情報セキュリティ報告書

平成 24 年5月　内閣府

目　　次

はじめに

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、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、その背景には情報通信の多様化と利用者の増大があります。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、サイバーテロ攻撃、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が挙げられます。こうした脅威は、各府省庁等、我が国政府機関が外国からのサイバーテロにおいて真っ先に標的にされていることを考慮すると、民間企業にも増して対策を強化すべきとも言えます。このため Web サイトなどのシステム面においても情報セキュリティ対策を強化していく必要があります。

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）の更新の際に、検疫認証システムや電子メールの暗号化機能を導入するなどのシステム強化を行っているところです。

平成23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たものです。

現段階では、大きな課題等はありませんが、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

1　平成23年度の総括

(1)　平成23年度の評価

- 情報セキュリティ対策の実施状況の自己点検結果

内閣府職員の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。）を行った結果は、適切に実施していることが判明しました。

- 情報システムごとの状況

内閣府の各情報システムの端末、公開用ウェブサーバ、メールサーバ、DNSサーバについて調査したところ（5. (2)情報システムごとの対策）、端末、公開用ウェブサーバ、メールサーバ、DNSサーバは、いずれも100％の情報セキュリティ対策が実施されていることを確認いたしました。

- 教育・啓発

内閣府では、ほとんどの職員がe-ラーニングにより情報セキュリティ教育の学習ができるため、ほぼすべての職員がe-ラーニングを受講しました（注）。

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ました。

（注）　一部のe-ラーニングシステムを利用できない職員向けには、情報セキュリティ掲示板上にe-ラーニングと同じ内容の資料を掲載し、情報セキュリティ教育を実施。

- 調達・外部委託

内閣府では、情報処理業務または情報システムの構築・改修を外部に委託する際には、委託先においてもポリシー、技術基準及び関連規程・実施手順記載の内容と同等のセキュリティ対策を実施する必要があるため、「外部委託における情報セキュリティ対策実施規程」の遵守を調達仕様書に反映させること等により、外部委託による業務の遂行に必要な情報セキュリティ水準の確保を図っています。

- その他取り組んだ事項

内閣府では、最近官民を問わず、標的型メール攻撃（サイバー攻撃の一種）による被害が増大していることを重視し、全職員を対象に心当たりの無いメールを受け取った場合に、添付ファイルを開くことや、メールに含まれるリンク先にアクセスしないようにするための訓練を実施しました。

- 情報セキュリティに関する障害・事故等の報告

内閣府におきましては、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。

(2)　翌年度の目標

・　内閣府では、「内閣府本府情報セキュリティポリシー及び内閣府本府情報セキュリティポリシー技術基準」（以下、ポリシー・技術基準という。）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ます。

特に、情報の提供に際しては、内閣府職員（情報提供者）から受け取った人がどのように扱うべき資料かが分かるように、職員間でやり取りするための基準である情報の格付に代えて

「部外秘」などの分かり易い表記に変更することも含めて一層の周知徹底に努めます。

・　内閣府では、新たな通信手段を利用した国民からの広聴手段の利用、及び動画中継などの新たな情報提供に伴い、例外措置申請の確実な実施やその管理を適切に行い、情報セキュリティに関する障害・事故等の防止に努めます。

2 報告の基本情報

(1) 内閣府の概要

内閣府は、①内閣の重要政策に関する内閣の事務を助けること、及び②内閣総理大臣が担当するにふさわしい行政事務、を担っています。

① 恒常的かつ専門的な対応が必要な特定の内閣の重要政策に関する企画立案・総合調整という役割で、具体的には、経済財政政策、科学技術政策、防災、男女共同参画、沖縄政策、北方対策、青少年育成、金融、食品安全、消費者、食育、少子化対策、高齢社会対策、障害者施策、交通安全対策、犯罪被害者等施策、自殺対策などを所掌しています。

