2013.7.1

情報セキュリティニュース ＜2013 No.2＞

ISO/IEC 27001 の改訂動向と最新ドラフトの概説

1. はじめに：ISO/IEC 27001 の審議動向

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である ISO/IEC 27001(以下「ISO 27001」という)は、2005 年に発行され、今年で発行から 8 年になる。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、2005 年に策定された ISO 27001 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、現在は FDIS(Final Draft of International Standard: 最終ドラフト)の段階まで到達し、順調にいけば 2013 年秋から冬頃に改訂版としてリリースされることが予定されている。

本稿では、ISO 27001 の改訂に向けた理解の一助となるべく、公開ベースでの最新ドラフトである DIS(Draft of International Standard)について概説する。

2. ISO/IEC DIS 27001 改訂の概説

2005 年の ISO 27001 発行後、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標準化されたことに伴い、ISO 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 27001 の改訂のポイントについて概説する。

2.1. 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 をはじめとして既に数多く発行され、これらを適用している組織も全世界的に非常に多い。中には ISO 9001、ISO 14001 のように数万組織が適用する規格も存在する。

ほぼすべてのマネジメントシステム規格は、PDCA サイクル[1]に基づいており、P・C・A の部分には共通要素が多い。しかし、これまでは共通要素が多いものの文書構成が統一されておらず、同じ内容・要件が規格によって違う場所に書かれていたり、用語の定義が異なっていたりするなど、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 規格を策定している国際標準化機構は、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共通テキストを開発[2]した。2012 年以降、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。

マネジメントシステム共通テキストが ISO 27001 に与える影響として、次の 3 点が挙げられる。

2.1.1. 文書構成の変更

統合の促進、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、現行のものから大きく変更される。

---

[1] Plan(計画), Do(実行), Check(確認), Act(改善) からなる改善サイクル。

[2] http://www.jsa.or.jp/itn/pdf/shiryo/iso_supplement_sl234.pdf

現行の ISO 27001 と、共通テキストに従い再構成された ISO DIS 27001 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 DIS 27001 の 0～10 の項目は、共通テキストのと同じものである。

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

改訂版の留意点の一つとしては、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 2 項に書かれている）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「リスクアセスメント手順の文書化」が 6 章、「リスクアセスメントの実施」が 8 章に、それぞれ分割して記載されている。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こととなっていたが、改訂後は Do フェーズに変わることになる。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。

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を参照するなどし、現行の ISO 27001 の記載が改訂後にどこに移動するのか、出来るだけ早期に把握し、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になる。ISO 27001 の認証を取得していない他規格の認証取得企業も一読しておくことをお勧めする。

2.1.2. 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 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。

2.1.2.1. 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、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。したがって、マネジメントシステム共通テキストにも採用され、今後の

すべての（リスクを扱う）マネジメントシステムは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[3]にて無料で閲覧することが出来る。

2.1.2.2. ISO 27001 への影響

ISO 31000 が ISO 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」であり、一般的に想像されやすい「ネガティブな影響」に限定されないことが特徴である。ISO 27001 における各用語は ISO/IEC 27000（用語と定義）を参照することとなっているが、ISO/IEC 27000 は 2012 年の改訂で既に ISO 31000 に準拠したリスクの定義となっており、ISO 27001 の改訂に合わせた今年の改訂でもその表現は維持されることが予想されている。これまでの ISMS では情報漏えいや紛失などによるネガティブなリスクを取り扱っていたが、今後は情報セキュリティマネジメントを確実に運用することによる「企業価値の向上」や、可用性の向上による「事業の拡大」などをはじめとした「ポジティブリスク」をどう特定し管理していくかも、一つのポイントになるだろう。

2.1.3. 予防処置の削除

マネジメントシステム共通テキストに準拠した今回の改訂では、「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」は単独の要求事項ではなくなった。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」との意図からであり、「6 章 1 項 リスク及び機会への取り組み」全体に従前の予防処置の考え方は内包されている。ただし、何が予防され、どの程度の効果が ISMS にあったのかを測定・評価することが 9 章で「パフォーマンス評価」として要求されており、結果として「予防」への要求は強化される。

3. 附属書 A（管理策）の最新化・整理・統合

2005 年に策定された ISO 27001 は 8 年が経過し、附属書 A の管理策も見直しが行われた。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、2005 年以後の状況などを反映した改訂を行われている。管理策の数は 2005 年版の 133 項目から DIS 版では 113 項目に整理された。本章では特に重要なポイントについて解説する。

3.1. 「電子商取引サービス」の改訂

2005 年版で「電子商取引サービス」として記載されていた管理策は、ISO DIS 27001 で「公衆ネットワーク上の業務処理サービス」と改訂され、より一般的な内容になった。例えばクラウドサービスなどを利用する場合の管理策がここに入ると予想される。「電子商取引は行っていない」と適用除外していた組織も、改訂後には本項の適用可否を改めて検討する必要があるだろう。

3.2. サプライチェーンに関する管理策の追加

ISO DIS 27001 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」をまとめた項目であるが、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

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

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、契約者の契約者を視野に入れる必要が出てくることも考えられる。

3.3. 情報処理施設の可用性についての管理策追加

ISO DIS 27001 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。つまり、情報の可用性を十分に評価・分析することを改訂版では求めていくことになる。可用性に関しては、現在の ISO 27001 関連ガイドラインでは十分にカバー出来ていない状況であることから、各組織は今後評価基準を確立する必要があるだろう。

3.3.1. 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時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一つのアプローチ方法ではないかと考える。

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

4. おわりに：組織は今何をすべきか

冒頭でも述べた通り、最終版の ISO 27001:2013 は 2013 年秋から冬の発行が予定されており、ISO DIS 27001 は現在進行形で審議が進められているところである。まだ発行までに修正される点もあろうが、現在のドラフトを見る限り現行の ISO 27001 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、事業領域を(企業そのものの存続も含めて)より幅広くカバーするように見直し、整理された規格であると評価することが出来る。

しかしながら、その実施プロセスへの要求は変化しており、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は忘れてはいけない。今後の規格改訂に備え、ISO 27001 認証取得組織が事前に行っておくこと、規格改訂後に行うことは以下のように整理できる。

4.1. 規格改定前に実施しておくこと

- 現行規格と改訂版との規格要求事項の記載場所の変更箇所確認
- 情報の可用性評価方法の検討
- マネジメントシステム共通テキストの理解
- ISO 31000 の理解

4.2. 規格改定後に実施すること

- ISMS 関連文書を改訂版に合わせて改訂する。
- ISMS の運用を改訂版の要求事項に適合させる。
- 現行のリスク管理策と改訂版の附属書 A とを比較し、情報セキュリティ関連の対応策（マニュアル化しているものがあればマニュアルも）を見直す。

参考文献

1. ISO/IEC DIS 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

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