コンピュータセキュリティ 11−11
（2000．9．8）

印鑑と電子印鑑 — 歴史と類似性の分析 —

佐々木良一　日立製作所システム開発研究所
郵便番号 244-0817 横浜市戸塚区吉田町２９２
sasaki@sdl.hitachi.co.jp

あらまし：インターネットの普及に伴い拡大している電子商取引の安全性を確保するための基本技術が電子印鑑（米国ではデジタル署名）である。その電子印鑑をさらに使いやすく、安全なものにするため、（１）印鑑と電子印鑑に関し、それぞれの歴史と利用形態、機能、不正使用方法などを調査し、（２）その上で、それらの類似性と相違点を分析した。その結果、電子印鑑の（１）証拠能力持続に関する信頼性の向上対策や、（２）捺印の実感欠如対策等が重要な課題であることを明らかにすることができた。
キーワード：デジタル署名、公開鍵暗号、歴史、セキュリティ、電子印鑑

Seal and Electronic Seal - Study on Their Histories and Similarities -

Ryoichi Sasaki, Systems Development Laboratory, Hitachi Ltd.
292 Yoshida-Cho Totsuka-ku Yokohama, 244-0817 Japan
sasaki@sdl.hitachi.co.jp

Abstract: Digital Signature or Electronic Seal is a basic technology for achieving security of extending Electronic Commerce on the Internet. In order to make Electronic Seal safer and easier to use, we researched the history, function and illegal usage of the Seal and the Electronic Seal. By comparing those of the Seal and the Electronic Seal, we found that (1) evidence ability of Electronic Seal for long duration and (2)reality of using Electronic Seal are important issues.
Keywords: Digital Signature, Public Key Cipher, History, Security, Electronic Seal

1. はじめに

インターネットの普及に伴い、電子商取引が急速に拡大してきている．この、電子商取引の安全性を確保するための基本技術が電子印鑑（電子捺印ともいう。米国ではデジタル署名Digital Signatureや電子署名Electronic Signature と呼ぶ。）である。電子印鑑の技術があったからこそ電子商取引が可能になったという意味で、電子印鑑とその基礎となった公開鍵暗号の技術は 20 世紀の最大の発明の１つといって良いだろう。

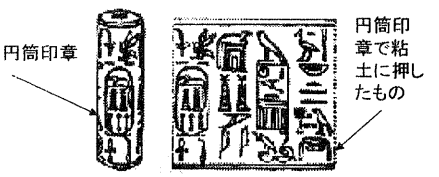
本稿では、印鑑（印章やはんこともいう）と電子印鑑に関し、それぞれの歴史と利用形態、機能、不正使用方法などの類似性と相違点を明確化すると共に、類似性の分析結果から電子印鑑をさらに使いやすく、安全なものにするための提案を行う。

なお、以降、印鑑を押すことを捺印、押したものを印影と呼ぶことにする。

2. 歴史

2.1. 印鑑の歴史[1)−4)]

印鑑は今から５５００年ほど前にシュメール人が初めて使用したといわれている[4)]．文字は今から約５１００年前、同じくシュメール人が発案した楔型文字が世界で最初のもの



（エジプト）

図1 円筒印章の一例

であるといわれているから、文字の無い時代に印鑑が使われていた事になる。文字の無い時代にどのようにして印鑑が使われたかという事であるが、以下のようにすることにより、大切なものの不正な抜き取りを防止したようである。

（1）粘土で出来た小さな物体であり、商品の種類を示す「数え駒」（トークン）を商品の数だけ用意し、全体を粘土で丸く包んだものの上に捺印し、それを商品と一緒に相手に送ったといわれる。

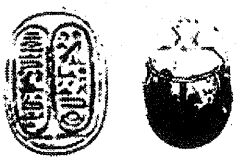
（2）また、特定の財貨を入れた荷物を縄で縛り、その結び目を粘土隗で覆って、その上に印章を捺したと言われる。いわゆる封印である。

