地方公共団体と情報セキュリティ

～　ISMS への第 1 歩　～

情報セキュリティマネジメント

システム（ISMS）

2016 年 3 月 8 日

JIPDEC

一般財団法人日本情報経済社会推進協会

～ はじめに ～

不正アクセス、情報漏えい、情報システムの障害など、情報セキュリティ問題はコンピュータを利用するすべての組織にとって無視できない重要問題となってきました。企業の場合でいえば、業種や規模の大小によらずすべての企業において、情報セキュリティ対策に真剣に取り組まなければならない時代となってきたわけですが、このことは行政機関とて例外ではありません。

組織としてレベルの高い情報セキュリティ対策に取り組もうとする場合、情報セキュリティマネジメントシステム（以下「ISMS」）の構築を考えることは極めて自然な選択です。ISMS とは、情報セキュリティに関する様々なリスクに対応するため、ISO/IEC 27001※1 という国際規格に基づき、個別の技術対策を始めとして、組織の総合的なマネジメントの形で情報セキュリティ対策を効率的、効果的に行うための仕組みです。現在、世界各国でISMS適合性評価制度が構築されていますが、その中でも、日本の取り組みは進んでおり、認証取得組織数が4,700を超えるまでになっています。また、世界的にみても、日本は ISMS 認証組織数が世界で最も多く、ISMS がわが国に幅広く浸透していることを象徴しています。

しかしながら行政機関に限ってみると、2015 年 12 月末現在、わが国では 6 の組織が ISMS 認証を取得しているにすぎません。世界的に見ると、オーストラリアには多数の行政機関がISMSに取り組んでいる州があり、台湾では総取得組織数約 400 のうち約 1/4 の 100 前後が行政機関及び公的セクターであるというように、行政機関の ISMS 取得の例は数多く見られます。4,700 を超える認証数に対してたった 6 というアンバランスは極めて特異な現象といえます。行政機関には企業とは違う特有の問題があって、それが ISMS への取り組みの障害になっているという声を耳にすることがあります。では、特有の問題があるとして、それは克服困難なものなのでしょうか。実は特有の問題と考えられているものも、その多くは工夫次第でさしたる障害にはならない場合がほとんどのようです。もし、漠然とした抵抗感のた

めに行政機関における ISMS への取り組みが阻害されているとすれば、残念なことです。

ISMS は、認証取得を前提とせずとも、その構築に取り組むことで組織の情報セキュリティの向上に大きな効果をもたらします。認証を得ている約 4700 件のほかに、認証は取得していないが ISMS には取り組んでいる組織が相当数に上ると見られています。とりあえず取り組んでみようかという場合に役に立つドキュメントも多数発行されています。しかしながら ISMS に関する一般に入手可能な様々な解説書などは、主として一般的な企業を想定して記述されており、行政機関にとっては、取っ付きにくい面があることは否めません。行政機関向けに親切に解説されている手引きのようなものはこれまで存在しませんでした。

そこで本書では、より多くの行政機関に ISMS に取り組んでもらいたいという期待を込めて、ISMS に取り組む際に直面するかもしれない行政機関特有な問題を洗い出し、一般企業と行政機関の「違いらしきこと」に焦点を当てて、その溝を埋めていくためのアドバイスやノウ・ハウをわかりやすさを心がけて記載しました。また、本書の改訂にあたり、ISMS の規格改正※1 へ対応すると共に、関連基準等※2 の更新状況を確認し、参照リンクの修正、一部基準に関する記述及びそれらに関連した本文の編集を行いました。

本書が行政機関の情報セキュリティ対策関係者の皆様の日頃の疑問を解くヒントになり、これまで躊躇されていた ISMS 構築へのきっかけとなりますことを願ってやみません。

一般財団法人情報経済社会推進協会（JIPDEC）
情報マネジメント推進センター

※1 ISO/IEC 27001 は、2005 年に発行されましたが、2013 年に、その改正版である ISO/IEC 27001:2013 が発行されました。日本においては、国内規格として JIS Q 27001:2006 が発行され、2014 年に、JIS Q 27001:2014 が発行されています（JIS Q 27001 において、その内容は ISO/IEC 27001 と一致している［IDT］と示されています）。

※2 「政府機関の情報セキュリティ対策のための統一基準群」等

～ 目次 ～

1. 地方公共団体にとっての ISMS 構築とは

1.1 ISMS に取り組もうとする地方公共団体としての課題

地方公共団体は情報セキュリティ対策上、政府機関（府省庁など）と同様の問題を抱えています。まず扱う資産の観点から言えば、国民や住民に関する機微な情報を含めた多くの個人情報を保有する組織であり、外交・外部折衝などに関わる場面で典型的に見られるよう機密情報を扱うことも多く、高い水準の情報セキュリティ対策が必要な組織です。次にマネジメントの観点から見ると、情報セキュリティ対策として何らかの対策を実施しようとする際に法律や政省令、条令等の制約を受ける場面があります。例えば公務員としての守秘義務の取り扱いは、情報セキュリティ対策上微妙な問題です。情報の機密性区分なども企業のように自由に決められるわけではありません。

地方公共団体には、政府機関と共通の特殊事情があるわけですが、一般論として制約がより少ない環境にあるようです。すなわち、地方公共団体は、首長を長としてピラミッド型の指揮命令系統を有し、予算なども首長のもとに一元的管理されているなどから、政府機関よりもむしろ民間企業と似たような環境にあるともいえます。

一方で、政府機関の場合、省のトップである大臣が徹底した情報セキュリティ対策をしようとしても、予算増額や人員増強などが必要となるような対策を機動的に行うことは当該省庁だけではできないという現実があります。官の立場では、民間の監査会社を使って外部監査や認証審査をしてもらうこと自体に抵抗があると考える組織もあります。

このような特殊事情が大きなハードルであるように思える場合もありますが、ISMS は、工夫次第で乗り切る策を見出すことができるものです。政府機関の場合でもそうですが、地方公共団体の場合ならなおさらです。

以下、「特殊事情」として意識されうる主要な課題を列挙してみましょう。

◆住民の方に安心してもらう説明

地方公共団体は、住民が求める安心（信頼と信用）を与える説明責任をはたす、及び行政事務のセキュリティ品質向上・効率化を確保する必要があります。ISMSの認証の仕組み[適合性評価制度]を利用するのも一つの方法です。

◆重要インフラ指針

地方公共団体は、住民の個人情報や企業の経営情報等の重要情報を多数保有し、他に代替することができない行政サービスを提供しています。また、業務の多くが情報システムやネットワークに依存しており、このことから、住民生活や地域の社会経済活動の保護のため、情報セキュリティ対策を講じてその保有する情報を守り業務を継続することが必要となっています。

