金融業務と認証技術：インターネット金融取引の安全性に関する一考察

松本 勉（まつもと つとむ）／岩下直行（いわしたなおゆき）

要　旨

わが国の金融機関の間でも、インターネットを利用した新しい金融サービスへの取組みが本格化しつつある。こうした新しい金融サービスを金融機関が安全に提供していくためには、情報セキュリティ技術、とりわけ認証技術を有効に活用していくことが不可欠である。オープンなネットワーク上での金融取引が拡大する中で、金融業界にとって、認証技術の重要性が急速に高まってきている。

認証技術という言葉は、金融業務とはあまり関係のない専門用語のように受取られてしまう傾向がある。しかし、金融機関にとって、「取引相手や取引内容の真正性を確認する」という意味での「認証」は、金融業務を構成する極めて重要で本質的な手続きのひとつである。本稿では、既存の金融業務において利用されてきた認証方式の変遷を辿るとともに、その視点から、インターネットを利用した金融業務においてセキュリティを確保するためには、認証技術をどのように利用していくべきかについて整理する。

キーワード：インターネット・バンキング、認証技術、デジタル署名、SSL

本稿は、1999年11月1日に日本銀行で開催された「第2回情報セキュリティシンポジウム」への提出論文に加筆・修正を施したものである。

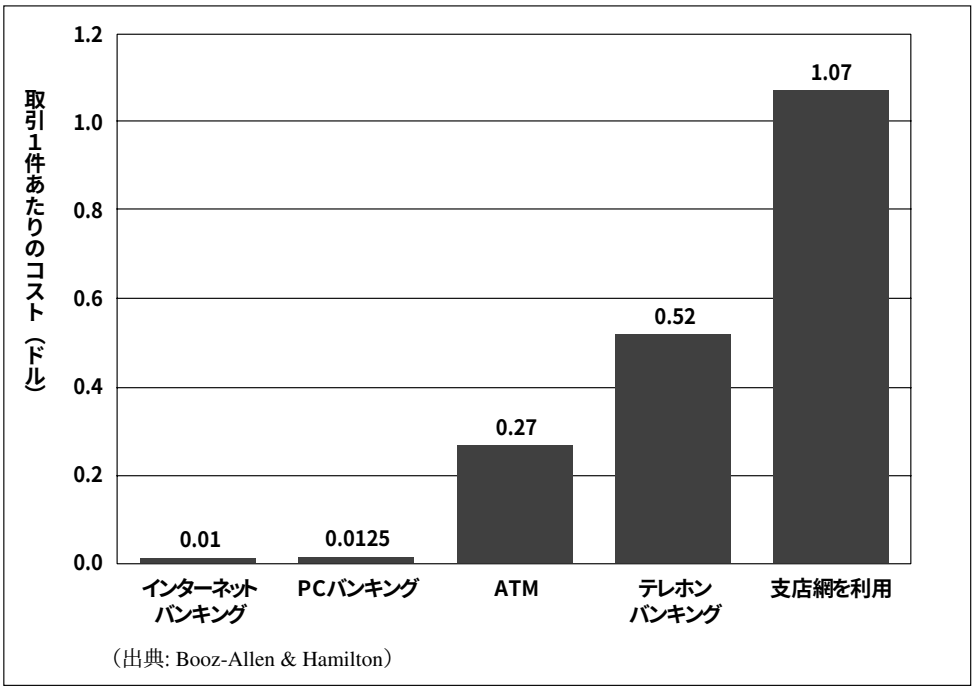
松本　勉　横浜国立大学大学院工学研究科（E-mail: tsutomu@mlab.jks.ynu.ac.jp）
岩下直行　日本銀行金融研究所研究第2課（E-mail: iwashita@imes.boj.or.jp）

1．インターネット金融取引の拡大と認証技術の重要性

世界中でインターネットが金融サービスの変革をもたらしている。米国や欧州では、インターネット専業銀行やオンライン取引に特化した証券会社のビジネスが拡大し、既存の金融機関もさまざまなオンライン・サービスの拡充を打ち出して対抗している。日本の金融機関は、従来、インターネットの活用にあまり積極的でないと指摘されていた[1]が、このところ、インターネットを利用した新しいサービスへの取組みを本格化する動きが目立っている。銀行業界では、インターネットを利用したオンライン取引サービスを拡充するとともに、振替手数料等を優遇して顧客をオンライン取引に誘導しようとする動きがみられる。大手銀行が情報通信事業者と共同でインターネット・バンキングの専業銀行を設立しようとする構想も発表された。証券業界でも、インターネットを利用したオンライン・トレーディングの業務を拡大する証券会社が増えている。1999年10月の株式売買委託手数料の完全自由化に伴い、格安な手数料を売物に、インターネットを主たる対顧客チャネルと位置付けた証券会社の新規参入も相次いでいる。

