ISMS　2013での変更点

S.Fushimi
Sofdela LLC

1

ISMSの概要

- ISMSは、ISO（国際標準化機構）とIEC（国際電気標準会議）の合同技術委員会であるJTC1内の専門委員会SC27が制定した、セキュリティマネジメントに関する国際規格です
- 最初のものが、ISO/IEC 17799規格として2001年に制定されたのち、2005年に内容改訂及びISO/IEC 27001への番号改変がされ、さらにその次の改訂が2013年に行われます（ました）
- ここでは、2013年改定の概要を説明します（訳語は仮のものです）

2

改訂の概要

- 形式上のもの
  - 他のマネージメントシステム（ISO9000等）と同じ文書内構造とした（ISO全体の足並みを揃えるという要請による）
- 内容上のもの
  - リスクについての観点は、一般的なリスク管理標準であるISO 31000:2009に依拠した
  - 従って、リスク分析の手法は、従来の「（資産表に基づく、）脅威＊脆弱性＊影響」の手法でなくてもよい（例えば、想定事故評価など）――ただし、機密性・完全性・可用性の3視点は維持
  - 改善の視点は、PDCAサイクルを強調せず、他の観点も許容（31000では他の側面を併記）（継続的改善実施ということが重要）
  - 管理策決定は、附属書に記載された項目から「選ぶ」のではなく、自律的に組織のコンテキストに基づいて管理策群を識別した後に、その視点に漏れがないかチェックするために附属書を参照すると明記された
  - 管理策の例示である附属書Aでは、情勢変化に合わせて構成を改善するとともに、管理的な側面での管理策にしぼり、技術的な管理策は他の規格の分担とした

3

規格の文書内構造の変化

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(ISO/IEC 27000のみ)
3 用語及び定義	3 用語及び定義(27000による)
4 情報セキュリティマネジメントシステム	4 組織コンテキスト
5 経営陣の責任	5 指導性
6 ISMS内部監査	6 計画
7 ISMSのマネジメントレビュー	7 支援
8 ISMSの改善	8 運用
	9 有効性評価
	10 改善
附属書A 管理目的及び管理策	附属書A 管理目的及び管理策
附属書B 附属書C	

全体的には他のマネージメントシステム文書と同じ構造とした

リスク評価に関する記述を含む点が他のマネジメントシステムとは大きく異なる

ISO/IEC 27002と整合したもの

4

適用宣言書（「計画」）

- 27001:2013は、全体に、「文書」類は、特定の文書名を要求しないという観点に立っている
- 「適用宣言書」（SOAと略記）だけは例外で、リスク分析・対応の決定の結果として、管理策の選択結果を明示するこの文書が必要としている
- 従来よく見られた、「とにかく附属書の管理策とどう対応しているか明示する（「選択」する）」というものとは異なる
- セキュリティ担当者にとっては、以前より作成が難しくなった感がある（うまく作れば、現場にとっては対応するのが現実的になったと思われる）
- なお、「ISMS基本方針」という文書化は不要となった（情報セキュリティ基本方針は必要）――日本の実務では、「ISMSマニュアル」を作ることが多いので、あまり影響ないが

5

適用範囲など（「組織コンテキスト」）

- ISMSの適用範囲（スコープ）は、従来から、組織が決定できたが、その決め方にはガイドがあった（「事業・組織・所在地・資産・技術の特徴」）
- 改訂後は抽象的な規定となった（ISMS成果達成に関連する事案、関係者の情報セキュリティ要求、組織の活動のインタフェースや依存関係などを勘案してISMSのスコープ、境界を決定する）
- リスク分析の前提として、組織の目的、ISMS実施能力、関係者からの要請や期待事項の把握が必要

6

リスク分析（「計画」）

- リスク分析は、ISO 31000:2009に依拠することを基本としたが、その枠内で独自の記述も多くある
- 旧規格のように、まず情報資産を特定し、それに対して脅威＊脆弱性＊影響分析をするという流れはなくなった
  - リスク（許容、評価実施）の基準確立
  - リスク評価結果の再現性確保
  - 各リスクとそのオウナーの識別
  - 各リスクの分析（想定される結果、頻度）とレベル決定
  - 分析結果と基準の比較による評定
- 「リスク対応」方策を管理策に展開し、それらをまとめて「適用宣言書」が作成される
- さらに「セキュリティ目標」と、その「達成計画」に展開する

