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

宮崎邦彦[†1,†2] 吉浦裕[†3] 岩村充[†4]
松本勉[†5] 佐々木良一[†6]

従来，電子文書の真正性（本人性）を保証するための技術として，電子署名技術が広く利用されてきた．これは電子署名技術の持つ，秘密鍵を知る者だけが署名を生成できる，という性質を利用したものである．秘密鍵を署名者以外には秘密に保つことにより，結果として電子文書の真正性が保証される．しかし，10〜20 年という長期の利用を考えた場合には，秘密鍵が秘密に保たれている，という条件は妥当であるとは限らない．そのため秘密鍵の秘匿性だけに依存せず第三者機関を用いた長期利用向け電子署名技術として，タイムスタンプ併用方式，ヒステリシス署名方式，署名延長サーバ利用方式など，さまざまな技術が提案されている．本稿では，それぞれの長期利用向け電子署名技術が要求する第三者機関の種類を明らかにする．また同じ種類の第三者機関を要求する場合であっても，第三者機関への依存度合いが異なる場合がある．そこで特に存在保証を行う第三者機関を取り上げ，信頼度という概念を導入することにより，ともに存在保証機関を利用する 2 つの技術，タイムスタンプ併用方式とヒステリシス署名方式の違いを明らかにする．以上により，長期利用向け電子署名技術を，今後の電子社会を支える基本技術として活用するにあたり，社会基盤として求められる第三者機関の役割が明確になると考える．

Evaluation Method for Digital Signature Schemes for Long-term Documents Based on Dependency to Third Parties

Kunihiko Miyazaki,[†1,†2] Hiroshi Yoshiura,[†3]
Mitsuru Iwamura,[†4] Tsutomu Matsumoto[†5]
and Ryoichi Sasaki[†6]

Digital signature is used as a technology which assures authenticity of digital documents. No one can issue a digital signature without a private-key, so if the private-key is kept secret for everyone except the signer, the document signed by him must be his document. However, it might not adequate for long-term usage that only signer knows the private-key. Then some technologies are proposed for long-term usage, that is, time-stamping, hysteresis signature, signature extension server, and so on. In this paper, we notice that each technology requires some third parties implicitly or explicitly. We clarify what kinds of third parties are required by each technology. In addition, we clarify how much each third party, especially existance assure party, is required by introducing the concept of trustworthiness of third party.

†1 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†2 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
†3 電気通信大学電気通信学部
Department of Electro-Communications, The University of Electro-Communications
†4 早稲田大学大学院アジア太平洋研究科
Graduate School of Asia-Pacific Studies, Waseda University
†5 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University
†6 東京電機大学工学部
Faculty of Engineering, Tokyo Denki University

1. はじめに

インターネットの普及にともない，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．

従来，電子署名技術の安全性評価は，攻撃者が署名用秘密鍵を知らないという仮定の下での偽造の困難性評価が主流であった[1)]．現在の電子署名の利用形態では，公開鍵証明書に有効期限を設定したり，公開鍵証

明書失効リストを配布したりすることで，この仮定の妥当性を担保している．しかし，今後，電子署名を，より広い範囲の電子社会を支える技術として活用しようとする場合に，この仮定がつねに妥当であるとは限らない[11]．たとえば，長期にわたる電子文書の利用においては，現在は困難とされている秘密鍵の推定が可能となるような技術革新や，管理者の不備による秘密鍵の漏洩などの運用にともなう人的なエラーが発生しないとも限らない．

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は「暗号ブレイク」と呼ばれ，この問題の重大さと対策の必要性が指摘されている．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が提案されている[2)~4)]．

このような問題への対策技術して知られている技術（以降，長期利用向け電子署名技術と呼ぶ）には，上述のヒステリシス署名のほか，電子公証サービス利用方式[7),13)]，タイムスタンプ併用方式[7)]，署名延長サーバ利用方式[13)]，MAC（Message Authentication Code）による電子証拠物利用方式[12)]，実行ハードウェア確認タグつき署名方式[9)]，などがある．

これらの長期利用向け電子署名技術は，アルゴリズムのみによって安全性が保証されるわけではない．それぞれの技術は，明示的あるいは暗黙のうちにさまざまな第三者機関の存在を仮定したうえで成り立っている．

本稿では，長期利用向け電子署名技術が保証すべき性質を，「時刻 t に生成されたとされる署名が，確かに署名者によって生成されたものであることが，署名検証時 $t'(>t)$ において検証者によって確認可能であること」と定義し，この性質を満たすために必要とされる第三者機関の役割に注目した各技術の比較，評価手法を提案する．

なお，長期利用向け電子署名技術の比較については，偽造の種類による比較[7)]や，暗号技術の危殆化の状態に注目した比較[10)]など，従来からいくつか知られているが，本稿で述べるような，第三者機関の役割に基づく比較は，著者らの知る限り行われていない．

本稿の目的は，第三者機関の役割に注目した長期利用向け電子署名技術の評価手法を提案し，この手法に基づいた比較を行うことにより，これらの技術を電子社会を支える基本技術として活用するために，社会基盤として求められる第三者機関の役割を明らかにすることにある．同時に，これらの技術の利用者に対して，自身の署名の正当性を保証するために，誰に，何を，どの程度依存しているのか，を明らかにすることにある．

本稿では，まず上記の性質を満たすために，各長期利用向け署名技術において必要とされる第三者機関の種類を明らかにする．本稿における第三者機関とは，署名検証者が検証のために必要となる「保証」を提供する存在と位置づけ，第三者機関の種類とは，その機関が「何を」保証するかによって区別されるものとする．したがって，いわゆる認証局や公証局のような特定の業務を行うために設けられた組織以外に，PGP（Pretty Good Privacy）における「他の利用者」なども本稿では第三者機関に含める．また，認証局も，PGP における他の利用者も，公開鍵の所有者を保証する，という意味において，同じ種類の第三者機関に分類する．

次に，各長期利用向け署名技術が，上で明らかにされた各第三者機関に対し，どの程度の信頼性を期待するのかという観点から，より詳細に比較を行う．具体的には，同じ種類の第三者機関を必要とする 2 つの技術，タイムスタンプ併用方式とヒステリシス署名方式を例にあげ，それぞれの技術が，あるデータの存在証明を行う第三者機関（存在保証機関と呼ぶ）に，どの程度依存しているかを比較する．

比較にあたって，本稿では，第三者機関があたえる保証の信頼度という新しい概念を導入する．存在保証機関が与える保証の信頼度と，タイムスタンプ併用方式，ヒステリシス署名方式それぞれによる検証結果の信頼度との相関を調べることにより，各技術の存在保証機関への依存度を明確にする．

なお，ヒステリシス署名方式の場合は，電子署名間に連鎖構造を有するため，検証結果の信頼度をいかに適切に算出するかが課題となる．なぜなら，ある電子署名の有効性に関する保証が，他の電子署名の有効性を保証するためにも利用されるからである．そこで本稿では，ヒステリシス署名が持つ連鎖構造の性質を分析し，ヒステリシス署名検証結果の適切な信頼度算出方法についても提案を行う．これにより結果として，ヒステリシス署名が持つ連鎖構造による利点が明らかとなる．

以下では，2 章において，長期利用向け電子署名技術が満たすべき性質を定義し，この性質を満たすと考えられている技術の概要を述べる．3 章において，各技術において必要となる第三者機関の種類を明確にし分類を行う．4 章において，第三者機関の信頼度とい

