平成 23 年度

情報セキュリティ報告書

平成 24 年５月

文部科学省

【　目　　次　】

１．　はじめに　～情報セキュリティ最高責任者からのメッセージ～

近年、情報通信技術の急速な進歩に伴い、情報セキュリティの脅威についても多様化・高度化・複雑化しております。平成 23 年度においては、防衛関連企業及び政府機関を標的としたサイバー攻撃により、コンピュータウィルスへの感染や情報漏洩等の被害が相次ぎ発生し、報道等においても大きく取りあげられ、社会問題となりました。

当省においても、遺憾ながら、昨年 12 月に個別事業のウェブサイトがサイバー攻撃を受け、ウェブサイトの一部改ざん及び個人情報の流出が判明しました。ウェブサイトの利用者及び個人情報が漏洩した方々には、大変なご迷惑やご心配をお掛けしましたことを心よりお詫び申し上げますとともに、今後は、より一層の情報管理の徹底を図るなど情報セキュリティ対策の強化を行ってまいります。

一方、平成 23 年 3 月 11 日に発生した東日本大震災を踏まえ、災害時における業務の継続性が改めて注目されていますが、災害時に業務を継続する上で必要な情報や情報システムを利用できるよう適切な対策を講ずることが、情報セキュリティ上重要であると考えられます。

当省では、教育の振興及び生涯学習の推進を中核とした豊かな人間性を備えた創造的な人材の育成、学術、スポーツ及び文化の振興並びに科学技術の総合的な振興を図ることを任務としており、任務を遂行する上で様々な情報を取扱っています。

これらの情報を、情報セキュリティの脅威から守ると共に、災害時等における不測の事態が発生した場合においても活用し業務を継続できるよう、以下の点を中心に情報セキュリティ対策に取り組んでまいりました。

(1)　専門家の確保による情報セキュリティ対策の推進体制の充実・強化
(2)　省内職員向けの情報提供及び研修による情報セキュリティの普及啓発
(3)　情報セキュリティ監査の拡充による情報セキュリティ対策の充実・強化
(4)　情報システム運用継続計画（IT-BCP）の取組による情報システム危機管理の強化

本報告書は、このことを踏まえ、平成 23 年度に実施した情報セキュリティ対策の取組、監査結果等についてまとめたものです。

情報セキュリティ対策は政府機関にとって重要な課題となっており、今後の情報技術の発達や環境の変化により、新たな情報セキュリティ上の脅威が出現してくることも想定されます。当省としてはそれらに適切に対処し、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。

情報セキュリティ最高責任者
（文部科学省大臣官房長）
前川　喜平

２．　情報セキュリティ対策の枠組

（１）　情報セキュリティに関する文書体系

当省では、「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。）に準拠した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、「文部科学省情報セキュリティポリシー」（以下「ポリシー」という。）を定めています。

また、省内 LAN 及びグループウェア等の共通基盤である行政情報システムについて、ポリシーに定められた遵守事項を運用していくための手順となる文書として、以下に掲げる 2 種類の実施手順書を整備しています。

- 行政情報システム利用手順書
- 行政情報システム管理手順書

（２）　情報セキュリティ対策の推進体制

当省では、情報セキュリティ対策を推進するために、統一管理基準及び統一技術基準並びにポリシーに基づき、以下に示す体制を整備しています。（図 1 参照）

①　情報セキュリティ最高責任者

情報セキュリティ対策に関する事務を統括します。大臣官房長が務めます。

②　文部科学省情報セキュリティ対策委員会

情報セキュリティについての協議、情報交換、体制の強化を図り、ポリシーの策定・変更等重要事項の決定を行います。情報セキュリティ最高責任者が委員長を務めます。

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、公正不偏の態度で監査を行い、結果を情報セキュリティ対策委員会に報告します。

