

Medicertified サービス
認証局管理運用規程
Version 2.00

財団法人 医療情報システム開発センター

2006年6月

改版履歴

版数	日付	内容
1.0 版	2003 年 7 月	初版発行
2.0 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

1. はじめに	1
1.1. 概要	1
1.1.1. 本認証実施規程の適用範囲	1
1.2. 本 CPS の名称と関連するオブジェクト識別子	1
1.3. 証明書が流通するコミュニティと証明書の適用範囲	1
1.3.1. 認証局 (Certification Authority)	1
1.3.2. 登録局 (Registration Authority)	1
1.3.3. エンドエンティティ (End Entity)	1
1.3.4. 適用範囲	1
1.4. 問い合わせ先	1
1.4.1. 主管部署	1
1.4.2. 照会窓口	2
1.4.3. 電子メールアドレス	2
1.5. 用語集	2
2. 一般条項	3
2.1. 義務	3
2.1.1. 認証局の義務	3
2.1.2. 登録局の義務	4
2.1.3. 証明書所有者の義務	4
2.1.4. リポジトリの義務	5
2.2. 責任	5
2.2.1. 認証局の責任	5
2.2.2. 登録局の責任	5
2.3. 財務上の責任	6
2.3.1. 賠償責任	6
2.4. 解釈及び執行	6
2.4.1. 準拠法	6
2.4.2. 分割、存続、合併及び通知	6
2.4.3. 紛争解決の手続	6
2.5. 手数料	7
2.5.1. 証明書発行及び更新料	7
2.5.2. 証明書アクセス料	7
2.5.3. 失効及び状況 (status) 情報アクセス料	7
2.5.4. 他サービス料	7
2.5.5. 払戻し	7
2.6. 情報の公表とリポジトリ	7
2.6.1. CA に関する情報の公開	7
2.6.2. 公表の頻度	7
2.6.3. 公表される情報に対するアクセス制御	7
2.6.4. リポジトリ	7
2.7. 準拠性監査	7
2.7.1. 監査頻度	7
2.7.2. 監査者の身元・資格	8

2.7.3. 監査者と被監査者の関係	8
2.7.4. 監査テーマ	8
2.7.5. 監査指摘事項への対応	8
2.7.6. 監査結果の通知	8
2.8. 秘密保持	8
2.8.1. 秘密扱いとする情報	8
2.8.2. 秘密扱いとしない情報	9
2.8.3. 証明書失効及び一時停止情報の開示	9
2.8.4. 法的執行機関への情報開示	9
2.8.5. 民事手続上の情報開示	9
2.8.6. 証明書所有者の要求に基づく情報開示	9
2.8.7. その他の理由に基づく情報開示	9
2.9. 知的財産権	9
2.10. 個人情報保護方針	10
3. 所有者の識別方法と本人確認方法	11
3.1. 新規発行時での所有者の本人確認方法	11
3.1.1. 名前の形式	11
3.1.2. 名前を意味あるものとする必要性	11
3.1.3. 各種の名前形式を解釈するための規則	11
3.1.4. 名前の一意性	11
3.1.5. 所有者の名前を決定する際の紛争解決手続	11
3.1.6. 登録商標の認識・認証・役割	11
3.1.7. 私有鍵の所有を証明するための方法	11
3.1.8. 法人代表者からの申請における認証	11
3.1.9. 法人代表者でない自然人の認証	12
3.1.10. 代理人による申請	13
3.2. 通常の更新	13
3.2.1. CA の通常更新	13
3.2.2. RA の通常更新	13
3.2.3. 証明書所有者の通常更新	13
3.3. 失効後の更新 - 鍵が危殆化していない場合	14
3.3.1. CA の失効後の更新 - 鍵が危殆化していない場合	14
3.3.2. RA の失効後の更新 - 鍵が危殆化していない場合	14
3.3.3. 証明書所有者の失効後の更新 - 鍵が危殆化していない場合	14
4. 運用上の要件	14
4.1. 証明書の申請	14
4.2. 証明書の発行	14
4.3. 証明書の受理	14
4.4. 証明書の一時停止と失効	14
4.4.1. 証明書の失効事由	14
4.4.2. 証明書の失効申請ができる者	15
4.4.3. 失効要求手続	15
4.4.4. 失効要求の猶予期間	15
4.4.5. 一時停止事由	15
4.4.6. 一時停止を申請できる者	15

4.4.7. 証明書の一時的停止手続.....	15
4.4.8. 一時的停止期間の限度.....	15
4.4.9. 失効リスト発行の頻度.....	15
4.4.10. 失効リスト確認の必要性.....	16
4.4.11. オンラインでの失効確認に対する可用性.....	16
4.4.12. オンラインでの失効確認の必要性.....	16
4.4.13. その他利用可能な失効確認公表手段.....	16
4.4.14. その他利用可能な失効確認公表手段における確認要件.....	16
4.4.15. 鍵の危殆化に関する特別な要件.....	16
4.5. セキュリティ監査の手続.....	16
4.5.1. 記録されるイベントの種類.....	16
4.5.2. 監査ログの処理頻度.....	16
4.5.3. 監査ログの保存期間.....	16
4.5.4. 監査ログの保護.....	16
4.5.5. 監査ログのバックアップ.....	17
4.5.6. 監査ログの収集システム.....	17
4.5.7. イベントを引き起こした人への通知.....	17
4.5.8. セキュリティ対策の見直し.....	17
4.6. 記録の保管.....	17
4.6.1. アーカイブの保存期間.....	17
4.6.2. アーカイブの保護.....	17
4.6.3. アーカイブのバックアップ手順.....	17
4.6.4. アーカイブの収集システム.....	17
4.6.5. アーカイブ情報の検証.....	17
4.7. 鍵の切替え.....	17
4.8. 危殆化と業務の継続性の保証.....	18
4.9. CA の終了.....	18
5. 建物・関連設備、運用、要員のセキュリティ管理.....	18
6. 技術的なセキュリティ管理.....	19
7. 証明書と失効リストのプロファイル.....	20
7.1. 証明書のプロファイル.....	20
7.2. 証明書失効リストのプロファイル.....	24
8. 本 CPS の管理.....	25
8.1. 改定手続.....	25
8.2. 公表と通知の手続.....	25
8.3. CPS の承認と通知の手続.....	25