金融機関がデリバリー・チャネルとしてインターネットを利用することによって、大幅なコスト削減が可能と考えられている。支店を設置して顧客と取引を行うのに比べ、取引コストが２桁も安いとの試算もある。米国のあるコンサルティン

図１　銀行におけるデリバリーチャネル別の取引コスト（試算値）



（出典: Booz-Allen & Hamilton）

1 Booz-Allen & Hamilton［1997］

グ会社の調査によれば、欧米の金融機関の多くは、今後10年間において最も重要な顧客とのインターフェイスとしてインターネットを挙げているという[2]。

インターネットは、行政サービスの変革をも促している。情報技術を利用することにより行政事務を効率的に処理しようとする試みについては米国政府が先行していたが、日本でも、行政手続きの電子化によるサービス向上を目指した「スーパー電子政府」構想が打ち出された。政府による法人登記の電子化に向けてのプロジェクトが進められているほか、認証技術を利用する際の法的な効果を明確化する電子署名法の立法化も予定されている。金融機関は、従来から、歳入・歳出金の取扱いなど、行政サービスと関連の深い実務を担当してきたが、電子化された行政事務と整合的な金融サービスの提供という観点からも、新しい技術に対応することが要請されている。

インターネットを利用した新しい金融サービスを金融機関が安全に提供していくためには、**情報セキュリティ技術**、とりわけ**認証技術**を有効に活用していくことが不可欠である。オープンなネットワーク上での金融取引が拡大する中で、金融業界にとって、認証技術の重要性が急速に高まってきている。

認証技術という言葉は、金融業務とはあまり関係のない専門用語のように受け取られてしまう傾向がある。しかし、金融機関にとって、「取引相手や取引内容の真正性を確認する」という意味での「認証」は、金融業務を構成する極めて重要で本質的な手続きのひとつであって、他人任せにできるものではないように思われる。本稿では、既存の金融業務において利用されてきた認証方式の変遷を辿り、金融業務と認証技術との繋がりを解説するとともに、その視点から、インターネットを利用する新しい金融業務においてセキュリティを確保するためには、認証技術をどのように利用していくべきかについて整理してみたい。

2．認証とは何か

インターネットにおける電子認証技術の重要性が強く認識されるようになった結果、「認証」とは「認証機関（CA: Certification Authority）を用いて公開鍵暗号によるデジタル署名を利用するための仕組み」を意味すると理解されるようになった。例えば、大蔵省の「電子マネー及び電子決済に関する懇談会」の報告においては、金融取引における認証業務とは、「これまで金融機関が対面により又は安全性の高いクローズド・ネットワークの活用を通じて行ってきた本人確認や通信内容の真正性確保をオープン・ネットワーク上で実現するサービス」とされている[3]。

しかし、情報セキュリティの立場からは、「認証」という言葉を使用する場合、**「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**

2 Booz-Allen & Hamilton［1996］
3 大蔵省銀行局・国際金融局、「電子マネー及び電子決済に関する懇談会報告書」第６章

認する機能」と、より広義に捉えることの方が自然である。どのようなネットワークを利用するか、どのような媒体を利用するかによって使用される技術は異なるが、上記のような効果を持つものを総称して「認証」と呼ぶ。そして、金融業務と認証技術との繋がりを理解するうえでは、こちらの広い定義に即して説明することが有用であるように思われる。

例えば、紙の世界における銀行との預金取引において、銀行に預金口座を作る際には、銀行取引用の印鑑を登録し、また銀行から預金通帳を交付して貰う。預金を引出す際には、真正な通帳と届出済みの印鑑を利用することで、預金引出しの請求者が、（通帳と印鑑を持つ）正当な利用者であることを確認しているといえる。したがって、この「通帳と印鑑」は、紙の世界において「認証」を行う方式といえる。同様に、「小切手とサイン」、「磁気カードと暗証番号」なども、「認証」を行う方式と理解できる。このように理解すると、金融業務においては従来から「認証」が重要であり、今後も認証技術が重要と考えられているという点は、自然に理解し得るものと思える。

