平成 23 年度
情報セキュリティ報告書

平成 24 年 5 月

環境省

目次

はじめに

環境省は、廃棄物対策、公害規制、自然環境保全、野生動植物保護などを自ら一元的に実施するとともに、地球温暖化、オゾン層保護、リサイクル、化学物質、海洋汚染防止、森林・緑地・河川・湖沼の保全、環境影響評価、放射性物質の監視測定などの対策を他の府省と共同して行うなど、幅広い分野を所管しており、業務で取り扱う情報の管理や業務を支援する大小様々な情報システムを運用しています。

これらの業務で取り扱う情報資産や情報システムを適切に管理し、利用するためには、Plan（ 計画）→ Do（実行）→ Check（評価）→ Act（改善）という、いわゆる PDCA サイクルを取り入れた情報セキュリティ対策に取り組む必要があります。

環境省は、これまでも、以下の点を中心に情報セキュリティ対策に努めてきました。

(1) 情報の機密性の格付け等、取り扱いの徹底

(2) 情報システムによる技術的対策

(3) 情報セキュリティ対策の実施状況についての自己点検と監査

平成 23 年度においては、サイバー攻撃に対する対処体制の強化や情報の適正な取り扱いの徹底、メールの誤送信防止に対する注意の徹底について引き続き注意喚起することに加え、なりすましメールへの対処として送信ドメイン認証の対応強化や、適切なデータの取り扱いを推進するための手段として暗号化やパスワード機能を有するセキュアＵＳＢや安全に大容量のデータ送受信を行うためのオンラインストレージシステムの運用を開始しました。

本報告書は、平成 23 年度に実施した情報セキュリティ対策の自己点検結果、監査結果等に基づき、環境省における情報セキュリティ対策の状況をとりまとめたものです。

平成 23 年度の自己点検結果については、点検対象項目を絞り込み重点化したことから、情報セキュリティ対策の取り組み状況は必ずしも十分とはいえない状況となっていますが、これらの項目については、今後より効果的・実践的な対応を検討し、更に徹底を図ることとします。一方で、情報セキュリティに関する意識の浸透については、これまで理解度が十分でなかった点についての向上や積極的な教育機会への参加がみられるなど、底上げが図られてきているところです。

平成 23 年度は、政府機関や企業を対象とした標的攻撃型メールの増加やサーバー攻撃の事案が発生するなど社会的な問題として取り上げられた事象があったことからも、情報セキュリティ対策の重要度は今後ますます高まっていくものと思われます。

今後より一層適切な情報セキュリティ対策を図るため、引き続き、情報セキュリティ対策の質の向上に努めてまいります。

平成 24 年５月
環境省最高情報セキュリティ責任者
（大臣官房長）　谷津　龍太郎

１．平成 23 年度の総括

（１） 平成 23 年度の評価

① 情報セキュリティ対策の実施状況の自己点検結果

環境省職員の情報セキュリティ対策の実施状況の自己点検を行った結果は、概ね適切に実施していることが明らかとなりました。しかしながら、十分に実施されていない対策事項も見られましたので、なお改善の余地があるものと考えています。

② 情報システムごとの状況

環境省の各情報システムの情報セキュリティ対策の実施状況については、重点的な調査を行った結果、全てのウェブサーバ、メールサーバ及びドメインネームサーバにおいて適切な情報セキュリティ対策が講じられていることを確認しました。

③ 教育・研修

環境省では、全職員が閲覧可能な省内の情報共有システムであるポータルサイトを活用し、情報セキュリティ対策についてのマニュアル、教材等を掲載し、各職員がいつでも情報セキュリティの学習ができる環境を整備するとともに、新規採用職員や外部からの転入者に対する集合研修を実施しています。また、情報システムを運用する課室の職員に対しては、総務省における IT 研修の受講を推奨し、セキュリティを含めた関連知識の向上に努めています。

なお、平成 21 年度及び平成 22 年度に実施した e-ラーニングによる研修については、東北地方太平洋沖地震後の緊急対応体制が長期化したため平成 23 年度は実施せず、情報セキュリティ教材を職員に配付し達成度を自己確認する方法で代替しました。

④ 調達・外部委託

環境省では、情報システムの調達や外部委託に際し、委託先の情報セキュリティ水準を確保するために、調達仕様書の記載事項を標準化し、また、求めるべき対策事項の解説資料を整備することなどにより、委託先の情報セキュリティ対策の履行状況の確認ができるようにするなど、適切な委託先管理を実施しています。さらに、情報システムごとに特有な事項については、調達案件のヒアリングにおいて情報化統括責任者（CIO）補佐官や最高情報セキュリティアドバイザーから、必要なセキュリティ要件が仕様書に盛り込まれるよう、助言を行っています。

⑤ その他取り組んだ事項

ア． セキュア USB メモリの導入

平成 22 年度から整備を推進してきました、暗号化機能、認証機能及びウィルス検知機能を有するいわゆるセキュア USB メモリを、平成 23 年度から本格的に導入するとともに、私

物や暗号化機能のない旧タイプの USB メモリについては、改めて利用禁止を周知徹底しました。

イ． オンラインストレージシステムの導入

平成 22 年度から整備を進めてきました、外部との大容量のデータの安全な受け渡しを可能とするオンラインストレージシステムの運用を本格的に開始し､外部サービスの利用制限を図りました。

ウ． ドメイン認証

環境省管轄の全てのドメインについて、メール送信時のドメイン認証設定（送信者のメールのドメインが正規のものか識別可能にし､偽装メールとの区別がつけられる環境を整備する処置）を推進しました。

