# 電子署名検証ガイドライン

V1.0.0

2013 年 6 月 5 日

タイムビジネス協議会

調査研究 WG

目次

# 1 はじめに

本書のスコープ、対象読者、構成、及び推奨する参照範囲は以下のとおりである。

**スコープ：**

- デジタル署名（PKI ベースの電子署名。以降、単に「署名」と呼ぶ）の検証処理に関するガイドライン（規約部分を含む）を定める。
- 規約には技術的有効性を確認するための要件を定義する。
  - 署名検証の共通要件と XAdES/CAdES 固有要件とを定義する。
  - PAdES 固有要件は今版ではスコープ外とする。
- 法的有効性に関してはスコープ外とする。
- 規約には既定値を示す。既定値であると判断する基準は、技術的な安全性確保を優先して決定することとし、各国の法規制等に依存する要素や適用領域の事情に依存する要素は極力排除することとする。
- 各実装における既定値との差分を明示するための供給者による適合宣言書の書式を提供する。

**対象読者：**

- 署名検証システムあるいはサービスの利用者。
- 署名検証システムあるいはサービスの調達者。
- 署名検証システムあるいはサービスの開発者（設計者および実装者）。

**構成：**

- 1 章：本章。本書のスコープ、対象読者、構成、使い方を記す。
- 2 章：本書が準拠すべき規格（引用規格）と参考となる文献（参考文献）を記す。
- 3 章：用語定義と略称を記す。
- 4 章：署名および署名検証の基本概念、署名検証アプリケーションおよび検証結果の概念モデルを記す。
- 5 章：署名検証の詳細要件（規約部分）を記す。
- 付録：供給者適合宣言書の書式及び実装に関わる参考情報等を記す。

**推奨する参照範囲：**

- 利用者は 3 章を参照し、4 章を読むことを推奨する。
- 調達者は 3 章を参照し、4 章、5 章を読むことを推奨する。
- 開発者は 2 章及び 3 章を参照し、4 章、5 章、付録を読むことを推奨する。

## 2 参照文献

### 2.1 引用規格


[1] ETSI TS 101 903 (V1.4.2): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[2] ETSI TS 101 733 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[3] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[4] ISO/IEC 9594-8:2005: "Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks".

[5] W3C Recommendation: "XMLSignature Syntax and Processing", 2008

[6] IETF RFC 3161: "Internet X.509 Public Key Infrastructure; Time Stamp Protocol (TSP)".

[7] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[8] ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[9] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

[10] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[11] ETSI TS 102 778-5: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

[12] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[13] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[14] IETF RFC 6238: "Extensible Markup Language Evidence Record Syntax (XMLERS)"

## 2.2 参考文献

[i.1] IETF RFC 4158: "Internet X.509 Public Key Infrastructure: Certification Path Building".

[i.2] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[i.3] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[i.4] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

# 3 用語定義と略称

## 3.1 用語

**高度電子署名（Advanced Electronic Signature (AdES)）：**

次の要件を満たす電子署名。

1) 署名者とユニークに関係付けられている
2) 署名者を特定することができる
3) 署名者単独の制御下にある手段で生成される
4) その後データが改ざんされたことを発見できるような方法でデータと関連付けられている

**注：**

以降、本書では高度電子署名を「署名」と略して用いる。

**証明書検証（certificate validation）：**

証明書そのものと証明書パスの有効性を確認する処理。

**制約（constraints）：**

上記で定義した署名の検証で照合する、規則、値、範囲、計算結果の抽象的に定式化したもの。

**署名対象データ（data to be signed）：**

署名されるデータ（例えば、文書や文書の部分)。署名によってデータに付与される署名属性を伴う。

注：署名対象データは、暗号による署名アルゴリズムの入力である。署名対象データと署名属性を入力として与える方法の仕様は、署名タイプ毎に仕様書で定義される。

**駆動アプリケーション（Driving Application (DA)）：**

SVA と呼ばれる電子署名検証のためのアプリケーション（を含む？)。SVA は DA に対して検証結果を返す。

**署名ポリシ（signature policy）：**

電子署名の生成や検証のための規則の集合。これに基づいて、特定のトランザクションの文脈における署名の有効性が決定する。

**署名検証（signature verification）：**

署名検証データを利用して署名の暗号化された値を検証する処理。

**署名有効性検証（signature validation）：**

署名の有効性を確認する処理。証明書の有効性検証や、署名検証を含め、署名がローカルなあるいは共通の署名ポリシが要求することに従っているかどうかを総合的に確認することを含む処理。

注：

・verification：正しいこと／事実であることを確かめる／実証する／検証すること

・validation：有効であること／妥当であることを認める／確認する／認証すること

**署名検証アプリケーション（Signature Validation Application (SVA)）：**

本書に定義された署名有効性検証処理を実装したアプリケーション。

注：署名有効性検証アプリケーションは、駆動アプリケーション（DA）との間で検証結果をやり取りする。

**検証制約（validation constraint）：**

電子署名の有効性を検証するときに SVA によって適用される基準。有効性検証制約は、形式的な署名ポリシ、設定ファイル、あるいは SVA の処理に組み込まれたものとして定義できる。

**検証情報（validation data）：**

署名者や検証者によって収集された、電子署名の有効性検証に必要なデータ。

注：証明書、失効情報（CRL や OCSP-Response）、タイムスタンプ、タイムマークなどを含む。

**検証者（verifier）：**

電子署名の有効性検証や検証を欲するエンティティ。

### 3.2 略語

| | |
|---|---|
| AdES | Advanced Electronic Signature |
| BES | Basic Electronic Signature |
| CAdES | CMS Advanced Electronic Signatures |
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| DA | Driving application |
| EPES | Explicit Policy-based Electronic Signature |
| LT | Long Term |
| LTA | Long-Term with Archive Time Stamp |
| LTV | Long Term Validation |
| OCSP | Online Certificate Status Provider |
| OID | Object Identifier |
| PAdES | PDF Advanced Electronic Signatures |
| PKIX | Public Key Infrastructure X. 509 |
| RSA | Rivest-Shamir-Adleman |
| SVA | Signature Validation Application |
| TSA | Time Stamping Authority |
| TST | Time-Stamp Token |
| URI | Uniform Resource Identifier |
| XAdES | XML Advanced Electronic Signatures |

# 4　概念モデル

## 4.1 署名および署名検証の基本概念

### 4.1.1 認証局と電子証明書

公開鍵暗号方式では、秘密鍵（Private key:私有鍵とも呼ばれる）と公開鍵（Public key）の 1 組の鍵ペアによる暗号技術がベースとなっており、電子署名の生成に秘密鍵を、その検証に公開鍵を用いる。電子署名の本人性を確保する上での前提事項は以下の 2 点である。

① 署名者本人以外が秘密鍵を使用できないこと

② 公開鍵が署名者の所有する秘密鍵とペアとなるものであることが担保できること

ここで、公開鍵の所有者を保証することが重要となる。

“信頼できる第三者機関”（Trusted Third Party、以下 TTP）が公開鍵の所有者を保証するモデルが認証局モデルであり、認証局は利用者の本人確認を実施した上で公開鍵の所有を証明する公開鍵証明書の発行を行い、秘密鍵と公開鍵の紐付けを保証する。公開鍵証明書には発行元の認証局の電子署名が付与され、一般的には電子証明書とも呼ばれる（本書では以下、証明書と記す）。

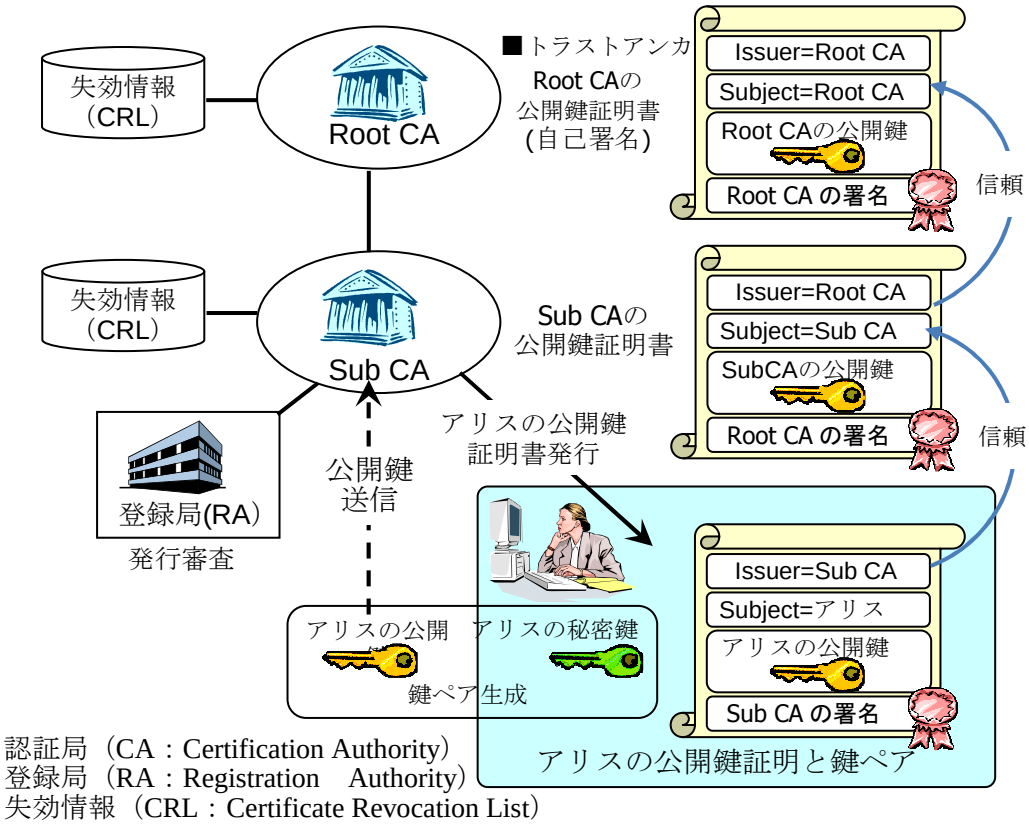


**図 1　認証局の階層構造と公開鍵証明書**

また、署名者は秘密鍵を本人以外が使用できないよう安全に管理する必要がある。秘密鍵の紛失や、鍵活性化に用いるパスワードの漏洩などにより、万一、秘密鍵が危殆化（本人性の証

明に使えなくなる状態）した場合、署名者は認証局に失効申請を行い、これを受けた認証局は無効となった証明書のシリアル番号を記載した失効情報に認証局の電子署名を付与して開示している。

尚、失効情報は CRL(Certification Revocation List)や失効リストとも呼ばれ、その更新頻度は失効した証明書の追加に合わせて実施される不定期な更新と、定期更新がある。

図 1 に、認証局の階層構造と公開鍵証明書の例をクライアント側で鍵ペア生成する場合について示す。

### 4.1.2 電子署名と署名検証の概要

■電子署名の法的定義

ここで、電子署名の法的定義を確認すると、電子署名法[1]2 条 1 項にて、

「電子署名」とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

(一部省略)

とされており本人性が確認できること、及び、改ざん検知ができることが電子署名の要件となっている。従って、電子署名の有効性を検証する場合は、本人性の確認、署名対象データの非改ざん性の確認の 2 点を実施する必要がある。

また、同法は、自然人を対象としており、電子署名に法的有効性を与えている(第 3 条)。

尚、同法による認定を受けた特定認証業務(認定認証業務とも呼ばれる)では証明書の有効期間は 5 年を超えないもの（同法、施工規則第 6 条）とされており、認定以外の認証業務においても、署名に用いる証明書の有効期間の基準とされている。

■電子署名の基本要件

電子署名のメカニズムは、署名対象文書に対して、ハッシュ関数にて演算実施、得られたハッシュ値を公開鍵暗号方式により署名者の秘密鍵を用いて暗号化したものが、署名データとなる。

電子署名の有効性を検証する際は、署名データを署名者の公開鍵で復号して得られたハッシュ値と、署名対象文書からハッシュ演算をして得られるハッシュ値を比較し、双方のハッシュ値の一致を確認することにより、公開鍵と秘密鍵の紐付け、及び、署名対象文書が改ざんされていないことが確認できるので、電子署名の本人性、非改ざん性を検証することができる。

尚、本書執筆現在、電子署名に用いられているハッシュ関数は SHA-1、公開鍵暗号は鍵長 1024bit の RSA 方式が大半を占めるが、将来的に暗号アルゴリズムの脆弱化が予想される

[1] 電子署名及び認証業務に関する法律（平成十二年五月三十一日法律第百二号）

ため、政府系の情報システムでは 2014 年 9 月以降、より強固な暗号アルゴリズムである SHA-2、RSA2048bit への移行が予定されている。
図 2 に署名と検証の概要を示す。

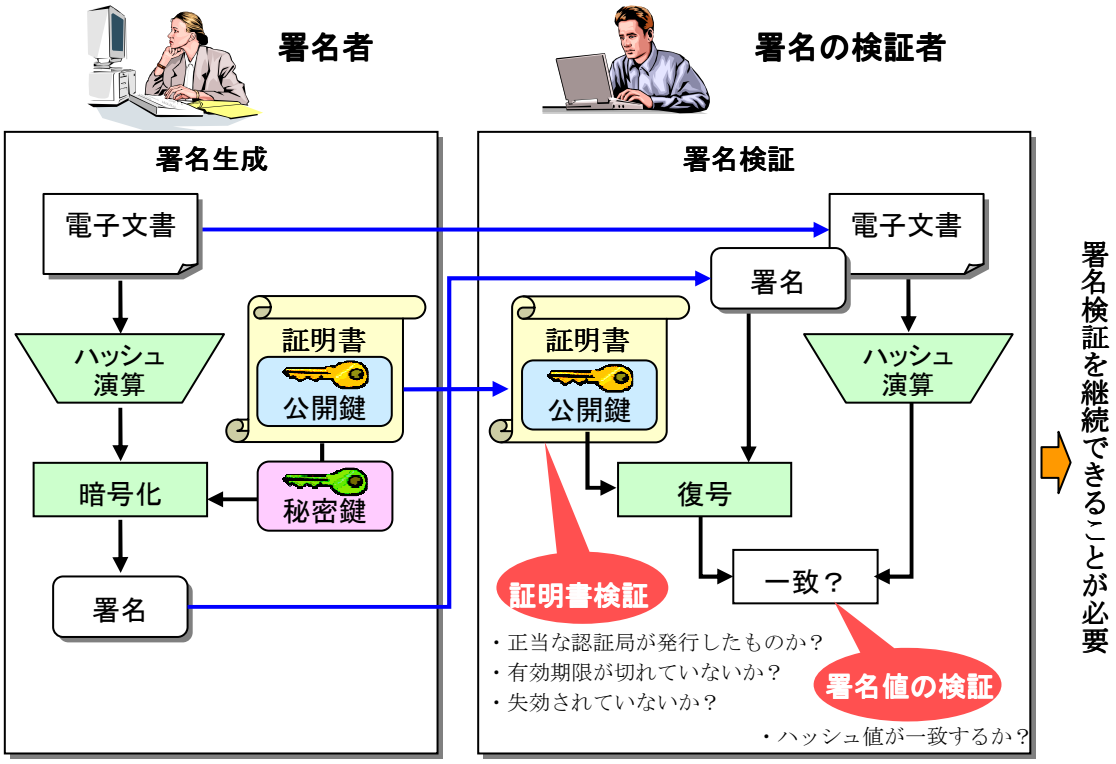


**図 2 署名と署名検証（RSA 署名の場合）**

また、電子署名を実施する際には、その目的に応じ、以下の項目に留意した適切な利用が必要となる。

（1） 署名文書の利用用途に応じた適切な証明書を用いること

目的に応じて利用できる証明書の範囲（例、認定認証業務など）が示されている場合それに従うこと。認証局が開示する「証明書ポリシ」（Certificate Policy、以下 CP）に発行基準や用途が規定されているので、該当する認証局から署名者本人に対して発行された正当な証明書を利用する必要がある。

（2） 電子署名を実施する際に証明書の有効期間を越えていないこと

証明書の有効期間は発行時点から通常 5 年を超えない範囲で設定[2]されているが、電子署名を実施する時点においてこの有効期間を越えていないことが必要となる。

（3） 失効していない証明書を用いること

[2] 電子署名法施行規則にて認定認証業務の証明書では有効期間は 5 年を超えることを認めていないため、他の証明書の場合でも、これに準ずる場合が一般的

署名時点で失効していない証明書の秘密鍵を用いる必要がある。

（4） 署名文書の利用期間を通じて、電子署名の正当性が確認可能であること。
法定保存期間等、署名文書の真正性の維持継続が必要な期間、電子署名の検証を可能とする必要がある。（証明書の有効期間を越えて署名検証を行う場合は、後述のAdES フォーマットなどを採用する必要がある）

【（４）の規定例】
国税関係書類においては、電子帳簿保存法施行規則（第 3 条第 5 項第 2 号ロ(3)）にて定められ、同法取扱通達 4-26 にてその方法について解説されている。また、医療関係書類では､厚労省の｢医療情報システムの安全管理に関するガイドライン第 4.1 版｣6.12 節にて定められ、法定保存期間等の一定の期間、電子署名の検証が継続できる必要があるとされている。

■署名検証の基本要件

一方、電子署名の検証は、電子署名法から見ると、署名の本人性と非改ざん性を確認する事が求めらる事となる。前者は「証明書検証」、後者は「署名値の検証」と定義され、上記、（１）～（４）を適切に確認し、また、署名文書が改ざんされていないことが確認できる必要がある。

・証明書検証（本人性の確認、上記（１）、（２）、（３）の確認）
署名に用いた証明書が正当な認証局から署名者本人に対して発行されたもので（１）、署名当時に有効期間が切れておらず（２）、失効していない有効な証明書（３）で有ったことを確認

・署名値の検証（非改ざん性の確認）
署名文書が改ざんされていないことをハッシュ値を比較することで確認

・署名文書の利用期間を通じて、電子署名の正当性が確認可能であること。（上記（４））

ここで署名検証は電子署名を付与し、一定期間経過した後に行われる行為であることに着目してみると、何時の時点の署名の有効性を確認するのかその時刻の設定によっては、証明書の失効や暗号アルゴリズムの脆弱化などの要因により、検証結果に影響を及ぼすことが考えられる。何時の時点での署名の有効性を検証するのか、本書ではその時刻を「検証基準時刻（validation reference time)」と定義している（5.1.6 参照)。例えば本来の署名検証の目的は署名時点における電子署名の有効性を確認することにあるので、検証基準時刻は“電子署名を付与した時点”となる。但し、次節のタイムスタンプを併用するなど、客観的な署名時刻が確認できない場合は、検証基準時刻は署名検証を実施する現在時刻となる。

