Ver.1.3
タイムビジネス推進協議会

タイムスタンプ長期保証
ガイドライン

平成１８年４月

タイムビジネス推進協議会

目　次

１．はじめに

１．１　背景と目的

2005 年 4 月から e-文書法が施行され、一定の手順を踏んでもとの文書に対する真実性の要件を満たせば、スキャナなどで取り込んだ電子化データ・文書に対して、紙媒体の原本と同等の証拠能力が認められることになる。たとえば、経理処理に要求される領収書などの確証を紙でなく電子データとして保存することが可能となるわけである。これを契機にその他の紙媒体の文書も電子化が進み、書類の保管費用の低減、さらにはその再利用性が高まることが期待されている。

（1）電子データの存在と非改ざんを担保

電子データ・電子文書が過去に遡って証拠能力を持つには、時間軸上のある時点で当該データ・文書が存在し、それが将来の時点で同一であること、を証明できることである。それをタイムスタンプで担保することが求められている。

このように電子データ・電子文書の存在・非改ざんを担保するには、信頼のおけるタイムスタンプを用いることが必須要件である。すなわち、タイムスタンプの発行主体と対象が明確であり、時刻の信頼性が確保されて、タイムスタンプトークンの非改ざん性が確認できる必要がある。ここで時刻の信頼性の確保とは、タイムスタンプの時刻が協定世界時(UTC)にまで遡って、その精度を確認できることであり、それには、タイムスタンプの方式夫々に対応した技術に基づいてシステムを構築し、適正に運用していること、および、そのタイムスタンプを利用する手順が適切でなければならない。

当協議会では、前者に対しては「信頼されるタイムスタンプ技術・運用基準ガイドライン」（平成 17 年 1 月）[1]を作成して、タイムスタンプ提供事業者および利用者双方に信頼の根拠を示し、後者については夫々の利用局面で適切なタイムスタンプ付与の指針を提示して、利用者が不適切な使い方に起因する証拠性の欠如に陥らないよう務めている。なお、時刻配信業務と時刻認証業務の信頼性を確認できるようにするための、第三者による枠組みとして、(財)日本データ通信協会の「タイムビジネス信頼・安心認定制度」が 2005 年 2 月 7 日に開始された。

（2）長期保証の枠組みと要件

このように､時を隔てて電子データの存在と非改ざんを担保するのがタイムスタンプの最大の特長であり、役割であるが、実際にはタイムスタンプにも有効期間、有効期限の制約がある。それに対して、保証対象文書の保存年数は、法令に基づく場合で 5 年(カ

[1] http://www.scat.or.jp/time/PDF/unyoukijunVer1.0.pdf

ルテやレントゲンフィルムなど)、7 年(請求書・契約書・見積書など)あるいは 10 年(株主総会の議事録など)から、文書の性格上、20 年あるいはそれ以上の保存が求められる場合まである。一回のタイムスタンプで保証するのは一般的には数年から十数年なので、それより長期にわたって担保するには工夫がいる。

文書の保存年数とタイムスタンプの保証期間の関係から、一回のタイムスタンプで文書の保存に対応できる場合のあることが判る。しかしながら、それで対応できないほど長期間の場合、あるいは、タイムスタンプの基礎となる暗号技術の脆弱性が判明した場合、現時点では再度タイムスタンプを付与して延長することになる。

タイムスタンプには後述のように、大別すると PKI 方式とリンク方式があるが、同じ方式で延長しても、別の方式で延長しても良い。ただし、従前のタイムスタンプが有効である間に再度、付与しなければならない。したがって、暗号技術の脆弱性が判明した場合は、再度、安全性の高い方式のタイムスタンプを緊急に付与する必要がある。

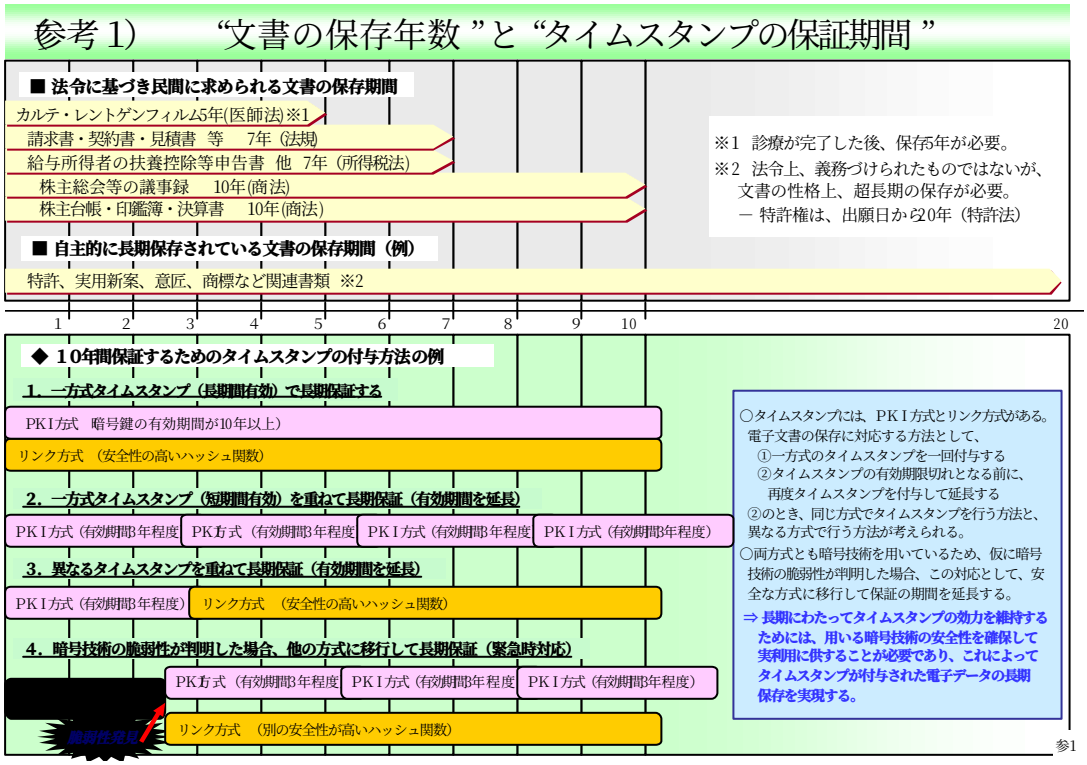


図１．１　“文書の保存年数”と“タイムスタンプの保証期間”

出典；第 60 回ﾃﾚｺﾑ技術情報ｾﾐﾅｰ　時刻認証技術の動向とタイムビジネスの普及（総務省）

（３）長期保証の要件

タイムスタンプを付与した時からその検証(確認)が必要とされる時までには、長い短いに問わず時間が経過するため、技術および環境がその間に変っている恐れが高い。この時間の重みに耐えるためのタイムスタンプの要件は何であるか、すなわち、

長期にわたる技術の進展と環境の変化に耐え、データの存在時刻と非改ざん性を担保するためには、タイムスタンプはどうあるべきかを明確に示すことが求められる。さらにそれをどのように実現するのか、利用する際どこに留意すべきか、を明示する必要がある。

タイムスタンプサービスの歴史は浅いので、前記のような長期保証が実際に必要とされるまで、まだ若干の余裕がある。また、将来の技術革新によって画期的な長期保証の技術が出現する可能性も考えられる。しかし、必要となってから仕組みを用意するのでは遅過ぎるのがタイムスタンプである。基本的な考え方は当協議会の「時刻認証基盤ガイドライン」（平成 16 年 5 月）[2]に記載されている長期保証の仕組みで良いので、本書では、現在の技術による長期保証の途を示して、それを実現するための技術と仕組みを詳細化し、最初のタイムスタンプを付与する時から利用者が予め留意しておくべきこと示す。

１．２　検討の方針

本ガイドラインの検討にあたっては、次の三点に留意した。

① 長期保証を中心とする

本書はタイムスタンプの「長期保証」に関わる事項に焦点を合わせることとし、タイムスタンプと時刻配信・時刻認証の全体については既発行の「時刻認証基盤ガイドライン」に、また、タイムスタンプの信頼性については「信頼されるタイムスタンプ技術・運用基準ガイドライン」を前提とする。

② 中立の姿勢を保つ

タイムスタンプには幾つかの方式が並存しているが、それぞれに特徴があり、一概に優劣を決めることが難しい。長期保証においても、サービスの詳細・提示方法に違いがあるが、存在と非改ざんを長期にわたって保証する点では同じである。

本書では特定の方式に偏らないよう、代表的な PKI 方式とリンク方式の長期保証方法を併記することとする。さらにはそれらの方式の一部を用いて異なる運用方式を構成する方法および、研究開発段階の方式にも参考で言及する。

③ 利用・適用の立場から実用を重視する

タイムスタンプの長期保証が現実の問題となるのは将来のことであり、現段階では主に机上で検証せざるを得ない。それは提供者のみならず、利用者においても同様である。そのためともすれば、過剰な仕組みを要請するか、逆に、簡便な方式で良いとするか、

[2] http://www.scat.or.jp/time/PDF/2004guideline.pdf

議論が極端になり易い。

それを防ぐため、長期保証の検討にあたっては、常に利用の原点に立ち返りつつ、現実的な実装を念頭におくよう留意した。

１．３　ガイドラインの構成

本書は長期保証を中心とする内容に絞った構成になっており、関連する情報は「時刻認証基盤ガイドライン」を参照することを前提としている。

（１）長期保証の要件

タイムスタンプの主要な方式である、PKI 方式とリンク方式それぞれについて、長期保証の視点からタイムスタンプ有効性の根拠を整理した上で、長期保証に求められる要件を記述する。「時刻認証基盤ガイドライン」に比べ、長期保証について詳細な説明となっている。方式によりその要件が異なるため、利用・適用上の留意点にもかなり違いがあることに注意する必要がある。

（２）長期保証の方法

基本的な考えは、タイムスタンプの有効期限が切れる前に、新たなタイムスタンプを重ねていくわけである。最初のタイムスタンプの有効性を如何に担保するかが鍵で、その有効性の検証を念頭において、二回目以降のタイムスタンプの付与対象とその時期が主な記載事項である。PKI 方式とリンク方式で要件が異なるように、方法が違うので、それぞれに実装方法、タイムスタンプ取得時の手順と検証について記述してある。

（３）デジタル署名付文書

デジタル署名付文書の場合、文書だけでなく、デジタル署名自体がタイムスタンプの付与対象になることを考慮する必要がある。この場合、長期経過後のデジタル署名の正当性を如何に確認するかが課題で、本節ではそのための手順と保存すべき情報、保存形式について特に記載してある。

（４）認証局(CA)の要件

PKI 方式ではタイムスタンプの信頼点を CA の発行する電子署名すなわち CA に置いている。したがって、CA に関する長期保証のための要件も明らかにしておく必要がある。ここでは TSA 証明書の有効期間中、TSA 証明書有効期間満了後および CA 証明書有効期間満了後の有効性保証について整理し、タイムスタンプの検証者、利用者、TSA、CA それぞれの満たすべき要件を述べる。

１．４　タイムスタンプの方式

本書では、長期保証の方法として、タイムスタンプの再付与による効力延長を基本とした方法を主題としているが、効力延長の対象となるタイムスタンプの方式については、PKI 方式とリンク方式の２方式に大別して記載している。

ここで、本書における PKI 方式とは、デジタル署名を利用した方式を指しており、(財)日本データ通信協会の「タイムビジネス信頼・安心認定制度」における以下の方式に対応している。

・　デジタル署名を使用する方式｛2005 年 6 月 15 日改訂基準対象｝

また、本書におけるリンク方式とは、ハッシュ関数によるリンクを利用した方式を指しており、(財)日本データ通信協会の「タイムビジネス信頼・安心認定制度」における以下の方式に対応している。

・　リンキング方式｛2005 年 6 月 15 日改訂基準対象｝
・　アーカイビング方式｛2005 年 10 月 5 日新設基準対象｝（このうち、ハッシュ関数によるリンクを利用したもの）

なお、PKI 方式及びリンク方式のタイムスタンプを効力延長の対象とした長期保証方式については、「平成１７年度　技術部会　実証実験分科会　長期保証 WG」において、それぞれ本書記載の方法に沿った実装の評価を行い、問題なく動作することを確認した。

２．タイムスタンプ長期保証

本章では、タイムスタンプ長期保証のための要件について記す。そのために、２．１でまずタイムスタンプの有効性を満たす要件について整理し、次に２．２において、それを長期にわたって維持するための要件について記す。

２．１　タイムスタンプの有効性

タイムスタンプトークン及び関連情報によって対象となる電子データの存在時刻が証明できるとき、タイムスタンプが有効であるという。本節では、PKI 方式、リンク方式それぞれについて、有効性を満たすための要件について記す。

２．１．１　PKI方式タイムスタンプの有効性

デジタル署名を利用したタイムスタンプ（PKI 方式タイムスタンプ）が有効であるのは次のすべての要件を満たす場合である。

（1）電子データとタイムスタンプとの関係を証明できること

PKI 方式タイムスタンプでは、対象とする電子データのハッシュ値をタイムスタンプトークンに含めることによって、対象データとタイムスタンプトークンとを対応付ける。安全なハッシュ関数（事実上、同一のハッシュ値が算出される異なる複数のデータが求められない）を利用することにより、ハッシュ値とデータとを事実上、一意に対応付けることができる。

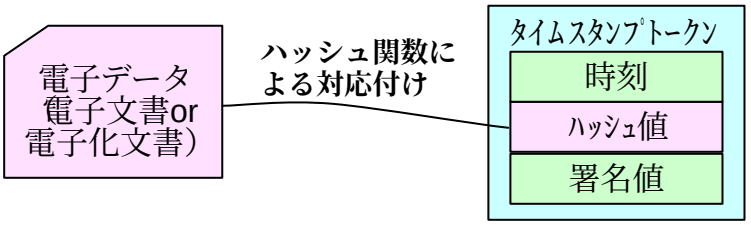


図２．１　電子データとタイムスタンプの関係

（2）タイムスタンプトークンの非改ざん性を確認できること

PKI 方式タイムスタンプでは、デジタル署名によってタイムスタンプトークンの非改ざん性を説明する。安全なデジタル署名アルゴリズムを利用することにより、タイムスタンプトークンが改ざんされていないことを証明することができる。

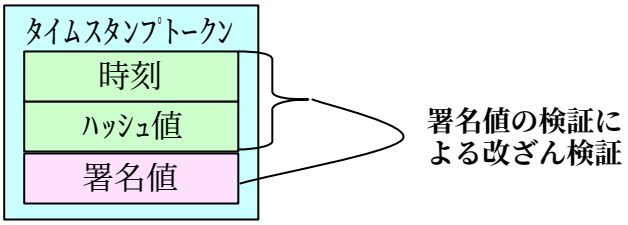


図２．２　タイムスタンプトークンの非改ざん性

（３）タイムスタンプの発行主体を確認できること

PKI 方式タイムスタンプではタイムスタンプの発行主体が誰であるかは、デジタル署名の生成に用いる秘密鍵と一対一に対応する公開鍵に対して認証局が発行する公開鍵証明書によって説明される。秘密鍵は本人のみが利用できる状態に維持されていることが前提である。

秘密鍵の安全性が確保され、公開鍵証明書の有効性が確保されることにより、タイムスタンプの本人性を確認することができる。

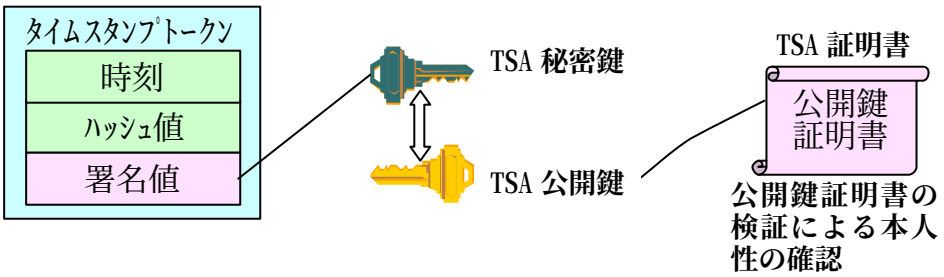


図２．３　公開鍵証明書による発行主体の確認

（４）信頼点の正当性を確認できること

PKI 方式タイムスタンプで用いられるデジタル署名や公開鍵証明書の正当性を確認するためには、その信頼点である（ルート）認証局の公開鍵証明書を基点とした認証パスが構築できなければならない。また、その信頼点自身が正当であり、正当な信頼点からタイムスタンプの公開鍵証明書を結ぶ認証パスが正しく構築されることを確認できる必要がある。

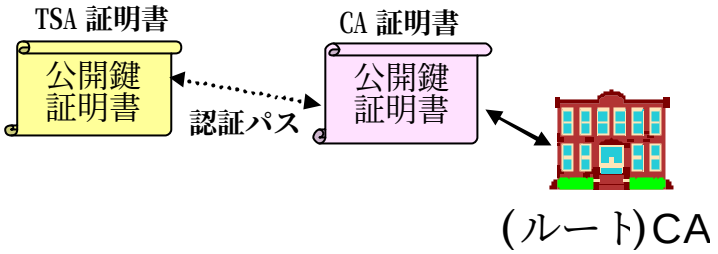


図２．４　CA 証明書による信頼点の正当性確認

（５）TSA が適切に運用されていることを確認できること

TSA が規定や基準等に沿った適切な運用を実施していることを確認できる必要がある。

２．１．２　リンク方式タイムスタンプの有効性

ハッシュ関数によるリンクを利用したタイムスタンプ（リンク方式タイムスタンプ）が有効であるのは、次の要件を満たす場合である。

（１）電子データとタイムスタンプとの関係を証明できること

リンク方式タイムスタンプでは、タイムスタンプトークンがまさにその電子データを対象とすることを証明できることが必要である。リンク方式タイムスタンプでは対象とする電子データのハッシュ値をタイムスタンプトークンに含めることによって、対象データと対応付ける。