エ． システム構築時の技術者向けガイドラインの導入

環境省管轄の Web システム構築において、技術者向けのガイドラインを作成しました。

⑥ 公表した情報セキュリティに関する障害・事故等の報告

平成 23 年度に公表した情報セキュリティに関する重大な障害・事故等はありませんでした。

（２） 平成 24 年度の目標

平成 24 年度に重点的に取り組む目標を以下のとおりとし、今後さらなる情報セキュリテイレベルの向上を目指していきます。

① 情報の格付け等、情報の適切な取り扱いの徹底についての一層の推進

② 全職員の更なる情報セキュリティに対する意識向上のための教育内容の充実・重点化

③ 情報セキュリティ対策のマニュアルを職員がより実践しやすいものとするための見直し

④ 情報セキュリティ対策に資するシステムの整備強化

２．報告の基本情報

（１） 環境省の概要

環境省は、地球環境保全、公害の防止、自然環境の保護及び整備その他の環境の保全(良

好な環境の創出を含む。以下、単に「環境の保全」 という。)を図ることを任務としています。環境省では、これらの任務の遂行を効果的・効率的に行うために必要な情報システムを構築・運用しています。

環境省で構築・運用している主な情報システムは、以下のとおりです。

① 環境省ネットワークシステム

職員が業務遂行に利用する LAN 回線、ソフトウェア及びハードウェアといった環境省の情報処理の基盤となる情報システム。

② 環境省電子申請・届出システム

国民の皆様がインターネットを利用して環境省への申請･届出を行うための情報システム。

③ 環境省電子入開札システム

環境省で物品等及び工事等を調達するに当たり、インターネットを利用した電子入札・開札を行うための情報システム。

（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、環境省の本省、地方環境事務所、環境調査研修所、国立水俣病総合研究センター、生物多様性センター及び国民公園管理事務所です。

（4） 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における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」
- 「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。)」
- 「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。)」

から構成される「政府機関の情報セキュリティ対策のための統一基準群」(以下「政府統一基準群」という。) において対象とする情報であって、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

本報告書の責任部署は環境省大臣官房総務課環境情報室です。

（６） 定員数

本報告書の対象となる環境省の定員数は、1,298 人（平成 23 年度末現在）です。

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

環境省では、政府統一基準群に準拠した「環境省情報セキュリティポリシー」(以下「ポリシー」 という。)及び「環境省情報セキュリティ対策マニュアル」(以下「マニュアル」という。)を平成 18 年 2 月に制定しました。

この「ポリシー」及び「マニュアル」は、環境省における情報セキュリティの確保に関する基本規範と位置付けられるものです。

「ポリシー」では、情報セキュリティの責任体制・推進体制、情報セキュリティ対策の教育、自己点検及び監査、並びに障害対応等の情報セキュリテイマネジメントに関する事項を規定しています。

「マニュアル」では、職員が日常的に実施すべき情報セキュリティ対策、情報システムの構築・運用・廃棄に係る情報セキュリティ対策等、行政事務を遂行する上で必要な具体的情報セキュリティ対策に関する事項を規定しています。

なお、これらについては平成 23 年度において、政府統一基準群の改訂に対応し、必要な見直しと修正を実施しました。

また、委託先が受託業務を実施する際の情報セキュリティ対策に関して、遵守すべき事項を記載した調達仕様書の雛型を整備するとともに、外部委託における情報セキュリティ対策を資料として整備しています。これらにより、各業務において共通に必要となる基本的なセキュリティ要件を漏れなく仕様に反映する作業を、効率的に実施できるようになっています。

（２） 情報セキュリティ対策の推進体制

① 情報セキュリティ対策に係る組織体制

情報セキュリティ対策は、職員全員が自ら取り組んでいくことはもちろんのこと、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く必要があります。

環境省では上記ポリシー及びマニュアルに基づき、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。

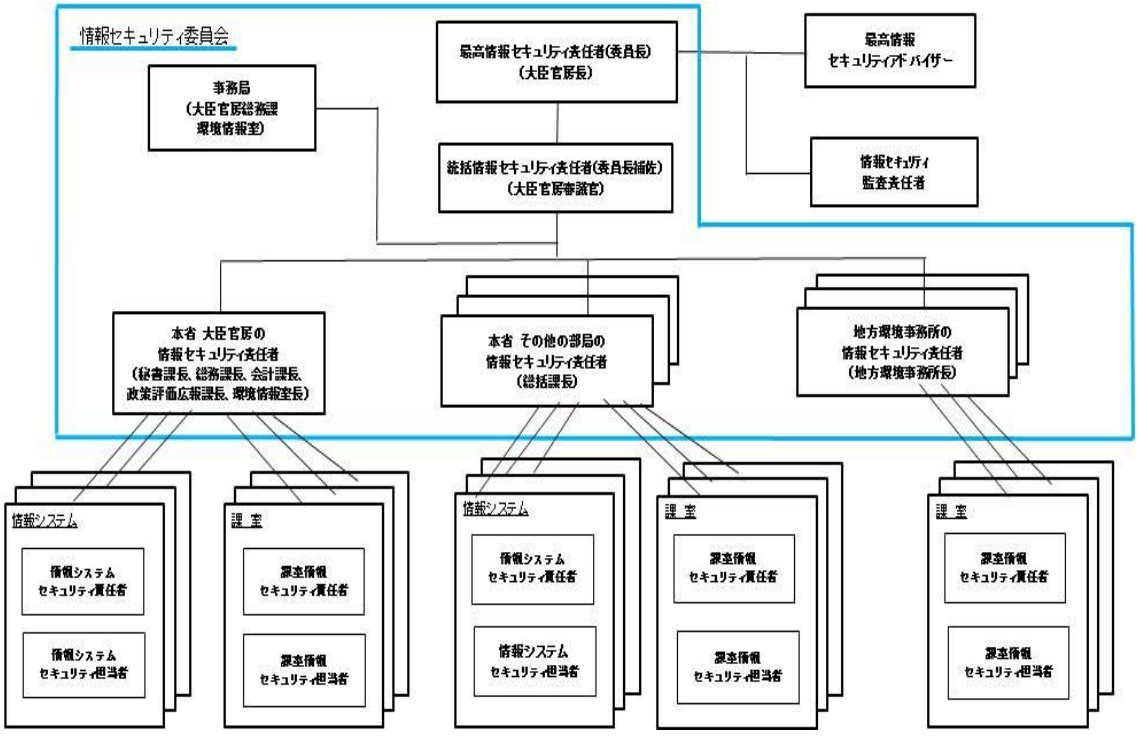
また、独自の情報システムを運用している部局においては、各システムの所管課室長を情報システムセキュリティ責任者とし、所管する情報システムの情報セキュリティ対策に取り組んでいます。

