テクノファＮＥＷＳ 第６７号

# テクノファNEWS

Technology Transfer

## 『ISO/IEC 27001,ISMS 認証基準差分研修の概要』

### 講師：ISMS 主任審査員、テクノファ講師　中島博文氏

ＩＳＯ／ＩＥＣ ２７００１規格が昨年１０月に発行された。情報セキュリティＭＳの２７０００シリーズ、第一番目の認証規格である。テクノファでは審査員の差分研修を開始したが、組織としても対応のあり方には大きな関心をお持ちかと思う。次回「附属書Ａ（要求事項）解説」と合わせて、ご講演の概要を紹介したい。

**ＩSMS認証の規格**　ISMS の認証は BS7799-2:2002 あるいは認証基準(Ver.2.0)で行われてきた。BS7799-2 が ISO に提案され、昨年 10 月 15 日に ISO/IEC27001：2005 として発行された。27001 の番号が付与されたのは、今後 27000 シリーズとしていくということである。JIS 版は JIS Q 27001:2006 として 4 月発行予定である(5 月 20 日に発行された)。27001 は、BS7799-2002 がベースで、基本的な考え方、規格の思想など内容は殆ど変わっていない。適用した管理策の有効性の評価を取り入れ、情報セキュリティマネジメントシステム(以下、ＭＳ)が確実にＰＤＣＡが回るようにするのが改訂の狙いである。ISMS 認証基準(Ver.2.0)の移行規格となる。

ISO/IEC 17799:2005（以降 17799 という）は、昨年 6 月 15 日に改訂された。規格の改訂時期にもあり、IT 技術やそれを使用する社会の変化に対応するために新しい情報セキュリティの枠組みで整理されたものである。27000 シリーズとして 27002 が割り当てられることとなっているが、“17799”の番号が馴染んでいることもあって、2007 年 4 月に規格番号を ISO/IEC 27002:2007 として移行することになっている。当該 ISMS の適用宣言書で適用とした管理策導入の助言と手引書としての位置付けに変更はない。JIS 版は、27001 と同時に、JIS Q 27002:2006 の規格番号を先取りして発行される予定である(5 月 20 日に発行された)。

中島博文氏

**２７０００シリーズ**　シリーズの構想を紹介しよう。
27000：ISO 9000 と同様、基本及び用語で構成。
27001：ISMS 要求事項。シリーズ 1 番で発行済。
27002：ISMS 実践のための規範。17799 が替わる。
27003：ISMS 実践の手引。27001 をサポートする。
27004：管理策の有効性を測定するガイドライン。パフォーマンスターゲットとは、測定とは、何時如何に測定するかといった内容である。JIPDEC ではこのガイドラインがまだ発行になっていないので‘NIST SP 800-55’を活用することを紹介している。本日ご参加の皆様も、どのように導入すればよいのか、審査はどのように行われるのか興味があるのかもしれませんが、本日は審査員研修

なので、“規格の意図は何か”という観点からご紹介することとしたい。

27005:情報セキュリティに関するリスクマネジメントをサポートするガイドライン。JIPDEC が、ISMS 認証基準(Ver.2.0)の導入のためにユーザーズガイドのリスクマネジメント編を発行している。その内容は ISO/IEC TR 0036 (JIS では、TR X 0036)を参照している。TR 0036 シリーズは、GMITS として呼ばれていたが、IT 分野だけでなく通信技術も加えて 2004 年に第 1 分冊 ISO/IEC 13335-1 が改訂され、MICTS(Management of Information and Communication Technology Security)と愛称を変えた。MICTS は、現在第一分冊 MICTS-1 が、旧 ISO/IEC TR 13335-1 及び -2 の内容を含むものとして発行され、残る-3,-4,-5 は、今後第 2 分冊 MICTS-2 として発行予定である。GMITS は 1997 年第 1 分冊が標準報告書：TR として発行されたが、今般、国際規格に種別を変更して制定された。また、この規格内容が 27000 シリーズに引用されることとなる。

27006, 27007：内容はまだ発表になっていないが、インシデント管理、災害や事業継続管理関連のものになるであろうといわれている。

**２７００１の主な変更点**　ISMS の要求仕様をより明確にし、PDCA プロセスしっかりと回すための改善ととらえていいと思う。主な変更点は次の５点である。

**ＩＳＭＳ適用範囲**(Scope)：セキュリティのインシデントは適用範囲の境界で起きる可能性が高い。境界の確認が重要だということである。これまでも暗に境界の必要性は示されていたが、境界を明示的に要求している。審査は適用範囲の境界の確認から始まる。

