情報セキュリティ報告書　概要資料

内閣官房

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		内閣官房は内閣の直属の機関として、他の府省庁以上に秘匿性の高い情報を扱うことから、高度な情報セキュリティ対策を講じる必要がある。そのため、内閣官房の特性を踏まえた情報セキュリティ教育、サイバー攻撃に関する情報の入手・分析等を行い、それらに対応する最新の情報に基づく注意喚起を行うなど情報セキュリティ対策を実施してきた。 平成23年度は、標的型攻撃メールの送付やHPの改ざんがあり、情報漏洩等は発生しなかったものの、サイバー攻撃のターゲットにされていると思われる事象が散見された。今後も最新の動向に留意しつつ一層の情報セキュリティ水準の向上に努めていく必要がある。
（2）当該年度の総括	平成23年度の取組（概要）	平成23年度は、サイバー攻撃について職員の理解を深めるための教育、ソーシャルハッキングの手口を用いる実践形式の標的型メール攻撃に対する訓練を実施した。
	平成23年度の取組（結果）	実践形式の標的型メール攻撃訓練については、実在の職員を装い、難易度を高めに設定して実施した。
	平成24年度の重点目標（概要）	標的型メール攻撃はソーシャルハッキングの技術を用いた新たな手口が日々生み出されていることから、新たな手口に対応し、攻撃を防ぐための教育を継続して実施する。

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）	内閣官房は、内閣直属の機関として秘匿性が求められる情報を取り扱う機関であることから、サイバー攻撃のターゲットになりやすいと考えられ、現に平成23年度は標的型攻撃を受けている。これらの攻撃を防ぐためには、セキュリティに関する職員教育の充実を図り、よりセキュリティに関する理解を深める事が重要であるが、教育の成果に係る効果測定が困難であり、次年度以降、引き続き工夫が必要である。
（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	セキュリティに関する理解を深めるため、自己点検についてはNISC提供の雛形を活用し、学習用例題については、実際の業務で起こり得る具体的な事例に修正した。また、サイバー攻撃の事例や標的型攻撃メールにおける具体的な攻撃手法等の最新の事例を解りやすく解説した教材を作成し、配布を行った。

内閣官房

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
標的型攻撃メールによるウイルス感染 （平成23年9月15日）	端末の隔離・交換	不審メールの見分け方、手口の周知
一部のWebサイトの改ざん （平成24年1月28日）	深夜に改ざんがあり、翌朝までに復旧	セキュリティ設定の検査・変更

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）
サイバー攻撃に関する理解を深めるための職員教育	政府機関に対するサイバー攻撃の増加に鑑み、サイバー攻撃の事例や標的型攻撃メールにおける具体的な攻撃手法に関する教材を作成し、教育教材として配布した。理解度を深めるために、サイバー攻撃が現実社会に与える影響や、ソーシャルハッキングの手口等について解りやすく解説を加えた。	NISC主催の標的型攻撃のメール訓練において、実在の職員名を用いる等、教育効果の向上を図った。