

改訂情報セキュリティ規格の 中小組織への有効活用

情報セキュリティ専門監査人 &
情報セキュリティ研究プロジェクト合同研究会

報告者：(株)ピーアンドアイ 長野加代子

はじめに

■ 情報セキュリティマネジメントシステム—要求事項

ISO/IEC 27001:2013 (JIS Q 27001:2014)



ISO/IEC 27001:2005 (JIS Q 27001:2006)

■ 情報セキュリティ管理策の実践のための規範

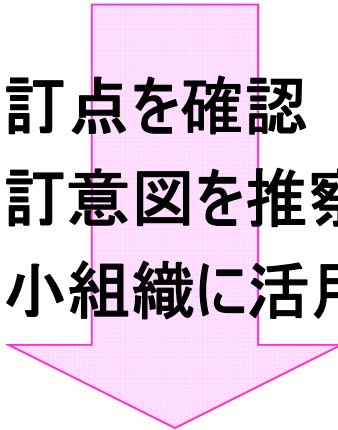
ISO/IEC 27002:2013 (JIS Q 27002:2014)



ISO/IEC 27002:2005 (JIS Q 27002:2006)

本研究の目的と手順

■ 改訂された情報セキュリティ規格

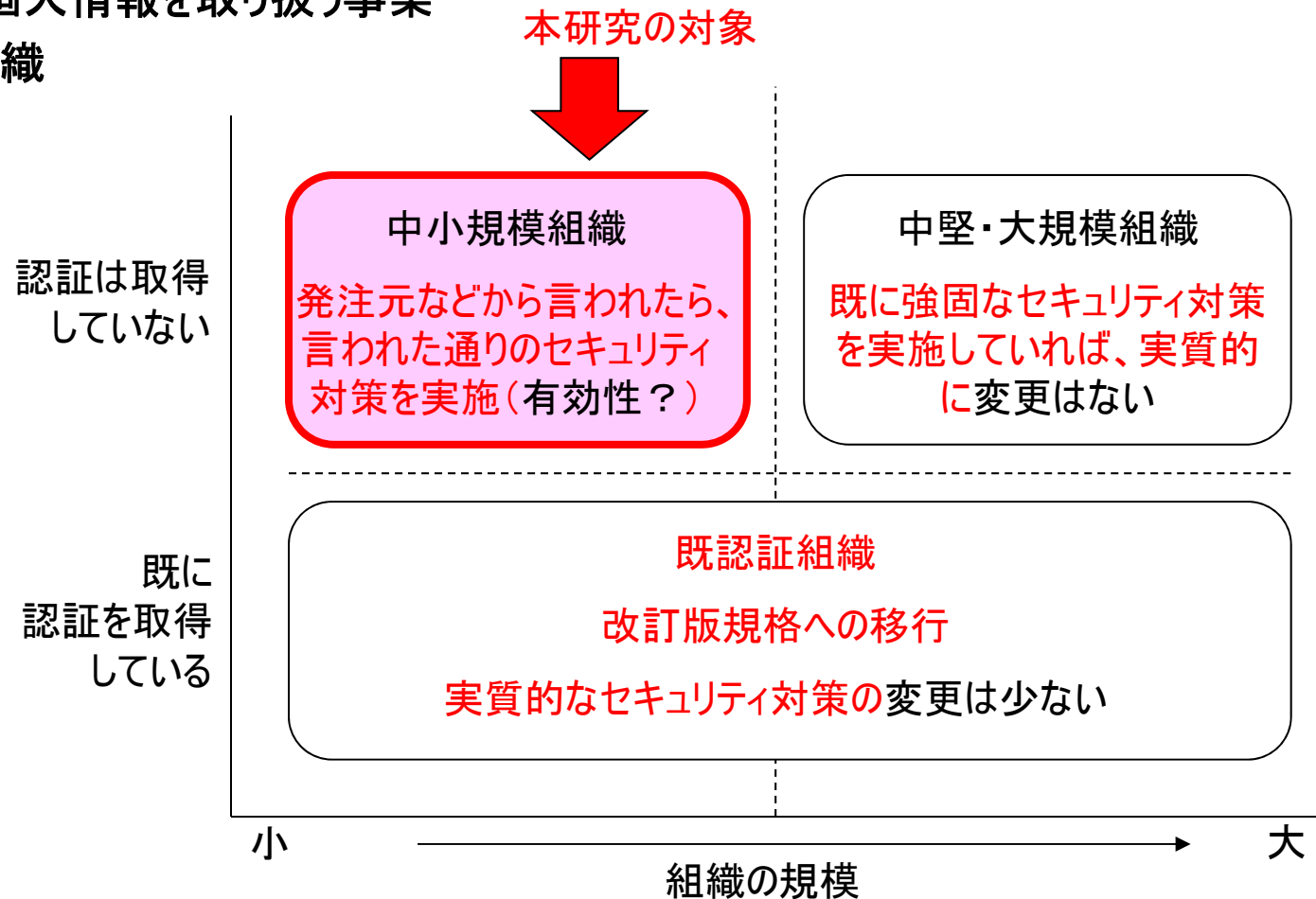
- 
- ①改訂点を確認
 - ②改訂意図を推察
 - ③中小組織に活用できる点を掘り出し

