CDA 文書電子署名規格

ver. 1.02

日本 HL7 協会

改訂履歴

版	改訂日附	重要度	改訂箇所	内容
1.01	2006 年 3 月 24 日	-	-	初版
1.02	2006 年 5 月 12 日	低	全体 まえがき ３．１ ４	ページ番号付け替え ５行目　有用よ　→　有用と １０行目　行い際　→　行う際 １１行目　もとめ　→　求め RFC3275 に規定される XML 文書～データ。　→ XML 文書～データで RFC3275 に規定されている。 １行目　対象にては　→　対象は

目次

まえがき

昨今、患者あるいは家族から診療の把握、あるいはセカンドオピニオンを得たいという要求が高まってきている。また、医療・介護機関の機能分化と施設間連携を高度化し、医療・介護の率向上が求められている。このような要求を満たすためには、医療・介護機関間および医療・介護機関と患者・利用者の間で流通する情報を電子化し、情報の密度や可用性を飛躍的に向上させることが有用と考えられている。そしてこのような電子化文書の規格として HL7 CDA が存在する。

医療・介護は様々な法律規則に則って行われるもので、さまざまな理由で作成される文書には作成者・責任者の署名または記名・押印が求められるものが存在する。電子化文書では電子署名法によって電子署名で署名または記名・押印に代えることができるが、本規格は CDA 文書に電子署名を行う際の規格を記述するものである。また診療文書には添付情報が存在するものが数多くあり、電子署名の対象情報にこれらの添付情報を含めることが求められることも多い。そのため、本規格には外部参照情報も電子署名の対象とする場合についても規定する。

なお、本規格の目標は、以下のとおりである。

(1) 患者ケア情報の提供に重点をおく
(2) システムを低コストで実現できるようにする
(3) 記述された情報は、再利用の可能性があるものとする
(4) さまざまなドキュメント生成アプリケーションで互換性をもつようにする
(5) その文書の転送方式や格納のメカニズムとは独立である
(6) すみやかに設計書を提供する
(7) オープンな標準を使う

1. 適用

本規格は、さまざまな目的で作成される CDA 文書に電子署名を付与する際に適用する。電子署名が必要か否かは本規格では規定しない。

2. 引用規格

本規格は、以下の規格を引用する。日付の付いた引用規格については、その日付以降に発行された修正票または改訂版は参照しない。しかしながら、本仕様書を使用する場合は、各規格の最新版を調べて必要に応じて適用するよう努めなければならない。

RFC3275　XML-Signature Syntax and Processing

保健医療福祉分野 PKI 認証局 証明書ポリシ(厚生労働省　平成 17 年)

ISO TS17090-1:2002 Health informatics -- Public key infrastructure -- Part 1: Framework and overview

ISO/TS 17090-2:2002 Health informatics -- Public key infrastructure -- Part 2: Certificate profile

ISO/TS 17090-3:2002 Health informatics -- Public key infrastructure -- Part 3: Policy management of certification authority

「タイムスタンプビジネスに係る指針―ネットワークの安心な利用と電子データの安全な長期保存のために―」（総務省、平成 16 年）

RFC3161　Internet X.509 Public Key Infrastructure Time-Stamp Protocol

XML Advanced Electronic Signatures (XAdES), (W3C 2003)

患者診療情報提供書規格　V1.00 （日本 HL7 協会　2006)

CDA 文書暗号化規格　V1.00 （日本 HL7 協会　2006)

3. 用語と定義

3.1　XML 電子署名

XML 文書に添付して文書作成者の身元を証明し、またその文書が改竄されていないことを保証するデータで RFC3275 に規定されている。XML 文書全体ではなくその一部にだけ署名を付けたり、また XML 文書の中に署名を含めたりといったことができる。

3.2　タイムスタンプサービス

データがある時刻に存在していたことを証明するサービス。データの作成者はタイムスタンプサービスを提供している第三者機関に依頼し、データの内容と現在時刻から作られたハッシュ値を用いるなどして電子署名を発行してもらう。データの受信者はその署

名を確認することで、記された時刻にそのデータが存在していたことと、それ以後データが改ざんされていないことを確認することができる。

3.3 HPKI

ISO TS17090 に規定された医師等の資格を記述することができる保健医療福祉分野の X509 電子証明書の規格。日本では、厚生労働省が「保健医療福祉分野 PKI 認証局 証明書ポリシ」として署名用 HPKI 電子証明書のポリシを定めている。

