

保健医療福祉分野 PKI 認証局 証明書ポリシー

平成 18 年 3 月

厚生労働省

(C) Ministry of Health, Labour and Welfare

改定履歴

版数	日付	内容	
初版	平成 17 年 4 月	初版発行	
1.1 版	平成 18 年 3 月	1.1 概要	セキュリティマネジメントに関する参照文書を JIS X 5080:2002 とした。
		3.2.3 個人の認証 <郵送の場合> 2 個人の本人性	本人性の確認が可能であるとして認証局が定める書類のうち一点について、当該書類のコピーの適当な空欄に実印を捺印して郵送することとした。
		3.2.3 個人の認証 <郵送の場合> 4 国家資格及び医療機関等の管理者権限	国家資格証明書等のコピーの郵送にあたり、当該証明書等のコピーの適当な空欄に実印を捺印し、印鑑登録証明書を添えて郵送することとしているが、本取扱を当該証明書等に本人の顔写真が貼付されていない場合に限定する旨の記述を削除した。
		4.2.1 本人性及び資格確認 <本人からの申請の場合> 2 国家資格を有する者への証明書発行 (2) 郵送の場合	国家資格免許証等のコピーの郵送にあたり、当該免許証等のコピーの適当な空欄に実印を捺印し、印鑑登録証明書を添えて郵送することとしているが、本取扱を当該免許証等に本人の顔写真が貼付されていない場合に限定する旨の記述を削除した。
		5.4.3 監査ログを保存する期間	最低 10 年間とした。
		6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間	CA 公開鍵証明書の有効期間は 20 年を超えないものとし、その私有鍵の使用は 10 年を超えないものとした。エンドエンティティの加入者の公開鍵証明書の有効期間は 5 年を超えないものとし、その私有鍵の使用は 2 年を超えないものとした。
		7.1.3 アルゴリズムオブジェクト識別子	基本領域の Signature アルゴリズムに以下を追加した。 sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13)
		9.3.1 秘密情報の範囲	「認証局が秘密保持対象として扱う情報を開示することができる場合」に関する記述の一部を削除した。

1	はじめに.....	1
1.1	概要.....	1
1.2	文書の名前と識別.....	2
1.3	PKIの関係者.....	3
1.3.1	認証局.....	3
1.3.2	登録局.....	3
1.3.3	加入者.....	3
1.3.4	検証者.....	4
1.3.5	その他の関係者.....	4
1.4	証明書の使用法.....	4
1.4.1	適切な証明書の使用.....	4
1.4.2	禁止される証明書の使用.....	4
1.5	ポリシー管理.....	4
1.5.1	本ポリシーを管理する組織.....	4
1.5.2	問い合わせ先.....	4
1.5.3	CPSのポリシー適合性を決定する者.....	4
1.5.4	CPS承認手続き.....	5
1.6	定義と略語.....	5
2	公開及びリポジトリの責任.....	12
2.1	リポジトリ.....	12
2.2	証明書情報の公開.....	12
2.3	公開の時期又はその頻度.....	12
2.4	リポジトリへのアクセス管理.....	12
3	識別及び認証.....	13
3.1	名称決定.....	13
3.1.1	名称の種類.....	13
3.1.2	名称が意味を持つことの必要性.....	13
3.1.3	加入者の匿名性又は仮名性.....	13
3.1.4	種々の名称形式を解釈するための規則.....	13
3.1.5	名称の一意性.....	13
3.1.6	認識、認証及び商標の役割.....	13
3.2	初回の本人性確認.....	13

3.2.1	私有鍵の所持を証明する方法	13
3.2.2	組織の認証	14
3.2.3	個人の認証	14
3.2.4	確認しない加入者の情報	18
3.2.5	機関の正当性確認	18
3.2.6	相互運用の基準	18
3.3	鍵更新申請時の本人性確認及び認証	18
3.3.1	通常の鍵更新時の本人性確認及び認証	18
3.3.2	証明書失効後の鍵更新の本人性確認及び認証	18
3.4	失効申請時の本人性確認及び認証	18
4	証明書のライフサイクルに対する運用上の要件	19
4.1	証明書申請	19
4.1.1	証明書の申請者	19
4.1.2	申請手続及び責任	19
4.2	証明書申請手続	20
4.2.1	本人性及び資格確認	20
4.2.2	証明書申請の承認又は却下	24
4.2.3	証明書申請手続期間	24
4.3	証明書発行	24
4.3.1	証明書発行時の認証局の機能	24
4.3.2	証明書発行後の通知	25
4.4	証明書の受理	25
4.4.1	証明書の受理	25
4.4.2	認証局による証明書の公開	25
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	25
4.5	鍵ペアと証明書の利用目的	26
4.5.1	加入者の私有鍵と証明書の利用目的	26
4.5.2	検証者の公開鍵と証明書の利用目的	26
4.6	証明書更新	26
4.6.1	証明書更新の要件	26
4.6.2	証明書の更新申請者	26
4.6.3	証明書更新の処理手順	26
4.6.4	加入者への新証明書発行通知	26
4.6.5	更新された証明書の受理	26
4.6.6	認証局による更新証明書の公開	26
4.6.7	他のエンティティへの証明書発行通知	26

