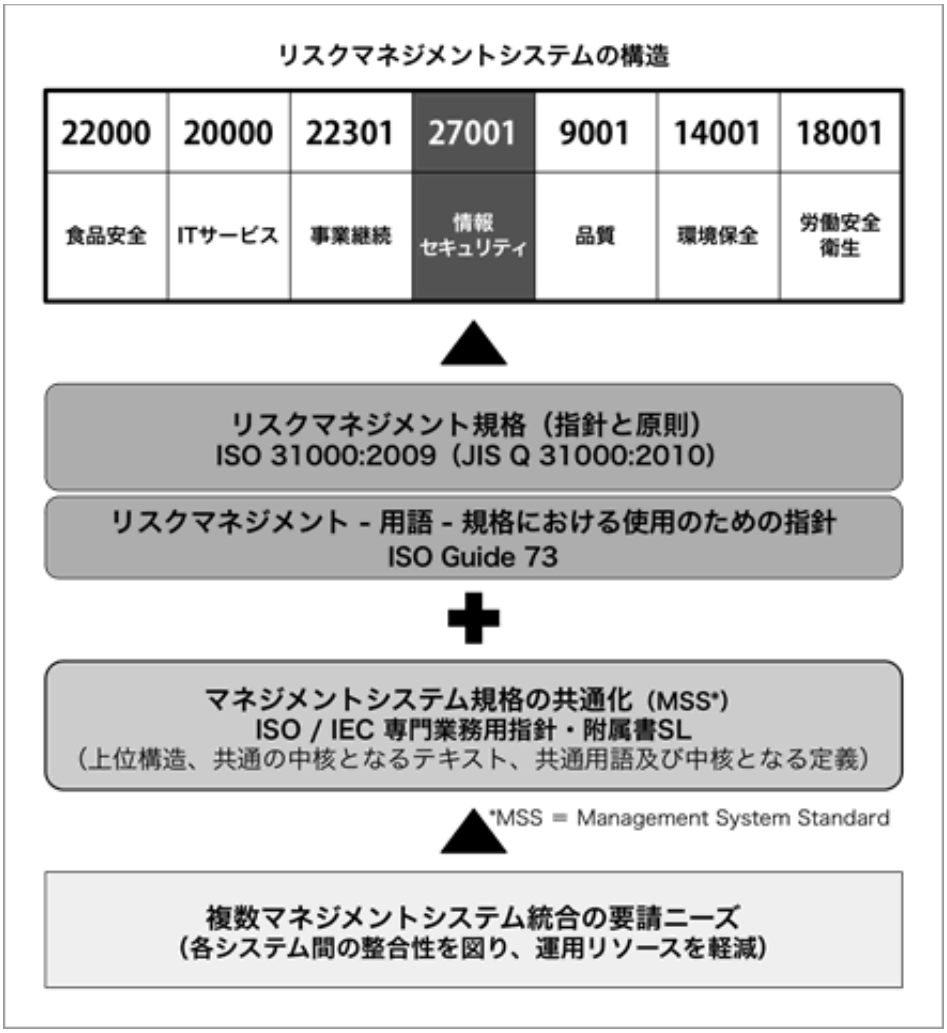
概要

情報セキュリティマネジメントシステム（ISMS）のISO270001規格の構成は、ISOガイド83およびISO31000等の要素が導入されたことによって３層で構成される規格となっています。

この背景には、品質や環境、事業継続、食品衛生等のリスクマネジメントシステムの構造を共通化し、取り組む組織が複数のマネジメントシステムを統合して活用できるようにすること。そして、さまざまな環境変化への対応を可能にすることにあります。

組織が直面するリスクは、情報セキュリティリスクだけではありません。さまざまな側面のリスクが複合的に組織の目的に対して影響を及ぼします。ISO31000をベースとしたリスクマネジメントシステムの活用によって、組織が直面する多側面のリスク対応を幅広く可能性にすることが期待されます。

ISMS（ISO27001）を構築・運用する上で、ISO31000の考え方を学ぶことは、マネジメントシステムを有効活用する上で重要なポイントとなるため、平行して解説します。



