IMES DISCUSSION PAPER SERIES

デジタル署名の長期利用について

田村 裕子・宇根 正志・岩下 直行
松本 勉・松浦 幹太・佐々木良一

Discussion Paper No. 2004-J-27

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 2004-J-27
2004 年 12 月

デジタル署名の長期利用について

田村裕子[†1]・宇根正志[†2]・岩下直行[†3]・松本勉[†4]・松浦幹太[†5]・佐々木良一[†6]

要　　旨

電子政府の推進や民間での電子文書の利用に関する法整備が進むにつれて、紙文書から電子文書への移行が進んでいる。電子文書は、紙文書とは異なり、痕跡を残さずに内容を改ざんすることが容易であるため、電子文書の一貫性確保、本人認証等を行うために、今後、デジタル署名の利用が拡大していくものと考えられる。ただし、デジタル署名が付与された電子文書の一貫性確認を長期的に実施しようとした場合、署名検証に必要なデータの損失や署名生成鍵の危殆化といった問題が発生し得る。署名の長期利用のためには、そうした問題に対して、あらかじめ対策を講じておく必要がある。これらの論点については、日本銀行金融研究所が開催した第 5 回情報セキュリティ・シンポジウムにおいて問題提起され、筆者達が、その後さらに考察を深めるための研究会を開催してきた。本稿は、同研究会における研究成果を取り纏めたものである。

本稿では、署名の長期利用をどのように位置付けるかについて議論し、署名検証を行う際の手続、問題点、既存の主な対策技術を整理する。そのうえで、署名の長期利用に関する具体例として、ETSI TS 101 733 の署名トークンについて考察を行う。この署名トークンは、PKI やタイムスタンプ等の既存のインフラによって実装可能であり、IETF や W3C の技術仕様においても採用されているほか、本署名トークンを利用した商用システムも既に提案されている。本稿では、署名再検証を可能するための十分条件を導出することにより、署名トークンを今後利用していくうえで留意すべき点や今後の課題を示す。

キーワード：デジタル署名、長期利用、ETSI TS 101 733
JEL classification: L86、L96、Z00

†1　日本銀行金融研究所（E-mail: yuuko.tamura@boj.or.jp）
†2　日本銀行金融研究所（E-mail: masashi.une@boj.or.jp）
†3　日本銀行金融研究所（E-mail: iwashita@imes.boj.or.jp）
†4　横浜国立大学大学院環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）
†5　東京大学生産技術研究所（E-mail: kanta@iis.u-tokyo.ac.jp）
†6　東京電機大学工学部（E-mail: sasaki@im.dendai.ac.jp）

目 次

1. はじめに

文書の電子化に向けた制度的な取組みが引続き進展している。政府部門においては、「行政手続等における情報通信の技術の利用に関する法律（通称: 行政手続オンライン化法、2003 年 2 月施行）」に基づき、国の行政機関が扱う申請・届出等の電子文書への移行が年々進んでおり、2003 年度末には対象手続の約 96 %が電子文書へ置き換えられた（総務省 [2004]）。こうした電子化を支えるインフラである政府認証基盤（GPKI）では、PKI（public key infrastructure）の要であるブリッジ認証局が府省認証局や認定認証業務を運営する民間認証局との間で相互認証を順次実施しており（2004 年 4 月末現在において 32）、民間と政府の間で電子認証を活用したデータ交信を可能とする枠組みが整備されてきている。

民間部門においては、法律等によって交付が義務づけられている書面の電子文書形式での交付を企図した「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律（通称：IT 書面一括法、2001 年 4 月施行）」に続いて、2004 年 11 月には、法律等によって保存が義務づけられている財務・税務関連文書や帳票等の電子的な保存を原則として容認する「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」が成立し、2005 年 4 月に施行することとなっている。このように、これまで紙媒体として保管されてきた文書や帳簿等の電子媒体での保存が容認される動きは、紙文書から電子文書への移行という大きな流れを一層加速させるものと思われる。

その一方で、電子文書は紙文書と異なり複写や改ざんが容易であることから、電子文書を長期にわたり保存する場合には、その作成者や一貫性を後日確認するための対策を講じておく必要がある。電子文書を専用システムに格納し、そのシステムへのアクセス管理や履歴管理を厳格に行うことによって、電子文書の一貫性等を事後的に確認できるようにするサービス（セキュア・アーカイブ）の提供も開始されている。しかし、このようなサービスの利用においては、セキュア・アーカイブの信頼性を損なうような事故等が生じた場合、アーカイブ内に格納されるすべての電子文書の信頼性も失うというリスクがある（松本・岩下 [2003]）。また、長期にわたって利用・保管される電子文書の範囲が拡大するに伴って、その利用形態が多様化するとともに、より厳格な電子文書の作成者や一貫性の確認が求められるアプリケーションの登場も予想される。したがって、セキュア・アーカイブといった技術のみに依拠せずとも電子文書の安全性を確保することのできる手段があるならば、その利用も検討すべきである。

電子文書の一貫性を確認するその他の手段としては、まず電子署名法によって法的効力が付与されたデジタル署名技術が挙げられる。デジタル署名の利用に関しても、PKI における認証機関の署名生成鍵が漏洩した場合、認証機関が発行し

た電子証明書に係るすべてのデジタル署名の信頼性が損なわれるという問題がある。しかし、セキュア・アーカイブにおける多くのデータの出入りに伴うリスクに比べ、認証機関の署名生成鍵は利用が限定されているほか、漏洩問題への対策も検討されている（宇根 [2003]）。長期にわたる安全性を向上させるための対策をデジタル署名を付与した電子文書に講じることができれば、電子文書の信頼性損失のリスクを分散させることができる。また、デジタル署名の付与された電子文書は一貫性を保った状態でネットワーク上を流通可能であることから、セキュア・アーカイブに保管される電子文書より広域にわたって利用可能であるという利点をもつ。

日本銀行金融研究所は、デジタル署名の長期利用に関する問題に関して、2003年3月に「デジタル署名の長期的な利用とその安全性」をテーマとして第5回情報セキュリティ・シンポジウム（日本銀行金融研究所 [2003]）を開催している。そのパネル・ディスカッションの参加者らにより、同席において議論された課題について考察を深めるため、その後複数回にわたってデジタル署名の長期利用に関する研究会を開催してきた。本稿は、これら研究会のメンバーによる考察成果をまとめたものである。

これまで電子政府や電子商取引で利用されてきたデジタル署名は、主として「取引の瞬間」における本人確認のように、短期的な利用目的で使われることが多かった。しかし、今後は、デジタル署名が署名の対象となった電子文書とともに一定期間保管され、その間に電子文書が改ざんされていなかったことやデジタル署名の作成者を後日再度確認するといった形態で活用されることになると考えられる。こうしたデジタル署名の利用形態を「デジタル署名の長期利用」と呼んだり、電子文書とデジタル署名を両方保管するという点に着目して「電子署名文書の長期保存」と呼んだりすることがある（松本・岩下 [2003]、ECOM[2002]、ECOM・JIPDEC[2004a]）。デジタル署名によって長期間にわたる電子文書の信頼性を確保する手法については現在検討が進められている段階にあり、現在は各種トラブルの発生に備え、どのような対策を講じるべきであるか模索中であるといえる。本稿では、デジタル署名技術によって電子文書の長期保存問題に焦点を当て、検討を行うこととする。

長期利用あるいは長期保存の用途でデジタル署名を利用する場合には、従来から指摘されているように、デジタル署名方式自体の安全性低下等、将来発生する可能性がある問題に予め対応しておくことが必要である（例えば、ECOM[2002]、松本・岩下 [2003]、佐々木ほか [2003]）。具体的には、署名方式自体の安全性低下のほかに、署名検証に必要となる電子証明書や証明書失効情報の損失、電子認証サービスの利用者や認証機関の署名生成鍵の漏洩等が主な問題として挙げられる。こうした事象が発生してしまった場合、署名の偽造を検知不可能になる、あるいは、署名の検証自体が実行困難となり、それまで保管していた電子文書が信頼で

きなくなるという結果を招く。さらに、問題が深刻となれば、既存の電子認証の仕組みやそのサービスに対する信頼も失われ、社会のインフラとして機能しなくなるおそれもある。

デジタル署名の長期利用問題に対応するために、デジタル署名を補強するさまざまな技術が既に提案されている（宇根 [2003]）。まず、署名検証に必要なデータが損失した状況への対策として、欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute）の技術仕様 ETSI TS（technical specification）101 733（以下、単に ETSI TS と記す）に規定される署名トークン（electronic signature token）や DVCS（data validation and certification server protocols）等が挙げられる。署名生成鍵の漏洩への対策技術には、ETSI TS の署名トークンに加え、フォワード・セキュア署名（forward-secure signature）、キー・インシュレイティッド署名（key-insulated signature）、イントリュージョン・レジリエント署名（intrusion-resilient signature）等が挙げられるほか、署名方式の危殆化までを想定した場合の対策としては、ヒステリシス署名（hysteresis signature）、実行ハードウエア確認タグ付き署名、MAC 付きデジタル署名等が提案されている。

本稿では、これら数多くの技術の中でも、署名検証に必要なデータの損失や、CA 署名生成鍵の漏洩といったトラブルに対応可能とされている ETSI TS の署名トークンに焦点を当てる。ETSI TS の署名トークンは、RFC 3126（Pinkas, Ross and Pope [2001]）としても規定されているほか、W3C（World Wide Web Consortium）において XML ベースの署名トークンとしても仕様が公開されており（Cruellas *et al.* [2003]）、標準的な技術仕様となっている。また、署名トークンを構成するデータは、既存の PKI において用いられる電子証明書や証明書失効情報等とタイムスタンプによって構成されており、既存のインフラを利用して比較的容易に実装可能であるという特徴をもつ。こうしたことから、ETSI TS の署名トークンを活用したシステムの検討が行われているほか（例えば、ECOM[2002]）、いくつかの商用システムも既に提案されている。

そこで、こうした効果について一定の環境を想定したうえで検討を行い、どのような条件を満足すれば署名検証が実行可能であるかを明確にする。ETSI TS の署名トークンを利用する際に、本検討結果において示される十分条件が当該利用環境において満足されていることを確認することによって、署名トークンが期待通りの効果を発揮するか否かが前もって判断できることとなる。本稿では、ETSI TS の署名トークンを用いた署名の検証可能性を考察することにより、デジタル署名を長期利用する際の問題点、および、留意点を明らかにするとともに、今後の検討の方向性について整理することとしたい。

本稿の構成は次のとおりである。まず、2 節において、デジタル署名や PKI の概要について整理し、署名検証においては通常どのような処理が実行されるかを

説明する。3 節では、デジタル署名の長期利用を「署名生成直後に 1 回目の署名検証が行われ、一定期間経過後に再度署名が検証される（署名再検証される）利用形態」と定義したうえで、署名再検証を実行する際に発生し得る問題を整理する。4 節では、3 節において整理した各問題への対策として既に提案されている技術を列挙し、それぞれの技術の特徴や最新の研究動向を紹介する。5 節では、ETSI TS の署名トークンに焦点を当てて分析を行う。具体的には、まず、検討の前提条件を整理したうえで、署名再検証に必要なデータを署名トークン以外から入手できない場合、および、認証機関の署名生成鍵が漏洩した場合において、各署名トークンにおいて再検証が可能となるための十分条件を導出する。さらに、本検討結果が階層型 PKI の環境においても拡張可能であることを示すほか、ETSI TS では明示的に記述されていない利用者の署名生成鍵が漏洩した場合の影響についても考察する。6 節では、今後の課題を挙げて論文を締めくくる。

2. デジタル署名とPKI

デジタル署名方式は、署名生成者の特定と、署名対象データの一貫性の確認を実現可能とする技術である。データ作成者が秘密に保持する署名生成鍵を用いて生成したデジタル署名は、署名生成鍵と対をなす署名検証鍵に関連付けられる。このような署名検証鍵が署名生成者に係るものであることを保証するのがPKIであり、認証機関（CA: certification authority）が発行する電子証明書を用いることによって、署名検証鍵がその所有者に係るものであることを確認する。

本節では、デジタル署名の長期利用について議論する前に、デジタル署名とPKIについて整理する。なお、本稿では、現在最も広く利用されている、計算量的安全性に基づくデジタル署名方式[1]を取り扱うこととする。

(1) デジタル署名技術

デジタル署名方式は公開鍵暗号技術の特性を利用することから、署名生成鍵と対をなす署名検証鍵を用いることでデジタル署名を検証できる。

デジタル署名の生成と検証の手続を簡単に示すと次のようになる[2]（図1参照）。あるメッセージ M に対するデジタル署名 S は、署名生成鍵を用いて M を一定のアルゴリズム（署名生成アルゴリズム）で変換することにより生成される。また、M と S を入手した署名検証者は、これらのデータと署名検証鍵を用いて、一定のアルゴリズム（署名検証アルゴリズム）を実行することにより、S を検証する。この検証が正常に終了すれば、検証者は「S が当該署名検証鍵と対をなす署名生成鍵の保持者によって生成されたものであり、M は改ざんされていない」ことを確認できる。

デジタル署名方式の安全性は、署名検証鍵から署名生成鍵を算出すること、および、署名生成鍵を用いることなく偽造署名を生成することが計算量的に困難であるという性質に依拠する。したがって、署名生成鍵はその所有者によって秘密に管理される必要があるが、署名検証鍵は公開することができるため、任意の第三者による署名検証が可能である。

---

[1]計算量的安全性に基づくデジタル署名方式とは、署名の偽造には膨大な費用と時間が必要であろうと予想され、署名偽造が事実上不可能であるような方式を意味する。一方、ある一定以上の情報を入手しない限り、無限の計算能力をもってしても署名偽造が困難であるような情報理論的安全性に基づくデジタル署名方式に関しても現在研究が進められている。

[2]デジタル署名方式には、メッセージ付録型とメッセージ復元型がある。メッセージ付録型では、署名検証アルゴリズムはメッセージとデジタル署名の入力に対し、署名を受理/拒否の結果を出力するが、メッセージ復元型では、署名の入力に対し、検証結果とメッセージを出力する。ここでは、メッセージ付録型の場合を想定して説明する。

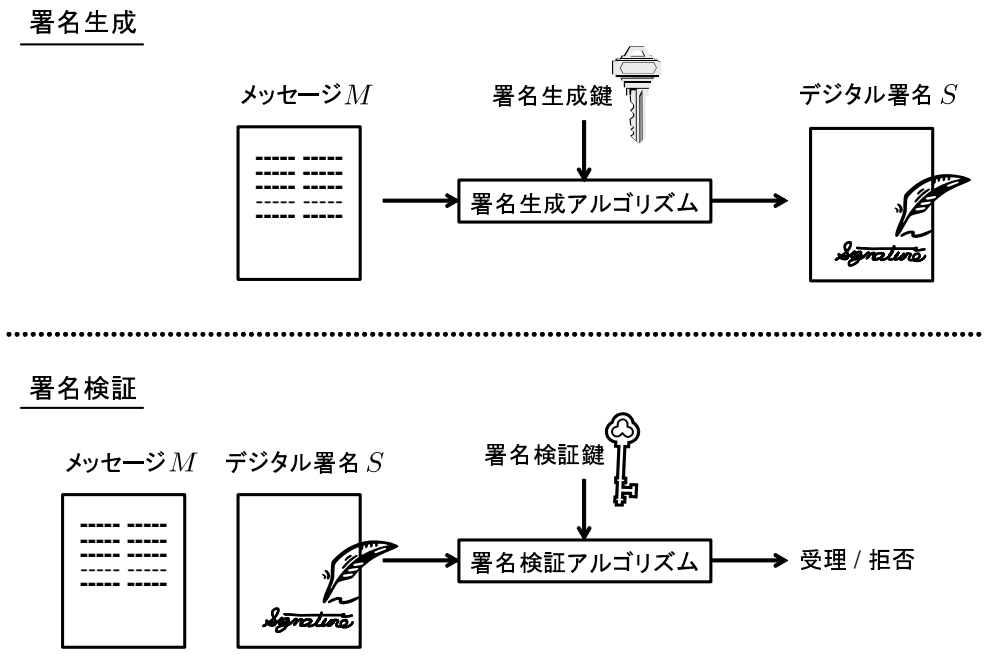

図 1: デジタル署名方式

(2) PKI の役割

デジタル署名を適切に利用するには、デジタル署名が署名作成者に係るものであること、および、署名生成鍵がその所有者によって適切に管理されていることが検証可能でなくてはならない。PKI は、これらの問題に対応する基盤を提供する。

PKI では、認証機関と呼ばれる第三者機関が、署名検証鍵とその所有者を関連付ける電子証明書を生成・発行する。電子証明書には、署名検証鍵や当該鍵ペアの所有者の識別子に加え、署名検証鍵の有効期間、および、これらのデータに対する認証機関によるデジタル署名が含まれる。このような認証機関の署名により、電子証明書が当該認証機関によって発行されたこととその一貫性が保証され、署名検証鍵と当該鍵ペアの保有者の対応関係が認証される。

こうした署名検証鍵とその所有者の対応関係には、署名生成鍵が正当な所有者によって適切に管理されていることが条件となる。したがって、所有者が署名生成鍵を紛失・漏洩した場合、認証機関は電子証明書を失効し、その旨を検証者に伝えなければならない。電子証明書の失効情報の通達方法としては、電子証明書失効リスト（CRL: certificate revocation list）を配布する方法と、特定の電子証明書の有効性に関する問合わせにリアルタイムで回答する OCSP（online certification status protocol）と呼ばれるプロトコルを利用する方法の 2 つが挙げられる。

PKI では、認証機関が正しく機能し、電子証明書、および、CRL が所有者や検証者にとって信頼できるものであることが前提となる。そこで、認証機関は、自身

の業務内容やセキュリティ対策に関する情報を認証運用規程（certification practice statement）として公表し、利用者から信頼を得る必要がある。また、既に信頼を得ている他の認証機関から電子証明書を発行してもらうことによって信頼を確立する場合もある。

(3) PKI を構成するエンティティ

PKI は、認証機関、利用者、検証者によって構成される。各エンティティの役割・機能は以下のとおりである。

- **認証機関**: 電子証明書の生成・検証用鍵ペアと CRL の生成・検証用鍵ペアを保持し、電子証明書および CRL を発行するエンティティ。本稿では、これらの生成鍵をまとめて CA 署名生成鍵と呼ぶ。また、認証機関が、他の認証機関に対して電子証明書や CRL（この場合、ARL: authority revocation list とも呼ばれる）を発行する場合には、電子証明書として、電子証明書検証用と CRL 検証用の 2 種類が発行される。

  トラスト・アンカーとなるルート認証機関では、これらの電子証明書に加えて、自己署名付きの電子証明書も発行される。また、自己署名付きの電子証明書の失効情報（以下では、CA 証明書失効情報と呼ぶ）を適宜公表する場合もある。

- **利用者**: 署名生成鍵と署名検証鍵を生成し、署名検証鍵に対する電子証明書を認証機関に発行してもらうエンティティ。利用者は署名生成鍵を用いてデジタル署名を生成する。以下では、利用者の署名生成鍵を利用者署名生成鍵と呼ぶ。

