3-11　今後のネットワーク社会活動の証拠性を支えるヒステリシス署名並びにその関連技術

3-11 Hysteresis Signature and Its Related Technologies to Maintain the Digital Evidence for Network Activities in Future Society

豊島　久　　宮崎邦彦
TOYOSHIMA Hisashi and MIYAZAKI Kunihiko

要旨

情報の流通が多様になることで、セキュリティ技術戦略の見直しの必要性が高まっている。例えば情報漏えい問題では、正当な活用を前提として漏えいを防ぐ直接的対策のみではなく、漏えい事実の検出・範囲の特定などを含め、いかに責任主体として妥当な扱いをしたかという証明責任を伴う体系的セキュリティ対策が求められる。この後者の軸となる課題を証拠性と呼ぶことにする。NICT では、2001 年より「次世代証拠基盤技術に関する研究開発」を行い、日立製作所がこれに取り組んだ。主となる成果は、電子署名の長期的安定性を支えるヒステリシス署名技術及びその検証技術開発である。ここでは、その取組成果及び関連研究について報告を行う。

Security Requirements are varied with rapid growth of Internet and mobile network in digitization progress of information. The necessity for reexamination of the security technological strategy is increasing. For example, the systematic security countermeasures which can prove having dealt with information appropriately are required in addition to direct security countermeasure such as encryption and access control. The problem of digital evidence occurs as a view which takes the lead for that. NICT started a research project "research and development about next-generation evidence based technologies" in 2001, and Hitachi tackled this. This paper reports overview of results of the research project and related topics which contain hysteresis signature for long-term documents and its verification technologies.

[キーワード]
証拠性，電子署名，ヒステリシス署名，署名履歴交差，説明責任
Digital evidence, Digital signature, Hysteresis signature, Log chain crossing, Accountability

1　はじめに

最近、情報管理責任など社会的観点からセキュリティ問題が大きく取り上げられることが多くなってきており、これらへの適切な対策が求められている。

しかし、特定の秘密情報などへのアクセス制御などと比較すると、多くの人がかかわる企業活動やその一部として情報システムが関連する情報漏えいなどの対策は、対策すべき範囲が広範に及ぶ。その結果、コストが膨大になる上に完璧性を期待すること自体が難しいのが実態である。

情報システムに限らない現実の社会活動では、すべての行為を事前確認するのではなく、一定の対策以上について例えば司法制度などをセーフティネットとして大半の活動がなされている。

一方従来、情報システムなどにおいて実用に供されているセキュリティ技術範囲は、不正アクセスなど個々事象に対する事前対策が主であった。

社会全体として情報流通が多様化し、情報の

価値が高まる今後の状況にあっては、事前対処型のセキュリティ対策に加えて、事後対処型の対策を講じバランス良くセキュリティ対策を組み上げることが必要となる。

電子的活動において、事後対処を可能にする上で基礎となるのが、証拠性の技術である。

中でも、電子署名技術は電子署名法が制定され、事後検証を行う上で最も重要な技術の一つである。

電子署名法はPKI基盤（Public Key Infrastructure）を前提として「電磁的記録の真正な成立の推定」を目的としている。したがって、元々主たる目的の一つが証拠性の確立にあったと言える。

しかし、PKI基盤の整備は一部で進んだものの、活用実態的には相手方の本人性確認を行う認証が一部で用いられているのみで、もう一つの目的の電子署名の証拠的活用はあまり進展していない。この理由は「電磁的記録に関する司法的判断が蓄積されていないために、その価値が示されていないこと」など、幾つか考えられるが、社会制度に先行してきちんとした技術基盤を確立しておくことが必要である。

技術面の問題の一つに、電子署名技術の長期的有効性確保の問題がある。

例えば、電子署名技術では暗号鍵を用いるが、この鍵自体に証拠性観点から言えば短期間とも言える有効期限がPKI基盤で定められており、有効期限以降では、有効期限以前に署名された電子文書も含め真正性が確認できなくなる。あるいは、鍵自体もデジタルデータであるために、いわゆる印鑑などと比較するとコピー・他者への伝送などが一般的に容易である。したがって、一度鍵が漏えいしてしまうと、過去の電子文書の証拠性を含めて影響範囲を限定することが困難になる可能性が残る。

このような背景の下、本研究では電子署名技術の問題解決を図り、電子署名を活用した証拠性確立を目標として技術開発を行った。

2　ヒステリシス署名技術

2.1　署名の長期利用における課題

インターネットの普及に伴い、各種文書の電子化が進んでいる。このような状況の中で電子文書の真正性（本人性）を保証する技術である電子署名技術の重要性がますます増している。今後は従来以上に、長期にわたって利用される文書の真正性保証、証拠力の保持を目的とした利用が進む。