3．金融業務で利用される認証方式の変遷

それでは、以上のような概念整理に基づき、あらためてこれまでの金融業務においてどのような認証方式が実際に利用されてきたかについて、方法・技術面からの若干の整理を試みたい。提供される金融サービスの内容や時代によって利用される要素技術は異なるが、基本的には、金融業務に要請される高度のセキュリティを効率的に実現するために、その時代において利用可能な認証方式の中から、適切なものが選択されてきたと考えることができる。

金融取引が電子化される以前の「紙の世界」では、偽造しにくい印刷を施した紙幣、小切手用紙、預金通帳などの紙の媒体と、サインや印鑑が利用されてきた。現在でもわが国の預金取引では、通帳と印鑑による認証が広く利用されている。

> **通帳と印鑑**：銀行の印鑑簿に登録された印影による認証。印鑑は技術的には偽造は容易であるが、対面取引、銀行店頭における監視により不正使用が抑止されている。

紙の世界での認証におけるセキュリティ対策は、紙を媒体とする限り、人と人との書面の受渡しが生じ、それがある程度不正を抑止する効果があったため、耐偽造性など技術的な特性はそれほど問題にはならなかったと考えられる。人が介在することによる不正抑制の効果は状況に応じて変化する不安定なものではあるが、文書偽造や詐欺に関する刑事罰等の効果もあって、不正取引の防止にそれなりに有効に機能してきたと評価できる。

しかし、金融業務の電子化がある程度進むと、事務コスト削減、利用者利便性の

向上のため、人を介在させない取引が増えてくる。そこで、電子化された金融業務における初歩的な認証方式として、暗証番号、パスワード等が利用されるようになった。現在のわが国における銀行預金の受け払いには、主として磁気カード（キャッシュカード）と暗証番号の組合せによる認証が利用されている。

> **磁気カードと暗証番号**：磁気カードという媒体の確認と、暗証番号のデータベース照合による認証。磁気カードの偽造は容易で、暗証番号も容易に推定できるケースがあるため、カードの盗用、偽造等の不正取引もみられるが、銀行店舗に設置されたCD、ATM等における監視等の効果もあって、深刻な事態には立ち至っていない。

暗証番号やパスワードという認証方式は、秘密情報を銀行と利用者との間で共有し､その情報を提示させることによって認証するという方式と考えることができる。したがって、その暗証番号は利用者と銀行（の照合システム）しか知らないことが前提となる。暗証番号の提示に際しては、その情報が外部に漏洩しないことが必要であり、通信経路のセキュリティが問題となる。このため、欧米の銀行のシステムでは、CDやATMの段階で入力された暗証番号をDESやトリプルDESで暗号化して照合システムに送信する仕組みとなっていることが多い。また、日本では、あまり暗号は利用されていないものの、暗証番号は、銀行のCD、ATMとホスト・コンピューターとの間に敷設されたクローズド・ネットワークを経由して送信されることが前提となっている。このほか、銀行の照合システムから外部に情報が漏洩しないための仕掛けも必要である。したがって、適切な対策を講じなければ情報の守秘性が担保されないオープンなネットワークにおいて、暗証番号やパスワードによる認証を行うためには、暗号技術を用いて通信経路を保護することが必須となる。

また、金融サービスの利用者が、自分の誕生日や電話番号など、推定が容易な暗証番号やパスワードを設定してしまい、盗用、偽造された磁気カードが不正使用されるケースも少なからず報告されている。注意深く設定された暗証番号やパスワードであっても、入力する手元を盗み見られるとか、入力装置に細工をされたことによって不正に盗用されてしまったという事例もある。こうした問題は、利用者自身の責任に帰着する部分もあるとはいえ、暗証番号やパスワードという初歩的な認証方式の限界を示しているものと考えられる。

４．適切な認証方式を選定するために

このようなこれまでの流れを振り返ってみても、金融機関が、「取引相手や取引内容の真正性を確認する」という意味での「認証」を有効かつ効率的に実現することは、既存の金融業務においても、容易なことではなかったことがわかる。もとより、金融サービスをビジネスとして提供する以上、認証を行うためだけに過大なコ

