平成 24 年度
情報セキュリティ報告書

平成 25 年 6 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～

文部科学省（以下「当省」という。）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います。

近年、我が国では、情報通信技術の急速な進歩に伴い、国民生活が飛躍的に向上する一方で、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、サイバー攻撃の手口もより巧妙化してきております。平成 24 年度においては、中央省庁や裁判所等を標的としたサイバー攻撃により、ウェブサイトの書き換えや情報漏洩等の被害が相次ぎ発生し、社会問題となったのは記憶に新しいところです。

このような状況において、昨年 9 月には、外局である文化庁のシステムがサイバー攻撃を受け、ウェブサイトの一部改ざんが発生し、一時当該サイトを閉鎖する事態となりました。このことによって、ご利用者の方々に、大変な御迷惑や御心配をお掛けしましたことを心よりおわび申し上げます。

当省では、かねてから文部科学省情報セキュリティポリシーを制定し、その運用を通じて情報セキュリティ対策を徹底してきたところでありますが、このことを受けて、以下の点を中心に情報セキュリティ対策のより一層の強化に取り組んでまいりました。

(1)　情報セキュリティ事案に対応する専門チーム（CSIRT）整備による体制強化
(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)　調達ガイドラインの策定等による情報セキュリティ対策の充実・強化
(4)　IT-BCP の整備による情報システム危機管理の強化

本報告書は、これらのことを踏まえ、平成 24 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。

平成２５年６月１１日
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、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 5 種類の実施手順書を整備しています。

- 情報システムに係る調達ガイドライン
- 情報システム管理手順書策定手引書
- CSIRT 運用手順
- 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下、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　区域情報セキュリティ責任者

区域（執務室、会議室、サーバ室等）ごとの情報セキュリティ対策に関する事務を統括します。

⑩　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。

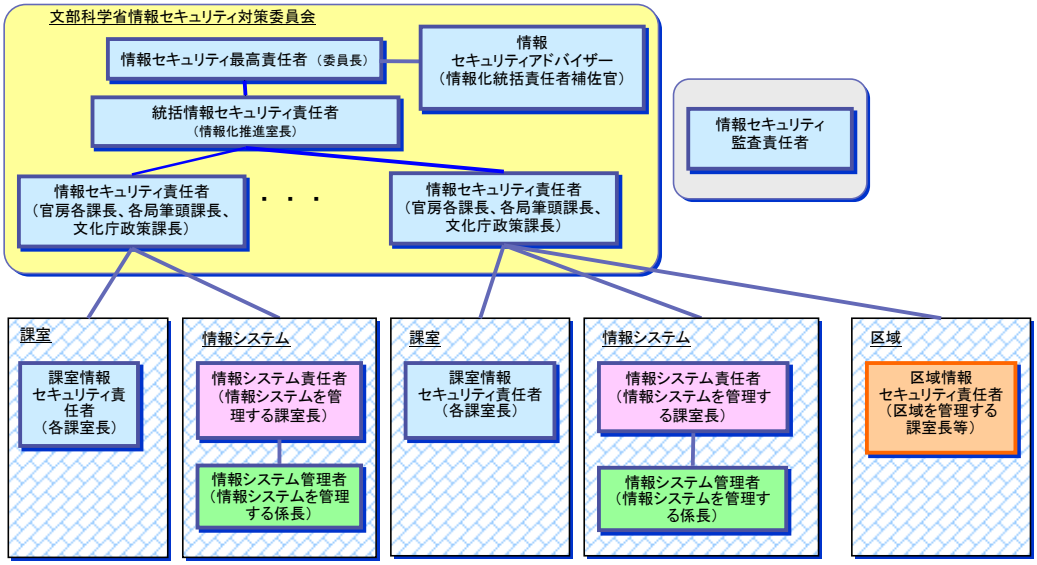

図 1 情報セキュリティ対策の推進体制

⑪　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、主な業務は以下のとおりです。

- 省内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。
- 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．　平成 24 年度の重点的な目標

