2007年3月23日

金融機関におけるコンピュータ・システム・リスク管理の現状と課題

日本銀行
BANK OF JAPAN

日本銀行金融機構局
システム関連考査担当
岩佐 智仁

本日のご出席者

業態	大手銀行、地域銀行、信用金庫、外国銀行、 証券会社、決済機関、協会・団体、ITベンダー
所属	システム企画・開発・運用部署、 リスク管理部署、総合企画部署、監査部署
職種	役員、管理職、ご担当者、 プロジェクトマネージャー、システムエンジニア
システム 運用形態	自営、単独アウトソース、共同センター、 本国（海外）
システム 構成	ホスト系、オープン系 全国規模ATMネットワーク、自社ATMなし

システム・リスク管理は、全てに共通する事項

システム・リスク管理に関する公表資料

「事例からみたコンピュータ・システム・リスク管理の具体策」（2007年3月15日、日本銀行ホームページ掲載）

―― 本日お手許に配布

―― 金融機関の頭取等の方にも別途送付済み

- 考査等で見られたシステム・リスク管理面の要改善事例やシステム障害事例を基に、管理上の具体策を紹介

  ―― リスク管理上の一般的な留意点は、以下の公表資料を参照

  「金融機関における情報セキュリティの重要性と対応策」（2000年4月）

  「わが国金融機関におけるシステム・リスクの管理状況と留意点」（2001年9月）

- どの金融機関でも起こり得る共通事例を列挙

  ―― 「障害対策」と「情報セキュリティ対策」は、より具体的な想定事例と対応策を整理

ご説明内容

1．システム・リスク管理の観点・項目 ⇒ まずは基本から

2．金融機関におけるリスク管理の実態 ⇒ PDCAサイクルの実施に苦労されている先が多い

3．PDCAサイクル実施の必要性 ⇒ リスク管理におけるPDCAサイクル実施の必要性を改めて説明

4．要改善事例と対応策 ⇒ 具体事例を紹介

5．リスク・ファクターの変化
（1）相互接続の拡大
（2）基盤技術の変化
（3）外部委託の進展
⇒ リスク・ファクターの変化に合わせて、対策を随時見直す必要

（2）に焦点を絞り ⇒ 6．オープン系システムの特徴と留意点

1．システム・リスク管理の観点・項目

（1）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

本日は、安定性・安全性・信頼性を説明

（２）管理の項目（1/2）

① システム・リスク管理の体制、プロセス

- 管理の枠組みや規程類の整備
- ＰＤＣＡサイクルの実施
- 委託先管理体制の整備や、報告内容の検証体制の確立

② システム企画・開発管理

- プロジェクトの進捗・品質管理体制の整備

③ システム障害管理

- マニュアル類の整備、訓練の実施
- 障害発生時の連絡・報告体制の確立
- 障害原因の究明、再発防止策の検討

（2）管理の項目（2/2）

④ 情報セキュリティ管理

- 重要情報へのアクセス管理（ID、パスワード管理）
- コンピュータ・ウィルス対策、外部侵入対策

⑤ 緊急時対応

- コンピュータ・システム、設備、要員の整備
- 実効性があるコンティンジェンシー・プランの作成
- 実運用に即した定期的な訓練の実施

⑥ システム監査

- システム監査部署の体制整備（外部監査の活用）
- 監査計画の策定
- 監査結果の反映、フォローアップ

２．金融機関におけるリスク管理の実態

（１）リスク管理の必要性の認識

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決済システムを形成
- 膨大な顧客情報を処理

障害時における業務停止や、不正アクセスによる情報漏洩は、金融機関経営において、極めて重大なリスク

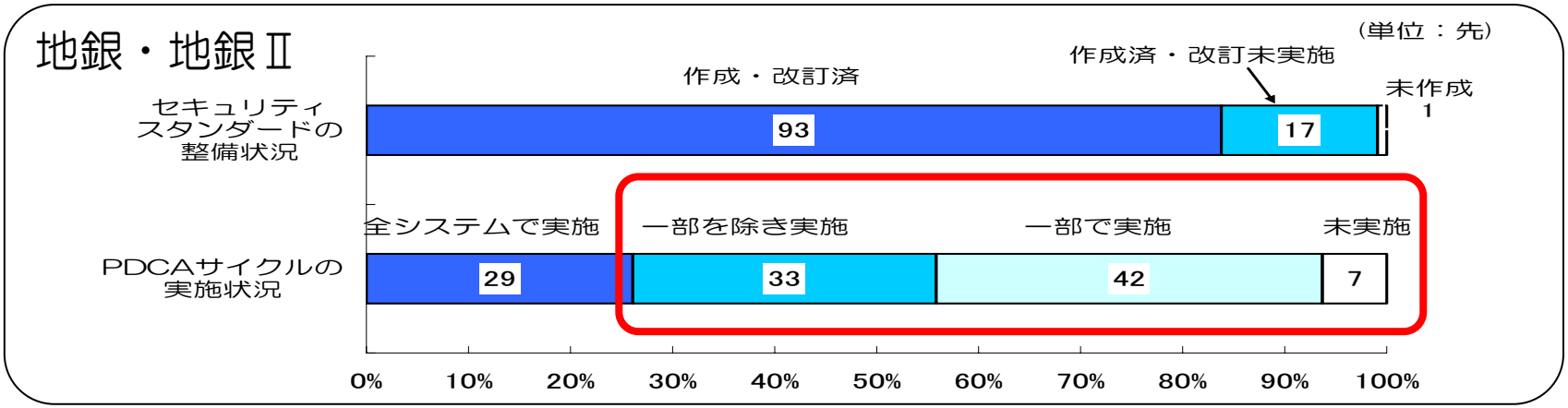
・小さなプログラム・ミス等が業務全体を止める可能性
・特定先で発生した障害が、他社に影響する可能性

