厚生労働省 HPKI ルート認証局
運用管理規程

Ver 1.52

令和 8 年 8 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 19 年 2 月 13 日	初版発行	
1.1	平成 25 年 9 月 1 日	認証用（人）証明書追加に伴う修正 SHA256 対応に伴う修正	
1.2	令和 2 年 10 月 12 日	1.3.2　登録局 1.3.3　加入者 1.5.2　問合せ先	「政策統括官付　情報政策担当参事官室」から「医政局研究開発振興課医療情報技術推進室」に変更
		2　公開及びリポジトリの責任 4.1.2　申請手続及び責任 4.4.2　認証局による証明書の公開 4.7.6　認証局による鍵更新証明書の公開 9.6.3　加入者の表明保証 9.6.4　検証者の表明保証	公開する情報の変更、及び変更に伴う文言修正
1.3	令和 4 年 10 月 12 日	1.3.2　登録局 1.3.3　加入者 1.5.2　問合せ先	「医政局　研究開発振興課医療情報技術推進室」から「医政局　特定医薬品開発支援・医療情報担当参事官室」に変更
		4.4.2　認証局による証明書の公開 4.7.6　認証局による鍵更新証明書の公開	リポジトリ（厚生労働省ホームページ）にて、サブ CA 証明書が公開されるサブ CA リポジトリのリンクを案内する旨を追記
1.4	令和 5 年 7 月 10 日	SHA1 対応終了に伴う修正	
		7.1　証明書のプロファイル 表 7.1.1　証明書とプロファイル対応表	SHA1 対応の記載の削除

		7.1.3　アルゴリズムオブジェクト識別子	「sha1WithRSAEncryption (1.2.840.113549.1.1.5)」の削除
		表 7.1.2、表 7.1.3、表 7.1.4、表 7.1.5、表 7.1.6、表 7.1.7	記載の削除
		7.2　証明書失効リストのプロファイル 7.2.1　バージョン番号 7.2.2　CRL/ARL と CRL/ARL エントリ拡張領域	SHA1 対応の記載の削除
		表 7.2.1、表 7.2.2、表 7.2.3、表 7.2.4、表 7.2.5、表 7.2.6	記載の削除
1.5	令和 5 年 12 月 20 日	1.5.2　問合せ先	「医政局　特定医薬品開発支援・医療情報担当参事官室」から「医政局　参事官（特定医薬品開発支援・医療情報担当）付医療情報室」に変更
1.51	令和 7 年 5 月 30 日	1.5.2　問合せ先	「医政局　参事官（特定医薬品開発支援・医療情報担当）付医療情報室」から「医政局参事官（医療情報担当）付医療情報室」に変更
1.52	令和 8 年 8 月 18 日	1.1　概要 5.2　手続的管理 5.4　監査ログの取扱い 5.5　記録の保管	依存文書、参考文書を最新版のものに変更
		1.3.1　認証局	他の保健医療福祉分野 PKI の Root CA と相互認証は実施していないかつ実施の想定もないため、それに関する本文を削除
		1.3.4　検証者	誤字の修正
		1.5.2　問合せ先	「問合せ」の表記ゆれを修正

		1.6　定義	鍵更新の定義を追記した。
		1.6　定義	ハッシュ関数の性質としてハッシュ値の生成が困難である衝突発見困難性の性質がある旨を追記
		1.6　定義	DES は脆弱性が指摘されており、NIST からは 2023 年以降は DES の利用を禁止することが提案されているため、DES に係る文章を削除
		1.6　定義	FIPS 140-3 の定義を追記
		1.6　定義	SHA-1 は脆弱性があり既に非推奨となるため、記載を削除し、その代わりに広く利用されている SHA-3 を追記
		2.2　証明書情報の公開 3.1.1　名称の種類 3.2.1　私有鍵の所持を証明する方法 4.7.1　証明書鍵更新の要件 5.1.7　廃棄物の処理 5.2.1　信頼すべき役割 6.7　ネットワークのセキュリティ管理 9.3.3　秘密情報を保護する責任 9.4.4　個人情報を保護する責任 9.6.1　認証局の表明保証	文章の体裁を修正
		3.2.2　組織の認証 4.2.1　本人性及び資格確認 4.7.2　鍵更新申請者 4.9.2　失効申請者 4.9.3　失効申請の処理手	「又は」の表記ゆれを修正

		順	
		1.6　定義と略語	「漏えい」の表記ゆれを修正
		4.1.1　証明書の申請者 4.3.2　証明書発行後の通知 4.4.1　証明書の受理	「平成 18 年度実証実験事業」に関する記述を削除
		4.1.2　申請手続及び責任	参照する章に関する表現を具体化
		4.7.6　認証局による鍵更新証明書の公開	「鍵更新証明書の公開」から「鍵更新された証明書」に変更
		4.7.6　認証局による鍵更新証明書の公開	「4.4.2　認証局による証明書の公開」へ参照する形に修正
		6.2.1　暗号モジュールの標準及び管理 6.2.7　暗号モジュールへの私有鍵の格納 6.2.11　暗号モジュールの評価 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用件	標準規格として、FIPS140-2 と FIP140-3 を併記する形に修正
		7.1.9　証明書ポリシ拡張フィールドの扱い	SHA-256 に修正
		9.6.1　認証局の表明保証	紙だけでなく電子データにも言及する形に修正
		2.2　証明書情報の公開 2.3　公開の時期又はその頻度 3.1.4　種々の名称形式を解釈するための規則 4.1.2 申請手続き及び責任 4.11　加入の終了 5.2.4　職務分轄が必要になる役割	参照する章に関する表記ゆれを修正した。

		5.5.5　記録にタイムスタンプをつける要件 5.5.7　アーカイブ情報を入手し、検証する手続 6.2.8　私有鍵の活性化方法 6.2.9　私有鍵の非活性化方法 6.2.10　私有鍵の廃棄方法 6.3.1　公開鍵のアーカイブ 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 9.3.1　秘密情報の範囲 9.6.1　認証局の表明保証 9.6.2　登録局の表明保証 9.6.4　検証者の表明保証 9.7　無保証 9.8　責任制限 9.16.5　不可抗力	
		1.6 定義と略語 6.4.1　活性化データの生成とインストール 6.4.2　活性化データの保護 9.6.3　加入者の表明保証 9.6.4　検証者の表明保証 9.16.3　分離条項	「規定」の表記を「規程」に修正した。
		9.11　関係者間の個々の通知と連絡	「FAX 番号」についての記載を削除した。
		1.3.2　登録局 1.3.3　加入者 1.5.2　問合せ先	「医政局　参事官（医療情報担当）付医療情報室」を「政策統括官（情報政策担当）付医療情報連携担当参事官室」とし

			た。

－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 3
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　ポリシ管理 4
1.5.1　本ポリシを管理する組織 4
1.5.2　問合せ先 4
1.5.3　CPS のポリシ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 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 14
3.2.5　機関の正当性確認 14
3.2.6　相互運用の基準 14
3.3　鍵更新申請時の本人性確認及び認証 14
3.3.1　通常の鍵更新時の本人性確認及び認証 14
3.3.2　証明書失効後の鍵更新の本人性確認及び認証 14
3.4　失効申請時の本人性確認及び認証 14
4　証明書のライフサイクルに対する運用上の要件 15
4.1　証明書申請 15
4.1.1　証明書の申請者 15
4.1.2　申請手続及び責任 15
4.2　証明書申請手続き 15
4.2.1　本人性及び資格確認 15
4.2.2　証明書申請の承認又は却下 15
4.2.3　証明書申請手続き期間 15
4.3　証明書発行 15
4.3.1　証明書発行時の認証局の機能 15
4.3.2　証明書発行後の通知 16
4.4　証明書の受理 16
4.4.1　証明書の受理 16
4.4.2　認証局による証明書の公開 16
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 16
4.5　鍵ペアと証明書の利用目的 16
4.5.1　加入者の私有鍵と証明書の利用目的 16
4.5.2　検証者の公開鍵と証明書の利用目的 16
4.6　証明書更新 17
4.6.1　証明書更新の要件 17
4.6.2　証明書の更新申請者 17
4.6.3　証明書更新の処理手順 17
4.6.4　加入者への新証明書発行通知 17
4.6.5　更新された証明書の受理 17
4.6.6　認証局による更新証明書の公開 17
4.6.7　他のエンティティへの証明書発行通知 17
4.7　証明書の鍵更新（鍵更新を伴う証明書更新） 17
4.7.1　証明書鍵更新の要件 17

4.7.2　鍵更新申請者 17
4.7.3　鍵更新申請の処理手順 18
4.7.4　加入者への新証明書発行通知 18
4.7.5　鍵更新された証明書の受理 18
4.7.6　認証局による鍵更新された証明書の公開 18
4.7.7　他のエンティティへの証明書発行通知 18
4.8　証明書変更 18
4.8.1　証明書変更の要件 18
4.8.2　証明書の変更申請者 18
4.8.3　証明書変更の処理手順 18
4.8.4　加入者への新証明書発行通知 18
4.8.5　変更された証明書の受理 18
4.8.6　認証局による変更証明書の公開 18
4.8.7　他のエンティティへの証明書発行通知 19
4.9　証明書の失効と一時停止 19
4.9.1　証明書失効の要件 19
4.9.2　失効申請者 19
4.9.3　失効申請の処理手順 20
4.9.4　失効における猶予期間 20
4.9.5　認証局による失効申請の処理期間 20
4.9.6　検証者の失効情報確認の要件 20
4.9.7　CRL/ARL 発行頻度 20
4.9.8　CRL/ARL が公開されない最大期間 21
4.9.9　オンラインでの失効／ステータス情報の入手方法 21
4.9.10　オンラインでの失効確認要件 21
4.9.11　その他利用可能な失効情報確認手段 21
4.9.12　鍵の危殆化に関する特別な要件 21
4.9.13　証明書一時停止の要件 21
4.9.14　一時停止申請者 21
4.9.15　一時停止申請の処理手順 21
4.9.16　一時停止期間の制限 21
4.10　証明書ステータスの確認サービス 21
4.10.1　運用上の特徴 22
4.10.2　サービスの利用可能性 22
4.10.3　オプショナルな仕様 22
4.11　加入の終了 22

