NISC National Information Security Center

政府機関の情報セキュリティマネジメントに関する評価
ベストプラクティス　～2006年度～

2007年8月3日

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

資料３－２

2006年度 情報セキュリティ・ベストプラクティス

NISC

★★ 省内ネットワークを活用した職員の支援
・eラーニングシステム　・実施手順等の運用
総務省　経済産業省

★★ 幹部職員の下で全庁一体となった対策の推進
警察庁

★★ 外部委託における情報セキュリティの確保
・専門家の参画　・調達仕様及び契約の整備
外務省　防衛省

その他の優れたプラクティス

★★ 担当者の情報セキュリティ知識向上のための施策
防衛省

★★ PMOにおける情報システムの安全性・信頼性確保への取組み
防衛省

省内ネットワークを活用した職員の支援　eラーニングシステム

背　景

- 府省庁で情報セキュリティ対策を実施するためには、情報セキュリティ教育の実施を的確に管理し、教育の実効性を確保することが重要である。
- 多数の職員を持つ省においては、情報セキュリティ教育の実施を管理するために、eラーニングシステムに管理機能を用意し、活用することも有効である。

ベストプラクティス

- 総務省では、地方支分部局を含めて、全職員を対象とした情報セキュリティ教育の実施、テスト及び管理のためにeラーニングシステムを導入している。
- 当該システムを利用して、部局の担当者も、所属職員ごとの受講有無、受講日時及びテスト結果を参照することができる。
- 各部局で受講状況を把握し、電子メールや省内の会議を通して受講を促すことにより、２００６年度は、情報セキュリティ教育の受講率は９６％を達成した。

効果：　情報セキュリティ教育の受講の徹底と管理負荷の軽減

評価指標：周知：教育⑦、⑧

総務省

省内ネットワークを活用した職員の支援　実施手順等の運用

背　景

- 府省庁の職員は、通常の職務に加えて、PCの利用や情報の取扱い等、様々な場面で情報セキュリティ対策の遵守も求められている。そこで、これらを定めた実施手順書等は、必要なものが、いつでも、容易に参照できることが重要である。
- また、実施手順書等は、日常の職務とは異なる知識を前提とする場合もあり、利用する職員を支援する仕組みや体制を府省庁に持つことも重要である。

ベストプラクティス

- イントラネット内に職員が自席のPCから参照できる「情報セキュリティコーナー」を設置し、情報セキュリティに係る基準、実施手順書等を常時閲覧できるよう整備している。
- 例えば「情報の格付け」等の目的から、該当する実施手順書等を検索できるようにしている。
- 職員がPCから利用できるヘルプデスクがあり、情報機器利用や情報セキュリティ対策に関する質問を受け付け、回答している。また、質問と回答をデータベースに蓄積して、参照可能としている。
- 多くの職員に有用であると考えられる質問･回答を選び、週1回程度、電子メールで全職員に送付している。

効果：　職員に求める情報セキュリティ対策の促進

評価指標：周知：啓発②

経済産業省

幹部職員の下で全庁一体となった対策の推進

背　景

- 府省庁においては、情報セキュリティに係る組織として、最高情報セキュリティ責任者その他の責任者等を置いている。これらの役割を持つ者は幹部職員の一部の者であることから、広く幹部職員に対して情報セキュリティに係る事項を周知することが、全職員への周知に重要である。
- 幹部職員が情報セキュリティの重要性を理解し、必要に応じ具体的指示を行うことにより、組織的に情報セキュリティの向上に取り組むことができる。

ベストプラクティス

- 長官を含む警察庁幹部が出席する定例会議等において、情報セキュリティ対策等の状況報告を随時行っている。また、当会議における審議を経ることにより、庁全体として統一した情報セキュリティ施策を機動的に推進している。

- 特に重要な課題については、技術面及び運用面等の具体的な対策内容を当該会議に報告することとし、審議及び指示を受けることにより、全職員に対する指示の迅速な周知・徹底を実現している。

効果：　トップダウンでの情報セキュリティ対策実施の周知・徹底

評価指標：計画：組織⑤

警察庁

外部委託における情報セキュリティの確保　専門家の参画

背　景

- 情報システムの構築・運用・保守等の外部委託については、情報セキュリティに関して委託先に実施を求める事項が多様であるとともに、適切な技術仕様の提示も必要となる。
- 他方では、府省庁における外部委託手続は、調達担当部門による標準の手続等を基本として行われることから、情報セキュリティ関連事項を適切に盛り込むためには、そのための手順及び雛形等を整備し、運用することが必要となる。

