

システムリスク管理に見られる問題点

昨今、セキュリティ管理や個人情報の保護など、システムリスク管理が経営の重要課題となりつつある。本稿では、NRI（野村総合研究所）が行ったシステムリスク管理に関するコンサルティングの最近の結果をベースに、システムリスク管理に見られる共通した問題点とその改善のためのポイントを紹介する。

システムリスク管理に見られる問題点とは

これまでNRIが実施したシステムリスクの評価を目的としたコンサルティングに基づいて、多くの企業に共通的に見られた問題点とそれを改善するためのポイントを紹介する。

今、経営資源としての情報資産（情報および情報システム）が重要視されている。そのような中で、システムに関わるこれらのリスクを正しく認識し、それに対する総合的な管理の仕組みを確立することが求められている。

12の共通的な問題点と改善のポイント

(1) 守るべき資産が把握されていない

システムリスク管理の対象として、情報システム部門が管理しているシステムのみをあげているケースが多い。情報システム部門以外の部門が独自に導入しているシステムやそこで管理されている情報も含めて、全社レベルで管理されなくてはならない。

(2) システムリスクに対する認識が不十分

アプリケーションシステムについてのリスクはある程度把握されているが、自社ネットワークやインターネット接続部分など、システムインフラに関わるリスク把握が不十分な

ケースが多い。現状評価や改善策の検討に先駆け、リスクの把握と評価を行うべきである。

(3) 体制・役割・責任分担が不明確

全社的なシステムリスクに関わる管理体制が未確立であったり、部門の役割・責任が不明確なケースが多い。全部門に関連する問題として、管理体制の確立を進めるべきである。

(4) システム開発の標準化が未確立

システムの設計開発時の品質確保とリスク低減策として、システム開発手法などの標準化が有効であるが、この取り組みが不十分なケースが多い。手法としての標準化の推進とともに、現場の経験、知恵、工夫を反映した品質評価方法の導入が、より効果的であろう。

(5) わがままなアプリケーションオーナー

アプリケーションオーナー（主管部署）がなかなかシステムの仕様を確定せず、そのしわ寄せでテスト工程を端折ることにより、システム品質が低下するケースが増加している。情報システム部門は、アプリケーションオーナーの役割やリスクをより明確に提示し、周知させるとともに、よりよいコミュニケーション

ョンルールを確立することが必要である。

(6) 開発と本番が渾然一体

本番環境でテストを実施したり、本番環境の顧客情報を自由にコピーして開発環境で利用するといった、開発サイドの融通性を重視しセキュリティを度外視するケースが多く見られる。今後、開発と本番環境の分離、顧客情報のマスキングの実施、協力会社に対する利用制限などを検討すべきである。

(7) ウィルス対策の不備

ウィルス対策は行っているものの、新たなウィルスが出現した際の社内への通報や暫定対策の連絡ルール、感染発生時の駆除ルールなどが確立していないケースが多い。予防のみならず、危機発生時の危機管理ルールの確立を目指し、対応策を検討すべきである。

(8) ファイアウォールは低い壁

ファイアウォールの監視体制が不十分で、不正アクセスを把握できず、適切な措置をタイムリーに講じることができないケースが多い。改めてファイアウォールの監視体制や対応レベル、問題発生時の対応ルール、新たな不正アクセス手段への速やかな防御方法などを見直すべきである。

(9) 不十分なデータセンターのゾーニング
データセンターの入退館ルールは確立して

いるが、同じIDカードでセンター内のどこにでも入室可能なケースがある。目的別、セキュリティレベル別のゾーニングとこれに応じたアクセスコントロールが重要である。

(10) 委託先のセキュリティ状況が不明

プログラム開発などの作業を外部に委託している企業は多い。それらの委託先でのセキュリティの遵守状況、要員へのセキュリティ教育の実施状況、遵守状況のチェックなどが不明なケースがある。遵守事項の明確化、委託契約の見直し、再教育などが必要である。

(11) セキュリティポリシーがない

セキュリティポリシーが存在しないということは、セキュリティに関する憲法、法律、条例などが無いまま経営が行われているに等しい。早急にセキュリティポリシーの基本方針を策定し、トップダウンで社内外に周知させながら、セキュリティスタンダード、各種ルールなどを体系的に策定していく必要がある。

(12) セキュリティに対する意識が低い

いくら素晴らしいルールを体系的に整備したところで、これを運営し遵守する社員、協力会社要員の意識・モラルが低ければ意味がない。セキュリティ教育を徹底するとともに、意識の向上に積極的に取り組む必要がある。

(野村総合研究所 水野 満)