4.12　私有鍵預託と鍵回復 22
4.12.1　預託と鍵回復ポリシ及び実施 22
4.12.2　セッションキーのカプセル化と鍵回復のポリシ及び実施 22
5　建物・関連設備、運用のセキュリティ管理 23
5.1　建物及び物理的管理 23
5.1.1　施設の位置と建物構造 23
5.1.2　物理的アクセス 23
5.1.3　電源及び空調設備 24
5.1.4　水害及び地震対策 24
5.1.5　防火設備 24
5.1.6　記録媒体 24
5.1.7　廃棄物の処理 24
5.1.8　施設外のバックアップ 25
5.2　手続的管理 25
5.2.1　信頼すべき役割 25
5.2.2　職務ごとに必要とされる人数 27
5.2.3　個々の役割に対する本人性確認と認証 27
5.2.4　職務分轄が必要になる役割 27
5.3　要員管理 27
5.3.1　資格、経験及び身分証明の要件 27
5.3.2　経歴の調査手続 27
5.3.3　研修要件 28
5.3.4　再研修の頻度及び要件 28
5.3.5　職務のローテーションの頻度及び要件 28
5.3.6　認められていない行動に対する制裁 28
5.3.7　独立した契約者の要件 28
5.3.8　要員へ提供する資料 28
5.4　監査ログの取扱い 28
5.4.1　記録するイベントの種類 28
5.4.2　監査ログを処理する頻度 28
5.4.3　監査ログを保存する期間 28
5.4.4　監査ログの保護 28
5.4.5　監査ログのバックアップ手続 29
5.4.6　監査ログの収集システム（内部対外部） 29
5.4.7　イベントを起こしたサブジェクトへの通知 29
5.4.8　脆弱性評価 29

5.5　記録の保管 29
5.5.1　アーカイブ記録の種類 29
5.5.2　アーカイブを保存する期間 29
5.5.3　アーカイブの保護 29
5.5.4　アーカイブのバックアップ手続 29
5.5.5　記録にタイムスタンプをつける要件 30
5.5.6　アーカイブ収集システム（内部対外部） 30
5.5.7　アーカイブ情報を入手し、検証する手続 30
5.6　鍵の切り替え 30
5.7　危殆化及び災害からの復旧 30
5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き 30
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 30
5.7.3　CA 私有鍵が危殆化した場合の対処 31
5.7.4　災害等発生後の事業継続性 31
5.8　認証局又は登録局の終了 31
6　技術的なセキュリティ管理 32
6.1　鍵ペアの生成と実装 32
6.1.1　鍵ペアの生成 32
6.1.2　加入者への私有鍵の送付 32
6.1.3　認証局への公開鍵の送付 32
6.1.4　検証者への CA 公開鍵の配付 32
6.1.5　鍵のサイズ 32
6.1.6　公開鍵のパラメータ生成及び品質検査 32
6.1.7　鍵の利用目的 32
6.2　私有鍵の保護及び暗号モジュール技術の管理 32
6.2.1　暗号モジュールの標準及び管理 32
6.2.2　私有鍵の複数人による管理 33
6.2.3　私有鍵のエスクロウ 33
6.2.4　私有鍵のバックアップ 33
6.2.5　私有鍵のアーカイブ 33
6.2.6　暗号モジュールへの私有鍵の格納と取り出し 33
6.2.7　暗号モジュールへの私有鍵の格納 33
6.2.8　私有鍵の活性化方法 33
6.2.9　私有鍵の非活性化方法 33
6.2.10　私有鍵の廃棄方法 34
6.2.11　暗号モジュールの評価 34

6.3　鍵ペア管理に関するその他の面 34
6.3.1　公開鍵のアーカイブ 34
6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間 34
6.4　活性化用データ 34
6.4.1　活性化データの生成とインストール 34
6.4.2　活性化データの保護 34
6.4.3　活性化データのその他の要件 35
6.5　コンピュータのセキュリティ管理 35
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 35
6.5.2　コンピュータセキュリティ評価 35
6.6　ライフサイクルの技術的管理 35
6.6.1　システム開発管理 35
6.6.2　セキュリティ運用管理 35
6.6.3　ライフサイクルのセキュリティ管理 35
6.7　ネットワークのセキュリティ管理 36
6.8　タイムスタンプ 36
7　証明書及び失効リスト及び OCSP のプロファイル 37
7.1　証明書のプロファイル 37
7.1.1　バージョン番号 37
7.1.2　証明書の拡張 37
7.1.3　アルゴリズムオブジェクト識別子 37
7.1.4　名称の形式 37
7.1.5　名称制約 37
7.1.6　CP オブジェクト識別子 38
7.1.7　ポリシ制約拡張 38
7.1.8　ポリシ修飾子の構文及び意味 38
7.1.9　証明書ポリシ拡張フィールドの扱い 38
7.2　証明書失効リストのプロファイル 48
7.2.1　バージョン番号 48
7.2.2　CRL/ARL と CRL/ARL エントリ拡張領域 48
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 54
9.3.1　秘密情報の範囲 54
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 55
9.4.1　プライバシープラン 55
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 57
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 59
9.7　無保証 59
9.8　責任制限 60

9.9　補償 60
9.10　本ポリシの有効期間と終了 60
9.10.1　有効期間 60
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 61
9.12.1　改訂手続き 61
9.12.2　通知方法と期間 61
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 62
9.16.1　完全合意条項 62
9.16.2　権利譲渡条項 62
9.16.3　分離条項 62
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 63

1　はじめに

1.1　概要

厚生労働省 HPKI ルート認証局運用管理規程（以下、「CP/CPS」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 CP/CPS は、保健医療福祉サービス提供者への署名用下位認証局証明書（以下、「署名用サブ CA 証明書」）と認証用（人）下位認証局証明書（以下、「認証用（人）サブ CA 証明書」）を発行する「厚生労働省 HPKI ルート認証局（以下、「ルート CA」という。）」の証明書ポリシである。

加入者及び検証者は、ルート CA によって発行された証明書を利用する時は、本 CP/CPS 及びその他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。

なお、本 CP/CPS 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 17090-1:2021 Health informatics − Public key infrastructure Part 1: Overview of digital certificate services
- ISO 17090-2:2015 Health informatics − Public key infrastructure Part 2: Certificate profile
- ISO 17090-3:2021 Health informatics − Public key infrastructure Part 3: Policy management of certification authority

また、本 CP/CPS は以下の文章を参照する。

- IETF/RFC 9810 - Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)
- IETF/RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- IETF/RFC 5280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List(CRL) Profile
- US FIPS140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules
- US FIPS140-3(Federal Information Processing Standard) : Security

Requirements for Cryptographic Modules

- JIS Q 27002:2024：情報技術－情報セキュリティ技術－情報マネジメントの実践のための規範
- 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、最終改正：令和 7 年 6 月 1 日法律第 68 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、最終改正：令和 7 年 6 月 30 日デジタル庁・法務省令第 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、最終改正：令和 7 年 6 月 30 日総務省・法務省・経済産業省告示第 4 号）

1.2　文書の名前と識別

本ポリシの名称を「厚生労働省 HPKI ルート認証局　証明書ポリシ」とする。本ポリシ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) jhpki(1) ca(5) A B C V }

A：証明書ポリシ　cp（1）

B：認証局の証明書種類　signature(1)，　authentication for individual(2)
　　authentication for organization (3)

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：証明書ポリシのメジャーバージョン番号　v(1)

また、本 CP/CPS で定める OID を表 1.2 に示す。

表 1.2　本 CP/CPS 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	1.2.392.100495.1.5.1.1.3.1
HPKI認証用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.3.1
HPKI認証用（組織）証明書ポリシ	1.2.392.100495.1.5.1.3.3.1
HPKI署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1

HPKI認証テスト用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.0.1
HPKI 認証テスト用（組織）証明証ポリシ	1.2.392.100495.1.5.1.3.0.1

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。

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、本認証局は本 CP/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

本認証局では、厚生労働省　政策統括官（情報政策担当）付医療情報連携担当参事官室が登録局の役割を担うこととする。

登録局は、適切な申請者の組織確認の業務を行い、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、登録局は本 CP/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、厚生労働省　政策統括官（情報政策担当）付医療情報連携担当参事官室からサブ CA の運用業務の実施を承認された組織であり、署名用サブ CA 証明書、認証用（人）サブ CA 証明書の証明書所有者である（以下、「署名用サブ CA 証明書と認証用（人）サブ CA 証明書の全てを意味する場合はサブ CA 証明書」と呼ぶ。）。サブ CA 証明書所有者の範囲は次のとおりとする。

・ サブ CA の運用業務の実施を承認された組織

1.3.4 検証者

検証者とは、デジタル署名を公開鍵証明書の公開鍵で検証する者をさす。

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/CPS で定めるサブ CA 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電子証明書の署名検証用

（2）　患者等の保健医療福祉分野サービス利用者の電子証明書の署名検証用

（3）　証明書失効リストの署名検証用

1.4.2　禁止される証明書の使用

本 CP/CPS で定めるサブ CA 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/CPS の管理組織は、本認証局の HPKI 認証局専門家会議とする。

1.5.2　問合せ先

本 CP/CPS に関する問合せ先を以下のように定める。

【問合せ先】

窓口：厚生労働省　政策統括官（情報政策担当）付医療情報連携担当参事官室

（以下、「厚生労働省」と呼ぶ。）

受付時間：10 時～17 時（平日）

電話番号：03-6812-7837

1.5.3　CPS のポリシ適合性を決定する者

本 CP/CPS 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/CPS 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 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。

・ 鍵更新（Key Update）
認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。 本 CP では、有効期間内に実施される鍵ペアの置換を「鍵更新」と定義し、有効期間を過ぎた後に行われる鍵ペアの生成は「鍵更新」ではなく、新規の鍵発行として扱う。

・ 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択する必要がある。

・ 鍵の預託（Key Escrow）
第三者機関に鍵を預託すること。

・ 鍵ペア（Key Pair）

私有鍵とそれに対応する公開鍵の対。

・ 加入者（Subscriber）
認証局から電子証明書を発行され、電子証明書内に記載された公開鍵に対応する私有鍵を用いて署名操作を行う者。

・ 加入者証明書
認証局から加入者に対して発行された公開鍵証明書のこと。

・ 危殆化（Compromise）
私有鍵等の秘密情報が盗難、紛失、漏えい等によって、その秘密性を失うこと。

・ 公開鍵（Public Key）
私有鍵と対になる鍵で、デジタル署名の検証に用いる。

・ 公開鍵証明書（Public Key Certificate）
加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の加入者情報、公開鍵、CA の情報、その他証明書の利用規則等が記載され、CA の署名が付される。

・ 自己署名証明書（Self Signed Certificate）
認証局が自身のために発行する電子証明書。発行者名と加入者名が同じである。

・ 失効（Revocation）
有効期間内に、何らかの理由（盗難・紛失など）により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には CA の判断で失効されることもある。

・ 私有鍵（Private Key）
公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の所有者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。

