印鑑と電子印鑑の歴史と類似性の分析

佐々木 良一[†] 宝木 和夫[††]

インターネットの普及にともな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，それぞれの歴史と基本機能，登録と証明方法，不正使用方法などを調査し，（2）そのうえで，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などが重要な課題であることなどを明らかにすることができた．

Analysis on History and Similarity of Seal and Electronic Seal

Ryoichi Sasaki[†] and Kazuo Takaragi[††]

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, registration authority, certification authority, 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.

1. はじめに

インターネットの普及にともない，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印鑑と同じような機能を持つ電子印鑑（電子捺印ともいう．米国ではデジタル署名 Digital 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 つといってよいだろう．

電子印鑑は広く用いられ始めたが，今後さらに普及し，社会の大切な基盤となることが予想される．したがって，これをさらに使いやすく安全なものにするために，各方面から分析を行い，その対策を検討することが必要となる．本論文では，印鑑と電子印鑑に関し，それぞれの歴史，基本機能，登録と証明方法，不正使用方法などを明確化するとともに，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方式と研究課題の提案を行う[1),2)]．

† 東京電機大学工学部
School of Engineering, Tokyo Denki University
†† 日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.

2. 印鑑と電子印鑑の歴史

2.1 印鑑と署名の歴史[3)~6)]

印鑑（印章やハンコともいう）は**表 1** に示すように今から 5300 年ほど前にシュメールの祭司や役人が初めて使用したといわれている[3)]．一方，文字は今から約 5100 年前，同じくシュメール人が発案した古拙文字が世界で最初のものであり，その後，楔形文字に発展していったといわれているから，文字のない時代に印鑑が使われていたことになる．文字のない時代に印鑑は，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の防止に使われたようである．

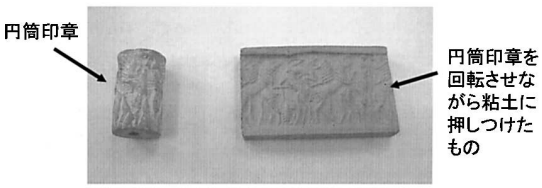
（1）粘土でできた小さな物体であり，品物の種類を示す「数え駒」（トークン）を品物の数だけ用意し，全体を粘土で丸く包んだものの上に捺印し，それを品物と一緒に相手に送ったり，貯蔵したりしたといわれる．

（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いわれる．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，大理石などででき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，文字が現れ，粘土板などの上に文

表 1 印鑑と電子印鑑の歴史
Table 1 History of Seal and Electronic Seal.

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(5300年前) △印章から署名へ (△シュメール人が古拙文字使用) △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での利用 △Rivestら具体的方式を提案(1978年)
	日本の出来事	△双方向捺印実験 △グループウエアで利用



メソポタミアの印章(紀元前約2600年)
(レプリカ:佐々木良一所蔵)

図 1 円筒印章の一例
Fig. 1 Sample of Cylinder Seals.

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った．

中国での印章の使用は，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）のものだといわれている．一方，紙は紀元 105 年に中国の蔡倫が発明したといわれており，5 世紀には紙が広く使われるようになってきた．これにともない，6 世紀初頭になって，朱泥を使い紙に直接的にハンコを捺す現在のような方式になってきたという．

日本における印章は，金印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る．私印が広く用いられ始めたのは戦国時代であり，武田信玄や上杉謙信などの戦国武将が私印として印鑑を好んで用いた．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という[4]．

なお，ヨーロッパでは 15 世紀ごろから印鑑の代わりに署名が用いられるようになる．これは,(1) 教育の普及により読み書きので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．19 世紀にはいるとヨーロッパでは印鑑はほとんど用いられなくなっていった．

2.2 電子印鑑の歴史[1),2)]

電子商取引においてトラブルを防止するためには，取引者の双方が，取引内容を承知し，改ざんも行われていないことを証明できなければならない．この解決策として出現したのが公開鍵暗号技術を利用する電子印鑑技術である．これらの具体的実現手段はすでにいろいろな本（たとえば文献 7) の p.195–p.196）に記述されているのでここでは省略する．

