2005年12月21日

第10回決済システムフォーラム

――決済における情報セキュリティ向上の現状と課題――

日本銀行　決済機構局　中山靖司

キャッシュカード偽造等問題

預金者保護法における預金者への補償ルール

・　預金者保護法（2005年8月成立 、2006年2月施行は、民法478条の特例として、以下の補償ルールを制定

民法478条「債権の準占有者に対してした弁済は、その弁済をした者が善意であり、かつ、過失がなかったときに限り、その効力を有する。」

▽　預金者に故意・重過失があれば、補償されない（金融機関に立証責任）

▽　預金者に故意・重過失のない場合の取扱い

取引形態　（個人預金者の取引）			新法
カード	偽造		100%補償
	盗難	預金者に故意・過失のない場合	100%補償 （但し、届出前30日間の被害に限定（注1））
		預金者に過失がある場合 （金融機関に立証責任）	75%補償 （但し、届出前30日間の被害に限定（注1））
窓口取引（通帳・印鑑）、インターネットバンキング			新法の対象外（注2）

（注1）　預金者が特別の事情を証明できれば、30日の補償期間は伸長される(最大2年)。

（注2）　附帯決議では、政府、 金融機関その他の関係者は、 以下の事項について特段の配慮をすべきものとされている。

①インターネットバンキングにかかる犯罪等
「速やかに、その実態の把握に努めその防止策および預貯金者等の保護のあり方を検討し必要な措置を講ずること」

②金融機関の窓口における不正な預貯金の払い戻し
「速やかに、その防止策および預貯金者の保護の在り方を検討し必要な措置を講ずること」

金融機関における約款改定の動き

・　新法成立を受けて、全銀協はカード規定試案（約款）を改定。

– 従来の全銀協カード規定試案は、民法478条の適用を前提に、盗難カード被害への補償を否定。また、偽造カード被害補償にも「預金者の無過失」の確認を必要としていた。

・　新しい約款には、補償ルール等、預金者保護法に定められた内容を記載。また、別途、過失や重過失の具体例を提示。

「重過失」の例
- 暗証番号をカード上に書き記した場合。
- 他人に暗証番号を知らせた場合。

「過失」の例
- 金融機関による個別具体的に行われる再三の注意喚起にも関わらず、生年月日等の類推されやすい暗証番号を使用し、免許証等の当該暗証番号を推測させる書類と一緒に盗取された場合。
- 暗証番号を書き記したメモ等をカードと一緒に保管又は携帯し、それらをカードと一緒に盗取された場合。

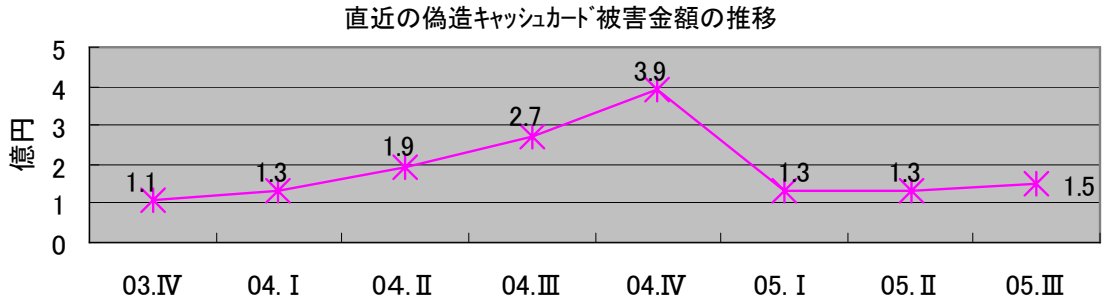
カード犯罪の被害状況

・　偽造キャッシュカードの被害状況（盗難被害に関しては統計なし）

単位：億円

	1997	1998	1999	2000	2001	2002	2003	2004	2005 1～9月
偽造キャッシュカード （件数）	－	－	－	－	0.2 (1)	0.2 (4)	3.0 (108)	9.8 (424)	4.1 (303)
(参考)偽造ｸﾚｼﾞｯﾄｶｰﾄﾞ	12	28	91	140	146	165	164	106	67

