

平成15年度保健医療福祉情報セキュリティ推進事業

ヘルスケア PKI 認証局証明書ポリシー

(暫定版)

財団法人 医療情報システム開発センター

【目次】

1. はじめに.....	1
1.1. 概要.....	1
1.1.1. 本証明書ポリシーの適用範囲.....	1
1.1.2. 本ポリシーが依拠する文書.....	1
1.1.3. 本ポリシーが参照する文書.....	1
1.2. 本ポリシーの名称とオブジェクト識別子.....	2
1.3. 本証明書が流通するコミュニティと証明書の適用範囲.....	2
1.3.1. 認証局 (Certification Authority).....	2
1.3.2. 登録局 (Registration Authority).....	2
1.3.3. エンドエンティティ (End Entity).....	2
1.3.4. 適用範囲.....	2
1.4. 問い合わせ先.....	2
1.4.1. 主管部署.....	2
1.4.2. 照会窓口.....	3
1.4.3. 電子メールアドレス.....	3
1.5. 用語集.....	3
2. 一般条項.....	4
2.1. 義務.....	4
2.1.1. 認証局の義務.....	4
2.1.2. 登録局の義務.....	5
2.1.3. 証明書所有者の義務.....	6
2.1.4. 検証者の義務.....	6
2.1.5. リポジトリの義務.....	6
2.2. 責任.....	6
2.2.1. 認証局の責任.....	6
2.2.2. 登録局の責任.....	7
2.3. 財務上の責任.....	7
2.4. 解釈及び執行.....	7
2.4.1. 準拠法.....	7
2.4.2. 分割、存続、合併及び通知.....	7
2.4.3. 紛争解決の手続.....	7
2.5. 手数料.....	8
2.6. 情報の公表とリポジトリ.....	8
2.6.1. CA に関する情報の公開.....	8
2.6.2. 公表の頻度.....	8
2.6.3. 公表される情報に対するアクセス制御.....	8
2.6.4. リポジトリ.....	8
2.7. 準拠性監査.....	8
2.7.1. 監査頻度.....	8
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	9
2.7.6. 監査結果の通知	9
2.8. 秘密保持	9
2.8.1. 秘密扱いとする情報	9
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	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. 組織の認証	11
3.1.9. 個人の認証	12
3.2. 通常の実行	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	13
3.3.1. CA の失効後の更新 - 鍵が危殆化していない場合	13
3.3.2. RA の失効後の更新 - 鍵が危殆化していない場合	13
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	13
3.4. 失効申請	13
3.4.1. CA の失効申請	13
3.4.2. RA の失効申請	14
3.4.3. 証明書所有者の失効申請	14
4. 運用上の要件	15
4.1. 証明書の申請	15
4.2. 証明書の発行	15
4.3. 証明書の受理	15
4.4. 証明書の一時停止と失効	15
4.4.1. 証明書の失効事由	15
4.4.2. 証明者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	16

4.4.7.	証明書の一時停止手続	16
4.4.8.	一時停止期間の限度	16
4.4.9.	失効リスト発行の頻度	16
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	17
4.5.	セキュリティ監査の手続	17
4.6.	記録の保管	17
4.7.	鍵の切替え	17
4.8.	危殆化と業務の継続性の保証	17
4.9.	CA の終了	17
5.	建物・関連設備、運用、要員のセキュリティ管理	18
5.1.	建物及び関連設備管理	18
5.1.1.	施設の位置と建物構造	18
5.1.2.	入退管理	18
5.1.3.	電源及び空調設備	18
5.1.4.	水害及び地震対策	18
5.1.5.	防火設備	18
5.1.6.	記録媒体	18
5.1.7.	廃棄物の処理	18
5.1.8.	オフサイト・バックアップ	18
5.2.	手続的管理	18
5.3.	要員管理	18
6.	技術的なセキュリティ管理	19
6.1.	鍵ペアの生成と実装	19
6.1.1.	鍵ペアの生成	19
6.1.2.	所有者への私有鍵の送付	19
6.1.3.	CA への公開鍵の送付	19
6.1.4.	証明書所有者への CA 公開鍵の配付	19
6.1.5.	鍵のサイズ	19
6.1.6.	公開鍵のパラメータ生成	19
6.1.7.	パラメータ品質の検査	19
6.1.8.	ハードウェア又はソフトウェアによる鍵ペア生成	19
6.1.9.	鍵の使用目的	19
6.2.	私有鍵の保護	20
6.2.1.	暗号モジュールに関する標準	20
6.2.2.	複数人による私有鍵の管理	20
6.2.3.	私有鍵のエスクロウ	20
6.2.4.	私有鍵のバックアップ	20
6.2.5.	私有鍵のアーカイブ	20
6.2.6.	暗号モジュールへの私有鍵の格納	20
6.2.7.	私有鍵の活性化方法	21

6.2.8. 私有鍵の非活性化方法	21
6.2.9. 私有鍵の廃棄方法.....	21
6.3. 鍵ペア管理に関するその他の面	21
6.3.1. 公開鍵の保管	21
6.3.2. 私有鍵と公開鍵の有効期間.....	21
6.4. 活性化用データ.....	21
6.5. コンピュータのセキュリティ管理.....	21
6.6. ライフサイクルの技術的管理.....	21
6.7. ネットワークのセキュリティ管理.....	22
6.8. 暗号モジュールの技術管理.....	22
7. 証明書と失効リストのプロファイル.....	23
7.1. 証明書のプロファイル.....	23
7.2. 証明書失効リストのプロファイル.....	29
8. 本ポリシーの管理	30
8.1. 改定手続.....	30
8.2. 公表と通知の手続.....	30
8.3. CP の承認と通知の手続.....	30

1. はじめに

1.1. 概要

1.1.1. 本証明書ポリシーの適用範囲

証明書ポリシー (Certificate Policy、以下 CP という) は、証明書に関して、適用範囲、セキュリティ基準、審査基準を示し、認証実施規程 (Certification Practice Statement、以下 CPS という) によって規定される内容とともに、証明書発行に関するポリシーを規定するものである。また、ヘルスケア PKI は、保健医療福祉分野において医療情報を地域で連携して利用するための公開鍵基盤である。

本ポリシーは、医療従事者用公開鍵証明書、患者 / 保健医療福祉サービス利用者用公開鍵証明書及び医療機関 / 保健医療福祉サービス供給組織用公開鍵証明書を発行する「ヘルスケア PKI 認証局」の証明書ポリシーである。

ヘルスケア PKI 認証局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、CP 及び認証局により開示される文書によって規定される。証明書所有者はヘルスケア PKI 認証局によって発行された証明書を利用する際、CP 及び認証局に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。

本 CP に準拠する個々の「ヘルスケア PKI 認証局」は、本 CP を基準にして個々の環境に適合した CPS を作成するものとする。なお、本 CP と CPS が抵触する場合は、CP が優先する。

本 CP は電子署名法 (電子署名及び認証業務に関する法律) に規定された「特定認証業務の認定」を受けた認証局のみを対象としているわけではなく、認定を受けない認証局も対象としている。したがって特定認証業務の認定を受ける場合は本 CP に従い CPS に「特定認証業務の認定」を受けるに足る詳細を規定するものとする。

1.1.2. 本ポリシーが依拠する文書

- ISO/DTS17090-1 保健医療情報 - 「公開鍵基盤 パート 1: フレームワーク、概観」
- ISO/DTS17090-2 保健医療情報 - 「公開鍵基盤 パート 2: 証明書プロファイル」
- ISO/DTS17090-3 保健医療情報 - 「公開鍵基盤 パート 3: 認証局のポリシー管理」

1.1.3. 本ポリシーが参照する文書

- ISO 17799-1:2000 情報技術 - 情報セキュリティ管理の運用規程
- IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
- IETF/RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
- IETF/RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP
- IETF/RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
- US FIPS 140-1、140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (<http://csrc.nist.gov/cryptval/>)
- 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)
- 電子署名及び認証業務に関する法律 (平成 12 年 5 月 31 日 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 3 月 27 日 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 4 月 27 日 総務省・法務省・経済産業省告示第 2 号)

