Medicertified 電子証明書

認証局管理運用規程

Version 3.10

一般財団法人　医療情報システム開発センター

2022 年 1 月

改版履歴

版数	日付	内容
1.00 版	2003 年 7 月	初版発行
2.00 版	2006 年 6 月	1.4.2　住所変更
		3.1　郵送申請追加に伴い全面書き換え
		4.7　TYPE-V で有効期間を 20 年に設定
2.10 版	2015 年 12 月	1.1.1　一般財団法人に変更(2011/4)
		1.2　一般財団法人に変更(2011/4)
		1.4.1　一般財団法人に変更 主管部署を変更(2011/4)
		1.4.2　一般財団法人に変更 照会窓口を変更 (2011/4)
		5　文書名の変更(2015/3)
		6　文書名の変更(2015/3)
		7.1　Issuer の Organization を SECOM Trust Systems CO.,LTD に変更(2014/8)
		7.1　Issuer の Common Name を SECOM Passport for Member CA1 に変更(2014/8)
		7.1　Issuer の Common Name を Medicertified TYPE-V-G2 に変更(2014/8)
3.00 版	2017 年 9 月	全体的な文言及び体裁の見直し
		組織部署名の変更
		サーバ証明書の追加
3.10 版	2022 年 1 月	7.1　証明書のプロファイルの識別情報の修正

目次

1. はじめに

1.1. 概要

Medicertified 電子証明書（以下、証明書）は、一般財団法人医療情報システム開発センター（以下、MEDIS-DC）が行う証明書の発行、失効、及び証明書を基礎とする公開鍵インフラストラクチャ（PKI：Public Key Infrastructure）の運用維持に関する諸手続及び証明書の発行、利用に関わる主体の責任を記述したものである。

MEDIS-DC が発行した証明書では、個人又は機関／組織とその公開鍵が一意に関連づけられることを証明し、その審査過程、登録、発行は、本認証局管理運用規程（以下、CPS）によって規定される。加入者は MEDIS-DC によって発行された証明書を利用する際、MEDIS-DC より開示される文書の内容を所有者自身の利用方法に照らし、評価する必要がある。

1.2. 文書の名前と識別

本文書の名称を「Medicertified 電子証明書　認証局管理運用規程」とする。MEDIS-DC にて発行する証明書及び関連サービスに割り当てられたオブジェクト識別子（OID）を以下に示す。

1.2.392.200119	一般財団法人　医療情報システム開発センター
1.2.392.200119.1.2.1.2.2	Medicertified Service CPS

1.3. PKI の関係者

1.3.1. 認証局

認証局（以下 CA）は、運用管理する機関として登録局（以下 RA）と証明書発行局（以下 IA)により構成される。

IA は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

IA は、以下の 2 つのサービスを利用する。

1. TYPE-S：セコムトラストシステムズ株式会社の Passport for member サービスを利用する証明書
   CPS は、「SECOM CA Service Certification Practice Statement」を参照のこと。
   https://repo1.secomtrust.net/spcpp/pfm20/

2. TYPE-V：デジサートジャパン合同会社の Managed　PKI サービスを利用する証明書
   CPS は、「Symantec Corporation STN-CPS」を参照のこと。
   https://www.jp.websecurity.symantec.com/repository/CPS/

1.3.2. 登録局

RA は、適切な申請者の本人確認、登録の業務を行う。

IA への証明書登録の業務は、安全に IA にオンラインでアクセスする。なお、証明書登録の業務は、発行、失効、更新の作業を含む。

1.3.3. 加入者

加入者とは、証明書発行申請を行い、CA により証明書を発行される個人あるいは組織をさす。

1.3.4. 検証者

検証者とは、本 CA から発行される電子証明書の有効性を検証する主体をいう。

1.3.5. その他の関係者

規定しない。

1.4. 証明書の使用方法

1.4.1. 適切な証明書の使用

MEDIS-DC の発行する証明書は以下の場合において使用されるものとする。

1. 機密情報の暗号化、認証のためのデジタル署名及びアクセスコントロールを通じたセキュリティの向上
2. 機密情報の交換のための同一性の保証

1.4.2. 禁止される証明書の使用

MEDIS-DC の発行する証明書は 1.4.1 で規定される用途以外には用いないものとする。

1.5. ポリシ管理

1.5.1. 本ポリシを管理する組織

本 CSP の維持管理は、MEDIS-DC が行う。

1.5.2. 問い合わせ先

一般財団法人　医療情報システム開発センター　Medicertified 電子証明書担当

住所：東京都新宿区神楽坂一丁目1番地三幸ビル

電話番号：03－3267－1924

e-mail アドレス：pki-info@medis.or.jp

1.5.3. CPS のポリシ適合性を決定する者

本 CPS の内容は MEDIS-DC 理事長によって決定される。

1.5.4. CPS 承認手続き

本 CPS の承認は MEDIS-DC 理事長の承認をもって、承認されたものとする。

1.6. 定義と略語

- CA(Certification Authority)：“認証局”
- CPS(Certification Practices Statement)：“認証局管理運用規程”

- CRL(Certificate Revocation List):“証明書失効リスト”“失効リスト”
- RA(Registration Authority):“登録局”
- IA（Issuing Authority）:”発行局”CA の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。

2. 公開及びリポジトリの責任

2.1. リポジトリ

リポジトリは CA の証明書、失効情報及び加入者の失効情報を保持する。

2.2. 証明書情報の公開

CA は、次のものを加入者と検証者にとって入手可能にするものとする。

1. MEDIS-DC によって、又は MEDIS-DC に代わって管理され、本 CPS を含んでいる利用可能な Web サイトの URL(Uniform Resource Locator)等
2. 本 CPS の下に発行された各証明書に関する情報

2.3. 公開の時期又はその頻度

MEDIS-DC は、CA に関する情報が変更されたときには直ちに、その情報を公開するものとする。

2.4. リポジトリへのアクセス管理

本 CPS、MEDIS-DC より別途開示される文書及び MEDIS-DC から発行された証明書の現在の状態などの公開情報は、読み取り専用とするが、特段のアクセス制御は行わない。

3. 識別及び認証

3.1. 名称決定

3.1.1. 名称の種類

本 CPS に基づいて発行される証明書に使用されるサブジェクト名は所有者名とする。

所有者名は Distinguished Name を使用する。ディレクトリのエントリとして Country、Organization、OrganizationUnit、CommonName、SerialNumber を用いる。この中で Country は必須で、ISO の 2 文字の国名識別子を用いる。日本は JP である。また CommonName は必須で、所有者の氏名（ローマ字表記）を含む必要がある。ただし、サーバ証明書は、CommonName に URL(FQDN 又は IP アドレス)を記載する。

