＜研究ノート＞

改訂情報セキュリティ規格の中小組織への有効活用

Effective application of the revised information security standard to small and medium-scale organizations

長野　加代子　Kayoko Nagano　(株) ピーアンドアイ
植野　俊雄　Toshio Ueno　ISU
齋藤　敏雄　Toshio Saito　日本大学

概要

情報セキュリティ規格が改訂された機会を捉え、主要な改訂内容を確認し、改訂の背景と狙いを明らかにした。その結果､次の５つのポイントが重要であることが浮き彫りとなった。(1) 組織の状況を把握し、課題を明確にする。(2) 課題に対する目標をトップダウンで決定する。(3) 目標に対するリスクと機会を決定する。(4) 実業務のプロセスに管理策を組み込む。(5) 管理策の有効性を評価し確認する。これらのポイントに着目した活用の方法を提案し、中小組織でも効果的なセキュリティ対策を講じることができることを示した。

キーワード：情報セキュリティ、改訂情報セキュリティ規格、中小組織

１．はじめに

2013 年 10 月に情報セキュリティの国際規格であ る ISO/IEC27001 が 改 訂（ISO/IEC 27001:2013）された。国内規格である JIS についても 2014 年 3 月 20 日に改訂版（JIS Q 27001:2014）が発行された。情報セキュリティ専門監査人部会と情報セキュリティ研究プロジェクトの合同研究会では、この改訂された規格を検討して改訂の背景と狙いを明らかにすることで、認証取得を目指さない中小組織にとっても役に立つポイントを抽出し、それらを効果的に活用する方策を見出すことを目的に研究を進めてきた。

本研究は、次のように構成される。２章では、最初に、改訂された情報セキュリティ規格から主要な改訂内容を確認し、改訂の狙いを明らかにする。次に、改訂の意図をその背景にまで遡りその真意を深読みし、新たな解釈を付け加える。最後に、改訂された規格の中から中小組織に対し有効に活用できるポイントを掘り出して整理する。３章では、個人情報を主として取り扱う中小組織を対象に、改訂情報セキュリティ規格を有効に活用したリスクマネジメントと管理策の選択について具体例を示すことで、活用の考え方を提案する。４章では、まとめと今後の課題を述べる。

２．ISO/IEC27001,27002 の主な改訂点とその解釈

主な改訂は、次の３点にある。

① ISO/IEC27001 の本文の章立て－「ISO/IEC 専門業務用指針」付属書 SL
②リスクアセスメント－ ISO31000（リスクマネジメント - 原則及び指針）
③新しい管理策の追加－「セキュア開発」、「サプライチェーン」、「冗長性」

本研究では、改訂の基本的な狙いは、次の２つにあると考えている。

①一つの組織で複数の ISO マネジメントシステムを運用する際の使い勝手を良くすること
②環境の変化に速やかに対応して、時代に合った管理策にすること

さらに付け加えれば、改訂に当たっては、より良いものにしようという心理も当然働いていたと

思われるので、業務現場で有効に活用される規格にするという狙いが強くあったと考えられる。

本研究では、この仮定に基づいて、新しく追加された部分を分析し、情報セキュリティの確保に有効な考え方と方策を抽出することを目的としている。管理策はそれを活用する組織によって必要に応じて選定されるので、管理策選定については次の３章に委ね、ここではISO/IEC27001本体の改訂点の中でどの組織にも共通して重要であると思われる項目を検討した。その結果、次の５項目を抽出した。組織の状況の把握、リーダーシップ、事業プロセスへのMS要求事項の統合、リスクと機会の決定、そして情報セキュリティリスクアセスメントである。以下ではこれらの各項目について改訂の狙いを明らかにし、その背景を検討し新たな解釈を付け加える。

(1) 組織の状況の把握

これは、規格（改訂版のISO/IEC 27001:2013及びJIS Q 27001:2014。以降単に規格という。）の「4. 組織の状況」の項目に規定されている。そこでは、マネジメントシステムの意図した成果を達成する組織の能力に影響を与える外部及び内部の課題を決定すること、利害関係者を特定し、その要求事項を特定すること、そして、これらを考慮してマネジメントシステムの適用範囲を決定すること、の３つが規定されている。改訂前は、同等の内容が序文に記述されていたが、今回の改訂で、新たに要求事項となった項目である。

