社会システムとしての電子認証と電子署名

PKI 相互運用技術 WG リーダー
セコム株式会社 IS 研究所　松本　泰

インターネットバンキング等のサービスにおいてフィッシングサイト、スパイウェア等を利用した金銭目的の犯罪が増加しています。今後、インターネットの利活用が進むほどにこうした金銭目的の犯罪は増加する可能性があります。こうした中、インターネットバンキングに限らずネットワーク基盤の利活用が求められています。e-Japan戦略の成果としてインターネット等におけるブロードバンドの普及などが挙げられており、そして、これらのIT基盤の利活用が次の課題とされています。しかし、これまでのIT基盤は、利活用を進めるにふさわしい十分なユーザ認証(電子認証)、セキュリティを提供しているとはいえず、結果としてインターネットの利活用を阻むことになるのではないでしょうか。一方、ネットワーク社会の安全、安心を推進する法制度として2001年に施行された電子署名法がありますが、電子署名法に基づく電子署名はとても普及しているとは言いがたい状況にあります。電子署名法は来年で施行5年を向かえ、その改正も検討されています。社会がIT技術やネットワークへの依存度を深めていくとするならば、ネットワーク社会の安全、安心を推進するための技術や法制度のあり方を考え直す必要があるのではないでしょうか。本稿では、こうした問題を考察します。

1. ネットワーク社会における電子認証の重要性

人、サービス、デバイスがシームレスに接続されていくネットワーク社会における電子認証(Authentication)の重要性は、技術者ならば誰もが感じていることではないでしょうか。政府が進める「e-Japan戦略」は、「元気、安心、感動、便利」な社会を目指すとされています。これは、いつでも、どこでも、誰にでも(人)、何にでも(デバイス、サービス)ネットワークを介して接続され、その中で様々なサービスを享受できるであろうことを前提に考えられています。しかし、多くの感動、便利を提供するサービスでは、単にネットワーク上で接続されるだけではなく、信頼関係を確立するための認証(Authentication)が重要になります。

安全、安心なネットワーク社会を実現するための重要な要素のひとつだと考えられる認証に対しては、これまでにない多様な要求が浮上しています。人の認証ということだけをとっても、プライバシー保護のための仮名による認証、人の色々な属性に関する認証、これらの認証がシームレスに接続されたネットワークにおいて、より大規模に、更に色々な組織を超えて行われること等が要求されています。さらに、何にでも接続される今後のネットワーク社会においては、人の認証だけでなく、デバイスやサービス等の認証も重要な役割を果たします。

こうした中、様々な認証技術が登場しているものの、今後のネットワーク社会で安心して使え、個々のネットワークや組織を超えた広範囲な認証を実現するには、まだ大きな壁があります。壁のひとつは相互運用性の問題です。これまでの多くの認証技術は、限られた環境で動作すればよく、相互運用性の問題が大きくクローズアップされることはありませんでした。

認証のセキュリティレベルの向上も重要な課題です。e-Japan戦略の成果としてインターネットにおけ

るブロードバンドなどの普及が挙げられていますが、これらのIT基盤の利活用が次の課題とされています。しかし、これまでのIT基盤は、利活用を進めるにふさわしい十分なユーザ認証(電子認証)とセキュリティを提供しているとは言えません。インターネットにおける認証はごく当たり前に利用されているにも限らず、そのセキュリティ等に対して何の評価基準もなく、また、実際に利用されている電子認証も低いセキュリティレベルのものが主流だと考えて間違いありません。低レベルの認証だけが様々なサービスに広範に利用されていることは、ネットワークの実質的な価値を下げているとも言えます。

それでは、これまでこうした問題を解決する努力がなされてこなかったのでしょうか。一般には法制度における政府の取り組みとして2001年に施行された電子署名法があると考えられています。しかし、現時点において電子署名は普及しているとは言えず、また、電子署名に対する様々な誤解もあるように思われます。まずは、この電子署名法から考察します。

2. 電子署名法

IT社会、電子社会に対応する法律として電子署名法があります。電子認証(Authentication)の基盤に関して、電子署名法が重要な役割を果たしていると思われている節がありますが、これは必ずしも正しくありません。このあたりから説明していきます。

