平成 23 年度
情報セキュリティ報告書

平成 24 年５月

総　務　省

【 目 次 】

１　はじめに　～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。

このような中、総務省においては、平成 23 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) 職員に対する情報セキュリティ教育
(2) 公開用ウェブサーバの対策状況の監査

(1) については、職員に対する情報セキュリティ教育及び自己点検の結果を踏まえて、一部改善の余地がある遵守事項を中心とした情報セキュリティ教材を作成し、情報セキュリティ対策の実施状況の改善を促しました。
(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。

また、個人情報の誤送信を踏まえ、個人情報の厳重かつ適正な管理に努めるとともに、昨今、防衛関連企業や衆参両院など、主要な機関に対する標的型攻撃が問題となる中、総務省においてもウイルス感染事案が判明したことを受け、情報セキュリティの一層の強化に取り組みました。

本報告書は、上記を始めとして、総務省が平成 23 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、平成 24 年度以降の対策実施に資するべく作成したものです。
総務省は、情報通信、行政の情報化等を所管する省として、情報通信技術の最新の動向等を踏まえ、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）
吉良　裕臣

２　報告の基本情報

この章では、本報告書が対象とする期間や組織等、報告に関する基本的な情報について明らかにする。

(1) 総務省の概要

総務省は、行政組織、公務員制度、地方行財政、選挙、消防防災、情報通信、郵政事業など、国家の基本的仕組みに関わる諸制度、国民の経済・社会活動を支える基本的システムを所管しており、国民生活の基盤に広く関わる行政機能を担っている。

(2) 情報セキュリティ関係機関の概要

総務省においては、情報セキュリティ政策会議[1]が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。）の下、情報セキュリティ対策を実施している。

(3) 対象とする期間

本報告書が対象とする期間は、平成 23 年４月１日から平成 24 年３月 31 日までの１年間である。

(4) 対象とする組織

本報告書が対象とする組織は、総務省本省、外局、地方支分部局等である。

(5) 対象とする情報

本報告書が対象とする情報は、「政府機関の情報セキュリティ対策のための統一規範」、「政府機関の情報セキュリティ対策のための統一管理基準」、「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」 等（以下「政府機関統一基準群」という。）に基づき、「総務省情報セキュリティポリシー（管理編）」及び「総務省情報セキュリティポリシー（技術編）」（以下「総務省情報セキュリティポリシー」という。）において、総務省における情報セキュリティ対策の対象とされている以下の情報である。

○　情報システム内部に記録された情報
○　情報システム外部の電磁的記録媒体に記録された情報
○　情報システムに関係がある書面に記載された情報

(6) 責任部署

本報告書の責任部署は、大臣官房企画課情報システム室である。

---

[1] 「情報セキュリティ政策会議の設置について」（平成 17 年５月 30 日高度情報通信ネットワーク社会推進戦略本部決定、平成 19 年 11 月 17 日改訂）に基づき、高度情報通信ネットワーク社会推進戦略本部に設置。