このため、地方公共団体は、国が定める重要インフラのうち、「政府・行政サービス（地方公共団体を含む）」として位置づけられており、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（ 平成 27 年5月 25 日、サイバーセキュリティ戦略本部決定。以下、「重要インフラ指針」という。）に基づき、情報セキュリティ水準の向上及び情報セキュリティ対策の浸透を推進することが求められています。

◆組織の内部名称と人の役割名称

一般的な企業で使われている用語と違うものがあります。例えば「経営陣」という用語ですが、これが地方公共団体では何に該当するかということを特定する必要があります。

◆予算制度の制約、人事管理の制約等

会計年度ごとの予算制度の硬直性、機動的な執行ができない、重要だからといって機動的に予算を増やせない。予算費目の立て方によって機動的な運用が制約されるなどの問題があります。

◆情報公開

情報公開制度の存在によって、地方公共団体の情報セキュリティ対策には企業には必要ない工夫が必要となることがあります。

これらの他にもまだ若干課題があります。例えば、地方公務員には罰則を伴う守秘義務が存在するので、情報漏えい対策に関して守秘義務の効果に依存した規

定があることで事足れりという対応が一部には見られました。しかし、それらを加えても「せいぜい片手から両手で数えられるくらいの違い」を乗り越えるノウ・ハウがわかればいいんだな」と思っていただければ本書の目的を達したことになります。

1.2 地方公共団体に向けて用意されている情報セキュリティ対策環境

総務省では、地方公共団体における情報セキュリティ対策の推進のため、ガイドライン等の整備、情報セキュリティ監査の推進、地方公共団体間の情報共有促進等の取り組みを行っています。その始まりは、2001 年 3 月に遡り、地方公共団体が情報セキュリティポリシーを策定する際の参考となるよう、「地方公共団体における情報セキュリティポリシーに関するガイドライン」(以下、「地方公共団体向けガイドライン」と言う。)が策定・公表されました。その後何回かの改定を経て、2015 年に直近の改定が行われ、2015 年 3 月版が公表されています。この改定は、新たな対策技術の動向、政府の情報セキュリティ政策の改定及び新たに成立した法令等を受けて見直しを行った結果を反映したものと思われます。

地方公共団体における情報セキュリティポリシーに関するガイドライン(2015 年 3 月改定)
http://www.soumu.go.jp/main_content/000348656.pdf

地方公共団体の場合、この地方公共団体向けガイドラインを参考にしながら、自らの情報セキュリティポリシーを策定するのが一般的です。

地方公共団体向けガイドラインを雛形として情報セキュリティポリシーを策定し、それを基に情報セキュリティマネジメントの体制を整え運用しようとする場合、ISMS の認証を取ることは可能なのでしょうか。認証を取得するとは、構築された情報セキュリティマネジメントシステムが第三者である認証機関によって JIS Q 27001 に定められた要件に適合していることが確認されること(コラム:ISMS 適合性評価制度の運用と審査、参照)です。その証として認証書(あるいは登録証)が、与えられます。

この場合、ISO/IEC 27001、27002 をベースに運用している一般的な企業とは見かけの異なる情報セキュリティポリシーによる運用となるわけですが、答えは「可能」です。

コラム：ISMS と管理策

情報の保護を目的とするマネジメントの仕組みを、情報セキュリティマネジメントシステム（ISMS）といいます。その仕組みを成立させるための必須と考えられるマネジメントの要素とその組み合わせ及び相互の関係を国際的合意のとれた要求仕様にまとめた規格が ISO/IEC 27001（JIS Q 27001 は、これを日本の国内規格としたもの）です。

27001 で示される ISMS は、情報セキュリティに関するリスクマネジメントを中核とするマネジメントプロセスと、リスク評価によって特定されたリスクに対して手を打つ対策（管理策とよびます）の集まりの組み合わせで、組織のマネジメントを行う仕組みとなっています。

27001 では、規格の文書の附属書 A に管理策のメニューが示されていて、組織はリスク対応の必要に応じて管理策を決定し、決定した管理策を附属書 A に示す管理策と比較し、必要な管理策が見落とされていないかを検証することができます。それらの管理策は、組織のシステムの要求事項としてマネジメントのプロセスに組み込み、それらを ISMS として構築することになります。また管理策は、リスク対応の正当な理由を示すことができれば、附属書 A 以外から採用することも可能です。

管理策の必須となる要件が 27001 の附属書 A に記載され、管理策の具体的な実践の代表的事例に関する記載が 27002 に実施の指針として示されています。管理策に付された章節に該当する番号で、27001 の附属書 A の管理策と 27002 の管理策の記述との対応関係を示しています。また、附属書 A に示された要件（管理目的）が守られていれば、27002 の実施の指針以外の実践（実装）による構築も可能で、審査上も適合しているものとみなされます。

ISMS では、JIS Q 27001 の附属書 A に示された管理策についてすべて吟味して、採用、不採用（理由が必要）の判断をすることが求められています。地方公共団体向けガイドラインを雛形とした場合、まずこの点をどうしたらよいかが疑問になります。その作業はどこでやられているのでしょうか。実は地方公共団体向けガイドラインを丁寧になぞって実行している場合は、結果的に JIS Q 27001 の附属書 A に示された管理策のほとんどについて対応して実施・運用がなされているのと同様の状態になっている場合が多いのです。この点については、コラム「ISMS 適合性評価制度の運用と審査」も参考にしてください。

事例:自治体の素顔－東京都 総務局情報通信企画部

ISMS 認証取得に取り組んだ背景

東京都総務局情報通信企画部(旧組織名称:総務局情報システム部)では、2006 年度に実施されたシステム監査において、「IT に関連した機密文書が多数あると推定され、他の部門より情報漏えいのリスクは大きいと考えられる」という指摘を受けたことや、全庁的に記録媒体の紛失等セキュリティ事故が顕在化したこと等により、情報セキュリティ対策の強化が課題となっていました。

また、東京都では、2007 年度に、情報セキュリティポリシー(東京都情報セキュリティ基本方針及び東京都情報セキュリティ対策基準)を改定し、情報セキュリティの強化を進めていたところであり、総務局情報通信企画部としても、都庁の基幹的なシステム・ネットワークを運用する都庁 IT の中枢部門として、高いセキュリティ体制が必要と考えていました。

そこで次の事由を考慮し、他部署に先駆けて ISMS 認証取得に取り組み、情報セキュリティレベル維持向上の体系的な仕組みを確立するとともに、他のシステム保有部門への普及のための先導的役割も果たすことにしました。

・より高いセキュリティ体制を実現するには、ISMS(情報セキュリティマネジメントシステム)を導入し、情報セキュリティを PDCA スパイラルで向上させることが有用である。

・第三者の評価による ISMS 認証により、情報漏えい等に対する都民の不安解消に寄与し都庁情報システムに対する信頼性向上に資する。

認証取得のポイント

東京都総務局情報通信企画部では、2007 年度に、基盤システム等を対象として、ISMS の要求事項でもある業務継続計画を策定し、また、ISMS 先行取得自治体等の調査を経て、ISMS 導入についての意思決定がされ、2009 年 7 月より ISMS の構築をスタートさせました。

