最新のISOの動向について
Recent standardization of Information Security at ISO

原田要之助†
Yonosuke Harada†

†情報セキュリティ大学院大学　情報セキュリティ研究科
† Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

要旨

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．

キーワード

情報セキュリティ, 管理策, 情報セキュリティマネジメント, リスクマネジメント, ISO/IEC 31000：2008, ISO/IEC27001：2013，ISO/IEC27002：2013

1. はじめに

ISO/IEC27000 シリーズは, 2013 年に大きく改定された．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ことが背景にある（付録 1 参照）．とくに，IT 分野では，ハードウェアの性能向上，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ている[1].

情報セキュリティの認証制度は，2005 年に ISO/IEC27001:2005[1]を要求条件として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）が参照されており．情報セキュリティマネジメントの最も基本となっている．本稿では，2013 年に改定された ISO/IEC27000:2013，27001:2013，27002:2013*[2]の改定および，その後の 27003，27004，27005 の改訂の方向性について解説する．最後に，情報セキュリティマネジメントの変遷と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

＊[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

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．

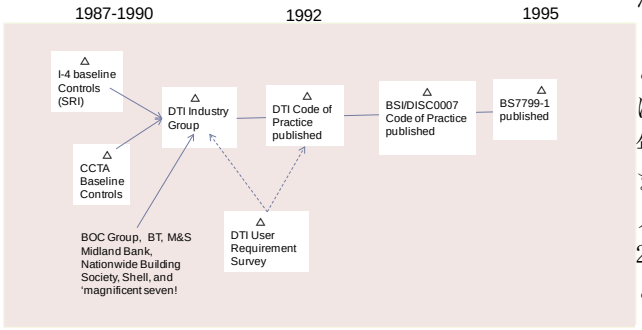

図 2-1 1995 年以前の情報セキュリティマネジメント

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．

一方，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した認証の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．

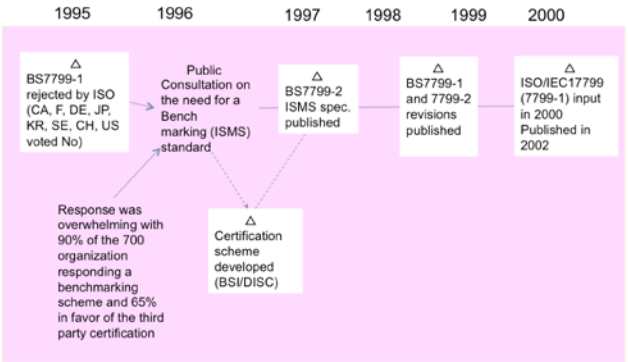

図 2-2 ISMS 黎明期の英国での情報セキュリティマネジメントの認証制度化

2.3 日本での情報セキュリティマネジメントと ISMS 認証制度

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.

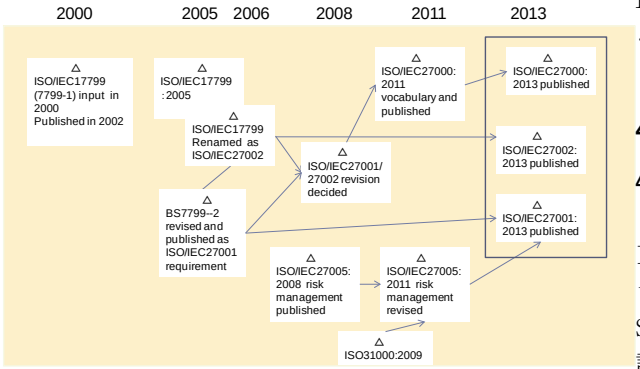

図 2-3 2000 年以降の国際規格としての発展

2005 年には, 日本や英国で ISMS 認証の順調な進展が見られることから, 国際的には ISMS の認証制度が広がると考えられるようになった. そこで, BS7799-1 が, ISO/IEC27001:2005 として国際規格として提案され, 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, 認証の番号体系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が差し替えられた).

3. ISO/IEC27000 のシリーズ規格

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. 規格の全体については, 付録 2 を参照のこと.

