金融に関するシステム監査概論

2010年10月

有限責任監査法人トーマツ
パートナー　福島 雅宏

本日お話しする内容は講師の私見であり、
講師の所属する法人の公式見解ではないことをご了承願います。

本研修のねらい

■「システム監査」は、様々な目的・形態・実施主体等により実施される。いくつかの観点での分類・整理を通して、システム監査の基本概念を理解する。

■金融機関に関連するシステム監査の類型とそれぞれの差異について理解する。

■金融機関におけるシステム監査の一例として、金融検査マニュアルに基づくシステムリスク監査の基本的な概念を理解する。

目次

1.システム監査の基本概念

1-1 システム監査の分類

法定監査と任意監査

■ 法定監査

- 金融商品取引法や会社法など、法律で監査を受けることを義務付けられている企業・団体に対する監査
  - 財務諸表監査、内部統制監査等

※財務諸表監査、内部統制監査におけるIT統制の検証が、システム監査に類するものに該当するが、IT統制そのものへの意見表明ではないため、その観点ではシステム監査ではない。

■ 任意監査

- 法定監査以外の監査
- 通常のシステム監査は任意監査

1-1 システム監査の分類

保証型監査と助言型監査

【情報セキュリティ監査制度（経済産業省）】

■保証型監査

- 「監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を伝達する監査の形態」

■ 助言型監査

- 「監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態」

（出典：「情報セキュリティ監査研究会報告書」（経済産業省））

下線講師付記

1-1 システム監査の分類

保証型監査と助言型監査

■ 日本公認会計士協会より、公認会計士または監査法人が行う保証業務に関する研究報告、実務指針等が公表されている。

- 「公認会計士等が行う保証業務等に関する研究報告」（監査・保証実務委員会研究報告第20号）
- 「ITに係る保証業務等の実務指針（一般指針）」（IT委員会報告第5号）
- 「情報セキュリティ検証業務」（IT委員会研究報告第39号）

■「 ITに係る保証業務等の実務指針（一般指針）」における保証業務

- 「～保証報告書の利用者に対して信頼性を付与するために、業務実施者が自ら入手した証拠に基づき基準に照らして判断した結果を結論として報告する業務～」
- 保証業務の内容がITに係るものに限定される。

1-1 システム監査の分類

外部監査と内部監査

- 外部監査
  - 外部利害関係者等のための外部目的の監査
- 内部監査
  - 経営者のための内部目的の監査

※監査実施主体による分類でないことに留意

1-2 システム監査の目的
主なシステム監査フレームワークにおける定義

フレームワーク	発行機関	目的・主旨
金融機関等のシステム監査指針	(財)金融情報システムセンター(FISC)	「情報システムの有効性、効率性、信頼性、安全性及び遵守性を達成できるよう、情報システムリスクを把握し、情報システムに係るコントロールが適切かつ効果的であることを、被監査部門から組織的に独立したシステム監査人が検証し、その結果を保証意見または助言勧告としてとりまとめ、経営者に報告する監査」
システム監査基準	経済産業省	「組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な監査人が検証または評価することによって、保証を与えあるいは助言を行い、もってITガバナンスの実現に寄与すること」
情報セキュリティ監査制度	経済産業省	「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと」

下線講師付記

1-2 システム監査の目的

主なシステム監査フレームワークにおける定義（つづき）

システム監査

情報システムにまつわるリスクに対する**コントロール**がリスクアセスメントに基づいて適切に**整備・運用**されているか

■「コントロール」（統制）に着目することが重要
■ コントロールの整備状況・運用状況の両面の観点で評価

【参考】
「システム監査基準」の平成16年改訂前の定義

「監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動」

下線講師付記

1-2 システム監査の目的

ITに係る統制

■「ITに係る内部統制の枠組み」（IT委員会研究報告第35 号）

- ITに係る内部統制の概念の理論的な整理を目的としたもの

- 自動化された業務処理統制
  - 「自動化された業務処理統制とは、情報の正確性、網羅性、適時性、正当性等の達成のためにアプリケーションシステムに組み込まれた内部統制」
- 全般統制
  - 「企業の自動化された業務処理統制等が、経営者の意図したとおり整備され、継続的に運用されることを支援するための仕組み、活動」
- 自動化された業務処理統制と全般統制の関係
  - 「全般統制の有効性は、自動化された業務処理統制が継続的に有効に機能しているという心証を与える。したがって、ある自動化された業務処理統制を支える全般統制が有効に機能していない場合、その自動化された業務処理統制が意図されたとおりに継続的に運用されているという心証を、全般統制以外の方法で得なければ、その自動化された統制活動が有効に機能していたとはいえないことになる。」

