金融高度化セミナー資料

2011年1月28日

金融機関におけるシステムリスク管理と委託先管理

日本銀行　金融機構局

日本銀行
BANK OF JAPAN

本日の説明内容

日本銀行金融機構局の公表ペーパー「金融機関におけるリスク管理の現状 —— 事例からみたリスク管理の具体策」、「金融機関におけるシステム共同化の現状と課題」を基に、システムリスク管理や委託先管理のポイントや留意点を説明する。

1. システムリスク管理の必要性
2. システムリスク管理のポイント
3. システムリスク管理に関する要改善事例
4. リスク・ファクターの変化
5. 委託先の管理状況、委託先管理の基本的な考え方
6. 人材の確保

1. システムリスク管理の必要性

システムは、・・・・・

- 業務を正確かつ効率的に遂行するうえで必要不可欠な存在
- 相互にネットワーク化され全体として大きな金融業務インフラを形成
- 膨大な顧客情報を処理

障害における業務処理停止や、不正アクセスによる情報漏洩は、金融機関経営において、重大なリスク

・小さなプログラム・ミス等が業務処理全体を止める可能性
・ある先で発生した障害が、他社に影響する可能性

金融機関では、システムリスクを主要リスクと位置付け、リスクを管理。

1. システムリスク管理の必要性（続き）

（参考）システムリスク管理の観点

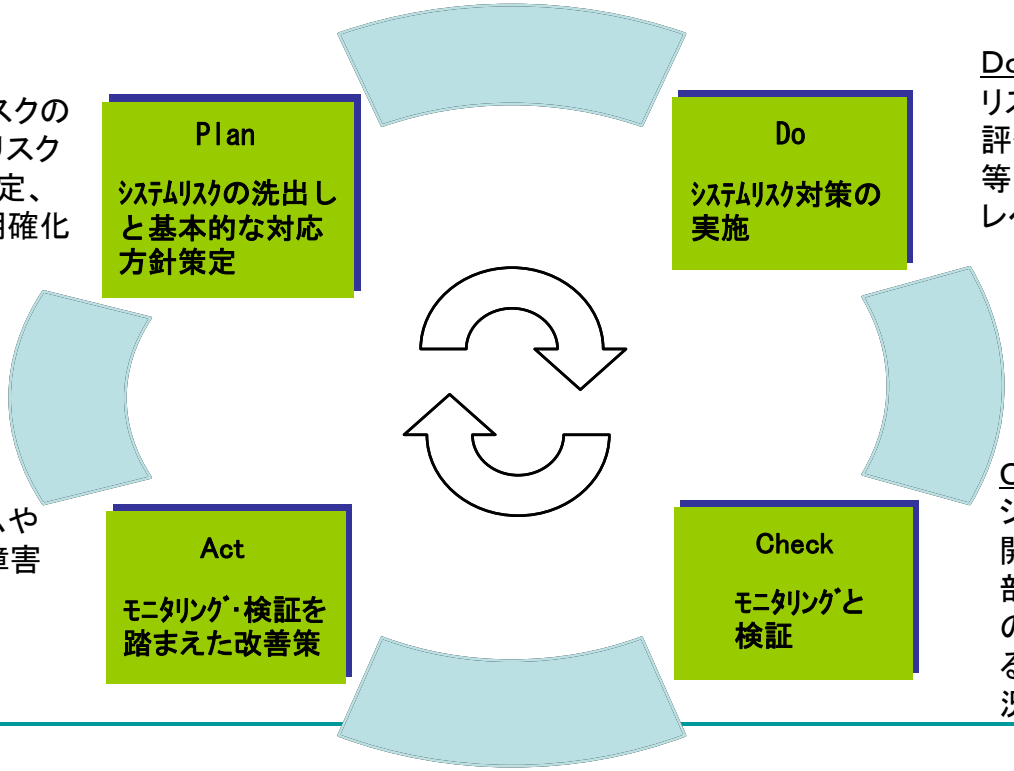
観　点	内　容	具体的なリスクの例
安定性 （可用性）	・災害、障害等からのシステムの保護	・システム・ダウンによる業務停止
安全性 （機密性） （完全性）	・犯罪、不正行為等からのシステムの保護	・内部不正による顧客情報の漏洩 ・ハッカーによる不正アクセス
信頼性	・システムが提供する情報や機能の正確性確保	・システムの提供する情報の誤りによる業務トラブルの発生
遵守性	・法令・規制・規程の遵守	・レピュテーションの低下
有効性	・経営や戦略の策定・実現に必要な情報・機能の提供	・不十分な情報に基づく経営戦略の策定
効率性	・高い生産性での情報・機能の提供	・システムの開発・運用コスト増加 ・システムの拡張性・柔軟性の低下

2. システムリスク管理のポイント

(1)システムリスク管理に関するPDCAサイクルの実施

- 全社的なシステムリスクのプロファイルを把握し、リスク管理強化策を検討のうえ、開発や運用の現場に反映していく一連のプロセスを構築。
- 障害分析やシステムリスク評価を踏まえ、自行に内在しているシステムリスクを把握。

Plan:
顕在化事象の収集、潜在リスクの状況把握、経営陣の認識、リスク管理方針と基本ルールの制定、システムリスク統括機能の明確化等



Do:
リスク管理の対応方針等に基づき、評価結果を踏まえた個別システム等へのリスク管理強化策、実務レベルのマニュアル類の整備

Act:
リスク対策が未了なシステムや分野への対処策、システム障害再発防止策の立案実施

Check:
システム障害分析を踏まえた開発管理体制等の評価や、部内検査等を通じたリスク対策の実効性評価、各部署におけるリスク管理ルールの遵守状況点検、システム監査等

2. システムリスク管理のポイント

(2)システム開発管理

- リソースの確保とプロジェクト管理体制の構築(ユーザーとの円滑なコミュニケーションの確立など)
- 進捗管理手続を整備(進捗の遅延等を早期に発見し、対処するための仕組みを作るなど)
- 開発管理規程等を整備(開発工程完了基準やリリース判定基準の整備、品質管理・性能評価の実施など)

(3)システム運用管理

- システムの稼働状況を監視(重要なシステムは、ハードやプログラムの稼働状況を監視するなど)
- キャパシティやパフォーマンスを管理(CPU、メモリ、ディスクなどの使用量に関し上限値を設けて稼働状況をモニターするなど)
- オペレーションを管理(適切なジョブ・コントロール、オペレーション・マニュアルの整備など)
- 維持管理、保守・サポートの実施(パッチ等の適用、保守要員等の確保など)

2. システムリスク管理のポイント

(4)システム障害対策、システム障害管理

- 障害の未然防止策、障害発生後の影響極小化策を講じる(システムの多重化、重要ファイルのバックアップ、障害対応マニュアル等の整備など)
- 障害の連絡、報告体制を整備
- 障害原因を分析し、再発防止策を検討・実施(複数の障害における傾向分析も活用)
- 障害訓練を実施(外部委託先やユーザー部門を含めた訓練も実施)

(5)情報セキュリティ対策

- システム開発と運用の職務を分離
- 本番データのセキュリティを確保(開発部署における本番データの使用に関するルールを定めるなど)
- 物理的なアクセスを管理(センターの入退室管理、外部記憶媒体等の管理など)
- 論理的なアクセスを管理(ID・パスワードの管理、アクセスの監視など)
- サイバーテロ対策、外部侵入対策を実施
- コンピュータ・ウィルス対策を実施