② 具体的には、ア）経済分析、沖縄振興など上記①の企画立案・総合調整に関連する行政事務、イ）栄典、NPO、政府広報、PKOなどを所掌しています。

内閣府の情報システムは、職員が行政端末を利用して業務遂行するための基幹システムである内閣府LANが中心ですが、上記の業務遂行のために、多くの独自システムを構築・運用しています。主なシステムは以下のとおりです。

① 政府研究開発データベース、総合防災情報システム、男女共同参画情報システム、食品安全総合情報システムなど

② 景気ウォッチャー調査、栄典事務効率化システム、NPO情報管理・公開システム、政府広報オンライン、国際平和協力業務に係る情報収集システムなど

(2) 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日までです。

(3) 対象とする組織

本報告書が対象とする組織は、内閣府本府の内部部局、地方支所分部局（沖縄総合事務局）、重要政策に関する会議、施設等機関、特別の機関、審議会等です。

なお、宮内庁、公正取引委員会、国家公安委員会、金融庁、消費者庁等の内閣府の外局は、各組織で情報セキュリティ対策を実施しているため、本報告の対象には含まれません。

(4) 対象とする情報

本報告書が対象とする情報は、ポリシーで対象としてい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及び情報システムに関係がある書面に記載された情報です。

(5) 本報告書の責任部署

内閣府大臣官房企画調整課情報システム室

(6) 定員数

本報告書の対象となる内閣府の定員数は、2,360人（平成23年12月末）。

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

内閣府では、「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」（以下、「統一管理基準」という。）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」（以下、「統一技術基準」という。）の策定に基づき、内閣府の対策基準であるポリシー・技術基準及び関係規程を平成23年6月に改訂及び策定を行いました。（注）

ポリシーでは、「総則」、「組織と体制の整備」、「情報についての対策」、「情報処理についての対策」、「情報システムについての基本的な対策」と分類しています。

技術基準では「総則」、「情報セキュリティ要件の明確化に基づく対策」、「情報システムの構成要素についての対策」、「個別事項についての対策」と分類しています。

関係規程は、ポリシー・技術基準の規定に基づく具体的な情報の対象と取扱方法をはじめ、障害・事故等の対応手順などの遵守事項を、日々の業務においてどのように運用していくかを明確にするために整備されるもので、以下の規程及び手順書を内閣府本府情報セキュリティ委員会または統括情報セキュリティ責任者が制定しています。

- 情報の格付及び取扱制限に関する規程
- 障害・事故等対応手順書
- 内閣府本府外での情報処理の手順書
- 内閣府本府支給以外の情報システムによる情報処理の手順書
- 内閣府本府外の情報セキュリティ水準の低下を招く行為の防止に関する規程
- 例外措置手順書
- 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
- ドメインの使用に関する規程
- 暗号化及び電子署名規程
- 機器等の購入における情報セキュリティ対策実施規程
- 外部委託における情報セキュリティ対策実施規程
- 内閣府本府情報セキュリティ委員会の運営について

（注） 政府全体として情報セキュリティ対策の強化・拡充するために、内閣官房情報セキュリティセンターが作成した情報セキュリティ対策の基準が、政府機関統一管理基準及び政府機関統一技術基準です。

各府省庁では、この基準を基本に独自の基準を作成しています。内閣府では、ポリシー・技術基準がこれに相当します。

(2) 情報セキュリティ対策の推進体制

情報セキュリティ対策は、上記のポリシー・技術基準及び関係規程に基づき、主体毎の権限と責任を明確にし、必要となる推進体制を確立して組織全体として取り組んでいるところです。