また SubjectDN の値は同じ IA の発行する証明書の中で対象を一意に示すものとする。対象を一意に決定するため CommonName あるいはその他の属性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する。

3.1.2. 名称が意味を持つことの必要性

証明書を効果的に使用するには、証明書に現れる相対識別名が検証者によって理解され、使用される必要がある。これらの証明書で使用される名前は、それらが割り当てられた加入者を意味のある方法で識別できるものとする。

3.1.3. 加入者の匿名性又は仮名性

本 CPS「3.2.3. 個人の認証」に規定する。

3.1.4. 種々の名称形式を解釈するための規則

ITU X.500 シリーズの識別名（Distinguished Name） 形式に従う。

3.1.5. 名称の一意性

証明書に記載されるサブジェクト識別名は、あいまいさがなく、CA の個別の加入者に一意であるものとする。

3.1.6. 認識、認証及び商標の役割

商標使用の権利については、商標所持者にすべての権利が留保されるものとする。MEDIS-DC は、必要に応じて、商標所持者に対し、商標に関する出願等の公的書類の提示を求めることがある。

3.2. 初回の本人性確認

3.2.1. 私有鍵の所持を証明する方法

CA に対し証明書発行要求を行う際には、CA より 2 系統にて配布される 2 種類のコードを必要とする。

3.2.2. 組織の認証

RA に対し組織名が記載された証明書を申請する者は、国又は自治体に対応した適切な文書の提示によって、自らの組織の実在性の確認を RA に提示するものとする。

RA は次の事項で組織が実在していることを確認する。

1. 法人代表者証明書及びサーバ証明書

・ 法人組織の場合：登記事項証明書、定款により実在確認を行う。なお、登記事項証明書、定款が既に RA に提出済みで当該書類の記載内容に変更がない場合は、直近の提出日より 5 年間は当該資料の提出を省略することができる。

・ その他関連事業者：国、地方公共団体等の機関で法人代表者の印鑑証明書、登記事項証明書等がない法人の場合においては、申請事業者を認可、管轄する上位団体の証明する存在、設立事由等が分かる客観的な書類により実在性の確認を行うものとする。

2. 個人証明書

法人代表者でない自然人からの申請であって、所属する法人名及び部署名・肩書きを証明書に含めることを要求する場合には、次の方法で組織の実在性と部署名・肩書きの妥当性を確認する。

・ 申請者が当該法人組織・部署に在籍し、当該肩書きを有することを管理部門の責任者又は法人代表者が証明する書類で当該法人組織・部署の在籍と肩書きを確認する。

・ 帝国データバンク企業コードを有する組織は、企業コードを申請書に記入することにより組織の実在確認を行う。なお、すでに法人代表者の Medicertified 電子証明書を取得している組織であって、RA に登記事項証明書を提出済みで記載内容に変更がない場合は、直近の提出日より 5 年間は企業コードの申立てを省略することができる。

・ 帝国データバンク企業コードを有しない組織は、組織の登記事項証明書等を提出することにより組織の実在確認を行う。なお、すでに法人代表者の Medicertified 電子証明書を取得している組織であって、RA に登記事項証明書を提出済みで記載内容に変更がない場合は、直近の提出日より 5 年間は登記事項証明書の提出を省略することができる。

3.2.3. 個人の認証

1. 法人代表者証明書及びサーバ証明書

RA は次の事項で法人組織及び代表者が実在していることを確認する。

・ 法人組織の場合：登記事項証明書及び印鑑証明書により確認を行うものとする。なお、登記事項証明書及び印鑑証明書が既に RA に提出済みで当該書類の記載内容に変更がない場合は、直近の提出日より 5 年間は当該資料の提出を省略することができる。

・ その他関連事業者：国、地方公共団体等の機関で法人代表者の印鑑証明書、登記事項証明書等がない法人の場合においては、申請事業者を認可、管轄する上位団体の証明する存在、設立事由等が分かる客観的な書類により確認を行うものとする。

2. 個人証明書

RA は、申請書に記載された申請者の氏名と住民票の写し又は戸籍謄本又は戸籍抄本に記録されている情報を照合することにより、申請者が実在すること（住民基本台帳に記録されていること）を確認する。なお、住民票の写し又は戸籍謄本又は戸籍抄本が既に RA に提出済みで当該書類の記載内容に変更がない場合は、直近の提出日より 5 年間は当該資料の提出を省略することができる。

また、証明書に旧姓等のビジネスネームを記載する場合は、申請者のビジネスネームを証明できる戸籍謄本等の公的証明書、もしくは申請者のビジネスネームを法人代表者又は管理部門の責任者が証明する書類のどちらか一方で確認を行うものとする。

3.2.4. 確認しない加入者の情報

認めない。

3.2.5. 機関の正当性確認

本 CPS「3.2.2. 組織の認証」及び「3.2.3. 個人の認証」で規定された書類の確認を実施することにより、正当性確認を行う。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申請時の本人性確認及び認証

3.3.1. 通常の鍵更新時の本人性確認及び認証

本 CPS「3.2.2. 組織の認証」及び本 CPS「3.2.3. 個人の認証」と同様の手順で認証を行う。

3.3.2. 証明書失効後の鍵更新の本人性確認及び認証

証明書失効後の鍵更新は、行わない。

3.4. 失効申請時の本人性確認及び認証

次の手順による。

1. 失効申請書を提出する。
2. 発行更新申請書と失効申請書の印影の一致を確認する。
   ただし、印影が異なる場合は、本 CPS「4.2.1. 本人性及び資格確認」に基づく確認を行う。

4. 証明書のライフサイクルに対する運用上の要件

4.1. 証明書申請

申請者は、以下の Medicertified 証明書の申請を行うことができる。

1. 法人代表者証明書:医薬品の治験および市販後副作用等報告、医療機器の不具合等報告を目的とした通信に使用することができる。
2. 個人証明書:申請電子データシステムを使った申請・届出等に利用することができる。
3. サーバ証明書:医薬品の治験および市販後副作用等報告、医療機器の不具合報告を目的としたサーバ間通信に使用することができる。ただし、法人代表者証明書のオプションとして、法人代表者証明書との同時申請に限る。