**リスクアセスメントへのアプローチ**：従来どおりにリスクアセスメントの方法は組織の情報セキュリティ要求事項に適した方法論を導くこととしているが、さらに、その方法論が比較可能で再現可能なこととする要求が追加された。

リスクアセスメントでリスクを受容可能な水準まで軽減するために“ISMS 基本方針及び目標”を設定するとの要求は、管理策の有効性の測定との関連から削除されたものと思われる。

**管理策の選択**：リスクアセスメント及びリスク対応のプロセスの結果から管理目的及び管理策を選択する際に、リスクを受容するための基準、法律、規制及び契約上の義務の要求事項を考慮することとしている。規格は、リスクアセスメント及びリスクプロセスの中で情報セキュリティ要求事項をはっきり意識した形で管理目的、管理策を選択するということが明確に位置付けされたと理解されるとよい。

**適用宣言書**：これまでは、リスクアセスメントの結果明らかに保有することとなった管理策は論理的には適用除外とすることが可能であったが、審査において現在実施している管理策であれば採用しましょうということになっていたと思う。リスクアセスメント及びリスク対応のプロセスから選択した管理目的及び管理策と選択した理由は従来どおりであるが、加えて、現在実施されている管理目的及び管理策も選択することとなる。リスクマネジメントの継続的改善の結果、管理策によってリスクが受容されていくわけで、それが現在実施されている管理策となっていく。従って、その経緯が追えればよいと考えられる。適用除外の理由は、適用範囲の要求との関係から明確にしなければならない。また、適用宣言書の用語の定義に、参考として、管理目的及び管理策は情報セキュリティ要求事項から明確にされるものであるとしている。

**ＩSMSの有効性**：ＭＳの有効性の評価は、内部監査及びマネジメントレビュー等を通して行っているが、それに加えて、選択した管理策が有効であるかどうかを測定する要求が追加された。選択した管理策又は管理策一式の有効性として、いわば 39 管理目的及び 133 管理策の網羅性を要求している。参考として、管理策の有効性を測定することにより、計画された管理目的が管理策によってどの程度達成されているのかを、管理者及び職員が判断することができるとしている。管理目的に着目して、何らかの指標で管理目的の達成度(管理策の成熟度)を測定する手順を明確にすることが求められている。

そのほかでは内部監査が外出しになった。これまではマネジメントレビューの中に位置づけられていたが、独立した章立てとなった。内部監査は経営陣のコミットメントできちっとやられてきたと思うが、他の ISO 規格と同様に経営陣のコミットメントの中で明確に回るようにせよということである。

**リスクの見直し**：リスクアセスメントについて、予め定められた間隔での見直しの要求が追加された。総じて変更点は以上のようなことが明確になった。

附属書 A は「Normative」、規定として要求事項である。本文の中では要求事項としては明記していないが、組織が適用宣言書に適用とした管理策が要求事項と考えればよい。第５章から第 15 章までの項番は、17799 と整合している。第 13 章にインシデント管理の分野が追加された。次に各章の変更点を紹介したいと思う。

0 序文：大幅な変更はない。OECD ガイドラインに言及している(付属書 B に原則を記述)。Act のレベルで、マネジメントレビュー、内部監査その他関連情報に基づく是正・予防処置が追加された。

1. 適用範囲：1.1　一般。“business”という言葉の、ISMS としての定義が行われた。参考 1 に事業 business の解釈があるが、すなわち、広義に、その組織の存在理由にかかわる活動と解釈される。参考 2 に 17799(管理策設計の手引)の位置付けが加わった。

2 引用規格：引用規格は 17799 だけになった。組織は管理策を適用とした場合に、その実装にあたっては 17799 を導入の手引きとするということである。

引用規格は、認証規格の一部をなすことになる。これまで引用規格としていた JIS Q 9001 や TR0008 の引用は審査の中で少し混同があった。例えば TR Q 0008(リスクマネジメントの定義)は、定義の表が良くできていて、リスクアセスメントはそのとおりにしなければならないとも読めた。あくまで言葉の定義であり要求事項ではない。

3 用語及び定義：追加された用語は 4 つ。

資産、組織にとって価値をもつもの(ISO/IEC 13335-1:2004 参照)である。JIPDEC は、従来資産と情報資産の区別をつけずに“情報資産”として扱ってきたが、原規格のとおりに使い分けることになる。