う概念を導入する．特に，存在保証機関を取り上げ，存在保証機関を利用する 2 つの技術，タイムスタンプ併用方式とヒステリシス署名方式，について，存在保証機関の信頼度と，検証結果の信頼度の関係について論じる．さらに，連鎖構造を利用した署名技術であるヒステリシス署名技術の検証結果の信頼度算出方法についても提案する．最後に 5 章においてまとめを述べる．

2. 長期利用文書向け電子署名関連技術

本稿で前提とする技術環境は以下のとおりである．

定義 1（前提とする技術環境） 時刻 t に生成されたとされる署名に対応する署名用秘密鍵は，署名検証時 $t'(>t)$ においては，秘密に保たれているとは限らない．

本稿では，上記の技術環境の下で，次で定義される性質を持つ電子署名技術を評価の対象とする．

定義 2（長期利用向け電子署名技術） 時刻 t に生成されたとされる署名が，確かに署名者によって生成されたものであることが，署名検証時 $t'(>t)$ において検証者によって確認可能であること

なお，一般に長期利用向け技術として知られる技術は，下記の 2 つに大別できる．

- 秘密鍵が危殆化することにより新たに偽造可能となる署名を限定する（危殆化した秘密鍵を使って過去に生成された署名の有効性については問わない）．
- 秘密鍵が危殆化する前に生成された署名の有効性を確認できるようにする（事後的に偽造を判別できるようにする）．

本稿では，定義 2 に示したように，後者の方針に基づく技術を評価の対象とし，前者は対象に含めない．

なお，前者の方針に基づく技術としては，Foward-Secure Digital Signature[18] や Key-Insulated Signature Scheme[14),15)] と呼ばれる技術が知られている．これらの技術では，1 つの公開鍵に対応する秘密鍵が複数存在し，その中の 1 つの秘密鍵が漏洩したとしても他の秘密鍵を推定することは困難であるように設計されている．そのため，秘密鍵を頻繁に（たとえば毎日）更新しておくことにより，たとえ，ある 1 つの秘密鍵が漏洩したとしても，他の期間の署名の偽造は防止できる☆．しかし，漏洩した秘密鍵を使って過去に正しく生成された署名の有効性については確認できないため，定義 2 に示した本稿で対象とする長期利用向け電子署名技術とは異なる技術であるといえる．したがって，本稿ではこれ以降取り扱わない．

本稿では，代表的な長期利用向け電子署名技術として以下の 6 つの技術を取り上げる．

(1) **電子公証サービス** 電子文書を誰がいつ作成したかを保証する第三者機関である電子公証システムを利用．長期利用したい文書自体を電子公証システムに預託して利用する．本技術のみ文書作成者側での署名生成を行わない☆☆．

(2) **タイムスタンプ併用** 電子文書がある時刻において存在しており，その時点から改ざんされていないことを保証する第三者機関であるタイムスタンプオーソリティーを利用．長期利用したい文書に対し，署名を付与し，その署名付き文書（あるいはハッシュ値）をタイムスタンプオーソリティーに送りタイムスタンプを付与してもらう☆☆☆．

(3) **署名延長サーバ利用** 公開鍵証明書の有効期間が切れる前に，より有効期間の長い署名を付与しなおす第三者機関である署名延長サーバを利用する．長期利用したい文書に対し，作成時に署名を付与した後，その署名に対応する公開鍵証明書の有効期間が切れる前に，署名延長サーバに再署名を要求する．以降，これを繰り返す．

(4) **ヒステリシス署名** 署名生成記録を履歴として残しておき，署名生成時にはその履歴を反映させることにより，履歴内に連鎖構造を構築する技術．履歴の信頼性向上のために，履歴の一部を定期的に第三者機関などに公開する．長期利用したい文書に対し，その時点における署名履歴を反映させながら，署名する．

(5) **MAC による電子証拠物** あらかじめ耐タンパ性のある署名生成装置内に署名用秘密鍵とは別に，MAC（Message Authentication Code）用の秘密パラメータを格納しておく．長期利用したい文書を作成するときは，署名生成と同時に，当該文

☆ Foward-Secure Digital Signature の場合は，1 つの秘密鍵からそれ以前の秘密鍵を推定することは困難であるが，それ以降の秘密鍵は容易に算出可能であるように設計されている．したがって，漏洩した秘密鍵が使われていたとき以前の署名の偽造は防止できるが，以降の署名の偽造は可能である．

☆☆ 電子公証サービスという言葉はさまざまなサービスを指すことがある．たとえば，タイムスタンプオーソリティーのことを電子公証と呼ぶこともある．ここでは，検証対象の電子文書を「誰が」「いつ」作成したかを第三者機関が保証するサービスを電子公証サービスと呼ぶ．

☆☆☆ タイムスタンプ併用方式で利用可能なタイムスタンプ方式自体には，多くの種類があり，それらの安全性および可用性に基づいた比較も知られている[8)]．また，実際にサービス提供されている例もある[19)~22)]．

書の MAC を生成し，これを署名付き文書の証拠とする．MAC 用秘密パラメータは将来にわたり漏洩しないという条件を仮定する．

(6) **実行ハードウェア確認タグつき署名方式** 署名ごとに，署名生成装置を特定可能する「実行ハードウェア確認タグ」を含める．タグの生成にあたっては，耐クローンモジュール☆を利用しタグの偽造を防止する．長期利用したい文書を作成するときは，署名生成装置の発行者である管理者との間でやりとりを行い「タグ」を生成し，これを署名とともに利用する．このタグは，耐クローンモジュールを利用しないと生成できないように設計されている．

3. 要求される第三者機関の種類

本章では，2 章にあげたそれぞれの長期利用向け電子署名技術が，上記の定義 2 を満たすために要求される条件について考察を行い，各技術の利用にあたり必要となる信頼できる第三者機関の種類を明らかにする．

3.1 第三者機関の定義

本稿における第三者機関は，以下のように定義される．

定義 3（第三者機関） 第三者機関とは，署名検証者が検証のために必要とするなんらかの事実に対する保証を，署名検証時において，提供する存在である．第三者機関の種類とは，その機関が何を保証するかによって，区別される．

注意 1 上記の定義による第三者機関には，下記の 2 つの場合が含まれる．

オンライン検証 署名検証時に第三者機関に問い合わせ可能な場合

オフライン検証 署名検証より以前（たとえば署名生成時）に，第三者機関が保証データを発行しておき，それを署名検証時に検証者側でローカルに確認可能な場合

なお，オフライン検証の場合は，あらかじめ第三者機関と署名検証者の間で，あるきまった手順で保証データが確認された場合には，その保証データは第三者機関によって認められたものとする，ということの合意がとれている必要がある．

注意 2 本稿における第三者機関には，いわゆる信頼できる第三者機関（例：認証局など）のような特定の業務を行うために設けられた組織以外に，PGP における「他の利用者」なども含まれる．また，たとえば，認証局も，PGP における他の利用者も，公開鍵の所有者を保証する，という点では同じであるので，同じ種類の第三者機関として分類される．

3.2 第三者機関の種類

2 章にあげた各長期利用向け電子署名技術を利用するために，必要となると考えられる第三者機関は，以下のとおりである．

文書本人性保証機関

電子文書の本人性を長期にわたり保証する第三者機関．上記の各技術のなかでは，(1) 電子公証サービスのみがこの種類の第三者機関を要求する．他の技術では，文書の本人性は，第三者機関が直接保証するのではなく，電子署名技術によって保証される．

