社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(11)
2003／7／17

紙文書を伴うヒステリシス署名システムの提案と評価

篠田 光秋† 上田 祐輔† 佐々木 良一†

†東京電機大学 〒101-8457 東京都千代田区神田 2-2
E-mail: †shinoda@isl.dendai.ac.jp

あらまし 電子商取引や電子政府の進展に伴い，デジタル署名文書を長期的に利用・保管する必要性が高まっており，長期的にデジタル署名の証拠性を保つ事ができる署名技術の一つとしてヒステリシス署名が考案されている．しかし，特定の第三者機関を利用するシステムに関しては検討されているが，第三者機関を利用しないヒステリシス署名システムに関しては，具体的に検討されていない．そこで，本稿では，既に現代社会の業務の一環として成り立っている紙文書によるやり取りをシステムに取り込み，特定の第三者機関を利用しないヒステリシス署名システムの提案と評価を行う．
キーワード ヒステリシス署名，署名履歴交差，署名履歴，信頼ポイント，紙文書

Proposal and evaluation of hysteresis signature system with paper document

Mitsuaki Shinoda† Yusuke Ueda† Ryoichi Sasak†

†Tokyo Denki University 2-2 Kanda Nishiki-Cho Chiyoda-Ku Tokyo, 101-8457 Japan
E-mail: †shinoda@isl.dendai.ac.jp

Abstract Progress of electronic commerce or the electronic government have lead, the necessity of using and keeping a digital signature document in the long run is increasing. The hysteresis signature has been devised as one of the signature technology which can keep the proof nature of a digital signature long-term. However, although the system using a specific third party is examined, the hysteresis signature system which does not use a third party is not examined concretely. Then, in this report, the exchange by the paper document already realized as part of the business of modern society is taken in to a system, and the proposal and evaluation of a hysteresis signature system which do not use a specific third party are performed.
Keyword Hysteresis Signature，Signature history intersection，Signature history，Trust Point，Paper document

1. はじめに

電子商取引や電子政府等の進展に伴い，電子署名技術の利用範囲が拡大してきている一方で，電子署名付き文書を長期的に利用・保管する必要性が高まっている．しかし，電子署名付き文書を長期的に運用する際に，秘密鍵の漏洩や推定等の脅威により，電子署名を利用したシステムの安全性が損なわれる可能性がある．

この様な問題の対策技術として，長期的に電子署名付き文書の証拠性を残すことが出来るヒステリシス署名が提案された．

しかしながら，特定の第三者機関を利用するシステムに関しては従来検討されているが，特定の第三者機関を利用しないヒステリシス署名システムに関しては，具体的に検討されていない．

そこで，本稿では，既に現代社会の業務の一環として成り立っている紙文書によるやり取りをヒステリシス署名システムに取り込み，特定の第三者機関を利用しないヒステリシス署名システムの提案及び実装，そ

して他のシステムとの比較評価を行う．

2. ヒステリシス署名システム[1]~[4]

2.1. ヒステリシス署名とは

ヒステリシス署名は，電子文書の長期運用の際に問題となる署名生成鍵の漏洩や推定による被害を最小限にするための対策技術の一つである．

この署名技術は，通常の電子署名方式を構成要素の一部として利用するものであり，署名生成する度に署名情報等を署名記録として署名履歴に残す．署名をする際には直前に履歴に残された署名記録を新たな署名情報の一部として取り込んでいくことにより，署名記録間に連鎖構造を持たせる署名技術である．署名履歴を IC カード等の耐タンパ性を有するモジュールに一貫性を保った状態で安全に保管しておく事で，過去に生成されたとされる署名を秘密鍵の漏洩等により偽造された場合でも，履歴の整合性を確認する事で署名の偽造を検知できる．（図 1 参照）