３　情報セキュリティ対策の枠組み

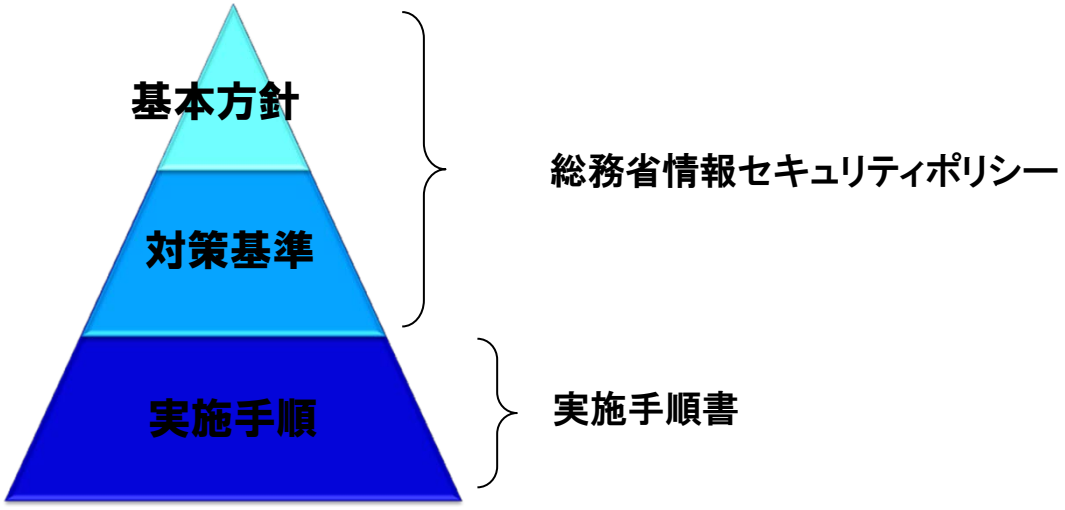
この章では、情報セキュリティ対策に関する文書体系や情報セキュリティ対策の推進体制といった総務省における情報セキュリティ対策の枠組みについて報告する。

(1) 情報セキュリティ対策に関する文書体系

総務省では、政府機関統一基準群に基づき、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として、総務省情報セキュリティポリシーを定めている。また、総務省情報セキュリティポリシーに定められた遵守事項を運用するための手順を示す文書として、以下の８種類の実施手順書を整備している（図１）。

○　障害・事故等対応手順書
○　省外での要保護情報の情報処理の手順書
○　省外へのファイル提供及びウェブサーバ公開における省外での情報セキュリティ対策への配慮に関する規程
○　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
○　情報セキュリティ対策のためのコーディング規約策定の手引き
○　人事異動等の際に行うべき情報セキュリティ対策実施規程
○　総務省支給以外の情報システムによる情報処理の手順書
○　総務省情報セキュリティポリシー例外措置手順書

図１　総務省情報セキュリティポリシー及び実施手順書の位置付け



(2) 情報セキュリティ対策の推進体制

総務省では、情報セキュリティ対策を推進するために、政府機関統一基準群、総務省情報セキュリティポリシー等に基づき、以下に示す体制を整備している（図２）。

① 最高情報セキュリティ責任者

総務省における情報セキュリティ対策に関する事務を統括している。総務省においては、大臣官房長が務めている。

② 最高情報セキュリティアドバイザー

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専門家として、総務省の情報セキュリティ対策について専門的な助言を行っている。総務省においては、総務省ＣＩＯ補佐官（情報セキュリティ担当）が務めている。

③ 情報セキュリティ委員会

総務省情報セキュリティポリシーの改訂等情報セキュリティに関する重要事項の決定を行う組織として設置している。総務省においては、情報セキュリティ委員会の委員長は、最高情報セキュリティ責任者が務めている。

④ 情報セキュリティ監査責任者

最高情報セキュリティ責任者の指示に基づき、情報セキュリティ監査に関する事務を統括する。総務省においては、大臣官房企画課情報システム室長が務めている。

⑤ 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を補佐するとともに、情報セキュリティ責任者を統括する。総務省においては、大臣官房企画課長が務めている。

