平成18年1月13日

金融高度化セミナー
「金融機関における情報セキュリティの高度化に向けて」

金融業界における情報セキュリティ問題とその対策について

日本銀行 金融研究所
情報技術研究センター長
岩下 直行

本資料の内容や意見は発表者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではありません。

本日のアジェンダ

1．金融業界における情報セキュリティ対策の何が問題か

2．偽造キャッシュカード問題
――被害の拡大とその教訓

3．インターネット・バンキングのセキュリティを巡って

4．金融機関のセキュリティに対する信頼を取り戻すために

１．金融業界における情報セキュリティ対策の何が問題か

歴史的建造物となっている古い銀行の建物の頑丈な外観、堅牢な金庫

↓

地震・火災・強盗などの脅威に対して、高い安全性を持っていることをアピールするもの

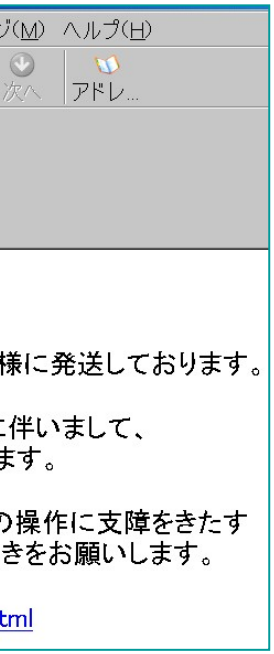
↓

顧客にとっての信頼の象徴であった。

しかし、、

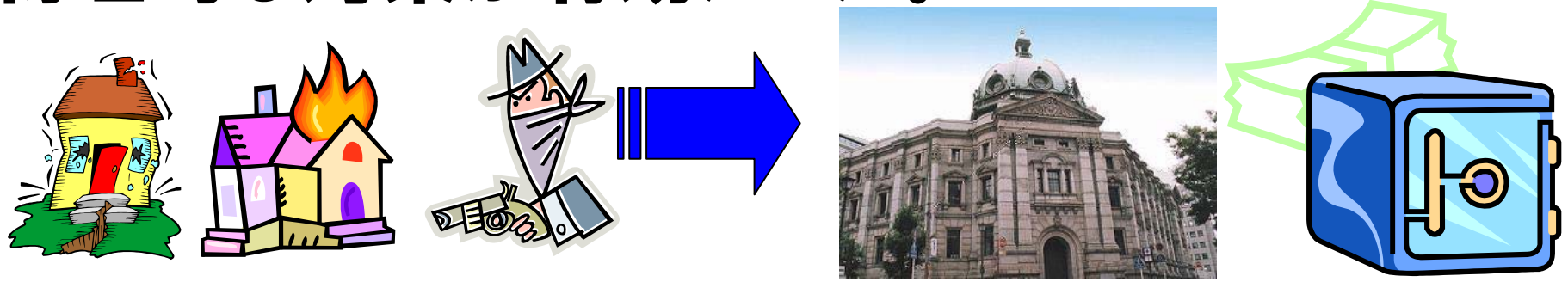
相次ぐ金融ハイテク犯罪

- 偽造キャッシュカード被害の拡大
- ATMに仕掛けられた隠しカメラによる偽造カード被害も
- インターネット・カフェのパソコンに仕掛けられたキー・ロガー
- 無差別に顧客に送りつけられるフィッシング詐欺メール
- スパイウェアへの感染によるパスワードの漏洩
- クレジットカード番号の大量漏洩