例えば、2005年4月に電子文書法が施行され、紙文書を電子化して保存することが認められるようになるが、その真正性を支えるよりどころとなるのは、電子署名やそれに基づくタイムスタンプである。このような保存文書は、比較的長期（例えば税務書類の場合7年間）の保管が義務付けられており、長期間経過後にその真正性を確認するケースもあり得る。

また、債権や手形あるいは遺言状のような、ある一定期間が経過した後に換金されたり、効力を発揮したりする文書が電子化された場合にも、同様に長期間経過後にその真正性を確認する必要が生じる。

このような長期にわたる証拠性を保持する目的で、従来の電子署名技術を用いた場合に、注意すべき点として、署名生成時点と、それから長期経過した後の署名検証時点とで、技術環境が異なっている可能性があるという点が挙げられる。例えば、署名生成時点では困難とされている秘密鍵の推定が、長期経過後には暗号解読手法や解読用コンピュータの飛躍的な進歩によって可能となったり、管理者の不備による秘密鍵の漏えいなどの運用に伴う人的なエラーが発生しないとも限らない。このような秘密鍵の秘匿性が失われる事態は暗号ブレイクと呼ばれる。

いったん暗号ブレイクが起こり、攻撃者が署名用秘密鍵を入手してしまうと、攻撃者は、正しい（正しく見える）署名を幾らでも後から（i. e. 署名検証時点に）容易に生成することが可能となる。結果として、たとえ正しく検証される署名であっても、もはや過去に正しく作られたものであったのか、後に攻撃者によって偽造されたものなのか、区別できなくなり、証拠性が失われてしまう。

本稿では、このような暗号ブレイクが生じた際にも、電子署名に基づく証拠性を保証可能とするヒステリシス署名技術[1]-[4]について、その概要と安全性及び我々が行った実装評価結果に

ついて述べる。

2.2 関連技術

長期利用向けの電子署名技術としては、ヒステリシス署名技術のほかにも、(a) フォワードセキュア署名方式[5]、(b) キーインシュレイテッド署名方式[6][7]、(c) 電子公証サービス利用方式[4][8]、(d) タイムスタンプ併用方式[4]、(e) 署名延長サーバ利用方式[8]、(f) MAC (Message Authentication Code) による電子証拠物利用方式[9]、(g) 実行ハードウェア確認タグつき署名方式[10]、などが知られている。

これらは大別して、以下の二つのアプローチに分類される。ヒステリシス署名は後者に分類される技術である。

(1) 鍵を一定期間ごと (例：1 日ごと) に更新することによって、仮に鍵が漏えいしたとしても、被害の範囲を限定する方式・・・(a)(b)

(2) 通常の署名検証手順に加え、他の検証手順を用意しておくことにより、鍵の漏えい時にも、正当な署名と偽造署名とを判定可能とする方式・・・(c)～(g)

前者のアプローチは、鍵を比較的短期的に更新していくため、鍵漏えいに対して有効性が高いと考えられるものの、暗号解読手法や解読用コンピュータの進歩によって、鍵の推定が可能となった場合にはあまり効果がない。一方、後者のアプローチでは、暗号ブレイクの原因を問わずに効果が得られる。ただし、これらの技術はそれぞれ何らかの第三者機関に依拠するなど、根拠とする仮定が異なることに注意を要する。これらの技術を第三者機関への依存度の観点から分類した結果については、[11]に示されている。ヒステリシス署名は、比較的第三者機関への依存度が少ない技術といえる。

2.3 ヒステリシス署名技術の概要

ヒステリシス署名は、過去の署名履歴を取り込みながら署名生成を行う方式である。これにより署名間に連鎖構造を築き、暗号ブレイク時にも偽造を困難にする。

ヒステリシス署名では、n 回目の電子署名生成時に n−1 回目の署名結果データのハッシュ値を作用させる (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、当該署名システム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電子署名とを組にして相手(検証者)に送るが、ヒステリシス署名では、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。