1990年代の後半に世界各国で電子署名法が成立した流れを受け、日本においても電子署名法が検討され2001年4月に電子署名法が施行されました。この電子署名法によって適正に行われた電子署名は、手書き署名や押印がなされた文書と同様に文書が真正に成立したとの推定効が与えられることとなりました。電子署名法は、旧来の紙文書における押印を、電子文書に対する電子署名により置き換えることを可能にすることで、紙を前提とした多くの法律を改正せずに、紙文書から電子文書への移行を可能にしています。

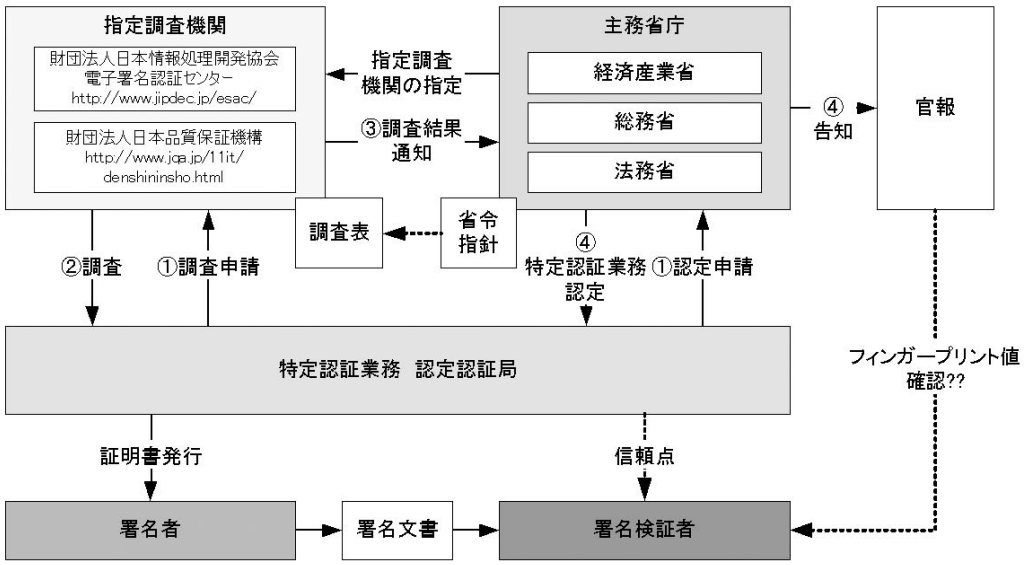
電子署名法は、これまで紙と押印を中心とした社会から、電子文書と電子署名を中心とした社会への足がかりとなり、今後の電子社会の中で大きな役割を担っていることは間違いありません。電子署名に利用されるPKI技術は、電子署名、電子認証、暗号などの機能を提供しますが、電子署名法自体の目的は、文書の署名に対するものです。従来の手書き署名や押印に代わる電子署名の役割は、現在の法制度の延長上にあり、法制度の上からは分り易いものがあります。しかしネットワークにおけるリモートの電子認証に対応する概念は、従来の法制度にはありません。そのため電子署名法は、ネットワーク環境における電子認証(Authentication)とは直接関係ないことに注意する必要があります。

電子署名法は民間に対する法律ですが、電子政府の認証基盤とされる政府認証基盤(GPKI: Government Public Key Infrastructure)も電子署名に対応した(Authenticationの基盤ではない) 基盤と言えます。実際GPKIが発行する証明書は、基本的に否認防止の署名を目的とした官職証明書(Certificate)です。政府認証基盤(GPKI)は、1999年末のミレニアムプロジェクトのアクションプランにおいて、電子申請、通知／交付のセキュリティを確保するための基盤の整備として始まっています。電子申請には民間からの申請書に申請者の電子署名を付すこと、政府からの通知／交付には政府官職の電子署名を付けることとされ、そのため電子署名は電子申請者や政府官職の本人性と申請文書や通知／交付文書の真正性を担保するために必須のものとされました。官職による署名は、多くの場合「人」の意思による署名ではありません。例えば電子申請の場合、何らかの府省内の一連の手続きや審査を経た後、申請に対して許可するといった文書に対して「官印」に代わる官職による署名がなされます。こうした官職の役割としても、一般的に電子認証(Authentication)は不要だったわけです。

