平成17年4月15日

金融庁偽造キャッシュカードSG
プレゼンテーション

偽造キャッシュカード
問題の現状とその対策

日本銀行 金融研究所
情報技術研究センター長
岩下 直行

日本銀行 金融研究所 情報技術研究センターと偽造カード問題との関わり

情報セキュリティ・シンポジウムによる金融業界の啓発

――1998年から、日本銀行において、金融業界関係者を招いて毎年開催。磁気ストライプカードと暗証番号による認証システムの脆弱性を指摘し、早期にICカードと生体認証の導入を行うべきとの提言を続けてきた。

ISO/TC68国内委員会における標準化活動

――金融分野で利用される暗号技術、ICカード、生体認証等の情報セキュリティ技術を担当する国際標準化機構（ISO）の国内事務局として、国内の金融機関に対し、暗証番号送信時の暗号化の必要性を訴えるなど、情報セキュリティ対策に関する啓蒙活動を続けてきた。

本日の説明のポイント

1.何が起こっているのか？

キャッシュカード偽造犯罪の実態と
その影響

2.何が悪かったのか？

磁気ストライプと暗証番号の脆弱性
＋　日本特有の要因

3.どうすればいいのか？

誰を守るためにどんな手段を講じるのか

1. 何が起こっているのか?

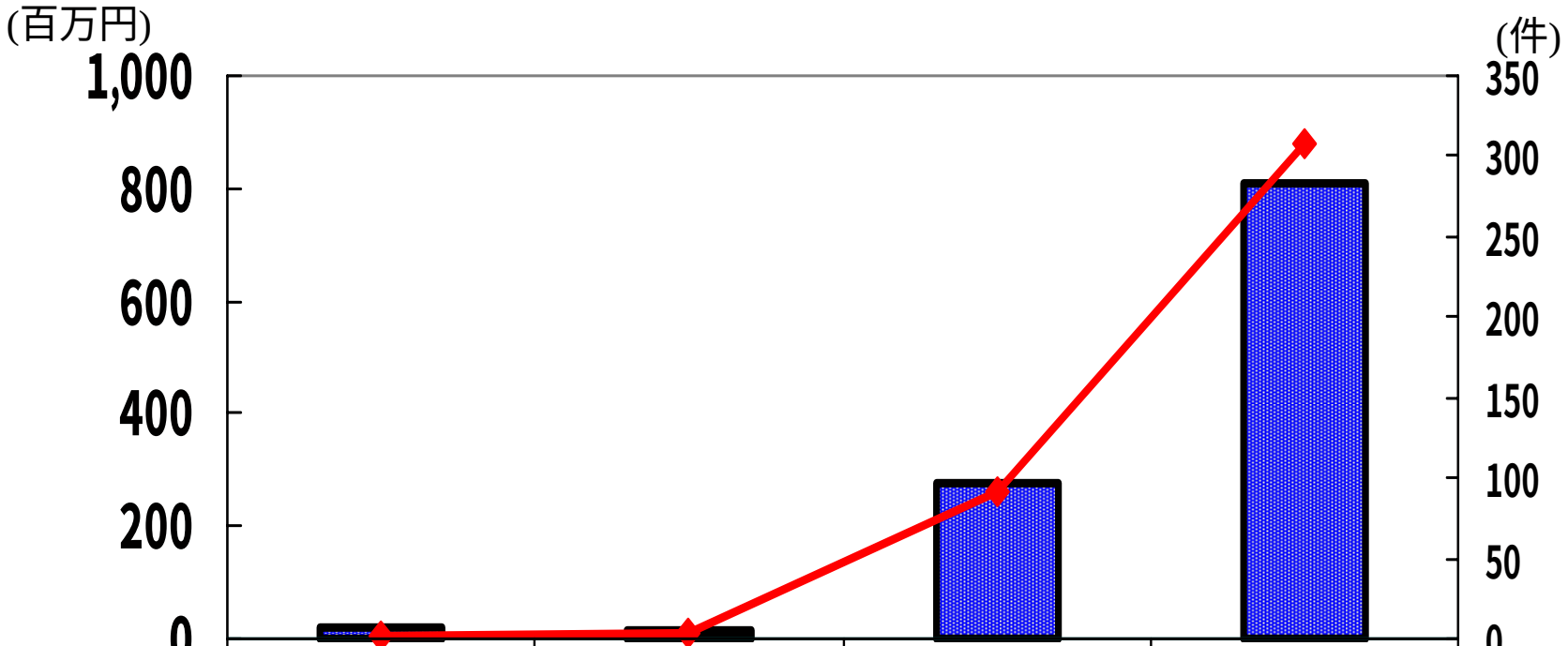
キャッシュカード偽造犯罪の実態とその影響

最近増加した偽造キャッシュカード事件の特徴

- 従来のキャッシュカードの不正利用犯罪は、預金者側に何らかの原因があるものが多かった。
- しかし最近は、
  - 預金者は、容易には推定できない暗証番号を設定している。
  - カード・通帳の盗難にも遭っていない。
  - ところが、偽造カードと暗証番号によって預金が不正に引き出されている。