学習項目

第１講　規格の背景

1　ISO規格の共通化

2　ISO31000（JIS Q 3100：2010）に基づくリスク概念の導入

3　ISO/IEC 専門業務用指針のポイント

4　ガバナンス強化への取り組み

5　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）

6　規格のポイント

6―1　適用範囲

6―2　予防処置の概念

6―3　法令及び規制の要求事項

6―4　ISO31000（JIS Q 31000：2010：リスクマネジメント―概要）との整合

6―5　リスクと機会

6―6　リスクアセスメント

6―7　情報セキュリティリスク対応

6―8　文書管理

6―9　附属書Ａ（管理目的及び管理策）の利用法

7　ISMS/ISO27001（JIS Q 27001：2014）規格要求事項の全体構成

1　ISO規格の共通化

グローバル版ISO27001は2013年10月1日に、日本国内でのJIS版は2014年3月20日に規格が改定され、リリースされました。

今後、品質や環境、情報セキュリティをテーマとしたISOマネジメントシステム規格は、各マネジメントシステムの共通化を目的としたISOガイド83にしたがって開発されます。そしてISO27001改定も、同様に開発・改定が進められました。

マネジメントシステム規格はISOガイド83「ISO/IEC 専門業務用指針 附属書SL Appendix 2」にしたがって、以下のように改定されました。

（１）HLS（High Level Structure）といわれる共通の規格構造を採用している

HLSとは、次のような規格の章立てのことです。

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

（２）各規格の共通部分の記述は、基本的にHLSの共通項目を採用する

共通項目は、次のような位置づけとなります。

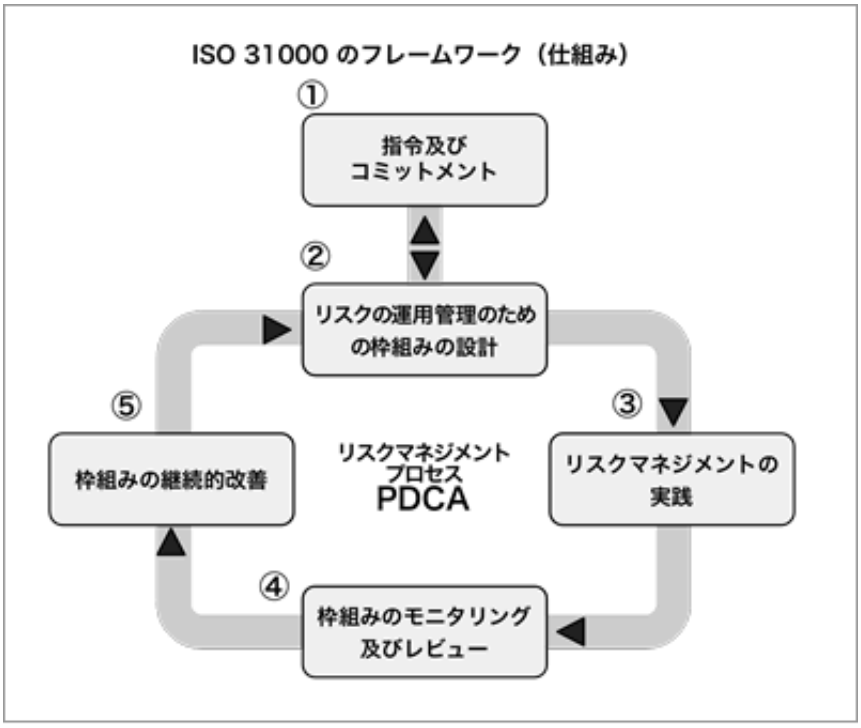
- ○ マネジメントシステム規格は、原則的には、共通項目を適用する
- ○ 1～10の規格項目の順番は変更できない
- ○ 各マネジメントシステム規格によって1～10の規格項目より下位の細分項目の順番は変更することができる
- ○ 各細分項目において、共通項目の意図を変更しない限りでの記述の追加や細分項目の追加などができる

