



金融機関のシステム環境の変化 とリスク管理の課題

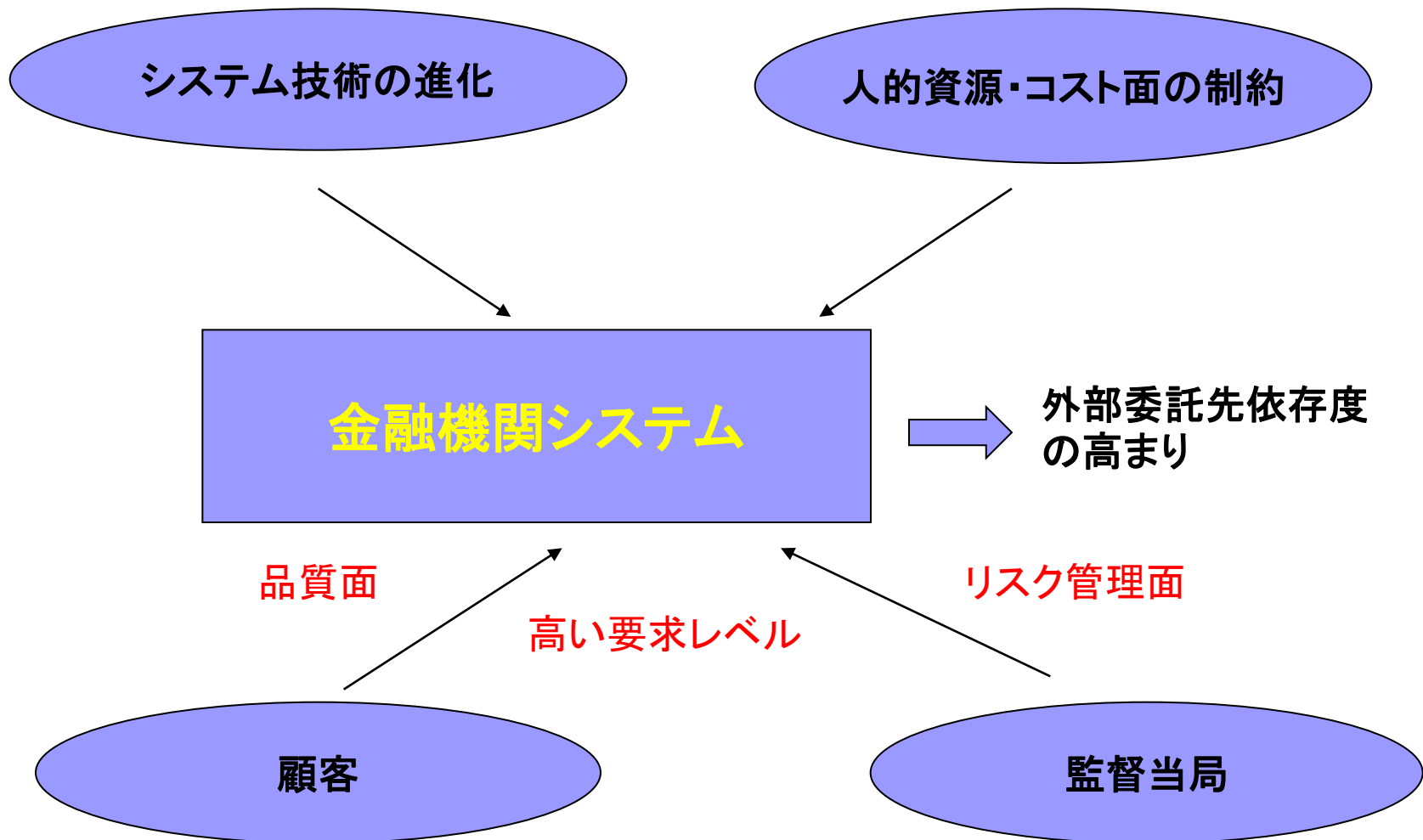
2010年10月
プロモントリー・フィナンシャル・ジャパン
江見 明弘



本日の説明内容

1. 金融機関システムを巡る最近の環境変化
 - (1) システム技術の進化
 - (2) システム外部委託の進展
2. システムリスク管理上の留意事項
 - (1) 経営陣の役割
 - (2) リスクベース・アプローチ
3. IT人材の育成

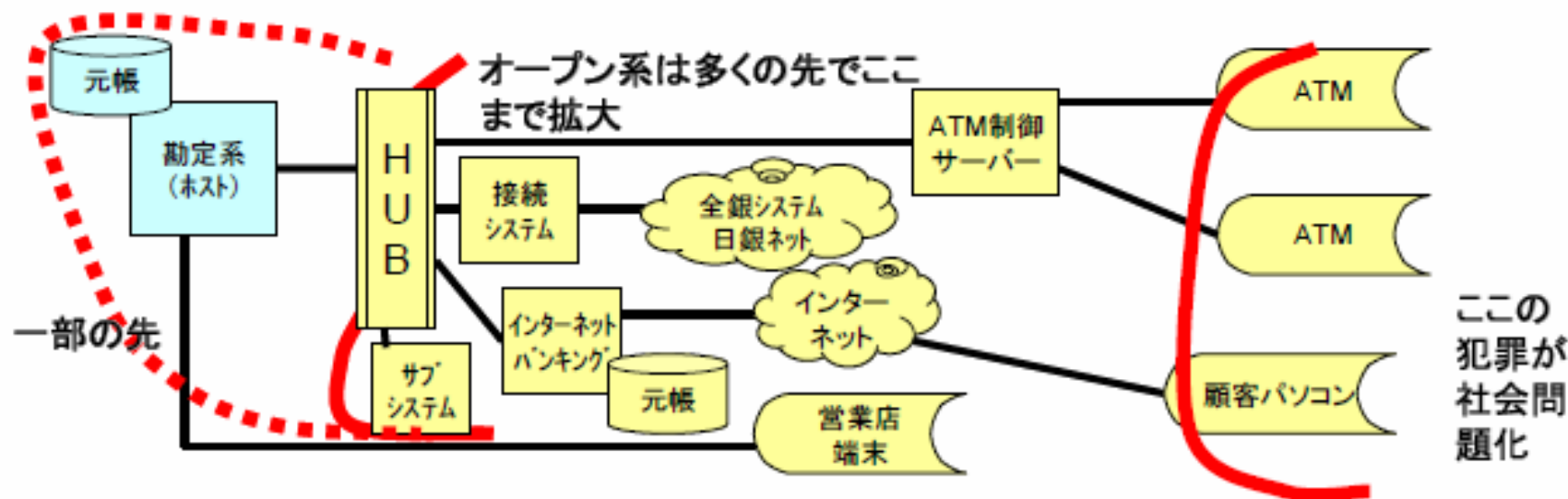
1. 金融機関システムを巡る最近の環境変化



(1) システム技術の進化

① オープン系システム技術の進化

▼ オープン系システムの採用拡大



(出所: 日本銀行金融高度化セミナー「システムリスク管理の現状と課題」(2007. 3))

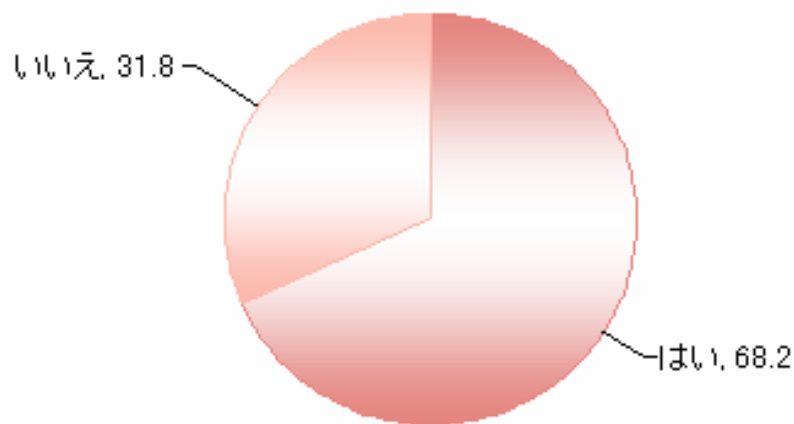
▼オープン系システムのリスク認識と対策

リスク認識	対策
ハードウェア ー メインフレームに比べ、機器単体では故障しやすい。	・ 機器の冗長化による可用性向上。
ソフトウェア ー 多種多様なソフトが組み合わさってシステムを構成しており、相性問題が起こりやすい。 ー OSの障害局所化機能、高付加制御機能等が弱い。 ー ウィルスに感染する。 ー 仕様が公開されているため、ソフトの脆弱性を突いた外部攻撃を受けやすい。	・ 入念な事前テストの実施(ex. パラレルラン・テスト)。 ・ メインフレーム系OS比劣後している機能を強化するためのミドルウェアの導入。 ・ ウィルス対策の実施。 ・ ソフトの脆弱性対策の実施(ex. WEBアプリの脆弱性対策)。
要素技術・ベンダー ー 要素技術が分散しているため、様々なスキル・ノウハウが必要。 ー ベンダーが複数に跨るため、障害時対応が難しい。	・ サーバの集中管理。 ・ 基盤を一元管理する部署の設置と強化。 ・ バグ・セキュリティホールの情報収集、パッチ適用の一元管理。 ・ 取り纏めベンダーの指定。

②インターネットバンキングの普及と犯罪手口の高度化

- インターネットバンキングサービスを提供する金融機関の割合
 - ー FISC「金融機関のシステム化アンケート」(2009. 3)
 - ・ 事象者向け……82. 4%
 - ・ 個人向け ……88. 4%
- 個人インターネットバンキングの利用状況(1／2)