2. システムリスク管理のポイント

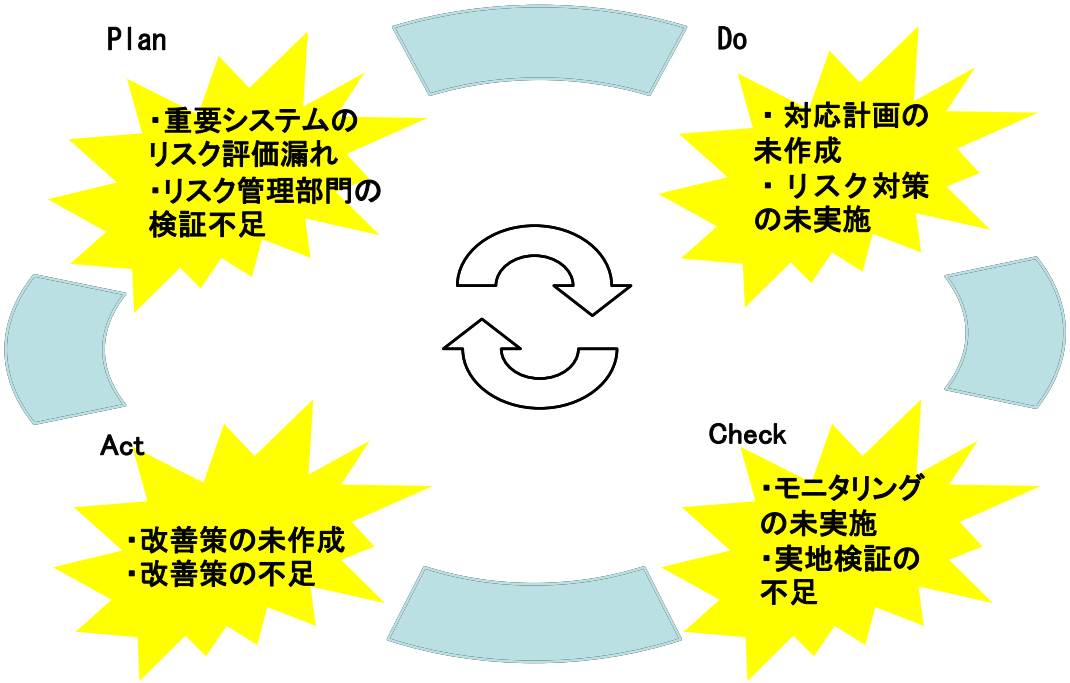
(6)システム監査

- リスクプロファイルを把握(規程等の遵守状況を確認するのみではなく、リスクプロファイルの抽出が適切にできているかをチェック)
- リスクプロファイルの変化に応じた監査を実施(監査計画を立て、効果的に監査を実施。外部監査も活用)
- 内部監査等で判明した問題点の改善状況をフォローアップ
- オープン系システムの利用拡大や新技術の採用など、システムリスクのプロファイルの変化を踏まえ監査要員を育成

3. システムリスク管理に関する要改善事例

①PDCAサイクルの実践

【要改善事例】
リスクの洗出しと対応方針の策定を起点としたPDCAサイクルが回っていない。



・ リスク管理体制の整備で満足するのではなく、PDCAサイクルを回す。

3. システムリスク管理に関する要改善事例

②リスク管理規程の定期的な見直し

【要改善事例】
分散系システムの利用が増えているにもかかわらず、システムリスク管理規程に利用システム形態の変化等が反映されていない。
暗号化強度等をシステム構築後見直していない。

- リスク管理規程（セキュリティポリシー等）は、作成後殆ど見直していない。
- コンピュータ処理能力の向上等により、犯罪者による暗号の解読が容易化。
- 偽造キャッシュカード、フィッシング等コンピュータシステムに関連した新たな金融犯罪への対応に遅れ。
- 適切な対策が取られていないため、犯罪の標的に。

・ 管理サイクルの適切な実施により、リスク管理規程や対策の陳腐化を防ぐ。

3. システムリスク管理に関する要改善事例

③EUC（End User Computing）システムのリスク評価

【要改善事例】
システムの重要度・脆弱性等の評価の尺度が部署ごとに異なったままで評価の基準を統一した全社横断的なリスク評価が行われていない。

- EUCシステムのため、システムリスク評価の対象外となっていた。
- このシステムのプログラム変更を行った際、十分なテストを行わなかった。
- システムリスク評価を行っていれば、開発管理が不十分なことを発見可能であった。

・ EUCシステムであっても、重要なものは全社的な基準でリスク評価を実施する。

3. システムリスク管理に関する要改善事例

④新規開発システムのリスク評価

【要改善事例】
　新規に開発したシステムのリスク評価を行っていないため、リスク管理規程を満たさないシステムが稼働。

- リスク評価は、現行システムのみを対象としている（開発中のシステムをリスク評価する仕組みがない）。
- 開発中のシステムに対しリスク評価を行わなかったために、稼働開始後のリスク評価で潜在リスクが発見された。
- 潜在リスクを解消するために開発後に対応を行ったが、開発途中に比べコストを要した。

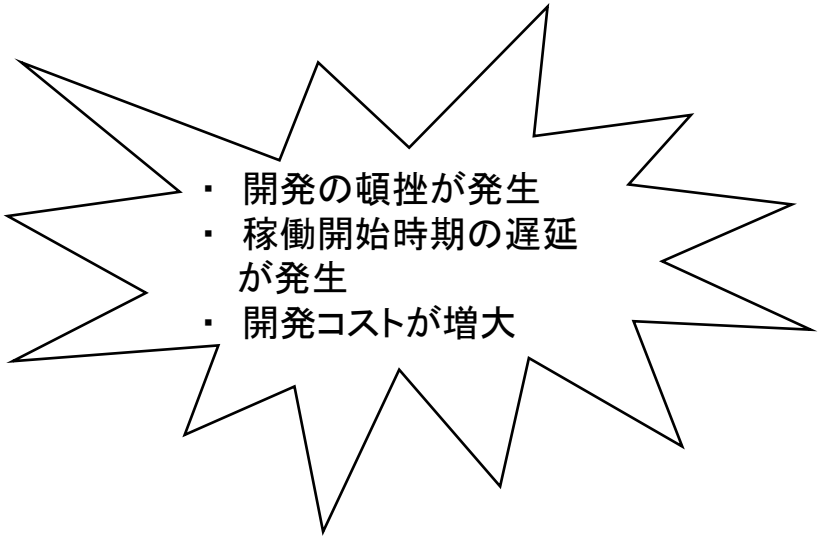
・ 現行システムだけでなく開発中のシステムもリスク評価を行う。

3. システムリスク管理に関する要改善事例

⑤開発プロジェクトの選定、管理の実施

【要改善事例】
　開発期間が長期に及ぶにもかかわらず、システム部門とユーザー部門だけでシステム化を承認し構築したため、開発計画の妥当性や開発するシステムのリスクが経営陣に事前に認識されていない。

開発プロジェクトの審査
- 開発規模が一定以上、開発期間が長期に及ぶもの、重要業務に関するものは、経営陣が開発の実施の要否を判断
- 計画の妥当性（目的、費用、期間、開発等）を審査
- 投資の有効性を審査
- リスクの有無、程度等を審査