4.7	証明書の鍵更新（鍵更新を伴う証明書更新）	27
4.7.1	証明書鍵更新の要件	27
4.7.2	鍵更新申請者	27
4.7.3	鍵更新申請の処理手順	27
4.7.4	加入者への新証明書発行通知	27
4.7.5	鍵更新された証明書の受理	27
4.7.6	認証局による鍵更新証明書の公開	27
4.7.7	他のエンティティへの証明書発行通知	27
4.8	証明書変更	28
4.8.1	証明書変更の要件	28
4.8.2	証明書の変更申請者	28
4.8.3	証明書変更の処理手順	28
4.8.4	加入者への新証明書発行通知	28
4.8.5	変更された証明書の受理	28
4.8.6	認証局による変更証明書の公開	28
4.8.7	他のエンティティへの証明書発行通知	28
4.9	証明書の失効と一時停止	28
4.9.1	証明書失効の要件	28
4.9.2	失効申請者	29
4.9.3	失効申請の処理手順	29
4.9.4	失効における猶予期間	30
4.9.5	認証局による失効申請の処理期間	30
4.9.6	検証者の失効情報確認の要件	30
4.9.7	CRL 発行頻度	30
4.9.8	CRL が公開されない最大期間	30
4.9.9	オンラインでの失効／ステータス情報の入手方法	31
4.9.10	オンラインでの失効確認要件	31
4.9.11	その他利用可能な失効情報確認手段	31
4.9.12	鍵の危殆化に関する特別な要件	31
4.9.13	証明書一時停止の要件	31
4.9.14	一時停止申請者	31
4.9.15	一時停止申請の処理手順	31
4.9.16	一時停止期間の制限	31
4.10	証明書ステータスの確認サービス	31
4.10.1	運用上の特徴	31
4.10.2	サービスの利用可能性	31

4.10.3	オプションな仕様	31
4.11	加入の終了	32
4.12	私有鍵預託と鍵回復	32
4.12.1	預託と鍵回復ポリシー及び実施	32
4.12.2	セッションキーのカプセル化と鍵回復のポリシー及び実施	32
5	建物・関連設備、運用のセキュリティ管理	33
5.1	建物及び物理的管理	33
5.1.1	施設の位置と建物構造	33
5.1.2	物理的アクセス	33
5.1.3	電源及び空調設備	33
5.1.4	水害及び地震対策	33
5.1.5	防火設備	34
5.1.6	記録媒体	34
5.1.7	廃棄物の処理	34
5.1.8	施設外のバックアップ	34
5.2	手続的管理	34
5.2.1	信頼すべき役割	34
5.2.2	職務ごとに必要とされる人数	34
5.2.3	個々の役割に対する本人性確認と認証	34
5.2.4	職務分轄が必要になる役割	35
5.3	要員管理	35
5.3.1	資格、経験及び身分証明の要件	35
5.3.2	経歴の調査手続	35
5.3.3	研修要件	35
5.3.4	再研修の頻度及び要件	35
5.3.5	職務のローテーションの頻度及び要件	35
5.3.6	認められていない行動に対する制裁	36
5.3.7	独立した契約者の要件	36
5.3.8	要員へ提供する資料	36
5.4	監査ログの取扱い	36
5.4.1	記録するイベントの種類	36
5.4.2	監査ログを処理する頻度	36
5.4.3	監査ログを保存する期間	36
5.4.4	監査ログの保護	36
5.4.5	監査ログのバックアップ手続	36
5.4.6	監査ログの収集システム（内部対外部）	36