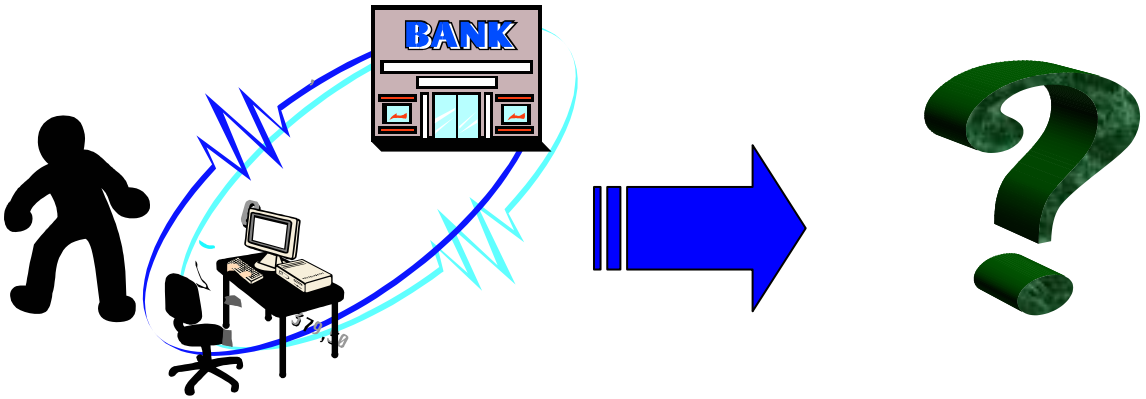


脅威の変化に応じて対策も変化させなければ

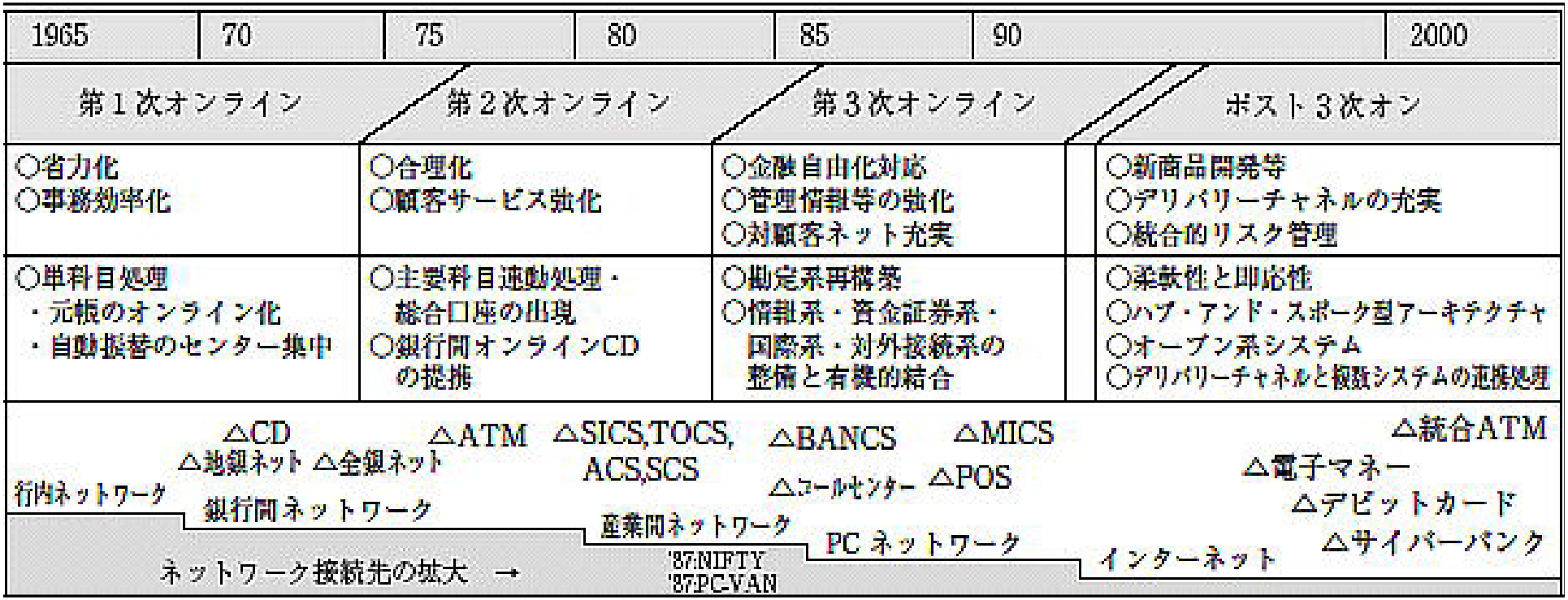
- 従来の物理的な脅威（地震、火災、強盗）には、物理的な対策が有効だった。



- ネットワーク経由で遠隔地から情報システムを攻撃する新しい脅威（金融ハイテク犯罪）に対して、有効な対策が採られているだろうか？



金融業界は、コンピュータによるネットワーク・システムを最も早い時期に整備した業種であった



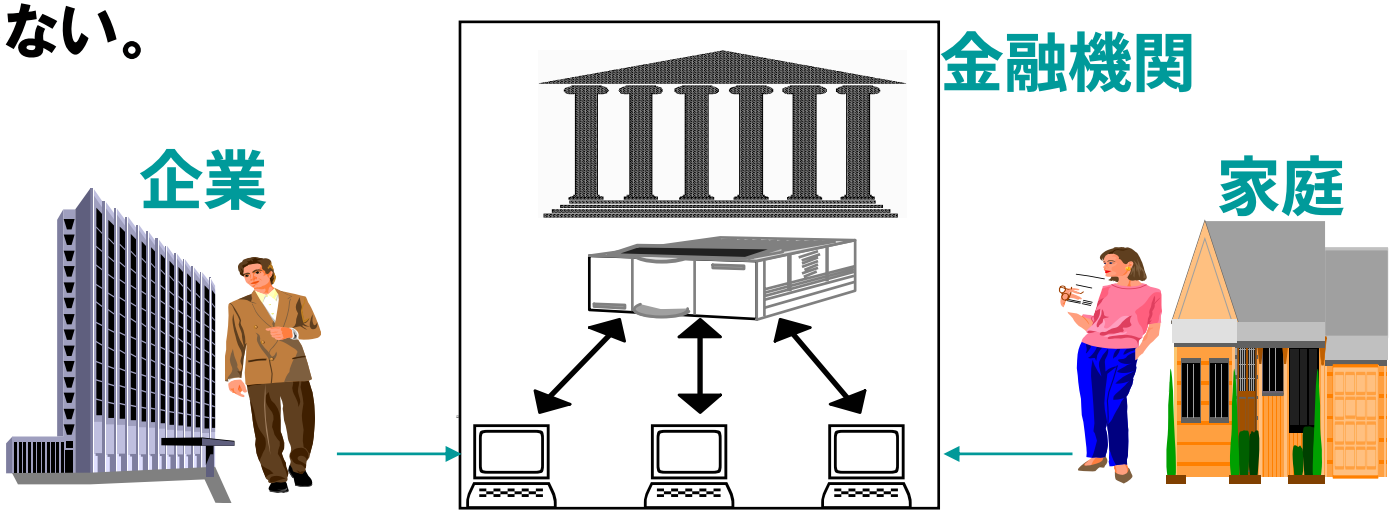
1970年頃に初めて導入されたキャッシュカードとCD/ATMの技術

基本設計を30年間にわたって維持

銀行のオンライン・システムの頑健性、安全性に疑いを持たれることはなかった。

従来の金融業界におけるセキュリティ対策の考え方

- 従来のポリシー：「閉じたシステム」「閉じたアーキテクチャー」
- 外部から物理的に隔離された専用のコンピュータ・システム。異なるシステム間の連動はあまり考慮されない。
- セキュリティ対策としては、専用回線等による物理的なアクセス制御、バックアップ手段の充実などが中心。
- セキュリティ対策にかかる情報は対外秘。詳細は一部の担当者しか知らない。



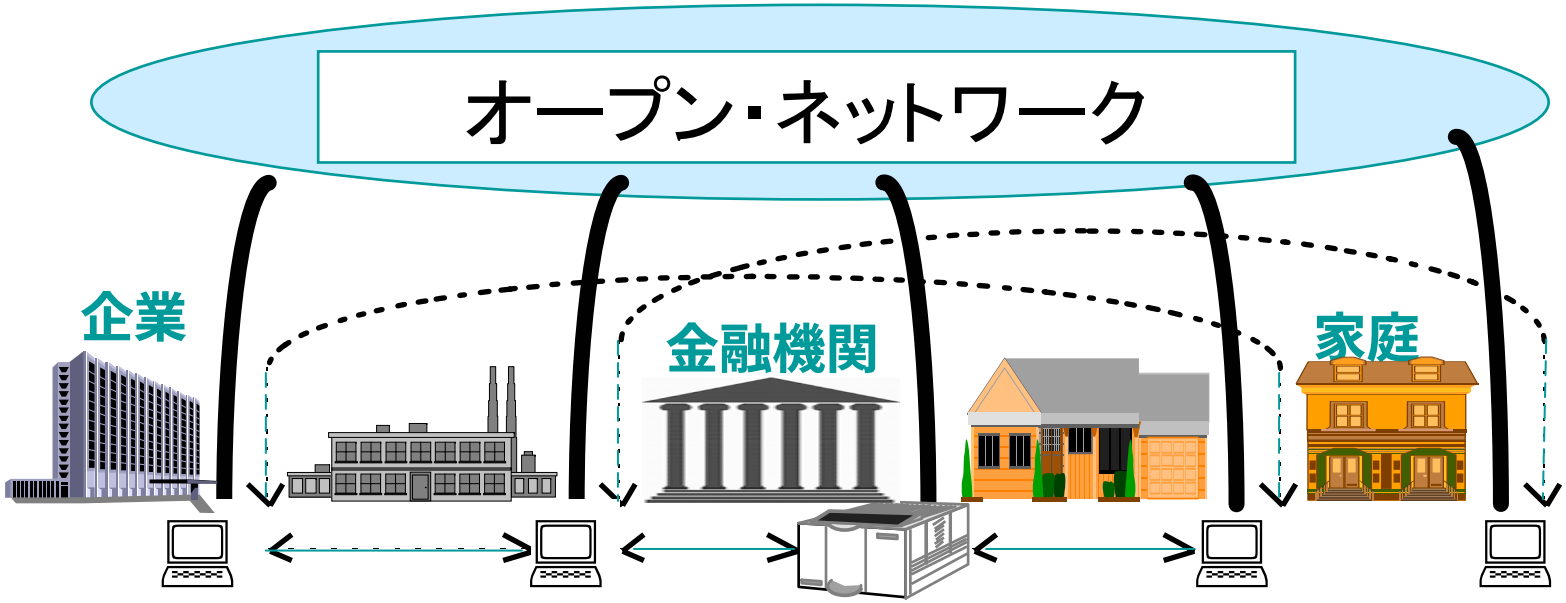
・ピラミッド型　・閉鎖型　・集中システム

8

しかし、情報技術の発達に伴い、従来の前提が崩れつつある

例：STP化、インターネット・バンキングの普及。

オープン・ネットワークを介して様々なシステムが相互に連動し合う仕組みとなっていくことを前提に、システム全体のデザインとセキュリティ対策を考え直す必要。



・水平型　・開放型（オープン・システム）　・分散システム

金融機関のセキュリティ対策はどうあるべきか

従来のセキュリティ対策のコンセプト

たまねぎ型

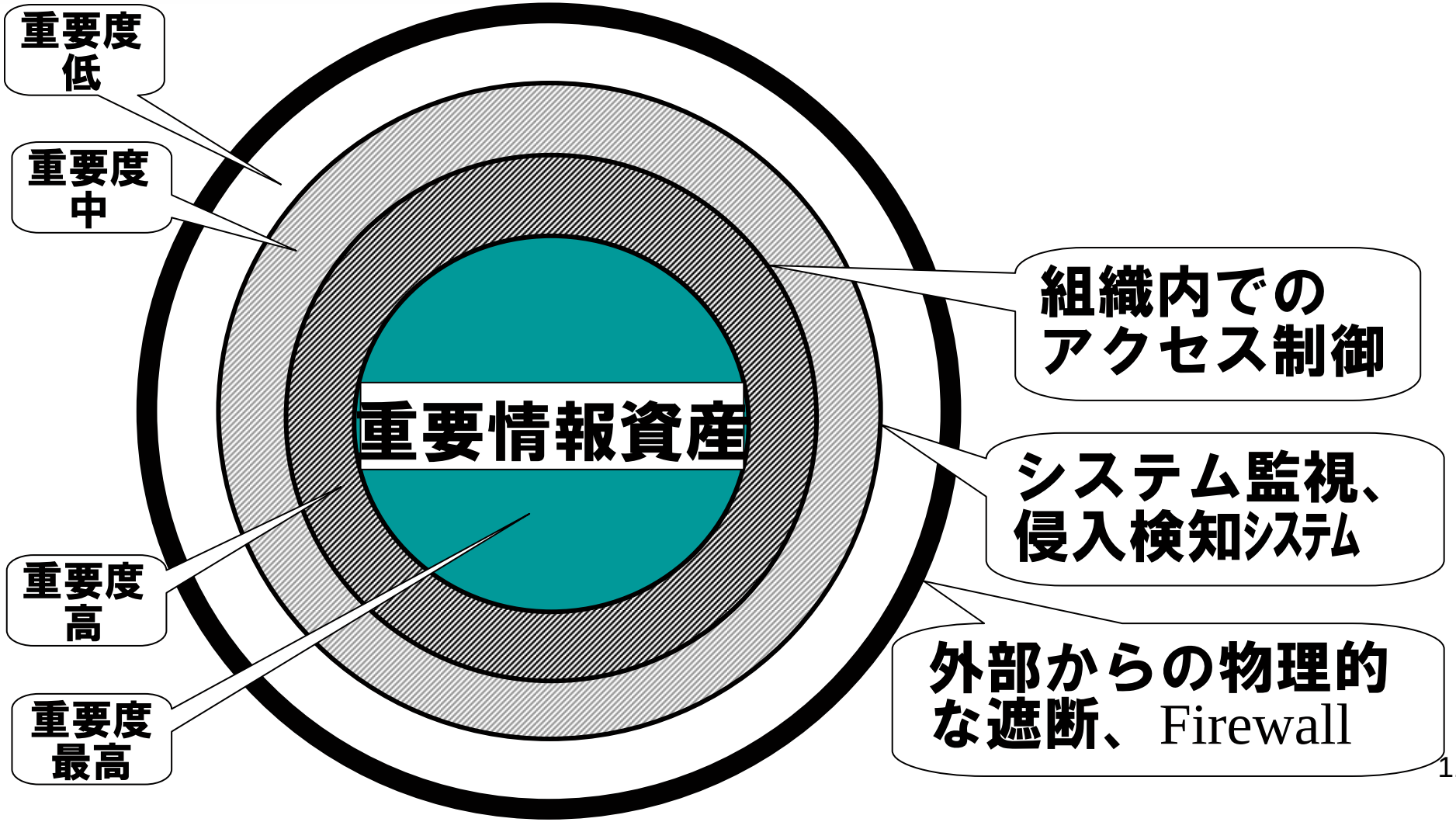
⇒ センターに集中した重要な情報を守る。
⇒ センターさえ守ればセキュリティが確保できる。

