責任追及性に基づく認証のレベル

菅　知之　　米倉昭利　　加藤寛之
（関西大学）　（電子署名・認証ｾﾝﾀｰ）　（KPMGﾋﾞｼﾞﾈｽｱｼｭｱﾗﾝｽ）

[概要]

ネット社会の発展は目覚しく、今後の可能性に大きな期待がかけられているが、一方ではハッカーや成りすまし等の不安要素も抱えている。非対面・非書面が特徴のネット社会は無責任社会になる潜在的な可能性を秘めているが、無責任社会には善良な市民は入ってこなくなり健全な発展は望めないので、責任追及性の確保が今後の発展のキーポイントである。ネット社会での活動は電子データとして記録されるため、ばらばらに存在する個人情報が容易に収集することができ、その結果として起こり得るプライバシー侵害はネット社会の発展阻害要因となる。責任追及性とプライバシー保護とのバランスこそがネット社会の発展の鍵であり、そのためにはリアル社会との接点を確保して責任追及性を備えた匿名性の導入が有効である。

The level of certification based on the traceability of responsibility

SUGA Tomoyuki (Kansai University)
YONEKURA Akitoshi (Electronic Signature & Authentication Evaluation Center)
KATO Hiroyuki (KPMG Business Assurance)

[Abstract]

The potential growth in the emerging network society is expected to be more fruitful. On the other hand, however, risks of hacking or spoofing are also recognized. Non-documentary and non-face-to-face communication in the network society will surely foster very little sense of social responsibility. Securing the way of tracing responsibility is considered as the key to future growth.

Activities in the network society can be recorded digitally and electronically. Therefore, personal information scattered across wide range of physical location can be easily collected by computers. The infringement of privacy as a result will become serious blocking factor for the development of the network society. The balance between the traceability of responsibility and privacy protection is key to the development of the network society. To this end, introduction of pseudonimity with traceability of responsibility is effective.

1 ネット社会の光と影

インターネットの普及によってリアル社会とは別のネット社会が出現した。インターネットは単なる通信ネットワークというよりも巨大な情報源と情報処理機能とそれらへのアクセス機能との複合体と考えることができる。

インターネットを通信機能として使う応用分野としてメッセージ伝達や意見交換を行うEメールやチャットがある。これらはビジネス面での利用だけでなく趣味的な領域でも使われていて、インターネット利用者の裾野を拡大している。WWWは巨大な情報源へのアクセス機構であり、この出現がインターネットの性格を根底からくつがえしたといっても過言ではない。

電子商取引はこれらの仕組みを組み合わせた応用分野で、企業と消費者、企業と企業、消費者と消費者の間における商取引をインターネット上で行うものであるが、更に一方のプレーヤとして政府や自治体を考えることによって、各種申請などの住民と政府・自治体とのやりとりもインターネット上に乗せる構想が動き出している。

このようにネット社会では直接顔を合わせることなく、買い物や意見交換をすることができ、各種の申請などもネットワーク上で電子的に行うことが出来る。

一方でハッカーによるデータ破壊や盗用がしばしば新聞紙上を賑わせ、泥縄式のセキュリティ対策実施が叫ばれているが、その実施状況は必ずしも充分とは云い難い。またコンピュータウイルスのインターネットを媒介とする伝播による被害もインターネットに対する不安材料の一つである。インターネットの非対面性を利用して他人に成りすまし、買い物をする詐欺の危険性も指摘されている。さらにメールをしつこく送りつけたり、HP（ホームページ）に嫌がらせをするネットストーカまで出現してインターネットには漠然とした不安感がつきまとっている。

ネット社会には利便性をもたらすものとして大きな期待感が寄せられているが、同時に不安感もあってリアル社会と同程度の信頼感を備えた実用性を持つ段階にはまだ至っていない。

2 責任追及性

ネット社会の活動は非対面・非書面が特徴であり、インターネットにつながる端末を実際に操作しているのはリアル社会に存在する人であるにもかかわらず、全く別のネット人格とも云うべきものが存在するかのような錯覚がある。

ネット社会におけるアイデンティティ（以下ではネットネームという）を確認する仕組みとしてPKIベースの証明書を利用する考え方が主流になっている。すなわち、認証局によって発行された証明書と自己のデジタル署名とを併せてネット経由で相手に示す（相手に送る）ことによって自身のアイデンティティを明確にする方式である。

証明書は申請時（登録時）に認証局で行う本人確認に基づいて発行されるが、本人確認の厳密さの違いによって証明の確かさに幾つかのレベルがあり得る。証明書と名が付きさえすれば、どの証明書も同じ確かさで証明しているわけではない。ここでいう本人確認とは本人の申請内容を別の裏付けで確認することである。別の裏付けとして通常使用されるのは他の目的で発行された証明（たとえば運転免許証とかパスポート）であり、別の認証局から他の目的で発行された電子証明書が使われることも有り得る。