この種類に属する第三者機関としては，法務省の電子公証サービスの中の私署証書の認証などがある．

署名鍵秘匿性（短期）保証機関

署名用秘密鍵の，短期における秘匿性を保証する機関．上記各技術はいずれも，長期における署名用秘密鍵の秘匿性は要求しない．一方，(1) 電子公証サービス以外の各技術では，短期における秘匿性は要求されている．したがって，上記の「性質」を満たすためには，検証時において，署名検証者が，署名用秘密鍵の署名生成時における短期の秘匿性を確認できなければならない．

また，(3) 署名延長サーバ利用は，署名生成時から署名検証時にいたるまで，継続的に再署名を繰り返し行う．したがって，署名者の署名用秘密鍵のみならず，再署名に使われる署名延長サーバの署名用秘密鍵（複数）の短期の秘匿性についても要求される．

この種類に属する第三者機関としては，署名装置（ハードウェア，ソフトウェア）の認定機関などが考えられる．しかし，このような認定機関であっても，署名生成時から長期経過後の署名検証時において，過去の時点における秘密鍵の秘匿性を保証することは，困難であろう．実際には，法律のサポートなどにより，「特に疑わしい状況がなければ，署名生成時から短期の間（たとえば公開鍵証明書の有効期間内）においては，秘密鍵は秘密に保たれていたと見なす」ことにな

☆ 耐クローンモジュールは「出力値がランダムであり，モジュールの入出力関係を表すテーブルを作成するにはモジュールに実際に入力を与えて出力を観察するという方法しか存在せず，そのためには莫大な時間と記憶領域を必要とする」という性質を持つ．なお現在のところ，実際に利用可能な耐クローンモジュールは存在していないが，実現方法や安全性評価方法などに関する研究はさかんに行われている[16),17)]．本稿では，将来的に利用可能となると考えられる重要な技術の 1 つとして，評価の対象に含めた．

ると考えられる☆.

署名鍵本人性保証機関

署名用秘密鍵の所有者を長期にわたり保証する機関.(1)電子公証サービス以外の各技術はいずれも，署名用秘密鍵の所有者がだれであるかを特定し確認できる必要がある．ただし，(5) MAC による電子証拠物，(6)実行ハードウェア確認タグつき署名方式については，署名用秘密鍵以外の秘密情報を利用しているため，このデータの所有者を特定，確認できれば，署名用秘密鍵の所有者を確認できなくてもよい.

この種類に属する第三者機関としては，秘密鍵に対応する公開鍵の所有者を特定する公開鍵証明書の発行機関である認証局や，PGP の場合における公開鍵データの公開用の Web サイトなどが考えられる．ただし，現状，これらの第三者機関の役割は，第三者機関への問合せ時点における署名用秘密鍵の所有者を保証することが主流であり，過去（署名生成時）における所有者を保証することは，あまり考えられていない.

署名技術保証機関

ベースとなる電子署名技術の安全性を保証する機関.(1)電子公証サービス以外の各技術はいずれも電子署名技術をベースに構成されている．したがって，少なくとも署名生成時においては，ベースとした署名技術が信頼できた（i.e.：すくなくとも署名生成時においては，署名用秘密鍵を知らない攻撃者は署名を偽造することができなかった）ことが署名検証時において確認できなければならない.

この種類に属する第三者機関としては，暗号技術評価事業（CRYPTREC）のような暗号評価機関が考えられる．ただし，署名検証時に，過去のある時点においてどの署名技術が信頼できたのか，を検証者が確認できるためには，暗号評価機関が継続的に評価事業を行い，その結果を公表することが望ましい.

存在保証機関

署名つき電子文書などの電子データの存在を保証する機関．上記各技術のうち，(2)タイムスタンプ併用，(4)ヒステリシス署名では，署名データが署名生成時に存在したことが，署名検証時において確認される必要がある.

この種類に属する第三者機関としては，タイムスタンプオーソリティーなどがあげられる．また，このほかにも，署名データを新聞などの刊行物に公開する，取引相手である他の利用者が所有している，などの方法によっても存在証明を行うことが可能である．したがって，新聞社，他の利用者などもこの意味の第三者機関となりうる．ただし，タイムスタンプオーソリティーと他の利用者を同列に扱うことは，信頼性の観点からは，適切とはいえない．この点については，次章において，第三者機関の信頼度という概念を導入し，より詳しく述べる.

秘密情報秘匿性（長期）保証機関

署名用秘密鍵以外のなんらかの秘密情報の長期にわたる秘匿性を保証する機関．上記各技術のうち，署名用秘密鍵とは異なる，なんらかの秘密情報の長期にわたる秘匿性を仮定するのは，(5) MAC による電子証拠物，(6)実行ハードウェア確認タグつき署名方式である.

(5) MAC による電子証拠物の場合は，MAC 生成用の秘密鍵が，長期にわたり秘匿性が保たれていることを仮定している．文献 12) で提案されている方式では，耐タンパ性のある署名装置を利用することで，これらの条件を満たすようにしている．この場合は，MAC 生成用秘密鍵に関するこれらの条件を保証する第三者機関としては，署名装置の認定機関などが相当すると考えられる.

(6)実行ハードウェア確認タグつき署名方式の場合は，単一の秘密情報を利用するのではなく，耐クローンモジュールを利用している．ただし，署名生成・検証時に実際に利用するのは，ハードウェアの発行者である管理者が保管するテーブルに含まれるデータのみである（このテーブルは，管理者がハードウェア発行時にあらかじめ，耐クローンモジュールにいくつかの入力を与え，その出力を保管しておくものである）．したがって，このテーブルデータが，長期の秘匿性が要求されるデータとなる.

この種類に属する第三者機関としては，署名用秘密鍵の秘匿性の場合と同様，署名装置（ハードウェア，ソフトウェア）の認定機関などが考えられる．ただし，(5) MAC による電子証拠物，(6)実行ハードウェア確認タグつき署名方式で利用される秘密情報は，長期にわたり秘匿性が保たれていなければならず，また，その事実を署名検証時点において確認できなければならないことに注意を要する.

秘密情報本人性保証機関

署名用秘密鍵以外のなんらかの秘密情報の所有者を保証する機関．上記と同様，署名用秘密鍵以外の秘密情報の所有者の確認可能性を仮定するのは，(5) MAC

☆ (3)署名延長サーバ利用の場合には，署名延長サーバが用いる（複数の）署名用秘密鍵についても同様に，この見なし事項を適用するものと考えられる．したがって，署名用秘密鍵の秘匿性に関する条件については，署名延長サーバは，他の技術よりも強い仮定をおいているといえる.

表 1 各長期利用向け電子署名技術が要求する第三者機関の種類
Table 1 Required third parties for each digital signature scheme for long-term documents.