④　統括情報セキュリティ責任者

情報セキュリティ最高責任者の指示のもと、ポリシーに基づき、情報セキュリティ対策を推進します。大臣官房政策課情報化推進室長が務めます。

⑤　情報セキュリティ責任者

局（官房各課、各局及び文化庁）内の情報セキュリティ対策に関する事務の統括・管理を行います。官房各課長、各局筆頭課長及び文化庁長官官房政策課長が務めます。

⑥　課室情報セキュリティ責任者

ポリシーに基づき、課（課、室及び班等）内の情報セキュリティ対策に関する事務を統括します。

⑦　情報システム責任者

各課が所管し運用する情報システムに対する情報セキュリティ対策に関する事務を統括します。

⑧　情報システム管理者

情報システム責任者の指示に従い、情報システムにおける情報セキュリティ対策を実施します。

⑨　情報セキュリティアドバイザー

情報セキュリティ最高責任者の求めに応じ、助言を行います。情報化統括責任者補佐官（以下「CIO 補佐官」という。）が務めます。

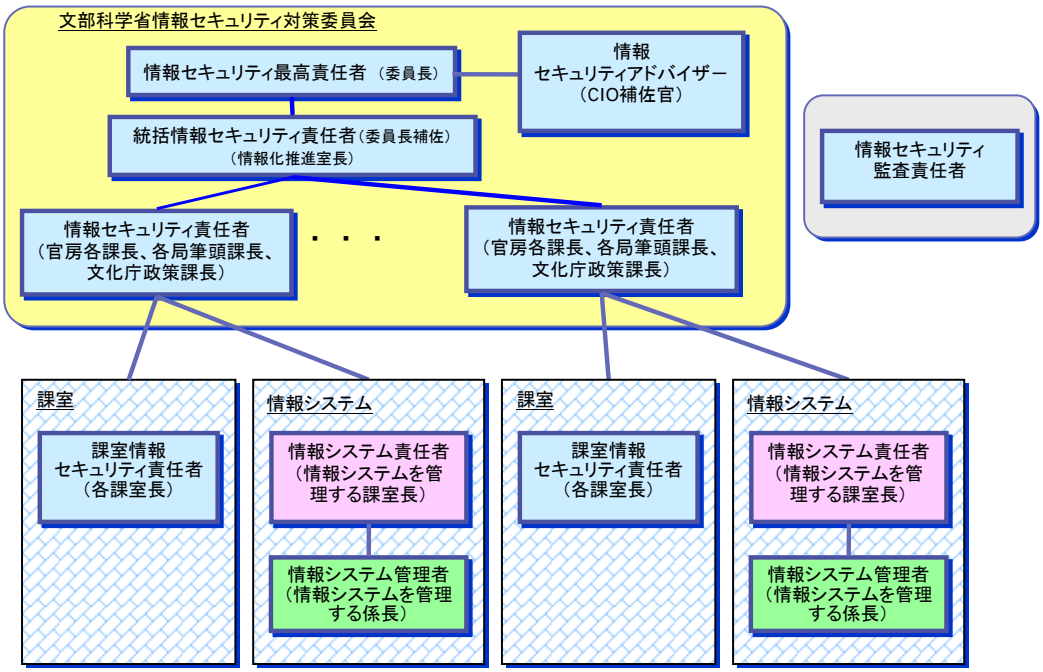


図 1 情報セキュリティ対策の推進体制

⑩　情報セキュリティ対策に係る推進部署

情報セキュリティ対策に係る推進部署は、大臣官房政策課情報化推進室が担当しており、主な役割は以下のとおりです。

- 情報セキュリティ対策に関すること。
- 文部科学省情報セキュリティ対策委員会に関すること。

- 情報セキュリティに係る他省庁との連絡調整に関すること。
- 当省所管の施設等機関、独立行政法人等の情報セキュリティ対策に関する指導、助言及び情報提供に関すること。
- 情報セキュリティに係る職員に対する普及啓発に関すること。

