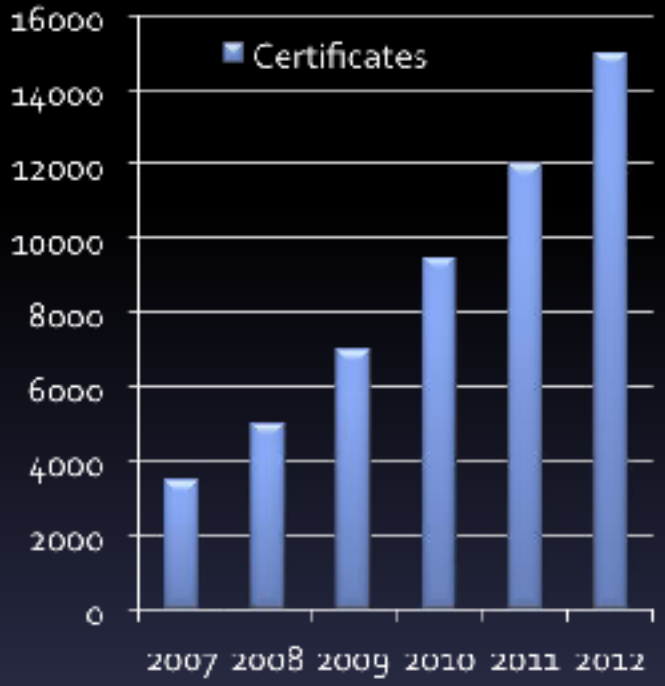
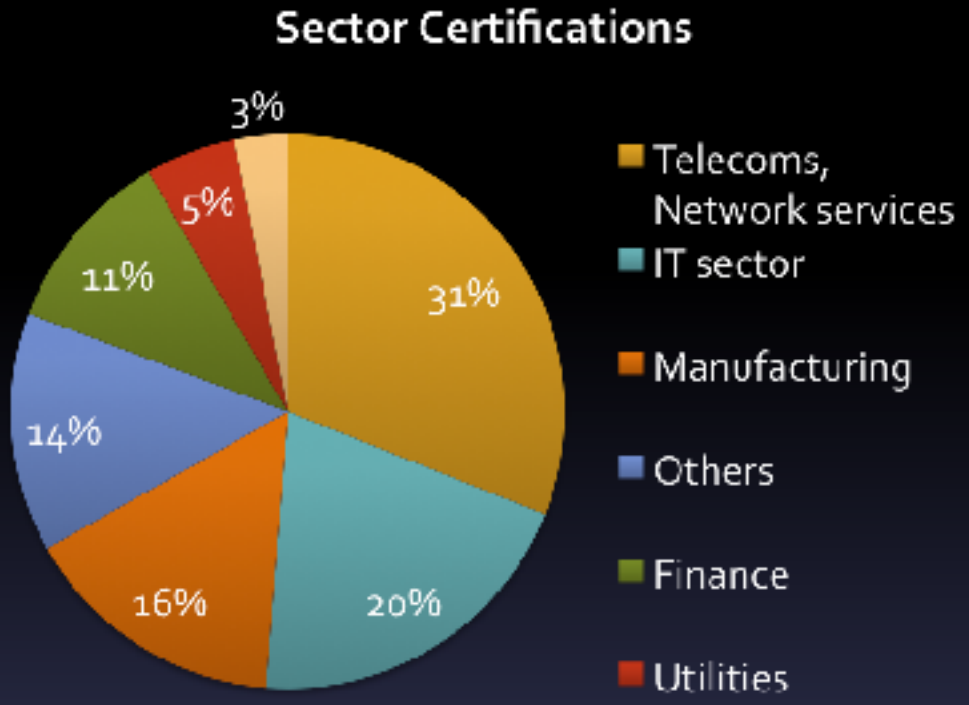
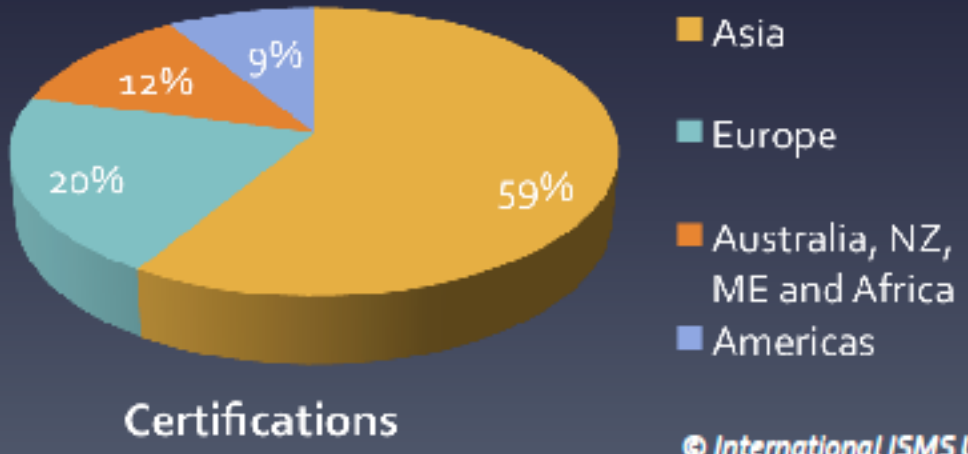
ISO/IEC27001&27002の改版の概要と最新情報

中尾　康二
KDDI株式会社　情報セキュリティフェロー
情報通信研究機構　主管研究員/研究統括

ISO/IEC 27001 ISMS Certifications







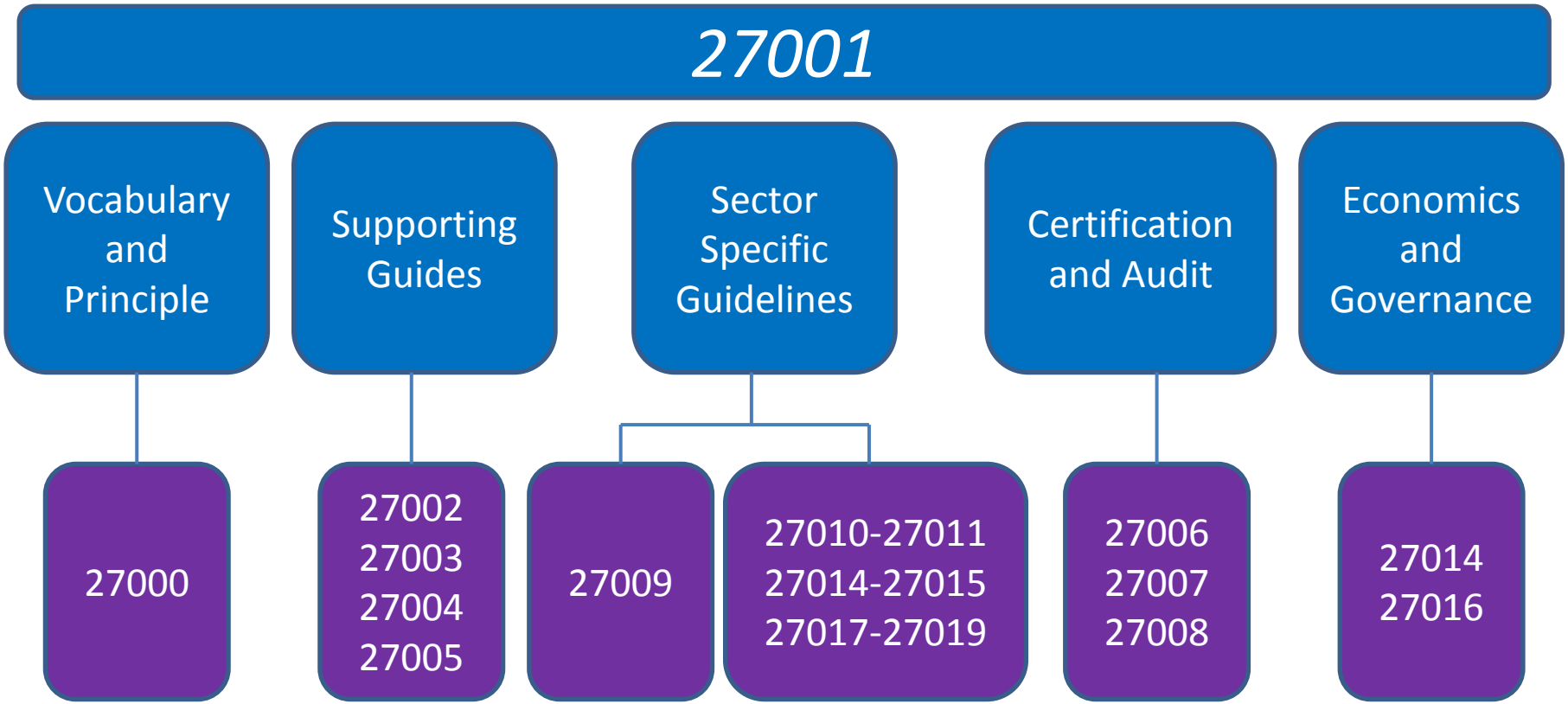
引用：SC27ワークショップ（韓国：2013）

各国のISMS認証取得登録発行数

出典：http://www.iso27001certificates.com/
2012年11月現在

日本	4152	オーストラリア	30	カナダ	10	ジャージー	2
英国	573	シンガポール	29	ノルウェー	10	カザフスタン	2
インド	546	クロアチア	27	スウェーデン	10	ルクセンブルク	2
台湾	461	スロベニア	26	スイス	9	マケドニア	2
中国	393	メキシコ	25	バーレーン	8	マルタ	2
ドイツ	228	スロバキア	25	ペルー	7	モーリシャス	2
チェコ共和国	112	ブラジル	24	チリ	5	ウクライナ	2
韓国	107	オランダ	24	エジプト	5	アルメニア	1
米国	105	サウジアラビア	24	オマーン	5	バングラディシュ	1
イタリア	82	アラブ首長国連邦	19	カタール	5	ベラルーシュ	1
スペイン	72	ブルガリア	18	スリランカ	5	ボリビア	1
ハンガリー	71	イラン	18	南アフリカ共和国	5	デンマーク	1
マレーシア	66	ポルトガル	18	ドミニカ共和国	4	エストニア	1
ポーランド	61	アルゼンチン	17	モロッコ	4	キルギスタン	1
タイ	59	フィリピン	16	ベルギー	3	レバノン	1
ギリシャ	50	インドネシア	15	ジブラルタル	3	モルドバ	1
アイルランド	48	パキスタン	15	リトアニア	3	ニュージーランド	1
オーストリア	42	コロンビア	14	マカオ	3	スーダン	1
トルコ	35	ロシア連邦	14	アルバニア	3	ウルグアイ	1
トルコ	35	ベトナム	14	ボスニア・ヘルツェゴビナ	2	イエメン	1
フランス	34	アイスランド	13	キプロス	2		
香港	32	クウェート	11	エクアドル	2	**Total**	**7940**

27001 Family



今後： Certification of ISM Professionals (ISO/IEC 27021)

27001 Family- サポートガイドライン

ISO/IEC 27002 (2013)	Code of Practice for Information Security Controls
ISO/IEC 27003 (2010)	Information Security Management System- Implementation Guidance
ISO/IEC 27004 (2009)	Information Security Management System- Measurements
ISO/IEC 27005 (2011)	Information Security Risk Management

現在、これらの改訂が開始されている。27001に規格化されている要求事項の実装、支援、ガイドなどのために。

27001 Family-セクター用ガイド

ISO/IEC 27009 策定中	The Use and Application of ISO/IEC 27001 for Sector/Service-Specific third party accredited Certifications
ISO/IEC 27010 (2012)	Information Security Management for inter-sector and inter-organizational communications
ISO/IEC 27011 (2008)	Information Security Management for telecommunications
ISO/IEC 27013 (2012)	Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

27001 Family-セクター用ガイド(2)

ISO/IEC 27015 (2012)	Information Security Management Guidelines for Financial Services
ISO/IEC 27017 策定中	Code of Practice for Cloud Security Control based on ISO/IEC 27002
ISO/IEC 27018 策定中	Code of Practice for PII Protection in Public Cloud acting as PII Processors
ISO/IEC 27019 (2013)	Information Security Management Guidelines based on ISO/IEC 27002 for process control system specific to the Energy Utility Industry