1.2. 本ポリシーの名称とオブジェクト識別子

本ポリシーの名称を「ヘルスケア PKI 認証局証明書ポリシー」とする。本ポリシー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
1.2.392.200119.1.1.1.2.1.3.1	ヘルスケア PKI 認証局署名用 CP
1.2.392.200119.1.1.1.2.2.3.1	ヘルスケア PKI 認証局認証用 CP
1.2.392.200119.1.1.1.1.1	ルート認証局(MEDIS ルート認証局)CP
1.2.392.200119.1.1.1.1.0	認証局テスト用証明書(MEDIS ルート認証局発行)
1.2.392.200119.1.1.1.2.0.(以降任意)	テスト用証明書

1.3. 本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。また、他の CA と相互認証を行うことがある。

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。

また、一時停止、一時停止解除を行うことがある。

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。IA への証明書登録の業務は、ヘルスケア PKI のインタフェースを用いて安全に 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。証明書所有者の範囲は次のとおりとする。

- ・医療従事者等のサービス供給者
- ・医療機関、及び、保健医療福祉サービス供給組織
- ・患者 / 保健医療福祉サービス利用者

1.3.4. 適用範囲

1. 医療従事者等のサービス供給者の署名検証用(医師及び薬剤師等の紹介状等の診療諸記録等への電子署名へ利用)及び、本人認証用
2. 患者 / 保健医療福祉サービス利用者の署名検証用(同意書等への電子署名への利用)及び、本人認証用
3. 医療機関 / 保健医療福祉サービス供給組織への署名検証用、及び、組織認証用

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

1.4.3. 電子メールアドレス

ヘルスケア PKI セキュリティポリシー委員会の責任者

電子メールアドレス : hpki-spc@medis.or.jp

1.5. 用語集

- 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 3.1.6)
- 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、その証明書及び、又はデジタル署名に依拠して行動する者。(ISO/TS17090-3 3.3.21)
- 非専門職 (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)
- 公的資格専門資格者(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 3.1.8)
- 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 ”
- hcRole(health care Role)
保健医療福祉分野での役割、資格
- 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する。
- LRA (Local Registration 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

CA は、登録プロセス、証明書に含まれる情報の検証、証明書の作成、発行、失効、停止、及び更新の管理を含めて、証明書の発行と管理のすべての局面に責任がある。CA は、CA のサービスと運用のすべての局面がこの CP の要件、表現、及び保証と CA の CPS に従って行われることを保証する責任がある。

ヘルスケア PKI 内の CA は、提供する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する。それらは、次のことを扱うものとする (SHALL)。

1. 適用可能な場合は、本 CP 2.1.3 で定義される証明書所有者の役割も含めて、証明書発行に先立つ証明書所有予定者の登録手続
2. 証明書発行に先立つ、証明書所有予定者のアイデンティティの認証手続
3. 証明書が与えられる人々に関して保持される個人情報のプライバシーを保持する手続
4. 証明書所有者及びディレクトリへの証明書の配布手続
5. 私有鍵危殆化の可能性に関する情報を受け取る手続
6. 証明書失効リストの配布手続 (発行頻度、発行方法、及び発行場所)
7. 鍵のサイズ、鍵生成プロセス、証明書の有効期間、鍵の再生成など、その他の鍵管理問題
8. セキュリティの管理と監査

この機能を果たすためには、基盤内の各 CA は、証明書所有者及び検証者にいくつかの基本的なサービスを提供する必要がある。これらの CA サービスを以下に列挙する。

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時には、各証明書所有者に通知するものとする (SHALL)。

IA は、証明書所有者の識別名を持つ証明書が失効又は停止される時には、証明書所有者に通知するものとする (SHALL)。

IA は、本 CP 4.4 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 (SHALL)。

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 CA の 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し、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 (SHALL)。

CA は、この証明書ポリシーに基づく証明書所有者の権利と義務を各証明書所有者に通知するものとする (SHALL)。このような通知は、証明書所有者同意書の形でもよい (MAY)。このような通知は、この 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、及びサービス提供の変更又は本 CP の変更の伝達も含めて、証明書所有者と CA 又は LRA 間の通信手続の記述を含むものとする (SHALL)。

CA 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 (SHALL)。

2.1.1.3. 証明書の申請から発行までの期間

CA は、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を、CPS に記述する。

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、この CP の該当する条項に従っていることを保証しなければならない (SHALL)。CRL 配布点のアドレスは、証明書に記述する。

(本 CP 7.1 (10) 参照)。

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 CP 6.2、6.3、及び 6.4 に従って確実に保護されていることを保証するものとする (SHALL)。

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ことを保証する (SHALL)。CA は、CA 運用に必要な操作のためだけに CA 職員に発行した私有鍵が、この目的のためだけに使用されることを保証する (SHALL)。

2.1.2. 登録局の義務

CA は、CA が責任を持つ身元確認と認証機能を RA に委任してもよい。

ヘルスケア組織の RA が果たす主要な機能は、最初の登録の際の証明書所有者の身元とヘルスケア上の役割の検証である。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 (SHALL)。RA の規則、認証方法は、特定の CA から独立して、個別に認定されてもよい (MAY)。

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信頼されなければならない。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信頼されなければならない。

RA は、CA に代わって果たす行為について個別に説明責任を負うこととする (RECOMMENDED)。

RA は、次のことを行うものとする (SHALL)。

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. 証明書申請情報及び登録記録を安全に伝送し、格納する。
4. (証明書失効申請を行う場合は) 本 CP 3.4.2 に従って失効申請を開始する。

2.1.2.1. 証明書失効申請

RA は、証明書失効申請の取扱いを行うことができる。一部のヘルスケア PKI 実装では、RA は、証明書失効申請手順を開始又は認証するために使用されてもよい (MAY)。適用可能な場合、RA は、認証した要求を適切な CA に転送するものとする (SHALL)。CA が使用するものと同じ基準を適用することによって、報告が真正であると RA が認めた場合、RA は、証明書識別情報と、オプションとしてその証明書を失効する記載理由を含んだ、署名つきメッセージを CA に送信する等の RA を認証できる方法により CA への証明書失効申請の処理を行うものとする (SHALL)。

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、各 RA の行動は監査可能であるものとする (SHALL)。イベントの監査記録及び監査証跡は、関連するポリシーに従ってイベント毎に生成されなければならない。

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なぜ生成されたかを管理できるように、ヘルスケア PKI 又はその CA 内の RA は、証明書の作成要求又は失効要求などのイベントを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 (SHALL)。

2.1.3. 証明書所有者の義務

ヘルスケア PKI の証明書所有者は、次のことを行うものとする (SHALL)。

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 CA 及び / 又は RA に通知する。
5. 証明書情報、ヘルスケア組織における役割又は地位の変更を RA 及び / 又は CA に通知する。
6. 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. 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。

また、ヘルスケア PKI の証明書所有者は、証明書が使用される医療情報機能に適したセキュリティトレーニングを受けたことを証明することが推奨される。

2.1.4. 検証者の義務

ヘルスケア PKI の検証者は、次の場合に限り、ヘルスケア証明書に依拠する権利を保有する。

1. 証明書が使用される目的が、本 CP の下で適切であった場合
2. 信頼することが信頼の時点で、検証者に知られているすべての状況を考慮に入れて、妥当であり、誠意によるものである場合
3. 証明書が失効又は停止されていないことを確認することによって、検証者が証明書の現在の有効性を確認した場合
4. 適用可能な場合は、検証者がデジタル署名の現在の有効性を確認した場合
5. 責任と保証の適用限界を承認した場合

2.1.5. 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。

CRL は、本 CP 4.4.9 の要件に従って、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

ヘルスケア PKI の CA の責任は、CA 部門の怠慢行為に限定する。特に、

1. CA 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. CA は、証明書所有者が生成した鍵に関しては、ヘルスケア PKI の指針に従って完全に生成されなかった場合は責任がないとみなす。
3. CA 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. CA は、ヘルスケア PKI の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. CA は、CA がこの 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。

ヘルスケア PKI の CA は、次のことに関して責任があるものとする。

6. CA 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 (SHALL)。
7. CA 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 (SHALL) 。この責任は、CA 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。
8. CA 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 (SHALL) 。
9. CA 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 (SHALL) 。

2.2.2. 登録局の責任

ヘルスケア PKI での RA の責任は、RA 部門の怠慢行為に限定する。

ヘルスケア PKI での RA の責任は、次のことに関しては限定されるものではない。(SHALL) 。

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づ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。
4. LRA が行った業務については、LRA 自身が責任を持つものとする。