（３） 情報セキュリティに関する中期的な取組

当省では、情報セキュリティレベルの向上を図るために、下図に示す事項を中心に中期的な取組を推進しています。

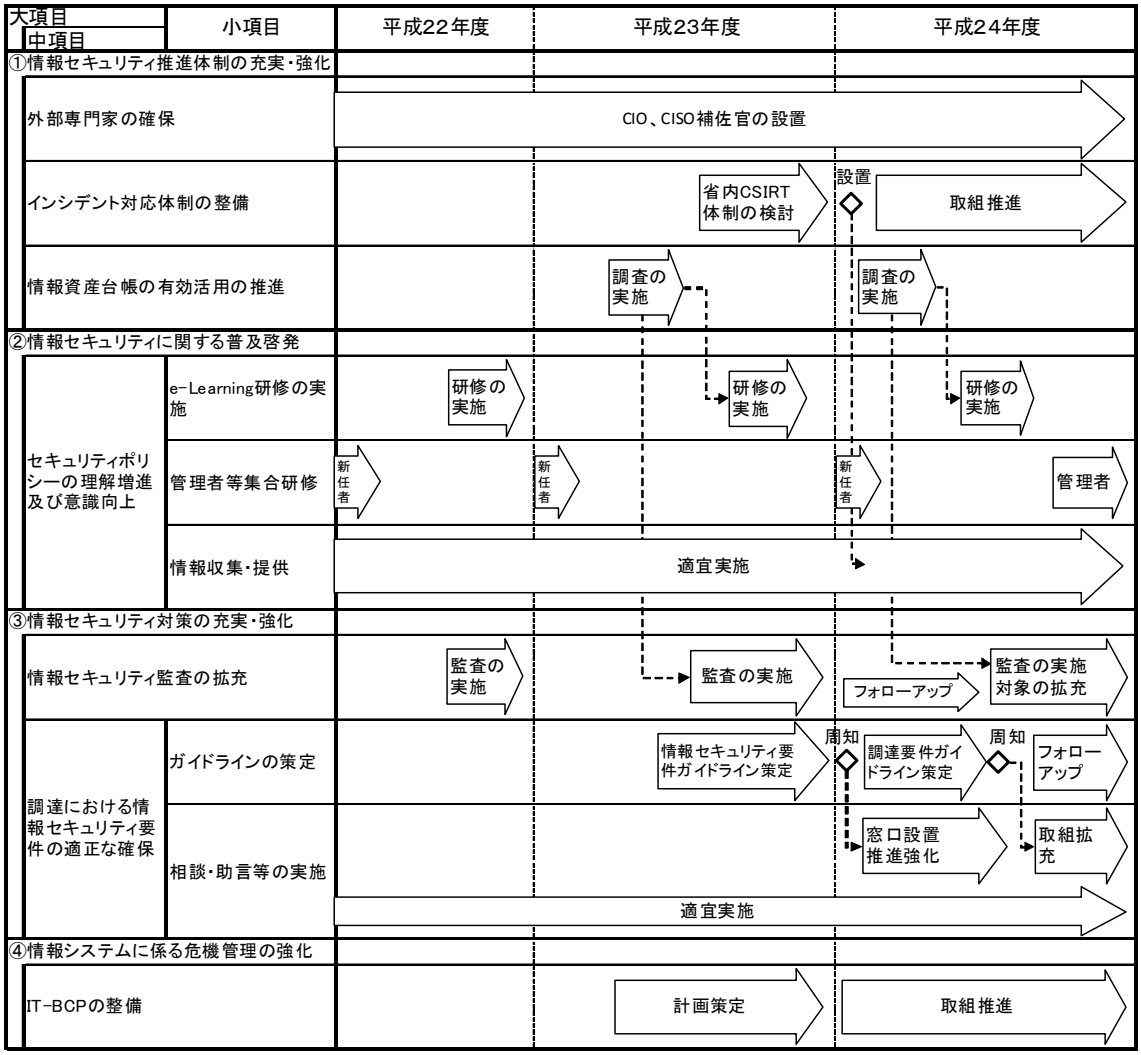


図 2 情報セキュリティに関する中期的な取組スケジュール

①　情報セキュリティ対策の推進体制の充実・強化

（ア）　専門家の確保

従来に引き続き、情報システム技術及び情報セキュリティに関する知見を有する専門家として、CIO 補佐官及び情報セキュリティアドバイザーを配置しました。CIO 補佐官及び情報セキュリティアドバイザーからの支援、助言等により情報セキュリティ対策の強化を図ります。

（イ）　インシデント対応体制の整備

インシデント対応体制を強化すべく、平成 23 年度は、省内 CSIRT（※）の整備に関する検討を進め、平成 24 年度には同体制を整備する予定です。

※CSIRT（Computer Security Incident Response Team）

CSIRT とはインシデントに対応する組織のことで、インシデント発生時は、報告、情報共有、緊急対応策の指示、原因分析等の迅速な対応、セキュリティ被害を最小限に抑えるための対応を行います。

（ウ）　情報資産台帳の有効活用の推進

毎年度、省内の情報システムの整備・運用状況の調査を行い、保有する情報システムに関する情報を把握し、緊急時における連絡体制の整備やソフトウェアにおける脆弱性に係る技術的支援等、収集した情報を有効に活用するため、情報資産台帳の整備を行っています。

平成 24 年度は、これまでの情報収集の精度や台帳の活用状況を踏まえて、調査様式の見直し等を行った上で、引続き情報資産台帳の整備に取り組みます。

②　情報セキュリティに関する普及啓発

（ア）　ポリシーの理解増進及び意識向上

ポリシーの理解増進及び意識向上のため、情報セキュリティに関する普及啓発を行います。

当省では全職員が情報セキュリティ教育を受講できるよう、e-Leaning 研修を実施しています。e-Learning 研修については、ポリシーの改定及び職員に対する情報セキュリティ対策の実施状況に係る自己点検（以下「自己点検」という。）の実施結果等を踏まえ、毎年度、研修内容の拡充・見直しを行います。また、平成 24 年度には、新たに情報システムの管理者向けの研修内容を整備し、同研修を実施する予定です。

情報セキュリティに関する情報収集及び職員向けの情報提供については、情報収集のための様式の制定及び周知、省内掲示板への情報表示に加え、各職員端末へのポップアップ表示等、職員が確実に情報を参照できる仕組みについても検討し、行い、さらなる情報セキュリティに関する普及啓発を行う予定です。

③　情報セキュリティ対策の充実・強化

（ア）　情報セキュリティ監査の拡充

毎年継続し実施している情報セキュリティ監査については、監査対象を拡充します。また、平成 24 年度には、監査後のフォローアップを充実させ、監査指摘事項に対する対応状況を確認する取り組みを強化します。

（イ）　調達における情報セキュリティ要件の適正な確保

情報セキュリティレベルを向上するため、調達仕様書の記載事項の標準化を行います。具体的には、平成 23 年度において「情報セキュリティ要件ガイドライン」を策定し、平成 24 年度には、情報セキュリティ要件以外を含めた「調達要件ガイドライン」を策定する予定です。

併せて、各調達課室における、それらの施策の浸透策として、従来からの情報システムの調達に関する相談の受付及び助言等の実施を拡充し、平成 24 年度には、それらの窓口担当者の設置等を行います。

④　情報システムに係る危機管理の強化

（ア）　IT-BCP（※）の取組

首都直下型地震等の不測の事態に備え、業務継続計画を策定しています。この中では、首都直下型地震における非常時優先業務を定め、業務の継続及び早期再開のための方法を示していますが、この非常時優先業務を継続するためには、情報システムの運用継続が不可欠となっています。また、首都直下型地震以外にも、日常的に起こりうる可能性の高いウィルス感染などを原因とする予期せぬシステム停止に備えることも重要です。そこで、安定的な業務遂行を目的に、情報システム運用継続計画を策定し、非常時の運用手順を周知します。