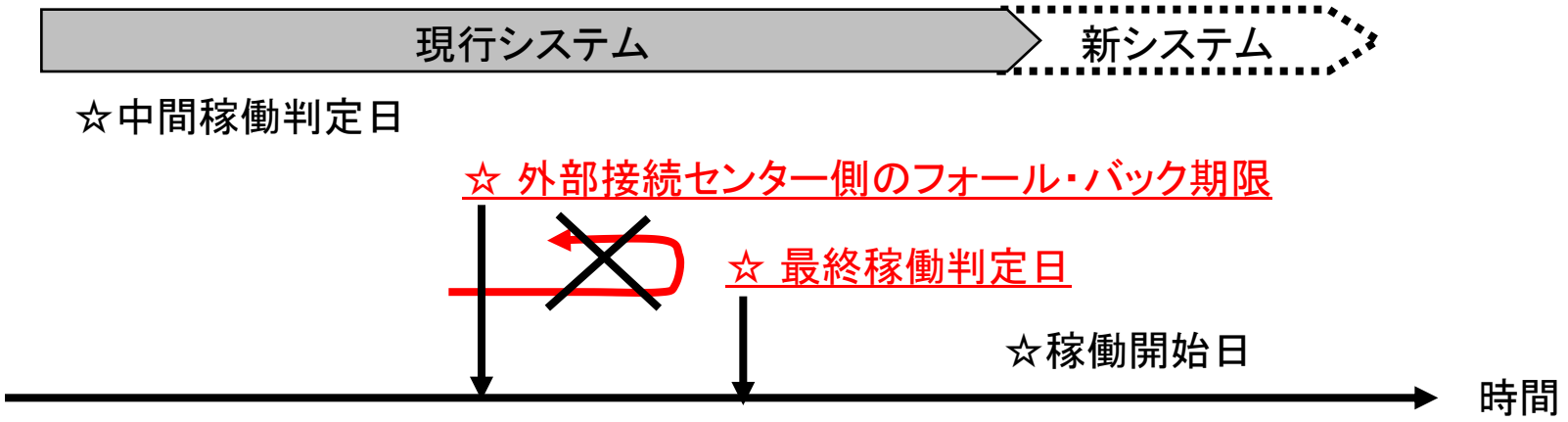


・　開発プロジェクトは、経営陣やリスク管理部門の審査を経て、計画の妥当性やリスクを事前に明らかにする。

3. システムリスク管理に関する要改善事例

⑥稼働判定の実施

【要改善事例】
最終稼働判定会議の開催日時が不適切。



・ 関係先のフォール・バック期限を踏まえ、最終稼働判定日を確定する。

3. システムリスク管理に関する要改善事例

⑦進捗管理手法の工夫

【要改善事例】
粗い線表と定性的な進捗管理のために、進捗の遅れが発見できなかった。

要件定義 → プログラム製造 → 総合試験 → 総合運転試験

・計画対比、若干の遅延が発生

この報告で進捗の真の遅れは発見できるか？

⇒定量的な進捗管理も一案

・ 定量的な進捗管理を行うなど工夫を講じ、進捗の遅れ等を発見できる体制を構築する。

3. システムリスク管理に関する要改善事例

⑧オペレーションマニュアルの整備

【要改善事例】
　重要機器が更改されたにもかかわらず、オペレーションマニュアルが更新されていない。

- 異例時オペレーションを行おうとしたが、オペレーションマニュアルがなかったため、対処に時間を要した。
- 更改した機器の安定稼働が確保されたため、委託先からのサポートがなくなったが、マニュアル整備が行われておらず、スキルが十分継承されていない。

・ 重要機器を更改した場合には、テストで運用習熟を図るとともに、オペレーションマニュアルや障害マニュアルを本番稼働前に整備する。

3. システムリスク管理に関する要改善事例

⑨作業の確認

【要改善事例】
機器やソフトウェア等の変更に当たって、作業の妥当性をチェックする体制が整備されていない。

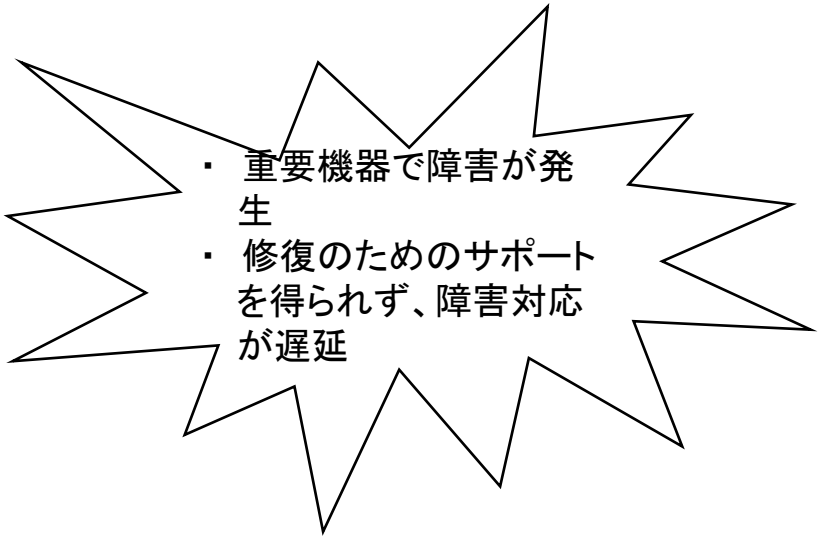
- 休日を利用して、システムの機能拡張を行った際、データの蓄積可能量を手作業で修正したが、これを誤った。
- 作業者以外の職員が、行った作業の内容を確認しなかったほか、本番機器等の修正ルールの中でも、作業のチェックに関する規定が定まっていなかった。

・ 本番機器やソフトウェア等を変更する場合には、作業の妥当性を確保するためのルールを定め、確実に励行する。

3. システムリスク管理に関する要改善事例

⑩保守対策の実施

【要改善事例】
　重要機器の保守契約が切れていたために、障害時にサポートが得られなかったほか、修復に必要な部品が確保できなかった。



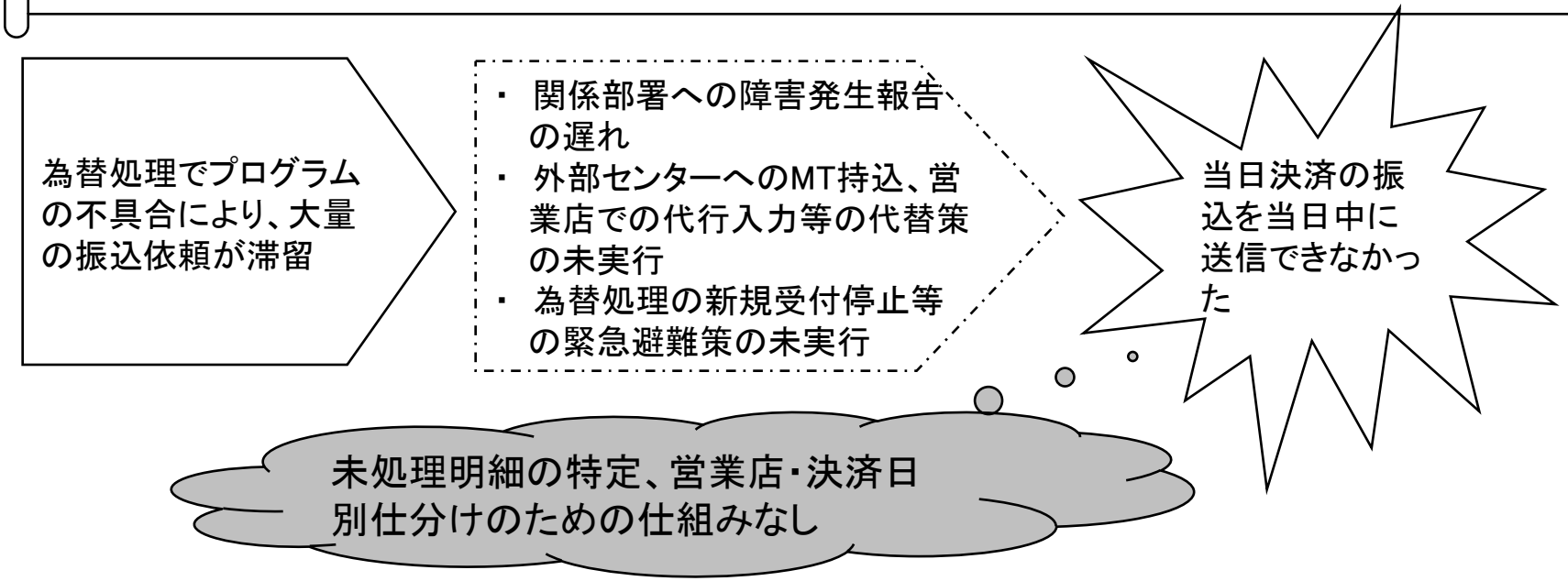
・ 重要機器の障害発生状況をモニターせず
・ 重要機器の保守契約の状況を定期的に確認せず
・ 障害発生に備えた委託先への連絡体制を定期的に更新せず

・ 重要な機器やソフトウェアの保守契約は、定期的に見直しを行い、システムの運用実態に即したものとする。
　―― 重要な機器やソフトウェアは計画的に更改する。
・ 障害時の連絡体制は定期的に見直しを行うほか、機器等更改時にも更新する。

3. システムリスク管理に関する要改善事例

⑪緊急時対策の整備

【要改善事例】
システム障害が発生した場合の、未処理データに関する緊急時対応が不十分。



・ 為替、口座振替等大量取引における未処理データ発生時のコンティンジェンシープランを策定する。
―― 未処理明細の特定や再処理方法の明確化。
・ 同プランに基づく実践的な訓練を行う。