・ 使用期間（Usage Period）
生成した鍵ペアを使用することができる期間を指す。

・ 証明書失効リスト（Certificate Revocation List、Authority Revocation List）
失効した電子証明書のリスト。
エンドエンティティの証明書の失効リストを CRL といい、CA の証明書の失効リストを ARL という。

・ 証明書発行要求（Certificate Signing Request）
申請者から認証局に電子証明書発行を求めるための要求。電子証明書を作成するための元となる情報で、その内容には、申請者の所在地、サーバアドレス、公開鍵などの情報が含まれる。

・ 証明書ポリシ（Certificate Policy：CP）
共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規程の集合。

・ 申請者
認証局に電子証明書の発行を申請する主体のこと。

・ 電子署名（Electronic Signature）
電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。

・ 登録局（Registration Authority：RA）
電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。登録局は、認証局の機能のうち、一部の業務を行う。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。

・ 認証局（Certification Authority：CA）
電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

・ 認証実施規程（Certification Practice Statement：CPS）
証明書ポリシに基づいた認証局運用についての規程集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

・ 登録設備室
認証業務用設備のうち、登録業務用設備のみが設置された室をいう。登録業務用設備とは、加入者の登録用端末や、加入者が初めて証明書をダウンロードする際に１度限り使用されるＩＤ、パスワード等を識別する為に用いる設備をいう。

・ 認証設備室
認証業務用設備（電子証明書の作成又は管理に用いる電子計算機その他の設備）が設置された室をいう。ただし、登録業務用設備のみが設置される場合を除く。

・ 発行局（Issuer Authority）
電子証明書の作成・発行を主として発行業務を行う機関。発行局は、認証局の機能のうち、一部の業務を行う。

・ ハッシュ関数（Hash Function）
任意の長さのデータから固定長のランダムな値を生成する計算方法。生成した値は「ハッシュ値」と呼ばれる。ハッシュ値は、ハッシュ値から元のデータを逆算できない一方向性と、異なる 2 つのデータから同一のハッシュ値の生成が困難である衝突発見困難性という性質を持つ。この性質からデータを送受信する際に、送信側の生成したハッシュ値と受信側でデータのハッシュ値を求めて両者を比較し両者が一致すれば、データが通信途中で改ざんされていないことが確認できる。

・ プロファイル（Profile）
電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたもの。

・ 有効期間（Validity Period）
証明書や CRL 等が有効とみなされる期間であり、有効期間開始日から有効期間満了日までの範囲を指す。

・ リポジトリ（Repository）
電子証明書及び証明書失効リスト、その他公開文書を公開するシステム。

・ リンク証明書
CA 鍵を更新する際に、新しい自己署名証明書（NewWithNew）と古い世代の CA 鍵と新しい世代の CA 鍵を紐付けるために発行される電子証明書。リンク証明書によって、世代の異なる CA から電子証明書を発行された加入者間での証明書検証が

可能となる。
リンク証明書には、新しい公開鍵に古い私有鍵で署名した証明書（NewWithOld）と、古い公開鍵に新しい私有鍵で署名した証明書（OldWithNew）がある。

・ ルート CA（Root CA）
階層型の認証構造において、階層の最上位に位置する認証局のこと。下位に属する認証局の公開鍵証明書の発行、失効を管理する。

（A～Z）

・ ARL （Authority Revocation List）
認証局の証明書の失効リスト。本 CP/CPS ではルート認証局証明書の失効リストを指す。証明書失効リストについては「証明書失効リスト」の定義を参照のこと。

・ CA（Certification Authority）
認証局を参照のこと。

・ CA 証明書
認証局に対して発行された電子証明書。

・ CP（Certificate Policy）
証明書ポリシを参照のこと。

・ CPS（Certification Practice Statement）
認証実施規程を参照のこと。

・ CRL（Certificate Revocation List）
エンドエンティティの証明書の失効リスト・本 CP/CPS ではサブ CA 証明書の失効リストを指す。証明書失効リストについては「証明書失効リスト」の定義を参照のこと。

・ CRL 検証
証明書失効情報が、認証局が発行する CRL に記載されているかを確認すること。

・ CSR（Certificate Signing Request）
証明書発行要求を参照のこと。

・ DN（Distinguished Name）
X.500 規格において定められた識別名。X.500 規格で識別子を決定することによって、加入者の一意性を保障する。

・ FIPS 140-2（Federal Information Processing Standard）
FIPS とは米国連邦情報処理標準で、FIPS140-2 は暗号モジュールが満たすべきセキュリティ要件を規定したもの。各セキュリティ要件に対して 4 段階のセキュリティレベル（最低レベル 1～最高レベル 4）を定めている。

・ FIPS 140-3（Federal Information Processing Standard）
FIPS140-3 は暗号モジュールが満たすべきセキュリティ要件を規定したもの。ISO/IEC 19790:2012 に基づいており、国際標準との整合性等が強化されている。各セキュリティ要件に対して 4 段階のセキュリティレベル（最低レベル 1～最高レベル 4）が定義され、レベルが上がるほど物理的・論理的な保護が強化される。

・ IA（Issuer Authority）
発行局を参照のこと。

・ OID（Object ID）
オブジェクト識別子を参照のこと。

・ PKI（Public Key Infrastructure）
公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。

・ RA（Registration Authority）
登録局を参照のこと。

・ RSA
公開鍵暗号方式の一つ。Rivest、Shamir、Adleman の 3 名によって開発され、その名前をとって名付けられた。巨大な整数の素因数分解の困難さを利用したもので、公開鍵暗号の標準として普及している。

・ SHA（Secure Hash Algorithm）
ハッシュ関数の一群。SHA-2 や SHA-3 等があり、任意の長さのデータから 256bit や 384bit 等一定の長さのハッシュ値を作成する。

- X.500
  ITU-T/ISO が定めたディレクトリサービスに関する国際基準。

- X.509
  ITU-T/ISO が定めた電子証明書及び証明書失効リストに関する国際標準。X.509v3 では、電子証明書に拡張領域を設けて、電子証明書の発行者が独自の情報を追加することができる。

2　公開及びリポジトリの責任

2.1　リポジトリ

リポジトリはルート CA の証明書と失効情報及びサブ CA の失効情報、その他、保健医療福祉分野 PKI に関する情報を保持する。

2.2　証明書情報の公開

本認証局は検証者又は加入者へ次に示す事項を公開する。検証者又は加入者は公開された情報を認証局から入手することができる。

＜検証者に公開する事項＞

- ルート CA の公開鍵証明書
- 本 CP/CPS
- CRL/ARL
- 検証者の表明保証に関する事項（「9.6.4　検証者の表明保証」に規定する）

＜加入者に公開する事項＞

- 本 CP/CPS
- 加入者の表明保証に関する事項（「9.6.3　加入者の表明保証」に規定する）

2.3　公開の時期又はその頻度

認証局は、認証局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、「4.9　証明書の失効と一時停止」に従うものとする。

2.4　リポジトリへのアクセス管理

本 CP/CPS、ルート CA 証明書、及び CRL/ARL などの公開情報は、加入者及び検証者に対しては読み取り専用として公開する。

3　識別及び認証

3.1　名称決定

3.1.1　名称の種類

本 CP/CPS に基づいて発行されるサブ CA 証明書に使用されるサブジェクト名は加入者名とする。

ルート CA 証明書及びサブ CA 証明書の加入者名は X.500 の Distinguished Name を使用する。保健医療福祉分野 PKI では、証明書の設定項目において C（国名）を JP とする。ルート CA 証明書には organizationalUnit は必須で、厚生労働省の組織名（ローマ字表記）を記載する。またサブ CA 証明書には CommonName は必須で、加入者の組織名（ローマ字表記）を含む文字列を記載する。

3.1.2　名称が意味を持つことの必要性

本 CP/CPS により発行する証明書の相対識別名は、検証者によって理解され、使用されるよう意味のあるものとする。

3.1.3　加入者の匿名性又は仮名性

規定しない。

3.1.4　種々の名称形式を解釈するための規則

名称を解釈するための規則は、「7　証明書及び失効リスト及び OCSP のプロファイル」に従う。

3.1.5　名称の一意性

本認証局が発行するサブ CA 証明書の加入者名（subjectDN）は、保健医療福祉分野 PKI 内で、特定の認証局を一意に指し示すものとする。

3.1.6　認識、認証及び商標の役割

規定しない。

3.2　初回の本人性確認

3.2.1　私有鍵の所持を証明する方法

申請者が生成した鍵ペアの公開鍵を提示して認証局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、認証局からのチャレンジ（認証局が

生成するランダムなデータやトークンで、申請者がこれに署名することで私有鍵の所有を証明する仕組み）に署名を行い、私有鍵の所有を証明するものとする。あるいは申請者が提出した証明書発行要求（CSR）の署名検証等により、私有鍵の所有を確認するものとする。

3.2.2　組織の認証

サブ CA 証明書を発行する組織は、厚生労働省からサブ CA の運用業務の実施を承認された組織のみとし、その承認行為、又は委任行為により組織の認証を行うこととする。

3.2.3　個人の認証

規定しない。

3.2.4　確認しない加入者の情報

認めない。

3.2.5　機関の正当性確認

規定しない。

3.2.6　相互運用の基準

規定しない。

3.3　鍵更新申請時の本人性確認及び認証

3.3.1　通常の鍵更新時の本人性確認及び認証

サブ CA 証明書を発行する組織は、厚生労働省からサブ CA の運用業務の実施を承認されるか委任された組織のみであるため、鍵更新時の確認は行わない。

3.3.2　証明書失効後の鍵更新の本人性確認及び認証

証明書発行と同様の手順とする。

3.4　失効申請時の本人性確認及び認証

加入者が認証局に失効申請を行うときには、次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. 証明書を失効する理由を明らかにする。

4　証明書のライフサイクルに対する運用上の要件

4.1　証明書申請

4.1.1　証明書の申請者

1. サブ CA 証明書

サブ CA 証明書の申請者は、厚生労働省からサブ CA の運用業務の実施を認められた保健医療福祉分野サービスの提供者とする。

4.1.2　申請手続及び責任

厚生労働省からサブ CA の運用業務を認められた組織は、所定の手続きに基づき、認証局の定める書類及び証明書発行要求（CSR）を提出することによりサブ CA 証明書の利用申請を行う。

また、サブ CA の運用業務を認められた組織は、申請にあたり、「1.3 PKI の適用範囲」と「9　その他の業務上及び法務上の事項」で規定される認証局の責任範囲及び加入者の表明保証の内容を理解し、それらに同意した上で利用申請を行うものとする。