適用範囲は、総務局情報通信企画部が所管する、全庁 5 万が利用するグループウエア、都庁と 600 ケ所の事業所を結ぶデータ通信ネットワーク、職員認証基盤

システムなど、8 つの基盤システムの運用管理及び保守業務としました。

ISMS 管理体制として、情報通信企画部長を「ISMS 最高責任者」とし、ISMS 管理責任者、管理職、係長により構成される情報通信企画部 ISMS 委員会を設置しました。

ISMS 導入を機に、あらためて ISMS の要求事項に沿った運用の実施を試みたわけですが、ISMS 規格の解釈や運用等の手順の文書化に苦労したため、先行取得自治体や外部の専門家の支援を部分的に受けたそうです。

2009 年 12 月末までには、ISMS 基本方針、ISMS 運用管理基準、リスクアセスメント手順書等を含む所要規定類の整備を含め、準備が整ったので、認証機関に審査を申請し、2010 年 1 月末に第一次審査を、3 月初旬に第二次審査を受け、3 月 30 日付けをもって ISMS 適合性評価制度における認証を取得しました。

ISMS の認証取得に当たっては、都の情報セキュリティポリシー等に基づき、教育やセキュリティ監査を実施するなど、認証取得前から一定レベルの対応が図られていたことの寄与が大きいと感じられているようです。また、リスクアセスメント時に用いる情報区分は、業務内容と照らし合わせ、理解されやすいように定義づけることや、セキュリティ監査者向けの研修を受講した他部署の情報化推進担当の管理職の方々に内部監査を実施していただくことなど、運用方法を工夫することをポイントとして挙げられていました。

認証取得してよかったこと

認証取得以前から、セキュリティポリシーに基づき、各種システムの運用などを手掛けており、技術的な側面におけるセキュリティ対策はある程度実施されていました。しかし、クリアデスクなどは職員のセキュリティ意識はあってもなかなか実行が伴わない等、実現が困難でした。

それが、ISMS の認証取得という、明確な共有の目標を立てることで、職員の意識が向上したことは、大きなメリットと感じられています。また、従来、見落としていた部分や仕組みとして確立されなかったものが明確になった点や、部全体としてセキュリティに取り組む体制が確立されたことが良かった点であるとされています。情報セキュリティの活動は、関係者に対し、その重要性を認識させ、役割と責任を担っ

ていただくことは、その活動を推進する上で非常に重要な点であると思います。また、情報セキュリティ意識が高まれば、地道な記録の取得などの対策も、その目的が明確になり、形骸化されることなく継続的に実施することが可能になります。

今後の課題

今後の課題としては、ISMS に関する事務処理が煩雑なので、文書、記録等の簡略化を図り、より ISMS を取り組みやすい活動にしていくことがあげられています。

また、システムにおけるスパムメール対策、標的型攻撃に対する訓練などを実施しましたが、今後、増加するであろうこれらの脅威への対応、また、ISMS の認証基準や規格の変更への対応等も課題とのことです。

さらに、自治体におけるクラウドの利用や庁外からのリモートアクセスに関するセキュリティ問題等、新たなリスクへの対応も、課題であるとのことです。

おわりに

これから ISMS の認証取得を目指している自治体の皆様に、次のようにエールを送って頂きました。

「セキュリティの重要性がますます叫ばれる昨今、ISMS を取得し、継続性のあるセキュリティ体制を築くことは非常に有意義なことです。

また、国際規格である ISMS を導入することで、現状のセキュリティ対策を客観的、網羅的に見直す機会となります。

定期的な委員会の開催や事務処理等大変なこともありますが、PDCA をまわしていくことにより、日々セキュリティレベルの向上を実感できるので、積極的にご検討いただきたいと思います。」

（2012 年 9 月 7 日のインタビューに基づき記載）

事例：自治体の素顔－三鷹市

ISMS 認証取得に取り組んだ背景

三鷹市では，1984 年に NTT の INS 実証実験を行うなど，ICT に早くから係わる機会があったことから、行政の電子化は市政の中心として積極的に取り組んでいました。行政の電子化，電子自治体の推進にあたっては、情報セキュリティの確保は重要な前提条件となることが、市長をはじめ多くの職員の共通理解となっています。そのため、情報セキュリティの取り組み状況を第三者の視点で確認する ISMS 認証の取得は、市民の皆さんから信頼を得る上でも重要であると認識されていました。ISMS 認証を取得する場合には、単にセキュリティ対策の導入・整備だけでなく、ISMS の運用に重きを置かなければなりません。三鷹市では、第三者による評価は公正さ、適正さを確保し、ISMS 活動の形骸化を防止する上でも役立つと考えています。

認証取得のポイント

三鷹市では、2002 年度に ISMS 導入についての意思決定がなされ、2003 年 4 月より ISMS の構築を行っています。ISMS の認証取得範囲は，全庁約 50 課のうち市民部を中心にした市民課、市民税課、資産税課、納税課、保険課などの 11 課となっています。当時は庁内に ISMS に関するノウ・ハウが無かったため、導入については外部の専門家の支援を仰ぐことにしたそうです。マネジメントシステムの構築や庁内教育体制の構築が主な支援となりました。10 月から ISMS の運用を開始し、2004 年 1 月から認証機関の審査を受けることができました。

ISMS の認証取得のためには、文書類の作成や運用状況の記録の保持などが重要となりますが、煩雑にならないように工夫をしたそうです。このことは、ISMS の維持継続のためには重要なポイントだと思います。また、ISMS の活動が形骸化しないようにするために、認証を取得した各課に ISMS 推進メンバーを配置し、日々の活動の中で情報セキュリティの重要性を伝えられるようにしているとのことです。ISMS 推進メンバーは、いずれ ISMS の認証取得対象ではない課に異動することになりますが、その際には情報セキュリティの重要性を現場の皆さんに伝えるなど、ISMS 認証対象外の組織への啓発活動にも貢献し、三鷹市庁全体のセキュリティ

レベルの向上に貢献しているとのことです。

なお、ISMS の認証取得範囲外であっても情報セキュリティが重要であることには変わりがありません。認証取得範囲外の課についても 3 年に 1 度の割合で情報セキュリティ点検を実施しているそうです。また、「情報セキュリティハンドブック」を職員全員に配布し、情報セキュリティの重要性を周知するとともに、適切な対策の実施につながるように工夫しているというのは、他の自治体でも参考になると思います。

これらの活動すべてに市長の強いコミットメントがあることが、三鷹市の特徴で、これが成功要因の一つだと思います。

認証取得してよかったこと

ISMS の認証は第三者評価に基づく認証という点で公正性が担保されています。そのため、より信頼性の高い形で市民に情報セキュリティの取り組みを周知できます。このことは、電子自治体を推進する上で非常に重要な点であると思います。市民の信頼がなければ電子自治体の施策は進みません。情報セキュリティが担保されていることは市民の信頼を得る上でも重要です。

