# [連載] グループISMS最適化への取り組み

**リコーグループは2004年にISMS認証を取得し、継続審査と更新審査を繰り返し現在に至っています。**
**この間、ステークホルダーの期待と要求に応え適用範囲の見直しを進め、信頼を創り上げてきました。**
**ISMSのモデルを業務に適用し一体化させ、その品質を高めてきた結果としてのISMS認証です。**
**次のステップとして、リコーグループはISMS最適化へ取り組んでいます。**
**ここではリコーグループのISMS最適化への取り組みについて、その概要を示します。**

## 1.グループISMS最適化への取り組み概要

### 1.1. ISMS最適化の目的

ISMS最適化の目的は「ISMSと業務を一体化させ、情報セキュリティレベルを維持した最適なマネジメントシステムを構築する」ことです。これは特に目新しいことではなくISMS導入目的そのものです。

しかし、情報セキュリティレベルが下がり、事件・事故が起きてしまっては、その目的は達成できません。また、形骸化した活動、過剰な施策によるコストの肥大化も考慮しなければなりません。

個人情報漏洩の事件・事故の防止など、機密性に注目してきた情報セキュリティですが、事業継続計画など、情報の完全性・可用性に対する期待・要求は高まっています。

**<コラム>　ISMSはなぜやっているのか**

ところで、ISMSというと、いろいろと機密性を重視した制約や禁止事項が多いように思われがちですが、それがすべてではありません。

もともと、情報は事業に活用するためにあります。

ISMSの基本コンセプトは、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランスよく維持し、改善すること」です。

もっと簡単にいうと、事業目的のために大切な情報および、その情報の管理に責任を持つ人を明確にし、

① 情報を使うべきでない人には制限し（機密性）

② 情報を常に正しい状態に維持し（完全性）

③ 情報を必要とする人が使いたいときに常にアクセスできる（可用性）

ように管理することです。

その際、情報の機密性・完全性・可用性のどれかを損なうようなリスクがあれば、リスクアセスメントデータベースを利用して、リコーグループ共通基準と照らし合わせます。そして、そのリスクをなくすか低減する対策、つまり「リスク対応計画」を施します。

これはISMSのためでなく日常業務そのものであり、ISMSは目的ではなく事業のための手段のひとつといえます。

リコーグループが目指しているのは、安全が保たれた状態で情報の活用を図りながら、意図しない人々への情報の漏えいを防止するという、情報の活用と保護の適切なバランスをとって利益創出を図る「情報セキュリティ経営」という考え方です。

（株）リコーIT/S本部ISMS月次セルフチェックから抜粋

## 1.2. ISMS最適化の目標

この目的を達成するためには、次の目標を設定し完遂する必要があります。

**1. 情報セキュリティレベルの把握**

情報セキュリティレベルを維持するためには、そのレベルが高いのか低いのかを把握します。これは経営陣の関心事である「コストをかけてISMSの認証を取得したが、情報セキュリティレベルはどの程度なのか、事件・事故は本当に起きないのか」の目安となります。

情報セキュリティレベルを把握することにより、その組織の強みや弱みを明確にしたスパイラルアップが望めます。

**2. 内部監査の適合性を基本とした有効性監査への移行**

標準・規定・ルールとの適合性は基本です。これを一歩進めて、有効なマネジメントシステムかどうかを内部監査で見極めます。内部監査がマネジメントシステムの有効性への視点へと移行することで、新たなリスクの発見とその対応に向けたPDCAサイクルを促します。

**3. コストの最適化**

組織ごとの方針や目標管理、活動計画、リスクアセスメント、内部監査などISMSに要するコストの多くは「人の活動」にかけられています。

過剰な施策、形骸化した情報セキュリティ活動、各組織に重複した作業などを見直し、コストの最適化を推進します。

## 1.3.　具体的な取り組み

これらの目標を実現する具体的な取り組みについて説明します。

最適化の対象となる組織を定め、ISMS活動、すなわち方針・目標・活動計画、リスクアセスメント、教育、内部監査、インシデント報告、およびマネジメントレビューなどの仕組みのうち、次の事項について最適化を試みました。

### 1.3.1. ISMS方針・目標・活動計画、ISMS文書、リスクアセスメント方針の共通化

1. 情報セキュリティ統括組織がISMS枠組みとなる方針・目標・活動計画を提供します。各組織はその機能の特性を考慮し、これをそのまま、あるいは修正して使用します。
2. 情報セキュリティ統括組織がISMSに関わる文書を共通化して提供します。各組織でのISMS文書の作成は不要です。
3. 情報セキュリティ統括組織がリスクアセスメント方針も共通化しています。リスクアセスメントすべき情報資産やアセスメントによるリスク対応を最適化します。

### 1.3.2. 情報セキュリティ統括組織による内部監査

1. 情報セキュリティ統括組織の内部監査員資格を持つメンバーが中心となって内部監査を実施します。ISMS最適化に取り組んだ初年度は、最適化の対象となる組織のすべての部署に対して統括組織が内部監査を実施しました。
初年度の統括組織による内部監査は、国内35組織、海外4組織の合計275部署に対して実施されました。
翌年度からは対象組織選択基準を定め、サンプリングによる内部監査を実施しています。
情報セキュリティレベルを維持したコスト最適化の主要な部分です。

2. 情報セキュリティ統括組織による内部監査の特長
情報セキュリティ統括組織による内部監査は以下に示す特長と効果をもたらします。

■情報セキュリティ統括組織の監査員は均一な監査を実施します。
標準化された監査手順、チェックシート、および監査手法を定めて内部監査を実施するため監査基準および監査結果のバラツキは最小です。

■マネジメントシステムの有効性の監査を実施します。
マネジメントシステムのPDCAサイクルが健全に回され、その有効性が確認されているかを監査します。

■被監査組織の情報セキュリティレベルの把握
情報セキュリティレベルは数値化され、例えば「B+（形式的）」、「A-（適切）」などのように標語化し参考としてレーダーチャートで図示します。

■資産の管理責任者のマネジメント（前年度比較）

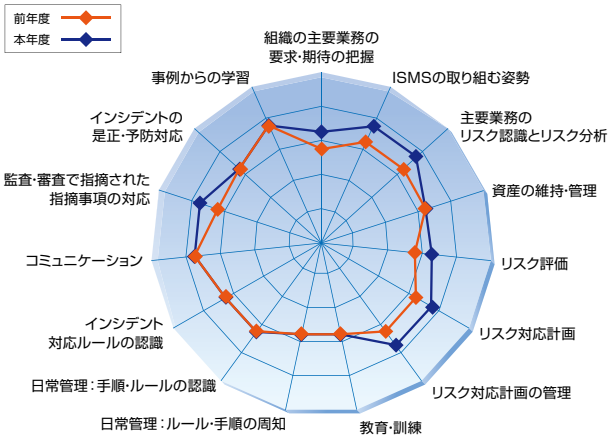


図1-1　マネジメントレベルレベルの把握

■被監査組織のサンプリング
重要な情報資産の有無、事件・事故の発生、前年度のマネジメントシステムの有効性や情報セキュリティレベルなどから被監査組織の部署をサンプリングし監査します。

■各組織で取り組んでいる有効な施策をストロングポイントとして評価し、これを他の組織の内部監査時に紹介しています。ストロングポイントのみならず、不適合の是正処置、インシデントの予防処置や再発防止策なども助言しています。

■内部監査の終了後も、情報セキュリティに関する相談や第二者監査の依頼に対応し、被監査組織とのより強固な関係を構築できます。