

平成 1 5 年度保健医療福祉情報セキュリティ推進事業

医療用公開鍵基盤ガイドライン

(暫定版)

財団法人 医療情報システム開発センター

目 次

第 1 章 保健・医療・福祉分野と公開鍵基盤	1
1 - 1 . 背景	1
1 - 2 . 目的	1
1 - 3 . 対象範囲	1
1 - 4 . 用語集	2
1 - 5 . 参照規格・法	18
第 2 章 基本的な方針と注意点	20
2 - 1 . 医療と PKI	20
2 - 2 . 電子署名と完全性	21
2 - 3 . 鍵ペアの生成と否認不能性	21
2 - 4 . 資格認証	21
2 - 5 . 暗号化	25
2 - 6 . 電子保存の真正性と長期にわたる署名の確認	25
2 - 7 . タイムスタンプ	26
第 3 章 公開鍵証明書と証明書失効リストのプロファイル	27
3 - 1 . 全体的な方針	27
3 - 2 . 文字コードセット	27
3 - 3 . 公開鍵証明書の基本領域	27
3 - 4 . 公開鍵証明書の一般的な拡張領域(RFC2459)	30
3 - 5 . 特別な (RFC2459 で定義されていない)拡張	32
3 - 6 . 証明書失効リストプロファイル	33
第 4 章 属性証明書のプロファイル	35
4 - 1 . 全体的な方針	35
4 - 2 . 文字コードセット	35
4 - 3 . 属性証明書の基本的なフィールド	35
4 - 4 . 属性証明書の一般的な拡張フィールド	37

第 5 章	証明書発行局の運用とポリシー	3 8
第 6 章	証明書発行局連携	3 8
第 7 章	時刻認証機構	3 8
第 8 章	権限管理への応用例	4 1
8 - 1	. PKI を応用した権限管理の方法	4 1
8 - 2	. 保健医療分野での権限管理のユースケース	4 1
付録		
付録 1	医療用セキュリティ技術委員会 委員名簿	4 8
付録 2	認証局証明書ポリシー例	追って補充
付録 3	HPKI-PDS	後日作成予定
付録 4	タイムスタンプポリシー例	後日作成予定

1. 保健・医療・福祉分野と公開鍵基盤

1-1. 背景

保健医療福祉分野では、カルテや診療録等の重要な個人情報の電子化が進みつつあり、その保存と検索、施設間連携などにおけるネットワークを介しての伝送・交換等において情報のセキュリティ確保や本人確認及びその資格と属性認証等がますます重要になってきている。

平成13年4月には、電子署名及び認証業務に関する法律（以下、電子署名法）が施行され、電子署名が手書の署名や押印と同等に通用する法的基盤が整備された。

また、政府認証基盤（GPKI）、経済産業省認証局、国土交通省認証局、総務省の住民基本台帳ネットワーク、法務省の商業登記に基礎を置く電子認証制度も進みつつある。

このように、ネットワーク時代の情報セキュリティを確保する手段として公開鍵基盤の整備、普及が着実に進みつつある。

前年度の「先進的情報技術活用型医療機関等ネットワーク化推進事業 - 電子カルテを中心とした地域医療情報化」により全国26箇所で実証実験が進められている。現段階ではまだそれぞれのプロジェクトのセキュリティレベルは様々であり、必ずしも統一された方式では動いていないが、将来的には共通化、標準化された方式により全国規模での互換性の確保が望まれる所である。

こうした状況を踏まえ、（財）医療情報システム開発センターでは平成13年度に医療用セキュリティ技術委員会を開催し、進行中の実証実験の成果も参考にしつつ保健医療福祉分野公開鍵基盤の標準となるような指針の策定を行った。

1-2. 目的

ネットワーク時代に対応した医療情報システムのセキュリティ確保のために、認証局、電子署名、証明書、通信ソフトウェア等についての技術上の課題を中心に整理し、プロトタイプ的设计検討及び予備テストなどを通じて問題点を明らかにし、保健医療福祉分野公開鍵基盤の標準となるガイドラインを策定する。

1-3. 対象範囲

本ガイドラインでは、保健医療福祉分野における公開鍵基盤を用いた証明書の発行、利用に関する運用についての指針を提供する事に主眼を置いている。

保健医療福祉分野で電子化情報を扱うためのセキュリティ対策にはこの他にも考慮すべき課題があるが、本ガイドラインでは取り上げていない。ISO17799（JIS X 5080:2002 情報技術 - 情報セキュリティマネジメントの実践のための規範）や経済産業省の情報システム安全対策基準などを参照されたい。通信経路や保存データの暗号化については、保健医療福祉分野に特異的な要件はなく、また必ずしも必須ではない場合もあり、本ガイドライ

ンでは取り上げていない。

1 - 4 . 用語集

(あ～ん)

・ **アイデンティティ (identity)**

証明書所有者の身元、正体。

・ **アーカイブ (archive)**

証明書の発行履歴、失効履歴等や鍵などを保管すること。

・ **アルゴリズム (algorithm)**

問題を解く為の計算方法や手順、方式など。

・ **暗号モジュール (cryptographic module)**

不正アクセスを防止する為、アクセスの記録、データ保護、データ消去等の機能を持った鍵の管理装置。

・ **エンティティ (entity)**

PKI を利用する人、機関、装置、アプリケーションソフトウェアなどの総称。

・ **エンドエンティティ (end entity)**

証明書を利用する者 / 物で私有鍵を所有し公開鍵証明書を利用する者 / 物。(人、機関、装置、アプリケーションソフトウェアなど)

・ **エントリ (entry)**

人、組織、ネットワーク機器などの属性情報をディレクトリ情報として表わしたもの。

・ **オブジェクト識別子 (OID: Object Identifier)**

名前、国名、使用アルゴリズムなどを世界で唯一の識別子として登録機関に登録した一意性のある、点で区切られた整数列。(例：1.2.840.113549.1.1.5.)

・ **オプション (option)**

必須ではないが実装してもよいこと。

- ・外注ディレクトリ(outsourced directory)

ISO/TS17090-3 の「7.4.4.12 オンライン失効チェック要件」において、失効状態チェックサーバを CA 以外に委託する場合の外部のディレクトリ/サーバ。

- ・鍵活性化(key activation)

ISO/TS17090-3 の「7.2.1.1.3 証明書の申請から発行までの期間」において、鍵を活性化するものによる鍵の有効化プロセス。

- ・鍵所有者(key holders)

ISO/TS17090-3 の「7.3.1.6 私有鍵の所有を証明するための方法」において、私有鍵の所有 (possession) を証明出来る者 / 物。

- ・鍵生成エンティティ(key generating entity)

ISO/TS17090-3 の「7.6.1.2 私有鍵の配付」において、鍵を生成する CA 又は信頼できる第三者。

- ・鍵生成組織(key generating organization)

ISO/TS17090-3 の「7.6.1.6 公開鍵のパラメータ生成」において、公開鍵パラメータを生成する CA 又は信頼できる第三者。

- ・鍵トークン(key tokens)

ISO/TS17090-3 の「7.2.1.3 証明書所有者の義務 2 項」において、鍵情報を含む一塊の情報。

- ・鍵ペア(key pairs)

私有鍵と、対応する公開鍵の組。

- ・患者 / 保健医療福祉サービス利用者(patient/consumer)

医療健康関連サービスを受給する人と医療健康情報システム関係者。(ISO/TS17090 3.1.6)

- ・完全性(integrity)

保存、受信などした情報が完全に元の情報と同一であり、改竄されていないこと。

- ・キーエスクロウ(key escrow)

第三者に鍵を寄託すること。

- ・危殆化(compromise)

危険にさらされること。私有鍵が危殆化したら、その証明書は直ちに失効させる。

- ・クライアント(client)

サービスを利用あるいは依頼する人、またはコンピュータ、またはソフトウェア。

- ・検証者(relying party)

証明書を受け取る者で、その証明書をを用いて検証することにより、その証明書および、またはデジタル署名に依拠して行動する者。(ISO/TS17090 3.3.21)

- ・公開暗号化鍵(public encipherment key)

ISO/TS17090-3の「7.6.1.3 証明書発行者への公開鍵配付」において、暗号化用公開鍵。

- ・公開鍵(public key)

公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵。

- ・公開鍵暗号(public key encipherment)

公開鍵方式による暗号化。

- ・公開鍵基盤(PKI: Public Key Infrastructure)

公開鍵証明書を使用した認証システムに必要な要件の総称。

基本要素：鍵と証明書のライフサイクル管理、認証機関(CA)、登録機関(RA)、証明書の保管・運用管理用ディレクトリの維持、完全な証明書失効システム、鍵のバックアップとリカバリの仕組み、タイムスタンプ機能など。

メリット：認証(受信側にとって送信側が確実に当人であることを保証)、秘匿性・機密性のある通信(盗聴防止、意図した特定の相手のみ読める)、否認防止(送信側がデータを送信したことを否定できない)、完全性(データが改竄されていないことを証明)。

- ・公開鍵証明書(PKC: Public Key Certificate)

公開鍵ペアの所有者であることを保証した電子証明書。所有者、公開鍵、有効期限などを含み、発行CAが署名したもの。エンドエンティティに対して発行するものと、CAに対して発行するものがある。CAに対して発行するものの中には、自己署名(セルフサイン)証明書と、他CAから発行されたCA証明書がある。

- ・公開鍵パラメータ(public key parameters)
公開鍵証明書に書き込まれる諸情報。
- ・サブジェクト識別名(subject Distinguished Name)
ISO/TS17090-3 の「7.3.1.4 名前の一意性」において、証明書所有者名。
- ・サブジェクト情報(subject information)
ISO/TS17090-3 の「7.2.2.2 登録局の責任」、「7.4.4.1 失効事由」において、証明書所有者の情報。
- ・サブジェクト名(subject name)
証明書の所有者名。
- ・支援組織従業員(supporting organization employee)
ISO/TS17090-3 の「7.2.1.1.5 私有鍵の保護」、「7.3.1.8 個人の認証」において、医療健康サービスを提供する組織(health care organization)を支援する組織の従業員。例えば、医療記録の口述筆記者や健康保険の苦情裁定人や薬剤受注係など。(ISO/TS17090 3.1.11)
- ・失効ポリシー(revocation policy)
ISO/TS17090-3 の「7.2.2.1 認証局の責任」「7.2.2.2 登録局の責任」において、局ポリシーの失効に関する部分。
- ・失効リスト(CRL: Certificate Revocation List)
証明書の有効期間中に、CA 私有鍵の危殆化等の理由で失効した証明書のリストで、証明書を発行した CA の署名付一覧表。
- ・私有鍵(private key)
非対称暗号アルゴリズムを使用した鍵で、その所有が通常は一つのエンティティに限定されるもの(ISO/TS17090 3.2.22)。公開鍵と対をなす秘密に保たれる鍵のこと。
- ・私有認証鍵(private authentication key)
ISO/TS17090-3 「7.6.2.4 私有鍵のバックアップ」において、認証用の鍵。
- ・私有復号鍵(private decipherment key)
ISO/TS17090-3 「7.6.1.2 私有鍵の配付」「7.6.2.4 私有鍵のバックアップ」「7.6.2.6 暗号モジュールへの私有鍵の入力」において、暗号復号用の私有鍵。

- ・住民基本台帳ネットワーク

各市町村で管理する住民基本台帳を基礎に、全国の市町村を電気通信回線で結び、住民基本台帳事務を効率化する。住民基本台帳カードは住民票の写しの広域交付、転入転出の特例及び本人確認の業務に利用される。また住基カードは、追加発行可能なマルチアプリケーションカードとして、住基ネットシステムにおける業務利用に必要な基本機能を備えると共に、住民基本台帳法により市町村の条例の定めるところにより、市町村の独自利用にも供される。

- ・証明書失効(certificate revocation)

ISO/TS17090-3「7.2.7.4 監査トピックス」において、証明書の期限が満了していなくても最早信頼できなくなって、証明書とその所有者の間の信頼の絆を断ち切る行為。(ISO/TS17090 3.3.10)

- ・証明書失効リスト(CRL: Certificate Revocation Lists)

ISO/TS17090-3「7.2.1.1 認証局の義務」において、失効した証明書のリスト。

- ・証明書所有者(certificate holder)

証明書の所有者。

- ・証明書発行局(Certificate Issuer, IA: Issuing Authority)

証明書には公開鍵以外の事項も証明書発行局によって書き込まれる。証明書発行局は記載事項に責任を負い、発行についてのポリシーを持っている。

- ・証明書発行者(certificate issuer)

