第 124 回月例研究会報告

報告者 No.422　本田 実

日時：2006 年 10 月 23 日（月）18:30～20:30
場所：中央大学駿河台記念館　2 階 281 号会議室
演題：「FISC 安全対策基準とコンティンジェンシープラン策定手引書の概要と改定について」
講師：（財）金融情報システムセンター（FISC） 監査安全部長　 郡山 信　氏

１．講演概要

システム監査の際に重要なポイントとなる「安全対策」と「コンティンジェンシープラン」の最新の内容について、（財）金融情報システムセンター（以下 FISC）監査安全部長 郡山信氏にご講演いただいた。講演は 2 部構成で、前半は FISC 安全対策基準の概要と改訂内容であり、後半は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の概要と改訂内容であった。講演後の 15 分間では、活発な質疑応答が行われた。

２．講演要旨

(1)はじめに
①FISC の概要
②FISC が刊行する情報セキュリティ関連のガイドライン等
(2)金融機関等コンピュータシステムの安全対策基準（以下 FISC 安全対策基準）の概要と改訂内容
①FISC 安全対策基準の概要
②偽造・盗難キャッシュカード対策
③インターネットバンキング不正対策
(3)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（以下コンティンジェンシープラン策定手引書）の概要と改訂内容
①コンティンジェンシープランが求められる背景
②コンティンジェンシープラン策定手引書の概要
③改訂のポイント
(4)現在の主な活動

３．講演の主な内容

(1)FISC 安全対策基準の概要と改訂内容
①FISC 安全対策基準の概要

金融機関等を取巻く環境要因として、システム化に内在するリスクや金融機関等に対する社会的要請がある。情報システムに関し、金融機関等のよりどころとなる共通の安全対策基準が必要との認識が醸成され、FISC 安全対策基準を策定した。本基準は、設備基準（138 項目）、運用基準（113 項目）、技術基準（53 項目）で構成されている。本基準の利用者は、金融機関や金融機関にシステムを提供するベンダーであり、金融庁の検査官も必要に応じ参照するとある。直近では、2006 年 3 月に FISC 安全対策基準の第 7 版として改訂した。主な改訂内容は以下のとおりである。

・インターネットバンキング対策
・オープン系システムのセキュリティ対策
・外部委託先の監査手続き
・法令対応 等

②偽造・盗難キャッシュカード対策

2003 年度後半より偽造キャッシュカードによる被害が急増してきている。2006 年 2 月 10 日に「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護に等に関する法律」（預金者保護法）が施行された。この法律を受け、今回の改訂では 15 の想定リスクに対して対応策（例えば覗き見防止策、不正機器の検出、伝送データの漏洩防止、カード発行事務の改善等）を策定し、基準に追加している。

例えば、想定リスク「ATM 等で暗証番号入力時に背後から覗き見」に対しては、覗き見防止策が対応策であり、基準の改訂内容は、「ATM 利用時に覗き見を防止する設備とすること（設 113、設 137、技 26 が対応）」である。

預金者保護法制定時における、残された課題としては、窓口取引の犯罪対応、インターネットバンキングの犯罪対応、強固な ATM システムの構築、相互利用性の確保が挙げられている。

③インターネットバンキング不正対策

インターネットバンキングを対象とする犯罪手口には、フィッシング、スパイウェア等が挙げられる。基準では 7 つの想定リスクに対して対応策（例えば、正当なサイトやメールの確認手段、顧客への啓蒙、認証方式の分析、本人認証方式の強化等）を策定し、基準に追加改訂している。

例えば、想定リスク「フィッシングメール等により偽サイトへ誘導される」に対しては、正当なサイトやメールの確認手段が対応策であり、基準の改訂内容は、「口座の不正利用防止のため顧客に注意喚起する事項として以下を記載（運 105-1）する。」である。

・金融機関からの正当なメールであることの確認手段
・金融機関の正当なサイトであることの確認手段

(2) コンティンジェンシープラン策定手引書の概要と改訂内容

①コンティンジェンシープランが求められる背景

わが国の重要インフラ分野が直面するリスクとして、自然災害（地震、火災、台風等）、事故･犯罪(システム障害、情報漏洩、停電、通信障害、テロ等)があり、その結果として、事業の継続、信用、社会的責任、営業利益、企業ブランド、マーケットシェア、企業の存続への影響を挙げている。

②コンティンジェンシープラン策定手引書の概要

金融機関はわが国の重要インフラであり、上記インフラ分野が直面するリスクを踏まえ、コンティンジェンシープラン策定手引書を作成した。手引書では、コンティンジェンシープランを次のように定義している。

コンティンジェンシープランとは、金融機関等のコンピュータセンター、営業店、本部機構等が災害や事故・犯罪・障害等により重大な損害を被り、業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことである。

コンティンジェンシープランの内容は以下のとおりである。

・想定する緊急事態と被害
・影響を受ける業務
・業務の優先度
・代替手段を用いた業務の継続方法
・必要となるリソース
・緊急時体制
・緊急時行動計画（初期対応・暫定対応・復旧対応）
・教育・訓練、維持管理方法

