情報セキュリティ対策統一基準及び各省庁の情報セキュリティ基準の分析と、それに対応する ISMS の活用について

研究員　榊　　勝

ISMS 認証審査(情報セキュリティマネジメントシステムが国際規格 ISO/IEC27001 (JISQ27001)に適合し、有効であることを審査する)において、BSK 審査員として、被認証組織を審査した際に、業務リスク評価のベースラインアプローチにおいて、JISQ27001 附属書Ａ113 項目と、ある政府機関の情報セキュリティ基準 70 項目に基づきリスク評価している現状を経験したことから、今回、ISMS 審査員の立場から政府機関の統一基準及び各省庁の情報セキュリティ基準とはどのような内容なのか比較・確認し、ISMS との関連性について検証するとともに政府機関の情報セキュリティ体制の構築・維持に ISMS を活用する方策について検証することとする。

１．各省庁における情報セキュリティの始まりと変遷

【各省庁の試行錯誤】

平成 12 年 1 月頃、各省庁のホームページが連続改ざんされる事件の多発が始まる。

2 月、内閣官房情報セキュリティ対策推進室が設置された。

その後、Web サーバの脆弱性への攻撃が連続して発生した。

7 月、政府機関対策として、情報セキュリティ対策推進会議において「情報セキュリティポリシーに関するガイドライン」が決定された。

12 月、重要インフラ対策として、情報セキュリティ対策推進会議において「重要インフラのサイバーテロ対策に係る特別行動計画」が決定された。

平成 13 年 9 月、米国同時多発テロの発生に伴い、政府レベルのサイバー攻撃への対応を中心とした対策が本格的に始動した。

【サイバー攻撃への対応を中心とした対策の実施】

平成 13～17 年、基本戦略に基づき策定する年度計画により対策を実施

平成 17 年 4 月、内閣官房情報セキュリティセンター設置

5 月、情報セキュリティ政策会議設置

【IT 障害への対応も含めた総合的な対策基盤づくりの推進】

平成 17 年 12 月､政府機関の情報セキュリティ対策のための統一基準(第１～３版)の決定

重要インフラの情報セキュリティ対策に係る行動計画の決定

【サイバー攻撃事態発生を念頭にした新たな環境変化への対応】

平成 21 年 2 月、政府機関統一基準(第４版)の決定

重要インフラの情報セキュリティ対策に係る第２次行動計画の決定

平成 23 年 4 月、政府機関の情報セキュリティ対策のための統一規範の決定

政府機関の情報セキュリティ対策のための統一管理基準の決定

平成26年5月、 政府機関の情報セキュリティ対策のための統一基準の策定
平成26年５月19日 情報セキュリティ政策会議

２．政府機関の統一基準

2014 年 5 月に策定された政府機関の情報セキュリティ対策のための統一基準の構成、位置付け、基本方針及び特徴を大枠的に確認することとする。

（１）政府機関の情報セキュリティ対策のための統一基準の全体構成

1）総則
①統一基準の目的、②統一基準の適用範囲、③統一基準の改訂、④法令等の遵守
⑤対策項目の記載事項、⑥情報の格付の区分、⑦情報の取扱制限、⑧用語定義
2）情報セキュリティ対策の基本的枠組み
①導入・計画(組織と体制の整備)、②運用、③点検、④見直し
3）情報の取扱い
①情報の取扱い、②情報を取扱う区域の管理
4）外部委託
①外部委託
5）情報システムのライフサイクル
①情報システムの企画・要件定義、②情報システムの調達・構築
③情報システムの運用継続計画
6）情報システムのセキュリティ要件
①情報システムのセキュリティ機能、②情報セキュリティの脅威への対策
③アプリケーション・コンテンツの作成・提供
7）情報システムの構成要素
①端末・サーバ装置等、②電子メール・ウェブ等、③通信回線
8）情報システムの利用
①情報システムの利用、②府省庁支給以外の端末の利用

（２）統一基準の位置付け

当該統一基準は、政府機関全体の統一的な枠組みを構築し、それぞれの府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要であることから、「政府機関の情報セキュリティ対策のための統一規範」(平成26年５月19日付情報セキュリティ政策会議決定)に基づく政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準として定められたものである。

