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）

平成 25 年6月 19 日

情報セキュリティ対策推進会議

目　　次

近年のサイバー攻撃を取り巻く国際的な情勢を俯瞰すると、情報システムや情報通信ネットワークを悪用した不正侵入、情報の窃取、改ざん、破壊、サービスの途絶といったサイバー攻撃の脅威がますます増大している。我が国においても諸外国と同様に、政府、民間などを問わずサイバー攻撃の脅威にさらされているところであるが、その手法は年々複雑・巧妙化してきている。

政府は、国民や国を守り、一層の発展に向けて、諸施策を遂行するため、国民から大切な情報を預かり、また、国としての意思決定等に不可欠な情報を保有している。そして情報システムを用いて国民に情報を提供し、また業務を執行するなど、様々な重要な情報を情報システムで処理している。政府としては、このような大切な情報やこれを取り扱う情報システムをサイバー攻撃などの脅威から守るために、これまで必要な対策の実施について全力で取り組んできたところである。

このような中、平成 24 年度においては、各府省庁と連携を取りながらサイバー攻撃などの事象が発生した際の体制づくりに特に注力したところである。具体的には、府省庁内における情報セキュリティ事象に迅速に対処するため、情報の集約・分析や責任者等への報告・連絡、関係機関との情報連携等の役割を担う体制として、組織内 CSIRT (Computer Security Incident Response Team)を全ての府省庁に整備した。また、昨年６月、政府一体となった対応が求められる事象が発生した際に、府省庁横断的に支援等を行うことが可能となるよう、情報セキュリティ緊急支援チーム（CYMAT）を設置し、職員に対して必要な研修・訓練を実施した。このほか、政府機関に対するサイバー攻撃が発生した際には、その都度、府省庁との間で迅速な情報共有などを図った。

このような取組を進めてきたところであるが、サイバー攻撃の脅威や手法については、世の中の技術の進歩等により容易に増大、複雑・巧妙化するものであり、引き続き、各府省庁と密接な連携のもと、サイバーセキュリティに関する様々な動向を迅速に把握するとともに、情報を収集・分析し、常に緊張感を持ち、情報セキュリティの更なる確保に向けて取り組んでまいりたい。

平成 25 年６月 17 日

政府 CISO
内閣官房情報セキュリティセンター長
櫻井　修一

第１編 平成 24 年度の情報セキュリティに関する脅威とその対策

第１節 平成 24 年度の我が国における情報セキュリティ事象の概要

近年、情報技術（以下「IT」と呼ぶ。）の高度化とその普及が進んでいる。世界中の企業等において、業務の高度化・効率化などの観点から、スマートフォンやクラウドコンピューティングサービスの本格的な利用拡大や、M2M[1]など、新しいITが注目されている。このようなITの高度化・普及に伴い、それらに係る情報セキュリティリスクが深刻化しつつある。

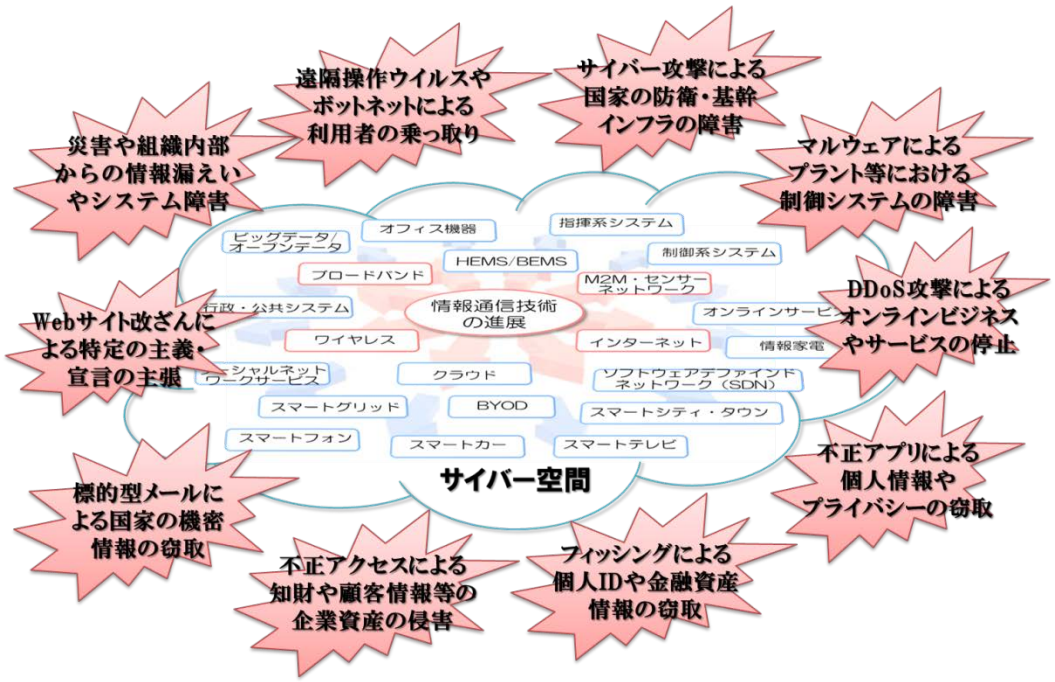


図 １－１ ITの高度化・普及に伴う情報セキュリティリスク深刻化のイメージ[2]

我が国における平成 24 年度の情報セキュリティ事象の例としては、個人情報漏えいに係る事象、データ消失事象、金融関連におけるフィッシング事象、遠隔操作ウイルス等による犯行予告事象、技術情報の流出事象など様々な事象があり、個人から、企業、重要インフラ企業、政府機関にいたるまで、幅広い領域において事象が発生した。

例えば、平成 24 年の上半期のみで、国内の個人情報漏えいに係る情報セキュリティ事象は 954 件あり、1 件の事象で約 40 万人分の個人情報が流出した事例があったという報告もある[3]。これらの事象の原因の 80%以上は、管理ミス、誤操作及び紛失・置き忘れ等の過失によるものであると報告されている（図 １－２）。

---

[1] Machine to Machine。ネットワークに繋がれた機械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。例えば、各種センサー・デバイス（情報家電、自動車、自動販売機、建築物、スマートフォン等）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、福祉等の多様な分野のサービスを実現するもの。

[2] http://www.nisc.go.jp/conference/seisaku/dai32/pdf/32shiryou0100.pdf［PDF］
「第 32 回会合 資料 1」（情報セキュリティ政策会議、平成 25 年２月 22 日）

[3] http://www.jnsa.org/
「2012 年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】」（特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）、平成 25 年４月 30 日）

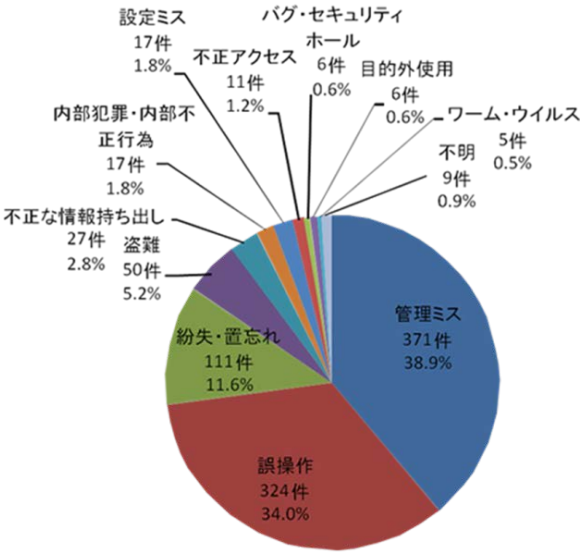


図 1－2 個人情報漏えいの原因

また、平成 24 年６月には、レンタルサーバ業者において、同事業者の過失により、顧客から預かっていたホームページやメール等のデータが大量に消失する事象も発生した。

一方、不正アクセス等の第三者による侵害が原因である情報セキュリティ事象に注目すると、不正侵入、情報の窃取や改ざん、破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃[4]等の、いわゆる「サイバー攻撃」と呼ばれるネットワーク経由の情報セキュリティ事象が多く、特に、国家や企業の機密情報等を窃取しようとするもの[5]や、重要なデータやシステムを破壊しようとするもの[6]などの事象が顕在化してきている。

例えば、警察庁では、平成 24 年中に合計 1,009 件の標的型メール[7]が国内の民間事業者等に送付されていたことを把握している[8]。

また、海外では、企業秘密等の窃取が狙われた標的型攻撃に外国政府の関与が疑われている問題も顕在化している[9]。今後、我が国に対しても外国政府が関与するサイバー攻撃が、いつ発生してもおかしくない状況にあり、グローバルなサプライチェーン等における一つの点への攻撃が他の拠点へも影響することが危惧される。

なお、平成 25 年３月に、韓国の複数の放送局や金融機関において、不正プログラム感染により同時多発的に大規模なシステム停止が発生する事象が発生したが、平成 24 年度に、国内において同様の事象の発生は確認されなかった。

---

[4] Distributed Denial of Services 攻撃（分散サービス不能攻撃）。

[5] 例えば、平成 23 年９月以降、議院、行政機関、防衛関連企業等への標的型攻撃による不正プログラム感染が発覚した。

[6] 例えば、平成 24 年８月頃、海外において、感染したコンピュータのマスターブートレコード（MBR）を改ざんするなどの手法を使って起動不能にさせる「Shamoon（シャムーン）」によるサイバー攻撃が発生した。

[7] ここでは、①迷惑メールと異なり、業務等に関連した内容を装うなど、一見すると正当なメールと区別がつきにくい、②市販のウイルス対策ソフトで検知できない不正プログラムに感染させようとする、との特徴があるメール。

[8] http://www.npa.go.jp/keibi/biki3/250228kouhou.pdf［PDF］
「平成 24 年中のサイバー攻撃情勢について」（警察庁、平成 25 年２月 28 日）

[9] 例えば、米国におけるトレードシークレット（営業秘密）の窃取の抑制に関する戦略である Administration Strategy on Mitigating the Theft of U.S. Trade Secrets（White House, Feb. 2013）や国防総省による年次報告書である Annual Report to Congress（Department of Defence, May 2013)参照。

第２節 政府機関等における情報セキュリティ事象に照らした対策の取組

1 概説

平成 24 年度の政府機関等[10]における公表された主な情報セキュリティ事象を、資料編Hに示す。事象の主な原因は、職員の過失・故意とサイバー攻撃によるものであった。そしてサイバー攻撃が原因となっている事象は、示威を目的とするものや、国の重要な情報をねらったと考えられるものなど、政府機関等に特有なものが多い。

また、政府機関等に対するサイバー攻撃には様々な方法やレベルがあるが、平成 24 年度の事象では、主に示威を目的とするものによるウェブサイト等への攻撃と、国の重要な情報がねらわれた攻撃が特に注目される。

以下では、平成 24 年度に主に見られた３種類の事象「過失・故意による事象」「ウェブサイト等の攻撃事象」「国の重要な情報をねらう攻撃事象」ごとに、政府機関等における平時の取組、発生事象の分析及び発生事象への対応状況などを述べる。

2 職員の過失又は故意による情報セキュリティ事象とその対策の取組

職員の過失又は故意による情報セキュリティ事象への対策については、主に、職員が遵守すべき各種法令等（国家公務員法、行政機関の保有する個人情報の保護に関する法律、人事院規則及び情報セキュリティポリシー等）を職員が遵守・徹底等するよう、教育等によって浸透を図っているところである。

政府機関においては、「政府機関の情報セキュリティ対策のための統一規範[11]」、「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[12]」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[13]」からなる「政府機関の情報セキュリティ対策のための統一基準群」に基づき、各府省庁が情報セキュリティポリシーを定め、これを基本として情報セキュリティ対策を実施している。

この一環として、平成 24 年９月と平成 25 年２月に、内閣官房情報セキュリティセンター（以下「NISC」という。）主催で、各省における情報セキュリティポリシーの策定及び浸透を円滑に行うことに資するべく、各省の情報セキュリティ部局の職員を対象に、「統一基準群についての講演」や「最新脅威とそれを踏まえた職員教育・意識啓発の在り方についての勉強会」を開催した。

また、各府省庁は、各府省庁における情報セキュリティポリシーに基づく対策の実施状況の把握を目的に、原則全ての行政事務従事者を対象に年次で自己点検を実施しており、NISCは結果を集約している。平成 24 年度の対策の実施率の結果を見ると、行政事務従事者

---

[10] ここでは、行政府、立法府、司法府及び独立行政法人等をいう。

[11] http://www.nisc.go.jp/active/general/pdf/kihan24.pdf［PDF］
「政府機関の情報セキュリティ対策のための統一規範」（情報セキュリティ政策会議、平成 24 年４月 26 日改定）

[12] http://www.nisc.go.jp/active/general/pdf/k304-111.pdf［PDF］
「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 24 年度版）」（情報セキュリティ政策会議、平成 24 年４月 26 日改定）

[13] http://www.nisc.go.jp/active/general/pdf/k305-111.pdf［PDF］
「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）」（情報セキュリティ対策推進会議（CISO 等連絡会議）、平成 24 年４月 18 日改定）

の実施率[14]は 96.8%となっており、対策の浸透が認められる。ただし、項目別に見ると、「情報の取扱い」に関する項目のうち、特に、情報の格付・取扱い制限の決定・明示等を求めている「情報の作成と入手」項目については、実施率がほかの項目と比べて若干低い数値であった。行政事務従事者にとって情報の格付の決定・明示等の基本的な対策事項であることから、行政事務従事者に対する教育をPDCA(Plan-Do-Check-Action)サイクルの一環として計画的に実施していくことが求められる（第２編 第１節 参照)。

事象について見ると、平成 24 年度においても、機密情報が格納された PC や記録媒体を紛失した事象や、ファイル交換ソフトの使用による情報漏えい事象など、一定数の事象が依然として発生している。今後、更に事象数を減らすためには、情報セキュリティポリシー等の浸透だけでなく、機密情報への厳格なアクセス権管理とアクセスログ収集解析の導入や、業務で庁舎から外部に持ち出した機密情報を外部で安全に扱う仕組みの導入などの技術的な対策の導入が考えられる。また、行政事務の実状として、職員が情報セキュリティポリシーに実質的に抵触する可能性があっても自宅等の外部で機密性のある情報を含むデータを扱う業務を実施せざるを得ない場合があるなど、行政事務の実施方法自体に問題がある場合もあり、行政事務プロセスの改善の観点で対策を検討することも必要と考えられる。

3 ウェブサイト等への攻撃事象とその対策の取組

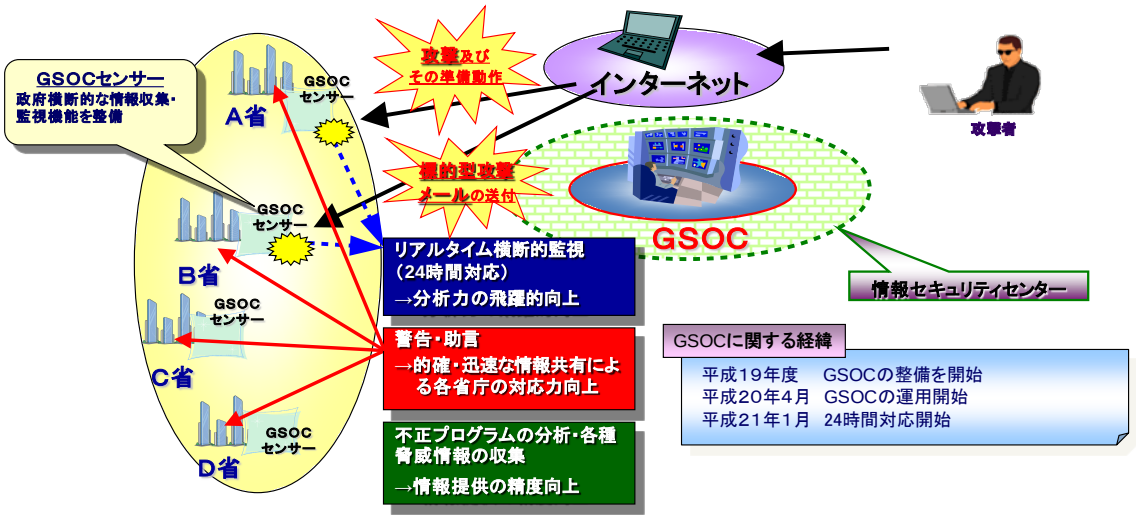
ウェブサイトへの攻撃のうち、不正アクセス（改ざん等）による攻撃は、ウェブサイトの設計開発段階で適切なセキュリティ対策を導入し[15]、運用時に随時ソフトウェア等の脆弱性対策をすることで、多くの攻撃を防ぐことができる。一方、DDoS攻撃対策は、攻撃の検知や緩和を行うための機器類の導入と運用や、通信事業者が提供する対策サービスの利用といった技術的・契約的な追加措置が必要であることから、費用対効果という観点を踏まえ、守るべき情報システムとして国民の生命や財産に関係するような重要なものを最優先で対処し、それ以外のものは優先度を下げるなど、メリハリを持って対策を講ずるアプローチが考えられる。

こうした事象に対し、NISC では、GSOC を設置し、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（コラム１ 参照)。

[14] 情報セキュリティポリシー記載の遵守内容について、責務が生じた者に占める対策を実施した者の割合。
[15] 例えば、IPA の「安全なウェブサイトの作り方」(http://www.ipa.go.jp/security/vuln/websecurity.html)や、LASDEC の「地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション)」(https://www.lasdec.or.jp/cms/12,28369,84.html)が参考にできる。

●コラム１： GSOC の概要

GSOC(Government Security Operation Coordination team)：政府機関情報セキュリティ横断監視・即応調整チーム。政府横断的な情報収集、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。内閣官房情報セキュリティセンターにおいて、平成 20 年(2008 年) 4 月から運用開始。



GSOC は、平時においては、ウェブサイト等への攻撃をはじ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。平成 24 年度においては、GSOC より 74 件の脆弱性情報を配信した（表 1－1）。

表 1－1 GSOC が配信したソフトウェアの脆弱性情報の件数の推移

	H22年度	H23年度	H24年度
・脆弱性情報等の配信	70 件	68 件	74 件

また、これらの政府機関等のセキュリティ対策を目的とした注意喚起以外にも、NISCでは国民のセキュリティ水準の低下を招くことを防止する観点から政府機関等が留意すべき事項も注意喚起文書として発出している。例えば、平成 24 年 7 月には、政府機関が国民向けに公開している情報システムにおいて、サポート有効期間が満了するJavaSE 6（又は対応する実行環境JRE 6）を国民のPCにインストールすることを推奨しないよう、注意喚起を発出した[16]（資料編G 参照）。

さらに、平成 24 年 9 月から平成 25 年 2 月にかけて、政府機関が運営するウェブサイトのうち約 300 画面を対象に、ウェブアプリケーションに関する脆弱性の有無について検査

[16] http://www.nisc.go.jp/active/general/pdf/javasupport_press_120717.pdf［PDF］
「JavaSE 6 のサポート有効期間の満了に係る対応について（注意喚起）」（NISC、平成 24 年 7 月 17 日）

を実施した。検査の結果、CVSS[17] を基にした４段階の評価基準のうち、最も危険性の高い「危険度高（CVSS基本値：7.0～10.0)」の脆弱性は検出されなかった。このレベルの脆弱性は、平成 23 年度の検査では検出されていたところ、その対策は進んでいると考えられる。また、「危険度中（CVSS基本値：5.0～6.9)」の脆弱性として、クロスサイトスクリプティング[18]の脆弱性が 10 画面（検査対象画面数の３％程度）検出された。これらについては計画的に対応を進めており、順次対応を終えているところである。

こうした脆弱性への対策促進については、システム担当者等への教育が重要であるところ、平成 24 年４月に、各府省庁の情報セキュリティ担当職員対象に、ウェブサーバのセキュリティに係る勉強会を開催した。勉強会では、外部専門家から、脆弱性を利用したウェブサーバへの攻撃事例や対策の必要性についての解説があり、脅威に関する知見や各種対策への理解を深めた。

なお、ウェブサイトへの不正アクセス等の攻撃への対策として、その設計開発段階で脆弱性を作り込まないようにウェブアプリケーションを開発するなど、適切なセキュリティ対策を導入することが重要である。

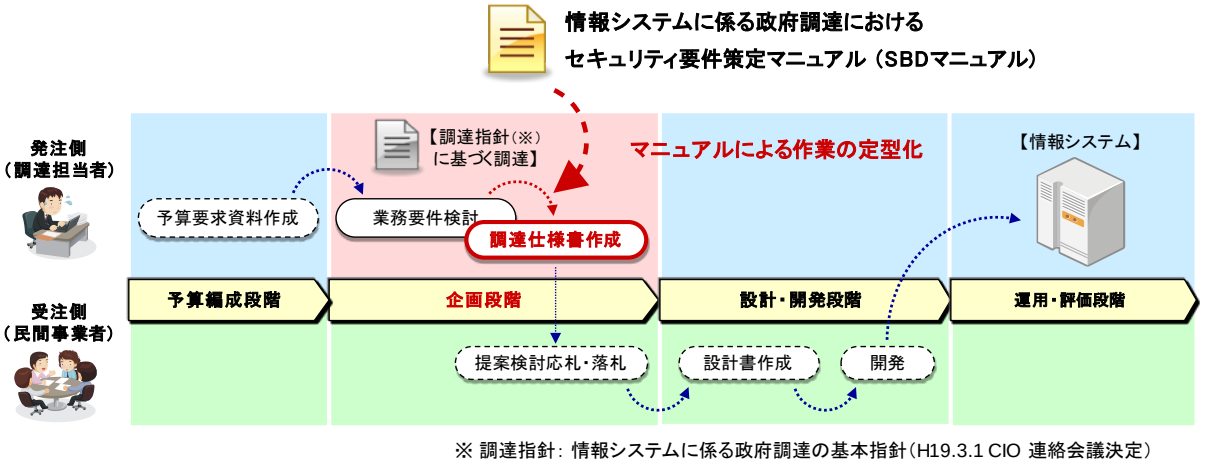
さらにNISCでは、ウェブサイトに限らず、情報システム構築時からセキュリティ対策を導入する取組として、情報セキュリティを企画・設計段階から確保するための方策（SBD: Security By Design）を推進しており、「政府機関の情報システムの調達における情報セキュリティ要件策定マニュアル[19]」の利用を推奨している（コラム２ 参照）。平成 24 年度は、同方策に係る勉強会を各府省庁において延べ 13 回開催した。

[17] 共通脆弱性評価システム（Common Vulnerability Scoring System)。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で、特定ベンダーに依存しない共通の評価方法により定量的に脆弱性の深刻さを評価できる。
[18] 利用者からの入力内容やHTTPヘッダの情報を処理してウェブページに出力するウェブアプリケーションで、ウェブページへの出力処理に問題がある場合に、そのウェブページにスクリプト等を埋め込まれてしまう脆弱性。この脆弱性を悪用した攻撃により、利用者のブラウザ上で不正なスクリプトが実行されてしまう可能性がある。
[19] http://www.nisc.go.jp/active/general/sbd_sakutei.html
「「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、平成 23 年 4 月 28 日）

●コラム２： 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

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（企画・設計・開発・運用・廃棄）における企画段階から情報セキュリティの観点を意識し、調達仕様にセキュリティ要件を適切に組み込むことが求められる。また、調達仕様におけるセキュリティ要件の曖昧さや過不足は調達側と供給側の相互理解と合意形成を阻害し、調達側と供給側の双方に不利益を発生させる要因となる。

このような問題意識を受けて、経験・知見を有する有識者やベンダーを交えた「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）に係る検討会」が開催され、行政情報システムにおける情報セキュリティ対策を考慮したライフサイクル管理の強化の実現に向けて、具体的な方策の検討が進められ、平成 23 年４月に、「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」がまとめられた。同マニュアルには、調達担当者がシステム特性に応じて「調達仕様書にセキュリティ要件を記載する方法」が解説され、「対策要件集」及び「対策要件選定作業の定型化」等のツールによって、調達担当者を支援する内容が記載されている。



※ 調達指針：情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）

このほか、サーバの集約化も管理を効率的・効果的に実施できることから、ウェブサイトへの攻撃に対する対策の一つといえる。こうした観点等から、各府省庁においては集約化計画に基づき集約化を進めている。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について、平成 24 年度の調査の結果、公開ウェブサーバ約 660 台、電子メールサーバ約 930 台であり、当該計画の基準となる平成 20 年 11 月時点の台数（公開ウェブサーバ約 1,000 台、電子メールサーバ約 1,900 台）に比べて、集約化が進んでいる状況が確認された。（第２編 第１節 参照）

これらの平時の取組に加え、政府機関への実際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[20]と認知された件数は、平成 24 年度は約 108 万件であった（表 １－２）。

[20] GSOC センサーにより検知・集積されたイベントのうち、多角的な分析により、正常なアクセス・通信とは認められなかったもの

表 1－2　GSOC センサーで認知された政府機関への脅威の件数の推移

	H22年度	H23年度	H24年度
・政府機関への脅威の件数	約 49 万件	約 66 万件	約 108 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を検知した際には当該政府機関への通報を行っており、平成 24 年度においては、175 件の通報を行った（表 1－3）。

表 1－3　GSOC センサー監視等による通報件数の推移

	H22年度	H23年度	H24年度
・センサー監視等による通報件数	181 件	139 件	175 件

このほか、自らの主義主張を誇示する目的でサイバー攻撃を行うものが、攻撃対象としようとする適当な組織やウェブサイトについて、SNS 等を用いて情報交換を行うケースもあるため、GSOC では、インターネット上の各種情報から動向を監視し、攻撃の予兆等については適宜注意喚起を実施している。

このような対策の取組を実施しているところであるが、平成 24 年度においても政府機関等のウェブサイト等への攻撃による改ざんや閲覧障害の情報セキュリティ事象が、府省庁から 6 件公表された。なお、独立行政法人等からは 10 件公表された。

例えば、平成 24 年 6 月には、「アノニマス」と名乗る国際的な集団が、平成 24 年 6 月 20 日に改正著作権法が成立したことを受け、我が国の政府機関等に対するサイバー攻撃を示唆する書き込みを海外のウェブサイト上で行ったため、各府省庁に情報共有を行うとともに、注意喚起を行った。

また、平成 24 年 9 月には多数のウェブサイト等に対するサイバー攻撃が確認された。本事象では、攻撃者は攻撃対象の選定に当たり、脆弱性を持つアプリケーションを使用しているウェブサイトを、検索エンジンを用いて調査していた可能性があり得ることを受け、NISC から各府省庁に対して同内容に関する注意喚起を行った（コラム３ 参照）。

●コラム３： ウェブサイトに係る脆弱性の確認及び対策の点検・実施についての注意喚起概要

○最近の攻撃の傾向
最近の攻撃の傾向として、検索エンジンを用い、攻撃対象のドメインを限定した上で、過去に脆弱性が存在したミドルウェア等で利用されるクエリー（問合せ）の特定文字列や、公開されるファイルの特定拡張子を検索文字列として検索することで、ミドルウェア等の脆弱性が放置されている可能性があるウェブサイトを検索し、これを攻撃対象としている可能性が指摘されている。

○注意喚起事項
ウェブサイトの改ざんに利用される既知の脆弱性については、ウェブサイトで利用するミドルウェア等の基盤ソフトウェアを適切に管理していれば防ぐことができるものと考えられる。よって、管理しているウェブサイト（外部委託等により構築・運用しているウェブサイトを含む。）において、改ざんの原因となる可能性の高い、ミドルウェア等の基盤ソフトウェア及びそれらに含まれるプラグイン等の脆弱性情報を確認し、アップデートやパッチ適用などの対策を行うこと、並びに権限設定等の再確認を行うこと等の対策を行う。

○参考
過去に脆弱性が存在し、改ざんの原因となる可能性があるミドルウェア等は下記の通り。脆弱性情報を確認する際の参考とされたい。（括弧内はミドルウェア固有の特定拡張子で、インターネット上に公開されるため、検索される可能性があるもの。）
Struts（do）、JBoss（ear、sar、seam 等）、ColdFusion（cfm）、Tomcat、WebSphere、WebLogic、Joomla!、Apache HTTP Server、IIS

4 国の重要な情報がねらわれた情報セキュリティ事象とその対策の取組

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、電子メールを利用したものがある。電子メールの添付ファイルに不正プログラムが含まれている、あるいは、本文中に不正プログラムが設置されているサーバの URL が記載されるなど、これらをメール受信者が開封したり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。

政府機関等においても、このようなメール受信者の端末を不正プログラム感染させることを目的とした電子メールが数多く受信されている。政府機関等では、このようなメールを不審メールと呼び、対処を行っている。不審メールの中には、本文が業務メールと見分けの付かない内容である場合や、差出人がなりすまされている場合もあり、巧妙に添付ファイルの開封等を誘導することが多い（図 １－３）。

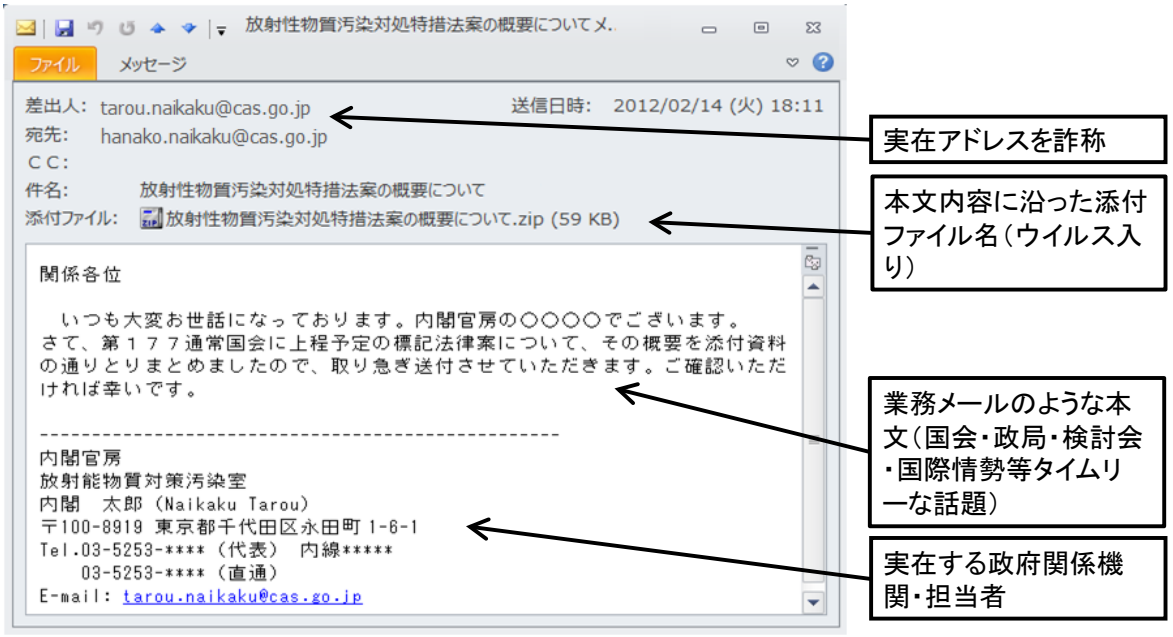


図 1－3 巧妙な不審メールのイメージ

政府機関では、平時においては、職員に対して不審メール受信時の対処方法についての教育を行うため、不審メールを模擬した訓練メールを職員に送信する訓練を行っている。NISC では、平成 24 年８月～12 月に、19 府省庁 約 12 万人の職員に対し、添付ファイルを開封するように巧妙化させたメールを送付し、ヒヤリハットを体験させる訓練メールを 1 人当たり２回送付し、不審メール受信の疑似体験の機会を提供した（資料編 A 参照）。

また、なりすましメール対策として送信ドメイン認証の導入を進めている（資料編 B 参照）。平成 24 年度の重点検査の結果、政府機関等が管理する電子メールサーバ（主に. go. jp ドメインを電子メールのアドレスとして利用しているもの）において、約 78%の電子メールサーバが、受信側における送信ドメイン認証技術を導入し、送信元のドメインをなりすます不審メールを検知している（第２編 第１節 参照）。

さらに、GSOC においては、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、平成 24 年度においては、415 件の注意喚起文書を発出した。（表 1－4）

表 1－4 不審メールに関する注意喚起の件数の推移

	H22年度	H23年度	H24年度
・不審メールに関する注意喚起の件数	118 件	209 件	415 件

このように、一般的な不審メールについて、複数の側面からの対策を実施しており、一定程度の対処ができている状況と言える。

一方、平成 24 年度において、政府機関等で複数件の不正アクセス等による情報窃取事象が発生している。ここで注目すべきは、これらは、原子力や宇宙開発などの重要な先端科学技術を扱う機関や、機微な情報を扱う特定の政府組織に対し、情報窃取等を目的とし、攻撃メール等によって職員の端末に送り込んだ不正プログラムをきっかけとして侵入を図るなど、組織的・持続的な意図をもって行われた、いわゆる標的型攻撃とおぼしきサイバー攻撃であったことである。

以下では、これらの標的型攻撃事象における NISC での傾向分析を紹介する。

なお、標的型攻撃の段階ごとの攻撃概要についてはコラム４を参照されたい。

●コラム４： 標的型攻撃の段階ごとの攻撃内容と特徴

IPAの「「新しいタイプの攻撃」の対策に向けた設計・運用ガイド（改定第２版)」において、標的型攻撃の段階ごとの攻撃内容と特徴が紹介されている[21]。

段階	攻撃内容	特徴
攻撃準備段階	(1) 攻撃対象に関連のある組織への攻撃 ・メール情報の窃取など	対象組織への初期潜入を成功させるため、ソーシャルエンジニアリングのためのメール文面や送付先を収集。
初期潜入段階	(1) 各種初期攻撃 ・標的型攻撃メール添付ウイルス ・ウェブ改ざんによるダウンロードサーバ誘導 ・外部メディア（USB 等）介在ウイルスなど	入り口の対策をすり抜け、システム深部に潜入。 素早く次の段階へ移行。 攻撃手法は使い捨て。
攻撃基盤構築段階	(1) バックドア（裏口）を使った攻撃基盤構築 ・ウイルスのダウンロードと動作指示 ・ウイルスの拡張機能追加 ・システム内部への攻撃基盤構築	構築された攻撃基盤は発見されない。 構築した攻撃基盤は再利用される。
システム調査段階	(1) 組織のシステムにおける情報の取得 (2) 情報の存在箇所特定	時間をかけて何度もしつこく行う。
攻撃最終目的の遂行段階	(1) 組織の重要情報の窃取 (2) 組織情報（アカウント等）を基に、目標を再設定	何度も攻撃を行うため情報窃取。 組織への影響を与える情報窃取。

[21] http://www.ipa.go.jp/security/vuln/newattack.html
「「新しいタイプの攻撃」の対策に向けた設計・運用ガイド（改定第２版)」（IPA、平成 23 年 11 月 30 日）

平成 24 年度の政府機関等に対する標的型攻撃メールは、多くの場合、職員が業務で利用している個人アドレス宛てに送信されたものであったが、中には問い合わせ先として組織のウェブサイト等で公開されている組織アドレスや職員が個人において契約している私用メールアドレス宛てに送信されたものもあった。

業務で利用している個人アドレスは、一般に組織のウェブサイト等で公開しているものではないが、業務上組織外の関係者とメールのやり取りをする過程で攻撃者に個人アドレスに関する情報を窃取された可能性が考えられる。また、個人アドレスが職員の氏名に基づいているなど規則性がある場合は職員名簿等から個人アドレスを推測される可能性もある。このほか、SNS や掲示板等インターネット上で職員個人に関する情報を収集することにより個人アドレスに関する情報を入手した可能性も考えられる。

攻撃メールの件名、本文等は受信者の業務に関連する内容のものが多かった。これは受信者に怪しまれずに攻撃メールに添付された不正プログラムを実行させるためと思われる。「資料送付」、「情報共有」、「作業依頼」など業務上のやり取りでよく使用される件名であったり、一部の攻撃メールには実際に送受信されたメールの内容がほぼそのまま利用されていたり、本文中の署名欄 [22]に実在する職員の氏名や連絡先が記載されているものもあった。問い合わせ先としてウェブサイト等で公開されていた組織アドレスに送信された攻撃メールには、通常の問い合わせのメールが送信され、職員から返信を受け取った後にその返信として不正プログラムが添付されたメールが送信される、という「やり取り型 [8]」のものが見られた。メールの送信元はフリーメールサービスのメールアドレスが多数を占め、その他に政府機関、企業、大学等のメールアドレスを詐称している攻撃メールが見られた。

添付された不正プログラムは実行ファイル形式のものが最も多く、Microsoft Word 形式、Microsoft Excel 形式、PDF 形式、一太郎形式のような文書ファイルも多く使用されていた。実行ファイル形式の不正プログラムを使用した攻撃メールの大半は不正プログラムが圧縮ファイルの状態で添付されており、ファイル名やアイコンの偽装により一見すると文書ファイルであるかのように偽装されているものもあった。また、拡張子の一部を変更した状態で攻撃メールに添付されたものや、不正プログラムの実行ファイルがパスワード付きの圧縮ファイルで攻撃メールに添付され、攻撃メールの本文に圧縮ファイルのパスワードが記載されているものもあったが、これらはメールサーバ等で行われる不正プログラムチェックを回避するための手段と思われる。

攻撃メールの中には、不正プログラムを添付する以外にメール本文にリンクを記載して受信者にリンク先へアクセスさせるものもあった。リンク先のウェブサイトはウェブブラウザ等の脆弱性を悪用してアクセスするだけで不正プログラムに感染させるような細工がされていたり、不正プログラムの実行ファイルが入った圧縮ファイルが置かれていたり、フリーメールサービスのログイン画面の偽物を用意して入力されたユーザ名とパスワードを窃取したりするような手口が使われていた。また、リンク先が政府機関のウェブサイトであるかのようにメール本文を偽装したものもあった。

攻撃メールに添付された不正プログラムと攻撃メール本文に記載されたリンク先のウェブサイトで脆弱性を悪用するものの大半は既に修正プログラムが公開されている脆弱性を悪用するものであったが、修正プログラムが公開される前の脆弱性（ゼロデイ脆弱性）を悪用するものも一部あった。

[22] メール本文中の文末等においてメール差出人の氏名や連絡先などの情報が記載されることが多い部分

●コラム５： 標的型攻撃の初期潜入段階における対策の困難性

標的型攻撃の初期潜入段階においては、不正プログラムが含まれるファイルを添付した電子メールが利用されることが多い。教育や訓練等によって、個々の職員がメールの添付ファイルを開封する確率を下げたとしても、組織に属する職員がある程度多い組織では、少なくとも一名の職員が添付ファイルを開封してしまう確率はそれほど下がらない（下表）。

例えば、組織の緊張感の度合いとして、個々の職員の開封確率が５％（メールを 20 通受け取ると１通の割合で添付ファイルを開封する）である場合であっても、組織に属する職員の 15 人に１通ずつメールが送付されれば、53.7％とほぼ半々の確率で誰かが開封し、100 人に１通ずつメールが送付されれば、99.4％とほぼ確実に誰かが開封してしまう。

標的型攻撃は、巧妙なメールを用い、特定の攻撃対象に執ように攻撃を行うことから、これを個々の職員の注意により、初期侵入段階で防ぎきることは非常に困難であると言える。

		個々の職員が添付ファイルを開封する確率		
		10.0%	5.0%	1.0%
メールを受信した職員数	15	79.4%	53.7%	14.0%
	50	99.5%	92.3%	39.5%
	100	100.0%	99.4%	63.4%
	500	100.0%	100.0%	99.3%

（内閣官房情報セキュリティ補佐官／東京電機大学　佐々木良一 教授　による分析）

5 国の重要な情報をねらうサイバー攻撃等に対応するための体制の整備

国の重要な情報をねらう高度なサイバー攻撃等に対しては、攻撃活動を速やかに検知し、情報が窃取される前にこれをくい止めることが重要である。

このため、平成 24 年６月 29 日、政府機関等の情報システムに対する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、NISC に情報セキュリティ緊急支援チーム（CYMAT：Cyber Incident Mobile Assistant Team）を設置した。

CYMAT は、NISC に常駐する職員だけではなく、各府省庁等の職員に対して内閣官房の併任辞令を発令するなどして、平成 25 年５月末現在、21 府省庁の計 50 名程度のメンバー（研修員含む。）で構成されている。

CYMAT の活動としては、サイバー攻撃等によって政府機関等の情報システムに障害の発生又はそのおそれがあり、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、政府 CISO である内閣官房情報セキュリティセンター長の指揮の下、発生事象の正確な把握のほか、被害拡大防止、復旧及び原因調査並びに再発防止のための技術的な支援及び助言等を行うこととしている。平成 24 年度においては、４件のサイバー攻撃事象について具体的な支援及び助言等を行った。

このほか、平時においては事象対処能力の向上を図ることを目的として、サイバー攻撃に関する最新動向や過去の情報セキュリティ事象事例の研究などを内容とした講義を毎月１回程度実施したほか、警察庁や防衛省の協力を得て、標的型攻撃や DoS 攻撃等への対処訓練、コンピュータ・フォレンジックスや不正プログラム解析等の手法についての技能を習得させるための訓練等の集中的実習を２回実施した。