（２）タイムスタンプトークンの非改ざん性を確認できること

リンク方式タイムスタンプでは、タイムスタンプトークンの非改ざん性は TSA に保管されている情報との照合によって証明される。このためリンク方式タイムスタンプの有効性確保には、照合用データが TSA において確保されている必要がある。

（３）タイムスタンプの発行者を確認できること

リンク方式タイムスタンプでは、タイムスタンプの付与及び照合において TSA の運営するサイト等への問合せを行う。リンク方式タイムスタンプの有効性確保には、問合せ先が想定している TSA が運営しているサーバであることを確認する必要がある。なお、TSA の運用の継続性が確保されない場合には、TSA が保管する照合用データ及びリンク情報ならびに当該データを用いた検証方法が利用者に提供され、それらが想定している TSA から提供されたものであることを確認する必要がある。

（4）信頼点までの正当性を確認できること

リンク方式タイムスタンプでは、タイムスタンプの正当性の確認に使用される情報の非改ざん性は、その正当性の確認に使用される情報に係るリンク情報について、明証化（明証化とは、「明らかに証拠となる状態とすること」を言う。明証化の例としては、新聞等の定期刊行物への掲載が挙げられる。）されたリンク情報の代表値までのリンクのつながりが確保されていることにより証明される。リンク方式タイムスタンプの有効性確保には、TSA が規定する方法により、リンク情報の代表値が明証化されていることが確認できるとともに対象のタイムスタンプトークンに係るリンク情報について、明証化されたリンク情報の代表値までの整合性が確保される必要がある。

（5）TSA が適切に運用されていることを確認できること

TSA が規定や基準等に沿った適切な運用を実施していることを確認できる必要がある。

２．２　タイムスタンプ長期保証の要件

前節を踏まえ、PKI 方式及びリンク方式タイムスタンプのそれぞれにつき、その有効性を長期にわたって保証するための要件について記す。

２．２．１　PKI方式タイムスタンプ長期保証の要件

PKI 方式タイムスタンプの長期保証のためには、２．１．１で述べた要件を長期間保証する必要がある。

（1）長期経過後に電子データとタイムスタンプとの対応関係を証明できること

ハッシュ関数は多対一関数であり、その安全性（非衝突性）は計算量的なものである。つまり同一のハッシュ値を持つ異なった複数のデータを求めるために消費する計算時間が十分に長い（事実上不可能である）ことで説明されるものである。従って長期経過に伴う技術の進歩により、安全性が損なわれてしまう（脆弱化する）可能性がある。

利用するハッシュ関数が脆弱化して非衝突性を保てなくなると、タイムスタンプが元の電子データのものであることを証明できなくなる。

長期として想定する期間によっては、その期間にわたって十分な安全性を確保できるハッシュ関数を用いることで対処可能である場合も考えられるが、技術の進歩を正確に予測することは難しく、予めハッシュ関数の脆弱化を想定した対処策を用意しておくことが望ましい。

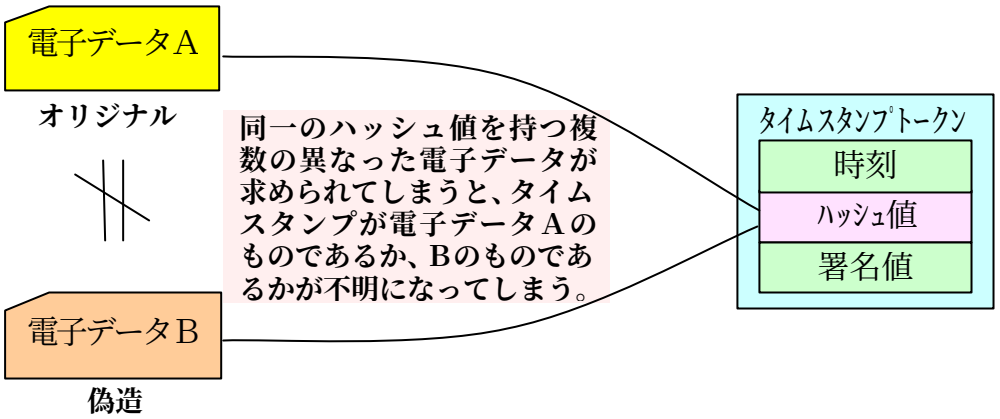


図２．５　ハッシュの衝突による電子データとタイムスタンプの関係の崩れ

（２）長期経過後にタイムスタンプトークンの非改ざん性を確認できること

デジタル署名アルゴリズムについても、その安全性は計算量的なものである。特にデジタル署名で用いるハッシュ関数は（１）と同様の問題を引き起こす。

利用するハッシュ関数が脆弱化して非衝突性を保てなくなると、タイムスタンプが偽造されたものであるか否かを判断できなくなる。

十分な長期間にわたって安全性の確保可能なアルゴリズムの利用、予めアルゴリズムの脆弱化を想定した対処法の用意が必要である。

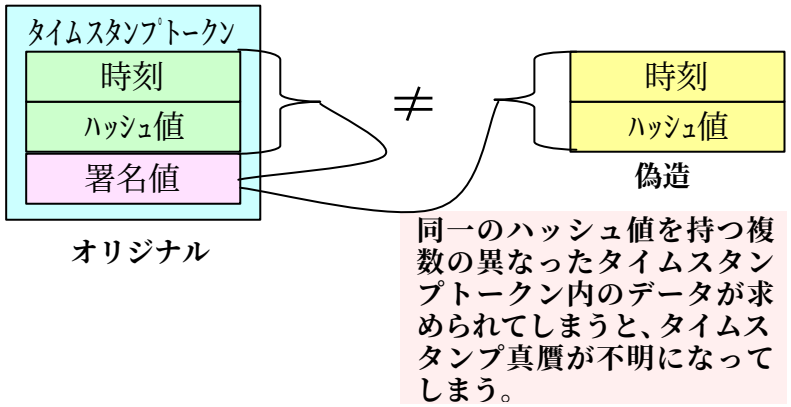


図２．６　署名の脆弱化によるタイムスタンプ真贋の不明化

（３）長期経過後にタイムスタンプの発行主体を確認できること

タイムスタンプの発行主体確認のためには、秘密鍵の安全性確保は必須要件である。HSM の利用や安全な運用管理により秘密鍵の漏洩を防止しなければならない。こうして漏洩防止ができたとしても、長期経過による技術の進歩により公開鍵アルゴリズムが脆弱化し、公開鍵から秘密鍵が算出可能となる場合が考えられる。公開鍵アルゴリズムが脆弱化に備える必要がある。

また、公開鍵証明書には１年から５年程度の有効期限が必ず存在するし、場合によっては失効も生じうる。有効期限後や失効後は公開鍵証明書の有効性は失われ、発行主体を保証することができなくなる。有効期限や失効に対処できることが必要である。

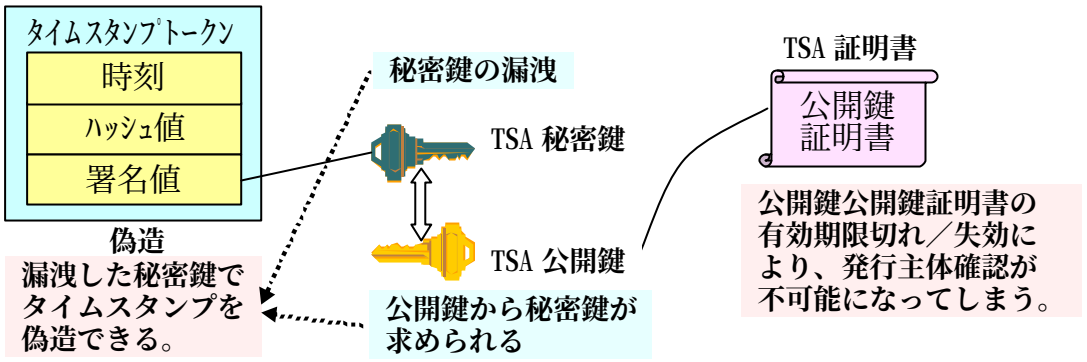


図２．７　公開鍵アルゴリズムの脆弱化による発行主体確認の不可能化

（４）長期経過後に信頼点の正当性を確認できること

公開鍵証明書検証に用いる信頼点が、当時実際に利用されていたものであることを確認できなければならない。正当な信頼点が実際に用いている鍵ペア（公開鍵と秘密鍵のペア）の偽造は困難であったとしても、見かけ上、所有者名や発行者名が同一である公開鍵証明書を偽造することは容易であり、偽造した公開鍵証明書に基づいて下位 CA あるいは TSA の公開鍵証明書を（鍵ペアを除き）すべて偽造することが可能である。単に保存してある検証情報に基づいて公開鍵証明書を検証するだけでは正しい判定はできない。

保存してある信頼点情報（ルート認証局の公開鍵証明書など）が、当時利用されていた信頼点情報と同一であるか否かを確認できることが重要である。

また、CP/CPS などに基づいて秘密鍵の用途が正しいことを確認できることも必要である。

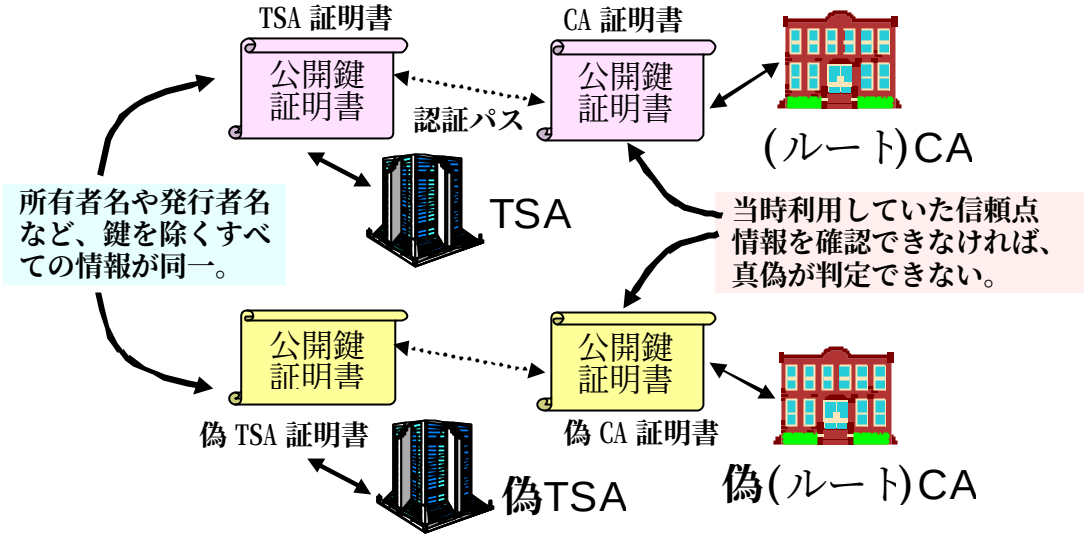


図２．８　信頼点偽造による TSA 証明書の無効化

（５）長期経過後に TSA が適切に運用されていたことを確認できること

TSA が当時、適切に運用されていたことを確認できることが望ましい。そのためには、TP/TPS 等を確認できると良い。

２．２．２　リンク方式タイムスタンプ長期保証の要件

リンク方式タイムスタンプの長期保証のためには、２．１．２で述べた要件を長期間保証する必要がある。

（１）長期経過後に電子データとタイムスタンプとの関係を証明できること

ハッシュ関数は多対一関数であり、その安全性（非衝突性）は計算量的なものである。つまり同一のハッシュ値を持つ異なった複数のデータを求めるために消費する計算時間が十分に長い（事実上不可能である）ことで説明されるものである。従って長期経過に伴う技術の進歩により、安全性が損なわれてしまう（脆弱化する）可能性がある。

長期として想定する期間によっては、その期間にわたって十分な安全性を確保できるハッシュ関数を用いることで対処可能である場合も考えられるが、技術の進歩を正確に予測することは難しく、予めハッシュ関数の脆弱化を想定した対処策を用意しておくことが必要である。

（２）長期経過後にタイムスタンプトークンの非改ざん性を確認できること

TSA が保管する照合用データが失われると、タイムスタンプが偽造されたものであ

るか否かを判断できなくなる。

十分な長期間にわたって照合用データを確保するため、TSA は照合用データの滅失・毀損を防止できる対処を行うことが望ましい。

また、リンク方式タイムスタンプにおいては、使用しているハッシュ関数に対する最新の安全性評価結果や TSA の事業方針によりタイムスタンプの有効期限が設定される。有効期限後はタイムスタンプの有効性が失われる可能性があるため、有効期限前のある時点でタイムスタンプが有効であったとともに、それ以降タイムスタンプトークンが非改ざんであることを確認できるための対処が必要である。

（3）長期経過後にタイムスタンプの発行者を確認できること

リンク方式タイムスタンプの付与及び照合においては、利用者は TSA の運営するサイト等への問合せを行うが、正しい問合せ先に対してタイムスタンプ付与もしくは照合の要求を行っていることを確認する必要がある。そのためには、TSA により問合せ先の認証が可能な方法により問合せ先の運営が継続されているとともに、利用者は問合せ先が正しい TSA が運用するサーバであることを確認する必要がある。なお、TSA の運用の継続性が確保されない場合には、利用者が信頼点までの正当性を確認する必要がある。そのためには、TSA が保管する照合用データ及びリンク情報ならびに当該データを用いた検証方法を利用者に提供し、利用者が明証化されているリンク情報の代表値までのリンクのつながりを確認することにより、想定している TSA から発行されたタイムスタンプであることを確認する必要がある。

（4）長期経過後に信頼点までの正当性を確認できること

利用者がリンク情報及び照合用データが改ざんされていないことを確認するため、TSA は、規定に従いリンク情報の代表値を明証化するとともに、そこまでのリンク情報及び照合用データの整合性を確保しなくてはいけない。また、利用者は TSA が規定していた信頼点において、リンク情報の代表値が明証化されていることを確認する必要がある。

また、ある時点のリンク情報は、過去のリンク情報や照合用データよりハッシュ関数を用いて計算される。そのため、リンク情報のつながりによる照合用データの非改ざん性の証明の効力は、使用されているハッシュ関数の安全性に依存しており、（1）と同様の問題がある。

利用しているハッシュ関数が脆弱化して非衝突性を保てなくなると、タイムスタンプトークンの照合用データが元のデータから改ざんされていないことを証明することが困難となる。

十分な長期間にわたって安全性の確保可能なアルゴリズムの利用、予めアルゴリズムの脆弱化を想定した対処策の用意が必要である。

なお、TSA の運用の継続性が確保されない場合には、利用者が信頼点までの正当性を確認する必要がある。そのためには、TSA が保管する照合用データ及びリンク情報ならびに当該データを用いた検証方法を利用者に提供し、利用者が明証化されているリンク情報の代表値までのリンクのつながりを確認する必要がある。

（5）長期経過後に TSA が適切に運用されていたことを確認できること

より信頼性を高めるために、TSA が適切に運用されていたことを確認できることが望ましい。そのためには、少なくとも当時の TP/TPS 等を確認できることが望ましい。

３．タイムスタンプによる長期保証の方法

タイムスタンプには有効期限があり、その有効期限を越えて長期に有効性を維持するためにはタイムスタンプが有効な間にタイムスタンプを新たに付与する手段により有効性を延長し長期保証する方法がある。以下は方式別に手段を解説する。

３．１　PKI方式タイムスタンプ

PKI 方式によるタイムスタンプでの長期保証は、対象文書のハッシュと対象文書の関係が確保できていて、かつそのハッシュが含まれるトークンが改ざんされてないことが証明できる必要がある。さらに利用されるタイムスタンプの秘密鍵の安全性を確保するため、タイムスタンプの発行元が明確で TSA 証明書が失効してないことと、正しく信頼できる時刻のトークンである必要がある。

タイムスタンプの検証が可能な期間は、TSA 証明書に設定された有効期間に依存し、有効期間の間は認証局（CA）より提供される失効情報（CRL）により検証が可能である。TSA 公開鍵証明書の有効期間を超えてそのタイムスタンプの有効性を保持したい場合は、将来に渡って検証する為に必要十分な情報を収集し、それらを元のタイムスタンプ対象データ、タイムスタンプトークンと一緒にまとめたものに対して、TSA 公開鍵証明書の有効期間内に新たなタイムスタンプを取得する必要がある。

有効期限以前に暗号の脆弱化の恐れがある場合においてはタイムスタンプの有効性を延長するために、脆弱化する前に検証に必要な失効情報などを全て収集し、より暗号強度の高いアルゴリズムのタイムスタンプを取得する必要がある。

