平成 23 年度 財務省情報セキュリティ報告書

財務省

平成 24 年 5 月

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、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連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）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、今後、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、政府全体の取組を踏まえ、国の予算や税の賦課・徴収といった国民生活に密接に関連する所掌事務の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います。その観点から、平成 23 年度は、以下の主な取組を実施しました。

- 地方支分部局を含むすべての財務省職員による情報セキュリティ対策の「自己点検」を実施しました。
- 「自己点検」の結果や、財務省の情報セキュリティ関係規程の内容、財務省所管の情報システムの管理・運営におけるセキュリティ対策の実施状況等について、監査を実施しました。その一部には外部監査を導入しました。
- 標的型メール攻撃や「なりすましメール」といった新たな脅威について、財務省職員への注意喚起や訓練、システム面での対応等の取組を行いました。
- 財務省の情報セキュリティ規程について、政府の統一基準の改定に合わせた見直しを行うとともに、情報の省外への持ち出し等について関連規則を具体化させました。
- 職員の情報セキュリティ意識の向上のため、①すべての職員を対象とした集合研修を 18 回にわたって実施、②常時自習が可能な e ラーニングの研修教材を見直し、③課室長や情報システム管理課室向けの研修を実施するなどの取組を行いました。

財務省においては、自己点検及び監査により、情報セキュリティ対策が適正に実施されていることが確認されております。また、その他の取組により、規程、システム、職員意識など複合的な観点から情報セキュリティの強化が図られています。本報告書では、こういった平成 23 年度の財務省の情報セキュリティ対策をご紹介します。

財務省としては、今後とも、内閣官房等の関係政府機関と連携し、情報セキュリティ対策の強化に努めてまいります。

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

---

* 情報窃取を目的として、特定の相手を狙い、送信者の詐称やタイトル又は本文の巧妙な記述内容によって、添付ファイルを開かせたり、メール本文中のリンク先をクリックさせることにより、ウイルスに感染させるメール。

２．本報告の基本情報

(1) 財務省の任務

財務省は、健全な財政の確保、適正かつ公平な課税の実現、税関業務の適正な運営、国庫の適正な管理､通貨に対する信頼の維持及び外国為替の安定の確保を図ることを任務としています。この任務を着実に実現するため、財務省においては、必要な情報システムを構築・運用することにより、効率的な事務運営に努めています。

（参考）財務省の主な情報システム

- 予算編成支援システム
- 通関情報総合判定システム（CIS）
- 国有財産総合情報管理システム
- 官庁会計システム（ADAMSⅡ）
- 国税総合管理システム（KSK システム）
- 国税電子申告・納税システム（e-Tax）
- 財務省行政情報化 LAN システム

(2) 対象とする期間

平成 23 年 4 月 1 日～平成 24 年 3 月 31 日

(3) 対象とする組織

財務省の全部局

具体的には、財務省本省の内部部局（大臣官房及び各局)、施設等機関（財務総合政策研究所、会計センター、関税中央分析所及び税関研修所）及び地方支分部局（財務局、税関及び沖縄地区税関）並びに国税庁の内部部局（長官官房及び各部)、施設等機関（税務大学校)、特別の機関（国税不服審判所）及び地方支分部局（国税局及び沖縄国税事務所）

(4) 対象とする情報

「政府機関の情報セキュリティ対策のための統一管理基準(平成 23 年 4 月 21 日 情報セキュリティ政策会議決定)」（以下「政府統一管理基準」という。）で定義された「情報」。すなわち、「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及び情報システムに関係がある書面に記載された情報」。

