平成23年度　情報セキュリティ報告書　概要　防衛省

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年度に顕在化した防衛産業などに対するサイバー攻撃事案は、幸いにも当省の情報システムが被害を被ることは防ぐことができましたが、日本でのサイバー攻撃の対策強化を行う上で、重要な警鐘を鳴らすものでありました。 防衛省・自衛隊が我が国の平和及び国民生活の安定・安全を確保するための各種の任務を適切かつ円滑に実施する上では、迅速・確実な指揮命令の伝達や情報共有を実現する情報システムが不可欠です。このような、防衛省・自衛隊における情報システムの安全性は国の安全保障に直結するものであるため、その情報セキュリティの確保は極めて重要であると認識しています。
(2) 当該年度の総括	H23年度の取組 (概要)	・　情報セキュリティ対策の実施状況に関する自己点検、職員に対する教育、情報システムの公開用ウェブサーバ、電子メールサーバへの情報セキュリティ対策の重点検査及び所持品検査等の特別検査を実施。 ・　類似業務の情報システムを統合しメールサーバ等の集約化を実施。
	H23年度の取組 (結果)	・　自己点検の結果は実施率１００％を達成。重点検査の結果から情報システムに対して十分な対策が講じられていることを確認。 ・　情報システムを統合し、メールサーバ等の集約化を実施することにより情報セキュリティ対策の効率化を実施。
	H24年度の重点目標 (概要)	最新のパターンファイルでも発見できない新種のウイルスも日々確認されており、個々の職員が不審メールに対する知識と対策を身につける必要がある。また、私有可搬記憶媒体の管理に関する規則違反が発生していることを踏まえ以下の取組を行う。 ・　職員への不審メール対策に関する教育の実施。 ・　職員に対する不審メールを模擬したメール送付による訓練の実施。 ・　私有可搬記憶媒体の管理に関する規則類の遵守の徹底。

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)	可搬記憶媒体の管理及び業務用データの取り扱い等に関する規則違反が発生していること。また、防衛省の調達における情報セキュリティについても強化を行うことが必要。
(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	可搬記憶媒体の管理及び業務用データの取り扱い等に関する規則違反の当事者に対して懲戒処分を実施。 昨年夏のサイバー攻撃事案の事実関係を踏まえ、関係規則を平成２３年１２月に改正し、契約企業に対し、保護を要する情報の取扱いの厳格化、人的教育の徹底等を図り対策を強化。また、防衛省内においても不審メールに対する訓練を実施。

平成23年度　情報セキュリティ報告書　概要　防衛省

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
当事者の規則遵守意識の欠如により、私有可搬記憶媒体を職場に持ち込み、職場の情報システムで使用。 同様の事案他5件	当事者に対する懲戒処分を実施	関係規則等の再教育を実施
当事者の規則遵守意識の欠如により、私有可搬記憶媒体を職場に持ち込み職場の情報システムで使用及び私有パソコンでの業務用データの取り扱い。 同様の事案他3件	当事者に対する懲戒処分を実施	関係規則等の再教育を実施
当事者の規則遵守意識の欠如により、官品可搬記憶媒体を無許可で使用。 同様の事案他1件	当事者に対する懲戒処分を実施	関係規則等の再教育を実施
当事者の規則遵守意識の欠如により、私有パソコンを職場に持込み使用。	当事者に対する懲戒処分を実施	関係規則等の再教育を実施

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）
情報システムの統合によるメールサーバ等の集約化	防衛省・自衛隊内各機関で個別に構築・利用していた情報システムについて、類似業務の情報システムを統合しメールサーバ等の集約化を実施	情報システムの統合により、メールサーバ等ハードウェアの削減並びに利用するソフトウェアの種類及びバージョンの削減を行い、情報システムの統合化によるセキュリティ対策の効率化及び運用管理コストの低減を図った。 情報システムの統合により、システムダウンの影響が非常に大きくなることから、バックアップサーバの設置やロードバランサによるサーバの負荷分散など、情報システムの可用性の確保に留意した。
ＵＳＢデバイス管理の導入（可搬記憶媒体（ＵＳＢメモリ）の強制的な使用制限）	ＵＳＢ接続の可搬記憶媒体を事前に登録したもの以外使用不可能とし、情報システムで使用する可搬記憶媒体を制限	未登録の可搬記憶媒体を使用不可能とすることにより、未登録である防衛省外の可搬記憶媒体からのウイルス感染を防止し、情報セキュリティの向上を図った。

平成23年度　情報セキュリティ報告書　概要　防衛省

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)
情報システム利用者の認証機能の変更	情報システムのログインカードとして身分証明書ICカードを利用	従来は、情報システム専用のログイン用ICカードを用いていたが、利用者離席時にログイン専用ICカードを端末のICカードリーダー等に残置するケースも考えられ、セキュリティ上の問題があった。 本人が常時携行するため、端末のICカードリーダー等に残置することがなく、なりすましのおそれの少ない身分証明書ICカードをログイン時の認証機能として利用することとし、本人以外による情報システムの不正利用の低減を図った。
不正プログラム対策の強化	複数種類のウイルス対策ソフトの導入	部内系領域、部外系領域及び部内系－部外系間の系間データ移動においてベンダーの異なる複数のウイルス対策ソフトを導入した。 これにより、不正プログラムを検知するためのパターンマッチングでの網羅性の強化及び領域を跨いで不正プログラムが移動する際の重層的なウイルスチェックを行うことにより不正プログラム対策の強化を図った。
部外への情報流出対策の強化	インターネットへのメール送信機能の限定	利用者の端末において、インターネットへのメールの送受信を行う領域 (部外系領域) を仮想端末上で動作するようにし、行政文書の作成等を行う領域 (部内系領域) から論理的に分離した。 部内系領域と部外系領域との間のデータ移動には専用のソフトウェアを利用することとしたことにより、端末で作成した行政文書のデータを利用者の不注意による誤送信等で部外に流出させてしまうおそれの低減を図った。
監査証跡の取得拡充	障害等の原因究明の手がかりとなる監査証跡を取得	外部への情報持出しなどが疑われる操作など、不審なファイル操作を詳細に確認するため、端末の動作履歴、媒体やプリンタへの出力履歴の取得を拡充 (端末に専用の証跡取得用プログラムを導入) することにより、情報システムの障害等が発生した際の原因究明資料とし、被害の拡大防止、再発防止を図った。