JIS Q 27001：2014への対応について

一般財団法人 日本情報経済社会推進協会
情報マネジメント推進センター
センター長　高取　敏夫

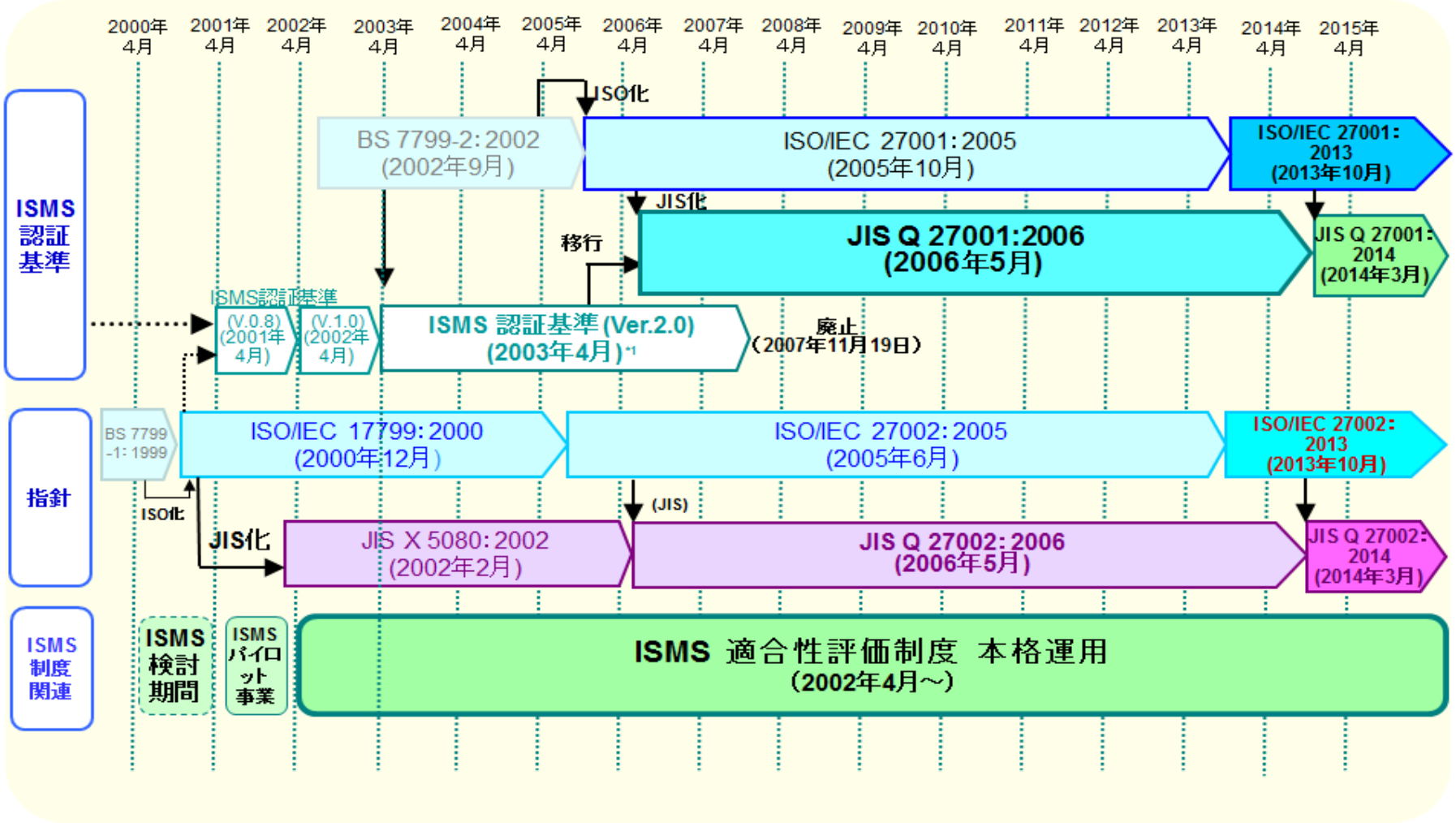
2014年10月3日

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

アジェンダ

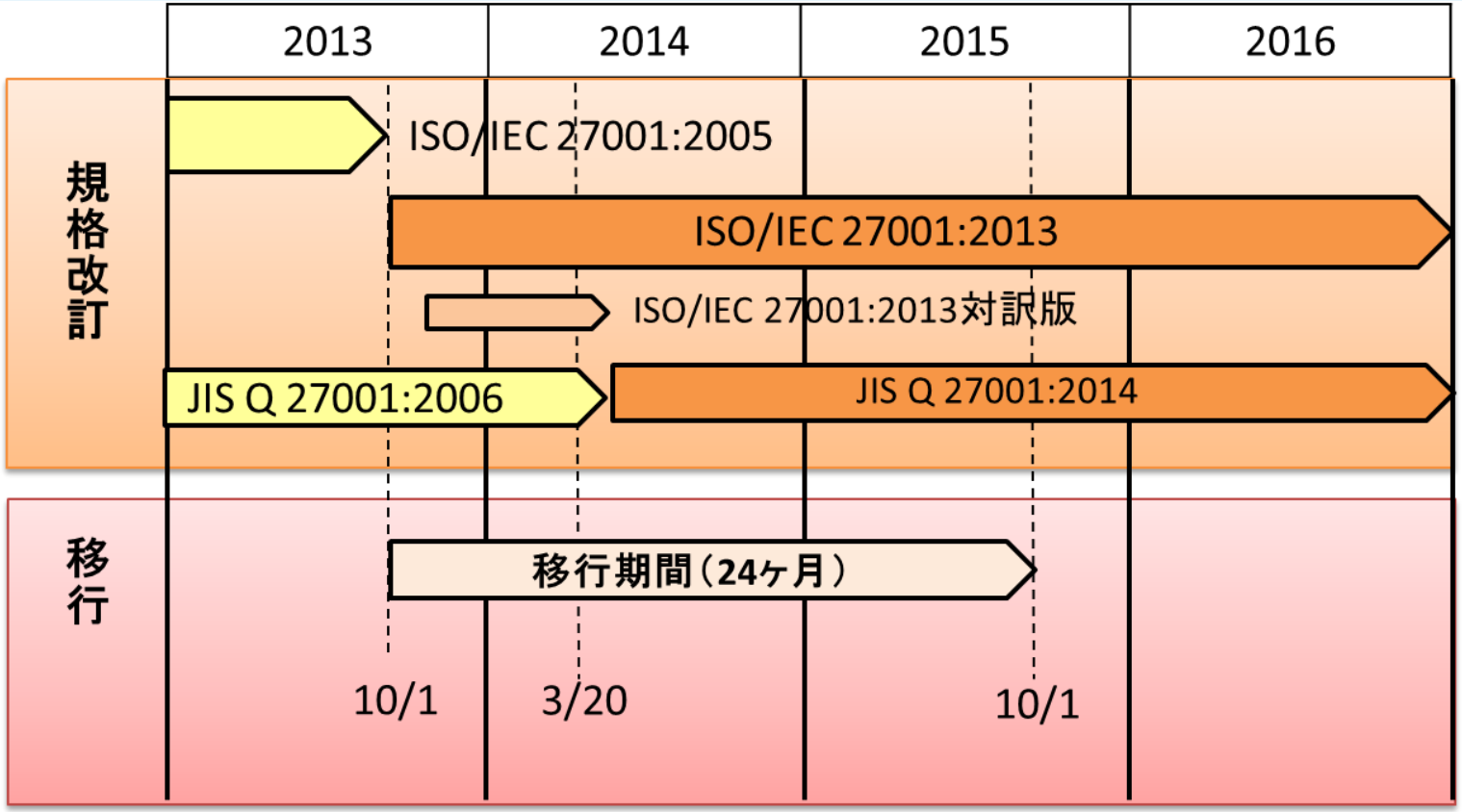
- ISMS認証の移行
- JIS Q 27001：2014改正の概要

ISO規格及びJIS規格制定の経緯



ISMS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。



ISMS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、JIS Q 27001:2014（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。

ISMS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、JIS Q 27001:2014（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27001:2014（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 27001:2014改正の概要