1-2 システム監査の目的

ITに係る統制（IT全般統制・IT業務処理統制）

2.システム監査の類型

2-1 財務諸表監査におけるIT統制の検証

■制度概要

- 会社法、金融商品取引法等に基づく財務諸表監査において、財務報告の信頼性に関する内部統制の検証の位置付けで実施される。
- ITの統制目標例

「①　準拠性：情報が会計原則、会計基準、関連する法律及び社内規則等に合致して処理されていること

②　網羅性：情報が漏れなくかつ重複なく記録されていること

③　可用性：情報が必要とされるときに利用可能であること

④　機密性：情報が正当な権限者以外に利用されないように保護されていること

⑤　正確性：情報が正確に記録され、提供されていること

情報システムが、企業の業務プロセスで要求される有効性及び効率性の水準を満たしているか否かは、監査人にとって直接的に評価する対象ではない」

（出典：「財務諸表監査における情報技術（IT）を利用した情報システムに関する重要な虚偽表示リスクの評価及び評価したリスクに対応する監査人の手続について」（IT委員会報告第3号）

■保証／助言

- 財務諸表監査自体は保証業務。ただし、IT統制に関して単独で保証を与えるものではない。

■実施者

- 外部監査人

下線講師付記

2-2 内部統制評価及び監査におけるIT統制の検証

■制度概要

- 金融商品取引法に基づく内部統制報告制度において、財務報告の信頼性に関する内部統制の評価及び監査の位置付けで実施される。
- 「ITへの対応」
  - 組織目標を達成するために予め適切な方針及び手続を定め、業務の実施において組織内外のITに対し適切に対応すること
- ITの統制
  - 全社統制のうちITに関するもの
  - IT全般統制
  - IT業務処理統制

2-2 内部統制評価及び監査におけるIT統制の検証（つづき）

■制度概要

- ITの統制目標

「①　業務の有効性及び効率性：情報が業務の効果的、効率的な遂行を支援するために適時に提供されること

②　準拠性：情報が関連する法令や会計基準、社内規則等に合致して処理されていること

③　信頼性：情報が組織の意思・意図に沿って承認され、漏れなく正確に記録・処理されること（正当性、完全性、正確性）

④　可用性：情報が必要とされるときに利用可能であること

⑤　機密性：情報が正当な権限者以外に利用されないように保護されていること

ITの統制として、財務報告の信頼性を確保するためのITの統制を整備しようとするものであり、財務報告の信頼性以外の他の目的を達成するためITの統制の整備及び運用を直接的に求めるものではない」

（出典：「財務報告に係る内部統制の評価及び監査に関する実施基準」

■保証／助言

- 内部統制監査自体は保証業務。ただし、IT統制に関して単独で保証を与えるものではない。

■実施者

- 評価：内部監査人等　　監査：外部監査人

2-3 18号／SAS70検証におけるIT統制の検証

■制度概要

- 業務委託会社の財務諸表監査を行う監査人に対し、業務受託会社の監査人が、監査基準委員会報告書18号またはSAS70による実務上の指針に基づき、業務受託会社の「内部統制の整備及び運用状況の検証報告書」を発行する。
- 業務委託会社及びその監査人は、発行された検証報告書を活用し、委託先における内部統制の整備及び運用状況を把握する。
- 委託業務における内部統制の一部として、IT統制が検証対象となる場合がある。

※SAS70：米国公認会計士協会（AICPA）が発行する監査基準書（Statements on Auditing Standards）の第70号（Service Organization）

