・本CP又は認証局が定めるCPS若しくはその双方に従って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。

・加入者の特定ができない場合で、緊急に失効させる必要があると認証局が判断した場合。

4.9.2 失効申請者

認証局は、次の1人又はそれ以上の者からの失効申請を受け付ける。

1. 本人の名前で証明書が発行された加入者若しくはその代理人
2. 認証局の職員

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。

＜本人からの失効申請の場合＞

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「4.2.1 本人性及び組織の認証」で用いた申請者の各種書類を参照する。

＜代理人からの失効申請の場合＞

代理人が失効を要求して来た場合は、当該代理人が正当な失効権限を持っていることを確認する。確認にあたっては、加入者の委任状の提出、本人死亡の場合などは、法定代理人と確認できる書類等の提出を求める。

当該証明書の実際の失効にあたっては、代理人を通じて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「4.2.1 本人性及び組織の認証」で用いた申請者の各種書類を参照する。

上記それぞれの確認と共に、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しなくてはならない。

＜認証局の職員からの失効申請の場合＞

認証局は「4.9.1 証明書失効の要件」の中の認証局の職員から失効申請があった場合は、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しなくてはならない。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なくてはならない。

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しなくてはならない。

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わなければならない。その期限はCPSに定めるものとする。

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。その期限はCPSに定めるものとする。

4.9.6 検証者の失効情報確認の要件

検証者は、署名者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発行頻度

変更がない場合においても、48時間以内に96時間以内の有効期限のCRLを発行する。この具体的な頻度と有効期限はCPSで規定するものとする。

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。また、認証局私有鍵（以下、CA私有鍵という）、加入者の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。

4.9.8 CRLが公開されない最大期間

CRL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、CA 署名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、本 CP「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 27002:2006 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。

削除: X 5080:2002

5.1 建物及び物理的管理

5.1.1 施設の位置と建物構造

認証局を運用する施設は、隔壁により区画されていて、施錠できることとする。

認証局システム（以下、CAシステム）を設置する施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、かつ建物構造上、これら災害防止のための対策を講ずる。また、施設内において使用する機器等を、災害及び不正侵入防止策の施された安全な場所に設置すること。

5.1.2 物理的アクセス

認証局を運用する施設は認証業務用設備の所在を示す掲示がされていないこと。また物理的なアクセスを制限する適切なセキュリティ管理設備を装備し、入退出管理を実施すること。入退出者の本人確認はCPSで定める方法により確実に行い、かつ入退出の記録を残すこととする。

認証設備室への立入は、立入に係る権限を有する複数の者により行われることとし、入室者の数と同数の者の退室を管理すること。設備の保守あるいはその他の業務の運営上必要な事情により、やむを得ず、立入に係る権限を有しない者を認証設備室へ立ち入らせることが必要である場合においては、立入に係る権限を有する複数の者が同行することとする。

登録設備室においては、関係者以外が容易に立ち入ることが出来ないようにするための施錠等の措置が講じられていること。

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とする。

また、空調設備により、機器が適切に動作する措置が講じられていることとする。

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とする。

また、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や、その他の耐震措置が講じられていることとする。

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とする。また、防火区画内に設置されていることとする。

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、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、認証局の定める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 施設外のバックアップ

バックアップ媒体は、認証局施設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、JIS Q 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第10章 通信及び運用管理」がこれに相当する。

削除: X 5080:2002

削除: X 5080:2002

削除: 8

5.2.1 信頼すべき役割

証明書の登録、発行、取消等の業務及び関連する業務に携わる者には、CA システムの設定やCA私有鍵の活性化等を担当する「CAシステム管理者」、加入者証明書の発行・失効を担当する「登録局管理者」、及び「監査者」などがあり、本CP上信頼される役割を担っている。認証局においては、業務上の役割を特定の個人に集中させず、前述のように複数の役割に権限を分離した上、個人が複数の役割を兼任することは避けること。

