コンピュータセキュリティ　18−37
(2002.　7.　19)

連鎖構造を用いた電子署名技術における信頼性評価手法の提案

宮崎　邦彦† 吉浦　裕† 岩村　充†† 松本　勉††† 佐々木良一††††

† 株式会社日立製作所 システム開発研究所　〒244−0817 横浜市戸塚区吉田町 292
†† 早稲田大学 大学院アジア太平洋研究科　〒169−0051 東京都新宿区西早稲田 1−21−1
††† 横浜国立大学 大学院環境情報研究院　〒240−8501 横浜市保土ヶ谷区常盤台 79−7
†††† 東京電機大学 工学部　〒101−8457 東京都千代田区神田錦町 2−2
E-mail: †{kunihiko,yoshiura}@sdl.hitachi.co.jp, ††iwamuram@mn.waseda.ac.jp,
†††tsutomu@mlab.jks.ynu.ac.jp, ††††sasaki@im.dendai.ac.jp

あらまし　暗号学的ハッシュ関数を用いて電子署名の安全性を向上させる手法（ヒステリシス署名）が提案されている．ヒステリシス署名技術とは，署名間に連鎖関係を構築することで，署名の偽造を困難にする技術である．すなわち，偽造を試みる攻撃者にとって見ると，単一の電子署名を改ざんするだけでは十分でなく，連鎖関係をも改ざんする必要が生じるため，偽造が一層困難になるというものである．ヒステリシス署名の安全性評価結果としては，従来，ハッシュ関数の一方向性を破るための計算量に基づく評価が知られている．しかし，この手法ではヒステリシス署名が持つ特徴，すなわち，ある署名に関する情報が他の多くの情報に反映してしまうことによる改ざん困難性，が十分に表現されていないという課題があった．本稿では，多数の署名履歴情報の信頼性から検証対象となる署名の信頼性を評価する一手法を提案し，連鎖関係を有する電子署名技術の安全性について論じる．

キーワード　電子署名，ヒステリシス署名

A Method for Evaluating Reliability of Digital Signature Schemes with Linking Structure

Kunihiko MIYAZAKI†, Hiroshi YOSHIURA†, Mitsuru IWAMURA††, Tsutomu MATSUMOTO†††, and Ryoichi SASAKI††††

† Systems Development Laboratory, Hitachi, Ltd.
292 Yoshida-cho,Totsuka-ku, Yokohama-shi, 244–0817 Japan
†† Graduate School of Asia-Pasific Studies, Waseda University
1–21–1 Nishi-Waseda, Shinjuku-ku, Tokyo, 169–0051 Japan
††† Graduate School of Environment and Information Sciences, Yokohama National University
79–7 Tokiwadai, Hodogaya-ku, Yokohama-shi, 240–8501 Japan
†††† Faculty of Engineering, Tokyo Denki University
2–2 Kandanishikicho, Chiyoda-ku, Tokyo, 101–8457 Japan
E-mail: †{kunihiko,yoshiura}@sdl.hitachi.co.jp, ††iwamuram@mn.waseda.ac.jp,
†††tsutomu@mlab.jks.ynu.ac.jp, ††††sasaki@im.dendai.ac.jp

Abstract　Hysteresis signature, which improves security of digital signatures by cryptographic hash functions, has been proposed. By hysteresis signature technique a linking structure among the signatures is constructed. That is, one signature affects others. This is a major characteristic of the hystresis signature. Although some reliability evaluation results are known which are based on onewayness of hash functions, these results are not represented the characteristic of the hysteresis signature properly. In this paper, we propose a method for evaluating reliability of digital signature schemes with a linking structure.

Key words　hysteresis signature, digital signature

1. はじめに

1.1 背　景

インターネットの普及により，電子商取引や電子申請などのネットワークインフラを用いた社会活動がはじまっている．このような電子的な手段による社会活動の進展に伴い，それらの活動根拠となった電子文書等の正当性保証の必要性は拡大する．しかし，長期間にわたり利用される電子文書に対する正当性保証技術については，まだ課題が多い．

電子文書の正当性を保証するために，最も基盤となる技術は電子署名技術であり，これは暗号技術に依存している．現在の暗号技術は秘密鍵の推定に関る計算の困難性の上に成り立っており，ある程度の期間であれば，電子文書の正当性を保証することが可能であると考えられている．しかし，20〜30 年という長期にわたる正当性保証のためには，現在の暗号技術だけでは十分とは言いがたい．なぜなら，20〜30 年という長期にわたる運用の間には，秘密鍵の推定が可能となるような技術革新や，秘密鍵の漏洩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からである．