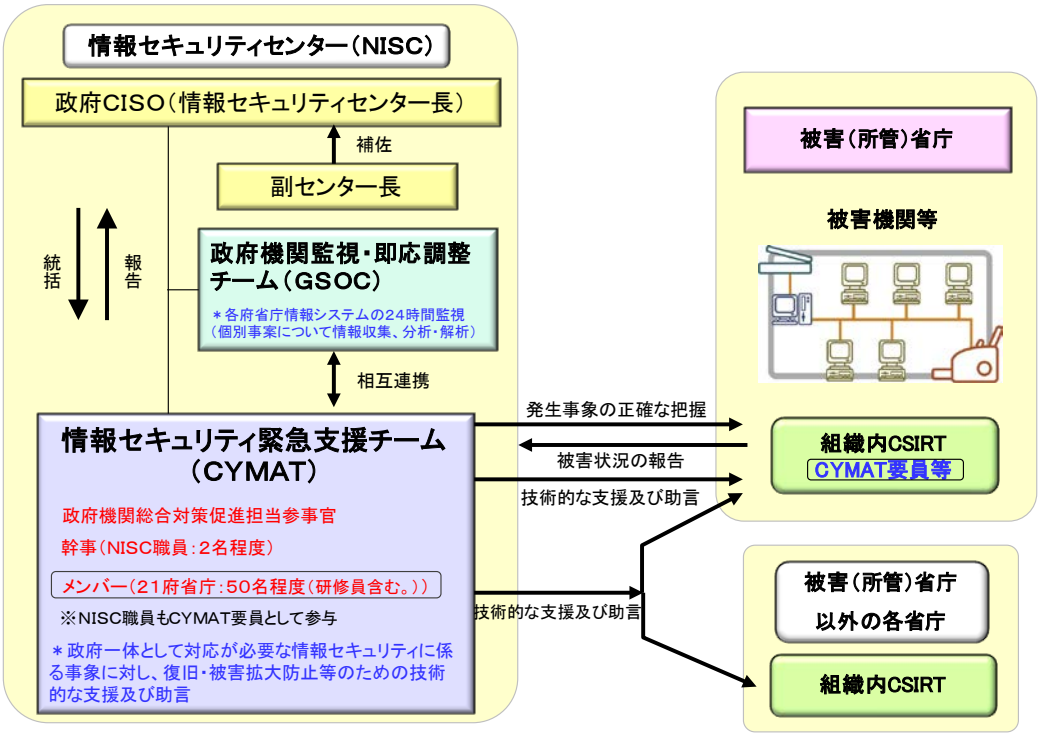


図　1－4　CYMAT の枠組み

また、各府省庁においても障害・事故等が発生した際、迅速かつ適切に対処するための政府一体となった枠組みを構築するため、平成 24 年度末までに全ての府省庁が CSIRT（Computer Security Incident Response Team）等の機能を有する体制を整備した。

平成 25 年３月には、大規模サイバー攻撃事態の脅威が現実化していることなどを踏まえ、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を実施した。

●コラム６：　CSIRT として求められる機能について

平成 24 年１月 19 日に開催された、情報セキュリティ対策推進会議官民連携の強化のための分科会報告においては、以下の各府省庁における CSIRT 等の必要５条件が提示され、各府省庁においてはこれを元に CSIRT 等の活動を行っている。

(1) 組織内向けにインシデント対応の窓口の明確化・一元化
(2) インシデントが発生している情報システムの稼働・停止等の実施又は勧告
(3) 外部との情報共有、連携の窓口となる PoC(Point of Contact)
(4) 情報システムの理解、情報システム部門との相互連携
(5) 内閣官房情報セキュリティセンター（NISC）への報告

NISC では、各府省庁における CSIRT の設置に向け、CSIRT への理解を深め、円滑な整備を図ることを目的に、平成 24 年７月と 11 月に、外部専門家を講師に招き、各府省庁の情報セキュリティ関係職員等を対象とする勉強会を開催した。この勉強会では、外部専門家が、CSIRT の概要や構築時の留意点や事例等を解説したほか、情報セキュリティ事象への

対応等に係る机上演習等も実施した。

NISC においては、今後各府省庁の CSIRT 等の機能の維持向上を図るほか、上述した、GSOC、CYMAT との連携も強化し、政府機関における情報集約・支援体制の枠組みの強化を図ることとしている。

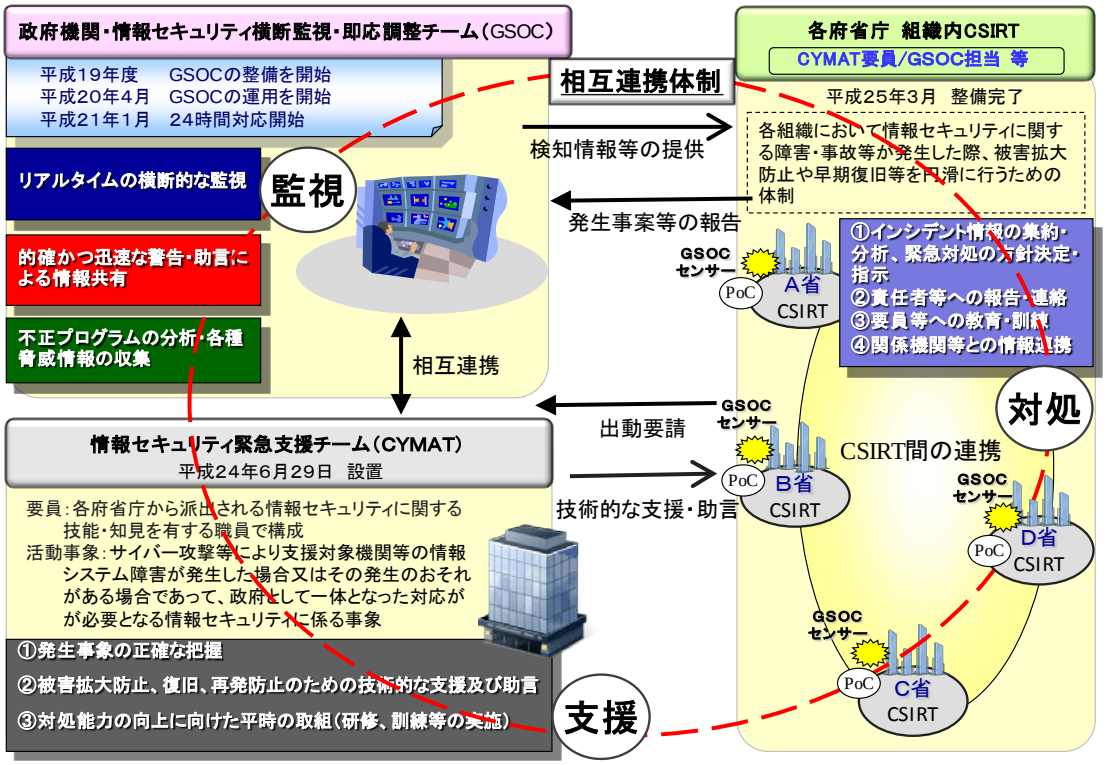


図　1－5　政府機関における情報集約・支援体制の枠組み

このほか、政府機関においては、内閣官房内閣情報調査室に置かれたカウンターインテリジェンス・センターを中核として、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・共有等を政府統一的に取り組んでいる。

6 政府機関の情報セキュリティに係るその他の取組

近年、急速に普及しているスマートフォン等のスマートデバイスは、多様な経路によるインターネットへの接続やアプリケーションのダウンロード等が容易である等利便性が高く、政府機関等においても今後業務利用拡大が予想される。一方、これらスマートデバイスは、不正なアプリケーションや不正プログラムも簡単にダウンロードされるなどの情報セキュリティ上の課題が多い。

こうした動向を踏まえ、NISC では平成 24 年４月に「政府機関のスマートフォン・タブレット端末の使用手順雛形（官支給品編）」を各府省庁に提示し、スマートデバイスを政府機関に導入する際のセキュリティ対策を促進してきた。さらに、昨今、私物端末を業務に利用する BYOD（Bring Your Own Device）の考え方が広まりつつあることを受け、政府機関等において私物端末が利用された場合のセキュリティ要件の考え方の整理の必要性について、各府省情報化統括責任者（CIO）補佐官等連絡会議の情報セキュリティワーキンググループにおいて検討が行われた（NISC はオブザーバとして参加。）。

ワーキンググループでは、私物端末の利用黙認や管理者の目の届かない範囲で私物端末を業務利用することによる情報セキュリティリスクの懸念等が議論され、組織の現状とリスクを把握し私物端末の業務利用に係る管理をしっかり行うこと（私物利用禁止ならば禁止の徹底、私物利用のニーズがある場合にBYOD管理の仕組みや技術策によりリスクを低減する措置を講ずること）が重要であるとの知見がまとめられた。さらにこの考え方のもと、BYOD実現形態と情報セキュリティを確保するための技術策と管理策についても整理が進められた。ワーキンググループの活動結果については、平成 25 年３月に「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」として公開された[23]（図 １－６）。

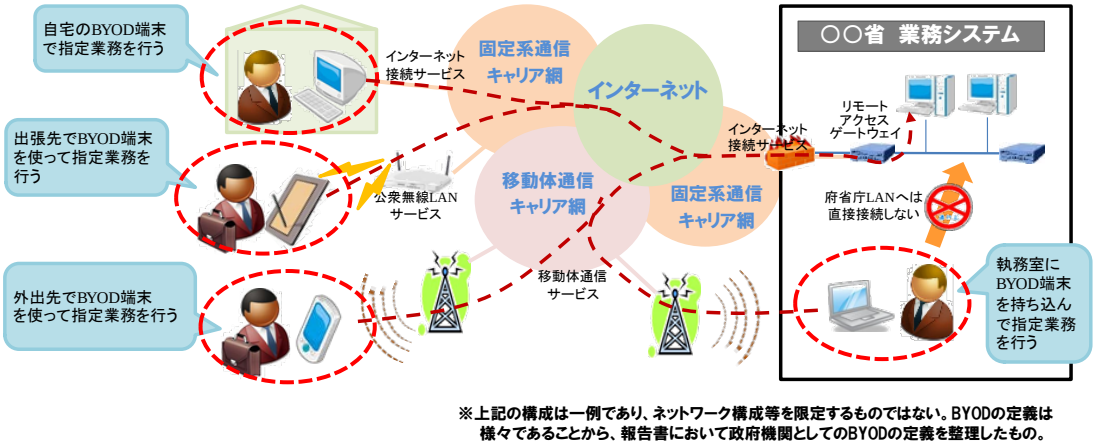


図 １－６ 政府機関において BYOD を実施する場合のイメージ図

また、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暗号アルゴリズム RSA（鍵長 1024 ビット）については、今後数年から十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。このような状況から、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、平成 25 年度（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きた（資料編 D 参照）。

平成 24 年４月には、暗号の危殆化の進行に伴う政府機関内の危険度判定とその情報の伝達フローを策定・決定した[24]。また、平成 24 年 10 月には、電子証明書を発行する各認証基盤との調整結果を踏まえ、平成 26 年（2014 年）９月下旬以降早期に発行する証明書を新しい暗号アルゴリズムを利用したものに切り替える等の具体的な移行スケジュール（図 １－７）を策定し、「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」を改定した[25]。

[23] http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf［PDF］
「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」（CIO 補佐官等連絡会議、平成 25 年３月）
[24] http://www.nisc.go.jp/conference/suishin/index.html#2012_2
「第５回会合」（情報セキュリティ対策推進会議（CISO 等連絡会議）、平成 24 年４月 18 日）
[25] http://www.nisc.go.jp/conference/suishin/index.html#2012_5
「第８回会合」（情報セキュリティ対策推進会議（CISO 等連絡会議）、平成 24 年 10 月 26 日）

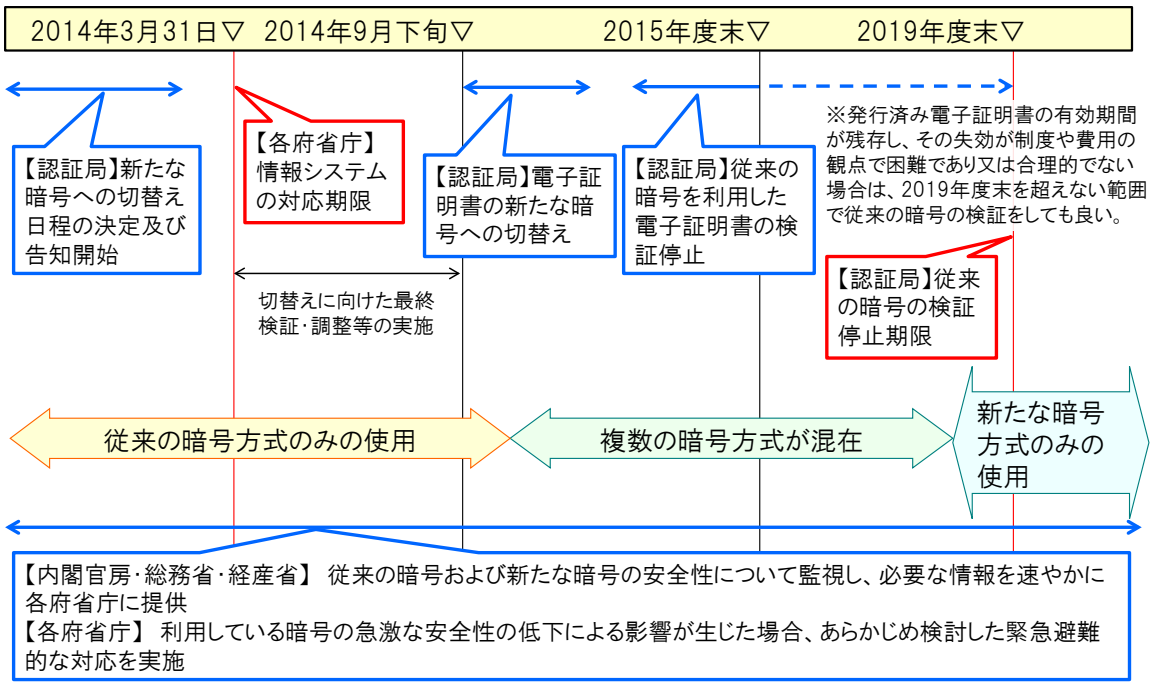


図 1－7 政府機関における暗号移行スケジュール

平成 25 年３月には、これまで電子政府で利用される標準の暗号技術として利用してきた「電子政府推奨暗号リスト」(平成 15 年 2 月 20 日公表) を 10 年振りに改定し、新たに「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト)」を策定・公表した[26] [27]。

また、平成 24 年６月に発生した、レンタルサーバ業者において顧客データが大量に消失した事象を受け、NISCから政府機関等に対し注意喚起文書を発出し[28]、クラウドサービスなど、約款による情報処理サービスを利用する際に契約内容や約款、運用手順等を改めて確認することや、自己でサーバを管理する場合のバックアップ運用法の確認等を促した。(資料編G 参照)

このほか、情報システムは政府機関等の業務遂行を支えるための基盤となっており、その運用継続性の向上が重要であることから、東日本大震災の教訓等を踏まえ、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」を改定し[29]、優先的に検討すべき対策等を拡充したほか、平成 24 年度に事例調査や文献調査を実施し、計画策定・改善の実例や留意事項、個別対策例を取りまとめた（資料編E 参照)。

[26] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000038.html
「「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」の公表」(総務省、平成 25 年３月１日)

[27] http://www.meti.go.jp/press/2012/03/20130301004/20130301004.html
「「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を公表します」(経済産業省、平成 25 年３月１日)

[28] http://www.nisc.go.jp/active/general/pdf/rentalsv_kanki_120702.pdf [PDF]
「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)」(NISC、平成 24 年６月 29 日)

[29] 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)

第３節 今後の方向

1 職員の過失又は故意による情報セキュリティ事象への対策強化

これまで、職員の過失又は故意による情報セキュリティ事象への対策は、主に教育等による情報セキュリティポリシー等の浸透を図る対策が行われており、自主点検の結果からは一定の浸透が図れていることが確認されている。一方で、平成 24 年度においても、一定数の情報セキュリティ事象が発生している。今後は、一層の情報セキュリティポリシーの浸透・遵守と、技術的対策の強化を図り、情報セキュリティポリシーをより実効的なものに改めるとともに、情報セキュリティマネジメントシステムの PDCA 運用を確実に実施できる取組を検討する。

2 不審メール等への対策強化

不審メールを模擬した訓練メールを職員に送信するという標的型メール攻撃に対する教育訓練は、職員が訓練メールを受信すること又は訓練メールを開封し“ヒヤリハット”体験することにより、職員に気づきを与える等の教育を目的としたものである。

しかし、時間の経過とともに職員の意識レベルは低下するなど、その訓練効果は一時的なものであるため、今後も本訓練等による継続的な意識啓発の取組を実施していく。

平成 25 年度については、訓練手法を改善しつつ、標的型メール攻撃に対する教育訓練を引き続き実施する予定。なお、今後、各府省庁が自ら同様の訓練を実施することも想定し、訓練実施運営のノウハウを取りまとめ、各府省庁に展開する等の、訓練の水平展開に係る取組も推進する。

また、標的型攻撃を受けた場合等、被害を最小限に止めるためには、迅速かつ適切な対応が必要となることから、職員の連絡・報告にかかる訓練を平成 26 年度から実施するため、訓練方法等の検討を行う。

3 リスク評価及び標的型攻撃等の対策推進

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、また情報システムへの依存度は一層増大しているため、情報システムの利活用における基盤的な環境としてその情報セキュリティの確保は、各府省庁の運営上、極めて重要な事項となってきている。このような状況の中、組織的・持続的な意図をもって行われる標的型攻撃など、外部からの情報窃取・破壊等を伴うサイバー攻撃への対処が喫緊の課題である。

標的型攻撃の本質が、外部の者によって為される、情報システム内部への侵入による情報窃取・破壊であることなどから、対策実施に当たっては内部統制的な手法だけでは不足であり、情報システムにおける適正な対策の実施及び監視・運用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である。

このため、各府省庁において、最高情報セキュリティ責任者の指揮の下、重点的に守るべき業務・情報を特定し、メリハリをもって計画的に資源を投入・配分し、多重的な防御の仕組みを実現するといった、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を確立することが不可欠である。

そのためには、標的型攻撃等の脅威に対して、情報システムのユーザであり情報を保全する者と連携しつつ、重点的に守るべき業務・情報を把握し、これらを取扱う情報システムにおけるリスクを評価した上で、対処の優先度や情報システム更改時期等を踏まえた対策の導入計画を策定し、その計画に基づき対策を着実に実施していく具体的なプロセスの実現が求められる。

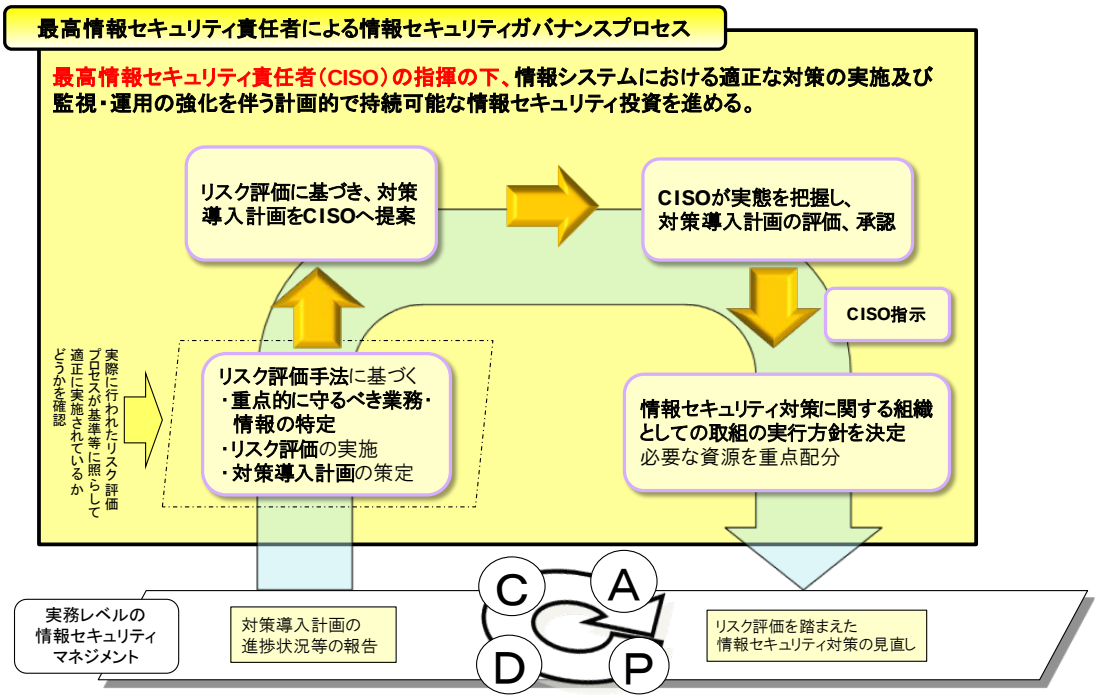


図 1－8 最高情報セキュリティ責任者による
情報セキュリティガバナンスの概要

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等の対策（情報システム内部への侵入等の攻撃シナリオとそれに対応する一連の情報システムの設計、監視強化等の対策のセット）について、産学官の専門家による検討会（各府省庁も参画）を開催して検討を進めているところである。（検討会の構成員は以下のとおり。）

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	総務省　情報流通行政局　情報流通振興課 情報セキュリティ対策室　標準化推進官
	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	

標的型攻撃等の脅威に対する対策については、情報システムの設計段階のみならず、運用段階における監視等も重要であるため、各省庁における情報システムの運用者等に対する教育、訓練が NISC により提供されるべきであり、また、新たな脅威（新たな攻撃手法等）の監視・把握、リスク評価手法や新たな脅威が顕在化した場合の対策の見直し、対策実施に係る教育・訓練等も含めて、継続的に実施していくべきであることから、これらの運用手法や具体的実施内容の検討についても、取り組んでいるところである。

その際、新たな脅威の監視・把握や対策の見直しについては、NISC だけでなく、官民の情報セキュリティ関係組織の知見を結集し、継続的に最新の攻撃手法等に対処できる枠組みを構築していくこと、また、対策実施に係る教育・訓練等については、攻撃者が最終目的を遂行することを未然に防止するために、実運用の中で各府省庁システム担当と各府省庁 CSIRT や CYMAT とが連携し、早期に攻撃の兆候を検知し、対処できることを主眼に実施していくことを前提としている。

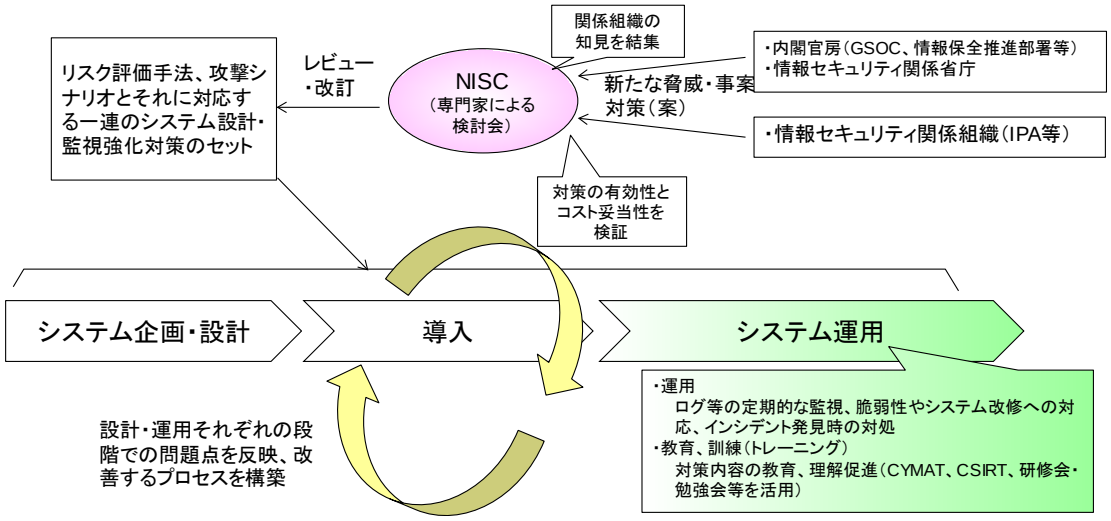


図 1－9 リスク評価手法及び対策の継続的な見直し・
情報セキュリティ関係組織との連携等の概要

4 情報システムの調達における国際基準に基づく適合性評価制度の活用

政府機関の情報システムについて、その設計、製造、設置等の段階において情報セキュリティの技術標準化やその適合性の評価結果の活用が必要であり、さらに、既知脆弱性への未対応、危殆化された技術の利用や不正プログラムを埋め込まれる等のサプライチェーン・リスクへの対応強化が必要である。具体的には、国際規格に基づく適合性評価制度[30]の活用について検討する。また、世界共通のセキュリティに関する調達要件として国際的に開発が進んでいるcPP（Collaborative Protection Profile：製品/技術分野ごとに必要となるセキュリティ要件が定義されたドキュメント）について、デジタル複合機等のIT製品の政府調達での活用を検討する。

[30] 国際貿易における IT セキュリティの評価及び認証のスキームとしては、例えば、CCRA（Common Criteria Recognition Agreement）がある。

第２編 平成 24 年度における各府省庁の取組と評価

第１節 各府省庁における取組の評価

本節では、各府省庁の情報セキュリティ対策の一層の充実・向上を図ることを目的として平成 24 年度の各府省庁の取組について評価した結果を報告する。

評価の内容は、NISCにおいて策定した「情報セキュリティ報告書作成のためのガイドライン及び政府機関における評価等の考え方 [31]」の第 2 部「政府機関における評価等の考え方」に基づいている。

なお、各府省庁の取組については第２編 第２節を参照されたい。

1 対策実施状況報告の評価

A) 対策実施状況報告の目的

対策実施状況報告は、各府省庁が「政府機関の情報セキュリティ対策のための統一規範 [11]」に基づき、自府省庁の行政事務従事者等の情報セキュリティ対策の実施状況を把握・評価し、取組が不十分なものについて改善を図ること等を目的とするものである。

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ほか、次年度の各種施策の検討等に反映させる。

B) 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 [11]」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 24 年度は、前年度に引き続き、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を行い、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った。当該報告の対象項目は、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、等の観点から NISC が指定した。

[31] http://www.nisc.go.jp/active/general/sec_report_guide.html
「情報セキュリティ報告書作成のためのガイドライン及び政府機関における評価等の考え方」（NISC、平成 24 年 12 月 12 日）

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[32]	政府機関の情報セキュリティ対策のための統一規範[11]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			
区域情報セキュリティ責任者			
障害・事故等に対応する責任者			
情報システムセキュリティ責任者・管理者[33]	システム責任者等		
行政事務従事者	左記同様		

C) 実施期間

平成 24 年 7 月から平成 25 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）

D) 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、各主体がその役割に応じて実施すべき対策事項を点検し、その結果を集計した上で NISC に報告し、NISC においてその結果を分析・評価した。

E) 政府機関全体の評価

ア) 対策実施状況報告の結果

平成 24 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。

a) 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[34]

全主体平均	責任者等	システム責任者等	行政事務従事者
98.5%	98.7%	99.8%	98.6%

[32] 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。
[33] 「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。
[34] 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。

b) 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 主体別の実施率及びその推移

	H20 年度	H21 年度	H22 年度	H23 年度	**H24 年度**
責任者等	97.5%	98.3%	99.5%	99.5%	**99.6%**
システム責任者等	97.2%	98.4%	99.3%	98.6%	**97.9%**
行政事務従事者	94.5%	97.1%	97.6%	95.9%	**96.8%**
全主体平均	96.9%	98.1%	98.9%	99.0%	**98.9%**

※平成 20 年度から同 22 年度までは全ての対策事項を網羅的に点検し、平成 23 年度以降は点検項目を重要な対策や実施率の低い対策等に重点化しており、集計対象等が異なるため、単純な比較はできない。

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は、以下のとおりである。

表 2－4 行政事務従事者の主な実施率

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	92.9%
情報の利用	98.7%
情報の移送	95.0%
情報の提供	96.1%
主体認証情報管理 ※パスワード等の適切な管理	97.1%
不正プログラムの感染防止対策	97.9%

イ）所見

・　新たに設置された組織において、セキュリティポリシーの整備や体制の立ち上げにリソースを投入したことや、ポリシーの周知期間の不足等から、把握率及び実施率が十分でないところがあった。今後は、こうした組織において着実なセキュリティポリシーの運用、対策の推進が期待される。かかる事情はあったが、全主体平均の把握率は 98.5%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維持したと考えられる。

・　責任者等の実施率は 99.6%となっており、また、実施率の推移からも高い水準が保たれており、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、更なる浸透が望まれる。

・　システム責任者等の実施率の推移では、平成 20 年度から同 22 年度にかけて実施率の向上が見られたものの、平成 23 年度から点検項目を重要な対策や実施が不十分な取組に重点化して集計したため、値は若干の低下が見られる。平成 24 年度の実施率は 97.9%であり、平成 23 年度に比して若干の低下が見られるが、これは、一部の組織において、総務省で進めている情報システムの洗い出し作業の成果を用いて、これまで把握できていなかった情報システムを確認し、これらのシステム責任者等に業務の徹底を図る過程等の影響があるものとみられる。

・　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。ただし、項目別に見ると、「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、実施率がほかの項目と比べて若干低い数値となった。行政事務従事者にとって情報の格付の決定・明示等の基本的な対策事項であることにかんがみ、特に、取組が十分といいきれない府省庁においては、行政事務従事者に対する教育を PDCA の一環として計画的に実施していくことが求められる。

F）府省庁別の評価

ア）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 2－1 のとおり。

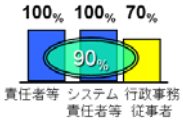
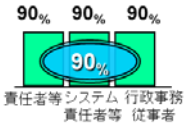
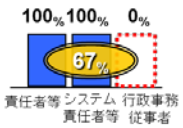
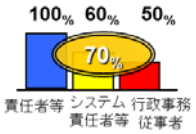
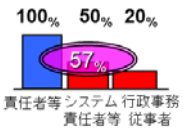
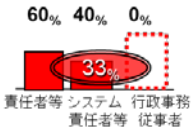
評価基準	把握率及び実施率	概要	評価パターン例
A	100%	適切に実施すべき対策について、全ての項目で統一基準群に準拠した対策が実施されている。	
B	80%≦x＜100%	適切に実施すべき対策について、概ね全ての項目で統一基準群に準拠した対策が実施されているが、一部の項目で不十分なものが含まれている。	 
C	60%≦x＜80%	適切に実施すべき対策について、不備の項目が一部に見られるなど、対策が遅れている。	 
D	60%未満	適切に実施すべき対策について、不備の項目が相当数見られるなど、対策が著しく遅れている。	 

図 2－1 対策実施状況報告の ABCD 評価

イ）把握率及び実施率の評価結果

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	B	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	A
復興庁	C	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

※復興庁は、平成 24 年 2 月発足。

2 重点検査の評価

A) 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。本検査では、各府省庁のウェブサーバ及び電子メールサーバ等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・評価し、取組が不十分なものについて改善を図ること等を目的とするものである。

また、検査項目については、平成 23 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。

NISC は、これら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ほか、次年度の各種施策の検討等に反映させる。

B) 検査期間

平成 24 年 7 月から平成 25 年 3 月
（検査基準日：平成 24 年 12 月 1 日）

C) 検査内容

表 2-6 検査内容

<table>
<tr><th>対　象</th><th>検査項目</th><th>検査項目とした理由</th></tr>
<tr><td>公開ウェブサーバ</td><td>・SSL バージョン 2 の無効化
・強度の弱い暗号方式の無効化
・SQL インジェクションの確認状況</td><td>NISC が平成 23 年度に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の結果を踏まえ、実施が求められる対策の実施状況を把握するため。</td></tr>
<tr><td></td><td>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サービス不能攻撃（DoS 攻撃、DDoS 攻撃）への対策</td><td>昨今の公開ウェブサーバにおけるサイバー攻撃の一般的な動向を踏まえ、実施が求められる対策の実施状況を把握するため。</td></tr>
<tr><td></td><td rowspan="2">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</td><td rowspan="2">サーバを計画的に安全な状態で運用するための基本的な対策であるため。</td></tr>
<tr><td>電子メールサーバ</td></tr>
<tr><td>ドメイン</td><td>電子メールの受信側における送信ドメイン認証技術導入状況</td><td rowspan="2">政府機関等を対象とする標的型攻撃の増大を踏まえ、実施が求められる対策の実施状況を把握するため。</td></tr>
<tr><td>ネットワーク等</td><td>標的型攻撃に対する出口対策状況</td></tr>
</table>

D) 結果

重点検査の各項目の実施率の結果は、以下のとおりである。

表 2－7 検査結果

対　象	検査項目		実施率
公開ウェブサーバ	SSL バージョン２の無効化		95%
	強度の弱い暗号方式の無効化		96%
	SQL インジェクションの確認状況		97%
	サービス不能攻撃対策	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	91%
		影響最小化への対応状況	93%
		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	92%
		対処手順や連絡体制の整備状況	97%
	OS のセキュリティアップデートの状況		100%
	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		100%
電子メールサーバ	OS のセキュリティアップデートの状況		100%
	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		100%
ドメイン	電子メールの受信側における送信ドメイン認証技術導入状況		78%
ネットワーク等	出口対策状況	不正プログラムの侵入及び拡大等防止（構築時）	100%
		標的型攻撃に利用されることへの防止	95%
		不正プログラムの侵入及び感染拡大等防止（運用時）	99%

※小数点以下四捨五入

E) 所見

公開ウェブサーバにおいては、各対策項目において 90%以上の実施率であり、おおむね、各府省庁において適切に対策が取り組まれていることが認められる。

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は、平成 23 年度の脆弱性検査において確認された暗号通信に係る脆弱性に係る対策であり、ほとんどの府省庁で対策が進んでいるものの、一部に取組が遅れている府省庁もあることから、これらの府省庁において対策の実施が求められる。

また、情報の漏えいや改ざんにつながるおそれのある SQL インジェクションの脆弱性は、上記脆弱性検査において多く検知されたものである。NISC では、注意喚起（平成 24 年 1 月 19 日付け事務連絡）を発出して、各府省庁に対して、検査業者等や簡易的な手段によって当該脆弱性の有無を確認すること等を求めた。これを踏まえ、重点検査では、動的遷移を行う画面があるなどの SQL インジェクションの脆弱性が技術的に存在しうるサーバについて、当該脆弱性の有無の確認を実施したかどうかを調査したところ、高い確認実施率であった。各府省庁では、こうした確認の結果見つかった SQL インジェクションの脆弱性について直ちに対処を行い、いずれも対処を完了している。今後とも、SQL インジェクションの脆弱性が技術的に存在しうる全てのサーバについて確認を行うとともに、迅速に対処していくことが求められる。

大量パケット送信型のサービス不能攻撃（DoS 攻撃、DDoS 攻撃）への対応状況については、一部の府省庁において対策の遅れが見られることから、引き続き対策の向上が必要である。

公開ウェブサーバのほか、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実施状況については、高い水準で実施されていることが確認された。しかしながら、これらの対策は、サーバを安全に運用するための基本的な対策であることを踏まえ、引き続き、対策に取り組むことが必要である。

電子メールの受信側における送信ドメイン認証技術は、電子メールを利用しているドメインの約 78%で導入されていた。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否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等の対策を行うことができる、いわば自組織を守るための対策である。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、NISC においては、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措置するよう促してきた。これを踏まえると、サブドメインまで検査対象に含んでの今回の結果は、比較的高い水準であったといえる。一方、自組織を不審メールから守るためには、導入した受信側における送信ドメイン認証技術による不審メールの判定結果に基づき、不審メールをフィルタリングしたり、メールの件名部分等にその旨の表現を挿入し、メール受信者に注意喚起を行ったりする等のシステム側における追加措置が必要不可欠であることから、今後はこれらの措置まで含めて適切に対策を進めていくことが求められる。

標的型攻撃に対する出口対策状況については、各対策とも高い水準で実施していることが認められる。しかしながら、昨今、情報の窃取等を目的とする標的型攻撃が数多く見られる状況を踏まえ、適切に対策を進めていくことが求められる。

このほか、サーバの集約化の観点から、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 660 台、電子メールサーバは約 930 台であり、サーバ集約化計画の基準となる平成 20 年 11 月時点の台数（公開ウェブサーバ約 1,000 台、電子メールサーバ約 1,900 台）に比べて、集約化が進んでいる状況が確認できた。

3 情報セキュリティ対策に係る推奨事例の選定

F) 推奨事例選定の目的

各府省庁が平成 24 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。

G) 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

H) 推奨事例及びその内容

ア) 推奨事例

第 10 回最高情報セキュリティアドバイザー等連絡会議（平成 25 年 5 月 27 日開催）において、推奨事例候補として 3 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、 3 件全てについて推奨事例とすることとした。

平成 24 年度の各府省庁の取組を受け、推奨事例とするものは次のとおりである。

○ コピー・プリンタ複合機の情報セキュリティ監査対象機器への追加（金融庁）
○ 職員への情報セキュリティ対策啓発のための e ラーニングの実施と徹底（外務省）
○ 基盤情報システムにおける本人認証強化を目的とした複数要素主体認証の導入（経済産業省）

イ) 推奨事例の内容及び選定理由

a) コピー・プリンタ複合機の情報セキュリティ監査対象機器への追加

- **内容**

近年におけるコピー・プリンタ複合機は、各メーカーとも組み込み型の Web サーバ機能を搭載しており、単なる出力装置に留まらずネットワークシステムの一部として機能している。

一方、その運用管理については、IT 部門ではなく総務部門等が担当しシステム上の脆弱性や情報漏えいリスクを IT 部門が認識していないというケースがあった。

このような状況を踏まえ、コピー・プリンタ複合機からデータが漏えいするリスクが考えられることから、情報セキュリティ監査の対象機器に加えた。

これにより、機能の高度化が進むコピー・プリンタ複合機に関する情報セキュリティ上のリスクを認識し、当該リスクを軽減することができた。

- **選定理由**

コピー・プリンタ複合機も PC と同様にネットワークに接続されている機器であるため、ネットワークを介するがゆえの脆弱性を十分に考慮し、対応する必要があるということを再認識できたことに加え、具体的に IT 部門がリーダーシップをとり、コピー・プリンタ複合機も情報セキュリティ監査の対象機器に加えることが情報セキュリティ・ガバナンスの観点から有効であると考えられる。

また、情報セキュリティ政策会議第 33 回会合において、「新たな情報セキュリティ戦略の方向性について」が討議されたところ、その中で執務室におけるコピー・プリンタ複合機等が、情報窃取の起点となる恐れが指摘されている。このような観点から、ネットワーク等で共有されている場合は、監査の対象とすることが望ましいと考えられる。

b）職員への情報セキュリティ対策啓発のための e ラーニングの実施と徹底

- **内容**

職員各自が e ラーニングによりパソコン上の教育用コンテンツから情報セキュリティ対策を習得するもので、一定期間内に学習が修了しない場合に自動的にインターネットの利用が制限される仕組みを構築した。

職員が e ラーニングを確実に受講することにより、最近の標的型攻撃等の脅威や、適切な情報管理の必要性について学ぶことができ、標的型メールの危険性や情報漏えい対策の重要性に対する各職員の認識が高まってきている。

- **選定理由**

情報セキュリティの教育・啓発は不断の取組が必要であるが、一方で、積極的に受講しない職員の存在も否定できないなど、教育を徹底することは難しい課題である。

これについて、未受講者に対してインターネット利用の制限を行うことは、職員へ必要な教育の効率的な実施の観点から工夫が感じられ、職員のセキュリティ意識の維持・向上に一定の効果があると考えられる。

c）基盤情報システムにおける本人認証強化を目的とした複数要素主体認証の導入

- **内容**

システムへのログインの際に、複数要素主体認証（ID/パスワード及び IC カード）を導入した。また、省外からのシステム利用においては、ID/パスワードに加え、ワンタイムパスワードによる認証機能を導入し、スマートフォンやタブレット等様々な端末からも安全に利用できるような環境を整備した。

これにより、省内及び障害におけるシステム利用に関し厳格な本人確認が行われることで、第三者によるシステムの不正利用が困難となった。

- **選定理由**

複数の主体認証要素を用いた認証機能を導入することにより、第三者による不正利用を防止する取組は、不特定多数の者が出入りする官署等において、今後一般的な情報セキュリティ対策になると考えられる。

また、本取組は、様々な端末からシステムの安全な利用ができることから業務効率の向上とセキュリティの確保を両立するものであり、参考とすべき事例であると考えられる。さらには、このような対策が行われない場合、フリーメールへの転送等が行われることも想定され、表面上は見えていないが潜在化しているリスクへの対応事例として推奨すべきと考えられる。

l）その他参考となる取組

平成 24 年度の推奨事例候補の選定に当たっては、当初、各府省庁から NISC に対して提出された取組の件数は 45 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 18 件に絞り込み、それらに対して、各府省庁の最高情報セキュリティアドバイザーを中心にして投票を実施した。そして、投票結果を基に、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 24 年度の推奨事例は３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なる内容が多く含まれることから、今後の各府省庁における情報セキュリティ対策に係る活動に役立てるため、以下に紹介する。

表 2-8 推奨事例以外の参考となる取組

取組概要	府省庁名
昨年度の自己点検の結果を踏まえ、改めて職員が実施すべき対策を周知。このほか、職員の自己点検内容の理解の一助となるよう、各点検項目に解説を付記した。	公正取引委員会
従来から実施している新規採用者や新任の課長、課長補佐、係長等への研修に加え、その他の職員研修においても、最高情報セキュリティアドバイザーによる講義を行った。	総務省
CSIRT の平時における活動の一環として、情報セキュリティに関連する情報を、日々収集することにより、省内における情報セキュリティ上の脅威を早期に察知し、対策を検討。本省及び在外公館へ注意喚起を行い、システム上の対策に活用するとともに、様々な会議等の場を通じて関係職員の情報セキュリティの意識啓発を継続的に実施している。	外務省
セキュリティ事案の発生や脆弱性情報の公表があった際等に、GSOC からの情報提供だけに頼らず、独自に情報収集を行い、結果をセキュリティ担当者に提供。組織内への速やかな周知を行った。	内閣官房
情報セキュリティポリシーのより効果的な運用を図るため、一般ユーザが遵守すべき事項と、システム整備担当者向けの仕様書に記載すべきシステム要件とを別個の通達として発出。対象者に応じた通達体系とした。	警察庁
情報システムの調達に関して、仕様書の雛形及びその解説を用意し、システムの実態に応じた見直しを可能としている。また、公開ウェブサーバの新規開発又は公開に係る調達仕様書については、PMO である情報化推進室によるレビューを義務付けた。	文部科学省
情報ネットワークの本省における集中管理が可能となり、標的型メール等の不審メールや不審サイトへのアクセスのブロック、ログ分析並びに事案対応等を統一的に実施する環境を整備した。	外務省
シンクライアント PC を導入し、端末からの情報漏えいリスクの低減を図るとともに、外部へのデータ移送時の対策強化として、USB 等外部メディアの強制暗号化やメール誤送信防止ツール等の仕組みを導入した。	経済産業省
セキュリティ USB メモリを一括購入して配布し、その他の USB メモリの使用は運用ルールとして全て禁止した。採用したセキュリティ USB メモリは、パスワード認証、暗号化等の各機能を有している。	人事院 （環境省）
私有可搬記憶媒体を省内の情報システムで使用禁止とした規則の実効性を高めるため、使用禁止とする専用のソフトウェアを情報システムに導入した。	防衛省
不審メール等が頻繁であり、その中に本物のマルウェアが入っていたことがある者について、メールアドレスを変更。新旧のアドレス併用期間を２週間ほど設け、変更による業務効率低下を防止した。	人事院
メールソフトウェアの振り分け機能を利用し、組織内、他省庁、外部からのメールを自動で振り分けさせ、外部からの添付及びリンク型のメールの差出人の確認を強化した。	復興庁
大容量ファイルを暗号化、期限付き、パスワード付きで安全に授受できる仕組みを導入した。要機密情報は移送手続きも同時に自動的に実施され、平易に利用することが可能である。	環境省