また、全庁ではなく一部の部署が ISMS の認証取得をする場合であっても意味があります。ISMS の認証取得をした部署の効果を全庁に広げることは可能です。三鷹市の場合でも、全庁の情報セキュリティ意識が高まり、対策が形骸化されることなく実施されています。そのため、一部の課で ISMS の認証を取得することも意味があります。

今後の課題

三鷹市の場合は，スマートフォンやクラウドコンピューティングの利用といった新しい ICT の活用に伴うリスク対応をどのようにするかが課題の一つとのことです。有効なセキュリティ対策の実施にめどが立たないと、新しい ICT を活用することはできません。特に、今回の大震災を受けて感じたことは、職員が庁舎に出勤できなくても外部からシステムにアクセスをして業務が継続できるようになる必要もあるのではないかということも課題の一つとなっています。

職員に対する情報セキュリティに係る教育は、多くの組織で重要な課題であり、

三鷹市の場合も同じようです。毎年新しい職員が入庁します。一度教育を受けていたとしても新しい脅威が発生したり、本人の意識が低まったりし、その対応が不十分であれば情報セキュリティ事故につながりかねません。継続的な教育の実施が重要です。効果的に継続して教育をしていけるようにすることが課題とのことです。

また、認証取得範囲外の課の情報セキュリティの向上も、今後の課題の一つとのことです。

おわりに

三鷹市のISMSを担当する部長から、「認証取得をすることで，職員の意識改革が進んだことを実感しています。大きな効果がありますので、積極的に取り組んで頂きたいと思います。」とこれから ISMS の認証取得を目指している自治体の皆様にエールを送って頂きました。

（2012 年 10 月 12 日のインタビューに基づき記載）

2. 地方公共団体の課題とつき合うためのノウ・ハウ

この章ではISMSに取り組もうとする地方公共団体のためにいくつかのノウ・ハウを紹介します。地方公共団体には民間企業とは異なる特有の課題があるのは事実ですが、情報セキュリティ対策を考えた場合、たいていは、同様の問題が企業にもあり、問題となる程度の差又は観点の違いで、共通あるいは類似の対策で対処可能なことが多いようです。

2.1 組織マネジメントのポイント

組織マネジメントの面で地方公共団体の特徴を考えてみます。すべての地方公共団体に当てはまるわけではありませんが、以下のような特徴がある場合があるようです。

- 人事異動で2～3年程度の短い期間で担当者が変わり、情報システムの専門家が育ちにくい。特に情報セキュリティの専門家はほとんどいない。
- 情報セキュリティのための役割を担う担当責任者等を設定しようとした場合、規定整備に手間がかかってなかなか前に進まない。
- 通常の各種業務の担当者に情報セキュリティ対策上の義務を負わせようとする場合、文書による指示などがないと動かない。
- 学校、病院、上下水道その他の事業部門等に対して、指揮命令が及びにくい。

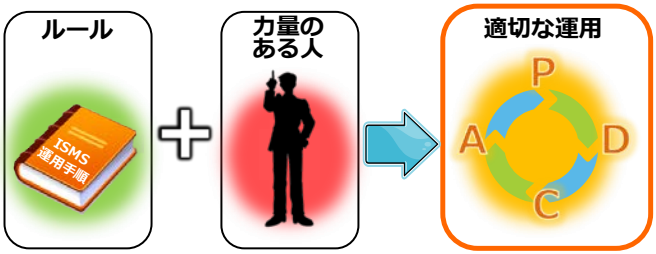
この他にも特徴があるかもしれませんが、上記については、民間企業においても程度の違いはありますが同様の問題を抱えており、それらに対する対応策に腐心しつつ取り組んでいます。

一般論として言えば、組織マネジメントについては、首長の下に指揮命令系統がはっきりしている地方公共団体は、政府機関に比べて民間企業との違いが少ないと言うことができるように考えます。つまり、組織マネジメントの観点では民間企業と類似のアプローチでものごとを判断していって、ほぼ枠組みを作りうると思われます。

一方、組織の中で使われているいろいろな名称が、官民で異なる点が苦労の源になることがあります。例えば ISMS に関する解説などには、「経営陣」という語が頻繁に登場します（規格ではトップマネジメントと呼ぶ）。「経営陣が受容可能なリスクの水準を決定」などという文脈が出てくるわけですが、政府機関の場合はこの経営陣（トップマネジメント）に該当する役割をだれに当てはめるか、どのように運用するかは現在のところかなりの難問です。しかしながらより民間に近いマネジメントを有する地方公共団体の場合は、この「経営陣」というのは、首長を含めた幹部に該当するとすることで、ほぼ問題なく読み替えられるでしょう。

コラム:マネジメントシステムと教育・訓練

JIS Q 27001 の「7. 支援」の項には、「7.2　力量、7.3　認識」があり、教育・訓練の重要性が強調されています。いくら立派な ISMS の手順を整備してもそれを実施する力量(意図した結果を達成するために、知識及び技能を適用する能力)が備わった人がいなければ、その ISMS は絵に描いた餅になってしまします。したがって、ISMS を適切に運用するためには手順のみならず、ISMS に定義された責任を割り当てた要員すべてが、要求された職務を実施する力量をもつことを確実にしなければなりません。

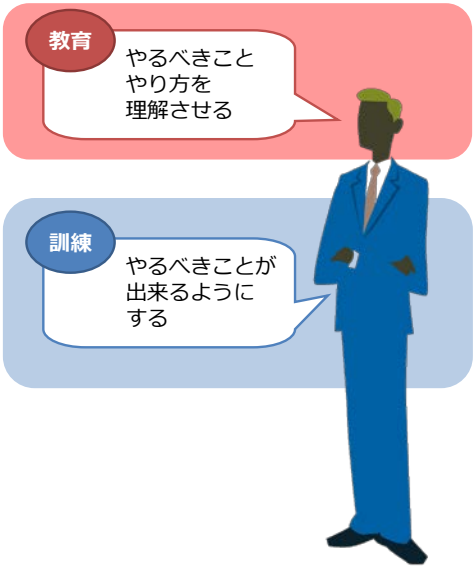


地方公共団体の場合は、組織全体の人事の仕組みとして 2～3 年毎に部署異動があるため、必要とされる力量の維持については非常に重要にも係わらず、その実施が困難な場合も多いようです。

地方公共団体の職員一般として求められる情報セキュリティに関する力量(例えば、住民のセンシティブな情報について外部とネットワークを使って通信する場合には、セキュリティ上の対策をする、というようなこと)は部署異動をしても職員一般としての経験を積んでいけば比較的容易に力量を獲得し、維持していくことができます。