※全銀協および日本クレジットカード産業協会調べ



（参考）ﾌﾟﾘﾍﾟｲﾄﾞｶｰﾄﾞの偽造被害総額

ﾃﾚﾌｫﾝｶｰﾄﾞ　数百億円
ﾊﾟﾁﾝｺｶｰﾄﾞ　630億円
ﾊｲｳｪｲｶｰﾄﾞ　数百億円

・　キャッシュカード犯罪は、「特定」の預金者への成り済まし行為である点でクレジットカード犯罪に類似しているが、不正利用による損害が金融機関によって補償されず、一般の消費者（預金者）が直接の被害者となったことが、大きな社会問題となった背景。

金融機関の対応

- ▽ ATM周りの安全対策強化
- ▽ ATMロック（携帯電話によるロック解除指示）
- ▽ ICキャッシュカードの導入
- ▽ 生体認証の導入
- ▽ 利用限度額引下げ
- ▽ メールによるATM利用通知
- ▽ 保険制度の導入
- ▽ 独自のサービス
- ▽ 顧客への安全対策啓蒙
  - ▪
  - ▪
  - ▪

個別行の対応だけでは限界

現在のCD/ATMネットワークでは、ICカードに対するCD/ATMの相互運用性が確保されていない。

＝＞他行のATMを利用した場合、セキュリティレベル（カード種別）に応じた利用限度額の設定が困難。

▽カード種別毎のセキュリティと利便性の現状

	偽造リスク対策	盗難リスク対策	ATM間の相互運用性
磁気ストライプカード	×	△（適切な暗証番号管理が前提）	○
ICカード	○	△（適切な暗証番号管理が前提）	×
生体認証機能付ICカード	○	○	×

▽ある銀行の例　＜１日当たりのATM利用限度額＞

キャッシュカード種別	ATMのタイプ	引出し	振込み
ICカード	ICカード対応ATM（現状は自行ATMの場合のみ）	100万円	200万円
	ICカード非対応ATM	50万円	100万円
磁気ストライプカード		50万円	100万円
（参考） 以前		500万円	500万円

※1　ICカード非対応ATMでは、ICカードもすべて磁気ストライプカードとして取り扱われる。
※2　利用限度額は、預金者の希望により個別に引下げることが可能。

- 当面は磁気ストライプカードとICカード／生体認証機能付ICカードの並存が不可避。だとすると、以下の2点が喫緊の課題。

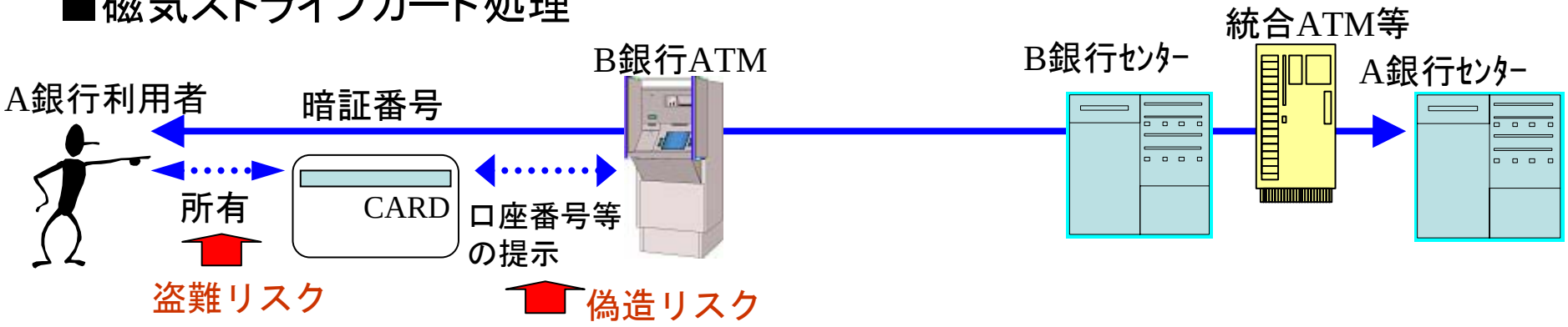
①全国どのICカード対応ATM機が利用されたとしても、ICカードは「ICカード」として認識できるようにすること（その結果、カード種別に応じた限度額の運用が可能となるようにすること）、