  という事件が続発した。

全国銀行協会「いわゆる偽造キャッシュカードによる預金等引出し」に関するアンケート結果



	'01年度	'02年度	'03年度	'04年4-12月
金額	19百万円	13百万円	277百万円	807百万円
件数	1件	3件	92件	307件

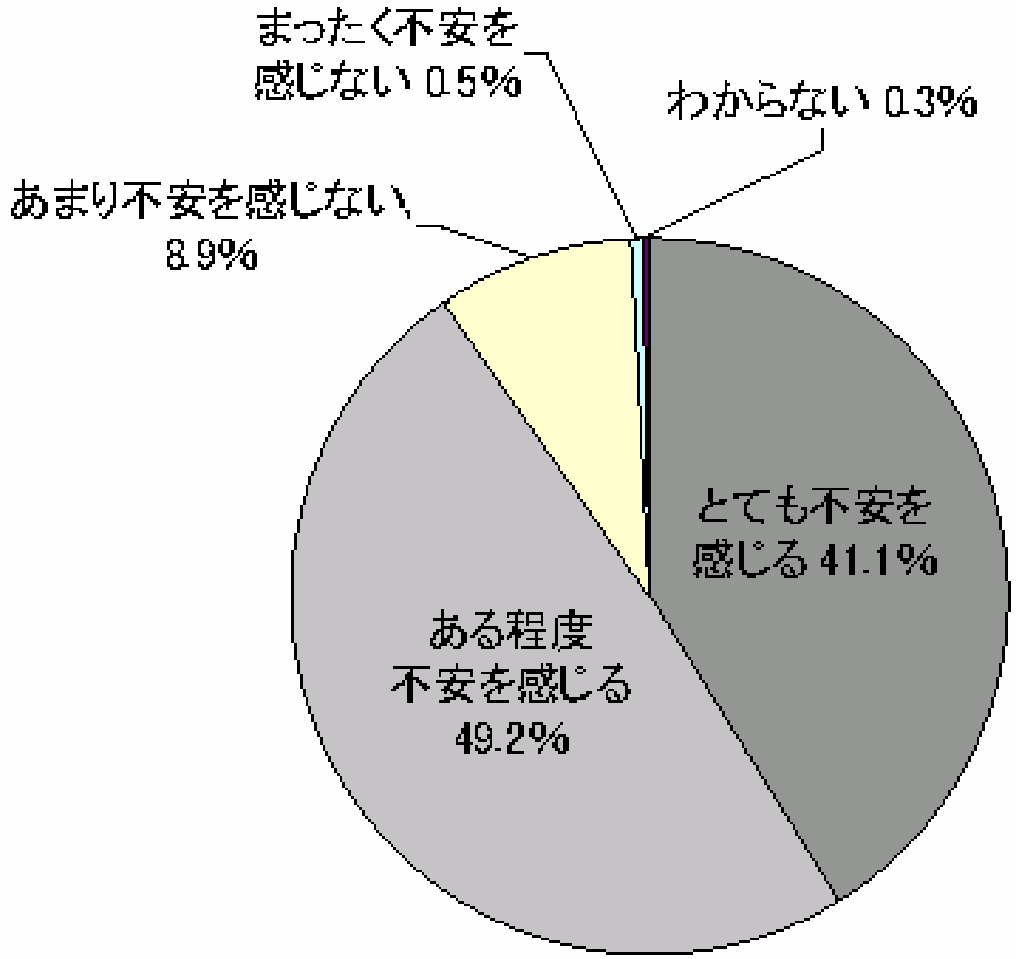
何故、偽造キャッシュカードがこれほど大きな社会問題となったのか？

偽造カードによる被害額は、全国で合計しても高々数億円。数百億円の被害となったプリペイドカード、クレジットカード等の偽造犯罪と比べれば、まだその規模は小さい。しかし、この事件がセンセーショナルに騒がれるのは、他のカード偽造犯罪とは異なり、一般の消費者（預金者）が被害にあい、その損害が補償されないという性格によるもの。