要求される第三者機関の種類	通常署名	(1)	(2)	(3)	(4)	(5)	(6)	対応すると考えられる第三者機関の例
文書本人性保証		○						法務省「電子公証制度」など
署名鍵秘匿性（短期）保証	○		○	◎	○	○	○	装置認定機関，法律のサポートに基づく仮定など
署名鍵本人性保証	○		○	○	○	△	△	(過去の証明書の有効性も確認可能な) 認証局など
署名技術保証	○		○	○	○	○	○	CRYPTREC などの暗号技術評価機関など
存在保証			○		○		△	タイムスタンプオーソリティー，新聞発表など
秘密情報秘匿性（長期）保証						○	△	装置認定機関など
秘密情報本人性保証						○	△	装置認定機関など
利用する第三者機関による分類	—	A	B	D	B	C	C	

○：要求される ◎：強く要求される △：他の種類の第三者機関で代替可

による電子証拠物，(6) 実行ハードウェア確認タグつき署名方式である．

この種類に属する第三者機関としては，署名装置（ハードウェア，ソフトウェア）の認定機関が，秘密情報の秘匿性に加え，本人性も保証する場合が考えられる．なお，署名用秘密鍵の場合と異なり，(5) MAC による電子証拠物，(6) 実行ハードウェア確認タグつき署名方式などで利用される秘密情報には，対となる公開情報（公開鍵に相当するもの）が存在しないため，一般的な認証局のような方式は利用できないことに注意を要する．

3.3 要求される第三者機関の種類による分類

以上に示した各種第三者機関のうち，署名用秘密鍵秘匿性（短期）保証機関，署名用秘密鍵本人性保証機関，署名技術保証機関，については，従来の電子署名技術の場合においても同様に必要とされる．文書本人性保証機関，存在保証機関，秘密情報秘匿性（長期）保証機関，秘密情報本人性保証機関は，長期利用向け電子署名技術に特有の第三者機関である．

これらの要求される第三者機関の種類に注目すると，長期利用文書対応各技術は，次の 4 通りに大別できる．

Type A 長期の本人性を第三者機関によって保証 ··· (1) 電子公証サービス

Type B 短期の本人性は電子署名技術によって保証．存在証明を第三者機関が行うことにより全体として長期の本人性も保証 ··· (2) タイムスタンプ併用，(4) ヒステリシス署名

Type C 短期の本人性は電子署名技術によって保証．長期の本人性は特別な秘密情報によって保証 ··· (5) MAC による電子証拠物，(6) 実行ハードウェア確認タグつき署名方式☆

Type D 短期の本人性は電子署名技術によって保証．長期にわたり継続的に保証しなおし続けることにより，長期の本人性も保証 ··· (3) 署名延長サーバ利用

Type A は，電子文書の本人性自体を第三者機関に依存させる方法である．法務省によって創設された「公証制度に基礎を置く電子公証制度」に基づくサービスのうち，「私署証書の認証」を行う場合などに相当する．

Type B，C，D はいずれも電子署名技術をベースとしているが，長期利用のために要求される条件が異なる．

Type B は，短期の本人性を電子署名技術によって保証したうえで，その署名つき電子文書の存在証明を第三者機関が保証することにより，全体として長期の本人性を保証している．

Type C は，短期の本人性は電子署名技術によって保証し，長期の本人性は，署名用秘密鍵とは別の秘密情報によって保証している．すなわち，長期にわたり，秘密情報が署名者のものであり，他の利用者からは秘匿され続けていることを保証する第三者機関を利用して，長期の本人性を保証している．

Type D は，短期の本人性を電子署名技術によって保証し，それを署名延長サーバが継続的に再署名を繰り返し，長期の本人性を保証するものである．

以上のように，長期利用向け電子署名技術を，利用するために要求される第三者機関の種類が明らかとなった（**表 1**）．

4. 第三者機関の信頼度に基づく評価手法

前章までで，長期利用向け電子署名技術を利用するために，それぞれ必要となる第三者機関の種類が明らかとなった．

ところで，従来，情報セキュリティ技術の評価においては，第三者機関は「信頼できる/できない」のいずれかであるとの仮定のうえで，全体の安全性が論じ

☆ (6) 実行ハードウェア確認タグつき署名方式については，特別な秘密情報が漏洩した場合にも対応可能な改良案も提案されている[9] が，この場合は，かわりに存在証明を第三者機関によっている．

られることが多かった．しかし，長期の利用を考えると，過去において信頼できた第三者機関であっても，将来にわたってその信頼性を保ち続けられるとは限らない．また一方で，たとえば，一連の取引の過程において関係があった他の利用者のように，信用性は高いとはいえないが，ある程度の有用性を持つ第三者機関もある．

したがって，長期利用向け電子署名技術の評価においても，各技術がそれぞれ必要とする第三者機関に対し，どの程度の信頼性を期待しているのか，を明らかにすることが望まれる．この点を明らかにすることにより，前章で同じ Type に分類された技術であっても（i.e.：同じ種類の第三者機関を必要とする技術であっても），その第三者機関に期待する信頼性，すなわち，どの程度その第三者機関に依存しているのか，については異なる可能性がある．

そこで本稿では，第三者機関の信頼度という新しい概念を導入し，「信頼できる/できない」の二値的な判断だけではなく，中間的な状態を適切に表現し，それが全体の安全性にどのようなかかわるかを考察する．

具体的には，前章で同じ Type B に分類された 2 つの技術，(2) タイムスタンプ併用方式と (4) ヒステリシス署名方式を取り上げ，それぞれが存在保証機関にどの程度依存しているかを，存在保証機関の信頼度に基づき評価し，2 つの技術の性質の違いを明らかにする．

4.1 存在保証機関の信頼度と検証結果の信頼度

本節では，存在保証機関が「信頼できる」とはどういうことであるか考察し，その考察に基づいて信頼度という指標を定義する．

存在保証機関とは，電子データの存在を保証する機関，つまり，あるデータ（署名つきメッセージなど）が存在したかどうかの問合せに対し，「存在した/しなかった」を回答する機関である．存在保証機関が信頼できるとは，この回答が信頼できることを意味する．

すなわち，当該データが本当に存在したときには「存在した」と回答され，当該データが存在しなかったときには「存在しなかった」と回答される場合に，その存在保証機関は信頼できるといえ，逆に，当該データが存在していたにもかかわらず「存在しなかった」と回答されたり，当該データが存在しなかったにもかかわらず「存在した」と回答されたりする場合には，その存在保証機関は信頼できない，といえる．

そこで本稿では，存在保証機関の信頼度を，存在保証機関からの回答が正しい回答である確率をもって定義する．より正確には，存在保証機関の信頼度と，検証結果の信頼度を以下のように定義する．

定義 4（存在保証機関の信頼度） 存在保証機関の与える保証の信頼度とは，あるデータ R に対し存在保証機関が与える保証の確からしさを表す値 $f_{\mathrm{ind\_rely}}(R) = (p_{\mathrm{ind}}(R), q_{\mathrm{ind}}(R), t_{\mathrm{ind}}(R))$ のことである．特に誤解の恐れがないときには，これを単に存在保証機関の信頼度と呼ぶ．ここで，$p_{\mathrm{ind}}(R)$，$q_{\mathrm{ind}}(R)$，$t_{\mathrm{ind}}(R)$ は，保証対象データ R ごとに以下で定義される．なお，以下で「R が存在した」とは，署名者の署名生成時に存在保証機関が R を入手し，存在保証機関のもとに存在していたことを意味する．署名検証時において，存在保証機関のもとに存在しているかどうかは問わない（存在保証機関の保証方法に依存する）．

- $p_{\mathrm{ind}}(R)$ R が存在していたとされる時刻において，本当に存在していたとき，当該存在保証機関によって「存在した」と判定される確率
- $q_{\mathrm{ind}}(R)$ R が存在していたとされる時刻において，本当は存在していなかったとき，当該存在保証機関によって「存在した」と判定される確率
- $t_{\mathrm{ind}}(R)$ 当該存在保証機関による R の判定結果（R が「存在した」と判定されたとき $t_{\mathrm{ind}}(R) = 1$，R が「存在しなかった」と判定されたとき $t_{\mathrm{ind}}(R) = 0$）

