防衛省情報セキュリティ報告書

平成２４年５月
防衛省

目次

はじめに

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。

防衛省においては、情報システム及び情報システムにおいて取り扱われるデータに関して、総合的かつ体系的な管理の基準及び当該管理を組織的に実施するための基本事項である、「防衛省の情報保証※に関する訓令」（平成１９年防衛省訓令第１６０号）を定めており、主に以下のような施策に取り組んでいます。

① 情報システムの整備等に当たって認証機能、アクセス制御機能及び証跡管理機能等各種機能を設けること並びにこれら各種機能を適切に運用、管理すること
② 防衛省の可搬記憶媒体の集中保管及び職場からの持ち出し時の許可並びに私有可搬記憶媒体の防衛省の情報システムでの使用を禁止すること
③ サイバー攻撃等に対処するため、連絡体制、処置要領及び情報収集、分析、配布要領等を定めた対処要領を策定すること

本報告書は、平成２３年度に防衛省が実施した情報セキュリティの具体的な取組内容、取組結果等について取りまとめたものです。

平成２３年度においては、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及び電子メールサーバへの情報セキュリティ対策の実施状況の重点検査、所持品検査等の特別検査を実施しました。この結果、おおむね適切な情報セキュリティ対策が取られていましたが、一部に不十分な事項があり、これらの事項について改善を図っていきます。

※ 防衛省においては、「防衛省の情報保証に関する訓令」（平成１９年防衛省訓令第１６０号）の中で、情報システム及び情報システムにおいて取り扱われるデータの機密性、完全性、可用性、識別認証及び否認防止を維持することを「情報保証」と定義していますが、「情報保証」は一般的に言われている「情報セキュリティ」と類似のものであることから、本報告書においては「防衛省の情報保証に関する訓令」及び「情報保証統括責任者」等の固有名詞を除き「情報保証」に代えて「情報セキュリティ」という用語を使用します。

また、平成２３年度においては、防衛省・自衛隊内での類似業務の情報システムを統合することでメールサーバ等の集約化を実施し、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りました。

今後とも、防衛省・自衛隊に対する国民の皆さまの期待に適切かつ確実に応えることができるよう、防衛省・自衛隊の活動にとって重要な基盤である情報システムの安全性を確保するため、情報セキュリティ対策の向上に努めてまいります。

情報保証統括責任者
（防衛省運用企画局長）
松本　隆太郎
平成２４年５月

１ 平成２３年度の総括

(1) 平成２３年度の評価

- 平成２３年度の重点事項

　平成２３年度は、防衛省・自衛隊内でこれまで利用していた防衛省中央ＯＡネットワーク・システム及び防衛監察本部事務用電算機を９機関共同事業として新たな防衛省中央ＯＡネットワーク・システムに統合し、メールサーバ等の集約化を実施しました。このことにより、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うことができ、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りました。

　また、平成２２年度の自己点検で対策実施状況が十分といえなかったバックアップの取得及びアクセス権の設定等についての教育並びに可搬記憶媒体経由によるウイルス感染の危険性の周知及び可搬記憶媒体の管理に関する教育を実施しました。

- 情報セキュリティ対策の実施状況に関する自己点検結果

　職員の情報セキュリティに関する規則の遵守状況について自己点検を行ったところ、適切に実施していることを確認しました。

- 情報システムごとの状況

　情報システムの公開用ウェブサーバ及び電子メールサーバへの情報セキュリティ対策の実施状況の重点検査を実施したところ、十分な情報セキュリティ対策が講じられていることを確認しました。

　今後も情報システムに対して各種の情報セキュリティ対策を講じていきます。

- 教育・啓発

　防衛省では、職員に対して毎年度一回以上情報セキュリティに関する教育を実施しています。

　毎年２月を「防衛省情報セキュリティ月間」と定め、平成２３年度においては、不審メール対策に関する教育教材を各機関に配布することにより、職員に対する情報セキュリティ教育を実施しました。

　また、平成２３年１１月から１２月にかけて不審メール訓練を実施し、職員に対して不審メール受信時の手順について教育・訓練を実施しました。

　これらの教育により、職員の情報セキュリティに関する知識の習得及び意識の高揚を図っています。

- 調達・外部委託

　防衛省では従来から、情報システムの調達・外部委託に関する情報セキュリティ対策として、「装備品等及び役務の調達における情報セキュリティの確保について」（防経装第９２４６号。２１．７．３１）を定め、装備品等及び役務の調達に関する保護すべき情報を取り扱う企業（保護すべき情報を取り扱う下請け企業を含む。以下「契約企業」という。）

に対して特約条項を適用し、契約企業における情報セキュリティ対策を求めています。また、防衛省は、契約企業の作成した情報セキュリティ基本方針等の確認及び契約企業の情報セキュリティ対策の実施状況の監査を行うことにより、情報システムの調達における情報セキュリティ対策を実施しています。

