# リスクマネジメントの取り組み方法

## Method of Risk Management

田上岳夫*
Takeo Tagami


### 要　旨

情報セキュリティマネジメントの実現に当たっては，情報資産に対するリスクマネジメント（リスクに関して組織を指揮し，管理する調整された活動）が不可欠です。しかしながら，リスクを認識し，評価し，対応するプロセスには，様々な考え方や方法があり，その実施においては，組織に適した体系的な取り組み方法を確立し，適切な手法を選択しなければなりません。

本稿では，リスクマネジメントの取り組み方法について説明します。

The most essential thing for realizing information security management is the risk management on information assets, as a regulated activity which controls and manages an organization.

There are, however, various views and methods in the process of risk perception, risk evaluation, and risk treatment. Therefore it is necessary to establish a systematic and appropriate method to an organization and to select an effectual method.

This paper introduces the effective methods of risk management.


### 1．まえがき

近年，情報の価値や情報システムの利便性の向上に伴い，情報漏えいやコンピュータウイルスへの感染など，情報セキュリティに関する事故や事件が多数発生しています。ひとたび事故や事件が起きると，組織は業務の停止や社会的信用の低下など，深刻なダメージを受けてしまうことになります。情報セキュリティ上のリスクから情報資産を守るためには，リスクマネジメントに関する体制を確立した上で，リスクを正しく認識し，評価し，適切に対応する必要があります。

リスクマネジメントは，組織の情報セキュリティマネジメントの実現において不可欠な活動であり，組織に適した体系的な取り組み方法を確立し，適切な手法を用いる必要があります。また，その取り組みにおいては，経営者の参画など，経営的な判断が求められます。

なお，ISMS（Information Security Management System）適合性評価制度においても，リスクマネジメントの考え方が取り入れられており，今後，ISMSの普及とともにリスクマネジメントの取り組みが広まっていくものと思われます。

### 2．リスクマネジメントの全体像

リスクマネジメントとは，TR Q 0008によれば「リスクに関して組織を指揮し，管理する調整された活動」と定義され，その全体像は，**図1**のとおりとなります。

TR Q 0008の定義は，リスクマネジメントの活動や用語の

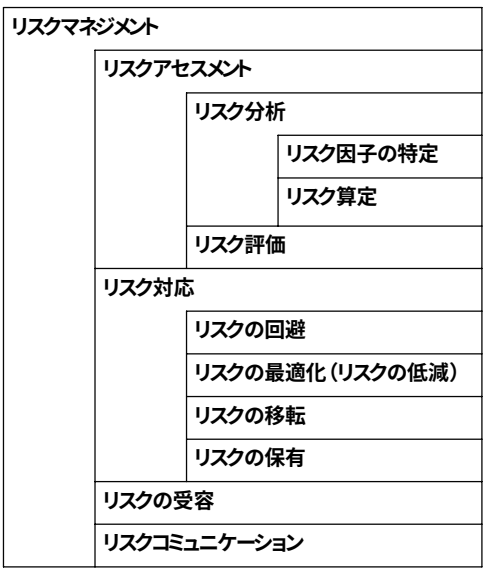


**図1　TR Q 0008に基づくリスクマネジメントの全体像**
**Fig.1　Outline of risk management based on TR Q 0008.**

＊ IT基盤システム開発事業部
IT Platform Systems Development Division

使い方の標準として，ISMS認証基準においても採用されており，本稿においてもTR Q 0008の定義を採用して説明します。

リスクマネジメントは，図1のとおり，「リスクアセスメント」，「リスク対応」，「リスクの受容」，「リスクコミュニケーション」を含むものと定義されています。さらに，「リスクアセスメント」は，「リスク分析」と「リスク評価」のプロセスにより定義されています。以下，それぞれの定義について説明します。

まず，リスク分析は，「リスク因子の特定」と「リスク算定」のプロセスにより構成されます。リスク因子の特定とは，リスク因子を発見し，一覧表を作成し，特徴づけるプロセスになります。リスク因子（脅威とぜい弱性の組合せ）の具体例としては，暗号化していないパソコンの盗難によって引き起こされる情報漏えいが挙げられます。リスク因子の特定に当たっては，情報資産を洗い出し，脅威とぜい弱性を明確化する作業を行います。

リスク算定とは，リスク因子の発生確率と結果の値を設定するために用いるプロセスであり，たとえば，特定したリスク因子について，「情報資産の価値」×「脅威の大きさ」×「ぜい弱性の度合い」の算出式によりリスク値を算出します。**図2**にTR X 0036におけるリスクマネジメントの関係を示します。リスク値が「情報資産の価値」，「脅威」，「ぜい弱性」により決定されることが分かります。

算出されたリスクとリスク基準（リスクの重大さを評価するために適用される尺度）を比較するプロセスがリスク評価になります。リスク基準は，経営者が受容可能なリスクの水準として決定したものになります。