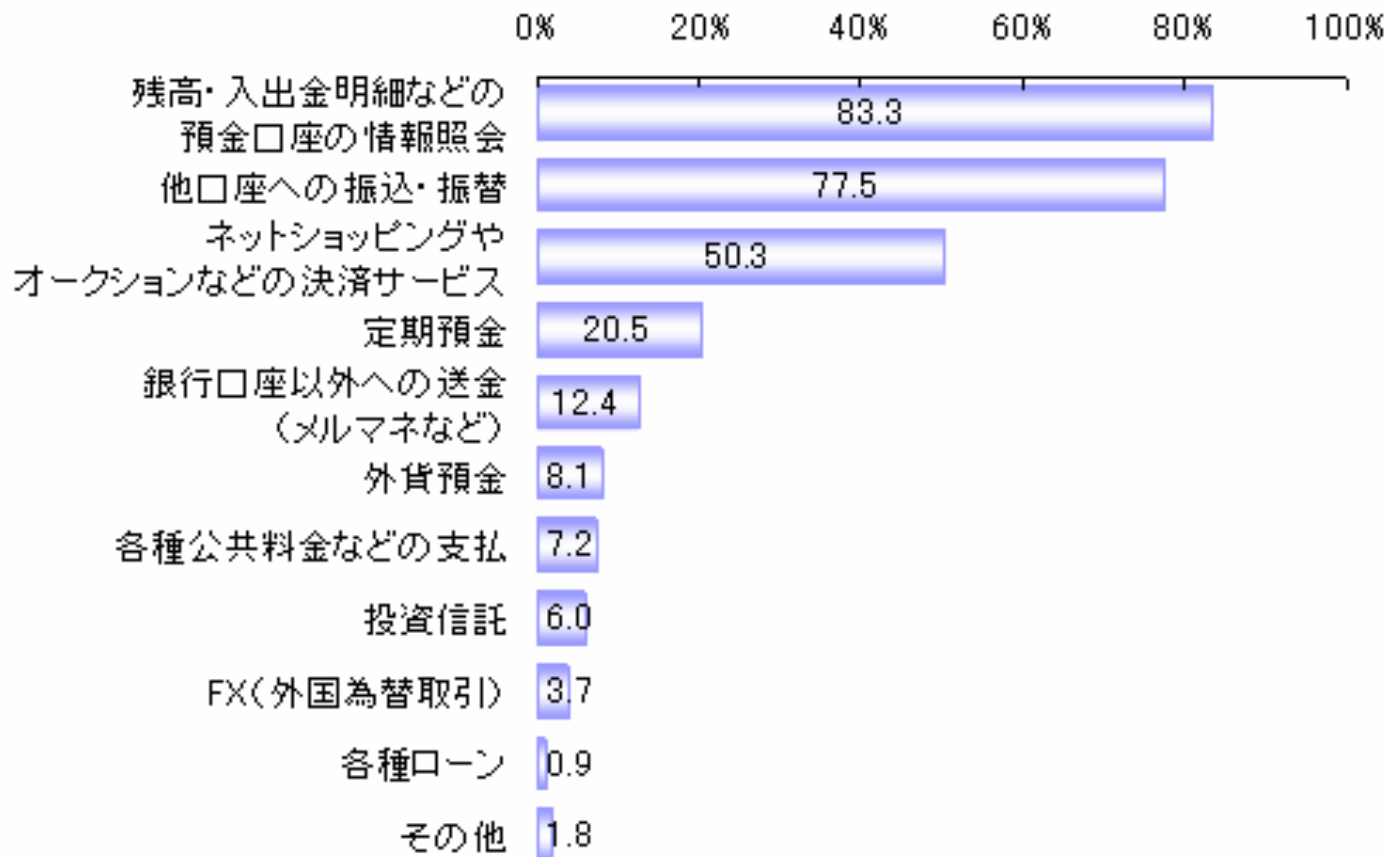
◇インターネットバンキング(パソコンから)の利用有無(n=1,000) 単位: %



(出所: 楽天リサーチ「インターネットバンキングに関する調査」(2009. 10))

■ 個人インターネットバンキングの利用状況(1/2)

◇インターネットバンキング(パソコンから)の利用状況(n=654) 複数回答 単位:%



(出所: 楽天リサーチ「インターネットバンキングに関する調査」(2009. 10))

■ インターネットバンキングを利用した犯罪状況

▼ 日本での偽造キャッシュカードとインターネットバンキングによる被害発生状況

時期		15年度	16年度	17年度	18年度	19年度	20年度
偽造キャッシュカード	件数 (件)	106	468	913	638	703	398
	被害額 (百万円)	331	1,063	980	576	435	267
	平均被害額 (万円)	312	227	107	90	61	67
インターネットバンキング	件数 (件)		1	49	102	233	127
	被害額 (百万円)		0	105	129	191	131
	平均被害額 (万円)		0	214	127	81	103

(注1) 各犯罪類型による被害発生の取りまとめ期間は以下のとおりであり、平成21年4月15日までに金融庁及び財務局に報告されたものを集計している。

■偽造キャッシュカード犯罪：平成12年4月から平成21年3月

■インターネットバンキング犯罪：平成17年2月から平成21年3月

(出所 金融庁「偽造キャッシュカード等による被害発生等の状況について」をもとに、FISCにて作成)

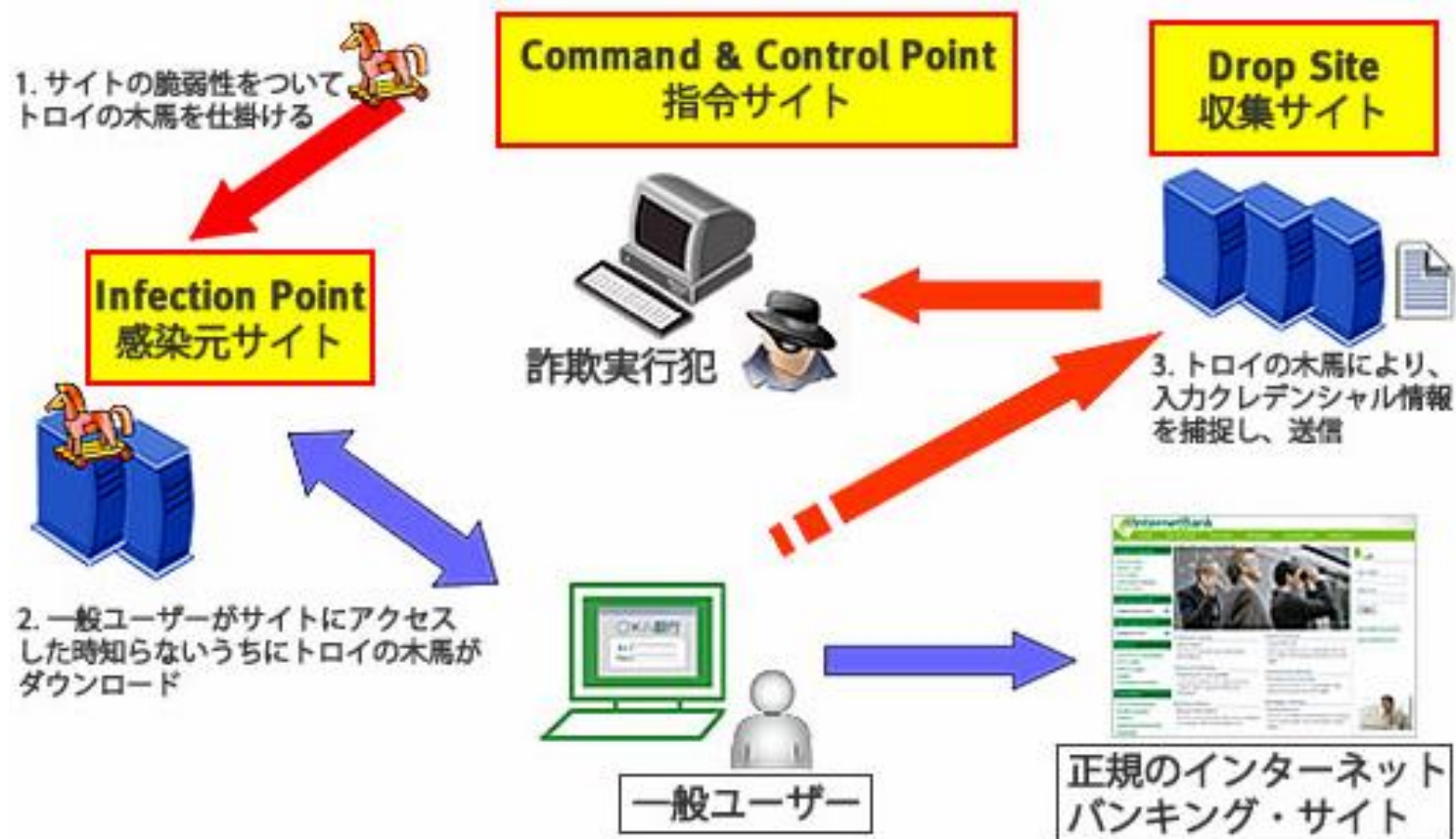
▼ (参考)英国でのインターネットバンキングによる被害発生状況

	2004年 1月から6月	2005年 1月から6月	2006年 1月から6月	2007年 1月から6月	2008年 1月から6月	増加率 (2007年 から2008年)
オンラインバン キング詐欺によ る被害額 (100万 単位)	£4	£14.5	£22.4	£7.5	£21.4	185%
フィッシング詐 欺の件数	126	312	5,087	7,224	20,682	186%
「運び屋」募集 の広告	NA	196	468	655	873	33%

(出所: APACS: 銀行共同支払決済機構)

■ インターネットバンキングを利用した犯罪手口の高度化(1/2)

