apache.html

- JVN Apache HTTPDサーバにサービス運用妨害(DoS)の脆弱性
  http://jvn.jp/cert/JVNVU405811/

3　その他

・　前述の「安全なウェブサイトの作り方 改訂第 5 版」にも各種脆弱性に対する対策が記載されておりますので、これに基づき公開ウェブサイトを構築してください。

・　内閣官房情報セキュリティセンターでは、平成 24 年度も各府省庁の公開ウェブサーバを対象とする脆弱性検査を実施することを検討しています。なお、検査対象のサーバについては、構築後 1 年程度の比較的新しく導入されたサーバを対象とする予定です。

以　上

第４節　東日本大震災における情報システムへの影響及び今後の対策

1 調査・分析の目的

平成 23 年３月 11 日に発生した東日本大震災は、地震、津波等による大規模停電やネットワーク障害等により、政府機関の情報システムにも大きな影響を及ぼした。このため、東日本大震災以来、震災の教訓を活かした情報システムの運用継続計画の必要性が改めて認識されることとなった。

こうした状況を踏まえ、政府機関の情報システムにおける運用継続性の強化に資することを目的に本調査・分析を実施した。本調査・分析では、震災での情報システムの被害状況や復旧対応上の反省等の情報を収集し、各被害の軽減・防止に有効な対策や留意事項等の知見を整理した。

2 調査・分析の概要

A) 実施期間

平成 23 年９月～平成 24 年３月

B) 調査の対象範囲

本調査は、本府省庁、地震又は津波による被害が大きかった東北３県（岩手、宮城、福島）並びに、計画停電等インフラによる影響が生じた首都圏の一部（東京、埼玉、千葉、神奈川、茨城、栃木、群馬）に所在する各府省庁の地方支分部局及び施設等機関を対象範囲とした（図　３－１５）。

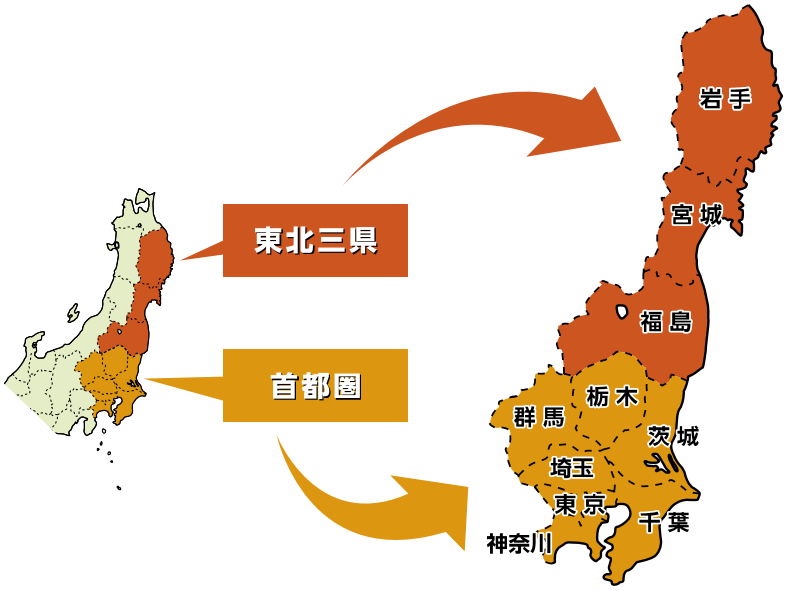


図 3-15　本調査の対象範囲

C) 調査方法

主にアンケート調査とヒアリング調査によるサンプル調査を実施し、被害状況や対策実施状況の実態をまとめた。

・アンケート調査
被災時に情報システムを復旧するために必要となる IT 資源（建屋、ハードウェア、データ等）について、事前の対策状況と被害状況に関するアンケートを実施した。アンケートの結果、効果のあった対策については、より具体的に実態を把握するため追加アンケートを実施した。
【第一回アンケート】　有効回答数 207 件
【第二回アンケート】　有効回答数 37 件

・ヒアリング調査
アンケート調査の結果から、一定の基準（比較的規模が大きく、かつ、被害の影響度が大きかった）から抽出した拠点に対し、状況の明確化や新たな知見の抽出を狙いとして、システム担当者に対するヒアリングを実施した。
【ヒアリング実施期間】　平成 23 年 10 月～12 月

D) 分析方法

調査結果から、事前対策の状況と被害状況との相関関係を求めることにより、該当する対策について効果の有無を分析した。

3 政府機関における情報システムへの影響

本調査・分析により明らかになった政府機関の情報システムへの影響について、地震・津波・計画停電の各脅威からの観点で概括する。

○ 地震による影響　　電力喪失とネットワーク障害による影響が大きかった。

今回の調査結果から、広域な電力喪失や、これに起因したネットワーク障害による影響が確認できた。具体的には、通信回線の遮断や輻輳等のため、システムの停止や縮退運用を余儀なくされた等の影響が生じていた。

