# リスクマネジメントに関するISMS要求事項改訂における課題と対応

# Issues and Approaches on the Revision of Risk Management Requirements in ISMS

○相羽 律子[1,2]，廣松 毅[2]
Ritsuko AIBA and Takeshi HIROMATSU

[1]株式会社日立製作所 情報・通信システム社　Hitachi, Ltd., Information and telecommunication Systems Company
[2]情報セキュリティ大学院大学　Institute of Inormation Security

**Abstract** ISO/IEC 27001 is one of the core standards of information security management system (ISMS) family of standards. It provides ISMS requirements and is used for ISMS certification. It is being revised in the regular revision process of ISO standards and will be published in 2013. One of the characteristics of ISMS is including risk management as one of the core activities. Thus, this paper focuses on the ISMS requirements related to risk management, and shows the issues identified in the revision process, then proposes how to approach to the issues.

**キーワード** 国際標準，情報セキュリティ，ISMS，リスクマネジメント，要求事項

## 1．はじめに

ICTの進展は社会における情報の価値を高め，その結果，情報漏洩や情報システムへの不正アクセスなどのリスクを増大させている．このような状況において情報セキュリティの重要性は高まるばかりである．また，情報セキュリティの対策に関しては完全は望めず，更にはコストと利便性のバランスを考慮した対策を講じなければならないという性質から，情報セキュリティマネジメントの重要性が強調されている．

このような状況の下で，情報セキュリティマネジメントに関する国際標準化が盛んに検討されている．そして，情報セキュリティマネジメントの組織内への導入支援を目的として，必要な取り組みを人的管理や運用などまで含めてシステムとしてまとめた情報セキュリティマネジメントシステム（以降ISMS）については，要求事項を示す認証規格が2005年に発行され，それに基づく認証制度も開始された．ISMSの認証取得済み組織は2012年6月現在，全世界では7,800以上[1]，日本国内では4,000以上[2]に達しており，比較的大きなマーケットをなしている．

他方，リスクマネジメントについても近年国際標準化が進んでいる．リスク全般を対象とした汎用的なリスクマネジメントに関するガイドライン規格は2009年に発行された．ISMSはその中心的活動としてリスクマネジメントを有するため，リスクマネジメントに関する国際標準化の動向にも大きく配慮する必要がある．

先に述べたISMSの認証規格は現在改訂作業中にある．ISMS認証を取得した組織の数を考慮するだけでもこの改訂がマーケットに与える影響は大きいことが想定できる．

したがって，本稿ではISMSの認証規格の改訂において考慮すべき点とそれらへの対応策について，特にリスクマネジメントに注目して述べる．

## 2．ISMSおよび関連する国際標準化の動向

### (1) ISMS関連国際規格の動向

ISMS関連の国際標準化はISO/IEC JTC1/SC27において進められている．ここで，ISOとは国際標準化機構（International Organization for Standardization），IECとは国際電気標準会議（International Electrotechnical Commission）であり，JTC1はISOとIECによる第一合同技術委員会（Joint Technical Committee 1）であって，情報技術（IT）分野の標準化を行うための組織である．SC27（Sub Committee 27）はセキュリティ技術（Security techniques）を担当するJTC1の下部組織にあたる．SC27はさらに下部組織として5つのWGを持ち，このうちのWG1がISMS関連の規格化を担っている．

中心となる規格はISMS要求事項を示した認証規格ISO/IEC 27001である．初版がISO/IEC 27001:2005として2005年に発行され，翌2006年には日本語に翻訳され日本工業規格（JIS Q 27001:2006）としても発行されている．またISO/IEC 27001は，ISO規格の定期見直しスケジュールに沿って，現在改訂作業中で，2013年度に改訂版を発行する予定で作業が進めてられている．

この他にも，WG1ではISO/IEC 27001によるISMSのインプリメンテーションをサポートするための各種ガイドライン規格や技術文書の発行も担っている．これらはISMSファミリ規格と呼ばれる．現在発行済み

[1] Information register of ISMS certificates, Number of Certificates Per Country (http://www.iso27001certificates.com/) に基づく数値
[2] 一般財団法人日本情報経済社会推進協会（JIPDEC），認証取得組織数推移，認証機関別・県別認証取得組織数 (http://www.isms.jipdec.or.jp/lst/ind/suii.html)に基づく数字．

あるいは検討中の ISMS ファミリ規格の一覧を表 1 に示す.