※IT-BCP（Information Technology - Business Continuity Plan）

安定的な業務遂行のために取り決めた情報技術に関する管理運営方針のことをいう。

３． 平成 23 年度の重点事項

平成 22 年度の情報セキュリティ対策の結果を踏まえ、以下の 2 点を重点事項として設定しました。

■ 情報の適切な管理を目指し、情報の格付や取扱制限の設定、明示を徹底するための教育・啓発を行う。

- 情報セキュリティ研修（e-Learning）の拡充
  - 研修コースの細分化
  - 研修コンテンツの大幅見直し
  - 理解度テストの強化・充実

- 情報の格付及び取扱制限に関する実務上の作業負担の軽減
  - ワープロソフトやメールソフトへの情報の格付及び取扱制限に関する自動表示機能の実装

■ 情報セキュリティ関係規程の体系の見直し、規程類の改定及び省内への周知を行う。

- 「行政情報システム利用手順書」及び「行政情報システム管理手順書」の改定
  - ポリシー改定に伴う上記手順書の改定及び周知

- 「情報セキュリティ要件ガイドライン」の作成
  - 外部委託を行う際に適切な情報セキュリティ要件を策定するためのガイドラインの作成

- 「情報システム管理手順書策定手引書」の作成
  - 各事業担当課室において所管する情報システムの管理手順書をポリシーに基づき適切に策定するための手引書の作成

４．　平成 23 年度における情報セキュリティ対策の取組

情報セキュリティ対策の周知徹底及び評価・見直しを図るため以下の取組を実施しました。

（１）　情報セキュリティ推進体制の充実・強化

①　専門家の確保

平成 22 年度までは、外部専門家からの支援及び助言を任務とした CIO 補佐官及び情報セキュリティアドバイザーについては、1 名による兼務となっていましたが、平成 23 年度からは、各々1 名を確保し、専門家を 1 名から 2 名の体制に強化しました。

②　インシデント対応体制の整備

（ア）　省内CSIRT体制の検討

大臣官房政策課情報化推進室内に整備する計画（平成 24 年度）となっている省内 CSIRT の体制の検討を進めました。

（イ）　GSOC(※)体制の充実・強化

緊急時における連絡体制や緊急時対応能力を向上させるため、GSOC 担当窓口を３名から５名に増員し、体制の強化を図りました。

※GSOC（Government Security Operation Coordination team）

内閣官房情報セキュリティセンターが主体となり、政府機関情報システムの 24 時間監視を行っている「政府横断的な情報収集・分析システム」のことをいう。

③　情報資産台帳の有効活用の促進

当省が管理･運用する情報システムについて、省内担当課室に対して一斉調査を行い、平成 22 年度に整備した情報資産台帳を更新し、情報セキュリティ面では緊急時における連絡体制の把握・セキュリティ脆弱性情報の提供等に活用しました。

④　外部委託先の適正な管理

情報システムの開発等の業務を外部委託する際には、調達仕様書に委託先に求める情報セキュリティ要件や遵守事項等を記載し、業務開始時にはプロジェクト計画書等により実施内容を具体化させ、委託先や納品物における適正な情報セキュリティ水準の確保に努めています。

また、委託先における情報セキュリティ対策の履行状況について、委託先からの定期的な報告や委託先への監査等により、問題点がないか確認するとともに、必要があれば改善を指導しています。

（２）　情報セキュリティに関する普及啓発

①　ポリシーの理解増進及び意識向上

（ア）　情報セキュリティ関係規程の見直し

ポリシーと運用の差を解消すること、及びポリシーをより理解しやすい内容とすることなどを目的として、行政情報システム利用手順書及び行政情報システム管理手順書の見直し作業を行い、平成 23 年 12 月 15 日に改定し、職員に周知しました。

（イ）　e-Learning研修の実施

ｱ）教育計画の策定、教育の企画等

全職員を対象とし、職員の役割、平成 22 年度の実施評価及びポリシーの改定を踏まえた教育実施計画を策定しました。

ｲ）対象者の役割に応じた教育教材の整備

職員にポリシーをより理解させることに重点を置き、ポリシーの内容を実業務と関連付けて学習できる e-Learning 用教材として改定・整備しました。

整備にあたっては、職員をポリシーで規定する各役割に応じ全ての職員を対象とする「行政事務従事者コース」、情報システム責任者、情報システム管理者を対象とする「情報システム責任者・情報システム管理者コース」、情報セキュリティ責任者、課室情報セキュリティ責任者を対象とする「情報セキュリティ責任者・課室情報セキュリティ責任者コース」の 3 つのコースとしました。

また、職員のポリシーへの理解度を深める方策として、平成 22 年度と比較しテストの設問数を増やすとともに、その難易度を高めました。

ｳ）教育の実施

e-Learning システムを活用した情報セキュリティ教育を実施しました。実施期間は、11 月 1 日からおおむね 3 ヶ月間を集中的に取り組む期間として設定し、97%の職員が受講を完了しました。

ｴ）教育受講状況の管理

e-Learning システムを利用することにより、迅速な受講状況の把握が可能となり、未受講者に対する督促を行うなど適正な受講者管理を行いました。

②　その他研修の実施

新規採用者については、平成 22 年度に引き続き、毎年 4 月に実施される新規採用者等研修において、情報セキュリティに関する研修を実施し、ポリシーや情報システムの利用に係る留意事項について説明を行いました。