しかしながら、昨年夏のサイバー攻撃事案の事実関係を踏まえ、防衛省の調達における情報セキュリティに関する特約条項等を平成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しました。

- その他取り組んだ事項

防衛省中央ＯＡネットワーク・システムにおいて、以下の施策により情報セキュリティ対策の強化を図っています。

- 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）
- 情報システム利用者の認証機能の変更
- 不正プログラム対策の強化
- 部外への情報流出対策の強化
- 監査証跡の取得拡充

また、防衛省では、可搬記憶媒体等の不正な持ち込み及び持ち出しを防止するための抜き打ちでの所持品検査並びに秘密等データの取扱いを許されていないパソコンに保存されているデータの抜き打ち検査を行う特別検査を実施しています。抜き打ちでの検査を行うことで特別検査の実効性を高めることにより、私有可搬記憶媒体の利用等による情報流出の未然防止を図っています。

- 情報セキュリティに関する障害・事故等の報告

平成２３年度は、私有可搬記憶媒体及び私有パソコンに関する違反行為に対する隊員の処分を行いました。

なお、平成２３年度において外部への業務用データの流出は確認されておりません。

(2) 翌年度の目標

防衛省の情報システムにおいては、最新のパターンファイルを使用した対策ソフトによりシステム的なウイルス対策措置を行っております。しかし、ネットワークの世界では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、各利用者においても不審メールに対する知識と対策を身につけ、情報セキュリティ意識の向上を図ることが必要です。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、平成２４年度には以下の取組みを行います。

① 職員への不審メール対策に関する教育の実施
② 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
③ 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 報告の基本情報

(1) 防衛省の概要

防衛省・自衛隊は、わが国に対する武力攻撃事態等への対処のみならず、大規模災害への対応や、ＰＫＯ活動や国際緊急援助活動をはじめとする海外での活動など、幅広い任務を有しています。

これらの任務を円滑・適切に実施するためには、中央から陸上、海上、航空自衛隊の部隊等に対する指揮命令の伝達、中央と部隊等の間の情報共有などを迅速かつ確実に行う必要があり、このため、防衛省・自衛隊においては、各種の情報システムを整備してきました。

(2) 対象とする期間

本報告書では、平成２３年４月１日から平成２４年３月３１日を対象としています。

(3) 対象とする組織

本報告書では、防衛省内部部局の他、防衛大学校、防衛医科大学校、防衛研究所、統合幕僚監部、陸上自衛隊、海上自衛隊、航空自衛隊、情報本部、技術研究本部、装備施設本部、防衛監察本部、地方防衛局、自衛隊情報保全隊、自衛隊指揮通信システム隊、自衛隊体育学校、自衛隊中央病院、自衛隊地区病院及び自衛隊地方協力本部を対象としています。

(4) 対象とする情報

本報告書では、防衛省における情報システム及び情報システムにおいて取り扱われるデータ並びに情報システムの仕様、設計、機器の設置場所その他の情報システムの管理に関する事項を記載した文書を対象としています。

(5) 本報告書の責任部署

防衛省運用企画局情報通信・研究課情報保証室

(6) 定員数

本報告書の対象となる防衛省の定員数は、２６９，４３５人（平成２４年３月３１日）です。

(7) 情報システム予算額

平成２３年度の防衛省の情報システムの予算額は、約１，８６８億円です。

３ 情報セキュリティ対策の枠組み

(1) 情報セキュリティ対策に関する文書体系

防衛省では、政府機関が統一的な枠組みの中で、各府省庁が情報セキュリティの確保のために採るべき対策及びその水準を更に高めるための対策の基準として定められた「政府機関の情報セキュリティ対策のための統一基準群」（以下「政府機関統一基準群」という。）に準拠し、「防衛省の情報保証に関する訓令」（平成１９年防衛省訓令第１６０号。以下「情報保証訓令」という。）及び「防衛省の情報保証に関する訓令の運用について」（防運情第９２４８号。１９．９．２０。以下「運用通達」という。）を制定しています。

この「情報保証訓令」及び「運用通達」（以下「情報保証訓令等」という。）は、防衛省における情報セキュリティの確保に関する基本規範と位置付けられるものです。

「情報保証訓令」では、防衛省の情報セキュリティに関する組織及び体制、情報システムに係る対策、防衛省の可搬記憶媒体に係る対策、私有パソコン及び私有可搬記憶媒体の取扱い、教育及び訓練、サイバー攻撃等への対処、対策実施状況の確認等情報セキュリティを確保する上で必要な基本的事項を定めています。

「運用通達」は、「情報保証訓令」の各条項を実施する上で必要な具体的な事項を定めたものであり、例えば、情報システムに設ける脆弱性対応のための機能として、ウイルス対策ソフトの導入を行うこと、ウイルス対策ソフトの更新を行うこと等を定めています。

