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）

平成 23 年５月 31 日

情報セキュリティ対策推進会議

目次

はじめに

情報セキュリティ対策推進会議（CISO 等連絡会議）において、本日、平成 22 年度の政府機関における情報セキュリティに係る年次報告を取りまとめた。本報告は、内閣官房長官を議長とする情報セキュリティ政策会議で平成 22 年５月に決定された「国民を守る情報セキュリティ戦略」において各府省庁の最高情報セキュリティ責任者（CISO)が作成することとなった情報セキュリティ報告書について CISO 等連絡会議自身で評価し、「自ら問題意識を持って情報セキュリティ対策の改善を図る」ことを目指したものである。

本報告では、まず、情報セキュリティ対策に影響を及ぼす内外の情勢を俯瞰した。平成 22 年度はこれまで以上に、政府機関の情報セキュリティを取り巻く状況は厳しさを増し、様々な脅威が顕在化した一年であった。また、平成 23 年３月 11 日の東日本大震災により多数の情報システムも被災し、業務継続計画の観点や緊急時の情報システムのあり方についても、多くの課題が明らかとなった。

次に、政府機関の取り組み状況について検討した。政府機関における情報セキュリティのための統一基準に基づいて、各府省庁は情報セキュリティ対策を実施してきており、その実施状況は内閣官房において取りまとめている。また、職員の利用する端末、サーバ類の情報セキュリティ対策について重点的な検査を内閣官房において行った。平成 22 年度は、これまでの継続的な取り組みの結果、全体としては高い水準に達していると認められるが、一部にはまだ十分ではない事項も残っており、引き続き、政府全体の情報セキュリティレベルの向上を推進していくことが必要である。また、これらの取り組みが形骸化しないように、各府省の取り組み、その評価については、更なる工夫も必要である。

本報告に基づき、内閣官房と各府省庁は、それぞれの対策の改善を行う持続的な取り組みを図ることにより、政府機関の情報セキュリティ対策の実効性が上がったことを平成 23 年度の年次報告において確認できることを期待したい。

第１章 平成 22 年度の情報セキュリティに関する動向と政府機関の取組

第１節 国内外における情報セキュリティに関する動向

平成 22 年度の我が国の内外における情報セキュリティに関する動向について、概観を述べる。

（１）国境を越えたサイバー攻撃の増加

(a) DDoS 攻撃の脅威（様々な動機で積極的にクラッキング行為を行う個人・組織等の関与）

平成 22 年度は、海外及び我が国の政府機関、民間企業等へ複数の攻撃元から行われるサービス不能攻撃（Distributed Denial of Service Attack 以下「DDoS 攻撃」という。）を始めとするサイバー攻撃事案が活発化した年であった。記憶の新しいところでは、平成 23 年３月に韓国の大統領府、国家情報院、外務省、国防省、国会を含む約 40 のサイトに対してDDoS攻撃が加えられたとの報道があった。他にも、インド、イラン、フランス、米国、エジプト、北朝鮮、ブラジル、ジンバブエ等多数の国々の政府機関、民間企業等に対して、DDoS 攻撃が仕掛けられた事案が発生しているとの報道がある。これらの事案については、政治状況に応じて様々な理由で積極的にクラッキング行為を行う個人・組織等が多数関与していると考えられている。

我が国においても、政府機関のウェブサイトへ大規模な DDoS 攻撃が仕掛けられる脅威が今後増大化する可能性はある。

(b) 狙われる政府機関、公的企業等の機密情報

海外では、政府機関、公的企業等に対して、機密情報の窃取を目的としたサイバー攻撃が発生している。例えば、カナダや米国では、政府機関に対して海外から機密情報の窃取を目的としたサイバー攻撃が発生したとの報道があり、また Microsoft 社（MS 社）の Internet Explorer のセキュリティパッチを公開する前の脆弱性（ゼロデイの脆弱性）を利用して、大手検索サイトを含む 30 社以上に攻撃を仕掛け、各企業の機密情報を窃取しようとした事例も報道されている。

（２）複雑・巧妙化する攻撃

(a) 標的型メール攻撃の増加・巧妙化

フィッシング行為やウイルス感染を目的として、特定の組織・人物に送付される標的型メール攻撃の事例は、従来からあったが、文面・送信元がより巧妙化してきている。例えば、東日本大震災に便乗して、

「原発、放射能」「節電、計画停電」「地震、津波」といった関連の情報を装った標的型メール攻撃が日本国内のユーザへ数多く送付される事例が多数発生していると報道された。

海外においても、米国の政府職員や政府との契約企業の職員を含む多くの人々へ、ホワイトハウスからのクリスマスメールを偽った標的型メール攻撃が送信された事例等の発生が報道されている。

(b) ボットネットの拡大

新種のボットが増加し、それらの感染によるボットネットが拡大しているとの報告が発表された。容易にボットを作成できるツールキットも流布しており、今後もボットネットの拡大は続くと思われる。

(c) オフライン環境下へのウイルス/ワーム感染

イラン等で、Stuxnet と呼ばれるワームにより核関連施設の産業機器が停止した可能性があるとの報道があった。これは、インターネットに直接接続されていないネットワーク（オフライン環境下のネットワーク）にも、USB メモリ等の外部電磁的記録媒体を経由してワーム感染が拡大する可能性を指摘する事例であり、ネットワークに直接接続していない情報システムは、ウイルス/ワームに感染しにくいというこれまでの概念を見直すきっかけとなった事例でもある。

(d) ゼロデイ攻撃（汎用ソフトウェア製品の脆弱性情報）

MS 社の Windows 等の OS 及び Adobe Systems 社の Adobe Reader 等の汎用ソフトウェア製品は、各開発ベンダの努力により、セキュリティ水準は向上しているが、発見される脆弱性は引き続き多い。また、発見された脆弱性について、修正用プログラムが公開される前に、その脆弱性を突いて攻撃する事例（ゼロデイ攻撃）が顕著になってきているとの報告がある。なお、政府機関において感染事例の報告はないが、Gumblar や Conficker 等のように平成 21 年度に猛威を振るったマルウェアも引き続き感染事例が発生している。