一方、業務特有のセキュリティに関連する力量(例えば, ファイアウォールの設定に関すること)については新たに習得する必要があります。専門性が非常に高いことは専門業者に業務委託をすることになると思いますが、その場合でも少なくとも

業務委託先の作業を監督するだけの力量（例えば、事業者が実施したファイアウォールの設定の妥当性について事業者から説明をうけて判断する力量）は必要となってきますので、その程度の情報セキュリティに関連する専門性を力量として備えていなければなりません。業務委託先の社員が情報セキュリティの事故を起こしている場合も多いと思いますが、その事故の理由の多くは委託元が業務委託先を適切に管理、監督できていないことによるものだと思われます。業務委託先を管理、監督できる程度の情報セキュリティに関する力量をもった職員を地方公共団体に維持するためには、情報セキュリティに関してある程度の専門性を持たせておくべき人を複数選んでおき、人事異動の際にも配属する部署に考慮する（例えば、情報システムの運用部署での経験を2年経て、他部署に異動したとしても、異動先で情報セキュリティの担当者に任命したり、その後の異動で再び情報システムに関連する部署へ異動させたりする）などの工夫が必要となってくるでしょう。ISMS の認証を一部の部門で取得しているだけでも、適切な力量を組織として維持しなければならないことの重要性が認識され、人事異動や責務の与え方に工夫を加えることで、組織全体としての情報セキュリティ対策の有効性は向上します。



さて，必要な力量を得るために重要となるのが、教育・訓練です。教育とは，簡単にいえば頭で理解できるようにすることです。例えば、秘密情報を外部の方に電子メールで送信する場合は、文書にパスワードをつけて送るといった運用手順がなぜ必要でどのようにすればできるかを理解できるようにすることが教育となります。

一方、訓練とは、簡単に言えば体が動くということです。例えば、秘密情報を外部の方に電子メールで送信する場合に、適切なソフトウェアを使って適切なパスワードをつけて送信することができるようにすることが訓練となります。もちろん、日常的で簡単な作業はある程度頭で理解しておけば、ほぼ実施できる場合もあります。しかし、危機対応といった通常はあまり起こらないが起こった場合には非常に重要な手順というのは、その実施が確実にできるように訓練をすることが重要です。例えば、ウイルスに感染した場合に情報システム部門の担当者がとるべき対応は、頻繁には起こらないため確実に実施できるように教育をうけて頭で覚えるだけでなく、体が動くように訓練しておく必要があります。

部門異動が多い、地方公共団体の場合には、教育・訓練、なかでも訓練が非常に重要となってきます。

2.2 情報セキュリティと情報セキュリティリスク

情報セキュリティ

情報セキュリティとは、組織にとって価値ある情報を次の特性の喪失から保護することをいいます。

・機密性（Confidentiality）－ 不正な開示またはアクセスから情報を保護する。

（規格の定義※：認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性）

例：個人のクレジットカード情報、財務情報または住民のカード情報で、その所有者が機密保持を期待しているものを、不正な開示またはアクセスから保護すること、または機密の設計仕様、調査研究の結果、市場予測及び分析を、不正な開示から保護すること。

・完全性（Integrity）－ 不正な変更または損壊（偶発的なものを含め）から情報を保護し、情報の正確さ及び真正性を維持する。

（規格の定義※：正確さ及び完全さの特性）

例：個人の医療記録、個人情報、住民情報または組織の事務・会計の記録、行政事務、給与、請求書及び／または在庫管理プロセスなど業務システムの有効かつ効率的な運営に不可欠な情報は、正確でなければなりません。

・可用性（Availability）－ 情報への正当なアクセス権を持つ者に対して不当なアクセス拒否が行われないよう情報を保護する。

（規格の定義※：認可されたエンティティが要求したときに、アクセス及び使用が可能である特性）

例：組織の IT システムのデータベースサーバがサービス妨害（DoS）攻撃（コンピュータウィルスによるものなど）を受けると、そのデータベースにある情報は利用できなくなり、重大なシステム障害を招くことがあります。

またノートパソコン、スマートフォンなどのモバイル端末機器が盗まれると、その所有者はその機器に記録されていた情報にアクセスできなくなります。可用性及び

サービス妨害にかかわる問題により、組織の業務が長期的に妨げられることもあります。定期的にバックアップされている情報があれば回復は可能です。

※「JIS Q 27000:2014 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」より

情報セキュリティリスク

インターネットや携帯電話のオープンな通信の普及にともなって、世界中の組織において、情報セキュリティへの関心が高まっています。過去 20 年間、多くの組織が、情報セキュリティが不十分であったためリスクにさらされてきました。

組織の活動・事業を行う手段として、また莫大な量の情報にアクセスする手段としてインターネットの利用が拡大するにつれ、こうしたリスクにさらされる可能性が劇的に増大しています。スマートフォンなどの携帯電話などモバイル・テクノロジーを用いたより広い範囲に対する接続及び業務アクセスに対する需要も急増しています。

情報の喪失、損傷、盗難、利用できなくなることが起こると、組織及びユーザの信頼感が損なわれます。インターネットを通じての情報漏洩、または組織情報及び個人の情報を保存したノートパソコンなどの携帯機器の盗難、IT システムの損傷、その他ぜい弱性のあるデータ源からの漏洩を通じて、個人・住民のデータの盗難が起こる可能性があります。IT システムへの依存度が高まるにつれて、事業及び社会は多くのリスクに直面します。したがって、組織はこうしたリスクを認識し、組織の活動・事業及びユーザの保護のための管理されたアプローチを採用することが求められます。

業務プロセス及びサービスの外部委託も前例のない増加がみられ、一方サプライチェーンはその規模を拡大し続けています。多くの組織がサプライチェーン及び外部委託業務に関与していますし、またその情報セキュリティリスクを看過することはできません。入札、契約、サービス品質保証契約に関しては、多くの場合、供給者が適切な情報セキュリティの対策を講じていることが要求されます。こうした状況の中、関連するリスクを管理する際の情報セキュリティの重要性が一層重視されています。

さらに、最近の法令や規制の多くには、行政の組織を含めて各組織が遵守しな

ければならない情報セキュリティの要求事項が定められています。

各々の組織（供給者を含め）が、情報セキュリティの観点から、以上のような様々なリスクに対応することが必要です。

コラム：最近のトピックス ～標的型攻撃への対応～

標的型攻撃が増えているというが、自分（の部署）は大丈夫という過信が被害を大きくしてしまいます。例えば、上部組織や監督官庁からのメッセージを受信することがある場合に、組織の変更や人事異動が重なると、読まざるを得ないとの意識で警戒心もゆるみ、もっともらしい添付ファイルを開いてしまうことはないでしょうか。