4.2　証明書申請手続き

4.2.1　本人性及び資格確認

サブ CA 証明書の申請者は、厚生労働省からサブ CA の運用業務を承認、又は委任された組織であるため本人性及び資格確認は実施しない。

4.2.2　証明書申請の承認又は却下

規定しない。

4.2.3　証明書申請手続き期間

規定しない。

4.3　証明書発行

4.3.1　証明書発行時の認証局の機能

本認証局は、サブ CA 証明書の申請者から提出された証明書発行要求（CSR）に対し、本認証局の署名を付してサブ CA 証明書を発行する。発行したサブ CA 証明書は、本認証局が定める格納媒体に格納し、所定の手続きに基づき申請者以外の第 3 者に渡らない

よう安全に交付する。

4.3.2　証明書発行後の通知

認証局は、サブ CA 運用業務実施組織に、サブ CA 証明書と発行通知書を交付することによりサブ CA 証明書を発行したことを通知したものとみなす。

4.4　証明書の受理

4.4.1　証明書の受理

認証局は、サブ CA 証明書を交付した後、サブ CA 運用業務実施組織がサブ CA 証明書を受領した旨を、受領書の受領により確認する。

サブ CA 運用業務実施組織は、交付されたサブ CA 証明書の記載内容を確認のうえ疑義又は問題点がある場合は、本認証局から発送後 30 日以内に、本認証局に対してその旨を報告しなければならない。

なお、認証局は、証明書を交付してから 30 日以内に受領書の受領が確認できない場合、サブ CA 証明書を失効させる。

4.4.2　認証局による証明書の公開

認証局は、サブ CA 証明書をリポジトリ（厚生労働省ホームページ）にて公開しない。但し、リポジトリにて、サブ CA 証明書が公開されるサブ CA リポジトリのリンクを案内する。その目的はサブ CA 証明書をサブ CA のリポジトリとルート CA のリポジトリの二箇所にて公開することにより利用者の混乱を招くことをさける為である。

4.4.3　他のエンティティに対する認証局による証明書発行通知

規定しない。

4.5　鍵ペアと証明書の利用目的

4.5.1　加入者の私有鍵と証明書の利用目的

加入者は、サブ CA 私有鍵を「1.4.1　適切な証明書の使用」における用途にのみ利用する。

4.5.2　検証者の公開鍵と証明書の利用目的

検証者は、署名検証の用途で公開鍵と証明書を利用する。

4.6　証明書更新

4.6.1　証明書更新の要件

本CP/CPSに則り認証局から発行される証明書は､鍵更新を伴う更新のみを許可する。従って、鍵の更新を伴わない証明書更新は行わない。

4.6.2　証明書の更新申請者

規定しない。

4.6.3　証明書更新の処理手順

規定しない。

4.6.4　加入者への新証明書発行通知

規定しない。

4.6.5　更新された証明書の受理

規定しない。

4.6.6　認証局による更新証明書の公開

規定しない。

4.6.7　他のエンティティへの証明書発行通知

規定しない。

4.7　証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1　証明書鍵更新の要件

認証局は、以下の条件を満たす時に証明書の更新申請を受け付ける。なお、更新可能期間は認証局が定める証明書の有効期間の開始日から終了日までとする。

- 更新対象証明書が存在すること。
- 証明書が有効期間内のものであること。
- 証明書が失効されていないこと。
- 有効期間内で、認証局で定める期間に申請があったこと。

4.7.2　鍵更新申請者

鍵更新申請者は、厚生労働省からサブ CA の運用業務を承認、又は委任された組織とする。

4.7.3　鍵更新申請の処理手順

「4.2.1 本人性及び資格確認」に定める本人性確認並びに資格確認を行う。

4.7.4　加入者への新証明書発行通知

認証局は、「4.3.2 証明書発行後の通知」に定める発行通知を行う。

4.7.5　鍵更新された証明書の受理

認証局は、「4.4.1 証明書の受理」に定める方法により、加入者の証明書の受理を確認する。

4.7.6　認証局による鍵更新された証明書の公開

「4.4.2　認証局による証明書の公開」に定めるものとする。

4.7.7　他のエンティティへの証明書発行通知

規定しない。

4.8　証明書変更

4.8.1　証明書変更の要件

本 CP/CPS に則り認証局から発行されるサブ CA 証明書は、証明書変更を行わない。

4.8.2　証明書の変更申請者

規定しない。

4.8.3　証明書変更の処理手順

規定しない。

4.8.4　加入者への新証明書発行通知

規定しない。

4.8.5　変更された証明書の受理

規定しない。

4.8.6　認証局による変更証明書の公開

規定しない。

4.8.7　他のエンティティへの証明書発行通知

規定しない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

認証局は、次の場合に証明書を失効するものとする。

＜加入者による失効申請の場合＞

次の各項に該当する場合、加入者は失効申請を行わなくてはならない。

- サブ CA 私有鍵の危殆化が認識されたか、その疑いがある場合。
- サブ CA 証明書に含まれる該当の情報が正確でなくなった場合。
- サブ CA 証明書の使用を中止する場合。

加入者からの失効申請と確認された場合は、理由の如何に関わらず証明書を失効させなくてはならない。

＜認証局による失効申請の場合＞

次の各項に該当する場合、証明書を失効させる。

- 加入者が、本 CP/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。
- サブ CA 私有鍵の危殆化が認識されたか、その疑いがある場合。
- サブ CA 証明書に含まれる該当の情報が正確でなくなった場合。(例えば、組織名の変更があった場合等。
- 本 CP/CPS に従ってサブ CA 証明書が適切に発行されなかったと認証局が判断した場合
- サブ CA 証明書交付後、30 日を過ぎても加入者から受領書が返送されなかった場合。

4.9.2　失効申請者

認証局は、厚生労働省からサブ CA の運用業務を承認、又は委任された組織からのみ失効申請を受け付ける。

4.9.3　失効申請の処理手順

認証局は、失効申請の受領の判断を行い受理する場合は「3.4 失効申請時の本人性確認と認証」に従って、以下の手順を実施した上で証明書の失効を行う。

＜加入者からの失効申請の場合＞

厚生労働省からサブ CA の運用業務を承認、又は委任された組織は、所定の手続きに基づき、認証局の定める書類を提出することによりサブ CA 証明書の失効申請を行う。本認証局は、失効を要求している申請者が、失効される証明書に記されている加入者であることを確認する。確認にあたっては、最低限、認証局で保存してある「4.1.2 申請手続及び責任」で提出された申請者の各種書類を参照する。

上記の確認と共に、証明書の失効理由を確認し、その真偽についても確認を実施しなくてはならない。

この手順により証明書の失効を実施した場合は、CRL を発行する。また、証明書の失効の事実を認証局の定める方法により申請者に通知する。

＜認証局による失効申請の場合＞

認証局は「4.9.1 証明書失効の要件」の中の認証局からの失効申請の場合は、速やかに当該証明書を特定し、失効の事由の真偽の確認を実施する。また、失効事由が真実であった場合は速やかに証明書を失効させる。

証明書の失効を実施した場合は、CRL を発行する。また、証明書の失効の事実を認証局の定める方法により申請者に通知する。

4.9.4　失効における猶予期間

「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行うものとする。

4.9.5　認証局による失効申請の処理期間

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。

4.9.6　検証者の失効情報確認の要件

検証者は、サブ CA 証明書の公開鍵を使う時に有効な CRL/ARL を使用して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。

4.9.7　CRL/ARL 発行頻度

本認証局は、CRL/ARL の発行頻度を決定し、決定した頻度に従い CRL/ARL の更新を行う。

1. CRL/ARL の有効期間を 96 時間とし、48 時間ごとに更新する。
2. サブ CA 証明書の失効を行った場合は、CRL/ARL を更新する。
3. ルート CA 私有鍵が危殆化し、又はその恐れがある場合は、直ちに発行した全ての証明書を失効させ、CRL/ARL を発行する。

4.9.8 CRL/ARL が公開されない最大期間

CRL/ARL は発行後 24 時間以内に公開される。

4.9.9 オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10 オンラインでの失効確認要件

規定しない。

4.9.11 その他利用可能な失効情報確認手段

使用しない。

4.9.12 鍵の危殆化に関する特別な要件

認証局は、ルート CA 私有鍵の危殆化の際には関連組織に直ちに通知するものとする。

4.9.13 証明書一時停止の要件

一時停止は行わない。

4.9.14 一時停止申請者

一時停止は行わない。

4.9.15 一時停止申請の処理手順

一時停止は行わない。

4.9.16 一時停止期間の制限

一時停止は行わない。

4.10 証明書ステータスの確認サービス

4.10.1　運用上の特徴

規定しない。

4.10.2　サービスの利用可能性

規定しない。

4.10.3　オプショナルな仕様

規定しない。

4.11　加入の終了

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

4.12　私有鍵預託と鍵回復

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場合を除き、預託されないものとする。また、署名目的の私有鍵の回復も行わない。

4.12.1　預託と鍵回復ポリシ及び実施

規定しない。

4.12.2　セッションキーのカプセル化と鍵回復のポリシ及び実施

規定しない。

5　建物・関連設備、運用のセキュリティ管理

これらは、JIS Q 27002:2024 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、次の項目をカバーする。

5.1　建物及び物理的管理

5.1.1　施設の位置と建物構造

本認証業務のための設備を維持・運用するための場所である認証設備室については、下記のセキュリティを確保する。

1. 認証設備室は、外部からの侵入が容易にできないようセキュリティが確保された建物の内部に、物理的な仕切りに囲まれた区画（「サイト」ともいう。）の施設とし、物理的な階層構造の中に設置する。
2. 認証設備室については、独自のセキュリティ基準を設けることにより、認証業務用設備が物理的に安全な環境において運用する。
3. 認証設備室及び認証設備室が設置された建物等には、その施設に認証業務用設備があることを示す掲示及びパンフレット等への記載を一切行わない。

5.1.2　物理的アクセス

認証設備室への入退室においては、下記のセキュリティを確保する。

1. 認証設備室への入室においては、入室を許可されない者の不正侵入を防止するため、入室を許可された運営要員の生体をあらかじめ生体認証装置に登録し、生体が登録された 2 人の運営要員の生体認証が行なわれることにより、入室を可能とするとともに、生体認証装置により入退室の記録が行われる。
2. 認証設備室への入室においては、入室操作の時間と入室操作の試行回数をチェックすることにより、許可されない者が室内に不正侵入できないようにする。また、そのチェックにより検知した異常については、24 時間監視を行っている監視室へ警告する。入室権限者が認証設備室へ入室する場合については、認証業務責任者が日常の入退室チェックと作業ごとの入退室記録の確認を行う。日常の入退室チェックの方法は、アラームが発生した場合に、直接現場に行き入退室のチェックを行う方法による。
3. 認証設備室からの退室においては、入室した運営要員の人数と退室する運営要員の人数が同じであることをチェックすることにより、入室した運営要員が室内に無用に残留できないようにする。
4. 認証設備室が無人（運営要員が完全に退室）状態においては、モーションセンサーにより、室内の状況を常時監視し、何らかの動きを検知できるようにする。