ベストプラクティス

- 情報システムに係る外部委託に関して、情報システム担当部門に適用する省内手続を定めている。本手続において、情報システム担当部門は、標準の調達仕様書に加えて、委託先に求めるべき情報セキュリティ関連事項を定めた省内規程も適用すべきことを定めている。
- また、本手続において、情報システムの調達仕様について、情報セキュリティ担当部門及び情報セキュリティ専門家であるCIO補佐官による審査及び決裁を受けることとしている。審査の対象は、情報セキュリティに係る契約条項及び技術仕様を含む。
- 審査にあたり、必要に応じ、情報システム担当部門からヒアリングを行い、調達仕様の策定について指導している。さらに、情報システム担当部門の要請があれば、審査に先立ち、事前相談を受けている。

効果：　外部委託における適切な調達仕様・契約の策定

評価指標：実施：調達・外部委託③

外務省

外部委託における情報セキュリティの確保　調達仕様及び契約の整備

背　景

- 情報システムの構築･運用･保守等の外部委託については、情報セキュリティに関して委託先に実施を求める事項が多様であるとともに、適切な技術仕様の提示も必要となる。
- 他方では、府省庁における外部委託手続は、調達担当部門による標準の手続等を基本として行われることから、情報セキュリティ関連事項を適切に盛り込むためには、そのための手順及び雛形等を整備し、運用することが必要となる。

ベストプラクティス

- 情報システムの外部委託に関する調達仕様及び契約に記載する情報セキュリティ関連事項は、調達担当部門が策定している省内標準の雛形に含めている。
- 当該情報セキュリティ関連事項には、委託先における情報セキュリティ管理項目と、構築する情報システムにおける情報セキュリティ機能要件及び保証要件を含んでいる。
- これらは、政府機関統一基準／省庁基準の遵守事項を満足するものともなっており、雛形に従うことにより、基準を遵守することとなる。

効果：　外部委託における適切な調達仕様･契約の策定

評価指標：実施：調達・外部委託①、②

防衛省

担当者の情報セキュリティ知識向上のための施策

背　景

- 情報セキュリティ対策管理部門においてその業務を効果的に遂行するためには、情報セキュリティに係る専門知識・技術を持つ要員の確保が重要。
- このためには、当該部門の目標に基づき職員のキャリアパスを設定し、計画的に要員を養成する必要がある。

プラクティス

- 情報セキュリティ対策管理部門が組織として保有すべき情報セキュリティ知識を明確にし、専門的な知識・実務経験を考慮して職員を配置。
- 例年、数名の職員を国内外の大学院・大学等へ2年程度派遣し、情報セキュリティ事案についての対処・管理手法等を習得させることにより、情報セキュリティ対策の基幹要員を養成。
- 帰任後は省内の情報セキュリティ対策管理部門に配置し、習得した知識・技術を活かす職務に従事させている。

効果：　情報セキュリティ対策管理部門の専門能力の向上・維持

評価指標：計画：資源①

防衛省

PMOにおける情報システムの安全性・信頼性確保への取組み

背　景

- 『IT新改革戦略』（IT戦略本部、平成18年1月19日）に基づき、各府省において、情報化統括責任者(CIO) の下に、情報システムの企画、開発、運用、評価等の業務について責任を持って統括する体制としてプログラム・マネジメント・オフィス (PMO) が整備されている。
- PMOが情報システムの安全性・信頼性の確保に関与することにより、情報セキュリティ水準の向上に寄与することが期待される。

プラクティス

- 業務・システム最適化対象システムの構築において、その要求仕様策定段階で、情報セキュリティ要件定義（機能要件）及び保証要件の妥当性について、PMOにおいて組織的に評価・確認している。
- 情報システムが持つべき機能要件及び保証要件は、省の基準として、情報システムに応じて適用する複数の水準を米国防省の基準を参考に定めている。
- 策定した機能要件及び保証要件は、セキュリティを担当するCIO補佐官が確認し、省内審議委員会の承認を得ることとしている。

効果：　情報システムや取り扱う情報に適したセキュリティ機能装備の確保