さらに、最高情報セキュリティアドバイザーを置き、本報告書の作成を含め、当省の情報セキュリティマネジメントに関して助言を得ています。

環境省の情報セキュリティ対策の推進及び重要事項を決定する組織として、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。

平成 23 年度においては情報セキュリティ委員会を５回開催し、情報セキュリティ対策に関する計画の策定、ポリシーの改訂、サイバー攻撃に対する注意喚起等を行いました。

図１　環境省の情報セキュリティ体制



② 情報セキュリティ対策に係る推進部署の体制

環境省の情報システムの整備及び管理を担当している大臣官房総務課環境情報室では、情報セキュリティに係る以下の役割を担っています。

- 情報セキュリティ担当

情報セキュリティに関する事務を統括し、情報セキュリティ関連規程の整備や情報セキュリティ対策の教育、監査等を実施しています。

- システム管理整備担当

ポリシーを踏まえ、情報処理の基盤となる環境省ネットワークシステムの運用や省内各課室の業務に係る個別業務システムの運用支援を行っています。

（3） 監査等

① 情報セキュリティ監査の実施

情報セキュリティの水準を適切に維持していくためには、ポリシー及びマニュアルを適切に整備・運用することによってその実効性を確保し、その準拠性と妥当性の有無を客観的に確認する必要があります。また、情報セキュリティ対策の実施状況を適切に評価し、評価結果に応じて見直しを行うという PDCA サイクルを適切に運用することが重要です。

これらの点を踏まえ、環境省の情報セキュリティ監査は、ポリシー及びマニュアルに基づき、独立性を有する外部の監査組織に委託して実施しています。なお、監査対象となる情報システムは、毎年度、情報システムの運用状況等を考慮して選定しています。

② 平成 23 年度監査計画の概要

ア． 情報セキュリティポリシー準拠性監査

環境省の全業務を対象範囲としたポリシー及びマニュアルの査読調査の実施

イ． 自己点検に関する監査

USB メモリの不正持出し等内部における不適切な行動のリスクの評価を重点事項とした、自己点検票の確認調査、インタビュー調査及び外部委託先を含む現場調査(執務室、機器設置場所、アーカイブ媒体保管場所)の実施

ウ． 外部からの侵入検査（脆弱性診断）

環境省ネットワークシステム及び環境省ホームページ上の Web アプリケーションを対象範囲とし、外部からの不正侵入、改ざん等に関する検査の実施

③ 監査の結果

ア． 情報セキュリティポリシー準拠性監査の結果

情報セキュリティポリシー準拠性監査の結果、重要情報に関する情報漏えい等の大きな損失を直ちに発生させる重大な不備がないことが確認されました。

なお、ポリシー及びマニュアルの査読調査において前年度の同調査において不備が指摘されていた事項について、大半が修正させていたものの一部未修整の事項があることが確認されました。

イ． 自己点検に関する監査の結果

自己点検票の確認調査、インタビュー調査及び現場調査から情報の格付け及び PC の取扱いに関して、現場での実施状況に関する軽微な不備が確認されました。

また、USB メモリーの取扱い等については、平成 22 年度から情報セキュリティ面で向上している点もありますが、未だ改善の余地があることが確認されました。

ウ． 外部からの侵入検査（脆弱性診断）の結果

一部のサイトにおいて、SQL インジェクション及びクロスサイト・スクリプティングの脆弱性が検出されました。

④ 監査の結果を踏まえた対応

ア． 情報セキュリティポリシー準拠性監査結果への対応

査読調査での指摘事項について適切な修正を行うこととします。

イ． 自己点検に関する監査結果への対応

- 業務で利用される PC 及び USB メモリは、私物や暗号化機能等がないものの利用の禁止を改めて周知し、セキュリティ管理部門から貸与するセキュリティ管理されたものの利用を周知徹底しました。
- 外部との大容量データ受け渡しにおいて、ポリシーに基づく手続を遵守した利用が可能となるようセキュリティ管理されたオンラインストレージシステムの利用を周知し、外部のサービス利用の禁止を改めて周知徹底しました。
- 現場で利用されている情報に関して、情報の格付けに関する教育を継続実施するとともに、抜け漏れ防止を念頭にした格付け明示の手段等を検討します。
- ポリシーへの遵守状況を監視（モニタリング）できる仕組みを検討します。

ウ． 外部からの侵入検査(脆弱性審査)結果への対応

データの不正取得や改ざんなどの損失や踏み台として利用される可能性のある事項については直ちに修正に取り組みとともにその他の脆弱性が確認されたサイトも含めて Web アプリケーションシステムの見直し及び修正を実施しました。

また、修正した内容に関する再検査を実施します。

（４） 業務・システム最適化における取組の管理

環境省では、情報システムの予算要求段階、仕様書策定の各段階において、CIO 補佐官及び最高情報セキュリティアドバイザーによるヒアリングを実施しています。その際に、適宜、情報セキュリティ対策についてもシステムや業務の特性に応じて、指導助言を行うことで情報システムの安全性・信頼性を確保するための取組を管理しています。

（５） 情報資産台帳の整備と活用

環境省では、省内の各情報システムの情報システムセキュリティ責任者、システムを所有する部署、ハードウェア・ソフトウェア・ネットワークに関する各情報を網羅した情報資産台帳を整備しています。

この情報資産台帳は、情報システムの状況の把握に活用するとともに、各システムの情報セキュリティ対策を適切に維持・改善するための資料としても活用しています。

（６） 情報セキュリティ対策に関する文書の見直し状況

環境省では、政府統一基準群の改訂が行われた際には、ポリシー及びマニュアルに適切に反映させ、準拠性を確保することとしています。また、情報セキュリティ監査で指摘を受けた場合や運用上での不具合が生じた場合においても、適宜これら文書の見直しを行っています。