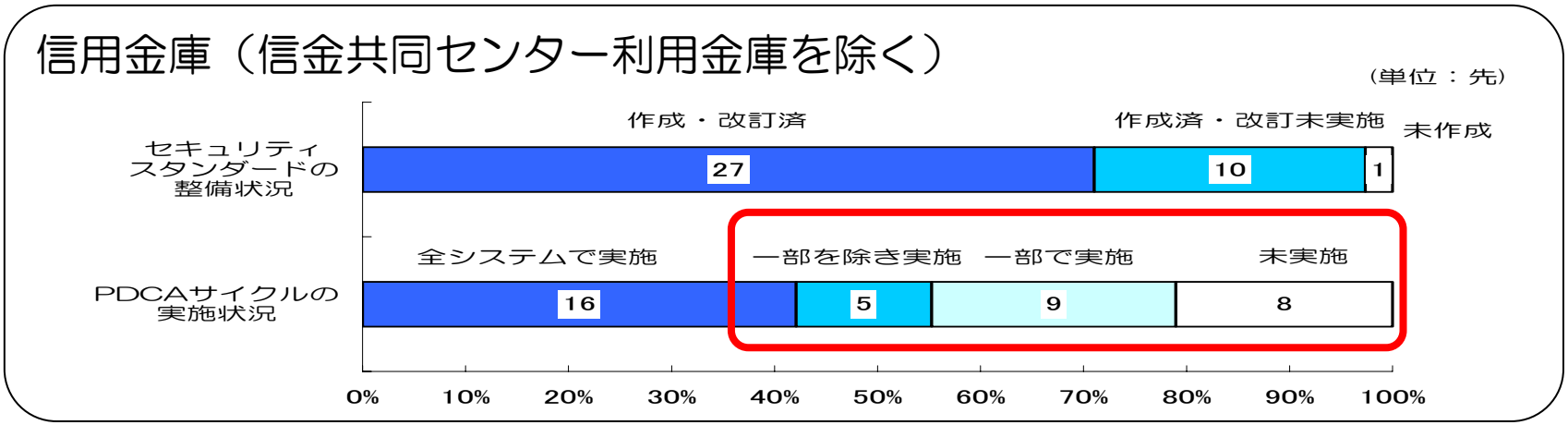
このため金融機関では

システム・リスクを主要リスクと位置付け、リスク管理規程の制定やPDCAサイクルの実施を通し管理体制を整備

（2）PDCAサイクル実施にかかる実態

■ 規程を「作成」かつ「改訂済」ながら、ＰＤＣＡサイクルを十分に実施している先は多くない



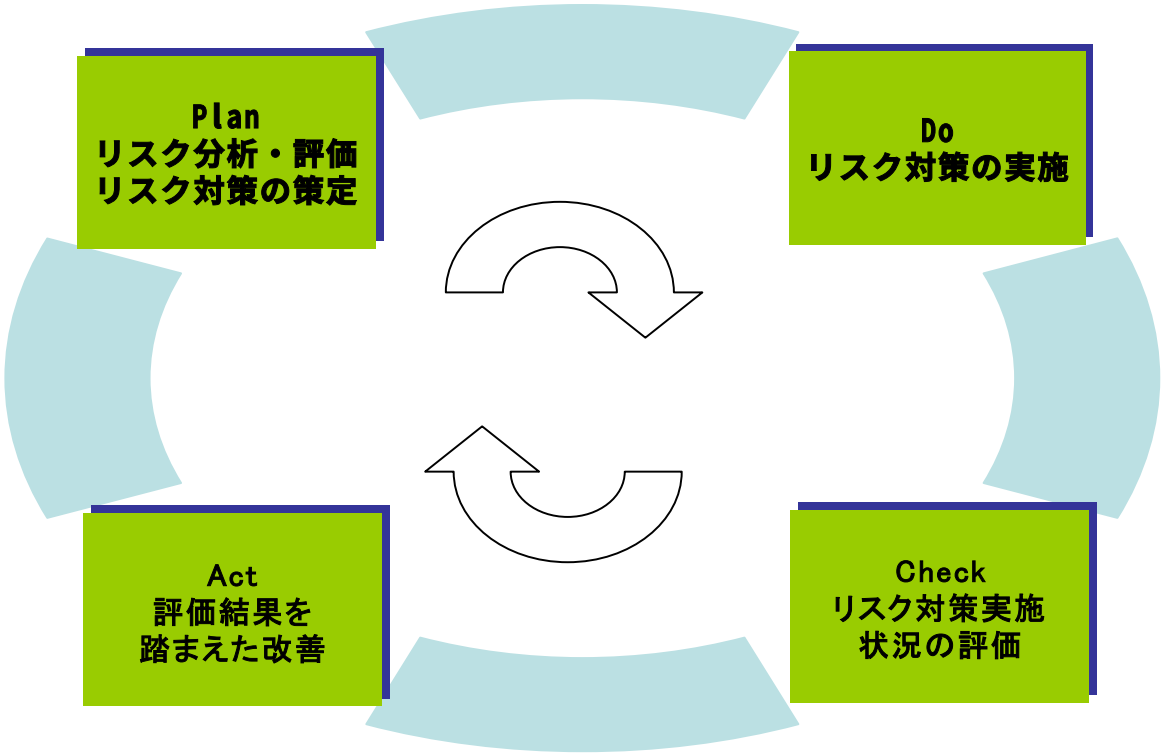


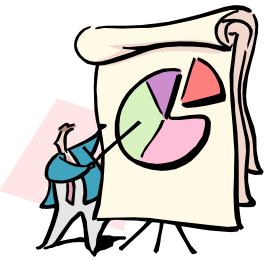
2006年に日本銀行が実施した地域金融機関のアンケート結果から

３．PDCAサイクル実施の必要性

（１）基本的な枠組み

- システム・リスクを一定以下に抑えることが目的
- 全社的なシステム・リスク管理の規程を、開発や運用の現場に反映していく一連のプロセス





（２）リスクの分析・評価

- システム設計や運用、利用状況が、基本方針で定めた基準をクリアしていることを確認
- 基本方針等と実態のギャップを把握し、リスクの内容・大きさを分析・評価
- 経営層は現状を認識し、資源の割り当てや新技術の導入などにより、有効なリスク対策の実施に繋げる

これらを定期的に実施していないと、以下のような問題に

４．要改善事例と対応策

（１）リスク管理体制・プロセス（1/4）

① システム・リスク管理の体制、プロセス

② システム企画・開発管理

③ システム障害管理
④ 情報セキュリティ管理
} 次の講演者が説明

⑤ 緊急時対応 } 2006年9月19日：金融高度化セミナー

⑥ システム監査 } 今回は説明の対象外