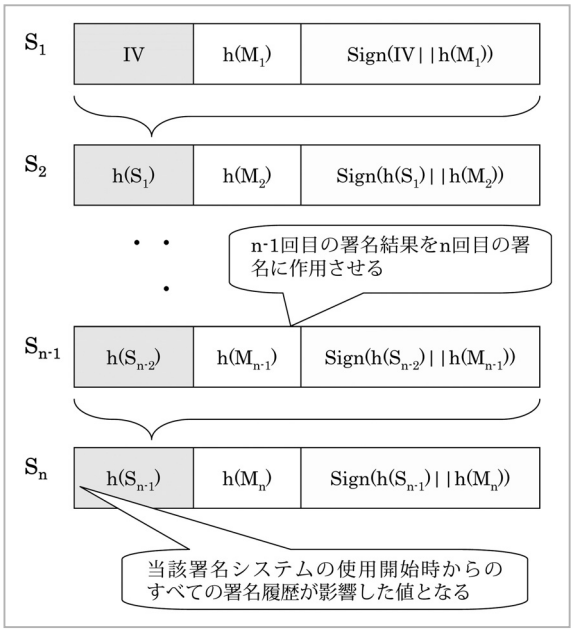

図1 ヒステリシス署名生成 (概要)

[ヒステリシス署名生成]

【入力 (外部)】メッセージ M_n

【入力 (内部)】秘密鍵、署名生成記録 S_{n-1}

【出力 (外部)】署名 $H(S_{n-1})$、$Sign(H(S_{n-1})||H(M_n))$

【出力 (内部)】署名生成記録 S_n

ステップ 1：あらかじめログデータとして保存しておいた一つ前の署名生成記録 S_{n-1} のハッシュ値 $H(S_{n-1})$ を計算し、連鎖用データとする。

ステップ 2：ステップ 1 で計算した連鎖用データ $H(S_{n-1})$ と、署名対象メッセージ M_n のハッシュ値 $H(M_n)$ を結合したデータ $H(S_{n-1})||H(M_n)$ に対し、秘密鍵を利用して署名を生成する。

ステップ 3：$H(S_{n-1})$、$Sign(H(S_{n-1})||H(M_n))$ を署名としてメッセージ M_n とともに、送信する。

ステップ4：$S_{n-1}||H(M_n)||Sign(H(S_{n-1})||H(M_n))$ を、新たな署名生成記録 S_n として保存する。

ヒステリシス署名付きメッセージを受け取った受信者は次のように署名検証を行う（通常取引時）。

［ヒステリシス署名検証］

【入力】メッセージ M_n、署名 $H(S_{n-1})$、$Sign(H(S_{n-1})||H(M_n))$、公開鍵

【出力】OK or NG

ステップ 1：M_n のハッシュ値 $H(M_n)$ と、署名として送信されてきた $H(S_{n-1})$ とを結合し、$H(S_{n-1})||H(M_n)$ を計算する。

ステップ 2：$H(S_{n-1})||H(M_n)$ と $Sign(H(S_{n-1})||H(M_n))$ を入力とし、公開鍵を利用した通常の署名検証を行う。

ステップ 3：OK or NG を出力

暗号ブレイク後に過去に生成されたヒステリシス署名の検証を行う際には、上記の手順により検証しただけでは十分ではない。なぜなら既に暗号ブレイクしているため、上記の手順によって検証 OK となるような署名は、正当な署名者以外にも生成できるからである。したがって、この場合には、メッセージ受信者、あるいは、署名の正当性を判定する調停者は、上記の手順に加え、署名者が保存している署名生成記録の中に当該署名に相当する署名生成記録 S_n が含まれていることを確認し、さらに、署名生成記録 S_n の正当性を次のように検証する。ここで S_m は最新あるいは過去に新聞紙上等に公開されているなど、何らかの意味で正当性が保証されている署名生成記録であるとする。

［署名履歴検証］

【入力】検証対象署名生成記録 S_n、公開鍵、署名生成記録 S_{n+1},,, S_m

【出力】OK or NG

ステップ 1：S_n に含まれる $H(S_{n-1})||H(M_n)$ と $Sign(H(S_{n-1})||H(M_n))$ を入力とし、公開鍵を利用した通常の署名検証を行う（単独署名履歴検証）。

ステップ 2：S_n のハッシュ値が、署名生成記録 S_{n+1} に含まれる $H(S_n)$ に一致することを確認（後の履歴との整合性確認）。

ステップ 3：n：=n+1 とする。n<m ならステップ 2 に戻る。

ステップ 4：ステップ 1 から 3 のうち一つでも確認できなければ NG を出力し、そうでなければ OK を出力。

以下では、上記のヒステリシス署名の安全性に関する基本的な検討結果について述べる。安全性の検討に当たっては、将来における暗号ブレイクの可能性を考慮し、次のような前提の下で行った。