3. システムリスク管理に関する要改善事例

⑫システム障害対策の整備

【要改善事例】
障害分析やリスク評価などによってリスクを把握しながら、リスクの削減策を講じてこなかった。

障害・セキュリティ侵害	リスク管理策
ハードウェアに起因した障害	機器の二重化、定期保守、切替え訓練の実施等
ソフトウェアに起因した障害	レビュー、テストの充実等
システム性能に起因した障害	性能・負荷テストの実施、定期的な監視
運用・保守に起因した障害	運用・障害マニュアル、プログラム登録手順書等の整備、運用訓練の実施
情報セキュリティ侵害	ユーザーID管理、暗号化等の適切なセキュリティ対策の実施

・ システム障害、情報セキュリティ侵害の相当部分は金融機関側の適切なリスク管理により回避できる。

3. システムリスク管理に関する要改善事例

⑬重要情報の管理

【要改善事例】
顧客情報など重要情報のアクセス管理が十分ではないほか、高権限IDの管理が十分ではない。

- 従業員が顧客情報にアクセスし、当該情報を持出し可能な外部記憶媒体に収録。
- 従業員が高権限IDを不正に利用して、重要情報を取得 。
- 顧客情報が外部に持ち出された。

・ 重要情報はしかるべきアクセス制御を施し、高権限IDは厳格に管理する。また、重要情報の取扱いルールを定め、容易に持出しすることができないようにすることが重要。

3. システムリスク管理に関する要改善事例

⑭アクセス・ログの管理

【要改善事例】
アクセス・ログが検証されていないなど、高権限者への牽制が不十分。

- アクセス・ログはログイン履歴しか取得しておらず、ファイルへのアクセス者を特定できない。
- ログ・ファイルは編集しなければ検証が困難な形式のため、アクセス・ログの検証が実施されていない。
- ログ・ファイルには一般のユーザーIDでもアクセスできるため、ログの改竄・消去が可能。

・ アクセス・ログは、①アクセス者の特定等不正アクセスへの牽制効果を有すること、②検証可能な形式で出力されること、③改竄等ができないことが必要。

3. システムリスク管理に関する要改善事例

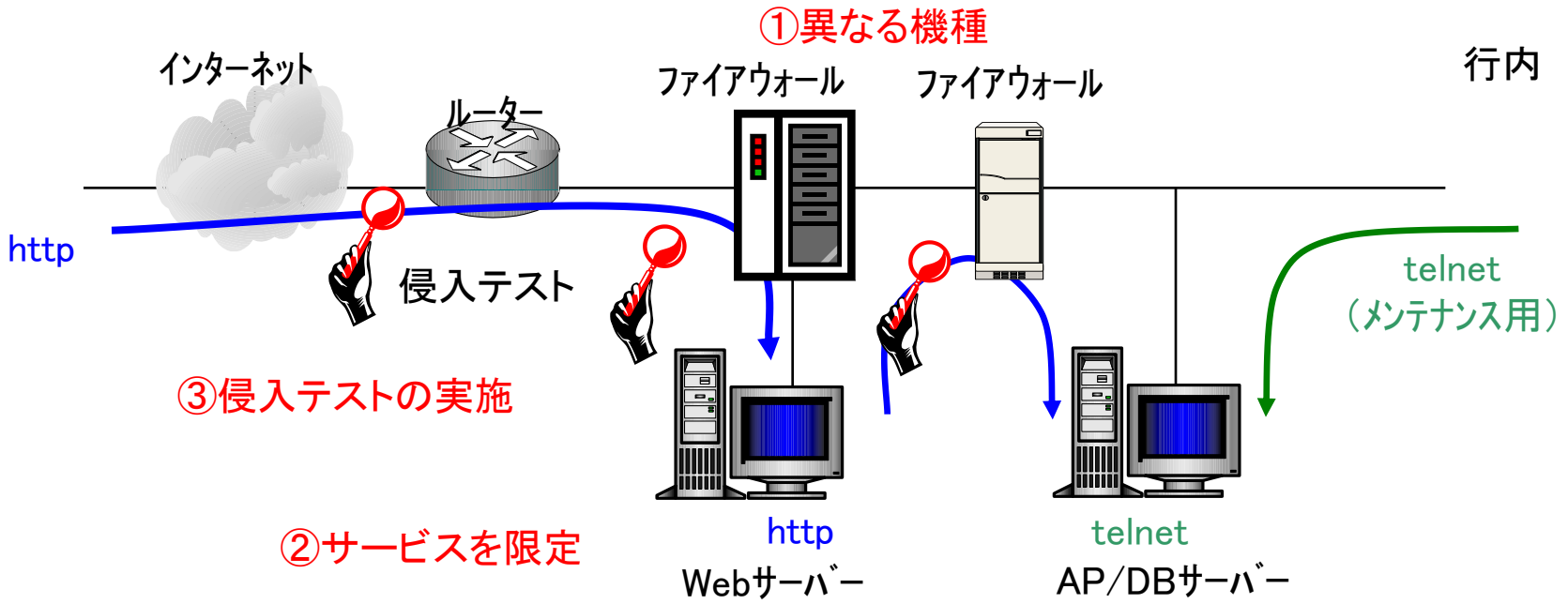
⑮外部からの不正アクセス対応

【セキュリティポリシーに見合う正しい構成】

① ファイアウォールは複数台設置すること。その際には、セキュリティ上の不具合に備えて、異なる機種とすること。

② 利用可能なプロトコルおよびサービスを限定すること。

③ ファイアウォールに対する侵入テストを定期的に実施すること。



3. システムリスク管理に関する要改善事例

⑮外部からの不正アクセス対応（続き）

【要改善事例】

① ファイアウォールが同一の機種

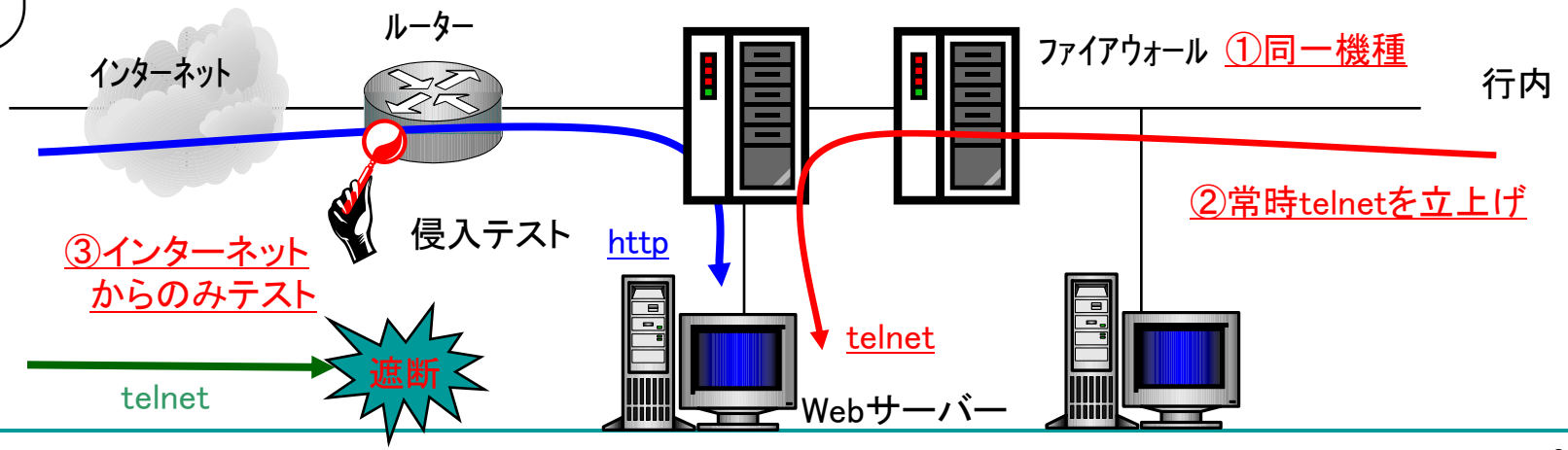
⇒ 片方機種のリプレース時に、維持管理を容易にするため、同一機種に変更。

② Webサーバーで不要なサービスを立上げ

⇒ 月1回のログ収集を内部から簡単に行うため（サーバー設置室に出向く手間が省ける）、常時telnetを立上げ（ログ収集を行う委託先のニーズ）。

③ ファイアウォールに対する侵入テストは未実施

⇒ インターネット上からのみテストを実施。ルーターのフィルタリングで殆どのプロトコルが遮断される。



3. システムリスク管理に関する要改善事例

⑯システム監査の強化

【要改善事例】
監査が規程の遵守状況の確認に止まっている。
監査では外部委託先のリスク管理状況の適切性を検証していない。

- 規程の遵守状況は検証しているものの、規程自体が不十分な点を監査で把握していない。
- 共同センター等サービス提供会社において適切なリスク管理プロセスが構築されているかどうかを確認していない。