マネジメントシステムの目標は、PDCAサイクルを回すことに留まるのではなく、例えば大切な情報を持っているので守りたい、顧客が情報とサービスをいつでも使えるようにするといったISMSを導入した理由、すなわち、事業上の意図した成果を達成することが、マネジメントシステムの目標である。そのために自社の課題を明確にし、その上で自社の状況にあったISMSを導入することが肝要であると強調している。

この点は自明のことであるが、つい見失いがちであり、そうならないよう常に明確にしておくことを要求事項に格上げしたものと解釈できる。さらに、これから取得しようとしている組織が抱く、どこから手を付けたら良いかわからないといった疑問、そしてマネジメントシステムを回すことに気を取られて活動が形骸化してしまっている認証取得済みの組織の問題に、今回の改訂が一つの回答を与えているのではないかと解釈できる。

(2) リーダーシップ

規格の５章が「リーダーシップ」の項目である。規格の「5.1 リーダーシップ及びコミットメント」において、トップマネジメントは次に示す事項によって、ISMSに関するリーダーシップ及びコミットメントを実証しなければならないと規定されている。ここで示す事項の中には、以下の項目が新しく追加されている。

a) 情報セキュリティ方針及び情報セキュリティ目的を確立しそれらが組織の戦略的な方向性と両立することを確実にする。

b) 組織のプロセスへのISMSの要求事項の統合を確実にする。

e) ISMSがその意図した成果を達成することを確実にする。

h) その他の関連した管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する。

全体を概観すると、改訂前の版の規格では、「5. 経営陣の責任」、「5.1 経営陣のコミットメント」であったものが、この規格では、「リーダーシップ」、「リーダーシップ及びコミットメント」に強化されている。また以前は、文末が、基本方針を確立する、役割及び責任を確立するというように、確立するとなっていたが、今回の改訂では、実証しなければならないとなり、コミットメント、つまり責任から一歩踏み込み、責任を果たしていることを実証することを要求しており、トップマネジメントの役割が強化されている。

さらに、組織の戦略的な方向性と合致する、情報セキュリティ方針及び情報セキュリティ目的を決定するという項目が追加されている。

経営の戦略的な方向性を決定しているのは経営者であるので、経営者が主導することではじめて、情報セキュリティが組織にとって有用なものとなると謳っていると解釈できる。

(3) 事業プロセスへのMS要求事項の統合

プロセスへの統合は、規格の5.1 b）に新しく追加された項目で、規格では、組織のプロセスへのISMS要求事項の統合を確実にするとなっている。組織のプロセスと漠然と記述されているが、次の２つの統合を総合して、統合されたプロセスを作ることを意味していると解釈できる。

①事業プロセスにマネジメントシステム（ISMS）を統合すること

②業務プロセスに情報セキュリティ対策を統合

すること

この追加された項目の背景を深読みすると、トップの関与が弱く、このためセキュリティ目的が戦略的な方向性と一致していない現状が散見されること、及びその結果として、マネジメントシステムが経営と分離してしまっている、また、セキュリティ対策も業務と分離してしまっているという課題の存在が浮かび上がる。

(4) リスクと機会の決定

これは、規格の「6. 計画」に新たに追加された項目で、外部及び内部の課題、利害関係者の要求事項を考慮して、意図した成果を達成するために、リスク及び機会を決定すると規定されている。

この項目の追加では、意図した成果を達成するための計画を立てること、及びその計画にはプロセスへの統合と有効性の評価を含めることが強く求められていると解釈できる。前述の (1) 組織の状況の把握の項を受けて、計画と実行について、同じことをここでも記述しており、かなり強調したかったことが推察できる。