⑥ 情報セキュリティ責任者

部局内の情報セキュリティ対策に関する事務を統括する。

⑦ 情報システムセキュリティ責任者

所管する情報システムに対するセキュリティ対策に関する事務を統括する。

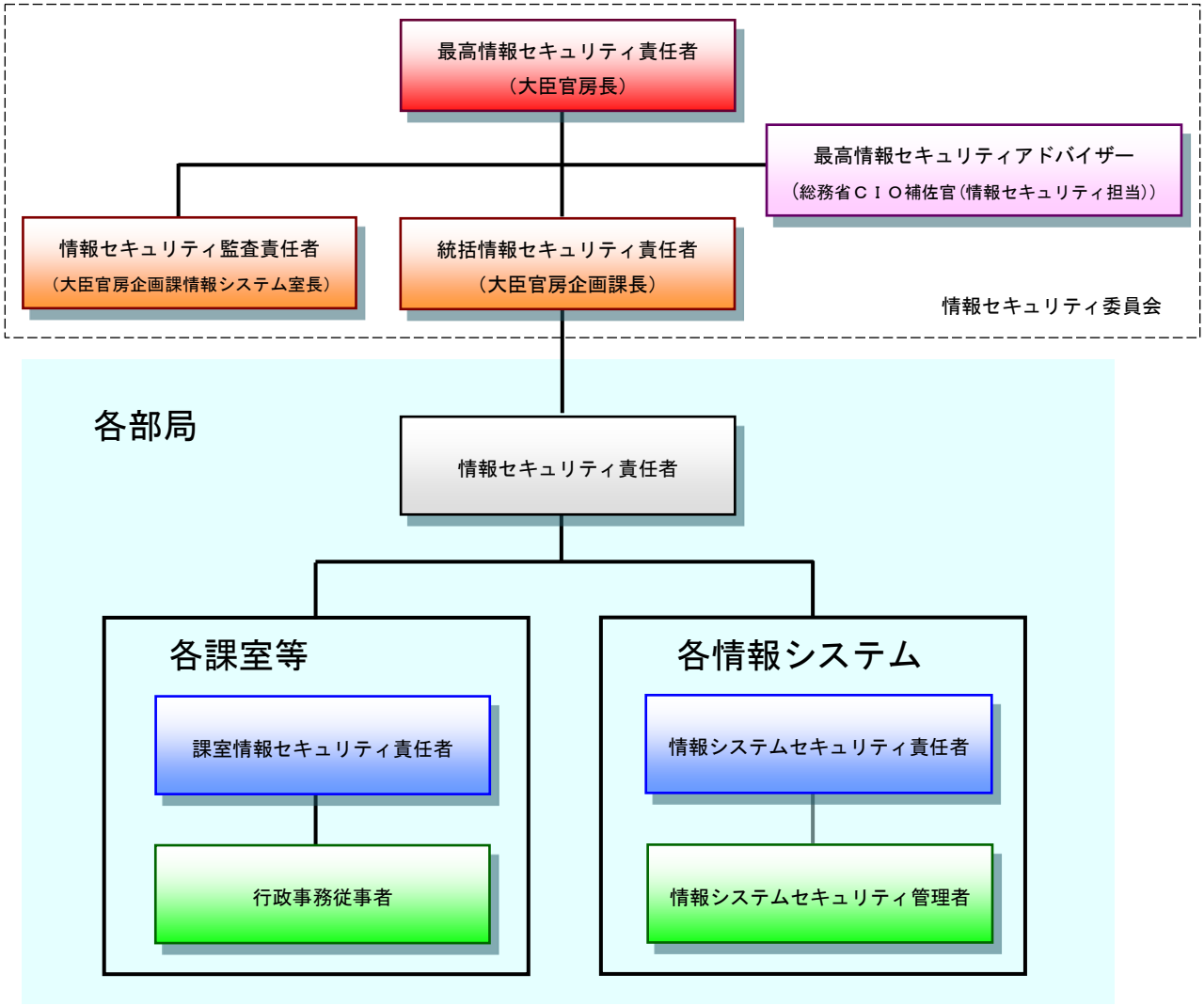
⑧ 情報システムセキュリティ管理者

所管する情報システムの管理業務における情報セキュリティ対策を実施する。

⑨ 課室情報セキュリティ責任者

課室等における情報セキュリティ対策に関する事務を統括する。

図２　総務省における情報セキュリティ対策の推進体制



４　平成 23 年度における情報セキュリティ対策の実施状況

この章では、総務省において平成 23 年度に実施した情報セキュリティに関する教育及び自己点検、情報システムの重点検査、情報セキュリティ監査等の情報セキュリティ対策の実施状況について報告する。

