DM-4-01-051

情報システムにおける情報セキュリティ対策実施規程

策定手引書

2006 年 3 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2006/3/31	初版

目次

1　本書の目的

本書は、府省庁において情報システムのライフサイクルにあわせて情報セキュリティ対策を実施する際に適用する規定（以下「情報システムにおける情報セキュリティ対策実施規程」という。）を整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（NISD-K303-052、以下「政府機関統一基準」という。）に準拠する省庁基準と、省庁基準を具体化する一連の実施手順群を整備することが求められている。「情報システムにおける情報セキュリティ対策実施規程」は、これらの実施手順の一つとして策定し、府省庁内において情報システムに情報セキュリティ対策を実施する場合に適用するものである。すなわち、情報システムセキュリティ責任者がこれに従うことにより、政府機関統一基準に基づく省庁基準の関係する規程を遵守することになるものである。

情報システムは、目的業務を円滑に遂行するため、情報システムのライフサイクルを通じて様々な要件を満たすことが必要となる。その要件の中には、情報システムのライフサイクルで発生する様々な脅威に対応するためのセキュリティの観点からの要件も含まれる。そして、セキュリティの要件を満足するためには、情報システムのライフサイクルを通じて適切な情報セキュリティ対策を実施し、実施した情報セキュリティ対策を PDCA サイクルによって、見直ししていかなければならない。

本書は、これらの背景の下で、「情報システムにおける情報セキュリティ対策実施規程」に含めるべき手順及び記述例を具体的に示し、もって統一基準及び省庁基準への準拠性、業務手順への適用性等において適切な規定の整備に資することを目的とする。

2　規定に記載すべき事項

「情報システムにおける情報セキュリティ対策実施規程」には、以下の事項を具体化する手順等を記載すること。

2.1　政府機関統一基準（NISD-K303-052）に定める情報システムにおける情報セキュリティ対策に係る遵守事項

4.3.1　情報システムのセキュリティ要件（１）情報システムの計画・設計
4.3.1　情報システムのセキュリティ要件（２）情報システムの構築・運用・監視
4.3.1　情報システムのセキュリティ要件（３）情報システムの移行・廃棄
4.3.1　情報システムのセキュリティ要件（４）情報システムの見直し

3　文書構成例

「情報システムにおける情報セキュリティ対策実施規程」は、以下の文書構成で作成することが考えられる。

1　本手順の目的
2　本手順の対象
　2.1　対象者
3　用語の定義
4　情報システムの計画
　4.1　体制の確保
　4.2　情報システムの分析
　4.3　情報システムのセキュリティ要件
　4.4　情報システムにおける情報セキュリティ対策の選択
5　情報システムの設計・構築
　5.1　設計・構築における情報セキュリティ対策
6　情報システムの運用
　6.1　運用における情報セキュリティ対策
7　情報システムの移行・廃棄
　7.1　移行・廃棄における情報セキュリティ対策
8　情報セキュリティ対策の見直し
　8.1　情報セキュリティ対策の見直し
9　ST 評価・ST 確認と IT セキュリティ評価及び認証制度の活用
　9.1　ST 評価・ST 確認の手続
　9.2　ISO/IEC15408 に基づく IT セキュリティ評価及び認証制度の利用

4　策定する上での留意事項

「情報システムにおける情報セキュリティ対策実施規程」は、以下のことに留意して策定する。

(1) 「情報システムにおける情報セキュリティ対策実施規程」は、府省庁における全ての情報システムと情報システムセキュリティ責任者が広く適用できる記述とすると利用しやすいものとなる。

(2) 「情報システムにおける情報セキュリティ対策実施規程」は、情報システムのライフサイクルに沿って記述すると理解されやすいものとなる。

5　参考資料

「情報システムにおける情報セキュリティ対策実施規程」の策定に際しては、以下の資料が参考となる。

5.1 国際規格及び諸外国を含む政府及び政府関係機関の資料

(1) ISO/IEC 17799「Information technology - Security techniques - Code of practice for information security management」(JIS X 5080)

(2) SLCP-JCF／共通フレーム 98（ISO/IEC 12207）

(3) 経済産業省「システム管理基準」

(4) IT セキュリティ評価及び認証制度 ISO/IEC 15408「Common Criteria」(JIS X 5070)

(5) 独立行政法人情報処理推進機構（IPA）IT セキュリティ評価及び認証制度（JISEC）
http://www.ipa.go.jp/security/jisec/index.html

5.2 政府以外の資料

(1) なし。

6 雛形の利用方法

別紙 1 の雛形を参考にして、「情報システムにおける情報セキュリティ対策実施規程」を策定すると効率的である。別紙 1 の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 統括情報セキュリティ責任者又は情報セキュリティ責任者が規程を策定することを想定している。
- 情報システムセキュリティ責任者が規程を利用することを想定している。
- 大規模な情報システム等であり、情報システムのライフサイクルにおける業務を外部委託する場合、「外部委託におけるセキュリティ対策実施規程」に記載された事項を考慮するべきである。
- 個別の情報セキュリティ対策の適用に関する詳細については、別途情報セキュリティ関係規程を定め、これを遵守することを要求する必要がある。

6.2 手直しポイント

「情報システムにおける情報セキュリティ対策実施規程」を策定するに当たり、以下の点について手直しをする必要がある。

(1) 雛形において/・・・/ 形式で示す設定値（担当者名、手順書名等）については、各府省庁内の定めに合わせる。

(2) 雛形において【・・・の場合】形式で示す記述については、想定される案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

(3) 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。

(4) 雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜、補う。