2.3. 財務上の責任

本 CP では、規定をしない。

2.4. 解釈及び執行

2.4.1. 準拠法

本 CP は、ISO 17799:2000 に準拠している。本 CP の運用にあたっては、日本国内法及び通知等がある場合はそれを優先するが、CP に反映し、公開文書として公開するものとする。

2.4.2. 分割、存続、合併及び通知

本 CP は、CP 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、ポリシーが更新されるまで、他のセクションは事実上有効に存続するものとする (SHALL) 。

本 CP 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 CP の方針に同意し責任をもち続けるものとする。

2.4.3. 紛争解決の手続

証明書の発行主体である、各認証局において定められる。

2.5. 手数料

本 CP では、規定をしない。

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 (SHALL)。

1. CA によって、又は CA に代わって管理され、CP を含んでいる利用可能な Web サイトの URL 等
2. 本 CP の下に発行された各証明書 (証明書所有者の証明書を公開する場合)
3. 本 CP の下で発行された各証明書の現在の状態
4. CA が運営の基準としている認定又はライセンス基準 (CA が運営されている管轄区域でそれらの認定又はライセンス基準が適用可能な場合)

2.6.2. 公表の頻度

CA は、CA に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CP セクション 4.4 に従うものとする (SHALL)。

2.6.3. 公表される情報に対するアクセス制御

CP、CPS、証明書、及びそれらの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 (SHALL)。

2.6.4. リポジトリ

RA 又は CA リポジトリに証明書所有者に関して保持される情報は、次のようであるものとする (SHALL)。

1. 最新に保たれる (変更の 24 時間以内、状況によっては更に早く更新される)。
2. ISO 17799-1:2000 と同等以上の規格、又は認可された認定あるいはライセンス基準に従って管理される。

2.7. 準拠性監査

準拠性監査は、多くの PKI 相互運用性モデルの不可欠なコンポーネントである。

2.7.1. 監査頻度

本 CP に従って証明書を発行する CA は、本 CP の要件に完全に従っているということを検証者が満足する形で確立するものとする (SHALL)。

CA 準拠性監査は毎年、CA 業務を直接行っている部門から独立した、PKI に精通した第三者によって行われるものとする (SHALL)。

2.7.2. 監査者の身元・資格

CA は、CA 業務を直接行っている部門から独立した、PKI に精通した第三者に定期監査を委託するものとする。

2.7.3. 監査者と被監査者の関係

監査者は、CA 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を持たないものとする (SHALL)。

2.7.4. 監査テーマ

証明書所有者登録、証明書登録、危殆化した鍵の報告、及び証明書失効などのイベントが監査されるものとする (SHALL)。

監査は、一般に、CP 及び関連する CPS の準拠性をカバーする。

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、各 CA が定めるセキュリティポリシー委員会（以下、ポリシー委員会）が対応を決定するものとする。この指摘事項に関しては、ポリシー委員会が、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、その措置を本サービスの運用管理者に指示する。ポリシー委員会はあらかじめ監査指摘事項への具体的対応を CPS により定めておくこと。講じられた対策の結果はポリシー委員会、及び、その関連組織に報告され、評価されるとともに、次の監査において確認されること。

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が発見された CA 又は RA は、証明書所有者及び検証者に直ちに通知するものとする（SHALL）。

2.8. 秘密保持

2.8.1. 秘密扱いとする情報

1. 証明書所有者の個人情報で、RA が本人確認の目的で収集をしたが、証明書に含まれない情報は、秘密に保たれるものとする（SHALL）（身分証明書、経歴調査、自宅住所、連絡先の詳細など）。この情報の一部は、証明書所有者の同意を得て、その証明書所有者のディレクトリリスティングに含めることがある。
2. 私有鍵

2.8.2. 秘密扱いとしない情報

1. 公開鍵
2. ヘルスケア専門資格者と非公的資格ヘルスケア専門職の役割
3. ヘルスケア上の専門性

2.8.3. 証明書失効及び一時停止情報の開示

CA は、証明書所有者の証明書失効又は停止の理由に関する情報を秘密に保つものとする（SHALL）。

2.8.4. 法的執行機関への情報開示

秘密情報は、証明書所有者の明白な同意に基づいて、又は法律の下での要求に従ってだけ公開されるものとする（SHALL）。

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（SHALL）。

2.8.6. 証明書所有者の要求に基づく情報開示

秘密情報は、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要求に従って、証明書所有者によって指名された関係者に開示されるものとする（SHALL）。

2.8.7. その他の理由に基づく情報開示

秘密情報は、法律により認められた方法による要求に従ってのみ開示されるものとする。

2.9. 知的財産権

本 CP では、規定をしない。

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 CP 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 CountryName、LocalityName、OrganizationName、OrganizationUnitName、CommonName、SurName、GivenName、e-mail を用いる。この中で CountryName 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、所有者がヒトである場合、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。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。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。

LocalityName、OrganizationName、OrganizationUnitName はオプションで使用目的を規定しない。SurName はオプションで、使用する場合は日本の姓名の「姓」に相当する値を格納する。GivenName はオプションで、使用する場合は日本の姓名の「名」に相当する値を格納する。

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

本 CP では規定をしない。

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

CP は、名前クレーム紛争が発生した状況で適用される名前クレーム紛争解決手続を持つものとする (SHALL)。

3.1.6. 登録商標の認識・認証・役割

本 CP では、規定をしない。

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。

3.1.8. 組織の認証

ヘルスケア組織、支援組織、又は組織に代わって活動する個人は、国又は自治体に対応した適切な文書の提示によって、自らの存在とヘルスケアでの役割の証拠を RA に提示するものとする (SHALL)。

及び適用可能な場合は AA も、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 (SHALL)。

RA は組織若しくは団体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. 組織若しくは団体が実在していること、及び、その組織が保健医療福祉機関あるいはその他関連事業者であること (実在性及び有資格性) の識別

法人組織の場合 : 登記簿謄本、法人印鑑証明書等により実在確認を行う。また、保健医療福祉機関であることを証明する書類 (開業届け等の受理書等の写し) により行う。

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 (開業届けの受理書、保険事業者の指定書等の写し) 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、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有資格性の確認を行うものとする。

2. 組織若しくは団体の名前にお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署名 (自署) 押印を行っていること。

法人組織の場合 : 法人印鑑証明書等により確認を行う。

個人事業者の場合 : 代表者個人の印鑑証明書等により確認を行う。

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 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 1. 及び 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。

上記の手続でぜい弱性を生じない範囲及びその主旨を変更しない範囲で「商業登記に基礎を置く電子認証制度」及び「公的個人認証サービス制度」を利用することに置き換えても良い。

3.1.9. 個人の認証

医療従事者等のサービス供給者、患者 / 保健医療福祉サービス利用者としての個人は、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 (SHALL)。本 CP では、認証機関の窓口において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、出生の年月日、男女の別、住所」(以下「基本 4 情報」という。) と住民票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

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。

3. 国家資格保有の確認

医療専門家の国家資格免許を認証するためには、関係官庁によって発行された職業上の国家資格免許状や身分証明書又はその写しを RA に提示するものとする (SHALL)。

上記の手続でぜい弱性を生じない範囲及びその主旨を変更しない範囲で「商業登記に基礎を置く電子認証制度」及び「公的個人認証サービス制度」を利用することに置き換えても良い。また、公開されたアクセス可能な公的資格台帳がある場合はこれを利用することを妨げない。

3.2. 通常の更新

3.2.1. CA の通常更新

CA 情報の通常の鍵更新は、元の記録が作成されたときに使用された元の文書に基づいて行われるものとする (SHALL)。

3.2.2. RA の通常更新

RA 情報の通常の鍵更新は、元の記録が作成されたときに使用された元の文書に基づいて行われるものとする (SHALL)。

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、元の記録が作成されたときに使用された元の文書又は記録を再び参照することによって行われるものとする (SHALL)。

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。

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の再提出を必要とするものとする (SHALL)。

3.3.2. RA 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必要とするものとする (SHALL)。

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 (SHALL)。

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。

3.4. 失効申請

3.4.1. CA の失効申請

ヘルスケア PKI 内の CA が別の CA に失効申請を行うときには、次のようにするものとする。

1. 証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請書に私有鍵で署名して、メッセージを暗号化し、関連するドメイン CA に送信する方法や CA を認