（前提 1）署名生成時点（取引発生時点）では暗号はブレイクしていない。したがって、署名付きメッセージ受信者は取引の際には通常の署名検証により検証されれば、そのメッセージを受け入れる。

（前提 2）署名付きメッセージの有効期間内に、署名者の秘密鍵情報が何らかの原因によって不正者の知るところとなり、署名を偽造される可能性がある。

（前提 3）ハッシュ関数の一方向性（より正確には第二原像困難性。以下単に一方向性と呼ぶ。）は、将来にわたりブレイクされることはない。

このとき、上記の検証手順に関する次の命題が成り立つ。

命題 1：S_n が署名生成記録 S_{n+1} を用いた上記の署名履歴検証手順によって検証されたとする。このとき、S_{n+1} が偽造でなければ S_n も偽造でない。ただし、S_i が偽造である、とは、S_i が上記の署名履歴検証手順によって検証され、かつ、S_i に含まれるメッセージのハッシュ値 $H(M'_i)$ が、署名者が本来作ったメッセージ M_i のハッシュ値とは異なることとする。

証明：S_{n+1} が偽造でなく、かつ、S_n が偽造である、と仮定する。本来署名者が生成した署名の対象メッセージを M'_n、その署名生成記録を S'_n とすると、S_n $(=H(S_{n-1})||H(M_n)||Sign(H(S_{n-1})||H(M_n)))$ は偽造であるから、$H(M_n) \neq H(M'_n)$ である。したがって $S_n \neq S'_n$ となる。一方、署名履歴検証ステップ 2 を満たすから、$H(S'_n)$ は、偽造ではない（i. e. 署名者が本来 n+1 番目に作った署名に対応する）署名生成記録 S_{n+1} に含まれる $H(S_n)$ と、一致しなければならない。これは、ハッシュ関数 H の一方向性に反する。ゆえに、S_{n+1} が偽造でなければ S_n も偽造でない。

系 2：任意の n（<m）に対し、S_m が偽造でなく、かつ、すべての $n \leqq i < m$ について、検証対象署名生成記録 S_i、公開鍵、署名履歴 S_{i+1} を入力とした時の署名履歴検証手順による出力が OK で

あれば、S_n は偽造でない。
証明：明らか（命題を繰り返し適用すればよい）。

系 2 から、署名者によって生成されたことが確かに分かっている署名に対応する署名生成記録から、連鎖を順に（より過去の方向に）さかのぼれる範囲にある署名生成記録に対応する署名は、すべて確かに署名者によって署名されたものと認められることが証明される。

したがって、署名者は、署名生成記録を欠落のないように完全な形で保存しておき、かつ、その時点で最新の署名については確かに署名者自身によって署名されたことを証明できるようにすることにより、署名履歴に含まれるすべての署名について、署名者自身によって署名されたことを示すことが可能となる。

より具体的に、ヒステリシス署名の構成要素として、署名方式としては、1024-bit RSA 署名、暗号学的ハッシュ関数としては、SHA-1（160-bit 出力）を用いた場合を例にとって検討する。これらの構成要素について、現在知られている安全性（攻撃に必要とされる計算量）は表 1 のとおりである。

表1　ヒステリシス署名の構成要素の安全性

構成要素	攻撃の種類	攻撃に必要な計算量のオーダー
1024-bit RSA署名	公開鍵から秘密鍵を算出する	2^{80}
SHA-1 (160-bit出力)	同じ出力値を与える２つの異なる入力値を見つける [ハッシュ関数の衝突困難性に対する攻撃]	2^{80} (脚注1)
	与えられた出力値から(元の入力とは異なる)入力値を一つ見つける [ハッシュ関数の一方向性に対する攻撃]	2^{160}

1　2005 年 2 月に SHA-1 の衝突困難性が 2^{69} 程度の計算量で攻撃可能というニュースがあった。本稿執筆時点ではその詳細は明らかにされていないが、仮にこれが事実だとすれば、以降の議論では衝突困難性の計算量は、2^{80} ではなく 2^{69} と読み替える必要がある。ただし、本文中で述べるようにヒステリシス署名の安全性は、ハッシュ関数の一方向性（第二原像困難性）に帰着されるため、衝突に関する脆弱性は、最終的なヒステリシス署名の安全性には影響を与えない。すなわち過去に生成された SHA-1 を使ったヒステリシス署名の真正性は、衝突困難性が脆弱化した後であっても確認可能である。