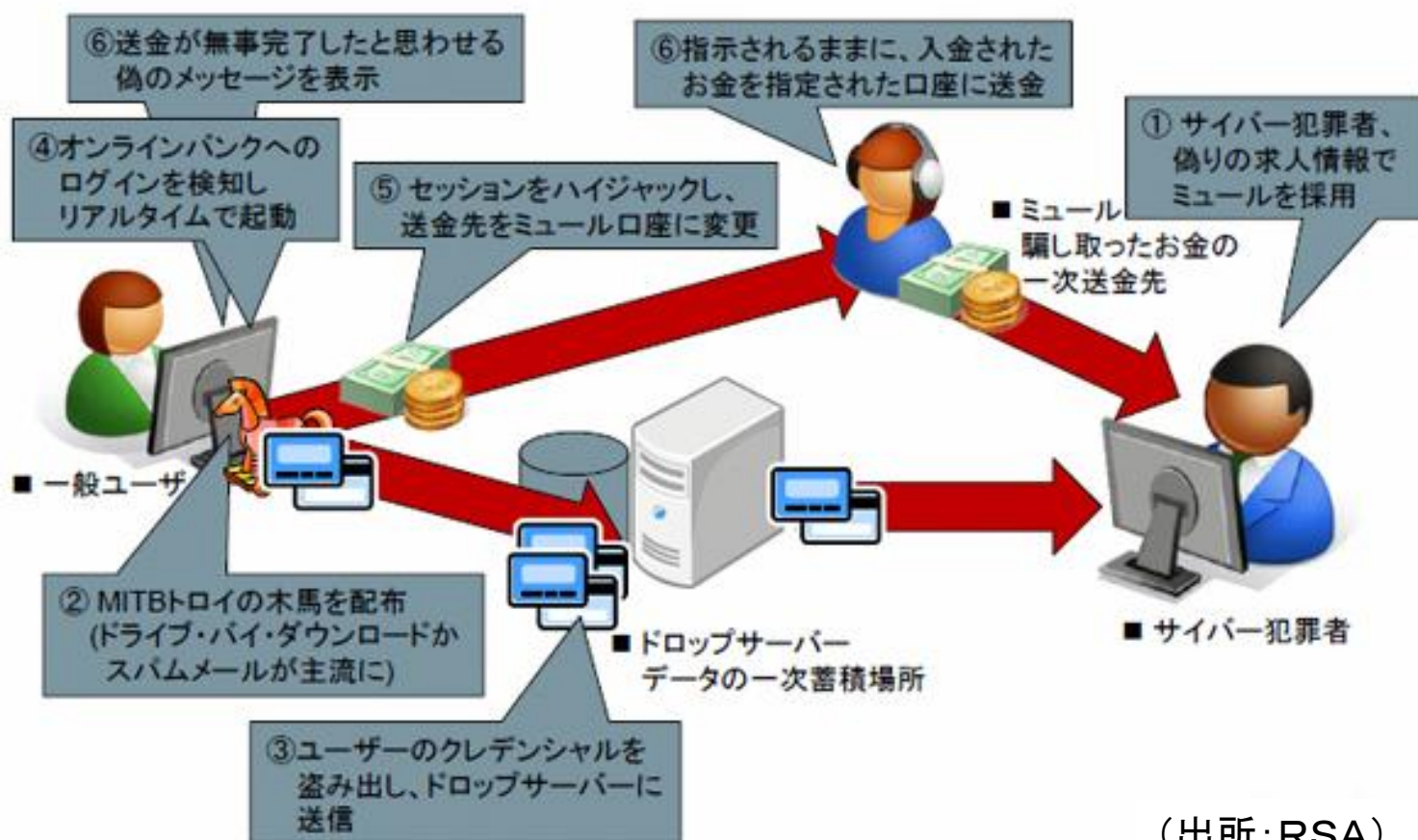
▼ トロイの木馬



(出所:RSA)

■ インターネットバンキングを利用した犯罪手口の高度化(2/2)

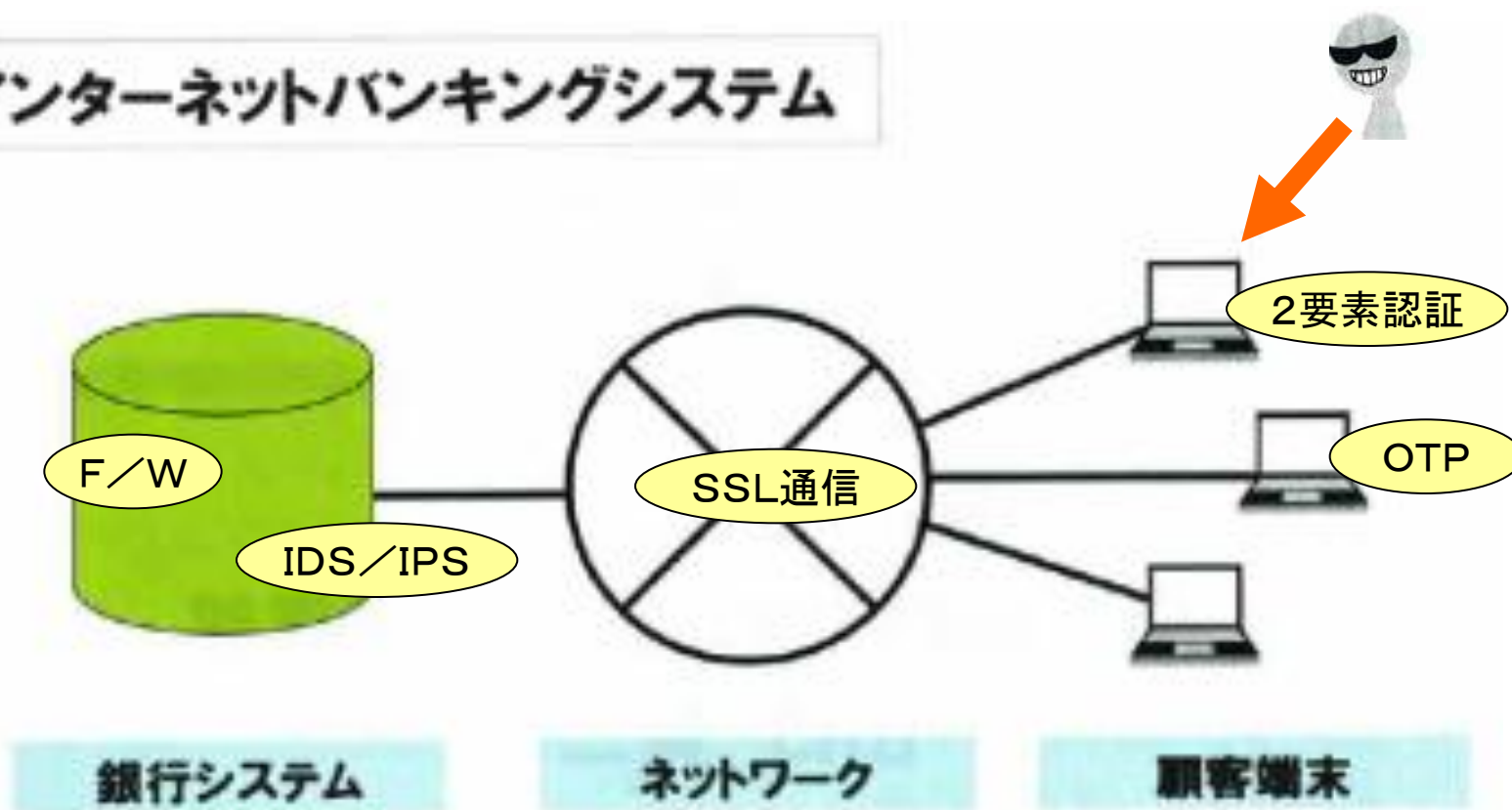
▼ Man-in-the-Browser (MITB)攻撃



(出所:RSA)

インターネットバンキングにおけるシステムリスク管理の守備範囲？

インターネットバンキングシステム



③システムの仮想化技術の進化とクラウドコンピューティング

■ システム仮想化

「一つの物理的サーバを、複数の論理的サーバに分割し、各々でシステムを稼働させることができるようにすること」

(メリット)