注意 3 $p_{\mathrm{ind}}(R)$ が大きいほど，また，$q_{\mathrm{ind}}(R)$ が小さいほど，その保証を与える存在保証機関は，より信頼できるといえる．以下では，$0 \leq q_{\mathrm{ind}}(R) \leq 1/2 \leq p_{\mathrm{ind}}(R) \leq 1$ を仮定する．また，判断材料がないなどの理由により，判定ができない場合には，第三者機関が与える保証の信頼度は，$f_{\mathrm{ind\_rely}}(R) = (1/2, 1/2, 1)$ と設定するものとする．なお，$t_{\mathrm{ind}}(R)$ は便宜上 1（「存在した」）と設定している．

注意 4 上記の定義から，R が存在していたとされる時刻において，本当に存在していたとき，当該存在保証機関によって「存在しなかった」と判定される確率は $1 - p_{\mathrm{ind}}(R)$ と，また，R が存在していたとされる時刻において，本当に存在しなかったとき，当該存在保証機関によって「存在しなかった」と判定される確率は $1 - q_{\mathrm{ind}}(R)$ と表される．

定義 5（検証結果の信頼度） 署名つきメッセージ R の検証結果の信頼度とは，検証者が，存在保証機関が与えた保証に基づいて，署名つきメッセージ R を判定した結果「確かに署名者によって生成された署名である」と判定したときに，それが真に正しい結果である確率 $f_{\mathrm{rely}}(R)$ のことである．

以下，(2) タイムスタンプ併用，(4) ヒステリシ

ス署名それぞれについて，存在保証機関の信頼度 $f_{\mathrm{ind\_rely}}(R)$ から検証結果の信頼度 $f_{\mathrm{rely}}(R)$ を算出する方法について述べる．これにより，検証結果の信頼度に与える，存在保証機関の信頼度の影響が明らかとなり，各技術の存在保証機関に対する依存度を評価可能となる．

4.2 タイムスタンプ併用方式

4.2.1 検 証 方 法

タイムスタンプ併用方式では，署名生成時に，署名つきメッセージ（またはそのハッシュ値）をタイムスタンプオーソリティーに送り，タイムスタンプを付与してもらう．このタイムスタンプを利用した長期経過後の検証手続きの概要は，以下のとおりである．

(1) 通常の電子署名の検証手順に従って,（署名生成時における）署名の有効性を検証する．
(2) タイムスタンプの有効性を確認する☆．

この検証手続きのうち，存在保証機関（この場合はタイムスタンプオーソリティー）が与える保証に相当するのは，(2) の有効性の判定結果である．

4.2.2 検証結果の信頼度

本項では，タイムスタンプ併用方式の検証結果の信頼度算出方法について述べる．

今，署名つきメッセージ R に対する (2) の有効性確認結果が「存在した」であり，存在保証機関の信頼度が $f_{\mathrm{ind\_rely}}(R) = (p_{\mathrm{ind}}(R), q_{\mathrm{ind}}(R), 1)$ であったとする．

このとき，長期経過後の検証手続きによる検証結果の信頼度，すなわち,「署名つきメッセージ R が確かに署名者によって生成されたものである」という判定結果が正しい結果である確率 $f_{\mathrm{rely}}(R)$ を算出するためには,「存在保証機関が R の存在を確認したという条件下における，署名つきメッセージ R が真に存在していたことの条件付確率」を求めればよい．したがって，

$$f_{\mathrm{rely}}(R) = \frac{p_{\mathrm{ind}}(R)}{p_{\mathrm{ind}}(R) + q_{\mathrm{ind}}(R)} = \frac{1}{1 + (q_{\mathrm{ind}}(R)/p_{\mathrm{ind}}(R))}$$

と表すことができる．

4.3 ヒステリシス署名方式

4.3.1 検 証 方 法

ヒステリシス署名方式では，署名生成時に，署名生成記録を署名履歴として保管しておき，次の文書に対し署名生成をするときには，その署名生成記録のハッシュ値を含めて署名生成を行う．これにより，署名履歴に残された署名生成記録間には，ハッシュ関数を利用した連鎖構造が形成されることになる．

この連鎖構造を有する署名履歴を利用した長期経過後の検証手続きの概要は，以下のとおりである（詳細は第 A.1 節参照）．

(1) 通常の電子署名の検証手順に従って,（署名生成時における）署名の有効性を検証する．
(2) 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 R_m が存在することを確認する．
(3) 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を確認する．
(4) 署名履歴中に含まれる署名生成記録 $R_m, R_{m+1}, \ldots, R_k$ が確かに存在していたことを確認する．

この検証手続きのうち，存在保証機関が与える保証に相当するのは，(4) の存在確認結果である．

ここで注意すべき点は，タイムスタンプ併用方式の場合は，1 つの署名検証のために利用される存在保証機関からの保証は，1 つだけであったのに対し，ヒステリシス署名方式では，署名履歴中に含まれる署名生成記録の個数の（一般には複数の）保証が利用されている点である．したがって，ヒステリシス署名方式に基づく検証結果の信頼度は，複数の存在保証機関の信頼度を適切に反映したものでなければならず，タイムスタンプ併用方式の場合とは異なったものとなる．

本稿では，ヒステリシス署名方式に基づく検証結果の信頼度を算出するにあたり，この点を適切に反映するために，次のような方針に従って算出することとした．

検証結果の信頼度は，検証対象となる署名に対応する署名生成記録 R_m の信頼度と，他の署名生成記録 $R_{m+1}, \ldots, R_k$ の信頼度とから算出されると考えられる．すなわち,「検証対象の署名（R_m に対応）は確かに署名者によって生成された署名である」が正しい検証結果であることの確率は，R_m の信頼度が存在保証機関から与えられる以前に，まず他の署名生成記録 $R_{m+1}, \ldots, R_k$ の信頼度から事前確率として求められる．この事前確率のもとで，さらに存在保証機関から R_m の信頼度 $f_{\mathrm{ind\_rely}}(R_m)$ が与えられたときに,「検証対象の署名（R_m に対応）は確かに署名者によって生成された署名である」が正しい検証結果であることの事後確率を算出すれば，最終的な検証結果の信頼度 $f_{\mathrm{rely}}(R_m)$ が求められる☆☆．

☆ 有効性の確認方法はオンライン検証方式，オフライン方式など，タイムスタンプ方式ごとに異なる．

☆☆ タイムスタンプ併用方式の場合の検証結果の信頼度は，事前確率を 1/2 と仮定した場合に相当する．

この検証結果の信頼度の算出方法については，次項でより詳細に述べる．

4.3.2 検証結果の信頼度

本項では，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，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，連鎖構造を有する 2 つの署名生成記録間の信頼度の関係をを明らかにする．次に，前項に述べた方針に従い，信頼度算出手法を具体的に提案する．

定義 6（検証結果の信頼度の事前確率と事後確率） 署名生成記録 $R_m, R_{m+1}, \ldots, R_k$ を使った署名検証結果「検証対象の署名（R_m に対応）は確かに署名者によって生成された署名である」の信頼度の**事前確率**とは，R_m の信頼度が存在保証機関から与えられる以前に，他の署名生成記録 $R_{m+1}, \ldots, R_k$ の信頼度をもとに算出される，上記の署名検証結果が正しい判定結果である確率のことである．以下これを単に，R_m に関する事前確率と呼び，$f_{\mathrm{pri}}(R_m)$ で表す☆．また，事前確率 $f_{\mathrm{pri}}(R_m)$ のもとで，さらに存在保証機関から R_m に対する信頼度 $f_{\mathrm{ind\_rely}}(R_m)$ が与えられたとき，上記の署名検証結果が正しい判定結果であることの**事後確率**を，R_m に関する事後確率と呼び，$f_{\mathrm{post}}(R_m)$ で表す．これが最終的な検証結果の信頼度 $f_{\mathrm{rely}}(R_m)$ となる．