1. はじめに

1.1. 概要

1.1.1. 本認証実施規程の適用範囲

Medicertified サービスは、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 CPS によって規定される。証明書所有者は 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. 本 CPS の名称と関連するオブジェクト識別子

本文書の名称を「Medicertified Service CPS」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	（財）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. 証明書が流通するコミュニティと証明書の適用範囲

1.3.1. 認証局 (Certification Authority)

認証局（以下 CA）は、運用管理する機関として証明書発行局（以下 IA）と登録局（以下 RA）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。

1.3.2. 登録局 (Registration Authority)

RA は、適切な申請者の本人確認、登録の業務を行う。RA は本人確認、登録の業務を、RA が事前に審査し認定した組織（以下、LRA という）に委託することがある。

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. エンドエンティティ (End Entity)

エンドエンティティは、証明書所有者と署名検証者（以下、検証者）から構成される。証明書所有者とは、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. 適用範囲

MEDIS-DC の発行する 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およびアクセスコントロールを通じた電子メール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. 問い合わせ先

1.4.1. 主管部署

（財）医療情報システム開発センター 研究開発部

1.4.2. 照会窓口

(財)医療情報システム開発センター 研究開発部
住所 : 東京都文京区西片 1 - 17 - 8
Tel 番号 : 03 - 5805 - 8203

1.4.3. 電子メールアドレス

電子メールアドレス : pki-info@medis.or.jp

1.5. 用語集

- ・ CA(Certification Authority) : “ 認証局 ”
- ・ CP(Certificate Policy) : “ 証明書ポリシー ”
- ・ CPS(Certification Practices Statement) : “ 認証実施規程 ”
- ・ CRL(Certificate Revocation List) : “ 証明書失効リスト ” “ 失効リスト ”
- ・ RA(Registration Authority) : “ 登録局 ”
- ・ IA (IssuingAuthority)
” 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。
- ・ LRA (LocalRegistration Authority)
証明書を発行する組織と所在地の違う別組織であり、RA 業務において本人の確認 (認証)
証明書発行申請処理、証明書失効申請処理を行う組織である。

2. 一般条項

2.1. 義務

2.1.1. 認証局の義務

MEDIS-DC は、MEDIS-DC の Medicertified サービス（以下、本サービスという）と運用のすべての局面が、本 CPS に従って行われることを保証する責任がある。

MEDIS-DC は、本サービスについて利用可能なポリシーと手続を持つものとし、次のことを扱うものとする。

1. 本 CPS および CP に基づき証明書の発行、管理を行う
2. 証明書申請の際に、申請書から提供される情報を誤りなく証明書に反映させる
3. 本 CPS および CP に基づき、MEDIS-DC の営業日のサポート提供期間（日本時間の 10 時 12 時、13 時 17 時）に問い合わせを受け付ける

2.1.1.1. 証明書の発行、停止、及び失効の通知

IA は、証明書所有者の識別名を持つ証明書が発行される場合には、各証明書所有者に通知するものとする。

IA は、本 CPS に従って、検証者が証明書失効リスト (CRL) を入手できるようにするものとする。

2.1.1.2. CA の表現の正確性

IA が証明書を発行するとき、証明書所有者に証明書を発行したことで、証明書に記載されている情報が CP に従って検証されたことを CA が保証する。証明書所有者に対して証明書を生成する又は証明書を活性化するデータを安全に送付した時点で、このような検証がおこなわれたことの通知とする。

MEDIS-DC は、CP に基づく証明書所有者の権利と義務を、証明書所有者同意書により各証明書所有者に通知する。証明書所有者同意書は、CP に基づいて発行された証明書の許される用途、証明書所有者の鍵の保護に関する責任の記述を含むものとする。MEDIS-DC は、鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取消し、及び紛争解決を処理するための手続を証明書所有者に通知する。

2.1.1.3. 証明書の申請から発行までの期間

証明書所有者が鍵活性化物の生成後に鍵活性化プロセスを完了しなければならない最大期間は 30 日間とする。その期間を経過した場合、再度証明書の申請手続を行う必要がある。

2.1.1.4. 証明書の失効と更新

IA は、証明書の期限切れ、失効、及び更新のいかなる手続も、本 CPS の該当する条項に従って行われる。CRL 配布点のアドレスは、証明書に記述する。

2.1.1.5. 私有鍵の保護

CA は自身が保有又は格納する私有鍵及び活性化データが本 CPS に従って確実に保護される。

2.1.1.6. CA 私有鍵の使用制限

CA は、CA の証明書署名用私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されるものとする。CA は、CA 運用に必要な操作のためだけに CA 職員が発行した私有鍵が、この目的のためだけに使用されるものとする。

2.1.2. 登録局の義務

RA は、登録の際の証明書所有者の身元の検証を行う。RA は、CA が自ら使用するのと同じ規則と認証方法に従うものとする。

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、証明書所有者は、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、CA に代わって認証機能を果たすので、CA の証明書所有者認証ポリシーに従っていることと正しい証明書所有者情報を CA 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タイムリーに CA 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、その署名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. 証明書所有者の身元を認証したことを CA 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。