公開鍵暗号の概念が 1976 年に Diffie と Hellman によって，IEEE Transaction on Information Theory の招待論文[12)]として発表され，同じ論文の中で電子印鑑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，概念的検討にとどまっている．その後，1978 年（特許としては 1977 年に出願）に Merkle と Hellman によって開発された具体的公開鍵暗号である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[13)]．論文の表題からもデジタル署名（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．

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用いられている．また，電子印鑑専用の方式である DSA や ESIGN なども開発された．

いろいろな印鑑（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．たとえば，多重署名や電子仮署名[17)]，しきい値署名，ブラインド署名，否認不可署名などがある．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署名[11)]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．

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ようになったのは，Zimmermann がデジタル署名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．

なお，公開鍵暗号については，イギリスの CESG（British Communications-Electronics Security Group）や米国の NSA（National Security Agency）などの諜報機関において，1976 年以前に発明されていたという説もある[14),15)]．すなわち，イギリスにおいては 1970 年に James Ellis が，“Non-Secret Encryp-

tion” という名で公開鍵暗号に相当する概念を考案し，1973 年には Clifford Cocks が，RSA と類似の方式を考え付いたとしている[14]．また，NSA（National Security Agency）の Bobby Inman は，Diffie と Hellman の発明の 10 年前に NSA は公開鍵暗号を持っていたと主張している[15]．しかし，これらはいずれも公開鍵暗号を暗号化に用いるためのものであり，電子印鑑の技術を提案するものではない．したがって，電子印鑑の発明の栄誉は引き続き，主に，Diffie と Hellman に帰すべきであろう．

日本においては，Diffie と Hellman によって公開鍵暗号や電子印鑑に関する発表があった直後から，調査，研究が開始されていたようであり，1980 年に出版された一松信の「暗号の数理」という入門書[24]にはすでに公開鍵暗号の解説がなされている．

電子印鑑システムが最初にいつごろ実用化されたかは不明である．日立の宝木，白石，佐々木は，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[17]．そこでは，RSA 処理の高速化のために，ハードウエアと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 1 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）．

3. 印鑑と電子印鑑の登録と証明[2]

3.1 印鑑の登録と証明

印鑑の登録と証明ならびに無効化については，今から 3700 年ほど前のハムラビ王治下のバビロニアですでに行われていたという．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[3]．

日本においても印鑑登録や印鑑証明は戦前から行われていたようであるが，具体的にいつから始まったかは筆者には不明である．現在の日本では，印鑑登録や印鑑証明（より正確には印鑑登録証明）は，以下のように行われている．

（1）個人用印鑑
（a）登録先：市役所や町村役場
（b）背景となる法律：法律はなし．条例などで対応．
（2）法人用印鑑
（a）登録先：登記所（法務省）
（b）背景となる法律：商業登記法

このうち，個人用印鑑に関する印鑑登録は通常，以下に示すようにして行われている[25]．

（1） 申請者は，住所，氏名，年齢などを書いた申請書と，印鑑と，免許証など写真つきの証明書を用意し，市役所などに提出する．
（2） 市役所では，本人性を免許書などによって確認し，住所，氏名，年齢などを住民基本台帳に照合することで実在性を確認する．
（3） そのうえで，印影を登録するとともに申請者に印鑑登録証（印鑑登録カードというところもある）を発行する．

このようにして登録した印鑑の証明書は以下のようにして入手し，利用することができる．

（4） 登録したのと同じ役所に行き，登録時に得た印鑑登録証を示し，印影つきの印鑑登録証明書を入手する．
（5） 登録したのと同じ印鑑を契約書などに捺印し，上記の印鑑登録証明書を，それに添付する．これにより，契約書などに捺された印影が登録したものと同じであることが人間の目によって確認できる．