5.4.7	イベントを起こしたサブジェクトへの通知	37
5.4.8	脆弱性評価	37
5.5	記録の保管	37
5.5.1	アーカイブ記録の種類	37
5.5.2	アーカイブを保存する期間	37
5.5.3	アーカイブの保護	37
5.5.4	アーカイブのバックアップ手続	37
5.5.5	記録にタイムスタンプをつける要件	37
5.5.6	アーカイブ収集システム（内部対外部）	37
5.5.7	アーカイブ情報を入手し、検証する手続	38
5.6	鍵の切り替え	38
5.7	危殆化及び災害からの復旧	38
5.7.1	災害及び CA 私有鍵危殆化からの復旧手続き	38
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	38
5.7.3	CA 私有鍵が危殆化した場合の対処	38
5.7.4	災害等発生後の事業継続性	38
5.8	認証局又は登録局の終了	39
6	技術的なセキュリティ管理	40
6.1	鍵ペアの生成と実装	40
6.1.1	鍵ペアの生成	40
6.1.2	加入者への私有鍵の送付	40
6.1.3	認証局への公開鍵の送付	40
6.1.4	検証者への CA 公開鍵の配付	40
6.1.5	鍵のサイズ	40
6.1.6	公開鍵のパラメータ生成及び品質検査	40
6.1.7	鍵の利用目的	41
6.2	私有鍵の保護及び暗号モジュール技術の管理	41
6.2.1	暗号モジュールの標準及び管理	41
6.2.2	私有鍵の複数人によるコントロール	41
6.2.3	私有鍵のエスクロウ	41
6.2.4	私有鍵のバックアップ	41
6.2.5	私有鍵のアーカイブ	41
6.2.6	暗号モジュールへの私有鍵の格納と取り出し	41
6.2.7	暗号モジュールへの私有鍵の格納	42
6.2.8	私有鍵の活性化方法	42
6.2.9	私有鍵の非活性化方法	42

6.2.10	私有鍵の廃棄方法	42
6.2.11	暗号モジュールの評価	42
6.3	鍵ペア管理に関するその他の面	42
6.3.1	公開鍵のアーカイブ	42
6.3.2	公開鍵証明書の有効期間と鍵ペアの使用期間	42
6.4	活性化用データ	43
6.4.1	活性化データの生成とインストール	43
6.4.2	活性化データの保護	43
6.4.3	活性化データのその他の要件	43
6.5	コンピュータのセキュリティ管理	43
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	43
6.5.2	コンピュータセキュリティ評価	44
6.6	ライフサイクルの技術的管理	44
6.6.1	システム開発管理	44
6.6.2	セキュリティ運用管理	44
6.6.3	ライフサイクルのセキュリティ管理	44
6.7	ネットワークのセキュリティ管理	44
6.8	タイムスタンプ	44
7	証明書及び失効リスト及び OCSP のプロファイル	45
7.1	証明書のプロファイル	45
7.1.1	バージョン番号	45
7.1.2	証明書の拡張 (保健医療福祉分野の属性を含む)	45
7.1.3	アルゴリズムオブジェクト識別子	45
7.1.4	名称の形式	45
7.1.5	名称制約	45
7.1.6	CP オブジェクト識別子	46
7.1.7	ポリシー制約拡張	46
7.1.8	ポリシー修飾子の構文及び意味	46
7.1.9	証明書ポリシー拡張フィールドの扱い	46
7.1.10	保健医療福祉分野の属性 (hcRole)	49
7.2	証明書失効リストのプロファイル	54
7.2.1	バージョン番号	54
7.2.2	CRL と CRL エントリ拡張領域	54
7.3	OCSP プロファイル	55
7.3.1	バージョン番号	55
7.3.2	OCSP 拡張領域	55

8	準拠性監査とその他の評価	56
8.1	監査頻度	56
8.2	監査者の身元・資格	56
8.3	監査者と被監査者の関係	56
8.4	監査テーマ	56
8.5	監査指摘事項への対応	56
8.6	監査結果の通知	56
9	その他の業務上及び法務上の事項	57
9.1	料金	57
9.1.1	証明書の発行又は更新料	57
9.1.2	証明書へのアクセス料金	57
9.1.3	失効又はステータス情報へのアクセス料金	57
9.1.4	その他のサービスに対する料金	57
9.1.5	払い戻し指針	57
9.2	財務上の責任	57
9.2.1	保険の適用範囲	57
9.2.2	その他の資産	57
9.2.3	エンドエンティティに対する保険又は保証	57
9.3	業務情報の秘密保護	58
9.3.1	秘密情報の範囲	58
9.3.2	秘密情報の範囲外の情報	58
9.3.3	秘密情報を保護する責任	58
9.4	個人情報のプライバシー保護	58
9.4.1	プライバシーポリシー	58
9.4.2	プライバシーとして保護される情報	58
9.4.3	プライバシーとはみなされない情報	59
9.4.4	個人情報を保護する責任	59
9.4.5	個人情報の使用に関する個人への通知及び同意	59
9.4.6	司法手続又は行政手続に基づく公開	59
9.4.7	その他の情報開示条件	59
9.5	知的財産権	60
9.6	表明保証	60
9.6.1	認証局の表明保証	60
9.6.2	登録局の表明保証	61
9.6.3	加入者の表明保証	61