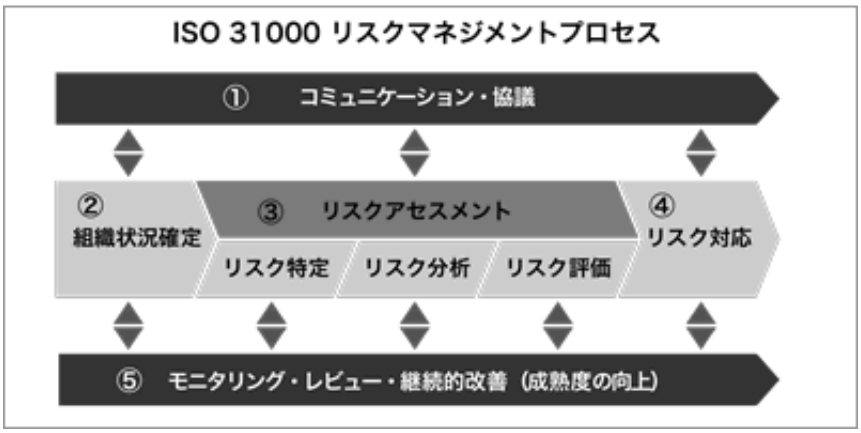
これらによって、マネジメントシステムの活動を支えるマニュアル（基本規程類）はHLSにそって構成されることになります。

2　ISO31000（JIS Q 3100：2010）に基づくリスク概念の導入

原則的にすべてのマネジメントシステムにISO 31000リスクマネジメント規格の概念・原則と指針が導入されました。

情報セキュリティにおいても、エンタープライズリスクマネジメント（ISO 31000）の考え方をベースに構築・運用されることになります。





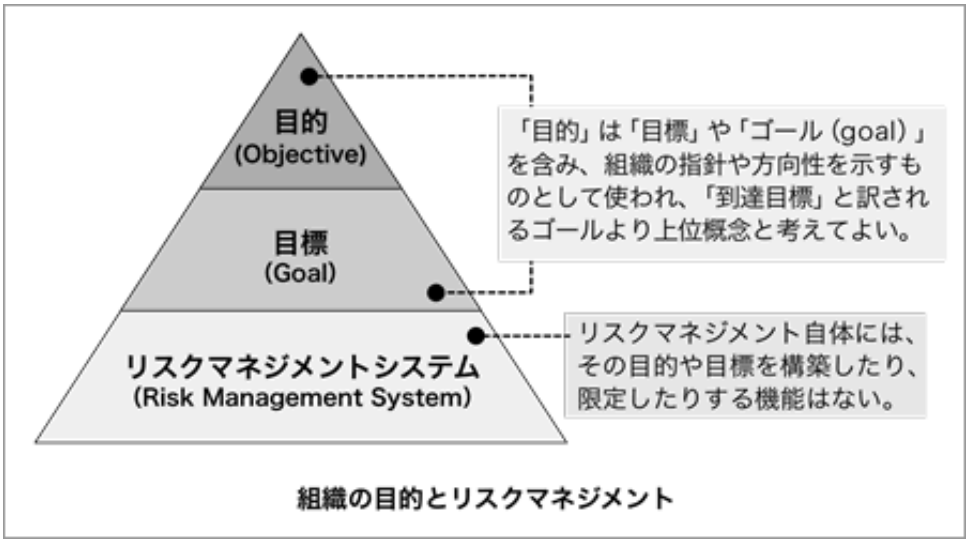
3　ISO/IEC専門業務用指針のポイント

（ISO/IEC 専門業務用指針 附属書SL Appendix 2）

ISO31000や業務用指針附属書SLでは、エンタープライズ（全体的）なリスクマネジメントの視点から、以下のような考え方を採用しています。

■ 組織を取り巻く状況の把握

・組織の内部・外部の課題、利害関係者のニーズを把握する
・現状のレビュー（現状の正しい認識）から、マネジメントシステムを計画する
・「意図した成果」（indeed outcome）＝方針・目的・目標を明確にする