過去の主なカード偽造犯罪

偽造対象	テレホンカード	パッキーカード（パチンコ用カード）	クレジットカード	ハイウェイカード
被害総額	数百億円（？）	630億円	164億円（15年のみ）	百億円程度（？）
主な被害者	NTT	三菱商事、NTTデータ	各クレジットカード会社、損害保険会社	道路公団等

質問:キャッシュカードを使用することに不安を感じていますか？



【 調査概要 】

調査地域:全国

調査対象:
男女20 才以上で
キャッシュカードを利用
する銀行預金者
(有効回答1034人)

調査時期:
2005年2月4日～8日

(マクロミル社のネット
リサーチ結果による)

過去のカード偽造犯罪との違い

過去のカード偽造犯罪においては、その被害者はカード発行者・システム運営者であった。プリペイドカードの偽造では、運営者が得られたであろう収入が得られないという形で損害が発生するため、利用者に負担を転嫁することは難しかった。他方、クレジットカードは、元々ある程度の不正利用による損失を想定して高めの手数料が設定されており、それを前提に運営者が保険に加入しているため、原則として、消費者（カード利用者）には被害が及ばない仕組みとなっている。

これに対し、銀行の預金取引において損害が発生した場合、被害者は利用者であり、かつ、銀行が被害を補償しないルールとなっていた。そもそも銀行は、預金取引においてクレジットカードのような損失が発生することを想定しておらず、それに見合った手数料を徴求しているわけでもない。今後、更に被害が拡大した場合、現在のビジネスモデルのまま、銀行が被害者に補償していくことは困難であり、業務の見直しが必要となっている。

偽造の手口に関する様々な報道とその信憑性

犯行手口	被害者の責任度合い	手口の信憑性
盗んだキャッシュカードを使い、暗証番号は誕生日などの個人情報から推定する。	推定されやすい番号としたのは、暗証番号の管理上の問題。	事実。 過去に実害が生じた事例多数。
ゴルフ場の貴重品ロッカーの暗証番号をカメラで盗み撮りまたは内部者の協力により入手し、キャッシュカードをスキミング。預金口座の暗証番号はロッカーの暗証番号から推定。	預金口座の暗証番号とロッカーの暗証番号を同じにしたのは暗証番号の管理上の問題。ゴルフ場にも管理責任がある。	事実。 逮捕された偽造グループが実際に利用した手口であることが判明している。
ATMやデビットカードを利用した際に、その通信内容が盗聴され、漏洩したカード情報から偽造カードが作成される。暗証番号も同時に漏洩。	被害者に落ち度はなく、盗聴を許したATMを管理する銀行や販売店の責任。	NTT内部者が関与したケースなどを除けば、盗聴が確認されたことはない。ただし、リスクがないとは言い切れない。
満員電車内などでポケットや鞄の中の磁気カードが外側からスキミングされる。	(もし実現した場合)被害者に落ち度はない。	磁気カードの非接触スキミングは不可能。暗証番号も推定できない。

2. 何が悪かったのか？

磁気ストライプと暗証番号の脆弱性
＋　日本特有の要因

現在のキャッシュカードが脆弱なことはかねてより指摘されてきた

- 偽造の容易な磁気ストライプカード
  偽造技術の裾野が広がり、情報が公知となったことにより、従来よりも偽造が容易となった。
- 4桁の暗証番号の限界
  利用者による不適切な設定・運用を排除できず、銀行システムの外部で漏洩してしまうリスクが高い。

―― これらの問題点は、日本のみならず、欧米の金融業界でも同様である。

例えば、日本銀行・金融研究所で1999年11月に開催された第2回情報セキュリティ・シンポジウムでは、現在のキャッシュカードが認証手段として十分な強度を持たないことが指摘されている。

「(a)磁気ストライプカードの偽造が容易になっていること、(b)暗証番号の盗用や推定が巧妙に行われるようになっていること、

等から、「これまで大丈夫だったので、これからも大丈夫」と判断することには慎重であるべきと思われる。

磁気カードよりも安全性の高いICカードの採用や、暗証番号に加えてバイオメトリック認証を導入することについて、検討のスコープを広げていくべきであろう。」

―― 1999年11月に開催したシンポジウムのキーノート・スピーチより
(松本勉・岩下直行「金融業務と認証技術」、『金融研究』19巻別冊1号)