一方で、地震の揺れによるシステムラックの倒壊等、ハードウェアの再調達を必要とするような被害はほとんど確認できなかった。これは、システムラックの固定措置等、基礎的な対策の効果によるものと考えられる。

アンケート及びヒアリングから得た主な地震による影響を以下に示す。
・建屋に対する被害の傾向としては、躯体自体への影響は見られず、壁のヒビやタイルの剥がれ、エレベータの故障等であった。
・システムラック損壊等、ハードウェアへの甚大な被害報告は確認できていない。

・大規模な停電が発生し通信回線も使用不能となったため、情報システムが使用できない状態が２日間程度続いた。
・電力回復後に通信回線も復旧し、情報システムも問題なく使用再開できた。

○　津波による影響　　**建物損壊やネットワーク寸断に対する影響が大きかった。**

津波による影響として、土砂や浸水による建物や設備（電源等）の損壊・流失や、交通網・通信回線の途絶が確認できた。これらは、復旧の長期化や代替拠点への移転を余儀なくさせる等、甚大な被害を引き起こす想定外の脅威であった。特に、建物や設備、ネットワーク、人的被害の影響が大きく表れていた。

アンケート及びヒアリングから得た主な津波による影響を以下に示す。
・被害の大半は建物の１階部分が水没したことによるものだった。中には３階天井付近まで浸水した拠点もあった。
・被害の大半は、浸水によるネットワーク機器や周辺機器類の損壊、通信回線の断絶等であった。
・拠点によっては、周辺の浸水により外部から孤立した状態が数日間続いた。
・業務再開までの時間が数週間～数ヶ月と長期化し、代替地への移転を余儀なくされた拠点もあった。

○　計画停電による影響　　**人的リソースに対する負荷が大きかった。**

今回の調査結果からは、計画停電によって稼働中のサーバが正常終了しなかったことによるシステム障害は確認できていない。
しかしながら、事前のシステム停止作業等、計画停電への対応が度々生じたことや、通常は情報システムで行う業務を手作業で代替したこと等による人的リソースに対する負荷の影響が表れていた。

アンケート及びヒアリングから得た主な計画停電による影響を以下に示す。
・計画停電の実施情報が直前に変更される等曖昧であったため、システム停止作業に苦慮した。
・計画停電に備え、ベンダに対して夜間も含めた待機要請を複数回行ったが、実際に停電は実施されなかった。
・計画停電に備え、注意事項の周知徹底（データ保存やシステム停止等）に多大な労力を費やした。

4　今後の対策

今回の調査・分析によって得られた知見から高い効果が見込める対策について、比較的大きな予算措置は必要とせず速やかに対策の検討・着手が可能な対策を「短期で対応が可

能な対策」として示す。また、中長期的な検討が必要な対策を「中長期的な対策」として示す。

A) 短期で対応が可能な対策

○ 電力やネットワーク等の外部サービスの停止に備えた対策

外部サービスによる電力供給が停止した場合に備え、自家発電装置の総電力容量を勘案し、非常時でも運用継続が必要な情報システムを事前に決定しておくことが求められる。また、非常時には停止させる情報システムにおいて、正常に停止できるように無停電電源装置を適切に維持することが求められる。

その他、ネットワークの停止に備えた対策として、ネットワークの冗長化が考えられるが、この時、主回線と副回線が同時被災することを避けるための対策が望まれる。

○ ハードウェアの損壊、データの損失等、情報システムへの直接的な被害に備えた対策

今回の調査結果から、バックアップデータの外部保管や復旧手順書の整備等、従来から重要性が認識されていた災害対策は、総じて東日本大震災においても有効性が認められた。一方で、そのような対策は「当然基本として実施されている」と認識されがちであるが、必ずしも実施されていないケースも確認できた。府省庁においては、情報システムに必要な対策が適切に実施されているか改めて確認し、対策を推進していくことが求められる。また、実施済みの対策が非常時においても正常に機能することを確認しておくことが求められる。

○ 非常時の対応能力の向上を図るための対策

非常時において重要なのは、組織や個人が、発生した状況を見極め、迅速に対応方針を決め、行動できる力である。このような対応能力の向上を図るため、非常事態を疑似体験する訓練を通して継続的に経験を積むことは、非常に有効であると考えられる。

B) 中長期的な対策

非常時でも運用継続が求められる重要な業務で使用する情報システムにおいては、情報システムの更新等のタイミングで、災害リスクの低い立地条件を満たす外部の堅牢なデータセンタの利用を検討することが望ましい。この時、ネットワーク経由で情報システムを利用することとなるため、新たにネットワーク停止のリスクが発生する。これに備え、モバイル端末からの情報システムの利用等、複数の情報システムの利用手段が可能であることが望ましい。

