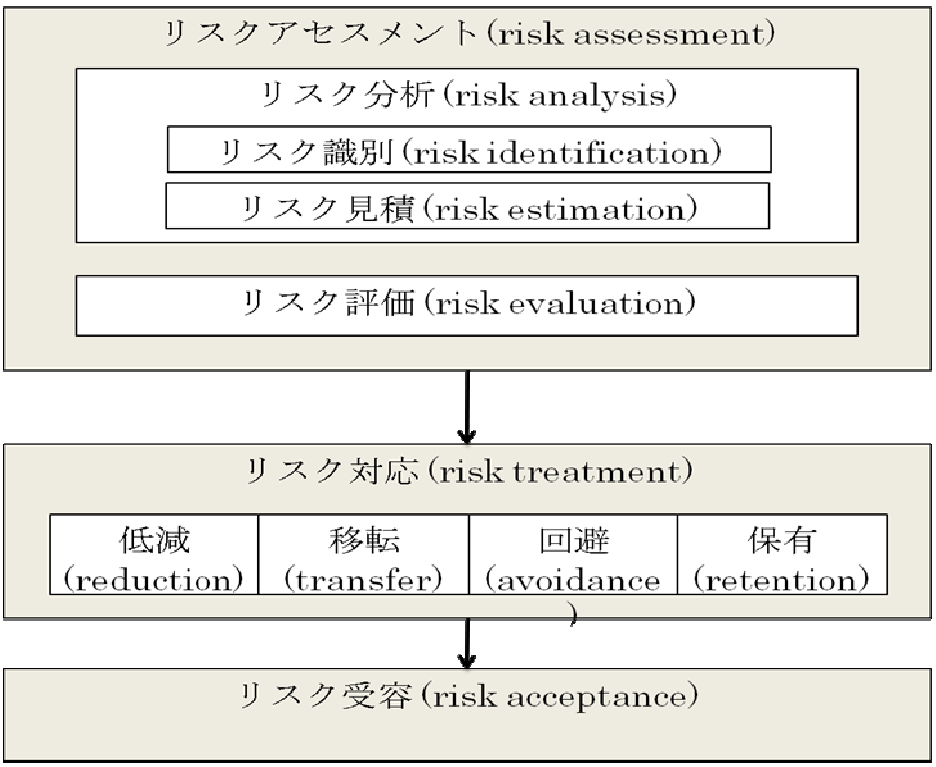
リスクアセスメント

リスクとは，情報の CIA いずれかの特性を損なうような事象として，どのようなものがどの程度の確率で発生し，その結果，どのような業務への影響があるか，を意味します．リスクアセスメントでは潜在的なリスクを分析した上で，どのような対応が必要とされるかを検討します．リスクアセスメント，リスク対応，リスク受容の相互関係と内訳については次の図をご参照下さい．




リスクアセスメントの具体的な方法については

- JIS TR X 0036-3 第 3 部 IT セキュリティマネジメントのための手法 (ISO/IEC TR 13335-3:1998 の日本語訳)
- ISO/IEC 27005:2008 情報技術－セキュリティ技術－情報セキュリティリスクマネジメント (対訳版有り)
- ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応 付録 1: ○○メディカル社の事例

・ ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-リスクマネジメント編

などの参考資料にあります.

本センターでの具体的なリスクアセスメント手法は ISMS マニュアルに含まれておりますが，資料 1 としても抜きだしてあります．資産一覧や具体的なリスクアセスメント結果は資料には入れておりません．リスクアセスメント結果については CIO の承認が必要であり，その際に使用している説明資料が資料 2 の「主要残留リスク報告書」です.「主要」と述べているのは，残留リスクという言葉が対策後の潜在的なリスク全般を表しているためで，資料 2 では対策によって変化するリスクと，対応を検討する必要が有るが当面は受容するリスクを中心にまとめています．なお，ここでも一部の技術的な情報は削除されています.

リスクマネジメントプロセスでは適用宣言書の作成が求められます．これは，ISO/IEC 27002 で詳細に説明がされており ISO/IEC 27001 の附属書 A に概略が記載されている管理策 133 の中から，どれを採用し，どれを採用していないのか，また，必要に応じて何を追加したのかを理由とともに説明した文書です．資料 3 として入れてあります.