しかし、実際の金融機関の情報資産の分布は、

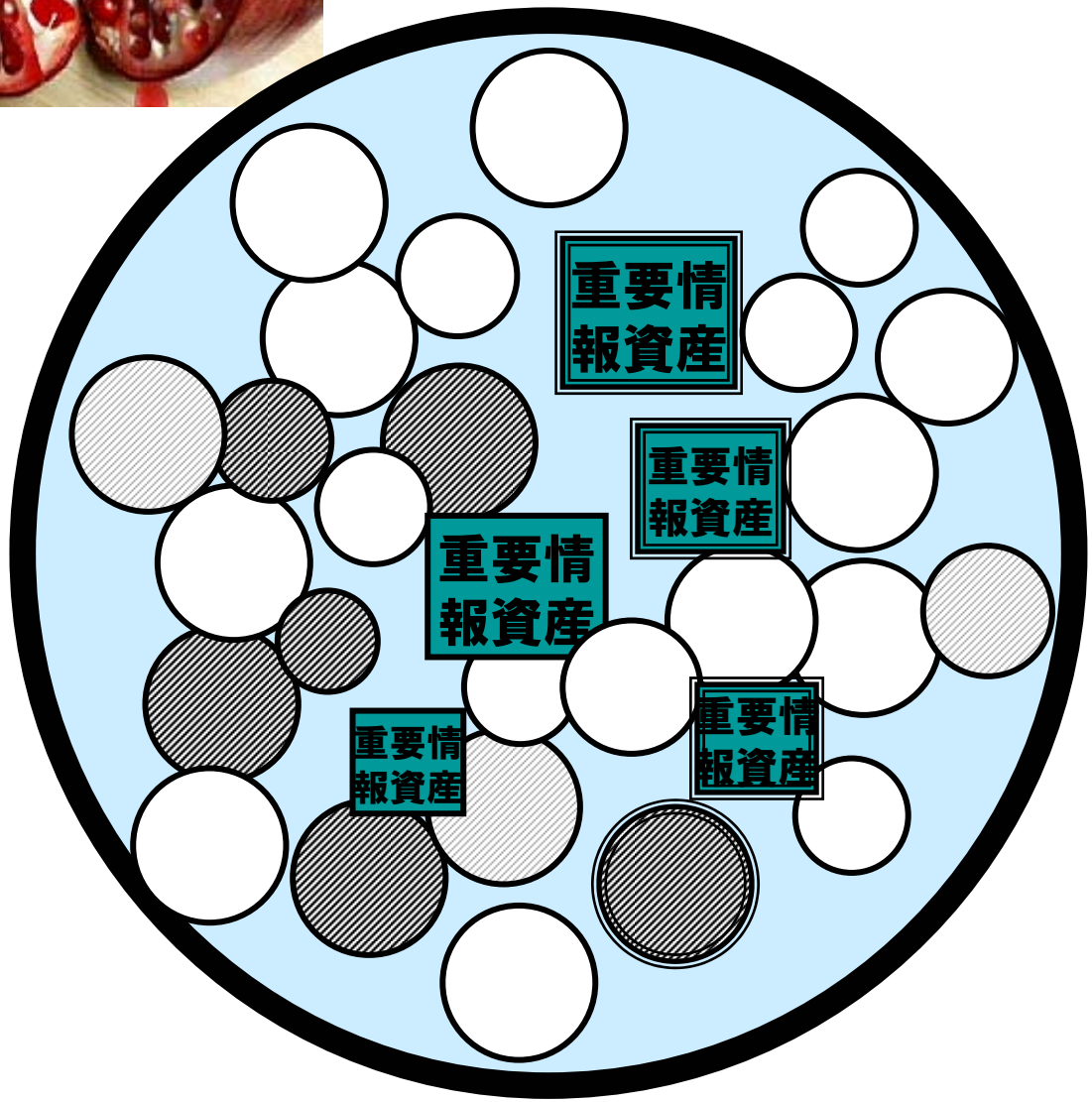
ざくろ型

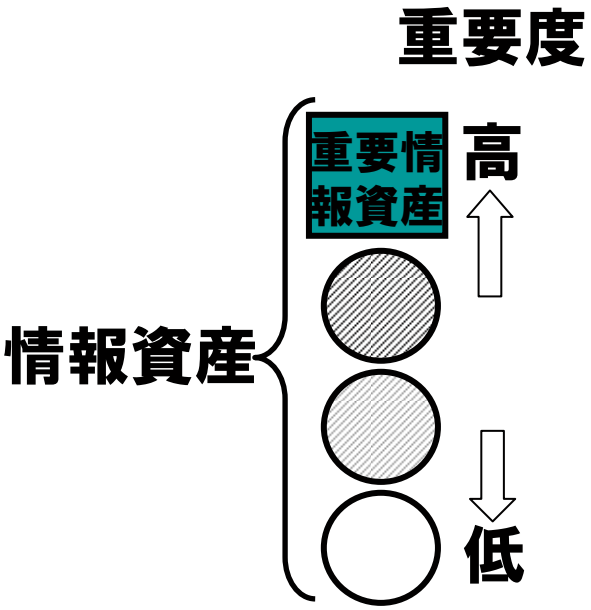
⇒ 高いセキュリティを必要とする部分が散在。
⇒ 従来とは違ったコンセプトが必要になる。

従来、企業内の情報資産の分布は「たまねぎ型」（同心円状）と考えられ、それに応じたセキュリティ対策が講じられてきた。



しかし、情報技術革新に伴い、実際の情報資産の分布は「ざくろ型」に近いものとなってきており、それに応じたセキュテリィ対策が必要となってきている。





情報技術革新による金融機関のシステムの変化を踏まえたセキュリティ対策が必要

金融機関の情報システムの基幹である**勘定系システム**は、引き続き**レガシー技術**を利用して構築されている。このため金融機関は、セキュリティ対策の重心をレガシー系に置き勝ちであった。

しかし、基幹にレガシー技術を利用していても、**顧客とのインターフェース部分**や**身の回りシステム**に分散系の技術が広く利用されている以上、仮にそこに問題があれば、業務全体が滞ってしまう。