注：ISO/IEC 27018の策定は、SC27/WG5で進められている。

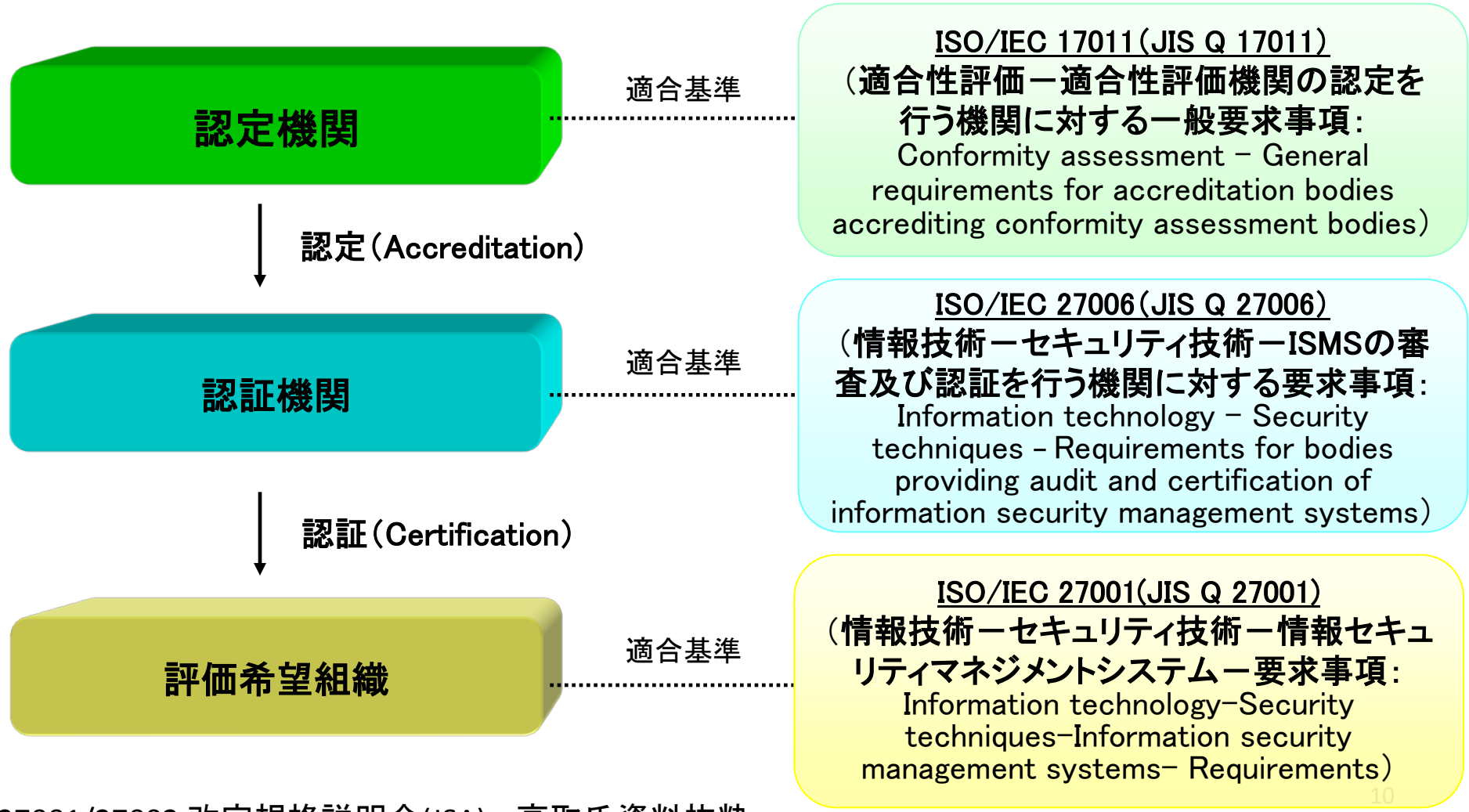
27001 Family-ガバナンス、エコノミクス

ISO/IEC 27000 (2013)	**Information Security Management Systems – Overview and Vocabulary**
ISO/IEC 27015 (2013)	**Governance of Information Security**
ISO/IEC 27016 (2013)	**Information Security Management – Organizational Economics**

27001 Family-認証・監査の規格

ISO/IEC 27006 (2011)	Requirements for Bodies providing Audit or Certification of Information Security Management Systems
ISO/IEC 27007 (2011)	Guidelines for Information Security Management Systems Auditing
ISO/IEC 27008 (2011)	Guidelines for Auditors on ISMS Controls

ISMS適合性評価制度における適合基準



27001/27002 改定規格説明会(JSA)　高取氏資料抜粋

27001 Familyにおける重要規格
2013年に改定完了（ほぼ同時）

ISO/IEC 27000　(11月、2013年）

27001ファミリー全体概要と用語

ISO/IEC 27001　(10月1日、2013年）

ISO/IEC 27002　(10月1日、2013年）

27001 Family
ISO/IEC 27000　について

１）DISから直接IS（国際規格）に昇格
　（NBからの反対がなかったため）

２）国際規格では、

Information technology-Security techniques-Information security management systems-Overview and vocabulary

３）JIS化作業におけるJIS Q27000では、

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－~~概要及び~~用語

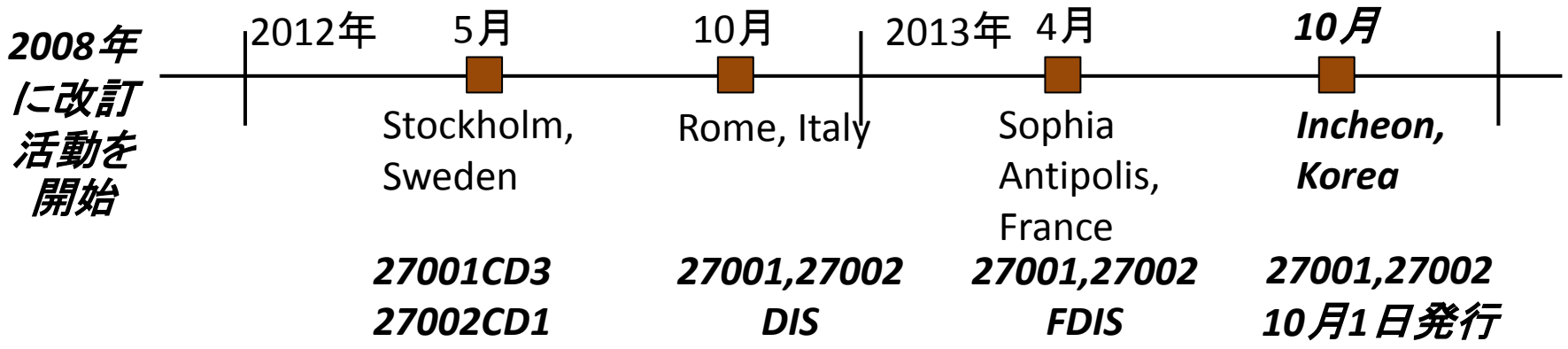
４）Future version development of ISO/IEC 27000の検討がすでに開始されている。

ISO/IEC 27001改定の概要

ISO/IEC 27001, 27002の審議経過

SC27meetingの審議の概要

- 年２回の開催
- WG1～WG5 of SC27
- 50+ヵ国、150+人程度の参加
- 会議ではEditing meeting
  - ✓ 各国より提出されたコメントによる編集会議
  - ✓ 会議後は、編集会議の結果のまとめ(Resolutions）と新しいTextが配布



27001/27002 改定規格説明会(JSA)　山崎氏資料抜粋

I. ISO/IEC 27001 改正の特徴

1. ISMSの要求事項を定める標準であり、ISMS認証基準として使われる点で、2005年版を継承している。（ISO/IEC 27001:2013の1. Scopeを参照）

2. 本規格をとりまく2005年以後の動向に対応している。
   (1) マネジメントシステム規格の共通化の適用
   (2) 新しいビジネス環境及びシステム環境への対応

1. ISO/IEC 27001:2013の”Scope”：

- 2005年版の継承 -

- **“1. Scope” の字句は一部異なるが、主旨は2005年版とほぼ同等**

  （抜粋）:
  This International Standard specifies the requirements for ***establishing, implementing, maintaining and continually improving*** an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

  ・・・・・・

  この規格は，組織の状況の下で，ISMS を*確立し，実施し，維持し，継続的に改善する*ための要求事項 について規定する。この規格は，組織のニーズに応じて調整した情報セキュリティのリスクアセスメント 及びリスク対応を行うための要求事項についても規定する。

  ・・・・・・

➔ **要求事項を規定しているのであって、実施する順序を意味していない**

（注）27001:2005 establishing, implementing, operating, monitoring, reviewing, maintain and improving

2. 本規格を取り巻く2005年以降の動向への対応
(1)マネジメントシステム規格の共通化の適用

① ISOのマネジメントシステム規格（以降MSSと言う）

- 品質： ISO 9001:2008
- 環境： ISO 14001:2004
- 情報セキュリティ： ISO/IEC 27001:2005
- ITサービス： ISO/IEC 20000-1
- 事業継続： ISO 22301:2012　　等

② 共通化の目的

- 組織が複数のマネジメントシステムを導入することを考慮して、マネジメントシステム間の整合性向上を図り、組織の負担を軽減する。

（注）それぞれのマネジメントシステム規格は、今後も独立して存在する。

(1)マネジメントシステム規格の共通化の適用

③ 共通化の方法

- 新たに開発あるいは改正するマネジメントシステム規格に対して、***上位構造、共通テキストと共通用語定義***の使用を義務付け。
- このための***上位構造、共通テキストと共通用語定義***を下記文書で規定している。
  ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, Third edition, 2012
  - ***Annex SL*** (Normative) Proposals for management system standards
    - Appendix 2 (normative) High level structure, identical core text and common terms and core definitions for use in Management Systems Standards
- 27001:2013でこの***上位構造、共通テキストと共通用語定義***を適用している。

(1)マネジメントシステム規格の共通化の適用

- ***上位構造***は共通の目次であり、このレベルでは、ISMSの色が見えない。

ISO/IEC 27001:2005
0 序文
1 適用範囲
2 引用規格
3 用語及び定義
4 情報セキュリティマネジメントシステム
5 経営陣の責任
6 ISMS内部監査
7 ISMSのマネジメントレビュー
8 ISMSの改善
附属書 A（規定）管理目的及び管理策

ISO/IEC 27001
0 序文
1 適用範囲
2 引用規格
3 用語及び定義
4 組織の状況
5 リーダーシップ
6 計画
7 支援
8 運用
9 パフォーマンス評価
10 改善
附属書 A（規定）管理目的及び管理策

27001/27002 改定規格説明会(JSA)　山崎氏資料抜粋

MSSの要求事項の例

- ***共通テキスト***に対して、XXXを「情報セキュリティ」に置き換え、「情報セキュリティ固有の内容のテキスト」を変更・追加する。

4. 組織の状況

4.1 組織及びその状況の理解

4.2 利害関係者のリーズ及び期待の理解

4.3 **情報セキュリティ**マネジメントシステムの適用範囲の決定

組織は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない。

a) 4.1 に規定する外部及び内部の課題

b) 4.2 に規定する要求事項

c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

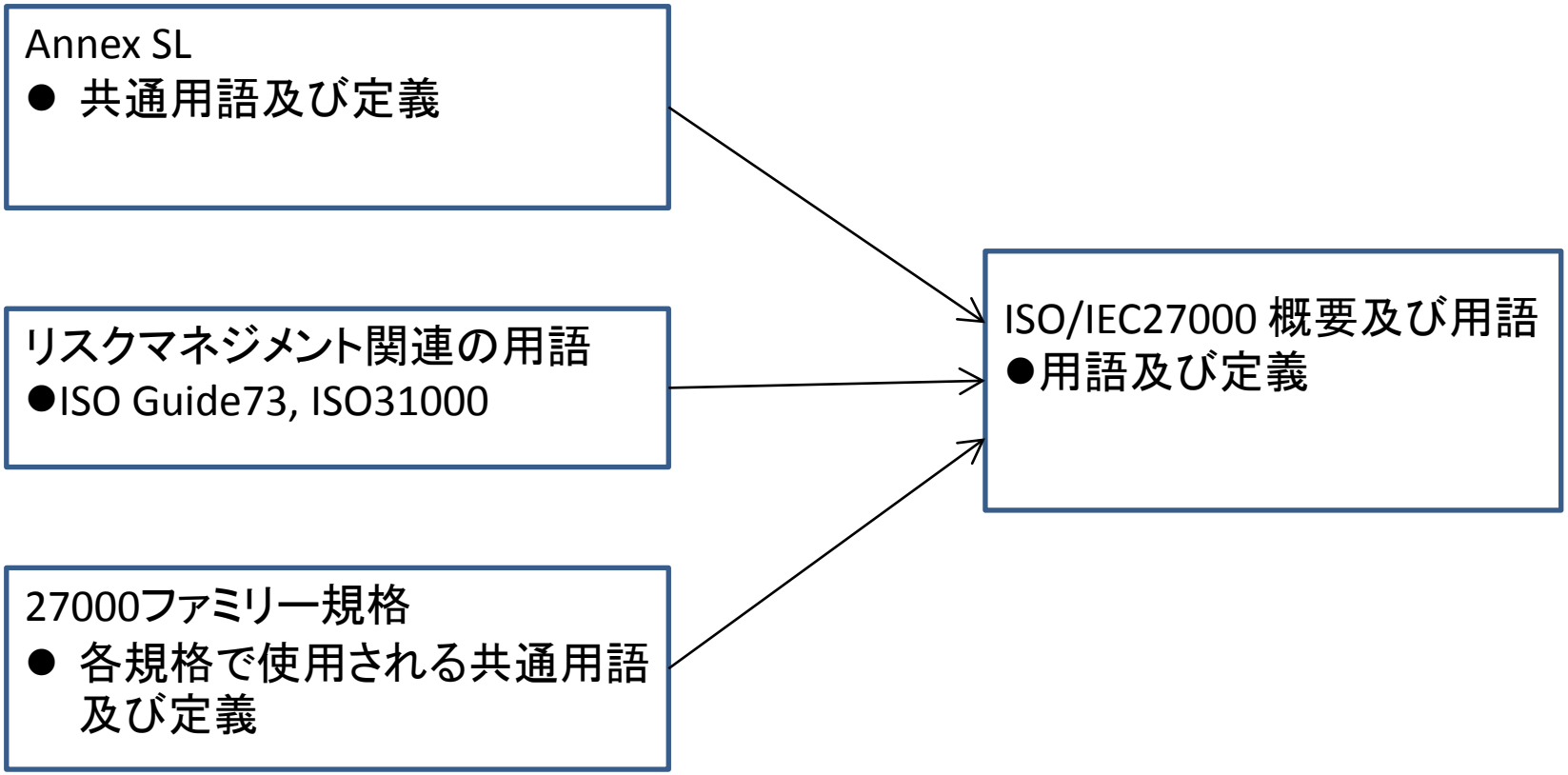
ISMS の適用範囲は，文書化した情報として利用可能な状態にしておかなければならない。

