JAHIS

ＪＡＨＩＳ標準　２３－ｘｘｘ

Japanese Association of Healthcare Information Systems Industry

ＪＡＨＩＳ
ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.3.0

２０２３年ｘ月

一般社団法人 保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.3.0

ま　え　が　き

本規格は保健医療福祉分野における電子署名を行うに際して、相互運用性と署名検証の継続性を確保するために策定されたものである。

平成 12 年に「電子署名及び認証業務に関する法律」が成立し、日本において電子的な署名が認められて以来、電子署名は電子契約などの分野において徐々に活用されつつある。保健医療福祉分野においても、平成 17 年 3 月に厚生労働省により「医療情報システムの安全管理に関するガイドライン」（以下、「安全管理ガイドライン」と言う）が策定され、署名・押印が義務付けされた文書等を電子的に作成する際において電子署名を代替に用いる場合及び e-文書法に対応して、スキャナ等により電子保存する場合について電子署名の基準が明記された。また、同年 4 月には、同省にて「保健医療福祉分野 PKI 認証局　証明書ポリシ」【1】が策定され、国際標準に準拠した保健医療福祉分野向けの PKI（HPKI）の発行ルールが確定した。また、IT 新改革戦略においても HPKI の推進が明記され、普及に向けた各種施策が行われているところである。

JAHIS は、産業界の業界団体として、これら国の施策に協力するとともに、普及促進を図るための相互運用性の確保を図ることが重要な役割であることから、2008 年 3 月に、JIS X/5092 および 5093（後の ISO14533）をベースに「ヘルスケア PKI を利用した医療文書に対する電子署名規格」を制定し、2013 年 3 月に、当時の最新動向を踏まえ、Ver.1.1 として改定を実施した。そして、ISO 14533-3 において、PDF 電子署名(PAdES)の長期署名プロファイルが策定されたことを受け、ヘルスケア分野における相互運用性を考慮して PAdES のプロファイルの制約について 2017 年 7 月に JAHIS 標準として「ヘルスケア PKI を利用した医療文書に対する電子署名規格 PAdES 編 Ver.1.0」を策定した。2019 年 2 月に Ver.1.1 と PAdES 編 Ver.1.0 を統合し、JAHIS 電子処方箋実装ガイドにて規定したフォーマットを記載した「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」を策定した。

今般、ETSI（欧州電気通信標準化機構）より JSON に対する電子署名の長期署名プロファイル(JAdES)が策定されたことを受け、ヘルスケア分野における相互運用性を考慮して JAdES のプロファイルの制約について検討を行うと共に、各規格の最新動向を踏まえ改定を行った、「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.3.0」を発行するものである。

本規格は、JAHIS 会員各社の意見を集約し、「JAHIS 標準」の一つとして発行したものである。したがって、会員各社がシステムの開発・更新に当たって、本規格に基づいた開発・改良を行い、本規格に準拠していることをその製品のカタログ・仕様書等に示し、さらにその製品の使用においてユーザが理解すべき内容を説明する場合などに使われることを期待している。

また本規格は上記ガイドラインで示された電子署名、タイムスタンプに関連する要求事項を、実装レベルで解説した規格であり、電子署名機能を利用するシステムを導入しようとしている施設が参照し利用することは歓迎するところである。ただし、当該システムが電子署名法及びその他の法、政令、省令、通知、ガイドラインなどに合致しているか否かの判断は、自己責任の下で自ら判断する必要があることに留意されたい。なお、本規格で扱う電子署名要件は、参照規格及び技術動向にあわせて変化する可能性がある。JAHIS としても継続的に本規格のメンテナンスを重ねてゆく所存であるが、本規格の利用者はこのことにも留意されたい。

２０２３年Ｘ月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会

<<　告知事項　>>

本規格は関連団体の所属の有無に関わらず、規約の引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い、本規格に準拠する旨を表現することは厳禁するものとします。

本規格ならびに本規約に基づいたシステムの導入・運用についてのあらゆる障害や損害について、本規約作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本規約についての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目次

第１章　適用範囲

１.１ 目的

異なるシステム間において、電子署名及びタイムスタンプが付された電子文書の署名検証及び証明書検証を確実に行うために、電子署名フォーマットについての標準規格を制定し、電子署名ソフトウェア、署名検証ソフトウェアなどの互換性、署名検証の継続性を確保する。

１.２ 策定方針

電子署名の互換性の確保、及び不正な署名の流通防止のために、署名の生成、検証及び証明書検証において最低限行わねばならないことについて明確に定める。

通常の署名検証に加えて医療分野特有の検証要件として、HPKI のポリシへの準拠性を確認できることが必要であることを明確に定める。

電子保存において必要となる長期真正性担保のために長期署名フォーマット（CAdES【2】、XAdES【3】、PAdES【4】及びJAdES【5】）を採用することとする。

１.３ 対象となるシステム

電子署名機能及び署名検証機能を含む医療アプリケーションの構築に利用可能な署名ライブラリ、並びに、単独または医療アプリケーションと連動して動作する、電子署名専用プログラム又は署名検証専用プログラムが対象である。

本規格の適用対象外の医療アプリケーションとは署名データを直接的に処理しないものであり、署名ライブラリまたは電子署名専用プログラム、署名検証専用プログラムを介して、署名、及び署名検証結果を取り扱うものである。また、そのためのアプリケーションインタフェース及びユーザインタフェースは本規格の対象外である。適用対象のものと対象外のものとの関係を図 1.3.1 に示す。図 1.3.1 の網掛けの部分が適用対象のプログラム及びライブラリで、それ以外は適用対象外となる。

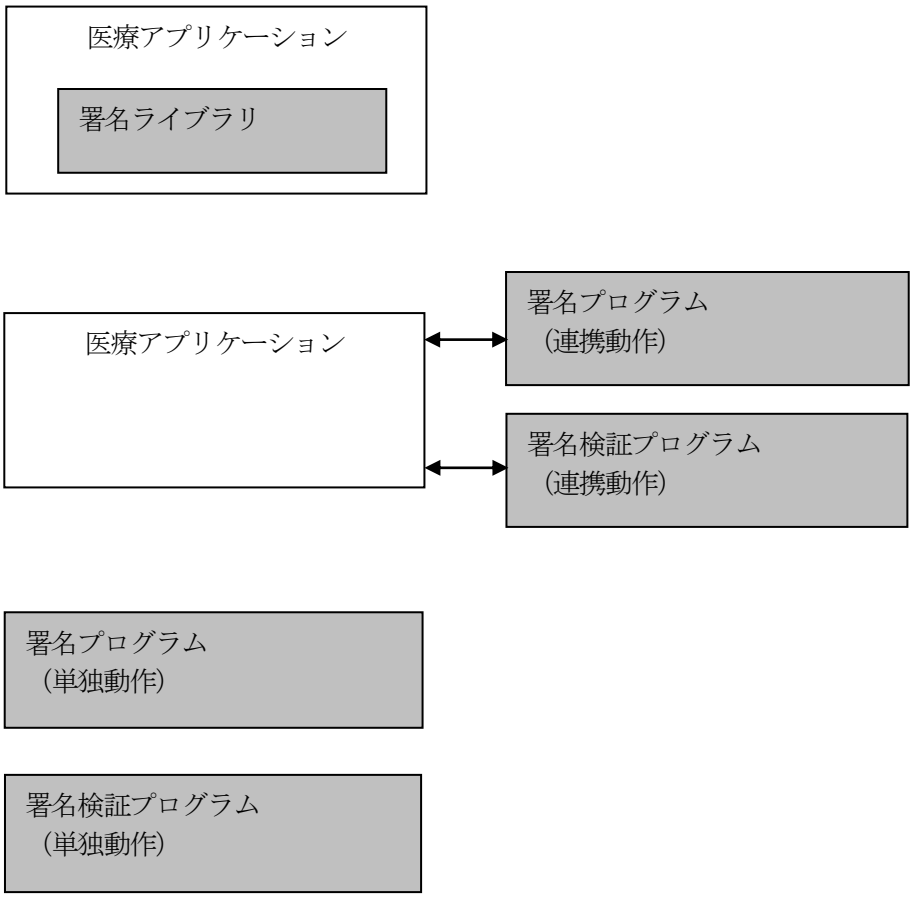

図 1.3.1 対象範囲

処理階層の例を図 1.3.2 に示す。本例における対象範囲を処理階層で見ると署名アプリケーション層（署名ライブラリ、電子署名専用プログラム、及び署名検証専用プログラム）となる。したがって、CSP、PKCS#11 以下のモデル部分は本規格の対象外である。

HPKI では、厚生労働省の CP にて、「エンドエンティティの加入者私有鍵の格納モジュールは、US FIPS 140-2 レベル 1【6】と同等以上の規格に準拠するものとする。」とされており、私有鍵（秘密鍵）を格納する媒体としては IC カード以外にも USB トークン又はソフトウェアトークン等も利用できる。

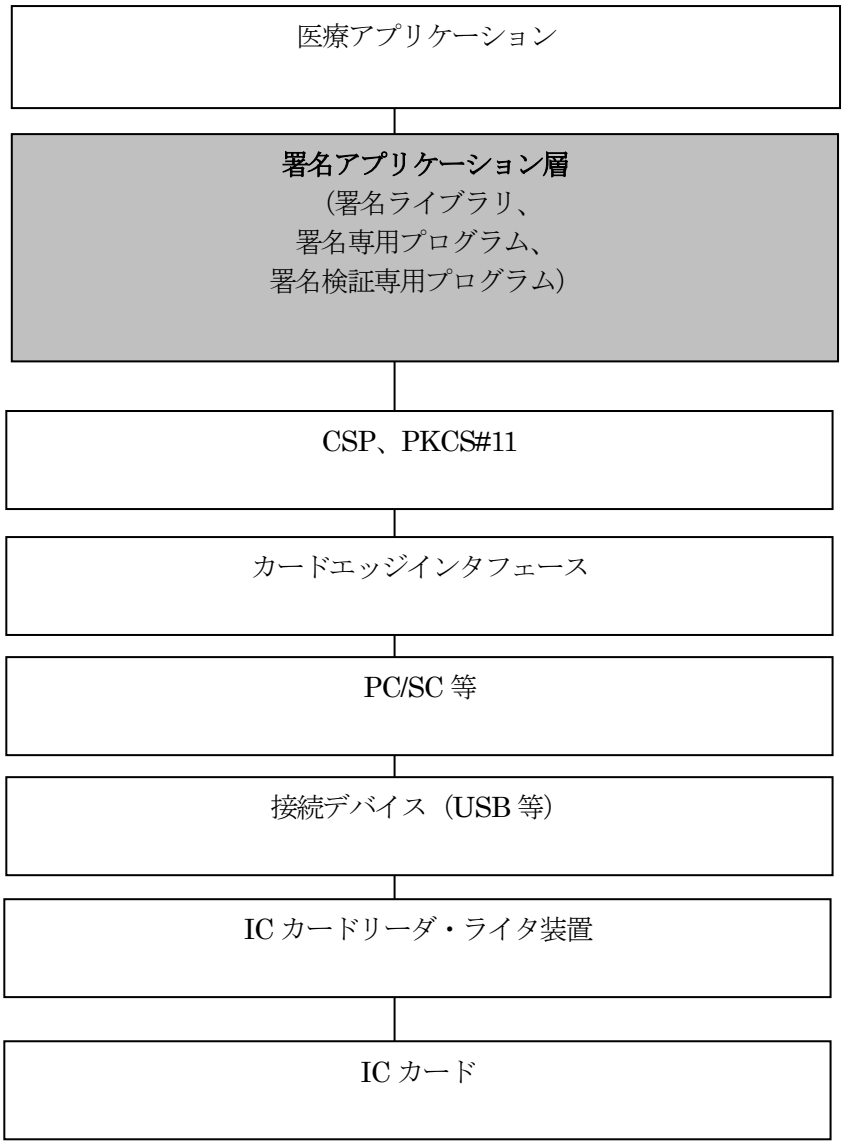

図 1.3.2 処理階層の例

1.4 対象となるユースケース

1.4.1 概要

署名は、電子記録の否認防止の目的で電子データに付与される。実際の医療機関における運用において、対象となるユースケースは下記のように分類されると考えられる。

(1) 対外文書（診療情報提供書、診断書など）に対する電子署名
(2) 法令等で保存が義務付けられた文書の電子保存を目的とした電子署名
(3) その他の内部文書（検査レポート、読影レポートなど）に対する電子署名
(4) 紙文書をスキャナにより電子化して保存する際の電子署名（e 文書法対応）
(5) アクセスログへの電子署名

以下に、上記の分類に基づいてユースケースを記述するが、これは、網羅的なリストではなく、代表的なユースケースの一例であることに留意されたい。

1.4.2 対外文書に対する電子署名

医療機関から外部組織に対して発行される文書（印刷物）には多様なものがあるが、電子化が考えられる対外文書として下記のようなものが考えられる。

- 退院証明書、診断書
- 診療情報提供書（いわゆる「紹介状」）
- カルテ開示要求による情報提供（カルテ情報）
- 治験結果

これらの文書を電子化した場合には長期に保存する運用が想定されるため、本規格で定める長期署名が有効であろう。署名を適用する場合のユースケースは下記のように考えられる。

- 退院証明書、診断書

何らかの申請の際に必要な文書であり、受領側がその内容の真正性と作成者の属性（医師の資格属性等）を確認する必要がある。これらの書類が電子化された場合には、電子署名が付与されていることにより、容易にその真正性と作成者の属性（hcRole）を受領者側が確認できるため、電子署名の有効なケースであると考えられる。

- 診療情報提供書

地域医療を支援する施設では、病院/診療所から発行された診療情報提供書は医師の記名押印または署名が必要である。電子化した場合にも電子署名が必要である。受領者側においても、必要な期間内での妥当な検証が行えることを保証する必要があるため、電子署名の有効なケースであると考えられる。

- カルテ開示要求による情報提供

患者からのカルテ開示要求に従って、電子カルテの内容を出力して提供するもの。基本的に医療機関から患者への情報提供であるため、内容の真正性担保及び否認防止機能への要求は高い。電子署名が有効なケースであると考えられる。

- 治験結果

医療機関等にて治験結果を電子的に作成する際、個人情報が含まれる場合は「安全管理ガイドライン」に準拠した取り扱いが必要である。また、厚労省の「医薬品等の承認又は許可等に係る申請等に関する電磁的記録・電子署名利用のための指針」（平成 17 年 4 月 1 日発行、通称 ER/ES 指針）に従った電子署名を付与する必要がある。治験結果は長期に保存する運用が想定されるため、本規格で定める長期署名が有効であろう。

1.4.3 法令等で保存が義務付けられた文書の電子保存を目的とした電子署名

法令等により医療機関に保存が義務付けられた文書には、たとえば下記のようなものがある。

（参考：「厚生労働省：第９回医療情報ネットワーク基盤検討会
参考資料２　法令上作成保存が求められている書類」
https://www.mhlw.go.jp/shingi/2004/06/s0624-5e.html）

- 診療録（医師、歯科医師、等）
- 助産録（助産師）
- 歯科技工に係る指示書（歯科医師）
- 救急救命処置録（救命救急士）
- 記録（歯科衛生士）
- 照射録（診療放射線技師）
- 処方箋（医師、歯科医師）
- 調剤録（薬剤師）
- 病院日誌（病院）
- 各科診療日誌（病院）
- 手術記録（病院）
- 検査所見記録（病院）

平成 11 年 4 月の通知「診療録等の電子媒体による保存について」によって、これらの文書のうち法令で記名・押印を行う義務のあるもの以外の電子的保存が認められた。さらに、その後の「e 文書法」の施行により、電子署名を付与することで電子的な保存が認められた文書が追加された。ここで、電子保存が認められている文書の一覧については、常に最新版の「安全管理ガイドライン」を参照すること。

これらの文書を電子化した場合に想定される署名の必要性の程度、及び署名を適用する場合のユースケースは下記のように考えられる。いずれの場合においても、一般に電子証明書の有効期間は、法定保存期間よりも短いが、法定保存期間内での検証が保証されていなければならない。したがって、本規格で定める長期署名方式が必要となる。

- 法令等により記名・押印を行う義務のある文書

  法令等により記名・押印が義務付けられているのであるから、電子的な保存にあたっての電子署名の付加は必須である。この際の電子署名付与の手順は下記の通りである。

  1. 当該の文書を発行する際に、発行者の電子署名を行う。
  2. 「安全管理ガイドライン」に従い、電子署名を行った情報を「真正性」「見読性」「保存性」を保った方法で保存する。

- 法令等により記名・押印を行う義務のない文書

  法令等による記名・押印の義務がないので、電子署名の適用は必須ではないが、「真正性」と否認防止の上で、技術的対策を行う場合には電子署名の付与が望ましい。

  署名付与の手順等は、上記の「法令等により記名・押印を行う義務のある文書」のケースと同じである。

1.4.4 内部文書に対する電子署名

ここでいう「内部文書」は、上記の「法令等で保存が義務付けられた文書」を除外して考える。具体的には各医療機関が独自に規定する、「検査レポート」及び「読影レポート」のようなものである。各種の伝票類もこれに含まれると考えられるが、電子カルテが運用されている医療機関であれば、オーダエントリシステムも運用されていると思われるので、これらが別に扱われるケースはないかもしれない。若干意味合いは異なるが、hcRole のマネジメントの用途で、「契約書」のようなものもこの範疇と考えてよい。

1.4.5 紙文書をスキャナにより電子化して保存する際の電子署名（e 文書法対応）

e 文書法に基づき、診療記録を電子化（紙による記録のスキャンによる読み取り）する際にはその作業者(または、責任者) の署名を行い、責任の所在をトレースできるようにする。電子化された診療記録は、記録が改ざんされていないかどうかを、任意に検証することができる。診療のつど発生する検査伝票などを電子

化する場合と比較すると、過去に蓄積された紙カルテなどの文書を電子化する場合では、より厳格な運用が求められるのでガイドラインに従い適切な運用を行う必要がある。

１.４.６ アクセスログへの電子署名

電子記録に対するアクセスログは、膨大なデータになるため、一定期間を超えたものは、別の単位として保存される。アクセスログを退避する際においても、その改ざんが行われていないことを保証するために、システム管理者の署名を付けることが考えられる。

第２章　引用規格・引用文献

【1】保健医療福祉分野 PKI 認証局　署名用証明書ポリシ 1.9 版, 厚生労働省, 2023

【2】CAdES

(1) “CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures”, EN 319 122-1 及び”CAdES digital signatures; Part 2: Extended CAdES signatures”, EN 319 122-2
注記　https://www.etsi.org/standards から入手可能。

(2) "Cryptographic Message Syntax", IETF RFC5652 及び"Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility", IETF RFC5035
注記　https://www.ietf.org/standards/rfcs/から入手可能。

(3) “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)", ISO 14533-1:2022

【3】XAdES

(1) XML 署名仕様
XML-Signature Syntax and Processing W3C Recommendation 11 April 2013 及び IETF RFC3275
注記　https://www.w3.org/TR/xmldsig-core/から入手可能。

(2) “XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures”,　EN 319 132-1 及び”XAdES digital signatures; Part 2: Extended XAdES signatures”, EN 319 132-2
注記　https://www.etsi.org/standards から入手可能。

(3) “Processes, data elements and documents in commerce, industry and administration − Long term signature − Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)”, ISO 14533-2:2021

(4) "https://www.w3.org/TR/XAdES/", W3C Note

【4】PAdES

(1) "Document management — Portable document format — Part 2: PDF 2.0", ISO 32000-2:2020

(2) " 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)", ISO 14533-3:2017

【5】JAdES

(1) “JAdES digital signatures;Part 1: Building blocks and JAdES baseline signatures”, TS119 182-1
注記　https://www.etsi.org/standards から入手可能。

(2) IETF RFC 7515 (May 2015):　JSON Web Signature (JWS)
注記　https://datatracker.ietf.org/doc/html/rfc7515/から入手可能。

【6】FIPS PUB 140-2 "Security Requirements for Cryptographic Modules",National Institute of Standard Technology, Dec 3, 2002

【7】"Internet X.509 Public Key Infrastructure Time-Stamp Protocol", IETF RFC3161 及び"ESSCertIDv2 Update for RFC 3161", IETF RFC5816

第３章　用語の定義

【あ】

・アクセスログ
　情報の作成、変更、参照、削除などの記録。

・アプリケーション
　特定の目的を果たすための機能を提供するソフトウェア。

・インタフェース
　プログラム、装置及び操作者といった対象の間で情報のやりとりを仲介するもの。また、その規格。

【か】

・改ざん
　情報を管理者の許可を得ずに書き換える行為。

・見読性
　電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること。
　（「医療情報システムの安全管理に関するガイドライン　第 5.2 版」厚生労働省）

・公開鍵証明書
　加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の加入者情報、公開鍵、CA の情報、その他証明書の利用規則等が記載され、CA の署名が付される。
　（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

【さ】

・失効
　有効期限前に、何らかの理由（盗難・紛失など）により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には CA の判断で失効されることもある。
　（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

・失効情報
　公開鍵証明書の有効性を確認できるよう、認証局から開示される情報。無効になった証明書のシリアル番号等をリストアップした失効リスト（CRL: Certification Revocation List）、又はオンラインでの証明書有効性の確認要求に対し応答を返す OCSP レスポンダ（OCSP: Online Certificate Status Protocol）があるが、CRL を採用している認証局が一般的。また、認証局は通常、証明書の有効期限を越えて失効情報を開示していない。

・私有鍵
　公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の所有者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。
　（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

・証明書ポリシ(CP: Certificate Policy)
　共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。
　（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

・署名検証
　電子署名が正当なものか確認する行為。以下のように証明書検証と署名値の検証から構成される。
　（証明書検証：証明書の正当性、有効性の検証）
　　①　署名に用いた証明書が正当な認証局から発行されたものであること

② 署名当時に証明書の有効期間が切れていないこと
③ 失効していない有効な証明書で有ったこと
（署名値の検証：署名対象データが改ざんされていないかどうかの検証）
④ 署名対象文書のハッシュ値と署名データから得られるハッシュ値が等しいこと

・真正性
正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていること。
（「医療情報システムの安全管理に関するガイドライン　第 5.2 版」厚生労働省）

・相互運用性
異なったアプリケーション又はシステム、構成コンポーネント間で情報の伝達または共有がなされ相互に接続、あるいは利用できる共通性を持つこと。

【た】

・タイムスタンプ
デジタルデータに対し「その情報がある時刻以前に存在し、その後改ざんされていない」ことを証明する技術の事。その証明のためにタイムスタンプ局から発行されるデータをタイムスタンプトークンというが、略してタイムスタンプと呼ばれることもある。

・デバイス
コンピュータに搭載あるいは接続されるハードウェア。

・電子署名
電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。
（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

【な】

・認証局(CA: Certification Authority)
電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。
（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

・認証パス(Certification Path)
信頼点（トラストアンカ）となる CA から検証対象である証明書までを結ぶ一連の証明書の繋がり。

【は】

・ハッシュ関数
任意の長さのデータから固定長のランダムな値を生成する計算方法。生成した値は「ハッシュ値」と呼ばれる。ハッシュ値は、ハッシュ値から元のデータを逆算できない一方向性と、異なる 2 つのデータから同一のハッシュ値が生成される衝突性が困難であるという性質を持つ。この性質からデータを送受信する際に、送信側の生成したハッシュ値と受信側でデータのハッシュ値を求めて両者を比較し両者が一致すれば、データが通信途中で改ざんされていないことが確認できる。
（「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版）」（厚生労働省））

・否認防止
電子署名により発信者が後でその文書を作成したことなどを否認出来ないようにすること。

・保存性
記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されること。
（「医療情報システムの安全管理に関するガイドライン　第 5.2 版」厚生労働省）

【ら】
・ライブラリ
ある機能を提供するプログラム部品群。単体では動作せずソフトウェアの一部として組み込まれることで機能する。

【C】
・CDA (Clinical Document Architecture)
診療に関する文書を、電子的にシステム間で交換する目的で定められた文書のマークアップ規格。
・CSP(Cryptographic Service Provider)
Microsoft 社による暗号化のためのソフトウェアコンポーネント。

【E】
・ES-BES
CAdES、XAdES、PAdES、JAdES における基本署名フォーマット。署名者の情報と署名を格納したもの。署名対象文書を含む場合と含まない場合がある。
・ES-T
ES-BES フォーマットに署名タイムスタンプを付加したフォーマット。タイムスタンプにより署名時刻の証拠性が担保できる。
・ES-C
ES-T フォーマットに対し、検証情報を特定できるよう署名者及びタイムスタンプ局の証明書を検証するために必要な各証明書および失効情報のハッシュ値のリストを追加したもの。現在ほとんど使用されないフォーマットであり本書では対象としない。
・ES-XL
ES-T フォーマットまたは ES-C フォーマットに対し、各証明書および CRL を追加し、署名及びタイムスタンプの有効性検証に必要な情報を組み込んだもの。
・ES-A
ES-XL の署名データ及び検証情報全体にアーカイブタイムスタンプを付与したもの。署名暗号アルゴリズムの脆弱化に起因する署名データの改ざんを保護できる。