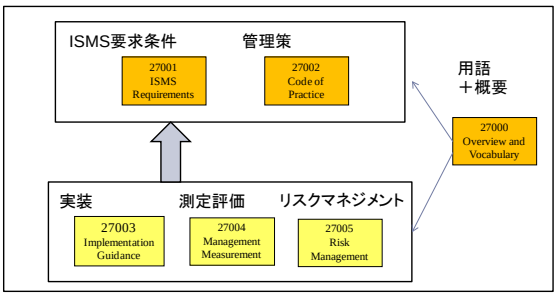

図 3-1 ISO/IEC27000 のファミリー規格について

現在の ISO/IEC27003, 27004, 27005 は ISO/IEC27001,27002:2005 と整合がとられており, ISO/IEC27001,2700:2013 とは整合しない. そのため, ISO/IEC SC27 で改定作業が実施されている. ISO/IEC27000:2014 (Overview and Vocabulary : 概要と用語) *3 [17] は, ISO/IEC27001:2013 年版との対応がとられている.

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 (共通性) 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 (以下, MSS共通要素という) [18]が採択された.

この一連のISO によるMSS共通用は2012年2月に発効され, 今後, ISOで開発, 制定, 改正される全てのマネジメントシステムは, 採用することが義務付けられた[19]*4. 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要求されるPDCAが中心となっている.

- (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 3-1 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 MSS 共通要素に追加されたリスク関連

*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.
*4 これらの 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.

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*5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．

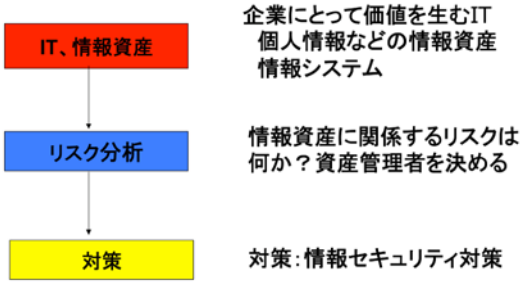

図 4-3 ISO/IEC27001:2005 でのリスク分析の考え方

ISO/IEC27001:2013[20]では，リスクマネジメントについては，ISO31000:2009 Risk Management[21]また，リスクの用語についてはISO Guide73:2009[22]に基づくことになった．一方，ISO31000では，リスクを「目的に対する不確かさの影響」と定義している．この定義だけでは，分かりにくいため，注記として，「リスクは，ある事象の結果とその発生の起こりやすさとの組み合わせとして表現されることが多い」及び，「リスクは，起こりうる事象，結果又はこれらの組合せについて述べることによって，その特徴を記述することが多い」と述べており，事象，結果を用いて説明している．さらに，リスク特定を，「リスクを発見，認識及び記述するプロセス」と定義しており，「リスク特定には，リスク源，事象，それらの原因及び起こりえる結果の特定が含まれる」と，リスク源*6，事象*7を用いて説明している．これを図示すると，図4-4のようになる．

図 4-4　ISO31000のリスクの考え方[21]，[22]

図4-4では，あるリスクを引き起こす可能性のあるリスク源（Risk Source）に対して，事象が不確かに発生して，影響の結果が起こることを示している．なお，ここでの結果は，当初の目的に対してプラスにもマイナスにもなる［22］．

ISO/IEC27001:2013 では，ISO31000に基づくとしているため，図4-3のように，最初に情報資産を特定することから始まらない．まず，リスク源としての情報そのものを想定して，この情報を脅かす事象（機密性，完全性，可用性を脅かすもの）がどのように影響するかを考えることになる．ISO31000の考えに基づくため，根本的にリスクに対する考え方を変えることになる．

1990年代から2008年頃までは，情報は無形物であり，物理的なメディア（紙，コンピュータ内部のメモリ，ハードディスク，通信ネットワークなど）に格納されている．この物理的なメディアには管理者が紐付いている．また，データオーナーでもある．このことから，情報そのものではなく，情報資産という有形物を対象とすることで，管理責任が明確となる．さらには，これらのメディアには，それぞれに脆弱性があり，この脆弱性に脅威が働き，リスクが生じるというよう概念で説明されてきた．

