ＡＴＭ-Ｂａｎｋ ＩＴにおけるセキュリティへの取り組み

筒井　良子　　近藤　和洋

近年，ネットワーク技術の発展に伴い，金融機関が提供するサービスが多様化し，預金者の利便性が高まっている。その一方で，これらサービスに使われる技術の裏をつく犯罪が増加している。

ATMにおいても，偽造カードや盗難カードによって，口座にある預金を一斉に引き出す事件が急増しており，犯罪防止策に向けたセキュリティへの関心が高まっている。

本稿では，ATMに求められているセキュリティ環境について述べると共に，今年3月に発表したＡＴＭ-ＢａｎｋＩＴでの取り組みを紹介する。

ATMを取巻く犯罪

以下に金融庁の調査によるこれまでの被害状況を示す。**図1**，**図2**から，偽造カードによる被害が平成15年から急増していることが分かる[1)]。

今までに分かっているATMの不正な引き出しには，主に以下の手口のものがある。

- 預金者がATMを操作するところを盗み見した後で，カードをバッグや財布ごと，引ったくりするなどして盗み，預金者が警察に通報するまでの間に，預金を引き出す。

- 空き巣などで，キャッシュカードと一緒に，運転免許証など個人情報が分かるものを盗み，そこに記載された生年月日や電話番号などから暗証番号を類推し，預金を引き出す。

- 他人のカードデータをスキャンニングしてカードを作成し，ATMで預金を引き出す。

これらの中には預金者本人が，いつカードやデータを盗まれたのか全く気づかないケースも多く，本人が銀行に行って預金残高を確認しない限り，事件が露見しない場合もある。

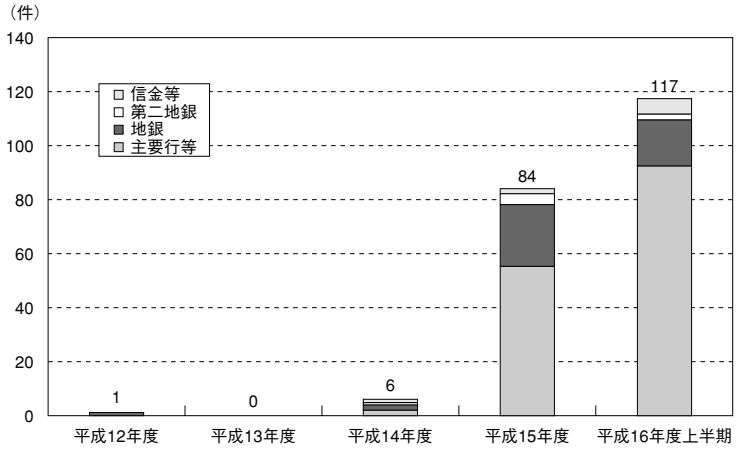

図1　偽造カードによる被害件数推移

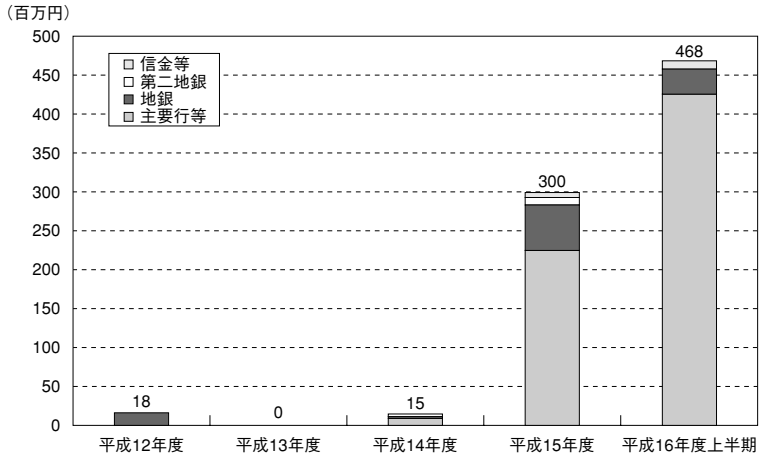

図2　偽造カードによる被害額推移

金融業界での取り組み

これらの事例を受け，全銀協では以下の取り組みを実施している。

- ●偽造が極めて困難なICキャッシュカードの標準仕様を制定
- ●預金者に対するキャッシュカードや暗証番号の取り扱いに関する注意喚起を実施（平成15年～16年）
- ●偽造キャッシュカード被害の補償ルールを決定（平成17年10月）