また、「情報保証訓令等」を各機関等で実施する際の細部事項を各機関等ごとに定めることとしており、統合幕僚監部では、「統合幕僚監部及び自衛隊指揮通信システム隊の情報保証に関する達」（自衛隊統合達第２３号。２０．３．２５）、陸上自衛隊では、「陸上自衛隊の情報保証に関する達」（陸上自衛隊達第６１－８号。１９．１２．１７）、海上自衛隊では、「海上自衛隊の情報保証に関する達」（海上自衛隊達第３７号。１９．１２．２５）、航空自衛隊では、「航空自衛隊における情報保証に関する達」（航空自衛隊達第１４号。２０．３．３１）等を定めています。

(2) 情報セキュリティ対策の推進体制

- 情報セキュリティ対策に係る組織体制（図１参照）
  - 情報保証統括責任者

    防衛省の情報保証に関する事務を統括する者として、情報保証統括責任者を置いています。
  - 情報保証監査統括責任者

    防衛省の情報保証の監査に関する事務を統括する者として、情報保証監査統括責任者を置いています。
  - 情報保証責任者

    各機関等の情報保証に関する事務を監督する者として、各機関等に

情報保証責任者を置いています。

- 情報システム情報保証責任者
  防衛省の情報システムについて、整備、維持管理、廃棄等のライフサイクル全般にわたる情報セキュリティの確保に関する事務を行う者として、情報システム情報保証責任者を置いています。
- 部隊等情報保証責任者
  各部隊等における可搬記憶媒体の管理等の事務を行う者として、部隊等情報保証責任者を置いています。
- 事案対処統括責任者
  防衛省のサイバー攻撃等の対処に関し、機関等の連携活動を統括する者として、事案対処統括責任者を置いています。
- 事案対処責任者
  各機関等においては、各機関等の情報システムへのサイバー攻撃等の未然防止及び対処に関し、情報システム情報保証責任者を統制し、又は情報システム情報保証責任者に対して技術的支援を行う者として、事案対処責任者を置いています。

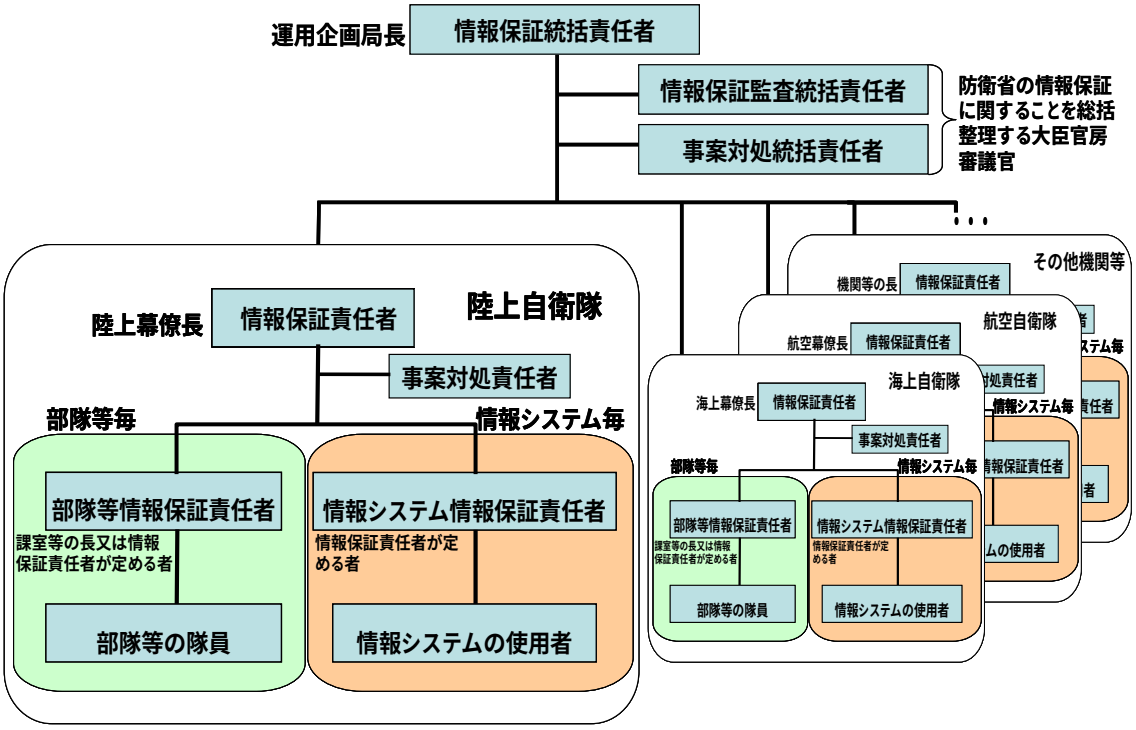

図１ 防衛省の情報セキュリティ体制

- 情報セキュリティ対策に係る推進部署の体制
  防衛省の情報システムの整備及び管理に関すること等を担当する部署として、運用企画局に情報通信・研究課があり、この情報通信・研究課の中に、情報システムの情報保証の確保に関する事務をつかさどる情報