2.1.2.1. 証明書失効申請

証明書の失効申請において、RA は申請者が対象証明書の所有者本人もしくは、正当な代理人であるか、失効理由は正しいかを確認する必要がある。

2.1.2.2. 監査

RA の信頼性に対する保証を提供するため、及び内部監査を実施する職員に情報を提供するために、RA は、監査可能な業務履歴を残す必要がある。記録必要イベントについては文書又はシステムによる監査ログとして必要期間保管管理されるものとする。

2.1.2.3. 保管

将来の検証に備え、証明書がどのようにまた何故生成されたかを管理できるように RA は、証明書の作成要求又は失効要求などの業務履歴をその該当する証明書の有効期間満了後、10 年間保管するものとする。

2.1.3. 証明書所有者の義務

本 CA の証明書所有者は、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. 私有鍵及び（適用可能な場合は）鍵トークン（鍵配付媒体）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. 適用する CP、又は証明書所有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. 適用する CP に従って鍵ペアを使用する。
8. 証明書所有者同意書に署名することによって、これらの義務に正式に同意する。

2.1.4. リポジトリの義務

証明書は検証者にとって入手可能であるものとする。ただし、証明書所有者の証明書は本 CA のリポジトリにおける開示しない。

CRL は、検証者にとって入手可能であるものとする。

2.2. 責任

2.2.1. 認証局の責任

2.2.1.1. 保証

MEDIS-DC は CA として、本 CPS 及び適用する CP に規定した内容を遵守して証明書の発行、失効を含む認証サービスを提供し、CA 私有鍵の信頼性を含む認証業務の信頼性の確保を保証する。

MEDIS-DC は、次のことに関して責任がある。

- 1.MEDIS-DC は、鍵配付プロセス中の私有鍵の危殆化に責任があるものとする。
- 2.MEDIS-DC は、身元確認と認証に関する文書化されたポリシー及び手続が遵守されたことが証明できない限り、個人の身元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ものとする。この責任は、MEDIS-DC が結合に誤りがあることを知っていたか疑っていた状況、又は知っているべきか疑うべき状況にも及ぶものとする。
- 3.MEDIS-DC は、その失効ポリシー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ものとする。
- 4.MEDIS-DC は、その失効ポリシー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ものとする。

2.2.1.2. 免責

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

1. MEDIS-DC は、私有鍵の証明書所有者による紛失に関しては責任がないとみなす。
2. 3. MEDIS-DC は、私有鍵が CA において危殆化したこと、又は鍵生成プロセス中に、文書化されたポリシー及び手続が遵守されなかったことで、私有鍵をより危殆化され易くしたか、私有鍵の実際の発覚をもたらしたことが証明されない限り、CA が生成する私有鍵の危殆化に関して責任がないとみなす。
4. MEDIS-DC は、本 CPS もしくは適用する CP 及び手続が遵守されなかったことが偽造をもたらしたか、ポリシー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とみなす。
5. MEDIS-DC は、CA が本 CPS 及び適用する CP の条項に従わなかったことが原因で検証者がこうむった直接損害のみに責任を限定する。

2.2.2. 登録局の責任

MEDIS-DC での RA の責任は、RA 部門の怠慢行為に限定する。MEDIS-DC での 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ー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。この責任は、RA が結合されたサブジェクト情報が誤りであると知っていたか、疑っていた状況又は知っているべきか疑うべき状況にも及ぶ。
2. RA は、その失効ポリシー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、その失効ポリシー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。

2.3. 財務上の責任

2.3.1. 賠償責任

1. MEDIS-DC が本規定 2.2.2 項及び 2.2.2 項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、MEDIS-DC の責に帰することができない理由から生じた損害、MEDIS-DC 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。

2. エンドエンティティが、本規定に定める義務を履行せず、または本規定 2.2.2 項に定める責任に違反したことにより、MEDIS-DC が損害を被った場合には、MEDIS-DC はエンドエンティティ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。

3. 本規定 2.3.1 項(2)のエンドエンティティによる証明書利用制限において、エンドエンティティが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エンドエンティティがすべての責任を負うものとする。当該トラブルにより MEDIS-DC が損害を被った場合は、エンドエンティティは MEDIS-DC に対し当該損害を賠償するものとする。また、本規定 4.4 項記載の失効申請において、エンドエンティティ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エンドエンティティ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 MEDIS-DC が損害を被った場合は、エンドエンティティは MEDIS-DC に対し当該損害を賠償するものとする。

4. 本規定 2.1.4 項(1)の証明書利用制限において、検証者が使用目的の範囲を超えて証明書を使用した結果被った損害については、検証者が一切の責任を負うものとし、MEDIS-DC は何ら賠償責任を負わないものとする。また、検証は一般的にソフトウェアで自動的に行われるが、検証の最終判断は検証者の責任である。検証者が有効性を確認できないにもかかわらず証明書を利用した結果被った損害については MEDIS-DC は一切賠償責任を負わないものとする。

2.4. 解釈及び執行

2.4.1. 準拠法

CA、証明書所有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。

2.4.2. 分割、存続、合併及び通知

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。

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

2.4.3. 紛争解決の手続

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 が適用する CP 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。

2.5. 手数料

2.5.1. 証明書発行及び更新料

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。

2.5.2. 証明書アクセス料

証明書アクセス料は、別途定められるものとし、事前に関係者に周知される。

2.5.3. 失効及び状況 (status) 情報アクセス料

失効及び状況(status)情報アクセス料は、別途定められるものとし、事前に関係者に周知される。

2.5.4. 他サービス料

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。

2.5.5. 払戻し

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。

2.6. 情報の公表とリポジトリ

2.6.1. CA に関する情報の公開

CA は、次のものを証明書所有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、適用する CP を含んでいる利用可能な Web サイトの URL 等
2. 本 CPS が適用する CP の下に発行された各証明書に関する情報