この当時の印鑑は円筒印章と呼ばれるもので、大理石などで出来た円筒の周りに刻印を施し、それを粘土などの上で押し付けつつ回転させることにより印鑑の持ち主しかつけられないマークをつけたのである（図1参照）。その後、円筒印章は、財貨を保護するための壷，瓶、籠などの容器を保護するのに用いられるようになった。ここでは、壷などの口の部分を布で覆い、縄で縛ったものの上を粘土で覆いここに円筒印章によってしるしをつけたのである。このように円筒印章は所有権を主張し、財産を保護するためのもっとも効果的な手段とみなされ、鍵が無い時代にその代用を勤めたのである．電子印鑑においては、公開鍵暗号の秘密鍵の使用が捺印のトリガーとなり、鍵と印鑑は強い関連を持つが、ここでも鍵と印鑑は関連があったのは興味深い。

その後、文字が現れ、粘土板などの上に文字を書きそれに、双方の印鑑で捺印を施すことにより契約を行うようになっていく。

どの国も最初は円筒印章を使ったようであり、エジプトにおいても最初は円筒印章が使われた。4400 年ほど前の第六王朝時代よりコガネムシの形をしたスカラベ印章（図2参照）が長く使われた。この時代、パピルスに書いた文書に直接捺印するのではなくパピルスを丸め周りにひもで縛り結び目に粘土をかぶせスカラベ型印章で封印したようである。円筒型印章と比べ、小さな物にも簡単に捺印できた。

今から 3500 年ぐらい前になるとヒッタイト人が、ボタン型印章に長い柄をつけたスタンプ型印章を使い始めた。その後、ササン朝ペルシャなどでは円錐型印章やドーム型印章が使われるようになっていく。



（エジプト）

図2　スカラベ型印章の一例

古代ローマでは、当時の衣服にポケットが無かったこともあり，指輪型印章がひろく使われた様である。かって、ローマ人が契約のときに使った鉄製の指輪型印章が婚約の場合にも用いられ、男性がこれを婚約者の左手の薬指にはめると婚約が成立するものとされていたという[1]。なお、当時左手の薬指は直接心臓につながっていると信じられていたようである。

中国の印章の使用は、メソポタミアなどに比べかなり遅く、実物によって確認できる最も古い印章は、周王朝後期の戦国時代（紀元前 480—221 年）のものだと言われている[1]。一方、紙は紀元１０５年に中国の蔡倫が発明したと言われており、5世紀には紙が広く使われるようになってきた。これに伴い、6世紀初頭になって、朱泥を使い紙に直接的にハンコを押すようになってきたという。

日本における印章は、金印（図3参照）などのように中国から与えられたものは古くからあったようである。しかし、官印として広く使われ始めたのは奈良時代になってからであり、戦国武将が私印として印鑑（図3参照）を好んで用いた。江戸時代には農民や町人もハンコを使っていたようであり、ハンコを彫ることが職業として成り立っていた[3]。

紀元57年の金印

武田信玄の印章

上杉謙信の印章

図3　日本の印章の例

2.2. 印鑑と署名

ヨーロッパで、自筆で署名が行われるようになるのは、15 世紀からで、（1）教育の普及により読み書きの出きる人が増え識字率があがったことと、（2）ルネッサンス以降の人文主義の昂揚により、個人の人格に対する自覚が生まれたことによるといわれている[1]。15 世紀から 16 世紀にかけては各種の文書において印章と署名が重視されるようになり、19 世紀になると印章はほとんど署名に取って代わられた。その後も、信書の封印に赤い蝋を落としその上に印鑑をおすという習慣は 20 世紀のはじめまで続けられたが、それも今では使われることは少ない。

一方、日本では未だに印鑑が中心になっている。日本でも戦国時代から江戸時代の初期

に武将などが用いた花押（図４参照）は署名の一種であるがその後あまり使われなくなった。江戸時代以降の日本の識字率は世界でもトップクラスであったといわれており、識字率の低さが署名の普及をはばんだとは考えにくい。ヨーロッパで署名が使われ、日本で印章が使われることについては、（１）日本では、個の確立が不十分であり、個人ベースの署名ではなく、家や組織をあらわす印章が使われたとか[1]、（２）西欧の署名は、神への誓約としてなされるので、署名を真似る心配が無いのに対し、神を持たない日本では根付かず、上から下へと下賜される官印の延長として印章が使われている[5]とか、（３）江戸時代に苗字を持つのが百姓にとって特権であり、その特権意識を満たすために姓を刻した印章を持つようになったが、明治時代になり全ての人が姓を持つようになってもその習慣が続けられた[3]、とか言われるがどれも説得性に乏しい。今後、その理由を探っていきたいと思う。