したがって、1024-bit RSA 署名と SHA-1 ハッシュ関数を用いてヒステリシス署名を構成した場合、上述した前提条件は、計算量だけに着目すれば、次のように言い換えることができる。
（前提 1）署名生成時点（取引発生時点）では、攻撃者は 2^{80} 以上のオーダーの計算量は利用できない。
（前提 2）署名付きメッセージの有効期間内に、攻撃者は 2^{80} 以上のオーダーの計算量が利用可能になる。
（前提 3）署名付きメッセージの有効期間内に、攻撃者は 2^{160} 以上のオーダーの計算量は利用できない。

すなわち、署名付きメッセージの有効期間内に攻撃者が 2^{160} 以上のオーダーの計算量が利用できるようにならない限り、命題 1 が成立することを意味する。これは、現在広く利用されている 1024-bit RSA 署名が 2^{80} のオーダーの計算量をかけると偽造可能になるのに対し、ヒステリシス署名の偽造に必要な計算量は 2^{160} のオーダーの計算量であることを示しており、大きく安全性が向上しているといえる。また、この安全性は、ハッシュ関数の一方向性によるものであり、通常の電子署名の場合のように情報の秘匿性には依存しない。

以上の安全性に関する基礎検討結果をまとめると、ヒステリシス署名の安全性には、従来の電子署名技術と比較し、以下のような特徴がある。

(1) 偽造に必要な計算量が従来の電子署名技術と比較して大きい（例：1024-bit RSA 署名と SHA-1 ハッシュ関数を用いた場合、約 2^{80} 倍となる）。
(2) 特定の秘密情報の秘匿性以外の要因に基づく安全性を有するため、将来的な鍵漏えいに対応可能。

なお、安全性の検討に当たり、前提とした「ハッシュ関数の一方向性は将来にわたりブレイクされない」という条件については、前提とすることの妥当性に議論があり得る。すなわち、電子署名がブレイクされるという前提に立っているにもかかわらず、ハッシュ関数の安全性は仮定するというのは、公平な評価ではないのではないか、という意見もあり得る。しかし本研究開

発においては、以下のような理由から、電子署名がブレイクされていながらハッシュ関数の一方向性はブレイクされていない、という仮定が十分妥当な条件であると考える。

［理由 1］攻撃に必要な計算量が電子署名の場合と比較して非常に大きい。

表 1 に示したように、ハッシュ関数の一方向性を破るために必要な計算量は 2^{160} のオーダーであると考えられており、現在知られている最良の攻撃法を用いて、公開鍵から署名用秘密鍵を逆算するために必要と見積もられている計算量（2^{80} のオーダー）と比較して非常に大きい。なお、ヒステリシス署名において脅威となり得るのは、署名者が過去に作った署名履歴と整合するように、攻撃者があとから署名履歴及び署名を偽造することである。この偽造を成功させるためには、ハッシュ関数の衝突困難性を破るだけでは十分でなく、一方向性を破る必要があることに注意を要する。

［理由 2］特定の情報の秘匿性によらない。

電子署名では、いったん署名用の秘密鍵が漏えいしてしまえば、正しい（正しく見える）署名を幾らでも容易に生成することが可能である。しかしハッシュ関数の場合は、このような秘密情報は存在しない。したがって、「ある情報さえ知っていれば一方向性を破ることができる」という事態は起こり得ない。また、仮に一度、一方向性を破ることに成功したとしても（i. e. ある与えられた出力値となる入力値を見つけることができたとしても）、もう一度、一方向性を破るためには、一回目と同じだけの労力をかけなければならない（i. e. 別の与えられた出力値となる入力値を見つけるためには一回目と同じだけの計算量をかけなければならない）。

［理由 3］量子コンピュータに対する脆弱性が知られていない。

現在のコンピュータアーキテクチャと全く異なるコンピュータである量子コンピュータという技術が研究されている。実用化にはまだ時間を要すると考えられているが、仮に実用化されたとすると、現在の公開鍵暗号技術（電子署名技術を含む）は、短時間のうちに解読可能となることが知られている。一方、ハッシュ関数については、量子コンピュータの特性を生かした効率的な攻撃手法は今のところ知られていない。したがって、ハッシュ関数は、量子コンピュータという新しい技術に対する耐性も高いと考えられる。

以上のような理由により、将来、何らかの理由により、現在の電子署名技術が危殆化したとしても、ハッシュ関数の一方向性を破るには、更に非常に多くの時間を要するものと考えられる。したがって、本研究においては、「ハッシュ関数の一方向性は将来にわたりブレイクされない」という条件を前提とすることは妥当であると考えられる。

