情報セキュリティ報告書　府省庁別概要資料　　法務省

法務省 Ministry of Justice

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		法務省では，情報通信技術を積極的に導入・活用し，行政サービスの質の向上等に努めてきましたが，情報通信技術への依存が高まるにつれ，サービスの停止や情報の漏えい等の情報セキュリティに関する事案が与えるインパクトも大きくなっています。特に，法務省が取り扱う情報の性質を考慮すれば，情報セキュリティに関する事案が発生した場合には，法務行政の遂行に著しい支障を来すことは言うまでもありません。このような事態を招かないようにするとともに，万が一，発生した場合には，その影響を最小限にとどめることができるように，情報セキュリティ対策の実施状況を把握・評価して，その維持・改善を行う各取組を一連の流れとするマネジメントサイクルを体系的かつ継続的に実施し，情報セキュリティの更なる向上に取り組んでまいります。
（2）当該年度の総括	平成23年度の取組（概要）	・「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」の分冊・改訂に伴う対応 ・情報セキュリティ対策の教育・意識啓発に係る取組 ・情報セキュリティマネジメントサイクルの充実・強化
	平成23年度の取組（結果）	・昨今の情報セキュリティに係る問題意識や技術的・環境的な変化に対応するため，省庁対策基準及び省庁対策基準に規定された対策内容を具体的に実施するための要領等を一部改正した。 ・「情報セキュリティ月間」に，情報セキュリティに関する専門研修として，法務本省に勤務する課室等情報セキュリティ責任者を対象とした集合研修を実施した。 ・自己点検に関する監査の対象を各地方官署に勤務する職員まで拡大した。 ・情報処理業務を外部委託する際の調達仕様書に盛り込む情報セキュリティ対策について，最高情報セキュリティアドバイザー等による指導・助言を行った。
	平成24年度の重点目標（概要）	・これまでの取組を継続しつつ，役割に応じた情報セキュリティ対策の教育を実施すること。 ・「標的型メール攻撃の対応訓練」を法務本省において実施すること。

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）	・自己点検結果の正確性向上 ・情報セキュリティ教育の充実 ・情報システムのセキュリティ水準の維持・向上 ・情報システムの調達におけるセキュリティ対策の確認
（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	・自己点検に関する監査の対象拡大・監査における質問（ヒアリング）項目の充実 ・役割に応じた情報セキュリティ教育の実施（教育教材の整備） ・脆弱性の修正プログラム等を適用するまでの期間短縮や適用頻度の見直し ・調達仕様書に記載する内容の確認及びセキュリティ要件の策定状況の確認

情報セキュリティ報告書　府省庁別概要資料　　法務省

法務省 Ministry of Justice

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
事故者は，平成19年1月ころから平成22年9月ころにかけ，①自己所有のUSBメモリに職務上の情報を保存して庁舎外に持ち出し，②貸与を受けた法務省管理のUSBメモリの適正な管理を怠り，同USBメモリを紛失し，③他の職員の識別コードを使用して，サーバに不正アクセスしたもの。	事故者が保有する情報を回収し，情報流出の防止を図った。	該当庁において，情報の管理を徹底するよう職員研修を実施し，注意喚起を行った。
事故者は，平成23年10月ころ，モバイルパソコンにおいて作成した文書を出力し，同文書をキャリーバッグに入れて帰庁したところ，同文書が紛失していることに気が付いたもの。	移動経路を検索したほか，遺失物等について関係機関に照会を行った。	情報の取扱いを一層慎重に行うよう関係職員を指導した。
事故者は，平成23年12月，使用権限のないID・パスワードを使用して内部のネットワークに不正アクセスし，閲覧が許可されていないファイルを閲覧したもの。	証跡を確認し，情報の持ち出し又は漏えいがないか確認した。また，ID・パスワードの変更のほか，情報セキュリティの強化策について検討した。	法務省情報セキュリティ対策基準等の遵守のほか，電磁的記録に対するアクセス制御，保存場所又は保存方法等，適正な管理について，所管各庁に注意喚起文書を発出した。

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）
標的型メール攻撃の対応訓練（試行実施）	独自に訓練を実施することで，法務省職員をターゲットとした巧妙ななりすましメールの作り込みが可能になった。内部LAN上に待ち受けサーバを構築し，簡易な方法で実施することができた。	訓練の対象となった職員は，実体験を通じて，不審メールが到達する可能性があることを認識できた。次回は，更に開封時の初動対応・報告まで含めた訓練の実施を検討する。
情報セキュリティに関する専門研修	課室等情報セキュリティ責任者を対象として，外部講師を招いて専門研修を実施した。	課室等情報セキュリティ責任者に，最新の脅威や標的型メール攻撃の仕組みを教育することで，情報セキュリティ上の役割や責務を認識させることができた。