デジタル署名検証ガイドライン

第 1.0 版

2021 年 3 月 31 日

NPO 法人
日本ネットワークセキュリティ協会
電子署名ワーキンググループ

目次

1 はじめに

1.1 背景と目的

デジタル化とネットワーク化の進展に伴い、デジタルデータの保証と取り扱う人やサービスの信頼性が、これまで以上に必要とされるようになっている。中でもデータの作成責任とその真正性は、アナログ時代においては「署名」や「押印」によって担保されてきた。デジタル時代においては、それに相当する技術として「電子署名」がある。

署名は文書等にそれが付与され、受領者が署名を確認することで文書等の真偽や価値の判断材料となる。しかし、可視データであるアナログの「署名」や「押印」と違い、「電子署名」は機械処理としての「署名検証」が必要であり、検証ツール（ソフトウェア）に依存することになる。さらに、電子署名は様々な要素から構成されており、その判定は注意を要する。その判定基準が検証ツールによって異なると、同じデータに対する判定が異なる結果となり、デジタル化の阻害要因となりかねない。それを防ぐため、次世代電子商取引推進協議会（ECOM）平成18年度成果「電子文書長期保存ハンドブック」など、署名検証の判定基準について検討されてきた。本書は、電子署名のうち公開鍵暗号技術に基づくデジタル署名について検証のガイドラインを示すため、タイムビジネス協議会（TBF）2013年作成の「電子署名検証ガイドライン」を引き継いで更新したものである。

1.2 スコープ

電子署名とは、電磁的記録（電子文書）に関連付けられ、検証により確認可能な、電子的措置であり、その効力を持たせるために様々な方式がある。欧米では電子署名(electronic signature)とデジタル署名(digital signature)を区別し、電子署名は広い意味で、本人と電子文書との関係を示すために本人が作成した電子データを指し、デジタル署名は、署名者の身元とデータが改ざんされていないことを、公開鍵暗号技術を使って検証できる技術を指す。

本書では、デジタル署名の中でも特に規格が整備され、相互運用性、国際流通性に優れた先進電子署名（AdES）を取り上げ、以後、電子署名（又は単に署名）と記した場合はこれを指すものとする。特に規約部分では、国際標準として規定されたCAdES、XAdES、PAdESのプロファイルを対象として検証の処理を示す。なお、本書では技術的な判定基準について述べるが、法的有効性に関してはスコープ外とする。

1.3 本書の位置付けと構成

本書は、先進電子署名（AdES）の検証処理に関するガイドライン（規約部分を含む）を定めるものである。

- 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CAdES、XAdES、PAdESの固有要件とを定義する。

- 規約には、技術的な安全性確保を優先して決定した値を規定する（規定値と呼ぶ）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。
- アプリケーションの提供者が各実装における規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（設計者及び実装者）。

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：用語定義と略語を記す。
- 4 章：署名の基本概念とデータ形式を記す。
- 5 章：署名検証の概念モデルと検証の詳細要件（規約部分）を記す。
- 付属書：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、5.1 節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、付属書を読むことを推奨する。

2 参照文献

2.1 引用規格

[1] ISO 14533-1:2014: "Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)"

[2] ISO 14533-2:2012: "Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)"

[3] ISO 14533-3:2017: "Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)"

[4] ISO 32000-2:2017: "Document management -- Portable document format -- Part 2: PDF 2.0"

[5] EN 319 122-1: “CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures”

[6] EN 319 122-2: “CAdES digital signatures; Part 2: Extended CAdES signatures”

[7] EN 319 132-1: “XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures”

[8] EN 319 132-2: “XAdES digital signatures; Part 2: Extended XAdES signatures”

[9] EN 319 142-1: “PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures”

[10] EN 319 142-2: “PAdES digital signatures; Part 2: Additional PAdES signatures profiles”

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

[12] IETF RFC 6818: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

[13] IETF RFC 8398: "Internationalized Email Addresses in X.509 Certificates"

[14] IETF RFC 8399: "Internationalization Updates to RFC 5280"

[15] ISO/IEC 9594-8:2017: "Information technology -- Open Systems Interconnection -- The Directory - Part 8: Public-key and attribute certificate frameworks".

[16] W3C Recommendation: "XMLSignature Syntax and Processing Version 2.0", 2015

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

[18] IETF RFC 5816: "ESSCertIDv2 Update for RFC 3161"

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

[20] IETF RFC 8933: "Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection"

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

[22] IETF RFC 6283: "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] TS 119 172-1: "Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents"

[i.3] TS 119 172-2: "Signature Policies; Part 2: XML format for signature policies"

[i.4] TS 119 172-3: "Signature Policies; Part 3: ASN.1 format for signature policies"

[i.5] TS 119 172-4: "Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists"

[i.6] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.7] EN 319 102-1 & TS 119 102-1: "Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"

[i.8] TS 119 102-2: "Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"

[i.9] IETF RFC 5698: Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)

[i.10] 電子文書長期保存ハンドブック：次世代電子商取引推進協議会,2007.3
https://www.jipdec.or.jp/archives/publications/J0004262

[i.11] 電子署名検証ガイドライン V1.0.0：タイムビジネス協議会 調査研究 WG, 2013.6.5

3 用語定義と略語

3.1 用語

用語は一般的なものを除き、ISO、IETF RFC、JIS、ETSI などの規格に基づく。

引用規格 (normative references)：

本書が参照する規格。

ベース仕様 (base specification)：

プロファイルのベースとなる仕様。例えばPAdESであれば、ベース仕様はPDFのISO 32000-2となり、プロファイルはISO 14533-3となる。

プロファイル (profile)：

標準化においてプロファイルとは、ベースとなる仕様（引用規格）の部分集合（サブセット）となる。先進電子署名においては、ISO 14533シリーズで定義されたISOプロファイルと、欧州のENとしてのBaseline署名(プロファイルと呼んでいないが事実上はプロファイル)がある。

先進電子署名 (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、本書では先進電子署名を「署名」と略して用いる。

【コラム１】

■AdESという呼称の経緯

1999年に発行されたEU電子署名指令（Directive 1999/93/EC）で"Advanced Electronic Signature"が定義されている。"Advanced Electronic Signature"は日本では「先進電子署名」あるいは「高度電子署名」と訳される。ただし、略称となる"AdES"は用いられていない。

初期ETSIの電子署名に関する規格（例えば"ETSI TS 101 733 V1.2.2 (2000-12); Electronic signature formats"）でこの定義を参照しているが、"Advanced Electronic Signature"の略称として"AdES"を当ててはいない。

最初に"AdES"の略称を用いたのは"ETSI TS 101 903 V1.1.1 (2002-02); XML Advanced Electronic Signatures (XAdES)"であり、その後、CMSの電子署名規格（ETSI TS 101 733 V1.6.3 (2005-09); CMS Advanced Electronic Signatures (CAdES)）でも"AdES"（実際には"CAdES"であるが）が用いられるようになった。

2014年に成立したEUのeIDAS規則（eIDAS Regulation）でも電子署名指令の定義は引き継がれており、"Advanced Electronic Signature"に対して電子署名指令とほぼ同等の定義が与えられているが、略称"AdES"が用いられていないのは電子署名指令と同様である。また

eIDAS 規則では自然人が生成する電子署名（Electronic Signature）に加え、法人が生成するｅシール（Electronic Seal）の概念を導入し、"Advanced Electronic Seal"の要件を定義している。

その後、ETSI では"ETSI TS 119 122-1 V1.0.1 (2015-07)"や"ETSI TS 119 102-1 V1.0.1 (2015-07)"などの規格から、"AdES"を略称ではなく固有名詞として扱い、CMS、XML、PDF それぞれに対する署名として"CAdES Digital Signature"、"XAdES Digital Signature"、"PAdES Digital Signature"を、又その総称として"AdES Digital Signature"を用いるようになった。"AdES"が"Advanced Electronic Signature"あるいは"Advanced Electronic Seal"のどちらの略称であるかが区別できないこと、両者の要件を満たす共通技術としてデジタル署名（Digital Signature）が想定されていること、ETSI が制定する規格がデジタル署名を対象としていることなどからそのような対応となったと考えられる。

署名レベル（signature level）：

先進電子署名において、プロファイル定義されている 4 つの署名のレベル（生成段階）を示す。

証明書の認証パス検証（certification path validation）：

証明書チェーンの有効性を確認する処理。

(署名検証)制約（constraints）／検証制約（validation constraint）：

先進電子署名の有効性を検証するときに署名検証アプリケーション（SVA）が照合する、規則、値、範囲、計算結果の抽象的に定式化したもの。形式的な署名ポリシー、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。

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）。

注：署名対象データは、公開鍵暗号技術による署名処理の入力となる。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、署名フォーマットごとに標準規格で定義される。

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に対して検証対象や制約情報を与えて検証を依頼するアプリケーション。SVA は DA に対して検証結果を返す。

署名ポリシー（signature policy）：

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）：

検証対象のデータに対して公開鍵暗号技術により、改ざんがないことを確認する処理。

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ー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 と validation の違い

・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。

検証情報（validation data）：

署名者や検証者によって収集された、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)、タイムスタンプなどを含む。

検証者（verifier）：

署名の有効性検証や検証を行うエンティティ。

3.2 略語

BES	Basic Electronic Signature
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 Protocol
OID	Object Identifier
PKIX	Public Key Infrastructure using X. 509、IETF PKIX ワーキンググループ
RSA	Rivest,Shamir,Adleman による公開鍵暗号方式
SVA	Signature Validation Application
TSA	Time Stamping Authority
TST	Time-Stamp Token
URI	Uniform Resource Identifier

4 デジタル署名

4.1 デジタル署名の概念モデル

4.1.1 デジタル署名の基本原理

紙文書や物理的な媒体における署名（サイン）や押印は、署名対象の作成者を示すとともに、署名対象が真正であることを示すためのものである。電子文書など電子データにおいても、その作成者（文責）と非改ざん性を証明するために、様々な電子署名方式が考案されている。中でも公開鍵暗号を用いたデジタル署名は、技術の整備と標準化が進み、最も普及している署名方式と言える。

デジタル署名では、公開鍵暗号の署名鍵で生成した署名は、対となる検証鍵でのみ有効性を検証できる。また署名鍵を署名者のみが保有する秘密鍵（Private key:私有鍵とも呼ばれる）とすることで、他人が同じ鍵を生成できず、検証鍵を公開して公開鍵（Public key）とすることで、誰でも検証可能となる。つまり、秘密鍵を保有する人が署名したことと、検証結果により元のデータの改ざん有無が分かる。

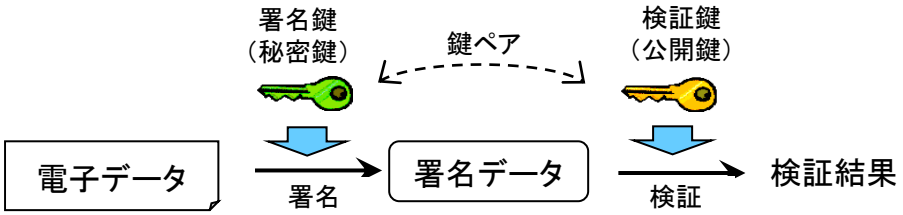

図 4.1.1-1 公開鍵暗号による署名・検証

なお、公開鍵暗号の一種である RSA 暗号の場合、署名処理として暗号化、検証処理として復号が行われる。

4.1.2 電子証明書と認証局、公開鍵基盤(PKI)

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

本人以外が使用できないことについては、一般的には IC カードなどに格納して本人が適切に管理することにより実現される。その上で署名の本人性を担保するには、公開鍵が誰のものであるか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（ペアとなる秘密鍵の所有者）を保証するモデルが認証局モデルである。認証局（CA）は利用者（秘密鍵の所有者）の本人確認を実施した上で公開鍵の所有名義人であることを証明する公開鍵証明書の発行を行い、利用者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デジタル署名が付与され、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）。本

人確認等を行い、利用者と鍵の紐付けを担う機能を取り出して登録局（RA）と呼ぶことがある。

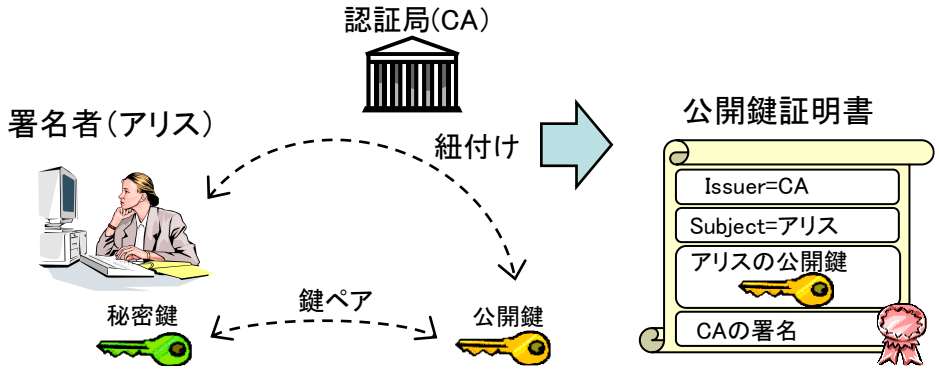

図 4.1.2-1 認証局と公開鍵証明書

【コラム２】

■電子署名の法的定義

電子署名法（電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第百二号））2 条 1 項にて、「電子署名」は、以下のとおり規定されている。

―――

「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）

―――

つまり、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（同 3 条）。なお、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、施行規則第 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。

なお、認証局同士が連携して信用関係を構築することがある。階層型の信用関係の場合、上位の認証局が下位の認証局の証明書を発行し、最上位の認証局（ルート CA）は自分で自分を証明する自己署名証明書を発行する。上位の認証局に証明される認証局は中間 CA（Intermediate CA）と呼ばれる。

また、署名者は秘密鍵を安全に管理する必要があるが、秘密鍵の紛失や、秘密鍵の活性化に用いるパスワードの漏洩などにより、秘密鍵が危殆化（本人性の証明に使えなくなる状態）する可能性がある。その場合、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する。この失効情報は証明書失効リスト（CRL：Certificate Revocation List）と呼ばれ、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 4.1.2-2 認証局の階層構造と公開鍵証明書に、認証局の階層構造と公開鍵証明書の例を示す。このように、公開鍵・秘密鍵と所有者の紐付けを保証する仕組みや失効を確認できる情報の提供を含めて基盤として整備されたものが公開鍵基盤（PKI:Public Key Infrastructure）である。

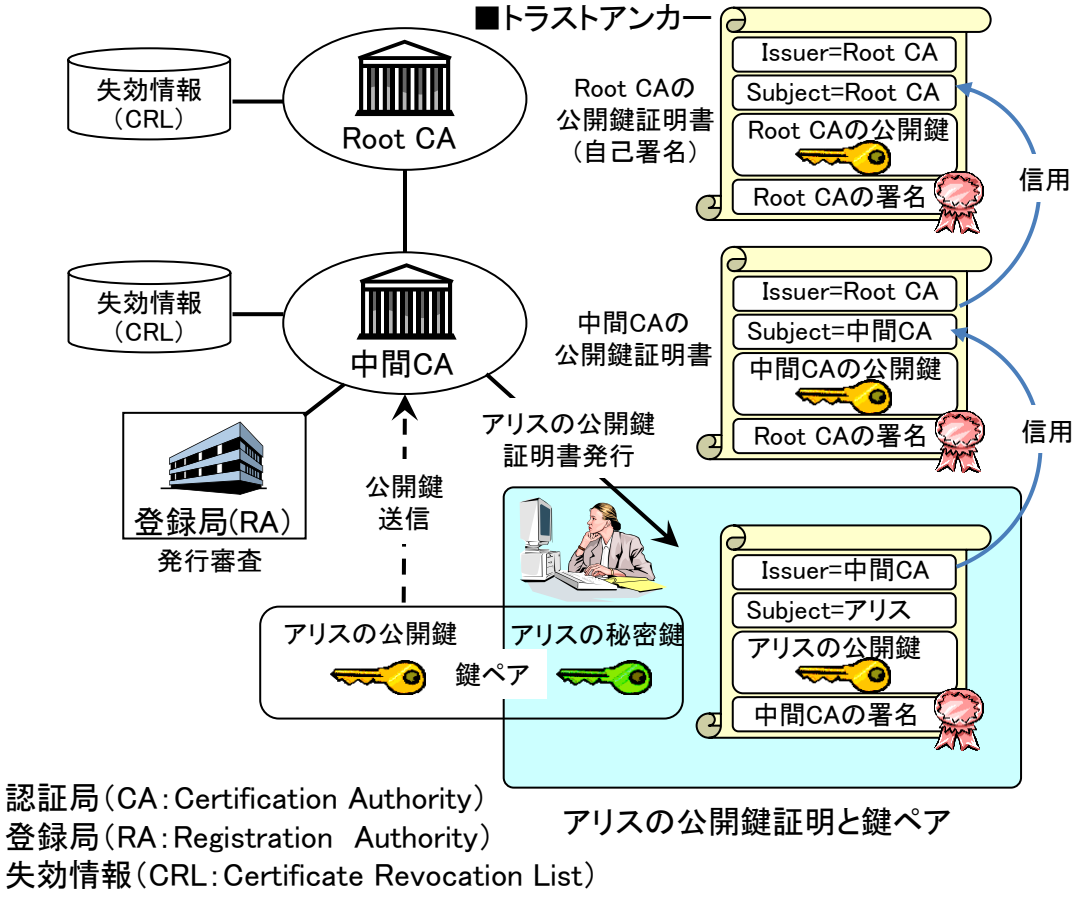

図 4.1.2-2 認証局の階層構造と公開鍵証明書

4.1.3 デジタル署名のメカニズムと基本要件

デジタル署名の署名データは、署名対象文書に対して、署名鍵を用いて署名アルゴリズムによる所定の署名処理を施したものである。RSA 署名の場合、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

暗号化したものとなる。

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検証処理を行う。RSA 署名の場合、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。図 4.1.3-1 署名と署名検証（RSA 署名の場合）に RSA 署名のメカニズムを示す。

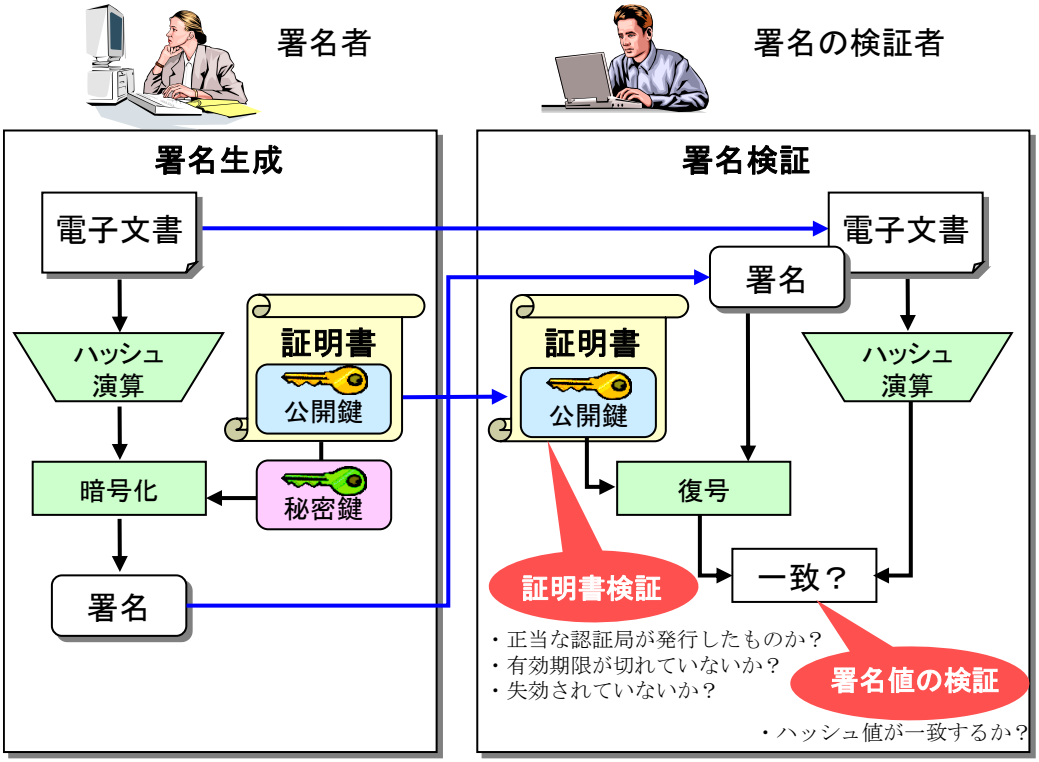

図 4.1.3-1 署名と署名検証（RSA 署名の場合）

また、署名を実施する際には、その目的に応じ、以下の要件に留意する必要がある。

（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「証明書ポリシー」（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） 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に設定されているが、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

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、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、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)

なお、署名に用いられるハッシュ関数や暗号アルゴリズムは、計算機関連の技術進化とともに解読のリスクが高まるため、署名の正当性確認を可能とするためには、より長い鍵、より強度の高いアルゴリズムに移行していかなければならない。

【コラム３】

■署名の基本要件（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、厚生労働省の「医療情報システムの安全管理に関するガイドライン第 5.1 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。