証できる方法により行われるものとする。

3.4.2. RA の失効申請

ヘルスケア PK I 内の RA が CA に失効申請を行うときには、次のようにするものとする (SHALL)。

1. 失効を要求する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請書に私有鍵で署名して、メッセージを暗号化し、関連するドメイン CA に送信する方法や RA を認証できる方法により行われるものとする。

3.4.3. 証明書所有者の失効申請

ヘルスケア PK I 内の証明書所有者が CA に失効申請を行うときには、以下の手順に従うものとする。

1. 失効を申請する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請に私有鍵で署名して、メッセージを暗号化し、関連したドメイン CA に送信する。

私有鍵を含んでいるトークンが紛失又は盗まれた場合等証明書所有者がデジタル署名付きの要求を開始できない場合は、他の何らかの手段を用い、証明書を取得するために提供したものと同等の本人確認のための書類を添える。

署名付き失効申請を必要とすることは、鍵危殆化が疑われる場合でも矛盾しないことに注目すべきである。失効申請は、本当に証明書所有者からのものであるか、又は、第三者が危殆化した鍵を使用して要求を開始したかのどちらかであり、いずれにしても鍵は失効されるべきである。

4. 運用上の要件

4.1. 証明書の申請

本 CP では、規定をしない。

4.2. 証明書の発行

本 CP では、規定をしない。

4.3. 証明書の受理

本 CP では、規定をしない。

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 CP、適用可能な 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. 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（例えば、ヘルスケア専門資格者が特定の組織から退職した場合）
5. CA が、本 CP 及び / 又は適用可能な 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
6. いかなる理由でも、証明書所有者又は認定ヘルスケア提供者の認定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、CA 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
- ・IA の職員
- ・IA と連携している RA の職員

4.4.3. 失効要求手続

失効要求が CA によって受領されたとき、セクション 3.4 に従って、CA 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載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。

4.4.4. 失効要求の猶予期間

証明書の失効要求の結果として取られる処置は、受領後直ちに開始されるものとする。

4.4.5. 一時停止事由

ヘルスケア PKI 内の CA は、停止をサポートしてもよい。証明書の停止を正当化する識別された事由には、

次のものが含まれる。

1. 私有鍵の危殆化の疑いがある場合。停止は調査中にも起きる。
2. 証明書に関する情報が明確化されるまで。
3. 証明書所有者が停止を要求した場合。
4. ローカルのヘルスケア PKI ドメイン内で決定されたその他の事由。

4.4.6. 一時停止を申請できる者

CA が停止をサポートしている場合、証明書の停止は、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。

- ・その名前で証明書が発行された証明書所有者
- ・IA の職員
- ・IA と連携している RA の職員
- ・検証者

4.4.7. 証明書の一時停止手続

停止要求が CA によって受領されたときには、前述の 4.4.5 に従って、CA は次のようにするものとする。停止要求が証明書所有者からであると主張されている場合、要求者の身元を確認する。停止要求の理由を確認して、それが真実であると実証された場合は、証明書を停止する。

4.4.8. 一時停止期間の限度

証明書の停止期間は、(情報の確認などに) 必要な調査の期間に限られるものとする (SHALL)。停止は 10 営業日を超えないことが推奨される。

4.4.9. 失効リスト発行の頻度

失効の通知は直ちに公開する。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/ARL をチェックすべきである。検証者は、CRL/ARL を少なくとも毎日、失効の有無を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

CA 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 の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

署名して応答する機能を備えたオンライン証明書状態チェックのサーバを利用しオンライン失効チェックを可能とする場合は、サーバと証明書所有者が安全な通信を確立できるようにする必要がある。証明書の真正性の検証は CA によって実現されてもよく、また CA ではなく、有効性確認局又は外注ディレクトリを使用し検証されてもよい。

4.4.13. その他利用可能な失効確認公表手段

本 CP 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 CP 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 署名鍵の危殆化の際には、CA は MEDIS ルート認証局及び関連組織に直ちに通知するものとする。

4.5. セキュリティ監査の手続

セキュリティ監査手続は、ISO 17799-1:2000 と同等以上の規格に従うものとする。

例えば、ISO/IEC17799:2000 の

第 8 章 通信及び運用管理

第 9 章 アクセス制御

第 10 章 システムの開発及びメンテナンス

第 12 章 適合性

等がこれに相当する。

4.6. 記録の保管

記録は、ISO 17799-1:2000 と同等以上の規格に従って保管されるものとする。

例えば、ISO/IEC17799:2000 の

第 10 章 システムの開発及びメンテナンス

第 12 章 適合性

12.1.3 組織の記録の安全防護

等がこれに相当する。

4.7. 鍵の切替え

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

セキュリティ監査手続は、ISO 17799-1:2000 と同等以上の規格に従うものとする。

例えば、ISO/IEC17799:2000 の

第 7 章 物理的及び環境的セキュリティ

第 8 章 通信及び運用管理

第 11 章 事業継続管理

等がこれに相当する。

4.9. CA の終了

CA が運営を停止する場合には、運営の終了時に直ちに証明書所有者に通知し、CA の鍵と情報の継続的な保管を手配するものとする (SHALL)。また、MEDIS ルート認証局及び関連している組織のすべてに対しても通知するものとする (SHALL)。

CA の運営がより低い保証レベルで運営されている別の CA に譲渡される場合には、運営が譲渡される CA によって発行された証明書は、譲渡に先立ち、その CA によって署名された CRL を通じて失効されるものとする (SHALL)。

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取決めを行うこと。

5. 建物・関連設備、運用、要員のセキュリティ管理

これらは、ISO 17799-1:2000 と同等以上の規格、又は認可された認定あるいは免許基準に従うものとする。これは、セクション5に適用され、次の項目をカバーする。

5.1. 建物及び関連設備管理

5.1.1. 施設の位置と建物構造

隔壁により区画されていること。

5.1.2. 入退管理

入退出者の本人確認方法を定められた方法により確実にを行い、かつ入退出の記録を残すこと。

認証設備室への立入りは、立入りに係る権限を有する複数の者により行われること。設備の保守その他の業務の運営上必要な事情により、やむを得ず、立入りに係る権限を有しない者を認証設備室へ立入らせることが必要である場合においては、立入りに係る権限を有する複数の者が同行すること。

5.1.3. 電源及び空調設備

室内において使用される電源設備について停電に対する措置が講じられていること。

5.1.4. 水害及び地震対策

水害の防止のための措置が講じられていること。

認証業務用設備は通常想定される規模の地震による転倒及び構成部品の脱落等を防止するための構成部品の固定その他の耐震措置が講じられていること。

5.1.5. 防火設備

自動火災報知器及び消火装置が設置されていること。防火区画内に設置されていること。

5.1.6. 記録媒体

アーカイブデータ、バックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続きに基づき適切に搬入出管理を行う。

5.1.7. 廃棄物の処理

機密扱いとする情報を含む書類・記録媒体の廃棄については、所定の手続きに基づいて適切に廃棄処理を行う。

5.1.8. オフサイト・バックアップ

物理的管理は、ISO 17799:2000 と同等以上の規格に従うものとする（SHALL）。

バックアップ媒体は、メインサイトにおける災害が発生しても、その災害によって損傷しないように、十分に離れた所に置くことが望ましい。

5.2. 手続的管理

手続的管理は、ISO 17799:2000 と同等以上の規格に従うものとする。

例えば、ISO/IEC17799:2000 の「第8章 通信及び運用管理」がこれに相当する。

5.3. 要員管理

人事的管理は、ISO 17799:2000 と同等以上の規格に従うものとする。

例えば、ISO/IEC17799:2000 の「第6章 スタッフのセキュリティ」がこれに相当する。

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

証明書所有者の公開鍵 / 私有鍵のペアは、次のものによって生成されるものとする。

1. CA

2. 証明書所有者。ただし CA によって承認された鍵管理機能又はアプリケーションを使用して生成されるものとする。

CA の署名鍵生成及び管理は、認証設備室内で複数の者によって専用の電子計算機を用いて行われること。

6.1.2. 所有者への私有鍵の送付

私有鍵が証明書所有予定者によって生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、証明書所有者に引き渡されるものとする (SHALL)。CA はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする (SHALL)。ただし、このようなコピーが後述の 6.2.4 に従って鍵のバックアップの目的で保持される場合は除く。

6.1.3. CA への公開鍵の送付

公開鍵が CA によって生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、CA に引き渡されるものとする。