2.4 実装評価

本節では、ヒステリシス署名機能を実際にプロトタイプシステムとして実装したときの評価結果について述べる。

開発したプロトタイプシステムは、ヒステリシス署名機能をメールクライアントにプラグインとして組み込んだものである。ヒステリシス署名を構成する基本アルゴリズムとしては、署名アルゴリズムに 160-bit ECDSA 方式、ハッシュ関数に SHA-1 方式を利用した。

このプログラムを Intel ®Pentium®Ⅲ プロセッサ 650MHz のマシンで実際に動作させたときの実行時間を測定したところ、署名生成機能による署名作成の処理時間は、約 5.35ms であった。これは公開鍵を用いた従来の署名作成の処理時間約 5.17ms と比較して 3.5 %程度の増加であった。また、署名検証に要する時間は、約 9.54ms であり、従来の署名検証処理時間約 9.46ms と比較して1%未満の増加であった。ただし暗号ブレイク後には、更に署名履歴検証が必要となる。これに要する時間は、10,000 個の履歴をたどる場合で、約 1.7 秒であった。これは実用的な処理時間であると考える（Intel 及び Pentium は、米国及びその他の国におけるインテルコーポレーション又はその子会社の商標又は登録商標です。）。

以上の実装評価により、ヒステリシス署名技術が、処理時間をほとんど増加させることなく、安全性を向上可能な技術であることが確認された。

3　ネットワーク環境における証拠性確保への取組

3.1　ネットワーク環境における課題

前節で述べたように、各利用者における証拠性の確保のための手段として、ヒステリシス署名は有効である。今後は更にネットワークを通じた社会活動を支える上で、ネットワーク全体として、いかに証拠性を確保するかが重要となる。

ヒステリシス署名やそのほかの長期利用向け技術では、第三者機関が重要な役割を果たすが、ネットワーク全体での証拠性確保という観点からは、単なる中央機関への一極集中型のアプローチには次のような課題がある。

(1) 現在はもちろん将来にわたり中央機関の権威性が必要となるすべての証拠情報を中央機関に預託しなければならず、中央機関の負荷・責任は非常に大きなものとなる。

(2) 中央機関の信用が万一失われた場合に社会的影響が甚大である。

(3) プライバシー保護に関して利用者が不安を感じる可能性がある。

そこで本稿では、ヒステリシス署名方式で構築された署名生成記録間の連鎖構造を利用し、中央機関－一般利用者間及び一般利用者相互間で分散的に証拠を確保する方式について述べる。

3.2　署名履歴交差技術の概要

ヒステリシス署名によって各利用者自身の署名履歴に連鎖構造が築かれるようになった。この連鎖関係を更に他の利用者へ広げていくのが署名履歴交差技術である。

例えば、利用者 A と利用者 B との取引においては、しばしば、「利用者 A がサインした契約書に対し、利用者 B がサインする」といったことが行われる。これにヒステリシス署名を用いるとまず、利用者 A の署名には、それ以前に利用者 A が施した署名に関する情報が反映されているため、この利用者 A の署名を含むデータに対し、利用者 B が自分自身の署名を施すことにより、利用者 B の署名履歴に、利用者 A の署名履歴が取り込まれることになる。さらに利用者 A がこの A と B がサインした契約書に、受取りを確認する意味で再度署名し保存しておくと、今度は反対に、利用者 A の署名履歴に、利用者 B の署名履歴が取り込まれることになる。このように他の利用者との間で、通常の取引を通じて、署名の交換を繰り返すことにより、ある利用者の署名履歴を改ざんするためには、他の利用者の署名履歴との整合性をも考慮しなければならなくなる。これが履歴交差の原理である。

このような交差を各利用者間で繰り返し行うことにより、図 2 に示したように、様々な利用者の署名履歴間に関係性が生じ、ネットワーク全体としての証拠性が高まることが期待される。

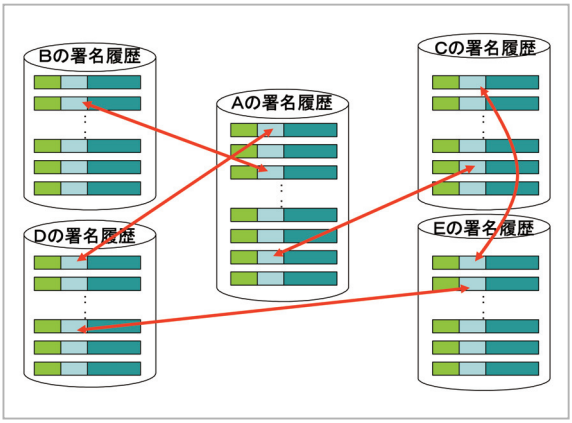

図2　署名履歴交差

3.3　開発内容

本節では、前節で述べた署名履歴交差技術を実装した結果について述べる。

前節では、利用者間で署名を繰り返すことにより、履歴交差が実現されると述べたが、実際にはこれだけでは「だれのどの署名生成記録」が「だれのどの署名生成記録」と連鎖しているか、を検索することが容易ではなく、検証が困難になる。