情報セキュリティ事象、及び情報セキュリティインシデント(何れも ISO/IEC TR 18044:2004)が追加された。「セキュリティインシデント」はセキュリティ事件・事故の用語を使用してきたが、顕在化に至らずとも懸念されるセキュリティ事象も含む確率的な意味合いを持つので「セキュリティインシデント」をそのまま使う。

残留リスク(ISO/IEC Guide 73)が追加された。

見直された定義は 5 つ、可用性、機密性、情報セキュリティ、完全性、適用宣言書である。可用性、機密性、完全性は ISO/IEC 13335-1:2004 を、情報セキュリティは 17799 を引用。可用性説明文の‘entity’は個人や団体ということ。関係あるエンティティでは、規格において顧客との関係、契約上の義務が出てくるが、顧客とのアクセスはさまざまである。プロセスもエンティティに入ることになる。

適用宣言書は組織の ISMS に関連して、適用する管理目的及び管理策を記述した文書である。「参考」欄に、管理目的および管理策は、組織の情報セキュリティに対して以下に基づくこととして、リスクアセスメント及びリスク対応のプロセスの結果及び結論、更に法的又は規制要求事項、契約上の義務、事業上の要求事項を加え、情報セキュリティの要求事項を明確に位置付けよと言う。従来は「リスクアセスメントの結果から」だった。

宣言書の作成方法としては、管理目的及び管理策の適用理由として、「契約上の義務から」、「事業上の要求事項から」、「法的又は規制要求事項から」、「リスクアセスメント及びリスクプロセスの結果から」問い、その観点から選択したことがわかるようにすればよいと思う。新しい適用宣言書は、管理目的を達成する目的は何か、法的要求事項或いは組織の事業上の要求事項との関係を明確にすることに意味がある。あと 7 つの用語は変わらない。

4 情報セキュリティマネジメントシステム：

4.2.1　ISMSの確立：a) 適用範囲は大幅追加の変更である。“当該適用範囲からの除外の詳細及びその理由(1.2 参照)も含め”と、ISMS の適用範囲及び“境界を定義する”が追記された。組織全体を適用範囲とする場合でも、組織内にあった機能をアウトソーシングすることになれば、その境界がセキュリティ上重要である。ある事業範囲を適用除外する際に、事業、組織、所在地、資産及び技術の特徴等が明確になることに加え、適用除外される部分の詳細と境界を明確にすること。また、(1.2 参照)とあり、適用宣言書の適用除外項目の理由も精査することが求められる。審査は「境界」の確認から始めていく。判定委員会においては「適用範囲」が主要な審議課題でもある。

4.2.1c) リスクアセスメントの取組方法の策定：先にも述べたが“ISMS 基本方針と目標を設定する”要求が削除された。

c)1) 情報セキュリティの 3 つの要求事項を勘案し、リスクアセスメントの方法を特定することに変わりはない。要求事項の 1 つは当該 ISMS に適していること。主に当該 ISMS の中でリスクアセスメントをしてリスク対応をして行くプロセスになる。あとの 2 つは明確にされた事業上の情報セキュリティ要求事項と識別された法的及び規制要求事項である。法的、規制及び契約上の要求事項は、管理策 A.15.1.1「適用法令の識別」で明確にし、文書化することが要求されており、特に、“要求事項を満たすための組織の取組み方法を明確に定める”ことが要求されていることは注目する必要がある。

c)2) “リスクを受容するための基準の作成、受容可能なリスク水準の特定”とリスク受容の基準の作成が追加された。この基準と水準は、5.1f)参照となっているから、経営陣が決める必要がある。登録審査では、多くの企業がコンサルタントに支援してもらってリスクアセスメントを行っており、手順書の中で、この基準と水準が書き込まれてい

るのを見る。導入時にはいたしかたないことかもしれない、一回りすればマネジメントレビューでこの水準と基準を経営陣が決めることではある。しかし、導入時にも経営陣の明確な関与が必要である。リスクアセスメントにおけるリスク値の算定が定性的なものを相対値化しており、リスク受容基準も定性的なものとなるから、それに意味づける必要がある。喩えが適当ではないかもしれないが、例えばリスクを受容するための基準を血圧としよう。私は高齢になったので高血圧になっているが、高血圧は、病院で測る場合は下が90、上が150以上で、家で測る場合は下が80、上が140以上と定められている。その他にも低血圧、至適血圧など血圧のバロメーターが作られている。医者に行って血圧の測定を継続して、160を超えたころに“そろそろ薬を使いましょうか”と言われいよいよ高血圧症になったか、その値がその人における“水準”ということになる。血圧を下げるために、運動をしたり、体重を調整したり、過労にならないようにする“管理策”を実行しながら、その効果があったかどうか“血圧測定”をする。マネジメントレビューでは、160とした“水準”がこのままで良いのか、やはり140とした方が良いのかが検討され、さらに高血圧の基準自身も検討する必要があるかどうかも検討される。リスクマネジメントも同じように行われるということである。やはり効果測定も重要なことである。