7

リスク評価と対応（「運用」）

- 必要なセキュリティプロセス実装
- 運用上のセキュリティの計画とその実装・管理
- 定期的なリスク再評価
- リスク対応の計画、実施と対応時情報の文書化

8

能力と設備（「支援」）

- ISMS実施上の資源の確保
- セキュリティ要員能力の確保
- 全般的な意識向上（気づき）
- コミュニケーション（報告・連絡等）
- 文書化と文書管理・配布

9

改善の視点（「有効性評価」「改善」）

- 改善に関連する要素には次のものがある
  - 「支援」、その他のISMSの要素の有効性確保策
  - マネージメントレビュー
  - 内部監査
  - 測定と有効性評価
  - 不適合に対する是正活動、原因究明活動
  - 不適合と是正活動の記録
  - ISMSの継続的改善

10

トップダウンの視点（「指導性」）

- 経営陣が、情報セキュリティ基本方針（ポリシー）や、セキュリティ上の組織の役割を決定することは旧規格と同様

11

新規格での管理策ドメイン

A.5	情報セキュリティ基本方針	
A.6	情報セキュリティのための組織	
A.7	人的資源のセキュリティ	
A.8	資産の管理	
A.9	アクセス制御	
A.10	暗号	新規独立
A.11	物理的及び環境的セキュリティ	
A.12	運用セキュリティ	分割
A.13	通信セキュリティ	分割
A.14	システム取得・開発及び保守	
A.15	供給者関係	新規独立
A.16	情報セキュリティインシデントの管理	
A.17	事業継続管理の情報セキュリティの側面	
A.18	順守	

合計３ドメイン増えた

12

管理策 (1/13)

番号	タイトル	対応する旧項目
A.5	情報セキュリティ基本方針	A.5
A.5.1	情報セキュリティの管理の方向	A.5.1
A.5.1.1	情報セキュリティの基本方針	A.5.1.1
A.5.1.2	情報セキュリティの基本方針のレビュー	A.5.1.2
A.6	情報セキュリティのための組織	A.6
A.6.1	内部組織	A.6.1
A.6.1.1	情報セキュリティの役割と責任	A.6.1.3, A.8.1.1
A.6.1.2	職務の分割	A.10.1.3
A.6.1.3	関係当局との連絡	A.6.1.6
A.6.1.4	専門組織との連絡	A.6.1.7
A.6.1.5	プロジェクト管理における情報セキュリティ	（新規）
A.6.2	モバイル機器及びテレワーキング	A.11.7
A.6.2.1	モバイル機器の基本方針	A.11.7.1

13

管理策 (2/13)

番号	タイトル	対応する旧項目
A.6.2.2	テレワーキング	A.11.7.2
A.7	人的資源のセキュリティ	A.8
A.7.1	雇用前	A.8.1
A.7.1.1	選考	A.8.1.2
A.7.1.2	雇用条件	A.8.1.3
A.7.2	雇用期間中	A.8.2
A.7.2.1	経営陣の責任	A.8.2.1
A.7.2.2	情報セキュリティの意識向上、教育及び訓練	A.8.2.2
A.7.2.3	懲戒手続	A.8.2.3
A.7.3	雇用の終了及び変更	A.8.3
A.7.3.1	雇用の終了又は変更の責任	A.8.3.1
A.8	資産の管理	A.7
A.8.1	資産に対する責任	A.7.1

14

管理策 (3/13)

番号	タイトル	対応する旧項目
A.8.1.1	資産目録	A.7.1.1
A.8.1.2	資産の管理責任者	A.7.1.2
A.8.1.3	資産利用の許容範囲	A.7.1.3
A.8.1.4	資産の返却	A.8.3.2
A.8.2	情報の分類	A.7.2
A.8.2.1	情報保護レベルの分類	A.7.2.1
A.8.2.2	情報のラベル付け	A.7.2.2
A.8.2.3	情報の取扱い	A.10.7.3
A.8.3	媒体の取扱い	A.10.7
A.8.3.1	取外し可能な媒体の管理	A.10.7.1
A.8.3.2	媒体の処分	A.10.7.2
A.8.3.3	物理的媒体の配送	A.10.8.3
A.9	アクセス制御	A.11

15

管理策 (4/13)

番号	タイトル	対応する旧項目
A.9.1	アクセス制御に対する業務上の要求事項	A.11.1
A.9.1.1	アクセス制御方針	A.11.1.1
A.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	A.11.4.1
A.9.2	利用者アクセスの管理	A.11.2
A.9.2.1	利用者登録と登録削除	A.11.2.1, A.11.5.2
A.9.2.2	利用者アクセスのパラメータ設定	（新規）
A.9.2.3	特別アクセス権の管理	A.11.2.2
A.9.2.4	利用者の秘密認証情報の管理	A.11.2.3
A.9.2.5	利用者アクセス権のレビュー	A.11.2.4
A.9.2.6	アクセス権の削除又は調整	A.8.3.3
A.9.3	利用者の責任	A.11.3
A.9.3.1	利用者の秘密認証情報の利用	A.11.3.1
A.9.4	システム及び応用プログラムのアクセス制御	A.11.5, A.11.6

