リスクアセスメント体系図

以下の図は、リスクアセスメント体系の1つのモデルを示したものです。
以下のモデルでは、既存の管理状況（管理策）をISO/IEC 27001（JIS Q 27001）附属書Aとのギャップ分析にて基本管理策を決定し、別途、資産（情報資産）に対するリスク評価を行い、基本管理策の採用できないものを追加管理策として決定し補う、組合せアプローチとなっています。
なお、このモデルのベースライン・アプローチでのギャップ分析からリスクの対応への一連の流れが、決定した管理策が、ISO/IEC 27001（JIS Q 27001）附属書Aと比較して、必要な管理策が見落とされていないことを検証する役割も果たしています。

ベースライン・アプローチ

社内規程書
・社内規定類一覧
・既に実施されている管理策

ISO/IEC 27001（JIS Q 27001）附属書A
（管理策）

対比

ギャップ分析

既に組織内にある情報セキュリティ管理策（規定化されたもの等）とISMS規格の附属書Aの管理策を対比させ、実施の有無および該当の有無のギャップを分析する。

Y：実施されている
P：一部実施
N：実施されていない
N/A：該当しない

P, Nへの対策を検討

基本管理策

ギャップ分析対策表
結果、一部実施されている項目および実施されていない項目に関して、どのような対策を講ずるかを検討する（対策を「ギャップ分析対策表」へ記載）。

基本管理策で十分かを検討

リスクへの対応

脆弱性が受容レベル以上の情報資産のみ対策を検討し、「基本管理策」だけで十分かを検討し、不足がある場合における対応を検討する。

・対応方法の選択
（回避、低減、移転、保有）
・低減可能な管理策の検討
・基本管理策の採用
・残留リスクの承認

リスクグループ分析対策表

追加管理策

基本管理策ではカバーしきれないリスクに対し、個別の「追加管理策」を検討する（「リスクグループ分析対策表」へ記載）。

リスクグループ分析対策表
・関連規程および管理策などの見直しなど

管理策の文書化

講じられた対策の中で、リスク対応を明確にし、組織としての情報資産への管理策を文書化。

社内規程書
・決定された管理策は、ルール化するために各規程として明文化されることになる。

適用宣言書
・ISO/IEC27001の附属書Aの管理策について、自社がどの管理策を適用するか・しないかを宣言する文書を作成する。

リスク対応計画書
・リスク対応に関する計画書
（必要に応じて）

詳細リスク分析

情報資産の洗い出しと資産評価

・組織内にある全ての情報資産を「情報資産台帳」洗い出す。
・資産価値を、情報の機密性（Confidentiality）および完全性（Integrity）、可用性（Availability）に分けて評価を行う。

（仮）情報資産台帳（A部門）
（仮）情報資産台帳（B部門）
（仮）情報資産台帳（C部門）

集める

グルーピングと平準化

重要性や属性が同じで、結果的に適用されるセキュリティ対策が同じであれば、同じグループとしてまとめて管理することが効率的である。

・洗い出した資産を、資産価値や属性（保管形態や保管期間、用途等）が一致するものを一つのグループとする。
・グルーピングした資産に対して、再度、資産評価（C, I, A）の確認を行い、客観性のある資産ランクの平準化を行う。

情報資産台帳

・脅威・脆弱性の評価
・リスク値の算出
・受容レベルの決定

脅威一覧表

脅威の洗い出し

・考え得る脅威（「資産に影響を与え、損失を発生させる直接の要因」）を洗い出す。

ISO/IEC 27001:2023　5.7 脅威インテリジェンス
・情報セキュリティの脅威に関連する情報を収集及び分析し，脅威インテリジェンスを構築しなければならない。

2026.02.04