ストを掛けることはできないし、利用者に過大な負担を課すこともできない。かといって、不正行為が容易な認証方式を採用してしまい、十分な不正対策が講じられなかった場合、利用者に被害が生じたり、金融機関自身が損害を被るリスクがあり、またそもそも金融サービスの提供者として十分な責任を果たしていないことになってしまう。

現在利用されている「通帳と印鑑」や「磁気カードと暗証番号」といった認証方式は、上記のような利害得失の比較考量の結果選定されたというわけではないが、現状、実用レベルとしてはほぼ問題のないセキュリティを実現できていると判断して良いだろう。これは、金融機関が長年にわたってこれらの認証方式の経験を蓄積していることに加え、運用上も人手をかけた監視を組合せていることによる面が大きい。しかし、①将来にわたって、現在と同じ金融サービスに現在と同じ認証方式を継続して危険はないか、②今後、新たな環境（例えば、オープンなネットワーク環境）で新たな金融サービスを提供する場合、現在の認証方式の延長で考えて良いか、については、慎重な検討を要すると思われる。

①の将来にわたる継続の問題については、(a) さまざまな技術革新によって印鑑、印影、各種印刷物、磁気カード等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、(c) 金融機関側も、店舗の人員削減等により、従来ほどのセキュリティ対策への配慮が期待できないおそれがあること、等を考えると、「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。したがって、既存の金融取引で利用される認証方式についても、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といった選択肢について、検討のスコープを広げていくべきであろう。

また、②の新しい環境への対応という問題については、例えばインターネットを利用した金融サービスを提供する場合、既存の金融業務とのアナロジーで、「『通帳と印鑑』『磁気カードと暗証番号』と同等なセキュリティを実現する」といった考え方は適当ではない。従来、ある程度の「人手による監視」が存在していた金融取引を、ネットワーク上で人手をかけずに実現しようとする場合、前提となる利用環境が異なるのだから、従来はとくに問題とはならなかったことが、新たな欠陥となる可能性がある。また、単に「最新の電子認証技術を導入すれば解決する」という問題でもない。新しいサービスを提供しようとする金融機関が、新しい利用環境において考えられるリスクや損害を適切に見積もり、新しい目で適切な認証方式を選択する必要があるだろう。

5．オープン・ネットワーク上の金融サービスにおける認証方式

オープンなネットワーク上における認証を実現するための技術として、公開鍵暗号によるデジタル署名などの電子認証技術が有効であることは、以前から良く知ら

れていた。デジタル署名は、認証機関による公開鍵証明書を利用することにより、オープンな環境で不特定多数の利用者との認証に利用される際に、その威力を発揮する技術である。しかし、この技術が利用可能となるためには、①利用者が自ら情報通信ネットワークに接続していること、②公開鍵暗号の演算が可能となる高度な計算能力を持つコンピューターを利用していること、③認証機関による公開鍵証明書の発行という社会的インフラが整備されていること、等の条件を必要とする。このため、一部のホールセール金融取引を除けば、金融業界を含めて、デジタル署名が実用化されることはほとんどなかった。

しかし、インターネットの出現がすべてを変えた。一般の消費者が高性能のパソコンでインターネットに接続するようになったので、上記①と②の条件はクリアされた。また、③の条件もクリアされつつある。インターネット上で利用される公開鍵証明書（デジタルIDとか認証書などと呼ばれる）を発行する認証ビジネス専門会社が設立されたり、決済サービス提供業者が自ら認証業務を営むことによって、インフラ整備が進みつつある。

こうした電子認証技術を実用化して金融取引に利用する場合、SSL[4]やSET[5]、SECE[6]などといった技術が採用されることが多い。とくに、SSLは、インターネットを利用したオンライン銀行取引、証券取引において現在もっとも標準的に利用されている技術であるため、以下では、SSLを金融サービスに利用する場合のセキュリティについてやや詳しくみてみよう。

6．インターネット金融取引とSSL

良く知られているように、インターネット上でWebサーバーにアクセスする際に、Netscape CommunicatorやInternet Explorerといった無償で配布されているクライアント・ソフトにあらかじめ組み込まれたSSLの機能を用いて、暗号通信、サーバー認証、クライアント認証を実現することが可能となる。一般の利用者にとっては、わざわざ自分のパソコンにソフトウェアをインストールしなくても使用できるため、SSLは広く普及しており、インターネット金融取引においても広く利用されている。