6.1.4. 証明書所有者への CA 公開鍵の配付

公開鍵は証明書に結合されるので、公開鍵は、作成後直ちに証明書とともに証明書所有者に送られるものとする。公開鍵の引渡しには、証明書の引渡しと同じ手続が適用されるものとする。

6.1.5. 鍵のサイズ

鍵の最小サイズは、使用されるアルゴリズムに依存する。CA 証明書の鍵の最小サイズは、RSA アルゴリズムの場合、2048 ビットとする (SHALL)。他のアルゴリズムを使用する CA 証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする (SHALL)。CA 以外の証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同等のアルゴリズムの場合、1024 ビットとする (SHALL)。他のアルゴリズムを使用する CA 以外の証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする (SHALL)。

6.1.6. 公開鍵のパラメータ生成

公開鍵パラメータは、CA により生成されるものとする (SHALL)。

6.1.7. パラメータ品質の検査

パラメータの品質チェックは、監査組織の役割とする (SHALL)。

6.1.8. ハードウェア又はソフトウェアによる鍵ペア生成

鍵の生成は、安全な方法で行われるものとする。

6.1.9. 鍵の使用目的

署名を目的とする署名用証明書においては、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証明書プロファイルの keyUsage のビットの内、nonRepudiation 以外のビットをオンにしないこととする。

認証を目的とする認証用証明書を発行する場合には、digitalSignature と keyEncipherment 以外のビットを立てないものとする。

また、認証を目的とする認証用証明書を発行する場合は、署名を目的とする署名用証明書を発行する CA とは別の CA とする。

データの暗号化目的には別個の鍵ペアがあるものとするが本 CP では扱わない。

* 認証用鍵を否認防止目的のための署名に共用した場合は認証プロトコルで用いられる署名機能によっては、悪意により、否認防止対象文書のハッシュ値に電子署名を行わせるかもしれないぜい弱性を持つ場合があることを留意すべきである。

6.2. 私有鍵の保護

本 CP では 2 つの鍵ペアが存在すべきことを推奨する。1 つは、暗号のためのペアであり、CA は私有鍵をバックアップすることができる。もう 1 つは、本人認証又はデジタル署名鍵であり、この私有鍵はエスクロウしてはならない。

6.2.1. 暗号モジュールに関する標準

CA 署名鍵は、US FIPS 140-2 レベル 2 と同等以上の規格に準拠するものとする。ただし、電子署名法に適合させる場合は、CA 署名鍵は、US FIPS 140-2 レベル 3 と同等以上の規格に準拠するものとする。他の証明書は、US FIPS 140-2 レベル 1 と同等以上の規格に準拠するものとする。

6.2.2. 複数人による私有鍵の管理

私有鍵は業務上又は診療行為上緊急に必要な場合を除き所有者の管理とし、複数人の管理は認めない。

6.2.3. 私有鍵のエスクロウ

認証又はデジタル署名のために使用される私有鍵は、法律によって必要とされる、あるいは、本人以外が私有鍵を利用できない機能を持った預託機構に預ける場合を除き、エスクロウされないものとする。

6.2.4. 私有鍵のバックアップ

可能な場合、証明書所有者は私有鍵をバックアップすることが推奨される (RECOMMENDED)。(私有鍵がソフトウェアトークンに格納されている場合など。)

私有認証鍵又はデジタル署名鍵は、証明書所有者の管理の下で完全にバックアップされるものとする (SHALL)。バックアップされた鍵は、証明書所有者の環境 (仕事場、部課、又は組織) 内に保持されるものとする (SHALL)。

私有鍵は、一次のコピーとして必要なレベルより低くない保護レベルでバックアップされるものとする。

6.2.5. 私有鍵のアーカイブ

CA は証明書所有者の私有鍵をアーカイブしない。

6.2.6. 暗号モジュールへの私有鍵の格納

私有鍵がエンティティの暗号モジュールで生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従って、又は同様に安全な方法で、モジュールに入力されるものとする。

6.2.7. 私有鍵の活性化方法

ヘルスケア PKI においては、証明書所有者だけが私有鍵を活性化することができる。証明書所有者は、私有鍵の活性化の前に、私有鍵を保護している暗号モジュール又はアプリケーションに認証されるものとする。この認証は、パスワード、パスフレーズ、又はバイOMETリックの形式を取ってよい。非活性化された私有鍵は、アクセス制御されたハードウェア又は / 及び暗号化された形式で保管されるものとする。

6.2.8. 私有鍵の非活性化方法

鍵が非活性化されアクセス制御されないメモリに格納されている場合は、メモリが割当て解除される前に、鍵がメモリから消去されるものとする。鍵が格納されていたディスク領域は、その領域がオペレーティングシステムに解放される前に上書きされるものとする。暗号モジュールは、事前設定された非活動期間の後に自動的に私有鍵を非活性化するものとする。

6.2.9. 私有鍵の廃棄方法

私有鍵の使用の終了時には、私有鍵及びそのすべてのコピーは、確実に破壊されるものとする。
私有鍵破棄手続は、CPS 又は公的に入手可能な文書で記述するものとする。

6.3. 鍵ペア管理に関するその他の面

6.3.1. 公開鍵の保管

公開鍵は、後日の署名の検証を可能にするために、信頼できる第三者によって保管される必要がある。CA は、公開鍵が保管されたことを保証する責任があるものとする。

6.3.2. 私有鍵と公開鍵の有効期間

CA 以外の公開鍵と私有鍵の使用は、3 年を超えないものとし、その後新しい鍵ペアが発行されるものとする。属性証明書は業務上の必要性により、より短い期間でも良い。CA の公開鍵と私有鍵の使用は、10 年を超えないものとし、その後新しい鍵ペアが発行されるものとする。

6.4. 活性化用データ

活性化データは、一意で予想不能なものとし、証明書所有者に安全に伝えられるものとする。

6.5. コンピュータのセキュリティ管理

これらは、ISO 17799-1 : 2000 と同等以上の規格、又は認可された認定あるいは免許基準に従うものとし (SHALL) また、次の問題をカバーするものとする。

[IETF RFC 2527 セクション 6.5.1 特定のコンピュータセキュリティの技術的な要件

[IETF RFC 2527 セクション 6.5.2 コンピュータセキュリティの評価

6.6. ライフサイクルの技術的管理

これらは、ISO 17799-1 : 2000 と同等以上の規格、又は認可された認定あるいはライセンス基準に従うものとし、また、次の問題をカバーするものとする。

[IETF RFC 2527 セクション 6.6.1 システム開発の管理

[IETF RFC 2527 セクション 6.6.2 セキュリティマネジメントの管理

[IETF RFC 2527 セクション 6.6.3 ライフサイクルのセキュリティ評価

6.7. ネットワークのセキュリティ管理

これは、ISO 17799-1 : 2000 と同等以上の規格、又は認可された認定あるいはライセンス基準に従うものとする。

例えば、ISO/IEC17799:2000 の

第 8 章 通信及び運用管理

8.5 ネットワークの管理

第 9 章 アクセス制御

9.4 ネットワークのアクセス制御

等がこれに相当する。

6.8. 暗号モジュールの技術管理

これは、ISO 17799-1 : 2000 と同等以上の規格、又は認可された認定あるいはライセンス基準に従うものとする。

例えば、ISO/IEC17799:2000 の

第 10 章 システムの開発及びメンテナンス

10.3 暗号による管理策がこれに相当する。

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

ヘルスケア PKI の CA が発行する証明書は、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。ヘルスケア PKI の所有者の電子証明書の登録情報は、次の表のとおりとする。Issuer の DN は CPS 及びその他開示文書に記述される。

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)	オプション (1)
	Organization (組織名)	組織をあらわす名称とする。 例) MEDIS-DC (1)
	Organization Unit (組織単位名)	オプション 例) MEDIS-CA (1)
	Common Name (発行名)	cn= MD-HPKI-XX-YYYYY (2) 例) MD-HPKI-01-MEDIS-CA-for-nonRepudiation
Subject (発行申請者)	Country (国名)	c=JP (固定)
	LocalityName (地域名)	オプションで使用目的を規定しない
	Organization (組織名)	オプションで使用目的を規定しない
	OrganizationUnit (組織単位名)	オプションで使用目的を規定しない
	Common Name (発行申請者名)	cn=Taro Suzuki 例) (3)
	serialNumber	オプション serialNumber=XXXXX 例) (4)
	surName (姓)	surName=Suzuki (例) (5)
	givenName (名)	givenName=Taro (例) (5)
	E-mail (電子メール)	使用しない (6)