- **検証者**: 利用者が生成した署名を検証するエンティティ。

一般に、認証機関の各種機能を、証明書発行機関（certificate issuer）、登録機関（registration authority）、証明書生成機関（certificate manufacturer）、リポジトリ等の複数のエンティティが担う状況も想定されるが、本稿ではそれらの機能を分離せず、1 つのエンティティが担うこととする。また、複数の認証機関によって PKI が構成される場合には、階層型や相互認証型といった形態が存在するが（宇根 [2002]）、本稿では、議論を単純化するため、単独認証機関によって構成される PKI を想定する（図 2 参照）。

以降では、利用者に対して発行される電子証明書を利用者証明書、認証機関に対して発行される（自己署名付き）電子証明書を CA 証明書と呼ぶ。なお、CA 証

明書と呼ぶときは、特に断らない限り、利用者証明書検証用 CA 証明書と CRL 検証用 CA 証明書の両者を指すものとする。

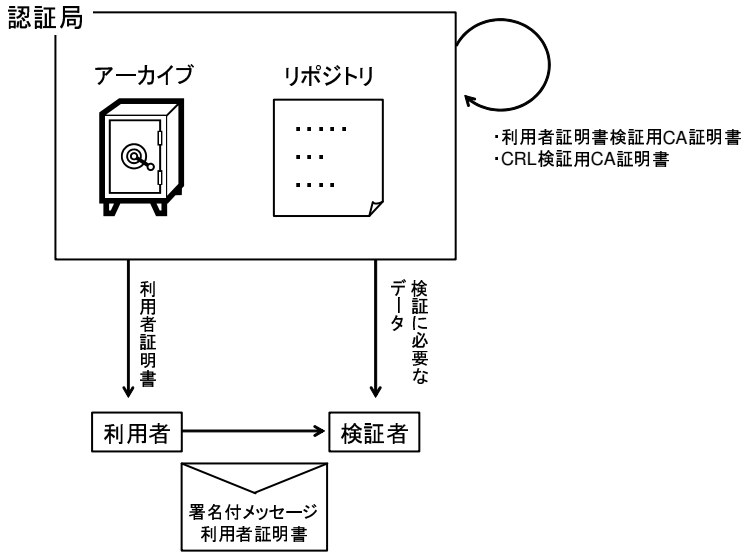

図 2: 単独認証機関による PKI

(4) 署名検証

イ. 署名検証において確認すべき事項

特定認証業務の中でも代表的なものとして日本認証サービスの「AccreditedSign パブリックサービス 2」（以下、AccreditedSign と呼ぶ）とセコムトラストネットの「セコムパスポート for G−ID」（以下、セコムパスポートと呼ぶ）を取り上げ、これらの認証運用規程と利用者規程を参照することにより、署名検証の標準的な手続を整理する。認証運用規程については、AccreditedSign パブリックサービス 2 標準規程（V2.2、日本認証サービス [2004b]）、および、セコムパスポート for G−ID 認証運用規定（Version 1.70、セコムトラストネット [2004a]）を参照する。また、利用者規程については、AccreditedSign パブリックサービス 2 依存者同意書（日本認証サービス [2004a]）、および、利用者利用規定（セコムトラストネット [2004b]）を参照する。これらの利用者規程は、いわゆる署名ポリシー（signature policy）の内容の一部に対応するものと考えることができる。

これらの認証運用規程および利用者規程では、署名検証を行ううえで、以下の事項を確認することが検証者に義務付けられている。

認証パス上の電子証明書、および、利用者証明書が、
- 認証機関によって発行されたものであること、
- 有効期間内であること、
- 失効していないこと、
- 利用目的および使用範囲が適切であること。

上記確認の必要性とその手段については、本稿で想定する PKI の枠組みにおいて考えると、以下のように整理することができる。

- **認証機関によって発行されたものであること**: 利用者証明書については、利用者証明書検証用 CA 証明書を用いて、利用者証明書に含まれる認証機関の署名を検証することで、当該認証機関によって発行されたものであることを確認する。また、認証機関の CA 証明書に関しては、自己署名であるため、認証機関によって発行されたものであることを署名検証以外の別の手段で確認する。

- **有効期間内であること**: 電子証明書（利用者証明書、CA 証明書）には、有効期間が設けられており、その間は、署名生成鍵を適切に管理することが、利用者や認証機関に義務付けられている。しかし、有効期間満了後は、対応する署名生成鍵が適切に管理されているか否かの判断が困難となるため、検証者は署名生成時点が電子証明書の有効期間内であることを確認する必要がある。ただし、検証者が署名生成日時を特定する手段をもたない場合には、検証時点が有効期間内であることを確認すればよい。また、有効期間が改ざんされているか否かは、CA 証明書を用いた電子証明書の検証によって確認する。

- **失効されていないこと**: 利用者証明書が失効されているか否かは、CRL を参照することで確認する。CRL には認証機関によるデジタル署名が付与されており、CRL が当該認証機関によって発行されたこと、および、一貫性が保たれていることを、CRL 検証用 CA 証明書を用いて確認する。また、CA 証明書については、CA 証明書失効情報を用いて失効の有無を確認する。

- **利用目的および使用範囲が適切であること**: 利用者証明書の拡張領域に含まれる鍵の利用目的（key usage）が適切であるか、すなわち、署名検証目的の鍵であることが明示されているか（digitalSignature や nonRepudiation の属性が指定されているか）といった確認を行う。

署名生成時点（もしくは、検証時点）が電子証明書の有効期間内であるか否か、また、その時点において電子証明書は失効していたか否かを確認可能とするため、利用者、認証機関、および、検証者が十分な精度で同期した時計を持つことを仮定する。

ロ. 署名検証処理

上記の 4 項目のうち、証明書の利用目的や使用範囲が適切であることの確認を除く 3 項目に焦点を当てると、各処理は以下の手順で実行されると考えられる。本稿では、失効情報を入手する手段として、CRL を直接参照するケースを想定する。なお、AccreditedSign、および、セコムパスポートにおいては、利用者証明書と CRL の生成に用いる署名生成鍵は同一であるため、発行される CA 証明書は 1 種類であるが、ここでは認証機関が異なる 2 種類の署名生成鍵を利用するものとする。

処理 1: CA 証明書失効情報を用いて、利用者証明書検証用 CA 証明書が失効していないことを確認する。

処理 2: 処理 1 の利用者証明書検証用 CA 証明書を用いて、利用者証明書が認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 3: CA 証明書失効情報を用いて、CRL 検証用 CA 証明書が失効されていないことを確認する。

処理 4: 処理 3 の CRL 検証用 CA 証明書を用いて、CRL が認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 5: 処理 4 の CRL を用いて、処理 2 の利用者証明書が失効されていないことを確認する。

上の処理 1〜5 の実行に必要となるデータは以下のとおりである。

- **データ 1** CA 証明書失効情報。ただし、認証機関によって公表されたことが確認可能であるもの。(処理 1、3 に対応)
- **データ 2** 利用者証明書検証用 CA 証明書。ただし、認証機関によって発行されたことが確認可能であり、有効期間内であるもの。(処理 1、2 に対応)
- **データ 3** 利用者証明書。ただし、有効期間内であるもの。(処理 2、5 に対応)
- **データ 4** CRL 検証用 CA 証明書。ただし、認証機関によって発行されたことが確認可能であり、有効期間内であるもの。(処理 3、4 に対応)
- **データ 5** CRL。ただし、最も新しく発行されたもの。(処理 4、5 に対応)

これらのデータが入手できれば、検証者は利用者証明書が認証機関によって発行されたこと、有効期間内であること、失効していないことを確認することができ、署名検証が実行可能となる。

(5) 署名検証に必要なデータの入手方法

AccreditedSign、セコムパスポートにおける認証運用規程を参照して、前節 (4) ロ. のデータ 1〜5 の標準的な入手方法を整理する。

- **CA 証明書失効情報（データ 1）**：CA 証明書失効情報に関しては、その取扱いは各認証運用規程によって異なるものの、類似の情報はいずれも公表される扱いとなっている。

  AccreditedSign における自己署名証明書の取扱いにおいては、CA 署名生成鍵が危殆化（漏洩）した場合、あるいは、その疑いが生じた場合には、「証明書の失効等検証に必要な情報」をリポジトリにおいて公表する旨が記載されている[3]。この情報が CA 証明書失効情報に対応すると考えられる。また、当該 CA 署名生成鍵を用いて生成したすべての利用者証明書を失効させ、その失効情報を反映した CRL に対して、危殆化した CA 署名生成鍵を用いて署名することが規定されている。この CRL の検証には危殆化した CA 署名生成鍵に対応する CA 証明書が必要であることから、CA 証明書を失効しない旨が記載されており、認証業務終了の際も、CA 証明書を失効しないとある。アーカイブにおける CA 証明書失効情報の管理に関しては、「証明書署名鍵管理（鍵生成、保管、活性化／非活性化、バックアップ／復元、破棄）と対応する自己署名 SCA 証明書発行の実施に伴う」紙およびデジタル・データで運用される帳票を 10 年間保管する旨が記述されており、CA 証明書失効情報がこうした情報に含まれる可能性がある。

  セコムパスポートにおいても、CA 署名生成鍵が危殆化した場合、および、認証業務終了の場合には、リポジトリを通じて鍵の危殆化等の事実を公表する旨が記載されている。CA 証明書の失効については、「発行したすべての加入者証明書、相互認証証明書及び自己発行証明書について取消の手続を行う」との記載はあるが、ここで議論している CA 証明書に対応する「自己署名証明書」を失効させるとの記述はない。利用者利用規定においても、自己署名証明書の一貫性を確認しなければならないとの記述はあるが、その失効の有無の確認については記載されていない。アーカイブにおける CA 証明書失効情報の管理については、「加入者への説明の記録」や「CA の秘密鍵の作成及び管理に関する記録」を当該電子証明書の有効期間満了日から最低 10 年間保管する旨が記載されており、CA 証明書失効情報がこうした情報に含まれる可能性がある。

[3]ただし、「本同意書（依存者同意書を指す）に同意した依存者だけが、検証を実施するために、このリポジトリを使用することができます」と記述されており、署名検証を行う際には、何らかの手段で当該認証機関にリポジトリの使用申請を行う必要があるとみられる。

- **CA 証明書（データ 2、4）**：有効期間内の CA 証明書は当該認証機関のリポジトリから入手可能であるケースが多く、AccreditedSign とセコムパスポートのいずれにおいてもインターネット経由でリポジトリから CA 証明書を入手できるようになっている。CA 証明書の有効期間は、AccreditedSign では 10 年 10 日、セコムパスポートでは 10 年 30 分である。また、有効期間満了後の CA 証明書は、当該認証機関のアーカイブにおいて有効期間満了後 10 年程度保管される場合が一般的であり、上記の 2 つの認証業務においても同様の扱いとなっている。

  また、CA 証明書が当該認証機関によって発行されたものであることの確認は、リポジトリにおいて公開されるフィンガー・プリント（CA 証明書のハッシュ値）との照合によって確認される。フィンガー・プリントは、ldap、もしくは、https を利用して配布される。

- **利用者証明書（データ 3）**：一般に、利用者証明書はデジタル署名とともに、検証者に送付される。その有効期間は、AccreditedSign では、2 年 30 日、または、3 年 30 日であり、セコムパスポートでは 1 年 30 分と設定されている。なお、端数に満たない日数は、利用者証明書取得等のための期間である。

  認証機関が発行したすべての利用者証明書、および、その作成に関する記録は、利用者証明書の有効期間満了後も、アーカイブにおいて 10 年程度保管されるケースが多い。上記の 2 つの認証業務においても同様である。

- **CRL（データ 5）**：有効期間内の CRL は、当該認証機関のリポジトリから入手可能であるケースがほとんどである。AccreditedSign 、セコムパスポートのいずれにおいても、CRL の有効期間は 24 時間と設定されており、利用者証明書が失効される都度 CRL は更新される。失効された利用者証明書は、当該証明書の有効期間内は CRL に掲載され、有効期間が満了すると CRL から削除される。また、発行されたすべての CRL はアーカイブにおいて有効期間満了後 10 年程度保管されるケースが多い。

各認証業務は、アーカイブ・データの漏洩、滅失、毀損の防止措置のため、防災、防犯、防火、防水機能を持つ保管庫の使用等により、アーカイブ・データを物理的に安全な状態で保管することを規定している。AccreditedSign では、天災にも対応できるようバックアップ・データを遠隔地において保管する。また、保管期間の満了したデータは確実に破棄されるとしている。

また、アーカイブに保管された電子証明書や証明書の失効情報の開示については、AccreditedSign、セコムパスポートのいずれにおいても、どのようなエンティティに対してどのような場合に開示するのかが認証運用規程の中で明確に記載さ

れていない。ただし、認証機関が保管する機密情報[4]については、捜査機関や法執行機関等への開示、民事手続上の開示、利用者証明書名義人からの要請に基づく開示が可能である旨が記述されていることから、少なくともこれらの事由があればアーカイブに保管されているデータも開示されるであろうと思われる。

以上を整理すると、AccreditedSign、および、セコムパスポートにおいては、データ 1〜5 は、認証機関によって発行されてから有効期間満了後 10 年程度まで認証機関のリポジトリ、もしくは、アーカイブにおいて保管される。また、アーカイブのデータは、物理的にも厳重な管理の下に置かれ、紛争発生時や利用者の要求に応じて提供される。したがって、現状の標準的な PKI においても、同様にデータ 1〜5 は認証機関によって保管されることになると考えられ、署名生成時点を特定する手段が別途利用できるならば、電子証明書の有効期間満了後も、アーカイブのデータを用いて署名の検証を実行できる可能性があるといえよう。

[4]電子証明書や CRL 等は機密情報に該当しないとされている。

3. デジタル署名の長期有効性を巡る問題

(1) デジタル署名の長期利用

現行の PKI の枠組みにおいては、一般にデジタル署名の検証は利用者証明書の有効期間内に行うことが前提とされているようであり、デジタル署名の利用は、電子商取引等における「取引の瞬間」に留まっている。

2001 年に施行された「電子署名及び認証業務に関する法律」により、一定の条件をみたすデジタル署名は、手書き署名や押印の効果と同等の法的効力を認められることとなった。また、2004 年 11 月、民間において保存が義務付けられている文書・帳簿の電子保存を可能とする統一的な法律である「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」が成立し、2005 年 4 月に施行することとなっている。こうした制度的枠組みの変化によって、紙の文書から電子文書への移行が加速され、電子文書の長期利用のニーズは一層高まると思われる。したがって、デジタル署名の効果を長期にわたって維持し、利用するうえでの問題点を明確にし、どのように対策を講じていくかを検討することが必要である。

(2) 長期利用とは

まず、デジタル署名の長期利用という概念に着目し、その概念整理からはじめる。まず、これまでに発表されたデジタル署名、電子認証関連の主な 5 つの文献を取り上げ、これらの文献における「署名の長期利用」の捉え方を参照する。

ETSI TS 101 733 (version 1.5.1): ETSI TS(ETSI[2003]）は、検証者が署名検証に必要なデータを入手できない状況、あるいは、認証機関の署名生成鍵が漏洩した状況においても署名検証を可能とする署名トークンを規定しており、長期利用のための署名トークンと呼んでいる。こうした記述から、本技術仕様は、上記のようなトラブルの発生が想定される状況において署名検証を実行する場合を署名の長期利用と位置づけているとみることができる。

電子商取引推進協議会・日本情報処理開発協会 調査報告書: 電子商取引推進協議会（ECOM）と日本情報処理開発協会（JIPDEC）による電子署名文書長期保存に関する実用化動向調査報告書（ECOM・JIPDEC[2004a]）は、「検証したい電子文書の電子署名が生成された当初は有効であっても、公開鍵証明書の有効期限が過ぎたとき、または公開鍵証明書が失効したときには、その検証のもととなる公開鍵証明書が保証されない。そのため、電子署名の有効

性も確認できないといったことが問題視されている」と説明している。そのうえで、こうした問題が発生した後も署名検証を実行可能とすることが署名の有効性を長期にわたり維持することであるとしている。このような記述から、ECOM の本調査報告書においては、主に、利用者証明書の有効期間満了後において署名の検証を実行する場合を署名の長期利用と捉えていると考えられる。

IPA PKI 関連技術解説: 情報処理推進機構（IPA）セキュリティセンターによる PKI 関連技術解説（IPA[2004a]）では、電子文書の長期保存に関して、「電子署名文書を長期にわたり有効な状態で保存する場合、暗号鍵の危殆化やアルゴリズムの弱体化から来る偽電子文書を作らせないために、様々な考慮が必要となってきます」を説明しているほか、電子署名長期保存に必要な考慮として、「証明書の有効期限が切れると、署名の検証が行えなくなってしまいます」という電子証明書の有効期限切れの問題を挙げている。こうしたことから、本技術解説では、署名の安全性低下等のトラブルの発生と電子証明書の有効期限切れの両者を想定し、そうした状況において署名検証を実行するケースを署名の長期保存（すなわち長期利用）と呼んでいると考えられる。

宮崎ほかの論文: 宮崎ほか [2003] 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」と定義している。この定義から、宮崎ほかの論文では、署名生成時点と検証時との時間的間隔ではなく、検証者が事後的に署名検証を行うか否かに着目し、そうした事後的な署名検証を行う場合を署名の長期利用と捉えていると考えられる。

松本＝岩下の論文: 松本・岩下 [2003] では、「署名・捺印のある紙の文書が、取引の瞬間における作成者の意思の確認という役割に加えて、事後的に確認可能な証拠という役割も果たしている」と説明し、「デジタル署名の付与された電子文書が、署名・捺印のある紙の文書の代替物として実務に利用されていくために解決しなければいけない課題として、デジタル署名の長期的な利用の問題をとり上げ」ていることから、デジタル署名を用いて電子文書の一貫性や署名生成者の確認を事後的に行う場合をデジタル署名の長期利用と呼んでいると考えることができる。

以上の文献の考え方を整理すると、以下の 3 つに分けることができる。

1. 事後的に署名を再度検証することを想定した利用を署名の長期利用とする。

2. 利用者証明書の有効期間後に署名を再度検証することを想定した利用を署名の長期利用とする。

3. 署名方式の危殆化や署名生成鍵の漏洩といったトラブルが発生することを想定した利用を署名の長期利用とする。

まず、上記 1. の考え方は宮崎ほかの論文や松本＝岩下の論文で採用されており、長期利用とそれ以外を明確に区別可能であるというメリットがある。また、この考え方をベースとすれば、上記 2.、3. において挙げられている利用者証明書の有効期間切れや署名方式の危殆化等のトラブルも、デジタル署名を長期利用する際に発生し得る問題として捉えやすいという利点がある。上記 1. の考え方は、特定の時点を境に時間軸を分割して長期利用を定義するものではない。このため、署名方式の危殆化や署名生成鍵の漏洩等、どのタイミングで発生するか事前には（ある程度予測できるかもしれないが、正確には）わからないトラブルも、署名の長期利用での問題として位置付けることが可能となる。

上記 2. の考え方についても、署名の事後的検証の有無をベースとしたうえで利用者証明書の有効期間をベンチマークとしており、長期利用とそれ以外を明確に区別可能であるという利点がある。ECOM・JIPDEC の調査報告書、IPA の PKI 関連技術解説においてはこの考え方を採用していると考えられる。この考え方に軸足を置くとすると、利用者証明書の有効期間内において署名を検証するという形態での利用は長期利用に該当しないことになる。しかし、署名の長期利用において問題とされている署名方式の安全性低下や署名生成鍵の漏洩といったトラブルは利用者証明書の有効期間満了後であるか否かによらず発生する可能性があり、署名の長期利用に特有の問題として各種トラブルについて議論するのは困難である。