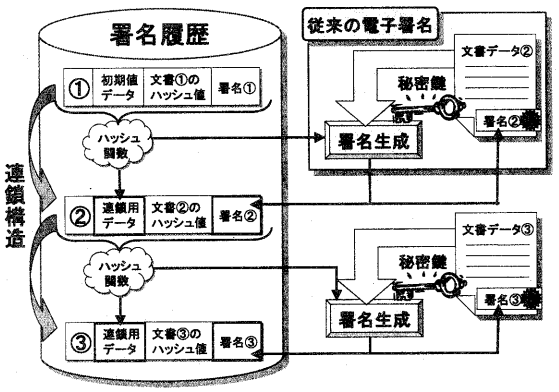

図 1. ヒステリシス署名

検証は，公開鍵による通常の署名検証以外に，履歴検証として，署名履歴中の署名記録の連鎖性を検証すると共に，署名記録とそれに対応する署名との検証も行う事が出来る．よって，例え不正者がある文書の内容や署名を偽造しようとしても，署名間で連鎖構造をなしている為，１つの文書や署名の偽造だけでなく，連鎖をなす全ての署名記録が署名履歴中で一貫性を保つように偽造する必要がある．

以上の事から，ヒステリシス署名では，署名の偽造は困難であると考えられている．

2.2. 署名履歴交差

署名履歴交差とは，署名履歴中のある署名記録を他人の署名履歴中の署名記録に取り込むことにより，自分の署名履歴と他人の署名履歴との間にも署名履歴の連鎖性を築くものである．これにより不正者が署名を偽造する際に，署名者の署名履歴のみならず，他人の署名履歴の改竄も必要となるため，偽造はより一層困難となる．（図 2 参照）

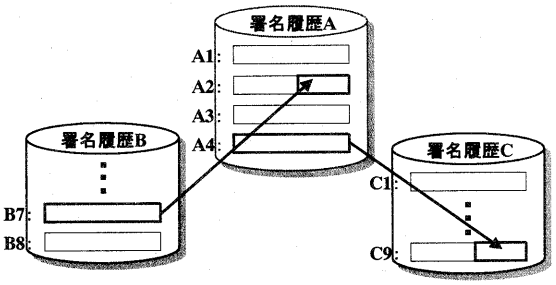

図 2. 署名履歴交差

2.3. 信頼ポイント

信頼ポイントとは，署名生成記録に対応するヒステリシス署名付き文書が，当該利用者により確かに生成された事が保障された署名記録の事である．

信頼ポイントを定期的に作成する事で，欠落あるいは改竄された署名記録以前の署名記録の真偽も検証可能となると共に，不正な署名記録を限定化する事ができる．（図 3 参照）

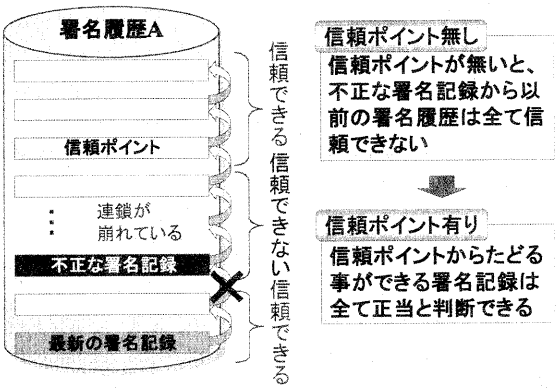

図 3. 信頼ポイント

このような信頼ポイントを作成し,利用する為には，定期的に第三者機関に貯託・公開する方法が考えられる．第三者機関としては以下のようなものが挙げられる．

- インターネット上のデータベースセンタ
- 新聞等のメディア

また，システムを利用するユーザ同士が信頼でき，結託などの問題が無いと場合は，署名履歴交差も信頼ポイントを作成する為の有効な方法の１つとされている．

以上のような技術を基盤として，ヒステリシス署名システムは成り立っている．

3. 従来のシステム

従来，検討されているヒステリシス署名システムは基本的に第2節で述べた技術から成り立っている．そこで，基本的な技術を省いた各方式が持つ特徴と問題点を以下に記す．

3.1. 従来の方式A（以下，方式Aと呼ぶ）[2]