XXXを情報セキュリティに置き換え

共通テキストに追加したテキスト

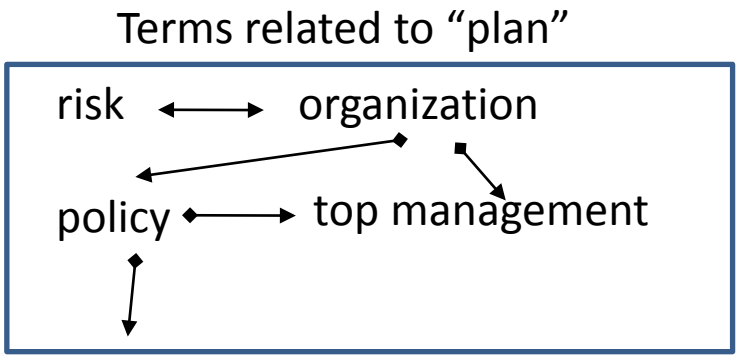
(1) マネジメントシステム規格の共通化の適用（共通用語の設定）

- ***共通用語定義***と、ISO/IEC27000 family of standardsの用語との関係



(1) マネジメントシステム規格の共通化の適用（共通用語の設定）

- ***共通用語定義***の設定と各マネジメントシステムとの関係
  ISOのマネジメントシステム規格全体（例えば、ISMS, QMS, EMS）で共通に使用する用語と定義を設定
  - 計画に関連する用語
    - organization
    - risk
    - objective
    - policy
    - top management
  - 運用に関連する用語
    - process
    - outsource
  - パフォーマンス評価に関連する用語
    - measurement
    - audit
  - 改善に関連する用語
    - corrective action



Concept diagram

(2)新しいビジネス環境及びシステム環境への対応（主要な変更点）

① リスクマネジメントの規格 ISO 31000への対応

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

② 組織の方針を明確にする情報セキュリティ目的の導入

➔箇条5.1 リーダーシップ及びコミットメント
➔箇条5.2 方針
➔箇条6.2 情報セキュリティ目的及びそれを達成するための計画策定
➔箇条8.1 情報セキュリティ目的を達成するための計画の実施
➔箇条9.3 マネジメントレビューで情報セキュリティ目的の達成を含む情報セキュリティパフォーマンスに関するフィードバック

③ 分野別のISMSを確立するための2005年版の拡張

➔箇条6.1.3 情報セキュリティリスク対応

ISO/IEC27001改正の詳細

WG1 SD3の発行

SC27/WG1 Resolutions（2013年10月仁川会議）

Resolution 14:Document for Publication

ISO/IEC JTC1/SC27/WG1 instructs the SC27 Secretariat to take the necessary action to publish the revised Text of ***WG1 SD3 – Mapping Old --to-New Editions of ISO/IEC 27001 and ISO/IEC 27002*** contained within SC27 N13143 as a **freely available document** on the SC 27 and other appropriate websites.

注記1.
WG1 SD3 was published on 25th October, 2013, and this document is also freely accessible from the public SC 27 web site at: http://www.jtc1sc27.din.de/sbe/wg1sd3

WG1/SD3の例
「4. 組織の状況(Context of the organization)」

ISO/IEC 27001:2013	ISO/IEC 27001:2005
4.1Understanding the organization and its context	8.3 Preventive action
4.2 a) Understanding the needs and expectations of interested parties	***New requirement***
4.2 b) Understanding the needs and expectations of interested parties	5.2.1 c) Provision of resources 7.3 c) 4) Review output 7.3 c) 5) Review output
4.3 Determining the scope of the information security management system	4.2.1 a) Establish the ISMS
4.3 a) Determining the scope of the information security management system	4.2.1 a) Establish the ISMS 4.2.3 f) Monitor and review the ISMS
4.3 b) Determining the scope of the information security management system	4.2.3 f) Monitor and review the ISMS
4.3 c) Determining the scope of the information security management system	***New requirement***
4.3 Determining the scope of the information security management system – Last sentence	4.3.1 b) General 4.3.2 f) Control of documents
4.4 Information security management system	4.1 General requirements 5.2.1 a) Provision of resources

「0. 序文」

- 2006年版の箇条0　序文:「プロセスアプローチ」と「PDCAモデル」が削除された。

「プロセスアプローチ」と「PDCAモデル」いう概念が無くなったのではなく、MSS（付属書SL）のSL.5.2の「MSS(Management System Standard)_マネジメントシステム規格」の定義に、「組織が特定の目的を達成するために方針、プロセス及び手順を策定し、それらを体系的に管理するための要求事項又は指針を提供する規格」とあり、その注記1に「有効なマネジメントシステムは、通常、意図した成果を達成するために”Plan-Do-Check-Act”のアプローチを用いた組織のプロセスを管理(managing)することに基づく。」と記述されている。

解説

MSSの標準として、プロセスアプローチや、PDCAモデルは、27001を使用した組織が、自組織のマネジメントシステムを構築する時に、組織のプロセスのベースに採用すればよいという考えで、規格の要求事項としては削除されたものである。

「0. 序文」

- ISO/IEC 27001:2013の「箇条0. 序文、0.1 概要」におけるISMSに関する重要な記述

① この規格は，***情報セキュリティマネジメントシステム（以下，ISMS という。）を確立し，実施し，維持 し，継続的に改善するための要求事項***を提供する。
② ISMS は，***リスクマネジメントプロセスを適用すること***によって情報の機密性，完全性及び可用性を保護し，かつ，リスクを適切に管理しているという信頼を利害関係者に与える。
③ この規格で示す要求事項の順序は，***重要性を反映するものでもなく，実施する順序を示すものでもない***。本文中の細別符号［例えば，a)，b)，又は 1)，2)］は，参照目的のためだけに付記されている。

解説

ISO/IEC 27001:2013では、「ISMSの要求事項を提供するものであり、ISMSを確立し、実施し、維持し、継続的に改善するための手順を示すガイドラインではない。」ことを強調しており、要求事項のみを記述するように意図して規格化している。

「4. 組織の状況(Context of the organization)」-1

4.1　組織及びその状況の理解：(新規)

ISMSを確立，実施，維持及び継続的改善をしようとする組織は、組織を取り巻く状況を理解する一つとして、ISMS外部及び内部の課題を決定することが要求される。それらの課題とは、2005年版のPDCAサイクルの図に描かれた「利害関係者の情報セキュリティの要求及び期待」を含み、ISMSの構築に影響を与える事項である。

これらの課題を明確にするには、組織の行なう事業の内部環境と外部環境を洗い出し、それらの関係を明らかにする必要がある。

4.2　利害関係者のニーズ及び期待の理解：(4.2 a)は新規、それ以外は改訂)

4.1に関連し、利害関係者の特定とその期待・要求事項を明確にすることが求められる。利害関係者とは、組織の情報セキュリティによって影響を受けるか、組織の情報セキュリティに影響与えるかの何れかの関係者である。

解説

4.1、4.2とも新しい要求事項である。有効なISMSを構築するには、自組織を知り（組織の状況の理解）、相手（利害関係者）を知る（ニーズ及び期待）事が重要である。新しい要求事項は、物事を進める基本を要求している。ISO31000に詳細な記述がある。

「4. 組織の状況(Context of the organization)」-2

4.3 情報セキュリティマネジメントシステムの適用範囲の決定：（4.3 c)は新規、それ以外は改訂）

2005年版の要求事項である「適用範囲からの除外について、その詳細及びそれが正当である理由」が、「適用可能性の決定」の要求（MSS）に変更となった。但し、ISMSとして追加した考慮事項として、「c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係」によって、適切な適用範囲について、適用範囲からの除外も含めて検討することが求められていると考えてよい。

4.4 情報セキュリティマネジメントシステム：(改訂）

「この規格の要求事項に従って、ISMSを確立し，実施し，維持し，継続的に改善」することが求められている。2005年版では、規格要求項目の構成自体がPDCAサイクルを要求していたが、2013年版ではMSSとして共通化された要求事項の構成にはそのような配慮はなされていない。組織は、自分の判断で規格の要求事項を取り入れたマネジメントプロセスを作ることが求められる。

解説

4.3の適用範囲は、4.1と4.2を考慮した上で、組織のISMS適用範囲を決める必要がある。言い換えると、適用範囲は、「組織の状況」を満足することが、要求されている。4.4は、新規の要求事項ではないが、本規格への適合性を求めている部分である。

「5. リーダーシップ(Leadership)」

5.1　リーダーシップ及びコミットメント：(5.1 b)は新規、それ以外は改訂)

情報セキュリティ方針に加えて情報セキュリティ目的を確立することが加わった。さらに、トップマネジメント（経営陣）のリーダーシップと、管理層がリーダーシップを実証出来るように支援すること、が加わった。

5.2　方針：（改訂）

「ISMS基本方針と情報セキュリティ基本方針」が、「情報セキュリティ方針」に統一された。さらに、情報セキュリティ方針に、情報セキュリティ目的の設定の枠組みに加えて、情報セキュリティ目的を含むことが、加わった。

5.3　組織の役割、責任及び権限：（改訂）

パフォーマンスの報告を要求するという部分が追加された。

解説

5.1、5.2ともに、基本的な部分では旧版とほぼ同じ内容を要求している。但し、「情報セキュリティ方針」に関しては、管理策のA.5.1.1で「情報セキュリティ方針群」として、アクセス制御や情報分類などのトピック毎の方針策定が要求されている。

5.3は、実質的にはおこなわれているはずだが、要求事項となった。

「6. 計画(Planning)」-1

6.1　リスク及び機会への取り組み：(6.1.1 a), b), c)、6.1.2 a), a) 2)、6.1.3 c)が新規、それ以外は改訂）

(1) マネジメントシステム規格の**リスクマネジメント規格は、ISO31000**を決定。

(2) リスクの定義が「目的に対する不確かさの影響」に変更された。従って、評価可能な目的の設定が求められる。「不確かさ」は、プラスもあればマイナスもある。その他に、新しい概念として、「リスク機会」、「リスク基準」、「情報 を実施するための基準」、「リスク所有者」、「リスクのレベル」、「リスクの優先順位」などがある。

(3) また、リスク対応もこれまで「低減（管理策の適用）、受容、移転、回避」の4つであったが、「ISO 31000 リスクマネジメント」との整合化を図ったことにより、「リスクの回避、リスク機会の追求、リスク源の除去、起こりやすさを変える、結果を変える、リスク共有、リスク保有」の7つに変更された。

解説

リスクマネジメントについて、「ISO31000　リスクマネジメント」との整合化が図られたことにより、新しい概念が導入されたので、新しい概念に対応するための整備が求められている。（6.1.1はMSSで、6.1.2と6.1.3はISMS固有）

(1) リスクマネジメントの規格 ISO 31000への対応

- **マネジメントシステム規格の共通化においては、リスクマネジメント規格は、ISO 31000を使用が決定**
  - ① マネジメントシステムの共通テキストには、リスクマネジメントの記述はない。マネジメントシステムには、リスクマネジメントの要求事項を持つものと持たないものがある。
  - ② 従って、ISO/IEC 27001:2013では、情報セキュリティリスクマネジメントに関する記述は、以下の通りである

    「6.1.3 情報セキュリティリスク対応の注記」

    この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，ISO 31000に規定する原則及び一般的な指針と整合している。
  - ③ 該当テキストは、主に「6 Planning」に置かれている。

(2) リスクマネジメントの規格 ISO 31000への対応
- ISO/IEC27001リスクの定義 -

- **新しい時代に対応したISO 31000に基づくリスクマネジメント**

① リスクの定義:

- 2005年版では、「事象の発生確率とその結果の組み合わせ (combination of the probability and its consequence)」
- 2013年版では、「目的に対する不確かさの影響」

② ISMSにおける新しい「リスクの定義」に基づくリスクの把握の意味:

- **「情報セキュリティ目的」**に対する不確かさを与えるものは何か、に関して**リスク源(Risk source)**に基づいて**アセスメント（リスクの特定、分析、評価）**することになる。

③ リスク所有者（risk owner）

- 27001:2013では、情報セキュリティのリスクを運用管理について責任及び権限 をもつ人又は主体を、リスク所有者（Risk owner）として、定義している。

リスクの用語定義

2.68 リスク（risk）
目的に対する不確かさの影響．（JIS Q 0073:2010の1.1参照）

注記1
影響とは，期待されていることから，好ましい方向又は好ましくない方向にかい（乖）離することをいう．
注記2
不確かさとは，事象（2.25），その結果（2.14）又はその起こり安さ（2.45）に関する，情報，理解又は知識が，たとえ部分的にでも欠落している状態をいう．
注記 3
リスクは，起こり得る事象（2.25），結果（2.24）又はこれらの組み合わ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．
注記 4
リスクは，ある事象（周辺状況の変化を含む．）の結果（2.14）とその発生の起こりやすさ（2.45）との組み合わせとして表現されることが多い．
注記 5
ISMSの文脈においては，情報セキュリティリスクは，情報セキュリティ目的に対する不確かさの影響として表現することがある．
注記 6
情報セキュリティリスクは，脅威（2.83）が情報資産のぜい弱性（2.89）又は情報資産グループのぜい弱性（2.89）に付け込み，その結果，組織に損害を与える可能性に伴って生じる

組織の方針を明確にする情報セキュリティ目的の導入

- 企業活動に貢献するための情報セキュリティ目的の確立

（事例）

情報セキュリティ目的
(組織の最高位)

- **顧客に影響するインシデントを減らし、企業活動における事業の信頼性を確保する（*インシデント=前年比50%*）**

情報セキュリティ目的
(営業部門)

- ***お客様情報を含むパソコンの紛失インシデントの減少（前年比50％）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

情報セキュリティ目的
(システム部門)

- ***システム要因によるインシデントの減少（前年比50％）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

情報セキュリティ目的
(サービス部門)

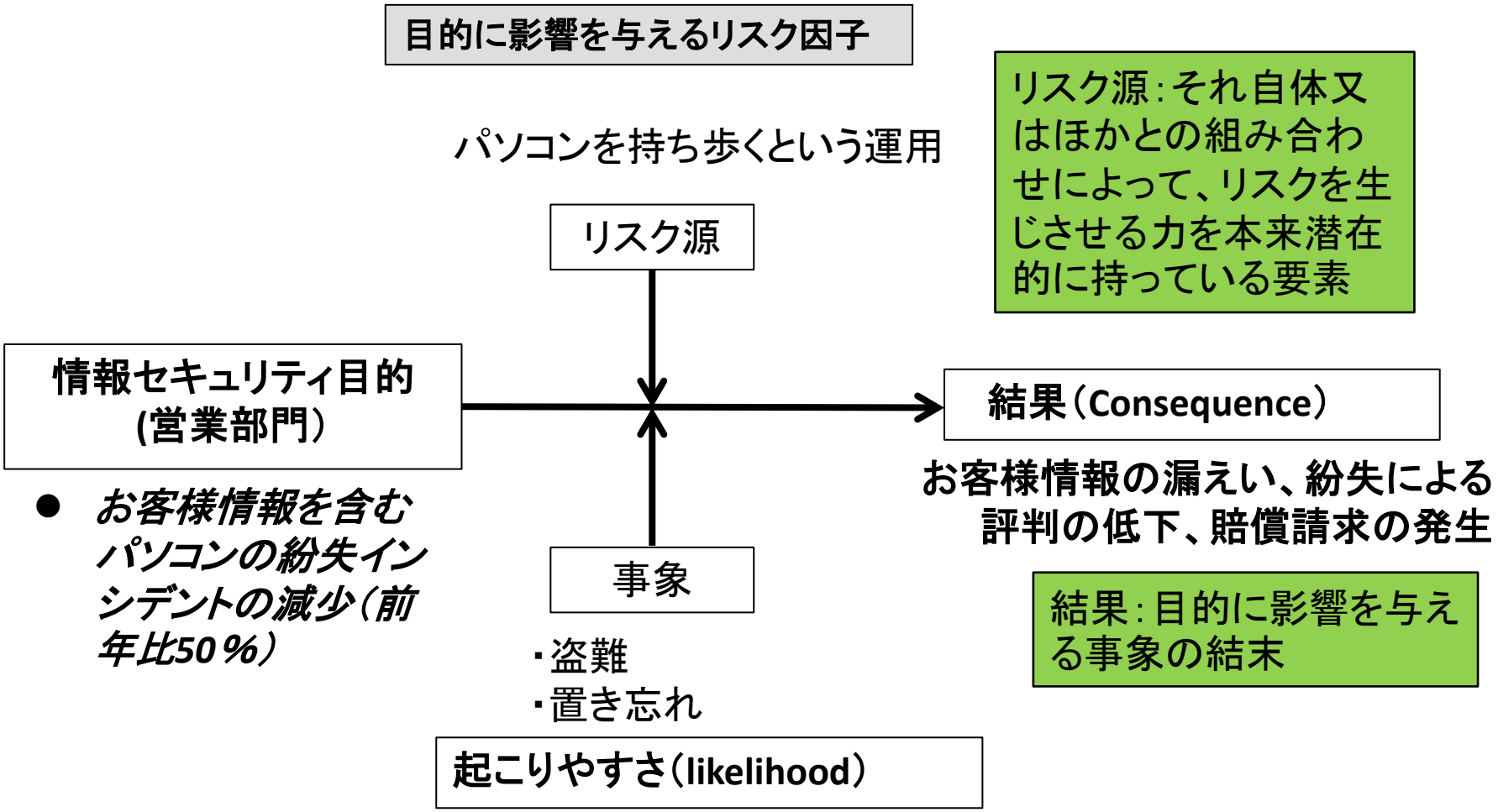
- ***お客様サービス提供前に必ずSLAを締結（サービス毎に100%）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

27001/27002 改定規格説明会(JSA)　山崎氏資料抜粋

情報セキュリティリスクの概念（事例１）

リスクの定義＝目的に対する不確かさの影響



情報セキュリティリスクアセスメントのプロセス（事例の図）

リスクの定義＝目的に対する不確かさの影響

目的に影響を与えるリスク因子

ハッカーの不正侵入による情報の破壊、流出を防止する。

情報セキュリティ目的

リスク源

セキュリティ更新プログラムの機能不足と定期更新の不徹底

リスク源：それ自体又はほかとの組み合わせによって、リスクを生じさせる力を本来潜在的に持っている要素

結果（Consequence）

バックドアからの情報盗難による信用・評判の低下と損害賠償請求

- *システム要因によるインシデントの減少（セキュリティ更新プログラムの適用不備によるインシデント発生:0％）*

事象

ハッカーが不正侵入、バックドアの設置を含む不正活動の実行

結果：目的に影響を与える事象の結末

起こりやすさ（likelihood）

中尾の“RISK”の解釈（更新）

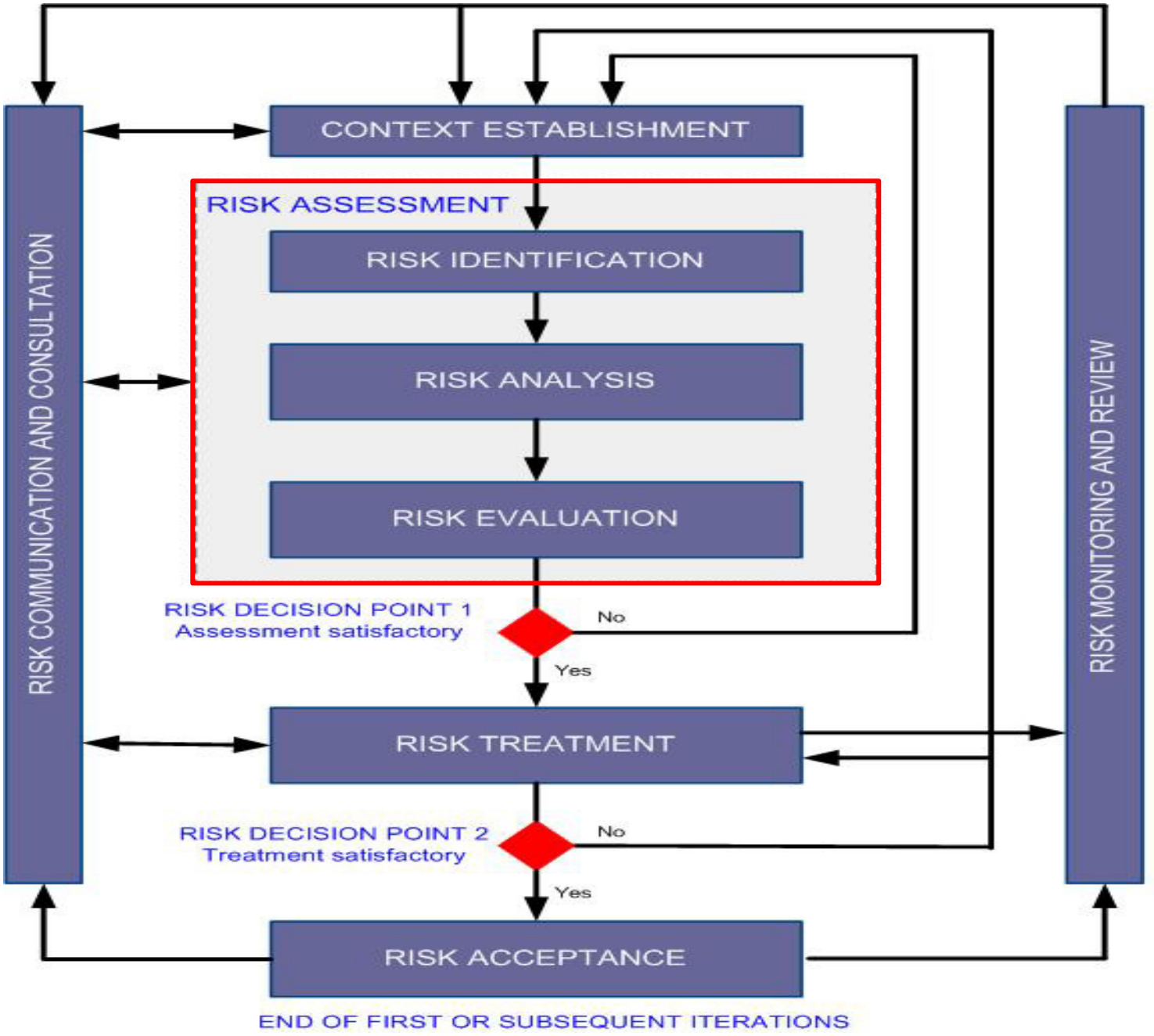
ISO 31000 : ***risk = the effect of an uncertainty on objectives***

“effect”は、結果/インパクトとして表現される。すなわち、それは、目的に影響するイベント(event)及びリスク源による結果である。”uncertainty”は、そのuncertaintyの原因であるイベントが起こる「起こりやすさ(likelihood)」に起因する。イベントは、潜在的なセキュリティインシデント（事故/事件）、攻撃、セキュリティ喪失のことを指す。

従って、RISKとは、以下の観点から表現ができる。(by Ted Humphrey)
「 *a combination of the consequence (e.g. the impact) of an event (e.g. Security incident, attack, compromise) and the likelihood of occurrence of the event.*
イベント（潜在的なインシデント、攻撃など）の結果（すなわち、インパクト）、及びそのイベントの生起する起こりやすさの結果の組み合わせである。」

例：
The ***objective*** : システム要因によるインシデントの削減（前年度比50%）
The ***event*** (potential cause of the uncertainty) : マルウェアによる攻撃/事故など
The ***consequences*** (the effect of the uncertainty) : 情報窃取、システム停止など

正確には、リスクを特定するとは：
「リスク源」、「イベント（事象）」、及び「それらの原因及び起こり得る結果」を特定すること



ISO/IEC 27005 — Illustration of an information security risk management process

個々の用語の定義

リスクアセスメント（risk assessment）
リスク特定，リスク分析及びリスク評価のプロセス全体。

リスク特定（risk identification）
リスク（2.68）を発見，認識及び記述するプロセス。（
注記 1
リスク特定には，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。
注記 2
リスク特定には，過去のデータ，理論的分析，情報に基づいた意見，専門家の意見及びステークホルダのニーズを含むことがある。

リスク分析（risk analysis）
リスクの特質を理解し，リスクレベルを決定するプロセス。
注記 1
リスク分析は，リスク評価及びリスク対応に関する意思決定の基礎を提供する。

リスク評価（risk evaluation）
リスク及び／又はその大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセス。
注記
リスク評価は，リスク対応に関する意思決定を手助けする。