4.1.1. 証明書の申請者

1. 法人代表者証明書:法人代表者とする。
2. 個人証明書:自然人とする。

4.1.2. 申請手続及び責任

認証局で定める以下のいずれかの手続きによって証明書の発行更新申請を行う。

1. 認証局へ申請書を持参して申請する場合:本人もしくは代理人が RA へ申請書を持参して申請する。
2. 代表者証明書を郵送により申請する場合:本人もしくは代理人が RA へ申請書を郵送して申請する。
3. 個人証明書を郵送により申請する場合:本人が RA へ申請書を郵送して申請する。

4.2. 証明書申請手続き

4.2.1. 本人性及び資格確認

1. 本人もしくは代理人であることの確認

＜対面申請の場合＞

次の方法のいずれかのものにより、申請者と称する者が実在性の確認された申請者本人であること(住民基本台帳に記録されている者であること)を確認する。

- 官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を貼付してあるものの提示を求める方法
- 本人であることを証明できる前項以外の官公庁の発行した書面(各種健康保険の被保険者証、各種年金の年金手帳等)の 2 種類以上の提示を求める。

＜郵送申請の場合＞

申請に際して RA から配布する参照番号通知書、請求書を申請者宛に特例型本人限定受取郵便で送付する。郵便物の受け取り時に郵便局職員が運転免許証等を確認することで本人性を確認する。

2. 正当な代理人であることの確認

次の全ての方法により、代理人と称する者が正当な代理人であることを確認する。

- 申請者本人の有効な印鑑証明書の提示を求める。
- 前項の印鑑で押印された委任状の提示を求める。

4.2.2. 証明書申請の承認又は却下

RA は、書類や本人性の確認がとれた場合は、承認する。

RA は、書類不備や本人性の確認等の審査過程において疑義が生じた場合には、利用申請を却下することができる。

4.2.3. 証明書申請手続き期間

RA は、証明書申請に基づいて、速やかに証明書の発行を行う。

4.3. 証明書発行

4.3.1. 証明書発行時の認証局の機能

証明書の発行は、IA の CPS による。

4.3.2. 証明書発行後の通知

RA は、電子証明書を交付することにより電子証明書を発行したことを通知したものとみなす。

4.4. 証明書の受理

4.4.1. 証明書の受理

申請者が証明書発行に必要な情報を用いて、証明書をダウンロードした時点で、その証明書を受理したものとする。

4.4.2. 認証局による証明書の公開

CA は、証明書の鍵の公開は、行わない。

4.4.3. 他のエンティティに対する認証局による証明書発行通知

規定しない。

4.5. 鍵ペアと証明書の利用目的

4.5.1. 加入者の私有鍵と証明書の利用目的

Medicertified 証明書は以下の場合において使用されるものとする。

1. 機密情報の暗号化、認証のためのデジタル署名及びアクセスコントロールを通じたセキュリティの向上
2. 機密情報の交換のための同一性の保証

4.5.2. 検証者の公開鍵と証明書の利用目的

検証者は、署名検証の用途で公開鍵と証明書を利用する。

4.6. 証明書更新

4.6.1. 証明書更新の要件

規定しない。

4.6.2. 証明書の更新申請者

規定しない。

4.6.3. 証明書更新の処理手順

規定しない。

4.6.4. 加入者への新証明書発行通知

規定しない。

4.6.5. 更新された証明書の受理

規定しない。

4.6.6. 認証局による更新証明書の公開

規定しない。

4.6.7. 他のエンティティへの証明書発行通知

規定しない。

4.7. 証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1. 証明書鍵更新の要件

証明書記載情報が前回と同一（E-mail を除く）の場合は更新とする。

4.7.2. 鍵更新申請者

本 CPS「4.1.1. 証明書の申請者」と同一とする。

4.7.3. 鍵更新申請の処理手順

本 CPS「4.1.2. 申請手続き及び責任」と同一とする。

4.7.4. 加入者への新証明書発行通知

本 CPS「4.3.2. 証明書発行後の通知」と同一とする。

4.7.5. 鍵更新された証明書の受理

本 CPS「4.4.1. 証明書の受理」と同一とする。

4.7.6. 認証局による鍵更新証明書の公開

本 CPS「4.4.2. 認証局による証明書の公開」と同一とする。

4.7.7. 他のエンティティへの証明書発行通知

規定しない。

4.8. 証明書変更

4.8.1. 証明書変更の要件

証明書の変更は行わない。

4.8.2. 証明書の変更申請者

規定しない。

4.8.3. 証明書変更の処理手順

規定しない。

4.8.4. 加入者への新証明書発行通知

規定しない。

4.8.5. 変更された証明書の受理

規定しない。

4.8.6. 認証局による変更証明書の公開

規定しない。

4.8.7. 他のエンティティへの証明書発行通知

規定しない。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の要件

RA は、次の場合に証明書を失効するものとする。

1. 加入者が、本 CPS、又はその他の契約、規制、あるいは、有効な証明書に適用される法に基づく義務を満たさなかった場合
2. 私有鍵の危殆化が認識されたか、妥当な疑いがある場合
3. 加入者の特定ができない場合で、RA が失効させる必要があると判断した場合

4. RA が、本 CPS に従って証明書が適切に発行されなかったと決定した場合
5. 加入者の要求があった場合

4.9.2. 失効申請者

証明書の失効は、次の 1 人又はそれ以上の者によって要求されるものとする。

1. その人の名前で証明書が発行された加入者
2. RA の職員

4.9.3. 失効申請の処理手順

RA は、失効申請を受理する場合は、本 CPS「3.4. 失効申請時の本人性確認及び認証」に従って、以下の手順を実施した上で証明書の失効処理を行うものとする。失効処理の結果は、RA 管理システムによって証明書状態を確認することができる。

1. 失効を要求している申請者が失効される証明書に記されている加入者であることを確認する。
2. 加入者の代理人から申請があった場合は、代理人が失効をもたらすに十分な権限を持っていることを確認する。
3. RA が失効させる場合には、失効の理由を確認し証明書を失効する。

4.9.4. 失効における猶予期間

証明書の失効処理は、失効申請があってから RA が失効申請の受付を行い、証明書失効申請処理の登録を行った後、即時に CA によって行われる。また、失効処理の結果は CRL に反映される。