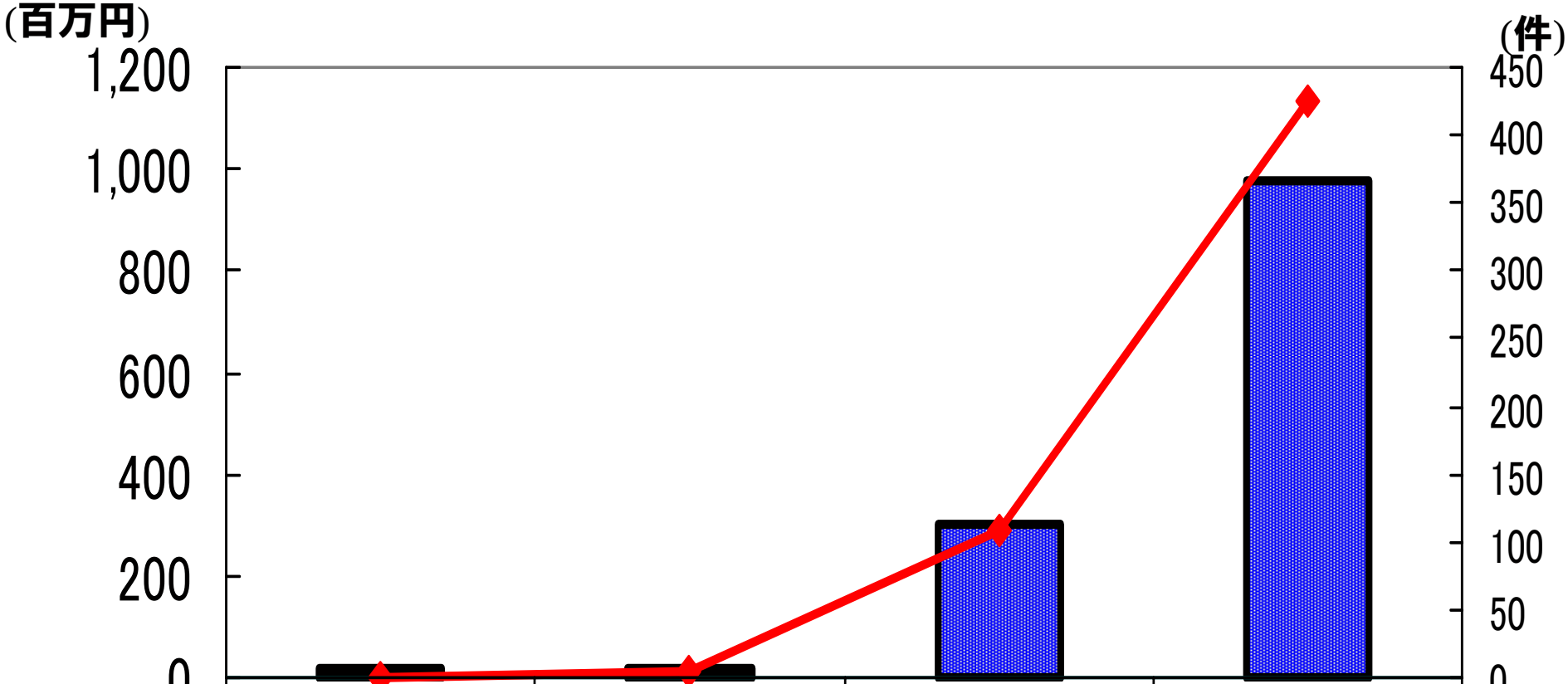
⇒ 金融業界は、レガシー系のみならず、**分散系も含めたシステム全体**のセキュリティ対策を強化していく必要があるのではないか。

どの範囲を？　どのレベルまで？

- 金融機関は、顧客の財産を預かり、管理する立場にあるため、預金取引の安全性確保はもとより、個人情報保護、不正侵入対策、ウィルス対策等の情報セキュリティ対策について**他の産業よりも高い水準を達成**することが要求されている。
- 従来、金融機関があまり活発に利用して来なかったインターネット上でのシステム運行において、攻撃者に出し抜かれないためには、金融機関側も十分に**情報を収集**し、「賢く」なっている必要がある。
- 対策を進める上では、金融機関内部においてセキュリティ対策に関する議論をタブーにしないことが大切。脅威を認識することから対策が始まる。

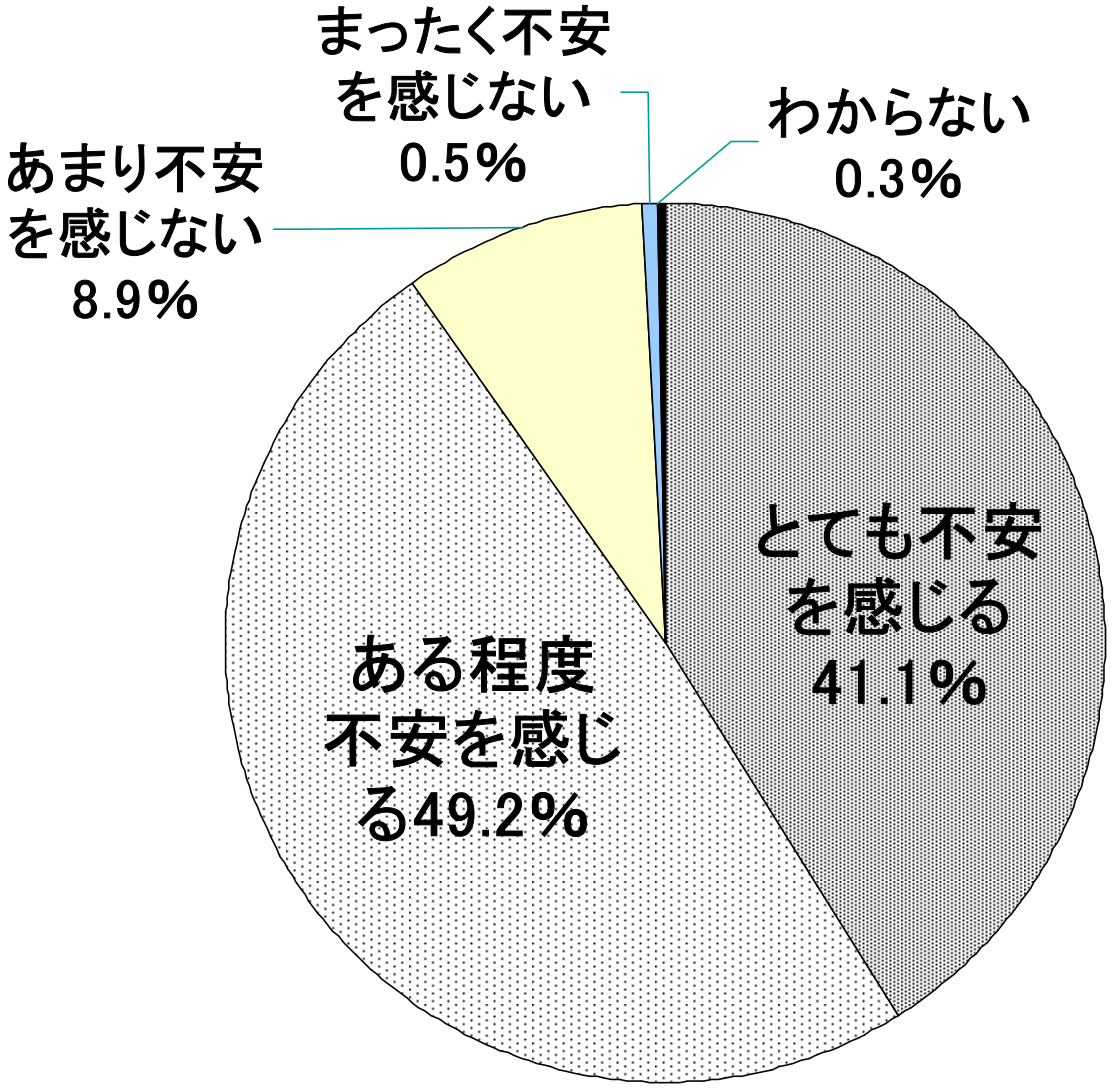
2．偽造キャッシュカード問題
――被害の拡大とその教訓

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年度
金額	19百万円	16百万円	300百万円	975百万円
件数	1件	4件	108件	424件

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

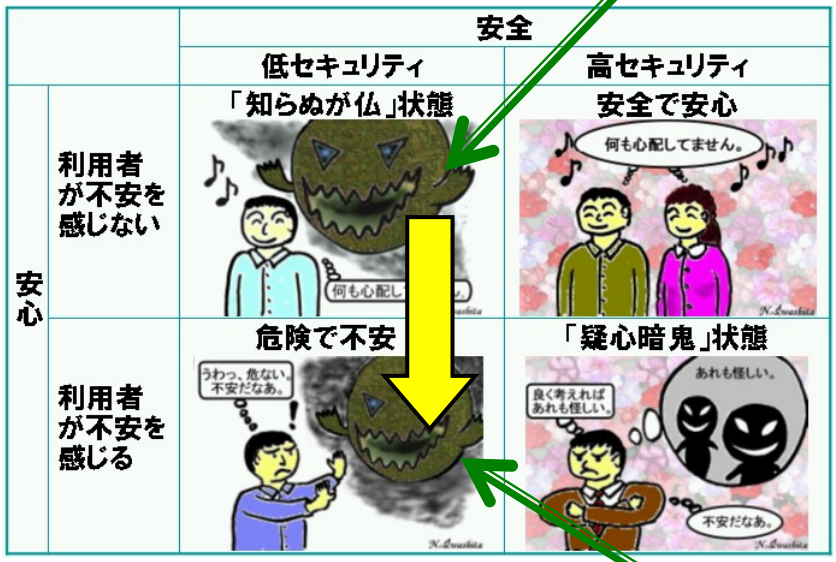
調査対象：
男女20 才以上で
キャッシュカードを利用
する銀行預金者
（有効回答1034人）