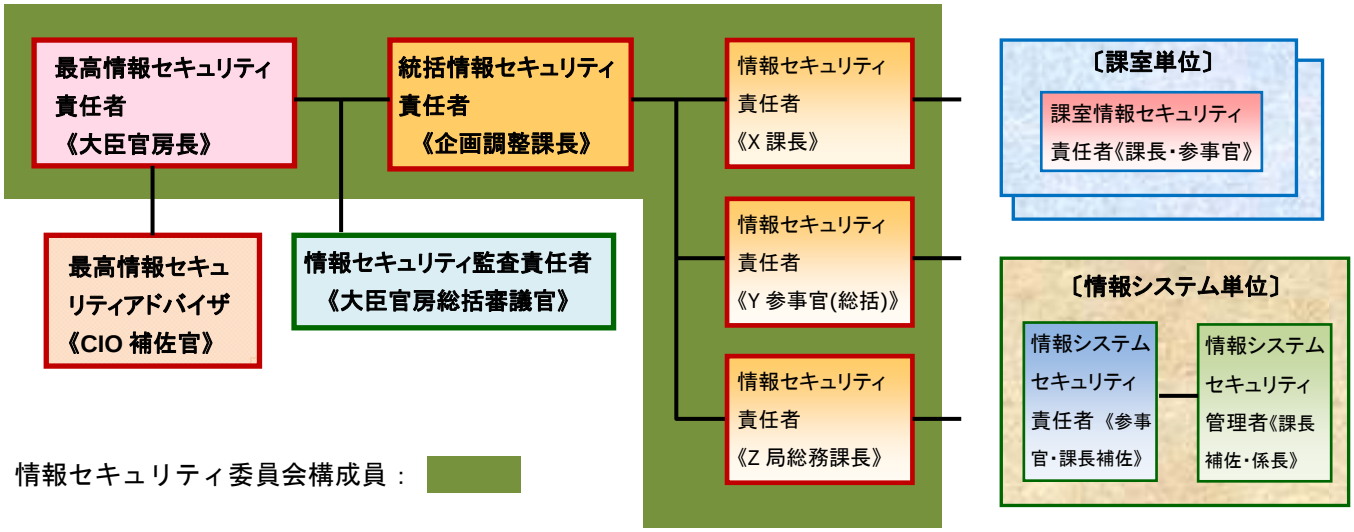
内閣府では、図1に示すとおり、最高情報セキュリティ責任者の下、各部局に情報セキュリティ責任者、各課室に課室情報セキュリティ責任者を置き、それぞれの責務に応じて、情報セキュリティ対策に取り組んでいます。

また、最高情報セキュリティアドバイザ（内閣府CIO補佐官）には、情報システムに関するアドバイスのみならず、本報告書の作成を含め、内閣府の情報セキュリティ対策の助言をいただいております。

さらに、上記2.(1)で紹介しました独自システムを運用している部局においては、情報システムセキュリティ責任者及び同管理者を任命し、それぞれの責務に応じて、情報セキュリティ対策に取り組んでいます。

また、情報セキュリティ教育及び自己点検など、全職員を対象とした情報セキュリティ対策は、情報システム室から各部局の情報セキュリティ担当者に依頼して実施しています。

図1　内閣府の情報セキュリティ体制



委　員　長　：　最高情報セキュリティ責任者
委員長代理　：　統括情報セキュリティ責任者
委　　員　：　情報セキュリティ責任者
（オブザーバー出席が可）
・最高情報セキュリティアドバイザ
・情報セキュリティ監査責任者