(1) このいずれか 1 つ又はいずれかの組合せで、CA を一意に特定できる名前。

- (2) 発行者の性格や証明書の目的を表す一般的に知られる CA の名称。
IA 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 ”を付加するものとする。“ 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 ”の値が変わる。
“ YYYYY ”は各認証局の名称をあらわす文字列とするが、ヘルスケア PKI 内で同一の名称とならないように決定する。
- (3) 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。
- (4) serialNumber はオプションとし、使用時は、XXXXX に認証局において一意となる番号を使用する。
- (5) surName と givenName はオプションで、使用する場合は、それぞれ、姓、名を格納する。
- (6) RFC3280 では、このフィールドを使用しないことが推奨され、電子メールアドレスを使用する場合は、SubjectAltName に格納することが推奨されている。

ヘルスケア PKI の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)	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 (ISO TS17090)。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)	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)	署名を目的とする署名用証明書においては、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証明書プロファイルの keyUsage のビットの内、nonRepudiation 以外のビットをオンにしないこととする。また認証を目的とする認証用証明書において digitalSignature の他に keyEncipherment のビットを立てるものとする。
certificatePolicies (2.5.29.32)	証明書の OID を格納。 (7) 1.2.392.200119.1.1.1.2.1.3.1 ヘルスケア PKI 認証局署名用証明書 1.2.392.200119.1.1.1.2.2.3.1 ヘルスケア PKI 認証局認証用証明書
subjectAltName (2.5.29.17)	多バイト文字コードの名前を使用する場合は、UTF-8 を使用して、ここに格納。 (8) また、電子メールアドレスを使用する場合は、ここに格納。
subjectDirectoryAttributes (2.5.29.9)	ISO TS 17090 に準拠した hcRole attribute を記述するものとする。HcRole 以外の attribute を使用しない。 (9)
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。 (10)

- (7) 証明書の OID の内、次のものはテスト用証明書である。
 - ・ 1.2.392.200119.1.1.1.1.0 : MEDIS ルート認証局が発行するテスト用証明書。
 - ・ 1.2.392.200119.1.1.1.2.0.(以降任意): 下位認証局が発行するテスト用の証明書。
- (8) 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する。
- (9) 次の国家資格が対象となる。
 - hcRole で使用する値 対応する国家資格

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

- (10) このフィールドは OCSP レスポンダを利用しない限り必須。OCSP レスポンダを採用する場合は使用しない。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 とすることを推奨する。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るが、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する。

ヘルスケア PKI の各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。

	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)	
Issuer フィールド						
CountryName	C	C	C	C	C	
LocalityName	O	O	O	O	O	
OrganizationName	C	C	C	C	C	
OrganizationUnitName	O	O	O	O	O	
CommonName	C	C	C	C	C	
Subject フィールド						
CountryName	C	C	C	O	C	
LocalityName	O	O	O	O	O	
OrganizationName	O	O	O	O	C	
OrganizationUnitName	O	O	O	O	O	
CommonName	C	C	C	C	C	
GivenName	O	O	O	O	N	
SurName	O	O	O	O	N	
e-Mail	O	O	O	O	O	

C : 必須。O : オプション。N : 使用しない。SP : 専門職。

	国家資格専門職	その他資格専門職	非専門職	患者/保健医療福祉サービス利用者	医療機関(組織)	備考
version	C	C	C	C	C	X.509 v3
serialNumber	C	C	C	C	C	IA の中で一意
signature	C	C	C	C	C	(11)
issuer	C	C	C	C	C	
validity	C	C	C	C	C	(12)
subject	C	C	C	C	C	
subjectPublicKeyInfo	C	C	C	C	C	(13)
issuerUniqueID	N	N	N	N	N	
subjectUniqueID	N	N	N	N	N	
authorityKeyID	M	M	M	M	M	
subjectKeyID	M	M	M	M	M	
keyUsage	C	C	C	C	C	
extKeyUsage	O	O	O	O	O	(14)
privateKeyUsagePeriod	N	N	N	N	N	(15)
certificatePolicies	M	M	M	M	M	
policyMappings	N	N	N	N	N	
subjectAltName	M	M	M	M	M	
issuerAltName	N	N	N	N	N	
subjectDirectoryAttributes	M	O	O	O	O	
hcRole	M	N	N	N	N	ISO TS17090
basicConstraints	N	N	N	N	N	
nameConstraints	N	N	N	N	N	
policyConstraints	N	N	N	N	N	
CRLDistributionPoints	M	M	M	M	M	
authorityInformationAccess	O	O	O	O	O	
qualifiedCertificateStatements	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。

(11) signature フィールドには署名アルゴリズムの OID を格納する。

総務省及び経済産業省の「暗号技術検討会 2001 年度報告書」では、次の 5 つの署名アルゴリズムが電子政府暗号候補にあげられている。

1. sha1WithRSAEncryption (1.2.840.113549.1.1.5)
2. RSA-PSS- with-sha1 (1.2.840.113549.1.1.10)
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)

本 CP では、アルゴリズムを特に規定しないが、現時点での互換性を考慮し、少なくとも最も広く

用いられている sha1WithRSAEncryption (1.2.840.113549.1.1.5)は実装しておくことを推奨する。使用する署名アルゴリズムは CPS 及び公開文書に規定される。

- (12) 公開鍵証明書の有効期間である。終了期限が 2049 年未までの場合は UTCTime 形式で表示し、グリニッジ標準時を使用する (YYMMDDhhmmssZ)。分単位までの表示も許されるが、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する。2050 年以降は GeneralizedTime 形式を使用する (YYYYMMDDhhmmssZ)。
- (13) 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する。アルゴリズム識別子は OID で指定する。総務省及び経済産業省の「暗号技術検討会 2001 年度報告書」では、次の 3 つのアルゴリズムが示されている。

- 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)

署名アルゴリズムと同様で、本 CP ではアルゴリズムを規定しない。しかし現時点での互換性を確保するために、少なくとも最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る。使用する署名アルゴリズムは CPS 及び公開文書に規定される。

- (14) keyUsage 以外の公開鍵の使用目的を示す。subject が人又は組織で、keyUsage で nonRepudiation 又は 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る。
- (15) このフィールドは使用することを推奨しない。このフィールドが空の時のデフォルト値は、証明書の有効期間とする。

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 CP7.1 の 11 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. 本ポリシーの管理

8.1. 改定手続

この CP に対するいかなる変更にも先立って、ヘルスケア PKI セキュリティポリシー委員会は、本 CP の基に関連するすべての CA に通知し、コメントを求めるものとする (SHALL)。ポリシーの変更は、ヘルスケア PKI セキュリティポリシー委員会によって承認されるものとする。

8.2. 公表と通知の手続

CA の公認の代表者によってデジタル署名された証明書ポリシー文書の電子コピーが、次のように入手可能にされなければならない。

1. すべての検証者が利用できる Web サイト上
2. 電子メールでの要求

8.3. CP の承認と通知の手続

CPS は、CA サービスの実装と鍵ライフサイクル管理の手続を正確に詳述する。それは CP より詳細であり、CA のセキュリティを確保するために秘密に保たれる情報が含まれていてもよい (MAY)。CP は、ヘルスケア PKI セキュリティポリシー委員会によって承認されるものとする。

変更履歴

1.公開鍵証明書発行の際の本人確認の厳格性

本人確認の方法については、概ね次の4つのレベルが想定される。

(地方公共団体における個人認証基盤検討委員会平成12年3月発行「地方公共団体における個人認証基盤の在り方について」を参考)

総務省の平成14年2月28日発行の「地方公共団体による公的個人認証サービス制度の創設について」の中の本人確認はレベル3であるので、本CPもレベル3とした。診察券として用いる場合はレベル2で良いのではないかとの意見もあったが、患者情報へのリモートアクセスにも使用されるのでレベル3とした。レベル2も認める場合はOIDを変更して発行することになるが認めていくかは今後の運用状況により見直していくこととする。

(1) 本人確認のレベル

(レベル1)(rudimentary assurance)

申請者から提出された電子メールのアドレスが当該申請者に対して正しく送信できるものであることだけを確認する。本人の同一性確認は行わない。

(レベル2)(basic assurance)

オンラインにより申請者から提出された申請書の内容について、住民基本台帳等の記載内容と照合する。

(レベル3)(medium assurance)