一旦，秘密鍵が不正者の手にわたると，当該鍵に基づく全てのネットワークにおける社会活動の内容は全く保証され得ないものとなり，社会的に大きな影響を及ぼす．なぜなら，不正者が過去に遡って各種の電子文書をあたかも正当なであるかのように作成することが可能となるためである．この結果，本来の署名生成者にとっては，身に覚えがない電子文書が偽造されて不利益を被るばかりか，さらには自分が過去に正しく作成した電子文書の正当性までもが疑われる可能性が高い．

長期にわたって電子文書の正当性を保証する手段が確立されない限り，電子的な手段による社会活動は，短い期間で完結する活動のみに限定されたものとなり，それ以上の進展は望めない．

1.2 従来技術

松本，洲崎，岩村らは，上記のような，暗号解読用のコンピュータ能力の飛躍的向上や，運用における人的エラーに起因する秘密鍵漏洩などの，第三者による電子署名の偽造を可能とする事象を「暗号ブレイク」と呼び，この問題の重大さと対策の必要性を指摘している．さらに，仮に暗号ブレイクがおきたとしても署名の正当性を長期にわたり保証できる技術として，ヒステリシス署名技術を提案している [1]〜[3].

宮崎らは，ヒステリシス署名の安全性を，偽造に必要な計算量の観点から分析している [4]．これによればヒステリシス署名の安全性は，連鎖を形成する際に利用されるハッシュ関数の一方向性の強度に依存する．たとえば 1024-bit RSA 署名方式と SHA-1 ハッシュ関数を利用してヒステリシス署名を構成した場合に，偽造に必要な計算量は，もとの RSA 署名と比較しおよそ 2^{80} 倍と見積もられている．

一方，洲崎らは，電子署名の偽造への対策手法として、(1) タイムスタンプの併用，(2)Foward-Secure Digital Signature, (3)Fail-stop signature, (4) ヒステリシス署名の 4 つ技術を挙げ、それぞれの有効性の考察を行っている [5]．これによれば，[1] で指摘された暗号ブレイク問題への解決となりうる方法は，タイムスタンプの併用と，ヒステリシス署名の 2 つであるとされている．ただし，タイムスタンプ併用方式の場合は，すべての電子署名付きメッセージに対し，タイムスタンプを押すことが必要になるという，実現上の課題も指摘されている．

1.3 提案技術

本稿では，ヒステリシス署名の検証方法によって確認される正当性について考察を行い，ヒステリシス署名における署名の偽造とは，どういうことであるかを定義する．また，この意味における偽造の困難性が，署名履歴の信頼性に依存することを明らかにした上で，署名履歴の信頼性評価手法を提案し，ヒステリシス署名の安全性について考察する．

なお，従来 [4] では，主として署名履歴の偽造に要する計算量の観点から安全性が分析されているが，本稿では，ヒステリシス署名の特徴である，ある署名に関する情報が他の多くの情報に反映してしまうことによる改ざん困難性，の観点からの分析を行う．

以下，第 2 節では，ヒステリシス署名の概要について述べる．第 3 節では，署名検証の結果が署名履歴の信頼性に依存することを示し，ヒステリシス署名における署名の偽造を定義する．第 4 節では，署名履歴の信頼性評価の一手法を提案し，第 5 節では，ヒステリシス署名の安全性について考察する．

2. ヒステリシス署名の概要

本節では，連鎖構造を用いた電子署名技術であるヒステリシス署名の概要を示す．

なお，本来ヒステリシス署名とは，「あるエンティティが署名対象となるメッセージに電子署名を施す際に，当該エンティティのそれ以前の署名生成履歴などといったヒステリシス情報を電子署名付きメッセージにつづりこんでいく方式」全般をさす用語であるが [1]，本稿では，その具体的な一実現形態である，チェイニング署名方式 [2] を検討の対象とする．以下，単にヒステリシス署名といったときには，このチェイニング署名を指すものとする．

2.1 表記法

$Sign()$： 従来の電子署名方式における署名生成処理
$Verify()$： 従来の電子署名方式における署名検査処理
$h()$： 一方向性ハッシュ関数
$A||B$： 二つのデータ A, B を連結したデータ
K_s： Alice の署名生成鍵
K_v： Alice の署名検査鍵
n： Alice がヒステリシス署名生成を行った回数
IV： 初期値
M_n： n 番目の署名対象メッセージ
S_n： n 番目のヒステリシス署名付きメッセージ
R_n： n 番目のヒステリシス署名生成記録
H_n： n 回目のヒステリシス署名生成を行った後の署名生成履歴（1 回目から n 回目までのヒステリシス署名生成記録を連結したデータ

