テクノファＮＥＷＳ 第６８号

テクノファNEWS
Technology Transfer

ISO/IEC 27001 附属書Ａの管理目的と管理策概要

講師：ISMS主任審査員、テクノファ講師　中島博文氏

ISO／IEC 27001規格附属書Aは、ISO／IEC 17799：2005の管理策をshallに書き換えた要求事項である。ISMS認証基準Ver. 2. 0と対比してどう改訂されたか、JIS発行前の講演の中から要旨を紹介する。

細かなことであるが、附属書A. は、“詳細管理策”として馴染んでいたが、“詳細”を規格の用語としては使用せずに“管理目的及び管理策”となった。また、管理目的ごとに、“管理目的”と表記していたものが、ISO/ IEC 17799:2005（以下、17799）の記述と同様に“目的”としている。

変更の概要　今回の変更は基本的には情報セキュリティの枠組みの再整備と思って欲しい。社会や技術の変化、或いは情報セキュリティ管理のあり方を踏まえて、最新の管理策として再編成したということである。IT 技術の変化をみると、BS7799 が生まれた 1995 年頃はまだメインフレームが中心でそろそろダウンサイジングが叫ばれた頃である。コンピュータの利用がメインフレームから“分散、モバイル、ワイヤレス環境”重視に変化してきたことによりセキュリティも追随していかなければならなくなった。ハッカーが OS の技術的脆弱性を狙うことになり“技術的脆弱性のタイムリーな管理”が必要ともなっている。インターネットで簡単に情報を収集する環境を作ることができ、その環境で情報が盗まれることが発生してくることにもなり、いわゆる“モバイルコードに対する管理策”が必要となっている。

また、企業の事業上の変化で大きいのは、本業とアウトソーシングを勘案した経営になってきているということである。セキュリティの面からすれば、いわゆる第三者とのインターフェースが重要であるから、“外部組織”と“第三者の提供するサービスの管理”を充実させている。ISMS 認証基準 Ver.2.0(以下、Ver.2.0)では、4.組織のセキュリティにおいて、組織の資産に対して第三者がアクセスするセキュリティと外部委託によるセキュリティ、8.通信及び運用管理における“外部委託による施設管理”、10.システム開発及び保守における“外部委託におけるソフトウェア開発”の外部組織とのセキュリティインターフェースを規定していた。それらを、“外部組織、第三者と顧客”に概念定義して、A.6.2“外部組織”、A.10.2“第三者が提供するサービスの管理”及び A.12.5.5“外部委託によるソフトウェア開発”に整理してより明確な組織のセキュリティ維持を狙っている。

もうひとつの大きな観点は、国際的なコンプライアンスへの推進である。OECD は、加盟各国がそれぞれの法制度の中で、協調して情報セキュリティを維持するためにガイドラインを制定した。このガイドラインをマネジメントシステムとして確立するための規格が ISO/IEC 化された意義は大きい。また、JIPDEC は、J-SOX 法における IT の内部統制のツールとして、この規格が支援することも視野に入れているようである。

こういうところが変更の概要である。審査の立場としては、この再整理されたところ（差分）を頭に置きながら審査をして行くことになるだろう。

章立ての変更　ISO/ IEC 27001:2005(以下、27001)と Ver.2.0 を比較し、変更になったところを見よう(A.12、13、15 の下線部)。

章立ての変更

ISO/IEC 27001:2005	ISMS 認証基準(Ver.2.0)
A.5 セキュリティ基本方針	3. セキュリティ基本方針
A.6 情報セキュリティのための組織	4. 組織のセキュリティ
A.7 資産の管理	5. 資産の分類及び管理
A.8 人的資源のセキュリティ	6. 人的セキュリティ
A.9 物理的及び環境的セキュリティ	7. 物理的及び環境的セキュリティ
A.10 通信及び運用管理	8. 通信及び運用管理
A.11 アクセス制御	9. アクセス制御
A.12 情報システムの取得、開発及び保守	10.システムの開発及び保守
A.13 情報セキュリティインシデント管理	6.3 セキュリティ事件・事故及び誤動作への対処 8.1.3 事件・事故管理手順 12.1.7 証拠の収集等
A.14 事業継続管理	11.事業継続管理
A.15 コンプライアンス	12.適合性