5. 認証設備室の入室及び退室並びに認証設備室内での作業については、監視カメラにより、運営要員の活動を記録する。
6. 認証業務用設備の補修工事等に際し、入室権限を有する運営要員以外の者が認証設備室へ入室しなければならない場合は、認証業務責任者の事前の許可を得て、入室権限を有する作業監督者 2 人が同行し監督することにより、認証設備室への入室ができるものとする。非入室権限者の認証設備室への入退室時には、非入室権限者が確実に入退室したことを認証業務責任者が対面にて確認を行う。

5.1.3 電源及び空調設備

認証業務用設備については、商用電源が断たれた場合に認証システムの異常停止又はサービスの中断を防止するために、設置された無停電源装置（UPS：Uninterruptible Power Supply）及び自家発電装置からの給電を行う。また、認証設備室は、専用の空調システムにより温度及び湿度の制御を行う。

5.1.4 水害及び地震対策

認証設備室は、建物の 2 階以上に設置され、洪水・津波等の水害から守り、漏水対策も施す。また、耐震対策を講じた建物に設置するとともに、認証設備室に設置される機器については、地震による移動及び転倒等を防止する措置を講じる。

5.1.5 防火設備

認証設備室は、建築基準法に適合した耐火建物の中に設置する。また、認証設備室は、建築基準法に適合した防火区画に設置し、自動火災報知器及び消火設備を設置する。

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、耐火キャビネット又は耐火金庫等の施錠された安全な保管場所で管理する。

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、情報の漏えいがないよう、下記の方法で行う。

1. 紙等に記録された情報
   - 文書等については、シュレッダー等により、記載された内容を確認できないよう処理する。
2. 補助記録媒体等に記録されたデータ
   - 磁気テープ、運用で用いる IC カード等については、無効データの上書き等を行なった上で完全消去する等により、記録されたデータを確認できないよう

処理する。また、補助記録媒体の物理的な破壊により、記録されたデータを復元できないよう処理する。

3. コンピュータ機器等に記録されたデータ

・ コンピュータディスク、暗号化装置等については、完全な初期化を行うことにより、記録されたデータを確認できないよう処理する。また、本認証局のルート CA 私有鍵のバックアップが格納された記録媒体については、物理的な破壊により、記録されたデータを復元できないよう処理する。

5.1.8 施設外のバックアップ

本認証局は、施設外へのバックアップは行わない。

5.2 手続的管理

手続的管理は、JIS Q 27002:2024 と同等以上の規格に従うものとする。

5.2.1 信頼すべき役割

本認証業務に携わる運営要員とその業務は、表 5-1 に示す。

表 5-1 本認証局の運営要員の役割

運営要員の区分	業　　務
厚生労働省 HPKI ルート認証局責任者（以下「認証局責任者」という。）	・認証局運営方針の決定及び運営方針変更の決定 ・本認証局の監査指摘事項への対応指示 ・認証業務責任者に対するルート CA 証明書の発行、更新、廃棄の指示 ・認証業務責任者の任命、解任 ・生成されたルート CA 私有鍵のバックアップの保管 ・ルート CA 私有鍵のバックアップ及びバックアップからのリストア ・ルート CA 私有鍵の初期化及びバックアップ媒体の破壊 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応の統括 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応と関連組織への報告
受付審査担当者	・サブ CA 証明書の利用申請、失効申請及び更新申請に係る審査 ・認証局へのサブ CA 証明書の発行、失効及び更新要求 ・生成されたルート CA 私有鍵のバックアップの保管 ・ルート CA 私有鍵のバックアップ及びバックアップからのリストア ・ルート CA 私有鍵の初期化及びバックアップ媒体の破壊 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊

運営要員の区分	業　　務
	急時における対応
認証業務責任者	・上級 IA 操作員、一般 IA 操作員及びシステム保守員の任命・解任 ・上級 IA 操作員、一般 IA 操作員及びシステム保守員への作業指示 ・上級 IA 操作員との合議制操作によるルート CA 私有鍵の生成 ・生成されたルート CA 私有鍵のバックアップの保管 ・ルート CA 私有鍵のバックアップ及びバックアップからのリストア ・ルート CA 私有鍵の初期化及びバックアップ媒体の破壊 ・ルート CA 私有鍵の廃棄 ・上級 IA 操作員及び一般 IA 操作員に対するルート CA 証明書、サブ CA 証明書及び PKI 運用関係者証明書の発行、更新及び失効指示 ・上級 IA 操作員及びシステム保守員に対する CA 証明書及びフィンガープリントのリポジトリ登録指示 ・認証設備室の維持管理、認証設備室のセキュリティ監査イベント（アーカイブ）の採取及び検査 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における作業指示
上級 IA 操作員	・認証業務責任者との合議制操作によるルート CA 私有鍵の生成 ・ルート CA 私有鍵のアクティベーション及び非アクティベーション ・CA システムの起動及び停止 ・ルート CA 私有鍵の初期化及びバックアップ媒体の破壊 ・ルート CA 私有鍵のバックアップ及びバックアップからのリストア ・CA システムのバックアップ ・CA 証明書、サブ CA 証明書及び PKI 運用関係者証明書の発行処理、更新処理及び失効処理 ・CRL/ARL の生成及び送付 ・CA システムのセキュリティ監査イベント（アーカイブ）の採取 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応
一般 IA 操作員	・ルート CA 私有鍵のアクティベーション及び非アクティベーション ・CA システムの起動及び停止 ・ルート CA 証明書、サブ CA 証明書及び PKI 運用関係者証明書の発行処理、更新処理及び失効処理 ・CRL/ARL の生成及び送付 ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応

運営要員の区分	業　　務
システム保守員	・CA システムのハードウェア・OS 等のセットアップ ・リポジトリのバックアップ ・ルート CA 証明書及びフィンガープリントのリポジトリへの登録 ・リポジトリメンテナンス（コンテンツ更新等） ・ルート CA 私有鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応

5.2.2　職務ごとに必要とされる人数

本認証業務に携わる運営要員の最低限必要な人数は、各運営要員 1 人とする。

5.2.3　個々の役割に対する本人性確認と認証

CA システムへアクセスし、ルート CA 私有鍵の操作やサブ CA 証明書発行、失効に係わる操作等の重要操作を行う権限者は、認証局責任者により任命される。

また、CA システムへのアクセスには、IC カードに格納された PKI 運用関係者証明書を使用した本人しか持ち得ない私有鍵を用いた強固な認証を行う。

5.2.4　職務分轄が必要になる役割

ルート CA 私有鍵について、「表 5-1 本認証局の運営要員の役割」に示す運営要員が実施する重要操作においては、適切な複数人による管理を採用する。

5.3　要員管理

信頼される役割を担う者は、認証局の業務に関して、操作や管理の責務を負う。認証局の運営においては、これら役割の信頼性、適合性及び合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1　資格、経験及び身分証明の要件

認証局の業務運営に関して信頼される役割を担う者は、認証局運営組織の採用基準に基づき採用された職員とする。CA システムを直接操作する担当者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解しているものを配置する。

5.3.2　経歴の調査手続

信頼される役割を担う者の信頼性と適格性を、認証局運営組織の規則の要求に従って、任命時及び定期的に検証すること。

5.3.3　研修要件

信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受けなければならない。

5.3.4　再研修の頻度及び要件

規定しない。

5.3.5　職務のローテーションの頻度及び要件

規定しない。

5.3.6　認められていない行動に対する制裁

規定しない。

5.3.7　独立した契約者の要件

規定しない。

5.3.8　要員へ提供する資料

規定しない。

5.4　監査ログの取扱い

セキュリティ監査手続きは、JIS Q 27002:2024と同等以上の規格に従うものとする。

5.4.1　記録するイベントの種類

認証局は、CA システム、リポジトリシステム、認証局に関するネットワークアクセスの監査証跡やイベント・ログを手動或いは自動で取得出来る。

5.4.2　監査ログを処理する頻度

認証局は、監査ログを 3 ヶ月に 1 度以上定期的に検査する。

5.4.3　監査ログを保存する期間

監査ログは、最低 10 年間保存される。

5.4.4　監査ログの保護

認証局は、認可された人員のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、権限を持たない者の閲覧や、改ざん、不正な削除から

保護する。

5.4.5　監査ログのバックアップ手続

監査ログは、月１回の頻度でバックアップを取り記録媒体に保存する。

5.4.6　監査ログの収集システム（内部対外部）

規定しない。

5.4.7　イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8　脆弱性評価

規定しない。

5.5　記録の保管

記録は、JIS Q 27002:2024と同等以上の規格に従って保管されるものとする。

5.5.1　アーカイブ記録の種類

認証局 は、以下の情報をアーカイブする。

- 本認証局から発行する証明書の発行/失効に関する処理履歴
- CRL/ARL の発行に関する処理履歴
- ルート CA 証明書
- サブ CA 証明書
- サブ CA 証明書の発行、更新及び失効申請に関わる書類

5.5.2　アーカイブを保存する期間

アーカイブする情報は、記録が作成されてから最低 10 年間は保存する。

5.5.3　アーカイブの保護

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可された者しかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。

5.5.4　アーカイブのバックアップ手続

アーカイブは、月次でバックアップを行い記録媒体に保存する。

5.5.5　記録にタイムスタンプをつける要件

「5.5.1　アーカイブ記録の種類」で規定する情報の記録時間は、処理を行った日付を記録する。

5.5.6　アーカイブ収集システム（内部対外部）

アーカイブの収集機能は、本認証局の CA システム及びリポジトリの機能とし、業務及びセキュリティに関する重要な事象をアーカイブとして収集する。

5.5.7　アーカイブ情報を入手し、検証する手続

「5.5.1　アーカイブ記録の種類」で規定する情報については、「5.5.3　アーカイブの保護」で規定する方法により、可用性と完全性が確保された形で安全に保管される。

5.6　鍵の切り替え

認証局は、15 年に一度ルート CA 私有鍵の更新を行う。ルート CA 私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成される。

ルート CA 私有鍵の更新と共にルート CA 証明書の更新も実施される。この更新においてもルート CA 私有鍵生成の場合と同様に、複数人の立会いのもと執り行われる。