なお, ISMS ファミリ規格の中には情報セキュリティリスクマネジメントに関する規格（ISO/IEC 27005:2011）もある. このことからも, ISMS においてリスクマネジメントが重要な位置を占めることを確認できる.

**表 1 発行済みまたは検討中の ISMS ファミリ規格**

| 規格番号 ※ISO/IECは省略 | タイトル ※冒頭のInformation technology - Security techniques - は省略 | ステータス | 発行年 |
|---|---|---|---|
| 27000 | Information Security Management System - Overview and vocabulary | 改訂2版検討中 | 2009 |
| 27001 | Information Security Management System - | 改訂2版検討中 | 2005 |
| 27002 | Code of practice for information security controls | 改訂2版検討中 | 2005 |
| 27003 | Information Security Management System - | 初版発行 | 2010 |
| 27004 | Information Security Management - Measurement | 初版発行 | 2009 |
| 27005 | Information Security Management System - Information security risk | 改訂2版発行 | 2011 |
| 27006 | Requirements for bodies providing audit and certification of information security management systems | 改訂2版発行 | 2011 |
| 27007 | Guidelines for information security management systems | 初版発行 | 2011 |
| 27008 TR | Guidelines for auditors on information security controls | 初版発行 | 2011 |
| 27010 | Information Security Management for inter-sector and inter-organizational communications | 初版検討中 | - |
| 27011 | Information Security Management guidelines for telecommunications organizations based on ISO/IEC | 初版発行 | 2008 |
| 27012 | Guidelines for e-Government | プロジェクトキャンセル | - |
| 27013 | Guidelines on the integrated implementation of 27001 and 20000-1 | 初版検討中 | - |
| 27014 | Governance of information security | 初版検討中 | - |
| 27015 | Information Security Management guidelines for financial services | 初版検討中 | - |
| 27016 TR | Information Security Management - organisational | 初版検討中 | - |
| 27017 | Guidelines on information secuirty controls for the use of cloud computing services based on ISO/IEC 27002 | 初版検討中 | - |

### (2) リスクマネジメントに関する国際規格の動向

リスクマネジメントについても近年国際標準化の検討が進んでいる. ISO 規格として既に, リスクマネジメント関連用語を定義した規格（ISO Guide 73:2009, 改訂 2 版）とリスクマネジメントに関するガイドライン規格（ISO 31000:2009）が発行されている.

リスクマネジメントは情報セキュリティ分野に限らず, 古くから金融, 医療, 食品, 交通安全など様々な分野で適用されている. ISMSで想定するリスクは主に情報セキュリティリスクであり, 顕在化すると組織に甚大な損害をもたらすものと考えられている. しかし, 一般にはリスクとはより広い概念を持つ. たとえば, 企業が新しいビジネスに投資することもひとつのリスクとして考えられる. この場合のリスクは, 情報セキュリティリスクと異なり, 損害だけでなく, 利益を生む可能性も含んでいる. 先に述べたISO Guide 73:2009およびISO 31000:2009はいずれも, こうしたリスク全般を対象とした規格である.

ISO 31000:2009及びISO Guide 73:2009は, 技術管理評議会（Technical Management Board, 以降TMB）の直下に設置された作業グループISO/TMB/WG on Risk Managementで検討され発行に至った. これは, リスクマネジメントに関する規格検討のために設置された専門作業グループである.

ISO Guide 73 は初版が 2002 年に既に発行されているが, ISO 31000 開発にあたり, そのための用語規格として併せて検討が行われ, ISO 31000 の発行と同時期に, 改訂版 ISO Guide 73:2009 が発行された.

リスクマネジメントに関連するISO規格化は引き続き検討状況にあり, ISO 31000のインプリメンテーションを支援するガイドライン規格などが検討中の状況である. 発行済みあるいは検討中の規格を表2に記す.