平成 23 年度は、政府統一基準群の改訂を踏まえ、平成 24 年 2 月にこれら文書の改訂（第 5 版）を行いました。

（７） 業務継続計画の策定

環境省では、平成 17 年９月に中央防災会議が決定した「首都圏直下型地震対策大綱」に基づき、平成 20 年７月に首都直下型地震発生を想定した「環境省業務継続計画」を策定しています。これに基づき、当省における重要業務の継続を確保する観点から、業務の基盤システムである 環境省ネットワークシステムに関する事項を含めて対応を図っています。

環境省ネット ワークシステムの中枢の機器については、耐震対策、電源の多重化等を図ったデータセンターに設置しており、昨年発生した東北地方太平洋沖地震においても被災地周辺の地方拠点の通信断を除き、システムへの影響は発生しませんでした。しかし、首都圏直下型地震も想定震度が高く修正されるなど、首都圏においても東北地方太平洋沖地震クラスの地震の発生リスクに対する備えが求められることから、業務継続計画の見直しも検討しつつあるところです。

４．平成 23 年度の重点事項

平成 23 年度においては、システム的な対応の強化として、平成 22 年度から導入を進めてきたセキュア USB メモリ及びオンラインストレージシステムの本格運用を進めることで、無許可 USB メモリの利用禁止の徹底及び外部のオンラインストレージの利用禁止の徹底を進めました。

セキュア USB メモリについては、繰り返し周知するとともに、関係部局の協力のもと省内でのデータの受け渡しの際にセキュア USB メモリの利用を義務づけることにより、着実に利用が根付いてきました。

また、オンラインストレージシステムについては、原則として Web フィルタリング機能

により外部システムへの接続を制限するとともに、NISC の協力も得て、外部システムの利用を監視し、その時点で接続制限許可されていない外部システムの利用が確認された際には、直ちに状況確認の上、接続を制限することとしています。

５．情報セキュリティ対策の実施状況

5.1　情報セキュリティ対策の実施状況の自己点検

（１） 課題と対策

①　自己点検の概要

環境省では、情報セキュリティ対策の各遵守事項について、毎年 1 回、実施状況の自己点検(以下「自己点検」 という。)により自己評価を行っています。

自己点検の対象者は、平成 18 年度及び 19 年度は課室長クラス以上とし、平成 20 年度からは全行政事務従事者を対象としています。

自己点検の項目は、NISC の点検項目を参照し、責任者等（最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ監査責任者・実施者、情報セキュリティ責任者及び課室情報セキュリティ責任者)、システム責任者等（情報システムセキュリティ責任者・管理者及び権限管理を行う者)、行政事務従事者の３つの区分に分類し、各主体において実施すべき情報セキュリティ対策に沿った内容としています。

なお、平成 23 年度においては、NISC から提供された自己点検シートを有効活用し、特に確認が必要な情報の取り扱いに関する事項等を重点的に確認するため、点検項目数を減らしました（責任者等：のべ 80 項目→のべ 51 項目、システム責任者等：のべ 145 項目→のべ 24 項目、行政事務従事者：91 項目→6 項目)。

②　平成 22 年度自己点検結果に基づく課題と対策

平成 22 年度においては、全行政事務従事者のうち自己点検票を提出した者の割合である把握率が前年度の 94.4%から 98.0%へと向上しましたが、100%に至っていない状況です。

各種対策の実施状況を表す実施率については、ポリシー全般としては職員の実施率が 94.0%であり、概ね適切に実施している結果となりました。一方で、機密性の明示、格付けに従った取り扱い・保存、情報の移送・提供といった、情報の取り扱いに関する遵守事項については、相対的に実施率が低い結果となりました。

これらの点については、一層の教育とともに、行政事務従事者毎に取り扱いの解釈が異なることなどを減らすための運用ルール、ガイドラインの更なる整備とともに、情報システムにより対策を徹底させることが可能な事項については、システムによる対応を進めることで、全体的なセキュリティの向上を目指す必要があると考えています。

これらを踏まえ、平成 23 年度においては、引き続き教育を行うとともに、機密性の格付

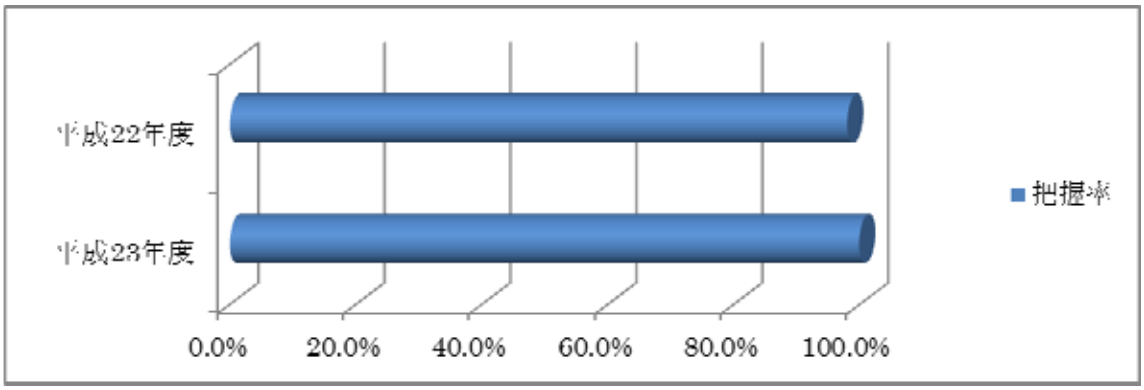
け及び明示を行う際の解説を加えた機密性表示例のテンプレートを利用するための周知を行いました。また、平成 22 年度に整備した暗号化やパスワード機能を持つセキュア USB 及び安全なデータ授受を行うためのオンラインストレージの運用を開始し、利用の徹底を周知しました。

（２） 平成 23 年度自己点検結果の状況

① 把握率

把握率（全行政事務従事者のうち自己点検票を提出した者の割合）は、平成 23 年度は全体で 99.9%であり、自己点検自体への取り組みはほぼ全省に浸透してきているといえます(図 2 参照)。