犯罪に遭った預金者が，暗証番号やキャッシュカードの管理に落ち度がなかった場合に，金融機関が被害額を全額補償することが決められた[2) 3)]。

また，財団法人金融情報システムセンターは，これら犯罪への対策として，2005年4月に，改めて金融情報システムに関する安全対策基準を発表した。

金融庁でも2005年6月の「偽造キャッシュカードに関するスタディグループ最終報告書」の中でATMをはじめとした金融情報システムへの提言を行っている[4)]。それらを受け，金融機関側では以下のような対策を実施しはじめている。

- ●ICキャッシュカードの導入（平成14年～）
- ●利用限度額の個別設定サービス（平成14年～）
- ●利用限度額の引き下げ
- ●ATMでの支払い取り引きの時間帯，場所を預金者が設定できるサービス（平成17年～）
- ●生体認証による本人確認（平成16年～）
- ●異常取り引き検知システム

ＡＴM-ＢａｎｋＩＴでの取り組み

当社が今年3月に発表したＡＴM-ＢａｎｋＩＴ（**写真1**）では，4つの商品コンセプトを基に開発を行った。

① 高セキュリティ化

犯罪の予防対策，犯罪に対する監視強化の観点からセキュリティ機能を充実させた。（詳細は後述する。）

② 高信頼性と運用コストの削減

装置の信頼性を大幅に向上し，長期間の無人運用を実現した。また，紙幣スタッカを大容量化し，現金警送コストの削減に貢献する。

写真1　ＡＴM-ＢａｎｋＩＴ

③ 快適な操作性

光表示機能で操作を誘導する。また，ユニバーサルデザインの思想を取り入れ，障害者，高齢者等にとっての使いやすさにも配慮した。

④ 拡張性と多機能性

今後，非接触ICカードや携帯電話が生活のあらゆる場面で活用されることを想定し，これらと連携したサービスが提供できるよう，専用ユニットの搭載を可能とした。

その中でも，高セキュリティ化は，ＡＴM-ＢａｎｋＩＴで最も注力した分野である。以下に具体的な取り組み内容を示す。

（1）犯罪の予防対策

①カード偽造防止

●ICキャッシュカード

ＡＴM-ＢａｎｋＩＴのハードウェアは，ICキャッシュカードに標準で対応している。ICキャッシュカードは従来の磁気カードに比べ耐タンパー性が高く，カード内のスキミングや不正データの書き込みが困難なため，カード偽造を防止することができる。

●レシートの口座番号マスキング

ATMで発行されたレシートからキャッシュカード内の

データを割り出し，カードを偽造する手口もあると考えられるため，レシートに表示される情報の一部をマスキングし，全てのデータが分からないようにする。

②本人確認の精緻化

●生体認証

ＡＴＭ-ＢａｎｋＩＴでは利用者の本人確認手段として従来の暗証番号に代わり，生体認証技術を利用することが可能である。ＡＴＭ-ＢａｎｋＩＴでは，生体認証の掌静脈認証（**写真2**），指静脈認証，アイリス（虹彩）認証といった3方式に対応することができ，ユーザのニーズに応じて，これらの中から選択することができる。

生体認証は，ICキャッシュカード内に預金者本人の生体データを登録しておき，ATMを使用する際にはそれを読み取るセンサに掌や指，目をかざし，ICキャッシュカード内のデータと照合することにより本人確認を行う。一般的にこれら生体認証技術の誤認識率は0.01%以下と非常に低く，推測可能な従来の暗証番号に比べ，他人が盗んだカードを用いて不正に引き出すことは非常に困難となる。