なお，印鑑をなくしたり，本人が死亡したりした場合に，届出によって印鑑登録を停止する仕組みになっている．

3.2 電子印鑑の登録と証明

電子の世界の印鑑や署名に対し，このような印鑑登録と印鑑登録証明を行う機構を認証機関（あるいは，認証局．英語では Certification Authority 略して CA）という．すなわち，C さんの作った公開鍵 Pc を A さんの公開鍵 Pa であるというのを防ぐためのものである．認証機関の機能については 1978 年には MIT などですでに研究が行われてきたようである[16]．実際に広く使われ始めたのは商用インターネットが普及した 1990 年代中盤からでないかと思う．日本で認証機関のサービスが開始されたのは 1996 年からで，日本ベリサイン（株）によるものが最初であろう．

なお，デジタル署名（電子印鑑）に用いている公開鍵を認証機関が認証する場合は文字どおり印鑑登録，印鑑証明の機能になるが，認証機関は，メールなどの暗号のための鍵交換用公開鍵暗号の鍵の認証にも用いられる場合がある．したがって，認証機関の機能はより正確には，公開鍵の持ち主を認証することにあるといえる．

認証機関の処理の概要は以下に示すとおりである[10]（**図 2** 参照）．

（1） 申請者 A さんは公開鍵と秘密鍵の対を生成
（2） 公開鍵証明書の申請者が公開鍵と必要な情報を認証機関に提出
（3） 認証機関が公開鍵証明書に記述する内容の正当

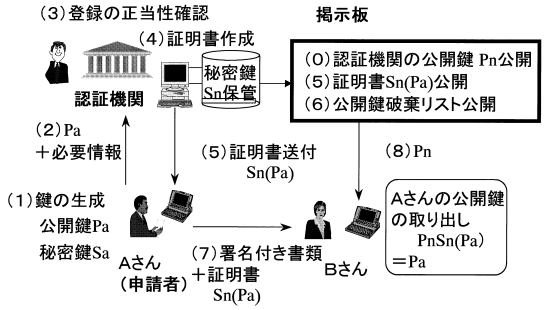


図 2 認証機関の目的と機能
Fig. 2 Objectives and function of Certification Authority.

性を確認

(4) 認証機関が公開鍵証明書を作成し，自らの秘密鍵によって署名

(5) 公開鍵証明書を申請者に送付するとともに，第三者もアクセス可能な場所に保管

(6) 必要に応じて公開鍵証明書の破棄（無効化）を行い，公開鍵破棄リスト（CRL：Certificate Revocation List）の形で破棄した公開鍵証明書を周知

(7) 申請者 A さんはデジタル署名付きの取引文書と上記の証明書を取引相手の B さんに送付

(8) B さんは，認証機関の公開鍵 Pn を入手し，証明書に含まれている A さんの公開鍵 Pa を取り出したうえで，本物の A さんが取引文書に記述された内容に同意していることを確認

なお，(1) に関しては，公開鍵と秘密鍵の対を利用者側のパソコンや IC カードで生成する方式が一般的であるが，ドイツでは認証機関で生成し，秘密鍵を IC カードなどに入れて利用者に渡す方式も採用されている．(6) において，公開鍵証明書の破棄（無効化）は，秘密鍵を申請者が紛失したような場合に実施される．

また，認証機関で公開鍵証明書に書いた内容の正当性を確認すると書いたが，認証機関の機能から登録対応の事務と正当性の確認の部分を取り出し，登録機関（RA：Registration Authority）という別の組織として扱う場合もある．認証機関を認証する認証機関を階層的に設置する場合もあり，最上位の認証機関をルート CA と呼ぶ．

4. 印鑑と電子印鑑の比較

4.1 基本機能と歴史に関する比較

紙の世界では取引において証拠性を保つため，**図 3** 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文書を書き，(2) 双方が印鑑を捺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ともに，(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，米国やヨーロッパ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呼び，(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．

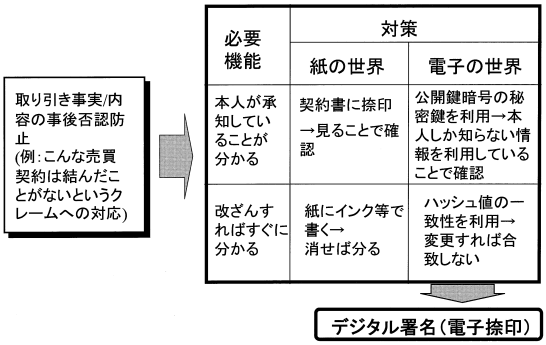


図 3 印鑑と電子印鑑の比較
Fig. 3 Comparisons of Seal and Electronic Seal.