②生体認証機能付ICカードにあっても一定の相互運用性を確保すること、

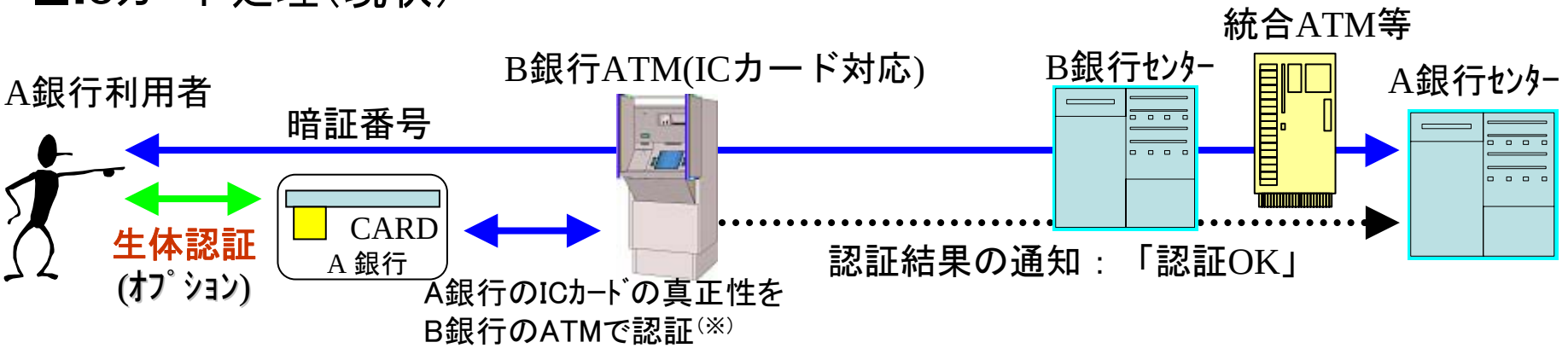
  - その実現によって、個別行レベルでのICカード導入のインセンティブが高まり、金融機関全体としてICカードの普及が図られることを期待。

キャッシュカードの認証処理

■磁気ストライプカード処理



■ICカード処理（現状）



（※） 暫定的な措置であり、将来的には、A銀行のICｶｰﾄﾞの真正性は、A銀行ｾﾝﾀｰで認証する予定（2011/4月以降）

インターネットバンキングを巡る問題

現実的な脅威となりつつあるPhishing

最近増加しつつある犯罪事案

①「キーロガー」ソフト

- 不特定多数の人が利用するインターネットカフェのパソコンに、利用者の操作履歴を記録する「キーロガー（key logger）」ソフトが仕掛けられ、盗まれたIDとパスワードを使って資金が不正に引出された＜03年2月＞。

② スパイウェア

- インターネットバンキングを利用する顧客のパソコンが、電子メールで送られてきた不正プログラム（スパイウェア）に感染。ID等を盗まれ、複数行の顧客の資金が別の口座に不正に振り込まれた＜05年7月＞。
- その後、法人顧客当てに、スパイウェア入りのCD-Rを送りつける犯罪も．．．