(5) 本報告の担当部局

財務省大臣官房文書課業務企画室（以下「業務企画室」という。）

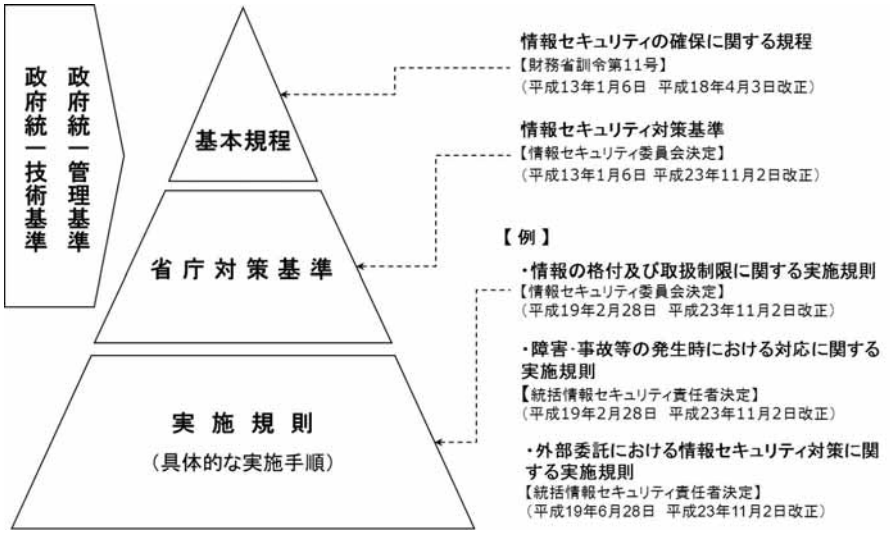
３．情報セキュリティ対策の枠組み

(1) 情報セキュリティ対策に関する文書体系

財務省では､「情報セキュリティの確保に関する規程（財務省訓令第 11 号)」において、財務省の情報セキュリティ対策に関する体制等について定めています。また、政府機関全体の統一的な枠組み（「政府統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準（平成 23 年 4 月 21 日 情報セキュリティ政策会議決定)」（以下「政府統一技術基準」という。)）を踏まえ、情報セキュリティ対策に係る基本的な事項について、「情報セキュリティ対策基準」（以下「財務省対策基準」という。）を定めています。

さらに、「財務省対策基準」で定められた事項の具体的な実施手順等について、155 本の実施規則等を整備しています（以下「財務省実施規則」という。）。

図１．財務省の情報セキュリティ関連文書体系



(2) 情報セキュリティ対策の推進体制

財務省では、図２に示すとおり、最高情報セキュリティ責任者及び統括情報セキュリティ責任者の下、各部局に情報セキュリティ責任者を置き、情報セキュリティ対策を推進しています。また、各情報セキュリティ責任者の下、各課室等に課室情報セキュリティ責任者（課室長等）、各情報システムに情報システムセキュリティ責任者（当該情報システムの所管課室長等）を置いています。なお、財務省の情報セキュリティ対策に係る総合調整については、業務企画室が担当しています。

① 情報セキュリティ委員会

「財務省対策基準」の策定又は変更並びに財務省における情報セキュリティ対策の評価及び見直し、その他情報セキュリティの確保に関する事務を総括する組織として、情報セキュリティ委員会を設置しています。委員長は最高情報セキュリティ責任者、副委員長は統括情報セキュリティ責任者、委員は財務省本省等の情報セキュリティ責任者が務めています。

② 最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

情報セキュリティ対策に関する事務を統括します。財務省では、大臣官房長が務めています。

③ 最高情報セキュリティアドバイザー

財務省の情報セキュリティ対策の企画立案・実施等について、最高情報セキュリティ責任者や業務企画室に助言を行います。財務省では、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を最高情報セキュリティアドバイザーに指名しています（平成 23 年度は村田正憲補佐官）。

（注）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。

④ 情報セキュリティ監査責任者

情報セキュリティ監査に関する事務を統括します。財務省では、大臣官房審議官又は大臣官房参事官が務めています。

⑤ 統括情報セキュリティ責任者

情報セキュリティ責任者を統括します。財務省では、大臣官房文書課長が務めています。

⑥ 情報セキュリティ責任者

部局における情報セキュリティ対策に関する事務を統括します。財務省では、大臣官房各課長、各局総務課長等及び地方支分部局の総務部長等が務めています。国税庁においても同様に情報セキュリティ責任者を置いています。