職　　務	情報セキュリティに係る責務
最高情報セキュリティ責任者	内閣府本府における情報セキュリティ対策に関する事務を総括する責任を負う。（体制の整備、年度自己点検計画の策定等）
情報セキュリティ監査責任者	内閣府本府における情報セキュリティ監査に関する事務を統括する責任を負う。（年度情報セキュリティ監査計画の策定、監査を実施する者に対する指示等）
統括情報セキュリティ責任者	情報セキュリティ責任者を統括する責任を負う。（連絡体制・関係規程の整備、職員に対する情報セキュリティ対策教育の実施等）
情報セキュリティ責任者	所管する単位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責任を負う。（体制整備、例外措置の許可、自己点検票・実施手順の整備、自己点検指示等）
課室情報セキュリティ責任者	課室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責任を負う。（所管する事務や職員における情報の取扱い等に関して判断。特に情報システムの持出し、私物パソコンの業務利用等に関する許可・届出等）
情報システムセキュリティ責任者	所管する単位における情報システムごとの情報セキュリティ対策の管理に関する事務を統括する責任を負う。（情報システムの持出し、私物パソコンの業務利用等に関する許可・届出、セキュリティ機能の設計等、利用手順書等の整備、安全区域の管理等）
情報システムセキュリティ管理者	所管する単位における情報システムごとの情報セキュリティ対策の実施について責任を負う。（定められた手順や判断された事項に従い、対策を実施）

(3) 監査等

内閣府では、政府機関統一管理基準及び同技術に準拠して策定されたポリシー・技術基準及び関係規程・実施手順に基づき、各情報システムが適切に運用され、実効性が確保されているか、その準拠性と妥当性の有無を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、脆弱性の有無の点検を中心に情報システムに対する情報セキュリティ監査も実施しています。

そして、準拠性監査及び情報システムに対する情報セキュリティ監査は、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。

- 準拠性監査

平成23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23年11月～平成24年3月にかけて監査を実施しました。

【監査結果及び改善提案】

平成23年度に実施した「準拠性監査報告書」（平成24年3月2日）においては、

① 本府支給以外の情報システムにより情報処理を行う必要がある場合の手続について、これまでの課室情報セキュリティ責任者だけでなく、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に改め、情報システムセキュリティ責任者の許可を加えること、

② 情報システムセキュリティ責任者が暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいては、「暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能としなければならない。」との規定の書き出しにおいて、電子署名の付与だけでなく検証においても本規定が適用されるように改めることが必要、との改善提案がありました。

【監査報告書に基づく対応の実施】

平成23年度に実施した「準拠性監査報告書」において、平成22年度「準拠性監査報告書」で改善提案のあった下記の1件は、実施されているとの監査結果でした。

「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」の4.2 情報セキュリティ監査責任者が行う措置の対象者について、以下のとおり修正した。

『情報セキュリティ監査責任者の転出に伴う・・・措置』

→『情報セキュリティ監査実施者の転出に伴う・・・措置』

- 自己点検の監査

平成23年4月に策定した「平成23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、課室情報セキュリティ責任者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名及び職員45名を対象に平成23年12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。

【監査結果及び改善提案】

監査対象職員の自己点検結果は実施率、到達率ともに 100％であったところ、自己点検どおりに実施していることを確認しました。

このため、改善提案を行なう必要はありませんでした。

- 情報システムに対する情報セキュリティ監査

平成23年8月に『食品安全総合情報システム』の情報セキュリティ監査として、サーバ及びWebアプリケーションに対するセキュリティ診断を行い、システム上の脆弱性の点検を実施しました。

【監査結果及び改善提案】

監査結果では、特に問題となる脆弱性はありませんでした。

4　当該年度の重点事項

(1)　重点事項の目標、実績及び評価

平成22年度の情報セキュリティ報告書では、①ポリシー及び技術基準の改訂・作成に伴い、解説資料等に関してポイントを絞った内容に改めるなど、職員が利用し易い内容に改善すること、②情報システムごとの対策において、DNSサーバの対策を万全（100％）にすること、を目標としていました。

①については、平成23年6月に改訂・作成を行うとともに、同時に改訂した情報セキュリティ掲示板の解説資料及びe-ラーニング教材の内容を大幅に簡素化するとともに、外部への情報提供を行う場合などの対策など、特に気を付けるべき内容については詳しく解説するように改めました。