（１）リスク管理体制・プロセス（2/4）

① 計画（Plan）

【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、全社横断的な確認が取られていない

- Aシステムの所管部署は、自らの業務に照らし合わせ、重要度「低」と評価
- Aシステムが算出したデータを利用するBシステムは、経営上必要不可欠なシステムのため、重要度「高」
- Aシステムは「低」クラスのリスク対策しか取られていなかったため停止
- Bシステムが利用不可となり経営上打撃

全社レベルにおけるリスク評価結果の整合性確認

（１）リスク管理体制・プロセス（3/4）

② 実施（Do）

【要改善事例】
ユーザー部署の重要システムがリスク管理対象外となっているため、リスク対策が不十分

- リスク管理対象システムの洗い出しは、システム部署主導で実施
- ユーザー部署所管システムの中に重要システムがあるが、ユーザー部署は、リスク管理のプロセスを把握しておらず、管理対象に指定されずリスク対策が不十分
- 当該システムが停止し経営に重大な影響

ユーザー部署所管システムを含めたリスク管理の実施
―― システム部署の適切な関与

（１）リスク管理体制・プロセス（4/4）
③ 確認（Check）、処置（Act）

【要改善事例】
リスク管理規程に最近の環境変化を反映していない

- 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
- 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対応に遅れ
- 適切な対策が取られていないため、犯罪者の的に

