資料4

情報セキュリティの観点から考える金融ITの将来像

日本銀行 金融機構局
金融高度化センター長
岩下 直行

本資料の内容や意見は発表者個人に属します。
日本銀行あるいは金融機構局の公式見解を示すものではありません。

目次

１．なぜ今、金融ITの改革が必要なのか

1-1. 日本銀行金融機構局金融高度化センターの取り組み

ITを活用した金融の高度化に関するワークショップを開催

2014年11月11日
日本銀行金融機構局
金融高度化センター

金融高度化センターでは、2014年10月9日、日本銀行本店にて、「ITを活用した金融の高度化に関するワークショップ（第1回）」を開催しました。

金融分野では既に幅広くITが使われていますが、今後より戦略的にITを活用し、金融を一層高度化していくことが求められています。金融の最前線でIT活用に取り組まれている方々とこれからの見通しや課題について議論する目的で、本ワークショップを開催しました。

1－2．銀行にとってのITとイノベーション

① 金融業界は1970年代の第一次銀行オンラインシステムの時代から、ITを重要な経営資源と位置付けてきた。

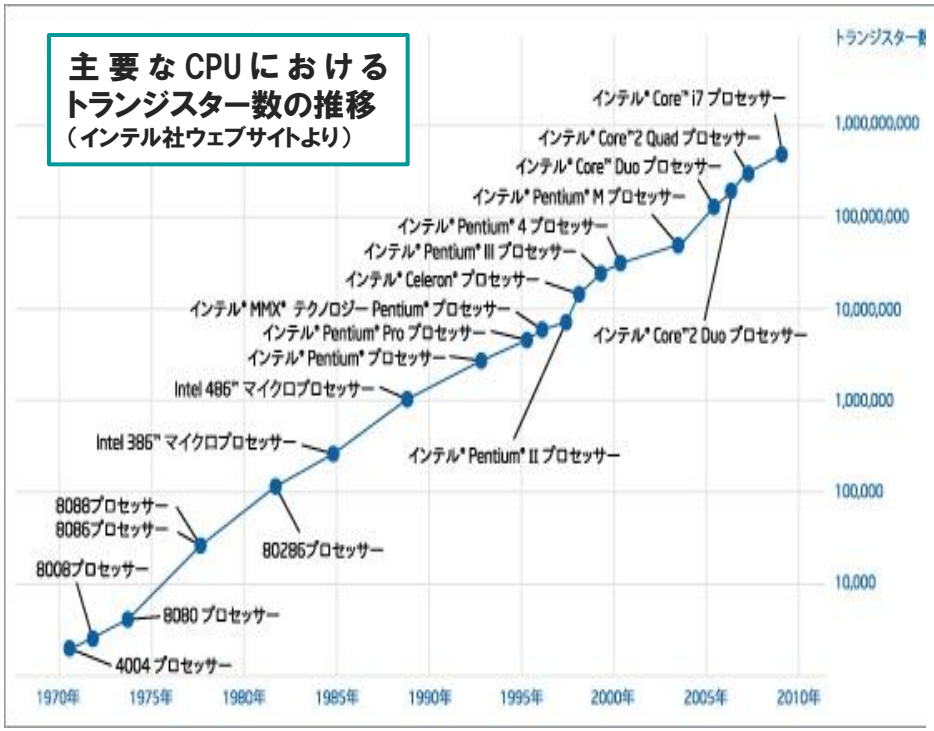
② しかし、銀行の業務の現場では、本来ITが持つ力が十分に発揮されていないと指摘されている。

