金融ビジネスにおける
情報セキュリティのあり方について
－偽造キャッシュカード問題に関する
スタディグループ最終報告書を足がかりに－

金融庁総務企画局企画課
金融研究研修センター　研究官
杉浦　宣彦

わが国の金融犯罪の現状と変化

・偽造キャッシュカード被害の急激な増加

‘02年　3件 → ‘04年（4－12）　307件

（13百万円）　　（807百万円）

キャッシュカード使用に不安を感じる人　　約90%

過去のカード犯罪との違い（＝クレジットカードとの違い）

預金者が被害に遭い、補償されないという性格。

・隠しカメラ等によるカード番号や暗証番号の盗撮

マクロミル社　のネットリサーチ結果（2005年2月）

・カードIDの悪用・偽造カードの被害額　年間200億円強

→ 大きな社会問題になる原因・・・。

原因はなにか？

・磁気ストライプカードの脆弱性

技術進歩で偽造が容易に。 4桁暗証番号（利用者の設定・管理の問題＋銀行システム外部への漏洩）

ICカード化やバイオメトリクス認証の導入検討が必要か？

→ 1990年代より指摘が…（松本・岩下「金融業務と認証技術」『金融研究』19巻別冊1号）

・システムの見直しの遅れ

業界全体の基本インフラ変更のコンセンサスが得られなかった。不良債権問題等、別問題が優先課題に…。情報セキュリティ対策が不十分に・・・。

・犯罪の国際化

ATM関連の犯罪は、欧州で多発しているケースに類似してきている。

金融庁の対応

2005年2月22日　『金融庁偽造キャッシュカード問題に関する金融庁の対応』
「偽造キャッシュカード問題に関するスタディグループ」スタート。
延べ19回の会合
対象：偽造カードから盗難カード、最終的には、情報システムセキュリティの問題までカバー。

2005年6月24日　最終報告書

―偽造・盗難キャッシュカード被害発生の予防策
・被害拡大の抑止策を中心として―

（1）顧客サービスに直結する事項

所持認証・記憶認証・生態認証・利用限度額の引き下げ・顧客対応

（2）主として金融機関サイドで取り組む事項

セキュリティ対策、防犯基準（対策）、被害の早期発見、暗号化、被害の偽装対策

（3）監督サイドで取り組む事項

わが国の金融ネット犯罪の現状
ーインターネットバンキングによる犯罪

- フィッシング詐欺

・利用者層の拡大
・個人情報の漏えい（カードとの違い）
・保険の適用なし

犯罪件数増加・被害拡大

わが国における予防策等の状況
ー情報セキュリティ対策

- **システムに関する各種基準の制定**

ICカード仕様，ATMの設置等に関する基準

システムセキュリティの安全基準

- **電子認証への関心の高まり**

▪「偽造キャッシュカード問題」＝「金融機関の認証システム」の問題のひとつ

・「認証の安全性」、「システムコスト」、「金融取引のリスク評価」、「消費者保護」、これらを含めた「認証システムのベストプラクティス」を考える必要性が…。

・わが国の金融業界をめぐるコンピューターシステム・ネットワークのあり方を再考する必要性があるのではないか・・・

わが国における予防策等の状況
－法律面における状況

- 刑事法

・電磁的記録不正作出罪（刑法161条の２）
・「支払用カード電磁的記録に関する罪」（刑法163条）
・「電子計算機使用詐欺罪」（刑法246条の２など ）

→　情報システムへの脅威に対する事前抑止効
×　損害が発生した場合の事後的救済

わが国における予防策等の状況

－法律面における状況

- 民事法
  - ・預金過誤払いをめぐる一連の判例
    - → 民法478条　約款法理
      - ＋弁済者＝金融機関の注意義務違反
  - ・預金者保護法の成立
    - → 適用範囲の制限
      - × 通帳，インターネットバンキング

金融ビジネスにおける
情報システムセキュリティのあり方

＜金融機関の採るべき防止策として考えられるもの＞

- **顧客への啓蒙教育**
- **技術的対応**
  送信者Webサーバー認証の採用
  異常取引検知システムの導入　等
- **組織的対応**
  全社的防止・発生時対応チームの組成
  偽サイトの調査・モニタリング
  情報の他金融機関・業者との共有
  大口資金移動制限　等　　etc.…