保証室があります。この情報保証室が防衛省の情報セキュリティ対策に係る推進部署となり、また、各機関等においても情報セキュリティの担当部署が設置されています。

(3) 監査

- 監査の概要

　監査については、監査の対象、方法、判断基準等を定めた年度の監査計画書を作成し、当該年度内に必要な監査を実施するようにしています。

　定期監査は、規則の遵守状況に関し職員が行った自己点検の結果について行うこととしています。

　各機関等の情報保証責任者は、防衛省の情報保証訓令及びこの訓令に基づき定められた規則の遵守状況について、毎年度１回、職員に自己点検を行わせています。しかし、情報セキュリティ対策について職員が規則を遵守して適切な運用を行っていることを確認するためには、職員の自己点検だけでなく、自己点検結果の妥当性を確認するために独立性を有する者による監査を実施することが必要です。このため、各機関等の情報保証責任者は、自己点検の結果を踏まえて、自己点検の対象となっている情報セキュリティ対策が実際に行われているかどうかを確認するためにサンプリング調査を実施しています。

- 監査の実施

　各機関等の情報保証責任者においては、機関等内で監査を行うに当たって、監査の計画、監査の項目その他必要な事項を定めることとしています。また、監査を行うに当たっては、監査の対象となる部署とは異なる部署に監査を行わせることで第三者的視点を確保することにより、監査の実効性を高めるようにしています。

- 監査結果及び監査報告

　自己点検結果を提出した職員から監査対象となる職員をサンプリングし、これらの職員が自己点検結果どおり規則を遵守しているかについて監査を行った結果、自己点検における自己評価が適切であったことが確認されました。

(4) 政府機関統一基準群と情報保証訓令等の差異

- 運用承認

　防衛省においては、情報システムの運用等を開始するに先立ち、情報システムに必要とされる情報セキュリティ対策が技術基準に基づいて適切に設けられていることなどを、情報システムの整備に責任を有する者以外の者が確認し、情報システムの運用を承認する手続（運用承認）等を定めています。これは、情報システムに導入する情報セキュリティ対策を決める際に、情報システムの整備に責任を有する者のみならず、運用ニーズを代表する者や、第三者的立場から情報セキュリティ対策を検証する者が連携して関与することにより、情報システム毎の運用環境や運用ニーズに適合させつつ所要の情報セキュリティのレベルを確保する

ための仕組みです。

- 私有パソコン及び私有可搬記憶媒体の取扱い

　防衛省においては、私有パソコンの職場及び船舶の居住区画への持込みや、私有可搬記憶媒体の防衛省の情報システムでの使用を禁止しています。また、私有パソコン及び私有可搬記憶媒体で外部の者に知られることで業務に支障を与えるおそれのある情報等を取り扱うことを禁止しています。

(5) 情報セキュリティ対策に関する文書の見直し状況

　政府機関統一基準群の改訂が行われた際には、必要に応じて情報保証訓令等を改正し、政府機関統一基準群への準拠性を確保しています。また、障害・事故等の原因分析及び情報システムの技術の進展等を反映し、適宜、情報保証訓令等の見直しを行っています。

４　平成２３年度の重点事項

(1) サーバ集約化

・ 目標

これまで利用していた防衛省中央ＯＡネットワーク・システム及び防衛監察本部事務用電算機を９機関共同事業とした新たな防衛省中央ＯＡネットワーク・システムに換装することに伴い、市ヶ谷地区所在９機関のシステム仕様を統一することを基本とし、メールサーバ等の集約化を実現することとしました。

・ 実績

９機関が個々に構築していた情報システムを一つの情報システムに統合することにより、これまで各機関が個別に保有していたメールサーバ等ハードウェアの集約化を行いました。

・ 評価

情報システムの統合に伴い、情報システムで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うことができ、今までに比べソフトウェアの脆弱性対応、バージョン管理等セキュリティ対策の効率化を図りました。

また、メールサーバ等ハードウェアの削減を行うことにより、情報システムの合理化による運用コストの低減を図りました。

なお、今まで個別に構築していた情報システムを一つの情報システムに統合したため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、新システムへの換装時には情報システムの可用性の確保に留意しました。