(3) リスクマネジメントの規格 ISO 31000への対応
- 情報セキュリティリスク対応のプロセス -

- 7つのリスク対応の選択肢:

① リスクを発生させる活動を開始しない、または継続しないと決定することによって、そのリスクを回避(avoid)すること;

② リスクを取る(take)または増加(increase)させることにより、機会(好影響を与えるもの)を追求すること;

③ リスク源(risk source)を取り除くこと;

④ 起こりやすさ(likelihood)を変えること;

⑤ 結果(consequence)を変えること;

⑥ 一つまたは複数の他者とそのリスクを共有(share)すること;および

⑦ 充分な情報を得たうえでの決定により、そのリスクを保有(retain)すること。

リスク対応の選択肢

1）リスクを発生させる活動を、開始または継続しないと決定することによって、リスクを回避（avoid）すること。
例えば、地震の頻発する地域へのデータセンタの新設を中止すること。

2）ある機会を追求するために、リスクをとる（take）または増加（increase）させること。
例えば、市場を拡大するために、関連市場に、工場を建設すること。その結果、技術情報が流出するリスクが増加する。

3）リスク源（risk source）を除去すること。
例えば、システムから、情報漏えいの原因となるウィルスを除去すること。または、パソコン利用形態の運用を変更することなど。

4）起こりやすさ（likelihood）を変えること。
例えば、データデンターの設置場所を、地震の多い場所から、地震が全く発生しない場所に移設する。または、（技術的にではあるが）マルウェアが攻撃を行う通信ポートを閉じること。

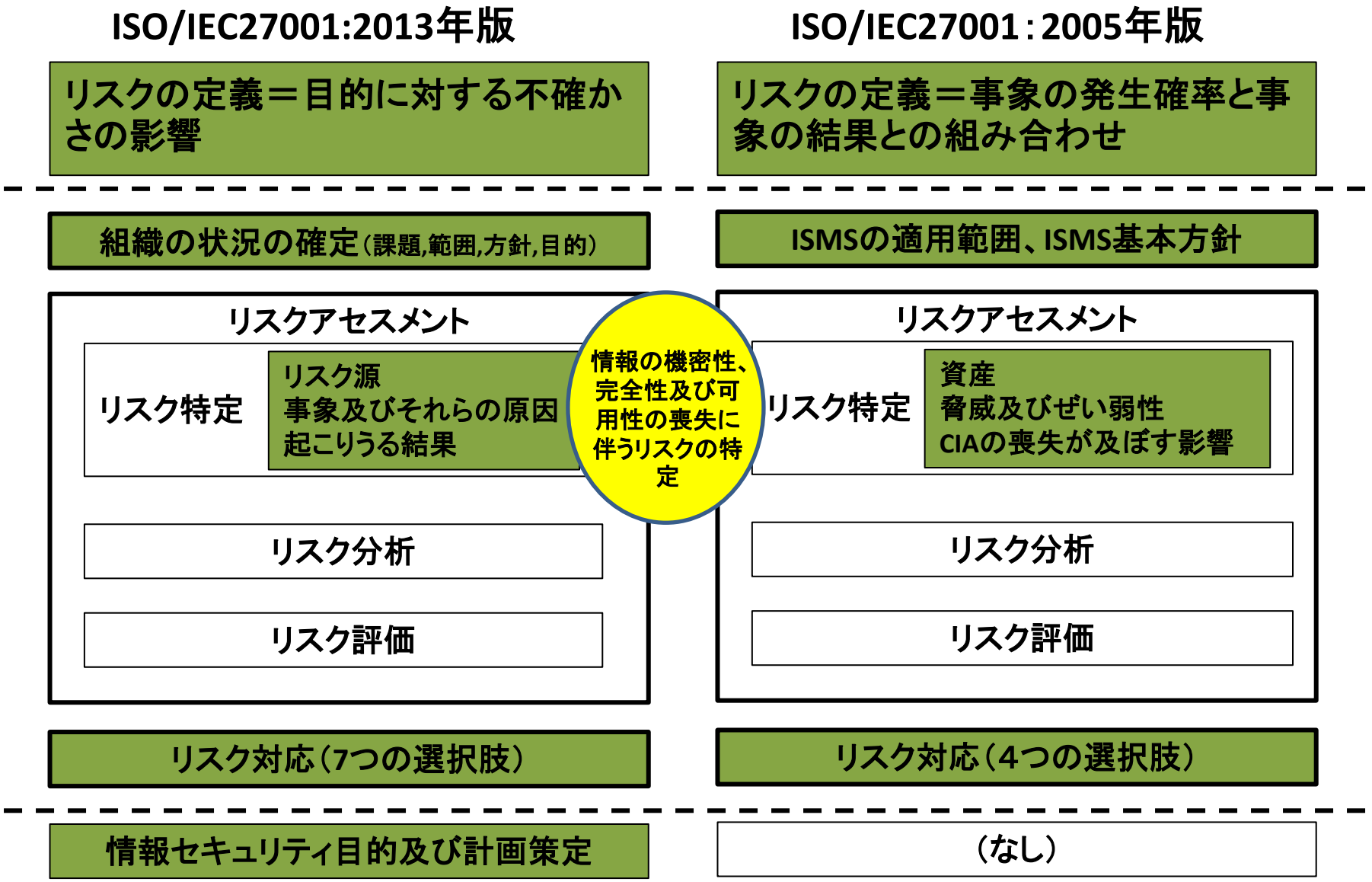
5）結果（consequence）を変えること。
例えば、データのバックアップを実施し、データの喪失が発生しても、損失とならないように対応すること。DDoS等のインパクトを、回線容量、システム耐久性をあげることで、結果を変えること。

6）一つまたは複数の他者とそのリスクを共有（share）すること。
例えば、保険に加入し、セキュリティ事故の損害賠償の補償を受けること。

7）情報に基づいた選択によって、リスクを保有（retain）すること。

ISO/IEC 27001の2013年版と2005年版との比較

（情報セキュリティリスクに関係する項目）



27001/27002 改定規格説明会(JSA)　山崎氏資料抜粋

(4) 分野別のISMSを確立するための2005年版の拡張
① ISO/IEC27001 Annex A以外の管理策群の許容

- 管理策の選択について
  - ISO/IEC 27001:2005 の場合 (4.2.1 g) :

    The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover the identified requirements.

    このプロセスの一部として、Annex A の中から、特定した要求事項を満たすために適切なように、管理目的及び管理策を選択しなければならない。

(4) 分野別のISMSを確立するための2005年版の拡張
① ISO/IEC27001 Annex A以外の管理策群の許容

- **管理策の選択について**
  - ISO/IEC 27001:2013 の場合 (6.1.3 b), c)):

    The organization shall define and apply an information security risk treatment process to:

    b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

    c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

    d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions,

  - リスク対応選択肢を実施するために必要な全ての管理策を決定する
  - Annex A 以外の管理策群の使用も想定している。ただし、Annex Aとの対応付けを要求している。
  - 必要な管理策を含んでいるSoAの作成（produce）を要求している

(4) 分野別のISMSを確立するための2005年版の拡張
② 分野別ISMS認証制度の整備

- ISO/IEC 27000 ファミリー規格で、Sector specific standards（分野別指針）が増加している。
  - ISO/IEC 27010: 組織間コミュニティ（業界団体等）向け
  - ISO/IEC 27011: 通信事業者向け
  - ISO/IEC 27015: 金融サービス向け
  - ISO/IEC 27017: クラウドコンピューティング向け
  - ISO/IEC 27018: クラウドコンピューティングにおけるPII情報の管理
- Sector specific standard と ISO/IEC 27002 の関係
  - ISO/IEC 27002 を前提として、
  - 分野固有の管理策、実施の手引、又は関連情報を追加することにより、
  - ISO/IEC 27002 を当該分野向けに拡張している。

(4) 分野別のISMSを確立するための2005年版の拡張
② 分野別ISMS認証制度の整備

- ISO/IEC 27001:2013 に加えて Sector specific control set を用いる場合、Annex A及びSoAの考え方や方法に関して、27001:2005の要求事項を拡大して引き継ぐことの規格化作業が開始されている
- この点を整備する規格の開発がローマ会議で英国から提案され、その後、新規プロジェクト提案 (New Work Item Proposal) が承認された。
- フランスのソフィアアンチポリス会議及び仁川会議で、プロジェクトは、ISO/IEC 27009として、編集作業が実施された。

(4) 分野別のISMSを確立するための2005年版の拡張
② 分野別ISMS認証制度の整備

- この新規プロジェクトにより Sector specific control set standard を用いたISMS認証の制度が整備されると、次のような分野対応のISMS認証が成立することになる。

  - ISMS認証：　従来からの認証、ISO/IEC 27001
  - クラウドユーザ向けISMS認証：　＋ ISO/IEC 27017
  - クラウドプロバイダ向けISMS認証：　＋ ISO/IEC 27017
  - 通信事業者向けISMS認証：　＋ ISO/IEC 27011

(4) 分野別のISMSを確立するための2005年版の拡張
② 分野別ISMS認証制度の整備

ISMSのマネジメントシステム規格

ISO/IEC 27001
- ISMS要求事項 (本文)
- Annex A (27002実践規範を基に)

Sector specific controlsの位置づけ

- 27017 Cloud Security Controls
- Other sector specific controls (27018 etc.)

27017 Cloud Security Controlsが、information security risk assessment及びinformation security risk treatment, 及びinformation security audit等に、適用される

「6. 計画(Planning)」-2

6.2 情報セキュリティ目的及びそれを達成するための計画：(6.2 b), c), f), g), h), i) が新規、それ以外は改訂）

(1) 2013年版では、情報セキュリティ目的を関連する部門及び階層毎に確立することを求めている。

(2) 「目的」は原文では「objectives」である。objectivesは、日本語に訳される際に、「目的」又は「目標」と複数の言葉に訳されている（ISO9000では「目標」）。日本語では「目的」と「目標」は異なる概念であるが、「objectives」は2つの意味を持っているとされる。

(3) 日本語の目標は英語では「Target」又は「goal」と訳されることが多いが、targetは、目標地点、目標数字、目標期限など、具体的な数字で表わされることが多く、goalは、通常最終到達点という意味で使われている。

(4) 目的は、「（実行可能な場合）測定可能である。」事が求められており、定量的又は定性的な測定指標が必要となる。

解説

この規格で「目的」としているのは、単に目的のみを設定するのではなく、そこに至る道しるべ（目標）を用意し、目的を達成することを確実にすることが望まれており、目的(objectives）の中に、目標の意味が含まれていることが、注記の中に、記述されている。

(1) 組織の方針を明確にする情報セキュリティ目的の導入

- 企業活動に貢献するための情報セキュリティ目的(Information security objectives)の確立

① 組織の情報セキュリティ目的の構造:

- 組織で、情報セキュリティ目的の設定のための枠組を確立
- トップマネジメントが設定する組織の最高位の情報セキュリティ目的
- ***最高位の情報セキュリティ目的から関連する部門及び階層までの情報セキュリティ目的を展開***

② 情報セキュリティ目的の要件:

- 情報セキュリティ方針と整合している。
- ***測定可能である。情報セキュリティ目的を定めて、測定可能な目標を設定***して、進めていくのが、有効な進め方である。
- 適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。

③ 情報セキュリティ目的を達成するための計画:

- 実施事項
- 必要な資源
- 責任者
- 達成期限
- 結果の評価方法

(2) 組織の方針を明確にする情報セキュリティ目的の導入

- 企業活動に貢献するための情報セキュリティ目的の確立

（事例）

情報セキュリティ目的
(組織の最高位)

- **顧客に影響するインシデントを減らし、企業活動における事業の信頼性を確保する（*インシデント=前年比50%*）**

情報セキュリティ目的
(営業部門)

- ***お客様情報を含むパソコンの紛失インシデントの減少（前年比50％）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

情報セキュリティ目的
(システム部門)

- ***システム要因によるインシデントの減少（前年比50％）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

情報セキュリティ目的
(サービス部門)

- ***お客様サービス提供前に必ずSLAを締結（サービス毎に100%）***

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

27001/27002 改定規格説明会(JSA)　山崎氏資料抜粋

ISO/IEC 27002改定の概要

ISO/IEC 27002

- 旧版
  ISO/IEC 27002:2005 (ISO/IEC 17799:2005)

  Information technology – Security techniques - Code of practice for information security management, 2005-06-15

- 改定版
  ISO/IEC 27002:2013

  Information technology – Security techniques - Code of practice for information security controls, 2013-10-01

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

ISO/IEC 27002 改定の主旨

- この規格が、情報セキュリティマネジメントの視点で情報セキュリティ管理策を広く提示し、ISMSの確立、実施、維持及び継続的な改善における管理策の実施にも活用できる、実務的な指針として国際的に広く活用されていることを踏まえ、その役割を継承する。
- 組織における情報の管理・取扱いに関する技術及び環境の変化に対応する。
- 幅広い利用者に向けて、この規格を一層使いやすいものにする。

