【特集】

続・決済システム高度化の焦点

政府・自民党からの問題提起を受けて、金融界は現在、国内送金の24時間365日化、送金電文と一緒に送る請求情報等の大容量化に向けた検討を進めている。背景には、インターネットの普及に伴う人々の生活やビジネスの変化に、金融機関の決済サービスが追いついていないという指摘がある。日常的には預金・貸出に焦点があたることが多いが、決済機能は金融機関の最後のよりどころといっていい。決済サービスが変われば、金融機関のシステムが変わり、金融機関のあり方も変わっていくだろう。

銀行の情報システムの新しい設計思想

情報セキュリティの観点から考える金融ＩＴの将来像

「半導体の集積度は18カ月で2倍になる」（ムーアの法則）。しかし、銀行がその恩恵を十分に受けているようには思えない。その原因は、銀行界がいち早くＩＴ化に取り組み、閉鎖的なネットワークを前提とした情報システムを完成させたため、インターネットを前提とする技術進歩からおいてきぼりをくってしまったことにあると考える。オープンネットワークを前提としたセキュリティ思想を取り入れることは、銀行の情報システム全体の効率化につながる。

日本銀行金融機構局
審議役・金融高度化センター長
岩下　直行

決済サービスの高度化を巡って

アップルペイやペイパル、スマホ決済など、インターネットを利用した決済サービスの技術革新が相次ぐなかで、わが国の銀行の決済サービスの高度化に関する議論が盛り上がってきた。その根底には、新しい便利な決済サービスがインターネット経由で普及すると、わが国の銀行が提供してきた伝統的な決済サービスが利用されなくなるのではないか、そうした取引が主流になった将来には、銀行が現在の立場をとって代わられてしまうのではないか、という危機感がある。

わが国の銀行は大変早くから、ＩＴを重要な経営資源と位置付けてきた。１９７０年代の第１次オンラインシステムに始まり、累次にわたる銀行のシステム更新が社会的な注目を集めた。一般の理解では、銀行はすでにＩＴを幅広く活用していると受けとめられている。他方、銀行の情報システムでは、本来ＩＴがもつ力が十分に発揮されていないと指摘する声も根強い。

堅牢性や高度な可用性を誇る銀行の勘定系システムは、反面、柔軟性が乏しく、現場のニーズの変化に迅速に対応できない、あるいはシステムの維持管理や

制度対応に多大なコストと時間を要する、といった問題が指摘されている。

ＩＴは企業の経営戦略におけるイノベーションの手段として利用されるものなのだが、銀行にとってのＩＴは、むしろ経営戦略を制約し、イノベーションを阻害する一因になっている感さえある。そうした状況を改善するためにも、決済サービスの高度化への取組みをきっかけとして、銀行の情報システム全体を見直していくことが必要なのではないだろうか。

ムーアの法則が働かない銀行界

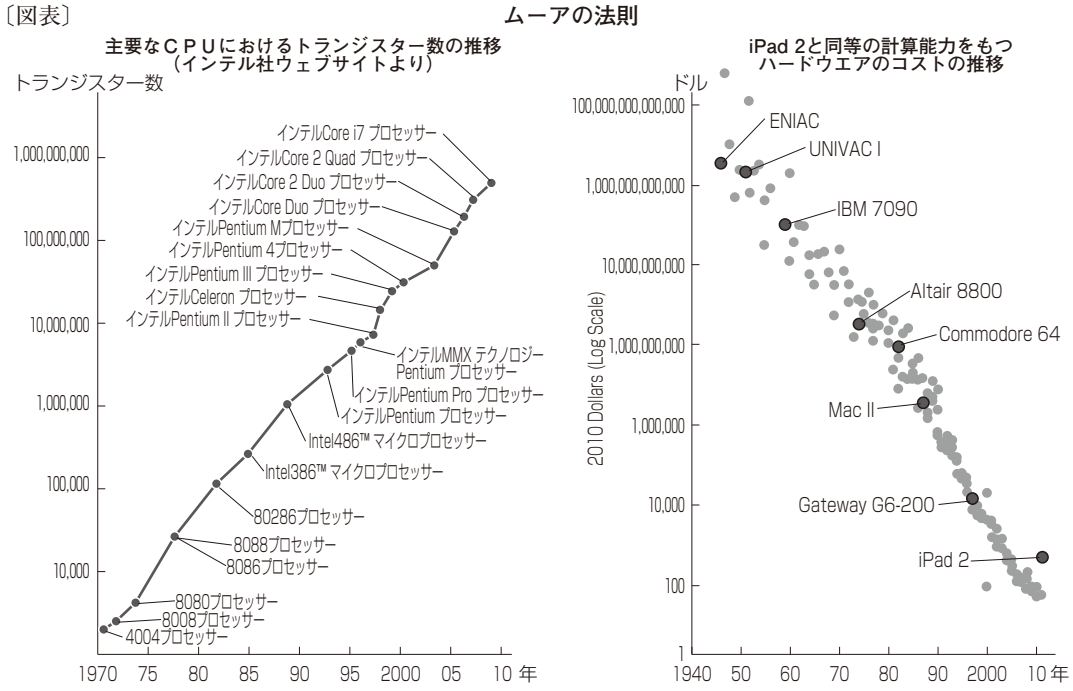
ＩＴの世界では、米インテル社の共同創業者であるゴードン・ムーアが１９６５年に示した「ムーアの法則」という経験則が知られている。「半導体の集積度は18カ月で2倍になる」というこの法則が示すとおり、コンピュータのハードウェアのコスト・パフォーマンスは年を追うごとに改善してきた。つまり、さまざまな情報機器や情報システムにおいて、同じ機能であればコストは年々安くなり、同じ費用を投ずれば性能が年々高度化している。近年の社会全般における急速なＩＴ化は、ムーアの法則によってもたらされたものといえる。