サブ CA 証明書については、加入者からの更新依頼がある場合、サブ CA 私有鍵の有効期間に応じて 5 年から 10 年に一度更新を行う。

5.7　危殆化及び災害からの復旧

5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き

認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局員全員に適切な教育・訓練を実施する。

- ルート CA 私有鍵の危殆化
- 火災、地震、事故等の自然災害
- システム（ハードウェア、ネットワーク等）の故障

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

ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時の際には、可能な限り速やか

に、加入者、検証者にリポジトリにより通知する。

5.7.3　CA 私有鍵が危殆化した場合の対処

ルート CA 私有鍵が危殆化又その恐れが生じた場合は、認証局責任者の判断により、速やかに認証業務を停止するとともに、認証局で規定された手続きに基づき、全てのサブ CA 証明書の失効を行い、CRL/ARL を開示し、ルート CA 私有鍵を廃棄する。更に、原因の追求と再発防止策を講じる。

5.7.4　災害等発生後の事業継続性

災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、認証局で規定された手続きに基づき、加入者及び検証者に情報を公開する。

5.8　認証局又は登録局の終了

1. 本認証サービスの廃止日までに有効期間の残っている全てのサブ CA 証明書を失効し、その失効リストはリポジトリに 5 年間公開する。
2. 本認証サービスを廃止する場合、廃止日の 90 日前までに加入者に書面で通知するとともに、リポジトリに廃止理由を公開する。
3. 廃止時には、ルート CA 私有鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。

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

CA 鍵ペアは、認証設備室内に設置された専用の暗号モジュール（HSM）を用いて、複数人の立会いのもと、権限を持った者による操作により生成される。

6.1.2　加入者への私有鍵の送付

サブ CA 証明書の私有鍵は、加入者にて生成するため、認証局から加入者へ私有鍵の送付は行わない。

6.1.3　認証局への公開鍵の送付

サブ CA 証明書は、本認証局で生成するため、加入者から本認証局へ配送されない。

6.1.4　検証者への CA 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、本認証局のリポジトリにて公開するものとする。

6.1.5　鍵のサイズ

本認証局で生成する鍵のサイズは、下記のとおりとする。

1. 本認証局の鍵のサイズは、RSA アルゴリズムの 2048 ビット
2. サブ CA の鍵のサイズは、RSA アルゴリズムの 2048 ビット

6.1.6　公開鍵のパラメータ生成及び品質検査

公開鍵パラメータは、信頼できる暗号モジュールによって生成される。公開鍵パラメータの品質検査も暗号モジュールにより行うものとする。

6.1.7　鍵の利用目的

ルート CA 証明書及びサブ CA 証明書の鍵は、keyCertSign と cRLSign のビットを使用する。

6.2　私有鍵の保護及び暗号モジュール技術の管理

6.2.1　暗号モジュールの標準及び管理

ルート CA 私有鍵の格納モジュールは、US FIPS 140-2 レベル 3 又は US FIPS 140-

3 レベル 3 と同等以上のものを使用する。ただし、2026 年 9 月 22 日以降に新たに導入する格納モジュールは、US FIPS 140-3 レベル 3 と同等以上のものを使用する。

6.2.2 私有鍵の複数人による管理

本認証局のルート CA 私有鍵の生成及び管理は、本認証局の鍵の管理を担う複数人の運営要員よって行われ、かつ、そのうちの 1 名だけではできない方法によって認証設備室にて行う。

6.2.3 私有鍵のエスクロウ

ルート CA 私有鍵は、法律によって必要とされる場合を除き、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

本認証局のルート CA 私有鍵は、本認証局の鍵の管理を担う複数人の運営要員よって行われ、かつ、そのうちの 1 名だけではできない方法によって認証設備室内でバックアップされ、複数に分割されたバックアップ用の鍵として保管する。バックアップ用の鍵の個々については、一つずつ権限を有する者以外が触れることができないアクセス制御などの措置がされ、耐火等の防災措置がとられた異なる場所に施錠して保管する。

6.2.5 私有鍵のアーカイブ

認証局はサブ CA 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と取り出し

本認証局のルート CA 私有鍵をバックアップ用の鍵からリストア(復元)する場合は、本認証局の鍵の管理を担う複数の運営要員によって認証設備室にて行う。

6.2.7 暗号モジュールへの私有鍵の格納

ルート CA 私有鍵は、FIPS 140-2 レベル 3 又は FIPS 140-3 レベル 3 相当の暗号化装置によって生成し、暗号化して暗号化装置内に保存する。

6.2.8 私有鍵の活性化方法

ルート CA 私有鍵の活性化の方法は、認証局室内において「6.2.2 私有鍵の複数人による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.9 私有鍵の非活性化方法

ルート CA 私有鍵の非活性化の方法は、認証局室内において「6.2.2 私有鍵の複数人

による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.10　私有鍵の廃棄方法

ルート CA 私有鍵を破棄しなければならない状況の場合、認証局室内で「6.2.2　私有鍵の複数人による管理」と同じく、複数名の権限を有する者によって、私有鍵の格納された HSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。

6.2.11　暗号モジュールの評価

ルート CA 私有鍵の格納モジュールは、FIPS 140-2 レベル 3 又は FIPS 140-3 レベル 3 と同等以上のものを使用する。ただし、2026 年 9 月 22 日以降に新たに導入する格納モジュールは、US FIPS 140-3 レベル 3 と同等以上のものを使用する。

6.3　鍵ペア管理に関するその他の面

6.3.1　公開鍵のアーカイブ

「5.5.2　アーカイブを保存する期間」及び「5.5.3　アーカイブの保護」で規定するとおり行う。

6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間

公開鍵証明書の有効期間と鍵ペアの使用期間については、表 6-1 に示す。

表 6-1 公開鍵証明書の有効期間と鍵ペアの使用期間

	公開鍵証明書有効期間	鍵ペア使用期間
本認証局	30 年	15 年
サブ CA	20 年以下	10 年以下

6.4　活性化用データ

6.4.1　活性化データの生成とインストール

認証局において用いられるルート CA 私有鍵の活性化データは一意で予測不能なものとし、その生成とインストールは別途定める規程に従い実施する。

6.4.2　活性化データの保護

認証局において用いられるルート CA 私有鍵の活性化データは、別途定める規程に従い安全に保護される。

6.4.3　活性化データのその他の要件

規定しない。

6.5　コンピュータのセキュリティ管理

6.5.1　特定のコンピュータのセキュリティに関する技術的要件

認証業務用設備は、ファイアウォールを介して外部ネットワークと接続し、不正アクセスを検知・防止する。本認証業務で用いる暗号化装置は、FIPS140-2 レベル 3 又は FIPS 140-3 レベル 3 相当の暗号化装置を用いる。

CA システムへのログイン時には、「5.2.3　個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。

6.5.2　コンピュータセキュリティ評価

本認証局で使用する製品については、セキュリティに関する情報等を定期的に収集し、最新のセキュリティ技術の最新動向を踏まえて、使用する製品が設けたセキュリティに関する基準を満たすよう維持管理する。

6.6　ライフサイクルの技術的管理

認証局 のハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、随時本 CP/CPS の見直し及びセキュリティチェックを行う。

6.6.1　システム開発管理

本認証局のシステムは、適切な品質管理が行われた信頼できる組織で開発されたものを使用する。

本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持する。

本認証局のシステムに係る機器、OS 及びアプリケーションを更新する場合は、更新前に試験等を行い、互換性を確保する。

6.6.2　セキュリティ運用管理

本認証局のシステムについては、別に定めるセキュリティに関する規程(以下「セキュリティ規程」という。)の定めに従い、適切な運用を行う。

6.6.3　ライフサイクルのセキュリティ管理

規定しない。

6.7　ネットワークのセキュリティ管理

本認証局のネットワークについては、セキュリティ規程の定めに従い、適切な運用を行う。また、定期的な評価を実施し、ネットワーク運用がセキュリティ規程を満たすよう、下記の措置を行い、維持する。

1. 認証業務用設備を構成するネットワーク及びリポジトリを構成するネットワークに対する不正アクセスを検知し、防止するためのファイアウォール及び不正侵入検知システムによる制御及び監視
2. 証業務用設備を構成するネットワーク上の通信データの漏えい及び盗聴防止のための暗号化

6.8　タイムスタンプ

本認証局は、正確な時刻源を取得し、NTP（Network Time Protocol）を使用し認証業務用設備の時刻同期を行う。

7　証明書及び失効リスト及び OCSP のプロファイル

7.1　証明書のプロファイル

本認証局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。

本 CP/CPS に従い発行される証明書は以下表 7.1.1 の通りとする。

表 7.1.1　証明書とプロファイル対応表

証明書種別	基本領域 プロファイル	拡張領域 プロファイル
SHA-256 対応ルート CA 証明書	表 7.1.8	表 7.1.9
SHA-256 対応署名用サブ CA 証明書	表 7.1.10	表 7.1.11
SHA-256 対応認証用（人）サブ CA 証明書	表 7.1.12	表 7.1.13

7.1.1　バージョン番号

本認証局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ることとする。

7.1.2　証明書の拡張

本認証局が発行する証明書の拡張領域のプロファイルは表 7.1.1 の拡張領域プロファイルの通りとする。

7.1.3　アルゴリズムオブジェクト識別子

基本領域の Signature アルゴリズムは以下の通りとする。

sha256WithRSAEncryption (1.2.840.113549.1.1.11)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとする。

RSAEncryption (1.2.840.113549.1.1.1)

7.1.4　名称の形式

Issure と Subject の名前の形式は表 7.1.8、表 7.1.10、表 7.1.12 に示される。

7.1.5　名称制約

用いない。

7.1.6　CP オブジェクト識別子

別途規定する。

7.1.7　ポリシ制約拡張

使用しない。

7.1.8　ポリシ修飾子の構文及び意味

本 CP/CPS を参照する URL を含める。

7.1.9　証明書ポリシ拡張フィールドの扱い

本 CP/CPS の OID を格納する。

表 7.1.2、表 7.1.3、表 7.1.4、表 7.1.5、表 7.1.6、表 7.1.7　SHA1 対応終了に伴い削除

表 7.1.8　SHA-256 対応厚生労働省 HPKI ルート認証局証明書プロファイル

（基本領域）

項目	設定	説明
Version	○	Ver3 とする。
SerialNumber	○	同一認証局が発行する証明書内でユニークな値とする。
Signature	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 30 年（UTCTime で設定する。）
Issuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.9）参照

