Vol.2014-EIP-63 No.10
2014/2/21

情報セキュリティマネジメント規格の改訂と問題点について

原田 要之助[†1]

ISO/IEC27001 /27002 が 2014 年 10 月に改定された．改訂にあたっては，旧バージョンから IT の急速な技術進歩，利活用の変化，社会の変化，サイバー攻撃など新 しい現実に向けて，様々な工夫がなされている．本稿では，改訂の内容から始め，今後の ISMS の方向などを論じる．また，新旧バージョンを比較することに より，この 20 年ほどにおける情報セキュリティマネジメントの進展についてまとめる．さらに，改定の内容，考え方，注意すべき点などをについて述べる．

A study on Revision of ISO/IEC27001/27002 and its impact

YONOSUKE HARADA[†1]

ISO/IEC27001/27002 (International standard for Information Security Management) have revised at October, 2014. This paper overviews the major changes on those document from Information Security management, especially, how the standard is focused on topics and change the weight of importance among subjects. Also, the improvement on IT technologies, legislations, business manner, management tools are discussed how standards are considered. In the end, some suggestions to standards are studied and proposed for next revision.

1. はじめに

ISO/IEC27000 シリーズは，2013 年に大きく改定された．これは，前回の改定が 2005 年であり，この 8 年間に情報セキュリティをとりまく環境が大きく変わった．とくに，IT 分野では，ハードウェアの性能向上，ソフトウェアの仮想技術やセキュアコンピューティング，インターネットのバックボーンおよびアクセス回線の速度の向上，サイバー攻撃や情報漏えいの増加，IT 分野の法制度の制改訂など，さまざまな分野で変化が起きた．詳細については，付録 1 に述べる．

情報セキュリティの認証制度では，2005 年に ISO/IEC27001:2005[1]を要求条件として ISMS（Information Security Management System：情報セキュリティマネジメントシステム）適合性評価制度（以下，ISMS という）が始まった．2013 年末時点では，全世界で約 8,000 事業所，日本国内では約 4,500 事業所*1が認証されている[2]. とくに，ISMS 認証は，国内的には企業の契約や政府の入札要件などさまざまな用途に用いられている．また，CSA（Cloud Security Alliance）による STAR(クラウドサービスの認証制度) [3]では，CCM（Cloud Control Matrix）[4]の管理策の検証として ISMS の管理策（ISO/IEC27001 の Annex A）が参照されている．

本稿では，2013 年に改定された ISO/IEC27000:2013，27001:2013，27002:2013*2の改定について解説する．また，改定版の使い方，注意すべき点などを論じ残された課題についてまとめる．最後に，情報セキュリティマネジメントの変遷から，今後，情報セキュリティマネジメントの進展について論じる．

2. 情報セキュリティマネジメント規格の変遷

2.1 情報セキュリティマネジメント規格の黎明期

情報セキュリティマネジメントは，1990 年以前には，ホストコンピュータのセキュリティとして議論されてきた．この時代には，ホストコンピュータがデータセンタなどの中で物理的に隔離された環境の中で利用されてきたため，セキュリティについてはデータセンタ内部でのハードウェアの管理やシステムの運用面での論理的なアクセス管理が中心となってきた．1990 年代になって，クライアントサーバ環境に変わる中で，企業の多くが，物理的に離れた環境に設置された複数の機器をネットワークで接続し，様々な関係者が情報システムを利用するようになった．このような状況のなかで，英国の DTI(Department of Trade and Industry)のもとで,英国の大企業が集まって情報セキュリティの管理策をまとめた．これらの企業は，ネットワークを接続したり，情報を交換したりするときに，相手の情報セキュリティの管理状況が分からないままに，自社の機密

＊1 ISMS 認証は，組織（企業など）の事業所や部署を対象に認証を受けることができる．なお，P マークでは組織単位に認証を受ける．

＊2本稿では，ISO/IEC27001 の場合は，27001 の複数の版を総称したものとし，ISO/IEC27001:2005 と年号をつけるものは特定の年次の版を指す

情報を相手に渡せない．そこで，企業で共通に実施されているベースラインとしてのセキュリティ管理について1992 年に調査を実施して，その結果をまとめた．企業間での取引に関係することから DTI がまとめ役となったものの，国による規制にすると貿易上不利となるので，自主的なフレームワークと考えて,DISCPD0003”Code of practice for Information Security Management” [5]とした．この規範は，様々な企業の参考になること，規範を維持管理する必要があることから，英国の BSI(British Standard Institute 英国規格協会)が，英国の規格 BS7799-1 [6]として引き継ぐことになった．この経過を図 2-1 に示す．

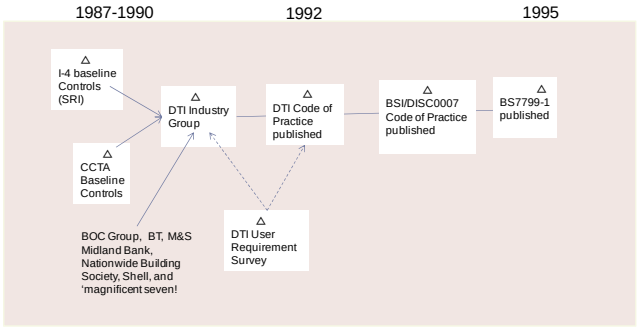


図 2-1 1995 年以前の情報セキュリティマネジメント

2.2 情報セキュリティマネジメントの規格の国際化

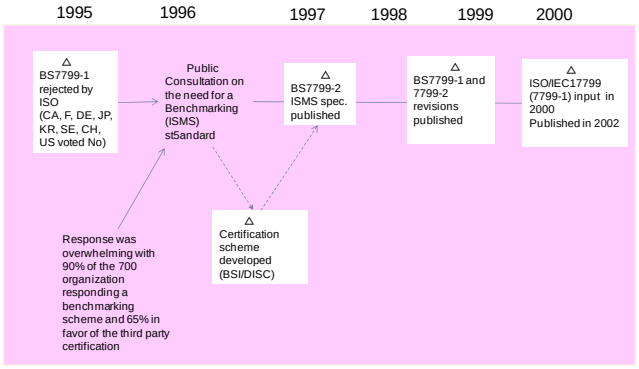
BSI では，1995 年当時，品質や環境の国際認証をリードしており，BS7799-1 も，国際間で企業が情報セキュリティを国際間で取り決めする際に利用するのに適しているとして，国際規格として ISO に提唱した．しかし，標準化を担当している ISO/IEC JTC 1/SC 27 - IT Security techniques （情報セキュリティの標準化を担当しているグループ）では，主要国が基準の必要性に疑問を呈して反対した．