電子署名と電子認証を理解する上で、認証(Authentication)と認証(Certification)、2つの「認証」という用語は、多くの混乱の元になっています。多くの法律用語において「認証」は、英語のCertificationを意味します。それに対して、サーバ等によるユーザの真正性の確認を意味することも認証(Authentication)と呼ばれます。Certificationは、何らかの権威者が発行する証明書により、何らかのことを証明することです。公としての行政機関は、従来からこのCertificationを数多く行っており、その証としての証明書の発行を行なってきました。そのため法制度等において「認証」は、Certificationを意味することが多い訳です。そのためCertificationの電子化自体も多くの場合、電子署名の技術を用いて実現されています。

電子署名法の施行により、民間に証明書を発行する認証業務のうち一定の基準を満たすものは総務大臣、経済産業大臣及び法務大臣の認定を受けることができる制度が導入されました。この特定認証業務認定では、認証局に対する認定の基準を定めていますが、内容としては認証局の設備や運用に関するものであり、特に、証明書を発行する本人身元確認と、証明書と鍵を本人に結びつける作業に関して非常に高いハードルを課しています。特定認証業務認定の基準は、現在のところ、電子署名、電子認証に関連した日本国内の唯一の基準と言えます。図1に特定認証業務認定の関連を示します。

図1

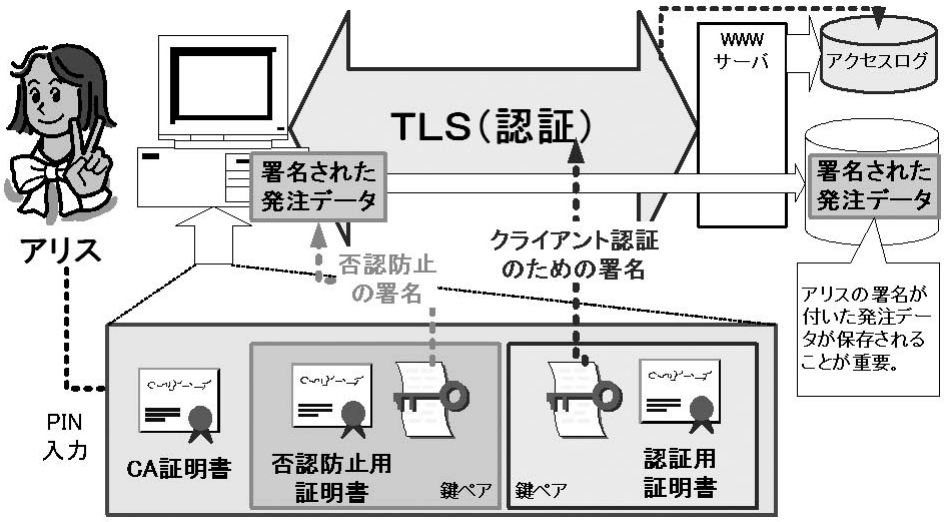


次に電子署名と電子認証を技術とビジネスの面から説明します。

3. 電子署名と電子認証の技術の違い

PKIを利用した否認防止のための署名(ここでは自署名と表現します)と認証(Authentication)は、共にプライベート鍵による署名(プリミティブな操作としての署名を単に「署名」と表現します)を利用して実現されています。しかし、自署名と認証では、そのプライベート鍵による署名の意味が大きく異なります。証明書の発行自体も、自署名と認証で使い分けている例もあります。図2に署名と認証を使い分けている例を示します。

図2



ここでアリスは、2つの証明書に対応した2つのプライベート鍵による署名を使いクライアント認証と文書への電子署名を行っています。PKIは、強い認証(Strong Authentication)を提供しますが、この強い認証を利用することによりセキュアにサーバに電子文書を渡すといったことができ、サーバ側ではそのアクセスログを残すことができます。しかし、それだけでは、電子契約などで要求される「実印での捺印」の代わりにはなりません。契約文書などに自署名を施す場合、アリスは、この文章の内容を熟読した上で自分の意志を持って自署名を行います。利害関係者間の文書のやり取り等では、アリスの自署名が施された電子文書自身が相手に送付され、その署名された電子文書が保存されることが重要になります。このような自署名は、否認防止の署名と呼ばれます。こうした否認防止目的で使用される証明書には、証明書に含まれる証明書拡張フィールドの鍵使用目的(Key Usage)に non-repudiation（否認防止）bit が設定されます。non-repudiation bit が設定された証明書に対応するプライベート鍵で(否認防止のための)署名を行う場合、そのアプリケーションは必ず署名者に自署名する文書を提示する必要があります。