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）

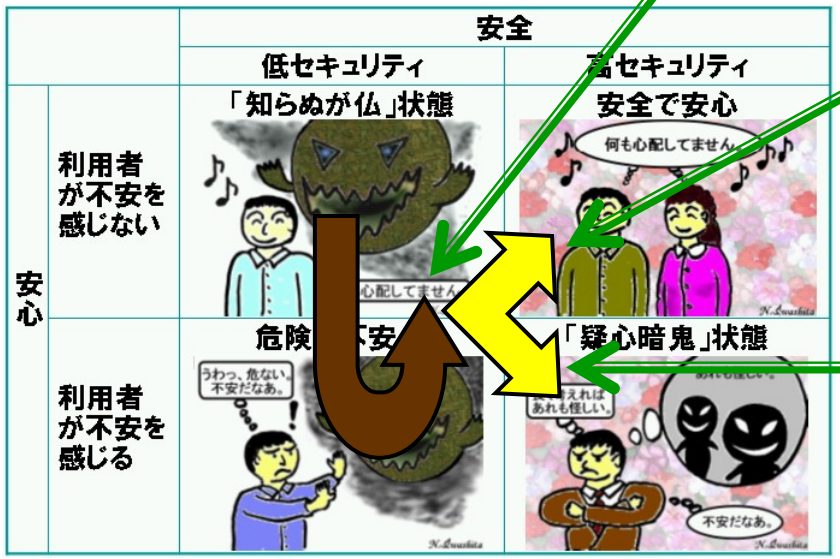
利用者の不安を解消するためにはどうすればよいか
――「安心・安全」の4象限分析で考える

		安全	
		低セキュリティ	高セキュリティ
安心	利用者が不安を感じない	「知らぬが仏」状態 	安全で安心 
	利用者が不安を感じる	危険で不安 	「疑心暗鬼」状態 



キャッシュカードを利用した預金取引については、従来は、潜在的な犯罪のリスクはあったものの、それがほとんど顕現化しなかった（社会が安全で犯罪が発生しなかった、あるいは、犯罪が発生しても利用者に実害が生じなかった）ため、利用者は預金取引に不安を感じていなかった（「知らぬが仏」状態）。

しかし、ハイテク金融犯罪が多発し、一部の利用者に実害が生じたため、利用者が強い不安を感じるようになった（「危険で不安」な状態）。



金融機関が被害の補償を表明し、預金者保護法が成立した結果、利用者の不安感は鎮まりつつある。しかし、また利用者に実害が及ぶ事件が起きれば、不安感は再燃しかねない。

今後、目指すべきなのは、かつての「知らぬが仏」状態に戻ることではなく、本当の意味で「安全で安心」な状態を実現すること。

しかし、一歩間違えば、「折角セキュリティ対策を講じて、安全となっても、利用者がそれを信頼しない」という「疑心暗鬼」状態に陥りかねない。

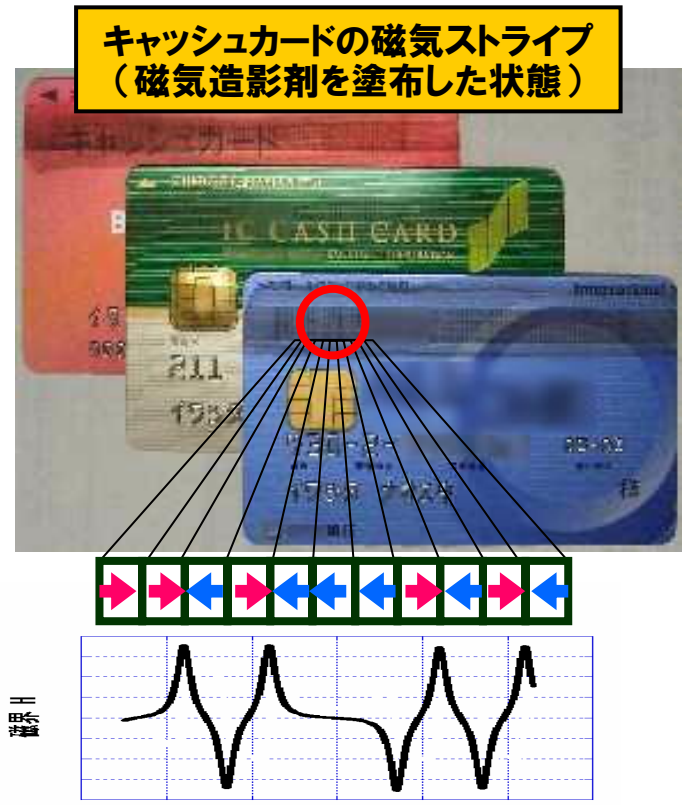
そうならないためにも、「利用者に不確かな情報しか与えず、安全と錯覚させる」のではなくて、「実効性のあるセキュリティ対策を講じた上で、利用者に正確な情報を伝え、信頼を勝ち得ていく」努力が必要。

偽造キャッシュカード問題の原因

現在のキャッシュカードによる預金引出しが脆弱であることは、かねて指摘されてきた。

- 偽造の容易な磁気ストライプカード
- 4桁の暗証番号の限界

  ⇒ 利用者による不適切な設定・運用を排除できないため、推定されたり、金融機関のシステムの外部で漏洩してしまうリスクがある。



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		分野	内訳	
誕生日	89人（46%）	工夫のない誕生日	53人	その他	2001	映画のタイトル（1941も）
		誕生日をアレンジ	14人		1568	身長156.8cmだから
		家族の誕生日	10人		4789	名前画数。4画7画8画9画
		他人の誕生日	12人		1425	カードを作った時刻 14時25分
電話番号	34人（18%）	自宅	17人		3612	番地。3丁目6番12号
		実家	11人		1789	フランス革命
		彼、彼女	3人		1467	人の世むなし応仁の乱
		その他	3人		1134	文化放送
受験番号	7人（4%）	大学受験と模試の受験			0101	丸井
出席番号	5人（3%）	3419	3年4組19番		0480	民法480条（受取証書の持参人への弁済）
語呂合わせ	13人（7%）	4126	（4人）ヨイフロ		7777	気分で
		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			

（のべ194人調査）　週刊文春 1995年10月12日号より引用

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）

問題があることは分かっていたのに、何故、システムの見直しができなかったのか。

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。

⇒ 金融機関のセキュリティに対する利用者の**信頼を大きく損なう**結果に

キャッシュカードとATMのセキュリティ対策に関する現状評価

- 偽造キャッシュカード問題に際して、金融業界は、**被害を補償**することを表明し、ATMの**引出限度額**を引き下げるなど、被害を限定する対策を講じた。
- また、犯罪の未然防止対策として、**ICカード化**、**生体認証**の導入等への取り組みを表明した。ただし、実際に対策を実施した先は限られており、また、実施した先についても、普及率は高くない。
- 金融機関における預金引出しにおいては、引き続き、磁気ストライプカードと暗証番号による認証が主流であり、スキミング犯罪の**根は絶たれていない**。

キャッシュカードとATMのセキュリティを抜本的に見直すには？（その１）

ICカード化によってキャッシュカードの偽造を防ぐ。

—— 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、磁気ストライプが廃止されて初めて効果あり**。

—— 偽造被害発生時に預金者に補償することを前提とすると、利用者にはあえてコストを掛けてICカードに切り替えるインセンティブはあまり働かない。どのようにして普及させるかが問題。