リスク対応は，リスクを変更させるための方策を選択し，実施するプロセスです。リスク評価の結果，リスク対応を行うことが決定したリスクについて，リスクの回避，リスクの最適化（低減），リスクの移転，リスクの保有の４つから選択することになります。情報セキュリティ対策として一般的に用いられるリスク対応方法は，リスクの最適化

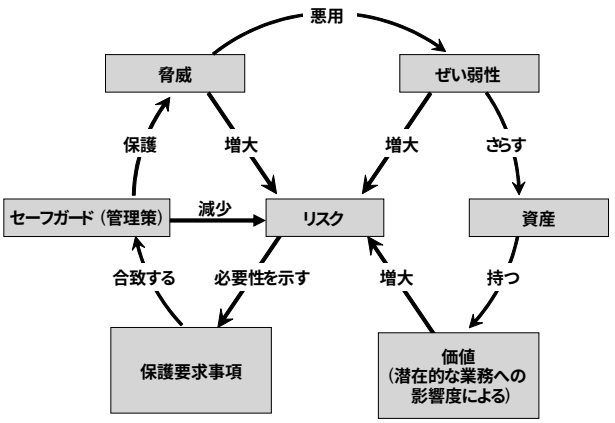


**図2　TR X 0036におけるリスクマネジメントの関係**
**Fig.2　Relation of risk management in TR X 0036.**

（低減）です。業務自体を中止することになるリスクの回避や，保険への加入または外部への業務委託によるリスクの転化は，一般的にリスクの最適化（低減）が困難な場合や多額の損害費用が発生する場合に選択すべきものです。リスク対応に当たっては，まずはリスクを低減するにはどうすればよいか検討します。

リスクの受容は，リスクを受容する意思決定であり，具体的には経営者がリスクアセスメントやリスク対応の結果，残留リスクが受容可能なリスク以下であることを確認し，承認します。

## 3．リスクマネジメントの枠組みと取り組み方法

リスクマネジメントは，情報セキュリティに関するリスク因子を特定した上でリスクの評価を行い，適切なリスク対応を行うことにより，組織への損害の発生を未然に防止するとともに，事故・事件が発生した場合に損害を最小化することを目的としています。

本章では，JIS Q 2001:2001を踏まえたリスクマネジメントの枠組みとその取り組み方法について説明します。

### 3.1　リスクマネジメントの方針・体制

リスクマネジメントの実施に当たっては，組織全員の理解と協力が不可欠であるため，リスクマネジメントに関する方針を定め，周知を図るようにします。リスクマネジメントの方針としては，組織の特徴から，特に保護したい事業（業務）や資産，優先的に実施したいセキュリティ施策などを明らかにし，リスクマネジメントの目的や行動指針としてまとめるとよいでしょう。

リスクマネジメントの体制は，最高経営者をトップとし，その責任を明確にした上で，情報システムの企画，開発，運用などを行う部門を中心に，法務部門，総務部門，監査部門などからなる横断的な組織を構築するようにします。情報セキュリティ運営委員会などの情報セキュリティに関する横断的な組織がすでに存在する組織では，すでに体制がある分，進めやすいでしょう。横断的組織で全体調整を行うとともに，個々の組織員に対する教育や啓発などを行うことにより，組織全員の理解と協力を得やすい体制づくりが実現でき，リスクマネジメントを効率的かつ円滑に進めやすい環境になります。

### 3.2　リスクマネジメントの計画

リスクマネジメントの体制と方針に基づき，事業におけるリスクマネジメントの計画を立てます。まず，リスクアセスメントやリスク対応の方法，最高経営者の関与のタイミング，リスク対応計画のフォロー方法などを定め，リスクマネジメントの実施に関するスケジュールを作成します。

リスクアセスメントの方法については，TR X 0036では，次の4つのアプローチが紹介されています。

（1）ベースラインアプローチ

基本的なリスクの存在を想定した上で，既知の規定や基準（JIS X 5080など）を参照して，管理策を導入します。

(2) 非形式的アプローチ

担当者の経験や判断に基づくアプローチです。構造的な方法ではないため，実施する者の経験によって結果に影響が生じてしまいます。

(3) 詳細リスク分析

情報資産ごとに資産価値やリスクを算出していくアプローチです。ISMSにおけるリスクアセスメント方法として一般的に実施されている方法です。

(4) 組合せアプローチ

複数のアプローチを併用します。たとえば，ベースラインアプローチに基づき全体のアセスメントを実施し，重要な情報システムについて詳細リスク分析を実施する方法が挙げられます。

リスクアセスメントの方法などが決定したら，各作業項目の責任者および担当者の割当て，各作業結果の関係者への周知方法の決定，リスクマネジメントにかかわる各作業手順の策定などを行い，計画を確実なものとします。