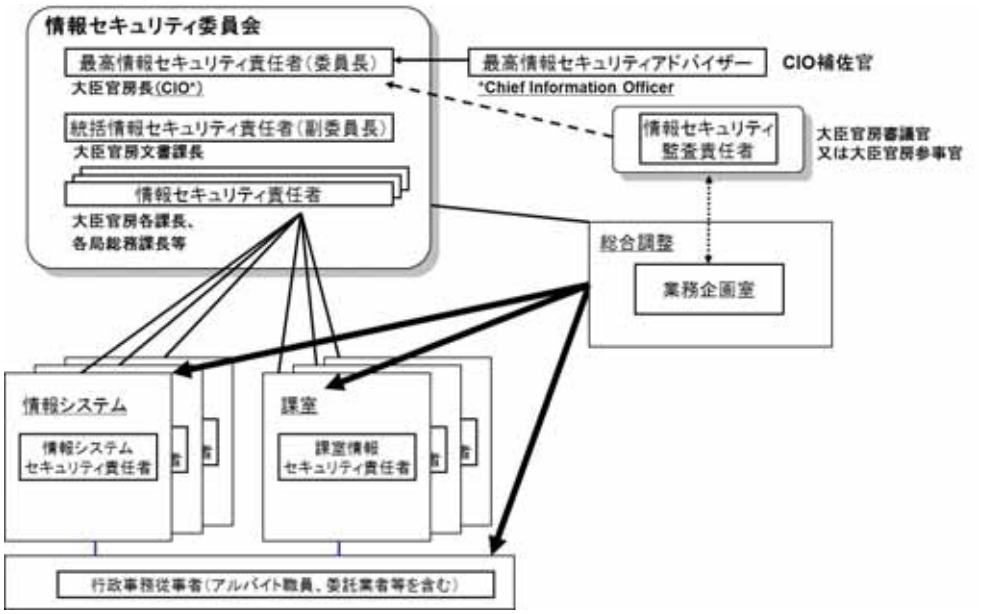
⑦ 情報システムセキュリティ責任者・管理者

情報セキュリティ責任者が指定する情報システムに対する情報セキュリティ対策の管理に関する事務を統括します。財務省では、情報セキュリティ責任者が指名する職員（情報システムを所管する課室長等）が務めています。情報システムセキュリティ責任者は、所属する部局の職員から情報システムセキュリティ管理者を指名し、情報セキュリティ対策の管理に関する事務の一部を処理させています。

⑧ 課室情報セキュリティ責任者

情報セキュリティ責任者が指定する課及び課に準ずる組織（地方支分部局においては部及び部に準ずる組織）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ます。財務省においては、情報セキュリティ責任者が指名する職員（財務省本省では各課室長等）が務めています。

図２ 財務省の情報セキュリティ体制



４．平成 23 年度の情報セキュリティ対策の取組

(1) 情報セキュリティ対策の自己点検

① 概要

財務省では、「財務省対策基準」に基づき、財務省の職員（行政事務従事者）に対して、「財務省対策基準」や「財務省実施規則」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 18 年度の導入以降、自己点検の対象を順次拡大し、平成 20 年度からはすべての財務省職員（国税庁職員を含む、また、非常勤職員や賃金職員を含む）を対象として実施しています。

平成 23 年度の自己点検は、財務省のすべての職員（行政事務従事者 79,091 名）を対象として実施しました。また、最高情報セキュリティ責任者、情報セキュリティ監査責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者、情報システムセキュリティ責任者・管理者については、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。