インターネットを利用した銀行取引や証券取引を提供する金融機関の増加に伴い、提供するサービスの差別化を図るため、「取引の安全性」を強調する金融機関が増えてきている。例えば**「わが社のインターネット・サービスは、128ビットSSLを用いているから安全です」**などといった説明が、テレビ・コマーシャルや新

4 SSL（Secure Sockets Layer）Version 3：Netscape社が提唱する暗号通信、認証等のセキュリティ機能が付加された暗号通信プロトコル。

5 SET（Secure Electronic Transactions）：VISAとMasterCardによって提案された、インターネット上でのクレジットカード決済を安全に実現する技術仕様。

6 SECE（Secure Electronic Commerce Environment）：SETに準拠して日本で作成された、インターネット上で銀行取引、クレジットカード取引を安全に行うための技術仕様。

聞・雑誌の広告などを通じて、一般の利用者向けに流されるようになってきた。しかし、こうした説明は、「SSLで利用される共通鍵の鍵長」というたったひとつのパラメータに焦点を当てた、ややミスリーディングな説明である。

逆に、インターネット金融取引の入門書や雑誌記事には、**「SSLと呼ばれる安全保護対策が講じられているので、セキュリティ上の問題はありません」**などと記述されることがある。こちらは、「SSLを利用している」という情報のみに着目した解説であり、やはり正確に理解されているとはいえない。SSLはその使い方によって、比較的高度なセキュリティ対策ともなり得るし、簡易な対策にとどまることもある。そうした機能を正確に理解せずに、「SSLなら安全」、「128ビットなら安全」といった評価を与えることは適当ではない。

7．SSLの構造とそのオプション

SSL version 3では、クライアントとサーバーの間の通信手順は、次のように行うことが定められている[7]。

クライアント		サーバー	概要
①交信要求メッセージ {クライアント乱数、セッションID、利用可能認証方式リスト等}	→→→		クライアントからサーバーに交信を要求。乱数、ID、認証方式リスト等を送信。
	←←←	②交信受諾メッセージ {サーバー乱数、セッションID、利用認証方式等}	サーバーが応答。乱数とIDを交換し、使用する認証方式等を決定。
		●サーバー公開鍵証明書 ●サーバー鍵交換情報 ●クライアントの証明書送付要求 ③送信完了メッセージ	サーバーが、決定された認証方式に基づき、必要に応じて、サーバーの証明書やクライアントへの証明書送付要求を送信。
●クライアント公開鍵証明書 ④クライアント鍵交換情報 ●クライアント公開鍵証明書確認	→→→		クライアントが、必要に応じて証明書を送信し、鍵交換情報（サーバーの公開鍵で乱数を暗号化したもの）を送信。
⑤暗号パラメータ交換 ⑥送信完了メッセージ			①②④で交換した乱数を組み合せてセッション鍵を生成し、クライアントから送信。
	←←←	⑦暗号パラメータ交換 ⑧送信完了メッセージ	サーバーも同様に暗号を送信し、疎通を確認する。
アプリケーションのデータ	←→	アプリケーションのデータ	交換されたセッション鍵を用いて共通鍵暗号により暗号通信を行う

①:必須項目、●:オプション項目

7 Freier, Karlton and Kocher［1996］。

SSLに対応したWebサーバーのシステムを実装する場合、設計者は、多くのオプショナルな機能から、必要なセキュリティ・レベルに合わせてパラメータを設定できる。機能の選択方法によっては、比較的安全性の高い暗号通信とサーバー認証、クライアント認証を行うこともできるし、強度の弱い暗号通信しかできない場合もある。選択できる主なパラメータを整理すれば、次の表のようになる。

機能	安全性高い←選択できる主なパラメータ→安全性低い
サーバー認証	公開鍵証明書あり／公開鍵証明書なし
クライアント認証	公開鍵証明書あり／公開鍵証明書なし
公開鍵暗号（鍵交換）アルゴリズム	RSA、Diffie-Hellman
公開鍵暗号の鍵長（法のサイズ）	1024 bit／768 bit／512 bit
共通鍵暗号アルゴリズム	トリプルDES、DES、IDEA、RC4、RC2
共通鍵暗号の鍵長	168 bit（トリプルDES）／128 bit（RC4、IDEA）／56 bit（DES）／40 bit（DES、RC4、RC2）

