マルチメディア通信と分散処理 97－3
コンピュータセキュリティ 8－3
（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1）

― コンセプトと概要 ―

松本 勉[†] 岩村 充[#] 佐々木 良一[♭] 松木 武[♭]

[†]横浜国立大学 [#]早稲田大学 [♭]日立製作所

あらまし 計算量的仮定に基づく暗号による電子署名方式は，技術環境が変化すれば，十分な安全性をずっと保ち続けられるとは限らないという性質を持つ．よって，本来自分だけが持つはずの暗号的署名生成機能を他のエンティティが持っているという状況が生じえる．このため，自分が署名した覚えのない電子文書が提示されたとしても，自分は署名していないことを調停者に対して証明できること，すなわち「電子署名アリバイ（電子署名の非生成証明）」を実現する機構が求められる．我々は，署名生成者の署名履歴――これには他のエンティティの署名履歴との交差が含まれる場合もある――に依存して署名生成を行うという「ヒステリシス署名」とそれを基礎とする電子署名アリバイ実現機構を提案する．
キーワード：電子署名，アリバイ，暗号ブレイク，ヒステリシス署名，チェイニング署名，履歴交差

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 1. Concepts and Basic Schemes

Tsutomu Matsumoto[†] Mitsuru Iwamura[#] Ryoichi Sasaki[♭] Takeshi Matsuki[♭]

[†]Yokohama National University [#]Waseda University [♭]Hitachi, Ltd.

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 forge 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

ネットワークを介して離れた相手と非対面で取引等を行う場合，守秘性の確保，相手の認証や，データの改ざん防止などのために，暗号化や電子署名などの暗号技術が有用である．ただし，多くの暗号技術の安全性は解読や偽造に要する計算量が莫大だという仮定に基づくため，解読や偽造への理論的解析の進展やコンピュータの処理性能の向上などにより，導入時に想定された安全性が保ち続けられるとは限らない．そのため，使用する暗号鍵をある頻度で更新するとか，暗号鍵のビット長を増やしていくといった対策が必要である．

しかし，このような対策では太刀打ちできない課題もある．その一つがいわゆる暗号ブレイク時における電子署名の過去においての非生成を証明する（アリバイ）という，**2.** で述べる問題である．この「電子署名アリバイ問題」に対する解決方法の方向性を **3.** において探り，我々の提案である「ヒステリシス署名」のコンセプトを **4.** において，また「履歴交差」のコンセプトを **5.** で示す．さらにこれらを用いた電子署名アリバイ実現機構の概要を **6.** で論じ，**7.** で本論文をむすぶ．

2. 電子署名アリバイ問題

電子署名の作成時と検査時に技術環境が大きく変化した場合に起こりえる重大な事態について考えよう．たとえばEC (Electronic Commerce) のシステムでは，債権や手形のように，ある期間が経過した後に換金されるものが流通する．債務者が電子債権にディジタル署名を施す際には，その時点で望みうる最も優れたディジタル署名方式を用い，妥当だと考えられるビット長の署名生成鍵を用いていたとする．

そうであっても，時がたち電子債権の換金時点においては，債務者が電子債権への署名に使用していたディジタル署名アルゴリズムのセキュリティが著しく低いことが明らかとなっていたり，債務者の秘密の署名生成鍵が（公開の署名検査鍵等から算出されるなどして）漏洩していたりする可能性がある．そのような場合に，不正者によって偽造された電子債券が持ち込まれたならどうなるだろう（図1）．このような脅威から利用者を保護するには，与えら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，あるいは当該利用者以外のエンティティによって偽造されたものなのかを判別できるようにしておくことが必要である．

すなわち，本来自分だけが持つ暗号的署名生成機能を自分以外のエンティティが持っているおそれのある状況で，自分が署名した覚えがない電子文書が提示されたときに，署名していないことを調停者に対して証明できること――「電子署名アリバイ」が求められる．アリバイ(alibi)とは，元来，現場への非存在証明の意味であるが，本論文では「署名の非生成証明」の意味も担わせる．