4.1.4 署名データの形式

署名データは標準規格により、署名対象のデータとそのハッシュ値を暗号化した署名値及び各種パラメータ（属性）を含めて、下図の論理構成として規定されている。

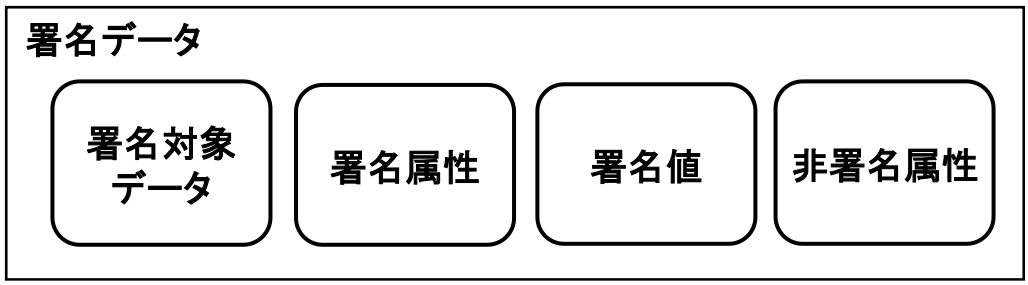

図 4.1.4-1 署名データの論理構成

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こともできる。署名対象データと署名データの形式には、図 4.1.4-2 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。

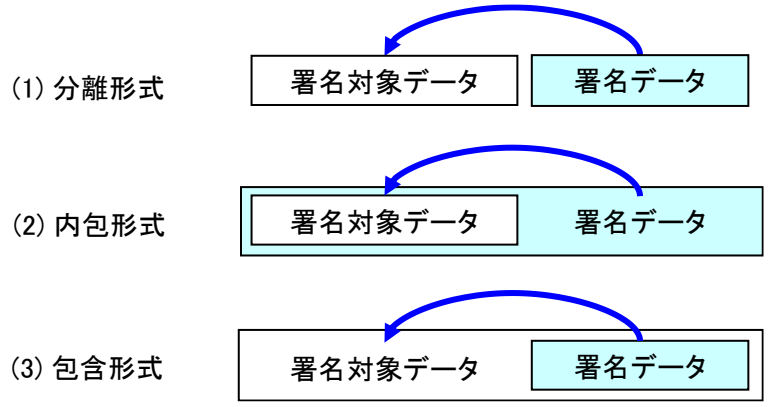

図 4.1.4-2 署名対象データと署名データの形式

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できる。既存アプリケーションで署名対象データを取り扱っている場合など、アプリケーション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付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、アプリケーション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よいので扱いが容易。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ことが必要となり、作成できるファイル形式には制限がある（例：PDF や XML など）。

4.2 時刻の保証と長期署名フォーマット

4.2.1 時刻情報とタイムスタンプ局

署名の要件として、署名時点での証明書の有効性が問われることとなるが、そのためには署名時刻等を保証する客観的な時刻情報が必要となる。署名を生成するコンピュータの時刻情報を使用すると、故意か否かに関わらず、正確性が保証されない。

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）である。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）を付与することにより、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と、それ以降、改ざんされていないことが証明可能となる。

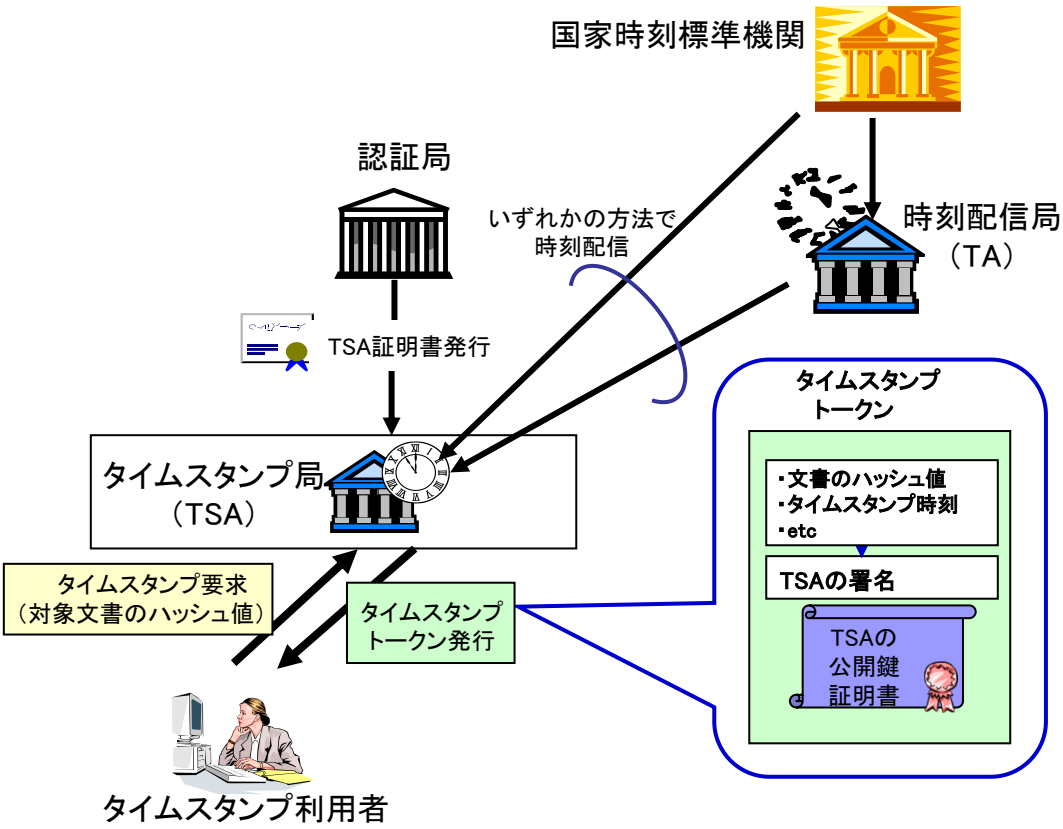

図 4.2.1-1 タイムスタンプ局の概要（デジタル署名方式(RFC3161)の場合）

4.2.2 長期的な署名の担保と署名の延長

鍵や証明書には有効期間があり、法定保存期間が定められた文書を保存する場合など、有効期間を越えて、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。

また通常、認証局は証明書の有効期間を越えて失効情報を公開しないことが多い。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できないことがある。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、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（先進電子署名）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。なお、証明書チェーン上の認証局は、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発行する認証局の 2 つの認証ドメインにおける全ての認証局となることに留意されたい。

・タイムスタンプ局の証明書

・署名者の証明書

・証明書チェーン上の認証局の証明書

・上記全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 4.2.2-1 長期署名フォーマットによる署名延長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、以下である。

- **署名タイムスタンプ**
  署名が存在した時刻を特定可能にするために、署名値に付与されるタイムスタンプ
- **アーカイブタイムスタンプ**
  暗号アルゴリズムの危殆化、認証局の変更、証明書の期限切れや失効があったとしても将来検証できるように、署名対象及び検証情報を包括的に保護するためのタイムスタンプ。署名の検証可能な期間を延長するために使用する。
- **コンテントタイムスタンプ**（オプション）
  署名対象データそのものに対して、オプションで付与可能なタイムスタンプ。署名タイムスタンプは、署名時点以降の署名対象データの存在証明となるが、コンテントタイムスタンプは署名タイムスタンプより前に行い、署名対象データが「いつから」存在したのかを示すことができる。
- **ドキュメントタイムスタンプ**
  PAdES に用いることができる DocTimeStamp で指定される汎用的なタイムスタンプのための PDF フィールドであり、PDF 文書に対してデジタル署名をせずに直接行うタイムスタンプ、署名タイムスタンプ、アーカイブタイムスタンプの 3 つの用途に用いることが

できる。どの用途であるかは、データのコンテキストで判断する必要がある。PAdES では、署名と署名タイムスタンプを CAdES-T 形式でも与えることができ、その場合は、署名タイムスタンプ用途のドキュメントタイムスタンプは使用しない。

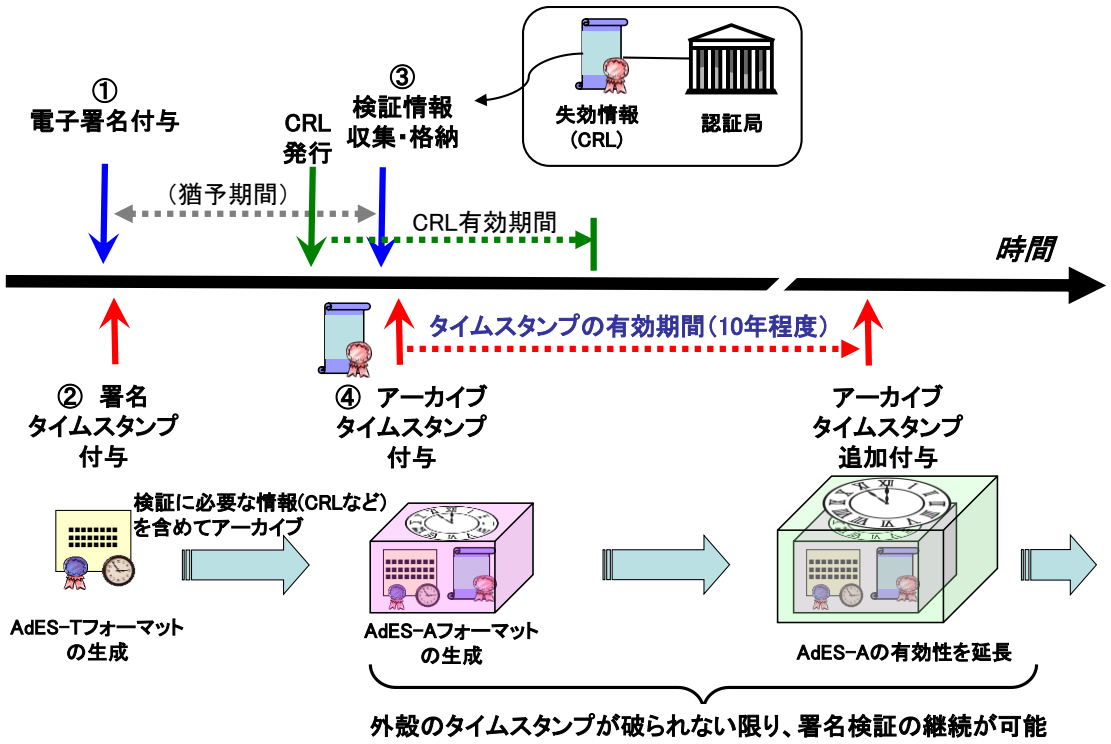

図 4.2.2-1 長期署名フォーマットによる署名延長

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の有効性に関する情報などの様々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（5.2 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全ての証明書、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

4.2.3 AdES フォーマット

AdES では前述のとおり、署名の後、署名時刻を確定するため署名タイムスタンプを付し、その後、署名及びタイムスタンプが失効していないことを示す検証情報を付加し、期限切れ等で失効する前にアーカイブ用のタイムスタンプを付す。さらに期限切れ等が発生する前に、検証情報を付加してアーカイブタイムスタンプを重ねるライフサイクルとなる。

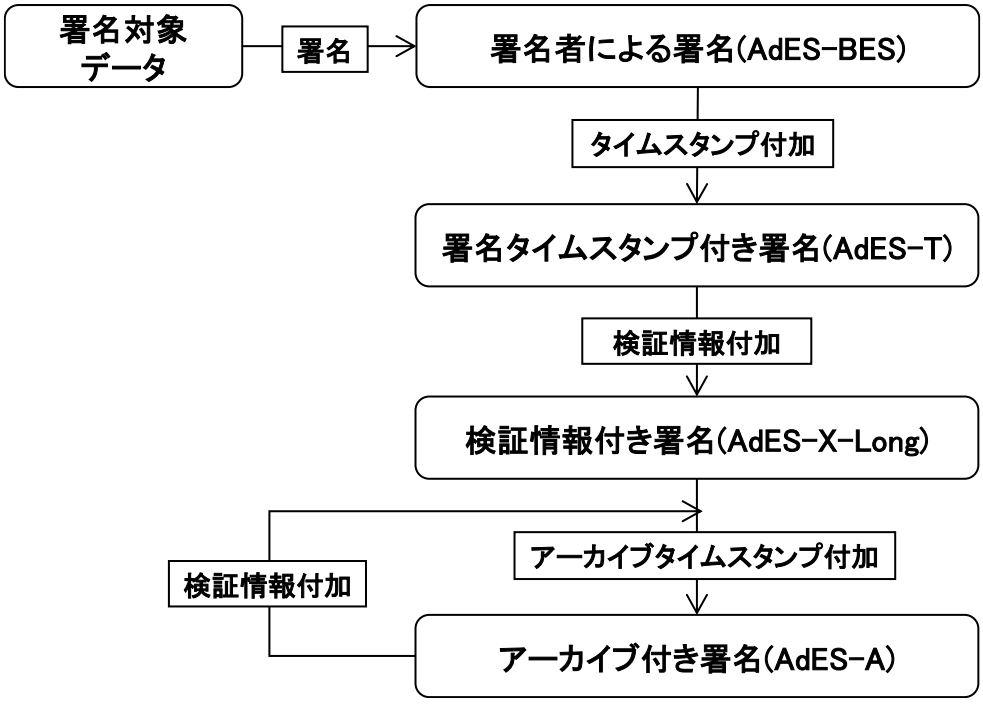

図 4.2.3-1 署名データのライフサイクル

各フェーズにおけるデータフォーマットの論理的な構成は以下のとおりである。

(1) 署名者による署名を付した署名データ (AdES-BES)

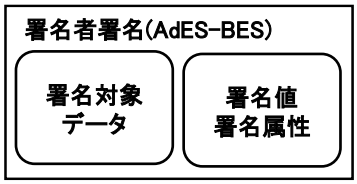

図 4.2.3-2 署名者による署名 (AdES-BES)

(2) 署名タイムスタンプを付した署名データ (AdES-T)

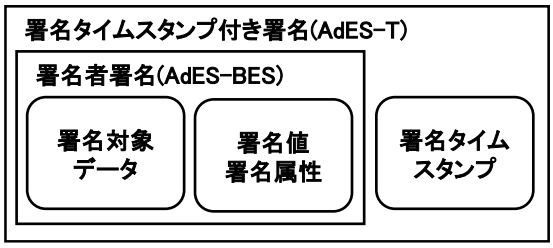

図 4.2.3-3 署名タイムスタンプ付き署名 (AdES-T)

(3) 検証情報を付加した署名データ (AdES-X-Long)

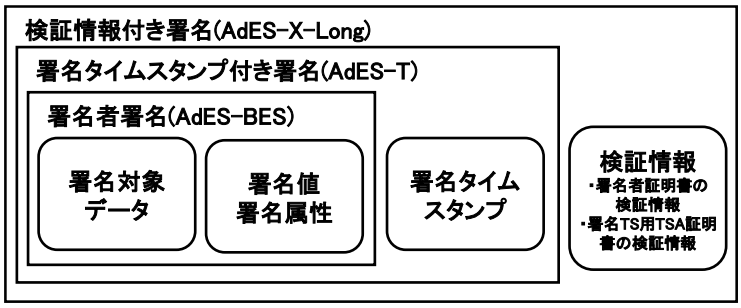

図 4.2.3-4 検証情報付き署名 (AdES-X-Long)

AdES-X-Long はアーカイブタイムスタンプを付与する前段として、必要な検証情報が付与された状態である。ここで AdES-X-Long の検証情報は、タイムスタンプを付していないデータのため、改ざんの危険性がある。通常は、速やかにアーカイブタイムスタンプを付与するか、用途に従った処理を行うことになる。

【コラム４】

■電子処方箋における AdES-X-Long の利用

2018 年 7 月に厚労省から公開された「電子処方箋 CDA 記述仕様　第 1 版（平成 30 年 7 月)」に基づき、JAHIS（一般社団法人保健医療福祉情報システム工業会）では電子処方箋実装ガイドを定めている。その規約においては、処方を行った医師が電子処方箋に署名を付与した後、処方箋と医師の署名の両者を署名対象に含めた文書全体に対して調剤を行った薬剤師が署名を付与することとしている。この際、医師の署名を XAdES-X-Long の形式とした上で薬剤師が署名を付すことにより、医師の署名の検証情報を保存可能としている。

(4) アーカイブ用のタイムスタンプを付した署名データ (AdES-A)

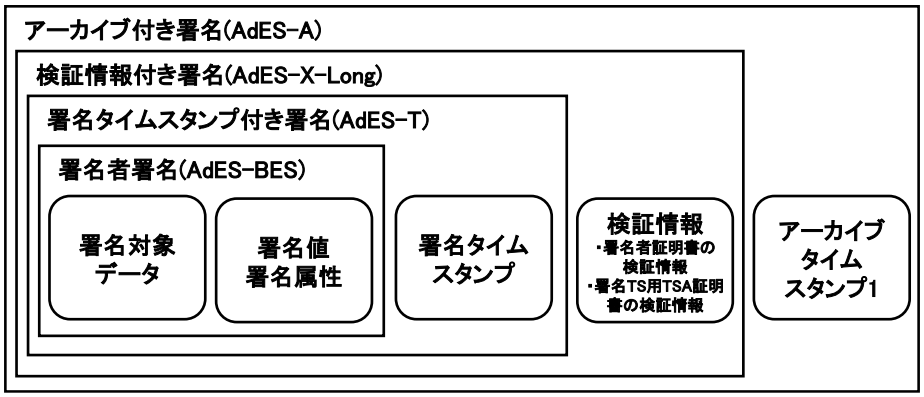

図 4.2.3-5 アーカイブ付き署名 (AdES-A)

(5) 2回目のアーカイブ用タイムスタンプを付した署名データ (AdES-A)

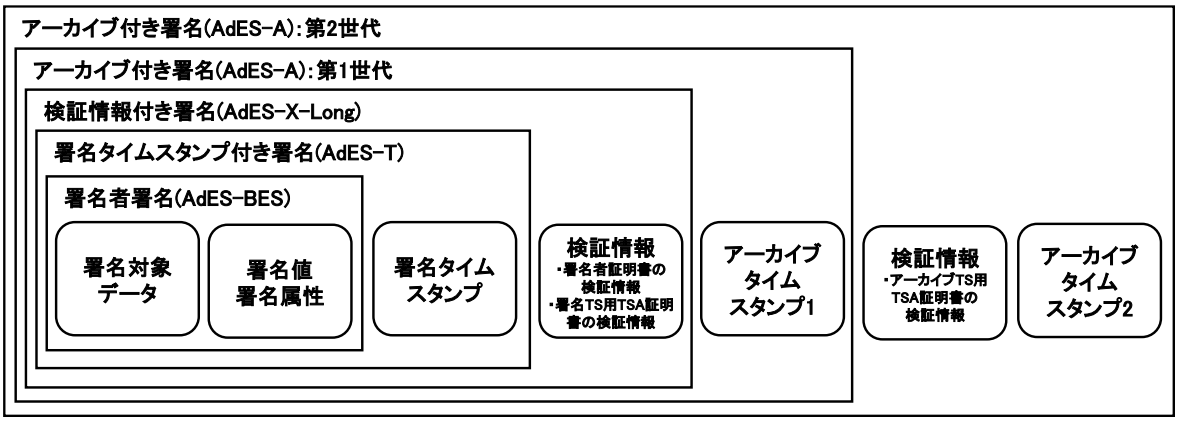

図 4.2.3-6 第2世代のアーカイブ付き署名 (AdES-A)

また、AdES フォーマットは、署名対象ファイル種別に応じて以下の種類が規定されている。

■CAdES

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 ファイ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、包含形式の全てに用いることができる。

■PAdES

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。

5 デジタル署名の検証

5.1 署名検証の概念モデル

5.1.1 署名検証の基本要件

署名検証の基本要件は、署名の基本要件に対応して、署名の本人性と非改ざん性を確認することとなる。前者は「証明書検証」、後者は「署名値の検証」と定義され、前者は署名の基本要件である（1）～（4）を適切に確認し、後者は署名対象データの署名値を公開鍵で検証処理することで確認する。

ここで署名検証はデジタル署名を付与し、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、いつ時点における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。いつ時点における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（5.2.7 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“署名を付与した時点”とすることが理想であるが、通常、署名を付与した時刻を客観的に証明することができない。そこで、検証基準時刻はタイムスタンプを併用するなどによる客観的な署名の時刻となり、それが確認できない場合は、署名検証を実施する現在時刻となる。

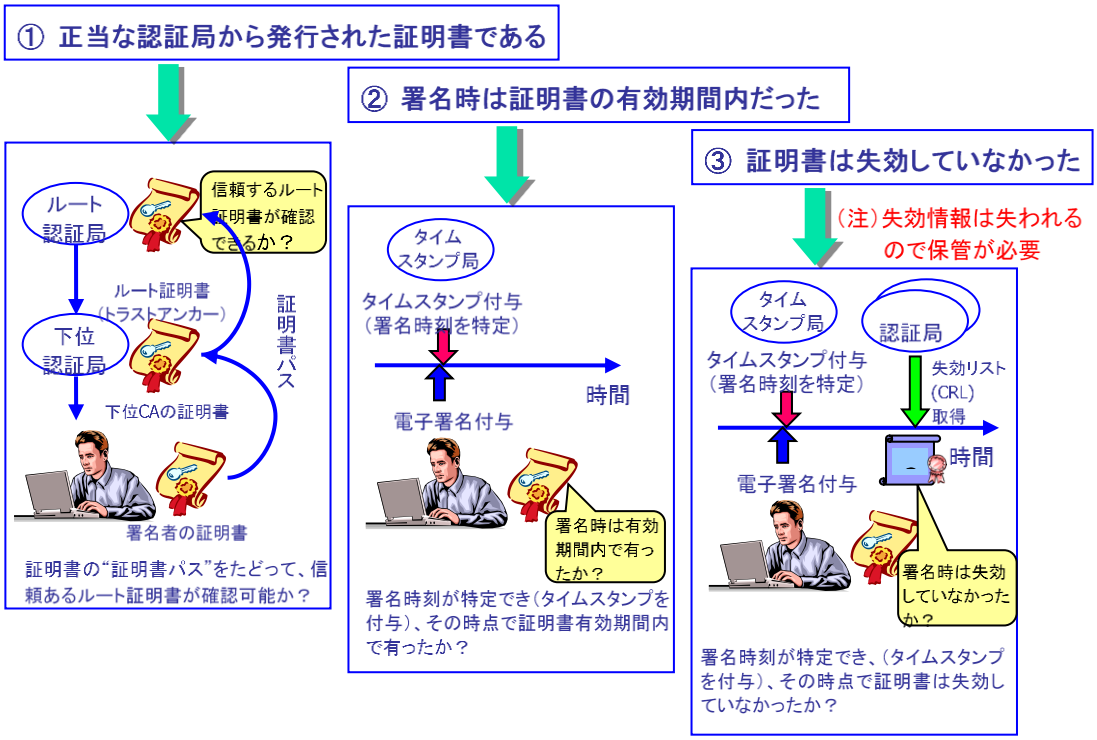

図 5.1.1-1 証明書検証の要素

証明書検証に際しては電子署名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ていたこと
(2)　署名当時に証明書の有効期間が切れていなかったこと
(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 5.1.1-1 では、(1)から(3)を図示しているが、(1)及び、(2)に関して、署名時刻がいつであったのか客観的に示すためにタイムスタンプが利用されること、また署名時点での証明書の有効性を確認するために失効情報が保管されることが必要である。