現在、SSLを用いて実用化されているインターネット金融取引の中には、利用者の公開鍵証明書を用いたクライアント認証と、128ビットの共通鍵暗号を組み合わせたものから、クライアント認証を行わず、40ビットの共通鍵暗号を利用するものまで、さまざまなバリエーションがある。

利用者に公開鍵証明書を取得させ、これを用いてクライアント認証を行った場合、（認証機関の運営と利用者の秘密鍵管理の適正性を前提として）デジタル署名によって、利用者本人からの入力であることを確認したり、送信データの否認防止機能を実現することができる。一方、クライアント認証を行わない場合、SSLは暗号通信機能しか提供しないため、クライアント認証はパスワードを利用して行うこととなる（SSLが実現する通信経路の守秘により、パスワードの漏洩を防いでいる）。つまり、同じSSLを利用したシステムといっても、デジタル署名による電子認証を行うシステムと、パスワードによる認証にとどまるシステムの２種類に分かれることとなる。

また、良く知られているように、共通鍵暗号の鍵長については、米国政府の暗号輸出規制の関係で、米国以外では解読の容易な40ビット対応のブラウザーしか利用できなかったが、徐々に輸出規制が緩和されるとともに、金融取引目的であれば128ビット対応版が利用可能になりつつある。鍵長が長い方が全数探索攻撃に対する強度が高いが、このパラメータは比較的違いがわかりやすいこともあって、「128ビット利用可能」が安全性の証のようにいわれることがある。しかし、上記のように、128ビットであるか否かは、SSLのセキュリティ・レベルを規定するパラメータのひとつに過ぎないことに注意が必要である。

これに対し、共通鍵暗号用の鍵交換やデジタル署名に利用されるRSA公開鍵暗号の鍵長は、あまり話題にされることはないが、同様の問題を抱えている。RSA公開鍵暗号の鍵長も、米国の暗号輸出規制の関係から512ビットに制限されていたため、現在、インターネット金融取引で利用されているものは、ほととんどが鍵長512ビットである。最近、768ビットや1024ビットといった長いRSA公開鍵が利用できるブラウザーも提供され始めているが、まだ一般には普及していない。512ビットのRSA公開鍵（N＝P×Q、PとQは素数）が、1999年8月、オランダの暗号研究者を中心とした研究グループによってPとQとに実際に素因数分解されたことからも明らかなように、金融取引の目的で利用するとすれば、鍵長40ビットの共通鍵暗号も、鍵長512ビットの公開鍵暗号も、いずれも十分な安全性を持っているとはいいがたい。

もちろん、システムの作りが複雑で、クライアント側に専用ソフトを組み込む必要のあるSETやSECEと比べると、SSLは比較的簡単に利用することができるという利点があるし、「手軽に使えるSSLを採用したサービスはセキュリティが甘い」とは直ちに断定できないことにも注意が必要である。SSLを部品として組み込んだシステムであっても、システム全体への配慮如何では、ある程度のセキュリティ上のニーズに応えられる優れたシステムになりえるからである。したがって、大切なのは、システム全体のセキュリティをどう守るかということである。

8．システム全体のセキュリティを守るために

SSLのような通信プロトコルは、オープンなネットワークでのセキュアな金融取引を実現するうえで有用な要素技術であるが、決してそれ単体で存在するものではないことには注意が必要である。電子認証技術自体としても、

（1） デジタル署名検査鍵（公開鍵）の登録時に、認証機関が行う本人確認の厳格さはどの程度が求められ、実効あるものにできるのか。
（2） デジタル署名生成鍵の生成が正しく行われることはどう確認するのか。
（3） デジタル署名生成機能（署名生成鍵を含むソフトウェアないしICカードなど）が他人の手に渡るかもしれない。
（4） デジタル署名生成機能が本人の意思どおり働くことはどう確認するのか。
（5） 理論および計算機技術の進展によりデジタル署名方式自体がある日安全でなくなるかもしれない。
（6） 署名生成鍵を紛失しても認証機関に届けないかもしれない。
（7） 公開鍵証明書（署名検査鍵）が失効した後はどうするのか。
（8） 認証機関が災害やサーバーテロ等の犠牲になるかもしれない。
（9） 証明が必要となった時に、認証機関が存在していないかもしれない。

