1F4

情報セキュリティからみた電子署名法の特徴と問題点

(筑波大学　大学院システム情報工学研究科)小出篤史・
(同　大学院人文社会科学研究科)星野豊・
(同　大学院システム情報工学研究科)岡本栄司

Features and Problems of Digital Signature Law from a Viewpoint of Information Security

Graduate School of Systems and Information Engineering, University of Tsukuba
Koide, Atsushi;
Graduate School of Humanities and Social Sciences, University of Tsukuba
Hoshino, Yutaka;
Graduate School of Systems and Information Engineering, University of Tsukuba
Okamoto, Eiji

電子署名法・電子化基盤社会・情報セキュリティ・人間的側面・技術的側面

１．はじめに

デジタルコンテンツを主体とする社会を「電子化基盤社会」とよぶならば、電子化基盤社会の実現に向け、立法をはじめとする法律論と併せ、それを実現するための要素技術についても今後は等しく重要になってくることが考えられる。これら要素技術を「不当な利用を排除」という側面に注目し、情報（財に関する）セキュリティという点からみたときには、暗号や認証といった音楽や映像などのデジタルコンテンツの限定受信などの著作権管理技術がよく知られているが、デジタルコンテンツにおいて反復かつ継続的になされる「申込、契約」という側面を考えるならば、「確かに申し込みした」ということを電子的に保証するための技術－電子署名が不可欠なものとなっていくことが考えられる。

本報告では、2001 年に施行された電子署名法の概要に触れ、次いで計算量的な安全性について説明する。その上で、想定事例をもとに安全性についての特徴と問題点を提示する。

２．電子署名法の概要

２．１　電子署名の特徴と電子署名法

「電子署名」とは、人が行う署名や押印を電子的に行うものと解される。従来の署名押印についての検証は、人による筆跡鑑定によりなされていたため、「おそらく本人がした本人のサインらしい」程度しか判明しなかったが、電子署名では、電子証明書や公開鍵といった電子データを利用して、少なくとも本人の署名と同一か否かについては、確定した検証を行うことができる。

電子署名法（電子署名及び認証業務に関する法律）は「電磁的記録に記録された情報について本人による電子署名（略）が行われているときは、真正に成立したものと推定する。」旨規定している（3 条）。このように、電子署名は暗号をはじめとする技術上だけでなく、法律上にも一定の裏付けがなされており、契約書の記名捺印など証書ベースの紙で行っていたものが電子化されることが期待されている。

２．２　電子署名の効力

電子署名法において規定する電子署名とは、より重要な契約を想定しており、実社会における実印と印鑑証明書に相当するものであると説明されることが多い。

民事訴訟法 228 条 1 項は「文書は、その成立が真正であることを証明しなければならない。」と規定しているが、文書の真正を疑わせるものとして、なりすましや強迫、錯誤など、さまざまな抗弁事由が存在し、厳格な立証責任を課すことは、当事者にとって酷な結果になりかねないため、同条 4 項では、「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」と規定することにより、極度の立証責任を負わせることを回避し、本人又はその代理人の署名又は押印がある場合における私文書の法的安定性を確保している。

一方、電子署名法は「電磁的記録に記録された情報について本人による電子署名（略）が行われているときは、真正に成立したものと推定する」（3 条）ものであるから、電子署名があれば、本人又はその代理人の署名又は押印がある私文書と同等のものと推定されるので、民事訴訟において証拠として提出すれば裁判所に採用される可能性は高いことになる筈である。

２．３　電子署名の仕様と利用例

電子署名法に規定される具体的な電子署名の仕様については、「電子署名及び認証業務に関する法律施行規則」において以下[1]の通り定められている。

第二条　法第二条第三項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。

一　ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因数分解

二　大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算

三　楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算

四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

これは、素因数分解問題や離散対数問題といった一定の計算量的に難しいとされている問題を仮定しているものと考えられる。

現段階で、電子署名法に規定される電子署名が利用されている例としては、平成 19 年分及び 20 年分の個人所得税の確定申告における e-Tax での申請について、時限立法ではあるが 2 年間で最大 5,000 円の特別控除を認めており、税額控除という金銭的なインセンティブを付与することで、限定された意味ではあるが、利用の促進が図られている。

