第１２７回月例研究会報告

No.２４０　馬場孝悦

日時：２００７年４月２３日 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：「金融機関等のシステム監査指針（第３版改訂について」
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

金融機関がシステム監査を実施するときの基準となる「ＦＩＳＣ金融機関等のシステム監査指針」の第３版改訂と「ＦＩＳＣ安全対策基準第７版追補」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「システム監査指針」の改訂内容についてであり、後半は「安全対策基準」第７版追補内容とＦＩＳＣガイドライン検索システムの紹介であった。

２．講演要旨

(1)ＦＩＳＣ紹介
①ＦＩＳＣの概要
②ＦＩＳＣが刊行する主なガイドライン等

(2)ＦＩＳＣシステム監査指針第 3 版発刊の経緯と改訂方針，改訂内容

①初版（1987 年 7 月発刊）の構成
②第 2 版（2000 年 7 月発刊）の構成
リスクとコントロールの概念を導入
③第 3 版　改訂方針
下記事項に対応する。
・法律・制度変更への対応
個人情報保護法、預金者保護法、
金融商品取引法　等
・技術・社会情勢の変化への対応
オープン系システムの普及、
外部委託業務の多様化、
金融庁・経済産業省等のマニュアル、ガイドラインの公表　等
・事件・犯罪への対応
大規模システム障害、
偽造・盗難カード犯罪、
インターネット取引犯罪　等
・金融機関等のコンピュータシステムの安全対策基準・解説書（第 5 版～第 7 版）の対応
・金融機関等におけるコンティジェンシープラン策定のための手引書（第 3 版）の対応
④第 3 版の構成
・改訂にあたって
・エクゼクティブサマリー
・本書の利用にあたって
・第１部　フレームワーク
・第２部　チェックポイント集
・資料編
・付表（委員名簿）
⑤第１部　フレームワーク
・第Ⅰ章　システム監査の概念
・第Ⅱ章　システム監査の実践
・第Ⅲ章　システム監査実施上のポイント
⑥第２部　チェックポイント集
・チェックポイント集について
・チェックポイント集一覧表
・用語解説
・要点項目１　情報システムの計画と管理
・要点項目２　情報システムリスクの管理
・要点項目３　情報セキュリティ
・要点項目４　システム開発
・要点項目５　システム運用
・要点項目６　システム利用
・要点項目７　入出力等の処理
・要点項目８　ネットワーク
・要点項目９　システム資産・資源管理
・要点項目１０　外部委託
・要点項目１１　ｺﾝﾃﾝｼﾞｪﾝｼｰﾌﾟﾗﾝ
・要点項目１２　ドキュメンテーション
＊ＥＵＣは第２版では要点項目としてまとめられていたが、ＥＵＣも通常のシステムとできるだけ同様に管理するべきであるという趣旨で独立した要点項目とせずに重複部分は統合し、ＥＵＣ独自部分は他の要点項目に追記、「情報システム部門以外の部門が管理する情報システム上の考慮点」を「要点項目２　情報システムリスクの管理」に追記された。
＊スプレットシートなどにおいてマクロ等で開発するなど容易に改変できる環境で作

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

成したシステムを「簡易システム」と定義し、監査対象として追記された。

⑦資料編
- 資料１　安全対策基準に基づくリスク分析表(例)
- 資料２　システム監査中長期計画書(例)
- 資料３　システム監査基本計画書(例)
- 資料４　システム監査個別計画書(例)
- 資料５　システム監査調書(例)
- 資料６　システム監査報告書(例)
- 資料７　参考文献・関連Ｗｅｂ

⑧チェックポイント集の項目数

「要点項目」－「大項目」－「小項目」の３レベルで構成され、「小項目」毎に「リスク」,「コントロール」,「チェックポイント」が記載されている。

改訂項目数は下記のとおりである。

	新設	削除	変更	各項目数
要点項目	0	1	0	12
大項目	3	6	2	57
少項目	6	13	14	169
リスク	26	19	15	314
コントロール	38	32	31	376
チェックポイント	163	86	143	1101