■保証／助言

- 保証業務

■実施者

- 外部監査人

2-4 情報セキュリティ監査制度

■制度概要
- 民間企業や政府、地方公共団体の情報セキュリティ対策の監査を目的とし、2003年に経済産業省により開始された。
- 監査実施者の行為規範である「情報セキュリティ監査基準」と、監査にあたっての判断の尺度となる「情報セキュリティ管理基準」とからなる。
- 情報システムのセキュリティだけでなく、情報資産全体のセキュリティマネジメントが監査の対象。

■保証／助言
- 「助言型監査」と「保証型監査」の監査方式が示されている。

■実施者
- 外部監査人または内部監査人

2-5 システムリスク監査

■制度概要
- 特に定められた制度・フレームワークはない。
- 一般的には、金融検査マニュアルや、「金融機関等のシステム監査指針」（FISC）に基づくシステムリスク管理態勢の適切性についての監査を指すことが多い。

■保証／助言
- 通常は助言型監査

■実施者
- 外部監査人または内部監査人

3.金融機関における システムリスク監査

3-1 金融検査マニュアルの位置付け・性格

（1）金融検査官用のマニュアルとしての性格

あくまでも検査官が金融機関を検査する際に用いる手引書である。

（2）金融機関向けのガイドラインとしての性格

各金融機関においては、自己責任原則に基づき、経営陣のリーダーシップの下、創意・工夫を十分に生かし、それぞれの規模・特性に応じた方針、内部規程等を作成し、金融機関の業務の健全性と適切性の確保を図ることが期待される。

システム監査の基準

3-1 金融検査マニュアルの位置付け・性格（つづき）

規制・法制度の変遷

内部統制＝リスク管理のためのシステム

⇒　システム監査の目的：内部統制の評価＝リスク管理態勢の評価

施行日等	規制及び法制度	発行機関
1992年9月	「内部統制 ― 統合された枠組み（Internal Control-Integrated Framework）」	COSO
1998年9月	「銀行組織における内部管理体制のフレームワーク」	バーゼル委員会
1999年7月	**「預金等受入機関に係る金融検査マニュアル」**	金融監督庁
2003年6月	「リスク新時代の内部統制　―　リスクマネジメントと一体となって機能する内部統制の指針」	経済産業省
2005年7月	「会社法」において、内部統制システムを一般的制度として導入	
2005年8月	「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組みについて」	経済産業省
2006年6月	「金融商品取引法」において、内部統制報告書の提出義務を規定	
2007年2月	「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」	企業会計審議会