組織の目的とリスクマネジメント

■ 事業プロセスへの統合

・事業プロセスとマネジメントシステム要求事項との統合（トップマネジメントの要求事項）
・事業プロセスとは、生産活動や営利事業だけではなく、管理（間接部門）を含んだ通常の組織活動を含む

■ リスクと機会の決定

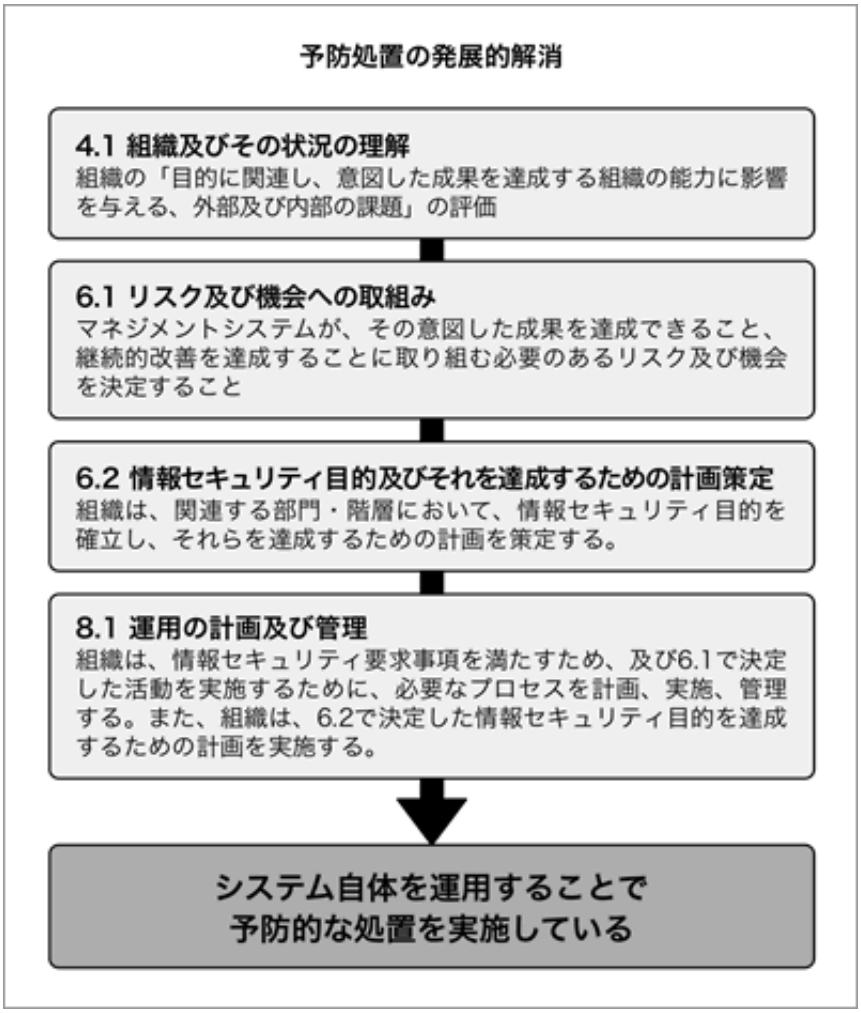
・「リスク」及び「機会」（opportunity）という言葉の導入
・「組織の状況」で特定した課題等を優先順位付けして取り組みを計画
・ISO31000に規定するリスクの概念をベースとする

■ 文書化された情報

・「文書」「記録」の用語を、「文書化された情報」に統一
・「文書」「記録」の電子化に対応（音声・画像・動画等の形式を含む）

■ 予防処置の発展的解消（用語の削除）（参照：附属書SL Appendix 3）

・マネジメントシステム自体が予防的な活動（予防処置）であるため
・予防処置の概念が各箇条に組み込まれた



附属書SL Appendix 3（抜粋）

・この上位構造及び共通テキストには、「予防処置」の特定の要求事項に関する箇条はない。これは、マネジメントシステム活動自体の重要な目的の一つが、予防的なツールとしての役目を持つ為である。