9.6.4	検証者の表明保証	62
9.6.5	他の関係者の表明保証	62
9.7	無保証	62
9.8	責任制限	63
9.9	補償	63
9.10	本ポリシーの有効期間と終了	64
9.10.1	有効期間	64
9.10.2	終了	64
9.10.3	終了の影響と存続条項	64
9.11	関係者間の個々の通知と連絡	64
9.12	改訂	64
9.12.1	改訂手続き	64
9.12.2	通知方法と期間	65
9.12.3	オブジェクト識別子 (OID) の変更理由	65
9.13	紛争解決手続	65
9.14	準拠法	65
9.15	適用法の遵守	65
9.16	雑則	65
9.16.1	完全合意条項	65
9.16.2	権利譲渡条項	66
9.16.3	分離条項	66
9.16.4	強制執行条項 (弁護士費用及び権利放棄)	66
9.16.5	不可抗力	66
9.17	その他の条項	66

1 はじめに

1.1 概要

証明書ポリシー（Certificate Policy、以下 CP という）は、証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるものである。また、保健医療福祉分野 PKI は、保健医療福祉分野において情報を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、保健医療福祉サービス提供者及び保健医療福祉サービス利用者への署名用公開鍵証明書を発行する「保健医療福祉分野 PKI 認証局」の証明書ポリシーである。

保健医療福祉分野 PKI 認証局が発行した証明書は、個人とその公開鍵及び資格属性等が一意に関連づけられることを証明するものである。認証局が証明書を発行するにあたって、その審査過程、登録、発行及び失効方法は、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。

加入者及び検証者は、保健医療福祉分野 PKI 認証局によって発行された証明書を利用する時は、CP 及び認証局により開示される文書の内容を、その利用方法に照らして評価する必要がある。

本 CP に準拠する個々の「保健医療福祉分野 PKI 認証局」は、本 CP を基準にして、個々の環境に適合した認証実施規程（Certificate Practice Statement、以下 CPS という）を作成するものとする。なお、CPS が本 CP に抵触する場合は CP が優先する。

本 CP は、電子署名及び認証業務に関する法律（以下、電子署名法という）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。従って、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必要がある。

なお、本 CP は以下の文書に依存して構成される。

- ・ IETF/RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
- ・ ISO/TS 17090-1:2002 Health informatics - Public key infrastructure Part 1 : Framework and overview
- ・ ISO/TS 17090-2:2002 Health informatics - Public key infrastructure Part 2 : Certificate profile
- ・ ISO/TS 17090-3:2002 Health informatics - Public key infrastructure Part 3 : Policy management of certification authority

また、本 CP は以下の文章を参照する。なお本 CP ではセキュリティマネジメントに関する部分は JIS X.5080:2002 を参照しているが、セキュリティマネジメント全体を考える場合は ISO 17799 :2005 も参照することが望ましい。

- ・ ISO 17799:2005 Information technology - Code of practice for information security management
- ・ IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
- ・ 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 FIPS140-2(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 文書の名前と識別

本ポリシーの名称を「保健医療福祉分野 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、厚生労働省より「保健医療福祉分野の公開鍵関連分野」のオブジェクト識別子 (OID) を「1.2.392.100495.1」と割り当てる。その基本体系を示す。

OID の基本体系

{ iso(1) member-body(2) jp(392) mhlw(100495) jhpk(1) ca(5) A B C V }

A : 証明書ポリシー cp (1)

B : 認証局の証明書種類 signature(1), authentication(2)

C : セキュリティ保証レベル (n) n=0, 1, 2, 3, 4 (0 はテスト用、3 は HPKI の業務用)

V : 証明書ポリシーのメジャーバージョン番号 v(1)

