第 119 回月例研究会報告

日時：2006 年 1 月 30 日(月)18：30～20：30

場所：中央大学駿河台記念館 280 号会議室

演題：「ＩＳＯ／ＩＥＣ27001：2005 の最新動向」

講師：財団法人日本情報処理開発協会　情報セキュリティ部ＩＳＭＳ制度推進室室長
　　高取　敏夫　氏

報告者　No. 555　松枝　憲司

１．講演要旨

(1)　ISMS に関連する国際規格化の背景

ISO27000 シリーズとして、以下のような体系化が計画されている。

ISO/IEC27000（基本及び用語）／ISO/IEC27001(ISMS 要求事項)／
ISO/IEC27002（実践規範）／ISO/IEC27003(実施の手引き)／ISO/IEC27004(測定)／
ISO/IEC27005(ISMS リスクマネジメント)

(2)　ISO／IEC27001 への移行計画

①　ISMSVer2.0 による初回審査の期限は、JISQ27001 発行時から半年の間。

②　Ver2.0 による維持審査期限は、JISQ27001 発行時から 1 年半。

③　JISQ27001 による初回審査は、JISQ27001 発行時以降。

④　Ver2.0 から JISQ27001 への移行期間は、JISQ27001 発行時から、1 年半の間。

(3)　ISO／IEC27001 と ISMS 認証基準(Ver.2.0)との差分(本文の要求事項)

「ISMS の内部監査」が「マネジメントレビュー」から独立したり、「管理策の有効性の測定」や「文書化に関する要求事項」等の差分があるが、ISMS の Ver1.0 から Ver2.0 の変更に比較すれば差異は小さい。

(4)　ISO／IEC27001 と ISMS 認証基準(Ver.2.0)との差分(附属書Ａの要求事項)

管理目的の数としては、ISO/IEC27001：2005 に「7 個」追加された。

また管理策の数は、ISMSVer2.0 は「127 個」から、ISO/IEC27001：2005 は「133 個」に変更となった。

２．講演の内容

(1) ISMS に関連する国際規格化の背景

現在 ISMS の認証を取っている事業所数は 1,300 余りにのぼり、そのうち 8 事業所は ISO／IEC27001：2005 に移行済みである。日本の認証事業所数は、世界的に見て圧倒的にトップの状況である。

ISMS のこれまでの経過は次の通りである。

①　英国規格 BS7799-1(ベストプラクティス)が、2000 年 12 月に ISO 化（ISO／IEC17799：2000）され、2002 年 2 月に JIS 化（JISX5080：2002）された。

②　2005 年 6 月に、ISO／IEC17799：2005 と改訂された。2006 年 4 月に JIS 化

（JISQ27002：2006）される予定。また 2007 年には、ISO／IEC27002：2007 と規格番号が変更される予定である。

③ 英国規格 BS7799-2(認証基準)をベースに ISMS 認証基準が策定され、現在の ISMS 認証基準(Ver.2.0)は、BS7799-2：2002 に準拠している。

④ 英国規格 BS7799-2 をベースに、2005 年 10 月に ISO／IEC27001：2005 が制定された。2006 年 4 月に JIS 化（JISQ27001：2006）される予定。

「ISO／IEC27000 シリーズの体系化」

① ISO/IEC27000：ISMS の基本を説明し関連する用語を規定(基本及び用語)

② ISO/IEC27001：情報セキュリティマネジメントシステムへの要求事項

③ ISO/IEC27002（17799）：情報セキュリティマネジメントシステムの実践規範

④ ISO/IEC27003：情報セキュリティマネジメントシステムのための実装の手引（現在の「ISMS ユーザガイド」相当）

⑤ ISO/IEC27004：情報セキュリティマネジメントの測定（管理策がどの程度有効に機能しているかを測定するためのガイド）

⑥ ISO/IEC27005：情報セキュリティリスクマネジメント（現在の「ISMS ユーザーズガイドリスクアセスメント編」に相当）

(2) ISO／IEC27001 への移行計画

① ISMS の Ver2.0 による初回審査の期限：JISQ27001 発行時（現在は 2006 年 4 月）から半年の間まで。

② Ver2.0 による維持審査期限：JISQ27001 発行時から、1 年半の間。

③ JISQ27001 による初回審査：JISQ27001 発行時以降可能となる。

④ Ver2.0 から JISQ27001 への移行期間：JISQ27001 発行時から、1 年半の間で Ver2.0 と JISQ27001 との差分の更新審査を行う。

(3) ISO／IEC27001 と ISMS 認証基準(Ver.2.0)との差分(本文の要求事項)

主なものを以下に示す。

① 「情報セキュリティ基本方針」→「ISMS 基本方針」に変更。ISMS 基本方針は情報セキュリティ基本方針を含んだ上位概念

② 管理策の有効性の測定：「文書化に関する要求事項」として「情報セキュリティに関するプロセスの効果的な計画、運用及び管理を確実に実施するため、また管理策の有効性を測定する方法を説明するために、組織が必要と判断した文書化された手順」が追加された。有効性の結果をマネジメントレビューへインプットすること。

