JAHIS 標準 07-005

Japanese Association of Healthcare Information Systems Industry

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

2008年3月

保健医療福祉情報システム工業会

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

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、「安全管理のガイドライン」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、今般、「JAHIS　HPKI 電子署名規格　V1.0」を策定することとし、ここに JAHIS 標準として公開するものである。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やその他の法、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、参照規格や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。

2008 年 3 月

保健医療福祉情報システム工業会
セキュリティ委員会

<< 告知事項 >>

本ガイドラインは関連団体の所属の有無に関わらず、ガイドライン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ガイドラインの準拠する旨を表現することは厳禁するものとします。

本ガイドラインならびに本ガイドラインに基づいたシステムの導入・運用についてあらゆる障害や損害について、本ガイドライン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ガイドライン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　目的と策定方針

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や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【2,3,4】を採用することとする。また、相互運用性向上のために長期署名フォーマットの利用方法を規定した JIS 規格【5,6】（本規格原案作成時は原案）に準拠する形で規格を作成する。

署名対象文書のフォーマットについては限定しないが、医療分野向け XML ドキュメント規格である HL7　CDA 文書【7】に対する署名付与方式については、実際の署名の付与例を付録にて明示する。

第２章　適用範囲

２.１ 対象となるシステム

電子署名機能、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、及び、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、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関係を図 2.1.1 に示す。図 2.1.1 の網掛けの部分が適用対象のプログラム、ライブラリで、それ以外は適用対象外となる。

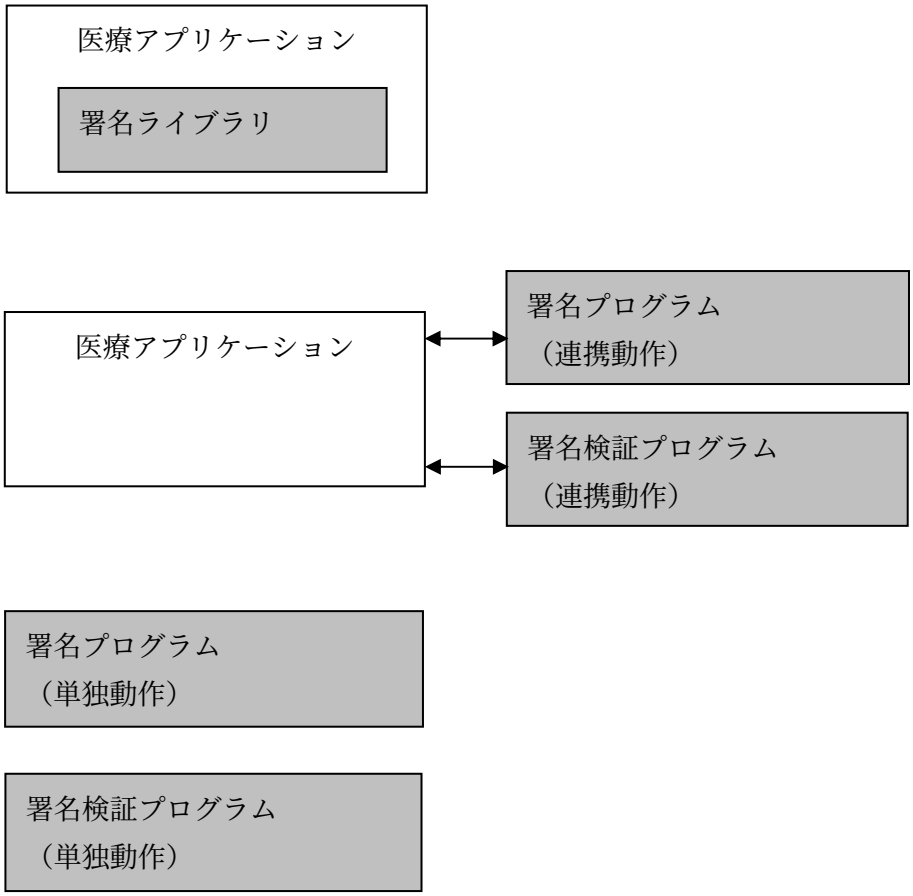

図 2.1.1 対象範囲

処理階層の例を図 2.1.2 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（署名ライブラリ及び電子署名専用プログラム、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【8】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 トークンやソフトウェアトークン等も利用できる。

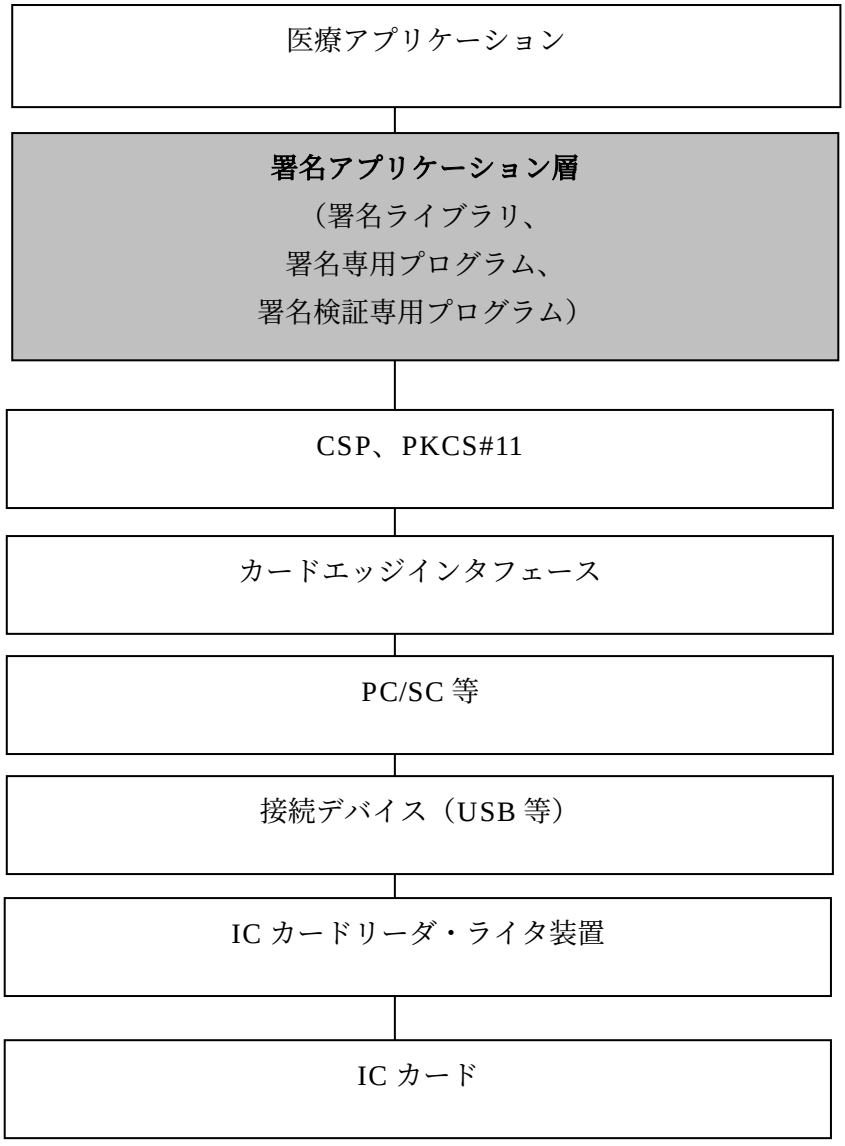

図 2.1.2 処理階層の例

　

