

保健医療福祉分野 PKI 認証局 証明書ポリシー (案)

Version 0.9

平成×年×月

厚生労働省

(C) Ministry of Health, Labour and Welfare

改定履歴

版数	日付	内容
***	平成*年*月	初版発行

－目次－

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.....	3
1.3.5	その他の関係者.....	3
1.4	証明書の使用方法.....	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.....	4
1.6	定義と略語.....	4
2	公開及びリポジトリの責任.....	11
2.1	リポジトリ.....	11
2.2	証明書情報の公開.....	11
2.3	公開の時期又はその頻度.....	11
2.4	リポジトリへのアクセス管理.....	11

3	識別及び認証	12
3.1	名前決定	12
3.1.1	名前の種類	12
3.1.2	名前が意味を持つことの必要性	12
3.1.3	加入者の匿名性又は仮名性	12
3.1.4	種々の名前形式を解釈するための規則	12
3.1.5	名前の一意性	12
3.1.6	認識、認証及び商標の役割	12
3.2	初回の本人性確認	12
3.2.1	私有鍵の所持を証明する方法	12
3.2.2	組織の認証	13
3.2.3	個人の認証	13
3.2.4	確認しない加入者の情報	17
3.2.5	機関の正当性確認	17
3.2.6	相互運用の基準	17
3.3	鍵更新申請時の本人性確認及び認証	17
3.3.1	通常鍵更新時の本人性確認及び認証	17
3.3.2	証明書失効後の鍵更新の本人性確認及び認証	17
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	証明書申請手続き期間.....	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用途.....	26
4.5.1	加入者の私有鍵と証明書の利用用途.....	26
4.5.2	検証者の公開鍵と証明書の利用用途.....	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	オプション的な仕様	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	手続き的管理	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	職務分割が必要になる役割.....	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.....	35
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.....	36
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	鍵の使用目的.....	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	複数人による私有鍵の管理.....	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	私有鍵と公開鍵証明書の有効期間.....	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	48
7.1.4	名前の形式	48
7.1.5	名前制約	48
7.1.6	CPオブジェクト識別子	48
7.1.7	ポリシー制約拡張	48
7.1.8	ポリシー修飾子の構文及び意味	48
7.1.9	証明書ポリシー拡張フィールドの扱い	48
7.2	証明書失効リストのプロファイル	51
7.2.1	バージョン番号	51
7.2.1	CRLとCRLエントリ拡張領域	51
7.3	OCSPプロファイル	52
7.3.1	バージョン番号	52
7.3.2	OCSP拡張領域	52
8	準拠性監査とその他の評価	53
8.1	監査頻度	53
8.2	監査者の身元・資格	53
8.3	監査者と被監査者の関係	53
8.4	監査テーマ	53
8.5	監査指摘事項への対応	53

8.6	監査結果の通知	53
9	その他の業務上及び法務上の事項	54
9.1	料金	54
9.1.1	証明書の発行又は更新料	54
9.1.2	証明書へのアクセス料金	54
9.1.3	失効又はステータス情報へのアクセス料金	54
9.1.4	その他のサービスに対する料金	54
9.1.5	払い戻し指針	54
9.2	財務上の責任	54
9.2.1	保険の適用範囲	54
9.2.2	その他の資産	54
9.2.3	エンドエンティティに対する保険又は保証	54
9.3	企業情報の秘密保護	55
9.3.1	秘密情報の範囲	55
9.3.2	秘密情報の範囲外の情報	55
9.3.3	秘密情報を保護する責任	55
9.4	個人情報のプライバシー保護	56
9.4.1	プライバシープラン	56
9.4.2	プライバシーとして保護される情報	56
9.4.3	プライバシーとはみなされない情報	56
9.4.4	個人情報を保護する責任	56
9.4.5	個人情報の使用に関する個人への通知及び同意	56
9.4.6	司法手続又は行政手続に基づく公開	56
9.4.7	その他の情報開示条件	57

9.5	知的財産権.....	57
9.6	表明保証.....	57
9.6.1	認証局の表明保証.....	57
9.6.2	登録局の表明保証.....	58
9.6.3	加入者の表明保証.....	58
9.6.4	検証者の表明保証.....	59
9.6.5	他の関係者の表明保証.....	60
9.7	無保証.....	60
9.8	責任制限.....	60
9.9	補償.....	61
9.10	本ポリシの有効期間と終了.....	61
9.10.1	有効期間.....	61
9.10.2	終了.....	61
9.10.3	終了の影響と存続条項.....	61
9.11	関係者間の個々の通知と連絡.....	61
9.12	改訂.....	62
9.12.1	改訂手続き.....	62
9.12.2	通知方法と期間.....	62
9.12.3	オブジェクト識別子（OID）の変更理由.....	62
9.13	紛争解決手続.....	62
9.14	準拠法.....	62
9.15	適用法の遵守.....	62
9.16	雑則.....	63
9.16.1	完全合意条項.....	63

9.16.2	権利譲渡条項	63
9.16.3	分離条項.....	63
9.16.4	強制執行条項（弁護士費用及び権利放棄）	63
9.16.5	不可抗力.....	63
9.17	その他の条項.....	64