しかし、銀行の情報システム投資の中心である勘定系システムの開発現場の実感としては、コストの劇的な低下も、性能の大幅な向上も起こっているとは感じられない。これはいったいなぜだろうか。

その一つの答えは、「銀行業界は先行してＩＴ化に取り組み、それを完成させてしまったから」というものだろう。１９７０～80年代、わが国の銀行は他の業界に先んじてＩＴ化を進めた。それが一定の完成をみてから、勘定系システムの基本的なつくりは大きくは変わっていない。たとえば、銀行間ネットワークの通信電文や、キャッシュカードの磁気ストライプの仕様は、数十年間維持されている。

一方、銀行以外の世界では、90年代以降、インターネットが爆発的に普及し、ハードウェアのコスト・パフォーマンス向上

〔図表〕



（出所） Michael Greenstone and Adam Looney, "A Dozen Economic Facts About Innovation," HAMILTON PROJECT POLICY MEMO, 2011.

の裾野も大きく広がった。社会全体のＩＴ化が急速に進展するなかで、銀行はおいてきぼりをくったかたちになったのだ。そういう状況がしばらく続くと、銀行が利用するシステム技術基盤、ＩＴガバナンス体制、業務推進体制が、古い技術を前提としたものに固定化してしまい、変革を阻むことになる。今後は、こうした呪縛を解きほぐしつつ、銀行の情報システムの見直しを進めていく必要があるだろう。

外部からの隔離によるセキュリティ

これからの銀行の情報システムは、どのような設計思想に基づいて構築されるべきなのだろうか。銀行の情報システムの将来像を描くうえで重要なのは、どのようなポリシーで銀行システム全体のセキュリティを守るか、という点にあると思う。

現在、銀行は、情報システムのセキュリティ確保の手段として「外部からの隔離」という素朴な考え方に頼っている。しかし、社会全体のＩＴ化の進展によりその考え方は徐々に適切ではなくなってきており、新しいアプローチが必要になってきている。

銀行は、その業務をＩＴ化した当初から、外部と隔離された閉域のネットワークを構築し、接続先を本支店や金融業界内に限定することを基本としてきた。銀行以外の世界で技術革新が進み、インターネットが普及しても、銀行はできる限り、「外部からの隔離」を続けようとしてきた。インターネットバンキングのような対外接続の経路を例外扱いとして厳重に監視すれば、それ以外はネットワークの隔離によって外部からの攻撃を受けることはない。その考え方に基づいて、隔離された内部では、比較的素朴な認証手段が採用されている。銀行店舗に設置されたＡＴＭで磁気カードと４ケタの暗証番号による本人確認が用いられているのがその象徴である。