第２節 各府省庁における情報セキュリティ対策の取組

本節では、平成 24 年度の各府省庁の情報セキュリティ対策の取組の状況を報告する。

1 内閣官房

最高情報セキュリティ責任者からのメッセージ

内閣官房は内閣の直属の機関として、他の府省庁以上に秘匿性の高い情報を扱うことから、高度な情報セキュリティ対策を講じる必要があるため、内閣官房の特性を踏まえた情報セキュリティ教育、サイバー攻撃に関する情報の入手・分析等を行い、それらに対応する最新の情報に基づく注意喚起を行うなど情報セキュリティ対策を実施してきました。

平成２４年度においては、政府機関の公開情報等を利用し、問い合せを装うといった、巧妙な手口を用いた標的型攻撃と思われるメールの送信を多数受け、平成２３年度に引き続き、内閣官房がサイバー攻撃のターゲットにされていることが明らかとなる事象が散見されました。幸いにもウイルス感染や情報漏洩といった重大な事故に至らなかったことは、これまで実施してきた情報セキュリティ対策が一定の効果を上げた結果と言えますが、サイバー空間における脅威は日々増大しており、情報セキュリティの水準には、ここまで達成していればよいという限度はありません。

また、府省庁の壁を越えて連携し機動的な支援を行う組織として、情報セキュリティ緊急支援チーム（ＣＹＭＡＴ※1）が情報セキュリティセンターに設置されたことを受け、内閣官房ＣＳＩＲＴ※2を設置し、セキュリティ事案発生時に被害を最小化し、迅速な復旧を支援する体制を新たに整備しました。

情報セキュリティ対策は決して現状維持に止まることなく、平成２５年度以降においてもさらに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。

平成２５年４月１５日
最高情報セキュリティ責任者
内閣総務官　河内　隆

※１　ＣＹＭＡＴ： Cyber incident Mobile Assistant Team
※２　ＣＳＩＲＴ： Computer Security Incident Response Team

A) 平成 24 年度の総括

ア）平成 24 年度の評価

平成２４年度は、政府機関に対するサイバー攻撃の増加に鑑み、サイバー攻撃についての職員の理解を深めるための教育、ソーシャルハッキングの手口を用いる標的型攻撃に関する実践的な訓練及びＳＮＳ利用で発生した事件について事例紹介を行った。

また、平成２３年度の自己点検及び監査の結果を踏まえ、実施手順書等の追加整備を行うとともに、自己点検時の学習用教材に実際の業務で起こり得る事例を用い、より職員の理解度を深める教育を実施した。

個別業務システムについては、重点検査結果は良好であるものの、部局で運用しているＨＰ更新用ＰＣ（通常、スタンドアロン扱いのとなっているもの）について、セキュリティ管理が適切に行われていないものがあったことから、対策の検討が必要と考えられる。

イ）平成 25 年度の目標

a)　標的型攻撃等に対応した職員教育の実施

標的型攻撃に用いられるメールの内容は、ソーシャルハッキングの技術を用いた新たな手口が日々生み出されていることから、新たな手口に対応し、攻撃を防ぐための職員教育を実施する。

b)　自己点検の工夫

自己点検の実施に当たっては、設問の意図が正確に伝わるよう工夫をし、より正確に内閣官房の情報セキュリティ対策の状況が把握できるように努める。

c)　情報セキュリティ関係規程の整備及び見直し

「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統一技術基準」が情報セキュリティ政策会議で決定され次第、既に整備されているポリシーや実施手順書等を見直し、準拠させる。

d)　情報システムを用いた情報発信に係るセキュリティ対策の検討

ソーシャルネットワーキングサービスを活用した情報発信の増加が想定されるため、そのようなサービスを利用する場合の情報セキュリティの在り方について検討を行い、対策を講じる。

B) 情報セキュリティ対策の実施状況

ア）省庁対策基準に関する自己点検結果

a)　一般職員（行政事務従事者）

本年度における自己点検は、ＮＩＳＣにおいて指定した項目（昨年度において、違反が認められた遵守事項、実施率が低かった遵守事項及び統一基準改正で新たに追加された遵守事項）について検査を行っているが、「情報の作成と入手」における取扱について、理解が不足していることが明らかとなった。職員の理解力の向上及びセキュリティポリシーの遵守に向けて一層の対策実施が必要と考えられる。

b)　課室長級職員（情報セキュリティ責任者、情報セキュリティ副責任者、課室情報セキュリティ責任者）

課室長級職員については、情報セキュリティ対策として、情報セキュリティ教育を行わなければならないこととされているが、実施不足等の回答が見受けられ、また、区域情報セキュリティ責任者においては、情報取扱区域における管理及び利用制限に係る検討が未実施等の回答が散見されたことから、完全な実施に向けて一層の取り組

みが必要と考えられる。

c) 情報システム担当職員（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）

システム担当職員については、システムの運用に関するドキュメント類について一部未整備があること、セキュリティホール対策に関する記録について不備があることが明らかになった。セキュリティ対策の完全な実施に向けてなお一層の取り組みが必要と考えられる。

イ）情報システムごとの状況

該当無し

ウ）監査の状況

a) 関係規程に関する準拠性監査

- **統一基準とポリシーの準拠性監査**

統一基準が要求する事項を満たしていることが確認された。

- **ポリシーと実施手順等の整合性確認**

各実施手順書は、ポリシーで要求されている項目を概ね満たしていることが確認された。

b) 自己点検に関する監査

- **情報セキュリティ対策の体制に関する監査**

点検結果は、監査時の調査票回答結果と一致しており、適切に自己点検が実施されていることが確認された。

- **執務室における情報セキュリティ対策の実施状況に関する監査**

点検結果は、監査時の調査票回答結果と一致しており、適切に自己点検が実施されていることが確認された。

エ）教育・啓発

府機関に対するサイバー攻撃の増加に鑑み、標的型攻撃メールをはじめとしたサイバー攻撃全般に関する理解を深める事、また、スマートフォンの普及と共に利用者が増加したＳＮＳの潜在的リスクの理解を目的とした内閣官房情報セキュリティ教育教材を作成し、職員に配布した。

サイバー攻撃については、攻撃のパターンを類型化し、攻撃の対象、攻撃の目的等を分かりやすく解説し、その内標的型攻撃メールについては、当該メールを判別するためのポイントの解説をした。また、ＳＮＳについては、Twitter や Facebook 等で発生した事件を具体的に取り上げ、その要因等を解説することにより、ＳＮＳの潜在的リスクの解説をした。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

平成 24 年度は、内閣官房において情報セキュリティに関する障害・事故等の発生は無かった。

イ）公表した障害・事故等の概要、それに対する対応等

該当無し

最高情報セキュリティアドバイザーからのメッセージ

内閣官房は、内閣総理大臣、内閣官房長官のスタッフとして比較的フラットで多様かつ流動的な組織となっている。主任大臣の下、内閣の事務をラインで分担する他の府省庁と異なる組織構造となっており、情報セキュリティポリシーを徹底させるため、固有の困難さを有している。一方で、各府省庁の情報セキュリティ対策の調整を行う内閣官房情報セキュリティセンター(ＮＩＳＣ)、また、高度な情報保全を行う必要のある内閣情報調査室も置かれており、政府の情報セキュリティ対策の範を示すことも期待されている。

内閣官房は官邸ウェブサイトなど、サイバー空間において、ＳＮＳの活用も取り入れ、政府あるいは我が国を代表した情報発信を行っている。また、政府の高度な情報を他の府省庁から集約するとともに自ら収集を行っている。こうした特性のある内閣官房においては、近年の政府機関等に対する不審メール送付の増大をはじめとする新たな攻撃に対して、特に高度な情報システム運用上の機密確保対策が求められている。一旦、標的型攻撃に用いられる不正プログラムを起動させてしまうと、その後は、いわゆるハッキング手口によりシステム内部への侵入を許してしまうことになりかねず、情報窃取等の目的が遂行される前にいち早く対処が求められるからである。

このような認識のもと、最高情報セキュリティ責任者である内閣総務官は、内閣官房内にＣＳＩＲＴを立ち上げ、情報セキュリティの実質的なインシデントを未然に防止し、インシデントの兆候を発見した場合に早急に最高情報セキュリティ責任者以下関係者に報告し、対処する体制を整えたところである。また、職員に対しては、内閣官房への着任時及びその後継続的に丁寧な職員教育について、実施の徹底を図るよう指示するなどの努力を重ね、標的型攻撃への対策実施等を通じて、情報セキュリティ上の脅威は極めて高いことを自覚させるべく取り組んできている。システム運用面においては、適切な脆弱性対策を継続し、セキュリティの高度化を図るよう務めた。

今後、内閣官房がサイバー攻撃や情報の窃取を企図する者にとっての標的となり、サイバー攻撃等の状況がますます厳しくなる可能性が否定できない中、最高情報セキュリティ責任者である内閣総務官は、引き続き、情報セキュリティ責任者をはじめとする幹部の意識を高め、また、職員の意識向上に対する取り組みを継続することが必要となる。併せて、サイバー攻撃等への耐性を高めるためのシステム面の一層の強化といった取組が求められる。

我々、最高情報セキュリティアドバイザーも内閣総務官、総務官室スタッフに対し専門的な見地からアドバイスを行い、セキュリティリスクを見極め、その対応を行うセキュリティの質の向上を深めていきたい。今後とも、情報セキュリティへの取組が進むことで、情報の安全性がさらに高まることを期待する。

平成２５年４月１５日
最高情報セキュリティアドバイザー
中川　健治／三角　育生

2 内閣法制局

最高情報セキュリティ責任者からのメッセージ

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。このため、情報システムに対して政府統一基準群に係る重点的検査を実施し、また、情報セキュリティ監査、情報セキュリティ教育、職員の情報セキュリティ対策に係る自己点検などを実施してまいりました。

平成２４年度においては、インシデントが発生した場合に迅速に対応するための体制としてCSIRTの運用手順を新たに整備しました。

平成２５年度以降も、リスク・脅威への対策や職員向け教育の充実を図り、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
平成 25 年 5 月 30 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

情報セキュリティ対策のうち、情報セキュリティ教育について、情報漏えい等遵守すべき事項に関する教育資料の充実を図るほか、文書のライフサイクルについても情報セキュリティ教育の一環に盛り込むなど、職員の理解を深めるための教育を行いました。

イ) 平成 25 年度の目標

平成２４年度に引き続き情報システムの適切な情報セキュリティ対策及び重点検査を実施するとともに、情報セキュリティ対策に関する自己点検及び監査を実施します。

また、平成２４年度の自己点検の結果を踏まえた情報のライフサイクルに関する教育や標的型メール攻撃に対する対処に関する教育を充実させるほか、平成２４年度に整備した CSIRT の運用を円滑かつ迅速に行うことができるよう訓練を行うなど、情報セキュリティレベルの向上を図ります。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

自己点検結果は、行政事務従事者において、昨年度に比べ向上しているものの一部未実施の項目がわずかながら見られました。

イ) 情報システムごとの状況

端末及びサーバ類に対する対策のほか、毎年度、政府統一基準群で定められた遵守事項の実施状況に係る重点的な検査（以下「重点検査」という。）を実施しました。

Web サーバに関しては、ASP サービスを利用しているため重点検査の対象外となっていますが、業務を外部に委託して実施する際には、内閣法制局と同等の情報セキュリティ水準を委託先に求め、確保する必要があります。このため、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しています。

ウ) 監査の状況

監査の結果、以下のとおり全体として重大な指摘事項はなく、高いレベルで情報セキュリティ対策が実施されていることが確認されました。

・内閣法制局情報セキュリティポリシーの政府統一基準群への準拠性に関する監査
　政府統一基準群が要求する事項を満たしていることが確認されました。
・各種実施手順書の内閣法制局情報セキュリティポリシーへの準拠性に関する監査
　各種実施手順書は、内閣法制局情報セキュリティポリシーで要求されている項目を満たしていることが確認されました。
・自己点検の適正性に関する監査
　自己点検結果は、監査時の調査票回答結果と整合性があり、適切に自己点検が実施されていることが確認されました。

エ）教育・啓発

内閣法制局では、毎年度、係長級以下の職員には職員研修の際に、課長補佐級以上の職員には法令整備会議の際に、それぞれ一定の時間を確保して情報セキュリティ教育を実施しています。また、情報セキュリティ関係規程類や NISC から送付される「不審メール情報」等についても、イントラネットへの掲載と併せて全職員にメールを送信して周知しています。

C) 情報セキュリティに関する障害・事故報告

内閣法制局では、情報セキュリティに関わる障害・事故等は発生しませんでした。

最高情報セキュリティアドバイザーからのメッセージ

情報セキュリティに対する脅威は年々増大しています。その要因としては、情報化の進展により重要な情報が様々に電子化された情報資産として取り扱われ蓄積されてきていること、情報技術の進展により情報資産への攻撃手法が高度化、多様化していること、が挙げられます。特に政府機関はその性格上攻撃目標として狙われる可能性が高いといえます。

内閣法制局は、政府機関の中でも組織的には小規模で情報システムも大規模なものは保有しておりませんが、法令関連情報、人事・会計情報等重要な情報資産を保有しており、それらのセキュリティを確保するためにリスクに見合った対策を実施しております。

今年度は教育、自己点検、情報システムの重点検査及び監査等、情報セキュリティの維持、向上に向けて着実な活動を展開してきました。さらに標的型攻撃対策の一つとして、メールの取扱いの訓練や不審メールに対する職員への注意喚起等へも取り組みました。結果としてセキュリティ障害・事故がゼロであったこと、監査結果が良好であったことは評価できます。ただ、今年度重点的に実施された情報のライフサイクルにおける行政事務従事者向けの自己点検結果からは、情報リテラシー（利用能力）の向上の面で、さらなる改善の余地が見受けられます。

今後は、計画、実施、監査・点検、見直しという情報セキュリティマネジメントの PDCA サイクルを着実に回す中で、今年度の活動から得られた課題への対策を組み込み、セキュリティレベルを継続的に改善させることが重要と考えます。

最高情報セキュリティアドバイザーとしては、内閣法制局の実状に合ったアドバイスを適切に提供し、当局のセキュリティレベルの更なる向上に貢献する所存であります。

最高情報セキュリティアドバイザー（内閣法制局 CIO 補佐官）
吉田 幸彦
平成 25 年 5 月 30 日

3 人事院

最高情報セキュリティ責任者からのメッセージ

人事院は、公務の民主的かつ能率的な運営を国民に対し保障するという国家公務員法の基本理念の下、人事行政の公正の確保と職員の利益の保護等その使命の達成に努めており、広く人事行政に関する事務を所管しています。

我が国では、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、不正アクセスやウイルス感染による情報漏えいのリスク・脅威は増大するなど、政府機関等の保有する情報に対する情報セキュリティ対策の重要性がますます高まってきています。

とりわけ、昨今は政府機関等に向けた「標的型諜報攻撃」「ウエブサイト改ざん」等のサイバー攻撃が頻発しており、これらに適切に対処するためには、各職員が正しい知識と判断基準を持って業務に従事しなければなりません。

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、組織として情報セキュリティ対策に取り組む必要があります。

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各種の計画等に基づき、「内閣官房情報セキュリティセンター（「ＮＩＳＣ：National Information Security Center)」(以下「ＮＩＳＣ」という。）と連携し、人事院における情報セキュリティ対策を実施しています。

本報告書は、平成 24 年度に人事院が実施した情報セキュリティ対策の具体的取組、監査結果等についてとりまとめたものです。今後も情報セキュリティをとりまく環境の変化や情報通信技術の動向を踏まえ、情報セキュリティ上の脅威に適切に対応し、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。

平成 25 年４月

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

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

人事院では、平成 24 年度において目標とした教育・自己点検の充実及び外部専門家による監査の実施などにより情報セキュリティレベルの更なる向上に努めました。それらを実施することにより職員の情報セキュリティに対する認識が高まり、人事院の情報セキュリティレベルの向上が図られたと考えます。

イ) 平成 25 年度の目標

平成 25 年度においては、一層の情報セキュリティ対策の向上を図るため以下の目標に取り組むこととしたい。

- 対象者を明確にし、各対象者に応じた内容に重点をおいた研修の実施
- 情報セキュリティ対策向上のための情報技術の活用

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

職員による情報セキュリティ対策の実施状況を確認するため、情報の利用等に着目し、情報の格付や取扱制限などの重点項目に絞り込んで自己点検を行いました。その結果、全体としては適切に対策が実施されているが、一部で徹底されていない状況があることが確認されました。これら明確になった課題については継続して改善に取り組んでいます。

イ) 情報システムごとの状況

人事院における情報システムの利用、運用局面について情報セキュリティ監査を実施し、情報セキュリティの規程に準拠した対策が実施されていることを確認しました。今後もこの状態を維持するよう努めます。また、内閣官房及び総務省で実施した政府情報システム棚卸しにより、これまでシステムとして認識されていなかったシステムが新たに認識されたことから、それらのシステムセキュリティ責任者に対する研修を強化したいと考えます。

ウ) 監査の状況

情報セキュリティの水準を維持・向上させるためには、情報セキュリティ対策の実施状況を適切に評価し、改善すべき点を見直す、というＰＤＣＡ（注）サイクルを回すことが重要です。

人事院では、人事院情報セキュリティポリシーが政府機関統一基準群に準拠しているかを評価し、定められた対策が適切に実行されているかを確認するため、毎年度情報セキュリティ監査を実施しています。

(注)ＰDCA・・・計画（Plan)、実行（Do)、評価（Check)、改善行動（Act）の頭文字

エ) 教育・啓発

情報セキュリティ対策に対する理解を浸透させるため、院内イントラネットを利用した e-ラーニングを全職員に受講させるとともに、新規採用職員及び情報セキュリティ担当者等に集合研修を行ったほか、地方事務局（所）職員が会議のために本院に集合した機会を活用して研修を実施するなど様々な機会を通じて教育・啓発を行いました。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

人事院においては、情報セキュリティに関する障害・事故等が発生した場合は、障害・事故等の報告・対応手順書に基づき、情報セキュリティ責任者又は情報システムセキュリティ責任者がその状況を把握するとともに、対処方針の決定、関係者への連絡等を迅速に行い、結果報告書を最高情報セキュリティ責任者に提出することとしています。また、事案対応後に発生原因の調査、再発防止策を策定した上で、最高情報セキュリティ責任者に報告することとなっています。

最高情報セキュリティアドバイザーからのメッセージ

本院は、我が国の人事行政に広範な権限を有し、また、その業務の性質上、情報システムに大量の重要情報を保有しています。そのため、本院では、業務の効率性とのバランスをとりながら、厳重な情報セキュリティ対策を取る必要があります。

本院では、これまでもそのように厳重な情報セキュリティ対策をとってまいりましたが、平成 24 年度は、以下のような重点事項を定め、対策を推進しました。

- 職員に対する情報セキュリティ教育（標的型攻撃メール訓練を含む）

  新規採用職員等への集合教育の実施及び全職員を対象とする情報セキュリティ学習環境のイントラネット上での整備を行った。

  標的型メール攻撃に対する認識を深めるとともに、模擬標的型攻撃メールを用いた訓練を再三行い、職員の注意を喚起した。

- CSIRT の設置

  本院内に CSIRT を設置し、情報セキュリティインシデントに機動的に対応する体制を整備した。

- 情報セキュリティポリシーの改定

  「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」の改定により、「区域情報セキュリティ責任者」が新設されたことに伴い、本院の「情報セキュリティポリシー」についても、「区域情報セキュリティ責任者」についての規程を盛り込むなど、改定を行った。

平成 25 年度は「標的型メール」や「遠隔操作ウイルス」のようなサイバー攻撃が前年度よりもますます多様な形で仕掛けられることが予想されるため、これまでの施策を継承し、さらに強化する必要があります。

職員教育においては、集合研修、イントラネット上での e-ラーニングなど、職員が情報セキュリティに関する知識を得る機会をさらに増やし、教材などの内容もより充実させることが急務です。

また、これに加えて「標的型攻撃」への情報技術面での対策（マルウエアが内部に侵入することを前提として、外部へのデータ流出を防ぐ「出口対策」等）についても最新の情報を幅広く収集し、研究しておく必要があります。

以上の課題を踏まえ、本院では、平成 25 年度においても、情報セキュリティ対策を強力に推進して参ります。

平成 25 年４月

人事院最高情報セキュリティアドバイザー
宮　崎　晋　吾

4 内閣府

最高情報セキュリティ責任者からのメッセージ

内閣府では、内閣の重要政策に関する内閣の事務を助けること、及び内閣総理大臣が担当するにふさわしい行政事務を行っており、社会全体の模範となるよう、率先して情報セキュリティ対策に取り組む必要があります。

具体的には、世論調査、機械受注統計などの調査原票（個人情報または特定企業の情報）をはじめ、各部局での政策立案過程における検討資料といった機密性の高い情報を日常業務の中で扱っております。こうした情報の漏洩が政府への信用失墜につながるとの認識を内閣府の職員全員に浸透させることなど、情報セキュリティ対策の重要性の周知・徹底に努めているところです。

また、情報通信の多様化と利用者の増大に伴い、システム面においても情報セキュリティ対策の重要性が益々高まっております。具体的には、インターネットや情報システムの利便性が向上する一方で、サイバー攻撃、不正アクセス、ウィルス感染やフィッシングサイトからの情報漏えいなどのリスク・脅威が増大していることに対処する重要性が増しています。平成 23 年 7 月以降に多発した衆・参両議院及び各省庁等へのサイバー攻撃や不審メールが身近な脅威となっています。

内閣府におきましては、不正アクセスやコンピュータ・ウィルスの感染による情報漏洩・改竄等の情報セキュリティ障害等が生じないよう、内閣府 LAN（基幹ネットワークシステム）の更新などの機会があるごとに最新のセキュリティ強化のための対策を行っているところです。

平成 24 年度におきましては、サーバ等のシステムに対する監視も怠りなく行っているため、重大な情報セキュリティ障害等の問題は発生しませんでした。

本報告書は、内閣府が平成 24 年度に実施した情報セキュリティ対策の具体的取組等についてとりまとめたものです。

内閣府では、今後ともシステム上のセキュリティ対策の強化と職員向けセキュリティ教育徹底の両面から、引き続き情報セキュリティ対策の強化に努めてまいります。

最高情報セキュリティ責任者
（内閣府大臣官房長）
阪本　和道

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

e-ラーニングの実施率の向上に努めるなど、各職員の情報セキュリティ対策に対する理解と実行レベルの底上げに重点的に取り組みました。

また、政府機関においても標的型メール攻撃による被害が増大していることを重視し、全職員を対象に標的型メール攻撃訓練を実施しました。

イ) 平成 25 年度の目標

「内閣府本府情報セキュリティポリシー及び同技術基準」の遵守徹底のために、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、最近の国内で発生した主な情報セキュリティ障害・不正アクセスによる被害事例を紹介しながら、情報セキュリティ教育、新人研修等により周知徹底に今後とも努め、職員が理解し易い内容に改善します。

具体的には、内閣府では、他省庁・民間企業等と多くの人事交流が行われています。そのため、人事異動に伴う新人教育の機会が多くあります。そこで、官房人事課との連携を強化し、新人研修の機会においては、情報漏洩防止のための注意喚起を必ず行うことなどの啓発強化に努めます。また、e-ラーニングの受講教材においても政府機関における被害事例を掲載し、職員への注意喚起を行っています。教育用資料更新の際には、内閣府の職員として特に気を付けるべき事例に絞るなどの工夫にも努めます。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

平成 24 年度全職員を対象にした自己点検を提出した者の割合である把握率は、前年度に続き、100%（完全実施）となりました。

把握した職員のうち、対策を実施した者の割合である対策実施率の主体別の状況は、前年度に続き、100%（完全実施）となりました。

イ) 情報システムごとの状況

平成 24 年度における公開用 Web サーバ、メールサーバ、DNS サーバは、不正プログラム対策（最新のアンチウイルスソフトウェア等の導入状況）、情報保護対策（電子メール利用時の通信の暗号化機能の導入状況）などの対策事項の実施率は 100%でした。

ウ) 監査の状況

内閣府では、統一基準群（統一管理基準、統一技術基準等）に準拠して策定されたポリシー・技術基準及び関係規程・実施手順について、統一基準群との準拠性と実効性について客観的に確認しています。

これが以下の監査のうちの準拠性監査です。

また、内閣府では、職員がポリシー・技術基準等の規程に基づく情報セキュリティ対策を遵守しているかどうかについて、毎年度自己点検を行うとともに、自己点検の監査も実施しています。

さらに、内閣府内の各情報システムが、ポリシー・技術基準及び関係規程・実施手順に基づいて、適切に管理・運用されているかを評価し、各情報システムにおける情報セキュリティのレベルを向上させるための助言を行うことを目的として監査も実施しています。

そのうちの、準拠性監査は、監査の客観性の確保及びより専門的な観点から脆弱性の点検を行うために外部の第三者組織に委託して実施しています

a) 準拠性監査

平成 24 年度は、統一管理基準・統一技術基準との準拠性を中心に、ポリシー・技術基準及び関係規程について、外部の監査組織に委託して平成２４年７月～9 月にかけて監査を実施しました。

b) 自己点検の監査

平成 24 年 3 月に策定した「平成 24 年度自己点検に関する監査実施計画書」により、サンプル選定した部局について、情報セキュリティ責任者 1 名、区域情報セキュリティ責任者 1 名、課室情報セキュリティ責任者 1 名、障害・事故等に対応する責任者 1 名、情報システムセキュリティ責任者及び同管理者各 2 名、権限管理を行う者 1 名及び職員 99 名を対象に平成 24 年 10 月に自己点検の回答内容（各職員とも 100%実施）が正しいかを確認するための監査を実施しました。

エ) 教育・啓発

内閣府では、毎年度、当該年度の研修計画に基づき、 e-ラーニングにより情報セキュリティ教育を実施しています。

また、新規採用職員の集合研修において情報セキュリティ教育を行うなど、各職員の情報セキュリティ対策に対する理解の浸透に努めています。

C) 情報セキュリティに関する障害・事故報告

ア) 情報セキュリティに関する障害・事故等の把握

内閣府では、「障害・事故等対応手順書」に基づき、(ｱ)対処承認権限者である課室情報セキュリティ責任者、区域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に報告を行うとともに、(ｲ)情報セキュリティ責任者関係部署（大臣官房企画調整課情報システム室、大臣官房総務課）等にも報告を行う。(ｳ) 対処承認権限者である課室情報セキュリティ責任者等は、対処を実施する者に指示を行うとともに、再発防止策承認権限者である情報セキュリティ責任者に報告を行う。(ｴ) 報告を受けた情報セキュリティ責任者は、最高情報セキュリティ責任者に報告を行う。

なお、対外公表を行う事案などの他省庁と情報共有すべき障害・事故等については、情報セキュリティ責任者関係部署（大臣官房企画調整課情報システム室）から内閣官房情報セキュリティセンターに報告を行う。

イ) 公表した障害・事故等の概要、それに対する対応等

内閣府では、平成 24 年度において、以下の a)から c)の情報セキュリティに関する障害・事故等を経験しました。

a) 内閣府職員を騙った詐称メール被害

- **情報セキュリティに関する障害・事故等の発生日時**

  平成 24 年 4 月 4 日の夕刻、10 月 11 日の夕刻

- **概要**

  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たことが判明しました。

- **原因**

  外部の何者かが、内閣府職員のメールアドレスを窃取したことによるものです。

- **内閣府の対応**

内閣府ホームページにおいて、国民に対して注意喚起を行うとともに、報道関係者にも周知しました。　詐称されたメールアドレスを拒否設定するとともに、内閣官房情報セキュリティセンターに報告しました。

また、内閣官房情報セキュリティセンターでは、各省庁に対して当該メールアドレスに対する注意喚起を行っています。

- **原因が省庁対策基準（ポリシー）違反によるものか否か**

今回の事例では、メールアドレスを窃取された職員の不注意によるものとは考えられないため、ポリシー違反には該当しません。

- **再発防止策**

内閣府職員のメールアドレスを掲載している内閣府ホームページを差し替えるなどを行うとともに、メールアドレスの詐称防止のために、内閣府ホームページにおいてはメールアドレス掲載を禁止としていることを再周知しました。

b)　原子力安全委員会事務局がホームページに掲載したマスキング（黒塗り）情報が参照可能な状態となっていた事例

- **情報セキュリティに関する障害・事故等の発生日時**

平成 24 年 6 月 12 日の午後 9 時頃

- **概要**

原子力安全委員会事務局が 6 月 12 日午後 9 時頃に原子力安全委員会ホームページに掲載した「全交流電源喪失事象検討ワーキンググループ関係資料の公開までの経緯について」の資料のうち、電力会社とのやりとりの電子メールの資料において、特定のソフトウェアを用いることで個人情報等のマスキングが外せる状態でした。

- **原因**

PDF で黒塗りに使用した画像（図形）の削除が容易にでき、その下の文字の表示が可能となることを掲載担当者が理解していなかったことによるものです。

- **内閣府の対応**

上記の状況を 6 月 13 日午前 10 時 30 分頃に確認し、ただちに個人情報等のマスキングが外せない資料に差し替えをしました。

- **原因が省庁対策基準（ポリシー）違反によるものか否か**

ポリシー1.3.1.5(1)情報の提供の(b)（付加情報からの不用意な情報漏洩）に該当します。

- **再発防止策**

内閣府職員（特に Web 担当）が参照する「内閣府ホームページ利用上のその他事項：情報漏洩防止」の中で注意喚起している事項を遵守するように内閣府内に改めて周知しました。

なお、この注意喚起の内容には、「ホームページ掲載資料からの情報漏えいについての PDF 事例:掲載した PDF から黒塗りしたはずの個人情報が抽出できてしまった。」として、今回の事例を代表例として掲載しています。

c)　メールアドレスの流出事例

- **情報セキュリティに関する障害・事故等の発生日時**

平成 24 年 9 月 13 日（木）午後

- **概要**

平成 24 年 9 月 13 日（木）午後、政策統括官（共生社会政策担当）の担当者が、障害者政策委員会第 3 小委員会の委員及び専門委員並びに委員・専門委員秘書に受

信者に見える形で電子メールを送信しました。

- **原因**

送信先メールアドレスを BCC に入力すべきところを誤って宛先に入力して送信してしまったため、計 21 件のアドレスが受信者に見える形での送信となりました。

- **内閣府の対応**

「メールを送信する際の注意事項」を総括担当参事官名で発出し、再発防止に努めることとし、報道関係者にも公表しました。

- **原因が省庁対策基準（ポリシー）違反によるものか否か**

ポリシー1.3.1.5(1)情報の提供の(b)（付加情報からの不用意な情報漏洩）に該当します。

- **再発防止策**

部局内の全職員に対し誤送信防止の注意喚起を行うとともに、下記の追加措置を講ずることとしました。

・ 室内職員を 3 名程度のグループ別にして、複数の部外者へメールを送信する場合は、必ずグループに所属する他の職員 1 名が確認してから送信することとする。
・ BCC の宛先に事前登録した場合は、グループ内で共有し総括担当に報告させるとともに適正に処理されているか総括担当が確認することとする。

最高情報セキュリティアドバイザーからのメッセージ

情報伝達・収集手段の多様化に伴い、内閣府においても政府インターネットテレビなどにおいて動画中継による国民への情報提供を行っている他、ツイッターやアイデアボックスなどを利用して国民からの意見を聴取することに努めている。

このような新たな通信手段を用いた国民との情報交換手段の多様化に伴い、不正アクセス、ウィルス感染やフィッシングサイトからの情報漏えいなどのリスクが増大している。増大するリスク対策として、サイバー攻撃や不審メール対策を中心に最新版のアンチウイルスソフトの導入、検疫認証システム、内閣府外への電子メールの暗号化機能を中心とした情報セキュリティ対策を強化していく必要がある。

さらに、東日本大震災の経験を踏まえ、物理的なシステムのバックアップ対策の強化を検討している。具体的には、媒体バックアップ、無停電電源装置、自家発電装置、耐震又は免震設備等の対策が考えられる。これらについては、既に殆どの対策を導入しているシステムもある一方、まだこれらの対策を完了していないシステムも存在する。対策を完了していないシステムに関しては、優先順位の高い対策から順次取り入れることが課題である。

また、内閣府は、幅広い分野での国民への情報提供や政府全体の政策を統括する業務などを担っている。これらの業務を遂行する中で職員が日常取扱っている情報のほとんどが機密性の高い情報である。一方、障害・事故等の大部分が不注意やミスによるものとの報告もある。そこで情報システム面での対策強化だけでなく職員全員のセキュリティポリシーの完全遵守を目指し、情報セキュリティ対策を漏れなく行う必要がある。

内閣府は、各省庁、地方自治体及び民間企業等との人事交流が盛んに行われており、新たに内閣府職員となった職員に対する情報セキュリティ教育を間断なく行う必要性があることから、今後とも各職員における情報セキュリティ対策の更なる理解向上に努める必要があると考える。

このような観点から、情報セキュリティ教育に力を入れることが重要であると認識しており、そのための一環として、最高情報セキュリティアドバイザとしては、分かりやすい教育資料及びセキュリティを重視した調達仕様書テンプレート案を作成中である。

最高情報セキュリティアドバイザとしては、情報システム構築・更新の際などの情報システムに関するアドバイスのみならず、このような職員教育も含めて、総合的な改善・対策を支援していく所存である。

最高情報セキュリティアドバイザ
谷口英宣
（内閣府 CIO 補佐官）
平成 25 年 4 月 1 日

5 宮内庁

最高情報セキュリティ責任者からのメッセージ

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，様々な情報資産や情報システムを適切に管理し，利用するためには，組織として情報セキュリティ対策に取り組む必要があります。

宮内庁は，これまで，情報セキュリティ教育及び職員を対象とした情報セキュリティ対策実施状況の自己点検と職員向けの注意喚起を中心に，セキュリティ対策を推進してきました。

現段階では重大な課題等は発見されておりませんが，リスク・脅威への対策や職員向け教育は，常に改善と努力が必要です。宮内庁は，今後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。

宮内庁最高情報セキュリティ責任者
（長官官房審議官）牧野　尊行
平成 25 年 4 月 24 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度の重点事項として，政府機関の情報セキュリティ対策のための統一基準群の改定に伴い，宮内庁の情報セキュリティポリシーや関連規程を見直し，職員へ周知しました。

また，政府機関等に対する標的型メール等のサイバー攻撃が増えていることに対し，職員が適切に対処できるよう研修教材の内容を充実させ，情報セキュリティ研修や標的型メール訓練を実施しました。

情報セキュリティ研修や標的型メール訓練の実施により，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。

イ) 平成 25 年度の目標

平成 25 年度の重点目標は，職員の情報セキュリティに対する意識の向上とそれによる情報セキュリティ対策の推進とし，以下の取組を実施します。

・情報セキュリティ教育・訓練の充実
・標的型メール攻撃等に適切に対処するため，職員が正しい判断基準を持てるよう情報セキュリティ研修教材の見直し

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

宮内庁職員の情報セキュリティ対策実施状況について自己点検を行った結果，おおむね適切に実施していることが明らかとなりましたが，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。

イ) 情報システムごとの状況

宮内庁の各情報システムの情報セキュリティについては，重点検査を行った結果，ウェブサーバ及び電子メールサーバ等において必要な対策が講じられていることが確認されました。引き続き，適切な情報セキュリティ対策の実施に努めます。

ウ) 監査の状況

監査の内容は，宮内庁の情報セキュリティ関連規程類の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統一技術基準への準拠性や，情報セキュリティ対策自己点検に関する監査及び情報システムの情報セキュリティ対策の実施状況の監査です。

監査の結果，規程類の準拠性については，改善が必要とされる特段の指摘事項はありませんでした。情報セキュリティ対策自己点検については，情報セキュリティ責任者等，情報システムセキュリティ責任者等及び職員に対して，自己点検における全項目の回答内容が正しいか確認し，自己点検が適正に実施されていることが確認されました。しかし，若干ながら，宮内庁情報セキュリティポリシーの趣旨の理解が不十分であることを示す事例も見受けられました。情報システムの情報セキュリティ対策の実施状況については，宮内庁情報セキュリティポリシーに則った手順書どおりに利用できており，実際のシステム設定も手順書等と整合していることが確認でき問題はありませんでした。

エ) 教育・啓発

情報セキュリティ対策を着実に実施するためには，情報を取り扱う職員それぞれが情報セキュリティ関連規程に基づく具体的なセキュリティ対策を理解し，遵守することが

肝要であり，そのためには，職員に対する教育，研修が重要なものと考えています。

宮内庁では，情報セキュリティ教育についての年度計画を策定し，集合研修や職員用電子掲示板を利用した自習教育を実施しています。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 2 回ずつ，6 月と 3 月に実施し，対象者の業務上必要となる知識レベルに応じた教育教材を作成しています。

また，教材には，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を適宜記載しています。さらに，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，課題や取るべき対策を具体的に説明するようにしています。

特に今年度は，政府機関を標的とした「サイバー攻撃」が多発したこと及び当庁においても「標的型メール攻撃訓練」を実施したことを踏まえ，「標的型メール攻撃」に焦点を当てた解説を行いました。

定期研修のほか，自己点検の実施や「標的型メール攻撃訓練」の実施等が，職員の意識向上に寄与するものと推察します。今後も，充実した教育機会の提供や教材の整備に努めます。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

宮内庁では，万一，情報セキュリティに関する障害・事故等が発生した場合には，障害時の対応手順（障害等対応規程）や緊急連絡網により，発生箇所の責任者がその状況を把握し，関係者に連絡することになっており，障害・事故等に対応した後は，再発防止策を策定し，最高情報セキュリティ責任者に報告することになっています。

イ）公表した障害・事故等の概要、それに対する対応等

平成 24 年 4 月から 9 月にかけて当庁職員が同僚の ID・パスワードを使用して，内部のネットワークへ不正アクセスし，同僚の業務メールを閲覧したという事案が発生し処分を行いました。この事案は，職員一人一人がポリシーの定める遵守事項を実践していれば防止することもできたことから，再発防止策のため職員用電子掲示板にて全職員へパスワードの管理等について注意喚起を行いました。

最高情報セキュリティアドバイザーからのメッセージ

NISC による標的型メール攻撃訓練及び公開ウェブサーバ脆弱性検査の結果に加え，日々刻々と多様に巧妙化・複雑化する攻撃手法が編み出されていく現状にあっては，現時点で情報セキュリティ対策が十分に施されていたとしても，それに満足することなく，人的な対策（主に職員の情報セキュリティに関する知識・意識の向上）と技術的な対策（主に情報システムそのものの情報セキュリティ対策）の両方を継続的に行っていくことが重要です。

人的な対策については，職員が自身のこととして考えられるように情報セキュリティ研修などのコンテンツの拡充をはかりつつ，今後も情報セキュリティ教育研修などを通じて基本となるポリシーの周知・徹底に努めます。

技術的な対策については，宮内庁ネットワークシステムのセキュリティ強化（主に標的型攻撃対策）について限られた予算の中で最大限の効果が発揮されるような調達仕様書の作成に加え，単に装置を導入するだけでなく，情報システムの運用におけるインシデント対応の迅速化と被害の最小化を図る体制の強化を行っていくことが推奨されます。

宮内庁最高情報セキュリティアドバイザー
根本直樹
平成 25 年 4 月 24 日

6 公正取引委員会

最高情報セキュリティ責任者からのメッセージ

公正取引委員会においては，平成 24 年度には，情報セキュリティに関する重大な障害，事故等は発生しておらず，また，緊急に対応が必要な重大な課題も発生していません。

しかし，情報セキュリティを取り巻く環境は常に変化しており，企業や官公庁に対する不正アクセスや不審メールによる攻撃等，情報セキュリティに対する脅威は増加する状況にあります。公正取引委員会は，その業務の特性上，多くの企業に関する情報を取り扱うため，公正取引委員会が使用するシステムについて，常に，これらの脅威に対して十分な対策を採ることが必要不可欠なものと考えています。

そこで，公正取引委員会では，平成 24 年度において，内閣官房情報セキュリティセンターとの連携を図りつつ，情報セキュリティに対する脅威への対応策の整備や，全職員に対する情報セキュリティに関する最新情報の提供や教育内容の充実によって，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おります。

今後も，公正かつ自由な競争を促進して，一般消費者の利益を確保するとともに，我が国経済の健全な発達を図るという，公正取引委員会の役割を十分に果たすため，情報セキュリティ対策の充実に努めてまいります。

最高情報セキュリティ責任者
（官房総括審議官）
松　尾　　勝
平成 25 年 4 月 25 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

a) 情報セキュリティ対策の実施状況に係る自己点検結果

平成 23 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重点的に取り組んだ結果，全職員の情報セキュリティ対策の実施率は，平成 23 年度のものよりも改善しました。

b) 情報システムごとの状況

情報システムに係る重点検査では，一部の調査項目について情報セキュリティ対策の実施率は 100%には至りませんでしたが，他の調査項目では全て実施率 100%となりました。

c) 教育・啓発

情報セキュリティ対策に関し，e-ラーニング研修や集合研修を実施し，職員の情報セキュリティ対策の理解向上に寄与しています。

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，職員の理解の向上及び意識の向上が図られました。

d) 調達・外部委託

情報処理業務を外部委託によって行う場合には，職員が，調達仕様等に含めるべき事項を示した規程や，情報の保護に関する誓約書のひな形を随時参照できるようにしており，必要な情報セキュリティ水準の確保に寄与しています。

e) 情報セキュリティに関する障害・事故等の報告

前述の取組を実施した結果，情報セキュリティに関する障害・事故等は発生しませんでした。

なお，公正取引委員会内に，障害・事故等が発生した際に，迅速な復旧等を行うための体制を設置しました。

イ) 平成 25 年度の目標

公正取引委員会では，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っていきます。

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，訓練等の対策を採っていきます。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

平成 23 年度に実施した自己点検では，一部の情報セキュリティ対策の実施項目について実施状況が十分とはいえない結果となりました。そのため，職員の情報セキュリティ対策の実施状況の改善に重点的に取り組むこととし，職員が実施すべき対策内容の周知，研修内容の見直し，点検項目への解説の付記などの取組を行いました。その結果，全職員の情報セキュリティ対策の実施率は，平成 23 年度のものよりも改善することができました。