本人確認は発行する証明書の利用目的に応じた厳密さで行われる。換言すれば、その証明書が使われる応用分野において必要な責任追及性によって必要な本人確認の厳密さがきまる。厳密な本人確認を経て発行された証明書ほど確かな証明（認証）を行っているということができ、証明の確かさ（認証の確かさ）のレベルという概念を考えることができる。

ネット社会における責任追及性とはネットネームからリアル社会の人格に遡及できることと考えられ、証明の確かさのレベルが高い証明書ほど高い責任追及性を持つと考えられる。換言すれば、責任追及性の確保とは何らかのトラブルが起きた場合に、その相手に対して督促、告訴などの解決のための行動を取れることと考えられる。

責任追及性は実在性と本人性とに分けて捉えることができる。ここで実在性とは申請された名前の人が確かに実在することをいい、本人性とは証明書発行を申請している本人が間違いなく申請名義人であることをいう。本人性は本人だけが携行する（広義の）身分証明書によって証明される。運転免許証、パスポート、健康保険証などが広義の身分証明書に該当する。これに対して実在性を証明するものを事実証明書という。事実証明書は住民票、戸籍抄謄本などのように本人に関する事実を証明するものではあるが、それを携行している人がその本人であるとは限らないものである。実在性が確かであればあるほど、また本人性が確かであればあるほど、責任追及性は高いと考えることができる。

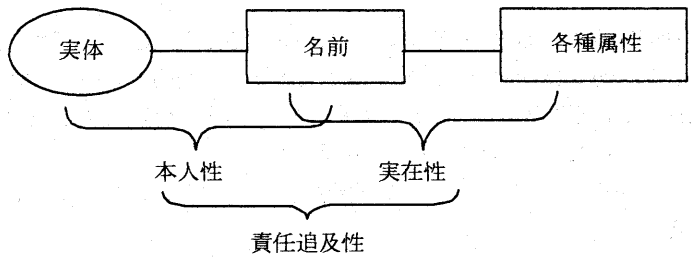

図１　実在性と本人性の関係

実在性／本人性の確認を証明書によって行う場合、その証明書の信頼性が問題になる。証明書の信頼性は、本来の使用目的と証明内容、発行機関の信頼性、証明書の偽造の難しさから判断されるのが普通である。更に本人性の確認に使用される身分証明書では、所持者（提示者）がその証明書の正当な持ち主であることを確認する仕組みの有無とその仕組みの安全さも大きな要素になる。顔写真の貼付はこの仕組みの典型的な例である。

発行機関としては、公的機関の方がその中立性から民間機関よりも高い信頼性を持つと判断されることが多い。偽造対策の観点からは、ただの紙に印刷したものよりも特殊な加工を施されたものの方が信頼性は高い。

前述のように本人確認は提示された証明書によって行うことが多いが、それ以外に各種データベースへの問い合わせ、郵便による確認返送、電話による確認などの手段が使われる場合もある。郵便のあて先は通称などの場合もあり、必ずしも公的に認知された実在性を持つとは限らないが、郵便が届くということには少なくともある程度の社会的な実在性を認めることができよう。

本人性の確かさのレベル（段階）はさまざまに考えることができようが、少なくとも３つのレベルを考えることができる。すなわち、パスポートや運転免許証のような公的機関の発行した顔写真付の身分証明書で確認されるレベル、保険証のような公的機関ではあるが顔写真のない身分証明書で確認される

レベル、何も確証のないレベルである。また、実在性に関しても同様に少なくとも３つのレベルが考えられる。すなわち、戸籍謄抄本や住民票のような公的に認知された実在性を証明する確証があるレベル、郵便が届く事実のようなある程度社会的に認められた実在性が確認できるレベル、何も確証のないレベルである。

本人確認の目的から考えると、本人性の方を実在性よりも優先して考えるべきである。その考えに基づくと、上記のそれぞれの３レベルの組み合わせで意味があるのは次のような４つのレベルになる。

表１　本人性と実在性に基づく認証（証明）のレベル付けの一例

認証のレベル	本人性	実在性	責任追及性
1	○	○	高
2	△	○	中（高）
3	△	△	中（低）
4	－	－	低

3 プライバシーの危機

リアル社会では人は物理的に離れて互いに関連のないさまざまな所でさまざまな行動をとる。それらの行動は記録されないか、電子的でない形での記録に残されるものが圧倒的に多く、記録が残されたとしても全く関連のない場所にそれぞれ存在しているに過ぎない。ある人の行動記録を一箇所に集めて参照する実際的手段がないことが結果としてプライバシー保護をもたらしている。