３．１．１　タイムスタンプトークン

この章では、タイムスタンプトークンのデータ構成について PKI 方式のタイムスタンプである ISO/IEC18014-2(PKI 方式)や RFC3161 などの規格のように規格化され公開されたトークンであることが望ましい。規格化されたものであれば将来に渡りデータ構造が確認でき互換性が維持できることになる。

３．１．２　実装要件

TSA 公開鍵証明書の有効期間を超えてそのタイムスタンプの有効性を保持する為に、新たなタイムスタンプを取得していく際のデータ構成は、図３．１の様になる。

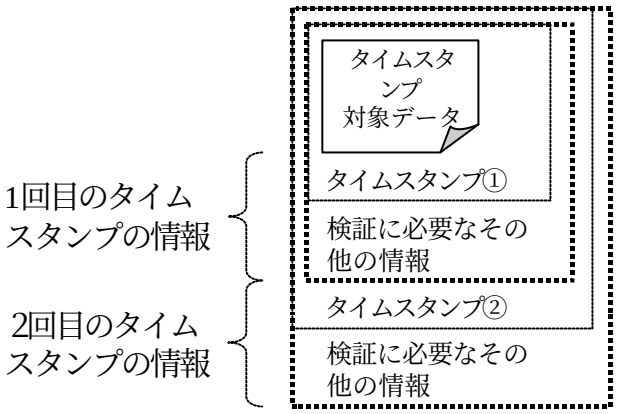


図３．１ 長期有効性確保の為のタイムスタンプにおけるデータ構成

図３．1 の中の「検証に必要なその他の情報」とは即ち、TSA 公開鍵証明書の有効期間内だけでなく、有効期間を過ぎた後でもタイムスタンプの検証をする為に必要な情報であり、具体的には次のとおりである。

- **タイムスタンプ対象データ**
- **タイムスタンプトークン**
- **TSA 公開鍵証明書**
- **TSA 公開鍵証明書に対する CRL（ARL）**
- **TSA 公開鍵証明書の認証パス及び、その構築に必要な情報**
  - **Root-CA に至るまでの CA 公開鍵証明書**
  - **Root-CA に至るまでの CA 公開鍵証明書に対する CRL（ARL）**
  - **Root-CA に至るまでの CA に対する CP/CPS**
- **TSA の TP/TPS**

これらは、検証プログラム上でロジカルに検証処理できるものもが殆どであるが、TP/TPS はそのデータ形式が規格化されていないだけでなく、必ずしも電子データで保管されるとも限らない為、最終的には文書化された TP/TPS を人の目で判読して全体の整合性を確認する事が必要となる。

また、個々のタイムスタンプ対象データに対して、比較的情報量の多い TP/TPS を含んでタイムスタンプを取得し、保存するのは運用上現実的ではない。よって TP/TPS に関しては、タイムスタンプ利用者が上記仕組みとは独立した形で保管しておいても良い。
さらに、長期に渡ってタイムスタンプの有効性を保証するためには、検証するためのアプリケーションが永続的に存在するとは限らないため、将来改めて検証アプリケーションを作れるように TP/TPS にタイムスタンプトークンのプロファイルが公開されていることが望ましい。

なお、TP/TPS とタイムスタンプトークンとは TSA ポリシーの識別子が TP/TPS の中で

定義され、それが、タイムスタンプトークンの中にポリシーとして設定される事で関連付けられる。

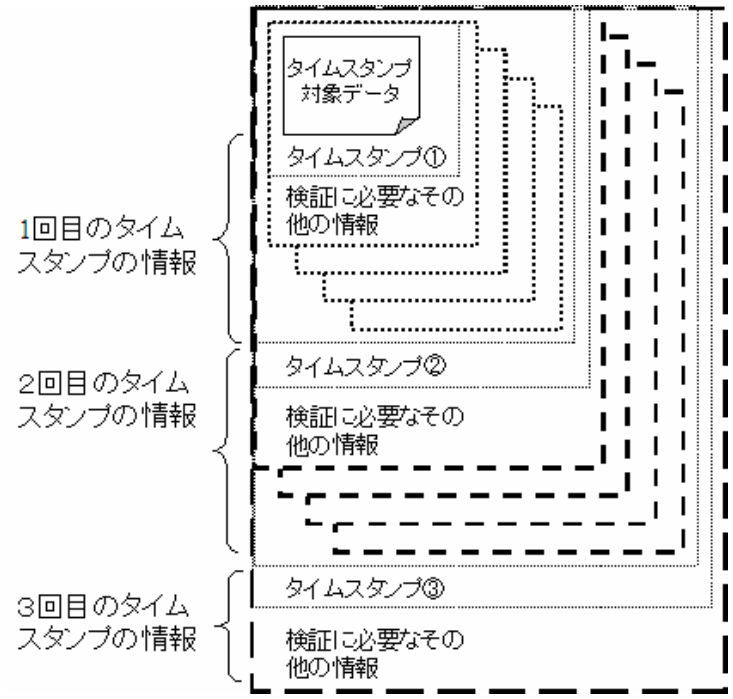


図３．２　複数のデータに対してタイムスタンプを重ねていく場合

図３．１では図解の便宜上、一つのタイムスタンプ対象データに対して、一対一の関係でタイムスタンプを重ねていくように表現しているが、実際は図３．２の様に一対一である必要はなく、複数の「１回目のタイムスタンプの情報」に対して２回目のタイムスタンプを取得しても良いし、更に２回目、３回目のタイミングで複数束ねた情報に対してタイムスタンプを取得して行っても良い。ただし、その場合は次の事項に留意する必要がある。

① タイムスタンプの対象となった複数のデータの順序などを含む構成情報を将来にわたって維持・判別できる状態にしておく必要がある。

② タイムスタンプの対象となる情報を増大させると、本来検証したい情報以外のものも検証者の手元にある必要性が発生するので、例えば検証者に対して情報開示できるものとできないものを区別してタイムスタンプ対象にまとめる必要がある可能性がある。

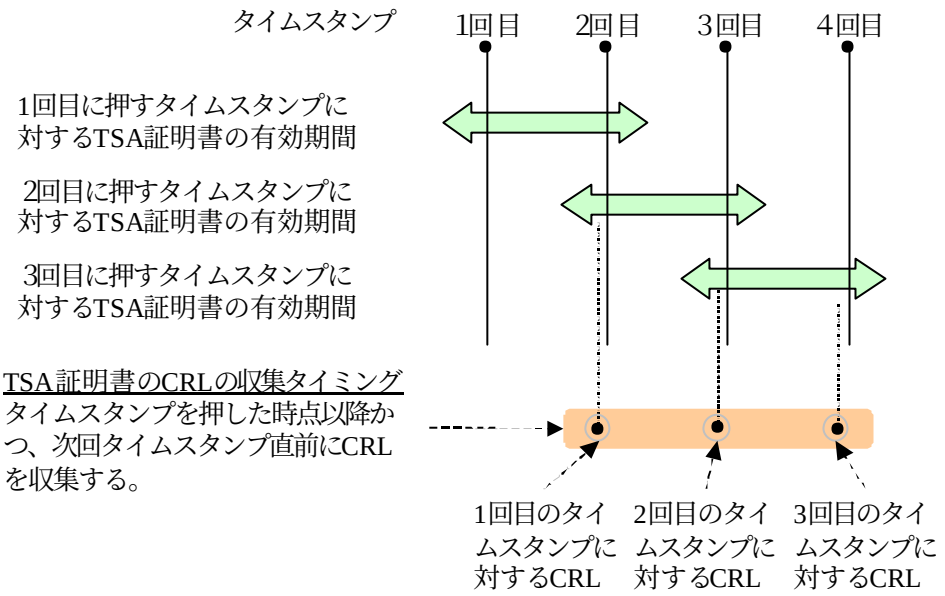
３．１．３　新たなタイムスタンプ取得時の手順

① 既にタイムスタンプの有効性が失われている情報に対して、有効性を延長させる処置は不可能である。よって過去に付与されているタイムスタンプの検証を行い、それらの有

効性を確認する事を強く推奨する。

② タイムスタンプ後、タイムスタンプ生成以降に発行された TSA 証明書の CRL(ARL)、中間 CA の CRL(ARL)、及び TSA、CA の公開鍵証明書など、前述の「タイムスタンプ検証に必要な情報」を各機関のリポジトリからダウンロードして収集しておく。図３．３は TSA の公開鍵証明書に対する CRL(ARL)を収集するタイミングのイメージを図式化したものであるが、TSA の公開鍵証明書を取得するタイミングは、その証明書が失効される可能性を考慮して、次にタイムスタンプを取得するタイミングにより近い事が望ましい。

③ 上記①のタイムスタンプの有効期間内に、タイムスタンプの対象となったデータ、及び上記①で収集した情報も含めたものに新たなタイムスタンプを取得する。



※CRL以外に、TSA証明書、CA証明書の収集タイミングは、それらの有効期限内ならいつでも良いが、システム構築上、CRL収集時点が妥当かと思われる。

図３．３　TSA 公開鍵証明書に対する CRL の収集タイミング

３．１．４　タイムスタンプの検証

「３．１．１」で述べた長期有効性保証の為のタイムスタンプを検証する際は、各 TSA 公開鍵証明書の有効期間内に検証するロジックとは異なる。
有効期間内においては、通常は次のような検証処理を行っている。
タイムスタンプ対象データのハッシュ値を計算し、タイムスタンプトークン内のハッシュ値と比較する。

① タイムスタンプトークン自体の検証を行う。
(ア) TSA 秘密鍵でハッシュ値を暗号化されたデータを TSA 公開鍵で復号し、その値とタイムスタンプトークンに含まれるハッシュ値とを比較する。
(イ) TSA 公開鍵証明書の認証パスを構築（ルート CA 公開鍵証明書などのトラストアンカに至るまでの情報を収集）し、CA 公開鍵証明書、CRL（ARL）などの検証を行う。その際通常は各公開鍵証明書に記述されている URL から CRL(ARL)をダウンロードする事になる。
(ウ) ルート CA 公開鍵証明書に関しては、その Fingerprint 値を、公知されている情報と比較する。（通常は検証を行う環境で信頼のおけるルート CA の証明書がセキュアにストアされているので、Fingerprint 値を目視確認する必要は無い）

② 検証者が予め知らされたリポジトリ上にある TP/TPS の内容を検証者の判断により、必要に応じて内容を確認する。

有効期間を過ぎた時点では、上記検証処理の中で次の箇所が異なる。
① 各証明書の CRL(ARL)は、公開鍵証明書に記述されている配布ポイントから検証時点で取得するのではなく、予め保存され、その上にタイムスタンプされた CRL(ARL)を参照して検証する事により、CA 及び TSA の公開鍵証明書がタイムスタンプを押した時点では失効されていなかった事を確認する。

② TSA 公開鍵証明書に対する CRL(ARL)の発行日時は、タイムスタンプ日時以降である事を確認する。

③ ルート CA 公開鍵証明書に関しては、その Fingerprint 値を、公知されている情報と比較する。（検証環境にルート CA 公開鍵証明書がストアされていない事を想定）

④ 検証者が過去に取得した TP/TPS、もしくは新たにタイムスタンプを重ねた対象データ内の TP/TPS の内容について必要に応じて確認する。（TSA 自体もしくは TSA のリポジトリ上にはタイムスタンプの日時時点での TP/TPS が存在しない可能性を想定）

⑤ タイムスタンプに使用された暗号アルゴリズムが過去時点（再タイムスタンプ時点）において、脆弱化していなかったのかどうかの確認を必要に応じて実施する。（信頼のできる機関、あるいは、検証者が、過去に使用された暗号アルゴリズムの安全性に係わる情報を維持管理していることを想定）

３．１．５　データフォーマット

複数の文書１つにまとめて再タイムスタンプをしていく場合、そのデータフォーマットの要件は、「新たにタイムスタンプを追加していく過程のアルゴリズム、及びデータフォーマットは公開されている事」である。例えば、２度目以降のタイムスタンプの対象となる情報はそれぞれ独立したファイルだとすれば、それらを、公開されたアルゴリズムを使ったツールを利用して一つのファイルに一まとめにし、そのファイルに対してタイムスタンプを生成していく、という事も考えられる。また、増分更新形式の文書フォーマットである PDF 形式／XML 形式などのファイル形式においても、前者の例のように置き換えて実施する事も可能である。

ちなみに、デジタル署名の有効性長期保証に関しては、RFC3126 などにデータフォーマットが規格化されており、タイムスタンプの有効性を延長するために応用されることが期待される。

３．２　リンク方式タイムスタンプ

３．２．１　リンク方式タイムスタンプ長期保証の要件の整理

リンク方式タイムスタンプについて、２．２．２で述べた長期保証の要件をまとめると、以下の事項となる。

＜長期保証の要件＞

① ハッシュ関数に係る要件

２．２．２（１）及び（４）のハッシュ関数に係る記載事項をまとめると、タイムスタンプ対象データのハッシュ値の計算及びリンク情報の計算に使用されるハッシュ関数の脆弱化に対して、タイムスタンプの対象データの非改ざん及び存在日時の確認を可能とする対処策を TSA が用意するとともに、利用者が当該対処策を実施することが要件となる。

② 有効期限に係る要件

２．２．２（２）の有効期限に係る記載事項をまとめると、タイムスタンプの有効期限が過ぎた後も、タイムスタンプの対象データの非改ざん及び存在日時の確認を可能とする対処策を TSA が用意するとともに、TSA 及び利用者が当該対処策を実施することが要件となる。

③ リンク情報に係る要件

２．２．２（４）のリンク情報の整合性に係る記載事項をまとめると、TSA がリンク情報の整合性を確保するための措置を講じるとともに、リンク情報の不整合に対して対処を実施することが要件となる。

④　タイムスタンプの発行者に係る要件

２．２．２（３）の記載事項をまとめると、利用者がタイムスタンプ付与・照合時の問合せ先の認証を実施することと、運用の継続性が確保されない場合には照合用データ及びリンク情報ならびに当該データを用いた検証方法が利用者に提供され、その提供元が確認できることが要件となる。

⑤　信頼点に係る要件

２．２．２（４）のリンク情報の代表値の明証化に係る記載事項をまとめると、利用者がリンク情報の代表値の確認を実施することが要件となる。

⑥　TSA の運用に係る要件

２．２．２（５）の記載事項をまとめると、TSA が TSA による内部監査あるいは TA による外部監査のログ、TSA ポリシー等を利用者に開示し、利用者が当該文書の内容を確認することが要件となる。

３．２．２　リンク方式タイムスタンプ長期保証の実現例

長期保証の要件①及び②を満たすため、効力が切れた後のタイムスタンプが有効であったことの確認を可能とするための実現例を以下に記載する。

なお、以下の実現例の説明においては、「タイムスタンプ A」とは、既に付与されており、効力が切れる時期が近づいているタイムスタンプをいうこととし、「タイムスタンプＢ」とは、タイムスタンプ A の効力が切れた後に対象データの非改ざんと存在日時の確認を可能とするために新たに付与するタイムスタンプをいうこととする。

（１）利用者がタイムスタンプＡの照合に必要となる全てのデータを収集する場合

長期保証の要件①及び②について、ハッシュ関数の脆弱化が発生した場合やタイムスタンプの有効期限が満了した場合には、タイムスタンプＡの検証が成功することを確認した後、タイムスタンプ A の効力が切れる前に、下記のデータに対して、より長く効力が持続するタイムスタンプ B を付与することにより、タイムスタンプ A の効力が切れた後にも対象データの非改ざんと存在日時の確認が可能となる。

＜タイムスタンプ B の対象データ＞

① タイムスタンプ A の対象データ
② タイムスタンプトークン A
③ タイムスタンプ A から明証化されたリンク情報の代表値までのリンクの確認に使った照合用データ
④ タイムスタンプ A から明証化されたリンク情報の代表値までのリンクの確認に使ったリンク情報

図３．４に、上記①～④のデータ例を示す。

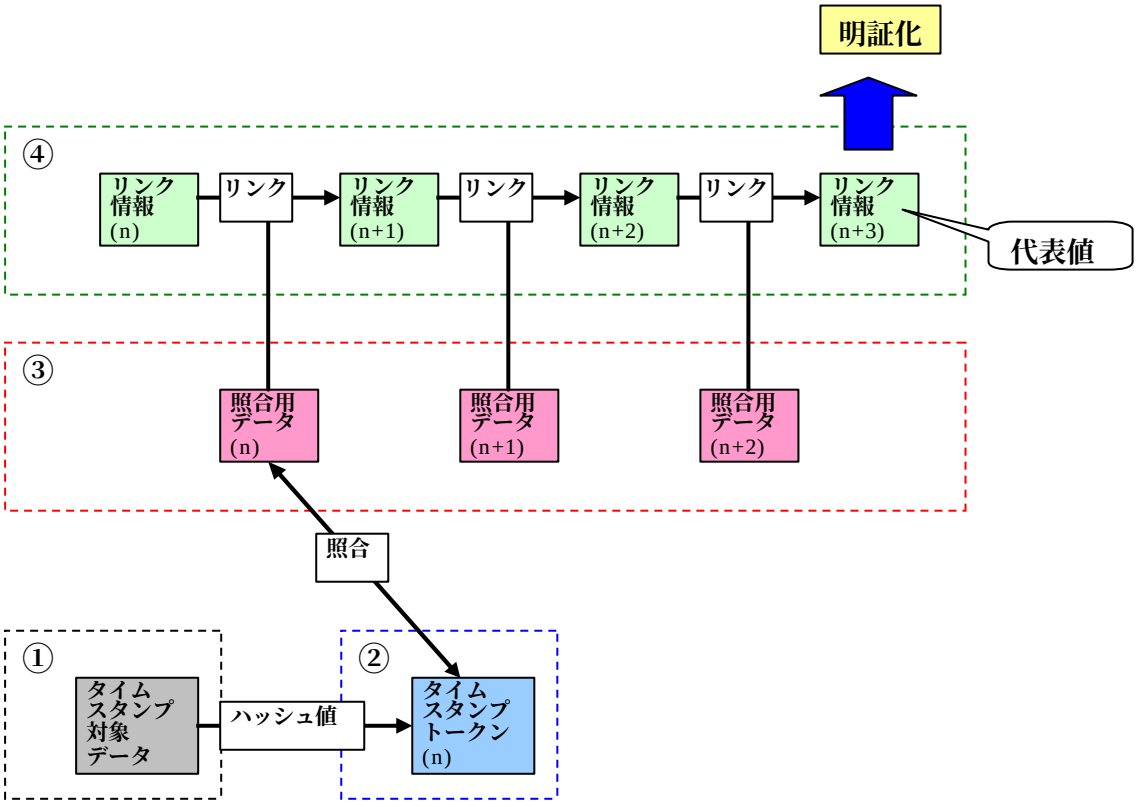


図３．４　タイムスタンプ B の対象データ例

利用者が上記のデータに対するタイムスタンプ B の付与を実施するため、TSA はタイムスタンプ A に係るリンク情報及び照合用データならびに当該データを用いた検証方法を利用者に提供する必要がある。