なお，日本では，後年，BS7799-1 が持ち込まれたときに，この実践規範は誰もが従うべきガイドラインと誤解された．一部には,BS7799-1 や ISACA の CobiT[7]などの海外のフレームワークが意味する概念が分かりにくいことから，ベストプラクティスとして紹介された．これは，多くの日本企業は，省庁などからのガイドラインを利用するという受け身のマインドであつたため，フレームワークなど自社の都合で決めるという新しい概念について取扱いに苦慮したためである．また，多くの企業担当者にとっては，“お上からの通達”の方が，内部での意思決定が楽であったという企業カルチャにもよる．このように，企業からの要請が多かったため，結局は，経済産業省が，JIS X.5080 [8]をベースに情報セキュリティ管理基準 V.1[9]を 2003 年に策定している．

1997 年には経済産業省では，情報処理サービス業情報システム安全対策実施事業所認定基準[10]を策定して，事業者を認定する制度を準備していたこともあり，英国からの BS7799-1 の国際規格化に反対している．ただし，日本企業の一部には，既に DTI の翻訳も出回っており，セキュリティポリシの策定や内部のセキュリティ基準としての利用が始まっていた．さらに，グローバルな企業にとっては，国内と国外で規格が異なることへの反対もあった．

英国では，BS7799-1 を利用する組織が増えており，この規格をベースに情報セキュリティを構築していることの認証ニーズが顕在化していた．そこで，1997 年に情報セキュリティマネジメントの要求条件を BS7799-2[12]として制定し，この要求条件をもとに国内を対象にした認証制度を開始した．これらの規格は 1999 年に一部改訂された．

また，各国とも，企業が情報セキュリティマネジメントの国際規格を必要としていることから，2000 年に BS7799-1 が国際規格 ISOIEC7799:2000 となることを承認した．この経過を図 2-2 に示す．



7

図 2-2 ISMS 黎明期の情報セキュリティマネジメント

2.3 情報セキュリティマネジメントの規格の国際化

日本では，2000 年に ISO/IEC17799 の国際規格化に賛成したあと,ISMS の国内での認証制度を検討して,2001 年から，JIPDEC(情報処理開発協会)が ISMS の認証制度のパイロット事業を行い，この成果を受けて 2002 年 4 月より，ISMS の本格運用を始めた．認証規格としては，要求条件を BS7799-2，管理策は ISO/IEC17799:2000 を用いた．この経過を図 2-3 に示す．

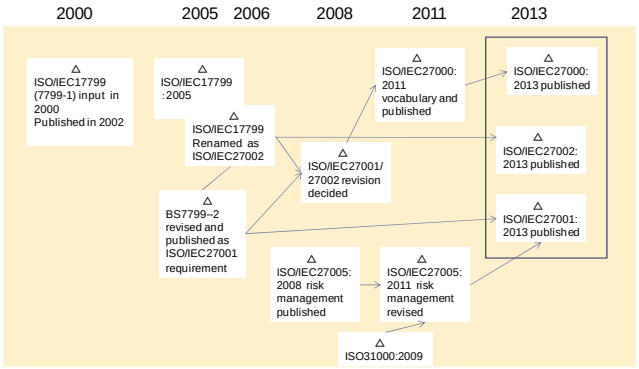


図 2-3 2000 年以降の国際規格としての発展

2005 年には，日本や英国での ISMS の順調な進展が見られることから，BS7799-1 が，ISO/IEC27001:2005 として国際

規格となった．また，同時に ISO/IEC17799：2000 も内容を見直して，ISO/IEC17799：2005 が発行された．この規格は，名称を合わせることから，ISO/IEC27002：2005 に名称変更された（内容は変えずに表紙のみ差し替え）．

3. ISO/IEC27000 シリーズについて

ISO/IEC 27001 と 27002 の規格は，ISO/IEC27000:2012[13]の用語を始め，ISMS を実装するための規格 ISO/IEC27003:2010 [14]，運用で定量的な管理をする場合の測定項目に関する規格 ISO/IEC27004:200[15]，リスクマネジメントに関する規格 ISO/IEC27005:2011[16]が開発されている．これらの規格は，ISO/IEC27000 ファミリー規格と呼ばれている．これを図 3-1 に示す．規格名は，付録２を参照のこと．なお，現在の規格の，27003，27004，27005 は 2005 年の規格と整合がとられており，ISO/IEC 27001:2013 や 2700:2013 年とは整合しない．現在，ISO/IEC SC27 で改定作業が実施されている．なお，ISO/IEC27000:2014（Overview and Vocabulary：概要と用語）*3[17]については，ISO/IEC27001:2013 年版との対応がとられている．