2.6.2. 公表の頻度

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。

2.6.3. 公表される情報に対するアクセス制御

CP、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。

2.6.4. リポジトリ

MEDIS-DC は証明書所有者及び検証者が CRL/ARL 情報にアクセスできるようにリポジトリを維持管理する。リポジトリは X.500 ディレクトリシステムで、アクセスに用いるプロトコルは HTTP (HyperText Transfer Protocol) 又は LDAPv3 (Light Weight Directory Access Protocol バージョン 3) を用いる。リポジトリ内の情報は Web インタフェース等を通じてアクセス可能である。なお、MEDIS-DC では、証明書所有者の証明書は公開しない。

2.7. 準拠性監査

2.7.1. 監査頻度

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

2.7.2. 監査者の身元・資格

MEDIS-DC は、CA の準拠性監査について CA 業務を直接行っている部門から独立した、PKI に精通した者を監査者として内部的に選定する。

2.7.3. 監査者と被監査者の関係

監査者は、MEDIS-DC とは別個の組織に属することによって、被監査者から独立しているものとする。監査者は、被監査者に対しての特別な利害関係のないものとする。

2.7.4. 監査テーマ

定期監査では、MEDIS-DC が運営する CA が、本 CPS 及び適用する CP 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。

- ・ 責任者、管理者、担当者の業務運用
- ・ CA 私有鍵の管理
- ・ ソフトウェアの機能
- ・ 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
- ・ 物理的環境
- ・ 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 が必要と認めた場合に、MEDIS の定めた監査目的に基づいて実施する。

2.7.5. 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 が対応を決定する。この指摘事項に関しては、MEDIS 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 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。

2.7.6. 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、CA 又は RA は、MEDIS、エンドエンティティ、本 CA に関連する組織、証明書所有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 に提出される。監査報告書の開示は、MEDIS 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 10 年とする。

2.8. 秘密保持

2.8.1. 秘密扱いとする情報

CA が保持する証明書所有者の情報は、証明書、CRL、証明書所有者同意書、本 CPS 及び CP 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、CA 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。

証明書所有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。CA 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。

2.8.2. 秘密扱いとしない情報

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。

- ・ 公開鍵
- ・ CA 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
- ・ CA 以外の出所から、機密保持の制限無しに CA に知られた、あるいは知られるようになった情報
- ・ 開示に関して証明書所有者によって承認されている情報

2.8.3. 証明書失効及び一時停止情報の開示

MEDIS-DC は、証明書所有者の証明書失効の理由に関する情報を秘密に保つものとする。ただし、証明書が失効される場合、失効された証明書の失効事由、失効日時が CRL 情報に含まれる。この失効事由のコードは機密とみなされず、全証明書所有者及び検証者に共有される。失効に関するその他の詳細情報は原則として開示しない。なお、MEDIS-DC においては一時停止は行わない。

2.8.4. 法的執行機関への情報開示

MEDIS-DC で取扱う情報に関して、法的根拠に基づいて情報を開示するように請求があった場合は法の定めに従って法執行機関へ情報を開示する。

2.8.5. 民事手続上の情報開示

秘密情報は、証明書所有者の明白な同意に基づいて、又は法律の下で認められた法廷からの命令の提示によってだけ公開されるものとする。

2.8.6. 証明書所有者の要求に基づく情報開示

証明書所有者から権利若しくは利益を侵害され又は侵害されるおそれがある等の理由により秘密情報の開示要求があった場合は、本人確認の後、利用申込み時に証明書所有者から提出された当該者に係る情報を開示する。

開示の申請方法は、要求している証明書所有者からの（証明書所有者のデジタル署名のある）認証された電子メール、又は署名付き文書による申請とし、署名付き文書による申請の場合の本人確認は当初の証明書申請時に必要とした本人確認書類の再提出により行う。

2.8.7. その他の理由に基づく情報開示

前述及び法律により認められた方法による要求以外のその他の事由に基づく情報開示は行わない。

2.9. 知的財産権

証明書所有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. 証明書 : MEDIS-DC に帰属する財産である
2. CRL : MEDIS-DC に帰属する財産である

3. 識別名 (DN) : 証明書に対して対価が支払われている限りにおいて、その名前が付与された者に帰属する財産である
4. 証明書所有者の私有鍵 : 私有鍵は、その保存方法又は保存媒体の所有者にかかわらず、公開鍵と対になる私有鍵を所有する証明書所有者に帰属する財産である
5. 証明書所有者の公開鍵 : 保存方法又は保存媒体の所有者にかかわらず、対になる私有鍵を所有する証明書所有者に帰属する財産である
6. 証明書所有者同意書、本 CPS、CP : MEDIS-DC に帰属する財産 (著作権を含む) である。
7. 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、MEDIS-DC にて作成されたソフトウェア等提供される文書、情報は MEDIS-DC に帰属する財産 (著作権を含む) である。

2.10. 個人情報保護方針

本 CA は、個人情報の重要性を認識し、次のように取扱う。

1. 個人情報を取扱う部門ごとに管理責任者を置き、個人情報の適切な管理を行う。
2. 個人情報を収集する場合、収集目的を知らせた上で、必要な範囲の情報のみを適法かつ公正な手段で収集する。
3. 証明書所有者から提出を受けた個人情報は、証明書における本サービス上の責任を果たす目的にのみ使用する。
4. 証明書所有者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対し本書と同等の条件を義務付けるものとする。
5. 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざん及び漏えい等から保護する責任を持ち、これに努めている。
6. 証明書所有者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、証明書所有者自身であることが MEDIS-DC において確認できた場合に限り、MEDIS-DC において保管している証明書所有者の個人情報を本人に開示する。
また、証明書所有者の個人情報に誤りや変更がある場合には、証明書所有者からの申出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。証明書所有者は MEDIS-DC に開示を求める場合、「2.8.6 証明書所有者の要求に基づく情報開示」に記述された方法により申請を行うものとする。
7. MEDIS-DC は、職員に対して個人情報保護の教育活動を実施している。
8. 証明書所有者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護のポリシーを適宜見直し、改善を行う。