また、選択したリスクアセスメントの方法が比較可能で再現可能であることの要求が追加された。リスクアセスメントの結果を比較するためには、結果が安定している必要があり（いつもほぼ同じ結果がえられること）、再度測定してもほぼ同じ結果がでることが必要である。リスクアセスメントの方法論の参考情報としてISO/IEC TR 13335-3が紹介されている。今後MICTS-2に改訂され、さらにISO/IEC 27005にガイドラインとして制定される予定である。リスクアセスメントの方法論は文書化の要求となったが、これまでも多くの企業でリスクアセスメント手順書を策定していたと思うので問題はなかろう。

d) リスクを識別：“資産及び資産の保有者(オーナー)の特定”と情報資産が資産に、責任者が保有者となる。保有者には解説があり、財産の所有者ではなく“責任をとる”人のこと。情報システムでは、従来、データを情報システム部門が管理していることから、業務部門はその利用者という錯覚がある。データの管理者は業務部門にあることを理解する必要がある。

e)2) アセスメントをする際に“現在実施されている管理策を考慮する”というのは、その管理策によって、脆弱性が低くなっていることであり、経営陣がきちんと認識できるように、適用宣言書にも反映することが求められている。

g) 管理目的及び管理策の選択。大幅に変更された。“リスクアセスメント及びリスク対応のプロセスで明確にされた要求事項を満たすために”と目的が明確になった。また“この選択では、リスクを受容するための基準 4.2.1c)2)、法律、規制及び契約上の要求事項を考慮する”。このような形でリスク対応をし、管理目的、管理策を選択する時のプロセスを明確にすることを要求している。

j) 適用宣言書。j)2)現在実施中の管理目的及び管理策を含むこと、j)3)附属書 A 管理目的・管理策で適用除外した理由の明記が各要求事項になった。適用宣言書は外部公表も考慮し、外向け用と管理用の中向け適用宣言書という位置付けもよい。

**4.2.2 ＩSMSの導入及び運用**。ここで新たな要求事項は d) 管理策の有効性評価。管理策一式とはグループだが、測定方法には個々もあればグループもある。測定の目的はリスクが本当に減ったかどうか測定することである。リスクアセスメントの流れからすると、まずリスクを減らす管理目的は何かを知ることから始めると良い。

実際審査の場面では、組織がリスクアセスメントの結果から、管理策を直接選択している場合が多く、管理目的を選択している認識が薄い場合が多い。識別されたリスクに対して、そのリスク対応するための目的である管理目的を認識できれば、管理目的を達成するためのいくつかの管理策が導かれるはずである。管理策の有効性とは、管理目的の達成度と見ることもできる。

その測定法は、定量的に扱えるものもあれば、定性的なものを統計的に処理する必要があるものもある。その測定法の定義が要求事項となった。

ISO/IEC 27004でガイドラインを提供されることになるが、現在WDのレベルでも各国から分厚いコメントが提出されているようで、まだ紆余曲折があろう。当面、JIPDECは、IPAの報告書のセキュリティの定量的尺度を紹介している。例えば“情報資産の定期的なリスク見直し率”といった感じである。いわゆる管理策の成熟度の測定で、情報セキュリティ監査制度で試みられた127の詳細管理策に対して、７～９個のサブコントロールを用意して、アンケート調査によりその成熟度を、助言型と認証型に分類、セキュリティ分野のレーダーチャートに表したが、この方法もヒントになるであろう。

規格は網羅性を要求している。経営陣がセキュリティの全体状況を把握することが必要であるということで、その状況についてすべての管理策に

ついて詳細な測定が必要であるといっているわけではない。基本的なセキュリティ分野についてはマネジメントレビューで経営陣が判断することも含めて合理的な測定が望まれる。