などのさまざまな問題点にどう対処していくかという課題がある。（4）について若干補足すると、デジタル署名は、印鑑のように本人が実際に押すわけでなく、実作

業を行うのはコンピューターのソフトウェアやハードウェアであって、それらが本人の意思どおり間違いなく働くことの確認は意外と難しい。例えばICカードを使ってある文書にデジタル署名をつけようとしたら、不正なアプリケーション・ソフトウェアが異なる文書に対してもデジタル署名をつけてしまい、そのことにその場では本人が全く気づかないといった事態も考えられる。また、(6) については、デジタル署名を生成する秘密鍵を紛失したらすみやかに認証機関に届け出ることが通常要請されるであろうが、不注意あるいは故意によって届け出が行われないこともありえる。それが本人の被害だけにとどまればよいが、そうとは限らない点が問題である。

さらに、例えば、インターネット・バンキングであれ、電子政府構想などにおける電子的な行政への書類申請事務であれ、認証機関とデジタル署名が重要な機能を果たすことは事実であるが、それだけでは事務は完結しない。例えば、デジタル署名を確認してデータベースを更新したり、銀行や行政機関のアプリケーション・システムが安全・確実に処理を行うことが要請される。その意味では、電子認証を支えるPKI（Public Key Infrastructure）や認証機関、更にはデジタル署名の利用者による秘密鍵の管理が重要なことはいうまでもないが、電子認証技術を利用する個々の業務システムにおいて、システム全体のセキュリティをどう確保するかということが最終的な目標となることは、常に意識しておく必要がある。いいかえるならば、どんなに優れた認証技術を利用しようと、各業務を処理するシステムのセキュリティがお粗末では、意味がないということである。このことは、ともすれば電子認証技術そのものの安全性という狭い分野に関心が集中しがちであることを考えると、常に考慮しておくべき点と思われる。

９．デジタル署名以外の電子認証技術

また、同じような視点として、「電子認証の有効性を担保するためのセキュリティ対策は、その電子認証がどのような用途に利用されるかによって変化する」ということも重要と思われる。例えば、電子認証技術の用途によって公開鍵証明書のセキュリティ・クラス（本人性の確認の厳格さの程度）を使い分ける、といった運用が行われているが、そもそもこうした方法ではカバーしきれない業務もある。

ひとつの典型的な例は、電子公証と呼ばれる分野である。ある文書がある時点で存在したことを何十年後までも証明したい、というニーズがある。例えば、2010年の時点において、2001年に生成されたとされるデジタル署名についてその真偽が問題になったとする。そのデジタル署名を検査するための公開鍵証明書の有効期限は2003年であって、とうの昔に過ぎている、というような事態が生じた時の問題である。

こうした問題に対して、現在のデジタル署名を利用したシステムは解を提供することができない。基本的に、認証機関とデジタル署名を利用する認証技術は、「何

十年」といった長期の要請には応えられない。これは、デジタル署名という技術が、公開鍵暗号という時間とともに安全性が低下していく技術と、認証機関を営む組織の信頼性に依存している以上、将来にわたっての安全性の担保という面からは不確実性を抱えており、限界があるからである。

この問題を解決するための技術として、デジタルタイムスタンプと呼ばれる認証技術が存在する。例えば、秘密鍵の漏洩やデジタル署名アルゴリズムへの攻撃といった将来のリスクを回避するため、ハッシュ関数のみで階層構造を作り、最上位のハッシュ値を公開することにより、証拠性を担保する仕組みである。このような機能は、現在の紙ベースの書類が果たしているものだが、それを通常のデシタル署名を利用したスキームで実現させることは難しく、ハッシュ関数や、鍵長の長い特別なデジタル署名といった別の技術体系が必要とされている。

もちろん、こうした技術についても、例えば利用しているハッシュ関数の安全性が損なわれた場合はどうするか、十分と考えられていた鍵長が十分でなかった場合はどうするか、という議論があり得る。これらの問題はまだ解決されていない今後の検討課題であるが、こうした課題が残っていることからもわかるとおり、どこかの時点で、ある技術を前提に制度やシステムを固定してしまうことは難しく、認証技術についての継続的な検討が必要とされている。

金融業務において電子認証技術を利用していく際には、例えば紙の技術によって実現している効果を実現しようとした際に、このような課題が残っていることを考慮して検討していくことも大切であろう。