ISO/IEC 27002 改定内容の概観

1. 2005年版を継承している。
   - 多くの管理策は、2005年版の管理策を継承している。標題と管理策が同一か、ほぼ同一。
2. 他方で、2005年以後の新しい動向や概念を取り入れている。
   - 14.2 開発及びサポートプロセスにおけるセキュリティ
   - 15 供給者関係

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

ISO/IEC 27002 改定内容の概観

3. 情報セキュリティ管理策の指針を提供する。技術的な詳細については、一般的な管理策の解釈や、他の規格に譲ることにした部分がある。
   - 例えば、旧版の「11.4 ネットワークのアクセス制御」のいくつかの管理策を削除している。
4. 陳腐化した記事を書き換え、又は削除している。
   - 旧版の「10.9 電子商取引」を書き換えた。
   - 旧版の「12.5.4 情報の漏えい」を削除した。
5. 各所で記述を改善している。

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

ISO/IEC 27002 改定の特徴　標題

- 管理策が主題であることを標題で明示。

  旧版

  Information technology – Security techniques - Code of practice for information security management

  改定版

  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

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

ISO/IEC 27002 改定の特徴　位置づけ

- 2005年版における本標準の位置づけを維持し、改定版でこれを明文化している。
「1 適用範囲」（Scope）より:

この規格は、次の事項を意図する組織への適用を目的としている。

a) ISO/IEC 27001 に基づくISMS を実施するプロセスで、管理策を選定する。

b) 一般に受け入れられている情報セキュリティ管理策を実施する。

c) 固有の情報セキュリティマネジメントの指針を作成する。

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

ISO/IEC 27002 箇条構成　新旧対比(1/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
0　Introduction	0　Introduction
1　Scope	1　Scope
――	2　Normative references
2　Terms and definitions	3　Terms and definitions
3　Structure of this standard	4　Structure of this standard
4　Risk assessment and treatment	――

ISO/IEC 27002 箇条構成　新旧対比(1/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
0　序文	0　序文
1　適用範囲	1　適用範囲
ーーー	2　引用規格
2　用語及び定義	3　用語及び定義
3　規格の構成	4　規格の構成
4　リスクアセスメント及びリスク対応	ーーー

ISO/IEC 27002 箇条構成　新旧対比(2/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
5 Security policy	5 Security policies
6 Organization of information Security	6 Organization of information security
7 Asset management	8 Asset management
8 Human resource security	7 Human resource security
9 Physical and environmental Security	11 Physical and environmental security
10 Communications and operations management	12 Operations security
	13 Communications security
11 Access control	9 Access control

箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 箇条構成　新旧対比(2/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
5　セキュリティ基本方針	5　情報セキュリティのための方針群
6　情報セキュリティのための組織	6　情報セキュリティのための組織
7　資産の管理	8　資産の管理
8　人的資源のセキュリティ	7　人的資源のセキュリティ
9　物理的及び環境的セキュリティ	11　物理的及び環境的セキュリティ
10　通信及び運用管理	12　運用のセキュリティ
	13　通信のセキュリティ
11　アクセス制御	9　アクセス制御

箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 箇条構成　新旧対比(3/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
12 Information systems acquisition, development and maintenance	14 System acquisition, development and maintenance
	10 Cryptographic controls
-----	15 Supplier relationships
13 Information security incident management	16 Information security incident management
14 Business continuity management	17 Information security aspects of business continuity management
15 Compliance	18 Compliance
管理策　133項目	**管理策　114項目**

箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 箇条構成　新旧対比(3/3)

旧版　ISO/IEC 27002:2005	改定版　ISO/IEC 27002:2013
12　情報システムの取得、開発及び保守	14　システムの取得、開発及び保守
	10　暗号
-----	15　供給者関係
13　情報セキュリティインシデントの管理	16　情報セキュリティインシデント管理
14　事業継続管理	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
15　順守	18　順守
管理策　133項目	**管理策　114項目**

箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 箇条構成　改定版

改定版
5 情報セキュリティのための方針群
6 情報セキュリティのための組織
7 人的資源のセキュリティ
8 資産の管理
9 アクセス制御
10 暗号
11 物理的及び環境的セキュリティ
12 運用のセキュリティ
13 通信のセキュリティ
14 システムの取得、開発及び保守
15 供給者関係
16 情報セキュリティインシデント管理
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
18 順守

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

箇条2　参照規格

“2 Normative references”

- ISO/IEC 27000 を参照規格としている。
  - ISO/IEC 27000 ファミリー規格に共通の用語及び定義を ISO/IEC 27000 に置いている。
  - ISO/IEC 27002 の用語及び定義も ISO/IEC 27000 へ移したため、ISO/IEC 27000 が ISO/IEC 27002 に必須の規格となっている。
  - 旧版には、参照規格の箇条はない。

箇条3　用語及び定義

“3 Terms and definitions”

- 用語及び定義は、ISO/IEC 27000 を参照することを指示している。

- ISO/IEC 27000 の用語及び定義の他に、ISO/IEC 27002 には、用語及び定義はない。

旧版　箇条4

- 旧版
  「4. リスクアセスメント及びリスク対応」

  – 改定版では、旧版の本箇条を削除している。
  – ISO/IEC 27002 の位置づけを、リスクアセスメントとリスク対応で選択の対象とする管理策一覧を提示するものとした。

  – 改定版では、リスクマネジメントの記事は、序文の「0.2 情報セキュリティ要求事項」及び「0.3 管理策の選定」に残っている。
  – ISMSにおいて、リスクマネジメントの要求事項と指針は、ISO/IEC 27001 及び ISO/IEC 27005 を参照する。

箇条4　規格の構成

- 旧版の「3 規格の構成」を継承している。

- 情報セキュリティ管理策を提示する箇条5から箇条18の構成の説明
  - 「箇条」 (14)
  - 「カテゴリ（管理目的、目的）」 (35)
  - 「管理策」 (114)
  - 管理策に伴う「実施の手引」及び「関連情報」

箇条5～18　箇条、カテゴリ、管理策

- 次葉以降で、箇条5～18について、主な改定内容を解説する。
  - 多岐にわたる今回の改定内容を網羅するものではない。

箇条5　情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

目的　情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。

箇条5　情報セキュリティのための方針群

- 旧版
  「5.1.1 情報セキュリティ基本方針文書」

- 改定版
  「5.1.1 情報セキュリティのための方針群」

管理策

情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知することが望ましい。

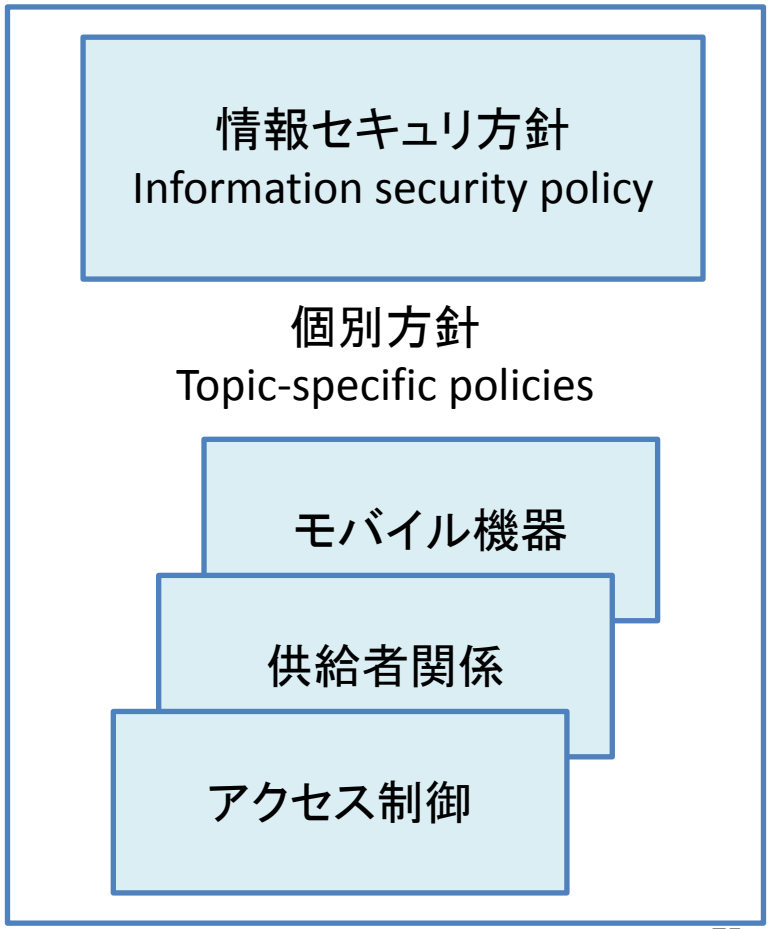
箇条5　情報セキュリティのための方針群

旧版

情報セキュリティ
基本方針文書
Information security policy

改定版

情報セキュリティ方針群
Information security policies



- 改定版でトピックごとの「個別方針」を追加

27001/27002 改定規格説明会(JSA)　山下氏資料抜粋

箇条6　情報セキュリティのための組織

6.1　内部組織

目的　組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.2　モバイル機器及びテレワーキング

目的　モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

箇条6　情報セキュリティのための組織

- 旧版
  「6 情報セキュリティのための組織」
  「6.1 内部組織」
  「6.2 外部組織」
- 改定版
  「6 情報セキュリティのための組織」
  「6.1 内部組織」
  「6.2 モバイル機器及びテレワーキング」

  – 改定版では、この箇条に組織のマネジメントが及び範囲の管理目的と管理策を置くこととして、「外部組織」は外した。
  – 旧版の「6.2.3 第三者との契約におけるセキュリティ」を改定版の「15 供給者関係」へ移動。

箇条6　情報セキュリティのための組織

- 旧版
  「6.1.1 情報セキュリティに対する経営陣の責任」
  「6.1.2 情報セキュリティの調整」

  – 旧版の 6.1.1 は、改定版では「7.2.1 経営陣の責任」が人的資源についての経営陣の責任の範囲で関係する。
  – 旧版の 6.1.2 は、削除している。

  – ISO/IEC 27001 との重複が理由とされたが、議論のあるところである。

箇条6　情報セキュリティのための組織

- 旧版
  「6.1.3 情報セキュリティ責任の割当て」
  「8.1.1 役割及び責任」
- 改定版
  「6.1.1 情報セキュリティの役割及び責任」

  – 改定版で、旧版のこれらの二つの管理策を一つに統合している。

  – 旧版の「8. 人的資源のセキュリティ」は、従業員等の個人が主題であるため、組織における役割と責任は箇条6に整理したもの。

箇条7　人的資源のセキュリティ

7.1 雇用前

目的　従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.2 雇用期間中

目的　従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。

7.3 雇用の終了及び変更

目的　雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。

箇条7　人的資源のセキュリティ

- 旧版
  「8 人的資源のセキュリティ」
- 改定版
  「7 人的資源のセキュリティ」
  - 「雇用前」「雇用期間中」「雇用の終了又は変更」からなる構造は維持している。

箇条7　人的資源のセキュリティ

- 改定版の箇条7では、対象とする人的資源を組織で管理できる者に限定している。

	旧版	改定版
従業員　employee(s)	○	○
契約相手　contractor(s)	○	○
第三者の利用者　third party user(s)	○	―

「第三者の利用者には、組織への一般来訪者、組織が開設するウェブサイト（ネットバンキングなど）を利用する個人などが含まれる。ただし、ウェブサイトの完全公開情報の閲覧については除外する。」（「JIS Q 27002:2006」箇条8 の注記より。）

  - これらの者は組織で管理する人的資源ではなく、「雇用前」「雇用期間中」「雇用の終了又は変更」の概念も適用できないため、改定版では箇条7の適用対象から除外した。

箇条7　人的資源のセキュリティ

- 管理策での対応例

> 7.2.2　**情報セキュリティの意識向上，教育及び訓練**
> **管理策**
> 組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受け，また，定めに従ってその更新を受けることが望ましい。

  - 第三者の利用者には通常はこれが適用できないため、この管理策の対象から除外している。

箇条7　人的資源のセキュリティ

- この箇条の解釈においては、従業員及び契約相手の範囲が国又は組織によって異なる場合があることに留意。
- 日本での目安は
  - 従業員：雇用契約に基づき就業規則を適用する者
  - 契約相手：業務契約は結ぶが就業規則は適用しない者
- 契約相手の例：
  - 派遣労働者、コンサルタント、弁護士
- 「7.2.3 懲戒手続」は、従業員に適用されるが、契約相手は対象としていない。

箇条7　人的資源のセキュリティ

- 旧版
  「8.3.3 アクセス権の削除」
- 改定版
  「9.2.6 アクセス権の削除又は修正」

  – 「8　人的資源のセキュリティ」に置いていた本管理策を、「9 アクセス制御」の「9.2 利用者アクセスの管理」に移した。
  – これにより、雇用の終了又は変更に伴う場合だけでなく、一般的なアクセス権の削除又は修正に位置付けた。