（３）情報流出事案

(a) 海外及び我が国の政府機関からの情報流出

平成 22 年度は、行政機関内部の非公開情報が流出した事例も発生し、社会的に大きな問題となった。

海外でも、Wikileaks 等のサイトにおいて、外交文書等が流出、暴露されたとの報道があった。

(b) オンライン経由の情報流出

インターネットが普及し始めて以降、システムにオンライン経由で

侵入され、個人情報等が流出される事件はあとを絶たない。平成 22 年度も、大手のゲーム会社が運営するサイトで、ゲームのアカウント情報が流出したり、認証や暗号化等のサービスを提供する企業で、暗号化製品に関する機密情報が窃取されたりする等の多数の事例がある。

（４）情報システムの障害・事故等

障害・事故等により情報システムが停止し、社会生活に影響を及ぼす事例も発生している。例えば、東日本大震災により、複数の市町村で住民基本台帳や戸籍を管理する情報システムが破壊され、データが滅失するという事態が発生した。これらに対しては、別に保管されていたバックアップデータにより概ね復旧する見込みである。また、海外ではマルウェアの感染により、救急サービスが停止する事例があり、我が国でも東日本大震災に伴う大量の義援金振込で、大手銀行のシステムが停止した事例も発生している。

（５）ネットワーク環境の進化による新たな課題

(a) クラウドサービスの利用拡大に伴う課題

平成 22 年度は、ネットワークを介して提供されるサービス（いわゆる「クラウドサービス」）の活用が一層進んだ年となった。

政府機関においては、クラウドサービスで扱う情報の特性に応じて、情報が保管される所在地についても留意する必要が生じている。

(b) スマートフォンに対する攻撃増加

海外においては、米国で陸軍兵にスマートフォンを普及させる活動が進んでいる等、政府機関等においてもスマートフォンの利用が今後増加する可能性がある。一方で、スマートフォンへのウイルス/ワーム感染等の攻撃事例の発生頻度も高くなってきているとの報告もある。

(c) SNS の利用増加に伴う課題

Twitter 社の提供する Twitter 等のソーシャルネットワークサービス(Social Network Service 以下「SNS」という。)の普及に伴い、アカウントのなりすましやデマ情報の流布等の問題が顕著になってきた。例えば、東日本大震災に伴い、節電や原子力発電所等に関連する情報に関して事実と異なる内容の情報が広く流布される等の事例も発生した。

また、SNS をマーケティングや広報などに利用している組織が増え、不適切な発言や機密情報の漏えいが発生する事例も出ている。

(d) IPv4 の払い出し終了に伴う IPv6 移行時の課題

Internet Assigned Numbers Authority (IANA) の管理する IPv4 アドレスが、平成 23 年２月３日に地域インターネットレジストリへ全て払い出しが行われ、新たな IP アドレスの割当が困難となった。そのため、IPv6 への対応検討が急務となる事態になっているが、その際に注意すべき情報セキュリティ課題の洗い出しは、現在のところ十分といえる状態ではない。

(e) DNS Security Extensions (DNSSEC) への対応

従来から、DNS キャッシュポイズニング攻撃への根本的な対応策の一つとして、DNS における応答の正当性を保証するための拡張仕様である DNSSEC の整備が求められていた。平成 22 年度は、ルートゾーン及び「.jp」が DNSSEC に対応したほか、主要な ISP 事業者においても DNSSEC への対応が完了し、DNS における応答の正当性を保証するための仕組みが整い始めている。

(f) 暗号の危殆化対応

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

我が国の政府機関においては、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年４月 22 日情報セキュリティ政策会議決定)に基づいて、2013 年度末までに新しい暗号アルゴリズムを利用可能な状態に移行させるために準備を進めているところであり、引き続き動向を注視する必要がある。

なお、本移行指針は、コンピュータの計算性能の向上を主な危殆化の要因とした場合の予測[1]に基づいて策定されているが、現在報告されているコンピュータの計算性能の向上トレンド[2]も当時の予測に沿ったものである。

第２節 政府機関の取組

政府機関に向けては、次のような取組を進めてきた。

---

[1] 暗号技術検討会 2006 年度報告書（平成 19 年３月 CRYPTREC 暗号技術検討会）

[2] Top500.org (http://www.top500.org/)

（１）情報セキュリティ対策推進会議の設置

最高情報セキュリティ責任者(CISO)の機能強化の一環として、各府省庁の官房長等からなる、最高情報セキュリティ責任者等連絡会議（以下「情報セキュリティ対策推進会議」という。）を設置し、平成 22 年 12 月に情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議という形で第 1 回会議を開催した。この場で、各府省庁の最高情報セキュリティ責任者が平成22年度情報セキュリティ報告書を策定すること等を再確認した。

（２）最高情報セキュリティアドバイザー等連絡会議の設置

情報セキュリティ対策推進会議の下に、情報セキュリティに係る専門的知見を各府省庁の取組の高度化に反映させるため、最高情報セキュリティアドバイザー等連絡会議を設置し、第 1 回会議を開催した。この場で、平成 22 年度情報セキュリティ報告書の作成において配慮すべき点を助言として取りまとめ、共有を行った。

（３）「情報セキュリティに係る年次報告書」（情報セキュリティ報告書）の試行的な作成

各府省庁の最高情報セキュリティ責任者は、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上記会議での議論を踏まえ、省内外の知見を活用しつつ、情報セキュリティ報告書を試行的に作成した。

（４）政府機関統一基準群の整備

昨今の情報セキュリティに係る問題意識、そして、Gumblar 等のウェブ改ざん型攻撃や標的型メール攻撃といった脅威やクラウドコンピューティングといった技術的・環境的な変化に対応するため、既存の政府機関統一基準の抜本的な見直しを行い、「政府機関の情報セキュリティ対策のための統一規範」を新たに制定するとともに、これまでの政府機関統一基準を「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」（基本的基準）と「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」（技術的基準）に分離し政府機関統一基準群として整備した。