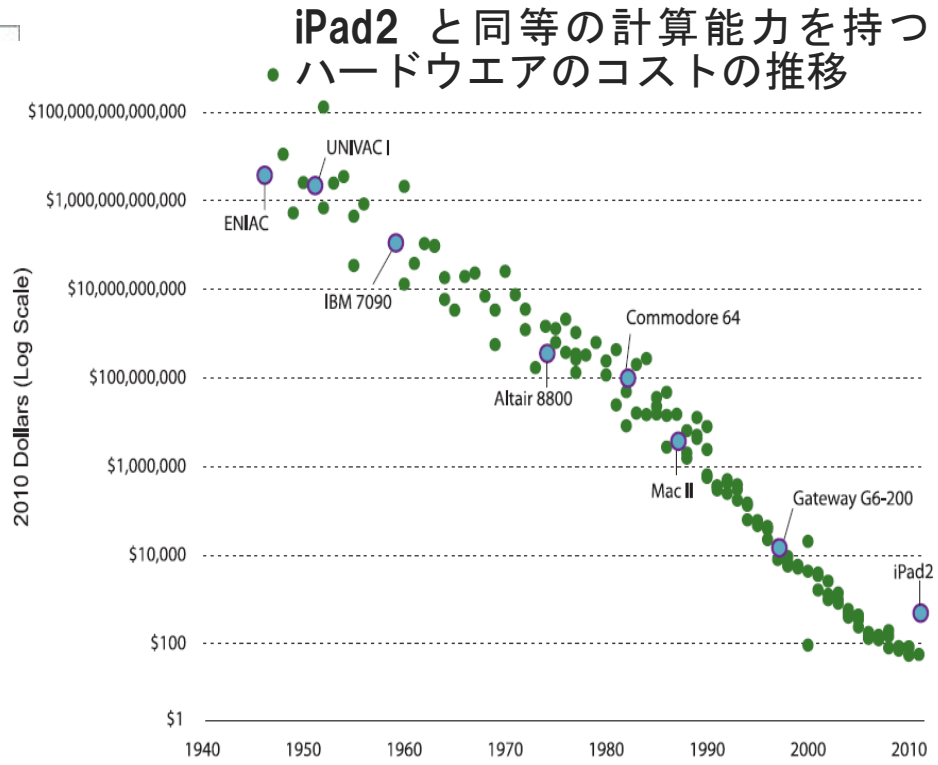
③ 堅牢性や高度な可用性を誇る銀行の情報システムは、半面、柔軟性が乏しく、維持管理や制度対応に多大なコストと時間を要する。

④ 本来、ITは業務の現場におけるイノベーションの手段として利用されるべきもの。しかし、銀行のITは、むしろイノベーションを阻害する一因となっているのではないか、という指摘もある。

1-3. ムーアの法則

ムーアの法則：「半導体の集積度は18か月で2倍になる」という経験則。この法則は数十年にわたって観察され、コンピュータのハードウエアのコスト・パフォーマンスは年を追うごとに改善している。





出典：Michael Greenstone and Adam Looney, "A Dozen Economic Facts About Innovation," HAMILTON PROJECT POLICY MEMO, 2011.

1-4. ムーアの法則が働かない金融IT

しかし、金融ITの現場の実感としては、劇的なコストの低下も、性能の劇的な向上も起きていないように感じられる。これは一体なぜか。

ひとつの答え：「銀行が先にIT化に取り組み、それを完成させてしまったから」

1970-80年代　銀行のIT化が他の業界に先行し、その時代において高い完成度を達成

1990年代以降　インターネットが爆発的に普及し、ハードウエアのコスト・パフォーマンスも向上

⇒「普通のIT」と「金融IT」とが乖離することに。

1-5. 金融ITの変革を

銀行が急速なITの進歩に置いてきぼりをくった状況が長く続いてしまうと、

① 銀行が利用するシステム技術基盤、

② 銀行のITガバナンス体制、

③ 銀行の業務推進体制

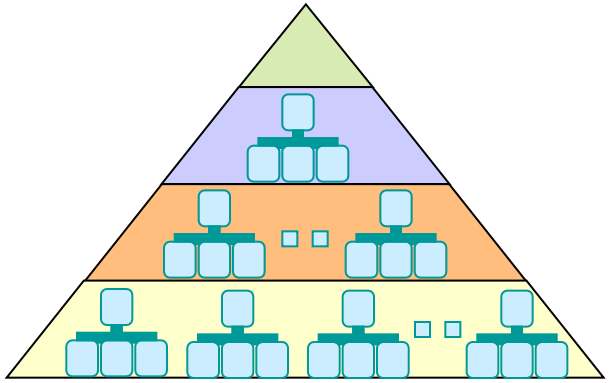
が、古いITシステムを前提としたものに固定化してしまい、金融ITの変革を阻むことになる。

これらを解きほぐしつつ、銀行の情報システムの安定性、安全性を確保した上で、銀行の経営課題を効率的かつスピーディに解決していくためにも、金融ITを改革していくことが必要である。