２.２ 対象となるユースケース

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。

２.２.１ 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もしく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「安全管理のガイドライン」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。

２.２.２ 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

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」
http://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）
- 処方せん（医師）
- 調剤録（薬剤師）
- 病院日誌（病院）
- 各科診療日誌（病院）
- 処方せん（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、電子保存が認めれられている文書の一覧については、常に最新版の「安全管理のガイドライン」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. 「安全管理のガイドライン」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、電子署名の付与が望ましい。そのことは、「安全管理のガイドライン」にも記されている。

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。

２.２.３ 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」や「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。

２.２.４ 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）

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。

２.２.５ 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３章　本規格で規定する電子署名方式の概要

「安全管理のガイドライン」7.4 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」（2007 年 5 月：JAHIS 標準 07-001）の 7.4 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。

３.１ 電子署名の基本要件

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や 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 3.1.1 に署名と検証の概要を示す。

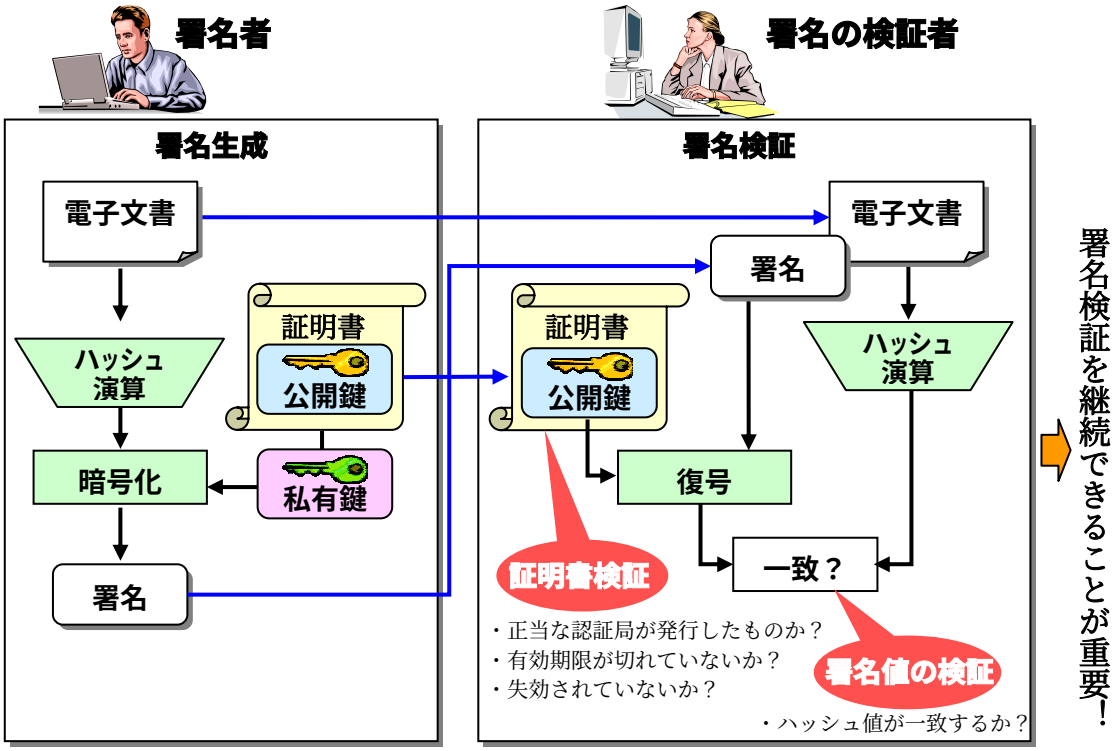

図 3.1.1 署名と署名検証

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 3.1.2 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。

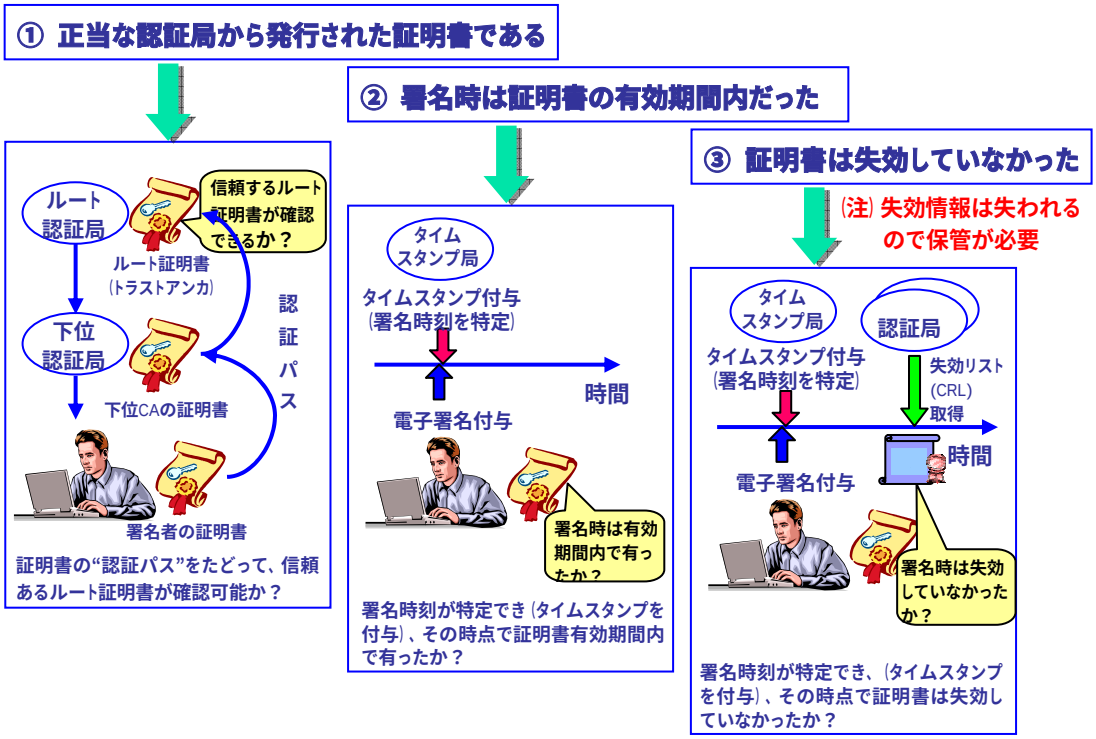

図 3.1.2 証明書検証の要素

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【2,3】や XAdES【4】など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出来るようにしておく

（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や署名値、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 3.1.3 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。