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

（２）システム企画・開発管理（1/3）

① システム・リスク管理の体制、プロセス

② システム企画・開発管理

③ システム障害管理

④ 情報セキュリティ管理

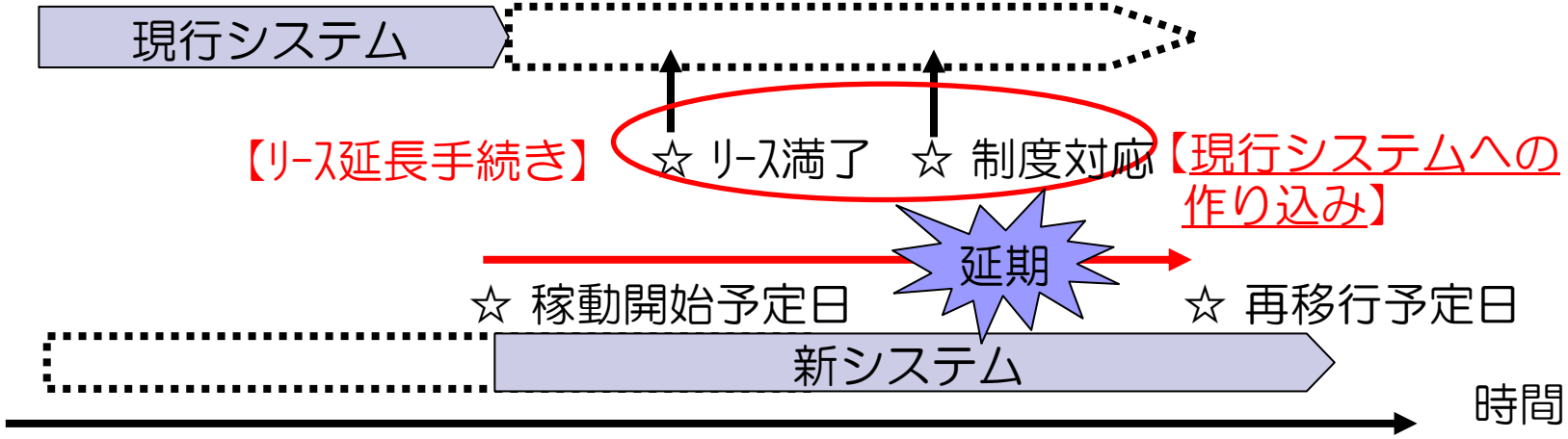
⑤ 緊急時対応

⑥ システム監査

（２）システム企画・開発管理（2/3）

① プロジェクトの管理体制

【要改善事例】
新システムの稼動を延期する場合に必要となる作業が、洗い出されていない

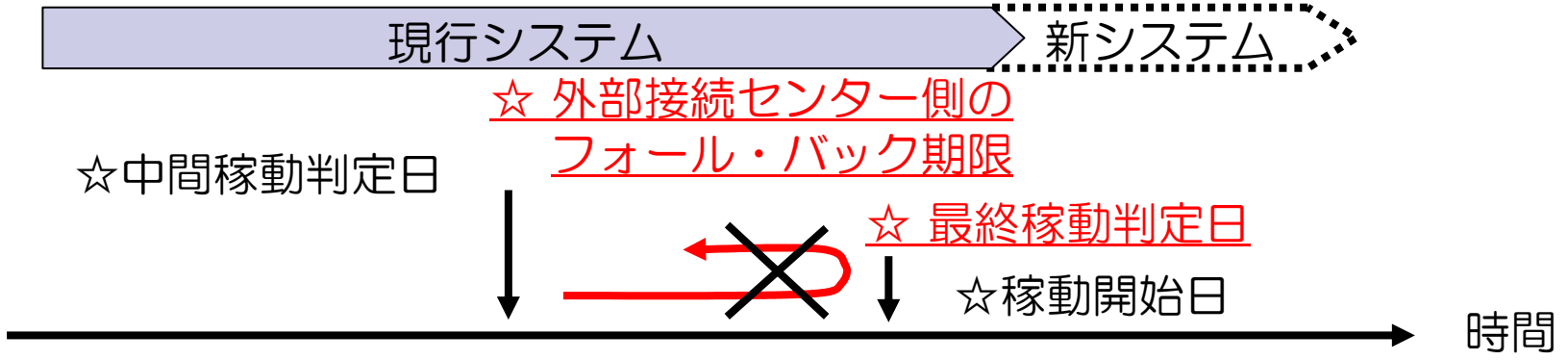


作業項目・負担を事前に洗い出し、
対応方法を決めておく必要

（２）システム企画・開発管理（3/3）

② 稼動判定

【要改善事例】
最終稼動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、
最終稼動判定日を確定する必要