- JIS Q 27001：2014改正の意義
- JIS Q 27001：2014とJIS Q 27001：2006との対比
- JIS Q 27001：2006 附属書Aとの対応
- JIS Q 27001:2014 改正のポイント(1)～(9)
- ISO MSS共通要素の概要
- ISO MSS共通要素の各章の構成
- JIS Q 27001:2014の構成(1)～(3)
- JIS Q 27001：2014の各箇条の関係

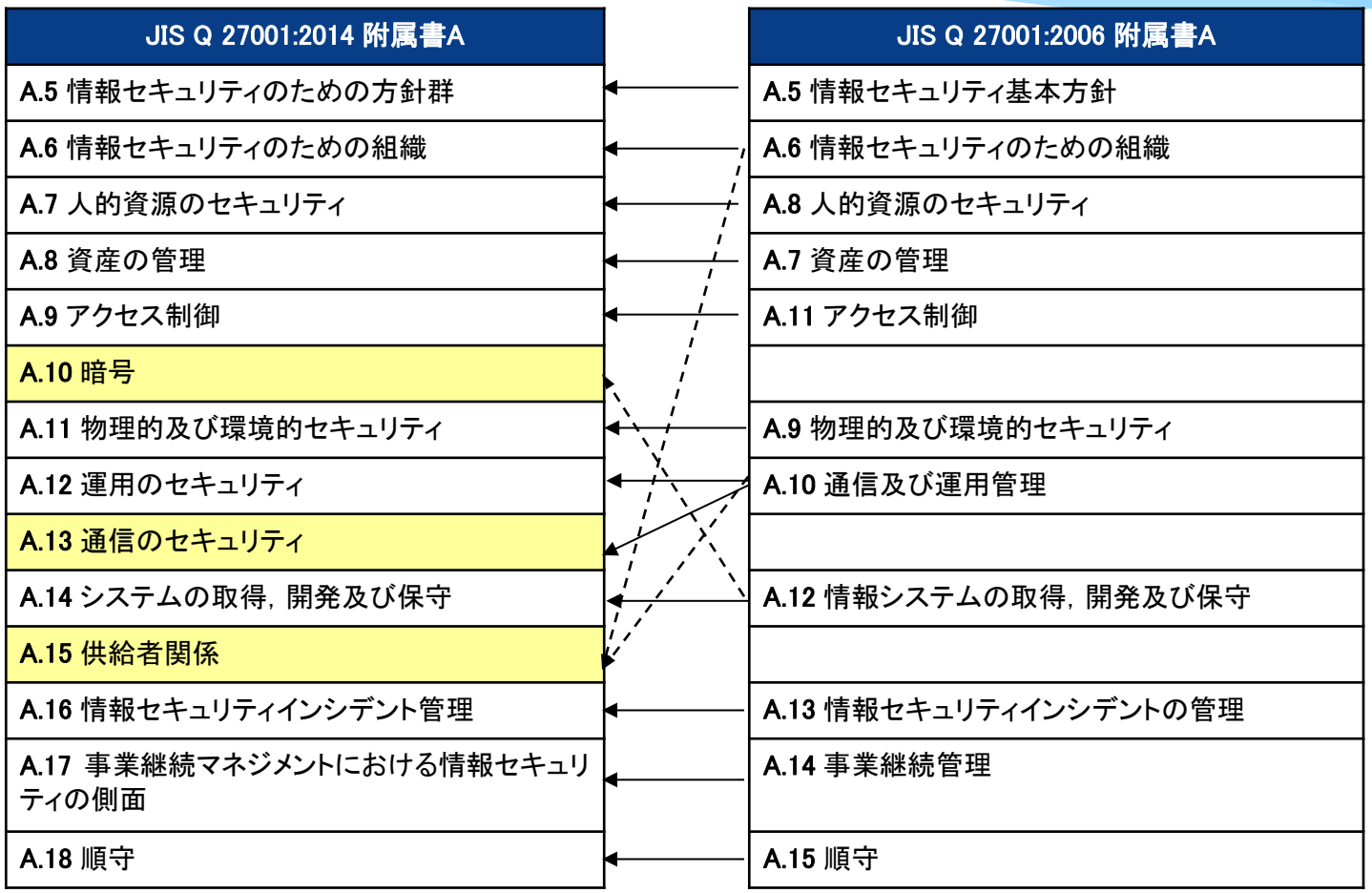
JIS Q 27001:2014 改正の意義

- JIS Q 27001:2014は、ISO MSSの共通要素を取り込んだタイプAのマネジメントシステム規格となっているので、効果的に組織のマネジメントシステムを構築・運用することが可能である。
- 組織が運用する他のマネジメントシステムとの親和性も高まり、ISMS導入の一層の効果が期待できる。
- 既にISMS認証を取得されている組織は、現在の仕組みを大幅に変更することはないが、従前に比べ計画段階における経営的な視点での見直しが必要である。

JIS Q 27001:2014と JIS Q 27001:2006との対比

JIS Q 27001:2014	JIS Q 27001:2006
0 序文	0 序文
1 適用範囲	1 適用範囲
2 引用規格	2 引用規格
3 用語及び定義	3 用語及び定義
4 組織の状況	4 情報セキュリティマネジメントシステム
5 リーダーシップ	5 経営陣の責任
6 計画	6 ISMS内部監査
7 支援	7 ISMSのマネジメントレビュー
8 運用	8 ISMSの改善
9 パフォーマンス評価	附属書A(規定) 管理目的及び管理策
10 改善	附属書B(参考) OECD原則及びこの規格
附属書A(規定) 管理目的及び管理策	附属書C(参考) 規格の比較
参考文献	参考文献

JIS Q 27001:2006 附属書Aとの対応



JIS Q 27001:2014 改正のポイント(1)

- ISO MSS共通要素の適用

- JIS Q 27001:2014は、ISO MSS共通要素を適用して開発されたマネジメントシステム規格となっており、その上で、情報セキュリティに不可欠なISMS固有の要求事項が規定されている。
- リスクアセスメント及びリスク対応のプロセスは、ISO 31000：2009（JIS Q 31000:2010)との整合が考慮されている。