平成 23 年度の情報セキュリティ対策の結果等を踏まえ、平成 24 年度の重点的な目標を以下のとおり設定しました。

（1）情報セキュリティ推進体制の充実・強化

- 省内 CSIRT の体制を整備する。

（2）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
  - 管理者等を対象とした集合研修を実施する
- 情報セキュリティ維持に関する訓練
  - 標的型攻撃メール訓練を実施する
- 自己点検の結果を踏まえた取組事項
  - 「情報の格付及び取扱制限」の判断基準を整備し、周知する
  - 情報の作成・入手時における「情報の格付及び取扱制限」の決定及び明示の実践を徹底する

（3）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を策定し周知する
  - 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組
  - ウェブサイトにおけるぜい弱性の排除

（4）情報システムに係る危機管理の強化

- IT-BCP の整備
  - 平成 23 年度に策定した計画に基づく具体的な取組の推進

４． 平成 24 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 インシデント対応体制の整備

平成 24 年 11 月、「CSIRT 運用手順」を定め、大臣官房政策課情報化推進室内に省内 CSIRT 体制を整備しました。省内 CSIRT 体制は、情報セキュリティインシデントが発生した際にポリシーに基づき被害を最小化するとともに迅速な復旧支援等を行うことが役割です。

平成 24 年 9 月以降、以下の事案について情報を収集し、関係機関への注意喚起と情報提供、早急に実施すべき対策についての依頼等を行い、対応の迅速化、効率化に努めました。

- 尖閣諸島関係と思われる本府省庁、独立行政法人等へのサイバー攻撃（平成 24 年 9 月）

注:上記は､省内 CSIRT 体制が正式に発足する前の準備段階における対応でした。

② 専門家の継続的な配置とプロジェクト・マネジメント・オフィス（以下、「PMO」という。）体制の拡充

平成 24 年度も継続して外部専門家による CIO 補佐官及び情報セキュリティアドバイザー各 1 名ずつの 2 名体制を確保しました。

また、当省では、「IT 新改革戦略」（平成 18 年 1 月 19 日 IT 戦略本部決定）に基づき､省内における情報化促進を担う PMO の役割を大臣官房政策課情報化推進室が担っています。PMO は、省内の情報化を適正に推進するため、他部局へのより積極的な関与と調整が求められます。よって PMO の体制を補強するため、PMO 業務の支援を外部委託しました。

③ 情報資産台帳の適正な維持

インシデント対応に備え、情報資産台帳の内容をメンテナンスし、今後も継続して活用できるよう、人事異動等により生じた担当者情報（連絡先等）の変更等を適切に更新・反映しました。

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。（後述「調達時における情報セキュリティ要件の適正

な確保」）

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

統一管理基準及び統一技術基準が改定されたことを受け、平成 24 年 11 月 5 日にポリシーを改定しました。これに伴い、新設された情報取扱区域及び区域情報セキュリティ責任者を把握するため、省内に照会を行い、取りまとめた結果を周知しました。

今回のポリシー改定では、「区域情報セキュリティ責任者」（執務室、会議室等の区域ごとの情報セキュリティ対策に関する事務を統括する）が新設されたため、関係する職員（各部署の庶務担当等）に対して、ポリシー改定の趣旨について事前に説明を行いました。（平成 24 年 9 月）

（イ）　情報システム管理者向け集合研修

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として「情報システムに係る調達ガイドライン」を、情報システムの運用に当たり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として「情報システム管理手順書策定手引書」を平成 24 年 6 月 25 日に策定し、ポリシーの改定に伴い、平成 24 年 11 月 28 日に改定しました。また、「情報システムに係る調達ガイドライン」の利用促進を目的として、各部署のシステム管理者等を対象に以下の集合研修を実施しました。