第５節 各府省庁における主な取組事例（推奨事例）

1 推奨事例の選定対象と選定目的

各府省庁が平成 23 年度に独自に取り組んだ情報セキュリティ対策を選定対象として推奨事例を選定する。これにより、当該府省庁の独自性や創意工夫を評価しモチベーションを高めるとともに、府省庁間における取組事例の共有を通じて政府機関全体としての情報セキュリティマネジメント水準の向上を図ることを目的としている。

2 選定の方法

各府省庁の情報セキュリティ報告書に記載されている取組事項から取り上げた推奨事例候補となり得る取組について、最高情報セキュリティアドバイザー等連絡会議で相互に評価した上で推奨事例候補として NISC へ推薦する。NISC は推薦された取組事例から、他府省庁の模範となる工夫が見られる、参考にすべき優れた取組事例であることを基準として、推奨事例を選定する。また選定に当たり特に以下の二点を重視する。

・政府機関全体への展開・共有に取組やすく、費用・能力も含め実施可能であること
・情報セキュリティマネジメント水準の向上につながること

3 推奨事例

A) 推奨事例

第８回最高情報セキュリティアドバイザー等連絡会議（平成 24 年５月８日開催）において、推奨事例候補として５件が推薦され、NISC は推薦された候補について改めて検討を行った。結果、５件全てについて推奨事例とすることとした。

平成 23 年度の各府省庁の取組を受け、新たに推奨事例とするものは次のとおりである。

○ 障害・事故等が発生した場合を想定した、より迅速かつ的確な対応のための支援体制の充実化（外務省）
○ 情報セキュリティ関係資料のワンストップ化（経済産業省）
○ 省内課室における情報管理に係る運用手続きや体制整備の検討・策定（経済産業省）
○ 不審メール受信時の対策の強化（２件）
　・受信したフリーメール情報と不審メール情報の照合及びポップアップメッセージによる注意喚起（文部科学省）
　・メールフィルターによる不審メール対策の強化（国土交通省）

B) 推奨事例概要

ア）障害・事故等が発生した場合を想定した支援体制（CSIRT 体制）の充実化

障害・事故等の発生時により迅速かつ的確に対応し、普段からの事前準備体制を整えるべく、省内の CSIRT 体制を充実し、CSIRT メンバーによる机上演習を行いつつ、実際に機能するマニュアルを整備してきている。また、有識者等の専門家を講師として招き、CSIRT メンバーや一般職員向けに研修や勉強会を随時開催し意識啓発に努めている。

イ）情報セキュリティ関連資料のワンストップ化

省内イントラネットのトップページに「情報セキュリティコーナー」としてバナーを設け、職員がいつでも必要な資料を閲覧できるように情報セキュリティ関係の資料をワンストップ化して掲示した。資料は内容ごとに分類し、常に最新の情報が掲載されるよう適宜追加・見直しを行っている。結果的に、単純な問合せであれば参照先を指示するのみで解決できるようになり、情報セキュリティ担当職員の業務効率化にも寄与している。

ウ）省内課室における情報管理に係る運用手続きや体制整備の検討・策定

情報管理の徹底を目的として、省内課室における情報管理に係る運用手続きや体制整備を検討し、経済産業省情報セキュリティポリシーに従い、(イ）保有する情報の洗い出し、(ロ）機密性の格付の決定、(ハ）情報の格付に応じた取扱いの決定を行い、課内の体制整備を行った。結果として、課室ごとに適切なリスクマネジメントに取り組めるようになり、また、機密性の高い情報を省内で横断的に把握することが可能となった。

エ）不審メール受信時の対策の強化

①受信したフリーメール情報と不審メール情報の照合及びポップアップメッセージによる注意喚起

受信したフリーメール情報と GSOC から提供される不審メール情報をメールソフト上で自動的に照合し、酷似するものについては警告メッセージを表示して職員に注意喚起を行っている。また、フリーメールを開封しようとするとポップアップメッセージが表示される仕組みも構築した。

②メールフィルターによる不審メール対策の強化

外部から受信するメール全てについて、省庁ドメインの詐称が疑われるメールや、フリーメールドメインから送信されたメールについて、警告文を本文中に挿入する機能をメールフィルターに追加した。

C) 選定理由

ア）障害・事故等が発生した場合を想定した支援体制（CSIRT 体制）の充実化

今後、各府省庁において CSIRT の機能を有する体制を整備していくこととされているが、CSIRT 体制を充実させるためには継続的な教育・研修は欠かすことのできないものである。本取組では、障害・事故等とその対応を机上演習し、実用可能なマニュアルの整備を通じ CSIRT メンバーの意識啓発を図っている。さらには、教育・研修を通じて外部専門機関や専門家との人的、組織的な連携も広げている。これから CSIRT 体制を整備しようとする各府省庁が平時に行う準備として参考にすべき活動が多く盛り込まれた取組である。