- 情報セキュリティ方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしなければならない。

JIS Q 27001:2014 改正のポイント(2)

適用範囲

- JIS Q 27001:2006では、「事業・組織・所在地・資産・技術の特徴の見地から、ISMSの適用範囲及び境界を定義し、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も含めるものとする。」としていた。
- JIS Q 27001:2014「4.3 ISMSの適用範囲の決定」では、「その境界及び適用可能性を決定し、適用範囲を決定するとき、外部及び内部の課題、利害関係者のニーズ及び要求事項、インタフェース及び依存関係を考慮しなければならない。」とし、より広い観点からISMSの適用範囲及び境界を定義することを求める内容となった。

JIS Q 27001:2014 改正のポイント(3)

予防処置の概念

- JIS Q 27001:2006「8.3予防処置」項では、「組織は、ISMSの要求事項に対する不適合の発生を予防するために、起こり得る不適合の原因を除去する処置を決定しなければならない。」としていた。
- JIS Q 27001:2014「組織及びその状況の理解」では、マネジメントシステムの目的には、本来、予防的なツールとしての役割をもつために、組織の目的に関連し、意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を広い視点で評価をすることを要求している。さらに「6.1 リスク及び機会に対処する活動」においても、広い視点でISMSが意図した成果を達成できること確実にすることを要求している。

JIS Q 27001:2014 改正のポイント(4)

法令及び規制の要求事項

- JIS Q 27001:2006では、「法令及び規制の要求事項並びに契約上のセキュリティ義務を明確にし、これを扱う。」としていた。
- JIS Q 27001:2014「4.2 利害関係者のニーズ及び期待の理解」では、「組織は、ISMSに関連する利害関係者及びその利害関係者の情報セキュリティに関連する要求事項を決定しなければならない。」とし、「利害関係者の要求事項には、法的及び規制要求事項並びに契約上の義務を含めてもよい。」としている。
- 組織が利害関係者の利益のため、適用される法令及び規制の要求事項を特定し、常に最新化させ、周知し、順守状況を意識して取り組むことは当然の要求事項であると考えられる。

JIS Q 27001:2014 改正のポイント(5)