3-2 システムリスク監査と財務報告に係るIT統制の検証との比較

【システムリスクの定義】
システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクをいう。

－財務報告に係るIT全般統制

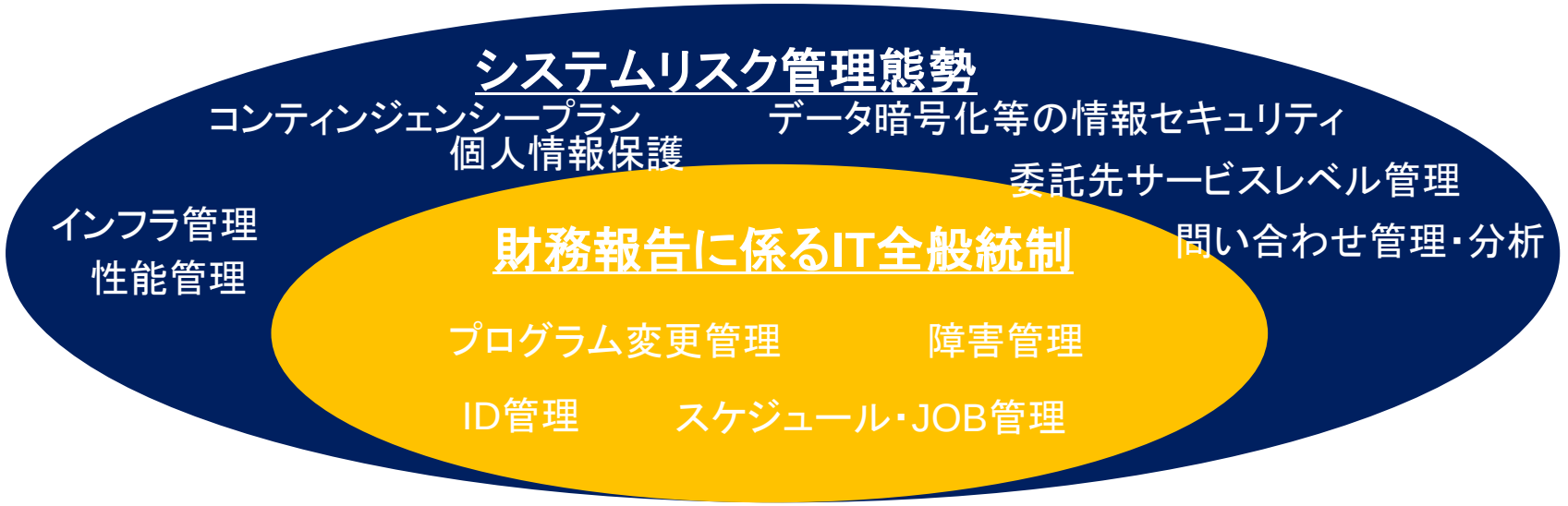
財務報告目的の内部統制の検証を行う。

→検証範囲は財務諸表の信頼性に関わる範囲に限定される。

－システムリスク監査

金融機関が業務の健全性及び適切性の観点からシステムリスク管理態勢の整備・確立を行っているかどうかについて検証する。

→検証範囲には業務活動の有効性・効率性や法令遵守等の観点を含み、より広範にわたる。



3-3 金融検査マニュアルの構造

平成19年の改訂

■ 改訂前検査マニュアル

- 管理方針や組織体制・規定の整備を求める（＝**静的態勢の整備**）

■ 改訂後検査マニュアル

・既存の態勢を常に改善していく動的プロセスとしての内部管理態勢（=**動的態勢・PDCAサイクルの検証**） ～単なる「体制の整備」は終わった

・金融検査評定制度の評定段階との整合性・・・経営陣による態勢構築と経営陣が果たす役割、責任の明確化

→三段構成

「Ⅰ．経営陣による態勢整備・確立状況」

～経営陣による内部管理態勢の整備およびPDCAサイクルの有効性の検証

「Ⅱ．管理者による態勢整備・確立状況」

～管理者及び管理部門が果たすべき役割と負うべき責任

「Ⅲ．個別の問題点」

～個別具体的な論点について

※Ⅱ．Ⅲ．で問題が発見された場合にはⅠ．のどの部分が有効に機能していないかを検証する。

・個別項目の新設

✓ATMでの盗難・偽造カードの不正利用に対する対応。

✓インターネット取引におけるフィッシング詐欺への対応。

✓銀行法改正に伴うシステム関係の業務委託先への検査対応。

3-3 金融検査マニュアルの構造（つづき）

Ⅰ.経営陣によるシステムリスク管理態勢の整備・確立状況

経営陣による態勢整備

Plan 方針の策定 → Do 規程・組織体制の整備 → Check 評価 → Action 改善活動

既存の態勢を改善していくためのPDCAサイクルがまわっているか？

Ⅱ.管理者によるシステムリスク管理態勢の整備・確立状況

管理者

管理部門

問題点が認められる場合、Ⅰ．のいずれの要素の欠如又は不十分に起因して発生したものであるか？
→川下から川上への検証プロセス

Ⅲ.個別の問題点

情報セキュリティ管理

システム企画・開発・運用管理等

防犯・防災・バックアップ・不正利用防止

Ⅰ．またはⅡ．のいずれの要素の欠如又は不十分に起因して発生したものであるか？

「金融検査マニュアル便覧」（社団法人金融財政事情研究会）より作成

3-4 システムリスク監査の効果的な実施

- 金融検査マニュアルでは、適切なリスク管理を行うための態勢整備が期待されているが、システムリスク態勢の構築や、構築した態勢を維持強化するためには、モニタリング機能としてシステムリスク監査の継続的な実施をひとつの手法として活用することが有効。
- 金融検査マニュアルを基準とした評価を基本としつつ、「金融機関等のシステム監査指針」(FISC)等の各基準を評価項目へ導入することや、評価結果、環境変化等を踏まえた個別テーマを設定することにより、モニタリング機能としてのシステムリスク監査がより有効になる。