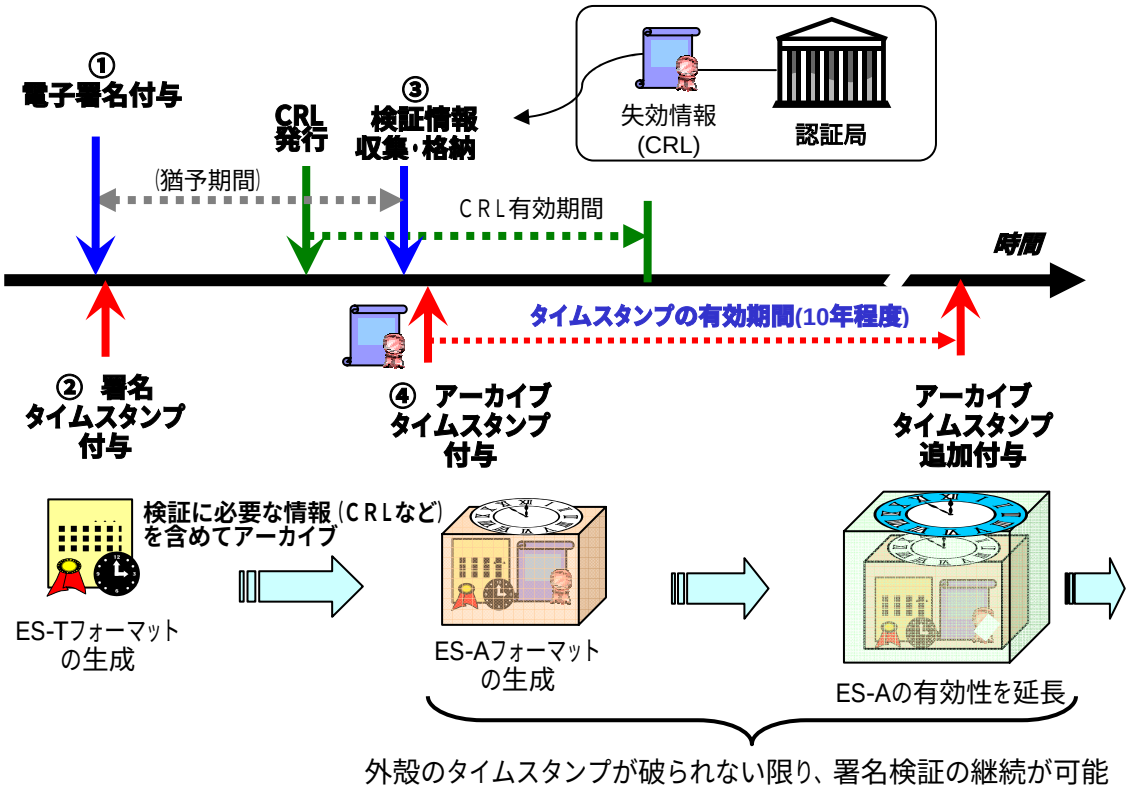

図 3.1.3 長期署名フォーマットによる署名延長

[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

３.２ 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や暗号アルゴリズムの脆弱化、認証局や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や省令、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や暗号アルゴリズムの脆弱性が発見されたり、万一、認証局や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 3.2.1 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や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、私有鍵をサーバや 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、「公開鍵証明書の有効期間は 5 年を越えないものとし、その私有鍵の使用は 2 年を越えないものとする。」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。

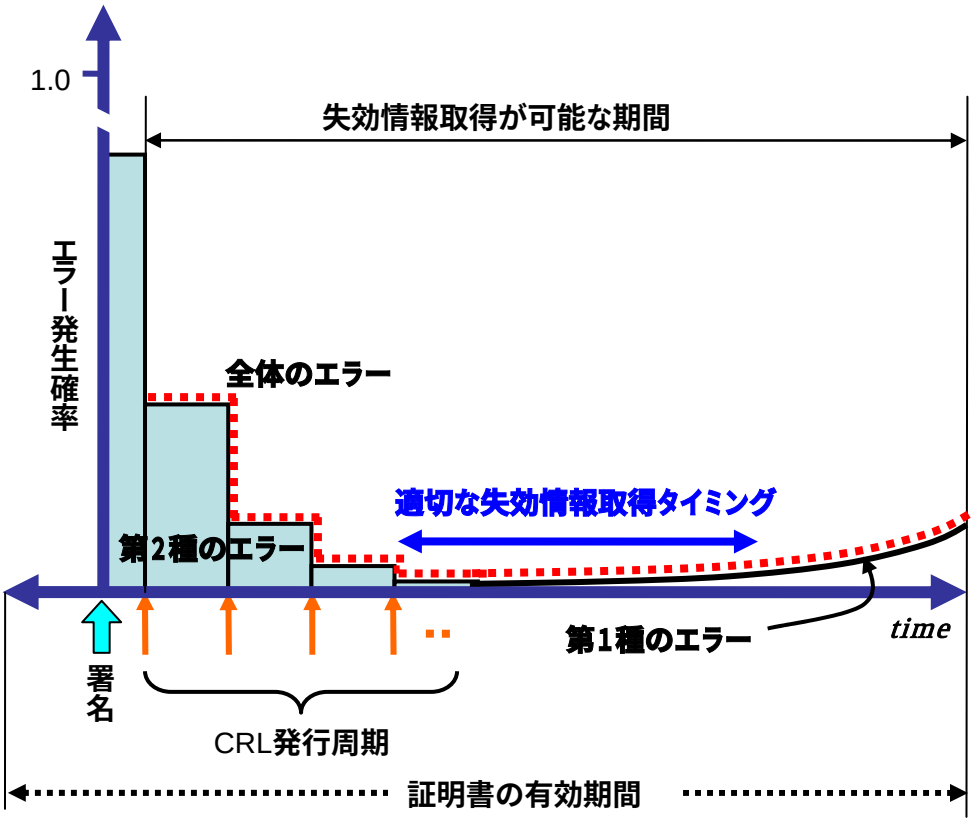

図 3.2.1 失効情報の取得のタイミングのイメージ

３.３ 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の形式には、図 3.3.1 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や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。

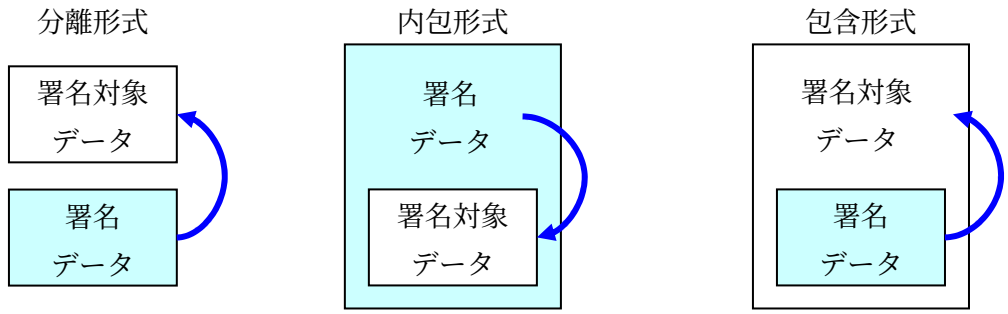

図 3.3.1 署名対象データと署名データの形式

３．４ 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 3.4.1 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、4 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二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。稟議書や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、文書フォーマットや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。