証明書を発行する者。

- ・証明書ポリシー(CP: Certificate Policy)

共通の安全要求をもって、特定のコミュニティ及び/もしくはアプリケーションクラスへの証明書の適用性を示す指定されたルール集。(ISO/TS17090 3.3.15)

- ・署名私有鍵(signing private key)

ISO/TS17090-3「7.2.1.2 登録局の義務」において、署名用の私有鍵。

- ・真正性(authenticity)

真実で正しいこと。本物。

- ・政府認証基盤(GPKI: Government Public Key Infrastructure)

国民等と行政との間でインターネット等を利用してやり取りされる電子文書について、その文書が真にその名義人によって作成され、内容に改変がないことを相互に確認するための仕組み、基盤。具体的には、公開鍵暗号方式による署名を用いた行政機関側の認証システムであり、ブリッジ CA と各府省 CA から構成される。

- ・相互認証(cross certifying, cross-certified)

ISO/TS17090-3「7.2.1.1 認証局の義務」「7.4.9 CA の終了」において、認証局同士の認証により、それぞれが発行した証明書の信頼性を相互に保証すること。

- ・相対識別名(relative distinguished name)

ISO/TS17090-3「7.3.1.2 意味を持った名前的重要性」において、証明書に現れる名前は、証明書の所有者を意味のある方法で割り当てられた名前を確認できること。

- ・属性 (attribute)

証明書所有者を識別・区別するための諸情報。属性型（例えば、氏名、所属、役職など）と属性値（例えば、鈴木太郎、総務部、課長）からなる。

- ・属性認証局(AA: Attribute Authority)

属性証明書の発行局。

- ・属性証明書(AC: Attribute Certificate)

属性証明書の所有者の属性を証明する属性認証局のデジタル署名付き証明書。

- ・属性証明書発行局(attribute certificate authority)

属性証明書の発行機関。

- ・属性証明書発行者(attribute certificate issuer)

属性証明書の発行者。

- ・属性認証(attribute authentication)

属性証明書発行機関(attribute certificate authority)が属性証明書所有者の属性を認証し AA の電子署名をした属性証明書を発行する。主に所有者のアクセス権限管理に使う。

- ・ソフトウェアトークン(software token)

ISO/TS17090-3「7.6.2.4 私有鍵のバックアップ」において、私有鍵をソフトウェアで所定のメモリにバックアップ保管する場合。

- ・タイムスタンプ(time stamp)

事柄の発生時刻を証明するためのタイムスタンプ発行機関(TSA: Time Stamp Authority)の署名付き時刻証明書。

- ・チャレンジ(challenge)

通信相手の検証を行う方式の一つであるチャレンジアンドレスポンス方式において、検証する側がある値(チャレンジ)を送り、検証される側が私有鍵で暗号化した値(レスポンス)を送り返し、共通鍵又は対応する公開鍵で復号し相手を検証する。チャレンジの値を毎回変えることにより万一レスポンスが盗聴されても再利用されにくい。

- ・ツリー構造(tree structure)

データ構造、情報表現方法の一つで、木の根本(root)から順次分岐点(node)を介して枝分かれしてゆく構造。例えば、国(日本) - 都道府県(東京) - 区(港) - 赤坂、の様に国(root)から都道府県(node)の枝に分かれ、更に区市町村に枝分かれしてゆく様な構造。

- ・デジタル署名(digital signature)

公開鍵基盤を用いた電子署名の実装。

- ・デジタル署名鍵(digital signature key)

デジタル署名用の鍵。

- ・ディレクトリ(directory)

元は電話帳、住所録など名前で検索するデータ集で、データベースにおいてはファイル名の一覧表。公開鍵基盤においては、証明書が保管されているサーバから該当する証明書を名前等を指示して検索、引き出しする機能。

- ・ディレクトリリスティング(directory listing)

ISO/TS17090-3「7.2.8.1 秘密保持すべき情報のタイプ」において、証明書所有者の個人情報に格納しておくディレクトリ。

- ・電子署名(electronic signature)

デジタルデータの正当性を保証するために付けられる署名。

- ・電子署名法

電子署名及び認証業務に関する法律。真正成立の推定、私文書限定、本人性確認と非改竄性確認など。

- ・電子保存(electronic archiving)

電磁的にデジタル情報を保存しておくこと。医療分野では平成11年に厚生省局長通知「診療録等の電子媒体による保存について」で、真正性の確保、見読性の確保、保存性の確保、を満たすことで診療録等の電子保存が可能となった。

- ・登録局(RA: Registration Authority)

証明書発行申請者の本人確認、登録を行い証明書発行の基となる登録原簿を持つ機関。独立した登録局とする場合とCAの一部とする場合がある。

- ・トークン(token)

情報の一塊り。

- ・ドメイン(domain)

CA局が管轄する領域。

- ・認証鍵(authentication key)

ISO/TS17090-3「7.6.1.9 鍵の使用目的」において、認証に用いる鍵。

- ・認証実施規定(CPS: Certification Practices Statement)

証明書ポリシーに基づいた認証局運用についての規定集。CAの証明書発行において使用する実務規定。(ISO/TS17090 3.3.16)

- ・認証局(CA: Certification Authority)

証明書の発行・更新・失効、CA等の鍵の生成・保護及び証明書所有者の登録を行う機関で、単にCAという場合は証明書発行業務及び登録業務を含む。

証明書発行者。一人以上の検証者(relying party)により信頼されている機関で証明書の生成と割り当てを行う。検証者の鍵を生成する事もある。(ISO/TS17090 3.3.14)

- ・認定ヘルスケア提供者(sponsored health care provider)

ヘルスケアサービス提供者でその実務領域で規制を受けた専門資格者ではないがそのヘルスケアコミュニティで活動しており、規制を受けたヘルスケア組織により認定されてい

る者。(ISO/TS17090 3.1.9)

・ハッシュ(hash)

元のデータからより短い所定の長さのデータを計算する方法。公開鍵基盤では元の長い文書の文字列を暗号化・復号化するのは大変なので、例えば160ビットの長さにハッシュ関数で圧縮してから暗号化したものを電子署名として送り、受信側で復号し、圧縮していない元の文書のハッシュを計算して合っていれば改竄されていない事が確認できる。ハッシュ関数は元のデータが少しでも変われば値が変わり、またハッシュ値からは元のデータが推測し難い性質を持つものが使われる。

・ハードウェアトークン(hardware token)

ISO/TS17090-3「7.6.1.1 鍵ペアの生成」において、生成した鍵ペアを安全なハードウェアメモリに保管する手段。

・非公的資格ヘルスケア専門職(non-regulated health professional)

ヘルスケア組織に雇われている人で、ヘルスケア専門資格者でない人。例として、予約を処理する受付係又は秘書、あるいは患者の健康保険を確認する責任を負っている業務管理者。(ISO/TS17090 3.1.5)

・ビットストリング(bit string)

ビット列のこと。

・否認防止(non repudiation)

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

・フィールド(field)

証明書の所定の領域。

・プロトコル(protocol)

コンピュータシステム間で通信を行うための規約、手順。特に異機種間での接続を行うとき重要となる。

・プロファイル(profile)

証明書や失効リストに記載するデータの内容と配置を決めた約束事で、RFC2459 及び ISO/TS17090-2 Certificate Profile に規定されている。

- ・ **プロブレムリスト(problem list)**

患者の問題点、例えば検査結果の異常値、薬の副作用などを列挙したもの。

- ・ **ヘルスケアコミュニティ(health care community)**

ISO/TS17090-3「7.3.1.8 個々(人)の身元の認証」において、“認定ヘルスケア提供者”(sponsored health care provider)が活動している社会。

- ・ **ヘルスケア証明書(health care certificate)**

ISO/TS17090-3「7.2.1.4 検証者の義務」において、そのヘルスケアドメインで通用する証明書。

- ・ **ヘルスケア専門資格者(regulated health professional)**

国家レベルで認定された団体により、あるヘルスケアサービスを行う資格を与えられた人。(ISO/TS17090 3.1.8)

- ・ **ヘルスケア CP(health care Certificate Policy)**

ISO/TS17090-3「7.2.4.2 分割、存続、合併、通知」において、そのヘルスケアドメインの証明書ポリシ。

- ・ **ヘルスケア PKI ドメイン(health care PKI domain)**

保健医療分野で公開鍵基盤を共有する範囲、領域。

- ・ **ポリシ(policy)**

公開鍵基盤において認証局、証明書等を設計、運用するための基本方針、規則を記述した文書。

- ・ **本人確認(identity authentication)**

他人がなりすましていないか、本人の真正性を確認すること。

- ・ **有効性確認局(validation authority)**

ISO/TS17090-3の「7.4.4.12 オンラインでの失効確認要件」において、失効リストをCA以外に委託する場合の確認機関。

- ・ **ライブラリ(library)**

予め用意されているプログラム集やデータ集。

- ・ランダム(random)
乱数(random number, random digit)。
- ・リポジトリ(repository)
証明書及び失効リストを格納し公表するデータベース。
- ・ログ(log)
通信記録、コンピュータの操作記録、ホームページのアクセス記録等。

(A-Z)

- ・ AA(Attribute Authority) : “ 属性認証局 ” 参照
属性証明書を発行することにより特権を与える機関。(ISO/TS17090 3.3.1)
- ・ AC(Attribute Certificates) : “ 属性証明書 ” 参照
- ・ attribute : “ 属性 ” 参照
- ・ Attribute Certificates : “ 属性証明書 ” 参照
- ・ Audit
監査 (draft-ietf-pkix-ac509prof-09.txt 4.3.1 参照)
- ・ Bridging CA
ブリッジ認証局(BCA)。BCA が複数の CA を認証することにより、それぞれの CA は相互に認証を行わなくても、BCA を信頼拠点として各 CA 下のユーザは他の CA の証明書を信頼できる様にする。普通 BCA は CA の認証を専門に行い、エンドエンティティの認証は行わない。
- ・ CA(Certification Authority : “ 認証局 ” 参照)
- ・ CA 管轄区域(CA domain)
認証局が管轄している領域。
- ・ CA 信任団体(CA accreditation body)
ISO/TS17090-3 「7.2.7.5 欠点の結果として取られる行動」において、CA を信任する上位団体。

- **Consumer**

保健医療福祉サービス利用者。医療情報システムの関係者。(ISO/TS17090 3.1.6)

- **CP(Certificate Policy : “ 証明書ポリシー ” 参照)**

- **CPS(Certification Practices Statement) : “ 認証実施規定 ” 参照**

- **CRL(Certificate Revocation List) : “ 証明書失効リスト ” “ 失効リスト ” 参照**

- **CRL 配布点(CRL Distribution Point)**

証明書失効リストを入手できる場所・アドレス。

- **Cross/Bridge Certs : Cross Certificates、 Bridge Certificate 参照**

- **Cross Certificates**

CA の相互認証。CA が相手の CA を認証し CA 用の証明書を発行する。

- **Devices**

識別可能なコンピュータ制御された装置又は機器で私有暗号鍵を所有しているもの。この定義に合致する認定された医療機器や、医療情報システムに使われる機器で治療や診断に直接役割を持たない物も含まれる。(ISO/TS17090 3.1.2)

- **Directory Information Tree**

ツリー構造を持ったディレクトリ情報。

- **End Entity : “ エンドエンティティ ” 参照**

- **End Entity Certificates**

エンドエンティティ用の証明書。

- **hcRole(health care Role)**

保健医療福祉分野での役割、資格。

- **Health Care Certificate Types**

保健医療福祉分野における証明書の種類。

- ・ **HIS サーバ(Hospital Information System Server)**
病院情報システムのサーバ。

- ・ **Holder**
証明書の所有者。

- ・ **HTTP, http(Hyper Text Transfer Protocol)**
インターネットの WWW サーバと HTML(Hyper Text Markup Language : ホームページ記述言語)でやり取りするための通信規約。

- ・ **ID**
識別情報。

- ・ **IETF(Internet Engineering Task Force)**
インターネットの技術的活動部会。インターネットにおけるプロトコルの技術開発、標準化を主な目的としている。作成された仕様は RFC(Request For Comments)と呼ばれる。

- ・ **Individual**
医療従事者や患者などのサービス受給者、関係者の総称。

- ・ **ISO/IEC**
国際標準化機構 ISO(International Organization for Standardization)と国際電気標準化会議 IEC(International Electrotechnical Commission)の合同技術委員会 (JTC-1: Joint Technical Committee)で作成された標準。