**表 2 発行済みまたは検討中のリスクマネジメントに関する規格**

| 規格番号 | タイトル | ステータス | 発行年 |
|---|---|---|---|
| ISO Guide 73 | Risk management -- Vocabulary | 改訂2版発行 | 2009 |
| ISO 31000 | Risk management - Principles and guidelines | 初版発行 | 2009 |
| ISO 31004 | Risk management - Guidance for the implementation of ISO 31000 | 初版検討中 | - |
| ISO/IEC 31010 | Risk management -- Risk assessment techniques | 初版発行 | 2009 |

## 3. ISO/IEC 27001改訂における課題

### (1) 改訂にあたり留意すべき点

ISMSはリスクマネジメントをその中心的活動として持つことに特徴がある. というのも, 組織が保有するリスクの種類やそれらリスクに対して組織が対応すべき内容は, 組織の性質や経営者の判断によって異なるためである. つまり, 汎用的に適用できる情報セキュリティ対策集は存在せず, 効果的な情報セキュリティ対策を行なうために, 組織は自らリスクマネジメントを実施し, リスクを識別, 評価し, それに基づきリスク対応策を決定しなければならない. 言い換えると, リスクマネジメントとは, 組織が決定した情報セキュリティ対応策が, 組織に適したものであることの根拠を示すものといえる.

以上のことから, 本稿ではISMS要求事項のうち, 特にリスクマネジメントに関する要求事項に着目し, それらを改訂するにあたり留意すべき点について述べることにした.

考慮すべき点として, 次の3点をあげる. これらを抽出した理由及び課題の詳細については, 以降の節で個別に記す.

・ISO/IEC 31000との整合性
・ISO/IEC 27001:2005（現版）との対応付け
・ISMSのリスクマネジメントとして必要な詳細度の判断

### (2) ISO/IEC 31000との整合性

ISO/IEC 27001およびISO 31000は，共にリスクマネジメントのプロセスおよびフレームワークを規定しており，その内容は類似点が多い．一方，ISO 31000がリスク全般を対象とするのに対し，ISO/IEC 27001は主として情報セキュリティリスクを対象としている．このため，ISO/IEC 27001のリスクマネジメントはISO 31000を情報セキュリティに特化して適用したものとみなすことができる．したがって，ISO/IEC 27001の改訂において，ISO 31000との関係を整理することは欠かせないものといえる．

そもそも，現在発行されているISO/IEC 27001:2005は，リスクマネジメントに関連する用語としてISO Guide 73:2002を参照している．これは，ISO 31000の発行と併せて発行された第2版ISO Guide 73:2009の前の版であるが，現版と同様にリスク全般を対象に記述されていた．すなわち，ISO 27001は，従来から汎用的リスクマネジメントの定義のもとで，情報セキュリティに特化したリスクマネジメントを規格化しようという方針のもとで作成されたことを確認できる．

以上のことから，今回のISO/IEC 27001の改訂にあたっては，発行されたリスクマネジメントの汎用規格ISO 31000との整合性を考慮すべきということができる．

一方で，いかにして整合性をとるかについては，十分な検討が必要である．ISO/IEC 27001が要求事項を示す規格であるのに対して，ISO 31000はガイドライン規格であるため，その記述レベルには差がある．要求事項として何が必要かを判断し，ISO 31000から抽出するという作業が必要となる．

### (3) ISO/IEC 27001:2005（現版）との対応付け

ISMS認証を取得しているユーザ組織は，認証規格の改訂により要求事項が変更されると，認定機関が示す移行期間中に，新たな要求事項に沿うよう組織の取組みを変更しなければならない．変更内容が大きくなれば，ユーザ組織への負担も当然増える．現在7,800超の組織が認証を取得していることを考えるとき，要求事項の変更がマーケット全体に与える影響は大きい．

要求事項に大幅な変更が発生する場合には，旧版と比較してどのような変更が行なわれたのかを，変更の目的と共に明らかにする必要がある．これは，変更の必要性および妥当性を客観的に示すことを目的としている．また，変更に伴いどのような作業が発生するかを容易に判断できるようにすることも重要である．これにより，要求事項の変更に伴うユーザ組織の対応にかかる負荷を軽減することができる．

こうした配慮はISMSの認証制度を継続する意味において大変意味がある．仮に認証規格の大幅な変更が頻繁に行なわれ，その目的がユーザ組織に理解されなかったりすると，それは認証制度そのものへの不信感につながり，認証の継続に疑問を生じさせる．また，変更の必要性および妥当性を確認できない場合には，ユーザ組織だけでなく，認定機関や認証（審査）機関も認証制度への不信感を募らせる．その結果が認証制度の存続に影響を及ぼすことは容易に想像できる．ISMS認証制度の維持，普及は情報セキュリティマネジメントを普及させ，情報セキュリティの保たれた社会を実現することに貢献する．この意味で，認証制度は維持されなければならず，ユーザ組織や認定期間，認証（審査）期間に配慮した取組みも重要といえる．