③ 「文書管理」として「必要とする人にとって文書が使用可能であることを確実にし、また文書がその分類区分に適用される手順に従って移動、保管、及び完全に廃棄されることを確実にする。」とあり、ISO9000 より厳しい。

④ 「ISMS の内部監査」は、内容は ISMS 認証基準 Ver2.0 の「ISMS の内部監査」と

ほぼ同じで、大項目となった。

(4) ISO／IEC27001 と ISMS 認証基準(Ver.2.0)との差分(附属書Ａの要求事項)

① 管理目的の数としては、ISO/IEC27001：2005 に「7 個」追加された。

NO	項番	管理目的
1	Ａ．８．１	雇用前
2	Ａ．８．２	雇用期間中
3	Ａ．８．３	雇用の終了又は変更
4	Ａ．１０．２	第三者が提供するサービスの管理
5	Ａ．１０．９	電子商取引サービス
6	Ａ．１２．６	技術的ぜい弱性管理
	Ａ．１３	情報セキュリティインシデントの管理
7	Ａ．１３．２	情報セキュリティインシデントの管理策及びその改善

② 管理目的の数として、ISMSVer2.0 から「4 個」削減された。

NO	項番	管理目的
1	４（３）	外部委託
2	６（１）	職務定義及び雇用におけるセキュリティ
3	６（２）	利用者の訓練
4	７（３） ７（３）① ７（３）②	その他の管理策 クリアデスク及びクリアスクリーンの個別方針 資産の移動

③ 管理策の数は、ISMSVer2.0 は「127 個」から、ISO/IEC27001：2005 は「133 個」に変更となった。内訳として「17 個」の管理策が追加された。

NO	項番	管理策
1	Ａ．６．１．１	情報セキュリティに対する経営陣の責任
2	Ａ．６．１．７	専門組織との連絡
3	Ａ．６．２．２	顧客対応におけるセキュリティ
4	Ａ．７．１．２	資産の保有者
5	Ａ．７．１．３	資産利用の許容範囲
6	Ａ．８．２．１	経営陣の責任
7	Ａ．８．３．１	雇用の終了又は変更に関する責任
8	Ａ．８．３．２	資産の返却
9	Ａ．８．３．３	アクセス権の削除
10	Ａ．９．１．４	外部及び環境の脅威からの保護
11	Ａ．１０．２．１	第三者が提供するサービス
12	Ａ．１０．２．２	第三者が提供するサービスの監視及びレビュー
13	Ａ．１０．２．３	第三者が提供するサービスの変更に対する管理
14	Ａ．１０．４．２	モバイルコードに対する管理策
15	Ａ．１０．９．２	オンライン取引
16	Ａ．１０．１０．３	ログ情報の保護
17	Ａ．１２．６．１	技術的ぜい弱性の管理

④ Ver2.0 の管理策から「11 個」削減された。

NO	項番	管理策

1	４（１）①	情報セキュリティ運営委員会
2	４（１）⑤	専門家による情報セキュリティの助言
3	４（３）①	外部委託契約におけるセキュリティ要求事項
4	６（３）③	ソフトウェア誤動作の報告
5	８（１）⑥	外部委託による施設管理
6	９（４）②	指定された接続経路
7	９（４）④	ノードの認証
8	９（５）⑥	利用者を保護するための脅迫に対する警報
9	１０（３）②	暗号化
10	１０（３）③	デジタル署名
11	１０（３）④	否認防止サービス

３．質疑

（１） ISMS 基本方針と情報セキュリティ基本方針の区分について

従来からあった関連する用語を、この２つに統一した。ISMS 基本方針が情報セキュリティ基本方針より上位の概念である。必ずしも２種類の文書を要求しているわけではなく、１つの文書でもよい。

（２） 「セキュリティ計画」という用語が出てきた理由について

「セキュリティ計画」とは、リスク対応計画、法令等の対応計画、管理策の見直し計画、研修の見直し計画等、セキュリティに関する様々な計画の総称である。

「セキュリティ計画書」があるわけではない。

４．所感

現在の ISMS 制度の ISO への移行というタイムリーなテーマということもあり、多数の受講者が参加していた。私のクライアントにも、ISMS 認証基準 Ver2.0 から ISO27001 への切替えが必要という企業があり、非常に関心をもって受講した。

高取氏の「ISO/IEC27001：2005」と「ISMS 認証基準 Ver2.0」の相違点に関する資料による説明で、大きな変更点の概要等について全体を把握することができた。

質疑応答にもあったが、用語の変更については、実務担当者からすると神経質にならざるを得ないと感じた。

また ISMS の認証取得事業所数が 1300 余りで世界一、2 位のイギリスでようやく 3 桁、アメリカにいたっては数 10 社程度と聞いて、ISMS に対する日本の熱心さがよくわかった。我が国においては、今回の ISO 化に伴い、より一層 ISMS の認証取得にシフトしていくのではないかと思った。情報セキュリティビジネスマーケット及びシステム監査人のビジネスチャンスが大いに拡大していると感じられた。

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