A.12 情報システムの取得、開発及び保守。取得が加わった。ある組織がシステムを開発し自ら使い保守していく、その時のセキュリティ問題を管理策ととらえていた。今や自ら開発するというだけではなく、いろいろな意味で取得をするので“情報システム取得”が追加されたのである。今までの審査の場面では、これは開発したものではなく提供を受けているものだからVer.2.0の「業務用システムのセキュリティはない」とか、適用除外するとかいうことであった。これは取得によりセキュリティ問題が生ずる訳だから、これも積極的に捉えてもらうことになる。

A.13 情報セキュリティインシデントの管理が新規に起こされた。Ver.2.0では、6.人的セキュリティの中で、6.(3)セキュリティ事件・事故及び誤動作への対処という要求で、事件・事故の速やかな報告を要求していた。また事件・事故管理手順の要求が8.通信及び運用管理の中にあった。そしてセキュリティ問題の重要な事件・事故の証拠収集は12.適合性の中にあった。これらを再整理して情報セキュリティインシデント管理ということに位置付けたということである。ISO/IEC TR 18044標準報告書(以下、TR18044)の和訳はまだないが、インシデント管理のPDCAの回し方のガイドラインである。これを基本に置き直して要求事項として章立てされたものである。

A.15 コンプライアンス（JISでは“順守”）、今まではJIS X 5080の「適合性」という用語を使って来た。英和対訳版では「コンプライアンス」としている。JIPDEC講習で規格制定委員は、“コンプライアンス”は、“法的順守”の意味合いが強いので、A.15.1はよいのだが、A.15.2とA.15.3は、法的意味が薄れるので、“コンプライアンス”の用語を使用するのに躊躇しているようであった。

なお、A.14 事業継続管理は「11.(1)事業継続に関する種々の面」とやや大風呂敷的な表現だった。企業には必ず事業を継続する計画や管理の仕組がある。その事業継続計画全体の中に整合をとった形で、「情報セキュリティの側面」に関することとして取組むということだ。分かりやすくなったが内容は殆ど変わらない。章立ての変更は以上である。

17799との関連からすると、5～15章の11の章が27001附属書Aに完全対応して要求事項(shall)として位置付けられている。

管理目的の変更概要　管理目的は7項が追加、4項が削除されて36項→39項になった。

まず追加では、Ver.2.0の6.人的セキュリティは、(1)雇用、(2)訓練、(3)懲戒手続であった。27001では、A.8人的資源のセキュリティにA.8.1 雇用前、A.8.2 雇用期間中、A.8.3 雇用の終了又は変更という形で管理目的が分けられ整理された。従業員に対する人的なセキュリティである。

◆27001で、追加された「管理目的」
1. A.8.1　雇用前(6.(1)を削除、新たに追加)
2. A.8.2　雇用期間中(6.(2)を削除、新たに追加)
3. A.8.3　雇用の終了又は変更(新規)
4. A.10.2　第三者が提供するサービスの管理(新規)
5. A.10.9　電子商取引サービス(8.(7)がA.10.8とA.10.9に分離)
6. A.12.6　技術的ぜい弱性管理(新規)
7. A.13.2　情報セキュリティインシデントの管理及びその改善(8.(1)③、6.(3)④、12.(1)⑦の管理策で再構成)

A.10 通信及び運用管理では、A.10.2 第三者が提供するサービスの管理が新規。

8.(7)が一部分離されA.10.9 電子商取引サービスとして新規になっている。

更にA.12.6 技術的ぜい弱性管理が新規である。ウィンドウズのアップデートのようなことにタイムリーに対応していこうというような意図の管理策と言えば素人にも分かりやすいだろうか。