（３）統一基準制定(平成 26 年５月 19 日)時の基本方針

制定時の基本方針は、次のとおりである。

① 政府機関統一基準は、原則として、全ての府省庁において共通的に必要とされる情報セキュリティ対策を包含するものとして策定する。
② 政府機関統一基準は、責任体制、実施体制及び対策内容について、各府省庁が準拠で

きるように、各府省庁の実状を踏まえて策定する。
③ 政府機関統一基準は、国際的な基準等との整合性に配慮して策定する。

（4）統一基準の特徴

先ずは、大きくは、次のように対象情報を中心にＰＤＣＡ的に展開している。

・情報の格付の区分及び取扱制限→・情報セキュリティ対策の基本的枠組み(組織と体制の整備→運用→点検→見直し)→・情報の取扱い→・情報を取扱う区域の管理→・外部委託

次に、その対象情報を取扱う情報システムについては、・情報システムのライフサイクル→・情報システムのセキュリティ要件→・情報システムの構成要素→・通信回線→・情報システムの利用と詳細に展開している。

統一基準制定(平成 26 年５月 19 日)時に、取り巻く環境の変化に対応して、対象情報を取扱う情報システムの管理策について詳細に規定している。

３．各省庁の情報セキュリティ基準の特徴・対応範囲の確認

主要な省庁の情報セキュリティ基準をリストアップすると次のようになる。

省庁名	情報セキュリティ基準名：上段	基本・主要構成：下段
環境省	環境省情報セキュリティポリシー（第 7 版）26.10.27 特徴：JIS Q 27001 の本文（第 4 項から第 10 項）基本事項に対応したものであり、管理策については、附属書Ａ（A.5～A.17）の情報システムの管理策を中心に展開されている。	
	1）総則・情報セキュリティ基本方針	2)情報の格付の区分・取扱制限
	3）用語定義	4）組織・体制の整備
	5）ポリシー・対策推進計画の策定	6）情報セキュリティ関係規程の運用
	7）例外措置	8）教育
	9）情報セキュリティインシデントへの対処	10）情報セキュリティ対策の自己点検
	11）情報セキュリティ監査	12）情報セキュリティ対策の見直し
	13）情報の取扱い．	15）外部委託
	14）情報を取り扱う区域の管理	16）約款による外部サービスの利用
	17）ソーシャルメディアサービスによる情報発信	18）情報システムに係る台帳等の整備
		19）機器等の調達に係る規定の整備
	20）情報システムの企画・要件定義	22）情報システムの運用・保守
	21）情報システムの調達・構築	25）情報システム運用継続計画の整備・整合的運用の確保
	23）情報システムの更改・廃棄	
	24）情報システムについての対策の見直し	26）情報システムの運用継続計画
	27）情報システムのセキュリティ機能	28）情報セキュリティの脅威への対策
	29）端末・サーバ装置等	30）電子メール・ウェブ等
	31）通信回線	32）情報システムの利用
	33）環境省支給以外の端末の利用	

総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 27 年 3 月版）27.3.27 特徴：JIS Q 27001 の本文（第 4 項から第 10 項）、及び附属書Ａ（A.5～A.17）の管理策における、それぞれの主要な事項を中心に展開されている。
	1)策定及び導入　2)運用 3)評価・見直し　4)本ガイドラインの構成と対策レベルの設定 5)情報セキュリティ基本方針 6)情報セキュリティ対策基準　7)物理的セキュリティ 8)人的セキュリティ　9)技術的セキュリティ 10)運用　11）外部サービスの利用 12）評価・見直し　13)用語の定義
経済産業省	情報セキュリティ管理基準（平成 20 年改正版） 特徴：統一管理基準に沿った内容となっている。
	マネジメント基準 1）情報セキュリティマネジメントの確立 2）情報セキュリティマネジメントの導入と運用 3）情報セキュリティマネジメントの監視およびレビュー 4）情報セキュリティマネジメントの維持および改善 5)文書管理および記録の管理 管理策基準 1)セキュリティ基本方針　2）情報セキュリティのための組織 3)資産の管理　4)人的資源のセキュリティ 5)物理的及び環境的セキュリティ　6)通信及び運用管理 7)アクセス制御　8)情報システムの取得、開発及び保守 9)情報セキュリティインシデントの管理　10)事業継続管理 11)順守
警察庁	警察情報システムの情報セキュリティ要件について（通達平成 25 年 3 月 7 日） 特徴：警察情報及び情報システムに特化した管理策の展開となっている。
	1)目的　2)用語の定義　3)物理的対策　4)利用者認証　5)暗号　6)ネットワーク　7)サーバ等　8)不正プログラム対策　9)電子メール及びウェブ 10)外部記憶媒体の利用　11)証跡の取得　12)モバイル端末　13）設計、調達、運用及び廃棄　14)機器の購入 15)プログラム開発 16)外部委託 17)ドキュメント及び記録簿　18)経過措置　19)例外　20）警察庁と接続されないシステム
防衛省	装備品等及び役務の調達における情報セキュリティの確保について（平成 23 年 12 月 28 日） 特徴：防衛省の保護すべき情報及び情報システムに特化した管理策の展開となっている。