(2) 調達における情報セキュリティの確保の強化

調達における情報セキュリティの確保の強化については、第５．４項に記載します。

５ 情報セキュリティ対策の実施状況

５．１ 情報セキュリティ対策の実施状況に関する自己点検

(1) 課題と対策

・ 自己点検について

情報保証訓令及び同訓令に基づき定められた規則に関する職員の遵守状況について、毎年度、職員に自己点検を行わせています。自己点検は、職員が自ら遵守状況を点検することにより、情報保証訓令等の遵守を促すとともに、職員に情報保証訓令等の規定を再確認させることにより、改めてその周知を図ること等を目的としています。

・ 平成２２年度自己点検結果に基づく課題と対策

平成２２年度に実施した自己点検では、自己点検の対象者である職員のうち、規則の遵守状況が把握できた者（以下「自己点検提出者」という。）の割合を示す把握率は、責任者※1１００．０%、システム※2１００．０%、職員９８．７%でした。

対策実施状況に関しては、自己点検提出者のうち、遵守事項を守る責務が生じた者（以下「遵守事項対象者」という。）で、全ての遵守事項を実施した者の占める割合を示す実施率は、責任者１００．０%、システム１００．０%、職員９９．９%でした。

また、遵守事項対象者のうち一定の割合（１００%、９５%、９０%）以上の者が対策を実施した遵守事項の割合である到達率は、【到達率１００】※3責任者１００．０%、システム１００．０%、職員９５．９%でした。なお、【到達率９５】※4及び【到達率９０】※5での各主体での到達率は１００．０%でした。

対策実施状況については、バックアップの取得及びアクセス権の設定等一部に十分とはいえない項目が見られることから、平成２３年度の課題は、これら対策実施状況で十分とはいえない項目についての改善を行うことでした。この対策として、職員に対して、対策実施状況で十分とはいえなかった項目を含む教育を定期的に実施しました。

※1：情報保証統括責任者、情報保証監査統括責任者、情報保証責任者、部隊等情報保証責任者

※2：情報システム情報保証責任者

※3：全遵守事項対象者が対策を実施した遵守事項の割合

※4：９５%以上の遵守事項対象者が対策を実施した遵守事項の割合

※5：９０%以上の遵守事項対象者が対策を実施した遵守事項の割合

(2) 平成２３年度自己点検結果の状況

・ 防衛省全体の把握率

平成２３年度の自己点検の対象者である職員のうち、規則の遵守状況が把握できた者の割合である把握率は、１００．０％を達成しました。（表１参照）

表１ 自己点検の把握率

対象年度	責任者	システム	職員
平成２２年度	１００．０％	１００．０％	９８．７％
平成２３年度	１００．０％	１００．０％	１００．０％

・ 防衛省全体の実施率

自己点検提出者のうち、全ての遵守事項を実施した者の割合である実施率は、全ての主体で１００．０％を達成しました。 （表２参照）

表２ 主体別実施率

対象年度	責任者	システム	職員
平成２２年度	１００．０％	１００．０％	９９．９％
平成２３年度	１００．０％	１００．０％	１００．０％

・ 防衛省全体の到達率

遵守事項対象者のうち一定の割合（100%、95%、90%）以上の者が対策を実施した遵守事項の割合である到達率は、全ての主体において【到達率１００】において１００．０％を達成しました。（表３参照）

表３ 主体別到達率

【到達率１００】

対象年度	責任者	システム	職員
平成２２年度	１００．０％	１００．０％	９５．９％
平成２３年度	１００．０％	１００．０％	１００．０％

【到達率９５】

対象年度	責任者	システム	職員
平成２２年度	１００．０％	１００．０％	１００．０％
平成２３年度	１００．０％	１００．０％	１００．０％

【到達率９０】

対象年度	責任者	システム	職員
平成２２年度	１００．０％	１００．０％	１００．０％
平成２３年度	１００．０％	１００．０％	１００．０％

表１、２及び３の数値は小数点以下２桁目を切捨て。

(3) 総評

平成２３年度の自己点検では、把握率、主体者別実施率及び主体別到達率の各項目について、１００．０%の結果を得ました。このことから、対策は適切に実施されている状況にありますが、今後もこの水準を維持して行けるよう、引き続き職員に対する教育を実施していきます。

５．２ 情報システムごとの状況

(1) 課題と対策

防衛省の情報システムに係る対策が不十分な場合、情報の流出、改ざん、破壊等の原因となり、防衛省の業務等に重大な影響を及ぼすおそれがあることから、適切なＯＳの最新化（パッチ適用（アップデート））及びアプリケーションソフトの最新化（パッチ適用（アップデート））を実施する必要があります。そして、これらの対策が確実に実施されているかどうかを定期的に確認することが必要です。このため、防衛省で使用している情報システムの公開用ウェブサーバ及び電子メールサーバに対して、重点検査を実施しています。

なお、平成２２年度の重点検査では、各情報システムの公開用ウェブサーバ及び電子メールサーバに関する情報セキュリティ対策の実施率は１００%であり、十分な情報セキュリティ対策を講じていることが確認できました。