2.2 ヒステリシス署名生成・検証処理手順

ヒステリシス署名作成・検証処理手順は，下記のとおりである．

ヒステリシス署名生成処理

Step 1. （署名生成フェーズ）署名対象メッセージ M_n のハッシュ値 $h(M_n)$ を算出する．

Step 2. 保存してある署名生成履歴 H_{n-1} に含まれる最新の署名生成記録 R_{n-1} のハッシュ値 $h(R_{n-1})$ を算出する．ただし，1 回目のヒステリシス署名生成処理においては，以降の手順でハッシュ値 $h(R_{n-1})$ の代わりに初期値 IV を用いる．

Step 3. Step 1，2 で算出した二つのハッシュ値を連結したデータ $h(M_n)||h(R_{n-1})$ に対して，署名生成鍵 K_s を用いて従来の署名生成処理を行い，電子署名付きメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ を生成する．

Step 4. 署名対象メッセージ M_n，最新の署名生成記録のハッシュ値 $h(R_{n-1})$，および電子署名付きメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ を連結し，ヒステリシス署名付きメッセージ

$$S_n = M_n||h(R_{n-1})||Sign_{K_s}(h(M_n)||h(R_{n-1}))$$

を生成する．

Step 5. （署名生成履歴更新フェーズ）二つのハッシュ値 $h(M_n)$，$h(R_{n-1})$ と電子署名付きメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ とを連結し，署名生成記録

$$R_n = h(M_n)||h(R_{n-1})||Sign_{K_s}(h(M_n)||h(R_{n-1}))$$

を生成する．

Step 6. 保存してある署名生成履歴 H_{n-1} と署名生成記録 R_n とを連結し，署名生成履歴

$$H_n = H_{n-1}||R_n$$

を生成して保存する．

ヒステリシス署名検証処理（通常時の署名検証処理）

通常時（i.e. 暗号ブレイク以前）における，ヒステリシス署名付きメッセージ S_n の検証は，次のように行う．

Step 1. ヒステリシス署名付きメッセージ S_n に含まれる署名対象メッセージ M_n のハッシュ値 $h(M_n)$ を算出する．

Step 2. Step 1 で算出したハッシュ値 $h(M_n)$ と，ヒステリシス署名付きメッセージ S_n に含まれるハッシュ値 $h(R_{n-1})$ および電子署名付きメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ と，Alice の公開鍵証明書に含まれる署名検査鍵 K_v とを用いて従来の署名検証処理

$$h(M_n)||h(R_{n-1}) \stackrel{?}{=} Verify_{K_v}(Sign_{K_s}(h(M_n)||h(R_{n-1})))$$

を行う．

ヒステリシス署名検証処理（暗号ブレイク後の署名検証処理）

暗号ブレイク以降における，ヒステリシス署名付きメッセージ

$$S_m = M_m||h(R_{m-1})||Sign_{K_s}(h(M_n)||h(R_{m-1}))\ (1 \leqq m \leqq n)$$

の検証処理は，上記の通常時の検証処理に加えて，次のように行う．

Step 1. Alice が保存している署名生成履歴 H_n のなかに，検証対象となっているヒステリシス署名付きメッセージに対応する署名生成記録

$$R_m = h(M_m)||h(R_{m-1})||Sign_{K_s}(h(M_n)||h(R_{m-1}))$$

が含まれていることを確認する．確認できなければ，検証失敗として終了．

Step 2. $k = m$ とし，以下の署名生成履歴 H_n の整合性検証を行う．

i. 署名生成履歴 H_n に含まれる署名生成記録 R_{k-1} のハッシュ値 $h(R_{k-1})$ を算出する．

ii. 署名生成記録 R_k の中のハッシュ値 $h(R_{k-1})$ が，上で算出した $h(R_{k-1})$ と同じ値であることを確認する．確認できなければ，Step 3 へ．

iii. $k < n$ であれば，$k := k+1$ とし，i へ．そうでなければ，Step 3 へ．

Step 3. 署名生成履歴 H_n のうち整合性が確認できた署名生成記録 $R_m, \ldots, R_k$ の中に**あらかじめ信頼できることが分かっている署名生成記録**が存在すれば，検証成功（正当な署名である）として終了．そうでなければ検証失敗として終了．

ここで，「あらかじめ信頼できることが分かっている署名生成記録」とは，ヒステリシス署名がベースとしている暗号技術以外の要因によって，その存在および非改ざん性が保証されている署名のことを指す（[2] における「信頼ポイント」に相当する）．具体的な例としては，耐タンパ性のある署名生成装置の中に格納されている署名や，過去に新聞等によって発表された署名，あるいは，信頼できる第三者機関によって保証されている署名などに対応する署名生成記録が挙げられる．