2．金融ITの現状と課題

2-1. 現在の金融ITの特徴

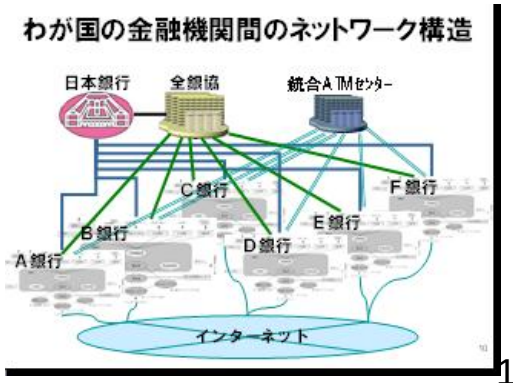
① 各銀行、集中決済機関によるセキュリティ・ドメイン毎に、分断された閉域のネットワークが構築され、それがピラミッド型に積み重なった構造。



② 通信速度が低速であった時代のシステムの基本構造を継承しているため、通信電文フォーマットは短い固定長を基本とし、できるだけ通信ネットワークに負荷をかけない仕組み。新機能は端末に限定して付加される。

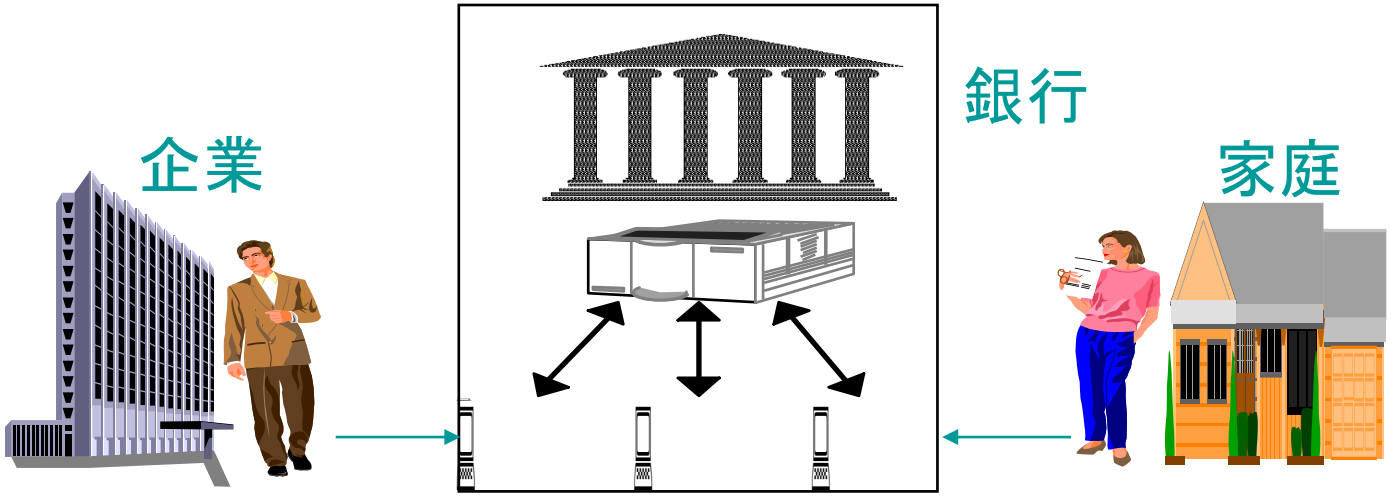
項番	カラム位置	桁数	項目
1	1	1	データ区分
2	2～3	2	持込種別コード
3	4	1	コード区分
4	5～14	10	会社コード
5	15～54	40	依頼人名
6	55～58	4	振込指定日（月日）
7	59～62	4	仕向金融機関コード
8	63～77	15	仕向金融機関名
9	78～80	3	仕向店舗コード
10	81～95	15	仕向店舗名
11	96	1	依頼人預金種目
12	97～103	7	依頼人口座番号
13	104～120	17	空きエリア

③ 外部接続先を（主として）金融業界内に限定することによって、セキュリティ侵害のリスクを低下させ、万一問題が発生した場合の責任分担を明確にしている。逆に、一般利用者との接続による新しいサービスの提供には不向き。