4.9.5. 認証局による失効申請の処理期間

RA は、有効な失効申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書の失効情報を反映させる。

4.9.6. 検証者の失効情報確認の要件

Mediertified 電子証明書には、CRL の格納先の URL を記載する。検証者は、CRL を確認して証明書の有効性を確認するものとする。

4.9.7. CRL 発行頻度

IA の CPS による。

4.9.8. CRL が公開されない最大期間

IA の CPS による。

4.9.9. オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10. オンラインでの失効確認要件

規定しない。

4.9.11. その他利用可能な失効情報確認手段

使用しない。

4.9.12. 鍵の危殆化に関する特別な要件

規定しない。

4.9.13. 証明書一時停止の要件

一時停止は行わない。

4.9.14. 一時停止申請者

規定しない。

4.9.15. 一時停止申請の処理手順

規定しない。

4.9.16. 一時停止期間の制限

規定しない。

4.10. 証明書ステータスの確認サービス

4.10.1. 運用上の特徴

規定しない。

4.10.2. サービスの利用可能性

規定しない。

4.10.3. オプショナルな仕様

規定しない。

4.11. 加入の終了

加入者が、証明書の利用を終了する場合、本 CPS「4.9. 証明書の失効と一時停止」に規定する失効手続きを行うものとする

4.12. 私有鍵預託と鍵回復

4.12.1. 預託と鍵回復ポリシ及び実施

IA の CPS による。

4.12.2. セッションキーのカプセル化と鍵回復のポリシ及び実施

IA の CPS による。

5. 建物・関連設備、運用のセキュリティ管理

5.1. 建物及び物理的管理

5.1.1. 施設の位置と建物構造

IA の CPS による。

5.1.2. 物理的アクセス

RA の登録端末は、施錠された専用区画に置く。

IA については、IA の CPS による。

5.1.3. 電源及び空調設備

IA の CPS による。

5.1.4. 水害及び地震対策

IA の CPS による。

5.1.5. 防火設備

IA の CPS による。

5.1.6. 記録媒体

IA の CPS による。

5.1.7. 廃棄物の処理

IA の CPS による。

5.1.8. 施設外のバックアップ

IA の CPS による。

5.2. 手続的管理

5.2.1. 信頼すべき役割

IA の CPS による。

5.2.2. 職務ごとに必要とされる人数

IA の CPS による。

5.2.3. 個々の役割に対する本人性確認と認証

IA の CPS による。

5.2.4. 職務分轄が必要になる役割

IA の CPS による。

5.3. 要員管理

5.3.1. 資格、経験及び身分証明の要件

RA については、MEDIS-DC の職員による。

IA については、IA の CPS による。

5.3.2. 経歴の調査手続

RA については、MEDIS-DC の職員規程による。

IA については、IA の CPS による。

5.3.3. 研修要件

RA については、MEDIS-DC の職員規程による。

IA については、IA の CPS による。

5.3.4. 再研修の頻度及び要件

RA については、MEDIS-DC の職員規程による。

IA については、IA の CPS による。

5.3.5. 職務のローテーションの頻度及び要件

RA については、規定しない。

IA については、IA の CPS による。

5.3.6. 認められていない行動に対する制裁

RA については、MEDIS-DC の職員規程による。

IA については、IA の CPS による。

5.3.7. 独立した契約者の要件

IA の CPS による。

5.3.8. 要員へ提供する資料

IA の CPS による。

5.4. 監査ログの取扱い

5.4.1. 記録するイベントの種類

IA の CPS による。

5.4.2. 監査ログを処理する頻度

IA の CPS による。

5.4.3. 監査ログを保存する期間

IA の CPS による。

5.4.4. 監査ログの保護

IA の CPS による。

5.4.5. 監査ログのバックアップ手続

IA の CPS による。

5.4.6. 監査ログの収集システム(内部対外部)

IA の CPS による。

5.4.7. イベントを起こしたサブジェクトへの通知

IA の CPS による。

5.4.8. 脆弱性評価

IA の CPS による。

5.5. 記録の保管

5.5.1. アーカイブ記録の種類

IA の CPS による。

5.5.2. アーカイブを保存する期間

IA の CPS による。

5.5.3. アーカイブの保護

IA の CPS による。

5.5.4. アーカイブのバックアップ手続

IA の CPS による。

5.5.5. 記録にタイムスタンプをつける要件

IA の CPS による。

5.5.6. アーカイブ収集システム(内部対外部)

IA の CPS による。

5.5.7. アーカイブ情報を入手し、検証する手続

IA の CPS による。

5.6. 鍵の切り替え

IA の CPS による。

5.7. 危殆化及び災害からの復旧

5.7.1. 災害及び CA 私有鍵危殆化からの復旧手続き

IA の CPS による。

5.7.2. コンピュータのハードウェア、ソフトウェア、データが破損した場合の対処

IA の CPS による。

5.7.3. CA 私有鍵が危殆化した場合の対処

IA の CPS による。

5.7.4. 災害等発生後の事業継続性

IA の CPS による。

5.8. 認証局又は登録局の終了

MEDIS-DC が運営を停止する場合には、少なくとも 60 日前に加入者、検証者を含むその他の関係者に文書、Mail、Web 等により通知する。MEDIS-DC において発行されたすべての証明書は、CA の終了日までに失効される。すべての証明書を失効した後、MEDIS-DC は加入者に対して証明書の失効を通知する。