方式Aでは，ユーザの結託を防ぐ為に，センタを介して署名履歴交差を行っている．具体的には，センタをデータ転送の仲介者としての役割を果たし，センタ内でランダムに選択されたユーザ同士で署名履歴交差を行うものである．

ユーザ間の結託の問題について考慮する必要がない場合には，センタを必要としない．しかし，システムを広い範囲で運用する場合は，結託の問題を考慮せざるを得ないといえる．

3.2. 従来の方式B（以下，方式Bと呼ぶ）[3]

方式Bでは，署名生成時だけでなく，署名検証時にも署名記録として署名履歴に取り込む事により，センタを利用しなくとも,効率的に署名履歴交差を行える．これにより，署名付き文書を受け取った側は，受け取った署名の情報を履歴に残す事ができる為，確かに署名付き文書を受け取った事を証明でき，相手の否認を防ぐ事ができるようになっている．

これにより，正規ユーザは不正ユーザが元々送ってきた署名付き文書を受け取った証拠を履歴に残すことができる為，ユーザ同士の結託による問題を防ぐ事ができると考えられる．

このシステムは，署名履歴交差の際に利用する第三者機関を必要としないが，ユーザや署名履歴を保管するモジュールを完全に信頼する事ができない限り，信頼ポイントを貯託・公開する第三者機関を利用する必要がある．

3.3. 従来システムの問題点

以上の事から，従来のシステムでは共に以下のような操作をする際に第三者機関を利用する必要がある事が分かる．

- 方式A：署名履歴交差及び信頼ポイントの貯託・公開
- 方式B：信頼ポイントの貯託・公開

（図4参照）

このように第三者機関を利用する事で，以下のような問題点が考えられる．

・コスト：

第三者機関を利用した場合，ユーザが負担するコストが必然的に高くなってしまう．

・負荷集中：

第三者機関に障害が起こった場合，システムに及ぼす被害が大きい．

・信頼性：

信頼ポイントを公開した直後であれば，当該利用者により確かに生成された署名記録である事が分かる．しかし，長期的に信頼ポイントを保管するとなると，実際に第三者機関が不正を行わないとしても，ユーザは本当にその信頼ポイントが以前に自分が公開した信頼ポイントと同一のものであるかを覚えているとは限らない．

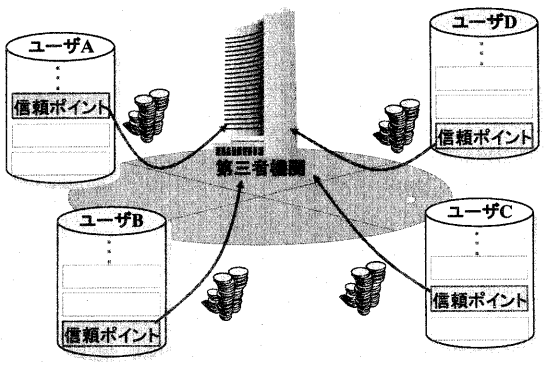

図4. 第三者機関の利用のよる問題点

また，単純に第三者機関を利用せずに，署名履歴交差のみで各ユーザの署名履歴の証拠性を保つような方式にした場合は以下のような問題点が生じると思われる．

- ユーザ同士で信頼ポイントを保管し合う事になる為，各ユーザは相手の信頼ポイントの保管責任を負う事になる．
- 自分の署名記録（信頼ポイント）が他のユーザの署名履歴に含まれている事を証明したくても，他のユーザが信頼ポイントを確実に保管し，それを証明してくれるとは限らない．

そこで本稿では，これらの問題点を考慮して，第三者機関を利用しないヒステリシス署名システムの考案と検討を行った．

4. 提案システム

4.1. システムの概要

本システムは，ヒステリシス署名を行い，署名記録を履歴に残していく中で，システムのユーザ間でやり

取りされる署名付き文書データとそれに対応する署名記録を定期的あるいは任意で紙出力し，出力された紙を正式書類として扱う事で，署名履歴データの信頼性を保っていくというものである．