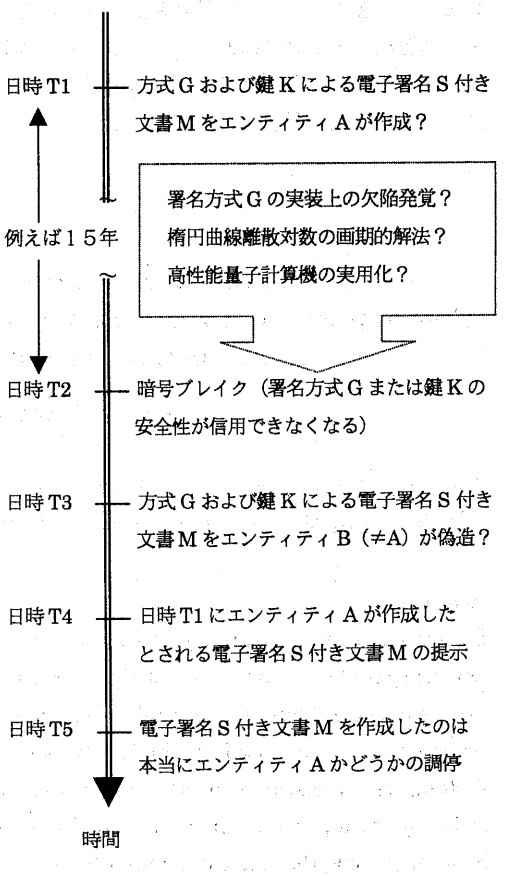


図1. 技術環境変化と電子署名アリバイ問題

3. 電子署名アリバイ実現へのアプローチ

例えば，情報理論的に安全な電子署名方式を利用することにより本論文で想定しているような状況がそもそも存在しえないようにするということは一つのアプローチである．しかし，情報理論的に安全でありしかもEC等の実用に耐えられると認められる電子署名方式はまだ出現していない．

より現実的な方法としては，1つまたは複数のTTPに，電子署名付き文書の全文またはそのハッシュ値を保管してもらうという方法もある．あるいはいわゆるディジタルタイムスタンプ技術[1]もある．たとえば利用者が信頼する1つまたは複数の第三者機関（TTP: Trusted Third Party）にタイムスタンプ（時刻印）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の利用が考えられる[2][3]．しかし，このように何らかのTTPを利用する方式の場合，TTPに負荷が集中し，利用者が必要な時に利用できないという危険性もある．また，TTPの署名を用いる方式の場合は，TTPの署名生成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というおそれもある．

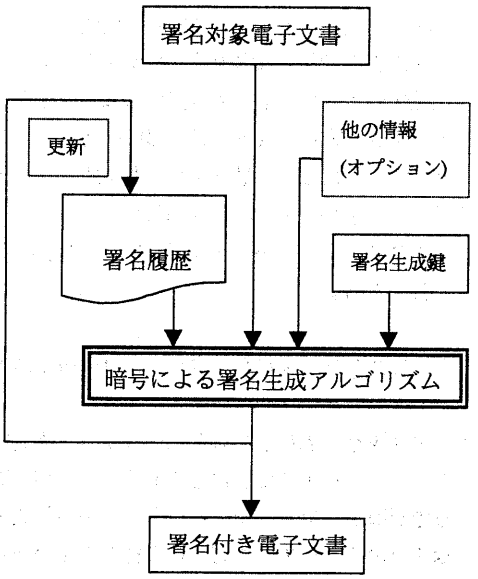


図2. ヒステリシス署名の生成

これに対しTTPを頼るのではなく，電子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により，当該利用者が生成した電子署名であるか否かを事後になっても確認可能とするというアプローチも考えられる．これが本論文における我々の主要提案である．