何故、システムの見直しがなされなかったのか。

金融業界はICカード導入の準備は進めていたが、

(1) 過去30年間利用され続けてきた技術を新しい技術に移行するきっかけが掴めなかったこと、

(2) 金融業界全体の基本インフラを変更する業界内の幅広い合意が得られなかったこと、

等から、ICカードや生体認証などの新技術の導入にかかる意思決定が先送りされてしまった。

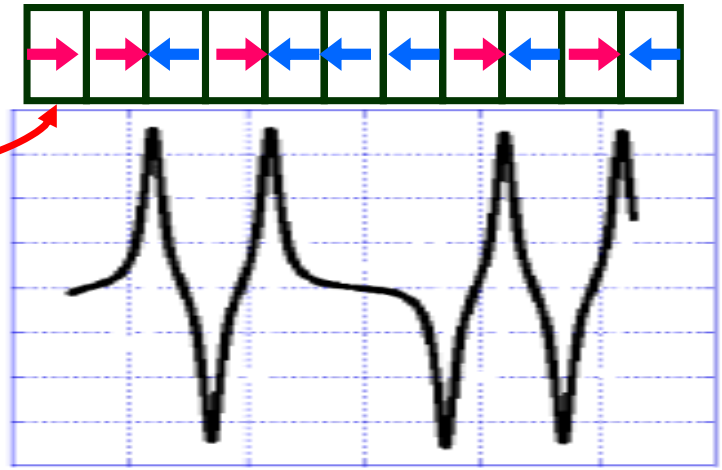
⇒ 社会問題化を受けて、新技術の導入が急務に

【参考】磁気ストライプカードとICカード

名称	磁気ストライプカード	ICカード	
		接触型ICカード	非接触型ICカード
外見			
特徴・用途	プラスチックカードの表または裏に貼り付けた磁気ストライプ（オーディオテープと同じ材質の磁気テープ）に、80文字程度の情報を記録して利用するもの。	プラスチックカードに極めて薄い半導体集積回路（ICチップ）を埋め込み、情報を記録・処理できるようにしたもの。磁気ストライプカードに比べてデータ容量が大きく、データの暗号化も可能であり、偽造にも強い。 接触型ICカードは、カードに設置された接点(端子)を経由して端末がデータを取得する方式で、クレジットカードに広く利用されているほか、キャッシュカードのICカード化もこのタイプを用いる。	非接触型ICカードは、ICチップのほかアンテナが内蔵されており、微弱な電波を利用して端末と交信する。EdyやSuicaに使われている。

磁気ストライプカードの磁気パターンは容易に偽造･複製できる

キャッシュカードの磁気ストライプ
(磁気造影剤を塗布した状態)



偽造ノウハウは雑誌やインターネットから容易に入手可能

磁気カードライターも通信販売で購入可能

銀行のキャッシュカードの暗証番号を何にしているのかの調査

分野	人数	内訳	
誕生日	89人 (46%)	工夫のない誕生日	53人
		誕生日をアレンジ	14人
		家族の誕生日	10人
		他人の誕生日	12人
電話番号	34人 (18%)	自宅	17人
		実家	11人
		彼、彼女	3人
		その他	3人
受験番号	7人 (4%)	大学受験と模試の受験	
出席番号	5人 (3%)	3419	3年4組19番
語呂合わせ	13人 (7%)	4126	(4人) ヨイフロ
		1168	ビビンバ
		2180	ニイハオ
		909	ワクワク
		439	与作
		3594	三国志
		168	イロハ
		9602	苦労人 など

分野	内訳	
その他	2001	映画のタイトル (1941も)
	1568	身長156.8cmだから
	4789	名前画数。4画7画8画9画
	1425	カードを作った時刻 14時25分
	3612	番地。3丁目6番12号
	1789	フランス革命
	1467	人の世むなし応仁の乱
	1134	文化放送
	0101	丸井
	0480	民法480条 (受取証書の持参人への弁済)
	7777	気分で

利用者は、適切な暗証番号を設定していないことが多い。

(のべ194人調査)

週刊文春 1995年10月12日号より引用

加えて、日本特有の要因も

- キャッシュカードに利用される技術については、日本も、欧米の多くの国も、偽造の容易な磁気ストライプカードと４桁の暗証番号の組合せであり、大きな差はない。
- しかし、日本の場合、①預金引出限度額が高いため、被害者が大きな損害を受け易い、②回線の暗号化など、システム全体のセキュリティ対策が明確なものとなっていない、という特有の問題が存在する。

日本特有の問題①: 預金引出限度額の高さ

欧米との大きな違い：銀行券の利用が多い

――日本では、パーソナル・チェックは全く利用されておらず、クレジットカードやデビットカードの普及率も、欧米と比べるとまだ低い。決済の現場で、大量の銀行券が利用されている。