改訂点を深読みして、
新たな解釈を加えて、
活用できる点を抽出する

■ 中小組織への活用法を提案

研究の対象とする組織

- ・ISMS認証未取得
- ・ISMS認証取得そのものを目的としない
- ・企業秘密・個人情報を取り扱う事業
- ・中小規模組織



ISO/IEC27001,27002の主な改訂

- 27001(本文)の章立て
 - 「ISO/IEC 専門業務用指針」付属書SL
- リスクアセスメントの部分
 - ISO31000 リスクマネジメントーガイドライン
- 新しい管理策の追加ー27002(管理策)
 - 「セキュア開発」、「サプライチェーン」、「冗長性」

改訂意図の理解

☆ **共通化**によって複数のISOを運用するときの使い勝手を良くする

☆ 時代に合った《管理策》とする

★ よりビジネス志向で実際に有効な価値のある規格とする(推測)

ISO/IEC27001の改訂点

活用できそうな改訂点

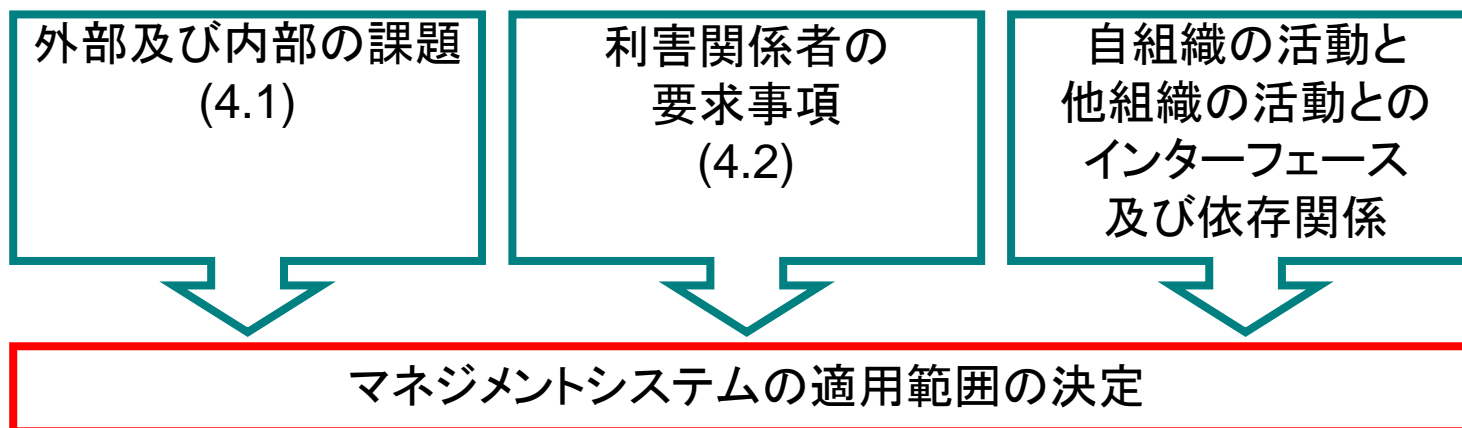
- ★ **組織の状況**
 - 組織の内部・外部の課題、利害関係者のニーズを把握
- ★ **リーダーシップ**
 - トップマネジメントが情報セキュリティ方針、情報セキュリティ目的を確立
 - 事業プロセスへのMS要求事項の統合
- ★ **計画**
 - 課題及び要求事項を考慮して、リスク及び機会を決定
 - リスクアセスメント:ISO 31000 に規定するリスクの概念をベース
- **支援**
 - 「文書」「記録」の用語を「文書化した情報」に統一
- **運用**
 - 定期的なリスクアセスメント、リスク対応、リスク対応計画の実施、見直し
- **パフォーマンス評価**
 - 監視、測定、分析及び評価
- **改善**
 - 予防処置の削除(MSの運用自体が予防的なツール)