本システムでは，以下のような理由からシステムに紙文書を介入させた．

(1) ディジタルデータよりも信頼性が高い．
(2) 紙文書に不正があった場合，分かりやすい．
(3) 既に業務の一環となっている為，安心感がある．
(4) 紙文書とディジタルデータが対応していれば，ディジタルデータの改竄は無意味となる．
(5) トラブルから裁判沙汰になった際には，紙文書の方が扱いやすい．

通常はディジタルデータのみによるやり取りを行う．そして，署名記録の保証を受けたい場合（信頼ポイントを得たい場合），もしくは，署名付き文書データを紙の正式書類として欲しい場合は追加処理を加え以下のようにやり取りを行う．

【署名生成者】

通常処理：

①「文書データに署名を行うと同時に署名履歴に署名記録を保存」

⇒例えば，借用書や納品書・領収書・請求書などの電子文書にICカードを用いて署名をする．ICカードの中身は最新の署名記録が常に保存してある状態にある．ICカードの機能としては，アクセス制御機能，署名生成機能，鍵ペア生成機能などがある．

次にICカードに保存してあった署名記録をはき出して署名履歴に追加し，ICカードの署名記録領域に署名後の最新の署名記録に更新する．署名履歴は署名を行うたびに容量が増えていくのでハードディスクなどに保存しておくようにする．

②「文書データと署名データを検証者に送信」

⇒署名付き文書を公開鍵証明書とともに取引相手（検証者）に送信する．

追加処理（定期的もしくは任意で行う）：

③「文書データ，署名データに加えリクエストを検証者に送信」

⇒取引データを正式な書類として欲しい場合，もしくは信頼ポイントの証明が欲しい場合に，署名履歴の保証として電子文書を紙文書として署名者宛に送付してもらう事を要求する．

【署名検証者】

通常処理：

①「署名データの正当性を検証」

⇒検証者は送信されてきた署名付き文書を署名者の公開鍵証明書から公開鍵を取り出して検証を行う．

②「相手の署名記録データを作り，それに署名する事で相手情報を署名履歴に保存」

⇒検証がOKならば署名者の署名記録に対してICカードを用いてヒステリシス署名を行う．

追加処理（リクエストがあった時に行う）：

③「紙文書の出力」

⇒紙出力用プログラムを用いて文書データとそれに対応する署名記録データを結合し，そのデータを紙へ出力（但し，結合されるデータは互いに対応していなければ結合できないようになっている）．

④「紙文書を署名生成者に送付」

⇒紙出力後,実印又はサイン等を書類に付加した後に，署名生成者に送付し，受け取った署名者は送付された紙文書の内容と署名記録を電子文書から目視による比較で確認する．

また，契約書等であれば実印やサインが必要と思われるが，領収書や納品書等であれば，企業などが領収書等に使用する固有の書類に出力する事も一つの方法である．

システムの流れは下図のようになっている．

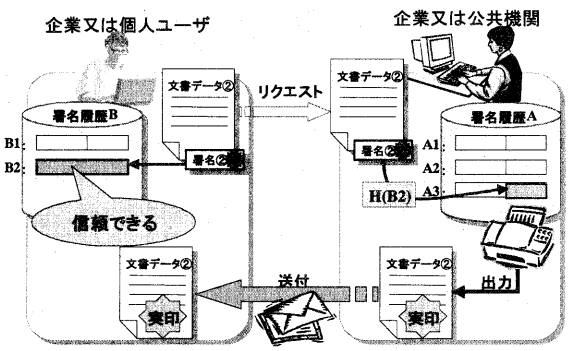

図6. システムの流れ

4.2. システムの特徴

本システムは，通常のディジタルデータによるやり取りに実世界でもやり取り出来る正式書類の紙出力処理を介入させた事が大きな特徴である．

他のユーザが持つモジュール内や第三者機関に保管してある信頼ポイントを信用できなくなった場合，ある時点の文書データと署名記録が正式書類として存在すれば，その時点以前の連鎖構造をなす署名記録は信用する事ができるといえる．つまり，履歴データ内の署名記録とリンクした正式書類を定期的または任意に得る事で，履歴データの信頼性と証拠性を向上させ