イ）情報セキュリティ関連資料のワンストップ化

情報セキュリティに関する情報を体系的に提供することは、必要な情報へのアクセスが容易となることで職員への周知徹底が図りやすくなること、また、各種問合せ窓口の明確化によりマネジメント水準全体の向上にも寄与することが期待される。一方、取り組むためのコストの観点からも、本取組に特別な情報システムは不要であり、比較的着手しやすい点も含めて優れた取組事例であるといえる。また、この取組によって情報セキュリティ担当者の業務効率化、省力化も実現されている。

ウ）省内課室における情報管理に係る運用手続きや体制整備の検討・策定

個別の情報資産の洗い出しと格付の徹底は情報セキュリティ対策の基本的な取組であり、基本的な実施方法をルール化することは望ましい取組といえる。また、その策定に当たって複数のパイロットケースを構築し、それらを他の課室が参照して自課室のルールを作成するというプロセスを採ったことは、職員一人ひとりの情報管理意識の向上に寄与し、PDCA サイクルを向上させる自律的な行動にもつながるものである。

エ）不審メール受信時の対策の強化

①受信したフリーメール情報と不審メール情報の照合及びポップアップメッセージによる注意喚起

標的型メールはフリーメールからのものが多いことに加え、自組織の受信したメール情報を利用してカスタマイズしていることから、より精度の高い効果が期待される。また、注意喚起としてポップアップメッセージを表示することは、ウイルス感染等を抑止する効果が期待できる。

②メールフィルターによる不審メール対策の強化

不審メールの排除には、システム的に排除可能であればその対応が望ましい。本取組はフリーメールドメインから送信されたメールには警告文を本文中に挿入するという簡易な方法でそれを実現している。また保守契約の範囲内で実施されており、他府省庁でも取組みやすいものである。

4 所見

A) 平成 22 年度の推奨事例に関する各府省庁での採用・取組状況について

各府省庁で議論し実態に則した独自の取組へと発展させることを期待し、平成 22 年度は次の５つの取組を推奨事例と定めた。

≪平成 22 年度の推奨事例≫

○標的型メール攻撃に対する訓練
○自己点検内容の徹底した重点化
○秘密文書の管理に関する規程と情報セキュリティ関連規程の統合
○検疫認証システムの導入、自府省庁外への電子メールの暗号化機能の導入及び IPv6 も考慮した公開ウェブサーバのセキュリティ対策
○LAN パソコンのワープロソフト及び電子メールにおける情報の格付を自動付与する仕組みの導入

これら推奨事例に関する各府省庁での取組状況について、平成 24 年３月にアンケートを実施した（表　3-1 参照）。結果、５つの推奨事例のうち、「標的型メール攻撃に対する訓練」「自己点検内容の徹底した重点化」「LAN パソコンのワープロソフト及び電子メールにおける情報の格付を自動付与する仕組みの導入」の３件については、NISC が推奨事例と定めた意図を各府省庁において十分に把握し検討され、それぞれの活動へと浸透させていることが認められた。

一方、「秘密文書の管理に関する規程と情報セキュリティ関連規程の統合」「検疫認証システムの導入、自府省庁外への電子メールの暗号化機能の導入及び IPv6 も考慮した公開ウェブサーバのセキュリティ対策」の２件については、内容的に単年度で取組むことが困難な内容であると考えられ、アンケートで検討中や準備中と回答した府省庁も複数あった。従って、この２件は引き続き推奨事例と位置づけ、依然として対策が不十分と自ら認識する府省庁については継続して取組を進めていただきたい。

表 3-1　平成 22 年度の推奨事例実施状況に関するアンケート結果

推奨事例	概要	回答府省庁数	主なコメント
標的型メール攻撃に対する訓練	不正なプログラムをメールで送り込む攻撃に適切に対応するとともに、職員の情報セキュリティ意識向上を図る目的で実施。実在の不審メール情報等を題材に訓練メールを作成し職員へ送付、訓練メールを開封した職員へは注意喚起を促すコンテンツを表示した。実施結果を分析し教育内容にも反映している。	採用 17	NISC が行った訓練に参加。
		不採用 3	平成 24 年度は訓練を実施予定。