3. ヒステリシス署名の偽造

本節では，上述の暗号ブレイク後におけるヒステリシス署名の検証処理について考察を行い，処理結果が署名履歴の信頼度に依存していることを明らかにする．さらに，この点を明示的に議論できるようにするために，署名検証処理を一般化し，検証結果を「信頼度」付きで出力するように変更した処理手順を提案する．また，この一般化された検証処理により「ヒステリシス署名の偽造」とはどういうことかを定義する．

なお，以下では，ハッシュ関数の一方向性は仮定する．すなわち，与えられたハッシュ値を出力するような入力メッセージを見出すことは困難であると仮定する．

3.1 ヒステリシス署名検証手順の考察

ここでは，2. 節に示した暗号ブレイク後における署名検証処理について，考察を行う．

暗号ブレイク後の署名検証処理は，大きく次の3つの処理からなる．

a. 署名履歴中に検証対象となる署名に対応する署名生成記録が存在することの確認
b. 署名履歴が有するハッシュ関数に基づく連鎖構造が保たれていることの確認
c. 署名履歴中に「あらかじめ信頼できることがわかっている署名生成記録」が存在することの確認

a と b が確認されることにより，ハッシュ関数の一方向性を仮定した上で，「もし署名履歴中に信頼できる署名生成記録が含まれていれば，検証対象となる署名に対応する署名生成記録も信頼できる」ことが分かる．a，b で確認すべきことは明確であり，入力として与えられたデータだけで判定することが可能である．

これに加えてさらに，c が確認されることにより，上記の結果とあわせて，最終的に「検証対象となる署名に対応する署名生成記録は信頼できる」ことが分かる．ただし，c では，署名生成記録が信頼できるか否かを判断する必要がある．これは，ヒステリシス署名がベースとしている暗号技術以外の要因によって，その存在および非改ざん性が保証されているか否かを判定するものであり，入力データだけから機械的に判定することはできない．

以上をまとめると，暗号ブレイク後の署名検証処理とは，「検証対象となる署名生成記録が信頼できるか否かを，署名履歴に含まれる他の署名生成記録が信頼できるか否かにより判定する処理である」といえる．すなわち，暗号ブレイク後の署名検証処理の結果は，署名履歴に含まれる他の署名生成記録の信頼度によって決まる．

ところで，他の署名生成記録が信頼できるか否かという判定は，一般には「信頼できる／できない」という2値的なものではなく，連続的なものであると考えるのが妥当であろう．また，信頼できる署名生成記録が一つしか含まれない場合と，多く含まれる場合では，複数の場合の方が検証結果の信頼度は高いと考えるのが妥当であろう．しかし，このような信頼度の概念は，上記の署名検証手順では明示的には表現できない．

そこで以下では，暗号ブレイク後における署名検証処理を一般化し，署名履歴の信頼度を，検証結果の信頼度として出力する方式を提案する．

3.2 一般化されたヒステリシス署名検証処理

本節では，2. 節で述べた暗号ブレイク後のヒステリシス署名検証処理を一般化し，検証結果に信頼度を含められるようにする．

具体的には，ヒステリシス署名検証処理（暗号ブレイク後の署名検証処理）を次のように変更する．

信頼度付きヒステリシス署名検証処理（暗号ブレイク後の署名検証処理）

暗号ブレイク以降における，ヒステリシス署名付きメッセージ

$$S_m = M_m||h(R_{m-1})||Sign_{K_s}(h(M_n)||h(R_{m-1}))(1 \leqq m \leqq n)$$

の検証処理は，通常時の検証処理に加えて，次のように行う．

Step 1. Alice が保存している署名生成履歴 H_n のなかに，検証対象となっているヒステリシス署名付きメッセージに対応する署名生成記録

$$R_m = h(M_m)||h(R_{m-1})||Sign_{K_s}(h(M_n)||h(R_{m-1}))$$

が含まれていることを確認する．確認できなければ，検証失敗として終了．

Step 2. $k = m$ とし，以下の署名生成履歴 H_n の整合性検証を行う．

i. 署名生成履歴 H_n に含まれる署名生成記録 R_{k-1} のハッシュ値 $h(R_{k-1})$ を算出する．
ii. 署名生成記録 R_k の中のハッシュ値 $h(R_{k-1})$ が，上で算出した $h(R_{k-1})$ と同じ値であることを確認する．確認できなければ，Step 3 へ．
iii. $k < n$ であれば，$k := k+1$ とし，i へ．そうでなければ，Step 3 へ．

Step 3. 署名生成履歴 H_n のうち整合性が確認できた署名生成記録 $R_m, \ldots, R_k$ について，それぞれの信頼度を設定する．

Step 4. Step 3 で設定された各署名生成記録の信頼度から，検証対象となる署名に対応する署名生成記録 R_m の信頼度を算出し，これを検証結果（「検証成功」）の信頼度として出力する．