①組織の状況

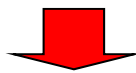

2005では序文
⇒2013では要求事項

- 4 組織の状況
- 4.1 組織及びその状況の理解
 - マネジメントシステムの意図した成果(intended outcome)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の決定
- 4.2 利害関係者のニーズ及び期待の理解
 - 利害関係者と、その利害関係者の要求事項、法規制要求事項を決定
- 4.3 マネジメントシステムの適用範囲の決定

↳ ISO 31000 5.3.1
「組織の外部及び内部の状況の確定」



①組織の状況の深読み

- 何故ISMSを導入するのか・・・意図した成果
 - ⇒内外の課題を解決し、利害関係者のニーズ・期待に応える
- 
- 自社の「課題」を明確にする、自社の「導入目的」を決定する
- 当然のこと・・・でも見失いがち ⇒ 明確にしておく
- 未取得の組織・・・「どこから手を付けたら良いかわからない」
 - 既取得の組織・・・「MSを回すことに気を取られて、形骸化する」
- 
- これらに、回答を与える

②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


- ISMSに関するリーダーシップ及びコミットメントを**実証**
 - a)情報セキュリティ方針、**情報セキュリティ目的**の確立 ⇔ **戦略的方針**
 - b) ISMS要求事項と**組織のプロセスの統合**
 - e) ISMS が**「意図した成果」**を達成
 - h)関連した管理層が、リーダーシップを発揮できるように支援する

