システムリスク管理のあり方

インターネットに代表されるEビジネスの拡大にともない、セキュリティ管理を含めた総合的なシステムリスク管理の必要性が高まっている。システムリスク管理は金融監督庁の検査マニュアルにも明記され、銀行・証券・生損保では整備が必須な要件となりつつある。本稿では、まず着手すべきシステムリスク管理について述べる。

システムリスク管理の必要性

Eビジネスが飛躍的に成長するにつれて、Webサイトへの不正アクセスや情報漏洩など、「セキュリティ」の社会問題化が進んでいる。また、アクセス増加による回線のパンク、システム障害によるサービス停止などが引き起こすビジネスへの影響は甚大なものとなりつつある。

しかし、従来のセキュリティ対策やコンティンジェンシープランでは、対象となる脅威の種類や対象となるシステム・情報の範囲が限定されていて、いわば局所的かつ対症療法的な対策に留まっている。

一方、金融監督庁は1999年７月、「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）」を公表し、銀行などに対して信用リスク、市場関連リスクなどと同等の位置づけで、システムリスク管理態勢の整備を求めている。これは今後証券、生損保業界への展開も予想される。

経営資源として情報資産（システム・情報）が最重要視されている現在、改めて企業を取り巻くシステムリスクを認識し、これに対する総合的なリスク管理態勢を確立することが必要となる。

なお、システムリスク管理の必要性は、金融業界に限った話ではない。BtoB（企業対企業）、BtoC（企業対個人）のEビジネスに参入する製造業、流通業にも必須要件であり、さらに今後の個人情報法制定を見据えるならば、個人情報の取り扱いに関わるセキュリティ対策という点から、システムリスク管理はほぼすべての企業で必須条件となろう。

表１　情報資産をとりまく「脅威」の例

自然的	地震、風水害、火災など
社会的	（デマなどによる）故意の集中利用など
技術的	故障・動作不良、陳腐化など
人為的	（故意および過失による）物理的破壊、不正改鼠、漏洩、盗取、詐取、ハッカー、ウィルス配布など

「脅威」の認識

システムリスク管理を検討するうえで、まず自社の情報資産を取り巻く「脅威」を正しく認識することが重要である。

脅威の代表例としては、表１のようなものがあげられる。情報資産すべてについて、「どのイベント（業務処理、システム機能）のどの部分に、いかなる脅威が存在しているか」を把握し、もし何らかのリスクが発生した場合には、どの程度の損失を被る恐れがあ

るかを認識しておくべきである。

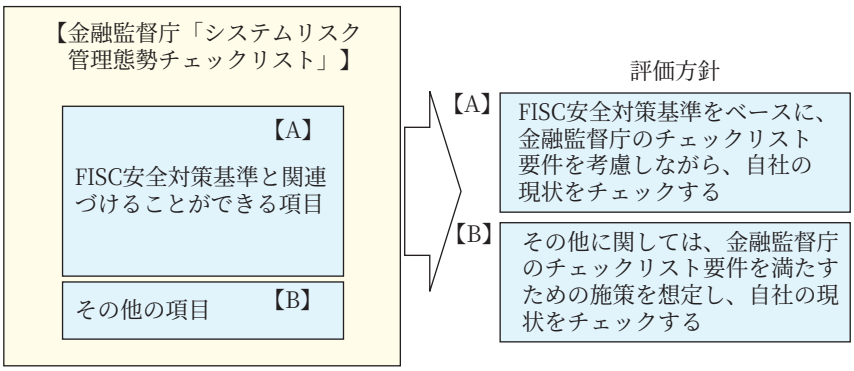

図１　金融監督庁のチェックリストの構造

システムリスク管理態勢確立のアプローチ

ここではまず、一般的なシステムリスク管理態勢確立の手順を紹介する。

①現在のシステム、情報、ルール、施策の整理と、想定される「脅威」の抽出、および「脆弱性（対策の弱点、限界）」の把握
②リスクの想定（「損失度合」の予測）
③現状の問題点、課題の総括
④リスク管理ポリシーおよびリスク管理体系の策定
⑤各種リスク管理ルール策定
⑥システムでの対策方針、計画策定
⑦リスク管理の組織整備計画策定
⑧監査方針、監査計画策定
⑨教育方針、教育計画策定
⑩全般的なアクションプラン策定

