時事通信社「金融財政」（1998 年 6 月 29 日）掲載

解説　◆電子マネー・電子決済のためのセキュリティ対策◆

金融業務に利用される暗号技術と国際標準化

日本銀行金融研究所調査役　岩下　直行

いよいよ日本でも、大規模な電子マネーの実証実験が始まった。インターネット・バンキングを提供する銀行も増えている。こうした新しい金融サービスを技術面から支えているのが暗号技術である。暗号は、わが国の金融業界ではこれまであまり利用されていなかったが、オープンなネットワークの上で金融サービスを提供する場合には不可欠な基礎技術である。わが国の銀行も、金融業務に利用される暗号技術の国際標準化動向等を踏まえ、技術面のキャッチアップを急ぐ必要がある。

電子マネー、電子決済を支える暗号技術

電子マネーの実用化に向けた実証実験が、わが国でも活発化してきた。今年は首都圏を中心に、数万人規模の参加者を募ったプロジェクトがいくつも計画されている 。IC カードを利用した電子的支払手段を店頭での小口決済に利用するという構想は十年以上前から実験されてきたが、最近の電子マネー、電子決済のプロジェクトが従来のものと異なるのは、店頭での支払いもさることながら、インターネット上で「電子商取引」を行うための手段として提案されているところにあるように思われる。

世界中に張り巡らされ、数千万人が利用しているインターネットの上で、安全かつ効率的な資金決済が可能になれば、その波及効果は極めて大きいものがある。地域や国境を越えた形で、インターネット上にバーチャル・エコノミーとでも言うべき新しい経済圏が発生し、究極的な意味での金融のグローバル化が実現するからだ。

インターネットは、それ自体はセキュリティを確保する機能を持たないネットワークであるため、現在提案されている電子マネー、電子決済のプロジェクトは、いずれも独自の暗号技術を用いて、金融取引にふさわしいセキュリティー水準を確保しようとしている。

ただ、こうした暗号技術は急激な技術革新にさらされており、常に「完全な」セキュリティーを保証できるものではない。このため、そのコストをも考えながら、常に適切なセキュリティ対策を講じていく必要がある。その意味で、これからの金融業務においては、暗号技術を正しく利用し、評価する能力が必要とされていると言えよう。

暗号と金融―米国で商用化

暗号と金融という組み合わせは、多少奇異な印象を与えるかもしれないが、金融業界における暗号の利用には、実はかなり長い実績がある。暗号は、かつては軍事情報や外交機密の秘匿のために利用されるものであった。しかし、1977 年に、DES 暗号が米国政府標準暗号に認定され、ビジネス分野で利用されるようになってから、暗号の商用利用が急速に広がった。DES 暗号の開発・普及の背景には、コンピューター・ネットワークを利用して資金決済情報や顧客の秘密情報を送受信する際に、情報の改ざんや不正侵入を防止したいという米国金融業界の強いニーズがあったと言われている。

米国を中心に、銀行の決済ネットワークには DES 暗号を利用したセキュリティー装置が次々に導入され、金融業界は暗号技術の最大のユーザーとなった。こうした経験の延長と考えれば、金融業界が暗号技術を活用した電子マネー、電子決済の実験に積極的に取り組んでいることは、ある意味で当然のことと言えるだろう。

暗号は、データを第三者には判読不能な形態に変換し（暗号化）、「カギ」と呼ばれる特殊な情報を持っている人にだけ、元のデータに戻すこと（復号化）を可能にする技術だ。だから機密の保護に使えるのだが、それだけではない。送られてきた暗号文が「カギ」によって意味のある文章として判読できたとすると、受信者側は、その暗号文を作成したのは「カギ」を知っている人だと推定することができる。例えば取引データを送信者と受信者しか知らない「カギ」で暗号化すれば、安全性の高い権限確認の手段として機能させることができる。

このように、ビジネス分野で利用される暗号は、通信の秘密を守る機能（守秘）だけでなく、情報が正当な利用者によって作成されたもので、改ざんを受けていないことを確認する機能（認証）が重要になる。この認証機能は、従来は小切手などに署名･なつ印することによって実現されてきたもので、これを通信ネットワーク上で実現するために、暗号が利用されているのだ。そう考えると、金融と暗号との関係も理解しやすい。

わが国のセキュリティー対策

一方、わが国の金融業界では、これまであまり暗号技術に関する関心が高くはなかった。これには理由がある。これまでわが国の金融業界が構築してきた決済ネットワークが、企業内、業界内に閉じたものであったためだ。わが国の金融機関は、巨大なコンピューター・センターにメーンフレームを並べ、支店との間を専用回線でつなぐことにより、システムを外部から物理的に隔離して

きた。このようなシステムにおいては、ネットワーク提供者が利用者のアクセスを厳格に管理すれば、システム全体のセキュリティを高めることが可能である。

例えば、銀行の現金自動支払機で預金を引き出す取引をみてみると、キャッシュカードと四ケタの暗証番号を入力すればよく、高度な暗号技術など利用されていない。これは、現金自動支払い機が銀行の店舗内に設置されており、銀行のコンピューター・センターとも専用回線で接続された「閉じたシステム」だったからだ。このような環境の下でシステム全体のセキュリティーが確保されているのであれば、盗聴や改ざんのリスクも低いので、暗証番号程度でも権限確認の手段として十分機能する。わが国の銀行のオンライン・システムは、外部から物理的に隔離された「閉じたシステム」であったため、暗号は補完的なセキュリティ対策と位置付けられてきた。