（５）NISC と関連する公的機関との協力覚書の締結

NISC と関連する公的機関（(独）情報通信研究機構（NICT)、(独）産業技術総合研究所（AIST）及び（独）情報処理推進機構（IPA））と

の間で協力覚書の締結を行い、情報セキュリティの脆弱性等に関連する情報共有を進めるとともに、独立行政法人の研究者の知見を蓄積・活用して、政府機関統一基準群等の施策への反映を図った。

（６）公開ウェブサーバに対する脆弱性検査の実施

検査を希望する府省庁の公開ウェブサーバについて、主なものをサンプル抽出し脆弱性検査を実施した。更に、その検査結果を最高情報セキュリティアドバイザー等連絡会議において共有した。

（７）政府機関から発信する電子メールに係るなりすましの防止

悪意の第三者が政府機関又は政府機関の職員になりすまし、一般国民や民間企業等に害を及ぼすことが無いよう、各府省庁に対しSPF(Sender Policy Framework)等の送信ドメイン認証技術の採用を推進した。

（８）政府職員に対する教育・意識啓発の推進

情報セキュリティ対策上の役割に応じた教育教材の雛型を作成し、全府省庁に配付することで、政府職員の情報セキュリティに対する教育・意識啓発の推進に努めた。

（９）「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の策定

オンライン手続に応じたセキュリティ確保策として、適切な認証と電子署名を選択するための「ものさし」となる、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を作成した。本資料は平成 22 年 8 月開催の各府省情報化統括責任者（CIO）連絡会議第 41 回会合において決定された。

（１０）「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」の取りまとめ

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、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を確保するための方策について検討するため、主要ベンダー等を構成員とする検討会を開催した。当該検討会での議論の結果、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、

情報セキュリティ対策が適切に組み込まれる仕組みの構築及び組み込むべき情報セキュリティ要件を取りまとめ、「情報システムに係る政府機関におけるセキュリティ要件策定マニュアル」を平成 23 年 3 月に策定した。

（１１）「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

首都直下型地震等の大規模地震からマルウェア感染（不正プログラム）まで多岐に渡る様々な危機的事象のうち、何らかの事象を原因とした情報システム停止に備えた必要な対策に取り組むため、中央省庁の情報システム運用継続計画に含める事項を具体的に示すガイドラインを整備した。

（１２）その他（NISC から各府省庁へ注意喚起の事務連絡発出等）

平成 22 年度に発生した事象の内、NISC で緊急性が高いと判断した脆弱性等については、表 1 のとおり政府機関に対し事務連絡を発出し、迅速な注意喚起を行った。

表 1　平成 22 年度に発出した事務連絡

年月日		発出した事務連絡
平成 22 年	4 月 12 日	送信ドメイン認証に関する取組について
	5 月 12 日	旧型から最新版ブラウザへの移行について（依頼）
	6 月 10 日	各府省庁において Twitter 等を利用する場合の対応について
	9 月 10 日	「情報セキュリティ早期警戒パートナーシップガイドライン」に係る協力の運用開始
	9 月 13 日	障害・事故等が発生した場合に備えた緊急連絡先の提供について(依頼)
	9 月 15 日	各府省庁等ウェブサイトに係る適切な運営について（注意喚起）
	11 月 19 日	情報管理ソリューション製品の導入状況等に係る調査について（調査依頼）
平成 23 年	3 月 24 日	データセンター利用時の災害対応の確認について

(a) 送信ドメイン認証に関する取組について

各府省庁に対して、保有する.go.jp ドメインについて DNS サーバ上において送信ドメイン認証の設定を実施すること、及び、不審メール対策の観点から受信側メールサーバにおける対策について採用を検討することを促すもの。

(b) 旧型から最新ブラウザへの移行について（依頼）

Internet Explorer（IE）6 を利用している場合には、IE8 への移行を勧告。またシステム構築又は更改時は運用期間全体に渡った安全環境の維持や、リスク分散の観点から複数ブラウザの利用検討を依頼するもの。

(c) 各府省庁において Twitter 等を利用する場合の対応について

公務として Twitter 等を利用するに際しては、政府ドメイン名の使用を徹底すること、また当該対応が困難な場合は、なりすまし防止等に向けた適切な対処を行うことを依頼するもの。

(d) 「情報セキュリティ早期警戒パートナーシップガイドライン」に係る協力の運用開始

「情報セキュリティ早期警戒パートナーシップガイドライン」に基づき、(独）情報処理推進機構セキュリティセンター（IPA/ISEC）から NISC へ送られたウェブサイトに係る脆弱性関連情報等を、NISC が各府省庁の連絡窓口へ通知、対応状況の定期的な確認を行う。また NISC は各府省庁窓口から受けた修正完了通知を IPA/ISEC へ通知する運用につき周知するもの。

(e) 障害・事故等が発生した場合に備えた緊急連絡先の提供について（依頼）

各府省庁との連絡体制を確認するため、緊急連絡先の事前提供を依頼するもの。

(f) 各府省庁等ウェブサイトに係る適切な運営について（注意喚起）

FTP サーバ等の ID 及びパスワードの厳重な管理と適切な更新等を要請するもの。

(g) 情報管理ソリューション製品の導入状況等に係る調査について（調査依頼）

情報管理ソリューション製品のアクセス制御機能や証跡管理機能について、各府省庁の着実な対策実施に万全を期すべく、各府省庁における具体的な導入状況を調査するもの。

(h) データセンター利用時の災害対応の確認について

東日本大震災を受け、各府省庁が外部委託している情報システムに

ついて、被災時においても適切な情報セキュリティ対策を講じることができるよう、委託先の災害対応体制（建物、立地、災害対策）を確認するもの。

第２章 政府機関の取組の評価

平成 21 年度に「情報セキュリティ報告書専門委員会報告書」(2009 年 9 月 11 日情報セキュリティ報告書専門委員会決定)で、「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」が策定されたことを受け、各府省庁は、「情報セキュリティ 2010 2(1)①イ)『情報セキュリティに係る年次報告書』(情報セキュリティ報告書)に係る取組の推進」に従い、平成 22 年度は、各府省庁にて情報セキュリティ報告書を試行的に作成した。

また、NISC では「政府機関における評価等の考え方」に基づき、各府省庁に対して、政府機関全体の情報セキュリティ対策実施状況の報告（以下「対策実施状況報告」という。）並びに端末、ウェブサーバ及び電子メールサーバの情報セキュリティ対策について重点検査（以下「重点検査」という。）の実施を求め、評価を行った。