2.3. 電子印鑑の歴史

公開鍵暗号の概念が１９７６年に Diffie と Hellman によって、論文６）の中で提案され、同じ論文の中で Digital Signature の概念が提案されている。ただし、ここでは具体的な公開鍵暗号の方式は提案されておらず、その後，1978 年（特許としては 1977 年に出願）に Merkle と Hellman によって発表されたナップサック暗号は 1982 年に Shamir によって解読されてしまった。現在でも使われている具体的な公開鍵暗号方式 RSA は、1978 年に当時 MIT にいた Rivest, Shamir, Adleman の 3 人によって開発された[7]。論文の表題からも Digital Signature すなわち、電子印鑑の実現を最重要な課題にしていたことが分かる。

徳川家康の花押　　織田信長の花押

図4　花押の一例

その後、公開鍵暗号方式としては、ラビン暗号や、エルガマル暗号、楕円曲線暗号などが開発され電子印鑑にもちいられている。また、デジタル署名（電子印鑑）専用の方式であるＤＳＡやＥＳＩＧＮなども開発された。

いろいろな捺印（署名）の形態を電子の世界で実現するための種々の方式の開発も行われてきた。例えば、多重捺印や電子仮捺印、しきい値捺印、ブラインド捺印、否認不可捺印などがある。これらの中でも、1983 年にオランダの Chaum によって開発されたブラインド捺印（署名）[9]の活用範囲は大きい。これにより電子投票や電子マネーにおける匿名性の確保が可能となった。

電子印鑑システムが最初にいつ頃実用化されたかは不明である。日立の宝木らは、1987 年ごろには、２者間で安全な取引きを可能とするため電子仮捺印を利用した双方向電子捺印のプロトシステムを開発し、実験を行っていた[8]。そこでは、RSA 処理の高速化のために、ファームウエアの開発も行い、ＲＳＡ暗号の 512 ビット鍵長の印影（署名）を一つ作るのに 0.13 秒で実現している（当時のパソコンでは 5 分以上かかっていた）。日立の製品としては、1994 年にグループウエアソフト GroupeMax に電子捺印の機能を組み込んだのが最初である。

公開鍵暗号や電子印鑑が暗号の専門家以外に広く知られる様になったのは、

表1 印鑑と電子印鑑の歴史

印鑑	年代	3000BC　2000BC　1000BC　紀元　1000AD　2000AD
	外国の出来事	△シュメール人が円筒印章使用　△印章から署名へ （△シュメール人が楔形文字使用）　△中国で紙に朱泥捺印 △粘土版の契約書に捺印　△中国で印章使用
	日本の出来事	△金印拝受△私印の普及 △官印の使用
電子印鑑	年代	1975年　1980年　1985年　1990年　1995年　2000年
	外国の出来事	△Hellmanら概念提案(1976年)　△PGPで利用△SSL/SET △Rivestら具体的方式を提案(1978年)　での利用
	日本の出来事	△双方向捺印実験 △GroupMaxで利用

Zimmermann が電子印鑑の機能を組み込んだPGP（Pretty Good Privacy）を配布した、1992 年頃からだろう。現在では電子商取引用プログラムや WWW 用のブラウザソフトなどの中で広く用いられている。

表１に示すように、印鑑が５０００年以上の歴史を持つのに対し、電子印鑑は２０年強の歴史しか持たない。しかし、公開鍵暗号はこの２０００年の最大の発明に上げる人がいるほど画期的なものであり、その応用システムである電子印鑑も非常に影響の大きい発明である。この電子印鑑の発明の栄光は、Diffie と Hellman ならびに Rivest, Shamir, Adleman の両方にささげられるべき物であり、どちらの貢献がより大きいかといえば前者であると思う。

なお、１９７６年以前に英国や米国において公開鍵暗号に関する開発が行われたという説もあるが確認できていない。今後の課題である。

3. 印鑑と電子印鑑の比較

3.1. 印鑑と電子印鑑の基本的機能の関連

紙の世界では取引きにおいて証拠性を保つため、図５に示すように、（１）紙の上にインクなどの消えないもので取引き文書を書き、（２）双方が印鑑を押し合うという形で対応してきた。これにより、（１）文書が改ざんされてないことを示すと共に、（２）印鑑という本人しか持ってないものを使うことにより、本人がその取引に合意していることを示している。（１）は万国共通のものであるが、（２）は、それぞれの国の文化に依存するものであり、西欧などでは署名が用いられてきた。なお、（１）の機能をメッセージ認証機能とよび、（２）の機能をエンティティ認証機能とかユーザ認証機能と呼んできた。