【H】
・HL7 (Health Level Seven)
保健医療情報交換のための標準規格の名称、また、その策定団体の名称。
・HPKI (Health care PKI)
保健医療福祉分野での公開鍵基盤。

【I】
・ISO(International Organization for Standardization)
電気分野を除く全産業分野の国際的な標準規格を策定するための団体。

【J】
・JSON(JavaScript Object Notation)
データ記述言語の一つ。名称と構文は JavaScript におけるオブジェクトの表記法に由来する。

・JWS(JSON Web Signature)
RFC7515 で定義されるデジタル署名またはメッセージ認証コードで保護された JSON を使用したコンテンツを表す。

【O】

・OID(Object IDentifier)（オブジェクト識別子）

オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

(「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版)」(厚生労働省))

【P】

・PC/SC(Personal Computer / Smart Card)

Microsoft 社による、各社が製造する IC カード、IC カードリーダ・ライタを、Windows 環境上で相互利用できるようにするためのインタフェース仕様。

・PDF(Portable Document Format)

ISO 32000-2 で定義される Portable Document Format のファイルフォーマット。

・PKCS#11

米 RSA Security 社が定めた公開鍵暗号技術をベースとした規格群である PKCS (Public Key Cryptography Standards)の内、暗号トークンに関するインタフェース標準。

・PKI(Public Key Infrastructure)

公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。

(「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ（1.9 版)」(厚生労働省))

【T】

・TSA(Time Stamping Authority)

タイムスタンプ局のこと。時刻の信頼性及び信頼できる第三者機関であることが求められるが、「時刻認証業務の認定に関する規程」（令和 3 年 4 月 1 日、総務省告示第 146 号）に基づく認定制度がある。

【W】

・W3C(World Wide Web Consortium)

WWW で利用される技術の標準化をすすめる団体。

【X】

・XML(eXtensible Markup Language)

文書及びデータの意味及び構造を記述するためのマークアップ言語の一つ。

第４章　記号および略号

この規格では、次の記号および略語／表記を用いる。

PKI	公開鍵暗号基盤（Public Key Infrastructure）
CA	認証局（Certificate Authority）
CRL	証明書失効リスト（Certificate Revocation List）
OCSP	オンライン証明書状態取得プロトコル（Online Certificate Status Protocol）
CP	証明書ポリシ(Certificate Policy)
CDA	医療文書規格(Clinical Document Architecture)
CSP	(Cryptographic Service Provider)
DSS	(Document Security Store)
ES-BES	電子署名(Electronic Signatures Basic Electronic Signature)
ES-C	(Electronic Signatures Complete validation reference data)
ES-T	(Electronic Signatures Time-stamped)
ES-XL	(Electronic Signatures eXtended long validation data)
ES-A	(Electronic Signatures Archive validation data)
HL7	(Health Level Seven)
HPKI	(Health care PKI)
ISO	国際標準化機構(International Organization for Standardization)
JSON	(JavaScript Object Notation)
JWS	(JSON Web Signature)
OID	オブジェクト識別子(Object IDentifier)
PDF	(Portable Document Format)
PKCS	(Public Key Cryptography Standards)
PKI	公開鍵暗号基盤（Public Key Infrastructure）
PC/SC	(Personal Computer / Smart Card)
TSA	(Time Stamping Authority)
VRI	(Validation-Related Information)
W3C	(World Wide Web Consortium)
XML	(eXtensible Markup Language)

第５章　本規格で規定する電子署名方式の概要

５.１ 電子署名の基本要件

「医療情報システムの安全管理に関するガイドライン(第 5.2 版)」6.12 章で示された、電子署名、タイムスタンプの要件は、JAHIS にて「保存が義務付けられた診療録等の電子保存ガイドライン Ver.4」(2022 年 6 月：JAHIS 標準 22-007) の 6.8 章にて解説しているので参照されたい。本規格では、さらに電子署名とタイムスタンプの付し方について実装のガイドとして、より具体的に規定するものである。

電子署名に求められる基本的な要件は、上記の厚労省ガイドライン及び JAHIS ガイドラインで示されているように、

(1) 有効な証明書を用いて電子署名を付与すること

(2) 法定保存期間等、署名対象文書の真正性の維持継続が必要な期間、電子署名の検証が可能であることの２点である。"電子署名の検証"とは、「署名に用いた証明書が正当な認証局から発行されたもので、署名当時に有効期間が切れておらず、失効していない有効な証明書で有ったこと」を確認する"証明書検証"と「署名対象文書が改ざんされていないこと」を確認する"署名値の検証"から成る。図 5.1.1 に署名と検証の概要を示す。

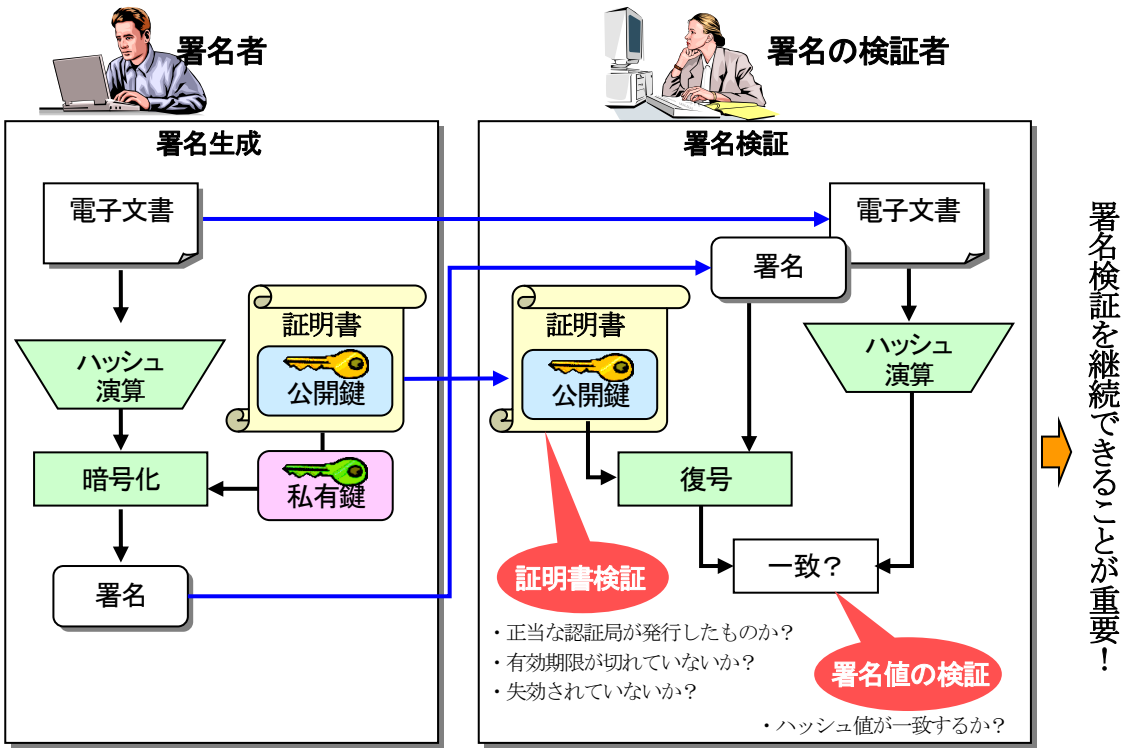

図 5.1.1 署名と署名検証

法定保存期間が定められた文書を保存する場合、将来にわたり一定期間、署名検証が可能であることが必要となる。その際、特に「証明書検証の継続性」に対して留意する必要がある。証明書検証に際しては図 5.1.2 に示すように、以下の 3 点を確認する。

(1) 署名に用いた証明書が正当な認証局から発行されたものであること

(2) 署名当時に証明書の有効期間が切れていないこと

(3) 失効していない有効な証明書を用いて署名していたこと

ここで、上記(1)及び、(2)を実現するために、署名時刻が何時であったのか客観的に示せる事が必要となる。またその時点での証明書の有効性を確認するためには、失効情報を保管する必要がある。

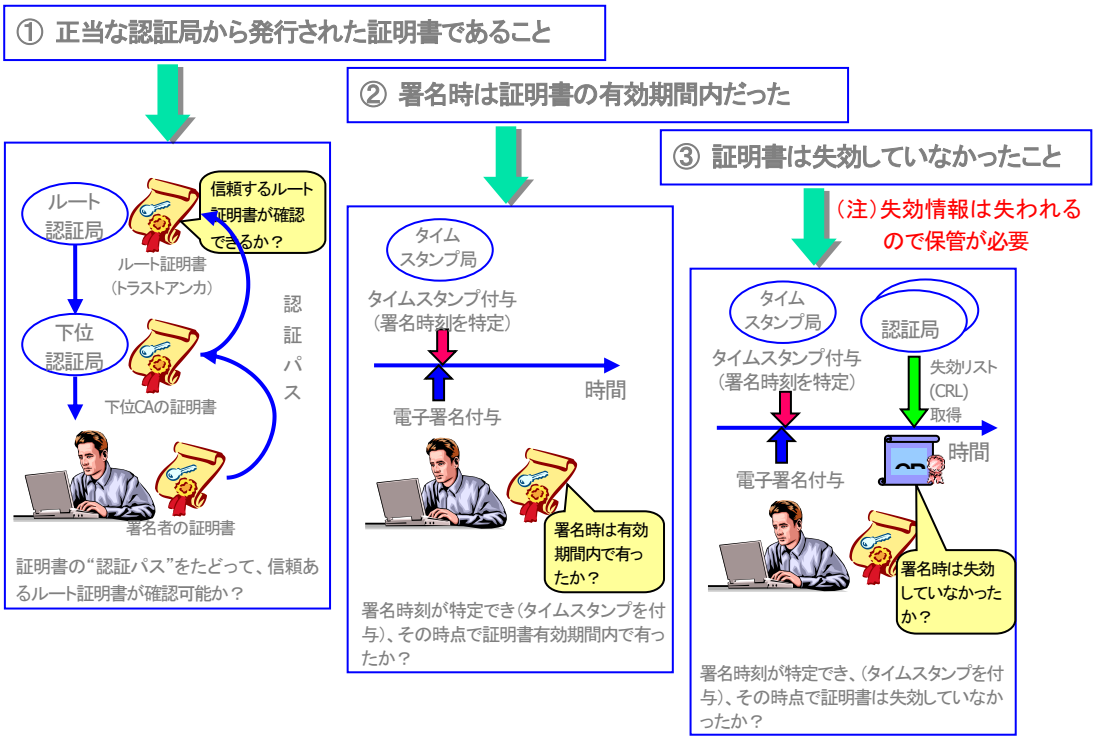

図 5.1.2 証明書検証の要素

通常、認証局は証明書の有効期間を越えて失効情報の公開はしていないので、その期間を過ぎると証明書の有効性の確認が出来ないことになる。即ち、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。

したがって、本規格が参照する CAdES【2】、XAdES【3】、PAdES【4】又は JAdES【5】の標準仕様に示されるように、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) 署名後すみやかに「署名タイムスタンプ」を付与し、その時刻に署名が存在していたことを証明できるようにしておく
(3) 証明書検証に必要となる、以下の検証情報を収集格納する。
タイムスタンプ局の証明書、署名者の証明書、認証パス上の認証局の証明書[1]
上記のすべての認証局の失効情報
(4) 上記の署名対象文書及び署名値、検証情報全体に対して「アーカイブタイムスタンプ」を付与

図 5.1.3 に上記手順のフローイメージを示す。ここで、各タイムスタンプの役割は、

・署名タイムスタンプ
電子署名時刻の信頼性を確保する
・アーカイブタイムスタンプ
署名文書と失効情報をタイムスタンプの暗号アルゴリズムにより保護し、長期に渡り電子署名の真正性を継続することにある。すなわち、タイムスタンプによりその時刻に署名が存在していたことを確認し、有効な証明書を用いて署名した事を後日検証可能とするのである。

[1]認証パス上の認証局は、署名者の証明書を発行する認証局とタイムスタンプ局に証明書を発行する認証局の 2 つの認証パス上の認証局となることに留意されたい。

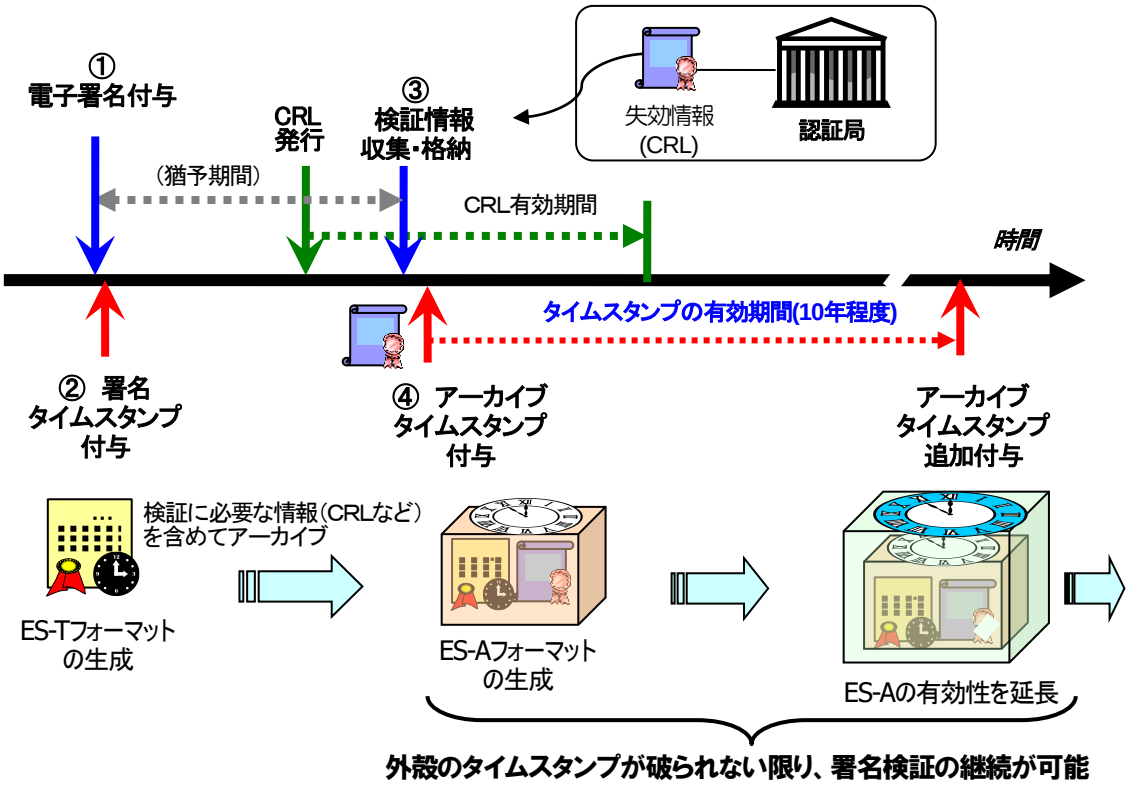

図 5.1.3 長期署名フォーマットによる署名延長

5.2 失効情報の取得タイミング

署名タイムスタンプを付与した後に、検証情報を収集格納するが、この際取得する失効情報は、大前提として証明書の有効期間内に取得する必要がある。これは、大多数の認証局が証明書の有効期間を過ぎて失効情報を公開していないため、証明書有効期間終了までに失効情報を取得しないと失効情報が失われてしまう恐れがあるためである。また、署名後、あまり長期間経過すると使用されているハッシュ及び暗号アルゴリズムの脆弱化、認証局及びタイムスタンプ局の私有鍵の危殆化などのリスクが考えられる。したがって、失効情報を適切なタイミングで取得し、アーカイブタイムスタンプを付与すべきであろう。

失効情報を証明書が有効なうち取得するのであれば、その取得タイミングに法及び省令、技術標準等での定めはないが、電子署名を付与した後、一定の猶予期間をおいて取得することが望ましいとされている。これは、万一、不正に入手した証明書（私有鍵）で電子署名を付与されることを防止するためである。

失効情報を取得するタイミングは、証明書の有効期間内であれば任意に決めることができるが、以下の 2 種類のリスクに留意されたい。

(1)　正しい署名を無効とするリスク（第 1 種のエラー）
署名の有効性を消失してしまうリスク。
署名当時は有効な署名であったにもかかわらず、その後、使用しているハッシュ及び暗号アルゴリズムの脆弱性が発見されたり、万一、認証局及びタイムスタンプ局の私有鍵の危殆化が発生されたりした場合、署名の有効性が疑われてしまう。有効なアーカイブタイムスタンプを付与する前に、このような事態が発生した場合は有効な長期署名フォーマットが作成出来なくなる。

(2)　不正な署名を有効とするリスク（第 2 種のエラー）
失効が未反映の失効情報を取得してしまうリスク。
不正に取得した証明書（私有鍵）で署名したデータであるにもかかわらず、失効情報取得のタイミングが早過ぎ、その証明書失効がまだ反映されていない失効情報を用いて長期署名フォーマットを作成してしまうケース。このような不正な署名文書を提出された場合、反論が困難となる。

上記のリスクを考慮した、失効情報の取得タイミングのイメージを図 5.2.1 に示す。
なお、たとえ、署名後に不慮の証明書失効が有ったとしても、署名タイムスタンプがすでに付与されている場合、署名時刻が特定可能であり、失効情報中の失効時刻と比較し、失効前に署名されていることが証明できる。
実際に失効情報の取得タイミングを決定する際には、署名者の証明書の有効期限及び署名対象文書の利用形態、運用要件と、上記のリスクを勘案して判断されることとなる。

私有鍵の管理方法が厳格であれば、失効リスクが少なくなり、上記、第 2 種のエラーは減少する。例えば、署名されたドキュメントを同一日に相手先に配布する必要が有る場合、私有鍵をサーバ又は HSM（Hardware Security Module）に格納して厳格に管理し、私有鍵へのログオン認証も 2 要素認証とするなど、私有鍵の危殆化可能性を低くした上で、同一日に失効情報を取得する運用も考えられる。また、署名済みのドキュメントはその後、アーカイブされるだけなら、月次処理で失効情報を取得する運用も考えられる。その際は、署名後の証明書の有効期間が常に 1 ヶ月以上あるような運用が前提となる。
HPKI の証明書を用いる場合は、厚生労働省の証明書ポリシにて、「エンドエンティティの加入者の公開鍵証明書の有効期間は発行の日後の加入者の 5 回目（加入者が発行を受けている署名用電子証明書の有効期間が満了する日の前に、CPS で定める更新の期間内に加入者が新たな署名用電子証明書の発行の申請をし、新たな署名用電子証明書の発行を受けるときにあっては 6 回目）の誕生日とする。」とされている。証明書の有効期間内であれば、任意の時点で失効情報を取得し、長期署名フォーマットを構築する事が可能である。
なお、アーカイブタイムスタンプも証明書の有効期間内に付与する必要があるが、第 1 種のエラーを考慮し署名ドキュメントを保護する意味で、検証情報を格納した後のなるべく早い時期に付与することが望ましい。

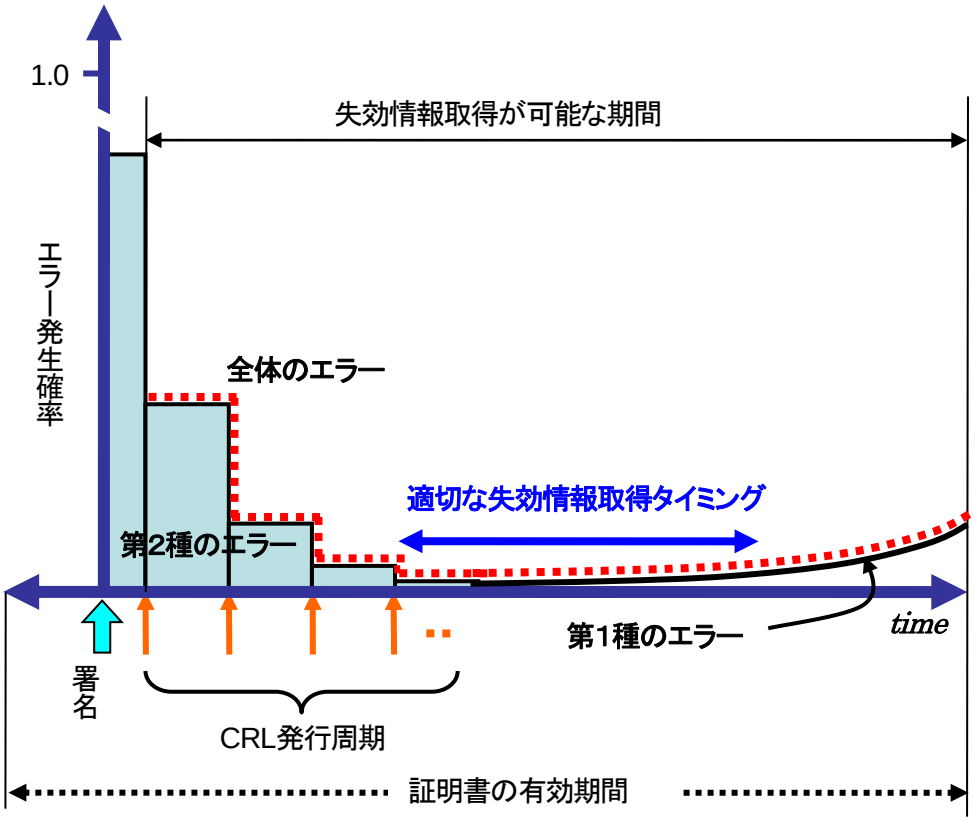

図 5.2.1 失効情報の取得のタイミングのイメージ

５.３ 署名データの形式について

署名対象データと署名データとを１つのファイルに統合して作成することもできるが、独立した２つのファイルとして作成する事もできる。署名対象データと署名データとの形式には、図 5.3.1 に示されるように、以下の３つがある。

(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場合。署名対象データの形式は問わず、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。既存アプリで署名対象データを取り扱っている場合など、アプリ側への影響が少なくて済む。一方、署名対象データと署名データを紐づけて管理する必要がある。

(2)　内包形式（Enveloping 型）

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

(3)　包含形式（Enveloped 型）

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

署名の形式は、署名対象データのファイル形式、それを利用するアプリケーションの要件等により、どの形式を採用するか適切に判断して選択されたい。

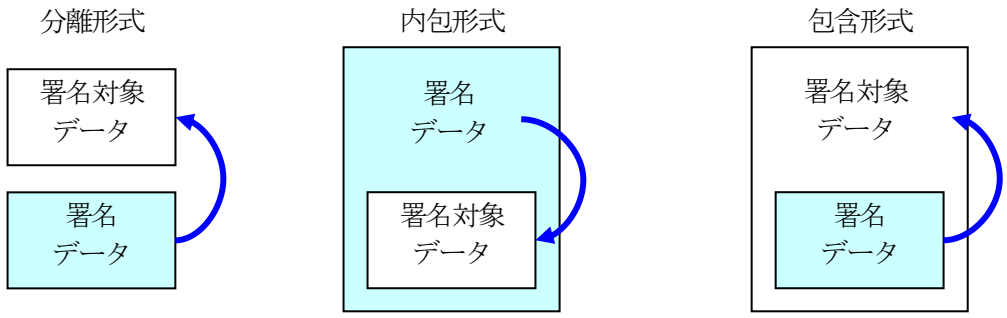

図 5.3.1 署名対象データと署名データとの形式

５.４ 複数人による署名について

複数人により署名が付与されるケースは、図 5.4.1 に示されるように、以下の３つの分類に大別できる。

(1)　並列署名（Independent Signature）

同一の文書を署名対象として、各自がそれぞれ署名するケース。契約書への署名など、同一文書を署名者全員が同意した際などに付与する署名。個々の署名は独立しており、複数の署名情報（SignerInfo、6 章で解説）を作成することにより、本規格の長期署名フォーマットを適用できる。

(2)　直列署名（Embedded Signature）

第 1 の署名者の署名データに対して第２の署名者が署名するケース。署名に対して署名を重ねて行く Counter Signature 属性を利用することにより作成される。稟議書及び報告書の承認のように署名の連鎖が有るような場合に適用される署名。本規格の長期署名フォーマットを応用し直列署名を作成することは可能であるが、直列署名への本規格の適用は規定しない。アプリケーション側にて、別途追加ルールを定めて運用することが必要となる。

(3)　直列署名の応用形

第 1 の署名者が署名した文書に、第２の署名者がコメントを追記し署名するケース。署名対象データと第１の署名者の署名データ、および自ら追記したコメント全体を対象として第２の署名を付与する。

読影医が署名した読影レポートへ、主治医がコメントして署名を付与するような場合への適用が考えられる。本規格の長期署名フォーマットをこのようなケースに応用する場合は、文書フォーマット及びアプリケーションで追記型署名の扱いについて別途規定する必要がある。