自己点検内容の徹底した重点化	自己点検への職員の負担感を省き実効性を上げることを目的として、自己点検票の内容を重点化、記入の容易化を図った。結果、把握率の向上とともに、各職員自身が自らの役割を再認識し情報セキュリティに対する意識の向上にもつながった。	採用 20	NISC の点検票雛型を活用。
		不採用 0	ー
秘密文書の管理に関する規程と情報セキュリティ関連規程の統合	両規程の棲み分けが不明瞭なことから、秘密文書の管理に係る規程を情報セキュリティ関連規程等へ取り込み、職員の分かりづらさを解消させた。これにより機密性区分の統一や情報管理責任者の明確化が行われ、今後情報管理の徹底が一層強化されることを見込んでいる。	採用 3	具体的改定案を作成中。 現行規程で既に対応済み。
		不採用 17	両規程の棲み分けは明確。 重複項目は少数。特段の問題はない。
検疫認証システムの導入、自府省庁外への電子メールの暗号化機能の導入及びIPv6も考慮した公開ウェブサーバのセキュリティ対策	基幹ネットワークの更新にあわせて統合的なセキュリティ対策を実施した。内閣府 LAN のシステムに含まれるホームページを統合集約したことにより、効率的な運用が行われると同時に最新の対策が取られたシステム内での運用が可能となり安全性も向上した。	採用 8 （複数回答）	一部機能は導入済み。システム更改に向けて要件策定中。
		不採用 16 （複数回答）	費用対効果も含め検討中。 独自の運用により同等以上の効果を得られている。
LAN パソコンのワープロソフト及び電子メールにおける情報の格付を自動付与する仕組みの導入	文書作成時のヘッダに「機密性〇情報」、「〇〇限り」、メール作成時の件名に「機〇」が自動的に挿入されるようにした。〇の部分は職員が自ら格付等を記入することとなるため、具体的にどのような格付をして明示すればよいかを多数例示した「情報の格付マニュアル・情報の格付及び取扱制限のルール」を作成した。	採用 9	明記方法や記載例等のマニュアル、手順書をイントラネットに掲載。
		不採用 11	形式的な格付の記載を危惧。

B) 平成 23 年度の推奨事例の選定について

平成 23 年度の推奨事例候補の選定に当たっては、当初、NISC が各府省庁の情報セキュリティ報告書及び概要資料から抽出した取組の件数は 48 件に上った。重複する取組の整理や、他府省庁への模範とする工夫が見られるか等を検討した後 20 件に絞り込み、そ

れらを各府省庁に意見照会した。そして最高情報セキュリティアドバイザー等連絡会議で議論を行い、結果として平成 23 年度の推奨事例は５件とした。一方、推奨事例以外の各府省庁の取組についても参考とすべき内容が多く含まれることから、それらもここに紹介し、全体を総括して平成 23 年度の推奨事例の選定に関して所見を述べることとする。

表 3-2　推奨事例以外の参考とすべき取組

取組概要	府省庁名
自己点検結果を踏まえた情報セキュリティ教育（ｅラーニング）の見直しを実施。自己点検と教育を連携させ体系化することで、職員の理解度と統一的なレベル向上を図った。	公正取引委員会
脆弱性検査のフォローアップ強化。書面報告に加え、技術的な再検査を再度実施した。	文部科学省
暗号化、パスワードロック、遠隔操作での利用停止等の機能を有するセキュア USB を導入。	環境省
省内ネットワークからのみ申請可能なオンラインストレージシステムを構築。暗号化通信、期限付き、PW 付き、申請手続き等の機能を装備。	環境省
情報システム利用者の認証ログインカードとして身分証 IC カードを利用し、不正利用リスクの低減を図った。	防衛省
職員の情報セキュリティ意識向上・維持のために、状況に応じて講師や内容を変えた情報セキュリティ教育を、年間を通じて定期開催した。	厚生労働省
標的型メールを模倣した訓練メールを２回配信し、２回とも開封した職員に対して、訓練効果を高めるための座学研修を別途実施した。	経済産業省
本省及び地方支分部局も含めた省内全組織で自立した内部監査の実施体制を構築。セキュリティマネジメント水準を向上させた。	国土交通省
情報セキュリティ監査において外部監査を導入、客観的視点から課題を抽出し改善計画の立案に取り組んだ。	消費者庁
例年、無作為に抽出した業務システムに対して外部監査を実施。監査後には、脆弱性対策の進行状況を定期的に確認している。	外務省
国内外の情報セキュリティ関連情報の収集を日々行い、省内・在外職員への注意喚起や情報システムに関する対策への早期対策の検討に役立てた。	外務省
障害事故の原因究明の手掛かりとなる監査証跡の取得を強化。端末に証跡取得のプログラムを導入し、端末動作や外部出力の履歴取得を拡充した。	防衛省
自省が運営し外部公開している全てのウェブサーバについて、脆弱性検査を実施。脆弱性の検出状況について、推奨する対策等とともに報告書にまとめて担当者に通知し、脆弱性への対応が全て完了するまでフォローアップを実施。	総務省
登録したUSBメモリ以外の使用を強制的に排除するUSBデバイス管理を	防衛省

導入。情報流出やウイルス感染への対策を向上させた。	
部内系領域、部外系領域及び部内系－部外系間の系間データ移動において異なるウイルス対策ソフトを導入し、不正プログラムを検知するためのパターンマッチングでの網羅性の強化及び領域を跨いで不正プログラムが移動する際の重層的なウイルスチェックを行うことにより不正プログラム対策の強化を図った。	防衛省

表　3-2　推奨事例以外の参考とすべき取組の各取組は、各府省庁の最高情報セキュリティアドバイザーに意見照会をした推奨事例候補から、推奨事例となった５件を除いた15 件の取組である。教育・訓練に関するもの、脆弱性検査や監査に関するもの、情報共有に関するもの、情報システムによる対策強化に関するものなど、様々なタイプが揃った。