5.1.2 検証のアプリケーションモデル

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（DA：Driving Application）と署名検証アプリケーション（SVA：Signature Validation Application）に分けて考える（図 5.1.2-1）。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言う。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の表示を行う。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。本書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。

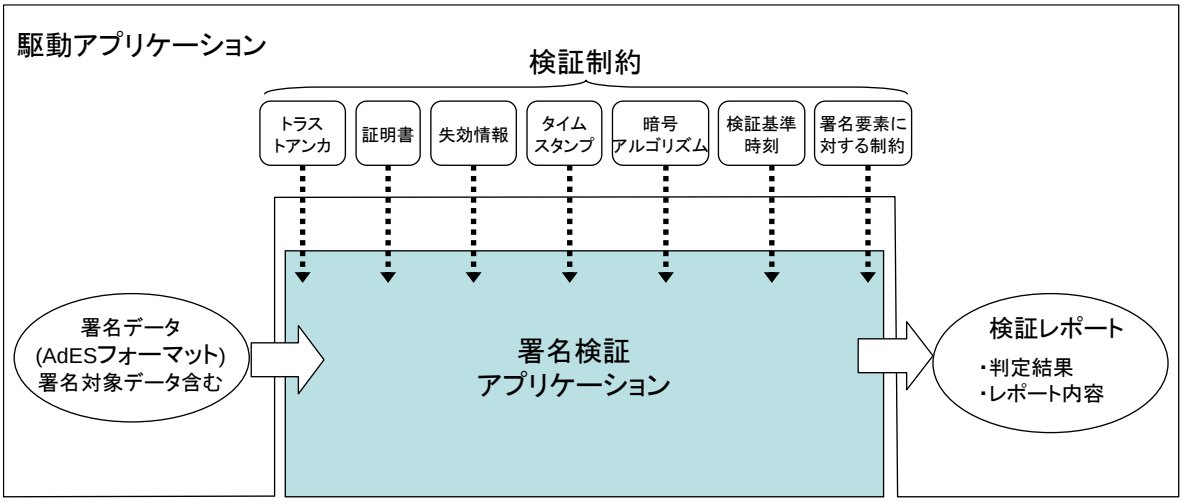

図 5.1.2-1 署名検証アプリケーションの概念モデル

検証レポートには署名データの判定結果や詳細なレポート内容が含まれる。

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ー、証明書の検証情報（中間 CA 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。

5.1.3 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。

なお、検証すべき項目に１つでも INVALID があれば、全体として INVALID であり、処理を終了できる。しかし、他にも INVALID の項目が存在する可能性があり、どこに問題があったかを知ることは検証として有用なことがあるため、検証処理を継続することは意味がある。逆に

INVALID の結果からは、他に INVALID の項目がなかったのか、処理を打ち切ったかが分からないため、どちらの実装であるかを供給者の適合宣言書に記して、明確にすべきである。

5.1.4 要求レベル（必須とオプション）の考え方

本書における検証要件のレベルを以下のように定める。

検証要件には、電子署名としてセキュリティを担保するために制約条件の違いなどに依存せず最低限実行しなければならないもの、用途に依存するがセキュリティを担保するためには意味があるもの、用途に依存して実行要否を決定するものに分けられ、それぞれのフィールドを、必須、存在時必須、オプションと規定する。

各々の処理方法は以下とする。

- 必須［M（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［E（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［O（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。

なお、後述の署名データの構成要素における M（Mandatory）/O（Optional）は、署名生成時の選択基準である（PAdES の場合は、禁止[P（Prohibited）]もある）。

また、本書の規定を基にして、さらに用途を限定したプロファイルを策定する場合、[Optional]の検証項目を[Mandatory if Exists] 又は[Mandatory]に、[Mandatory if Exists]の検証項目を[Mandatory]に再定義することは可能とする。しかし、[Mandatory]もしくは[Mandatory if Exists]の項目はセキュリティを担保するために必要な項目であり、これらを検証しない実装は供給者の適合宣言書に記して、その制約を明確にする必要がある。

5.2 検証プロセス

5.2.1 検証プロセスの考え方

検証は、前述のとおり、署名値の検証（非改ざん性の確認）、証明書の検証（本人性の確認）、及びそれらが署名生成されてからの使用期間中、有効であったことの確認をすることである。署名の延長を考慮すると、AdES の各フォーマットに対応する必要がある。フォーマットの詳細と準拠する規約を 5.3 に示す。署名を延長した場合は、検証の基準となる時刻が重要であり、各フォーマットにおける検証基準時刻の考え方を 5.4 に示す。

検証にあたっては、署名データの要素として、署名、タイムスタンプ、証明書を検証することになる。署名について 5.5 に、タイムスタンプについて 5.6 に、証明書について 5.7 に示す。

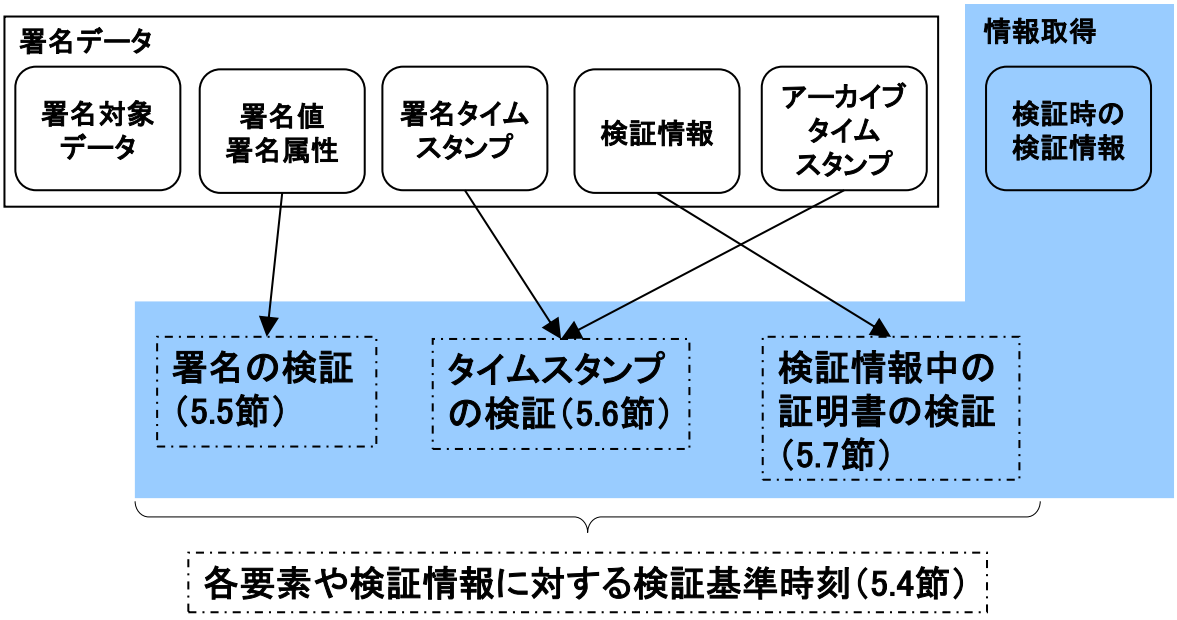

図 5.2.1-1　署名検証プロセス

なお、実際の利用用途に応じて、署名の使い方や扱いに制約を加えることがあり、検証もその制約に対応して行う必要がある。その場合、署名検証アプリケーションには、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規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。

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][i.4]準拠）
- 設定ファイル（独自形式）

- 実装ロジックへの埋め込み

次項以降に検証制約とその関連情報を示す。

5.2.2 トラストアンカー

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。

なお、欧州では認証局や各種サービスの情報を公的に一覧として整備し、確認できるようにした Trusted List がある。

5.2.3 証明書

署名データにトラストアンカー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、署名検証アプリケーション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。

5.2.4 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アプリケーション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）にはそれを利用することができる。適切な（すなわち、検証に利用が許容される）タイミングとしては、署名やタイムスタンプ生成後、猶予期間を経ていること、次のタイムスタンプ付与又は検証の時点で、失効情報の発行周期以内で最も新しい（鮮度が高い）ものであることが求められる（詳細は 5.4 を参照）。なお、実際には、ルート CA や中間 CA の失効情報、OCSP のタイミングなど、状況に応じて考慮が必要となる。

5.2.5 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。

実際には、暗号アルゴリズムの利用箇所は多岐にわたるとともに、その安全性の基準等が明確でないため、何らかの制約を設けない限り確認は困難となる。その課題と解決策案は「付属書C」に述べる。

5.2.6 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ー、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。

5.2.7 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基準とする時刻（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、その証明書をタイムスタンプ対象（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。

検証基準時刻における検証の考え方を整理すると、以下となる。

- 署名、コンテントタイムスタンプ
  - ・ 署名タイムスタンプがなければ現在時刻で検証
  - ・ 署名タイムスタンプがあればその時刻で検証
- 署名タイムスタンプ
  - ・ アーカイブタイムスタンプがなければ現在時刻で検証
  - ・ アーカイブタイムスタンプがあれば最も古いアーカイブタイムスタンプの

時刻で検証

- アーカイブタイムスタンプ群
  - 自分より新しいアーカイブタイムスタンプがなければ、現在時刻でそのアーカイブタイムスタンプを検証
  - 自分より新しいアーカイブタイムスタンプがあれば、その直後のアーカイブタイムスタンプの時刻で検証

5.2.8 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したりする場合がある。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、本書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。

5.3 検証データの全体構造

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(AdES-BES)

署名者による署名（AdES-BES）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。AdES-BES の論理的な構造と、検証要件の各節との関係を図 5.3.1-1 に示す。AdES-BES の仕様が記述された各規格の一覧を表 5.3.1-1 に示す。

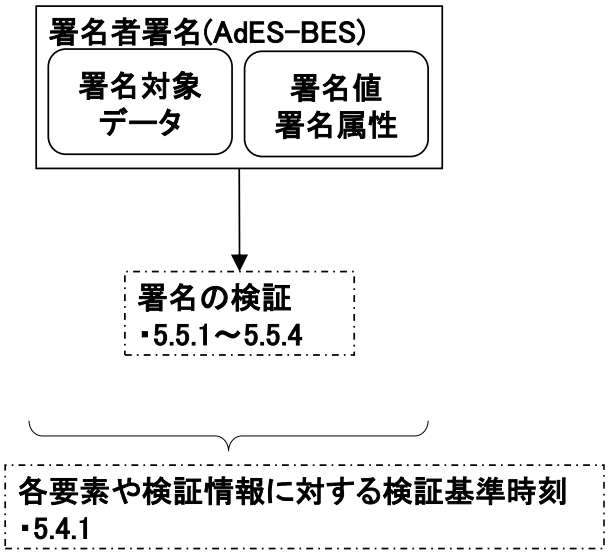

図 5.3.1-1 署名者による署名（AdES-BES）の検証

表 5.3.1-1 署名者による署名（AdES-BES）の規格

署名種別	ベース仕様	プロファイル	該当の署名レベル
CAdES	ETSI EN 319 122-1	ISO 14533-1(ISOプロファイル)	(未定義)
		ETSI EN 319 122-2(拡張プロファイル)	CAdES-E-BES / CAdES-E-EPES
		ETSI EN 319 122-1(欧州プロファイル)	CAdES-B-B
XAdES	ETSI EN 319 132-1	ISO 14533-2(ISOプロファイル)	(未定義)
		ETSI EN 319 132-2(拡張プロファイル)	XAdES-E-BES / XAdES-E-EPES
		ETSI EN 319 132-1(欧州プロファイル)	XAdES-B-B
PAdES	ISO 32000-2	ISO 14533-3(ISOプロファイル)	(未定義)
	ETSI EN 319 142-1	ETSI EN 319 142-2(拡張プロファイル)	PAdES-E-BES / PAdES-E-EPES
		ETSI EN 319 142-1(欧州プロファイル)	PAdES-B-B

5.3.2 署名タイムスタンプ付き署名(AdES-T)

署名タイムスタンプ付き署名 (AdES-T) は署名者による署名(AdES-BES) とともに署名タイムスタンプを付与した形式である。AdES-T の論理的な構造と、検証要件の各節との関係を図 5.3.2-1 に示す。AdES-T の仕様が記述された各規格の一覧を表 5.3.2-1 に示す。

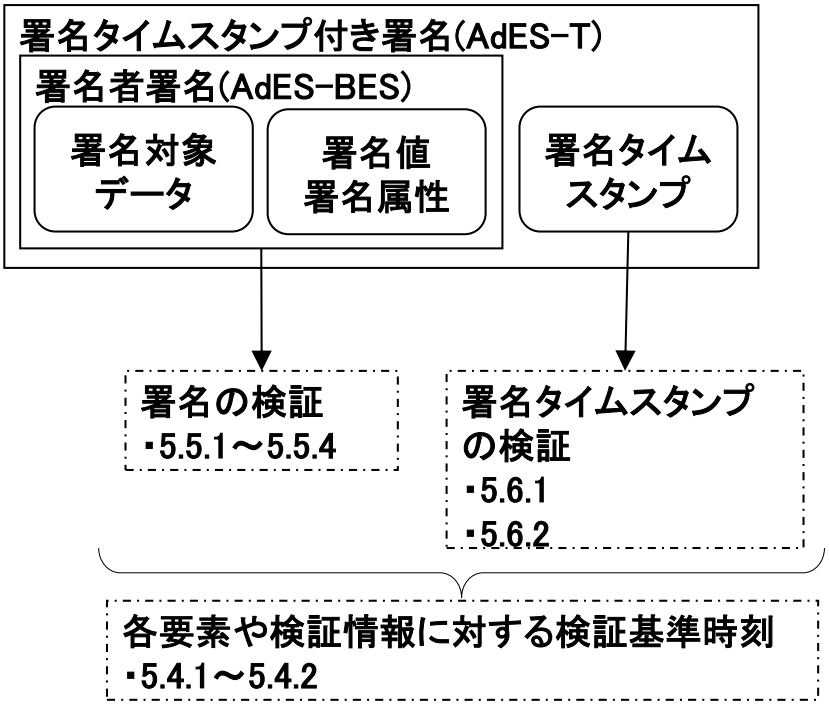

図 5.3.2-1 署名タイムスタンプ付き署名 (AdES-T) の検証

表 5.3.2-1 署名タイムスタンプ付き署名 (AdES-T) の規格

署名種別	ベース仕様	プロファイル	該当の署名レベル
CAdES	ETSI EN 319 122-1	ISO 14533-1(ISO プロファイル)	CAdES-T
		ETSI EN 319 122-2(拡張プロファイル)	CAdES-E-T
		ETSI EN 319 122-1(欧州プロファイル)	CAdES-B-T
XAdES	ETSI EN 319 132-1	ISO 14533-2(ISO プロファイル)	XAdES-T
		ETSI EN 319 132-2(拡張プロファイル)	XAdES-E-T
		ETSI EN 319 132-1(欧州プロファイル)	XAdES-B-T
PAdES	ISO 32000-2	ISO 14533-3(ISO プロファイル)	PAdES-T
	ETSI EN 319 142-1	ETSI EN 319 142-2(拡張プロファイル)	PAdES-E-T
		ETSI EN 319 142-1(欧州プロファイル)	PAdES-B-T

5.3.3 検証情報付き署名(AdES-X-Long)

検証情報付き署名（AdES-X-Long）は、署名タイムスタンプ付き署名（AdES-T）に検証情報を格納した形式である。検証情報（証明書チェーン、OCSP レスポンス及び CRL 等）を格納することにより、認証局が存在しなくなったとしても検証情報付き署名単独で署名や署名タイムスタンプの検証を行うことができる。

AdES-X-Long の論理的な構造と、検証要件の各節との関係を図 5.3.3-1 に示す。AdES-X-Long の仕様が記述された各規格の一覧を表 5.3.3-1 に示す。

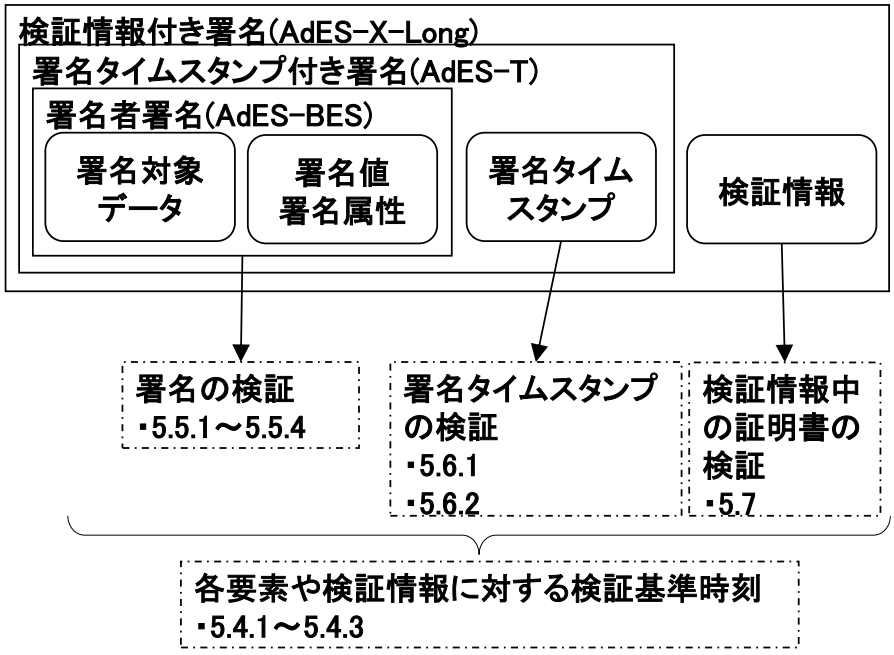

図 5.3.3-1 検証情報付き署名(AdES-X-Long)の検証

表 5.3.3-1 検証情報付き署名(AdES-X-Long)の規格

署名種別	ベース仕様	プロファイル	該当の署名レベル
CAdES	ETSI EN 319 122-1	ISO 14533-1(ISO プロファイル)	(未定義)
		ETSI EN 319 122-2(拡張プロファイル)	CAdES-E-X-Long
		ETSI EN 319 122-1(欧州プロファイル)	CAdES-B-LT
XAdES	ETSI EN 319 132-1	ISO 14533-2(ISO プロファイル)	(未定義)
		ETSI EN 319 132-2(拡張プロファイル)	XAdES-E-X-Long
		ETSI EN 319 132-1(欧州プロファイル)	XAdES-B-LT
PAdES	ISO 32000-2	ISO 14533-3(ISO プロファイル)	(未定義)
	ETSI EN 319 142-1	ETSI EN 319 142-2(拡張プロファイル)	PAdES-E-X-Long
		ETSI EN 319 142-1(欧州プロファイル)	PAdES-B-LT

5.3.4 アーカイブ付き署名(AdES-A)

アーカイブ付き署名(AdES-A)は検証情報付き署名 (AdES-X-Long) 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。

AdES-A の論理的な構造と、検証要件の各節との関係を図 5.3.4-1 に示す。 AdES-A の仕様が記述された各規格の一覧を表 5.3.4-1 に示す。

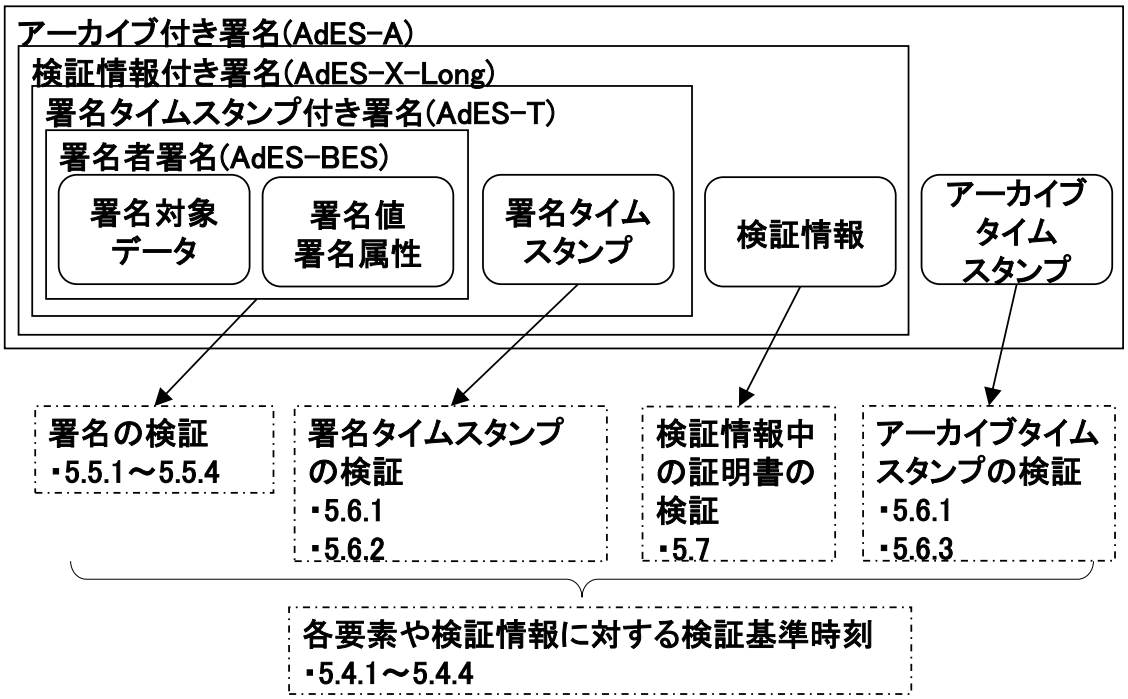

図 5.3.4-1 アーカイブ付き署名(AdES-A)の検証

表 5.3.4-1 アーカイブ付き署名(AdES-A)の規格

署名種別	ベース仕様	プロファイル	該当の署名レベル
CAdES	ETSI EN 319 122-1	ISO 14533-1(ISOプロファイル)	CAdES-A
		ETSI EN 319 122-2(拡張プロファイル)	CAdES-E-A
		ETSI EN 319 122-1(欧州プロファイル)	CAdES-B-LTA
XAdES	ETSI EN 319 132-1	ISO 14533-2(ISOプロファイル)	XAdES-A
		ETSI EN 319 132-2(拡張プロファイル)	XAdES-E-A
		ETSI EN 319 132-1(欧州プロファイル)	XAdES-B-LTA
PAdES	ISO 32000-2	ISO 14533-3(ISOプロファイル)	PAdES-A
	ETSI EN 319 142-1	ETSI EN 319 142-2(拡張プロファイル)	PAdES-E-A
		ETSI EN 319 142-1(欧州プロファイル)	PAdES-B-LTA

