2014.1.6

情報セキュリティニュース ＜2013 No.4＞

ISO/IEC 27001 2013 年版改訂のポイントと企業への影響

情報セキュリティマネジメントシステムに関する国際規格「ISO/IEC 27001:2013」が、ISO(国際標準化機構)と IEC(国際電気標準会議)の合同技術委員会 JTC 1 で投票にかけられ、2013 年 9 月に承認された。同規格が 2005 年に発行されて以来、8 年ぶりの改訂となる。本稿では本改訂のポイントとそれによる組織への影響と対策について説明する。

ISO/IEC 27001 は、その前身である英国規格の BS 7799-2 をベースとして 2005 年に発行された。ISO 規格は通常 5 年ごとに定期見直しが行われることとなっており、ISO/IEC 27001:2005 も 2009 年より改訂審議が始まった。その後様々な審議を経て、発行から 8 年になった 2013 年に、いよいよ改訂に至ったところである。

日本では、2002 年に BS7799-2 に基づいた ISMS 第三者認証制度が開始され、2006 年に ISO/IEC 27001:2005 ベースに移行、認証制度開始から 11 年が経過した 2013 年には、4420 の組織が認証を取得している(2013 年 12 月 18 日現在)。

1. ISO/IEC 27001 改訂のポイント

2005 年の ISO/IEC 27001:2005 発行後、多くの関連規格の発行やクラウド活用の隆盛など、情報セキュリティマネジメントを取り巻く状況そのものが変化したこと、またマネジメントシステム規格の構造や、リスクマネジメントの考え方などが ISO 内での議論によって標準化されたことに伴い、ISO/IEC 27001 も改訂時にそれらの影響を受けることとなった。ここでは、そうした他規格からの影響を中心に ISO/IEC 27001 の改訂のポイントについて解説する。

1.1. マネジメントシステム共通テキストへの準拠

まず、最大のポイントとしてマネジメントシステム規格のテキスト、構造が統一されたことが挙げられる。マネジメントシステム規格は、ISO 9001 をはじめとしてこれまでに数多く発行され、これらを複数適用している組織は全世界的に多数存在する。中でも ISO 9001、ISO 14001 などは全世界で数万組織が適用する規格である。

すべてのマネジメントシステム規格は、PDCA サイクル[1]に基づいているが、そのうちの P・C・A の部分にはどの規格にも共通した要素、要求事項が多い。しかしこれまではこれらの共通の要素について、①文書構成が統一されていない、②同じ要求事項が規格によって違う場所に書かれている、③用語の定義が異なる、など、複数のマネジメントシステムを調和、統合して運用することが難しい状況となっていた。

そのような状況の中で、ISO 規格を発行している国際標準化機構では規格間の整合性向上を図り組織の負担を軽減するため、5 年余りの歳月をかけてマネジメントシステム規格における、「企画の章立て」「規定文（要求事項)」「用語と定義」の 3 つについて共通テキスト[2]を検討し、2012 年には決定に至った。以降、新規に開発、改訂される全てのマネジメントシステム規格には共通テキストの適用を義務づけることとなった。

---

[1] Plan(計画), Do(実行), Check(確認), Act(改善) からなるマネジメントシステム改善サイクル。

[2] 「ISO/IEC 専門業務用指針第一部 統合版 ISO 補足指針 - ISO 専用指針附属書 SL」
http://www.jsa.or.jp/itn/pdf/shiryo/iso_supplement_sl234.pdf

マネジメントシステム共通テキストの適用が ISO/IEC 27001 に与える主な影響として、次の 3 点が挙げられる。

1.1.1. 文書構成の変更

統合運用の促進、可読性の向上のため、マネジメントシステム共通テキストを導入したマネジメントシステム規格では、文書構成が統一され、2005 年版から大きく変更されている。

ISO/IEC 27001:2005 と、共通テキストに従い再構成された ISO/IEC 27001:2013 の目次比較及び、移行先を表 1 に示す。

表 1 ISO/IEC 27001 新旧目次比較と移行概要

ISO/IEC 27001:2005		ISO/IEC DIS 27001:2013
0 序文	→	0 序文
1 適用範囲	→	1 適用範囲
2 引用規格	→	2 引用規格
3 用語及び定義	→	3 用語及び定義
4 情報セキュリティマネジメントシステム		4 組織の状況
4.1 一般要求事項		5 リーダーシップ
4.2 ISMS の確立及び運営管理		6 計画
4.3 文書化に関する要求事項	→	7 支援
5 経営人の責任		8 運用
6 ISMS 内部監査		9 パフォーマンス評価
7 ISMS のマネジメントレビュー		10 改善
8 ISMS の改善		
附属書 A	→	附属書 A
附属書 B		
附属書 C		