上記 3. の考え方は、ETSI TS、IPA の PKI 関連技術解説において触れられている。既存の文献では署名の長期利用の際に留意すべきトラブルとして署名方式の危殆化をはじめ数多くの事項が挙げられており、それらのトラブルの背景や影響度は千差万別である。したがって、署名の長期利用を定義する際には、それぞれ性質の異なるトラブルをどのように位置づけるかが問題となる。実際に検討を行う際には、画一的な基準によって署名の長期利用を規定するよりも、発生することが想定される、あるいは、想定すべきトラブル 1 つ 1 つについて個別に検討する方が適切ではないかと考えられる。

以上の考察から、本稿においては、上記 1. の考え方である事後的な署名の検証を想定するか否かに基づいて署名の長期利用を定義するのが相対的に有用であると考えられるため、次のとおり定義する。

デジタル署名の長期利用:	デジタル署名の生成者、および、署名対象データの一貫性を事後的に確認するための利用。署名生成直後に一度検証が行われるが、それから一定期間後に改めて署名検証が行われる。

以下では、署名生成時点から一定期間後に行われる長期利用のためのデジタル署名の検証を「再検証」と呼び、署名再検証に必要となる手続、および、署名再検証に係る問題点について整理する。

(3) 署名再検証

署名検証の実行が利用者証明書の有効期間内に限定される場合、署名生成時点もその有効期間内に含まれることから、検証者は署名生成時点を特定する必要はない。署名検証が利用者証明書の有効期間終了後に実行される場合には、署名生成時点を特定したうえで、署名生成時点において当該利用者証明書が有効であったこと、失効していなかったことを確認する必要がある。したがって、デジタル署名の再検証では、前節 (4) イ. と同様に以下の事項を確認することになると考えられる。

認証パス上の電子証明書、および、利用者証明書が、
- 認証機関によって発行されたものであること、
- 署名生成時点を有効期間に含むこと、
- 署名生成時点において失効していないこと。
- 利用目的および使用範囲が適切であること。

本稿では、上記の 4 項目のうち、利用目的や使用範囲が適切であることの確認を除く 3 項目に焦点を当て、これらの事項が確認可能な場合、検証者は**署名再検証を実行可能である**と呼ぶことにする。

また、署名生成時点が電子証明書の有効期間内であるか否か、また、署名生成時点における電子証明書の失効の有無を確認可能とするため、署名生成、および、署名再検証に携わるエンティティが十分な精度で同期した時計を持つことを仮定する。

上記確認に伴う処理は、署名生成時点（以下、t_S と記す）を確認したうえで、一般には以下の手順で実行されると考えられる（図 3 参照）。

処理 1: CA 証明書失効情報を用いて、利用者証明書検証用 CA 証明書が t_S におい

て失効していないことを確認する。

処理 2: 処理 1 の利用者証明書検証用 CA 証明書を用いて、利用者証明書が認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 3: CA 証明書失効情報を用いて、CRL 検証用 CA 証明書が t_S において失効していないことを確認する。

処理 4: 処理 3 の CRL 検証用 CA 証明書を用いて、CRL が認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 5: 処理 4 の CRL を用いて、処理 2 の利用者証明書が失効していないことを確認する。

上で整理した署名の再検証に係る処理 1〜5 を実行する際、検証者が入手する必要があるデータを列挙する。

- **データ 1** CA 証明書失効情報。ただし、認証機関によって公表されたことが確認可能であるもの。(処理 1、3 に対応)
- **データ 2** 利用者証明書検証用 CA 証明書。ただし、認証機関によって発行されたことが確認可能であり、t_S を有効期間に含むもの。(処理 1、2 に対応)
- **データ 3** 利用者証明書。ただし、有効期間と設定されている期間に t_S を含むもの。(処理 2、5 に対応)
- **データ 4** CRL 検証用 CA 証明書。ただし、認証機関によって発行されたものが確認可能であり、t_S を有効期間に含むもの。(処理 3、4 に対応)
- **データ 5** CRL。ただし、発行時刻が t_S として記載されているもの。(処理 4、5 に対応)

議論を単純にするために、署名生成から署名トークンの生成までの時間的間隔は無視できるものとし、上記データ 5 の CRL については、t_S において発行されたとみなすこととした。

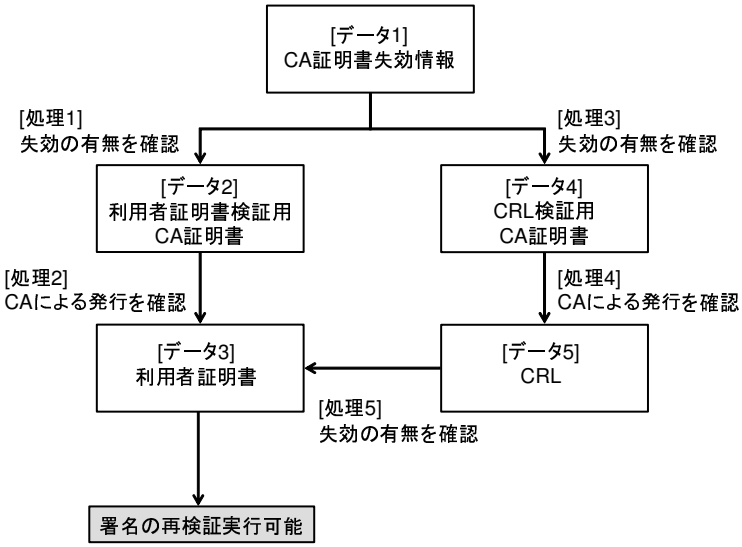

図 3: 署名再検証に係る処理

(4) 署名再検証に係る問題点

上記の 5 つのデータを入手できれば、検証者による署名の再検証は可能である。前節 (5) において整理したように、現行の PKI においては、CA 証明書、利用者証明書、CRL は有効期間満了後 10 年程度、認証機関のアーカイブに保管される。したがって、少なくとも 10 年程度は署名再検証が実行できる可能性がある。ただし、その間に各種トラブルの発生によって、再検証が実行不可能となるおそれもある。どのようなトラブルが想定されるかについては既に複数の文献（例えば、佐々木ほか [2003]）において議論されているが、その中でも代表的なものとして以下の 2 つを挙げることができる。

- **署名検証に必要なデータの破損・喪失**: 一般に、署名検証に必要なデータは有効期間内はリポジトリに格納されるほか、有効期間満了後は認証機関のアーカイブに格納される。しかし、すべてのデータを永久に保管し続けることは、現実的に困難であり、一般にはデータの保管期間が設定され、保管期間が終了したデータは確実に廃棄される。したがって、各種データのアーカイブ保管期間終了後に署名の再検証を実行しようとする場合には 認証機関から各種データを入手することが不可能となり、署名再検証を実行できなくなるおそれがある。

  また、署名の再検証を実行すると考えられる期間を有効期間内に含むような利用者証明書を準備するという方法も提案されている（佐々木ほか [2003]）。しかし、そうした方法を用いた場合であっても、災害や事故の発生等によって、認証機関が管理するデータが破損・喪失してしまう可能性もある。

- **署名生成鍵の漏洩**: 漏洩の可能性がある署名生成鍵としては、CA 署名生成鍵と利用者署名生成鍵が挙げられる。CA 署名生成鍵が漏洩した、あるいは、漏洩したと疑われた場合、利用者証明書や CRL の偽造が可能となり、署名再検証においてそれらの偽造を検知することは不可能となる。その結果、CA 署名生成鍵が漏洩する前に適切に生成されたすべての利用者証明書や CRL に関しても、認証機関が発行したものであるか否かを判断することが困難となり、そうしたデータを必要とする署名検証は実行不可能となってしまう。

  利用者署名生成鍵が漏洩した、あるいは、漏洩した疑いが生じた場合、漏洩した鍵による署名の偽造を検知することは不可能となり、当該利用者署名生成鍵によって適切に生成された過去のすべての署名が信頼を喪失してしまうこととなる。

  このような署名生成鍵の漏洩を引き起こす原因としては、署名方式の安全性上の問題や署名生成鍵の管理上の問題等多岐にわたる。こうした点に関しては、佐々木ほか [2003] において既に整理されているため、本稿ではこれ以上深く考察せず、いずれかの原因によって署名生成鍵が漏洩した状況を想定して議論を進めることとする。

4. デジタル署名の長期利用のための技術

前節において整理した署名の長期利用における問題への対策の研究は近年盛んに行われている。本節では、既存の対策技術を紹介する。

(1) 認証機関から署名検証に必要なデータが入手不可能な状況への対策技術

認証機関のリポジトリやアーカイブには署名再検証に必要なデータが一定期間保管されるケースが一般的であるが、アーカイブ保管期間の満了によりデータが廃棄される、または、災害や事故等によりデータが破損・喪失するといった場合には、検証者は署名再検証を実施困難となる。このような状況を想定した対策としては、

I. 署名検証に必要なデータを別途保管しておく、

II. 既に一度検証が行われ、その際に検証が問題なく成功したことを、何らかの手段で後から確認できるようにしておく、

といったアイデアが考えられる。上記 I. に相当する代表的な技術として ETSI TS 101 733 の署名トークンを、上記 II. に相当する代表的な技術として DVCS を紹介する。

イ. ETSI TS 101 733

ETSI TS 101 733 の署名トークンのいくつかは、長期にわたる署名検証を実行可能にすることを企図しており、RFC3126（Pinkas, Ross and Pope [2001]）においても規定されている。ETSI TS は、利用者証明書の有効期間満了後に署名再検証を実行する状況を想定し、その際にいくつかのトラブルに対応するための署名トークンを規定している。例えば、署名検証に必要なデータが入手不可能となるというトラブルに対応すべく、それらのデータを内部に格納した署名トークンが規定されている。署名トークンの構造等については次節において詳しく説明する。

ETSI TS の署名トークンを保管する方法についても既に検討結果が発表されている。ECOM では、署名を長期間にわたって検証可能にすることを目的とした「電子署名文書長期保存システム（ECOM[2002]）」のアイデアを提案しており、そのセキュリティ要件やシステム要件を明らかにしている。本システムでは、デジタル署名を ETSI TS の署名トークンの形式で保管することとしており、いくつかの種類の署名トークンが推奨されている。また、最近の ECOM・JIPDEC の調査報

告書（ECOM・JIPDEC[2004a]）においては、ECOM の電子署名文書長期保存システムと類似のアイデアに基づく商用システムがいくつか提供されている現状が紹介されている。

ロ. DVCS

DVCS は、過去に実施した署名検証が問題なく成功したことを後日確認可能にするための技術であり、RFC3029（Adams, Sylvester *et al.*[2001]）として規定されている。DVCS では、デジタル署名の検証を実行する DVC サーバを想定しており、DVC サーバが検証者に代わってデジタル署名の検証を実行し、その結果をデータ検証証明書（DVC: data validation certificate）として検証者に発行する。データ検証証明書には DVC サーバのデジタル署名が添付される。RFC3029 には、こうしたエンティティ間でのデータの交信方法、交信されるデータの構造、データ検証証明書の構造等が規定されている。

DVCS においては、DVC サーバが検証者から信頼されるエンティティ（trusted third party）であることを想定している。したがって、検証者は、データ検証証明書を予め取得しておくことによって、当該データ検証証明書の対象となっている署名の検証が DVC サーバによって実施され、署名検証に成功している事実を第三者に対して主張することが可能であると考えられる。ただし、データ検証証明書が DVC サーバによって発行されたこと、および、データ検証証明書の一貫性が確保されていることを同証明書のデジタル署名によって確認する必要があり、同署名についても長期利用を巡る問題が発生することになるといえる。

(2) 署名生成鍵の漏洩に対する署名偽造対策技術

署名生成鍵の漏洩への主な対策技術としては、フォワード・セキュア署名、キー・インシュレイティッド署名、イントリュージョン・レジリエント署名、ヒステリシス署名、実行ハードウエア確認タグ付き署名、MAC 付きデジタル署名が挙げられる。

また、ETSI TS においても、CA 署名生成鍵の漏洩を想定した署名トークンがいくつか規定されている。それらの署名トークンでは、署名トークンを構成するデータに対してタイムスタンプが付与されており、CA 署名生成鍵が漏洩したタイミングにおいてタイムスタンプの安全性も同時に低下することはないとの前提のもとで、署名偽造を検知可能であるとしている。

イ．フォワード・セキュア署名

フォワード・セキュア署名は、署名生成鍵の漏洩による被害が過去に生成した署名に及ばないようにする技術であると表現することができる（Anderson[1997]、Bellare and Miner[1999]、Abdalla and Reyzin[2000]、Itkis and Reyzin[2001]、Malkin, Micciancio and Miner[2002]）。通常のデジタル署名は、署名生成鍵がいったん漏洩してしまうと、過去に生成されたすべての署名は偽造されたものであるか否かを判断することが困難となる。これに対して、フォワード・セキュア署名では、署名生成鍵を短い期間（例えば 1 日）で更新し、使用期間が満了した署名生成鍵をその都度廃棄することによって、現在使用している署名生成鍵が漏洩したとしてもその署名生成鍵よりも古い署名生成鍵によって生成された過去のデジタル署名を偽造することを困難にする。

公開鍵を pk、pk の有効期間の分割数を $T(>1)$、期間 t で用いる署名生成鍵を sk_t とした場合におけるフォワード・セキュア署名方式の概要を図 4 に表わす。期間 t における署名生成は sk_t を用いて行われ、期間 $t+1$ の署名生成鍵 sk_{t+1} は、sk_t を一方向性関数に入力することによって得られる。したがって、sk_t が漏洩した場合、期間 $t+1$ 以降の署名生成鍵を容易に導出できるものの、sk_t から時点 $t-1$ 以前の署名生成鍵を導出することは困難である。このため、sk_{t-1} が完全に破棄されており、本署名方式自体の安全性が低下しないという仮定のもとで、期間 $t-1$ 以前の署名偽造は困難であるといえる。

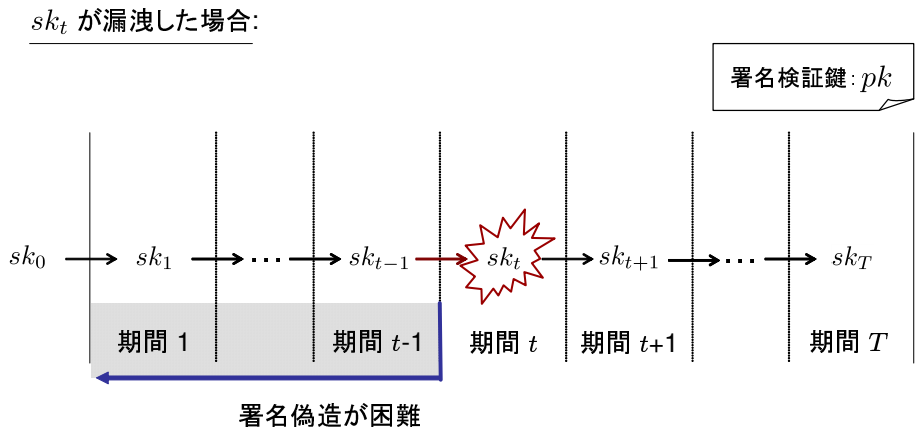

図 4: フォワード・セキュア署名の概要

もっとも、フォワード・セキュア署名が適切に機能するためには、どの時点の署名生成鍵が漏洩したのかを正確に検知することが必要であるが、そのための仕組みがフォワード・セキュア署名においてカバーされていないという問題点があ

る（高橋・洲崎・松本 [2002]）。したがって、フォワード・セキュア署名を実装する際には、署名生成鍵の漏洩を検知するための機構を別途準備することが求められる[5]。

ロ．キー・インシュレイティッド署名

キー・インシュレイティッド署名は、フォワード・セキュア署名と同様に、署名生成鍵を頻繁に更新することによって署名生成鍵の漏洩による署名の偽造の範囲を小さくしようというアイデアに基づいている（Dodis *et al.*[2002]）。ただし、キー・インシュレイティッド署名では、ある時点において署名生成鍵が漏洩したとしても、その署名生成鍵よりも古い署名生成鍵だけでなく新しい署名生成鍵をも導出することを困難にするという点でフォワード・セキュア署名とは異なる。このため、本署名では、署名生成鍵の漏洩がどの時点において発生したかは重要ではなくなる。

キー・インシュレイティッド署名では、署名生成鍵をベース鍵とユーザ鍵の 2 つに分ける。ベース鍵を sk^*、期間 t におけるユーザ鍵を sks_t とおいた場合の本署名方式の概要を図 5 に表わす。期間 t における署名生成は sks_t を用いて行われ、sks_t は、sk^* と sks_{t-1} を一方向性関数に入力することで得られる。したがって、仮に sks_t が漏洩していたとしても、sk^* が安全であるならば sks_{t-1} を導出することは困難であり、期間 $t+1$ 以降に生成されたとされる署名の偽造も困難であるという仕組みとなっている。また、署名生成鍵漏洩以前の期間における署名偽造も同様に困難である。

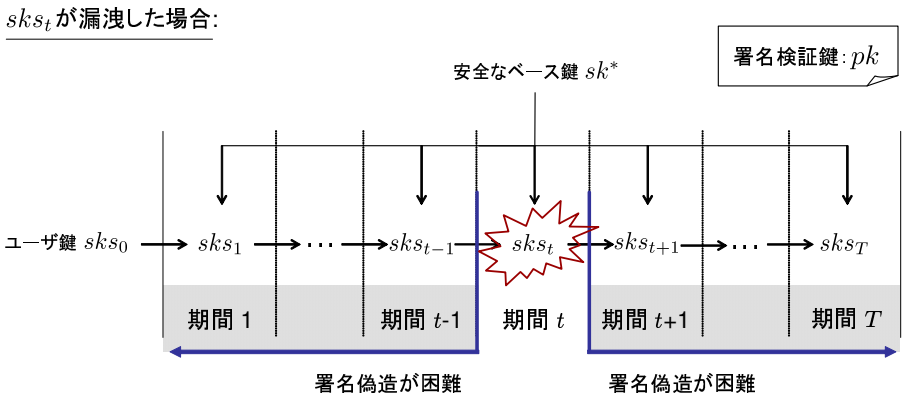

図 5: キー・インシュレイティッド署名の概要

[5] こうした問題点を意識し、署名生成鍵の漏洩を早期に検知するための機構が組み込まれたデジタル署名方式も提案されている（上山・四方・松本 [2003]）

ハ．イントリュージョン・レジリエント署名

イントリュージョン・レジリエント署名は、ベース鍵を更新させることによって、ベース鍵の物理的安全性の仮定を不要とした署名方式である（Itkis and Reyzin[2002]、Itkis[2003]）。イントリュージョン・レジリエント署名の場合、ベース鍵とユーザ鍵の両者ともに漏洩しない限り、ユーザ鍵が漏洩した期間以外に生成されたとされる署名の偽造は困難（キー・インシュレイティッド署名の性質）であり、両者が漏洩した場合であっても漏洩以前の期間に生成されたとされる署名の偽造は引続き困難（フォワード・セキュア署名の性質）である。