5.4 検証基準時刻と検証の観点

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 AdES-BES 検証における検証基準時刻と検証の観点

AdES-BES の生成プロセスと検証プロセスの関係を図 5.4.1-1 図 5.4.1-1 に示す。図 5.4.1-1 の時間軸に沿って生成プロセスと生成されるデータ、検証プロセスを示している。AdES-BES 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。AdES-BES 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 5.4.1-1 に示す。

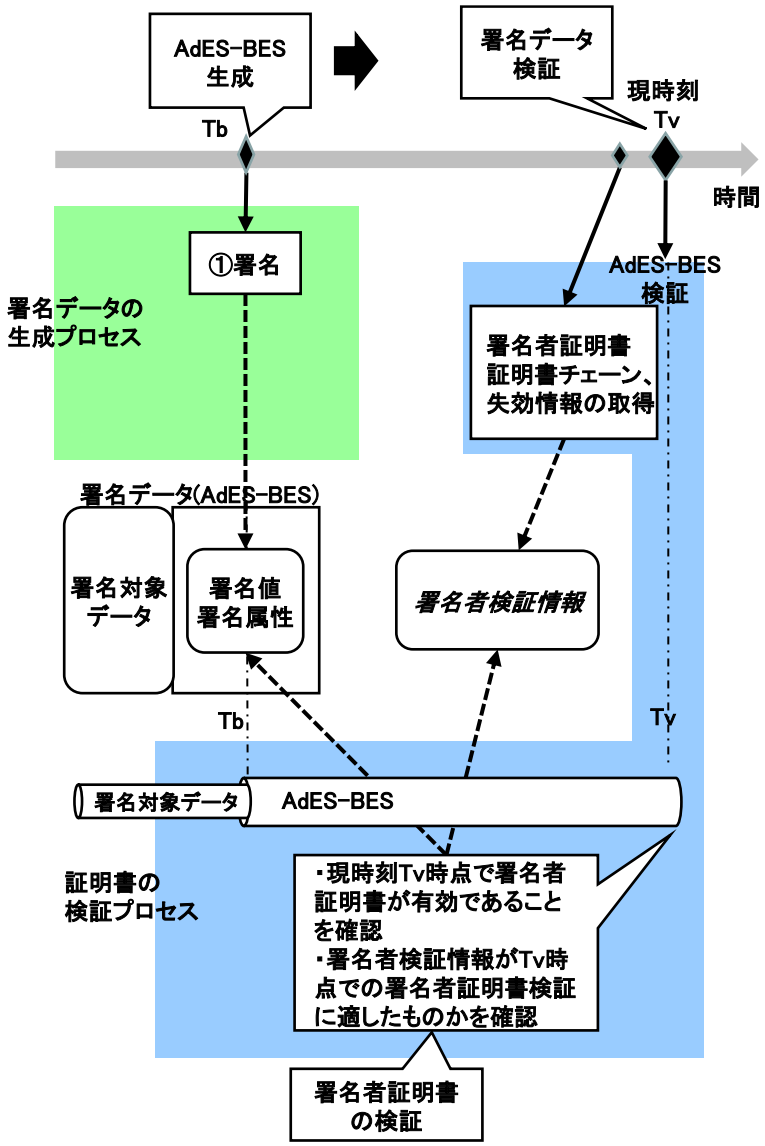

図 5.4.1-1 AdES-BES 生成と検証の関係

表 5.4.1-1 AdES-BES 検証における検証基準時刻と検証の観点

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・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 AdES-T 検証における検証基準時刻と検証の観点

AdES-T の生成プロセスと検証プロセスの関係を図 5.4.2-1 に示す。図 5.4.2-1 の時間軸に沿って生成プロセスと生成されるデータ、検証プロセスを示している。AdES-T 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 5.4.2-1 に示す。

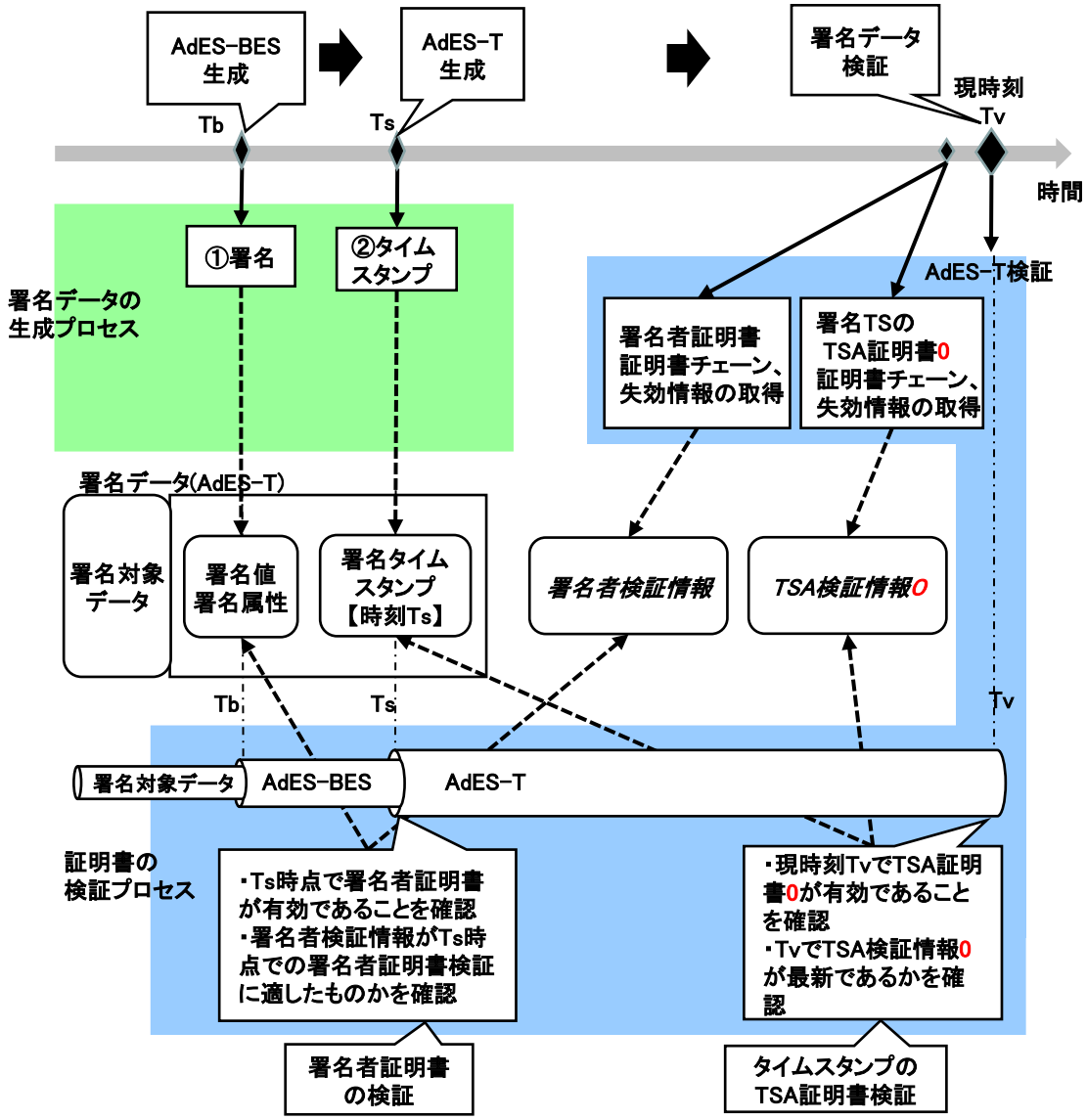

図 5.4.2-1 AdES-T 生成と検証の関係

表 5.4.2-1 AdES-T 検証における検証基準時刻と検証の観点

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
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。 ・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。 ・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

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
		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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・証明書が検証基準時刻において失効されていないこと (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。

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
	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。 ・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 ・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。 ・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 AdES-X-Long 検証における検証基準時刻と検証の観点

AdES-X-Long の生成プロセスと検証プロセスの関係を図 5.4.2-1 に示す。図 5.4.2-1 の時間軸に沿って生成プロセスと生成されるデータ、検証プロセスを示している。AdES-X-Long 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 5.4.2-1 に示す。

AdES-X-Long 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。AdES-X-Long は署名タイムスタンプ付き署名(AdES-T)の検証基準時刻と同様に考える。

なお、生成から時間が経過し、格納された検証情報の改ざんの危険性がある場合にはこれをアーカイブ付き署名等に利用することはできない。

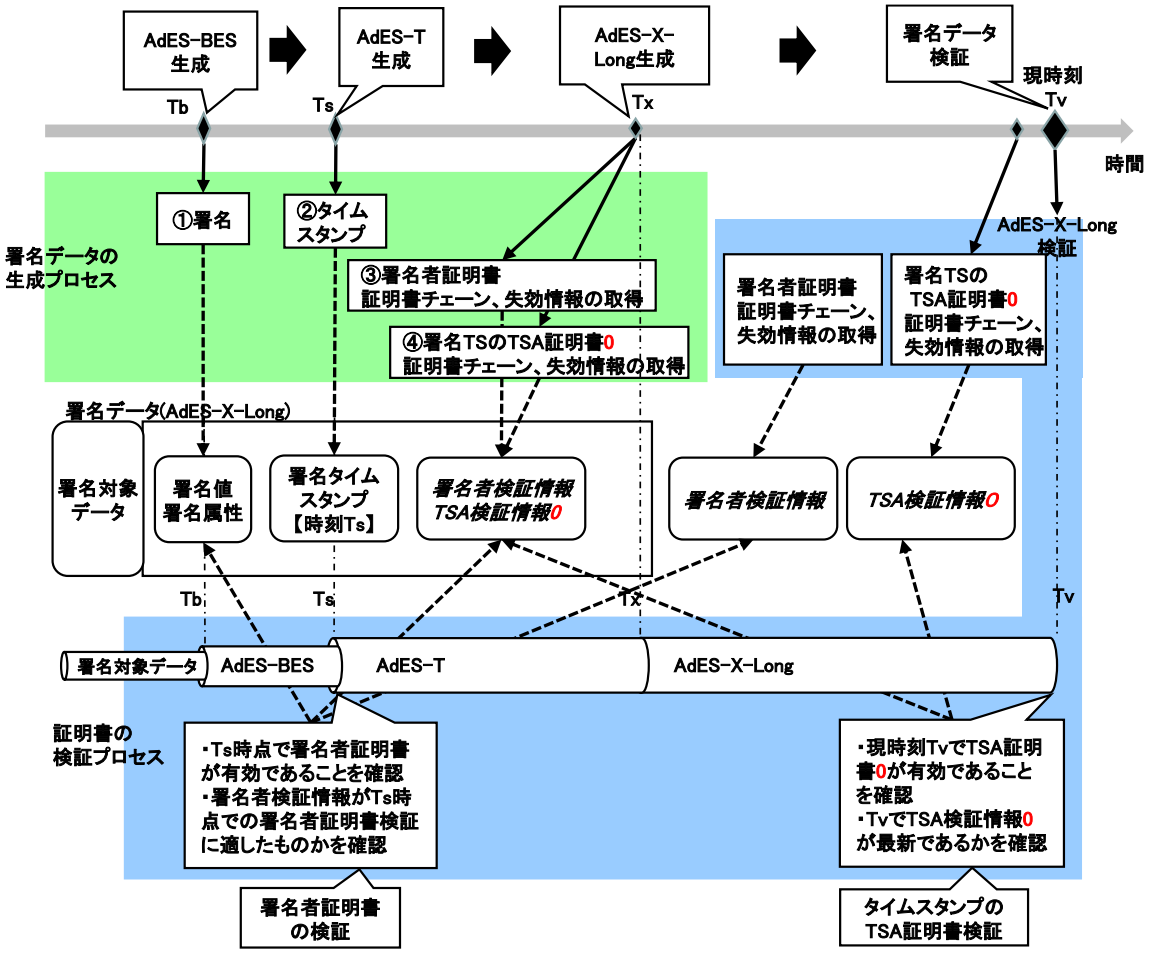

図 5.4.3-1 AdES-X-Long 生成と検証の関係

表 5.4.3-1 AdES-X-Long 検証における検証基準時刻と検証の観点

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
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。 ・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。 ・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	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。 ・証明書の有効期間内に検証基準時刻があ

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
局の証明書		ること ・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。 ・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 ・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。 ・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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・証明書が検証基準時刻において失効されていないこと (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。 ・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

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
		・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 ・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。 ・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 AdES-A 検証における検証基準時刻と検証の観点

AdES-A の生成プロセスと検証プロセスの関係を図 5.4.4-1 に示す。図 5.4.4-1 の時間軸に沿って生成プロセスと生成されるデータ、検証プロセスを示している。AdES-A 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 5.4.4-1 に示す。

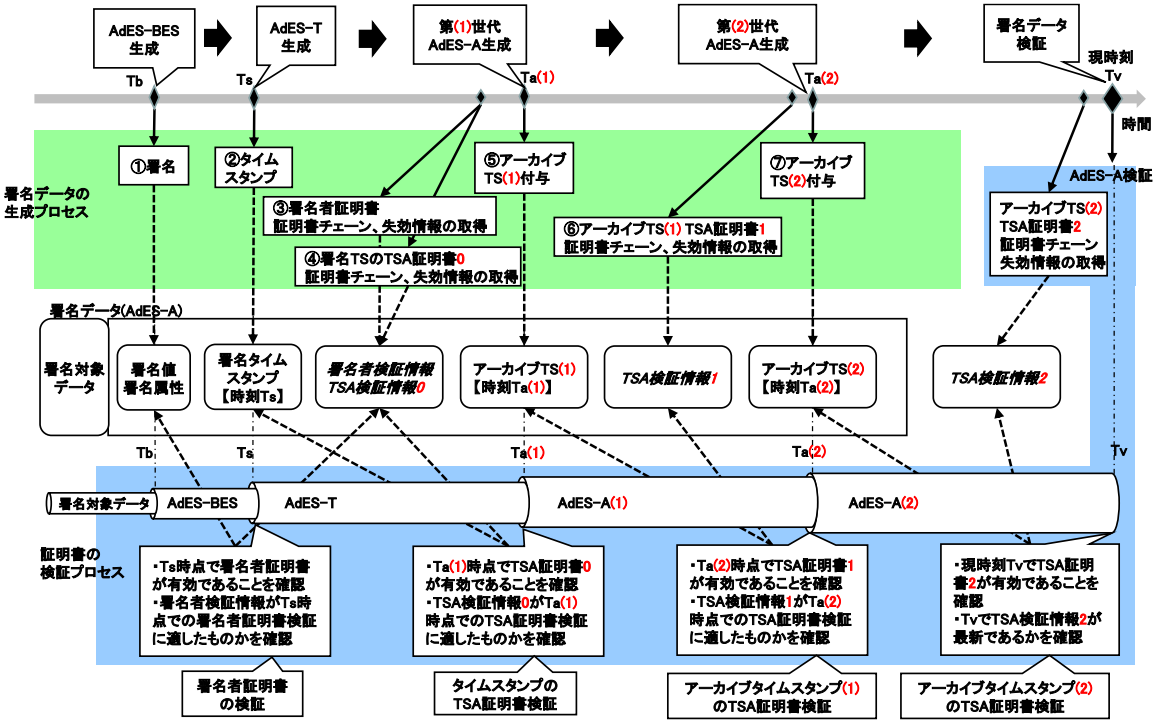

図 5.4.4-1 AdES-A 生成と検証の関係

表 5.4.4-1 AdES-A 検証における検証基準時刻と検証の観点

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
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。 ・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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・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。 ・検証基準時刻において安全であると考え

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
		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。 ・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	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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・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

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
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。 ・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。 ・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	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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・検証基準時刻において安全であると考え

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
		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。 ・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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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	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

検証対象の分類	検証対象の項目	検証基準時刻と検証の観点
	ズム、鍵長	う。 ・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。 ・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。 ・証明書の有効期間内に検証基準時刻があること ・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。 ・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 ・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。 ・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又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 5.5.1-1 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 ・脆弱化した時刻 ・脆弱性の内容
	署名アルゴリズム及び鍵長	検証基準時刻においてアルゴリズム又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 ・脆弱化した時刻 ・脆弱性の内容

M/E/O: Mandatory/mandatory if Exists/Optional

5.5.2 CAdES の検証要件

CAdES 署名は、検証基準時刻において次の検証要件に従い検証する。

表 5.5.2-1 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 5.5.2-2 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 ・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	

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	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 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 2) signedAttrs フィールドの MessageDigest の値	M	VALID	・判定結果
				INVALID	・判定理由 ・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 1) issuerAndSerialNumber の発行者とシリアル番号 2) subjectKeyIdentifier の主体者公開鍵識別子	M	VALID	・判定結果
				INVALID	・判定理由 ・不一致内容

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
	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 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 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 ・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 ・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: Mandatory/mandatory if Exists/Optional

表 5.5.2-2 署名データの構成要素（CAdES）

ASN.1 表記	要素	M/O		
		CAdES-BES	CAdES-T	CAdES-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

ASN.1 表記	要素	M/O		
		CAdES-BES	CAdES-T	CAdES-A
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	署名ポリシー識別子	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

ASN.1 表記	要素	M/O		
		CAdES-BES	CAdES-T	CAdES-A
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、検証基準時刻において次の検証要件に従い検証する。

表 5.5.3-1 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 5.5.3-2 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

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
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 ・SigningTime 要素 ・SignerRole 要素 ・SignatureProductionPlace 要素	O	VALID	・判定結果 ・オプション情報
				INVALID	・不正内容 ・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 1) SigningCertificateV2 (SigningCertificate) 要素 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
	署名者証明書の実体確認	CertificateValues 要素か KeyInfo 要又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	M	VALID	・判定結果
				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	M	VALID	・判定結果 ・証明書情報

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
		1) SigningCertificateV2(SigningCertificate)要素の IssuerSerialV2(IssuerSerial)要素と署名者証明書の Issuer と Serial Number が一致していること 2) SigningCertificateV2(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 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 ※ SigningCertificateV2(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である。		INVALID	・不正内容 ・証明書情報 ・DigestValue 要素 ・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	次の 2 つの値が一致すること	M	VALID	・判定結果 ・全参照 URL

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
		1) Reference 要素により参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 2) DigestValue 要素の値		INVALID	・不正参照 URI ・計算ハッシュ値 ・DigestMethod 要素 ・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 に従って正規化を行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 ・CanonicalizationMethod 要素 ・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: Mandatory/mandatory if Exists/Optional

表 5.5.3-2 署名データの構成要素（XAdES）

XML 表記	要素	M/O		
		XAdES-BES	XAdES-T	XAdES-A
ds:Signature	署名	M	M	M
Id (attribute of ds:Signature)	Signature 要素 Id 属性	M	M	M

XML 表記	要素	M/O		
		XAdES-BES	XAdES-T	XAdES-A
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:SigningCertificateV2 (xa:SigningCertificate)	署名者証明書の参照情報	O (a)	O (a)	O (a)
xa:SignaturePolicyIdentifier	署名ポリシー識別子	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

XML 表記	要素	M/O		
		XAdES-BES	XAdES-T	XAdES-A
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	-	-	O

XML 表記	要素	M/O		
		XAdES-BES	XAdES-T	XAdES-A
	ェクトのプロパティ群			
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:SigningCertificateV2(xa:SigningCertificate)、又は 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: Mandatory/mandatory if Exists/Optional

【コラム５】

■XAdES バージョン定義と規格

XAdES のバージョンは XML 名前空間（namespace）で指定され、その定義は ETSI TS 101 903 となる。2002 年 2 月に ETSI TS 101 903 V1.1.1 が公開された後で、V1.2.2、V1.3.2、V1.4.1 と合計 4 つのバージョンがある。このうち V1.1.1 と V1.2.2 は、V1.3.2 以降との互換性が無い為に利用してはいけない。V1.4.1 は V1.3.2 がベースとなり、追加要素を加えたものである。その為に V1.4.1 を利用する場合に正確には V1.4.1＋V1.3.2 の要素が必要となる。ETSI TS 101 903 以外の規格ではどの XAdES バージョンを利用しているかをよく理解して利用する必要がある。特に W3C Note は V1.1.1 のままであり使ってはいけない。ETSI EN 319 132-1 V1.1.0 (2016-04) が ETSI 最新の仕様ではあるが、XAdES バージョンとしては V1.4.1 である。