認証機関の窓口において申請者から提出された申請書の内容を住民基本台帳等と照合するとともに、官公署の発行した身分証明書等の本人確認を行うための書類の提示を求める。

(レベル4)(high assurance)

申請者から提出された申請書の内容を住民基本台帳等と照合した上で、申請者が申請を行った事実を認証機関が郵送その他の方法により当該申請者に対して文書で照会し、その回答書を認証機関に持参してもらう。

(2) OIDによる本人確認のレベルを分ける例

1.2.392.200119.A.B.C.D.E.3.V 本ポリシ(医療従事者等のサービス供給者用)

1.2.392.200119.A.B.C.D.E.2.V 本ポリシ(患者/保健医療福祉サービス供給者用)

2.OIDについて

OIDに関し以下のような基本体系とした。

基本体系:1.2.392.200119.A.B.C.D.E.F.V

ここで、A、B、C、D、E、F、Vは、MEDIS-DCにおいて管理対象を識別するために体系づけられるものである。

Aが「セキュリティ」を意味するものとして「1」の値をとり、

Bが「医療PKI」を意味するものとして「1」の値をとり、

Cが「証明書ポリシ」を意味するものとして「1」の値をとり、

Dが「認証局種類」を意味するものとしてルート認証局は「1」下位認証局は「2」の値をとり、

Eが「証明書種類」を意味するものとしてテスト用「0」、署名用「1」、認証用「2」の値をとり、

Fが「セキュリティレベル」を意味するものとし、ここでは、セキュリティレベルを解説1の1~4の4段階で表すものとする。

Vはガイドラインのメジャーバージョンの値とする。

3. Common Name について

「Issuer の CommonName に CP(証明書ポリシー)を示す文字列を入れるとした場合、CP のガイドラインのバージョンが変わる度に issuer を変更することになる。この事は、ガイドラインのバージョンアップの度に新たな証明書発行者に変更されることになり、新たな CA 局を立て直す必要が生じる。これは CA 局の運用がかなり複雑になってくる。一方、CP(証明書ポリシー)は、OID を取得し、証明書プロファイルの「certificatePolicies」に格納されるので、Issuer の CommonName に CP のバージョンを入れなくても、「certificatePolicies」の OID を参照することにより対応 CP が判別可能となる。

したがって、Issuer の CommonName は通常、一般に知られた認証局の名称（例えば Metropolitan Hospital Certificate Authority 等）を入れる場合が多いのでそのようにした方が良いと思われる。（もし CP 名を入れるとすると、バージョン番号は入れず、CP 名のみとし、CP の各バージョンのヒストリーと内容を Web 上で公開するとともに、対応する OID を「certificatePolicies」に入れるべきと思われる。）しかし、「certificatePolicies」は Mandatory で検証者が必ずしも解釈する必要がない。医療福祉分野ではポリシマッピングを一致させ、一致していない所は排除すべきで、必ず検証プログラムはバージョンをチェックすべきである。ポリシーが変更になれば厳密には認証局は新旧並列して運用する方法も考慮すべきかもしれない。

したがって、互換性やぜい弱性が損なわれない限りではバージョン記号の X.YY の YY を変更させる等の運用を行っていくこととし、ガイドライン原案のままとした。本課題は引き続き検討していくべきものである。

4. 「公的個人認証サービス制度」及び「商業登記に基礎を置く電子認証制度」の利用

「商業登記に基礎を置く電子認証制度」及び「公的個人認証サービス制度」を用いた本人確認やオンライン申請、磁気媒体による申請は今後の推進すべき課題である。公的個人認証基盤は法律案が検討されている状態なのでその動きを見守る必要がある。したがって本 CP の本バージョンでは「ぜい弱性を生じない範囲及びその主旨を変更しない範囲で置き換えても良い。」とした。

5. subjectDirectoryAttributes について

ガイドラインでは subjectDirectoryAttributes については、国家資格専門職の証明書においては“critical”としていたが、subjectDirectoryAttributes は TS17090 では“Mandatory”、RDC3280 では“must be non-critical”とされている。よって「ヘルスケア認証局証明書ポリシー（暫定2版）」の P.27 の表中の当該 subjectDirectoryAttributes および hcRole の国家資格専門職の証明書欄の「C」を「M」に変更する。これに伴い本 Attributes の証明書プロファイルのクリティカリティを True から False に変更する。

<TS17090-3 からの変更点について>

(1) 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 CP 6.2、6.3、及び 6.4 に従って確実に保護されていることを保証するものとする (SHALL)。(TS17090 と同じ)

以下の 3 行は暗号用鍵に関するものであり、本 CP では暗号用鍵は発行しないので TS17090 にある以下の 3 行は外した。

CA は自身がバックアップ又は保存した証明書所有者の私有復号鍵が本 CP 6.2 に従って保護されていることを保証するものとする (SHALL)。CA は、法によって必要とされない限り、証明書所有者の事前同意なしにいかなる他者にも私有復号鍵を開示しないものとする (SHALL)。

(注) 下記 5 行については、TS17090 にはあるが次の理由で外した。本 CA は資格を保有する本人が責任を持って申請するものとし、雇主が資格を認可する責任を持つものではない。また、暗号鍵は本 CP の範囲ではない。

「前述にかかわらず、CA は暗号データの回復の目的のために私有鍵のバックアップサービスを提供しても良い。その場合、非公的資格ヘルスケア専門職あるいは支援組織従業員も彼らの雇主のビジネスを実行するために証明書を受け取っているが故に、CA は、データ回復の目的のために、そのような取決めが証明書の発行前に合意されている場合は、非公的資格ヘルスケア専門職あるいは支援組織従業員の雇主に私有復号鍵を開示しても良い。」

(2) 2.1.2.1 証明書失効申請

RA は、証明書失効申請の取扱いを行うことができる。一部のヘルスケア PKI 実装では、RA は、証明書失効申請手順を開始又は認証するために使用されてもよい (MAY)。適用可能な場合、RA は、認証した要求を適切な CA に転送するものとする (SHALL)。(TS17090-3 と同じ)

(注) 以下の 3 行については、TS17090 にはあるが次の理由で外した。本 CA は、公的資格そのものを認可する登録局ではなく、他が認可した公的資格を確認して公的資格項目付き証明書を発行する。

「RA 自身が失効申請を開始してもよい (MAY)。(例えば、ヘルスケア専門資格者が不行跡により停職となり、RA がヘルスケア専門資格の登録局又は認可局である場合)、いずれにしてもレポートを認証するのは RA の責任である。」

(3) 2.2.1 認証局の責任 7 項 については下記、CP 修正案と TS17090 のいずれが良いか検討を行った。その結果医療上では本人確認を厳密に行う必要があることから、当面 CA の管理をより厳しく要求される TS17090 に従うこととし、今後の検討事項とした。

* CP 修正案 : CA は、本 CP 及び別途定める CPS に規定した内容を遵守して証明書の発行、失効を含む鍵管理サービスを提供し、CA 私有鍵の信頼性の確保を保証するものとする (SHALL)。

* TS17090-3 : CA 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 (SHALL)。この責任は、CA 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。

(4) 2.2.2 登録局の責任 1 項については下記、CP 修正案と TS17090 のいずれが良いか検討をおこなった。その結果上記 (3) と同様に医療上では身元確認を厳密に行う必要があることから、当面 RA の管理をより厳しく要求される TS17090 に従うこととし、今後の検討事項とした。

CP 修正案 : RA は、本 CP 及び別途定める CPS に規定した内容を遵守して証明書の発行、失効を含む鍵管理サービスを提供し、CA 私有鍵の信頼性の確保を保証するものとする (SHALL)。

TS17090-3 : 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、個人の身元とそれに関連づ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。

- (5) 2.7.2 監査者の身元・資格については下記、CP 修正案と TS17090 のいずれが良いか検討をおこなった。その結果、TS と同等の効果をもつ、現状に即した表現として修正案を採用した。

CP 修正案：CA は、CA の準拠性監査について CA 業務に精通している外部機関に定期監査を委託するものとする。

TS17090-3：監査者は、(ISO9000 認定など) 関連専門家団体への加入に必要な程度の情報システム監査者としての資格をもつものとする (SHALL)。監査者は、豊富な PKI 経験を持つものとする。正式な認定団体が存在する場合、監査者はその団体の要件を満たしているものとする。