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できる．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だからである．このような問題を解決するのが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を用いることにより，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．

印鑑と電子印鑑の歴史を比較すると前者が，5000 年以上の歴史を持つのに対し，後者はたかだか 30 年である．印鑑については，シュメール人が印鑑を使い始めてから日本人が使うまでに約 4000 年の歳月が経っているのに対し，電子印鑑の場合は，米国と日本ではほとんど差がない形（数年以内）で，研究や実用化がなされている．

4.2 電子印鑑の長所と欠点

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[23]：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[22]：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[22]：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，取引文書が読めれば，どんな取引かが分かり，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，本人の意思どおりに動いているかどうか確認するのが困難である[20]．

いずれも大切な研究テーマである．特に (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[21]．今後も，いろいろな方式の研究が大切になっているだろう．

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はますます重要になっていくと考えられる．

4.3 登録と証明に関する比較

印鑑の登録と証明ならびに無効化については，先にも述べたように今から 3700 年ほど前のハムラビ王治下のバビロニアですでに行われていたという．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．電子の世界の認証機関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．したがって，両方の機能ならびに方式はよく似ているといえる．しかし，厳密に検討すると以下に示すような違いがある．

(1) 印鑑の場合は，登録されているものと同じかどうかは，目で見ることで確認するのに対し，電子印鑑の場合は公開鍵暗号を用いパソコンの中で実施される．したがって，電子印鑑の場合は，チェック結果が実感の乏しいものになるという短所はある．ただし，きちんと運用さえしておけば，偽造などは印鑑の場合に比べ非常に難しいと考えられる．

(2) 電子印鑑に対する認証の安全性は，認証機関の秘密鍵の秘匿性に依存する．したがって，安全性を確保し，しかも何らかの理由により鍵情報が消失しても復元できる技術が大切になる．このため，閾値秘密分散法などの技術が研究されている[10]．

(3) 印鑑の場合には登録と証明を官庁が行うため，認証機関そのものをどこが認証するかということはあまり問題にならなかった．法体系や官僚機構の階層構造によって抽象的に作られていると見ることも可能であろう．一方，電子印鑑の認証の場合は民間も認証サービスを行っていることもありこれが問題になり，認証機関の認証のチェーンをどう構築するかが課題になる．通常は階層的な構造をとり，最上位にルート CA をもつことになる場合が多い．これにともない，別のルート CA 傘下の認証機関が発行した証明書を貰った場合に，どうやって簡単に正しい電子印鑑かを証明するために仕組みが必要になる．特に，国際間でこれを行うための仕組みの開発が重要になってくる．

4.4 不正に関する比較[1)]

印鑑に関する不正は印鑑の偽造と取引文書の偽造が考えられ，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) 他人になりすまして，偽の実印を登録する：本人にな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，取引文書の偽造は以下のようにすることにより可能である．

(3) 実際に朱肉を使い捺した印影を，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，印を捺させ，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[20)],(b) 重い処罰を設けることにより不正の発生を抑止したりしてきた．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，所領のないものは流罪，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うえ獄門，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いわれている[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は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．耐タンパー対策がますます重要になってくる．

(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，他人になりすますことにより可能である．認証機関における登録方法を安全で効率的なものにする努力が望まれる．

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

(4′) 電子印鑑についてはこれも直接的に対応する不正はない：ただし，ブラインド署名においては，印鑑と同様にだまして意図するものと異なる内容について印を捺させる（署名させる）という攻撃が考えられる．これらに対してはカットアンドチューズ法などの対策方式が提案されている．

