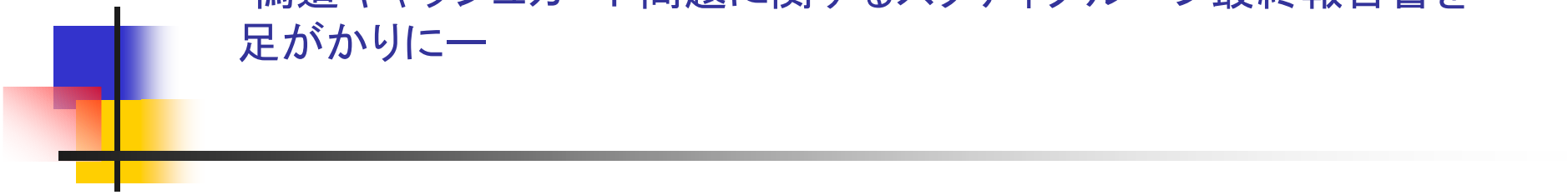
シンポジウム『バイオメトリクス最前線』 2005年10月4日
パネルディスカッション『金融機関のバイオメトリクス技術とその課題』

金融取引におけるバイオメトリクス認証のあり方について
ー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ー



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

金融取引と認証の問題は古くて新しい問題

―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）が重要性の認識は薄い傾向。

＜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・・・。

不良債権問題優先 → システム見直しの遅れ。

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や新しい電子金融ビジネスモデル

（例：　電子債権など）の検討が大きな転機に・・・

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**）

金融取引における認証システムの変遷
－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）バイオメトリクス認証と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。
- 生体認証データは究極のプライバシーの1つ
  同じようなものが複数存在しない＝認証としては高いレベルを保てる可能性＋暗証番号をめぐる問題も消える可能性も

金融機関におけるバイオメトリクス認証のあり方

様々な論点の検討が必要

・バイオメトリクス認証は生体情報という究極の情報を利用したもの

生体情報はセンシチブ情報（「個人情報保護ガイドライン」）
漏洩が発生すれば金銭以上の害の発生も？
また、バイオメトリクス認証は万人をカバーできない。
（例：身障者問題等）

・異なる金融機関が異なる方式の生体認証をしている現状

CD/ATMの相互利用に問題が・・・。（互換性の問題）

・技術の標準化がなされている段階ではない。

世界的な技術の標準化が行われていない。
欧米では、バイオメトリクス認証は、時期尚早の認識も…。

・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の必要性

－ICカードを前提としたベストプラクティスとは？

－ATM以外の様々な場面での認証も考慮に入れる必要性がある。

（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、
その他、金融以外の目的での利用　etc…

・より幅広い検討の必要性

－ 認証の保証（もしくは強度）＋既存のシステムも含めた認証システムの保証レベルや評価基準の確立が必要なのでは？

－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

－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する制度

・利用者が負うべきリスクの認識＝説明義務

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。
　　―「認証システム」の信頼は、「金融機関」への信頼につながる
　　―「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回避のために
　　＝認証が必要であるという認識は確立したのではないか・・・。

・ バイオメトリクス認証は有効な手段の一つ。
しかし、プライバシー、相互互換性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」の必要性、技術の標準化についてのさらなる検討が必要なのではないか

・ 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―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）