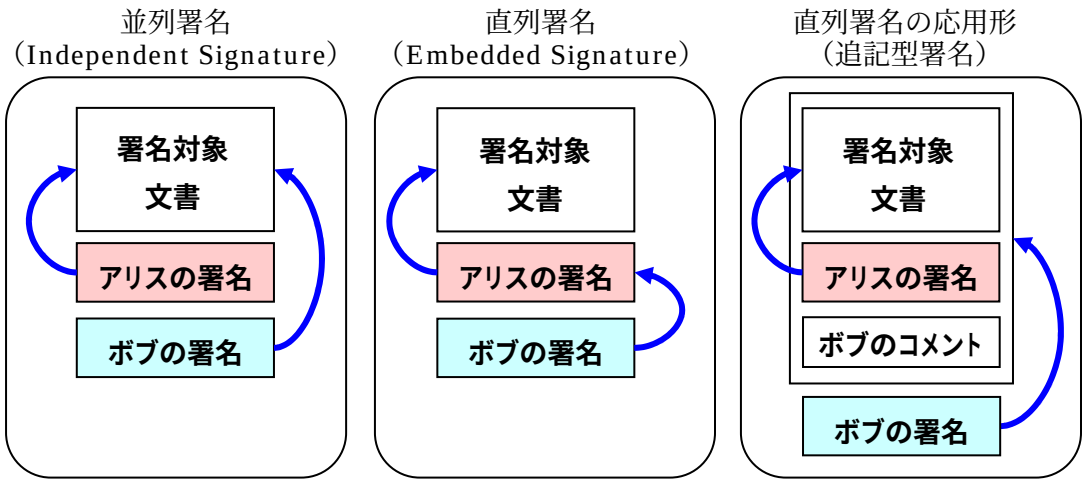

図 3.4.1 複数署名の種別

第４章　電子署名の規格

４.１ 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 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

・ES-X Long 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 署名データやタイムスタンプ、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 4.1.1 である。

これらの形式のうち、ES-C、ES-X Long 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-C、ES-X Long 単体での運用は対象外とする。また、ES 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。

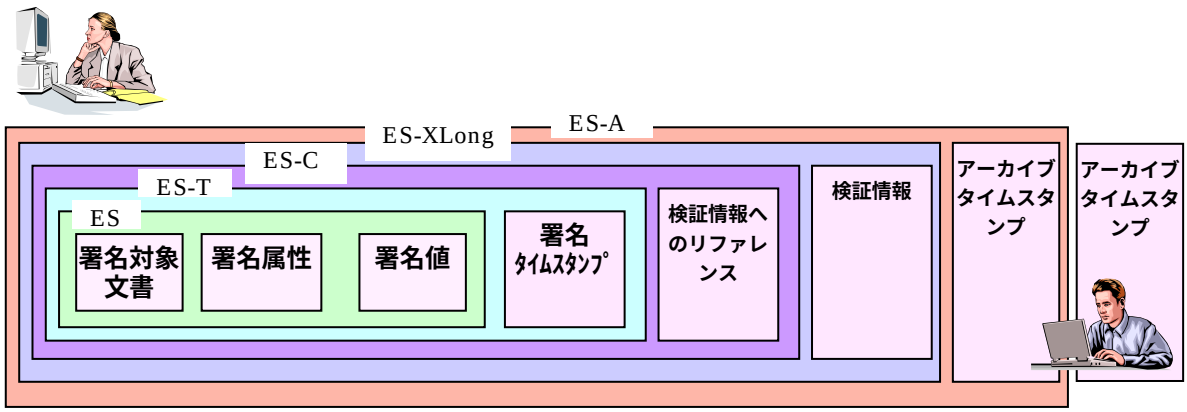

図 4.1.1 署名フォーマット各形式の関係

署名フォーマットの規格には CMS(Cryptographic Message Syntax)に基づく CAdES【2,3】と XML 署名に基づく XAdES【4】がある。署名対象となる文書フォーマットや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や選択可能な要素を定めたプロファイルを、CAdES については 4.3 節で、XAdES については 4.4 節で規定する。

４.２ 電子署名の検証（共通事項）

４.２.１ 参照する規格・資料

検証の各工程の詳細は、CAdES、XAdES の標準規格や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【9】を想定する。

４.２.２ ES の検証

４.２.２.１ ES の検証プロセス

ES 形式の検証プロセスを記述する。

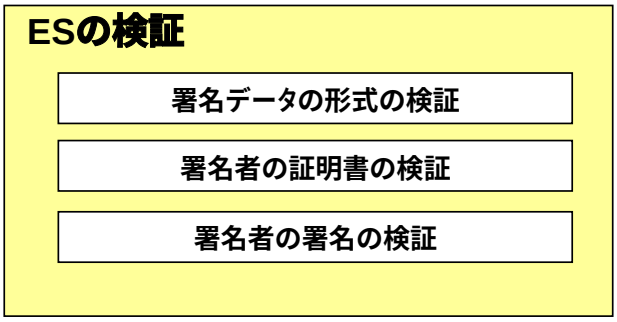

図 4.2.1 ES の検証プロセス

ES 形式の検証は図 4.2.1 で記述したプロセスで行う。プロセスや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) RFC3280 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 4.2.2.2 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

４.２.２.２ 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) RFC3280 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。

４．２．３ ES-T の検証

４．２．３．１ 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。

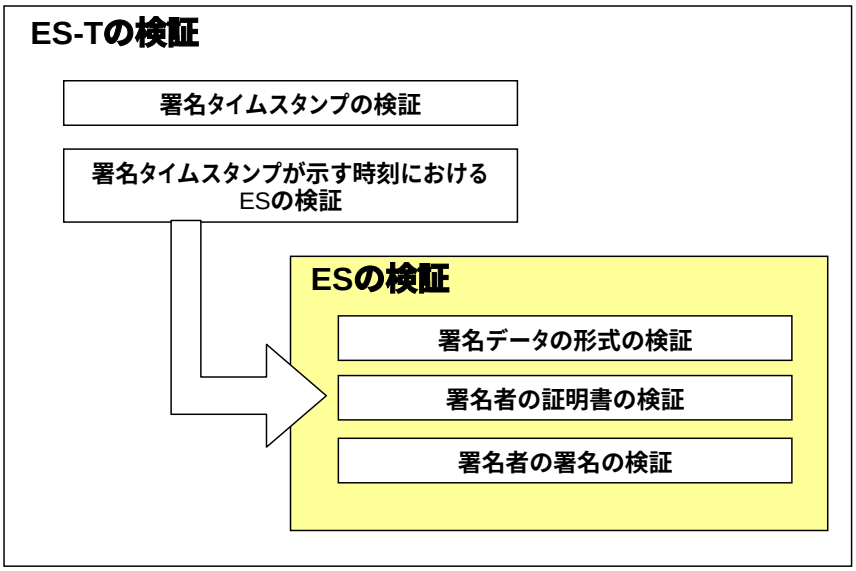

図 4.2.2 ES-T の検証プロセス

ES-T 形式の検証は図 4.2.2 で記述したプロセスで行う。プロセスや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 の検証

署名時刻に基づき ES 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 の検証

(2-2) ES の信頼点の正当性の確認

各プロセスの内容を 4.2.3.2 節で記述する。

４.２.３.２ 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 MessageImprint 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 の検証	(2-1) 署名時刻における ES の検証 署名タイムスタンプが示す時刻を想定して 4.2.2 節「ES 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 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や、認証局や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。