- ・ サーバ台数の削減
- ・ 保守・運用負担の軽減
- ・ サーバの稼働率アップ

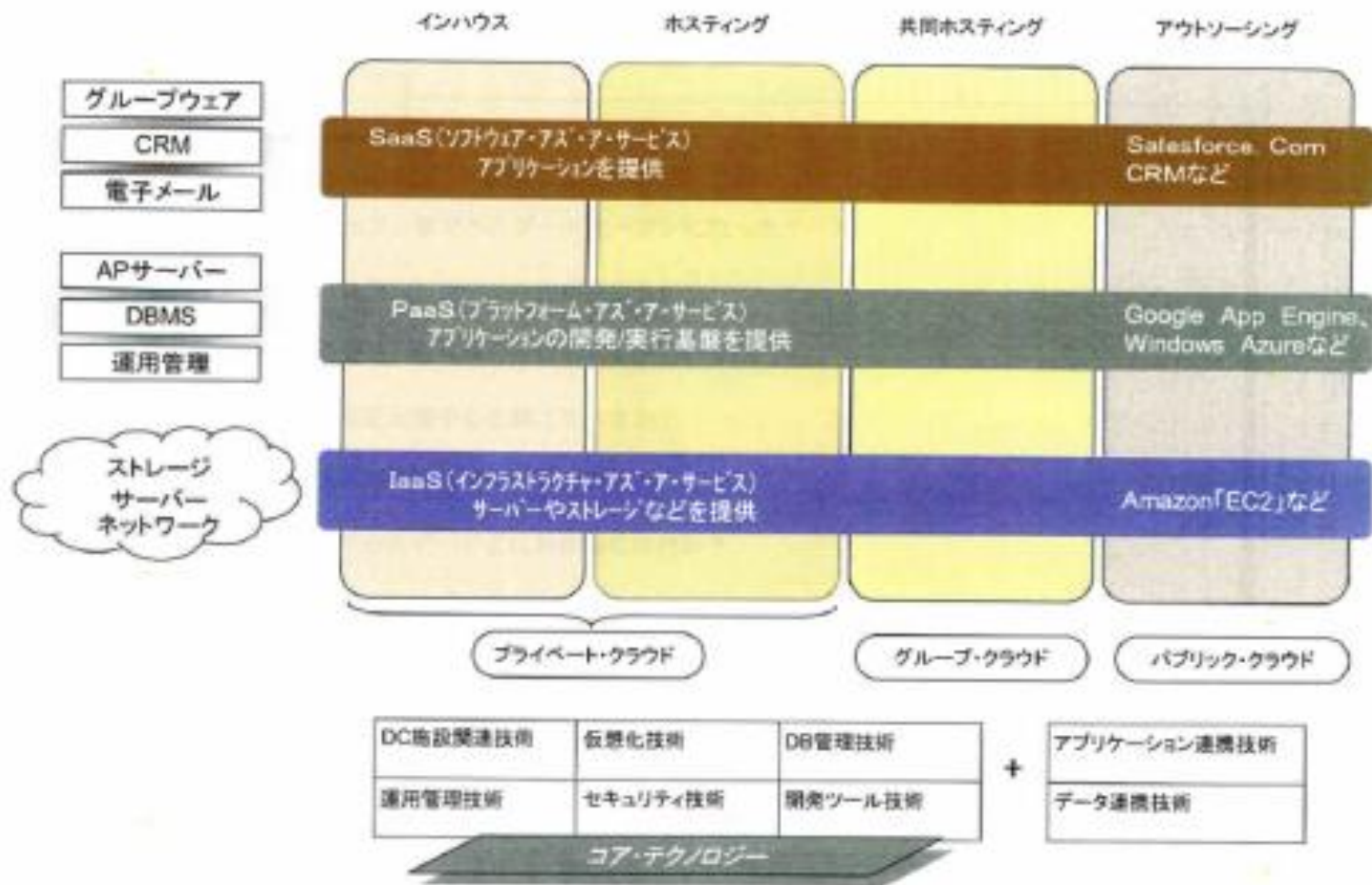
■ クラウドコンピューティング

「クラウド・コンピューティングとは、貯蔵／共有化された電算処理資源（ネットワーク、サーバ、ストレージ、サービス）を、ネットワークを介し必要に応じて利用可能とするモデル」（米国国立標準技術研究所の定義）

(特性)

- ・ オンデマンド／セルフサービス
 - ー ベンダーの人手を介することなく、自動化された形態でサービス利用が可能
- ・ ネットワークを介した利用
 - ー どこからでもサービス利用が可能
- ・ リソースの集中貯蔵
 - ー リソースの保管場所、保管形態を知ることなく、サービス利用が可能
- ・ 迅速なリソース確保／開放
 - ー 利用サービス資源の迅速なスケールアウト／インが可能
- ・ 計測可能なサービス
 - ー サービス利用の課金の透明性確保が可能

▼ クラウドコンピューティングのタイプ



(出所: FB&T)

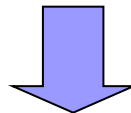
■ クラウドコンピューティングのメリット

クラウドコンピューティングの利用により、システム資源の安定性確保や規模拡張に頭を悩ませることなく(コスト負担を含め)、本来のコア業務に専念できる。

- コスト削減
 - ー システムの規模拡大に伴うコスト負担
 - ー 不稼動資源に対するコスト負担
- 迅速性
 - ー システム資源のスピーディーな提供
 - ー システム開発のスピードアップ

■ クラウドコンピューティングのリスク

- ー 殆どのリスクは、従来システムと共通ないしその延長線上のもの。
- ・ 情報セキュリティのリスク
 - ー サービス提供者のリスク対策が不十分なため、情報漏洩が発生するリスク
- ・ システム復旧のリスク
 - ー サービス提供者のリスク対策が不十分なため、障害時や災害発生時のシステム復旧が遅延するリスク
- ・ データ取得・復旧のリスク
 - ー データの所在が不明確であることに伴う、当局要請時やシステム障害時等におけるデータ取得・復旧の遅延リスク
- ・ リーガルリスク
 - ー システム・データが海外に所在することに伴い、外国の法規制を受けることになるリスク

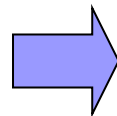


サービス提供者のリスク対策の明確化・可視化
(SLAの締結、立入調査権の確保、外部監査結果の入手など)