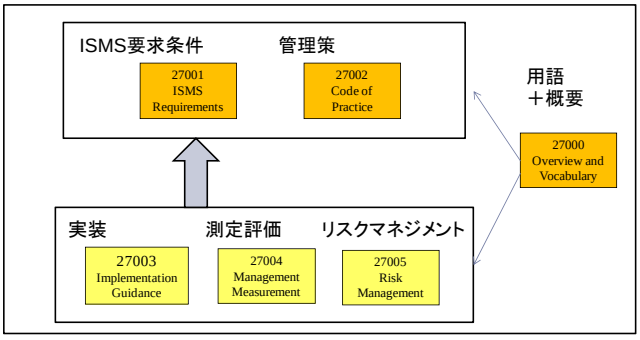


図 3-1 ISO/IEC27000 のファミリー規格について

4. ISO/IEC27001 の改定について

4.1 MSS 共通テキストへの準拠

ISOでは，2006年から2011年にかけて，ISO 9001，ISO 14001，ISO/IEC 27001などのISOマネジメントシステム規格（ISO MSS：ISO Management System Standard）の整合性を確保するための議論が行われて，MSS上位構造（HLS），MSS共通テキスト（要求事項）及び共通用語・定義[18]が開発された．この一連のISO MSS共通要素は2012年2月に承認され，今後，制定／改正される全てのISO MSSが原則としてこのISO MSS共通要素を採用して開発することが義務付けられた[19]．これらのISO MSS共通要素は，5月1日に発行されたISO/IEC Directives（専門業務用指針）のSupplement（補足指針）の改訂版の附属書SLに盛り込まれている．この構造を図4-1に示す．内容は，マネジメントシステムとしてのPDCAが中心となっている．

*3 この規格は 2010 年，2012 年，2014 年に改定されているので，利用するときには注意されたい．

- (1. 適用範囲)
- (2. 引用規格)
- (3. 用語及び定義)
- 4. Context of th
- e organization（組織の状況）
- 5. Leadership（リーダーシップ）
- 6. Planning（計画）
- 7. Support（支援）
- 8. Operation（運用）
- 9. Performance Evaluation（パフォーマンス評価）
- 10. Improvement（改善）MSS（Management System Standard）

図 4-1 ISO MSS 共通要素[15]より

ISO/IEC27001:2013の改定では，このMSSに準拠することになり，規格化にあたっては，どう共通要素を当てはめるかがが議論された．MSSに準拠することと，ISMSの最大の特徴であるリスクベースの考え方を取り入れることとなった．具体的には，MSSに以下の章を追加している．これを図 4-2に示す．

6.1.2 情報セキュリティリスクアセスメント
6.1.3 情報セキュリティリスク対応
8.2 情報セキュリティリスクアセスメント
8.3 情報セキュリティリスク対応

図 4-2 ISO MSS 共通要素に追加されたリスク関連

4.2 リスクベースの概念への変更

ISO/IEC27001:2005では，ISMSを実施するにあたって，リスクを特定するために，情報資産*4を洗い出して，次のように進める．これは，ほとんどの情報が紙，磁気記録媒体，メモリ，サーバ，PCなどの物理的な媒体に格納されていることと，これらの物理媒体は資産として管理されることが多いことによる．ISMSを採用する場合には，組織の膨大な情報に関連する資産を洗い出す必要があり，体系的かつ具体的に実施できることが必要となる．また，情報のリスクへの責任については，媒体を管理する管理者に一意に関係づけられるからである．これを図4-3に示す．

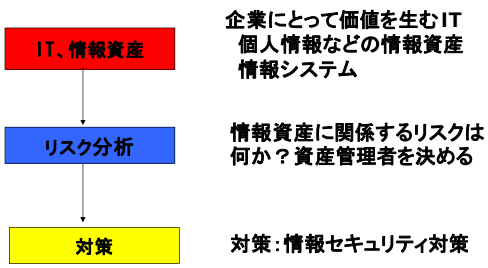


図 4-3 ISO/IEC27001:2005 でのリスク分析の考え方

ISO/IEC27001:2013[20]は，リスクについては，ISO31000:2009 Risk Management[21]及びISO Guide73:2009[22]に基づき，「目

*4 英語では，資産（asset）となっているが，ガイドラインの利用にあたって，誤解されないように，情報資産と呼称されている．

的に対する不確かさの影響」としている．これに基づき，情報へのリスクを考える場合，2000年代と2010年代で情報の捉え方が大きく変化した．具体的には，2010年代になって，ネットワークが高速・広帯域となったため，情報を一か所のサーバやPCで管理するのではなく，ネットワークに接続された複数のサーバに複数に分散して管理されたりするようになった．このようになると，資産管理者が情報に関して責任をとれないケースも出てくる．また，クラウドでは，物理的にどこに所在するかも不明である．そのため，情報が存在するポイントでリスクを管理する責任者を決めて，管理責任を果たさせるように拡張された．これを図4-4に示す．

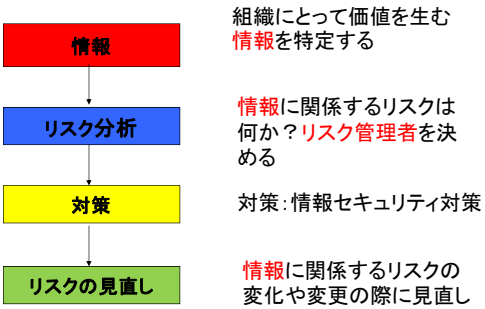


図 4-4 ISO/IEC27001:2013 でのリスク分析の考え方

すなわち，ISO/IEC27001:2013の「6.1.2 情報セキュリティリスクアセスメント」では，以下のようなプロセスが述べられている．

c) 次によって情報セキュリティリスクを特定する．
1) 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を特定するために，情報セキュリティリスクアセスメントのプロセスを適用する．
2) これらのリスク所有者を特定する．
d) 次によって情報セキュリティリスクを分析する．
1) c) -1)で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う．
2) c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う．
3) リスクレベルを決定する．
e) 次によって情報セキュリティリスクを評価する．

図 4-5 新しいリスク分析の考え方（ISO/IEC27001:2013[20]の6.1.4章より抜粋）

5. ISO/IEC27002 の改定について

5.1 DISC003 からの情報セキュリティマネジメントの変容について

ISO/IEC27002:2013[23]は，2章で述べたように，歴史の長い規格である．DISC0003を含めると既に，20年間にわたって5つ目の版が出版されているが，基本的な内容については，あまり変化はない．章について比較したものを表5-1に示す．