なお、本来は「企業のすべての情報資産を対象に、想定されるすべてのリスクに対応可能」なポリシー、ルールおよび施策を上記手順に沿って策定することが望ましい。

即効的な改善アプローチの実施

上記の総合的なアプローチに先駆け、まず短期間のうちに自社のシステムリスク管理のレベルの把握、緊急対策部分の特定化と強化を、即効的なアプローチによりまず実現することが望まれる。

(1)　現状の実施レベルの診断・評価

まず、現状の安全対策・セキュリティ対策の実施レベルの診断・評価を行う。

①基準とすべき資料

診断・評価の際、検証基準として参照すべき基本資料は、「システムリスク管理態勢の確認検査用チェックリスト」(金融監督庁 http://www.fsa.go.jp/）である。

さらに、これに準拠すべきと記されている「金融機関等コンピュータシステムの安全基準書」および「同解説書」(FISC：財団法人金融情報システムセンター編)、「金融機関等におけるコンティンジェンシープラン要領」および「金融機関等におけるコンティンジェンシープラン策定のための手引書」(FISC編）などがあげられる。

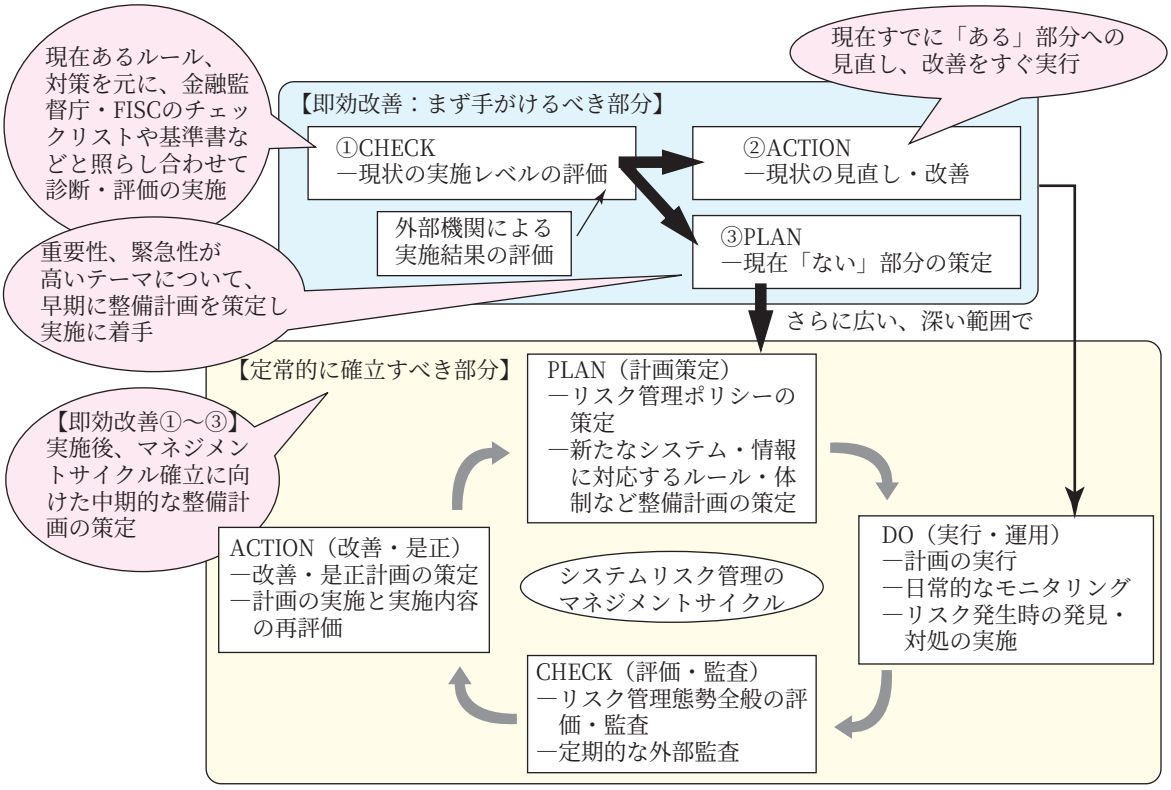

図２　システムリスク管理のマネジメントサイクル

②チェックのポイント

金融監督庁のチェックリストは総括的な表現が多いため、まず内容の解釈を行うとともに、前出の各種基準書、解説書の関連項目との関連づけを行うことが重要である。

NRI（野村総合研究所）では、システムリスク管理態勢強化のコンサルティングに取り組んでいるが、金融監督庁のチェックリストの構造を７ページの図１のようにとらえている。図１の評価方針に従って、詳細に評価を実施する際は、まずFISCの安全対策基準の詳細項目を細目と位置づけ、かつ金融監督庁のチェックリストに基づき、自社の現状をチェックすることを最初に実施すべきである。

③施策チェックの観点

現状の各種システムリスク管理のための施策をチェックする際、下記の点に留意する。

・ルール、マニュアル、具体的対策の有無
・役割分担、責任の明確度合
・ルール・マニュアルの定着レベル
・日常運用での証跡（記録、ログ）取得、モニタリングの有無
・定期的な評価・監査の実施
・評価・監査結果に基づく是正措置計画の

策定、是正措置の実行