- ・ **ITU-T(International Telecommunication Union-Telecommunication Standardization Sector)**
国際連合 (UN)の専門機関の一つである国際電気通信連合 (電気通信の改善、合理的利用を目的としている) の電気通信標準化部門。

- ・ **LRA**
Local RA。

- ・ **MD5(Message Digest 5)**
一方向性ハッシュアルゴリズムで 128bit のハッシュ値を生成する。

- **nonce**

反復攻撃を防ぐ為に用いられる大きな整数。一般的には疑似乱数を使って生成する事が多い。

- **Non Regulated Health Professional** : “ 非公的資格ヘルスケア専門職 ” 参照

- **NULL**

空を意味する制御文字。

- **OCSP レスポンダ(Online Certificate Status Protocol Responder)**

証明書の有効性を検証するためのプロトコルに従って検証結果を返すサーバ。

- **OID(Object Identifier)** : “ オブジェクト識別子 ” 参照

- **Organization**

主な活動がヘルスケアサービスや健康増進に関係している、公式に登録されている組織。
例：病院、インターネットヘルスケア Web サイト、ヘルスケア研究所など。(ISO/TS17090 3.1.4 health care organization)

- **PGP(Pretty Good Privacy)**

電子メールの暗号化と電子署名を公開鍵と私有鍵で行う方式で CA (認証局) を使わず信頼できる第 3 者の署名を使う。

- **PKC(Public Key Certificate)** : “ 公開鍵証明書 ” 参照

- **PKI (Public Key Infrastructure)** : “ 公開鍵基盤 ” 参照

- **Public Key Certificates** : “ 公開鍵証明書 ” 参照

- **Public Key Infrastructure** : “ 公開鍵基盤 ” 参照

- **Qualified Certificate**

RFC3039 Internet X.509 Public Key Infrastructure Qualified Certificate Profile で定義されており、自然人に対して発行される証明書で、何らかの法の適用を受ける身分、地位、資格、状態等を証明するもの。

- ・ **RA(Registration Authority)** : “ 登録局 ” 参照

- ・ **Regulated Health Professional** : “ ヘルスケア専門資格者 ” 参照

- ・ **RFC(Request For Comments)**
IETF が作成したインターネットに関する標準文書の総称。

- ・ **Root CA Certificates**
ルート CA の証明書。

- ・ **RSA アルゴリズム**
RSA 暗号のアルゴリズム。

- ・ **RSA 暗号**
公開鍵暗号方式の一つ。十分に大きな素数の積の因数分解が難しい事を利用している。公開鍵で暗号化し私有鍵で復号する親展通信、私有鍵で暗号化し公開鍵で復号するデジタル署名の双方に使える。

- ・ **SHA-1(Secure Hash Algorithm-1)**
任意の長さのデータから 160bit のハッシュ値を作成する方法。

- ・ **S/MIME(Secure/Multipurpose Internet Mail Extensions)**
電子メールの暗号化と電子署名を公開鍵と私有鍵で行う方式。

- ・ **SSL(Secure Socket Layer)**
WWW(World Wide Web)上での情報交換時に暗号化、認証を鍵と証明書を用いて行う。

- ・ **Subordinate CA Certificates**
ルート CA に信頼拠点を置くサブ CA の証明書。

- ・ **Time Stamp Authority(TSA)**
その情報とその時刻以前に存在したこと及びその後改竄されていないことを証明する為の信頼できる (第三者) タイムスタンプ発行機関。

- ・ **Time Stamp Protocol(TSP)**
 タイムスタンプ要求と応答の手順、方式。

- ・ **Time Stamp Token**
 タイムスタンプの入ったトークン。

- ・ **TLS(Transport Layer Security)**
 SSL より暗号が強化され TCP/IP 以外のプロトコルにも対応したセキュリティ技術。

- ・ **TSA (“ Time Stamp Authority ” 参照)**

- ・ **TSP (“ Time Stamp Protocol ” 参照)**

- ・ **TTP(Trusted Third Party)**
 依頼者から独立した信頼できる第三者機関。

- ・ **URL(Uniform Resource Locator)**
 インターネット上で探す対象のアクセス方法と場所の表記方法。
 (例 <http://www.medis.or.jp>)

- ・ **VPN(Virtual Private Network)**
 VPN 接続装置を使いデータをパケット単位で暗号化しインターネットのようなオープンなネットワーク上に仮想の専用通信路を設ける方法。

- ・ **Web サーバ**
 インターネット上の広域情報検索システム WWW(World Wide Web)に情報を提供するサーバ。

- ・ **X.509**
 ITU-T が定めた証明書及び CRL/ARL のフォーマット。X.509v3(Version3)では、任意の情報を保有するための拡張領域が追加されている。

1 - 5 . 参照規格・法

1 - 5 - 1 . 参照規格・法

(1) 電子署名法関連

(<http://www.miti.go.jp/policy/netsecurity/digitalsign.htm>)

(http://www.soumu.go.jp/joho_tsusin/top/densi_syomei/index.html)

・電子署名及び認証業務に関する法律（平成12年法律第102号）

・電子署名及び認証業務に関する法律施行規則（平成13年総務省 法務省 経済産業省令第2号）

・電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成13年総務省 法務省 経済産業省告示第2号）

(2) ISO-TC215 Health Informatics -WG4 Public Key Infrastructure

-ISO/TS 17090-1 Part1: Framework and overview

-ISO/TS 17090-2 Part2: Certificate profile

-ISO/TS 17090-3 Part3: Policy management of certification authority

(3) IETF(The Internet Engineering Task Force) RFC(Request For Comment)

(<http://www.ipa.go.jp/security/rfc/RFC.html>)

(<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509>)

・ RFC2459:Internet X.509 Public Key Infrastructure Certificate and CRL Profile

・ RFC2510:Internet X.509 Public Key Infrastructure Certificate Management Protocols

・ RFC2527:Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

・ RFC2560:Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP

・ RFC3039: Internet X.509 Public Key Infrastructure Qualified Certificate Profile

・ RFC3161:Internet X.509 Public Key Infrastructure Time-Stamp Protocol(TSP)

(4) draft-ietf-pkixac509prof-09.txt: An Internet Attribute Certificate Profile for Authorization

(<http://www.ietf.org/html.charters/pkix-charter.html>)

(5) ISO/IEC (日本規格協会 <http://www.jsa.or.jp>)

・ ISO9000 : 品質マネジメントシステム。

・ ISO17799(1-3) : 情報技術 - 情報セキュリティ管理実施基準。

(6) JIS (日本規格協会 <http://www.jsa.or.jp>)

- ・ JIS X 5080:2002 : 情報技術 - 情報セキュリティマネジメントの実践のための規範。
(ISO/IEC17799:2000)

(7) その他

- ・ US FIPS 140-1,140-2(Federal Information Processing Standard) :
Security Requirements for Cryptographic Modules
(<http://csrc.nist.gov/cryptval/>)

1 - 5 - 2 . 参考資料

(1) 政府認証基盤 (GPKI)ブリッジ認証局 CP/CPS

平成 1 3 年 4 月 2 5 日 行政情報化推進各省庁連絡会議幹事会了承

(<http://www.gpki.go.jp/cpcps.cpcps.pdf>)

(2) 情報システム安全対策基準 (平成 7 年 8 月 29 日通商産業省告示第 518 号)(制定)

(平成 9 年 9 月 24 日通商産業省告示第 536 号)(最終改正)

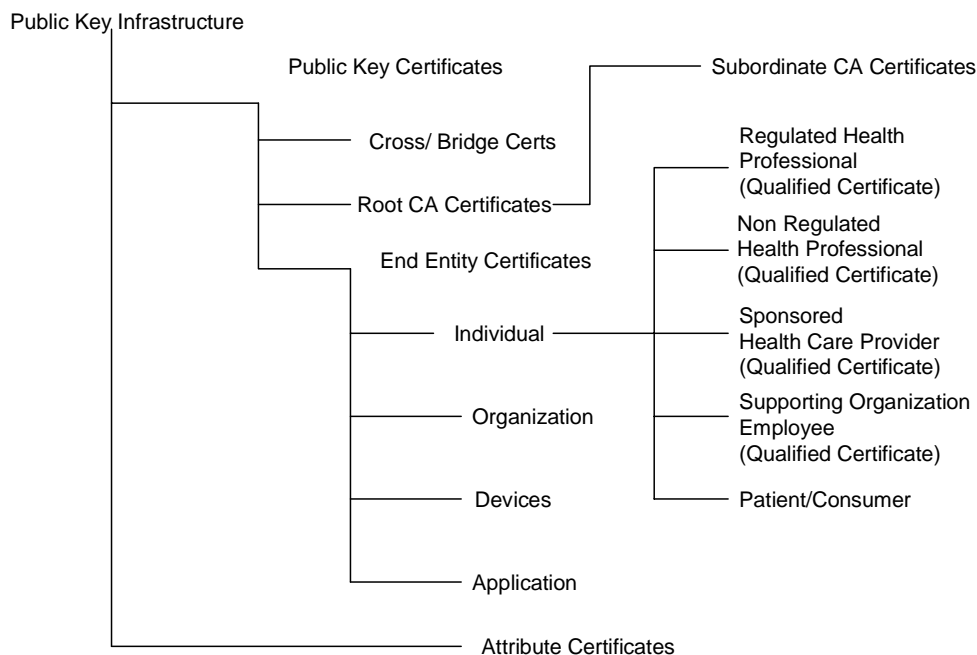
(<http://www.miti.go.jp/policy/netsecurity/downloadfiles/eseu03j.pdf>)

2 . 基本的な方針と注意点

2 - 1 . 医療とPKI

ITU-T X.509 で規定される公開鍵基盤(PKI)を医療で用いる場合、その目的はいくつか考えられます。ISO-TS 17090 には以下の図が示されています。

Figure 1 – Health Care Certificate Types



この中で **End Entity Certificates** の **Individual**、**Organization**、それから **Attribute Certificates** は適応分野で運用や証明書の型式をある程度定めることが必要になります。このドキュメントは主にこれらの証明書の保健・医療・福祉分野で用いる場合の運用と証明書型式について、主に技術的な観点からガイドラインを示しています。**Device** や **Application** に PKI を用いる場合、証明書のプロファイルで保健・医療・福祉分野で特別に考慮することはなく、また SSL/TLS や PKI-VPN のように各方面で応用されている例があり、それらを参考にすればよいでしょう。ただし用途によっては機器やアプリケーションに対する証明書の発行ポリシーは人や組織に対するものと同等の厳格さが要求されますので、そのような場合はこのガイドラインにあるポリシーと同等の厳格さを持つポリシーを条件にする必要があります。

2 - 2 . 電子署名と完全性

End Entity Certificates の中で **Individual**、つまり医療従事者や患者などのサービス受

給者に証明書を発行する場合と、Organization、つまり医療機関や保険者などの組織に証明書を発行する場合、その用途はいくつか考えられます。

用途の 1 つ目は「署名」で、これには法律や規則で定められている署名・捺印を電子的に行う場合と、法律や規則で定められてはいないが、情報作成・編集の責任者を明確にするために行う場合があります。また電子署名は通常、署名の対象となる情報のダイジェストに対して行われますので、もとの情報の完全性（真正性）の保証のための 1 つの手段としての意味がありますが、完全性については後であらためて取り上げます。法律や規則で定められている場合はわが国では「電子署名法」に準拠した証明書と署名方法が必要です。電子署名法では電子署名に用いる証明書は署名の目的のためだけに用いることが定められていますので、署名に用いる証明書およびそのペアの私有鍵は他の用途に用いてはいけません。法律・規則で定められていない署名に同じ証明書や私有鍵を用いるかどうかは、運用で定めなければなりません。今後の連携医療の発展を考えると、あまり狭い範囲だけで通用する証明書をを用いることは推奨されません。また証明書の数が増えるとそれだけ運用に負担がかかりますので、法的に有効な署名と同じものを用いると良いでしょう。

2 - 3 . 鍵ペアの生成と否認不能性

公開鍵の生成は PKI にとって重要な部分です。署名自体や署名の検証は計算量も少なく、高速に処理できますが、鍵の生成は計算量も多く、良い鍵を生成するためには厳密な乱数の発生が必要です。したがって鍵を生成するプログラムは厳密に選ぶ必要があります。これは証明書発行局の認証実施規定(Certification Practices Statement: CPS)でしっかり規定しておく必要があります。

