マルチメディア通信と分散処理　97－4
コンピュータセキュリティ　8－4
（2000．3．21）

# 暗号ブレイク対応電子署名アリバイ実現機構（その2）

## ― 詳細方式 ―

洲崎 誠一[†]　宮崎 邦彦[†]　宝木 和夫[†]　松本 勉[††]
[†]（株）日立製作所　システム開発研究所
[††]横浜国立大学　大学院工学研究科人工環境システム学専攻

あらまし
現在広く使われているディジタル署名は，公開鍵暗号技術の計算量的安全性に基づいたものであるため，時間経過にしたがってその安全性が徐々に失われる。そのため，電子債権等のように一定期間経過後に効力をもつような署名付き電子データの場合，当該期間中に秘密鍵が漏洩し，後日，自分が作成した覚えのないものを持ち込まれる恐れがある。このような課題に対し，我々は，公開鍵暗号技術の安全性が保たれなくなった場合においても，ディジタル署名の真偽を確認可能な「ヒステリシス署名」を提案する。本稿では，ヒステリシス署名に基づく暗号ブレイク対応電子署名アリバイ実現機構の一方式を示す。

# Alibi Establishment for Electronic Signatures: How to prove that you did not make the electronic signature in question even when the base cryptosystem was collapsed

## *Part 2. Concrete Schemes and Evaluation*

Seiichi Susaki[†], Kunihiko Miyazaki[†], Kazuo Takaragi[†]
and Tsutomu Matsumoto[††]
[†] Systems Development Laboratory, Hitachi, Ltd.
[††] Division of Artificial Environment and System, Yokohama National University

**Abstract**
Digital signature is relatively getting to lose its security because of computer power improvement. On the other hand, some kind of signatures must have long term of validity (e.g. over 20 years) in practical usage. Thus, we need reliable systems to keep validity of digital signature even if the base cryptosystem is collapsed. In this paper, we propose a "hysteresis signature" based system. In our system, we can distinguish valid signature and forged one with the signature log file which is stored safely by storing it in a smart card, by chaining the signature with previous signature, or moreover by intercrossing the signature with other signers' one.

## 1. はじめに

コンピュータの処理性能の向上などにより，これまで使われてきた暗号の安全性が脅かされ始めてきている。そのため，使用する暗号鍵のビット長を長くしたり，同じ暗号鍵を長期間使いつづけたりせず，定期的に変更するような対策がなされている。

しかし，EC（Electronic Commerce）システムでは，債権や手形のように，ある一定期間が経過した後に換金されるものがある。そのため，もし，換金時点で，債務者が電子債権にディジタル署名を施す際に使用した暗号アルゴリズムが破られていたり，債務者の秘密鍵が漏洩していた（公開鍵等から算出された）場合に，不正者によって偽造された電子債券を持ち込まれる恐れがある。

このような脅威から利用者を保護するためには，電子データに施されたディジタル署名が，当該利用者が生成したものなのか，あるいは不正者によって偽造されたものなのかということを判別できるようにする必要である。

これに対し，従来より，すべての利用者が信頼する第三者機関（TTP: Trusted Third Party）にタイムスタンプを付加してもらったり，副署してもらったりしておくといった方式が提案されている [1][2]。しかし，そのように何らかのTTPを利用する方式の場合，それらTTPの秘密鍵が漏洩するとシステム全体が利用できなくなってしまう恐れがある。また，TTPに負荷が集中し，利用者が必要な時に利用できない恐れもある。

そのようなことから，ディジタル署名を生成した履歴を利用者自身にも偽造困難な形で安全に保管することで，当該利用者が生成したディジタル署名であるか否かを事後になっても確認可能とするヒステリシス署名方式も提案されている[3]。

本稿では，そのようなヒステリシス署名に基づく暗号ブレイク対応電子署名アリバイ実現機構（以降では，署名アリバイ機構と略す）の一方式を提案する。

## 2. 署名アリバイ機構の概要

### 2.1 署名履歴の要件

利用者が生成したディジタル署名であるか否かを事後になっても確認可能とするためには，利用者の署名手段および署名履歴が以下のような要件を満たしていることが必要である。