Version	定義と XML 名前空間（2 行目）	ETSI TS 以外の採用規格
V1.1.1 (非推奨)	ETSI TS 101 903 V1.1.1 (2002-02) https://uri.etsi.org/01903/v1.1.1/	W3C Note 20 February 2003 https://www.w3.org/TR/XAdES/
V1.2.2 (非推奨)	ETSI TS 101 903 V1.2.2 (2004-04) https://uri.etsi.org/01903/v1.2.2/	（無し）

V1.3.2	ETSI TS 101 903 V1.3.2 (2006-03) https://uri.etsi.org/01903/v1.3.2/	ISO 14533-2:2012 https://www.iso.org/standard/79129.html
		JIS X 5093:2008
V1.4.1 + (V1.3.2)	ETSI TS 101 903 V1.4.1 (2009-06) https://uri.etsi.org/01903/v1.4.1/	ETSI EN 319 132-1 V1.1.0 (2016-04)
		ISO/DIS 14533-2:2021 https://www.iso.org/standard/79129.html

【コラム６】

■XAdES の SigningCertificate 要素と SigningCertificateV2 要素

XAdES の SigningCertificateV2 要素は ETSI EN 319 132-1 V1.1.0 (2016-04) から追加された新しい要素であるが名前空間は V1.3.2 となっている。これは SigningCertificateV2 要素が、ETSI TS 101 903 V1.3.2 (2006-03) で定義されていた SigningCertificate 要素をそのまま置き換える目的の為に追加された要素であるからである。

従来の IssuerSerial 要素下の X509IssuerName 要素では、署名証明書（X.509 バイナリ）の Issuer 部からテキスト形式（RFC 2253 準拠）に変換した識別名を利用していた。しかしながら色々な事情がありこの識別名が一意にならない問題があった。この為に SigningCertificate/IssuerSerial/X509IssuerName を使った検証を行わない検証器がほとんどであった。

SigningCertificateV2 要素では新たに IssuerSerialV2 要素として、Issuer と Serial を、署名証明書（X.509 バイナリ）からバイナリ（ASN.1/DER）のまま抜き出して結合する方式となった。これにより SigningCertificateV2 要素を使うことで Issuer（発行者）名が一意となるので間違いなく検証が出来るようになった。

以上から過去互換性の為に SigningCertificate 要素を使い続けることに問題は無いが、新しく実装する場合には SigningCertificateV2 要素が推奨される。欧州 eIDAS へ準拠する場合には SigningCertificateV2 要素が必須となる。検証器を実装する場合には両方に対応出来るようにすることが推奨される。

5.5.4 PAdES の検証要件

CAdES/XAdES は検証に必要又は関連する要素は基本的に署名フォーマットの中にある。しかしながら PAdES は基本的には必要とする要素は PDF フォーマットの中にあり、かつシリアル署名（複数署名）の仕様を利用して長期署名を実現している。この点が CAdES/XAdES と大きく異なり、検証方法や検証手順も異なってくる。

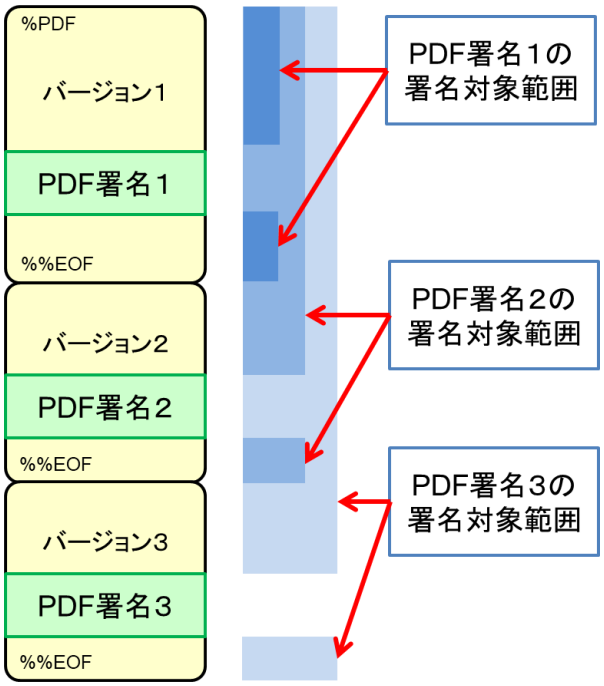

図 5.5.4-1 PAdES（PDF 署名）のシリアル署名構造

PAdES は PDF に埋め込む署名辞書として、署名（CAdES と PKCS#7 の 2 種類があり、/Type エントリーが /Sig）と、タイムスタンプトークン（ドキュメントタイムスタンプと呼ばれ、/Type エントリーが /DocTimeStamp）の 2 種類が利用可能となっている。署名には CAdES 署名と、過去の PDF 署名に対する後方互換性のために PKCS#7 署名も利用可能ではあるが、PKCS#7 署名は本書では扱わない。ただし基本的には PKCS#7 署名は CAdES 署名と同じと考えてよい。なおドキュメントタイムスタンプに関しては「5.6.4 ドキュメントタイムスタンプ」を参照。

PDF ファイル内に複数の署名辞書が存在する場合には個別に検証を行う必要がある。検証時にはその署名辞書の外（増分更新された場所）にタイムスタンプ（DocTimeStamp か CAdES-T）が存在した場合には、その署名辞書の検証には、外にある最も近いタイムスタンプ時刻を検証基準時刻として使う。署名辞書の外にタイムスタンプがない場合には現在時刻を検証基準時刻とする。なお PAdES の複数署名に関しては「B.2 PAdES 複数署名」を参照。

PAdES では PDF に埋め込む検証情報（証明書群と失効情報群）用の辞書として、DSS 辞書と VRI 辞書がある。検証のために利用可能な証明書や失効情報は CAdES データやタイムスタンプトークンにも埋め込むことが可能であるが、DSS 辞書/VRI 辞書に含まれる検証情報の優先度が高い。なお検証情報は外部から与えてもよい。

表 5.5.4-1 PAdES 関連 PDF 辞書の種類（PAdES）

種類	/Type エントリー	/SubFilter エントリー	備考
CAdES 署名辞書	/Sig	/ETSI.CAdES.detached	ISO 32000-2 定義（推奨） CAdES-BES か CAdES-T を指定可 Root / AcroForm / Fields / V から参照
PKCS7 署名辞書	/Sig	/adbe.pkcs7.detached /adbe.pkcs7.sha1	ISO 32000-1 定義（過去互換性） PKCS#7 形式でタイムスタンプ追加可 Root / AcroForm / Fields / V から参照 ※ 本書の対象外
DocTimeStamp 署名辞書	/DocTimeStamp	/ETSI.RFC3161	ISO 32000-2 定義 単独タイムスタンプ（RFC 3161） Root / AcroForm / Fields / V から参照
DSS 辞書	/DSS	（なし）	ISO 32000-2 定義（LTV 必須） 全体の検証情報：証明書/CRL/OCSP Root / DSS から参照
VRI 辞書	/VRI	（なし）	ISO 32000-2 定義（オプション） 署名ごとの検証情報：証明書/CRL/OCSP DSS から参照（Root / DSS / VRI）

PAdES とは本来長期署名の仕様ではあるが、PAdES を構成する CAdES 署名・ドキュメントタイムスタンプ・検証情報（DSS/VRI 辞書）は自由に組み合わせることが可能となる（PDF 仕様として自由な組み合わせが許されている）。またタイムスタンプとしては、CAdES に署名タイムスタンプ（CAdES-T）として埋め込む方法と、ドキュメントタイムスタンプ（DocTimestamp）として埋め込む方法の 2 種類がある。このために長期署名の AdES-BES・AdES-T・AdES-X-Long・AdES-A と言う署名レベル作成の流れが保証されるとは限らない。PDF の内部構造を解析して署名ごとに署名レベルを確認して検証を行う必要がある。特に CAdES 署名をせずにドキュメントタイムスタンプだけを付与する PAdES-DT 仕様（ISO 14533-3 Annex B.2）は、PAdES のみとなる。ドキュメントタイムスタンプに関しては「5.6.4 ドキュメントタイムスタンプ」を参照。

表 5.5.4-2 PAdES 辞書（PAdES）

PDF 辞書	要素	M/O			
		PAdES -BES	PAdES -T	PAdES -X-Long	PAdES -A
CAdES 署名辞書	CAdES-BES	M	M	M	M
CAdES-T	CAdES-T 埋め込みタイムスタンプ	-	M	M	M
DSS/VRI 辞書	検証情報 証明書と失効情報	-	-	M	M
DocTimeStamp 辞書	タイムスタンプのみ	-	M	-	M

M/O: Mandatory/Optional

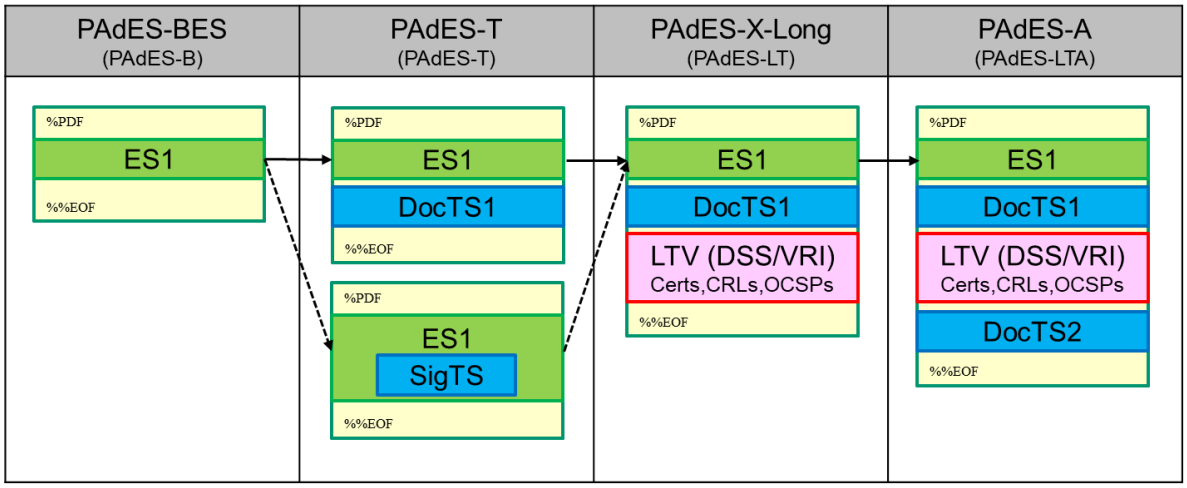

図 5.5.4-2 PAdES の署名レベル遷移

PAdES 署名は、検証基準時刻において次の検証要件に従い検証する。

表 5.5.4-3 検証要件（PAdES 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	PAdES 必須要素	表 5.5.4-4 の CAdES 署名辞書の必須要素が含まれること	M	VALID	・判定結果
				INVALID	・含まれていない必須要素
オプション要素	PAdES オプション要素	CAdES 署名辞書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	O	VALID	・判定結果 ・オプション情報

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
		・Name エントリー ・M エントリー		INVALID	・不正内容 ・不正項目の情報
CAdES 署名辞書	CAdES データ検証	CAdES 署名辞書の Contents エントリーに含まれる CAdES データが正しく検証できること	M	5.5.2 を参照	
	ByteRange 範囲のハッシュ値との比較	CAdES の Detached ハッシュ値と ByteRange 範囲から計算したハッシュ値が一致すること	M	VALID	判定結果
				INVALID	不正内容
DocTimeStamp 署名辞書	タイムスタンプトークン検証	DocTimeStamp 署名辞書の Contents エントリーに含まれるタイムスタンプトークンデータが正しく検証できること	M	5.6.1 を参照	
	ByteRange 範囲のハッシュ値との比較	タイムスタンプトークンのハッシュ値(MessageImprint)と ByteRange 範囲から計算したハッシュ値が一致すること	M	VALID	判定結果
				INVALID	不正内容
検証情報	検証情報の過不足	CAdES 署名辞書に含まれる署名証明書と、DocTimeStamp 署名辞書に含まれる TSA 証明書の検証に必要となる証明書と失効情報(CRL/OCSP)が取得できること 失効情報(OCSP/CRL)は CAdES データ内の revocationInfoArchival 属性(OID:1.2.840.113583.1.1.8)も参照することを推奨	M	VALID	・判定結果
				INVALID	・不正内容

M/E/O: Mandatory/mandatory if Exists/Optional

表 5.5.4-4 CAdES 署名辞書の構成要素（PAdES）

キー		種別	値	備考	M/O/P
/Type		Name	/Sig	省略時のデフォルトは /Sig	O
/Filter		Name	---	検証時の優先署名ハンドラの名前	M

キー		種別	値	備考	M/O/P
				※ アドビ社の標準は /Adobe.PPKLite ※ 署名ハンドラは登録が必要	
/SubFilter		Name	/ETSI.CAdES.detached	固定	M
/Contents		hex string	---	CAdES-BES か CAdES-T を大文字 Base16（HEX/16 進文字列）として格納。なお 0 でパディングしてよい。 ※ 詳細は「5.5.2 CAdES の検証要件」 ※ PDF 独自の revocationInfoArchivalz 属性（OID: 1.2.840.113583.1.1.8）を使って失効情報の埋め込みが可能。 ※ PDF 暗号化してはいけない	M
/ByteRange		Array	[start1 len1 start2 len2]	署名対象から Contents キー部を除いた範囲を指定（開始 1/長さ 1/開始 2/長さ 2）	M
/Cert		Array	---	署名辞書の証明書エントリーは使ってはいけない、存在しても無視する	P
/Name		Text	---	署名者名	O
/M		Date	---	署名時刻：ISO/IEC 8824 の ASN.1 形式（D:YYYYMMDDHHmmSSOHH’mm’） ※ 検証時の時刻に利用してはいけない	O
/Location		Text	---	署名場所	O
/Reason		Text	---	署名理由	O
/ContactInfo		Text	---	署名者へのコンタクト情報	O

M/O/P: **M**andatory/**O**ptional/**P**rohibited

表 5.5.4-5 DocTimeStamp（DTS）署名辞書の構成要素（PAdES）

キー	種別	値	備考	M/O/P
/Type	name	/DocTimeStamp	DocTimeStamp のときは必須	M
/Filter	name	---	検証時の優先署名ハンドラの名前 ※ アドビ社の標準は /Adobe.PPKLite ※ 署名ハンドラは登録が必要	M
/SubFilter	name	/ETSI.RFC3161	固定	M
/Contents	hex string	---	タイムスタンプトークンを大文字 Base16（HEX/16 進文字列）として格納。なお 0	M

キー	種別	値	備考	M/O/P
			でパディングしてよい。 タイムスタンプトークンにおける messageImprint フィールドの hashedMessage の値は、ByteRange に指定された範囲のハッシュ値とする。 ※ 詳細は「5.6.1 タイムスタンプ」 ※ PDF 暗号化してはいけない	
/ByteRange	array	[start1 len1 start2 len2]	署名対象から Contents キー部を除いた範囲を指定（開始 1/長さ 1/開始 2/長さ 2）	M
/Cert	array	---	署名辞書の証明書エントリーは使ってはいけない、存在しても無視する。	P
※ DocTimeStamp に Name, M, Location, Reason, ContactInfo キーは指定すべきではなく、存在したとしても検証時には無視する。				

M/O/P: Mandatory/Optional/Prohibited

表 5.5.4-6 DSS 辞書の構成要素（PAdES）

キー	種別	値	備考	M/O/P
/Type	name	/DSS	省略時のデフォルトは /DSS	O
/VRI	dict	ハッシュ値をキーとして VRI 辞書を値に持つ	Type が Sig の場合にはパディングの 0 も含めた Contents のバイナリの SHA-1 ハッシュ値を、DocTimeStamp の場合にはパディングの 0 を含めない Contents のバイナリの SHA-1 ハッシュ値を、指定	O
/Certs	array	証明書バイナリの配列	全体の検証に利用した証明書群の配列	O
/OCSPs	array	OCSP バイナリの配列	全体の検証に利用した OCSP 群の配列	O
/CRLs	array	CRL バイナリの配列	全体の検証に利用した CRL 群の配列	O

M/O/P: Mandatory/Optional/Prohibited

表 5.5.4-7 VRI 辞書の構成要素（PAdES）

キー	種別	値	備考	M/O/P
/Type	name	/VRI	省略時のデフォルトは /VRI	O
/Cert	array	証明書バイナリの配列	1 署名の検証に利用した証明書群の配列	O
/OCSP	array	OCSP バイナリの配列	1 署名の検証に利用した OCSP 群の配列	O
/CRL	array	CRL バイナリの配列	1 署名の検証に利用した CRL 群の配列	O

キー	種別	値	備考	M/O/P
/TU	date	検証した日時	非推奨、存在しても検証時に無視する	P
/TS	stream	検証した日時のタイムスタンプ	RFC 3161 形式のバイナリストリーム 非推奨、存在しても検証時に無視する	P

M/O/P: **M**andatory/**O**ptional/**P**rohibited

【コラム７】

■PDF バージョンと電子署名

PDF のバージョンは現在 1.0～2.0 までが存在する。1.0～1.7 までは Adobe 社が策定して仕様公開していたがその後 ISO に移管され、ISO 32000-1 で PDF1.7 が正式仕様となり、ISO 32000-2 で PDF2.0 が正式仕様となった。なお PDF 電子署名の仕様は PDF1.3 で追加された。

PDF ファイルではファイルの先頭に PDF バージョンが埋め込まれているが、残念ながらファイル本体の仕様と一致しない場合が多い。PAdES 仕様は PDF2.0（ISO 32000-2）で追加されたが、ファイルの先頭で宣言されるバージョンは PDF1.7 以前の場合もあるが、これは検証エラーの対象とはならない。

PAdES 仕様が ETSI で定義された時には、PDF1.7（ISO 32000-1）をベースとして PAdES 用の新しい仕様を追加したものとなっている。ETSI TS 102 778-1 V1.1.1 と ETSI EN 319 142-1 V1.1.1 はいずれも PDF1.7 プラス PAdES 仕様となっている。その後 PDF2.0(ISO 32000-2) が発行された時に PAdES 仕様も PDF2.0 として吸収された。

規格名	PDF Version	概要
PDF1.7 ISO 32000-1:2008 https://www.iso.org/standard/51502.html	1.7	Adobe 社から ISO に移管され、国際標準化された最初のバージョン
ETSI TS 102 778-1 V1.1.1 (2009-07)	1.7＋PAdES	PAdES 仕様の最初の定義
ETSI EN 319 142-1 V1.1.1 (2016-04)	1.7＋PAdES	eIDAS 向け、ETSI TS 102 778-1 から EU プロファイルを定義
PDF2.0 ISO 32000-2:2017(2020) https://www.iso.org/standard/75839.html	2.0	PAdES 仕様を取り込んだ PDF 正式仕様 PDF 全体仕様であり 1000 ページ近い
ISO 14533-3:2017 https://www.iso.org/standard/67937.html	2.0	ISO 32000-2 を使った PAdES プロファイル

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。ここに示す検証要件は、RFC 5280 X.509 証明書インターネットプロファイル、RFC 5652 CMS、RFC 3161 タイムスタンププロトコルに準じた検証内容であり、本書に固有の検証要件はない。

表 5.6.1-1 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 5.6.1-2 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 ・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

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
	の一致確認	2つの値が一致すること 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 2) signedAttrsフィールドの MessageDigestの値		INVALID	・判定理由 ・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 1) 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 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 ・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

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 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 2) MessagaeImprint の hashMessage の値	M	VALID	・判定結果
				INVALID	・判定理由 ・各ハッシュ値

M/E/O: Mandatory/mandatory if Exists/Optional

表 5.6.1-2 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	

ASN.1 表記	要素	M/O	備考
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	

ASN.1 表記	要素	M/O	備考
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: Mandatory/Optional

5.6.2 署名タイムスタンプ

(1) 署名タイムスタンプの検証基準時刻

もし電子署名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又は現在時刻を利用する。詳しくは 5.4 を参照。

(2) 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 5.6.2-1 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	

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 CAdES は表 5.6.2-2 参照 XAdES は表 5.6.2-3 参照 PAdES は表 5.6.2-4 参照	M	VALID	・判定結果
				INVALID	・タイムスタンプ MessageImprint 値 ・計算したハッシュ値 ・ダイジェストアルゴリズム

M/E/O: Mandatory/mandatory if Exists/Optional

表 5.6.2-2 CAdES 署名タイムスタンプ対象データのハッシュ算出手段

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 5.6.2-3 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

表 5.6.2-4 PAdES 署名タイムスタンプ対象データのハッシュ算出手段

PAdES 署名タイムスタンプ対象データのハッシュ算出手段
DocTimeStamp の仕様に従ってハッシュ値を算出する ※「表 5.6.4-1 PAdES-DT 検証要件（PAdES）」を参照。

5.6.3 アーカイブタイムスタンプ

(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又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。

(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 5.6.3-1 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 CAdES は表 5.6.3-2 参照 XAdES は表 5.6.3-3 参照 PAdES は表 5.6.3-4 参照	M	VALID	・判定結果
				INVALID	・タイムスタンプ MessageImprint 値 ・計算したハッシュ値 ・ダイジェストアルゴリズム