さらに鍵をどこで生成して、どのように管理するかも PKI にとって大変重要です。電子署名が確実に本人の署名であることを証明（否認不能性と呼びます）するためには、私有鍵は本人だけしか知らないということを証明することが必要です。そのためには鍵の生成を本人（証明書の所有者）が行うか、署名検証等の事後の運用で利害関係のない第 3 者が作成し、本人に送付後はただちにすべてのコピーを破棄する必要があります。証明書発行局と証明書の所有者は一般的に言って署名の検証に問題があった場合に対立関係になる可能性が高いので、電子署名を目的とする鍵は証明書発行局が生成することは、推奨されません。

2 - 4 . 資格認証

保健・医療・福祉分野では情報を扱う人の資格や役割が重要な場面が多くあります。PKI で資格や役割をあらわすためには 2 つの方法があります。1 つは公開鍵証明書に資格や役割を示すフィールドを定義して使う方法で、もう 1 つは属性証明書を使う方法です。この 2 つの方法にはそれぞれ特徴があり、使い分けを工夫する必要があります。属性証明書は公開鍵が含まれていなくて、通常は短い有効期間で使用します。また公開鍵がないために署

名との関連付けは属性証明書自体ではできませんので、対応する公開鍵証明書を一緒に用いる必要があります。

属性証明書と公開鍵証明書の使い方を検討するためにA病院の内科外来を担当するX医師が紹介されて受診した患者の過去の診療記録について紹介元のB医療機関に問い合わせる場合を考えてみます。X医師はB医療機関に対して問い合わせ書を作成して送りますが、B医療機関は問い合わせで来た人の身元や属性を確認することなしに、患者情報を返送することはできません。A病院の内科に患者を紹介したことはわかっていますので、問い合わせで来た人がA病院の内科担当の医師であることを確認すればよいことになります。

2 - 4 - 1 . 公開鍵証明書による資格認証

最初に公開鍵証明書だけですべての属性を証明する場合を考えてみます。この場合証明書にはXという人で、医師であって、A病院の従業員で、内科外来担当であることが記載されることになります。そしてこの証明書はB医療機関で信頼できるものであると判断されなくてはなりません。したがって証明書の発行者はB医療機関が信頼できる組織が発行したものである必要があります。A病院が大阪にあり、B医療機関が東京であることもありえますし、それ以外の医療機関とも同様な場合が起こりうることを考えると、事実上日本中ですべての医療機関から信頼される組織が証明書を発行する必要があります。

仮に財団法人医療情報システム開発センター（MEDIS-DC）が証明書を発行すると仮定します。MEDIS-DCはXが医師であることは厚生労働省に問い合わせることで理論的には確認することが可能です。またA病院が存在することも地方自治体等に問い合わせることで確認できます。これらは手間ではありますが、仕組みをうまく作れば現実にも可能でしょう。X医師がA病院に勤務していることも保険医登録情報などを用いればなんとかできるかも知れません。しかしX医師が内科外来担当であることはA病院に問い合わせる以外に確認の方法がありません。証明書発行の要請があるたびにその医療機関に勤務形態を確認しなければなりませんので、証明書発行の運用は複雑になります。これは証明内容に責任を持つ組織が1つの証明書に対して多数存在するため生じる複雑さです。また、もし発行したとしても内科外来担当から救急外来担当に変わった場合や、A病院からB病院に転勤した場合には証明書を失効させて、新しい証明書を発行しなければなりません。電子証明書は単なるファイルですので、いくつでもコピーすることができます。したがって電子証明書そのものをすべて廃棄し、それを確認することは現実には不可能ですので、証明書失効リスト（CRL）を発行します。証明書を使う人は常に最新のCRLを参照して、その証明書が失効していないかどうかを確認する必要があります。転勤や担当部署の変更は全国的に見れば日常的に起こっていますので、大量のCRLが常に存在することになり、PKI全体の運用に大きな負担になります。

つまり医療で必要なすべての属性を1つの公開鍵証明書に盛り込むことは現実には困難といえます。複数の公開鍵証明書を組み合わせる方法も考えられますが、もとの情報

と証明書を関連付けるためには電子署名を行う必要があります、公開鍵証明書の数だけ電子署名を重ねる必要があります。そのため電子署名の順序など複雑な取り決めをしなければなりませんし、CRL が大量に発生する問題は解決できません。

2 - 4 - 2 . 属性証明書による資格認証

属性証明書は技術的には公開鍵証明書の簡略版であり、比較的簡単に発行できますし、通常は数時間～数日といった短期間で無効になるようにしますので、資格や役割の変更があっても CRL を発行する必要性はほとんどありません。一方、属性証明書には公開鍵がありませんので、電子署名と直接対応付けることはできません。公開鍵証明書と組み合わせる必要があります。つまり属性証明書で資格認証を行うということは、公開鍵証明書と属性証明書の使い分けを考えることにほかなりません。

2 - 4 - 1 の公開鍵証明書だけで資格認証を行う場合にうまくいかない理由は証明内容に責任を持つ組織が複数存在することと、CRL が大量に発生することでした。従ってこれらの障害を取り除くことができるような属性証明書と公開鍵証明書の使い分けを考えればよいこととなります。公開鍵証明書は基本的には公開鍵が誰のものを証明するものです。この「誰」に対して責任を持つ組織が単純であり、「誰」があまり変化しなければ公開鍵証明書の運用は単純になり、それ以外の属性を属性証明書で証明すればよいこととなります。このような「誰」の定義には2つの場合を考えることができます。

1つ目は個人や法人といった人格を「誰」として扱う場合です。このような公開鍵証明書に対する署名は個人の「実印」や法人の「公印」に相当します。証明に責任を持つ組織は住民票情報を管理している地方自治体や法人登記または医療機関登録を管理している組織になります。これは公的個人認証基盤整備等として電子政府計画で整備されつつあり、制度的な問題は別として技術的には比較的容易に運用可能です。先の例で言えばXさんとA病院、B医療機関がそれぞれ公開鍵証明書を1つ持つこととなります。Xさんが医師であること、A病院の勤務医であること、内科外来担当医であることはすべて属性証明書で運用することとなります。この方法ではCRLは個人の死亡や法人の消失などの場合を除いてほとんど発生しませんし、属性証明書を証明内容ごとに複数使うことにすれば、証明内容に対する責任組織も単純です。ただし一般には属性証明書は有効期間が短いものですので、しばしば必要になる医師の資格を示す属性証明書もその都度、発行を要求しなければなりません。医師の資格に責任を持つのは厚生労働省ですから、たとえ地方自治体に業務を委託するとしても医師資格属性証明書の要求は多数が集中することになり、運用上の負荷になる可能性があります。医師のような公的資格は変更が極めて少ないので、属性証明書の有効期間を長くすることも考えられます。しかしこの場合は少ないとはいえ、資格喪失などがありますので、属性証明書のCRLの発行を考えなければなりません。CRLの発行はそれほど難しいことではありませんが、属性証明書を使うシステムがすべてCRLを検索しなければならなくなり、実装上の負担になる可能性があります。また属性証明書は公開鍵証

明書に関連付ける必要がありますが、属性証明書の有効期間が公開鍵証明書の有効期間を超えることはできないために、公開鍵証明書の有効期間が残り少なくなっている場合などは属性証明書の有効期間を変えなければならず、発行自体も複雑になります。

2 つ目は公的な資格を含めた個人を「誰」として扱う場合です。法人や組織は一つ目の場合と同じです。先の例では「医師である X さん」を公開鍵証明書で資格認証し、「A 病院の勤務医」、「A 病院の内科医外来担当医」を属性証明書で資格認証します。この場合は運用がもっとも単純になります。公的資格はほとんど変化しませんので、CRL の発生は少なく、証明内容の責任の所在も単純で明確です。唯一の問題は X さんが医師として署名する場合と、個人として署名する場合に証明書や私有鍵を使い分ける必要があることですが、あまり大きな問題にはならないでしょうし、心情的にはかえって好まれるかも知れません。公的資格には「医師」のような国家資格や「保険医」のような地方自治体に対する登録資格があり、現在の管理体制では責任の所在が異なる以上は証明書を分ける必要がありますが、これは制度的な整備や「保険医」の属性証明を医療機関や医師会などに委任することで、解決することが可能です。

このガイドラインは PKI を保健・医療・福祉分野に応用するための技術的な指針ですので、運用面の断定はしていませんが、公的な資格を公開鍵証明書で運用し、それ以外の属性は属性証明書で運用することを推奨しています。またその前提で証明書の形式などを規定しています。また当面は国家資格だけを公的な資格として本ガイドライン 3 章の hcRole 属性に取り入れています。これは制度的な整備などが整えば改定される可能性があります。

2 - 4 - 3 . 属性証明書発行局の運用

属性証明書 (AC) は属性証明書発行局 (AA) が発行します。公開鍵証明書の発行局 (CA) についてはこのガイドラインでもポリシーの提示を含めて詳細に記載していますが、AA については記載がありません。これは AC の流通範囲や運用が多彩であることが予想されるため、AA の運用も場合によって大きく変化します。例えば 1 つの医療機関内でアクセス制御に AC を使う場合と、地域医療連携で勤務先などの属性の証明に AC を使う場合では運用が大きく異なります。したがって特定の運用方針を推奨することが困難です。

しかし、一定の地域などで信頼できる属性証明書を発行するためには AA の運用や、AA 自体の証明書は相応の厳格さで運用する必要があります。そのためには CA のようにポリシーを定め、AA の証明書は一定以上の信頼性のあるものでなければいけません。その点に十分留意して運用をすることが期待されます。

2 - 5 . 暗号化

PKI は暗号化に用いることもできます。PGP や S/MIME は公開鍵証明書を用了認証と

暗号化を組み合わせたプロトコルで広く使用されています。アプリケーションやライブラリも数多く存在し、また保健医療福祉分野で特別な要素もありませんので、PKI を暗号化に用いること自体は簡単です。しかしただ 1 つ注意しなければならないことは、法的に有効であることが求められる署名に用いる証明書や私有鍵は暗号化に使ってはいけないということです。暗号化に用いた場合、頻回に鍵を使用しますので、鍵が解読される可能性が高くなります。したがって電子署名法でも暗号化に用いることを禁止しています。

また保健医療福祉分野の情報は利用できなければ意味がありません。暗号化によって万が一にも利用性が阻害されることがないように注意する必要があります。通信途中のような一時的な暗号化は問題がありませんが、データベースそのものを暗号化するような場合は、事故などが起こっても必要なときに速やかに復号できる必要があります。

2 - 6 . 電子保存の真正性と長期にわたる署名の確認

PKI は公開鍵暗号を基礎にありますが、公開鍵暗号の安全性は時間的に有限とされています。例えば 1024 ビットの RSA 暗号を用いる場合は 2 ~ 3 年程度の安全期間を前提に運用されることが多いでしょう。単純な情報交換やある時点での資格認証には問題がありませんが、保存された情報の署名の有効性を長期にわたって確認する必要がある場合には問題が生じます。法的に保存が義務付けられた情報は 3 ~ 5 年、あるいはそれ以上の間、真正性を保って保存しなければなりません。例えば 2 年の寿命の公開鍵暗号を用いる場合、公開鍵が作成され証明書が発行された直後に署名を行っても、その署名が確認できる、つまり PKI で真正性が保証されるのは高々 2 年です。したがって PKI を利用して電子保存の真正性を求める場合は工夫が必要です。

1 つは署名そのものの有効期間を延長する方法です。簡単に言えば有効期間が切れる前に新しい私有鍵と公開鍵証明書を作成し、再署名します。この方法は単純ですが、署名者ごとに署名の有効期間を管理し、再署名を依頼する必要があります。個別に再署名する限り、ほとんど不可能と考えてよいでしょう。システムで自動的に再署名する方法も考えられますが、私有鍵にシステムがアクセスできる必要があります。署名の否認不能性に影響を与えます。

2 つ目は署名の確認者を置く方法です。例えばすべての署名は有効期間が 1 ヶ月以上ある私有鍵および公開鍵証明書を用いて行うことと決めておき、その時点で確認されていないすべての署名を一ヶ月に一度確認します。そして有効であった署名のなされた情報のリストを作り、そのリストに確認者が署名を行います。これを確認済みリストとし、さらに確認者の署名の有効期間が過ぎる前に確認済みリストの署名確認を行い、そのリストを作成し、署名を行います。これを何度か繰り返せば一定期間の真正性は確認者の信頼性のもとに保証されます。

2 つ目の方法の応用として、確認リストを作成した時点で機能上および運用上で改ざん不可能な媒体（例えば第三者が監査可能な金庫保管した CD-ROM など）に固定して厳重に管理することも可能です。

