第１２２回月例研究会報告　　報告者 1186 宮下重美

日時：２００６年８月２日（火）１８：３０～２０．００
場所：中央大学駿河台記念館　２８１号室
演題：「政府機関の情報セキュリティ対策のための統一基準」
講師：内閣官房情報セキュリティセンター・内閣参事官補佐：佐藤慶浩氏

１．概要

「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）について、策定メンバーの「内閣官房情報セキュリティセンター」佐藤慶浩氏が、そのポイントを講演した。

２．講演要旨

①これまでは、“政府機関における情報セキュリティ対策”を問われても、政府機関により異なりますと答えざるを得なかったが、今回の統一基準により“各政府機関では最低基準が策定されており、これ以上の対策基準を追加している機関があります”と回答できる状況となった。
即ち、この統一基準は、政府各府省庁の「情報セキュリティ対策内容の整合化・共通化」を促進するために、各府省庁がとるべき情報セキュリティ対策を定めたものである。

②この統一基準は、４階層ある「政府機関統一基準文書群」の一つの階層である。
第１部から第 6 部までの構成となっている。総則、組織と体制の構築、情報についての対策、セキュリティ要件の明確化に基づく対策、情報システムの構成要素についての対策、個別事項について、となっている。詳細は、次のＵＲＬで入手できる。
http://www.nisc.go.jp/active/general/kijun01.html　＜公式ウェブページ＞
http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf＜解説書＞
前者の URL で、関連する各種情報を入手できる。
後者の解説書は、本基準の理解を助けるための参考・詳細資料であり、分り易い説明を逐条解説として追加している。

③政府機関統一基準文書群により、次が期待できる。
・各府省庁においては、政府機関統一基準に準拠して、自らの情報セキュリティポリシー（省庁ポリシー）の見直しを図り、対策の底上げを図ることができる。
・省庁ポリシーを反映した多数の実施手順書等を各府省庁が作成するうえで、手引き又は参考となり、各府省庁の利用に供することができる。
・各府省庁自らが行う自己点検と監査に基づく評価、当該評価結果をもとに情報セキュリティ政策会議が行う勧告、これらを受けて政府機関統一基準と省庁ポリシーを見直す、というＰＤＣＡサイクルの取組みが可能となる。

④この統一基準は政府機関用であり政府以外の利用を意図していないものであるが、政府以外の情報セキュリティ対策基準としても、取扱に注意しながら活用することも可能である。

３．講演の内容

（１）　政府機関統一基準文書群と政府機関統一基準
政府機関統一基準は、次に示すように、統一基準文書群の一つであり、４階層からなる。
①政府基本方針　　②統一基準運用基準　　③政府機関統一基準

④個別マニュアル群　（文書番号　K303）

なお、④は、2006年8月以降に、公開予定である。

（２） 政府機関統一基準の構成

第１部：総則　第２部：組織と体制の構築

第３部：情報についての対策　第 4 部：セキュリティ要件の明確化に基づく対策、

第５部：情報システムの構成要素についての対策

第６部：個別事項についての対策

これらは、“主たる対象者”　→“おおむね頻度”と対応する。

第２部：　総括　→年次

第３部：　全従事者　→日常業務

第４・５部：情報システム関係者　→情報システムのライフサイクル。段階毎

第６部：　各事項による　→各項目による

（３） 政府機関統一基準「第１部：総則」の構成

1.1.1　本統一基準の位置付け

構成と位置付け、個別マニュアルとの関係、各府省庁基準への反映適用対象範囲、などを述べる。

1.1.2　本統一基準の使い方

全体構成は、部・節・項－趣旨（必要性）－遵守事項（遵守事項本文・解説）となっている。

対策レベルの設定は、“当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない“として、次の「基本遵守事項」「強化遵守事項」で構成している。

a) 「基本遵守事項」は､保護すべき情報とこれを取り扱う情報システムにおいて、必須として基準化すべき対策事項

b) 「強化遵守事項」は､特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して基準化すべき対策事項

1.1.3　用語定義

本統一基準では、独自の用語使用があるので、もしも政府外で利用するのであれば確認が必要である。

（４） 政府機関統一基準「第２部：組織と体制の構築」の構成

2.1　導入　組織・体制の確立、役割の分離、違反と例外措置

2.2　運用　情報セキュリティ対策の教育、障害等の対応

2.3　評価　情報セキュリティ対策の自己点検、監査

2.4　見直し　情報セキュリティ対策の見直し

（５） 政府機関統一基準「第３部：情報についての対策」の構成

3.1　情報の格付け

情報セキュリティ委員会は、“行政事務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること“としている。