期間 t におけるベース鍵を skb_t、ユーザ鍵を sks_t とおいた場合のイントリュージョン・レジリエント署名の概要を図 6 に表わす。期間 t における署名生成は sks_t を用いて行われるが、sks_t は、sks_{t-1} と skb_{t-1} を一方向性関数に入力することで得られる。したがって、ユーザ鍵とベース鍵がともに漏洩しない限り、ユーザ鍵が漏洩した期間以外に生成したとされる署名を偽造することは困難である。また、期間 t までにユーザ鍵とベース鍵のいずれも漏洩した場合には、それ以降のユーザ鍵を導出できることから、期間 t 以降の署名偽造は可能となる。しかし、期間 $t-1$ 以前に生成されたとされる署名の偽造は引続き困難である。

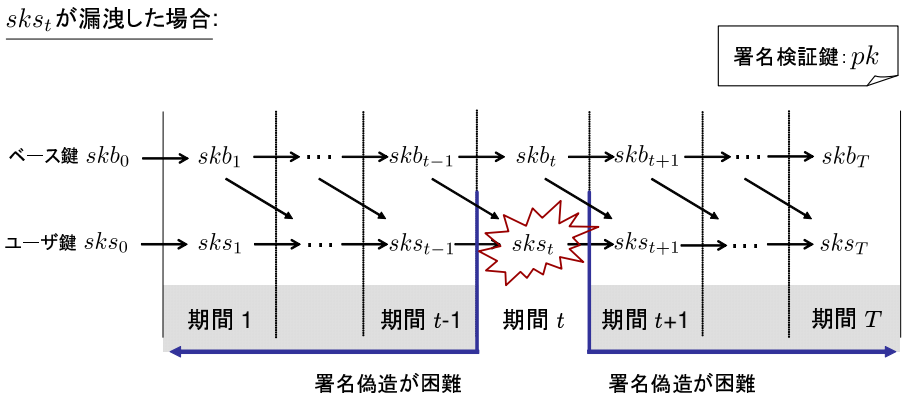

図 6: イントリュージョン・レジリエント署名の概要

ニ．ヒステリシス署名

ヒステリシス署名（hysteresis signature）は、デジタル署名が生成されたことのアリバイ（署名生成履歴）を偽造困難な形態で保管しておき、署名生成鍵が漏洩した場合でも、偽造された署名であるか否かを署名生成履歴との整合性確認によって判断する技術である（洲崎・松本 [2002]、宮崎ほか [2003]）。本署名では、署名を

生成する際にそれ以前の署名等を署名生成記録として署名に埋め込むことによって、その署名が過去のすべての署名を反映したかたちとなるという仕組みを採用している（図 7 参照）。複数の署名を生成した場合、それに伴って署名生成記録が連鎖構造を形成し、一連の署名生成記録は署名生成履歴として保管される（図 8 参照）。攻撃者が漏洩した署名生成鍵によって署名を偽造しようとした場合、単に署名のみを偽造しただけでは不十分であり、その署名の前後に生成されたとされるすべての署名も署名生成履歴と整合的になるように偽造しなければならず、攻撃のハードルが高くなると考えられる。ただし、そのためには、署名生成履歴を安全に保管しておくことが必要となる。

初期値を IV、ハッシュ関数を $\mathcal{H}$、署名生成関数を $Sign$、i 番目に生成される署名の対象となるメッセージを M_i、i 番目の署名生成記録を R_i としたときの署名生成、および、署名生成記録・署名生成履歴の構造を図 8 に示す。なお、$\mathcal{H}(R_i)||\mathcal{H}(M_i)$ は、$\mathcal{H}(R_i)$ と $\mathcal{H}(M_i)$ の結合（concatenation）を表わす。

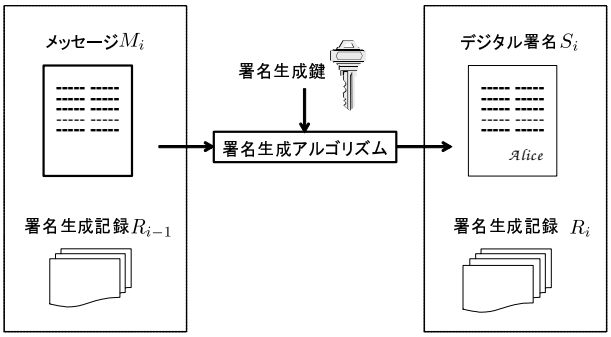

図 7: i 回目のヒステリシス署名生成の概要

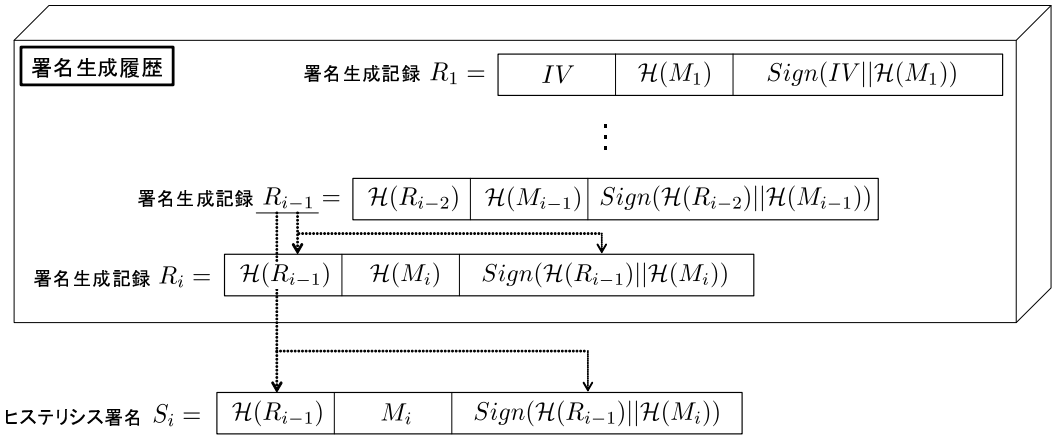

図 8: 署名生成記録の構造

i 回目のヒステリシス署名生成時において、署名者は、署名生成記録 R_{i-1} のハッシュ値 $\mathcal{H}(R_{i-1})$ を用いてヒステリシス署名 S_i を生成し、署名生成記録を R_i に更新したうえで署名生成履歴に R_i を追加する。検証者は、S_i を検証するとともに、安全に保管されている署名生成履歴の中に R_i が含まれていること、および、R_i 前後の署名生成記録の整合性が保たれていることを検証し、ヒステリシス署名が偽造されていないことを確認する。

ヒステリシス署名については、これまでにいくつかの評価研究の成果が発表されている。宮崎ほか [2003] は、ヒステリシス署名における検証結果の信頼度の概念を定めたうえで、署名生成履歴を管理するエンティティの信頼度が署名検証結果の信頼度にどのように影響するかを定量的に評価する手法を提案している。また、上田ほか [2004] は、ヒステリシス署名をコスト面から評価する手法を提案している。本手法では、署名生成履歴の一部が一定の確率で損失した場合のデータ損失コストと、署名生成履歴を管理するためのコストを定量的に評価することを可能にする。また、ECOM・JIPDEC の調査報告書（ECOM・JIPDEC[2004a]）では、ヒステリシス署名を用いた電子署名長期保存システム（DP1/Proofbox2:（株）日立製作所）も紹介されている。

ホ．実行ハードウエア確認タグ付き署名

実行ハードウエア確認タグ付き署名（以下、タグ付き署名と呼ぶ）は、検証対象の署名が特定のハードウエアにおいて生成された否かを確認することによって署名偽造を検知する技術である（松本・田中 [2000]、宇根・松本 [2002]）。どのハードウエアにおいて署名が生成されたかが明確になったとしても、その結果、当該署名が偽造されたものか否かが直ちに判明するとは限らない。しかし、通常署名生成鍵は IC カード等の特定のハードウエア内部において秘密に保管されるデータであり、特定のハードウエア以外において生成されたことが判明した署名は正規の手続に沿って生成された署名とはいえず、偽造されたものである可能性が高いと判断可能である。このような意味で、タグ付き署名も署名生成鍵の漏洩対策技術の 1 つと位置付けることができる。

タグ付き署名のポイントは、耐クローン・モジュール（clone resistant module）と呼ばれる特殊なモジュールを利用している点である。耐クローン・モジュールは、(i) 入出力を有する一種の関数として機能し、その入出力関係を再現可能な別のモジュールを複製することは困難である、(ii) 入力および出力の集合のサイズが極めて大きく、入出力関係を示すテーブルを格納できる記録媒体を準備することは困難であるという性質を有する（松本・田中 [2000]）。このようなモジュールは現時点では利用困難であるものの、耐クローン・モジュールを実現するためのアイ

デアがいくつか提案されているほか、その実現に向けた検討も行われている（松本・岩下 [2004]、松本ほか [2004]）。

タグ付き署名では、管理者と呼ばれるエンティティが、耐クローン・モジュールの入出力ペアを直接観察してその一部をテーブルとして保管したうえで、当該耐クローン・モジュールを署名生成用ハードウエアに組み込んで利用者に配布する。利用者は、署名生成を行う際に、管理者に対して耐クローン・モジュールの入力の送付を要求し、その入力に対する耐クローン・モジュールの出力と署名等からタグと呼ばれるデータを生成する。利用者は、そのタグを管理者に送付するほか、署名付きデータと結合してタグ付き署名とする。検証者は、タグ付き署名を構成する署名の検証を行うほか、タグ付き署名を管理者に提出し、タグの検証を依頼する。このように、タグ付き署名を実現するためには、耐クローン・モジュールの実現に加え、信頼できる第三者として管理者を準備することも必要となる。

へ．MAC 付きデジタル署名

MAC 付きデジタル署名（以下、MAC 付き署名と呼ぶ）は、署名生成の際に、署名対象のデータに対して MAC（message authentication code）を生成し、署名が偽造されたと疑われる場合には MAC を検証して偽造の有無を判定するという技術である（小森・松浦・須藤 [2001a,b, 2002]）。

MAC 付き署名において使用される署名生成用ハードウエアは、ハードウエア製造時にはデータの書込みが可能であるが、その後は書込みも不正な読出しも困難なメモリー領域を有し、その領域に MAC 生成用の秘密鍵が格納される。MAC 生成用の秘密鍵は署名生成用ハードウエアが利用されなくなるまで変更されないものの、署名生成鍵については、電子証明書更新時に新しい鍵を署名生成用ハードウエアに書き込むという処理が発生する。MAC 付き署名では、こうした書込みの際に署名生成鍵が漏洩する可能性を想定している。

MAC 付き署名の検証は、偽造されたと疑われている署名生成鍵が格納されている署名生成用ハードウエアを用いて MAC の生成を再現することによって実行される。偽造されたと疑われている署名とペアで保管されていた MAC と、再度生成された MAC を照合し、同一であれば当該署名は偽造されたものではないと判断され、そうでない場合には偽造されたものと判断されることとなる。

MAC 付き署名のポイントは署名生成用ハードウエア内に格納される MAC 生成用秘密鍵の安全性であり、本署名を実装した際に MAC 生成用秘密鍵が署名生成鍵とともに漏洩してしまうといった欠陥が現実に存在すると、どのような署名と MAC の偽造も検知不可能となる。こうした点を改善する手法として、MAC 生成用秘密鍵を署名生成ハードウエア内部において短い期間で更新するという方法が

提案されている（小森ほか [2003]）。更新の際には、新しい MAC 生成用秘密鍵から古い MAC 生成用秘密鍵を導出することが困難となるように一方向性関数が用いられているほか、更新後は古い鍵を破棄する仕組みとなっている。こうした鍵更新のアイデアは、前述のフォワード・セキュア署名と同様となっている。

5. ETSI TS 101 733 に基づく署名の再検証可能性

本節では、署名の長期利用を実現するための技術である ETSI TS の署名トークンについて分析を行う。ETSI TS は 10 種類の署名トークンを規定しており、これらのうち 6 つの署名トークンが、署名を長期利用する際の署名トークンとして推奨されている。前節で紹介したように、ETSI TS は IETF や W3C 等の技術仕様として規定されているほか、いくつかの商用サービスにも実装されているという実績をもつ。しかし、署名トークンの実装手法についてはいくつかの研究成果が発表されているものの（伊藤ほか [2004]、ECOM[2002]）、想定環境においてどのような条件が満足されていれば各署名トークンが期待どおりの効果を発揮するか否かに関しては、ETSI TS に記載されていない。

そこで、以下では、各署名トークンについて説明した後、ETSI TS において想定されているトラブルが実際に発生した状況のもとで、どのような条件が満足されるならば ETSI TS の署名トークンが効果を発揮し、原理的に署名再検証が可能となるのかを検討する。

(1) 想定環境

イ. エンティティ

ETSI TS が想定する環境は、認証機関、利用者、検証者に加え、調停者（arbitrator）、タイムスタンプ発行者（time-stamping authority）によって構成される。調停者とタイムスタンプ発行者の役割は次のとおりである。

- **調停者**: 利用者や検証者から中立的な立場にあり、利用者と検証者の間で署名の有効性に関して主張の相違が発生した場合、第三者の立場から署名の再検証を行うエンティティ。
- **タイムスタンプ発行者**: 署名トークンを構成するタイムスタンプを発行し、署名トークン内のデータが特定の日時に存在したことを証明するエンティティ。

ロ. タイムスタンプに関する想定

ETSI TS の署名トークンに利用されるタイムスタンプとしては、デジタル署名ベースの RFC3161（Adams, Cain *et al.*[2001]）に準拠したものが想定されているほか、以下の想定が置かれている。

1. タイムスタンプ生成用のデジタル署名方式には、利用者が用いる署名生成鍵

よりも長い鍵長の署名生成鍵が用いられる、あるいは、相対的に安全なアルゴリズムが採用される。

2. タイムスタンプ生成鍵は、厳重なセキュリティ管理のもとに置かれる。

3. 署名トークンに複数のタイムスタンプが含まれる場合、新しいタイムスタンプは古いタイムスタンプよりも高い安全性を有する、あるいは、異なるアルゴリズムを採用する。

4. タイムスタンプ検証用の証明書の有効期限が切れる前に、あるいは、タイムスタンプの安全性が低下する前に、より安全な新しいタイムスタンプを署名トークンに付与する。

このように、ETSI TS では、タイムスタンプ生成鍵の管理が利用者の署名生成鍵よりも厳重に管理されるケースを想定しているものの、後述するように、CA 署名生成鍵と同様にタイムスタンプ生成鍵も漏洩するという可能性を否定しているわけではない。ただし、CA 署名生成鍵とタイムスタンプ生成鍵が同時に漏洩するケースは想定されていないため、以下では、認証機関の署名生成鍵が漏洩するタイミングにおいて、タイムスタンプ生成鍵も同時に漏洩することはないと想定して議論を進めることとする。

(2) 10 種類の署名トークン

イ. BES

BES（basic electronic signature）は、RFC3852（cryptographic message syntax、Housley[2004]）の署名付きデータ（SignedData）に準拠した構成となっており、最も基本的な署名トークンである（図 9 参照）。本署名トークンは ETSI TS において「取扱いを可能とすることが必須」とされており、ETSI TS 準拠の署名生成・検証システムにおいては BES を利用可能であることが求められている。

本署名トークンの「署名生成者情報」に含まれる「署名データ（signature）」は、「署名の対象となる属性」から構成されるデータに対する利用者の署名である。また、「署名の対象となる属性」に含まれる「電子証明書識別子」は、利用者証明書を特定するデータであり、利用者証明書を発行した認証機関を表わすデータ、利用者証明書のシリアル番号、利用者証明書のハッシュ値から構成される。このため、利用者証明書のハッシュ値も「署名データ（signature）」の対象となっている。「ハッシュ関数識別子」については、「署名生成者情報」の外側と内側に組み込まれており、「署名生成者情報」の外側にある「ハッシュ関数識別子」には、当該 PKI

において利用が可能とされるハッシュ関数の識別子のリストが格納される。これに対して、「署名生成者情報」の内部にある「ハッシュ関数識別子」には、当該署名トークン生成に用いられるハッシュ関数（1 つ）の識別子が格納される。

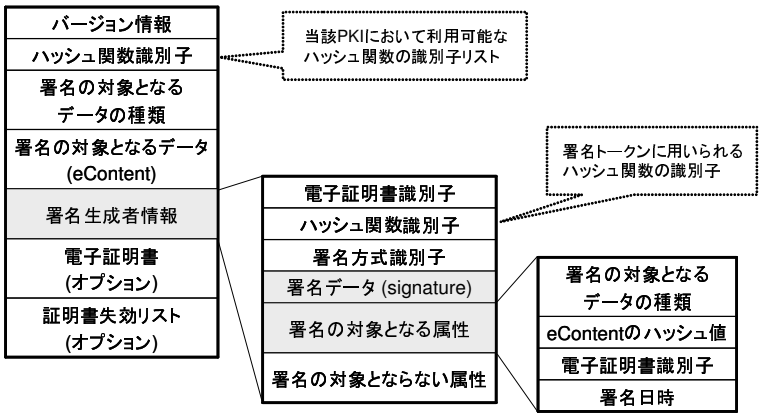

図 9: BES の構成

ロ. EPES

EPES（explicit policy electronic signature）は、署名ポリシーの識別子を BES に追加したものであり、当該署名がどの署名ポリシーに準拠したものかを明示する署名トークンである。署名ポリシーの識別子は、BES の「署名の対象となる属性」に追加される（図 10 参照）。

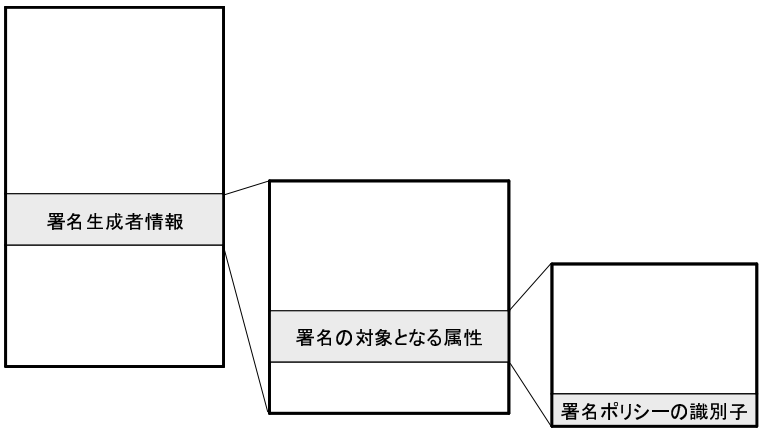

図 10: EPES の構成

ハ. ES-T

ES-T（electronic signature with time）は、BES あるいは EPES にタイムスタンプ（以下、TS-EST と記す）を追加する署名トークンである。TS-EST は「署名データ（signature)」に対するタイムスタンプであり、署名データ（signature）は電子証明書識別子に対して生成されるため、利用者証明書のハッシュ値に対して間接的にタイムスタンプが付与されるかたちとなっている。TS-EST には、RFC3161 に規定されるタイムスタンプ・トークン（TimeStampToken）が採用され、BES の「署名の対象とならない属性」の部分に格納される（図 11 参照)。