４．２．４ ES-A の検証

４．２．４．１ 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。

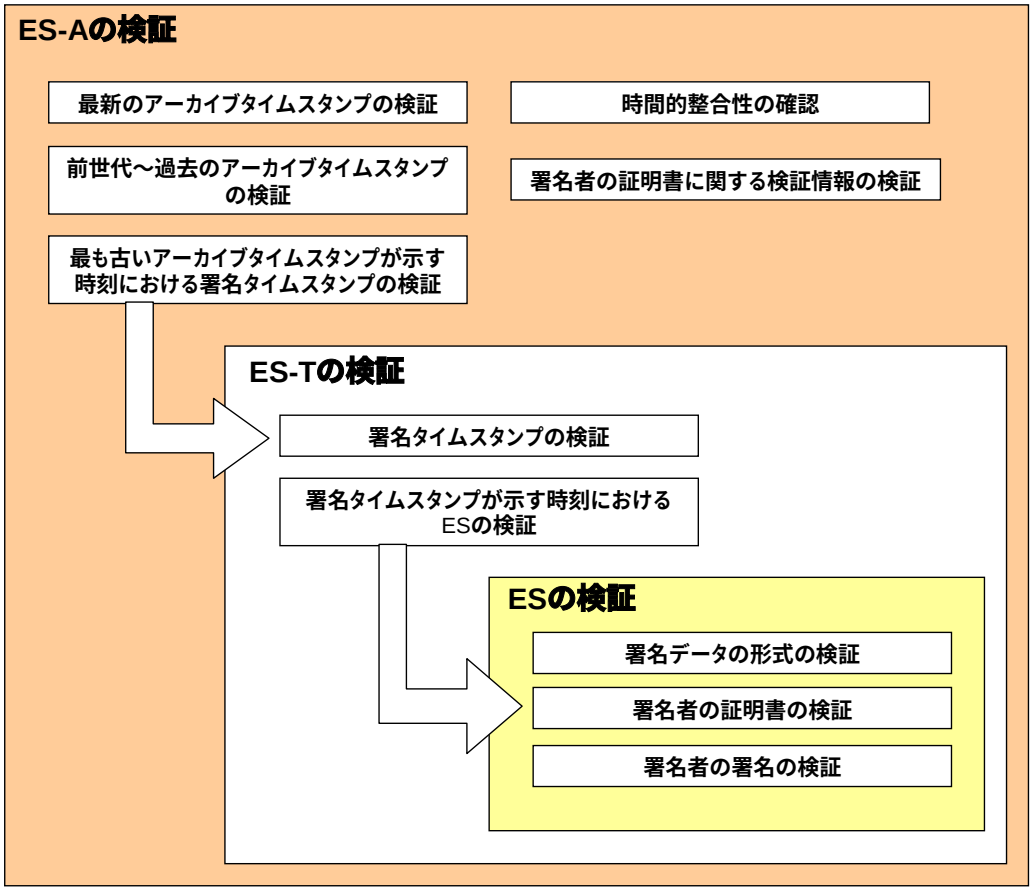

図 4.2.3 ES-A の検証プロセス

ES-A 形式の検証は図 4.2.3 で記述したプロセスで行う。プロセスや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 の検証

署名時刻における ES の有効性を検証する。

(5-1) 署名時刻における ES の検証

(5-2) ES 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 4.2.4.2 節で記述する。

４.２.４.２ 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 MessageImprint 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 4.2.4 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	(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。

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。	(3-4) 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 4.2.3.2 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 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 4.2.2 節「ES の検証」を実施する。
	(5-2) ES 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。

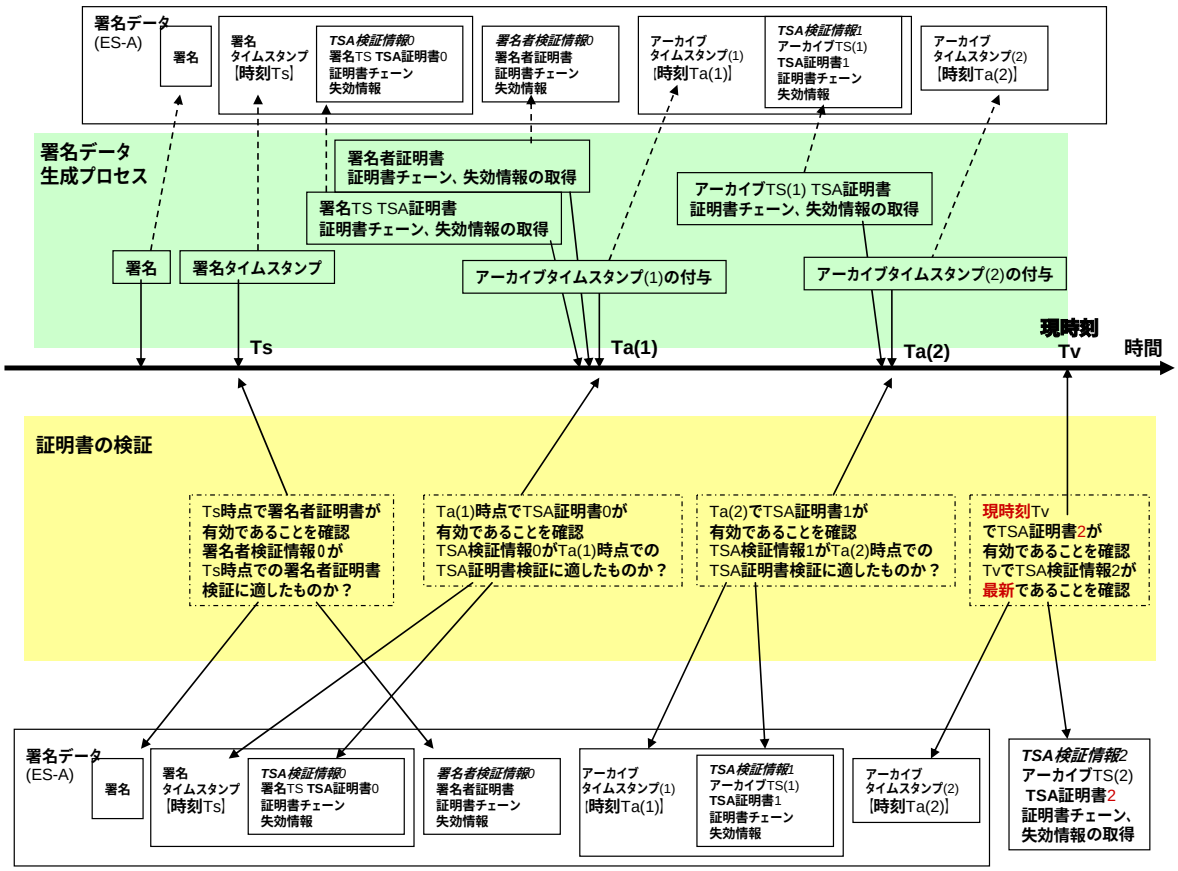

図 4.2.4 ES-A の検証に用いる時刻情報（第二世代アーカイブタイムスタンプの場合）

４.３ CAdES に関する規格

CAdES の生成及び検証に関する要件を示す。
4.3.1 節にこの規格で参照する引用規格を示し、4.3.2 節にこの規格で定義するプロファイルの概要を、4.3.3 節に CAdES の構造を示す。4.3.4～4.3.6 節にプロファイルの要件を示し、4.3.7 節に各構成要素の概要を示す。
なお、本章の各図表及び用語の説明は、ECOM（次世代電子商取引推進協議会）作成の長期署名に関する JIS 原案「CMS 利用電子署名 （CAdES） の長期署名プロファイル」からの抜粋に加筆したものである。

４.３.１ 引用規格

・CAdES 仕様

ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES)

注記　http://pda.etsi.org/pda/queryform.asp から入手可能。

・CMS 仕様

IETF RFC 3852 Cryptographic Message Syntax

注記　http://www.ietf.org/rfc.html から入手可能。

４.３.２ 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出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 4.3.1 に示す。

