

## 1. CISOのメッセージ、平成23年度の総括・平成24年度の重点目標

(1)CISOのメッセージ		文部科学省では、業務で取扱う情報について、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、省内職員に対する情報セキュリティの普及啓発、情報セキュリティ監査の拡充、情報システム運用継続計画策定等を中心に取り組んできたところである。本報告はその取組、監査結果等について報告するものである。今後とも、新たな情報セキュリティの脅威にも適切に対応し、引き続き、情報セキュリティの維持・向上に努めてまいりたい。
(2)当該年度の総括	平成23年度の取組(概要)	自己点検、情報システム・重点検査、教育等の情報セキュリティ対策の他、外部監査事業者による情報セキュリティ監査、情報セキュリティ関係規程の見直し、インシデント対応の体制強化等を実施した。
	平成23年度の結果	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たが、情報セキュリティ関係規程、インシデント対応の体制等の整備を進めるとともに、自己点検においても職員の情報セキュリティ意識は高い水準が保たれており、省内の情報セキュリティ対策は従前より強化されつつある。
	平成24年度の重点目標(概要)	調達要件ガイドラインの策定及び周知、標的型不審メールの対処に関する訓練、情報システム管理者向けの集合研修、及び2. (1)の課題への対応を重点的に実施する。

## 2. 情報セキュリティ対策の実施状況

(1)自府省庁の課題 (自己点検結果、情報システム・重点検査、教育・啓発、調達・外部委託等)	<ul style="list-style-type: none"> <li>①自己点検の結果を踏まえた課題 情報の作成及び入手時における情報の格付及び取扱制限の明示等が十分に徹底されていない。</li> <li>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 システムの脆弱性を突いたウェブサイトの改ざんが発生した。</li> </ul>
(2)(1)で記述した課題に対する対策状況・改善に向けた指示	<ul style="list-style-type: none"> <li>①の課題への対策 情報の格付及び取扱制限の必要性及び判断基準の周知</li> <li>②の課題への対策 調達におけるセキュリティ要件の確保、ウェブサイトにおける脆弱性プログラムの排除</li> </ul>

## 3. 情報セキュリティに関する障害・事故等

障害・事故の概要、原因分析	府省庁の対応	再発防止策
平成23年12月19日に個別事業のWebサイトの一部が改ざんされ、個人情報が出た。	Webサイトを一時閉鎖し、原因究明を行った結果、システムの一部に脆弱性があることが判明したため、問題プログラムの修正を行い、1ヶ月後に再開した。	Webサイト全体に対し第三者によるセキュリティチェックを行い、同様の事故が発生しないように再発防止に努めた。

## 4. 具体的な情報セキュリティ対策の実施内容等

実施概要(テーマ)	内容(取組の起点・背景、実施目的、具体的な工夫、費用、アピールポイント等)	効果(定量評価、できたこと・できなかったこと、期待される効果等)
脆弱性検査のフォローアップ強化	個別事業のwebサイト改ざん事故を受け、今年度において脆弱性検査を実施した情報システムの検出事項の対応状況について、従来の書面による報告に加え、技術的な再検査を実施し、フォローアップを徹底して行った。	プログラムの修正が必要な脆弱性の場合にはその修正後に再度の脆弱性検査を行うことにより、当該情報システムにおける脆弱性が残存していないことを技術的に確認する効果が期待される。
フリーメールと不審メール情報の照合による注意喚起	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機能を実装した。	フリーメールによる不審メールの開封を未然に防止し、ウィルスへの感染や情報流出を抑止する効果が期待される。

実施概要(テーマ)	内容(取組の起点・背景、実施目的、具体的な工夫、費用、アピールポイント等)	効果(定量評価、できたこと・できなかったこと、期待される効果等)
調達における情報セキュリティ要件策定ガイドライン等の作成	情報システムのPDCAサイクルにおけるセキュリティ確保のため、調達仕様書に必要なセキュリティ要件の盛り込みを支援するための担当者向けガイドラインやシステム管理手順書の雛型及び解説を作成し、情報システムの実態に応じた手直しができるようにしている。なお、調達ガイドラインは、要件定義業務、設計・開発・構築、運用・保守の3つについてひな型及びその解説を用意しており、設計・開発・構築時の調達仕様書のひな型については、「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る。	調達時や運用時において、必要な情報セキュリティ要件が確保され、適切なセキュリティを組み込んだシステムの実現に寄与することが期待される。
情報の格付及び取扱制限の雛型自動表示	情報の格付及び取扱制限に係る明示を徹底するため、文書作成時のヘッダー及びメール作成の件名に機密性及び取扱制限の雛形(【機密性○ 情報(取扱制限)】)が自動的に挿入されるようにした。〈昨年度推奨事例の実践〉	職員に対し、情報の格付及び取扱制限の決定を促す効果が期待され、漏れ等のミス防止や習慣化が期待される。