- インターネットサービスの利便性の低下に
- 画一的メニューでは顧客ニーズに対応×

セキュリティ・レベル × 利便性

組み合わせを数種類用意

Ex.大口決済：セキュリティレベル高

小口決済：利便性優先

- 顧客に選択してもらうことが必要

- 金融機関にとって認証は預金者等の顧客に信頼の高いサービスを行うために非常に重要な役割を果たすもの。
  - ー「認証システム」の信頼は、「金融機関」への信頼につながる
  - ー「偽造キャッシュカード問題」 -> 金融機関の信頼の低下
- 金融機関の認証のベストプラクティスを確立するための「ガイドライン」「フレームワーク」の整備の必要性
  - ーCD/ATM、窓口での認証、オンラインバンキング、etc…
  - ー金融機関の認証システムのToBeモデルの策定

認証の保証レベル(or認証の強度のレベル)、金融取引のリスク評価、
消費者保護(補償制度)を含む包括的な情報セキュリティガイドライン
策定が必要なのではないか・・・。

金融機関の（認証システムを含む）情報セキュリティ・システム全体の問題

偽造キャッシュカード問題

補償問題
- 責任負担
- 被害者成りすまし
- 預金者のカード管理努力

セキュリティ対策のためのコスト
- 預金額や取引内容に応じた対策
- 認証強度のバランス
- ATM回線のセキュリティ

利便性と認証技術
- 耐タンパ性
- 相互運用性
- 暗証番号(認証）の強度

盗難キャッシュカード
盗難通帳への問題

オンラインバンキング等
における犯罪の問題

・・・・等々

- 金融機関の認証のベストプラクティスを確立するための「ガイドライン」「フレームワーク」の整備の必要性
  - CD/ATM、窓口での認証、オンラインバンキング、etc･･･についてのルールの策定。
  - 認証の保証レベル(or認証の強度のレベル)、金融取引のリスク評価、消費者保護(補償）制度、これらのトータルなガイドライン（事務ガイドラインへどう織り込むか）
  - 金融機関の認証システムのありかたとその水準

    ＝金融機関の情報セキュリティマネジメントのあり方はどうあるべきか
    効率化のためのシステムからセキュリティと組み合わさった新しい
    ビジネスモデル　のシステムへ

「認証システム」の信頼＝「金融機関」への信頼につながる

何をすればよいのか？

現状：①過去の検討・研究実績の再検討
②認証制度への認識の高まり
③各金融機関のシステムへの投資が上昇
している（特に安全対策）。

しかし、①どこまでやればいいのか？、②　どのように導入するのが一番効率的なのか？という疑問が・・・。

- 金融機関の情報セキュリティ対策のあり方
  - ・情報システムセキュリティ担当のチーム組成
  - ・顧客・他金融機関・大手ネット会社企業等との協力態勢の構築
  - ・偽サイト・フィッシングメール等のモニタリング態勢の整備等
- 金融監督面から…

  決済の安定性・決済リスク・

  システムの安定性をどう見るか

- 法律面から
  - ・責任分解点の明確化
    - ー決済システムのアウトソース化（ブラックボックス化）が進行＝情報の非対称性の発生
    - ーどこまでが誰の責任範囲なのか？
    - ー事故発生時のリカバリーはどうするのか？危機対応策は？
  - ・事故発生時の顧客との責任関係の分析が必要

適切な情報システムとセキュリテイを構築するには？

①包括的なセキュリティプランの提案の必要性

- 金融機関の実務とあった運用しやすい、部分的ではなく、包括的なセキュリティ対策が必要。
- 各金融機関のレベルに適合しているのか
- 最終利用者にもわかりやすいもの。
  （リスク管理サイクル原則の公表）

②システムの認証・監査も必要なのではないか

電子認証の活用＋認証機関をさらに誰がそのレベルを検査・確認するのか・・・。

＝金融機関のみならず、電子商取引全体の安全性をどう担保するのか・・・。