2-2. わが国の従来の決済システムの構造

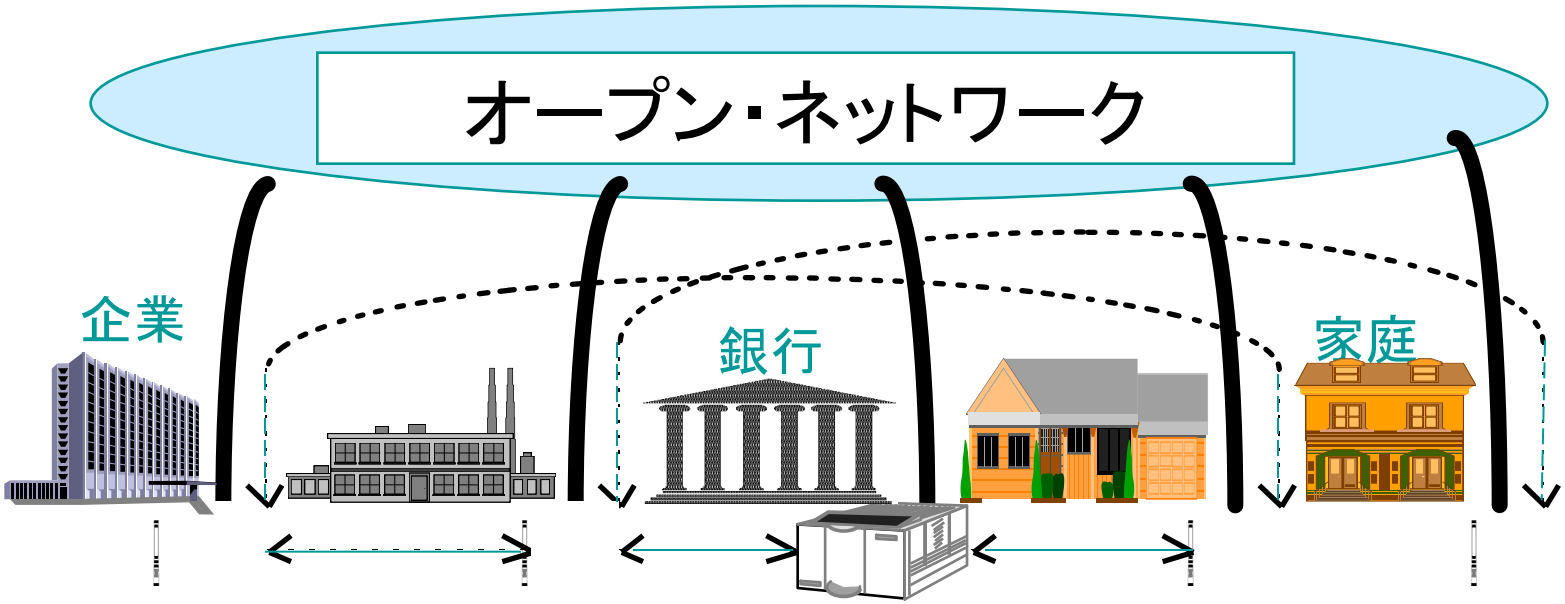
- 従来のポリシー:「外部からの隔離によるセキュリティ」
- 銀行の内と外とを隔離し、コンピュータ・システムに対する外部からの攻撃を困難にする作戦。隔離壁の内側では、比較的シンプルな認証手段を採用し、利便性、効率性を重視する傾向にある。
- 銀行外部のシステムとの連動はあまり想定されていない。



2-3. 情報技術の発達に伴い、従来の前提が崩れてきている

例：STP化、金融EDI、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、決済システムを含む様々なシステムが相互に連動することを前提に、銀行システムの基本設計を考え直す必要が生じている。