A.13.2 情報セキュリティインシデントの管理及びその改善、「章立て」のところで説明した通り。

一方、Ver.2.0から削除された管理目的は4項。先ほど説明した通り4.(3)外部委託は再編成されて、A6.2 外部組織へ統合されている。6.(1)職務定義書も再編成され、この用語は使用していない。6.(2)利用者の訓練も削除された。

特徴的なのは7.(3)その他の管理策。「クリアデ

◆Ver.2.0 から削除された「管理目的」
1. 4.(3)外部委託(A.6.2 へ統合)
2. 6.(1)職務定義及び雇用におけるセキュリティ(A.8.1 へ)
3. 6.(2)利用者の訓練(A.8.2 へ)
4. 7.(3)その他の管理策(混乱を生じるタイトルのため削除。構成していた管理策は A.9.2、A.11.3 へ

スク、クリアスクリーンポリシー」、これが物理的、環境的セキュリティとその他の管理策という名前についていると、どうも相応しくないということで、A.11.3 利用者の責任に移動した。タイトルから混乱が生じたため削除したということである。

管理策は 127 から 133 となった。管理策「9.(4)②指定された接続経路」、また今まで殆どの組織が適用除外していた「9.(5)⑥利用者を保護するための脅迫に対する警報」は削除されている。以上が変更の概要だが、管理策の変化については以下、項番毎に説明する。[新規、大幅変更に下線]

A.5 セキュリティ基本方針 A.5.1 情報セキュリティ基本方針。基本方針には「情報セキュリティ基本方針」と「ISMS 基本方針」が存在する。その位置付けは、ISMS 基本方針の一部として経営者の情報セキュリティの基本方針があるということである。情報セキュリティ基本方針では、目的での direction の訳が「指針→方向性」に変わり、「事業上の要求事項、関連する法令及び規則を考慮すること」が追加された。経営陣に承認された基本方針は全従業員のみでなく、「関連する外部関係者」にも公表、通知することが要求項目になった。

A.6 情報セキュリティのための組織 タイトルは何回か変ってきた。初め'Security organization'、Ver.2.0 で'Organizational security'となり、今回が'Organization of information security'である。これは管理策であるから組織が焦点だということである。構造は「内部組織」と「外部組織」になった。A.6.1 内部組織。内部組織のもつセキュリティ維持ということである。「情報セキュリティ運営委員会」は、小さい組織にとって実装することは難しいだろうという理由で削除、A.6.1.1 に吸収された。委員会は削除されたが、大きな組織では横断組織という意図は「調整」で対処すること。委員会も機能しているならばそのまま継続するがよい。A.6.1.1 情報セキュリティに対する経営陣の責任が新規になった。経営陣のコミットメントということで明確にすること。A.6.1.7 専門組織との連絡が新規、4.(1)⑤専門家助言はここに吸収され削除。A.6.2 外部組織。「第三者」が「外部組織」でくくり直された。外部組織には第三者、外部委託、顧客があり、それぞれに関するセキュリティということで整理された。因みに 8.通信及び運用管理の外部委託によるサービスは、A.10.2 第三者が提供するサービスの管理(新規)へ移項。A.6.2.2 顧客対応におけるセキュリティが新規、顧客が組織の情報又は資産にアクセスする際のセキュリティの要求事項への対処ということ。A.6.2.3 第三者との契約におけるセキュリティ、記述は変ったが考え方は従前と同じである。外部組織の審査の時には、外部組織をどのように整理しているか、それに対して A.6.2.1 外部組織に関係したリスクの識別はどのように行われているか、A.6.2.2、A.6.2.3 でどう対応しているかといった審査をすることになる。

A.7 資産の管理 構造的には重要事項を明確にすること。A.7.1 資産に対する責任では、資産の保有者(JIS は管理責任者)の指定、利用者自身の責任を明確にするための資産の利用の許容範囲に関する規則に関する管理策が増えている。

A.7.1.2 資産の保有者(JIS は管理責任者)、新たに管理策として位置付けるということである。

A.7.1.3 資産利用の許容範囲も新規である。資産の利用については、利用する範囲がどのレベル、どの範囲かということをきちっと決め文書化することが新たに加わった。