教育面では、自己点検と情報セキュリティ教育を連携させた取組、通年で定期的な教育機会を設け時々の状況に応じたテーマで教育を実施する取組など、教育効果の向上や継続性に関する工夫が随所に見られた。教育は即日成果が上がる類のものではないが、個々の職員に着実に情報セキュリティ意識を浸透させていくために最も注力すべき取組の一つである。

脆弱性検査や監査に関する取組としては、脆弱性の改修後に技術的な再検査を実施した取組、地方支分部局等も含めた内部相互監査を行える体制づくりに注力した取組など、各府省庁が限られたリソースの中で成果を上げるべくフォローアップを強化した取組が複数見られた。これらの活動は、強固な情報システムや情報セキュリティ体制を構築するためには有効性の高い取組といえる。

情報共有に関しては、推奨事例とした情報セキュリティに関係する情報をイントラネット上に集約する取組の他にも、自組織の体制強化のために独自に国内外の最新情報を収集し発信する取組があった。情報収集や情報共有は担当部門として日常的な活動であるが、早期に把握した脅威情報に基づいて自組織の体制強化へも貢献が期待される重要な取組の一つと考えられる。また、担当者の得意分野に応じて様々なソースやレベルから着手することが可能であり、その結果として担当者自身のスキル向上や業務効率化につながる一面もあるため、日々の業務負担を差し引いても取り組む意義は十分にあると考えられる。

その他、情報システムに係る取組として、セキュア USB の導入やオンラインストレージの活用、情報システムの利用者認証の強化、監査証跡の取得拡充に関するプログラムの導入等、幅広い取組が見られた。

平成 23 年度は最高情報セキュリティアドバイザー等連絡会議での議論を経て、新たに５件の取組を推奨事例として決定した。NISC ではこれらの取組が政府機関全体に適切な形で浸透するよう技術的な支援、情報の提供等の活動を実施していく。一方、各府省庁においては、推奨事例を自府省庁の実態に即しながら独自の取組へと発展させ、次年度以降の情報セキュリティ報告書へそれらの活動が記載されることを期待している。また、

推奨事例以外の参考とすべき取組についても、是非自府省庁の情報セキュリティ対策に係る活動の参考としていただきたい。

第4章 平成 24 年度に取り組むべき政府機関の課題

平成 23 年度における国内外の情報セキュリティに関する動向や政府機関における取組の評価結果等を踏まえ、平成 24 年度に取り組むべき主な課題として、以下の事項があげられる。

1 情報セキュリティに関する動向を踏まえた課題

A) 巧妙化している標的型攻撃の発生等に対応するための体制の整備

平成 23 年度は、政府機関や国の重要な情報を扱う企業等を対象とした標的型攻撃が顕在化した。今後、こうした攻撃手法は、より巧妙化することが予想されることから、それぞれの政府機関においてインシデントに機動的に対応するための組織内 CSIRT 等の機能を有する体制を早急に整備していく必要がある。また、大規模なインシデント等が発生した際に、政府機関として迅速かつ的確に対応するためには、能力を持った者が組織を越えて機動的に支援できるような協力体制の構築も必要である。なお、体制を構築し適切な運用を図るためには、平素から要員の技能の維持向上を図るための継続的な研修や、各府省庁や関係機関と連携した対処訓練を定期的に実施していくことも重要である。

B) スマートフォンに対する情報セキュリティ対策の強化

スマートフォンやタブレット端末の利用が拡大し、平成 23 年度には国内出荷台数の過半数をスマートフォンが占める見通しとなっている[19]。これらスマートフォンやタブレット端末は、クラウドサービスや SNS 等と連携することによる利便性の向上や業務で使用する BYOD（Bring Your Own Device）の拡大等、ネットワーク環境の進化に合わせて IT を利用する環境も、今後ますます進化していくことが予想される。

一方で、スマートフォンやタブレット端末に格納された個人情報や機密情報を標的とした攻撃も顕在化しつつあるため、その動向について十分注視するとともに、BYOD の利活用等を含め情報セキュリティ対策が確実に実施されるよう政府機関統一基準群の見直しを図っていく必要がある。

C) 利用環境の変化に対する情報セキュリティ対策の強化

複数の府省庁で共通的に使用する基盤となる情報システムについては、これを使用する府省庁の情報システムと連携して運用管理され、相互に影響を及ぼす関係にあることから、全体として適切な情報セキュリティ水準が確保されるような枠組みを構築していく必要がある。

また、政府横断的な検討が進められている社会保障・税番号制度及び国民 ID 制度については、国民の安心と利便性を確保するため、適切な個人情報保護と情報セキュリティに配慮した制度の具体化に向けた検討を行っていく必要がある。