### 4.1.3 タイムスタンプ局の役割

証明書検証においては、署名時点での証明書の有効性が問われることとなるが、ここで署名時刻等を保証する客観的な時刻情報が必要となる。

この役割を担う信頼できる第三者機関（TTP）がタイムスタンプ局（Time Stamp Authority：TSA）であり、電子文書に正確な時刻情報を含むタイムスタンプトークン（TST）を付与し、タイムスタンプ時刻以前からその電子文書が存在していたことを証明し、それ以降、改ざんされていないことを証明可能とする。

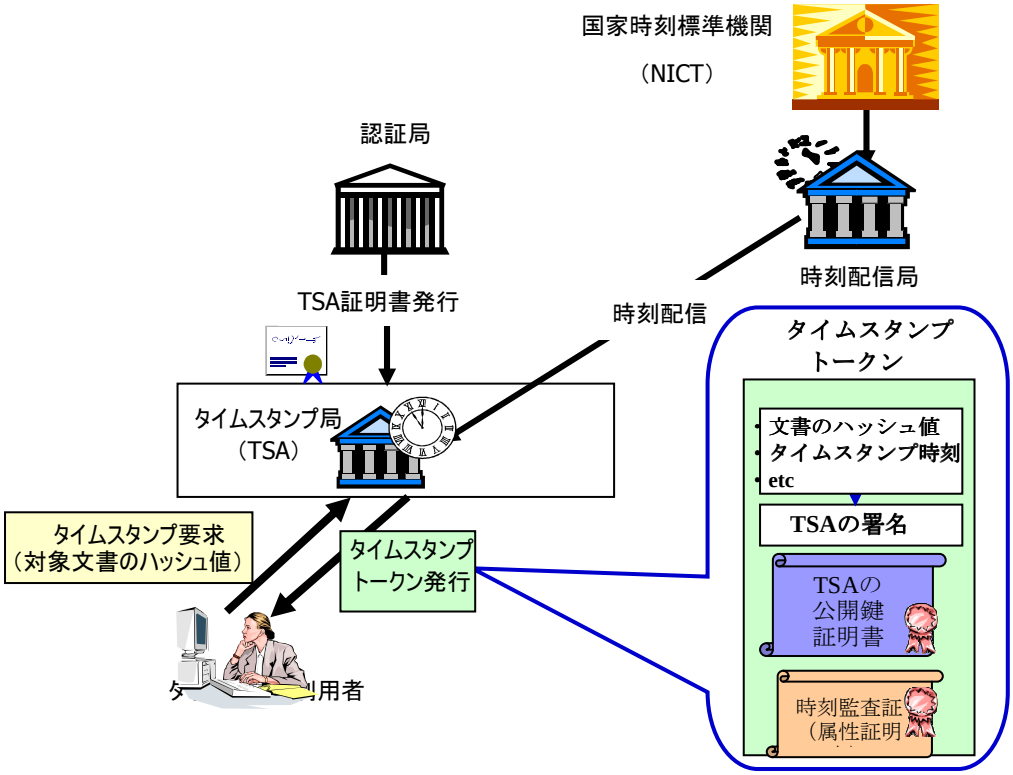


図 3 タイムスタンプ局の概要（デジタル署名方式の場合）

### 4.1.4 長期署名の考え方（AdES フォーマット）

法定保存期間が定められた文書を保存する場合など、将来にわたり一定期間、署名検証が可能であることが必要となる。その際、特に「証明書検証の継続性」に対して留意する必要がある。証明書検証に際しては 4.1.2 の■電子署名と署名検証の基本要件で述べた以下の 4 点を確認することになる。

（1） 署名文書の利用用途に応じた適切な証明書を用いること
（2） 署名当時に証明書の有効期間が切れていないこと
（3） 失効していない証明書を用いて署名していたこと
（4） 署名文書の利用期間を通じて、上記（１）～（３）が確認可能であること。

図 4 では、(1)から(3)を図示しているが、(1)及び、(2)を実現するために、署名時刻が何時で有ったのか客観的に示せる事が必要となるのでタイムスタンプを利用する。また署名時点での証明書の有効性を確認するためには、失効情報を保管する必要がある。

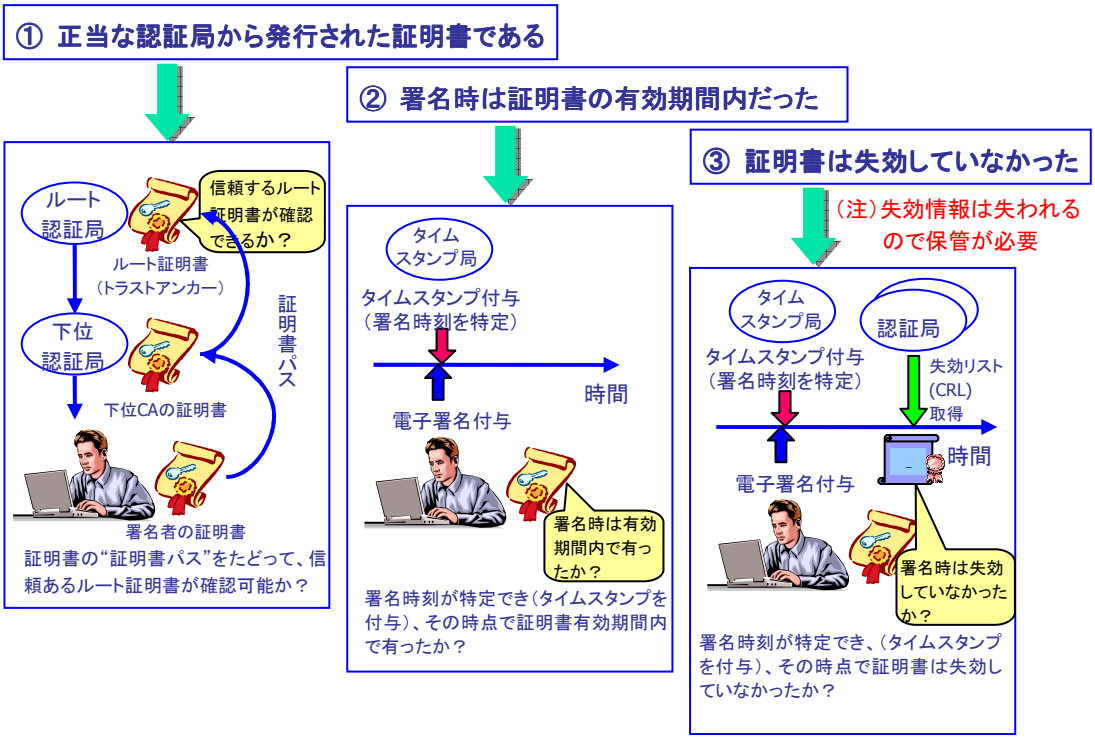


図 4 証明書検証の要素

通常、認証局は証明書の有効期間を越えて失効情報の公開はしていない。すなわち、失効情報には失効した証明書のシリアル番号が記載されているが、多くの認証局では失効情報の肥大化をさけるため、失効した証明書の有効期間が過ぎるとそれらのシリアル番号は失効情報から消去される。従って、証明書の有効期間を越えて証明書の有効性の確認が出来ないことになる。従って、署名検証を継続する必要がある場合は、失効情報を確保しておく必要がある。

このような問題を解決するために、電子署名の有効性を証明書の有効期間や失効、さらには、署名に用いた暗号アルゴリズムが脆弱化した後も維持できる署名規格として、AdES (Advanced Electronic Signature : 高度電子署名)がある。このフォーマットに示されるように、証明書検証に必要な失効情報等のデータを合わせて保存し、タイムスタンプを付与することが有効である。その手順の概要は、以下となる。

(1) 署名対象データ全体に対して電子署名を付与

(2) 署名直後にタイムスタンプ(署名タイムスタンプ)を付与し、署名時刻を特定しておく

(3) 証明書検証に必要となる、以下の検証情報を収集格納する。

タイムスタンプ局の証明書

署名者の証明書

証明書パス上の認証局の証明書[3]

[3] 証明書パス上の認証局は、署名者の証明書を発行する認証局とタイムスタンプ局に証明書を

上記のすべての認証局の失効情報

(4)　上記の署名対象文書や署名値、検証情報全体に対してタイムスタンプ（アーカイブタイムスタンプ）を付与

図 5 に上記手順のフローイメージを示す。ここで、各タイムスタンプの役割は、

- 署名タイムスタンプ
  電子署名時刻の信頼性を確保する
- アーカイブタイムスタンプ
  署名文書と失効情報をタイムスタンプの暗号アルゴリズムにより保護し、長期に渡り電子署名の真正性を継続する

ことにある。即ち、タイムスタンプにより署名時刻を特定して、検証基準時刻とし、その時刻において、有効な証明書を用いて署名した事を後日検証可能とするのである。

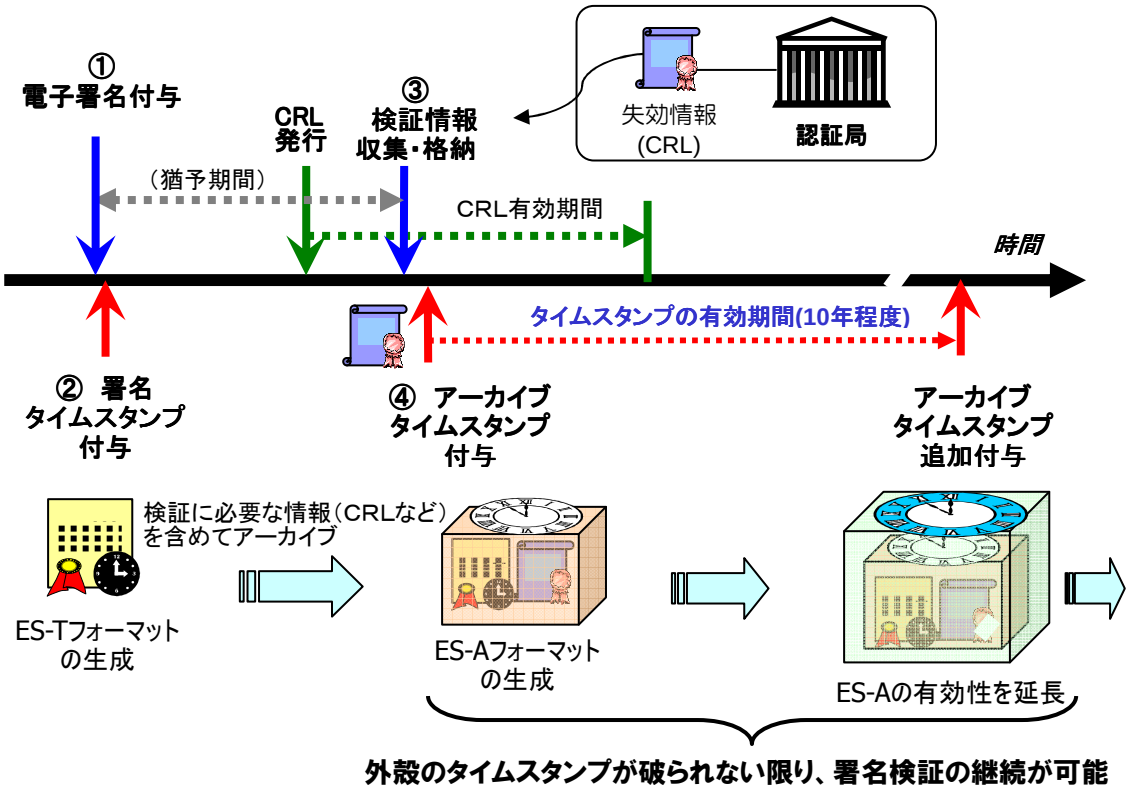


図 5 長期署名フォーマットによる署名延長

署名検証に必要となる情報には、署名対象データと署名値以外に、関連する証明書や失効情報、また、署名文書の利用目的に応じたトラストアンカーの制限や暗号アルゴリズム

---

発行する認証局の２つの認証ドメインでのすべての認証局となることに留意されたい

の有効性に関する情報などのさまざまな情報が必要となる。これら、署名検証に必要となる前提条件のことを、検証制約（Validation constraints）と呼び、以下のようなものが挙げられる（5.1 参照）。

- 署名文書の利用目的に合致した証明書を発行する認証局のトラストアンカー
- 証明書パスに含まれるすべての証明書、証明書の利用用途などの制約
- 失効情報
- タイムススタンプ
- 検証基準時刻
- 有効と認められる暗号アルゴリズムの制約
- 署名データを構成する要素に対する制約

### 4.1.5 署名データの形式と AdES の種類

署名対象データと署名データは 1 つのファイルに統合して作成することもできるが、独立した 2 つのファイルとして作成する事もできる。署名対象データと署名データの形式には、図 6 に示されるように、以下の 3 つに大別でき、利用形態に応じて選択することができる。

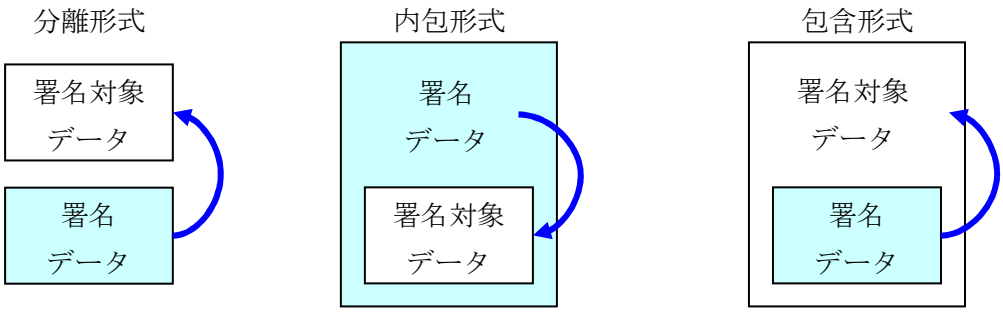


**図 6 署名対象データと署名データの形式**

それぞれ、以下のような特徴がある。

（1） 分離形式（Detached 型）

署名対象データとは独立して、署名データを作成する形式。署名対象データの種別は問わず、あらゆるファイル形式に対して署名データが作成きる。既存アプリで署名対象データを取り扱っている場合など、アプリ側への影響が少なくて済む。一方、署名対象データと署名データを紐づけて管理する必要がある。

（2） 内包形式（Enveloping 型）

署名データの中に署名対象データを格納（内包）して作成する形式。署名対象ファイルと署名データが 1 つのファイルとなるので扱いやすい。一方、アプリなどで署名対象データを利用する場合、署名データから、署名対象データを取り出す必要がある。

（3） 包含形式（Enveloped 型）

署名データが署名対象データの中に含まれる（包含）形で作成する形式。(2)と同様に 1 つのファイルを管理すれば良いので扱いが容易。一方で、署名対象データのファイル形式が、電子署名をサポートしている事が必要となり、作成できるファイル形式には制限がある（例：PDF や XML など）。

また、AdES フォーマットには、上記の署名形式や署名対象ファイル種別に応じて以下の種類がある。

■CAdES（CMS Advanced Electronic Signatures）

汎用的な署名ファイル形式である CMS（Cryptographic Message Syntax）をベースとした AdES。署名対象データのファイルの形式は限定されないため、広く様々なファイルへ電子署名を付与できる。分離形式、内包形式の電子署名に用いられる。

■XAdES（XML Advanced Electronic Signatures）

XML ファイルルを対象とした電子署名形式である XML 署名をベースとする AdES。分離形式、内包形式、包含形式のすべてに用いることができる。

■PAdES（PDF Advanced Electronic Signatures）

PDF ファイルの内部構造の中へ署名データを埋め込む包含形式の AdES。署名対象ファイルは PDF 形式に限定されるが、署名された PDF ファイルを単独で扱うことができ、Adobe® Reader®でも検証できる利点がある。

### 4.2 署名検証アプリケーションの概念モデル

4.1 節で述べた署名データの検証処理の実装には、PC やデバイス等で実行されるグラフィカルユーザインタフェースを備えたソフトウェアや、コマンドラインツール、他のアプリケーションに組み込まれるライブラリやミドルウェア、Web アプリケーションや Web サービスなど様々な方法が考えられる。そのような様々な実装を概念的なモデルとして表現するために、この規格では駆動アプリケーションと署名検証アプリケーションに分けて考える（図）。署名検証アプリケーションとは、入力された署名データの検証を行い、署名データの判定結果やレポート内容を出力するモジュールのことをいう。署名検証アプリケーションは、駆動アプリケーションから入力された署名データを検証し、検証レポートを駆動アプリケーションに返す。駆動アプリケーションは検証レポートに基づいて検証者に検証結果を表示を行う。ソフトウェアの構成によっては駆動アプリケーションと署名検証アプリケーションが一体となっている場合もある。本規格では署名検証アプリケーションが実行すべき署名データの検証項目に関する要件を定めるものとする。

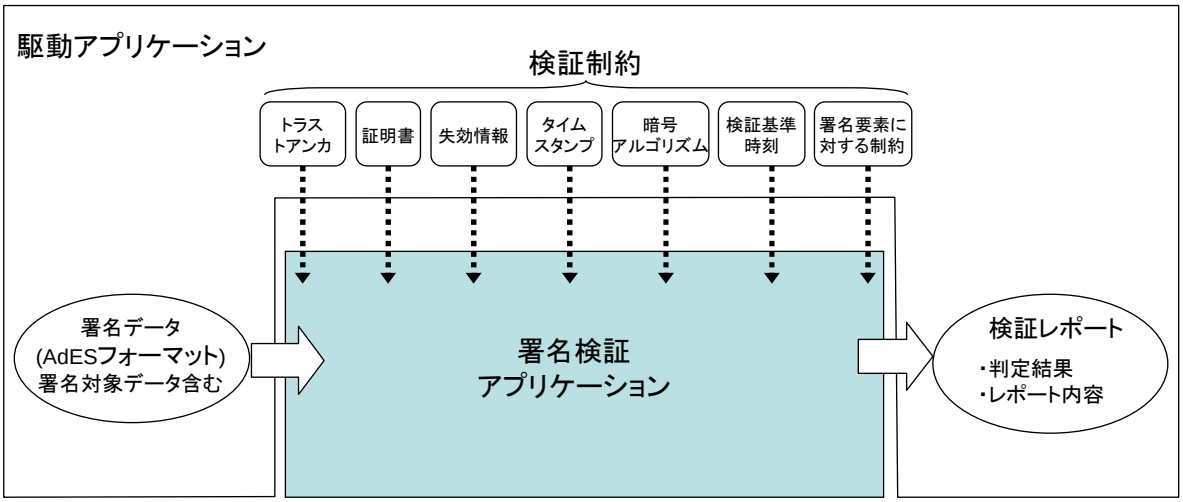


**図 7 署名検証アプリケーションの概念モデル**

検証レポートには署名データの判定結果やレポートの詳細な内容な情報が含まれる。

検証制約は署名検証アプリケーションが署名データの有効性を判断するときの条件を示すものである。検証制約には、例えば、検証者が信頼するトラストアンカ、証明書の検証情報（中間認証局証明書や失効情報）、証明書ポリシーや暗号制約などがある。検証制約は駆動アプリケーションを介して検証者が設定できる場合や、署名ポリシー等の記述に従い駆動アプリケーションが署名検証アプリケーションに入力する場合や、署名検証アプリケーションや駆動アプリケーションのコードに組み込まれている場合もある。証明書の検証情報については検証処理の実行時にオンラインで取得する場合もある。