なお、本年度は、希望する府省庁の公開ウェブサーバに対して、脆弱性検査も実施した。

政府機関における対策実施状況報告、重点検査の結果については、引き続き一部対策が不十分な部分や課題は残っているものの、各府省庁の情報セキュリティ対策は一定の水準を維持している。また、各府省庁独自の取組も多数報告されるなど、多面的な対策が講じられており、情報セキュリティへの対応力は着実に向上していると評価できる。

第１節 対策実施状況報告の評価

（１）対策実施状況報告の目的

「政府機関の情報セキュリティ対策のための統一基準（第４版）(平成21年度修正)」(平成22年５月11日情報セキュリティ政策会議決定。)に基づく各府省庁の情報セキュリティ対策の実施状況について把握するため、各府省庁は、取組状況を NISC に報告する。

NISC は、政府機関の対策実施状況を分析・評価し、課題及びその改善に向けた今後の取組について報告する。

（２）実施対象

対策実施状況報告は、政府機関統一基準の第 1.2 部から第 2.3 部に定められた遵守事項に基づく取組全般を対象と想定している。平成 22 年度における報告については、保護すべき情報とこれを取り扱う情報システムにおいて必須とされている基本遵守事項全てを報告対象とした。具体的には、表 2 のとおり。

表 2　対策実施状況報告の実施対象

遵守事項の主体[3]	対象職員	遵守事項
最高情報セキュリティ責任者	全て対象[4]	全て対象
情報セキュリティ委員会		
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		
情報システムセキュリティ責任者・管理者		
課室情報セキュリティ責任者		
行政事務従事者		

（３）実施期間

平成 22 年６月から平成 23 年３月にかけて実施
（各府省庁の実情に応じ、最適な点検対象期間・点検時期等を設定）

（４）実施方法

政府機関統一基準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実施しているか否かを統計的に把握するために、実施主体ごとの対策実施状況について、各府省庁において把握・集計した上で NISC に報告し、NISC においてその結果を分析・評価した。

（５）政府機関全体の評価

(a) 対策実施状況報告の結果（政府機関全体）

平成 22 年度の政府機関全体の対策実施状況報告の結果は以下のとおり

(ｱ) 把握率（状況が把握できた者の割合）（△：マイナス。以下同様。）

表 3　把握率（全府省庁平均）

把握率（全府省庁平均）	平成 22 年度	平成 21 年度	増減
全主体平均	99.2%	99.3%	△0.1%
責任者等[5]	99.3%	99.1%	0.2%

[3] 「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。「情報セキュリティ関係規程を整備した者」及び「許可権限者」については、府省庁が指定するそれぞれの主体の中に含む。

[4] 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。

[5] 最高情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者、情報セキュリティ監査実施者、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、許可権限者及び情報セキュリティ関係規程を整備した者

システム責任者等[6]	99.3%	99.0%	0.3%
行政事務従事者	99.2%	99.3%	△0.1%

(ｲ) 実施率（把握した者のうち、責務が生じた者に占める対策を実施した者の割合）

表 4　実施率（全府省庁平均）

実施率（全府省庁平均）	平成22年度	平成21年度	増減
全主体平均	98.9%	98.1%	0.8%
責任者等	99.5%	98.3%	1.2%
システム責任者等	99.3%	98.4%	0.9%
行政事務従事者	97.6%	97.1%	0.5%

(ｳ) 到達率（把握した者のうち、責務が生じた一定の割合以上の者が対策を実施した遵守事項の割合）

表 5　到達率（全府省庁平均）

到達率（全府省庁平均）	平成22年度	平成21年度	増減
全主体平均			
100%実施した割合	80.7%	83.0%	△2.3%
95%以上実施した割合	93.4%	91.6%	1.8%
90%以上実施した割合	97.0%	94.9%	2.1%
責任者等			
100%実施した割合	99.0%	96.8%	2.2%
95%以上実施した割合	99.4%	97.7%	1.7%
90%以上実施した割合	99.5%	98.2%	1.3%
システム責任者等			
100%実施した割合	88.0%	90.0%	△2.0%
95%以上実施した割合	95.8%	92.6%	3.2%
90%以上実施した割合	98.3%	95.6%	2.7%
行政事務従事者			
100%実施した割合	52.9%	59.9%	△7.0%
95%以上実施した割合	84.4%	84.8%	△0.4%
90%以上実施した割合	92.8%	90.3%	2.5%

[6] 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責任者を含む複数の者が主体となっているものを含む）、情報システムセキュリティ管理者及び権限管理を行う者

(b) 所見

- 把握率は 99.2%となっており、今回の報告対象が政府機関の全ての行政事務従事者であることに鑑みれば、全体的に高い水準を達成したといえる。しかしながら、対策実施状況の把握は、PDCA サイクルにおけるC（評価）のプロセスに相当し、情報セキュリティ水準の維持・向上に不可欠であることから、政府機関全体で把握率 100%を達成すべく、今後更なる向上が望まれる。
- 責任者が対策を実施した割合は 99.5%（前年度より 1.2%増）となっており、対策の浸透が認められる。ただし、これらの者が実施すべき対策は、職員の行動の基礎となる規程の整備等といったもので、その重要性に鑑みれば、本来、全ての対策が実施されているべきであり、更なる浸透が望まれる。
- システム責任者等が対策を実施した割合は、99.3%（前年度より 0.9%増）となっており、対策の浸透が認められる。ただし、行政事務では重要な情報を取り扱う情報システムを利用しており、情報システムにはより高い情報セキュリティ対策が求められることから、更なる浸透が望まれる。
- 行政事務従事者が対策を実施した割合は、97.6%(前年度より 0.5%増)となっており、対策の浸透が認められる。ただし、一部の項目には十分といえない項目がみられる。特に、「情報の取扱い」に関する項目について、平成 21 年度より改善は認められるものの、まだ取組が不十分な府省庁が多く、課題が認められる。このため、取組が進んでいる府省庁においてはこれを向上・維持し、遅れている府省庁においては改善措置の速やかな実施が求められる。
- 到達率は「100%実施した割合」が全主体平均で 80.7%（平成 21 年度より 2.3%減）となっており、平成 21 年度を下回る結果となった。特に行政事務従事者の「100%実施した割合」は 52.9%となっており、昨年より 7.0%減と大幅に減少している。これは、自己点検票の雛型を点検実施者が点検内容を理解しやすいように改善したことで、各府省庁において、平成 21 年度より実態に即した点検が実施できたことも要因であると考えられる。到達率が増加して、行政事務従事者における対策の実施の浸透が見られる府省庁もあるが、政府機関全体としては、更なる向上が望まれる。
- 引き続き自己点検票の改善を図り、より正確に実情を把握し、取組が十分でない項目についての情報セキュリティ対策を行うことで、政府全体の情報セキュリティレベルの向上を推進していく。