(1) 情報セキュリティに関する教育及び自己点検

①　概要

（ア）　情報セキュリティに関する教育

総務省情報セキュリティポリシー、実施手順書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。

（イ）　情報セキュリティ対策の自己点検

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。なお、政府機関統一基準群等において、政府機関における情報セキュリティ対策推進の観点から、政府機関統一基準群に基づく各府省庁における情報セキュリティ対策の実施状況について、ＮＩＳＣに報告することが定められている。

②　対象者

情報セキュリティに関する教育及び自己点検の対象者は、総務省におけるすべての職員（出向者及び非常勤職員を含む。）である。

③　内容及び手法

情報セキュリティに関する教育及び自己点検の内容は、職員の役職及び職務の内容に応じて以下の３つに区分し、それぞれの区分で実施すべき情報セキュリティ対策に沿ったものとした。

○　課室情報セキュリティ責任者
○　情報システムセキュリティ責任者・管理者
○　行政事務従事者

また、e-ラーニングシステムを活用し、情報セキュリティ教育及び第１回自己点検を同時に実施した後、第１回自己点検の結果を踏まえて、一部改善の余地がある遵守事項を中心とした情報セキュリティ教材を作成し、情報セキュリティ対策の実施状況の改善を促した上で、第２回自己点検を実施した。

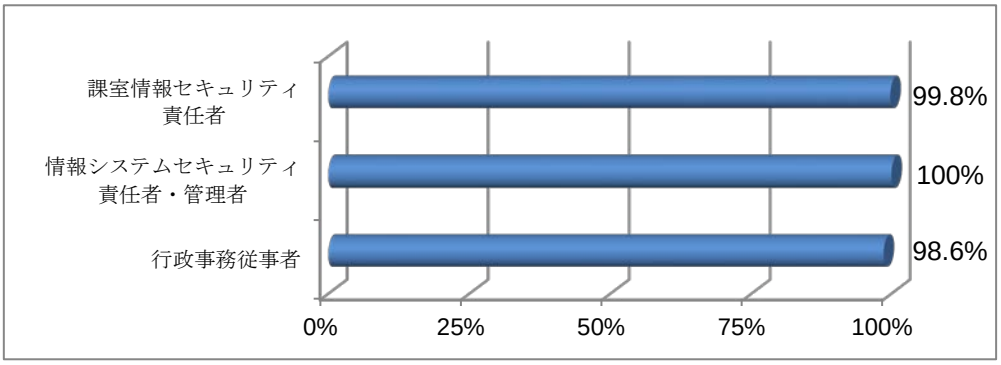
なお、自己点検の結果については、外部監査を実施することにより、その適正性及び信頼性を確認した。

④　結果

（ア）　把握率

把握率（報告対象者のうち、対策実施状況が把握できた者の割合）は、課室情報セキュリティ責任者は 99.8%、情報システムセキュリティ責任者・管理者は 100%、行政事務従事者は 98.6%であった。（表１）

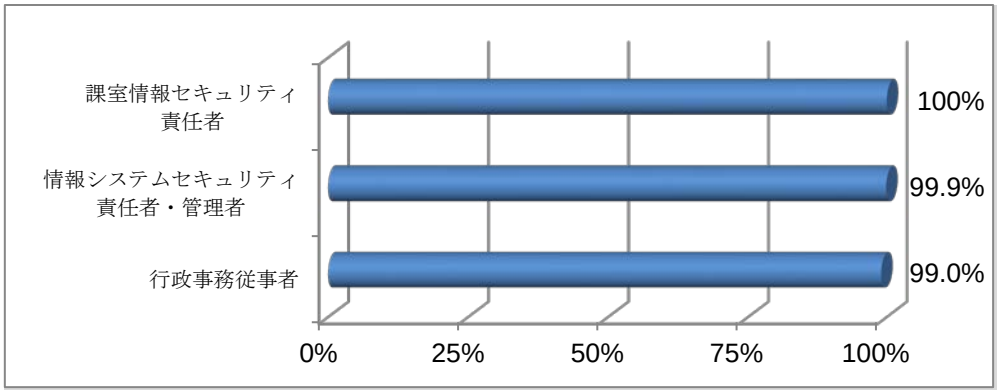
表１　把握率（区分別）



（イ）　実施率

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）は、課室情報セキュリティ責任者は 100%、情報システムセキュリティ責任者・管理者は 99.9%、行政事務従事者は 99.0%であった。（表２）