(2) システム外部委託の進展

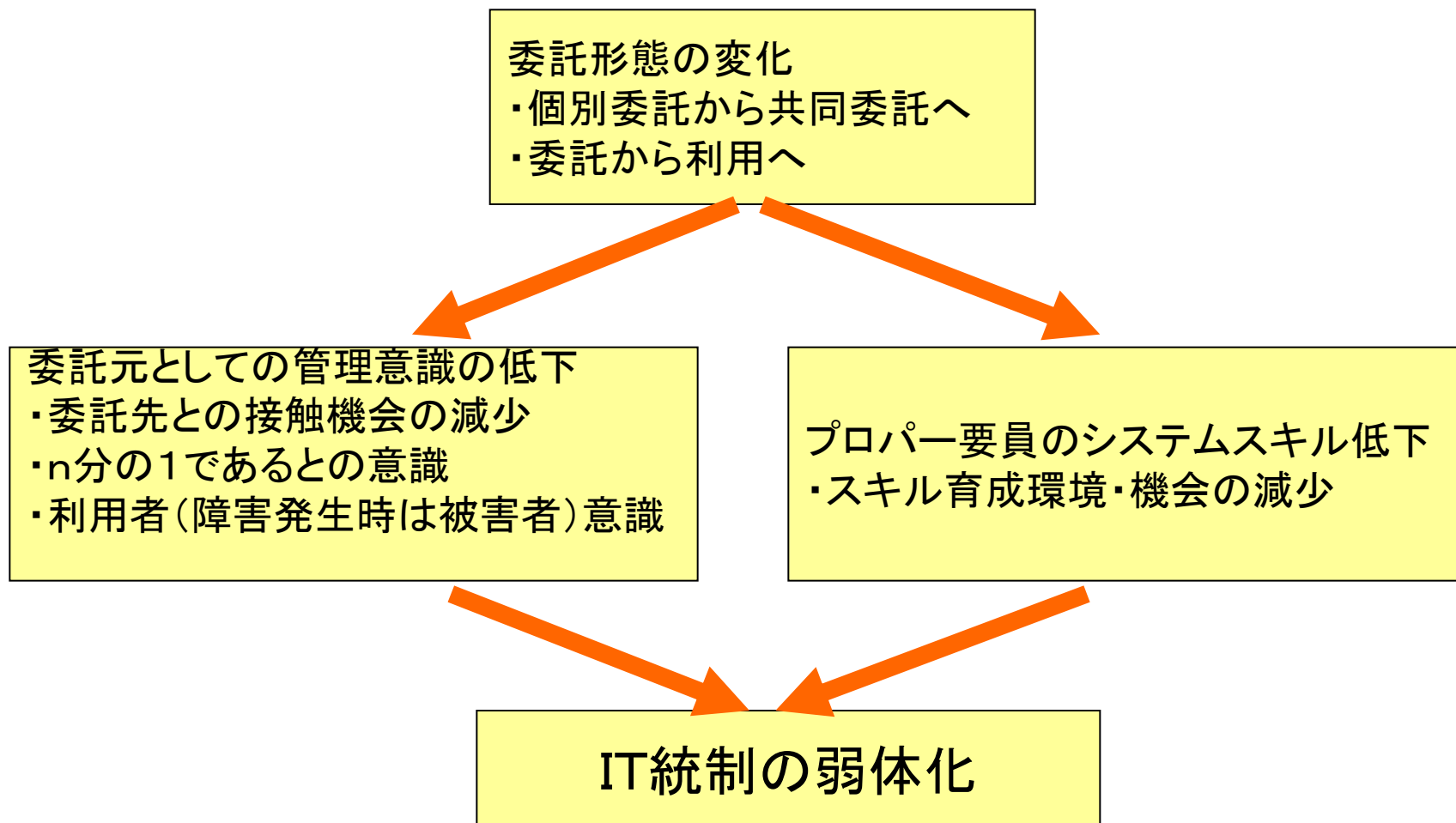
システム技術の高度化・多様化

システム関連コストの圧縮要請

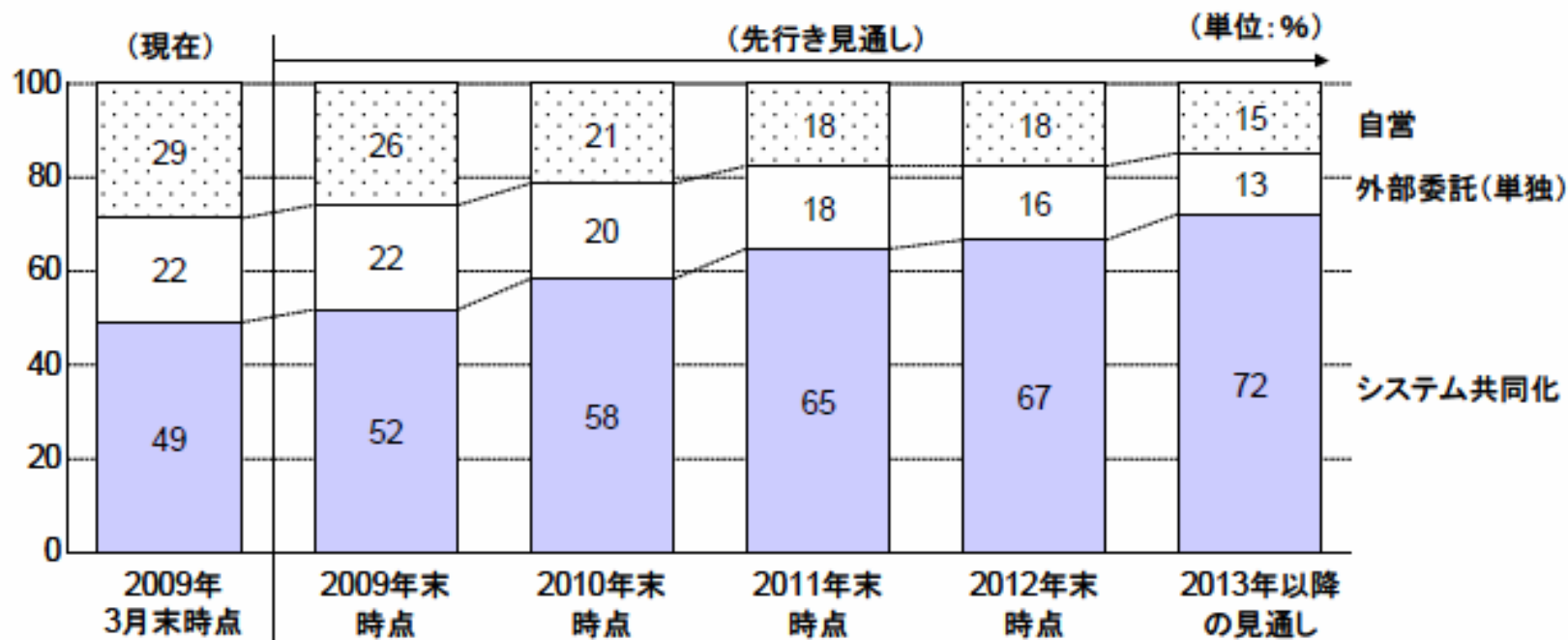


外部委託先依存度の高まり

▼ 外部委託の進展がIT統制に与える影響



▼ 地域銀行における勘定系システム共同化の進展



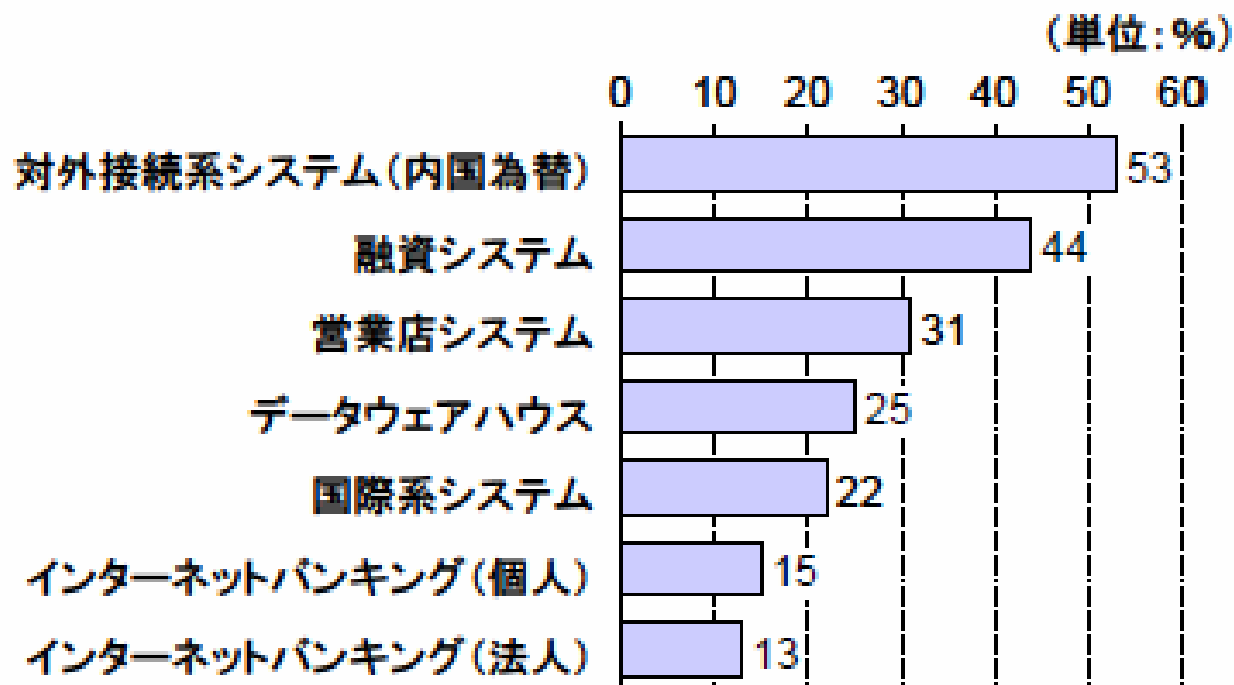
(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼ 主要な勘定系システム共同化(2009/12月時点)

	ベンダー	利用(予定)先数	システム基盤	実現方式(注)	AP提供者
BeSTA	NTTデータ	9(6)	メインフレーム	④	ベンダー
MEJAR	NTTデータ	0(3)	メインフレーム	④	ベンダー
じゅうだん会	日本IBM	6(1)	メインフレーム	①or③	銀行
CHANCE PROJECT	日本IBM	4(2)	メインフレーム	③	銀行
TSUBASAプロジェクト	日本IBM	0(5)	n.a.	n.a.	ベンダー
Bank Vision	日本ユニシス	2(6)	Windows	②	ベンダー
NEXT BASE	日立	5(4)	メインフレーム	④	ベンダー
STELLA CUBE	NTTデータ	0(8)	メインフレーム	④	ベンダー
STAR-ACE	NTTデータ	6(0)	メインフレーム	④	ベンダー
PROBANK	富士通	4(0)	メインフレーム	①or②	ベンダー
NEXT SCOPE	日立	3(0)	メインフレーム	②	ベンダー

(注)①センターが別々、②同一センター内でホストコンピュータが別々、③ホストコンピュータを論理分割、④業務APロジックで分割(マルチバンク方式)

▼ 勘定系システム共同化の周辺業務取り込み状況



(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

⇒ 今後、勘定系システムから周辺系システムへと共同化範囲が広がる見通し

▼ システム共同化のメリット・デメリット

(メリット)

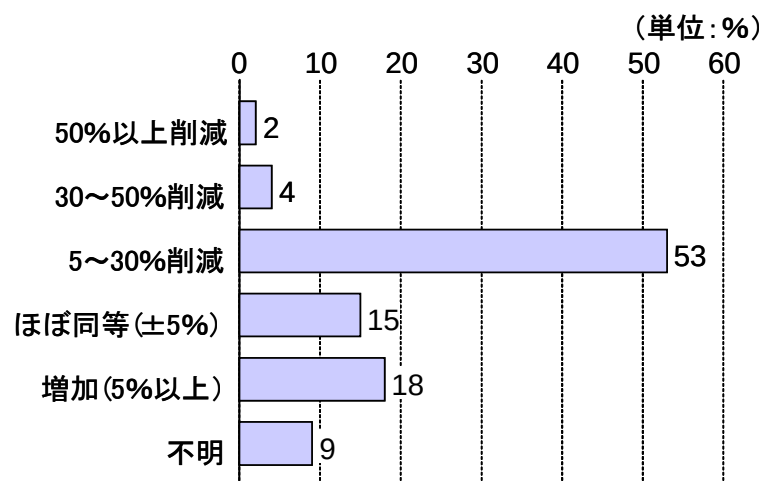
- ・ システム経費の削減
- ・ 自行システム要員の圧縮
- ・ 機能強化、サービスの充実
- ・ システムの信頼性・可用性・機密性の向上
- ・ システムの業務継続機能の向上

(デメリット)

- ・ システム仕様の柔軟性の低下
- ・ 開発スピードの低下
- ・ システムスキル・ノウハウの低下
- ・ 委託先管理の実効性低下
- ・ 次期システム検討の遅れ

▼システム共同化先のシステム経費の削減、自行システム要員の圧縮の圧縮

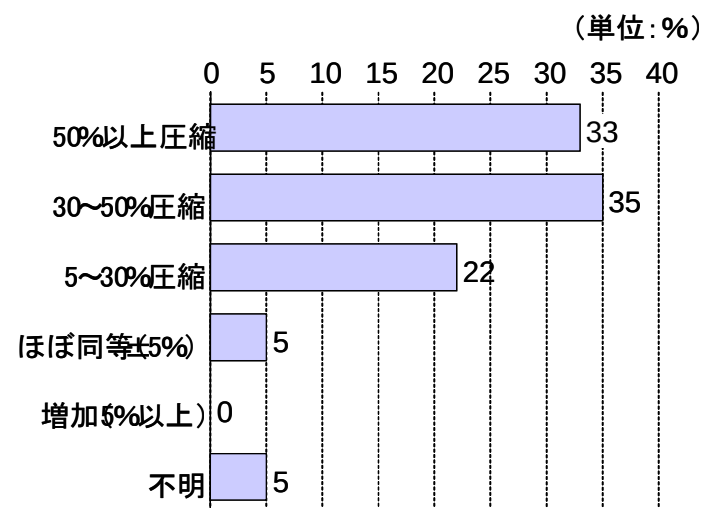
▽システム共同化に伴うシステム経費の削減効果



<集計対象金融機関数55>

※ 勘定系システム以外も含む、年間総システム経費比較

▽システム共同化に伴う自行システム要員の圧縮



<集計対象金融機関数>

※ 勘定系システム以外も含む、自行システム要員数の比較

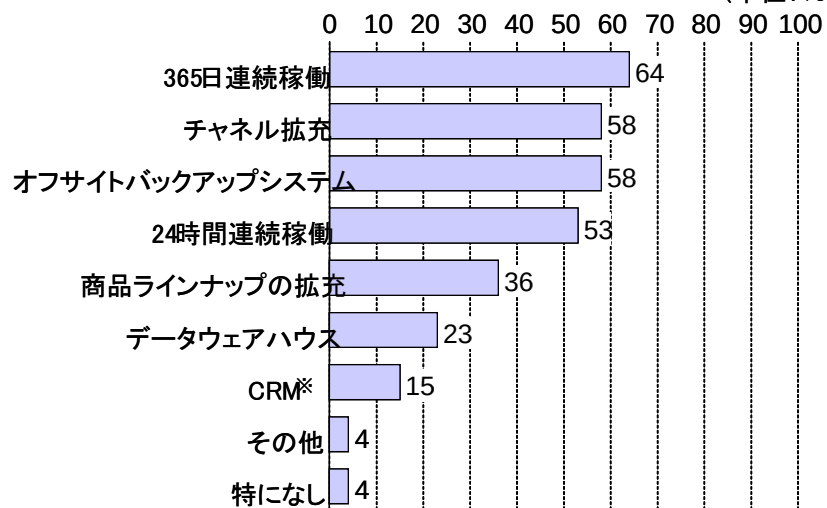
(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼ システム共同化先の機能強化、サービスの充実