- 利用者は，署名履歴の中に記載されないような手段で，自己のディジタル署名を正しく生成することができない。
- 利用者が生成したディジタル署名に対するログは，署名履歴の中にすべて記載される。
- 利用者の署名履歴は，利用者自身も含めて誰にも変更することができない。
- 署名履歴に何らかの変更が加えられた場合には，事後になってもその事実が正しく検証できる。

### 2.2 署名用ICカード

前項の要件を満足するためには，耐タンパー性のあるハードウェア装置を，ディジタル署名の生成，および署名履歴の保管に使用することが考えられる。特に，利用者の利便性を考慮すると，様々な場所（自宅，職場，店舗等）において署名生成可能な署名用ICカードが便利である。本稿で提案する署名アリバイ機構で使用する署名用ICカードの機能を以下に示す（図1参照）。

アクセス制御機能

- 利用者の認証
- 認証結果に基づく各種機能やデータに対するアクセス制御

鍵管理機能

- 秘密鍵，公開鍵の生成，保管
- 公開鍵の出力
- 入力された公開鍵証明書の保管

署名機能

- ディジタル署名の生成

署名履歴管理機能

- 署名履歴の更新，保管
- 署名履歴の出力

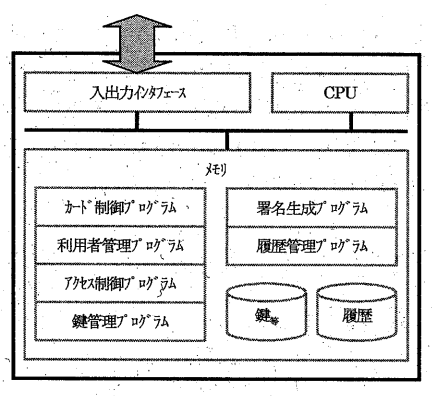


**図 1: 署名用 IC カード**

このように署名用 IC カードにすべての署名履歴が，利用者本人も変更できない状態で格納されていれば，覚えのない署名付き電子データが持ち込まれた場合にも，自己のカードから出力した署名履歴を提示することによって，自分が作成したものではないことを他の利用者に証明することができる。しかし，一般に IC カードの容量は 8Kbyte ～32Kbyte 程度（この中には IC カード自体を制御するためのプログラム等を格納する領域も含まれる）である。したがって，上記要件を満足したまま，署名履歴を署名用 IC カード外部に出力するための手段が必要となる。

## 3. Chaining Signature

### 3.1 方式の概要

署名用 IC カード内に格納された署名履歴は，カードの物理的な安全性によって保護されている。しかし，外部出力された署名履歴は容易に変更することが可能である。そこで，署名アリバイ機構では，個々の署名を連鎖させる Chaining Signature を採用する。

Chaining Signature は，図 2 に示すように，n 回目のディジタル署名生成時に n-1 回目の署名結果データのハッシュ値を作用させる署名方法である（1 回目は初期値 IV）。したがって，ある時点での署名結果データは，当該カードを使用開始してからのすべての署名履歴が影響した値となっている。

なお，通常の署名方式では，署名対象となるメッセージとディジタル署名とを組にして相手（検証者）に送るが，Chaining Signature では，それに加えて一つ前の署名結果のハッシュ値もあわせて送ることが必要となる。