### (4) ISMSのリスクマネジメントとして必要な詳細度の判断

現在発行されているISO/IEC 27001:2005に対する指摘で，リスクマネジメントに関する要求事項の中に詳細すぎてガイドラインレベルの内容になっているものがあるというものが，SC27/WG1の国際会合の場でコメントとして複数寄せられている．実際，ガイドライン規格であるISO 31000よりも詳細に記述されている箇所を確認することができる．いくつか例をあげる．ひとつめは適用範囲及び境界の定義に関するもので，ISO 27001では事業・組織・所在地・資産・技術の特徴の見地から定義することが要求されている．5つの観点をもって定義することは，ISO 27001特有の要求事項でありISO 31000には該当する記述は無い．別の例としては，リスクの特定に関するものがある．ISO 27001では組織が保護すべき資産を特定し，それら資産に対する脅威，識別された脅威がつけ込むかもしれないぜい弱性を特定することが要求されている．また，機密性，完全性及び可用性の喪失がそれらの資産に及ぼす影響について特定することも要求されている．ここで，資産，脅威，脆弱性の特定や機密性，完全性及び可用性の観点での影響の特定はISO 27001特有の要求事項であり，ISO 31000には該当する記述が無い．

上例の要求事項は，内容が詳細すぎるものの候補である．したがって，その記述レベルについて検討することは重要である．ただし，他方ではISO 31000よりも詳細な記述であることだけでは，要求事項として詳細すぎるとは言えないことにも十分留意しなければならない．情報セキュリティの特性により，ISMSのリスクマネジメントとしてISO 31000よりも詳細に要求すべき項目かもしれないためである．

すなわち，詳細すぎる要求事項と，詳細ではあるがISMSとしては必要な要求事項を見分けて，前者についてのみ必要なレベルに修正するという対応が必要である．

## 4．課題解消のための対応案

### (1) 課題解消のための対応方針

前章で記述した課題を解消するために取り組むべき内容を整理すると次のようになる．

a) ISO 31000と整合性をとるために追加・変更すべき要求事項の抽出と，適切な記述レベルでのそれらの追加

b) 詳細すぎる要求事項の抽出と，それらの適切な記述レベルへの是正
c) 現版（ISO/IEC 27005:2005）と改訂版の要求事項の対応付け
d) 変更点に関して，変更の目的および理由を明確にすること

a)および b)の活動としては，ISO 31000:2009 の記述と ISO 27001:2005 を対比することで，追加・変更すべき要求事項，および詳細すぎる要求事項の候補を抽出できる．抽出した項目の適切な記述レベルを決定するためには，変更に伴う影響度分析の実施を提案する．記述内容の対比方法や影響度分析の具体的な進め方については，案を次節から記す．

ここでの中心的な作業は上記の a)および b)の実施である．c)は，改訂結果が確定した後，2005 年版の要求事項と対応付ければよい．d)は，a)および b)を行なう過程で検討した内容を記録しておき，それらの中から変更の目的や理由に関するものを抜き出して整理するればよい．なお，c)および d)の内容は，規格の本文としては記述できないため，規格の付属文書として提供することなどを検討する．

### (2) ISO 31000 との対比

追加・変更すべき要求事項，および詳細すぎる要求事項の候補を抽出するために，どのように ISO 31000:2009 と ISO 27001:2005 を対比すべきか，作業の進め方を提案する．

先に述べたとおり，ISO/IEC 27001 が要求事項を示す規格であるのに対し，ISO 31000 はガイドライン規格であるため，記述レベルには差がある．したがって，両者の記述を単純に比較することはできない．そこでプロセスレベルでの比較を提案する．ISO 31000 にはリスクを管理するための汎用的プロセスが記されている．一方，ISO/IEC 27001:2005 もプロセスアプローチを採用しているため，各要求事項をプロセスとして捕らえることができる．また，プロセスにも何段階かの詳細度のレベルが存在するが，ISO 31000 と ISO/IEC 27001 が類似のプロセスを有することから，比較するプロセスが同じレベルにあるかどうか比較的簡単に判断できる．ISO 31000:2009 と ISO/IEC 27001:2005 のリスクマネジメントプロセスを対照した結果を表 3 に示す．表の左列は，ISO 31000:2009 のプロセスに相当するものとして，ISO 31000:2009 の箇条 5 の目次を記述した．右列には，対応する ISO/IEC 27001:2005 の要求事項の項目を記述した．