⇒　１日当りCD/ATMでの預金引出限度額

日本：数百万円　vs. 欧米：数万円

⇒　カード偽造グループに不正引出を試みるインセンティブを与えている。

⇒　とりあえずの対策としては、預金引出限度額をできる限り引き下げることが有効。しかし、数日間にわたって継続的に引き出す手口もある。

日本特有の問題②: 日本の金融機関の情報セキュリティ対策の問題

- 銀行の提供するCD/ATMネットワークは、顧客利便を追及して提携、接続を繰り返した結果、セキュリティ管理上、複雑化しすぎていないか？
- 通信情報(特に暗証番号)の通信経路における暗号化など、情報漏洩を防止する適切な対策が講じられているか？
- 顧客との責任分担の境界点は妥当か？
- 考え得るリスクについて、顧客に十分な説明を行っているか？

提携先の追加とセキュリティの維持

顧客の利便性・効率性を重視した提携先の追加によって、CD/ATMネットワークのセキュリティが損なわれていないか？

- デビットカード
  ——潜在的な不正利用リスクの増大
  ——決済データを仲介する加盟店の存在
  ⇒ 不正発生時の責任分担が不明確になる問題。
- コンビニATM
  —— 金融機関が責任を持って管理できる領域との違い。
  —— 元々そういうATM利用環境が想定されていたのか。

なぜ暗証番号を暗号化する必要があるか

推定されにくい暗証番号を設定し他人に見られないように入力する

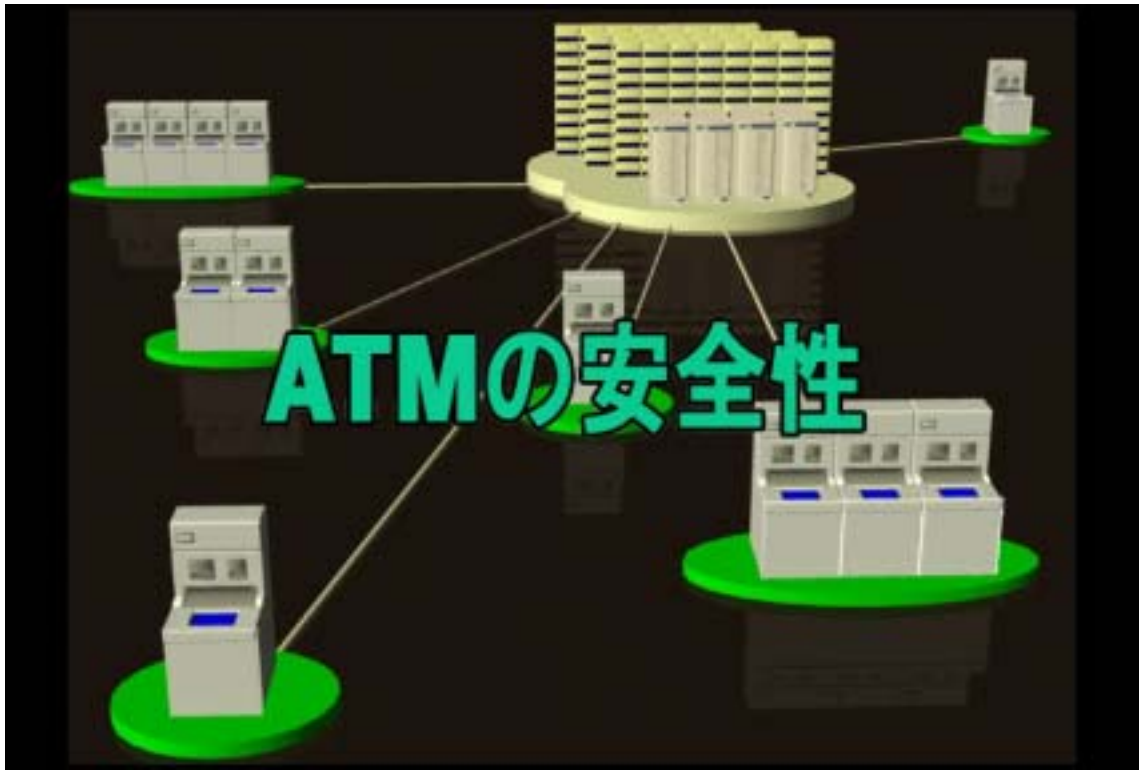
欧米の銀行では、従来から、ISO 9564に準拠し、CD/ATMに入力された暗証番号を直ちに暗号化して照合システムに送信するシステムが整備されていた。