（６）府省庁別の評価

(a) 評価方法

各府省庁の把握率/実施率について、NISC で ABCD 評価を行った。ABCD 評価の見方は、図 1 のとおり。

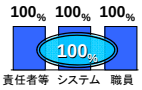
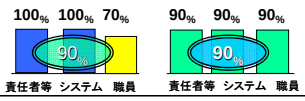
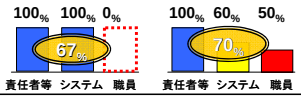
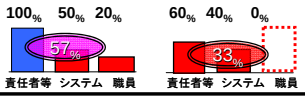
評価	実施率/(把握率)	対策状況	個別対策項目についての評価パターン例
A	100%	適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。	
B	80%≦x<100%	適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**対策が実施**されているが、**一部の項目で不十分なもの**が含まれている。	
C	60%≦x<80%	適切に実施すべき対策について、**不備の項目が一部に見られる**など、対策が遅れている。	
D	60%未満	適切に実施すべき対策について、**不備の項目が相当数、見られるなど**、対策が著しく遅れている。	

図 1　対策実施状況報告の ABCD 評価

(ｱ) 把握率評価

平成 22 年度の把握率（府省庁別）の評価は表 6 のとおり。

表 6　把握率評価結果（府省庁別）

府省庁名	評価
内閣官房	A
内閣法制局	A
人事院	A
内閣府	A
宮内庁	A
公正取引委員会	A
国家公安委員会(警察庁)	A
金融庁	B
消費者庁	A
総務省	B
法務省	A
外務省	A
財務省	A
文部科学省	B

厚生労働省	A
農林水産省	B
経済産業省	B
国土交通省	B
環境省	B
防衛省	B

(ｲ) 実施率評価

平成 22 年度の実施率（府省庁別）の評価は表 7 のとおり。

表 7　実施率評価結果（府省庁別）

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

第２節 重点検査の評価

（１）重点検査の目的

政府機関統一基準に基づく各府省庁における情報セキュリティ対策のうち、特に重要かつ緊急性を有する分野である端末、ウェブサーバ及び電子メールサーバの情報セキュリティ対策について重点検査を実施した。

（２）検査対象機関・システム等

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

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

（３）検査期間

平成 22 年６月から平成 23 年３月

（４）検査方法

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

表 8　重点検査の実施対象・検査内容

	端末	ウェブサーバ	電子メールサーバ
対象数	約 57 万台	約 900 台	約 1,200 台
不正プログラム対策	・OS のパッチ等の適用状況 ・端末を利用するユーザのパスワードの定期更新実施状況 ・主要なアプリケーションのパッチ等の適用状況 ・アンチウイルスソフトの運用状	・OS のパッチ等の適用状況 ・ウェブサーバ AP のパッチ等の適用状況等 ・アンチウイルスソフトの適用状況	・OS のセキュリティパッチ提供状況（アップデートの状況） ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況） ・電子メールコンテ

	況		ンツに対する不正プログラム対策の状況
不正アクセス対策	－	不正アクセス対策状況	－
情報保護対策	モバイル PC の暗号化機能の運用状況	利用者に対する権限管理等の実施状況	電子メールの受信に係わる利用者に対する認証等の実施状況
端末管理	端末の物理的対策状況（据置ノート型・モバイル端末）	－	－
サーバ管理	－	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況

（５）評価方法

「第２章第２節（４）検査方法」で確認した各府省庁の実施率について、NISC で ABCD 評価を行った。ABCD 評価の見方は、図 2 のとおり。

評価	実施率	対策状況	個別対策項目についての評価パターン例
A	100%	適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。	100% 100% 100% 100% 対策1 対策2 対策3
B	80%≦x<100%	適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**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。	100% 100% 70% 90% 対策1 対策2 対策3 90% 90% 90% 90% 対策1 対策2 対策3
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。	100% 100% 0% 67% 対策1 対策2 対策3 100% 60% 50% 70% 対策1 対策2 対策3
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。	100% 50% 20% 57% 対策1 対策2 対策3 60% 40% 0% 33% 対策1 対策2 対策3

図 2　重点検査の ABCD 評価

（６）総評

(a) 重点検査結果について

平成 22 年度の重点検査の評価（府省庁別）は表 9 のとおり。

表 9　重点検査の評価（府省庁別）

府省庁名	端　末	ウェブサーバ	電子メールサーバ	端末の台帳管理
	今回 H23.3 (前回 H22.3)	今回 H23.3 (前回 H22.3)	今回 H23.3 (前回 H22.3)	
内閣官房	Ａ（Ａ）	※Ａ（※Ａ）	Ａ（Ａ）	○
内閣法制局	Ａ（Ａ）	◆対象なし （◆対象なし）	Ａ（Ａ）	○
人事院	Ａ（Ａ）		Ａ（Ａ）	○
内閣府	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
宮内庁	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
公正取引委員会	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
国家公安委員会(警察庁)	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
金融庁	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
消費者庁	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
総務省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
法務省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
外務省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
財務省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
文部科学省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
厚生労働省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	△
農林水産省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
経済産業省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
国土交通省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
環境省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○
防衛省	Ａ（Ａ）	Ａ（Ａ）	Ａ（Ａ）	○