また、総務省が主催する情報システム統一研修に参加することにより、職員の知識向上を図りました。

なお、これら 2 つの研修に、約 300 名弱の職員が参加しました。

③　職員に対する情報提供

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。）又は情報システム管理運用委託業者等から提供される脆弱性情報、ウィルス情報、不審メール情報等を省内電子掲示板に掲載し、重要性又は緊急性の高い情報については適宜全職員向けにメールで注意喚起を行いました。

また、ポリシー及び情報セキュリティ関係規程の遵守を促進する方策として、それらの規程類を参照しやすくするために、省内電子掲示板への掲載方法を見直しました。

さらに、省内電子掲示板に、不正アクセス等の事象が発生した際の報告様式を掲載し、その運用を開始し、問題事象の発生についての迅速な情報収集及び十分な情報共有を図るようにしました。

表 1 省内注意喚起件数

情報提供	件数
全職員メール周知	5 件
不審メール情報	177 件
電子掲示板注意喚起	60 件

（３）　情報セキュリティ対策の充実・強化

①　調達時における情報セキュリティ要件の適正な確保

（ア）　情報セキュリティ要件ガイドラインの作成

省内職員が情報システムのライフサイクルを通じ、要件定義、設計・開発、運用の各段階における調達において、適切なセキュリティ要件を策定するためのガイドラインを作成しました。

情報セキュリティ要件ガイドラインについては、別添の資料として、要件定義業務の調達、設計・開発・構築の調達、運用・保守の調達の 3 つの仕様書のひな型、及びその解説を用意し、調達する情報システムの実態に応じて要件を修正できるようにしています。また、設計・開発・構築時の調達仕様書のひな型については、「情報セキュリティを企画・設計段階から確保するための方策（SBD: Security By Design）に係る検討会」（座長：山岡克式・東京工業大学大学院理工学研究科准教授）において、平成 23 年 3 月 30 日に取りまとめられた「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（※）の活用も踏まえた形で仕様書が作成できるようにしています。

※ 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル

政府機関における情報システムの調達仕様書に記載する「セキュリティ要件」の策定方法を解説することによって、調達側である政府職員が、情報システムの企画段階からセキュリティ対策を適切に組み込むことを目的として作成されたマニュアルのことをいう。

（イ）　情報システム管理手順書策定手引書の作成

各事業担当課室において所管する情報システムの運用に当たり、情報システム責任者及び情報システム管理者がポリシーに基づき実施すべき事項を管理手順書として策定するための手引書を作成しました。情報システム管理手順書管理手順書についても、別添の資料として、管理手順書のひな型、及びひな型に対する解説を用意し、解説を参照しながら、運用する情報システムの実態に応じて管理手順書の要件を修正できるようにしています。

（ウ）　相談・助言等の実施

調達仕様書を作成する省内各課の担当者から寄せられる質問や相談等の問い合わせに CIO 補佐官や情報セキュリティアドバイザー等が随時対応し、必要な情報セキュリティが確保されるように努めました。

表 2　相談件数

相談種類	件数
仕様書レビュー	18 件

②　情報の格付・取扱制限の自動表示

省内で作成・使用されるほとんどの文書（メールや磁器媒体に記録されたものを含む。）には、情報の格付（※）・取扱制限（※）を表示するルールになっています。これは、その情報を取扱う者が、的確に情報セキュリティ対策を遵守するための基本的な取り組みです。

しかしながら、その取り組みの実施状況が、必ずしも 100%であるとはいえないこと、情報の格付等を記載する手間の問題も鑑み、より適正かつ効率的な取り組みの実施のため、情報の格付等を自動的に表示する対応を行いました。具体的には、Microsoft Word、Excel、PowerPoint 及び一太郎の文書作成時のヘッダーや Notes 上のメールの新規、返信、転送メールの作成時に、情報の格付の雛型（【機密性○情報（取扱制限）】）が自動表示されるようにしました。

これにより、情報の格付や取扱い制限の明示の適正化を図りましたが、導入して日も浅くその効果が現れていないことから、今後は対策の必要性を継続的に周知・徹底していくことが必要であると考えられます。

※情報の格付

情報の機密性の度合いを示すもので、「機密性１情報」、「機密性２情報」のように表示する。

※取扱制限

その情報を取扱うことのできる組織や人の範囲を示すもので、「課内限り」のように表示する。

③　フリーメールと不審メール情報の照合による注意喚起

ウィルスへの感染やそれに伴う情報漏えいなど防止するために、受信したフリーメールの情報と GSOC から提供される不審メールの情報を Notes 上で自動的に照合し、酷似するものについては職員に対し警告メッセージを表示し、開封前の注意喚起を行う仕組みを導入しました。

④　情報セキュリティ対策の実施状況の自己点検

（ア）　内容及び手法

自己点検は、ポリシーの各遵守事項について、全ての職員自らが実施状況を確認し、自己評価を行うものです。

実施にあたり、自己点検対象者の利便性の向上及び集計の効率化を図るため教育と同様に e-Learning システムを活用しました。また、外部監査を実施することにより、その適正性を確保しています。

自己点検の結果は、職員の各役割に応じ、以下の区分ごとに把握しました。

ｱ）責任者等

情報セキュリティ最高責任者、情報セキュリティ対策委員会、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