10. おわりに

金融機関がオープンなネットワークを利用した新たな金融業務を拡大していくうえで、新しい認証技術が必要とされている。ここで強調しておきたいのは、認証技術についての検討が必要なのはインターネットを利用する場合に限らない、という点である。従来の金融取引において、「通帳と印鑑」とか「磁気カードと暗証番号」といった､比較的脆弱なセキュリティ技術でも深刻な事態に立ち至らなかったのは、そうした技術が利用される環境（対面取引）や通信インフラ（クローズド・ネットワーク）が、不正を排除する仕組みを持っていたという面が大きかったためと考えられる。しかし、金融機関を取り巻く環境は大きく変化しており、従来型のサービスをよりオープンなネットワークで提供するといった試みも拡大しつつある。このため、「従来は問題がなかったから大丈夫」と考えることは適当ではない。新しい金融サービスにチャレンジする場合はもちろんのこと、既存の金融サービスにおけるセキュリティ対策のあり方を考えるうえでも、考えられるさまざまなリスクを検討したうえで、有効な対策を講じていく必要がある。

今後、金融機関は、新しい情報技術や通信インフラを活用してその業務を展開していくことが要請されている。ところが、こうした新しい金融サービスの安全性に

ついて議論すると、「紙ベースと同等のセキュリティ」といった考え方が使われることが多い。既存の制度やルールとの関係を検討するためにやむをえない部分もあろうが、基本的には、紙ベースとは違った特性を持った電子の世界において、どのようなセキュリティ対策が適当かを考えることこそが重要と思われる。また、こうした新しい金融サービスを普及させていくためには、例えば電子的な金融取引でトラブルが生じた際にどのような事態となるのか、利用者があらかじめ見通せるような環境を整備しておくことも重要である。そうした地道な努力の積み重ねにより、わが国の決済システム全体の利便性、効率性、安全性を高めていくことは、わが国全体の利益に繋がることではないだろうか。

参考文献

宇根正志・岡本龍明、「最近のデジタル署名における理論研究動向について」、『金融研究』第19巻別冊第１号、日本銀行金融研究所、2000年4月

――――・中原慎一、「最近の金融業務における情報セキュリティ評価・認定を巡る動向について」、『金融研究』第19巻別冊第１号、日本銀行金融研究所、2000年4月

――――・松浦幹太・田倉昭、「デジタルタイムスタンプ技術の現状と課題」、『金融研究』第19巻別冊第１号、日本銀行金融研究所、2000年4月

大蔵省銀行局・国際金融局、『電子マネー及び電子決済に関する懇談会報告書』、1997年5月

大蔵省銀行局、『電子マネー及び電子決済の環境整備に向けた懇談会報告書』、1998年6月

中山靖司・小松尚久、「バイオメトリックスによる個人認証技術の現状と課題 ―― 金融サービスへの適用の可能性――」、『金融研究』第19巻別冊第１号、日本銀行金融研究所、2000年4月

谷口文一、「金融業務におけるPKI・電子認証について――技術面、標準化に関する最近の動向を中心に」、『金融研究』第19巻別冊第１号、日本銀行金融研究所、2000年4月

法務省民事局、「電子取引法制に関する研究会報告書」、1998年3月

松本 勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、『金融研究』第18巻第２号、日本銀行金融研究所、1999年4月

郵政省電気通信局、「21世紀デジタル社会の暗号政策への提言 －暗号通信の在り方に関する研究会報告書－」、1999年6月

Booz-Allen & Hamilton, Inc., “Internet Banking: A Survey of Current and Future Development,” February 1996.

――――, “Booz-Allen’s Worldwide Survey Revealed A Huge Perception Gap Between Japanese And American/European Banks Regarding Internet Banking,” 1997. (http://www.bah.com/press/jbankstudy.html)

Alan O. Freier, Philip Karlton and Paul C. Kocher, “The SSL Protocol Version 3.0,” November 18, 1996. (http://home.netscape.com/eng/ssl3/ssl-toc.html)

Tsutomu Matsumoto, “Human-Computer Cryptography: An Attempt,” 3rd ACM Conference on Computer and Communication Security, 1996.

――――― and Hideki Imai, “Human Identification Through Insecure Channel,” Advances in Cryptography - EUROCRYPT’91, Lecture Notes in Computer Science No.263, pp186-194, Springer-Verlag, 1991.

U.S. Department of Commerce, *The Emerging Digital Economy*, May 1998.