(5) 情報セキュリティリスクアセスメント

規格の 6.1.2 に次のように規定されている。

①リスクアセスメントのプロセスを定める

②機密性、完全性、可用性（CIA）の喪失に伴うリスクを特定する

③特定したリスクを分析する

④リスクを評価する（最初に決めたリスク基準と比較）

これを見ると、リスクアセスメントに関しては、基本的に変わっていないことが分かる。規格では、6.1.2 c）で情報セキュリティリスクを特定する、情報の CIA 喪失に伴うリスクを特定し、これらのリスク所有者を特定するとなっている。一方、ISO31000 では、「5.4.2 リスクの特定」で、組織の目的の達成を実現、促進、妨害、阻害、加速、遅延するリスクを包括的に特定するとなっていて、両者が確かに整合していることが見て取れる。そこで ISO31000 流に表現すると、

①セキュリティの目的を定める

②目的に対するリスクの特定、分析、評価をする

③目的に沿ったリスク対応（対策の選択）を行うとなる。

深読みすると、ISO31000 流にトップダウン方式でのリスクアセスメントも可能であると解釈できる。資産の個々のリスクではなく、目的を損なう情報のリスクをアセスメントする。逆に言えば、目的を損なわなければ、個々の資産は、リスクアセスメントの対象とする必要はない、とも言える。ボトムアップでもトップダウンでも、結局は重要な情報資産をアセスメントすることになるので、同じ結果を得ることになる。

以上の改訂された規格の狙いと意図に関する考察を踏まえれば、情報セキュリティ確保のための有効な方法は、次のようにまとめられる。

1）組織の外部及び内部の状況を把握し、組織にとっての重要課題を明確にする

2）課題に対する目標をトップダウンで決定する

3）目標に対するリスクと機会を決定し、費用対効果を重視して管理策を決める

4）実業務のプロセスに管理策を組み込み、マネジメントシステムの統合を図る
また、業務の中に組み込むことで管理策を確実に実施する

5）管理策の有効性を日常活動の中で評価し確認する

3．改訂情報セキュリティ規格の中小組織への活用

本章では、中小組織を対象として、改訂情報セキュリティ規格を有効に活用する考え方と方策を検討するが、具体的には中小組織として、次のような主に個人情報を取り扱う業種を想定している。

①販売業務
顧客からの購入申し込みを受け付け、顧客と購入内容をデータベースに登録し、顧客管理に利用する

②個人データのエントリ業務
個人に関する原始情報を預かり、データベース化する

③個人データのメンテナンス業務
個人に関する異動情報を預かり、データ内容の確認、データベースの更新、削除、抽出・出力などをする

④医療業務
患者の診療情報を電子カルテに入力し、データベース化する

以下では、前章で考察した、改訂版の規格に基づく情報セキュリティ確保のための有効な方法に沿って、適用の仕方を具体的に検討する。

(1) 重要課題の決定

これらの業務を担う中小組織にとって、情報セキュリティ面での重要課題はもちろん、取り扱う個人データの流出・不正使用・誤謬・滅失の防止になる。

(2) 目標の設定

経営者の視点で目標を決める。例えば、個人データの保護及び顧客の信頼の維持・向上を目標とする。

(3) リスクアセスメントと費用対効果を考慮した管理策の選定

次に、リスクアセスメントを実施する。個人データを取り扱う今回の例では、主に次の４つのリスクが特定できる。

①ネットワーク経由の外部からの不正アクセスによる個人情報盗用

②内部者による個人情報の不正持ち出し

③データ保存装置・媒体の紛失・盗難・不確実な廃棄による個人情報流出

④装置・媒体の故障あるいは誤動作による個人データの損壊・滅失

リスク対応としては、以下に示す個人情報、個人データの保護とモニタリングが基本になる(図１)。

①個人データを格納しているサーバや媒体の保護
サーバの隔離、サーバ設置場所への入室制限をかけて物理的にアクセス制限をかける、あるいはデータを暗号化する。

②データ管理のシステムのメンテナンスからの保護
OS 管理者、DBMS 管理者、そしてアプリケーション管理者の権限を管理する。

③業務上のデータ利用者からの保護
必ずアプリケーションを経由してデータへのアクセスを許可する、データの操作に制限をかける。

④システムのモニタリングとレビュー
ネットワーク / システム / データへのアクセス、業務上のデータ利用、システムのメンテナンスについてログ採取やログ記録を行い、ログ保存の監視、ログの内容の点検及びレビューを行う。