標的型メール攻撃は、マルウェア（悪意のある不正プログラム）を埋め込んだ文書ファイルが添付されたメールが、侵入のきっかけとなる場合が多いのです。添付ファイルを開くと、攻撃者が準備している別の場所のサーバに自動的に接続されてしまいます。庁内のネットワークから攻撃者が目的とする情報を勝手に盗み出して転送します。ある組織のパソコンがすでにマルウェアに感染して、メールの本文や添付ファイルを盗み出し、それが悪用され攻撃に使用される場合が多いようです。本物のメール本文や発信者情報が利用されているので、受け取った側では当然のように勘違いすることを狙った攻撃です。

実在する組織名、人物を名乗って、本物の文面で送られてくるメールを、それに関係する組織が受信してしまえば、添付ファイルを開く確率は高いことを狙っています。あなたの組織は、この攻撃に耐えることができるでしょうか。

遠隔操作される手口も利用される場合もあります。マルウェアへのリンクを埋め込んでおき、それをクリックすることで感染させるタイプも多いのです。実は、すでに感染してトロイの木馬型ウイルスを埋め込まれた状態で平静を装う潜伏期かもしれません。未知のタイプのウイルスをチェックするのは容易でないのです。

・この攻撃はどこから発信、中継、転送されているのでしょうか？
・攻撃はどのように行われているのでしょうか？
・接続されたサイトはどのような状態だったのでしょうか？

全方向型、全天候型で、普段からのトレーニングを通して、組織員全員の対応力を高める必要があります。たった一人のミスをなくすための手法は地道です。

2.3 予算制約と折り合うために

情報セキュリティリスクのすべてに対応することが理想ですが、一方で、地方公共団体においては、年度予算の原則、予算の使用について裁量の余地が狭いなど、民間企業と比較して多少の違いはあります。しかし、予算が常に足りないという基本的な問題は官民を通じたより上位の問題です。それに比べれば、違いの部分は、事前の工夫により、民間並みの問題レベルに十分緩和可能です。

ここでは、ISMS 実施にあたって直面する予算制約に起因し、官民の違いが意識される場面で緩和可能な課題のうち、将来悩みをかかえないために知っておく価値があるキーワードを紹介します。

各種の対策を予め選択し実施しようとする場合、予算の制約によって最善の対策が選べず、次善の策を選ぶか、または対策自体を断念せざるを得ない場合があります。断念する場合、企業においては、これを「リスクの受容」という考え方で処理することがあります。これは、費用対効果などの論理により、どのレベルのリスクなら受容できるかという基準を定めておき、その管理策を採用しないことによるリスクを、組織決定として覚悟してしまうことを意味します。しかしながら、行政機関の場合、この「リスクの受容」という名称も考え方も受け入れにくいという例が見られます。費用対効果を理由にリスクを受容するというような民間的価値判断をしにくい行政機関の場合は、可能なら「リスクを受容したわけではない」という前提で問題に対処したいところでしょう。

この問題に対して、リスクの受容という論理を使う代わりに、「例外措置」という考え方があります。すなわち、予算がなくて対策が打てないなら、それは本来あってはならないことであるが、この際やむなく例外的扱いとし、そのように措置したことをドキュメントとして明確化して、できれば次の期の予算では優先的に配慮すべく、忘れないように慎重に管理しよう、という発想です。対策できないことから目をそらし、そもそもリスクがなかったかのように開き直ったり、お茶を濁すのではなく、真摯にリスクに向き合って忘れないようにしようという態度は、この場合考えられる次善の策たりうるでしょう。

さて、リスクの受容、或いは例外措置という手段を使いながら、できていないことから目をそらさないようにする態度で ISMS を構築していくと、結果として予算担当

部局や議会との関係が打開できることがあります。この点については次節に述べます。

2.4 議会との関係

議会の存在は、地方公共団体の情報セキュリティ対策を考える際の特殊要因の一つです。とはいえ情報セキュリティ対策との関係での議会要因は、対策の拡充のために予算の増額が必要になった際、いかに議会の理解を得るかという場面に限定されると考えてよいでしょう。そのような観点で考えてみましょう。

この問題は、基本的にはそれぞれの地方公共団体ごとに工夫して対処すべき問題ですが、構造的には次のようなものではないでしょうか。

まず、情報セキュリティ対策のための予算増額という話題は専門的すぎて議会にかけづらい・・なぜかといえば、なぜその対策を行う必要があるのかなどという質問に行政側が適切に応答することが難しいため・・それゆえ議会の前に予算担当部局が立ちはだかって、議会で説明できないという理由で首を縦に振らない。

一般論として言えば、前述のような構図にはまってしまうのは、体系的でない情報セキュリティ対策では予算増の必要性を説得することが難しいからです。ISMS構築に取り組んで、各種管理策の必要性を吟味し、予算との関係でできないことをあぶりだし、どういうリスクに対して何をやる必要があるか、逆にこのままでは何を行うことができないため現在どういうリスクを負っているのかが体系的に説明できれば、正攻法で議会に説明する道も開け、議会での議論を通じて、住民の理解を得ることにもつながります。正攻法で議会と対面するなら、「リスクの受容」という論理も受け入れられる可能性があります。

なお、ISMS の実行のためにも、議会における説明のためにも、大局的な状況把握と戦略策定・説明責任を担える最高情報セキュリティ責任者（CISO:Chief Information Security Officer）を置くことができれば、かなり心強いでしょう。

2.5 情報公開

地方公共団体特有の問題があっても、たいていの場合民間企業にも同種の問題があって、程度の差、解釈・見方の問題として対応可能であるという例をあげてきましたが、情報公開制度だけは民間企業にはない行政機関特有の問題であると言えるかもしれません。

今日、ほぼ全ての地方公共団体において、条例に基づく情報公開制度が制定されていますが、同制度のもとで、機密情報の公開を迫られる場合があるとすると、これは民間にはないタイプのリスクとも考えられます。

しかしあまり杓子定規にこれをリスクとして取り上げるのも行き過ぎかも知れません。仮に情報を提供することになるとしても、管理された状況の下で行われる行為であり、不正アクセスによって管理の及ばない意図せざる形で情報が外部に出ることがありうるというリスクに比べればはるかに小さいリスクで、リスク分析の際に意識するとしても明記する必要はないかもしれません。事例を考えてみましょう。

情報システム部門では、構内 LAN システムの図面を機密扱いすることが普通です。これが外部に知られると、外部からの攻撃の参考にされてしまうからです。しかしながら、この構内 LAN システムについて情報公開請求があった場合、機密であるからという理由で拒絶できると確実に予想できるでしょうか。請求情報が個人情報のように法律の裏づけがあるなら、法律を根拠に拒絶する理屈が立つでしょうが、構内 LAN が守秘すべきものというのは、システム部門周辺限りの常識で、一般社会の理解が得られる保証はないため、拒絶可能と断言することは躊躇されます。

このような場合、現実に請求があったなら、担当としては、攻撃の参考にされない程度に情報を墨塗りして出すということを落としどころと考えるかもしれません。そうできるためには守秘の根拠を制度的にきちんと整備しておくことが肝要です。管理された情報公開の際に最後の墨塗りの妥当性を主張できるかどうかにつながる、情報公開制度と共存できる守秘制度のきちんとした整備が求められます。