3. 所有者の識別方法と本人確認方法

3.1. 新規発行時での所有者の本人確認方法

3.1.1. 名前の形式

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(TYPE-S のみ)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、電子署名法に適應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。

Organization、OrganizationUnit はオプションである。

3.1.2. 名前を意味あるものとする必要性

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証明書所有者を意味のある方法で識別できるものとする。

3.1.3. 各種の名前形式を解釈するための規則

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

3.1.4. 名前の一意性

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 の個別の証明書所有者に一意であるものとする。

3.1.5. 所有者の名前を決定する際の紛争解決手続

MEDIS-DC が証明する証明書所有者の名前に関する異義申立てについては、MEDIS-DC の責めに帰すべき事由がない場合、MEDIS-DC はすべての決定を行う権利を留保する。また、証明書所有者相互間の紛争発生時には、まず当事者間での解決を図るものとし、これにより解決できない場合、MEDIS-DC が最終裁決者となる。紛争の当事者は、この裁定に拘束される。

3.1.6. 登録商標の認識・認証・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。

3.1.7. 私有鍵の所有を証明するための方法

CA に対し証明書発行要求を行う際、公開鍵証明書と私有鍵との対応を証明するために、CA からのチャレンジに署名を行い、私有鍵の所有を証明するものとする。

なお、この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。

3.1.8. 法人代表者からの申請における認証

認証について、MEDIS-DC は MEDIS-DC 認証局証明書ポリシーに従うものとする。

法人代表者は、国又は自治体に対応した適切な文書の提示によって、自らの実在性と本人であることの確認を RA に提示するものとする。CA、RA は、申請側代表者の認証及び組織の名において行動する代表者を認証すると同様にこの情報を検証するものとする。

RA は法人代表者から証明書発行の申請があった場合、次の事項を確認する。

1. 法人が実在していることの識別

法人組織の場合：登記簿謄本、定款により実在確認を行う。

個人事業者の場合：個人事業者であることを証明する書類、代表者の印鑑証明、定款により確認を行う。

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、登記簿等がない法人の場合においては、RA が別途定める提示文書により、「金融機関等による顧客等の本人確認等に関する法律(本人確認法)」(平成 14 年法律第 32 号、平成 15 年 1 月 6 日施行)に準じた申請者の本人確認、及び、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. 法人の名前に於いて正当に代表者として認可されている者が、証明書発行の申請に押印を行っていること。

法人組織の場合：法人代表者の印鑑証明書により確認を行う。

個人事業者の場合：代表者個人の印鑑証明書により確認を行う。

その他関連事業者：国、地方公共団体等の機関で法人印鑑証明書、登記簿等がない組織の場合においては、MEDIS-DC が別途定める方法により確認を行う。

3. 申請者の本人確認

3.1.9 の 2. の方法による。

4. 証明書の申請書に記載された情報に虚偽がないこと。

3.1.9. 法人代表者でない自然人の認証

申請者である法人代表者でない自然人は、証明書発行に先立ち、自分の身元を RA に立証するものとする。MEDIS-DC は、申請者から提出された申請書の内容を以下の方法により確認するものとする。

1. 申請者が実在すること(実在性)の確認

申請書に記載された申請者の「氏名、住所」と住民票の写しまたは戸籍謄本または戸籍抄本に記載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(住民基本台帳に記載されていること)を確認する。

2. 申請者が本人であること(本人性)の確認

対面申請の場合は、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(住民基本台帳に記載されている者であること)を確認する。

(1)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

(2)本人であることを証明できる(1)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。

郵送申請の場合は、申請に際して MEDIS-DC から配布する参照番号通知書または Reference Number 通知書、請求書、電子証明書受領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日本国旅券等を確認することで本人性を確認する。

3. 法人代表者でない自然人からの申請であって、所属する法人名および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肩書きの妥当性を確認する。ただし TYPE-V のみとする。

・ 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、申請に際して登記簿謄本を提出し、提出から 5 年未満で記載内容に変更がな

い場合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、組織の登記簿謄本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、申請に際して登記簿謄本を提出し、提出から 5 年未満で記載内容に変更がない場合は企業コードの申立てを省略することができる。
- ・ 申請者が当該法人組織に在籍し、当該肩書きを有することを管理部門の責任者または法人代表者が証明する書類で当該法人組織の在籍と肩書きを確認する。

3.1.10. 代理人による申請

3.1.8 および 3.1.9 における申請において、MEDIS-DC は、本人に代わり代理人による申請を受理する。この際、代理人が自分の身元を RA に立証するものとする。MEDIS-DC は、代理人から提出された書類の内容を以下の方法により確認するものとする。なお、法人代表者以外の自然人の代理人による郵送申請は認めない。

1. 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。

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

2. 代理人が本人であること（本人性）の確認

対面申請の場合は、次の方法のいずれかのものにより、代理人と称する者が実在性の確認された代理人本人であること（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。

- (1) 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。
- (2) 本人であることを証明できる(1)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。

郵送申請の場合は、申請に際して MEDIS-DC から配布する参照番号通知書または Reference Number 通知書、請求書、電子証明書受領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日本国旅券等を確認することで本人性を確認する。