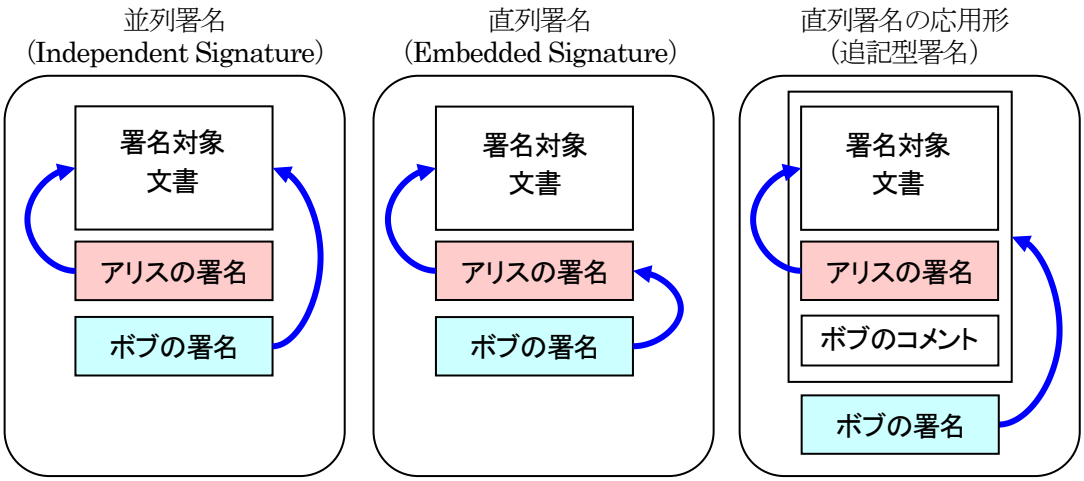

図 5.4.1 複数署名の種別

第６章　電子署名の規格

６.１ 電子署名の生成（共通事項）

署名フォーマットには以下の形式が含まれる。

・ES-BES　：署名者に関する情報と署名データを格納した形式
・ES-T　　：署名時刻を担保する署名タイムスタンプを付与した形式
・ES-C　　：署名検証のための一連の証明書と失効情報に対する参照情報を付与した形式。ただし、現在ほとんど使用されないフォーマットであり本書では特段取り扱わない。
・ES-XL　：署名検証のための一連の証明書と失効情報を格納した形式
・ES-A　　：署名データ及びタイムスタンプ、検証情報などを保護するためにアーカイブタイムスタンプを付与した形式

上記の各形式の関係を図示したものが図 6.1.1 である。

これらの形式のうち、ES-XL は ES-A を生成する過程の形式であると考え、本規格では ES-XL 単体での運用は対象外とする。また、ES-BES 形式についても署名時刻が確定できず署名付き文書を保存する用途には適さないため対象外とする。

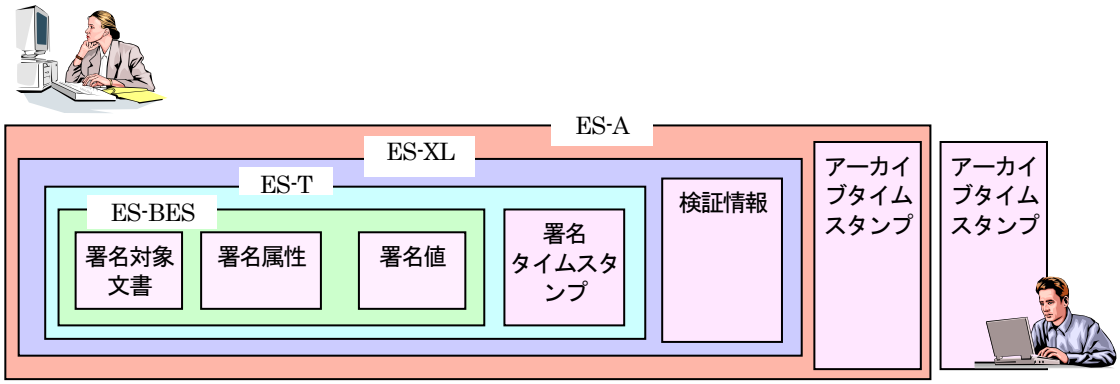

図 6.1.1 電子署名の形式の種類

署名フォーマットの規格には CMS(Cryptographic Message Syntax)に基づく CAdES【2】、XML 署名に基づく XAdES【3】、PDF 署名に基づく PAdES【4】及び JSON 署名に基づく JAdES【5】がある。署名対象となる文書フォーマット及びアプリケーションの用途に従って、いずれかの方式を選択することができる。

ES-T、ES-A を生成する場合に署名フォーマット中に含まれる必須の要素及び選択可能な要素を定めたプロファイルを、CAdES については 6.3 節で、XAdES については 6.4 節で、PAdES については 6.5 節で、JAdES については 6.6 節で規定する。

６.２ 電子署名の検証（共通事項）

６.２.１ 参照する規格・資料

検証の各工程の詳細は、CAdES、XAdES、PAdES 及び JAdES の標準規格並びにそれらを解説したガイドブック[2] などを参照すること。タイムスタンプは RFC3161【7】を想定する。

６.２.２ ES-BES の検証

６.２.２.１ ES-BES の検証プロセス

ES-BES 形式の検証プロセスを記述する。

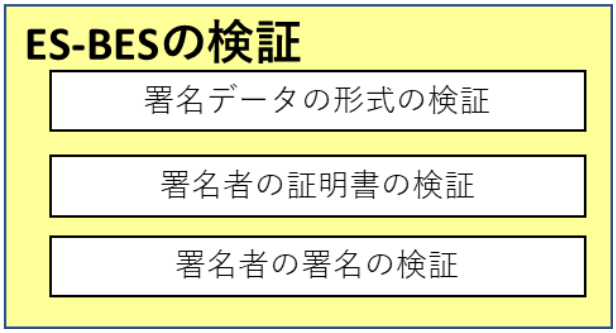

図 6.2.1 ES の検証プロセス

ES-BES 形式の検証は図 6.2.1 で記述したプロセスで行う。プロセス及び各工程の検証順序は問わない。

(1)　署名データの形式の検証

データ形式の正しさを検証する。

(2)　署名者の証明書の検証

署名者の証明書の有効性を検証する。以下の工程から成る。

(2-1) RFC5280 に準拠した検証

(2-2) HPKI 固有の検証

(3)　署名者の署名の検証

署名に改ざんがないことを検証する。以下の工程から成る。

(3-1)値の整合性の検証

(3-2)識別情報の整合性の検証

各プロセスの内容を 6.2.2.2 節で記述する。

[2] 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、平成 19 年 3 月

６.２.２.２ 検証プロセスの内容

検証プロセス	検証方法の概要
(1) 署名データの形式の検証	以下のすべてを確認する。 ･正しいデータ構造であること ･プロファイルで規定されている必須要素をもつこと ･バージョン番号の整合性
(2) 署名者の証明書の検証	(2-1) RFC5280 に準拠した検証 ･署名者の証明書に対して認証パス構築、認証パス検証を行う。
	(2-2) HPKI 固有の検証 以下のすべてを確認できるようにする。 ･HPKI 署名用証明書ポリシの OID を持つこと ･署名者証明書の hcRole 属性の値 確認方法に対する要件はこの文書の範囲外とする。利用形態に応じて適切な確認方法を講じること。
(3) 署名者の署名の検証	(3-1)値の整合性の検証 以下のすべてを確認する。 ･署名対象文書と、そのハッシュ値を照合する。 ･署名値を署名者の公開鍵により検証する。
	(3-2)識別情報の整合性の検証 ･署名者の識別情報と証明書が一致することを確認する。

６.２.３ ES-T の検証

６.２.３.１ ES-T の検証プロセス

ES-T 形式の検証プロセスを記述する。

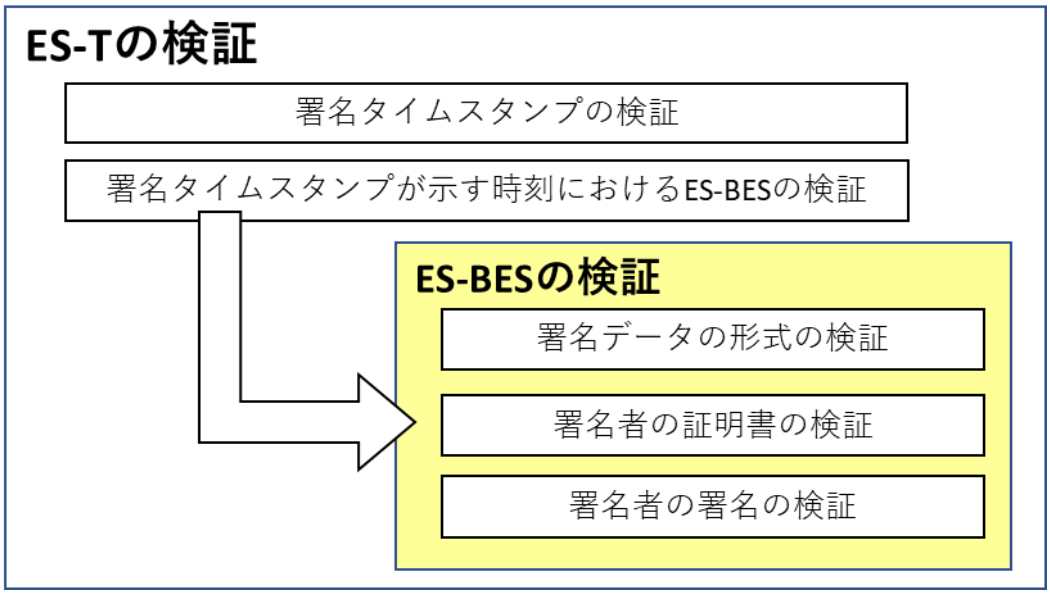

図 6.2.2 ES-T の検証プロセス

ES-T 形式の検証は図 6.2.2 で記述したプロセスで行う。プロセス及び各工程の検証順序は問わない。

(1)　署名タイムスタンプの検証

適切なタイムスタンプであることを検証する。以下の工程から成る。

(1-1) 署名タイムスタンプを発行した TSA の証明書の検証

(1-2) 署名タイムスタンプを発行した TSA の署名の検証

(1-3) 署名タイムスタンプとタイムスタンプ対象との整合性検証

(2)　署名タイムスタンプが示す時刻における ES-BES の検証

署名時刻に基づき ES-BES の検証を行う。以下の工程から成る。

(2-1) 署名時刻における ES-BES の検証

(2-2) ES-BES の信頼点の正当性の確認

各プロセスの内容を 6.2.3.2 節で記述する。

6.2.3.2 検証プロセスの内容

検証プロセス	検証方法の概要
(1) 署名タイムスタンプの検証	(1-1) 署名タイムスタンプを発行した TSA の証明書の検証 ·TSA 証明書に対して認証パス構築、認証パス検証を行い、検証時刻において有効な証明書であることを確認する。 ·TSA 証明書の鍵使用目的が適切であることを確認する。
	(1-2) 署名タイムスタンプを発行した TSA の署名の検証 ·TSA 証明書の公開鍵を用いてタイムスタンプトークンの署名値を検証する。
	(1-3) 署名タイムスタンプとタイムスタンプ対象との整合性検証 ·タイムスタンプトークンのハッシュ値と、タイムスタンプ対象となるデータ（署名者の署名値）を照合する。
(2) 署名タイムスタンプが示す時刻における ES-BES の検証	(2-1) 署名時刻における ES-BES の検証 署名タイムスタンプが示す時刻を想定して 6.2.2 節「ES-BES の検証」を実施する。署名タイムスタンプが示す時刻において、署名者の証明書が有効であることを確認する。
	(2-2) ES-BES の信頼点の正当性の確認 署名者の証明書に対する信頼点となる証明書の有効期限が経過するなど、ES-T データ生成後に長い期間を経た後に検証を行うことも考えられる。このような場合、(2-1)の認証パス検証で指定される信頼点が適切なものであるか確認する必要がある。 例えば、署名ポリシを記述するなど署名者と検証者の間で適切な信頼点に関する合意を明示化すること及び、認証局又は信頼できる第三者機関により管理された過去の証明書の識別情報と照合を行うなどが考えられるが、その具体的な方法はこの文書の範囲外とする。

６.２.４ ES-XL の検証

６.２.４.１ ES-XL の検証プロセス

ES-XL 形式の検証プロセスを記述する。

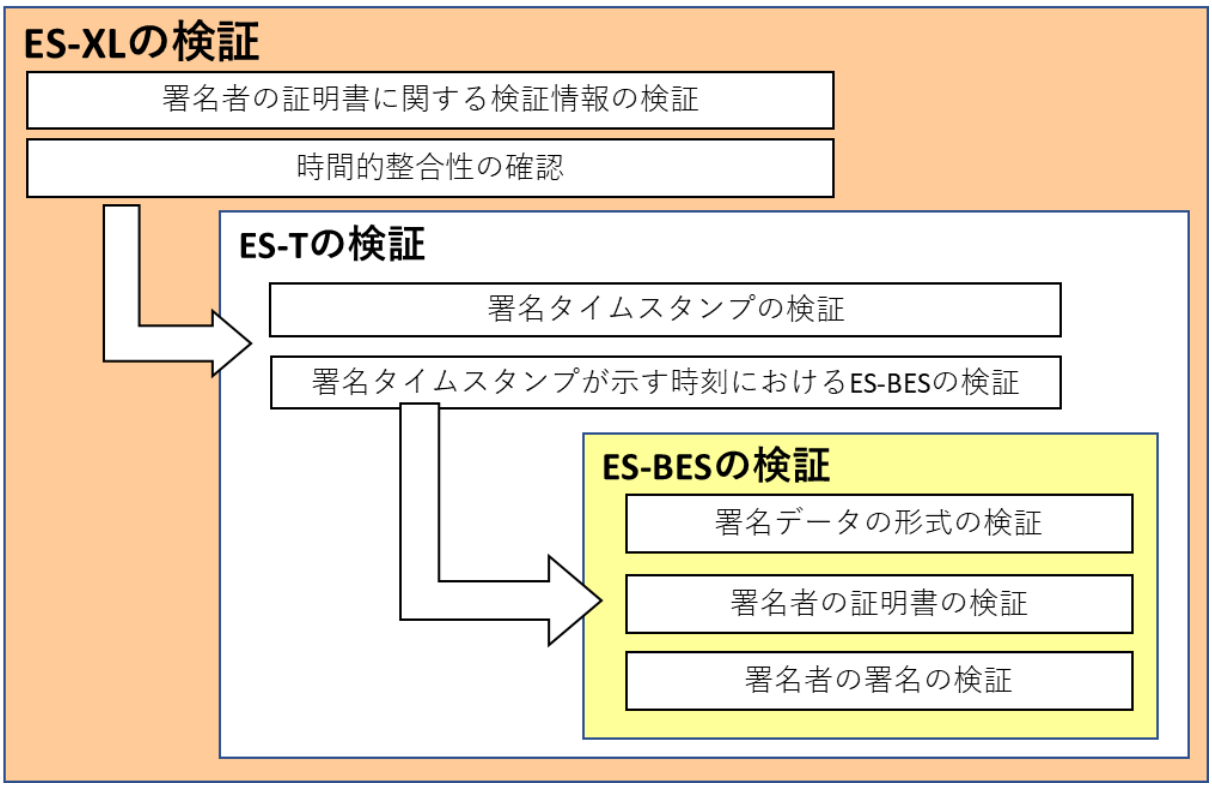

図 6.2.3 ES-XL の検証プロセス

ES-XL の検証は図 6.2.3 で記述したプロセスで行う。プロセス及び各工程の検証順序は問わない。

(1) 署名者の証明書に関する検証情報の検証
検証情報が適切であることを検証する。以下の工程から成る。
(1-1) 検証情報に含まれる証明書チェーンの有効性の検証
(1-2) 証明書の信頼点の正当性の確認
(1-3) 検証情報に含まれる失効情報の有効性の検証
(1-4) 失効情報の信頼点の正当性の確認

(2) 署名タイムスタンプの検証
適切なタイムスタンプであることを検証する。
(2-1) 検証時刻における署名タイムスタンプの検証
(2-2) 署名タイムスタンプの信頼点の正当性の確認

(3) 署名タイムスタンプが示す時刻における ES-BES の検証
署名時刻における ES-BES の有効性を検証する。
(3-1) 署名時刻における ES-BES の検証
(3-2) ES-BES の信頼点の正当性の確認

(4) 時間的整合性の確認

ES-XL は ES-T に対する検証情報が格納された ES-A 生成の際の中間フォーマットとして定義されている。

通常は ES-XL 単独で流通することは想定されていないが、ES-XL 単独で流通させるケースにおいて署名検証を行う際の注意点としては、中間フォーマットであるが故に検証時間の考え方、検証時の警告の仕方について、ES-XL 単独で利用するコミュニティ内でルールを作成し、適切に運用する必要がある。

６．２．４．２ 検証プロセスの内容

(1) 署名者の証明書に関する検証情報の検証 適切な検証情報が格納されていることを確認する。各懸賞情報の検証時刻における有効性を検証する。	(1-1) 検証情報に含まれる証明書チェーンの有効性の検証
	(1-2) 証明書の信頼点の正当性の確認
	(1-3) 検証情報に含まれる失効情報の有効性の検証 失効情報が発行された時間と検証時の時間を比較し、適切な失効情報であることを確認する。
	(1-4) 失効情報の信頼点の正当性の確認 失効情報の署名に用いられた証明書の有効性を検証するとき、その信頼点となる証明書が適切なものであることを確認する。
(2) 名タイムスタンプの検証	(2-1) 検証時刻における署名タイムスタンプの検証 検証時刻における TSA 証明書の有効性を検証する。
	(2-2) 署名タイムスタンプの信頼点の正当性の確認 署名タイムスタンプの TSA 証明書を検証する時点において、すでに信頼点となる証明書の有効性が切れていることが考えられる。(2-1)の認証パス検証を行う上で、信頼点となる証明書が適切なものであることを確認する。 その具体的な方法はこの文書の範囲外とする。
(3) 署名タイムスタンプが示す時刻における ES-BES の検証	(3-1) 署名タイムスタンプが示す時刻を想定し、(2)で有効性が確認された検証情報を利用して 6.2.2 節「ES-BES の検証」を実施する。
	(3-2) ES-BES の信頼点の正当性を確認する。 署名者の証明書を検証する時点において、すでに信頼点となる証明書の有効性が切れていることが考えられる。(3-1)の認証パス検証を行う上で、信頼点となる証明書が適切なものであることを確認する。その具体的な方法はこの文書の範囲外とする。
(4) 時間的整合性の確認	上記のうち時間的整合性確認で抜けている部分の整合性確認。署名タイムスタンプの時刻に対して検証情報の有効期間等の時刻の整合性を確認する。

６.２.５ ES-A の検証

６.２.５.１ ES-A 形式の検証プロセス

ES-A 形式の検証プロセスを記述する。

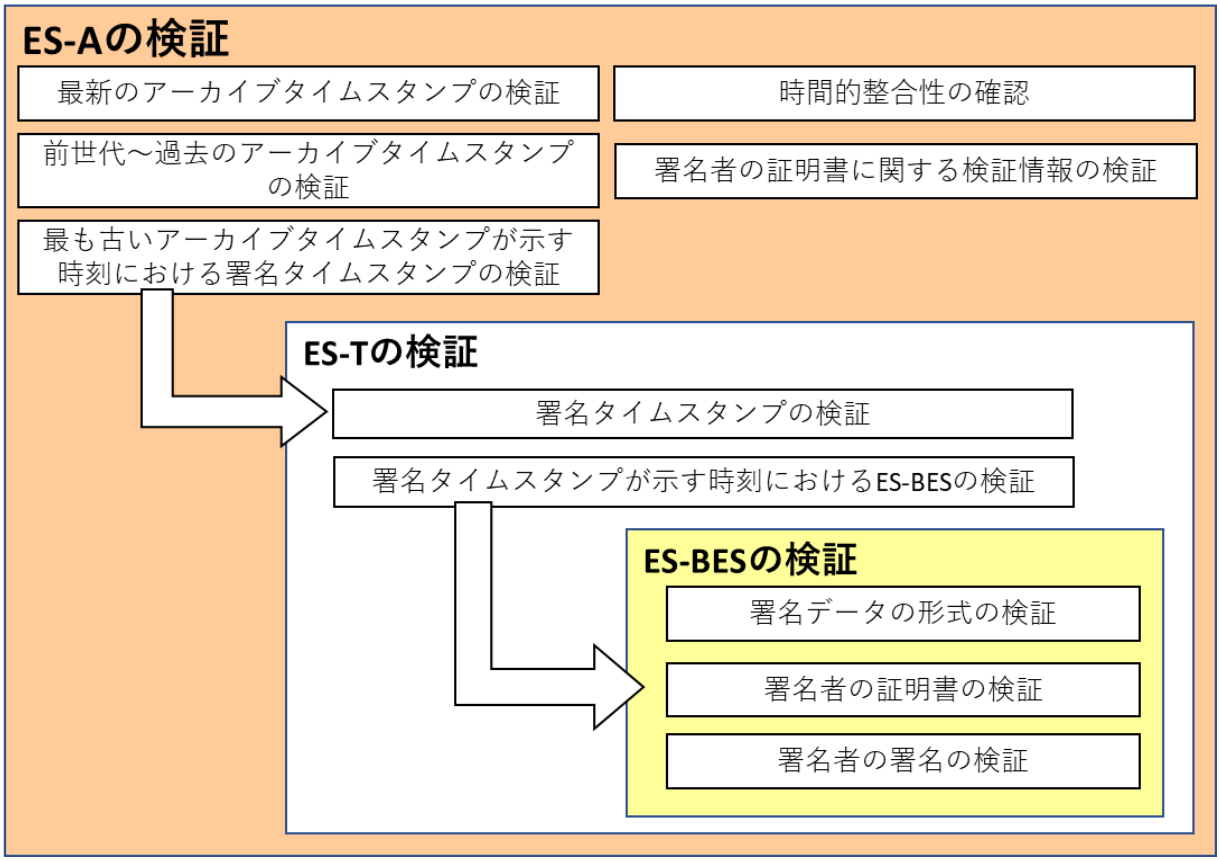

図 6.2.4 ES-A の検証プロセス

ES-A 形式の検証は図 6.2.4 で記述したプロセスで行う。プロセス及び各工程の検証順序は問わない。

(1)　最新のアーカイブタイムスタンプの検証

適切なタイムスタンプであることを検証する。以下の工程から成る。

(1-1) 最新のアーカイブタイムスタンプを発行した TSA の証明書の検証

(1-2) 最新のアーカイブタイムスタンプを発行した TSA の署名の検証

(1-3) 最新のアーカイブタイムスタンプとタイムスタンプ対象との整合性検証

(2)　前世代～過去のアーカイブタイムスタンプの検証（存在する場合）

アーカイブ時点で適切なタイムスタンプであったことを検証する。以下の工程から成る。

(2-1) アーカイブタイムスタンプを発行した TSA の証明書の検証

(2-2) アーカイブタイムスタンプを発行した TSA の署名の検証

(2-3) アーカイブタイムスタンプとタイムスタンプ対象との整合性検証

(2-4) アーカイブタイムスタンプの信頼点の正当性を確認する

(3)　署名者の証明書に関する検証情報の検証

アーカイブされている検証情報が適切であることを検証する。以下の工程から成る。

(3-1) 検証情報に含まれる証明書チェーンの有効性の検証

(3-2) 証明書の信頼点の正当性の確認

(3-3) 検証情報に含まれる失効情報の有効性の検証

(3-4) 失効情報の信頼点の正当性の確認

(4)　署名タイムスタンプの検証

適切なタイムスタンプであることを検証する。

(4-1) アーカイブ時刻における署名タイムスタンプの検証

(4-2) 署名タイムスタンプの信頼点の正当性の確認

(5)　署名タイムスタンプが示す時刻における ES-BES の検証

署名時刻における ES-BES の有効性を検証する。

(5-1) 署名時刻における ES-BES の検証

(5-2) ES-BES の信頼点の正当性の確認

(6)　時間的整合性の確認

各プロセスの内容を 6.2.5.2 節で記述する。

6.2.5.2 検証プロセスの内容

検証プロセス	検証方法の概要
(1) 最新のアーカイブタイムスタンプの検証	(1-1) 最新のアーカイブタイムスタンプを発行した TSA の証明書の検証 ·TSA 証明書に対して認証パス構築、認証パス検証を行い、検証時点における証明書の有効性を確認する。 ·TSA 証明書の鍵使用目的が適切であることを確認する。
	(1-2) 最新のアーカイブタイムスタンプを発行した TSA の署名の検証 ·TSA 証明書の公開鍵を用いてタイムスタンプトークンの署名値を検証する。
	(1-3) 最新のアーカイブタイムスタンプとタイムスタンプ対象との整合性検証 タイムスタンプトークンのハッシュ値と、タイムスタンプ対象となるデータ（アーカイブ対象領域）を照合する。
(2)前世代～過去のアーカイブタイムスタンプの検証（存在する場合） 検証対象となるアーカイブタイムスタンプに対し、 一世代後の（一世代新しい）アーカイブタイムスタンプが示す時刻を想定して「(1) 最新のアーカイブタイムスタンプの検証」と同様の検証を実施する。	(2-1) アーカイブタイムスタンプを発行した TSA の証明書の検証 一世代後のアーカイブタイムスタンプが示す時刻において、検証対象となるアーカイブタイムスタンプの TSA 証明書の有効性を確認する。 （検証時刻の関係は図 6.2.5 を参照のこと）
	(2-2) アーカイブタイムスタンプを発行した TSA の署名の検証
	(2-3) アーカイブタイムスタンプとタイムスタンプ対象との整合性検証
	(2-4) アーカイブタイムスタンプの信頼点の正当性の確認 アーカイブタイムスタンプの TSA 証明書を検証する時点において、すでに信頼点となる証明書の有効性が切れていることが考えられる。(2-1)の認証パス検証を行う上で、信頼点となる証明書が適切なものであることを確認する。その具体的な方法はこの文書の範囲外とする。
(3)署名者の証明書に関する検証情報の検証 適切な検証情報がアーカイブされていることを確認する。最も古いアーカイブタイムスタンプが示す時刻における有効性を検証する。	(3-1) 検証情報に含まれる証明書チェーンの有効性の検証
	(3-2) 証明書の信頼点の正当性の確認
	(3-3) 検証情報に含まれる失効情報の有効性の検証 失効情報が発行された時間とアーカイブタイムスタンプの時間を比較し、適切な失効情報であることを確認する。
	(3-4) 失効情報の信頼点の正当性の確認 失効情報の署名に用いられた証明書の有効性を検証するとき、その信頼点となる証明書が適切なものであることを確認する。
(4)署名タイムスタンプの検証	(4-1) アーカイブ時刻における署名タイムスタンプの検証 最も古いアーカイブタイムスタンプが示す時刻を想定して 6.2.3.2 節「(1) 署名タイムスタンプの検証」を実施する。最も古いアーカイブタイムスタンプが示す時刻における TSA 証明書の有効性を検証する。
	(4-2) 署名タイムスタンプの信頼点の正当性の確認 署名タイムスタンプの TSA 証明書を検証する時点において、すでに信頼点となる証明書の有効性が切れていることが考えられる。(4-1)の認証パス検証を行う上で、信頼点となる証明書が適切なものであることを確認する。その具体的な方法はこの文書の範囲外とする。
(5) 署名タイムスタンプが示す時刻における ES-BES の検証	(5-1) 署名タイムスタンプが示す時刻を想定し、(4)で有効性が確認された検証情報を利用して 6.2.2 節「ES-BES の検証」を実施する。