▽システム共同化に伴い、機能・サービスが充実された点

(複数回答)

(単位: %)



<集計対象金融機関数>

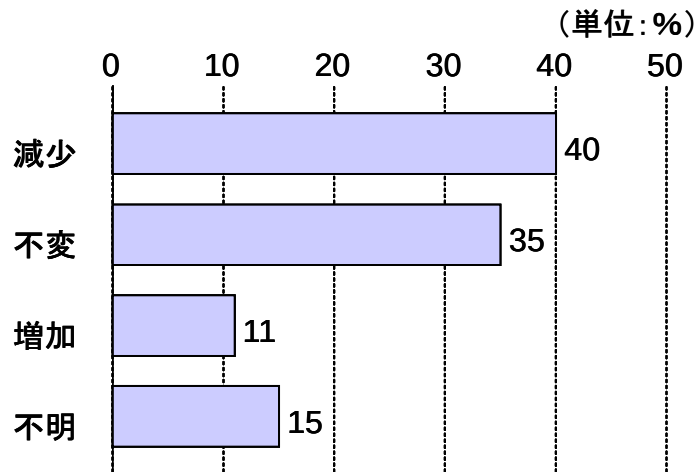
※ Customer Relationship Managementの略。詳細な顧客情報データベースを基に、企業が顧客との関係性をマネジメントする方法

(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼システム共同化先のシステム可用性の向上

▽ システム共同化に伴う

顧客影響障害の発生件数の変化

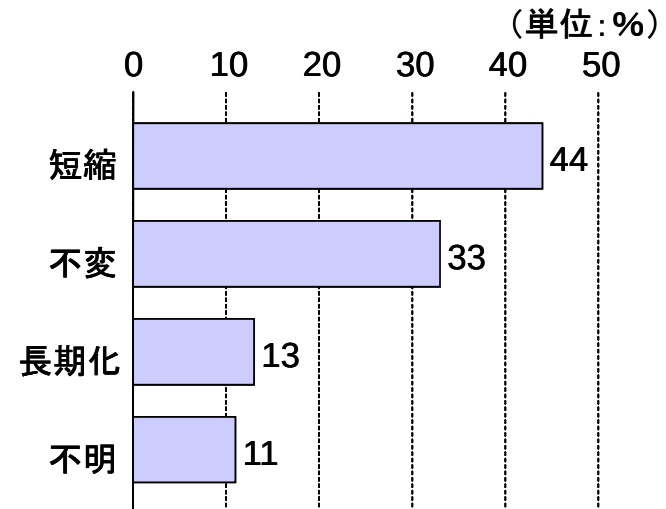


<集計対象金融機関数: 55>

※ システム共同化直後の初期障害を除く

▽システム共同化に伴う

障害発生後の復旧時間の変化

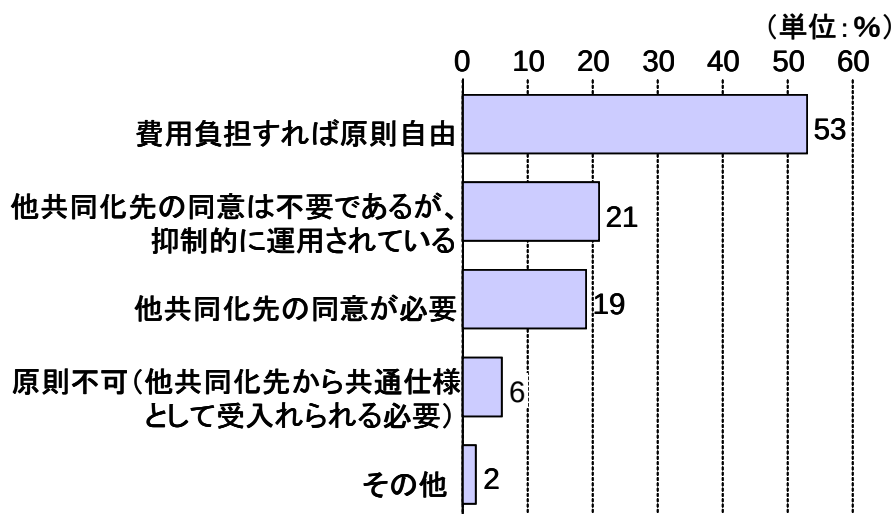


<集計対象金融機関数>

(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

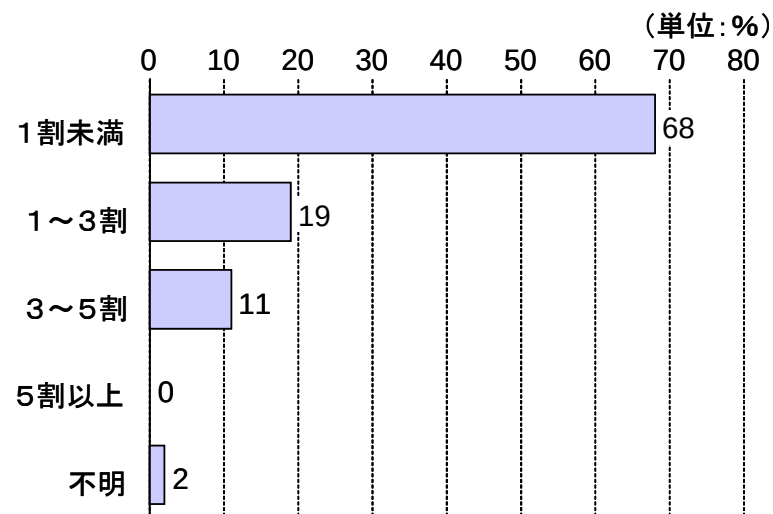
▼システム共同化先におけるシステム仕様の柔軟性の低下

▽ 自行独自のカスタマイズ(プログラム変更)の自由度



<集計対象金融機関数53>

▽ 共同システムの独自カスタマイズ率



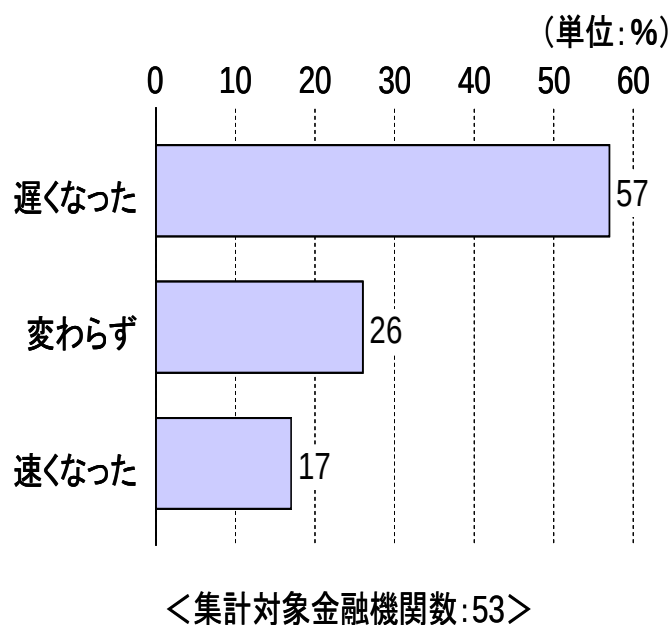
<集計対象金融機関数: 53>

※ 自行独自仕様のプログラムステップ数／全プログラムステップ数
(または、自行独自仕様の機能数／全機能数)

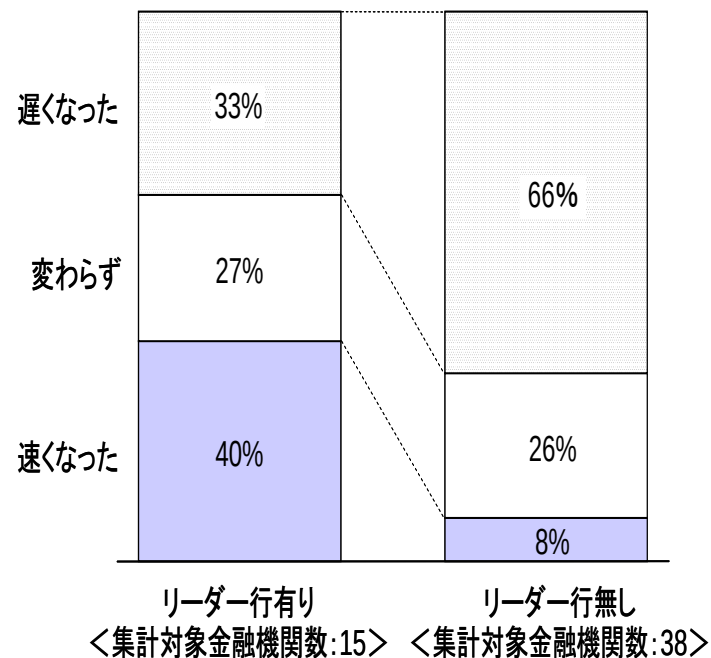
(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼システム共同化先における開発スピードの変化