16

管理策 (5/13)

番号	タイトル	対応する旧項目
A.9.4.1	情報へのアクセス制限	A.11.6.1
A.9.4.2	セキュリティに配慮したログオン手順	A.11.5.1, A.11.5.5, A.11.5.6
A.9.4.3	パスワード管理システム	A.11.5.3
A.9.4.4	特権ユーティリティの使用	A.11.5.4
A.9.4.5	プログラムソースコードへのアクセス制御	A.12.4.3
A.10	暗号	（新規独立）
A.10.1	暗号による管理策	A.12.3
A.10.1.1	暗号による管理策の利用策	A.12.3.1
A.10.1.2	鍵管理	A.12.3.2
A.11	物理的及び環境的セキュリティ	
A.11.1	セキュリティを保つべき領域	A.9.1
A.11.1.1	物理的セキュリティ境界	A.9.1.1
A.11.1.2	物理的入退管理策	A.9.1.2

17

管理策 (6/13)

番号	タイトル	対応する旧項目
A.11.1.3	オフィス、部屋及び施設のセキュリティ	A.9.1.3
A.11.1.4	外部及び環境の脅威からの保護	A.9.1.4
A.11.1.5	セキュリティを保つべき領域での作業	A.9.1.5
A.11.1.6	受渡し場所	A.9.1.6
A.11.2	装置	A.9.2
A.11.2.1	装置の設置及び保護	A.9.2.1
A.11.2.2	サポートユーティリティ	A.9.2.2
A.11.2.3	ケーブル配線のセキュリティ	A.9.2.3
A.11.2.4	装置の保守	A.9.2.4
A.11.2.5	資産の移動	A.9.2.7
A.11.2.6	構外にある装置のセキュリティ	A.9.2.5
A.11.2.7	装置の安全な処分又は再利用	A. 9.2.6
A.11.2.8	無人状態にある利用者装置	A.11.3.2

18

管理策 (7/13)

番号	タイトル	対応する旧項目
A.11.2.9	クリアデスク・クリアスクリーン方針	A.11.3.3
A.12	運用セキュリティ	A.10（分割）
A.12.1	運用の手順及び責任	A.10.1
A.12.1.1	操作手順書	A.10.1.1
A.12.1.2	変更管理	A.10.1.2
A.12.1.3	容量・能力の管理	A.10.3.1
A.12.1.4	開発施設、試験施設及び運用施設の分離	A.10.1.4
A.12.2	悪意のあるコードからの保護	A.10.4
A.12.2.1	悪意のあるコードに対する管理策	A.10.4.1
A.12.3	バックアップ	A.10.5
A.12.3.1	情報のバックアップ	A.10.5.1
A.12.4	ログと監視	A.10.10
A.12.4.1	事象ログ取得	A.10.10.1

19

管理策 (8/13)

番号	タイトル	対応する旧項目
A.12.4.2	ログ情報の保護	A.10.10.3
A.12.4.3	実務管理者及び運用担当者の作業ログ	A.10.10.4, A.10.10.3
A.12.4.4	クロックの同期	A.10.10.6
A.12.5	運用ソフトウェアの管理	A.12.4
A.12.5.1	運用システムのインストール	A.12.4.1
A.12.6	技術的脆弱性の管理	A.12.6
A.12.6.1	技術的脆弱性の管理	A.12.6.1
A.12.6.2	ソフトウェアインストールの制限	（新規）
A.12.7	情報システムの監査に対する考慮事項	A.15.3
A.12.7.1	情報システムの監査に対する管理策	A.15.3.1
A.13	通信セキュリティ	A.10（分割）
A.13.1	ネットワークセキュリティ管理	A.10.6
A.13.1.1	ネットワーク管理策	A.10.6.1

20

管理策 (9/13)