ｲ）システム担当

情報システム責任者、情報システム管理者

ｳ）行政事務従事者

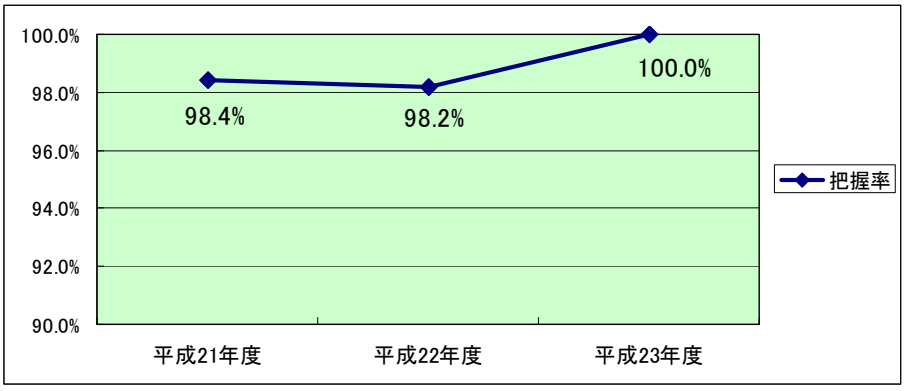
全ての職員

（イ）　自己点検結果の状況

ｱ）把握率

平成 23 年度の自己点検対象者のうち、自己点検を実施した者の割合である把握率は、100%を達成しました。

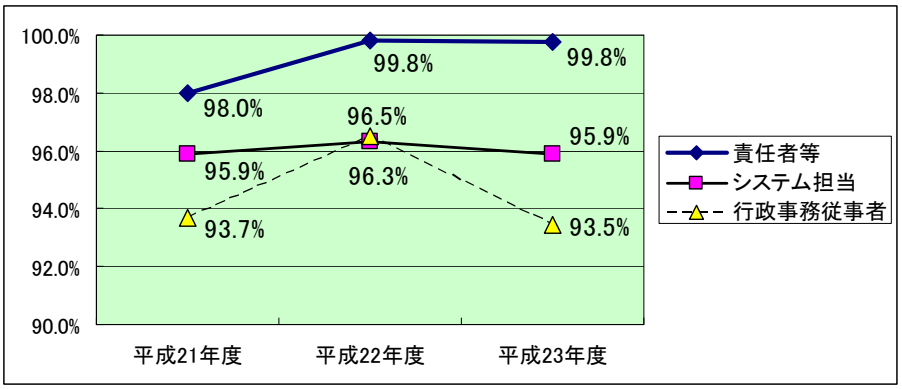
図 3 自己点検の把握率



ｲ）実施率

自己点検を実施した者のうち、点検項目にかかる対策を実施した者の割合である実施率の主体別の状況は、平成 22 年度とほぼ同水準になっています。

図 4 主体別実施率



⑤　情報システムの重点検査

（ア）　内容及び手法

情報システムの重点検査は、統一管理基準及び統一技術基準の遵守事項について、各府省庁の具体的な対策実施状況を確認するために、NISC が実施する調査であり、政府全体として PDCA サイクルの定着と浸透を確実なものとすることを目的として毎年実施されるものです。平成 23 年度の調査は、NISC が作成及び配布する調査票に基づき、公開ウェブサーバ、電子メールサーバに対して行なわれました。

調査結果は、統一管理基準及び統一技術基準における各遵守事項の実施率によって以下の評価基準に基づき評価され、NISC が公開ウェブサーバ、電子メールサーバの各々に対する評価結果（A、B、C、D）を各府省庁に通知しています。

表 3 重点検査の評価基準

評価	実施率
A	X=100%
B	80%≦X＜100%
C	60%≦X＜80%
D	X＜60%

（イ）　情報システムの対策状況

ｱ）公開ウェブサーバ

全ての公開ウェブサーバの OS のアップデート状況、アプリケーションのアップデート状況、HTTPS 通信の脆弱性対策、サービス不能攻撃対策の実施率は、99%（評

価：B）です。なお、未実施の対策については、平成 24 年 5 月に実施し、実施率 100%になる予定です。

ｲ）電子メールサーバ

全ての電子メールサーバの OS のアップデート状況、アプリケーションのアップデート状況の実施率は、平成 22 年度に引き続き、全て 100%（評価：A）です。

⑥　送信ドメイン認証の取組み

なりすましメールが顕著になっていることから、その防止策として、当省で所管している 15 のドメインについて、送信ドメイン認証技術を導入し、送信側の SPF（※）の公開設定を行いました。SPF 設定率は 100%となっています。

※SPF（Sender Policy Framework）

電子メールにおける送信ドメイン認証のひとつ。差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる。

⑦　情報セキュリティ監査の拡充

毎年度、継続して実施している情報セキュリティ監査について、対象システムを平成 22 年度の 6 システムから 8 システムに拡充し、情報セキュリティ監査の実施方法の強化を図りました。また、監査結果に基づく指摘事項については、対象システム毎の個別に対応状況の確認を継続的に行いました。