また，リスクマネジメントの初期段階において，個人情報の保護，知的財産権の保護といった組織の業種・業態に伴い遵守を要求される法令・規制上の要求事項についても識別し，リスクマネジメントの枠組みのなかで対応方法を検討，実施できるようにする必要があります。法令・規制上の要求事項は，事業上およびセキュリティ上の要求事項の検討と同じ枠組みのなかで検討，対応すべき重要事項です。

こうした一連の活動により，リスクマネジメントを計画し，枠組みを確立することができます。

### 3.3 リスクマネジメントの実施と維持

リスクマネジメントの計画を策定した後は，その計画に従ってリスクマネジメントを実施することになります。リスクアセスメントにおいては，情報資産を漏れなく洗い出し，計画に定めた方法によりリスク分析とリスク評価を実施します。

リスクアセスメントに続いて実施するリスク対応では，受容できないリスクに対して，リスク対応の具体策の検討と経営資源の割当てなどを行い，リスク低減のための活動を実施します。対応することが決定したリスクに対しては，確実に実施することが重要であり，リスク対応計画を立て，対応の優先順位や対応実施者を管理するようにします。

さらに，事件・事故が発生した場合の緊急時対応手順・復旧手順の整備，組織内外との協力・連絡関係の検討，教育・訓練を実施します。意思決定者と他のステークホルダーの間におけるリスクに関する情報の交換または共有を行うリスクコミュニケーションも重要な活動の1つになります。

### 3.4 リスクマネジメントの見直し

リスクマネジメントは，組織に導入された後もその活動が維持されなければなりません。リスクも環境の変化（法制度の変化，事業上の変更，場所の変更など）によって変化するため，リスクアセスメントの結果は見直しをしていかなければなりません。リスクマネジメントについても環境の変化に応じて見直されなければなりません。場合によっては，リスクマネジメントの枠組み自体も変化に合わせて見直す必要があります。この見直しは，定期的に実施するとともに，大きな変化があった場合などに随時見直す必要があります。なお，見直しのタイミングについては，リスクマネジメント活動の一環として，その計画のなかで定義しておきます。

最高経営者は，リスクマネジメントの見直しと連動し，リスクマネジメントの適切性や有効性についてレビューを行い，改善のための意思決定を行います。

## 4．リスクマネジメントにおけるポイント

適切なリスクマネジメントを行うためのポイントとして，最高経営者の関与が挙げられます。最高経営者は，組織に合わせたマネジメント体制を構築するとともに，自らリーダシップを発揮し，方針や計画の策定，レビューなどにおいて経営の意思を確実に反映しなければなりません。リスクにどこまで対応するか，どのリスクへの対応を優先させるかなどを判断するのは，最高経営者になります。特にリスクを残留する判断は，経営的観点で判断を行わねばなりません。

また，事故・事件の発生を前提としてリスクマネジメントを実施することも重要になります。リスクマネジメントは損害の発生を未然に防ぐことを目的としていますが，リスクを完全になくすことはできません。したがって，事件・事故の発生時の損害を最小化するために，平常時に緊急時対策と復旧対策について策定しておくことも，リスクマネジメントにおける重要な対応の1つになります。

## 5．おわりに

リスクマネジメントの重要性が叫ばれているものの，適切なリスクマネジメントを実施している組織はまだ少ないと思われます。NECは，今後とも業界団体や標準化団体，官民の委員会活動などを通して，リスクマネジメントやリスクアセスメント分野の発展に寄与していきたいと考えています。

### 参考文献


1) TR Q 0008:2003 (ISO/IEC Guide73:2002 Risk management − Vocabulary − Guideline for use in standards リスクマネジメント−用語−規格において使用するための指針)，日本規格協会.
2) JIS Q 2001:2001,「リスクマネジメントシステム構築のための指針」，日本規格協会.
3) TR X 0036-1:2001,「ITセキュリティマネジメントのガイドライン−第1部: ITセキュリティの概念及びモデル」，日本規格協会.
4) TR X 0036-2:2001,「ITセキュリティマネジメントのガイドライン−第2部: ITセキュリティのマネジメント及び計画」，日本規

格協会.
5) TR X 0036-3:2001,「ITセキュリティマネジメントのガイドライン－第3部: ITセキュリティマネジメントのための手法」日本規格協会.
6)「ISMSユーザーズガイド: ISMS認証基準（Ver2.0）対応　（リスクマネジメント編)」, 日本情報処理開発協会.
7)「リスクアセスメント調査報告書」Ver1.0, 日本セキュリティ監査協会.

## 筆者紹介

Takeo Tagami
**田上　岳夫**（たがみ　たけお） 1995年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター主任。システムズアーキテクト。日本システム監査人協会会員。