DM6-01-071

別紙１：雛形

機器等の購入における情報セキュリティ対策実施規程

雛形

2007 年 11 月

内閣官房情報セキュリティセンター

本書の位置付け

本書は、「機器等の購入における情報セキュリティ対策実施規程」を策定する場合の雛形であり、「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」の 2 に示す規程に記載すべき事項を、同 3 に示す文書構成例の枠組みの中に記載したものである。

本書の利用方法

本書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。
  - 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（付録）。
  - 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。

手直しポイント

「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（組織名等）については、各府省庁の定めに合わせる。
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。
③ 雛形に記載した［6.1.1(1)(a)］等の項番は、「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) の該当する項番である。雛形を利用して策定する規定には、含めなくてよい。

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

商標について

- UNIX は、米国及びその他の国における The Open Group の登録商標又は商標です。
- Linux は、Linus Torvalds の米国及びその他の国における登録商標又は商標です。
- Windows は、米国 Microsoft Corporation の、米国、日本及びその他の国における登録商標又は商標です。

目次

1　本規程の目的

*［○○省］*において情報機器及びソフトウェア（以下機器等という。）を購入して業務に使用する場合には、これらの機器に情報を保有し、また機器を介して行政事務従事者が*［○○省］*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。

本規程は、機器等の購入において情報セキュリティの観点から行うべき手続を定め、もって*［○○省］*における情報セキュリティの確保に資することを目的とする。

2　本規程の対象者

本規程は、購入する機器等を構成要素とすることとなる情報システムの情報システムセキュリティ責任者を対象とする。

3　本規程を適用する機器等の購入の範囲

(1) 本規程は、*［○○省］*における機器等の購入に適用する。

(2) 本規程における機器等の購入には、リース契約等、売買契約以外の方法による機器等の調達を含む。

(3) 本規程における機器等の購入には、情報システムの構築を外部委託により行う場合であって、当該委託にあわせて機器等を購入する場合を含む。

4　機器等に求めるセキュリティ要件

［政府機関統一基準 6.1.1(1)(a)］

4.1　求めるセキュリティ要件の原則

購入する機器等は、原則として、情報セキュリティの観点から以下のセキュリティ要件を満たすものであること。

(1) 求められるセキュリティ機能を持つこと

当該機器等に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。

【規程利用者への補足説明】

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当該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。

(2) セキュリティ修正が提供されること

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に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。

UNIX®、Windows® を含むオープン系システムではなく、メインフレームシステム等で稼動するソフトウェアについては、その脆弱性が指摘されることは一般にないため、セキュリティ修正の提供を求める必要はない。

(3) その他の保守・点検等が行われること

以下の保守・点検等のうち、情報システムセキュリティ責任者が情報セキュリティの確保に必要と認めるものが適用可能であること。

- 情報機器の保守・点検等
- ソフトウェア及びファームウェアの修正及び更新の提供
- 情報システムセキュリティ責任者が必要と認めた機器等の脆弱性検査

4.2 標準的に求めるべきセキュリティ要件

前節の原則に基づき、機器等に標準的に求めるセキュリティ要件を「機器等に標準的に求めるセキュリティ要件」のとおりに定める。本要件は、統括情報セキュリティ責任者が定め、維持する。「機器等に標準的に求めるセキュリティ要件」については、付録を参照されたい。

なお、「5 機器等の選定」の手続において、本要件を満たすものと確認した機器等について確認したことの記録を本要件とあわせて維持し、爾後の利用に供することも、手続の簡略化に有効である。

4.3 機器等に求めるセキュリティ要件の決定

［6.1.1(1)(a)］

情報システムセキュリティ責任者は、機器等の選定に当たり、以下の手順で当該機器等に求めるセキュリティ要件を定めること。

(1) 当該機器等の利用方法に照らして、「機器等に標準的に求めるセキュリティ要件」を採用することが適切であるか否かを判断すること。

(2) 「機器等に標準的に求めるセキュリティ要件」を採用しない場合には、以下の手続を踏むこと。

- 同表中「(1) セキュリティ機能を持つこと」の内容を採用しない場合には、当該機器等に求めるセキュリティ機能要件を定めた上で、これに基づき求めるセキュリティ機能を定めること。
- 同表中「(2) セキュリティ修正が提供されること」の内容を採用しない場合には、それに代わるセキュリティ要件を定めること。
- 同表中「(3) その他の保守・点検等が行われること」の内容を採用しない場合には、それに代わるセキュリティ要件を定めること。

5 機器等の選定

(1) 情報システムセキュリティ責任者は、「4.3 機器等に求めるセキュリティ要件の決定」で定めたセキュリティ要件を情報セキュリティ以外の要件に加味して機器等を選定すること。［6.1.1(2)(a)］
なお、「機器等に標準的に求めるセキュリティ要件」を採用した場合で、当該要件を満たすものであると確認した機器等について確認したことの記録を残し、爾後の利用に供することは、手続の簡略化に有効である。

(2) 情報システムセキュリティ責任者は、機器等について満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行うときは、当該要求仕様への対応について IT セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用すること。［6.1.1(2)(d)］