プロセスの対応付けができたら，プロセスごとに両者の記述を比較する．すなわち，表 3 で対応付けられた ISO 31000:2009 と ISO/IEC 27001:2005 の項目の記述内容を比較する．比較結果に対し，次に示す方針を適用して作業をすすめることで，追加・変更すべき要求事項，および詳細すぎる要求事項の候補の抽出，また，要求事項の改訂案の作成を行なう．

・ISO 31000:2009 の記述のうち，プロセスの主たる活動に相当し，かつ ISO/IEC 27001:2005 に記述がないものについて追加すべき要求事項の候補として抽出する．ISO 31000:2009 の該当する記述を，ISO/IEC 27001: 2005 の他の要求事項と同じ詳細度の記述となるように修正し，改訂案とする．
・ISO/IEC 27001:2005 の要求事項で ISO 31000:2009 よりも詳細なものを詳細すぎる要求事項の候補として抽出する．ISO 31000:2009 に合わせて抽象することで改訂案を作成する．
・ISO 31000:2009 と同等のことを述べていながら，用語や表現が異なる ISO/IEC 27001:2005 の要求事項を，変更すべき要求事項の候補として抽出する．ISO 31000:2009 と表現を合わせることで改訂案を作成する．

**表 3 リスクマネジメントプロセスの対照**

| ISO 31000 | ISO/IEC 27001 |
|---|---|
| 5.1 General | - |
| 5.2 Communication and consultation | |
| 5.3Establishing the context | - |
| 5.3.1 General | - |
| 5.3.2 Establishing the external context | 4.2.1 a), b)3) |
| 5.3.3 Establishing the internal context | 4.2.1 a), b)3), c)1) |
| 5.3.4 Establishing the context of the risk management process | 4.2.1 a), b)4), c), d), e), f), g), j), i), j) |
| 5.3.5 Defining risk criteria | 4.2.1 c)2) |
| 5.4 Risk assessment | - |
| 5.4.1 General | - |
| 5.4.2 Risk identification | 4.2.1 d) |
| 5.4.3 Risk analysis | 4.2.1 e) |
| 5.4.4 Risk evaluation | 4.2.1 e) |
| 5.5 Risk treatment | - |
| 5.5.1 General | - |
| 5.5.2 Selection of risk treatment options | 4.2.1 f), g) |
| 5.5.3 Preparing and implementing risk treatment plans | 4.2.1 g), 4.2.2 a), b) |
| 5.6 Monitoring and review | 4.2.3 d) |
| 5.7 Recording the risk management process | 4.3.1 |

### (3) 改訂に伴う影響分析の実施

ここでは，前節で作成した改訂案をもとに影響度分析を実施することを提案する．この分析結果によって改訂内容を確定することが目的である．影響度分析の観点としては，ユーザ組織に対する影響と規格の品質への影響の 2 つをあげる．それぞれの分析の進め方を以下に記す．

・ユーザ組織に対する影響

ユーザ組織に対する影響を分析するために，ISMS 認証取得済みのユーザ組織に対してアンケートやヒアリングを行う．収集するのは，要求事項の改訂に伴い，組織においてどの程の変更や追加の作業が発生し，どの程度の負荷が生じるかといった情報である．また，変更の結果 ISMS がどのように改善できるかについての情報も収集することが望ましい．収集した情報をもとに，負の影響が大きいものについては，維持すべき品質や変更に伴う効果を考慮した上で改訂案を見直す．ユーザ組織に対する影響を重視するのは，前述のとおり，彼らの意見が ISMS 認証制度の存続に深く影響するためである．

ユーザ組織に対するアンケートは，実際に行われた事例がある．この事例では，ISO/IEC 27001 改定作業における委員会原案（Committee Draft，以降 CD）をユーザ組織に示し，ISO/IEC 27001:2005 が CD に変更された場合の影響についてアンケート調査を実施した．アンケート実施者は，ISO/IEC JTC1SC27/WG1 小委員会[3]（国内委員会）であり，日本 ISMS ユーザグループ[4]の協力を得て，同グループの会員企業が回答者となった．アンケート結果は影響評価レポート [1]としてまとめられ，ISO/IEC JTC1/SC27/WG1 メンバ内で開示されている．本レポートの実施要領および質問票の一部を図 1 に一部掲載する．影響評価レポートは英文のため，図 1 の記述は仮訳である．