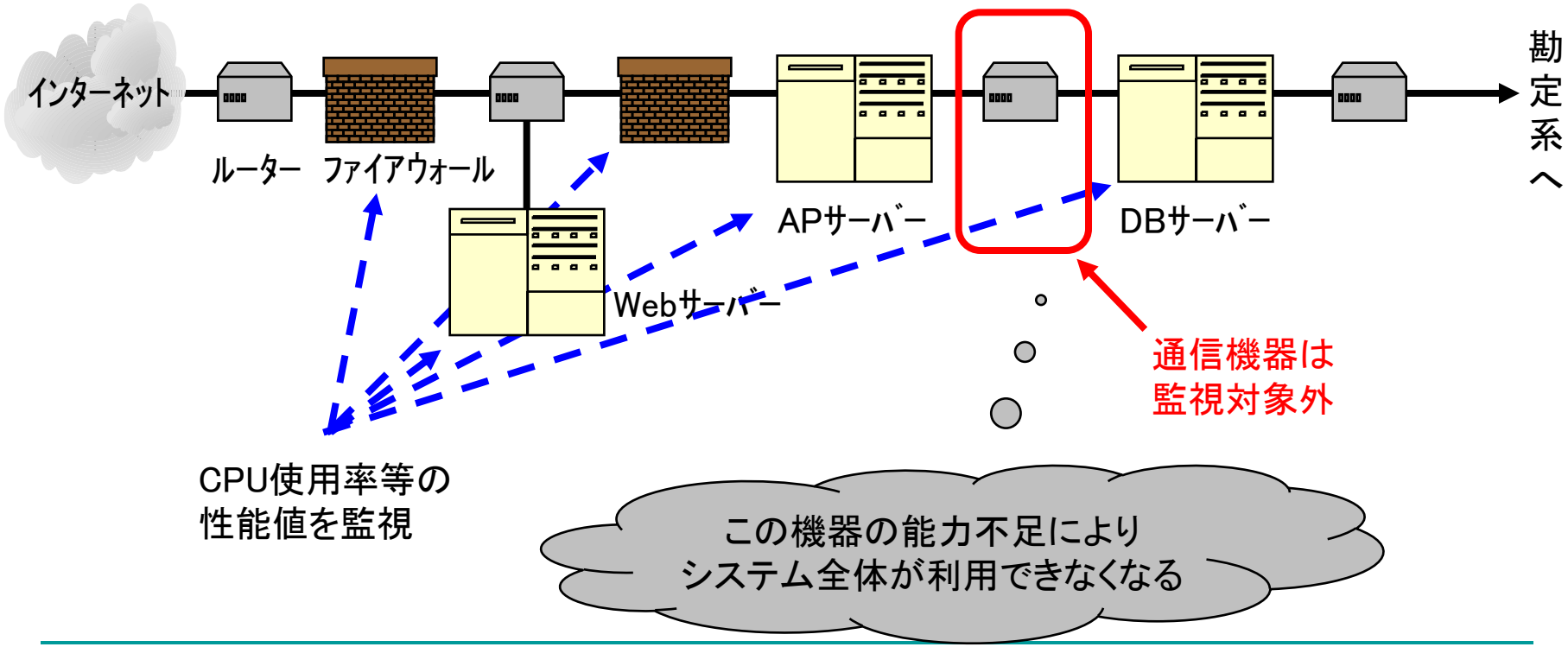
- リスクプロファイルを明らかにすることも監査の目的。
- リスクプロファイルの変化に応じた監査を実施する。
  —— 特に部署を跨る課題の抽出にはシステム監査が有効。
- 外部監査やコンサルティングも必要に応じ活用する。

4. リスク・ファクターの変化

(1)システムの大規模・複雑化が進み、相互接続が拡大

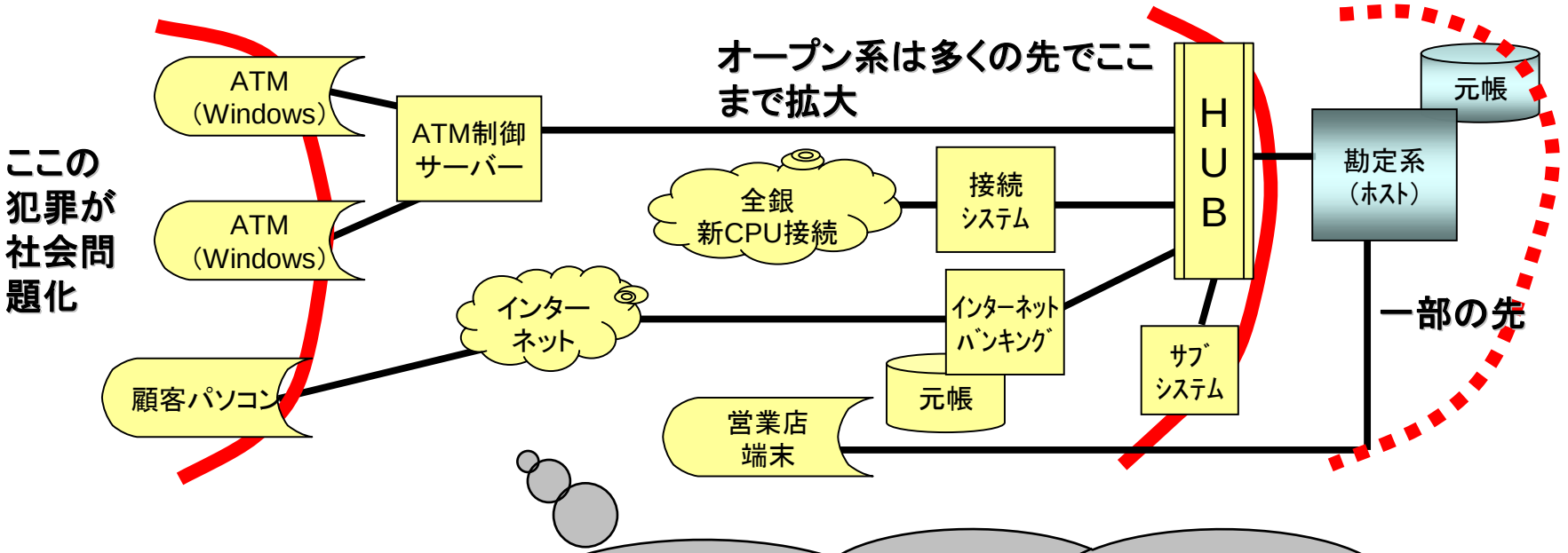
・ 一つのシステムの不具合や処理能力不足が、システム全体の処理時間の遅延に繋がる。

—— 障害発生時には他社へも影響。



4. リスク・ファクターの変化

（1）システムの大規模・複雑化が進み、相互接続が拡大（続き）



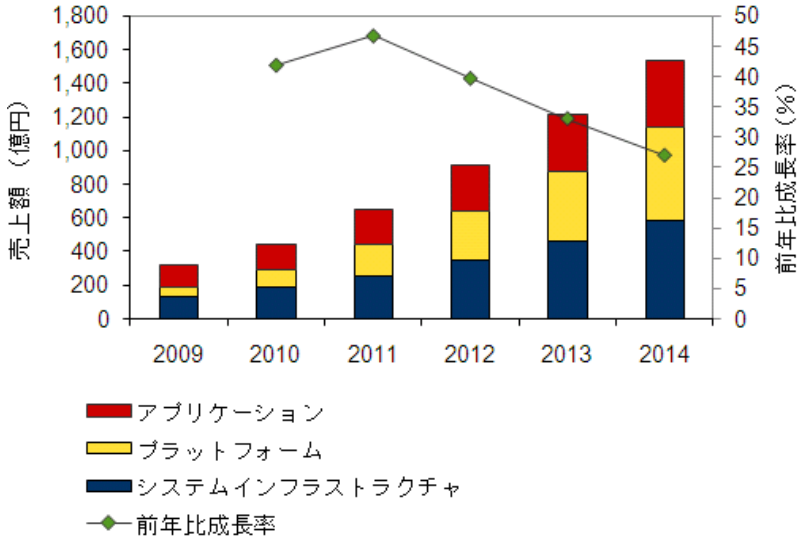
- 金融機関内部のシステムに目を向けると、インターネット・バンキングに加え、決済関連の業務処理、ATMシステム等をオープン系システムで構築している先が増加。
- 社会的には、偽造キャッシュカード、フィッシング詐欺等、顧客接点部分での犯罪が問題化。