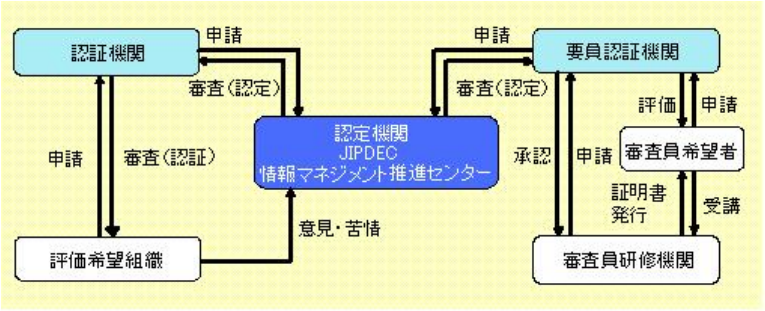
コラム：ISMS 適合性評価制度の運用と審査

ISMS 適合性評価とは、企業や自治体などの組織が構築した情報セキュリティマネジメントシステム（略称：ISMS）が JIS Q 27001（ISO/IEC 27001）に適合しているかを、認定された認証機関による審査により評価することです。

情報セキュリティマネジメントシステムとは、組織の情報を守ることを目的として、組織の方針、手段及びプロセスを管理し、継続的に改善するための組織的及び技術的な施策と運営を行う枠組みです。

JIS Q 27001 は、国際規格 ISO/IEC 27001（Information technology － Security techniques － Information security management systems － Requirements：情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）を日本語で記述し制定したもので、企業や自治体などの組織が ISMS を構築するための要求事項をまとめた規格です。また、構築された ISMS 及びその運用がこの要求事項に合っているかを確認するための認証基準として使用します。この認証基準に対する適合性の確認を、直接に事業上の利害関係がない第三者の立場で行うことを認証審査とよび、認証審査と認証取得の登録を行う組織を認証機関、認証審査を行う人を認証審査員とよびます。

ISMS 適合性評価制度は、企業や自治体などの組織が構築した ISMS が JIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、その審査を実施する審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みです。なお、審査員になるために必要な研修を実施する「審査員研修機関」は、要員認証機関が評価し承認します。



2016 年 X 月現在 ISMS の認証機関は、国内で 26 機関あります。

3. どんな組織も悩むこと

3.1 適用範囲の考え方

ISMS の認証は、一つの組織として組織自らを律する機能と管理とが存在し情報セキュリティを確実に実現運用できるものならば、部門単位でも取得することができます。このため、ISMS に取り組む組織にとって、認証範囲を組織全体（会社なら全社）でいくか、一部の部門で取得するかの選択肢があります。

組織全体で認証取得を目指すことがトップダウンで決まるなら、この問題はバイパスできますが、ISMS への取り組みがボトムアップで始まる場合、多かれ少なかれこの問題に直面します。大きな組織であれば特にそうで、いきなり全組織で取得に取り組むことは実際問題として組織内の意思決定が難しい場合も多くあります。

中堅以上の規模の地方公共団体であれば、おそらく同じ問題に直面します。そこで現実的なアプローチとしては、まず適用範囲を一部局に限り、そこの認証取得を目指し、その後徐々に範囲を拡大するという漸進作戦が考えられます。最初の部局としては、多くの情報を管理している情報システム部門がやりやすいかもしれません。

情報システム部門だけでも認証を取得することは大きな意義があります。一部局であっても、そこに ISMS の実際的知識と経験が蓄積されれば、その後適用範囲を組織全体に拡げて ISMS に取り組む際の有効なエンジンになります。情報システム部門など組織の一部で ISMS の認証を取得し、そのあと徐々に認証範囲を拡大していくという姿勢は推奨されます。

認証範囲の拡大は、リスク分析を適切に行った上で優先度を決めて、重要な情報を所持・管理している部門から組織全体へ、例えば人事・会計部局や情報の出入り口となる窓口部局など、ステップ・バイ・ステップで適用範囲を広げていくアプローチが実際的でしょう。そして、管理体系が独立している水道事業、公営交通、学校、病院などへ広げていくことができれば、理想的です。

ただし、いかなる認証範囲であっても、その中に存在する内外の課題やリスクに対応することが重要であることは言うまでもありません。

コラム：セキュリティ文化について

2002 年に OECD の情報セキュリティガイドラインが改訂され、13 年が経過しました。このガイドラインは、セキュリティ文化の発展を促進することによって、絶えず変化を続けるセキュリティの環境に対応するものです。セキュリティ文化とは、情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れることを指します。このガイドラインは、ネットワーク及びシステムの安全な設計及び利用が、インシデント発生後に後付けで導入されることが余りにも多かった時代を否定し、適切な情報セキュリティの設計、思想を初期から導入することの重要さを明示しています。また、情報ネットワークへのすべての参加者の利益、並びにシステム、ネットワーク及び関連するサービスの性質を適切に考慮したアプローチのみが、効果的なセキュリティを提供し得るとしています。さらに、すべての参加者は、自らの役割に応じて、関連するセキュリティリスクと予防手段を認識し、責任を持って、情報システム及びネットワークのセキュリティを強化するための措置をとるという考え方が重要であることを示しています。

セキュリティ文化の普及

セキュリティ文化の普及には、強いリーダーシップと広範囲に及ぶ理解者・賛同者、つまり適切な参加者が必要となります。セキュリティ文化の普及により、すべての参加者間でセキュリティの必要性が理解されるとともに、セキュリティ計画及びマネジメントが優先的に取組まれるようになります。セキュリティ文化が醸成されれば、セキュリティの課題は、政府及び企業、またすべての参加者にとっての関心事項となるだけではなく、責任を持つべき事項として認識され、情報システム及びネットワークの運用について恒久的にセキュリティを向上させることが可能となります。

行政機関におけるセキュリティ文化の育成

行政機関は、セキュリティ文化を醸成し、普及させる大事な役割を担うことは言うまでもありません。一方、行政機関においては、おおよそ 2 年ごとに人事異動があ

り、十分な引き継ぎもないまま、主要業務は前任の実務を把握するものの、構築した情報セキュリティマネジメントシステムについては、多くはそれに対する認識の欠如から形骸化させてしまうことがあります。

しかし、高度な情報セキュリティが要求される組織、とりわけエネルギー、交通、金融、通信及び情報などの社会基盤を担う重大インフラや市民及び企業にサービスを提供する行政機関にとっては、このようなことはあってはなりません。