▽ システム共同化に伴う開発案件提案から稼働開始までのスピード感の変化



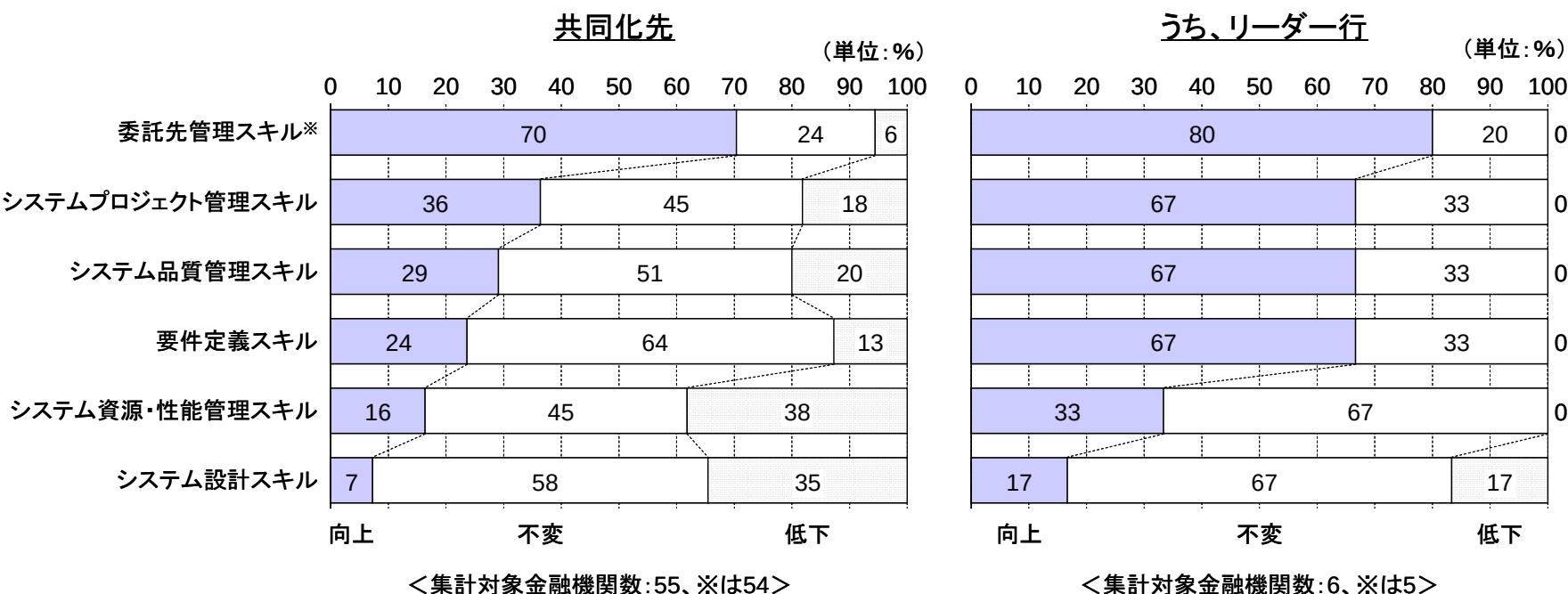
▽ リーダー行の有無と開発スピードの変化との関係



(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼システム共同化先におけるシステムスキル・ノウハウの変化

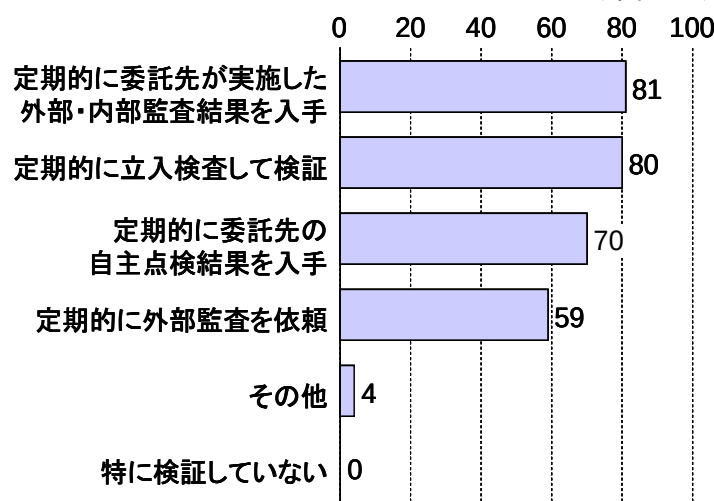
▽ システム共同化に伴う自行職員のスキル変化



(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

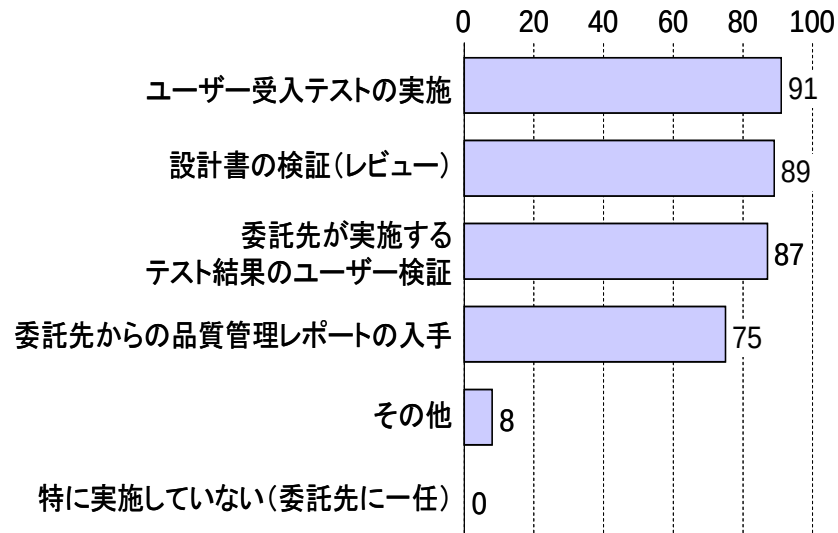
▼システム共同化先における委託先管理実施状況

▽ 共同化先が実施している委託先管理手段
(複数回答) (単位: %)



<集計対象金融機関数:54>

▽ 共同化先が実施している品質管理手法
(複数回答) (単位: %)

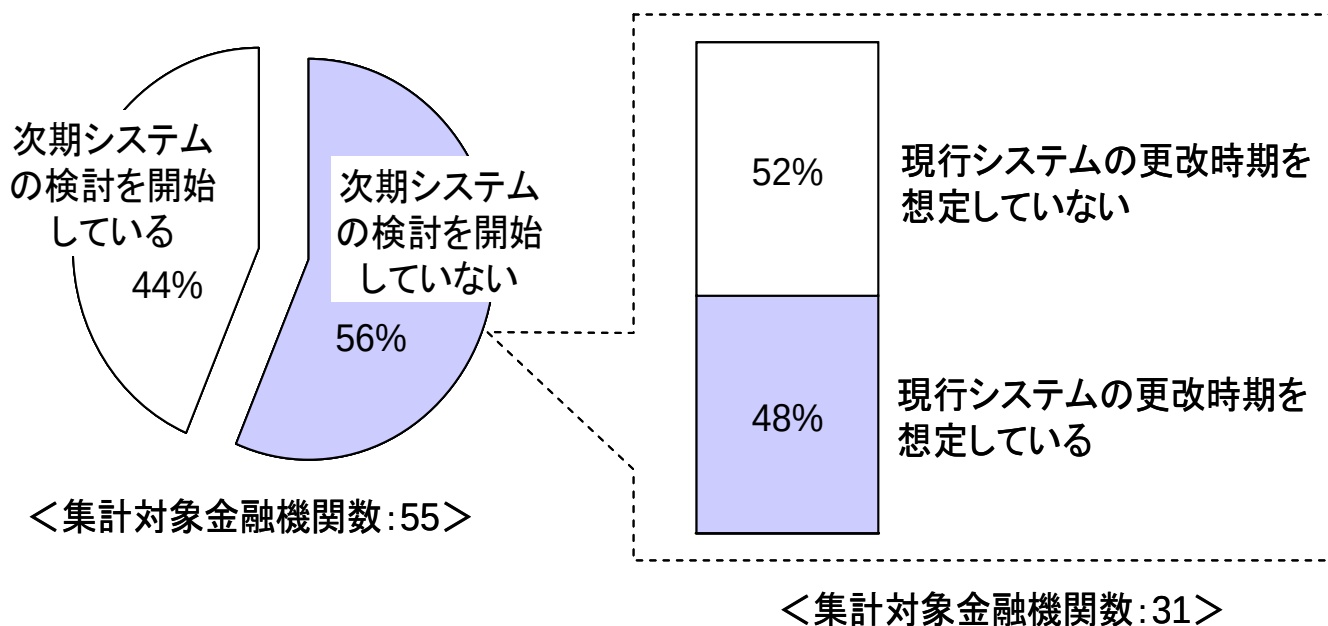


<集計対象金融機関数:53>

(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

▼システム共同化先における次期システム検討の遅れ

▽ 共同化先における次期システムの検討状況と、 現行システムの更改時期の想定有無



(出所: 日本銀行「金融機関におけるシステム共同化の現状と課題」(2009. 6))

2. システムリスク管理上の留意事項

(1) 経営陣の役割

- 外部委託への依存度が高まったとしても、経営陣の役割は基本的に変わらない。
- 経営陣は、システムを経営に直結する問題として捉え、システムリスク管理を重視する必要。
⇒ 一度、システムリスクが顕現化すると、経営に重大な影響。

事例1： みずほ銀行の大規模システム障害(2002年)

- ー 旧3行システムの暫定統合時の障害。十分なシステム品質の見極めができないままシステム統合に踏み切ったことが原因であるが、背景にはシステム統合の難しさに対する経営陣の認識の甘さ。

事例2： 三菱UFJ証券の大規模情報漏洩(2009年)

- ー 元職員の内部犯行が直接の原因であるが、背景には脆弱な情報セキュリティ管理態勢に対する経営陣の認識の甘さ。

■ 経営陣の役割

⇒ 外部委託の進展という実態を踏まえたうえで、以下の戦略・方針策定を自ら率先して推進する必要。

- システム戦略方針の策定
- システムリスク管理態勢の整備・確立
- システムリスク管理方針の策定
- システムリスク管理プロセスの策定
- 危機管理体制の整備方針の策定
- 人材育成方針の策定