このような機能をコンピュータの世界で実現するにあたり、印影などの原情報をそのままデジタル化して、電子商取引文書につけたのでは簡単に不正を行うことが出きる。コンピュータを用いればその取引文書を修正したり、印影などを他の取引文書に移すことは容易であるからである。

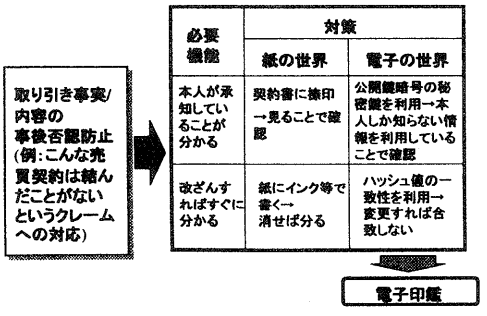


図5 印鑑と電子印鑑

このような問題を解決するための手段が、図５に示すように公開鍵暗号を利用する電子印鑑（デジタル署名）である。ここでは、（１）本人しか知らない公開鍵暗号の秘密鍵が用いることにより、本人が承知していることを示し、（２）ハッシュ値などの一致性を検証することにより改ざんすれば分かる仕組みになっている。

ところで、電子印鑑（デジタル署名）は印鑑と署名のどちらにより近いだろう。鍵の管理と印影の生成にＩＣカードのような持ち物を使う点で、報告者は印鑑に近いと思う。

3.2. 印鑑登録と印鑑証明の機能の比較

日本では、印鑑登録や印鑑証明（より正確には印鑑登録証明）が官庁によって行われており，個人用印鑑は市役所や町役場などが、法人用印鑑は法務省で扱ってきた。

電子の世界では、このような事を行う機構を認証局（Certificate Authority 略して CA）といい、認証局サーバを利用し、公開鍵暗号などの技術を用いて行っている．認証局のサービスは、法務省などの官庁だけで無く、VeriSign などの民間組織でも行われている。

今から４１００年ほど前のハムラビ王治下のバビロニアでは、印章をなくした場合には、悪用を防ぐため紛失の事実が公告されるような仕組みになっていたと言う[1]。ここでは、印章の特徴、所有者の名前、紛失の日時などが記載され、証人および書記が捺印することにより、該当する印章の効力停止が正式に公示されたのである．電子の世界の認証局においても失効リストの管理は重要な機能であり、類似の処理が行われている．

以上より、印鑑登録や印鑑証明、印鑑失効に関する処理は電子の世界と現実の世界で良く似たものになっているといえる。

なお、他国でも官庁によって、実際の印鑑や署名の登録や証明、失効などの処理が行われているかについては現状では不明である。また、電子印鑑の認証局サービスについては、１９８０年頃にはＭＩＴで既に研究が行われていたようであるが原典にあたっていない。この詳細についても今後の課題である。

3.3. 不正に関する比較

印鑑に関する不正は表２のようなものが考えられる。まず、印鑑の偽造は、以下のようにすることにより実現できる。

（１）他人の実際の印鑑と類似のものを偽造する：優秀なハンコ職人を確保することで可能である。最近のパターン認識技術と、印をロボットに作らせる技術を使えば容易に実現できるであろう。

（２）他人に成りすまして、偽の実印を登録する：本人に成りすませれば予想以上に簡単な処理で登録することができる。

また、取引き文書の偽造は以下のようにす

表2 印鑑と電子方式における不正方式の対応

	紙の世界（印鑑）	電子の世界（電子印鑑）
印鑑の偽造	（1） 他人の実際の印鑑と類似のものを偽造する	（1‘） 公開鍵暗号の秘密鍵を不正に入手する
	（2） 他人に成りすまして、偽の実印を登録する	（2‘） 自分の作成した公開鍵を他人の公開鍵だと偽る
文書の偽造	（3） 実際に朱肉を使い押した印影を、ハトロン紙などで押さえて写し、それを別の契約文などの捺印欄に押し付けうつす	（3‘） 直接的に対応する不正はない：ただし、捺印付きの取引き文書自体をコピーするなどによる不正は可能
	（4） 文書を作成し、印を押させ、その後、文を追加する	（4‘） 直接的に対応する不正はない：ただし、正当な取引き文書のハッシュ値と同じになる別の文書を作れれば不正を行うことが可能