箇条8　資産の管理

8.1 資産に対する責任

目的　組織の資産を特定し、適切な保護の責任を定めるため。

8.2 情報分類

目的　組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.3 媒体の取扱い

目的　媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。

箇条8　資産の管理

- 旧版
  「7 資産の管理」
- 改定版
  「8 資産の管理」

- 旧版の構成を継承し、「媒体の取扱い」を
  旧版の「10 通信及び運用管理」からここへ移している。
  「8.1 資産の管理」
  「8.2 情報分類」
  「8.3 媒体の取扱い」

箇条8　資産の管理

- 旧版の「7.2.2 情報のラベル付け及び取扱い」を二つに分けている。

  「8.2.1 情報の分類」

  「8.2.2 情報のラベル付け」

  「8.2.3 資産の取扱い」

  – ラベル付けをする者と資産を取り扱う者が異なることを考慮したもの。

箇条8　資産の管理

- この規格で取り上げる資産が、情報に関連する資産であることを明確にしている。

旧版
7.1.1　**資産目録**
管理策　　すべての資産を明確に識別し、また、重要な資産すべての目録を作成し、維持することが望ましい。

改定版
8.1.1　**資産目録**
管理策　　情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

箇条8　資産の管理

- 箇条7以外において、情報及び資産にアクセスし、これらを取り扱う者

<table>
<tr><th>旧版</th><th colspan="2">改定版</th></tr>
<tr><td>従業員
employee(s)</td><td colspan="2">従業員
employee(s)</td></tr>
<tr><td>契約相手
contractor(s)</td><td>契約相手
contractor(s)</td><td rowspan="2">外部の利用者
external party user(s)</td></tr>
<tr><td>第三者の利用者
third party user(s)</td><td></td></tr>
</table>

  - 改定版「外部の利用者」
＝旧版「契約相手」＋「第三者の利用者」
    - contractor(s)とthird party user(s) の区別は、資産の管理（箇条8）及びアクセス制御（箇条9）などの管理策において重要でない場面があることを考慮して、両者をあわせてexternal party user(s) とした。

箇条8　資産の管理

- 外部の利用者の用例

旧版
8.3.2　**資産の返却**
管理策　　全ての**従業員、契約相手及び第三者**の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産全てを返却することが望ましい。

改定版
8.1.4　**資産の返却**
管理策　　全ての**従業員及び外部の利用者**は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却することが望ましい。

箇条9　アクセス制御

9.1 アクセス制御に対する業務上の要求事項

目的　情報及び情報処理施設へのアクセスを制限するため。

9.2 利用者アクセスの管理

目的　システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

9.3 利用者の責任

目的　利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

9.4 システム及びアプリケーションのアクセス制御

目的　システム及びアプリケーションへの、認可されていないアクセスを防止するため。

箇条9　アクセス制御

- 旧版
  「11 アクセス制御」
- 改定版
  「9 アクセス制御」
  - 旧版
    「11.5 オペレーティングシステムのアクセス制御」
    「11.5.1 セキュリティに配慮したログオン手順」
    「11.5.3 パスワード管理システム」
    「11.6 業務用ソフトウェア及び情報のアクセス制御」
    「11.6.1 情報へのアクセス制限」
    - これらの管理策はシステムとアプリケーションに共通に適用すべきものであることから、改定版では11.5と11.6を統合した。
  - 改定版
    「9.4 システム及びアプリケーションのアクセス制御」

箇条9　アクセス制御

- 改定版
  「9.4 システム及びアプリケーションのアクセス制御」
  「9.4.1 情報へのアクセス制限」
  「9.4.2 セキュリティに配慮したログオン手順」
  「9.4.3 パスワード管理システム」
  「9.4.4 特権的なユーティリティプログラムの使用」
  「9.4.5 プログラムソースコードへのアクセス制御」

箇条9　アクセス制御

- 旧版
  「11.4 ネットワークアクセス制御」
  「11.4.2 外部から接続する利用者の認証」
  「11.4.3 ネットワークにおける装置の識別」
  「11.4.4 遠隔診断用及び環境設定用ポートの保護」
  「11.4.6 ネットワークの接続制御」
  「11.4.7 ネットワークのルーティング制御」
  - 改定版では、これらの管理策を削除している。
  - ISO/IEC 27002 をマネジメントの視点からの管理策実施に関する指針として、技術的個別事項は省く方向。
  - 改定版に「9.1.1 アクセス制御方針」「9.1.2 ネットワーク及びネットワークサービスへのアクセス」及び「13.1.1 ネットワーク管理策」は存続している。削除された上記管理策の内容は、組織におけるこれらの実施方法として導出することはできる。

箇条9　アクセス制御

- 旧版
「11.2.3 利用者パスワードの管理」
「11.3.1 パスワードの利用」
- 改定版
「9.2.4 利用者の秘密認証情報の管理」
「9.3.1 秘密認証情報の利用」
  - 旧版
「パスワード」
  - 改定版
「秘密認証情報」secret authentication information
    - 改定版では、認証の手段に秘密鍵、ワンタイム・パスワードなどの、パスワード以外の手段も含めて一般化している。

箇条10　暗号

10.1　暗号による管理策

目的　情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

箇条10　暗号

- 旧版
  「12.3 暗号による管理策」
- 改定版
  「10 暗号」
  　「10.1 暗号による管理策」

  – 暗号による管理策は情報システムの運用と開発の両面に関係することから、一つの独立した箇条を充てることにした。
  – 二つの管理策、実施の手引、関連情報は旧版を踏襲している。

箇条11　物理的及び環境的セキュリティ

11.1 セキュリティを保つべき領域

目的　組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.2 装置

目的　資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。

箇条11　物理的及び環境的セキュリティ

- 旧版
  「9 物理的及び環境的セキュリティ」
- 改定版
  「11 物理的及び環境的セキュリティ」
  - 旧版から大きな変更はない。
  - 旧版の「11 アクセス制御」から、次の二つの管理策をこの箇条に移している。
    - 「11.3.2 無人状態にある利用者装置」
    - 「11.3.3 クリアデスク・クリアスクリーン方針」

箇条12　運用のセキュリティ

12.1 運用の手順及び責任

目的　情報処理設備の正確かつセキュリティを保った運用を確実にするため。

12.2 マルウェアからの保護

目的　情報及び情報処理施設がマルウェアから保護されることを確実にするため。

12.3 バックアップ

目的　データの消失から保護するため。

箇条12　運用のセキュリティ

12.4 ログ取得及び監視

目的　イベントを記録し、証拠を作成するため。

12.5 運用ソフトウェアの管理

目的　運用システムの完全性を確実にするため。

12.6 技術性脆弱性管理

目的　技術的ぜい弱性の悪用を防止するため。

12.7　情報システムの監査に対する考慮事項

目的　運用システムに対する監査活動の影響を最小限にするため。

箇条12　運用のセキュリティ

- 旧版
「10 通信及び運用管理」
- 改定版
「12 運用のセキュリティ」

  – 旧版では一つの箇条に含めていた通信と運用を分離した。
    - IT基盤を通信・通信機器と情報システムで構成するものとした。
    - 情報システムについて、開発（箇条14）と運用（箇条12）の対比を明確にした。

  – 「10.2 第三者が提供するサービスの管理」は、委託関係の一つとして「15 供給者管理」へ移した。

箇条13　通信のセキュリティ

13.1　ネットワークセキュリティ管理

目的　ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

13.2　情報の転送

目的　組織の内部及び外部に転送した情報のセキュリティを維持するため。

箇条13　通信のセキュリティ

- 旧版
  「10 通信及び運用管理」
- 改定版
  「13 通信のセキュリティ」

  – 旧版の「10 通信及び運用管理」から、通信に関する管理策を取り出して一つの箇条にした。
  – 「10.2 第三者が提供するサービスの管理」は、委託関係の事項であり、「15 供給者管理」へ移した。

箇条13　通信のセキュリティ

- 旧版の「10.8 情報の交換」は、改定版では箇条13に置いている。
  - 「情報の交換（exchange）」は、用語を「情報の転送（transfer）」とした。双方向の移動でなく、一方向の移動が基本であるため。

- 旧版の「6.1.5 秘密保持契約」を、改定版では「13.2.4 秘密保持契約又は守秘義務契約」として箇条13に置いている。

- 「13.1 ネットワークセキュリティ管理」はネットワーク上の通信が対象である。これに対し、「13.2 情報の転送」は、媒体の移動などネットワーク上の通信以外の移動（広い意味での「コミュニケーション」）も対象としている。

箇条14　システムの取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

目的　ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

14.2 開発及びサポートプロセスにおけるセキュリティ

目的　情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。

14.3 試験データ

目的　試験に用いるデータの保護を確実にするため。

箇条14　システムの取得、開発及び保守

- 旧版
「12 情報システムの取得、開発及び保守」
- 改定版
「14 システムの取得、開発及び保守」
  - 旧版の「10.9 電子商取引サービス」を一般化して箇条14へ移動した。
  - 旧版の「12.2 業務用ソフトウェアでの正確な処理」の下の管理策は、改定版の新規管理策「14.2.5 セキュリティに配慮したシステム開発の原則」に含まれる。
  - システムの開発について、ライフサイクルの観点から管理策を整備・拡充した。
「14.2 開発及びサポートプロセスにおけるセキュリティ」

それぞれについて、次葉以降で詳説する。

箇条14　システムの取得、開発及び保守

- 旧版
  「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」
- 改定版
  「14.1.2 公共ネットワーク上のアプリケーションサービスのセキュリティ」
  「14.1.3 アプリケーションサービスのトランザクションの保護」

  – 旧版における「電子商取引」という用語・概念を、改定版では新しい用語・概念に一般化している。

箇条14　システムの取得、開発及び保守

- 旧版
  「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」
- 改定版
  「14.2.5 セキュリティに配慮したシステム構築の原則」
  - 旧版のこれらの指針（特に12.2.1及び12.2.2）は、現在では体系的なセキュアプログラミングの一部である。
  - 改定版では、システム構築の一部にセキュアプログラミングの内容も含め、このことを「関連情報」で明示。

箇条14　システムの取得、開発及び保守

- 改定版

「14.2 開発及びサポートプロセスにおけるセキュリティ」
「14.2.1 セキュリティに配慮した開発のための方針」※
「14.2.2 システムの変更管理手順」
「14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー」
「14.2.4 パッケージソフトウェアの変更に対する制限」
「14.2.5 セキュリティに配慮したシステム構築の原則」※
「14.2.6 セキュリティに配慮した開発環境」※
「14.2.7 外部委託による開発」
「14.2.8 システムセキュリティの試験」※
「14.2.9 システムの受入れ試験」

※　新規管理策

– 改定版で、開発及びサポートプロセスにおけるセキュリティの管理策を充実させた。旧版に対して下線の管理策を追加している。

箇条14　システムの取得、開発及び保守

改定版で追加した管理策（14.2）

14.2.1 **セキュリティに配慮した開発のための方針**
　ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用することが望ましい。

14.2.5 **セキュリティに配慮したシステム構築の原則**
　セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用することが望ましい。

14.2.6 **セキュリティに配慮した開発環境**
　組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護することが望ましい。

14.2.8 **システムセキュリティの試験**
　セキュリティ機能（functionality）の試験は、開発期間中に実施することが望ましい。

箇条15　供給者関係

15.1 供給者関係における情報セキュリティ

目的　供給者がアクセスできる組織の資産の保護を確実にするため。

15.2 供給者のサービス提供の管理

目的　供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

箇条15　供給者関係

- 旧版
「6.2.3 第三者との契約におけるセキュリティ」
「10.2 第三者が提供するサービスの管理」
- 改定版
「15 供給者関係」

  - 外部委託、サプライチェーン等、外部の製品及びサービスの調達・利用に関する管理策を、改定版では箇条15にまとめている。
    - 調達者の情報を供給者がアクセス又は管理すること等に伴う情報セキュリティリスクへの対応である。
    - 他の箇条が、組織が自ら管理する情報についての管理策であることと区別される。
    - この内容は、ISO/IEC 27036 Information security for supplier relationships でさらに展開されている。

箇条15　供給者関係

- 改定版
  「15 供給者関係」
  「15.1 供給者関係におけるセキュリティ」
    「15.1.1 供給者関係のための情報セキュリティの方針」※
    「15.1.2 供給者との合意におけるセキュリティの取扱い」
    「15.1.3 ICTサプライチェーン」※
  「15.2 供給者のサービス提供の管理」
    「15.2.1 供給者のサービス提供の監視及びレビュー」
    「15.2.2 供給者のサービス提供の変更に対する管理」
    ※　新規管理策

箇条15　供給者関係

改定版で追加した管理策

15.1.1 **供給者関係のための情報セキュリティの方針**
　組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化することが望ましい。

15.1.3 **ICT サプライチェーン**
　供給者との合意には，ICTサービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