③ フィッシング

- 実在の金融機関名等を騙って、ID等の入力を促す内容のフィッシングメールが不特定多数の顧客に送付された＜04年11月-05年7月＞。

海外ではサービス停止の被害も

- 海外では、フィッシングによってアカウント情報を詐取した攻撃者に，口座にアクセスされることを防ぐため、オンライン・バンキングのサイトを一時的に閉鎖した例も。

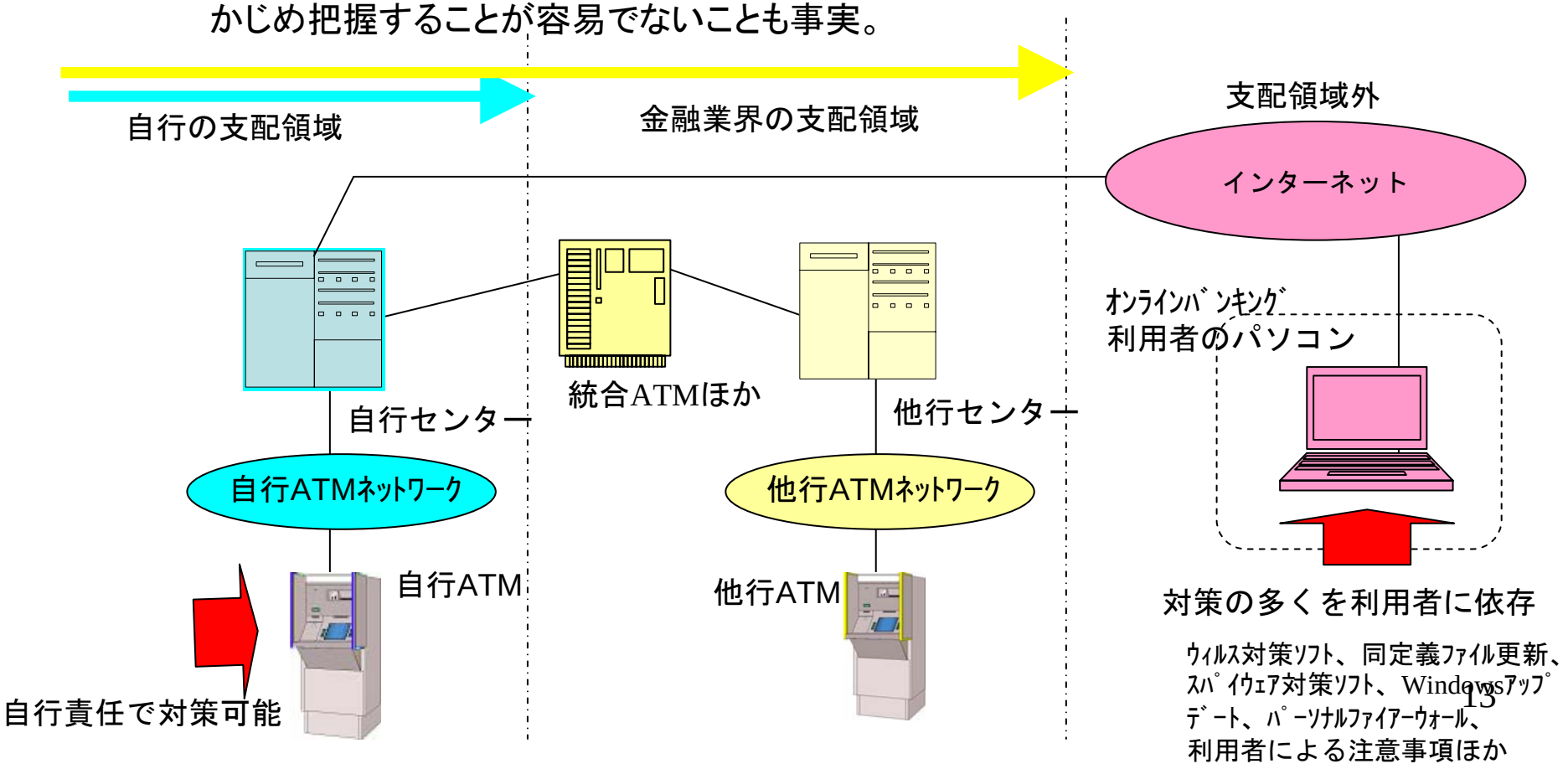
2003年12月　A銀行（英）
2005年10月　B銀行（ニュージーランド）
2005年10月　C銀行（スウェーデン）

——紙に印刷されたﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞが標的。

インターネットバンキングの特殊性（1）

① 利用者のパソコンを取引端末としているため、金融機関が行える対策に限界。最終的には利用者のITリテラシーに依存（実際には、リスクの存在に対する認識が不足）。

– 技術進歩が速いために、利用者にとって、リスクを生み出す罠やリスクの規模をあらかじめ把握することが容易でないことも事実。



インターネットバンキングの特殊性（2）

② フィッシング自体を取り締まる法律が未整備。

– 警察庁では、詐欺/窃盗に至らない段階（偽のホームページの開設等）で、防止、検挙することが何よりも重要とし、フィッシング行為自体を業務妨害罪、著作権法（複製権侵害、公衆送信権侵害等）違反等で検挙するよう努める方針を発表（2004年12月）。

