

情報セキュリティ報告書（概要版）

宮内庁

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		宮内庁は、内閣総理大臣の管理の下にあって、皇室関係の国家事務を担い、業務で取り扱う情報や情報システムも多岐にわたっている。宮内庁においては、これまで、情報セキュリティ教育及び職員を対象とした情報セキュリティ対策実施状況の自己点検と職員向けの注意喚起を中心に、セキュリティ対策を推進してきた。現段階では重大な課題は発見されていないが、今後も引き続き情報セキュリティの維持・向上に努めていく。
(2) 当該年度の総括	平成23年度 of 取組 (概要)	・統一規範、統一管理基準及び統一技術基準に準拠して、宮内庁ポリシーの体系を改定した。 ・情報システム調達の仕様書作成時におけるセキュリティ要件策定手順の標準化の検討を行った。 ・職員研修で標的型メールの事例を解説した。
	平成23年度 of 取組 (結果)	標的型メール訓練の実施と職員研修の効果により、セキュリティ上の脅威に対する職員の理解が深まったと考えられる。「セキュリティ要件策定手順」を検討し、セキュリティ要件策定の重要性を、担当職員に周知することができた。
	平成24年度 of 重点目標 (概要)	・情報セキュリティポリシーや関連規程の見直しを行う。 ・職員が標的型サイバー攻撃等に適切に対処できるよう、情報セキュリティ教材を充実するとともに、研修・訓練の機会を確保する。

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)	昨今の政府機関等に向けられた標的型サイバー攻撃に適切に対処するためには、職員各自が情報セキュリティ対策を正しく理解し、判断基準を持って行動しなければならない。そのためには、継続的なセキュリティ教育の実施が課題として上げられる。 また、自己点検、重点検査等において大きな問題は発見されていないものの、各情報システムの運用面における適切なセキュリティ対策の維持を今後も継続していく必要がある。
(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	昨今の情報セキュリティ情勢を踏まえ、教育用の教材として標的型メールの具体例を多数取り上げ、受講者にとって理解しやすい内容となるように工夫した。また、これらの集合教育教材は、職員用電子掲示板に掲載し、職員の閲覧に供している。

情報セキュリティ報告書（概要版）

宮内庁

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
情報セキュリティに関する重大な障害・事故は発生していない。		

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)
情報セキュリティ教育の充実	情報セキュリティの基礎知識を整理しつつ、標的型サイバー攻撃を理解できるよう、教材の内容に工夫を加えた。	前期と後期に分けて職員研修の場を設けたこと及び「標的型メール攻撃の訓練」が実施されたことがあいまって、職員の理解がより深まったと考えられる。