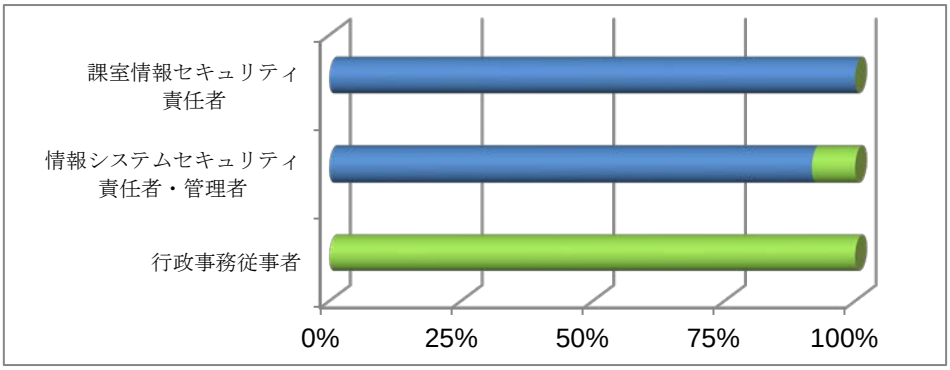
表２　実施率　（区分別）



（ウ）　到達率

到達率（把握した者のうち、政府機関統一基準群に掲げられている各遵守事項について、一定の割合（100%、95%、90%）以上の者が対策を実施した事項の割合）は、到達率が 100 の場合、課室情報セキュリティ責任者は 100%、情報システムセキュリティ責任者・管理者は 91.7%、行政事務従事者は 0%であった。到達率が 95 の場合、課室情報セキュリティ責任者、情報システムセキュリティ責任者・管理者、行政事務従事者のいずれも 100%であった。（表３）

表３　到達率（区分別）



（エ）　自己点検の結果の総括

（ア）～（ウ）を踏まえると、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たと言える。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、情報セキュリティ対策の自己点検の状況を e-ラーニングシステムから確認し、未実施者に対して実施を促すとともに、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ことが必要である。

(2) 情報システムの重点検査

①　概要

情報システムの重点検査は、各府省庁における政府統一基準群に準拠した情報セキュリティ対策の実施状況を確認するためにＮＩＳＣが実施する調査であり、十分な対策が取られていない府省庁に改善を促すことをもって政府機関全体の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されるものである。本年度は、ＮＩＳＣが配布する調査票に基づき、公開用ウェブサーバ、電子メールサーバを対象に実施した。

②　結果

（ア）　公開用ウェブサーバ

すべての公開用ウェブサーバにおいて、重点検査項目（表４）として掲げられた対策は、100%の実施率を達成した。

表４　公開用ウェブサーバに関する重点検査項目

対策の種類	重点検査項目
不正プログラム対策	・ＯＳのパッチ等の適用状況（アップデートの状況） ・ウェブサーバアプリケーションのパッチ等の適用状況（アップデートの状況）
脆弱性の調査	・ＳＳＬバージョン２の無効化状況 ・ＳＳＬ通信で弱い暗号方式の無効化状況
大量パケットと送信型のＤｏＳ攻撃への対策	・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サービス不能攻撃への対応状況 ・サービス不能攻撃を受けた場合、影響最小化への対応状況 ・サービス不能攻撃に関する監視対象の特定、監視方法及び監視記録の保存期間策定への対応状況 ・サービス不能攻撃発生時の対処手順や連絡体制整備の対応状況

（イ）　電子メールサーバ

すべての電子メールサーバにおいて、重点検査項目（表５）として掲げられた対策は、100%の実施率を達成した。

表５　電子メールサーバに関する重点検査項目

対策の種類	重点検査項目
不正プログラム対策	・ＯＳのパッチ適用状況(アップデートの状況) ・電子メールサーバアプリケーションのパッチの適用状況（アップデートの状況）