4. リスク・ファクターの変化

（2）新技術の採用

- 経営のニーズ、ユーザー部門のニーズを背景に、新技術の採用がこれまで以上に期待されるようになってきている。
- システム部門としても、開発期間、要員、費用等の制約を考えると、新技術の採用は魅力的なケースがある。

（参考）国内クラウドサービス市場



Notes:
- パブリッククラウドに相当するIDCクラウドサービス市場定義に基づく。
- BPOサービス、導入支援／システム／アプリケーション開発などのプロフェッショナルサービスは含まれていない。
- プラットフォームは「アプリケーション開発／デプロイメント」に該当。
- システムインフラストラクチャは、「サーバー」「ストレージ」「セキュリティ、システム管理などのシステムインフラストラクチャソフトウェア」に該当。

出典：IDC Japanプレスリリース「国内クラウドサービス市場予測を発表」(2010年9月)

- 新技術の採用に当たっては、これまでに経験したことのないリスクを抱えることも想定されるので、事前のリスクの洗出しと対応策の検討が重要になってくる。

（参考）クラウドサービスレベルのチェックポイント（抜粋）

【アプリケーション運用】

（可用性）

・サービス時間、サービス稼働率

・計画停止予告通知、サービス提供終了時の事前通知

・突然のサービス停止に対する対処

・ディザスターリカバリ、重大障害時の代替手段

・アップグレード方針

（信頼性）

・平均復旧時間、目標復旧時間

・サービス提供状況の報告方法等

・システム監視、ログの取得

・障害発生件数、障害監視・通知プロセス

（性能）

・応答時間、バッチ処理時間

（拡張性）

・カスタマイズ性

・外部接続性

・提供リソースの上限、同時接続利用者数

【サポート】

・障害対応時間

・一般照会対応時間

【データ管理】

・バックアップの方法、取得・保存期間

・データの整合性検証

・データ消去の要件

・暗号化

・データ漏洩・破壊時の保障等

・解約時のポータビリティ

・マルチテナントストレージのキー管理

【セキュリティ】

・公的認証の取得

・第三者評価

・情報取扱い、情報取扱者の制限

・セキュリティインシデントのトレーサビリティ

・データの保存方針、記憶媒体の安全対策

・マルチテナント下でのセキュリティ対策

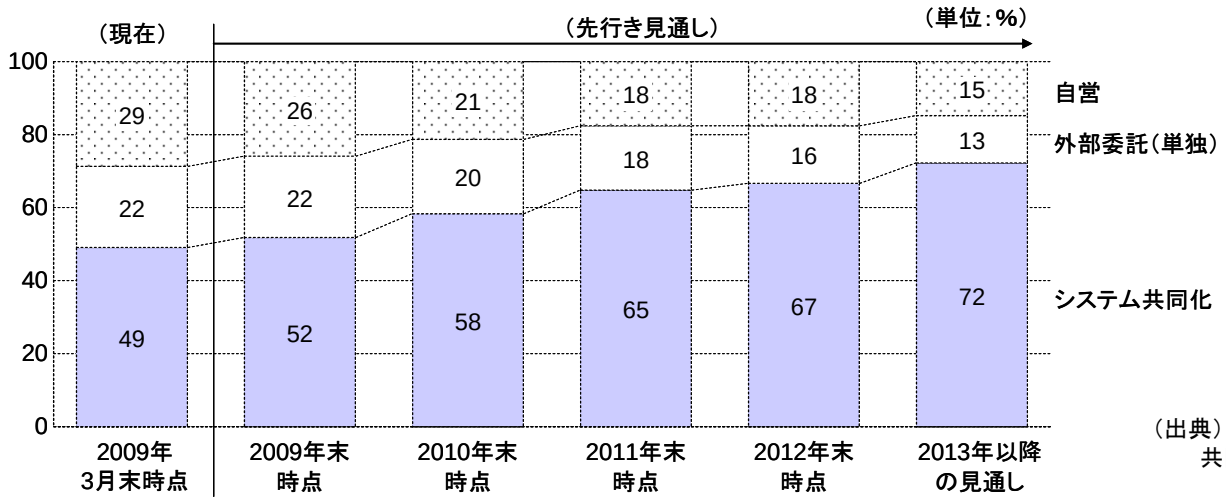
出典：経済産業省「クラウドコンピューティングと日本の競争力に関する研究会」(2010年8月)

4. リスク・ファクターの変化

(3)システム開発・運用の外部委託の進展

- 大手金融機関:システム開発・運用部署は外部委託(子会社化等)。
- 地域銀行:ITベンダーが提供する共同システムの利用(システム共同化)が進展。

▽ メインセンターの運営形態の動向



(出典)「金融機関におけるシステム共同化の現状と課題(2009)」

<集計対象金融機関数:108>

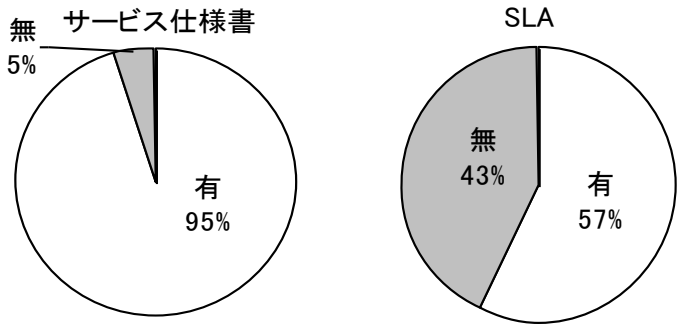
- 外部委託が進展するなかで、適切な委託先管理が必要になっている。

５－１．委託先の管理状況

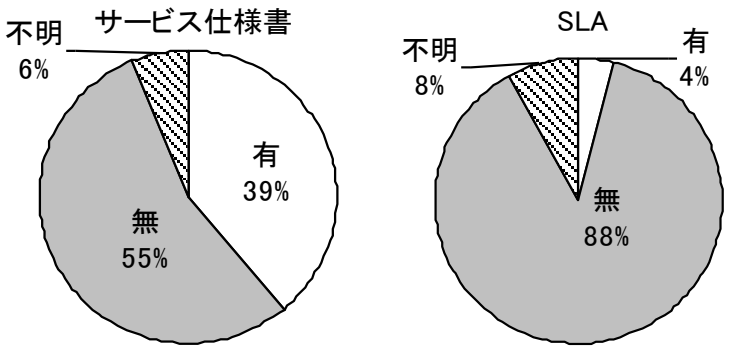
（1）役割分担・責任範囲の明確化

- 地域銀行では、9割以上の先がサービス仕様書により役割分担・責任範囲を明確化。6割弱の先がSLA(Service Level Agreement)によりサービス水準を明定化。
- 信用金庫では、サービス仕様書の締結先は4割弱。また、SLA締結先は4%。