・水平型　・開放型（ｵｰﾌﾟﾝ・ｼｽﾃﾑ）　・分散ｼｽﾃﾑ

3. 偽造キャッシュカード問題から10年を経て

3-1. 10年前に日本で起こったこと

2004年～2005年初: 偽造キャッシュカードによる不正預金引出が急増し、社会問題化。金融機関の情報セキュリティ対策に関する世間の関心が高まる。

2005年2月: 金融庁・偽造キャッシュカード問題に関するスタディグループ発足。

2005年6月: スタディグループ報告書公表。

2005年8月:「偽造・盗難カード預貯金者保護法」公布。

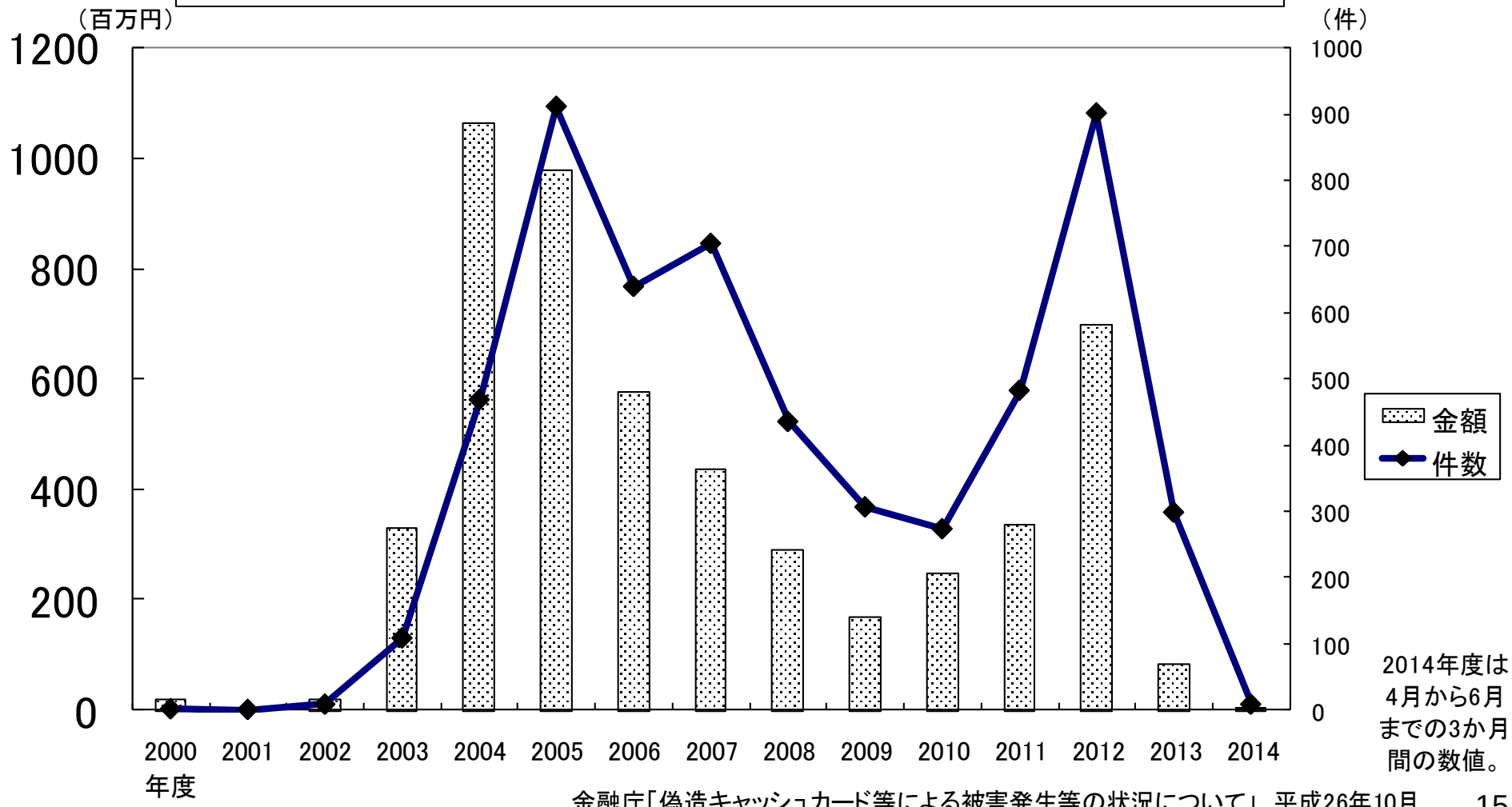
2006年2月10日: 同法施行。

⇒ 偽造・盗難カードによる不正預金引出に伴う被害については、原則として金融機関が被害者に補償を行うことになった。

⇒ その後、多くの銀行が希望者を対象にICカードや生体認証を導入し、ATMの改造も進めたものの、その普及は一部にとどまり、現在も磁気ストライプカードと4桁暗証番号が広く利用されている。

