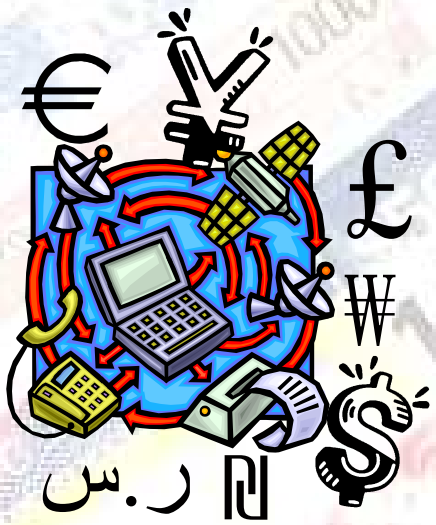
2008年6月28日

第1回ITリスク研究会

パネル「ITリスク学はいかにすれば有益なものとなりうるか」

# 金融業界の立場から

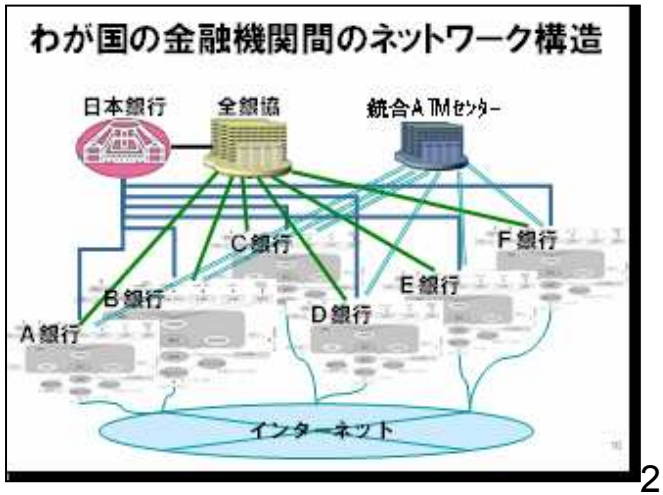


日本銀行 金融研究所情報技術研究センター長
岩下 直行

# 2つのお題

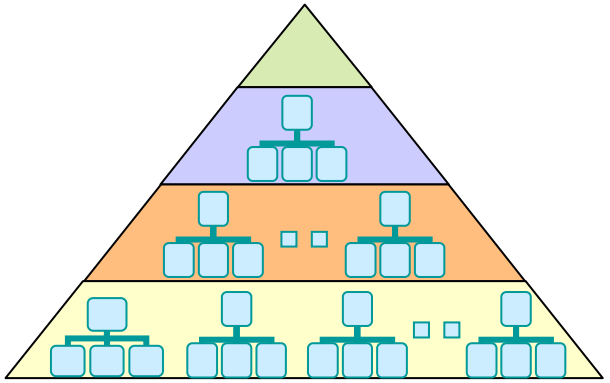
1. ITリスク学のとらえ方に関する意見
2. ITリスク学に期待するもの

## 「金融機関はITリスクの塊」



# 金融情報ネットワークの特徴

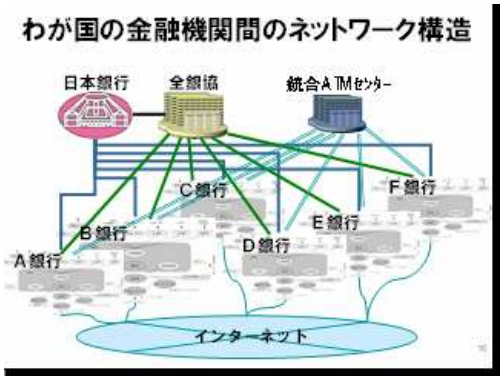
① 各金融機関、集中決済機関によるセキュリティ・ドメイン毎に、分断された閉域のネットワークが構築され、それがピラミッド型に積み重なった構造。



② 通信速度が低速であった時代のシステムの基本構造を継承しているため、通信電文フォーマットは短い固定長を基本とし、できるだけ通信ネットワークに負荷をかけない仕組み。新機能は端末に限定して付加される。

| 項番 | カラム位置 | 桁数 | 項目 |
|---|---|---|---|
| 1 | 1 | 1 | データ区分 |
| 2 | 2～3 | 2 | 持込種別コード |
| 3 | 4 | 1 | コード区分 |
| 4 | 5～14 | 10 | 会社コード |
| 5 | 15～54 | 40 | 依頼人名 |
| 6 | 55～58 | 4 | 振込指定日（月日） |
| 7 | 59～62 | 4 | 仕向金融機関コード |
| 8 | 63～77 | 15 | 仕向金融機関名 |
| 9 | 78～80 | 3 | 仕向店舗コード |
| １０ | 81～95 | 15 | 仕向店舗名 |
| １１ | 96 | 1 | 依頼人預金種目 |
| １２ | 97～103 | 7 | 依頼人口座番号 |
| １３ | 104～120 | 17 | 空きエリア |

③ 外部接続先を（主として）金融機関に限定することによって、セキュリティ侵害のリスクを低下させ、万一問題が発生した場合の責任分担を明確にしている。逆に、一般利用者との接続による新しいサービスの提供には不向き。