実施要領（抜粋）

対象：日本 ISMS ユーザグループの参加企業
評価項目：添付質問票
評価基準：
① 組織の ISMS にとって特にインパクトは無い
② 組織の ISMS にとってマイナスのインパクトがある
③ 組織の ISMS にとってメリットがある
④ その他
評価方法：
評価基準に従って，上記①から④の中から選択する．
選択の理由，どのようなインパクトがあるか等の補足説明を（できるだけ）記述する．

質問票（抜粋）

Q. ISO 31000 への適用により，ISMS の要求事項が以下のとおり変更となる．これによりどのようなインパクトが考えられるか．
(1) リスクアセスメント及びリスク対応の記述がハイレベルな表現になり，詳細な記述が無くなる一方で，リスクアセスメント及びリスク対応のプロセスの信頼性改善は，引き続き要求事項となる．
(2) リスクアセスメントにおいて，資産，脅威，脆弱性に関する記述が無くなる．

**図 1** 影響評価レポート（抜粋）

・規格の品質への影響

規格の品質への影響は，ISMS 認証制度の認定機関および ISMS 適合審査を実施する認証（審査）機関に対して実施したアンケートやヒアリング結果を用いて評価する．認定機関も認証（審査）機関も要求事項への適合性判断を担う専門家であるため，要求事項の変更に伴い，それに適合するように実装されたリスクマネジメントの品質がどのように変化するかを想定できるためである．

改訂に伴い品質が著しく低下することは，制度存続の観点から避けなければならない．品質の低下は，ISMS 認証取得済み組織が大きな情報セキュリティ事故を起こし，その原因が不適切な情報セキュリティマネジメントにあるというケースを多発させるかもしれない．そのような事態になれば ISO/IEC 27001 の認証規格としての信頼性は損なわれ，認証制度は存続できなくなるかもしれない．

一般には，品質の低下の原因のひとつに，要求事項の抽象化がある．要求事項の具体性が緩和された結果，従来と比較して組織の取り組み内容に幅が出るためである．ただし，要求事項の抽象化に伴う負の影響は，ISMS 認証取得済のユーザ組織からは引き出しにくい．なぜならユーザ組織は，詳細な要求事項に沿った対応をしているため，多くの場合，要求事項が抽象化されてもすぐの活動変更は必要ないからである．このことは，要求事項の抽象化に関しては，ユーザ組織への配慮は必要ないと思わせがちである．しかしこれは間違いである．要求事項の抽象化に関しても，その理由はユーザ組織に対しても明確にすべきである．なぜなら，従来取り組んできた負荷の高い要求事項が改訂に伴い突然不要になり，その理由も明らかにされないという状況では，ユーザ組織の不信感を招くからである．

**(4) 改訂案の例**

最後に改訂案の例として，ISO 31000:2009 に合わせて ISO 27001 の要求事項を抽象化する場合の例を記す．ただし，これは案段階のものにすぎない．改訂内容を確定するためには，前節に示した影響度分析を実施し内容の妥当性を検討する必要がある．

リスクの特定において，ISO/IEC 27001:2005 が要求する資産，脅威，脆弱性を特定するプロセスを削除し，ISO 31000:2009 の記述レベル合わせる改訂案を例としてあげる．ISO/IEC 27001:2005 および ISO 31000:2009 の該当記述，および改訂案を図 2 に示す．ここで，ISO 31000:2009 の記述は，資産，脅威，脆弱性の特定に関する記述はないものの，ガイドライン規格であるため，記述のレベルは ISO 27001:2005 と比較してかなり詳細であることが確認できる．また，改訂案については，リスクの特定プロセスにおいて，ISO 31000 が資産，脅威，脆弱性の特定に関して記述していないことから，これらの記述をもたない案となっていること，また，その記述の詳細度は ISO/IEC 27001:2005 と同等のレベルを維持していることが確認できる．