そこで、これらの情報をユーザ検索ファイルとして管理することとした。なお、だれがだれと関係を持つかという情報はプライバシーにかかわる情報であるので、これらの情報は、署名履歴とは独立して管理することとした。

また、署名履歴交差の頻度が高い方が、安全性の観点からは望ましいが、一般の利用者が他の利用者との間で署名を繰り返すケースは常にあるとは限らないため、それに代わって中央機

関に預託することが考えられる。ただし、単なる中央機関への一極集中型のアプローチには前述のような課題がある。

そこで、開発したプロトタイプシステムでは、図3に示したように、中央機関に階層構造を設け、即時応答可能なWeb公開機関と、長期にわたる証拠性確保が可能な新聞公開機関との2階層に分けることにより、負荷分散と安全性の向上を両立させた。

すなわち、まず利用者は、Web公開機関に定期的にその時点での最新の署名生成記録を預ける。Web公開機関はこれに自身の署名(ヒステリシス署名)を付与した上でWebサイト上に公開することにより、その署名生成記録が確かに存在したことを保証し、だれからでも確認できるようにする。つまり、Web公開機関は、各利用者の証拠性を支える直接的なトラストアンカーとして機能する。

一方、Web公開機関は、定期的に、その時点でのWeb公開機関自身の最新の署名生成記録を新聞公開機関に送り、新聞公開機関は、これを新聞紙上等に掲載する。

一度新聞紙上に掲載された情報は、それが大量に印刷され、また多くの図書館等で保管されることから、単なるデジタルデータの場合と比較して、事後的に改ざんすることは著しく困難であると考えられる。

このことから、新聞公開機関は、Web公開機関の証拠性を支える直接的なトラストアンカーとして機能することになる。また間接的には、一般利用者の証拠性を支えるトラストアンカーにもなっている。

一般利用者が、直接新聞公開機関を利用することは、データ量的にも、コスト的にも現実的ではないが、このような階層構造を設けることにより、実質的に直接利用するのと同等の効果を、効率的に得られることになる。

なお、この階層構造は更に多層化することも可能であり、将来的には、ネットワーク社会全体の証拠性を支えるセーフティネットとして構築されることが望まれる。

3.4 今後の課題

以上述べたように署名履歴交差に基づく分散的なアプローチにより、ネットワーク全体としての高い証拠性を確保可能となった。

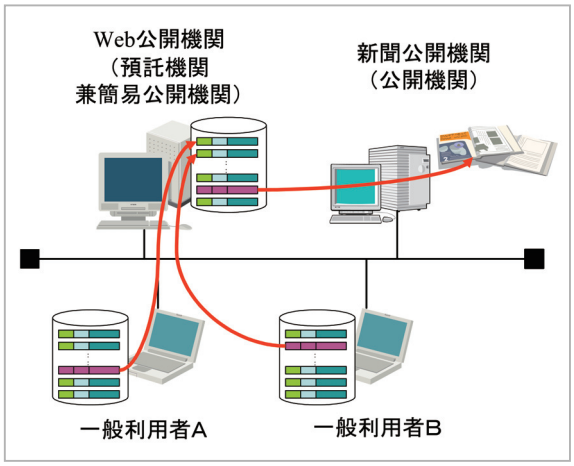

図3 中央機関の階層化

今後の課題としては、上述したより広範なセーフティネットの構築のほか、このように確保された証拠情報に基づく署名の適切な検証を一般利用者にいかに提供するか、ということが挙げられる。

現在までに開発したプロトタイプシステムでも、署名の検証は行っているが、これには分散確保されたデータを集めるという作業が必要となる。これは一般利用者にとっては負荷が大きい。さらには、本技術の特徴として、一部のエンティティの信頼性が失われた場合であっても全体としては信頼性を保てるケースがあるが、これを適切に判断するのは容易でない。

このような課題を解決するための一つのアプローチとしては、検証代行サービスを提供することが挙げられる。これはヒステリシス署名に限らず、他の署名方式を利用する上でも有効なアプローチであると考えられ、社会基盤としての整備が望まれる。