このように，印鑑に関する不正方法を明確化し，電子印鑑への不正が考えられないかという検討をすることにより電子印鑑をさらに安全なものにしていくことができると考えられる．

5. おわりに

以上，印鑑と電子印鑑に関し，それぞれの歴史と基本機能，登録と証明の方法，不正使用方法などの類似性と相違点を明確化した．その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方式の提案や，そのために大切となる研究項目の提案を行った．

電子印鑑の歴史の部分については，発表されていないことや，調べきれていないことも多いと思う．関係者からの情報によってさらに充実したものにしていきたいと思っている．

謝辞 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教授，岩手県立大学の山根信二氏にあつくお礼を申し上げる．特に，松本教授には，多数の貴重なご指摘をいただき，本文の中にも一部反映させていただいた．

参考文献

1) 佐々木良一：印鑑と電子印鑑　歴史と類似性の分析，情報処理学会コンピュータセキュリティ研究会，CSEC11-11 (2000).
2) 佐々木良一：印鑑と電子印鑑（その 2） 登録と証明の機能と制度の分析，情報処理学会コンピュータセキュリティ研究会シンポジウム CSS2000 (2000).
3) 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).
4) 門田誠一：はんこと日本人，大巧社 (1997).
5) ドミニク・コロン（著），池田　潤（訳）：オリエントの印章，学芸書林 (1998).
6) H・ウーリッヒ（著），戸叶勝也（訳）：シュメール人類最古の文明の源流を辿る，三修社 (1998).
7) 佐々木良一ほか：インターネットセキュリティ入門，岩波新書 (1999).

8) 櫻井三子：PKI，情報セキュリティ，山口　英，鈴木裕信（編），共立出版 (2000).
9) Adams, C. and Lloyd, S.: *Understanding Public-Key Infrastructure Concepts, Standards and Deployment Considerations*, Macmillan Technical Publishing (1999).
10) ジュリスト「電子取引特集号」No.1183 (2000).
11) Chaum, D.: Blind Signatures for Untraceable Payments, *Advances in Cryptology, Proc. CRYPTO'82*, pp.192–203, Prenum Press (1983).
12) Diffie, W. and Hellman, M.: New Direction in Cryptography, *IEEE, Trans. Inf. Theory*, Vol.IT-22, No.6, pp.644–654 (1976).
13) Rivest, R.L., Shamir, A. and Adleman, L.: A Method of Obtaining Digital Signature and Public Key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
14) http://www.cesg.gov.uk/about/nsecret/home.htm
15) http://www.research.att.com/~smb/nsam-160/index.html
16) Kohnfelder, L.M.: Toward a Practical Public-Key Crypotsystem, B.Sc. Thesis, Department of Electrical Engineering, MIT (1978).
17) 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，Vol.107, No.1, pp.46–53 (1987).
18) 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 (1998).
19) 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，Vol.19, 別冊 No.1, pp.55–104 (2000).
20) 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，Vol.19, 別冊 No.1, pp.1–14 (2000).
21) 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, pp.13–17 (2000).
22) 佐々木良一ほか：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).
23) 松本勉氏よりの私信
24) 一松　信：暗号の数理，講談社 (1980).
25) 電子商取引実証推進協議会認証・公証 WG：認証のレベルと本人確認方式に関する提言 (2000).

(平成 12 年 11 月 29 日受付)
(平成 13 年 3 月 9 日採録)

佐々木良一（正会員）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て平成 13 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．昭和 58 年電気学会論文賞受賞．平成 10 年電気学会著作賞受賞．著書に，「インターネットセキュリティ入門」（岩波新書，1999），「インターネットコマース新動向と技術」（共編著，共立出版，2000）等．IEEE，電子情報通信学会，電気学会等の会員．情報処理学会コンピュータセキュリティ研究会主査．

宝木　和夫

1977 年東京工業大学大学院修士課程制御専攻修了，同年日立製作所入社，システム開発研究所セキュリティシステム研究部所属．現在，暗号と情報セキュリティ技術の研究に従事．同研究部部長．工学博士．IEEE，電子情報通信学会，電気学会各会員．