③　重点検査結果の総括

公開用ウェブサーバ、電子メールサーバのすべての検査において、100%の実施率を達成した。今後もこの状態を維持するため、引き続き政府機関統一基準群及び総務省情報セキュリティポリシー等に基づく適切な情報セキュリティ対策の実施に努める。

(3) 情報セキュリティ監査

①　概要

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、「平成 23 年度総務省情報セキュリティ監査計画書」に基づき、情報セキュリティ監査実施部局及び被監査部局以外の第三者による情報セキュリティ監査を実施した。

② 監査の内容

実施した情報セキュリティ監査の内容は、以下のとおりである。

（ア） 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

総務省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ことを確認する監査。

（イ） 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

実施手順書が、総務省情報セキュリティポリシーに準拠していることを確認する監査。

（ウ） 自己点検の適正性監査

情報セキュリティ対策の自己点検結果が、総務省における情報セキュリティ対策の実施状況を適切に反映していることを確認する監査。

（エ） 例外措置の申請の監査

総務省情報セキュリティポリシーの例外措置の申請に対して、総務省情報セキュリティポリシー例外措置手順書に基づき適切な審査が実施されていることを確認する監査。

（オ） 主要な情報システムの運用に関する監査

総務省が運用する情報システムから選定した主要な情報システムについて、政府機関統一基準群及び総務省情報セキュリティポリシーに準拠した運用管理規程が策定され、運用管理規程に準拠した運用管理が行われていることを確認する監査。

（カ） 公開用ウェブサーバの対策状況の監査

総務省が運営し外部に公開しているすべてのウェブサーバについて、ネットワーク及びウェブアプリケーションの脆弱性の有無を確認する監査。

③ 監査の結果

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、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。

（ア） 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

総務省情報セキュリティポリシーは、政府機関統一基準群が要求する事項をおおむね満たしていることが確認された。

（イ） 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

実施手順書は、総務省情報セキュリティポリシーが要求する事項をおおむね満たしていることが確認された。

（ウ） 自己点検の適正性監査

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た。

（エ） 例外措置の申請の監査

例外措置の申請及び許可状況は、総務省情報セキュリティポリシーが要求する事項をおおむね満たしていることが確認された。

（オ） 主要な情報システムの運用に関する監査

監査対象の情報システムは、総務省情報セキュリティポリシー及び各情報システムの運用管理規定に基づいて適切に運用されていることが確認された。

（カ） 公開用ウェブサーバの対策状況の監査

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。脆弱性の検出状況については、推奨する対策等とともに報告書にまとめて情報システムの担当者に通知するとともに、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。

(4) 職員に対する情報提供・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ため、以下の取組を実施した。

① セキュリティ情報の提供

ＮＩＳＣ、最高情報セキュリティアドバイザー及び情報セキュリティ支援業者から提供される脆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）等を省内に広く周知し、必要な情報セキュリティ対策の実施を促した。

② 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

職員の情報セキュリティに対する理解の促進及び適切な情報セキュリティ対策の実施を目的として、最高情報セキュリティアドバイザーから、下記のような機会を通して、各種の情報提供を実施した。

（ア） 新規採用者等向け研修

新規採用者や新任の課長、課長補佐、係長等への研修の中で、最高情報セキュリティアドバイザーによる情報セキュリティに関する講義を行った。

（イ） 情報セキュリティに関する相談会の開催

最高情報セキュリティアドバイザーによる情報セキュリティに関する相談会を開催した。

③ イントラネットにおける情報発信

総務省情報セキュリティポリシーや実施手順書、情報セキュリティに関する教育教材等、情報セキュリティに関連する情報をイントラネット上に掲示し、職員が日常的に参照できるようにした。

(5) その他の取組事項

① 標的型攻撃への対応

総務省におけるウイルス感染事案を踏まえ、ウイルス感染防止対策の強化に努めるとともに、未知のウイルスに感染した場合にも、早期に感染を発見し、被害の拡大の防止に努めるため、主に以下の対応を進めた。