その際、平成 22 年度の自己点検において、把握率（すべての対象者のうち、自己点検の結果を報告した者が占める割合）、対策実施率（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）がすべて 100%であったところ、平成 23 年度も同様の結果が得られているか確認しました。また、到達率（すべての遵守事項のうち、対策実施率が一定の割合（100%・95%以上・90%以上）に到達している遵守事項が占める割合）については、対策実施率 100%・95%以上・90%以上を基準値として状況を確認しました。

② 結果

イ．把握率（すべての対象者のうち、自己点検の結果を報告した者が占める割合）

平成 23 年度の把握率は、前年度と同様、100.0%でした。（表３参照）

表３ 把握率の推移

年度	把握率
平成 21 年度	100.0%
平成 22 年度	100.0%
平成 23 年度	100.0%

ロ．対策実施率（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）

平成 23 年度の対策実施率は、前年度と比較し、情報セキュリティ責任者等について 100.0%から 99.9%に微減、その他の行政事務従事者について 100.0%から 99.8%に微減しました。（表４参照）

表４ 主体別対策実施率の推移

年度	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・管理者	その他の行政事務従事者
平成 21 年度	100.0%	100.0%	99.9%
平成 22 年度	100.0%	100.0%	100.0%
平成 23 年度	99.9%	100.0%	99.8%

ハ．到達率（すべての遵守事項のうち、対策実施率が一定の割合（100%・95%以上・90%以上）に到達している遵守事項が占める割合）

平成 23 年度は、対策実施率 95%以上を基準値とした場合、到達率は 100%でした（すなわち、すべての遵守事項の対策実施率が 95%以上）。しかしながら、対策実施率 100%を基準値とした場合、到達率は、情報セキュリティ責任者等について 98.0%（51 項目中 50 項目）、その他の行政事務従事者について 16.7%（6

項目中１項目）でした。（表５参照）

表５ 主体別対策到達率（平成 23 年度）

基準値	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・管理者	その他の行政事務従事者
対策実施率 100%	98.0%	100.0%	16.7%
対策実施率 95%以上	100.0%	100.0%	100.0%
対策実施率 90%以上	100.0%	100.0%	100.0%

③ 総評

以上の結果を踏まえると、平成 23 年度において、財務省では、一部の遵守事項について対策実施率が微減しましたが､引き続きすべての遵守事項の対策実施率が 95%以上であるなど､「財務省対策基準」や「財務省実施規則」の遵守事項は概ね適正に実施されている状況と言えます。財務省では、今後とも、遵守事項が適正に実施されるよう、職員の教育等の取組を行うこととしています。

(2) 情報セキュリティ監査

財務省では、省内における情報セキュリティ対策の状況を確認し、その後の対策に活用するため、毎年度、情報セキュリティ監査計画書を策定し、情報セキュリティ監査責任者の下、情報セキュリティ監査を実施しています。

その際、監査の客観性を担保するため、主要な情報システムについて外部監査を実施するとともに、その他の情報システム及び職員の自己点検に関する内部監査については、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立ち会いを一部導入しています。内部監査の立ち会いについては、幹部職員（財務省本省の各局総務課長等）を主な対象とすることにより、幹部職員の情報セキュリティに関する意識の向上と、組織内のトップダウンによる効果的な情報セキュリティ対策を図っています。また、地方支分部局を含めて監査を実施することにより､財務省全体のセキュリティ対策の適正性の確保に努めています。

以上の観点から、平成 23 年度は以下のとおり監査を実施し、その結果を最高情報セキュリティ責任者に報告しました。

① 情報セキュリティ関係規程に関する準拠性監査

「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)」､「政府統一管理基準」及び「政府統一技術基準」に対する「情報セキュリティの確保に関する規程」及び「財務省対策基準」の準拠性、並びに財務省の「情報セキュリティの確保に関する規程」及び「財務省対策基準」に対する各部局の「実施規則」等の準拠性について、最高情報セキュリティアドバイザーによる監査を実施し、それぞれ準拠していることを確認しました。