4 まとめ・今後の展開

冒頭で述べたとおり、セキュリティニーズが高度化することに伴い、セキュリティ技術が果たすべき役割の一部も変化する必要がある。フォレンジクス(Forensics)といった言葉が脚光を浴びつつあること自体が、ネットワーク活用の発達を背景として、様々な社会性を問われ始め

ていることの現れであると言える。

本報告で述べた証拠性へのアプローチについては、フォレンジクスやアカウンタビリティ（Accountability）などの言葉を出すまでもなく重要である。

この視点を強化したセキュリティ対応モデルを実現していくことで、情報漏えいなどの高度なセキュリティニーズに対して有効な対策を講じることが可能になる。

このようなアプローチは、個々の法人などが電子的活動に伴う説明責任を果たすことから進展していくものと考えられる。しかし、それらの対策の最終的理想像では、個別システム・個別法人で閉じるものではなく、社会機構的なものの構築を必要とする。業界団体あるいは地域経済圏など幾つかのレイヤの機構が構築されるべきであり、最後に、バックボーンとして、国家レベルの公証ネットワークなどというようなセーフティネット構築が期待されるものである。

しかし現実的には、ようやく電子的活動の個別事象について正当性が議論され始めた段階であり、今後の司法的判断の積み重ねなどを待つ必要がある。

ただし一方では、ログによる事実の推定などが徐々に行われつつある。これらの過程の中で適切な判断根拠が確立されていくこともまた必要である。

正しく、証拠性トラストの軸として電子署名活用を再度見直し、国家レベルの戦略として開発・整備を進めるべき領域であるともいえる。当然、証拠性がいつでも確認できる透明性を兼ね備えるべきことは言うまでもない。

そのような発展プロセスが想定されることからも論文中に触れたとおり、ネットワークを活用した分散的アプローチを講じていくことが望ましい。ヒステリシス署名技術に代表される今回の技術開発は、来るべきそのようなニーズに対して、一定の技術的対応策を提示することができたものと評価している。

今後は、ここで開発した技術を適用することで証拠性アプローチの必要性を実証していくとともに、例えば公証ネットワークとしてヒステリシス署名技術の更なる研究・開発などを推進していく必要がある。

謝辞

本研究を進めるに当たり、多数の貴重なご助言、ご指導いただいた早稲田大学岩村充教授、横浜国立大学松本勉教授、東京電機大学佐々木良一教授、電気通信大学吉浦裕助教授、明治大学夏井高人教授の各位に謹んで感謝の意を表する。

参考文献

1 松本勉，岩村充，佐々木良一，松木武，“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第 8 回研究発表会，2000.

2 洲崎誠一，宮崎邦彦，宝木和夫，松本勉，“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.

3 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，pp.42-48，共立出版，2000.

4 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.

5 Mihir Bellare and Sara K.Miner, "A Forward-Secure Digital Signature Scheme", In Proc. of Crypto, pp.431-448, 1999.

6 Yevgeniy Dodis, Jonathan Katz, Shouhuai Xi, and Moti Yung, "Key-Insulated Public Key Cryptosystems," EUROCRYPY 2002, Lecture Notes in Computer Science, Vol.2332, pp.65-82, Springer-Verlag, 2002.

7 Yevgeniy Dodis, Jonathan Katz, Shouhuai Xi, and Moti Yung, "Strong Key-Insulated Signature Schemes", International Workshop on Practice and Theory in Public key Cryptography (PKC2003), Lecture Notes in Computer Science, Vol.2567, pp.130-144, Springer-Verlag, 2003.

8 電子商取引実証推進協議会認証・公証ワーキンググループ，“電子文書長期保存に関する中間報告”，H12－認証・公証WG-3，2001.

9 小森旭，松浦幹太，須藤修，“電子商取引における紛争解決のための電子証拠物に関する分析”，2002 年暗号と情報セキュリティシンポジウム予稿集, 電子情報通信学会，pp.627-632，2002.

10 宇根正志，松本勉，“実行ハードウェア確認タグ付きディジタル署名方式”，情報処理学会研究報告，2002-CSEC-18，pp.245-252，2002.

11 宮崎邦彦，吉浦裕，岩村充、松本勉，佐々木良一，“第三者機関への依存度に基づく長期利用向け電子署名技術評価手法の提案”，情報処理学会論文誌，Vol.44，No.08，2003.

豊島 久（とよしま ひさし）
株式会社日立製作所公共システム営業統括本部公共ビジネス企画本部主管
公共情報システム、情報セキュリティ

宮崎邦彦（みやざきくにひこ）
株式会社日立製作所システム開発研究所第７部研究員
暗号、情報セキュリティ