DM6-01-071

機器等の購入における情報セキュリティ対策実施規程

策定手引書

2007 年 11 月

内閣官房情報セキュリティセンター

改訂履歴

改定日	改定理由
2006/3/31	初版
2006/6/16	IT セキュリティ評価及び認証制度に基づく認証の取得を製品の選択に利用する際の参考資料を追記（5 章）。
2007/11/9	政府機関統一基準(第２版)の策定等に伴う修正等

目次

1　本書の目的

本書は、情報機器及びソフトウェア（以下機器等という。）の購入に伴う情報セキュリティ関係の手続を定める規程（以下「機器等の購入における情報セキュリティ対策実施規程」という。）を統括情報セキュリティ責任者が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(第２版)」（NISD-K303-071、以下「政府機関統一基準」という。）に基づく省庁対策基準及び関係する規定を整備することが求められている。一方、府省庁の業務を円滑に遂行するためには必要な手順を具体的に示した実施手順を整備することが望まれることから、当該実施手順に従い業務を行えば結果として省庁対策基準も遵守することとなる手順書を策定することが適切である。「機器等の購入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、機器等の購入における情報セキュリティ対策の実施に適用するものである。

府省庁においてサーバ装置、端末、通信回線装置、ソフトウェアその他の機器等を購入して業務に使用する場合には、これらの機器等に情報を保有し、また機器等を介して行政事務従事者が府省庁の情報へアクセスすることとなるため、必要なセキュリティ機能が装備されていない場合や購入後に情報セキュリティ対策が継続的に行えない場合は、情報セキュリティが維持できなくなるおそれがある。このため、機器等の購入に当たっては、情報セキュリティ維持の観点から適切な機器等を選定することが求められる。

本書は、これらの背景の下で、「機器等の購入における情報セキュリティ対策実施規程」に含めるべき事項を具体的に示し、もって適切な規定の整備に資することを目的とする。

2　規程に記載すべき事項

「機器等の購入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して記載すること。

2.1　政府機関統一基準（NISD-K303-071）に定める機器等の購入に係る遵守事項

6.1.1　機器等の購入　(1) 情報セキュリティ確保のための府省庁内共通の仕組みの整備

6.1.1　機器等の購入　(2) 機器等の購入の実施における手続

3 文書構成例

「機器等の購入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 本規程の目的
2 本規程の対象者
3 本規程を適用する機器等の購入の範囲
4 機器等に求めるセキュリティ要件
  4.1 求めるセキュリティ要件の原則
  4.2 標準的に求めるべきセキュリティ要件
  4.3 機器等に求めるセキュリティ要件の決定
5 機器等の選定
6 機器等の納入時の確認
7 機器等の保守・点検等
8 本規程に関する相談窓口

付録 機器等に標準的に求めるセキュリティ要件

4 策定する上での留意事項

「機器等の購入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。

4.1 適用範囲

「機器等の購入における情報セキュリティ対策実施規程」は、府省庁における機器等の購入に適用するものとする。機器等とは、情報機器等及びソフトウェアをいう（政府機関統一基準「1.1.3 用語定義」）。

機器等の例：

- サーバ装置関連
  - サーバ装置
  - オペレーティングシステム（OS）
  - ミドルウェア（DBMS、アプリケーションサーバ、グループウェア、運用管理ソフトウェア、セキュリティ対策ソフトウェア等）
  - 汎用アプリケーションプログラム（ウェブサーバ、メールサーバ等）
  - 業務プログラム
- 端末関連（PCを含む）
  - 端末装置
  - オペレーティングシステム（OS）
  - ミドルウェア（運用管理ソフトウェア、セキュリティ対策ソフトウェア等）
  - 汎用アプリケーションプログラム（ブラウザ、メーラ、文書処理プログラム等）