- リスク及び機会
  - JIS Q 27001:2014「6.1 リスク及び機会に対処する活動」の6.1.1では、「ISMSの計画を策定するとき、組織は、4.1に規定する課題及び4.2に規定する要求事項を考慮し、次の事項のために対処する必要があるリスク及び機会を決定しなければならない。」としている。
  - ISO 31000:2009（JIS Q 31000:2010）によると、リスクは「目的に対する不確かさの影響」のことであり、「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乖離すること」としている。
  - 組織の事業リスクを理解する上では、ISO 31000「5.3 組織の状況の確定」を考慮して、「4.1 組織及びその状況の理解」との整合を確保することが、リスクマネジメントの重要なポイントとであると考えられる。

JIS Q 27001:2014 改正のポイント(6)

- リスクアセスメント
  - JIS Q 27001:2006では、「リスクアセスメントに対する組織の取組み方を定義する。」としていた。
  - JIS Q 27001:2014では、リスクアセスメントに関する要求事項の記述レベルをISO 31000:2009（JIS Q 31000:2010）に合わせたと考えられる。そのため、要求事項の上位レベルの記述（情報セキュリティリスクを特定する）には、CIA（機密性、完全性及び可用性）の視点でリスクを特定することが要求されており、JIS Q 27001:2006に沿ったリスクアセスメントも具体的な方法の1つとして引き続き有効である。さらにJIS Q 27001:2014では、リスクアセスメントの選択の幅が広がり、組織の実情に沿ったリスクアセスメントの方法の適用が可能になった。

JIS Q 27001:2014 改正のポイント(7)

情報セキュリティリスク対応

- JIS Q 27001:2006では、「リスク対応のための選択肢を特定し、評価する。」適切な管理策は、リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために選択・導入し、この選択には、法令、規制及び契約上の要求事項と同じく、リスク受容基準も考慮する。適用宣言書及びリスク対応計画を作成する。リスク対応計画及び残留リスクについて、経営陣の承認を得る」こととしていた。
- JIS Q 27001:2014「6.1.3 情報セキュリティリスク対応」では、「組織は、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。これには、リスクアセスメントの結果を考慮して、適切な情報セキュリティリスクの対応の選択肢を選定し、選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。決定した管理策を附属書Aに示す管理策と比較し、必要な管理策が見落とされていないことを検証し、適用宣言書及び情報セキュリティリスク対応計画を作成する。情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について、リスク所有者の承認を得る」こととしている。

JIS Q 27001:2014 改正のポイント(8)

文書化した情報

- JIS Q 27001:2006 では、「ISMSが要求する文書は、保護し、管理しなければならない。また、必要な管理活動を定義するために、文書化した手順を確立しなければならない。」としていた。
- JIS Q 27001:2014「7.5 文書化した情報」では、「ISMS及びこの規格で要求されている文書化した情報及びISMSの有効性のために必要であると組織が決定した文書化した情報は、確実に管理しなければならない。」としている。ここでの文書化した情報の定義は、組織が管理し、維持するよう要求されている情報、及びそれが含まれている媒体としている。
- JIS Q 27001:2006では、「文書と記録の管理」が区別され異なる要求事項でしたが、JIS Q 27001:2014 では、「文書化した情報の管理」としてまとめられた。

JIS Q 27001:2014 改正のポイント(9)

- 附属書 A（管理目的及び管理策）
- JIS Q 27001:2006では、「附属書Aの中から～管理目的及び管理策を選択」することが要求されていたが、ISO/IEC 27001:2014では、「必要な全ての管理策を決定」し、この管理策を「附属書Aに示す管理策と比較し、必要な管理策が見落とされていないことを検証する」ことが求められるようになった。これにより、組織は附属書Aだけではなく、任意の管理策群を適用することも可能となった。
- JIS Q 27002:2014では、従来の規格と比較すると、近年の脅威の変化に対応すべくその範囲を広め、管理策の記載に関しては表現をやや抽象化することで、いくつかの管理策を統合させ、詳細な管理策については、関連するISO/IEC 27000ファミリ規格を参照させるようになった。