▽ 地域銀行



▽ 信用金庫



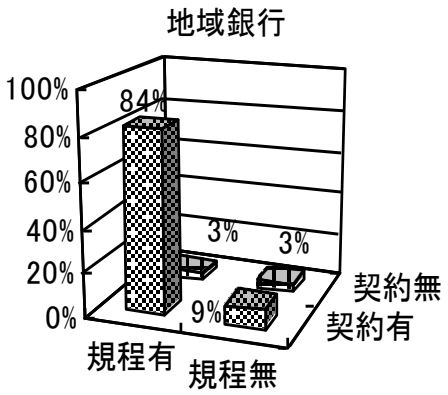
（出典）「金融機関におけるシステム共同化の現状と課題（2009）」

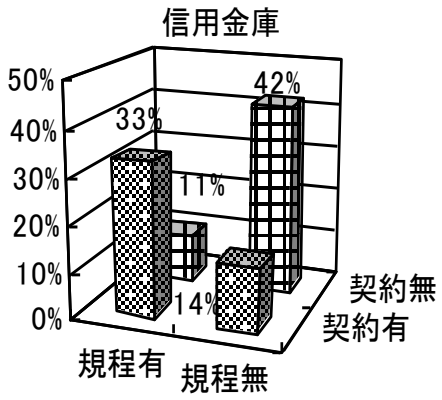
５－１．委託先の管理状況

（２）情報セキュリティポリシー・スタンダードの遵守

- 地域銀行では、委託先の遵守義務を規程上明定し、契約上も義務を課していると回答した先が8割強。
- 信用金庫では、規程上も契約上も遵守を求めていない先が4割を上回り、規程上明定されていても契約上義務を課していない先を加えると、過半が委託先に遵守を求めていない。

▽　情報セキュリティーポリシー・スタンダード遵守に対する規程・契約面の対応





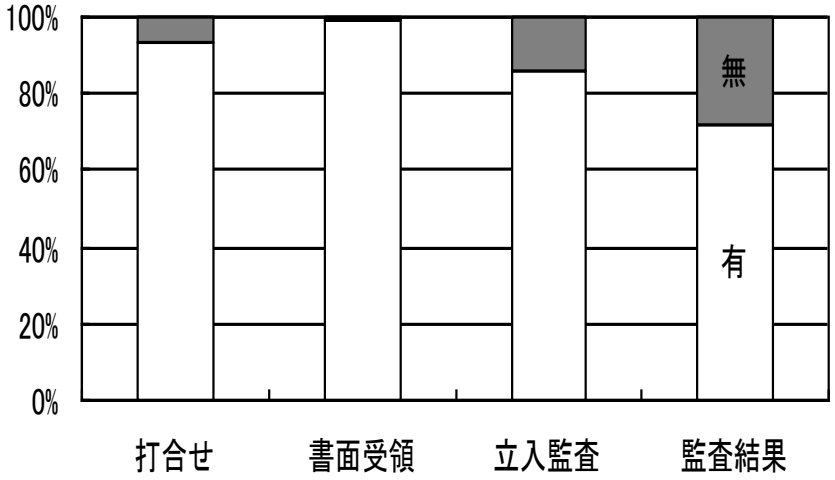
（出典）「金融機関におけるシステム共同化の現状と課題（2009）」

５－１．委託先の管理状況

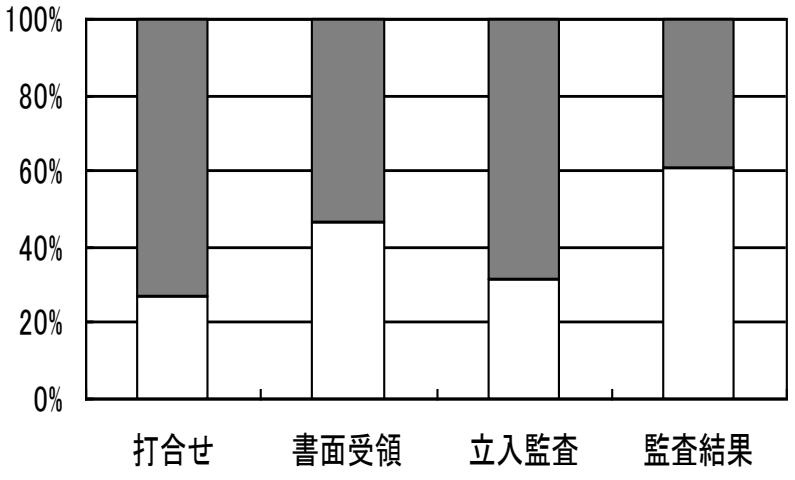
（３）委託先の管理手段①

- 地域銀行では、定例打合せ、報告の書面受領の実施率が9割を超えているほか、立入監査や監査結果の入手も7割以上の先で実施。
- 信用金庫では、定例打合せ、報告の書面受領、立入監査の実施先は半数未満。

▽ 地域銀行の委託先管理手段の導入状況



▽信用金庫の委託先管理手段導入状況



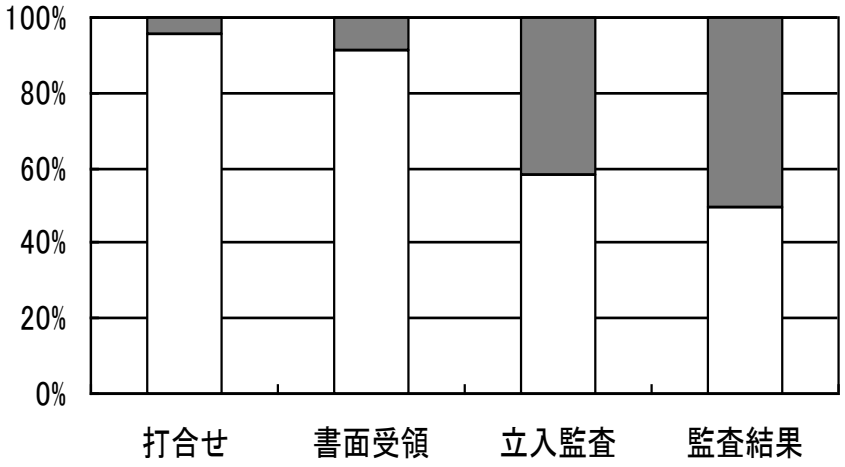
（出典）「金融機関におけるシステム共同化の現状と課題（2009）」

５－１．委託先の管理状況

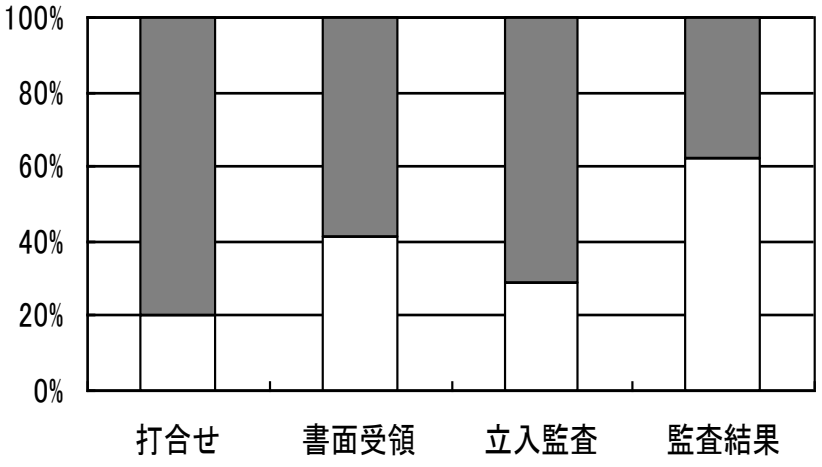
（３）委託先の管理手段①（続き）

- 信用金庫のうち自営先では、定例打合せや書面受領の実施率が9割を超えているほか、過半の先で立入監査や監査結果の入手も実施。
- 共同事務センター利用先では、各種管理手段の実施率は総じて低い。

▽自営信金の委託先管理手段導入状況



▽共同事務ｾﾝﾀｰ利用信金の委託先管理手段導入状況



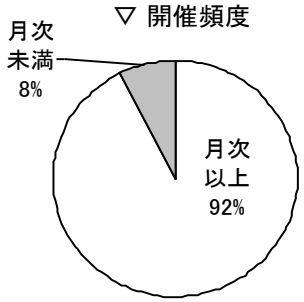
（出典）「金融機関におけるシステム共同化の現状と課題（2009）」

5－1. 委託先の管理状況

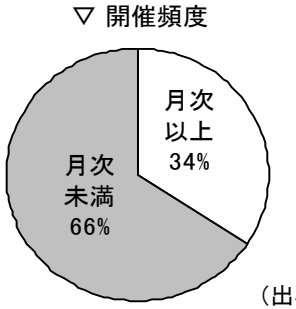
（3）委託先の管理手段②

- 地域銀行では、定例打合せや書面受領は、実施先のうち9割強の先が、月次ないしそれ以上の頻度で実施。
- 信用金庫では、定例打合せや書面受領を月次ないしそれ以上の頻度で実施している先は、実施先の3～4割。