（ア） 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標的型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、以下を実施した。

（ⅰ） 不審なメールへの適切な対応についての職員への周知・徹底

新種のウイルスも日々生み出されており、ウイルス対策ソフトウェアが防御できないウイルスもあることから、職員に対し、ウイルスへの感染を防ぐため、差出人名や件名に心当たりがない不審なメールを受信した場合は、メールを開封せずに担当部署に連絡すること、また、受信したメールの添付ファイルを開いた又は本文中の URL をクリックした後に当該メールは不審なメールであったことに気付いた場合は、ウイルスの拡散を防ぐため、直ちに LAN ケーブルを抜き、担当部署に連絡することを周知・徹底するよう注意喚起を行った。

（ⅱ） 標的型攻撃に対する訓練

総務省においては、平成 13 年度以来、職員に対して不審なメールを装ったメールを送付し、職員が不審なメールへの適切な取扱いを身に付けるよう努めてきた。しかしながら、平成 23 年 11 月に総務省におけるウイルス感染事案が判明したことを踏まえ、不審なメールを装ったメールの文面を実際の不審なメールにより近いものとした上でメールを送付し、職員の不審なメールへの適切な対応の強化を図った。

（iii） 不審メール情報の共有

ＮＩＳＣから提供される不審メール情報について、省内に広く周知し、職員に対し、不審なメールへの適切な対応を呼びかけた。

（イ） 総務省ＬＡＮにおける情報セキュリティの強化

ウイルス感染防止対策の強化に努めるとともに、未知のウイルスに感染した場合にも、早期に感染を発見し、被害の拡大を防止するため、総務省ＬＡＮにおいて、

○ウイルス感染防止対策の強化
○ウイルスに感染した場合であっても、早期に感染を発見できる仕組みの整備
○ウイルス感染の拡大を防止する仕組みの整備
○外部への情報の流出を極力食い止める仕組みの整備
○情報が流出した場合であっても、流出した情報を可能な限り特定できる仕組みの整備

といったように、想定される局面ごとに、情報セキュリティの一層の強化に努めている。

② 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。

このため、省内各部局等が行う情報システムの調達に資するため、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。

また、調達に当たっては、ＣＩＯ補佐官への相談会を開催し、調達仕様書案等の妥当性確認を行っており、その中で、情報セキュリティ要件についても、確認を行っている。

③ 職員用端末へのセキュリティ対策シールの貼付

職員が、総務省情報セキュリティポリシーに基づく情報セキュリティ対策を日常的に参照できるよう、これらをまとめたシールを作成し、職員用端末へ貼付している。

④ 障害・事故等への対応

平成 23 年度は、以下の障害・事故等が発生した。

○個人情報の誤送信（１件）

総務省中国総合通信局において、平成 23 年４月 13 日（水）９時 53 分と 10 時 34 分の２度に分けて、管内の複数の電気通信事業者の担当者（計 144 宛先）に対し、事務連絡メールをそれぞれ一斉送信した際、災害時連絡先として登録された

個人の電話番号、メールアドレス（延べ 49 件）を記載したファイルを添付した形で送信した。

これを受け、本件で御迷惑をおかけした関係者の方々に対し、直ちに御報告とお詫びを申し上げるとともに、当該メールの削除をお願いした。

今後このような事態が生じないよう、個人情報の厳重かつ適正な管理を実施する。

○情報流出を伴うウイルス感染（１件）

総務省において、平成 23 年 11 月、総務省職員用の 23 台の端末が、新種のトロイの木馬型ウイルスに感染していたことが判明するとともに、これらの端末から、当該感染により、何らかの情報が外部に送信されたことが確認された。

なお、外部に送信された情報には、業務で関わった方の名刺情報などの個人情報、職員やその家族の個人情報、業務上の情報が含まれている可能性がある。

これを受け、総務省における情報セキュリティを一層強化するため、ウイルス感染防止対策の強化に努めるとともに、未知のウイルスに感染した場合にも、早期に感染を発見し、被害の拡大の防止に努められるよう、対策を進めている。