3-2. 偽造キャッシュカードによる預金等不正払戻し

偽造カード問題の根は絶たれていないため、2008年頃に問題が一旦沈静化した後も再び被害が増える局面があったが、2013年以降は件数、金額とも激減している。

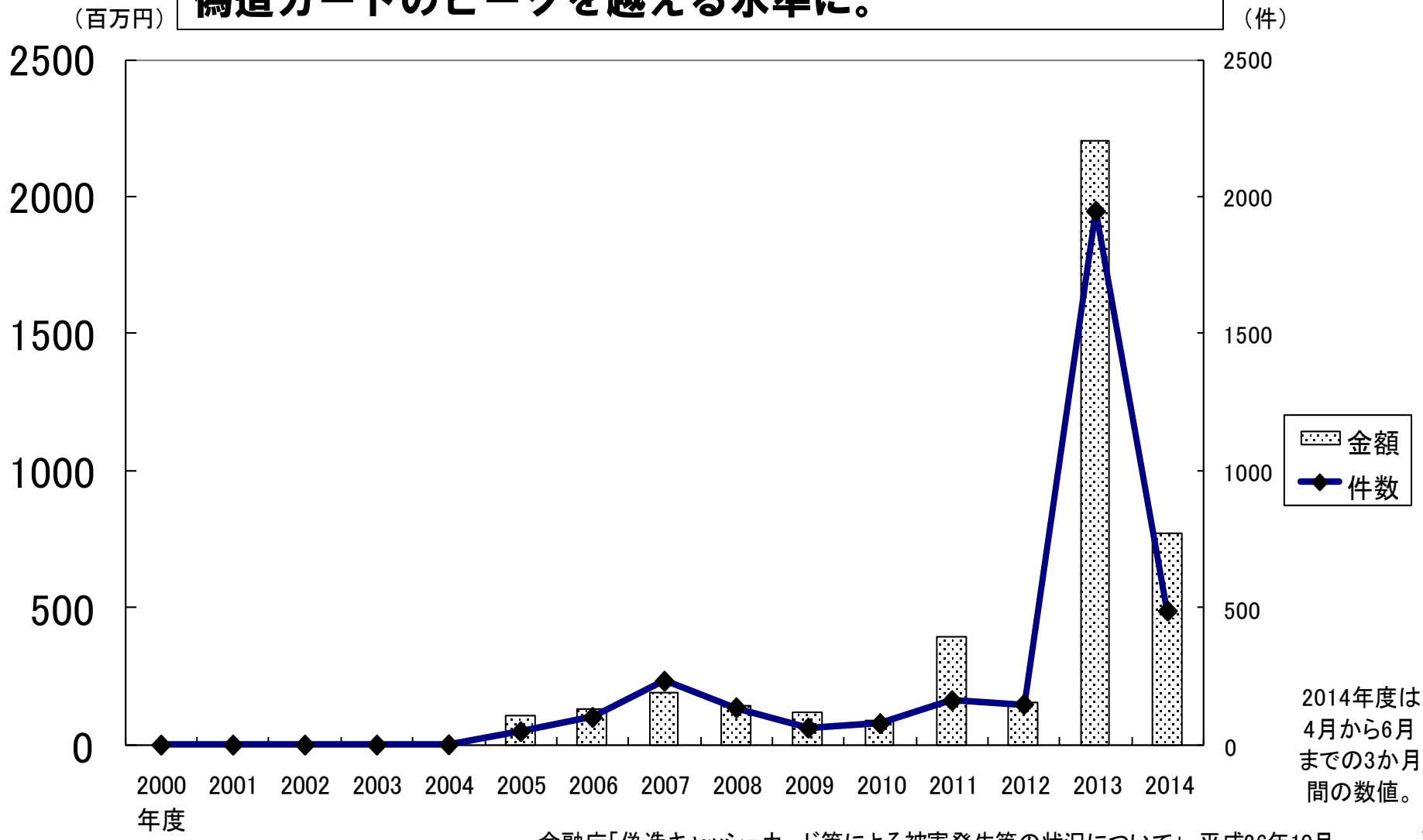


2014年度は4月から6月までの3か月間の数値。

金融庁「偽造キャッシュカード等による被害発生等の状況について」、平成26年10月

3-3. インターネットバンキングによる預金等不正払戻し

2013年以降、偽造カードの被害が沈静化する一方で、インターネットバンキングの被害が急増し、被害額は偽造カードのピークを越える水準に。



金融庁「偽造キャッシュカード等による被害発生等の状況について」、平成26年10月

4. 米国におけるクレジットカード番号漏洩問題との比較

4-1．10年前に米国で起こったこと

インターネット上で利用されるクレジットカード番号の漏洩、不正使用が急増。

2004年から2005年にかけて、クレジットカード決済業務請負業者であるCardSystems社のシステムが不正侵入を受け、同社のサーバーに保存されていたカードの所有者、アカウント番号、有効期限などのデータが4000万件以上流出。過去に例のない大規模な漏洩事件であったため、大きく報道され、社会問題化した。