箇条16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

目的　セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

箇条16　情報セキュリティインシデント管理

- 旧版
「13 情報セキュリティインシデントの管理」
- 改定版
「16 .1 情報セキュリティインシデントの管理及びその改善」
  「16.1.1 責任及び手順」
  「16.1.2 情報セキュリティ事象の報告」
  「16.1.3 情報セキュリティ弱点の報告」
  「16.1.4 情報セキュリティ事象の評価及び決定」※
  「16.1.5 情報セキュリティインシデントへの対応」※
  「16.1.6 情報セキュリティインシデントからの学習」
  「16.1.7 証拠の収集」
  - 改定版では、旧版の5個の管理策を継承し、さらに、2個の管理策（※）を加えた。
  - 2011年9月に発行された ISO/IEC 27035 Information technology – Security techniques – Information security incident management の成果を改定版に反映したもの。

ISO/IEC 27035（全体）(WG4)

ISO/IEC 27035-1

- Title: Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management (Revision of 27035)
- Next stage: 4th WD

ISO/IEC 27035-2

- Title: Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response (Revision of 27035)
- Next stage: 4th WD

ISO/IEC 27035-3

- Title: Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations (Revision of 27035)
- Next stage: 4th WD

箇条17　事業継続マネジメントの情報セキュリティの側面

17.1 情報セキュリティ継続

目的　情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むことが望ましい。

17.2 冗長性

目的　情報処理施設の可用性を確実にするため。

箇条17　事業継続マネジメントの情報セキュリティの側面

- 旧版
「14 事業継続管理」
- 改定版
「17 事業継続マネジメントの情報セキュリティの側面」
「17.1 情報セキュリティ継続」
  - 旧版、改定版共に、組織の事業継続マネジメントの一部として求められる情報セキュリティの継続性確保を目的とする箇条であるが、重点が異なる。
    - 旧版（14）：　業務プロセスの保護と再開に重点。これを支えるものとして、情報システムの継続的運用と回復がテーマ。
    - 改定版（17.1）：　情報セキュリティ及び情報セキュリティマネジメントの継続と回復が主題。
    - 旧版の管理策を実施していても、改定版の管理策を実施していることには必ずしもならない。

箇条17　事業継続マネジメントの情報セキュリティの側面

- 改定版
  「17.2 冗長性」
  「17.2.1 情報処理施設の可用性」

> 17.2.1 **情報処理施設の可用性**
> 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。

  - 旧版では、情報或いは情報を保有する資産の可用性に関する管理策が体系的には見えにくかった。改定版では、この管理策で情報処理施設について可用性確保の対応を包括的に示している。
  - 情報処理施設の可用性確保は事業継続マネジメントの一部でもあるため、本管理策を箇条17に置いた。

箇条18　順守

18.1 法的及び契約上の要求事項の順守

目的　情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

18.2 情報セキュリティのレビュー

目的　組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

箇条18　順守

- 旧版
  「15 順守」
  　「15.1 法的要求事項の順守」
  　「15.2 セキュリティ方針及び標準の順守、並びに技術的順守」
- 改定版
  「18 順守」
  　「18.1 法的及び契約上の要求事項の順守」
  　「18.2 情報セキュリティのレビュー」
  - 旧版から大きな変更はない。
  - 旧版では「6.1 内部組織」にあった「6.1.8 情報セキュリティの独立したレビュー」を、改定版で18.2.1に移した。

管理策の新旧対比表

- ISO/IEC JTC 1/SC 27/WG 1で作成したISO/IEC 27001 及び ISO/IEC 27002 それぞれの新旧対比が、SC 27事務局の DIN (Deutsches Institut für Normung) のサイトに掲載されている。
  http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=wg1sd3
  - ISO/IEC 27002 管理策の新旧対比は、1 対 1 対応のものの他、追加、削除、部分的対応など、単純でないものも少なくない。
  - ISO/IEC 27002:2005 の管理策を実施している組織がISO/IEC 27002:2013 へ移行する場合、上記新旧対比を参考にしつつ、管理策の実施状況について改定版に基づき検証する必要がある。
    - 改定版への移行において本表に基づく管理策番号の置換えだけでは、管理策の実施状況を正確に把握することにはならない。

ISO/IEC 27002 をとりまく規格群（1）

- ISO/IEC 27002 は、より詳細な指針群の基礎に位置付けられる。

ISO/IEC 27002 の箇条、カテゴリ	主な関連規格
13.1 ネットワークセキュリティ管理	ISO/IEC 27033, Network security
15 供給者管理	ISO/IEC 27036, Information security for supplier relationships
16 情報セキュリティインシデント管理	ISO/IEC 27035, Information security incident management
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	ISO/IEC 27031, Guidelines for information and communication technology readiness for business continuity
18.1 法的及び契約上の要求事項の順守	ISO/IEC 29100, Privacy framework
18.2 情報セキュリティの独立したレビュー	ISO/IEC 27007, Guidelines for information security management systems auditing

- 分野別指針
  - ISO/IEC 27002 を包含し、分野別の状況に対応する管理策及び実施の手引を追加
  - ISO/IEC 27011（通信事業）、ISO/IEC 27017（クラウドコンピューティング［開発中］）、など

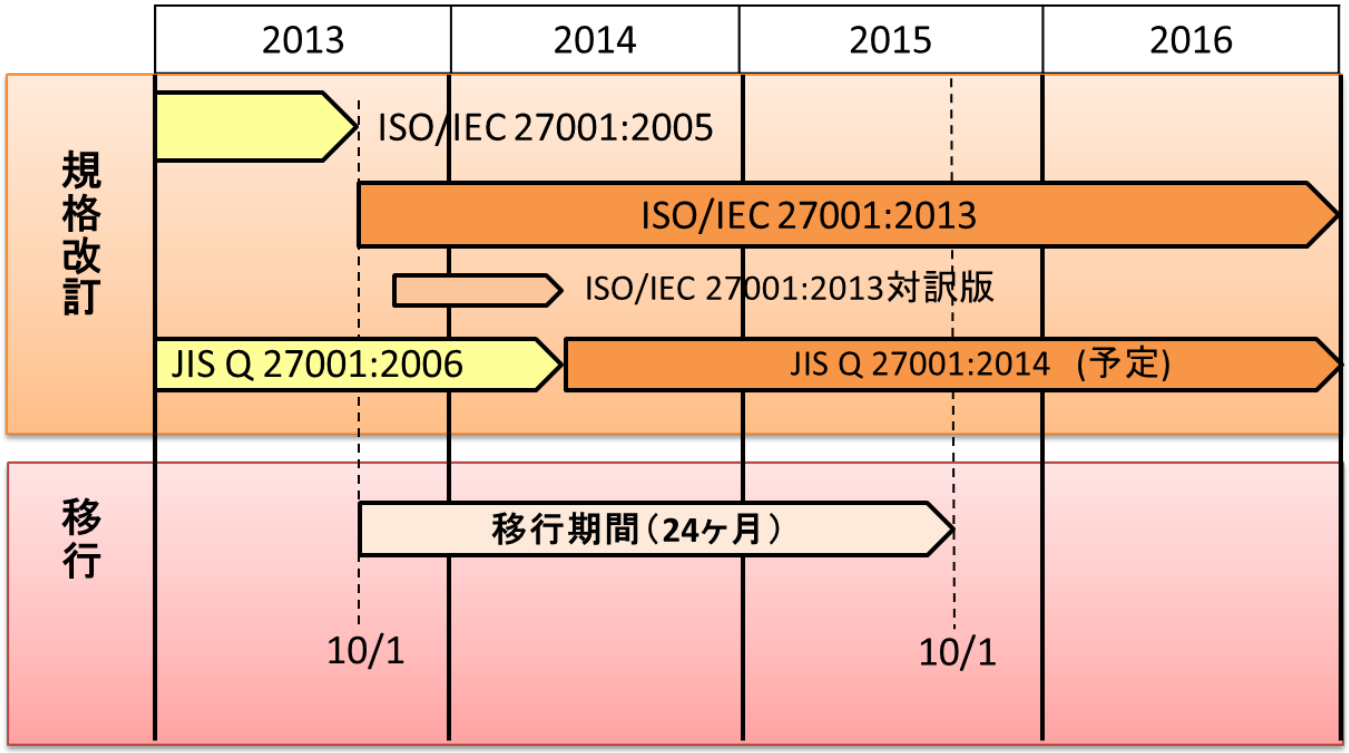
- 分野別指針に基づく「分野別ISMS」の検討
  - 開発中のISO/IEC 27009による

ISO/IEC 27002 をとりまく規格群（2）
セクター別ISMSガイドラインの国際規格化状況

ISO/IEC	**規格タイトル（日本語タイトルは仮訳）**	制定状況
27009	セクター/サービス分野別の第三者の認定された認証のためのISO/IEC27001の利用及び適用 （ISO/IEC 27001**のセクター固有の適用－要求事項**(Sector-specific application of ISO/IEC 27001 – Requirements)）	制定中 （タイトルを変更中）
27010	セクター間及び組織間コミュニケーションのための情報セキュリティマネジメント	制定済み
27011	ISO/IEC27002に基づく通信事業者のための情報セキュリティマネジメントガイドライン	改訂中
27015	金融サービスのための情報セキュリティマネジメントガイドライン	制定済み
27017	ISO/IEC27002に基づくクラウドコンピューティングサービスのための情報セキュリティ管理策の実践規範	制定中
27018	パブリッククラウドコンピューティングサービスのためのデータ保護管理策の実践規範	制定中
27019	エネルギー業界向けプロセス管理システムのためのISO/IEC27002に基づく情報セキュリティマネジメントの指針	制定済み

認証の移行

- 移行の期間はIAFの方針(IAF Resolution 2013-13)に従い、規格発行から2年間(2015年10月1日まで)とする。
- 移行計画のイメージを下図に示す。



27001/27002 改定規格説明会(JSA)　高取氏資料抜粋

認証の移行計画

① JIS Q 27001:2006（ISO/IEC 27001:2005）による初回認証審査（新規の認証）は、ISO/IEC 27001:2013の規格発行後1年以内に登録を完了すること。また2015年10月1日までに、ISO/IEC 27001:2013への移行を完了すること。

② ISO/IEC 27001:2013発行後、認証機関は適用規格としてISO/IEC 27001:2013又はJIS Q 27001:2006（ISO/IEC 27001:2005）のいずれの規格を使用するかについて組織と合意するとともに、適用規格として使用した規格を審査計画、審査報告書及び認証文書で明記すること。また、ISO/IEC 27001:2013による初回審査の場合には、認証機関はISO/IEC 27001:2013に基づいて認証審査をするための手順が完備していること。

③ JIS Q 27001:2006（ISO/IEC 27001:2005）で認証登録されている組織に対しては、ISO/IEC 27001:2013発行後の維持審査（サーベイランス）又は再認証審査において、ISO/IEC 27001:2013への移行のための差分審査を含むことが望ましい。

認証の移行に関する留意事項

① 既存又は新規の組織に対する審査計画は、ISO/IEC 27001:2013の規格発行後6ヶ月経過時点からは適用規格としてISO/IEC 27001:2013を含むことが望ましい。

② 規格の改訂内容に対する差分審査を行うだけの目的で認証機関が追加の訪問を実施することは、要求しない。

③ JIS Q 27001:2006（ISO/IEC 27001:2005）で認証登録されている既存の組織については、ISO/IEC 27001:2013規格中の変更内容に不適合を指摘することがあっても、当該不適合は移行期間の終了までは登録に対して不利益な影響を及ぼさないこと。

④ 認証文書に記載されている規格名称は、当該審査計画で記載されていた版と整合していること。通常は既存の組織に対してISO/IEC 27001:2013を適用した結果に基づき、認証機関が認証文書を新しくすることであり、この認証文書はそれまでの認証のサイクルを変更しないことが望ましい。ただし、完全な更新審査を実施した場合はこの限りではない。

JIS Q 27001:2006の改訂に関する取扱い

① ISO/IEC 27001:2013の発行に伴い、JIS Q 27001:2006の改訂も予定されている。JIS Q 27001:2006の改訂版が発行されたら、このJIS規格に基づく認証が望まれる。

② 移行の期限は、ISO/IEC 27001:2013と同じ2015年10月1日までとする。

③ JIS Q 27001:2006が改訂されるまでに用いる日本語としては、日本規格協会発行のISO/IEC 27001:2013対訳版を参考とする。

おわりに

1）2013年中に、重要規格（27000/27001/27002）の規格化を終えることができ、JIS化作業に着手できたことにより、国際規格の改版作業からくるISMS認証制度（日本）への影響は少なくすることができたのではないか。

2）国際的な規格の流れからすると、各種の「マネジメントシステム規格」間のギャップをなくし、マネジメントシステム認証のより効率的な取得、運用を推進する方向にある。

3）しかしながら、最近の脅威や発生する事故/事件に鑑みると、ISMS認証の取得は「BASIC」で、組織/企業の独自の環境、及び特性を十分に考慮した、情報セキュリティに関わる総合的な対策（管理策）の適用、運用が望まれるところである。

4）そのために発生する費用についても、適正なものに抑え、より効率的なISMSの運用、実践が期待され、必要な人材育成、専門家との連携も鍵となると考える。