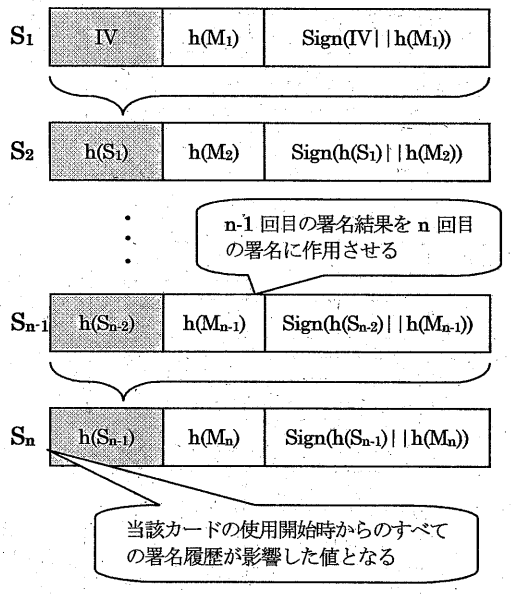


**図 2: Chaining Signature**

### 3.2 Chaining Signature の特徴

Chaining Signature では，最新の署名結果だけを署名履歴として署名用 IC カードの中に保管しておけば，それ以前の署名履歴は IC カード外部（例えば，PC のハードディスク等）に出力する

ことが可能である。なぜなら，図3に示すように，外部出力された署名履歴に何らかの変更が加えられた場合でも，署名用 IC カード内部に残された署名履歴を用いることで，変更が加えられたことをいつでも検知できるからである（本稿では，署名用 IC カード内に残された署名履歴のように，署名履歴全体の正当性を検証する上で，信頼の基となる部分を信頼ポイントと呼ぶ）。

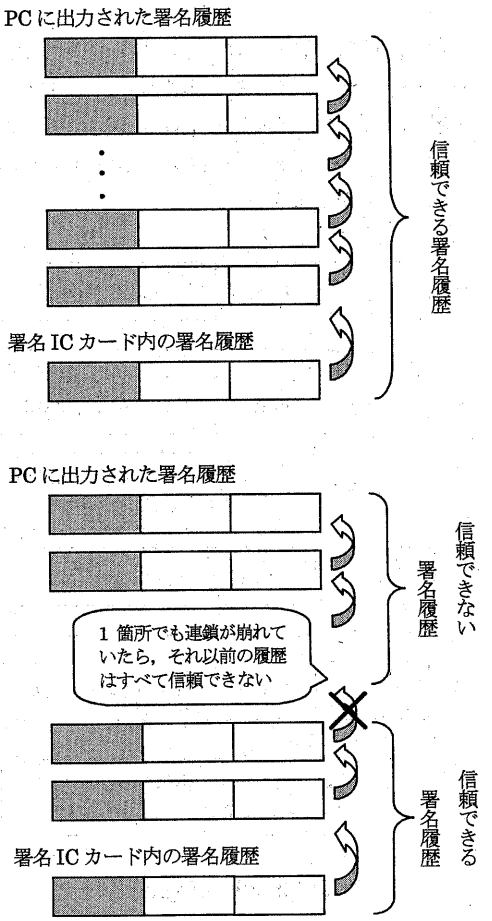


**図 3: 署名履歴の検証**

しかし，外部に出力した署名履歴が破壊されてしまうと，利用者は，覚えのない署名付きメッセージが持ち込まれた場合に，自分が作成したものではないことを他の利用者に証明することができなくなってしまう。そのため，署名履歴を保管するための TTP をいくつか設置し，利用者が定期的に署名履歴を預託するようにすればよい。この TTP は，システムの安全性に影響を及ぼすような秘密情報をもつ必要がなく，また，リアルタイム性も要求されないため，十分現実的だと考える。

### 3.3 調停プロトコル

本節では，ある利用者（署名者）が，別の利用者（持込者）から，覚えのない署名付きメッセージを持ち込まれた場合の調停者による調停作業の手順（調停プロトコル）について説明する。調停プロトコルを図4に示す。