②については、平成23年度の点検結果において100％を達成しました。

(2)　障害・事故等の再発防止状況

沖縄総合事務局LANにおいて、ネットワークアクセスの監視等を強化するとともに、IDSの進化版（検疫ネットワーク、新種ウィルスを含む不審な挙動をキャッチする機能）を有したシステムを導入するなどの情報セキュリティ対策の強化を図り、平成23年度においては、不正プログラムによる被害等は、発生していません。

5 情報セキュリティ対策の実施状況

(1) 府省庁対策基準に関する自己点検結果

(ア) 課題と対策(平成22年度の自己点検結果より)

平成 22年度自己点検結果は、把握率、到達率ともに100%でした。

(イ) 自己点検結果の状況

平成23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(表1参照)。

表1 自己点検の把握率

対象年度	把握率
平成 22 年度	100 %
平成 23 年度	100 %

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(表2参照)。

表2 主体別対策実施率

対象年度	責任者	システム担当	職員
平成 22 年度	100%	100%	100%
平成 23 年度	100%	100%	100%

把握した職員のうち、対策を実施した遵守事項の割合(注)を以下の3区分(100%、95%、90%)でみると、どの主体でも前年度に続き、100%(完全実施)となりました(表3参照)。

表3 主体別到達率

【到達率100】

対象年度	責任者	システム担当	職員
平成 22 年度	100%	100%	100%
平成 23 年度	100%	100%	100%

【到達率 95】

対象年度	責任者	システム担当	職員
平成 22 年度	100%	100%	100%
平成 23 年度	100%	100%	100%

(注) 到達率とは、主体別対策実施率で実施の対象職員の集計結果において、その回答のうちの「実施不足」または「一部未実施」以外の回答をした割合(主に、「実施」または「該当なし」)の割合)。

【到達率 90】

対象年度	責任者	システム担当	職員
平成 22 年度	100%	100%	100%
平成 23 年度	100%	100%	100%

(ｳ) 総評

平成23年度は、前年度に続き、職員の遵守割合、到達率ともに100％（完全実施）となりました。

今後とも、「平成23年度の総括 (2) 翌年度の目標」で掲げているように、引き続き、情報セキュリティ教育、新人研修等により周知徹底に努めます。

(2) 情報システムごとの対策

(ｱ) 課題と対策

平成23年度における対策状況は、下記のとおり対策事項の実施率は100％となりました。

(ｲ) 情報システムの対策状況

平成23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) 総評

内閣府では、個別システムも含め、すべての情報システムの情報セキュリティ対策が100％の実施率を維持できるように努めます。

(3) 教育・啓発

(ア) 教育

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。

なお、内閣府本府情報セキュリティ掲示板の掲載資料であるポリシー・技術基準及び関係規程及びこれらの解説書等に関する職員からの照会に対しては、情報システム室の担当から回答を行っています。

《対象者の役割に応じた教育教材の整備》

内閣府では、e-ラーニングのコースとしては、職員用（全職員が対象）の他、情報セキュリティ責任者向け及び課室情報セキュリティ責任者向けの3コースを用意しています。

このほか、内閣府本府情報セキュリティ掲示板におきましては、全ての職責について、以下の基本的な遵守事項の解説書を作成しています。

- 職員の責務
- 情報セキュリティ委員会の責務
- 最高情報セキュリティ責任者の責務
- 情報セキュリティ監査責任者の責務
- 統括情報セキュリティ責任者の責務
- 情報セキュリティ責任者の責務
- 課室情報セキュリティ責任者の責務
- 情報システムセキュリティ責任者の責務
- 情報システムセキュリティ管理者の責務

《教育受講状況の管理》

e-ラーニングについては、受講の有無を定期的に確認し、実施時期の通知後の一定期間（1か月以上）e-ラーニングを未受講のままである職員に対しては、受講促進メールを送信することにより、受講促進を図っています。