る事ができる．

また，利便性の面においての特徴として，例えば，単なる分散型で履歴データを個人で保管しておく場合において自分の履歴データの信頼性を証明するためには，相手（検証者）の協力が必要になってくる．つまり，履歴交差をしてもらった相手から，自分の署名記録をもらう必要がでてくる．このような行為を行う上で問題となることは検証者が協力しないことである．これは，信頼のおけない相手との取引などで起こることが考えられ，このようになると，履歴データを証明することは難しくなり，信頼性が低くなる．

このような事態を解決するために，紙文書をシステムに介入させたことは，大きな利点といえる．たとえ相手が信頼のおける者でなくとも，紙文書として正式な書類を貰っておけば，自分自身で履歴データを証明することができるため，利便性の面を考えると非常に高いといえる．

5. システムの実装

5.1. IC カードの利用方式の検討

本システムでは，署名を生成する時に，耐タンパ性を有する IC カードを利用して行うことを前提条件としている．従って IC カード内のデータの改竄は，第三者をはじめ，署名者自身もできないようになっている．

しかし，長期に渡り，IC カードを利用していくと IC カードが何らかの原因で故障するなどして，読み込めなくなる危険性がある．この対策として，本システムでは，IC カード内に最新の署名記録のみを保存していく方式を取っている．これは，IC カードの中に署名記録を溜めていく方式を取ると，保管しきれない容量になった時にハードディスクなどに掃き出す必要がある．このような方式を取った場合，IC カードの故障による被害は大きなものとなってしまう．

そこで，本システムでは，毎回署名記録の掃き出しを行い，IC カード内の最新の署名記録を更新させる事により，被害を最小限に抑えるようにした．（図 8 参照）

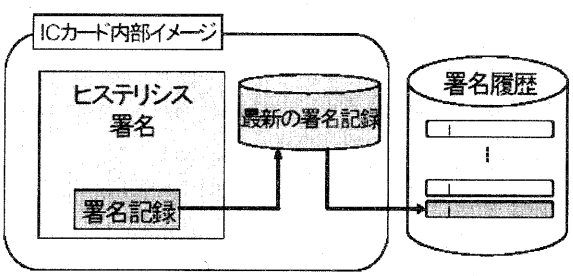

図 8.IC カードの利用

5.2. プロトシステム

本システムのプロトタイプを Visual C++ 6.0 により実装した．

実装したプロトシステムの暗号化機能には，Microsoft CryptoAPI を利用した．

署名履歴への登録等はあるが，通常の電子署名方式を構成要素の一部として利用している為，署名の際の処理時間に関しては，単純な RSA 署名等とほぼ変わらない結果となった．但し，紙出力を行う場合は，印刷時間が掛かるが，以下のような紙文書を出力するだけなので，企業等で業務の一環として行うのであれば，問題は無いと思われる．

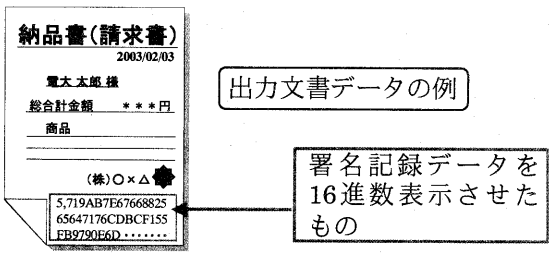

図 9. 出力文書

今回，紙文書と共に出力される署名記録の情報は 16 進数で表示する形をとった．今後は，透かしや 2 次元バーコードにより実現する事を考慮している．

6. 比較評価

本システムとの比較対象として，前述した従来の 2 つの方式に加え，第三者機関も紙文書も伴わず，信頼ポイントのやり取りも完全にユーザ同士で行う方式（以下，方式 C と呼ぶ）を挙げ，比較評価を以下の表に記す．

表 1. 他方式との比較

比較対象 / 比較指標	方式A[2]	方式B[3]	方式C	提案方式
コスト	×	△	○	△
通信量	×	○	○	○
信頼ポイントの信頼性	△	△	×	○
情報の集中によるリスク	△	△	○	○

・コスト：

方式 A と方式 B は，共に第三者機関を利用する為，必然的にユーザはコストを負担する事になる．特に，方式 A は，「履歴交差」と「信頼ポイントの貯託・公開」の 2 つの操作を行う為，最も低い評価となってい

る.