### 4.3 署名判定結果の概念モデル

署名データの判定結果には以下の種類がある。

- VALID (有効)

  署名者による署名やタイムスタンプの対象となったデータの改ざんがなく、かつ、署名者やタイムスタンプを発行したタイムスタンプ局の身元が信頼できると判断された状態。検証すべき項目の全てが VALID であるとき、署名データ全体を VALID と判定する。VALID である署名データは少なくとも以下の全ての内容を満たしている。

  - 署名者による署名やタイムスタンプのハッシュ値や署名値が正しく検証できること。
  - 署名者の証明書やタイムスタンプ局の証明書が信頼できること。例えば、信頼する認証局から発行されていることや、有効期間内にあること、失効されていないこと等。

- INVALID (無効)

  検証すべき項目のうち少なくとも 1 つが INVALID と判断された場合、署名データ全体を INVALID と判定する。

- INDETERMINATE (未確定)

  入手された情報による設定では VALID もしくは INVALID と判定するには不十分である。例えば、署名検証アプリケーションの実行時に検証に必要な失効情報を入手できず、証明書の失効状態を確認することができなかった場合には、INDETERMINATE として判定される。INDETERMINATE と判定された署名データは、他の証拠となる情報と照らし合わせた場合に、VALID もしくは INVALID として判定することもできる。

# 5 検証要件

## 5.1 検証制約

署名検証システムには、検証対象となる署名データ（署名対象のコンテンツを含む）だけでなく、外部からの情報を参照する必要がある場合がある。また、署名利用分野の必要に応じて検証結果を規約で定める既定値と異なる値としたい場合、差分を制約条件として与えることが考えられる。これらの情報を総称して検証制約と呼ぶこととする。

検証制約の与え方としては次の方法が考えられる。

- 署名ポリシー（[i.2][i.3]準拠）
- 設定ファイル（独自形式）
- 実装ロジックへの埋込み

以下に検証制約とその関連情報を示す。

### 5.1.1 トラストアンカ

署名データに検証情報としてルート証明書が含まれる場合がある。ところが、署名データに含まれていることを根拠にルート証明書を署名（タイムスタンプ、失効情報を含む）検証時に信頼できると、あるいは過去の署名生成時に信頼していたと判断することはできない。従って、信頼点については現在のもの／過去のものを問わず、検証処理に外部から与える必要がある。

### 5.1.2 証明書

署名データにトラストアンカにいたる認証パス上の証明書のセットが含まれる場合とそうでない場合がある。含まれない場合、署名検証ステムに外部から与える必要がある。

認証パスが複数存在する場合、通るべきパスに制限を加える必要がある場合がある。このような場合、検証処理に外部から制約条件を与える必要がある。

また、証明書内の要素に対して既定値ではオプショナルなものを検証する必要がある場合や、その要素の値がある条件を満たす必要がある場合がある。このような場合も、それらの条件を検証処理に外部から制約として与える必要がある。

### 5.1.3 失効情報

有効期限が切れていない証明書の失効状態を確認するために、失効情報を署名検証システムに外部から与える必要がある。署名データ（タイムスタンプ含む）に検証情報として失効情報が含まれる場合があり、それが対象となる署名データ（タイムスタンプ含む）の失効情報として適切なとき（検証基準時刻の観点から適切なタイミングに発行されているとき。詳細は 5.3 を参照）にはそれを利用することができる。

### 5.1.4 暗号アルゴリズムの脆弱性に関する情報

署名データ（証明書、失効情報、タイムスタンプ等を含む）の生成には各種暗号アルゴリズムが用いられ、その種別は OID 等で署名データに含まれる。ところが、各暗号アルゴリズムが利用された時点で脆弱でなかったことを示す根拠は署名データには含まれない。従って、各暗号アルゴリズムが利用された時点で脆弱でなかったことを確認するためには外部の情報を参照する必要がある。

### 5.1.5 タイムスタンプ

適用領域や法制度の要請等により、信頼すべきタイムスタンプを選別する必要がある場合がある。信頼すべきタイムスタンプであるか否かを判断するために、タイムスタンプトークンに含まれるタイムスタンプポリシ、発行者、信頼点、精度等の要素に関する制約を外部から与える必要がある場合がある。

### 5.1.6 検証基準時刻（validation reference time）

証明書の有効性や暗号アルゴリズムの非脆弱性を判断する際に規準とする時刻（検証基準時刻と呼ぶ）は検証対象により適切に選ぶ必要がある。

対象となる証明書についての検証基準時刻は、その証明書を MessageImprint の計算対象に含む有効なタイムスタンプトークンのうち、最も古いものの示す時刻であり、該当するタイムスタンプがない場合、検証処理を実行する時刻となり、検証処理に外部から与える必要がある。

また、暗号アルゴリズムについての検証基準時刻は、対象となる暗号アルゴリズムにより計算された結果を MessageImprint の計算対象に含む有効なタイムスタンプトークンのうち、最も古いものの示す時刻であり、該当するタイムスタンプがない場合、検証処理を実行する時刻となり、検証処理に外部から与える必要がある。

### 5.1.7 署名要素に対する制約

適用領域や法制度等の要請により、署名データを構成する各種要素について、規約において検証必須として規定されている要素の検証を不要としたり、逆に検証オプションとして規定されている要素の検証を必須とする場合がある。このようなときに外部より検証制約としてそれらの条件を指定することができる。ただし、本規約で必須と規定している要素の検証を不要とすることは、安全性の観点から望ましくない。

## 5.2 要求レベル（必須とオプション）の考え方

この規格の検証要件のレベルを以下のように定める。

- 必須 [Mandatory]
  この検証項目は必ず実行しなければならない。この検証項目に必要なフィールドが署名データに存在しない場合には INVALID と判定する。
- 存在時必須 [Mandatory if Exists]
  該当するフィールドが署名データに存在する場合には、この検証項目は必ず実行しなければならない。該当するフィールドが存在しない場合には、この検証項目をスキップしてよい。
- オプション [Optional]
  この検証項目を実行するか否かはアプリケーションの要件に依存する。

この規格に基づくプロファイルを規定することで、[Optional]の検証項目を[Mandatory if Exists]または[Mandatory]に、[Mandatory if Exists]の検証項目を[Mandatory]に再定義することもできる。

[Mandatory]の選択基準は、電子署名としてセキュリティを担保するために最低限実行しなければならない事項。検証の制約条件の違いなどに依存しないもの。

[Mandatory if Exists]の選択基準は、電子署名の特定のフィールドの使用は電子署名の用途に依存しているが、そのフィールドは電子署名のセキュリティを担保するために意味をもつもの（要検討）。

[Optional]の選択基準は、電子署名の特定のフィールドの使用方法が電子署名の用途に依存しているもの。

[Mandatory]もしくは[Mandatory if Exists]の項目を検証しない実装は自己宣言書に記すこと。

### 5.3 検証の全体構造

この節では署名データの各形式における論理的な構成と各要素の検証方法が記述された節への参照関係について述べる。

#### 5.3.1 署名者による署名(Simple ES)

Simple ES は署名者による署名のみが付与された基本的な形式である。Simple ES の論理的な構造とこの規格の検証要件の各節との関係を図に示す。Simple ES の仕様が記述された各規格の一覧を表 1 に示す。

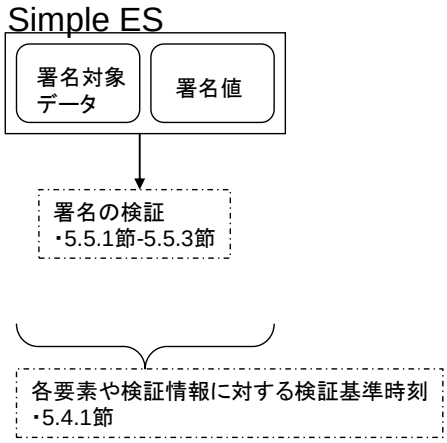


図 8 Simple ES の検証

表 1 Simple ES の規格

| 規格分類 | 規格種別 | 対象フォーマットタイプ |
|---|---|---|
| ベース規格 | CAdES(ETSI TS 101 733) | CAdES-BES |
| | | CAdES-EPES |
| | XAdES(ETSI TS 101 903) | XAdES-BES |
| | | XAdES-EPES |
| | PAdES(ETSI TS 102 778) | PAdES-Basic |
| | | PAdES-BES |
| | | PAdES-EPES |
| プロファイル | ETSI CAdES baseline profile | B-Level |
| | ETSI XAdES baseline profile | B-Level |
| | ETSI PAdES baseline profile | B-Level |
| | ISO 14533-1 | - |
| | ISO 14533-2 | - |

### 5.3.2 署名タイムスタンプ付き署名(ES with signature timestamp)

ES with signature timestamp は署名者による署名(Simple ES)と共に署名タイムスタンプを付与した形式である。ES with signature timestamp の論理的な構造とこの規格の検証要件の各節との関係を図に示す。ES with signature timestamp の仕様が記述された各規格の一覧を表 2 に示す。

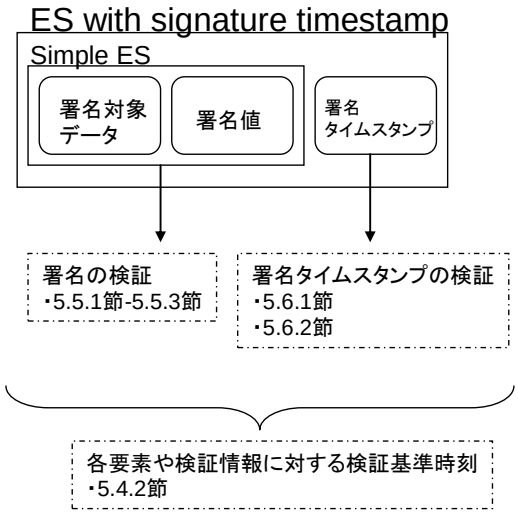


図 9 ES with signature timestamp 検証

表 2 ES with signature timestamp の規格

| 規格分類 | 規格種別 | 対象フォーマットタイプ |
|---|---|---|
| ベース規格 | CAdES(ETSI TS 101 733) | CAdES-T |
| | XAdES(ETSI TS 101 903) | XAdES-T |
| | PAdES(ETSI TS 102 778) | PAdES-Basic |
| | | PAdES-BES |
| | | PAdES-EPES |
| | | PAdES-LTV<br>(NOTE)DocumentTimeStamp を署名タイムスタンプとして利用する場合 |
| プロファイル | ETSI CAdES baseline profile | T-Level |
| | ETSI XAdES baseline profile | T-Level |
| | ETSI PAdES baseline profile | T-Level |
| | ISO 14533-1 | CAdES-T |
| | ISO 14533-2 | XAdES-T |

### 5.3.3 検証情報の参照付き署名(ES with validation data reference)

ES with validation data reference は ES with signature timestamp に検証情報の参照を格納した形式である。検証情報の参照のみを格納した CAdES-C や XAdES-C の形式と、検証情報の参照へタイムスタンプを付与した CAdES-X type1/type2 や XAdES-X type1/type2 の形式が定義されている。この規格では AdES-X type1/type2 のタイムスタンプをリファレンスタイムスタンプと呼ぶ。

ES with validation data reference の論理的な構造とこの規格の検証要件の各節との関係を図に示す。ES with validation data reference の仕様が記述された各規格の一覧を表 3 に示す。

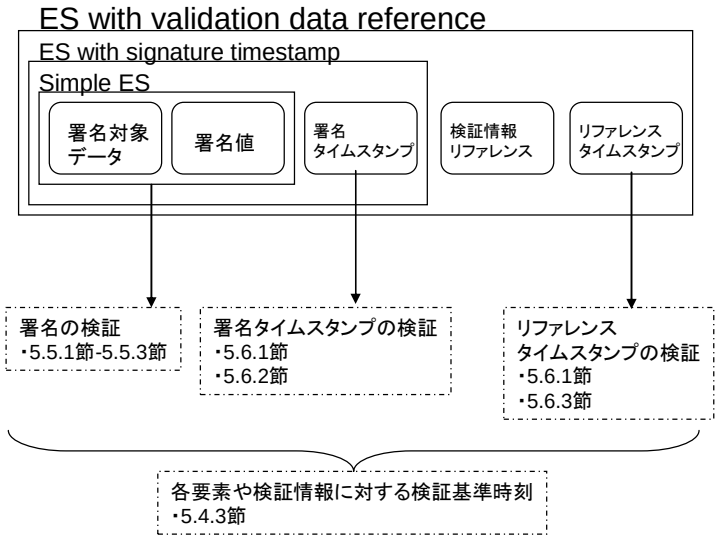


**図 10 ES with validation data reference の検証**

**表 3 ES with validation data reference の規格**

| 規格分類 | 規格種別 | 対象フォーマットタイプ |
|---|---|---|
| ベース規格 | CAdES(ETSI TS 101 733) | CAdES-C |
| | | CAdES-X type1 |
| | | CAdES-X type2 |
| | XAdES(ETSI TS 101 903) | XAdES-C |
| | | XAdES-X type1 |
| | | XAdES-X type2 |
| | PAdES(ETSI TS 102 778) | - |
| プロファイル | ETSI CAdES baseline profile | - |
| | ETSI XAdES baseline profile | - |
| | ETSI PAdES baseline profile | - |
| | ISO 14533-1 | - |

| | | |
|---|---|---|
| | ISO 14533-2 | - |

### 5.3.4 検証情報付き署名(ES with validation data)

ES with validation data は ES with signature timestamp または ES with validation data reference に検証情報を格納した形式である。格納された検証情報を用いて署名や署名タイムスタンプの検証を行うことができる。

ES with validation data の論理的な構造とこの規格の検証要件の各節との関係を図 11 ES with validation data の検証に示す。ES with validation data の仕様が記述された各規格の一覧を表 4 に示す。

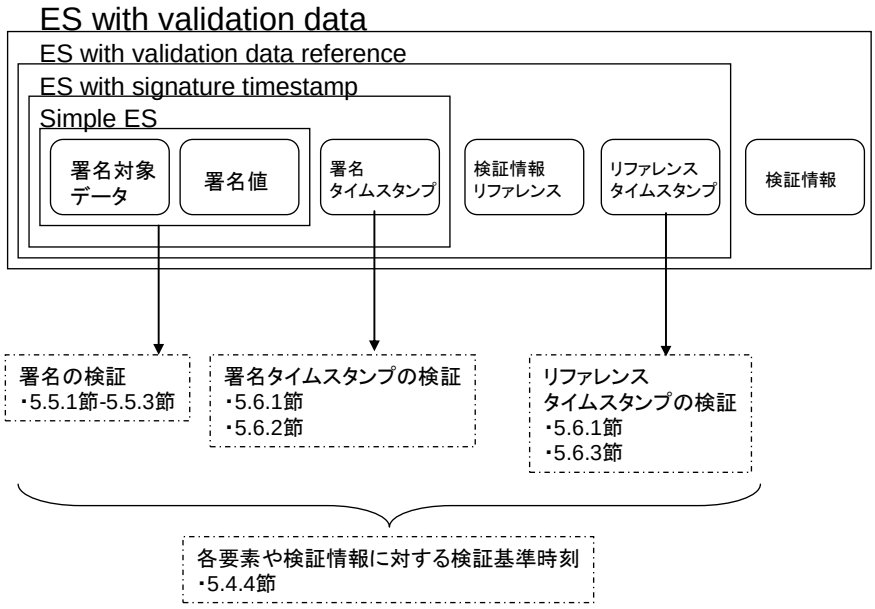


図 11 ES with validation data の検証

表 4 ES with validation data の規格

| 規格分類 | 規格種別 | 対象フォーマットタイプ |
|---|---|---|
| ベース規格 | CAdES(ETSI TS 101 733) | CAdES-X Long |
| | XAdES(ETSI TS 101 903) | XAdES-X Long |
| | PAdES(ETSI TS 102 778) | PAdES-LTV |
| プロファイル | ETSI CAdES baseline profile | LT-Level |
| | ETSI XAdES baseline profile | LT-Level |
| | ETSI PAdES baseline profile | LT-Level |
| | ISO 14533-1 | - |
| | ISO 14533-2 | - |

### 5.3.5 アーカイブ付き署名(ES with archive validation data)

ES with archive validation data は ES with validation data にアーカイブ用のタイムスタンプ(アーカイブタイムスタンプ、LongTermValidation タイムスタンプ、ドキュメントタイムスタンプ)を格納した形式である。ES with archive validation data の形式ではリファレンスタイムスタンプはオプションである。

ES with archive validation data の論理的な構造とこの規格の検証要件の各節との関係を図 11 ES with validation data の検証に示す。ES with archive validation data の仕様が記述された各規格の一覧を表 5 に示す。