一方，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．また，ハードウェア，ソフトウェアは仮想化技術を多様化するようになった．そのため，物理的なメディアと情報を紐付けることが困難となり，資産管理者が自分の情報がどこにあるか不明となる場合も起きるようになった．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，自分の直接の管理下に保護しなければならない情報が物理的にないため，管理責任をとれない．そこで，ISO/IEC27001:2013では，情報に対するリスクを管理する責任者を決めて，管理責任を果たせるように変更された．これを図4-5に示す．

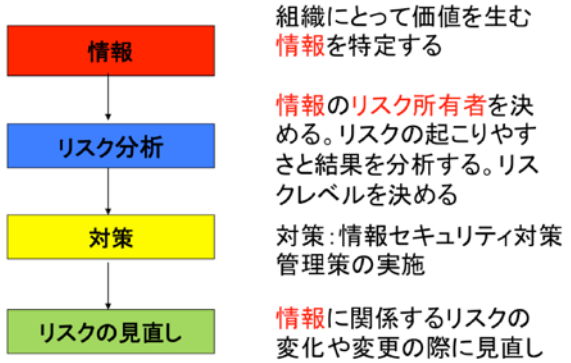

図 4-5 ISO/IEC27001:2013 でのリスク分析の考え方

*5 英語では，資産（asset），日本語では情報資産とされている．
*6 それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素（無形の場合もある）
*7 ある一連の周辺状況の出現又は変化

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，以下のように具体的なプロセスが述べられている．

c) 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) 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) 情報セキュリティリスクを評価する．

図 4-6 新しいリスク分析の考え方*8

ここでの問題点は，リスク分析については，今までの情報セキュリティで用いられてきた，「脆弱性に脅威が働いて，リスクが発生する」という概念が拡張されたとしている点である．一見，リスク源にはリスクになりうるものが全て含まれているように見えるが，ソフトウェアの脆弱性のように，存在が分かっているものの，発見されていないものと，脆弱性が分かっていないものを同等に扱うことになる．

多くの企業では，ISO/IEC27001:2005に基づいて，情報資産をベースに図4-3のプロセスで情報セキュリティマネジメントが実施されている．リスク分析においては，一般的には，情報資産の価値×脆弱性×脅威のレベルをリスクとして評価する（詳細リスク分析の場合）ことが多い．

しかし，図4-5のリスク源については，脆弱性と脅威を分けないため，脆弱性が問題なのか，脅威が問題なのかが明確にならないため，ISMSなどを既に実施している主体にとっては，移行が難しいかもしれない．なお，佐藤らは，ISO31000の考え方を用いた情報セキュリティのインシデントについて類型化を行っており，リスク対策が可能としている[27]．したがって，ISO31000をベースにする図4-5の場合も，具体的な実施方法などの事例の蓄積で解決するかもしれない．

ISO/IEC27001:2013に移行するにあたっては，次のような経過措置を講じながら，段階的に進めることになると考えられる．

まず，今までの情報資産を洗い出して，物理的に管理できる情報資産の場合については，資産管理者がリスク所有者と考えられる．一方，クラウドなど情報資産がどこに存在するのか不明な場合や資産管理者を特定できない場合には，情報のデータオーナーをリスク所有者とする．これは，リスクが起きたときに，責任をとる主体になるからである．このように，情報資産の管理の実態をベースに実務的なリスク分析を実施するのがよいのではないか．

なお，ISO/IEC27001:2013は，MSSをベースにして，必要最小限の項目を追加しているだけであり，これだけでは十分なリスク分析や対応ができないという声があり，現在，ISO/ IEC27005がISO/IEC27000シリーズのリスク分析の規格として改訂が検討されている．ISO/ IEC27005:2011はISO31000に準拠しているが，リスク所有者についての言及はない．また，ISO31000をベースに，リスク特定→リスク分析→リスク評価→リスク対策のプロセスについては言及されているものの，リスクコミュニケーションと協議やモニタリング及びレビューについては言及されていない．また，脆弱性，脅威との関係についても述べられていない．そのため，ISO/ IEC27005の早期の改訂が望まれる．なお，リスク所有者をベースにすると新しいリスクについての分析が可能となる．例えば，TNOでは，リスクをリスク所有者のネットワークと考える．すなわち，外部からのリスクと内部からのリスクに分けて整理している．今までのリスクでは，ownerという概念がなかったため，リスクをネットワークでとらえることはなかった．今後，リスクについて新しい観点からの研究がなされることを期待したい．