番号	タイトル	対応する旧項目
A.13.1.2	ネットワークサービスのセキュリティ	A.10.6.2
A.13.1.3	ネットワークの領域分割	A.11.4.5
A.13.2	情報の移転	A.10.8
A.13.2.1	情報移転の方針及び手順	A.10.8.1
A.13.2.2	情報移転に関する合意	A.10.8.2
A.13.2.3	電子的メッセージ通信	A.10.8.4
A.13.2.4	秘密保持又は非開示合意	A.6.1.5
A.14	システム取得、開発及び保守	A.12
A.14.1	情報システムのセキュリティ要求事項	A.12.1
A.14.1.1	セキュリティ要求事項の分析及び仕様化	A.12.1.1
A.14.1.2	公開ネットワーク上の応用サービス	A.10.9.1, A.10.9.2
A.14.1.3	応用サービストランザクションの保護	A.10.9.3
A.14.2	開発、支援プロセスにおけるセキュリティ	A.12.5

21

管理策 (10/13)

番号	タイトル	対応する旧項目
A.14.2.1	セキュリティに配慮した開発方針	（新規）
A.14.2.2	システム変更管理手順	A.12.5.1
A.14.2.3	運用プラットフォーム変更後の応用ソフトウェアの技術的レビュー	A.12.5.2
A.14.2.4	パッケージソフトウェアの変更に対する制限	A.12.5.3
A.14.2.5	セキュリティに配慮したシステム技術の原則	（新規）
A.14.2.6	セキュリティに配慮した開発環境	（新規）
A.14.2.7	外部委託による開発	A.12.5.5
A.14.2.8	システムセキュリティ試験	（新規）
A.14.2.9	システムの受入れ	A.10.3.2
A.14.3	試験データ	（新規）
A.14.3.1	システム試験データの保護	A.12.4.2
A.15	供給者関係	（新規独立）
A.15.1	供給者関係のセキュリティ	A.6.2

22

管理策 (11/13)

番号	タイトル	対応する旧項目
A.15.1.1	供給者関係の情報セキュリティ方針	A.6.2.3
A.15.1.2	供給者との合意におけるセキュリティの記述	A.6.2.3
A.15.1.3	ICTサプライチェイン	（新規）
A.15.2	供給者サービスの受渡し管理	A.10.2
A.15.2.1	供給者サービスの監視及びレビュー	A.10.2.2
A.15.2.2	供給者サービスの変更に対する管理	A.10.2.3
A.16	情報セキュリティインシデントの管理	A.13
A.16.1	情報セキュリティインシデントの管理及び改善	A.13.1, A.13.2
A.16.1.1	責任及び手順	A.13.2.1
A.16.1.2	情報セキュリティ事象の報告	A.13.1.1
A.16.1.3	情報セキュリティの弱みの報告	A.13.1.2
A.16.1.4	情報セキュリティ事象の評価と決定	（新規）
A.16.1.5	情報セキュリティインシデントへの対応	（新規）

23

管理策 (12/13)

番号	タイトル	対応する旧項目
A.16.1.6	情報セキュリテイインシデントからの学習	A.13.2.2
A.16.1.7	証拠の収集	A.13.2.3
A.17	事業継続管理の情報セキュリティの側面	A.14
A.17.1	情報セキュリテイ継続	A.14.1
A.17.1.1	情報セキュリテイ継続の計画	A.14.1.2
A.17.1.2	情報セキュリテイ継続の実装	（新規）
A.17.1.3	情報セキュリテイ継続の検証、レビュー及び評価	A.14.1.5
A.17.2	冗長性	（新規）
A.17.2.1	情報処理設備の可用性	（新規）
A.18	順守	A.15
A.18.1	法的及び契約上の順守	A.15.1
A.18.1.1	適用法令及び契約上の要求事項の識別	A.15.1.1
A.18.1.2	知的財産権	A.15.1.2

24

管理策 (13/13)

番号	タイトル	対応する旧項目
A.18.1.3	記録の保護	A.15.1.3
A.18.1.4	プライバシーと個人特定情報の保護	A.15.1.4
A.18.1.5	暗号を用いた管理策の規制	A.15.1.6
A.18.2	情報セキュリティのレビュー	A.15.2
A.18.2.1	情報セキュリティの独立したレビュー	A.6.1.8
A.18.2.2	セキュリティ方針及び標準の順守	A.15.2.1
A.18.2.3	技術的順守レビュー	A.15.2.2

旧規格での管理策総数 １３３項目 → 減少 → 新規格での管理策総数 １１４項目

25

改訂スケジュール

- 2013/春 DIS案 承認
- 2013/秋 FDIS案 承認（予定）
- 2013/年末～2014/初頭　規格 発行（予測）

- 認証制度への適用（通常の場合）
  - 国際規格発行後にJIS規格も変更される（予定）
  - 規格発行後は、新規／更新の認証は新規格による
  - 従来取得してある認証は有効期間中継続される

（注　本プレゼンは、FDIS文書内容に基づいています）

26