いずれにしても単純に電子署名をしたから長期の保存の真正性が確保されると考えてはいけません。

2 - 7 . タイムスタンプ

電子署名によって署名時点での真正性が証明可能であり、また前節にのべたような工夫を行えば一定期間の真正性も確保できると説明しましたが、保健医療福祉分野の場合、情報が作成された時刻や、順番が重要です。虫垂炎と診断した時点と虫垂炎の手術を行った時点がこの順か、逆の順かで大きく意味が変わってきます。したがって一般に保健医療福祉分野では電子署名を行った時刻が大変重要で、信頼性のある時刻情報を付加する必要があります。訴訟等で証明力を確保しようと思うと、時刻の信頼性は第三者にとっても信頼できるものでなければなりません。本ガイドラインでも第 7 章でタイムスタンプについて述べていますが、基本的にはすべての署名にタイムスタンプがあることが求められます。

第三者に信頼される時刻情報を付加するためにはタイムスタンプ発行機関は保健医療福祉機関から独立した信頼できる第三者機関（Trusted Third Party : TTP）が行うことが理想ですが、しっかりした監査によって信頼性が説明可能であれば、保健医療福祉機関内部やそのグループ内に置くことも可能です。

3 . 公開鍵証明書と証明書失効リストのプロファイル

3 - 1 . 全体的な方針

保健・医療・福祉分野での公開鍵証明書プロファイルは ITU-T X.509 推奨規格第 3 版に準拠するものとし、すなわち RFC2459 に規定されているプロファイルに従うものとします。ITU-T X.509 推奨規格は RFC2459 以外にも ISO/IEC9594-8 として登録されていますが、このガイドラインで参照した文書は RFC2459 です。このガイドラインでは日本の保健・医療・福祉分野で公開鍵基盤を用いるための制限や追加項目を中心に記載しています。実装に際しては必ず RFC2459 を参照してください。また原則として ISO TS 17090 に準拠しています。

3 - 2 . 文字コードセット

名前などの文字コードセットは RFC2459 で PrintableString, BMPString および UTF-8String を使用することが定められています。(2003 年以降は UTF-8String のみ。) したがって Subject フィールド等において UTF-8 で許される範囲の多バイトコードを使用することができます。しかし実装を容易にするために、また国際的な互換性に配慮して、基本領域では多バイト文字コードを使用しないこととします。さらに RFC2459 であらかじめ定義されている拡張領域で、subjectAltName 以外のフィールドでは多バイト文字コードを使用しないこととします。また subjectAltName 拡張フィールド、および後述する RFC2459 で定義されていない拡張フィールドで多バイト文字コードを用いる場合は UTF-8 を使用することとします。

3 - 3 . 公開鍵証明書の基本領域

3 - 3 - 1 . version

version フィールドの値は 2 とします。これは X.509 version 3 に準拠していることを示します。

3 - 3 - 2 . serialNumber

公開鍵証明書のシリアル番号です。証明書発行局の中で一意で、再使用しません。

3 - 3 - 3 . signature

signature フィールドには証明アルゴリズムの OID を格納します。ISO TS 17090 および日本の電子署名法に関連した「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」では次の 6 つのアルゴリズムが示されています。

1. md5WithRSAEncryption (1.2.840.113549.1.1.4)
2. sha1WithRSAEncryption (1.2.840.113549.1.1.5)

3. **dsa-with-sha1 (1.2.840.10040.4.3)**
4. **ecdsa-with-sha1 (1.2.840.10045.4.1)**
5. **sha1WithESIGNSignature (0.2.440.5.5.3.4)**
6. **md5WithESIGNSignature (0.2.440.5.5.3.3)**

暗号技術の進歩により、新しいアルゴリズムが開発される可能性はあり、また既存のアルゴリズムに欠点が発見される可能性があります。したがってこのガイドラインではアルゴリズムを規定しません。しかし現時点での互換性を考えれば、少なくとももっとも広く用いられている上記の2は実装しておくことが推奨されます。

3 - 3 - 4 . issuer

Issuer フィールドには証明書発行者の名前が入ります。名前は Directory Information Tree 構造に従った Distinguish Name (DN)を使用することとされており、ISO TS17090 ではディレクトリのエントリとして CountryName, LocalityName, OrganizationName, OrganizationUnitName, CommonName を挙げています。この中で CountryName と CommonName は必須です。このツリー構造の名前は証明書発行局が一意に特定できる必要がありますが、証明書発行局の一意性は X.509 の規定上は保障する手段がありません。したがって互換性を考慮する範囲で運用上、一意になるように定める必要があります。また再利用してはいけません。CountryName は国名が入りますが、この属性は必須とし、ISO の 2 文字の国名識別子を用いることとします。日本は JP です。LocalityName, OrganizationName, OrganizationUnitName はいずれもオプションですが、このいずれか1つまたはいずれかの組み合わせで、証明書発行局を一意に特定できる名前を格納します。CommonName は必須で、証明書発行局のポリシーを端的に示す文字列を格納しますが、その先頭に “MD-HPKI-XX” を付加するものとします。“XX” は “01” です。これはこの証明書がこのガイドラインに準拠していることを示します。またこのガイドラインが改定された場合には準拠している証明書の “XX” の値が変わります。

3 - 3 - 5 . validity

公開鍵証明書の有効期間です。終了期限が 2049 年末までの場合は UTCTime 形式で表示し、グリニッジ標準時を使用します (YYMMDDhhmmssZ)。分単位までの表示も許されますが、2050 年以降と変化を少なくする意味で秒単位まで表示することとします。2050 年以降は GeneralizedTime 形式を使用します。(YYYYMMDDhhmmssZ)

3 - 3 - 6 . subject

Subject には証明書所有者の名前が入ります。名前は Directory Information Tree を使用することとされており、ISO TS17090 ではディレクトリのエントリとして CountryName, LocalityName, OrganizationName, OrganizationUnitName, CommonName, SurName,

GivenName, e-mail を挙げています。この中で CountryName は必須で、3 - 3 - 3 と同様の国名コードを格納します。日本は JP です。また CommonName は必須で、所有者がヒトである場合、電子署名法に適応するためには所有者の氏名（ローマ字表記）を含む必要があります。同様に所有者が法人である場合、法人名（ローマ字表記）を含む必要があります。また CommonName の値は同じ証明書発行局の発行する証明書の中で対象を一意に示すものとし、同姓同名の可能性があるので、氏名に資格登録番号のような ID 番号を付加することが求められます。対象が一意に決まるということは CommonName に同じ値を再利用するのは証明書の更新を行う場合だけということです。LocalityName, OrganizationName, OrganizationUnitName はオプションで使用目的を規定しません。SurName はオプションですが存在する場合は日本の姓名の「姓」に相当する値を格納します。GivenName はオプションですが存在する場合は日本の姓名の「名」に相当する値を格納します。E-mail はオプションですが、存在する場合は電子メールアドレスを 1 つ格納します。

3 - 3 - 7 . subjectPublicKeyInfo

証明書所有者の公開鍵のアルゴリズム識別子と公開鍵を格納します。アルゴリズム識別子は OID で指定します。ISO TS 17090 および日本の電子署名法に関連した「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」では次の 4 つのアルゴリズムが示されています。

1. RSAEncryption (1.2.840.113549.1.1)
2. id-dsa (1.2.840.10040.4.1)
3. id-ecdsa (1.2.840.10045.2.0)
4. id-ESIGN (0.3.4401.5.3.3.2)

署名アルゴリズムと同様で、このガイドラインではアルゴリズムを規定しません。しかし現時点での互換性を確保するために、少なくとももっとも広く用いられている上記の 1 は実装しておくことが推奨されます。

3 - 3 - 8 . issuerUniqueIdentifier

このフィールドは使用しません。

3 - 3 - 9 . subjectUniqueIdentifier

このフィールドは使用しません。

3 - 4 . 公開鍵証明書の一般的な拡張領域(RFC2459)

3 - 4 - 1 . authorityKeyIdentifier

証明書発行局の公開鍵証明書を厳密に識別するための情報を格納します。keyIdentifier, authorityCertIssuer, authorityCertSerialNumber の3つのサブフィールドからなりますが、本ガイドラインでは keyIdentifier だけを使用します (ISO TS17090)。keyIdentifier は証明書発行局の公開鍵を SHA-1 ハッシュした値とします。AuthorityKeyIdentifier フィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3 - 4 - 2 . subjectKeyIdentifier

証明書所有者の公開鍵を厳密に識別するための情報を格納します。所有者公開鍵を SHA-1 ハッシュした値を格納します。このフィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3 - 4 - 3 . keyUsage

所有者公開鍵の使用目的を示すフィールドです。データはビットストリングで、

digitalSignature (0)

nonRepudiation (1)

keyEncipherment (2)

dataEncipherment (3)

keyAgreement (4)

keyCertSign (5)

CRLSign (6)

EncipherOnly (7)

DecipherOnly (8)

以上の9つが RFC2459 で定義されています。それぞれの属性は RFC2459 を参照してください。このフィールドは必須で、かならず値が必要です。また保健・医療・福祉分野で、Subject が人や組織の場合で法的に有効な署名に用いる場合は nonRepudiation 以外のビットをオンにしないこととします。またそれ以外の署名に用いる場合も digitalSignature と nonRepudiation 以外のビットをオンにしないこととします。(電子署名法)

3 - 4 - 4 . extendedKeyUsage

keyUsage 以外の公開鍵の使用目的を示します。subject が人または組織で、keyUsage で nonRepudiation または digitalSignature を指定した場合、このフィールドを使わないことが推奨されます。(電子署名法)

このフィールドはオプションです。

3 - 4 - 5 . privateKeyUsagePeriod

このフィールドは証明書更新の祭に一定期間古い署名の検証を可能とするために使用しますが、実装しているクライアントソフトウェアが少なく、使用しないほうがよいでしょう。このフィールドはオプションです。

3 - 4 - 6 . **certificatePolicies**

証明書発行局の証明書発行ポリシーの OID を格納します。このフィールドは必須で、本ガイドラインに付属するポリシーの OID を格納していることが推奨されます。つまり証明書発行局はこのガイドラインに付属するポリシーで運用されることを推奨します。

このフィールドをクライアントが解釈できるかどうかは任意です。

3 - 4 - 7 . **policyMappings**

証明書発行局の公開鍵証明書以外では使用しません。このフィールドはオプションです。

3 - 4 - 8 . **subjectAltName**

証明書所有者の別名を格納します。多バイト文字コードの名前を使用する場合はここに格納します。このフィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3 - 4 - 9 . **issuerAltName**

使用しません。

3 - 4 - 10 . **subjectDirectoryAttributes**

証明書所有者の属性を格納できます。RFC2459 では一般的な目的で使用することは推奨されていませんが、後述の `hcRole attribute` に限って使用することとします。それ以外の `attribute` を含めてはいけません。

3 - 4 - 11 . **basicConstraints**

証明書発行局の公開鍵証明書以外では使用されません。証明書発行局の公開鍵証明書では必須であり、値が必要です。

3 - 4 - 12 . **nameConstraints**、**policyConstraints**

この2つのフィールドは証明書発行局の公開鍵証明書以外では使用されません。これらのフィールドはオプションです。

3 - 4 - 13 . **CRLDistributionPoints**

CRL の配布点または参照点を示します。このフィールドは OCSP レスポンダを利用しな

い限り必須です。OCSP レスポンダを採用する場合は使用しません。

互換性を考慮する場合、インターネット上で最も汎用的なプロトコルである HTTP をサポートするのが望ましいため、CRL を Web サーバに格納し、CRLDistributionPoints の値をその URL とすることを推奨します。また、ISO/TS17090 では OCSP レスポンダ (authorityInformationAccess) について明確な規定がないため、本フィールドが必須になっていますが、OCSP レスポンダを採用する場合は本フィールドの代わりに authorityInformationAccess フィールドに OCSP レスポンダのアドレスを記載します。

3 - 4 - 14 . authorityInformationAccess

CA に関する情報を取得する方法と場所を記載することができますが、このガイドラインでは OCSP (Online Certificate Status Protocol : RFC2560) レスポンダを使用する場合に OCSP レスポンダのアクセス方法とアドレスを記載します。それ以外の用途には使いません。このフィールドは OCSP レスポンダを採用していない場合は使用しません。