オープンなネットワークでも有効な認証手段を

もし銀行がインターネットの決済サービスのような新しい分野でイノベーションを競っていく必要があるのであれば、現在の「外部からの隔離によるセキュリティ」に依存し続けるわけにはいかなくなる。むしろ、インターネットのさまざまな取引にシームレスに連動できるように、銀行の情報システムを現行のクローズドなシステムから、可能な範囲でオープンなものへと切り替えていく必要に迫られよう。そういう環境でも守るべき情報資産を守れるように、セキュリティにかかる基本設計を考えなおしていく必要があるだろう。

たとえば、金融ＥＤＩでは、商流ネットワークからの情報をもとに、銀行が資金決済を実行することが求められている。しかし、銀行としては、自らが全体を管理しているわけではない商流情報ネットワークからの情報を信頼して資金決済を実行するのはむずかしい。不特定多数が関与するオープンなネットワークからの情報に基づいた取引を処理するのであれば、暗証番号のような素朴な認証手段に頼るわけにはいかない。銀行外の情報システムと資金決済が連動するような電子商取引についても同様である。

そうした個々の取引について利用可能で、かつオープンなネットワークを経路として使っても安全な、新しい認証手段を普及させ、それに基づいた業務を進める体制を整備していくことが望ましいだろう。

秘匿によるセキュリティ向上からの脱却を

こうした技術的な対策に加えて、重要と思われるのが、セキュリティ保護にかかる思想の切り替えである。

現在、銀行の情報システムで利用されている安全対策の具体的な内容は、秘密とされることが多い。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きた。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。せっかく対策を講じても、それを秘匿していたのでは安全性を

判断することもできないし、万一、セキュリティ侵害が疑われる事象に遭遇した際に、問題がないことを立証することもむずかしくなる。

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。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。

インターネットバンキングの認証手段の変遷

現在、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、フィッシングやウイ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、ウイルス感染による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。

「トランザクション認証」とは、口座振替等の銀行取引を起動するつど、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である。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むずかしいとしても、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、現在、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。その延長線上には、銀行の情報システムの新しい設計思想のヒントがある。

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で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もとでは、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。それは、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、取引ごと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。

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、そのまま銀行のシステム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、現在の基本設計のもと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いえるが、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。

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、銀行がコストをかけて守る領域を限定することも可能になる。設計思想しだいでは、銀行システム全体をより身軽なものに置き換えることもできる。ただし、そのためには、すべての預金者に、新たな認証手段を配布する必要があり、ハードルが高いと思われるかもしれない。

しかし、それはあながち無茶な構想ではない。欧州の多くの国では、キャッシュカードがすべてＩＣカード化されている。そのＩＣカードを、トランザクション認証のためのセキュリティトークンとして利用する技術も普及している。日本において、キャッシュカードをＩＣカード化し、それをトランザクション認証にも利用することにすれば、インターネットバンキングとＡＴＭ取引の両方の安全対策を一気に高度化することができる。

最近、欧州のみならず北米でもＩＣカード化が進みつつある。わが国もいずれＩＣカードに切り替え、磁気ストライプを廃止することが必要となるが、そうした対策を個別に打つのではなく、業界をあげて戦略的に対処していくべきではないだろうか。

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えないと思われる。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だろう。

マイナンバー制度との関係

銀行が10億枚に達するといわれる既往発行キャッシュカードを全面的にＩＣカード化することは大変なことだ。そもそも、過去に発行されたカードの保有者の住所などが把握されていないケースも少なくない。そういう状態であることは、マネー・ローンダリング対策の観点からも問題なのだが、容易に解決できることではない。ただし、タイミングによっては、マイナンバー対応と同時に実施することで、多くの問題を一気に解決できる可能性がある。

15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、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。将来の法改正が前提となるが、いずれかの時期にこの付番作業を実施しなければならないのだとすれば、それに合わせて、ＩＣカード化、インターネットバンキングのトランザクション認証化、預金者データの確認の作業を同時に実施することが効率的と思う。将来の制度対応を見据えて、セキュリティ対策と銀行システムの進化をあわせて検討する価値があるのではないだろうか。

（本稿の意見にかかる部分は筆者の個人的見解であり、日本銀行の見解を表すものではない。）

いわした　なおゆき
84年慶應義塾大学経済学部卒、日本銀行入行。94年に日銀金融研究所に異動し、以後約15年間、金融分野における情報セキュリティ技術の研究に従事。同研究所・情報技術研究センター長、下関支店長、11年7月から日立製作所　情報・通信システム社に出向、13年7月決済機構局参事役、14年5月から現職。