A.7.2.2 情報のラベル付け及び取扱の一連の手順を決め、実行を強調。資産の分類及びラベル付けの考え方は従来通りである。

A.8 人的資源のセキュリティ インシデントはまさに人的セキュリティの問題として多く発生する。Ver.2.0 では、6.(1)職務定義及び雇用におけるセキュリティとしてだけ扱ってきたが、雇用に対して全面的に対応することが強調された。情報セキュリティ事象の発生する側面として雇用前の問題、雇用中の問題、退職時の問題とそれぞれ目的に従って整理された。

A.8.1 雇用前(新規)では A.8.1.1 役割及び責任、2 選考、3 雇用条件のような形に整備されている。

A.8.2 雇用期間中(新規)については更に A.8.2.1 経営陣の責任(新規)として、「経営者は関連する一人一人に方針・手順に沿ったセキュリティを実行させること」を強調している。A.8.2.3 懲戒手続、従業員のセキュリティ違反に対する抑止効果を引き出す管理策である。審査に行ってよく遭遇するが、セキュリティ違反を犯した従業員に対する懲戒手続が明確になっていない場合が多い。"就業規則にあります"という説明を受けることも多い。就業規則は懲戒を規定しているだけである。ここの要求は懲戒に対する正式手続だ。従業員がセキュリティ違反を犯した場合に、どのような手順で懲戒になるのか、事前に正式な手続があることが重

要である。懲罰委員会はどのようにして開かれるのか、本人に申し開きの場を与えられるのか、その正規の懲戒手続を確認することが重要である。

A.8.3 雇用の終了又は変更(新規)、退職及び異動についての責任である。A.8.3.1 雇用の終了又は変更に関する責任、A.8.3.2 資産の返却で利用していた資産を返却すること、そして A.8.3.3 アクセス権の削除、総て新規である。資産の返却、アクセス権の削除は一般的に行われることで、管理策とすることが強調されている。

A.9 物理的及び環境的セキュリティ A.9.1.4 外部及び環境の脅威からの保護が新規で、物理的環境のセキュリティ、自然災害及び人的災害からの物理的保護を強調している。Ver.2.0 での 7.(1)⑤物の受け渡し場所からの情報設備の隔離だけではなく認可されていない者の立入りも考慮、A.9.1.6 一般の立ち寄り場所及び受渡し場所という形で範囲を広げている。A.9.2 装置のセキュリティでは、電源以外の問題が A.9.2.2 支援ユーティリティ（JIS はサポートユーティリティ）として強調されている。

ここのポイントは Ver.2.0 での「7.(3)その他の管理策」である。この位置付けがはっきりしていなかったため混乱を生じていた。「その他の管理策」を削除し、もっと相応しいところに移動したということで基本的な構造は変わらない。「その他」の 7.(3)①クリアディスク及びクリアスクリーンの個別方針は A.11.3 利用者の責任へ移項、資産の移動は 7.(3)②から A.9.2.7 として、装置、情報又はソフトウェアは「事前」認可なしでは構外に持ち出さないことに。A.9.2.5(構外のセキュリティ)、A.9.2.6 (処分、再利用)とともに装置のセキュリティとして構成の位置付けになっている。

A.10 通信及び運用管理 27001 では、この領域の管理策が充実した。第三者が提供するサービスの管理が追加された。そして情報の交換(A.10.8)に対応する管理策が再整理されている。また運用の一環としての監視ということで、監視(A.10.10)の管理策、これは特にログが重要になっていることからログの取得が整理されている。

A.10.1 運用の手順及び責任。Ver.2.0 の 8.(1)③の事件・事故対応手順は A.13 インシデント管理へ、⑥外部委託管理は A.10.2 第三者のサービス管理へ、それぞれ相応しい場所へ移動した。

A.10.2 第三者が提供するサービスの管理が新規、A.10.2.1 第三者が提供するサービス(運用)、2.2 監視及びレビュー、2.3 変更に対する管理という形で整備され、第三者が提供するサービス周辺の管理が強化された。