3 - 5 特別な (RFC2459 で定義されていない) 拡張

3 - 5 - 1 hcRole attributes

拡張フィールドの定義ではなく、subjectDirectoryAttributes の属性の 1 つとして保健医療福祉分野で役割および職種などの属性を指定する目的で定義します。hcRole Attribute のフォーマットは ISO TS 17090 に準拠しますが、当分の間、国家資格である保健・医療・福祉分野の職名だけを使用し、Attribute の値は PrintableString で表現するものとします。なお、hcRole 属性自体の OID は ISO TS 17090 で定義されたものを使用します。今後、保健・医療・福祉分野のわが国の職種が体系的に定義され、OID を取得することが必要で、これらが整備された時点で hcRole の使用方法については再検討が必要と考えられます。

当面 hcRole で使用できる値

Medical Doctor	医師
Dentist	歯科医師
Pharmacist	薬剤師
Medical Technologist	臨床検査技師
Radiological Technologist	診療放射線技師
General Nurse	看護師
Public Health Nurse	保健師
Midwife	助産師
Physical Therapist	理学療法士
Occupational Therapist	作業療法士

Orthoptist	視能訓練士
Speech Therapist	言語聴覚士
Dental Technician	歯科技工士
National Registered Dietitian	管理栄養士
Certified Social Worker	社会福祉士
Certified Care Worker	介護福祉士
Emergency Medical Technician	救急救命士
Psychiatric Social Worker	精神保健福祉士

3 - 5 - 2 qualifiedCertificateStatements

証明する内容が公的に認められたものであることを示すための拡張フィールドで、ISO TS17090 で記載されています。しかし、Qualified Certificate 自体は RFC3039 で定義されており、単純に拡張フィールドを 1 つ追加するだけで実装するには無理がある。TS17090 の記載も不十分でこのままでは実装困難である。したがってこのガイドラインでは使用しないこととします。

3 - 6 . 証明書失効リストプロファイル

RFC2459 に準拠します。

	CAの証明書	国家資格のSP	その他のSP	非専門職	サービス受給者	医療機関(組織)	
version	C	C	C	C	C	C	
serialNumber	C	C	C	C	C	C	
signature	C	C	C	C	C	C	
issuer	C	C	C	C	C	C	
validity	C	C	C	C	C	C	
subject	C	C	C	C	C	C	
subjectPublicKeyInfo	C	C	C	C	C	C	
issuerUniqueID	N	N	N	N	N	N	
subjectUniqueID	N	N	N	N	N	N	
authorityKeyID	M	M	M	M	M	M	
subjectKeyID	M	M	M	M	M	M	
keyUsage	C	C	C	C	C	C	
extendedKeyUsage	N	O	O	O	O	O	
privateKeyUsagePeriod	O	O	O	O	O	O	
certificatePolicies	M	M	M	M	M	M	
policyMappings	M	N	N	N	N	N	
subjectAltName	M	M	M	M	M	M	
issuerAltName	N	N	N	N	N	N	
subjectDirectoryAttributes	N	C	O	O	O	O	
hcRole	N	C	N	N	N	N	ISO TS17090
basicConstraints	C	N	N	N	N	N	
nameConstraints	O	N	N	N	N	N	
policyConstraints	O	N	N	N	N	N	
CRLDistributionPoints	M	M	M	M	M	M	
authorityInformationAccess	O	O	O	O	O	O	
qualifiedCertificateStatements	N	N	N	N	N	N	ISO TS17090

C：必須でクライアントが解釈できることが必要。M：必須だがクライアントは解釈できるかどうかは任意。O：必須ではないが実装してもよい。N：使用しない。SP 専門職

4 . 属性証明書のプロファイル

4 - 1 . 全体的な方針

このガイドライン作成時点で属性証明書は RFC ではなく、IETF Internet draft で、`draft-ietf-ac509prof-09.txt` として参照可能です。このガイドラインではこの Internet draft に準拠することとします。このガイドラインで述べるのは原則として `draft-ietf-ac509prof-09.txt` で記述されている事項以外に日本の保健・医療・福祉分野で公開鍵基盤を用いるための制限や追加項目です。実装に際しては `draft-ietf-ac509prof-09.txt` を参照してください。

4 - 2 . 文字コードセット

公開鍵証明書と同様に `PrintableString`、`BMPString`、`UTF-8String` を使用することができますが、`Attributes` 以外では多バイト文字コードを使用しないこととします。`Attributes` もできるだけ多バイト文字コードを使用しないことが推奨されます。

4 - 3 . 属性証明書の基本的なフィールド

4 - 3 - 1 . `version`

`version` フィールドの値は 1 です。これは v2 であることを示しています。

4 - 3 - 2 . `holder`

`holder` は属性証明書の所有者を示します。`draft-ietf-ac509prof-09.txt` では `baseCertificateID`、`entityName`、`objectDigestInfo` の 3 つのオプションのうち、1 つが存在することになっていますが、保健・医療・福祉分野では `baseCertificateID` だけを用いることとします。`BaseCertificateID` は所有者の PKC の `issuer` と `serial number` からなります。`draft-ietf-ac509prof-09.txt` では `issuer UniqueIdentifier` もオプションで使用可能ですが、このガイドラインでは使用しないこととします。`BaseCertificateID` を用いる場合、AC は常に PKC とペアで使用する必要があります。

4 - 3 - 3 . `issuer`

属性証明書の発行者を示します。V1Form と V2Form があり、V2Form を用いることになっています。V2Form は `issureName`、`baseCertificateID`、`objectDigestInfo` の 3 つのオプションから 1 つを選択することになっていますが、`issuerName` を使用することとします。`issuerName` のフォーマットは PKC の `issuer` と同じ形式です。すなわち、ディレクトリのエントリとして `CountryName`、`LocalityName`、`OrganizationName`、`OrganizationUnitName`、`CommonName` が使用可能で `CountryName` と `CommonName`

は必須です。CountryName は国名が入りますが、この属性は必須とし、ISO の 2 文字の国名識別子を用いることとします。日本は JP です。LocalityName, OrganizationName, OrganizationUnitName はいずれもオプションですが、このいずれか 1 つまたはいずれかの組み合わせで、証明書発行局を一意に特定できる名前を格納します。

CommonName は必須で、証明書発行局のポリシーを示す文字列を格納しますが、その先頭に “ MD-HPKI-XX ” を付加するものとします。“ XX ” は “ 01 ” です。これはこの証明書がこのガイドラインに準拠していることを示します。またこのガイドラインが改定された場合には準拠している証明書の “ XX ” の値が変わります。

4 - 3 - 4 . signature

属性証明書発行者の電子署名のアルゴリズムを示します。PKC の signature と同じです。

4 - 3 - 5 . serialNumber

属性証明書のシリアル番号です。属性証明書発行局の中で一意の番号であり、再使用しません。

4 - 3 - 6 . attrCertValidityPeriod

属性証明書の有効期間を示します。PKC の有効期間と同じ形式ですが、一般に短く設定されます。

4 - 3 - 7 . attributes

attributeType と attributeValue からなり、1 つの属性証明書では attributeType はユニークです。つまり同じ attributeType の attributes は 1 つしか書けません。ただし 1 つの attributeType に対して attributeValue は複数あってもかまいません。attributeType は OID を用いますが、当面は draft-ietf-ac509prof-09.txt で定義されている attributeType だけを用いるものとします。attributeValue は UTF-8 string を用いることができますが、可能な限り多バイト文字は使用しないこととします。

attributeValue で汎用性のあるものは登録制にして、将来の OID 化に備える必要があります。

4 - 3 - 8 . issuerUniqueID

属性証明書発行局を一意に指定する ID ですが、このフィールドは使用しません。

4 - 4 属性証明書一般的な拡張フィールド

属性証明書には次の6つの拡張フィールドを使用することができます。ただし、すべてオプションで必須ではありません。したがって特定のドメインでいずれかの拡張フィールドを用いる場合はドメイン内で仕様の整合性をはかる必要があります。

4 - 4 - 1 Audit Identity

holder と **Audit** の対象者が異なる場合に使用することができます。これを用いる場合は値がなければいけません。

4 - 4 - 2 AC Targeting

属性証明書が有効な対象システムまたはプロトコルを指定します。このフィールドが存在し、クライアントが対象に含まれない場合、クライアントは属性証明書を拒否しなければなりません。このフィールドを使用する場合は値がなければいけません。

4 - 4 - 3 Authority Key Identifier

発行者の公開鍵の識別子を格納します。PKC の **KeyIdentifier** と同じです。値は空でもかまいません。

4 - 4 - 4 Authority Information Access

発行者の情報のアクセス方法とアドレスを指定します。このガイドラインでは OCSP レスポンダのアクセス方法とアドレスを指定する以外には使用しません。値は空でもかまいません。

4 - 4 - 5 CRL Distribution Points

証明書失効リストのアクセス方法を指定します。PKC と同様です。属性証明書の一般的な運用では有効期間を短く設定するために CRL を使用しなくてよい場合が多いことに注意してください。値は空でもかまいません。

4 - 4 - 6 No Revocation Available

証明書失効リストが存在しないことを示すフィールドで値は常に **NULL** です。このフィールドが存在すれば CRL はありません。

5 . 証明書発行局の運用とポリシー

保健医療福祉分野で公開鍵証明書が広範囲で利用できるためには証明書発行局のポリシーが一致している必要があります。本ガイドラインでは署名と資格認証に用いる証明書を発行する証明書発行局のポリシー（付録2）を作成し、OID を定めています。本ガイドラインに準拠する署名および資格認証に用いる公開鍵証明書を発行する証明書発行局はこのポリシーを採用しなければいけません。CPS はこのポリシーに矛盾しない限り自由に定めることができます。また付録3の PKI Disclosure Statement (PDS)も採用し公開することが推奨されます。

6 . 証明書発行局連携

公開鍵証明書は証明書発行局（CA）が複数ある場合、信頼性の連携を行うためには何らかの方法で CA 間の信頼性の伝達が必要になります。信頼性を伝達する方法には3つの方法がよく知られています。

1つ目は、1つの Root CA から樹状に CA を配置し、基本的なポリシーを共有する方法です。このような証明書を受け取ったクライアントは証明書を Root CA の方向にたどり、信頼している Root CA に行き着けば、その証明書自体を信頼します。

2つ目は Bridging CA を用いる方法で、Bridging CA はそれぞれの CA に対して証明書を発行します。Bridging CA が信頼できればそれが証明している CA はすべて信頼できることとなります。

3つ目は Cross Certificate で、信頼性を伝達したい CA が相手の CA に証明書を発行します。相互に発行する場合があります。

1つ目の方法は3つ目の方法の特殊な形と考えることもできます。いずれの方法にも欠点と長所があり、本ガイドラインでは特に規定したり推奨したりしません。実際に証明書連携が必要な場合が起こったときに改定の上、言及することとします。

7 . 時刻認証機構

7 - 1 . Time Stamp Protocol (RFC3161)について

診療情報の大部分は法的に保存義務があり、また証拠性が求められます。一連の情報は時系列にしたがって因果関係や従属関係があることが多く、時刻および時系列は重要です。したがって信頼できる時刻情報を情報に付属させることは重要で、そうすることによって証拠性や証明力の増加が期待できます。信頼できる時刻情報を付加することを時刻認証と呼びます。時刻認証の方法はいくつか存在し、信頼性が説明できるものであればどれを利用してかまいませんが、PKI の応用として Time Stamp Protocol (RFC3161)があります。

これは Time Stamp Authority を用い、クライアントから送られる情報のハッシュを含むリクエストに対して、時刻情報を付加し、署名をおこなって返すサービスで、Time Stamp Authority さえ信頼できれば構築も容易であり、十分な信頼性を持つものです。本ガイドラインでは TSP の使用を推奨します。

RFC3161 にはいくつかの選択可能なオプションがあり、実装の仕方によっては互換性のない Time Stamp Token ができます。したがって本ガイドラインでは推奨する選択を含めて TSP の詳細を定めることとします。

7 - 2 . TSA の公開鍵証明書

TSA の公開鍵証明書の形式は本ガイドライン 3 章に従いますが、3 - 4 - 4 の extendedKeyUsage フィールドは必須で、その値は id-kp-timestamping (OID: 1.3.6.1.5.5.7.3.8) です。

7 - 3 . ハッシュアルゴリズム

ハッシュアルゴリズムは規定しませんが、現時点では SHA-1 と MD5 を使用するべきで、SHA-1 はかならず実装することを推奨します。

7 - 4 . nonce

nonce は使用することとし、64 ビットの整数を使用することとします。nonce が偶然重ならないように、擬似乱数を用います。

7 - 5 . extensions フィールド

タイムスタンプ要求メッセージおよび応答メッセージでは extensions フィールドは使用しないこととします。

7 - 6 . accuracy フィールド

タイムスタンプ応答メッセージで、accuracy フィールドは必ず存在するものとします。Accuracy は 1 秒以下でなければなりません。accuracy の値は実測値ではなく、1 秒としてもかまいません。