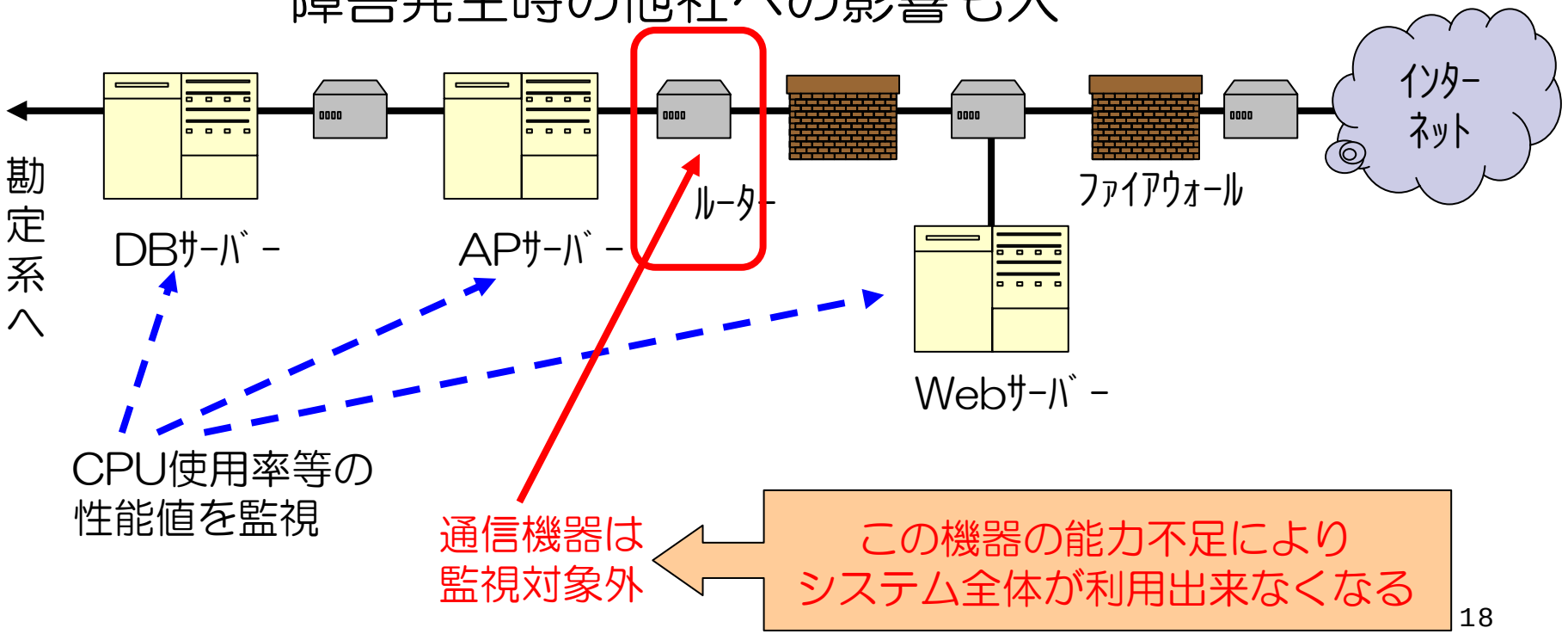
さらに加えて、新たな環境変化を取り込む必要がある

5．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、相互接続も拡大

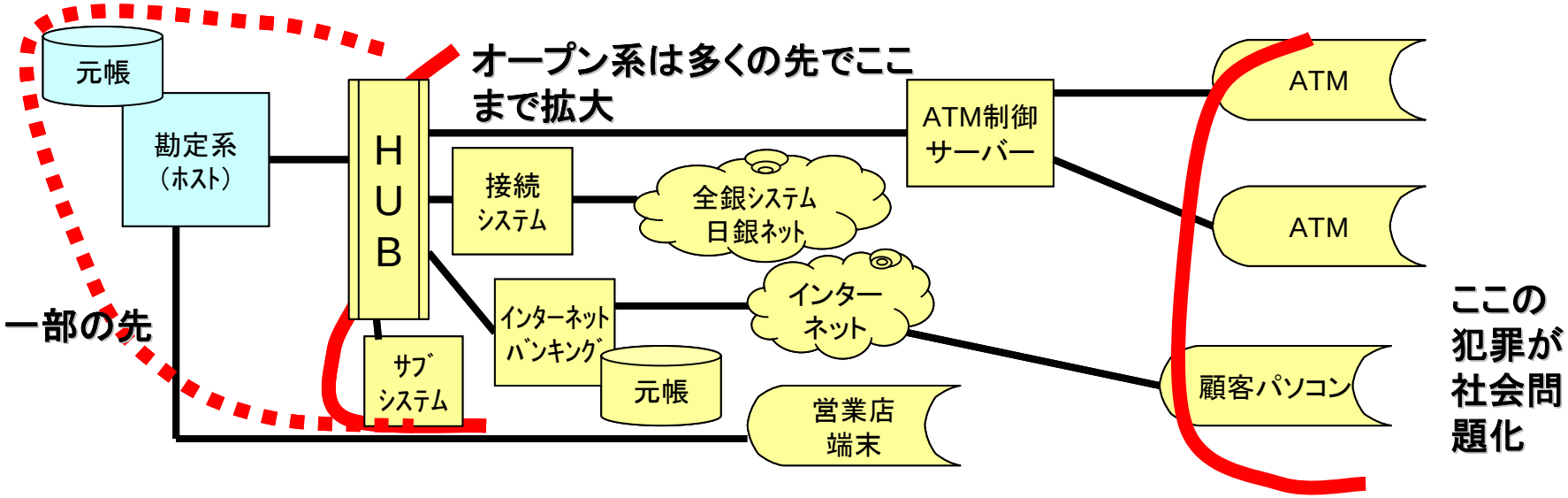
- 一つのシステムの不具合や処理能力不足が、システム全体の処理遅延に繋がる

——障害発生時の他社への影響も大



（2）オープン（分散）系システムの採用拡大など基盤技術が変化

- 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
- 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