4.2.2d) 参考、「管理策の有効性を測定することにより、計画された管理目的が管理策によりどの程度達成されているのかを管理者及び職員が判断することができる」、強調しておきたいことである。

**4.2.3 ＩSMSの監視、見直し**：チェック段階である。

a) 次のこと(5項目)を行うため、監視及び見直しのための手順や他の管理策を実施する。その中で、“4)指標を利用することにより、セキュリティ事象の検出を容易にし、その結果セキュリティインシデントを防止する”と表現をかえ、また、“処置を決めること”が“5)セキュリティ違反を解決するためにとった処置の有効性を判断する”と変更された。

ISMSは予防のシステムである。起きたら後は修復しかない。事件が起きる前の監視の仕方が審査の重要な判断材料になる。その時利用する指標には、技術的な指標もあれば人的な指標もあろう。

指標を利用する意図を知り、セキュリティ事象の検知を容易にする。その結果セキュリティインシデントを防止する。そのための指標だということを認識してほしい。

b) ＭＳの有効性に関する定期的見直しの中に有効性の測定結果が加わりＭＳの有効性の把握のために日常的なセキュリティ管理策の測定結果を判断材料とすることが明記された。

c) “セキュリティ要求事項が満たされていることを検証するために、管理策の有効性を測定する”が追加され、日常的なセキュリティ管理状況の把握が明確になった。

d) “あらかじめ定められた間隔でリスクアセスメントの見直しを行い、残留リスク及び識別された受容可能なリスク水準の見直しを行う。その際、次の事項に生じる変化を考慮に入れる(1～6)”、大幅追加された。特に“5)実施された管理策の有効性”を考慮する必要がある。

g) “監視及び見直しの活動で検出された事項を踏まえて、セキュリティ計画を更新する”が追加された。セキュリティ計画が突然出てくるが、計画にはリスク対応計画以外にもいろいろあるだろうということだ。計画はリスク対応管理策に限らない。例えば契約、法律及び規制上の要求事項に対する計画などである。

**4.2.4 ＩSMSの維持、改善**：c) 大幅変更され分かり易くなった。“全利害関係者に講じた処置を伝達し合意を得る”が、“状況に応じた詳細さで講じた処置及び改善を伝達し、該当する場合は今後の進め方について合意を得る”となり合理的に対応できるようになった。

**4.3 文書化に関する要求**：4.3.1“文書は経営陣の決定に関する記録を含むこと。経営陣の決定及び基本方針まで活動が追跡できること、記録された結果が再現可能なこと”。文書で“選択した管理策から遡って、当該管理策、リスクアセスメント、リスク対応のプロセスの結果まで関連が実証できること”。更に“遡ってISMS基本方針及び目的までの関連が実証できること”、重要なポイントである。

g) リスクアセスメントの方法と有効性の測定結果の文書化要求。マネジメントレビューとのつながりで有効性の測定結果は7.2f)インプット(新規)に、そして7.3 e)有効性測定方法についてもPDCAを回す(新規)ということである。

4.3.2f) は、セキュリティの管理策である。“必要とする人が使用可能である。文書はその分類区分の手順に従って移動、保管、廃棄される”(新規)。ISMS文書の取扱手順を決めることになる。

**5.1 経営陣のコミットメント**：f)“リスクを受容するための基準4.2.1f)”が加わり、g)“内部監査実施”が追加された。内部監査は章立てされ(6参照)、経営陣のコミットが要求される。

**5.2 経営資源、6 内部監査**、内容に特段変更はない。

**7.2 マネジメントレビュー**(以下、M/R)**へのインプット**。変更ではないが、e)“ぜい弱性又は脅威”に留意。最初に気付くのはぜい弱性だ。ぜい弱性の観点からリスクアセスメントをする。新しい情報資産が加わるとこれに対して新しいぜい弱性が出てくる。一般に脅威は変わらないが、例えば地震が殆どない地域では地震を脅威と認識していない。一度地震が起きると脅威となる。このような例はそうざらにはない。そして、f) 有効性の測定結果4.2.3c)が加わった。