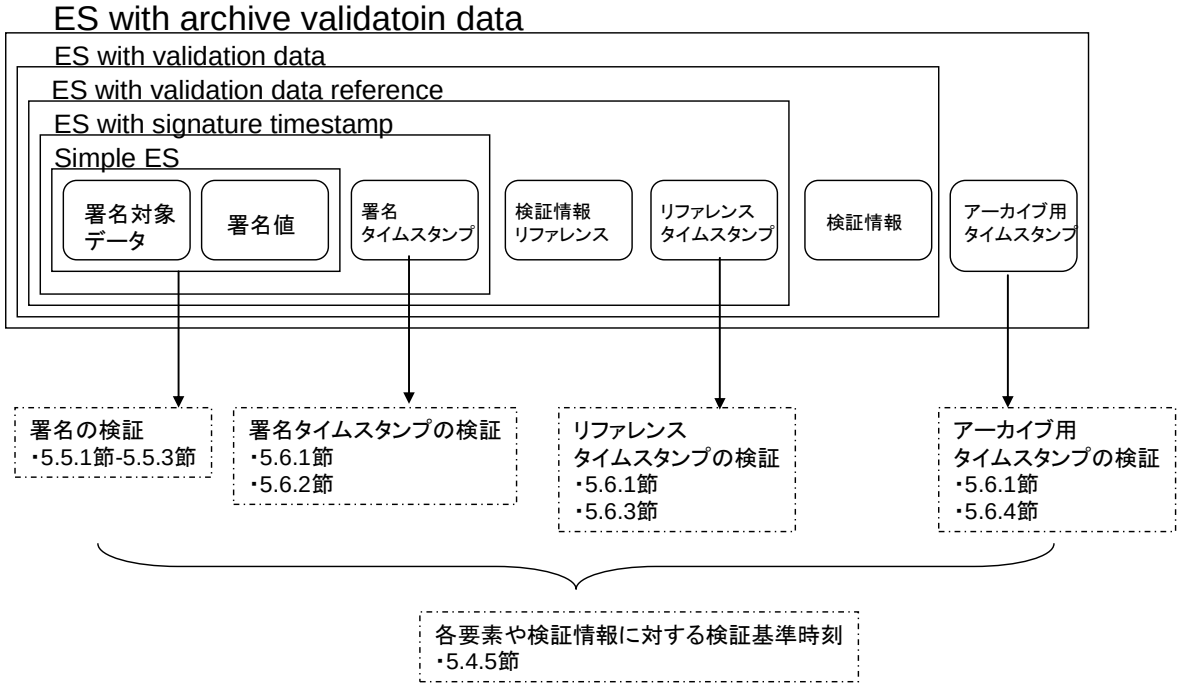


図 12 ES with archive validation data の検証

表 5 ES with archive validation data の規格

| 規格分類 | 規格種別 | 対象フォーマットタイプ |
|---|---|---|
| ベース規格 | CAdES(ETSI TS 101 733) | CAdES-A(archive timestamp) |
| | | long term validation タイムスタンプ |
| | XAdES(ETSI TS 101 903) | XAdES-A |
| | PAdES(ETSI TS 102 778) | PAdES-LTV |
| プロファイル | ETSI CAdES baseline profile | LTA-Level |
| | ETSI XAdES baseline profile | LTA-Level |
| | ETSI PAdES baseline profile | LTA-Level |
| | ISO 14533-1 | CAdES-A |

| | | |
|---|---|---|
| | ISO 14533-2 | XAdES-A |

### 5.4 検証基準時刻

署名データの有効性を判断する場合、署名やタイムスタンプ、証明書などの有効性を確認するときの基準となる時刻（検証基準時刻）が重要である。特に、長期保存の場合には複数のタイムスタンプが用いられていることで時刻の関係が複雑となり、不適切な検証基準時刻での検証を行った場合には、不正に生成された署名データを受け入れてしまう危険性もある。この節では、検証対象と検証基準時刻の関係を示す。

#### 5.4.1 Simple ES 検証における検証基準時刻

Simple ES の生成プロセスと検証プロセスの関係を図に示す。図の時間軸の上部に生成プロセスの過程を、時間軸の下部に検証プロセスの過程を示している。Simple ES では署名生成時刻が保証されないため、検証者が検証を行う時刻に基づき有効性を判断する。Simple ES 検証における検証基準時刻の考え方と有効性を判断すべき項目を表 6 に示す。

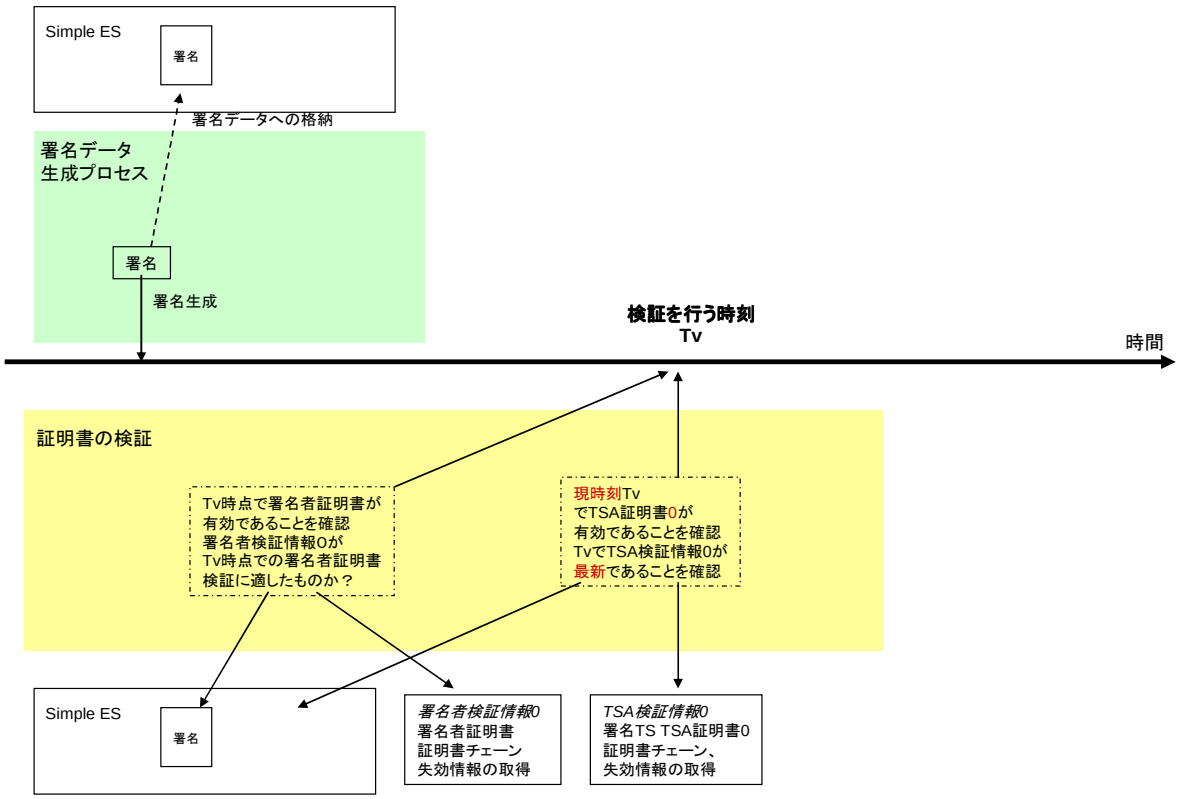


図 13 Simple ES 生成と検証の関係

表 6 Simple ES 検証における検証基準時刻の考え方

| 検証対象の分類 | 検証対象の項目 | 検証基準時刻の考え方 |
|---|---|---|
| 署名者による署名 | 署名生成に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられ |

| | | |
|---|---|---|
| | | るアルゴリズムや鍵長を使用していること |
| 署名者の証明書 | 認証パス上の証明書 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |

### 5.4.2 ES with signature timestamp 検証における検証基準時刻

ES with signature timestamp の生成プロセスと検証プロセスの関係を図に示す。図の時間軸の上部に生成プロセスの過程を、時間軸の下部に検証プロセスの過程を示している。ES with signature timestamp 検証における検証基準時刻の考え方と有効性を判断すべき項目を表 7 に示す。

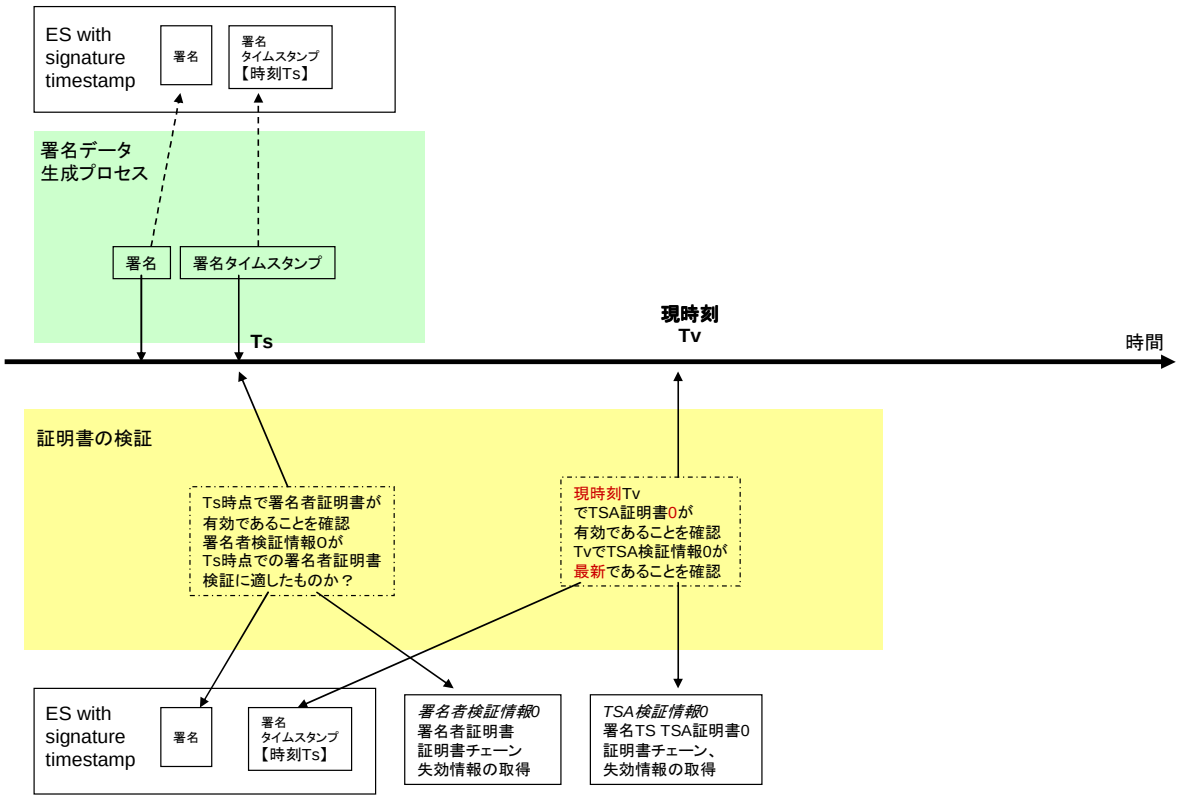


図 14 ES with signature timestamp 生成と検証の関係

表 7 ES with signature timestamp 検証における検証基準時刻の考え方

| 検証対象の分類 | 検証対象の項目 | 検証基準時刻の考え方 |
|---|---|---|
| 署名タイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |

| | | |
|---|---|---|
| 署名タイムスタンプを生成したタイムスタンプ局の証明書 | 認証パス上の証明書 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者による署名 | 署名生成に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者の証明書 | 認証パス上の証明書 | 署名タイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと<br>(NOTE)署名タイムスタンプが複数存在する場合には最も古い署名タイムスタンプの時刻を検証基準時刻とする。 |
| | 認証パス上の証明書に関する失効情報 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること |

| | | |
|---|---|---|
| | | ・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |

### 5.4.3 ES with validation data reference 検証における検証基準時刻

リファレンスタイムスタンプのない ES with validation data reference については ES with signature timestamp の検証基準時刻と同様に考える。リファレンスタイムスタンプが含まれる ES with validation data reference の生成プロセスと検証プロセスの関係を図に示す。図の時間軸の上部に生成プロセスの過程を、時間軸の下部に検証プロセスの過程を示している。リファレンスタイムスタンプが含まれる ES with validation data reference 検証における検証基準時刻の考え方と有効性を判断すべき項目を表 8 に示す。

ES with validation data reference の検証を行うとき、検証情報の参照情報を示した属性が検証に使用する証明書と失効情報と一致するか確認することもできる。

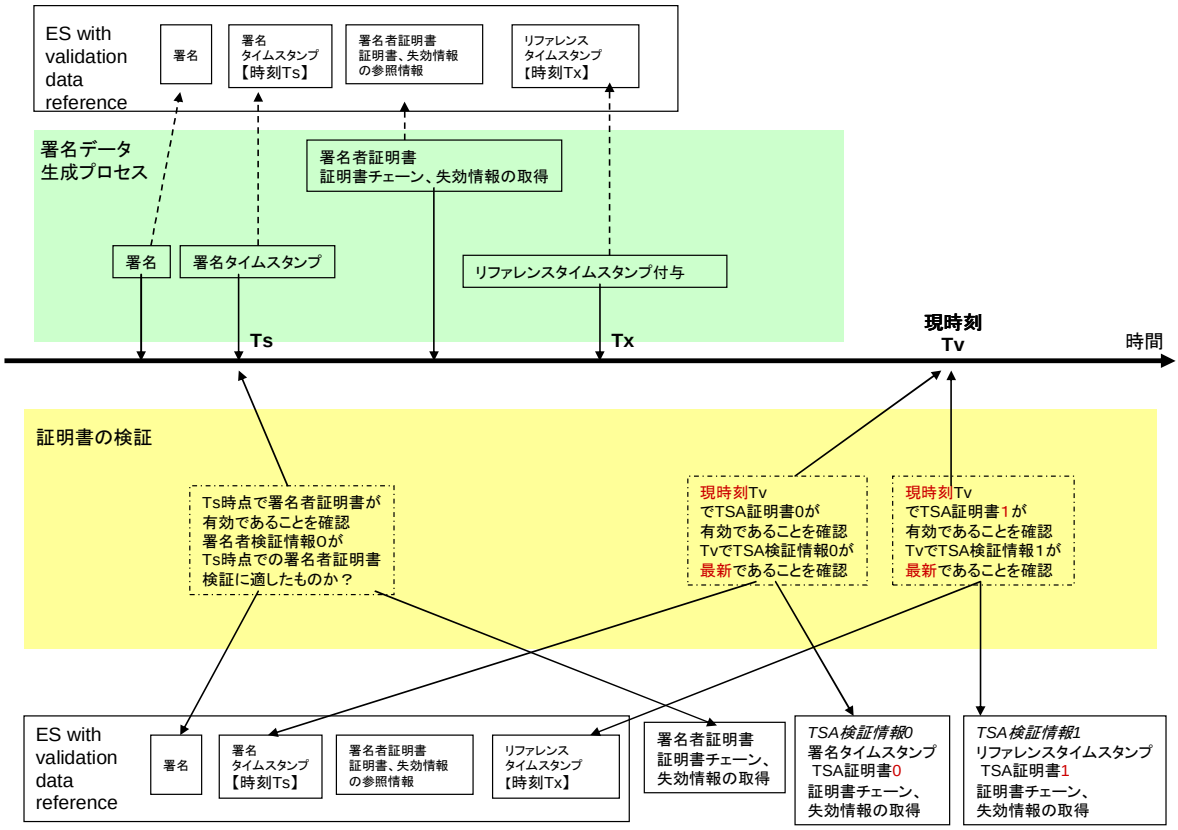


図 15 ES with validation data reference 生成と検証の関係

表 8 ES with validation data reference 検証における検証基準時刻の考え方

| 検証対象の分類 | 検証対象の項目 | 検証基準時刻の考え方 |
|---|---|---|
| リファレンスタイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |

| | | |
|---|---|---|
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| リファレンスタイムスタンプを生成したタイムスタンプ局の証明書 | 認証パス上の証明書 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 検証情報の参照情報の属性 | 参照情報に使用されているハッシュアルゴリズム | リファレンスタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| 署名タイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | リファレンスタイムスタンプの MessageImprint の対象に署名タイムスタンプが含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリ | リファレンスタイムスタンプの MessageImprint の対象に署名タイムスタンプ |

| | | |
|---|---|---|
| | ズム、鍵長 | が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名タイムスタンプを生成したタイムスタンプ局の証明書 | 認証パス上の証明書 | 検証情報の参照情報に証明書が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証情報の参照情報に失効情報が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証情報の参照情報に証明書や失効情報が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者による署名 | 署名生成に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 署名値を MessageImprint の対象に含んでいる最も古いタイムスタンプ検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者の証明書 | 認証パス上の証明書 | 署名タイムスタンプの時刻を検証基準時刻とし |

| | | |
|---|---|---|
| | | て以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証情報の参照情報に失効情報が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 検証情報の参照情報に証明書や失効情報が含まれる場合にはリファレンスタイムスタンプの時刻を、それ以外の場合には検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |

### 5.4.4 ES with validation data 検証における基準時刻

ES with validation data は署名データ内に格納された証明書や失効情報を用いて検証を行うことができる。検証基準時刻については ES with signature timestamp や ES with validation data reference と同様に考える。

### 5.4.5 ES with archive validation data 検証における基準時刻

ES with archive validation data の生成プロセスと検証プロセスの関係を図に示す。図の時間軸の上部に生成プロセスの過程を、時間軸の下部に検証プロセスの過程を示している。ES with archive validation data 検証における検証基準時刻の考え方と有効性を判断すべき項目を表 9 に示す。

