金融機関の情報システムに求められる継続的な安全対策

企業の情報システムには、企業を取り巻く環境の変化によって生じるリスクへの迅速な対応が求められている。本稿では、金融機関の情報システムの安全対策について財団法人金融情報システムセンター（FISC）が定めたガイドラインの概要を紹介し、その活用にあたって留意すべき点、および活用方法について考察する。

情報システムに求められる安全対策

情報システムは、いまや企業活動にとってきわめて重要な役割を担っており、情報システムが停止した場合には、業務を平常どおりに行うことが困難であるばかりでなく、取引先や顧客にも大きな影響を及ぼすことになる。

このような事態を引き起こす原因はさまざまである。たとえば2004年10月の新潟県中越地震では、水の供給が止まったことで、コンピュータセンターの空調設備が稼動しないことによるセンターの機能停止が懸念されるなど、社会インフラの障害というリスクがあらためて指摘された。また、インターネットを通じて侵入するコンピュータウイルスの被害も後を絶たず、金融機関のサイトを装うフィッシングや、キーロガー（キー入力を読み取るプログラム）などにより個人情報を盗み出す犯罪も、インターネットを利用したサービスの拡大を背景に多発している。

このように、災害や犯罪の危険はつねに存在することから、企業には情報システムに対するリスクを定期的に見直し、継続的な安全対策を実施することが求められる。とはいえ、情報システムの安全対策は相応のコストがかかり、その効果について客観的に評価することが困難であるのも事実である。したがって、企業にとってはどの程度のレベルの安全対策を実施すべきかということが問題となる。

FISCの安全対策ガイドライン

そこで金融業界ではFISCが中心となり、金融機関やコンピュータメーカーの専門家、学識者などが参加した専門委員会が安全対策実施のためのガイドラインとして、『金融機関等コンピュータシステムの安全対策基準・解説

表1　FISC安対基準の構成

基準名	基準の概要	関連ガイドライン
設備基準	コンピュータシステムが収容される建物・設備を自然災害や不正行為などから守るための設備面の対策	情報システムの設備ガイド*1 ISMSガイドライン*2
運用基準	コンピュータシステムの信頼性および安全性の向上を図るための、開発・運用管理体制などについての対策	情報システムの設備ガイド*1 ISMSガイドライン*2
技術基準	コンピュータシステムの信頼性および安全性の向上に関するハードウェア・ソフトウェアなど技術面の対策	情報システムの設備ガイド*1

＊1：社団法人電子情報技術産業協会（JEITA）策定　＊2：財団法人日本情報処理開発協会（JIPDEC）策定

野村総合研究所
システムコンサルティング事業本部
金融ITマネジメントコンサルティング部
システムコンサルタント
藤渡亮輔（ふじとりょうすけ）
専門は証券会社システムの設計、業務コンサルティングなど

表2　FISC手引書の構成

工　程	作業内容
①必要性の認識と推進組織の編成	経営層の意思決定により、緊急時対応計画策定の組織を編成
②予備調査と基本方針の決定	緊急事態（リスク）の洗い出しとその影響、対策に必要な経営資源を想定し、各業務の優先度を評価し緊急時対応方針を決定
③緊急時対応計画の立案	緊急事態（リスク）の詳細シナリオを設定し、緊急時体制を決定の上、代替手段、初期・暫定・本格復旧対応を検討し、プランの維持管理体制を構築
④緊急時対応計画の決定	経営層による緊急時対応計画承認を受け、全社的に周知徹底
⑤緊急時対応計画の維持管理	定期的な訓練により実効性を確保するとともに、実効性のある内容になっているかを監視し、継続的に改訂

書』（以下、FISC安対基準）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（緊急時対応計画）策定のための手引書』（以下、FISC手引書）を作成している（表1および表2参照）。このガイドラインは、その時々の課題や関連法規の変更などに対応して随時改定されている。とくに関連法規（個人情報保護法、預金者保護法など）に対しては、施行されるまでに改訂を完了するという迅速な対応に努めている。

ガイドラインの活用方法

この専門委員会でFISC安対基準の改訂内容を検討する際に、個々の基準を「～すること」と「～が望ましい」のどちらで表現するかに議論が集中することがある。しかし、基準がどのように表現されようと、基準に書かれた対策を実施すれば安全が確保されると考えるのは誤解である。FISC安対基準は、ただ書かれた基準を実施するために活用するものではなく、各企業の緊急時対応計画のなかで、リスクを回避・軽減・予防する安全対策のベストプラクティスとして活用すべきである。

では、安全対策の検討・実施に際しての、ガイドラインの具体的な活用方法の例をあげてみよう。

まず、FISC手引書に従って緊急時対応計画を策定する場合は、「予備調査と基本方針の決定」の工程でリスクを洗い出し、業務の優先順位を付け、優先順位が高い順にリスクを評価（頻度と影響）する。次に、評価結果に基づいて優先順位が高いリスクが顕在化しないようコントロールする（安全対策の実施、保険によるリスクの移転など）。

また、FISC安対基準はその時々の課題や関連法規の変更に合わせて随時改訂されているので、企業は可能であれば同じタイミングで、上記手順で自社の緊急時対応計画と安全対策を見直すべきである。

このように、緊急時対応計画のなかでFISC安対基準を活用することで、企業の緊急時対応方針に基づいた安全対策をベストプラクティスの中から選択・実施でき、ある一定レベルのリスクコントロールが可能となる。 ■