しかし，まだ実施率は 100%には至っておらず，改善の余地がありますので，引き続き，情報セキュリティ対策に係る教育や注意喚起を図り，全職員の情報セキュリティ対

策の意識向上と実施状況の改善に努めていきます。

イ）情報システムごとの状況

情報システムに係る重点検査では，一部の調査項目について情報セキュリティ対策の実施率は 100%には至りませんでしたが，他の調査項目では全て実施率 100%となりました。

今後も適切な情報セキュリティ対策を実施し，情報セキュリティレベルの維持・向上に努めていきます。

ウ）監査の状況

毎年度，情報セキュリティ対策の改善のため，情報セキュリティに係る監査計画を策定し，これに基づいた監査を実施しています。平成 24 年度については，平成 25 年２月から３月にかけて，①当委員会の情報セキュリティ関係規程と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同技術基準との準拠性監査，②職員の自己点検結果を踏まえた情報セキュリティ対策の実施状況に係る監査，③情報システムの脆弱性検査に係る監査等を実施し，いずれも問題がないことを確認しました。

エ）教育・啓発

情報セキュリティ対策に関し，全職員を対象とした e-ラーニング研修を実施したほか，管理職員及び新規・中途採用職員に対しては，これに加えて集合研修も実施しており，職員の情報セキュリティ対策の理解向上を図っています。今後も，研修等を通じて，情報セキュリティに対する全職員の理解を深めるように努めていきます。

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，重点的に取り組むべき事項として，職員への不審メール情報の発信，教育，標的型メール攻撃訓練等を実施した結果，職員の理解の向上及び意識の向上が図られました。今後も，継続的に職員への注意喚起を行い，不審メールによる攻撃への対策を採っていきます。

C) 情報セキュリティに関する障害・事故報告

情報セキュリティに関する障害・事故等は発生しませんでした。

なお，障害・事故等が発生した際，被害を最小化するとともに，迅速な復旧等を行うための体制として，公正取引委員会内にＣＳＩＲＴ（Computer Security Incident Response Team）を設置しました。ＣＳＩＲＴでは，障害・事故等の詳細把握，対応策の検討・実施，関係機関との情報共有等を行うこととしています。

最高情報セキュリティアドバイザーからのメッセージ

公正取引委員会では，情報セキュリティ対策で重要な役割を果たすのは人であるとの観点から，毎年，新規採用者，全職員及び管理職向けの情報セキュリティ研修等を行っており，研修における理解度確認テスト，情報セキュリティ対策の実施状況についての自己点検とフィードバックを行い，ＰＤＣＡサイクルを回しています。その効果は毎年発揮されており，平成 24 年度は平成 23 年度と比べて，自己点検結果と研修時の理解度確認テスト結果が共に改善されています。また，標的型メール攻撃対策では，全職員に対して，繰り返し周知を行っており，情報セキュリティ対策に対する意識が向上していると理解しています。

他方，標的型メール攻撃訓練においては，訓練用メールの文面をより現実に則したものとした結果，開封率（訓練用メールに添付されたファイルを開封した又はＵＲＬをクリックした割合）が，平成 23 年度の結果を上回りました。こういった訓練での教訓を活かして，日々の標的型メール攻撃に対する意識の維持・向上が重要になると理解しています。また，情報セキュリティ事件・事故への対応の強化として，平成 24 年にＣＳＩＲＴ体制が公正取引委員会に構築されました。この強化とともに，職員に対して今後も継続的な情報セキュリティに対する意識の維持・向上を図り，職員各々の実践により，情報セキュリティ対策を強化することが推奨されます。

公正取引委員会最高情報セキュリティアドバイザー
（公正取引委員会ＣＩＯ補佐官）
根　本　　直　樹
平成 25 年４月 25 日

7 警察庁

最高情報セキュリティ責任者からのメッセージ

警察では、限られた警察力をより効果的に発揮するため、数多くの情報システムを導入している。これらのシステムにおいて、停止、情報漏えい等の事故が発生した際の影響は計り知れない。そこで、警察庁では、「警察情報セキュリティ訓令」等の規定を定め、職員に遵守させている。

本年度は、警察情報セキュリティポリシーを改正し、警察庁ＣＳＩＲＴを設置したほか、標的型メール攻撃対策に重点的に取り組んだ。平成 24 年度に警察庁における情報セキュリティ上の重大な事故は発生していないが、引き続き諸対策の継続・強化に努めたい。

警察庁情報通信局長　佐野　淳
平成 25 年４月 30 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

a) 警察情報セキュリティポリシーの改正

区域管理に係る規定の整備、モバイル端末に係る情報セキュリティ対策の強化等を実施したほか、ユーザ向けの規定とシステム整備者向けの規定とを分割し、より職員に浸透しやすい通達体系とした。

b) 警察庁ＣＳＩＲＴの設置

平成 24 年５月、警察庁ＣＳＩＲＴを設置し、警察内部の情報セキュリティインシデントに対処する体制を整備した。その後、情報セキュリティインシデントに適切に対処した。

c) 標的型メール攻撃に係る取組

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、注意を呼びかけた。

イ) 平成 25 年度の目標

一層の情報セキュリティの確保を図るため、各級の管理者に対する教育等を行い、組織全体の情報セキュリティレベルを更に高める。特に、情報セキュリティ監査を例年よりも実地を重視したものとし、更なる強化を図る。

また、情報セキュリティインシデントの態様に応じたより機動的な対処が可能となるよう、警察庁ＣＳＩＲＴの体制の見直しを行う。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

全ての職員及び情報セキュリティに係る各管理者等が自己点検を実施し、全ての者が、役割ごとに警察情報セキュリティポリシーに規定されている遵守事項を全て遵守していることを確認した。今後もこの水準を維持するため、継続的に情報セキュリティに関する教育を実施していく必要がある。

イ) 情報システムごとの状況

a) ネットワークの分離

外部と接続されたネットワークと、警察内部のＷＡＮシステムのネットワークとを完全に分離することで、警察情報を窃取等するための外部からの攻撃を不可能にしている。

b) 外部記録媒体の利用制限措置

許可なく外部記録媒体を利用できなくするための技術的措置を講じることで、電子計算機から要機密情報を持ち出す際には、上司がパソコン上で許可手続を行う必要がある。

c) 個人所有の外部記録媒体の利用禁止措置

上司の許可を受けて外部記録媒体を利用する場合であっても、公用の外部記録媒体以外は利用できなくする技術的措置を講じている。

ウ）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。）を実施している。監査を実施した結果、各システムの情報セキュリティ対策は良好であり、情報セキュリティ侵害事案を想定した訓練の実施、毎月の情報セキュリティに関する教育の実施等、積極的な取組がみられたが、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。

監査終了後、監査報告書を最高情報セキュリティ管理者に提出するとともに、改善を求める事項、検討を要する事項等を、情報セキュリティ委員会の審議を経て決定し、対象部署の長に指示した。指示を受けた対象部署の長は、当該指示の内容を踏まえ、速やかに必要な措置をとり、その結果を最高情報セキュリティ管理者に報告することとされている。

エ）教育・啓発

警察では、職員に対し、必要な知識等を習得させるための教育訓練等を行う機関である警察大学校に様々な課程を設け、警察の各分野における高度な教育を行っているところ、その中で情報セキュリティに対する理解を深められるよう講義を行った。特に、情報セキュリティについて指導する者を育成するための課程を設け、警察情報セキュリティポリシーにおける規定事項、情報セキュリティに関する技術、情報セキュリティインシデント発生時の対応等について、実践的な訓練を交えて講義を行った。

C）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

警察庁では、国民生活又は警察活動に重大な支障が生じ得る情報セキュリティに関する障害、事故等（以下「情報セキュリティインシデント」という。）が発生した場合の措置要領を定めている。その概要は次のとおりである。

○　職員は、情報セキュリティインシデントを認知した場合は、当該職員が属する機関の情報管理を担当する所属に速やかにその概要を報告する。あわせて、被害の拡大を防止するための一時的な措置を講じる。

○　報告を受けた所属は、警察庁情報セキュリティ管理者に速やかに報告する。このとき、警察庁情報セキュリティ管理者は、当該インシデントの種別に応じて、関係する所属の長に連絡する。

○　情報セキュリティ管理者は、関係するシステムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者と緊密に連携し、当該インシデントの原因調査及び再発防止策を講じる。

イ）公表した障害・事故等の概要、それに対する対応等

公表した障害・事故はない。

最高情報セキュリティアドバイザーからのメッセージ

警察は多くの個人情報等を保有しており、その管理を徹底する必要があることから、警察職員は警察情報セキュリティポリシーを遵守し、情報システムを様々な脅威から守り、情報流出等の防止を図っている。情報セキュリティ対策には、「これで大丈夫。」という終わりはなく、新たな攻撃手法や巧妙化する手口等に対し、現在執っている対策で十分なのか、それとも更なる対策が必要なのかを検討・評価し、必要に応じて改善する、いわゆるＰＤＣＡサイクルを繰り返し回し、課題解決に向けた取組を継続していく必要がある。

今後とも、自己点検、訓練等の基本的な取組を継続するとともに、監査による確認を的確に行い、一層の情報セキュリティの確保に努めていくことが重要と考える。

警察庁情報通信局情報管理課長　羽室　英太郎
平成 25 年４月 30 日

8 金融庁

最高情報セキュリティ責任者からのメッセージ

金融庁の行政の政策目的は、金融システムの安定、利用者の保護・利用者利便の向上、公正・透明な市場の確立です。

金融庁では、これらの目的を達成するため、「有価証券報告書等電子開示システム」(EDINET)の運営や、民間金融機関等の検査・監督や、市場のルール遵守状況の監視等を行うため、日々、電子的に民間金融機関や市場関係者等から報告や資料の提出を受け、その内容について、金融庁の内部で、各種の情報システムを用いて整理・分析する等、情報システムを積極的に活用しています。

このように、金融庁において活用している情報システムは、金融資本市場における重要な情報インフラの一部を構成するとともに、個別の民間金融機関や市場関係者の情報等、非常に機密性の高い情報を取扱っているという特徴があります。

このため、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きたところです。しかしながら、昨今政府関係機関に対するサイバー攻撃が巧妙化しつつあり、中には重大な情報セキュリティ事案となったものもあります。幸い金融庁では重大な情報セキュリティ事案は発生しておりませんが、金融庁においても情報セキュリティ対策を推進する態勢の整備が、ますます重要になっていると考えております。

以上を踏まえ、金融庁では、今後も、新たなリスク・脅威に適切に対応する不断の努力を続けるとともに、職員の意識の更なる向上と実施の徹底を図るため、情報セキュリティ教育・訓練の一層の充実に努めてまいります。

総括情報セキュリティ責任者(金融庁総務企画局総括審議官・森　信親)
平成 25 年 4 月

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度においては、以下のような情報セキュリティ対策を実施。

①情報セキュリティ自己点検

全職員及び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実施状況について点検を行った結果、概ね適切に実施されていた。

②技術的セキュリティ対策の推進

全ての情報システムのウェブサーバ、電子メールサーバ等の機器を対象に、技術的な情報セキュリティ対策（以下「技術的セキュリティ対策」という。）の実施状況の点検を行い、全ての項目で適切に実施されていることを確認。

また、電子メールの誤送信を軽減するための機能を導入するとともに、不審メール送信に利用されることの多いフリーメール・アドレスからのメールを受信した場合に、職員に警告を与える機能を導入し運用を開始。

③情報セキュリティ教育

全職員が情報セキュリティに関する知識を習得するための研修を受講した。

④情報セキュリティ監査の実施

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た。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組んでいる。

⑤緊急対応体制の強化

情報システムのセキュリティに関する脅威が発生した際の対応体制を強化するため、緊急時の対応機能を有した専門的なチーム CSIRT を設置した。

イ) 平成 25 年度の目標

平成 25 年度においては、引続き以下のような取組みを実施して、更なる情報セキュリティの改善に努める。

①情報セキュリティ自己点検の実施

②技術的セキュリティ対策の推進

③情報セキュリティ教育・訓練の充実

④情報セキュリティ監査の実施

⑤平成 25 年度における重点的な取組として、導入を計画している次期庁内 LAN システムの更改にあわせて情報セキュリティ対策を強化する。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

職員、課室長及び情報システム管理者を対象として、情報セキュリティ対策の実施状況を確認するため、全職員を対象に情報セキュリティ自己点検を実施し、概ね適切に実施されていることを確認した。

イ) 情報システムごとの状況

全ての情報システムのウェブサーバ、電子メールサーバ等の機器を対象に、技術的セキュリティ対策の実施状況に関する検査を実施した結果、いずれの機器についても適切に処理されていることを確認した。

また、平成 24 年度には、電子メールに関する技術的セキュリティ対策強化のため、以下の措置を講じた。

(a) 電子メールの誤送信による情報漏えい事案を防止するため、誤送信を軽減するための機能を導入。

(b) 不審メール送信に利用されることの多いフリーメール・アドレスからのメールを受信した場合に職員に警告を与える機能を導入。

ウ) 監査の状況

金融庁情報セキュリティポリシーに基づき、毎年度、情報セキュリティ監査を実施している。

平成 24 年度においては従来から監査対象としている各種サーバやクライアント PC 等に加え、ネットワークに接続されたコピー・プリンタ複合機等を監査対象に含めた。

監査の結果、各システムの情報セキュリティ対策は概ね適切に行われていることが確認できた。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いる。

エ) 教育・啓発

職員の情報セキュリティに関する知識の習得を図るため、目的に応じた複数の情報セキュリティ研修を実施している。

また、情報セキュリティに関する訓練として NISC が主催した標的型メール攻撃教育訓練に参加し、職員の不審メールに対する対応能力の確認を行った。

オ) その他取り組んだ事項

①標的型攻撃等に関する対策を強化するため、金融庁 CSIRT を平成 24 年 5 月に設置。
②情報漏えいの可能性を検証するため、退職者が使用していたクライアント PC のログ・チェックを制度化。
③外部委託先の管理に関する取組。
④資産台帳の整備と活用。

C) 情報セキュリティに関する障害・事故報告

ア) 情報セキュリティに関する障害・事故等の把握

平成 24 年度中に情報セキュリティに関する重大な障害、事故等は発生していない。

イ) 公表した障害・事故等の概要、それに対する対応等

平成 24 年度中に情報セキュリティに関する重大な障害、事故等は発生していない。

情報セキュリティアドバイザーからのメッセージ

近年、標的型攻撃と呼ばれるサイバー攻撃による被害が、中央省庁や民間企業等国内外を問わず発生しているようです。標的型攻撃の特徴は、次のようにまとめられます。

1)攻撃手法が多様化・複雑化しており、複数の手法を組み合わせる攻撃が散見されること

2)攻撃手法自体が進化すること

3)攻撃自体が攻撃される側にとって極めてわかりづらいこと

4)被害状況把握が極めて困難であること

さらには攻撃の痕跡が消去されている例もあると言われるなど、極めて防御が難しい状況となっており、マルウェアやコンピュータウィルスの感染や不正アクセスをゼロとすることは現実的ではないと言わざるを得ません。さらには、USB メモリや重要情報が記載された紙の紛失に関しても同様のことが言えるでしょう。

金融庁では、民間金融機関等から提出された機密性の高い情報を取扱っていることから、高度の情報セキュリティ水準を維持していく必要があることから、平成 24 年 5 月に金融庁 CSIRT を立ち上げ、セキュリティ事故発生時に、被害状況把握・被害最小化・事故原因究明・再発防止を重視した活動を行っています。さらには、監査手法や監査対象を直近の脅威に対向するための情報セキュリティ監査の実施、「計画」・「対策実施」・「チェック」・「改善」のサイクルに根ざした継続的な情報セキュリティ対策の推進、情報セキュリティ担当者による各部署への情報セキュリティ教育、職員のセルフチェック等により情報セキュリティ確保に努めています。

金融庁　情報セキュリティアドバイザー
村瀬 一郎
平成 25 年 4 月

9 消費者庁

最高情報セキュリティ責任者からのメッセージ

情報通信技術の進歩と普及に伴うＩＴ化の進展により、国民生活や社会経済活動の多くの面において、いまや情報システムの利活用は重要な社会基盤となり、行政機関における行政事務の分野においても、ＩＴ化によって効率化や迅速化が図られてきました。一方で、情報セキュリティにおけるリスクも多様化・高度化・複雑化し、近年においては、行政機関等を標的としたサイバー攻撃による被害が多く発生しており、こうした様々な脅威から、取り扱う情報を確実に保護するため、行政機関における情報セキュリティ対策はさらに必要不可欠となっています。

消費者庁は、消費者・生活者の利益とは何かを第一に考え、消費者目線をもって行動する行政機関として、消費者が安心して安全で豊かな消費生活を営むことができる社会の実現に向け、消費者被害の防止、悪徳商法や不当表示の規制のための消費者安全法や景品表示法、特定商取引法等の所管する法律の厳正な執行に加えて、各種消費者行政推進のための調査・分析や情報発信、地方消費者行政の支援、個人情報保護の全般的推進等を主な業務として担っています。
このような行政上の役割を果たすため、多数の個人情報や機密情報を取扱う当庁においては、継続的かつ安定的な行政事務の実施を確保するとともに、国民の安全、安心及び信頼の下に電子政府を構築し、我が国の電子政府の基盤としてふさわしいセキュリティ水準を達成するよう、適切な情報セキュリティ対策の実施や状況変化に応じた対策実施状況の評価、見直し等、継続的に情報セキュリティ対策に取り組んでいます。

当庁では、情報セキュリティポリシーをはじめとする各種情報セキュリティ管理に関する規程類を整備・運用するとともに、管理する情報システムに対する情報セキュリティ対策の実装やその管理体制の構築等を推進してきましたが、国内外をはじめとした周辺環境における情報セキュリティに係る様々な変化をうけ、平成 24 年度は、情報セキュリティ対策の評価及び見直しを行いました。国民生活や社会経済活動の多くの面において、情報通信技術の進歩と普及に伴うＩＴ化の進展により、いまや情報システムの利活用は重要な社会基盤となり、行政機関における行政事務においても、ＩＴ化による効率化や迅速化が図られてきました。一方で、情報セキュリティにおけるリスクも多様化・高度化・複雑化し、近年においては、行政機関等を標的としたサイバー攻撃による被害が多く発生し、様々な脅威から、取り扱う情報を確実に保護するため、行政機関における情報セキュリティ対策は、さらに必要不可欠となっています。

本報告書は、平成 24 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とりまとめたものです。今後も様々なリスク・脅威への対策や職員向け教育の充実等、不断の改善努力が不可欠であることを基本認識として、当庁では、今後も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
（消費者庁次長）
松田 敏明
平成 25 年４月 26 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度は、各種情報セキュリティ管理に関する規程類について、セキュリティ動向を踏まえた見直しを実施しました。また、ｅラーニングシステムを活用した教育や、障害・事故等への対応状況を含む情報セキュリティ対策の実施状況に係る外部監査を行いました。加えて、情報セキュリティに係る障害・事故等による被害の最小化や迅速な復旧支援の実現のため、当庁内の CSRIT（Computer Security Incident Response Team）として「消費者庁情報システムに係るセキュリティインシデント対応チーム」（以下「消費者庁 CSRIT」といいます。）の体制整備を行いました。

情報セキュリティ対策の実施状況に係る自己点検の実施においては、責任者を含む当庁職員は適切に情報セキュリティ対策を実施していることが確認されました。

当庁の情報システムについては、自己点検及び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。
当庁の情報システムは、平成 25 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。

イ) 平成 25 年度の目標

当庁は、平成 25 年度の重点実施事項に係る目標を以下のとおり定め、情報セキュリティレベルの向上を目指していきます。

・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、教育資料の内容充実とその周知を行います。
・行政事務を適切に実施するため、情報資産の格付や取扱制限に従った情報管理を推進し、障害・事故等の防止に努めます。
・自己点検や外部監査を実施し、情報セキュリティ対策の適切性を客観的に評価します。
・スマートフォンやタブレット等のスマートデバイスの業務利用に伴い必要となる情報セキュリティ対策について、リスクの程度やコスト等を踏まえた検討を行います。
・情報システムの更新に向け、情報資産を確実に保護するために必要となる情報セキュリティ対策について検討します。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

平成 24 年度に実施した自己点検では、全職員を対象に実施した結果、責任者を含む全ての職員が適切な情報セキュリティ対策を実施していることを確認しました。行政事務従事者における情報セキュリティ対策の実施状況については、平成 23 年度の自己点検結果から向上しており、これは、平成 23 年度の自己点検において確認された課題事項について、情報セキュリティ教育により周知徹底を図ったことが寄与したものと思われます。

イ) 情報システムごとの状況

当庁が保有している情報システムにおける情報セキュリティ対策の実施状況は、問題ない状況です。
平成 25 年度に情報システムの更新を予定しており、必要な情報セキュリティ対策を整理し、更新後も適切に安全かつ安心な環境を維持できるよう、取り組んでいきます。

ウ）監査の状況

当庁では、平成 24 年度の情報セキュリティ監査を内部で実施するとともに、情報セキュリティに関する教育実施内容及び実施状況や、庁内行政事務実施における情報セキュリティ対策の実施状況、情報セキュリティに係る障害・事故等に係る対応体制及び対応状況等の適切性について、重点的に監査する必要がある範囲と位置付け、第三者の視点からの客観的な評価と、専門的な知見及び民間事業者を含む多様な事例に基づく効果的な改善策の策定を目的として、独立性を有する外部の監査組織に一部委託して実施しました。

監査の結果、当庁の情報セキュリティ対策は、問題なく適切に実施されていることが確認されました。

エ）教育・啓発

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を実施するとともに、ｅラーニングコンテンツを常時参照可能とし、教育内容について都度確認して情報セキュリティ対策を適切に実施できる環境を整備しています。また、理解度テストを実施し、満点獲得をもって受講完了とする運用を行い、確実な理解度向上を図っています。

また、情報セキュリティに関する関係資料についても、適宜、追加更新を行い、周知するように教育・啓発を行っています。

オ）その他取り組んだ事項

多様化・高度化・複雑化する情報セキュリティリスクから、当庁が管理する情報を保護し、被害を最小限に抑えるため、情報セキュリティインシデントに係る情報集約及び収集やインシデント発生時における緊急対応の統括、庁外機関を含む関係者との情報連携等を行う体制として、平成 24 年度に「消費者庁 CSIRT」の整備を行いました。

今後、当庁で発生する情報セキュリティインシデントに対し、消費者庁 CSIRT を中心に組織的な対応を行い、被害の最小化、迅速な復旧、効果的な再発防止策の実施等に取り組んでまいります。

C）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

情報セキュリティに関する障害・事故等の把握については、当庁が定める手順書に基づき、最高情報セキュリティ責任者及び関係する責任者等へ報告・通知を行っています。

イ）公表した障害・事故等の概要、それに対する対応等

当庁において、平成 24 年度は該当する障害・事故等は発生していません。

最高情報セキュリティアドバイザーからのメッセージ

消費者庁では、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多数取り扱うという業務特性を踏まえ、情報セキュリティポリシー及び関連する規程類の整備や、情報セキュリティ対策のための体制整備に取り組むとともに、ＰＤＣＡサイクルの手法を用いた継続的な評価及び改善に努めています。

一方で、行政機関を対象とした標的型攻撃やウェブサイトの改ざんといったサイバー攻撃が一昨年度から継続的に発生しており、多くの行政機関では「新しいタイプの攻撃」に対応するため出口対策を中心とした情報セキュリティ対策強化が必要となっています。そうした中、当庁においては、標的型攻撃が成功した際に発生することが想定される不正サイトへのアクセスの有無を定期的にチェックする等、サイバー攻撃の対象となった場合を想定した対策を平成 23 年度より実施し、安全な行政機関の実現に努めています。

平成 24 年度の自己点検において、対策の実施率、到達率がいずれも 100.0%を達成できたことは、職員に対する継続的な情報セキュリティ対策の周知徹底による結果であると考えています。また、平成 24 年度は、情報セキュリティポリシー及び関連する規程類の見直しや、障害・事故等に対する対応状況の監査など、より確実な情報セキュリティ対策の実現に向けて取り組んでまいりました。

今後は、更なる情報セキュリティの向上に向け、情報セキュリティ教育の充実や、情報セキュリティ監査の実施等について継続的に取り組んでいくとともに、他府省庁を始めとした関係機関との連携強化や、官民一体となった対策の実現に向けた検討など、より高いレベルでの情報セキュリティ対策の実現を図っていくべく、最高情報セキュリティアドバイザーとして、情報セキュリティ技術に関するアドバイスのみならず、組織としての総合的な対策・改善についても支援していく所存です。

最高情報セキュリティアドバイザー
堤 淳司
平成 25 年４月 26 日

10 復興庁

最高情報セキュリティ責任者からのメッセージ

本報告書は、平成 25 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 24 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取りまとめたものである。

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２月の発足から、迅速かつ着実に様々な取組を進めてきた。

例えば、CIO 補佐官及び最高情報セキュリティアドバイザーを任用したほか、情報セキュリティポリシーをはじめとする関連規程も整備した。さらに、情報セキュリティ対策の実施状況の自己点検や内部監査、職員に対する情報セキュリティ教育も実施するなど、必要な取組については、平成 24 年度中に、概ね措置したものと考えている。

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、平成 25 年度以降も、単に前年度の対策を踏襲するのみにとどまらず、新規で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いく。

最高情報セキュリティ責任者
復興庁統括官　　岡本　全勝
平成 25 年５月 20 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度の重点事項（各種規程等の整備及び情報セキュリティ体制の整備）については、概ね達成できた。また、自己点検については概ね問題のない結果となり、これまでの運用で特に問題が生じていないことが確認された。このほか、更なる職員教育の徹底など、今後改善すべき課題の把握も併せて実施した。

イ) 平成 25 年度の目標

各種規程の整備、体制の強化、情報セキュリティ教育の充実、格付けや取扱制限に従った情報管理の推進等に取り組み、更なる情報セキュリティレベルの向上を目指す。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

平成 24 年度の自己点検では、自己点検結果の提出率は 78.5%となった。また、対策実施率は、情報セキュリティ責任者等にあっては 100%に達し、非常に良い結果となった。一方、行政従事者については、対策実施率が 86.6%、到達率（100%）、到達率（95%）及び到達率（90%）がそれぞれ 66.9%、72.6%及び 78.3%となり、概ね問題のない結果となったが、一部に改善すべき事項も見られた。これは、当庁職員が民間企業等を含めた出向者により構成されていること、ポリシーの周知期間が極めて短かったこと等が主たる要因と考えられる。

今後は、職員への教育を充実し、ポリシーをはじめとする規程等の周知徹底を図りつつ、更なる職員教育の徹底など、今回明らかになった課題の改善に取り組むほか、必要に応じ、各種手続の見直し等も検討したい。

イ) 情報システムごとの状況

復興庁ホームページ等の情報システムは、クラウド上でのサービス提供型の運用を行っており、事業者との間で締結された SLA に則り運用している。また、毎週一回の定例会議において、事業者から情報セキュリティに係る内容を含む運用報告を受けている。

なお、自ら単独で運用する情報システムは保有しておらず、ネットワークや電子メール、グループウェア等については内閣府 LAN システムを利用しており、内閣府 LAN の利用規程に則り運用している。

ウ) 監査の状況

ポリシー及び技術基準について、NISC の協力を得て、統一管理基準及び統一技術基準との準拠性監査を実施したが、特段の問題は認められなかった。

また、庁外への情報発信を行う広報班を対象として内部監査を実施したが、特段の問題は認められなかった。

エ) 教育・啓発

情報セキュリティに関する規程等の関係資料を、全職員が参照可能な庁内イントラネット上に掲示し、常時閲覧できる環境を整備している。また、各資料は必要に応じ追加・更新を行い、職員への周知を図っている。

オ）その他取り組んだ事項

不審メールの大半がフリーメールから送信されていることに着目し、インターネットから送信されるメールを振り分ける運用を行い、職員の注意を喚起することにより、セキュリティ事故の抑制を図っている。

C) 情報セキュリティに関する障害・事故報告

平成 24 年度は、報告すべき情報セキュリティに関する障害・事故等は発生していない。平成 25 年度以降も、無障害・無事故を継続すべく、引き続き適切な情報セキュリティ対策の実施に努めていく。

最高情報セキュリティアドバイザーからのメッセージ

情報システム技術が進歩していく中、社会の情報システムへの依存度が高まっている。復興庁においても、被災地の一刻も早い復興を目指し、クラウドサービス等情報技術のサービスを利用し情報を発信してきたところ。

復興庁では、本年度はセキュリティポリシー等の規程類の整備を第一に取り組み、ITBCP に係る緊急連絡網の整備を含め、最低限の対応はできたと考える。また、自己点検及びセキュリティ教育に十分な時間がかけられなかった反面、自己点検結果の提出率は 78.5%に上り、対策実施率についても、情報セキュリティ責任者等にあっては 100%に達するなど、非常に良い結果であった。また、行政従事者については、対策実施率が 86.6%、到達率(100%)、到達率（95%）及び到達率（90%）がそれぞれ 66.9%、72.6%及び 78.3%となった。この結果は、短期の実施期間や、規模に照らして出先機関が多い組織特性に鑑みれば概ね問題ないものと考える。

復興庁では、秘匿性の高い情報等を多数取り扱う場合がある一方、復興関連の業務も今後更なる増加が見込まれ、適切な情報セキュリティ対策の実施とその管理は欠かせないものとなっている。今後は、情報セキュリティに係る監査や、関連規程類の見直し更新を適切に行うほか、情報セキュリティ教育等にもさらに注力していく。

最高情報セキュリティアドバイザーとしては、情報セキュリティ対策の充実に向け、情報セキュリティに関するアドバイスのみならず、システムの在り方等も視野に入れて支援していく所存。

最高情報セキュリティアドバイザー
澤田　滋
平成 25 年 5 月 20 日

11 総務省

最高情報セキュリティ責任者からのメッセージ

近年の情報通信技術の急速な進展に伴い、情報システムの利活用が進む一方で、不正アクセスやウイルス感染による情報漏えいといった脅威も増大しています。

政府機関等に対するサイバー攻撃が引き続き確認される中、総務省においては、平成 24 年度は、以下の情報セキュリティ対策を重点的に行いました。

(1) 職員による不審なメールへの適切な対応の強化等
(2) 公開用ウェブサーバの対策状況の監査

(1) については、職員に対し、不審なメールへの適切な対応についての注意喚起、最新の脅威に即した不審なメールへの適切な対応に関する訓練及び不審メール情報の共有を実施しました。また、ホームページ閲覧によるウイルス感染の脅威が増していることを踏まえた注意喚起も行いました。
(2) については、外部に公開しているすべ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、脆弱性への対応がすべて完了するまでフォローアップを実施しました。

総務省は、情報通信、行政の情報化等を所管する省として、平成 25 年度においても、情報通信技術の最新の動向等を踏まえるとともに、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。

最高情報セキュリティ責任者
（総務省大臣官房長）
門山　泰明

平成 25 年 6 月 7 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度は、以下の情報セキュリティ対策を重点的に行った。

・職員による不審なメールへの適切な対応の強化等

職員に対し、不審なメールへの適切な対応についての注意喚起、最新の脅威に即した不審なメールへの適切な対応に関する訓練及び不審メール情報の共有を実施した。また、ホームページ閲覧によるウイルス感染の脅威が増していることを踏まえた注意喚起も行った。

・公開用ウェブサーバの対策状況の監査

外部に公開しているすべ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、脆弱性への対応がすべて完了するまでフォローアップを実施した。

イ) 平成 25 年度の目標

情報通信技術の最新の動向等を踏まえるとともに、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る。

特に、(1) 総務省情報セキュリティポリシー等の見直し、(2) 情報セキュリティに関する教育及び自己点検、(3) 最新の脅威を踏まえた職員への訓練・情報提供等、(4) 最新の攻撃手法を踏まえた情報セキュリティ監査、に重点的に取り組む。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

総務省における情報セキュリティ対策の基本方針及び情報セキュリティ対策基準である情報セキュリティポリシー等についての理解を促進し、情報セキュリティ対策を着実に実施することを目的として、情報セキュリティに関する教育を実施した上で、情報セキュリティ対策の実施状況を確認することを目的として、情報セキュリティ対策の自己点検を実施した。

自己点検の結果、総務省においては、求められる情報セキュリティ対策がおおむね実施されていることが確認された。しかしながら、社会全体で情報セキュリティ対策の必要性が高まる中、今後も、情報セキュリティに関する教材の改善を図り、職員の情報セキュリティ対策についての理解を促し、対策が着実に実施されるよう努める。

イ) 情報システムごとの状況

総務省における情報システムの情報セキュリティ対策の実施状況を確認し、十分な対策が取られていない情報システムに改善を促すことをもって情報セキュリティ対策の向上を図ることを目的として、情報システムに対する検査を実施した。

検査の結果、総務省においては、求められる情報セキュリティ対策がおおむね実施されていることが確認された。今後もこの状態を維持するため、引き続き適切な情報セキュリティ対策の実施に努める。

ウ) 監査の状況

省内の情報セキュリティ対策の改善に資することを目的として、以下の情報セキュリティ監査を実施した。

・総務省情報セキュリティポリシーの政府機関統一基準群への準拠性監査

・実施手順書の総務省情報セキュリティポリシーへの準拠性監査

・自己点検の適正性監査
・例外措置の申請の監査
・主要な情報システムの運用に関する監査
・公開用ウェブサーバの対策状況の監査

監査の結果、総務省においては、一部の公開用ウェブサーバにおいて脆弱性が検出されたほかは、全体として重大な指摘事項はなく、適切に情報セキュリティ対策が実施されていることが確認された。なお、脆弱性の検出状況ついては、推奨する対策等とともに担当者に通知し、ぜい弱性への対応がすべて完了するまでフォローアップを実施した。

今後もこの状態を維持するため、引き続き適切な情報セキュリティ対策の実施に努める。

エ）教育・啓発

職員に対してセキュリティ情報を提供し、情報セキュリティ対策の適切な実施を促すことを目的として、ぜい弱性情報及び注意喚起（ウイルスについての警告、ソフトウェアの更新指示等）等の省内周知、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及びイントラネットにおける情報セキュリティに関連する情報発信を実施した。なお、最高情報セキュリティアドバイザーによる研修は、対象を拡大し、職員に対する一層の啓発に努めた。

オ）その他取り組んだ事項

(1) 情報システム調達におけるセキュリティ対策

情報システムの開発等の業務を外部に委託して実施する際には、総務省が求める情報セキュリティの水準が、委託先においても確保される必要がある。

このことから、情報システムの調達等における情報セキュリティ対策手順書を作成し、調達仕様に記載する情報セキュリティ対策等や情報保護・管理要領等の記載例を示すことにより、必要な情報セキュリティ水準の確保を図っているほか、調達に当たってＣＩＯ補佐官への相談会を開催し、情報セキュリティ要件を含む調達仕様書案等の妥当性確認を行っている。

(2) 職員による不審なメールへの適切な対応の強化

特定の組織を標的にしてウイルスメールを送付する攻撃によるウイルス感染を防止するためには、職員一人一人が、攻撃の対象となり得ることを認識し、不審なメールへの適切な対応を身に付ける必要がある。このことから、不審なメールへの適切な対応についての注意喚起、最新の脅威に即した不審なメールへの適切な対応に関する訓練及び不審メール情報の共有を実施した。

(3) 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

ホームページ閲覧によるウイルス感染の脅威が増していることを踏まえ、細心の注意を払ってホームページを閲覧するよう注意喚起を行った。

(4) CSIRT の構築

総務省における障害・事故等への対応を行うため、平成 14 年 7 月以降、順次、CSIRT（Computer Security Incident Response Team）の整備を進めた。CSIRT は、大臣官房企画課長を体制の責任者、大臣官房企画課情報システム室を担当課とし、情報セキュリティ専門家を含む体制として整備している。CSIRT においては、障害・事故等の未然防止策の実施のほか、障害・事故等発生時の早期発見、適切な状況把握、原因分析、被害拡大防止、情報セキュリティ強化等の実施に取り組んでいる。

C) 情報セキュリティに関する障害・事故報告

○ホームページの閲覧障害

平成 24 年 9 月、総務省統計局ホームページにおいて、閲覧がしにくい状況が断続的に発生した。ホームページへのアクセスが短時間に集中したことが、本事象の原因と考えられる。

最高情報セキュリティアドバイザーからのメッセージ

情報セキュリティへの関心が高まる中、総務省においては、変化し続ける攻撃手法に対応するために、各種情報の収集や対策の強化に努めています。

本年度は、最高情報セキュリティアドバイザーとして、防御・検知・対処の対策をバランスよく実現するべきとアドバイスをしました。標的型攻撃を始めとするサイバー攻撃は、常に攻撃手法が変化しており、その情報の収集と対策の具体的な方針を示すことが総務省の情報セキュリティを守る上で重要となっています。

また、本年度もシステムの設計、開発、構築、運用等の調達における CIO 補佐官相談会において、セキュリティの見地から各種アドバイスを行いました。脅威が変化している中、セキュリティ対策も従来の考え方だけでなく、新しい脅威への対策も盛り込めるように推奨しています。

そして、新入職員や新任職員の方等にセキュリティに関する研修を通じて、サイバー攻撃に関する注意喚起を行うことができました。システムを扱う各職員の注意が、サイバー攻撃の被害の最小化に欠かせないと考えています。

今後もサイバー攻撃の脅威は増大していくものと思われ、攻撃手法も変化を続けていくものと考えられます。したがって、情報収集や体制の整備を引き続き行っていくことが必要と考えています。

最高情報セキュリティアドバイザー　三輪　信雄
平成 25 年 6 月 7 日

12 法務省

最高情報セキュリティ責任者からのメッセージ

法務省では，基本法制の維持及び整備，法秩序の維持，国民の権利擁護，国の利害に関係のある争訟の統一的かつ適正な処理並びに出入国の公正な管理といった任務を全うするため，国民の資産・財産情報である登記情報，国民生活の安全・安心に欠かせない刑事関連情報，適正な出入国管理を行うための情報等の電子化を進めるとともに，情報セキュリティの維持を図りながら，行政サービスの質の向上や業務の最適化・効率化に努めてまいりました。

平成２４年度は，政府機関等のウェブサイトの改ざん又はアクセス集中によるサービス妨害といった被害が発生したことや，標的型攻撃による情報の窃取事案等が発生したことについて，大きく取り沙汰された一年になりました。最近では，遠隔操作ウイルスによる犯罪，スマートフォンを狙ったマルウェアの激増，サイバー空間の防衛等といったニュースを目にする機会も増え，社会的関心の高まりを感じています。

幸いにも，平成２４年度には，法務省の保有する情報システムがサイバー攻撃を受けて機密情報等が漏えいするといった事態は発生しませんでしたが，個人情報の誤掲載や個人情報の盗難といった障害が３件発生しました。いずれも情報が悪用されたという事実には接していませんが，万一，法務省の保有する情報が漏えい等した場合には，平穏な市民生活や円滑な経済活動を脅かす事態を招くおそれがあるということを深く反省し，より一層，情報セキュリティ対策の推進を図り，障害を発生させない最善の努力を尽くすとともに，「事故前提社会」といわれている現状認識の下，障害が発生した場合であっても，迅速かつ的確に対応できるよう職員の教育又は訓練に積極的に取り組んでまいります。

平成２５年４月２６日
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

A) 平成 24 年度の総括

ア）平成 24 年度の評価

ア　省庁基準の見直し

平成２３年度に，「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」（平成１７年９月１５日情報セキュリティ政策会議決定）が廃止され，新たに「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）が策定されたこと等を受けて，ますます多様化・高度化・複雑化する脅威に対応するため，平成２４年９月に，「法務省情報セキュリティ対策基準」を廃止して，新たに「法務省における情報セキュリティ対策の基本方針」及び「情報取扱基準」ほか６件の対策基準（以下これらを総称して「法務省基準」という。）を制定しました。

イ　情報取扱区域のクラス分け

情報取扱区域を，それぞれの区域に設置する機器等の重要度，それぞれの区域で取り扱う情報の重要度，それぞれの区域に講じられた対策の強度等に応じて，クラス０から３までの４段階に区分しました。

ウ　標的型攻撃に対する対応

(ｱ)　インターネットからのメールを受ける情報システムに送信元を確認する仕組（送信ドメイン認証技術）を導入しました。

(ｲ)　不正プログラムに感染するおそれがあるウェブサイトや過去に不正プログラムの配布先として登録されたウェブサイトへの通信を制御しました。

以上のような情報システムの対策に加えて，外部事業者に委託して，法務本省に勤務する職員に対する「標的型攻撃メールの対応訓練」を実施しました。

エ　法務省ＣＳＩＲＴの設置

情報セキュリティに関する障害が発生した場合の対応組織（以下「法務省ＣＳＩＲＴ」という。）を設置するとともに，法務省ＣＳＩＲＴへの報告を含めた「障害対応要領」を制定して，平成２５年２月１日から運用を開始しました。

イ）平成 25 年度の目標

ア　巧妙化する標的型攻撃の脅威から法務省の保有する情報及び情報システムを保護するため，平成２５年度も標的型攻撃メールの対応訓練を実施して，職員の教育に努めます。

イ　障害が発生した場合の対応能力を強化するため，法務省ＣＳＩＲＴを中心とした教育及び訓練を実施するとともに，ＣＩＳＯのガバナンス強化に取り組み，限られた人員，予算の中で，最大の効果が得られるよう，守るべき対象の重要度に応じた適切な情報セキュリティ対策を講じます。

ウ　客観性・独立性が確保された外部専門家による監査の拡大・充実を図り，情報セキュリティ対策の実施状況等の評価に結び付けます。

エ　情報システムの運用管理を担当する職員のスキルの確認及び情報セキュリティ意識の向上を図るため，情報システムの対策実施状況等に関するヒアリングを実施します。

B) 情報セキュリティ対策の実施状況

ア）省庁対策基準に関する自己点検結果

本省部局等単位で法務省基準に準拠した運用を行っているか，行政事務従事者自らが自己点検を実施しました。

平成２４年度は，内閣官房情報セキュリティセンターが策定した自己点検票を活用するとともに，自らに課せられた情報セキュリティ対策（遵守事項）を確認させて，自己点検の理解を深めさせるため，事前確認問題も配布しました。この事前確認問題は，平

成２５年度以降も引き続き活用し，情報セキュリティ対策の自己点検の充実を図ります。
なお，平成２３年度に引き続き，自己点検結果の正確性を確認するために地方官署に勤務する職員の自己点検に関する監査を実施しました。この取組は，継続して実施していきます。