なお，この改訂案については，資産，脅威，脆弱性を特定するプロセスを削除することによって ISMS リスクマネジメントの品質が低下するかという観点で，分析されなければならない．すなわち，ISMS 認定機関および認証（審査）機関へアンケートやヒアリングを行い，その結果をもって影響度分析を実施することが望ましい．

---

[3] ISO/IEC JTC 1 への対応を主目的とする一般社団法人 情報処理学会 情報規格調査会(http://www.itscj.ipsj.or.jp/index.html) の下部組織．SC27/WG1 への対応を行なう国内委員会．

[4] ISMS の既認証取得企業を中心に，今後 ISMS 認証取得を予定する企業，ISMS コンサルティング企業，ISMS 標準化賛同企業などが連携することにより，ISMS 関連技術を共有し，お互いの経験に基づく意見交換・議論を進め，日本における健全かつ効果的な ISMS 普及・促進に貢献することを目的とする団体．(http://j-isms.jp/)

ISO 31000:2009 の記述

5.4.2 Risk Identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

ISO/IEC 27001:2005 の記述

4.2.1 Establish the ISMS

d) Identify the risks.

1) Identify the assets within the scope of the ISMS, and the owners2) of these assets.
2) Identify the threats to those assets.
3) Identify the vulnerabilities that might be exploited by the threats.
4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

ISO 27001 の改訂案

The organization shall apply information security risk assessment process that

- identifies, analyses and evaluates information security risks concerning the preservation of confidentiality, integrity and availability of information
- identifies the information security risk owners.

**図 2 ISO 31000:2009, ISO/IEC 27001:2005 および改訂案の記述の比較**

尚，ここであげた例の場合には，影響度分析とは別に一般的な観点から，ISO 31000:2009 に合わせた抽象化によるメリットを見つけることも出来る．たとえば，組織が ISMS の他にも事業継続や環境などのリスクマネジメントを伴う複数のマネジメントシステムのインプリメンテーションを検討している場合を想定してみる．このようなケースは比較的頻繁に発生する．リスクの特定において，資産，脅威，脆弱性の特定プロセスを要求しているのは ISMS のみである．複数マネジメントシステムのリスクマネジメントの統合を組織が推進する際に，この差分が統合を難しくする場合がある．リスク特定において，ISMS ではまず資産を特定しなければならないが，事業継続など他のマネジメントシステムでは資産の特定が意味をなさない，または想定しにくいかもしれない．このような場合には，リスクマネジメントの手順を統合しにくい結果となる．したがって，ISMS の要求事項から資産，脅威，脆弱性の特定プロセスを削除することは，リスクマネジメント手順の統合の観点からは望ましいことと考えることもできる．

最終的には，ISMS 品質低下の観点での分析結果や上記のメリットを総合的に見て判断し，その上で改訂案を確定させることが重要である．

## 5．まとめ

本稿では，リスクマネジメントに関する ISMS 要求事項の改訂において留意すべき事項を述べた．ひとつは，リスクマネジメントの汎用規格 ISO 31000 との整合性をとることについて，それが必要な理由と整合性をとるためのアプローチ案を述べた．また，改訂に伴う影響度分析を実施することを提案した．これは，ISMS 要求事項として必要とされる詳細度を決定するための方法として述べ，分析の進め方についても提案した．ただし，本稿では改訂作業の進め方の案を述べたにすぎないため，ここで提案した内容は，実際の改訂作業に適用した上で，予想した結果が得られているかを分析することが必要である．

また，本稿では ISMS 要求事項のうちリスクマネジメントに関するもののみを対象としたが，それ以外の要求事項についても検討する必要がある．なお，その際に考慮すべき事項として，ISO/TMB/TAG13-JTCG において現在開発されているマネジメントシステムに共通して適用する「規格の構造，テキスト及び用語」がある．これらはマネジメントシステムを伴う認証規格すべてに対し，原則適用するよう強制されるため，ISO/IEC 27001 も現在，適合作業を進めている．共通のものとして示される「規格の構造，テキストおよび用語」と ISO 27001 を比較し，必要な改訂を検討する際にも，本稿で述べた改訂の進め方は部分的に適用することができるため、本稿は良い参考情報となると考える．

## 参考文献

1) 日本工業標準調査会(JISC), National Body of Japan (2012) : ISO/IEC JTC 1/SC 27 N10961, BIA (Business Impact Analysis) Report on ISO/IEC 27001/27002