	(5-2) ES-BES の信頼点の正当性を確認する。 署名者の証明書を検証する時点において、すでに信頼点となる証明書の有効性が切れていることが考えられる。(5-1)の認証パス検証を行う上で、信頼点となる証明書が適切なものであることを確認する。その具体的な方法はこの文書の範囲外とする。
(6) 時間的整合性の確認	上記のうち時間的整合性確認で抜けている部分の整合性確認。 署名タイムスタンプの時刻、アーカイブタイムスタンプ時刻に対して時刻の整合性を確認する。

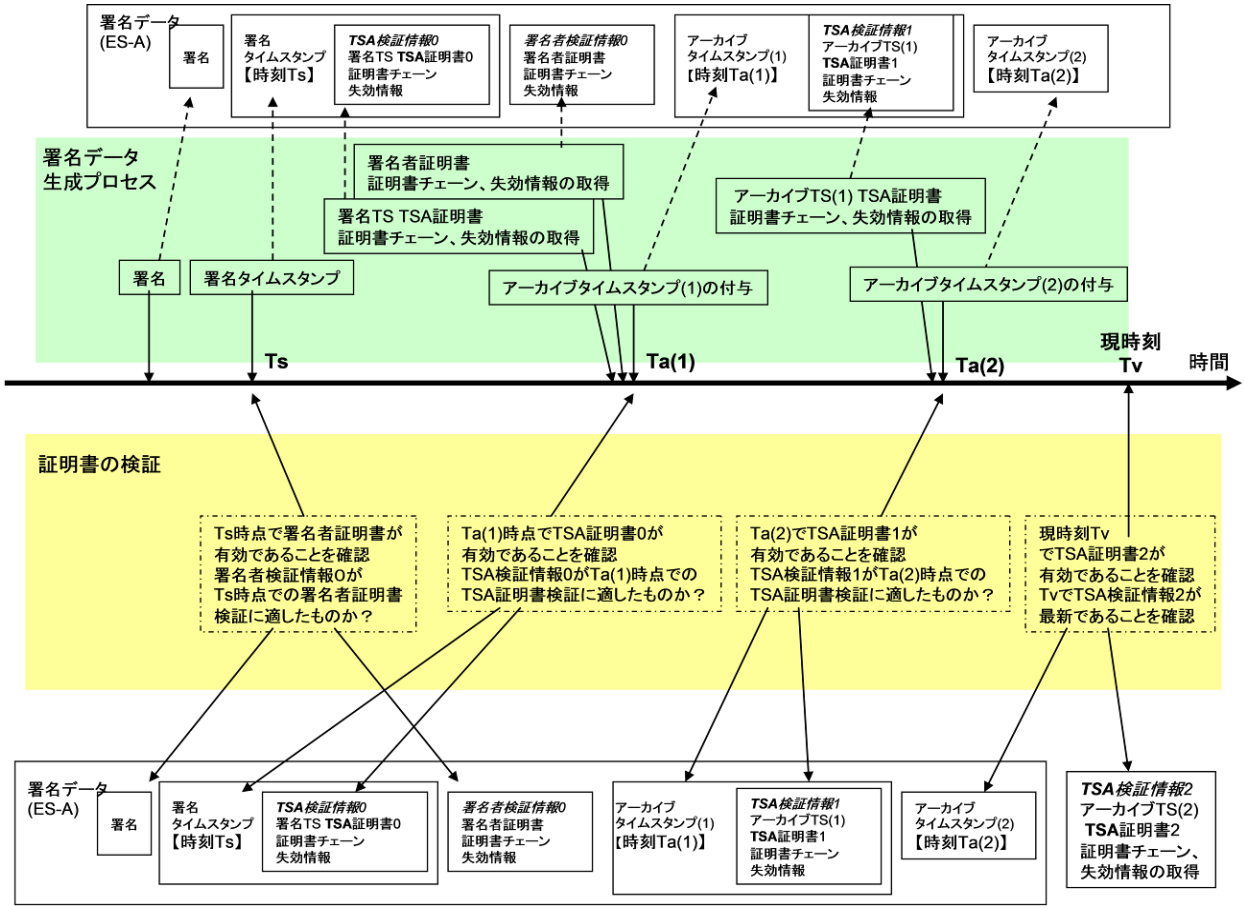

図 6.2.5 ES-A の検証に用いる時刻情報（第二世代アーカイブタイムスタンプの場合）

６.３ CAdES に関する規格

６.３.１ 概要

CAdES の生成及び検証に関する要件を示す。

6.3.2 節にこの規格で定義するプロファイルの概要を、6.3.3 節に CAdES の構造を示す。6.3.4 節に要求レベルの表現法、6.3.5～6.3.6 節にプロファイルの要件を示し、6.3.7 節に各構成要素の概要を示す。

６.３.２ 定義する長期署名プロファイル

電子署名を長期にわたって検証可能にするためには、相互運用性が確保されていることのほかに、署名時刻の特定が可能であることに加え、署名対象及び検証情報を含む署名に関する情報の改ざん検知が可能であることが必要である。この規格では、CAdES に関して、次の二つのプロファイルを定義することによって、この要求を満たす。

(1)　CAdES-T プロファイル

署名タイムスタンプが付与された署名データの生成及び検証に関するプロファイル。

(2)　CAdES-A プロファイル

アーカイブタイムスタンプが付与された署名データの生成及び検証に関するプロファイル。

ここで、CAdES-T データと CAdES-A データの関係を図 6.3.1 に示す。

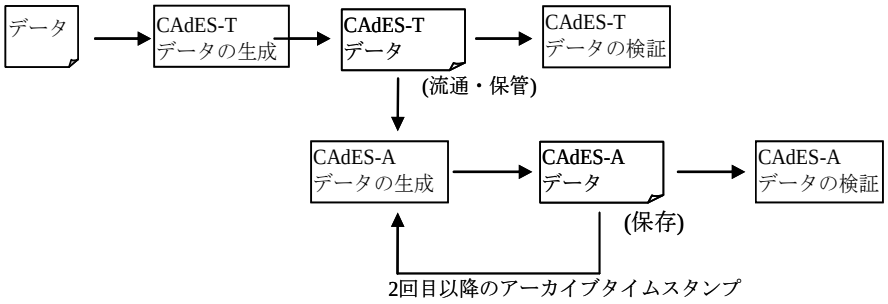

図 6.3.1 CAdES-T データと CAdES-A データの関係

６.３.３ CAdES のデータ構造

CAdES のデータ構造のベースは、署名付きデータである。署名付きデータは、署名対象をカプセル構造化して取り込み、複数の署名者の署名を格納することができる

(図 6.3.2.の破線部分)。図 6.3.3 に、署名付きデータの構造を示す。

注記 署名付きデータは、コンテント情報のテンプレートに従って、コンテント種別が "署名付きデータを表す識別子(id-signedData)" のコンテントとして定義される。

署名者毎の署名情報は、署名者情報として構造化されている（図 6.3.4)。

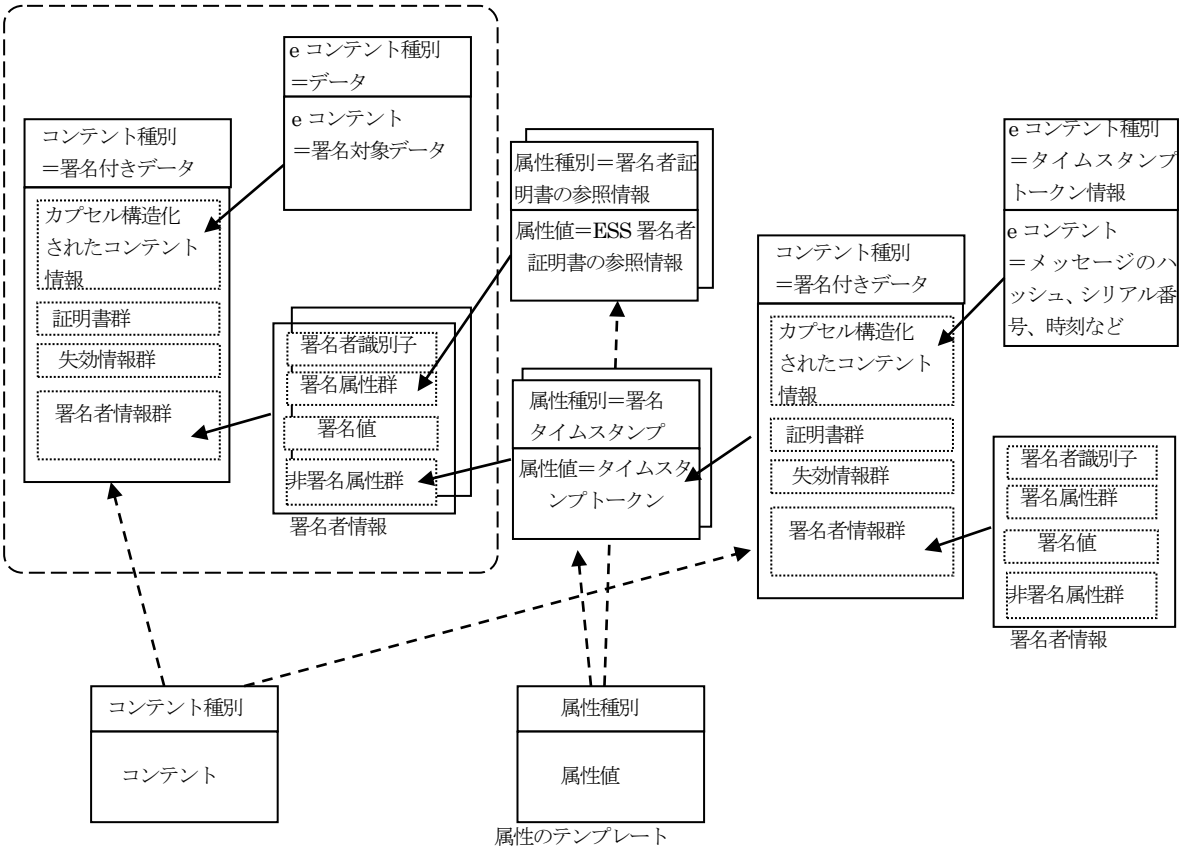

図 6.3.2 CAdES のデータ構造

コンテント種別		
コンテント	暗号メッセージ構文の版数	
	ダイジェストアルゴリズム識別子群	
	カプセル構造化されたコンテント情報	コンテント種別
		コンテント
	証明書群	
	失効情報群	
	署名者情報群	

図 6.3.3 署名付きデータの構造

署名者情報の版数
署名者識別子 （発行者及びシリアル番号　または　対象者鍵識別子）
ダイジェストアルゴリズム識別子
署名属性群
署名アルゴリズム識別子
署名値
非署名属性群

図 6.3.4 署名者情報の構造

６.３.４ 要件レベルの表現法

この規格では、CAdES-T データ及び CAdES-A データを構成する各要素に対する、プロファイルとしての要求レベルとして、次の表現法を定義する。

(1)　必須

この要求レベルを持つ要素は必ず実装しなければならない。この要求レベルの要素が、選択肢となる下位要素を持つ場合は、少なくともその下位要素の一つを選択しなければならない。また、この要求レベルの要素が、任意選択要素の下位要素の一つである場合は、その任意選択要素を選択するときはこの必須要素も選択しなければならない。

(2)　任意選択

この要求レベルを持つ要素の実装は任意とする。

(3)　要別途規定

この要求レベルを持つ要素の実装は任意とするが、基本的に相互運用性の確保を前提としているため、使用しないことを推奨する。ただし、特定のユースケースにおいて利用者の合意に基づき、合意の範囲内で使用することを妨げるものではない。使用する場合はその処理に関して、別途に詳細な仕様を規定しなければならない。

(4)　禁止

この要求レベルを持つ要素は、データ中に含めてはならない。検証時は、その要素を無視してよい。

６.３.５ CAdES-T に関する要件

表 6.3.1 ContentInfo コンテント情報

要素	要求レベル	条件/値
ContentType コンテント種別	必須	SignedData を表す識別子
Content コンテント	必須	SignedData

表 6.3.2 SignedData 署名付きデータ

要素	要求レベル	条件/値
CMSVersion 暗号メッセージ構文の版数	必須	
DigestAlgorithmIdentifiers ダイジェストアルゴリズム識別子群	必須	
EncapsulatedContentInfo カプセル構造化されたコンテント情報	必須	
・・eContentType コンテント種別	必須	
・・eContent コンテント	任意選択	
CertificateSet （Certificates） 証明書群	任意選択	
・・Certificate 証明書	任意選択	
・・AttributeCertificateV2 属性証明書２版	禁止	
・・OtherCertificateFormat その他形式の証明書	禁止	
RevocationInfoChoices （crls） 失効情報の群	任意選択	
・・CertificateList 失効情報	任意選択	
・・OtherRevocationInfoFormat その他形式の失効情報	要別途規定	
SignerInfos 署名者情報群	必須	
・・単一の署名者情報	任意選択	
・・複数の署名者情報	任意選択	

表 6.3.3 SignerInfo 署名者情報

要素	要求レベル	条件/値
CMSVersion 暗号メッセージ構文の版数	必須	署名者識別子が発行者及びシリアル番号なら 1 対象者鍵識別子ならば 3
SignerIdentifier 署名者識別子	必須	
・・IssuerAndSerialNumber 発行者及びシリアル番号	任意選択	
・・SubjectKeyIdentifier 対象者鍵識別子	任意選択	
DigestAlgorithmIdentifier ダイジェストアルゴリズム識別子	必須	
SignedAttributes 署名属性群	必須	
SignatureAlgorithmIdentifier 署名アルゴリズム識別子	必須	
SignatureValue 署名値	必須	
UnsignedAttributes 非署名属性群	必須	

表 6.3.4 及び表 6.3.5 に記載されていない署名属性要素及び非署名属性要素の要求レベルは"要別途規定"とする。

表 6.3.4 SignedAttributes 署名属性

要素	要求レベル	条件/値
ContentType コンテント種別	必須	
MessageDigest メッセージダイジェスト	必須	
SigningCertificateReference 署名者証明書の参照情報	必須	
・・ESSSigningCertificate ESS 署名者証明書の参照情報	任意選択 a)	
・・ESSSigningCertificateV2 ESS 署名者証明書の参照情報 2 版	任意選択 a)	
・・OtherSigningCertificate 他の署名者証明書の参照情報	禁止	
SignatgurePolicyIdentifier 署名ポリシ識別子	禁止	ISO 14533:2021 で禁止となったため、要求レベルを変更
SigningTime 署名時刻	任意選択 b)	
ContentReference コンテント参照情報	要別途規定	
ContentIdentifier コンテント識別子	要別途規定	

ContentHints コンテントのヒント	要別途規定	
CommitmentTypeIndication コミットメント識別表示	要別途規定	
SignerLocation 署名者所在地	要別途規定	
SignerAttribute 署名者の属性情報	要別途規定	
ContentTimestamp コンテントタイムスタンプ	要別途規定	
タイムマークなどその他の方式	要別途規定	
注 a) ESS 署名者証明書の参照情報、ESS 署名者証明書の参照情報 2 版のいずれか一つを選択。 注 b) 未実装の場合は無視。		

表 6.3.5 追加非署名属性

要素	要求レベル	条件/値
CounterSignature カウンタ署名	任意選択	
署名時刻を確定する情報	必須	
・・SignatureTimestamp 署名タイムスタンプ	必須	RFC3161 で定義されるタイムスタンプ3
・・タイムマークなどその他の方式	禁止	

[3] タイムスタンプを取得し CAdES データへ格納する方法、及び、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

６.３.６ CAdES-A に関する要件

CAdES-A プロファイルは、CAdES-T データの拡張として定義される。CAdES-T データの非署名属性群に追加する、CAdES で定義された各要素は、表 6.3.6 に示す要求レベルに従う。この表に定義されていない要素の要求レベルは"要別途規定"である。なお、ArchiveTimestamp のバージョンについては、日本における ArchiveTimestampV2 による継続的な検証を維持するため、要求レベルについては、ArchiveTimestampV2 の利用を前提とした記載としている。ArchiveTimestampV3 を利用する場合は付録 2 を参照の上利用する事。

表 6.3.6 追加非署名属性

要素	要求レベル	条件/値
CounterSignature カウンタ署名	要別途規定 a)	
Trusted time 信頼された時刻	必須	
・・SignatureTimeStamp 署名タイムスタンプ	任意選択	RFC3161 で定義されるタイムスタンプ
・・Time Mark or other method like archive time-stamp as its replacement タイムマークなどその他の方式	任意選択	
CompleteCertificateReferences 完全な証明書参照情報群	必須 a) （検証処理に対しては任意選択）	
CompleteRevocationReferences 完全な失効参照情報群	必須 a) （検証処理に対しては任意選択）	
・・CompleteRevRefs CRL CRL 形式の失効参照情報群	任意選択	
・・CompleteRevRefs OCSP OCSP 形式の失効参照情報群	任意選択	
・・OtherRevRefs 他の形式の失効参照情報群	禁止	
Attribute certificate references 属性証明書の参照情報群	禁止	
Attribute revocation references 属性失効情報の参照情報群	禁止	
CertificateValues 証明書群	必須 a)	
・・CertificateValues 証明書	任意選択	
・・CA 等による証明書の保管	禁止	
RevocationValues 失効情報群	必須 a)	
・・CertificateList CRL による失効情報	任意選択	
・・BasicOCSPResponse 基本 OCSP 応答	任意選択	

・・OtherRevVals 他の失効情報	禁止	
・・CA 等による失効情報の保管	禁止	
CAdES-C-timestamp CAdES-C データへのタイムスタンプ	禁止	
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	禁止	
（改ざん検知を可能とする情報）	必須	
・・ArchiveTimestampV3 アーカイブタイムスタンプ id-aa-ets-archiveTimestampV3	任意選択	
・・ArchiveTimestampV2 アーカイブタイムスタンプ id-aa-48	任意選択	RFC3161 で定義されるタイムスタンプ4
・・ArchiveTimestampV1 アーカイブタイムスタンプ id-aa-27	任意選択	ETSI/TS 101 733 v1.4.0 もしくはそれ以前で定義される。 RFC3161 で定義されるタイムスタンプ 4
・・Evidence Record 証拠記録	任意選択	RFC 4998 で定義される証拠のレコード構文（ERS）
・・タイムマークなどその他の方式	禁止	
注 a）これらのタイプのタイムスタンプを適用した後は、要素を追加してはならない。		

[4] タイムスタンプを取得し CAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

６.３.７ 各構成要素の概要

６.３.７.１ ContentInfo コンテント情報の要素

・ContentType コンテント種別

暗号メッセージの種別。これはオブジェクト識別子であり、この暗号メッセージの種別を定義した機関によって割り当てられた一意に定まる整数列である。

・Content コンテント

暗号メッセージの内容。この内容は、コンテント種別によって一意に定められる。

６.３.７.２ SignedData 署名付きデータの要素

・CMSVersion 暗号メッセージ構文の版数

署名付きデータの構文の版数。

・DigestAlgorithmIdentifiers ダイジェストアルゴリズム識別子群

ダイジェストアルゴリズムの集まり。

・EncapsulatedContentInfo カプセル構造化されたコンテント情報

署名対象文書（データ）及びそれに関する情報。

・eContentType e コンテント種別

署名対象文書（データ）のデータ型を一意に識別するオブジェクト識別子。

・eContent e コンテント

署名対象文書（データ）のデータバイト列を格納する。省略することによって、"外部署名"を構成することが可能になる。

・CertificateSet (certificates) 証明書群

証明書の集まり。認識される"ルート"または"最上位の証明機関"から署名者情報群に含まれるすべての署名者までの連鎖を含むことができる。

(1) 証明書
(2) 属性証明書 2 版
(3) その他形式の証明書

この規格では、(1) 証明書のみを対象とする。

・RevocationInfoChoices (crls) 失効情報群

証明書失効リスト(CRL)の集まり。証明書群に含まれる証明書が有効か否かを決定するための情報を含むことができる。

(1) 失効情報
(2) その他形式の失効情報

・SignerInfos 署名者情報群

署名者情報の集まり。0 個も含めて、どのような数の署名者情報も含むことがある。

６.３.７.３ SignerInfo 署名者情報の要素

・CMSVersion 暗号メッセージ構文の版数

署名者情報の構文の版数である。署名者識別子が発行者及びシリアル番号ならば、値は 1 でなければならない。対象者鍵識別子ならば、値は 3 でなければならない。

・SignerIdentifier 署名者識別子

署名者の証明書を特定する（それによって署名者の公開鍵も特定する。）。署名者の公開鍵は、受信者が署名を検証するのに必要である。署名者の公開鍵を特定するための二つの選択肢を提供する。

・IssuerAndSerialNumber 発行者及びシリアル番号

署名者の証明書を、発行者の識別名及び証明書のシリアル番号によって識別する。

・SubjectKeyIdentifier 対象者鍵識別子

署名者の証明書を X.509 の対象者鍵識別子の拡張値によって識別する。

・DigestAlgorithmIdentifier ダイジェストアルゴリズム識別子
署名者に使われたメッセージダイジェストのアルゴリズム及び関連するパラメータを識別する。メッセージダイジェストのアルゴリズムは、関連する署名付きデータのダイジェストアルゴリズム識別子群領域に挙げられているものでなければならない。
・SignedAttributes 署名属性群
署名される属性の集まり。任意選択であるが、存在する場合はDER 符号化と、少なくともコンテント種別とメッセージダイジェストの二つの属性を含まなければならない。
・SignatureAlgorithmIdentifier 署名アルゴリズム識別子
署名者に使われたメッセージダイジェストのアルゴリズム及び関連するパラメータを識別する。
・SignatureValue 署名値
署名の値。
・UnsignedAttributes 非署名属性群
署名対象とはならない属性の集まり。