コンティンジェンシープラン策定のサイクルは以下のとおり。

・第１工程：必要性の認識と推進組織の編成

・第２工程：予備調査と基本方針の決定
・第３工程：コンティンジェンシープランの立案
・第４工程：コンティンジェンシープランの決定
・第５工程：コンティンジェンシープランの維持決定

③改訂のポイント

・手引書構成の全面的な見直し
内容の見直しに先立ち、手引書の構成を全面的に見直し、既存の内容を分離した。具体的には、「プロセス」編についてはプラン策定の手順や策定プロジェクトの運営について記載した。「考慮事項」編については、過去の事例等、プラン策定時に考慮すべき入力情報を詳細に記載した。「参考例」編については、帳票イメージや金融機関等の実例を紹介した。

・中央防災会議の報告書の反映
平成17年9月公表の「首都圏直下地震対策大綱」の要求について金融機関としての対応を検討した。具体的に反映した項目は、「発災直後 3 日間程度の応急対応時期の要求内容」、「帰宅困難者問題への対策」、「緊急連絡体制の整備・通信手段の多様化」、「水・燃料の確保」についてである。

・新潟県中越地震における金融機関の対応事例の反映
発災当時の金融機関の対応事例について現地調査を行い、今後、プランを策定する上で有効となる考慮事項を検討した。調査の結果、対策がうまくなされていた点は、自家発電機や回線の二重化、免震構造化の成果、災害対策本部の早期設置であり、課題を残した点は、初期の連絡体制の問題、社会インフラ等の供給停止に伴う燃料や水の確保の問題、自宅が倒壊した職員の宿泊場所確保の問題、交通・輸送の問題であった。手引書にはこれらに加えて、お詫びポスターの雛形、監督当局からの要請事項の事例紹介、各金融機関で実施した震災直後の主な対応内容等を記載した。

・教育・訓練、維持管理等の充実
実効性のあるプランを維持するために、当項目について記載の充実を検討した。具体的には、教育・訓練について手順を見直すとともに、記載の充実を図り、継続的改善の一環として、定期的な内部監査を手順に追加した。

・自然災害以外のリスクについて
自然災害以外のリスクとして、大規模システム障害、風評リスク、情報漏洩リスク、サイバー攻撃リスクを取り上げ、それぞれリスクの特性を整理し、考慮点をまとめた。

(3)現在の主な活動

①システム監査指針（第3版改訂）2007年3月予定
個人情報保護、偽造・盗難キャッシュカード、インターネットバンキング、外部委託、SOX法等を反映する予定。

②安全対策基準（第7版改訂）追補版の検討
ATM取引やインターネット取引に関連した新たな事故・犯罪対応や、金融庁情報セキュリティ検討会の結果を、反映する予定。

③内閣官房情報セキュリティ政策会議 重要インフラ防御施策の対応

４．主な質疑応答

(1)首都直下地震ではマグネチュード7.3は最低ラインなのか。
→最低ラインではない。首都圏においてはマグネチュード7.3をベースとして考えた。

(2)いつまでに金融機関等に対応するように指導するのか。
→FISC の基準は自主基準である。FISC は啓蒙はするが、強制力は持たない。基準は、①「すること」、②「することが望ましい」、③「参考情報」の３つのレベルがあり、

いずれも各金融機関が判断することになる。

(3)基準には、「速やかに対応する」という表現が多いが、時間的にどれくらいと考えればよいか。

→可能な限り早くということで、時間的な設定はしていない。

(4)NISTの暗号化について、具体的なものまで言及しているのか。

→基準には電子政府推奨暗号リストを参考として掲載している。しかし、古いシステムでは、利用できる暗号製品は限られ、選択の幅は限定されると考える。現実的には、個別のシステム環境に応じ、暗号方式や製品が選択されると考える。

５．所感

情報システムの安全対策とコンティンジェンシープラン策定は、組織体にとって重要な課題である。組織体において、これらはその存続のための必要要件といえる。

FISCでは1985年に安全対策基準の初版を発行し、以来版を重ね、現在は第7版を発行している。技術革新の早いICT分野において、陳腐化させずタイムリーに、かつより実効性のある対応を反映してきたのは、FISC関係者の大いなる功績といえる。FISC安全対策基準は、金融機関だけでなく、他業種でも大いに参考になるもので、私自身、流通業、不動産業、官公庁などの各分野にも利用させて頂いた。

FISC安全対策基準やコンティンジェンシープラン策定手引書は、想定リスクを網羅的に設定し、それに基づいて改訂内容を策定している。基準は「すること」「望ましい」「例示」としてまとめられており、大変現実的で使いやすい。

中小金融機関からメガバンクまでが、適用すべき基準が同じということはない。本基準は網羅的に定められているが、採用については金融機関に委ねられている。今後は、過剰投資、重複投資などを防ぐために、金融機関の成熟度を設定し、それに基づいて対策を講じるというフレームも必要かもしれない。

以上

編集・発行　NPO法人 日本システム監査人協会　月例研究会・会報編集部
事務局　tel. 03-3666-6341　Fax.03-3666-6342　saajjk1 (at) titan.ocn.ne.jp