本実現例において、タイムスタンプ A に係る対象データの非改ざんと存在日時の確認をする際には、利用者は上記のタイムスタンプ B の対象データ及びタイムスタンプトークン B を保持し、それらを用いて以下を確認する必要がある。

＜確認事項＞

① タイムスタンプ B の検証に成功すること
② タイムスタンプトークン A に含まれるハッシュ値と、その対象データから計算されるハッシュ値が一致すること
③ タイムスタンプトークン A の照合用データを使用し、タイムスタンプトークン A の照合が成功すること
④ タイムスタンプ A の照合用データ及びタイムスタンプ A に係るリンク情報について、明証化されたリンク情報の代表値までのリンクの整合性が確保されていること

⑤ タイムスタンプ B が付与された時点で、タイムスタンプ A に係る TSA ポリシーにおいて、安全なハッシュ関数を使用する旨を明記していたこと
⑥ タイムスタンプ B がタイムスタンプ A の有効期間内に付与されていること

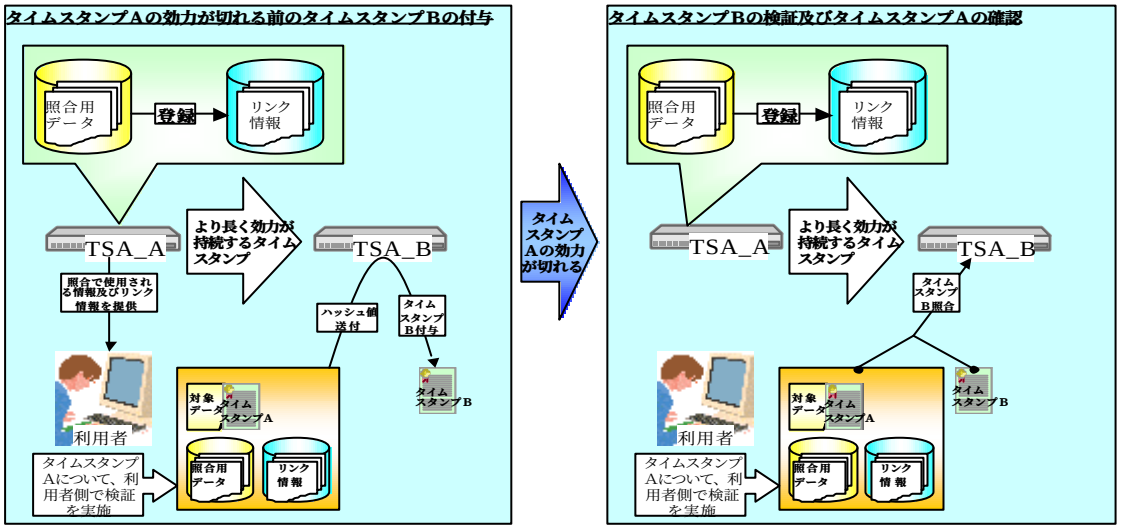


図 3．5　利用者が全ての情報を収集する実現例

（2）タイムスタンプAを発行した TSA の照合業務が継続される場合

なお、（1）の場合の実現例においては、リンクの方式によっては保管が必要な情報が膨大となるとともに利用者側でのタイムスタンプ A に係る検証作業の実施が困難である場合があり得る。タイムスタンプ A を発行した TSA による照合業務が継続される場合には、利用者の負担が軽い方法として、利用者がタイムスタンプAの検証が成功することを確認した後、タイムスタンプ A の効力が切れる前に下記のデータに対して

タイムスタンプ B を付与する方法もある。

＜タイムスタンプ B の対象データ＞

① タイムスタンプ A の対象データ

② タイムスタンプトークン A

本実現例において、タイムスタンプ A に係る対象データの非改ざんと存在日時の確認をする際には、利用者は上記のタイムスタンプ B の対象データ及びタイムスタンプトークン B を保持し、それらを用いて以下を確認する必要がある。

＜確認事項＞

① タイムスタンプトークン A に含まれるハッシュ値と、その対象データから計算されるハッシュ値が一致すること

② タイムスタンプ A に係る TSA に問合せを行い、問合せ先が正当な TSA であること

③ タイムスタンプ A に係る TSA に問合せを行い、タイムスタンプトークン A の照合が成功すること

④ タイムスタンプBが付与された時点で、タイムスタンプ A に係る TSA ポリシーにおいて、安全なハッシュ関数を使用する旨を明記していたこと

⑤ タイムスタンプ B がタイムスタンプ A の有効期間内に付与されていること

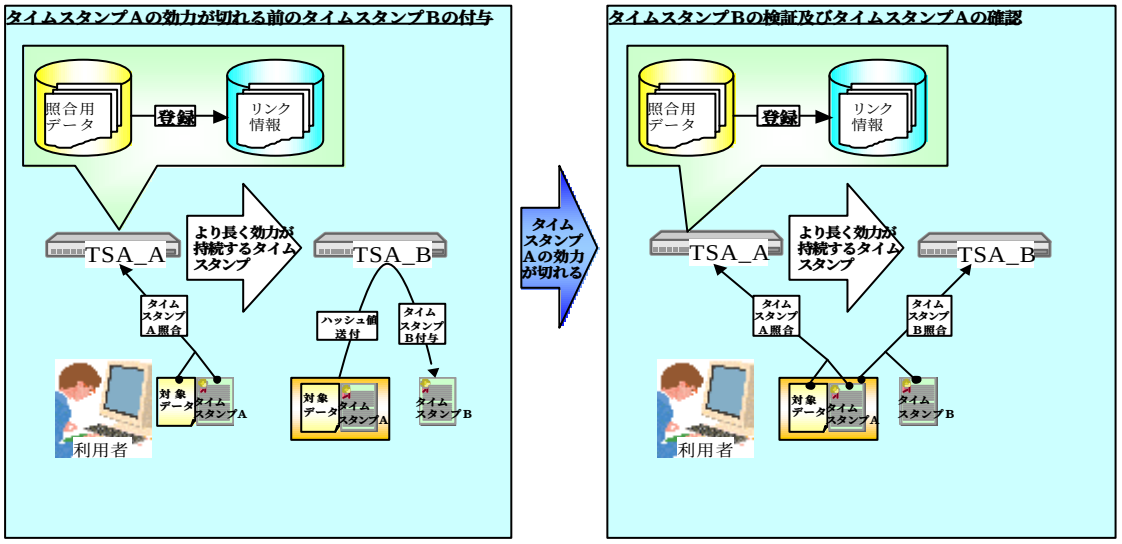


図 3．6　照合業務が継続される場合の実現例

但し、リンク情報の生成に使用するハッシュ関数の脆弱化が発生した場合は、リンク情報及び照合用データの非改ざんを証明するため、TSA は下記のデータに対してタイムスタンプ B を付与する等の対処を実施する必要がある。

＜ハッシュ関数脆弱化時の TSA 側でのタイムスタンプ B の対象データ＞

① 脆弱化したハッシュ関数で計算されたリンク情報に係る照合用データ

② 脆弱化したハッシュ関数で計算されたリンク情報

３．２．３　リンク方式のタイムスタンプの長期保証を実現するために実施すべき事項

３．２．２に示したタイムスタンプの長期保証を実現させるために、TSA で継続的に実施する必要がある事項についての実現例を下記に示す。

（１）ハッシュ関数の二重化（長期保証の要件①）

長期保証の要件①について、ハッシュ関数の脆弱化が発生した際には、（１）の対処を実施することによりタイムスタンプ A の効力が切れた後にも対象データの非改ざんと存在日時の確認が可能となる。但し、いつハッシュ関数の脆弱化が発生するかは予測が困難であり、タイムスタンプ A の有効性が確保されている間にタイムスタンプ B の付与を実施するための猶予が無い場合が想定される。そのための対処の実現例としては、図 3.7 に示すようにハッシュ関数を使用する処理（タイムスタンプ対象データのハッシュ値の計算及びリンク情報の計算）について、2 種類の異なるハッシュアルゴリズムを使用して完全に並列化する方法が考えられる。この並列化によりにより、片方のハッシュ関数の脆弱化が発生した場合にも、もう片方のハッシュ関数が脆弱化するまでの間は有効性を確保することが可能となり、タイムスタンプ B の付与を実施するための猶予が確保できる。

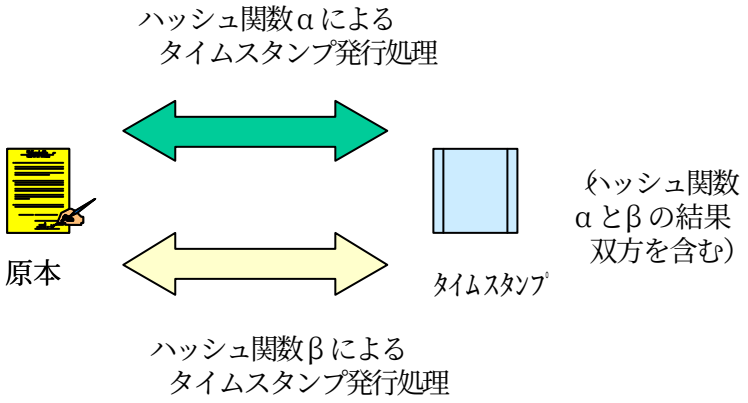


図 ３．７　ハッシュ関数の二重化の実現例

（2）リンク情報の整合性の確保及び不整合への対処（長期保証の要件③）

長期保証の要件③について、TSA はリンク情報の整合性を確保するとともに、TSA が保持するリンク情報のリンクのつながりにおいて不整合が発見された場合には、整合性の確保されたリンク情報を復旧する必要がある。実現例としては、TSA がリンク情報のつながりを定期的に確認するとともに照合用データやリンク情報のバックアップデータを保管し、リンク情報の不整合が発見された場合は、バックアップデータより正常なリンク情報を復旧する方法が考えられる。但し、万一何らかの事由により正常なリンク情報が復旧できない場合には、定期的に明証化されている代表値で区切られた区間のうち、当該不整合が含まれる区間に係るタイムスタンプは有効性が証明できないため、早急にその旨を利用者に通知する等の措置が必要となる。

（3）タイムスタンプ付与・照合時の問合せ先の認証（長期保証の要件④）

長期保証の要件④について、タイムスタンプの付与・照合を要求する際には、問合せ先が正当な TSA により運営されていることが確認できる方法により行い、確認を実施する必要がある。実現例としては、問合せ先を認証できるような通信方式の採用が考えられる。なお、TSA の運用の継続性が確保されない場合には、TSA が保管する照合用データ及びリンク情報ならびに当該データを用いた検証方法が利用者に提供され、それらが想定している TSA から提供されたものであることを確認する必要がある。実現例としては、運用が終了する際に、利用者に照合用データ及びリンク情報ならびに当該データを用いた検証方法を提供する方法が考えられる。

（4）リンク情報の代表値の確認（長期保証の要件⑤）

長期保証の要件⑤について、リンク情報の代表値の明証化においては、長期経過後にその内容を確認可能とする必要がある。実現例としては、国立国会図書館へ納本されている出版物へ掲載する方法が考えられる。

（5）TSA ポリシーの作成・公開及びタイムスタンプトークン内への識別情報の記載（長期保証の要件⑥）

長期保証の要件⑥について、TSA の運用については、長期経過後にその内容を確認可能とする必要がある。実現例としては、TSA ポリシーに TSA の運用方針を記載して公開するとともに、タイムスタンプトークンに TSA ポリシーを識別する OID を記載する方法が考えられる。

４．デジタル署名付文書を対象とする場合

PKI 方式タイムスタンプのデータフォーマットは、標準のデジタル署名フォーマット（RFC 3852, Cryptographic Message Syntax (CMS)）である。しかし、タイムスタンプでない一般のデジタル署名付文書とタイムスタンプとではいくつかの相違があるため、長期保証の要件も異なる部分がある。

本章では、PKI 方式タイムスタンプとタイムスタンプでない一般のデジタル署名付文書との相違点から、一般のデジタル署名付文書の有効性長期保証の要件をあげ、その有効性を長期にわたって保証するための方法を示す。

４．１　デジタル署名付文書の長期保証との関係

電子データにデジタル署名を添付し、それを検証するための典型的なパタンを図４．１に示す。

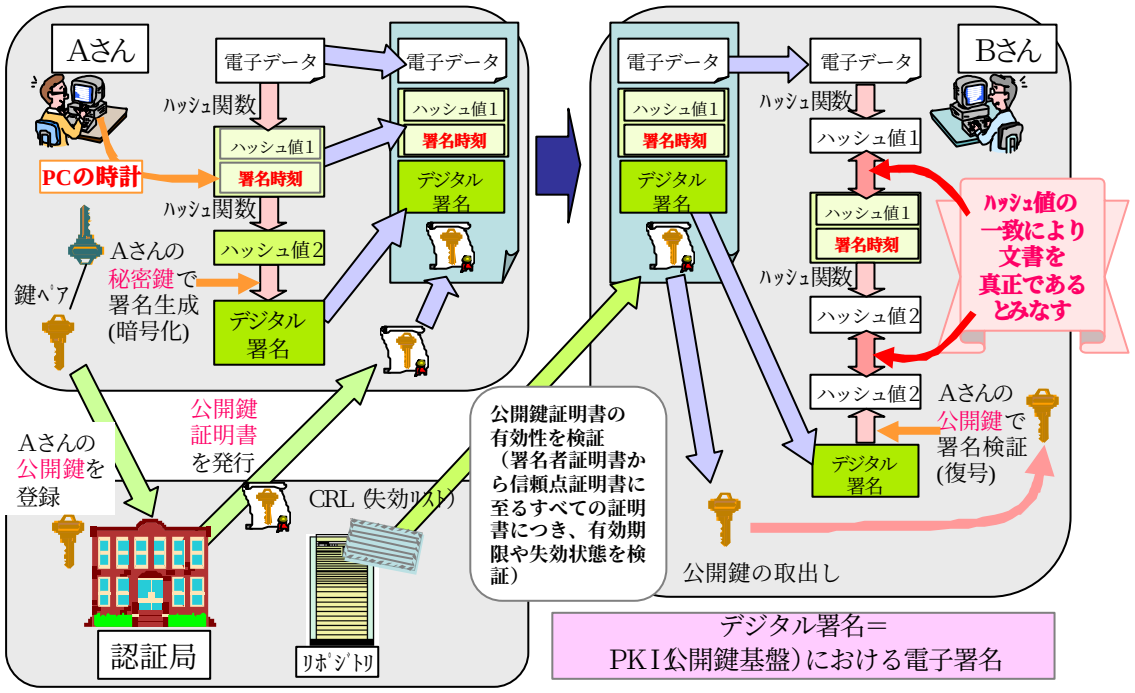


図４．１　デジタル署名

PKI 方式タイムスタンプはデジタル署名を用いているため、デジタル署名を添付された電子データ（これをデジタル署名付文書と呼ぶこととする）の一種であると見ることができるが、タイムスタンプでない一般のデジタル署名付文書とタイムスタンプとでは次の点が異なる。

（1）署名対象とタイムスタンプ対象

PKI 方式タイムスタンプにおける署名対象は、タイムスタンプ対象情報のハッシュ値や時刻情報を含むタイムスタンプ情報であり、タイムスタンプトークンの中にはタイムスタンプの対象である電子データ自体を含まない。一方、タイムスタンプでない一般のデジタル署名付文書の場合、署名の対象は電子データであり、標準の署名データ形式の中に電子データ自体を含むことができる。

（2）署名時刻

タイムスタンプの中には、厳密に管理された安全な時刻源より得た正確な時刻情報が含まれる。タイムスタンプでない一般のデジタル署名付文書にも署名時刻の情報を含めることができるが、その時刻源は署名生成プログラムが動作する PC の時計であるため、署名者が自由にコントロールできてしまう。つまり改ざんが可能であるため、信頼できない。