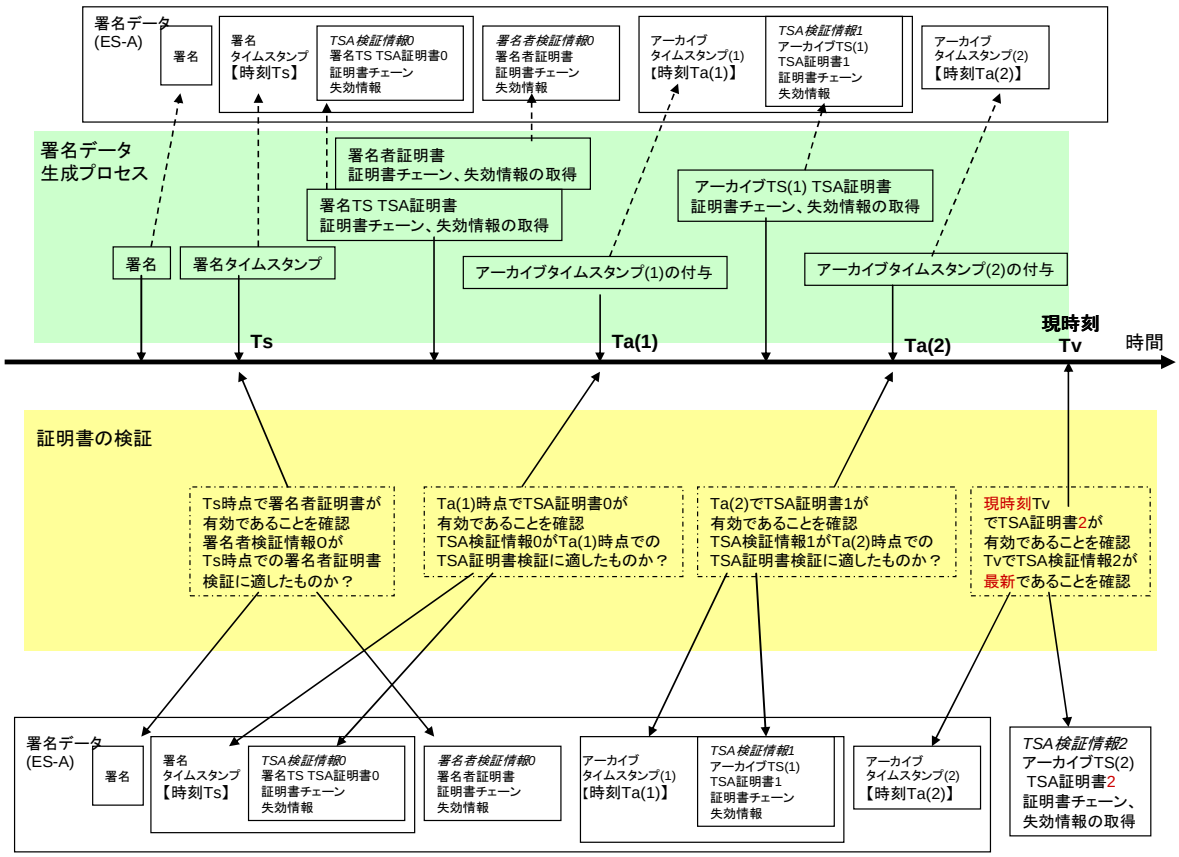


図 16 ES with archive validation data 生成と検証の関係

表 9 ES with archive validation data 検証における検証基準時刻の考え方

| 検証対象の分類 | 検証対象の項目 | 検証基準時刻の考え方 |
|---|---|---|
| 最新のアーカイブタイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |

| | | |
|---|---|---|
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 最新のアーカイブタイムスタンプを生成したタイムスタンプ局の証明書 | 認証パス上の証明書 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 過去のアーカイブタイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | このアーカイブタイムスタンプをMessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | このアーカイブタイムスタンプをMessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 過去のアーカイブ | 認証パス上の証明書 | このアーカイブタイムスタンプを |

| | | |
|---|---|---|
| タイムスタンプを生成したタイムスタンプ局の証明書 | | MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | このアーカイブタイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | このアーカイブタイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| リファレンスタイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | このタイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | このタイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| リファレンスタイムスタンプを生成 | 認証パス上の証明書 | 証明書を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻 |

| | | |
|---|---|---|
| したタイムスタンプ局の証明書 | | として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 失効情報を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 証明書や失効情報を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名タイムスタンプのタイムスタンプトークン | タイムスタンプ対象（MessageImprint）に使用されているハッシュアルゴリズム | 署名タイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムを使用していること |
| | 署名生成に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 署名タイムスタンプを MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名タイムスタンプを生成したタイムスタンプ局の証明書 | 認証パス上の証明書 | 証明書を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されてい |

| | | |
|---|---|---|
| | | ないこと |
| | 認証パス上の証明書に関する失効情報 | 失効情報を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、猶予期間など） |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズム、署名アルゴリズム、鍵長 | 証明書や失効情報を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者による署名 | 署名生成に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 署名値を MessageImprint の対象に含んでいる最も古いタイムスタンプ検証を行う時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |
| 署名者の証明書 | 認証パス上の証明書 | 署名タイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・証明書の有効期間内に検証基準時刻があること<br>・証明書が検証基準時刻において失効されていないこと |
| | 認証パス上の証明書に関する失効情報 | 証明書を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・失効情報発行者の証明書の有効期間内に検証基準時刻があること<br>・失効情報発行者の証明書が検証基準時刻において失効されていないこと<br>・失効情報の発行日時が検証基準時刻と比較して許容できるものであること（失効情報の鮮度、 |

| | | |
|---|---|---|
| | | 猶予期間など) |
| | 認証パス上の証明書や失効情報に使用されているハッシュアルゴリズムや署名アルゴリズム、鍵長 | 証明書や失効情報を MessageImprint の対象に含んでいる最も古いタイムスタンプの時刻を検証基準時刻として以下の確認を行う。<br>・検証基準時刻において安全であると考えられるアルゴリズムや鍵長を使用していること |

### 5.5 署名の検証要件

もし ES がアーカイブ情報を有している場合には、検証基準時刻として最も古いタイムスタンプ時刻を利用する。それ以外の場合には、検証基準時刻として有効な検証時刻または現在時刻を利用する。詳しくは 5.4 を参照。

#### 5.5.1 アルゴリズムの有効性の確認

検証制約により、検証基準時刻において利用している暗号アルゴリズムの脆弱性が見つかっておらず有効であることを確認する。

**表 10 検証要件（アルゴリズムの有効性）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| 暗号アルゴリズム | ダイジェストアルゴリズム | 検証基準時刻においてアルゴリズムの脆弱性が見つかっていないこと | M | VALID | ・判定結果 |
| | | | | INVALID | ・検証基準時刻<br>・脆弱化した時刻<br>・脆弱性の内容 |
| | 署名アルゴリズムおよび鍵長 | 検証基準時刻においてアルゴリズムまたは鍵長の脆弱性が見つかっていないこと | M | VALID | ・判定結果 |
| | | | | INVALID | ・検証基準時刻<br>・脆弱化した時刻<br>・脆弱性の内容 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

#### 5.5.2 CAdES の検証要件

CAdES 署名は、基準時刻において次の検証要件に従い検証する。

**表 11 検証要件（CAdES 署名）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| データ構造 | データ構造の正当性確認 | データ構造が表 12 の必須構成要素を満たしていること | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由<br>・ 不足要素 |
| | CMS データ形式の確認 | ContentType が signed-data のオブジェクト識別子であること | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由 |

| | | | | | |
|---|---|---|---|---|---|
| 署名者証明書 | 署名者証明書のパス構築とパス検証 | 5.7.1 の署名者証明書の検証要件に従って検証できること | M | 5.7.1 を参照 | |
| 署名 | digestAlgorithms フィールドの有効性確認 | Content の digestAlgorithms フィールドが 5.5.1 のダイジェストアルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | digestAlgorithm フィールドの有効性確認 | signerInfo の digestAlgorithm フィールドが 5.5.1 のダイジェストアルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | MessageDigest 属性の一致確認 | signerInfo において、次の 2 つの値が一致すること<br>1) digestAlgorithm フィールドで指定されたアルゴリズムで算出した eContent の値に対するハッシュ値<br>2) signedAttrs フィールドの MessageDigest の値 | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由<br>・ 各ハッシュ値 |
| | sid フィールドと署名者証明書の一致確認 | sid フィールドにおける次のいずれかの要素が署名者証明書の該当項目と一致すること<br>1) issuerAndSerialNumber の発行者とシリアル番号<br>2) subjectKeyIdentifier の主体者公開鍵識別子 | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由<br>・ 不一致内容 |

| | | | | | |
|---|---|---|---|---|---|
| | SigningCertificate 属性における署名者証明書のハッシュ値の一致確認 | 次の 2 つの値が一致すること<br>1) SigningCertificate 属性のアルゴリズムで算出した署名者証明書のハッシュ値<br>2) SigningCertificate 属性に含まれるハッシュ値 | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由<br>・ 各ハッシュ値 |
| | SigningCertificate 属性における発行者識別情報の一致確認 | SigningCertificate 属性の issuerSerial の発行者識別名とシリアル番号が署名者証明書の該当項目と一致すること | E | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由<br>・ 不一致内容 |
| | signatureAlgorithm フィールドの有効性確認 | signerInfo の signatureAlgorithm フィールドが 5.5.1 の署名アルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | 署名者証明書（公開鍵）による署名値の有効性確認 | signerInfo の signatureAlgorithm と digestAlgorithm で指定されたアルゴリズムに従い、署名者証明書より取得した公開鍵で、signerInfo の署名値と signedAttrs のハッシュ値の整合性が確認できること | M | VALID | ・ 判定結果 |
| | | | | INVALID | ・ 判定理由 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

**表 11 署名データの構成要素（CAdES）**

| ASN.1 表記 | 要素 | M/O | | |
|---|---|---|---|---|
| | | ES | ES-T | ES-A |
| ContentType | コンテント種別 | M | M | M |
| Content | コンテント | M | M | M |

| | | | | |
|---|---|---|---|---|
| CMSVersion | 暗号メッセージ構文の版数 | M | M | M |
| DigestAlgorithmIdentifiers | ダイジェストアルゴリズム識別子群 | M | M | M |
| EncapsulatedContentInfo | カプセル構造化されたコンテント情報 | M | M | M |
| eContentType | e コンテント種別 | M | M | M |
| eContent | e コンテント | O | O | O |
| CertificateSet (Certificates) | 証明書群 | O | O | O |
| Certificate | 証明書 | O | O | O |
| AttributeCertificateV2 | 属性証明書 2 版 | O | O | O |
| OtherCertificateFormat | その他形式の証明書 | O | O | O |
| RevocationInfoChoices (crls) | 失効情報群 | O | O | O |
| CertificateList | 失効情報 | O | O | O |
| OtherRevocationInfoFormat | その他形式の失効情報 | O | O | O |
| SignerInfos | 署名者情報群 | M | M | M |
| CMSVersion | 暗号メッセージ構文の版数 | M | M | M |
| SignerIdentifier | 署名者識別子 | M | M | M |
| IssuerAndSerialNumber | 発行者及びシリアル番号 | O | O | O |
| SubjectKeyIdentifier | 対象者鍵識別子 | O | O | O |
| DigestAlgorithmIdentifier | ダイジェストアルゴリズム識別子 | M | M | M |
| SignedAttributes | 署名属性群 | M | M | M |
| ContentType | コンテント種別 | M | M | M |
| MessageDigest | メッセージダイジェスト | M | M | M |
| SigningCertificateReference | 署名者証明書の参照情報 | M | M | M |
| ESSSigningCertificate | ESS 署名者証明書の参照情報 | O | O | O |
| ESSSigningCertificateV2 | ESS 署名者証明書の参照情報 2 版 | O | O | O |
| OtherSigningCertificate | 他の署名者証明書の参照情報 | O | O | O |
| SignatgurePolicyIdentifier | 署名ポリシ識別子 | O | O | O |
| SigningTime | 署名時刻 | O | O | O |
| ContentReference | コンテント参照情報 | O | O | O |
| ContentIdentifier | コンテント識別子 | O | O | O |
| ContentHint | コンテントのヒント | O | O | O |
| CommitmentTypeIndication | コミットメント識別表示 | O | O | O |

| | | | | | |
|---|---|---|---|---|---|
| SignerLocation | 署名者所在地 | O | O | O |
| SignerAttribute | 署名者の属性情報 | O | O | O |
| ContentTimestamp | コンテントタイムスタンプ | O | O | O |
| SignatureAlgorithm | 署名アルゴリズム識別子 | M | M | M |
| SignatureValue | 署名値 | M | M | M |
| UnsignedAttributes | 非署名属性群 | O | M | M |
| CounterSignature | カウンタ署名 | - | O | O |
| | 署名時刻を確定する情報 | - | M | M |
| SignatureTimestamp | 署名タイムスタンプ | - | O | O |
| | タイムマークなどその他の方式 | - | O | O |
| CompleteCertificateRefs | 全証明書参照情報群 | - | - | M |
| CompleteRevocationRefs | 全失効参照情報群 | - | - | M |
| CompleteRevRefs CRL | CRL 形式の失効参照情報群 | - | - | O |
| CompleteRevRefs OCSP | OCSP 形式の失効参照情報群 | - | - | O |
| OtherRevRefs | 他の形式の失効参照情報群 | - | - | O |
| Attribute certificate references | 属性証明書の参照情報群 | - | - | O |
| Attribute revocation references | 属性失効情報の参照情報群 | - | - | O |
| CertificateValues | 証明書群 | - | - | M |
| CertificateValues | 証明書 | - | - | O |
| | CA 等による証明書の保管 | - | - | O |
| RevocationValues | 失効情報群 | - | - | M |
| CertificateList | CRL による失効情報 | - | - | O |
| BasicOCSPResponse | 基本 OCSP 応答 | - | - | O |
| OtherRevVals | 他の失効情報 | - | - | O |
| | CA 等による失効情報の保管 | - | - | O |
| CAdES-C-timestamp | CAdES-C データへのタイムスタンプ | - | - | O |
| Time-stamped cert and crls reference | タイムスタンプが付与された証明書及び失効情報に関する参照情報 | - | - | O |
| | 改ざん検知を可能とする情報 | - | - | M |
| ArchiveTimestampV2 | アーカイブタイムスタンプ id-aa-48 | - | - | O |
| ArchiveTimestamp | アーカイブタイムスタンプ id-aa-27 | - | - | O |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | Long Term Validation タイムスタンプ | - | - | O |
| | | | | | タイムマークなどその他の方式 | - | - | O |

M/O: **M**andatory/**O**ptional

### 5.5.3 XAdES の検証要件

XAdES 署名は、基準時刻において次の検証要件に従い検証する。

**表 13 検証要件**（XAdES 署名）

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| 署名構造 | XAdES 必須要素 | 表 14 の必須要素が含まれるか参照されていること | M | VALID | ・判定結果 |
| | | | | INVALID | ・含まれていない必須要素 |
| | SignedProperties 要素 | SignedProperties を参照する Reference 要素が存在し Type 属性が正しくセットされていること | M | VALID | ・判定結果 |
| | | | | INVALID | ・不正内容 |
| オプション要素 | XAdES-BES オプション要素 | XAdES-BES に含まれる以下のオプション要素が正しく使われていること<br>・SigningTime 要素<br>・SignerRole 要素<br>・SignatureProductionPlace 要素 | O | VALID | ・判定結果<br>・オプション情報 |
| | | | | INVALID | ・不正内容<br>・不正項目の情報 |
| | XAdES-EPES オプション要素 | XAdES-EPES に含まれる SignaturePolicyIdentifier があれば検証して正しいことを確認すること | O | VALID | ・判定結果 |
| | | | | INVALID | ・不正内容 |
| 署名者証明書 | 署名者証明書の指定確認 | 次のどちらかで署名者証明書が指定されていること<br>1) SigningCertificate 要素<br>2) Reference 要素で参照されている KeyInfo 要素 | M | VALID | ・判定結果 |
| | | | | INVALID | ・不正内容 |
| | 署名者証明書 | CertificateValues 要素か | M | VALID | ・判定結果 |

| | | | | | |
|---|---|---|---|---|---|
| | の実体確認 | KeyInfo 要素または検証要件により署名者証明書の実体が確認できること | | INVALID | ・不正内容 |
| | 署名者証明書の一致確認 | 署名者証明書の参照と実体が一致していること<br>1) SigningCertificate 要素の IssuerSerial 要素と署名者証明書の Issuer と Serial Number が一致していること<br>2) SigningCertificate 要素の DigestValue 要素と署名者証明書のハッシュ値が一致していること<br>3) KeyInfo 要素に X509IssuerSerial 要素がある場合に署名者証明書の Issuer と Serial Number が一致していること<br>※ SigningCertificate 要素に署名者証明書の認証パス構築に必要ない証明書が指定されている場合には失敗とすべき | M | VALID | ・判定結果<br>・証明書情報 |
| | | | | INVALID | ・不正内容<br>・証明書情報<br>・DigestValue 要素<br>・Issuer と Serial Number 要素 |
| | 署名者証明書のパス構築とパス検証 | 5.7.1 の署名者証明書の検証要件に従って検証すること | M | 5.7.1 を参照 | |
| 参照データ | Reference 要素 | 次に 2 つの値が一致すること<br>1) Reference 要素により参 | M | VALID | ・判定結果<br>・全参照 URL |

| | | | | | |
|---|---|---|---|---|---|
| | | 照されている対象を、Transforms 要素があれば正規化を行った上で DigestMethod 要素により指定されたダイジェストアルゴリズムに従ってハッシュ値を計算した値<br>2) DigestValue 要素の値 | | INVALID | ・不正参照 URI<br>・計算ハッシュ値<br>・DigestMethod 要素<br>・DigestValue 要素の値 |
| | DigestMethod 要素 | 5.5.1 のダイジェストアルゴリズムの有効性に従って検証すること | M | 5.5.1 を参照 | |
| 署名データ | SignatureValue 要素 | SignedInfo 要素を CanonicalizationMethod に従って正規化をおこなった結果と署名者証明書の公開鍵を使い、SignatureMethod で指定された署名アルゴリズムにより、SignatureValue 要素の整合性が確認できること | M | VALID | ・判定結果 |
| | | | | INVALID | ・不正内容<br>・CanonicalizationMethod 要素<br>・SignatureMethod 要素 |
| | SignatureMethod 要素の有効性確認 | 5.5.1 の署名アルゴリズムの有効性に従って検証すること | M | 5.5.1 を参照 | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

