情報セキュリティ報告書

平成24年5月

人事院

はじめに ～最高情報セキュリティ責任者のメッセージ～

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益々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「標的型メール」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23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。今後も環境の変化や情報通信技術の動向を踏まえ、新たな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24年5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

1 平成23年度の総括

(1) 重点施策

人事院では、平成23年度の情報セキュリティ対策として、特に以下の事項について重点的に取り組みました。

- 職員に対する情報セキュリティ教育及び自己点検の充実
- 情報漏えい事故防止のための情報技術の活用
- 標的型メール攻撃への訓練

(2) 平成23年度の状況及び施策

① 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、新規採用職員には集合研修として情報セキュリティ教育を行いました。また各職員がいつでも情報セキュリティを学習できるように、教材を用いた学習環境をイントラネット上に整備しました。

② 自己点検の実施結果

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。

③ 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、引き続き努めていきます。

④ 調達・外部委託

Webサーバ（ホスティングサーバを利用している）委託業者において、DDos攻撃に備えて当院のWebサーバの稼働状況を24時間365日、自動監視を行い、もし異常を検知した場合には不審な通信を遮断させるとともに、速やかにその状況を当院に連絡させることとしました。

⑤ その他取り組んだ事項

情報の作成時における格付と取扱制限の明示を徹底するため、LAN端末の電子メールソフト、文書作成ソフト等に、情報の格付及び取扱制限の表示フォームを自動付与する機能を導入しました。

職員が標的型攻撃メールの特徴を理解し、対処方法を修得するため、全職員を対象として標的型攻撃メール訓練を行いました。

⑥ 情報セキュリティに関する障害･事故等の報告

平成23年度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。

(3) 平成24年度の目標

人事院では、重点的に取り組む目標を以下のとおり設定し、情報セキュリティレベルの更なる向上を目指します。

- 全職員の情報セキュリティ意識向上のために、教育･自己点検を充実します。
- 情報セキュリティ外部監査を実施し、情報セキュリティ対策の状況を客観的に評価し、改善課題を明確にします。

2 報告の基本情報（人事院における情報セキュリティ対策の枠組）

(1) 人事院の概要

人事院は、国家公務員法に基づき設置された中央人事行政機関であり、公務員人事管理の公正性を確保すること、労働基本権制約に対する代償として職員の利益の保護を図ること及び人事行政の専門機関として、社会一般の情勢に的確に対応した施策を推進し、国民から信頼される効率的な行政運営を確保することを主な使命としており、このため内閣の所轄の下において強い独立性と中立性を与えられています。

(2) 人事院情報セキュリティ報告書の対象とする期間

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) 人事院における情報セキュリティ対策の対象とする組織

本報告書が対象とする組織は、人事院本院、公務員研修所、各地方事務局（所）及び国家公務員倫理審査会です。

(4) 人事院における情報セキュリティ対策の対象とする情報

本報告書が対象とする情報は、情報システムの内部に記録された情報、情報システムの外部の電磁的記録媒体に記録された情報及び書面に記載された情報です。

書面に記載された情報とは、情報システムに入力した情報を記載した書面、情報システムから出力した情報を記載した書面及び情報システムに関する設計書等です。

これらは、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「統一基準群」という。）で定義されています。

(5) 人事院情報セキュリティ報告書作成責任部署

人事院事務総局総務課広報情報室

3 人事院における情報セキュリティ対策の枠組

(1) 情報セキュリティ対策に関する文書の体系

人事院では、統一基準群の改定に基づき、情報セキュリティ対策を実施するための「人事院情報セキュリティポリシー（管理基準編）」及び「人事院情報セキュリティポリシー（技術基準編）」（以下「人事院情報セキュリティポリシー」という。）を改定しました。

そして、人事院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していくため、以下のような各規程等を整備しています。