自署名と認証では、その脅威も異なります。ネットワーク社会において、なりすましや盗聴といった脅威が語られていますが、自署名に対する脅威にもうひとつ、「内容を理解せず(させずに)自署名を行う(行わせる)」という脅威があります。例えば、「手形の裏書の意味を知らずにいわゆる自署名をさせられた」といったことが起きえます。PKIを利用した認証においては、その認証プロセスの中で乱数などに署名させて、その署名結果を検証することで認証を行います。認証のための署名においては、利用者は署名内容(認証プロトコル中の乱数など)を確認することはなく、また、認証のプログラムも利用者に意識をさせずに署名操作を行うことが多い訳です。それに対して自署名では、署名者が必ず自署名の対象となる文書を確認する必要があります。

以上のようなことからIDカードには、複数の証明書とプライベート鍵を格納して自署名や認証などの用途に応じて使い分ける例が多く見受けられます。欧州の市民カードや、米国の政府職員向けに発行されるPersonal Identity Verification（個人ID認証：PIV)等では、複数の証明書とプライベート鍵がIDカードに格納され、そのプライベート鍵を保護するためのメカニズムも異なります。欧州の市民カードの場合、認証用のプライベート鍵による署名では、

カード保有者がカードのPINを入力し保有者認証を行なった以降は、カードに記録された認証用のプライベート鍵が認証の都度自動的に署名します。これに対して自署名のプライベート鍵では、一回の自署名操作、つまりひとつの文書の自署名毎にPINの入力が必要な仕様になっています。これはカード自体が､「内容を理解せずに自署名してしまうこと」を防ぐ仕組みを有していると言えます。日本の公的個人認証サービスでは、証明書の non-repudiation（否認防止）bit が設定された否認防止目的の証明書のみが発行されています。従って、公的個人認証サービスの発行する証明書を電子認証(Authentication)に利用するのは避けるべきです。

次にビジネスの面から「電子署名」と「電子認証」の違いを考察します。

4. 電子署名と電子認証の用途の違い

電子署名は、契約文書などの経済活動等において必要不可欠な重要書類を紙文書から電子文書への移行を促すためには必須の技術です。電子署名法自体は、紙と押印を電子文書と電子署名に置き換える法律であり、主に既存の法制度に依存します。そのため既存の紙文書を中心とした業務が多い業界に対しての影響が大きいと言えます。

一方、ネットワークの安全、安心を提供するということ、特にネットワークを介した情報共有、機密情報保護等においては、電子署名ではなく電子認証が重要な役割を果します。また、現状の電子署名法に対応した電子署名は、非常に重要ではありますが、現時点において一般市民にとっては必要不可欠なものとは言いがたい面があります。一般市民にとっては電子署名以前に、実印を使用することもそれほど多くはありません。これに対してネットワークにおける電子認証は、インターネットが普及した現在では一般市民にとってもごく当たり前に利用されています。デジタルデバイドなどの問題はあるにしても、インターネットや社内イントラの利用者などは、ほとんどの場合、何らかのネットワークを介したリモート電子認証を利用しています。

このように当たり前に利用されているにも限らず、インターネット上で広く利用されている電子認証に対しては何の評価基準もなく、実際、低いセキュリティレベルの電子認証の利用に留まっていると考えて間違いありません。そして、低レベルの認証だけが様々なサービスに広範に利用されている事実は、結果としてインターネット上のサービスに対して不安を植えつけることとなり、そうしたことが、より高度なネットワークの利活用を阻むことになっている面があります。

前述したように旧来からの法制度には、ネットワークを介したリモート認証に対応するものがないこともあり、ネットワーク社会の安全、安心を提供する認証に対して、現状においては法制度、政策的な対応は何もない状況にあると言えます。インターネットビジネスは、法制度などからの規制に縛られず発展してきた経緯があり、結果として電子署名の要求は少ないというのが現状です。こうした業界でも高い付加価値のサービスを行うためには、一定の保証レベルを持った電子認証が必要とされているはずですが、認証の技術や運用の標準化、そのセキュリティ基準等は未整備であり、電子認証の利用者にとってもサービスを提供する側にとっても、その利便性とリスクを測りかねている状況にあると言えます。表1に電子認証(Authentication)と電子署名の比較を示します。