従って、デジタル署名付文書が有効であるための要件を、２．１．１に挙げた５項目と対比させて整理すると次のようになる。

表４．１　有効であるための要件の比較

	PKI 方式タイムスタンプ	その他のデジタル署名付文書
1	電子データとタイムスタンプとの関係を証明できること	－ （電子データがデジタル署名付文書に含まれていれば、デジタル署名付文書の非改ざん性の確認で十分。）
2	タイムスタンプトークンの非改ざん性を確認できること	デジタル署名付文書の非改ざん性を確認できること
3	タイムスタンプの発行主体を確認できること	デジタル署名の本人性を確認できること
4	信頼点の正当性を確認できること	信頼点の正当性を確認できること
5	TSA が正しく運用されていることを確認できること	－ （署名者の自己責任により正しく運用されていることが前提）
6	－ （上記（５）により正確な時刻が付与されていることが前提）	デジタル署名存在時刻を確認できること

デジタル署名付文書の長期保証においてタイムスタンプの長期保証要件と大きく異なるのは、まずそのデジタル署名（あるいはデジタル署名付文書）の存在時刻を確定する（図４．２　①）必要があることである。デジタル署名付文書の非改ざん性の確認やデジタル

署名の本人性の確認のための検証情報は、その確定時刻を基準として収集する（図４．２②）必要がある。その後、デジタル署名付文書と検証情報を改ざん不可あるいは改ざん検知可能な状態（図４．２　③）で長期にわたり保存（図４．２　④）する。

デジタル署名（あるいはデジタル署名付文書）の存在時刻の確定のためにはタイムスタンプを付与すればよい。そのタイムスタンプで示された時刻に基づき、その時点で有効な認証パスやその時刻以降に発行されたことが確認できる CRL などの検証情報を集める。デジタル署名付文書や検証情報等の証拠情報は、一体化あるいは別々に改ざん不可あるいは改ざん検知可能な状態で保存する。そのためにはタイムスタンプを利用することができる。このとき、タイムスタンプの有効期間を超えて有効性を保証しようとする場合、タイムスタンプを更に重ねて付与することが必要となる場合がある。

デジタル署名付文書の有効性再検証（デジタル署名がある時点において有効であったことの確認）のためには、まずデジタル署名（あるいはデジタル署名付文書）の存在時刻をタイムスタンプにより確認（図４．２　⑤）する。検証情報等の証拠情報が改ざんされていないことを確認（図４．２　⑥）の上、タイムスタンプによって示された時刻を想定してそれら証拠情報を確認（図４．２　⑦）する。なお、この際の証拠情報の確認には、デジタル署名及び認証パスの検証と、信頼点の確認（当時実際に利用されていた正当な信頼点であるかどうかの照合）を含む。

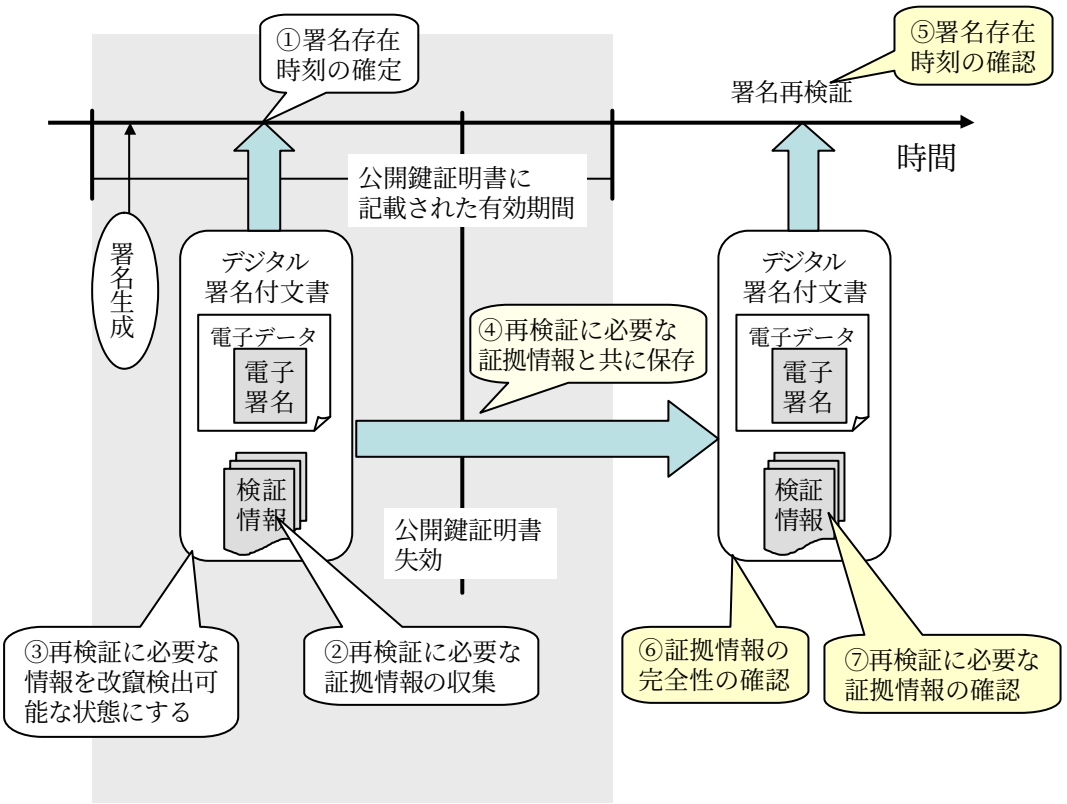


図４．２　デジタル署名付文書の長期保証の要件

このように、デジタル署名付文書の長期保証要件は、PKI 方式タイムスタンプの長期保証要件とほぼ同等であるが、デジタル署名付文書の長期保証のためには存在時刻確定のためのタイムスタンプを要する点が異なる。

なお、デジタル署名（デジタル署名付文書）には長期保証のための標準フォーマットが存在するが、タイムスタンプ（タイムスタンプ付文書）には現時点で長期保証のための標準フォーマットが存在しない点も異なる。

４．２　デジタル署名付文書を対象とする場合の方法

４．２．１　長期経過後のデジタル署名の正当性の確認方法の基本的な枠組み

ここでは、４．１で挙げられたデジタル署名付文書の長期保存における要件を満たすために必要な手順、および長期経過後にデジタル署名付文書の正当性を確認するための方法について説明する。

長期経過後にデジタル署名の存在時刻、デジタル署名付文書の非改ざん性、デジタル署名の本人性、および信頼点の正当性を確認するためには、次のような手順で必要な情報を保存しておく必要がある（図４．３）。

（１）デジタル署名時刻確定のタイムスタンプの付与

デジタル署名だけでは信頼ある署名生成時刻を確定できないため、署名者による改ざんや否認を防止できない。このため、デジタル署名が付与された後、デジタル署名が付与された時刻を確定するためにタイムスタンプを付与する。ここで、タイムスタンプの具体的な方式は、PKI 方式、リンキング方式のどちらでも良い。タイムスタンプの付与の対象、およびタイミングは以下のようになる。

（ア）　対象

付与対象は以下のどちらかである。

- デジタル署名自体（デジタル署名の存在時刻を確定する。署名対象文書については、電子署名の存在時刻が確定することにより間接的に存在時刻を確定する。）
- デジタル署名及び署名対象文書自体（デジタル署名と署名対象文書から構成されたデータの存在時刻を確定することになる）

（イ）　タイミング

デジタル署名が付与された後、出来るだけ速やかにタイムスタンプを付与する。

（2）デジタル署名の検証に必要な情報の収集

デジタル署名に付与されたタイムスタンプの時刻に基づき、デジタル署名の検証に必要な信頼点までの証明書パス情報や失効情報(CRL,ARL など)を収集する。

（ウ） 対象

以下にあげたものを収集する

- **署名者の公開鍵証明書**
- **署名者の公開鍵証明書に対する CRL など**
- **Root-CA に至るまでの CA 公開鍵証明書**
- **Root-CA に至るまでの CA 公開鍵証明書に対する CRL や ARL など**

（エ） タイミング

長期経過後に署名の有効性を確認する場合は、これらの情報を使って有効性を確認するため、①の時点で署名の検証が正しく終了できるような情報を収集する必要がある。したがって、以下の要件が満たされている期間内に収集する必要がある。

- **デジタル署名の存在時刻確定のために付与されたタイムスタンプ有効期間内**
- **デジタル署名が有効である間**

ただし、署名者の公開鍵証明書の CRL に署名者証明書が失効した事実が反映されるには、CRL の発行周期に従ったタイムラグが生じる。そのため、厳密には上記の要件に加えて、存在時刻確定のタイムスタンプを付与した後で発行された CRL を収集するという要件も加えることが望ましい。

（3）デジタル署名、署名対象文書、②で収集した署名の有効性確認に必要な証明書や失効情報、および存在時刻確定のために付与されたタイムスタンプ（①）を長期的に改ざん検知可能な状態で保存する。

（オ）対象

保管対象は具体的には次のようになる。

- **デジタル署名**
- **署名対象文書**
- **デジタル署名の検証に必要な信頼点までの証明書パス情報や失効情報(証拠情報)**

  - 署名者の公開鍵証明書
  - 署名者の公開鍵証明書に対する CRL など
  - Root-CA に至るまでの CA の公開鍵証明書
  - Root-CA に至るまでの CA の公開鍵証明書に対する CRL（ARL）など
  - Root-CA に至るまでの CA に対する CP/CPS
- タイムスタンプ
- タイムスタンプの有効性を延長するための情報（タイムスタンプの方式によって異なる）

（カ）タイミング

以下の要件が満たされている間に適切に保管する必要がある。

- デジタル署名の存在時刻確定のために付与されたタイムスタンプ有効期間内
- デジタル署名の検証に必要な信頼点までの証明書パス情報や失効情報が有効である間

（キ）保管方法

また、これらの情報の保管に関しては、必ずしも特定のフォーマットに従う必要はなく、必要な情報が適切に保管されていればよい。具体的な保管方法としては、本稿で説明している以下のような方式が考えられる。

- PKI 方式タイムスタンプを用いた長期保管
- リンク方式タイムスタンプを用いた長期保管

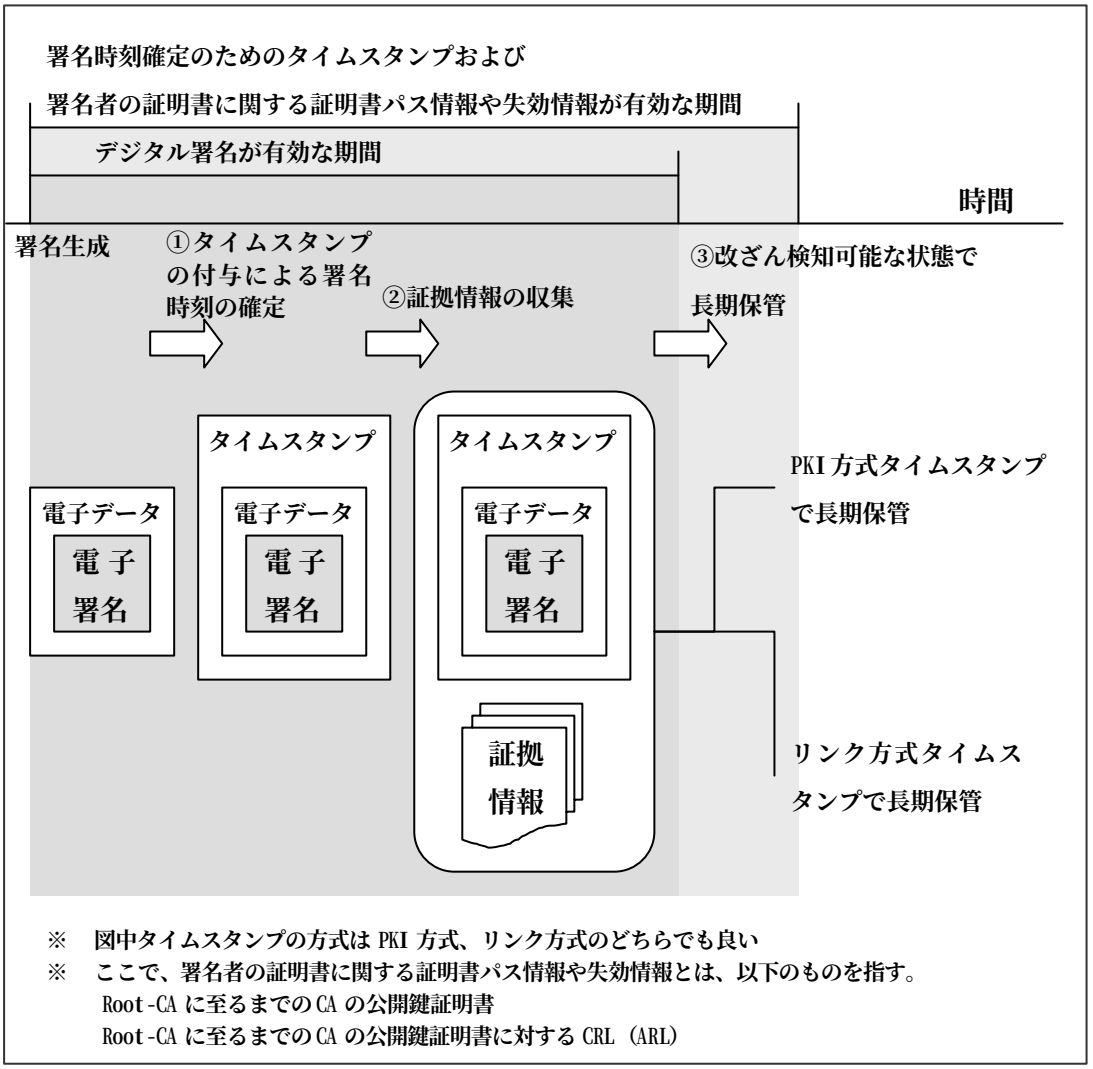


図４．３　長期経過後のデジタル署名存在時刻の確認とデジタル署名の本人性の確認の方法

以上をもとに、デジタル署名付文書が過去の特定の時点で有効であったことを長期経過後確認する手順は以下のようになる。

1. **４．２．１の①で示される信頼できる署名時刻を確認する。**
2. **４．２．１の③で示されるデジタル署名の有効性を長期経過後に確認するための情報が、最初に保管されてから現在に至るまで改ざんされていないことを確認する（確認方法は保管方式に依存する）。**
3. **１．で確認した時刻においては署名が有効であったことを非改ざん性が確認された証拠情報を用いて確認する。信頼点の正当性は公知化されたFingerprint値と認証局の自己署名証明書のFingerprint値と比較する。**

４．２．２　デジタル署名付文書の非改ざん性の長期的な維持の方法

表4．1に示したように、デジタル署名が有効であるための要件にはいくつか存在する。その中の一つに「デジタル署名付文書の非改ざん性」があるが、それを長期的に維持することを考えた場合に考慮すべき事項がある。ここで、デジタル署名の存在時刻の確定のために付与するタイムスタンプの付与対象により対応が異なるので、それぞれについて説明する。なお、タイムスタンプについては「e-文書法におけるタイムスタンプ適用ガイドライン」（平成 17 年 1 月）[3]に示されるように、以下の二通りの場合が考えられる。

①　デジタル署名にタイムスタンプを付与する場合
②　デジタル署名と署名対象文書の両方を含んでタイムスタンプを付与する場合

①の「デジタル署名にタイムスタンプを付与する場合」では、デジタル署名の存在時刻と非改ざん性はタイムスタンプにより直接確認し、署名対象文書の存在時刻と非改ざん性は付与されたデジタル署名により間接的に確認する。ここで、デジタル署名と署名対象文書との関係は、PKI 方式タイムスタンプと同様に署名対象文書のハッシュ値によって一意に対応づけられる。したがって、デジタル署名付き文書の非改ざん性を長期経過後も確認可能とするためには、ハッシュ関数の脆弱化にも対応できるように署名対象文書とデジタル署名の対応関係も長期的維持する必要がある。そのためには、署名対象文書とデジタル署名の両方を改ざん検出可能な状態で長期間保管すれば良い。

一方、②の「デジタル署名と署名対象文書の両方を含んでタイムスタンプを付与する場合」では、タイムスタンプにより直接デジタル署名と署名対象文書の存在時刻と非改ざん性を直接確認可能である。したがって、この場合デジタル署名付き文書の非改ざん性を長期的に維持するためには、本ガイドラインで述べる方法でタイムスタンプの有効性を延長すれば良い。

４．２．３　長期経過後に信頼点の正当性を確認について

デジタル署名や公開鍵証明書の正当性を長期経過後も確認するためには、その信頼点まで認証パスの構築が長期経過後も確認できる必要があるが、それに加えて信頼点自体の正当性も長期経過後に確認できる必要がある。長期経過後にも信頼点の正当性を確認するためには、認証局が、自己署名証明書が有効な間にそのフィンガープリントを公知のものとするなどの対策が考えられる。

[3] http://www.scat.or.jp/time/PDF/tekiyouguidelineVer1.0.pdf

４．２．４　長期保存フォーマット

デジタル署名付文書の署名の有効性を長期的に維持するための文書フォーマットとして署名フォーマット技術が規定されている。署名フォーマットは「ETSI TS 101 733 V1.5.1：Electronic Signature Formats」において規定されており、RFC3126 にもなっている。また、XML 署名に対応した署名の長期保存フォーマットとして、「ETSI TS 101 903 V1.2.2：XML Advanced Electronic Signatures(XAdES)」が規定されている（XAdES は、W3C では note として公開されている）。図４．４に長期保存フォーマットの例を示す。