これらは、職員がいつでも閲覧できるようにイントラネットに掲載しています。

- 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
- セキュリティ教育実施手順書
- 障害・事故等の報告・対処手順書
- 外部委託における情報セキュリティ対策実施規程
- 人事院外での情報処理の手順書（モバイルＰＣ編）
- 院内ＬＡＮ運用手順書
- 機器等の購入における情報セキュリティ対策実施規程
- 人事院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手順書
- 人事院内におけるＰＣ利用手順書（ＰＣ利用者編）
- 人事院支給以外の情報システムによる情報処理の手順書（ＰＣ編）

(2) 人事院における情報セキュリティ対策の推進体制

人事院では情報セキュリティ対策を推進するために、統一基準群及び人事院情報セキュリティポリシーに基づき、以下に示す体制を整備しています（図1）。

① 最高情報セキュリティ責任者

情報セキュリティ対策に関する事務を統括します。人事院では最高情報セキュリティ責任者は

総括審議官が務めています。

② 情報セキュリティ委員会

人事院情報セキュリティポリシーの策定等を行う機能を持つ組織として、最高情報セキュリティ責任者を委員長とする情報セキュリティ委員会を設置しています。

③ 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。人事院では、平成23年度における情報セキュリティ監査責任者は、事務総局審議官が務めています。

④ 統括情報セキュリティ責任者及び情報セキュリティ責任者

情報セキュリティ責任者は、所管する部門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。

統括情報セキュリティ責任者は、情報セキュリティ責任者を統括する者として事務総局総務課長が務めています。

⑤ 情報システムセキュリティ責任者

情報セキュリティ責任者により指名され、所管する情報システムの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（セキュリティ機能の設計、利用手順書等の整備、安全区域の管理等）。

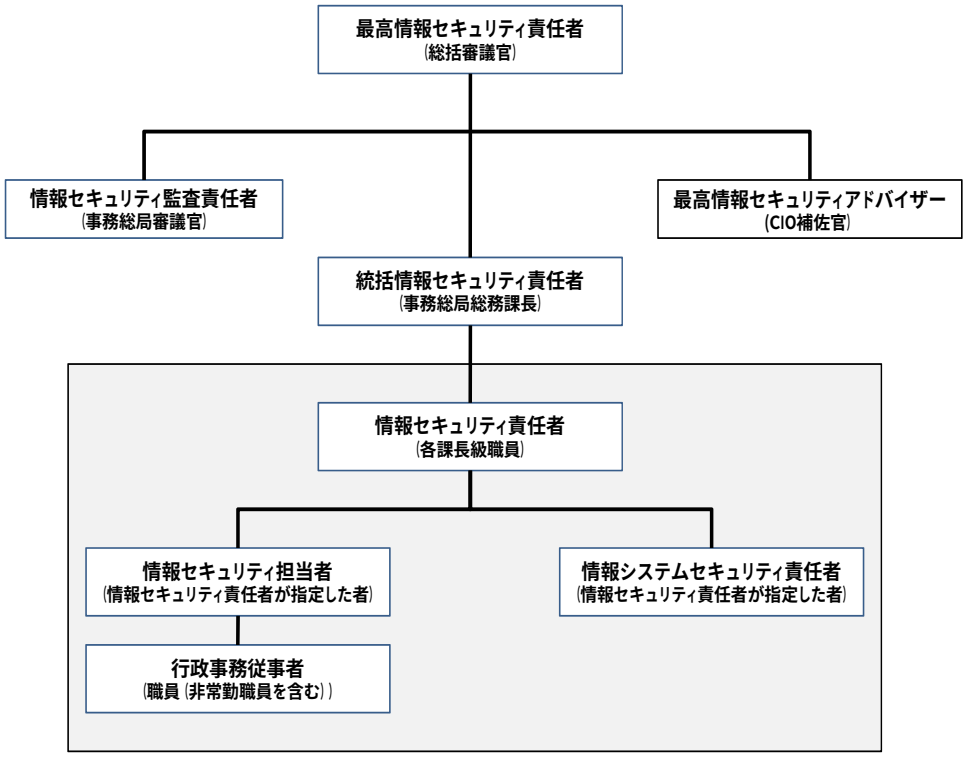
⑥ 情報セキュリティ担当者

情報セキュリティ責任者により指名され、情報セキュリティに関する事務を補助します。

⑦ 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を置き、情報セキュリティ対策に関する様々な事務への支援・助言等を行います。人事院ではCIO補佐官が務めています。