表5-1 情報セキュリティ管理策の変遷

ISO/IEC27002'2013	DISC PD0003	BSI7799-1	27002:2000	27002:2005
リスク分析		序文	序文	3
5 情報セキュリティのための方針群	1	3	3	5
6 情報セキュリティのための組織	2	4	4	6
7 人的資源のセキュリティ	4	6	6	8
8 資産の管理	3	5	5	7
9 アクセス制御	7	9	9	11
10 暗号	(8)	(10)	(10)	(12)
11 物理的及び環境的セキュリティ	5	7	7	9
12 運用のセキュリティ	6	8	8	10
13 通信のセキュリティ	6	8	8	10
14 システムの取得，開発及び保守	8	10	10	12
15 供給者関係	–	–	–	–
16 情報セキュリティインシデント管理	–	–	–	13
17 事業継続マネジメントにおける情報セキュリティの側面	9	11	11	14
18 順守	10	12	12	15

まず，DTIのDISC0003では，企業の情報セキュリティに関する共通の基盤とするための最小限の情報セキュリティ対策がリストアップされている．また，コントロール目標やコントロール（管理策）という概念は述べられていない．これが，BS7799-1に引き継がれた時点で，リスクベースの概念が導入され，リスク分析を実施して，セキュリティの要求条件を明確にして，管理策を選択するという概念が持ち込まれた．これば，現在のISO/IEC27002のベースとなっている．

なお，リスク分析については，2005年の改訂の時点で，この基準だけでリスク分析からリスク対策，管理策の導入，見直しができるようになった．これは，BS7799-2が国際規格となっていないため，リスク分析からのアプローチを導入することにしたためである．したがって，ISO/IEC27002:2005年版はある意味，組織が情報セキュリティマネジメントを実施する上で，自己完結した規格であったと言えよう．2007年に始まった改定では，ISO/IEC27001と27002での規格の作られたタイミングの違いで，ずれが生じていた部分や齟齬がある部分の修正が必須のこととなった．

5.2 2005 年版と 2013 年版の位置づけの変更

1) 27001 と 27002 の関係について

27001は認証のための要求条件であり，具体的な管理策については付属書Aに述べている．この関係を図5-1に示す．

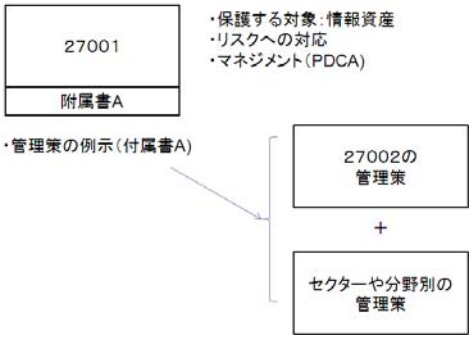


図5-1 ISO/IEC27001付属書AとISO/IEC27002の管理策の関係

この付属書Aは，管理目的と管理策の対応表であり，具体的な管理策の内容については記載されていない．2005年の改訂では，こ

の管理目的と管理策は，27002の5章以降の章と対応するように策定されている．また，今後，27002をベースにセクター別などの管理策群を追加できる構造が可能としている．

2) 27002 のタイトルの変更

2013年の改訂では，2つの規格間の整合性をとることが重視さてたため，ISO/IEC27002:2005に記載されていたリスク分析などがなくなり，管理策のみの規格となった．また，2つの規格の位置づけを明確にするため，規格のタイトルが，ISO/IEC27002:2005では，「Information technology- Security techniques - Code of practice for information security management（情報セキュリティ管理の実践のための規範）」となっていたものを，「Information technology- Security techniques - Code of practice for information security controls（情報セキュリティ管理策の実践のための規範）」と変えている．そのため，27002単独では情報セキュリティマネジメントを遂行することができなくなっている点に注意する必要がある．

5.3 章構成と管理策について

管理目的，管理策の多くは，基本的には，ISO/IEC27002:2005のものを継承，踏襲している．内容的には，章の表題と管理策がほぼ同一となっている．両者の関係を図5-2に示す．ただし，実施の手引きや関連情報については，見直されているものが多いので，管理策が同じといっても，注意が必要である．

図5-2　ISO/IEC27002:2005と2013の章構成の対応[24]

管理策については，技術的なものやマネジメントに整合しないものが削除されて，133の管理策が114に削減された．2005年以降に，ISO/IEC SC27では，多数の技術分野の規格が策定されており，とくに，ネットワークのセキュリティ，情報セキュリティインシデント管理などのガイドラインが策定されている．また，事業継続計画したがって，管理策の選択や実施にあたっては，ISO/IEC27002:2013に詳述するのではなく，必要な部分については他の規格を参照して，マネジメントとして実践する必要がある部分を詳述して，重複を防いでいる．そのため，参照されているガイドラインを参考にする必要がある．この関係を図5-2に示す．また，参照されるガイドラインを表5-2に示す．

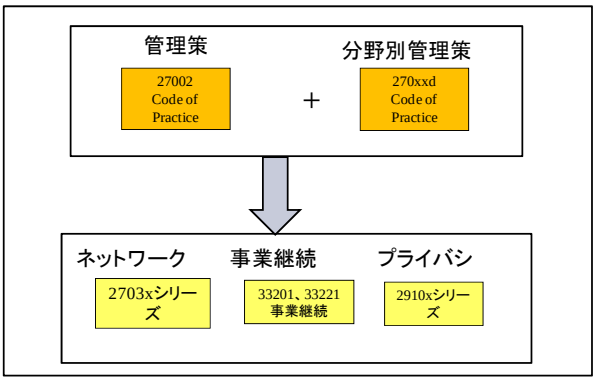


図5-3　管理策と他のガイドラインの関係

表 5-2　ISO/IEC27002:2013 が参照しているガイドライン

	分野と参照規格
13	ネットワークセキュリティ管理 ISO/IEC 27033, Information technology - Security techniques - Network security, Parts 1, 2, 3, 4 and 5
15	サプライチェーンのセキュリティ管理 ISO/IEC 27036, Information technology - Security techniques - Information security for supplier relationships, Parts 1, 2 and 3
16	情報セキュリティインシデント管理 ISO/IEC 27035, Information technology - Security techniques - Information security incident management ISO/IEC 27037, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence
17	事業継続管理 ISO/IEC 27031, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity ISO 22313, Social security - Business continuity management systems - Guidance
18	プライバシのフレームワーク ISO/IEC 29100, Information technology - Security techniques - Privacy framework