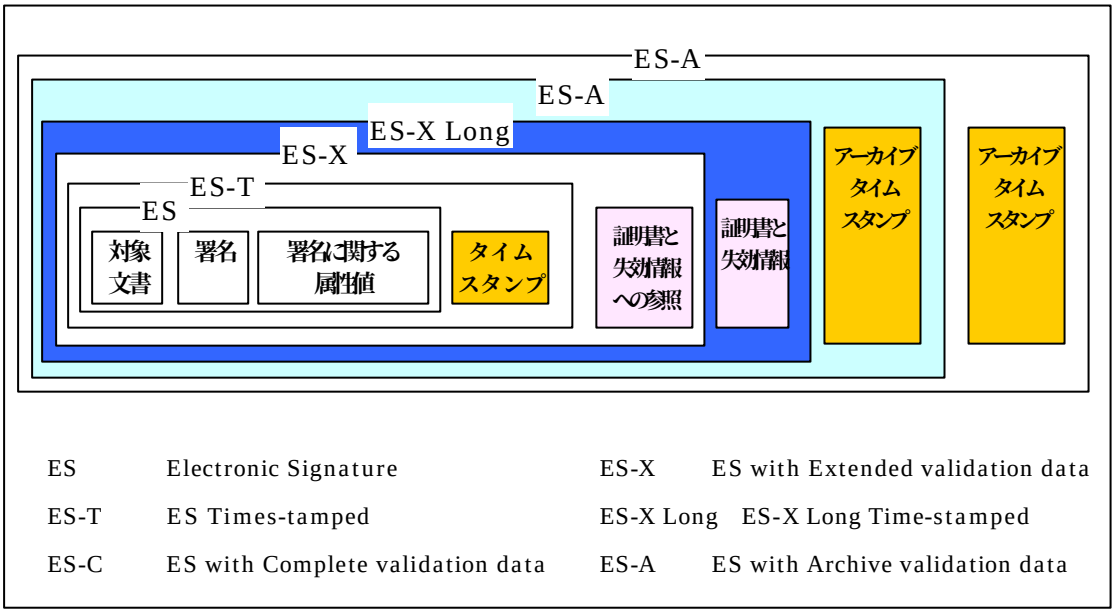


図４．４　デジタル署名の長期保存フォーマットの例

長期保存フォーマットの利用はデジタル署名の長期保存するための必須要件ではないが、以下のような利点がある。

- 署名および署名対象文書の保管方式について客観性が高い説明が可能となる。
- 署名者と長期経過後の署名の有効性の確認を行う者の間の相互運用性が高まる。

現在、数多くのデジタル署名付文書が何らかの署名フォーマットに従い作成されている。しかし、これらの署名フォーマットは長期経過後の署名の有効性の確認を想定した構成となっていないことが多く、簡単に長期保存フォーマットへ移行できない可能性がある。したがって、長期保存を考慮していない既存のデジタル署名付文書を長期保存フォーマットの形式で今後長期的に保管するためには、長期保存フォーマットを構成する際に注意と工夫が必要である。

５．環境等の用件

５．１　CA の要件

本節では、PKI 方式タイムスタンプの長期保証を検討する上で、TSA 証明書を発行する CA に関する要件を定める。PKI 方式タイムスタンプでは、長期保証において対象とする期間を以下の 3 つのフェーズに分けて考えることができる。

(1) TSA 証明書の有効期間中
(2) TSA 証明書の有効期間満了後～
(3) CA 証明書の有効期間満了後～

(1)は、長期保証に関わらず一般的にタイムスタンプが利用される状況、つまり TSA がタイムスタンプを付与可能な期間である。(2)は、TSA 証明書の有効期間が満了し、ただし TSA 証明書を発行した CA 証明書の有効期間内の任意の時点を指すものとする。(3)は、(2)よりも未来で、CA 証明書の有効期間も満了した後の任意の時点を指すものとする。

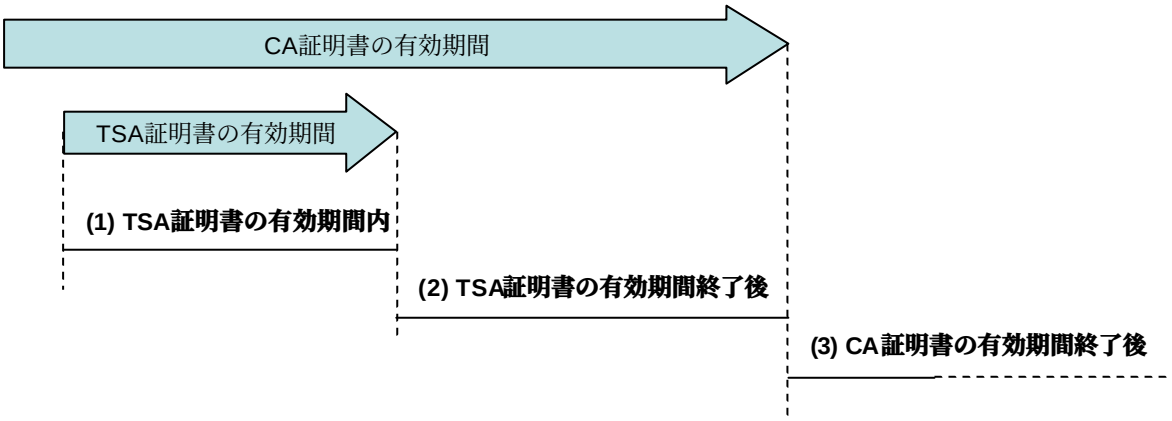


図５．１　長期保証で考慮すべき 3 つの期間

ここでは有効期間の満了に限らず、CA 事業者が CA 証明書の有効期間内に事業を終了する場合も含めて検討するものとする。
実際にタイムスタンプが有効であることを検証できるのは(1)の期間のみであるが、長期保証を考える上では、(2)や(3)の任意の時点において、(1)の期間にタイムスタンプが有効であったことを示せなければならない。
本節では、(1)の期間にタイムスタンプが有効であったことを、(2)や(3)の任意の時点におい

て利用者が示すことができるようにするために、CA に求める要件を定義する。

なお、ここではタイムスタンプを新たに付与する場合については考慮しない。タイムスタンプを新たに付与することによってタイムスタンプトークンが入れ子になっているような場合であっても、着目するタイムスタンプトークンを発行した TSA 証明書と、その CA 証明書についてのみ捉えて考えるものとし、入れ子となっている他のタイムスタンプトークンとの関連については考慮しない。
例えば図５．2 で、タイムスタンプトークン(1)の有効性について着目するならば、TSA 証明書(1)とその発行元となる CA 証明書について、タイムスタンプトークン(2)の有効性について着目するならば TSA 証明書(2)とその発行元となる CA 証明書について考慮すればよい。

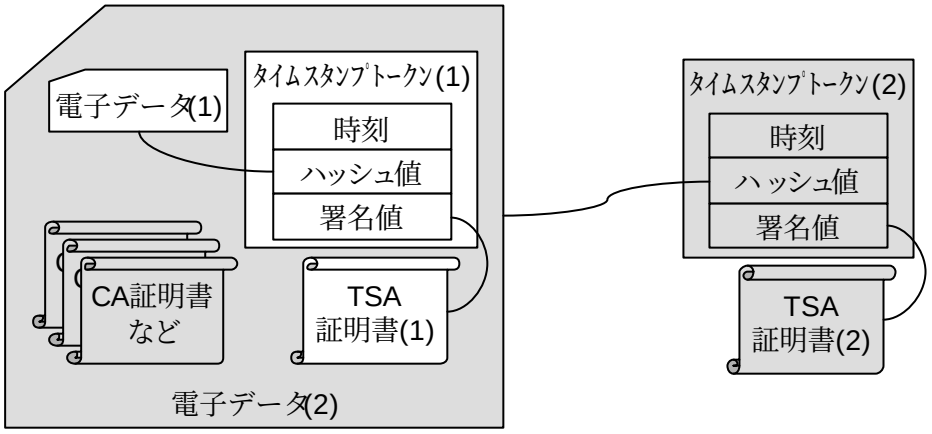


図５．２　タイムスタンプが入れ子になっている場合

５．１．１　TSA 証明書の有効期間中の有効性保証

TSA 証明書の有効期間中においてタイムスタンプの有効性を示せることは、長期保証に関わらず PKI 方式タイムスタンプの一般的な要件である。PKI 方式タイムスタンプにおいて、TSA 証明書を発行する CA に求められる要件は、「信頼されるタイムスタンプ技術・運用基準ガイドライン」[4](以下、[ガイドライン]と表記)の 2.4 節において定められている。
また長期保証を実現するためには、利用者はこれらの要件に加えて、付与されたタイムスタンプが付与された時点で有効であることを確認しておくべきである。

[ガイドライン]も含め、以上の点から各パーティに求められる要件は以下のように考えることができる。

- CA は、下記[ガイドライン]要件を満たさなければならない。また、下記[ガイドライン]

[4] http://www.scat.or.jp/time/PDF/unyoukijunVer1.0.pdf

要件を満たしていることが、CP/CPS 等公開情報によって第三者に対して明確にされていなければならない。

- CA は、自身の CA 証明書を検証者の必要に応じて提供できなければならない。
- TSA は、下記[ガイドライン]要件を満たす CA から TSA 証明書の発行を受けなければならない。
- 利用者は、下記[ガイドライン]要件を満たす CA から証明書を発行された TSA から、タイムスタンプの付与を受けなければならない。また付与されたタイムスタンプが有効であることを検証しておくべきである。
- 検証者は、TSA 証明書の発行元である CA が下記[ガイドライン]要件を満たしていることを CP/CPS 等公開情報によって確認しなければならない。

なお参考までに、[ガイドライン]が定める主な要件を以下に挙げておく。詳細については[ガイドライン]を参照されたい。

- CA の責任
  - CA は、TSA の管理する秘密鍵が、発行する TSA 証明書の公開鍵に対応したものであることを確認すること。
  - CA は、時刻認証事業者の存在を確認し、発行する TSA 証明書の主体者名との関係を証明すること。
- CA 証明書が失効した場合の対処
  - TSA 証明書の有効期間内に CA 証明書が秘密鍵の危殆化などの理由で失効した場合は、CA は直ちに失効処理を行い、TSA に通知を行なうこと。
  - この際に発生したトラブルに関しては CA が責務を負うこと。
- TSA 鍵の更新
  - 時刻認証事業者に対して、TSA 証明書の有効期間よりも短い範囲で TSA 秘密鍵の活性化期間を定め、活性化期間終了後は当該秘密鍵を廃棄するよう確認すること。
  - CA は、鍵の更新に際して、TSA の存在と、証明書の使用目的を確認できること。
  - CA は、証明書の更新を行うに際して、既存の TSA 秘密鍵の破棄を確認できること。
- TSA 証明書の失効
  - TSA 証明書の CRL を定期的に発行し、危殆化時の影響を最小化している CA であること。
  - TSA 証明書が失効した時などの緊急時には、速やかに新しい CRL を発行できること。
    - ✧ TSA として定められた基準を満たさなくなったとき、および TSA が閉局する場合は、証明書を失効させられること。
    - ✧ CA は TSA 証明書の失効に理由コードを記載していること。

- リポジトリの公開
  - 検証情報の公開: 常に安全に参照できるリポジトリに、発行した全ての TSA 証明書について、信頼の起点となるルート認証局から当該 TSA 証明書までの証明書チェーンの検証に必要となる一連の証明書情報や失効情報、あるいはその取得方法について利用者に公開すること。また、これらの情報や取得方法に変更があった場合には速やかにリポジトリへ反映させること。
  - 過去の検証情報: 前項に記した情報または取得方法については、発行した全ての TSA 証明書の有効期間終了後も相当期間以上長期にわたって検証できるよう、利用者に対して公開すること。
  - CP、CPS、TSA の審査記録、TSA 証明書の発行記録を TSA 証明書の失効情報を TSA 証明書の有効期限後または相当期間以上長期にわたって、安全に保管し、開示できるようにしていること。
- CA 業務の終了
  - CA が TSA に対する認証業務を終了する場合、利用者がタイムスタンプを検証するために必要な、5 項に定めた情報またはその取得方法を、TSA 証明書の有効期限後または相当期間以上長期にわたって参照できるよう、他の信頼できる機関に引き継げるように定めていること。

５．１．２　TSA 証明書の有効期間満了後の有効性保証

TSA 証明書が有効でなくなった後にタイムスタンプの有効性を示すためには、「タイムスタンプを付与した時点あるいは過去に検証した時点において当該 TSA 証明書が有効であったこと」を示せなければならない。

このためには前項５．１．１の要件に加えて、検証者は以下について確認する必要がある。

- タイムスタンプ付与時点が当該 TSA 証明書の有効期間内であること
- タイムスタンプ付与あるいは付与後の検証時点において当該 TSA 証明書が失効されていなかったこと
- 当該 TSA 証明書が、その有効期間に関する項目を除いて CA 証明書によって検証できること

これらの確認を行うために、検証者は以下の情報を入手する必要がある。

- 当該 TSA 証明書
- タイムスタンプ付与あるいは付与後の検証時から当該 TSA 証明書の有効期間満了までの間に発行されたいずれかの失効リスト
- 当該 TSA 証明書を発行した CA の証明書

一方 CA は、検証者の必要に応じて以下を提供できなければならない。

- 当該 TSA 証明書を発行した CA の証明書
- [ガイドライン]要件を満たしていることを第三者に対して明確に示している CP/CPS 等の公開情報

５．１．３　CA 証明書の有効期間満了後の有効性保証

CA 証明書が有効でなくなった後にタイムスタンプの有効性を示すためには、タイムスタンプを付与した時点で当該 TSA 証明書だけでなく CA 証明書も有効であったことを示せなければならない。加えて、タイムスタンプ付与時の信頼点である CA 証明書の正当性についても示せなければならない。

このためには、検証者は前項５．１．２の要件に加えて以下について確認する必要がある。

- タイムスタンプ付与時が当該CA証明書の有効期間内(かつ当該TSA証明書の有効期間内)であること
- タイムスタンプ付与時に当該 CA が５．１．１に示す CA 要件を満たしていたこと

これらの確認を行うために、検証者は以下の情報を入手する必要がある。

- 当該 CA 証明書
- タイムスタンプ付与時に当該 CA が５．１．１に示す CA 要件を満たしていたことを示す CP/CPS 等の(タイムスタンプ付与時における)公開情報およびタイムスタンプ付与時に当該情報が公開されていた事実

このうち、2 点目の「公開されていた事実」は長期保証における CA 要件として最も重要な項目であるため、次項において詳しく解説する。

一方 CA は、そのサービスを継続している間は検証者の必要に応じて以下を提供できなければならない。

- 当該 TSA 証明書を発行した CA の証明書(あるいはその発行履歴)
- タイムスタンプ付与時に当該 CA が５．１．１に示す CA 要件を満たしていたことを示す CP/CPS 等の(タイムスタンプ付与時における)公開情報

なお、CA がサービスを中止あるいは終了した場合、これらの情報が CA から提供されることは難しいかも知れない。CA はサービス終了後も一定期間これらの情報を提供できることが望ましいが、あらかじめ前述のように公知化しておくなど利用者に対する配慮がなされるべきである。

５．１．４　信頼点の公知化

前節で検証者が入手すべき情報として 2 点目に挙げている「公開されていた事実」とは、タイムスタンプ付与時における公開情報そのものと、それがタイムスタンプ付与時から改ざんされていないものであることを示す情報によって成立すると考えられる。例えば、一連の公開情報についてのハッシュ値を算出しタイムスタンプ付与時点以前に新聞等に公告されていることで、検証者はタイムスタンプ付与時点において当該 CA が要件を満たしていたことを確認できる。具体的には、以下のような要件を満たすことで実現されると考えられる。

1. タイムスタンプ付与以前に、CA 要件を満たすことを示す CP/CPS 等の情報(以下公開情報)が CA によって公開されていること。
2. 公開情報のハッシュ値を新聞等に公告し、公開情報が公告時点で改ざんされてないものであることを公知化する。
3. 公知化する時期はタイムスタンプ付与以前が好ましいが、タイムスタンプ付与以前に公知化されていない場合には、タイムスタンプ付与後速やかに公知化されるべきである。
4. 公告対象については以下の要件が求められる。
   - 公告されたハッシュと公開情報が一致することを確認したいと考える(利用者を含む)第三者が公告後速やかに入手できるもの(例えば新聞全国紙など)である必要がある。
   - 刊行後長期に渡って見読性を確保(例えば国会図書館等に改変されずに収蔵)できる必要がある。
   - 刊行日が公知(例えばほぼ毎日刊行されることが自明である新聞など)であるなど、公知化した時点を特定できる必要がある。
5. 公告されたハッシュ値と公開情報が一致しない場合、CA は公開情報の信頼性が欠けていることについての責を負うべきである。
6. 公告対象は刊行後、第三者によって長期見読可能な形で改ざんできないよう保管される。例えば国会図書館のような公的機関がマイクロフィルムで保管する刊行物に公告されていると、将来第三者から公知の推定効が働きやすいと考えられる。
7. 将来において、CA の信頼性について確認する必要が生じた場合は、見読可能な媒体を確認することで、公知化した時点を特定し、タイムスタンプ付与時点で信頼点の信頼性が確立されていたことを確認できる。