図1　人事院における情報セキュリティ体制



(3) 情報セキュリティ監査等

①　情報セキュリティ監査の概要

情報セキュリティの水準を向上し、維持するためには、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評価するため、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

②　情報セキュリティ監査の内容

人事院では、以下の情報セキュリティ監査を実施しました。

◆　人事院情報セキュリティポリシーの準拠性監査

人事院情報セキュリティポリシーが、統一基準群に準拠していることを確認します。

◆　各実施規程等の準拠性監査

各実施規程等が、人事院情報セキュリティポリシーに準拠していることを確認します。

◆　自己点検の適正性に関する監査

情報セキュリティの自己点検が適正に実施されていることを確認します。

◆　情報システムに関する監査

人事院の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を監査します。監査対象は、情報システムのライフサイクルを考慮して選定します。

③　情報セキュリティ監査の結果

監査の結果、全体として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。

◆　人事院情報セキュリティポリシーの統一基準群への準拠性に関する監査

統一基準群が要求する基本遵守事項を網羅していることを確認しました。

◆　各実施規程等の人事院情報セキュリティポリシーへの準拠性に関する監査

各実施規程等は、人事院情報セキュリティポリシー内容と整合が取れており、網羅されていることを確認しました。

◆　自己点検の適正性に関する監査

自己点検が適正に実施されていることを確認しました。

◆　情報システムに関する監査

監査対象の情報システムについて、人事院情報セキュリティポリシーに基づき適正に運用されていることを確認しました。

④　情報システムセキュリティ診断の実施

外部からの不正アクセスやウイルス等による攻撃に対する、インターネット接続環境及びＬＡＮシステムにおけるセキュリティレベルについてセキュリティ診断を実施した結果、不備は認められませんでした。

4　平成23年度の重点事項

(1)　重点事項の目標、実績及び評価

①　職員に対する情報セキュリティ教育及び自己点検の充実

人事院情報セキュリティポリシーの周知徹底を図るため、院内イントラネット上の教育環境を整備しました。また、自己点検については、自己点検の効果を高めるため、行政事務従事者向け

の点検項目を絞り込み、実施しました。

② 情報漏えい事故防止のための情報技術の活用

職員が行う「情報の格付と取扱制限の明示」を支援することを目的として、メール作成時の件名に「機○」、文書作成時に「機密性○情報」、「○○限り」のような書式が確実に付加されるように設定しました。

③ 標的型メール攻撃への訓練

職員が標的型メール攻撃に正しく対処できることを目的として、標的型メールを実体験する訓練を行いました。具体的には添付ファイルや本文にURLを記載した訓練用メールを職員に送信することによって、危険性の認識を深めることにつながりました。

(2) 障害・事故等の再発防止に向けた取り組み状況

平成22年度に発生した書類の盗難紛失事案を受けて、以下の再発防止策を講じています。

- 最高情報セキュリティ責任者から人事院全職員に対して、情報の厳格な管理についてあらためて周知徹底を図る。
- 各情報セキュリティ責任者に対して、所管する情報について取扱い等が徹底されるよう再指導を行う。
- 要機密情報について、人事院情報セキュリティポリシーに則った取扱いの徹底を図るとともに当該情報の管理方法の見直しを行う。

この結果、平成23年度においては、同様の障害・事故等は発生しておりません。

5 情報セキュリティ対策の実施状況

(1) 自己点検

① 自己点検の概要

政府機関として情報セキュリティ対策を推進するため、各府省庁が統一基準群に基づく情報セキュリティ対策の実施状況を自己点検し、NISCに報告することが定められています。