システムリスク管理態勢に関する各種スタンダードを基準とした評価
－「金融検査マニュアル」(金融庁)
－「金融機関等のシステム監査指針」(FISC)
－「金融機関等コンピュータシステムの安全対策基準」(FISC)

システム管理態勢に関する各種スタンダードを取り入れることで、モニタリング基準を強化

評価結果、環境変化等を踏まえたテーマ毎の評価
－新システム導入等、重要なシステム環境の変化があった場合
－法令・制度的に求められる管理態勢等
－異なる監査手法の導入（技術的セキュリティ診断の導入など）

リスクの高い分野や法的、制度的に求められる管理態勢については、テーマに沿った個別の監査基準や手続を設定し実施する

システムリスク管理態勢の継続的なモニタリング

3-4 システムリスク監査の効果的な実施（つづき）

各種スタンダードの活用

▪「金融機関等のシステム監査指針」(FISC)、「金融機関等コンピュータシステムの安全対策基準」(FISC)等により、金融庁検査マニュアルを補足する。

預金等受入金融機関に係る検査マニュアル				本システムリスク監査におけるチェックポイント等	
大項目	中項目	小項目	チェック項目	監査のチェックポイン	査閲資料
Ⅲ.個別の問題点	2.(2)システム企画・開発態勢	①企画・開発態勢	(ⅰ)信頼性が高くかつ効率的なシステム導入を図る企画・開発のための内部規程・業務細則等を整備しているか。	① 信頼性が高くかつ効率的なシステム導入を図る企画・開発のための内部規程・業務細則等を整備しているか。	・「リスク管理規程」 ・「情報システム管理規程」 ・「システム開発管理規程」
			(ⅱ)システム企画・開発を行うに当たり、例えば、機械化委員会等の横断的な審議機関を設置し検討しているか。	① 情報システム運営委員会等が設置され、その責任、権限、開催要領に係る手続きが定められているか。 ② 上記の手続は取締役会等の承認を得ているか。 ③ 情報システム運営委員会等の構成は、全社的な情報システム運営を行うために次のような構成になっているか。 （例） － 情報システム担当役員 － 情報システム部門の責任者 － 本部各部門等の責任者 － EUC実施部門の責任者　等	・「情報システム運営委員会規程」 ・「情 員 ・情 会

「金融機関等のシステム監査指針」での補足

4.検査事例から学ぶシステムリスク監査の着眼点

「Ⅰ.経営陣によるシステムリスク管理態勢の整備・確立状況」

1. 方針の策定

【チェック項目概略】

•取締役の役割・責任

•戦略目標

•システムリスク管理方針の整備・周知　　等

【指摘事例】

•「経営陣は、セキュリティポリシーに規定すべき内容に係る理解が不足していることから、保護されるべき情報資産や保護すべき理由等を定めていないなど、不適切なものとなっている。［地域銀行］」（検査指摘事例集H18）

【着眼点】

•金融機関においては、情報システムの安全対策を組織として統一された方針に基づいて策定する必要があり、そのためには経営層が関与し、方針・ルールを明文化する必要がある。

•上位の方針の不備が、下位規程の不備及び実態面のリスクにつながる可能性がある。

「Ⅰ.経営陣によるシステムリスク管理態勢の整備・確立状況」

2. 内部規程・組織体制の整備

【チェック項目概略】

•内部規程の整備・周知

•オペレーショナル・リスクの総合的な管理部門の態勢整備

•各業務部門及び営業店等におけるオペレーショナル・リスクの総合的な管理態勢の整備

•取締役会等への報告・承認態勢の整備　　等

【指摘事例】

•「取締役会は、重要なシステムの開発遅延による計画の大幅な変更を余儀なくされているなどの問題に対して、進捗報告の定期的な報告を求めていない等。[地域銀行]」（検査指摘事例集H22）

【着眼点】

•リスク事象について、取締役会への報告態勢が整備され、実効的に機能することが重要。「情報と伝達」は内部統制の重要な要素の一つ。

「Ⅰ.経営陣によるシステムリスク管理態勢の整備・確立状況」

3. 評価・改善活動

【チェック項目概略】

•分析・評価

•改善活動

【指摘事例】

•「顧客に影響を及ぼす重大障害が多数発生している中、経営会議は、品質改善計画や障害に備えたコンティンジェンシープラン、障害発生時の対応などについて報告や改善状況を求めていない。［主要行等及び外国支店銀行］」（検査指摘事例集H22）