表 1 に示した ISO/IEC 27001:2013 の 0～10 の章構成は、先述したとおり、共通テキストと同じものである。

新しい構成は、PDCA サイクルが規格要求事項上で明確になった(Plan が 4～7 章、Do が 8 章、C が 9 章、A が 10 章)。

ここでの留意点は、現在の ISMS(情報セキュリティマネジメントシステム)でのリスクアセスメントに関する内容（現在は 4 章に書かれている）が 6 章(Plan)及び 8 章(Do)に分かれて記載されることだろう。具体的には「定期的なリスクアセスメントの実施」が 6 章、「運用中における臨時のリスクアセスメント」が 8 章に、それぞれ分割して記載された。これまで ISMS のリスクアセスメントは Plan フェーズで行われる整理となっていたが、改訂後は Do フェーズでのリスクアセスメントについても明記された。これは、組織を取り巻く状況の変更（拠点の移転、事業の撤退、追加、ステークホルダーの大規模な変更など）が ISMS の運用中に突発的に発生した場合、Plan フェーズに戻るのではなく、Do フェーズの中でリスクアセスメントを行い修正する、と整理されたと理解できる。この点、ISMS における PDCA サイクルの位置付けを理解し直す必要があるだろう。

これはほんの一例であり、既に認証を取得している組織は上記の表や ISO が発行した新旧対照表[3]を参照するなどし、2005 年版の ISO/IEC 27001 の記載が改訂後どこに移動したのかを把握の上、文書構成とその意図について理解・整理しておきたい。

また、ISO 9001, 14001 等も 2015 年頃と言われる次回改訂時には本構成に準拠すること

[3] http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=wg1sd3

になる。ISO/IEC 27001 の認証を取得していない他規格の認証取得組織も、先述したマンジメントシステム共通要素については、一読しておくことをお勧めする。

1.1.2. ISO 31000 に準拠したリスクマネジメント

マネジメントシステム共通テキストの導入に伴い、ISO/IEC 27001 のリスクマネジメントは ISO 31000(リスクマネジメント－原則及び指針)に準拠することとなった。

1.1.2.1. ISO 31000 とは

ISO 31000 は、すべてのリスクを管理するための汎用的なプロセスと、そのプロセスを組織の業務に効果的に組み込んでいくための枠組みとして 2009 年に作成され、以来リスクマネジメントに関する事実上の標準として利用されているものである。マネジメントシステム共通テキストにもその考え方の多くが採用され、今後のすべてのマネジメントシステムには結果的にこの枠組みが適用されることになる。

なお、ISO 31000 は、日本では JIS Q 31000 として公表されており、JISC(日本工業標準調査会)の Web サイト[4]にて無料で閲覧することができる。

1.1.2.2. ISO/IEC 27001 への影響

ISO 31000 が ISO/IEC 27001 に与える影響として最も大きなものの一つが「リスク」の定義である。ISO 31000 による定義は「目的に対する不確かさの影響」である。言いかえれば、リスクとは計画に対するブレであり、上ブレ、下ブレの両方を含む概念だということである。一般的に想像されやすい「ネガティブな影響（下ブレ)」に限定されないことに留意が必要である。ISO/IEC 27001 における用語や定義は現在最終ドラフトの状況である ISO/IEC 27000 を参照することになっており、これは間もなく改訂されることが予定されている。ISO/IEC 27000 は前回の 2012 年改訂で既に ISO 31000 に準拠したリスクの定義となっており、ISO/IEC 27001 の改訂に合わせた今回の改訂でも、マネジメントシステム共通テキストに準拠しつつ、その表現が維持されることが見込まれている。ISO/IEC 27001 の 2013 年版では、組織に対し「ISMS の適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスク(6.1.2 c)」を特定し管理することを求めている。この中には「機密性喪失のリスクを積極的に取っていくことで情報の可用性を向上させ、事業の拡大を目指す」と言ったようなリスクを積極的に上ブレさせていくような内容も当然に含まれるだろう。