※：内閣官房のウェブサーバについては、内閣府との共有システムを除く

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

○：整備済、△：一部未整備、×：未整備

(b) 所見

政府機関統一基準に基づく各府省庁における情報セキュリティ対策のうち、端末、ウェブサーバ及び電子メールサーバの情報セキュリティ対策について重点検査を実施したところ、全ての検査対象項目において、政府機関統一基準に準拠した対策が適切に実施されている。ただし、端末の管理台帳が一部未整備な府省庁があった。

端末の管理台帳を整備することは、継続的な情報セキュリティ対策を講じていく上で、重要な構成要素の一つである。そのため、管理台帳が未整備な部局に対しては、当該府省庁の管理部局が率先して指導し、管理台帳を整備することを求める。

今後は、各府省庁においては情報セキュリティ対策の維持・向上を引き続き行うとともに、客観的な視点による継続的な検査の実施が必要である。

第３節 公開ウェブサーバの脆弱性検査

（１）検査概要

(a) 検査期間

平成 22 年 11 月～12 月

(b) 検査対象

希望府省庁における公開ウェブサーバ（8 省庁、45IP[7]）

(c) 検査方法

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

(d) 検査内容

・プラットフォームに関する検査
・DoS 攻撃に対する脆弱性の検査
・ウェブアプリケーションに関する検査

（２）検査内容詳細

(a) プラットフォームに関する検査

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

[7] NISC で実施した脆弱性検査の検査対象であり、各府省庁が独自に実施している脆弱性検査の検査対象は含まれていない。

(4)	手動による侵入検査

(b) DoS 攻撃に対する脆弱性の検査

	検査内容
(1)	SYN flood 攻撃
(2)	UDP flood 攻撃
(3)	Connection Flood 攻撃

(c) ウェブアプリケーションに関する検査

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

（３）検査結果概要

Web アプリケーションに関する検査では、SQL インジェクションやクロスサイトスクリプティングといった個別のアプリケーションに見られる危険度の高い脆弱性を検知したため、即座に対処を実施した。

また、プラットフォームに関する検査では、強度の弱い暗号方式でも通信が可能であるといった危険度は低い脆弱性を複数のサイトで検知した。これらの脆弱性情報を全府省庁と共有することで、政府機関全体の情報セキュリティ対策の向上に活用した。

第４節 推奨事例

（１）推奨事例の選定対象と選定目的

各府省庁が平成 22 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、政府機関全体としての情報セキュ

リティマネジメント水準の向上を図ることを目的としている。

（２）選定の方法

各府省庁の情報セキュリティ報告書に記載されている事項から取り上げた推奨事例候補となり得る取組を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、その結果、推奨事例候補として５件の取組事例をNISCに推薦した。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、推奨事例を選定した。また選定に当たり特に以下の二点を重視した。

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

（３）推奨事例

(a) 推奨事例

最高情報セキュリティアドバイザー等連絡会議において、推奨事例候補として５件が推薦され、NISCは５件の候補について改めて検討を行った。結果、５件全てについて推奨事例とすることとした。

平成22年度の推奨事例は次のとおりである。

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

(b) 推奨事例概要

(ｱ) 標的型メール攻撃に対する訓練

不正なプログラムをメールで送り込む攻撃に適切に対応するとともに、職員の情報セキュリティ意識向上を図る目的で実施。実在の不審メール情報等を題材に訓練メールを作成し職員へ送付、訓練メールを開封した職員へは注意喚起を促すコンテンツを表示した。実施結果を分析し教育内容にも反映している。

(ｲ) 自己点検内容の徹底した重点化

自己点検への職員の負担感を省き実効性を上げることを目的として、自己点検票の内容を重点化、記入の容易化を図った。結果、把握率の向上とともに、各職員自身が自らの役割を再認識し情報セキュリティに対する意識の向上にもつながった。

(ｳ) 秘密文書の管理に関する規程と情報セキュリティ関連規程の統合

両規程の棲み分けが不明瞭なことから、秘密文書の管理に係る規程を情報セキュリティ関連規程等へ取り込み、職員の分かりづらさを解消させた。これにより機密性区分の統一や情報管理責任者の明確化が行われ、今後情報管理の徹底が一層強化されることを見込んでいる。

(ｴ) 検疫認証システムの導入、内閣府外への電子メールの暗号化機能の導入及び IPv6 も考慮した公開ウェブサーバのセキュリティ対策

基幹ネットワークの更新にあわせて統合的なセキュリティ対策を実施した。内閣府 LAN のシステムに含まれるホームページを統合集約したことにより、効率的な運用が行われると同時に最新の対策が取られたシステム内での運用が可能となり安全性も向上した。

(ｵ) LAN パソコンのワープロソフト及び電子メールにおける、情報の格付を自動付与する仕組みの導入

文書作成時のヘッダーに「機密性○情報」、「○○限り」、メール作成時の件名に「機○」が自動的に挿入されるようにした。○の部分は職員が自ら格付等を記入することとなるため、具体的にどのような格付をして明示すればよいかを多数例示した「情報の格付マニュアル・情報の格付及び取扱制限のルール」を作成した。

(c) 選定理由

(ｱ) 標的型メール攻撃に対する訓練

標的型メール攻撃が増加しその偽装も巧妙となる一方、技術的手段で完全に防ぐことは難しく、職員がその被害を受けるリスクは高まっている。その中で単なる知識としてだけではなく模擬訓練を受けることは自分自身にもあり得るリスクとして職員の意識向上や注意喚起に効果的であり、実際の場面での対応力の強化につながることが考えられる。

(ｲ) 自己点検内容の徹底した重点化

自己点検内容の記入を理解しやすい内容とすることは職員の自己点検への負担感を解消することに留まらず、情報セキュリティに対する理解を深める教育的効果を有する。その結果、把握率のみなら

ず府省庁全体における実施率向上にもつながりセキュリティマネジメントの向上に資する。

(ｳ) 秘密文書の管理に関する規程と情報セキュリティ関連規程の統合

各府省庁のセキュリティポリシーでは、情報システムに関係のない書面は対象外とされるが、社会的には情報システムに関係のない書面に係る漏えい事故等も情報セキュリティ事故として認識される。紙の文書をも情報セキュリティの対策範囲に明示的に広げた両規程の統合は推奨されるべき取組である。

