共通基準を軸にグループISMSの基盤づくりを

リコーグループでは、2007年3月に共通基準を策定し、
2007年4月から本格的にグループ各社への共通基準の展開･定着を推進しています。
この共通基準により、各社の情報セキュリティ対応レベルの継続的向上を図り、
お客様に新しい価値を提供するためのさらなる基盤強化を目指しています。

グループ全体のセキュリティレベル向上を目指して

リコーグループが、情報セキュリティへの取り組みを通じて企業の社会的責任を果たし、企業価値の向上を図るためには、グループ会社間の垣根を越え、各社の情報セキュリティを一定以上に引き上げるセキュリティレベルの「共通化」が重要です。

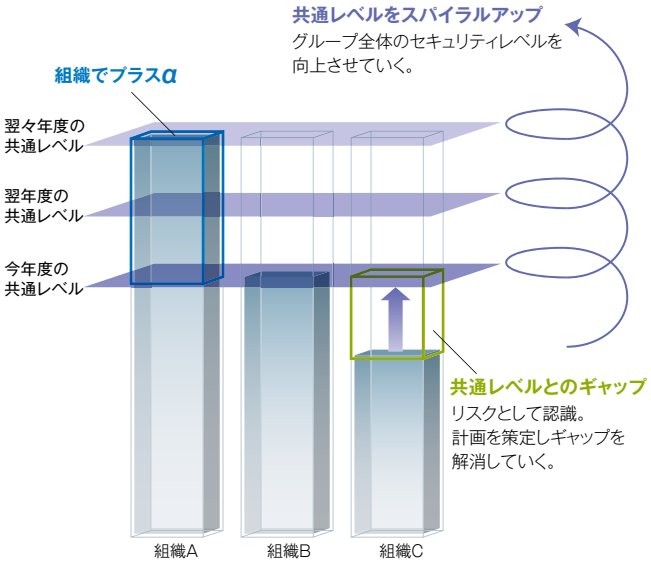
同じグループ会社といえども、規模や企業文化にはさまざまな違いがあり、その業務も、会社によって研究･開発･設計･生産･販売･サービス等多岐にわたります。また、個別に取り組む情報セキュリティのレベルにも差が生まれがちです。リコーグループでは、こうしたさまざまな問題を解決し、情報セキュリティ活動の基盤となるグループISMSをさらに有効なものにするためには、グループ全体の統一したセキュリティポリシーとなる共通基準が必要であると考えました。また、国際規格ISO/IEC27001では、個別の安全対策についてどこまで実施すべきかまでは規定していないため、具体的な実施基準が必要でした。そこで、この国際規格の要求に合わせ、リスクの大きさに応じた実施基準の検討を2005年12月から始め、2007年3月に「リコーグループ共通基準」として策定し、2007年4月から本格的にグループ会社への展開･定着を推進しています。

情報資産の重要性に合わせた共通基準

こうした共通基準を策定し、グループ会社に展開する目的は、各社の情報セキュリティを一定以上に引き上げる「共通化」を進め、その共通化したセキュリティレベルを継続的にスパイラルアップさせることにあります。この目的を達成するためには、ISMSの枠組みを利用してリコーグループ各社の情報資産を棚卸しし、一つひとつの情報資産に対してリスク分析を実施し、どこが弱いのかを突きとめ、それに対する適切な管理策を打つことが必要です。

こうした視点から、リコーグループ共通基準では、情報資産の種類別にその取り扱いの基準を決めています。情報コンテンツ、物理的資産、ITシステム、サービス、協力組織に大きく分類し、それぞれに業務上の重要性の程度によって、「必要対策」「推奨対策」の2段階のチェック項目を定めました。

■共通レベルのスパイラルアップイメージ

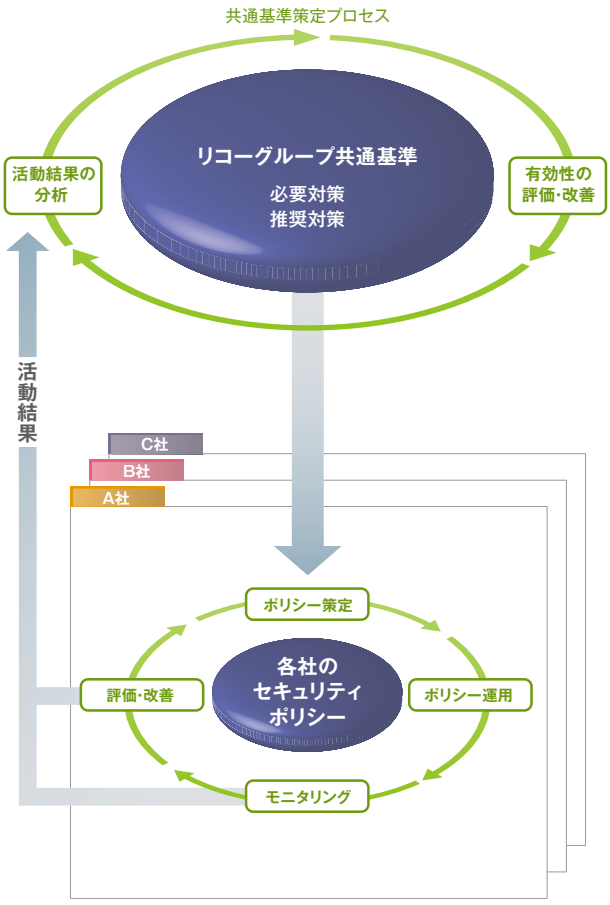


共通基準を軸に、各現場に合わせたポリシーを策定

グループとして必ず順守すべき「必要対策」について、各現場の情報資産管理責任者が、当該情報資産に適用される要求事項･セキュリティレベルと現状の管理レベルを比較し、ギャップの有無を確認しながらリスク評価し、リスク対応のための管理策を実施します。また、各社の業務特性によって任意に選択できる「推奨対策」については、同様の比較により、各現場の特性に合わせてリスク対応の必要性を判断することができ、さらに組織の機能･特色･状況によって順守

すべき追加事項がある場合は、独自の管理策を付加することもできます。こうしてグループ共通基準は各現場に合わせて最適化され、各社のセキュリティポリシーとして策定されていきます。策定されたセキュリティポリシーは、日常業務の中に組み込まれて運用され、現場マネージャーが日常管理のPDCAを回す中で実施·改善を進めています。
また、こうした情報資産の取り扱いだけではなく、組織における管理レベルをチェックするためにマネジメントシステムの状況についてもアセスメントし、PDCAが適切に回っているかを確認することもできます。このようなリスクアセスメント手順を円滑に実施するために、専用ツールも開発しています。

■共通基準を軸に各社でリスクアセスメント



より簡素化されたリスクアセスメントが実現

「共通基準を軸にした情報セキュリティマネジメント」の特長は、共通基準ベースの簡素化されたリスクアセスメント手法の導入です。これにより、業務の最前線で情報資産を管理している現場マネージャーのリスク評価·対応が、従来よりも簡易化されました。さらに、内部監査および外部審査を通じて、第三者が適合性や有効性を確認できる仕組みも整備しました。このようなグループ各社におけるセキュリティ活動の結果は本社の統括部門に集約され、共通基準の評価·改善に活用されます。外部の環境変化やリコーグループの状況に合わせて共通基準を更新し、グループ全体でセキュリティレベルをスパイラルアップしていきます。

■グループ共通基準の画面サンプル