表中の、「○」設定する、「×」は設定しないことを表す。

表 7.1.9　SHA-256 対応厚生労働省 HPKI ルート認証局証明書プロファイル

（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	この証明書の公開鍵の SHA-256 ハッシュ値	
authorityCertIssuer	○		
directoryName		c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
authorityCertSerial	○	この証明書の証明書シリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-256 ハッシュ値	FALSE
KeyUsage	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	×		-
policyMapping	×		-
subjectAltName	○		-
CountryName	○	JP	
OrganizationName	○	厚生労働省	
OrganizationUnitName	○	政策統括官	
OrganizationUnitName	○	厚生労働省ＨＰＫＩルート認証局Ｖ２	
issuerAltName	×		FALSE
subjectDirectoryAttributes	×		FALSE
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
directoryName	○	c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2 cn=RARL	
uniformResource Identifier	○	http://hpki.mhlw.go.jp/repository/rlist/rarl2.crl	

subjectInfoAccess	×		FALSE
authorityInfoAccess	×		FALSE

表中の、「○」は設定する、「×」は設定しないことを表す。

表 7.1.10　SHA-256 対応署名用サブ認証局証明書プロファイル

（基本領域）

項目	設定	説明
Version	○	Ver3 とする。
SerialNumber	○	同一認証局が発行する証明書内でユニークな値とする。
Signature	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 20 年以下（UTCTime で設定する。）
Issuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	下位認証局の組織名
OrganizationUnitName	○	下位認証局の下位組織名
CommonName	○	HPKI-01-※-forNonRepudiation ※認証局を唯一に識別できる文字列を設定する。
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.11）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.11　SHA-256 対応署名用サブ認証局証明書プロファイル

（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-256 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-256 ハッシュ値	FALSE
KeyUsage	○	KeyCertSign ｜ CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.1.3.1	
policyQualifiers	○		
cPSuri	○	http://hpki.mhlw.go.jp/repository/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2 cn=SARL	

			uniformResource Identifier	○	http://hpki.mhlw.go.jp/repository/rlist/sarl2.crl	
subjectInfoAccess				×		-
authorityInfoAccess				△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.12　SHA-256 対応認証用（人）サブ認証局証明書プロファイル

（基本領域）

項目	設定	説明
Version	○	Ver3 とする。
SerialNumber	○	同一認証局が発行する証明書内でユニークな値とする。
Signature	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 20 年以下（UTCTime で設定する。）
Issuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	下位認証局の組織名
OrganizationUnitName	○	下位認証局の下位組織名
CommonName	○	HPKI-01-※-forAuthentication-forIndividual ※認証局を唯一に識別できる文字列を設定する。
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.13）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.13　SHA-256 対応認証用（人）サブ認証局証明書プロファイル

（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-256 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-256 ハッシュ値	FALSE
KeyUsage	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.2.3.1	
policyQualifiers	○		
cPSuri	○	http://hpki.mhlw.go.jp/repository/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	

				cn=SARL	
			uniformResource Identifier	○	http://hpki.mhlw.go.jp/repository/rlist/sarl2.crl
subjectInfoAccess				×		-
authorityInfoAccess				△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

7.2　証明書失効リストのプロファイル

7.2.1　バージョン番号

認証局が発行する CRL/ARL 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。

SHA-256 対応 CRL の基本領域のプロファイルを表 7.2.7 に、ARL の基本領域のプロファイルを表 7.2.10 に示す。

7.2.2　CRL/ARL と CRL/ARL エントリ拡張領域

SHA-256 対応 CRL エントリの拡張領域のプロファイルは、以下の表 7.2.8 の通りとする。CRL 拡張領域のプロファイルは、以下の表 7.2.9 の通りとする。

SHA-256 対応 ARL エントリの拡張領域のプロファイルは、以下の表 7.2.11 の通りとする。ARL 拡張領域のプロファイルは、以下の表 7.2.12 の通りとする。

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.2.1、表 7.2.2、表 7.2.3、表 7.2.4、表 7.2.5、表 7.2.6　SHA1 対応終了に伴い削除

表 7.2.7　SHA-256 対応証明書失効リストのプロファイル（CRL 基本領域）

フィールド	設定	説明
Version	○	Ver2 とする。
Signature	○	表 7.1.10 の Signature と同様とする。
Issuer	○	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
ThisUpdata	○	CRL 発行日時（UTCTime で設定する。）
NextUpdate	○	thisUpdate + 96 時間（UTCTime で設定する。）
RevokedCertificates	○	
UserCertificate	○	失効した証明書の serialNumber を記載。
RevocationDate	○	失効日時を記載する。
CrlEntryExtensions	○	拡張領域（表 7.2.8）参照
CrlExtentions	○	拡張領域（表 7.2.9）参照

表 7.2.8　SHA-256 対応証明書失効リストのプロファイル
（CRL エントリ拡張領 crlEntryExtentions）

フィールド	設定	説明	Critical
ReasonCode	○		FALSE
HoldInstructionCode	×		-
InvalidityDate	×		-
CertificateIssure	×		-

表 7.2.9　SHA-256 対応証明書失効リストのプロファイル
（CRL 拡張領域 crlExtentions）

フィールド	設定	説明	Critical
AuthorityKeyIdentifier	○		FALSE
keyIdentifier	○	認証局証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName		c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
authorityCertSerial	○	認証局証明書の証明書シリアル番号	
IssuerAltName	×		-
CRLNumber	○	128bit 以下の正の整数	FALSE
DeltaCRLIndicator	×		-
IssueingDistributionPoint	○		TRUE
distributionPoint	○		
fullName	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName		c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2 cn=SARL	

	onlyContainsCACerts	○		TRUE
FreshesCRL		×		-

表 7.2.10　SHA-256 対応認証局失効リストのプロファイル（ARL 基本領域）

フィールド	設定	説明
Version	○	Ver2 とする。
Signature	○	表 7.1.10 の Signature と同様とする。
Issuer	○	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
ThisUpdata	○	ARL 発行日時（UTCTime で設定する。）
NextUpdate	○	thisUpdate + 96 時間（UTCTime で設定する。）
RevokedCertificates	○	
UserCertificate	○	失効した証明書の serialNumber を記載。
RevocationDate	○	失効日時を記載する。
CrlEntryExtensions	○	拡張領域（表 7.2.11）参照
CrlExtentions	○	拡張領域（表 7.2.12）参照

表 7.2.11　SHA-256 対応認証局失効リストのプロファイル
（ARL エントリ拡張領 crlEntryExtentions）

フィールド	設定	説明	Critical
ReasonCode	○		FALSE
HoldInstructionCode	×		-
InvalidityDate	×		-
CertificateIssure	×		-

表 7.2.12　SHA-256 対応認証局失効リストのプロファイル

（ARL 拡張領域 crlExtentions）

フィールド	設定	説明	Critical
AuthorityKeyIdentifier	○		FALSE
keyIdentifier	○	認証局証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName		c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
authorityCertSerial	○	認証局証明書の証明書シリアル番号	
IssuerAltName	×		-
CRLNumber	○	128bit 以下の正の整数	FALSE
DeltaCRLIndicator	×		-
IssueingDistributionPoint	○		TRUE
distributionPoint	○		
fullName	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName		c=JP o= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2 cn=RARL	
onlyContainsCACerts	○		TRUE
FreshesCRL	×		-

7.3　OCSP プロファイル

7.3.1　バージョン番号

規定しない。

7.3.2　OCSP 拡張領域

規定しない。

8　準拠性監査とその他の評価

8.1　監査頻度

厚生労働省ルート認証局の準拠性監査は、認証局構築時に厚生労働省によって行われる納入検査において、その準拠性の検査が完了するため、その後の準拠性監査は実施しない。但し、その準拠性を維持するために、これとは別途、年 1 回の間隔で、認証局にて内部監査を実施する。

8.2　監査者の身元・資格

認証局は、認証局業務を直接行っている運営要員以外の者から選出した監査者により、内部監査を実施するものとする。

8.3　監査者と被監査者の関係

監査者は、本認証局の運営要員以外の者から選出し、被監査者から独立しているものとする。監査者は、被監査者と特別な利害関係を持たないものとする。

8.4　監査テーマ

監査は、本 CP/CPS の準拠性をカバーする。

8.5　監査指摘事項への対応

認証局は、認証局責任者の指示のもと、監査における指摘事項に対する改善措置を実施する。

8.6　監査結果の通知

監査者によって証明書の信頼性に影響する重大な欠陥が発見された認証局又は登録局は、加入者、検証者及び HPKI 認証局専門家会議に直ちに通知するものとする。

9　その他の業務上及び法務上の事項

9.1　料金

規定しない。

9.1.1　証明書の発行又は更新料

規定しない。

9.1.2　証明書へのアクセス料金

規定しない。

9.1.3　失効又はステータス情報へのアクセス料金

規定しない。

9.1.4　その他のサービスに対する料金

規定しない。

9.1.5　払い戻し指針

規定しない。

9.2　財務上の責任

規定しない。

9.2.1　保険の適用範囲

規定しない。

9.2.2　その他の資産

規定しない。

9.2.3　エンドエンティティに対する保険又は保証

規定しない。

9.3　企業情報の秘密保護

9.3.1　秘密情報の範囲

本認証局が保持する加入者の情報は、証明書、CRL/ARL、各認証局が定める CPS の一部として明示的に公表されたものを除き、秘密保持対象として扱われる。本認証局は、法の定めによる場合及び加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しない。

本認証局は、かかる法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続き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、秘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。

また組織の合併等に関連してアドバイスする弁護士、会計士、金融機関及びその他の専門家に対しても、本認証局は秘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。

サブ CA 私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、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、秘密保持対象情報である。認証局は、「8.6 監査結果の報告」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、これらの情報を外部へ開示しない。

9.3.2 秘密情報の範囲外の情報

本認証局が発行する証明書及び CRL/ARL に含まれている情報は秘密情報として扱わない。

その他、次の情報も秘密情報として扱わない。

- 本認証局以外の出所から、秘密保持の制限無しに公知となった情報
- 開示に関して加入者によって承認されている情報

9.3.3 秘密情報を保護する責任

本認証局は「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏えいに係わる脅威に対して合理的な保護対策を実施する責任を負う。

ただし、本認証局が保持する秘密情報を、法の定めによる場合及び加入者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得た者は契約あるいは法的な制約によりその情報を第三者に開示することはできない。にもかかわらず、そのような情報が漏えいした場合、その責は漏えいした者が負う。

9.4 個人情報のプライバシー保護

9.4.1 プライバシープラン

厚生労働省 HPKI ルート認証局において提供するサービスの円滑な運営に必要な範囲で、本認証局の加入者の情報を収集する場合がある。収集した情報は利用目的の範囲内で適切に取り扱う。本認証局では、加入者の情報を本認証局が提供する認証業務のサービスを円滑に運営するために、加入者の組織確認、及び電子証明書の送付先として利用する。

また、本認証局では、収集した情報について、法令に基づく開示請求があった場合、その他特別な理由のある場合を除き、利用目的以外の目的のために自ら利用、又は第三者に提供しない。更に、本認証局は、収集した情報の漏えい、滅失又はき損の防止その他収集した情報の適切な管理のために必要な措置を講じる。