	1)趣旨　2)定義　3)対象　4) 情報セキュリティ基本方針等の作成 5) 情報セキュリティ基本方針等　6)組織のセキュリティ 7)保護すべき情報の管理　8)人的セキュリティ 9)物理的及び環境的セキュリティ　10)通信及び運用管理　11)アクセス制御 12) 情報セキュリティ事故等の管理　13)遵守状況等

４．統一基準に対する主要省庁の情報セキュリティ基準の分類

主要省庁の情報セキュリティ基準を大別すると、次のような分類・特徴となる。

区分	該当基準	特徴
ケース１	環境省、経済産業省のように、殆ど、統一基準に沿った内容の情報セキュリティ基準	統一基準の特徴である対象情報を中心にＰＤＣＡ的に展開している。
ケース２	総務省、警察庁、防衛省のように、当該省庁の情報及び情報システムに特化した管理策を中心とする情報セキュリティ基準	当該省庁の対象情報に特化した管理策の展開となっており、取り巻く環境の変化に対応して，対象情報を取り扱う情報システムの管理策について詳細に規定している。

５．統一基準と ISMS との比較

(1) 次に「統一基準」と、国際規格である｛ISMS：JISQ27001:2014｝とを大枠的に比較することとする。

統一基準	ISMS：JIS Q 27001:2014
統一基準の目的・適用範囲	1 適用範囲
・目的　・適用範囲　・改訂　・法令等の遵守　・対策項目の記載事項	4.3 情報セキュリティマネジメントシステムの適用範囲の決定
情報の格付の区分及び取扱制限	
・情報の格付の区分	A.8.1.1　資産目録
・情報の取扱制限	A.8.1.3　資産利用の許容範囲
情報セキュリティ対策の基本的枠組み	
・導入・計画 ① 導入 ・組織と体制の整備 ・府省庁対策基準と対策推進計画の策定 ②運用 ・情報セキュリティ関係規程の運用 ・例外措置	4.4 情報セキュリティマネジメントシステム 5.3 組織の役割、責任及び権限 A.6.1 内部組織 6.2 情報セキュリティ目的及びそれを達成するための計画策定 7.5.3 文書化した情報の管理