ｱ）情報システムに係る調達ガイドライン等説明会（5 月、12 月に各 2 回、計 4 回実施。延べ 28 名が参加）

ｲ）SBD マニュアル説明会（5 月、12 月に各 1 回、計 2 回実施。延べ 14 名が参加）

ｱ)については、ガイドライン改定のポイント、具体的な活用方法の解説のほか、情報化推進室によるフォローアップについて解説しました。

ｲ)については、調達仕様書におけるセキュリティ要件を導出するツールとして活用するため、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。）による紹介を行いました。

（ウ）　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 23 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。

整備に当たっては、ポリシーで規定する職員の各役割に応じて、以下の 5 コースを用意しました。

- 行政事務従事者コース（全職員が該当）
- 情報システム責任者コース
- 情報システム管理者コース
- 情報セキュリティ責任者コース
- 課室情報セキュリティ責任者コース

また、職員のポリシーへの理解度を深めるため、行政事務従事者コースにおいては、昨年度の自己点検の結果より、対策が不十分であった情報の格付及び取扱制限について、教育資料の充実を図り（後述「自己点検の結果を踏まえた取組事項」）、情報システム責任者コース及び情報システム管理者コースにおいては、標的型攻撃に関する内容を取り入れました。

ｳ) 教育の実施

全職員（延べ 2853 名）が e-Learning の受講（理解度確認テストを含む）を完了しました。

ｴ) 教育受講状況の管理

e-Learning システムの活用により、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等、対象者数が増加している中で、当省全体として、研修内容の習得についての適切な管理を行いました。

② 情報セキュリティ維持に関する訓練

標的型メール攻撃に関する教育・意識啓発のため、訓練用の標的型攻撃メールの受信体験を通じて、同攻撃への適切な対処を職員に身につけさせることを目的として、「平成 24 年度標的型メール攻撃に対する教育訓練」（NISC 主管）を実施しました。

（ア） 訓練の概要

職員に宛てて、「標的型攻撃」を模した訓練用メール（「ウイルス感染源ファイルに見立てたファイルを添付」又は「不正サイトに見立てた URL をメール本文に記述」）を送信しました。

訓練メールに添付されたファイルを開いたり、訓練メール本文中の URL をクリックしたりした職員には、注意を促す「教育コンテンツ」を表示しました。

（イ） 訓練の対象者

1 回目：176 部局 2,909 名の職員　2 回目：176 部局 2,838 名の職員

（ウ） 訓練結果（平成 24 年度　標的型メール訓練実施結果報告書より抜粋）

● 開封率（※）について

開封とは「訓練用の添付ファイルを開いた」若しくは「メールの本文に記載されている URL をクリックした」ことを指します。

開封率とは、言わば標的型メール攻撃が『成功』した率で、今回の訓練結果は次のとおりです。

1 回目：36.4%　　2 回目：21.0%

（※）開封率の計算式

開封率（%）＝｛開封者の数｝÷｛訓練対象者数｝×100

● アンケート調査結果より

「添付ファイルを開いた、又はリンクをクリックした理由」として「習慣で開封した」「不審な点はないと思った」が挙げられています。標的型メールは日常の業務（メールによるコミュニケーション）に紛れ込んでいるため、区別は難しいのですが、それゆえに用心深さが求められます。

また、「不審に思ったものの、業務に関係するメールだと思い、開いた」（つまり、不審なメールと認識したにもかかわらず開封した）という回答もありました。不審メールに気付いた場合は、習慣や自己判断で開封せず、必ず報告する必要があります。

一方、「不審メール」だと思った理由として、「差出人に心当たりがなかったこと」「宛名の書き方、件名・本文の内容を見て、自分に宛てられたものではないと判断できたこと」等が挙げられていました。

● 訓練メールへの返信について

今回の訓練メールに対して、「自動応答設定」により返信したケースのほか、訓練メールを「相手が宛先アドレスを間違えたため自分宛に届いた」と善意に解釈し、手動で「確認のための返信」をしたケースがありました。

もし本物の標的型攻撃メールであった場合、これに返信することにより、実在するメールアドレスや個人名、組織名等の詳細な情報を攻撃者に与えてしまう（すなわち、新しい標的型メールの材料となる）という危険性があります。