4. 電子署名・タイムスタンプ

電子署名・タイムスタンプの対象は、CDA 文書の本文ファイルについてのみとする。CDA 文書から参照される外部参照ファイルに関しては直接の署名対象とはしない。これらの外部参照ファイルに改竄のないことを証明し、参照したことに関する責任の所在を明らかにするために、CDA 文書の本文ファイルへの署名の効果を及ぼしたい場合は、本文ファイルの参照ポイントを記載する部分に参照ポイントを示す URI のほかに、対象外部参照ファイルのハッシュ値およびそのハッシュを計算したハッシュ関数の識別子を記載する。ハッシュ値およびハッシュ関数の識別子は HL7 ver.3 のデータタイプ ED を用いて記載する。したがってとりうるハッシュ関数は SHA-1 および SHA-256 に限定される。実際の記法は CDA Release 1 に準拠した CDA 文書の場合は本規格の付属書 A を参照すること。CDA Release 2 に準拠した文書の場合は referrence によって示し、ExternalAct、 ExternalDocument、ExternalObservation、および External Procedure においては text: ED を必須とする。

4.1 電子署名タイムスタンプの形式

電子署名タイムスタンプの形式については、RFC3275 に規定される形式の中で、Enveloping signature を使用する。多重署名を許容可能とする。またタイムスタンプが要求される場合は W3C の XAdES-T 形式で記述される。長期署名を行う場合は XAdES の関連規格に基づいて記述される。

４.2　電子署名

法律・規則で定められた署名または記名・押印に代えて電子署名を行い場合は電子署名法および関連規則に準拠した電子署名を行う。認定特定認定事業者の発行する署名用公開鍵証明書、公的個人認証サービスの公開鍵証明書および厚生労働省 HPKI 認証局専門家会議の認める HPKI 認証局の発行する署名用公開鍵証明書を用いる。署名の付与および検証は RFC3275 従う。ただし Enveloping Signature を用いるものとする。

HPKI 認証局の発行する署名用公開鍵証明書を用いる場合は Subject Directory Attributes の HcRole Attribute を検証時に確認する必要がある。

公的個人認証サービスを用いる場合は現状では特定の法人、団体、行政機関等しか検証できないことに留意しなければならない。

４.2.1　署名アルゴリズムについて

電子署名を行う際に使用する暗号化アルゴリズム及びハッシュアルゴリズムの組み合わせは以下のもののいずれかを使用し、検証アプリケーションは対象となる署名に用いられている証明書を発行したＣＡのＣＰまたはＣＰＳに検証に関する事項が規定されている場合は、それにしたがって検証できなければならない。特に規定がない場合は証明書プロファイルの仕様にしたがって検証できなければならない。

- sha1WithRSA Encryption（1.2.840.113549.1.1.5）
- sha256WithRSA Encryption（1.2.840.113549.1.1.11）
- sha384WithRSAEncryption (1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (1.2.840.113549.1.1.13)

４.3　タイムスタンプ

RFC3161 に定義されるタイムスタンププロトコルを用い、TSA（Time Stamp Authority）からタイムスタンプトークンを取得する。取得したタイムスタンプトークンは署名付与時に生成される W3C の XAdES-T 形式で記述される。

タイムスタンプは、「タイムスタンプビジネスに係る指針―ネットワークの安心な利用と電子データの安全な長期保存のために―」（総務省、編成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認証した時刻認証業者のものを用いるものとし、第 3 者がタイムスタンプを検証できるものとする。

- 署名文書にはタイムスタンプを付与し、安全な電子保存を可能とする。
- TSA とのインターフェイスは RFC3161 で定義されるプロトコルに従って実装される。

付属書 A　CDA Release1 準拠文書における外部文書の参照　（Informative）

CDA Release1 準拠の CDA 文書において外部参照ファイルを用い、電子署名の影響を外部ファイルに及ぼす手段の例を記載する。

外部参照リンクは CDA 文書の本文の levelone – body – section – paragraph – content – local_markup に記載する。

local_markup タグの下に mref タグ、digest_method タグ、digest_value タグを持ち、mref タグで参照先ファイルの URI を指定する。digest_method タグで参照先ファイルのダイジェストを作成するハッシュ関数を OID で指定する。ハッシュ関数は SHA-1 および SHA-256 が使用可能であるが SHA-256 を推奨する。digest_vaue タグでは参照先ファイルのダイジェスト値を格納する。ダイジェスト値の表示は、もとのハッシュ値（バイナリ）を BASE64 でエンコードした文字列とする。