なお，以下の議論では，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．

4.3.2.1 連鎖構造に関する考察

本目では，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，2 つの署名生成記録 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 1 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，すなわち過去の署名生成時点に確かに存在した署名生成記録であれば，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，R_i と R_{i+1} が連鎖している場合には，R_i に関する事前確率 $f_{\mathrm{pri}}(R_i)$ と，R_{i+1} に関する事後確率 $f_{\mathrm{post}}(R_{i+1})$ との間に，$f_{\mathrm{pri}}(R_i) \geq f_{\mathrm{post}}(R_{i+1})$ という関係が成り立つといえる．以下で述べるヒステリシス署名検証結果の信頼度算出にあたっては，この関係式を利用する．

4.3.2.2 ヒステリシス署名検証結果の信頼度算出方法

本目では，前目の考察をふまえ，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．

今，2 つの署名生成記録 R_i と R_{i+1} が連鎖しているとし，それぞれ存在保証機関によってある信頼度で「存在した」と判定されたとする．すなわち，$f_{\mathrm{ind\_rely}}(R_j) = (p_{\mathrm{ind}}(R_j), q_{\mathrm{ind}}(R_j), 1) \quad (j = i, i+1)$ であったとする．このとき，R_{i+1} に関する事後確率は，$f_{\mathrm{post}}(R_{i+1}) = p_{\mathrm{ind}}(R_{i+1})/(p_{\mathrm{ind}}(R_{i+1}) + q_{\mathrm{ind}}(R_{i+1}))$ となる☆☆．

一方，R_i に対して与えられた信頼度 $f_{\mathrm{ind\_rely}}(R_i)$ も考慮したときの R_i が実際に署名生成時において存在していた確率，すなわち R_i に関する事後確率を考える．R_{i+1} に関する事後確率は分かっている．また，R_i は R_{i+1} と連鎖しているから，4.3.2.1 目での考察結果より，R_i に関する事前確率 $f_{\mathrm{pri}}(R_i)$ は，$f_{\mathrm{pri}}(R_i) \geq f_{\mathrm{post}}(R_{i+1})$ を満たす．したがって，R_i に関する事後確率 $f_{\mathrm{post}}(R_i)$ は，

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

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，それぞれに対する存在保証機関による信頼度を $f_{\mathrm{ind\_rely}}(R_i)$ $(m \leq i \leq k)$ としたとき，R_m に関

☆ より厳密には，どの範囲の署名生成記録を利用したかを明記すべきであるが，文脈から明らかなので省略する．

☆☆ この場合 R_{i+1} よりあとの署名生成記録は検証時に利用していないので，R_{i+1} に関する事前確率を 1/2 として計算している．

する事後確率 $f_{\mathrm{post}}(R_m)$ は，

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

を満たす．ただし，

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

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

とする．

（証明）上の議論を繰り返し適用すればよい．

注意 5 命題 1 により，存在証明機関によって与えられた保証の信頼度から，検証結果の信頼度，すなわち，「署名つきメッセージが確かに署名者によって生成されたものである」という判定結果が正しい結果である確率，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，簡単のため，命題 1 の右辺の値をヒステリシス署名の検証結果の信頼度 $f_{\mathrm{rely}}(R_m)$ とする．

注意 6 命題 1 において，

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

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

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

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「存在した」と判断されれば，検証結果の信頼度は高くなるし，「存在しない」と判断されれば，検証結果の信頼度は低くなる．また $p_{\mathrm{ind}}(R_i) = q_{\mathrm{ind}}(R_i) = 1/2$ のときは，$t_{\mathrm{ind}}(R_i)$ によらず検証結果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，ヒステリシス署名検証結果の信頼度に影響を及ぼさない．

これらの性質は，本目に示したヒステリシス署名検証結果の信頼度算出方法の妥当性を支持するものであると考えられる．

4.4 存在保証機関の信頼度に基づく比較

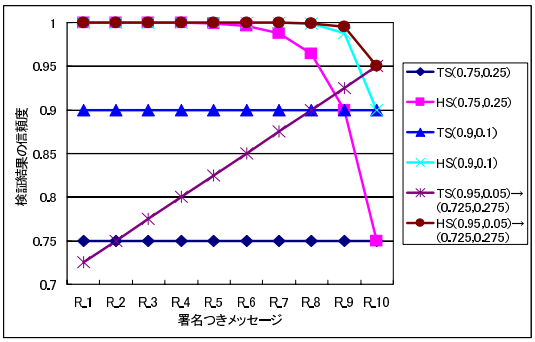
以上の議論により，タイムスタンプ併用方式とヒステリシス署名方式の存在保証機関への依存度が明らかになった（**表 2**）．これらを比較すると，たとえ同じ第三者機関を要求する技術であっても，その依存度は技術ごとに異なる可能性があることが分かる．

表 2 存在保証機関の信頼度に基づくタイムスタンプ併用方式とヒステリシス署名方式の比較

Table 2 Comparison between a digital signature with a time-stamping and a hysteresis signature in terms of the trustworthiness of existance assure parties.

	検証結果の信頼度 $f_{\mathrm{rely}}(R_j)$ $(m \leq j \leq k)$
タイムスタンプ併用	$\frac{P_{\mathrm{ind}}(R_j)}{P_{\mathrm{ind}}(R_j)+Q_{\mathrm{ind}}(R_j)}$
ヒステリシス署名	$\frac{\prod_{i=j}^{k} P_{\mathrm{ind}}(R_i)}{\prod_{i=j}^{k} P_{\mathrm{ind}}(R_i)+\prod_{i=j}^{k} Q_{\mathrm{ind}}(R_i)}$

署名生成履歴 $R_m, R_{m+1}, \ldots, R_k$ を用いて検証を行ったときに「R_j に対応する署名が署名者によって生成された署名である」が正しい検証結果である確率．



TS：タイムスタンプ併用方式，HS：ヒステリシス署名方式

図 1 タイムスタンプ併用方式とヒステリシス署名方式の検証結果の信頼度

Fig. 1 Trustworthiness of a digital signature with a time-stamping and a hysteresis signature.