③ 自己点検の結果を踏まえた取組事項

平成 23 年度自己点検の結果、洗い出された課題について以下のように取り組みました。

（ア） 「情報の格付及び取扱制限」の必要性及び判断基準の周知

e-Learning 研修の学習教材の見直しを実施し、公開前情報の格付明示及び公開時の格付削除について追記する等、「情報の格付及び取扱制限」に関する記述

を充実させました。また、判断しやすくするための一律的な判断基準の策定については、文部科学省で取り扱っている情報が多種多様であるため、今後 NISC が主体となり政府全体で推進することとされているリスク評価に係る取組（※）の動向を踏まえた上で、継続して対応していきます。

（※）リスク評価に係る取組

標的型攻撃等の外部脅威から、重要な情報を保護するための対策を重点強化するため、平成 26 年度からの本格実施を目指して NISC が主体となって検討している取組です。この取組のプロセスにおいて、各府省庁は機微な業務領域及びその領域に対する脅威を特定しリスク評価をした上で、CISO（文部科学省では、情報セキュリティ最高責任者である大臣官房長）に評価結果並びに対策の実施状況及び今後必要となる対策等について報告し、その承認の下、必要なセキュリティ対策予算を重点投資することとなっています。

（イ） 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

ポリシーで定める情報セキュリティ責任者等で構成される筆頭課長等会議（平成 24 年８月開催）にて、自己点検の結果において「情報の格付及び取扱制限」に係る対策が不十分であったことを踏まえ、各課での取組として、機密性２以上の情報に対する格付及び取扱制限の明示徹底について、統括情報セキュリティ責任者である大臣官房政策課情報化推進室長より周知依頼しました。

④ その他研修の実施

（ア） 新規採用者向け研修

新規採用者については、平成 23 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、省内電子掲示板に e-Learning 研修の教育資料を掲載し、研修を受講できなかった年度途中の新規採用者等が e-Learning 研修システムにログインしなくても閲覧できるようにしました。

（イ） 情報セキュリティセミナー

2 月の情報セキュリティ月間に併せて、文部科学省関係機関の情報セキュリティ対策担当者等を対象とした情報セキュリティセミナーを開催し、情報セキュリティ意識の向上に努めました。

本セミナーでは、昨今のインシデント発生の状況に鑑み、「ウェブサイトのセキュリティ強化とインシデント対応」を主要テーマとし、サイバー攻撃事案の傾向やウェブサイトに必要なセキュリティ対策等に関する講演を行いました。

セミナーには 344 名が参加し、アンケートでは、70%～90%の受講者が「参

考になった」と回答しました。

⑤　職員に対する情報提供

NISC 又は情報システム管理運用委託業者等から提供されるぜい弱性情報、ウイルス情報、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。

表 1 省内注意喚起件数

情報提供	件数
ウイルス及び不審メール情報	439 件
ぜい弱性等情報	53 件 （内、メールによる周知は 4 件）
サイバー攻撃に関する注意喚起	8 件
全職員向け注意喚起	2 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）　情報システムに係る調達ガイドラインの策定・周知

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策定し、省内に周知しました。

情報システムに係る調達ガイドラインについては、別添の資料として、要件定義の調達、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」（SBD 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。

平成 24 年度は、9 件の情報システムの調達案件について、情報セキュリティ要件を仕様書に組み込むために本調達ガイドラインが適用されました。

（※）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
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です。

（イ）　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合せに 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。

平成 24 年度は、11 件の仕様書レビューを行いました。

（ウ） 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。

② 情報セキュリティに関する障害・事故等を踏まえた取組

（ア） ウェブサイトにおけるぜい弱性の排除

公開ウェブサーバはセキュリティ事故の発生率が高いことと、情報システムに対するセキュリティの確保は、構築又は更新の調達時が重要であるため、公開ウェブサーバを含む情報システムを新規に構築又は更新する際、情報化推進室にて調達仕様書の内容を検証しました。