2004年12月、クレジットカードの国際ブランド5社が共同でセキュリティ基準「PCI DSS」を策定。加盟店や決済代行事業者がこれを採用し、審査機関による審査を受ける仕組みが徐々に定着。

PCI DSS（Payment Card Industry Data Security Standard）

…情報セキュリティに対する具体的な実装を規定したセキュリティ基準。例えば、暗証番号の入力装置における暗号化については、ISO 9564等の既存の標準が引用され、その順守が求められている。

⇒ しかしその後も、大規模なカード番号漏洩事件が頻発 している（Heartland Payment Systems社<2009年>、TARGET社<2013年>、Home Depot社<2014年>）。

4-2. 銀行ATMのセキュリティに対する指摘

- 日本でも、クレジットカード業界では、PCI DSSが普及しつつある。クレジットカード業界から、日本の銀行ATMで国際クレジットカードを利用する場合(注)のセキュリティについて、以下のような指摘を受けることがある。この指摘は妥当なものなのだろうか。

> 日本独自仕様の銀行カードとATMには、もう一つ問題がある。国際ブランドのカード会社や決済ネットワーク会社が接続の条件として求めている国際セキュリティ基準を満たしていない点である。日本のATMの通信暗号化処理は国際的に見て極めて脆弱であり、海外の金融機関と比べて情報漏えいなどが起きやすい状態にある。発展途上国の金融機関の国際対応ATMよりもセキュリティ水準が低い危険な状態といえる。
>
> 「キャッシュレス革命2020」 p182

（注）「日本の銀行ATMで国際クレジットカードを利用する」ことの是非やその対応方法については、本件とは別の観点から検討が必要である。

4-3. 銀行ATMのセキュリティを立証できるか

- 国際クレジットカード取引では、暗証番号(PIN)は取引認証の瞬間のみに利用されるべきものと考えられており、それを端末側で保存することはセキュリティ上のルールとして禁止されている。PCI DSSやISO 9564といった国際標準は、これを担保するために、PINを装置に入力した瞬間に暗号化することを規定しており、そのための専用機器が広く利用されている。
- これに対し、日本の銀行ATMについては、そのような明文の規定はない。銀行システム一般において、暗証番号のような機密情報を保存する場合には暗号化すべしというルールはあるものの、それをATMの内部でどのように適用するかは実装側に任されている。過去に、内部者が関与したセキュリティ侵害において、銀行ATMのログからPINが復元されてしまった事件があったが、そういう作りとなっていること自体が、欧米のルールでは容認されないことである。
- 実際には、日本の銀行ATMにおいても暗証番号は極めて慎重に取り扱われており、外部に漏洩することはほとんど考えられない。とはいえ、そうであることを外部に立証することは容易ではないだろう。

4-4.「秘匿によるセキュリティ向上」からの脱却を

- こうした問題を回避するためには、業界内でできるだけ具体的な標準仕様を定めてそれを公開し、その標準に基づいてシステムを構築していくことが望ましい。
- 従来、日本の銀行システム開発においては、その内部構造を外部から秘匿することが、セキュリティ確保のために大切と考えられていた。それは、「秘匿によるセキュリティ向上（security through obscurity）」と呼ばれる古い考え方である。むしろ積極的に、外部からも参照できる具体的な標準仕様に準拠していくことが、安全性を外部にアピールする際にも説得的である。
- 日米でほぼ同時に発生したセキュリティ侵害事件への対応は、両国で対照的な取り組みとなった。必ずしも米国が上手に問題を解決したわけではないが、業界で技術標準を策定してそれを順守していくという対応には、学ぶべき点が多くあるように思う。

5. ネットバンキングの認証手段にみる金融ITの可能性

5-1. インターネットバンキングの認証手段の変遷

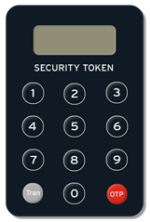
- インターネットバンキングのセキュリティ対策については、攻撃手口の高度化と被害額の急増を受けて、利用する認証手段を早急に見直していかなければならない状況にある。
- 単純なパスワードや乱数表による本人認証は、フィッシングやウィルスによる情報盗取の被害を受けやすいため、より高度なセキュリティ対策に変更していくことが必須となっている。

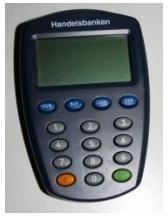
- 単純な情報盗取への対策として、OTP（ワンタイムパスワード）による本人認証が増えつつあるが、ウィルス感染によるMitB（Man in the Browser）攻撃を想定した場合、それでも十分ではない。