3.2　情報の取扱

情報の取扱について、情報のライフサイクルに沿って、作成・入手．利用．保存．移送．提供．消去．について述べている。

例えば、「情報の作成・入手」においては、“その業務以外の情報の作成又は入手の禁止、情報の作成又は入手時における格付けの決定と取扱制限の検討、格付けと取扱制限の明示、格付けと取扱制限の継承、格付けと取扱制限の変更、など”

を述べている。

（6） 政府機関統一基準「第４部：情報セキュリティ要件の明確化に基づく対策」の構成

4.1　情報セキュリティの機能：主体認証機能から暗号と電子署名など６項目

具体的には、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能、保証のための機能、暗号と電子署名について述べている。

なお、ここで述べている「遵守事項」は“if ,then 構造”により、

例えば、次のような記述構造を採用している。

(a) ○○○を行う必要性の有無を検討すること

(b) ○○○を行う必要性があると求めた情報システムには、○○○を行う機能を設けること。

これは、自己点検・監査の際に問題があった場合に、(a)の検討の問題なのか、(b)の実施の問題なのかを切り分けて責任の所在を明確にするためである。

4.2　情報セキュリティの脅威：セキュリティホール対策など３項目

具体的には、セキュリティホール対策、不正プログラム対策、サービス不能攻撃対策、について述べている。

4.3　情報システムのセキュリティ要件：情報システム計画・設計など４項目。

具体的には、情報システムのライフサイクルに沿って、情報システム計画・設計．構築・運用・監視．移行・廃棄．見直し、について述べている。

（7） 政府機関統一基準「第５部：情報システムの構成要素についての対策」の構成

5.1　施設と環境　施設設備の安全区域と対策管理

5.2　電子計算機　電子計算機．端末．サーバ類の設置・運用・終了時の対策

5.3　アプリケーションソフトウェア　通信回線介在のアプリ．電子メール．ウェブの導入・運用時の対策

5.4　通信回線　通信回線．府省庁内．府省庁外回線の構築・運用時対策

（8） 政府機関統一基準「第６部：個別事項についての対策」の構成

6.1　調達・開発にかかわる情報セキュリティ対策

機器等の購入、外部委託、ソフトウェア開発

6.2　個別事項

府省庁外での情報処理の制限,支給以外の情報処理の制限

6.3　その他

府省庁外の情報セキュリティ水準の低下を招く行為の防止、事業継続計画(BCP)との整合的運用の確保など

（9） その他

統一基準作成時の配慮事項、もしも政府機関以外で活用を考える場合の方法について、講演された。

この統一基準は政府機関用に策定しているが、あえて民間事業者等が利用するとした場合、利用価値があるとのことである。

「政府機関以外での活用方法」の要点（活用ポイント・注意点）は次のとおり。

DO：①情報セキュリティ対策体制の修正検討

②情報の対象の修正検討

③格付け・取扱制限表・明示の定義の修正検討

④定義用語の修正検討

⑤一括置換が可能である。　例：　行政業務→業務

⑥強化遵守事項の取捨選択　など

DONOT

① 部・節・項の構成を変更しない。

② 主語をセキュリティ体制上の役割以外にしない

（具体的な組織名等としないこと）

③ 述語を統合しない。

以下、省略

４．感想

①情報セキュリティ政策会議が国として策定した「政府機関の情報セキュリティのための統一基準」の取組み姿勢、概要、がわかり易く講演され理解できた。特に、我々の関心が深い部分であり、その基本的な考え方、構成、構造、編集手法について、研鑽資料を提供していただき、感謝申しあげたい。

②この統一基準を府省庁基準として使用する際の関係を“標識（＝本統一基準）と運転席（＝各府省庁）”で例えている点は興味深いものがあった。

③本統一基準において、年度計画・情報のライフサイクル・情報システムのライフサイクルを“フラクタルなＰＤＣＡ”として捉えている。

この統一基準では「リスクアセスメント」という表現がでてこない。“情報の対策レベルの設定、格付けを日常業務の中で全員参加により行うことが「リスク判断」である”との意味をこめているとしている。リスクアセスメントに関わる一つの実行形式が示されたと考える。

④この統一基準の第４部・第５部の遵守事項はそのままチェックリストとして使用が可能である。即ち、教育理解度の再確認としての自己点検、オンタイム・チェックリストとしての自己点検に利用できるものであり、この便利さと活用が注目を引いた。

⑤この統一基準を活用することにより“専任監査者でなくてもある程度の監査が実施でき、監査専門家はさらに高レベル・高品質の監査業務に専念できる可能性がある”ことが示唆され、一つの活用の発想が示された、と考える。

以上、貴重なご講演に感謝申しあげたい。

以上

編集・発行　NPO 法人 日本システム監査人協会　月例研究会・会報編集部
事務局　tel. 03-3666-6341　Fax.03-3666-6342　saajjk1（at）titan.ocn.ne.jp