—— ICカードであれば何でも安全という訳ではない。
ICカードが偽造された例：欧州のpay-TV用ICカード、フランスの銀行カード

⇒ ICカードの**安全性評価**が必要。ICカードが解析されたとしても、システム全体のセキュリティが損なわれないような設計にすることも大切。

キャッシュカードとATMのセキュリティを抜本的に見直すには？（その２）

通信回線の暗号化等により暗証番号漏洩を防ぐ。

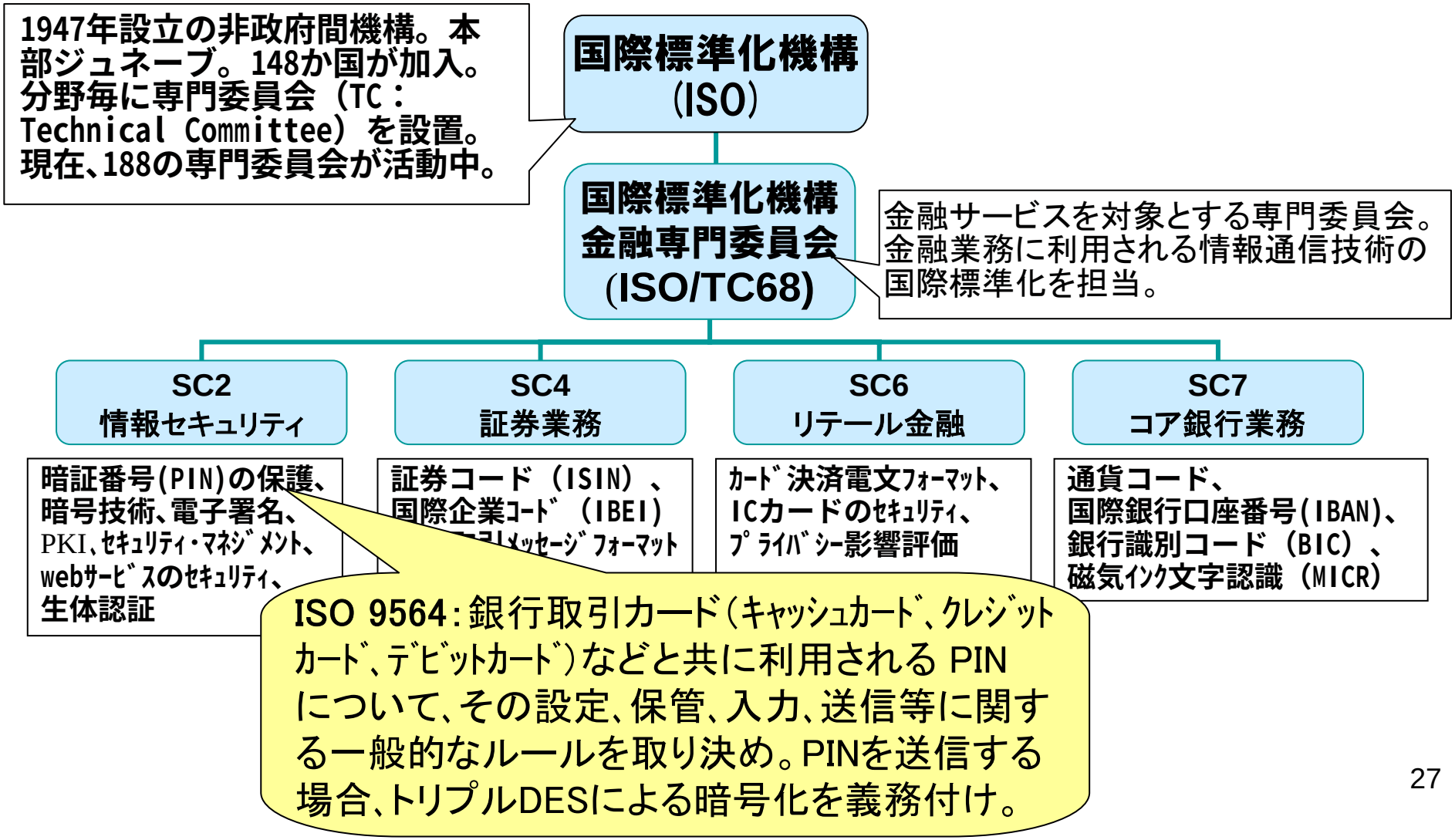
――推定され難い暗証番号とするための預金者啓発。

――仮に漏洩して不正引出しが発生した場合、「金融機関側からは漏れてない」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保護されているか。
- 通信回線において機密を保護するためには、適切な暗号アルゴリズム・鍵長の選択と、適切な実装が不可欠。
- ISO/TC68が規定している国際標準 ISO 9564が参考になる。

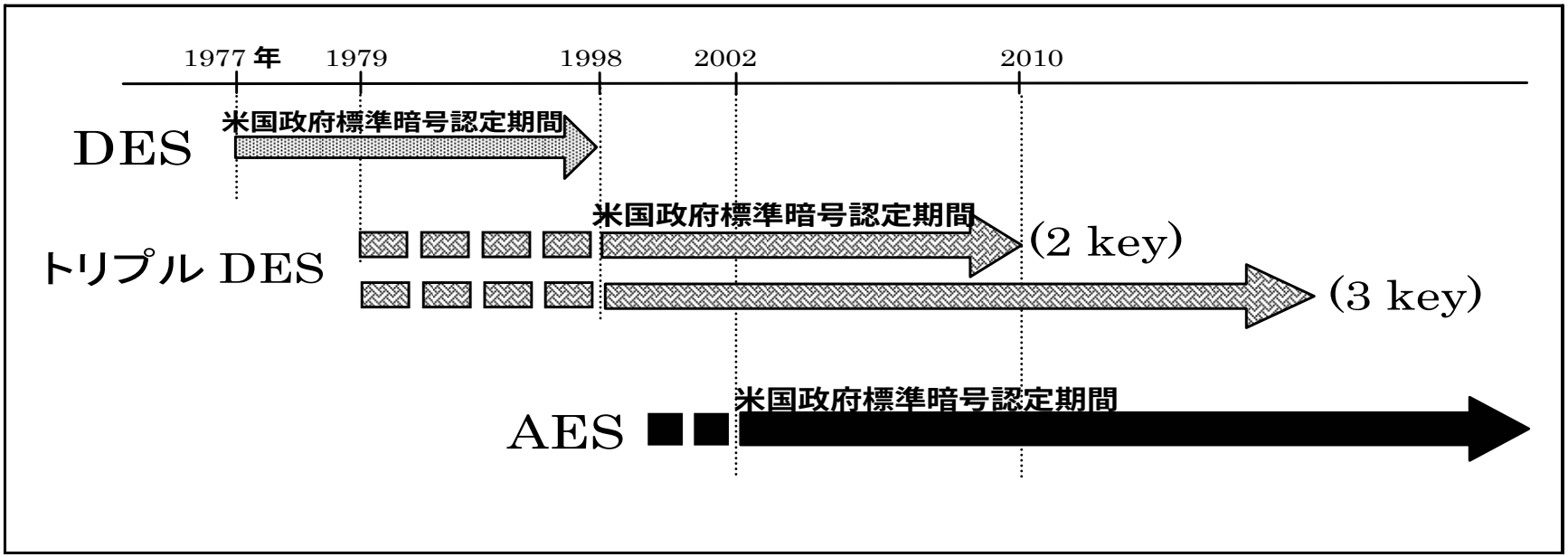
ISO/TC68における金融技術の国際標準化

国際標準化機構・金融専門委員会(ISO/TC68)は、金融分野で利用される情報通信技術の国際標準化を担当する委員会であり、預金者の安全確保、金融システムの安定のために、金融機関が採用すべき適切なセキュリティ対策等について、国際標準の審議・検討を行っている。



暗号技術の「2010年問題」

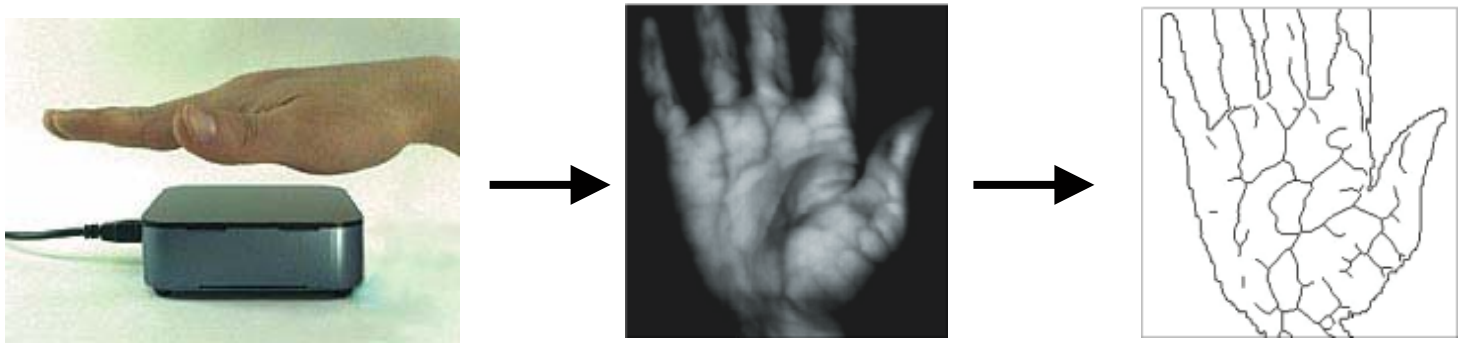
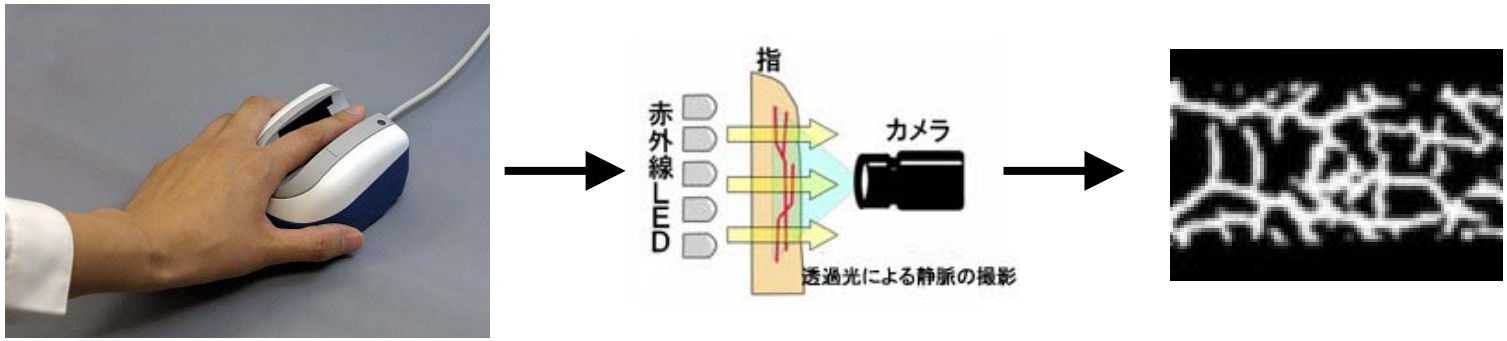
しかし、実は、ISO 9564等で利用されている現在の国際標準暗号（2key-トリプルDES、1024bit RSA、SHA-1）は、暗号技術的に見ると、既に時代遅れのものになりつつあり、2010年には、米国の政府機関による「お墨付き」が失効してしまう。こうした環境変化を踏まえて、先を読んだ対策を講じていく必要がある。