**表 14 署名データの構成要素（XAdES）**

| XML 表記 | 要素 | M/O | | |
|---|---|---|---|---|
| | | ES | ES-T | ES-A |
| ds:Signature | 署名 | M | M | M |
| Id | Signature 要素 Id 属性 | M | M | M |
| ds:SignedInfo | 署名に関する情報 | M | M | M |
| ds:CanonicalizationMethod | 正規化方式 | M | M | M |
| ds:SignatureMethod | 署名方式 | M | M | M |
| ds:Reference | コンテント参照情報 | M | M | M |
| ds:Transforms | 変換処理 | E | E | E |
| ds:DigestMethod | ダイジェスト方式 | M | M | M |

| | | | | | |
|---|---|---|---|---|---|
| ds:DigestValue | ダイジェスト値 | M | M | M |
| ds:SignatureValue | 署名値 | M | M | M |
| ds:KeyInfo | 鍵情報 | O (a) | O (a) | O (a) |
| ds:Object | オブジェクト | M | M | M |
| xa:QualifyingProperties | 署名修飾プロパティ | M | M | M |
| xa:SignedProperties | 署名対象プロパティ | M | M | M |
| xa:SignedSignatureProperties | 署名対象の署名プロパティ | M | M | M |
| xa:SigningTime | 署名時刻 | O | O | O |
| xa:SigningCertificate | 署名者証明書の参照情報 | O (a) | O (a) | O (a) |
| xa:SignaturePolicyIdentifier | 署名ポリシ識別子 | O | O | O |
| xa:SignatureProductionPlace | 署名生成場所 | O | O | O |
| xa:SignerRole | 署名者の肩書 | O | O | O |
| xa:SignedDataObjectProperties | 署名対象データオブジェクトのプロパティ | O | O | O |
| xa:DataObjectFormat | データオブジェクト形式 | O | O | O |
| xa:CommitmentTypeIndication | コミットメント種別表示 | O | O | O |
| xa:AllDataObjectsTimeStamp | 全データオブジェクトに対するタイムスタンプ | O | O | O |
| xa:InvalidualDataObjectsTimeStamp | 個別データオブジェクトに対するタイムスタンプ | O | O | O |
| xa:UnsignedProperties | 非署名対象プロパティ | - | M | M |
| xa:UnsignedSignatureProperties | 非署名対象署名プロパティ | - | M | M |
| xa:CounterSignature | カウンタ署名 | - | O | O |
| xa:SignatureTimeStamp | 署名タイムスタンプ | - | M | M |
| xa141:TimeStampValidationData | 署名タイムスタンプ証明書群及び失効情報群（V1.4.1） | - | O | O (b) |
| xa:CompleteCertificateRefs | 全証明書参照情報群 | - | O | O |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | xa:CompleteRevocationRefs | 全失効情報参照情報群 | - | O | O |
| | | | | xa:AttributeCertificateRefs | 属性証明書参照情報群 | - | O | O |
| | | | | xa:AttributeRevocationRefs | 属性失効情報参照情報群 | - | O | O |
| | | | | xa:SigAndRefsTimeStamp | 署名及び参照情報に対するタイムスタンプ | - | O | O |
| | | | | xa:RefsOnlyTimeStamp | 参照情報に対するタイムスタンプ | - | O | O |
| | | | | xa:CertificateValues | 証明書群（署名者証明書） | - | O | M |
| | | | | xa:RevocationValues | 失効情報群（署名者証明書） | - | O | M |
| | | | | xa:AttrAuthoritiesCertValues | 属性証明書群 | - | O | O |
| | | | | xa:AttributeRevocationValues | 属性失効情報群 | - | O | O |
| | | | | *Archiving information* | *アーカイブ情報* | - | - | M |
| | | | | | xa:ArchiveTimeStamp | アーカイブタイムスタンプ | - | - | O |
| | | | | | xa141:ArchiveTimeStamp | アーカイブタイムスタンプ（V1.4.1） | - | - | O |
| | | | | | xa141:TimeStampValidationData | アーカイブタイムスタンプ証明書群及び失効情報群（V1.4.1） | - | - | O (c) |
| | | | xa:UnsignedDataObjectProperties | | | 非署名のデータオブジェクトのプロパティ群 | - | - | O |
| | | | | xa:UnsignedDataObjectPropertie | | 非署名のデータオブジェクトのプロパティ | - | - | O |
| | | xa:QualifyingPropertiesReference | | | | 署名修飾プロパティの参照情報 | - | - | O |

本表における XML 名前空間
xmlns:ds="http://www.w3.org/2000/09/xmldsig#
xmlns:xa="http://uri.etsi.org/01903/v1.3.2#
xmlns:xa141="http://uri.etsi.org/01903/v1.4.1#

(a) 署名者証明書は xa:SigningCertificate または ds:Reference 要素で参照された ds:KeyInfo のいずれかにおいて指定すること。

(b) 署名タイムスタンプの証明書群と検証情報群は xa141:TimeStampValidationData を使わない場合には、署名者証明書用の xa:CertificateValues と xa:RevocationValues に入れるか、タイムスタンプトークン自体に埋め込むこと。

| |
|---|
| (c) アーカイブタイムスタンプの証明書群と検証情報群は xa141:TimeStampValidationData を使わない場合には、タイムスタンプトークン自体に埋め込むこと。 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

## 5.6 タイムスタンプの検証要件

### 5.6.1 タイムスタンプ

タイムスタンプは、次の検証要件に従い検証する。

**表 15 検証要件（タイムスタンプ）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| データ構造 | データ構造の正当性確認 | データ構造が表 16 の必須構成要素を満たしていること | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由<br>・不足要素 |
| | CMS データ形式の確認 | ContentType が signed-data の識別子であること | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由 |
| | 署名対象データ形式の確認 | eContentType が TSTInfo のオブジェクト識別子であること | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由 |
| TSA 証明書 | TSA 証明書のパス構築とパス検証 | 5.7.2 の TSA 証明書の検証要件に従って検証 | M | 5.7.2 を参照 | |
| TSA の署名 | digestAlgorithms フィールドの有効性確認 | Content の digestAlgorithms フィールドが 5.5.1 のダイジェストアルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | digestAlgorithm フィールドの有効性確認 | signerInfo の digestAlgorithm フィールドが 5.5.1 のダイジェストアルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | MessageDigest 属性 | signerInfo において、次の | M | VALID | ・判定結果 |

| | | | | | |
|---|---|---|---|---|---|
| | の一致確認 | 2 つの値が一致すること<br>1) digestAlgorithm フィールドで指定されたアルゴリズムで算出した eContent の値に対するハッシュ値<br>2) signedAttrs フィールドの MessageDigest の値 | | INVALID | ・判定理由<br>・各ハッシュ値 |
| | SigningCertificate 属性における TSA 証明書のハッシュ値の一致確認 | 次の 2 つの値が一致すること<br>3) SigningCertificate 属性のアルゴリズムで算出した TSA 証明書のハッシュ値<br>4) SigningCertificate 属性に含まれるハッシュ値 | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由<br>・各ハッシュ値 |
| | signatureAlgorithm フィールドの有効性確認 | signerInfo の signatureAlgorithm フィールドが 5.5.1 の署名アルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | TSA 証明書(公開鍵)による署名値の有効性確認 | signerInfo の signatureAlgorithm と digestAlgorithm で指定されたアルゴリズムに従い、TSA 証明書より取得した公開鍵で、signerInfo の署名値と signedAttrs のハッシュ値の整合性が確認できること | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由 |

| | | | | | |
|---|---|---|---|---|---|
| タイムスタンプ対象データ | hashAlgorithm フィールドの有効性確認 | eContent(TSTInfo) における MessageImprint の hashAlgorithm フィールドが 5.5.1 のダイジェストアルゴリズムの検証要件に従って検証できること | M | 5.5.1 を参照 | |
| | タイムスタンプ対象データとの整合性確認 | eContent(TSTInfo) において、次の 2 つの値が一致すること<br>1) MessagaeImprint の hashAlgorithm フィールドで指定されたアルゴリズムで算出したタイムスタンプ対象データのハッシュ値<br>2) MessagaeImprint の hashMessage の値 | M | VALID | ・判定結果 |
| | | | | INVALID | ・判定理由<br>・各ハッシュ値 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

**表 16 タイムスタンプトークンデータの構成要素**

| ASN.1 表記 | 要素 | M/O | 備考 |
|---|---|---|---|
| ContentType | コンテント種別 | M | |
| Content | コンテント | M | |
| CMSVersion | 暗号メッセージ構文の版数 | M | |
| DigestAlgorithmIdentifiers | ダイジェストアルゴリズム識別子群 | M | |
| EncapsulatedContentInfo | カプセル構造化されたコンテント情報 | M | |
| eContentType | e コンテント種別 | M | TSTInfo のオブジェクト識別子 |
| eContent | e コンテント | M | TSTInfo |
| version | タイムスタンプトークンのフォーマットバージョン | M | |
| TSAPolicyId | サービスポリシーの識別子 | M | |

| | | | | |
|---|---|---|---|---|
| | | MessageImprint | タイムスタンプ対象のハッシュ情報 | M | |
| | | hashAlgorithm | ハッシュアルゴリズムの識別子 | M | |
| | | hashedMessage | ハッシュ値 | M | |
| | | serialNumber | タイムスタンプトークンのシリアル番号 | M | |
| | | genTime | タイムスタンプトークン生成時刻情報 | M | |
| | | Accuracy | 時刻精度 | O | |
| | | Ordering | タイムスタンプトークン発行の順序性の有無 | M | |
| | | Nonce | 乱数 | O | |
| | | tsa | タイムスタンプユニットの識別情報 | O | |
| | | extensions | 拡張領域 | O | |
| | CertificateSet (Certificates) | | 証明書群 | O | |
| | Certificate | | 証明書 | O | |
| | AttributeCertificateV2 | | 属性証明書 2 版 | O | |
| | OtherCertificateFormat | | その他形式の証明書 | O | |
| | RevocationInfoChoices (crls) | | 失効情報群 | O | |
| | CertificateList | | 失効情報 | O | |
| | OtherRevocationInfoFormat | | その他形式の失効情報 | O | |
| | SignerInfos | | 署名者情報群 | M | |
| | CMSVersion | | 暗号メッセージ構文の版数 | M | |
| | SignerIdentifier | | 署名者識別子 | M | |
| | | IssuerAndSerialNumber | 発行者及びシリアル番号 | O | |
| | | SubjectKeyIdentifier | 対象者鍵識別子 | O | |
| | DigestAlgorithmIdentifier | | ダイジェストアルゴリズム識別子 | M | |
| | SignedAttributes | | 署名属性群 | M | |
| | | ContentType | コンテント種別 | M | TSTInfo のオブジェクト識別子 |
| | | MessageDigest | メッセージダイジェスト | M | |
| | | SigningCertificateReference | 署名者証明書の参照情報 | M | |
| | | ESSSigningCertificate | ESS 署名者証明書の参照情報 | O | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | ESSSigningCertificateV2 | ESS 署名者証明書の参照情報 2 版 | O | |
| | | | | OtherSigningCertificate | 他の署名者証明書の参照情報 | O | |
| | | SignatureAlgorithm | | | 署名アルゴリズム識別子 | M | |
| | | SignatureValue | | | 署名値 | M | |
| | | UnsignedAttributes | | | 非署名属性群 | O | |
| | | | CompleteCertificateRefs | | 全証明書参照情報群 | O | |
| | | | CompleteRevocationRefs | | 全失効参照情報群 | O | |
| | | | | CompleteRevRefs CRL | CRL 形式の失効参照情報群 | O | |
| | | | | CompleteRevRefs OCSP | OCSP 形式の失効参照情報群 | O | |
| | | | CertificateValues | | 証明書群 | O | |
| | | | | CertificateValues | 証明書 | O | |
| | | | | | CA 等による証明書の保管 | O | |
| | | | RevocationValues | | 失効情報群 | O | |
| | | | | CertificateList | CRL による失効情報 | O | |
| | | | | BasicOCSPResponse | 基本 OCSP 応答 | O | |
| | | | | OtherRevVals | 他の失効情報 | O | |

M/O: **M**andatory/**O**ptional

### 5.6.2 署名タイムスタンプ

署名タイムスタンプの検証基準時刻

もし ES がアーカイブ情報を有している場合には、検証基準時刻として最も古いタイムスタンプ時刻を利用する。それ以外の場合には、検証基準時刻として有効な検証時刻または現在時刻を利用する。詳しくは 5.4 を参照。

署名タイムスタンプの検証要件

署名タイムスタンプを、検証基準時刻において次の検証要件に従い検証する。

**表 17 検証要件（署名タイムスタンプ）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| タイムスタンプトークン | タイムスタンプトークンの検証 | 5.6.1 のタイムスタンプ検証要件に従って検証すること | M | 5.6.1 参照 | |
| タイムスタンプの MessageImprint 値 | 署名タイムスタンプの MessageImprint（ハッシュ）値 | 署名タイムスタンプのハッシュ値と、計算値を比較して一致すること<br>CAdES は表 18 参照<br>XAdES は表 19 参照 | M | VALID | ・判定結果 |
| | | | | INVALID | ・タイムスタンプ MessageImprint 値<br>・計算したハッシュ値<br>・ダイジェストアルゴリズム |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

**表 18 CAdES 署名タイムスタンプ対象データのハッシュ算出手段**

| CAdES 署名タイムスタンプ対象データのハッシュ算出手段 |
|---|
| signerInfo における signature（署名値）に対してハッシュ値を算出する |

**表 19 XAdES 署名タイムスタンプ対象データのハッシュ算出手段**

| XAdES 署名タイムスタンプ対象データのハッシュ算出手段 |
|---|
| ds:SignatureValue（署名値）要素に対して正規化した上でハッシュ値を算出する |

### 5.6.3 リファレンスタイムスタンプ

#### 5.6.3.1 リファレンスタイムスタンプの検証基準時刻

もし ES がアーカイブ情報を有している場合には、検証基準時刻として最も古いタイムスタンプ時刻を利用する。それ以外の場合には、検証基準時刻として有効な検証時刻または現在時

刻を利用する。詳しくは 5.4 を参照。

#### 5.6.3.2 リファレンスタイムスタンプの検証要件

リファレンスタイムスタンプを、検証基準時刻において次の検証要件に従い検証する。

**表 20 検証要件（リファレンスタイムスタンプ）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| タイムスタンプトークン | タイムスタンプトークンの検証 | 5.6.1 のタイムスタンプ検証要件に従って検証すること | M | 5.6.1 参照 | |
| タイムスタンプの MessageImprint 値 | リファレンスタイムスタンプの MessageImprint（ハッシュ）値 | リファレンスタイムスタンプのハッシュ値と、計算値を比較して一致すること<br>CAdES は表 21 参照<br>XAdES は表 22 参照 | M | VALID | ・判定結果 |
| | | | | INVALID | ・タイムスタンプ MessageImprint 値<br>・計算したハッシュ値<br>・ダイジェストアルゴリズム |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

**表 21 CAdES リファレンスタイムスタンプ対象データのハッシュ算出手段**

| CAdES リファレンスタイムスタンプ対象データのハッシュ算出手段 |
|---|
| ※ TBD (to be determined) |

**表 22 XAdES リファレンスタイムスタンプ対象データのハッシュ算出手段**

| XAdES リファレンスタイムスタンプ対象データのハッシュ算出手段 |
|---|
| ※ TBD (to be determined) |

5.6.4 アーカイブタイムスタンプ

### 5.6.4.1 アーカイブタイムスタンプの検証基準時刻

もし最終アーカイブタイムスタンプの場合には、検証基準時刻として有効な検証時刻または現在時刻を利用する。それ以外の場合には、検証基準時刻として最も古いタイムスタンプ時刻を利用する。詳しくは 5.4 を参照。

### 5.6.4.2 アーカイブタイムスタンプの検証要件

アーカイブタイムスタンプを、検証基準時刻において次の検証要件に従い検証する。

**表 23 検証要件（アーカイブタイムスタンプ）**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| タイムスタンプトークン | タイムスタンプトークンの構造 | 5.6.1 のタイムスタンプ検証要件に従って検証 | M | 5.6.1 参照 | |
| タイムスタンプの MessageImprint 値 | アーカイブタイムスタンプの MessageImprint（ハッシュ）値 | アーカイブタイムスタンプのハッシュ値と、計算値を比較して一致すること<br>CAdES は表 24 参照<br>XAdES は表 25 参照 | M | VALID | ・判定結果 |
| | | | | INVALID | ・タイムスタンプ MessageImprint 値<br>・計算したハッシュ値<br>・ダイジェストアルゴリズム |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

表 24 CAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

| 対象規格 | アーカイブタイムスタンプ対象データのハッシュ算出手段 |
|---|---|
| RFC3126,<br>ETSI TS 101 733<br>v1.40 以前 | 以下の値（タイプや長さフィールドを除いた値フィールド）を順に連結した値に対してハッシュ値を算出する。<br>・encapContentInfo eContent の OCTET STRING<br>・signedAttributes<br>・SignerInfo の signature フィールド<br>・SignatureTimeStamp 属性<br>・CompleteCertificateRefs 属性<br>・CompleteRevocationRefs 属性<br>・CertificateValues 属性<br>・RevocationValues 属性<br>・ESCTimeStampToken 属性（存在する場合）<br>・TimestampedCertsCRLs 属性（存在する場合）<br>・最古から検証対象までの一連の ArchiveTimeStamp（昇順） |
| ETSI TS 101 733<br>v1.7.3 | 以下の値（タイプや長さを含む）を順に連結した値に対してハッシュ値を算出する。<br>・singedData に含まれる encapContentInfo<br>・外部の署名対象のデータ（encapContentInfo の eContent が省略された場合）<br>・signedData に含まれる certificates と crls フィールド（存在する場合）<br>・signerInfo に含まれる全ての要素(※1)<br><br>※1 unsignedAttrs（非署名属性）は、次の条件で再構成する。<br>- 検証対象以降の ArchiveTimeStamp を除く。<br>- 各属性の配置順序とバイナリエンコーディングの内容は変更しない。 |

表 25 XAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

| 対象規格 | XAdES アーカイブタイムスタンプ（Not distributed case） | |
|---|---|---|
| ETSI TS 101 903<br>v1.3.2 | Reference 要素 | 以下の順序で Reference 要素を取り出し指定された正規化を行った上で連結する<br>・全 Reference 要素（必須：SingedInfo 内の出現順） |
| | XMLDSIG 要素 | 以下の順序で XMLDSIG 要素を取り出し指定された正規化を行った上で連結する<br>・SignedInfo 要素（必須）<br>・SignatureValue 要素（必須）<br>・KeyInfo 要素（存在する時のみ） |

| | | |
|---|---|---|
| | 非署名属性要素 | 以下の順序で UnsignedSignatureProperties の要素を取り出し指定された正規化を行った上で連結する<br>・SignatureTimeStamp 要素（必須）<br>・CounterSignature 要素（存在する時のみ）<br>・CompleteCertificateRefs 要素（存在する時のみ）<br>・CompleteRevocationRefs 要素（存在する時のみ）<br>・AttributeCertificateRefs 要素（存在する時のみ）<br>・AttributeRevocationRefs 要素（存在する時のみ）<br>・CertificateValues 要素（必須）<br>・RevocationValues 要素（必須）<br>・SigAndRefsTimeStamp 要素（存在する時のみ）<br>・RefsOnlyTimeStamp 要素（存在する時のみ）<br>・ArchiveTimeStamp 要素（計算対象より内側に存在する時のみ） |
| | 署名対象ではない Object 要素 | Reference 要素で参照されていない Object 要素を全て指定された正規化を行った上で連結する |
| | ハッシュ値の計算 | 以上全てを順番に連結した結果のハッシュ値を計算する |
| ETSI TS 101 903<br>v1.4.1 | Reference 要素 | 以下の順序で Reference 要素を取り出し指定された正規化を行った上で連結する<br>・全 Reference 要素（必須：SingedInfo 内の出現順） |
| | XMLDSIG 要素 | 以下の順序で XMLDSIG 要素を取り出し指定された正規化を行った上で連結する<br>・SignedInfo 要素（必須）<br>・SignatureValue 要素（必須）<br>・KeyInfo 要素（存在する時のみ） |
| | 非署名属性要素 | UnsignedSignatureProperties 要素の下を全て指定された正規化を行った上で連結する、CertificateValues 要素と RevocationValues 要素は必須要素 |
| | Object 要素 | 全ての Object 要素を全て指定された正規化を行った上で連結する |
| | ハッシュ値の計算 | 以上全てを順番に連結した結果のハッシュ値を計算する |