ることにより可能である。

（3） 実際に朱肉を使い押した印影を、ハトロン紙などで押さえて写し、それを別の契約文などの捺印欄に押し付けうつす：20年ほど前に銀行で実際にこのような事件が起こっている。

（4） 文書を作成し、印を押させ、その後、文を追加する：文を追加すれば分かるような書面を通常作るが、だましてブランクにしておいて、後で追加するなどは可能である。

紙の世界の印鑑は安全だと考えられがちだが、いずれも、不正が予想以上に簡単である。これを防止するために、（a）対面処理を行うことにより実行の意思を鈍らせたり[12]、（b）重い処罰を設けることにより不正の発生を抑止してきた。しかし、印章の偽造やこれを用いた文書の偽造は昔から繰り返し行われてきたようであり、いろいろな罰則が記述されている[3]。中世の日本では、「御成敗式目」の中に、「謀書」の罪は、武士の場合は領地を没収し、所領の無いものは流罪、庶民の場合は焼印と規定されている。江戸時代は文書偽造の首謀者は引き回しの上獄門、共犯者も死罪を課せられたという[3]。さらに、外国でも、ヨーロッパの古文書学は、文書の真偽を究明しようとする努力の中で発達したものだと言われている[3]。

印鑑に対するそれぞれの不正方法に対応する電子印鑑に関する不正も、表2に示す通りであり、以下のようなものがある。

（1‘）公開鍵暗号の秘密鍵を不正に入手する：公開鍵暗号の解読やＩＣカードに対する耐タンパー攻撃により可能である。

（2‘）自分の作成した公開鍵を他人の公開鍵だと偽る：認証局への登録時に、他人に成りすますことにより可能である。

（3‘）直接的に対応する不正はない：ただし、捺印付きの取引き文書自体をコピーするなどによる不正は可能である。

（4‘）これも直接的に対応する不正はない：ただし、正当な取引き文書のハッシュ値と同じになる別の文書を作れれば不正を行うことができる。ただし、これは一般に、計算量的に困難である。

印鑑と電子印鑑の両方について、不正方法の十分性の検討や、不正と罰則[10]等の調査をさらにしていく必要がある。

4. 電子印鑑の改良方向

以上述べたように、印鑑と電子印鑑は基本的には同じような機能を果たしている。しかし、電子印鑑の長所には次のようなものがある。

（1） 離れたところで印影付きの文書の作成が可能：ネットワークを経由して電子的な商取引が可能である。

（2） 捺印後の文書の改ざんが困難：ハッシュ値を用いることにより、文書の追加や改ざんが容易に検知できる。一方、紙の世界では、文字を追加しても気がつかない場合がある。

（3） 電子印鑑はデジタルデータなので物理的な表現形態を選ばない[15]：いかなる表現形態の電子文書にも添付することができ、文書と印影のデータを紙に印字することもできる。

一方、電子印鑑の短所は以下のようなことが考えられる。

（1） 証拠能力の持続に関する信頼性[13]：紙の世界では、50年以上にわたり、多くの印影付きの文書が保管され、証拠として有効に機能してきた。電子印鑑は、50年以内に秘密鍵を入れたＩＣカードが壊れたり、公開鍵暗号が破られたりする可能性が否定できない。

（2） 印影付き書類全体のコピーと再使用の可能性[13]：紙の世界では、印影付き

文書全体をコピーしたものは証拠とならなかった。電子印鑑では、印影と文書を丸ごとコピーするとそれらは、証拠として機能してしまう。したがって、電子マネーや電子小切手に、電子印鑑を適用する際はこの問題の解決が必要である。

（3）印鑑が盗まれた場合の検知[13]：紙の世界では印鑑が盗まれれば、実際に印鑑がなくなっているのですぐに分かり、紛失などの対応により対策を講じることができた。これに対し、電子印鑑では秘密鍵がコピーされ盗まれてもすぐに検知できるとは限らず、対策が遅れ、被害が大きくなる可能性がある。