- ITセキュリティ評価・認証制度とは、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であり、独立行政法人情報処理推進機構（IPA）が運営している。
http://www.ipa.go.jp/security/jisec/index.html
認証を取得している場合には、製品名等製品を特定する情報及び認証番号を購入先の事業者に報告させること。認証取得は、上記ウェブページにある認証製品リストで確認することができる。
認証取得の範囲が、当該機器等に求めるセキュリティ機能要件と合致していることを確認する必要がある。

  なお、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ことについては、以下の資料もあわせて参照されたい。
  - ○ 「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）

6 機器等の納入時の確認

［6.1.1(1)(b)、(2)(b)］

(1) 情報システムセキュリティ責任者は、機器等の納入を受けるに際して、当該機器等に求めるセキュリティ要件を満たしていることを必要に応じて確認し、その結果を納品検査における判断に加えること。確認する事項は、以下に挙げるもののうち必要と認めるものとすること。

- 求めるセキュリティ機能が装備されていることを、納入される仕様書の査

閲、機器等の操作等により確認する。

- セキュリティ修正が最近のものまで適用されていることを、納入される仕様書の査閲等により確認する。
- 保守・点検等が行われることを、納入される仕様書の査閲等により確認する。

7　機器等の保守・点検等

［6.1.1(2)(c)］

(1) 情報システムセキュリティ責任者は、情報セキュリティ対策に関する保守・点検等が必要であると認めた場合には、機器等の購入先又は他の事業者に保守・点検を行わせること。
当該手続は、府省庁において行うこととした事項を除き、*［「外部委託における情報セキュリティ対策実施規程」］*に従うこと。

8　本規程に関する相談窓口

(1) 情報システムセキュリティ責任者は、緊急時の対応又は本規程の内容を超えた対応が必要とされる場合には、統括情報セキュリティ責任者に相談し、指示を受けること。

(2) 情報システムセキュリティ責任者は、本規程の内容について不明な点又は質問がある場合には、統括情報セキュリティ責任者に連絡し、回答を得ること。

付録　機器等に標準的に求めるセキュリティ要件

「4.2 標準的に求めるべきセキュリティ要件」の内容を以下のとおりに定める。表中の(1)、(2)及び(3)の意味については「4.1 求めるセキュリティ要件の原則」を参照されたい。

	機器等の種別		(1) セキュリティ機能を持つこと	(2) セキュリティ修正が提供されること	(3) その他の保守・点検等が行われること
1	サーバ装置関連	サーバ装置（ハードウェア）	利用目的に応じた信頼性を持つものであること。 例：内蔵する記録装置が、適切な RAID であること等。	―	保守・点検等がなされること。
2		オペレーティングシステム（OS）	当該ソフトウェアについて「取り扱う情報」「管理者」及び「利用者」に着目した、 ①主体認証機能、 ②アクセス制御機能、 ③権限管理機能及び ④証跡管理機能 を持つこと。 なお、UNIX® 系 OS（Linux® を含む。）及び Windows® は、これらの機能を持つものと認められる。	必要 ただし、メインフレームシステム等、オープン系システム以外のものには適用しない。	ソフトウェアの修正及び更新が提供されること。
3		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）			
4		汎用アプリケーションプログラム（メールサーバ、ウェブサーバ等）			
5		業務プログラム	当該プログラムごとに判断すること。	個別に必要性を判断すること。	個別に必要性を判断すること。
6	端末関連	端末（ハードウェア）	―	―	保守・点検等がなされること。
7		オペレーティングシステム（OS）	当該ソフトウェアについて「取り扱う情報」「管理者」及び「利用者」に着目した、 ①主体認証機能、 ②アクセス制御機能、 ③権限管理機能及び ④証跡管理機能 を持つこと。 UNIX® 系 OS（Linux® を含む。）及び Windows® は、これらの機能を持つものと認められる。	必要	ソフトウェアの修正及び更新が提供されること。
		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）		必要	
8		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）		必要	
9		業務プログラム	当該プログラムごとに判断すること。	個別に必要性を判断すること。	個別に必要性を判断すること。
10	通信回線装置	ファイアウォール	上記「サーバ装置関連」のミドルウェアと同じ。	必要	ソフトウェア及びファームウェアの修正及び更新が提供されること。 機器について保守・点検等がなされること。
		ルータ、スイッチ等	装置ごとに必要なセキュリティ機能を判断する必要がある。	個別に必要性を判断すること。通信プロトコルを取り扱うファームウェア等に関して修正が必要になる場合がある。	

11	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）	府省庁内 LAN を外部ネットワークに接続することにより、外部から府省庁内 LAN へ侵入する手段となる可能性に留意し、要求仕様を策定すること。例えば、府省庁内 LAN とファクシミリ送信に使用する外部ネットワークが、当該複合機の内部において物理的に接続されることとならないこと。 修理等のために複合機又はそのハードディスク等記録媒体を搬出することを想定し、必要に応じ、記録媒体内の情報の漏えいを防止する機能を持つものであること。	個別に必要性を判断すること。汎用の OS を搭載している場合等に必要になり得る。	個別に必要性を判断すること。
12	電磁的記録媒体	必要に応じ、情報の移送及び府省庁外での情報処理に使用するものについて、暗号化機能を持つものであること。	―	―