**7.3 M/Rからのアウトプット**。b)“リスクアセスメント計画及びリスク対応計画の更新”が追加された。c) 管理策の修正対象としてc)5)“契約上の義務”が追加された。今改訂で特に“契約上の義務”がクローズアップされているから意識して欲しい。6)「リスク受容可能な基準」については5.1f)で説明した。

e)“管理策の有効性を測定する方法の改善”が追加された。

**8.2 是正処置**:“ISMSの導入及び運用に関連した”が“ISMS要求事項に対する不適合”に変わった。是正処置の対象が広くなった。“ISMSの導入及び運用における不適合の識別”が“不適合の特定”に短縮された。

是正処置については、詳細管理策8.(4)③「障

害記録」で“障害については報告を行い、是正処置をとること”として、ISMS の運用に関連した是正処置となっていた。情報システムの運用にかかわる障害では、一般に障害報告書が起こされる、その中で、不適合を特定して是正処置手順をとることとなるが、その場合に是正処置報告書を使用することは現実的でない。運用実態に合わせて、是正処置を取る事項を決めることができるようになった。因みに当該の管理策は A.10.10.5「障害のログ取得」“障害のログを取得し、分析し、また、障害に対する適切な処置を講じること”となっている。

**8.3 予防処置**：ISMS は殆どが予防処置がいかに機能するかによって MS の継続的な改善が可能となる。“不適合の発生を未然に防ぐための処置”から“ISMS 要求事項への起こり得る不適合が発生することを防止するために、その原因を除去する処置”に変わった。また b)“不適合の発生を予防するための処置の必要性の評価”が追加された。予防処置は、追加の管理策となることが多い。リスクアセスメントの結果からリスクを受容可能な水準まで低減することでリスク対応してリスクマネジメントが実施されているとすれば、追加の管理策は、さらにリスクを低減することになる。従って、その追加の管理策の予防処置としての必要性について評価しないと過大なリスク対応となって ISMS の主旨から外れることになる。予防処置は一拍おいて、その処置をすべきかどうか経営陣の判断が必要であることを意味している。

“⑤変化したリスクの識別、変化したリスクに注意を払う”は要求事項を規定することでないので削除され、“組織はリスクの変化を識別すること。また大きく変化したリスクに重点を置いた予防処置に関する要求事項を識別すること”と整理された。“予防処置の優先順位については、リスクアセスメントの結果に基づいて決定すること”と参考情報の“不適合を予防するための処置は、多くの場合、是正処置よりも費用対効果が高い”との規定は同じである。

**全体を通して** 用語の使い方で「基本方針」と「目的」に注意が必要である。

“security policy”には、個々の管理策についての“policy”(個別方針)を指す場合と、それらを統括・統制する全般的な“policy”(基本方針)を刺す場合があり、“ISMS policy”を ISMS 基本方針との用語を使用するようだ。また、“information security policy”と情報セキュリティ方針も使用されており、ISMS 基本方針との関係は、規格の中で、“この規格の目的のために、ISMS 基本方針は、情報セキュリティ基本方針を包含する上位概念とする”としている。経営陣の責任に“情報セキュリティ基本方針”が要求されているが、これは、附属書 A.5.1 情報セキュリティ基本方針に関係している。附属書 A は、17799 と整合がとられており、17799 は、セキュリティガイドラインとして構成されている。セキュリティガイドラインを実践的に取り組むとマネジメントシステムを導入することになるが、基本方針はあくまでも情報セキュリティの基本方針である。従って管理策としては、経営陣が承認した“情報セキュリティ基本方針”を、全従業員及び関連する外部関係者に公表通知するとしている。27001 は先に発行された 17799 を取込もうということで ISMS 基本方針と情報セキュリティ基本方針との関係を整理する必要があり、規格の 4.2.1 b)の参考情報で先述のとおりとなった。

ISMS 基本方針は、情報セキュリティ基本方針にマネジメントの要素を加えたものであるから、行動指針を示す情報セキュリティ基本方針にマネジメントの要素を加えればよいことになる。その要素は、ISMS マニュアルそのものであることから、情報セキュリティ基本方針を包含した ISMS マニュアルが ISMS 基本方針(ポリシー)であると主張されるのも良いと思う。

“objectives”も同じように“an organization's overall policies and objectives”“business objectives”“ISMS policy, objectives, process and procedures”“information security policy and information security objectives”“control objectives and controls”などの用例があるが、そのすべてに“目的”をあてることになる。

JIS Q 27001:2006 は、翻訳規格なので、解釈に問題があれば原国際規格で理解をすることができるので、今後の実践の中で評価されることになると考えられる。

引用する附属書Aは規定と言うことで要求事項。17799 は should 文、附属書 A は shall 文である。附属書 B(参考)に“OECD 原則及びこの規格”附属書 C(参考)に“QMS,EMS、及びこの規格の比較”が追加される。【次号「附属書 A 解説」に続く】