6.3.7.4 Signed Attribute 署名属性として定義される要素
・ContentType コンテント種別
署名対象データのデータ型のオブジェクト識別子を保持する。署名属性が存在する場合には必ず含めなければならない。
・MessageDigest メッセージダイジェスト
署名対象データのハッシュ値を保持する。署名属性が存在する場合には必ず含めなければならない。
・SigningCertificateReference 署名者証明書の参照情報
署名者証明書を特定する情報（署名者証明書のハッシュ値）を保持する。
注記：本属性は署名者証明書を特定するという目的においては対象者鍵識別子と同じであるが、対象者鍵識別子は署名保護されるフィールドではないため、改ざんされてもその事実を署名検証時に検知することができないという脆弱性を補うことができる。
(1) ESS 署名者証明書の参照情報
(2) ESS 署名者証明書の参照情報 2 版
(3) ESS 署名他の署名者証明書の参照情報
・SignaturePolicyIdentifier 署名ポリシ識別子
署名ポリシを特定するための情報を保持する。署名ポリシは、署名者と署名の検証者が守るべき一連の規則。
・SigningTime 署名時刻
署名がなされた時刻を保持する。時刻の正確さは要求されない。
・ContentReference コンテント参照情報
他の署名文書へのリンクを保持する。
・ConentIdentifier コンテント識別子
署名対象文書のハッシュ値など、コンテントを一意に特定する情報を保持する。
・ContentHint コンテントのヒント
署名対象文書のデータフォーマットに関する補足情報を保持する。
・CommitmentTypeIdication コミットメント識別表示
署名者がどのような意図を持って署名したかを表明する情報を保持する。
・SignerLocation 署名者所在地
署名者の署名時における居所情報を格納する属性である。第三者によってその確かさが保証されたものではなく、署名者が署名時にその場所にいたと主張しているものである。
・SignerAttribute 署名者の属性情報
任意の署名者属性情報を保持する。署名者属性情報には大きく分けて、署名者が自分でそうだと主張している属性情報と、署名者がそうであると第三者が保証している属性情報の２種類があり、本属性にはその

どちらの属性情報も格納することができる。
・ContentTimestamp コンテントタイムスタンプ
署名対象文書に対するタイムスタンプ。署名時点より前に取っておいた署名対象文書の存在証明（つまりタイムスタンプ）を署名データに含めたい場合に利用する。
・タイムマークなどその他の方式
データが特定の時刻以前に存在したことを示すための、データと特定の時間を結びつける信頼される第三者機関からの監査証跡内の情報。

6.3.7.5 Unsigned Attribute 非署名属性として定義される要素
・CounterSignature カウンタ署名
署名値に対する署名。複数人が同一文書に署名する際、署名の順序に意味がある、もしくは意味を持たせたい場合に用いる。
・署名時刻を確定する情報
署名が存在した時刻を特定可能にするために、署名値に付されるタイムスタンプなどの情報。
(1) 署名タイムスタンプ
(2) タイムマークなどその他の方式
注記 タイムマークは、データが特定の時刻以前に存在したことを示すための、データと特定の時間を結びつける信頼される第三者機関からの監査証跡内の情報など。
・CompleteCertificateReferences 完全な証明書参照情報群
署名検証に必要な、署名者証明書から信頼点の証明書までの認証パス上のすべての証明書の参照情報（ただし署名者の証明書への参照情報は含まない）。1 署名につき一つだけ存在する。
・CompleteRevocationReferences 完全な失効参照情報群
署名検証に必要な、署名者から信頼点までの証明書に対する CRL あるいは OCSP 応答のすべての参照情報。1 署名に対して一つだけ存在する。
(1) CRL 形式の失効参照情報群
(2) OCSP 形式の失効参照情報群
(3) 他の形式の失効参照情報群
・AttributeCertificateReferences 属性証明書の参照情報群
関連する属性証明書の参照情報を保持する。
・AttributeRevocationReferences 属性失効情報の参照情報群
関連する属性証明書の失効情報（ACRL または OCSP レスポンス)の参照情報を保持する。
・CertificateValues 証明書群
完全な証明書参照情報群が参照する証明書及び署名者の証明書を保持する。1 署名につき一つだけ存在する。
(1) 証明書
(2) CA 等による証明書の保管
・RevocationValues 失効情報群
完全な失効参照情報群で参照される CRL と OCSP 応答の値を保持する。1 署名につき一つだけ存在する。
(1) CRL による失効情報
(2) 基本 OCSP 応答
(3) 他の失効情報
(4) CA 等による失効情報の保管
・CAdES-C timestamp CAdES-C データへのタイムスタンプ
認証経路を構成する全証明書参照情報付き署名(CAdES-C)全体に対するタイムスタンプ。1 署名につき複数存在可能。
・Timestamped cert and crls refernce 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

検証情報へのリファレンス（完全な証明書参照情報群及び完全な失効参照情報群）に対するタイムスタンプ。

・改ざん検知を可能とする情報

・ArchiveTimestamp アーカイブタイムスタンプ

改ざん検知を可能にするために、署名対象及び検証情報を含む署名に関する情報に付されるタイムスタンプ。

注記　id-aa-ets-archiveTimestampV3、id-aa-48 及び id-aa-27 はそれぞれ、ETSI/EN 319 122–1 v1.1.1、ETSI TS 101 733 V1.7.3 及び ETSI TS 101 733 V1.2.2 で定義されている。

・Evidence Record 証拠記録

RFC 4998 で定義される証拠のレコード構文（ERS）

・タイムマークなどその他の方式

データが特定の時刻以前に存在したことを示すための、データと特定の時間を結びつける信頼される第三者機関からの監査証跡内の情報など。

６.４ XAdES に関する規格

６.４.１ 概要

XAdES の生成及び検証に関する要件を示す。

6.4.2 節にこの規格で定義するプロファイルの概要を、6.4.3 節に XAdES の構造を示す。6.4.4 節に要求レベルの表現法、6.4.5～6.4.7 節にプロファイルの要件を示し、6.4.8 節に各構成要素の概要を示す。

６.４.２ 定義する長期署名プロファイル

電子署名を長期にわたって検証可能にするためには、相互運用性が確保されていることのほかに、署名時刻の特定が可能であることに加え、署名対象及び検証情報を含む署名に関する情報の改ざん検知が可能であることが必要である。この規格では、XAdES に関して、次の三つのプロファイルを定義することによって、これらの要求を満たす。

(1)　XAdES-T プロファイル

XAdES-T データの生成及び検証に関するプロファイル。

(2)　XAdES-XL プロファイル

XAdES-XL データの生成及び検証に関するプロファイル。

(3)　XAdES-A プロファイル

XAdES-A データの生成及び検証に関するプロファイル。

ここで、XAdES-T データ、XAdES-XL データ、及び XAdES-A データの関係を図 6.4.1 に示す。

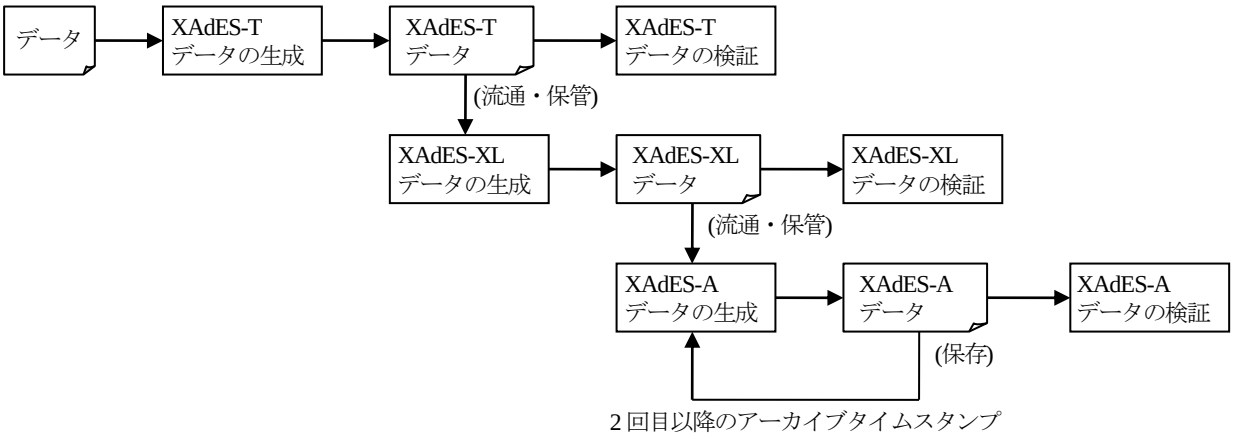

図 6.4.1 XAdES-T データ、XAdES-XL データ、及び XAdES-A データとの関係

６.４.３ XAdES データの構造

XAdES データの構造は、XML 署名の拡張形として定義される。図 6.4.2 に XAdES の構造の一例を示す。

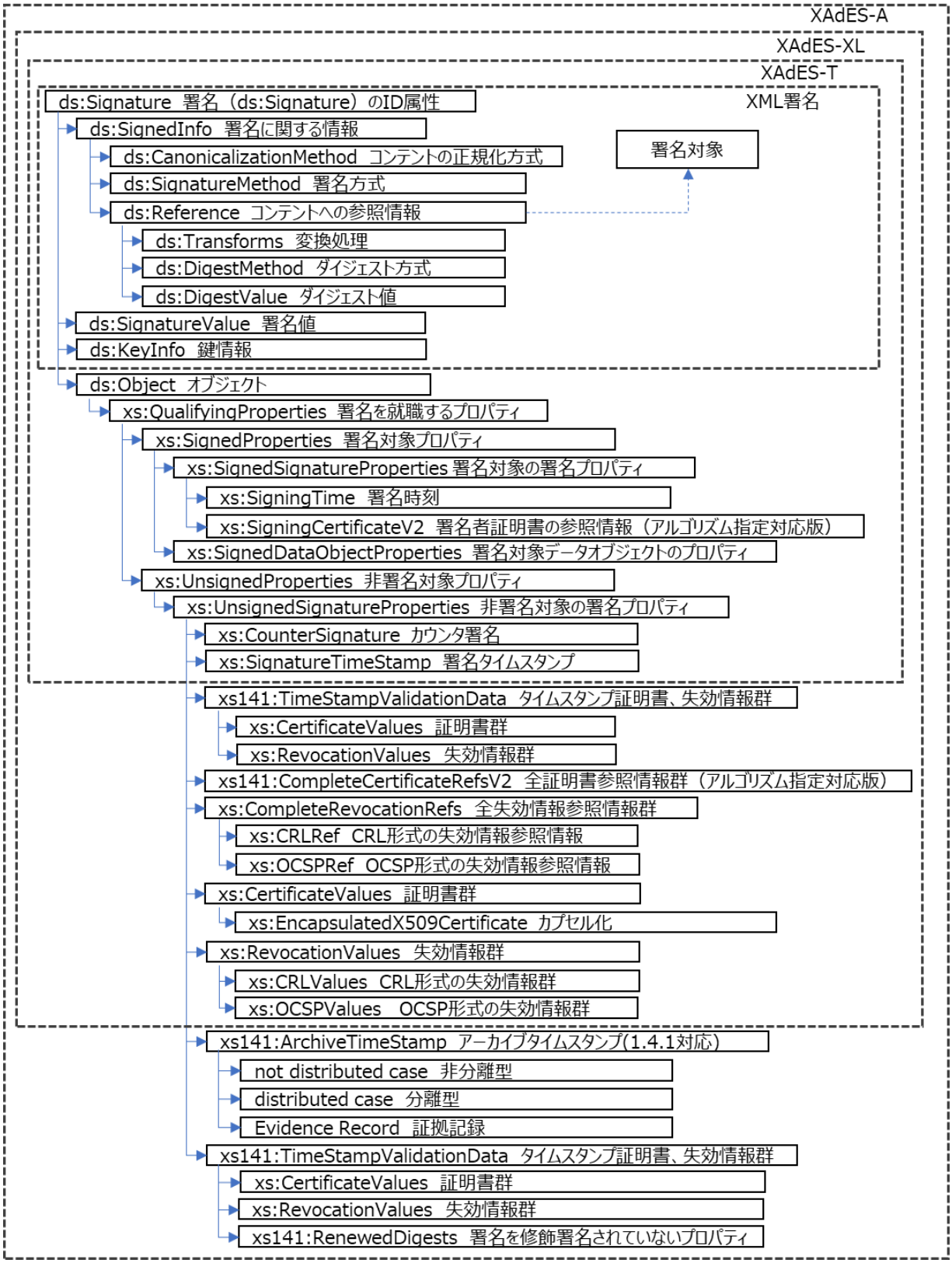

図 6.4.2 XAdES 構造の一例

６.４.４ 要求レベルの表現法

この規格では、XAdES-T データ、XAdES-XL データ及び XAdES-A データを構成する各要素に対する、プロファイルとしての要求レベルとして、次の表現法を定義する。

(1)　必須

この要求レベルを持つ要素は必ず実装しなければならない。この要求レベルの要素が、選択肢となる下位要素を持つ場合は、少なくともその下位要素の一つを選択しなければならない。また、この要求レベルの要素が、任意選択要素の下位要素の一つである場合は、その任意選択要素を選択するときはこの必須要素も選択しなければならない。

(2)　任意選択

この要求レベルを持つ要素の実装は任意とする。

(3)　要別途規定

この要求レベルを持つ要素の実装は任意とするが、基本的に相互運用性の確保を前提としているため、使用しないことを推奨する。ただし、特定のユースケースにおいて利用者の合意に基づき、合意の範囲内で使用することを妨げるものではない。使用する場合はその処理に関して、別途に詳細な仕様を規定しなければならない。

(4)　禁止

この要求レベルを持つ要素は、データ中に含めてはならない。検証時は、その要素を無視してよい。

６.４.５ XAdES-T に関する要件

表 6.4.1～表 6.4.3 に記載されていない要素の要求レベルは、要別途規定である。

表 6.4.1 Signature 要素

要素/属性	要求レベル	条件/値
署名（ds:Signature）の ID 属性	必須 a)	
ds:SignedInfo 署名に関する情報	必須	
・・ds:CanonicalizationMethod コンテントの正規化方式	必須	EXC-c14n（コメントなし版）又は C14n11
・・ds:SignatureMethod 署名方式	必須	
・・ds:Reference コンテントへの参照情報	必須	
・・・・ds:Transforms 変換処理	任意選択	
・・・・ds:DigestMethod ダイジェスト方式	必須	
・・・・ds:DigestValue ダイジェスト値	必須	
ds:SignatureValue 署名値	必須	
ds:KeyInfo 鍵情報	任意選択 b)	
ds:Object オブジェクト	必須	
注 a) XML 署名では“任意選択”であるが、ETSI EN 319 132 では“必須”である。 注 b) 鍵情報(ds:KeyInfo)か、または署名者証明書の参照情報（xs:SigningCertificateV2）（表 6.4.2）のいずれか一方が必要である。鍵情報を選択する場合（ETSI TS 101 903 v1.1.1 の場合は必須）は、下記の条件を満たす必要がある。 ・ds:KeyInfo 要素の下位要素に XML 署名で定義された署名証明書を含む ds：X509Data を含まなければならない。 なお、SigningCertificateV2 を併用しない場合は、X509Data は署名証明書のみとしなければならない。 ・ds：SignedInfo 要素には、ds：KeyInfo を参照する ds：Reference 要素を含まなければならない。		

表 6.4.2 Object 要素、SignedSignatureProperties 要素

要素	要求レベル	条件/値
xs:QualifyingProperties 署名を修飾するプロパティ	必須	対象属性に、署名要素の ID 属性の値を入れる
・・xs:SignedProperties 署名対象プロパティ	必須	
・・・・xs:SignedSignatureProperties 署名対象の署名プロパティ	必須	
・・・・・・xs:SigningTime 署名時刻	任意選択 a)	
・・・・・・xs: SigningCertificateV2 署名者証明書の参照情報（アルゴリズム指定対応版）	任意選択 a) b)	

・・・・・・xs: SigningCertificate 署名者証明書の参照情報	要別途規定 a) c)	
・・・・・・xs: SignaturePolicyIdentifier 署名ポリシ識別子	要別途規定	
・・・・・・xs: SignatureProductionPlaceV2 署名生成場所（アルゴリズム指定対応版）	要別途規定	
・・・・・・xs: SignatureProductionPlace 署名生成場所	要別途規定 d)	
・・・・・・xs: SignerRoleV2 署名者の肩書き（アルゴリズム指定対応版）	要別途規定	
・・・・・・xs: SignerRole 署名者の肩書き	要別途規定 d)	
・・・・xs: SignedDataObjectProperties 署名対象データオブジェクトのプロパティ	要別途規定	
・・・・・・xs: DataObjectFormat データオブジェクト形式	要別途規定 a)	
・・・・・・・・xs: Description データオブジェクト形式の説明	要別途規定	
・・・・・・・・xs: ObjectIdentifier データオブジェクト形式のオブジェクト識別子	要別途規定	
・・・・・・・・xs: MimeType データオブジェクト形式の MIME タイプ	要別途規定 a)	
・・・・・・・・xs: Encoding データオブジェクト形式のエンコーディング形式	要別途規定	
・・・・・・xs: CommitmentTypeIndication コミットメント種別表示	要別途規定	
・・・・・・xs: AllDataObjectsTimeStamp 全データオブジェクトに対するタイムスタンプ	要別途規定	
・・・・・・xs: IndividualDataObjectsTimeStamp 個別データオブジェクトに対するタイムスタンプ	要別途規定	
注 a) ETSI EN 319 132-1 v1.1.1 Baseline Signature.の場合は“必須”である。 注 b) 署名者証明書の参照情報(xs:SigningCerticicateV2)か、または鍵情報(ds:KeyInfo)(表 6.4.1)のどちらか一方が必要です。 注 c) 署名者証明書の参照情報(xs:SigningCertificate)か、または鍵情報(ds:KeyInfo)(表 6.4.1) のどちらか一方が必要である。 注 d) 過去の互換性と ETSI TS 101 903 v1.1.1 へ参照のため。		

表 6.4.3 Object 要素、UnsignedSignatureProperties 要素

要素	要求レベル	条件/値
xs: QualifyingProperties 署名を修飾するプロパティ	必須	
・・xs: UnsignedProperties 非署名対象プロパティ	必須	
・・・・xs:UnsignedSignatureProperties 非署名対象の署名プロパティ	必須	
・・・・・・xs:CounterSignature カウンタ署名	任意選択	

・・・・・・(署名時刻を確定する情報)	必須	
・・・・・・xs:SignatureTimeStamp 署名タイムスタンプ	必須	ETSI EN 319 132-1 v1.1.1 Baseline Signature の場合は“必須”である。 RFC3161 で定義されるタイムスタンプ5
・・・・・・other POE method その他の存在証明方法	禁止	
・・xs: UnsignedDataObjectProperties 非署名のデータオブジェクトのプロパティ	要別途規定	

5 タイムスタンプを取得し XAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

６．４．６ XAdES-XL に関する要件

表 6.4.4 に記載されていない要素の要求レベルは、要別途規定である。

表 6.4.4 UnsignedSignatureProperties 要素

要素	要求レベル	条件/値
xs141: TimeStampValidationData タイムスタンプ証明書、失効情報群	要別途規定	
・・xs: CertificateValues 証明書群	要別途規定	
・・xs: RevocationValues 失効情報群	要別途規定	
xs141: CompleteCertificateRefsV2 全証明書参照情報群（アルゴリズム指定対応版）	任意選択	
xs: CompleteCertificateRefs 全証明書参照情報群	要別途規定 a)	
xs: CompleteRevocationRefs 全失効情報参照情報群	要別途規定 a)	
・・xs: CRLRef CRL 形式の失効情報参照情報	任意選択	
・・xs: OCSPRef OCSP 形式の失効情報参照情報	任意選択	
・・xs: OtherRef 他の失効情報参照情報	禁止	
xs141: AttributeCetrificateRefsV2 属性証明書参照情報群（アルゴリズム指定対応版）	禁止	
xs: AttributeCetrificateRefs 属性証明書参照情報群	禁止	
xs: AttributeRevocationRefs 属性失効情報参照情報群	禁止	
xs141:SigAndRefsTimeStampV2 署名及び参照情報に対するタイムスタンプ（アルゴリズム指定対応版）	禁止	
・・not distributed case （非分離型）	禁止	
・・distributed case （分離型）	禁止	
xs: SigAndRefsTimeStamp 署名及び参照情報に対するタイムスタンプ	禁止	
xs141: RefsOnlyTimeStampV2 参照情報に対するタイムスタンプ（アルゴリズム指定対応版）	禁止	
・・not distributed case （非分離型）	禁止	
・・distributed case （分離型）	禁止	
xs: RefsOnlyTimeStamp 参照情報に対するタイムスタンプ	禁止	

xs: CertificateValues 証明書群	必須	
・・xs: EncapsulatedX509Certificate カプセル構造化された証明書	任意選択	
・・xs: OtherCertificate 他の証明書	禁止	
・・(CA 等による証明書の保管)	禁止	
xs: RevocationValues 失効情報群	必須	
・・xs: CRLValues CRL による失効情報群	任意選択	
・・xs: OCSPValues OCSP による失効情報群	任意選択	
・・xs: OtherValues 他の失効情報群	禁止	
・・(CA 等による失効情報の保管)	禁止	
xs: AttrAuthoritiesCertValues 属性証明書群	禁止	
xs: AttributeRevocationValues 属性失効情報群	禁止	
Any unsigned signature property defined in any other version of XAdES 異なる版の署名対象外署名プロパティ要素	要別途規定	
注 a) 過去の互換性と ETSI TS 101 903 v1.1.1 へ参照のため。ただし、これらの要素は廃止されており、新しい署名を作成するために使用することはできず、検証のためにのみ使用します。		

6.4.7 XAdES-A に関する要件

XAdES-A プロファイルは、XAdES-T データの拡張として定義される。XAdES で定義された非署名対象の署名プロパティ要素の各要素は、表 6.4.5 に示す要求レベルに従う。この表に定義されていない要素の要求レベルは"要別途規定"である。

表 6.4.5 UnsignedSignatureProperties 要素

要素	要求レベル	条件/値
Archiving (改ざん検知を可能とする情報)	必須	
・・xs141:ArchiveTimeStamp アーカイブタイムスタンプ(1.4.1 対応)	必須	
・・not distributed case (非分離型)	必須	RFC3161 で定義されるタイムスタンプ
・・distributed case (分離型)	禁止	
・・・・Evidence Record 証拠記録	禁止	RFC 6283 で定義される XMLERS
・・xs:ArchiveTimeStamp アーカイブタイムスタンプ(以前のバージョン用)	要別途規定 a)	
・・Other method 「ArchiveTimeStamp」に代わる他の方法	禁止	

・・xs141: TimeStampValidationData タイムスタンプ証明書、失効情報群	必須 b)	
・・・・xs: CertificateValues 証明書群	任意選択	
・・・・xs: RevocationValues 失効情報群	任意選択	
・・xs141:RenewedDigests 署名を修飾する署名されていないプロパティ	要別途規定 c)	
Any unsigned signature property defined in any other version of XAdES 異なる版の署名対象外署名プロパティ要素	要別途規定	
注 a) 過去の互換性と ETSI TS 101 903 v1.1.1 へ参照のため。ただし、これらの要素は廃止されており、新しい署名を作成するために使用することはできず、検証のためにのみ使用します。 注 b) 過去のタイムスタンプの検証には、トラストアンカまでの証明書と失効情報が必要である。 タイムスタンプ検証データには、TSA（タイムスタンプ権限）証明書からトラストアンカ証明書への証明書パス内の証明書と、そのような各証明書に関連する失効情報が必要である。タイムスタンプトークンの構造は、ISO 14533-2 付録 B に従うものとする。 注 c) マニフェスト要素のため		

６.４.８ 各構成要素の概要

６.４.８.１ 署名要素及び属性

・ID 属性

署名要素における ID 属性。長期署名では必須。

・署名に関する情報

署名値を計算する際の入力となる署名対象情報。

・コンテントの正規化方式

同じ意味を持つ XML 文書がビット単位で同じ表現の文書になるようにする変換処理の方式。

・署名方式

署名を生成または検証するときの署名アルゴリズム。

・コンテントへの参照情報

署名対象となる要素またはデータの参照先、及びそのダイジェスト値などを格納する。署名要素が署名対象と独立した形式（detached）、署名要素が署名対象の子要素となる形式（enveloped）、及び署名要素が署名対象の親要素となる形式（enveloping）がある。

注記 署名要素が対象の子要素となる形式の場合は、署名対象のデータ構造に署名要素のデータ構造を組み込む必要がある。

・変換処理

正規化などの変換処理。並べられた順番の通りに変換処理が行われる。

・ダイジェスト方式

署名対象のダイジェストの方式。

・ダイジェスト値

ダイジェストの値。この値は Base64 形式でエンコードされたものが使用される。

・署名値

署名の値。

・鍵情報

署名検証に使用される鍵情報。署名鍵の名前、署名鍵の値、文書外などにある鍵情報の取得方式、X.509 証明書などの、いずれかを格納する。

・オブジェクト

任意のデータを含むことができる要素。XML 署名中に複数存在することもある。

６.４.８.２ オブジェクト要素、署名対象プロパティ要素

・署名を修飾するプロパティ

署名に必要な追加のプロパティ。

・署名対象プロパティ

署名対象となるプロパティ。署名に関するプロパティと署名以外のプロパティとから成る。署名値の計算対象となるよう、コンテントへの参照情報(6.4.8.1)で参照される。