一方、ネット社会ではあらゆる行動がデジタルな電子情報として把握されるので、それをデジタルな電子的記録として記録することが可能である。

デジタルな電子情報はコンピュータによる処理が可能であり、各所に散在する膨大な記録の中から、ある人の行動に関する記録だけを抽出して収集することが技術的に可能である。名前を含んではいるが名前順に並べてない情報群から特定の名前の情報だけを抽出する処理を名寄せという。これは原理的には人間でも行える処理であるが、人間が行うためには膨大な時間を要するもので、コンピュータの高速性を生かして初めて可能になる処理である。

ネット社会における行動記録が電子的に記録されることと名寄せ処理の技術とによって、リアル社会には元々備わっていたプライバシー保護の要件がネット社会では失われ、プライバシーの暴露が起こる可能性が十分ある。

ECOMで実施したアンケート調査においても、自己に関するデータ流出の心配がECに対する不安材料のトップに挙げられているのは、上述のネット社会におけるプライバシー暴露の可能性が感覚的に認識されている証左であろう。

4 責任追及性を備えた匿名性

リアル社会における行動はネット社会でのようには記録が残されないことがプライバシーを保つことに役立っていることは前述の通りである。さらにリアル社会での行動には無名性、匿名性のものがかなりあり、それが対面社会でありながらプライバシーを保つ安全弁として機能している。駅のキオスクで新聞を買う時に誰も名前を名乗ることはしないし、食堂で何かを食べる時に名前を聞かれることはない。その場で取引が完了して、貸し借りの状況が残らない場合には無名性・匿名性が保たれる。

前述した様に、ネット社会では名寄せ技術のよってある名前の下に行われた行動全てが明らかにされてしまう可能性がある。ネット社会を無責任社会ではない健全なものにするためには、ネットネームを

実名だけに限定する考え方があるが、この場合にはプライバシーを保てなくなる可能性が高い。そこでの全ての行動に際して実名提示が義務付けられるとすれば、ネット社会はリアル社会よりも窮屈な社会になってしまう。その結果としてプライバシーが暴露されても実害のない活動だけが行われる社会に留まってしまい、ネット社会の大きな発展は期待できない。

ネット社会において匿名の使用を認めるとすれば、上述のようなプライバシーの問題は起こらないが、非対面に加えて匿名ということになれば極めて無責任な社会になる可能性が高い。従って単なる匿名ではなく責任追及性を備えた匿名の仕組みが必要である。

ネットネームを用いる時にはPKIに基づく証明書をネット上で提示して、自身の身分証明とすることについては前述した通りである。この仕組みにおいて証明書を発行する認証局はリアル社会とネット社会との両方に属する存在であり、二つの社会の唯一の接点と考えることができる。

認証局のこの性格を利用して、ネットネームとしては匿名（仮名）を認めながら（証明書上には匿名だけを表記することを認めながら）、責任追及性を確保する仕組みが可能となる。認証局では証明書発行申請時は実名に限って本人確認を実施すれば、その厳密さに応じたリアル社会における責任追及性を確保できる。匿名（仮名）と実名との対応は認証局だけが把握し、法執行機関からのしかるべき要請がない限り、その対応の秘密性が守られる仕組みは、責任追及性を確保した匿名の使用を実現するものである。

匿名を使用することによって、ネット社会において複数のアイデンティティを使い分ければ、名寄せによるプライバシーの暴露を自らの責任で防ぐことができる。

ネット社会での原則は匿名と実体との対応の確実さに応じたサービス提供である。対応の確実さを示すのは認証書上に表示された認証（証明）のレベルである。認証（証明）のレベルの高い認証書によって自分のアイデンティティを示す人には匿名であっても高度なサービスを、認証（証明）レベルの低い認証書しか示さない人にはそれなりのサービスしか提供しないというのが基本的な考え方である。

本来、匿名に対してはある程度以上の信頼感を持てないわけであるが、本当の身元を認証局が把握していることを示す認証のレベルが表示されていることで、匿名に対しても信頼感を持つことができる。

5　まとめ

ここでは認証局による証明行為の確かさにレベルを導入することにより、ネット上で提示されるアイデンティティの信頼度に幅を持たせ得ることを指摘し、その概念を匿名と組み合わせることによってプライバシー保護の方策とすることを提案した。「電子署名および認証業務に関する法律」における特定認証業務の認定も証明の確かさにレベルがあるとする考え方に立つものと推測できる。

リアル社会においてアイデンティティ提示の手段として広く用いられている印鑑では実印、銀行印、認印の使い分けが行われている。これは印影登録の有無、その登録時の本人確認手続き、印鑑証明書の有無からくる信頼度に基づく使い分けである。このように登録時の本人確認の厳密さに基づく信頼度のレベルをアイデンティティ提示手段に持ち込む考え方はリアル社会での従来からの慣行と十分連続性があり、ネット社会においても実現しやすいものと考える。