なお、ISO/IEC 27001 のリスクアセスメントが ISO 31000 と整合していることは要求事項 6.1 の注記として記載されている。

1.1.3. 予防処置の削除

今回の改訂により、「10 章 改善」の要求事項は「不適合及び是正処置」及び「継続的改善」の 2 つのみとなり、「予防処置」は単独の要求事項としては存在しなくなった。これは「マネジメントシステムの活動そのものが予防処置である」との意図から変更されたものである。ただし予防処置の考え方は「6.1 リスク及び機会への取り組み」に内包されている。また、ISMS のパフォーマンスを測定・評価することが 9 章で「パフォーマンス評価」として要求されているが、この中でいわゆる「予防処置」に対する効果測定と分析、評価を行うことも盛り込まれており、実質的な要求は強化されていると見ることができる。

[4] http://www.jisc.go.jp/

1.1.4. 文書・記録の用語の統合

これまでのマネジメントシステム規格では、文書と記録の 2 つが定義され、管理対象となっていたが、今回の改訂では「文書化された情報」として用語が統合された。この中で、従前では文書または記録と呼ばれていたものの読み分けとしては、「証拠として」という表現を目安にすると良い。「○○の証拠として、文書化された情報を保持する」と言った表現があれば、それは記録として扱うべきものである。なお、2013 年版における記録に関する要求事項は 2005 年版とほぼ同一である。

2. 附属書 A（管理策）の最新化・整理・統合

ISO/IEC 27001:2005 の附属書 A の管理策も見直しが行われた。2013 年版においても多くの管理策は 2005 年版のものを引き続き採用しているが、ISO では ISO/IEC 27001:2005 発行以後、ISO 27030 番台において技術的な内容をガイドラインとして整備してきた。それに伴い、今回の ISO/IEC 27001 の改訂では、既存の管理策に関しては本来「情報セキュリティマネジメント」として管理すべきもののみを残し、残りは他の規格を参照する方針が採られた。その結果、例えばネットワーク管理などの管理策は ISO/IEC 27033 を参照する形を取り、ISO/IEC 27001 の管理策からは削除されるなど、管理策の数は 2005 年版の 133 項目から 2013 年版は 114 項目に整理された。

本章ではその中で特に重要なポイントについて解説する。

2.1. サプライチェーンに関する管理策の追加

ISO/IEC 27001:2013 では、「供給者関係」という管理策が新規に追加された。これは 2005 年版の「A.6.2.3 供給者との契約におけるセキュリティ」や「A10.2 第三者が提供するサービスの管理」が整理・統合された項目であるが、A.15.1.3 に「ICT サプライチェーン」という項目が追加されていることに注意したい。「サプライチェーン」という表現から、2005 年版より広い範囲、つまり直接契約関係を結ぶ対象のみならず、例えば外部のデータセンターを利用する場合、非常用電源の燃料の継続的な供給状況を気にするなど、「契約者の契約者」をも視野に入れる必要があるだろう。

2.2. 情報処理施設の可用性についての管理策追加

ISO/IEC 27001:2013 では、A17.2.1 に「情報処理施設の可用性」が新規追加された。この管理策には「情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない」とある。特定した情報にどの程度の可用性が必要なのかが分からなければ、どの程度の冗長性が必要なのかを決定できない。即ち、情報の可用性を十分に評価・分析することが 2013 年版では求められていると言えよう。

2.2.1. 可用性評価の例

情報が使えない、というリスクは、一般的にそれが顕在化している期間が長引けば長引くほど被害、損失が拡大していく傾向にある。つまり可用性は「時間」という尺度で評価することが大半である。

可用性評価の基準例として以下のようなものが考えられる。評価の参考にして頂きたい。

- 情報が格納・利用されているシステムに許容される停止時間
- 情報が格納・利用されているシステムの目標稼働率
- 情報を利用する業務が災害に遭った場合の目標復旧時間

可用性に関しては、ISO/IEC 27031 がいわゆる IT-BCP のガイドラインとなっている。

この規格は対訳版も発行されていることから、可用性の要求事項を満たすための一助になるだろう。また、国内のガイドラインでは経済産業省が発行している「IT サービス継続ガイドライン」[5]も参考になるだろう。

3. JIS 化と第三者認証の動向

3.1. JIS 化の動向

ISO/IEC 27001:2005 は、JIS Q 27001:2006 として国内規格になっており、2013 年版も JIS 化作業が進められているところである。現在 JIS Q 27000, JIS Q 27001, JIS Q 27002 は意見受付公告（いわゆるパブリックコメント）にかけられており、順調に進めば 2014 年 3 月ごろの発行になると見られている。意見受付公告中の規格は日本工業標準調査会の Web サイト[6]から無料で閲覧することができる。