[注意 1] 上記の処理手順において，Step 3 で設定する信頼度や，Step 4 で算出する信頼度を，具体的にどのように設定，算出するかについては，いろいろな場合がありうる．たとえば，Step 3 の信頼度を 0, 1 の 2 値で与え，Step 4 での R_m の信頼度を，$\max_{m \leqq j \leqq k}\{R_j$ の信頼度 $\}$ と算出するものとすれば，この検証手順は，2. 節で示した検証手順と一致する．本稿では，ヒステリシス署名の特長をとらえる上で，より適切と考えられる信頼度算出モデルを 4. 節で提案する．

3.3 ヒステリシス署名の偽造

本節では，前節で述べた署名検証処理の一般化を踏まえ，ヒステリシス署名における偽造について定義する．

通常の電子署名の偽造については，次のように定義された．[5]

[定義 1]（電子署名の偽造） 署名生成者アリスとは異なる署名偽造者オスカーが生成した電子署名付きメッセージに対し，ボブがアリスの公開鍵証明書を用いて署名検証を行った結果，正当なものであると判定された場合，オスカーはアリスの電子署名の偽造に成功したという．

ヒステリシス署名における偽造の定義も，暗号ブレイク以前であれば，定義 1 を適用することができる．しかし，暗号ブレイク後の検証結果は信頼度付きで与えられると考えるので，この定義をそのまま用いることはできない．

そこで，本稿ではヒステリシス署名の偽造を次のように定義する．

[定義 2]（ヒステリシス署名の偽造） 署名生成者アリスとは異なる署名偽造者オスカーが生成した電子署名付きメッセージと署名生成履歴に対し，ボブがアリスの公開鍵証明書を用いて通常時における署名検証を行った結果，正当なものであると判

定され，さらに，署名履歴を用いた暗号ブレイク後の署名検証を行った結果，署名生成者アリスが本来生成した電子署名付きメッセージ（のうちの少なくとも一つ）と署名生成履歴に対する検証結果よりも，高い信頼度で正当なものであると判定された場合，オスカーはアリスの電子署名の偽造に成功したという．

4. 信頼性評価手法

本節では，前節で一般化されたヒステリシス署名検証処理に基づく，信頼度を具体的に算出する一手法を提案する．

まず，ハッシュ関数に基づく連鎖構造に関する基本的な考察を行い，信頼度算出方法が満たすべきと考えられる性質を明らかにする．次に，その性質を満たす信頼度算出手法を提案する．

なお，本節においても，ハッシュ関数の一方向性は仮定する．すなわち，与えられたハッシュ値を出力するような入力メッセージを見出すことは困難であると仮定する．

4.1 ハッシュ関数に基づく連鎖構造に関する考察

本節では，ハッシュ関数により連鎖した2つの署名生成記録間の信頼度について考察する．

今，署名生成記録 R_i と R_{i+1} が連鎖しているとする．すなわち，R_i は R_{i+1} の一つ前に生成した署名に関する署名生成記録であるとする．

もし，R_{i+1} が信頼できる署名生成記録であれば，すなわち署名者が過去の署名生成時点に生成した署名生成記録と同じであれば，R_i も信頼できる署名生成記録である．なぜなら，ハッシュ関数の一方向性により，R_{i+1} と正しく連鎖するように，R_i をあとから偽造することはできないからである．

一方，もし R_{i+1} が信頼できない署名生成記録であれば，すなわち署名者が過去の署名生成時点に生成した署名生成記録と異なれば，R_i は信頼できるかもしれないし，信頼できないかもしれない．なぜなら，暗号ブレイクを前提とすれば，R_i が信頼できようと，できなかろうと，R_i と正しく連鎖するように R_{i+1} をあとから偽造することは容易であるからである．

したがって，仮に「署名生成記録 R_i の信頼度」を「署名生成記録 R_i が正当である確率」と定義し（注：この定義はのちに変更しより精密化する），これを $f_{\mathrm{rely}}(R_i)$ であらわすとすると，$f_{\mathrm{rely}}(R_i) \geqq f_{\mathrm{rely}}(R_{i+1})$ が成り立つ．

4.2 個別信頼度設定方法

本節では，署名履歴に含まれる個々の署名生成記録の信頼度設定方法について述べる．

個々の署名生成記録が信頼できるか否かの判定には，主観的な要因が含まれる．まず署名生成記録ごとに，その履歴の保管状況や他の物理的媒体との関係などによって，適切な検査手順が選択され，その検査手順に従って正当なものであるか否かが判断されるものと考えられる．したがって，その判断結果の信頼性は，検査手順によって左右される．