一方、日本の銀行は、クローズド・ネットワークの利用を前提に、従来、あまり暗号を利用してこなかった。最近になって、暗号を利用する銀行も出始めているが、まだ限定的である。

銀行の照合システムから外部に情報が漏洩しないように注意する。

“ATMは専用線を使っているから安心”か？

中学校の技術家庭科教材
情報とわたしたちの生活　「ＡＴＭのしくみ」　より
http://kyoiku-gakka.u-sacred-heart.ac.jp/jyouhou-kiki/4203/



「ＡＴＭと銀行のコンピュータをつなぐネットワークに関しては、専用回線を使いますのでハッキングなどの心配はありません。」

「北海道銀行事件」(1982年)の教訓

日本電信電話公社の主任技術員が、地方銀行（北海道銀行亀田支店）が利用していた専用回線上を流れる情報を盗聴して入手した情報（カード情報、暗証番号）を利用してカードを偽造し、盗聴した暗証番号を入力してCD機から133万円を不正に引き出した事件。

=> 「専用線であれば安全」ということはない。

ISO/TC68における暗証番号のセキュリティを巡る議論

- **ISO（国際標準化機構）**
  - 様々な産業における国際標準化を担当する非政府間機構（1947年設立）。
- **ISO/TC68（金融専門委員会）**
  - 「金融サービス」を対象とする専門委員会
  - 金融業務に利用される情報通信技術、情報セキュリティ技術に関する国際標準化を担当

暗証番号(PIN)の取扱に関する国際標準: ISO 9564

Personal Identification Number (PIN) management and security

Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems

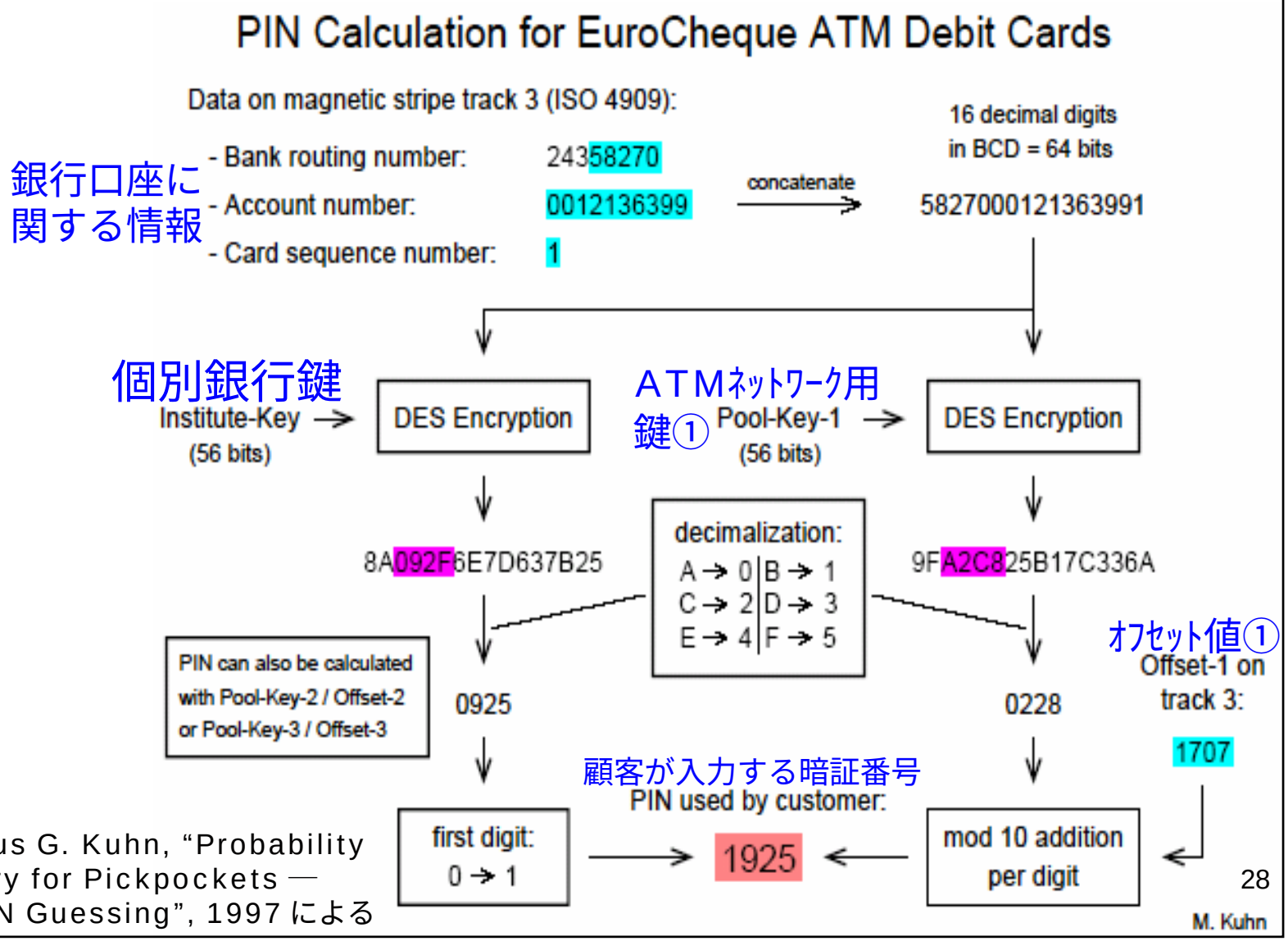
- 銀行取引カード(キャッシュカード、クレジットカード、デビットカード)等と共に利用される PIN について、その設定、保管、入力、送信等に関する一般的なルールを取り決め(例えば、PINは4桁以上)。
- PINに関る機器・ソフトは、不正に改変できないことが必要(4a)。
- PINを平文で保管するには、物理的に安全な環境が必要(4e)。
- PINを暗号化する場合、暗号化方式を明らかにしないことによってではなく、暗号鍵の秘匿によってその機密性を守ること(4d)。
- PINを暗号化する場合、同じPIN、同じ暗号鍵でも、異なる暗号文となること(乱数等により適切にパディングすること、4c)。
- PINを暗号化する場合、ISO 9564-2に規定された暗号アルゴリズムで暗号化すること(6.2)。