但し，提案方式においては，第三者機関の利用コストは当然かからないが，紙文書の扱いによるコストはかかる.この点に関する詳細な検討が今後必要となる.

・通信量：

方式Aでは，以下のような問題が生じる為，通信量が余計に掛かってしまう.

○履歴交差を行う度に，第三者機関とやり取りする必要がある.

○ランダムに選択されたユーザも第三者機関とやり取りをする必要がある.

・信頼ポイントの信頼性：

方式Aと方式Bでは，長期間に渡り信頼ポイントを貯託・公開した時，ユーザが以前に貯託・公開した信頼ポイントの値を覚えているとは限らない．新聞等に掲載する方式をとれば，問題は無いと思われる．しかし，インターネット上のデータベースサーバ等を利用した場合は，第三者機関が不正を行わないとしても，本当に正しい信頼ポイントの値かどうかは，ユーザには分からないと思われる.

また，方式Cでは，自分の信頼ポイントが他のユーザの署名履歴に含まれている事を証明したくても，他のユーザが「協力したくない」「署名履歴を消失してしまった」というケースが考えられる.

提案方式であれば，信頼ポイントも一緒に印字された書類を自分で保持する事になるので，以上のような問題にも対応できる.

また，紙文書によるやり取りは，従来から慣れ親しんでいる事である為，目に見えないディジタルデータによるやり取りよりも安心感があると考えられる.

・情報の集中によるリスク：

方式Aと方式Bのように，各ユーザの信頼ポイントを第三者機関に貯託・公開する場合，第三者機関に何らかの障害が起こった際のシステム全体に与える被害が大きいものとなってしまう.

7. おわりに

以上，紙文書を伴うヒステリシス署名システムの提案と評価を行った.

あらゆる文書や手続が電子化される一方で，最終的に電子情報を紙に印刷している人は意外に多い.また，書類の証拠性や信頼性は電子データよりも明らかに高く，慣習化・確立化されている為，IT が発達したとしても紙という媒体が人間生活から消滅する事はないといえる.

一方，電子の世界のみでは，署名システムが正しく安全に動作している事を実感し辛いのも現状である.

以上の事を踏まえると，電子の世界と紙の世界との対応関係も今後重要な課題の一つともなり得る.

今後，どの程度の頻度で紙出力するのが最適なのか，コストや安全性，利便性を考慮した上で，検討していく予定である.

また，長期的に電子署名付き文書を運用する際に重要となる「公開鍵証明書の期限切れ」,「署名の効力切れ」,「公開鍵暗号の危殆化」等の問題が起こった時のヒステリシス署名システムにおける具体的な対処法について検討も行っていく予定である.

文　献

[1] 岩村充，宮崎邦彦，松本勉，佐々木良一，松木武“電子署名におけるアリバイ証明問題と経時証明問題－ヒステリシス署名とデジタル古文書の概念－”コンピュータサイエンス誌 bit Vol.32, No.11, 共立出版(2000)

[2] 洲崎誠一，松本勉“電子署名アリバイ実現機構－ヒステリシス署名と履歴交差－”情報処理学会論文誌 Vol.43, No.8, pp.2381-2393 (2002)

[3] 谷本幸一，宮崎邦彦，伊藤信治，吉浦裕“署名履歴交差を利用したヒステリシス署名の実現方法”情報処理学会 CSS2002 (2002)

[4] 宇根正志“デジタル署名生成用秘密鍵の漏洩をめぐる問題とその対策”日本銀行金融研究 Discussion PaperNo.2002-J-32 (2002)