- このため、MitB攻撃への耐性が高く、諸外国でも実装が進んでいる「トランザクション認証」の必要性が高まってきている。

5-2. OTPからトランザクション認証へ

「トランザクション認証」…口座振替等の銀行取引を起動する都度、利用者が電卓型のセキュリティトークンを操作するなどして取引内容を入力し、それによって生成した認証子を添付して取引電文を送信する仕組み。利用者ごと、取引の内容ごとに異なる認証子が生成されて取引電文に添付されるため、電文が送受信されるネットワーク全体を信頼することが難しいとしても、銀行は、取引電文がその利用者によって生成されたと信頼することができる。





- 従来の銀行システムとインターネットとの接点であるインターネットバンキングにおいて、こうした新しい安全対策の必要性が高まっていることは注目に値する。それは、将来的には、銀行システムのセキュリティの基本設計に影響を与え得るものだからである。

5-3. 新たな認証手段は銀行システムの自由度を上げるか？

- 従来の銀行システムは、独自のネットワークを銀行本支店間および銀行業界内とのみ接続することによって、外部からの攻撃を遮断してきた。こうした基本設計の下では、暗証番号やパスワードといった素朴なセキュリティ対策で十分と考えられた。その結果、システム開発のコストを抑制し、顧客利便性の確保に寄与してきた一方、銀行システムが外部のネットワークと接続することを困難にしてきた。
- インターネットバンキングも、当初は顧客のパソコンまでの領域を安全な接続領域と想定し、素朴なセキュリティ対策を採用していた。しかし、不正送金を企てる攻撃者側の技術が進化した結果、「外部からの隔離によるセキュリティ」を徹底することが困難になり、取引毎の認証という新しい技術による解決が必要となった。
- こうした技術を採用することを前提とするのであれば、銀行取引において、より自由な外部のネットワークとの接続が可能になるかもしれない。

6. 今後の展望

6-1. オープンなネットワークに対応していくために

- インターネットを中心に電子商取引が拡大し、新たな決済手段の利用が拡大しているが、この分野における銀行の存在感は希薄である。銀行はセキュリティ上の理由から、電子商取引やEDIといった一般のインターネット上の取引データを、そのまま銀行システムの内部に取り入れて活用することができていない。かといって、ネットワークを開放すれば、現在の基本設計の下ではセキュリティが維持できないというジレンマに陥る。
- インターネットバンキングにおいてトランザクション認証の仕組みが必要とされているように、取引ごとの認証機能を高度化すれば、こうした問題に対処できる可能性がある。
- 2001年に電子署名法が成立し、個々の取引電文に安全な電子署名や認証を付与するための技術的、制度的基盤は整備されていると言えるが、それらが金融の実務において広く活用されることはこれまでなかった。それは、銀行システムのセキュリティを守る手段として、電子署名や電子認証ではなく、「外部からの隔離」が採用されてきたからである。

6-2. 新たな認証手段が生み出すもの

- 銀行システム全体を隔離するのではなく、メッセージの内容と認証技術によって預金者の意図が確認できるようになれば、銀行がコストを掛けて守る領域を限定することも可能になる。設計思想次第では、銀行システム全体をより身軽なものに置き換えられるかもしれない。
- トランザクション認証のためのセキュリティトークンを現在のキャッシュカードのように普及させることができれば、ATM取引の安全対策を高度化することにも利用できる。
- 電子署名の仕組みをユーザー側に整備させたり、電子認証のためのセキュリティトークンを配布したりすることはコストがかかる。しかし、ムーアの法則により、その費用は年を追うごとに低下する。
- 中長期的な視点からみると、銀行システムのセキュリティの基本設計は、こうした方向に変わっていかざるを得ないと思われる。こうした変化に対応して銀行システム全体をより効率的なものに見直していくことが、今後の大きな課題となると思われる。

6-3. マイナンバー制度との関係

- 2015年中にはマイナンバーが全国民に配布される予定であるが、制度開始当初は、銀行預金は付番対象にはなっていない。しかし、政府税調・マイナンバー・税務執行ディスカッショングループの報告書により、将来的には、マイナンバーを預金口座に付番していくことが提案されている。
- 将来の制度対応を見据えて、銀行と預金者とを繋ぐ新たなデバイスの導入を検討する価値があるのではないか。