ヒステリシス署名検証結果の信頼度は，検証対象となる署名に関する署名生成記録のみが存在保証機関によって保証されていた場合には（i.e.：表 2 で $k = j$ の場合には），ちょうどタイムスタンプ併用方式の場合と一致する．しかし，その他の署名生成記録についても存在保証機関によって保証が得られる場合（たとえば署名を生成するたびに毎回第三者機関を利用していた場合）には，一般には，タイムスタンプ併用方式よりも検証結果の信頼度は高くなる．

いいかえると，ヒステリシス署名の場合は，タイムスタンプ併用方式の場合よりも，比較的信頼度の低い存在保証機関を利用した場合であっても，検証結果の信頼度は同程度になる可能性がある．

図 1 は，存在保証機関の信頼度が，$(0.9, 0.1, 1)$ の場合，$(0.75, 0.25, 1)$ の場合，および古いデータになるに従って $(0.95, 0.05, 1)$ から $(0.725, 0.275, 1)$ へ徐々に下がっていく場合（過去のデータの信頼度が曖昧になっていく場合）について，タイムスタンプ併用方式と，ヒステリシス署名方式で得られる検証結果の信頼

度を比較した図である．

たとえば，ヒステリシス署名の場合，存在保証機関の信頼度が $(0.75, 0.25, 1)$ であるときの R_9 に関する検証結果の信頼度は $f_{\mathrm{rely}}(R_9) = 0.9$ となるが☆，タイムスタンプ併用方式の場合，検証結果の信頼度は $f_{\mathrm{rely}}(R_i) = 0.75$ となる．タイムスタンプ併用方式で，検証結果の信頼度が 0.9 となるためには，存在保証機関の信頼度はもっと高くなければならない．たとえば，存在保証機関の信頼度が $(0.9, 0.1, 1)$ であれば，検証結果の信頼度が 0.9 となる．

また，ヒステリシス署名の場合，より古い署名ほど信頼度が高まることが分かる．特に，存在保証機関の信頼度が古いデータになるに従って $(0.95, 0.05, 1)$ から $(0.725, 0.275, 1)$ に下がっていく場合，タイムスタンプ併用方式では，検証結果の信頼度もそれに応じて下がるが，ヒステリシス署名では，この場合であっても信頼度が向上していることは注目に値する．これはヒステリシス署名がハッシュ関数による連鎖構造を持つため，古い署名つきメッセージほど，多くの存在保証機関から保証を得ることができるからである．

なお，署名生成記録の中に,「存在しない」と判断される記録が多く含まれている場合には，ヒステリシス署名方式の検証結果の信頼度がタイムスタンプ併用方式の場合よりも低くなることもありうる．ただし,「存在しない」と判断されるということは,「存在したかどうか分からない」と判断されることとは異なることに注意を要する（「存在しない」という判断は，たとえば，ある署名記録が存在したとされる場所に，実は別の署名生成記録が存在していた場合などになされる）．

以上に示した存在保証機関の例にみられるとおり，同じ第三者機関を要求する技術であっても，その依存度合いは，異なったものになる可能性がある．したがって，利用者から見れば，最終的に検証結果に対して要求される信頼度にあわせ，適切な第三者機関を利用することが重要であるといえる．

4.5 提案指標の他技術への適用

本稿では，第三者機関がどの程度信頼できるか，を表現するために，信頼度という指標を導入することにより,「信頼できる/できない」の二値的な基準では表現できなかった中間的な状態を表すことが可能となった．さらに，この指標を存在保証機関に適用することにより，ともに存在保証機関を利用する 2 つの技術，タイムスタンプ併用方式とヒステリシス署名方式の，存在保証機関への依存度の差を明らかにした．本節では，この信頼度指標の，他技術への適用可能性について述べる．

存在保証機関の場合と同様にして，3 章に述べた他の種類の第三者機関に対しても,「保証する性質が実際に真であったときに『真である』と判定する確率 p」と「保証する性質が実際は偽であったときに『真である』と判定する確率 q」の組によって，信頼度を定義することは可能である．

たとえば，3 章で Type A に分類した電子公証サービスが利用する第三者機関「文書本人性保証機関」の場合であれば,「保証対象文書が実際に文書作成者が作成した文書であったときに『文書作成者が作成したものである』と判定する確率 p」と,「実際には文書作成者が作成した文書でなかったときに『文書作成者が作成したものである』と判定する確率 q」によって定義される．

ただし，この信頼度指標を用いて，個々の長期利用向け電子署名技術の評価を行うためには，さらに，それぞれの技術の特性を考察したうえで，第三者機関の信頼度が，検証結果の信頼度にどのように影響するかを調べる必要がある．

ヒステリシス署名の場合は，1 つの署名の検証に利用される存在保証が，複数の存在保証機関から与えられているため，ハッシュ関数による連鎖構造の持つ性質を分析する必要があった．この分析の結果，複数の保証の信頼度から検証結果の信頼度を算出する式が明らかになった．

また，電子公証サービスの場合は，検証結果が，1 つの文書本人性保証機関から与えられる保証のみに基づいている．そのため，検証結果の信頼度を算出するためには，文書本人性保証機関から「文書作成者が作成したものである」との判定結果を得たときにおける，実際に文書作成者が作成した文書である条件つき確率を求めればよい．したがって，電子公証サービスの検証結果の信頼度は $p/(p+q)$ となる．

このように，第三者機関に対して信頼度指標を適用し，個々の長期利用向け電子署名技術の特性を考察することにより，各技術の，第三者機関への依存度の観点からの評価が可能となる．この方針に基づいて，本稿にあげた他の長期利用向け電子署名技術の評価を行うことについては今後の課題である．

このほか提案指標が適用可能な技術としては，タイムスタンプ技術があげられる．本稿では，タイムスタンプ技術は，長期利用向け電子署名技術で利用される一要素技術として取り扱っていた．しかし，タイムスタンプ技術自体にも，連鎖構造を持つものや持たない

☆ R_{10} に関する検証結果の信頼度は $f_{\mathrm{rely}}(R_{10}) = 0.75$ である．

ものなど，いろいろな方法が提案されており，それらの評価，比較をするうえで，提案指標は有用であると考えられる．

たとえば，文献 19) や文献 22) のサービスでは，ヒステリシス署名と同様に，ハッシュ関数を利用した連鎖構造を導入し，一部の情報を第三者機関に保証してもらうことにより，信頼度の向上を図っている．したがって，ヒステリシス署名の場合と同様の評価が可能であると考えられる．

より詳しく述べると，これらのサービスでは，多数の利用者から送られてきたタイムスタンプ対象データのハッシュ値を，ハッシュ関数を用いて二分木状に連鎖させ，super hash value（SHV）と呼ばれるデータを生成する．さらにこの SHV を，1 週間に一度，新聞紙上に広告掲載することによって，サービス提供者の不正を防止している．つまり，SHV の値を新聞によって保証している．

タイムスタンプ検証時に，検証者が，検証対象のタイムスタンプデータから新聞公開された SHV の値までの一連の連鎖を入手可能であるとすれば☆，新聞を第三者機関（存在保証機関）と見なし☆☆，信頼度指標を適用することができる．連鎖の構造はヒステリシス署名の場合とは異なり二分木状に形成されているが，ある 1 つの保証対象データから，一方向性を持つハッシュ関数によって計算された情報が，新聞（存在保証機関）に継続的に何回も掲載されることになるため，検証結果の信頼度については，ヒステリシス署名の場合と同様に，過去のタイムスタンプほど高くなるという結果が得られる．これは，ハッシュ関数による連鎖構造が，タイムスタンプ技術の信頼度向上にも貢献しうることを示している．

5. ま と め

本稿では，長期利用向け電子署名技術の評価手法として，それらの技術が利用する第三者機関に注目した手法を提案し，各技術の比較・評価を行った．

具体的には，まず，第三者機関の種類，すなわち何を保証する第三者機関が要求されるか，という点を明らかにした．

さらに，同じ種類の第三者機関を要求する技術であっても，第三者機関への依存度が異なる可能性があることに注目し，ともに存在保証機関を利用する 2 つの技術，タイムスタンプ併用方式とヒステリシス署名方式を取り上げ，存在保証機関の信頼度，がそれぞれの技術によって得られる最終的な検証結果に与える影響を明らかにした．

また，存在保証機関の信頼度と検証結果の信頼度との相関を調べるあたっては，ヒステリシス署名が署名生成記録間に連鎖構造を有する点に着目し，この点を適切に評価する検証結果の信頼度算出方法を提案した．これにより，タイムスタンプ併用方式と比較して，最終的な検証結果の信頼度がより高くなる可能性を示した．