(ｴ) 検疫認証システムの導入、内閣府外への電子メールの暗号化機能の導入及び IPv6 も考慮した公開ウェブサーバのセキュリティ対策

基幹システムに関わる取組であるため時期やコスト面の課題は大きいが、一歩踏み込んだ統合的な技術的対策として参考となる取組である。また今後の運用実態や実績結果に関する評価についても共有していくことにより、政府機関全体のマネジメント水準の向上に寄与するものと考えられる。

(ｵ) LAN パソコンのワープロソフト及び電子メールにおける、情報の格付を自動付与する仕組みの導入

情報の格付は情報セキュリティ対策の基本的な取組であり、職員への意識付けは日常的に徹底させなければならないが、失念することもあり得る。自動挿入により格付を強制させることは、格付漏れ等のミスの防止、習慣化につながり、さらに、情報の格付に関するマニュアル等を参照させることは職員への教育的効果も期待できる。

（４）所見

推奨事例候補として各府省庁の情報セキュリティ報告書、府省庁別概要資料から NISC が抽出した取組件数は 43 件に上った。いずれの取組も各府省庁の実情を鑑みた工夫が随所に見られ、自ら推奨事例として取り上げて欲しいという【自薦】へも３府省庁から“立候補”があった。

今回推奨事例とはならなかったが、各府省庁の取組の一例を挙げると、各職員が遵守すべき情報セキュリティ対策に関する事項を周知・徹底するために、情報セキュリティ確保のためのポイント集を作成し多頻度で各自が再確認できるようにした取組が複数の府省庁で見られた。こうした教育面での取組は地道ではあるが継続性を軸にして広く着実に情報セキュリティ意識の浸透、向上に貢献したものと思われる。また、頻発する情報漏えい対策として、セキュア USB の導入やオンラ

インストレージの活用を検討し開始している府省庁も複数あった。これら情報システムによる技術的対策は費用対効果を見積らねばならないが、人的な対策コストや事故リスクを分析し必要と判断したならば早急な予算化と導入が望まれる。その他、管理・マネジメント面での取組も数多く見られた。最高情報セキュリティ責任者と最高情報セキュリティアドバイザーが定期的に会合を実施する取組や、最高情報セキュリティアドバイザーが調達仕様書のチェックを定例化する取組は、些細な問題であっても必要な対策を速やかに行え、事故の未然防止に役立つと考えられる。

平成 22 年度は、特に５つの取組を推奨事例に定めた。NISC においては、これらの取組が政府全体に浸透するよう各府省庁に支援を行っていくものとする。各府省庁においては、当該推奨事例について議論し実態に即した独自の取組へと発展させるとともに、次年度以降の情報セキュリティ報告書でその取組と結果について記載されることを期待している。

第３章 平成 23 年度に取り組むべき政府機関の課題

平成 23 年度に取り組むべき主な課題は、次のとおり。

（１）情報セキュリティに関する動向を踏まえた課題

(a) 業務継続能力の強化

平成 23 年３月に発生した東日本大震災においては、行政サービスを提供する情報システムが機能不全に陥り、長期間にわたって行政サービスの提供が中断するなど、業務継続の観点からの対策の重要性が再認識された。東日本大震災のような大規模自然災害、さらにはそれに起因する停電を想定した上で、適切に行政サービスの提供が維持されるよう、あらかじめ業務継続計画を策定するなど業務継続能力の強化を図る必要がある。

(b) 標的型メール攻撃への対応

文面・送信元がより巧妙化してきている標的型メール攻撃の脅威に対して、今回、選定された推奨事例の取組を参考にし、標的型メール攻撃を想定した訓練を実施するなど、各府省庁において対応の強化を図る必要がある。

(c) 新たな技術に対する情報セキュリティ対策の強化

クラウドコンピュータ技術、スマートフォン、SNS、IPv6 等の新たな技術に関する動向を踏まえ、これら新たな技術の活用において情報セキュリティを確保する上で必要となる方策を検討するとともに、政府機関統一基準群についても、情報通信技術や環境の変化を踏まえた見直しを実施する必要がある。

(d) 安全な暗号利用の促進

政府機関における安全な暗号利用の促進のため、近年、安全性の低下が指摘されている暗号アルゴリズムからの着実な移行を図るとともに、急激な安全性の低下に備えた緊急避難的な対応について、引き続き検討を行う必要がある。

(e) 情報流出防止への取組

政府機関職員として最低限実施すべき事項をまとめた啓発資料を活用して、実際の事故・事例を踏まえた意識啓発を行うとともに、情報システムの効率的・継続的なセキュリティの向上に努めるなど、情報流出防止への取組の強化を図る必要がある。

（２）政府機関における取組に係る評価結果等を踏まえた課題

(a) 対策実施状況報告及び重点検査に係る評価結果を踏まえた課題

各府省庁における対策実施状況報告及び重点検査に係る評価結果から、各府省庁の情報セキュリティ対策は一定の水準を維持しているとはいえるが、一部の基本的な項目において十分とはいえない実施状況が確認されている。各府省庁においては、自府省庁の対策実施状況を踏まえ、適切に PDCA サイクルを回していく必要がある。

また、各府省庁においてより実態に即した点検が行われるよう、対策実施状況報告における点検方法の改善についても検討を行う。

(b) 公開ウェブサーバの脆弱性検査結果を踏まえた課題

一部の府省庁の公開ウェブサーバにおいて危険度の高い脆弱性があることが、平成 22 年度に実施した脆弱性検査により判明している。平成 23 年度においても、希望府省庁に対して、公開ウェブサーバの脆弱性検査を実施し、得られた結果を全府省庁で共有して、政府機関全体の対策状況の底上げを図る必要がある。

(c) 情報セキュリティ報告書の記載内容を踏まえた課題

各府省庁が作成した情報セキュリティ報告書から、平成 22 年度に幾つかの府省庁において、深刻な情報漏えいにつながりかねない障害事故等が発生していたことが分かる。これら障害事故等の事例及びそれに基づき実施された対策について、発生府省庁だけではなく他府省庁においても参考とすることにより、政府全体で障害事故等の発生防止に向けた取組を強化していく必要がある。