これらの要件を最も容易に実現する例としては、CA が公開情報のハッシュ値を新聞の全国紙に公告するという方法が考えられる。全国紙であれば、第三者が速やかに公告対象を容易に入手でき、公開情報との不一致を確認することができる。また、国立国会図書館法

に基づく納本制度により、ほとんどの全国紙は国会図書館よる長期見読性や収蔵時の非改ざん性を容易に確保できる。

将来の検証者は、国会図書館から当時の新聞のマイクロフィルムを確認することで、TSA 証明書発行元である CA が確かに当時の公開情報に基づいた運用を行っていたことを信頼することができると考えられる。

このような公知化の手法は、将来に渡って信頼性を確保したい CA に限らず、利用者に長期保証を提供する TSA などにも実施可能な手法であるが、基本的には信頼性を確保する主体である CA が自ら実施するべきだと考えられる。このように「公開されていた事実」は公知とすることによって成立すると考えられるが、CA を信頼する判断はあくまで検証者に委ねられるため、利用者はできる限り将来においても信頼性が高いであろう認証局から発行された TSA 証明書を持つ TSA を利用すべきである。

５．１．５　まとめ

CA 証明書の有効期間満了後まで含めて有効性を保証する必要がある場合、検証者、利用者、TSA、CA はそれぞれ以下の要件を満たさなければならない。

- 検証者要件:
  - TSA 証明書の発行元である CA が[ガイドライン] の CA 要件を満たしていることを CP/CPS 等公開情報によって確認しなければならない。
  - タイムスタンプ付与あるいは付与後の検証時点(TSA 証明書の有効期間内)において当該 TSA 証明書が失効されていなかったことを確認しなければならない。
  - 当該 TSA 証明書が、その有効期間に関する項目を除いて CA 証明書によって検証できることを確認しなければならない。
  - タイムスタンプ付与時が当該 CA 証明書の有効期間内かつ当該 TSA 証明書の有効期間内であることを確認しなければならない。
  - タイムスタンプ付与時に当該 CA が[ガイドライン]の CA 要件を満たしていたことを確認しなければならない。

- 検証者が必要とする情報:
  - 当該 TSA 証明書
  - タイムスタンプ付与あるいは過去の検証時から当該 TSA 証明書の有効期間満了までの間に発行されたいずれかの失効リスト
  - 当該 TSA 証明書を発行した CA の証明書
  - タイムスタンプ付与時に当該 CA が[ガイドライン]の CA 要件を満たしていたこと

を示す CP/CPS 等の(タイムスタンプ付与時における)公開情報

- CA 要件:
  - CA は、[ガイドライン]の CA 要件を満たさなければならない。また、[ガイドライン]の CA 要件を満たしていることが、CP/CPS 等公開情報によって第三者に対して明確にされていなければならない。
  - サービスを継続している間は、必要に応じて以下の情報を検証者に提供できなければならない。
    - ✧ 当該 TSA 証明書(あるいはその発行履歴)
    - ✧ タイムスタンプ付与時から当該 TSA 証明書の有効期間満了までの間に発行されたいずれかの失効リスト(あるいはその発行履歴)
    - ✧ 当該 TSA 証明書を発行した CA の証明書

Ver.1.3
タイムビジネス推進協議会

● 参　考

参考１

1．セキュア保管型タイムスタンプ長期保証

本文においてタイムスタンプの長期保証について、その要件、および実現方法を記述してきた。実現方法は一言で表現すると、タイムスタンプが有効である時点において、再度、タイムスタンプを付与し、そのことによって二つ目のタイムスタンプが持つ有効期間分の保証を確保する、ということである。

本参考においては、本文で述べた方式の一部を用いて異なる運用方式を構成する方法を紹介する。ここで紹介する方法は、技術的に完結するという厳密な意味において、本文で述べた方法に比較して不足する部分があり、その不足部分を、運用の規定化、監査の実施等によって補う必要がある。本参考には、それらの運用に関わる部分を詳述している。

１．１　セキュア保管型による方式概要

セキュア保管型タイムスタンプ長期保証方式においては、保管対象データとして、

（１）タイムスタンプ付与対象の電子データ
（２）タイムスタンプ
（３）タイムスタンプ検証に使用した情報

を、一括して厳密な運用の下に管理して保管する。それ以降は、そのような運用の下で保管されている状態で長期間の保存を行う。時間経過後、読み出しが必要になった際には、所定の手続きによって読み出しを行う。つまり、一括して厳密な運用の下に管理して保管されていたこと、言い換えるとセキュアに保管されていたことを証明することにより、保存されていた情報の真正性を確認し、それによって、本文２．２で示されたタイムスタンプ長期保証の５種の要件を充足し、タイムスタンプの有効性を長期にわたって保証する。本方式は、タイムスタンプ方式に係らず適用可能である。ただし、保管対象データの構成要素である「タイムスタンプ検証に使用した情報」は、タイムスタンプ方式に依存した内容となる。PKI 方式タイムスタンプとリンク方式タイムスタンプにおける具体例を以下に記す。

表１．１　タイムスタンプ検証に使用した情報例

方式	タイムスタンプ検証に使用した情報の例
PKI 方式 タイムスタンプ	・ タイムスタンプ検証に係る情報 例えば、認証パス情報、CRL/ARL） ・ TSA 運用や CA 運用を示す情報 例えば、TP/TPS、CP/CPS） ・ 検証方法に係る情報 例えば、タイムスタンプに含まれるアルゴリズム識別子など）

リンク方式 タイムスタンプ	・ タイムスタンプ検証で使用したリンク情報及び照合データに係る情報（例えば、リンク情報と照合データそのもの） ・ 検証対象のタイムスタンプに係る明証化されたリンク情報の代表値に係る情報（例えば、明証化されたリンク情報の代表値、明証化時期、及び明証化された場所の情報） ・ TSA 運用を示す情報（例えば、TP/TPS） ・ 検証方法に係る情報

冒頭で述べた通り、技術的に完結するという厳密な意味において不足する部分が存在するため、技術的要素だけでなく、管理ポリシー・管理ルールの策定などの運用的要素について十分注意を払う必要がある。また、適切に運用していたことを立証する方法も明確にしておく必要がある。そのため、本記述内容だけでなく、文書や記録の管理に関する標準的な規格も参照することが必要になると思われる。例えば、該当する規格としては、以下のようなものがある。

表１．２　標準的な規格例

規格	内容
ISO 15489-1:2001 Information and documentation – Records management – Part 1: General	記録管理の基本原則を記述。この原則は、適切な記録作成、記録のキャプチャ、記録の管理を保証する。
ISO/TR 15489-2:2001 Information and documentation – Records management – Part 2: Guidelines	ISO15489-1 で述べられた基本原則に準拠した記録管理の手続きを記述。
ISO/TR 15801:2004 Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability	ビジネス情報をイメージデータとして電子保存するときの推奨実践方法を示す。コンピュータシステム内で作成されたイメージデータやコンピュータシステム内に存在するイメージデータの内容が、システム内で作成、または、システム内に取り込まれて以降、改ざんされていないことを示すことができる方法を記述。

１．２　セキュア保管型実現のための共通要件

１．２．１　前提

セキュア保管型で保管の対象とするデータは１．１．で述べた三種類とし、これら情報の真正性は確認済みとする。
セキュア保管型に登録するタイミングは、本文４．２．１で示された図４．３の③改ざん検知可能な状態で長期保管、とされる時点とする。

１．２．２　共通要件

（１）登録時刻の保証
タイムスタンプの有効性が失われる前にそのデータが保管されていたことを証明できること。

（２）非改ざん性の保証
保管対象データが保管されている間、改ざんされていないことを証明できること。

（３）保存性の保証
後日、保管対象データを読み出すことができるように、保管対象データの損失、破壊、読出しが不可能な状態にならないようにすること。

（４）保管対象データと取り出しデータの同一性の保証
取り出されたデータが、指定された保管対象データと同一であり、差し替えなどがなされていないことを証明できること。

１．３　セキュア保管型実現方式概要および留意点

セキュア保管型を実現するために考えられる４種類の方式について、それぞれの実現方法の概要、およびそれぞれに特有の留意点を述べる。

１．３．１　可搬媒体方式

記録情報を、追記型記録機能（W.O.R.M.機能）を持つ媒体に記録する運用方式を規定する。媒体に、１．２．１で示した保管対象データを書き込み、１．２．２．の共通要件を満たすよう運用する。

１．３．１．１．可搬媒体方式における留意点

（１）登録時刻の保証

いかなる場合でも媒体全体の情報を別の媒体に書き写すことは可能である。従って、運用によっては、媒体に書き込まれた時刻の保証が困難になる可能性がある。

これを回避する方策として、媒体個々にユニークかつ書き換え困難な番号（媒体 ID）を付与して個々の媒体を識別することを可能にし、かつ、個々の媒体に収納された保管対象データと収納時刻を記録する管理台帳を作成し運用することが考えられる。媒体 ID は、同じ番号が存在せず、一度書き込まれたものは書き換えが非常に困難であり、かつ管理ソフトウェアによって読み出しが可能であること、これらが保証されることが望ましい。

この管理台帳の運用によって、媒体全体の情報を別の媒体に書き写したとしても、元の収納との弁別は可能となり、従って最初の登録時刻の確認が可能である。

管理台帳の仕様については、「行政文書の管理方策に関するガイドライン（平成 12 年 2 月 25 日）(*)」などに準じたものとすることが望ましいと考えられる。

(*) http://www.soumu.go.jp/gyoukan/kanri/gaido.htm

この方式の信頼性を高めるために、媒体 ID の書き換え困難性は技術的に考察されるべきであり、媒体 ID をユニークに付与する運用方法、管理台帳の運用方法などについては運用規定を定め、定期的に監査を受けることなどが考えられる。

（２）媒体の期待寿命、装置寿命

W.O.R.M.機能を持つ媒体として種々の製品が存在するが、それらの期待寿命と、文書の保存期間との関係に留意が必要である。つまり、一般的な W.O.R.M.機能を持つ媒体の期待寿命は１０年～５０年程度であるが、その寿命より、文書の保存期間が長い場合には、媒体から媒体への移し替えが必要になるため、その移し替え運用を明確化しておく必要がある。また、実際の媒体の寿命は、媒体の保存状態によって期待寿命より短くなる可能性があるため、媒体の保存環境にも留意が必要である。

媒体を取り扱う装置(装置を動かすソフトウェアを含む)において、製品としての寿命、製品サポート期間は有限であると考えられる。従って、製品としての寿命、製品サポート期間が、文書の保存期間より短い場合、媒体および装置の移し替えを含む対策を明確化しておく必要がある。

１．３．２　自主運営ストレージ方式

記録情報の管理責任者自らが管理する記録装置において、記録情報を記録する運用方式を規定する。記録装置内で用いる記録媒体種別（W.O.R.M.，Rewritable など）について、運用方式に差がある場合は、個々の運用方式を規定する。

１．３．２．１　自主運営ストレージ方式における留意点

（１）運営者の監査

運営者自身が正当でない行為を成さない、成していないことの証明をする必要がある。そのための方策として、運営について、監査を受けることが有効である。

（２）使用装置の信頼性

運営者が使用する装置としての信頼性の担保が必要である。その担保のため、第三者による信頼性の確認が可能な方法、例えば標準規格（一例としてＦＩＰＳ１４０－１または２、レベル３相当）に準拠した装置を使用するなど、が考えられる。

また、使用する装置の仕様として、ECOM のガイドライン(例：電子署名文書長期保存に関する中間報告、平成 13 年 3 月)等で示される原本性保証システムを参考にすることも有効である。

（３）情報の管理

保管期間中、継続して以下の情報の管理を行う。

１）収納時刻：１．２．１　で述べた保管対象データを、装置に収納した時刻
２）アクセスログを取得し、その情報を改ざん検知可能な状態で記録
３）監査を実行し、その情報を改ざん検知可能な状態で記録

（４）読み出し時管理

読み出し時の処理フローを明確にする。１．２．１で述べた保管対象データについて、上記(3)で述べた情報を組み合わせた形で読み出しに対応する。読み出しを受けた側において、読み出し時の処理フロー、保管対象データ、保管期間中の管理情報を合わせて解釈することを可能とすることが重要である。

１．３．３　アウトソーシングストレージ方式

記録情報の管理責任者が､自己でない他社が管理する記録装置において記録情報の記録を委託する場合において、委託を受けた側での記録運用方式を規定する。記録装置内で用いる記録媒体種別（W.O.R.M.，Rewritable など）について、運用方式に差がある場合は、個々の運用方式を規定する。

１．３．３．１　アウトソーシングストレージ方式における留意点：運用方式信頼性

運用を委託しようとする者に対して、自主運営ストレージ方式において述べた留意点(運営者の監査、使用装置の信頼性、情報の管理、読み出し時管理)を含む運用方式を公開することによって公平性、公証性を確保する。第三者による信頼性の確認が可能な方法、例えば標準規格（一例として、情報セキュリティマネジメントシステム(ISMS)）の認証を取得する、また、運用あるいは運営について定期的に監査を受けること、などが考えられる。

１．３．４　長期使用を前提とした電子署名方式

長期使用を前提とした電子署名方式を使用したデータ管理システムを用いて保管対象データを管理する方式を規定する。ここでは、電子署名方式の具体例として、ヒステリシス署名を例にあげる。

１．３．４．１　ヒステリシス署名技術概要

ヒステリシス署名技術は、署名間に連鎖構造を持たせ、署名の安全性、有効性を長期間維持する機能を提供する。これにより、ヒステリシス署名対象の電子データの完全性（非改ざん性）を長期にわたって保証することが出来る。この技術内容に関しては、ECOM のガイドライン（例：電子署名文書長期保存に関するガイドライン、平成 14 年 3 月）や日本銀行金融研究所の IMES Discussion Paper(例：No. 2003-J-4「デジタル署名の長期的な利用とその安全性について」)に記載があるため、これらの文献を参照されたい。

１．３．４．２　共通要件に対する実現方法

（1）非改ざん性の保証

ヒステリシス署名を利用したセキュア保管方式では、電子データ、タイムスタンプデータ、検証に使用した情報から構成される保管対象データに対してヒステリシス署名を作成する。ヒステリシス署名は、ヒステリシス署名の付与対象となる保管対象データの完全性（非改ざん性）を保証する。

次図は、保管対象データを格納するデータ管理システム内で実行されるヒステリシス署名作成手順の一例である。ヒステリシス署名#k(k=1～n)は、受け取った保管対象データ#k と直前に生成されたヒステリシス署名#k-1(k=0 は、ダミー値でよい)を署名対象データとして生成される。作成されるヒステリシス署名全ては、署名履歴として保管される。また、定期的に署名履歴の情報（例えば、その時の最新のヒステリシス

署名のハッシュ値）を新聞などで公知化することにより、署名履歴のトラストアンカを生成する。これにより、データ管理システムの管理者による署名履歴に対する改ざん不正を抑止するとともに、署名履歴の信頼性を向上させる。

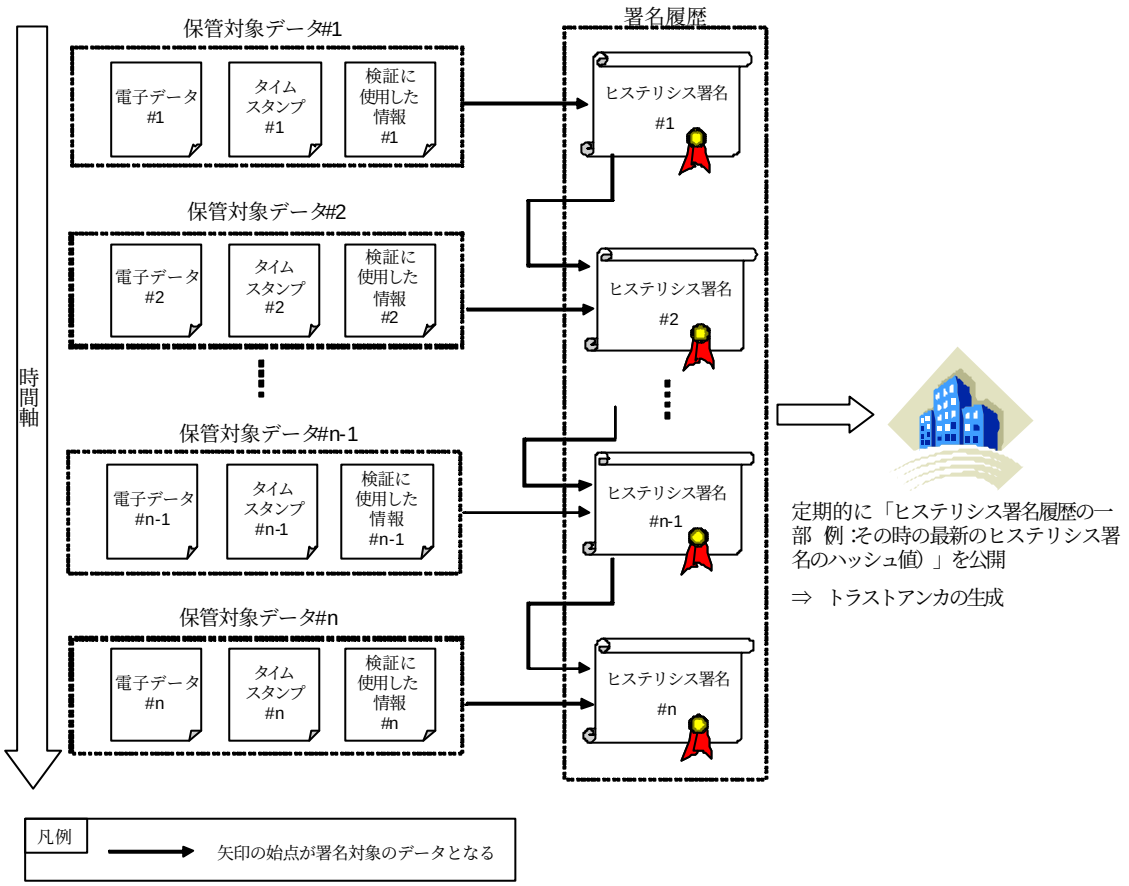


図１．１　保管対象データに対するヒステリシス署名作成手順例

（２）登録時刻の保証

保管対象データの登録時の証明に関しては、署名履歴の公知化日時を拠り所にして、それよりも以前に存在していたことを証明することで可能である。また、定期的に、ヒステリシス署名データ作成時にタイムスタンプ事業者から取得したタイムスタンプも署名対象として含めることにより、ヒステリシス署名作成時刻（＝保管対象データ登録時刻）を保証し、定期的な公知化日時の代用とすることも可能である。