[19] 出展 ： MM 総研 2012 年 3 月 13 日発表記事に基づく

D) 安全な暗号利用の促進

現在、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は、第１章第１節 5　　B）に記述したとおり、危険度１（理論的な暗号解読アルゴリズムが公開された状態）であり必ずしも安全とは言えない状態である。このため、平成 23 年度は、暗号アルゴリズムの急激な安全性の低下に備え、緊急避難的な対応計画（コンティンジェンシープラン；平成 22 年度に策定済み）に係る発動要件の決定を行う等の取組を実施した。

今後、各府省庁においては、平成 24 年度に改定が予定されている新たな電子政府推奨暗号リストの内容も踏まえ、安全性の低下が指摘されている暗号アルゴリズムからの着実な移行を実施することが求められる。

また、NISC においては、暗号アルゴリズムの安全性の状況の監視及び認証事業者等外部動向の把握を行い、必要な情報を速やかに各府省庁に提供することが必要である。

2 政府機関における取組に係る評価結果等を踏まえた課題

A) 対策実施状況報告及び重点検査に係る評価結果を踏まえた課題

平成 23 年度の政府機関における対策実施状況報告、重点検査の結果によれば、全体として、一定水準以上の情報セキュリティ対策を確保していると言えるが、一方で「情報の取扱い」に関する項目について、昨年度より改善は認められるものの、まだ取組みが不十分な省庁が多い等、職員に対する教育プログラムの更なる充実強化が必要である。また、システム面においては、「SSL バージョン２の無効化」や「強度の弱い暗号方式の無効化」、「大量パケット送信型の DoS 攻撃への対応」等について必ずしも適切な対応が図られていないところもあり、政府機関全体として対策が確実に実施されるよう、必要な措置を講じていく必要がある。

B) 「東日本大震災における政府機関の情報システムに対する被災状況の調査及び分析」を踏まえた課題

東日本大震災における政府機関の情報システムに対する被災状況の調査及び分析を行った結果、優先的に取り組むべき対策がいくつか挙げられており、これらについては、各情報システムに適用した際の費用対効果も検討した上で、情報システムの運用継続に向けた対策に速やかに反映していくとともに、自府省庁の情報システム運用継続計画を適時見直していくことが必要である。

C) 公開ウェブサーバの脆弱性検査結果を踏まえた課題

平成 23 年度に実施した同検査の結果、複数の府省庁の公開ウェブサーバにおいて、危険度高に相当する脆弱性が確認された。各府省庁においては、NISC の発出した注意喚起等に基づき、管理している公開ウェブサーバについて確認の上、脆弱性の存在しないことが確認できない場合には、関係者及び関係事業者と調整の上、適切に措置を講ずることが求められる。

また、平成 24 年度においても、引き続き公開ウェブサーバの脆弱性検査を実施し、得られた結果を全府省庁で共有して、政府機関全体の底上げを図っていく必要がある。

D) 送信ドメイン認証に関する取組結果を踏まえた課題

政府機関において、送信ドメイン認証に関する取組を推進した結果、平成 24 年３月 31 日現在で、政府機関における送信側 DNS サーバの SPF 設定率は、97%以上を達成した。この結果、我が国のほとんどの政府ドメイン（第３レベルの go.jp ドメイン）にはなりすまし対策が講じられていることとなり、メールを受信する側において SPF 対策が適切に講じられてさえいれば、政府機関の職員を騙った単純ななりすましが困難な状態となった。今後は、政府機関における受信側 SPF 対策を進めるだけでなく、この事実を国民に向けても広く周知し、受信側対策の一層の推進を促していくことが必要である。

また、平成 24 年度は、各府省庁において引き続き、SPF レコードの末尾を"-all"と記述することやサブドメインに係る対策、受信側における SPF 対策を推進するとともに、DKIM や S/MIME 等の暗号技術を利用した対策を積極的に検討していくことが求められる。

E) 標的型不審メール対処訓練結果を踏まえた課題

平成 23 年度に実施した標的型不審メール対処訓練は、政府機関において大規模に実施する初めての取組であったが、実施府省庁の担当者へのヒアリング結果によれば、「有効であった」との回答が大半を占めていたことから、一定の有効性はあったと認められる。

本訓練を一過性のものとすることなく、今後も巧妙化すると予想される攻撃手法の動向を把握するなどして、平成 24 年度以降も訓練手法を改善しつつ、継続していくことが必要である。

また、各府省庁においては、自組織で最大の効果を上げるための訓練方法や内容を熟考し、主体的に取り組むことが求められる。

F) 政府機関情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築

政府機関の情報システムにおいて適切に情報セキュリティ対策を講じるためには、情報システムのライフサイクルにおける企画・設計段階から調達仕様にセキュリティ要件を適切に組み込むことが重要である。その観点から、NISC は平成 23 年３月に「情報システムに係る政府機関におけるセキュリティ要件策定マニュアル」（SBD マニュアル）を策定し各府省庁に情報提供を行った。しかし、各府省庁の調達仕様書に記載すべきセキュリティ要件が十分ではないと思われるケースが存在しており、また、SBD の活用事例も少なく、十分普及しているとは言い難い状況である。