3.2. 通常の更新

3.2.1. CA の通常更新

CA 情報の通常の更新は、新規登録時と同様な方法により行われる。

3.2.2. RA の通常更新

RA の業務担当者の通常の更新は、新規登録時と同様な方法により行われる。

3.2.3. 証明書所有者の通常更新

証明書所有者情報の通常更新は、以下の方法により行われる。

1. 証明書の記載内容に変更が無く、新規登録時から 5 年未満の場合の通常更新
本人の実在性確認資料の提示を省略することができる。
2. 新規登録時から 5 年以降の場合の通常更新
新規登録時と同様な方法により行われる。
3. 証明書の記載内容に変更が請じた場合
新規登録時と同様な方法により行われる。

3.3. 失効後の更新 - 鍵が危殆化していない場合

3.3.1. CA の失効後の更新 - 鍵が危殆化していない場合

証明書が鍵危殆化以外の理由で失効された後の鍵の更新は、認証局を認定するために使用された元の情報を MEDIS-DC に再提出するものとする。

3.3.2. RA の失効後の更新 - 鍵が危殆化していない場合

RA の業務担当者の鍵の危殆化以外の理由で証明書が失効された後の情報更新は、RA を認定するために使用された元の情報の再提出をするものとする。

3.3.3. 証明書所有者の失効後の更新 - 鍵が危殆化していない場合

証明書所有者の通常の更新は、証明書所有者情報の元の記録が作成されたときに使用された元の文書の提出、又は使用された元の記録の参照を必要とするものとする。元の文書が無効になっているか廃棄されていた場合は、元の文書相当の証明書所有者を特定できる代替文書を使用してよい。

4. 運用上の要件

4.1. 証明書の申請

証明書の発行申請者は、MEDIS-DC により事前に周知された方法に従い、証明書の発行申請を行う。発行申請者は、証明書の発行申請を行うにあたり、CP、証明書所有者同意書、その他 MEDIS-DC より開示された文書の内容を承諾しているものとする。すべての証明書の発行申請は、本 CPS 及び CP の方法により RA によって審査される。

4.2. 証明書の発行

RA は、本 CPS 「3.識別と認証」に基づく発行申請者の審査、本人確認を行い、RA 管理システムにアクセスし、CA に発行申請者を登録し、証明書の発行申請を行う。申請方法は、RA 管理者によるアクセスコントロールによって、RA 業務用の端末より RA 受付システムに対して証明書登録・発行申請を行う。CA は申請された証明書を発行するための処理を行い、証明書発行に必要な情報を発行申請者へ通知する。

4.3. 証明書の受理

CA より発行申請者へ送付された証明書発行に必要な情報を用いて、発行申請者と CA サーバ間のセキュアなオンライン通信を介し、CA が証明書を発行し、発行申請者がそれを受け取った時点で、その証明書を受容したものとする。

4.4. 証明書の一時停止と失効

4.4.1. 証明書の失効事由

IA は、次の場合に証明書を失効するものとする。

1. 証明書所有者が、本 CPS、適用する CP、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. 証明書に含まれる該当のサブジェクト情報が正確でなくなった場合
4. 証明書所有者の所属組織が変更された場合
5. MEDIS-DC が、本 CPS 及び適用する CP 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
6. いかなる理由でも、証明書所有者の要求があった場合

証明書所有者、RA、及び認定者は、証明書のサブジェクト情報が不正確であることに気づいた場合には、MEDIS-DC に知らせる義務がある。

4.4.2. 証明者の失効申請ができる者

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。

- ・その人の名前で証明書が発行された証明書所有者
- ・当サービスに関わる MEDIS-DC の職員

4.4.3. 失効要求手続

4.4.3.1. 証明書失効申請手続

証明書所有者は、事前に定められた手続によって、RA 管理者に失効申請を行う。RA 管理者は CA に証明書失効申請を行う。

4.4.3.2. 証明書の失効処理

RA 管理者は次のようにするものとする。

1. 失効を要求しているエンティティが失効される証明書に記されている証明書所有者であることを確認する。
2. 要求者が証明書所有者の代理人として行動している場合は、要求者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. 失効の理由を確認し、それが真実であると実証された場合は、証明書を失効させる。

RA 管理者が失効申請を行った後、即座に証明書は失効処理が行われる。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。

4.4.4. 失効要求の猶予期間

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。

4.4.5. 一時停止事由

本サービスでは一時停止は行わない。

4.4.6. 一時停止を申請できる者

本サービスでは一時停止は行わない。

4.4.7. 証明書の一時停止手続

本サービスでは一時停止は行わない。

4.4.8. 一時停止期間の限度

本サービスでは一時停止は行わない。

4.4.9. 失効リスト発行の頻度

CRL は証明書失効の有無に関わらず、24 時間以内に更新される。CRL に変更があった場合はいつでも更新する。ただし、CA 私有鍵の危殆化等が発生した場合は、CRL を直ちに発行するものとする。

4.4.10. 失効リスト確認の必要性

検証者は、別のエンティティの公開鍵を使い始めるときは常に、CRL をチェックすべきである。検証者は、証明書の検証に必要な関連する CRL チェックし証明書状態の確認を行うものとする。

4.4.11. オンラインでの失効確認に対する可用性

本サービスでは、保守等にてシステムを停止する以外においては、検証者に対して、CRL をリポジトリで 24 時間公開し、チェックを可能とする。

4.4.12. オンラインでの失効確認の必要性

本サービスでは OCSP 等のオンライン証明書状態チェック機能を提供しない。

4.4.13. その他利用可能な失効確認公表手段

本 CPS では、規定をしない。

4.4.14. その他利用可能な失効確認公表手段における確認要件

本 CPS では、規定をしない。

4.4.15. 鍵の危殆化に関する特別な要件

CA 署名鍵の危殆化又は危殆化のおそれが発生した際には、CA は本サービス提供者及び関連組織に直ちに通知するものとする。また、CA 署名鍵の危殆化時は、その鍵にて署名した有効な証明書のすべてを速やかに失効させるものとする。