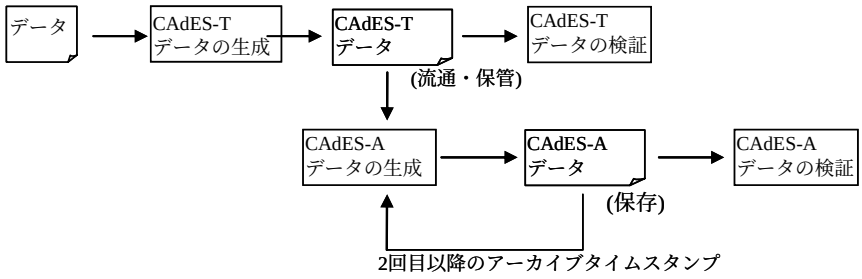

図 4.3.1 CAdES-T データと CAdES-A データの関係

４.３.３ 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 4.3.2.の破線部分）。図 4.3.3 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 4.3.4）。

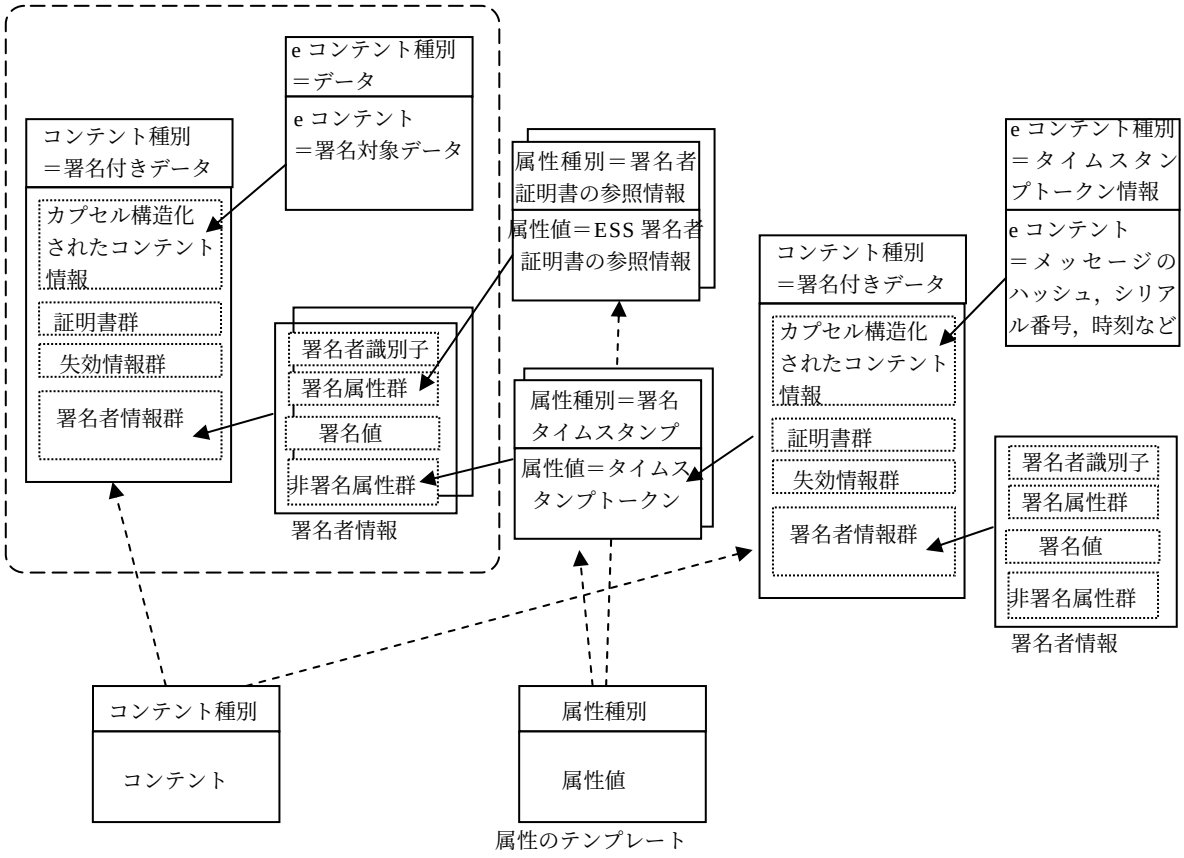

図 4.3.2 CAdES のデータ構造

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 4.3.3 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 4.3.4 署名者情報の構造

４.３.４ 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、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。

４.３.５ CAdES-T に関する要件

表 4.3.1 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 4.3.2 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	必須	

署名者情報群		
・・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 4.3.3 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	
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	
SignatureAlgorithm 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 4.3.4 及び表 4.3.5 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 4.3.4 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	
SignatgureAlgorithmIdentifier 署名ポリシ識別子	要別途規定	
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	
ContentHint 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	
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 4.3.5 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	

４.３.６ 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 4.3.6 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。

表 4.3.6 追加非署名属性

要素	要求レベル	条件/値
CompleteCertificateRefs 完全な証明書参照情報群	必須 （検証処理に対しては任意選択）	
CompleteRevocationRefs 完全な失効参照情報群	必須 （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	要別途規定	
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	

[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。

・・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	
・・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	要別途規定	
・・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	
・・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
・・ArchiveTimestamp アーカイブタイムスタンプ id-aa-27	任意選択	RFC3161 で定義されるタイムスタンプ 4
・・タイムマークなどその他の方式	禁止	

[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。

４.３.７ 各構成要素の概要

４.３.７.１ 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。

４.３.７.２ 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。

４.３.７.３ 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。

４.３.７.４ 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(竄)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。

４.３.７.５ 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。
・SignatureTimestamp 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、署名値に付されるタイムスタンプ。
・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。
・CompleteCertificateRefs 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。
・CompleteRevocationRefs 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。
a)証明書群
・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

・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。
・ArchiveTimestamp アーカイブタイムスタンプ
改ざん(竄)を検知可能にするために、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-48 及び id-aa-27 はそれぞれ、ETSI TS 101 733 V1.7.3 及び ETSI TS 101 733 V1.2.2 で定義されている。

４.４ XAdES に関する規格

XAdES の生成及び検証に関する要件を示す。
4.4.1 節にこの規格で参照する引用規格を示し、4.4.2 節にこの規格で定義するプロファイルの概要を、4.4.3 節に XAdES の構造を示す。4.4.4～4.4.6 節にプロファイルの用件を示し、4.4.7 節に各構成要素の概要を示す。なお、本章の各図表及び用語の説明は、ECOM（次世代電子商取引推進協議会）作成の長期署名に関する JIS 原案「XML 署名利用電子署名（XAdES）の長期署名プロファイル」からの抜粋に加筆したものである。

４.４.１ 引用規格

・XAdES 仕様

ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

注記　http://pda.etsi.org/pda/queryform.asp から入手可能。

・XML 署名仕様

XML-Signature Syntax and Processing W3C Recommendation 12 February 2002

注記　http://www.w3.org/TR/xmldsig-core/から入手可能。

４.４.２ 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(竄)検出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、次の二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-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 データと XAdES-A データの関係を図 4.4.1 に示す。