⑨改訂内容

重要な改訂内容についてその背景や改訂内容について具体的にご講演いただき、非常に勉強になったがこれを紹介するためには本会報をすべて割いても紹介しきれないため、まとめのみの紹介にとどめる。

監査指針第3版改訂ポイント

最新の法律・制度への対応

個人情報保護法、預金者保護法、日本版ＳＯＸ法等の要求事項を反映

金融情報システムを取り巻く社会情勢への対応

Ｗｅｂシステム、インターネットバンキング、外部委託の多様化等のリスクを考慮

「第１部　フレームワーク」の記載充実

経営者関与の重要性、ＩＴガバナンス、内部統制の考え方、システム監査の具体事例等内容を大幅に改編

(3)ＦＩＳＣ安全対策基準第７版追補改訂の背景と改訂内容

①改訂の背景初版
- 安全対策基準策定の背景
- 安全対策基準の改定手順
- 安全対策基準の最近の改訂動向
- 情報セキュリティに関する検討会（金融庁主催平成 18 年 3 月～6 月）
- 事故・犯罪状況
  －偽造キャシュカードの被害状況
  －盗難キャシュカードの被害状況
  －インターネットバンキングの被害状況
- 平成 18 年度安全対策基準検討テーマ

②改訂の内容
- セキュリティ対策の検討のあり方（リスク分析，ＰＤＣＡサイクルの確立）
- ＡＴＭシステム
  －キャシュカード・暗証番号に関する対策
  －防犯体制・防犯設備に関する対策
  －不正防止・情報漏洩防止に関する対策
  －システムに関する対策
  －顧客からの届出受付体制の整備
- インターネットバンキング
  －本人認証方式に関する対策・留意点
  －システムに関する対策
  －顧客からの届出受付体制・被害拡大防止に関する対策
  －顧客への注意喚起

③平成 18 年度安全対策基準の検討テーマ

平成 18 年度安全対策基準の検討テーマは下記の 6 項目である。

Ａ．金融庁「情報セキュリティに関する検討会」検討結果

Ｂ．警察庁「金融機関の防犯基準」（平成 17 年 12 月改正）

Ｃ．モバイルバンキングのリスク分析

Ｄ．情報セキュリティ政策会議による第一次情報システム基本計画対応（政府の重要インフラ防御に関する施策の対応）

Ｅ．暗号化・異常取引検知システムの方策・導入方向の調整

Ｆ．日本版ＳＯＸ法（内部統制に関する実施基準とのギャップ分析）

Ｄは充足されていることが確認され、改訂項目はなかった。

Ｅは電子政府推奨暗号リストの暗号方式の採用

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

が望ましいと本文中に記載した場合、技術・製品の選択範囲が狭まるおそれなどがあり、参考のままに留めた。

Ｆとのギャップ分析した結果現時点では改訂すべき項目はないが、今後も引き続き検討課題とした。

Ａ，Ｂ，Ｃの結果で第７版追補の改訂項目は下記のとおりである。（新設項目はない）

	設備	運用	技術	計
項目数	１３８	１１３	５３	３０４
変更数	１	１８	９	２８

(4)ＦＩＳＣガイドライン検索システム

安全対策基準、システム監査指針などのガイトラインを検索したり、検察条件にあうものをＥｘｃｅｌ出力したりできる検索システムが提供されている。

３．所感

ＦＩＳＣのガイドラインは業界の自主基準でありその扱いは各金融機関が判断することになるが、事実上の金融機関の標準であり、私自身もデータセンターのアウトソーシング業務のシステム監査などでシステム監査指針や安全対策基準を利用させてもらった。今回の改訂は時代の流れを反映して、より使いやすくなった。信頼性・安全性を求める他業種の方にも参考になることであろう。

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