・署名対象の署名プロパティ

署名対象となる署名に関するプロパティ。

・署名時刻

署名者が主張する署名時刻。

・アルゴリズム指定対応した署名者証明書の参照情報

署名者の証明書（アルゴリズム指定対応版）。

・署名者証明書の参照情報

署名者の証明書。

・署名ポリシ識別子

署名ポリシを特定するための情報。

・署名生成場所（アルゴリズム指定対応版）
アルゴリズム指定対応した署名が生成された場所。第三者によって保証されたものではなく署名者が主張している場所。
・署名生成場所
署名が生成された場所。第三者によって保証されたものではなく署名者が主張している場所。
・署名者の肩書き（アルゴリズム指定対応版）
アルゴリズム指定対応した署名者が主張する署名者の肩書き、または属性証明書で保証された肩書き。
・署名者の肩書き
署名者が主張する署名者の肩書き、または属性証明書で保証された肩書き。
・署名対象データオブジェクトのプロパティ
署名対象のうちの、データオブジェクト（文書）に関連するプロパティ。
・データオブジェクト形式データオブジェクト形式のヒント。以下の要素の少なくとも１つが含まれている必要がある。
a)データオブジェクト形式の説明
署名されたデータオブジェクトに関連するテキスト情報
b)データオブジェクト形式のオブジェクト識別子
署名されたデータオブジェクトのタイプの識別子
c)データオブジェクト形式の MIME タイプ
署名されたデータオブジェクトの形式を示す MIME タイプ値(RFC2045 で定義)
d)データオブジェクト形式のエンコーディング形式
署名されたデータ オブジェクトのエンコーディングの指示
・コミットメント種別表示
署名者がどのような意図を持って署名したかを表明する情報。
・全データオブジェクトに対するタイムスタンプ
署名生成前の署名対象に対するタイムスタンプ。
・個別データオブジェクトに対するタイムスタンプ
署名生成前の特定の署名対象に対するタイムスタンプ。

6.4.8.3 オブジェクト要素、非署名対象プロパティ要素
・署名を修飾するプロパティ
署名に必要な追加のプロパティ。
・非署名対象プロパティ
署名対象とはならないプロパティ。
・非署名対象の署名プロパティ
署名対象外の署名に関するプロパティ。
・カウンタ署名
署名値に対する署名。複数人が同一文書に署名するとき、署名の順序に意味がある場合、または意味を持たせたい場合に用いる。
・署名時刻を確定する情報
署名が存在した時刻を特定可能にするために、署名値に付されるタイムスタンプなどの情報。
(1)　署名タイムスタンプ
(2)　その他の存在証明方法
注記　データが特定の時刻以前に存在したことを示すための、データと特定の時間を結びつける信頼される第三者機関からの監査証跡内の情報など。
・非署名のデータオブジェクトのプロパティ
データオブジェクト（文書）に関連する署名対象とはならないプロパティ。

6.4.8.4 XAdES-XL に関する非署名対象の署名プロパティ要素

・タイムスタンプ証明書、失効情報群

タイムスタンプに関する検証情報を格納。

a)証明書群

b)失効情報群

・全証明書参照情報群（アルゴリズム指定対応版）

アルゴリズム指定対応した署名者を除く証明書チェーンを構成するすべての証明書参照情報のかたまり。

・全証明書参照情報群

署名者を除く証明書チェーンを構成するすべての証明書参照情報のかたまり。

・全失効情報参照情報群

署名者証明書の証明書チェーンの検証に必要なすべての失効情報参照情報のかたまり。

a)CRL 形式の失効情報参照情報

b)OCSP 形式の失効情報参照情報

c)他の失効情報参照情報

・属性証明書参照情報群（アルゴリズム指定対応版）

アルゴリズム指定対応した関連する属性証明書に関する参照情報のかたまり。

・属性証明書参照情報群

関連する属性証明書に関する参照情報のかたまり。

・属性失効情報参照情報群

関連する属性証明書の失効情報に関する参照情報のかたまり。

・署名及び参照情報に対するタイムスタンプ（アルゴリズム指定対応版）

アルゴリズム指定対応した署名及び参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。

・署名及び参照情報に対するタイムスタンプ

署名及び参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。

・参照情報に対するタイムスタンプ（アルゴリズム指定対応版）

アルゴリズム指定対応した参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。

・参照情報に対するタイムスタンプ

参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。

・証明書群

署名者証明書の証明書チェーンを構成するすべての証明書のかたまり。

(1) カプセル構造化された証明書

(2) 他の証明書

(3) CA 等による証明書の保管

・失効情報群

署名者証明書の証明書チェーン検証に必要なすべての失効情報のかたまり。

(1) CRL による失効情報群

(2) OCSP による失効情報群

(3) 他の失効情報群

(4) CA 等による失効情報の保管

・属性証明書群

関連する属性証明書のかたまり。

・属性失効情報群

関連する属性証明書に対する失効情報のかたまり。

・異なる版の非署名対象の署名プロパティ要素

異なる版の XAdES で定義された署名対象とはならない署名プロパティ。

６．４．８．５ XAdES-A に関する非署名対象の署名プロパティ要素

・改ざん検知を可能とする情報

改ざん検知を可能にするために、署名対象及び検証情報を含む署名に関する情報に付されるタイムスタンプなどの情報。

(1) アーカイブタイムスタンプ(1.4.1 対応) 非分離型と分離型、証拠記録(RFC 6283 で定義される XMLERS)が定義されている。

(2) アーカイブタイムスタンプ（以前のバージョン用）

(3) 「ArchiveTimeStamp」に代わる他の方法

(4) タイムスタンプ証明書、失効情報群

a)証明書群

b)失効情報群

・署名を修飾する署名されていないプロパティ

マニフェスト要素のための署名を修飾する未署名の修飾プロパティ

・異なる版の署名対象外署名プロパティ要素

異なる版の XAdES で定義された署名対象とはならない署名プロパティ。

６.５ PAdES に関する規格

６.５.１ 概要

PAdES の生成及び検証に関する要件を示す。

6.5.2 節にこの規格で定義するプロファイルの概要を示す。6.5.3 節に要求レベルの表現法、6.5.4～6.5.7 節にプロファイルの要件を示す。

６.５.２ 定義する長期署名プロファイル

電子署名を長期にわたって検証可能にするためには、相互運用性が確保されていることのほかに、署名時刻の特定が可能であることに加え、署名対象及び検証情報を含む署名に関する情報の改ざん検知が可能であることが必要である。この規格では、PAdES に関して、次の二つのプロファイルを定義することによって、この要求を満たす。

(1)　ES-T(PAdES-T)プロファイル

署名タイムスタンプが付与された署名データの生成及び検証に関するプロファイル。

(2)　ES-A(PAdES-A プロファイル)

アーカイブタイムスタンプが付与された署名データの生成及び検証に関するプロファイル。

ここで、PAdES-T データと PAdES-A データとの関係を図 6.5.1 に示す。

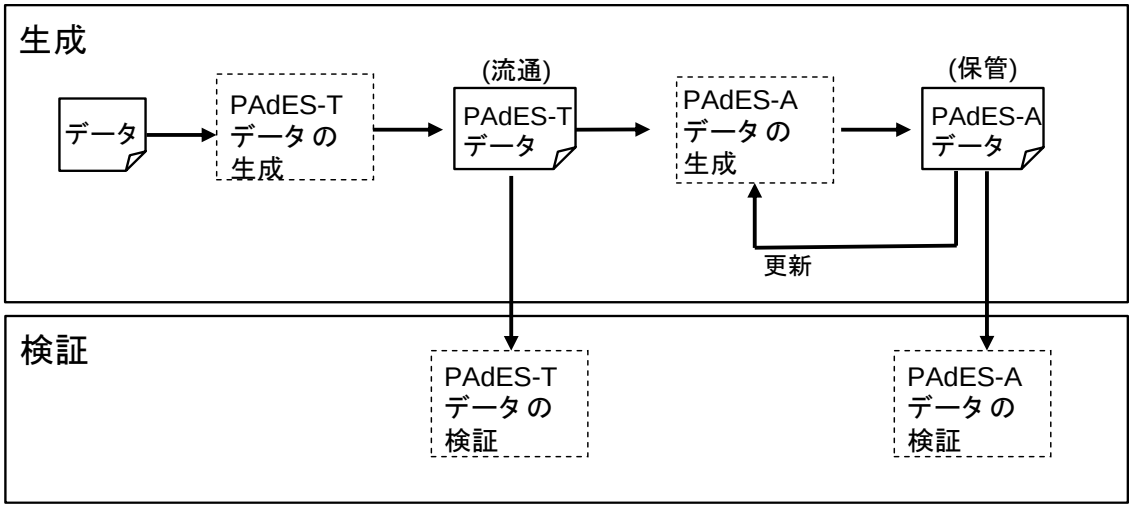

図 6.5.1 PAdES-T データと PAdES-A データとの関係

６.５.３ 要求レベルの表現法

この規格では、プロファイルとしての要求レベルとして、次の表現法を定義する。

(1)　必須

この要求レベルを持つ要素は必ず実装しなければならない。この要求レベルの要素が、選択肢となる下位要素を持つ場合は、少なくともその下位要素の一つを選択しなければならない。また、この要求レベルの要素が、任意選択要素の下位要素の一つである場合は、その任意選択要素を選択するときはこの必須要素も選択しなければならない。

(2)　任意選択

この要求レベルを持つ要素の実装は任意とする。

(3)　要別途規定

この要求レベルを持つ要素の実装は任意とするが、基本的に相互運用性の確保を前提としているため、使用しないことを推奨する。ただし、特定のユースケースにおいて利用者の合意に基づき、合意の範囲内で使用することを妨げるものではない。使用する場合はその処理に関して、別途に詳細な仕様を規定しなければならない。

(4)　禁止

この要求レベルを持つ要素は、データ中に含めてはならない。検証時は、その要素を無視してよい。

６.５.４ PAdES-T プロファイルに関する要件

PAdES-T は署名値がそれ以降に続くタイムスタンプによって保護され、署名値の存在証明が可能となるフォーマットである。PAdES の電子署名では PDF 内の領域（署名辞書）に電子署名データが格納される。PAdES-T プロファイルは電子署名データの非署名属性の領域に署名タイムスタンプ属性(SignatureTimestamp)が格納されたものである。なお、電子署名データの形式は CAdES 形式とする。PAdES-T プロファイルの PDF データ構造のイメージ図を図 6.5.2 に示す。

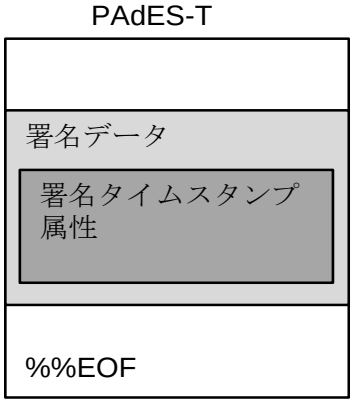

図 6.5.2 PAdES-T プロファイルの PDF データ構造のイメージ

PDF 内に電子署名を格納するための署名辞書に関する要件を表 6.5.1 に示す。

表 6.5.1 PAdES-T プロファイルの署名辞書

要素	要求レベル	条件/値
Type	任意選択	Sig
Filter	必須	
SubFilter	必須	ETSI.CAdES.detached
Contents	必須	表 6.5.2 を参照
ByteRange	必須	
M	必須 a)	
Cert	禁止	
Location	任意選択	
Reason	任意選択	
ContactInfo	任意選択	
注 a) 実装の相互運用性のために必須とする。ただし、M の要素がない署名データであったとしても、それを理由として検証失敗としてはならない。また、M の時刻を証明書検証における基準時刻として用いてはならない。		

署名辞書に格納される CAdES 電子署名の要件を表 6.5.2 から表 6.5.5 に示す。

表 6.5.2 署名辞書の Contents に入る ContentInfo

要素	要求レベル	条件/値
ContentType	必須	id-signedData
Content	必須	表 6.5.3 を参照

表 6.5.3 Content に格納する SignedData 署名付きデータ

要素	要求レベル
CMSVersion	必須
DigestAlgorithmIdentifiers	必須
EncapsulatedContentInfo	必須
- eContentType	必須
- eContent	任意選択
CertificateSet (Certificates)	必須
- Certificate	必須 a)
- AttributeCertificateV2	禁止
- OtherCertificateFormat	要別途規定
RevocationInfoChoices (crls)	任意選択
- CertificateList	任意選択
- OtherRevocationInfoFormat	要別途規定
SignerInfos	必須 b)
- signerInfo	必須
注 a) 相互運用性の観点から少なくとも署名者証明書を格納することを求める。 注 b) SignerInfo は一つのみ。複数あってはならない。	

表 6.5.4 SignerInfo 署名者情報

要素	要求レベル
CMSVersion	必須
SignerIdentifier	必須
- IssuerAndSerialNumber	要別途規定
- SubjecKeytIdentifier	要別途規定
DigestAlgorithmIdentifier	必須
SignedAttributes	必須
SignatureAlgorithmIdentifier	必須
SignatureValue	必須
UnsignedAttributes	要別途規定

表 6.5.5 及び表 6.5.6 に記載されていない署名属性要素及び非署名属性要素の要求レベルは"要別途規定"とする。

表 6.5.5 SignedAttributes 署名属性

要素	要求レベル
ContentType	必須
MessageDigest	必須
SigningCertificateReference	必須
- ESS SigningCertificate	任意選択
- ESS SigningCertificateV2	任意選択 a)
- OtherSigningCertificate	要別途規定
SignaturePolicyIdentifier	要別途規定 b)
CommitmentTypeIndication	要別途規定 b)
SignerIdentifier	要別途規定
ContentTimestamp	要別途規定
SigningTime	禁止
ContentReference	禁止
ContentIdentifier	禁止
ContentHints	禁止
SignerAttributes	要別途規定 c)
SignerLocation	任意選択 d)

注 a) PAdES using CAdES signatures を新たに生成する場合には、signingCertificateV2 を使用すること。
注 b) ISO/DIS 32000-2 の 12.8.3.4.4 節を参照のこと。
注 c) ISO/DIS 32000-2 の 12.8.3.4.3 節を参照のこと。
注 d) SignerLocation 属性または署名辞書の Location 要素のいずれか一方を使用すること。

表 6.5.6 追加非署名属性

要素	要求レベル
SignatureTimestamp	必須
CounterSignature	禁止
CompleteCertificateRefs	禁止
CertificateValues	禁止
CompleteRevocatoinRefs	禁止
RevocationValues	禁止
CAdES-C timestamp	禁止
Time-stamped cert and crls reference	禁止
ArchiveTimestamp(v1/v2/v3)	禁止

また、PDF データへの格納に関して以下を要件とする。

- 一つの PDF データ内に、複数の署名辞書を格納してもよい。電子署名を含んだ署名辞書のそれぞれは PDF の増分更新によって追加すること。
- PDF データ内に DSS(Document Security Store)を含んではならない。
- PDF データ内に電子署名以外の署名辞書（DocumentTimestamp）を含んではならない。

６.５.５ PAdES-A に関する要件

PAdES-A プロファイルは、PAdES-T データの拡張として定義される。PAdES-A は署名対象のデータ、署名データ、タイムスタンプ、署名データ及びタイムスタンプに関する検証情報を保護する形式である。PAdES-A の PDF データ構造のイメージを図 6.5.3 に示す。

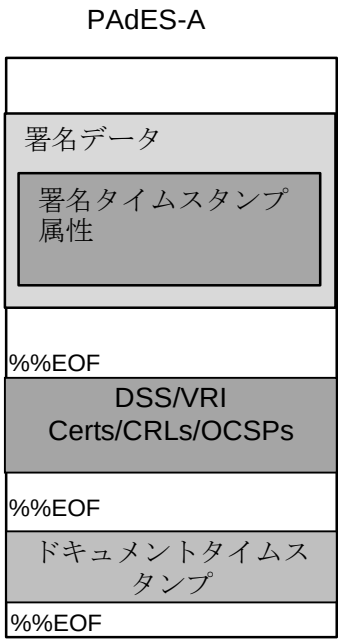

図 6.5.3 PAdES-A プロファイルの PDF データ構造のイメージ

PAdES-T に対して表 6.5.7 で示す要素を追加する。

表 6.5.7 PAdES-A プロファイルで追加する要素

要素	要求レベル
Document Security Store (DSS) 辞書	必須
Document timestamp 辞書（署名辞書）	必須 (表 6.5.8 参照)

DSS 辞書及び、DSS 辞書から参照される VRI 辞書の要件は ISO 32000-2 に従う。DSS 辞書には、それ以前に含まれる全ての署名データとタイムスタンプの検証に必要な証明書チェーン、失効情報を格納する。DSS 辞書を追加した後に、ドキュメントタイムスタンプ（Document Timestamp）を付与することで、これらの情報を保護する。

表 6.5.8 Document Timestamp 署名辞書の要件

要素	要求レベル	条件/値
Type	必須	DocTimeStamp
Filter	必須	
SubFilter	必須	ETSI.RFC3161
Contents	必須	TimeStampToken a)
ByteRange	必須 b)	
Reference	禁止	
Changes	禁止	
Name	禁止	
M	禁止	
Cert	禁止	
Location	禁止	
Reason	禁止	
ContactInfo	禁止	
R	禁止	
V	任意選択	0
Prop_Build	任意選択	
Prop_AuthTime	禁止	
Prop_AuthType	禁止	
注 a) RFC 3161 のタイムスタンプを使用する。 注 b) バイトレンジは Contents フィールドを除いた PDF ファイル全体（署名辞書を含む）を範囲とする。		

署名データ及びタイムスタンプ、検証情報の保護のために付与されたドキュメントタイムスタンプに使用されている証明書の有効期限が切れる前に、新たなドキュメントタイムスタンプを追加することで、有効性の延長を行うことができる(PAdES-A の更新)。PAdES-A の更新は PDF の増分更新を用いて以下の手順で行う。

1）ドキュメントタイムスタンプの検証に必要な証明書チェーン及び失効情報を PDF のストリームオブジェクトとして追加し、それらのオブジェクトに対する参照を含んだ DSS を追加する。

2）1）で追加した要素を保護する形で、新たなドキュメントタイムスタンプを追加する。

６.５.６ 各構成要素の概要

６.５.６.１ PAdES-T プロファイルの署名辞書

・Type 要素

辞書のタイプが署名であることを指定する。

・Filter 要素

署名を検証するときに優先して使用する署名ハンドラ名。

・SubFilter 要素

署名辞書の署名値とキー情報のエンコーディング名。

・Contents 要素

署名値。

・ByteRange 要素

署名対象のバイト範囲。

・M 要素

署名がなされた時刻を保持する。時刻の正確さは要求されない。

・Cert 要素

署名および署名検証に使用する証明書チェーン。なお、先頭の証明書は署名者証明書を格納する。

・Location 要素

署名した場所。

・Reason 要素

署名した理由。

・ContactInfo 要素

署名者に連絡するための署名者の情報。

６.５.６.２ 署名辞書の Contents に入る ContentInfo

・ContentType 要素

暗号メッセージの種別。これはオブジェクト識別子であり、この暗号メッセージの種別を定義した機関によって割り当てられた一意に定まる整数列である。

・Content 要素

暗号メッセージの内容。この内容は、コンテント種別によって一意に定められる。

６.５.６.３ Content に格納する SignedData 署名付きデータ

・CMSVersion 要素

CMS のバージョン。

・DigestAlgorithmIdentifiers 要素

ダイジェストアルゴリズムの集まり。

・EncapsulatedContentInfo 要素

署名対象文書（データ）及びそれに関する情報。

　・eContentType 要素

　署名対象文書（データ）のデータ型を一意に識別するオブジェクト識別子。

　・eContent 要素

　署名対象文書（データ）のデータバイト列を格納する。省略することによって、"外部署名"を構成することが可能になる。

・CertificateSet (Certificates) 要素

証明書の集まり。認識される"ルート"または"最上位の証明機関"から署名者情報群に含まれるすべての署名者までの連鎖を含むことができる。この規格では、(1) 証明書のみを対象とする。

(1) Certificate 要素
証明書
(2) AttributeCertificateV2 要素
属性証明書 2 版
(3) OtherCertificateFormat 要素
その他形式の証明書

・RevocationInfoChoices (crls) 要素
証明書失効リスト(CRL)の集まり。証明書群に含まれる証明書が有効か否かを決定するための情報を含むことができる。
(1) CertificateList 要素
失効情報
(2) OtherRevocationInfoFormat 要素
その他形式の失効情報

・SignerInfos 要素
署名者情報の集まり。0 個も含めて、どのような数の署名者情報も含むことがある。

6.5.6.4 SignerInfo 署名者情報

・CMSVersion 要素
署名者情報の構文の版数である。署名者識別子が発行者及びシリアル番号ならば、値は 1 でなければならない。対象者鍵識別子ならば、値は 3 でなければならない。

・SignerIdentifier 要素
署名者の証明書を特定する（それによって署名者の公開鍵も特定する。）。署名者の公開鍵は、受信者が署名を検証するのに必要である。署名者の公開鍵を特定するための二つの選択肢を提供する。
・IssuerAndSerialNumber 要素
署名者の証明書を、発行者の識別名及び証明書のシリアル番号によって識別する。
・SubjecKeytIdentifier 要素
署名者の証明書を X.509 の対象者鍵識別子の拡張値によって識別する。

・DigestAlgorithmIdentifier 要素
署名者に使われたメッセージダイジェストのアルゴリズム及び関連するパラメータを識別する。メッセージダイジェストのアルゴリズムは、関連する署名付きデータのダイジェストアルゴリズム識別子群領域に挙げられているものでなければならない。

・SignedAttributes 要素
署名される属性の集まり。任意選択であるが、存在する場合は DER 符号化と、少なくともコンテント種別とメッセージダイジェストの二つの属性を含まなければならない。

・SignatureAlgorithmIdentifier 要素
署名者に使われたメッセージダイジェストのアルゴリズム及び関連するパラメータを識別する。

・SignatureValue 要素
署名の値。

・UnsignedAttributes 要素
署名対象とはならない属性の集まり。

6.5.6.5 SignedAttributes 署名属性

・ContentType 要素
署名対象データのデータ型のオブジェクト識別子を保持する。署名属性が存在する場合には必ず含めなければならない。

・MessageDigest 要素
署名対象データのハッシュ値を保持する。署名属性が存在する場合には必ず含めなければならない。

・SigningCertificateReference 要素
署名者証明書を特定する情報（署名者証明書のハッシュ値）を保持する。
注記：本属性は署名者証明書を特定するという目的においては対象者鍵識別子と同じであるが、対象者鍵識別子は署名保護されるフィールドではないため、改ざんされてもその事実を署名検証時に検知することができないという脆弱性を補うことができる。
(1) ESS SigningCertificate 要素
ESS 署名者証明書の参照情報
(2) ESS SigningCertificateV2 要素
ESS 署名者証明書の参照情報 2 版
(3) OtherSigningCertificate 要素
ESS 署名他の署名者証明書の参照情報
・SignaturePolicyIdentifier 要素
署名ポリシを特定するための情報を保持する。署名ポリシは、署名者と署名の検証者が守るべき一連の規則。
・CommitmentTypeIndication 要素
署名者がどのような意図を持って署名したかを表明する情報を保持する。
・SignerIdentifier 要素
署名者の証明書を特定する（それによって署名者の公開鍵も特定する。）。署名者の公開鍵は、受信者が署名を検証するのに必要である。署名者の公開鍵を特定するための二つの選択肢を提供する。
・ContentTimestamp 要素
署名対象文書に対するタイムスタンプ。署名時点より前に取っておいた署名対象文書の存在証明（つまりタイムスタンプ）を署名データに含めたい場合に利用する。
・SigningTime 要素
署名がなされた時刻を保持する。時刻の正確さは要求されない。
・ContentReference 要素
他の署名文書へのリンクを保持する。
・ContentIdentifier 要素
署名対象文書のハッシュ値など、コンテントを一意に特定する情報を保持する。
・ContentHints 要素
署名対象文書のデータフォーマットに関する補足情報を保持する。
・SignerAttributes 要素
任意の署名者属性情報を保持する。署名者属性情報には大きく分けて、署名者が自分でそうだと主張している属性情報と、署名者がそうであると第三者が保証している属性情報の２種類があり、本属性にはそのどちらの属性情報も格納することができる。
・SignerLocation 要素
署名者の署名時における居所情報を格納する属性である。第三者によってその確かさが保証されたものではなく、署名者が署名時にその場所にいたと主張しているものである。