CA が終了する場合には、その CA の記録の安全な保管又は廃棄を確実にするための最善の手配を行うものとする。

6. 技術的なセキュリティ管理

6.1. 鍵ペアの生成と実装

6.1.1. 鍵ペアの生成

IA の CPS による。

6.1.2. 加入者への私有鍵の送付

IA の CPS による。

6.1.3. 認証局への公開鍵の送付

IA の CPS による。

6.1.4. 検証者への CA 公開鍵の配付

ホームページで公開する。

6.1.5. 鍵のサイズ

RSA 方式で鍵長 2048 ビットとする。

6.1.6. 公開鍵のパラメータ生成及び品質検査

IA の CPS による。

6.1.7. 鍵の利用目的

IA の CPS による。

6.2. 私有鍵の保護及び暗号モジュール技術の管理

6.2.1. 暗号モジュールの標準及び管理

IA の CPS による。

6.2.2. 私有鍵の複数人によるコントロール

IA の CPS による。

6.2.3. 私有鍵のエスクロウ

IA の CPS による。

6.2.4. 私有鍵のバックアップ

IA の CPS による。

6.2.5. 私有鍵のアーカイブ

IA の CPS による。

6.2.6. 暗号モジュールへの私有鍵の格納と取り出し

IA の CPS による。

6.2.7. 暗号モジュールへの私有鍵の格納

IA の CPS による。

6.2.8. 私有鍵の活性化方法

IA の CPS による。

6.2.9. 私有鍵の非活性化方法

IA の CPS による。

6.2.10. 私有鍵の廃棄方法

IA の CPS による。

6.2.11. 暗号モジュールの評価

IA の CPS による。

6.3. 他の鍵ペアの管理方法

IA の CPS による。

6.3.1. 公開鍵のアーカイブ

IA の CPS による。

6.3.2. 公開鍵証明書の有効期間と鍵ペアの使用期間

IA の CPS による。

6.4. 活性化用データ

6.4.1. 活性化データの生成とインストール

IA の CPS による。

6.4.2. 活性化データの保護

IA の CPS による。

6.4.3. 活性化データのその他の要件

IA の CPS による。

6.5. コンピュータのセキュリティ管理

6.5.1. 特定のコンピュータのセキュリティに関する技術的要件

IA の CPS による。

6.5.2. コンピュータセキュリティ評価

IA の CPS による。

6.6. ライフサイクルの技術的管理

6.6.1. システム開発管理

IA の CPS による。

6.6.2. セキュリティ運用管理

IA の CPS による。

6.6.3. ライフサイクルのセキュリティ管理

IA の CPS による。

6.7. ネットワークのセキュリティ管理

IA の CPS による。

6.8. タイムスタンプ

IA の CPS による。

7. 証明書及び失効リスト及び OCSP のプロファイル

7.1. 証明書のプロファイル

Medicertified 証明書の基本領域のプロファイルは、以下のとおりとする。

対象	フィールド	識別情報（例）
Issuer （発行者）	Country（国名）	c=JP（固定）
	LocalityName （地域名）	使用しない
	Organization （組織名）	・SECOM Trust Systems CO.,LTD.（TYPE-S） ・THE MEDICAL INFORMATION SYSTEM DEVELOPMENT CENTER （TYPE-V）
	Organization Unit （組織単位名）	・SECOM Passport for Member 2.0（TYPE-S） ・使用しない（TYPE-V）
	Common Name （発行者名）	・SECOM Passport for Member CA”数字”（TYPE-S） ・Medicertified TYPE-V - G2（TYPE-V）
Subject （発行申請者）	Country（国名）	C=JP（固定）
	LocalityName （地域名）	使用しない
	Organization （組織名）	・Medical Information System Development Center(TYPE-S) ・THE MEDICAL INFORMATION SYSTEM DEVELOPMENT CENTER （TYPE-V）
	OrganizationUnit （組織単位名）	法人代表者証明書の場合 OU＝Title 肩書を表す名称 OU＝Company Name 組織名を表す名称
		個人証明書の場合 ・使用しない（TYPE-S） ・法人代表者証明書と同様（Type-V）
		サーバ証明書の場合 OU＝Company Name 組織名を表す名称
	Common Name （発行申請者名） ※1	法人代表者証明書／個人証明書 CN＝発行対象者名（例：CN=Taro Medis）
		サーバ証明書の場合 CN＝FQDN 又は IP アドレス（例：CN=www.medis.or.jp）

	serialNumber	法人代表者証明書の場合 ・SERIALNUMBER=YYY（※2）（TYPE-S） ・使用しない（TYPE-V）
		個人証明書の場合 ・SERIALNUMBER=XXXXXYYY（※2）（TYPE-S） ・使用しない（TYPE-V）
	surName（姓）	使用しない
	givenName（名）	使用しない
	E-mail（電子メール）	使用しない

（※1）SubjectDN の値は同じ IA の発行する証明書の中で対象を一意に示すものとする。同姓同名の可能性があるので、CommonName あるいはその他の属性(serialNumber、uid 等)に資格登録番号のような ID 番号を付加しても良い。対象を一意に決定するため CommonName あるいはその他の属性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する。

（※2）XXXXX には RA 組織コードで固定される。YYY には加入者番号を含める事ができる。

Medicertified 証明書の各フィールドの使用は、以下のとおりとする。

		TYPE-S	TYPE-V	備考
Issuer	CountryName	C	C	
	LocalityName	N	N	
	OrganizationName	C	O	
	OrganizationUnitName	C	O	
	CommonName	N	C	
Subject	CountryName	C	C	
	LocalityName	N	N	
	OrganizationName	C	C	
	OrganizationUnitName	C	C	
	CommonName	C	C	
	GivenName	N	N	
	SurName	N	N	
	e-Mail	N	N	

C：必須。O：オプション。N：使用しない。

7.1.1. バージョン番号

証明書は、X509 Version 3 フォーマット証明書形式により作成され、X.500 識別名（Distinguished Name、以下 DN という）により一意に識別されるものとする。

7.1.2. 証明書の拡張

証明書の各拡張フィールドのプロファイルは、以下の表のとおりとする。

フィールド	説明
authorityKeyIdentifier (2.5.29.35) (TYPE-S のみ)	発行者の公開鍵識別子　(発行者公開鍵の 160bit SHA-1 ハッシュ値)
subjectKeyIdentifier (2.5.29.14) (TYPE-S のみ)	主体者の公開鍵識別子　(主体者公開鍵の 160bit SHA-1 ハッシュ値)
keyUsage (2.5.29.15)	digitalSignature と keyEncipherment のビットを立てる。
certificatePolicies (2.5.29.32)	証明書ポリシーの OID 及び CPS の URL を格納する。 ・TYPE-S の場合はセコムトラストシステムズ㈱の CPS の OID 及び URL が記載される。 ・TYPE-V の場合は MEDIS－DC の OID 及び URL が記載される。
subjectAltName (2.5.29.17)	電子メールアドレスを格納する。
basicConstraints (2.5.29.19) (TYPE-Vのみ)	CA 証明書と加入者証明書を区別する。
CRLDistributionPoints (2.5.29.31)	DirectoryName で CRL の配布点を指定する。