### 5.7 証明書の検証要件

署名やタイムスタンプの検証では署名値の検証で利用する証明書の検証を行う必要がある。証明書を検証するには、トラストアンカーとなるルート証明書までの証明書パスを辿り、有効期限、失効確認、証明書や CRL の拡張領域などを確認する必要がある。また、それらを確認する時に利用する検証基準時刻は署名フォーマット形式（ES、ES-T、ES-A）ごとに異なり、署名者証明書、TSA 証明書それぞれにおける検証要件も異なる。

なお、署名者証明書及び TSA 証明書の検証で利用する情報は次のとおりである。

- 署名者証明書もしくは TSA 証明書
- トラストアンカーを含む証明書及び失効情報のセット
- 制約条件

以下に、証明書検証の検証要件及び検証基準時刻について署名フォーマット形式ごとに解説する。本節で用いる記号の意味は以下の通りである。

Tv：検証処理を実行した時刻

Ts：署名タイムスタンプの時刻

Ta(k)：第 k 世代のアーカイブ（ドキュメント）タイムスタンプの時刻

### 5.7.1 ES における証明書

ES における証明書の検証では、以下の検証要件及び検証基準時刻で証明書検証を実施する。検証で利用する検証基準時刻の詳細については 5.4 の検証基準時刻を参照のこと。

- 署名者証明書
  - 表 26 の検証要件を満たす検証を実施する。
  - 検証処理を実行した時刻【**Tv**】を検証基準時刻とする。
- 署名者証明書の失効情報に付与された署名に対する証明書
  - 表 27 の検証要件を満たす検証を実施する。
  - 検証処理を実行した時刻【**Tv**】を検証基準時刻とする。

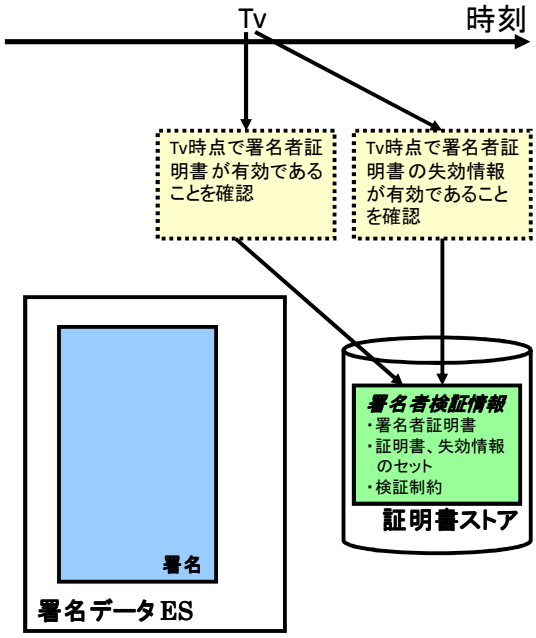


図 17 ES における証明書検証と検証基準時刻の関係

**表 26 検証要件(署名者証明書)**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| 証明書パス構築 | データ構造の正当性確認 | 証明書､失効情報の構造が正しい | M | VALID | ・判定結果 |
| | | 証明書､失効情報の構造が不正 | | INVALID | ・失敗理由 |
| | 拡張領域における制約の確認 | 制約を満足している | M | VALID | ・判定結果 |
| | | 制約（basicConstraints, policyConstraints など）を満足しない | | INVALID | ・失敗理由<br>・満足していない制約 |
| | 証明書パス構築の確認 | 署名者証明書からトラストアンカーまでの証明書パスを構築 | M | VALID | ・判定結果<br>・検証基準時刻<br>・証明書パス |
| | | 署名者証明書がない | | INDETERMINATE | ・未確定理由 |
| | | 上位証明書がない | | INDETERMINATE | ・未確定理由 |
| | | トラストアンカーに辿りつかない | | INDETERMINATE | ・未確定理由 |
| 証明書パス検証 | 証明書の改ざん確認 | 署名検証に成功 | M | VALID | ・判定結果 |
| | | 署名検証に失敗 | | INVALID | ・失敗理由<br>・証明書または失効情報 |
| | 失効確認 | 失効している | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書が失効情報に載っていた場合､失効時刻が検証基準時刻より前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・失効理由<br>・失効時刻<br>・証明書パス |
| | 有効期間の確認 | 証明書が有効期間内である | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書の有効期限が切れている | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |
| | | 証明書が有効期間前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| | アルゴリズムの有効性確認 | アルゴリズムが危殆化していない | M | VALID | ・判定結果 |
| | | アルゴリズム(署名アルゴリズム、鍵長など) が危殆化している | | INVALID | ・失敗理由<br>・証明書または失効情報<br>・危殆化したアルゴリズム |
| 失効情報 | **【ES-T、ES-A の場合のみ】**<br>失効情報の妥当性確認 | 失効確認を行った失効情報が制約条件に従った時刻以降かつ署名者証明書の有効期限内に発行されている | M | VALID | ・判定結果 |
| | | 失効確認を行った失効情報が制約条件に従った時刻以降かつ署名者証明書の有効期限内に発行されていない | | INDETERMINATE | ・未確定理由<br>・検証基準時刻<br>・失効情報 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

表 27 検証要件（失効情報に付与された署名に対する証明書）

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| 証明書パス構築 | データ構造の正当性確認 | 証明書、失効情報の構造が正しい | M | VALID | ・判定結果 |
| | | 証明書、失効情報の構造が不正 | | INVALID | ・失敗理由 |
| | 拡張領域における制約の確認 | 制約を満足している | M | VALID | ・判定結果 |
| | | 制約（basicConstraints, policyConstraints など）を満足しない | | INVALID | ・失敗理由<br>・満足していない制約 |
| | 証明書パス構築の確認 | 署名者証明書からトラストアンカーまでの証明書パスを構築 | M | VALID | ・判定結果<br>・検証基準時刻<br>・証明書パス |
| | | 署名者証明書がない | | INDETERMINATE | ・未確定理由 |
| | | 上位証明書がない | | INDETERMINATE | ・未確定理由 |
| | | トラストアンカーに辿りつかない | | INDETERMINATE | ・未確定理由 |
| 証明書パス検証 | 証明書の改ざん確認 | 署名検証に成功 | M | VALID | ・判定結果 |
| | | 署名検証に失敗 | | INVALID | ・失敗理由<br>・証明書または失効情報 |
| | 失効確認 | 失効している | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書が失効情報に載っていた場合、失効時刻が検証基準時刻より前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・失効理由<br>・失効時刻<br>・証明書パス |
| | 有効期間の確認 | 証明書が有効期間内である | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書の有効期限が切れている | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |
| | | 証明書が有効期間前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| | アルゴリズムの有効性確認 | アルゴリズムが危殆化していない | M | VALID | ・判定結果 |
| | | アルゴリズム(署名アルゴリズム、鍵長など)が危殆化している | | INVALID | ・失敗理由<br>・証明書または失効情報<br>・危殆化したアルゴリズム |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### 5.7.2 ES-T における証明書

ES-T における証明書の検証では、以下の検証要件及び検証基準時刻で証明書検証を実施する。検証で利用する検証基準時刻の詳細については 5.4 の検証基準時刻を参照のこと。

- 署名者証明書
  - 表 26 の検証要件を満たす検証を実施する。
  - 署名タイムスタンプの時刻【**Ts**】を検証基準時刻とする。
- 署名者証明書の失効情報に付与された署名に対する証明書
  - 表 27 の検証要件を満たす検証を実施する。
  - 検証処理を実行した時刻【**Tv**】を検証基準時刻とする。
- 署名タイムスタンプの TSA 証明書
  - 表 28 の検証要件を満たす検証を実施する。
  - 検証処理を実行した時刻【**Tv**】を検証基準時刻とする。

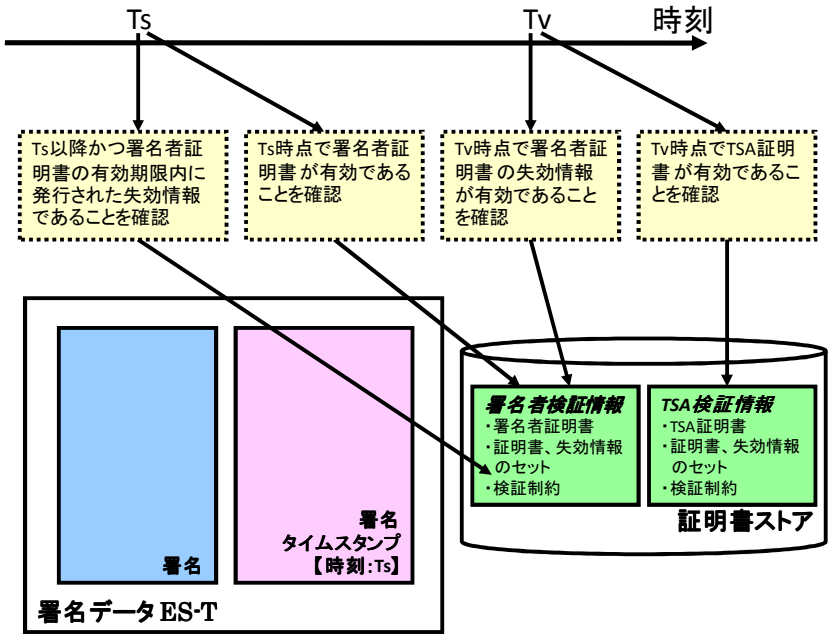


図 18 ES-T における証明書検証と検証基準時刻の関係

**表 28 検証要件(TSA 証明書)**

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| 証明書パス構築 | データ構造の正当性確認 | 証明書、失効情報の構造が正しい | M | VALID | ・判定結果 |
| | | 証明書、失効情報の構造が不正 | | INVALID | ・失敗理由 |
| | 拡張領域における制約の確認 | 制約を満足している | M | VALID | ・判定結果 |
| | | 制約（basicConstraints, policyConstraints など）を満足しない | | INVALID | ・失敗理由<br>・満足していない制約 |
| | 鍵拡張利用目的の確認 | 鍵拡張利用目的に id-kp-timeStamping かつ critical が存在している | M | VALID | ・判定結果 |
| | | 鍵拡張利用目的に id-kp-timeStamping かつ critical が存在していない | | INVALID | ・失敗理由 |
| | 鍵利用目的の確認 | 鍵利用目的に digitalSignature もしくは／かつ nonRepdiation がある | O | VALID | ・判定結果 |
| | | 鍵利用目的に digitalSignature もしくは／かつ nonRepdiation がない | | INVALID | ・失敗理由 |
| | 証明書パス構築の確認 | 署名者証明書からトラストアンカーまでの証明書パスを構築 | M | VALID | ・判定結果<br>・検証基準時刻<br>・証明書パス |
| | | 署名者証明書がない | | INDETERMINATE | ・未確定理由 |
| | | 上位証明書がない | | INDETERMINATE | ・未確定理由 |
| | | トラストアンカーに辿りつかない | | INDETERMINATE | ・未確定理由 |
| 証明書パス検証 | 証明書の改ざん確認 | 署名検証に成功 | M | VALID | ・判定結果 |
| | | 署名検証に失敗 | | INVALID | ・失敗理由<br>・証明書または失効情報 |

| 検証対象 | 検証内容 | 判定基準 | M/E/O | 判定結果（状態） | レポート例 |
|---|---|---|---|---|---|
| | 失効確認 | 失効している | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書が失効情報に載っていた場合、失効時刻が検証基準時刻より前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・失効理由<br>・失効時刻<br>・証明書パス |
| | 有効期間の確認 | 証明書が有効期間内である | M | VALID | ・判定結果<br>・検証基準時刻 |
| | | 証明書の有効期限が切れている | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |
| | | 証明書が有効期間前である | | INVALID | ・失敗理由<br>・検証基準時刻<br>・証明書パス |
| | アルゴリズムの有効性確認 | アルゴリズムが危殆化していない | M | VALID | ・判定結果 |
| | | アルゴリズム（署名アルゴリズム、鍵長など）が危殆化している | | INVALID | ・失敗理由<br>・証明書または失効情報<br>・危殆化したアルゴリズム |
| 失効情報 | 失効情報の妥当性確認 | 失効確認を行った失効情報が制約条件に従った時刻以降かつ署名者証明書の有効期限内に発行されている | O | VALID | ・判定結果 |
| | | 失効確認を行った失効情報が制約条件に従った時刻以降かつ署名者証明書の有効期限内に発行されていない | | INDETERMINATE | ・未確定理由<br>・検証基準時刻<br>・失効情報 |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### 5.7.3 ES-A における証明書

ES-A における証明書の検証では、以下の検証要件及び検証基準時刻で証明書検証を実施する。各検証で利用する検証基準時刻の詳細は 5.4 の検証基準時刻を参照のこと。

- 署名者証明書
  - 表 26 の検証要件を満たす検証を実施する。
  - 署名タイムスタンプの時刻**【Ts】**を検証基準時刻とする。
- 署名者証明書の失効情報に付与された署名に対する証明書
  - 表 27 の検証要件を満たす検証を実施する。
  - 最初のアーカイブタイムスタンプの時刻**【Ta(1)】**を検証基準時刻とする。
- 署名タイムスタンプの TSA 証明書
  - 表 28 の検証要件を満たす検証を実施する。
  - 最初のアーカイブタイムスタンプの時刻**【Ta(1)】**を検証基準時刻とする。
- アーカイブタイムスタンプの TSA 証明書
  - 表 28 の検証要件を満たす検証を実施する。
  - ［過去のアーカイブタイムスタンプの場合］第 k 世代アーカイブタイムスタンプの直後にある第 k+1 世代アーカイブタイムスタンプの時刻**【Ta(k+1)】**を検証基準時刻とする。
  - ［最新のアーカイブタイムスタンプの場合］検証処理を実行した時刻**【Tv】**を検証基準時刻とする。

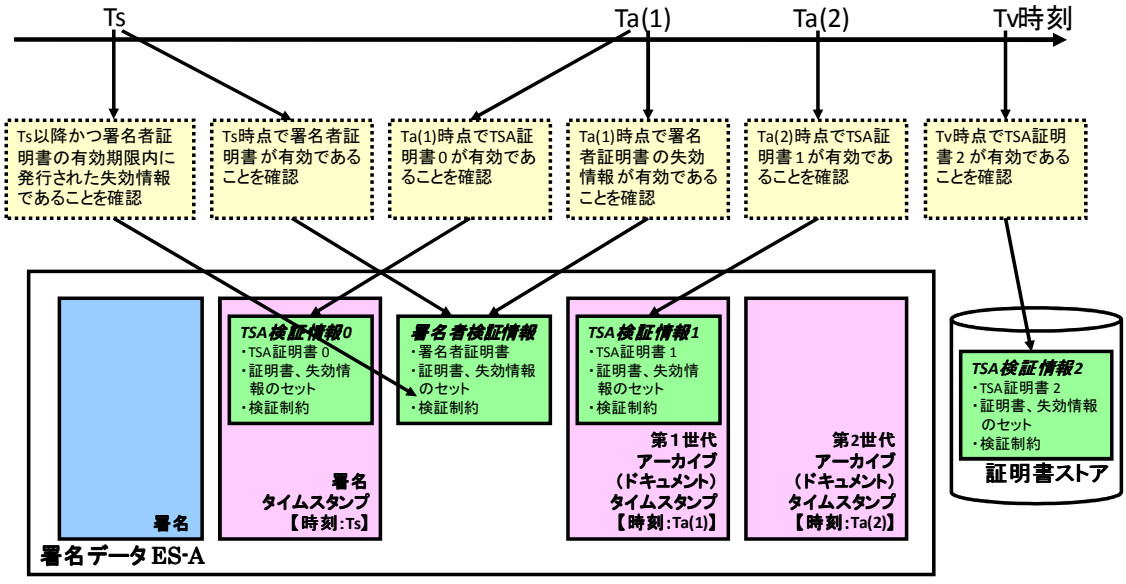


図 19 ES-A における証明書検証と検証基準時刻の関係（第 2 世代の場合）

## 付属書 A(規定):
## 供給者適合宣言書及び供給者適合宣言書の別紙

### A.1 序文

この付属書は、署名検証手順の要件に対する供給者適合宣言書の様式を規定する。

### A.2 供給者適合宣言書の様式

**署名検証手順の要件に対する供給者適合宣言書**

番号：_

発行者の名称：

発行者の住所：_

宣言の対象：

上記宣言の対象は、次の署名検証手順の要件に適合している。

| 文書番号 | タイトル | 版番号/発行日 |
|---|---|---|
| TS　xxx xxx | 署名検証ガイドライン | V1.0.0/2013-05-08 |

実装されている要素は別紙（A.3 参照）のとおりである。

追加情報：

(個々に動作確認結果などを記載することができる)

代表者又は代理者の署名：

_____

(発行場所及び発効日)

_____

(氏名、役職)

### A.3 供給者適合宣言書の別紙の様式

供給者適合性宣言書の別紙には A.4 から A.6 の各項目を含まなければならない。

### A.4 検証手順

#### A.4.1 共通

##### A.4.1.1 アルゴリズムの有効性確認

**参照: 表 10 検証要件(アルゴリズムの有効性)**

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| 暗号アルゴリズム | ダイジェストアルゴリズム | M | | VALID. | |
| | | | | INVALID | |
| | 署名アルゴリズム | M | | VALID. | |

| | | | | | |
|---|---|---|---|---|---|
| | および鍵長 | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.1.2 タイムスタンプの検証要件

参照: 表 15 検証要件(タイムスタンプ)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| データ構造 | データ構造の正当性確認 | M | | VALID | |
| | | | | INVALID | |
| | CMS データ形式の確認 | M | | VALID | |
| | | | | INVALID | |
| | 署名対象データ形式の確認 | M | | VALID | |
| | | | | INVALID | |
| TSA 証明書 | TSA 証明書のパス構築とパス検証 | M | | | |
| TSA の署名 | digestAlgorithms フィールドの有効性確認 | M | | | |
| | digestAlgorithm フィールドの有効性確認 | M | | | |
| | MessageDigest 属性の一致確認 | M | | VALID | |
| | | | | INVALID | |
| | SigningCertificate 属性における TSA 証明書のハッシュ値の一致確認 | M | | VALID | |
| | | | | INVALID | |
| | signatureAlgorithm フィールドの有効性確認 | M | | | |
| | TSA 証明書（公開鍵）による署名値の有効性確認 | M | | VALID | |
| | | | | INVALID | |
| タイムスタンプ対象データ | hashAlgorithm フィールドの有効性確認 | M | | | |
| | タイムスタンプ対象データとの整合性確認 | M | | VALID | |
| | | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.1.3 署名タイムスタンプの検証要件

参照: 表 17 検証要件(署名タイムスタンプ)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| タイムスタンプトークン | タイムスタンプトークンの検証 | M | | | |
| タイムスタンプの MessageImprint 値 | 署名タイムスタンプの MessageImprint（ハッシュ）値 | M | | VALID | |
| | | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.1.4 リファレンスタイムスタンプの検証要件