② 自己点検に関する監査

情報セキュリティ責任者、課室情報セキュリティ責任者、情報システムセキュリティ責任者・管理者及び行政事務従事者の一定数（人数の平方根に相当する数）を抽出し、情報セキュリティ対策の実施状況に関する自己点検（上記）の結果について内部監査を実施しました。その一部については、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立ち会いの下で実施しました。これらの監査により、自己点検が適正に実施されていることを確認しました。

③　情報システムに関する監査

財務省が管理･運営している情報システムの一定数(総数の平方根に相当する数)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 23 年度は、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（下記参照)。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 24 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。

（参考）最高情報セキュリティアドバイザーによる主な指摘

－運用・保守業者とのサービスレベル合意書（SLA）の締結・見直し

（情報システムの稼働率、不具合時復旧時間（RTO）等の適切な設定など）

－サーバ室等の物理的セキュリティの確保

（施錠の徹底、ガラス窓の保護、床面配線の回避など）

－非常時対応の整備

（消火設備・免震設備の整備、データバックアップの見直しなど）

(3) 標的型メール攻撃への対応

平成 23 年度、財務省では、標的型メール攻撃について以下の取組を行いました。

・ 内閣官房情報セキュリティセンター（NISC）等との情報共有により、特定のメールアドレスからのメールをシステム上で自動的に遮断。
・ 日々の業務における標的型メール攻撃のリスクへの意識を高めるため、職員に対する注意喚起を実施（注意喚起メールの配信、ポータルサイトのトップページに注意喚起のバナーを表示、送信者の詐称が行われやすいフリーメールアドレスから受信したメールの上部に注意喚起文をシステム上で自動表示等)。

また、内閣官房が主催した「標的型メール攻撃訓練」に参加し、財務省本省の中で無作為抽出された職員に対して疑似の標的型メールを送付する訓練を実施しました。

さらに、地方支分部局への立ち入り監査の際、あわせて、最高情報セキュリティアドバイザーを講師として､標的型メール攻撃への対応を含む総合的な情報セキュリティ対策に関する講習会を実施しました。

(4) なりすましメールの防止に関する取組

平成 23 年度、財務省では、すべてのインターネット上のドメイン（xxx.go.jp）について、SPF（Sender Policy Frameworks）による送信ドメイン認証技術を導入しました。このことにより、財務省から送付するメールについては、送信者情報のドメインを詐称していないこと（なりすましメールではないこと）を示すことができます。受信者側において送信元を検証する機能を設定した場合、財務省のドメインを詐称するメール（なりすましメール）を遮断することが可能となります。

また､なりすましメールを防止するため､利用していないドメインを廃止するとともに、メール送信を行わないドメインについてメール送信を行わない旨 SPF の設定を行うなど

の取組を行いました。

(5) 情報セキュリティ規程の見直し

① 政府機関統一基準群の改定に合わせた見直し

平成 23 年 4 月、「政府機関の情報セキュリティ対策のための統一基準」(平成 22 年 5 月 11 日 情報セキュリティ政策会議決定) が「政府統一管理基準」及び「政府統一技術基準」に分割されました。また、その内容についても、政府機関におけるクラウド技術の利用並びにウェブの改ざん・標的型メール攻撃など外部からの不正アクセスによる脅威への対応等の観点から見直しが行われました。

財務省においては、以上の政府機関統一基準群の改定に合わせて、「財務省対策基準」やそれに準拠して制定されている「財務省実施規則」の改定を行いました。

② 情報の移送・提供に関する実施規則の整備等

機密性情報の移送・提供 (用語については下記参照) について、当該移送・提供のための許可申請・届出の手続をより具体化し、職員の日々の業務における適正な情報管理を徹底するため、「政府統一管理基準」を踏まえて「財務省対策基準」の改定や「情報の移送・提供に関する実施規則」の整備に取り組みました。