次にこれらのリスク対応にふさわしい費用対効果を考慮した管理策を選定する。

中小組織の場合には、人及び技術的な問題を考慮することが必要になる。そこで管理策を選定する前に、採用する情報システムの形態を検討することが重要になる。例えば、データの格納庫であるサーバをスタンドアロン形態にすれば、ネットワーク経由の外部からの不正アクセスを考えなくて済むのでリスク対応が軽減でき、したがって適用する管理策も縮小できる。ただし、スタンドアロン形態を採用することによって派生するデメリットを考慮する必要がある。

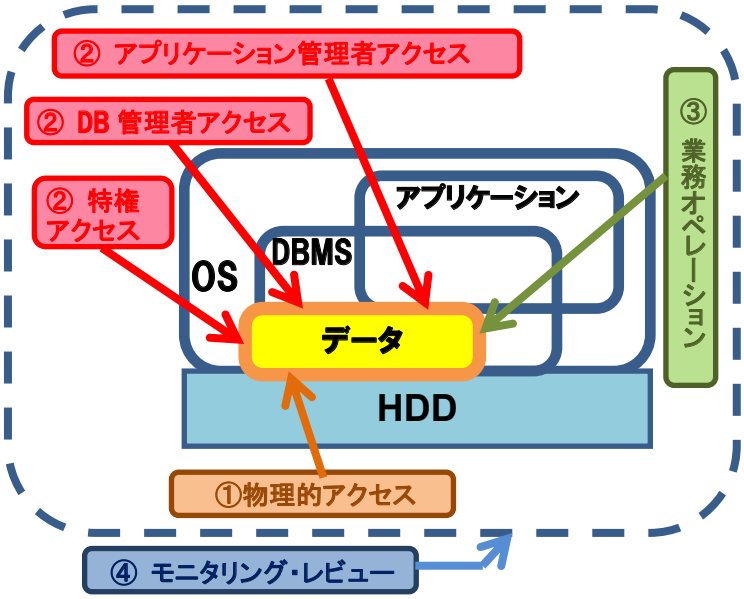

図１　対処すべきアクセスと監視

(4) 選定した管理策を実業務のプロセスの中に組み込み、確実に実施する

業務手順の中に情報セキュリティのための管理策を組み込む。具体的には、日・週・月・半期等に行われる活動を、業務スケジュールの中に組み込む。また PDCA サイクルを回す中に組み込む。

(5) 日常業務の中で、管理策の有効性を点検する。

通常の業務の中で、特権使用記録、オペレーション日誌、作業報告、業務日誌等を監視し、点検し、レビューし、そして保存する。

4. おわりに

本研究では、情報セキュリティ規格の改訂の狙いとその背景にある意図を考察した。それを踏まえて、経営資源に限りのある中小組織に対して有効に活用できるポイントを明らかにし、具体的に適用する考え方と方法を提示した。

中小組織と一口に言っても、多くの業種に散在し、また規模も多様である。取り扱う情報と情報資産も組織によって異なる。その意味で、中小組織の情報セキュリティ確保のためには、業種及び取り扱う情報の特性に応じた個別の対応が求められる。本研究では主に、個人情報を取り扱う業種に特定して考察したが、その他の業種あるいは情報を取り扱う組織に対しても同様に、役に立つガイドラインが求められる。これらの作成は、今後の課題である。

本研究は、情報セキュリティ専門監査人部会と情報セキュリティ研究プロジェクトの合同研究会で進めてきた研究の成果である。合同研究会のメンバーには深く感謝する。

参考文献

1) JIS Q 27001:2014 情報セキュリティマネジメントシステム－要求事項（ISO/IEC 27001:2013 Information security management systems-Requirements）
2) JIS Q 27002：2014 情報セキュリティ管理策の実践のための規範（ISO/IEC 27002:2013 Code of practice for information security controls）
3) JISQ31000:2010 リスクマネジメント－原則及び指針（ISO 31000:2009, Risk management － Principles and guidelines）