A.10.3 システムの計画作成及び受入れ、管理目的には変更ないが A.10.3.1 容量・能力の管理では資源の利用を監視・調整すること、A.10.3.2 システムの受入れでは受入れ前に加え開発中にも適切な試験を実施することをそれぞれ強調。

A.10.4 悪意のあるコード及びモバイルコードからの保護は今までは管理策が一つ、一般的にはウイルスへの対応のような管理策であった。新たに A.10.4.2 モバイルコードに対する管理策が入った。モバイルコードとは何か。入力を要求しているものに対して、コード化されたもので入力をする。コードがきちっと管理できないと安全性、可用性、セキュリティ問題が生ずる。利用者が気づかないで情報が動いて行くわけだが、そういう中で潜んでいる悪意のコードを抑えていく管理策である。

A.10.5 バックアップ、A.10.6 ネットワークセキュリティ管理、A.10.6.2 ネットワークサービスのセキュリティ、内製、外部委託を問わず管理上の要求事項を洗い出し、関係者間で合意することを強調。

A.10.7 媒体の取扱いは今までの 8.(6)がほぼ同じで移項。

A.10.8 情報の交換、8.(7)のところが整備されている。目的が組織内部で交換した情報だけでなく、「外部と交換した情報、ソフトウェア」も含めて、内外の情報に対するセキュリティを求めている。ここでは正式な交換方針を持つこと、そして手順を持つことを求める。更に A.10.8.4 電子的メッセージ通信、8.5 業務用情報システムが大幅変更され、情報の交換のところを整備している。

A.10.9 電子商取引サービスが新規に入った。今までは電子商取引ということは、電子商取引におけるセキュリティ、いわゆる事業上に関する商取引の中で、広くオンライン取引として技術的側面を強調したこととして、オンライン取引、オンライントランザクションに関連する情報の保護を強調していた。新規の A.10.9.2 オンライン取引では、電子商取引の時に公開されている情報で商取引するということで、公開されている情報をこの中に含めて管理策としての整備を要求している。

A.10.10 監視。通信及び運用管理で重要な監視を整備し直している。監査ログ(記録)取得の問題、システムの使用状況監視の問題、そして新設されたログ情報の保護の問題ということで A.10.10 を起こしている。A.10.10.3 ログ情報の保護が新規である。A.10.10.4 実務管理者及び運用担当者の作業ログは、後半の定期的チェックが削除された。A.10.10.5 障害のログ取得、以前は「是正処置をとる」とされていたが、レベルにあった「適切な処置

を講じる」こととなり、規格本文で言う是正処置報告書等は必ずしも必要ではなくなった。監視にはA.10.10.6 クロックの同期が必要なので、監視の中に組み入れられた。旧来アクセス制御にあった「9.(7)システムアクセス及び使用状況の監視」は、運用管理のカテゴリーであるということでA.10.10 監視へ一括移動している。

A.11 アクセス制御 A.11.1 アクセス制御に対する業務上の要求事項。A.11.1.1 アクセス制御方針、基本的な制御方針のレビューを強調する。A.11.2 利用者アクセスの管理、2.1 利用者登録、2.4 利用者アクセス権のレビューが一部変更。A.11.3 利用者の責任の中に A.11.3.3 クリアデスク・クリアスクリーン方針(7.(3)その他の管理策)がここに組み入れられた。利用者の責任だということである。

A.11.4 ネットワークのアクセス制御、旧「ノードの認証」は新項番 A.11.4.2 へ統合。9.(5)①にあったA.11.4.3 ネットワークにおける装置の識別が前と少し違うところか。

A.11.5 オペレーティングシステムのアクセス制御には特段の変更はない。A.11.6 業務用ソフトウェア及び情報のアクセス制御は今まで通りだが、監視が A.10.10 へ移項。A.11.7 モバイルコンピューティング及びテレワーキング、今まで通りである。