5.4 セキュリティポリシについて

ISO/IEC27002:2005では，組織の情報セキュリティポリシであり，ISO/IEC27001:2005のISMSポリシと用語が異なり，かつ，両者の関係が不明確であった．ISO/IEC27002: 2013では，方針文書でなく，方針（群）に関する管理策とした．ポリシを策定する際，この中から選択して，組織のポリシを策定することになり，両者の齟齬が解消された．なお，組織が実施する管理策をどのように選択するかが分かり易くするために，各章の管理策の方針にあたるもの「許可されるIT使用の方針」「ネットワークセキュリティの方針」「外部委託の方針」「モバイルデバイスの方針」　等が集められ，選択できる構造としている．

5.5 組織について

ISO/IEC27002:2005では，6章に組織について，経営者，マネジメントが詳しく詳述されていた．ISO/IEC27002:2013では，管理策として必要な最小限の内部組織について役割が述べられているだけとなった．とくに，経営層の役割については，ISO/IEC27014:2013

情報セキュリティガバナンス[25]を参照することとなった．一方，組織にとっては，昨今のモバイル環境でのビジネス遂行が重要な管理対象となっている．これを反映する形で，6.2章にモバイル機器およびテレワーキングが設けられている．ISO/IEC27002：2005までは，アクセス制御の一項目でしかなかった管理策群が，重要な観点としてクローズアップされている．

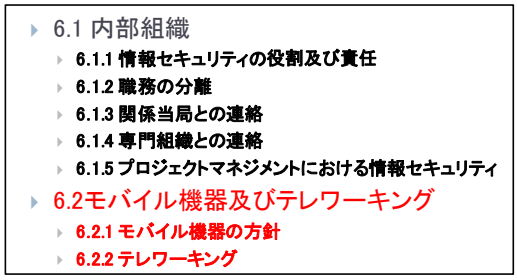


図5-2　ISO/IEC27002:2013の組織について

5.6　新しい概念や用語の整理

ISO/IEC27002：2013では次の新しい概念を取り入れている．

①　関係者の整理

今まで，関係者としては，従業員，契約者，第三の利用者となっていたが，第三の利用者が分かりにくく，どこまで，組織のセキュリティの管理対象とするかが曖昧となる原因であった．これを，供給者関係（supplier relationships）という概念を持ち込み整理した．一方，組織の Web にアクセスしてくる利用者は第三者として管理対象とはしないこととなった．

②　秘密認証情報

パスワード以外のバイオメトリックス，秘密鍵などパスワード以外の手段も認証のための手段となっている現実に合わせた新しい概念を取り入れた．ただし，管理策の多くは，パスワードを念頭においたものとなっている．

③　2005 年版の古い用語を見直した

「10.9 電子商取引サービス」，「10.9.1 電子商取引」，「10.9.2 オンライン取引」，「10.9.3 公開情報」が，2013 年版では，「14.1.2 公共ネットワーク上の業務処理サービスのセキュリティ」，「14.1.3 業務処理サービスのトランザクションの保護」となっている．

④　開発に関する具体的な内容を削除

セキュアプログラミングの進展，SOX などによる内部統制の進展などとバッテッングしないように，一部の管理策を削除している．「12.2 業務用ソフトウェアでの正確な処理」「12.2.1 入力データの妥当性確認」「12.2.2 内部処理の管理」「12.2.3 メッセージの完全性」「12.2.4 出力データの妥当性確認」など．

⑤ロールベース（役割に基づく）のアクセス制御

「9.2.1 利用者登録および登録削除」については，「 9.2.1利用者登録および登録削除　User Registration and de-registration」と「9.2.2　利用者アクセスの提供　User Access Provisioning」の二つに分けられた．これは，アクセスについては，組織に配属された時点でIDが登録され，アクセス権の付与については，正式な利用申請に基づいて役割からアクセス権を提供（Provisioning）する考え方である．

5.7　通信と運用の分離

ISO/IEC27002:2005では，「10 通信及び運用管理」が管理策も多く，他の章とのバランスが悪かった．これについては，ISO/IEC27002:2013では，「12 運用のセキュリティ」と「13 通信のセキュリティ」に分けられた．とくに，情報セキュリティマネジメントでは，運用に重点が置かれたのが見てとれる．

5.8　ログについての誤解を訂正

ログについては，ISO/IEC27002:2005から，監査ログ（Audit log）という概念が持ち込まれた．これは，ログ情報を闇雲に集めるのではなく，監査などの目的に合わせて収集するという意味であったが，監査ログという言葉が説明なしに用いられており，マネジメントに必要なログの収集と読まれないという誤解が生じていた．そのため，ISO/IEC17799:2000まで用いられていたイベントログに戻すことになった．ここでのイベントログの収集は，利用者の活動，例外処理，過失及び情報セキュリティ事象を記録し，保持し，定期的にレビューするためとしている．

5.9　事業継続管理の位置づけの変更

事業継続管理は，そもそものガイドラインのDISC0003での主要な目的であった．しかし，2012年にISO/IEC22301・22323などの事業継続管理が新しいマネジメントシステムとして独立した．そのため，ISO/IEC27002:2013では「14 事業継続管理」から，「17 事業継続管理の情報セキュリティの側面」とスコープを情報セキュリティの範囲に主題を限定した．この観点から，新しい「17.2（冗長性）」の管理策が追加され，具体的には，「17.2.1 情報処理施設の可用性」を重視し，「情報処理施設は，可用性の要求に対応するために十分な冗長性を実装することが望ましい．」としている．