> 警視庁ハイテク犯罪対策総合センターは、インターネットサービス会社「ヤフー」のＨＰを勝手に複製し、会員のパスワードなどを入手するフィッシング詐欺を行っていた大阪市の会社員（42）を、著作権法違反容疑で逮捕した。同センターによると、フィッシング詐欺事件の摘発は全国で初めて。

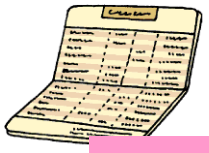
③ 一方、インターネットバンキングは、全預金者向けの標準サービスではなく、利用者の意思に基づいて提供されるサービス（ネット専業銀行等は例外）。

（参考）国内関連法令による検挙の可能性

②偽ホームページの開設
（著作権法違反、不正競争防止法違反、業務妨害罪？）

①架空名義口座開設or購入
（改正本人確認法違反）

被害者口座



架空名義口座

ATM

⑤不正な資金移動指図
（不正ｱｸｾｽ禁止法違反、
電子計算機使用詐欺罪）

ID,PassWord

④ID、ﾊﾟｽﾜｰﾄﾞ等の不正入手
（？？？）

被害者

犯人

⑥現金引出し
（窃盗罪）

③偽ﾎｰﾑﾍﾟｰｼﾞへの誘導ﾒｰﾙ送信
（業務妨害罪、電子ﾒｰﾙ送信適正化法違反？）

これまでの金融機関の対応の例

▽利用者の啓蒙

- 各金融機関のホームページ上での注意喚起。

▽セキュリティ対策の強化

- 【事前対策】 本人認証の強化
  - 乱数表を使ったパスワード入力、画面に表示されたキーボードをマウスで選択してパスワードを入力する仕組み（ソフトウェアキーボード）の導入等。
  - ただし、こうした対策でもマウスの操作を記録されたり(mouse logger) 、操作時の画面のイメージが漏洩(screen scrapper)すると防ぎきれないため、二要素認証とすることが望ましい（米では連邦金融機関検査審議会<FFIEC>が、2006年末までに二要素認証を導入するよう通告）。
  - IPアドレスによる接続端末の制限ほか
- 【事後対策】 不正の早期検知
  - 前回ログイン時刻の表示、取引結果のメール通知

▽振込み限度額の引下げほか

- １日の限度額を、例えば1,000万円から300万円に引下げ等。
- 振込先を事前登録先に限定。

増えつつあるキーロガー、新たな手口

- 米のセキュリティ企業iディフェンスは11月15日（米国時間）、スパイウエアの一種である「キーロガー」が急増し、05年の発見件数は6200件に迫りそうだと発表 した。前年比では65%増。銀行などがフィッシング対策を強化したため、新しい 手口としてキーロガーが増えているとみられる。

（参考）欧州〇〇銀行の事件

2004年10月、欧州の〇〇銀行で不正アクセスがあり、ロンドン事務所から約2億2000万ポンド（約451億 円）を盗もう という試みがあったことを英国の国家ハイテク犯罪部(National Hi-tech Crime Unit: NHTCU) が明らかにした。

犯行グループ は、清掃員として事務所に入りこみ、スパイグッズのような器具、ハードウェアのキーロガーをキーボードのUSBポートに仕掛けていた。器具は英国で20ポンド （4100円）程度と安価で、見た目にもケーブルと同化して目立たないため、こうした器具が世の中に存在することを知らない人にとっては気づきようがないものであった。

不正にアクセスされた情報は口座番号、パスワードなどの機密情報。同行によれば、10件の口座から世界中の銀行の口座に送金しようとする資金盗難の試みがあったが、犯行グループは送金には失敗したとのこと。

（参考）Hardware Keyloggerの例

①USBケーブルタイプ

②コネクタプラグタイプ

取り付けは、これらの機器をパソコンとキーボードケーブルの間に挟んで繋ぐだけ！

高度化が進む広義Phishing

- Spyware（PC上で操作履歴を取得<keylogger等>）
- Classic Phishing（偽メールや偽Webサイト）
- Pharming（DNSやhostsファイルの改竄）
- Evil Twins（不正な無線LANアクセスポイント）
- Proxy, man in the middle attack（不正中継による改竄）
- Trojan Horses and Malware（PC上で取引指図を改竄ないし勝手に指示等、あるいはリモートアクセス）
- ？？？（現時点では想像すらできない攻撃？）