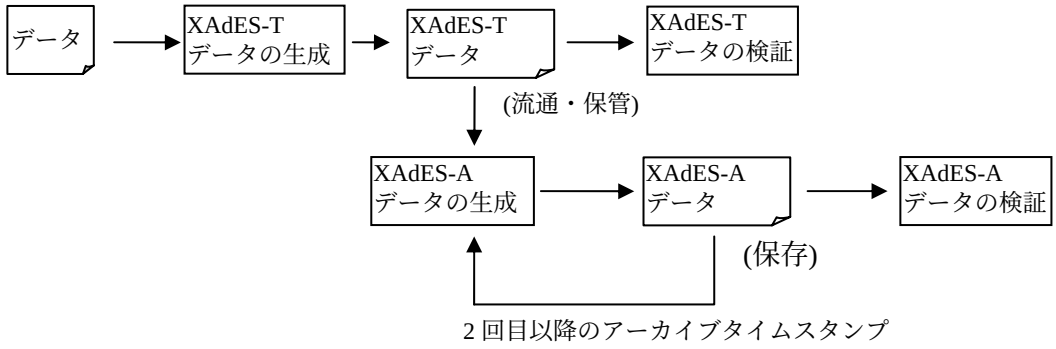

図 4.4.1 XAdES-T データと XAdES-A データとの関係

４.４.３ 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 4.4.2 に XAdES の構造の一例を示す。XML 署名の定義に従って、"署名"要素が最上位要素となる図 4.4.3 の基本構造を持つ。図 4.4.4 に"オブジェクト"要素の構造を示す。また、"署名対象プロパティ"要素の構造を図 4.4.5 に、"非署名対象プロパティ"要素の構造を図 4.4.6 に示す。

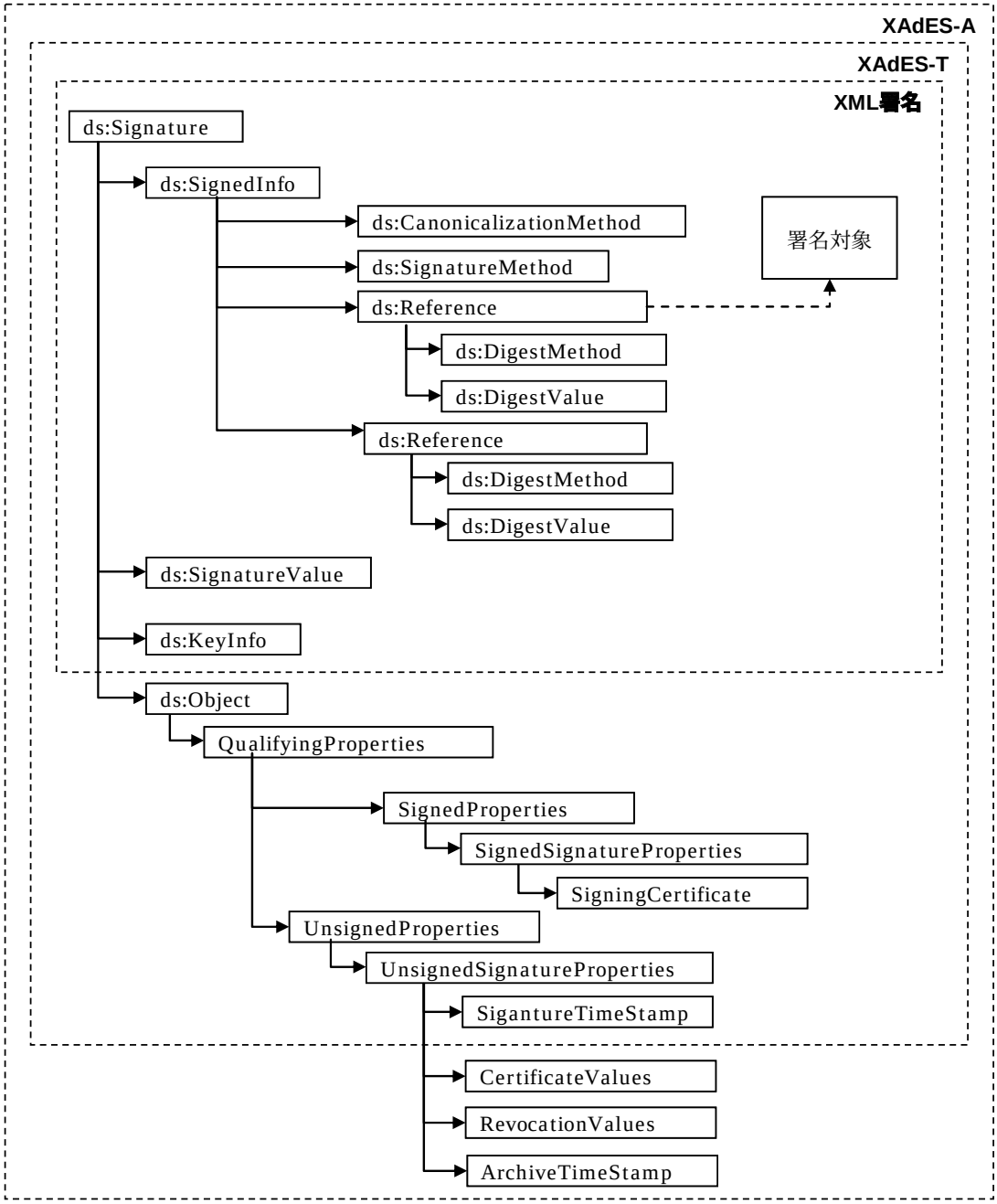

図 4.4.2 XAdES 構造の一例

署名	署名に関する情報	正規化方式	
		署名方式	
		コンテントへの参照情報	変換処理
			ダイジェスト方式
			ダイジェスト値
	署名値		
	鍵情報		
	オブジェクト		

図 4.4.3 XAdES データの基本構造

オブジェクト	署名を修飾するプロパティ	署名対象プロパティ
		非署名対象プロパティ
	署名を修飾するプロパティを特定する参照情報	

図 4.4.4 オブジェクトの構造

署名対象プロパティ	署名対象の署名プロパティ	署名時刻
		署名者証明書
		署名ポリシ識別子
		署名生成場所
		署名者の肩書き
	署名対象データオブジェクトのプロパティ	データオブジェクト形式
		コミットメント種別表示
		全データオブジェクト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

図 4.4.5 署名対象プロパティ

<table>
<tr><td rowspan="20">非署名対象プロパティ</td><td rowspan="19">非署名対象の署名プロパティ</td><td colspan="2">カウンタ署名</td></tr>
<tr><td rowspan="2">署名時刻を確定する情報</td><td>署名タイムスタンプ</td></tr>
<tr><td>タイムマークなどその他の方式</td></tr>
<tr><td colspan="2">全証明書参照情報群</td></tr>
<tr><td rowspan="3">全失効情報参照情報群</td><td>CRL 形式の失効情報参照情報</td></tr>
<tr><td>OCSP 形式の失効情報参照情報</td></tr>
<tr><td>他の失効情報参照情報</td></tr>
<tr><td colspan="2">属性証明書参照情報群</td></tr>
<tr><td colspan="2">属性失効情報参照情報群</td></tr>
<tr><td colspan="2">署名及び参照情報に対するタイムスタンプ</td></tr>
<tr><td colspan="2">参照情報に対するタイムスタンプ</td></tr>
<tr><td rowspan="3">証明書群</td><td>カプセル構造化された証明書</td></tr>
<tr><td>他の証明書</td></tr>
<tr><td>CA 等による証明書の保管</td></tr>
<tr><td rowspan="4">失効情報群</td><td>CRL による失効情報群</td></tr>
<tr><td>OCSP による失効情報群</td></tr>
<tr><td>他の失効情報群</td></tr>
<tr><td>CA 等による失効情報の保管</td></tr>
<tr><td colspan="2">属性証明書群</td></tr>
<tr><td colspan="2">属性失効情報群</td></tr>
<tr><td rowspan="2">改ざん検知を可能とする情報</td><td>アーカイブタイムスタンプ</td></tr>
<tr><td>タイムマークなどその他の方式</td></tr>
<tr><td colspan="2">異なる版の非署名対象の署名プロパティ</td></tr>
<tr><td colspan="3">非署名のデータオブジェクトのプロパティ</td></tr>
</table>