以上により，長期利用向け電子署名技術を，今後の電子社会を支える基本技術として利用するにあたり，社会基盤として求められる第三者機関の役割が明確になったと考える．

謝辞 宮崎邦彦は，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．宮崎邦彦は，東京大学大学院情報理工学系研究科における指導教授としてご指導賜った今井秀樹教授に，つつしんで感謝の意を表する．本研究自体の方向性に対して数々のご助言を賜るとともに，具体的な方式などに関し，活発にご議論いただいた（株）日立製作所の豊島久，松木武，宝木和夫，手塚悟，洲崎誠一，大本周広，伊藤信治，谷本幸一の各氏に，つつしんで感謝の意を表する．また，本稿の修正にあたり数々の有益なご助言を賜った査読者の方々に，あわせて感謝の意を表する．

参 考 文 献

1) 岡本龍明, 山本博資：現代暗号, 産業図書 (1997).
2) 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).
3) 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).
4) 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).
5) 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

☆ 現在，実際に提供されているサービス形態では，この一連の連鎖を検証者が入手可能であるかどうかは不明である（タイムスタンプデータの実証をセンタが行うサービスが提供されている）．

☆☆ 新聞自体はもともと存在保証をすることが目的のサービスではないが，情報を紙という物理的な媒体に印刷し大量に発行するため，そこに掲載された事実をあとから覆すことは容易ではない．そのため，結果的に存在保証機関としての機能を果たすことになる．

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).
6) 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).
7) 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).
8) 宇根正志，松本 勉：可用性および安全性の観点からみた各タイムスタンプ方式間の関係，情報処理学会論文誌，Vol.43, No.8, pp.2644–2658 (2002).
9) 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).
10) 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，日本銀行金融研究所ディスカッションペーパーシリーズ，2002-J-32 (2002).
11) 松本 勉，岩下直行：デジタル署名の長期的な利用とその安全性について，日本銀行金融研究所ディスカッションペーパーシリーズ，2003-J-4 (2003).
12) 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，pp.627–632, 電子情報通信学会 (2002).
13) 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).
14) Dodis, Y., Katz, J., Xi, S. and Yung, M.: Key-Insulated Public Key Cryptosystems, *EUROCRYPY 2002*, Lecture Notes in Computer Science, Vol.2332, pp.65–82, Springer-Verlag (2002).
15) Dodis, Y., Katz, J., Xi, S. and Yung, M.: 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).
16) Matsumoto, H. and Matsumoto, T.: Artifactmetric Systems, Technical Report of IEICE, 100 (323), pp.7–14, Institute for Electronics, Information and Communication Engineering (2000).
17) Matsumoto, H. and Matsumoto, T.: An Evaluation Method for a Magnetic Artifact-metric System, *IPSJ Journal*, Vol.43, No.8, pp.2458–2466, Information Processing Society of Japan (2002).
18) Bellare, M. and Miner, S.K.: A Forward-Secure Digital Signature Scheme, *Proc. Crypto*, pp.431–448 (1999).
19) Surety, Inc.: Surety — Products & Services. http://www.surety.com/products.php
20) アマノ株式会社：e-timing（時刻認証，デジタルタイムスタンプ，電子文書改ざん検知）. http://www.e-timing.ne.jp/
21) セイコーインスツルメンツ株式会社：セイコーインスツルメンツ株式会社. http://www.sii.co.jp/ni/tss/
22) 株式会社 NTT データ：電子文書証明サービス SecureSeal(R). http://www.nttdata.co.jp/services/security/pdf/itsp_03pdf_01.pdf

付　　録

A.1 ヒステリシス署名方式の詳細

A.1.1 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
$A||B$ ：2 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つきメッセージ
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

A.1.2 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 $h(R_{n-1})$ のかわりに初期値 IV を用いる．
Step 3. Step 1，2 で算出した 2 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，電子署名つきメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ 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 $h(R_{n-1})$，および電子署名つきメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ を連結し，ヒステリシス署名つきメッセージ

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

を生成する．

Step 5. （署名生成履歴更新フェーズ）2 つのハッシュ値 $h(M_n)$，$h(R_{n-1})$ と電子署名つきメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ 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，ヒステリシス署名つきメッセージ S_n の検証は，次のように行う．

Step 1. ヒステリシス署名つきメッセージ 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，ヒステリシス署名つきメッセージ S_n に含まれるハッシュ値 $h(R_{n-1})$ および電子署名つきメッセージ $Sign_{K_s}(h(M_n)||h(R_{n-1}))$ 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．

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

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

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 の中に，検証対象となっているヒステリシス署名つ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，2-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，それぞれの有効性を判定した第三者機関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．

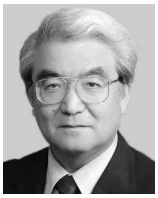
(平成 14 年 12 月 4 日受付)
(平成 15 年 6 月 3 日採録)

宮崎 邦彦（正会員）

1973 年神奈川県生．1998 年東京大学大学院数理科学研究科修士課程修了．同年株式会社日立製作所入社．現在に至るまで，同社システム開発研究所にて，暗号，情報セキュリティ技術に関する研究開発に従事．また，2003 年 4 月より東京大学大学院情報理工学系研究科博士課程在学中．電子情報通信学会会員．

吉浦　裕（正会員）

1981 年東京大学理学部情報科学科卒業．同年日立製作所入社，日立研究所，システム開発研究所に勤務．2003 年より，電気通信大学電気通信学部人間コミュニケーション学科助教授．自然言語処理，知識処理，情報セキュリティ，著作権保護の研究に従事．理学博士．電子情報通信学会，人工知能学会各会員．



岩村　充

1950 年東京都生．1974 年 3 月東京大学経済学部卒業．1974 年 4 月日本銀行入行，ニューヨーク駐在員等を経て 1996 年 12 月企画局兼信用機構局参事．1998 年 1 月より早稲田大学大学院アジア太平洋研究科教授（現職）．2002 年 3 月早稲田大学博士．専門は社会情報学および金融論.「法とコンピュータ学会」理事．著書に『銀行の経営革新』（東洋経済新報社),『サイバーエコノミー』（東洋経済新報社),『企業金融の理論と法』（東洋経済新報社),『金融システムの将来展望』（金融財政事情研究会・編著）等がある．

松本　勉（正会員）

1986 年東京大学大学院博士課程修了，工学博士．同年横浜国立大学工学部専任講師．同助教授，教授を経て，2001 年より同大学大学院環境情報研究院教授．1981 年より暗号や情報セキュリティの研究に従事.「明るい暗号研究会」創設メンバー．現在，暗号アルゴリズム，情報利用管理，ディジタル証拠性，情報ハイディング，バイオメトリクス，人工物メトリクス，耐タンパーソフトウェア等に広く関心を持つ．国際暗号学会 IACR 理事．暗号技術検討会構成員．ASIACRYPT ’96 プログラム委員長．ASIACRYPT 2000 実行委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．

佐々木良一（正会員）

1971 年東京大学卒業．同年日立製作所入所．システム開発研究所にてセキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所主管研究長兼セキュリティシステム研究センタ長等を経て現在東京電機大学工学部教授．工学博士（東京大学）．情報処理学会論文賞，電気学会論文賞，著作賞受賞．著書に,『インターネットセキュリティ入門』（岩波新書．1999 年）等．情報処理学会フェロー，理事．情報処理学会コンピュータセキュリティ研究会顧問．IFIP TC11 日本代表．