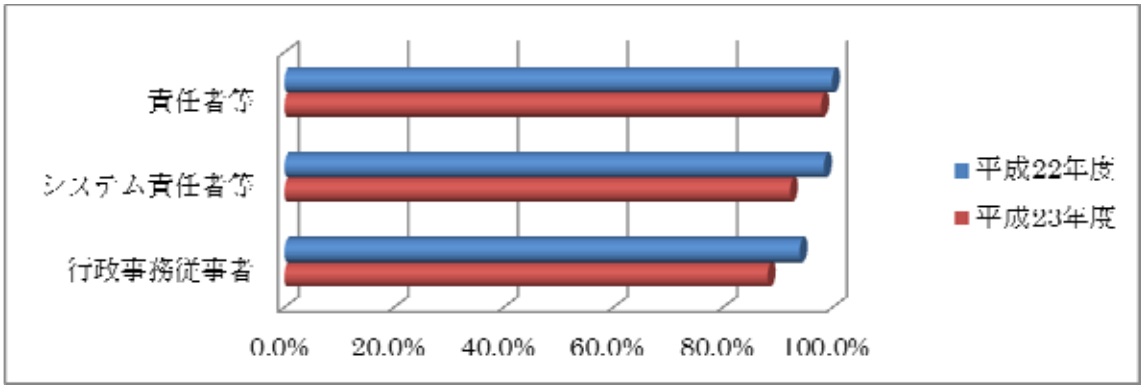
図２　自己点検の把握率



② 実施率

実施率（自己点検票を提出した者のうち情報セキュリティ対策を実施した者の割合）について主体別の状況をみると、平成 23 年度は責任者等 97.9%、システム責任者等 92.2%、行政事務従事者 88.1%といずれの主体も前年度を下回る結果となりました (図３ 参照)。

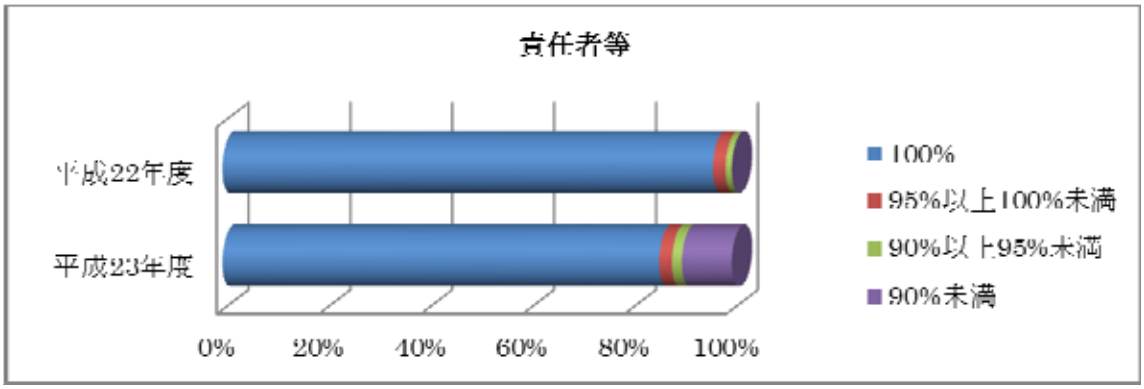
図３　主体別実施率

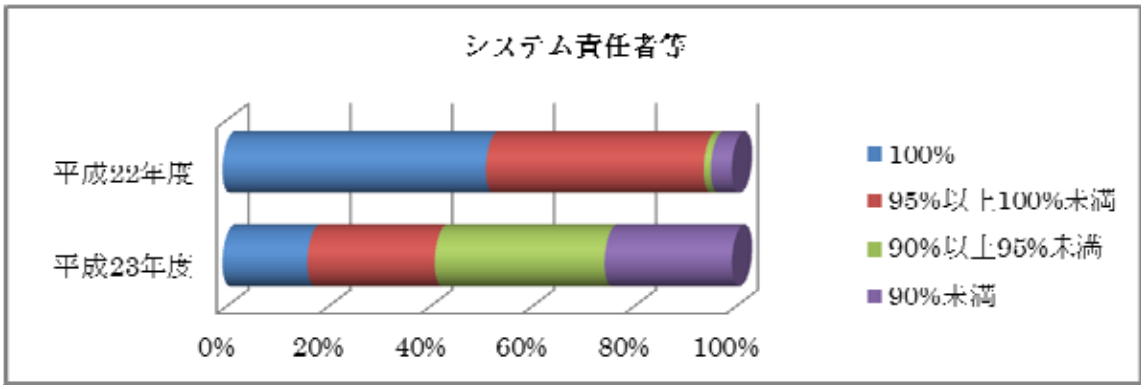


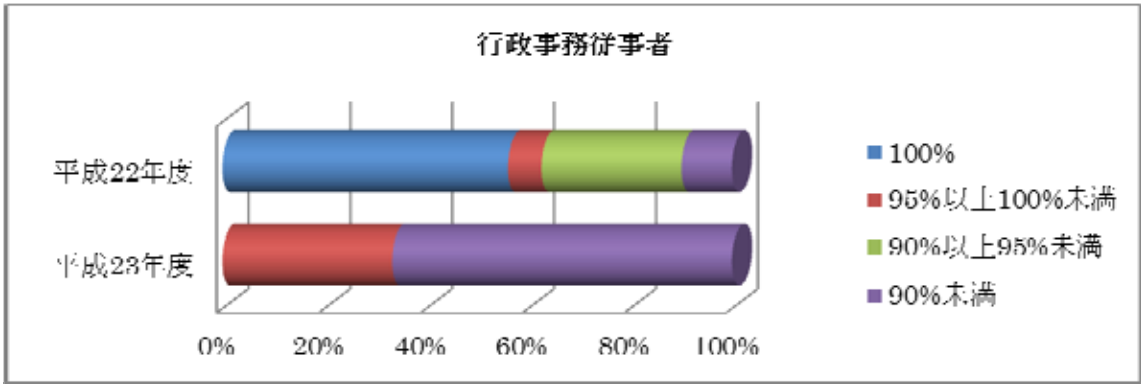
③　到達率

到達率（自己点検を行った遵守項目について、自己点検票を提出した者のうち一定の割合(100%、95%、90%)以上の者が対策を実施した項目の割合）については、「100%実施した割合」は、責任者等 86.3%、システム責任者等 16.7%、行政事務従事者 0.0%、「95%以上実施した割合」は、責任者等 88.2%、システム責任者等 41.7%、行政事務従事者 33.3%、「90%以上実施した割合」は、責任者等 90.2%、システム責任者等 75.0%、行政事務従事者 33.3%であり、平成 23 年度は各主体とも前年度を下回る結果となりました（図４参照）。