② 自己点検の対象

人事院では、全職員（出向者、非常勤職員を含む）を対象とし、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、行政事務従事者の3つの区分に分け、それぞれの主体が実施すべき情報セキュリティ対策項目について、自己点検を実施しました。

③ 自己点検結果の課題と対策

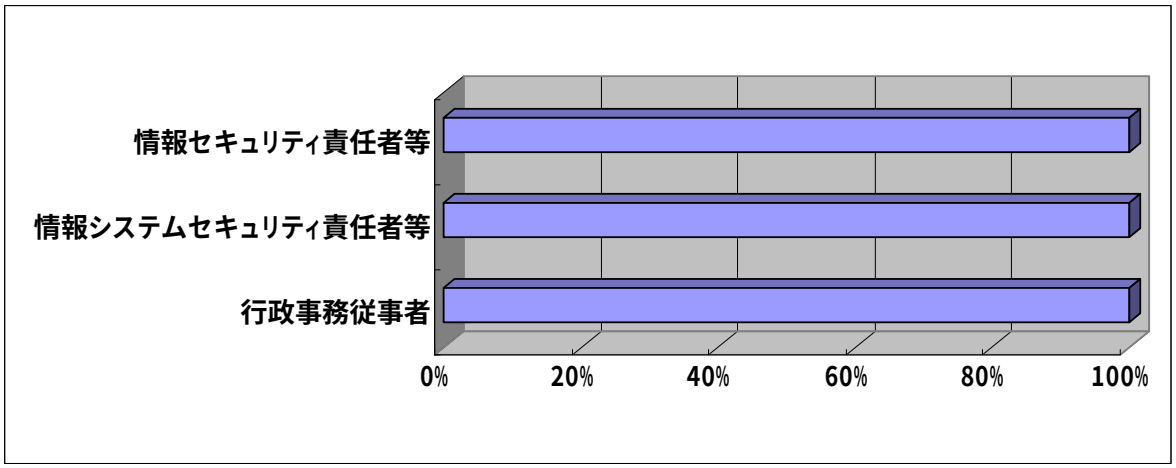
把握率、実施率は概ね適切でしたが、行政事務従事者における到達率については改善の余地が認められました。そのため、情報セキュリティ対策の浸透が更に図られるよう、情報セキュリティ責任者による指導等を徹底しました。

④　自己点検結果の状況

◆　人事院全体の把握率

自己点検を提出した者の割合である把握率は、人事院全体として前年度に引き続いて100.0%を達成しました（図2）。

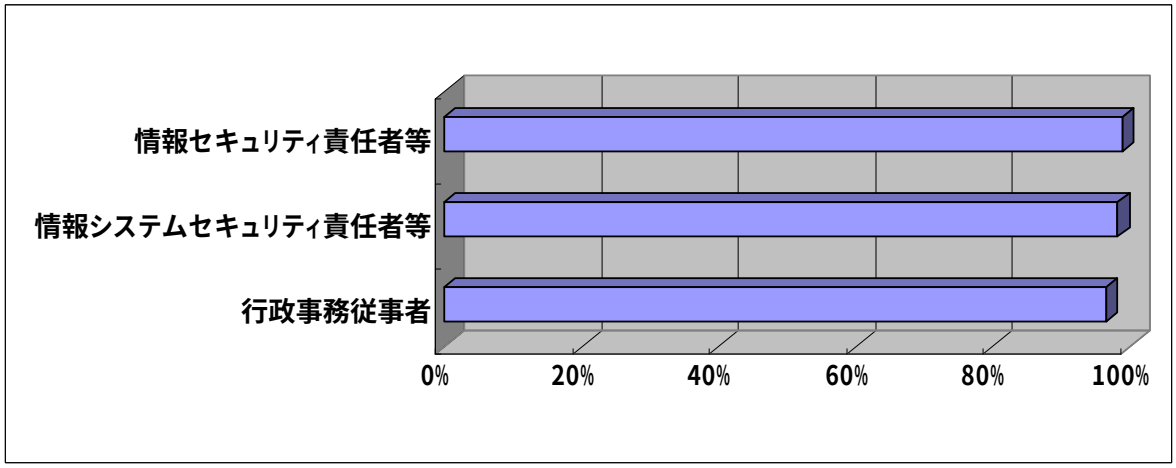
図2　主体別の把握率



◆　人事院全体の実施率

自己点検提出者のうち、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、情報セキュリティ責任者等（課長等）が99.0%、情報システムセキュリティ責任者が、98.3%、行政事務従事者については96.5%となっています（図3）。