平成２３年度の重点検査の課題は、各種情報セキュリティ対策の実施率が前年度同様の高い水準を維持していることを確認することでした。

(2) 情報システムの対策状況

平成２３年度の重点検査の結果は以下のとおりです。

表４　公開用ウェブサーバ

検査・調査項目		対策実施率
サーバの運用に関する検査・調査	ＨＴＴＰＳ通信を行うサーバにおける脆弱性に対する対応	１００．０%
	大量パケット送信型のサービス不能攻撃への対策の状況	１００．０%
	ＯＳの最新化の状況	１００．０%
	ウェブサーバアプリケーションの最新化の状況	１００．０%

表５　電子メールサーバ

検査・調査項目		対策実施率
サーバの運用に関する検査・調査	ＯＳの最新化の状況	１００．０％
	電子メールサーバアプリケーションの最新化の状況	１００．０％

(3) 総評

平成２３年度の重点検査の結果、情報システムの公開用ウェブサーバ及び電子メールサーバについて十分な情報セキュリティ対策を講じていることが確認できました。

今後も情報システムの公開用ウェブサーバ及び電子メールサーバに対して各種の情報セキュリティ対策を実施することで、対策実施率１００％の維持に努めていきます。

５．３ 教育・啓発

(1) 教育計画の策定、教育の企画等

情報セキュリティを確保するためには、職員の情報セキュリティに関する知識の習得及び意識の高揚を図るため、情報セキュリティに関する教育を行うことが必要です。

防衛省では、一般職員向けに、毎年度一回以上、課室等毎の教育及び機関毎の集合教育等を通じて、日常的に情報システムを利用する際に遵守すべき事項を中心に教育を実施しています。また、情報セキュリティ対策担当者向けの教育として、機関毎の集合教育を通じて、高度な技術的事項を含めた教育を実施しています。

教育を行うに当たっては、以下の事項に留意するようにしています。

・職員の職務に応じた教育を実施すること。
・計画に基づく定期的な教育を実施すること。
・適切な資料を活用した教育を実施すること。

また、防衛省においては、情報セキュリティの確保に向けた活動を集中的に実施する期間として、毎年２月を「防衛省情報セキュリティ月間」と定め、平成２３年度においては、年度末までに換装を行う情報システムの利用者に対して、システム換装の際の教育時に情報セキュリティ部門の担当者が出向き、情報システムの特性に合わせた情報セキュリティに関する教育を実施しました。

(2) 教育内容等

一般職員に対しては、パスワード、ユーザＩＤ等の認証情報の管理、バックアップの取得、アクセス権の設定、可搬記憶媒体の取り扱い及び電子メール受信上の注意点等、情報システムを安全に利用

するために遵守しなければならない事項について教育を実施しています。また、情報セキュリティ対策担当者に対しては、一般職員から許可を求められる手続きに関すること、情報システムに設けた機能を適切に運用してくこと、情報システムを管理する上で必要な文書を整備すること等についての教育を実施しています。

(3) 対象者の役割に応じた教育教材の整備

防衛省では、一般職員向けには、日常的に情報システムを利用する際に遵守すべき事項を中心に平易に理解させることができる教育教材を整備し教育を実施しています。また、情報セキュリティ対策担当者向けには、高度な技術的事項を含めた情報セキュリティ対策担当者として必要な知識を習得できる教育教材を整備し教育を実施しています。さらに、平成２３年度の「防衛省情報セキュリティ月間」においては、主に不審メール対策に関する教育教材を各機関に配布しました。

(4) 情報セキュリティ対策担当者の知識向上等

情報セキュリティ関連部署の職員については、部内の教育課程への入校、国内外の大学等への留学などにより、情報セキュリティに関する知識及び技能の向上を図っています。

(5) 不審メール訓練の実施

平成２３年１１月から１２月にかけ、内閣官房情報セキュリティーセンターが行う政府機関における不審メール訓練の一環とし、防衛省においても不審メール訓練を実施しました。

これは、訓練対象の職員に対して不審メールを模擬したメールを送付し、不審メール受信時の手順等を訓練し、模擬メール中の添付ファイルを開封するなど不適切な取り扱いを行った場合には、教育用コンテンツに誘導することにより、不審メールを受信した際の注意事項の教育を行い不審メール対策の強化を図りました。

５．４ 調達・外部委託

(1) 外部委託先の管理

防衛省では、「装備品等及び役務の調達における情報セキュリティの確保について」（防経装第９２４６号。２１．７．３１。以下「装備品等調達情報セキュリティ通達」という。）を定め、契約企業との契約に「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」を適用することで、契約企業に情報セキュリティ対策の実施を求めています。