通信事情は著しく変化し、情報にアクセスするための機器は、その種類と数の増加とともにその性質も多様化しています。以前のホストマシンやサーバなどを組織内で運用する形態から、委託業者にシステム・機器の運用を委ねるアウトソーシングやクラウドを利用する形態、並びにワイヤレス及び多様化するモバイル機器を活用するスタイルが混在し、セキュリティ管理が複雑化しています。その結果、情報の性質、量及びその取扱いに関するリスクに大きな変化が生じているにも関わらず、それらに追随した対応をすることができず、セキュリティインシデントに巻き込まれてしまうケースも少なくありません。このような事態を重大インフラや行政機関が運用するシステムで起こすわけにはいかないのは、いうまでもありません。

セキュリティ文化を醸成し、未知の脅威にも対応する

行政機関で、セキュリティ文化を醸成することで、行政に関わるすべての参加者が、セキュリティが保たれた情報システム及びネットワークの運用について考え、評価し、影響しあう、「リスクコミュニケーション」が確立されることが期待されます。このことは、増加する標的型攻撃、遠隔操作、未知のタイプのマルウェアなど「技術面」だけでは対応が難しい、「人の弱点」を巧みに突くタイプの攻撃の防御にも大いに役立ちます。そのため、行政機関は社会全体でセキュリティ文化の普及に向けた取組みが行われるための基礎を構築するための活動に対して、今以上に注目するべきであると考えます。セキュリティ文化が確立した組織では、該当する要員すべてが自らの業務を通して情報セキュリティについての活動の意義とその重要性を認識し、情報セキュリティマネジメントシステムの目的の達成に向け、どのように貢献できるかを考えることを確実なものとすることができます。

3.2 どこまで徹底するか

情報セキュリティ対策を担うことになった責任者が、ほぼ全員通過する悩みは、「何から」手をつけたらよいか、「何をどこまで」やればよいのか、という問題です。情報セキュリティとは、100%セキュアというような完璧がない世界で、またこれだけやれば合格という一般的な基準の設定も現実的に存在しない世界です。

情報セキュリティ対策のレベルを高めよう、より高い安全を実現しようとすれば、そのための費用は青天井にせまる状況が生じがちで、官民を問わず予算制約の中で対策を選択するためには、当然ながら、対策の徹底度が問われ、その組織としての現実的な最適解（組織の活動・事業としての存続の観点にもとづく）を探り経営判断を行うことが必要となる場面があります。民間の場合だと、守るべき情報の価値、事故・インシデントが生じた場合の影響度、回復費用、その他様々な問題を、金銭換算を含めて考慮し、これ以上なら採用しないというような考え方がありえますが、行政の場合、金銭換算が困難なケースが多い、という違いがあります。また市民の側から見て、行政とはミスを犯さない存在であってほしい（無謬性原則とも関連）という期待があることから、コスト面から対策はここまでとし、その結果一定のリスクがある、というような説明をするはめにはなりたくない、という事情があったりもします。

このように、行政機関は、民間と比べて、費用対効果の観点から対策を選ぶという論理が適用しにくい側面を持つため、「何から」や「何を」についてはガイドラインのようなものを参考にしながらある程度選択できるとしても、「どこまで」については手がかりを得られないケースが想定されます。

どうすればこの「どこまで問題」を克服できるか、残念ながら常に応用可能な処方箋はないのが実情です。そこで、結局多くの組織ではこの問題に対して、他の組織と同等レベルを実現するという常識的な対応をすることになりがちです。これはポリシーのない態度のように見えますが、泥棒対策一般論である「周囲より弱いところが狙われる」という事実を考えれば、他所より弱い対策ではだめだ、という常識には叶っています。

さて、そもそも情報セキュリティ対策には「これをこれくらいやればよい」などという

最適解はない、というのが現実ですから、その現実に対応する仕組みが ISMS には内在しています。それは PDCA（Plan/Do/Check/Act）です。

どこまでやればよいかは最初は不明でも、とりあえず仮水準を決めて実施し、PDCA の仕組みに乗って実施状況を毎年モニタし、定めた基準や仕組みを継続的に見直し、必要に応じて改善していく、この継続の努力の結果として、「どこまで問題」は事実上解決されることになります。一度で解を求めるのではなく、毎年の不断の努力の積み重ねによって問題に対処する、そうした仕組みを持つことがマネジメントシステムです。「どこまで問題」に悩む組織ほど、ISMS の実施が救済策になるというわけです。

～ 後記 ～

地方公共団体は、行政機関であるとともに、首長を長に頂き、かつ議会を有するという点では、民間企業とは異なる特徴を有する組織ですが、類似点も多く、それゆえ ISMS 構築に取り組むことはさほど特別なことではないはずです。しかしながら、実際には取り組み事例がごくわずかしかないという現状は、ISMS が民間企業専用のものであって地方公共団体には適していない又は難しいものだという誤解によっているのではないか、という ISMS 関係者の思いから本書は企画されました。

本書は ISMS 取得のための総合虎の巻ではありませんし、地方公共団体の皆様が本書を読んだだけで、ISMS 取得のための特別なノウ・ハウをすべて理解できるというものでもありません。簡単に読み通せるようなもので、ISMS に取り組む際に躓きそうなところをざっと目を通していただき、いわば食わず嫌いの ISMS をちょっと試食して、なんとか食べられるかな、と思っていただく、本書はそのような動機付けの役割を果たす期待がこめられています。

本書が、多くの地方公共団体の関係者の方々の目に留まり、ISMS 実施の動機付けの役割を果たせることを願っております。

ISMS 適合性評価制度技術専門部会
一般財団法人日本情報経済社会推進協会（JIPDEC）

本ハンドブック及びISMSユーザーズガイドのダウンロード提供及びISMS適合性評価制度に関するFAQ、認証機関/認証取得組織情報の参照などを次のサイトからご利用いただけます。

URL: http://www.isms.jipdec.or.jp/isms.html

ISMS適合性評価制度技術専門部会

（順不同・敬称略）

氏名	会社・機関名
駒瀬　彰彦	株式会社アズジェント【主査】
丸山　満彦	デロイト トーマツ リスクサービス株式会社【副主査】
相羽　律子	株式会社日立製作所 情報・通信システム社
小寺 くれは	KPMGコンサルティング株式会社
佐藤　慶浩	株式会社 日本HP
竹下　和孝	株式会社筑波総合研究所
中村　良和	日本マネジメントシステム認証機関協議会 （BSIグループジャパン株式会社）
平野　芳行	独立行政法人 情報処理推進機構
松尾　正浩	株式会社三菱総合研究所

（2016年3月8日現在）

2016 年 3 月発行

発行者：一般財団法人日本情報経済社会推進協会(JIPDEC)

〒106-0032　東京都港区六本木 1-9-9　六本木ファーストビル

TEL 03-5860-7570　FAX 03-5573-0564

URL http://www.isms.jipdec.or.jp/

一般財団法人
日本情報経済社会推進協会
(JIPDEC)
〒106-0032 東京都港区六本木１丁目９番９号
六本木ファーストビル内
TEL 03-5860-7570　FAX 03-5573-0564
URL http://www.isms.jipdec.or.jp/