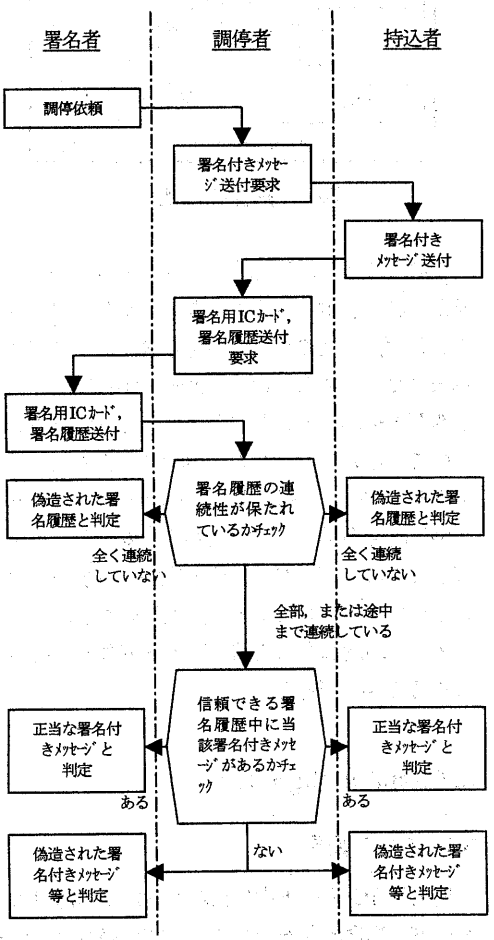


**図 4: 調停プロトコル**

① 持込者より署名付きメッセージを，署名者より署名用 IC カードと署名履歴(カード外に保管されているもの) を提出させる。

② 署名履歴の連続性が保たれているかどうかを確認する。ここで，全く連続性が保たれていなければ，当該署名履歴が偽造されたものだと判断する。

③ 署名履歴の連続性が完全に保たれている場合，その信頼できる署名履歴の中に，当該署名付きメッセージに関するものがあれば，当該署名付きメッセージは正当なものと判断する。また，無ければ，当該署名付きメッセージは偽造されたものと判断する。

④ 一方，署名履歴の連続性が途中まで保たれている場合，信頼できる署名履歴部分に当該署名付きメッセージに関するものあれば，当該署名付きメッセージは正当なものと判断する。また，無い場合には，これだけでは真偽を判定できないため，その他の利用者等から当該署名者が生成した署名付きメッセージを集め，署名履歴を再構築して判断する。

## 4. 信頼ポイント

### 4.1 署名履歴の欠落

署名アリバイ機構では，利用者の署名履歴がきちんと保管されていることを前提としている。しかし，ハードウェアの故障等も含め，何らかの原因により一部の署名結果データが欠落してしまうことも考えられる。図 3 にも示したように，Chaining Signature の場合，欠落した署名結果データより以前に署名されたものは，その真偽を判別することができないという問題がある。

### 4.2 信頼ポイントの追加

#### 4.2.1 基本的な考え方

前節で述べた課題に対し，あらかじめ署名履歴の中に信頼ポイントを適宜追加するようにしておくことで，欠落した署名結果データより以前に署名されたものの真偽も検証可能になるものと考えられる（図 5 参照)。

そのような信頼ポイントを追加するための方法として，利用者同士が相互に補助し合う「履歴交差方式」と，センタが定期的に公開するチャレンジデータを用いた「センタ利用方式」を提案する。