③ 情報システム基盤更新に伴う情報セキュリティ対策の強化

平成 24 年度においては、当省の LAN・グループウェア等の情報システム基盤の更新に伴い、証跡の収集・管理機能を強化するとともに、標的型攻撃による不正プログラムの侵入及び感染拡大を防止するため、各種セキュリティ対策の強化を図りました。

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。

実施に当たり、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、障害・事故等に対応する責任者、権

限管理を行う者

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

当省における全報告対象者のうち、実際に自己点検を行い、その結果を報告した者の割合を把握率と言います。

平成 24 年度の把握率は 100%です。過去 2 年間、報告対象者が増加している中で、平成 23 年度に引き続き、徹底した状況把握を行っています。

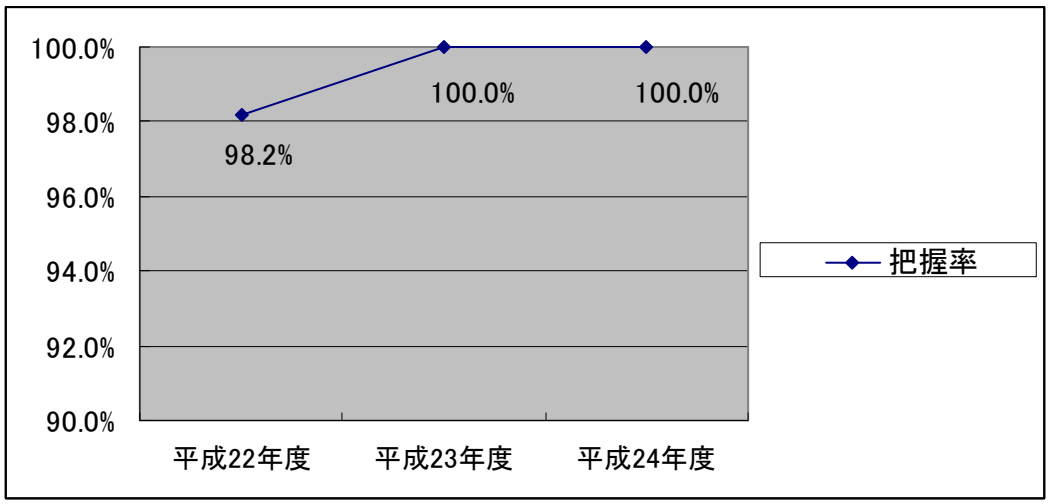

図 2 自己点検の把握率

ｲ) 実施率

各点検項目について、当該項目に係る情報セキュリティ対策を「実施できている」と自己評価した割合を実施率と言います。平成 24 年度における主体別（※）の実施率は、図 3 のとおりです。