参照: 表 20 検証要件(リファレンスタイムスタンプ)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| タイムスタンプトークン | タイムスタンプトークンの検証 | M | | | |
| タイムスタンプの MessageImprint 値 | リファレンスタイムスタンプの MessageImprint（ハッシュ）値 | M | | VALID | |
| | | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.1.5 アーカイブタイムスタンプの検証要件

参照: 表 23 検証要件(アーカイブタイムスタンプ)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| タイムスタンプトークン | タイムスタンプトークンの構造 | M | | | |
| タイムスタンプの MessageImprint 値 | アーカイブタイムスタンプの MessageImprint（ハッシュ）値 | M | | VALID | - |
| | | | | INVALID | - |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

## A.4.2 CAdES 検証

### A.4.2.1 CAdES の検証要件

参照: 表 11 検証要件(CAdES 署名)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| データ構造 | データ構造の正当性確認 | M | | VALID | |
| | | | | INVALID | |
| | CMS データ形式の確認 | M | | VALID | |
| | | | | INVALID. | |
| 署名者証明書 | 署名者証明書のパス構築とパス検証 | M | | | |
| 署名 | digestAlgorithms フィールドの有効性確認 | M | | | |
| | digestAlgorithm フィールドの有効性確認 | M | | | |
| | MessageDigest 属性の一致確認 | M | | VALID | |
| | | | | INVALID | |
| | sid フィールドと署名者証明書の一致確認 | M | | VALID | |
| | | | | VALID | |
| | SigningCertificate 属性における署名者証明書のハッシュ値の一致確認 | M | | VALID | |
| | | | | INVALID | |
| | SigningCertificate 属性における発行者識別情報の一致確認 | E | | VALID | |
| | | | | VALID | |

| | | | | | |
|---|---|---|---|---|---|
| | signatureAlgorithm フィールドの有効性確認 | M | | | |
| | 署名者証明書（公開鍵）による署名値の有効性確認 | M | | VALID | |
| | | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.2.2 CAdES 署名タイムスタンプ対象データのハッシュ算出手段

参照: 表 18 CAdES 署名タイムスタンプ対象データのハッシュ算出手段

| 検証内容 | 実装 (Y/N) |
|---|---|
| signerInfo における signature（署名値）に対してハッシュ値を算出する | |

### A.4.2.3 CAdES リファレンスタイムスタンプ対象データのハッシュ算出手段

参照: 表 21 CAdES リファレンスタイムスタンプ対象データのハッシュ算出手段

| 検証内容 | 実装 (Y/N) |
|---|---|
| ※ TBD (to be determined) | |

### A.4.2.4 CAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

参照: 表 24 CAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

| 対象規格 | 実装 (Y/N) |
|---|---|
| RFC3126, ETSI TS 101 733 v1.40 以前 | |
| ETSI TS 101 733 v1.7.3 | |

## A.4.3 XAdES 検証

### A.4.3.1 XAdES の検証要件

参照: 表 13 検証要件(XAdES 署名)

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装 (Y/N) | 状態 | 報告 |
| 署名構造 | XAdES 必須要素 | M | | VALID | |
| | | | | INVALID | |
| | SignedProperties 要素 | M | | VALID | |
| | | | | INVALID | |
| オプション要素 | XAdES-BES オプション要素 | O | | VALID | |
| | | | | INVALID | |
| | XAdES-EPES オプション要素 | O | | VALID | |
| | | | | INVALID | |
| 署名者証明書 | 署名者証明書の指定確認 | M | | VALID | |
| | | | | INVALID | |
| | 署名者証明書の実体確認 | M | | VALID | |
| | | | | INVALID | |
| | 署名者証明書の一致確認 | M | | VALID | |
| | | | | INVALID | |
| | 署名者証明書のパス構築とパス検証 | M | | | |
| 参照データ | Reference 要素 | M | | VALID | |
| | | | | INVALID | |
| | DigestMethod 要素 | M | | | |
| 署名データ | SignatureValue 要素 | M | | VALID | |
| | | | | INVALID | |
| | SignatureMethod 要素の有効性確認 | M | | | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.4.3.2 XAdES 署名タイムスタンプ対象データのハッシュ算出手段

参照: 表 19 XAdES 署名タイムスタンプ対象データのハッシュ算出手段

| 検証内容 | 実装 (Y/N) |
|---|---|
| ds:SignatureValue（署名値）要素に対して正規化した上でハッシュ値を算出する | |

### A.4.3.3 XAdES リファレンスタイムスタンプ対象データのハッシュ算出手段

参照: 表 21 XAdES リファレンスタイムスタンプ対象データのハッシュ算出手段

| 検証内容 | 実装 (Y/N) |
|---|---|
| ※ TBD (to be determined) | |

### A.4.3.4 XAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

参照: 表 25 XAdES アーカイブタイムスタンプ対象データのハッシュ算出手段

| 対象規格 | 実装 (Y/N) |
|---|---|
| ETSI TS 101 903 v1.3.2 | |
| ETSI TS 101 903 v1.4.1 / v1.4.2 | |

## A.5 データ

### A.5.1 タイムスタンプトークンデータ要素

参照: 表 16 タイムスタンプトークンデータの構成要素

| ASN.1 表記 | M/O | 実装 (Y/V/N) | 備考 |
|---|---|---|---|
| ContentType | M | | |
| Content | M | | |
| CMSVersion | M | | |
| DigestAlgorithmIdentifiers | M | | |
| EncapsulatedContentInfo | M | | |
| eContentType | M | | Object identifier of "TSTInfo" |
| eContent | M | | TSTInfo |
| version | M | | |
| TSAPolicyId | M | | |
| MessageImprint | M | | |
| hashAlgorithm | M | | |
| hashedMessage | M | | |
| serialNumber | M | | |
| genTime | M | | |
| Accuracy | O | | |
| Ordering | M | | |
| Nonce | O | | |
| tsa | O | | |
| extensions | O | | |
| CertificateSet (Certificates) | O | | |
| Certificate | O | | |
| AttributeCertificateV2 | O | | |
| OtherCertificateFormat | O | | |
| RevocationInfoChoices (crls) | O | | |
| CertificateList | O | | |
| OtherRevocationInfoFormat | O | | |
| SignerInfos | M | | |
| CMSVersion | M | | |

| | | | | | |
|---|---|---|---|---|---|
| | | SignerIdentifier | M | | |
| | | IssuerAndSerialNumber | O | | |
| | | SubjectKeyIdentifier | O | | |
| | | DigestAlgorithmIdentifier | M | | |
| | | SignedAttributes | M | | |
| | | ContentType | M | | Object identifier of "TSTInfo" |
| | | MessageDigest | M | | |
| | | SigningCertificateReference | M | | |
| | | ESSSigningCertificate | O | | |
| | | ESSSigningCertificateV2 | O | | |
| | | OtherSigningCertificate | O | | |
| | | SignatureAlgorithm | M | | |
| | | SignatureValue | M | | |
| | | UnsignedAttributes | O | | |
| | | CompleteCertificateRefs | O | | |
| | | CompleteRevocationRefs | O | | |
| | | CompleteRevRefs CRL | O | | |
| | | CompleteRevRefs OCSP | O | | |
| | | CertificateValues | O | | |
| | | CertificateValues | O | | |
| | | *Storage of the certificate by CA* | O | | |
| | | RevocationValues | O | | |
| | | CertificateList | O | | |
| | | BasicOCSPResponse | O | | |
| | | OtherRevVals | O | | |

M/O: **M**andatory/**O**ptional

### A.5.2 CAdES データ要素

**参照: 表 12 署名データの構成要素(CAdES)**

| ASN.1 表記 | | | | M/O | | | 実装 (Y/V/N) |
|---|---|---|---|---|---|---|---|
| | | | | ES | ES-T | ES-A | |
| ContentType | | | | M | M | M | |
| Content | | | | M | M | M | |
| | CMSVersion | | | M | M | M | |
| | DigestAlgorithmIdentifiers | | | M | M | M | |
| | EncapsulatedContentInfo | | | M | M | M | |
| | | eContentType | | M | M | M | |
| | | eContent | | O | O | O | |
| | CertificateSet (Certificates) | | | O | O | O | |
| | | Certificate | | O | O | O | |
| | | AttributeCertificateV2 | | O | O | O | |
| | | OtherCertificateFormat | | O | O | O | |
| | RevocationInfoChoices (crls) | | | O | O | O | |
| | | CertificateList | | O | O | O | |
| | | OtherRevocationInfoFormat | | O | O | O | |
| | SignerInfos | | | M | M | M | |
| | | CMSVersion | | M | M | M | |
| | | SignerIdentifier | | M | M | M | |
| | | | IssuerAndSerialNumber | O | O | O | |
| | | | SubjectKeyIdentifier | O | O | O | |
| | | DigestAlgorithmIdentifier | | M | M | M | |
| | | SignedAttributes | | M | M | M | |
| | | | ContentType | M | M | M | |
| | | | MessageDigest | M | M | M | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | SigningCertificateReference | M | M | M | |
| | | | ESSSigningCertificate | O | O | O | |
| | | | ESSSigningCertificateV2 | O | O | O | |
| | | | OtherSigningCertificate | O | O | O | |
| | | | SignatgurePolicyIdentifier | O | O | O | |
| | | | SigningTime | O | O | O | |
| | | | ContentReference | O | O | O | |
| | | | ContentIdentifier | O | O | O | |
| | | | ContentHint | O | O | O | |
| | | | CommitmentTypeIndication | O | O | O | |
| | | | SignerLocation | O | O | O | |
| | | | SignerAttribute | O | O | O | |
| | | | ContentTimestamp | O | O | O | |
| | | SignatureAlgorithm | | M | M | M | |
| | | SignatureValue | | M | M | M | |
| | | UnsignedAttributes | | O | M | M | |
| | | | CounterSignature | - | O | O | |
| | | | *Trusted signing time* | - | M | M | |
| | | | SignatureTimestamp | - | O | O | |
| | | | *Time Mark etc.* | - | O | O | |
| | | | CompleteCertificateRefs | - | - | M | |
| | | | CompleteRevocationRefs | - | - | M | |
| | | | CompleteRevRefs CRL | - | - | O | |
| | | | CompleteRevRefs OCSP | - | - | O | |
| | | | OtherRevRefs | - | - | O | |
| | | | Attribute certificate references | - | - | O | |
| | | | Attribute revocation references | - | - | O | |
| | | | CertificateValues | - | - | M | |
| | | | CertificateValues | - | - | O | |
| | | | *Storage of the certificate by CA* | - | - | O | |
| | | | RevocationValues | - | - | M | |
| | | | CertificateList | - | - | O | |
| | | | BasicOCSPResponse | - | - | O | |
| | | | OtherRevVals | - | - | O | |
| | | | *Storage of the revocation infomation by CA* | - | - | O | |
| | | | CAdES-C-timestamp | - | - | O | |
| | | | Time-stamped cert and crls reference | - | - | O | |
| | | | *Archiving information* | - | - | M | |
| | | | ArchiveTimestampV2 | - | - | O | |
| | | | ArchiveTimestamp | - | - | O | |
| | | | Long Term Validation Timestamp | | | O | |
| | | | *Time Mark etc.* | - | - | O | |

M/O: **M**andatory/**O**ptional

### A.5.3 XAdES 構文の XML 要素

**参照: 表 14 署名データの構成要素(XAdES)**

| XML 表記 | | | | M/E/O | | | 実装 (Y/V/N) |
|---|---|---|---|---|---|---|---|
| | | | | ES | ES-T | ES-A | |
| ds:Signature | | | | M | M | M | |
| Id (attribute of ds:Signature) | | | | M | M | M | |
| | ds:SignedInfo | | | M | M | M | |
| | | ds:CanonicalizationMethod | | M | M | M | |
| | | ds:SignatureMethod | | M | M | M | |
| | | ds:Reference | | M | M | M | |
| | | | ds:Transforms | E | E | E | |
| | | | ds:DigestMethod | M | M | M | |

| | | | | | |
|---|---|---|---|---|---|
| ds:DigestValue | M | M | M | |
| ds:SignatureValue | M | M | M | |
| ds:KeyInfo | O (a) | O (a) | O (a) | |
| ds:Object | M | M | M | |
| xa:QualifyingProperties | M | M | M | |
| xa:SignedProperties | M | M | M | |
| xa:SignedSignatureProperties | M | M | M | |
| xa:SigningTime | O | O | O | |
| xa:SigningCertificate | O (a) | O (a) | O (a) | |
| xa:SignaturePolicyIdentifier | O | O | O | |
| xa:SignatureProductionPlace | O | O | O | |
| xa:SignerRole | O | O | O | |
| xa:SignedDataObjectProperties | O | O | O | |
| xa:DataObjectFormat | O | O | O | |
| xa:CommitmentTypeIndication | O | O | O | |
| xa:AllDataObjectsTimeStamp | O | O | O | |
| xa:InvalidualDataObjectsTimeStamp | O | O | O | |
| xa:UnsignedProperties | - | M | M | |
| xa:UnsignedSignatureProperties | - | M | M | |
| xa:CounterSignature | - | O | O | |
| xa:SignatureTimeStamp | - | M | M | |
| xa141:TimeStampValidationData | - | O | O (b) | |
| xa:CompleteCertificateRefs | - | O | O | |
| xa:CompleteRevocationRefs | - | O | O | |
| xa:AttributeCertificateRefs | - | O | O | |
| xa:AttributeRevocationRefs | - | O | O | |
| xa:SigAndRefsTimeStamp | - | O | O | |
| xa:RefsOnlyTimeStamp | - | O | O | |
| xa:CertificateValues | - | O | M | |
| xa:RevocationValues | - | O | M | |
| xa:AttrAuthoritiesCertValues | - | O | O | |
| xa:AttributeRevocationValues | - | O | O | |
| *Archiving information* | - | - | M | |
| xa:ArchiveTimeStamp | | | O | |
| xa141:ArchiveTimeStamp | | | O | |
| xa141:TimeStampValidationData | | | O (c) | |
| xa:UnsignedDataObjectProperties | - | - | O | |
| xa:UnsignedDataObjectPropertie | - | - | O | |
| xa:QualifyingPropertiesReference | - | - | O | |

本表における XML 名前空間
xmlns:ds="http://www.w3.org/2000/09/xmldsig#
xmlns:xa="http://uri.etsi.org/01903/v1.3.2#
xmlns:xa141="http://uri.etsi.org/01903/v1.4.1#

(a) 署名者証明書はxa:SigningCertificateまたはds:Reference要素で参照されたds:KeyInfoのいずれかにおいて指定すること。

(b) 署名タイムスタンプの証明書群と検証情報群は xa141:TimeStampValidationData を使わない場合には、署名者証明書用の xa:CertificateValues と xa:RevocationValues に入れるか、タイムスタンプトークン自体に埋め込むこと。

(c) アーカイブタイムスタンプの証明書群と検証情報群はxa141:TimeStampValidationDataを使わない場合には、タイムスタンプトークン自体に埋め込むこと。

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

## A.6. X.509 証明書

### A.6.1 X.509 証明書パス検証

**参照: 表 26 検証要件(署名者証明書)**

| 検証対象 | 検証内容 | ステータス | 報告(オプショナル) |
|---|---|---|---|

| | | M/E/O | 実装（Y/N） | 状態 | 報告 |
|---|---|---|---|---|---|
| 証明書パス構築 | データ構造の正当性確認 | M | | VALID | |
| | | | | INVALID | |
| | 拡張領域における制約の確認 | M | | VALID | |
| | | | | INVALID | |
| | 証明書パス構築の確認 | M | | VALID | |
| | | | | INDETERMINATE | |
| 証明書パス検証 | 証明書の改ざん確認 | M | | VALID | |
| | | | | INVALID | |
| | 失効確認 | M | | VALID | |
| | | | | INVALID | |
| | 有効期間の確認 | M | | VALID | |
| | | | | INVALID | |
| | アルゴリズムの有効性確認 | M | | VALID | |
| | | | | INVALID | |
| 失効情報 | | M | | VALID | |
| | | | | INDETERMINATE | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.6.2 署名者証明書の X.509 証明書パス検証

**参照: 表 27 検証要件（失効情報に付与された署名に対する証明書）**

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装（Y/N） | 状態 | 報告 |
| 証明書パス構築 | データ構造の正当性確認 | M | | VALID | |
| | | | | INVALID | |
| | 拡張領域における制約の確認 | M | | VALID | |
| | | | | INVALID | |
| | 証明書パス構築の確認 | M | | VALID | |
| | | | | INDETERMINATE | |
| 証明書パス検証 | 証明書の改ざん確認 | M | | VALID | |
| | | | | INVALID | |
| | 失効確認 | M | | VALID | |
| | | | | INVALID | |
| | 有効期間の確認 | M | | VALID | |
| | | | | INVALID | |
| | アルゴリズムの有効性確認 | M | | VALID | |
| | | | | INVALID | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

### A.6.3 TSA 証明書の X.509 証明書パス検証

**参照: 表 28 検証要件（TSA 証明書）**

| 検証対象 | 検証内容 | ステータス | | 報告(オプショナル) | |
|---|---|---|---|---|---|
| | | M/E/O | 実装（Y/N） | 状態 | 報告 |
| 証明書パス構築 | データ構造の正当性確認 | M | | VALID | |
| | | | | INVALID | |
| | 拡張領域における制約の確認 | M | | VALID | |
| | | | | INVALID | |
| | 鍵拡張利用目的の確認 | M | | VALID | |
| | | | | INVALID | |
| | 鍵利用目的の確認 | O | | VALID | |
| | | | | INVALID | |
| | 証明書パス構築の | M | | VALID | |

| | | | | | |
|---|---|---|---|---|---|
| | 確認 | | | INDETERMINATE | |
| 証明書パス検証 | 証明書の改ざん確認 | M | | VALID | |
| | | | | INVALID | |
| | 失効確認 | M | | VALID | |
| | | | | INVALID | |
| | 有効期間の確認 | M | | VALID | |
| | | | | INVALID | |
| | アルゴリズムの有効性確認 | M | | VALID | |
| | | | | INVALID | |
| 失効情報 | 失効情報の妥当性確認 | O | | VALID | |
| | | | | INDETERMINATE | |

M/E/O: **M**andatory/mandatory if **E**xists/**O**ptional

## 付属書 B（参考）
## 参考文献


- ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status Information".
- ETSI TS 101 862: "Qualified certificate Profile".
- ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".
- ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".
- ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".
- ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".
- ETSI TS 103 173: [i.5] ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011), Revision 1.0, 30. June 2011.
- Commission Decision 2009/767/EC amended by Commission Decision 2010/425/EU.
- Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.