【着眼点】

•経営陣によるPDCAが実効的に機能することが、リスク管理態勢が有効に機能するための必要条件。

•「川下から川上へ」の評価。

「Ⅱ.管理者によるシステムリスク管理態勢の整備・確立状況」

1. 管理者の役割・責任

【チェック項目概略】

•システムリスク管理規程の整備

•組織体制の整備　　等

【指摘事例】

•「管理者は、システムリスク管理規程においてシステムリスク管理の状況の評価方法等を定めていないほか、システムリスクに係る安全対策基準を具体化していないことから、各システムのリスク評価が不十分なものとなっている。[地域銀行]」（検査指摘事例集H18）

•「情報セキュリティ管理者について、委託先におけるセキュリティ管理状況を把握しておらず、セキュリティに関する重要情報が流出しているほか、OAシステム等の重要システムのサーバ設置場所への入室権限を職務の実態からみて必要のないものに対して与えているなど、不適切なものとなっている。[主要銀行及び外国銀行支店]」（検査指摘事例集H17）

【着眼点】

•組織として統一された方法で、全社的にリスクを把握し、リスクに応じた対策を講じる仕組みが有効に機能することが必要。

「Ⅱ.管理者によるシステムリスク管理態勢の整備・確立状況」

2. システムリスク管理部門の役割・責任

【チェック項目概略】

•システムリスクの認識・評価

•見直し　等

【指摘事例】

•「システムリスク管理部門は、各部が運用する部門サーバーの管理について適切なモニタリングや指導を行っていないことから、データファイルの管理やバックアップの確保、監視体制の整備が行われていない。［地域銀行］」（検査指摘事例集H18）

【着眼点】

•システムリスク管理部門は、システム部門が所管するシステムだけでなく、部門システムについてもリスクを認識し、管理策を講じることが必要。

「Ⅲ.個別の問題点」

1. 情報セキュリティ管理

【チェック項目概略】

•情報セキュリティ管理等の役割・責任

•不正使用防止

•コンピュータウィルス等

【指摘事例】

•「情報セキュリティ管理者は、情報資産の管理状況の点検結果を踏まえた対応策や計画を策定していないほか、コンピュータセンターに設置している顧客情報等の照会が可能な営業店端末に対してアクセス制限等によるセキュリティ対策を講じていない。[地域銀行]」(検査指摘事例集H18)

•「営業店において、本部サーバーを通じ外部との接続が可能になったにもかかわらず、コンピュータウィルスの侵入を防止するための方策が講じられてこなかったことから、営業店のパソコンにスパイウェアが侵入している。[信用金庫及び信用組合]」(検査指摘事例集H18)

【着眼点】

•情報セキュリティの技術的な対策だけでなく、情報セキュリティマネジメントが有効に機能することが必要。

「Ⅲ.個別の問題点」

1. 情報セキュリティ管理（つづき）

【チェック項目概略】

•インターネットを利用した取引の管理

•偽造・盗難キャッシュカード対策

【指摘事例】

•「システム担当部署は、インターネットバンキングについて、不正利用等は発生していないと誤って認識して、規程等の整備を行っていないことから、預金の不正払い戻しや詐欺等の犯罪を想定し具体的な保障方針などを策定していない。［地域銀行］」（検査指摘事例集H22）