A.12 情報システムの取得、開発及び保守 「取得」が加わった。A.12.1.1 セキュリティ要求事項の分析及び仕様化は今まで通り。A.12.2 業務用ソフトウェアでの正確な処理では、入力データの妥当性確認、内部処理の管理、メッセージの完全性、出力データの妥当性確認、従来通りである。

A.12.3 暗号による管理策では、A.12.3.1 暗号による管理策の利用方針。ここに技術的な管理策、暗号化、ディジタル署名、否認防止サービスが吸収され、利用方針のマネジメント項目として整理された。あとは A.12.3.2 かぎ管理である。A.12.4 システムファイルのセキュリティはファイル管理の問題として、A.12.4.1 運用ソフトウェアの管理、4.2 システム試験データの保護、4.3 プログラムソースコードへのアクセス制御で従来通りである。

A.12.5 開発及びサポートプロセスにおけるセキュリティにある A.12.5.4 情報の漏えい。私はこれを見て、いろいろなセキュリティ事件・事故が多発していることからそれを取り入れたのだと解釈した。17799 には隠れチャネルという表現がなく、情報漏洩の可能性抑止というマネジメント項目になっている。残念ながら「隠れチャネル」の用語は消えたが、実質的には隠れチャネル対策と受けとめよう。17799 は開発中の情報の漏洩というところまでは特に意図していない。要はソフトウェアに潜んできて、ダウンロードしたらそこに隠れチャネルがあった。そういうところに情報の漏洩が起こるということで、今までの管理策が“情報の漏えい”という言葉になったと受けとめて欲しい。

新規目的 A.12.6 技術的ぜい弱性管理、A.12.6.1 技術的ぜい弱性の管理である。要求事項は使用しているシステムのぜい弱性に関する情報をタイムリーに入手、内容を検討して対応せよという。また状況評価し関連するリスクにも手を打てという。

A.13 情報セキュリティインシデントの管理 この事項では、インシデント管理に関する PDCA を規定している TR 18044 の考え方を引用している。Ver.2.0 で使用している“情報セキュリティ事件・事故”は、“information security incident”であるが、JIS 化に際して確率のニュアンスを含め“情報セキュリティインシデント”に翻訳する予定だ。また、インシデントの原因となる“情報セキュリティ事象”の用語を新たに追加している。

A.13.1 では、インシデントになる可能性のある“情報セキュリティ事象”を報告することを管理目的としている。Ver.2.0 では、報告の対象が“事件・事故”であったが“事象”であることに注意が必要である。A.13.1.1 情報セキュリティ事象の報告と A.13.1.2 セキュリティ弱点の報告で構成される。つまりセキュリティ事象な弱点を時機を失しないように是正処置をとることができるように連絡することを確実にするための管理策である。

A.13.2 は、インシデント管理と改善のための管理策で構成されている。インシデント管理に関して A.13.2.1 責任及び手順、改善に向けて A.13.2.2 インシデントからの学習、保全のために A.13.2.3 証拠の収集の３つの管理策である。

A.14 事業継続管理 Ver.2.0 では「事業継続管理の種々の面」と言った。A.14.1 事業継続管理における情報セキュリティの側面、組織として事業継続計画や管理の枠組みの中で情報セキュリティに関する側面についてきちっと取り組めということである。内容は少し分かりやすくなったが、実質的には A.14.1.1～5 まで前の要求とそう変わってはいない。

A.15 コンプライアンス 冒頭でも触れたが、Ver.2.0 では「適合性」という用語を使ってきた。今後は、“コンプライアンス”（JIS では“順守”）となる。ISMS 制度を運用してきて、情報セキュリティの要求事項として“契約上の要求事項”が重要であることがわかってきた。特に“SLA：サービス・レベル・アグリーメント”が必要であることも明確になってきている。情報セキュリティ要求事項は明確にしてリスクアセスメントを行い、

リスク対応してリスクマネジメントをするのがISMS である。“契約上の要求事項”を含めてA.15.1 では、法的要求事項を満たすための組織の取組み方法を文書化して維持し、最新に保つことを要求している。Ver.2.0 の 12.(1)の内容よりは厳しい要求となっている。