■ 5.2 方針

- 「方針」を確立 …… 組織の目的に対して適切
「目的」を含む

②リーダーシップの深読み

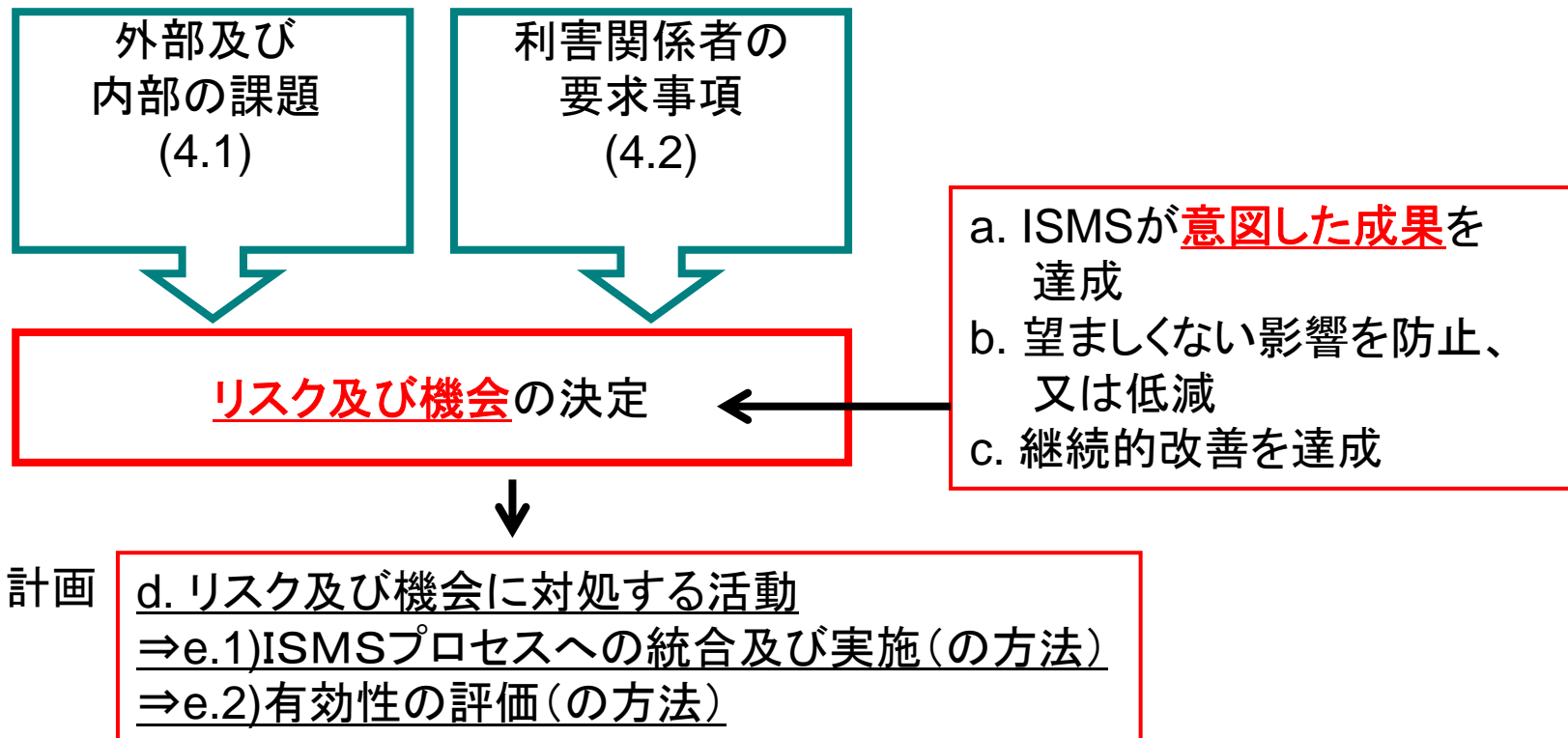


- 経営陣の役割が強化されている
 - リーダーシップが追加、実証を要求
 - 経営の戦略的な方向性と合致する、方針、目的の決定
 - 組織のプロセスへのISMS要求事項の統合
 - 事業プロセス(経営)にマネジメントシステムを統合する
 - 業務プロセス(実務)に情報セキュリティ対策を統合する
 - 現状の課題: トップの関与が弱い、
セキュリティ目的が組織の戦略と合致していない、
マネジメントシステムが経営と分離、セキュリティ対策が業務と分離
(推測)
- 
- リーダーシップの発揮によって、有効性が高まる(はずだ)
 - 業務プロセス(実務)に情報セキュリティ対策を組み込むことが、有効に機能させるためには、重要である(と考えられる)

統合されたプロセス

③計画（リスク及び機会に対処する活動）

- 6 計画
- 6.1 リスク及び機会に対処する活動
- 6.1.1 一般



③計画(リスク及び機会に対処する活動)の深読み

- **リスクと機会を決定し、それに対する計画を立てる**
 - 「4.1組織及びその状況の理解」に対応し、計画(、と実施)について規定
 - 予防処置
 - プロセスへの統合・有効性の評価
- リスク＝「**意図した成果**」の達成を阻害するリスク
- 機会＝ポジティブ＝「**意図した成果**」の達成を促進する機会
 - 例:クラウド＝可用性向上(Pos)、機密性低下(Neg)、トレードオフ
 - 事業上の機会、改善の機会の両方を含む

- **自社の目的・目標**に合わせたISMSを計画・実行する

強調

③計画(情報セキュリティリスクアセスメント)

- リスクアセスメントのプロセスを定めて適用する
 - リスク受容基準とリスクアセスメントを実施する基準
 - 手順(プロセス)
- リスクの特定
 - CIAの喪失のリスク、リスク所有者
- リスクの分析
 - 生じた場合の結果、起こりやすさ、リスクレベル
- リスクの評価
 - リスク基準との比較、対応の優先順位付け



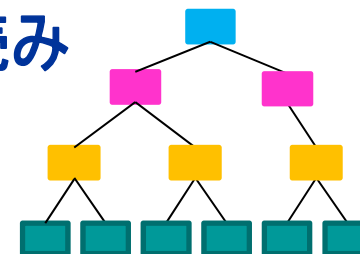
③計画(情報セキュリティリスクアセスメント)

- ISO/IEC 27001:2013のリスクアセスメント
 - 6.1.2d) 情報セキュリティリスクを特定
(情報のCIA喪失リスクを特定、リスク所有者を特定)

- ISO 31000リスクマネジメントのリスクアセスメント、リスク対応
 - 5.4.2 リスク特定
組織の目的(≒目標)の達成を、実現、促進、妨害、阻害、加速、遅延するリスクを包括的に特定

- ISO 31000流に表現すると・・・ ← ISO 31000と整合
 - ①「セキュリティの目標」を定める
 - ②目標に対するリスク特定・分析・評価
 - ③目標に沿ったリスク対応(セキュリティ対策選択)

③計画（情報セキュリティリスクアセスメント）の深読み



- 従来どおりのボトムアップ方式（詳細分析）でもよいが、ISO 31000流に、トップダウン方式での分析も可能
- 資産の個々のリスクではなくて、目的・目標を損なうリスクをトップダウン方式でアセスメントする



- 目的・目標を損なわなければ、個々の資産はリスクアセスメントの対象とする必要はない
- 結果的には「重要な情報資産を特定してリスクアセスメントすることと同じになる“はず”