M/E/O: Mandatory/mandatory if Exists/Optional

表 5.6.3-2 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

関連規格の種類	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
archivetimestamp（RFC3126, ETSI TS 101 733 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。 ・encapContentInfo eContent の OCTET STRING ・signedAttributes ・SignerInfo の signature フィールド ・SignatureTimeStamp 属性 ・CompleteCertificateRefs 属性 ・CompleteRevocationRefs 属性 ・CertificateValues 属性 ・RevocationValues 属性 ・ESCTimeStampToken 属性（存在する場合） ・TimestampedCertsCRLs 属性（存在する場合） ・最古から検証対象までの一連の ArchiveTimeStamp（昇順）
archivetimestamp V2（ETSI TS 101 733 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。 ・singedData に含まれる encapContentInfo ・外部の署名対象のデータ（encapContentInfo の eContent が省略された場合） ・signedData に含まれる certificates と crls フィールド（存在する場合） ・signerInfo に含まれる全ての要素(※1)

関連規格の種類	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
	※1 unsignedAttrs（非署名属性）は、次の条件で再構成する。 - 検証対象以降の ArchiveTimeStamp を除く。 - 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。
archivetimestamp V3（EN 319 122-1 Ver. 1.1.1)	以下の手順でハッシュ値を算出する。 i) ats-hash-index-v3 属性の作成 アーカイブタイムスタンプ対象の署名データ(signedData)から以下の要素を含んだ ats-hash-index-v3 属性を作る。この ats-hash-index-v3 属性は ii)で作成する archive-time-stamp-v3 属性のタイムスタンプトークンの unsignedAttrs に格納される。 ・certificatesHashIndex signedData.certificates のそれぞれの要素(CertificateChoices のインスタンス)のハッシュ値から成るシーケンス ・crlsHashIndex signedData.crls のそれぞれの要素(RevocationChoices のインスタンス)のハッシュ値から成るシーケンス ・unsignedAttrValuesHashIndex unsigndAttrs のそれぞれの属性の attrType と attrValues の AttributeValue インスタンスを連携したオクテット列に対するハッシュ値から成るシーケンス ii) アーカイブタイムスタンプ対象ハッシュ値(message imprint)の算出 以下の要素のバイナリエンコーディング（修正を加えず、tag, length, value を含む）を順に連結し、message imprint のハッシュ値を算出する。 ● signedData.encapContentInfo.eContentType ● 署名対象コンテンツ（署名時の message-digest 属性でハッシュ計算の元となった対象と同じもの）から算出したハッシュ値 ● アーカイブタイムスタンプ対象の signerInfo の version, sid, digestAlgorithm, signedAttrs, signatureAlgorithm,signature（登場順） ● i)で作成した ats-hash-index-v3 属性 iii) archive-time-stamp-v3 属性の作成 ii)で算出した message imprint に対してタイムスタンプを付与し、そのタイムスタンプトークンを元に archive-time-stamp-v3 属性を作成する。同タイムスタンプトークンの unsignedAttrs に i)の ats-hash-index-v3 属性を格納する。 ※V3 以前のバージョンのアーカイブタイムスタンプを含む場合など、上記では割愛

関連規格の種類	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
	した詳細な規定については左記規格を参照のこと。

表 5.6.3-3 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

関連規格の種類	XAdES アーカイブタイムスタンプ（Not distributed case）	
XAdES V1.3.2 ※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 ・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 ・SignedInfo 要素（必須） ・SignatureValue 要素（必須） ・KeyInfo 要素（存在するときのみ）
	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 ・SignatureTimeStamp 要素（必須） ・CounterSignature 要素（存在するときのみ） ・CompleteCertificateRefs 要素（存在するときのみ） ・CompleteRevocationRefs 要素（存在するときのみ） ・AttributeCertificateRefs 要素（存在するときのみ） ・AttributeRevocationRefs 要素（存在するときのみ） ・CertificateValues 要素（必須） ・RevocationValues 要素（必須） ・SigAndRefsTimeStamp 要素（存在するときのみ） ・RefsOnlyTimeStamp 要素（存在するときのみ） ・ArchiveTimeStamp 要素（計算対象より内側に存在するときのみ）
	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
XAdES V1.4.1 ※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 ・全 Reference 要素（必須：SingedInfo 内の出現順）

関連規格の種類	XAdES アーカイブタイムスタンプ（Not distributed case）	
	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 ・SignedInfo 要素（必須） ・SignatureValue 要素（必須） ・KeyInfo 要素（存在するときのみ）
	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
※1 XAdES V1.3.2 の XML 名前空間名は https://uri.etsi.org/01903/v1.3.2/ ※2 XAdES V1.4.1 の XML 名前空間名は https://uri.etsi.org/01903/v1.4.1/		

表 5.6.3-4 PAdES 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

PAdES 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
DocTimeStamp の仕様に従ってハッシュ値を算出する ※「表 5.6.4-1 PAdES-DT 検証要件（PAdES）」を参照。

5.6.4 ドキュメントタイムスタンプ

ドキュメントタイムスタンプはPDFのようなドキュメントに対してタイムスタンプのみを署名とは別に付与する方式のタイムスタンプである。執筆時点においてはPAdESのDocTimeStamp（PAdES-DT）仕様のみとなる。PAdESのDocTimeStampは、PAdES-TやPAdES-Aでは署名タイムスタンプ的にもアーカイブタイムスタンプ的としても利用が可能である。ここでは署名抜きでドキュメントタイムスタンプを利用するPAdES-DT仕様（ISO 14533-3 Annex B.2）について解説する。

PAdES-DT仕様も長期署名化（LTA化）による有効期限の延長が可能となっている。CAdES署名の代わりにDocTimeStampのみを指定した後で、DSS/VRI辞書とアーカイブタイムスタンプとしてのDocTimeStampを追加することで長期署名化が可能となる。DocTimeStamp署名辞書とDSS/VRI辞書に関しては「5.5.4 PAdESの検証要件」を参照。

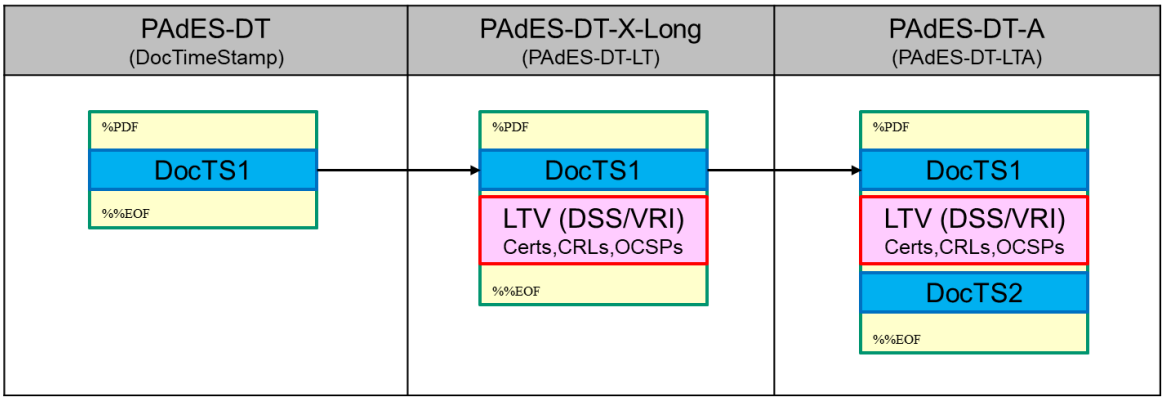

図 5.6.4-1 DocTimeStamp（PAdES-DT）の署名レベル遷移

表 5.6.4-1 PAdES-DT 検証要件（PAdES）

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	PAdES-DT 必須要素	表5.5.4-5のDocTimeStamp署名辞書の必須要素が含まれること	M	VALID	・判定結果
				INVALID	・含まれていない必須要素
オプション要素	PAdES-DT オプション要素	DocTimeStamp 署名辞書に Name, M, Location, Reason, ContactInfo エントリー要素が含まれないこと	O	VALID	・判定結果 ・オプション情報
				WARNING	・不正内容 ・不正項目の情報
DocTimeStamp 署名辞書	タイムスタンプトークン検証	DocTimeStamp 署名辞書の Contentsエントリーに含まれるタイムスタンプトークンデータが正しく検証できること	M	5.6.1 を参照	
	ByteRange範囲のハッシュ値との比較	タイムスタンプトークンのハッシュ値(MessageImprint)と ByteRange 範囲から計算したハッシュ値が一致すること	M	VALID	判定結果
				INVALID	不正内容
検証情報	検証情報の過不足	DocTimeStamp署名辞書に含まれる TSA 証明書の検証に必要となる証明書と失効情報（CRL/OCSP）が取得できること	M	VALID	・判定結果
				INVALID	・不正内容

M/E/O: Mandatory/mandatory if Exists/Optional

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、それらを確認するときに利用する検証基準時刻は署名フォーマット形式（AdES-BES、AdES-T、AdES-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とおりである。

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 AdES-BESにおける証明書

AdES-BES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。

なお、図中の「証明書検証のための初期値と取得情報」には、証明書失効情報、証明書ポリシー制約処理のための初期値、名前制約のための初期値等を含む。(以後同様)

- 署名者証明書
  - 表 5.7.1-1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 5.7.1-2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。

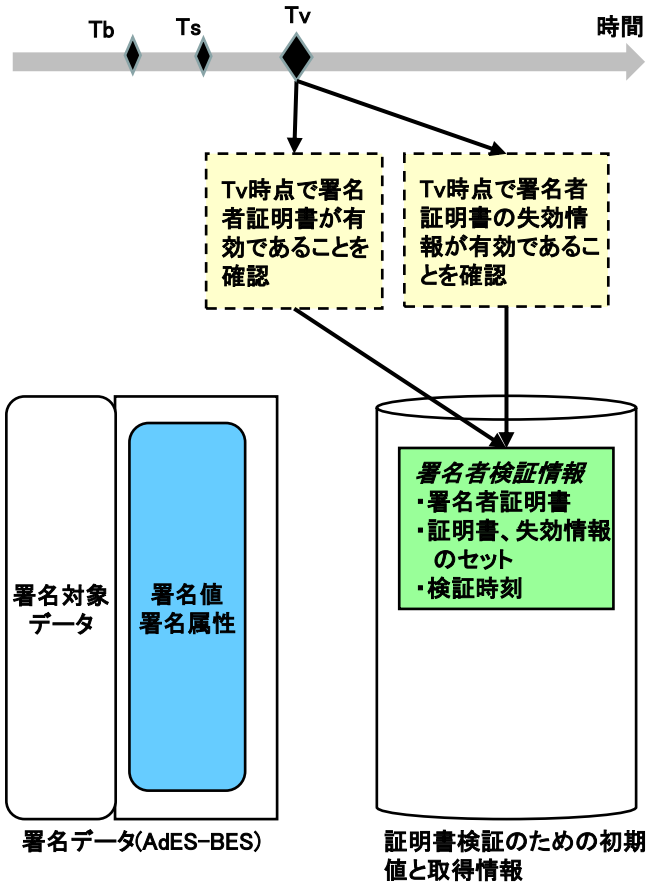

図 5.7.1-1 AdES-BES における証明書検証と検証基準時刻の関係

表 5.7.1-1 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 ・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 ・検証基準時刻 ・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

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
		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 ・証明書又は失効情報
	失効確認	失効していない	M	VALID	・判定結果 ・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 ・検証基準時刻 ・失効理由 ・失効時刻 ・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 ・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 ・検証基準時刻 ・証明書パス
		証明書が有効期間前である		INVALID	・失敗理由 ・検証基準時刻 ・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 ・証明書又は失効情報 ・危殆化したアルゴリズム
失効情報	**【AdES-T、AdES-A の場合のみ】**失効情報の妥当性	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

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
	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ない		INDETERMINATE	・未確定理由 ・検証基準時刻 ・失効情報

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

表 5.7.1-2 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 ・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 ・検証基準時刻 ・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 ・証明書または失効情報
	失効確認	失効していない	M	VALID	・判定結果 ・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 ・検証基準時刻 ・失効理由 ・失効時刻 ・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
	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 ・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 ・検証基準時刻 ・証明書パス
		証明書が有効期間前である		INVALID	・失敗理由 ・検証基準時刻 ・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 ・証明書又は失効情報 ・危殆化したアルゴリズム

M/E/O: Mandatory/mandatory if Exists/Optional

5.7.2 AdES-T における証明書

AdES-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 5.7.1-1 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 5.7.1-2 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 5.7.2-1 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。

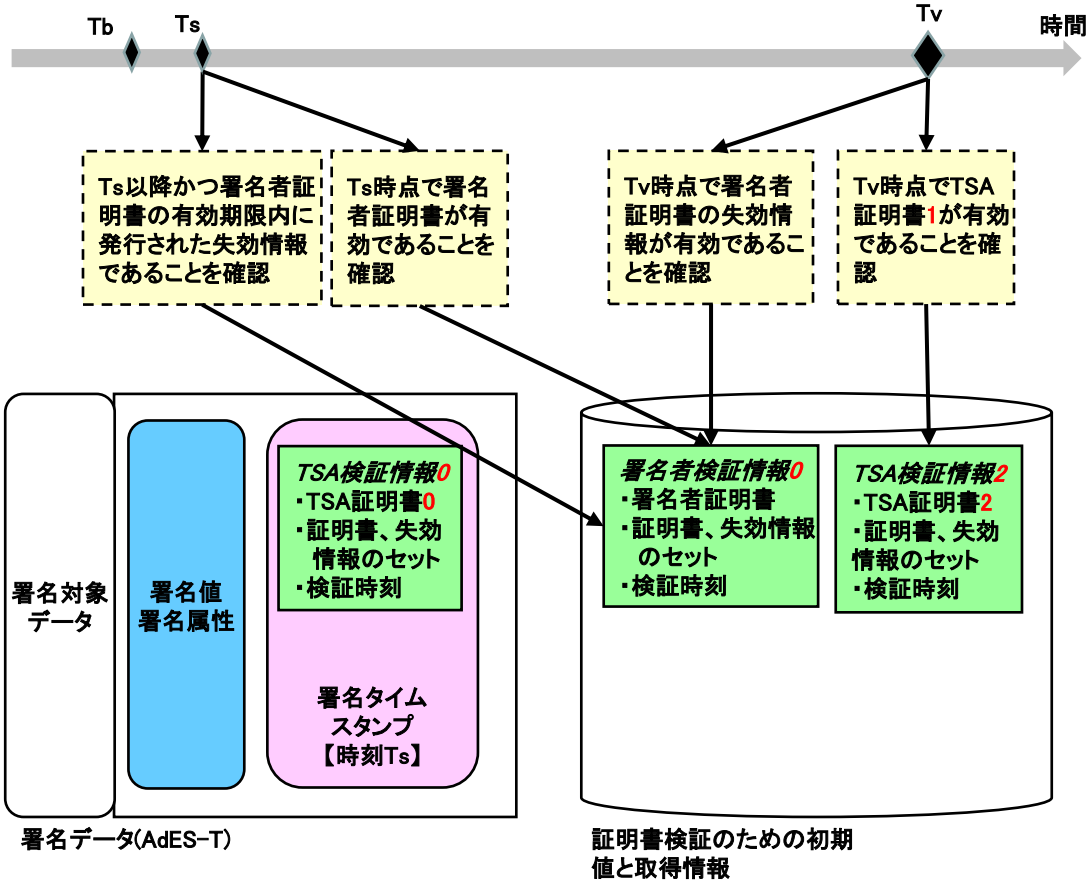

図 5.7.2-1 AdES-T における証明書検証と検証基準時刻の関係

表 5.7.2-1 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 ・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

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
		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 ・検証基準時刻 ・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 ・証明書又は失効情報
	失効確認	失効していない	M	VALID	・判定結果 ・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 ・検証基準時刻 ・失効理由 ・失効時刻 ・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 ・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 ・検証基準時刻 ・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
		証明書が有効期間前である		INVALID	・失敗理由 ・検証基準時刻 ・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 ・証明書又は失効情報 ・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 ・検証基準時刻 ・失効情報

M/E/O: Mandatory/mandatory if Exists/Optional

5.7.3 AdES-A における証明書

AdES-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 5.7.1-1 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 5.7.1-2 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 5.7.2-1 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 5.7.2-1 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。

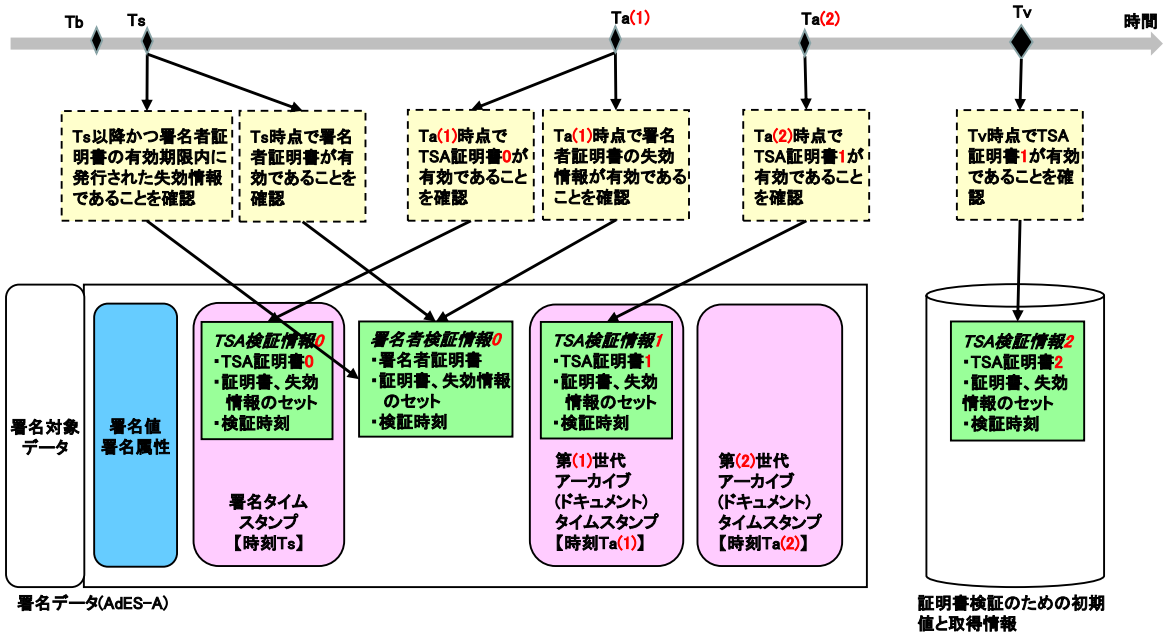

図 5.7.3-1 AdES-A における証明書検証と検証基準時刻の関係（第 2 世代の場合）

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。

タイトル	版番号/発行日
デジタル署名検証ガイドライン	第X.X版/2021-xx-xx

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 5.5.1-1 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		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
暗号アルゴリズム	ダイジェストアルゴリズム	M		VALID	
				INVALID	
	署名アルゴリズム及び鍵長	M		VALID	
				INVALID	

M/E/O: Mandatory/mandatory if Exists/Optional

A.4.1.2 タイムスタンプの検証要件

参照：表 5.6.1-1 検証要件（タイムスタンプ）

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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: Mandatory/mandatory if Exists/Optional

A.4.1.3 署名タイムスタンプの検証要件

参照：表 5.6.2-1 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		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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: Mandatory/mandatory if Exists/Optional

A.4.1.4 アーカイブタイムスタンプの検証要件

参照：表 5.6.3-1 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		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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: Mandatory/mandatory if Exists/Optional

A.4.2 CAdES 検証

A.4.2.1 CAdES の検証要件

参照：表 5.5.2-1 検証要件（CAdES 署名）

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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	M		VALID	
				INVALID	

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
	シュ値の一致確認				
	SigningCertificate 属性における署名者証明書のハッシュ値の一致確認	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: Mandatory/mandatory if Exists/Optional

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 5.6.2-2 CAdES 署名タイムスタンプ対象データのハッシュ算出手段

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 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 5.6.3-2 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

関連規格の種類	実装 (Y/N)
archivetimestamp	
archivetimestampV2	
archivetimestampV3	

A.4.3 XAdES 検証

A.4.3.1 XAdES の検証要件

参照：表 5.5.3-1 検証要件（XAdES 署名）

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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	

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
	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: Mandatory/mandatory if Exists/Optional

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 5.6.2-3 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 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 5.6.3-3 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

関連規格の種類	実装 (Y/N)
XAdES v1.3.2 (https://uri.etsi.org/01903/v1.3.2/)	
XAdES v1.4.1 (https://uri.etsi.org/01903/v1.4.1/)	

A.4.4 PAdES 検証

A.4.4.1 PAdES 署名関連辞書

参照: 表 5.5.4-1 PAdES 関連 PDF 辞書の種類 (PAdES)

PDF 辞書	要素	実装 (Y/N)
CAdES 署名辞書	CAdES-BES / CAdES-T	
PKCS7 署名辞書	PKCS#7	
DocTimeStamp 辞書	ドキュメントタイムスタンプ	
DSS 辞書	全体の検証情報 (証明書と失効情報)	
VRI 辞書	署名ごとの検証情報 (証明書と失効情報)	

参照: 表 5.5.4-3 検証要件 (PAdES 署名)

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
署名構造	PAdES 必須要素	M		VALID	
				INVALID	
オプション要素	PAdES オプション要素	O		VALID	
				INVALID	
CAdES 署名辞書	CAdES データ検証	M		5.5.2 参照	

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
	ByteRange 範囲のハッシュ値との比較	M		VALID	
				INVALID	
DocTimeStamp 署名辞書	タイムスタンプトークン検証	M		5.6.1 参照	
	ByteRange 範囲のハッシュ値との比較	M		VALID	
				INVALID	
検証情報	検証情報の過不足	M		VALID	
				INVALID	

M/E/O: Mandatory/mandatory if Exists/Optional

A.4.4.2 PAdES CAdES 署名の PAdES 拡張属性

参照: 表 5.5.4-3(一部) CAdES 署名の検証情報 (PAdES)