表１　電子認証と電子署名の比較

	電子認証（Authentication）	電子署名（Signature）
手段	現状は色々な認証のメカニズムが乱立しているが、広範に利用されているのは低レベルのものが多い	電子署名はPKI以外の現実的な手段はない
法制度	現状、法制度との結び付きはなく、認証のレベルもバラバラでユーザからは差がわからない（クライテリアが未整備）	電子署名法、e−文書法など法制度との結び付きが深い
マーケット＆利用	比較的新しい業界に需要がある。今後のユビキタスネットワーク時代のユーザ認証、機器認証の需要は測り知れない	紙に依存した比較的レガシーな業界に需要が多い。効率化するために電子化、IT化を推進したいが電子署名などの敷居の高さが壁になっている。
普及の鍵	普及には新しいビジネススキームの創造が重要（安全安心のための法整備が検討されるべき）	普及には業務知識、そして効率化のためのBPR（Business Process Reengineering）が伴うことを理解する必要がある
キーワード	ネットワーク上の安全、安心。ID管理、ID連携（Identity Federation）	e−文書法対応、電子文書保存、電子契約

それでは、色々な認証のメカニズムが乱立しておりユーザ(サービス利用者、サービス提供者)にとって差が分らない電子認証において、それらをわかりやすく利用するためのガイドライン作成などの動きはないのでしょうか。海外では、特に電子政府に関連した電子認証に関するガイドライン作りが積極的に行なわれており、次にその例を説明します。

5. 電子認証のガイドライン作り

認証に関連した技術は非常に幅広いものがあります。様々な電子認証技術はボトムアップに独自に発展してきた経緯があるため、それぞれの認証技術に依存した用語等も多く、これが混乱を招いている面もあります。認証技術の多様性は、その重要性とは裏腹に電子認証技術の全体像を非常に分かり難くしています。様々な認証技術が出現しており、そうした技術を利用した製品開発ベンダー等が、その技術の優位性をアピールしています。しかし、こうした技術が客観的に、まして経済性も含めて評価されることは、さほど多くありません。こうしたことからも経済性とセキュリティを考慮した認証のベストプラクティスを示すことは容易ではありません。

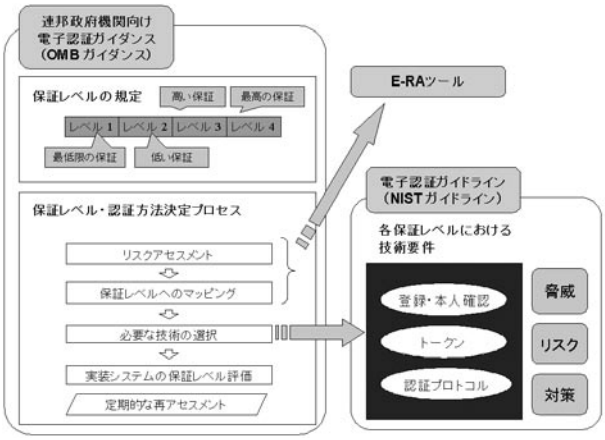
一般に電子認証を考えるには、認証対象のエンティティ（人、サーバ、デバイス等)、認証のメカニズム(認証方式、プロトコル等)、認証される範囲(認証ドメイン)などの明確化が必要になりますが、これからのネットワーク社会においては、より広い認証ドメインが求められ、この広い認証ドメインにおいて、広いが故に複数の認証対象のエンティティと、複数の認証メカニズムが混在していくことになると考えられます。

セキュリティへの要件が高まり個々の認証技術も複雑になる中で、用途に応じた認証のベストプラクティスを示すことが非常に重要になりつつあります。こうした動きが海外の電子政府における電子認証の取り組みとして見られるようになってきました。米国、英国、オーストラリア、ニュージーランドといった国々の電子政府では、複数の保証レベルを持った、また必ずしも特定の技術に依存しない電子認証のガイドラインを発行しています。その上で電子政府において利用する認証(Authentication)プラットフォームの