３．電子署名をめぐる問題点

電子署名法に規定される電子署名そのものの安全性は前述したとおり、素因数分解問題や（有限体上や楕円曲線上の）離散対数問題といった一定の計算量的に難しいとされている問題を仮定した上で成り立っていることを想定している。

電子署名法は、紙ベースの証拠調べ中心である現行法下では、デジタルデータそのものが証拠として採用されうる余地を成文化したという意味において画期的なものである。しかし、電子署名を利用する環境、電子署名インフラを、情報システム上で行われる社会システム、社会基盤としてとらえた場合には、また考慮すべき側面が存在する。

第一は、人である。電子署名のパラメータ生成、作成、検証おける電子署名のライフサイクル全般には、認証機関における電子署名基盤がかかわっている。電子署名基盤は確かにコンピュー

[1] 一は、ＲＳＡ署名、二は、ＤＳＡ署名、三は、楕円ＤＳＡ署名、四は、例えば双線形性ペアリングを用いたもの（ショート署名など）が対応するものと考えられる。同等の安全性を基準にした場合、ショート署名は三に規定する「 楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算」の困難性に基づきながらも、楕円ＤＳＡ署名 に比較して署名サイズを半分程度に低減できることが知られている。

タが中心であるが、それらを利用するのは人間であり、それらを攻撃するのもまた人間であることを考えると、電子署名の安全性に関して、人間的側面からの考察を行うことはごく自然であるとともに、最も重要な観点である。

第二は、技術である。電子署名における技術的な安全性は、計算量的に難しいとされている問題に基づいているとされている。確かに、計算量的に難しいとされている問題の仮定が破られれば、電子署名の安全性は崩壊することになる。しかし、電子署名の安全性は、第一の人間的側面を除いても、計算量的に難しいとされている問題以外にも存在することを保障しているわけではなく、現在判明している限りでも若干のリスクが存在する。

従って、以下では、電子署名をめぐるリスクとして、人間的側面からのリスク、技術的側面からのリスクからの２つの側面から検討する。

４．電子署名をめぐるリスク

４．１　人間的側面からのリスク

電子署名の安全性を、電子署名を管理する認証機関について検討してみる。電子署名のパラメータ生成、作成において、署名を作成するための鍵（秘密鍵）の管理の問題があげられる。伝統的な（理論上における）電子署名方式では、秘密鍵は秘密であり漏洩することはないと仮定していた。しかしながら、実社会おいては情報流出事件が近年引きも切らず現実に発生しており、この仮定は性善説に過ぎ、現実に即していないというべきである。そこで、認証機関において内部犯行者の故意によるケースと組織的な管理体制不備などの過失による 2 点から電子署名の人間的側面からのリスクについて検討してみたい。

４．１．１　内部犯行者など故意によるもの

第一は、認証機関における内部関係者の不正によるリスクが考えられる。悪意のある内部関係者（内部犯行者）は、内部犯行者単独で特定の利用者の電子署名を秘密鍵により作成し、利用者の同意を得ずに内部犯行者の有利になる契約を行うこと等が考えられる。しかしながら、結果としての契約内容が内部犯行者に有利となっていることから、何らかの「足がつく」ことは避けられないため、内部犯行者の単独犯行はレアなケースであるといえる。

内部犯行者のほかに不正利用者と結託して加害行為を行うことも考えられる。例えば、二重売買によって発生した権利は対抗要件を備えた第三者に対抗できないことを利用し、土地、建物の売買を仮装して不正な利得を得るケースである。議論を民事法上に限定するならば、内部犯行者と不正利用者が結託していることが立証されない限り、無効ないし取消は困難である。