（３）システム開発・運用の外部委託の進展

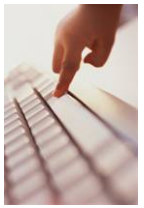
■ 金融機関自らが行う必要がある事項まで、委託先に任せきりにする事例

【事例１】

新システム構築時に、機器の処理能力を確定する際、将来の事務量の増加率を委託先が試算

⇒ 委託先は、既存業務のみを試算対象にしていたため、新たな業務を追加したところ、能力不足が顕現化

⇒ または、非現実的である大幅な増加率により試算を行った結果、必要以上の能力の機器を購入



【事例２】

ユーザー受け入れテストまでも委託先に依頼

⇒ 業務要件の誤認など、期待通りに構築されていない可能性

６．オープン系システムの特徴と留意点

（１）オープン系の定義と特徴（1/3）

■ 安定性（可用性）面・信頼性面のリスク管理上のポイントは、オープン系とホスト系で共通する部分が多い

		オープン系	ホスト系	リスク管理上のポイント
安定性・信頼性	処理方式	【分散】 業務処理ごとに複数の小型ｺﾝﾋﾟｭｰﾀ（ｻｰﾊﾞｰ）で稼働	【集中】 複数の業務が少数の大型ｺﾝﾋﾟｭｰﾀで稼働 ― ただし、ディスク、回線、　端末等複数の機器も利用している	各機器が、システム全体として設計通りに機能していることの見極め ― 例えば、性能評価時におけるボトルネックの見極め
	ベンダー	【多数】 例えば、ﾊｰﾄﾞｳｪｱはA社、DBはB社など複数のﾍﾞﾝﾀﾞｰの機器により構成されている	【限定】 周辺機器も含めて単一ﾍﾞﾝﾀﾞｰであることが多い ― もっとも、ｺﾝﾋﾟｭｰﾀはA社、 端末はB社、AP開発はC社とﾏﾙﾁﾍﾞﾝﾀﾞｰ環境ともいえる	機器障害時の責任分界点の取決めなど、マルチベンダー環境下における適切なベンダー管理

（１）オープン系の定義と特徴（2/3）

- 一方、安全性（機密性、完全性）面のリスクは、オープン系システムで新たに生じる事項が多い（ホスト系では生じる可能性が低いリスク）

		オープン系	ホスト系	留意点
安全性	技術仕様	【公開】 誰もが入手可能な状況で公開	【非公開】 原則非公開。限られた範囲の仕様を入手するだけでも高額な費用を要する	① ウィルス・チェック・ソフト、ファイアウォール等セキュリティ製品の導入と、適切な維持管理 ② 不特定多数の接続を前提とした適切なアクセス権限の設定と、ID・パスワードの厳格な管理 ③ ファイアウォールに対する侵入テストによる検証
	ウィルス	【有り】 公開仕様を悪用し、ウィルスを作成	【無し】 ホスト系が感染するウィルスは皆無	
	ネットワーク	【オープン】 インターネット等不特定多数が利用しているネットワークを利用していることが多い	【クローズ】 利用者が限定されているネットワークを利用していることが多い	

（１）オープン系の定義と特徴（3/3）

- オープン系システムの導入は、勘定系の中心部分まで浸透する様相
  —— 勘定系ホストそのものへのオープン系システムの採用も、従来のインターネット専業銀行など一部の先から、一部地銀等にも拡大中
- オープン系システムの拡大につれ、金融機関個別のシステムおよび決済システム全体のリスク・ファクターは変化
- 金融機関は、変化に見合うリスク管理対策を実施する必要

情報セキュリティ等、専門的・技術的分野に関して、委託先依存度が高い傾向
—— 特に、ファイアウォールの信頼性テストや、不正侵入の検知方法等
外部からのセキュリティ侵害事例は、今のところ少ないが、こうしたリスク変化の動向を先取りし、所要のリスク管理対策を実施する必要がある

（2）具体的な留意点（1/5）

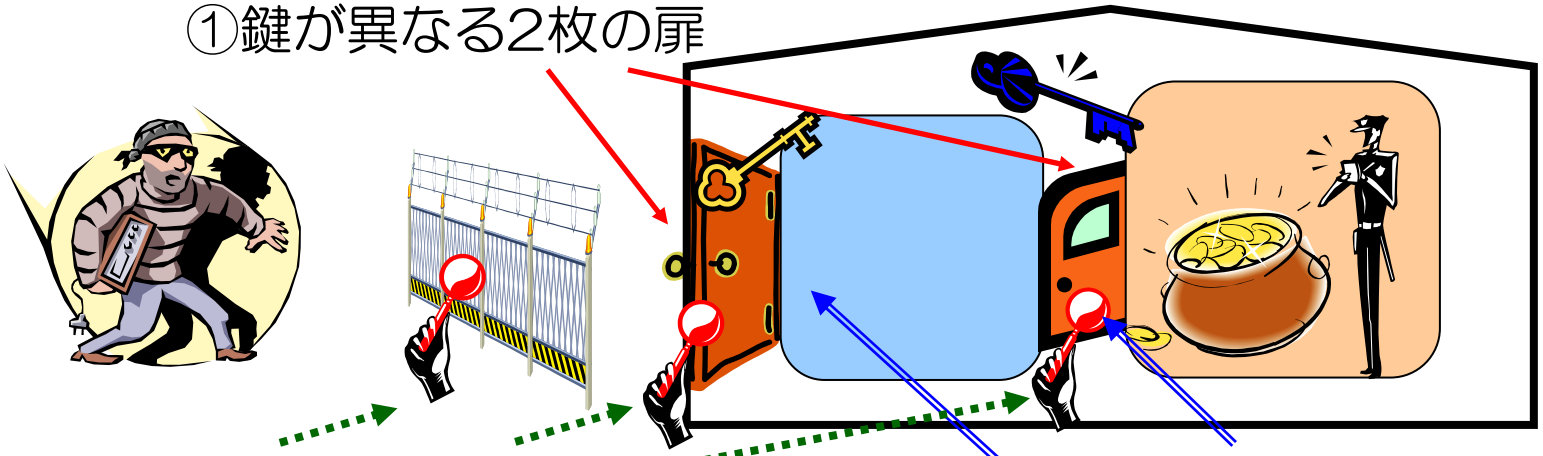
■ セキュリティー・ポリシーの枠組みは整っているが、ポリシー通りに運用されていない事例