・上位構造及び共通テキストは、4.1において、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」の評価を要求している。 さらに、6.1において、「マネジメントシステムが、その意図した成果を達成できること、継続的改善を達成することに取り組む必要のあるリスク及び機会を決定」することを要求している。

・これらの２つの要求事項はセットで“予防処置”の概念を網羅し、かつ、リスク及び機会を見るような、より広い視点をもつと見なされる。

・6.1 リスク及び機会への取り組み
分野固有の規格では、その分野に固有の「リスク」を定義することもできる。JIS Q 31000では、一部の分野固有の規格で利用できるような「リスク」の定義を示している。さらに、各分野において、正式な「リスクマネジメントアプローチ」に関する必要性を明確化することが望ましい。

・８．運用

この箇条の背景にある概念として、この箇条が、組織のマネジメントシステムの運用だけではなく、組織の全般的な運用にも適用されるということを意図している。

4　ガバナンス強化への取り組み

ISMSを組織の目的達成のために貢献させるためには、利害関係者の理解を得て、ガバナンス活動を通じて実効性の高い組織活動とすることが重要です。

要求事項では、最初に経営的な視点でISMSの役割を特定することが求められます。

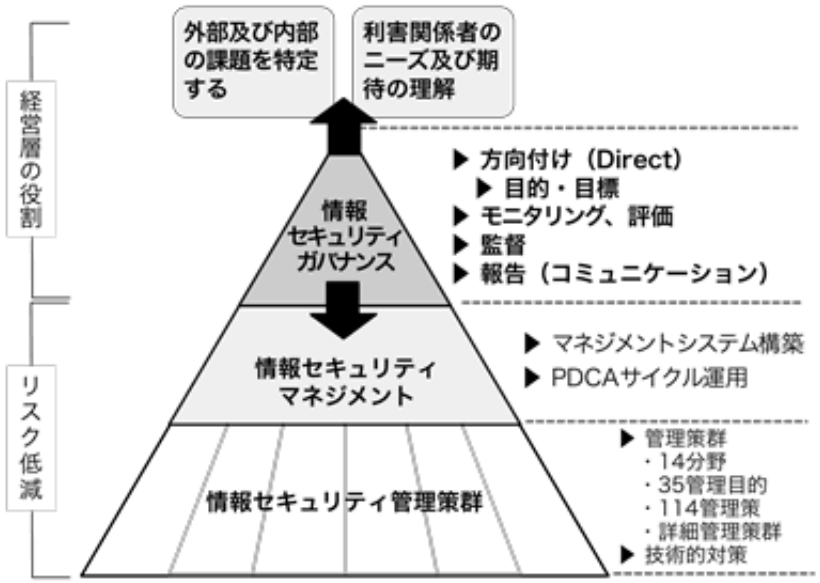
例えば、４．組織の状況では、
4.1 組織及びその状況の理解として、組織の状況を理解するために外部及び内部の課題を特定することが求められています。

また、4.2 利害関係者のニーズ及び期待の理解では、
関連する利害関係者の特定とその要求事項を決定し、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を考慮するが求められています。

また、トップマネジメントは、５．リーダーシップで、
組織の戦略的な方向性を確実にするとともに、リーダーシップとコミットメントを明示する必要があり、その責任に重点が置かれるようになっています。

このように経営的要素が加味された仕組みを構築することで、組織のガバナンス（目的に対する管理機能）を強化するためのマネジメントシステムとして活用することが可能です。

情報セキュリティガバナンスの体系



▶ 情報セキュリティガバナンス

経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを構築・運用することであり、経営層がISMSにおける「コミットメント」を行う上での活動に該当する。

フレームワークは、以下のの5つの活動から構成される

1）経営戦略やリスク管理の観点から行う「**方向付け（Direct）**」
2）状況を可視化する「**モニタリング（Monitor）**」
3）結果を判断する「**評価（Evaluate）**」
4）プロセスが機能していることを確認する「**監督（Oversee）**」
5）結果を利害関係者等に提示する「**報告（Report）**」