A.15.2 セキュリティ方針及び標準の順守、並びに技術的コンプライアンス（JIS では“順守”）。A.15.2.1 セキュリティ方針及び標準の順守、ここは皆さん内部監査でやるとして組み立てられる。確かに内部監査での確認も一つの方法である。更に、A.15.2.2 技術的コンプライアンス（JIS では“順守”）の点検、これは監査ではない。ここはセキュリティ実施標準の遵守に関して定めに従って点検、検査出来ているかということが要求事項であり、本来は日常的な監視、点検活動の要求事項と捉えてほしい。

A.15.3 情報システムの監査に対する考慮事項。運用システムの点検を伴う監査要求事項及び活動は、リスクを最小限に抑えるために慎重に計画されること。監査によって運用中のシステムが動かなくなったということになってはまずい。監査に対する考慮事項ということである。

説明は以上である。

講演中の中島博文氏

ざっとまとめよう。今回の 27001 の発行は基本的な考え方や構造を変えるというよりは、PDCA プロセスの要求仕様の明確化ととらえ方がよいと冒頭申し上げた。従って、審査においてもマネジメントシステムの PDCA をしっかりと確認することが求められる。また、選択した管理策の有効性の測定により、日常的なリスク管理の効果が把握される。小さな PDCA 活動とともに、その結果を含めて、セキュリティ監査の結果、インシデント、改善提案及び利害関係者からのフィードバックにより、ISMS の有効性をレビューするという大きな PDCA を確認することになる。

ISMS の機能は、QMS と同様のレベルまで規格が整備されてきたと思う。プロセス・アプローチの説明に示されているモデルは業務プロセスではなく、リスクマネジメントプロセスとなっている。それが理解しにくいとよく聞く。このモデルで重要なことは、利害関係者からの情報セキュリティ要求事項及び期待をインプットとして、リスクアセスメントにより特定されたリスクに対して管理目的を設定して管理策を適用していくことである。それは業務プロセスに対する情報セキュリティ管理であり、業務プロセスにセキュリティサービスが提供されることと理解すると業務プロセスとの関係が理解しやすくなる。これまでのところ、企業が作成する ISMS マニュアルは、規格のおうむ返しの場合が多く、業務プロセスに対する合理的なリスクマネジメントの姿が見えて来ない。また、リスクアセスメントが難解なこともあって、その過程で特定されたリスクに対応するための“管理目的”が十分に明確になっていないことも多い。**管理策の有効性の評価は、“管理目的”の達成度の測定により導かれる**ので、審査員の視点も“管理目的”に着目することが強く望まれる。

よく ISMS の審査員は、“マネジメントシステムに強い人”と“セキュリティに強い人”がいるといわれる。審査機関にも特徴が現れつつある。その両方のバランスがとれると良いと思うのだが。

27001 の管理目的及び管理策の審査は、新たな 11 の情報セキュリティ領域(ドメイン)と管理目的に着目することが必要である。17799 の改訂により、最新の技術に対応するための情報セキュリティ領域と管理目的が再構成されたからだ。

ISMS 審査登録機関の認定に関する EA 指針 最後に EA7-03 に少し触れておきたい。QMS も EMS も認定機関は、審査機関に対して認定基準を要求するとともに、指針を提供している。

Ver.2.0 では、ISO 化されていなかったために、JIPDEC は EA（欧州認定協力機構）が発行した EA-7/03(情報セキュリティマネジメントシステム審査登録機関の認定に関する EA 指針)を翻訳して、JIP-ISAC100 として制定した。各審査機関は昨年 10 月から適用している。

審査機関に対する認定基準に関する指針であるが、“不適合の定義”から始まって“審査のための準備、審査、審査報告、登録に関する決定、サーベイランス及び更新審査の手順”などの指針が示されており、この指針が審査要領に反映されていることを認識しておいてほしい。

皆様のご活躍をお祈りします。　【終り】