5.10 プライバシーと PII について

ISO/IEC27002:2013では，今までの個人情報を「18.1.4 プライバシーおよび個人を特定できる情報（PII)の保護管理策」に拡張している．「プライバシーおよびPIIの保護は，適用がある場合には，関連する法令及び規制の要求に従って確実にすることが望ましい．」としており，国内的には影響は限定的であるが，海外拠点においてISMSを構築するときには，その地の法令等が関連しないか厳重にチェックする必要がある．

5.11 暗号の管理策について

ISO/IEC27002:2013では，暗号が様々な管理策が暗号化に触れていることから，単独の章にまとめられている．具体的な管理策については利用方針と鍵管理の２つとなっている．

5.12 法令遵守について

ISO/IEC27002:2013では，法的な問題について，従来よりも，法令遵守を強調している．例えば，暗号の利用では，貿易での制限について述べ，供給者関係では，国が異なるサービスについての法的な問題に注意を促している．知的財産関係では，ライセンスの問題や著作権について述べている．さらに，アクセスログの取得，監視カメラ，採用前のスクリーニングなど個人情報の収集に関わる管理策では，地域の法令・法制度との調整・遵守を今までより強調している．

ISMS(情報セキュリティマネジメントシステム)の拡張

5.13 ISMS の管理策について

ISMS の認証では，図 5-1 に示したように，ISO/IEC27001 は付属書 A から管理目的に合わせて管理策を選択することになっている．この付属書 A は，ISO/IEC27002 の管理目的と管理策に対応している．2008 年に ISO/IEC27011:2008 が策定され，通信分野では，27002 と 27011 を組み合わせて認証を受けられるようになった．また，2012 年には，ISO/IEC IR27015 が金融分野を対象に策定された．この関係を図 6-1 に示す．

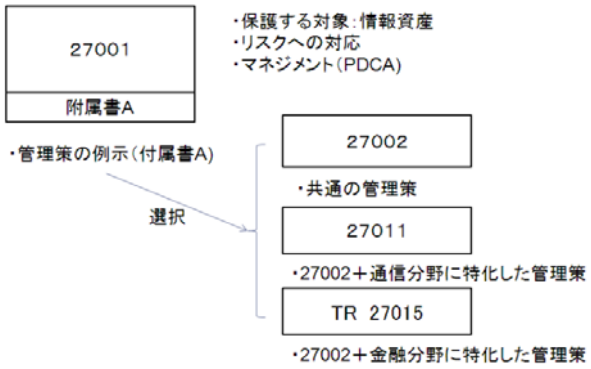


図6-1　分野別の管理策の追加

クラウドについては，当初，ISO/IEC27002 の管理策に追加する案も検討されたが，開発のスケジュールが合わないことやクラウドのサービスでは，サービス提供側，サービル利用側と分かれるため，ISO/IEC27002 に追加するのは得策でないこと．経済産業省が 2011 年に「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を策定した．ガイドラインは，ISO/IEC27002 と組み合わせて利用すること意図している．日本はこの構造を ISO/IEC SC27 に提案して，ISO/IEC 27017 の開発が始まった．これを図 6-2 に示す．

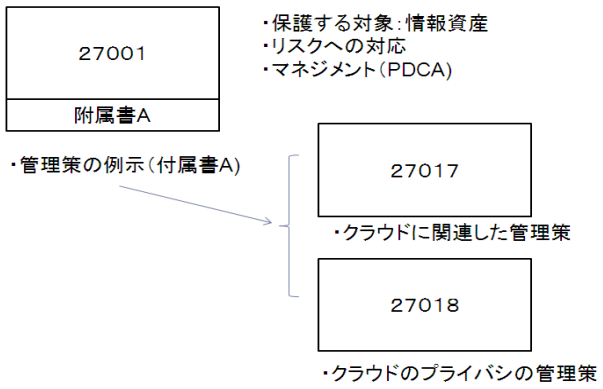


図6-2　クラウドの管理策の追加

このように ISMS の認証については，分野別やクラウド，プライバシーなどを組み合わせて認証できれば，組織が外部に対して説明責任を高めることができる．ISO/IEC SC27 では，図 6-1 や図 6-2 の構造をより，一般化して，管理策の追加が容易な構造をとることができるようにガイドライン ISO/IEC27009 を策定中である．図 6-3 に示す．このガイドラインができれば，基本部分としての ISO//IEC27002 と分野別やサービス別に追加の管理策で認証をより専門化でいるようになる．これによって，ISMS の認証がより，利用者に魅力的なものとなると考えられる．

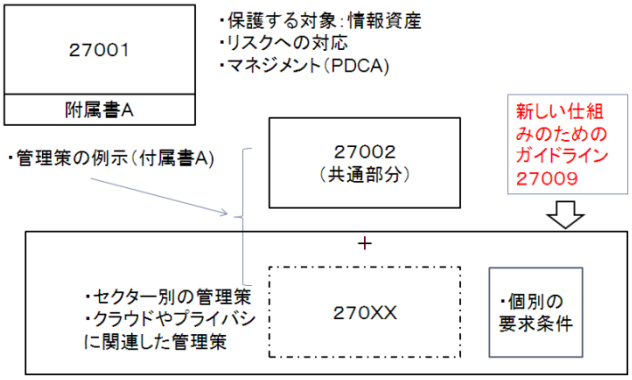


図6-3　分野別の管理策を追加できる仕組み

6. 情報セキュリティマネジメントの課題

情報セキュリティマネジメントは，この 20 年間に大きく進化して，ISMS による認証制度も大きく成長した．また，IT の技術進歩やマネジメントの進化のおかげで，管理方法についても変遷している．事業継続計画については，重症性が認知されて，別の体系として独立した．これに合わせて，情報セキュリティ本来の管理策である可用性に落ち着いた．また，インシデント管理については，2005 年の改訂で盛り込まれたが，さらに詳細化されて，一つの管理分野となっている．現在は，サプライチューンセキュリティなど供給者関係が同様に独立した管理体系となると考えられる．