7 - 7 . ordering フィールド

タイムスタンプ応答メッセージで、ordering フィールドは必ず存在し、値は true でも false でもかまいません。つまり Timestamp Client は ordering フィールドの値が false でも、その Timestamp を無効と判断してはいけません。

7 - 8 . タイムスタンプ応答メッセージの電子署名

タイムスタンプ応答メッセージの電子署名のアルゴリズムは規定しませんが、現状では sha-1withRSAencryption を用いることを推奨します。

7 - 9 . Time Stamp Policy, TSA Practice Statement, TSA Disclosure Statement

タイムスタンププロトコルでは Time Stamp Policy を OID で指定し、要求に含めることで、共通の方針を確認することができます。小規模な実験などでは policy を指定しなくても運用は可能ですが、他分野との共用や、逆に一定の基準を満たした Time Stamp を使用することを保証するためには policy を活用することが求められます。

近い将来、保健医療福祉分野で用いる Time Stamp Protocol 用に policy を作成し、その OID を公開する予定です。

また TSA は policy の実現方法やサービス利用の具体的な手順を記載した TSA Practice Statement および、利用者に関連する部分だけを簡明に記述した TSA Disclosure Statement を用意し公開することを推奨します。

7 - 10 . 伝送方法

RFC3161 ではタイムスタンプメッセージの伝送方法は規定されていませんが、このガイドラインでは少なくとも http をサポートすることを推奨します。インターネットのような汎用経路を通過する場合は SSL/TLS を用いることを推奨します。

8 . 権限管理への応用例

保健医療分野においては、診療行為をはじめとして、診断書、処方箋の発行、各種患者情報へのアクセスなど、ほとんどあらゆる事象に際して、利用者の身元確認（本人確認）と同時に、利用者の資格や属性の確認が要求される。利用者の本人性や資格、属性によって、行為の遂行や情報へのアクセスを許可あるいは制限することを権限管理とよぶ。

ネットワーク化社会において、本人確認は PKI を利用して行うことができる。ここでは、この PKI をさらに権限管理に応用して、利用者認証と権限管理を統一的行う方法について説明する。

8 . 1 . PKI を応用した権限管理の方法

PKI を応用した権限管理は、1) 公開鍵証明書に記載された本人性に基づく方法、2) 公開鍵証明書に記載された属性(hcRole)に基づく方法、3) 属性証明書に記載された属性に基づく方法、がある。いずれの場合も、本人性あるいは属性とそれに対して許可あるいは制限される権限との対応付け（アクセス制御リスト、アクセス制御マトリクスなど）が必要である。以下にそれぞれの方法の特徴について説明する。

1) 公開鍵証明書に記載された本人性に基づく方法

個人単位でのきめ細やかな権限管理が可能。一方で、アクセス制御リストは長大となり、また、担当医が変わることなどに頻繁な変更が必要となり、管理が煩雑となる。

2) 公開鍵証明書に記載された属性(hcRole)に基づく方法

公開鍵証明書のみで本人確認と属性確認が可能である。アクセス制御リストは短く、また更新も少ないと考えられる。一方で、個人の属性が公開される、属性の変更に際して公開鍵証明書の破棄、再発行を伴うなどの問題点がある。さらに、公開鍵証明書の発行者と資格などの属性の付与者が異なる場合の対応が難しい。

3) 属性証明書に記載された属性に基づく方法

職位や所属などをその管理者が独自に属性証明書として認証する方法で、比較的きめ細やかな権限管理が可能である。アクセス制御リストは比較的短く、また更新も少ないと考えられる。一方で、属性認証局の運用や属性証明書の発行、破棄などに伴うコストが発生する。

8 . 2 . 保健医療分野での権限管理のユースケース

ここでは、保健医療分野において、権限管理が必要とされている事例をユースケースとして例示する。保健医療分野で権限管理は、主としてオーダ、診断書、処方箋などの電子署名を必要とする文書の作成と確認、および、診療情報の閲覧に際して重要である。

8.2.1. 電子署名を必要とする文書の作成と確認

8.2.1.1. アクタ

電子署名を必要とする文書を作成する際には、その責任の所在を明確にし、その実行時に作成者を確認し、文書を作成する権限のあったことを検証する必要がある。電子署名付き文書交換でのアクタとは、それ自身の責務においてある文書に署名し、発行できる役割を有する個人あるいはエンティティをいう。想定されるアクタは以下のとおりである。

1) 医療受給者

患者、保護者、代理人、身元引受人、など

2) 医療供給者

医師、歯科医師、看護師、薬剤師など

3) 機関

医療機関、保健所、厚生省、保険支払基金、保険会社、検査会社など

8.2.1.2. 電子署名を必要とする文書

電子署名を必要とする文書は、作成者によって以下のとおりに分類される。

1) 医療受給者が作成する文書

外来予約、入院承諾書、手術承諾書、カルテ開示要求など

2) 医療供給者が作成する文書

診療情報提供書、診断書、処方箋、診断レポート、外注検査依頼など

3) 機関が作成する文書

検査結果報告、診療報酬請求、各種届出、各種統計調査、診断書要求、保険資格確認など

8.2.1.3. 情報交換のタイミング

情報交換のタイミングは、インターネット上での情報交換という観点から、コネクションレス型とトランザクション型に分類することができる。コネクションレス型の情報交換では、実質的に情報の送信のみで、そのレスポンスは存在しない。トランザクション型の情報交換では、情報の送信が発生するとそれに応じた一連の文書交換が発生する。

1) コネクションレス型

入院承諾書、手術承諾書、診療情報提供書、診断書、診断レポート、外注検査依頼、検査結果報告、各種届出

2) トランザクション型

外来予約、カルテ開示要求、処方箋、診療報酬請求、各種統計調査、診断書要求、保険資格確認

8.1.1.4. 電子署名の検証

電子署名の確認に際して、電子署名の検証のみを行えばよい場合（本人認証）とその属性を確認（属性認証）しなければならない場合とがあると考えられる。

1) 本人認証のみ

外来予約、入院承諾書、手術承諾書、カルテ開示要求、外注検査依頼、診療報酬請求、各種届出、各種統計調査、診断書要求、保険資格確認

2) 属性認証

診療情報提供書、診断書、処方箋、診断レポート

8.1.1.5. トップレベルユースケース

以上をまとめると、電子署名を必要とする文書の作成と確認のトップユースケースは大まかに以下の4種類に分類されると考えられる。

8.1.1.5.1. コネクションレス型-本人認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

8.1.1.5.2. コネクションレス型-属性認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

受信者は、送信者の属性認証を行う。

8.1.1.5.3. トランザクション型-本人認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

受信者は、レスポンスに電子署名を付与し、送信者に返送する。

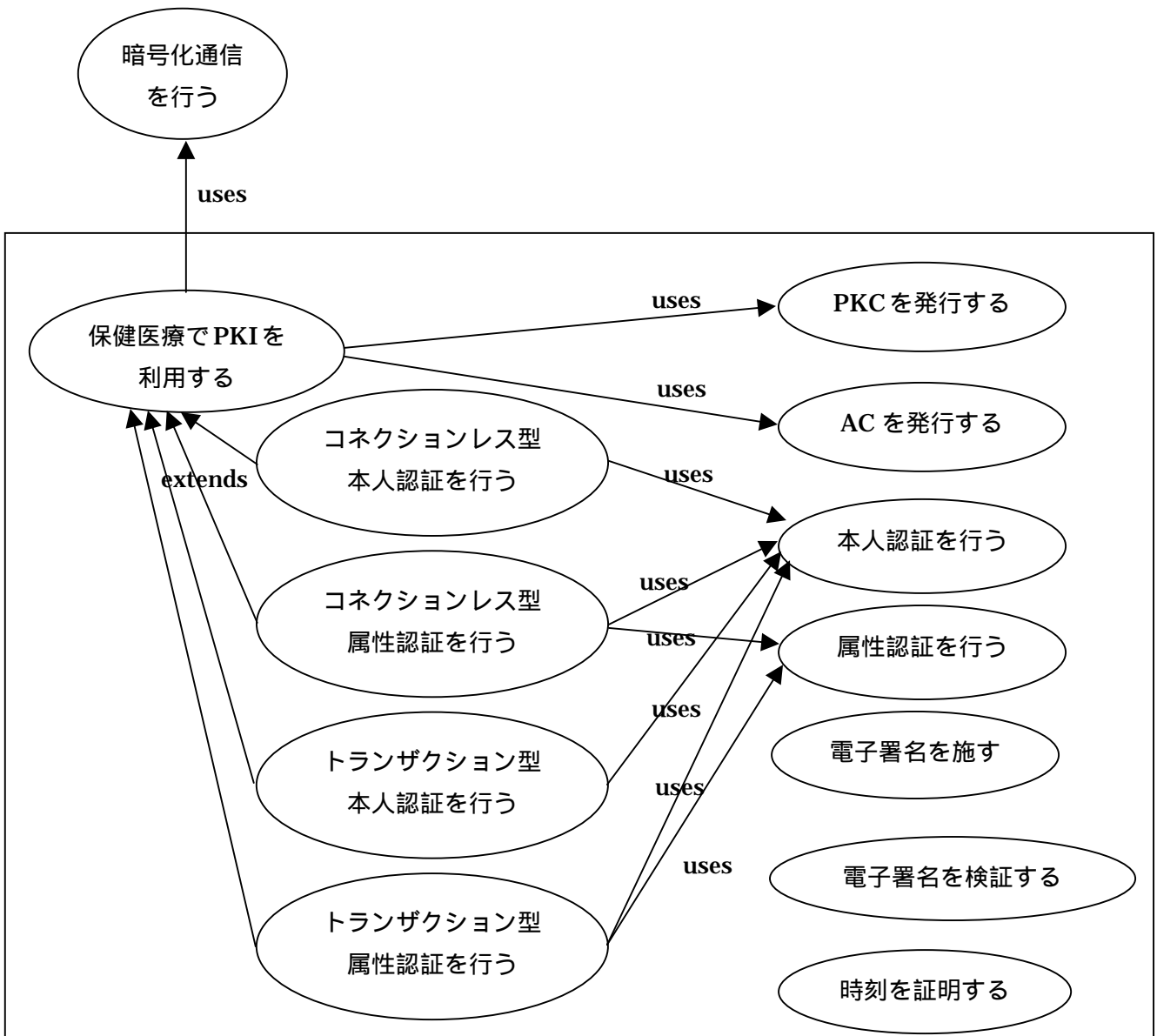
8.1.1.5.4. トランザクション型-属性認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

受信者は、送信者の属性認証を行う。

受信者は、レスポンスに電子署名を付与し、送信者に返送する。



8.2.2. 診療情報の閲覧

8.2.2.1. アクタ

診療情報を閲覧するアクタは現在のところ、医療供給者（医師、歯科医師、看護師、薬剤師など）が中心であると考えられる。今後、医療受給者本人がインターネットを介して自宅から自分の診療情報にアクセスするようなケースも想定されるが、これは、医療供給者の利用者別の権限管理と同様に考えることができる。