（ア）　情報セキュリティ監査の概要

統一管理基準及び統一技術基準並びにポリシーに基づき、情報セキュリティ監査責任者が情報セキュリティ監査計画書を作成し、実施しています。実施にあたっては、監査の独立性及び客観性を担保するため、外部の監査事業者に委託しています。

（イ）　情報セキュリティ監査の内容

ｱ）ポリシーに関する統一管理基準及び統一技術基準への準拠性監査

ポリシーが統一管理基準及び統一技術基準に準拠した内容となっていることを確認するための監査です。

ｲ）情報セキュリティ関係規程に関するポリシーへの準拠性監査

情報システムの利用手順書や管理手順書の情報セキュリティ関係規程がポリシーに準拠した内容となっていることを確認するための監査です。

ｳ）運用の準拠性監査

実際の運用がポリシー及び情報セキュリティ関係規程に準拠していることを確

認するための監査です。

ｴ）自己点検の適正性監査

自己点検の内容及び結果が妥当かつ適正であることを確認するための監査です。

ｵ）情報システムの技術的脆弱性診断

個別の情報システムの情報セキュリティ対策のうち脆弱性に対する技術的対策が妥当であることを確認するための監査です。

（ウ）　監査結果の総括

監査の結果、以下のとおり情報システムの技術的脆弱性診断において改善を要する事項が発見されたため、情報システムの責任者及び管理者による脆弱性に対する修正プログラムの適用等、改善への取組みが必要となりました。

その他のポリシー等関係規程類の準拠性や、運用の準拠性、自己点検の適正性においては、おおむね問題がないことを確認することができました。

ｱ）ポリシーに関する統一管理基準及び統一技術基準への準拠性監査

ポリシーは、統一管理基準及び統一技術基準の内容を継承し、統一管理基準及び統一技術基準に準拠した文書であることが確認されました。

ｲ）情報セキュリティ関係規程に関するポリシーへの準拠性監査

行政情報システム利用手順書及び行政情報システム管理手順書は、平成 22 年度の情報セキュリティ監査において、対象範囲と対象者が不明確であるため、当該手順書を読む者に混乱を招く事項があると指摘されていましたが、平成 23 年度の改定により当該指摘事項は改善され、また、ポリシーにも準拠していることが確認されました。

ｳ）運用の準拠性監査

情報の格付・取扱制限の明示に係る遵守事項を除き、おおむねポリシー及び情報セキュリティ関係規程に準拠した運用が行われていることが確認されました。

なお、情報の格付・取扱制限の明示に係る遵守事項については、自己点検において実施していないと回答した職員に追加ヒアリングを実施したところ、情報の格付・取扱制限の明示については認識しているものの、その目的や、情報の作成時及び入手時に決定する格付の判断基準を十分に理解していないことがわかりました。

ｴ）自己点検の適正性監査

自己点検実施者の中からサンプリング抽出により、質問対象者、質問項目、実施方法の妥当性について、それぞれ確認した結果、実施された情報セキュリティ対策の自己点検は適正であったことが確認されました。

オ）情報システムの技術的脆弱性診断

脆弱性に対する修正プログラムを一部適用していないことなどの原因により、情報の漏えいや、改ざんに繋がる脆弱性・システムやサービス停止等の業務の中断に繋がる脆弱性が、複数発見されたため、各監査対象システムの担当者に中間報告を行い、その対応を依頼しました。その後、脆弱性の残存の有無を確認するため、同様の技術的脆弱性診断を行い、ほとんどの脆弱性が適正に対応されていることを確認しました。

（４） 情報システムに係る危機管理の強化

① IT-BCPの取組

文部科学省首都直下地震対応業務継続計画で定めた非常時優先業務を継続する、又は日常的に起こりうる可能性の高いウィルス感染などを原因とする予期せぬシステム停止に備えるために、行政情報システム、メールシステム、ホームページの運用に関する運用継続計画の基本方針、非常時の対応計画、事前対策の策定・計画及び訓練・維持管理計画をとりまとめました。

５． 情報セキュリティに関する障害・事故等報告

平成 23 年 12 月 19 日（月曜日）、「科学技術週間」ウェブサイト（http://stw.mext.go.jp）の一部が改ざんされているとの連絡を利用者より受け、事故の状況を調査した結果、個人情報の流失が判明しました。

同日 15 時 30 分頃から、同ウェブサイトのサーバを停止し、原因の究明を開始したところ、システムの一部に脆弱性があることが判明したため、問題のプログラムを修正し、脆弱性への耐性を強化のうえ、平成 24 年 1 月 19 日に同ウェブサイトを再開しました。

また、ウェブサイト全体に第三者機関によるセキュリティチェックを実施し、問題がないことを確認しました。

詳細については、「科学技術週間ウェブサイトの不正アクセスについて」ウェブサイト（http://www.mext.go.jp/b_menu/houdou/23/12/1314690.htm）をご覧ください。

６． 情報セキュリティ対策に関する平成 23 年度の総括

（１） 総括

平成 23 年度は第 3 章に示した重点項目を中心に取り組んできました。その結果、情報セキュリティの向上に向けて、制度上、管理体制上の整備が進みました。また、自己点検の分析結果からは、職員のセキュリティ意識も引き続き高水準が保たれていると考えられます。また、これらから省内のシステムの運用については、一定のセキュリティ水準が確保できていると思われます。