＜安全な防犯基準とそれに見合う建物＞

① 扉は1枚目が破られたことを想定して2枚設置すること。その際には、鍵が異なるA扉とB扉にすること

② 扉は常時閉めておき、真の訪問者が来たときに開けること

③ ピッキング等に備えて、それぞれの鍵の信頼性確認を、警備会社に定期的に依頼すること



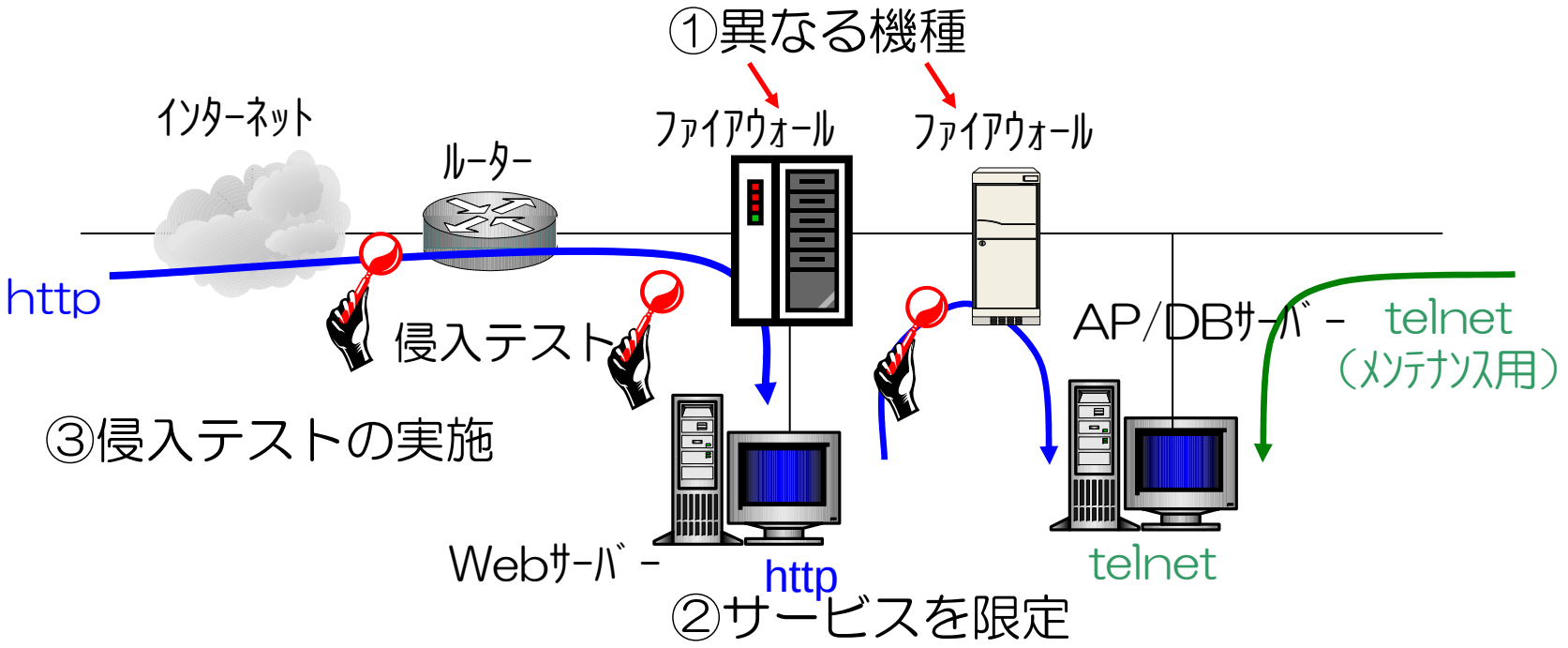
（2）具体的な留意点（2/5）

＜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



（2）具体的な留意点（3/5）

＜犯罪者に狙われやすい建物＞

① 扉は1枚目が破られたことを想定して2枚設置。ただし同じ鍵の扉

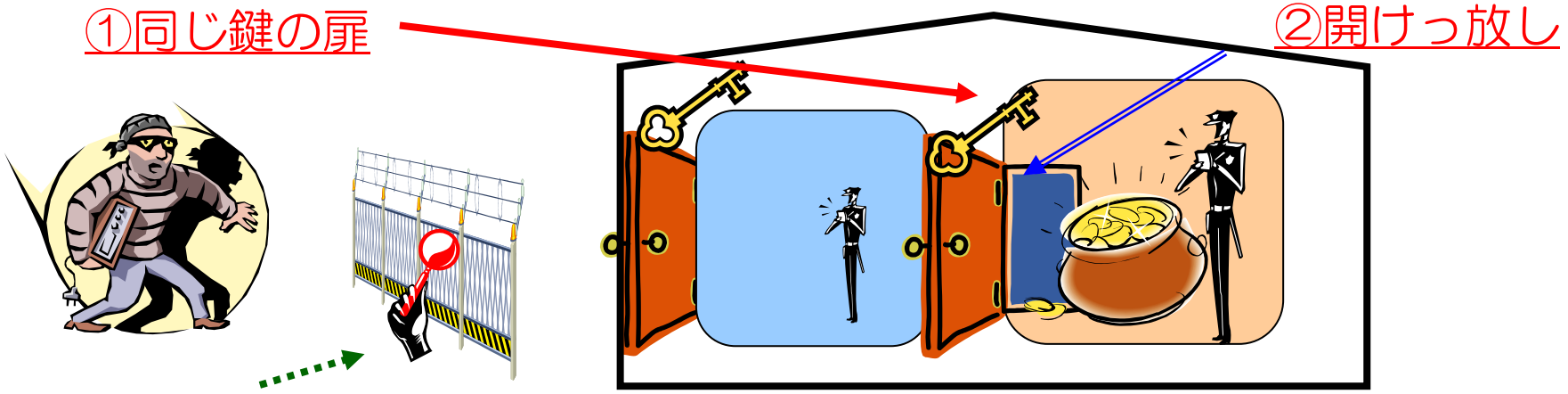
⇒ 同一メーカーから買う方が安価。修理依頼先が1先であるため連絡時に楽

② 内側の扉は開けっ放し

⇒ 警備員は、数時間おきに左側の部屋の安全性も確認する必要。外側の扉が閉まっていることもあり、毎回鍵を開ける手間を省き開けっ放し

③ 外にあるフェンスの信頼性のみ確認