機密性:情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保すること。

移　送:財務省の庁舎の外に、情報を記録した電磁的記録媒体 (USB メモリ、CD-ROM 等) 若しくは書面を運搬すること。

提　供:財務省の組織外の者に、電磁的に記録された情報を送信すること (電子メールの送信)、情報を記録した電磁的記録媒体 (USB メモリ、CD-ROM 等) 若しくは書面を引き渡すことをいう。

(6) 情報セキュリティ教育の充実

平成 23 年度は、情報セキュリティ教育の充実について重点的に取り組みました。

① 一般職員に対する研修

イ. 情報セキュリティ研修

財務省では、「財務省対策基準」に基づき、すべての職員 (非常勤職員やアルバイトを含む行政事務従事者)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、集合形式の研修を実施しています。

平成 23 年度、財務省本省では、すべての職員を対象とした講習を実施し、最高情報セキュリティアドバイザー及び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などについて説明を行いました。研修の実施回数については、９月に 10 回、２月に８回の計 18 回開催することにより、職員が業務の状況に合わせて研修を受講できるよう配慮しました。また、行政事務従事者を管理する立場にある課室情報セキュリティ責任者向けの情報セキュリティ研修を新設しました (10 月に計２回実施)。

また、平成 23 年度は、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るようにしました。集合研修を未受講の職員に対しては、e ラーニングによる自習を個別に求めています。

ロ．職員の意識向上に向けた取組

財務省では、情報セキュリティ対策の基本的事項として、以下の「情報管理７か条」をポスター等で職員に周知し、職員の意識向上に取り組んでいます。

（参考）情報管理７か条

第１条　情報の無許可持ち出し絶対禁止
第２条　私物の USB メモリ等は絶対使用しない
第３条　知らない人からのメール、怪しいファイルは開かない
第４条　ウイルスが検知されたら報告する
第５条　メール送信は再確認で誤送信防止
第６条　フォルダへの適切なアクセス制限を設定
第７条　パスワードは人に見せない教えない

② 情報システム関係部局の職員に対する研修

イ．財務省全体管理組織（PMO：Program Management Office）に対する教育

財務省全体管理組織（PMO）である業務企画室の職員に対しては、最高情報セキュリティアドバイザーが、情報セキュリティの専門家の立場から、日々の業務の中で助言を行っています。

ロ．情報システムの個別管理組織（PJMO：Project Management Office）に対する教育

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）の職員に対しては、業務・システムの最適化に係るプロジェクト・マネジメントのほか、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。平成 23 年度は、９月と 10 月の計２回開催しました。

また、個別管理組織（PJMO）においては、総務省行政管理局が実施している情報システム統一研修等に積極的に参加しています。

(7) 障害・事故等への対応

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又は課室情報セキュリティ責任者に速やかに連絡するとともに、所定の様式により障害・事故等の状況を報告することとされております。また、情報セキュリティに関する緊急連絡網を整備しており、障害・事故等が発生した部局は、業務企画室に速やかに情報提供し、業務企画室では、事態を踏まえ必要に応じて、省内幹部や内閣官房情報セキュリティセンター（NISC）等に連絡することとされております。

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又は課室情報セキュリティ責任者がマニュアル等に基づき指示を行うこととされています。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が情報セキュリティ責任者及び業務企画室に提出されます。

今後とも、障害・事故等に適切かつ迅速に対応できるよう、関連する規程の見直しや緊急連絡網のアップデートを定期的に行う予定です。

(8) 外部委託先の管理

財務省では、「外部委託における情報セキュリティ対策に関する実施規則」に基づき、「財務省対策基準」に規定する情報セキュリティの水準を外部委託先に求めることとしています。また、同規則は、外部委託を実施する情報システムセキュリティ責任者や課室情報セキュリティ責任者は、委託先の選定にあたり最高情報セキュリティアドバイザーの意見を聴くこと、委託先による情報セキュリティ対策の履行状況について定期的に確認することなどを定めています。