5. ISO/IEC27002 の改定について

5.1 情報セキュリティ管理策の変遷

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[26]

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

*8 ISO/IEC27001:2013[20]の 6.1.4 章より抜粋，図では原書と同じ章番号を採用している

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．これは，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

ISO/IEC27001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[26].

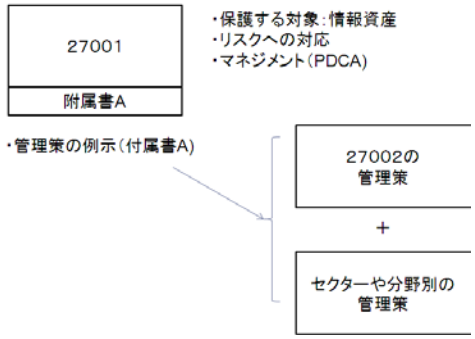

図5-1　ISO/IEC27001付属書AとISO/IEC27002の管理策の関係

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．具体的には，27002の5章以降の章と対応する．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，ISO/IEC27002:2005のタイトルは，「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．すなわち，2005年版では単独で情報セキュリティマネジメントを遂行できるが，2013年版では管理策のみとなった．すなわち，2013年版は，単独では情報セキュリティマネジメントができないことに注意する必要がある[26].

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．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]

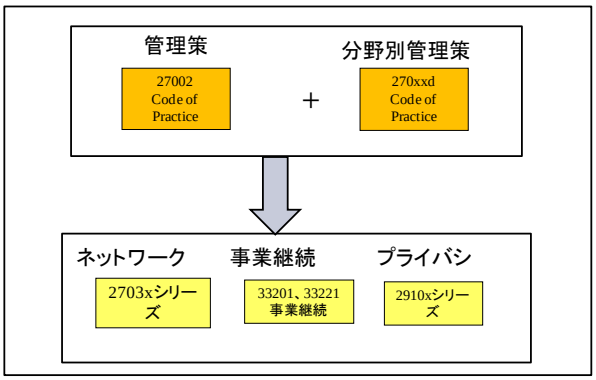

図5-3　管理策と他のガイドラインの関係[26]

5.4　管理策の変更について

管理策については，内容が全面的に見直されて，133の管理策が114に削減されている．

管理策の変更については，以下の3つのパターンに分けられる．①新しく管理策が追加されたもの，②既存の管理策が見直されて更新されたもの，③管理策が廃止や削除されたものがある．以下に述べる．

① 新しく管理策が追加されたもの

新しいリスクを想定した管理策なので，組織にとってはリスク分析をして，自組織にリスクが関連しないか検討することが求められる．とくに，リスクが自組織に強く関連する場合には，リスクの重大性を考慮して管理策の追加などが必要となる．

例えば，暗号の管理策は10章として独立した．これは，暗号がより広く組織で利用されるようになっており，開発の章だけで取り扱うと，運用面での管理がおろそかになるという懸念から，独立させたものである．

② 既存の管理策が見直されて更新されたもの

見直されたもののなかには，管理策の移動・拡充，他の規格との関係で既存の管理策を見直したものなどがある．

(1) 管理策の移動，拡充

例えば，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ている(図5-2参照)．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．これは，組織とってモバイルのリスク管理が重要となっているとの規格策定の立場からのメッセージでもあるので，組織という観点から，管理策を考えるべきであろう．