⇒ 殆どの泥棒は、外側のフェンスを乗り越えられないため、ここさえ確認しておけば、全体が安全だと過信



③フェンスのみテスト（これで良ければ扉は要らない・・・）

（2）具体的な留意点（4/5）

＜問題がある構成＞

① ファイアウォールが同一の機種

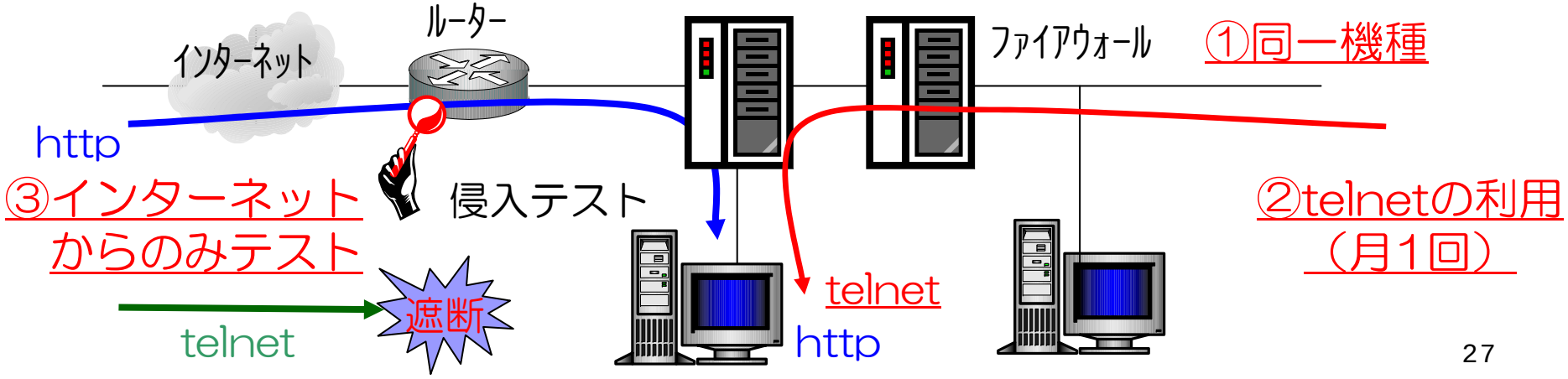
⇒ 構築当初は異なる機種。片方機種のリプレース時に、委託先が維持管理の容易性に重点を置き、同一機種に変更

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



（2）具体的な留意点（5/5）

- IT現場のリスク管理がセキュリティ・ポリシーと乖離する要因

① アウトソーシング拡大により、アウトソース先の運行管理の利便性・容易性を優先した体制となりがちで、かつ金融機関の確認が手薄になっている

② 先進的なシステム技術を取り入れた新規案件を進める中で、既存システムのリスク軽減に関する維持管理作業が疎かになりがち（特に専門的部分は委託先に任せきりになりやすい分野）

終わりに

PDCAサイクルを定期的に実施することにより、
これらの不適切な扱いの殆どは防ぐことが出来る

ご清聴ありがとうございました