・業務とルールの乖離に対する必要に応じた改善の実施など

なお、「ルールは規定されていないが、実運用上はほぼ遵守されている」事項の実施レベル評価は、「ほぼできている」と評価せず、「できていない」と評価し、ルールの規定化、可視化を求めるという、厳格な視点が求められる。

(2)　現状の診断・評価結果の是正と改善

必要な範囲について、見直し・改善計画を立て実行する。実行結果の再評価も重要である。

マネジメントサイクルの確立

現状の水準が低いものやルール、対策がないもの、規定化されていないものは、改善計画を立て順次着手が必要だが、「改善を実施したら、それで終わり」ではない。継続的なシステムリスク管理のマネジメントサイクルを確立することが重要である（図２参照）。

そのためにも、計画立案時には、改めて前述の「システムリスク管理態勢確立のアプローチ」を踏まえる必要がある。とりわけ、システムリスク管理ポリシーの明確化、システムリスク管理の全体ルール体系の整備、システムリスク管理業務に対する監査手順書の整備、システム開発プロジェクト管理やシステムリリースに関する方針・手順の整備などを順次策定し、定着化させていく取り組みが重要である。

また、Eビジネス関連のシステムリスク管理に関して、全体からくくり出して先行的に整備することは、ビジネスリスクそのものの低減にも有効な施策となろう。

さらに、金融監督庁のチェックリストでは対応しきれていない、知的所有権やビジネスモデル特許など、システムに関連するコンプライアンス対策をはじめとする各種リスクに対しても、明確な指針とルールを定めることが望ましい。

実施に当たって

「金融監督庁、FISCの基準は銀行向きで、自分たちにはハードルが高すぎる」という声をよく耳にするが、自分たちのハードル、すなわちシステムリスク管理ポリシーがないのであれば、いったん詳細に「脅威、管理実態、あるべき姿」を確認し、システムリスク管理ポリシーを明確化したうえで「ここまでやればいい」という基準、指針を定めるべきである。

なお、即効的な改善アプローチでは、「まずは内部で自己診断」するのが一般的であるが、即効的な改善策を立案した段階で、「脅威の把握レベル、ルールの有効性、セキュリティ技術方式選択の妥当性」を高めるために、外部機関の評価を受けることも有効であろう。

（野村総合研究所　水野　満）