2005年度　JESAP　電子署名・認証フォーラム

金融取引の電子化と認証の問題

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

金融取引と認証

金融取引と認証のつながりは古くて新しい問題

（1）従来の認識と転機

従来から金融の世界では電子認証システムは多用されてきた。　（例：インターネットバンク、貿易金融など）

←― 重要性の認識は薄い傾向があった。

＜背景＞

金融関連システムは、クローズな世界という考え方

暗号化、電子署名も同様・・・。

しかし、この１年で大きな変化が・・・

偽造キャッシュカード問題が大きな転機に・・・

－偽造キャッシュカード問題の原因（システム・技術関連）

①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）

②システムの見直しの遅れ

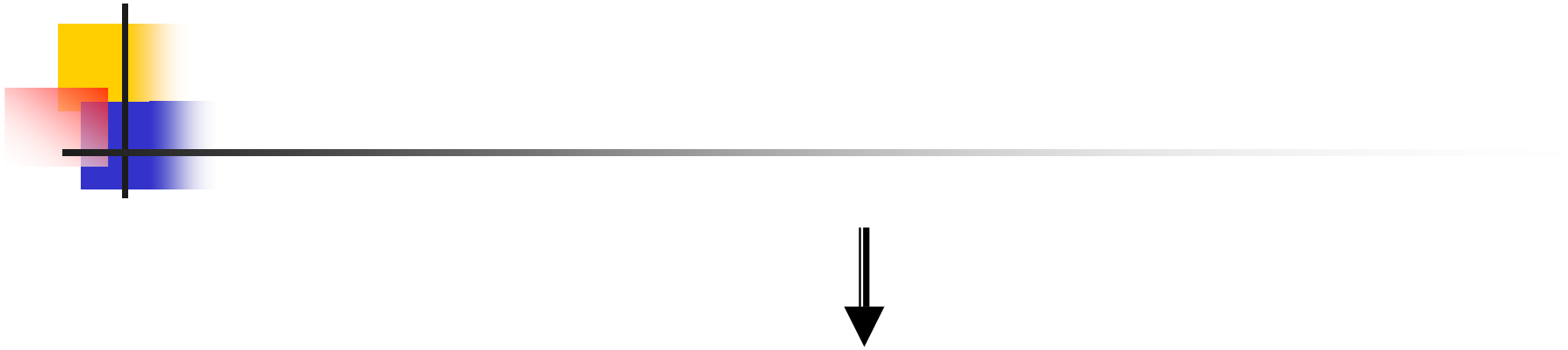
業界全体の基本インフラ変更のコンセンサスが得られなかった。
不良債権問題等、別問題が優先課題に…。

（２）新しいビジネスモデル登場の可能性

－電子債権法の検討（IT政策パッケージ2005等）

売掛債権譲渡や手形利用の場合の欠点の克服、インターネットを利用することで、多様な参加者がどこからでも参加できる技術革新を反映したサービスの提供、電子債権原簿の書き換えでの対抗要件の付与。

→電子データの受渡しの段階で電子認証サービスが必要。



- 「偽造キャッシュカード問題」は現在の「金融機関の認証システム」の問題のひとつ。
- 「電子債権構想」は、金融取引における電子認証の新たなニーズへつながる可能性。
- 「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機会なのでは・・・

認証とは何か

・利用者確認情報

検証者が利用者の主張する身元の検証をする際に利用する情報

認証はその情報を検証する作業。

例：キャッシュカードでは利用者（＝預金者）の検証を金融機関、CD/ATMが行なう。インターネットバンク・サービスであればユーザー番号、ID番号の組み合わせ。

・認証の3要素　－　「利用者確認情報」の3つの要素

- **記憶認証**
  暗証番号等による認証
- **所持認証**
  キャッシュカード本体の所持
- **属性認証（生体認証）**
  指紋、顔、静脈、虹彩、etc…
- 複数の要素を組み合わせた認証（**2要素認証、多要素認証など**）

認証システムの変遷
ーキャッシュカードを例に

（1）磁気ストライプ型キャッシュカード （従来型）

・元々は「記憶による認証」「所持による認証」の2要素認証

⟶ 簡単なスキミング、容易な偽造

「所持認証」の原則が成り立たない状況

・「記憶による認証」の暗証番号

漏洩に預金者が気づかない＋通帳ベース＝届出の遅れ

–> 「偽造キャッシュカード」問題の深刻化に・・・

・発行済み磁気ストライプ型キャッシュカード（3億枚程度）の問題

即日に全てのカードを他のタイプ（ICカード等）へは不可能

現在の「磁気ストライプ型キャッシュカード」を前提とした対策が必要

基本的には、限度額の引き下げが有効策？

「磁気ストライプ型キャッシュカード」＝「低い保証レベルの認証」のみを提供するという位置づけ、認証レベルと限度額の相関関係

（2）ICカード型キャッシュカード

・偽造が極めて困難
　「所持による認証」の確立
　秘密鍵を取り出せない構造（耐タンパ性）
・カードと暗証番号の適切な管理が必要
　磁気ストライプ型と同じ問題。カード紛失・盗難時の速やかな届出が重要。
・ICカード型キャッシュカードへの移行への問題点
　①コスト負担の問題
　②互換性のための磁気ストライプ・ICカード共存の問題
　③認証のタイプのより限度額も別々にするという考え方も？
　　＝保証レベルと限度額の整合性

（3）生体認証とICキャッシュカード

- 金融機関側が「生体認証情報」持つやり方
  ＝「生体認証情報」（顔、虹彩、指紋、静脈など）をデータベース化する方式
- Match-on-Card (MOC) モデル
  ＝ カード上に「生体認証情報」、カード内で比較検証
  金融機関は利用者の生体認証情報を直接持たない形式。
  現在の生体認証対応ICキャッシュカードはこれが多い。
- 「生体認証対応キャッシュカード」に対するセキュリティ基準不在
  ＋ 異なる金融機関のCD/ATMでの利用の問題（互換性）

⟶ 客観的なセキュリティ評価のための基準とが必要
現在は、標準がない。相互運用性の問題。

金融機関の認証システム
認証のベストプラクティスの検討の必要性

- **認証のベストプラクティス 策定の必要性**
  - ー磁気ストライプとICカードが並存する現状においてのベストプラクティス
  - ーICカードを前提としたベストプラクティス
  - ーATM以外の様々な認証を考えたベストプラクティス
  - （例）銀行窓口取引、デビットカード、インターネットバンキング、etc…
- **検討範囲**
  - ー 認証の保証レベルもしくは、（or認証の強度のレベル）
    既存のシステムも含めた認証システムの保証レベルを評価する。
  - ー金融取引のリスク評価
    - ・金銭的ロス、機密情報（暗証番号、生体情報）の漏洩、などの観点
    - ・金融取引のリスクに応じた認証の保証レベル
      ＝高い限度額の口座は高いリスクを伴う
  - ー利用者消費者保護(補償制度)
    - ・認証システムでカバーしきれないところを保険などで補償
    - ・利用者が負うべきリスクを認識してもらう＝リスクの移転

まとめ

- 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。
  - 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」やスパイウエア問題
    - –> 金融機関とってのレピュテーショナルリスクに
- 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においてあるべきモデルの策定

↓

認証の保証（＝強度）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の必要性

（『偽造カード問題に関するスタディグループ最終報告書ー偽造・盗難キャッシュカードの予防策・被害拡大の抑止策を中心として』（H17年6月）参照）