年度によって変動はありますが、実施率はいずれの区分においても高い水準を維持しています。

実施率が 100%の項目についても、情報セキュリティ監査によりその妥当性を検証しています。

また、実施率が 100%に満たない部分については、状況に応じて適切な対策を講じていく必要があります。

このように自己点検により抽出された課題に取り組むことが、当省における「情報セキュリティの PDCA サイクル」の活性化につながります。

（※）主体別

責任者等：

統括情報セキュリティ責任者、情報セキュリティ責任者、
課室情報セキュリティ責任者等

システム担当：

情報システム責任者、情報システム管理者

行政事務従事者：

全職員（行政事務従事者）

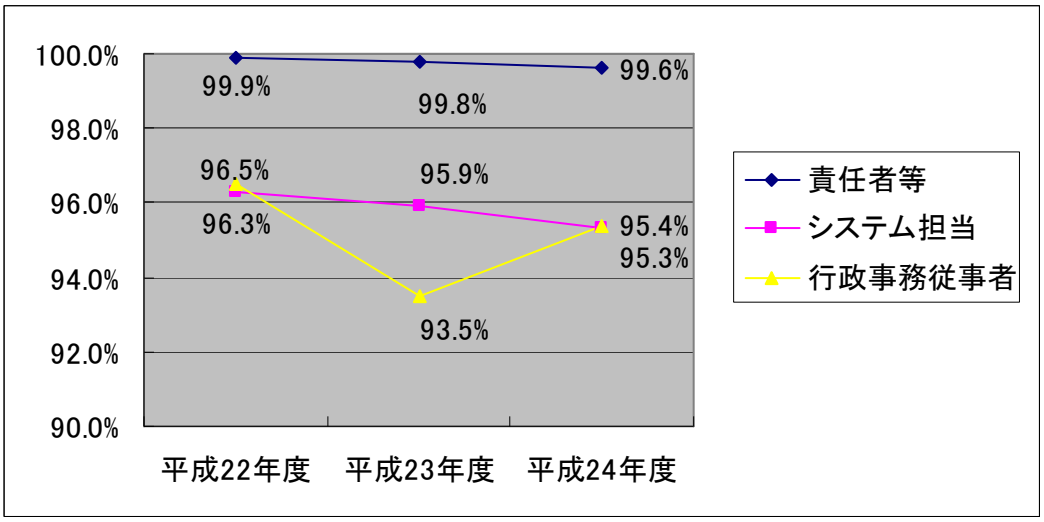

図 3 主体別実施率

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します。

平成 24 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、電子メール、ドメイン、DNS、ネットワーク等に対して行いました。

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 2 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

当省が管理する全ての公開ウェブサーバにおける、ぜい弱性検査、DoS 攻撃対策、サーバ OS のパッチ適用、ミドルウェア等のパッチ適用、ウェブアプリケーションにおける SQL インジェクション対策等の実施率は 95.1%（評価Ｂ）です。なお、未実施の対策については、平成 24 年 12 月に実施し、実施率は 100%になっています。

ｲ) 電子メールサーバ

当省が管理する全ての電子メールサーバにおけるサーバ OS のパッチ適用、電子メールサーバアプリケーションのパッチ適用等の対策の実施率は 100%（評価：A）です。

ｳ) ドメイン

当省が管理する全てのドメインについて、受信側における送信ドメイン認証技術の導入状況を NISC に報告しました。

ｴ) ネットワーク

当省がインターネットに接続して運用しているネットワークについて、システム構築時、システム運用過程において講じている標的型攻撃に対する出口対策の実施率は 100%（評価：A）です。

⑥ 情報セキュリティ監査

(ア) 情報セキュリティ監査の概要

情報セキュリティ監査は、当省における情報セキュリティ対策の状況を客観的に評価することにより、今後取り組むべき課題を明らかにします。

平成 24 年度の情報セキュリティ監査計画書は、ポリシーに基づき、情報セキュリティ監査責任者が作成しました。実施に当たっては、監査の独立性及び客観性を担保するため、また情報セキュリティに係る技術的専門性を担保するため、外部の専門事業者に委託しました。

(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ぜい弱性診断

個別の情報システムの情報セキュリティ対策のうちぜい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。

診断の結果洗い出されたぜい弱性について正しく対処されていることを確認するため、中間報告後、一定期間を経て再診断を行います。

（ウ） 監査結果の総括

ネットワーク、サーバ、ウェブアプリケーションに関するぜい弱性診断の結果、いくつかの改善すべき事項が発見され、それらについては、情報システムの責任者及び管理者による修正プログラムの適用等の改善対策を行い、再診断により正しく対処されていることを確認しました。

また、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も検出された課題については、原因を分析し改善への取組を行う予定です。

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

ポリシー全体としては、統一基準に準拠していると評価されましたが、一部、統一基準と整合していなかったり、ポリシーの内部で統一が取れていない点が指摘されました。これらの課題については、次回のポリシー改定時に対応する予定です。

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

「情報システムに係る調達ガイドライン」及び「情報システム管理手順書策定手引書」を対象として、これらがポリシーに準拠しているかについて監査しました。その結果、全体としてはおおむね整合していると評価されました。