後述の (12) にて再度の検討内容を記述している。

- (6) 2.7.5 については下記、CP 修正案と TS17090 のいずれが良いか検討をおこなった。その結果、TS は欠陥カテゴリーにより CA 管理団体の対応を定めている (MAY) が、具体性が乏しいので、技術的進歩と合わせて CPS で具体的に定めるほうが望ましいとのことで、「ポリシ委員会はあらかじめ監査事項への具体的対応を CPS により定めておくこと」との文言を追加し、修正案を採用することとした。

CP 修正案：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、各 CA が定めるセキュリティポリシ委員会 (以下、ポリシ委員会) が対応を決定するものとする。この指摘事項に関しては、ポリシ委員会が、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、その措置を本サービスのサービス運用管理者に指示する。講じられた対策の結果はポリシ委員会、相互認証先、及び、その関連組織に報告され、評価されるとともに、次の監査において確認されること。

TS17090-3：欠点に対して取るべき行動 監査で違反が発見された場合、CA は是正措置を取る (SHALL)。もし CA が監査結果に対して適切な措置を取らなかった場合、CA を管理する団体は次のようにしても良い (MAY)。

1. 違反を指摘するが、次の監査まで運用を続けることを許す。又は、
2. 失効に先立ち問題の是正を保留し、最大 30 日間 CA の運用の続行を許す。又は、
3. CA の証明書は失効する。(注：サービスを中断する恐れがあるので、CA を停止することはできない)

これらのいずれの処置を取るべきかに関する決定は、違反の重大さに基づくものとする。(SHALL)

欠陥カテゴリー - 危機的

CA が CA 認定団体 (このような認定が CA が運用する管轄区域内に存在する場合) によって決定された CPS の不可欠なセクションに従うことができなかった場合は、危機的な欠陥として分類されるものとする (SHALL)。例えば、認証局が費用のかかる手続を省略したために証明書が危殆化したことが検出された場合は、危機的な欠陥として分類されるものとする (SHALL)。

CA がその管轄区域で認定されていた場合、認定を直ちに撤回する。CA の証明書は上記の項目と同様に失効する。

欠陥カテゴリー - 重度

CA が CPS の重要な要素に従わず、それが保証プロセスの一部と評価されていた場合には、重度な欠陥として分類されるものとする (SHALL)。例えば、事業の十分な連続性を維持していない CA が識別された場合は、重度な欠陥として分類されるものとする (SHALL)。

同時に追加のイベントが CA に影響を与えた場合、又は CA が数日以内に準拠性問題を改善できな

った場合には、問題の危機的な欠陥への格上げが課されるものとする（SHALL）。

欠陥カテゴリ - 部分的

CPS への準拠違反は、保証プロセスの一部として評価され、重大な欠陥になる十分な可能性はないが、CA の運用の完全性に影響を与える可能性がある場合、部分的な欠陥として分類されるものとする（SHALL）。例えば、時代遅れのセキュリティポリシー及び手続は、部分的な失敗として分類されるものとする（SHALL）。

このカテゴリ内の追加の欠陥が検出された場合、又は CA が 30 日以内に準拠性問題を改善できなかった場合には、問題の重度な欠陥カテゴリへの格上げが課されるものとする（SHALL）。

欠陥カテゴリ - 軽度

部分的な欠陥になる恐れはないと見られるが、CA の運用の完全性に対する全体的な影響を軽減するために対処すべきである準拠違反は、部分的な欠陥として分類されるべきである。例えば、管理上の欠陥（不正確な料金請求など）は、軽度な欠陥として分類されるべきである。

このカテゴリ内の追加の欠陥が検出された場合、又は CA が次の定期監査までに準拠性問題を改善できなかった場合には、問題の部分的な欠陥への格上げが課されるものとする（SHALL）。

- (7) 3.1.7 私有鍵の所有を証明するための方法 については下記の、本 CP の案と TS17090 のいずれがよいか検討をおこなった。その結果、TS17090-3 の CA からの定期的なチャレンジはオプション(MAY)なので、実現性を考えてシステムの負担を減らすよう外した。

CP 修正案：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。

TS17090-3：鍵所有者は、CA に対して行う要求に電子的にサインすることにより私有鍵の所有を証明する必要があり、また CA からのチャレンジサインすることを定期的に求められるかも知れない。

- (8) 以下の項の、sponsored health care provider 等の記述部分は、日本の現状から見て曖昧なので削除した。

* 4.4.1 証明書の失効事由 1 項 の the employer (in the case of a non-regulated health professional or supporting organization employee、 or the sponsor (in the case of a sponsored health care provider)

* 4.4.2 証明書の失効申請ができる者 TS17090-3 7.4.4.2 3. the sponsor of a sponsored health care provider

* 4.4.6 一時停止を申請できる者 TS17090-3 7.4.4.6 3. the sponsor of a sponsored health care provider

- (9) 4.4.7 証明書の一時停止手続

停止要求が CA によって受領されたときには、前述の 4.4.5 に従って、CA は次のようにするものとする（SHALL）。（TS17090-3 と同じ）

停止要求が証明書所有者からであると主張されている場合、要求者の身元を確認する。

TS17090-3 1 項の or from the individual or organization which made the application for the certificate on behalf of a device or application は対象外なので外した。Or from the sponsor of a sponsored health care provider は（8）と同様の理由で外した。

停止要求の理由を確認して、それが真実であると実証された場合は、証明書を停止する。（TS17090-3 4 項と同じ）

TS17090-3 7.4.4.7 の 2.confirm the identity of the requester where the suspension request is

purported to be from the individual or organization which made the application for the certificate on behalf of a device or application は 1 項と紛らわしくまた対象外なので外した。

TS17090-3 7.4.4.7 3.confirm that the requester has the sufficient authority to effect suspension, if the requester is acting as the sponsor of the Certificate holder は (8) と同様の理由で外した。

(10) 2.1.1.6 CA 私有鍵の使用制限

「CA アプリケーションへのアクセスと操作のために」となっているが限定的すぎて、下位認証局のシステム、運用を限定してしまう可能性があるため、「CA は、CA 運用に必要な操作のためだけに CA 職員に発行した私有鍵が、この目的のためだけに使用されることを保証する。」と変更した。

例：RA、LRA 間での業務運用上必要となるメールへの署名等

(11) 2.1.2 登録局の義務

「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署名するためだけに使用されることを保証する。」について

趣旨は RA 担当者なり RA サーバの私有鍵が、証明書申請に必要な作業にのみ使用されることを保証していることと思われる。

申請処理のログイン時点で本人特定、証明書確認を行い、処理時においてその担当者の行った行為は監査ログとして記録されるといったシステムにおいても、申請書に署名を行うことと同等の機能を持つものと考えられる。汎用性を考え証明書申請への署名に限定しない方向で検討し、

「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。」とした。

(12) 2.7.1 監査頻度

2.7.2 監査者の身元・資格

外部機関への定期監査の委託は望ましいと思われるが現状、日本において PKI に関して明確な資格がない為、内部における監査が確実に実行できるものであれば CA の信頼性は維持できるものと思われる。「CA 業務を直接行っている部門から独立した、PKI に精通した第三者によって行われるものとする (SHALL) 」という表現に変更し、内部監査における監査も可能とした。

2.7.3 監査者と被監査者の関係

同様な理由で、「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。」という表現変更を行った。

(13) 6.1.9 鍵の使用目的

次に記述される署名目的と認証目的の 2 種類の証明書を発行することとした。

・ 1.2.392.200119.1.1.1.2.1.3.1 の OID を持つ署名用証明書においては、keyUsage に nonRepudiation 以外のビットは立てないこととする。

・ 1.2.392.200119.1.1.1.2.2.3.1 の OID を持つ認証用証明書においては keyUsage に digitalSignature と keyEncipherment の両方をたてることとした。

暗号目的のデュアルキーペアの証明書ではなく、シングルキーペアの証明書の場合、その鍵ペアでデータを暗号化した場合で、私有鍵が紛失、破壊された場合、2 度とデータの復元を行うことが難しく、その事態を避ける趣旨で ISO17090 は keyUsage に digitalSignature と nonRepudiation 以外のビットは立てないことと記述したものと考察する。ゆえに、署名を目的とした証明書においては、今まで通り keyUsage に digitalSignature と nonRepudiation 以外のビットは立てないこととするが、認証目的で使用する証明書においては、keyUsage に digitalSignature と keyEncipherment の両方を同時に立てることとした。