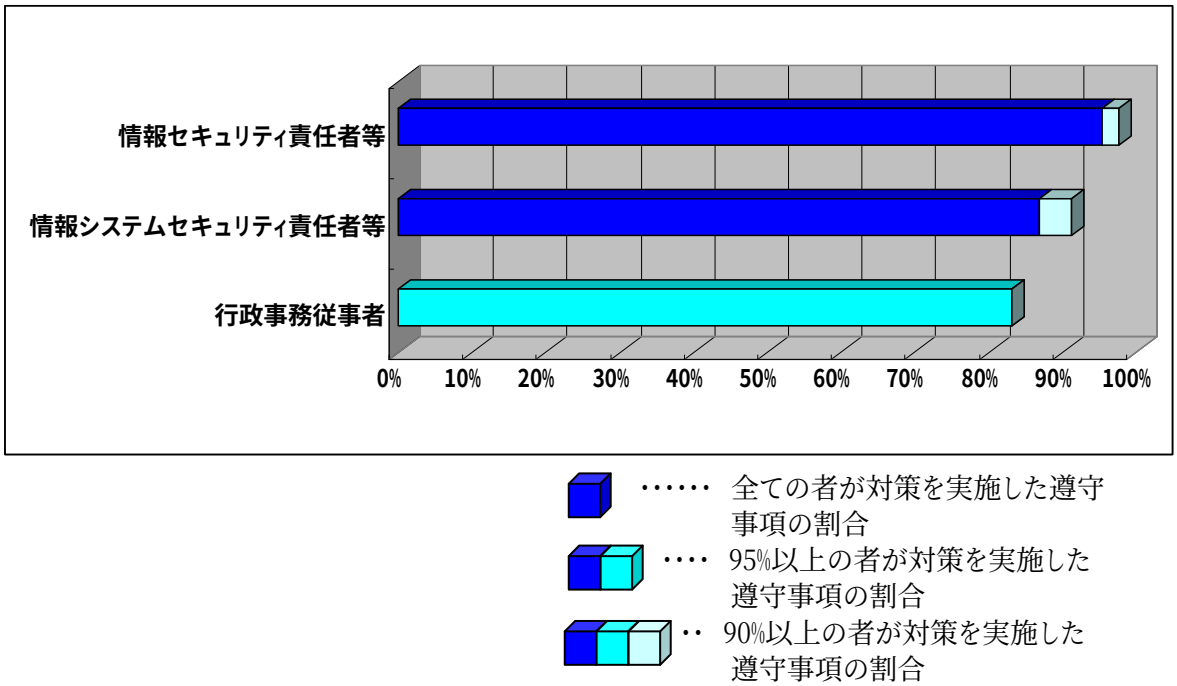
図3　主体別の実施率



◆　人事院全体の到達率

到達率（把握した者のうち、責務が生じた一定の割合（100%、95%以上、90%以上）の者が対策を実施した遵守事項の割合）は、図4のとおりです。

図4　主体別の到達率



⑤　総評

平成23年度の把握率は100%でしたが、実施率については改善の余地があります。

人事院情報セキュリティポリシーの遵守について、行政事務従事者に更なる周知徹底を行い指導するよう情報セキュリティ担当者に指示しました。

また、情報の格付の表示について一部未実施の者が見受けられたことから、改めて格付表示の徹底を指導しています。

(2)　情報システムごとの状況

人事院の公開用ウェブサーバ、電子メールサーバについて、統一基準群に規定された事項の遵守状況をＮＩＳＣが作成した調査票に基づき検査した結果、各調査項目における対策の実施率はいずれも100%でした。