5．平成 24 年度の情報セキュリティ対策の予定

(1) 情報セキュリティ研修、自己点検、監査の見直し（前倒し実施等）

情報セキュリティ研修の集合研修については、従来の９月・10 月から７月・８月へ、自己点検については、従来の 11 月から 10 月へ、それぞれ実施時期の前倒しを図ります。また、情報セキュリティ監査については、関係規程に関する準拠性監査などから早期に着手し、自己点検に関する監査は従来の２月実施から 11 月･12 月実施へ前倒しを図ります。このように前倒し実施することにより、年内に研修、自己点検及び監査を一通り終了させ、年明け以降それらを踏まえたセキュリティ対策を講じることが可能となります。

また、情報セキュリティ研修については、対象者のカテゴリーをさらに細分化し、それぞれのカテゴリーを踏まえて研修内容の見直しを行います。監査については、自己点検結果等の内部監査における監査証跡の提出の厳密化、情報システム監査の対象の拡大といった施策により、実効性の改善を目指します。

(2) 標的型メール攻撃への更なる対応

平成 24 年度も、財務省として内閣官房が主催する「標的型メール攻撃訓練」に参加することとしています。その際、財務省本省の職員のみならず、国税庁や財務局、税関における外部とのメールのやり取りが可能な職員もすべて訓練の対象とすることにより、標的型メール攻撃への更なる対応を進める予定です。

(3) 次期財務省行政情報化 LAN システムの導入に合わせた技術的な対策強化

標的型メール攻撃によるウイルス感染や USB メモリの紛失等による機密情報･個人情報の流出といった、他の政府機関における情報セキュリティ事案の頻発を踏まえ、次期財務省行政情報化 LAN システムの導入（平成 25 年１月１日運用開始予定）に合わせて、LAN の通信状況の管理や情報漏えい防止の強化を進めるなど、技術面から情報セキュリティ対策の強化を行うこととしています。

(4) 情報セキュリティ規程の見直し

今般、政府機関等を対象とした標的型メール攻撃等への対応、情報技術や利用環境の変化を踏まえた対応、調達時におけるセキュリティ要件の確保やリスク分析の確実な実施等の観点から、「政府統一管理基準」及び「政府統一技術基準」等の見直しが行われました。財務省においても、これを踏まえ、「財務省対策基準」「財務省実施規則」を改定します。

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～

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、電子書籍等の新たな情報技術が普及し始めています。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新た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組は一瞬たりとも手を抜くことが許されません。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セキュリティの確保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います。情報技術の導入にあたっては、情報システムの効率的な運用、セキュリティの確保、業務効率の向上といった多面的かつ柔軟な取組が求められており、費用と効果のバランスを図りつつ、注意深く業務システム及び情報処理システムの改善を進めていくことを重要視しています。

財務省のセキュリティ対策に関しては、現状において特段のシステム障害・事故等が発生していないことから、情報システムや執務 PC 環境に関する技術面のセキュリティ対策については十分に行われていると言えます。しかしながら、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必要があるなど、以下のような改善の余地があります。

一つは、いわゆるソーシャル・エンジニアリング対策の推進です。職場によっては紙資料等が山積しており、情報漏えいの危険があります。また、外部委託先からの情報漏えいの可能性も否定できません。更に、標的型メール訓練の結果が示すように、職員の自己防衛スキル向上は急務です。このような事態を改善するため、ペーパーレス化の推進を含む執務環境の改善対策や外部サービス活用時における対策実施の有効性確保といった人的な対策の高度化・深堀りや物理面の環境改善にも力点を置いた、総合的なセキュリティ対策に取り組んでいく必要があります。

もう一つは、自己点検や監査等の対策の更なる推進です。セキュリティ事故は小さな穴から発生することも多く、自己点検で統一基準の 100%実施に近い高水準を達成しているとはいえ、行政事務従事者一人ひとりの意識を更に高め、対策実施の有効性を向上させる必要があります。

私は、CIO（情報化統括責任者）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本格的な情報セキュリティ内部統制への取組について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