- ○ 業務プログラム
- 通信回線装置
  - ○ ファイアウォール
  - ○ ルータ、スイッチ
- 複合機（印刷機能及びファクシミリ機能をあわせ持つ機器等）
- 電磁的記録媒体
  - ○ CD、DVD
  - ○ USBメモリ

4.2 求められる情報セキュリティ対策

機器等の購入においては以下の情報セキュリティ対策が求められるため、これらを機器等の選定基準に含めること。

(1) 当該機器等が、求められるセキュリティ機能要件を満足するセキュリティ機能を持つこと。

(2) 情報セキュリティの維持のためセキュリティ修正（脆弱性を解消するための修正）を適用する必要があるソフトウェアの場合には、以下の条件を満たすこと。

- 納品時に必要なセキュリティ修正が適用されていること。
- 納品後に必要なセキュリティ修正が継続的に提供され、適用できること。

(3) 情報セキュリティの維持に保守・点検等が必要な機器等の場合には、納品後に保守・点検等が購入先又は他の事業者により行われること。

4.3 情報システムとの関係

機器等は、情報システムの構成要素となる。情報システムにおけるセキュリティ要件の一部は個々の機器等に対するセキュリティ機能要件となるため、機器等の購入においては、当該セキュリティ機能要件を満足するセキュリティ機能を持つものを選定する必要がある。なお、情報システムにおけるセキュリティ要件の全体は、個々の機器等が有するセキュリティ機能のみによって満足されるわけではなく、機器等が保有する機能を利用すること並びに、安全区域等の物理的対策、組織及び人の運用による対策その他情報システムをとりまく様々な対策を実施することにより満足されることとなる。

情報システムの構築とは別に購入する機器等においても、ネットワークを通して情報システムに接続し、又は電磁的記録媒体により情報の移入・移出を行う等により情報システムの構成要素となるため、情報システム全体についての情報セキュリティ維持の観点から、その購入において適切な選定を行うことが求められる。

4.4 機器等の種類に応じた対策の適用

求められる情報セキュリティ対策及び選定基準については、当該対策の確実な実施及び事務の軽減を図るため、機器等の種類ごとに標準的なセキュリティ要件及び選定

基準を示し、情報システムセキュリティ責任者の利用に供することが望ましい。

4.5　汎用製品等の選定における判断結果の記録

セキュリティ要件への対応については、必ずしも機器等の購入の都度判断する必要はない。多くの場合に過去の判断結果が有効であるため、判断結果の記録を残すことにより、爾後の負担を軽減することができる。特に、汎用のサーバ装置、端末及びソフトウェアについては、過去の判断結果が参考になる場合が少なくないものと想定される。

5　参考資料

「機器等の購入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。

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

本参考資料は、IT 製品・システムにセキュリティ機能が実装されていることを国際的に合意された規格である ISO/IEC 15408 (Common Criteria) に基づき評価し、認証するための制度に関して解説したものである。

(2) 『情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書』
内閣官房情報セキュリティセンター、2007 年 11 月

本参考資料の「付録 C　IT セキュリティ評価及び認証制度を活用した機器等の購入について」に、機器等の購入において IT セキュリティ評価及び認証制度及び認証製品リストを利用する際の考慮事項及び参考情報が記載されている。

6　雛形の利用方法

別紙１の雛形を参考にして、「機器等の購入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。

機器等の購入においては求めるセキュリティ要件を満足するか否かを判断することになるが、必ずしも購入の都度判断する必要はなく、過去の判断を参考にしてよい場合が多い。このため、以下の方法により手続の簡略化を図っている。

(1) 機器等の種類ごとに標準的に求めるセキュリティ要件を府省庁において策定し、

利用する。

(2) セキュリティ要件に照らした判断の結果を記録し、爾後の参考とする。

6.2 手直しポイント

(1) 雛形において*[・・・]* 形式で示す設定値（組織名等）については、各府省庁内の定めに合わせる。

(2) 既存の調達関連その他の規定との整合性を考慮し、適切に統合、相互参照する。