（4）実感の欠如：紙の世界の捺印は、取引き文書が読めれば、どんな取引きかが分かり、捺印したことも、自分の印鑑に対応し、文書に朱肉がつくことによって確認が容易である。一方、電子印鑑における捺印機構は、本人の意思どうりに動いているかどうか確認するのが困難である[12]。

（2）（3）については、かなり研究が進んでいるが、（1）と（4）については、まだ緒に就いたばかりである。これらの研究の進展が待たれる。

上記の（1）に関連して著者らは、暗号が破られても電子印鑑の安全性を確保するための一方式を提案した[14]。今後も、改良を加えるとともに、実用化を進めていく予定である。

また、（4）は東大の今井秀樹教授が名づけたヒューマンクリプトといわれる分野の研究である。完全な問題の解決は難しいが、少なくとも、意識しないで捺印してしまうことのないようにしていく必要がある。また、不正などがあれば自分の持ち物であるＩＣカードがアラームを出すようになっていれば安心して使えるだろう。今後、このヒューマンクリプトの研究を強化していきたいと考えている。

5. おわりに

以上、印鑑と電子印鑑に関し、それぞれの歴史と利用形態、機能、不正使用方法などの類似性と相違点を明確化すると共に、類似性の分析結果から電子印鑑をさらに使いやすく、安全なものにするための提案を行った。

最後に、情報の提供をいただいた東京大学の今井秀樹教授、横浜国立大学の松本勉助教授、日立の宝木和夫博士にあつくお礼を申し上げる。特に、松本助教授には、多数の貴重なご指摘を頂き、本文の中にも一部反映させていただいた。

なお、本稿は急遽、まとめたものであるので不十分な点が多い。既にいただいたご指摘や、今後、明確になっていく事項に基づきさらに良いものにしていきたいと思っている。本稿の過ちのご指摘や、関連する情報（例えばこの時点でこんなものを開発していたなど）の提供をいただければ幸いである。

6. 参考文献

1）新関欽哉「ハンコロジー事始め　印章が語る世界史」日本放送出版協会、１９９１
2）新関欽哉「ハンコの文化史」ＰＨＰ研究所、１９８７
3）門田誠一「はんこと日本人」大巧社、１９９７
4）ドミニク・コロン（池田潤訳）「オリエントの印章」学芸書林、１９９８
5）石川九楊「二重言語国家・日本」日本放送出版協会、１９９９
6）W. Diffie, M. Hellman " New Direction in Cryptography ", IEEE, Transaction Information Theory, Vol. IT – 22, No. 6, November, pp. 644- 654, 1976
7）R. L. Rivest, A. Shamir, L. Adleman " A Method of Obtaining Digital Signature and Public Key Cryptosystems ", Comm. Of ACM, Vol. 21, No.2, pp120-126 (1978)
8）宝木和夫、白石高義、佐々木良一「ＩＣカード利用電子取引用認証方式」電気学会論文誌Ｃ分冊、107 巻 1 号、pp46-53、1987 年 1 月号
9）D. Chaum " Blind Signatures for Untraceable Payments ", Advances in Cryptology – Proceedings of CRYPTO'82, pp. 192-203, Prenum Press, 1983
１０）　信森毅博、「認証と電子署名に関する法的問題」、日本銀行金融研究所 discussion Paper No.98-J-6
１１）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」日本銀行金融研究所　金融研究 2000 年 4 月、第１９巻、別冊第１号、ｐｐ５５－１０４
１２）松本勉、岩下直行、「金融業務と認証技術：　インターネット金融取引きの安全性に関する一考察」、日本銀行金融研究所 金融研究 2000 年 4 月、第１９巻、別冊第１号、ｐｐ１－１４
１３）佐々木良一他、「インターネットセキュリティ 基礎と対策技術」オーム社、１９９６
１４）松本勉、岩村充、佐々木良一、松木武、「暗号ブレーク対応電子署名アリバイ実現機構（その１）　― コンセプトと概要 ― 」、情報処理学会コンピュータセキュリティ研究会、８―３、ｐｐ１３―１７、 2000 年 3 月 21 日
１５）松本勉氏よりの私信