たとえば，ある署名生成記録が，新聞等のマスメディアで紙として発表されていたものであったとすると，新聞に本当に掲載されていたか否かということを調べることによって判断される．この検査手順は明確であり，その判断結果の信頼性は高いといえる．一方，別のある署名生成記録が，署名者以外の第三者の手に渡っていたものであったとすると，その第三者が所有しているか否かを調べることにより，正当なものであるかどうかが判断される．この場合は，新聞に掲載されていた場合と比較すれば，判断結果は曖昧なものと言えるであろう．

このような署名生成記録ごとに異なる検査手順により判断された結果を統一的に扱うために，本節では，各署名生成記録の信頼度を，当該署名生成記録を検査するのに用いた検査手順の信頼度によって定義することにする．すなわち次のように定義する．

[定義 3]（署名生成記録の個別信頼度） 署名生成記録 R_i の個別信頼度とは，R_i の検査手順によって決まる値 $f_{\mathrm{ind\_rely}}(R_i) = (p_{\mathrm{ind}}(R_i), q_{\mathrm{ind}}(R_i), t_{\mathrm{ind}}(R_i))$ のことである．ただし，$p_{\mathrm{ind}}(R_i), q_{\mathrm{ind}}(R_i), t_{\mathrm{ind}}(R_i)$ は，他の署名生成記録とは独立に，以下で定義される．

- $p_{\mathrm{ind}}(R_i)$ R_i が正当であるとき，当該検査手順によって「正当」と判定される確率 $(1/2 \leqq p_{\mathrm{ind}}(R_i) \leqq 1)$
- $q_{\mathrm{ind}}(R_i)$ R_i が偽造であるとき，当該検査手順によって「正当」と判定される確率 $(0 \leqq q_{\mathrm{ind}}(R_i) \leqq 1/2)$
- $t_{\mathrm{ind}}(R_i)$ 当該検査手順による R_i の判定結果（R_i が「正当」と判定されたとき $t_{\mathrm{ind}}(R_i) = 1$, R_i が「偽造」と判定されたとき $t_{\mathrm{ind}}(R_i) = 0$）

[注意 2] 判断材料がない等の理由により，ある署名生成記録 R_i の検査ができない場合には，個別信頼度は，$f_{\mathrm{ind\_rely}}(R_i) = (1/2, 1/2, 1)$ と設定するものとする．なお，$t_{\mathrm{ind}}(R_i)$ は便宜上1（「正当」）と設定しているが，0（「偽造」）と設定してもよい．（次節での信頼度算出方法には影響を与えない）

4.3 信頼度算出方法

本節では，ヒステリシス署名検証結果の信頼度を算出する方法を提案する．

まず，ヒステリシス署名検証結果の信頼度を次のように定義する．

[定義 4]（署名生成履歴の信頼度） 署名生成履歴 H_n の署名生成記録 R_m に関する信頼度とは，R_m が実際に正当である確率 $f_{\mathrm{post\_rely}}(R_m)$ のことである．文脈から対象としている署名生成記録が明らかな場合には，これを単に署名生成履歴の信頼度と呼ぶ．また，ヒステリシス署名付きメッセージ S_m と署名生成履歴 H_n に対する信頼度付きヒステリシス署名検証処理結果の信頼度とは，署名生成履歴 H_n の署名生成記録 R_m に関する信頼度のことである．

次に，前節で定義した署名生成記録の個別信頼度から，署名生成記録の信頼度をどのように算出するかについて述べる．

今，署名生成記録 R_i と R_{i+1} が連鎖しているとし，それぞれ適切な検査手順によって正当であると判定されたとする．すなわち，$f_{\mathrm{ind\_rely}}(R_j) = (p_{\mathrm{ind}}(R_j), q_{\mathrm{ind}}(R_j), 1)$ $(j = i, i+1)$ であったとする．このとき，R_{i+1} が実際に正当である確率を，$f_{\mathrm{post\_rely}}(R_{i+1})$ と書くと，他に条件がなければ，$f_{\mathrm{post\_rely}}(R_{i+1}) = \frac{p_{\mathrm{ind}}(R_{i+1})}{p_{\mathrm{ind}}(R_{i+1}) + q_{\mathrm{ind}}(R_{i+1})}$ である．

一方，R_i が実際に正当である確率を考える．R_i は R_{i+1} と連鎖しており，また，R_{i+1} が実際に正当である確率が分かっている．さらに，4.1節での考察結果から，R_i が実際に正当であること