イ）情報システムごとの状況

内閣官房情報セキュリティセンターの依頼に基づき，平成２４年１２月１日時点のウェブサーバ（公開用）及びメールサーバの情報セキュリティ対策の実施状況について検査しました。

検査項目及び検査結果は，次のとおりです。

(1) ウェブサーバ（公開用）

ア 検査項目

(ｱ) サーバの保有台数の調査

(ｲ) サーバの運用に関する検査／調査

ＨＴＴＰＳ（暗号化）通信を行うサーバにおける脆弱性に関する調査，大量のパケット送信型のサービス不能攻撃への対策の状況，ＯＳの最新化の状況

イ 検査結果（実施率）

１００％（実施台数／全体の台数）

(2) メールサーバ

ア 検査項目

(ｱ) サーバの保有台数の調査

(ｲ) サーバの運用に関する検査／調査

ＯＳの最新化の状況

イ 検査結果（実施率）

１００％（実施台数／全体の台数）

(3) 総評

全てのウェブサーバ（公開用）及びメールサーバについて，情報セキュリティ対策が適切に講じられていることが確認されました。引き続き，高いレベルで情報セキュリティ水準を維持できるよう努めてまいります。

メールサーバについては，送信メールの機密性又は完全性が侵害されない対策を講じるほか，踏み台にされて標的型攻撃に悪用されることのないよう，高いレベルで情報セキュリティ水準を維持できるよう努めてまいります。

ウ）監査の状況

(1) 監査の概要

内閣官房情報セキュリティセンターが指定する監査項目を盛り込んだ監査計画書（情報セキュリティ監査責任者が策定し，最高情報セキュリティ責任者が承認）に基づき，監査を実施しました。

平成２４年度に実施した監査は次のとおりです。

(2) 監査事項

ア 関係規程の準拠性監査

(ｱ) 統一基準群と法務省基準の準拠性の監査

(ｲ) 法務省基準と情報セキュリティ関係規程の準拠性の監査

イ 自己点検に関する監査

(ｱ) 情報セキュリティ管理体制に関する監査

(ｲ) 執務室における情報セキュリティ対策の実施状況に関する監査

(ｳ) 情報システムに対する情報セキュリティ対策の実施状況に関する監査

ウ その他の監査

(ｱ) 例外措置の適用審査結果記録の整備状況監査

(ｲ) 情報システムの脆弱性監査（外部委託事業者）

(3) 監査結果等

監査の結果全般としては，緊急に改善する必要のある事実は認められず，おおむね適正に運用されているとの結果報告を受けました。

平成２４年度は，情報システムの運用管理を担当する職員のスキルの確認及び情報セキュリティ意識の向上を図るため，情報システムに対する情報セキュリティ対策の実施状況に関する監査として，重点検査の対象となった情報システム（ウェブサーバ（公開用）及びメールサーバ）について，その運用状況等のヒアリングを実施しました。平成２５年度もこの取組を継続していきたいと考えています。

エ）教育・啓発

法務省では，毎年，企画担当情報セキュリティ責任者が「年度教育計画」を企画・立案して情報セキュリティ対策の教育を実施しており，平成２４年度は，「全職員用」，「情報システムセキュリティ責任者用」及び「課室等情報セキュリティ責任者用」のテキストをそれぞれ整備して，役割に応じた情報セキュリティ対策の教育を実施しました。

実施した情報セキュリティ対策の教育の概要は，次のとおりです。

(1) 教育の目的

法務省基準に規定されている行政事務従事者の遵守事項を再確認させることにより，行政事務における情報の適正な取扱いの徹底を図り，もって，法務省内の情報セキュリティ対策水準の維持・向上に努める。

(2) 教育資料の整備

ア テキスト（教育教材）

イ 参考資料（教育教材を補足する詳細な資料）

ウ 理解度チェックシート（教育効果を確認するための資料）

(3) 実施期間

平成２４年６月１５日から平成２５年２月４日まで

(4) 教育担当者

本省情報セキュリティ責任者又は情報セキュリティ責任者が指名する者

(5) 教育受講状況の管理

本省情報セキュリティ責任者は，本省部局等単位で教育の受講状況を取りまとめ，企画担当情報セキュリティ責任者に報告します。当該報告を受けた企画担当情報セキュリティ責任者は，法務省全体の受講状況を把握・整理した上で，最高情報セキュリティ責任者及び法務省情報セキュリティ委員会に報告します。

なお，平成２４年度における受講状況は，約９８％であり，正当な理由なく情報セキュリティ教育を受講していない行政事務従事者はいませんでした。

(6) 教育の効果測定

受講者の理解度，情報セキュリティ対策の浸透度を測るため，平成２３年度に引き続き，質問形式のチェックシートを配布し，教育効果の把握に努めました。

C）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

「情報セキュリティ２０１２」（平成２４年７月４日情報セキュリティ政策会議決定）において，各府省庁に情報セキュリティインシデントに関する緊急時対応の機能を有した専門的部隊（ＣＳＩＲＴ:Computer Security Incident Response Team）を組織して，専門的・実務的な情報共有を図ることが定められたことを受け，既存の「障害対応要領」の見直しを行い，情報セキュリティに関する障害が発生した場合の報告手順及び対応手順を新たに制定するとともに，「法務省における情報セキュリティに関する障害の対応組織設置要綱」を定めて，平成２５年２月１日から「法務省ＣＳＩＲＴ」の運用を開始しました。

イ）公表した障害・事故等の概要、それに対する対応等

平成２４年度は３件の情報セキュリティに関する障害が発生しました。いずれも情報が悪用された事実は確認されていませんが，障害を発生させたことについて深く反省し，法務行政の信頼回復に努めてまいります。

障害を発生させた機関においては，既に再発防止策を講じていますが，省内においても同種同様の事案を発生させないよう，情報の共有を図り，再発防止に努めていきたいと考えます。

以下は３件の事案概要等になります。

(1)　１件目

ア　概要

平成２４年５月，リサイクルショップで購入したワープロ内部に，法務省において作成したと思われる個人情報を含む職務上の情報が残存しているとの情報提供があったもの。

イ　原因

ワープロの所有者であった職員が，職務上の情報がワープロ内部に残存しているか否かを確認しないまま，リサイクルショップにワープロを売却し，適切な廃棄がなされなかったため。

ウ　障害の対応状況

職員が情報提供者の自宅に赴き，ワープロ内部の情報が確実に削除されたことを確認し，事案を公表した。

エ　再発防止策

職員研修の実施を指示し，所管各庁に対して，注意喚起文書を発出した。

(2)　２件目

ア　概要

平成２４年６月，ホームページに掲載されたファイルに，個人情報が記載された文書が添付されているとの情報提供があったもの。

イ　原因

ホームページに掲載するファイルは末尾まで内容及び枚数を確認又は精査すべきところ，十分な確認をしないまま，掲載してしまったため。

ウ　障害の対応状況

(ｱ)　情報提供に基づき，内容を確認後，直ちに当該ファイルの閲覧を停止し，事案を公表した。

(ｲ)　ホームページに謝罪及び削除依頼の文書を掲載し，国立国会図書館に対し，当該ファイルの利用制限の申出を行った。

エ　再発防止策

(ｱ)　個人情報の管理について注意喚起するとともに，スキャナーでＰＤＦ化する際や，ホームページに掲載する情報を作成する際の確認を徹底するよう指示した。

(ｲ)　職務研究会及び職員全体研修を実施して再発防止を徹底し，所管各庁に対して，注意喚起文書を発出した。

(3)　３件目

ア　概要

平成２５年１月，地下鉄内で個人情報が保存されたＵＳＢメモリと個人情報が記載された書面が入った鞄の盗難に遭ったもの。

イ　原因

個人情報を庁舎外で所持する際に必要とされる重大な保管責任と細心の注意を払う意識が欠けていたため。

ウ　障害の対応状況

(ｱ)　地下鉄の忘れ物センター等に照会し，警察署に被害届を提出して，事案を公表した。

(ｲ)　紛失した情報がインターネット上に流出していないか一定の期間確認を行った。

エ　再発防止策

所管各庁に対して，注意喚起文書を発出した。

最高情報セキュリティアドバイザーからのメッセージ

平成２３年度に地方官署まで拡大した自己点検に関する監査は，平成２４年度も引き続き実施することができ，法務省全体の取組として省内に浸透してきたものと評価しています。

また，平成２４年度は，情報システムの情報セキュリティ対策の実施状況に関する監査として，情報システムの運用管理業務に携わる職員に対するヒアリングを実施しました。情報システムのセキュリティを維持するためには，情報システムの運用管理体制を充実させる必要があり，特に昨今の情報セキュリティを取り巻く環境の変化等を考慮すれば，いつ情報システムに障害が発生しても不思議ではありませんので，情報システムを運用管理する職員の危機意識の向上や外部事業者を監督する能力等の向上が欠かせません。引き続き，情報システムの運用管理業務に携わる職員のスキルの確認及び情報セキュリティ意識の向上を図り，情報システムを運用管理する体制の充実・強化に取り組んで行きたいと考えます。

平成２４年度は，情報セキュリティインシデント緊急支援チーム（ＣＹＭＡＴ）における教育及び訓練等が開始されました。法務省においては，法務省ＣＳＩＲＴを設置して，障害発生時の報告手順や対応手順の見直しも行いましたが，法務省ＣＳＩＲＴの運用を軌道に乗せるためには，法務省ＣＳＩＲＴの構成員であるＣＹＭＡＴ要員の育成や法務省ＣＳＩＲＴの庶務との連絡調整を行う職員の育成，情報セキュリティに関する知識の習得及び対応能力の強化等が欠かせません。法務省ＣＳＩＲＴは，情報セキュリティに関する障害が発生した場合におけるレスポンスチームという位置付けですが，平常時における連絡訓練や想定訓練等を実施して，緊急時の対応の強化につなげていきたいと考えています。

平成２４年度は３件の情報セキュリティに関する障害が発生しており，いずれも，職員の不注意や気の緩みといったことに端を発する事案でした。法務省の組織規模又は組織構成及び取り扱う情報の性質等を考慮すれば，情報セキュリティガバナンスをより一層強化していく必要があると考えていますので，職員による情報の取扱いの徹底を図っていきたいと考えています。

平成２５年４月２６日
最高情報セキュリティアドバイザー
大 成 宣 行

13 外務省

最高情報セキュリティ責任者からのメッセージ

平成２４年度においては、いわゆる標的型メール攻撃(※1)やＤＤｏＳ攻撃(※2)等が頻発し、政府関係機関や民間会社の被害が多数報告されました。特に、特定の組織や個人を狙う標的型メール攻撃については、益々巧妙化しており、ウィルスに感染してもウィルス対策ソフトによる検知が困難になってきています。このような中、当省においても、省内のインターネットに接続されたパソコンから外部へ情報が流出した疑いがある事案が発生いたしました。当省では、平成２４年度の情報ネットワークの最適化の完了により、本省及び在外公館に対する情報セキュリティ対策を、本省で一元的に効率よく行えるようにしました。また、職員一人ひとりがウィルス感染や情報漏洩を起こさないよう、今まで以上に認識し、心掛ける必要があります。そのため、昨年度に引き続き、ｅラーニングによる研修、自己点検による情報セキュリティ対策状況の確認、加えてＮＩＳＣ主催の標的型メール攻撃訓練への全省的な参加等を実施しました。

また、スマートフォンは昨今急速に普及しており、業務への利用が広がっていることを背景として、スマートフォンを狙ったウィルスも急増していることから、当省においても安全な利用のための利用規則の整備をすすめています。

当省内におけるＣＳＩＲＴ（ＧＩＳＩＲＴと呼称）(※3)については、平成２３年２月に体制整備を行い、平成２４年度においては、関係職員への研修や演習を実施し、本体制の意識向上を図りました。

以上、これら取組により、当省における情報セキュリティに関する知識や意識の一層の向上をはかるとともに、今後とも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
平成２５年４月２５日

(※1) 標的型メール攻撃：情報窃取のためのメールを利用したサイバー攻撃
(※2) ＤＤｏＳ攻撃：インターネットサイトへのアクセス障害を企てた攻撃
(※3) ＣＳＩＲＴ：Computer Security Incident Response Team
ＧＩＳＩＲＴ：Gaimusho Information Security Incident Response Team

A) 平成 24 年度の総括

ア）平成 24 年度の評価

平成２４年度における情報セキュリティ対策の取組としては、ＣＳＩＲＴ（ＧＩＳＩＲＴ）体制の充実、省員の意識啓発並びに情報ネットワーク最適化を行い、以下のとおり、着実に対策が実施されつつあることを認識しております。

ア　情報ネットワーク最適化により、本省及び在外公館に対する情報セキュリティ対策を、本省で一元的に行うことができるようになり、より迅速な対策の実施が可能となりました。

イ　平成２４年度の重点的な計画であるＣＳＩＲＴ（ＧＩＳＩＲＴ）体制の充実ならびに意識啓発につきましては、引き続き、説明会や演習を実施した結果、更なる意識向上が図られました。

ウ　職員への意識啓発のための取組として、ｅラーニングによる情報セキュリティ対策の習得等に努力してきました。更に、情報セキュリティ対策自己点検を本省と全在外公館の職員とシステムを対象に実施し、高い実施率を達成するとともに、標的型メール攻撃訓練へも本省及び１４４在外公館の職員が参加し、標的型メールに対する職員の認識向上を確認しました。また､その他様々な機会を通じて、本省及び在外公館の職員に対し情報セキュリティ意識の向上に努めました。

エ　スマートフォン及びタブレット端末のセキュリティ対策の取組として､省内ホームページや研修会の機会を通じて､セキュリティ対策について周知等を行うことにより職員の意識向上を図りました。さらに、安全に利用するための利用規則の整備やシステム上の対策を進めています。

イ）平成 25 年度の目標

平成２５年度の情報セキュリティ対策については、基本的な対策に加え、今後益々増えることが予想される標的型メール攻撃への全職員への一層の意識啓発を図ります。また、当省内のＣＳＩＲＴ（ＧＩＳＩＲＴ）体制の充実のため、特に演習及び訓練の機会を増やすと共に、演習結果を踏まえた、インシデントレスポンスのためのマニュアルの整備を図ります。

B) 情報セキュリティ対策の実施状況

ア）省庁対策基準に関する自己点検結果

自己点検開始以来１００％達成を継続している把握率(※1)については、平成２４年度においても、職員に対し電子的な自己点検実施の機会を拡大するなどの工夫を行い、その維持に努めました。また、実施率(※2)については情報セキュリティ責任者等及び情報システムに関わる情報システムセキュリティ責任者等については１００％となっていますが、行政事務従事者についてはわずかに１００％達成に至らず、ｅラーニング等を活用し、職員の教育受講機会の拡大に努めることとします。

（※１）把握率：自己点検対象者を母数に、実際に自己点検を実施した割合です

（※２）実施率：自己点検を実施した者のうち対策を「実施」と回答した者の割合です。

イ）情報システムごとの状況

政府統一基準群に準拠した情報セキュリティ対策が実施されているかを確認するために、ＮＩＳＣの調査票を元に毎年実施している調査では、当省は、平成１９年度からすべての調査対象について実施率１００％を達成しています。

平成２４年度の調査においても１００％を達成しました。

今後も引き続き１００％を達成するよう政府統一基準群に基づく情報セキュリティ対策を実施していく予定です。

ウ）監査の状況

平成２４年度においては、自己点検に関する監査、ＤＮＳサーバの脆弱性監査、公開ウェブサーバの脆弱性監査及び例外措置の申請及び許可状況に関する監査を行い、各監査項目において問題の無いことを確認しました。

エ）教育・啓発

外務省では、職員の情報セキュリティ意識の向上を図るために、年度当初に「情報セキュリティ対策教育計画」を策定しています。

各種集合研修における教育、ｅラーニング、情報セキュリティ関連情報の収集と職員への提供、ＣＩＯ補佐官による情報提供等により、職員に年一回以上の情報セキュリティ教育の受講機会を提供しています。また様々な機会を通じて、最新の情報セキュリティに関する情報の共有に努めています。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

外務省においては、障害・事故等を発見した職員は、「情報セキュリティ責任者」又は「情報システムセキュリティ責任者」に対して報告し、報告を受けた情報セキュリティ責任者又は情報システムセキュリティ責任者は必要に応じて統括情報セキュリティ責任者へ報告することを「外務省情報セキュリティポリシー」にて定め、職員への周知・教育を実施するとともに、統括情報セキュリティ責任者は、重要な情報システムについて、その情報システムセキュリティ責任者及び情報システム取扱責任者の緊急連絡網の整備を指示しています。

統括情報セキュリティ責任者が受領した報告については、必要に応じて最高情報セキュリティ責任者へ報告します。

イ）公表した障害・事故等の概要、それに対する対応等

平成２５年１月２８日、内閣官房情報セキュリティセンター（ＮＩＳＣ）からの情報提供を受け、当省で調査を行ったところ、当省のパソコンからインターネット上の外部サーバへの不審な通信が確認され、同パソコンから約２０通の文書の流出の疑いがあることが判明しました。当省としては、上記事実を受け、直ちに当該外部サーバへの情報流出を防止する処置を実施するとともに、外部専門家を交え、当該情報流出の詳細を分析しています。今回の事案は、秘密文書を扱わないオープンＬＡＮ（インターネットに接続されたネットワーク）におけるものであり、流出した疑いがある文書の機密指定はいずれも「秘」に当たらないもの（機密性２以下）です。今後とも情報流出の防止に努めるとともに、情報セキュリティ対策の徹底に万全を期していくこととします。

最高情報セキュリティアドバイザーからのメッセージ

平成２４年度もサイバー攻撃手法の一層の進化・複合化が進み、ソーシャル・エンジニアリングの要素を色濃く反映した標的型攻撃が政府機関や企業に対して仕掛けられ、国際的に見ても、まさにサイバー戦争の幕開けを予感させる年となっています。ＣＩＳＯのメッセージにもあるように、当省においても、情報流出事案が発生し、職員一人ひとりが情報セキュリティに対する取り組みを強化してゆく必要性がますます高くなってきています。

昨年も述べたとおり、攻撃手法や標的の変化に対しては、従来の侵入防止に主眼を置いた防御策だけでは対応できず、侵入を前提とした多重防御や不審な通信の監視や遮断といった出口対策が必要となっています。出口対策を有効なものとするためにも、職員各位の意識の向上が欠かせないものとなっています。

特に、当省は在外公館が全世界に点在しており、各公館が直接攻撃にさらされるという構造的な特徴をもっています。そのため、定期的な教育・訓練を行い、攻撃を受けた際の対応を日常的に意識しておくことが重要であると考えます。今後も攻撃を受けること、侵入されることを前提とし、侵入があっても被害を極小化する技術的対策や組織的な対応策の検討を継続していただきたい。

外務省最高情報セキュリティアドバイザー
山岸　篤弘
松井　充

14 財務省

最高情報セキュリティ責任者からのメッセージ

近年、情報通信技術の進歩により情報システムの利便性が高まる一方、標的型メール攻撃に象徴されるようにウイルス感染や不正アクセスによる情報漏えい等のリスクが増大しています。そのため、機密性が高い行政情報や個人情報、また、国民の生活に密接に関係し改ざんや紛失が許されない情報を取り扱う政府機関においては、情報システムの開発・運営や日々の事務の実施の中で情報セキュリティ対策を適切に講じることが求められております。

このような中、政府としては、平成 22 年 12 月、各府省庁の最高情報セキュリティ責任者（CISO：Chief Information Security Officer）が一堂に会する「情報セキュリティ対策推進会議（CISO 等連絡会議）」において、各府省庁の CISO 等の連携の下、政府における情報セキュリティ対策の推進を図ることとなりました。また、平成 23 年度は、政府機関や防衛産業など国の重要な情報を扱う民間企業に対する標的型メール攻撃が発生したことを受けて、政府において標的型メール攻撃に関する訓練が実施されたほか、CISO 等連絡会議に「官民連携の強化のための分科会」が設置され、情報セキュリティ対策における官民連携の強化策について検討が行われました。

財務省としても、政府全体の取り組みを踏まえ、情報セキュリティに不測の事態が生じないよう、積極的に取り組んでまいりましたが、平成 24 年度は、サイバー攻撃によるセキュリティ事案が判明するなどの事態が発生しました。これらの事態を重く受け止め、保存文書の暗号化等の対策を講ずるとともに、情報セキュリティ・インシデントに対処するためのチーム（CSIRT：Computer Security Incidents Response Team）の設置等体制を整備するなど、情報セキュリティ対策について、関係機関ともより緊密に連携しつつ、一層の強化を図りました。

平成 25 年度も、引き続き内閣官房情報セキュリティセンター（NISC：National Information Security Center）等の関係機関との連携を緊密に図りながら、業務で扱う情報の機密性の要求度等に応じた対策の強化に取り組み、従来実施してきた定型的な業務の合理化を行いつつ、メリハリをもった対策を実施してまいります。

財務省最高情報セキュリティ責任者
（財務省大臣官房長）
香川 俊介

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

財務省では、政府全体の取り組みを踏まえ、情報セキュリティに不測の事態が生じないよう、積極的に取り組んでまいりましたが、平成 24 年度に、サイバー攻撃によるセキュリティ事案が判明するなどの事態が発生しました。

これらの事態を受け、保存文書の暗号化等の対策を講じたほか、障害・事故等に適切かつ迅速に対応できるよう、関係する規程の見直しを行い、サイバー攻撃等が発生した際、機動的に対応するため CSIRT の設置等の体制を整備しました。

また、関係機関との連携も緊密に図りながら、情報セキュリティ対策の一層の強化に取り組んでまいりました。

イ) 平成 25 年度の目標

平成 25 年 1 月に開催された、第 9 回 CISO 等連絡会議において議題となった「情報の機密性の要求度等に応じたセキュリティ対策の重点強化」に沿って、内閣官房情報セキュリティセンター（NISC）等の関係機関との連携を緊密に図りながら、業務で扱う情報の機密性の要求度等に応じた対策の強化に取り組み、従来実施してきた定型的な業務の合理化を行いつつ、メリハリをもった対策を実施してまいります。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

財務省では、情報セキュリティ対策基準に基づき、財務省の職員に対して、情報セキュリティ対策基準等の遵守事項の実施状況について、行政事務従事者が自ら確認する「自己点検」を実施しています。

平成 24 年度の自己点検は、財務省のすべての職員を対象として実施しました。また、情報セキュリティ責任者等については、それぞれの職責に応じた遵守事項が適正に実施されているか確認する自己点検も実施しました。

点検の結果、情報システムの利用方法や情報の取り扱いに関する一部の遵守事項の実施について、十分ではないところが認められたため、遵守事項が適正に実施されるよう、引き続き職員の教育強化等に取り組んでまいります。

イ) 情報システムごとの状況

財務省では、政府全体の取り組みを踏まえ、情報セキュリティに不測の事態が生じないよう、不審メールに関する対策や内閣官房情報セキュリティセンター（NISC）による公開ウェブサーバの脆弱性検査の結果に基づき対策を実施するなど、積極的に情報システムの対策に取り組んでまいりました。

しかしながら、平成 24 年度に、サイバー攻撃によるセキュリティ事案が判明するなどの事態が発生したことから、情報セキュリティ対策の一層の強化に取り組んでまいりました（詳細については、以下「 C) イ) 公表した障害・事故等の概要、それに対する対応等」参照。）。

ウ) 監査の状況

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）又は最高情報セキュリティアドバイザー及び業務企画室による監査（内部監査）を実施しました。平成 24 年度も引き続き実際にサーバの状況を点検するなど、物理的なセキュリティ確保にも留意して監査を行いました。

これらの監査により、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

できましたが、一部の情報システムについては、サーバ室の入退室管理に係るセキュリティの確保等について、最高情報セキュリティアドバイザーにより指摘が行われました。これらの点については、当該システムの担当部局において改善を図る予定であり、その結果については、平成 25 年度の監査においてフォローアップすることとしています。

エ）教育・啓発

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に係る研修を受講するよう、集合研修等の研修を実施しています。集合形式の研修では、最高情報セキュリティアドバイザーや外部講師が講師を務め、コンピュータウイルスの脅威や政府・財務省における情報セキュリティに関する規程等について説明を行いました。

また、平成 23 年度からは、e ラーニングによる研修教材を上記の集合研修と同等の内容に充実し、業務多忙などにより集合研修に参加できなかった職員についても、e ラーニングによる自習が可能となり、集合研修を未受講の職員については、e ラーニングによる自習を求めています。

情報システムを調達・運用している情報システムの個別管理組織（PJMO：Project Management Office）の職員に対しては、システム調達・運用時の情報セキュリティ対策について、毎年度、最高情報セキュリティアドバイザーによる研修を実施しています。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

財務省では、「障害・事故等の発生時における対応に関する実施規則」に基づき、障害・事故等を発見した行政事務従事者は、情報システムセキュリティ責任者等に速やかに報告するとともに、情報システムセキュリティ責任者等は大臣官房文書課に連絡することとしております。

障害・事故等への対応にあたっては、報告を受けた情報システムセキュリティ責任者等がマニュアル等に基づき指示を行うこととしております。また、障害・事故等の収束後は、結果及び再発防止策をまとめた報告書を情報セキュリティ責任者及び大臣官房文書課に提出することとしております。

イ）公表した障害・事故等の概要、それに対する対応等

平成 24 年度は、国有財産情報公開システムに対する不正なファイルの蔵置や職員用パソコンのウイルス感染が判明するという事態が発生しました。

これらの事態を重く受け止め、保存文書の暗号化を始め、インターネットからの不正侵入防止、インターネットへの不正送信防止などの対策の強化に加え、情報システムの対策を有効なものとするために、操作・通信履歴（ログ）の管理の強化を進めてまいりました。

また、障害・事故等に適切かつ迅速に対応できるよう、障害・事故等の技術的な対応については、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情報化統括責任者補佐官（CIO※補佐官）が中心的な役割を果たせるように、体制の強化に取り組みました。更に、サイバー攻撃等が発生した際、機動的な対応を行うためのチームである CSIRT の設置や緊急連絡体制の強化等に取り組んでまいりました。

※ 情報化統括責任者（CIO：Chief Information Officer）とは、府省全体の行政情報化の推進に関する責任者であり、財務省では大臣官房長が務めています。

最高情報セキュリティアドバイザーからのメッセージ

情報技術の進歩は非常に早く、クラウド・サービス、スマートフォン等の新たな情報技術が定着し始めています。また、オープンガバメント等、行政サービスに対するニーズも日々高まってきています。その一方で、標的型メール攻撃に代表される高度かつ執拗な脅威が世の中を騒がしているように、情報セキュリティに対する取り組みは一瞬たりとも気を抜くことが許されず、日々各種対策の拡充に追われているといっても決して過言ではありません。行政機関においては、こうした情報技術の進展や行政ニーズの高度化にあわせた情報セキュリティの確保・強化が重要な課題となっています。

財務省は、電子政府を効率的かつ効果的に推進する観点から、自らの業務システムに対して迅速かつ着実に情報技術の導入を行っており、その際には情報システムの運用効率、セキュリティの確保、業務効率の向上といった費用と効果のバランスを重要視しています。情報セキュリティを取り巻く環境としては、昨今の行政機関等を標的にしたサイバー攻撃、たとえば明確な目的をもった組織的な不正アクセスやハッキング行為の脅威に日夜晒されており、待ったなしの対策強化を求められています。今後は、重大なシステム障害・事故等の芽となる情報セキュリティ・インシデント発生の初期段階から情報収集・分析し、情報システムに関する技術面の対策・防御策に結びつける努力が重要と言えます。また、ユーザの利用環境面からのセキュリティ対策については、標的型メール攻撃の見分け方を身に付けるのみならず、事後的な緊急対処についても外部委託先を含めて万全を期すなど、総合的な情報セキュリティ対策強化に取り組んでいく必要があります。

今後の重要課題としては、人的対策、環境・物理面での対策の一層の推進、及び自己点検や監査等の発見的対策の更なる推進、並びに情報セキュリティ・マネジメント強化のための PDCA サイクルの改善が挙げられます。具体的には、執務環境整備等の人的・物理面での予防的な情報漏洩対策と事後的補完策の充実、外部委託先の履行状況管理の厳密化を含むインシデント対応の高度化、そして事案・事故へ緊急対処するための組織・体制の運営効率化、最大活用化などです。

私は、CIO 補佐官を兼任する立場から、上記を踏まえ、一層の内部監査の高付加価値化と情報セキュリティマネジメントシステムの定着化への取り組みについて誠心誠意支援していく所存です。財務省が我が国の安心・安全な電子政府の模範となるよう努めてまいりたいと思います。

財務省最高情報セキュリティアドバイザー
（CIO 補佐官）
村田 正憲

15 文部科学省

情報セキュリティ最高責任者からのメッセージ

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。

近年、我が国では、情報通信技術の急速な進歩に伴い、国民生活が飛躍的に向上する一方で、情報セキュリティの脅威についても多様化・高度化・複雑化し、サイバー攻撃の手口もより巧妙化してきております。平成 24 年度においては、中央省庁や裁判所等を標的としたサイバー攻撃により、ウェブサイトの書き換えや情報漏洩等の被害が相次ぎ発生し、社会問題となったのは記憶に新しいところです。

また、昨年 9 月には、外局である文化庁のシステムがサイバー攻撃を受け、ウェブサイトの一部改ざんが発生し、一時当該サイトを閉鎖する事態となりました。このことによって、ご利用者の方々に、大変なご迷惑やご心配をお掛けしましたことを心よりお詫び申し上げます。

当省では、かねてから文部科学省情報セキュリティポリシー（以下「ポリシー」という）を制定し、その運用を通じて情報セキュリティ対策を徹底してきたところでありますが、このことを受けて、以下の点を中心に情報セキュリティ対策のより一層の強化に取り組んでまいりました。

(1) 情報セキュリティ事案に対応する専門チーム（CSIRT）整備による体制強化
(2) 省内職員向けの情報提供及び研修による情報セキュリティの普及啓発
(3) 調達ガイドラインの策定等による情報セキュリティ対策の充実・強化
(4) IT-BCP の整備による情報システム危機管理の強化

本報告書は、これらのことを踏まえ、平成 24 年度に実施した情報セキュリティ対策の取組、監査結果等についてまとめたものです。

情報セキュリティ対策は政府機関にとって重要な課題となっており、今後の情報技術の発達や環境の変化により、新たな情報セキュリティ上の脅威が出現してくることも想定されます。当省としてはそれらに適切に対処し、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。

平成 25 年 6 月 11 日
情報セキュリティ最高責任者
（文部科学省大臣官房長）
前川　喜平

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度は前年度までの取り組みを継承し、「省内 CSIRT の整備等管理体制の拡充」、「関連規程の整備と周知徹底」、「各種技術的対策の実装」等を行うとともに、当省における情報セキュリティ対策の水準を把握し、今後の課題を明らかにするために「自己点検」、「情報セキュリティ監査」を行いました。

自己点検、情報セキュリティ監査の結果、当省においては一定の情報セキュリティレベルを確保できていると思われます。それと同時に、更なる向上のための課題を明らかにすることができました。

また、情報セキュリティ維持に関する訓練として標的型メール攻撃訓練を実施し、標的型メール攻撃に対する職員の意識啓発に一定の効果を上げることができました。

一方で、平成 24 年 9 月、文化庁のウェブサイトが改ざんされるというセキュリティ事案が発生しました。この事案では「国指定文化財等データベース」を停止するに至りました。また、同時期に、当省所管の独立行政法人、国立大学法人等でもハッカー集団によるサイバー攻撃やウイルス感染による情報流出などが発生しました。

当省のみならず政府機関全体へのサイバー攻撃が頻発していることからも、サイバー攻撃とその兆候を見逃さず、すばやく対応する必要があり、そのためには CSIRT を通じて NISC や他府省と問題意識を共有し、緊密な情報連携体制を実現することが重要課題であると認識します。

イ) 平成 25 年度の目標

平成 25 年度においても引き続き情報セキュリティ対策に係る自己点検、情報セキュリティ監査等を実施し、情報セキュリティ対策の評価と見直しを行うとともに、平成 25 年度における重点的に取り組む事項を以下のとおり設定します。

a) 情報セキュリティに関する普及啓発

- 最近の手口も考慮した標的型メール訓練の継続的な実施及び標的型メールへの対応に係る教育の充実
- 政府全体で推進することとされているリスク評価の取組及び継続的な教育を通じた情報の格付及び取扱制限の理解促進
- 情報セキュリティの障害・事故等を踏まえた情報システム管理者向けの教育の見直し

b) 情報セキュリティに関する自己点検

- 自己点検の円滑な実施のための対策立案と実行
- 自己点検結果を改善活動につなぐための仕組みの確立

c) 情報セキュリティ監査

- 情報セキュリティの障害・事故等を踏まえた監査内容の見直し

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

a) 把握率

当省における全報告対象者のうち、実際に自己点検結果を報告した者の割合が把握率です。平成 24 年度の把握率は 100%でした。過去 2 年間、報告対象者が増加している中で、平成 23 年度に引き続き、徹底した状況把握ができました。

b) 実施率

各点検項目について、「情報セキュリティ対策が実施できている」と自己評価した割合が実施率です。平成 24 年度における主体（※）別の実施率は、主体により若干の差はありますが、いずれも高い水準（95%以上）でした。

（※）ここでいう主体とは、情報セキュリティ管理体制上の役割です。

責任者等：　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等
システム担当：　情報システム責任者、情報システム管理者
行政事務従事者：全職員（行政事務従事者）

イ) 情報システムごとの状況

a) 内容及び手法

統一管理基準及び統一技術基準の遵守事項についての具体的な対策実施状況を確認するため、NISC が作成及び配布する調査票に基づき、公開ウェブ、電子メール、ドメイン、DNS、ネットワーク等に対して行いました。調査結果は、統一管理基準及び統一技術基準における各遵守事項の実施率によって評価されます。

b) 情報システムの対策状況

以下の項目について対策状況を調査し、NISC に報告しました。

・当省が管理する全ての公開ウェブサーバ
・当省が管理する全ての電子メールサーバ
・当省が管理する全てのドメイン
・当省がインターネットに接続して運用しているネットワーク

ウ) 監査の状況

a) 情報セキュリティ監査の概要

情報セキュリティ監査は、当省における情報セキュリティ対策の状況を客観的に評価し、今後取り組むべき課題を明らかにするために実施しました。

b) 情報セキュリティ監査の内容

・ポリシーの準拠性監査（ポリシーが統一管理基準及び統一技術基準に準拠した内容となっているか）
・情報セキュリティ関係規程の準拠性監査（ポリシー実施手順がポリシーに準拠した内容となっているか）
・運用の準拠性監査（実際の運用がポリシー及び情報セキュリティ関係規程に準拠しているか）
・自己点検の適正性監査（自己点検の実施内容が適正か）
・脆弱性診断（個別の情報システムの脆弱性に対する技術的対策が妥当か）

c) 監査結果の総括

ネットワーク、サーバ、ウェブアプリケーションにおいて発見された脆弱性については、修正プログラムの適用を行い、再診断により正しく対処されていることを確認しました。

ポリシー等関係規程類の準拠性や、運用の準拠性、自己点検の適正性において検出された問題点については、原因を分析し、今後継続して改善への取り組みを行う予定です。

エ) 教育・啓発

当省における情報セキュリティ普及啓発のため、以下の各施策に取り組みました。

①平成 25 年 2 月の情報セキュリティ月間に併せて、文部科学省関係機関の情報セキュ

リティ対策担当者等を対象とした情報セキュリティセミナーを開催し、情報セキュリティ意識の向上に努めました。
②当省が策定した新たな情報セキュリティ関係規程「情報システムに係る調達ガイドライン」の利用を促進するため、各部署のシステム管理者に対し集合研修を企画、実施しました。
③NISC 等から提供される注意喚起情報を省内電子掲示板に掲載するとともに、緊急性の高い情報については全職員向けにメールで発信しました。
④標的型メール攻撃に関する教育・意識啓発のため、「平成 24 年度標的型メール攻撃に対する教育訓練」（NISC 主管）を実施しました。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

文部科学省においては、今年度１件の情報セキュリティに関する事故を把握しています。

イ）公表した障害・事故等の概要、それに対する対応等

a）文化庁・「国指定文化財等データベース」ウェブサイトの改ざん

- **発生日時**

平成 24 年 9 月 24 日（月）朝、当該ページが改ざんされていることが発覚しました。

- **概要**

文化庁が運営する「国指定文化財等データベース」のウェブサイトがサイバー攻撃により改ざんを受け、トップページが「尖閣諸島（沖縄県）と中国国旗の合成画像」に書き換えられました。

文化庁では、改ざんを発見した直後に当該ウェブサイトの公開を停止し、被害状況の調査、原因究明と再発防止策の検討を開始しました。再発防止策を講じた上で平成 25 年 3 月 28 日にサービスを復旧しました。

- **障害・事故の原因**

「国指定文化財等データベース」のプログラムの一部に不備があり、そこに不正なアクセスがなされた結果、トップページが書き換えられました。

- **対応**

（暫定措置）

更なる攻撃と被害の拡大を防止するため、事象の発覚直後に委託事業者に連絡し、当該ウェブサイトの公開を停止しました。

これに伴い「国指定文化財等データベース」を休止し、文化財に関する情報を検索する場合は、「文化遺産オンライン(http://bunka.nii.ac.jp/)」を利用するよう、ウェブサイト上でアナウンスしました。

（恒久措置）

今回の事象の再発を防止するため、プログラムの修正を行い、システムの再構築を行いました。

- **再発防止策**

情報システム管理者向けの教育について見直しを図るとともに、脆弱性診断を強化して、再発防止に努めます。

最高情報セキュリティアドバイザーからのメッセージ

文部科学省では、この報告書に示した情報セキュリティ対策を、計画的に実施してきました。この結果、職員の情報セキュリティに関する意識の維持向上が図られ、省内の情報セキュリティも一定の水準を保っていると考えています。しかし、一方で標的型攻撃に代表されるインシデントが毎日のように報道されており、文部科学省を含む行政機関においても、新たな脅威への対応を含む一層の情報セキュリティ対策が重要な課題となっています。

この報告書本文では触れられていませんが、文部科学省の IT システムが更新され、本年 1 月より順次運用が開始されています。新システムにおいては、職員の利便性向上と情報セキュリティ強化の両面からいくつかの新しい仕組みが導入されています。今後は、これらの仕組みを利用シーンに合わせてきめ細かくチューニングすることにより、業務効率の改善と同時に、情報セキュリティの一層の向上が実現できるものと確信しています。

とはいえ、情報セキュリティ対策には完璧な対策は存在しません。情報セキュリティ確保の根幹は職員一人一人の意識と行動です。情報セキュリティ責任部門だけでなく、職員全員の防衛意識の維持と向上が不可欠です。しかし、現状ではセキュリティに対する職員の意識やスキルにはバラつきがあると判断せざるを得ず、継続した教育・訓練が必要です。また、職員が発注する情報システムについて、そのライフサイクルを通じ、要件定義、設計・開発、運用の各段階において、適切なセキュリティ要件を策定できるスキルを身につけてゆく必要があります。本年度はこのためのガイドラインを作成しましたが、今後はそれらのより広範な活用促進と効果のアセスメントが期待されます。

文部科学省では、本年度の反省を踏まえ、NISC など政府内外の関連部門と密接に連携を取りながら、情報セキュリティに関する各種情報や技術動向を注視しつつ、この報告書に示された計画・施策を着実に推進してまいります。

平成 25 年 6 月 11 日
情報セキュリティアドバイザー
（文部科学省 CIO 補佐官）
岩崎　進

16 厚生労働省

最高情報セキュリティ責任者からのメッセージ

厚生労働省は、医療や年金、雇用対策など、国民生活に直結する政策を担っています。こうした業務で取り扱う個人情報等を含む情報資産については、適切な運用管理の下、組織全体としての情報セキュリティ対策を的確に実施することが不可欠であり、今後とも継続的にその充実・強化に取り組んでいくことが必要です。

平成 24 年度においては、政府機関を狙った標的型メール攻撃等のサイバー攻撃事案が増加する中、サイバー攻撃事案発生のタイミングや、情報セキュリティ月間、各種研修等様々な機会を捉え、職員に対する意識啓発・注意喚起等に取り組みました。特に増加が著しい標的型メール攻撃への対応については、厚生労働省独自の標的型メール攻撃対応訓練の実施にも取り組むほか、メール受信時に必要な注意喚起文をメールヘッダーに追記し、注意を促すシステム面での対応も行いました。

また、障害・事故等が発生した際には、これまでも迅速かつ適切に対処するための体制確保等に努めてまいりましたが、政府機関全体の方針を踏まえ、必要な機能等を備えた厚生労働省ＣＳＩＲＴ（Computer Security Incident Response Team）を設置し、緊急対応態勢の強化を図りました。

厚生労働省においては、本報告書で紹介しているとおり、情報セキュリティ対策に関する教育をはじめとする取り組みを実施してきていますが、情報セキュリティ対策の遵守状況や標的型メール攻撃に対する意識など今後とも取り組みを進めていくべき部分があります。

情報セキュリティ対策は、政府機関にとって重要な課題となっており、厚生労働省としても、今後も情報セキュリティを取り巻く環境や情報通信技術の動向等を踏まえつつ、新たなリスク・脅威にも適切に対応するため、必要な教育・訓練などについて、平成 24 年度の実施内容を一層充実させるなど、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
平成 25 年 4 月 25 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度においては、情報セキュリティ教育の実施や障害・事故等に備えた連絡体制の整備を主とした取り組みを進めてきたところであり、自己点検及び監査の結果において一定の成果が見られました。今後とも、さらに職員の情報セキュリティに対する意識が徹底されるよう、教育、訓練、研修や緊急連絡体制の再確認など必要な取り組みを進めてまいります。

a) 情報セキュリティ教育等の実施

職員が情報セキュリティの理解を深められるようオンライン研修のコンテンツの見直しを行うとともに、昨今の政府機関を狙ったサイバー攻撃の増加状況を踏まえ、システム面で標的型メール攻撃対策の強化はもとより、標的型メール攻撃の脅威と対策について、毎年度電子政府利用促進週間をとらえ、情報システムセキュリティ責任者・管理者や行政事務従事者を対象とする集合研修で対策の重要性についての講義を行うとともに、新規採用時からの意識の徹底が重要であることから、初任者研修に情報セキュリティに関するより具体的な説明を行いました。