属性	実装 (Y/N)
失効情報 revocationInfoArchival 属性 (OID: 1.2.840.113583.1.1.8)	

A.4.4.3 PAdES-DT 対応

参照: 表 5.6.4-1 PAdES-DT 検証要件 (PAdES)

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
署名構造	PAdES-DT 必須要素	M		VALID	
				INVALID	
オプション要素	PAdES-DT オプション要素	O		VALID	
				INVALID	
DocTimeStamp 署名辞書	タイムスタンプトークン検証	M		VALID	
				INVALID	
	ByteRange 範囲のハッシュ値との比較	M		VALID	
				INVALID	
検証情報	検証情報の過不足	M		VALID	
				INVALID	

M/E/O: Mandatory/mandatory if Exists/Optional

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 5.6.1-2 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/N)	備考
ContentType			M		
Content			M		
	CMSVersion		M		
	DigestAlgorithmIdentifiers		M		
	EncapsulatedContentInfo		M		
		eContentType	M		Object identifier of "TSTInfo"

ASN.1 表記	M/O	実装 (Y/N)	備考
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 5.5.2-2 署名データの構成要素（CAdES）

ASN.1 表記	M/O			実装 (Y/N)
	CAdES-BES	CAd ES-T	CadES-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	

ASN.1 表記	M/O			実装 (Y/N)
	CAdES-BES	CAd ES-T	CadES-A	
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 5.5.3-2 署名データの構成要素 (XAdES)

XML 表記	M/E/O			実装 (Y/N)
	XAdES-BES	XAdES-T	XAdES-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:SigningCertificateV2	O (a)	O (a)	O (a)	
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	

XML 表記	M/E/O			実装 (Y/N)
	XAdES-BES	XAdES-T	XAdES-A	
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:SigningCertificateV2/xa:SigningCertificate 又は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: Mandatory/mandatory if Exists/Optional

A.5.4 PAdES のデータ要素

参照: 表 5.5.4-2 PAdES 署名関連辞書 (PAdES)

PDF 辞書	M/O				実装 (Y/N)
	PAdES-BES	PAdES-T	PAdES-X-Long	PAdES-A	
CAdES 署名辞書	M	M	M	M	
CAdES-T	-	M	M	M	
DSS/VRI 辞書	-	-	M	M	
DocTimeStamp 辞書	-	M	-	M	

M/O: Mandatory/Optional

参照: 表 5.5.4-4 CAdES 署名辞書の構成要素 (PAdES)

キー	種別	値/備考	M/O/P	実装 (Y/N)
/Type	name	/Sig	O	
/Filter	name	優先署名ハンドラの名前	M	
/SubFilter	name	/ETSI.CAdES.detached	M	
/Contents	hex string	CAdES-BES 又は CAdES-T	M	
/ByteRange	array	[start1 len1 start2 len2] 署名対象	M	
/Cert	array	利用禁止、存在しても無視する	P	
/Name	text	署名者名	O	
/M	date	署名時刻：ISO/IEC 8824 の ASN.1 形式 (D:YYYYMMDDHHmmSSOHH’mm’) ※ 検証時の時刻に利用してはいけない	O	
/Location	text	署名場所	O	
/Reason	text	署名理由	O	
/ContactInfo	text	署名者へのコンタクト情報	O	

M/O/P: Mandatory/Optional/Prohibited

参照: 表 5.5.4-3(一部) CAdES 署名の検証情報 (PAdES)

属性	実装 (Y/N)
失効情報 revocationInfoArchival 属性 (OID: 1.2.840.113583.1.1.8) 対応	

参照: 表 5.5.4-5 DocTimeStamp (DTS) 署名辞書の構成要素 (PAdES)

キー	種別	値/備考	M/O/P	実装 (Y/N)
/Type	name	/DocTimeStamp	M	
/Filter	name	優先署名ハンドラの名前	M	
/SubFilter	name	/ETSI.RFC3161	M	
/Contents	hex string	タイムスタンプトークン	M	
/ByteRange	array	[start1 len1 start2 len2] 署名対象	M	
/Cert	array	利用禁止、存在しても無視する	P	

M/O/P: Mandatory/Optional/Prohibited

参照: 表 5.5.4-6 DSS 辞書の構成要素 (PAdES)

キー	種別	値/備考	M/O/P	実装 (Y/N)
/Type	name	/DSS	O	
/VRI	dict	ハッシュ値をキーとして VRI 辞書を値に持つ	O	
/Certs	array	証明書バイナリの配列	O	

キー	種別	値/備考	M/O/P	実装 (Y/N)
/OCSPs	array	OCSP バイナリの配列	O	
/CRLs	array	CRL バイナリの配列	O	

M/O/P: Mandatory/Optional/Prohibited

参照: 表 5.5.4-7 VRI 辞書の構成要素 (PAdES)

キー	種別	値/備考	M/O/P	実装 (Y/N)
/Type	name	/VRI	O	
/Cert	array	証明書バイナリの配列	O	
/OCSP	array	OCSP バイナリの配列	O	
/CRL	array	CRL バイナリの配列	O	
/TU	date	検証した日時	P	
/TS	stream	検証した日時のタイムスタンプ	P	

M/O/P: Mandatory/Optional/Prohibited

A.6 X.509 証明書

A.6.1 X.509 証明書パス検証

参照: 表 5.7.1-1 検証要件 (署名者証明書)

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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: Mandatory/mandatory if Exists/Optional

A.6.2 署名者証明書の X.509 証明書パス検証

参照：表 5.7.1-2 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		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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 5.7.2-1 検証要件（TSA 証明書）

検証対象	検証内容	ステータス		レポート(オプショナル)	
		M/E/O	実装 (Y/N)	状態	レポート項目
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	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）: PAdES 関連情報

CAdES と XAdES は記述フォーマットが ASN.1/DER か XML かの違いがあるが、署名属性的にはほぼ同じ構造と言える。しかし記述フォーマットに PDF を利用した PAdES の場合にはかなり構造が異なる。また PDF の特性として同じ目的のために複数の記述や組み合わせが可能であるために、PDF の元仕様となる ISO 32000-2 を見ただけでは PAdES として長期署名の利用が難しいと言う側面もある。そのために PAdES 長期署名ではプロファイルである ISO 14533-3 を理解する必要がある。本付属書 B では ISO 14533-3 に記述されている内容をベースに PAdES を長期署名として利用する場合に必要となる参考情報をまとめる。

B.1 PAdES 署名レベル判定

PAdES の署名レベルの判定には幾つか注意が必要となる点がある。1 つにはデジタル署名を利用せずタイムスタンプのみの仕様である PAdES-DT があること。もう 1 つはタイムスタンプとして、署名辞書として埋め込まれる CAdES への署名タイムスタンプ（CAdES-T）と、単独で追加できるドキュメントタイムスタンプ（DocTimeStamp）の 2 種類があることである。

ドキュメントタイムスタンプは PDF 構造的にその前にある全てを直接保証しているが、タイムスタンプ付き署名（CAdES-T）の場合には PDF 構造的にその前にある全てを保証しているのはデジタル署名となり、署名タイムスタンプはそのデジタル署名を保証することになり、間接保証と言える。しかしどちらも同じ扱いとして PDF 構造的にその前にある全てを保証すると判断してよい。

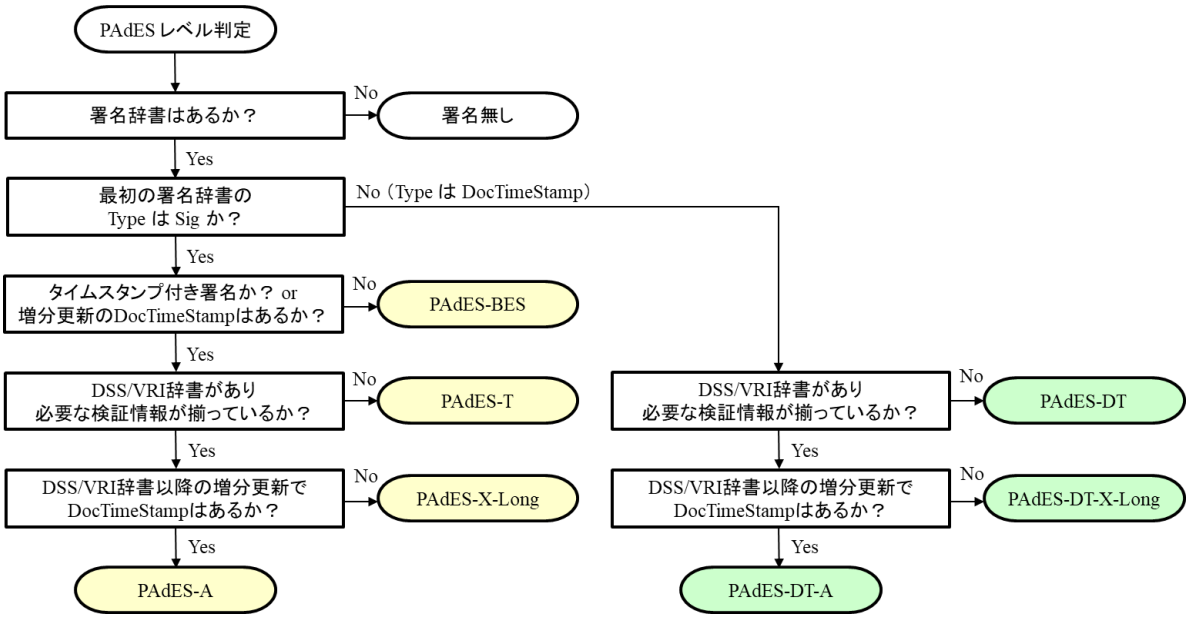

図 B.1-1　PAdES の署名レベルと種類の判定方法

B.2 PAdES 複数署名

PAdES には 1 つの PDF ファイルに対して複数署名を行うことが可能となっているが、この場合には各署名単位で検証を行う必要がある。この場合にあるドキュメントタイムスタンプが、1 つ目の署名ではアーカイブタイムスタンプになり同じ PDF 中にある 2 つ目の署名では署名タイムスタンプになることもあり得る。また検証情報（証明書群と失効情報群）をまとめる DSS/VRI 情報は上書きされるために、1 つの PDF では 1 つしか存在できないことにも注意が必要となる。ここでは ISO 14533-3 の「E.3 Example of the PAdES-A profile」に記載されている例を通して複数署名の検証の考え方を説明する。

➢ 複数署名の例１：1 つが PAdES-A でもう 1 つは PAdES-T となる場合

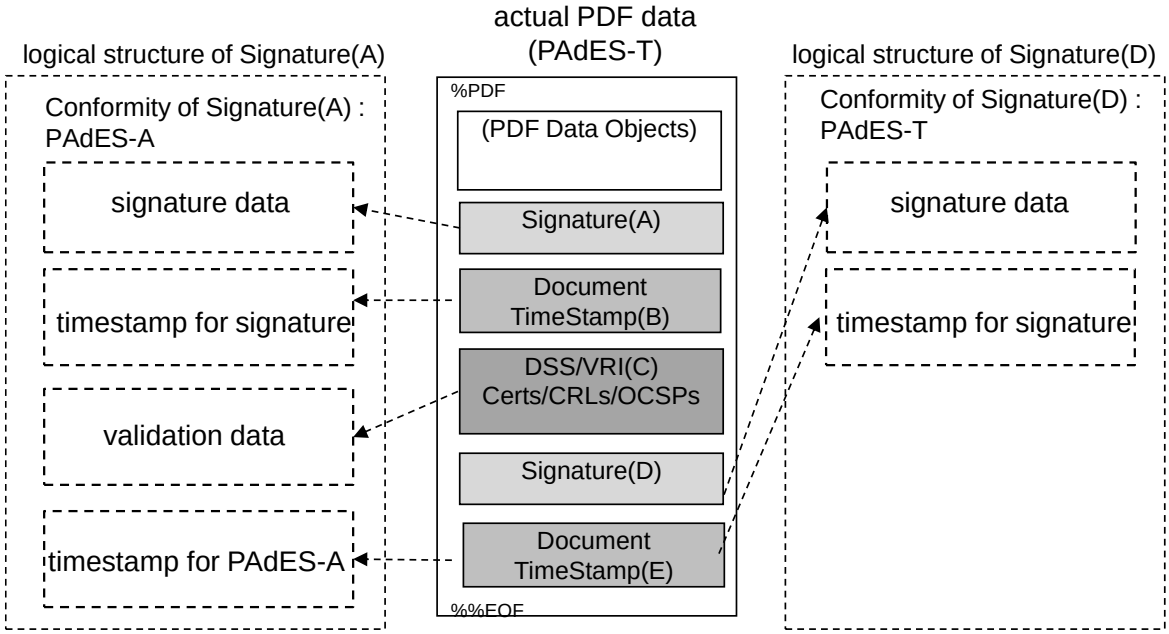

図 B.2-1 複数署名の例１：1 つが PAdES-A でもう 1 つは PAdES-T となる場合の構造

CAdES 署名辞書は Signature(A) と Signature(D) の 2 つがある。図の左側が Signature(A) の署名レベル構造で、図の右側が Signature(D) の署名レベル構造となっている。

1. Signature(A) に関しては DocumentTimeStamp(B) が署名タイムスタンプとなり、その後に Signature(A) と DocumentTimeStamp(B) の検証情報 DSS/VRI(C) が存在する。さらに DocumentTimeStamp(E) がアーカイブタイムスタンプとなるので、PAdES-A となる。

2. Signature(D) に関しては DocumentTimeStamp(E) が署名タイムスタンプとなり、その後に増分更新がないので、PAdES-T となる。DSS/VRI(C) より前の Signature(A) と DocumentTimeStamp(B) と DSS/VRI(C) は、Signature(D) の検証には影響しない。

➢ 複数署名の例２：両方共に PAdES-A となる場合

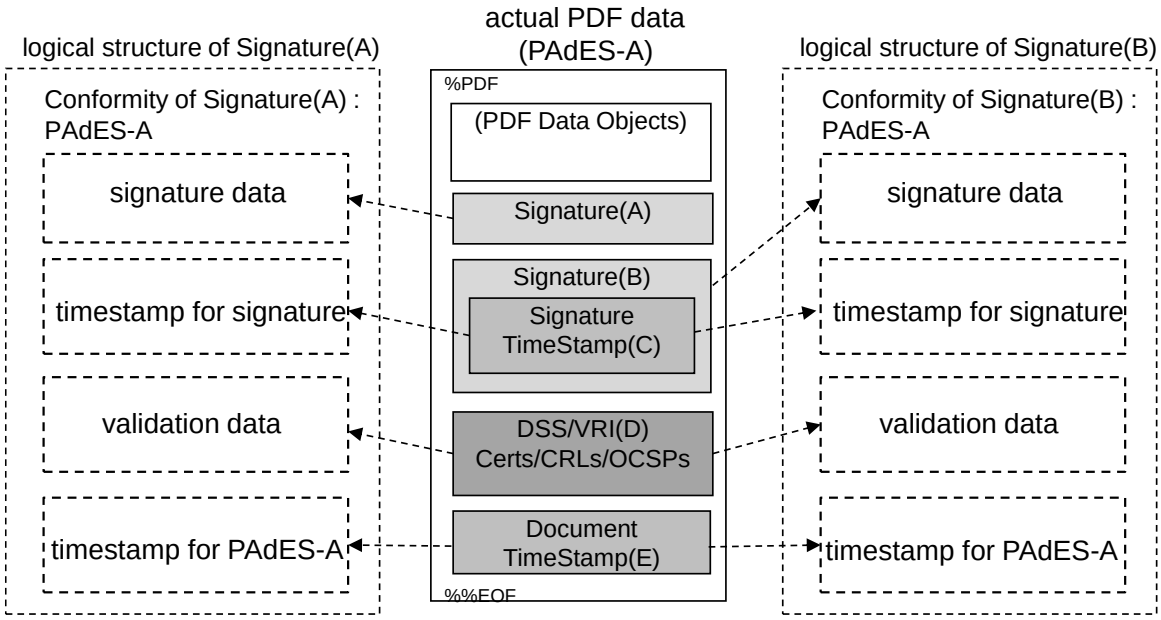

図 B.2-2 複数署名の例２：両方共に PAdES-A となる場合の構造

CAdES 署名辞書は Signature(A) と Signature(B) の 2 つがある。図の左側が Signature(A) の署名レベル構造で、図の右側が Signature(B) の署名レベル構造となっている。

1. Signature(A) に関しては続く Signature(B) が CAdES-T 形式でタイムスタンプを含むために、Signature(B)のタイムスタンプが署名タイムスタンプとなり、その後に Signature(A) と Signature(B) の検証情報 DSS/VRI(D) が存在する。さらに DocumentTimeStamp(E) がアーカイブタイムスタンプとなるので、PAdES-A となる。

2. Signature(B) に関しては CAdES-T 形式でタイムスタンプを含むために、Signature(B) 埋め込みのタイムスタンプが署名タイムスタンプとなり、その後に Signature(B) の検証情報 DSS/VRI(D) が存在する。さらに DocumentTimeStamp(E) がアーカイブタイムスタンプとなるので、こちらも PAdES-A となる。

B.3 PAdES 署名後の増分更新

PAdES 仕様では PDF の増分更新（Incremental Update）により情報を追加していく。増分更新では、任意の新規情報が追加できるとともに、既存情報の上書きも可能となる。PDF/PAdES の仕様にはないが、署名後に増分更新可能となる情報は PDF の本体データ以外の情報のみとなる。

PDF は印刷イメージをファイル化したフォーマットであるが、署名後に見た目が変更されてはならないと言う理解もできる。見た目が変更できてしまう（例えば記載されている契約金額の変更等ができてしまう）と署名者の意図が保証できなくなるためである。なお署名外観は注釈として追加されるので本体データの変更とは見なされない。つまり署名後に追加が可能となる外観は、本文データとは分離された注釈データのみとなる。PAdES を厳密に検証するのであれば、増分更新された情報に本体データが含まれていないことを確認する必要がある。目視にて確認する 1 つの方法として、署名後に追加された増分更新を省くことで、署名時の外観を復元（署名時バージョンの復元）する PDF アプリケーションもある。

検証情報を保持する DSS 辞書は PDF に 1 つしか許されないために上書きにて増分更新していく必要があるが、このときには古い DSS 辞書に含まれていた証明書群と失効情報群は新しい DSS 辞書にも含まれるべきである。

PAdES デジタル署名に対する攻撃手段として度々この増分更新が使われている。全てを実装にて検証することは困難であるかもしれないが、検証者は知識として増分更新の問題については認識しておくべきである。

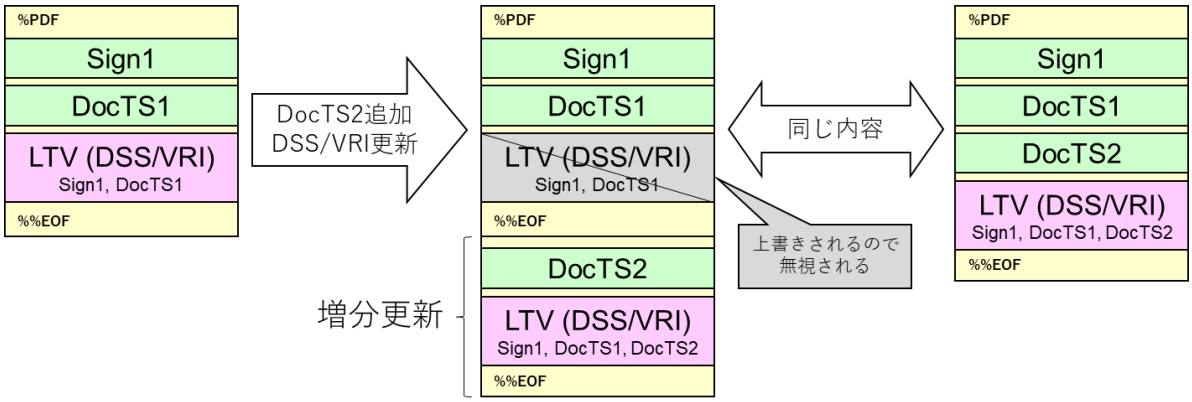

図 B.3-1 増分更新による DSS/VRI の更新例

B.4 PAdES 署名と PDF 暗号化仕様

PDF はパスワードや証明書（公開鍵）を利用した、RC4 又は AES（128bits/256bits）による暗号化仕様が認められている。PDF 暗号化は PDF ファイル全体を暗号化するものではなく、オブジェクトや文字列等が暗号化される。なお署名辞書の Contents エントリーも HEX 文字列であるが、これは暗号化の対象外となっている。

PDF 暗号化仕様と PAdES 署名仕様は同時に利用することが可能となっている。ただし未暗号化状態の PAdES 署名後に暗号化することはできない。PDF 暗号化仕様と PAdES 署名仕様を同時に使うのであれば署名前に暗号化をしておく必要がある。

B.5 PAdES 署名の Acrobat Reader による検証

PDF の読み込みと表示として Adobe Acrobat Reader® （以降 Acrobat Reader）がデファクト標準として利用されることが多い。Acrobat Reader も PAdES の検証に対応しているが、その検証内容が本書と一致している保証はない。そのために Acrobat Reader の検証では VALID になっても本書の検証では INDETERMINATE や INVALID となる可能性もあるし、またその逆もあり得る。

また Acrobat Reader の検証設定に依存する場合もある。例えば本書では検証基準時刻としてタイムスタンプの時刻を利用しているが、Acrobat Reader のデフォルト検証設定では 「署名が作成された時刻」 として署名辞書中の M エントリーの署名時刻も利用する。本書と検証結果を一致させるためには、この設定を 「署名に埋め込まれている保証された時刻（タイムスタンプ）」 に変更する必要がある。他にも幾つか検証設定があるので注意が必要である。