Personal Identification Number (PIN) management and security
Part 2: Approved algorithm for PIN encipherment

- かつては、米国国内標準（ANSI X3.92:1981）を引用して
  DES暗号のみを規定していた。
  ⇒ 欧米のCD/ATMでは、暗証番号の暗号化にDES暗号を
  利用していた。
  ⇒ 1990年代に入って、DES暗号の強度が低下。
  ⇒ 米国の金融業界が、DES暗号に代わる暗号アルゴリズムを
  自ら標準化（ANSI X9.52 トリプルDES）。
- 現在は、推奨アルゴリズムとしてトリプルDESとRSAのみを記載。
  ⇒ 欧米のCD/ATMは、DES暗号からトリプルDES暗号に移行。

米国の金融業界では、業界団体と主要銀行が中心となって、
経営レベルで暗号アルゴリズムの問題が討議されている。

【参考】 ドイツのユーロチェック・カードにおける暗証番号の生成方式 (1997年以前の方式)



Markus G. Kuhn, “Probability Theory for Pickpockets — ec-PIN Guessing”, 1997 による

3. どうすればいいのか？

誰を守るためにどんな手段を講じるのか

誰を守れば良いのか？ ―2つの視点

(1)カード偽造団から預金者を守る

――スキミングを受けにくくする。暗証番号を盗用されにくくする。

――偽造カード被害を発見したら、直ちに連絡できる仕組みを作る。

――取引限度額を、預金者の利便性を損なわない範囲内で、引き下げあるいは任意に設定できるようにシステムを変更。

――被害が生じても、保険でカバーできるようにする。

⇒ しかし、銀行が被害を全面的に補償することをコミットすれば預金者は守られるため、「預金者のためには」これらの対策の必要性は低下する。むしろ、過剰に守られてしまう結果、預金者側のカードや暗証番号の管理が杜撰になる可能性がある。

⇒ 銀行が補償をコミットした場合、「被害者に成りすます」ことにより、銀行から補償金を詐欺する犯罪が発生する惧れがある。

この結果、

(2)カード偽造団から銀行を守る という視点も必要になる。

カード偽造被害に対する補償の影響

①高額の預金引出限度額の要請

②脆弱な磁気ストライプカードと4桁暗証番号

⇒ 「被害者に成りすます」犯罪の誘引が大きく、銀行が無制限に補償することをコミットしてしまうと、銀行に大規模な被害が生じる惧れ。

⇒ 消費者保護のための補償にあたっては、①、②の何れか（または両方）を是正の要。

①預金引出限度額の引き下げ

- 短期的に取りうる殆ど唯一の方法。
- 預金者の利便性とのトレードオフ。
  ――窓口時間外における多額の預金引出しニーズは、実際にどの程度あるのか？
- 利用者に選択させるのは意味があるか？
  ――犯罪者はあえて上限額を引き上げて被害者に成りすます惧れ。
  ――高額の取引限度額を求める預金者(個人事業主?)に対しては、セキュリティや補償の条件が一般預金者と異なる預金サービスを異なる価格で提供することが必要。
- 1日の上限額？一定期間の上限額？
  ――被害者が長期間気づかなければ、被害額は拡大。
  ――米国のように、定期的にステートメントを送る必要は？