9.4.2 プライバシーとして保護される情報

認証局は、次の情報を保護すべき個人情報として取り扱う。

- 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。
  例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- CRL/ARL に含まれない加入者の証明書失効又は停止の理由に関する情報。
- その他、認証局が業務遂行上知り得た加入者の個人情報。

9.4.3 プライバシーとはみなされない情報

次の情報は、秘密情報として扱わない。

- 公開鍵証明書
- CRL/ARL に記載された情報

9.4.4 個人情報を保護する責任

認証局は「9.4.2 プライバシーとして保護される情報」で規定された情報を保護するため、内部及び外部からの情報漏えいに係わる脅威に対して合理的な保護対策を実施する責任を負う。

9.4.5 個人情報の使用に関する個人への通知及び同意

認証局は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6　司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、認証局は情報を開示することができる。

9.4.7　その他の情報開示条件

規定しない。

9.5　知的財産権

認証局と加入者との間で別段の合意がなされない限り、認証局が提供する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。

- サブ CA 証明書：認証局に帰属する財産である
- サブ CA 証明書の私有鍵：私有鍵は、その保存方法又は保存媒体の所有者に関わらず、公開鍵と対になる私有鍵を所有する加入者に帰属する財産である
- サブ CA 証明書の公開鍵：保存方法又は保存媒体の所有者に関わらず、対になる私有鍵を所有する加入者に帰属する財産である
- 本認証局より公開された CRL/ARL：認証局に帰属する財産である
- 本 CP/CPS：認証局に帰属する財産（著作権を含む）である

9.6　表明保証

9.6.1　認証局の表明保証

認証局は、その運営にあたり、本 CP/CPS に基づいて、加入者及び検証者に対して次の認証局としての責任を果たすものとする。

- 提供するサービスと運用のすべてが、本 CP/CPS の要件に従って行われること。
- 証明書の発行時に、申請者の申請内容の真偽の確認を確実に行うこと。
- 認証局が証明書を発行する時は、証明書に記載されている情報が本 CP/CPS に従って検証されたことを保証すること。
- 公開鍵を含む証明書を加入者に確実に届けること。
- 認証局で定める失効ポリシに従って失効事由が生じた場合は、証明書を確実に失効すること。
- CRL/ARL などの重要事項を認証局の定める方法により、速やかに入手できるようにすること。

- 認証局の定める方法で、本 CP/CPS に基づく加入者の権利と義務を各加入者に通知すること。
- 鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取り消し、及び紛争解決をするための手続きを加入者に通知すること。
- 「5　建物及び関連施設、運用のセキュリティ」及び「6　技術的セキュリティ管理」に従い認証局を運営し、私有鍵の危殆化を生じさせないこと。
- ルート CA 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こと。
- 申請者から提出された証明書発行等に関わる各種の書類及び電子データの滅失、改ざんを防止し、10 年間保管すること。
- 認証局の発行する証明書の中で、加入者に対して、加入者の名称（subjectDN）の一意性を検証可能にしておくこと。

9.6.2　登録局の表明保証

登録局は、認証局から独立して登録局を運営する場合、加入者、検証者、認証局に対して次の責任を果たすものとする。また、登録局は、認証局に代わって果たす行為について個別に責任を負う。

- 認証局の発行する証明書の中で、加入者に対して加入者の名称（subjectDN）の一意性を検証可能にしておくこと。
- 証明書申請情報を認証局に安全に送付し、登録記録を安全に保管すること。
- 証明書失効申請を行う場合は、「4.9.3　失効申請の処理手順」に従って失効申請を開始すること。
- 将来の検証のため、また証明書がどのように、何故生成されたかを管理可能なように、証明書の作成要求又は失効要求などのイベントを、認証局に移管した場合を除き、証明書の有効期間満了後 10 年間保管すること。

9.6.3　加入者の表明保証

加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任

   証明書発行申請を行う場合、認証局に提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。
2. 証明書記載事項の担保責任

   証明書の記載内容について証明書の受領時に確認を行い、申請内容と相違ないかを確認すること。また、記載内容について現状との乖離が発生した場合には、

速やかに当該証明書の失効手続きを行うこと。

3. 鍵などの管理責任

　私有鍵を保護し、紛失、暴露、改ざん、又は盗用されることを防止するために妥当な措置を取ること。

4. 各種の届出に対する責任

　私有鍵の紛失､暴露､その他の危殆化､又はそれらが疑われる時には､本 CP/CPS に従って速やかに届け出ること。

　また、証明書情報に変更があった場合は、本 CP/CPS に従って速やかに届け出ること。

5. 利用規程の遵守責任

　加入者は、本 CP/CPS 及び本項を読み、その利用規程及び禁止規程を遵守すること。

9.6.4　検証者の表明保証

検証者は以下の責任を果たすものとする。

1. 利用規程の遵守責任

　検証者は、本 CP/CPS 及び本項を読み、その利用規程及び禁止規程を遵守すること。また、証明書の利用に際しては信頼点の管理を確実に行うこと。

2. 証明書記載事項の確認責任

　検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。

- 証明書の署名が正しいこと
- 証明書の有効期間内であること
- 証明書が失効していないこと
- 証明書の記載事項が､「7　証明書及び失効リスト及び OCSP のプロファイル」に記述されているプロファイルと合致していること。特に、次の 2 点の検証を実施することは HPKI 署名用証明書として重要である。
  - OID 及び Issuer の CN が本 CP/CPS に一致していること
  - KeyUsage には KeyCertSign と CRLSign のみが立てられていること

9.6.5　他の関係者の表明保証

規定しない。

9.7　無保証

認証局は、「9.6.1　認証局表明保証」及び「9.6.2　登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

また、「9.16.5　不可抗力」で規定される不可抗力によるサービス停止によって加入者、若しくはその他の第三者において損害が生じた場合、認証局は一切の責任を負わない。

9.8　責任制限

認証局は、加入者において電子証明書の利用又は私有鍵の管理その他加入者が注意すべき事項の運用が不適切であったために生じた損害に対して責任を負わない。

また、認証局及び登録局の責任は、認証局及び登録局の怠慢行為により本 CP/CPS に定められた運用を行わなかった場合に限定する。

なお、「9.6　表明保証」に関し、次の場合、認証局は責任を負わない。

- 認証局に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- 加入者又は検証者が自己の義務の履行を怠ったために生じた損害
- 加入者又は検証者のシステムに起因して発生した一切の損害
- 加入者又は検証者が使用する端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 認証局の責に帰することのできない事由で電子証明書及び CRL/ARL に公開された情報に起因する損害
- 認証局の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する業務又は取引上の債務等、一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害

9.9　補償

規定しない。

9.10　本ポリシの有効期間と終了

9.10.1　有効期間

本 CP/CPS は、作成された後、「HPKI 認証局専門家会議」により審査、承認されるこ

とにより有効になる。また、「9.10.2 終了」で記述する本 CP/CPS の終了まで有効であるものとする。

9.10.2 終了

本 CP/CPS は、「9.10.3 終了の影響と存続条項」で規定する存続条項を除き、「HPKI 認証局専門家会議」が無効と宣言した時点又は「HPKI 認証局専門家会議」が機能を果たさなくなった場合、無効になる。

9.10.3 終了の影響と存続条項

文書が終了した場合であっても、「9.3 企業情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」に関する責務は存続するものとする。また、「HPKI 認証局専門家会議」において部分的な存続を定めた場合は、当該存続部分は有効なものとする。

9.11 関係者間の個々の通知と連絡

認証局から加入者への通知方法は、別項で特に定めるものを除き、電子メール、ホームページへの掲載、郵送による書面通知など認証局が適当と判断した方法により行うものとする。また、認証局から加入者の届け出た住所又は電子メールアドレスに宛てて加入者への通知を発した場合には、当該通知が延着又は不着となった場合であっても、通常到達すべき時に到達したものとみなす。

9.12 改訂

9.12.1 改訂手続き

「HPKI 認証局専門家会議」が本 CP/CPS の改訂を行う場合は、改訂に先立ち、本 CP/CPS に関連する全ての認証局に通知を行い、意見を求める。

本 CP/CPS が変更された時は、「HPKI 認証局専門家会議」によって承認する。

9.12.2 通知方法と期間

本 CP/CPS が改訂された場合、リポジトリを通じて、全ての加入者、関連する認証局及び検証者に速やかに公開する。公開の期間については、次のように定める。

- 重要な変更は、通知後 90 日を上限として、通知に定められた告知期間を経て効力を生ずる。なお、通知後、上記で示した方法に従い通知を行うことにより、変更を中止することもあり得る。但し、監査指摘事項などによる緊急を要する重要

な変更は、通知後、直ちに効力を生ずる。

・ 重要でない変更は、通知後直ちに効力を生ずる。

9.12.3 オブジェクト識別子（OID）の変更理由

本 CP/CPS の変更があった場合には、本 CP/CPS のバージョン番号を更新する。また、次の場合には、OID を変更する。

・ 証明書又は CRL/ARL のプロファイルが変更されたとき

・ セキュリティ上重要な変更がされたとき

9.13 紛争解決手続

加入者又は署名検証者と本認証局との間に、訴訟又は法的行為が起こった場合は、東京地方裁判所を管轄裁判所とする。

9.14 準拠法

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

9.15 適用法の遵守

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

9.16 雑則

9.16.1 完全合意条項

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

9.16.2 権利譲渡条項

規定しない。

9.16.3 分離条項

本 CP/CPS のひとつ又は複数の条項が司法の判断により、無効であると解釈された場合であっても、その他の条項の有効性には影響を与えない。無効と判断された条項は、法令の範囲内で当事者の合理的な意思を反映した規程に読み替える。

9.16.4　強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5　不可抗力

以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、「9.7 無保証」の規定により認証局は免責される。

- 火災、雷、噴火、洪水、地震、嵐、台風、天変地異、自然災害、放射能汚染、有害物質による汚染、又は、その他の自然現象
- 暴動、市民暴動、悪意的損害、破壊行為、内乱、戦争（宣戦布告されているか否かを問わない）又は革命
- 裁判所、政府又は地方機関による作為又は不作為
- ストライキ、工場閉鎖、労働争議
- 認証局の責によらない事由で、本 CP/CPS に基づく義務の遂行上必要とする必須の機器、物品、供給物若しくはサービス（電力、ネットワークその他の設備を含むがそれに限らない）が利用不能となった場合

9.17　その他の条項

本 CP/CPS を採用した認証局又は登録局が別の組織と合併若しくは別の組織に移管、譲渡する場合、新しい組織は本 CP/CPS の方針に同意し責任を持ち続けるものとする。