証明書の各拡張フィールドの使用は、以下の表のとおりとする。

	TYPE-S	TYPE-V	
version	C	C	X.509 v3
serialNumber	C	N	IA の中で一意
signature	C	C	
issuer	C	C	
validity	C	C	
subject	C	C	
subjecPublicKeyInfo	C	C	
issuerUniqueID	N	N	
subjectUniqueID	N	N	
authorityKeyID	M	N	
subjectKeyID	M	N	
keyUsage	M	M	
extKeyUsage	N	N	
privateKeyUsagePeriod	N	N	
certificatePolicies	M	M	
policyMappings	N	N	
subjectAltName	M	M	(※3)
issuerAltName	N	N	
subjectDirectoryAttributes	M	M	
basicConstraints	N	N	
nameConstraints	M	M	
policyConstraints	N	N	
CRLDistributionPoints	M	M	
authorityInformationAccess	N	N	
qualifiedCertificateStatements	N	N	
NetscapeCertType	M	M	
NetscapeBaseUrl	M	N	
NetscapeRevocationPolicies	M	N	

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

(※3) E-mail アドレスを格納する。

7.1.3. アルゴリズムオブジェクト識別子

IA の CPS による。

7.1.4. 名称の形式

7.1 証明書のプロファイルによる。

7.1.5. 名称制約

規定しない。

7.1.6. CP オブジェクト識別子

規定しない。

7.1.7. CPS のポリシ制約拡張

使用しない。

7.1.8. ポリシ修飾子の構文及び意味

CPS の URL を含むものとする。

7.1.9. 証明書ポリシ拡張フィールドの扱い

CPS の OID 及び URL が記載される。

7.2. 証明書失効リストのプロファイル

7.2.1. バージョン番号

CRL は、X.509CRL フォーマット形式のバージョン 2 に従うものとする。

7.2.2. CRL と CRL エントリ拡張領域

CRL のプロファイルを、以下に示す。

フィールド	TYPE-S	TYPE-V
version	V2	
signature	sha256RSA	
issuer	SECOM Passport for Member CA11	Medicertified TYPE-V - G2
thisUpdate	CRL の発行日	
nextUpdate	この日までに次の CRL が発行される。	
RevokedCertificate	失効した証明書のシリアルナンバー及び失効日を含む失効した証明書のリスト	
CRL Extentions authorityKeyIdentifier	発行者の公開鍵識別子 -	
CRL Extentions CRLNumber	CRL の発行順を示す整数値	

7.3. OCSP プロファイル

規定しない。

7.3.1. バージョン番号

規定しない。

7.3.2. OCSP 拡張領域

規定しない。

8. 準拠性監査とその他の評価

8.1. 監査頻度

MEDIS-DC は、本 CPS に従って証明書を発行する CA が、本 CPS に従って運営されているかについて、定期監査を行う。

8.2. 監査者の身元・資格

MEDIS-DC は、CA の準拠性監査について PKI に精通した者を監査者として内部的に選定する。

8.3. 監査者と被監査者の関係

監査者は、CA 業務を直接行っている部門から独立した、被監査者に対しての特別な利害関係のないものとする。

8.4. 監査テーマ

定期監査では、MEDIS-DC が運営する CA が、本 CPS を遵守して運営されているかを中心に監査する。主な監査内容は、次のとおりである。

1. 責任者、管理者、担当者の業務運用
2. ソフトウェアの機能
3. ハードウェアプラットフォーム及びネットワーク監視システム
4. 物理的環境
5. セキュリティ技術の最新動向を踏まえた設備、規定等の妥当性評価

等。

不定期監査は、MEDIS-DC が必要と認めた場合に、MEDIS-DC の定めた監査目的に基づいて実施する。

8.5. 監査指摘事項への対応

監査報告書で指摘された事項（通常改善事項又は緊急改善事項）に関しては、MEDIS-DC が対応を決定する。この指摘事項に関しては、MEDIS-DC が、セキュリティ技術の最新の動向を踏まえ、問題が解決されるまでの対応策も含め、その措置を責任者に指示する。講じられた対策の結果は MEDIS-DC に報告され、評価されるとともに、次の監査において確認される。

8.6. 監査結果の通知

監査者によって証明書の信頼性に影響する重大な欠陥（危機的、重度の欠陥）が発見された場合に、IA 又は RA は、MEDIS-DC、加入者、CA に関連する組織、加入者及び検証者に直ちに通知するものとする。

監査報告書は、監査人から MEDIS-DC に提出される。監査報告書の開示は、MEDIS-DC の判断によるものとする。

定期及び不定期監査の実施に係る監査調書及び監査報告書は、保管管理者を定め、許可されたものだけがアクセスできるよう保管管理する。監査報告書の保管期間は関連する証明書の有効期間の満了か

ら少なくとも 10 年間とする。

9. その他の業務上及び法務上の事項

9.1. 料金

9.1.1. 証明書の発行又は更新料

証明書発行料金、更新料金は、別途定められるものとし、事前に関係者に周知される。

9.1.2. 証明書へのアクセス料金

証明書アクセス料金は、別途定められるものとし、事前に関係者に周知される。

9.1.3. 失効又はステータス情報へのアクセス料金

失効及びステータス情報アクセス料金は、別途定められるものとし、事前に関係者に周知される。

9.1.4. その他のサービスに対する料金

本 CPS によらない個別のサービスについては、別途定められるものとし、事前に関係者に周知される。

9.1.5. 払い戻し指針

証明書の有効期限内に何らかの理由により、証明書を失効した場合においても料金の払戻しは行われない。

9.2. 財務上の責任

9.2.1. 保険の適用範囲

MEDIS-DC は、認証局の継続的な運営に必要とされる十分な財務的基盤を維持するものとする。

9.2.2. その他の資産

規定しない。

9.2.3. 加入者に対する保険又は保証

規定しない。

9.3. 業務情報の秘密保護

9.3.1. 秘密情報の範囲

RA が保持する加入者の情報は、証明書、CRL、加入者同意書、本 CPS の一部として明示的に公表されたものを除き、機密保持対象として扱われる。CA は、法の定めによる場合又は個人の書面による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。

係る法的手続、司法手続、行政手続あるいは法律で要求されるその他の手続に関連してアドバイスする法律顧問及び財務顧問に対し、RA は機密保持対象として扱われる情報を開示することができる。

加入者の署名及び認証用の私有鍵は、その所有者によって機密保持すべき情報である。本サービスの PKI は、いかなる場合でもこれらの鍵へのアクセス手段を提供していない。