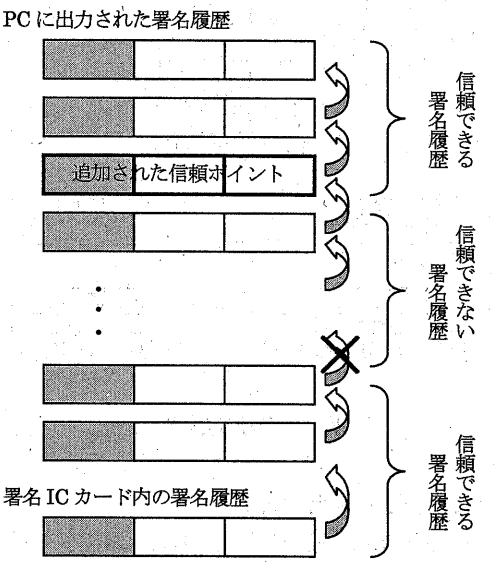


**図 5: 信頼ポイントの追加**

#### 4.2.2 履歴交差方式

履歴交差方式とは，図 6 に示すように，各利用者が Chaining Signature を利用している環境において，利用者間で適宜署名付きメッセージを交換し合い，互いの署名履歴を交差させることによって，署名履歴の信頼性（偽造困難性）を高めるとともに，信頼ポイントを追加する方法である。すなわち，前述の Chaining Signature がそれ以前に自分が行った署名の履歴を継承する方法であるのに対し，履歴交差方式は，自分だけでなく他利用者の署名の履歴をも継承していく方法である。

履歴交差方式を利用する場合は，署名履歴を交差させる利用者同士の結託を防ぐため，TTP が署名付きメッセージを交換し合う相手を振り分けるようにしたほうがよい。

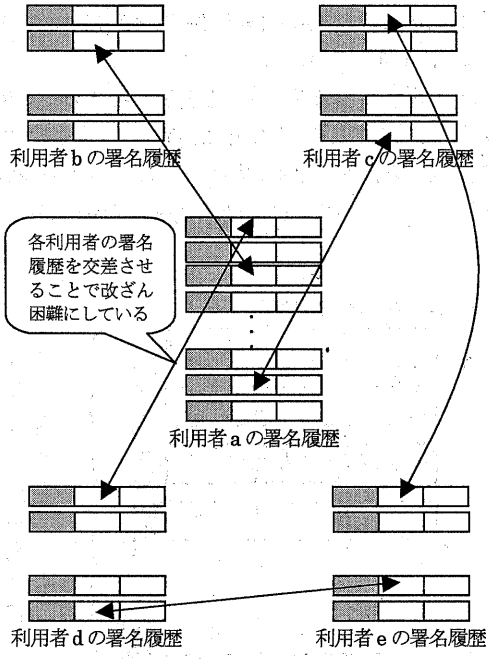


**図 6: 履歴交差方式**

#### 4.2.3 センタ利用方式

センタ利用方式では，以下のような手順によって，利用者の署名履歴の中に信頼ポイントを追加する。

① センタは，チャレンジデータをランダムに生成し，ある決められた期間，すべての利用者に対して公開する。
② 利用者は，センタが公開しているチャレンジデータを取得してディジタル署名を施し，自己の署名履歴に当該チャレンジデータに関する署名結果データを含ませる（これが信頼ポイントとなる）。さらに，その署名付チャレンジデータをセンタに送信する。
③ センタは，利用者から決められた期間内に送信されてきた署名付チャレンジデータだけを安全に保管する。

本センタ利用方式は，また，負荷の少ない簡単な手順で，システム全体の安全性に関わるような秘密情報を TTP が管理することなく，利用者がディジタル署名を施した日時を保証するためのサービス，すなわちタイムスタンプサービスを実現することができる。

## 5. おわりに

本稿では，電子データに施されたディジタル署名が，正規利用者によって生成されたものなのか，あるいは不正者によって偽造されたものなのかということを，署名履歴を用いることによって判別できるようにするヒステリシス署名の概念に基づいた署名アリバイ機構の具体的方式を提案した。また，Chaining Signature や履歴交差方式，センタ利用方式等といった署名履歴の信頼性を高める方法の有用性も示した。署名アリバイ機構は，電子債権等のように，署名付き電子データが一定期間経過した後に何らかの効力をもつような環境において特に有効である。今後は，プロトタイプシステムを開発し，より定量的に評価する。

## 参考文献

[1] C. Adams 他，Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP), IETF PKIX-WG Internet Draft, Jan. 2000
[2] C. Adams 他，Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols，IETF PKIX-WG Internet Draft, Oct. 1999
[3] 松本勉 他，暗号ブレイ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研究発表会，2000 年 3 月