4.5. セキュリティ監査の手続

4.5.1. 記録されるイベントの種類

CA サーバ上で起こったイベントは、それが手動的、自動的か否かに関わらず、日付、時刻、イベントを発生させた主体、イベント内容等が監査ログファイルに記録される。また、監査にて必要となる入退室記録、作業記録等の非システムイベントにおいても記録するものとする。

CA システムにおける運用の正当性を証明するために必要な監査ログとして、以下の操作等について履歴を記録する。

- ・ CA 鍵の操作
- ・ システムの起動・停止
- ・ データベースの操作
- ・ 権限設定の変更履歴
- ・ 証明書の発行
- ・ 証明書の失効
- ・ CRL の発行

4.5.2. 監査ログの処理頻度

MEDIS-DC においては監査ログを定期的に精査する。

4.5.3. 監査ログの保存期間

監査ログは、最低 10 年間は保持される。

4.5.4. 監査ログの保護

MEDIS-DC によって認可された人員のみが監査ログファイルにアクセスすることができるように

するために、厳密な管理を行う。許可されていない者が閲覧、修正及び削除をすることから保護する。

4.5.5. 監査ログのバックアップ

監査ログは、CA サーバデータベースとともに、オフラインの記録媒体にバックアップがとられ、それらの媒体は安全な施設に保管される。

4.5.6. 監査ログの収集システム

監査ログの収集システムは、CA サーバシステムに内在している。

4.5.7. イベントを引き起こした人への通知

監査ログに記録されたイベントを引き起こした人、システム、又はアプリケーションに対して通知、監査ログを公開する義務はない。

4.5.8. セキュリティ対策の見直し

ログ検査結果、各種システム運用情報、システムに関するセキュリティ情報、資源管理情報等により定期的に見直しを行い、認証局運用においてセキュリティが一定水準以上に保てるように常に対策を行うものとする。

4.6. 記録の保管

4.6.1. アーカイブの保存期間

CA サーバデータベースの履歴は、最低 10 年は保存される。監査ログファイルの履歴は、最低 5 年保存される。

4.6.2. アーカイブの保護

CA サーバデータベースは、暗号化され保護されている。CA サーバ上の監査ログについては、本 CPS「4.5.4 監査ログの保護」に記述のとおりである。

紙及び外部記憶媒体は物理的セキュリティによって保護され、MEDIS が許可したもの以外アクセスできないように制限された施設に保存される。また、その施設は、温度、湿度、磁気等の環境上の脅威からも保護される。

4.6.3. アーカイブのバックアップ手順

CA サーバデータベースは、自動的にサーバ上にバックアップがとられる。さらに、CA サーバシステム、監査ログとともに外部記憶媒体に格納される。

4.6.4. アーカイブの収集システム

CA サーバデータベース用の履歴収集システムは、CA サーバシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CPS「4.5.6 監査ログの収集システム」に記述のとおりである。

4.6.5. アーカイブ情報の検証

アーカイブデータは、媒体の耐性を考慮し、定期的に媒体の状況確認を実施する。

4.7. 鍵の切替え

TYPE-S では、CA の鍵の有効期間は 10 年とし、5 年ごとに更新を行う。TYPE-V]では、CA の鍵

の有効期間は20年とし、10年ごとに更新を行う。CA 私有鍵を用いて行う署名は、CA 私有鍵の更新時を除いて、常に最新の鍵によって行われる。

CA の鍵の切替えは、自己署名証明書の記載内容変更時、及び上記に定めた更新期日に至った際に行われる。

証明書所有者が公開鍵を別の公開鍵に円滑に切替えることができるように、CA は、切替え日の30日前に新しい証明書を発行して、その日以降は新しい証明書を使用する必要がある日付を証明書所有者に明確に知らせなければならない。

4.8. 危殆化と業務の継続性の保証

CA 私有鍵の危殆化の場合及び災害等により証明書所有者、検証者へ CRL の提供が72時間を超えて停止する等の場合、最低限次の手順を実行し、安全な環境を修復する。

- ・ CA 私有鍵が危殆化し、又は危殆化したおそれがある場合には直ちに発行したすべての証明書について失効の手続を行う。
- ・ CA 私有鍵の危殆化、又は災害等による障害発生的事实をリポジトリに掲載することにより、証明書所有者及び検証者に告知する。
- ・ CA 私有鍵が危殆化し、又は危殆化したおそれがある場合及び、災害又は認証業務用設備の故障等により利用者へ CRL の提供が72時間を超えて停止し、かつ、証明書所有者に対してその停止的事实を告知できない場合においては、直ちに当該障害の内容、発生日時、措置状況等確認されている事項を関連する組織に通報する。
- ・ 発生した不測事態の性質によって、CA の運用に従事する者のパスワードをすべて変更する。
- ・ 発生した不測事態の性質によって、CA 室入退室権限及び鍵の変更あるいは失効をする。
- ・ ディレクトリが使用不能の場合、ディレクトリデータ、当該認証業務の運用用の証明書、及び CRL をリストアする。ディレクトリ破壊の疑いがあった場合、バックアップからリストアする。

1. 窓口設置

災害や深刻な信頼性喪失により復旧を行う場合には、証明書所有者に対して状況を通知できる体制をとり、さらに証明書所有者が状況確認を行えるよう専用窓口を設置する。

2. 復旧確認

正常な復旧を確認した後、RA に対して復旧を通知する体制をとる。

3. 証明書の再発行

CA の信頼性喪失を理由で失効を行った証明書については、正常に復旧を確認した後、証明書再発行手続を行う。

4.9. CA の終了

MEDIS-DC が運営を停止する場合には、最低60日以上前に証明書所有者、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 の終了日まで失効される。すべての証明書を失効した後、MEDIS-DC は証明書所有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。