しかし、残念ながら、一方で、省外に置かれたウェブサイトで 1 件のセキュリティ・インシデントが発生しました。

当省では外部委託事業の成果を広く一般に公開するため、事業委託先に情報公開サイトの構築・運営をも委託する事例があります。今後はこのようなサイトについても、省内と同等のセキュリティ水準を確保するよう、これまで以上に管理体制を強化していく必要があります。

また、今回のインシデント対応では貴重な経験が得られました。この経験は平成 24 年度以降の CSIRT 活動に生かしていきます。

なお、外部の事業者による情報セキュリティ監査では、監査対象システムのいくつかで、数点の脆弱性が指摘されました。これらのうち重要度又は緊急度の高いものについては既に対策が講じられておりますが、前述のインシデント発生も踏まえて、引き続き監査体制を強化していきます。

（２） 課題

平成23年度の取組結果を踏まえた、平成24年度に取り組むべき主な課題は、次のとおりです。

■ 自己点検の結果を踏まえた課題

⇒「情報セキュリティに関する普及啓発」の一環として取り組みます。

- 「情報の格付及び取扱制限」の必要性及び判断基準の周知
- 情報の作成・入手時における「情報の格付及び取扱制限」の決定及びその明示の徹底

■ 情報セキュリティに関する障害・事故等を踏まえた課題

⇒「情報セキュリティ対策の充実・強化」の一環として取り組みます。

- ウェブサイトにおける脆弱性プログラムの排除
- 調達時における情報セキュリティ要件の確保

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 年度においても引続き、各情報システムの重点検査、情報セキュリティ対策に関する自己点検、情報セキュリティ監査を実施し、情報セキュリティ対策の評価・見直しを行います。

すでに設定している中期的な取組の計画及び平成 23 年度の情報セキュリティ対策の結果を踏まえ、平成 24 年度に重点的に取り組む事項を以下のように設定します。

■ 情報セキュリティ推進体制の充実・強化

- 省内 CSIRT の具体的な体制の整備

■ 情報セキュリティに関する普及啓発

- ポリシーの理解増進及び意識向上
  - 管理者等集合研修の実施
- 情報セキュリティ維持に関する訓練
  - 標的型不審メールへの対処に関する訓練の実施
- 自己点検の結果を踏まえた取り組み事項【平成 23 年度の課題に伴うもの】
  - 「情報の格付及び取扱制限」の必要性及び判断基準の周知
  - 情報の作成・入手時における「情報の格付及び取扱制限」の決定及びその明示の徹底

■ 情報セキュリティ対策の充実・強化

- 調達仕様書の記載レベルの標準化
  - 調達要件ガイドラインの策定及び周知
  - 調達仕様書に関する相談窓口の設置及び同窓口の利用促進のための周知
- 情報セキュリティに関する障害・事故等を踏まえた取り組み【平成 23 年度の課題に伴うもの】
  - ウェブサイトにおける脆弱性プログラムの排除

■ 情報システムに係る危機管理の強化

- IT-BCP の整備
  - 平成 23 年度の計画策定をもとにした具体的な取組の推進

８． おわりに　～情報セキュリティアドバイザーからのメッセージ～

文部科学省では、この報告書に示した情報セキュリティ対策を、着実にかつ計画的に実施してきました。この結果、職員の情報セキュリティに関する意識の維持向上が図られ、省内の情報セキュリティも一定の水準を保っていると考えています。これは、外部監査機関により実施された情報セキュリティ監査の結果からも見てとれます。

しかし、一方で、省外に設置され、運営を外部に委託している情報公開ウェブシステムの一つで、その脆弱性に起因するセキュリティ・インシデントが発生しました。今後は、この経験を踏まえ、各種対策の省外への横展開にも取り組むことが必要です。

この報告書本文では触れられていませんが、来年度には本省の IT システムの更改が予定されています。更改案には経費削減策や利便性向上策の他、いくつかの情報セキュリティ強化策が盛り込まれています。これにより、業務効率の改善と同時に、情報セキュリティの一層の向上が実現できるものと確信しています。

情報セキュリティ対策は、一朝一夕に出来るものではありません。また、完璧な対策は存在しません。情報セキュリティ責任部門だけでなく、職員全員の継続的な活動が不可欠です。本省では、NISC など政府内外の関連部門と密接に連携を取りながら、情報セキュリティに関する各種情報や技術動向を注視しつつ、この報告書に示された計画・施策を着実に推進してまいります。

情報セキュリティアドバイザー
（文部科学省 CIO 補佐官）
岩崎　進

９．　【参考】本報告の基本情報

（１）　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 年間です。

（２）　対象とする組織

本報告書が対象とする組織は、文部科学省です（文部科学省とは、本省内部部局及び水戸原子力事務所並びに文化庁のことをいう）。

（３）　対象とする組織の所掌事務

文部科学省は、教育の振興及び生涯学習の推進を中核とした豊かな人間性を備えた創造的な人材の育成、学術、スポーツ及び文化の振興並びに科学技術の総合的な振興を図るとともに、宗教に関する行政事務を適切に行うことを任務とし、文部科学省設置法（平成 11 年 7 月 16 日法律第 96 号）第 4 条に掲げる事務を所掌します。

（４）　対象とする情報

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）　責任部署

文部科学省大臣官房政策課情報化推進室