の事前確率 $f_{\text{pri\_rely}}(R_i)$ は，$f_{\text{pri\_rely}}(R_i) \geqq f_{\text{post\_rely}}(R_{i+1})$ を満たす．したがって，R_i が実際に正当である確率 $f_{\text{post\_rely}}(R_i)$ は，

$$
\begin{aligned}
& f_{\text{post\_rely}}(R_i) \\
&= \frac{f_{\text{pri\_rely}}(R_i)p_{\text{ind}}(R_i)}{f_{\text{pri\_rely}}(R_i)p_{\text{ind}}(R_i) + (1 - f_{\text{pri\_rely}}(R_i))q_{\text{ind}}(R_i)} \\
&\geqq \frac{f_{\text{post\_rely}}(R_{i+1})p_{\text{ind}}(R_i)}{f_{\text{post\_rely}}(R_{i+1})p_{\text{ind}}(R_i) + (1 - f_{\text{post\_rely}}(R_{i+1}))q_{\text{ind}}(R_i)} \\
&= \frac{p_{\text{ind}}(R_{i+1})p_{\text{ind}}(R_i)}{p_{\text{ind}}(R_{i+1})p_{\text{ind}}(R_i) + q_{\text{ind}}(R_{i+1})q_{\text{ind}}(R_i)}
\end{aligned}
$$

となる．

より一般に次の命題が成り立つ．

［命題 1］ ハッシュ関数による連鎖関係が確認可能な一連の署名生成記録 $R_m, R_{m+1}, \ldots, R_k$ に対し，それぞれの個別信頼度を $f_{\text{ind\_rely}}(R_i)$ $(m \leqq i \leqq k)$ としたとき，R_m が実際に正当である確率 $f_{\text{post\_rely}}(R_m)$ は，

$$
f_{\text{post\_rely}}(R_m) \geqq \frac{\prod_{i=m}^{k} P_{\text{ind}}(R_i)}{\prod_{i=m}^{k} P_{\text{ind}}(R_i) + \prod_{i=m}^{k} Q_{\text{ind}}(R_i)}
$$

を満たす．ただし，

$$
P_{\text{ind}}(R_i) = \begin{cases} p_{\text{ind}}(R_i) & \text{if } t_{\text{ind}}(R_i) = 1 \\ 1 - p_{\text{ind}}(R_i) & \text{if } t_{\text{ind}}(R_i) = 0 \end{cases}
$$

$$
Q_{\text{ind}}(R_i) = \begin{cases} q_{\text{ind}}(R_i) & \text{if } t_{\text{ind}}(R_i) = 1 \\ 1 - q_{\text{ind}}(R_i) & \text{if } t_{\text{ind}}(R_i) = 0 \end{cases}
$$

とする．

（証明）上の議論を繰り返し適用すればよい． □

［注意 3］ 命題 1 により，個別信頼度から履歴全体の信頼度を算出（より正確には下から評価）することが可能となる．以下，特に断らない限り，命題 1 の右辺の値を署名生成履歴の信頼度と呼ぶ．

［注意 4］ 命題 1 において，

$$
(\text{右辺}) = 1 \Big/ 1 + \prod_{i=m}^{k} \frac{Q_{\text{ind}}(R_i)}{P_{\text{ind}}(R_i)}
$$

である．一方，$p_{\text{ind}}(R_i), q_{\text{ind}}(R_i)$ の定義から，

$$
\frac{Q_{\text{ind}}(R_i)}{P_{\text{ind}}(R_i)} \begin{cases} \leqq 1 & \text{if } t_{\text{ind}}(R_i) = 1 \\ \geqq 1 & \text{if } t_{\text{ind}}(R_i) = 0 \end{cases}
$$

が成り立つ．したがって，署名履歴に含まれるある署名生成記録が「正当」と判断されれば，署名生成履歴の信頼度は高くなるし，「偽造」と判断されれば，署名生成履歴の信頼度は低くなる．また $p_{\text{ind}}(R_i) = q_{\text{ind}}(R_i) = 1/2$ のときは，$t_{\text{ind}}(R_i)$ によらず署名生成履歴の信頼度は変化しない．つまり，十分な判断材料を持たない署名生成記録は，全体の署名生成履歴の信頼度に影響を及ぼさない．

これらの性質は，本稿における署名生成履歴の信頼度の定義の妥当性を支持するものであると考えられる．

5. ヒステリシス署名の安全性

本節では，偽造困難性の観点からヒステリシス署名の安全性について再考する．

ヒステリシス署名における偽造の成功とは，「本来の署名者の署名よりも高い信頼度で検証されること」であった．また検証結果の信頼度は，検証に用いた署名生成履歴の信頼度によって決まる．したがって，偽造を試みる不正者の戦略は次の 2 通りが考えられる．

a. 本来の署名生成履歴と整合するように署名を偽造する
b. 偽造した署名にあわせて署名生成履歴も作り直す

a の方針で偽造を行うためには，ハッシュ関数の一方向性を破る，すなわち与えられたハッシュ値を出力するような入力メッセージを見つける必要がある．これは [4] で分析されているように通常の電子署名の偽造と比べても著しく困難であるといえる．すなわち，ハッシュ関数の一方向性がヒステリシス署名の安全性の根拠の一つとなっている．

