情報セキュリティ報告書　府省庁別概要資料　　財務省

1．CISOのメッセージ、平成23年度の総括

(1) CISOのメッセージ		機密情報等を扱う政府機関は、情報システム開発・運営や日々の事務の中で情報セキュリティ対策を適切に講じることが必要。財務省は、政府全体の取組を踏まえ、国の予算や税の賦課・徴収といった国民生活に密接に関連する所掌事務の情報セキュリティに不測の事態が生じないよう、積極的に取り組んでいる。今後とも、内閣官房等の関係政府機関と連携し、情報セキュリティ対策の強化に努めていく。
(2) 平成23年度の総括	平成23年度の取組(概要)	主な取組：①全行政事務従事者による自己点検、②規程、自己点検、システムに関する監査、③標的型メール攻撃等への対応、④規程の見直し、⑤eラーニングなど教育の充実
	平成23年度の取組(結果)	自己点検及び監査により、情報セキュリティ対策が適正に実施されていることを確認。 その他の取組により、規程、システム、職員意識など複合的な観点から情報セキュリティを強化。
	平成24年度の取組予定(概要)	主な予定：イ) 研修、自己点検、監査の前倒し実施等、ロ) 標的型メール攻撃への更なる対応、ハ) 次期財務省LAN導入に合わせた技術的な対策強化、ニ) 規程の見直し

2．財務省における情報セキュリティ対策の実施状況

(1) 財務省における対策とその課題	①すべての行政事務従事者による自己点検 すべての遵守事項で高い対策実施率を確保。対策が概ね適正に実施されていることを確認。 ②情報セキュリティ関係規程、自己点検、情報システムに関する監査 情報セキュリティ関係規程の準拠性を確認。自己点検が適正に実施されていることを確認。 情報システムについても、各システムが概ね適正に運営・管理されていることを確認したが、一部システムについて、業者との契約の内容や、物理的セキュリティ、非常時対応等に改善を要するなどとした。 ③標的型メール攻撃及びなりすましメールへの対応 → 「4．」を参照。 ④規程の見直し → 政府統一基準を踏まえた改定のほか、独自の見直しを実施(「4．」を参照)。 ⑤教育の充実 ・すべての行政事務従事者を対象として、集合研修を多数回実施(9月・2月に計18回) ・行政事務従事者を管理する立場にある課室情報セキュリティ責任者向け研修を新設(10月に2回) ・eラーニングの研修教材を充実し、自習を呼びかけ ・情報システムの個別管理組織(PJMO)職員向け研修を実施(9月・10月に計2回)

情報セキュリティ報告書　府省庁別概要資料　　財務省

(2) 課題に対する対応	①自己点検：今後とも、遵守事項が適正に実施されるよう、職員の教育等の取組を行う。 ②監査：改善の指摘を受けた情報システムについては、各担当部局において改善を図る。平成24年度の監査においてフォローアップを行う予定。 ※なお、情報セキュリティ研修、自己点検、監査については、結果を踏まえた対策を早期に講じることが重要であるとの観点から、平成24年度は前倒し実施の予定。

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
特段の障害・事故等は見られなかった。		

4．その他の情報セキュリティ対策の実施内容等

実施概要	内容	効果
標的型メール攻撃について、職員に対する注意喚起等の取組を実施	内閣官房主催の訓練への参加、特定のアドレスからのメールを自動的に遮断する等の取組のほか、 ・ポータルサイト及びメールで注意喚起情報を配信 ・フリーメールアドレスから受信したメールについて注意喚起文を自動表示	日々の業務における標的型メール攻撃のリスクへの意識を高める
なりすましメール防止のため、SPFによる送信ドメイン認証技術の導入等の対策を実施	財務省のすべてのドメイン（xxx.go.jp）に送信側SPFの設定を実施したほか、 ・利用していないドメインを廃止 ・メール送信を行わないドメインについてメール送信を行わない旨SPFの設定を実施	財務省のドメインを詐称するメール（なりすましメール）の防止に資する
「情報の移送・提供に関する実施規則」の整備	機密性情報の移送・提供について、当該移送・提供のための許可申請・届出の手続をより具体化するため、「情報の移送・提供に関する実施規則」の整備に取り組んだ	日々の業務における適正な情報管理を図る