ISO MSS共通要素の概要

- ISOマネジメントシステム規格の増加を受けて、ISOによりマネジメントシステム規格（MSS: Management System Standard）間の整合化が検討された。その結果、2012年5月に「ISO/IEC専門業務用指針 第1部 統合版ISO補足指針」「附属書SL（規定）マネジメントシステム規格の提案」として発行され、今後全てのMSSはこれを適用することになった。
- 附属書SLの狙いは、「合意形成され、統一された、上位構造、共通の中核となるテキスト、並びに共通用語及び中核となる定義(MSS共通要素)を示すことによって、ISOマネジメントシステム規格の一貫性及び整合性を向上させることである。」とされている。
- MSS共通要素は、この附属書SLに規定されている。詳細については、次のURLを参照されたい。
  http://www.jsa.or.jp/itn/pdf/shiryo/isohosoku_taiyaku1405.pdf

ISO MSS共通要素の各章の構成

1　適用範囲

2　引用規格

3　用語及び定義

4　組織の状況
- 4.1　組織及びその状況の理解
- 4.2　利害関係者のニーズ及び期待の理解
- 4.3　XXXマネジメントシステムの適用範囲の決定
- 4.4　XXXマネジメントシステム

5　リーダーシップ
- 5.1　リーダーシップ及びコミットメント
- 5.2　方針
- 5.3　組織の役割、責任及び権限

6　計画
- 6.1　リスク及び機会への取組み
- 6.2　XXX目的及びそれを達成するための計画策定

7　支援
- 7.1　資源
- 7.2　力量
- 7.3　認識
- 7.4　コミュニケーション
- 7.5　文書化した情報

8　運用
- 8.1　運用の計画及び管理

9章　パフォーマンス評価
- 9.1　監視、測定、分析及び評価
- 9.2　内部監査
- 9.3　マネジメントレビュー

10　改善
- 10.1　不適合及び是正処置
- 10.2　継続的改善

（注記　共通テキストのXXXには、分野固有の修飾語が入ります。
ISO/IEC 27001の場合には、情報セキュリティが入ります。）

JIS Q 27001:2014の構成（1）

ISO/IEC 27001:2013（JIS Q 27001:2014）	概略
0 序文	ISMSは、リスクマネジメントを適用することで、情報セキュリティを確保し、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。 ISMSを、組織のプロセス及びマネジメント構造全体の一部として、組み込む。 この規格で示す要求事項の順序は、その重要性を反映するものでもなく、またそれを実施する順序を示すものでもない。
1 適用範囲	箇条4から箇条10に規定する要求事項の例外はみとめられない。
2 引用規格	ISO/IEC 27000を適用する。
3 用語及び定義	ISO/IEC 27000で規定されている用語及び定義を適用する。
4 組織の状況	
4.1 組織及びその状況の理解	組織における状況を理解することが重要である。外部・内部の課題の決定については、ISO 31000:2009の5.3の外部・内部の状況を参照する。
4.2 利害関係者のニーズ及び期待の理解	関連する利害関係者の特定とその要求事項を決定する。利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めることが考慮される。
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の適用範囲を決めるために、その境界及び適用可能性を決定する。このとき、組織は、4.1に規定する外部及び内部の課題、4.2に規定する要求事項を考慮する。
4.4 情報セキュリティマネジメントシステム	組織は、ISMSを確立、実施、維持及び継続的に改善する。
5 リーダーシップ	
5.1 リーダーシップ及びコミットメント	トップマネジメントは、ISMSに関するリーダーシップとコミットメントを実証する。
5.2 方針	トップマネジメントは、情報セキュリティ方針を確立する。
5.3 組織の役割、責任及び権限	トップマネジメントは、情報セキュリティに関連する役割に対して、責任及び権限を割り当て、伝達することを確実にする。

JIS Q 27001:2014の構成(2)