しかし、両文書については、用語の一部が不統一である等、ポリシーと整合しない部分が指摘されました。これらについては、次回の調達ガイドライン改定時に対応する予定です。

ｳ）運用の準拠性監査

サンプリング調査により、職員へのアンケート調査を行い、自己点検結果との整合性を確認した結果、おおむねポリシーに準拠した運用がなされていることが確認されました。

しかし、「職員に機密性２の認識が不足している」という課題が検出されました。現状を放置すると、情報漏えい等の事故につながるリスクがあります。職員は、業務で取り扱う情報の機密性について正しく認識する必要があり、今後は、そのための施策を検討し、対応する予定です。

ｴ) 自己点検の適正性監査

自己点検の適正性をヒアリング及び資料閲覧により監査した結果、全体としてはおおむね適正であることが確認されました。

しかし、「自己点検結果を改善につなぐ仕組み、及び改善の報告を上げる仕組みがない」という課題が検出されました。

現状を放置すると、自己点検の効果が現れず、問題が解決されないというリスクがあります。今後は、現状を改善するための施策について検討し、対応する予定です。

ｵ) 情報システムの技術的ぜい弱性診断

当省が指定したネットワーク、サーバ、ウェブアプリケーションに対して、当省の内部及び外部からぜい弱性診断を実施した結果、複数のぜい弱性が発見されました。その結果については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、ぜい弱性の残存の有無を確認するため、再診断を行い、ほとんどのぜい弱性が適正に対応されていることを確認しました。また未対応のぜい弱性については、対応予定時期を確認しました。

（4）情報システムに係る危機管理の強化

① IT-BCP の取組

平成 23 年度に策定した IT-BCP に基づき、本計画の策定・運用及び非常時の体制について検討し、体制確立を進めました。

また、非常時のデータ消失を防ぐため、バックアップを取得し、データを復旧できるようにしました。

５． 情報セキュリティに関する障害・事故等報告

平成 24 年 9 月 24 日、文化庁の「国指定文化財等データベース」が改ざんされるという情報セキュリティ侵害事案が発生しました。文化庁では、改ざんを発見した直後に当該ウェブサイトの公開を停止し、被害状況の調査、原因究明と再発防止策

の検討を行いました。再発防止策を講じた上で平成 25 年 3 月 28 日にサービスを復旧しました。

経緯は以下のとおりです。

- 平成 24 年 9 月 24 日、文化庁の「国指定文化財等データベース」WEB サイトのトップページが改ざんされている（尖閣諸島（沖縄県）の魚釣島に中国国旗を合成した画像が貼り付けられている）ことが判明しました。
- 文化庁では、同 WEB サーバを管理・運営する会社に WEB サイトの公開停止を指示し、WEB サーバのログを解析しました。その結果、WEB サイトのセキュリティホール（弱点）を突いた、SQL インジェクションが原因であることが分かりました。
- 文化庁では、今回の事象の再発を防止するため、プログラムの修正を行い、システムの再構築を行った上、平成 25 年 3 月 28 日にサービスを復旧しました。

今後も同様のサイバー攻撃が繰り返される危険性が高いことから、NISC や他の府省とも協調し、再発防止のための有効な取組を継続します。

６． 情報セキュリティ対策に関する平成 24 年度の総括

（1）総括

平成24年度は第3章に示した重点項目を中心として情報セキュリティの向上策に取り組みました。前年度までの取組を継承し、省内CSIRTの整備等、管理体制の拡充、関連規程の整備と周知徹底、各種技術的対策の実装等を行うとともに、当省における情報セキュリティ対策の水準を把握し、今後の課題を明らかにするために自己点検、情報セキュリティ監査を行いました。

自己点検、情報セキュリティ監査の結果、当省においては一定の情報セキュリティレベルを確保できていると思われます。同時に、更なる向上のための課題を明らかにすることができました。