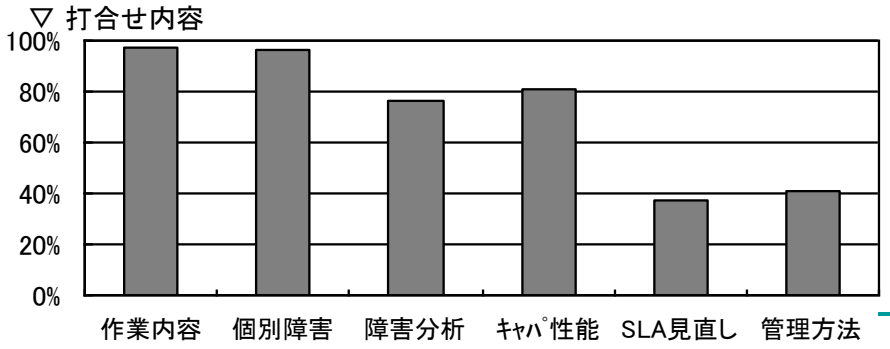
▽ 地域銀行

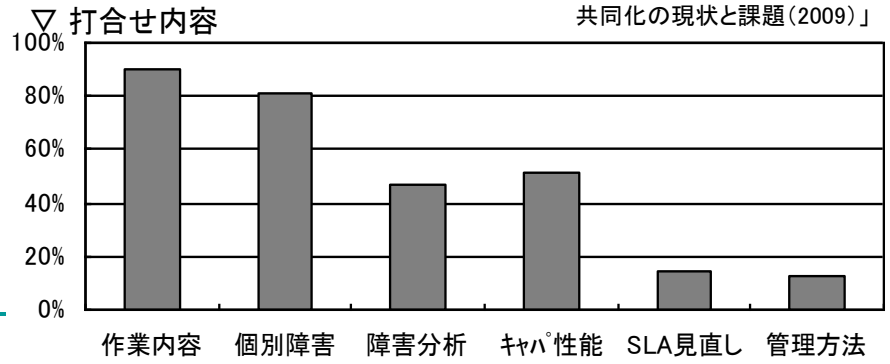


▽ 信用金庫



（出典）「金融機関におけるシステム共同化の現状と課題（2009）」



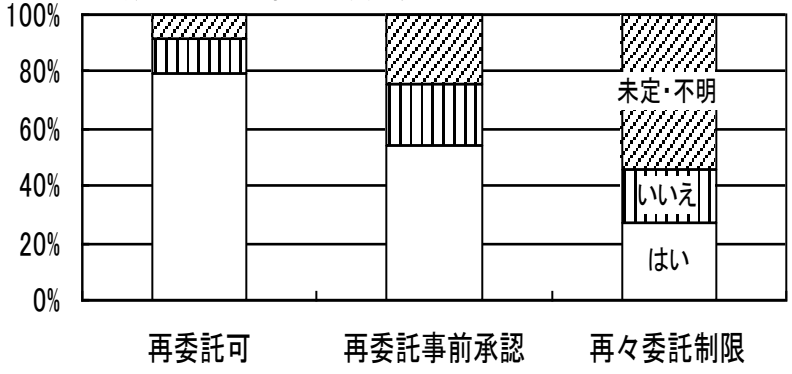


５－１．委託先の管理状況

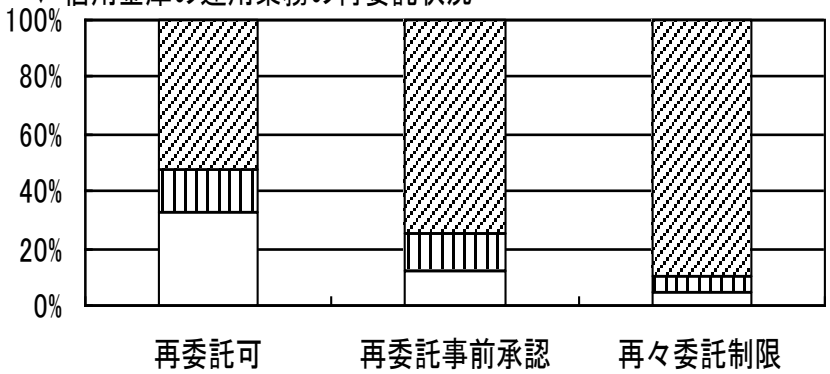
（4）再委託の管理

- 地域銀行では、8割弱の先で外部委託先からの再委託を認めているが、再委託時の事前承認制度の導入は5割強で、再々委託に関する　制限を実施している先は3割程度。
- 信用金庫では、再委託可能と回答した先は3割強で、5割強が定めなし、もしくは不明と回答。再委託時の事前承認制度の導入、再々委託に関する制限を実施している先は少数。

▽ 地域銀行の運用業務の再委託実施状況



▽ 信用金庫の運用業務の再委託状況



（出典）「金融機関におけるシステム共同化の現状と課題（2009）」

５－２．委託先管理についての基本的な考え方

（１）委託先管理の必要性

【委託先管理でよく聞かれる悩み①】
「外部委託した以上、当該委託対象業務に係る責任は委託先にあるので、委託先管理の必要性が乏しいのではないか。」

- リスク管理の重要性は、業務が外部委託されたとしてもなくなることはない。
  ―― 例えば顧客や外部組織に負う対外的な責任は変わらない。
- 委託対象業務についてのリスク管理レベルを、金融機関自らが行う業務の管理レベルに比べて、引き下げることは適当でないケースが少なくない。
- 委託先の選定基準（サポート体制、サービスレベルなど）を整備する。

５－２．委託先管理についての基本的な考え方

（２）委託先管理に関する資源制約

【委託先管理でよく聞かれる悩み②】
「外部委託にマンパワーをかけていては、マンパワー不足解消という外部委託の効果が減殺されてしまう。」

- 委託先管理とは、委託先の作業を逐一チェックすることではない。
- 委託先管理とは、委託先のリスク管理体制・プロセスが有効に機能しているか確認する（それに必要な範囲での委託作業内容の確認）。
- 委託先と、金融機関自身とのセキュリティポリシー・スタンダードとの擦り合わせ。

５－２．委託先管理についての基本的な考え方

（３）委託形態の多様化と委託先管理

【委託先管理でよく聞かれる悩み③】
「ベンダー提供システムを利用しているだけで、自行庫側が主導権を発揮する場面はそもそも限られているので、委託先管理は困難。」

- 委託先において大規模なシステム障害や情報漏洩が発生した場合、「管理が難しい」という言い訳が通用するか？
- 委託形態によって実行可能な委託先管理手段は異なる。
- 委託契約の手法として、最近、SLAの締結が目立ってきている。SLA等の活用も一案。
- 委託先との契約締結に当たっては、法務部門やコンプライアンス部門の適切な関与を得る。

５－２．委託先管理についての基本的な考え方

（４）委託先管理のスキルを有する人材の育成

【委託先管理でよく聞かれる悩み④】
「システムを全面的に委託しているので、自行庫内にシステムに関するノウハウが蓄積されないようになり、その結果、委託先管理を行おうにもスキルのある人材がいない。」

- 委託先との人材ローテーション等による委託先管理要員の育成。
- 共同システム利用先が連携した委託先管理の実施。

6. 人材の確保

- リスク管理に止まらず、システム部門の人材確保・育成が大きな課題。
- 経営陣がこうした課題を認識して、リーダーシップを発揮して対応することが重要。

システム部門に対する要請

- システム開発に対する強いニーズ
- 多種多様な技術、ハード・ソフトの発達
- 投資額の抑制

システム部門のおかれた環境

- アウトソーシングの活用等による人員スリム化
- 新規採用の抑制、高齢化
- 他部門とのローテーションの停滞

人材をどのように確保するか

ご清聴ありがとうございました

本資料に関する照会先

日本銀行　金融機構局　考査企画課　システム・業務継続グループ　岩佐、志村、熊坂

tel: 03-3664-4333

email: csrbcm@boj.or.jp