# 金融機関における可用性への高い要請

## バックアップセンターの保有状況

（単位：%）

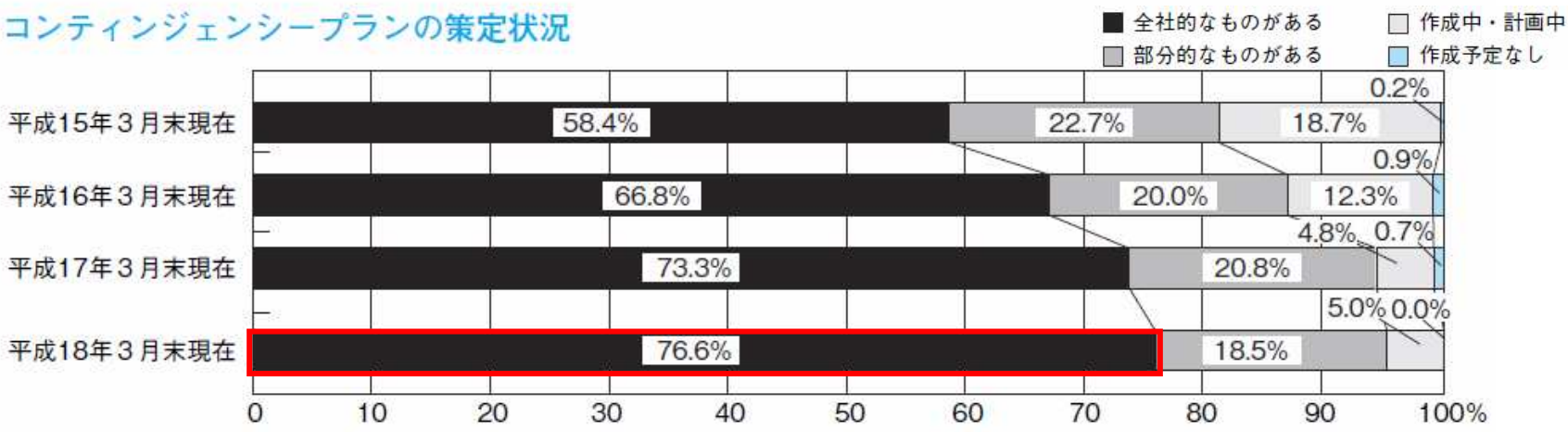
| | 実施済 | 一部実施 | 計画・検討中 | 未実施 |
|---|---|---|---|---|
| 平成11年３月末 | 39.9 | | 14.8 | 45.2 |
| 平成13年３月末 | 41.4 | | 13.7 | 45.0 |
| 平成15年３月末 | 41.6 | 3.6 | 16.3 | 38.5 |
| 平成17年３月末 | 52.9 | 6.3 | 16.3 | 24.5 |

## 本部・営業店等における自家発電設備の設置状況

（単位：%）

| | 実施済 | 一部実施 | 計画・検討中 | 未実施 |
|---|---|---|---|---|
| 平成11年３月末 | 26.1 | 37.2 | 5.3 | 31.4 |
| 平成13年３月末 | 31.9 | 39.3 | 3.3 | 25.5 |
| 平成15年３月末 | 32.9 | 40.9 | 2.5 | 23.7 |
| 平成17年３月末 | 37.2 | 42.9 | 1.9 | 18.0 |

## コンティンジェンシープランの策定状況




（資料）金融情報システムセンターによる金融機関へのアンケート調査

# システム障害のリスク…昔からあったリスク

・1984年11月　世田谷電話局ケーブル火災事件
・1985年11月　バンク・オブ・ニューヨーク事件
・2002年4月　みずほ銀行システム統合時のシステム障害
・2005年11月　東京証券取引所の）障害による取引停止

金融機関のシステムの可用性に対する極めて高度な要求
　⇒事前テストを更に充実させて障害発生率を下げるべきか？
　⇒テストをどこまでやれば適切か？　その基準は？
　⇒むしろ、金融機関のシステムの技術革新を阻害している面も
（それが将来的にはもっと大きなリスクに繋がる惧れも）

# セキュリティ侵害のリスク…最近認識されたリスク

・偽造カード問題
・インターネット・バンキングのセキュリティ
・個人情報保護

キャッシュカードの「絶対的な安全」を求める声
⇒利用限度額の引き下げ…利用者の利便性を犠牲にしている面も

インターネット・バンキングの認証方式の変遷
⇒かつては過度に複雑な認証手順を要求し、全く普及せず
⇒ベーシック認証のみのサービスが普及するも、攻撃対象に
⇒被害を避けるために高度な認証方式に移行

個人情報保護のための厳しい内部規定
⇒ある程度は必要な反面、業務遂行の効率性を阻害している部分も

# どんな議論が必要とされているか

- 今の対策は足りないのか、行きすぎなのか/その評価の軸はどこに置くべきなのか
- 現実には、システム障害をゼロにすることはできないので、「起きてしまった時、どうするか」というアプローチが大切。

  ⇒RTGS、DVP、コンチプラン、BCP/BCM、責任分解点
- 以前は、有効な対策が普及していなかったこともあって、「対策を講じましょう」と言っておけば大体正しかった。
- しかし、実際に様々な対策が講じられるようになり、対策の妥当性や効果が検証可能となると、最適解を求める努力が必要になる。
- 対策のコスト、対策を講じなかった場合のコストを正確に見積もって比較

  ⇒定量化された、科学的な分析が必要とされている

  ⇒例えば、「社長が謝罪するコスト」をどう見積もればいいのか？

# ITリスク学に期待するもの

- 「障害対策、セキュリティ対策をしましょう」というプロバカンダはいらない
- 開発部門が「なぜその対策を講じることが必要なのか」を説明するための材料を提供できないか
- 実際のシステムで選択されている対策について、ITリスクとの対比で、不足／過剰を判定する分析ができないか
- 「望ましい対策」を押し付けるのではなく、利用者側の事情を組み入れて、より良いソリューションを探索するモデルは作れないか、その場合、達成水準に対する客観的な評価をどう組み合わせるか
- システム・インテグレーションにおけるセキュリティ・マージンの取り方と、各要素技術の脆弱化との関連
- 「学際研究の罠」に嵌らないために