5. 建物・関連設備、運用、要員のセキュリティ管理

MedicertifiedTYPE-S については、セコムトラストネット株式会社 SECOM Passport for

members Certificate Practice Statement 第 5 章を準用する。Medicertified TYPE-V については、日本ベリサイン株式会社 OnSite CPS 第 5 章を準用する。

6. 技術的なセキュリティ管理

MedicertifiedTYPE-S については、セコムトラストネット株式会社 SECOM Passport for members Certificate Practice Statement 第 6 章を準用する。Medicertified TYPE-V については、日本ベリサイン株式会社 OnSite CPS 第 6 章を準用する。

7. 証明書と失効リストのプロファイル

7.1. 証明書のプロファイル

Medicertified 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、また証明書は 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。Medicertified 証明書の登録情報は、次の表のとおりとする。

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.net Co., Ltd. (TYPE-S) ・ THE MEDICAL INFORMATION SYSTEM DEVELOPMENT CENTER (TYPE-V)
	Organization Unit (組織単位名)	・ SECOM Passport for Member (TYPE-S) ・ 使用しない (TYPE-V)
	Common Name (発行名)	・ 使用しない (TYPE-S) ・ Medicertified TYPE-V (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)	Secom Trust (TYPE-S) 組織をあらわす名称とする (TYPE-V)
	OrganizationUnit (組織単位名)	Secom Trust (TYPE-S) 肩書きをあらわす名称とする (TYPE-V)
	Common Name (発行申請者名)	cn=Taro Suzuki 例) (1)
	serialNumber	・ serialNumber=XXXXX-YYYYYYZZ (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) RA が審査、本人確認を行った発行申請者 (発行後は、所有者と呼ぶ) の姓名。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。YYYYYY には証明書所有者番号を含めるものとする。

証明書拡張フィールドは次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)	IA の公開鍵証明書を厳密に識別するための情報を格納する。keyIdentifier, authorityCertIssuer, authorityCertSerialNumber の 3 つのサブフィールドからなるが、本 CP では keyIdentifier だけを使用する。keyIdentifier は IA の公開鍵を SHA-1 ハッシュした値とする。
subjectKeyIdentifier (2.5.29.14) (TYPE-S のみ)	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する。所有者公開鍵を SHA-1 ハッシュした値を格納する。
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ネット(株)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)	ここに電子メールアドレスを格納する。
basicConstraints (2.5.29.19)	CA 証明書とエンドエンティティ証明書を区別する。
CRLDistributionPoints (2.5.29.31)	DirectoryName にて CRL の配布点を指定する。

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

		TYPE-S	TYPE-V	備考
Issuer	CountryName	C	C	
	LocalityName	N	N	
	OrganizationName	C	C	
	OrganizationUnitName	C	C	
	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。

	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	
subjectPublicKeyInfo	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。

7.2. 証明書失効リストのプロファイル

CA が発行する 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。
CRL のプロファイルは、次の表のとおりとする。

C・・・必須

O・・・オプション

証明書リスト領域

フィールド	critical flag	CRL	備考
version	-	C	1
signature	-	C	2
issuer	-	C	3
thisUpdate	-	C	4
nextUpdate	-	C	4
RevokedCertificates	-	C	
userCertificate	-	C	
revocationDate	-	C	4
crlEntryExtensions		C	5
reasonCode	n	C	6
invalidityDate	n	O	
CRL Extentions			
authorityKeyIdentifier	n	C	
keyIdentifier	-	C	7
cRLNumber	n	C	

1 v2(1)

2 採用するアルゴリズムは、本 CPS7.1 の 7 に従う。

3 printableString(ただし 2003 年 12 月 31 日以降に UTF8String へ移行)

4 UTCTime

5 使用する拡張については、下記参照

6 removeFromCRL は使用しない

7 RFC2459 "4.2.1.2 Subject Key Identifier" (1) に従う

8. 本 CPS の管理

8.1. 改定手続

MEDIS-DC は、証明書所有者、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 において改定内容を検討し、その妥当性が確認され、MEDIS-DC 理事長による承認を得た後に、実施される。

本 CA が行う認証業務の内、電子署名法における認定を受けている場合等においては、本 CPS、適用する CP、関連文書に変更が生じた際に、主務大臣又は関係団体による確認を実施し、必要に応じて再認定の申請を行い、主務大臣又は関係団体の再認定後に改定実施するものとする。

8.2. 公表と通知の手続

本 CPS は公開する。本 CA が適用する CP 及び関連文書が改定される場合、更新した CP を公開するか、又は本 CA が提供するリポジトリに改定告知文書を公開することで行われる。この改定告知文書は、CP 及び関連文書の変更と同じ効果をもつものとする。なお、本 CPS 及び適用する CP 及び関連文書の改定は、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。

CP 及び関連文書改定に伴う通知は、本サービスが提供するリポジトリに改定告知書又は更新後の CP 及び関連文書を公開することにより行うこととし。改定実施日は改定告知書、CP 及び関連文書に明記されるものとする。

8.3. CPS の承認と通知の手続

本 CPS の承認は MEDIS-DC 理事長の承認をもって、承認されたものとし、変更実施日は承認後即日とする。ただし、本 CA が適用する CP 及び関連文書の内容変更においては、改定された CP 及び関連文書又は改定告知書を、証明書所有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 週間以上前までにリポジトリ内に告知する。証明書所有者は、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。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 CP 及び関連文書は証明書所有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証明書所有者及び検証者は、入手した証明書の使用を中止するものとする。