【着眼点】

•インターネットバンキングのリスクについての認識およびリスクへの対応が必要。

「Ⅲ.個別の問題点」

1. 情報セキュリティ管理（つづき）

【参考】インターネットバンキングのセキュリティ対策(FISC安全対策基準第7版追補改訂 Ⅳ.1 (2)より作成）

フェーズ	リスク	対策
Ⅰ. 金融機関内のシステム・体制の構築	情報の流出	✓重要な情報の機密保護対策 ✓外部委託先のアクセス権限の明確化 ✓重要なデータについての暗号化 ✓アクセス履歴の管理
Ⅱ. インターネットバンキング利用時	スパイウェアによるID・認証情報の漏えい	✓顧客への注意喚起(不審なCD-ROMへの対応、最新セキュリティの適用など)
	フィッシングサイトでのID・認証情報の詐取	✓顧客への注意喚起 ✓電子メール運用方針の明確化 ✓第三者機関の証明書によるサイト認証
	IDと認証媒体の盗難	✓顧客への注意喚起 ✓リスク分析に基づく認証方法の選択
	パスワードの再交付過程での漏えい	✓パスワード再発行時の本人確認の厳格化 ✓乱数表等の本人確認媒体の管理方法の明確化
Ⅲ. 不正取引の発生時	なりすまし行為	✓適切な本人確認機能の導入 ✓ワンタイムパスワードの使用 ✓顧客への注意喚起
Ⅳ. 被害発生時	異常取引を検知しにくい	✓アクセス日時の表示 ✓取引結果の表示とメール通知 ✓登録メールアドレス変更時の本人確認
	多額の損害が発生する	✓資金移動先や限度額の設定
	証拠が確保できない	✓復旧作業時のデータ取得 ✓顧客対応方針の明確化 ✓不正使用取引、不正取引失敗ログの記録

「Ⅲ.個別の問題点」

3. 防犯・防災・バックアップ・不正利用防止

【チェック項目概略】

- システム開発・運用部門の相互牽制体制
- システム企画・開発体制
- システム運用体制
- システム監査

【指摘事例】

- 「システム障害への対応については、システムリスク管理部門が障害報告書を作成することにしているが、明確な作成基準がないことから、部門長が軽微と判断した障害や営業店で復旧した障害については、ATMの停止など顧客に影響を及ぼす障害であっても報告書は作成されず、取締役会にも報告されないなど、障害の原因分析や再発防止策の検討が適切に行われる態勢となっていない。[地域銀行]」(検査指摘事例集H18)

【着眼点】

- リスク事象の発現であるシステム障害については、根本原因にさかのぼって再発防止策を講じるとともに、障害傾向の分析等により、発生を未然に防止する取り組みも必要。

「Ⅲ.個別の問題点」

3. 防犯・防災・バックアップ・不正利用防止

【チェック項目概略】

•防犯対策

•コンピュータ犯罪・事故等

•防災対策

•バックアップ

•コンティンジェンシープランの策定

【指摘事例】

•「コンティンジェンシープランについては、オンライン稼働中など被災のタイミングに応じたシナリオが想定されていないうえ、消失した取引データの具体的な復元手順が定められていないなど、実効性のあるプランとなっていない。[地域銀行]」(金融検査指摘事例集 H18)

【着眼点】

•コンティンジェンシープランについては、その実効性についても評価する。

「Ⅲ.個別の問題点」

5. システム関係の業務委託先の検証

【チェック項目概略】

•システムリスクの認識・評価

•委託者による監査又は外部監査

•セキュリティレベルの合意

•企画・設計・開発・テストでの金融機関の関与

•品質管理体制の整備

•金融機関への定期的な報告

•システム障害発生時の連絡体制　　等

【指摘事例】

•「システムリスク管理部門は、情報システムの開発や管理等を外部委託先に業務委託しているものの、運営規程等において、具体的な委託管理項目及び評価項目等を定めていないことから、コンピュータ稼働環境の整備や機器の保守・点検などに係る評価が十分に行われていない。[主要行等及び外国銀行支店]」(金融検査指摘事例集 H22)

【着眼点】

•委託業務内容に適合した管理項目・評価項目が設定されていることが必要。

•検査マニュアルのチェック項目は、業務委託先に対するものであるが、委託元についても適切な状況把握・管理が求められる。

5.まとめ

5．まとめ

✓システム監査の諸類型については、それぞれの目的・対象範囲等を正しく理解することが重要。

✓システムリスク監査において、リスク管理態勢を適切に評価するためには、金融検査マニュアルの構造やチェック項目の趣旨を理解することが必要。

✓個別事象の検出だけでなく、その原因となるマネジメントプロセスの有効性についても評価する。

✓必要に応じて、「金融機関等のシステム監査指針」(FISC)等により補足することも有用。ただし、単なるチェックポイントの確認に終わらず、監査対象にとって重要な内部統制は何かを識別し、その有効性を評価することが重要。