５　情報セキュリティ対策に関する平成 24 年度の計画

平成 24 年度は、以下の事項に重点的に取り組む。

(1) 総務省情報セキュリティポリシー等の見直し

昨今の標的型攻撃への対策等を念頭に政府機関統一基準群の改定がなされたことを踏まえ、総務省情報セキュリティポリシー等を見直し、総務省において必要な情報セキュリティ対策が実施されるよう努める。

(2) 情報セキュリティに関する教育及び自己点検

情報セキュリティに関する教育の内容について、政府統一基準群の改定を踏まえた総務省情報セキュリティポリシーの改定内容、平成 23 年度の自己点検の結果、情報セキュリティ監査の結果及び昨今の情報セキュリティを取り巻く情勢等を踏まえ、より効果的なものとなるよう見直しを実施する。

また、情報セキュリティ対策の自己点検を実施して、情報セキュリティ対策の実施状況を確認し、その結果を踏まえて情報セキュリティ対策の実施状況の改善を促す。

(3) 最新の脅威を踏まえた職員への訓練、情報提供等

標的型攻撃によるウイルス感染を防止するため、職員に対し、最新の脅威を踏まえ、不審なメールへの適切な対応を周知・徹底するよう引き続き注意喚起を行う。併せて、職員に対して最新の脅威に即した不審なメールを装ったメールを送付し、職員が不審なメールへの適切な対応を強化するよう努める。

また、不審メール情報や脆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）等を省内に広く周知し、必要な情報セキュリティ対策の実施を促す。

さらに、個人情報の厳重かつ適正な管理に努める。

(4) 最新の攻撃手法を踏まえた情報セキュリティ監査

総務省が運営し外部に公開しているすべてのウェブサーバについて、最新の攻撃手法を踏まえ、ネットワーク及びウェブアプリケーションの脆弱性の有無を確認する監査を実施する。

また、本監査以外のこれまでに実施してきた情報セキュリティ監査についても、より効率的な監査方法を検討し、監査の対象となる部署の負担の軽減も図りつつ、網羅性及び深度をバランスよく両立させた上で、実施する。

６　おわりに　～最高情報セキュリティアドバイザーからのメッセージ～

総務省では、システム関連から教育、啓発まで幅広く情報セキュリティ対策を行ってきた。しかしながら万全というわけにはいかず、本報告書に記載されているような事故を起こしてしまったことは、誠に遺憾である。

サイバー攻撃の脅威が増す中、新しい脅威に対応した新しい取組が求められている。最近見られるサイバー攻撃では、従来のウイルスワクチンや侵入検知システム等では防ぎきれないものが少なくない。防御や検知に関わる従来のセキュリティシステムや運用を見直しており、再発防止の取組に努めている。

事故が起きないように防御策を強化することはもちろんのことながら、万が一のときを想定し、より早く検出する仕組みや、素早く的確に判断し対処する仕組みへの取組を強化した。

一方で、セキュリティの強化に伴う利便性の低下にも配慮しており、新しい技術への対応を含め、セキュリティと利便性を高い次元で実現するべく情報収集、研究に努めている。

また、総務省に導入するシステムにおいては、その新規構築案件の調達段階からセキュリティ要件の組込みが必要であるため、ＣＩＯ補佐官による相談会を適宜開催し、チェックやアドバイスを行っている。また、システムの更改時点でも構築時点では想定されていなかった事項についても改善を行うよう推奨する取組を行っている。

今後も、必要に応じて関係機関とも連携し、新しい脅威の情報収集やセキュリティ対策の強化に努める。また、クラウドやスマートフォンなどのモバイル端末などの新しい技術の活用に関しても、セキュリティ上の問題を最小限にするように検討を進める。

総務省最高情報セキュリティアドバイザー
（総務省ＣＩＯ補佐官（情報セキュリティ担当））
三輪 信雄