モバイルコンピューティングでは，個々の管理策となっているが，MDM（Mobile Device Management）というシステム化が図られて自動化が進んでいる．運用面では，MDM の管理が新しい課題となっている．また，物理セキュリティ分野では，入退室のシステムが自動化され，このシステムの脆弱性や運用がマネジメントの新たな課題となっている．このように，情報セキュリティマネジメントは，ある情報セキュリティの問題が表出すると，まず，問題が検討されて，対策として，ポリシの策定，ルール化，しくみの定常化と進み，新しく導入されたしくみについては，範囲が大きい場合には，それだけでマネジメントシステムが必要となるため，独立したものとなる．一方，システム化さ

れたものについては，システムの運用が新しい課題となりマネジメントが深化していく．すなわち，情報セキュリティマネジメント全体としてのPDCAも重要な課題となっている．国際規格はこれらの動向を後追いするものの，時間遅れが問題となっている．

7. まとめ

情報セキュリティマネジメントは，この20年間のITの進歩や利用面の変化で位置づけが大きく変わってきている．企業のほとんどが情報セキュリティの対策を実施するようになっている．これを支えてきたのがISO/IEC27001と27002と言えよう．今回の改訂では，ISMSの認証が，ISO9000，14000などと共通なフレームワークとなり，企業等の組織にとってより身近なツールとなる．本稿では，この20年間の動向を俯瞰して,改定の位置づけを明らかして,新しい規格の動向とISMSの将来像について紹介した．さらに，情報セキュリティマネジメントは，今後，運用面が拡充して別の管理体系となるなり，自動化して運用そのものが変わることを紹介した．

8. 謝辞

本研究を実施するにあたり，ISO/IEC SC27の会議に出席するために，2007年～2011年はISACA（情報システムコントロール協会），2012年はJISC（情報処理規格協会）から旅費を支援して頂きました．ここに感謝いたします．
また，本研究を実施するにあたり，アドバイスやコメントを頂いたISO/IEC SC27国内委員会の委員，情報セキュリティ大学院大学の教授，原田研究室の学生，客員研究員の皆様に感謝いたします．

9. 参考文献

[1] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements, 2005年
及びJIS Q27001:2006 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
[2] JIPDEC, 認証取得組織数推移，認証機関別・県別認証取得組織数，www.isms.jipdec.jp/lst/ind/suii.html，2014年1月アクセス
[3] CSA, Security, Trust & Assurance Registry (STAR), //cloudsecurityalliance.org/star/，2014年1月アクセス
[4] CSA, Cloud Controls Matrix v3.0, cloudsecurityalliance.org/download/cloud-controls-matrix-v3/, 2014年1月アクセス
[5] DTI, DISC PD0003, Code of practice for Information Security Management, DTI, 1993年9月
[6] BS7799-1, Code of practice for Information Security Management, 1997 年9月
[7] ISACA, CobiT(Control Objectives for IT) version 3, 2000年
[8] JIS X5080:2002 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の実践のための規範－，2002年（廃止）
[9]経済産業省，情報セキュリティ管理基準 （平成15年に経済産業省告示第112号として制定され, 平成20年に改正), www.meti.go.jp/policy/netsecurity/.../IS_Management_Standard.pdf，2014年1月アクセス
[10] 経済産業省，情報処理サービス業情報システム安全対策実施事業所認定基準（通商産業省告示 406 号），1997年制定，2001年廃止
[11] ISO/IEC 17799:2000, Code of practice for Information Security Management, 2000年
[12] BS7799-2, Information security management systems -- Requirements, 1997年
[13] ISO/IEC 27000:2012, Information security management systems - Overview and vocabulary
[14] ISO/IEC 27003:2010, Information security management system implementation guidance
[15] ISO/IEC 27004:2009, Information security management measurements
[16] ISO/IEC 27005:2011, Information security risk management
[17] ISO/IEC 27000:2014, Information security management systems - Overview and vocabulary
[18] ISO, Annex SL(normative) Proposals for management system standards, www.unit.org.uy/misc/AnexoSL.pdff，2014年1月アクセス
[19] ISO/TMB/TAG 対応国内委員会事務局,ISO マネジメントシステム規格の整合化に関して（ISO/TMB/TAG13-JTCG の動向）,2012 年 5 月，www.jsa.or.jp/stdz/mngment/PDF/mns_4.pdf, 2014年1月アクセス
[20] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements, 2013年
[21] ISO 31000:2009 - Risk management（JIS Q31000:2010 リスクマネジメント-原則及び指針），2009年
[22] ISO Guide 73 : 2009, Risk management-Vocabulary,（JIS Q0073：2010 (リスクマネジメント用語），2009年
[23] ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls, 2013年
[24] ISO/IEC SC27, SD3 Mapping Old?New Editions of ISO/IEC27001 and ISO/IEC27002, SC 27 N13143, 2013年10月，www.jtc1sc27.din.de/sixcms_upload/media/3031/SD3.pdf，2014年1月アクセス
[25] ISO/IEC 27014:2013 Information technology - Security

techniques - Governance of information security

10. 付録１

10.1 外部環境の変化

・球環境の変化→ITによるモニタリングシステム
・自然災害の増加→気象のIT情報の重要性
・グローバル化（経済，取引，流通，旅行，情報，・・・）
・企業へのITの普及（全企業の99%がPCを活用）
・テロの頻発→テロリストもITを利用
・中国，インド，ロシア，ブラジル，南アフリカなどの経済発展→携帯電話やインターネットを利用
・EUの拡大（27カ国）