構築、または、検討を行なっています。これらの国々では、認証プラットフォームを使って電子政府のセキュリティレベルの向上を目指している訳ですが、それだけではなくコストの削減も目標にしています。

これらの中で実際に一番進展しているのは、米国電子政府における電子認証フレームワークを推進する米国e-Authenticationイニシアチブです。e-Authenticationイニシアチブでは、最上位のポリシを行政管理予算局(Office of Management and Budget：OMB)が電子認証ガイダンスとして提供しており、その中で4つの保証レベルを示しています。そして、この４つの保証レベルを前提に適応アプリケーションのリスク評価を行い、必要な保証レベルのマッピングを行なうなどの保証レベルと認証方法の決定プロセスを示しています。４つの保証レベルに対応した技術要件は、米国の標準技術局(NIST：National Institute of Standards and Technology)が「電子認証ガイドライン」として提供しています。この「電子認証ガイドライン」は、NISTの文書として「NIST Special Publication 800-63」として識別され、米国電子政府の情報セキュリティのための一連の文書のひとつという位置づけにもなっており、米国政府の調達などに要求される電子認証技術のガイドラインを実質的にも提供しています。図3に、これらの文書の関連を示します。

図３



このように電子認証は各国がガイドライン等の整備に乗り出した状況です。では日本においても既に整備が進んでいるはずの電子署名についてはどうなのでしょうか。

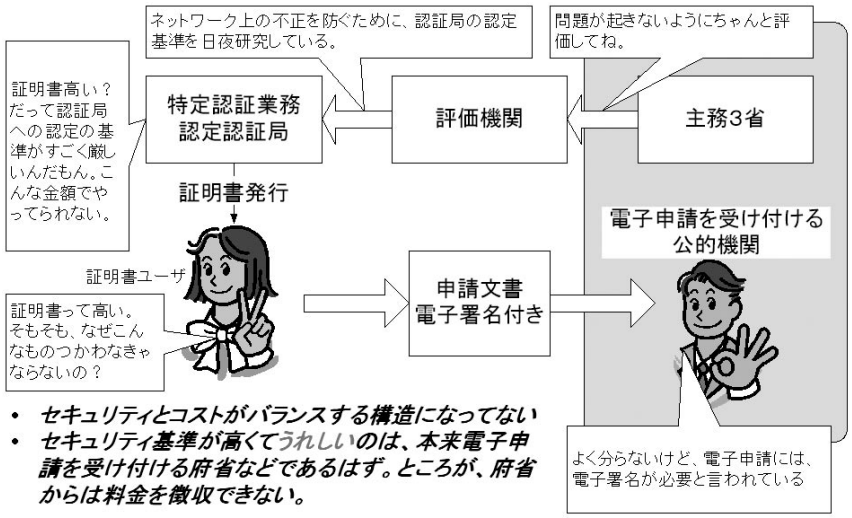
6. 電子署名の普及

ブロードバンド等のネットワークの普及や技術の発展に対して、電子署名の普及が進んでいないという声が強いのが現状です。電子署名の普及の課題は、技術的な問題以外の部分にあります。「紙と印鑑」の文化から「電子文書と電子署名」の文化へ移行するために、まずはこれまでの慣習の壁を越える必要があります。また、企業内だけであっても「紙と印鑑」から「電子文書と電子署名」への移行は、業務の本質的な変革が要求されます。電子署名がなされた電子文書は、これまでITの普及が困難だった業務を劇的に改善する可能性も秘めています。電子署名を利用した、更に効率的な電子社会へと移行させるために、これまでの人々が「最適」と思ってきた実務の意識を変える必要もあるかもしれません。

法制度との関係も深い電子署名は、法制度的な課題も多々あるという指摘もあります。電子署名法、IT書面一括法、e-文書法などIT関連の法制度の整備は進んでいますが、民事法領域のIT化対応には課題が多く、例えばこれまで商取引を支えてきた手形法は、紙の手形を前提としています。結局のところ、現在の社会は「紙と押印」を前提にした社会であり、様々な法制度も紙文書を前提に最適化されており、電子文書を前提にした社会への移行には大きな変革を伴うことになります。またIT技術による効率化も重要ですが、法制度の観点からは、同時に不正に強く、透明性の高い社会を目指すべきです。そのためには電子署名の普及は重要な意味を持つはずです。