TS-EST は署名生成時点を推定するために署名トークンに付与されるものであり、ETSI TS には、利用者が署名生成直後にタイムスタンプ発行者から取得することが望ましいと記述されている。TS-EST はデジタル署名によって実現されることから、TS-EST を検証する、すなわち、TS-EST に含まれるタイムスタンプ発行者のデジタル署名を検証する際には、タイムスタンプ発行者の電子証明書の有効性等を検証する必要が出てくる。こうした検証に必要となる CA 証明書や CRL 等のデータも、タイムスタンプ発行者のデジタル署名と同様に TS-EST に格納されることとなっている。

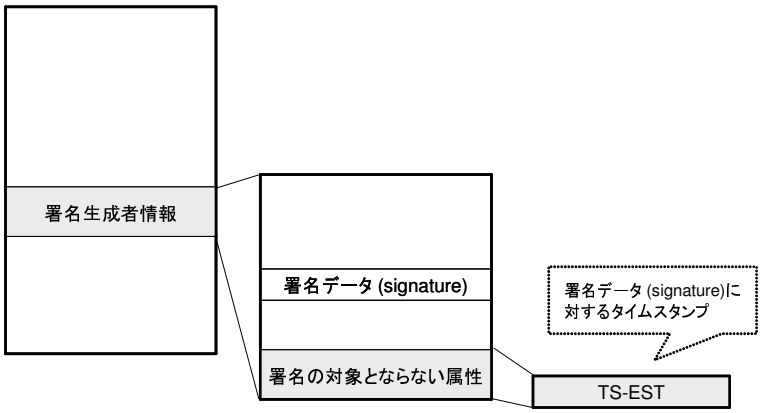

図 11: ES-T の構成

ニ. ES-C

ES-C（electronic signature with complete validation data references）は「認証パス上に位置する電子証明書の参照データ」と「失効情報の参照データ」を ES-T の「署名の対象とならない属性」に追加したものである（図 12 参照)。ただし、「認証パス上に位置する電子証明書の参照データ」には、ルート認証機関（ETSI

TS においては “trusted CA” と記述されている）が発行する証明書の参照データも含まれる扱いとなっているものの、「失効情報の参照データ」には、ルート認証機関の証明書の失効情報は含まれないこととなっている点には留意が必要である。

「認証パス上に位置する電子証明書の参照データ」は、電子証明書のハッシュ値（必須）と電子証明書の発行者を識別するデータ（オプション）から構成される。「失効情報の参照データ」については、CRL の場合、CRL のハッシュ値（必須)、CRL 発行者の識別データ（以下、オプション)、発行日時、シリアル番号から構成される。OCSP メッセージの場合、OCSP メッセージ生成者の識別データ（必須)、生成日時（必須)、ハッシュ値（オプション）から構成される。また、CRL や OCSP メッセージ以外の形態で失効情報を格納することも可能となっている。

検証者は、ES-C を用いることによって、認証機関のリポジトリに改めて問い合わせすることなく「認証パス上に位置する電子証明書の参照データ」と「失効情報の参照データ」を得ることができる。ただし、これらのデータが実際に保管される具体的な場所や保管方法については記述されていない[6]。

失効情報については、ETSI TS では、電子証明書の失効申請から CRL への反映までに一定のタイム・ラグが存在する可能性を考慮し、署名生成から一定時間が経過した後に CRL を入手して署名トークンを形成することとされている。この「一定期間」について具体的な記述はないが、CRL の場合では、署名生成後に新しく更新された CRL を入手するまでの期間に相当すると考えられる。

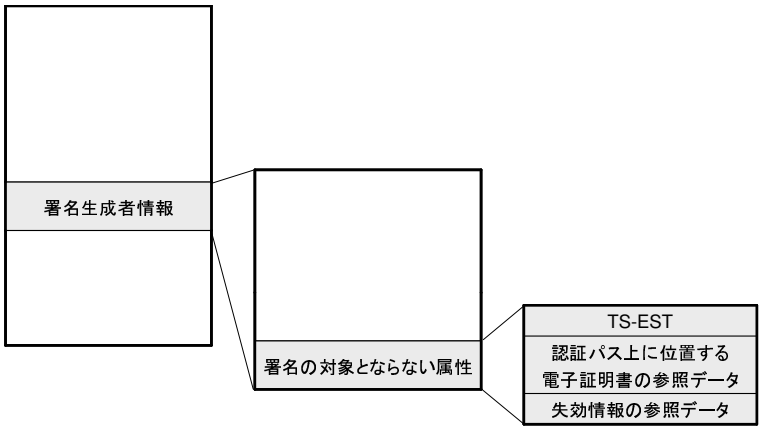

図 12: ES-C の構成

[6]ETSI TS では、“Storing the references allows the values of the certification path and the CRLs or OCSPs responses to be stored elsewhere, reducing the size of a stored electronic signature format” とのみ記述されている

ホ. ES-X Long

ES-X Long（extended long electronic signature）は、署名の長期利用の際に推奨されている署名トークンの 1 つであり、認証パスを構成する電子証明書と失効情報を署名トークンに組み込むことで、これらのデータを署名トークン以外から入手困難なケースにも対応できるとされている。ES-X Long は、ES-C の「署名の対象とならない属性」の部分に、「認証パス上に位置する電子証明書」と「失効情報」を組み込んだ形態となっている（図 13 参照）。

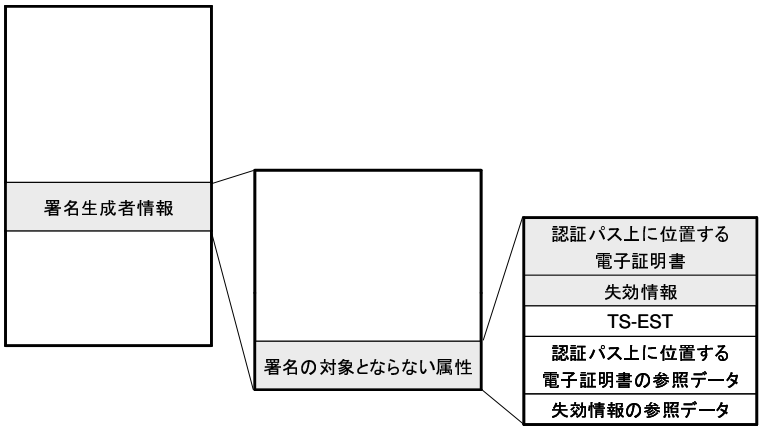

図 13: ES-X Long の構成

ヘ. ES-X Type1

ES-X Type1（extended electronic signature with time type1）も、署名の長期利用の際に推奨されている署名トークンの 1 つであり、ES-C にタイムスタンプ（以下、TS-Type1 と記す）を追加したものである（図 14 参照）。TS-Type1 は、「署名データ（signature）」、TS-EST、「認証パス上に位置する電子証明書の参照データ」、「失効情報の参照データ」に対して付与され、ES-C の「署名の対象とならない属性」に追加される。本署名トークンは、CA 署名生成鍵が漏洩した場合、あるいは、漏洩したと疑われる場合に対応できるとされている。

ト. ES-X Type2

ES-X Type2（extended electronic signature with time type2）も、CA 署名生成鍵が漏洩した場合、あるいは、漏洩したと疑われる場合にも対応できるとされている署名トークンである。ES-X Type1 との相違点はタイムスタンプの対象となる

データにある。ES-X Type2 では、TS-Type1 の代わりに、「認証パス上に位置する電子証明書の参照データ」と「失効情報の参照データ」に対するタイムスタンプ（以下、TS-Type2 と記す）が含まれる（図 14 参照）。

ES-X Type1 と ES-X Type2 におけるタイムスタンプの相違点について、ETSI TS では、「ES-X Type2 は、同一の署名生成鍵によって生成される複数のデジタル署名において、同一の参照データを添付する場合、タイムスタンプの生成処理の回数を ES-X Type1 に比べて少なくすることができる」と説明しており、CRL が更新される間に大量の署名を生成するようなアプリケーションにおいては ES-X Type2 が計算量の観点で相対的に有用であるとしている。いったん TS-Type2 を生成しておけば、CRL が次に更新されるまでの間には TS-Type2 の対象となるデータは変化しないため、その間に生成される署名トークンに上記 TS-Type2 を組み込むことができる。

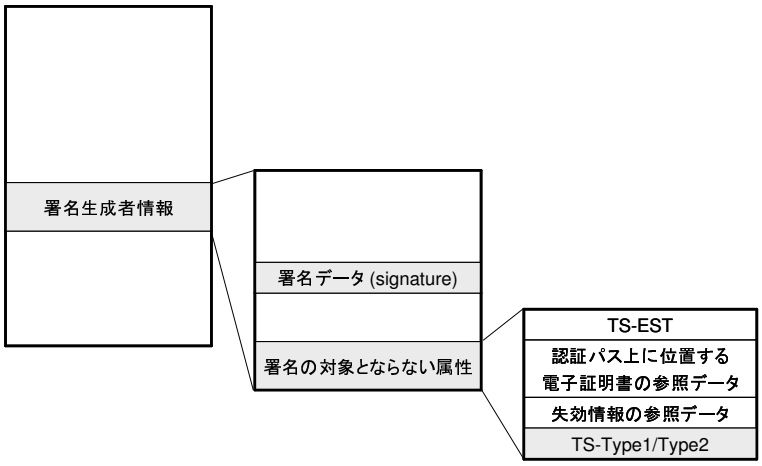

図 14: ES-X Type1/Type2 の構成

チ. ES-X Long Type1

ES-X Long Type1（extended long electronic signature with time type1）は、ES-X Type1 の「署名の対象とならない属性」に、「認証パス上の電子証明書」および「失効情報」を追加する署名トークンである（図 15 参照）。ETSI TS では、署名トークン以外から電子証明書や失効情報を入手できなくなった場合、および、CA 署名生成鍵が漏洩した場合に対応できるとされている。

リ. ES-X Long Type2

ES-X Long Type2（extended long electronic signature with time type2）は、ES-X Type2 の「署名の属性とならない属性」に、「認証パス上に位置する電子証明書」および「失効情報」を格納する署名トークンである（図 15 参照）。本署名トークンも、ES-X Long Type1 と同様に、署名トークン以外から電子証明書や失効情報を入手できなくなった場合、および、CA 署名生成鍵が漏洩した場合に対応できるとされている。

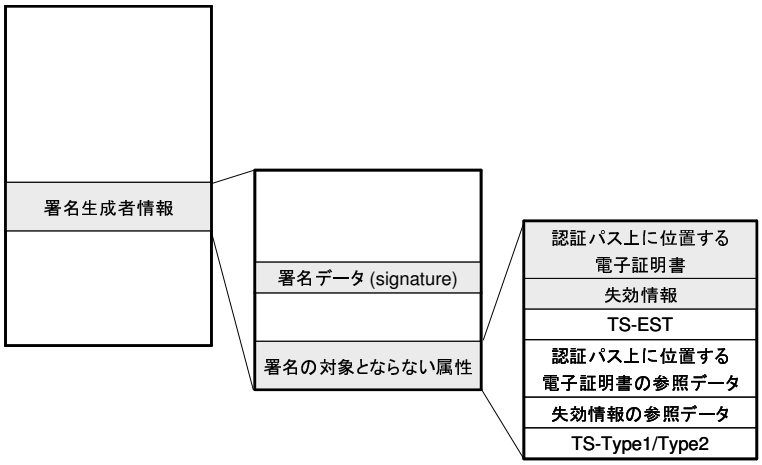

図 15: ES-X Long Type1/Type2 の構成

ヌ. ES-A

ES-A（archival electronic signature）は、ES-X Long、ES-X Long Type1、ES-X Long Type2 のいずれかにおいて、署名トークンを構成するデータ全体に対するタイムスタンプ（以下、TS-ESA と記す）を入手し、TS-ESA を「署名の対象とならない属性」に組み込む署名トークンである（図 16 参照）。本署名トークンでは、署名トークン以外から電子証明書や失効情報を入手できなくなった場合、CA 署名生成鍵が漏洩した場合に加え、署名トークンに含まれるタイムスタンプ（ただし TS-ESA を除く）やハッシュ関数（ただし TS-ESA に採用されているものを除く）の安全性が低下した場合にも対応可能であるとされている。

TS-ESA の安全性低下に関して、ETSI TS では、TS-ESA の安全性が低下した場合には、古い TS-ESA で利用されていたものとは別のアルゴリズムに基づいて新しい TS-ESA を ES-A 全体に対して再度生成し、ES-A の「署名の対象とならな

い属性」に追加することとしている。その場合、新しく生成された TS-ESA が古い TS-ESA よりも高い安全性を実現するために、タイムスタンプ用の署名生成鍵の鍵長を長くしたり、別の署名方式を採用するといった配慮が求められている。

ECOM の調査報告書（ECOM[2002]）の中で示されている電子署名文書長期保存システムでは、デジタル署名は ES-A の形式で長期保存されることが望ましいとされている。

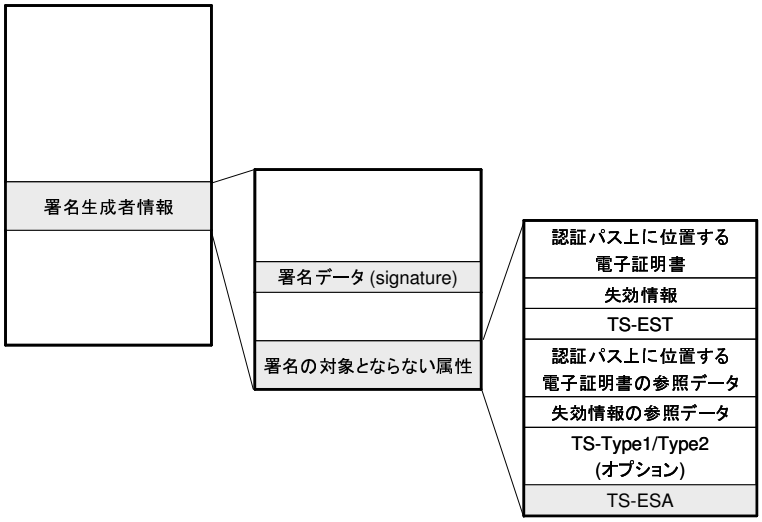

図 16: ES-A の構成

ル. ETSI TS の推奨署名トークン

ETSI TS では、デジタル署名を長期にわたって再検証可能な状態としておく際に考慮すべきトラブルとして 3 つの状況を想定し、調停者による署名再検証を可能とするよう、それぞれに対応可能な署名トークンを推奨している。各トラブルに対応可能とされている署名トークンは次のとおりである。

1. 認証パス上に位置する電子証明書および失効情報を署名トークン以外から入手困難な場合: ES-X Long、ES-X Long Type1、ES-X Long Type2、ES-A
2. 認証パス上に位置するいずれかの CA 署名生成鍵（電子証明書、CRL、OCSP メッセージ生成用）が漏洩した場合: ES-X Type1、ES-X Type2、ES-X Long Type1、ES-X Long Type2、ES-A
3. タイムスタンプやハッシュ関数の安全性が低下した場合: ES-A

ES-X Type1、ES-X Type2 は上記 1. の推奨署名トークンに含まれないほか、ES-X Long は上記 2 の推奨署名トークンに含まれないが、それらの効果の違いを明確にするため、以下では、ES-X Long、ES-X Type1、ES-X Type2、ES-X Long Type1、ES-X Long Type2、ES-A の 6 種類の署名トークンに対して上記 1.、2. の状況を想定した署名トークンの効果を検討する。上記 3. で挙げられているタイムスタンプやハッシュ関数の安全性低下については、以下の検討では想定しないこととする。

上記 1. の状況が具体的にどのようなケースを指すのかについては、ETSI TS には詳しく記述されていない。ただし、ETSI TS では、通常の PKI のほかにタイムスタンプ発行者と調停者が存在する環境を想定しており、それ以外の特殊なエンティティは登場しない。こうした点を考慮すると、CA 証明書や CRL といった署名検証に必要なデータは PKI の枠組みの中で保管される、すなわち、認証機関のリポジトリやアーカイブで保管されることを想定していると考えることができる。その場合、上記 1. の状況は、主として、認証機関のトラブルやアーカイブでの保管期間満了といった事由によって発生することを前提にしたものであると思われる。

なお、署名の長期利用における問題の 1 つである「利用者署名生成鍵の漏洩」については ETSI TS では触れられていない。しかし、CA 署名生成鍵の漏洩を想定していることを考慮すると、利用者署名生成鍵の漏洩が発生する状況も想定しておくことが自然であると考えられる。したがって、ETSI TS が想定する状況における各署名トークンの効果の検討の後、利用者署名生成鍵の漏洩時の効果についても考察を行うこととする。

(3) 署名トークン以外から再検証に用いるデータを入手不可能な場合の署名再検証可能性

ここでは、まず本節 (2) ル. の 1. で説明した状況、すなわち、調停者が電子証明書や失効情報を署名トークン以外から入手不可能となる状況を想定する。そのうえで、3 節 (3) において整理した署名再検証に係る処理が、調停者によって実行可能か否かに焦点をあて、どのような条件のもとで署名再検証が実行可能となるかを検討する。

本節 (2) で説明したように、ETSI TS の署名トークンでは、利用者証明書を署名トークン内に格納するか否かについては任意としているが、通常はデジタル署名と利用者証明書は一緒に管理される場合が多い。したがって、以下の検討においては、各署名トークン内に利用者証明書が格納されるものとする。

イ. ES-X Long による再検証可能性

ES-X Long には、利用者証明書、CRL、CA 証明書、CRL の参照データ、CA 証明書の参照データが含まれる。したがって、調停者は署名トークンから、3 節 (3) のデータ 3（利用者証明書)、データ 5（CRL）を入手可能である。しかし、CA 証明書失効情報が含まれておらず、調停者はデータ 1（CA 証明書失効情報）を入手することができない。また、ES-X Long には CA 証明書が含まれるが、それらが認証機関によって発行されたことを署名トークン内のデータから確認することが困難であり、データ 2、データ 4 （認証機関によって発行されたことが確認可能な CA 証明書）も入手不可能である。この結果、調停者は 3 節 (3) の処理 1〜5 を実行することができず、本稿で想定している通常の署名再検証の手続に沿って、ES-X Long に含まれるデータのみを用いた署名再検証は困難であるといえる。

ただし、以下の条件 A〜C が満たされ、データ 1、2、4 を別途入手可能であるならば、処理 1〜5 を実行可能となり ES-X Long による署名再検証も可能となる。

- **条件 A**: 調停者は、認証機関が公表したと認められる CA 証明書失効情報を入手する。
- **条件 B**: 調停者は、認証機関によって発行されたことが確認可能であり、t_S を有効期間に含む利用者証明書検証用 CA 証明書を入手する。
- **条件 C**: 調停者は、認証機関によって発行されたことが確認可能であり、t_S を有効期間に含む CRL 検証用 CA 証明書を入手する。

以上より、ES-X Long による署名再検証を可能とするための十分条件は、**条件 A かつ条件 B かつ条件 C** であるといえる。

ロ. ES-X Type1 と ES-X Type2 による再検証可能性

ES-X Type1 と ES-X Type2（以下、ES-X Type1/Type2 と略す）には、利用者証明書、3 つのデータ（利用者証明書、CA 証明書、CRL）に対する参照データが含まれるほか、これらのデータに対するタイムスタンプも含まれる。具体的には、利用者証明書の参照データに対しては TS-EST が付与され、その他の参照データに対しては TS-Type1 もしくは TS-Type2 が付与される。しかし、署名トークンからは 3 節 (3) で整理したデータ 1、2、4、5 が入手できず、ES-X Type1/Type2 内のデータのみを用いた署名再検証の実行は困難である。ただし、条件 D を、