キャッシュカードとATMのセキュリティを抜本的に見直すには？（その3）

偽造対策としてキャッシュカードをICカード化したとしても、盗用までは防止できない。盗難カードによる被害を防ぐためにも、暗証番号よりも高度な本人確認手段を導入することが一案。

⇒ ICカードに加えて**生体認証**によって成りすましを防ぐ。

てのひら静脈認証	
指静脈認証	

生体認証の問題点

- 金融機関相互のCDオンライン提携と、生体認証技術間の相互運用性、互換性の問題。
- 預金取引に対する信頼を取り戻す手段として、どこまで評価できるか（膨大な導入コスト、代替手段との比較）。
- 「生体認証は究極のセキュリティ対策」というイメージが先行している一方、実際のシステムに実装した場合の、運用面を含めたセキュリティを正確に評価することが困難であるため、方針を決めかねている金融機関も多い。

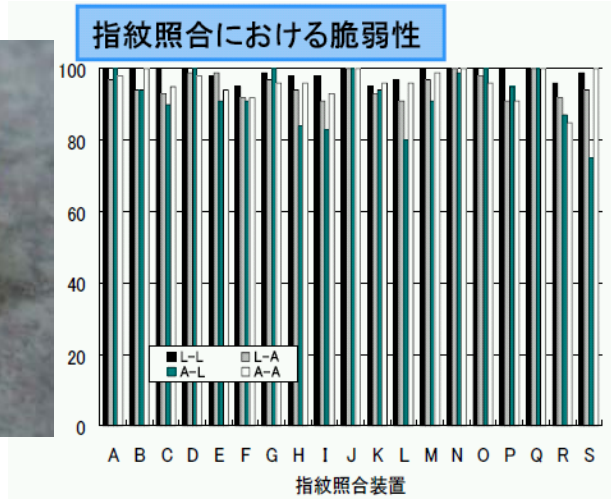
⇒ 安全性評価に対する正確な理解が必要。

生体認証を安心して利用していくために

- 生体認証による安全性を、正確に評価するための枠組み作りと、正しい理解が重要。
- 特に、生体認証を利用したシステムに固有の「身体的特徴の偽造による攻撃」に対する安全性評価と、その対策が練られる必要がある。

⇒ 生体検知機能の導入など

安価な材料で作製された人工指が、市販の指紋認証装置において高い受入率を示した



ニュース ▸キーワード：セキュリティ・ホール／生体認証／不正アクセス／不正侵入

[2005/07/01] バックナンバー

日経コンピュータ

静脈認証も安心できない？ 大根で作った偽造指で認証に成功

「静脈認証でさえ、偽造指に対するぜい弱性は否定できない」ーー。6月29日から7月1日まで東京で開催された「情報セキュリティEXPO」で、セミナーの演壇に立った横浜国立大学の松本勉教授はこう警告した。偽造/盗難キャッシュカード対策として金融業界で急速に普及しつつある静脈認証について、客観的なぜい弱性評価の必要性を示したものだ。

大根で作った偽造指

キャッシュカードとATMのセキュリティを抜本的に見直すには？（その４）

CD/ATM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。

情報セキュリティ対策の選択の難しさ

従来は、「カードは偽造しにくく、暗証番号も漏洩しない」という立場

↓

「暗証番号の漏洩がありうる」 ⇒ カードを偽造しにくくすれば良い ⇒ ICカード化

↓

「ICカードも偽造される可能性がある」 ⇒ 認証方式の高度化、ハードウエアの改良

↓

「カードの盗難にも対処しなければならない」 ⇒ 生体認証の利用

↓

「生体認証も偽造される可能性がある」 ⇒ 生体検知機能の付加

――― こうした対策について、どの段階まで対応することが適当か、実際に犯罪が発生するリスク、ビジネスとしての採算性、レピュテーション上の問題等を考慮して、各金融機関が立ち位置を定めていく必要がある。

――― その場合、「望ましい対策のあり方」の基準をどこに求めるべきか？

――― こうした観点からは、（相対的に金融機関をターゲットとしたハイテク犯罪の事例の多い）海外の金融機関における取り組み事例や、金融機関のセキュリティ対策に関する国際標準が参考になる。

利用者の協力を得ることは不可欠

- セキュリティ対策は足し算ではなくて**掛け算**で効いてくる。
  ―― 金融機関側が万全の対策を講じていても、利用者の不注意により被害が発生し得る。逆に、利用者が細心の注意を払っていても、万一、金融機関側の対策に見落としがあり、それが突かれれば被害が発生し得る。
  ―― このため、セキュリティ対策には利用者の協力が必要。もし、利用者が「金融機関なら補償してくれるから」という認識でいると、いずれは行き詰ってしまう。
- ①セキュリティ・レベル、②利用者の管理負担、③システム構築コストには、**トレードオフ**の関係がある。
  ―― 金融機関がビジネスとして金融サービスを提供する以上、システム構築コストには限界があるのだから、利用者にも一定の管理負担を求めていかないと、必要なセキュリティ・レベルを確保できない。
- 預金者保護法の下で、**利用者に適切な管理負担を担って貰えるようなルール作り**が、今後の重要な論点となる。

3. インターネット・バンキングのセキュリティを巡って

インターネット・バンキングにおける利用者認証の変遷

最近のインターネット・バンキングの利用者拡大の背景には、利用者認証方式が、複雑なものから簡便なものに変更されたことがある。

1997年頃　SET/SECEを利用したインターネット・バンキングの開始

比較的厳格な利用者認証方式を採用していたが、利用者が専用のソフトウエアをパソコンにインストールしたり、公開鍵証明書を取得してパソコンに組み込んだりするための作業負担が大きく、あまり普及しなかった。

2000年以降　SSL＋パスワード認証方式が登場

パソコンにあらかじめ組み込まれている暗号プロトコル（SSL）とパスワードを組み合わせて認証を行うSSL＋パスワード認証方式が主流となり、急速に普及した。

更に、最近のインターネット・バンキングでは、認証手段を二重化し、ログイン用のパスワードに加えて、特に重要な取引に関する操作については乱数表によるチャレンジ・レスポンス方式による認証が導入されることが多くなっている。

SSL＋パスワード認証方式

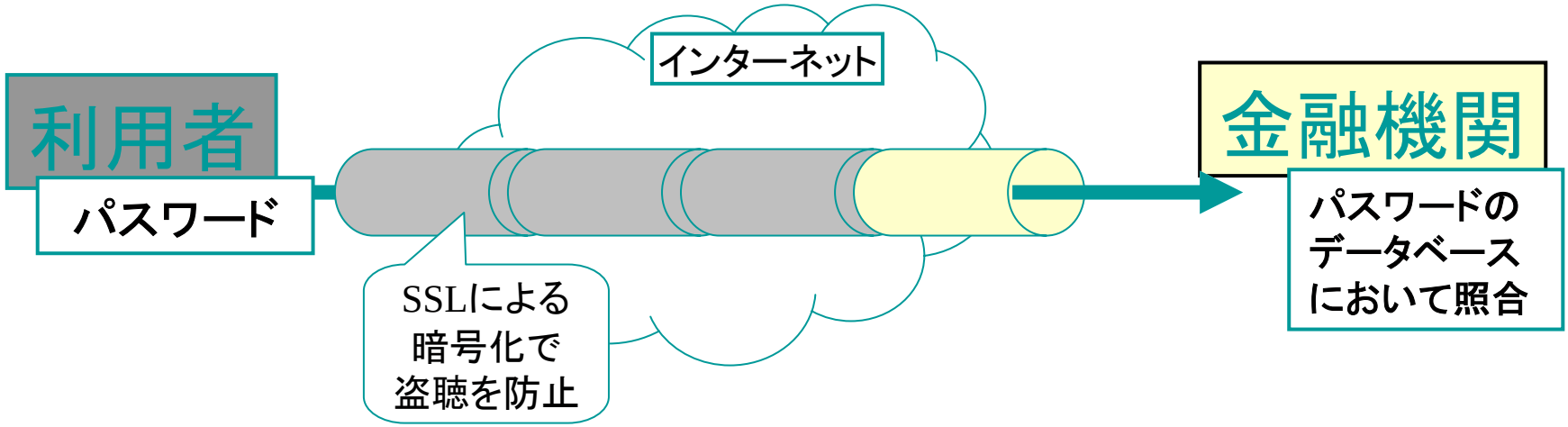
ある金融機関のホームページにおける説明：

【128bit SSL暗号化技術の採用】・インターネット通信時に128bit SSLという強力な暗号化技術を採用し、お客さまの重要な情報を保護しています。

128 bit SSL …SSLは、守秘や認証のためのさまざまな機能を有しているが、多くのインターネット・バンキングでは、暗証番号やパスワードの盗聴を防ぐための守秘機能のみが使われている。