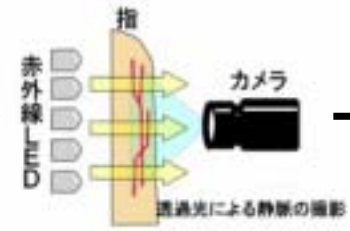
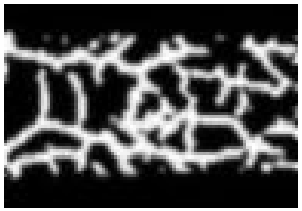
②カードとATMのセキュリティを抜本的に見直す

- 時間はかかるが、正攻法の偽造カード防止対策。
- キャッシュカードの偽造を防ぐ。
  - ——ICカード化は有効。ただし、ICカードの安全性評価が必要。
  - ——磁気ストライプが並存する限り、偽造が容易なことは変わらない。カード、ATM両方の切替が完了して初めて効果あり。
  - ——銀行が無制限に補償する前提であれば、利用者があえてICカードに切り替えるインセンティブはない。変更の強制が必要か？
- 暗証番号の漏洩を防ぐ。
  - ——仮に漏洩して不正引出しが発生した場合、責任の所在を明らかにすることが必要。「銀行からは漏れてない」と言えるためには、暗証番号の生成から廃棄まで、水も漏らさぬ機密保護が必要。
    - ☞ 預金口座開設時の書面からATMの通信回線まで、全ての局面で暗証番号の機密が守れること。預金者啓発も大切。
    - ☞ 適切な暗号化方式の選択と適切な実装。安全性評価が必要。

生体認証は万全か？

ICカードも盗用は可能。盗難カードの補償方針如何では、盗用の被害者成りすましを防ぐ意味からも、本人確認手段の高度化が必要とされる可能性。

——ただし、生体認証は技術としての成熟度に問題。拙速を避け、脆弱性を指摘する研究成果を踏まえてセキュリティ評価を適切に実施し続けることが必要。

てのひら静脈認証	  
指静脈認証	  

通信経路の暗号化を含むネットワーク・インフラの再構築

- 単にカードの耐偽造性を向上させ、カード保有者の本人認証を強化するだけではなく、システム全体のセキュリティ向上を図るべき。
- そのためには、ICカードを用いて生成する認証のための情報を、通信ネットワーク・インフラを通じて金融機関側と送受信する仕組みを構築していくことが必要。
- 金融機関向け通信ネットワーク・インフラの世代交代のタイミングをはかって、こうしたコンセプトを金融機関間で共有していくことが重要。

銀行のリテール戦略、銀行経営への影響

預金者の被害を減らすための正攻法は、コストを掛けて高度なセキュリティ対策を導入していくこと。しかし、現在の預金取引の銀行ビジネス上の位置付けを考えると、全ての金融機関がそのような対応が可能とも考えられない。

一方、セキュリティ対策は適当に済ませ、損害の補償で対応するという選択肢をとった場合も、問題が生じる。預金取引は、クレジットカードのように、預金額や送金額に比例した手数料を徴収するビジネス・モデルになっていないため、取引金額に応じて一定の比率で発生すると考えられる損害を無制限に補償し続けることはビジネス的に困難だからである。

こうした矛盾を解消するためには、例えば、現在の手数料体系を見直すことが考えられる。偽造カード問題は、休眠口座の扱いや、口座維持手数料の徴求など、銀行経営における預金取引の位置付けの再考を迫るものでもある。

おわりに

金融業界が巨大な情報システムを管理する装置産業になってしまっている以上、そこで利用されている技術を分析・研究し、脅威を未然に取り除くことは、金融業界自身の当然の責務。

銀行は、自らの情報システムの脆弱性を正確かつタイムリーに検知し、その情報を業界内で適切に共有し、その是正に戦略的に対応していくための体制を早急に構築していくことが必要。

金融業界全体の問題として、CD/ATMネットワーク全体のセキュリティを検討する体制を整備していくべきではないか。