一方，b の方針で偽造を行うためには，作り直した署名生成履歴の信頼度が，本来の署名者の履歴の信頼度以上であると判定されなければならない．これが不正者にとって実現可能であるか否かは，本来の署名者のヒステリシス署名の利用状況にも依存するため，一概には判断しにくい．

たとえば，本来の署名者がヒステリシス署名利用期間中に一度しか署名生成をしていなかった場合には，署名生成履歴の中に記録は 1 つしか残っていないことになる．したがって，この場合には署名生成履歴の信頼度はあまり高くはなり得ず，結果として偽造を成功させる余地を残す．

しかしこのような極端なケースを除いた，通常の利用形態においては，本来の履歴以上の信頼度を持つ偽造履歴を作り直すことはかなり困難であると考えれられる．なぜなら通常の利用形態においては，偽造対象となる署名以降にもすでに多くの署名が生成され，それらは他者の手に渡るなどにより信頼度が判定できる状態にあると考えられるためである．

この場合，各署名生成記録の個別信頼度があまり高くなくても，たくさん集まることによって全体の履歴の信頼度は非常に高くなる．たとえば，4.3 節で提案した履歴の信頼度算出方法にしたがえば，個別信頼度が $(85\%, 10\%, 1)$ の署名履歴が一つあるより，個別信頼度が $(60\%, 20\%, 1)$ の署名生成記録が 2 つあるほうが，全体の履歴の信頼度は高くなる．

したがって，本来の署名者にとっては，過去に署名したときから不正者が偽造を試みるときまでの間に築き上げた署名生成履歴の信頼度が，不正者に対する大きなアドバンテージとなる．不正者がこれを覆すことは，実際上，困難であろう．さらに，ヒステリシス署名の利用頻度が多いほど，この困難性は高まる．このような社会における関係性をも巻き込んだ偽造の困難性が，ヒステリシス署名の安全性のもう一つの根拠である．

以上をまとめると，ヒステリシス署名の安全性は主として次の二つの要因によって支えられているといえる．

I 連鎖構造を形成するハッシュ関数の一方向性
II 一つの署名生成の事実が他の多くの署名に反映すること

による事実否定の困難性

これらの条件は，仮に暗号ブレイクがおこったとしても，引き続き仮定できる可能性が高いと考えられる．

ただし，もしIが仮定できなくなった場合は，上述のaの方針に基づく偽造が成立する可能性がある．また，IIが仮定できなくなった場合には，bの方針に基づく偽造が成立する可能性がある．なお，いずれのケースも暗号ブレイクを仮定した場合にのみ成立することを注意しておく．

6. まとめ

本稿では，連鎖構造を用いた電子署名技術であるヒステリシス署名の検証処理について考察を行い，検証結果が署名生成履歴の信頼度に依存することを明らかにした．

さらに，この点を明確に議論できるようにするため，検証処理を一般化して，検証結果に信頼度の概念を含めるようにし，信頼度を算出する，ヒステリシス署名の信頼性評価手法を提案した．また，検証結果に信頼度を含めたことにより，ヒステリシス署名における偽造の概念が定義2に示したように明らかになった．

このヒステリシス署名の信頼性評価手法に基づき，ヒステリシス署名の偽造困難性の観点から安全性について考察した結果，ヒステリシス署名の安全性が，連鎖構造を形成するハッシュ関数の一方向性と，一つの署名生成の事実が他の多くの署名に反映することによる事実否定の困難性に基づいていることが明らかになった．

今後は，本稿で示した評価手法に基づき，ヒステリシス署名関連技術として[1]〜[3]で提案されている「履歴交差」技術の評価や，[5]で指摘されている署名者本人による偽造問題の分析などを行う．

宮崎邦彦，吉浦裕は，通信・放送機構の委託研究「次世代証拠基盤技術に関する研究開発」として研究を行った．

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 Vol32. No.11，共立出版，2000.

[4] 宮崎邦彦，洲崎誠一，吉浦裕，佐々木良一，松木武，“連鎖構造を用いたディジタル署名技術の安全性強化に関する一考察,” 第62回情報処理学会全国大会，2001.

[5] 洲崎誠一，松本勉，“電子署名の偽造に関する一考察,” 情報処理学会コンピュータセキュリティシンポジウム2001（CSS2001），2001.