(3)　情報セキュリティ教育・啓発

①　情報セキュリティ教育

人事院では、毎年度、人事院情報セキュリティポリシー、各実施規程等の内容についての理

解の促進、各種情報セキュリティ対策の着実な実施等を目的として、当該年度の研修計画に基づき、イントラネットを利用したe-ラーニング方式によりすべての職員に情報セキュリティ教育を受講する機会を保障しています。また、新規採用職員に対しては、公務における情報セキュリティ確保の重要性や具体的に取り組むべき対策について理解できるよう集合研修により情報セキュリティ教育を実施しています。

情報セキュリティ教育の教育内容については、統一基準群、人事院情報セキュリティポリシー等の改定に合わせて毎年更新しています。また、教育受講状況については、各情報セキュリティ責任者において確認し、報告することとしています。

② 職員に対する情報提供

職員に対してセキュリティ情報を効率的に提供するために、以下の取組を実施しています。

◆ 実施手順等の容易化や参照の容易化

情報セキュリティ関連規程類をイントラネットに掲載し、職員が容易に参照できるよう環境を整備しています。

◆ セキュリティ情報等の提供

NISC、GSOC（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）、運用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）について、イントラネットに掲載し広く周知し、知識向上を図っています。

(4) 調達・外部委託

人事院では、調達・外部委託において、統一基準群及び人事院情報セキュリティポリシーが適切に実施されるよう、外部委託における情報セキュリティ対策実施規程を整備しました。

具体的には、調達、契約、実施、納品・検収における各手続等について雛形を整備し、調達担当者が調達仕様書に情報セキュリティ対策に関して反映しています。

また、契約の締結に際しては、情報セキュリティ対策を契約条項に記載し、契約期間中における情報セキュリティ対策が確実に実施されるように取り組んでいます。

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

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・対処手順書に基づき、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。

(2)　公表した障害･事故等の概要、それに対する対応等

平成23年度においては、障害･事故等は発生していません。

7　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年度における情報セキュリティ対策の重点課題は以下のとおりです。

(1)　情報セキュリティ教育の拡充

平成23年度の自己点検で判明した課題（情報の格付と取扱制限等の付与）に対する改善の取り組みを継続します。具体的には、職員の理解促進に寄与するため、情報の格付と取扱制限の付与方法等を教材に組み入れます。

また、標的型メール攻撃等のサイバー攻撃に対する職員の注意を喚起するため、模擬訓練を継続して行います。

(2)　情報セキュリティ監査の拡充

情報セキュリティ外部監査を実施し、情報セキュリティの状況を客観的に評価します。

8 おわりに ～最高情報セキュリティアドバイザーのメッセージ～

情報セキュリティ対策とは、本来、業務（行政事務）の安定的遂行を支える基盤であり、業務の効率的な遂行に資するためのものです。業務と釣り合いを取ることによって、情報セキュリティ対策の効果が最大限に発揮されます。

平成23年度は、以下のような重点事項を定め、情報セキュリティ対策を推進してきました。

- ◆ 職員に対する情報セキュリティ教育

  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を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、模擬メールを用いた訓練を行い、職員の注意を喚起した。

- ◆ 情報処理対策に係る自己点検

  前年度の推奨取組事例を取り入れ、自己点検項目の絞込みを行った。

- ◆ 情報の格付に係る対策

  ＬＡＮ端末における電子メール及び文書作成ソフト等に、情報の「格付フォーム」を自動的に付与する機能を導入した。

平成24年度は「標的型メール」のようなサイバー攻撃が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、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-ラーニング教材の充実など、職員が情報セキュリティに関する知識を得る確実な機会を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（不正プログラムが内部に侵入することを想定した「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。

人事院最高情報セキュリティアドバイザー
無 川 紘 洋