3.2. 第三者認証について

第三者認証については、認定機関である JIPDEC(一般財団法人 日本情報経済社会推進協会)より以下の通りと発表されている。

- 2013 年版への移行　　：2015 年 10 月 1 日まで
- 2005 年版での新規取得：2014 年 4 月 1 日まで

既存の認証取得組織の 2013 年版への移行期限は「国際規格の発行から」おおむね 2 年間とされている。JIS 化されてから 2 年間ではないことに注意する必要がある。

ただし、自社の ISMS の運用スケジュール次第では、移行期限までの時間的余裕が少ないケースも生じうる。例えば年度にあわせて ISMS の運用を行っている組織では、2014 年 4 月から移行作業を開始しないと間に合わない可能性が高くなる。このような組織では JIS 化直後から移行作業を開始する必要が出てくるのである。

4. おわりに：組織は今何をすべきか

ISO/IEC 27001:2013 はすでに発行されており、認証を更新・取得しようとする組織はすぐに改訂内容を把握し、自社に適用する必要がある。ISO/IEC 27001:2013 は、ISO/IEC 27001:2005 の根幹を大きく変えることなく、他規格との親和性を高め、最新の社会状況を取り込み、また内容が整理された規格であると評価できよう。

しかしながら、ISMS の実施プロセスへの要求は変化しており、本稿で述べてきたようにいくつかの事項については追加で対応する必要があることを忘れてはいけない。組織が今後行うべきことは以下のように整理できる。

- 2005 年版と 2013 年版との規格要求事項の記載内容・記載位置の変更箇所確認
  - 特に現在認証を受けている組織は、先述した ISO のテキストや実際の規格文書を参照しながら、変更点を理解することが最も重要だろう。
- マネジメントシステム共通テキストの理解
  - マネジメントシステム共通テキストは、「マネジメントシステムはどのように構築されるべきか」を ISO 自身が定義したものであり、エッセンスである。情報セキュリティに限らず、マネジメントシステムの構築を企図する組織は必ず理解しておくべき文書である。
- ISO 31000 の理解
  - ISO/IEC 27001:2013 では、ISO 31000 をベースとしたリスクマネジメントを行う

[5] http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf
[6] http://www.jisc.go.jp/

ことを組織に期待している。これはすなわち ISO 31000 を理解してから ISO 27001:2013 ベースのマネジメントシステムを構築することが望ましいということを意味している。先述したとおり、ISO 31000 は JIS Q 31000 として発行されており、また日本語の解説書も多く発行されていることから、早期に理解しておきたい。

- 情報の可用性評価方法の検討
  - 情報の可用性リスクの評価・分析については、2005 年版の規格では実質的にはほとんど要求されていなかったことから、多くの組織が十分には実施していなかった。しかし、2013 年版では明確に管理策の一つとして可用性の確保が要求されているため、各組織では対応が必要となる。先述の通り、ISO/IEC 27031 や国内のガイドラインをベースに考えていくことで十分に対応できるだろう。
- 自組織における ISMS の 2013 年版要求事項への対応作業（文書改訂や運用の見直し）
  - ISO/IEC 27001:2013 及び関連規格、ガイドラインを十分に抑えた上で、いよいよ ISMS 文書と運用を 2013 年版対応にしていくことになる。先述の通り、認証の移行期間は ISO 発行から 2 年間であるが、国内での入手が容易になる JIS 化からは 1 年半しか残されていない。また移行審査の期限が 2015 年 10 月 1 日ということは、4 月～3 月で計画を組んでいる認証取得済み組織では実際には 2014 年度から対応を行う必要があることを示唆している。ここで改めて、自社のマネジメントシステムの運用スケジュールと、移行審査の期限とを見比べ、どのタイミングの審査で移行するか、しっかりと検討することを強くお勧めする。

参考文献

1. ISO/IEC 27001:2013 (国際標準化機構)
2. ISO/IEC 27001:2005 (国際標準化機構)
3. ISO/IEC 27002:2005 (国際標準化機構)
4. ISO 22301:2012 (国際標準化機構)
5. ISO/IEC 専門業務用指針, 第一部 統合版 ISO 補足指針 – ISO 専用手順:2012
6. IT サービス継続ガイドライン（経済産業省）

以上

インターリスク総研 コンサルティング第二部　BCM 第一グループ
主任コンサルタント 頼永　忍