ISO/IEC 27001:2013(JIS Q 27001:2014)	概略
6 計画	
6.1 リスク及び機会に対処する活動	
6.1.1 一般	ISMSの計画を策定するとき、組織は、4.1の課題及び4.2の要求事項を考慮し、リスク及び機会を決定する(ISMSがその意図した成果を達成できることを確実にするため、望ましくない影響を防止又は低減するため、継続的改善を達成するため)。
6.1.2 情報セキュリティリスクアセスメント	情報セキュリティのリスク基準を確立し、リスクを特定・分析・評価する。
6.1.3 情報セキュリティリスク対応	情報セキュリティリスク対応のプロセスを定め、リスク対応の選択肢を選定し、管理策を決定、適用宣言書及び情報セキュリティリスク対応計画を策定する。
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	組織は、関連する部門・階層において、情報セキュリティ目的を確立し、それらを達成するための計画を策定する。
7 支援	
7.1 資源	組織は、ISMSの確立、実施、維持及び継続的改善に必要な資源を決定、提供する。
7.2 力量	情報セキュリティパフォーマンスに影響を与える業務を組織の管理下で行う人々に必要な力量を決定、力量を備えることを確実にする。
7.3 認識	組織の管理下で働く人々は、情報セキュリティ方針、ISMSの有効性に対する自らの貢献、及びISMS要求事項に適合しないことの意味に関して認識をもつ必要がある。
7.4 コミュニケーション	組織は、ISMSに関する内部及び外部のコミュニケーションを実施する必要性を決定する。
7.5 文書化した情報	組織は、規格が要求する文書化した情報、及びISMSの有効性のために必要であると組織が決定した文書化した情報をISMSに含む。

JIS Q 27001:2014の構成(3)

ISO/IEC 27001:2013(JIS Q 27001:2014)	概略
8 運用	
8.1 運用の計画及び管理	組織は、情報セキュリティ要求事項を満たすため、及び6.1で決定した活動を実施するために、必要なプロセスを計画、実施、管理する。また、組織は、6.2で決定した情報セキュリティ目的を達成するための計画を実施する。
8.2 情報セキュリティリスクアセスメント	組織は、あらかじめ定めた間隔で、又は重大な変更の提案・重大な変化の発生のとき、情報セキュリティリスクアセスメントを実施する。
8.3 情報セキュリティリスク対応	組織は、8.2に対するリスク対応を実施する。
9 パフォーマンス評価	
9.1 監視、測定、分析及び評価	組織は情報セキュリティパフォーマンス及びISMSの有効性を評価する。
9.2 内部監査	組織は、あらかじめ定めた間隔で内部監査を実施する。
9.3 マネジメントレビュー	トップマネジメントは、あらかじめ定めた間隔で、ISMSをレビューする。
10 改善	
10.1 不適合及び是正処置	組織は、不適合が発生した場合、その不適合に対処し、その原因を除去するための必要な処置を実施し、是正処置の有効性をレビューする。
10.2 継続的改善	組織は、ISMSの適切性、妥当性及び有効性を継続的に改善する。

JIS Q 27001:2014 の各箇条の関係

5. リーダーシップ　5.1 リーダーシップ及びコミットメント　5.2 方針　5.3 組織の役割、責任及び権限

4. 組織の状況

4.1 組織及びその状況の理解

・組織をとりまく内外の課題

4.2 利害関係者のニーズ及び期待の理解

・ISMSに関連する利害関係者の要求事項

4.3 適用範囲の決定

・適用範囲の境界及び適用可能性

6. 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般
・リスク及び機会の決定

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

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

8. 運用

8.1 運用の計画及び管理
・6.1、6.2 を実施

8.2 情報セキュリティリスクアセスメント
・6.1.2 を実施

8.3 情報セキュリティリスク対応
・6.1.3 を実施

9. パフォーマンス評価

9.1 監視、測定、分析及び評価
情報セキュリティパフォーマンス及びISMSの有効性を評価

9.2 内部監査
有効に実施され、継続的に維持されているかを評価

9.3 マネジメント・レビュー
継続的改善の機会、及びISMSの変更の必要性を決定

10. 改善

10.1 不適合及び是正処置

10.2 継続的改善

7. 支援　7.1 資源　7.2 力量　7.3 認識　7.4 コミュニケーション　7.5 文書化した情報

ISMS認証の分野拡大を進め、

今後他のマネジメントシステムとの統合化を図り、

ISMS認証の付加価値の向上に努めたい。

〈問い合わせ先〉

一般財団法人 日本情報経済社会推進協会
情報マネジメント推進センター
TEL: 03-5860-7570
FAX: 03-5573-0564
Web: http://www.isms.jipdec.or.jp/