また、政府機関を狙ったサイバー攻撃事案発生時や情報セキュリティ月間などの様々な機会を捉え、最高情報セキュリティ責任者（ＣＩＳＯ）、統括情報セキュリティ責任者から全職員に障害・事故等発生時の適切な対応等について周知徹底を図るとともに、標的型メール攻撃に対する訓練を実施しました。

b) 障害・事故等に備えた連絡体制の構築・確認

平成 23 年度に発生した情報システムの障害・事故等（インシデント）については、USB メモリ紛失などの不注意やシステム的な脆弱性等に起因する事案であり、これらについては省内職員への注意喚起やシステム更改により対応を行いました。

厚生労働省では、障害・事故等を未然に防止するため、注意喚起やシステムの機能強化を講じていますが、現状ではサイバー攻撃を完全に防止することは不可能であるとの認識の下、攻撃を受けたときに被害の最小化等に取り組むことが重要であると考えています。このため、インシデント発生時に迅速な報告・情報共有、的確な対処を可能とするための体制の確保等が不可欠であることから、緊急連絡体制について、定期異動時期等を踏まえた体制の確認や、継続的な最新の体制の再確認を行うほか、障害・事故等発生時の対処手順の徹底を図っています。

平成 24 年度においては、障害・事故等が発生した際に迅速かつ適切に対処するため、ＣＳＩＲＴ（Computer Security Incident Response Team）機能を既存の情報セキュリティ対策の推進体制に組み込んだ厚生労働省ＣＳＩＲＴを設置し、緊急対応態勢の強化を図りました。

イ) 平成 25 年度の目標

a) 職員における情報セキュリティ意識の徹底

情報セキュリティ対策の意義について、昨今の政府機関等に対するサイバー攻撃の状況に係る情報提供等を行いながら、全職員に対する情報セキュリティ意識の徹底を図ることとし、あらゆる機会を通じて啓発、指導等に取り組むとともに、情報の適切な取扱いや障害・事故等への的確な対処についての継続的な周知・徹底を図ります。また、情報セキュリティ教育について、教材や内容についても、随時見直しを行い、職員が理解しやすいものとなるよう見直しを行うこととしています。

また、サイバー攻撃等の最新の状況を踏まえ、職員の対処能力の向上等を図ることを目的として、必要な教育訓練等の企画・実施に取り組んでいくこととします。

b)　障害・事故等に備えた連絡体制の構築・確認

サイバー攻撃をはじめとする障害・事故等の迅速かつ適切な報告及び対処を可能とするため、情報システムの管理・運用等を行う職員に対し、常日頃からの連絡体制及び対処手順の再確認を呼びかけるとともに、省内各部局と連携・協力し、障害・事故等発生時の連絡が円滑に行われるよう必要な訓練等を実施し、職員の情報セキュリティに対する意識の徹底を図ります。

B）情報セキュリティ対策の実施状況

ア）省庁対策基準に関する自己点検結果

平成 24 年度においては、平成 23 年度の自己点検結果において改善が必要とされた情報システムセキュリティ責任者・管理者の到達率※1の向上を図るべく、効果的な研修の実施等に取り組んだ結果、到達率（１００％）及び到達率（９０％）が向上し、到達率（９０％）でみると、対策を実施した遵守事項の割合が１００％となったことから、一定の成果が上がっているものと思われます。しかし、到達率（100%）及び到達率（95%）をみると、平成 23 年度の全府省庁平均の数値と比べた場合にこれを下回る状況となっていることから、情報システムセキュリティ責任者・管理者に対して、引き続き、様々な機会を活用し、セキュリティポリシー及び関連規程類の周知・徹底を図るとともに、最高情報セキュリティアドバイザーの支援を受け、研修教材や研修内容の見直しを行い、情報セキュリティ教育の充実を図ってまいります。

※１　到達率：すべての遵守事項のうち、実施率※2が一定の割合（100%・95%以上・90%以上）　に到達している遵守事項が占める割合
※２　実施率：自己点検の結果を報告した者のうち、遵守事項を適正に実施した者が占める割合

イ）情報システムごとの状況

厚生労働省では、年金、雇用など大量の個人情報を取り扱うシステムを多数有しているため、セキュリティ事案が発生し、情報の漏洩、改ざん、破壊等が起きた場合には、国民生活に与える影響は非常に大きなものとなりうるという特徴があります。

このため、障害・事故等が発生した場合に、国民に重大な影響を及ぼすシステムについては、昨今のセキュリティ事案を踏まえ、適切なセキュリティ対策を講ずるとともに、セキュリティ対策の実施状況を点検し、必要な改善等を行う必要があります。

平成 24 年度においては、全ての公開用ウェブサーバ、メールサーバ等を対象として、脆弱性の有無や、ソフトウェア等のセキュリティアップデートの適用状況を点検し、直ちに改善すべきものは改善するなど、適切に対処しています。

次年度以降もこれまでに引き続き、緊急の対処を必要とする脆弱性等が生じた場合には、即時に改善等に取り組むなど、適切に対処することとしています。

ウ）監査の状況

厚生労働省では、最高情報セキュリティ責任者（ＣＩＳＯ）の下、情報セキュリティ対策の実施体制の構築及び対策の実施に関する全般的な状況を確認するため、監査計画を策定して監査を実施し、その結果等に基づいて各種規程類の改定やシステムの改善措置等を講ずるとともに、監査結果等を踏まえて情報セキュリティ対策の方針等に活かすなどにより、効果的な情報セキュリティ対策の実施に取り組むこととしています。

平成 24 年度においては、平成 23 年度の監査結果に基づき計画的に対処することとしていた事項のフォローアップに加え、今年度の監査結果に基づき、直ちに改善が必要なものについては緊急に改善措置を講ずるとともに、計画的に対処すべきものについては、平成 25 年度の監査等においてフォローアップすることとしています。

なお、監査の実施に当たっては、適切な監査の実施を図るとともに、客観性・独立性を確保し、専門性の高い監査とするため、外部の専門家を活用して実施しています。また、監査をより実効的なものにするため、同一業者が連続した２年を受注できないように調達制限を課すこととしています。

エ）教育・啓発

a）教育計画

情報セキュリティ対策を適切に実践するためには、職員一人一人がセキュリティポリシー及び関連規程類を理解し、遵守することが必要となります。

このため、平成 24 年度においても、情報セキュリティ対策に関する教育の受講方法と受講後のフォローアップを盛り込んだ「情報セキュリティ対策教育計画」を策定し、適切な対策が実践されるよう努めています。

b）研修

研修については、オンライン研修（ｅ－ラーニング）、オフライン研修、集合研修を実施しています。

研修で使用する教材については、セキュリティポリシー及び関連規程類の改定や最新の情報セキュリティ事案の発生状況、更には平成 23 年度の各種点検・調査結果や研修受講後のアンケート結果等も踏まえ、適宜、見直しや修正を行い、平成 24 年度においても、情報システムの運用継続計画や調達時の情報セキュリティ要件の明確化に係る説明を追加しています。

c）訓練

標的型メール攻撃に対する対処方法や見分け方等の教育を行うとともに、NISC との連携のもと、標的型メールを模したメールを実際に職員に送付し、標的型メールをはじめ、不審メールへの対応の訓練を実施しました。また、訓練結果は、幹部会議、総務課長会議等において部局毎の訓練メール開封率を提示し、所属職員への注意喚起を行うとともに、訓練メールを開封した職員に対しては、情報セキュリティ責任者（情報セキュリティ管理者）を通じて個別に指導を実施しています。

さらに、平成 24 年度は、地方支分部局及び施設等機関職員も含め、厚生労働省単独で標的型メール攻撃訓練を実施しました。

d）普及・啓発

ア　全省的な取り組み

電子政府利用促進週間及び情報セキュリティ月間など、様々な機会をとらえ、情報セキュリティ対策の意識の徹底、セキュリティポリシー及び関連規程類の周知や情報セキュリティ事案を踏まえた注意喚起を行うことにより、情報セキュリティ対策に関する職員の一層の意識向上を図りました。なお、情報セキュリティ月間には、政府へのサイバーテロ攻撃等が多発している現状を踏まえ、職員のパソコン起動時にポップアップメッセージを表示する機能を活用した注意喚起を行いました。

イ　地方機関を対象とした取り組み

個人情報を実際の現場で取り扱う職員においては、個人情報の管理徹底が強く求められることから、非常勤職員の採用時を含め、セキュリティ対策や個人情報保護に関する研修テキストを作成して研修を実施し、職員の意識向上の徹底を図っています。

e）その他の取り組み

「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、NISC との連携のもと、情報システムセキュリティ責任者等に対する研修会を 24 年 6 月と 25 年 3 月の 2 回実施しました。

オ）その他取り組んだ事項

a）送信ドメイン認証技術導入の推進

厚生労働省から送信されるメールが確実に厚生労働省から送付されたものであることを保証するため、送信ドメイン認証（Sender Policy Framework）技術の導入が喫緊の課題となっていましたが、本報告書が対象とする組織で所有する go.jp ドメイン（○○○.go.jp）については、平成 23 年度に第 3 レベルへの導入が完了し、平成 24 年度は第 4 レベル以上のドメインへの導入を進めました。

b）標的型メール攻撃に対するシステム面での対応

政府機関を狙った標的型メール攻撃が増加していることを踏まえ、本省ＬＡＮシステムに不審メールの疑いがあるメール（発信元詐称、フリーメールアドレス等）を受信した際に注意を促すヘッダーをメール上部に表示する機能を追加しました。

C）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

情報セキュリティに関する障害・事故等への適切な対処を行うことを目的として、情報セキュリティに関する緊急連絡網及び障害・事故等が発生した場合等の対処及び報告等の手続を規定した「障害・事故等対処手順書」を整備しており、これに基づき、障害・事故等における影響の拡大防止と迅速な対応を図っています。また、緊急連絡網については、異動時期等を踏まえて体制の再確認を行い、定期的に更新を行っています。

イ）公表した障害・事故等の概要、それに対する対応等

平成 24 年度においては、重大な障害・事故等は発生していません。

最高情報セキュリティアドバイザーからのメッセージ

厚生労働省の施策は、国民生活と密接に関連した、年金、医療、育児、介護、雇用等を扱い、関連する情報資産には様々な個人情報を含む上に、情報システムも多岐にわたります。この情報システムの中には、社会保険オンラインシステムやハローワークシステムのような全国の地方支分部局、施設等機関にまたがる大規模システムも含まれていて、一旦、インシデントが発生すると国民生活にも影響を与えかねません。このため、厚生労働省においてもセキュリティポリシー等を遵守し、着実に PDCA を実践し、課題があれば一層の改善を行っていくことが重要になります。

平成 24 年度は、NISC と連携し、CSIRT 体制の整備、標的型メール訓練の実施、省内職員向けの SBD 研修の実施など更なるセキュリティ向上に向けた新たな試みを開始した事は評価できると思われます。

特に、脅威が増している標的型メール攻撃については、厚生労働省として独自に地方支分局も含む 5 万超の全職員に対し標的型メール訓練を実施できた事は評価できます。

一方、情報セキュリティ対策実施状況の自己点検結果を見ると、まだ改善の余地があり、教育・啓蒙活動等を通して、より一層の情報セキュリティ意識向上を図る必要があると思われます。

情報セキュリティ対策はますます重要な課題となっております。最高情報セキュリティアドバイザーおよびＣＩＯ補佐官としては、今後も情報セキュリティ技術の動向を注視し、新たなリスク・脅威にも適切に対応するとともに、概算要求確認時、調達仕様書審査時、提案書審査時等において情報セキュリティ要件について確認、助言・支援を行っていく所存です。

最高情報セキュリティアドバイザー（厚生労働省ＣＩＯ補佐官）
徳永　篤男
平成 25 年 4 月 25 日

17 農林水産省

最高情報セキュリティ責任者からのメッセージ

農林水産省では、①情報の格付や取扱制限などの情報の取扱ルールの明確化、②職員の情報セキュリティ意識向上の取組の強化、③情報システムの障害・事故発生時の対応体制の強化、④情報システムのセキュリティ対策の強化等を大きな目的として、情報セキュリティ対策を実施しています。

昨今の情報セキュリティを取り巻く状況を見ると、各府省庁や独立行政法人等の政府機関や国の重要な情報を扱う企業等に対するサイバー攻撃事案が顕在化しております。こうした事案は、個人情報や企業情報等の詐取又は改ざん、国民生活や社会経済にとって不可欠なサービスの停止等を引き起こす大きな問題となりえます。

農林水産省でも、海外からのものも含め、日々、高度化・多様化した標的型メール攻撃等を受ける事例が発生しています。重要事案の発生を受けて、本年１月には、サイバー攻撃による情報流出の可能性や対応策について、徹底的な調査を行うため、外部有識者等による委員会を設置しました。５月に同委員会は中間報告を公表し、その中で、行政文書の流出の可能性や情報流出に対する職員の危機意識の欠如等を指摘しております。

当省としては、中間報告を真摯に受け止め、今後のサイバー攻撃への対応等を改善していくため、対策の実施時期を明確にした工程表を速やかに作成し、可能なものから早期に対策を実行していくこととしております。その一つとして、内閣官房長官を議長とする政府全体の情報セキュリティの取組の中で、外部有識者の助言も踏まえつつ、本年３月に設置したＣＳＩＲＴ（Computer Security Incident Response Team：情報システムに係る障害・事故等への緊急対応チーム）を積極的に活用するなど、情報セキュリティを確保する体制の検討・見直しも随時進めています。

農林水産省では、今後も、内閣官房等の関係機関と連携を取りながら、職員の間で危機体験を共有しつつ、最も有効なファイアーウォールは職員の高いセキュリティ意識であるという認識の下、職員が一丸となって、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参ります。

平成２５年５月３１日
最高情報セキュリティ責任者
大臣官房長　　今井　敏

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

情報セキュリティの確保及びその強化・拡充を図るため、機密性が高い情報について、機密性に応じた的確な情報管理を徹底し、機密を保持するため、その管理手法を改善しました。

また、巧妙化する標的型メール攻撃等のサイバー攻撃に備えて、情報システムのセキュリティ対策の強化を図りました。

イ) 平成 25 年度の目標

農林水産省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、対策の実行に係る工程表を作成し、以下の取組を重点的かつ計画的に実施します。

①職員に対する教育を強化・拡充し、危機体験の共有やルールの遵守を含む、情報セキュリティの意識向上に努めます。
②情報システムの障害・事故等の発生に備えた体制を整備強化します。
③情報システムのセキュリティ対策の強化に努めます。
④情報の格付及び取扱制限の明示の徹底に努めます。
⑤情報セキュリティ関係規則の違反者への注意や指導の徹底等による再発防止の取組を強化します。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

職員がその業務上の情報セキュリティ対策の実施状況について、自己点検を実施しました。このような実態把握の結果を踏まえ、情報セキュリティの確保のために職員が更に対応を改善すべき内容を明確化し、取組の強化に努めました。

イ) 情報システムごとの状況

様々な脅威から情報システムを守るため、情報セキュリティ対策の強度とシステムの利用者の利便性のバランスを図りながら、それぞれの情報システムにとって最も有効な情報セキュリティ対策を実施するよう努めました。

ウ) 監査の状況

監査の客観性と専門性を確保するため、主要な情報システムの情報セキュリティ対策の運用状況監査と公開ウェブサーバ等の脆弱性診断については、外部の第三者組織に委託して実施するとともに、省内各部局の情報セキュリティ対策の運用状況については、担当職員による内部監査を実施しました。

エ) 教育・啓発

業務において適確な情報セキュリティ対策が実践できるよう、全ての職員とシステムの運用担当職員に対し、情報セキュリティ教育と注意喚起等を繰り返し行いました。

C) 情報セキュリティに関する障害・事故報告

ア) 情報セキュリティに関する障害・事故等の把握

農林水産省では、職員に対し、情報システムに異常やその兆候を発見した場合は、昼

夜を問わず、直ちに情報システムの責任者や管理者に報告することを求め、統括情報セキュリティ責任者の指示の下、障害・事故等の発生からの速やかな復旧作業の着手を行うこととしています。

また、このような障害・事故等の情報は、他部局への被害の拡大防止の観点から、直ちに統括情報セキュリティ責任者から、各情報システムの責任者や管理者に伝達し、適切な対応を促すほか、必要に応じ、省内の連絡網を利用して全職員へ注意喚起を行っています。

イ）公表した障害・事故等の概要、それに対する対応等

平成２５年１月、過去に受けた情報システムへのサイバー攻撃の資料を確認したところ、不審な通信のうち、少なくとも１回は意味のある情報の流出が疑われる通信があったことから、保存している通信記録等をもとに、サイバー攻撃による情報流出の可能性、サイバー攻撃への対応について、外部有識者の参加を得て、「農林水産省へのサイバー攻撃に関する調査委員会」を設置し、徹底的な調査を開始しました。

５月に同委員会は中間報告を公表し、一部の職員パソコン（５台）から、行政文書（１２４点）が外部に流出した可能性があること等が確認されました。

最高情報セキュリティアドバイザーからのメッセージ

この１年、標的型メール攻撃をはじめとした脅威への技術的対策強化を進めてきましたが、「農林水産省へのサイバー攻撃に関する調査委員会」の「中間報告」において、不審な通信に関する職員の調査・報告・連携・共有が不十分であったなど、危機対応ルールをはじめとしたセキュリティ・ガバナンスに重大な問題があったことが指摘されました。総合的な情報セキュリティ危機管理対応力の不足、ルール遵守状況を評価・点検・指導する現場アクション取組の不足など、早期にガバナンス強化を図る必要があります。また、ルール違反者に対してはシステム利用制限措置を講ずるなどの厳しい対応も必要との認識です。業務上の必要性から例外的な対応を要請されるケースもありますが、例外的対応にはそれに見合う技術的対策のみならず、セキュリティ管理体制とルールの明確化、ルール遵守状況の監視・点検等の活動・報告を義務づけ、これを１００%遂行できない限り、例外を認めることが無いように指導・助言してまいります。

セキュリティの要は人であると感じています。高度な情報セキュリティ人材の育成・確保も重要ではありますが、忍び寄る脅威に対して、まずは一人ひとりがセキュリティ確保のための正しい振る舞いを体得するための行動原理を、組織をあげて定着させることが重要との認識です。セキュリティ規則で決められたことを守り、“常に信憑性を確認する習慣”を正しく身につけ、ちょっとした違いや不自然さに気づく力を育てなければなりません。

そのため、セキュリティ対策におけるＰＤＣＡとしての点検と指導、教育と訓練を繰り返し実施し、情報セキュリティ対策全体としての費用対効果を高めるよう助言してまいります。

最後に、情報セキュリティ対策は情報を安心して利活用できるようにするために必要となる取組であり、情報利活用を禁止するためのものではありません。ですから、“あれは駄目、これも駄目”と言うのではなく、安全・安心のために“あれをしよう、これをしよう、そして守ろう”と前向きに取り組みましょう。

最高情報セキュリティアドバイザー
（農林水産省 CIO 補佐官）
久保田　智

18 経済産業省

最高情報セキュリティ責任者からのメッセージ

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急速に高まっている一方で、不正アクセスやウイルス感染による情報漏えいなどのリスク・脅威が増大しています。業務におけるシステムへの依存度が高まるなか、情報セキュリティ対策の重要性が益々高まっています。

経済産業省は、我が国の企業や重要インフラの情報セキュリティ水準を高めるための政策を担っています。従って、当省は、政府機関のみならず社会全体の模範となるよう、率先して情報セキュリティ対策に取り組む必要があります。

平成 24 年度は、引き続き防衛産業や重要インフラ、政府機関等に対する攻撃が発生し、こうした事案に対し内閣官房情報セキュリティセンターを中心に、関係政府機関による対策が進められて参りました。経済産業省は、政府部内のこうした対策を検討する場において積極的な貢献を果たして参りました。

同時に、自らの業務の遂行において最も重要なシステムのひとつである基盤情報システムの更改を行い、職員の情報システムの利用に係る利便性の向上を図るとともに、その中で様々なセキュリティ機能を実装するなど、技術面から情報セキュリティ対策の強化に努めて参りました。

さらに、省内各課室における情報管理の一層の徹底を図ることを目的に、情報管理に係る運用手続きや体制の整備など積極的な組織的な取り組みを行って参りました。

本報告書は、平成 24 年度に経済産業省が実施した情報セキュリティ対策の具体的な活動についてとりまとめたものです。現段階では、大きな課題は見つかっておりませんが、リスク・脅威への対策や職員向け教育など、不断の改善努力を進めることとしています。

経済産業省は、今後も引き続き、情報セキュリティの維持・向上に努めて参ります。

最高情報セキュリティ責任者
（経済産業省大臣官房長）
立岡　恒良
平成 25 年 4 月 24 日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度においては、経済産業省の業務遂行において最も重要かつ基本となる基盤情報システムの更改を行い、職員の情報システムの利用に係る利便性の向上を図るとともに、その中で様々なセキュリティ機能を実装するなど、技術面から情報セキュリティ対策の強化に努めて参りました。

更に、平成 23 年度に実施した省内課室の情報管理に係る運用手続きや体制の整備について、情報管理の一層の徹底を図るため、機密性の高い情報をメール送信する際に、省内宛には閲覧者指定システム（※）を利用し、省外宛には暗号化及び上長を「cc:」に追加する等のルールを導入するなど、様々な情報セキュリティ対策を実施して参りました。

また、平成 23 年度に発生した障害・事故等の再発防止状況につきましては、委託事業のウェブサイトの改ざん事案、及びウイルス感染事案の 2 件につき、ともに適切な再発防止対策を実施しております。

こうした各種の取り組みにより、職員の情報セキュリティに係る意識向上につながるとともに、情報セキュリティ対策の強化につながりました。

（※）閲覧者指定システム：情報漏えい防止の観点から、機密性の高い電子ファイル（PDF ファイル）に対して詳細なアクセス制限等の設定を可能とする仕組み。平成 24 年度に全職員が利用できる環境を整備。

イ) 平成 25 年度の目標

当省では、平成 25 年度に重点的に取り組む目標を以下のとおりとし、今後更なる情報セキュリティの向上を目指して参ります。

・省内課室の情報管理に係る運用手続きや体制の整備について、その実施状況を適宜把握するとともに、引き続き省内各課室における情報管理の実態について、改善状況の把握や必要により指摘・指導等に努めて参ります。
・平成 24 年度に更改した基盤情報システムの運用において、機密性の高い情報の漏えい防止の徹底に向けたデータの暗号化、アクセス制限付きフォルダや閲覧者指定システムの活用、複数要素主体認証などの技術的手段の定着・推進を図るとともに、新たな技術の導入等、更なる情報セキュリティ対策の高度化を図って参ります。
・職員教育の一環として実施する情報セキュリティ研修や省内周知等において、標的型メール攻撃への対応（訓練や注意喚起等）や当省関連の Web サイト改ざんへの対応等について、重点的に教育を実施して参ります。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

a) 総評

情報セキュリティ対策の実施状況の自己点検（以下、「自己点検」という。）は、経済産業省情報セキュリティ対策基準の各遵守事項について職員自らが実施状況を確認し、自己評価を行うものです。

平成 24 年度の自己点検については、全職員に対し情報セキュリティ対策の実施状況の自己点検を行った結果、概ね適切に実施されていることが確認できました。

b) 自己点検結果の状況

全職員（非常勤職員を含む）を対象に実施した平成 24 年度の自己点検の把握率（※）は 97.0%となり、また、実施率（※）は、各主体とも 9 割を超える高い値となりました。

（※）把握率：報告対象者のうち、自己点検を提出した者の割合。
（※）実施率：自己点検を提出した者のうち、全ての対策を実施した者の割合。

c）課題と対策

平成 24 年度の自己点検の結果は、把握率、実施率とも 9 割を超える高い水準を確保しています。これは、イントラネットを活用し、簡便に自己点検が実施できるよう技術的な環境を整備していることに加え、様々な普及周知の効果として、情報セキュリティ対策の必要性に関する職員の意識が高まってきたことによるものと考えられます。

イ）情報システムごとの状況

a）総評

当省で導入している情報システムの公開ウェブ、電子メール、ドメイン、及びネットワーク等に対する情報セキュリティ対策に関して、政府機関統一基準群で定められた遵守事項の実施状況に係る重点的な検査（以下、「重点検査」という。）を実施致しました。

平成 24 年度の重点検査については、対象とする全ての情報システムにおいて、公開ウェブ、電子メール、ドメイン、及びネットワーク等に対する情報セキュリティ対策の実施率は 100%であり、適切に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。

b）課題と対策

当省では、情報システムの情報セキュリティ対策は適切に講じられており、今後もこの状態を維持するよう、引き続き適切な情報セキュリティ対策の実施に努めて参ります。

ウ）監査の状況

a）情報セキュリティ監査の実施

当省では、政府機関統一基準群及び経済産業省情報セキュリティ管理規程に基づき、毎年度、情報セキュリティ監査を実施しています。

情報セキュリティの水準を適切に維持していくためには、政府機関統一基準群に準拠した経済産業省情報セキュリティポリシーを適切に整備・運用することによってその実効性を確保し、その準拠性と妥当性を客観的に確認する必要があります。

また、各業務システムの情報セキュリティ対策の実施状況を適切に評価し、評価結果に応じて見直しや改善を行うという PDCA サイクルを適切に実施することが重要です。

これらの点を踏まえ、当省の情報セキュリティ監査は、独立性を有する外部の監査組織に委託し実施しています。

平成 24 年度に実施した情報セキュリティ監査の結果は次のとおりです。

- **情報セキュリティ監査**

政府機関の情報セキュリティ対策のための統一基準群と経済産業省情報セキュリティポリシーとの準拠性監査、及び経済産業省情報セキュリティポリシーと各実施手順等との準拠性監査において、不備（不適格事項）は無いことが確認されました。今後は、経済産業省セキュリティポリシーの実効性を高めるべく、普及啓発の徹底や技術的対策の検討等を実施して参ります。

また、平成 23 年度に実施した情報セキュリティ監査結果で明らかになった課題及び問題点に対する改善状況の監査においては、指摘された課題及び問題点に係る事項は概ね対応が済んでいることが確認されましたが、一部の情報システムにおいて、軽微な不備（観察事項）があったため、引き続き確認することと致しました。

・ **システム監査等**

システム運用時における情報セキュリティ対策実施状況の監査においては、組織や個人に大きな影響を及ぼすような不備（不適格事項）は無いことが確認されました。なお、ログ保管・分析やパスワード管理等いくつかの事項において、軽微な不備（観察事項）が確認されました。今後は、各情報システムのライフサイクルや執行予算等も踏まえ、観察事項について引き続き確認・対応を図って参ります。

また、例外措置については、申請及び許可の手続きに係る監査を行い、全ての手続きに不備が無いことが確認されました。

b) 情報システムのセキュリティ診断の実施

情報システムの安全性を高めるため、基盤情報システム等各種システムについて、外部から擬似的な攻撃を行うなど、当該情報システムのセキュリティホールの有無や運用管理上の問題点の有無等を確認するため、セキュリティ診断を実施しています。

平成 24 年度は、更改を実施した基盤情報システムのサーバやネットワーク機器、及び Web アプリケーションに対し、診断ツールや各種手法を用いたセキュリティ診断を実施致しました。この結果、基盤情報システムのサーバやネットワーク機器、及び Web アプリケーションの一部に、攻撃に利用される可能性のある脆弱性が検出されましたが、サービスイン（平成 25 年 1 月）までに対応を実施しました。また、運用開始後においては、各種ベンダから提供される新たな脆弱性情報を確認し、速やかな対処を実施しています。

エ）教育・啓発

a) 教育

・ **教育計画の策定、教育の企画等**

情報セキュリティ対策を着実に取り組んでいくためには、職員一人一人が情報セキュリティ関連規程に基づく具体的な情報セキュリティ対策を理解し、日々実践していくことが大切です。そのためには、各職員に対し継続的に情報セキュリティ教育を行うことが必要です。

平成 24 年度では、引き続きイントラネットの一部に構築した「情報セキュリティコーナー」の運用を行い、適宜職員に必要な情報を提供するとともに、e-learning による情報セキュリティ研修を実施しました。この研修教材については、特に標的型サイバー攻撃に特化したものとして研修を実施したことに加え、標的型メール攻撃の教育訓練（平成 24 年 10 月、11 月）において、全職員をこの訓練の対象者とし、標的型メール攻撃の実態を自ら体験することにより、より身近に情報セキュリティの重要性を理解するきっかけとなるなど職員の情報セキュリティに対する意識がこれまで以上に高まりました。

・ **対象者の役割に応じた教育教材の整備**

教育教材については、課室情報セキュリティ責任者、一般職員及び新規採用職員等を対象とした情報セキュリティ教育の教材をそれぞれ整備しています。

平成 24 年度は、課室情報セキュリティ責任者、一般職員を対象とした情報セキュリティ教育の教材を見直すとともに、近時多数発生している標的型メール攻撃への対応等を追加致しました。また、新規採用職員や情報システム関係職員、留学等出向者に対しては、異動時などに必要な情報セキュリティ教育を集合研修により実施しています。

・ **教育受講状況の管理**

e-learning を利用した教育コンテンツについて、受講実績の有無、確認テストの成績等の受講状況を管理し、理解度の確認を行っています。全職員に対する e-learning 研修の確認テストでは、満点を獲得しない場合には履修済みとしなかっ

たため、受講者は研修内容を十分理解するまで確認テストを受けることとし、その理解度の徹底を図っております。

b) 情報セキュリティ対策等資料参照の容易化

情報セキュリティ関連規程や職員が取り組むべき具体的な情報セキュリティ対策等の資料を情報セキュリティコーナーに掲載し、職員がいつでも容易に参照できるよう教育環境を整備しています。

平成 24 年度は、基盤情報システムにおけるインシデント発生時の対応方法や経済産業省情報セキュリティポリシーの改正内容、各種標的型メール攻撃の内容や対応方法などを情報セキュリティコーナーに掲載しました。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

経済産業省では、情報セキュリティに関する重大な障害・事故等が発生した場合は、「障害及び事故等対応手順書」及び緊急連絡網により、障害・事故等に対応する責任者が実施した内容も踏まえ、障害及び事故等の原因を調査するとともに再発防止策を策定し、その結果を統括情報セキュリティ責任者に報告することとなっております。更に、統括情報セキュリティ責任者は、その内容を検討し、再発防止策を実施するために必要な措置を講ずるとともに、必要に応じ、最高情報セキュリティ責任者に報告することとなっております。

イ）公表した障害・事故等の概要、それに対する対応等

平成 24 年度において、公表すべき障害・事故等は発生しておりません。

最高情報セキュリティアドバイザーからのメッセージ

経済産業省では、平成 24 年度の基盤情報システムの更改に伴い、様々なセキュリティ対策を実施致しました。特に、職員の手元にあるパソコンにデータを保存するこれまでの方式から、職員の手元のハードウェアにはデータを残さないシンクライアント方式に変更致しました。また、認証方式に関しても、複数要素主体認証を導入し、セキュリティレベルを向上させました。これらのセキュリティ対策は、セキュリティレベルの向上のために行ないましたが、結果として、職員が省内の会議室にパソコンを持参し、ペーパーレス会議を行なうなど業務改革に資することにもなりました。

また、自宅や出張先など省外からインターネット経由で、安全性を確保しながら省内の情報システムにアクセスできるように環境を整備致しました。これにより、省内の情報システムの利用可能な範囲を拡大させることが可能となり、セキュリティを確保しつつ利用範囲を拡大し、結果として業務効率の向上に寄与できる基盤が作られました。更に、データセンターでデータを集中管理することにより、仮に職場等が災害にあった場合でも、業務継続や短期間での業務復旧が可能となりました。

一方、サイバー攻撃は、年々、組織化し本格化する傾向にあります。基盤情報システムの更改においては、現時点で想定できるサイバー攻撃への対策は、十分行なっておりますが、今後の高度化し複雑化するサイバー攻撃に対しては、継続的に検討し対応していく必要があります。

また、技術的なセキュリティ対策を有効かつ効果的に利活用するために、経済産業省情報セキュリティポリシーに基づいた各課室での情報の格付と取扱いルールの徹底及び定着化を引き続き推進し、総合的な情報セキュリティ対策を行なう必要があります。

経済産業省は、情報産業を所管すると共に、電子政府を強力に推進しており、自ら率先して情報技術の効果と情報セキュリティのバランスを図りつつ、ＩＴの利活用を推進できる情報セキュリティ対策を行なうことが重要であります。

最高情報セキュリティアドバイザー及び CIO 補佐官としては、電子政府及び経済産業省の業務効率化の推進、職員の生産性向上と情報セキュリティの確保のバランスを念頭において、総合的な改善・推進を支援していく所存です。今後も、経済産業省が電子政府の模範となるよう努めて参りたいと思います。

最高情報セキュリティアドバイザー
（経済産業省 CIO 補佐官）
満塩　尚史
平成 25 年 4 月 24 日

19 国土交通省

最高情報セキュリティ責任者からのメッセージ

経済活動や社会・国民生活の多くの面において情報通信技術の利用が一層進む中、国土交通省においても情報システムは業務を支える重要な手段となっています。一方、世界規模での情報通信技術の急速な普及・進展とともに、情報セキュリティ上のリスクも多様化・高度化しており、情報通信技術を安全・安心に活用し、業務を継続していくための不断の取組が必要不可欠となっています。さらに、昨今の情報窃取を目的として、特定の組織や個人に送られる標的型メールによるサイバー攻撃等の新たな情報セキュリティ上の脅威に対しても適切に対応していく必要があります。

国土交通省は、国土の開発利用保全、社会資本の整備、交通政策の推進、気象、海上の安全・治安確保等、広範な分野を担当するとともに、外局や地方支分部局等を含め多様な機能を持つ組織を擁する機関です。このため、これを支える情報システムの規模も大きく、その障害の発生は非常に大きな社会的影響を及ぼす可能性があることから、全職員が一丸となり、組織全体として適切な情報セキュリティ対策を実施していくことは極めて重要であります。

国土交通省においては、以前から、国土交通省情報セキュリティポリシーの制定及び運用を通じ、省内の体制構築と責任の明確化、状況の変化に応じた継続的な取組等、情報セキュリティ対策の徹底に努めてきました。また、情報セキュリティをとりまく社会的状況に応じて、職員を対象とした教育訓練の実施も進めつつあります。さらに、情報システムへのサイバー攻撃等の発生に際して緊急に対応する組織の整備も行っております。

本報告書は、平成２４年度に国土交通省が実施した情報セキュリティ対策に対する取組状況、その結果等についてとりまとめたものです。

情報セキュリティ対策を実施する上では、各部局において取扱う情報の内容や業務の実態を踏まえ、柔軟かつ確実な対策・措置を図ることが重要です。今後も、適切な情報の取扱い、情報システムの運用について、常日頃から緊張感を持って臨むよう全職員に周知徹底するとともに、新しい脅威に対しても時期を得た必要な対策を講じ、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。

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）
平成２５年６月１０日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成２３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きています。職員における情報の取扱等における情報セキュリティの必要性に対する認識は向上しているものの、一部のシステムにおける運用・保守等に係るセキュリティ対策については、セキュリティ確保のための措置を講じるべき事項も見受けられるため、各システム管理者に対して実施すべき措置の周知等を今後も継続していく必要があると考えています。

また、平成２４年度の新たな取組として、情報セキュリティインシデント対応を行う組織として国土交通省 CSIRT を設置したほか、昨今増加している標的型メール攻撃に対応した訓練を約４万人の職員に対して実施し、所要の成果を得ました。

イ) 平成 25 年度の目標

a) 情報セキュリティルールの職員への浸透に向けた施策

情報の格付けとそれに応じた取扱いの浸透や、システムの取扱いルールの徹底に向けて、各部局の業務を踏まえた取組を推進します。

b) 国土交通省 CSIRT が有効に機能するための施策

今年度設置した CSIRT が有効に機能するようにするため、連絡体制等について更なる周知徹底を図るとともに、実際の業務や訓練を通じて手順の見直しや拡充を行います。

c) 脅威の動向を踏まえた施策

既に取り組んでいる情報セキュリティ対策の着実な実施に加え、昨今増加している標的型メール攻撃や、ソーシャルメディア等に起因する脅威への対策を強化します。

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

今年度の情報セキュリティ対策の自己点検結果は、各役割別の把握率が１００％に達し、これまで行ってきた情報セキュリティに関する周知徹底により、意識が向上した成果と考えています。また、実施率についても、各役割別でそれぞれ９０％を越えています。

しかしながら、情報システムの管理に関する自己点検では、一部手順の未整備等の不備が見受けられたことから、今後は、これらの不備に重点を置いて更なる周知徹底、取組を推進して参ります。

イ) 情報システムごとの状況

今年度の情報システムにおける重点検査の結果から、ウェブサーバのセキュリティ対策と府省庁外との接続を行うネットワークにおけるセキュリティ対策に一部不足が見受けられました。これらのセキュリティ対策は年度内に不足を解消すべく取組を行ってきましたが、対策が完了していないものに対しても継続してフォローアップを行い、早期の解決に向けて取り組んで参ります。

ウ) 監査の状況

国土交通省は、地方支分部局や外局等を含め非常に大きな組織を有することから、各部局内で継続的、自律的に監査を行う部局内監査の仕組みを構築しています。部局内監査では、各部局において情報セキュリティ責任者が情報セキュリティ監査実施者を指名

し、当該部局内における自己点検の結果を踏まえて必要な監査を実施することにより、情報セキュリティポリシー及び関係規程に準拠していることを確認します。

部局内監査を実施した結果、一部の部局において、情報の格付けと明示、格付けに基づいた取扱い、外部記録媒体使用時におけるウィルスチェックの徹底等といった分野について、一部取組が不十分な例があることが見受けられましたが、それ以外では特に大きな問題点はなく、概ね情報セキュリティポリシー及びその関連規程に則った運用が実施されていることが確認できました。なお、発見された問題点や課題については、当事者に対して速やかに対策を講ずるよう、指示が行われています。

エ）教育・啓発

当省では、職員が守るべきルールとして、「情報セキュリティポリシー」、「国土交通省行政情報システム管理運営規則」を定めています。また、情報セキュリティポリシーの中から特に重要なポイントをまとめた「情報セキュリティ確保のためのお役立ち５つのポイント」のほか、ＰＣに関するパスワード設定方法、暗号化の方法等、ウィルスチェック方法等の関連情報を整理し、イントラネットに掲載しています。

また、不審メール対策として、一定の基準に基づくシステムでの自動破棄や、メッセージの挿入等による注意喚起を行い、セキュリティの確保に努めました。

併せて、標的型メール攻撃に関する教育・意識啓発のため、同攻撃に対し適切な対処が出来ることを目的とした擬似メールを用いた訓練を実施しました。

職員に対する研修としては、情報ネットワーク・セキュリティ基礎研修を年２回実施し、「国土交通省情報セキュリティポリシーの概要」についての講義を実施したほか、他の研修においても、可能な限り、情報セキュリティに係る内容を盛り込むことに努めています。

オ）その他取り組んだ事項

内閣官房情報セキュリティセンター主催の標的型メール攻撃に対する教育訓練（以下「標的型メール攻撃訓練」という。）について、平成２４年１０～１２月の間、６００以上の部局、約４万人の職員が参加し、２回にわたって実施いたしました。

また、当省の情報システムにおいて、情報セキュリティインシデントが発生した際、被害を最小化するとともに、迅速な復旧支援等を行うための体制として、平成２５年２月、総合政策局内に外部専門家であるインシデントアドバイザーを擁する国土交通省CSIRT（情報セキュリティインシデント対応チーム）を設置しました。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

国土交通省においては、万一情報セキュリティに関する障害・事故等が発生した場合、「障害・事故等報告及び対処手順」及び「緊急連絡網」に基づき対処することと定めています。

具体的には、行政事務従事者が情報セキュリティに関する障害・事故等を発見した場合、障害・事故等の内容に応じて、システム管理者または情報セキュリティ担当者に報告を行い、報告を受けたシステム管理者又は情報セキュリティ担当者は、情報セキュリティ責任者の承認の下、対処の指示及び関係者への連絡を行います。さらに、対処完了後に再発防止策を策定した上で、統括情報セキュリティ責任者に報告します。

なお、サイバー攻撃に係る情報の集約及び共有の一層の徹底を図るため、サイバー攻撃に関する情報を検知した場合には、内閣官房情報セキュリティセンターに速報することとしています。

イ）公表した障害・事故等の概要、それに対する対応等

○情報セキュリティに関する障害・事故等の把握
　平成２４年６月２６日（火）２１時２０分頃
○概要
　Ｗｅｂページが改ざんされたことにより、閲覧が不可となりました。
○障害・事故の原因
　Ｗｅｂサーバで使用しているソフトウェアの脆弱性を利用されたものです。
○府省庁の対応
　当該サーバを廃棄するとともに、侵入防止システムにおいて、Ｗｅｂサーバで使用しているソフトウェアへの不正アクセスを検知するための設定を実施するとともに、各事務所等に対して、各ソフトウェアのセキュリティパッチを最新にするよう依頼しました。
　また、公開サーバセグメントのセキュリティ対応状況について調査を実施し、セキュリティに脆弱性のあるサーバについての調査を実施しています。
○原因が省庁対策基準違反によるものか否か
　否
○再発防止策
　侵入防止システムによる対策を行うほか、新たなサーバを導入するとともに、システムを再構築します。

最高情報セキュリティアドバイザーからのメッセージ

昨今、日増しに情報セキュリティの脅威が高まっています。標的型メール攻撃による事案発生は枚挙にいとまがありませんし、また最近では２０１３年３月韓国における大規模なサイバーテロの発生は我々に大きな衝撃を与えました。情報セキュリティの推進は、技術的対策と人的な対策が車の両輪と言われていますが、どの様な攻撃であれその防御が強固であればあるほど、攻撃者は人間の弱みや習性を利用して攻撃をしかけてくるものです。その様な意味で「標的型メール攻撃訓練」は人的対策の一つの柱と言えるものです。国土交通省では昨年度に引き続き今年度も６００以上の部局、約４万人の職員を対象として２回の「標的型メール攻撃訓練」を実施しました。結果としては開封率０％は望むべくもありませんが、２回の訓練で開封率が大きく低減した事により、訓練の効果は大いにあったと評価しています。また国土交通省の一部の組織では毎月訓練を行うなど各組織の自主的な取組も実施され、情報セキュリティの重要性が認識されて実行に移されたと高く評価しています。本年度も引き続き「標的型メール攻撃訓練」を行い、情報セキュリティ意識の継続的な定着に努めていきたいと考えています。