（３）保存性の保証

保管対象データの保存性を保証するためには、保管対象データやヒステリシス署名データを格納するストレージ・メディアの信頼性や寿命などの情報を踏まえて、システムマイグレーションを行う必要があると思われる。

（４）保管対象データと取り出しデータの同一性の保証

保管対象データと取り出しデータの同一性に関しては、データ管理システムのデータ取り出し処理フロー仕様により確認することが可能である。

１．３．４．３　ヒステリシス署名技術方式における留意点

（１）秘密鍵の管理

ヒステリシス署名に使用する秘密鍵を安全に管理する必要がある。例えば、秘密鍵の漏洩を防ぐことを目的として、管理規定を定め、秘密鍵の管理を行う。また、定期的に監査を行うことが考えられる。

（２）署名履歴の管理

ヒステリシス署名の署名履歴の正当性を示す必要がある。例えば、署名履歴に対する不正アクセス・改ざんを防ぐことを目的として、管理規定を定め、署名履歴の管理を行う。また、定期的に監査を行うことが考えられる。

（３）暗号技術

ヒステリシス署名で使用する暗号技術(公開鍵暗号アルゴリズムやハッシュ関数)は、安全性が確認されたものを使用することが必要である。例えば、総務省と経済産業省が公表している電子政府推奨暗号リスト（平成 15 年 2 月 20 日）に掲載された暗号技術を使用することが考えられる。また、使用するハッシュ関数の脆弱化対策も明確に規定することが必要である。

参考２

２．DS-IMT 長期保証技術

本章では、開発・実験を進めているタイムスタンプの長期保証技術である DS-IMT 方式について述べる。DS-IMT 方式は、タイムスタンプに対して新たなタイムスタンプを付与することなしに、最初に付与したタイムスタンプの有効性を長期間にわたり保証できる新たな仕組みとして検討しているものである。

DS-IMT 方式の適用型

簡易型: タイムスタンプ対象データなしに、タイムスタンプトークンやその検証用データのみを保護する。

一般型：タイムスタンプ対象データ、タイムスタンプトークン、その検証用データを一緒にアーカイブし、それに付与したアーカイブタイムスタンプを保護する。

簡易型は、長期保証の有効期間が、使用されているハッシュ関数が安全な期間のみに限定されるが、タイムスタンプ対象データなしにタイムスタンプの長期保証が行える点に特徴がある。一般型は、タイムスタンプ対象データが必要なため、これを保持するユーザ自身が行う必要があるが、ハッシュ関数脆弱化のリスクを含めて対応できる。

なお、DS-IMT 方式は、長期保証対象となるタイムスタンプとして、PKI 方式、リンク方式のいずれにも対応するが、本稿では、PKI 方式への対応を中心に説明する。また、DS-IMT 方式の詳細は、参考文献[1],[2] を、また DS-IMT 方式による長期有効性保証の詳細については、[3],[4]をそれぞれ参照されたい。

２．１　DS-IMT 方式のねらい

PKI 方式のタイムスタンプの長期保証は､本ガイドライン節３で記述されているように、タイムスタンプの有効性を将来にわたってオフラインで検証するために必要十分な情報を収集し、それらを元にタイムスタンプ対象データ、タイムスタンプトークンと一緒にまとめたもの（アーカイブ）に対して、新たなタイムスタンプを取得することで実現できる。

一方、タイムスタンプの有効期間は、TSA 公開鍵証明書の有効期限切れや失効、CA 秘密鍵の漏洩、公開鍵暗号アルゴリズムやハッシュ関数の脆弱化などで限定される。したがって、アーカイブの作成が、上記の事態発生前になされたことを第三者が事後に検証できる形で証明する必要がある。DS-IMT 方式では、タイムスタンプ取得から上記事態発生までに十分な期間がある場合、高精度な絶対時刻を付与しなくても、その前後関係を特定できる点に着目し、この前後関係をハッシュ関数の安全性で証明できるようにする。

２．２　DS-IMT 方式の特徴

PKI 方式などのタイムスタンプは、国家標準に高精度で同期した基準時計を用いて、文書の存在をたとえば 2005 年 3 月 8 日 9 時 10 分 11 秒のように、絶対的な時刻を証明する機能をもつ。DS-IMT 方式では、絶対的な時刻を用いることなしにイベント登録時期の前後関係を、ハッシュ関数の安全性に基づいて証明する機能のみをもつ。絶対時刻については、分単位、時間単位、など粗い粒度での証明に限定されている。そのかわり、使用しているハッシュ関数の安全性が確保されていることを前提に、

- タイムスタンプの公開鍵証明書の有効期間や公開鍵暗号アルゴリズムの安全性に制限されない長期間にわたる証明が可能なこと、
- ユーザが長期有効性登録書の正しさを自己検証できること、
- ＴＳＡの内部不正などによる不正証明書発行を防止するため、ハッシュ集約過程を外部から監視できるダイナミック・スライス技術を利用していること、

などの特徴をもつ。

このように、DS-IMT 方式は、タイムスタンプの長期保証機能に特化して、そのために必要な機能のみを長期間提供できるように工夫したタイムスタンプ長期保証方式といえる。

２．３　DS-IMT 方式の処理の流れ

DS-IMT 方式でタイムスタンプ長期保証を行う構成の例を以下の図２．１に示す。この構成例では、イベント順序証明システムが DS-IMT 方式のサーバ機能を、また TSA と監査機関がクライアント機能を提供している。

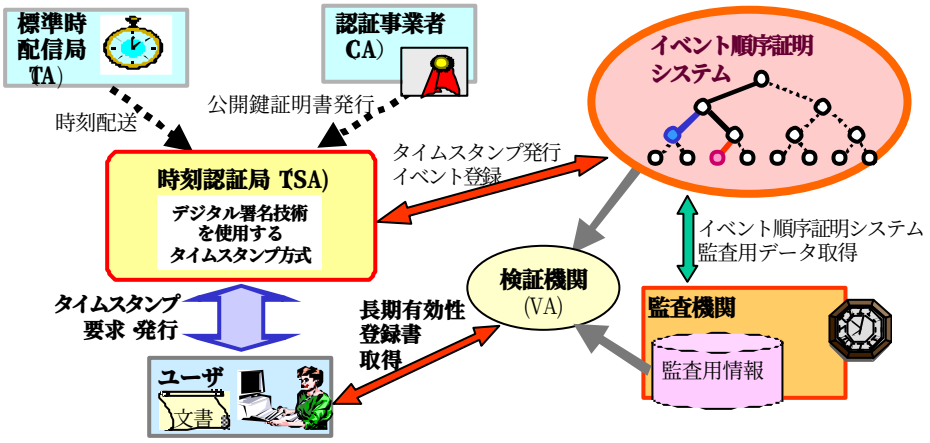


図２．１　DS-IMT 方式を用いたタイムスタンプ長期保証の構成例

DS-IMT 方式でのタイムスタンプ発行から長期有効性検証までの流れは大きく以下の 3 つのフェーズからなる。

フェーズ 1：ユーザからのタイムスタンプ要求に対する TSA のタイムスタンプ発行

図２．２に示すように、ユーザは、TSA に対して文書のハッシュ値を指定してタイムスタンプを要求し、その応答としてたとえば、PKI 方式のタイムスタンプを受け取る。このフェーズにおいて、ユーザは長期保証の仕組みを特段意識する必要がない。

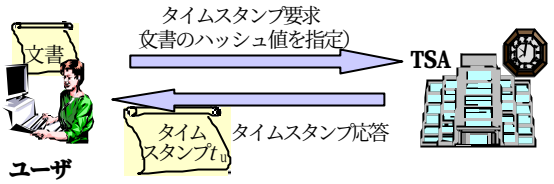


図2．2　フェーズ1: ユーザによるタイムスタンプ取得

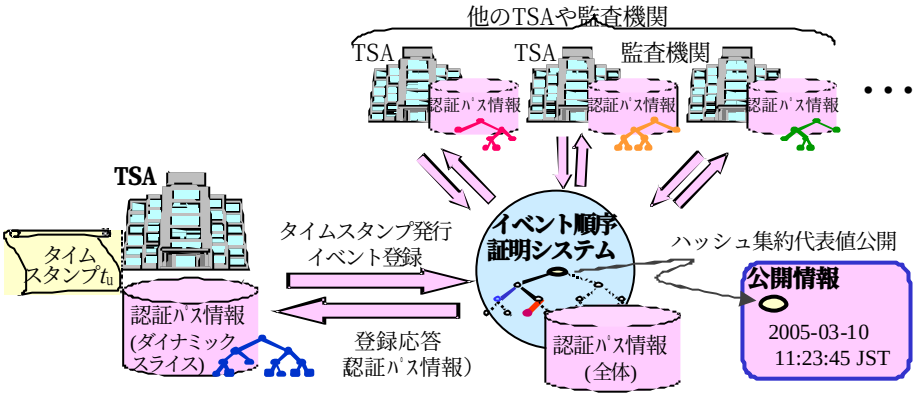


図2．3　フェーズ2 タイムスタンプのイベント順序証明システムへの登録、
およびハッシュ集約代表値の公開

フェーズ 2：TSA によるタイムスタンプのイベント順序証明システムへの登録とハッシュ集約代表値の生成と明証化

TSA は、図２．３に示すように、イベント順序証明システムに対して、発行済みタイムスタンプを登録する。この操作は、ユーザへのタイムスタンプの発行に対し遅滞なく行われることが望ましい。 この登録要求に対し、イベント順序証明システムはダイナミック・スライス情報で応答する。この情報は、ハッシュ集約過程の監査などに利用される。

イベント順序証明システムは、他の TSA や監査機関からも同様な登録要求を受け取ることができ、それらの集約結果として、ハッシュ集約結果の代表値を計算し明証化する。

なお、この例とは別の構成として、タイムスタンプ登録を TSA ではなく、ユーザ自身が行うことも考えられる。さらに、DS-IMT サーバ機能もユーザ側に実装し、監査、代表値の明証化、データのバックアップなどを外部にゆだねる構成も考えられる。

フェーズ 3：ユーザへの長期有効性登録書の発行とこれを用いた有効性検証

タイムスタンプの有効性検証の際は、検証を行うユーザは、図２．４に示すように、検証機関(VA)に対して、検証すべきタイムスタンプを付して長期有効性登録書要求を出し、その登録の事実を証明する以下の項目を持つ長期有効性登録書を受け取る（簡易型)。

① 登録されたタイムスタンプに対し、そのハッシュ値から明証化された代表値までのリンクデータである認証パス情報
② 上記認証パス情報のルート値に合致する明証化された代表値への参照情報
③ 必要ならば、タイムスタンプ登録日時をより詳細に特定するための監査用情報
④ 登録されたタイムスタンプ内の電子署名の検証に必要な証明書やＣＲＬ情報、およびそれに対する①～③の情報

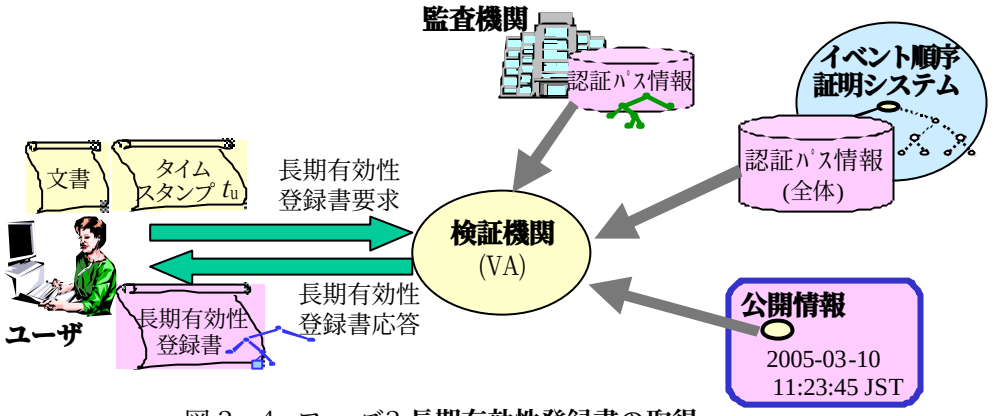


図 2．4　フェーズ3 長期有効性登録書の取得

長期有効性登録書要求は、タイムスタンプ取得から一定期間（たとえば１週間）後など、ハッシュ集約の代表値が明証化された後で、かつタイムスタンプの有効期間内に行う。ハッシュ関数の脆弱化が危惧される場合は、文書、タイムスタンプ、長期有効性登録書全体をアーカイブし、安全なタイムスタンプを再付与する（一般型）。

２．４ DS-IMT 方式によるタイムスタンプの長期保証

DS-IMT 簡易型によるタイムスタンプ長期保証は、ETSI TS 101 733 の ES-X Long Type2 形式に、また、一般型によるタイムスタンプ長期保証は ES-A 形式に対応する。前者は、タイムスタンプの安全性を前提に電子署名の公開鍵証明書の期限切れや失効、CA 秘密鍵の漏洩、公開鍵暗号アルゴリズムの脆弱化などのリスクに、また後者は、利用しているハッシュ関数の脆弱化にも対処できる([5]参照)。上記 ETSI 規定中の電子署名文書、署名検証情報およびそれに付与するタイムスタンプは、本方式では、それぞれ、長期保証対象とする PKI 方式タイムスタンプ、その有効性検証情報および長期有効性登録書に対応している。また、ES-A 形式のアーカイブに付与する新たなタイムスタンプは、本方式では、新たな PKI 方式タイムスタンプ、および、その DS-IMT 簡易型長期有効性登録書に対応する。

参考文献

[1] 石本, 小野, 堀田： イベント順序証明システムの実現機構，情報セキュリティ研究会, Vol.104 No.527, pp.33 – 38 (2004.12)

[2] 堀田，小野, 石本 ：スケーラブルで単一攻撃点のないイベント順序証明システム実現機構，電子情報通信学会，情報セキュリティ研究会, Vol.104 No.422, pp.1 – 8 (2004.11)

[3] 小野，堀田，石本：タイムスタンプ長期有効性保証フレームワーク，電子情報通信学会，オフィスインフォーメーションシステム研究会，(2005.3)

[4] 堀田，小野，石本：ダイナミック・スライス型リンキング方式による時刻証明の長期有効性保証方法，電子情報通信学会，オフィスインフォーメーションシステム研究会報告，(2005.3)

[5] 田村，宇根，岩下，松本，松浦，佐々木: デジタル署名の長期利用について，日本銀行金融研究所 IMES Discussion Paper Series No.2004-J-27 (2004.12)

Ver.1.3
タイムビジネス推進協議会

参加メンバー　ガイドライン分科会

（長期保証ＷＧメンバー）

（順不同・敬称略）

主　査	株式会社エイベック	本田　雅裕
リーダー	三菱電機株式会社	宮崎　一哉
メンバー	アマノタイムビジネス株式会社	市川　桂介
〃	株式会社ＮＴＴデータ	坂本　弘章
〃	株式会社ＮＴＴデータ	橋川　善之
〃	セコム株式会社	島岡　政基
〃	セコムトラストネット株式会社	西山　晃
〃	独立行政法人情報通信研究機構	岩間　司
〃	日本電気株式会社	後藤　淳
〃	日本電信電話株式会社 （現：工学院大学）	小野　諭
〃	株式会社 PFU	野口　隆弘
〃	株式会社日立製作所	谷川　嘉伸
〃	富士通株式会社	小谷　誠剛
〃	三菱化学メディア株式会社	入沢　芳久

【連絡先】

タイムビジネス推進協議会（ＴＢＦ）

〒160-0022
東京都新宿区新宿 1-20-2　**小池ビル**
財団法人テレコム先端技術研究支援センター
タイムビジネス推進協議会事務局
Tel.03-3351-8423
Fax.03-3351-6690
URL：http://www.scat.or.jp/time/