負荷軽減

まとめ

- 「組織の状況を把握し、期待・要求事項を把握し、トップマネジメントで組織の戦略に合った「目的」を決定し、リスクアセスメントを実施し、管理策を決定し、実業務のプロセスに管理策を組み込み、そして意図した成果を達成しているかを評価する」ことが情報セキュリティの有効性を高める、ということが、考察できる。
- 「目的」、「意図した成果」に焦点をあてることで、有効でかつコストパフォーマンスの高いセキュリティ対策が取れる

中小組織への活用

有効な活用

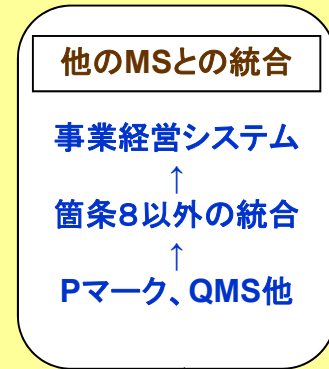
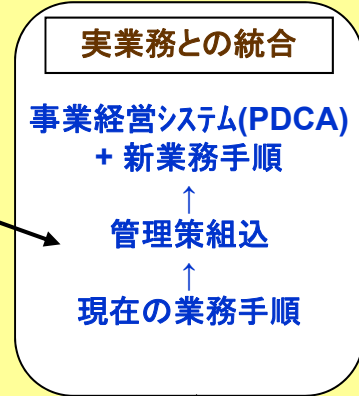
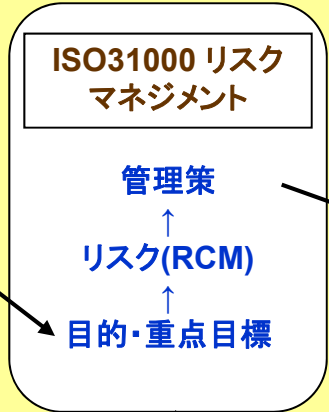
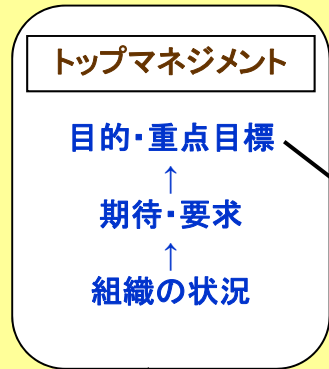
コストパフォーマンス

システム監査
有効に活用しているかを確認
有効な情報セキュリティ導入

ISO審査
規格適合性
管理策有効性
MS有効性

(マネジメントシステムの有効性)

(管理策の有効性)



- 4.1 外部・内部の課題決定
- 4.2a) 利害関係者の特定
- 4.2b) 要求事項の特定
- 4.3 適用範囲決定
- 5.1a) 方針・目的、目標確立

- 6.1.2a) リスク基準策定
- 6.1.2b) リスクアセスメント手順
- 6.1.2d) 目標に対するリスクを特定
- 6.1.2e) リスクを分析
- 6.1.2f) リスクを評価
- 6.1.3a) リスク対応を選択
- 6.1.3b) 必要な管理策を選定
- 6.1.3e) リスク対応計画を作成
これらはISO31000を参考
- 6.2 目的、達成計画

- 5.1b) 組織プロセスへの統合
- 6.1.1 リスク/機会に対処する活動
 - a) 意図した成果達成のリスク/機会
 - b) 悪影響防止/低減のリスク/機会
 - c) 継続的改善のリスク/機会
 - d) リスク/機会に対処する活動計画
- 8.1 運用の計画・実施・管理

- 5.1b) 組織プロセスへの統合
- 6.1.1e) 活動のプロセスの統合・実施方法

規格の改訂による監査への影響

- 業務プロセスを監査することによって、情報セキュリティを監査する
- 「情報セキュリティマニュアル」を見るのではなく、現場(=ビジネス)のプロセス(=記録)を見て、セキュリティを監査する
- ⇒ 監査のアプローチが変わってくる(かもしれない)
- ⇒ 監査人は業務を知らなくてはならない
- 事業に役立っているか、によって有効性の評価をする
- ⇒ 監査の視点がかわってくる(かもしれない)

研究会メンバー

- 主査: 齋藤 敏雄(日本大学)
- 植野 俊雄
- 川辺 良和
- 黒川 信弘
- 小谷野 幸夫
- 高野 美久
- 高橋 孝治
- 鳥越 真理子
- 内藤 裕之
- 永井 好和
- 西澤 利治
- 西川 征一
- 水谷 穰
- 山本 孟
- 芳仲 宏
- 長野 加代子