5.2.2 職務ごとに必要とされる人数

CA システムへの物理的又は論理的に単独でのアクセスを避けることができるような必要人数を定めること。

5.2.3 個々の役割に対する本人性確認と認証

認証局システム、登録局システムへアクセスし、CA 私有鍵の操作や証明書発行、失効に係わる操作等の重要操作を行う権限者は、認証局運営責任者により任命されること。

また、システムへの認証には当該業務へ専用に用いる IC カード等のセキュリティデバイスに格納された、本人しか持ち得ない権限者の私有鍵等を用いた強固な認証方式を採用すること。

5.2.4 職務分離が必要になる役割

CA 私有鍵の操作や CA システム管理者、登録局システム管理者の登録等の重要操作は、複数人によるコントロールを採用すること。

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。

なお、要員管理は、JIS Q 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第 8 章　人的資源のセキュリティ」等がこれに相当する。

削除: X 5080:2002

削除: X 5080:2002

削除: 6

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 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第 10 章　通信及び運用管理」、「第 11 章　アクセス制御」、「第 12 章　情報システムの取得、開発及び保守」、「第 15 章　順守」等がこれに相当する。

削除: X 5080:2002

削除: X 5080:2002

削除: 8

削除: 9

削除: 10

削除: 12

削除: 適合性

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、オフラインの記録媒体に CPS に定める頻度でバックアップが取られ、それらの媒体はセキュアな保管場所に保管される。

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 27002:2006 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、JIS Q 27002:2006 の「第 12 章 情報システムの取得、開発及び保守」、「第 15 章 順守」等がこれに相当する。

削除: ISO 17799:2005

削除: ISO/IEC17799:2005

削除: 調達

削除: 維持

削除: 適合性

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。

- 証明書の発行/取消に関する処理履歴
- CRL の発行に関する処理履歴
- 認証局の証明書
- 加入者の証明書
- 証明書申請内容の審議の確認に用いた書類
- 失効の要求に関わる書類

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

規定しない。

5.5.5 記録にタイムスタンプをつける要件

規定しない。

5.5.6 アーカイブ収集システム（内部対外部）

規定しない。

5.5.7 アーカイブ情報を入手し、検証する手続

規定しない。

5.6 鍵の切り替え

認証局は、定期的に CA 私有鍵の更新を行う。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。

CA 私有鍵の更新と共に自己署名証明書の更新も実施される。この更新においても 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。

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。

- 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、障害発生時には、可能な限り速やかに、加入者、検証者に情報公開用 Web サイト等により通知する。

5.7.3 CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又はそのおそれが生じた場合は、運用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、全ての加入者証明書の失効を行い、CRL/ARL を開示し、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

認証局が運営を停止する場合には、運営の終了の 90 日前までに加入者に通知し、認証局の鍵と情報の継続的な保管を手配するものとする。

認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めを行うこととする。

登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知する。

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

エンドエンティティの加入者の私有鍵が認証局で生成される場合は、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、加入者に引き渡されるものとする。認証局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。

6.1.3 認証局への公開鍵の送付

エンドエンティティの加入者の公開鍵が加入者により生成される場合は、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、認証局に引き渡されるものとする。

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、本ポリシを公開する機関のサイトで公開するものとする。

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。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。

エンドエンティティ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。他のアルゴリズムを使用するエンドエンティティ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。

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

認証局の鍵は、keyCertSign と cRLSign のビットを使用する。

エンドエンティティの鍵は、nonRepudiation 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

CA 私有鍵の格納モジュールは、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。

エンドエンティティの加入者私有鍵の格納モジュールは、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 私有鍵の複数人によるコントロール

CA 私有鍵の生成には、運用管理者と複数名の権限者を必要とする。また、鍵生成後の私有鍵の操作（活性化、非活性化、バックアップ、搬送、破棄等）においても複数名の権限者を必要とする。

6.2.3 私有鍵のエスクロウ

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。

エンドエンティティの加入者の私有鍵は、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

CA 私有鍵のバックアップは、安全な方法で行う。例えば、バックアップ作業の権限を有する複数人の立会いのもとで行うようにしたり、バックアップデータとして CA 私有鍵に関する情報を暗号化したり分散させて保管するなどの方法がある。

