偽造・盗難キャッシュカード事前予防策　議論の整理

Ⅰ．犯罪防止策一般

〔基本的な留意点〕

- 顧客のニーズを踏まえながら、利便性と安全性のトレードオフの関係に配慮した対応策をとることが必要。
- 取引金額に応じて、求められる本人認証のレベルは異なるべき。現在の本人認証レベルは現状の高額な取引限度額に見合っていないのではないか。
- セキュリティ対策の有効性、脆弱性を客観的に評価する仕組みを構築すべきではないか。
- 個別のセキュリティ対策の検討に加え、当該金融機関のシステム全体や金融機関間のネットワークのあり方についても検討されるべきではないのか。
- 直ちに取り組むべき課題、中期的に取り組むべき課題、長期的に目指していく方向性に分けて整理を行うべきではないか。

Ⅱ．個別の犯罪防止策

〔暗証〕

- 照合のシステムとしては、4 桁の数字はハードルとして機能しない場合が存在するのではないか。
- 数字以外に「英字」、「かな」、「カナ」の使用は、効果があるのではないか。
- 暗証の桁数を増やしたり、カードごとに異なる暗証を求めたりするのでは、一般の預金者が記憶できず、過大な要求となるのではないか。
- 高齢者の場合は、生年月日、電話番号などを使用することはやむをえないのではないか。
- カード内に暗証番号のある古いカードは、ＡＴＭで受け付けず、窓口誘導としてはどうか。

〔カード〕

- カードのセキュリティ評価を行うべきではないか。
- 磁気ストライプカードについて、有効期限を設けるべきではないか。それにより、期限ごとのセキュリティのグレードアップとカード送付

の際の本人確認が可能になるのではないか。

- 全国銀行協会において、ＩＣキャッシュカードの仕様を制定・管理しているが、同様に、磁気ストライプカードの標準仕様についても、いずれかの主体が管理・策定し、セキュリティのグレードアップを図るべきではないか。

  （注）磁気ストライプについては、物理的仕様がＪＩＳ規格となっているものの、搭載するデータ内容について、規格を管理し、改良する主体が不存在。
- キャッシュカードを交付する際には、あらかじめ預金者に対してカードを保持することのリスクや預金者として尽くすべき注意義務の内容を説明することが必要ではないか。
- 偽造キャッシュカード対策として有効なＩＣカード化（ＩＣカード対応ＡＴＭの普及を含む）を推進すべきではないか。
- ホワイトカードのチェックはＡＴＭで行うべきではないか。

〔生体認証〕

- 生体認証は第三の認証の仕組みとして、偽造及び盗難キャッシュカード被害ならびに被害偽装を防止する上で有効な対策ではないか。
- 生体認証は、技術としては成熟過程にあり、認証制度評価、装置のセキュリティ評価、運用基準等が不十分ではないか。特に第三者による客観的評価が不足しているのではないか。また、センシティブ情報の保護、認証方式やネットワーク上の通信方式の標準化、ユニバーサル・デザイン対応（本方式を利用できない特定の病気の方への対応を含む）等の問題について検討すべきではないか。
- ＩＣキャッシュカードと同様の標準仕様を生体認証についても策定すべきではないか。

〔ＡＴＭ及びその周辺における防犯措置〕

- 覗き見や盗撮等による暗証番号漏洩を防止するための措置について、何らかの防犯基準を設定すべきではないか。
- 防犯ビデオについて、その設置方法、保存期間、画質等について何らかの防犯基準を設けるべきではないか。
- 期限を設けるなどしてＩＣカードに対応したＡＴＭの普及を推進すべきか。生体認証に対応したＡＴＭについてはどうか。
- コンビニＡＴＭにおける防犯対策をどのように講じていくか。
- 無人店舗におけるＡＴＭの丸ごと盗難時の対応として、取引記録情報

の保護対策（暗号化、丸ごと盗難を感知しログ情報の自動消去）は十分であるか。

〔利用限度額の引き下げ〕

- 偽造及び盗難キャッシュカード被害を抑制するためには、利用限度額の引き下げが明確な即効性を有する方法ではないか。

〔被害の早期発見〕

- 異常取引の検知システムを早期に導入し、被害額を抑制することが求められているのではないか。
- 商品との関連付けが可能なクレジットカードに比べ、異常取引検知は難しいとの意見があるなかで、金融機関としてどのような異常取引検知の取組みを講ずるべきか。
- 預金者による被害の早期発見を可能とする仕組み（ステートメント方式への移行、電子メールによる個別取引の通知など）を検討すべきではないか。

〔暗号化〕

- 現在、ＡＴＭシステムにおいて、金融機関が採用している「暗号」（暗号アルゴリズム及び暗号に利用する鍵の管理）は国際基準に照らして十分なものといえるか。
- ＡＴＭ、ホストコンピュータを結ぶ専用線の使用に加え、暗号化は必要ではないか。

〔被害の偽装対策〕

- 被害の偽装を防止するため、
  - 保険における不正請求等防止制度と同様の制度を検討すべきではないか。
  - 被害の偽装を疑う合理的な根拠がある場合、預金者による警察への被害届の内容について、金融機関が警察に照会できる仕組みを構築するなど、被害偽装防止策について、警察・金融機関間の具体的協力関係を検討し、何らかの取り決めを締結すべきではないか。
- 偽装常習者の発見のため、盗難補償の実績の情報交換を金融機関間で行うことは有効か。その場合、個人情報保護の観点からの問題はクリアーできるのか。

- 利用限度額の引き上げを顧客に選択させた場合、偽装された被害が大きくなる可能性があるが、これをどのように防止するか。
- カード券面の偽造防止といった点にも留意すべきではないか。

Ⅲ．当局側の対応

〔金融庁の対応〕

- 金融機関におけるセキュリティ対策については、監督指針において明確に位置付けるべきではないか。
- 統合ＡＴＭや共同システムなど、金融機関外に存在するシステムで、直接に金融庁の検査・監督権限が及ばないものについても何らかの対応が必要ではないか。

〔警察庁の対応〕

- 現行の「防犯基準」については、主として銀行強盗を念頭において作成されているもの。これに基づいて金融機関は防犯対策に努めているが、社会情勢の変化に合わせて、偽造・盗難キャッシュカード犯罪等の犯罪にも対応できるようにすべきではないか。

〔金融システム情報センター〕

- 「金融機関等コンピュータシステムの安全対策基準」（金融情報システムセンター作成）は、金融庁検査において規範性を有していることに鑑み、十分な事項が盛り込まれていると評価できるか。

（以上）