平成23年度情報セキュリティ報告書(概要)

総務省 MIC Ministry of Internal Affairs and Communications

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		・平成23年度は、以下の情報セキュリティ対策を重点的に実施。 (1) 職員に対する情報セキュリティ教育 (2) 公開用ウェブサーバの対策状況の監査 ・また、個人情報の誤送信を踏まえ、個人情報の厳重かつ適正な管理に努めるとともに、総務省におけるウイルス感染事案を踏まえ、情報セキュリティの一層の強化に取り組んだ。 ・情報通信、行政の情報化等を所管する省として、情報通信技術の最新の動向等を踏まえ、新たな情報セキュリティ上の脅威にも適切に対応できるよう努める。
(2)当該年度の総括	平成23年度の取組(概要)	①情報セキュリティに関する教育及び自己点検 ②情報システムの重点検査 ③情報セキュリティ監査 ④標的型攻撃への対応
	平成23年度の取組(結果)	①、②：おおむね適切に実施された。③：一部の公開ウェブサーバにおいて脆弱性が検出されため、推奨する対策等とともに担当者へ通知し、対応が完了するまでフォローアップを実施。④：引き続き実施中。
	平成24年度の重点目標(概要)	（主要な機関へのサイバー攻撃が大きな問題になっている現状等を踏まえ、） ・総務省情報セキュリティポリシー等の見直し ・情報セキュリティに関する教育及び自己点検 ・最新の脅威を踏まえた職員への訓練、情報提供 ・最新の攻撃手法を踏まえた情報セキュリティ監査

2．情報セキュリティ対策の実施状況

(1)自府省庁の課題	情報セキュリティに関する教育及び自己点検において、一部改善の余地がある遵守事項があった。
(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	改善の余地がある遵守事項について、情報セキュリティ教育教材を作成し、情報セキュリティ対策の実施状況の改善を促した。

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
○個人情報の誤送信 総務省中国総合通信局において、平成23年４月13日（水）９時53分と10時34分の２度に分けて、管内の複数の電気通信事業者の担当者（計144宛先）に対し、事務連絡メールをそれぞれ一斉送信した際、災害時連絡先として登録された個人の電話番号、メールアドレス（延べ49件）を記載したファイルを添付した形で送信。	本件で御迷惑をおかけした関係者の方々に対し、直ちに御報告とお詫びを申し上げるとともに、当該メールの削除を依頼。	今後このような事態が生じないよう、個人情報の厳重かつ適正な管理を実施。
○情報流出を伴うウイルス感染 　総務省において、平成23年11月、23台のパソコンが新種のトロイの木馬型ウイルスに感染していたことが判明。 　また、これらのパソコンから、当該感染により、何らかの情報が外部に送信されたことを確認。	・報道発表によるお詫び。 ・各種調査。	ウイルス感染防止対策の強化に努めるとともに、未知のウイルスに感染した場合にも、早期に感染を発見し、被害の拡大を防止するための対応に努めている。

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	内容	効果
公開ウェブサーバの対策状況の監査	総務省が運営し外部に公開しているすべてのウェブサーバシステムについて、ネットワーク及びウェブアプリケーションの脆弱性の有無を確認。脆弱性の検出状況について、推奨する対策等とともに報告書にまとめて情報システムの担当者に通知し、対応が完了するまでフォローアップを実施。	公開ウェブサイトへの不正アクセスの防止。
標的型攻撃への対応	・職員の不審なメールへの適切な対応の強化（不審なメールへの適切な対応についての職員への周知・徹底、標的型攻撃に対する訓練、不審メール情報の共有）。 ・総務省ＬＡＮにおける情報セキュリティの強化。	・ウイルス感染防止対策の強化。 ・未知のウイルスに感染した場合の早期感染発見、被害の拡大防止。