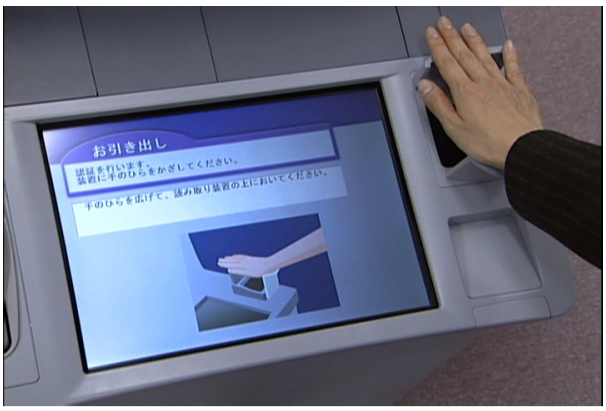

写真2　掌静脈センサでの認証のイメージ

③暗証番号の盗難への対策

●視野角制限フィルタ

ATMの表示画面にその視野を制限する特殊な視野角制限フィルタを設け，後方および横から入力内容（特に暗証番号）を盗み見られることを防止している。

●後方確認ミラー

ATMの前面に90°の広視野角ミラーがあり，操作している間に後ろに不審者がいないかを確認できる。また，犯罪者に対する抑止効果も期待される。

●暗証番号入力キーのスクランブル表示

ATM画面で暗証入力時のテンキーの配列を，取り引きごとにランダムに表示させる。視野角制限フィルタを導入していても，指の動きのみで暗証番号を読み取られる危険も考えられることから，このスクランブル表示のアプリケーションも準備した。

●ATMでの暗証変更機能

暗証番号は，類推や盗み見をされるリスクがあることから，類推されにくい番号に設定すること，また，番号の定期的な変更が望ましい。そのため，ATMの画面でも暗証番号の変更ができるようにした。

●ATMでの注意喚起

暗証番号を類推しにくいものに設定するよう，ATM画面に表示し注意を促す。

犯罪にあった預金者の45.2%が生年月日や電話番号，住所を元にした番号を使用しており[1)]，これらの個人情報から暗証番号を類推された可能性がある。

このため，画面で残高の定期的な確認や暗証番号の変更を呼びかける。あるいは，預金者の暗証番号が生年月日と合致する等の類推しやすいものである場合に，取り引きの都度，注意画面を表示させる。

●暗号化ピンパッド

暗証番号入力の専用キーとして，暗号化ピンパッドを搭載することも可能である。ピンパッドのユニット内部で暗号化をするため，ホストへの通信内容から暗証番号を解析されることを防止する。

④犯罪による高額引き出し対策

●引き出し限度額の変更機能

預金者自身がATM画面で引き出し限度額を変更することができる。引き出し限度額が大きいと預金者が被害に気づく前に，口座の残高を全て引き出されてしまうため，普段引き出しをする程度の限度額に下げることができる。限度額を上げる場合には窓口等での手続きが必要なため，ATMでの変更機能を第三者が悪用することもできない。

(2) 監視機能

①ATMの監視機能

●顧客カメラ

ATM前面の顧客カメラにより，取り引きがある都度，操作者の顔画像を取得することができる。多条件による検索機能と合わせてあり，犯罪性のある取り引き，特に盗難カードや偽造カードによる取り引きがあった場合に，事後の証拠資料となり得る。

●画像監視システム

支店内の監視カメラ画像を，DVRを経由して，センタの映像監視サーバの大容量HDDに記録する。HDDという1媒体による一元管理が可能なため，検索性に優れている。したがって，取り引きのトラブル，また犯罪があった場合にも，迅速な対応が可能である。また，ATMと連携し，取り引きがあるタイミングで画像を取得する機能を持つことができる。さらに，監視カメラの画像の動体解析により，不審人物，不審物を検出し，これらを自動で監視することも可能である。

(3) 24時間顧客対応

沖電気ではATM運用に関する関連会社（日本ビジネスオペレーションズ株式会社）により，ATMの監視業務の受託など総合的なサービスを提供している。専門会社にアウトソーシング委託することにより，24時間体制での顧客対応が可能となり，預金者が口座残高の異変に気づいた場合に早急に連絡を受け，キャッシュカードを無効化することにより被害拡大の防止を行うことができる。

◆◆

■参考文献

1）偽造キャッシュカード問題に関する実態調査結果の概要，金融庁，2005年2月
2）カード規定試案の改正について，全国銀行協会，2005年10月
3）偽造・盗難キャッシュカードに関する預金者保護の申し合わせ，全国銀行協会，2005年10月
4）偽造カード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，金融庁，2005年6月

●筆者紹介

筒井良子：Ryoko Tsutsui. システム機器カンパニー システム機器開発本部 システム設計第二部 ATM SEチーム
近藤和洋：Kazuhiro Kondou. システム機器カンパニー システム機器開発本部 システム設計第二部 ATM SEチーム チームリーダー