(イ) 実施手順等の容易化や参照の容易化

内閣府の情報セキュリティのコーナーでは、ポリシー・技術基準及び関連規程類だけでなく、上記の《対象者の役割に応じた教育教材》として、職責別の資料（特に、遵守すべき事項、よくある手続などをPower Point形式の資料で要約したもの）、及びこのうちの「職員の責務」を詳しく解説した「職員が行う情報セキュリティ対策〔特に重要な事項〕」をポリシー・技術基準の要約・解説資料として容易に参照できるようにしています。

(ウ) ひやり事案を含む障害・事故等の事例の活用

政府だけでなく、民間企業も含めて、サイバーテロ攻撃（不審メールに添付された不正プログラムによる情報窃取など）、個人情報の流出事例など、障害・事故等の事例のうち内閣府でも起こる得る事例をe-ラーニング、個別部局への説明及び職員向け研修の機会を通じて、注意喚起を行っています。

(4) 調達・外部委託

情報処理業務または情報システムの構築・改修などを外部に委託する際には、委託先においてもポリシー・技術基準及び関連規程・実施手順記載の内容と同等のセキュリティ対策を実施する必要があります。

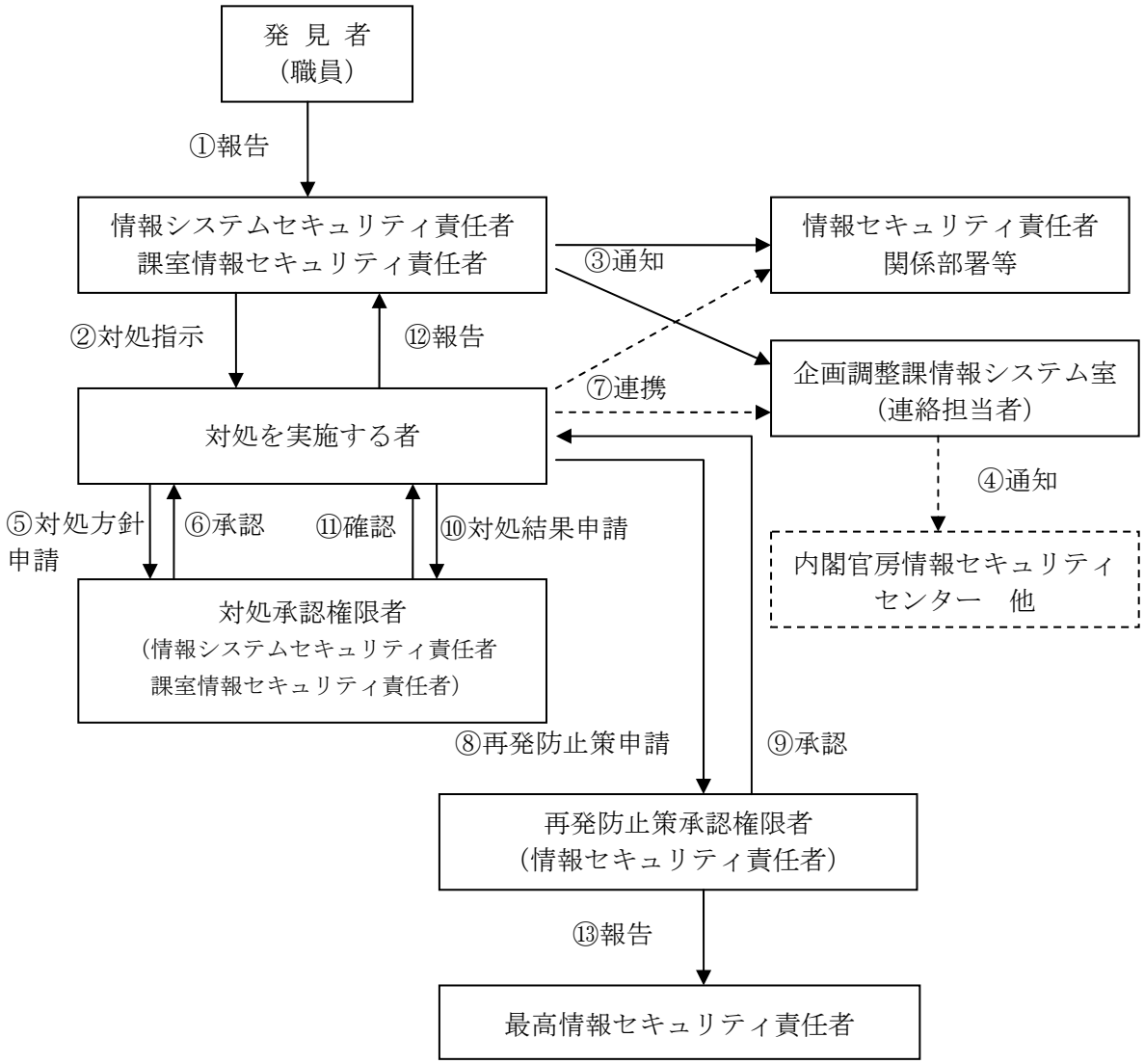
このため、内閣府では、外部委託を行う業務の範囲や外部委託の実施に係る検討手順、調達仕様書への記載要件として必要な事項を「外部委託における情報セキュリティ対策実施規程」において定め、調達担当者がこれを遵守することにより、外部委託による業務の遂行に必要な情報セキュリティ水準の確保を図っています。