また、本 CP で定める OID を表 1.2 に示す。

表 1.2 本 CP で定める OID

名称	オブジェクト識別子
HPKI 署名用証明書ポリシー	1.2.392.100495.1.5.1.1.3.1
HPKI 認証用証明書ポリシー (予約)	1.2.392.100495.1.5.1.2.3.1
HPKI 署名テスト用証明書ポリシー	1.2.392.100495.1.5.1.1.0.1
HPKI 認証テスト用証明書ポリシー (予約)	1.2.392.100495.1.5.1.2.0.1

1.3 PKI の関係者

1.3.1 認証局

認証局 (CA) は、証明書発行局 (IA) と登録局 (RA) により構成される。保健医療福祉分野 PKI では、認証局は複数の階層構成をとることができる。また、保健医療福祉分野 PKI の階層構成の頂点の認証局 (Root CA) は、本 CP に準拠する他の保健医療福祉分野 PKI の Root CA と相互認証を行うことがある。

発行局は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

但し、認証局は認証局の運営主体で定める CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部又は全部を外部に委託することができる。

1.3.2 登録局

登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を含む。

但し、登録局は認証局の運営主体で定める CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部を外部に委託することができる。

1.3.3 加入者

加入者とは、証明書所有者である。証明書所有者とは、証明書発行申請を行い認証局により証明書を発行される個人をさす。証明書所有者の範囲は次のとおりとする。

- ・ 保健医療福祉分野サービスの提供者及び利用者
- ・ 上記の提供者の内、以下の者がその有する資格において、あるいは管理者として署名を行う場合は、「その資格を有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。
- ・ 保健医療福祉分野に関わる国家資格を有する者
- ・ 医療機関等の管理者

1.3.4 検証者

検証者とは、加入者の署名を検証する者をさす。

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

本 CP で定める加入者証明書は、次に定める利用目的にのみ使用できる。

- (1) 医療従事者等の保健医療福祉分野サービス提供者の署名検証用
- (2) 患者等の保健医療福祉分野サービス利用者の署名検証用

1.4.2 禁止される証明書の使用

本 CP で定める加入者証明書は、署名検証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 CP の管理組織は、「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以下、「HPKI 認証局専門家会議」という）とする。

1.5.2 問い合わせ先

本 CP に関する問い合わせ先を以下のように定める。

【問い合わせ先】

窓口：厚生労働省 医政局 研究開発振興課 医療機器・情報室

受付時間：10 時～17 時

電話番号：03-3595-2430

FAX 番号：03-3503-0595

e-mail アドレス：hpki-cp@mhlw.go.jp

1.5.3 CPS のポリシ適合性を決定する者

CPS の本 CP への適合性を決定する者は、HPKI 認証局専門家会議とする。

1.5.4 CPS 承認手続き

本 CP は、HPKI 認証局専門家会議によって承認されるものとする。

1.6 定義と略語

(あ～ん)

- ・ アーカイブ (Archive)
電子証明書の発行・失効に関わる記録や、認証局のシステム運用に関わる記録等を保管すること。

- ・ 暗号アルゴリズム (Algorithm)
暗号化／復号には、対になる 2 つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる共通鍵暗号 (秘密鍵暗号) がある。前者には RSA、ElGamal 暗号、楕円曲線暗号などがあり、後者には米国政府標準の DES や近年新しく DES の後継として決まった AES などがある。

- ・ 暗号モジュール (Security Module)
私有鍵や証明書等を安全に保管し、鍵ペア生成や署名等の暗号操作を行うハードウェア又はソフトウェアのモジュール。

- ・ エンドエンティティ (EndEntity)
証明書の発行対象者の総称。公開鍵ペアを所有している実体 (エンティティ) で、公開鍵証明書を利用するもの。(個人、組織、デバイス、アプリケーションなど)
なお、認証局はエンドエンティティには含まれない。

- ・ オブジェクト識別子 (Object Identifier)
オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

- ・ 活性化 (Activate)
鍵を署名などの運用に使用することができる状態にすること。逆に、使用できなくすることを非活性化という。

- ・ 鍵長 (Key Length)
鍵データのサイズ。鍵アルゴリズムに依存する。暗号鍵の強度は一般に鍵の長さによって決まる。鍵長は長ければ長いほど解読困難になるが、署名や暗号メッセージを作成する際の時間もかかるようになる。情報の価値を見計らって適切な鍵長を選