(2) リスクベース・アプローチ

限られた資源のなかで、実効的かつ効率的なシステムリスク管理を行うため、残存リスクの大きさに応じたリスクベース・アプローチを徹底する必要。

① システムの品質管理

■ 留意しておくべきこと

- ・ 金融機関システムの品質に対する要求水準は高い
 - ー 顧客、監督当局、マスメディア
- ・ 原因と結果の非対称性
 - ー 大規模システム障害を引き起こすのに大きな原因は必要ない。
- ・ 品質とコストのバランス確保
 - ー 品質に完璧を期すほど、コストは加速度的に増加。

■ 金融庁監督指針の記述

「中小・地域金融機関向けの総合的な監督指針」

(Ⅱ－３－６－１－２ システム統合リスクの「リスク特性」とリスク軽減策)

- ・ システム統合リスクのリスク量は、事象(イベント)の発生確率と発生した場合の影響度(インパクト)の積で認識すべきものであり、銀行は、業容等を勘案した上で、徹底したリスク軽減策が求められることに留意する必要がある
- ・ 加えて、リスク軽減策に見合うコンティンジェンシープランを整備し、各種リスク事象が複合的に顕在化(障害が同時発生)しても、顧客に大きな影響を及ぼすことを回避できるような態勢を整備する

「主要行等向けの総合的な監督指針」

(Ⅲ－３－８－１－１ システム統合リスク)

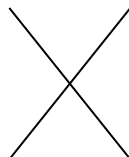
- ・ 主要行等の業容等からすれば、以下のような徹底したリスク軽減策が求められることに留意する必要がある
- ・ 発生する確率は低い事象でも、発生した時にはその影響が極めて大きいため、コンティンジェンシープランを発動しても制御し切れず、結果として顧客や決済システム等に大きな影響・障害を与えるリスク事象があることを重視し、そのようなシステム及び業務・事務を網羅的に洗い出して、徹底したテスト・リハーサル等により、これらの発生を確実に防止することが基本となる

■ 実効的かつ効率的な品質管理を行うためのポイント

・ システム・開発プロジェクトの重要性(リスクの大きさ)に応じたリスクベースな品質管理の徹底。

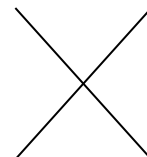
ー 例えば、開発プロジェクトにおいて徹底した品質向上を要するケースとそうでないケースの切り分け。

システム・開発
プロジェクトの
重要性



品質向上のためのメニュー

- (委託先成果物検証)
- ・設計書検証
- ・ソースコード・インスペクション
- ・テスト項目検証
- ・テスト結果検証, 等
- (テスト結果分析)
- ・障害発生傾向分析
- ・メトリックス分析
- ・すり抜け分析
- ・障害収束分析, 等
- (品質向上テスト実施)
- ・障害分析を踏まえた追加テスト
- ・連続日回しテスト
- ・ピーク日事務量テスト
- ・過負荷テスト
- ・いじわるテスト
- ・端末集中打鍵テスト
- ・顧客との接続テスト
- ・障害時運用テスト
- ・無影響確認テスト, 等



実施の範囲・
深度・網羅性

②外部委託先管理

■ 留意しておくべきこと

- ・ 業務の外部委託は、金融機関が当該業務に係る顧客への責任を免れるための理由にはならない。
- ・ 金融機関は当該業務に関して適切なリスク管理が外部委託先によって行われていることを、適切なモニタリングを通じて確保する必要がある。
- ・ 外部委託先による適切なリスク管理レベルは、当該委託業務の重要度に応じて定まるのであって、契約形態（委託か利用か、国内か海外か、等）により左右されるものではない。
- ・ 外部委託先のリスク管理が適切かどうかは、金融機関が自身のリスク管理基準に従い当該業務を行った場合と、同等レベルかどうかを判断基準とすべきである。
- ・ 外部委託先に対するモニタリング手法は、契約形態によっては制約を受けることもあり、適切にモニタリングできる範囲において柔軟であってよいと考えられる

■ 金融庁監督指針の記述

「主要行等向けの総合的な監督指針」

（Ⅲ－３－３－４－１ 外部委託・意義）

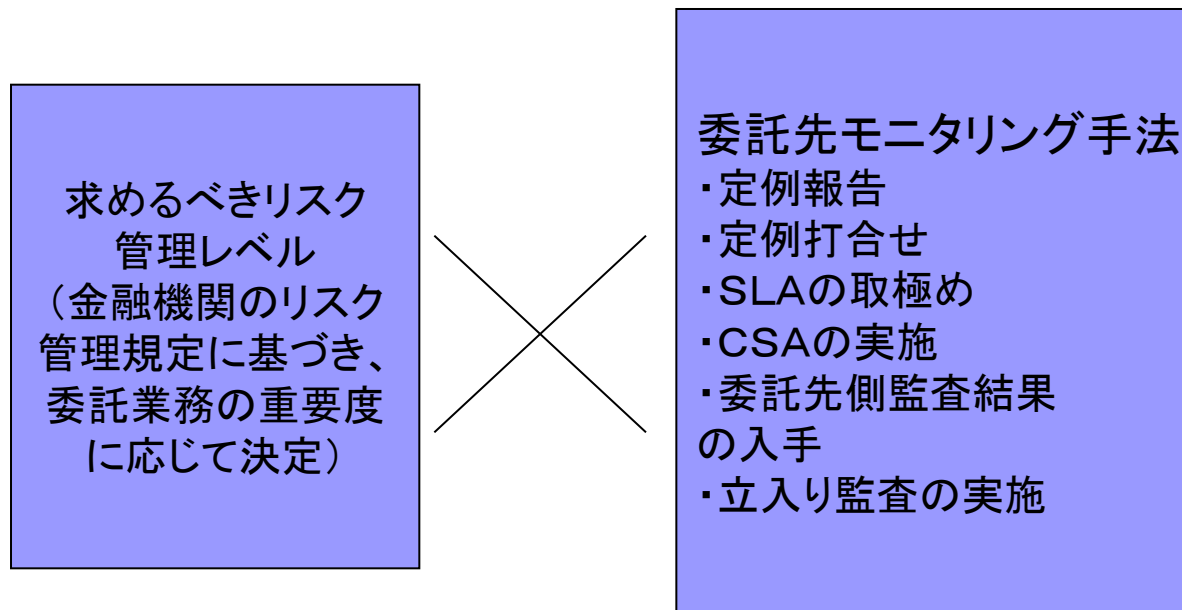
- ・ 銀行が外部委託を行う場合には、顧客を保護するとともに、外部委託に伴う様々なリスクを適切に管理するなど業務の健全かつ適切な運営を確保することが求められる
- ・ 外部委託には・・・形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む

（Ⅲ－３－３－４－２ 外部委託・主な着眼点）

- ・ 委託契約によっても当該銀行と顧客との間の権利義務関係に変更がなく、顧客に対しては、当該銀行自身が業務を行ったのと同等の権利が確保されていること

■ 実効的かつ効率的な外部委託先管理を行うためのポイント

- ・ 委託業務の重要度に応じた求めるべきリスク管理レベルの明確化と、契約形態に応じた適切なモニタリング手法の選定。
 - ー 契約の制約から適切なモニタリングが出来ない場合は、委託先の変更も考慮する必要。

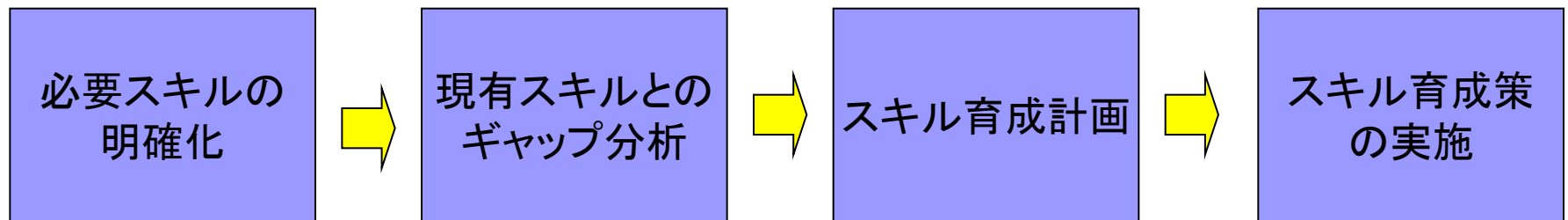


3. IT人材の育成

- 外部委託が進展する中で、システム部門に求められる役割とは、
 - ・ システム戦略の経営陣への提案
 - ・ ベンダー提案の評価
 - ・ システム開発プロジェクト管理(委託元として)
 - ・ 委託先管理

- 金融機関IT要員に求められるスキルとは、
 - ⇒ 「ユーザー部門とITベンダーの橋渡し」
 - ⇒ 但し、単なる「つなぎ屋」ではなく、付加価値を付けることが必要。
- ①システム戦略の策定・提案スキル
経営戦略とユーザーの業務ニーズを踏まえたシステム戦略を策定・提案できるスキル。
- ②システム企画スキル
IT技術进行评估し、製品の特性や能力を生かして実現可能なシステムを企画できるスキル。
ITベンダーの提案を正しく評価できるスキル。
- ③プロジェクトマネジメントスキル
システム開発プロジェクトのプロジェクトマネージャーとして、全体を統括し、委託先管理、プロジェクト管理を実行できるスキル。

▼ IT人材育成のステップ



- 併せて、魅力的なキャリアパスと正当な評価軸を整備し、IT要員のやる気を引出すことが重要。

▼スキル育成策

— スキル育成計画に沿って、中長期的に地道に取り組む他ない。

■ 研修

-- 外部セミナーへの参加

■ 資格取得

-- ITコンサルタント、ITアーキテクト、プロジェクトマネージャー

■ 委託先への派遣

-- システム開発、プロジェクト管理等の実務経験

-- ジョブローテーションへの組込み

■ 中途採用

-- 外部人材の活用

ご清聴有難うございました。