図４　主体別対策到達率







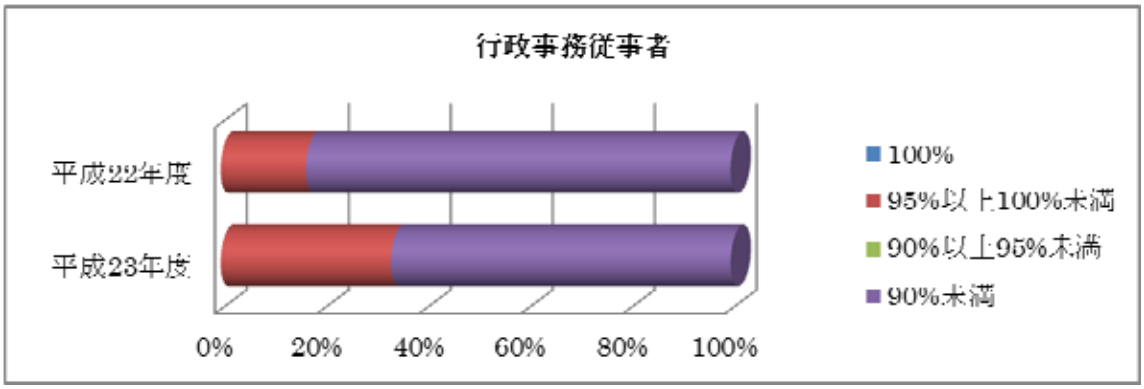
■ 100%の対象者が対策を実施した項目の割合
■■ 95%以上の対象者が対策を実施した項目の割合
■■■ 90%以上の対象者が対策を実施した項目の割合

（３） 総評

平成 23 年度の自己点検結果は、前年度と比較して把握率は向上しましたが、実施率、到達率は減少しました。これは、点検項目の重点化を図り点検項目数を、前年度より大幅に減らしたことにより、従来より実施率の高かった項目が点検項目からはずれたことが影響を与えているものと推測されます。

行政事務従事者については、情報の作成、入手、利用、保存、移送、提供及び消去の各段階での取り扱い等、特に確認が必要な項目を中心に点検を行いましたが、平成 22 年度の点検項目から平成 23 年度と同様の項目を抽出して比較したところ、若干ですが到達率が向上していることがわかりました（図５参照）。

図５　行政事務従事者到達率分析



また、震災後の非常時対応のため、申請等事前手続きが不十分な例が見受けられました。これは、今般の震災への対応として多数の緊急対応が発生したこととともに、通常を超える大幅な人員増強が平成 24 年１月に急遽発生したことから、新規採用者への教育期間が十分ではない段階での自己点検となったことが影響しているものと考えられます。

自己点検の内容については、セキュリティに関する難解な用語を平易な表現で解説し、理解度を深める努力を省内で続けている結果、ルールについては理解が深まってきていますが、非常時対応の長期化によってセキュリティのルールを軽視することのないよう、日常業務におけるセキュリティルールの周知徹底を引き続き行っていく必要があります。

一方で、自己点検票の確認調査、インタビュー調査及び現場調査から、情報の格付け及びPC や USB メモリの取り扱いに関して、一定の効果を上げていることが確認されました。また、情報の格付けに関しては、判断しにくい事例がある等の報告もありましたので、格付けや保存期間について、文章作成時の機密性表示や保存期間指定のシステム対応等、実効性のある対応を順次実施する必要があります。

紙媒体での要機密資料の保存に関して、情報量に対して充分な保管場所が確保できていないとう課題については、直ちに対応することは難しいことから、要機密情報の中でも特に機密性の高い情報について施錠管理を徹底し、これ以外の要機密情報についても順次対応を図っていく必要があります。

（４） 自己点検結果に基づく改善指示等の状況

環境省では、情報セキュリティ委員会を開催し、自己点検の結果を報告するとともに、委員である情報セキュリティ責任者を通じて全職員に対して情報セキュリティ対策の実施状況及び今後重点的に実施すべき対策の周知を繰り返し行いました。

また、平成 24 年度においては、自己点検結果を踏まえ、以下の点を中心とした対策の強化を検討することとしています。

- 書類作成時点で明記すべき格付けや機密性を確認するシステム的な仕組による格付け明示の徹底。
- 要機密情報の取り扱いについて、より具体的な対策につなげるための資料の充実及び教育の実施
- 対策を徹底するための効果的なシステムの整備・運用の改善

5.2　情報システムごとの状況

（１） 課題と対策

① 重点検査の概要

各課室等で運用する情報システムについては、費用対効果も念頭に置きつつインターネット上からの各種攻撃等に加え内部からの情報漏えいを防ぐなど、様々な観点での対策が重要となります。また、セキュリティを強化することにより安全性は高まりますが、一方で利便性の低下につながり、各種 Web　サーバなど一般の方にご利用いただくシステムの使い勝手が損なわれたり、内部の者の業務効率を低下させる場合があります。セキュリティの確保と利便性の維持という相反する点について、双方のバランスをとりつつ、セキュリティの向

上を図ることが必要となります。

こうしたことから､環境省では省内で導入し使用している情報システムごとの公開系サーバ（Web サーバ、メールサーバ等）に対する情報セキュリティ対策に関して政府統一基準群で定められた遵守事項の実施状況に係わる重点的な検査(以下「重点検査」という。）を毎年度実施しています。

② 平成 22 年度重点検査結果に基づく課題と対策

平成 22 年度の重点検査の結果は、各情報システムの端末、Web サーバ及びメールサーバに対する情報セキュリティ対策について実施率が 100%であり、不備は認められませんでした。