- **条件 D**: 調停者は、発行時刻が t_S として記載される CRL を入手する。

と置き、条件 A〜D が満足されるならば、調停者はデータ 1〜5 を入手して処理 1〜5 を実行可能となる。以上より、ES-X Type1/Type2 による署名再検証を可能とするための十分条件は**条件 A かつ条件 B かつ条件 C かつ条件 D** となる。

ハ. ES-X Long Type1 と ES-X Long Type2 による再検証可能性

ES-X Long Type1 と ES-X Long Type2（以下、ES-X Long Type1/Type2 と略す）には、利用者証明書、CRL、CA 証明書が含まれるほか、これらのデータの参照データに対するタイムスタンプである TS-Type1 もしくは TS-Type2 が含まれる。しかし、署名トークンには CA 証明書失効情報が含まれず、調停者はデータ 1 を入手できない。また、署名トークンに含まれる CA 証明書が認証機関によって発行されたことを確認することが困難であることから、データ 2、4 も署名トークンから入手できないことになる。ただし、データ 1、2、4 が入手可能であれば署名再検証を実行可能となることから、ES-X Long Type1/Type2 において署名再検証を可能とするための十分条件は ES-X Long の場合と同様に**条件 A かつ条件 B かつ条件 C** となる。

ES-X Long Type1/Type2 には、CA 証明書の参照データに対するタイムスタンプ TS-Type1 と TS-Type2 がそれぞれ付与されているが、これらは特定日時に CA 証明書が存在したことを示す効果をもつ。しかし、これらのタイムスタンプは、それだけでは CA 証明書が認証機関によって発行されたことを示すものではない。例えば、検証者やその他のエンティティが、適当な 2 種類の CA 証明書、利用者証明書、CRL の組を生成し、タイムスタンプを得て署名トークン全体を偽造するという攻撃も考えられる。

ニ. ES-A による再検証可能性

ES-A には、利用者証明書、CRL、CA 証明書が含まれるものの、ES-X Long、ES-X Long Type1/Type2 と同様に、データ 1、2、4 が含まれない。したがって、ES-A において署名再検証が実行可能となる十分条件も**条件 A かつ条件 B かつ条件 C** となる。

なお、ES-A に含まれるデータにはタイムスタンプ（TS-ESA）が付与される。TS-ESA は、署名トークンが特定日時に存在したことを確認する際に利用できるものの、TS-Type1 や TS-Type2 と同様に、署名トークンを構成する CA 証明書や CRL が認証機関によって発行されたことを示すものではない。

ホ. 考察

以上の検討結果は、以下の 2 点に整理することができる（表参照）。

1. ETSI TS が推奨している ES-X Long、ES-X Long Type1/Type2、ES-A のいずれにおいても、署名再検証が実行可能となるための十分条件は同一となる。すなわち、当該認証機関によって発行され、署名生成時点において有効であった CA 証明書を入手できれば、署名再検証可能である。

2. 推奨されているわけではない ES-X Type1/Type2 に関しては、推奨されている署名トークンに比べて、署名生成時点において発行された CRL を入手するという条件が十分条件に加わる。

以上の 2 点は、ETSI TS の署名トークンに含まれるデータが CA によって発行されたか否かを確認する手段、および、失効の有無を確認するための手段が準備されていないことを示すものである。したがって、署名トークン内のデータのみを利用せざるを得ない状況を想定する場合、CA 証明書の有効性を別途確認する手段をどのように確保するかについて検討することが必要である。

表 1: 署名再検証のための十分条件

署名トークン	十分条件
ES-X Long	A ∧ B ∧ C
ES-X Type1/Type2	A ∧ B ∧ C ∧ D
ES-X Long Type1/Type2	A ∧ B ∧ C
ES-A	A ∧ B ∧ C

（備考）表を見やすくするため、例えば条件 A は“ A ”と記している。また、∧ は“ かつ ”を表わすものとする。

既存の PKI の枠組み以外の仕組みを用いて上記課題に対応する方法としては、信頼できるエンティティが運営するセキュア・ストレージ・サービスの利用、他の利用者や各種メディアにおいて分散して保管されていたデータの利用が考えられる。

(イ) セキュア・ストレージ・サービスの利用

セキュア・ストレージ・サービスを利用する場合、次のような手続が考えられる。利用者と検証者は、署名トークン生成時に、セキュア・ストレージ・サービスの提供者（以下、単にサービス提供者と呼ぶ）に署名トークンの保管を依頼する。

その際、サービス提供者は、署名トークン内のCA証明書が確かに認証機関によって発行されたという事実を確認したうえで、CA証明書失効情報を入手し、CA証明書が失効していないことも確認する。その後、サービス提供者は、署名トークンをCA証明書失効情報とともに署名再検証に備えて保管する[7]。

こうしたサービスを利用できれば、後日、調停者は当サービスから入手した署名トークンに含まれるデータが認証機関によって発行されたと判断する根拠を得ることができ、署名検証に必要なデータすべてを入手可能となる。ただし、セキュア・ストレージ・サービスの提供者は利用者や検証者から信頼されていなければならない[8]。したがって、このようなサービスを実現するには相応のコストが必要となり、追加的なコスト負担が利用者や検証者に対して求められる。

ストレージ・サービスを用いた署名の長期利用形態は、ECOMによって電子署名文書長期保存システムとして提案されている（ECOM[2002]）ほか、いくつかの商用サービスも提供されている。実際に、こうした商用サービスを利用する際には、アプリケーションの実装環境において要求されるサービス運営主体の信頼度、アルゴリズムの強度、事故・災害への対応、サービス運営主体がサービス提供を中止した場合の対応等についてチェックすることが必要であろう。

(ロ) 分散するデータの利用

署名生成時点において有効であったCRL、CA証明書、CA証明書失効情報は、当該利用者以外のエンティティやメディアにおいても利用され、分散して保管されていると考えるのが自然である。したがって、特殊なシステムを導入しなくても、こうした分散したデータを保管するエンティティやメディアに対して、署名トークン内のデータとの整合性確認を依頼することによって、認証機関が発行したデータか否かを確認することができる可能性もある。このようなデータは、集中管理される認証機関のアーカイブやセキュア・ストレージ・サービスとは異なり、一部地域において災害や事故等が発生した場合でも活用できるという利点をもつ。また、信頼できる第三者を準備・利用する必要もない。

しかし、署名生成時点から長い時間が経過した後に再検証を実行する場合、そうした過去のデータを信頼に足るだけ十分に利用できるか否かという問題が残る。また、署名生成時点において当該PKIサービスを利用していたエンティティに対して個別にデータ照合の要請を行う等の手間も必要となるだろう。

---

[7] このように、セキュア・ストレージ・サービスにおいて必要とされる主たる機能は宮崎ほか[2003]で定義されている「存在保証」の機能に該当すると考えられる。

[8] こうした信頼を勝ち得る手段として、例えば、保管対象のデータに対して他のタイムスタンプ・サービスからタイムスタンプの発行を受けるといった方法も考えられる。

(4) CA 署名生成鍵が漏洩した場合の署名再検証可能性

ここでは、本節 (2) ル. の 2. に相当する、CA 署名生成鍵が漏洩した状況を想定し、各署名トークンによる署名再検証について検討を行う。

イ. 検討対象とする 3 つの状況

まず、CA 署名生成鍵が漏洩した場合の状況を整理する。調停者は、CA 署名生成鍵が漏洩していた事実を何らかの手段によって確認できたとする。このとき、利用者による署名生成と CA 署名生成鍵の漏洩の時間的前後関係を調停者が知る場合と知らない場合が想定され、次の 3 つに整理できる。

- **状況 1**: 調停者は、署名生成後に CA 署名生成鍵が漏洩したことを知る。
- **状況 2**: 調停者は、署名生成前に CA 署名生成鍵が漏洩したことを知る。
- **状況 3**: 調停者は、CA 署名生成鍵の漏洩時期を知らない。

以上の各状況のもとで、利用者証明書生成鍵または CRL 生成鍵が漏洩した場合について、それぞれ十分条件を導出する。以下では、CA 署名生成鍵が漏洩した時点を t_C とおく（図 17 参照）。

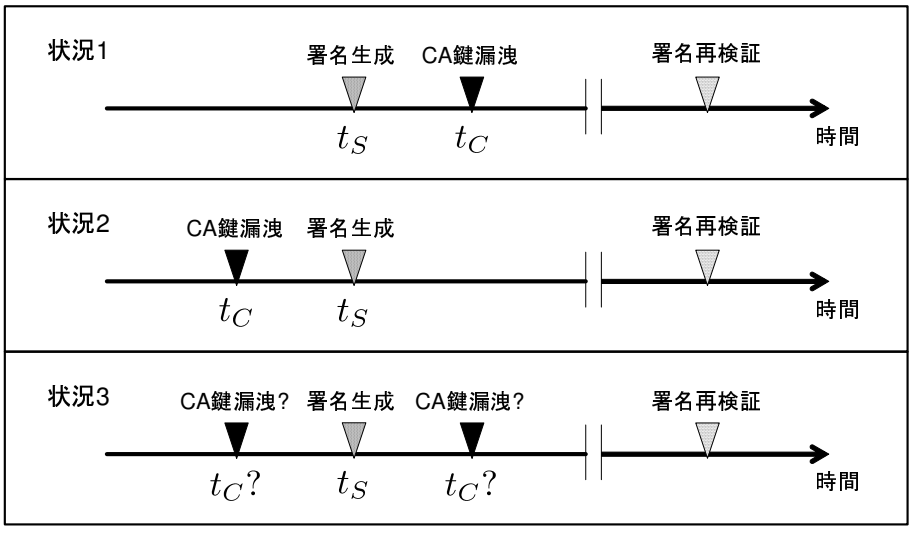

図 17: 3 つの状況

ロ. 状況 1 において利用者証明書生成鍵が漏洩した場合

いずれの署名トークンにおいても、タイムスタンプ（TS-EST）によって、利用者証明書が鍵が漏洩する以前に発行されたことを確認可能であり、利用者証明書生成鍵の漏洩が署名トークンを用いた再検証可能性に与える影響はない。このため、本節 (3) において導出した十分条件（表に示されるもの）がそれぞれ満たされるならば、各署名トークンにおいて 3 節 (3) における処理 1〜5 に沿って署名再検証を実行可能である。

ハ. 状況 1 において CRL 生成鍵が漏洩した場合

本ケースでは、調停者は t_C 以前に発行された CRL を入手する必要があり、署名トークンによって十分条件が異なる。

(イ) ES-X Long による再検証可能性

ES-X Long に含まれる CRL にはタイムスタンプが付与されていないため、CRL が t_C 以前に発行されたものであるか否かを判断することは不可能である。ただし、本節 (3) イ. における ES-X Long を用いた署名再検証のための十分条件に加え、t_S において発行されたことが確認可能な CRL を入手できれば、データ 1〜5 を入手可能となり、署名再検証は実行可能となる。この結果、条件 E を、

- **条件 E**: 調停者は、t_S において発行されたことが確認可能な CRL を入手する。

とおくと、ES-X Long における十分条件は**条件 A かつ条件 B かつ条件 C かつ条件 E** となる。

(ロ) ES-X Type1 と ES-X Type2 による再検証可能性

調停者は、発行日時が t_S と記載されている CRL を入手することができれば、ES-X Type1/Type2 に含まれる CRL の参照データに対するタイムスタンプ（TS-Type1/Type2）を用いて、当該 CRL が t_C 以前に発行されたことを確認することができる。したがって、十分条件は本節 (3) ロ. と同様に、**条件 A かつ条件 B かつ条件 C かつ条件 D** となる。

(ハ) ES-X Long Type1 と ES-X Long Type2 による再検証可能性

調停者は、TS-Type1/Type2 を用いることによって、署名トークン内の CRL が t_C 以前に発行されたことを確認可能である。したがって、本節 (3) ハ. と同様に、

十分条件は**条件 A かつ条件 B かつ条件 C** となる。

(ニ) ES-A による再検証可能性

調停者は、ES-A に含まれるタイムスタンプ（TS-ESA）を用いることによって、署名トークン内の CRL が t_C 以前に発行されたことを確認できる。したがって、十分条件は、本節 (3) ニ. と同様に**条件 A かつ条件 B かつ条件 C** となる。

ニ. 状況 2 において利用者証明書生成鍵が漏洩した場合

本ケースでは、t_C 以降は利用者証明書の偽造が可能であることから、t_S において署名トークン生成に用いられた利用者証明書も偽造されたとの疑いが生じる。したがって、署名トークン内に含まれる利用者証明書が認証機関によって発行されたことを 3 節 (3) の処理 2 では確認できず、利用者証明書検証用 CA 証明書を用いる方法とは別の手段が必要となる。そこで、条件 F を、

- **条件 F**: 調停者は、認証機関によって発行されたことが確認可能であり、t_S を有効期間に含む利用者証明書を入手する。

と置くと、各署名トークンの十分条件は以下のとおりとなる。

- ES-X Long: **条件 A かつ条件 C かつ条件 F**
- ES-X Type1/Type2: **条件 A かつ条件 C かつ条件 D かつ条件 F**
- ES-X Long Type1/Type2: **条件 A かつ条件 C かつ条件 F**
- ES-A: **条件 A かつ条件 C かつ条件 F**

このように、表 1 で整理した各署名トークンの十分条件に条件 F を追加する形となっているが、3 節 (3) の処理 2 を行わないため条件 B は不要となる。

ホ. 状況 2 において CRL 生成鍵が漏洩した場合

本ケースでは、t_C 以降は CRL の偽造が可能であることから、t_S において署名トークンの生成に用いられた CRL が偽造されたものであるか否かの判断が困難となる。このため、3 節 (3) の処理 4 では、CRL が認証機関によって発行されたものであることを確認できないことから、CRL 検証用 CA 証明書を用いる方法とは別の手段によって確認することになる。そこで、条件 G を、

- **条件 G**: 調停者は、認証機関によって発行されたことが確認可能であり、発行時刻が t_S として記載されている CRL を入手する。

と置くと、いずれの署名トークンにおいても十分条件は**条件 A かつ条件 B かつ条件 G** となる。この場合も、表 1 で整理した十分条件に条件 G を追加した形となるが、3 節 (3) の処理 4 を行わないため、条件 C は不要となる。また、ES-X Type1/Type2 においては、条件 G が満足されるとき条件 D は自動的に満足されるため十分条件から除かれる。

へ. 状況 3 において利用者証明書生成鍵が漏洩した場合

状況 1 と状況 2 のいずれの場合においても署名再検証可能であれば、状況 3 においても署名再検証は実行可能となる。したがって、各署名トークンにおける十分条件は次のとおりとなる。

- ES-X Long: **条件 A かつ条件 C かつ条件 F**
- ES-X Type1/Type2: **条件 A かつ条件 C かつ条件 D かつ条件 F**
- ES-X Long Type1/Type2: **条件 A かつ条件 C かつ条件 F**
- ES-A: **条件 A かつ条件 C かつ条件 F**

このように、状況 3 における十分条件は、状況 2 の十分条件に一致することとなる。

ト. 状況 3 において CRL 生成鍵が漏洩した場合

状況 3 における十分条件は、状況 1 と状況 2 のいずれの場合においても署名再検証可能とするものであればよいため、いずれの署名トークンにおいても、状況 2 と同様に、**条件 A かつ条件 B かつ条件 G** が十分条件となる。

チ. 考察

CA 署名生成鍵が漏洩した場合の署名再検証の可能性に関する検討結果を整理すると次のとおりである（表、参照）。

1. 状況 1 における十分条件は、CRL 生成鍵が漏洩した場合の ES-X Long 以外については、CA 署名生成鍵が漏洩しない場合の十分条件と同一となる。すなわち、調停者は、ES-X Type1/Type2 の場合は、外部から CA 証明書失効

情報、当該認証機関によって発行された CA 証明書、CRL を入手すればよい。また、ES-X Long Type1/Type2、ES-A の場合は、CA 証明書失効情報、当該認証機関によって発行された CA 証明書を入手できればよい。ただし、ES-X Long においては、署名トークン内に含まれる CRL にタイムスタンプが付与されていないため、CRL 生成鍵が漏洩した場合には、当該生成鍵の漏洩以前に発行されたものであることを別途確認する必要がある。

2. 状況 2、3 においては、本稿で想定した一般的な署名再検証の処理では、利用者証明書あるいは CRL が認証機関によって発行されたことを確認することが困難となる。この場合、別の手段を用いて認証機関によって発行されたと認められる利用者証明書や CRL を入手する、または、署名トークンに含まれる利用者証明書や CRL が認証機関によって発行されたことを別の手段で確認することができるならば、署名再検証が可能となる。

表 2: 利用者証明書生成鍵漏洩時における十分条件

署名トークン	各ケースにおける十分条件		
	鍵漏洩のない状況	状況 1	状況 2、3
ES-X Long	A ∧ B ∧ C		A ∧ C ∧ F
ES-X Type1/Type2	A ∧ B ∧ C ∧ D		A ∧ C ∧ D ∧ F
ES-X Long Type1/Type2	A ∧ B ∧ C		A ∧ C ∧ F
ES-A	A ∧ B ∧ C		A ∧ C ∧ F

表 3: CRL 生成鍵漏洩時における十分条件

署名トークン	各ケースにおける十分条件		
	鍵漏洩のない状況	状況 1	状況 2、3
ES-X Long	A ∧ B ∧ C	A ∧ B ∧ C ∧ E	A ∧ B ∧ G
ES-X Type1/Type2	A ∧ B ∧ C ∧ D		A ∧ B ∧ G
ES-X Long Type1/Type2	A ∧ B ∧ C		A ∧ B ∧ G
ES-A	A ∧ B ∧ C		A ∧ B ∧ G

このように、CA 署名生成鍵の漏洩を想定した場合、ETSI が推奨する署名トークンにおいては、状況 1 ではタイムスタンプが効果を発揮するため、通常の署名再検証時（CA 署名生成鍵が漏洩していない状況）に入手することが予定されているデータを入手すれば、CA 署名生成鍵の漏洩が発生しても署名再検証が可能

となる。これに対して、状況 2、 3 においては、タイムスタンプが効果を発揮せず、通常の署名検証時に予定されている方法以外の方法によって、利用者証明書や CRL が認証機関によって発行されたことを確認することが求められる。したがって、ETSI TS の署名トークンが CA 署名生成鍵漏洩時における対策として有効か否かは、鍵漏洩のタイミングと調停者によるその検知可能性に依存すると考えられる。

また、利用者証明書生成鍵と CRL 生成鍵が同一である場合など、これらの CA 署名生成鍵が同時に漏洩したときの十分条件は、それぞれの十分条件をともに満足するものとなる（表参照)。

表 4: CA 署名生成鍵漏洩時における十分条件

署名トークン	各ケースにおける十分条件		
	鍵漏洩のない状況	状況 1	状況 2、3
ES-X Long	A ∧ B ∧ C	A ∧ B ∧ C ∧ E	A ∧ F ∧ G
ES-X Type1/Type2	A ∧ B ∧ C ∧ D		A ∧ F ∧ G
ES-X Long Type1/Type2	A ∧ B ∧ C		A ∧ F ∧ G
ES-A	A ∧ B ∧ C		A ∧ F ∧ G