8.2.2.2. アクセス制限対象の診療情報の単位

アクセスを制限する診療情報の単位は、プロブレムリストや検査結果といった一塊の診療

情報であることが多いが、時には、個別の病名や特定の人名に関してのみ、アクセス制限を必要とする場合もある。

8.2.2.3. 閲覧制限のタイミング

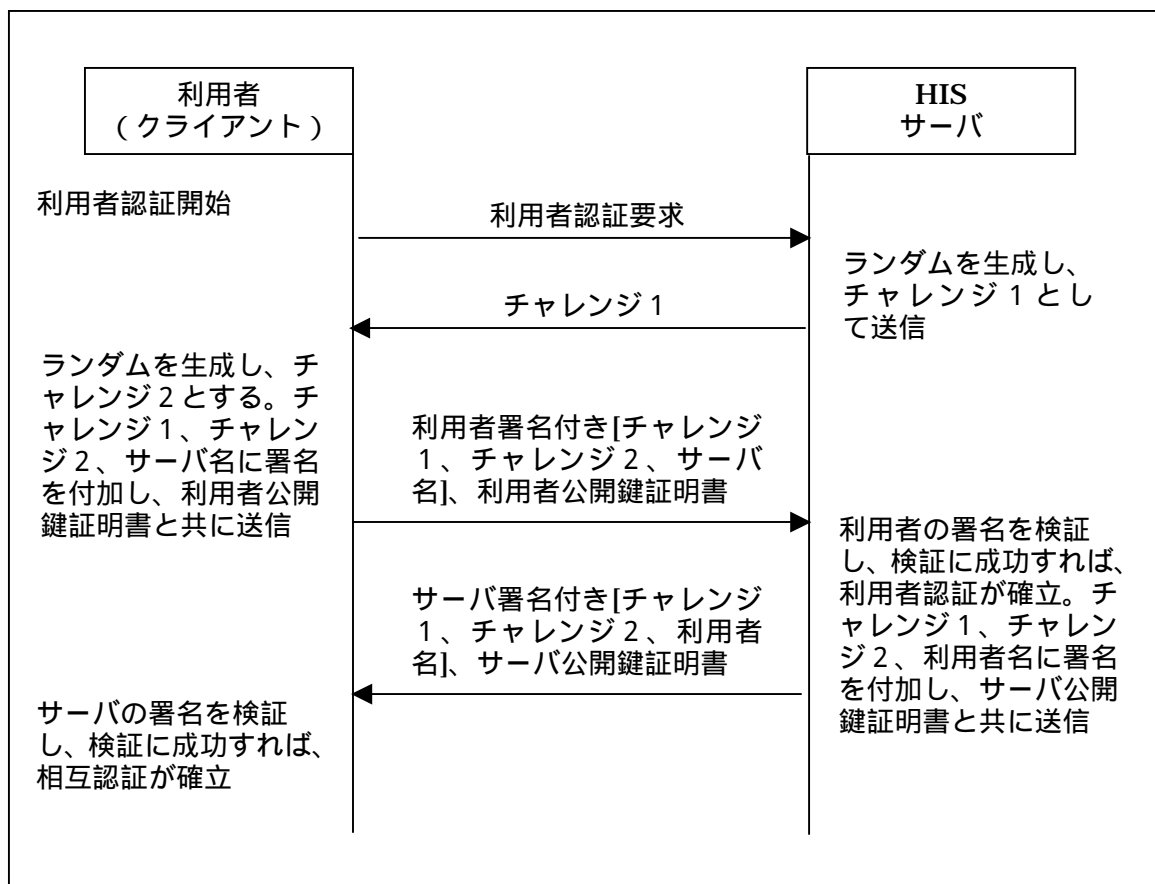
診療情報の閲覧制限は、診療情報サーバが診療情報を送信する際に送信内容を制限する方法と、クライアントシステムが受信した診療情報を利用者の権限に即して表示を制限する方法とがある。現状ではクライアントサイドでの閲覧制限も見られるが、セキュリティ上の観点からは、サーバサイドでの閲覧制限が望ましい。

8.2.2.4. トップレベルユースケース

診療情報の閲覧制限に関する権限管理のトップユースケースは大まかに以下の3種類に分類されると考えられる。

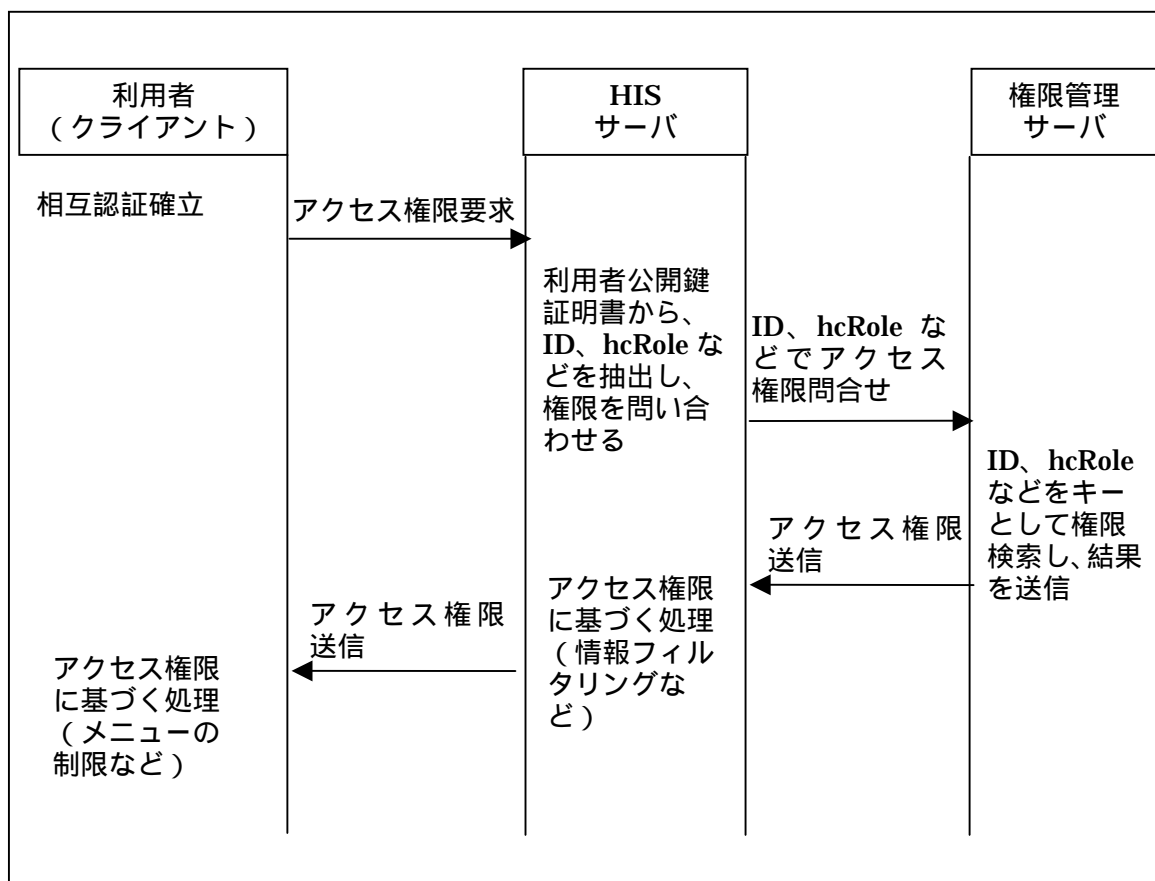
8.2.2.4.1. 公開鍵証明書に記載された本人性に基づく閲覧制限

本人確認が行われた後、個人ごとのアクセス制御リストに記述された項目について閲覧の許可、制限を行う。



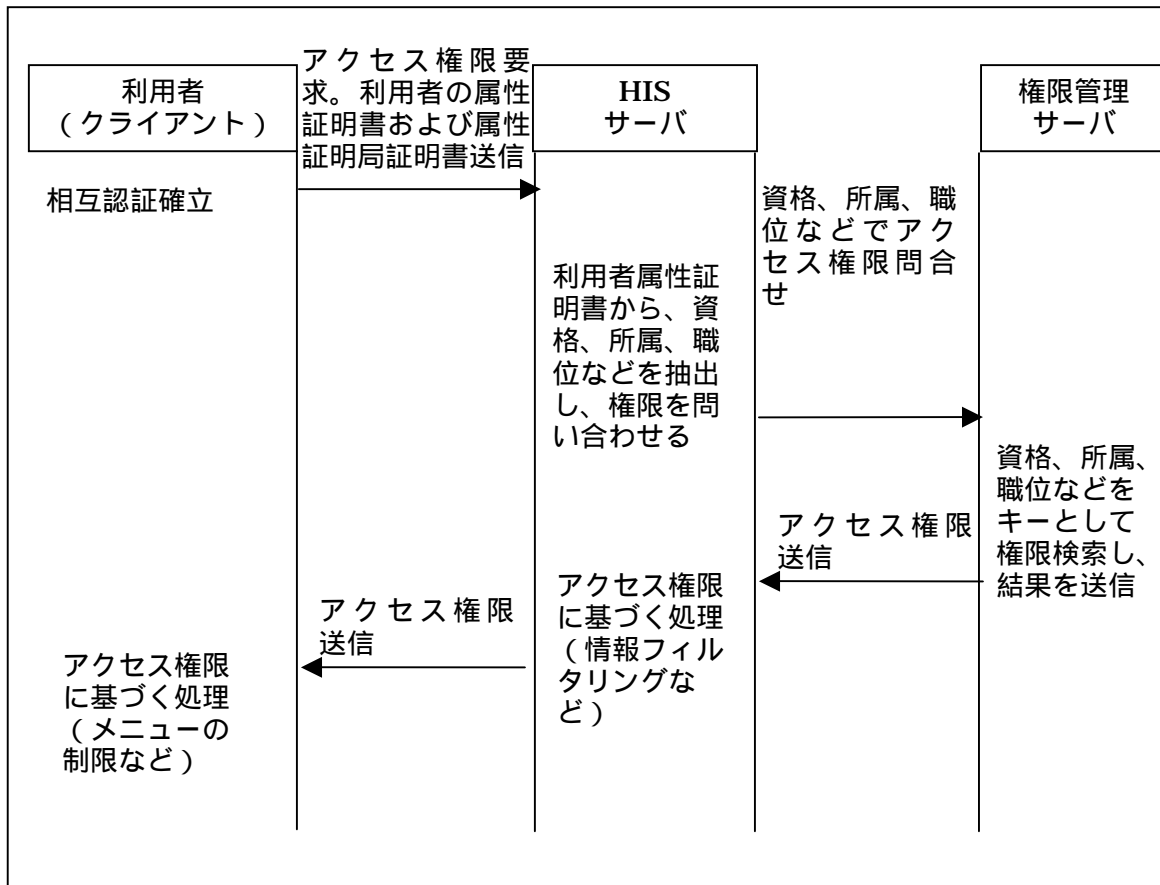
8.2.2.4.2. 公開鍵証明書に記載された属性(hcRole)に基づく方法

公開鍵証明書を用いた権限管理では、先の「本人認証」が行われたのち、hcRole や ID をもちいて閲覧権限を決定する。



8.2.2.4.3. 属性証明書に記載された属性に基づく方法

属性証明書を用いた権限管理では、利用者は、本人認証のために必要な公開鍵証明書と同時に、自分がアクセスしようとする情報に必要な属性を記した属性証明書を提出する。サーバはその属性証明書を検証した後、その属性に割り当てられた権限に従い、診療情報の閲覧を許可あるいは制限する。属性証明書には、職位や所属などの属性を記述することが多いが、ある情報に対するアクセス許可などをそのまま記述した属性証明書を発行することも可能である。このような属性証明書を利用すれば、毎回アクセス制御リストを参照する場合に比べ、効率的であるとともに、権限管理を分散することも可能となる。



付録1 平成13年度医療用セキュリティ技術委員会 名簿

山本隆一	大阪医科大学病院 医療情報部 助教授
坂本憲広	九州大学 医学部附属病院 医療情報部 講師
山口雅浩	東京工業大学 像情報工学研究施設 助教授
永井 肇	保健医療福祉情報システム工業会
中村茂之	保健医療福祉情報システム工業会
茗原秀幸	保健医療福祉情報システム工業会
吉村 仁	日本画像医療システム工業会
原嶋茂夫	日本画像医療システム工業会
西田慎一郎	日本画像医療システム工業会
細羽 実	島津製作所 医療情報システム室 室長
畠沢菊雄	日立コンピュータ機器 システム第2設計部 副部長
坪井俊明	NTTサイバーソリューション研究所 主幹研究員
川上幸生	(株)デジコム 代表取締役社長
鈴木優一	エントラストジャパン 取締役
菅原 忠	経済産業省商務情報政策局サ - ビス産業課 課長補佐
秋元正之	経済産業省商務情報政策局サービス政策課 調査係長
武末文男	厚生労働省医政局研究開発振興課医療技術情報推進室 室長補佐

事務局

開原成允	(財)医療情報システム開発センター 理事長
辻 良英	(財)医療情報システム開発センター 専務理事
山地正行	(財)医療情報システム開発センター 事務局長
喜多紘一	(財)医療情報システム開発センター 審議役
山田恒夫	(財)医療情報システム開発センター 研究開発部次長
後町長宏	(財)医療情報システム開発センター 研究開発部主席研究員
中久喜要	(財)医療情報システム開発センター 研究開発部主席研究員
町田悦郎	(財)医療情報システム開発センター 研究開発部主任研究員
濱田国彦	(財)医療情報システム開発センター 研究開発部主任研究員