→ 金融機関側における利用者認証はパスワードのみによって行われる

→ 利用者側における金融機関サーバーの確認には、サーバー証明書が使われているものの、それが有効に確認されるか否かは、利用者のリテラシーに依存する。



SSL＋パスワード認証方式の問題点

「SSL＋パスワード認証」は、インターネット・バンキングにおいて、無権限者による成りすましなどの攻撃を防止し、正規の利用者や金融機関自身に損害が生じる事態を回避するうえで、十分なセキュリティ対策とはいえないのではないか。

暗証番号・パスワードに対する基本的な攻撃

①考えられる全ての番号を試してみる（4桁なら、0000～9999まで1万通り）。
②パスワードに良く使われる単語を辞書から選び、次々に試してみる。

インターネット・バンキングの特殊性

①世界中からアクセスが可能なため、**不正行為の監視が難しい**。
②コンピューターに指示して**大量の試行を繰り返させる**ことができる。

→　従来、金融機関の店舗内で金融サービスを提供していた頃には問題とならなかった攻撃が、現実的な脅威となる。

金融機関側のシステムで、パスワード相違の認証エラーが一定回数を超えると入力を制限するといった防御機構が採用されている場合は？

→　様々なIDとパスワードをランダムに組み合せて大量の試行を行えば、防御機構を回避してIDとパスワードの組み合せを推定できてしまう可能性がある。

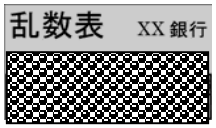
乱数表によるチャレンジ･レスポンス方式

利用者

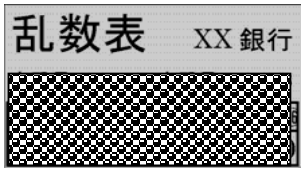
①インターネット経由で金融機関のホームページにアクセスし、SSL で保護された通信経路からログイン用の固定パスワードを入力する。

③資金振替指図を入力する。

⑤乱数表を参照し、チャレンジに対するレスポンス（位置に対応する乱数表の数値）を入力する。



⑦結果通知を確認する。



インターネット

チャレンジ（⑤⑬⑨①）

レスポンス（9,9,4,3）

金融機関

予め乱数表を作成し、利用者に郵送しておく。

②ログイン用の固定パスワードを認証し、システムへのアクセスを許可する。

④チャレンジ（乱数表における位置）をランダムに生成して送信する。

⑥当該利用者の乱数表データを照合し、チャレンジ・レスポンスの一致を確認する。認証に成功すれば、資金振替指図を処理し、結果を通知する。

乱数表によるチャレンジ・レスポンス方式の問題点

乱数表を導入する理由：ある取引における認証データ（チャレンジと利用者のレスポンス）が何らかの理由で漏洩してしまい、攻撃者に察知されたとしても、他の取引の認証におけるチャレンジが、漏洩したチャレンジとたまたま一致する確率は低いため、攻撃者による成りすましが困難となる、という効果を期待したもの。

しかし、

1．　金融機関側のシステムにおいて、攻撃者が取引入力のキャンセルを繰り返すことによって、自分にとって都合のよいチャレンジが出るまで「チャレンジの出させ直し」を行うことが可能な仕組みとなっていた場合、**１回の取引における認証データが漏洩しただけで成りすましが可能となってしまう**危険性。

2．　攻撃対象者を次々に変更しながら当て推量の入力を繰り返す攻撃により、認証エラーが一定回数を超えたら入力を制限するという防御機構を回避して、**乱数表の一部のデータを推定できてしまう**危険性。

などが指摘されている（松本勉・岩下直行、「インターネットを利用した金融サービスの安全性について」、『金融研究』21巻別冊１号、2002年）

- 最近、インターネットバンキング、ファームバンキングの利用者を、フィッシング、スパイウエア、キー・ロガー等によって陥れ、パスワードを盗み取ろうとする事件が相次ぎ、実際に不正送金による被害も発生している。
- そもそも、「パスワードが漏洩してしまうと、巨額の不正送金が可能となる」という**システムの仕様自体が問題**。こうした仕様は、フィッシング等の手口が現れる以前に考案されたものであり、新たな脅威を防ぎきれていない。
- 海外の金融機関の中には、利用者に**ワンタイム・パスワード生成機**を配付している事例もある。わが国においても、より抜本的な対策が必要ではないか。

４．金融機関のセキュリティに対する信頼を取り戻すために

対処していかなければならない問題

① 海外では、**暗証番号（PIN）はATMで暗号化**することが一般的だが、日本では暗号化は必須とは考えられていない。これについては、海外のクレジットカードブランドからの批判もあり、国内でも暗号化を実施している金融機関が出てきている。

② 現在、回線暗号やICカードで一般的に使われている暗号アルゴリズムは、**あと5年で安全性の保証が切れる**見込み。

③ キャッシュカードをICカード化し、生体認証を導入しても、それに対応していない磁気ストライプを利用したキャッシュカードは引き続き大量に流通しており、**スキミング犯罪の芽は摘まれていない**。

④ 生体認証技術については、生体情報の偽造を用いた攻撃法の存在が指摘されているが、**中身がブラックボックス**のため、どのようなリスクがあるのか評価が難しい。

⑤ インターネットバンキングやファームバンキングは、フィッシングやスパイウエアによって**暗証番号や乱数表情報の一部が漏洩**し、不正な送金が行われるリスクが一部で顕現化している。

金融機関のセキュリティに対する信頼を取り戻すためには、どうしたらよいのか

- 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た以上、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である。
- とはいえ、現在、金融機関の抱えている情報セキュリティ上の問題点は多方面にわたっており、巨額の投資費用を要したり、業界内の調整に時間を要するものも多く、一朝一夕に対応することは難しい。
- セキュリティ対策にどれだけの金額を投資するかという判断とは別に、**採りうる対策の有効性**についての**詳細な評価**が必要。その上で、各金融機関は、情報セキュリティ上の要請を自ら判断し、それを**ビジネスとの折り合い**をつけながら実施していくことが必要とされている。
- また、これらの対策については、**業界全体として**取組んでいかなければ実効性の得られないものも多い。業界内で話し合いを進めていくための共通認識を固めていくことが大切。

海外・他業態の動向

フランス: 国を挙げてICカード化に取り組んだ結果、国内の銀行取引カードを全てICカード化することに成功

ドイツ: 磁気カードに独自の偽造防止技術を組み入れることによって、スキミングの被害を抑制

米国: 金融業界を挙げて、情報セキュリティ技術の検討と実装を推進。業界内で脆弱性情報を検知、共有する仕組みとして、FS/ISAC(Financial Services/ Information Sharing and Analysis Center)と呼ばれる組織を設立している。

国内の他業態の動向: 情報通信業界が、2002年7月にTelecom-ISAC Japanを組成し、活動を開始。

専門家の育成と業界内の体制整備

- 海外では、暗号技術、ICカード等について、「金融機関が採用していること」が信頼の証とされているが、日本ではどうか。金融機関は、そのように認識されるだけの「**情報セキュリティ技術に対する眼力**」を持っていると認識されているだろうか。
- 各金融機関は情報システムを適切に運行していくために、情報セキュリティ技術の検討・分析に一定の経営資源を割り当て、**専門家を育成**していくことが必要。そうした専門家の評価に基づいて、情報システムのセキュリティ対策に戦略的に対応していくことが必要である。
- 各金融機関の対応と並行して、金融業界全体にかかわる情報セキュリティ問題に対処するため、**業界内で適切に情報を共有**する体制を整備・強化していくことが求められている。