JAHIS

ＪＡＨＩＳ標準　１７－００４

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 PAdES 編 Ver.1.0

２０１７年７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

HPKI 電子署名規格作成 WG

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PAdES編Ver.1.0

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た。
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JAHIS標準として本書を策定した。本書は分冊という位置づけであり、プロファイル以外の部分については、「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.1.1」を参照されたい。
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。

２０１７年７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、規格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格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、本規格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格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

1. 適用範囲

目的、策定方針、対象となるシステム、対象となるユースケースは「JAHIS ヘルスケア PKI を利用し医療文書に対する電子署名規格」に準ずる。

2. 引用規格・引用文献

【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】PAdES

（1）“Document management — Portable document format —Part 2 PDF 2.0”, ISO 32000-2

（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–

【3】「CDA 文書電子署名規格」、日本 HL7 協会

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

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

【6】"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF RFC5280

3. 用語の定義

下記以外の用語の定義は「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」に準ずる。

【P】

・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。

4. 記号および略語

下記以外の記号および略記は「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」に準ずる。

DSS	Document Security Store
VRI	Validation-related information

5. 本規格で規定する電子署名方式の概要

「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」に準ずる。なお、署名データの形式については、PDF 電子署名規格では包含形式（Enveloped 型）に限定される。

6. 電子署名の規格

電子署名の生成と検証は「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」の電子署名の生成と検証（共通事項）に準ずる。

6.1. PDF 電子署名(PAdES)に関する生成及び検証の要件

PAdES の生成及び検証に関する要件を示す。

6.1.1. 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、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 データの関係を図 6.1.1 に示す。

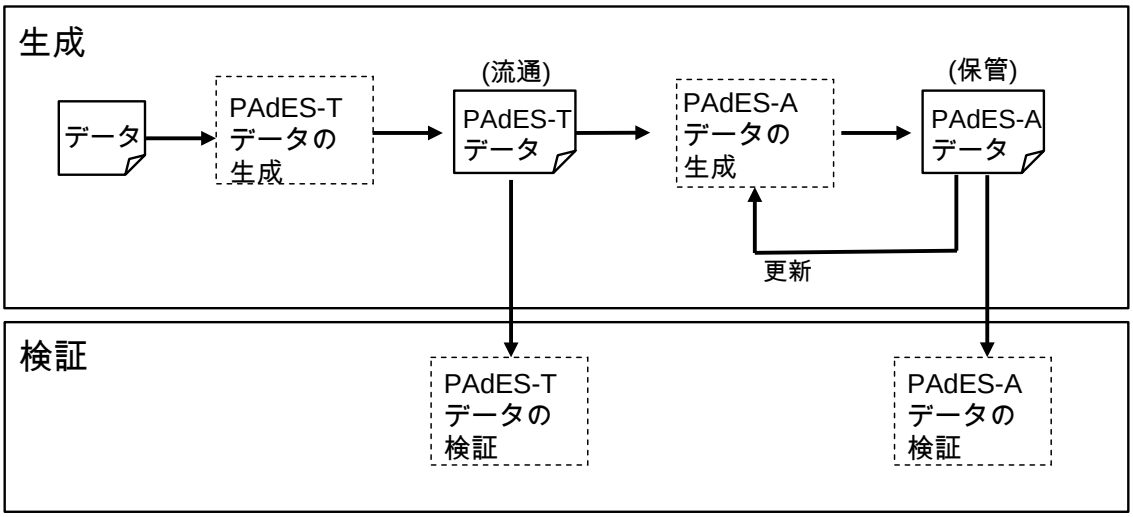

図 6.1.1 PAdES-T データと PAdES-A データの関係

6.1.2. 要件レベルの表現法

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、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。

6.1.3. 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(SignatureTimestap)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 6.1.2 に示す。

図 6.1.2 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 6.1.1 に示す。

表 6.1.1 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 6.3.2 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	

[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 6.1.2 から表 6.1.5 に示す。

表 6.1.2 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 6.3.3 を参照

表 6.1.3 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]
- v2AttrCert	禁止
- other	要別途規定
RevocationInfoChoices (crls)	任意選択
- crl	任意選択
- other	要別途規定
SignerInfos	必須 [b]
- signerInfo	必須

[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。.
[b] SignerInfo は一つのみ。複数あってはならない。

表 6.1.4 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
- subjectIdentifier	要別途規定
DigestAlgorithmIdentifier	必須
SignedAttributes	必須
SignatureAlgorithmIdentifier	必須
SignatureValue	必須
UnsignedAttributes	要別途規定

表 6.1.5 及び表 6.1.6 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 6.1.5 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]
CommitmentType	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
signer-attributes	要別途規定[c]
SignerLocation	任意選択[d]

[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。
[b] ISO 32000-2 の 12.8.3.4.4 節を参照のこと。
[c] ISO 32000-2 の 12.8.3.4.3 節を参照のこと。
[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 6.1.6 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
LongTerm Validation Data	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 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。

6.1.4. 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、署名データや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 6.1.3 に示す。