6.5.6.6 追加非署名属性
・SignatureTimestamp 要素
署名タイムスタンプ。
・CounterSignature 要素
署名値に対する署名。複数人が同一文書に署名する際、署名の順序に意味がある、もしくは意味を持たせたい場合に用いる。
・CompleteCertificateRefs 要素
署名検証に必要な、署名者証明書から信頼点の証明書までの認証パス上のすべての証明書の参照情報（ただし署名者の証明書への参照情報は含まない）。1 署名につき一つだけ存在する。

・CertificateValues 要素
完全な証明書参照情報群が参照する証明書及び署名者の証明書を保持する。1 署名につき一つだけ存在する。
⑴ 証明書
⑵ CA 等による証明書の保管
・CompleteRevocatoinRefs 要素
完全な失効参照情報群で参照される CRL と OCSP 応答の値を保持する。1 署名につき一つだけ存在する。
⑴ CRL 形式の失効参照情報群
⑵ OCSP 形式の失効参照情報群
⑶ 他の形式の失効参照情報群
・RevocationValues 要素
署名検証に必要な、署名者から信頼点までの証明書に対する CRL あるいは OCSP 応答のすべての参照情報。1 署名に対して一つだけ存在する。
⑴ CRL による失効情報
⑵ 基本 OCSP 応答
⑶ 他の失効情報
⑷ CA 等による失効情報の保管
・CAdES-C timestamp 要素
認証経路を構成する全証明書参照情報付き署名(CAdES-C)全体に対するタイムスタンプ。1 署名につき複数存在可能。
・Time-stamped cert and crls reference 要素
検証情報へのリファレンス（完全な証明書参照情報群及び完全な失効参照情報群）に対するタイムスタンプ。
・ArchiveTimestamp(v1/v2/v3)要素
改ざん検知を可能にするために、署名対象及び検証情報を含む署名に関する情報に付されるタイムスタンプ。

注記　id-aa-ets-archiveTimestampV3、id-aa-48 及び id-aa-27 はそれぞれ、ETSI/EN 319 122–1 v1.1.1、ETSI TS 101 733 V1.7.3 及び ETSI TS 101 733 V1.2.2 で定義されている。

6.5.6.7 PAdES-A プロファイルで追加する要素
・Document Security Store (DSS) 辞書要素
証明書検証に必要な検証情報（証明書、失効情報）
・Document timestamp 辞書（署名辞書）要素
文書に付与されたアーカイブタイムスタンプと関連情報。

6.5.6.8 Document Timestamp 署名辞書の要件
・Type 要素
辞書のタイプが署名であることを指定する。
・Filter 要素
署名を検証するときに優先して使用する署名ハンドラ名。
・SubFilter 要素
署名辞書の署名値とキー情報のエンコーディング名。
・Contents 要素
署名値。
・ByteRange 要素
署名対象のバイト範囲。
・Reference 要素

署名の参照辞書。
・Changes 要素
前の署名から行われた文書の変更情報。（変更したページ数、フィールド数、入力されたフィールド数）
・Name 要素
文書に署名した個人名、組織名等。
署名から名前を抽出できない場合に使用する。
・M 要素
署名がなされた時刻を保持する。時刻の正確さは要求されない。
・Cert 要素
署名および署名検証に使用する証明書チェーン。なお、先頭の証明書は署名者証明書を格納する。
・Location 要素
署名した場所。
・Reason 要素
署名した理由。
・ContactInfo 要素
署名者に連絡するための署名者の情報。
・R 要素
署名生成で使用された署名ハンドラのバージョン。
・V 要素
署名辞書のフォーマットのバージョン。
SubFilter の値のコンテキストにおける署名辞書の使用法に対応する。
署名の検証のために参照辞書が重要であると見なされる場合、値は 1 である。
・Prop_Build 要素
署名生成時の環境などの情報
・Prop_AuthTime 要素
署名者が最後に認証されてからの経過時間
・Prop_AuthType 要素
署名者を認証する方式。（PIN、生体認証等）

6.5.7 PAdES 検証に関する留意点

PDF ファイルにおいて、署名及びタイムスタンプの付与以降に、コンテンツそのものに影響を及ぼす場合（例えば、表示上に影響を及ぼすデータが追記された場合）、署名及びタイムスタンプの検証ソフトウェアあるいは PDF ビューアは、その旨を示す警告を提示すべきである。

PDF ビューアは、（複数ある場合は個々の）署名及びタイムスタンプの適用範囲の文書を表示することが可能であるべきである。ただし、署名タイムスタンプについては、対象とする署名を識別できるような情報を提示できればよい。

6.5.8 複数署名の扱いについて

PDF の増分更新により署名辞書を追記することで、一つの PDF データに複数の電子署名を付与することができる。複数の電子署名に対して PAdES-A を作成する場合には、以下に例示するようなケースがありえる。

図 6.5.4 は複数の PAdES-T の電子署名を連続的に付与するフローのケースである。これらの複数の PAdES-T を PAdES-A とする場合には、DSS/VRI に全ての電子署名と署名タイムスタンプに関する検証情報を格納し、ドキュメントタイムスタンプを付与する。このドキュメントタイムスタンプは、全ての電子署名と署名タイムスタンプに対するアーカイブタイムスタンプ（6.1 節参照）として機能する。

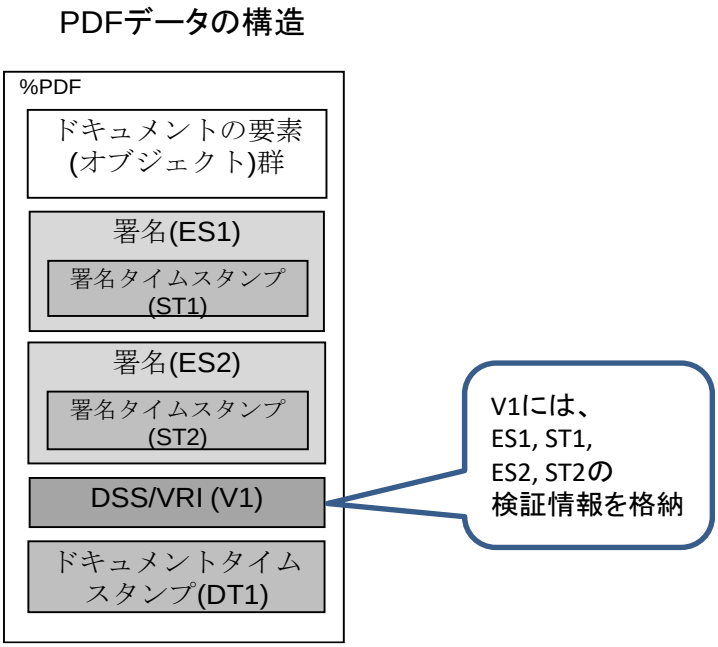

図 6.5.4 複数署名の例 1

図 6.5.5 は、ある電子署名の付与から時間が経過した後（証明書の有効期限を超える場合など）、別の電子署名を追加するフローのケースである。このケースでは、過去の電子署名に対する DSS/VRI およびドキュメントタイムスタンプを付与した後に、新たな電子署名を付与することとなる。新たな電子署名を長期保存する場合には、その電子署名に対する DSS/VRI およびドキュメントタイムスタンプを追加する。

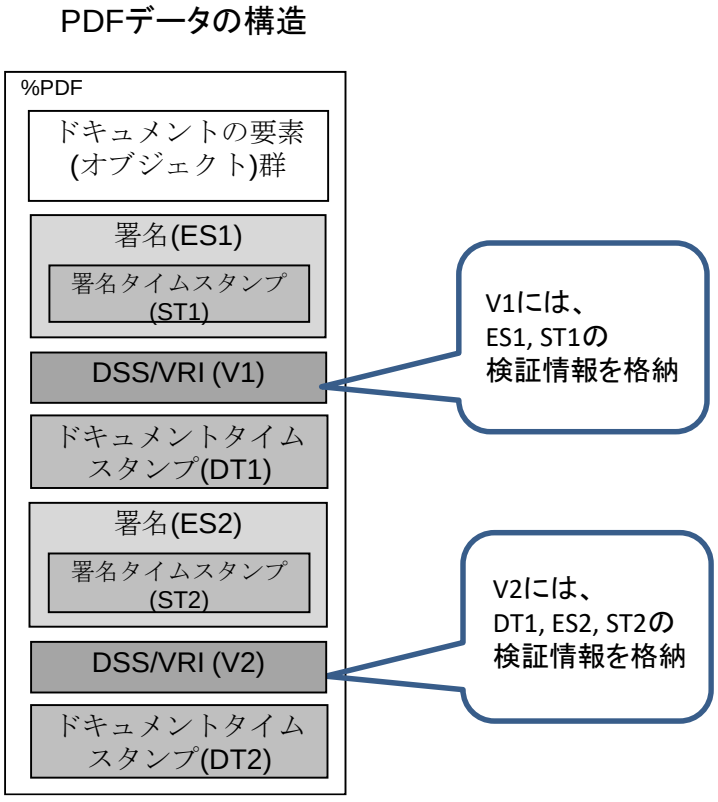

図 6.5.5 複数署名の例 2

６.６ JAdES に関する規格

６.６.１ 概要

JAdES の生成及び検証に関する要件を示す。

6.6.2 節にこの規格で定義するプロファイルの概要を、6.6.3 節に JAdES の構造を示す。6.6.4 節に要求レベルの表現法、6.6.5～6.6.7 節にプロファイルの要件を示し、6.6.8 節に各構成要素の概要を示す。

６.６.２ 定義する長期署名プロファイル

電子署名を長期にわたって検証可能にするためには、相互運用性が確保されていることのほかに、署名時刻の特定が可能であることに加え、署名対象及び検証情報を含む署名に関する情報の改ざん検知が可能であることが必要である。この規格では、JAdES に関して、次の三つのプロファイルを定義することによって、これらの要求を満たす。

(1)　JAdES-T プロファイル
　JAdES-T データの生成及び検証に関するプロファイル。

(2)　JAdES-XL プロファイル
　JAdES-XL データの生成及び検証に関するプロファイル。

(3)　JAdES-A プロファイル
　JAdES-A データの生成及び検証に関するプロファイル。

ここで、JAdES-T データ、JAdES-XL データ、及び JAdES-A データの関係を図 6.6.1 に示す。

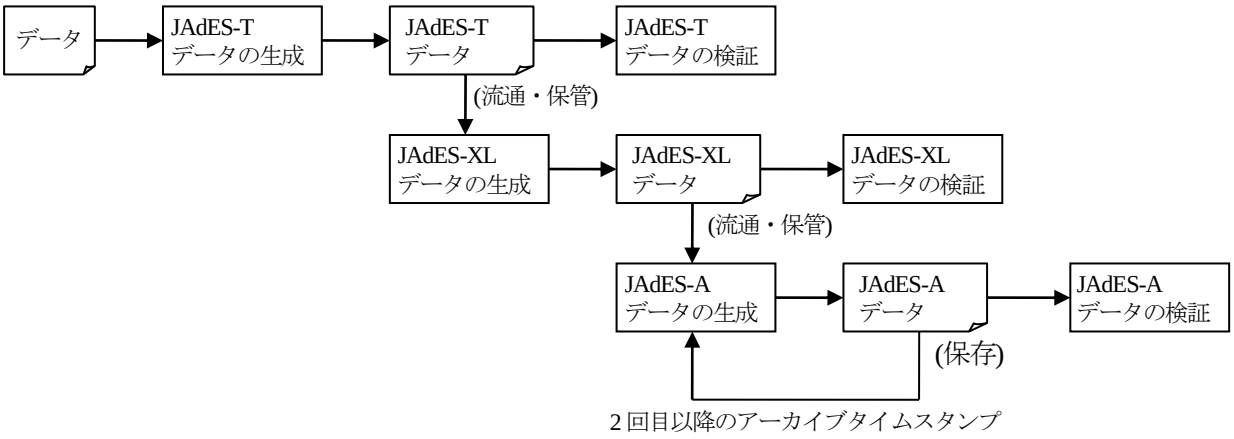

図 6.6.1 JAdES-T データ、JAdES-XL データ、及び JAdES-A データとの関係

６.６.３ JAdES データの構造

JAdES データの構造は、XML 署名の拡張形として定義される。図 6.6.2 に JAdES の構造の一例を示す。図 6.6.3 に JAdES　Serialization の構造を示す。

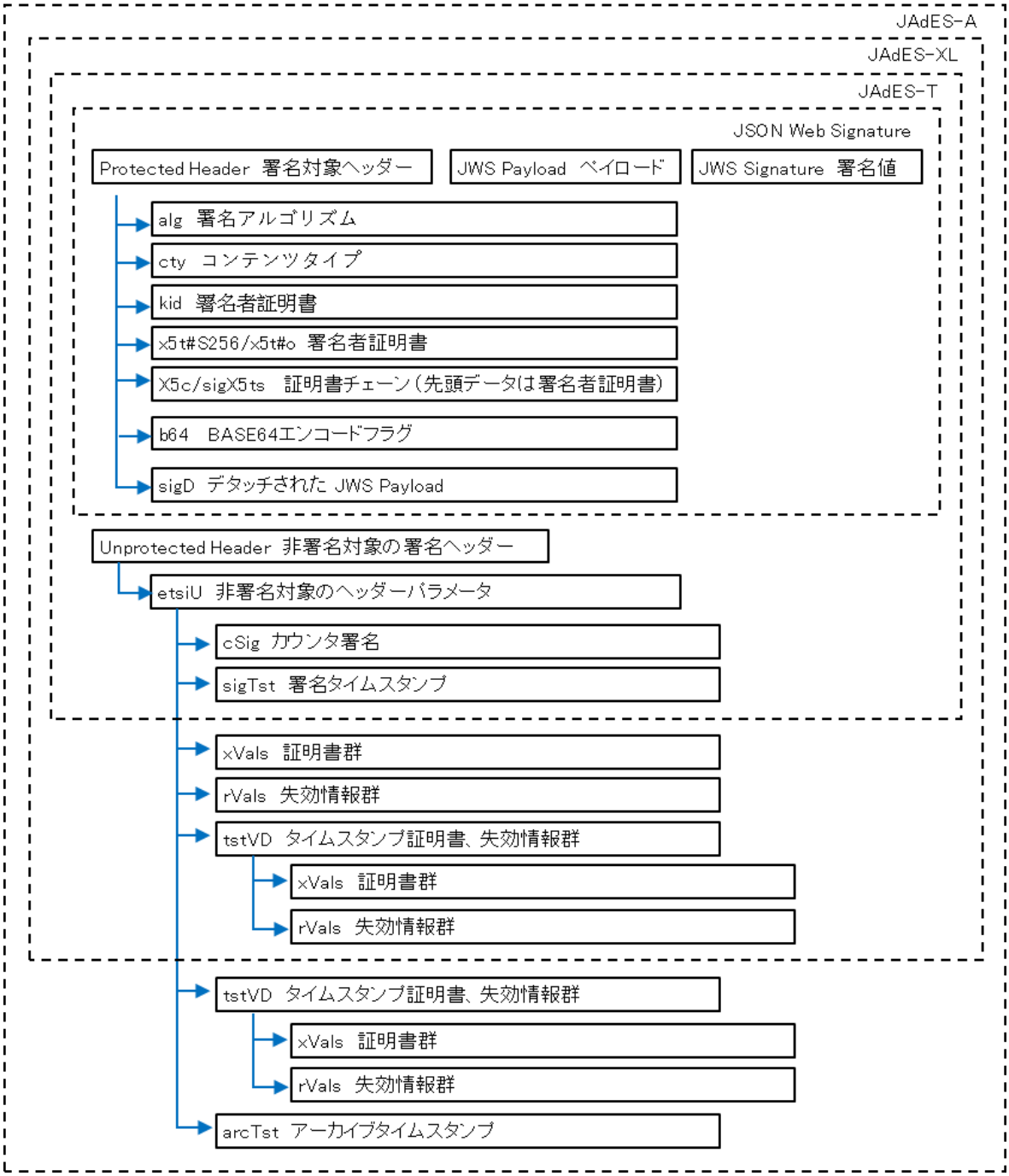

図 6.6.2 JAdES 構造の一例

構造	概略図	要求
JWS Compact Serialization	[Protected Header].[JWS　Payload].[JWS Signature]	使用禁止
JWS JSON Serialization （General）	[JWS Payload] [Signatures] 　[Protected Header] 　[Unprotected Header] 　[JWS Signature] 　: 　: 　[Protected Header] 　[Unprotected Header] 　[JWS Signature]	使用可
JWS JSON Serialization （Flattened）	[JWS Payload] [Protected Header] [Unprotected Header] [JWS Signature]	使用可

図 6.6.3 JAdES　Serialization 構造

６.６.４ 要求レベルの表現法

この規格では、JAdES-T データ、JAdES-XL データ及び JAdES-A データを構成する各要素に対する、プロファイルとしての要求レベルとして、次の表現法を定義する。

(1)　必須

この要求レベルを持つ要素は必ず実装しなければならない。この要求レベルの要素が、選択肢となる下位要素を持つ場合は、少なくともその下位要素の一つを選択しなければならない。また、この要求レベルの要素が、任意選択要素の下位要素の一つである場合は、その任意選択要素を選択するときはこの必須要素も選択しなければならない。

(2)　任意選択

この要求レベルを持つ要素の実装は任意とする。

(3)　要別途規定

この要求レベルを持つ要素の実装は任意とするが、基本的に相互運用性の確保を前提としているため、使用しないことを推奨する。ただし、特定のユースケースにおいて利用者の合意に基づき、合意の範囲内で使用することを妨げるものではない。使用する場合はその処理に関して、別途に詳細な仕様を規定しなければならない。

(4)　禁止

この要求レベルを持つ要素は、データ中に含めてはならない。検証時は、その要素を無視してよい。

６.６.５ JAdES-T に関する要件

表 6.6.1～表 6.6.4 に記載されていない要素の要求レベルは、要別途規定である。

表 6.6.1 Protected Header パラメータ

要素	要求レベル	条件/値
alg 署名アルゴリズム	必須	
cty コンテンツタイプ	任意選択	
kid 鍵情報	任意選択	
crit クリティカル	任意選択	
sigT 署名時刻	任意選択	
x5u 証明書チェーン（先頭データは署名者証明書）	禁止	
x5t 署名者証明書	禁止	SHA-1 の場合の要素
x5t#S256 署名者証明書	任意選択 a)	SHA-256 の場合、この要素を使用
x5t#o 署名者証明書	任意選択 a)	SHA-256 以外の場合、この要素を使用
sigX5ts 証明書チェーン（先頭データは署名者証明書）	任意選択 a)	
x5c 証明書チェーン（先頭データは署名者証明書）	任意選択 a)	
sigPId 署名ポリシ識別子	要別途規定	
sigPl 署名生成場所	要別途規定	
srAts 署名者の肩書き	要別途規定	
sdF データオブジェクト形式	要別途規定	
srCms コミットメント種別表示	要別途規定	
adoTst 全データオブジェクトに対するタイムスタンプ	要別途規定	
idoTst 個別データオブジェクトに対するタイムスタンプ	要別途規定	
b64 BASE64 エンコードフラグ	任意選択	
sigD デタッチされた JWS　Payload	任意選択	

要素	要求レベル	条件/値
注 a) 少なくとも 1 つのヘッダーパラメータが必要である。		

表 6.6.4 Unprotected Header パラメータ

要素	要求レベル	条件/値
etsiU 非署名対象のヘッダーパラメータ	必須	
・・cSig カウンタ署名	任意選択	
・・sigTst 署名タイムスタンプ	必須	RFC3161 で定義されるタイムスタンプ6

6 タイムスタンプを取得し JAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

6.6.6 JAdES-XL に関する要件

表 6.6.5 に記載されていない要素の要求レベルは、要別途規定である。

表 6.6.5 UnsignedProperties 要素

要素	要求レベル	条件/値
etsiU 非署名対象のヘッダーパラメータ	必須	
・・rRefs 全失効情報参照情報群	禁止	
・・axRefs 属性証明書参照情報群	禁止	
・・arRefs 属性失効情報参照情報群	禁止	
・・sigRTst 署名及び参照情報に対するタイムスタンプ	禁止	
・・rfsTst 参照情報に対するタイムスタンプ	禁止	
・・xVals 証明書群	必須	
・・・・x509Cert カプセル構造化された証明書	任意選択	
・・・・otherCert 他の証明書	禁止	
・・rVals 失効情報群	必須	
・・・・crlVals CRL による失効情報群	任意選択	
・・・・ocspVals OCSP による失効情報群	任意選択	
・・・・otherVals 他の失効情報群	禁止	
・・axVals 属性証明書群	禁止	
・・arVals 属性失効情報群	禁止	

6.6.7 JAdES-A に関する要件

JAdES-A プロファイルは、JAdES-T データの拡張として定義される。JAdES で定義された非署名対象の署名プロパティ要素の各要素は、表 6.6.6 に示す要求レベルに従う。この表に定義されていない要素の要求レベルは"要別途規定"である。

表 6.6.6 UnsignedSignatureProperties 要素

要素	要求レベル	条件/値
etsiU 非署名対象のヘッダーパラメータ	必須	
・・xRefs 全証明書参照情報群	禁止	
・・rRefs 全失効情報参照情報群	禁止	
・・axRefs 属性証明書参照情報群	禁止	
・・arRefs 属性失効情報参照情報群	禁止	
・・sigRTst 署名及び参照情報に対するタイムスタンプ	禁止	
・・rfsTst 参照情報に対するタイムスタンプ	禁止	
・・xVals 証明書群	必須	
・・・・x509Cert カプセル構造化された証明書	任意選択	
・・・・otherCert 他の証明書	禁止	
・・rVals 失効情報群	必須	
・・・・crlVals CRL による失効情報群	任意選択	
・・・・ocspVals OCSP による失効情報群	任意選択	
・・・・otherVals 他の失効情報群	禁止	
・・axVals 属性証明書群	禁止	
・・arVals 属性失効情報群	禁止	
・・tstVD タイムスタンプ証明書、失効情報群	必須	
・・・・xVals 証明書群	任意選択	
・・・・・・x509Cert カプセル構造化された証明書	任意選択	
・・・・・・otherCert 他の証明書	禁止	
・・・・rVals 失効情報群	任意選択	
・・・・・・crlVals CRL による失効情報群	任意選択	

・・・・・・ocspVals OCSP による失効情報群	任意選択	
・・・・・・OtherValues 他の失効情報群	禁止	
・・・・arcTst アーカイブタイムスタンプ	必須	
・・・・・・*not distributed case（非分離型）*	必須	RFC3161 で定義されるタイムスタンプ7
・・・・・・*distributed case（分離型）*	禁止	
・・・・・・タイムマークなどその他の方式	禁止	
注記 1 イタリック体は処理方式を示す。		

7 タイムスタンプを取得し JAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

６.６.８ 各構成要素の概要

６.６.８.１ 署名対象の指定

表 6.6.7 に署名対象の指定方法について示す。

表 6.6.7 署名対象の指定方法

ヘッダーパラメータ			説明	要求
JWS Payload			JWS で規定され、保護されるオクテットのシーケンス。Payload は、任意のオクテットシーケンスを含めることができる。	使用可
sigD	HttpHeaders		複数の HTTP ヘッダーを明示的に参照し、それらと HTTP メッセージボディに署名する。(HTTP リクエストデータに対して署名を行う。)	使用禁止
	URI references	ObjectIdByURI	指定された URL のデータに対して署名する。複数のリンクがある場合は連結したデータに対して署名を行う。	使用禁止
		ObjectIdByURIHash	ObjectIdByURI と同じ。 ただし、各データに対してハッシュ値を保管する。	使用可

①HttpHeaders

HttpHeaders を指定した場合の sigD 要素の要求レベルを表 6.6.8 に、HttpHeaders の場合の構造について図 6.6.5 に示す。

表 6.6.8 sigD 要素

要素	要求レベル	条件/値
Mid メソッド ID	必須	http://uri.etsi.org/19182/HttpHeaders
pars	必須	HTTP ヘッダーフィールドの小文字の名前の配列
hashM ハッシュメソッド	禁止	
hashV ハッシュ値	禁止	
ctys コンテンツタイプ	禁止	