金融ネットワークのオープン化の流れ

金融ネットワークのセキュリティーを、外部からの隔離によって守ることができていたのは、金融業界が他の業界に先駆けて独自の決済用コンピューター・ネットワークを構築していたからにほかならない。この前提が、最近の社会全体における情報ネットワークの広がりによって崩れつつある。

金融機関間取引の分野では、情報通信技術の急速な進歩と取引のグローバル化を受けて、複数のシステムがリンクする取引が増えてきている。売買、約定、決済等、複数のシステムに跨る取引を、できるだけ人手を介さずに、効率的に処理するためには、システムを相互接続し、入力されたデータを自動的に処理・転送する仕組みを作ることが必要である（このようなコンセプトを STP―Straight-Through Processing という）。しかし、これまでわが国の金融機関が採ってきたような「システムの隔離によってセキュリティを確保する」という方針だと、相互接続によってセキュリティの枠組みが崩れてしまう。このため、従来とは異なるセキュリティー対策を講じる必要が生じてくる。

対顧客取引の分野でも、EDI（電子データ交換）の普及、インターネットの発達に伴い、一般の企業や個人が何らかのコンピューター・ネットワークに接続している状況になってきているため、顧客は、金融サービスを自らが接続しているネットワークに対して提供して欲しいというニーズを持つようになっている。

例えば、金融 EDI を実現するためには、企業間取引のデータと金融データを組み合わせて処理する必要があるため、何らかの形で顧客側の EDI システムと、銀行の金融ネットワークに接点を作る必要がある。どのような方法を採るにしても、銀行システムのセキュリティ対策を考え直す必要が出てこよう。

デジタル署名による「認証」

金融ネットワークのオープン化が進み、ネットワークの提供者がシステム全体のセキュリティーを確保するという考え方が機能しなくなると、個々の取引単位のセキュリティを確保する手段として、暗号技術が非常に重要となってくる。例えば、オープンなネットワークの中で送信する資金支払い指図データの安全性を確保するために、デジタル署名による認証を行うとか、特定の相手以外には開示できない情報をオープンなネットワークで送信する場合に、暗号による秘匿を行うことが必要となる。

暗号は、機密保護を目的に利用されることが多いから、その技術も秘密にされていると思っている人も多いだろう。しかし、今日利用されている暗号のほとんどは、暗号化の具体的な手順となる計算式が公開されている。暗号アルゴリズムは、学者の研究対象となっており、その成果は論文や本の形で公表されている。それらを実装したプログラムもインターネット経由で簡単に手に入る。そして、どのような暗号をどのように利用すべきかについて、様々な国際標準がある。

暗号技術の国際標準化とは

金融業務における技術面の標準化の目的は、金融機関同士の間の情報交換に用いられるさまざまな約束ごとを統一し、ネットワーク参加者のだれもが取引に参加できるようにしたり、安全対策に関する不確実性を取り除くことにある。これまでわが国の金融業界は、電子資金移動にかかるプロトコル等、国内、業界内の標準化については円滑に対応してきた。

しかし、金融ネットワークがオープン化することに伴い、非金融業や海外とのシステムのリンクの必要が生じるようになってきており、従来よりもグローバルな標準化に対応していく努力が求められている。特に、暗号技術や情報セキュリティー技術については、「システムの隔離によるセキュリティー対策」という従来のコンセプトを見直していく過程で、こうした国際標準が参考になる。

金融機関が暗号技術を活用した金融サービスを提供しようとする場合、技術の選択や利用方法に関する一定の指針が設けられていれば、それに準拠することで最低限の安全性を保証できる。相互に接続し合っている金融ネットワークにおいては、各参加者が充足すべき最低限のルールを定めておくことが、ネットワーク全体の安全性確保の観点からも有効となる。こうした事情から、暗号を活発に利用している米国の金融業界を中心に、金融業務における暗号技術の利用方法の標準化が推進されてきた。この動きを国際的に支える役割を担って

いるのが、国際標準化機構・金融専門委員会（ISO/TC68）である。

ISO/TC68 の活動状況

国際標準化機構（ISO）は、各種国際標準の審議・制定を行う国際機関であり、鉱工業製品からサービスまで、幅広い分野を対象に標準化活動を行っている。実際の国際標準の審議は、業務分野ごとに設けられた専門委員会が担当している。TC68 はこうした専門委員会の一つであり、「銀行業務、証券業務およびその他の金融サービス」についての標準化を担当している。

TC68 は、資金決済や証券決済に関する銀行間通信フォーマット、金融取引に利用される IC カードの仕様などの国際標準を策定し、SWIFT やクレジットカード国際ブランド等を介してわが国の金融機関の活動にも影響を与えてきたが、暗号技術に関しても、情報セキュリティ・ガイドラインや暗号機器の安全性評価基準等、金融業務における暗号技術の利用についてさまざまな標準化活動を行っている。

最近の傾向としては、金融業界内に限定された技術標準だけではなく、インターネットの普及等を踏まえ、オープンなネットワーク上で提供される電子決済や電子商取引などの金融サービスも標準化の対象とするようになってきており、例えば、認証機関による公開カギ証明書の管理に関する技術規格の策定作業が進められている。

ISO/TC68 に加盟する二十一カ国では、中央銀行や銀行協会が事務局となって、実際に標準を利用する金融機関と協力しつつ、国際標準化活動を進めている。わが国では、日本銀行が、日本工業標準調査会からの委託を受け、TC68 に関する国際標準原案の検討や国内意見のとりまとめ、国際会議への出席等を行う国内審議団体となっている（事務局は金融研究所）。TC68 の国内審議は、銀行、証券会社、全銀協、日証協、メーカー、通信事業者、学者、官庁等の参加する定期的な国内委員会において行われている。

以　上