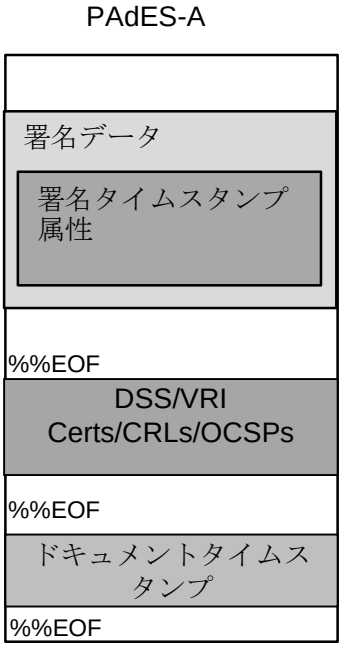

図 6.1.3 PAdES-A プロファイルの PDF データ構造のイメージ

PAdES-T に対して表 6.1.7 で示す要素を追加する。

表 6.1.7 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 6.1.8 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 6.1.8 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	

[a] RFC 3161 のタイムスタンプを使用する。
[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。

署名データやタイムスタンプ、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や失効情報を 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)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。

6.1.5. 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。

付録―１．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１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（「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」5.1 節参照）として機能する。

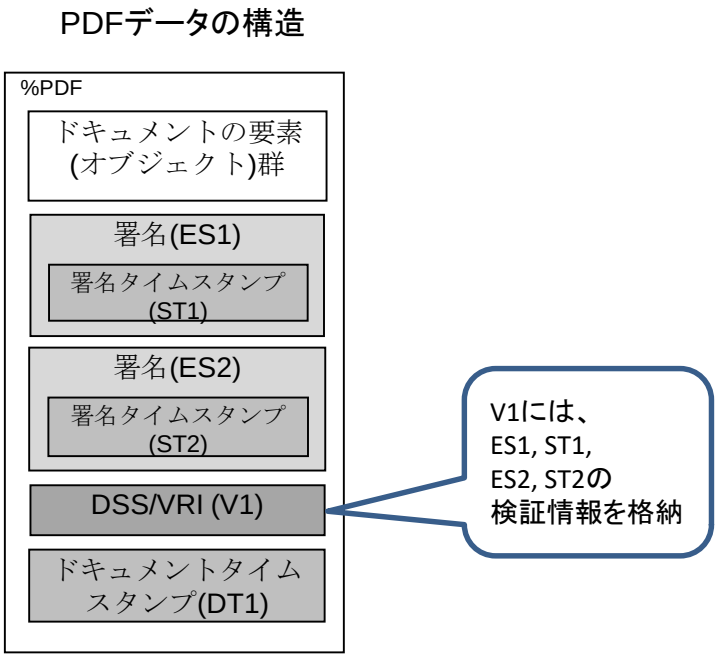

図１ 複数署名の例１

図 2 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。

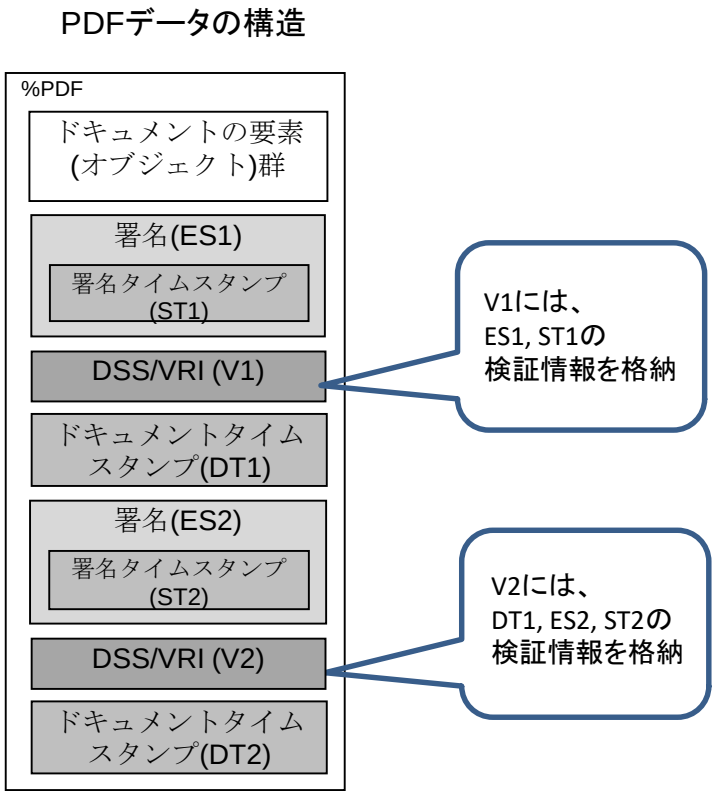

図 2 複数署名の例 2

付録―２．作成者名簿

作成者（社名五十音順）

下野　兼揮	(株)グッドマン
佐藤　雅史	セコム(株)
西山　晃	セコム(株)
佐藤　恵一	日本光電工業(株)
別府　嗣信	日本光電工業(株)
山岡　弘明	富士通(株)
長谷川　英重	(一社)保健医療福祉情報システム工業会（特別委員）
平田　泰三	(一社)保健医療福祉情報システム工業会（特別委員）
宮崎　一哉	三菱電機(株)
茗原　秀幸	三菱電機(株)
瀧　勝也	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
2017/7/11	Ver. 1.0	初版

（ＪＡＨＩＳ標準　１７－００４）
２０１７年7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 PAdES 編
Ver.1.0

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