6. 情報セキュリティに関する障害・事故等報告

(1) 情報セキュリティに関する障害・事故等の把握

「障害・事故等対応手順書」に基づき、下記の連絡の流れにより、最終的には、最高情報セキュリティ責任者に報告を行ないます。

【障害・事故等対応の処理フロー】



(2) 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23年度においては情報セキュリティに関する障害・事故等はありませんでした。

なお、内閣府は、内閣官房情報セキュリティセンターが、平成24年1月26日に実施したセキュリティ障害が発生したことを想定した「サイバーインシデント発生時における連絡体制の確認訓練」に参加し、緊急連絡体制の確認などの情報収集及び情報伝達に係る対処訓練を行ったところです。

7. 情報セキュリティ対策に関する次年度の計画

- 平成 24 年度は、内閣府の各情報システムの端末、公開用ウェブサーバ及び電子メールサーバのセキュリティについて、ポリシー・技術基準に基づき点検するための情報システムごとの対策(23 年度の結果は、5 (2))、情報セキュリティ対策に関する自己点検及び自己点検に関する監査を実施します(図2)。
- また、平成 23 年度に続き 24 年度においても、内閣府の Web サイトなどのインターネットを利用しているシステムの中から脆弱性の有無を診断するためのシステム監査を実施する予定です(図2)。

おわりに

情報伝達・収集手段の多様化に伴い、各府省庁においても新たな通信手段を利用した国民からの広聴手段の利用、及び動画中継などの新たな情報提供を行うようになってきている。

内閣府においても政府インターネットテレビや事業仕分けなどにおいて動画中継による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を利用して国民からの意見聴取する手段を広げることにも努めている。

このような新たな通信手段を用いた国民との情報交換の頻度が高まるとともに、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も増大していくことを想定しなければならない。具体的には、内閣府の職員以外との通信を行う場合のセキュリティ対策のため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の強化を続けていく必要がある。

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についても検討を行う必要がある。具体的には、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ところである。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が、これらの対策を完了していないシステムにおいては、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。一般的には、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が、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。

平成23年度の職員の自己点検結果をみると、情報セキュリティ対策の遵守率である到達率が昨年度に引き続き100％となるなど、基本的な情報セキュリティ対策の遵守については職員に浸透しつつあるものと評価できるが、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ものと考えている。

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を作成するための情報セキュリティ教材の原案を提示している。

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
（内閣府CIO補佐官）
野村　邦彦

図2　平成24年度の監査業務の全体像