図 4.4.6 非署名対象プロパティ

４.４.４ 要求レベルの表現法

この規格では、XAdES-T 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、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。

４．４．５ XAdES-T に関する要件

表 4.4.1～表 4.4.4 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 4.4.1 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	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 4.4.3）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 4.4.2 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 4.4.3 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 4.4.1）のどちらか一方が必要である。

表 4.4.4 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5
・・・・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	

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。

４．４．６ 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 4.4.5 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 4.4.5 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	要別途規定	
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	要別途規定	

・・(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	要別途規定	
・・(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	
(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	任意選択	
・・・・*not distributed case（非分離型）*	必須	RFC3161 で定義されるタイムスタンプ6
・・・・*distributed case（分離型）*	要別途規定	
・・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。		

４.４.７ 各構成要素の概要

４.４.７.１ 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。

・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

6 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。

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を格納する。

・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。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。

４.４.７.２ オブジェクト要素

・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(4.4.7.1)で参照される。

・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。

・署名を修飾するプロパティを特定する参照情報

署名に必要な追加のプロパティを特定する参照情報。

４.４.７.３ 署名対象プロパティ要素

・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。

・署名者証明書

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

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

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。

・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。

４.４.７.４ 非名対象プロパティ要素

・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)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。

　

４.４.７.５ 非署名対象の署名プロパティ要素

・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（竄）検知を可能とする情報

改ざん(竄)を検知可能にするために、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 XAdES で定義された署名対象とはならない署名プロパティ。

付録１：厚生労働省 HPKI の CP

保健医療福祉分野 PKI 認証局 証明書ポリシ　1.1 版　（平成１８年３月）
http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8a.pdf

付録２： HL7　CDA 文書に対する XML 電子署名の付与

1　概要

医療関連情報の電子化文書規格である HL7 CDA 文書（以下、CDA 文書）に電子署名を行う際の規格として CDA 文書電子署名規格【7】が存在する。ここでは、本規格で規定される電子署名と CDA 電子署名規格との整合性について記述する。なお、CDA 電子署名規格では、XML 署名、XAdES のそれぞれの現時点での最新版である W3C、ETSI TS 101 903 V1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES)【4】を参照するものとして説明する。

2　XAdES-T の適用について

CDA 文書電子署名規格では、XAdES-T について XAdES の標準仕様を参照しており本規格の内容をそのまま適用することができる。

付録３：参照規格

【1】「保健医療福祉分野 PKI 認証局　証明書ポリシ」、厚生労働省、2005

【2】CAdES

（1） "CMS Advanced Electronic Signatures (CAdES)," ETSI TS 101 733

（2） "Electronic Signature and Infrastructure (ESI); ASN.1 format for signature policies." ETSI TR 101 272 V1.1.1 (2003-12),
及び"Electronic Signature," IETF RFC3125

（3） "Cryptographic Message Syntax," IETF RFC3852,
及び"Enhanced Security Services," IETF RFC2634

【3】"Electronic signature formats for long term electronic signature," IETF RFC3126

【4】XAdES

（1） "XML Advanced Electronic Signature (XAdES)," ETSI TS 101 903 及び "http://www.w3.org/TR/XAdES/", W3C Note

（2） "XML format for signature policies," ETSI TR102 038 V1.1.1 (2002-04)
及び"Electronic Signature Policies," IETF RFC3125

（3） "XML-Signature Syntax and Processing," W3C Recommendation (Feb.,2002)及び IETF RFC3275

【5】「暗号メッセージ構文を利用した電子署名（CAdES）の長期署名プロファイルに関する要求事項」ECOM、2006

【6】「拡張可能なマーク付け言語を利用した電子署名（XAdES）の長期署名プロファイルに関する要求事項」、ECOM、2006

【7】「CDA 文書電子署名規格」、日本 HL7 協会

【8】FIPS PUB 140-2 "Security Requirements for Cryptographic Modules",National Institute of Standard Technology,May 25, 2001

【9】"Internet X.509 Public Key Infrastructure Time-Stamp Protocol," IETF RFC3161

付録４：単語及び略語

【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

プログラムや装置や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。

（「医療情報機器の安全管理に関するガイドライン　第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　証明書ポリシ（1.1 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　証明書ポリシ（1.1 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）や、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　証明書ポリシ（1.1 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　証明書ポリシ（1.1 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。
（「医療情報機器の安全管理に関するガイドライン　第２版」厚生労働省）
・相互運用性
　異なったアプリケーションやシステム、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したり、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　証明書ポリシ（1.1 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　証明書ポリシ（1.1 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　証明書ポリシ（1.1 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。
（「医療情報機器の安全管理に関するガイドライン　第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

CAdES や XAdES 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 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や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

・ES-Xlong

ES-C フォーマットに対し、各証明書および CRL を追加し、署名や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-Xlong の署名データや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 (HealthCare PKI)

保健医療福祉分野での公開鍵基盤。

【I】

・ISO(International Organization for Standardization)

電気分野を除く工業分野の国際的な標準規格を策定するための団体。

【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　証明書ポリシ（1.1 版)」(厚生労働省))

【P】

・PDF(Portable Document Format)

Adobe Systems 社によるコンピュータ上のドキュメントを扱うためのファイルフォーマットの１つ。

・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　証明書ポリシ（1.1 版）」（厚生労働省））

・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。

・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。

【T】

・TSA(Time Stamp Authority)

タイムスタンプ局のこと。時刻の信頼性や信頼できる第三者機関であることが求められるが、（財）日本データ通信協会によるタイムスタンプ認定制度がある。

【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)

文書やデータの意味や構造を記述するためのマークアップ言語の一つ。

付録５：作成者名簿

作成者（五十音順）

岡田	康	東芝住電医療情報システムズ㈱
岸田	幸博	キッセイコムテック㈱
熊野	顕生	富士通㈱
小西	由貴範	日本システック㈱
後藤	淳	日本電気㈱
酒井	雅啓	日本電気㈱
佐藤	雅史	セコム㈱
佐野	聡	松下電器産業㈱
瀧	勝也	三菱電機ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑｽﾞ㈱
竹田	忠雄	㈱NTTPC ｺﾐｭﾆｹｰｼｮﾝｽﾞ
長嶺	俊二	日本電気㈱
西田	慎一郎	㈱島津製作所
西山	晃	セコム㈱
長谷川	武史	日本電気㈱
長谷川	英重	JAHIS
原嶋	茂夫	横河電機㈱
松本	義和	サイバートラスト㈱
宮崎	一哉	三菱電機㈱
茗原	秀幸	三菱電機㈱

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

（JAHIS 標準 07-005）

2008 年 3 月発行

～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

～

発行元 保健医療福祉システム工業会

〒105-0001 東京都港区虎ノ門 1 丁目 19－9

（虎ノ門 TB ビル 6F）

電話　03-3506-8010　　FAX　03-3506-8070