しかし最近は、なりすましメール等による高度な標的型攻撃も増加してきており、不正な侵入を早期に発見する仕組みや、侵入された場合の被害の最小限化・拡大防止、迅速な復旧など、システム的な機能強化に加え、教育・訓練等による意識や注意力の向上にも努めていく必要があります。

（２） 情報システムの対策状況

平成 23 年度の重点検査では、環境省ホームページの公開用 Web サーバ及び電子メールサーバを対象に、それぞれに搭載している OS 等のソフトウェアのセキュリティ修正プログラムの適用状況や不正アクセス対策､不正プログラム対策等の情報セキュリティ対策実施状況について検査を行いました。

平成 23 年度の重点検査における情報システムの対策状況は、以下のとおりです。

① 公開用 Web サーバ

公開用 Web サーバの不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理の対策事項の実施率は、前年度に引き続き、全て 100%を達成しています。

② メールサーバ

メールサーバの不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理の対策事項の実施率は、前年度に引き続き、全て 100%を達成しています。

③ ドメインネームシステム（DNS）サーバ

ドメインネームシステム（DNS）サーバの不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理の対策事項の実施率は、前年度に引き続き、全て 100%を達成しています。

（３） 総評

情報システムの情報セキュリテイ対策については、順次データセンタへの統合を進め、統

一的な運用管理を図るなどの対策を講じており、平成 23 年度の対策事項の実施率は、前年度に引き続きすべて 100%となっています。今後もこの状態を維持するよう適切な情報セキュリティ対策を実施する必要があります。

（４） 特筆すべき事項

環境省の全行政事務従事者が利用している環境省ネットワークシステムにおいては、不正な外部アクセスへの対策として攻撃の監視や遮断、迷惑メール対策、コンピュータウイルス対策を実施しています。

特に、ウイルス対策については、メールに加え Web サイトの閲覧時のチェックも行うことで、改ざんされた Web サイトから送り込まれるウイルスへの感染を防ぐ効果を発揮しています。また、経路上のサーバ及び端末において、異なる製品によるウイルスチェックを行っており、比較的新しいウイルスに対しても安全性を高めることができます。一方で、最新のウイルスの場合、全てを完全に検知することはできない場合がありますが、従来よりなりすまし等を含め少しでも不審なメールがあった場合には直ちに環境情報室に相談することが省内利用者に浸透しており、より迅速な対処が図られています。

また、外部から資料を受領することが多い研修機関においては、外部講師が持参する USB メモリに対し、省内ネットワークから切り離した専用端末によるウイルスチェックを行うことにより、ウイルス感染のリスクの低減を図っています。

5.3　教育・啓発

（１） 教育

①　教育計画の策定、教育の企画等

環境省では、平成 21 年度より効率的な教育を実施するため、e-ラーニングによる研修を中心に、各種教材の整備、年度当初における新規採用者、転入者への集合研修を実施してきました。

平成 23 年度は、東北地方太平洋沖地震の緊急対応体制が長期化したため、e-ラーニングによる研修は実施せず、情報セキュリティの重点項目をまとめた研修資料を各職員に配付し、研修を行いました。併せて自己点検により、理解度、達成度を把握しました。平成 23 年度の自己点検結果から、この研修には一定の効果があったものと推測します。ただし、環境省は小規模な地方拠点が多数存在するため、これらの拠点に関しては e-ラーニングによる研修は特に有効と考え、平成 24 年度においては、e-ラーニングも含め、より効果的な教育の実施方法を検討します。

②　役割に応じた教育教材の整備

環境省では、研修教材やセキュリティ対策の実施のためのマニュアルは、役割に応じた対策のための資料として整備しており、これらの中でそれぞれの役割に当たる者が何をなすべ

きかを具体的に解説しています。なお、教育教材は、自己点検や監査結果を踏まえ、対応が不十分な事項についてその内容を充実し、最新の事件・事故の事例を取り込むなど、適宜見直しを図っています。

③　教育受講状況の管理

平成 23 年度は e-ラーニングを実施しなかったため、各課室の担当者を通じて受講状況の管理・報告を行いました。

④　情報セキュリティ対策担当者の知識向上等

情報セキュリティ対策担当者についても、役割毎の教材を整備しています。また、総務省における IT 研修の受講を推奨し、セキュリティを含めた関連知識の向上に努めています。

（２）　各種資料の整備と閲覧環境の整備

ポリシー及びマニュアル並びに各種参考情報を職員ポータルサイトに掲載し、全行政事務従事者が随時参照できる環境を整備しています。

（３）　情報セキュリティ事案発生時の周知徹底

外部での事件・事故や内部での注意喚起が必要な事例などについて、随時情報を収集し、情報セキュリティ担当者から全行政事務従事者へのメール及び職員ポータルサイトへの掲載により、迅速かつ全行政事務従事者が理解しやすい形での注意喚起及び情報セキュリティ対策の周知徹底を図っています。

5.4　調達・外部委託

環境省では、情報システムの開発や運用等の業務を外部に委託して実施する際には、委託先においてもポリシーに準ずる情報セキュリティ水準を求めています。

このため、環境省では、委託先が受託業務を実施する際の情報セキュリテイ対策に関して、遵守すべき事項を記載した調達仕様書の雛型を整備するとともに、外部委託における情報セキュリティ対策を資料として整備しています。さらに、情報システムごとに特有な事項については、調達案件のヒアリングにおいて CIO 補佐官や最高情報セキュリティアドバイザから、必要なセキュリティ要件が仕様書に盛り込まれるよう、助言を行っています。これらにより、情報システム開発や運用等の業務の際に外部委託先に求める情報セキュリティレベルを維持するよう努めています。

また、仕様書に情報セキュリティ対策の実施方法及び管理体制、情報の取り扱い、取り組みが不十分文は事件・事故が発生した場合の監査の受け入れ、業務完了時の報告等を明記することで各種対策が確実に講じられることを担保しています。