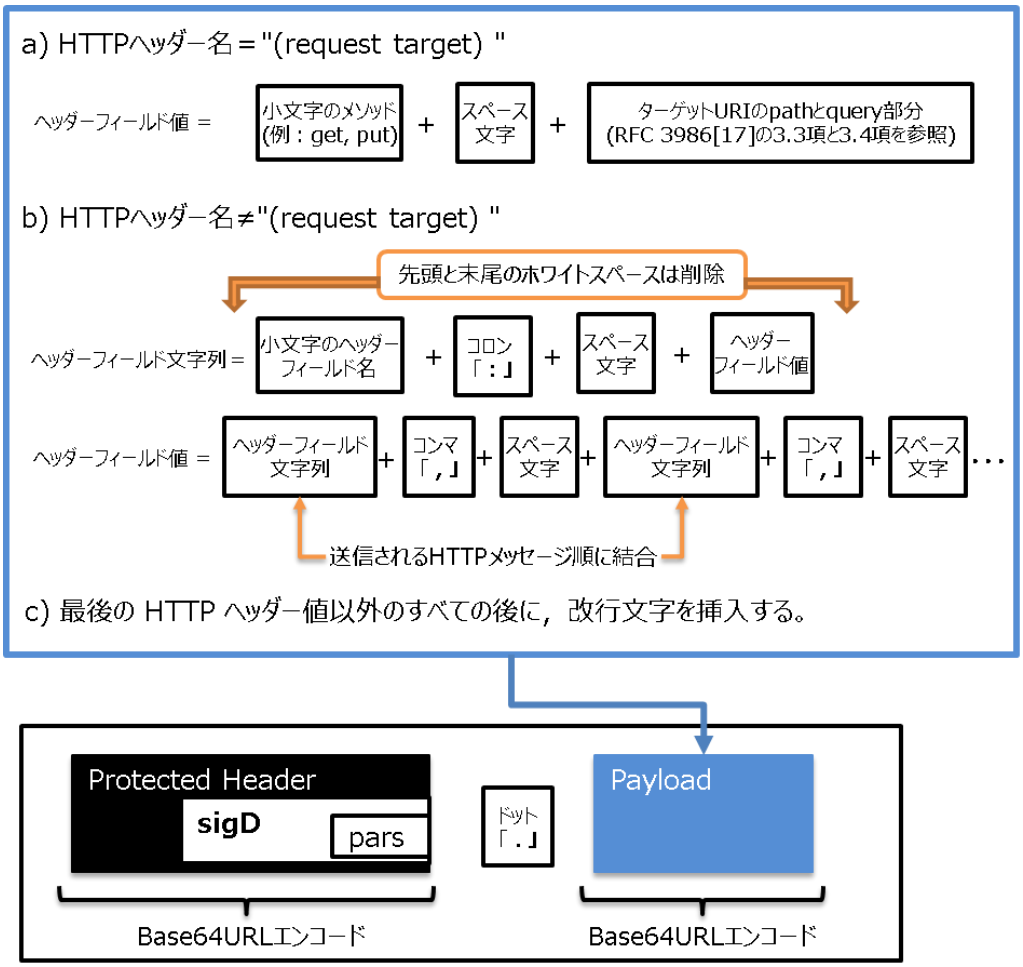

図 6.6.5 HttpHeaders の場合の構造

②ObjectIdByURIHash

ObjectIdByURIHash を指定した場合の sigD 要素の要求レベルを表 6.6.9 に、ObjectIdByURIHash の場合の構造について図 6.6.6 に示す。

表 6.6.9 sigD 要素

要素	要求レベル	条件/値
Mid メソッド ID	必須	http://uri.etsi.org/19182/ObjectIdByURIHash
pars	必須	URI の配列 （RFC3986 1.1.3）
hashM ハッシュメソッド	必須	
hashV ハッシュ値	必須	
ctys コンテンツタイプ	任意選択	

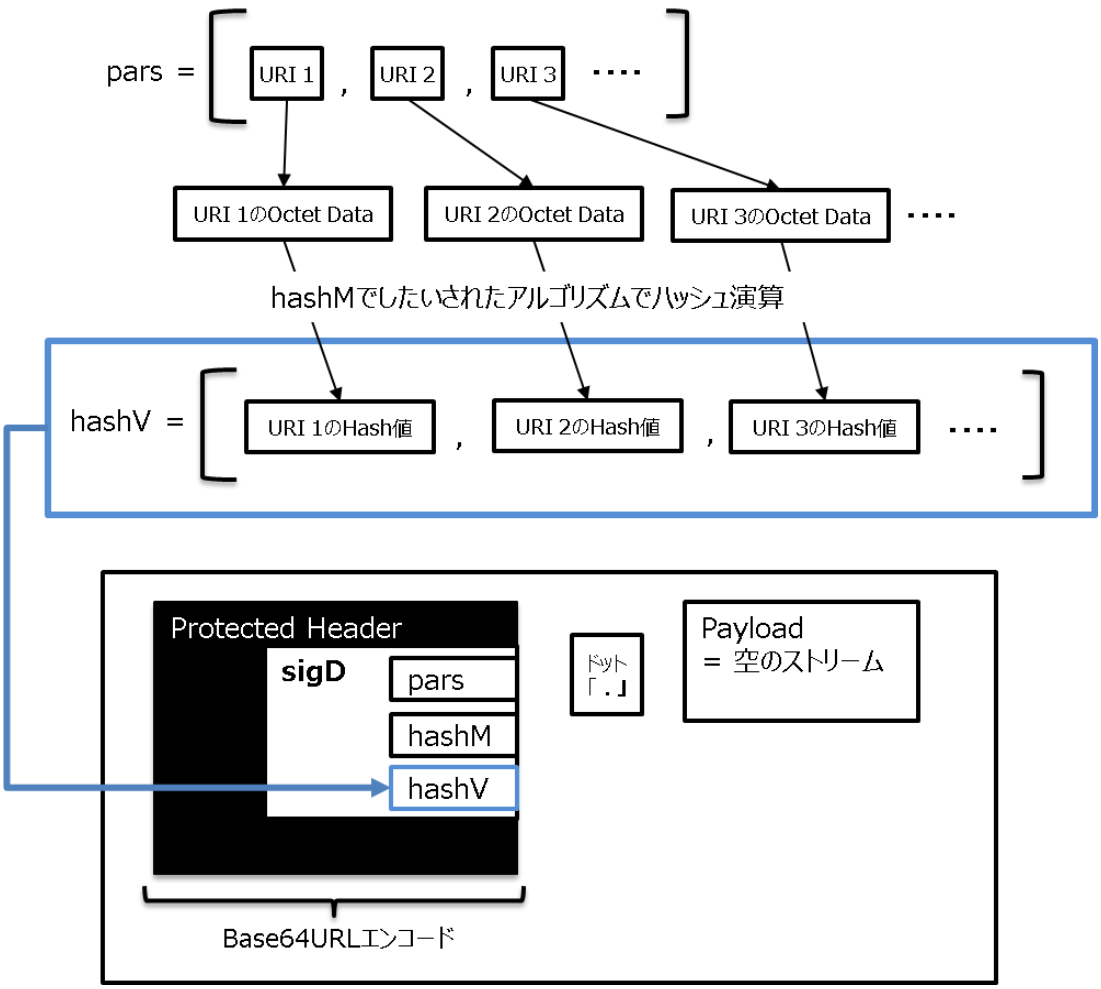

図 6.6.6 ObjectIdByURIHash の場合の構造

6.6.8.2 署名対象ヘッダーパラメータ

・署名アルゴリズム

署名を修飾する署名付きヘッダーパラメータ。

・コンテンツタイプ

JWS ペイロードを修飾する署名付きヘッダーパラメータ。

・鍵情報

署名証明書を識別するのに役立つヒントとして使用される署名付きヘッダーパラメータ。

・クリティカル

拡張機能を使用する JOSE ヘッダーに存在するヘッダーパラメータ名をリストする署名付きヘッダーパラメータ。

・署名時刻

署名者が署名プロセスを実行したと主張する時刻を指定する署名付きヘッダーパラメータ。

・署名者証明書

署名に使用されるキーに対応する証明書を識別する署名付きヘッダーパラメータ。

・証明書チェーン

署名証明書の認証パス内の証明書を識別する署名付きヘッダーパラメータ。

・BASE64 エンコードフラグ

ペイロードが JWS 署名の入力で ASCII か、エンコードが実行されていない JWS Payload 値自体かを規

定する署名付きヘッダーパラメータ。
・デタッチされた JWS Payload
Payload が外部参照する情報を指定する署名付きヘッダーパラメータ。

6.6.8.3 非署名対象ヘッダーパラメータ
・非署名対象の署名ヘッダーパラメータ
署名対象外の署名に関するヘッダーパラメータ。
・カウンタ署名
署名値に対する署名。複数人が同一文書に署名するとき、署名の順序に意味がある場合、または意味を持たせたい場合に用いる。
・署名時刻を確定する情報
署名が存在した時刻を特定可能にするために、署名値に付されるタイムスタンプなどの情報。
(1)署名タイムスタンプ
(2)タイムマークなどその他の方式
注記　タイムマークは、データが特定の時刻以前に存在したことを示すための、データと特定の時間を結びつける信頼される第三者機関からの監査証跡内の情報など。
・非署名のデータオブジェクトのプロパティ
データオブジェクト（文書）に関連する署名対象とはならないプロパティ。

6.6.8.4 非署名対象のヘッダーパラメータ
・全証明書参照情報群
署名者を除く証明書チェーンを構成するすべての証明書参照情報のかたまり。
・全失効情報参照情報群
署名者証明書の証明書チェーンの検証に必要なすべての失効情報参照情報のかたまり。
a)CRL 形式の失効情報参照情報
b)OCSP 形式の失効情報参照情報
c)他の失効情報参照情報
・属性証明書参照情報群
関連する属性証明書に関する参照情報のかたまり。
・属性失効情報参照情報群
関連する属性証明書の失効情報に関する参照情報のかたまり。
・署名及び参照情報に対するタイムスタンプ
署名及び参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。
・参照情報に対するタイムスタンプ
参照情報に対するタイムスタンプ。非分離型と分離型が定義されている。
・証明書群
署名者証明書の証明書チェーンを構成するすべての証明書のかたまり。
(1)　カプセル構造化された証明書
(2)　他の証明書
(3)　CA 等による証明書の保管
・失効情報群
署名者証明書の証明書チェーン検証に必要なすべての失効情報のかたまり。
(1)　CRL による失効情報群
(2)　OCSP による失効情報群
(3)　他の失効情報群
(4)　CA 等による失効情報の保管
・属性証明書群

関連する属性証明書のかたまり。

・属性失効情報群

関連する属性証明書に対する失効情報のかたまり。

・改ざん検知を可能とする情報

改ざん検知を可能にするために、署名対象及び検証情報を含む署名に関する情報に付されるタイムスタンプなどの情報。

(1) アーカイブタイムスタンプ　非分離型と分離型が定義されている。

(2) タイムマークなどその他の方式

・異なる版の非署名対象の署名プロパティ

異なる版の JAdES で定義された署名対象とはならない署名プロパティ。

６.６.９ JAdES に関する留意点

JAdES は策定されたばかりの仕様であり、今後改定がある可能性があることを留意の上利用すること。

付録１：参考情報

・X.509 証明書

"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF RFC5280 及び Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC6818

・厚生労働省 HPKI の CP

保健医療福祉分野 PKI 認証局 署名用証明書ポリシ　1.9 版　（令和５年７月）

https://www.mhlw.go.jp/stf/shingi/0000212714.html

付録 2：CAdES-A で ArchiveTimestampV3 を使用する場合の要件

6.3.6 CAdES-A に関する要件で記載したように、ArchiveTimestamp のバージョンについては、日本における ArchiveTimestampV2 による継続的な検証を維持するために、本編では ArchiveTimestampV2 を前提とした記載としているが、ArchiveTimestampV3 を利用する場合の要件について、表 付 2.1 に示す要求レベルに従うこととする。この表に定義されていない要素の要求レベルは"要別途規定"である。

詳細は ETSI の最新規格を参照すること。

表 付 2.1 追加非署名属性

要素	要求レベル	条件/値
CounterSignature カウンタ署名	要別途規定	
Trusted time 信頼された時刻	必須	
・・SignatureTimeStamp 署名タイムスタンプ	任意選択	RFC3161 で定義されるタイムスタンプ
・・Time Mark or other method like archive time-stamp as its replacement タイムマークなどその他の方式	任意選択 a)	
CompleteCertificateReferences 完全な証明書参照情報群	要別途規定	
CompleteRevocationReferences 完全な失効参照情報群	要別途規定	
・・CompleteRevRefs CRL CRL 形式の失効参照情報群	任意選択	
・・CompleteRevRefs OCSP OCSP 形式の失効参照情報群	任意選択	
・・OtherRevRefs 他の形式の失効参照情報群	禁止	
Attribute certificate references 属性証明書の参照情報群	禁止	
Attribute revocation references 属性失効情報の参照情報群	禁止	
CertificateValues 証明書群	要別途規定	
・・CertificateValues 証明書	任意選択	
・・CA 等による証明書の保管	禁止	
RevocationValues 失効情報群	要別途規定	
・・CertificateList CRL による失効情報	任意選択	
・・BasicOCSPResponse 基本 OCSP 応答	任意選択	
・・OtherRevVals 他の失効情報	禁止	
・・CA 等による失効情報の保管	禁止	

CAdES-C-timestamp CAdES-C データへのタイムスタンプ	禁止	
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	禁止	
（改ざん検知を可能とする情報）	必須	
・・ArchiveTimestampV3 アーカイブタイムスタンプ id-aa-ets-archiveTimestampV3	任意選択	
・・ArchiveTimestampV2 アーカイブタイムスタンプ id-aa-48	要別途規定 b)	RFC3161 で定義されるタイムスタンプ8
・・ArchiveTimestampV1 アーカイブタイムスタンプ id-aa-27	要別途規定 b)	ETSI/TS 101 733 v1.4.0 もしくはそれ以前で定義される。 RFC3161 で定義されるタイムスタンプ 4
・・Evidence Record 証拠記録	任意選択	RFC 4998 で定義される証拠のレコード構文（ERS）
・・タイムマークなどその他の方式	禁止	
注 a) ISO 14533-4 で定義されているその他の方法 注 b) 推奨されない属性		

8 タイムスタンプを取得し CAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

付録３：ヘルスケア PKI を利用した医療文書に対する電子署名規格 2.0 での XAdES の要件

付録 3-1: ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0 での XAdES-T に関する要件

過去の「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」によって長期署名されていた XAdES－T の検証を可能とするために、「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」で示していた XAdES－T に関する要件を示す。

表 付 3.1～表 付 3.4 に記載されていない要素の要求レベルは、要別途規定である。

表 付 3.1 Signature 要素

要素/属性	要求レベル	条件/値
署名（ds:Signature）の ID 属性	必須 a）	
ds:SignedInfo 署名に関する情報	必須	
・・ds:CanonicalizationMethod コンテントの正規化方式	必須	C14n
・・ds:SignatureMethod 署名方式	必須	
・・ds:Reference コンテントへの参照情報	必須	
・・・・ds:Transforms 変換処理	任意選択	
・・・・ds:DigestMethod ダイジェスト方式	必須	
・・・・ds:DigestValue ダイジェスト値	必須	
ds:SignatureValue 署名値	必須	
ds:KeyInfo 鍵情報	任意選択 b)	
ds:Object オブジェクト	必須	
注記　イタリック体は属性を示す。 注 a)　XML 署名では“任意選択”であるが、XAdES では“必須”である。 注 b)　鍵情報(ds:KeyInfo) か、または署名者証明書の参照情報（SigningCertificate）（表 6.4.3）のいずれか一方が必要である。鍵情報を選択する場合（XAdES v1.1.1 の場合は必須）は、その下位要素に XML 署名で定義された X.509 データを含まなければならない。		

表 付 3.2 Object 要素

要素	要求レベル	条件/値
QualifyingProperties 署名を修飾するプロパティ	必須	対象属性に、署名要素の ID 属性の値を入れる
・・SignedProperties 署名対象プロパティ	必須	
・・UnsignedProperties 非署名対象プロパティ	任意選択	

QualifyingPropertiesRefernece 署名を修飾するプロパティを特定する参照情報	要別途規定	

表 付 3.3 SignedProperties 要素

要素	要求レベル	条件/値
SignedSignatureProperties 署名対象の署名プロパティ	必須	
・・SigningTime 署名時刻	任意選択 a)	
・・SigningCertificate 署名者証明書の参照情報	任意選択 a) b)	
・・SignaturePolicyIdentifier 署名ポリシ識別子	要別途規定	
・・SignatureProductionPlace 署名生成場所	要別途規定	
・・SignerRole 署名者の肩書き	要別途規定	
SignedDataObjectProperties 署名対象データオブジェクトのプロパティ	要別途規定	
・・DataObjectFormat データオブジェクト形式	要別途規定	
・・CommitmentTypeIndication コミットメント種別表示	要別途規定	
・・AllDataObjectsTimeStamp 全データオブジェクトに対するタイムスタンプ	要別途規定	
・・IndividualDataObjectTimeStamp 個別データオブジェクトに対するタイムスタンプ	要別途規定	
注 a)　XAdES v1.1.1 の場合は“必須”である。 注 b)　署名者証明書の参照情報(SigningCertificate)か、または鍵情報(ds:KeyInfo)（表 6.4.1）のどちらか一方が必要である。		

表 付 3.4 UnsignedProperties 要素

要素	要求レベル	条件/値
UnsignedSignatureProperties 非署名対象の署名プロパティ	必須	
・・CounterSignature カウンタ署名	任意選択	
・・(署名時刻を確定する情報)	必須	
・・・・SignatureTimeStamp 署名タイムスタンプ	必須	RFC3161 で定義されるタイムスタンプ9
・・・・TimeMark タイムマークなどその他の方式	禁止	
UnsignedDataObjectProperties 非署名のデータオブジェクトのプロパティ	要別途規定	

9 タイムスタンプを取得し XAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

付録 3-2: ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0 での XAdES-XL に関する要件

過去の「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」によって長期署名されていた XAdES－XL の検証を可能とするために、「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」で示していた XAdES－XL に関する要件を示す。

表 付 3.5 に記載されていない要素の要求レベルは、要別途規定である。

表 付 3.5 UnsignedProperties 要素

要素	要求レベル	条件/値
CompleteCertificateRefs 全証明書参照情報群	任意選択　a)	
CompleteRevocationRefs 全失効情報参照情報群	任意選択　a)	
・・CRLRef CRL 形式の失効情報参照情報	任意選択	
・・OCSPRef OCSP 形式の失効情報参照情報	任意選択	
・・OtherRef 他の失効情報参照情報	禁止	
AttributeCetrificateRefs 属性証明書参照情報群	禁止	
AttributeRevocationRefs 属性失効情報参照情報群	禁止	
SigAndRefsTimeStamp 署名及び参照情報に対するタイムスタンプ	禁止	
RefsOnlyTimeStamp 参照情報に対するタイムスタンプ	禁止	
CertificateValues 証明書群	必須	
・・EncapsulatedX509Certificate カプセル構造化された証明書	任意選択	
・・OtherCertificate 他の証明書	禁止	
・・(CA 等による証明書の保管)	禁止	
RevocationValues 失効情報群	必須	
・・CRLValues CRL による失効情報群	任意選択	
・・OCSPValues OCSP による失効情報群	任意選択	
・・OtherValues 他の失効情報群	禁止	
・・(CA 等による失効情報の保管)	禁止	
AttrAuthoritiesCertValues 属性証明書群	禁止	
AttributeRevocationValues 属性失効情報群	禁止	
注 a)　XAdES v1.1.1 の場合は必須である。		

付録 3-3: ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0 での XAdES-A に関する要件

過去の「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」によって長期署名されていた XAdES－A の検証を可能とするために、「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」で示していた XAdES－A に関する要件を示す。

表 付 3.6 に記載されていない要素の要求レベルは、要別途規定である。

表 付 3.6 UnsignedSignatureProperties 要素

要素	要求レベル	条件/値
CompleteCertificateRefs 全証明書参照情報群	任意選択 a)	
CompleteRevocationRefs 全失効情報参照情報群	任意選択 a)	
・・CRLRef CRL 形式の失効情報参照情報	任意選択	
・・OCSPRef OCSP 形式の失効情報参照情報	任意選択	
・・OtherRef 他の失効情報参照情報	禁止	
AttributeCetrificateRefs 属性証明書参照情報群	禁止	
AttributeRevocationRefs 属性失効情報参照情報群	禁止	
SigAndRefsTimeStamp 署名及び参照情報に対するタイムスタンプ	禁止	
・・*not distributed case（非分離型）*	禁止	
・・*distributed case（分離型）*	禁止	
RefsOnlyTimeStamp 参照情報に対するタイムスタンプ	禁止	
・・*not distributed case（非分離型）*	禁止	
・・*distributed case（分離型）*	禁止	
CertificateValues 証明書群	必須	
・・EncapsulatedX509Certificate カプセル構造化された証明書	任意選択	
・・OtherCertificate 他の証明書	禁止	
・・(CA 等による証明書の保管)	禁止	
RevocationValues 失効情報群	必須	
・・CRLValues CRL による失効情報群	任意選択	
・・OCSPValues OCSP による失効情報群	任意選択	
・・OtherValues 他の失効情報群	禁止	

・・(CA 等による失効情報の保管)	禁止	
AttrAuthoritiesCertValues 属性証明書群	禁止	
AttributeRevocationValues 属性失効情報群	禁止	
TimeStampValidationData タイムスタンプ証明書、失効情報群	必須	
・・CertificateValues 証明書群	任意選択	
・・・・EncapsulatedX509Certificate カプセル構造化された証明書	任意選択	
・・・・OtherCertificate 他の証明書	禁止	
・・・・(CA 等による証明書の保管)	禁止	
・・RevocationValues 失効情報群	任意選択	
・・・・CRLValues CRL による失効情報群	任意選択	
・・・・OCSPValues OCSP による失効情報群	任意選択	
・・・・OtherValues 他の失効情報群	禁止	
・・・・(CA 等による失効情報の保管)	禁止	
(改ざん検知を可能とする情報)	必須	
・・ArchiveTimeStamp アーカイブタイムスタンプ	必須	
・・・・*not distributed case (非分離型)*	必須	RFC3161 で定義されるタイムスタンプ10
・・・・*distributed case (分離型)*	禁止	
・・タイムマークなどその他の方式	禁止	
異なる版の署名対象外署名プロパティ要素	要別途規定	
注記 1 イタリック体は処理方式を示す。 注記 2 XAdES v1.1.1 及び 1.2.2 は、属性証明書群及び属性失効情報群並びに非分離型及び分離型が未定義であり、v1.1.1 はさらに、属性証明書参照情報群及び属性失効情報参照情報群が未定義である。 注 a) XAdES v1.1.1 の場合は必須である。		

10 タイムスタンプを取得し XAdES データへ格納する方法、および、そのタイムスタンプを検証する方法が標準規格で明確に示されていることから、RFC3161 タイムスタンプを対象とする。

付録４：作成者名簿

作成者（社名五十音順）

有馬	一閣	（株）NTT データ
兵	昂	キヤノンメディカルシステムズ（株）
平山	照幸	（株）ケーアイエス
長谷川	英重	JAHIS 特別委員
平田	泰三	JAHIS 特別委員
佐藤	雅史	セコム（株）
西山	晃	セコム（株）
瀧	勝也	（株）テクノウェア
佐藤	恵一	日本光電工業（株）
梶山	孝治	富士フイルムヘルスケア（株）
宮崎	一哉	三菱電機（株）
茗原	秀幸	三菱電機（株）
酒巻	一紀	三菱電機インフォメーションシステムズ（株）

改定履歴		
日付	バージョン	内容
2008/03/25	V1.0	最初のバージョン
2013/03	V1.1	改定
2019/02	Ver.2.0	改定ならびに PAdES 編の統合
2023/xx/xx	Ver.3.0	改定ならびに JAdES の追加

Ver.2.0 から Ver.3.0 への改定概要

- JSON に対する電子署名の長期プロファイル（JAdES）に関する 6.6 章の追加
  - JAdES の追加に伴う、用語・略語の追加
- 外部規格・外部環境の変化に伴った変更
  - 引用規格・引用文献の見直し
  - 安全管理ガイドラインが改定されたことによる変更
    - ✧ 長期署名に関する参照が JIS から ISO に変化されたことに伴う変更
  - 保健医療福祉分野 PKI 認証局　署名用証明書ポリシが改定されたことによる変更
  - 6.3 章の CAdES に関する規格について、ISO_14533-1：2022 に改定されたことに伴う修正
  - 6.4 章の XAdES に関する規格について、参照先を ETSI から ISO_14533-2：2021 に変更したことに伴う修正
  - Ver.2.0 における「付録 2：HL7 CDA 文書に対する XML 電子署名の付与」について、IHE の DSG に基づく実装が HL7 において主流になりつつあるため削除
- ES-XL の署名検証を行う際の注意点の追加
- 読みやすさを考えた構成の見直し
- 日本においては ArchiveTimestampV2 による継続的な検証を維持するが、ArchiveTimestampV3 を利用する場合の要件について「付録 2：CAdES-A で ArchiveTimestampV3 を使用する場合の要件」として追加
- V.er.2.0 における 6.4 章が ISO_14533-2：2021 の改定に伴って大幅な要素の変更があったため、これまでの長期署名を検証可能することを目的として「ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」までで示していた XAdES の要件を、「付録 3：ヘルスケア PKI を利用した医療文書に対する電子署名規格 2.0 での XAdES の要件」として追加

（ＪＡＨＩＳ標準　２３－ｘｘｘ）
２０２３年X月発行

ＪＡＨＩＳヘルスケア PKI を利用した医療文書に対する電子署名規格
Ver.3.0

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070