10.2 技術の変化→IT の進歩が重要

・クラウド
・スマートフォン
・検索サービスの一般
・電子ショッピングの拡大楽天，Amazon
・放送のデジタル化
・写真のデジタル
・個人の無線LAN利用
・地球人口の半数以上が携帯電話を利用
・SNSの広がり
・高速大容量ブロードバンド
・組み込みコンピュータの広がり
・車の自動運転
・スマートグリッド
・スマートメータ
・電子マネーの拡大
・入退出管理システムの普及
・監視カメラのデジタル化と普及

10.3 関連法令・制度の変化　→IT，ネットワークへの対応

・個人情報保護法完全施行（2005）
・金融商品取引法の内部統制報告書制度（2007）
・特定電子メールの送信の適正化等に関する法律（2008）
・不正競争防止法の改正（2011）
・不正アクセス禁止法の改正（2012）
・不正指令電磁的記録：ウィルス作成罪（2011）
・著作権法改正（2012）
・プロバイダ責任制限法（2007）
・情報セキュリティガバナンス制度（2005-2010）
・情報セキュリティ監査制度（2004）

10.4 事件・事故

機密性（個人情報漏えい）
個人情報漏えい事故多発（JNSA・IISECのインシデント調査）
Winny利用ＰＣのウイルス(ワーム)（2005）
ボーダーレス（Sony個人情報流出（2011年））
米復員軍事省の管理する退役軍人の約2,000万件の個人情報漏えい（2006）
・自衛隊のイージス艦機密情報内部漏えい事件(2007)
・小規模な情報漏洩えいについては増加傾向にある（JNSAと情報セキュリティ大学院大学によるインシデント調査）

10.5 可用性・完全性

・全日空の発券システムで障害(2007)
・ファーストサーバの障害とデータ消失(2012)
・みずほ銀行システム障害（2011）
・Gumblerウイルスによる改ざん被害（2009）
・東京証券取引所システム障害（2005）
・311東日本大震災に伴う情報システムへの被害（2011）

10.6 その他

・食品偽装（2007）
・消えた年金記録問題(2007)
・Googleストリートビュー開始(2008)
・パンデミックが明らかにしたBCPの不備（2009）
・ウィキリークス（2010）
・イカタコウイルス作者　器物損壊容疑で逮捕（2010）
・尖閣諸島中国漁船衝突映像流出(2010)
・大阪地検特捜部証拠改竄事件(2010)
・アノニマス（2011）

11. 付録２　ISO/IEC27000 ファミリー規格

標準	英語名称	標準	実施年	概要	日本基準
ISO/IEC27000	Information technology – Security techniques – Information security management systems – Overview and vocabulary	標準あり	IS 2014	情報セキュリティ管理に関する用語集	JIS Q27000
ISO/IEC27001	Information technology – Security techniques – Information security management systems – Requirements	標準あり	IS 2013	情報セキュリティ管理の要求条件 ISMS認証基準	JIS Q27001
ISO/IEC27002	Information technology – Security techniques – Code of practice for information security management	標準あり	IS 2013	情報セキュリティ管理の技術管理項目	JIS Q27002
ISO/IEC27003	Information technology – Security techniques – Information security management system implementation guidance	標準あり 改訂開始	WD 2016	情報セキュリティの実装方法	
ISO/IEC27004	Information technology – Security techniques – Information security management measurements	標準あり 改訂開始	WD 2016	情報セキュリティ管理のための測定方法	
ISO/IEC27005	Information technology – Security techniques – Guidelines for information security risk management	標準あり 改訂開始	WD 2016	情報セキュリティ分野のリスク管理	未定
ISO/IEC27006	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	標準あり 改定中	IS 2011	ISMSの認証機関に対する要求条件	JIS Q27006
ISO/IEC27007	Information technology – Security techniques – Guidelines for information security management systems auditing	標準あり	IS 2011	情報セキュリティ内部監査のガイドライン	
ISO/IEC TR27008	Information technology – Security techniques – Guidance for auditors on information security management systems controls	標準あり	TR 2011	情報セキュリティ監査の技術ガイドライン	
ISO/IEC27010	Information technology – Security techniques – Information security management for inter-sector communications	標準あり	IS 2012	産業間の情報セキュリティ管理	
ISO/IEC27011	Information technology – Security techniques – Information security management guidelines for telecommunications organisations based on ISO/IEC 27002	標準あり 改訂開始	WD 2016	情報通信事業者が27002を用いて情報セキュリティ管理を実施するためのガイドライン	
ISO/IEC27013	Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	標準あり	IS 2012	ISO/IEC20000-1と27001の両方の認証を統合的に受けるときのガイドライン	
ISO/IEC27014	Information technology – Security techniques – Governance of Information security	標準あり	IS 2013	情報セキュリティガバナンスのガイドライン	JIS Q27014
ISO/IEC27015	Information technology – Security techniques – Information security management system for financial and insurance services sector	標準あり	IS 2013	金融・証券業向けの情報セキュリティ管理システム	

標準	英語名称	標準	実施年	概要	日本基準
ISO/IEC TR27016	Information technology – Security techniques – Information security management – Organizational economics	標準あり	IS 2014	ISMSの経済性	
ISO/IEC27017	Information technology – Security techniques – Guidelines on ISMS for the use of cloud computing services	標準化作業中	CD 2015	情報セキュリティ管理の要求条件 ISMS-Cloud認証基準	
ISO/IEC27018	Information technology – Security techniques – Guidelines on ISMS for the use of cloud computing services	標準化作業中	WD 2016	情報セキュリティ管理の要求条件 ISMS-プライバシ認証基準	
ISO/IEC27009	The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications	標準化提案中	WD 2016?	ISMS認証における要求条件に付加的な基準を組み合わせるときの考え方	

(2013年末の状況)

12. 付録３　ISO/IEC 27001:2013 の目次

13. 付録４　ISO/IEC 27002:2013 の目次