状況 2、3 においては、CA 証明書を用いる方法とは別の手段によって利用者証明書、および、CRL が認証機関によって発行されたことを確認することとなる（条件 F、条件 G）ため、条件 B と条件 C は不要となる。また、ES-X Type1/Type2 においては、条件 G によって条件 D は満足されるため、条件 D も除かれる。

ETSI TS の署名トークンが有効に機能するには、CA 署名生成鍵がどのタイミングにおいて漏洩したのかを即座に検知し、後日それを確認できるよう、認証機関が対策を講じておくことがまず必要である。ただし、認証機関内部者による不正行為によって鍵が漏洩した場合には、こうした認証機関による対策が有効に機能しなくなる、あるいは、外部から信頼されなくなる可能性もある。したがって、対策をより確実なものとするためには、状況 2、 3 を想定した対応も検討することが重要である。例えば、署名トークンをセキュア・ストレージ・サービスに保管してもらう手法や、他の利用者や各種メディアにおいて保管されているデータを利用することで、署名トークン内のデータが認証機関によって発行されたものか否かを確認するといった手法等が考えられる。いずれにせよ、調停者が実際にどのような方法によって、入手したデータを信頼するかは、ケース・バイ・ケースで判断されることになると考えられるため、各種の方法を比較・検討したうえで、適切と考えられる方法を採用して状況 2、3 に備えることになろう。

(5) 本結果の拡張：階層型 PKI の場合

これまでの ETSI TS の署名トークンの効果に関する分析においては、議論を単純化するため、単独認証機関で構成される PKI を想定した。しかし、PKI の構造はこのように単純なものばかりではなく、階層型や相互認証型等の信頼構造を有する PKI も存在している。

本節では、想定する PKI として階層型モデルを想定し（図 18 参照)、各トラブルに対する署名トークンの効果について分析を行う。認証機関は、証明書生成鍵と ARL（CRL）生成鍵を保持する。上位認証機関は、下位認証機関に対して、CA 証明書（証明書検証用 CA 証明書、ARL（CRL）検証用 CA 証明書）を発行するとともに、それらの失効リストとなる ARL（CRL）に署名を付与して公表する。なお、最上位に位置するルート認証機関は、下位認証機関に対する CA 証明書と ARL 以外にも、自己署名付きの CA 証明書を発行する。最下位に位置する認証機関は、エンド・ユーザである利用者に対して利用者証明書とそれらの失効リストである CRL を発行する。

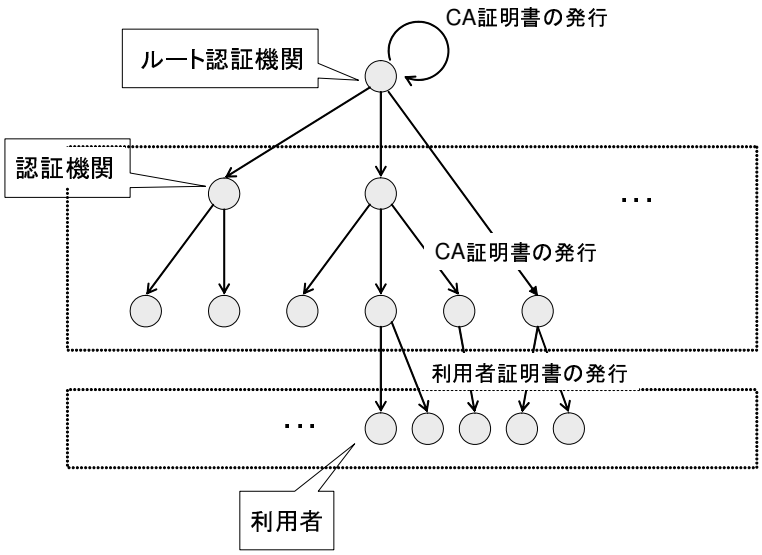

図 18: 階層型 PKI のモデル

イ．署名再検証

階層型モデルでは、ルート認証機関の CA 証明書から利用者証明書に向かって順に電子証明書を検証していく方法と、逆に利用者証明書からルート認証機関の CA 証明書に向かって順番に電子証明書を検証していく方法が考えられる。以下で

は、ルート認証機関の CA 証明書の検証からスタートする方法を取り上げて検討する。署名生成時点を t_S とおくと、署名再検証を実行するための処理は次のように拡張される。

処理 1: ルート認証機関の（自己署名）CA 証明書が t_S において失効していないことを確認する。

処理 2: 処理 1 の ARL 検証用 CA 証明書を用いて、ルート認証機関を発行者として記載している ARL がルート認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 3: 以下の処理 I、II、III を、認証パス上の上位の認証機関から下位の認証機関に向かって順に実行する。

処理 I: 上位認証機関の発行した ARL を用いて、CA 証明書が t_S において失効していないことを確認する。

処理 II: 上位認証機関の証明書検証用 CA 証明書を用いて、処理 I の CA 証明書が、上位認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 III: 処理 II の ARL 検証用 CA 証明書を用いて、ARL が当該認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。最下位の認証機関の場合には、CRL 検証用 CA 証明書を用いて、CRL が当該認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 4: 最下位に位置する認証機関の証明書検証用 CA 証明書を用いて、利用者証明書が認証機関によって発行されたものであり、その一貫性が確保されていることを確認する。

処理 5: 処理 3 の CRL を用いて処理 4 の利用者証明書が t_S において失効していなかったことを確認する。

以上の処理 1〜5 を実行する際に、検証者が入手する必要があるデータは次のとおりである（図 19 参照）。

- **データ 1** ルート認証機関の CA 証明書失効情報。ただし、ルート認証機関によって公表されたことが確認可能であるもの。（処理 1 に対応）

- **データ 2** ルート認証機関の証明書検証用 CA 証明書。ただし、ルート認証機関によって発行されたことが確認可能であり、t_S を有効期間に含むもの。（処理 1 に対応）

- **データ 3** ルート認証機関の ARL 検証用 CA 証明書。ただし、ルート認証機関によって発行されたことが確認可能であり、t_S を有効期間に含むもの。（処理 1、2 に対応）

- **データ 4** ルート認証機関を除く認証パス上に位置する証明書検証用 CA 証明書。ただし、t_S を有効期間に含むもの。（処理 3、4 に対応）

- **データ 5** ルート認証機関を除く認証パス上に位置する ARL 検証用 CA 証明書、および、CRL 検証用 CA 証明書。ただし、t_S を有効期間に含むもの。（処理 3 に対応）

- **データ 6** ARL。ただし、発行時刻が t_S 以降であり下位認証機関の CA 証明書の有効期間内となっているもの。（処理 2、3 に対応）

- **データ 7** 利用者証明書。ただし、有効期間と設定されている期間に t_S を含むもの。（処理 4、5 に対応）

- **データ 8** CRL。ただし、発行時刻が t_S として記載されているもの。（処理 3、5 に対応）

本節においても、利用者による署名生成から署名トークンの生成までの時間的間隔は無視できるものとし、CRL も t_S において発行されたとみなすことにする。

ロ. 署名トークン以外から再検証に用いるデータを入手不可能な場合の署名再検証可能性

ES-X Long、ES-X Long Type1/Type2、ES-A は、利用者証明書、認証パス上に位置する CA 証明書、各認証機関が発行する ARL、CRL を含む。したがって、調停者はデータ 4〜8 を入手可能である。しかし、前節までの議論と同様に、署名トークン内のデータから、ルート認証機関の CA 証明書が当該ルート認証機関によって発行されたこと、および、署名生成時点において失効されていなかったことを確認することができない。その結果、調停者は、データ 1〜3 を入手できず、処理 1〜5 を実行不可能となる。

ただし、以下の 3 条件が満たされるならば、データ 1〜3 を入手することができ、処理 1〜5 を実行可能となる。

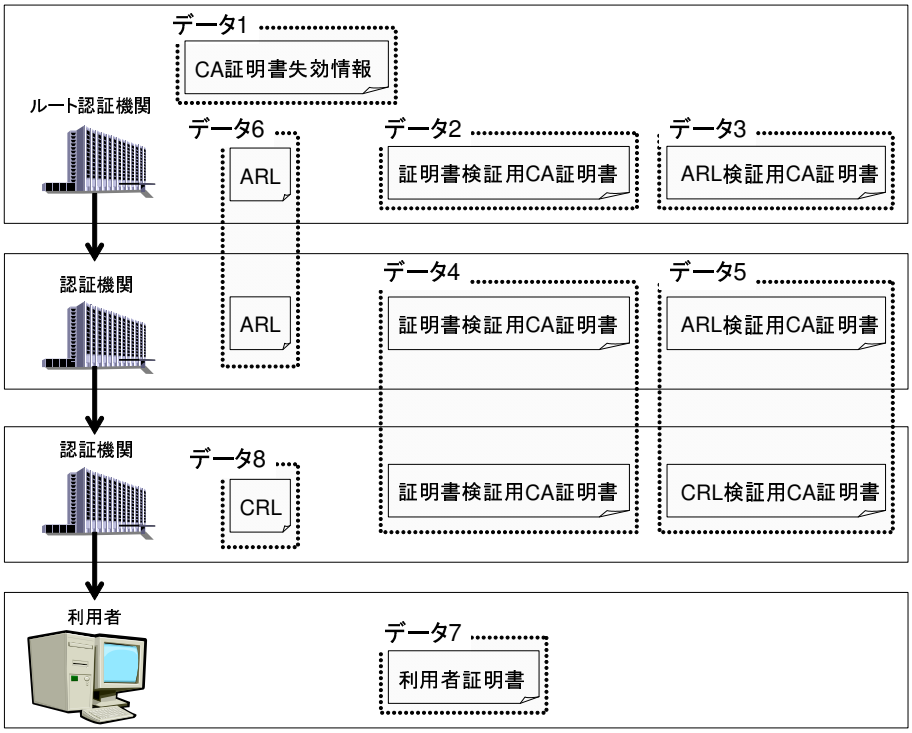

図 19: 署名再検証に必要なデータ

- **条件 H**: 調停者は、ルート認証機関が公表したと認められる CA 証明書失効情報を入手する。

- **条件 I**: 調停者は、ルート認証機関によって発行されたことが確認可能であり、t_S を有効期間に含むルート認証機関の証明書検証用 CA 証明書を入手する。

- **条件 J**: 調停者は、ルート認証機関によって発行されたことが確認可能であり、t_S を有効期間に含むルート認証機関の ARL 検証用 CA 証明書を入手する。

以上より、ES-X Long、ES-X Long Type1/Type2、ES-A において署名再検証を実行可能とするための十分条件は、**条件 H かつ条件 I かつ条件 J** となる。これらの条件は、本節 (3) イ. における条件 A、B、C にそれぞれ対応する。

ES-X Type1/Type2 の場合には、利用者証明書のほか、複数のデータ（利用者証明書、認証パス上に位置する CA 証明書、各認証機関の発行する ARL、CRL）の参照データが含まれるが、署名トークンからはデータ 7 以外のすべてのデータが入手不可能である。ただし、条件 H、条件 I、条件 J に加えて、以下の 3 条件が満足されるならば、処理 1〜5 を実行可能となる。

- **条件 K**: 調停者は、t_S を有効期間に含み、認証パス上に位置する証明書検証用 CA 証明書（ただし、ルート認証機関のものを除く）を入手する。

- **条件 L**: 調停者は、t_S を有効期間に含み、認証パス上に位置する ARL 検証用 CA 証明書（ただし、ルート認証機関のものを除く）および CRL 検証用 CA 証明書を入手する。

- **条件 M**: 調停者は、各認証機関の発行する ARL（ただし、発行時刻が t_S 以降であり、下位認証機関の CA 証明書の有効期間内と記載されるもの）、および、CRL（発行時刻が t_S と記載されるもの）を入手する。

CRL の入手以外の条件は、PKI のモデルを単独認証機関から階層型に拡張したことに伴って新たに追加されるものであり、ES-X Type1/Type2 における十分条件は、**条件 H かつ条件 I かつ条件 J かつ条件 K かつ条件 L かつ条件** M となる。

以上の結果を整理すると、表のとおりである。

表 5: 署名再検証に必要なデータを入手不可能な状況における十分条件

署名トークン	十分条件
ES-X Long	H ∧ I ∧ J
ES-X Type1/Type2	H ∧ I ∧ J ∧ K ∧ L ∧ M
ES-X Long Type1/Type2	H ∧ I ∧ J
ES-A	H ∧ I ∧ J

ハ. CA 証明書生成鍵漏洩時の署名再検証可能性

ここでは、本節 (4) において分類した 3 つの状況を想定し、認証パス上のいずれかの認証機関（以下、CA_i と記す）の CA 証明書生成鍵が漏洩した場合の署名トークンの効果を検討する。

CA_i の証明書生成鍵が漏洩した場合、CA_i より下位に位置する認証機関の CA 証明書の偽造を検知不可能となり、CA_i よりも下位の認証パスを偽造するという攻撃が成功してしまう。ただし、CA_i の下位の認証機関の CA 証明書が CA_i から発行されたことを確認できれば、署名再検証を実行可能である。

(イ) 状況 1

状況 1 においては、CA_i よりも下位の認証機関の CA 証明書（CA_i が最下位の認証機関の場合には利用者証明書）が t_C 以前に生成されたことを確認できれば、偽造されたものでないことが判明する。ES-X Long 以外の署名トークンにおいては、すべての CA 証明書と利用者証明書、あるいはその参照データにタイムスタ

ンプが付与されている。これにより、CA 証明書や利用者証明書が生成された時点よりも CA 署名生成鍵が漏洩した時点の方が後であることをタイムスタンプによって確認できるため、CA 証明書や利用者証明書が偽造されたものでないことを確認可能である。したがって、本節 (5) ロ. で示した十分条件（表）が満足されるならば、署名再検証が実行可能となる。

ES-X Long については、CA_i が最下位の認証機関である場合には、利用者証明書にタイムスタンプ TS-EST が付与されており、利用者証明書が生成された時点よりも CA 署名生成鍵が漏洩した時点の方が後であることをタイムスタンプによって確認可能である。したがって、この場合には十分条件は本節 (5) ロ. で示したものと同一となるが、CA_i が最下位の認証機関でない場合には、署名トークン内の CA 証明書にはタイムスタンプが付与されていないため、t_C 以前に発行されたことが確認可能な CA 証明書を入手できるならば、処理 1〜5 に沿って署名再検証が可能となる。そこで、条件 N を、

- **条件 N**: 調停者は、t_S を有効期間に含み、t_C 以前に発行されたことを確認可能な CA 証明書（ただし、発行者が CA_i と記載されるもの）を入手する。

とすれば、十分条件は、**条件 H かつ条件 I かつ条件 J かつ条件 N** となる。

(ロ) 状況 2

状況 2 においては、本節 (4) ニ. と同様にタイムスタンプが効果を発揮せず、CA 証明書や利用者証明書が上位認証機関から発行されたことを、本節 (5) イ. の処理 3、4 では確認できない。ただし、いずれの署名トークンにおいても、下記の条件 O が満足されるならば、こうした問題はクリアされることになる。

- **条件 O**: 調停者は、CA_i によって発行されたことが確認可能であり、t_S を有効期間に含む CA 証明書を入手する。CA_i が最下位の認証機関の場合には、CA_i によって発行されたことが確認可能であり、t_S を有効期間に含む利用者証明書を入手する。

上記の条件 O が満足されるとともに、本節 (5) ロ. において検討した十分条件が満足されるならば、各署名トークンにおいて署名再検証が実行可能となる。各署名トークンにおける十分条件は以下のとおりとなる。

– ES-X Long: **条件 H かつ条件 I かつ条件 J かつ条件 O**

– ES-X Type1/Type2: **条件 H かつ条件 I かつ条件 J かつ条件 K かつ条件 L かつ条件 M かつ条件 O**

– ES-X Long Type1/Type2: **条件 H かつ条件 I かつ条件 J かつ条件 O**

– ES-X A: **条件 H かつ条件 I かつ条件 J かつ条件 O**

ただし、CA_i がルート認証機関の場合には、証明書検証用 CA 証明書が不要となるため、条件 I は除かれる。

(ハ) 状況 3

状況 3 の場合は、状況 1 と状況 2 のいずれにも対応可能であればよい。したがって、十分条件は状況 2 と同一となる。以上の検討内容を整理すると表のとおりである。なお、ES-X Long においては、条件 O によって CA 証明書の発行者が確認できるため、条件 N は十分条件から除かれる。

表 6: 証明書生成鍵漏洩時における十分条件

署名トークン	各状況における十分条件		
	鍵漏洩がない状況	状況 1	状況 2、3
ES-X Long	H ∧ I ∧ J	H ∧ I ∧ J ∧ N H ∧ I ∧ J *	H ∧ I ∧ J ∧ O H ∧ J ∧ O **
ES-X Type1/2	H ∧ I ∧ J ∧ K ∧ L ∧ M		H ∧ I ∧ J ∧ K ∧ L ∧ M ∧ O H ∧ J ∧ K ∧ L ∧ M ∧ O **
ES-X Long Type1/2	H ∧ I ∧ J		H ∧ I ∧ J ∧ O H ∧ J ∧ O **
ES-A	H ∧ I ∧ J		H ∧ I ∧ J ∧ O H ∧ J ∧ O **

（備考）“*” は CA_i が最下位の認証機関の場合における十分条件であり、“**” は CA_i がルート認証機関の場合における十分条件である。

ニ. ARL、CRL 生成鍵漏洩時の署名再検証可能性

本節 (5) と同様に、3 つの状況において、認証パス上のいずれかの認証機関の ARL、CRL 生成鍵が漏洩した場合の署名トークンの効果について検討を行う。

(イ) 状況 1

ES-X Long を除く署名トークンにおいては、タイムスタンプが付与された ARL、CRL やその参照データが含まれるため、調停者は ARL や CRL が t_C 以前に発行されたことをタイムスタンプによって確認することができる。このように、タイムスタンプの効果により、ARL や CRL の生成鍵の漏洩が署名トークンを用いた署名再検証に与える影響はない。したがって、本節 (5) ロ. で示した十分条件（表 5）が満足されるならば、署名再検証が可能である。

ES-X Long の場合、署名トークン内に含まれる ARL や CRL にはタイムスタンプが付与されていない。ただし、t_C 以前に発行されたことが確認可能な ARL や CRL を入手できるならば、処理 3 の III. によって、それらは偽造されたものではないことが明らかとなるため、処理 1〜5 に沿って署名再検証が実行可能となる。そこで、条件 P を、

- **条件 P**: 調停者は、発行時刻が CA_i の下位認証機関の CA 証明書の有効期間内であり、t_S 以降 t_C 以前であることを確認可能な ARL（ただし、発行者が CA_i と記載されるもの）を入手する。CA_i が最下位の認証機関である場合には、t_S に発行されたことを確認可能な CRL（ただし、発行者が CA_i と記載されるもの）を入手する。

とおけば、ES-X Long における十分条件は**条件 H かつ条件 I かつ条件 J かつ条件 P** となる。

(ロ) 状況 2

状況 2 においては、タイムスタンプが効果を発揮せず、ARL あるいは CRL が CA_i によって発行されたことを処理 3 の III. によって確認することができない。ただし、別の手段によって上記事項を確認できれば署名再検証可能となる。条件 Q を、