このため、各府省庁においては、組織内で SBD マニュアルの普及促進を図ることや最高情報セキュリティアドバイザーが調達仕様書の作成段階から積極的に関与する等、適切なセキュリティ要件を調達仕様書に記載することにより、設計段階におけるセキュリティ要件の精緻化を行うことが求められる。NISC においては、SBD マニュアルの利便性・簡便性の向上、内容の高度化、各府省庁における普及促進の支援などに引き続き取り組むことが必要である。

G) 情報セキュリティ報告書の記載内容を踏まえた課題

各府省庁が作成した情報セキュリティ報告書から、平成 23 年度に幾つかの府省庁において、深刻な情報漏えいにつながりかねない障害・事故等が発生していたことが分かる。これら障害・事故等の事例及びそれに基づき実施された対策について、発生府省庁だけではなく他府省庁においても参考とすることにより、政府機関全体で障害・事故等の発生防止に向けた取組を強化していく必要がある。

また、情報セキュリティ報告書については、平成 24 年度から全ての府省庁において公表しており、他の府省庁における記載内容等も参考にしながら、より国民に分かりやすい情報セキュリティ報告書の作成が望まれる。

参考1　政府機関に係る情報セキュリティ対策の主な取組

時期(年月)	主な取組
平成 17 年４月	○　内閣官房情報セキュリティセンターの発足
平成 17 年 12 月	○　政府機関統一基準（初版）の決定
平成 18 年２月	○　第１次情報セキュリティ基本計画の決定
平成 18 年６月	○　セキュア・ジャパン２００６の決定
平成 19 年６月	○　セキュア・ジャパン２００７の決定
平成 19 年６月	○　政府機関統一基準（第２版）の決定 ＜主な改訂内容＞ IPv6 対応、踏み台対策、暗号モジュール試験・認証制度の利用、情報セキュリティ監査体制の明確化、情報システム台帳の整備
平成 20 年２月	○　政府機関統一基準（第３版）の決定 ＜主な改訂内容＞ DNS キャッシュポイズニング対策、 なりすましサイト対策としてのドメインネーム管理
平成 20 年４月	○　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 に係る移行指針の決定
平成 20 年６月	○　セキュア・ジャパン２００８の決定
平成 21 年２月	○　第２次情報セキュリティ基本計画の決定
平成 21 年２月	○　政府機関統一基準（第４版）の決定 ＜主な改訂内容＞ 第二次基本計画への対応(セキュリティアドバイザーの義務化)、ボット対策の強化、ウェブの閲覧・送信時の危険性への対応、無線 LAN 環境の脆弱性への対応、基礎編とシステム編への整理
平成 21 年６月	○　セキュア・ジャパン２００９の決定
平成 21 年６月	○　政府機関のサーバ集約化について決定
平成 21 年９月	○　情報セキュリティ報告書作成のためのガイドライン(情報セキュリティ報告書専門委員会報告書）の策定
平成 22 年５月	○　国民を守る情報セキュリティ戦略の決定
平成 22 年５月	○　政府機関統一基準（第４版（平成 21 年度修正））の決定 ＜主な改訂内容＞ 消費者庁の追加
平成 22 年７月	○　情報セキュリティ２０１０の決定
平成 23 年３月	○　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の策定
平成 23 年３月	○　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

平成 23 年４月	○ 統一管理基準及び技術基準の決定 ＜主な改訂内容＞ ・政府機関統一基準の全体構成の見直し － 統一管理基準（基本的基準）と統一技術基準（技術的基準）への分離 － 「政府機関の情報セキュリティ対策の強化に関する基本方針」を廃止し、新たに「政府機関の情報セキュリティのための統一規範」を策定 － 「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」を改正 ・クラウド技術や外部からの不正アクセスに係る対応、教育・人材育成に係る遵守事項の充実
平成 23 年５月	○ 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 22 年度）の決定
平成 23 年７月	○ 情報セキュリティ２０１１の決定
平成 24 年１月	○ 情報セキュリティ対策に関する官民連携の在り方について（官民連携の強化のための分科会報告）の決定
平成 24 年１月	○ 調達における情報セキュリティ要件の記載について（内閣官房副長官より各府省庁大臣官房長等あて）を通知
平成 24 年４月	○ 統一管理基準及び技術基準（平成 24 年度改定）の決定 ＜主な改訂内容＞ ・新たな脅威等への対応（標的型攻撃への対策、適切な管理者権限管理、障害・事故等への対処体制の整備、東日本大震災を踏まえた情報システム運用継続の取組） ・情報技術・利用環境の変化への対応（共通基盤システムのセキュリティ体制整備､情報を取り扱う区域の物理的セキュリティ対策、IPv6 に関する技術的対策等） ・基準の運用の実効性担保（調達における SBD マニュアルの活用、「基本遵守事項」「強化遵守事項」の一元化）