また、情報セキュリティ維持に関する訓練として標的型メール攻撃訓練を実施し、標的型メール攻撃に対する職員の意識啓発に一定の効果を上げることができました。

一方で、平成24年9月に、尖閣諸島関係と思われるサイバー攻撃が行われ、文化庁のウェブサイトが改ざんされるというセキュリティ事案が発生しました。この事案では「国指定文化財等データベース」を停止するに至りました。

このことを踏まえ、政府機関全体がサイバー攻撃の脅威にさらされているという認識の下、今回の事案への対処経験を活かし、ウェブサイトのぜい弱箇所の除去等の技術的対策、またNISCや他府省庁との情報共有によるサイバー攻撃の兆候の早期発見等により、再発防止策に注力します。

（2）課題

平成24年度の取組結果を踏まえた、平成25年度に取り組むべき主な課題は、次のとおりです。

① 自己点検、標的型メール攻撃訓練、情報セキュリティ監査の結果を踏まえた課題

自己点検及び自己点検に基づく監査の結果、「職員に機密性２の認識が不足していること」、「自己点検結果を改善につなぐ仕組み及び改善の報告が上がる仕組みがないこと」等の課題の存在が判明しました。

標的型メール訓練の実施及び事後のアンケートを分析した結果、不審メールに対する職員の対応に不十分な点があることが判明しました。

② 情報セキュリティに関する障害・事故等を踏まえた課題

当省に対し仕掛けられたサイバー攻撃からは、各情報システムには、未対応のぜい弱性が存在することが示唆されます。これらについては、技術的側面、運用的側面の両方からの対策が必要となります。

７． 情報セキュリティ対策に関する平成 25 年度の計画

平成 25 年度においても、引き続き自己点検、情報セキュリティ監査等を実施し、情報セキュリティ対策の評価と改善を行います。

また、平成 24 年度の情報セキュリティ対策における課題等を踏まえ、平成 25 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。

（1）情報セキュリティに関する普及啓発

① 最近の手口も考慮した標的型メール訓練の継続的な実施及び標的型メールへの対応に係る教育の充実

② 政府全体で推進することとされているリスク評価の取組及び継続的な教育を通じた情報の格付及び取扱制限の理解促進

③ 情報セキュリティの障害・事故等を踏まえた情報システム管理者向けの教育の見直し

（2）情報セキュリティに関する自己点検

① 自己点検の円滑な実施のための対策立案と実行

② 自己点検結果を改善活動につなぐための仕組みの確立

（3）情報セキュリティ監査

情報セキュリティの障害・事故等を踏まえた監査内容の見直し

（4）IT-BCP

教育訓練計画の作成と計画に沿った訓練の実施

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、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。しかし、一方で標的型攻撃に代表されるインシデントが毎日のように報道されており、文部科学省を含む行政機関においても、新たな脅威への対応を含む一層の情報セキュリティ対策が重要な課題となっています。

この報告書本文では触れられていませんが、文部科学省の IT システムが更新され、本年1月より順次運用が開始されています。新システムにおいては、職員の利便性向上と情報セキュリティ強化の両面からいくつかの新しい仕組みが導入されています。今後は、これらの仕組みを利用シーンに合わせてきめ細かくチューニングすることにより、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。

とはいえ、情報セキュリティ対策には完璧な対策は存在しません。情報セキュリティ確保の根幹は職員一人一人の意識と行動です。情報セキュリティ責任部門だけでなく、職員全員の防衛意識の維持と向上が不可欠です。しかし、現状ではセキュリティに対する職員の意識やスキルにはバラつきがあると判断せざるを得ず、継続した教育・訓練が必要です。また、職員が発注する情報システムについて、そのライフサイクルを通じ、要件定義、設計・開発、運用の各段階において、適切なセキュリティ要件を策定できるスキルを身につけてゆく必要があります。本年度はこのためのガイドラインを作成しましたが、今後はそれらのより広範な活用促進と効果のアセスメントが期待されます。

文部科学省では、本年度の反省を踏まえ、NISC 等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。

平成２５年６月１１日
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 通

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 24 年 4 月 1 日から平成 25 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