- **条件 Q**: 調停者は、CA_i によって発行されたことを確認可能な ARL（ただし、発行時刻が下位認証機関の CA 証明書の有効期間内であり、t_S 以降と記載されるもの）を入手する。CA_i が最下位の認証機関である場合、CA_i によって発行されたことを確認可能な CRL（ただし、発行時刻が t_S と記載されるもの）を入手する。

とおけば、本節 (5) ロ. において示した十分条件に条件 Q を追加することによって署名再検証が実行可能となる。この結果、各署名トークンにおける十分条件は、次のとおりとなる。

– ES-X Long: **条件 H かつ条件 I かつ条件 J かつ条件 Q**

– ES-X Type1/Type2: **条件 H かつ条件 I かつ条件 J かつ条件 K かつ条件 L かつ条件 M かつ条件 Q**

– ES-X Long Type1/Type2: **条件 H かつ条件 I かつ条件 J かつ条件 Q**

– ES-X A: **条件 H かつ条件 I かつ条件 J かつ条件 Q**

ただし、CA_i がルート認証機関の場合には、処理 2 を行わないため、条件 J は不要となる。

(ハ) 状況 3

状況 3 では、状況 1 と状況 2 のいずれにも対応可能であればよい。この結果、状況 3 における十分条件は状況 2 における十分条件と同一となる。検討結果を整理すると、表のとおりである。

なお、状況 3 での ES-X Long においては、ARL あるいは CRL が CA_i によって発行されたことが確認可能であるならば、その発行時刻も保証されることから、条件 P は十分条件から除かれる。

表 7: ARL あるいは CRL の生成鍵漏洩時における十分条件

署名トークン	各状況における十分条件		
	鍵漏洩がない状況	状況 1	状況 2、3
ES-X Long	H ∧ I ∧ J	H ∧ I ∧ J ∧ P	H ∧ I ∧ J ∧ Q H ∧ I ∧ Q *
ES-X Type1/2	H ∧ I ∧ J ∧ K ∧ L ∧ M		H ∧ I ∧ J ∧ K ∧ L ∧ M ∧ Q H ∧ I ∧ K ∧ L ∧ M ∧ Q *
ES-X Long Type1/2	H ∧ I ∧ J		H ∧ I ∧ J ∧ Q H ∧ I ∧ Q *
ES-A	H ∧ I ∧ J		H ∧ I ∧ J ∧ Q H ∧ I ∧ Q *

（備考）“*” は CA_i がルート認証機関の場合の十分条件である。

ニ. 考察

階層型 PKI における検討結果をまとめると以下のとおりである。

1. 署名トークンから署名再検証に必要なデータが入手できなくなる状況では、ES-X Type1/2 を除く署名トークンの十分条件（条件 H かつ条件 I かつ条件 J）は、単独認証機関の PKI における十分条件（条件 A かつ条件 B かつ条件 C）と対応する。ES-X Type1/Type2 の場合、認証パス上に位置する CA 証明書、ARL、CRL が含まれていないため、別途これらを入手するための条件が十分条件に追加される。

2. 認証機関 CA_i の署名生成鍵が漏洩した状況においては、まず、状況 1 のケースでは、ES-X Long を除く署名トークンにおいてタイムスタンプが効果を発揮し、単独認証機関の PKI の場合と同様に、CA 署名生成鍵が漏洩しない場

合における十分条件と同一となる。ES-X Long の場合には、ES-X Long 内の CA 証明書、ARL、CRL にタイムスタンプが付与されておらず、CA_i の署名生成鍵が漏洩した時刻以前に発行されたことを確認可能なデータを入手できれば、署名再検証が実行可能となる。

3. 状況 2、3 においては、タイムスタンプが効果を発揮せず、本稿で議論の前提とした標準的な署名検証手続では、CA 証明書、ARL、CRL が CA_i によって発行されたことを確認困難となるという点で、本節 (4) と同様の結論となる。ただし、CA_i によって発行されたと確認できる CA 証明書、ARL、CRL を入手できれば、署名再検証を実行可能となる。

以上の考察から、階層型 PKI における各署名トークンの署名再検証可能性は、基本的には単独認証機関の PKI の場合と同一となることが明らかとなった。また、階層型 PKI の場合には、署名再検証の際に、認証パス上に位置する CA 証明書や利用者証明書、これらに対応する ARL や CRL をすべてが用いられることから、ルート認証機関だけでなく、階層型 PKI を構成するいずれの認証機関も CA 証明書等のデータを適切に管理し続けることが求められるといえる。

(6) 利用者署名生成鍵が漏洩した場合について

本節では、ETSI TS において想定されている各種トラブルとして、署名再検証に用いられるデータが署名トークン以外から入手できなくなった場合と、CA 署名生成鍵が漏洩してしまった場合を想定して各署名トークンの署名再検証可能性について検討を行った。しかし、利用者署名生成鍵が漏洩してしまう可能性が少なくないと考えるのが自然であり、以下では、利用者署名生成鍵漏洩時の署名再検証可能性について簡単に考察する。

利用者署名生成鍵が漏洩した場合の署名再検証可能性も、CA 署名生成鍵の漏洩時における分析と同様に、状況 1〜3 に分けて考えることができる。すなわち、調停者が利用者証明書の鍵漏洩時点（t_C）よりも先に「署名データ（signature)」が生成されたことを知る場合を状況 1 とし、t_C よりも後に「署名データ（signature)」が生成されたことを知る場合を状況 2 とする。また、調停者が、状況 1 なのか状況 2 なのかを識別できない場合を状況 3 とする。

状況 1 では、いずれの署名トークンにおいても「署名データ（signature)」に対してタイムスタンプ TS-EST が付与されており、「署名データ（signature)」が t_C 以前に生成されたことを TS-EST によって調停者は確認することができる。したがって、タイムスタンプの効果によって、利用者署名生成鍵の漏洩の影響はなく、

署名再検証可能性の十分条件は、単独認証機関の場合には表、階層型 PKI の場合には表と同一となる。

状況 2 では、調停者は、署名生成時点において既に利用者署名生成鍵が漏洩した事実を知っており、「署名データ（signature）」が偽造されたものか否かを確認する手段を有していない。したがって、本稿で議論の前提としてきた署名再検証の手続は実行不可能となる。

状況 3 では、状況 1 と状況 2 を調停者が区別できず、状況 2 に陥っている可能性を否定できない。したがって、状況 2 と同様の結果となる。

以上のように、利用者署名生成鍵の漏洩においても、状況 1 のケースではタイムスタンプが効果を発揮することになる。しかし、状況 2、3 では署名再検証は実行不可能となってしまう。CA 証明書、ARL、CRL は当事者である利用者や検証者以外のエンティティが保管している可能性もあり、これらのデータが当該認証機関によって発行されたことを確認できる可能性も残されている。しかし、当事者以外のエンティティが署名の偽造の有無を確認することは一般に困難であると考えられることから、状況 2、3 が想定されるアプリケーションにおいては、現行の PKI の枠組みでは対応が困難であると思われる。この場合、4 節 (2) において紹介した署名生成鍵漏洩への対応技術を利用する等の方策について検討することも必要であろう。

6. おわりに

近年の紙文書から電子文書への急速な移行に伴い、デジタル署名は、取引の瞬間における短期的な利用だけでなく、署名が生成されてから一定期間後に改めて検証するという長期的な利用に用いられるようになるのではないかとみられる。本稿においては、デジタル署名の長期利用をデータの作成者および一貫性を事後的に確認するための利用と定義し、署名再検証において確認すべき事項を整理したうえで、デジタル署名の再検証可能性について考察を行った。デジタル署名を長期間再検証可能な状態に維持しておくためには、本稿において紹介した対策技術を用いる等によって、署名方式の安全性低下等をはじめとするさまざまな問題に適切に対応することが求められる。

その中でも、ETSI TS の署名トークンは、いくつかの技術仕様として規定されているほか、既存のインフラを利用して比較的容易に実装可能であるという特徴を持つことから、署名の長期利用を検討する際に候補となる技術の 1 つに数えられる。本稿では、ETSI TS の署名トークンにおいて原理的に署名再検証が実行可能となるための十分条件を示したが、署名トークンを採用する場合には、こうした十分条件が実際に満足されているか否かを見極めることによって対策の有効性を確認することができるであろう。ただし、ETSI TS に関してはいくつかの課題も残っており、引続き検討を行う必要がある。具体的には次の 3 つが挙げられよう。第 1 は、タイムスタンプの安全性低下に関する検討である。本稿では、ETSI TS の署名トークンを構成するタイムスタンプの安全性が低下するケースを想定しなかった。しかし、ETSI TS では、デジタル署名ベースのタイムスタンプの利用が想定されているため、上記のケースが各署名トークンの署名再検証可能性に与える影響について考察する必要がある。第 2 は、ハッシュ関数の危殆化に関する検討である。本稿では、ハッシュ関数が危殆化するケースを想定しなかったが、ハッシュ関数の危殆化も ETSI TS の想定するトラブルとして挙げられており、このような状況のもとでの検証可能性を検討する必要がある。第 3 は、署名トークンにおける十分条件を満足させる方法として説明した、セキュア・ストレージ・サービスを利用する方法や分散保管されているデータを利用する方法に関する検討である。実際に ETSI TS を署名の長期利用のための技術として採用する際には、上記の 2 つの方法を含め、本稿で示した十分条件をどのようにして満足させていくかを検討しなければならない。

また、デジタル署名を長期的に利用する際には、運用面からの検討も必要である。まず、署名再検証を可能とするために必要となるコストの問題である。署名の再検証は、電子証明書の有効期間の前後を問わず実行されることが考えられるが、電子証明書の有効期間は、本来署名の再検証が確実に実施可能であるべき期

間であり、PKI の運営主体は電子証明書の管理（CA 署名生成鍵の管理、電子証明書の失効処理）を適切に行う義務がある。そのため、電子証明書の有効期間内に発生し得るトラブルへの対応は、PKI の運営主体によって厳格に実施されることが求められる。一方、電子証明書の有効期間終了後では、PKI の運営主体に課せられる責任が非常に限定的となるケースもあり、署名再検証のための責任の所在は PKI 運営主体から利用者側へ変化するものと思われる。この場合、電子証明書の有効期間内のように、利用者が自分の責任を果たす限り署名の再検証が保証されるようなことは考えにくく、利用者が主体的に再検証を保証するための措置を講じる必要があろう。このように考えると、電子証明書の有効期限の前後で、利用者に求められる対策の内容が異なる可能性があり、電子証明書の有効期間後に署名の長期利用を目的として採用される技術としては、相対的にコストがかからない方法をとらざるを得ない。したがって、既存の対策技術のうちどれを採用すべきかを検討する際、当該アプリケーションの環境を考慮して想定すべきトラブルを明確化したうえで、安全性のみならずコストにも留意した対策の選択が求められよう。

本稿では、原理的に署名再検証が実行可能か否かという観点から、ETSI TS の署名トークンを用いた再検証を可能とするための十分条件に関して検討を行った。しかし、アプリケーションによっては、署名再検証に与えられる時間等が制限されるケースも考えられ、署名トークン外からのデータ入手に要する時間との関係で、十分条件を満足することが困難な場合もあろう。したがって、具体的なアプリケーションに本稿の議論を適用する際には、こうした運用上の課題にも対処することが求められる場合も出てくると思われる。このような課題についても、今後検討していく必要がある。

以　上

参考文献

伊藤信治・宮崎邦彦・本多義則・谷川嘉伸、「電子署名の長期保証に関する一考察」、『2004 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、2004 年、527〜532 頁

上田祐輔・佐々木良一・吉浦 裕・洲崎誠一・宮崎邦彦、「データ喪失を想定したヒステリシス署名方式評価手法の提案」、『情報処理学会論文誌』第 45 巻第 8 号、情報処理学会、2004 年、1966〜1976 頁

上山真貴子・四方順司・松本 勉、「署名生成機能の危殆化を検出できるディジタル署名方式」、『情報処理学会研究報告』2003–CSEC–22、情報処理学会、2003 年、143〜150 頁

宇根正志、「金融分野における PKI：技術的課題と研究・標準化動向」、『金融研究』第 21 巻別冊第 1 号、日本銀行金融研究所、2002 年、227〜283 頁

——、「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」、『金融研究』第 22 巻別冊第 1 号、日本銀行金融研究所、2003 年、15〜50 頁

——、岡本龍明、「最近のデジタル署名における理論研究動向について」、『金融研究』第 19 巻別冊第 1 号、日本銀行金融研究所、2000 年、55〜104 頁

——・田村裕子・岩下直行・松本 勉・松浦幹太・佐々木良一、「公開鍵証明書・失効情報欠損時における ETSI TS 101 733 に基づく署名の検証可能性」、『コンピュータセキュリティシンポジウム 2004 論文集』、情報処理学会、2004 年 a、439〜444 頁

——・——・——・——・——・——、「CA 鍵漏洩時における ETSI TS 101 733 に基づく署名の検証可能性」、『コンピュータセキュリティシンポジウム 2004 論文集』、情報処理学会、2004 年 b、445〜450 頁

——・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書』2002-CSEC-18、情報処理学会、2002 年、245〜252 頁

小森 旭・花岡悟一郎・松浦幹太・須藤 修、「署名鍵漏洩問題における電子証拠生成技術について」、『2003 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、2003 年、983〜988 頁

——・松浦幹太・須藤 修、「PKI に基づく C/S 型アプリケーションの安全性分析と証拠性評価」、『コンピュータセキュリティシンポジウム 2001 論文集』、情報処理学会、2001 年 a、319〜324 頁

——・——・——、「契約時に添える付加的な MAC に関する総合的分析」、『情報処理学会研究報告』2001–CSEC–15、情報処理学会、2001 年 b、31〜36 頁

——・——・——、「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、2002 年、627〜632 頁

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』第 43 巻第 8 号、情報処理学会、2002 年、2381〜2393 頁

佐々木良一・吉浦 裕・洲崎誠一・宮崎邦彦、「デジタル署名付文書の長期的安全性に関する考察」、『情報処理学会研究報告』2003–CSEC–21、情報処理学会、2003 年、13〜18 頁

情報処理推進機構（IPA）、『PKI 関連技術解説（最終更新日：2004 年 5 月 21 日）』、2004 年 a（http://www.ipa.go.jp/security/pki）

——、『タイムスタンプ・プロトコルに関する技術調査』、2004 年 b（http://www.ipa.go.jp/security/fy15/reports/tsp/documents/tsp2003.pdf）

セコムトラストネット株式会社、『セコムパスポート for G-ID 認証運用規定（Certification Practice Statement）Version 1.7』、2004 年 a

——、『利用者利用規定（セコムパスポート for G-ID、Ver. 1.20、2004 年 6 月 24 日現在）』、2004 年 b

総務省、『行政手続オンライン化法に基づき各府省が公表した事項等の概要』、2004 年

高橋知史・洲崎誠一・松本 勉、「Forward-Secure Digital Signature は役に立つか」、『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、2002 年、837〜842 頁

電子商取引推進協議会（ECOM）、『電子署名文書長期保存に関するガイドライン』、H13–認証・公証–3、2002 年

——・日本情報処理開発協会（JIPDEC）電子商取引推進センター、『電子署名文書長期保存に関する実用化動向調査報告書』、2004 年 a

——・——、『電子文書の長期保存と見読性に関する調査報告書』、2004 年 b

日本銀行金融研究所、「第 5 回情報セキュリティ・シンポジウムの模様 – デジタル署名の長期的な利用とその安全性 –」、『金融研究』第 22 巻第 2 号、日本銀行金融研究所、2003 年、1〜12 頁

日本認証サービス株式会社、『AccreditedSign® パブリックサービス 2 依存者同意書（2004 年 8 月 27 日版）』、2004 年 a

——、『AccreditedSign® パブリックサービス 2 標準規程 （V2.2）』、2004 年 b

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」、『金融研究』第 22 巻別冊第 1 号、日本銀行金融研究所、2003 年、1〜13 頁

——・——、「金融業務と人工物メトリクス」、『金融研究』第 23 巻別冊第 1 号、日本銀行金融研究所、2004 年、169〜186 頁

——・田中直樹、「計算の実行ハードウエアを確認する方法」、『コンピュータセキュリティシンポジウム 2000 論文集』、情報処理学会、2000 年、199〜204 頁

松本弘之・宇根正志・松本　勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第 23 巻別冊第 1 号、日本銀行金融研究所、2004 年、61〜140 頁

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』第 44 巻第 8 号、情報通信学会、2003 年、1955〜1969 頁

Abdalla, Michel, and Leonid Reyzin, "A New Forward-Secure Digital Signature Scheme," *Proceedings of Asiacrypt 2000*, LNCS 1976, Springer-Verlag, 2000, pp. 116–129.

Adams, Carlisle, Pat Cain, Denis Pinkas, and Robert Zuccherato, *Request for Comments 3161: Time-Stamping Protocol (TSP)*, 2001.

——, Peter Sylvester, Michael Zolotarev, and Robert Zuccherato, *Request for Comments 3029: Data Validation and Certification Server Protocols*, 2001.

Anderson, Ross, "Invited lecture," *4th Annual Conference on Computer and Communications Security*, 1997.

Bellare, Miher, and Sara K. Miner, "A Forward-Secure Digital Signature Scheme," *Proceedings of Crypto'99*, LNCS 1666, Springer-Verlag, 1999, pp. 431–448.

Cruellas, C. Juan, Gregor Karlinger, Denis Pinkas, and John Ross, *XML Advanced Electronic Signatures (XAdES)*, http://www.w3.org/TR/2003/NOTE-XAdES-20030220/♯ Syntax_for_XAdES_T_form, 2003.

Dodis, Yevgeniy, Jonathan Katz, Shouhuai Xi, and Moti Yung, "Key-Insulated Public Key Cryptosystems," *Proceedings of Eurocrypt 2002*, LNCS 2332, Springer-Verlag, 2002, pp. 65–82.

European Telecommunications Standards Institute (ETSI), *ETSI TS 101 733: Electronic Signatures and Infrastructure (ESI); Electronic Signature Formats*, v1.5.1, 2003.

——, *ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)*, v1.1.1, 2002.

Housley, Russell, *Request for Comments 3852: Cryptographic Message Syntax (CMS)*, 2004.

Itkis, Gene, "Intrusion-Resilient Signatures: Generic Constructions, or Defeating a Strong Adversary with Minimal Assumptions," *Proceedings of Security in Communication Networks 2002 (SCN 2002)*, LNCS 2576, Springer-Verlag, 2003, pp. 102–118.

——, and Leonid Reyzin, "Forward-Secure Signatures with Optimal Signing and Verifying", *Proceedings of Crypto 2001*, LNCS 2139, Springer-Verlag, 2001, pp. 332–354.

——, and ——, "SiBIR: Signer-Base Intrusion-Resilient Signatures," *Proceedings of Crypto 2002*, LNCS 2442, Springer-Verlag, 2002, pp. 499–514.

Malkin, Tal, Daniele Micciancio, and Sara K. Miner, "Efficient Generic Forward-Secure Signatures with an Unbounded Number of Time Periods," *Proceedings of Eurocrypt 2002*, LNCS 2332, Springer-Verlag, 2002, pp. 400–417.

Pinkas, Denis, John Ross, and Nick Pope, *Request for Comments 3126: Electronic Signature Formats for long term electronic signatures*, 2001.