また、昨年度は情報セキュリティインシデントの発生に対応する CSIRT を本省で組織化しました。これは国土交通省における、①情報セキュリティインシデント関連情報の集約と対処活動の効率化、②国土交通省全体としての情報セキュリティ水準の向上、③国土交通省の情報セキュリティに関する内外に向けたメッセージの発信、④他の組織との情報セキュリティに関する連携の構築、を目的として設置したものです。本年度はこの CSIRT の活動をより実のあるものにするため、国土交通省の各組織における情報セキュリティ責任者との連携を強化し、またそれを確実にするために訓練等も実施して行きたいと考えています。

国土交通省最高情報セキュリティアドバイザー　　岸田　明
平成２５年６月１０日

20 環境省

最高情報セキュリティ責任者からのメッセージ

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。また、平成 24 年度においては、原子力規制委員会が設置されたことで新たに重要な任務を担うこととなり、これらの業務遂行する上で取り扱う情報の管理や業務を支援する大小様々な情報システムを運用しています。

業務で取り扱う情報や情報システムを適切に管理し、利用するためには、Plan（計画）→ Do（実行）→ Check（評価）→ Act（改善）という、いわゆる PDCA サイクルを取り入れた情報セキュリティ対策に取り組む必要があります。環境省は、これまでも、以下の点を中心に情報セキュリティ対策に努めてきました。

(1) 情報の機密性の格付け等、取り扱いの徹底
(2) 情報システムによる技術的対策
(3) 情報セキュリティ対策の実施状況についての自己点検と監査

平成 24 年度においては前年度に引き続き、なりすましメール対策の強化や、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、職員の意識向上のための研修や注意喚起等を実施しました。特に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が浸透し、私物の USB メモリの利用禁止の徹底が進むなど一定の効果を上げているものと思われます。また、情報システムの機器の更新に合わせ、サイバー攻撃への監視体制の強化を図りました。

一方で平成 24 年度においては、委託先における個人情報の漏えいの問題や運営を外部に委託していた個別業務のホームページが外部から改ざんされるという事案が発生しました。これらに対しては直ちに原因の調査、対策の検討を進め、外部委託先の一層の管理、指導、省内への注意喚起を行うとともに、システム上の対策については、他のシステムにおいても外部からの攻撃への対策が十分であるか、改めての確認を進めることにより再発防止とともに情報セキュリティ対策の質の向上に努めてまいります。

平成 25 年 5 月 7 日
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

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

平成 24 年度は、平成 22 年度から整備を行っていたセキュア USB メモリやオンラインストレージシステムについて本格的な利用が始まりました。また、自己点検の結果や監査の内容を見てもまだ十分とは言えないものの、職員の情報セキュリティに対する意識についても徐々に高まってきている様子が窺えました。

一方で、情報セキュリティ障害・事故が発生してしまい、関係する方々に多大なご迷惑をおかけしてしまいました。自己点検や監査で明らかになった課題も含め、情報セキュリティ対策の改善に努めました。

イ) 平成 25 年度の目標

平成 25 年度は、以下の事項を重点的に取り組む目標とします。

- セキュアな Web メールの円滑な導入
- 情報セキュリティ障害・事故への対応と他のシステムへの水平展開
- 職員の情報セキュリティ意識の向上とシステム的な対策の利用促進

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

平成 24 年度の自己点検の結果は、把握率が 96.4%、実施率は責任者等が 98.0%、システム責任者等が 95.6%、行政事務従事者が 91.0%でした。実施率は、いずれの区分においても前年度から向上していました。

これらのことから概ね適切に情報セキュリティ対策が実施されている状況を確認しましたが、さらに実施率を高めていくことが必要です。

特に、書類を作成する際に情報の機密性や取扱制限等を明示するという対策については、前年度の自己点検で確認された課題であり、機密性表示の例や解説を示したテンプレートファイルの配布等の改善策を行っておりますが、まだ相対的に低い傾向が見られます。

機密性や取扱制限等の明示の他実施率が低かった項目については、次年度に向けた課題として、情報セキュリティに関する教育の重点項目とするなど、引き続き周知していくことが必要と考えています。

イ) 情報システムごとの状況

平成 24 年度の重点検査では、公開用 Web サーバ、メールサーバ、ドメイン、ネットワーク等を対象に情報セキュリティ対策の実施状況を確認しました。

公開用 Web サーバ、メールサーバについては、通信の暗号化、サービス不能攻撃対策、修正プログラムの適用、計画停電への対応等といった対策の実施率は 100%となっていました。

また、ネットワーク等についても標的型攻撃への出口対策の実施率が 100%となっていました。

一方で、ドメインについては、送信ドメイン認証技術の導入の実施率が 97.6%となっており、ごく一部のサーバで対策が未実施となっていました。

前年度までの重点検査では対策事項の実施率が 100%でしたが、平成 24 年度については 100%を達成していない事項がありました。対策未実施のサーバに関しては速やかに対応を行うことが必要と考えています。

ウ）監査の状況

平成 24 年度は、2013 年 2 月～3 月に、外部事業者に委託して、規程類の査読調査、インタビュー調査及び実地検査、脆弱性診断による情報セキュリティ監査を実施しました。

その結果、規程類の査読調査においては、環境省情報セキュリティポリシー、環境省情報セキュリティ対策マニュアル等に重大な不備はありませんでした。

インタビュー調査及び実地検査においては、メールの転送やセキュア USB 利用の際の取り扱い方法、書類の保管状況に大きなリスクがあることが検出されました。また、情報の格付けの表示、メール送付の際のパスワード設定、パソコンの盗難防止対策についても指摘事項として上がりました。これらの指摘事項への改善策として、セキュアな Web メールの導入を円滑に進めていくことや、平成 23 年度に行った文書のテンプレートの配付やセキュア USB メモリの導入などシステム的な対策について再度周知するとともに、毎年の研修や随時の注意喚起を行い対策実施の徹底などを、平成 25 年度当初から順次改善策を実施していく予定となっています。

脆弱性診断においては、一部のサイトにおいて、危険性の高い脆弱性として、SQL インジェクション及びクロスサイトスクリプティングの脆弱性が検出されました。この結果を受け、脆弱性が検出されたサイトの運用継続の必要性や代替手段での対応の可否を検討し、速やかに当該サイトを閉鎖するとともに、代替手段による対応を行うなど、直ちに改善策を実施しました。

エ）教育・啓発

平成 24 年度は、年度当初に新規採用者、転入者に対する集合研修を行い、環境省の業務を行うに当たって遵守する事項として環境省情報セキュリティポリシーや環境省情報セキュリティ対策マニュアルの内容を基に全般的に説明を行いました。

e ラーニング研修については平成 24 年 12 月から平成 25 年 1 月にかけて全職員を対象として行い、前年度の自己点検や監査の結果を踏まえて特に注意すべき点等を重点的に説明しました。

そのほか、省内外での情報セキュリティ事案に関する情報・事例を収集して、随時メールや省内の電子掲示板への掲載によって全職員に向けた注意喚起を行っています。また、各システムを管理する情報セキュリティ管理者や新規採用者に向けては、総務省における IT 研修の受講を推奨し、セキュリティを含めた関連知識の向上に努めています。

オ）その他取り組んだ事項

環境省では東日本大震災以降、外部での打合せなどのため職員が省外で業務を行うことが大幅に増えており、外出先でスムーズにメールのやり取りを行うことが業務上重要な事項となっていることから、平成 24 年度には、セキュアな Web メールの導入に向けて手続きや機能に関する検討を進めました。セキュアな Web メールは平成 25 年度中には利用を開始できる見込みとなっており、外出先等で業務を行う場合や緊急時の対応など、省外でメールのやり取りが必要になる職員は、安全性を確保してメールを利用することができるようになります。

また、平成 24 年度からは、平成 22 年度から整備を進めてきたセキュア USB メモリやオンラインストレージシステムの運用が本格的に始まり、それらを利用して安全に情報の移送や提供を行っています。

そのほか、平成 24 年 11 月には、環境省ネットワークシステムの更改を行いました。更改に際しては、情報セキュリティ面の向上についても検討を行っており、改ざん検知機能の導入や、外部からの不正侵入等の攻撃に対する監視サービス、通信事業者によるサービス不能攻撃の検知サービスの導入を行うとともに、ドメイン認証設定の推進やシステム構築時の技術者向けガイドラインの運用を引き続き実施しました。

C) 情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

環境省では、情報セキュリティに関する障害・事故等が発生した場合には、担当者は状況を把握の上、まず、各課室の情報セキュリティ責任者及び省内の情報セキュリティ対策を所管する環境情報室に直ちに報告します。それと同時に担当者は、統括情報セキュリティ責任者、最高情報セキュリティ責任者へ障害・事故等の状況を報告することとしています。迅速な報告とともに、以後の対策等についても検討し、再発防止策とあわせて省内へ注意喚起することで同様の障害・事故がない体制とするよう努めています。

イ）公表した障害・事故等の概要、それに対する対応等

平成 24 年度は、「エコチル調査における個人情報が記録された USB メモリの紛失」、「「CO2 みえ～るツール」サイトの改ざん」の障害・事故等が発生しました。

「エコチル調査における個人情報が記録された USB メモリの紛失」は、平成 24 年 12 月 7 日に環境省に連絡があり発覚したもので、その概要は、子どもの健康と環境に関する全国調査（エコチル調査）で高知県内の調査を担当している高知ユニットセンター（高知大学医学部内）において、調査参加者の個人情報（626 組の親子に関する住所、氏名、生年月日等）が記録された USB メモリをユニットセンターの執務室内で紛失したというものです。なお、本事故に関して個人情報の流出については確認されていません。

エコチル調査の業務を委託するにあたっては情報セキュリティ対策を実施するよう求めておりましたが、個人情報の USB メモリの保管はエコチル調査の実施手順には無く、外部委託先において情報の適切な取り扱いが行われていなかったこととなります。

本事故に関しては、高知ユニットセンターに対して、原因及び再発防止策に関する報告書を提出させました。また、環境省及び国立環境研究所（エコチル調査コアセンター）から、高知を含む全国 15 カ所のユニットセンターに対して、エコチル調査の実施手順に反して個人情報を含む書類の電子情報化を行うことのないよう改めて周知するとともに、個人情報の管理には万全を期すよう指示しました。

「「CO2 みえ～るツール」サイトの改ざん」は、平成 25 年 3 月 15 日に情報を入手して発覚したもので、その概要は、「CO2 みえ～るツール」サイト（光熱水費等の支出、くらしの改善メニュー、使用家電の型番等を入力することにより、生活に伴う CO2 排出量等を表示するウェブツール）について、委託先のサーバ上の設定ファイルが何者かに改ざんされていたというものです。

環境省では、直ちに本サイトのサービスを停止し、改ざんからサービス停止までの間に本サイトを閲覧された方に対して、お使いのパソコンについて直ちに最新のウイルス対策ソフトでスキャンするとともに、OS、PDF、Java、Flash 関連のソフトウェアについてアップデートを行い、セキュリティパッチを適用していただくことをお願いしました。

本件に関しては、詳細な内容や原因、影響等のほか、サーバの設定・運用状況に問題点等がなかったかについても現在調査を進めており、調査結果に基づいて必要な対応を進めてまいります。

最高情報セキュリティアドバイザーからのメッセージ

環境省は平成 24 年度に環境省ネットワークシステムの更改および原子力規制委員会ネットワークシステムの構築、環境省電子申請・届出システムの更改等を実施しました。また、情報システム担当職員は、これらの情報システムに係る業務を推進しながら、システムのセキュリティ機能の向上や、なりすましメールの対応、セキュリティ対する注意喚起、教育・指導等の取組を実施してきました。

中でも、以下に示す取組については、着実にセキュリティ水準を効果的に向上させたものとして、評価できます。

〇環境省ネットワークシステムにおける、送信ドメイン認証機能、不正な通信や侵入を防ぐ監視・分析とアクセス制御機能等の実装・整備による不正な攻撃への防御力の向上

〇セキュア USB メモリの本格利用開始によるウイルス感染や情報漏洩リスクの低減

〇オンラインストレージの普及促進による、大容量データ受け渡しにおける情報漏えいリスクの低減

しかしながら、平成 24 年度においては、公表した障害・事故が 2 件発生しました。そのうち 1 件については、平成 25 年度の計画にも記載されているとおり、他のシステムにおいても同様の危険性が存在していないかの確認及び対応を行うことにより、該当のシステムだけでなく省内全体のシステムについてセキュリティ向上に努めることが重要であり、速やかな対応が重要です。

また、緊急時対応の組織的体制として、CSIRT を整備したことは評価できます。今後、緊急時に有効に機能するかを継続的に検証・見直しを行い、実効性ある体制にスパイラルアップしていくことが重要となります。

このように、情報セキュリティのリスクは、年々高くなってきています。特に外部委託先の Web サイトにおける情報セキュリティリスクを認識し、適切な対処を実施し、インシデント発生時の速やかな対応等、国民への影響を最小限にとどめるために、着実に取組を推進することが重要です。

平成 25 年 5 月 7 日
環境省最高情報セキュリティアドバイザー
藪野　直子

21 防衛省

最高情報セキュリティ責任者からのメッセージ

近年政府機関や国の重要な情報を扱う企業などに対するサイバー攻撃事案が多発しています。幸いにも当省の情報システムへの被害は確認されていませんが、日々高度化・複雑化しているサイバー攻撃の増大をあらためて認識させられました。

防衛省・自衛隊が我が国の平和及び国民生活の安定・安全を確保するために各種の任務を適切かつ円滑に実施する上で、迅速・確実な指揮命令の伝達や情報共有を実現する情報システムが不可欠です。このような、防衛省・自衛隊における情報システムの安全性は国の安全保障に直結するものであるため、その確保は極めて重要であると認識しています。

平成２４年度においては、情報セキュリティ対策の実施状況に関する自己点検、職員に対する教育、情報システムの公開用ウェブサーバ及び電子メールサーバへの情報セキュリティ対策の実施状況の重点検査、所持品検査等の特別検査を実施しました。この結果、おおむね適切な情報セキュリティ対策が取られていましたが、一部に不十分な部分も見受けられており、引き続き情報セキュリティについて職員の興味や関心が持続するような施策を図っていきます。

今後とも、防衛省・自衛隊に対する国民の皆さまの期待に適切かつ確実に応えることができるよう、防衛省・自衛隊の活動にとって重要な基盤である情報システムの安全性を確保するため、情報セキュリティ対策の向上に努めてまいります。

情報保証統括責任者
（防衛省運用企画局長）
黒江　哲郎
平成２５年４月３０日

A) 平成 24 年度の総括

ア) 平成 24 年度の評価

・情報セキュリティ対策の実施状況に関する自己点検、職員教育、インターネット経由での脅威を最も受けやすい機材等に対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。
・情報システムのＵＳＢポート集中管理機能導入促進により、未登録媒体を介した情報流出やウイルス感染防止について強化されました。

イ) 平成 25 年度の目標

個々の職員がなりすましメールに対する知識と対策を身につけ、情報セキュリティ意識の向上を図るため、また、私有可搬記憶媒体の管理に関する規則違反が発生していることを踏まえ、平成２５年度には、以下の取組みを行います。

① 職員への不審メール対策に関する教育の実施
② 職員に対する不審メールを模擬したメール送付による訓練の実施
③ 私有可搬記憶媒体の管理に関する規則類の遵守の徹底

B) 情報セキュリティ対策の実施状況

ア) 省庁対策基準に関する自己点検結果

職員の情報セキュリティに関する規則の遵守状況について自己点検を行ったところ、適切に実施していることを確認しました。

今後もこの水準を維持して行けるよう、引き続き職員に対する教育を実施していきます。

イ) 情報システムごとの状況

情報システムの公開用ウェブサーバ及び電子メールサーバへの情報セキュリティ対策の実施状況の重点検査を実施したところ、十分な情報セキュリティ対策が講じられていることを確認しました。

今後も情報システムに対して各種の情報セキュリティ対策を講じていきます。

ウ) 教育・啓発

防衛省では、職員に対して毎年度一回以上情報セキュリティに関する教育を実施しています。

毎年２月を「防衛省情報セキュリティ月間」と定め、平成２４年度においては、大臣政務官からの訓示の配信、教育資料の各機関への送付及び情報セキュリティ担当者間の連絡体制の確認を行いました。

また、防衛省市ヶ谷駐屯地・基地においては、情報セキュリティ月間中に情報セキュリティを呼びかける構内放送の実施、情報システムログイン時に情報セキュリティ月間に関する画面を自動的に表示する等により、職員に対する情報セキュリティ意識の周知啓発を図りました。

エ) 調達・外部委託

・外部委託先の管理
防衛省では、契約に特約条項を適用することで、契約企業に情報セキュリティ対策の実施を求めています。また、防衛省が契約企業に求める情報セキュリティ対策

を示すとともに、契約企業の自主監査と防衛省の行う監査を通じてその確実な実施を図ることとしています。
・調達における情報セキュリティ確保の強化
　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、事案が発生した場合の防衛省への迅速な報告、セキュリティ対策及び教育・訓練についてそれぞれ強化を図りました。

オ）その他取り組んだ事項

・「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」に基づく対策の強化
・情報システムの利用者サポートの充実
・所持品検査等の特別検査の実施
・ソーシャルメディアの私的利用時の留意事項について周知

C）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

平成２４年度に公表した情報セキュリティに関する障害・事故等としましては、私有可搬記憶媒体及び私有パソコンの管理等に関する規則違反があります。なお、平成２４年度において、外部への業務用データの流出は確認されておりません。

イ）公表した障害・事故等の概要、それに対する対応等

平成２４年度に公表した情報セキュリティに関する障害・事故等に対する対応としまして、当事者に対する懲戒処分を実施いたしました。

最高情報セキュリティアドバイザーからのメッセージ

平成２４年度は、昨年度から顕在化した、国の重要な情報を扱う企業や政府機関に対するサイバー攻撃について引き続き多くの報道があり、また、遠隔操作ウイルスやインターネットバンキングを狙った攻撃の巧妙化など、サイバー空間での脅威の増大を示す年でもありました。

防衛省・自衛隊においては、従前から、サイバー攻撃対策を講じており、現在までにおいてサイバー攻撃による情報システムの異常等は発生いたしておりません。しかしながら、サイバー攻撃の脅威は増大してきているものと認識しており、引き続き、これらの施策を着実に実施していく必要があると考えております。

最高情報セキュリティアドバイザー
（運用企画局情報通信・研究課情報保証室長）
木村　和仙
平成２５年４月３０日

資料編

目　次

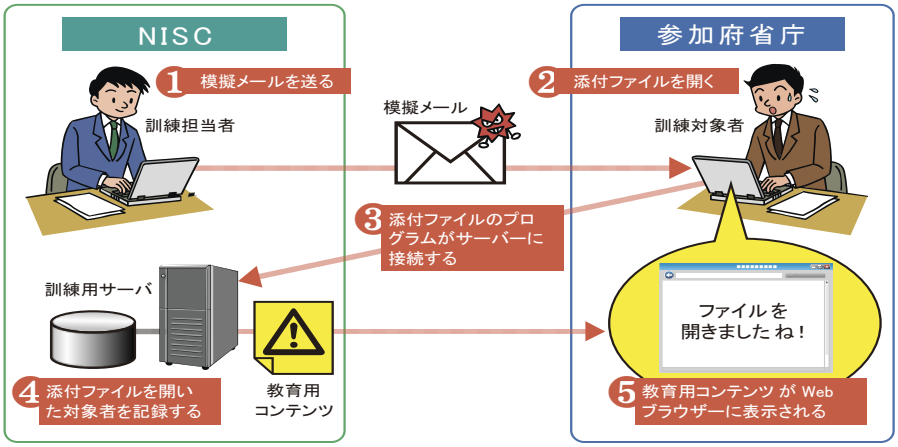
資料編A　標的型メール攻撃に対する教育訓練

1 訓練の目的・特徴

○　本訓練は、集合研修等と比較し「標的型メールを体験する」という体験型教育として大きな効果が期待できる。
○　訓練メールを開封することにより“ヒヤリハット”体験ができ、職員に気づきを与えるなど、高い教育効果が期待できる。
○　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、昨年度よりも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）を使用する。

2 訓練の概要

○　実施期間　：平成 24 年 8 月～12 月の 5 か月間
○　実施規模　：19 府省庁　約 12 万人（各訓練対象者毎に 2 回実施）
○　実施方法　：訓練メール送信から開封の記録までの流れ



①　訓練用メールサーバより訓練対象者に訓練（模擬）メールを送信
②　訓練メールを受信した訓練対象者が以下のいずれかの操作を行う
　・訓練メールの添付ファイルを開く
　・訓練メール本文に記載された URL をクリック
③　上記②の操作を行った訓練対象者は自動的に訓練用サーバに接続
④　訓練用サーバでは、アクセスしてきた訓練対象者をデータベースに記録
⑤　訓練対象者は、表示された開封者向け教育コンテンツを閲覧
※　各訓練実施終了 1 週間後にアンケートを実施

3 訓練の結果

○　1 回目訓練　開封率　　14.6%
○　2 回目訓練　開封率　　10.6%

4 結果の分析

○　訓練メールを巧妙化したことにより、開封率は昨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より多くの職員が“ヒヤリハット”を体験することができた。
○　２回目の訓練では、１回目の訓練と比較して開封率が低下した。
➢　開封率は、訓練メールの難易度等により変動。

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 まとめ及び今後について

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。

ただし、巧妙な標的型メール攻撃への対処を全ての職員に完璧に求めることは困難である。

したがって、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訓練を行うことが重要である。

また、訓練効果は一時的なものであり、時間の経過とともに意識レベルは低下するため、今後も継続的な意識啓発が必要である。

今後は、訓練のノウハウを取りまとめ、各府省庁が自ら訓練を実施出来るような取組も推進していく必要がある。

資料編B　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不正プログラム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」[35]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24年度については、「情報セキュリティ２０１２」[36]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」[37]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の採用を推進した。

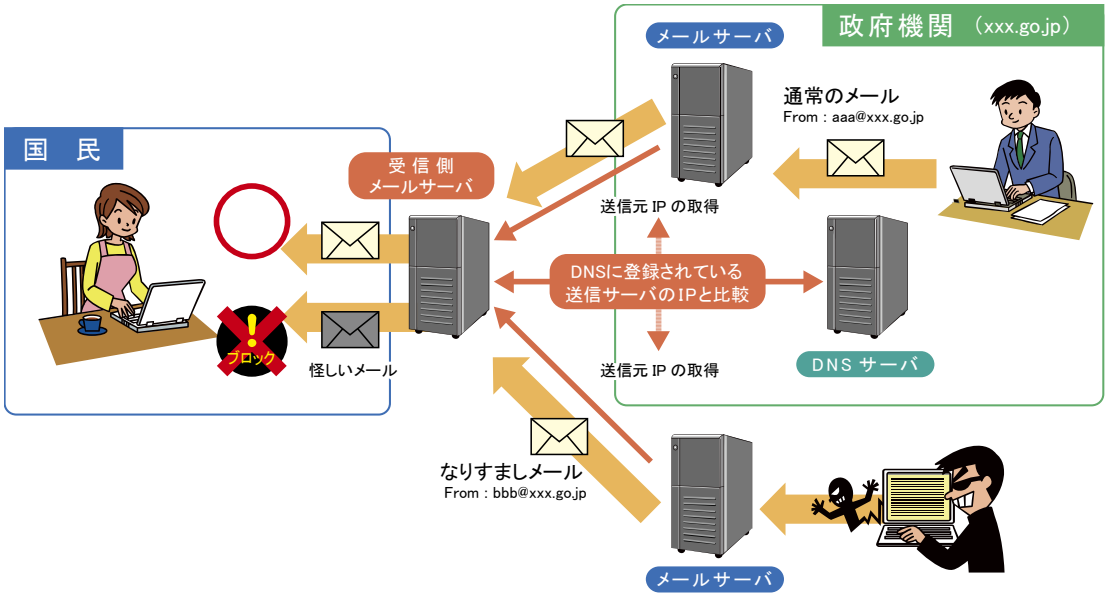


図 B-1　SPF を活用したなりすまし対策の概要

図B-1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[38]に公開する。受信側では、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。

[35] 平成21年2月3日情報セキュリティ政策会議決定
[36] 平成24年7月4日情報セキュリティ政策会議決定
[37] 平成24年4月26日情報セキュリティ政策会議決定
[38] 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。

2 取組の結果及び今後の課題

平成 24 年 10 月 26 日　第８回情報セキュリティ対策推進会議資料より一部加工

メールアドレスを詐称されないための対策の推進

これまでの主な取組

- 本省、外局、地方支分部局、独立行政法人等において、送信側SPFの導入を推進
- 主な取組内容
  ①DNSサーバにSPFレコードを記載
  （メール送信を行わないものについては、その旨のSPFレコードを記載）
  ②利用していないgo.jp ドメインについては、廃止

送信側SPF設定の現状

平成25年６月７日現在

	「-all」	「~all」	設定なし
第3レベル（xxx.go.jp）ドメイン	79．9%	13．0%	7．0%
第4レベル（yyy.xxx.go.jp）以上のドメイン	43．4%	6．7%	49．9%

今後の課題

- **送信側におけるSPF対策の推進**
  ⇒**第４レベル（yyy.xxx.go.jp）以上のドメイン**についても、DNSサーバへのSPFレコードの記載を徹底
  ⇒SPFレコードの末尾は” ~all ”ではなく、” –all ” を記述
  ”-all”：メールを送信するサーバのIPアドレスを明確に宣言
- **受信側におけるSPF対策の推進**
  ⇒メールサーバ等の更新時期に合わせて、**受信側SPF機能を導入**
  ※サブドメインも含め電子メールを利用しているドメインの約78%で導入（第２編第１節重点検査結果より再掲）
  ⇒SPF判定結果を**メール受信者が一目で分かるような周知方法（件名に「meiwaku」等）の検討**
- **SPF以外の対策技術の導入検討**
  ⇒暗号技術を利用する、**より強固な対策技術DKIM**のSPF対策との併用　等

資料編C　公開ウェブサーバの脆弱性検査

ここでは、平成 24 年度に 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ついて記述する。

1 検査の目的

インターネット上に公開されたウェブサーバは常に脅威にさらされており、公開ウェブサーバを狙った攻撃が依然として発生している。このため、公開ウェブサーバは、脆弱性がなく安全性の高い状態を維持し、脅威への対策を講じておくことが重要である。

本検査は、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、その結果等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を目的として実施した。

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判断した。

D) 検査期間

平成 24 年 9 月～平成 25 年 2 月

E) 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[39]（約 300 画面）

F) 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脆弱性の有無を確認した。

G) 検査内容

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。

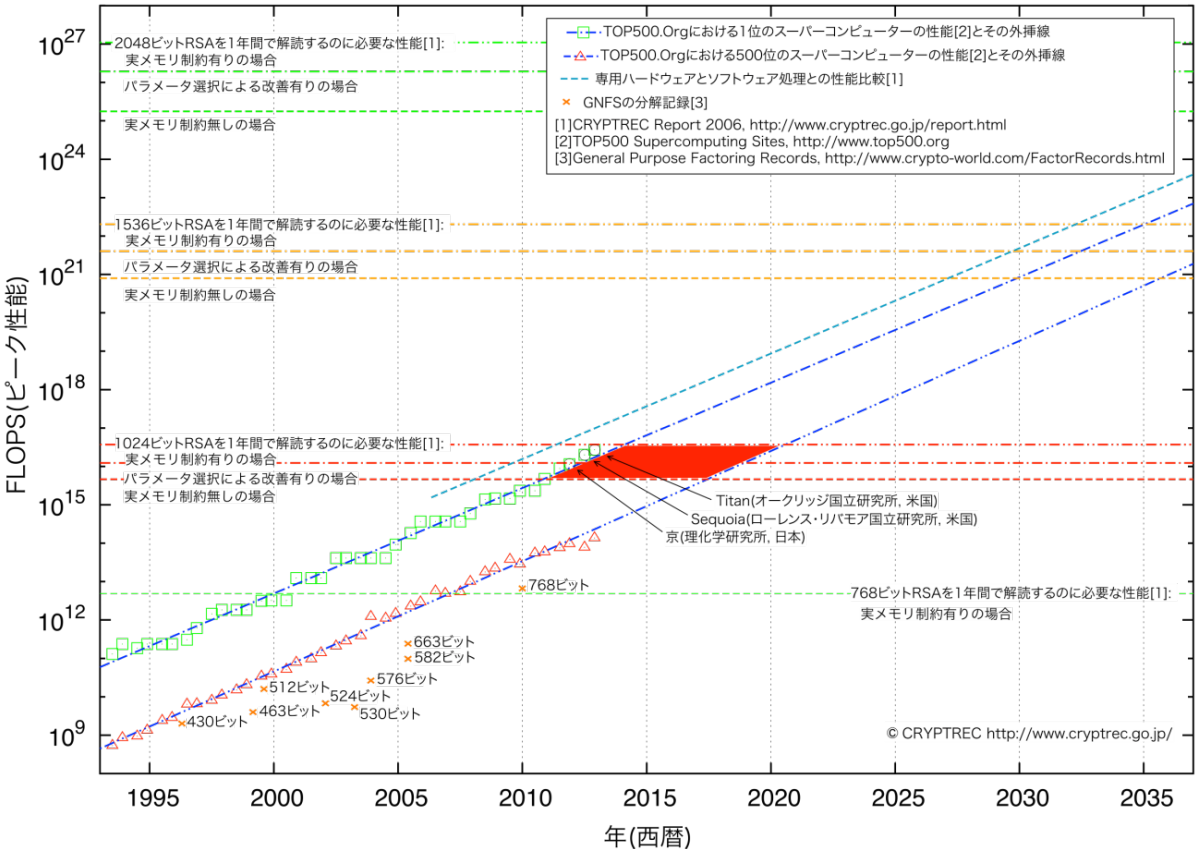
3 検査概要の概要

検査の結果、CVSS を基にした 4 段階の評価基準のうち、最も危険性の高い「危険度高（CVSS 基本値：7.0～10.0）」の脆弱性は検出されなかった。平成 23 年度の検査ではこのレベルの脆弱性が検出されていたところであり、その対策が進んでいる。また、「危険度中（CVSS 基本値：5.0～6.9）」の脆弱性として、クロスサイトスクリプティングの脆弱性が 10 画面（検査対象画面数の 3%程度）検出された。これらについては計画的に対応を進めており、順次対応を終えているところである。

[39] 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。

1 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暗号アルゴリズム RSA（鍵長 1024 ビット）については、今後数年から十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。



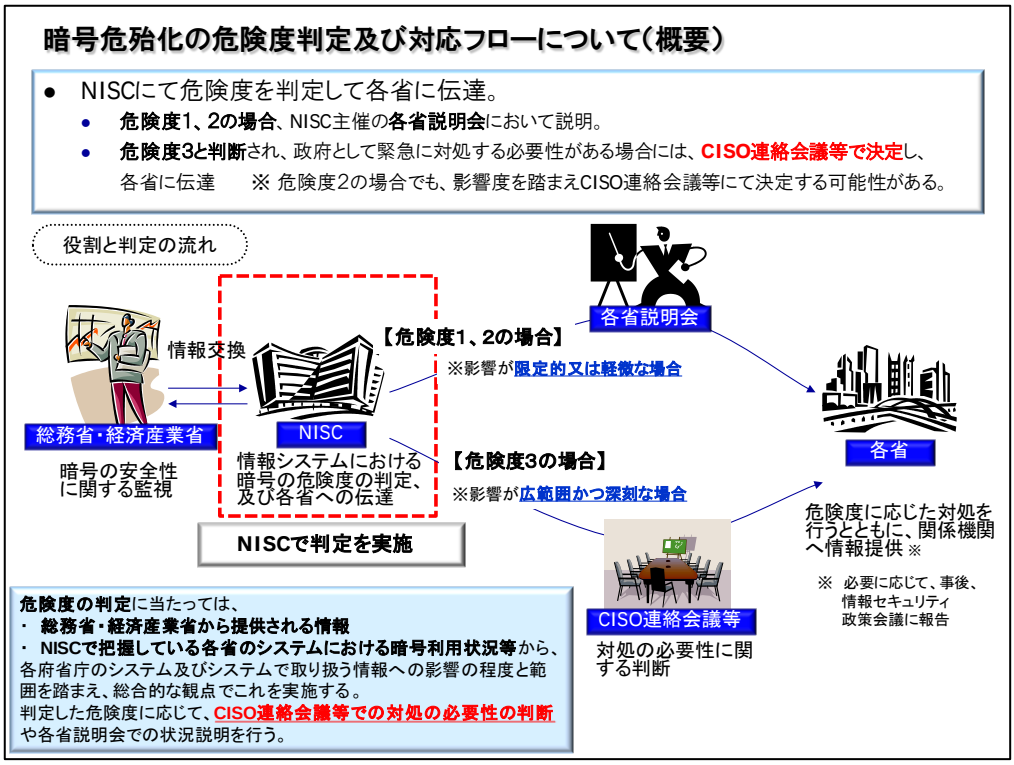
図D-1 一年間でふるい処理を完了するのに要求される処理性能の予測（平成 23 年 12 月更新）[40]

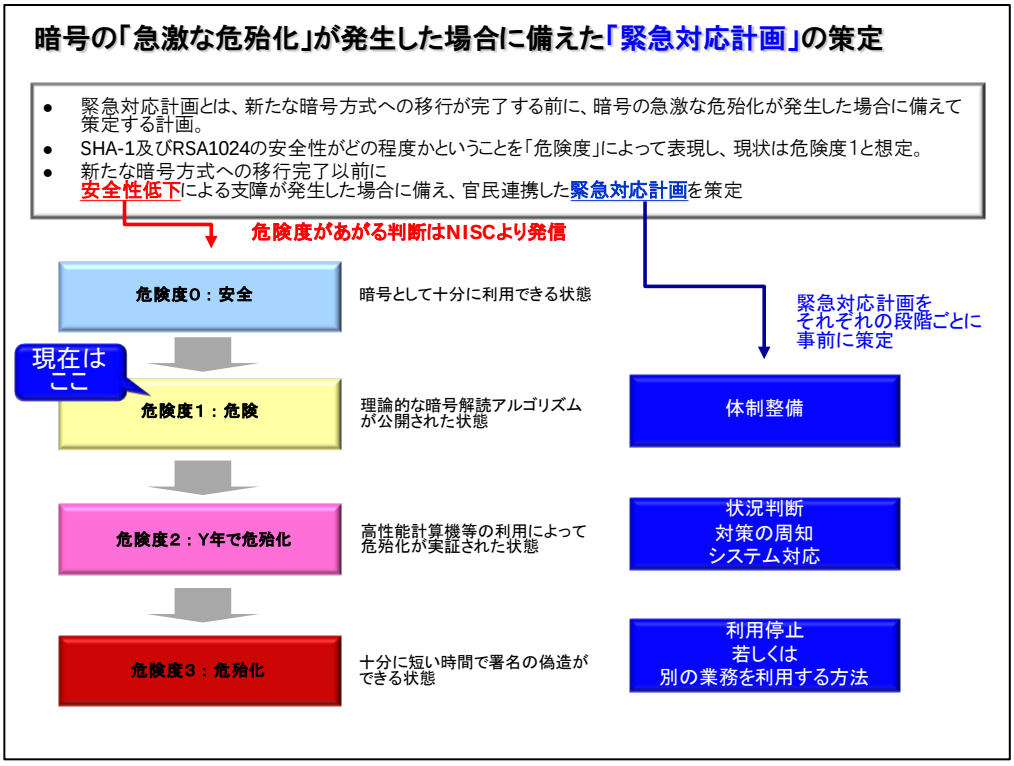
図 D-1 は、計算機の出現年数に対して演算性能をプロットしたものである。出現当時、世界トップの性能を持つ計算機については（□）、500 位相当の計算機は（△）によりプロットされている。両者とも過去 20 年にわたりムーアの法則に近似した指数的発達を示しており、今後も同様の発展が予想される。また、（×）は学術会議等で報告された、実際に各ビット数の素因数分解を達成した計算機の演算性能をプロットしている。
2012 年現在、仮にメモリを無制限に利用できる環境を仮定する場合においては、既知のアルゴリズム（一般数対ふるい法）を用いて 1024 ビット素因数分解を 1 年間で実行するのに匹敵する演算性能が、京により達成されている。

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

2 暗号危殆化の危険度判定及び対応フロー

平成 24 年 4 月、暗号の危殆化の進行に伴う政府機関内の危険度判定とその情報の伝達フローを策定・決定した[41]。





[41] http://www.nisc.go.jp/conference/suishin/index.html#2012_2
「第 5 回会合」（情報セキュリティ対策推進会議（CISO 等連絡会議）、平成 24 年 4 月 18 日）

暗号危殆化の危険度判定及び対応フローについて

平成 24 年４月 18 日
情報セキュリティ対策推進会議決定

暗号危殆化の危険度判定及び対応フローは次のとおりとする。

１　総務省及び経済産業省は、SHA-1 及び RSA1024 の安全性に関する監視を行い、内閣官房情報セキュリティセンター（以下「NISC」という。）への情報提供を行う。
２　NISC は、前項１により総務省及び経済産業省から情報提供を受けた場合は、提供された情報及び NISC で把握している各府省庁の情報システムにおける暗号利用状況等から、各府省庁の情報システム及び情報システムで扱う情報への影響の程度と範囲等を総合的に勘案し、その安全性を別表に示す「危険度」の０～３により判定する。
３　NISC は、前項２の判定の結果、「危険度」に変更がある場合は、変更後の「危険度」に応じて以下の対応を行う。
(1)　変更後の「危険度」が１又は２である場合、各府省庁に対する説明会を開催し、情報提供を行う。
(2)　変更後の「危険度」が３である場合、情報セキュリティ対策推進会議（以下「CISO 等連絡会議」という。）等を開催し、情報提供を行う。CISO 等連絡会議において、対処の必要性に関する判断を行う。
４　各府省庁は、前項３により情報提供を受けた場合は、「危険度」に応じて緊急対応計画の発動等必要な対処を実施するとともに、関係機関へ情報提供を行う。実施した対処内容については、必要に応じて、情報セキュリティ政策会議及び CISO 等連絡会議に報告する。

（別表）「危険度」の定義

危険度	状態	危険度に応じた対処の例
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

3 暗号移行指針の改定

平成 24 年 10 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」を改定した[42]。

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

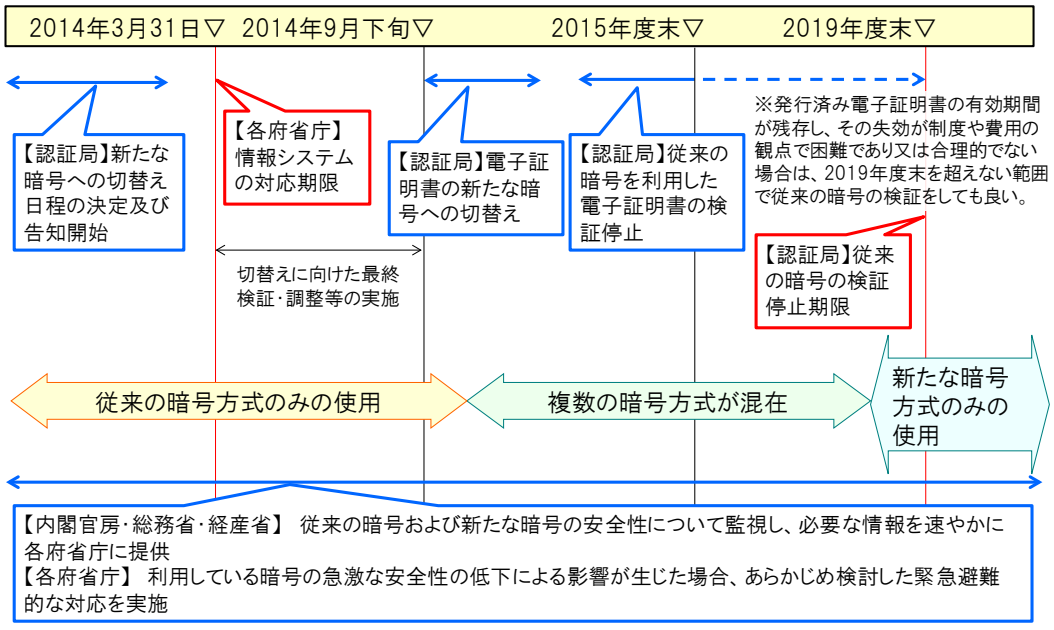
  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  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



[42] http://www.nisc.go.jp/conference/suishin/index.html#2012_5
「第 8 回会合」(情報セキュリティ対策推進会議 (CISO 等連絡会議)、平成 24 年 10 月 26 日)

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。

4 電子政府推奨暗号リストの改定

平成 25 年 3 月、これまで電子政府で利用される標準の暗号技術として利用してきた「電子政府推奨暗号リスト」（平成 15 年 2 月 20 日公表）を 10 年振りに改定し、新たに「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」を策定・公表した[43] [44]。

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	3-key Triple DES(注3)
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。
[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

1

[43] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000038.html
「「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の公表」（総務省、平成 25 年 3 月 1 日）

[44] http://www.meti.go.jp/press/2012/03/20130301004/20130301004.html
「「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」を公表します」（経済産業省、平成 25 年 3 月 1 日）

（注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20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注2） より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注3） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67 として規定されていること。
2） デファクトスタンダードとしての位置を保っていること。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（注5） KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6） より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

（注7） 平文サイズは64ビットの倍数に限る。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC(注11)
エンティティ認証		該当なし

（注8） 「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 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 128-bit RC4 は、SSL（TLS 1.0 以上）に限定して利用すること。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

平成24年度IT-BCP調査結果の概要

概　要

NISCは、平成23年3月、災害時等における政府機関の業務の継続性確保のため、「情報システム運用継続ガイドライン」（IT-BCPガイドライン）を示し、計画策定に当たっての定型的な手順・ひな形を各府省庁に提示。
これを踏まえて、平成24年度は、業務継続計画（BCP）とIT-BCPとの結び付きが重要であるとの観点から、事例調査及び文献調査を実施し、①計画の策定過程における留意事項や有効な取組を整理した「IT-BCP策定モデル」、②IT-BCPガイドラインに示された各種対策をより具体的に解説した「個別対策例」、としてそれぞれ取りまとめ。
各府省庁では、これらをIT-BCPガイドラインを補充する資料として活用し、より実効的な計画の策定・見直しにつなげる。