4. ヒステリシス署名

電子署名アリバイを実現するための方法として我々が提案するのは，署名の対象とする電子文書に署名を付与した時のヒステリシス情報すなわち履歴情報を綴り込むことである（図2）．

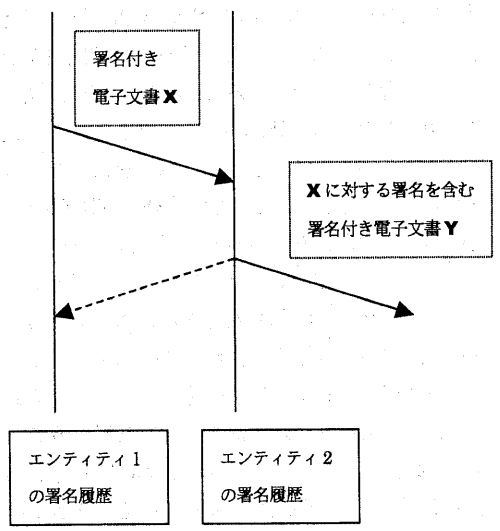
電子署名技術が，署名鍵の作成と解読における計算量の非対称性に依存する限り，コンピュータ技術の進歩により，暗号のブレイク状況，すなわち，署名生成鍵を持っているエンティティが本来の鍵所持者以外にも存在するという可能性を確率的に有意とみなさざるを得なくなる状況が生じることは避けられない．これが電子署名アリバイ問題における基本的な状況設定である．こうした状況でアリバイを実現するときの基本的な方法は，署名対象文書にその時の時間情報を綴り込んで署名することである．しかし，そうした時間情報を再現可能なデータとして綴り込む限りでは，過去に利用可能であった時間情報データを使って「過去の電子署名」を偽造することは一般に可能となってしまう．そして，こうした「過去の電子署名」偽造の可能性が存在する限り，調停者は電子署名のアリバイを承認することも崩すこともできない．

我々の提案は，時間情報を文書に綴り込むのではなく，署名者が過去に係わった署名付き電子文書の圧縮データを次々に綴り込んで行くことである．こうして次々に綴り込まれている電子署名付き文書の体系においては，「過去の電子署名」を偽造するためには，偽造しようとする電子署名が作成されて以降の全ての電子署名を整合的に偽造しなければならなくなる．これは「過去の電子署名」を偽造することの困難性を増加させることによって，署名を偽造することによる正しい業務実行者への攻撃を難しくするとともに，正しい業務実行

者にとっては，自らを，アリバイ偽造が困難な地位に置くことによって，悪意による攻撃に晒されたときの調停者への証明力を高める効果をもたらすのである．これがヒステリシス署名(hysteresis signature)の概念である．

5. 履歴交差

ヒステリシス署名の証明力は，こうしたヒステリシス署名付き文書が署名を作成したエンティティの手を離れ，他のエンティティの電子文書におけるヒステリシスとして署名に綴り込まれたとき，さらに飛躍的に向上すると考えられる（図3）．それは，第一には，こうした履歴情報の交差によりヒステリシス署名が拡散することは，「過去の電子署名」を偽造しようとするときの作業量を鼠算的に拡大させるからであり，第二には，そうした偽造作業に自分以外のエンティティを巻き込まざるを得なくなるということが，相互牽制の効果を働かせる（あるいは，相互牽制効果が働くだろうと，調停者に推定させる）からである．



ヒステリシス署名付き文書Xはエンティティ1のX生成時までの署名履歴を運び，エンティティ2がそれを含む署名を行うことによりエンティティ2の署名履歴に継承される．これはさらにヒステリシス署名付き文書Yによって運ばれる．

図3. 履歴交差

6. 電子署名アリバイ実現機構の概要

与えられた電子書名がある利用者が生成した電子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を用いて，自己の電子署名を正しく生成することができない．
- 利用者が生成した電子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．