また、情報セキュリティ報告書については、平成 23 年度から全ての府省庁において公表することとなるため、各府省庁においては平成 22 年度版の作成における経験等を踏まえ、国民に分かりやすい情報セキュリティ報告書の作成が望まれる。

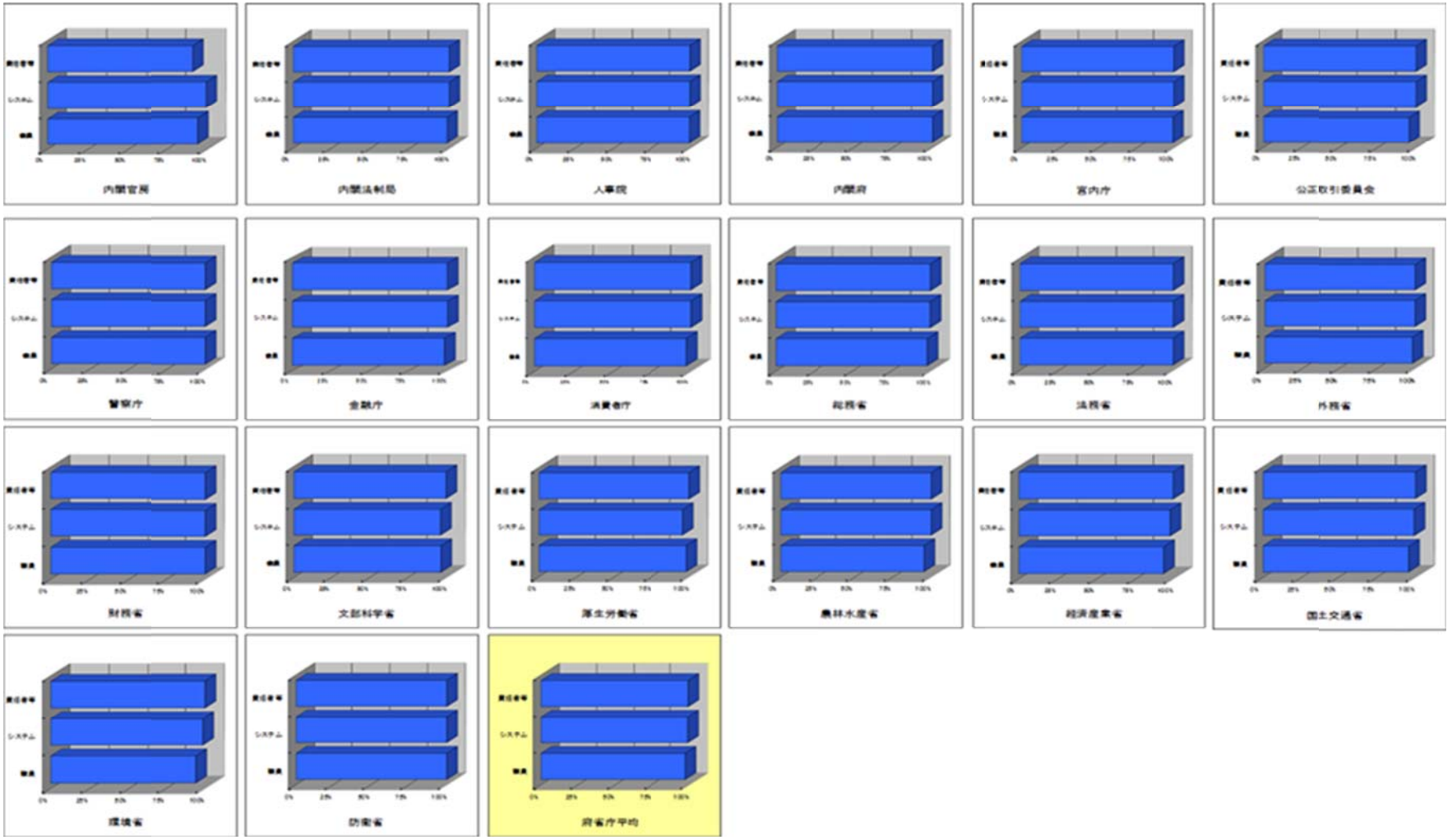
参考１　　政府機関に係る情報セキュリティ対策の主な取組

時期(年月)	主な取組
平成 17 年４月	○　内閣官房情報セキュリティセンターの発足
平成 17 年 12 月	○　政府機関統一基準（初版）の決定
平成 18 年２月	○　第１次情報セキュリティ基本計画の決定
平成 18 年６月	○　セキュア・ジャパン２００６の決定
平成 19 年６月	○　セキュア・ジャパン２００７の決定
平成 19 年６月	○　政府機関統一基準（第２版）の決定 ＜主な改訂内容＞ IPv6 対応、踏み台対策、暗号モジュール試験・認証制度の利用、情報セキュリティ監査体制の明確化、情報システム台帳の整備
平成 20 年２月	○　政府機関統一基準（第３版）の決定 ＜主な改訂内容＞ DNS キャッシュポイズニング対策、 なりすましサイト対策としてのドメインネーム管理
平成 20 年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５月	○　情報セキュリティ報告書専門委員会（第１回）の開催 ＜情報セキュリティ報告書専門委員会の開催状況＞ 2009 年５月　情報セキュリティ報告書専門委員会（第１回） 2009 年７月　情報セキュリティ報告書専門委員会（第２回） 2009 年７月　情報セキュリティ報告書専門委員会（第３回） 2009 年９月　情報セキュリティ報告書専門委員会（第４回）
平成 21 年６月	○　セキュア・ジャパン２００９の決定
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 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）と統一技術基準（技術）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「政府機関の情報セキュリティのための統一規範」に更新 ・「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」を修正 クラウド技術への対応、 外部からの不正アクセスに係る対応、 情報システムのセキュリティ強化に係る対応、 教育・人材育成の充実

（参考２）各府省庁の対策実施状況報告（平成 22 年度）の集計結果

○実施率



（参考２）各府省庁の対策実施状況報告（平成 22 年度）の集計結果

○到達率