トラストアンカーとなるルート証明書も、デフォルト設定では Adobe 独自認定基準の AATL（Adobe Approved Trust List）に登録されたルート証明書と、欧州基準の EUTL（European Union Trust List）を信頼している。しかし Windows 環境の場合には 「Windows 統合」 の設定を利用することで Windows 証明書ストアの 「信頼されたルート証明機関」 を利用することも可能となる。しかしデフォルト設定では Windows 証明書ストアの利用はオフになっているので注意が必要である。

Acrobat Reader の検証も今後バージョンアップにより更新されていくことが予想されるので都度確認しつつ、本書との差異があることを認識した上で利用する必要があるだろう。

付属書 C（参考）：暗号アルゴリズム

本書では「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。」とする暗号アルゴリズムや鍵長の確認要件が数カ所にわたり存在するが、本節では、この要件が曖昧でテストの実現が非常に困難であるという問題を整理し、その解決の方向性を示すこととする。

最初に、なぜ暗号アルゴリズムや鍵長の確認という要件が曖昧で実装困難であるのか、その理由を整理する。

本節では「検証基準時刻において安全性の観点から受け入れ可能な暗号アルゴリズムや鍵長を使用しているか確認する処理」を「受理アルゴリズム検証」と呼ぶことにする。

C.1 暗号アルゴリズムや鍵長の安全性確認の困難さについて

(1) AdES 署名フォーマット中の様々な箇所での暗号アルゴリズムの利用

AdES 署名フォーマットにおいて、フォーマット自体、タイムスタンプトークン、証明書や失効情報など至るところで暗号アルゴリズムや鍵長が使われているが、その要求レベルはフォーマットのフィールドごとに異なり一律で受理アルゴリズム検証を行うのは困難である。例えば、「何年何月以降は SHA-1 アルゴリズムの危殆化により使用不可」であると定めたとする。2020 年 11 月時点では下記に示すような問題が発生する。

(a) TimeStampToken の TSA 証明書を特定するための SigningCertificate 属性は SHA-1 アルゴリズムを使用している。
(b) OCSPResponse の失効検証対象の証明書を特定するための CertID は発行者の名前や鍵の特定に SHA-1 アルゴリズムを使用している。
(c) AdES 署名フォーマットの検証に直接は関係ないかもしれないが、証明書の検証情報の取得に TLS 通信を使用した場合、メッセージ認証に HmacSHA1 が使われる可能性がかなり高い。
(d) 証明書や CRL の鍵識別子 authorityKeyIdentifier、subjectKeyIdentifier の生成には多くの場合、SHA-1 アルゴリズムを使用する。

ある検証器に、SHA-1 を厳格に使用しないような設定をした場合、(a)、(b)、(c)でエラーが発生し検証失敗となる。フィールドごとにアルゴリズムの要求レベルが異なるため、一律にアルゴリズムを制限させることは困難なのである。

(2) アルゴリズムの安全性判断の組み込み

AdES 署名フォーマット、タイムスタンプトークン、CMS SignedData、証明書、失効情報の検証、及びそれらの検証で使用される暗号ライブラリにおいて、一般に受理アルゴリズム検証を行う機能はなく、OS やブラウザや暗号ライブラリが「現時点でサポートする暗号アルゴリズムや鍵長」に従って検証するだけである。従って、受理アルゴリズム検証は、狭義の検証器の外

で実装する必要があることを意味している。

(3) 長期にわたる暗号アルゴリズム利用環境の維持

前述のとおり、一般に検証は「現時点」で OS や暗号ライブラリがサポートしている暗号アルゴリズム及び鍵長で検証を行っていることに注意が必要である。現時点で危殆化しているアルゴリズムは実装から外されており、検証することができない。例えば、オープンソースの BouncyCastle Java ライブラリはかなり広範な暗号アルゴリズムや鍵長をサポートするが、OpenSSL ではデフォルトビルドでは危殆化されたアルゴリズムは組み込まれない。Microsoft Windows の CryptoAPI、.NET、Oracle Java JCE などは OpenSSL より暗号アルゴリズムのサポート範囲が狭い。W3C Cryptography API では古い危殆化したアルゴリズムは全くサポートされない。

AdES 署名フォーマットでは 10 年、数十年というスパンで検証可能な署名データを提供するものだが、10 年、数十年前に生成された署名について、当時の暗号アルゴリズムをサポートする実装が存在しないために検証できないという状況が容易に起こりうる。

一つの検証器で数十年オーダーの検証を行う必要がある場合、OS やライブラリを含めた実行環境の保存、維持もまた配慮しなければならない。検証器の対応する暗号アルゴリズムや鍵長の範囲もまた、明示する必要があるだろう。また、複数の検証器を用いて検証する必要がある場合、一気通貫した自動的な検証はおそらく不可能となるが、その検証手順についても明確にしておかなければならない。

(4) 検証基準時刻に受理可能な暗号アルゴリズムと鍵長の厳格な制限規定の不在について

暗号アルゴリズム及び鍵長の利用について幾つかのガイドラインが出ているが、何年何月まで、どの暗号アルゴリズムをどの鍵長で使ってよいかを判断するには幾つかの課題がある。

- 暗号利用についてガイドラインであって、遵守を強制するものではない。
- どの暗号アルゴリズムをどの鍵長で何年何月まで使ってよいとするのか、過去、現在、将来に対して明確にしているガイドラインがない。もしくは非常に少ない。
- ガイドラインごとにアルゴリズムの利用期限は異なることがある。
- ある暗号アルゴリズムを使って署名されたデータが将来、ある期間検証が可能とできるように、生成と検証とで利用の期限を変えてあるガイドラインがある。
- ガイドラインは暗号プリミティブに対して設定されているものであるため、AdES 署名に配慮した期限の設定が別途必要である。

暗号アルゴリズムの受け入れ期間を定める際に参照可能なガイドラインを示す。

- CRYPTREC 暗号リスト(電子政府推奨暗号リスト)

- 2003 年、2013 年に公開されており、政府機関の情報システムで利用可能な暗号アルゴリズムのリストを示している。
- 2013 年以降は数年ごとに改訂されている。
- 民間に対して強制するものではないが、民間も概ねこれに習っている。
- 推奨暗号リストと互換性維持の目的で運用監視暗号リストがある。
- 発行時点での判断を示すものであり、暗号アルゴリズムの使用可能期間の判断が難しい。
- 将来いつまで使えるのか示されていない。

・ 政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針
- 政府機関の情報システムにおける SHA-1 及び RSA1024 の使用可能期間を定めるもの。
- 民間に対して強制するものではないが、民間も概ねこれに習っている。

・ NIST SP800-57 Recommendation for Key Management Part 1 – General
- ビット数で示されるセキュリティ強度により、暗号アルゴリズムがいつまで利用可能かを示す。
- 安全性が境界線上にあるものは生成と検証とで使用可能期間を分けている。
- 2030 年までの利用可能判断を示す。
- 従来アプリケーションの互換性のために利用可能なケースも示している。
- 2005 年に初版が発行され、数年ごとに改訂されている。

・ NIST SP800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths
- 具体的な鍵長の利用可能範囲を示している。

どのガイドラインも、発行時点で利用可能な暗号アルゴリズムを示すものであり、AdES 署名のような時間の推移の中で、暗号アルゴリズムがどの期間利用可能であるかを直接示すものではないため、過去の改版を含めて精査し、使用可能期間を定める必要がある。

以上の理由から、暗号アルゴリズムや鍵長を安全であると一意に判断できる方法はなく、将来的には権威ある機関が AdES 署名に関する暗号アルゴリズムの利用可能期間を定め、それを参照して安全性の判断を行う必要があるだろう。

(5) ガイドラインで定められた期間以降の利用実態の反映

市場では、ガイドラインで暗号アルゴリズムや鍵長の利用期間を超えて利用するケースがあり、実際に SHA-1 や RSA 1024 のアルゴリズム移行のケースでもあった。

・ パブリックな公開鍵証明書については業界団体の基準により移行が行われた。
・ これに対し、社内システム、閉じたシステムでは様々な理由によりガイドラインの期間を超えて使用しているケースがある。

・ ガイドラインの対象範囲に含まれるか判断がつきにくい利用、例えば OCSP や証明書鍵識別子の利用などは SHA-1 が利用されている。
・ ガイドラインが互換性のためには利用可能としている暗号アルゴリズムの期限の判断が難しい。

(6) 暗号アルゴリズムの安全性に関する要求レベルの違い

国家間での重要な合意事項の締結や、高額な企業間の契約と、一般的な文書における署名では、暗号アルゴリズムに求められる安全性のレベルは異なる。攻撃者の観点からすれば、重要な文書では、専用ハードウェアを使って大きなコストと時間を払ってでも署名文書を改ざんしようとするが、一般的な文書ではそのような動機は働かない。重要な文書では、暗号アルゴリズム危殆化の兆候が見られれば速やかに暗号移行しなければならないが、一般的な文書では、可能な範囲で暗号移行をすればよいし、文書の相互運用性の要件を重要視するケースもあるだろう。

このように、署名文書を受理する際の暗号アルゴリズムや鍵長の利用可能期間は、署名文書が求める安全性によって異なるため、複数のレベルに分けて定義する必要があるかもしれない。

(7) 安全であるとする暗号アルゴリズムや鍵長の情報を与える標準フォーマットの不在

検証処理の自動化のためには、どの暗号アルゴリズムと鍵長がどの期間利用可能であるかを入力として与える必要があるが、この情報を与える標準的なフォーマットが存在しない。Proposed Standard(標準化への提唱)として RFC 5698 Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)として標準化されたが、市場で利用されているとは言えない。

以上のことから「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。」としている検証項目の確認は多くの課題が存在し、事実上検査項目として機能しないか、非常に困難であることが分かる。

C.2 AdES 署名検証の暗号アルゴリズム及び鍵長の安全性判断基準の一例

暗号アルゴリズム及び鍵長の安全性判断を、機械処理可能にするための基準の一例を以下に示す。

(1) 暗号アルゴリズムの対象範囲について

AdES 署名検証の暗号アルゴリズムの安全性判断においては以下の暗号アルゴリズムのみを検証すると定める、それ以外については制限しないことを明らかにする。

- 署名アルゴリズム
- ハッシュアルゴリズム

従って、例えば通信で使用されるその他のアルゴリズム等は制限されない。

(2) 対象暗号アルゴリズムの明確化

ガイドライン発行時点では以下の過去を含む以下の暗号アルゴリズムを検証可能とする。それ以外の暗号アルゴリズムが(1)のカテゴリに使われている場合には、検証失敗とする。

- 署名アルゴリズム：SHA-(1/256/384/512)withRSA、SHA-(1/256/384/512)withECDSA
- ハッシュアルゴリズム：SHA-(1/256/384/512)

(3) 暗号アルゴリズムの検証受け入れ可能期間を定めるリストの規定と開示

AdES 署名フォーマットの受け入れ可能な暗号アルゴリズム及び鍵長の使用可能期間を機械可読可能な方式で開示する。これを「(仮)AdES 署名検証受理のための暗号リスト」(以下リスト)とする。

- 規定は AdES 署名について専門知識を持つ権威ある機関が定めることが望ましい。
- 前節で定めたガイドライン及び猶予期間から総合的に判断して期間を定める。
- 適用範囲は、(4)に示す確認対象とする。
- 権威ある機関がリストを維持管理、開示する。
- リストは、過去全てから、次版改訂されるまで適用可能である。
- リストは基本的な基準を定めるものであり、業種、用途ごとに改変して使用することができる。

(4) AdES 署名フォーマットにおける安全性の確認対象について

本書における暗号アルゴリズムの安全性検証の対象は、署名者が指定可能な署名アルゴリズム、ハッシュアルゴリズム、署名鍵の鍵長とし、パブリックな認証局、タイムスタンプ局は認定基準により暗号アルゴリズムの安全性要件を満たしているものとし、安全性検証は行わない。

次表に、安全性検証の対象となるフィールド、対象でないフィールドについて CAdES を例に示す。

安全性検証の対象となる要素	CAdES における具体的な要素(フィールド)
署名者の署名プリミティブ	signerInfo 中の signature, signatureAlgorithm フィールド
署名対象データへのハッシュ	messageDigest 属性
署名値へのハッシュ(タイムスタンプを含む) ※1	signatureTimeStamp, archiveTimeStamp の messageImprint ※1: PAdES の VRI 辞書は署名値に対して SHA-1 固定で、参照するため安全性検証から除外する。
検証情報への参照	署名者 signerInfo の signingCertificate(V1,V2)属性、CertificateReference、RevocationInfoReference
安全性検証の対象とならない要素	
上述の署名フォーマットの対象となる要素以外の要素	
全ての証明書、CRL の署名、ハッシュアルゴリズム ※2 ※2: 証明書の subjectKeyIdentifier、authorityKeyIdentifier の計算には一般に SHA-1 が使用されているが、これも対象としない。	
OCSP レスポンスで使用される署名、ハッシュアルゴリズム※3 ※3 OCSP レスポンスは発行者の名前、鍵の参照に SHA-1 が使われているが、これも対象としない。	
タイムスタンプトークンで使用される暗号アルゴリズム	
その他の暗号アルゴリズム (共通鍵暗号、TLS 通信の暗号、HTTP 認証の暗号、鍵管理の暗号)	

(5) 安全性のレベルについて

安全性のレベルについて極めて重要な文書と、一般文書では保護すべきレベルが異なる。安全性のレベルについて「重要」と「一般」の 2 つのレベルを設けるものとする。

- 重要文書、データ(極めて重要な契約文書、国家レベルで保護が必要な文書等)
  - ✧ 調達コスト無制限で入手可能な専用ハードウェア、コンピュータを使用して数年でも解読することができない
  - ✧ 暗号解読事例が発見され次第即時利用停止
  - ✧ パブリック認証局の証明書発行で利用停止した時点で即時停止
- 一般的な文書、データ
  - ✧ 1000 万円程度で入手可能な専用ハードウェア、コンピュータを使用して数年でも解読することができない
  - ✧ 暗号解読事例が発見されて以降、原則として 3 年で利用停止
  - ✧ パブリック認証局の証明書発行で利用停止した時点で 1 ヶ月後停止

(6) 「(仮)AdES 署名検証受理のための暗号リスト」の記載項目とリスト例

リストのフォーマットは意味内容が同一であれば、JSON(C)、XML、ASN.1 などの提供が可能であるとする。以下に JSON 形式のリスト記載項目の例を示す。

```
{
  "listinfo": {
    "name": "JNSA AdES 署名検証受理のための暗号リスト(一般向け)",
    "issuer": "JNSA",
    "version": "1",
    "issue-date": "2020-11-20"
  }
  "list": {
    "RSA1024": {"to": "2014-03-31"}, // 政府機関情報システムの期限により
    "RSA2048": {"to": "2030-12-31"},
    "RSA3072": {},
    "RSA4096": {},
    "ECDSA128": {"to" : "2010-12-31"},
    "ECDSA192": {"to": "2030-12-31"},
    "ECDSA256": {},
    "ECDSA384": {},
    "ECDSA521": {},
    "MD5": { “from” : “1991-01-01” , "to": "2009-01-31"},
    "SHA-1", {"to": "2014-03-31"}, // 政府機関情報システムの期限により
    "SHA-256", { “from” : “2001-01-01” },
    "SHA-384", { “from” : “2001-01-01” },
    "SHA-512", { “from” : “2001-01-01” }
  }
}
```

```
{
  "listinfo": {
    "name": "JNSA AdES 署名検証受理のための暗号リスト(重要データ向け)",
    "issuer": "JNSA",
    "version": "1",
    "issue-date": "2020-11-20"
  }
  "list": {
```

```
    "RSA1024": {"to": "2010-12-31"}, // NIST SP800-57 Part1 より
    "RSA2048": {"to": "2030-12-31"},
    "RSA3072": {},
    "RSA4096": {},
    "ECDSA128": {"to" : "2010-12-31"},
    "ECDSA192": {"to": "2030-12-31"},
    "ECDSA256": {},
    "ECDSA384": {},
    "ECDSA521": {},
    "MD5": { "from" : "1991-01-01" , "to": "2009-01-31"},
    "SHA-1", {"to": "2010-12-31"}, // NIST SP800-57 Part1 より
    "SHA-256", { "from" : "2001-01-01" },
    "SHA-384", { "from" : "2001-01-01" },
    "SHA-512", { "from" : "2001-01-01" }
  }
}
```

- 利用可能期間については、関係するガイドラインを参照しながら、権威ある機関において専門家により定める。
- リストは利用可能期間の厳格なもの、緩和されたものなど幾つかのレベルを分けて提供される可能性がある。
- リストにはデジタル署名は施さないものとする。
- ECDSA においては、受理可能な楕円曲線名(named curve)との関係は、曲線ビット長で表現されるものとする。

安全な暗号アルゴリズムの利用開始と終了についての根拠を以下に示す。

- MD5（一般：1991 年 1 月-2009 年 2 月）
  - 1991 年に Rivest により発明
  - 2008 年 12 月 Alexander Sotirov の MD5 不正 CA 証明書の国際会議発表 [1]
  - 2009 年 1 月 ベリサイン MD5 証明書の発行停止 [1]
- SHA-1（一般: 1995 年 1 月-2014 年 3 月）
  - 1995 年 NIST が制定
  - 2005 年 Wang による効率的衝突検索アルゴリズムの提案
  - 2014 年 3 月 政府機関情報システムの利用終了
- SHA-2(224,256,384,512)（一般: 2001 年-）
  - 2001 年 NIST が PUB 140-4 として標準制定

- RSA 1024bit, ECC 160bit（セキュリティ強度 80bit）（重要 -2010 年 12 月）（一般 -2014 年 3 月）
  - 2010 年 NIST SP800-57 Part1
  - 2014 年 3 月 政府機関情報システムの利用終了
- RSA 2048bit, ECC 224bit（セキュリティ強度 112bit）（重要 -2030 年 12 月）（一般 -2030 年 12 月）
  - 2030 年 NIST SP800-57 Part1
- RSA 3072bit, ECC 256bit（セキュリティ強度 128bit）（重要 -なし）（一般 -なし）
  - 制限なし NIST SP800-57 Part1

(7) 「(仮)AdES 署名検証受理のための暗号リスト」の利用方法

暗号アルゴリズムの安全性検証のプロセスは、「5.1.2 節 検証のアプリケーションモデル」における暗号制約の処理に相当する。暗号アルゴリズムの安全性に関する制約については、本節で示されるような安全性判断の基準となる入力データとして「(仮)AdES 署名検証受理のための暗号リスト」が必要となる。「図 5.1.2-1 署名検証アプリケーションの概念モデル」の「暗号アルゴリズム」の検証制約として与えられるべきものであるが、本書では現時点でそのような記載はまだされていない。

暗号リストの利用方法の概念図を以下に示す。

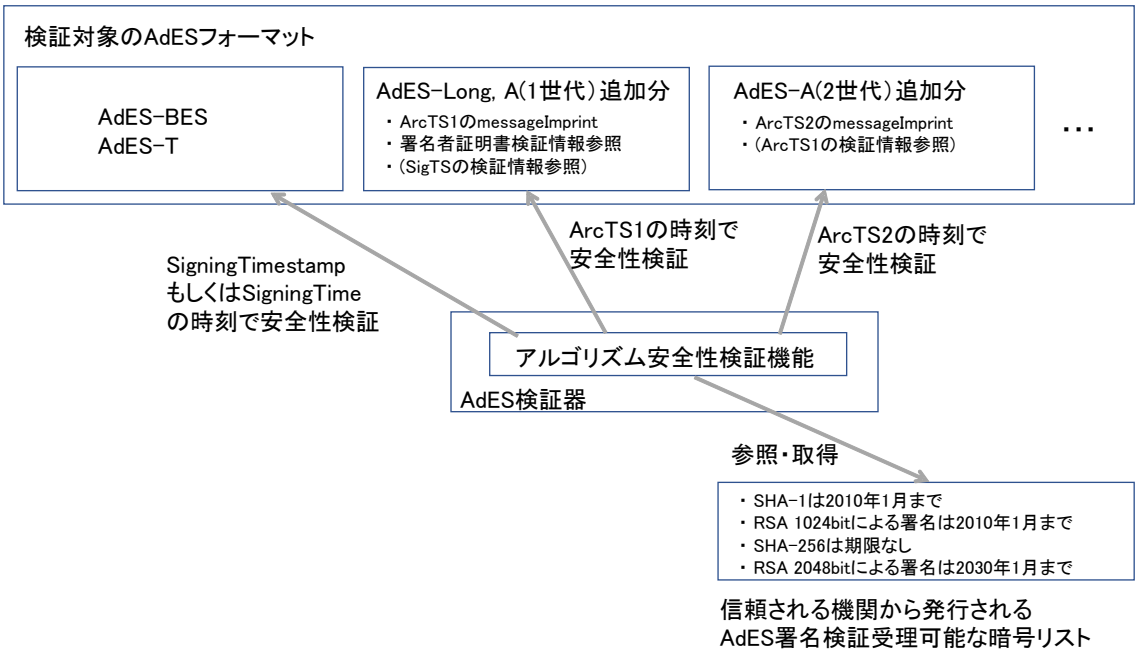

図 C.2-1 暗号リスト利用方法の概念図

作成メンバー（五十音順）

新井 聡（株式会社エヌ・ティ・ティ ネオメイト）
漆嶌 賢二（GMO グローバルサイン株式会社）
上条 桃花（株式会社エヌ・ティ・ティ・データ）
酒巻 一紀（三菱電機インフォメーションシステムズ株式会社）
佐藤 雅史（セコム株式会社）
杉崎 元（三菱電機インフォメーションネットワーク株式会社）
高丸 祐典（三菱電機インフォメーションシステムズ株式会社）
政本 廣志（日本ネットワークセキュリティ協会 電子署名 WG）
緑川 良子（三菱電機インフォメーションネットワーク株式会社）
宮崎 一哉（三菱電機株式会社）
宮地 直人（有限会社ラング・エッジ）