対象情報システムのモデル化

情報システムとして、次の2つを想定し、それぞれの特徴を踏まえつつ、必要な取組を検討。

モ　デ　ル	概　　要
個別業務システム	・個別業務に対して構築される情報システム（業務システムに共通に利用する情報システム基盤の全部又は一部も含む） ・同システムの構築・運用の担当部門は、業務を担当する部門と同一の部局
組織全体の情報システム基盤	・組織全体の情報システム基盤（省庁内ネットワーク、認証基盤、メール等） ・同システムの構築・運用の担当部門は、現場部局とは異なる部門（大臣官房総務課、情報システム課等）

平成24年度IT-BCP調査結果の概要

判明した課題とその対策①

	課　　題	必　要　な　対　策
①	業務部門等との連携 →情報システム部門のみでの計画を検討・策定　等	実効性のある計画を策定するには、情報システム部門単独で検討するのではなく、業務部門等とともに、目標復旧時間や対応手順、情報セキュリティレベル等を検討することが重要。CIO・CISOの指導の下、適宜CIO・CISOの承認を得ながら進めることも有効。 個別業務システムの担当部門では、業務部門における非常時優先業務を特定→対象業務が利用する情報システムの洗い出し→各業務の目標復旧時間、代替の有無の確認→情報システムの目標復旧時間を設定、の手順で検討。 組織全体の情報システム基盤の担当部門では、所管の情報システム基盤を洗い出し→基盤を利用している業務システムの洗い出し→業務システムの目標復旧時間の確認→情報システム基盤の目標復旧時間を設定、の手順で検討。 検討に当たっては、次表⑤のとおり、人間系でしばらく継続できる代替手段の検討が重要。
②	危機的事象、被害の想定 →対応困難な事象が検討事項に含まれていないケース　等	個別業務システム及び組織全体の情報システム基盤の担当部門ともに、業務継続計画を踏まえつつ、災害時の社会環境や情報システムの稼働に必要なリソースが制限されている状況を前提とした検討が必要。 対応困難な事象については、業務部門との間で代替手段の有無等を確認するなど、上記の連携による検討が有効。また、検討事項が残された場合においても、そのことを認識し続けることが必要である。

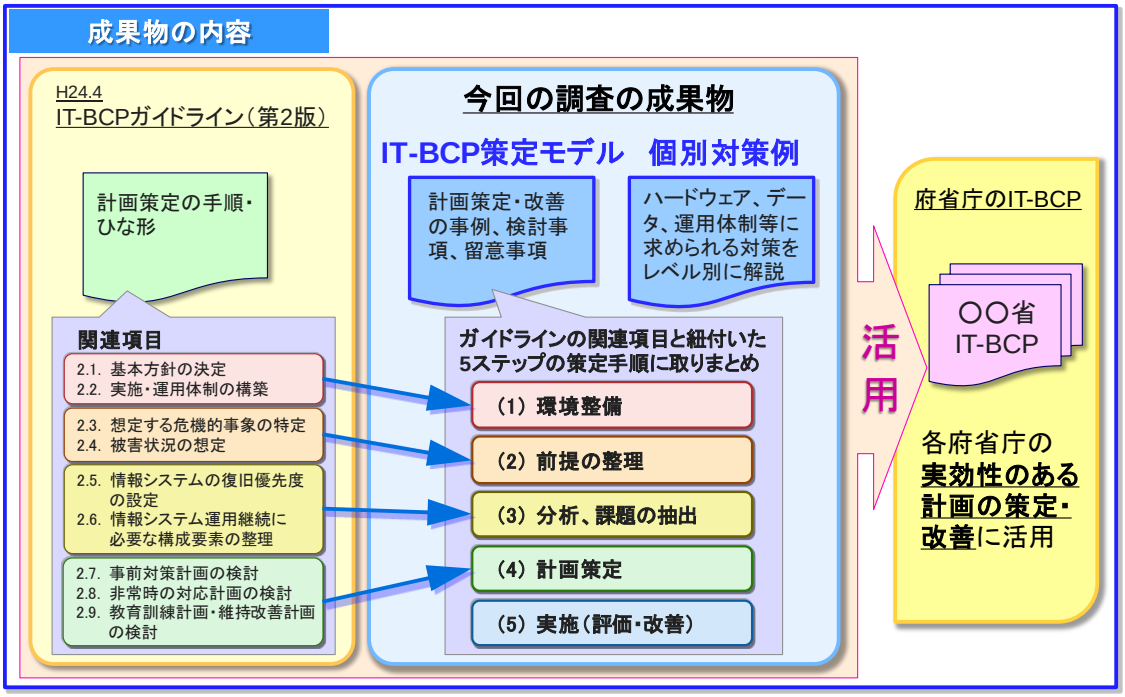
平成24年度IT-BCP調査結果の概要

判明した課題とその対策②

	課　　題	必 要 な 対 策
③	**教育訓練** →教育訓練が未実施　等	教育訓練は、計画が有効に機能するかどうかを実証できる重要な取組。 教育訓練で判明した問題点から改善につなげるとともに、対処手順等に習熟していくことが必要。 教育訓練においては、非常時対応能力の向上、事前対策内容の動作確認、検証を目的に、比較的簡易に実施できる机上訓練（読み合わせ、研修等）や、実働訓練（総合訓練、システム復旧訓練等）を計画的に実施することが必要。
④	**データ消失回避の対策** →同時被災しない場所へのデータ保管が不十分　等	業務再開時に必要なデータが消失しないように、同時被災しない場所にデータを保管しておくことは、システムの復旧優先度にかかわらず、実施すべき対策として位置付け。
⑤	**代替手段の検討** →手作業等による代替手段も対策の選択肢であるものの、これらを含めた検討が不足等	個別業務システム担当部門は、業務部門と協議の上、情報システムを利用しない手作業等による代替（電話やFAX等）が可能な場合は、情報システムの目標復旧時間を大幅に調整できることに留意。 東日本大震災時における対処業務において、初期段階では情報システムを介さず、電話、手書きメモ、FAXを活用する事例も確認。

平成24年度IT-BCP調査結果の概要

成果物の内容



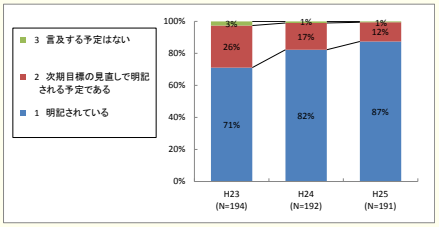
独立行政法人等の情報セキュリティ対策の現状について

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（191法人）
調査時点：平成25年3月末時点　（参考）前回調査:平成24年3月末時点に192法人

情報セキュリティ2012（2012年7月4日 情報セキュリティ政策会議決定）

Ⅳ 具体的な取組
3 政府機関等の基盤強化
コ 地方公共団体、独立行政法人等における情報セキュリティ対策の促進
(エ) 独立行政法人等における情報セキュリティ対策の推進（独立行政法人等所管府省庁）
a) 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) 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

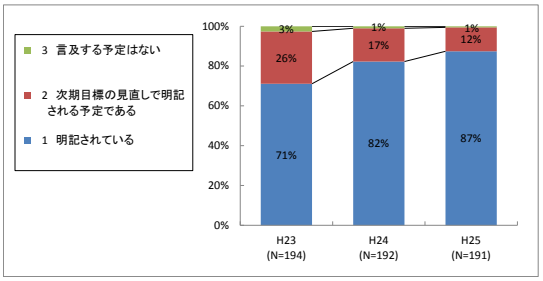
項番	対策内容	状況	H23(n)	H24(n)	H25(n)
1	情報セキュリティポリシーの策定	実施している	90%	92%	95%
2	情報セキュリティポリシーの見直し	実施している	81%	89%	92%
3	情報セキュリティポリシーの遵守状況の把握	実施している	79%	80%	82%
4	情報セキュリティ対策の中期目標への明記	実施している	97%	99%	99%
5	CISOの設置	置いている	88%	90%	92%
6	統括組織の設置	置いている	97%	97%	98%
7	注意喚起等に関する連携体制の整備	整備している	100%	100%	100%
8	職員の情報管理対策	実施している	92%	94%	96%

・解散予定(1%)を除きすべての法人が中期目標へ明記（又は明記予定）となっており、明記の割合も着実に増加している。
・情報セキュリティ対策に係るPDCAサイクルについては、対策実施状況の点検等による遵守状況の把握とそれに伴うポリシーの見直しが十分とは言い切れないところ、引き続き、独立行政法人等においてPDCAサイクルが徹底されるよう、所管する府省庁へのさらなる要請と必要な支援を行う。

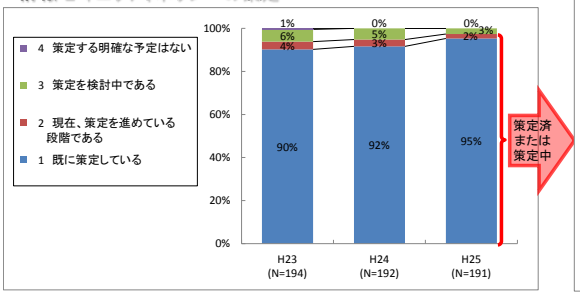
＜中期目標への明記及び情報セキュリティポリシーの策定状況＞

中期目標への明記を行っている法人数が増加（82%→87%）しているが、明記予定としている法人（12%）について、確実に中期目標へ盛り込まれるよう、引き続き取組みが必要である。なお、言及する予定はないとしている法人（1%）は解散予定である。また、情報セキュリティポリシーを策定中又は策定検討中の法人について、確実に結論を得るよう各府省庁には求めていくことが重要である。

情報セキュリティ対策に係る中期目標への明記（再掲）

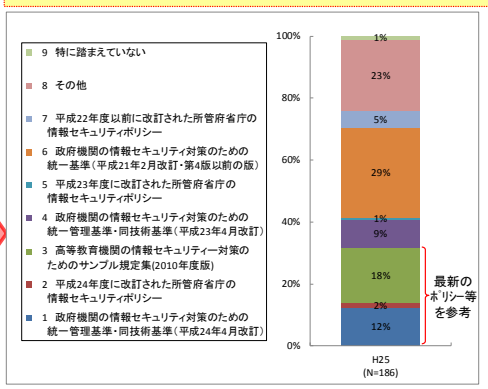


情報セキュリティポリシーの策定



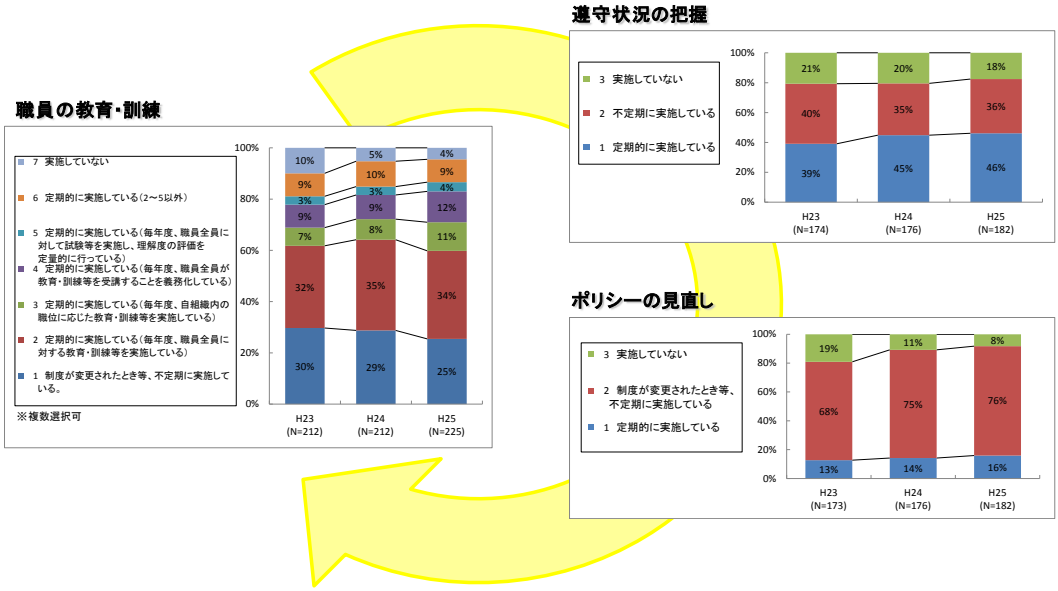
他の情報セキュリティポリシーの参照状況

（参考）『その他(選択肢#8)』の主なもの：
・政府機関の情報セキュリティ対策のための統一基準群（平成21年2月改訂・第4版以前）
・情報セキュリティポリシーに関するガイドライン（平成12年 情報セキュリティ対策推進会議）
・高等教育機関の情報セキュリティ対策のためのサンプル規定集(2010年度版より前の版)
・大学におけるセキュリティポリシーの考え方
・ISO27001,17799系



＜情報セキュリティポリシー策定済み法人の対策実施状況＞

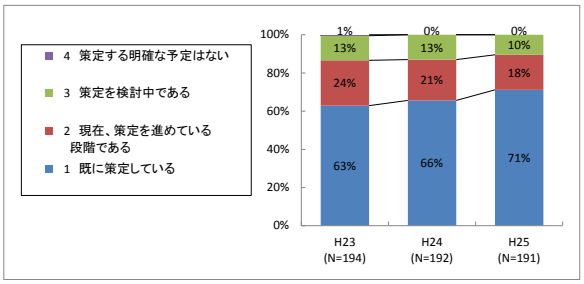
情報セキュリティポリシー策定済みの法人において、教育・訓練、遵守状況の把握、ポリシーの見直しに関する実施状況は進んでいるが、細則を検討中などの事情で、一部でこれらの対策が実施できていない法人も存在する。点検等による遵守状況の把握とそれに伴うポリシーの見直しが十分とは言い切れないところであり、引き続き、各対策について一層の対策水準の向上が求められる。



＜情報セキュリティ対策の運用に関する規程類の策定状況＞

情報セキュリティポリシーに基づくセキュリティ対策を円滑にするための規程、実施手順、マニュアル等の策定については一定の進捗が見られる。規程類の策定を検討中又は策定予定がない法人については、確実に規程類の整備が進められるよう、一層の対応強化が必要である。

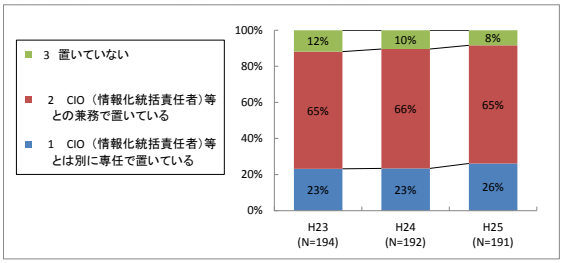
情報セキュリティ対策の運用に関する規程類の策定



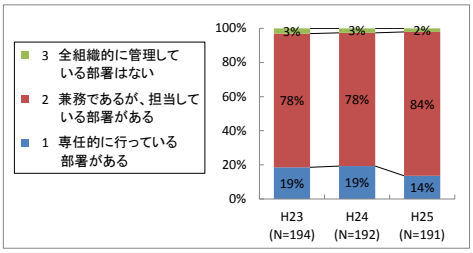
＜情報セキュリティ対策推進体制の整備＞

最高情報セキュリティ責任者（CISO）については8%の法人が設置していない（明文化されていない等）状況である。また、統括組織を設置していない法人も2%存在する。情報セキュリティ対策推進体制の構築に向けて、確実な設置が望まれる。

最高情報セキュリティ責任者（CISO）の設置



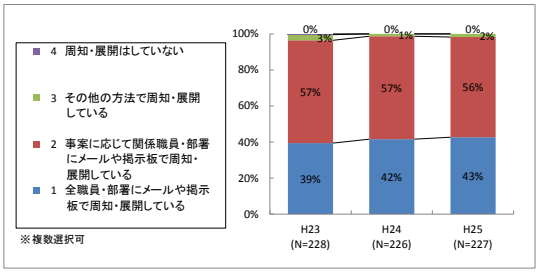
統括組織の設置



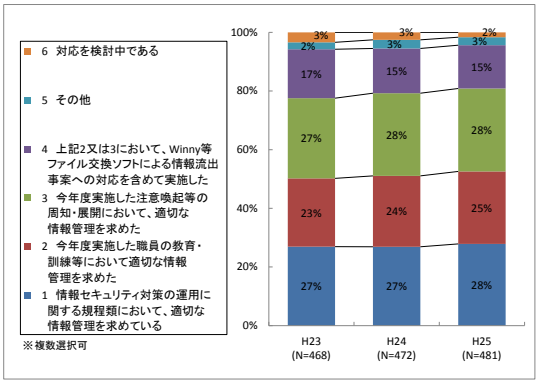
＜平常時の体制の整備＞

職員等への注意喚起等の周知・展開について対応が進み、全法人にて何らかの方法で職員等へ注意喚起等を行っている。職員の情報管理対策の徹底についても、規程類の整備や教員訓練の実施など、より実効性の高い対策を進められるようになっている。平常時の情報セキュリティ対策水準の一層の向上及び維持に向けて、引き続き対応の強化が望まれる。

注意喚起等の周知・展開方法



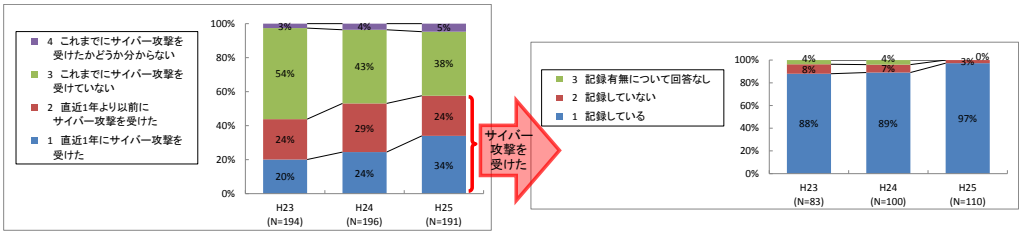
職員の情報管理対策



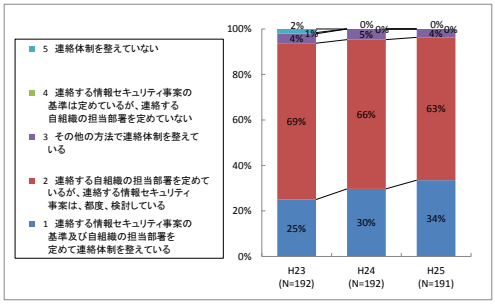
＜情報セキュリティ事案が発生した際の体制の整備＞

サイバー攻撃の認知数については年々増加しているため、攻撃を受けた場合に適切な対策がなされるよう、攻撃内容や被害状況等の記録を全ての法人において確実に実施させる必要がある。緊急時の体制構築については、所管府省庁への連絡体制及び情報システムの委託先を含めた対処等の体制整備が進んでいるが、すべての法人において事案の発生へ適切に対処できるよう、今後とも継続的な取組が必要である。

サイバー攻撃の認知と記録



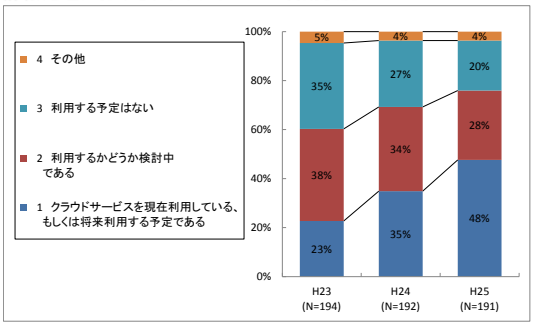
所管省庁への連絡体制



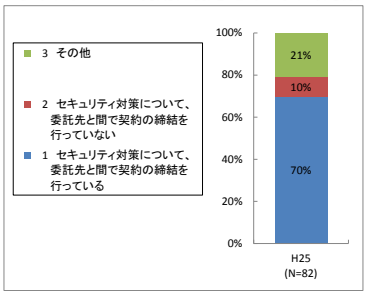
＜クラウドサービスの利用状況＞

クラウドサービスを利用（又は利用を検討）している法人は年々増加しているため、クラウドサービスの提供事業者である委託先との間でセキュリティ対策に関する契約を締結するなど、確実なセキュリティ対策が行われるよう今後も対応強化が必要である。

情報処理におけるクラウドサービス利用状況



クラウドサービス利用に係るセキュリティ対策



資料編G　NISC発出注意喚起文書

1 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）[28]

閣副安危第 373 号
平成 24 年 6 月 29 日

各府省庁等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）

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 20 日、ファーストサーバ株式会社が提供するレンタルサーバにおいて、顧客から預かっていたホームページやメール等のデータが大量に消失する事象が発生しました。この事象はサーバの管理及びバックアップに係る複数の原因が重なって起きたものです。（参考１）

つきましては、ホスティング等、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。）を利用する際、並びに各府省庁で自らデータを保管・運用する際の留意事項として、以下のとおり注意喚起をいたします。各府省庁におかれましては、以下を参考に、適切な対策を取っていただくよう、お願いいたします。

記

１．ファーストサーバ株式会社が提供するレンタルサーバ利用の有無の確認

貴府省庁において（特に地方支分部局等や委託業務等）、ファーストサーバ株式会社が提供するレンタルサーバ利用の有無をご確認ください。

２．クラウドサービス等、約款による情報処理サービスを利用する際の留意事項について

ファーストサーバ株式会社のサービスに限らず、クラウドサービスやホスティング等、約款に基づき役務の提供を受けている場合は、契約内容や約款、運用手順等を改めてご確認ください。一般的に、約款上、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。このため、利用者側である貴府省庁においても、契約内容や約款の内容を踏まえて利用するとともに、場合によっては、適切なバックアップの実施の必要性についてご検討ください。

＜管理基準 1.2.5.1 全般、1.3.1.3(1)(a)、技術基準 2.3.2.3(2)(b)＞

３．自営サーバにおけるバックアップ運用方法の再点検について

今回の事象では、本番環境とバックアップ環境に対して同時に更新プログラムを適用した結果、不具合が発生し、本番環境とバックアップ環境のいずれのデータも消失してしまう結果となったと言われております。

このため、貴府省庁において自営サーバを管理している場合においても、本番環境及びバックアップ環境に対する更新作業の運用について、今回の事象に合致する運用がされていないことを、改めてご確認ください。

1

４．所管する民間企業等に対する周知

所管する民間企業や関係団体等に対しても、必要に応じ、周知いただきますよう、お願いいたします。

（※括弧内は、対応する管理基準及び技術基準の項目を示す。）

（参考１）

・「ファーストサーバ　６月 20 日に発生した大規模障害に関する「よくあるご質問」（ファーストサーバ社）」（http://www.faq2.fsv.jp/faq/question.html）

・具体的な原因（ファーストサーバ社「大規模障害の概要と原因について（中間報告）」より引用）

① 脆弱性対策のための更新プログラムの不具合

ファイル削除コマンドを停止させるための記述漏れと、メンテナンスの対象となるサーバ群を指定するための記述漏れがあり、意図しないサーバまでメンテナンス対象となり削除されてしまった。

② メンテナンス時の検証手順の不備

検証手順ではメンテナンス対象サーバを確認すれば良いとなっていたため、検証環境の対象サーバ以外に影響が及んでいることを確認しないまま、本番環境でメンテナンスが実施された。

③ メンテナンス実施手順の不備

脆弱性対策のメンテナンスに関しては、本番環境、バックアップ環境の両方同時に更新プログラムを適用してしまい、このためバックアップ環境も消失する結果となった。（以前は本番環境のみ適用していたが、メンテナンス実施後ハードウェア障害が発生し、バックアップに切替えた途端に脆弱性対策が講じられていないシステムに戻ってしまう事象が発生したことがあり本番環境、バックアップ環境両方同時に行うようにした。）

（参考２）「約款による情報処理サービス」については、以下の統一基準群個別マニュアルも併せてご参照ください。

・「外部委託における情報セキュリティ対策実施規程　雛形付録」
http://www.nisc.go.jp/active/general/pdf/dm6-02-101_sample2.pdf

2 適切なログの管理による標的型攻撃対策について（情報提供）

（平成 24 年 7 月 5 日）[45]

閣副安危第 375 号
平成 24 年 7 月 5 日

各府省庁等情報セキュリティ担当課室長　あて
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　あて

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）

適切なログの管理による標的型攻撃対策について（情報提供）

昨今、国の機関や企業活動の大きな脅威となっている標的型攻撃への対策として、攻撃を未然に防ぐ各種対策の実施のみならず、実際に攻撃を受けた際に攻撃や被害の状況について把握ができるようにしておくための対策が重要です。そのためには、情報システムのログの取得・管理が必要ですが、ログの取得・管理に係る各種設定や運用が不十分であったため、事後の調査が困難となった事例も見受けられます。

これを受け、当センターは、昨年度、有識者による検討会を複数回開催し（検討会座長：佐々木良一　東京電機大学教授、NISC 情報セキュリティ補佐官）、標的型攻撃対策に資する適切なログ管理の在り方について、「平成 23 年度　政府機関における証跡管理の在り方の検討に関する調査報告書」として取りまとめ、NISC ホームページに公開いたしました。（http://www.nisc.go.jp/inquiry/index.html）本報告書では、各府省庁における機密性２以上の情報を扱う一般的な情報システムにおいて、比較的費用を伴わずに効果が見込める、早急に実施するべき対策の例を含めて取りまとめましたので、本事務連絡により情報提供いたします。各府省庁におかれましては、下記を参考に、担当職員や運用管理業務を委託している事業者への指導を行い、適切なログの取得・管理を行っていただいた上で、情報システムセキュリティ責任者等に運用状況を確認させることを推奨いたします。

なお、本報告書の内容については、「政府機関の情報セキュリティ対策のための統一基準群」に、適切に反映を行っていく予定です。

1

[45] http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf［PDF］
「適切なログの管理による標的型攻撃対策について（情報提供）」（NISC、平成 24 年 7 月 5 日）

記

＜括弧内は、統一基準上の関連する遵守事項を指す＞

Ⅰ．機器によらない全般的な対策

１．各ログ取得機器のシステム時刻を、タイムサーバを用いて同期する。

＜2.3.2.2(2)(d)，2.3.2.3.(2)(d),2.3.4.1(2)(e)＞

・調査時の複数機器のログの解析を迅速かつ十分に実施するため。（各ログの時刻が数秒ずれていても、これを補正する作業は大変困難である。）
・各ログ取得機器は、タイムサーバを用いた時刻同期ログについても取得する。
・精度や冗長性を高めるため、各ログ取得機器組織内ネットワークに設置したタイムサーバ（stratum2 サーバ）と代替のタイムサーバの複数のタイムサーバを利用することが望ましい。

２．ログは１年間以上保存する。

・過去の標的型攻撃事例から、攻撃事象の発見からさかのぼると攻撃の実施された時期はおおよそ 1 年以内であり、ログを１年間保存すれば、高い確率で攻撃の初期段階からのログを抽出することができるため。

３．複数のログ取得機器のログを、ログサーバを用いて一括取得する。

・攻撃者によるログの改ざんを簡便に防ぐことが出来るため。
・ログサーバのアクセス権を最小限とすることが望ましい。また、ログサーバについては、改ざん防止のために内部ネットワークに置く必要がある。
・高スペックな機器を利用する必要は無い。

４．攻撃等の事象発生が確認された場合の対処手順を整備する。

＜1.2.2.2(1)(c)＞

・攻撃等の事象発生が確認された場合に取るべき行動を検討し周知すること。不必要な行動をとってしまうことでログが上書きされ、原因究明が困難になってしまう恐れがあるため。

Ⅱ．機器別の対策

１．ファイアウォール：「外⇒内で許可した通信」と「内⇒外で許可・不許可両方の通信」のログを取得する。

・外部の攻撃者により侵入された通信と、その後のバックドア通信を把握するため。
・攻撃への対策とログ解析の効率化のため、外⇒内の通信は必要なものに限定することが望ましい。

２．Web プロキシサーバ：接続を要求した端末を識別できるログを取得する。

・バックドア通信で多く用いられる HTTP/HTTPS の情報から、C&C サーバの IP アドレス・感染端末の特定・活動の実態を把握するため。

３．他のシステムや機器の権限を管理するサーバ（LDAP, Radius 等）：管理者権限による操作ログを取得する。

・管理者権限の窃取等を把握するため。

４．メールサーバ：「メールの送受信アドレス」及び「メッセージ ID」のログを取得する。また、出来る限り「添付ファイル名」のログを取得する。

・標的型メールのログから、攻撃者に利用されたサーバやマルウェアの情報を把握するため。
・情報の窃盗（アップロード）に SMTP を利用するケースが見られるため。
・マルウェア対策ソフトウェアで検知できないマルウェアの情報を把握するため。

５．クライアント PC：マルウェア対策ソフトウェアの検知・スキャンログ・パターンファイルのアップデートログを取得する。

・マルウェアによる感染の実態を把握するため。

６．DB サーバ・ファイルサーバ：特別なログ設定は不要だが、確実にログを取得する。

・窃盗された情報等、攻撃を把握するために重要であるため。

以上

3 JavaSE 6 のサポート有効期間の満了に係る対応について（注意喚起）

（平成 24 年 7 月 17 日）[16]

事　務　連　絡
平成 24 年 7 月 17 日

各府省庁等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ブザーバー機関情報セキュリティ担当課室長等 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）

JavaSE 6 のサポート有効期間の満了に係る対応について（注意喚起）

本年 7 月 10 日付で、JPCERT コーディネーションセンターより当センター宛に注意喚起が発出されました。その内容は、Java SE 6 メジャー・リリースは、サポート有効期間の満了に伴い（参考１）、本年 12 月以降は脆弱性などを修正した「修正済みソフトウエア」の提供は行われなくなる一方、政府機関が国民向けに公開している情報システムの一部では、国民がその利用に際して JavaSE 6（または対応する実行環境 JRE 6)を国民の PC 等にインストールすることを推奨しているものがあり、注意が必要というものです。

本年 12 月以降に、政府機関の情報システムで JavaSE 6（JRE 6)を利用したり、国民の PC 等に JavaSE 6（JRE 6)をインストールすることを推奨したりすることは、国民や政府機関におけるセキュリティ水準の低下を招きます。政府機関統一管理基準 1.5.2.6 においても、府省庁外の情報セキュリティ水準の低下を招く行為を防止するための必要な措置を求めています。

つきましては、各府省庁におかれましては、自府省庁の情報システムについて、下記のとおり Java 環境の最新メジャー・リリースに係る適切なご対応をお願いいたします。なお、本件に係る対応状況については、平成 24 年度の重点検査の項目に追加し、フォローアップを行う予定です。

記

１．各府省庁で利用する Java 環境の最新版へのアップデート

本年 11 月末までに、自府省庁において利用する Java 環境を、最新バージョンの Java SE 7（JRE 7）にアップデートを行っていただきますよう、お願いいたします。

1

２．国民のPCにインストールを推奨する公開情報システムにおけるJava環境の最新版への対応等

国民のPC等にJava環境をインストールすることを求めている公開情報システムについては、利用者である国民側の情報セキュリティ水準の低下を招くおそれがあることから、速やかに、これが最新バージョンのJava SE 7（JRE 7）で動作することを検証するとともに、Webサイト等で表記する推奨動作環境をJava SE 7（JRE 7)とする（バージョンアップする）ご対応をいただきますようお願いします。

３．修正プログラム公開に係る定期的な対応の実施

Java SEは、修正プログラムの公開が、約3ヵ月に1回の頻度で、開発元の日本オラクル株式会社より行われています（参考２）。各府省庁におかれましては、政府機関統一技術基準「2.2.2.1　セキュリティホール対策」に基づき、定期的な修正プログラムの公開にあわせた、適切な対応をお願いいたします。

（参考１）
・Oracle Java SE サポート・ロードマップ（日本オラクル株式会社）
http://www.oracle.com/technetwork/jp/java/eol-135779-ja.html

（参考２）
・Critical Patch Updates, Security Alerts and Third Party Bulletin
（次回の公開予定日は、2012年10月16日）
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

資料編H　情報セキュリティ事象一覧

表 H-1　政府機関等に係る平成 24 年度の主な情報セキュリティ事象(※1)

年月(※2)		事象の概要（府省庁・機関名）	種別	主な報道機関名(※3)
平成24年	4月	防衛省では３月２６日、インターネット上に陸上自衛隊の車両管理に関する情報が流出していることを確認し、流出した経緯について確認を行っているところである。（防衛省）	過失／故意	NHK
		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たことが判明。（10 月にも発生）（内閣府）	その他	―
	5月	平成 24 年 5 月、（独）情報通信研究機構の Web サイトの一部が不正アクセスにより改ざんされた。（情報通信研究機構）	ウェブサイトへの攻撃	読売新聞
		平成 24 年 5 月 1 日、外部から機構のＰＣが外部のサイトと通信を行っている可能性がある旨の連絡があり、5 月 2 日の時点で 5 台のＰＣが外部サーバと意図しない通信をしていることが判明した。詳細調査の結果、合計 19 台が新種のマルウェアに感染し、その内 8 台から、ファイルサーバに格納されていた電子ファイル（ファイルの一部に個人情報を含む。核物質防護情報等の機微な情報は含まれていない。）が、平成 23 年 3 月から 7 月の間、流出した可能性が高いことが確認された。（原子力安全基盤機構）	情報窃取／不正プログラム感染	朝日新聞、日経新聞、産経新聞、毎日新聞、読売新聞、ＮＨＫ、時事通信、共同通信
		平成２４年５月，リサイクルショップで購入したワープロ内部に，法務省において作成したと思われる個人情報を含む職務上の情報が残存しているとの情報提供があったもの。（法務省）	過失	毎日新聞
		一般社団法人農林水産物等中国輸出促進協議会の事業に係る農林水産省の内部文書が何らかの経路で外部に提供されていた可能性があることが判明した事案。（農林水産省）	その他	産経新聞、日経新聞、毎日新聞、読売新聞
	6月	神奈川労働局横浜公共職業安定所の非常勤職員が職務上知り得た職歴情報を外部に漏らし、報酬を得ていたとして、愛知県警捜査二課に、国家公務員法（守秘義務）違反及び加重収賄罪の疑いで逮捕されたもの。（厚生労働省）	過失／故意	東京新聞、日経新聞、毎日新聞、読売新聞
		６月１２日午後９時頃に原子力安全委員会ホームページに掲載した電力会社とのやりとりの電子メールの資料において、特定のソフトウェアを用いることで個人情報等のマスキングが外せる状態にあり、個人情報等が漏えいした事実を６月１３日午前１０時３０分頃に確認し、ただちに個人情報等のマスキングが外せない資料に差し替えた。（内閣府）	過失／故意	朝日新聞、日経新聞、読売新聞
		国有財産情報公開システムのサーバ上に、国有財産と無関係のファイルが置かれていることが判明。（財務省）	ウェブサイトへの攻撃	朝日新聞、産経新聞、東京新聞、日経新聞、読売新聞
		アノニマスが 25 日に日本政府などを狙ったハッカー攻撃を示唆する声明をネットに掲示。国土交通省霞ヶ浦河川事務所の雨量計のデータなどを	ウェブサイトへの攻撃	朝日新聞、産経新聞、東京新聞、日経新聞、読売新聞、

		表示するページにも英語の文字列の書き込みがあった。(国土交通省)		
		アノニマスが 6 月 25 日に日本政府などに対するハッカー攻撃を示唆する声明をネットに掲示。この声明との関連性は不明であるが、同月 26 日、アクセス集中により最高裁判所が運営する WEB サイトが一時閲覧しづらい状態となった。(最高裁判所)	ウェブサイトへの攻撃	朝日新聞、産経新聞、東京新聞、日経新聞、毎日新聞、読売新聞
		平成２４年６月,ホームページに掲載されたファイルに,個人情報が記載された文書が添付されているとの情報提供があったもの。(法務省)	過失	―
	7 月	過去に複数の財務省職員用パソコンがウイルスに感染し、何らかの情報が外部に送信された可能性があることが判明。(財務省)	情報窃取／不正プログラム感染	日経新聞、毎日新聞、読売新聞
	8 月	8 月 14 日、自衛隊東京地方協力本部の 2 等陸曹の男性隊員が帰宅中、JR 総武線の電車内で隊員募集活動対象 51 人分の名前や住所、学校名などの個人情報を記載した用紙を紛失したと発表。(防衛省)	過失／故意	朝日新聞、日経新聞、毎日新聞
		8 月 17 日、HP の一部が改ざんされ、尖閣諸島に関する英文が表示される不具合が生じた。(奈良国立博物館)	ウェブサイトへの攻撃	朝日新聞、産経新聞、毎日新聞、読売新聞
	9 月	車検証に記載された個人情報を不正に漏らしたとして、愛知県警は、9 月 11 日、国土交通省関東運輸局東京運輸支局職員を国家公務員法(守秘義務) 違反の疑いで逮捕。(国土交通省)	過失／故意	朝日新聞、日経新聞、毎日新聞、読売新聞
		最高裁判所が運営する WEB サイトのトップページが、9 月 14 日、不正アクセスにより、「釣魚島は中国である」といった内容の文言等が表示されるように書き換えられた。(最高裁判所)	ウェブサイトへの攻撃	朝日新聞、産経新聞、東京新聞、日経新聞、毎日新聞、読売新聞
		平成 24 年 9 月、総務省統計局ホームページにおいて、アクセス集中により、一時閲覧がしづらい状態が生じた。(総務省)	ウェブサイトへの攻撃	朝日新聞、日経新聞、読売新聞
		9 月 24 日、文化庁が運営する「国指定文化財等データベース」のウェブサイトが改ざんされた。(文化庁)	ウェブサイトへの攻撃	朝日新聞、産経新聞、日経新聞、毎日新聞、読売新聞
		平成 24 年 9 月 18 日 0:00 頃～3:30 頃、政府インターネットテレビ Web サイトで、複数の IP アドレスから攻撃と考えられる大量アクセスがあり、サイトに通信アクセスが集中し、一時閲覧しづらい状態となった。なお、送信の中心は、中国本土からと思われる。(内閣府)	ウェブサイトへの攻撃	東京新聞、日経新聞、毎日新聞
		政策統括官（共生社会政策担当）の担当者が、障害者政策委員会第 3 小委員会の委員及び専門委員並びに委員・専門委員秘書に受信者に見える形で電子メールを送信。(BCC で送信すべき宛先を CC で誤送信したため) (内閣府)	過失／故意	―
	10 月	国内 5 大学のサーバーが不正アクセスされ、内 3 大学で氏名やメールアドレスの個人情報の流出があった。(東京大学、京都大学、東北大学、名古屋大学など)	情報窃取／不正プログラム感染	朝日新聞、産経新聞、毎日新聞、読売新聞
		工学研究科の教員が、学生に関する個人情報が含	過失／故	日経新聞

		まれているパソコンを学外に持ち出し、紛失した。(千葉大学)	意	
	11月	平成23年3月17日、PC1台がウイルスに感染し、平成24年11月21日までの間外部との通信が行われた。情報が外部に漏えいした可能性があるが、当該PCに保存されていた情報以外が漏えいした可能性はきわめて低い。(宇宙航空研究開発機構)	情報窃取／不正プログラム感染	産経新聞、東京新聞、日経新聞、毎日新聞、読売新聞
	12月	11月29日、「研究開発活動に係る不正行為に関する告発」を行うメールアドレス宛てに送られてきたメールから、3台のPCがウイルス感染し、内2台のPCから情報の漏洩があった。(日本原子力研究開発機構)	情報窃取／不正プログラム感染	朝日新聞、日経新聞、毎日新聞、読売新聞、
		平成24年12月7日、高知ユニットセンターよりコアセンターに対し、同ユニットセンターにおいて、エコチル調査参加者の個人情報が記録された調査票を電子情報化（pdfファイル化）して保管したUSBメモリを、執務室内で紛失した旨連絡があった。同ユニットセンターで気づいたのは、平成24年3月21日。個人情報の流出は確認されていない。(環境省 総合環境施策局 環境保健部 環境安全課 環境リスク評価室)	過失／故意	朝日新聞、高知新聞、毎日新聞、読売新聞、NHKオンラインニュース、産経ニュース、時事通信
平成25年	1月	平成２５年１月からの農林水産省へのサイバー攻撃に関する一連の報道を受け、情報セキュリティの専門家を含めた調査委員会を設置し、コンピュータを通じた不審通信の解明に関する調査等を行った結果、124点の行政文書が外部に流出した可能性があることが確認された事案。（農林水産省）	情報窃取／不正プログラム感染	朝日新聞、産経新聞、日経新聞、毎日新聞、読売新聞
		1月22日、同研究所のウェブサイトが改ざんされたと発表。個人情報や機密情報の流出は確認されていない。（農業環境技術研究所）	ウェブサイトへの攻撃	読売新聞
		地下鉄内で個人情報が保存されたＵＳＢメモリと個人情報が記載された書面が入った鞄の盗難に遭ったもの。（法務省）	過失	朝日新聞、毎日新聞、読売新聞、ＮＨＫ地方局、関西テレビ、毎日放送、読売テレビ
	2月	2月5日、外務省のパソコンからインターネット上の外部サーバへの不審な通信が確認され、パソコンから約２０点の文書（いずれも機密性２以下）が流出した疑いがあることを発表。(外務省)	情報窃取／不正プログラム感染	朝日新聞、産経新聞、日経新聞、毎日新聞、読売新聞
	3月	3月17日、同省が運営する生活のCO2排出量を可視化するサイト「CO2みえーるツール」のサーバーが改ざんされたと発表。閲覧すると、パソコンの状況等によってはパソコン内の情報を盗まれるおそれ。（環境省）	ウェブサイトへの攻撃	朝日新聞、産経新聞、東京新聞、日経新聞、毎日新聞、読売新聞

※1 平成24年度において、報道が確認された政府機関等(行政府、立法府、司法府及び独立行政法人等)に係る情報セキュリティ事象、あるいは、政府機関等が公表した情報セキュリティ事象のうち主な事象。例えば、独立行政法人等におけるウェブサイトへの攻撃事象については掲載した事象のほかに7件の事象が公表されている。

※2 「年月」は報道が確認された事象の場合報道年月を表し、確認されていない事象の場合は発生年月を表す。

※3 報道が確認されていない事象については「―」としている。

資料編Ⅰ　政府機関の情報セキュリティ対策に係るこれまでの主な取組

表 I-1　政府機関の情報セキュリティ対策に係るこれまでの主な取組

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）
平成24年４月	○ 暗号危殆化の危険度判定及び対応フローについて決定
平成24年５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改訂（第２版）
平成24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23年度）の決定
平成24年６月	○ 情報セキュリティ緊急支援チーム（CYMAT）の設置
平成24年７月	○ 情報セキュリティ２０１２の決定
平成24年10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に係る移行指針の改定
平成25年３月	○ 全府省庁において組織内CSIRTを整備