「装備品等調達情報セキュリティ通達」では、防衛省が契約企業に求める情報セキュリティ対策を示すとともに、契約企業の自主監査と防衛省の行う監査を通じてその確実な実施を図ることとしています。

(2) 調達における情報セキュリティ確保の強化

しかしながら、昨年夏のサイバー攻撃事案の事実関係を踏まえ、防衛省の調達における情報セキュリティに関する特約条項等を平成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しました。

また、政府全体として取り組んでいる官民間での情報共有の枠組みにおいて、この契約企業から得られた情報の共有を行い、情報セキュリティの向上に向けた政府全体の取組に寄与するものとしていきます。

表６　防衛省の調達における情報セキュリティに関する特約条項等の改正内容について

改正の骨子	改正の具体的内容
防衛省への迅速な報告	①　保護すべき情報が保存されたサーバ／パソコンにウイルス等への感染又は不正アクセスがあった場合には、直ちに防衛省へ報告することを義務化
	②　責任者・連絡担当者を明らかにした連絡系統図の作成
セキュリティ対策の強化	③　少なくとも週１回以上、ウイルス対策ソフトによるフルスキャンを実施
	④　保護すべき情報が社外へ漏えいしていないか、２４時間３６５日監視
	⑤　保護すべき情報へのアクセス記録については、３か月以上保存
	⑥　暗号化対策の強化
企業における教育・訓練の強化	⑦　社員への教育・訓練の実施状況を監査により確認（なりすましメールへの対応状況を重点的に確認）

５．５ その他取り組んだ事項

(1) 情報システムへのセキュリティ対策の強化

防衛省中央ＯＡネットワーク・システムにおいて、以下の施策により情報セキュリティ対策の強化を図っています。

- ＵＳＢデバイス管理の導入

  尖閣沖漁船衝突事件に係る情報漏えい事案が発生したこと等を踏まえ検討が行われた「政府における情報保全に関する検討委員会」において、必要と考えられる措置として「端末のデータの書き出し対策」が示されました。これを受けて情報システムでの情報流出防止対策を強化するため、運用管理サーバにシリアル情報の登録を行った可搬記憶媒体（ＵＳＢメモリ）以外の可搬記憶媒体を使用不可能としました。

  このことにより、未登録の可搬記憶媒体を介した情報流出を防止すると共に、未登録である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りました。

- 情報システム利用者の認証機能の変更

  従来は、情報システム専用のログイン用ＩＣカードを用いておりましたが、利用者離席時にログイン用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りました。

  このため、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されることがなく、なりすましのおそれの少ない身分証明書ＩＣカードをログイン認証機能として利用することで、本人以外による情報システムの不正利用の低減を図りました。

- 不正プログラム対策の強化

  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ました。

  このことにより、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りました。

- 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を限定するため、利用者の端末において、インターネットへのメール送受信を行う領域（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ました。

  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りました。

- 監査証跡の取得拡充

　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、被害拡大防止、再発防止を図ることとしています。

(2)　所持品検査等の特別検査の実施

- 所持品検査

　可搬記憶媒体等の不正な持込み及び持出しを防止するため、課室等ごとに、毎月１回以上の頻度で、職員が秘密等を取り扱う場所に出入りする際に抜き打ちで所持品検査を行うこと及びこれらの場所において勤務中の職員に対する抜き打ちの所持品検査を行うこととしています。

- パソコン内のデータ検査

　秘密等データの取扱いが許可されていないパソコンへの秘密等データの保存を防止するため、課室等ごとに、毎月１回以上の頻度で、秘密等データの取扱いが許可されていないパソコンのハードディスクへの秘密等データの保存の有無を確認するための検査を抜き打ちで行うこととしています。

- 特別検査チームによる検査

　上記の所持品検査及びパソコン内のデータ検査の実施に際し、第三者的視点を確保し、専門的な知見を活用することにより検査の実効性を高めるため、防衛政策局調査課情報保全企画室長又は運用企画局情報通信・研究課情報保証室長をチーム長とする特別検査チームを設け、課室等で検査を実施する者と共同して検査を行うこととしています。

６　情報セキュリティに関する障害・事故等報告

平成２３年度に公表した情報セキュリティに関する障害・事故等としては、以下のように私有可搬記憶媒体及び私有パソコンの管理等に関する規則違反がありました。

いずれの事案も情報保証訓令等関係規則の違反に該当するものであり、違反行為の当事者に対して懲戒処分が行われました。また、再発防止策として職員に対して関係規則等の再教育を実施しました。