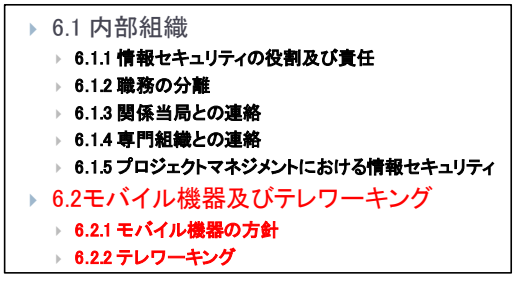

図5-2　ISO/IEC27002:2013の組織について

同様に，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．これは，多くの組織で，ITを利用するケースが広がったため，組織のメンバーとしてのIDとビジネスで利用する情報へのアクセス権限を分けるものであり，既存の中規模以上の組織では広く実施されている管理策である．

③ 管理策の廃止や削除

(1) 管理策が他の項目に吸収された場合

ネットワーク分野のようにシステム化されたものは，新たなシステムの管理が必要となる．また，他の管理策と統合される場合には，統合される管理策の対象範囲が広がるため，管理策の統合について，対象となるリスクの分析が求められることもあるので，注意が必要となる．インシデント管理では，既に，ISO/IEC27035が制定されて利用されている．そこで，ISO/IEC27002:2005では，内容を整合させて情報セキュリティ管理として必須の部分のみを述べている．したがって，実際の組織においては，インシデントを管理するチームと全体の情報セキュリティマネジメントを実施する担当で十分に話し合って，管理業務と管理策の実施を分担することが求められている．今後，ネットワークセキュリティではISO/IEC27033シリーズが拡充される．また，サプライチェーン管理では，ISO/IEC27036シリーズ，デジタルフォレンジクスでは，ISO/IEC27040シリーズが開発されているので，この動向に注意して無駄な管理策のバッティングを避けていくことが必要となる．

(2) 管理策が他の規格を参照している場合

例えば，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．

(3) 管理策がなくなり，実践の手引きに移った場合

例えば，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で管理策としては，不要となったものは実施の手引きに管理策を移している．これには，「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」などがある．

規格の管理策でなくなったかたといって，管理対象外にするのはリスクを招く可能性がある．実施の手引きに残っている限りにおいては，自組織のリスクを見ながら管理策として継続するか検討することが求められる．

新しい概念や用語の整理

ISO/IEC27002：2013では以下の新しい概念を取り入れている．

① 関係者の整理

今まで，情報セキュリティ管理の関係者としては，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っていた．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．この結果，管理対象が明確になり，曖昧さが解消された．

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．

６ まとめ

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，ISMSによる認証制度も大きく成長してきている．また，ITの技術進歩やマネジメントシステムの進化のおかげで，管理方法も大きく変遷している．とくに，当初から組み入れられてきた事業継続計画については，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．

とくに，2005年からの変化で大きいのは，モバイルコンピューティングとクラウドであろう．これへの対応で，27001では，情報資産管理者からリスク所有者へと管理の主体が変わった．また，モバイルの利用が組織の問題となり，管理がじゅうようとなっている．現在は，モバイルの端末や情報を管理するために， 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．一方， MDM自体の管理が新しい情報セキュリティマネジメントの課題となっている．物理セキュリティ分野では，多くの組織において，入退室管理のシステム化が進み，入退室管理が簡単になった分，システムの脆弱性やシステムで利用するIDカードの管理などの運用面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，人が対応するためのポリシの策定，使い方のルール化，しくみの定常化という段階で進む．新しく導入されたしくみについては，影響する範囲が大きい場合やリスクが大きい場合には，自動化されてシステムが導入されることが多い．一方，システムで自動化された場合には，当該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，しくみに対する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．

国際規格は上記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．管理策などが時間遅れで変更されるため，組織においては，管理面で二重手間になったりするケースもでてきている．これらの課題について今後，規格をどのタイミングで何をどう変更するかについて検討する必要がある．

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．

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 5 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
[26] 原田要之助, 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, 情報処理学会研究報告 IPSJ SIG Technical Report，Vol. 2014-EIP-63 No.10 2014年2月
[27] 佐藤亮太，間形文彦，高橋克也，桑名栄二，**情報セキュリティの失敗事例における原因の類型化とその対策に関する考察**，情報処理学会論文誌 54(9)，2208-2219，2013年6月

付録 1 [26]より

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）

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

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）

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）

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）

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）

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)