電子署名の普及は、電子署名法自体がネックとなっている面もあります。電子署名法に付随して電子署名法特定認証業務認定制度がありますが、この認

図4



定制度は、良くも悪くも高い保証レベルの証明書を自然人に発行する認証局の認定制度だと言えます。この高い保証レベルは、結果として高いセキュリティ要件の電子署名に利用できることになりますが、その反面高いコストもかかります。電子署名法は、ネットワーク社会の基盤となる法律であり、そのため、この電子署名法の不備による不正などを防がなくてはならないという強い意向が働き、認定基準も非常に厳しいものになっています。これは、不正等が起きにくい一方、使われにくい状況も生み出し、結果としてネットワーク社会の安全、安心を提供するはずの電子署名の普及を阻害している可能性があることに注意すべきです。図4に電子政府における電子署名法特定認証業務認定制度の課題を示します。

2005年に施行された通称e-文書法に関連した動向としてタイムスタンプサービスの普及があります。タイムスタンプサービスの主な方式のうちのひとつは、時刻が何らかの形で保証されたサーバが行なう電子署名によって実現されます。ところが電子署名法は、自然人によるいわゆる自署名がその範疇であり、こうしたサーバによる署名は、電子署名法の対象外となっています。ユビキタスネットワーク社会においては、認証を要するデバイスが人口よりもはるかに多く、またサーバによる署名が、人間が行うよりもはるかに多く想定されます。このような将来社会に対する法制度は、これまでの法制度の延長上にある「電子署名法」などの枠組みだけではカバーできず、新たな枠組みも検討される必要があると考えられます。

■ まとめ

ネットワーク社会への移行という環境変化により、今では顔を突き合せなくてもリアルタイムの取引ができるような状況になりつつあります。これまで契約者同士の取引の時間的地理的な距離のために紙ベースの処理(署名)が必要だった業務であっても、オンラインの電子認証によりその大部分を解決できるように、ビジネススキームからして抜本的に変わってしまえば署名でなく電子認証で済みます。このようなネットワーク社会では、サービス自体が信頼のおけるものであれば、認証及びその後の手続きのログなどを証跡とするといったことが一般的だと考えられます。2001年施行の電子署名法をはじめとする現行のIT技術の関連した法制度は、こうした環境の変化に追随できていない側面があります。こうした中、認証にお

ける基準等は未整備であり、これらにも起因するインターネットバンキング等における犯罪は、「サービス自体が信頼のおけるもの」といったことに疑問を抱かせ、インターネット上のサービスの信頼を揺るがしています。このような状況ではe-Japan戦略の次の目標とされるＩＴ基盤の利活用は進まないでしょう。

一方、電子署名が役に立たないかというと、全くそういったことはありません。「認証とログ」は特定のシステムに依存するため、長期間のセキュリティ（たとえば重要文書の長期保存など）や、組織を超えた広域のセキュリティといったことに対応できないという問題があります。標準化されたデータフォーマットを使い電子署名が施されたデータは、特定のシステムに依存しない独立したデータとしての普遍性を持ちます。これは、正にネットワーク社会に求められていることであるはずです。そして、IT化、ネットワーク化は、利便性のみならず、新たな不正行為をも招いていますが、電子署名は、こうしたことに対抗する技術であるはずです。

電子署名と認証の違いを中心に説明してきましたが、安心・安全なネットワーク社会を構築するためには、これらの技術を適切に使い分けるための技術、法制度、ビジネスモデルの三位一体となった検討がなされるべきでしょう。電子署名の普及が思うように進まないのは、技術、法制度、ビジネスモデルのバランスの悪さに起因しているように思われます。今後、安心・安全なネットワーク社会を目指していく上では、電子署名・認証の更なる技術開発、法制度の整備、新たなビジネスモデル創造などの更なる努力が求められます。

6. 参考

米国のE-Authentication
http://www.cio.gov/eauthentication/
電子認証技術ガイドライン（SP800-63）
http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
偽造キャッシュカード問題と認証システムの考察
http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf
電子署名・認証利用パートナーシップ 2004 年度報告書
http://www.japanpkiforum.jp/shiryou/FY2004/fy2004_jesap_report.pdf
電子署名法の在り方と電子文書長期保管に関する現状調査報告書　平成17年3月（財）日本情報処理開発協会