・情報セキュリティ対策の教育 ・情報セキュリティインシデントへの対処 ③点検 ・情報セキュリティ対策の自己点検 ・情報セキュリティ対策の監査 ④見直し ・情報セキュリティ対策の見直し	A.7.2.2 情報セキュリティの意識向上、教育及び訓練 A.16 情報セキュリティインシデント管理 9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
情報の取扱い ・規定の整備　　・目的外の利用等禁止 ・情報の格付・取扱制限 ・情報の利用・保存　・情報の運搬・送信 ・情報の提供・公表　・情報の消去 ・情報のバックアップ	 7.5.3 文書化した情報の管理 A.8.1.1 資産目録 A.8.2.3 資産の取扱い、A.11.2.5 資産の移動 A.12.3.1 情報のバックアップ
情報を取扱う区域の管理	A.11 物理的及び環境的セキュリティ
外部委託 ・外部委託 ・約款による外部サービスの利用 ・ソーシャルメディアサービスによる情報発信	 A.15.1 供給者関係における情報セキュリティ A.15.2 供給者のサービス提供の管理
情報システムのライフサイクル ・情報システムに係る文書等の整備 ・情報システムの企画・要件定義 ・情報システムの調達・構築 ・情報システムの運用・保守 ・情報システムの更改・廃棄 ・情報システムについての対策の見直し ・情報システムの運用継続計画	 A.13.1.1 ネットワーク管理策 A.14　システムの取得、開発及び保守 A.14.1.1 情報セキュリティ要求事項の分析及び仕様化
情報システムのセキュリティ要件 ・情報システムのセキュリティ機能 ・情報セキュリティの脅威への対策 ・アプリケーション・コンテンツの作成・提供	A.12.2 マルウェアからの保護 A.12.6 技術的ぜい弱性管理 A.13.1 ネットワークセキュリティ管理
情報システムの構成要素 ・端末・サーバ装置等 ・電子メール・ウェブ等	A.9 アクセス制御 A.10.1 暗号による管理策 A.11.2 装置
通信回線 ・通信回線	A.13 通信のセキュリティ

情報システムの利用 ・情報システムの利用 ・府省庁支給以外の端末の利用	 A.9.2 利用者アクセスの管理 A.9.3 利用者の責任

(2) 統一基準における ISMS：JIS Q 27001:2014 の活用について

統一基準の各項目とその構成内容に該当する ISMS：JIS Q 27001:2014 の条項名をリンクさせて、相互に対応していることを確認したが、統一基準に対して、ISMS は、本文（第 4 項から第 10 項）と附属書Ａ（A.5～A.18:113 項目）から広範囲にわたって統一基準をカバーしており、統一基準において、次の点において ISMS の条項をもっと具体的に活用しても良いのではないか。

JISQ27001:2014 の対応範囲	統一基準
本文（第 4 項から第 10 項）と附属書Ａ（A.5～A.18:113 項目）から成り、範囲的には、主要省庁の情報セキュリティ基準及び統一基準を広く、カバーしている。	①本文（第 4 項から第 10 項）については、9.1 監視、測定、分析及び評価、9.2 内部監査のみであり、4.組織の状況及び 6.計画についても活用することも検討の余地がある。 ② 附属書Ａ（A.5～A.18:113 項目）については、A.6 情報セキュリティのための組織から A.16 情報セキュリティインシデント管理と活用されているが、管理策については、もっと具体的に引用・明記してもよいのではないか。

６．まとめ

以上、統一基準に対する主要省庁の情報セキュリティ基準と、及び JIS Q 27001:2014 の内容を比較・確認してきたが、まとめると次のようになる。

（１） 統一基準においては、統一基準制定(平成 26 年５月 19 日)時の基本方針に「政府機関統一基準は、国際的な基準等との整合性に配慮して策定する」と掲げていることからも、前項 (2) で明記しているように、新たに制定された JISQ27001:2014 のリスク管理的な条項については積極に取り入れてもよいのではないか。

（２）主要省庁の情報セキュリティ基準においては、当該省庁の情報及び情報システムに特化した管理策になることはやむを得ないが、もう少し、情報及び情報システムにおけるリスクを洗い出して、つまり、JIS Q 27001:2014 の 4.1 組織及びその状況の理解における組織の外部・内部の課題を決定して、そして、6.1 リスク及び機会に対処する活動におけるリスク及び機会を決定して、それに対処する活動を計画するというプロセスアプローチを取り入れても良いのではないか。

（３）ISMS：JIS Q 27001:2014 は、前述してきたとおり統一基準及び主要省庁の情報セキュリティ基準を広くカバーしており、政府統一基準及び主要省庁の情報セキュリティ基準において、統一基準制定時の基本方針どおり ISMS：JIS Q 27001:2014 の関係条項を具体的に活用する必要がある。特に、A.17 事業継続マネジメントにおける情報セキュリティの側面を業務継続の側面から取り入れるなど、附属書Ａ（A.5～A.18:113 項の管理策の活用を具体的に引用・明記しても良いのではないか。