これらの要件を満たすために耐タンパー性のある環境を用意し，電子署名の生成および署名履歴の保管に利用する．この前提のもとで，電子署名アリバイ機構は，まず，署名生成者の署名履歴——これには他のエンティティの署名履歴との交差が含まれる場合もある——に依存して署名生成を行うというヒステリシス署名の生成を行い，署名生成者の支配領域内の署名履歴を更新する．署名履歴を他エンティティの支配領域内の記録に反映させる．署名生成者の署名履歴や他のエンティティの記録をもとに電子署名の非生成証明（アリバイ）を判断する．以上が提案のあらましである．

このメカニズムをやや詳しく述べると以下のとおりである．

1）ヒステリシス署名生成および署名履歴の更新プロセス

署名履歴に依存して署名を生成する．署名履歴を耐タンパー領域に記録しておく．その際，署名履歴が改ざんできないように個々の署名作成の記録を絡める．その絡め方には多様な方法がありえるが，姉妹論文[4]で詳述するチェイニング署名（chaining signature）の機構は効果的な方法の

一つである：これはその名のとおり，連鎖的な方法であり，署名履歴中にある<前データ>と署名対象文書から得られる２つ組

[<前データ>のハッシュ値，署名対象文書のハッシュ値]

を暗号的署名生成方式により署名生成鍵を用いて変換する．その結果できた電子署名を<ヒステリシス署名>とする．そして，３つ組

[<前データ>のハッシュ値，署名対象文書のハッシュ値，<ヒステリシス署名>]

を<現データ>として署名履歴に追記する．

２）署名履歴記録プロセス

署名履歴をどこに保存するかについて選択の余地がある．大別して署名者自身の支配領域と他のエンティティの支配領域とがありえる．基本は署名履歴を耐タンパー領域に記録しておくことである．

３）署名履歴信用性向上プロセス

署名履歴またはその一部を他のエンティティの支配領域に渡す場合と考える．その際，第三者（ブローカと仮称する）を介し，どこに送られどこに記録されるかが署名作成者の意思によらないようにすることが考えられる．ブローカが定められた機能を果たすことは信用する．署名履歴をブローカに送るときには，誰にいつと渡すかということを含んだヒステリシス署名をしておく．

また，上記プロセスで受け取った署名履歴を単に記録するだけでなく，それに対する自らのヒステリシス署名をブローカ経由で返すことも，署名履歴の信用性を向上するために役立つ．

ここで注目すべきことは，このプロセスで他エンティティのためにしたことが，履歴交差の概念から，自分の署名履歴の信用性を向上させ自らの利益につながるという特質が現れてくることである．

４）署名履歴収集＋署名履歴検査プロセス

さて，調停対象の電子署名が提示されたとき，その電子署名の生成者だとされるエンティティの署名履歴が全部揃えば正しい判断ができる．署名履歴が一部分しか揃わない場合には，得られた手がかりでできる限りの判断をする．

7. おわりに

本論文では，電子データに施された電子署名が，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判別するという，電子署名アリバイの問題を指摘した．署名履歴の活用がこの問題の解決にとって有効であることを踏まえ，「ヒステリシス署名」および「履歴交差」という２つのコンセプトを提案し，これらを基礎とする電子署名アリバイ実現機構の概要を示した．電子署名アリバイ実現機構は，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．電子署名アリバイ実現機構のより詳細なメカニズムは姉妹論文[4]で検討する．また，プロトタイプシステムを開発し，より定量的な評価をしていく予定である．

参考文献

[1] 宇根，松浦，田倉，“デジタルタイムスタンプ技術の現状と課題“ IMES Discussion Paper Series, 日本銀行金融研究所，1999年9月．

[2] C. Adams, et al, “Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP),“ IETF PKIX-WG Internet Draft

[3] C. Adams, et al, “Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols,“ IETF PKIX-WG Internet Draft

[4] 洲崎，宮崎，宝木，松本，“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 —,“ 情報処理学会コンピュータセキュリティ研究会第8回研究発表会，2000年3月．