４．１．２　組織的不備など過失によるもの

第二は、認証機関における何らかの組織的な不備によるリスクが考えられる。認証機関のコンピュータをはじめとする情報システムにおいて、認証機関として当然行うべき管理上の問題がある場合に発生するリスクである。コンピュータ上にウイルスや不正侵入などのセキュリティ対策をしていない、あるいは、サーバの設置している場所に入退室についての認証や記録などセキュリティ対策がされていない、などの場合が考えられる。このような場合は、不正な第三者が認証機関に侵入し、得られた秘密鍵をもとに署名作成が可能になることになり、得られた秘密鍵を匿名掲示板や裏サイトなどに書き込むことにより、さらに 2 次被害、3 次被害が引き起こされる。もし、このような事態になれば、既存に流通している正当な電子署名のみならず、電子署名のそのものの信頼が揺らぎかねないことが想定される。

４．２　技術的側面からのリスク

電子署名をめぐる 30 年にわたるビルドアンドスクラップの技術的歴史を長いとみるか短いと見るかはさておき、現在判明している限りでも若干のリスクが存在する。以下では、計算手法の進化によるものとコンピュータの進化によるリスクについて検討してみたい。

４．２．１　計算手法の進化によるもの

素因数分解問題や離散対数問題など、一定の問題を仮定しているが、技術的進歩により仮定が破られた例も存在する。例えば、判定 DH 問題[2]という計算量的に困難であるとされた問題がある。ところが、後に双線形性ペアリングというものができたことにより、判定 DH 問題そのものが多項式時間で判定することができるようになってしまった。かつては、本問題に基づいた電子署名を利用した応用システム（例えば、電子マネープロトコル）が提案されていたが、これらの安全性の基盤が揺らぐこともないわけではなかった。

しかしながら、 素因数分解問題や離散対数問題などの問題に基づいた RSA や DSA は、世界中の暗号研究者が効率的な解読方法について日々研究をおこなっている中、20 年程度近くも破られていないため、今後においてもおそらく破られることはないだろうといわれている。

４．２．２　コンピュータの進化によるもの

電子署名に利用されるパラメータについては、RSA での安全性を基準にしたとき 1990 年代前半では 512 ビットで充分な安全性が確保されているといわれていたものの、1990 年代後半には 1,024 ビットが推奨されるようになり、近年ではさらに 2,048 ビットが有力になりつつある。ムーアの法則に従ってコンピュータの性能が向上するならば、時間さえかければ解けるようになるかもしれないリスクはもちろん指摘されうる。ところが、パラメータの長さと計算時間の関係は、現在発見されている最も高速といわれている計算手法によったとしても、パラメータを長くすれば指数関係に準じて計算所要時間が増加する（準指数時間）関係にあるといわれている。そうであるとすると、前述した施行規則の仕様にのっとれば 100 年後における電子署名の安全性は疑問を投げかけざるを得ないが、今後 10 年～20 年程度では（直ちに偽造が可能になるという程度の）安全性については問題がないと結論づけられることになる。以上が、電子署名の安全性をめぐる通説であるが、その一方において根本を覆すような問題も指摘できる。

現在のコンピュータは、チューリング機械という計算モデルに従って設計されている。量子チューリング機械という近い将来実現するであろうと期待されている新しい計算モデルに基づいたコンピュータが提案されている。量子チューリング機械には量子重ね合わせという並列での計算結果の重ね合わせ効果により、どんなに高速な CPU を利用しても、従来のチューリング機械モデルのコンピュータでは準指数時間程度の膨大な時間がかかっていた計算が、無視できない確率で現実的時間に相当する多項式時間で解読できるといわれている。しかしながら、量子コンピュータそのものについての実現もさることながら、仮に実現したとしても、量子重ね合わせの結果からの解の識別が難しいという課題があり、まだまだ多くの時間がかかるものと予想される。

(参考文献)・中山信弘、「工業所有権法（上）特許法 第二版増補版」、p.5、弘文堂、2000 年
・内田勝也、「情報セキュリティ心理学とトラストの動向について」、2008-CSEC-41、pp. 7-12、2008 年
・西野哲朗、「量子コンピュータ入門」、東京電機大学出版局、1997 年

[2] G を素数位数 q の巡回群、g を G の原始元、a, b, c をランダム値とする。このとき、(G, q, g, g^a, g^b, g^{ab})と(G, q, g, g^a, g^b, g^c)を識別する問題のことをいう。