監査ログに含まれる情報及び監査報告書は、機密保持対象情報である。RA は、本 CPS に記載されてい

る場合及び法の定めによる場合を除いて、これらの情報を開示しない。

9.3.2. 秘密情報の範囲外の情報

証明書及び CRL に含まれている情報は機密保持対象外として扱う。その他、次の情報は機密保持対象外とする。

1. 公開鍵証明書
2. RAの過失によらず知られた、あるいは知られるようになった情報
3. RA以外の出所から、機密保持の制限無しにRAに知られた、あるいは知られるようになった情報
4. 開示に関して加入者によって承認されている情報

9.3.3. 秘密情報を保護する責任

RA は、本 CPS「9.3.1. 秘密情報の範囲」で規定された秘密情報を保護するために、内部及び外部からの情報漏洩に係る脅威に対する保護を実施する責任を負う。

9.4. 個人情報のプライバシー保護

9.4.1. プライバシーポリシ

MEDIS-DC は、個人情報は個人の人格の象徴であり、人が個人として尊重されるためには個人情報の適正な取扱いが不可欠であると考える。

また、MEDIS-DC はこれからのIT社会においては個人情報の保護は非常に重要な課題であり、個人情報を適切に管理することは社会的責務と考え、個人情報保護に関する方針を以下のとおり定め、役員、職員及び関係スタッフに周知徹底を図り、これまで以上に個人情報保護に努める。

1. 個人情報の取得・利用・提供

   MEDIS-DC は、個人情報を取得する場合には、事前に利用目的及び提供の有無を明確にし、本人の同意を得た上で、目的の範囲内において適切に利用し、目的外利用を行わないための措置を講じる。
2. 個人情報に関する法令・規範の遵守

   MEDIS-DC は、個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守する。また、そのために必要な JISQ15001:2006 に準拠した内部規程を整備して MEDIS-DC 内に周知徹底させるとともに、役員及び職員を教育し、適切に監督する。
3. 個人情報の安全対策（漏えい、滅失又はき損の防止及び是正）

   MEDIS-DC は、MEDIS-DC が取り扱う個人情報の漏えい、滅失又はき損などに関する万全の予防措置を講ずることにより、個人情報の安全性・正確性の確保を図り、万一の問題発生時には速やかな是正対策を実施する。
4. 苦情及び相談への対応について

   MEDIS-DC は、個人情報の取扱い及び個人情報保護マネジメントシステムに関する苦情及び相談を受付けて、適切、かつ、迅速な対応を行う。
5. 個人情報保護マネジメントシステムの継続的改善

   MEDIS-DC は、個人情報保護体制を適切に維持するため、個人情報保護マネジメントシステム

を継続的に見直し、改善を行う。

9.4.2. プライバシーとして保護される情報

RA は、次の情報を保護すべき個人情報として扱う。

1. RA が本人確認や審査の目的で収集した情報で、特定の個人を特定できる情報
2. CRL に含まれない加入者の証明書失効理由に関する情報
3. その他 RA が業務上知りえた加入者の個人情報

9.4.3. プライバシーとはみなされない情報

次の情報は秘密情報としては扱わない。

1. 公開鍵証明書
2. CRL

9.4.4. 個人情報を保護する責任

RA は、本 CPS「9.4.2. プライバシーとして保護される情報」で規定された情報を保護するために、内部及び外部からの情報漏洩に係る脅威に対する保護を実施する責任を負う。

9.4.5. 個人情報の使用に関する個人への通知及び同意

RA は、認証業務の利用に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6. 司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告があった場合、RA は情報を開示することがある。

9.4.7. その他の情報開示条件

個人情報を提供した本人又はその代理人から当該本人の個人情報の開示を求められた場合、RA は MEDIS-DC で定める手続きに従って情報を開示する。

9.5. 知的財産権

加入者との間で別段の合意がなされない限り、本サービスに関わる情報資料及びデータは、次に示す当事者の権利に属するものとする。

1. CRL ： IA に帰属する財産である
2. 加入者同意書、本 CPS ： RA に帰属する財産（著作権を含む）である。
3. その他 MEDIS-DC より提供する文書：本サービスを利用するにあたっての各種利用マニュアル、ホームページ上の文書、RA にて作成されたソフトウェア等提供される文書、情報は RA に帰属する財産（著作権を含む）である。

9.6. 表明保証

9.6.1. 認証局の表明保証

IA の CPS による。

9.6.2. 登録局の表明保証

RA は、登録の際の加入者の身元の検証を行う。

証明書及びそれに含まれる公開鍵の真正性と完全性が確信されるためには、加入者は、信頼できる機関に証明書を作成してもらわなければならない。RA は、認証機能を果たすので、正しい加入者情報を IA に渡していることを保証する義務がある。同様に、RA は、証明書失効申請を正確かつ速やかに IA に渡していることを保証する義務がある。

RA は、次のことを行うものとする。

1. RA がオンラインでその責務を果たしている場合は、その認証私有鍵が証明書申請に必要な行為のためだけに使用されることを保証する。
2. 加入者の身元を認証したことを IA に対して証明する。
3. 証明書申請情報等を安全な方法により IA に伝送し、申請書類、登録記録等を安全な方法により保管する。

9.6.3. 加入者の表明保証

加入者は、次のことを行うものとする。

1. 証明書申請の記述の正確さを保証し、証明書を受け入れることによって、証明書に含まれている情報のすべてが真実であることを承認する。
2. 自分の私有鍵を保護し、それらの紛失、開示、変更、又は無許可使用を防止するために妥当な措置をすべて取る。
3. 自分の私有鍵の紛失、開示、又は無許可使用を防止するためにあらゆる努力を払う。
4. 自分の私有鍵の実際の紛失、開示、又はその他の危殆化、又はそれらが疑われるときには、直ちに RA に通知する。
5. 証明書情報の変更を RA に通知する。
6. 本 CPS、又は加入者の責任を平易なことばで明瞭に述べた PKI 開示文書を読む。
7. 本 CPS に従って鍵ペアを使用する。
8. 証明書の同意書に同意することによって、これらの義務を果たす。

9.6.4. 検証者の表明保証

検証者は、次のことを行うものとする。なお、加入者の情報を信頼するかの判断は検証者の責任である。

1. 本CPSの遵守責任
2. 証明書記載事項の確認責任
3. 証明書の有効性確認責任

9.6.5. 他の関係者の表明保証

規定しない。

9.7. 無保証

RA の責任は、RA 部門の怠慢行為に限定する。特に下記については RA の責任外とする。

1. RA は、私有鍵の加入者による紛失に関しては責任がない。
2. RA は、本 CPS が適用する手続が遵守されなかったことが偽造をもたらしたか、ポリシ及び手続が偽造を許した事を示すことができた場合を除き、偽造された署名に関して責任がない。
3. RA は、RA が本 CPS の条項に従わなかったことが原因で検証者が被った直接損害のみに責任を限定する。