なお、平成２３年度において外部への業務用データの情報流出は確認されておりません。

表７　平成２３年度に公表した情報セキュリティに関する事案の概要等

情報セキュリティに関する障害・事故等の発生年月	概要	原因	府省庁の対応
平成 17 年 12 月から平成 19 年 4 月 (平成 19 年 4 月 6 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用及び私有ﾊﾟｿｺﾝでの業務用ﾃﾞｰﾀの取り扱い。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 7 月 29 日)
平成 18 年 4 月から平成 21 年 10 月 (平成 21 年 10 月 22 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 22 年 5 月 21 日)
平成 18 年 9 月から平成 23 年 3 月 (平成 23 年 3 月 3 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用及び私有ﾊﾟｿｺﾝでの業務用ﾃﾞｰﾀの取り扱い。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 7 月 4 日)
平成 19 年 3 月から平成 22 年 7 月 (平成 22 年 7 月 28 日発覚)	私有ﾊﾟｿｺﾝの職場への持込み。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 24 年 3 月 30 日)
平成 19 年 8 月から平成 20 年 9 月 (平成 20 年 9 月 26 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用及び私有ﾊﾟｿｺﾝでの業務用ﾃﾞｰﾀの取り扱い。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 4 月 11 日)
平成 20 年 3 月から同年 9 月 (平成 20 年 9 月 26 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 24 年 1 月 11 日)
平成 20 年 12 月から平成 21 年 7 月 (平成 21 年 9 月 10 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用及び私有ﾊﾟｿｺﾝでの業務用ﾃﾞｰﾀの取り扱い。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 4 月 15 日)
平成 22 年 3 月から平成 23 年 1 月 (平成 23 年 1 月 5 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 4 月 27 日)
平成 22 年 5 月 (平成 22 年 6 月 2 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 24 年 3 月 15 日)
平成 22 年 6 月 (平成 22 年 6 月 17 日発覚)	官品可搬記憶媒体の無許可での使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 4 月 15 日)
平成 22 年夏頃から 11 月 (平成 23 年 3 月 10 日発覚)	官品可搬記憶媒体の無許可での持出し。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 24 年 3 月 22 日)
平成 23 年 3 月 (平成 23 年 3 月 7 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 23 年 9 月 29 日)
平成 23 年 3 月 31 日 (平成 23 年 4 月 6 日発覚)	私有可搬記憶媒体を職場の情報ｼｽﾃﾑで使用。	当事者の規則遵守意識の欠如	当事者に対する懲戒処分 (平成 24 年 3 月 9 日)

７　情報セキュリティ対策に関する平成２４年度の計画

平成２４年度は、平成２３年度に引き続き、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及び電子メールサーバへの情報セキュリティ対策の実施状況の重点検査並びに所持品検査等の特別検査を実施していきます。

その他の情報セキュリティ対策として、個々の職員がなりすましメールに対する知識と対策を身につけ、情報セキュリティ意識の向上を図るため、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、平成２４年度には以下の取組みを行います。

①　職員への不審メール対策に関する教育の実施
②　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
③　私有可搬記憶媒体の管理に関する規則類の遵守の徹底

8　結び

平成２３年度には、国の重要な情報を扱う企業や政府機関に対するサイバー攻撃について、多数の報道がありました。防衛省・自衛隊においてはサイバー攻撃対策として、以前より、①情報通信システムの安全性の向上、②防護システムの整備、③規則の整備、④人材育成、⑤情報共有等の推進、⑥最新技術の研究等の施策を講じており、幸いにも、サイバー攻撃による情報システムの動作異常等は発生していません。しかしながら、サイバー攻撃の脅威は増大してきているものと認識しており、引き続き、サイバー攻撃対処について、これらの施策を着実に実施していく必要があります。

平成２４年３月、情報通信システムの安全性の向上に関して、防衛省市ヶ谷地区にある９機関のＯＡシステムを統合した「防衛省中央ＯＡネットワーク・システム」が運用を開始しました。本システムは、ＵＳＢデバイスの管理強化及び不正プログラムへの対策強化等、様々な情報セキュリティ対策の向上が図られており、防衛省・自衛隊に対するサイバー攻撃対処能力の向上に資するものであると考えています。

他方、残念なことではありますが、平成２３年度には、大多数の職員が情報セキュリティ関連規則を遵守しているにもかかわらず、一部の職員の規則遵守意識の欠如により、私有可搬記憶媒体の使用等に関する規則違反が発生しています。安易な私有可搬記憶媒体の使用は、情報システムにウイルス感染を引き起こす恐れがあるため、平成２４年度には、防衛省・自衛隊において、可搬記憶媒体経由のサイバー攻撃対策を強化していく予定にしています。またサイバー攻撃対策には、メールに関する対策も重要となりますので、不審メール対策に関する教育・訓練も実施していく予定にしています。これらの対策を重点的に実施していくことにより、可搬記憶媒体及びメールを利用したウイルス感染の防止に努め、防衛省・自衛隊に対するサイバー攻撃対処に万全を期して参りたいと考えています。

最高情報セキュリティアドバイザー
（防衛省運用企画局情報通信・研究課情報保証室長）
坂下　圭一