5.5　その他取り組んだ事項

（1） セキュアUSBメモリの導入

平成22年度から整備を続けてきた、セキュアUSBメモリ（集中管理が可能な暗号化機能、認証機能及びウィルス検知機能を有するUSBメモリ）を省内の各課室に約500個配付し、本格的な運用を開始しました。併せて、私物や過去に課室単位で導入していた暗号化機能のない旧タイプのUSBメモリの利用については、改めて利用禁止を周知徹底しました。また、無許可デバイスの利用を制限する方向で、さらなる検討を進めています。これにより、ウィルス感染の可能性が減るとともに、紛失・盗難等の場合でも、情報漏えいリスクを低減できることとなりました。

（2） オンラインストレージシステムの導入

これまでポリシーの遵守が不十分であった外部との大容量データの受け渡しの手段として、平成22年度から整備を進めてきた、情報の移送・提供時にWEB上の手続きを行うことで利用可能な、暗号化通信、期間限定の認証、データの自動削除機能を有するオンラインストレージシステムの運用を本格的に開始しました。併せて、外部ストレージシステムの利用の禁止を徹底しました。これにより、外部ストレージシステムの利用による万が一の情報漏えいリスクを減らした上で、情報の移送・提供の状況把握とルール順守を過度の負担なく適切に行うことが可能となりました。

（3） ドメイン認証

NISCからの指示に基づき、環境省管轄のメール発信を行う全てのサイトについて、メール送信時のドメイン認証設定（送信者のメールのドメインが正規のものか識別可能にし、偽装メールとの区別がつけられる環境を整備する処置）を推進し、徹底されたことを確認しました。

（4） システム構築時の技術者向けガイドラインの導入

環境省管轄のWebシステム構築において、技術者向けのガイドラインを作成しました。この中で、セキュリティ関連のプログラミングについては、独立行政法人情報処理推進機構(IPA）のガイドラインに準拠することとしています。これにより技術面の対応の標準化が推進されることが期待されます。

６．情報セキュリティに関する障害・事故等報告

6.1　障害・事故対応のワークフロー

環境省では、情報セキュリティに関する障害・事故等が発生した場合には、担当者は状況を把握の上、まず、各課室の情報セキュリティ責任者及び省内の情報セキュリティ対策を所管する環境情報室に直ちに報告します。それと同時に担当者は、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へ障害・事故等の状況を報告することとしています。迅速な報告とともに、以後の対策等についても検討し、再発防止策とあわせて省内へ注意喚起することで同様の障害・事故がない体制とするよう努めています。

6.2　公表した情報セキュリティに関する障害・事故等報告

平成 23 年度においては、該当する事例はありませんでした。

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 年度においては、政府統一基準群へのポリシーの準拠を進めるとともに、平成 23 年度の自己点検結果及び監査での指摘事項を踏まえ、引き続き、情報の格付けの明示や情報の移送、提供に関する手続きの徹底について、指導・教育をさらに進めるとともに、格付けの明示漏れ防止や安全な情報の移送､提供方法についての仕組みの検討をさらに進めるため、以下の点について対策の充実を図ります。

① 情報の格付け等、情報の適切な取り扱いの徹底についての一層の推進

- 書類作成時点で容易に格付けを判断できるシステム的な仕組を設け、業務で作成される各種資料や情報に対して、情報の格付け及び格付けの明示の徹底を図ります。

② 全職員の更なる情報セキュリティに対する意識向上のための教育内容の充実・重点化

- 各種手続きの明確化や機密性の追加説明の周知を図ります。

③ 情報セキュリティ対策のマニュアルを職員がより実践しやすいものとするための見直し

- 情報セキュリティ対策マニュアルの活用強化を図ります。

④ 情報セキュリティ対策に資するシステムの整備強化

- 平成 24 年度に更新予定の次期システムにおいて無許可デバイスの接続性減などシステム的な対応の強化を進めます。

おわりに

環境省は、環境に関する幅広い分野を所管しています。その所管する業務である廃棄物対策、公害規制、自然保護環境保全、野生動植物保護などでは、時間的な変化や複雑な影響を考慮して、機密性、完全性、可用性を判断しなければならない情報を取り扱っています。

環境省の情報システムは、基幹の環境省ネットワークシステム以外に、比較的小規模のホームページや業務システムが全国各地に多数散在しており、限られた予算と人員の効率的な活用に留意して、情報システムの効果的な運用や情報セキュリティの確保に努めて来ました。

このような状況の中、平成 23 年 3 月の東日本大震災や原子力発電所事故に伴うガレキ処理、環境中の放射性物質による被ばく線量を下げるための除染処理等、緊急を要する新たな業務に応じるための情報システムは、体制整備や設備導入に十分な時間をかけることができないまま運用が始まりました。

また、平成 23 年度は、環境省ネットワークシステムの職員用端末やプリンタの更改、次期ネットワークシステム更改準備時期とも重なりました。情報システム担当職員は、震災関連業務への対応と基幹システム更改業務に多くの時間を割く必要がありました。このような状況の中、暗号化携帯ハードディスクの活用や、送信ドメイン認証設定によるなりすましメール対策等の情報セキュリティへの取組を実施してきました。

中でも、以下に示す取組については、利用者への負担を増やすことなくセキュリティ水準を効果的に向上させたものとして、評価できます。

○セキュアＵＳＢメモリの導入と利用促進による、ウィルス感染や情報漏えいリスクの低減

○オンラインストレージの運用による、大容量データ受け渡しにおける情報漏えいリスクの低減とルール順守の向上

また、影響が大きいと思われる外部のセキュリティ事案等について、環境省の実情を十分に配慮し、全行政事務従事者に理解し易いよう工夫して迅速に周知するなど、タイムリーで効果的な注意喚起や情報提供を行いました。

以上のような取組の継続的な実施により一定の成果を上げ、情報セキュリティに関する職員の意識も徐々に向上してきました。

しかしながら、情報セキュリティのリスクは年々高くなって来ています。従来より積み上げてきた情報セキュリティ対策に加え、激しさを増す標的型攻撃や大規模自然災害発生への備え等、現場の実情やリスクの大きさ・特性に応じて、着実でバランスが取れた情報セキュリティの取組を、スパイラルアップにて推進することが重要です。

環境省最高情報セキュリティアドバイザー　安田　晃