9.8. 責任制限

RA の責任は、RA 部門の怠慢行為に限定する。RA は、次のことに関しては責任があるものとする。

1. RA は、身元確認と認証に関する文書化されたポリシ及び手続が遵守されたことが証明できない限り、個人のアイデンティティとそれに関連付けられたデジタル署名及びその他の認定情報との誤った結合に責任がある。
2. RA は、その失効ポリシに従って証明書を失効しなかったことに対して責任がある。
3. RA は、その失効ポリシで規定されていない理由のために証明書を失効したことに対して責任がある。

9.9. 補償

RA が本 CPS「9.6.2. 登録局の表明保証」に定める責任に違反して損害賠償責任を負う場合は別途定める金額を上限とする。ただし、RA の責に帰することができない理由から生じた損害、RA の予見の有無を問わず特別の事情から生じた損害、遺失利益については、賠償責任を負わないものとする。

加入者が、本 CPS「9.6.3. 加入者の表明保証」に定める義務を履行せず、又は本 CPS に定める責任に違反したことにより、RA が損害を被った場合には、RA は加入者に対し当該損害の賠償を請求することができるものとする。

加入者が、本 CPS「9.6.3. 加入者の表明保証」の適用範囲を超え、適用範囲外の用途に証明書を提示したことにより生じたトラブルについては加入者がすべての責任を負うものとする。当該トラブルにより RA が損害を被った場合は、加入者は RA に対し当該損害を賠償するものとする。また、本CPS「4.9. 証明書の失効と一時停止」において、加入者が失効申請義務を怠ったために生じた第三者のなりすましや検証者の誤判断等によるトラブルについては加入者が一切の責任を負うものとする。また、当該トラブルにより RA が損害を被った場合は、加入者は RA に対し当該損害を賠償するものとする。

9.10. 本 CPS の有効期間と終了

9.10.1. 有効期間

本CPSは、作成されたのち、MEDIS-DC 理事長により承認されることによって有効になる。また、本CPS「9.10.2. 終了」で記述する本 CPS の終了まで有効である。

9.10.2. 終了

本 CPS は、本 CPS「9.10.3. 終了の影響と存続条項」の規定を除き MEDIS-DC 理事長が終了を宣言した場合、終了する。

9.10.3. 終了の影響と存続条項

本 CPS が終了した場合でも、「9.3. 業務上の秘密保護」、「9.4. 個人情報のプライバシー保護」、「9.5. 知的財産権」に関する責務は存続する。

9.11. 関係者間の個々の通知と連絡

RA から加入者への通知方法は、特段の定めがあるものを除き、電子メール、ホームページへの掲載、郵送など RA が適当と判断した方法により行うものとする。また、RA から加入者の届け出た住所、FAX 番号又は電子メールアドレス宛てに加入者への通知を発した場合には、当該通知が延着又は不着となった場合でも、通常到達すべき時に到達したものとみなす。

9.12. 改訂

9.12.1. 改訂手続き

MEDIS-DC は、加入者、検証者に事前に了解を得ることなく本 CPS を改定する権利を有する。

本 CPS の改定は、MEDIS-DC において改定内容を検討しその妥当性が確認され、MEDIS-DC の理事長によって承認される。

MEDIS－DCは、承認されたCPSの改定告知書を加入者及び検証者に対して、その内容と変更実施日を変更実施日の 2 週間以上前までにホームページ上に告知する。

加入者は、告知日から変更実施日までの間、異議を申立てることができる。MEDIS-DC は、異議内容を検討しCPSを再改定することがある。

告知日から変更実施日までに異議申立てがない場合、改定された CPS は加入者に同意されたものとみなされる。

なお、改定内容に同意できない加入者及び検証者は、入手した証明書の使用を中止するものとする。

9.12.2. 通知方法と期間

本 CPS が改定される場合、更新した CPS を公開する。この改定告知文書は、CPS 及び関連文書の変更と同じ効果をもつものとする。本 CPS の改定は、変更履歴を表すバージョン番号と発行日付により識別される。

CPS 改定に伴う通知は、更新後の CPS を公開することにより行うこととし、改定実施日は改版履歴に明記されるものとする。

9.12.3. オブジェクト識別子（OID）の変更理由

規定しない。

9.13. 紛争解決手続

MEDIS-DC が行う証明書発行に関わる紛争について、MEDIS-DC に対して訴訟、仲裁を含む解決手段に訴えようとする場合、MEDIS-DC に対して事前にその旨を通知するものとする。なお、本 CPS 及び MEDIS-DC との事前に取決められた規約に定められた事項以外や、またこれらの文書の解釈において疑義が生じた場合は、各当事者はそれらの課題に対して誠意をもって協議を行うものとする。

RA、加入者及び検証者の所在地に関わらず、本 CPS の解釈、有効性及び MEDIS-DC が行う証明書発行に関わる紛争については、日本国の法律が適用される。調停、仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とする。

9.14. 準拠法

本 CPS は、「電子署名及び認証業務に関する法律」、「個人情報の保護に関する法律」及び関連する日本国内法規に準拠する。

9.15. 適用法の遵守

本 CPS の運用にあたっては、日本国内法及び公的通知等がある場合はそれを優先する。

9.16. 雑則

9.16.1. 完全合意条項

本 CPS は、本 CPS に定められたサービスに対して当事者間の完全合意を構成し、認証業務について記述された書面又は口頭による過去の一切の意思表示、合意又は表明事項に取って代わる。

9.16.2. 権利譲渡条項

関係者は、本 CPS に定める権利義務を担保に供することができない。ただし、MEDIS－DCが第三者に本 CPS に則った RA の移管もしくは譲渡を可能とする。

9.16.3. 分離条項

本 CPS は、CPS の 1 つのセクションが正しくないか無効であると判断した場合でも、CPS が更新されるまで、他のセクションは事実上有効に存続するものとする。

9.16.4. 強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5. 不可抗力

不可抗力によって損害が発生した場合、本 CPS「9.7. 無保証」の規定により RA は免責される。

9.17. その他の条項

本 CPS を採用した CA 又は RA が別の組織と合併する場合、新しい組織は本 CPS の方針に同意し責任を持ちつづけるものとする。