6.2.5 私有鍵のアーカイブ

認証局は加入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と取り出し

CA 私有鍵は、安全に格納することとする。例えば、認証設備室内にある暗号モジュール内に格納するなどの方法がある。

外部へのバックアップの転送や外部からのリストアの場合は、セキュアチャネルを通して行うものとする。

6.2.7 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。

6.2.8 私有鍵の活性化方法

CA 私有鍵の活性化の方法は、認証局室内において本 CP「6.2.2 私有鍵の複数人によるコントロール」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

CA 私有鍵の非活性化の方法は、認証局室内において本 CP「6.2.2 私有鍵の複数人によるコントロール」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

CA 私有鍵を破棄しなければならない状況の場合、認証局室内で本 CP「6.2.2 私有鍵の複数人によるコントロール」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。

加入者私有鍵破棄手続きは、CPS 又は加入者が入手可能な文書に記述するものとする。

6.2.11 暗号モジュールの評価

CA 私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 3 と同等以上のものを使用する。

エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 1 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

公開鍵は、後日の署名の検証を可能にするために、信頼できる方法でアーカイブする必要がある。認証局は、公開鍵が CPS で定める期間アーカイブされることを保証する責任があるものとする。

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 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。

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 年を越えないものとし、その私有鍵の使用は 2 年を越えないものとする。

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 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認証局で定められた規定に従い実施されるものとする。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、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認証局で定められた規定に従い実施され、加入者に安全に伝えられるものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、活性化データは予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。

6.4.2 活性化データの保護

認証局において用いられる CA 私有鍵の活性化データは、認証局で定められた規定に従い安全に保護される。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データが加入者に伝えられた後は、認証局においては完全に破棄し保管しないものとする。また、伝えられた活性化データは、認証局で定められた規定に従い、加入者により安全に保護するものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、認証局で定められた規定に従い、加入者により安全に保護するものとする。

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

認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を行うこと。

CA システムへのログイン時には、本 CP「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

ISO15408 を参考にセキュリティ基準を設ける等の対応を行い、客観的に評価を行うこと。

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 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

JIS Q 27002:2006「第 12 章 情報システムの取得、開発及び保守」と同等以上の規格に従うものとする。

削除: X 5080:2002「第 10 章

6.6.2 セキュリティ運用管理

JIS Q 27002:2006「第 12 章 情報システムの取得、開発及び保守」、「第 13 章 情報セキュリティインシデントの管理」、「第 14 章 業務継続管理」と同等以上の規格に従うものとする。

削除: X 5080:2002「第 10 章

削除: 11 章 事業

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

JIS Q 27002:2006 と同等以上の規格に従うものとする。

例えば、JIS Q 27002:2006 の「第 10 章 通信及び運用管理 10.6 ネットワークセキュリティの管理」、「第 11 章 アクセス制御 11.4 ネットワークのアクセス制御」等がこれに相当する。

削除: X 5080:2002

削除: X 5080:2002

削除: 8

削除: 8.5

削除: ネットワーク

削除: 9

削除: 9

6.8 タイムスタンプ

認証設備は、アプリケーション等において正確な日付・時刻を使用することとする。例えば、NTP サービスや GPS、電波時計等による時刻同期が挙げられる。

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CPの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。

本ポリシに従い発行される電子証明書のプロファイルは、基本領域のプロファイルを表7.1.1に示し、拡張領域のプロファイルを表7.1.2の通りとする。

なお、IssuerのDNはCPS及びその他開示文書に記述されることとする。

7.1.1 バージョン番号

本ポリシの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（保健医療福祉分野の属性を含む）

本ポリシに従い発行される電子証明書の拡張領域のプロファイルは以下の表7.1.2の通りとする。

subjectDirectoryAttributes 拡張で用いる保健医療福祉分野の属性（hcRole）については7.1.10で定める。

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。

- sha1WithRSAEncryption (1.2.840.113549.1.1.5)
- sha256WithRSAEncryption (1.2.840.113549.1.1.11)
- sha384WithRSAEncryption (1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (1.2.840.113549.1.1.13)

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7.1.1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

CPSを参照するURLを含めることができる。

7.1.9 証明書ポリシ拡張フィールドの扱い

本CPのOIDを格納する。

表 7.1.1　証明書のプロファイル（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	◎	
Validity	◎	
NotBefore	◎	
NotAfter	◎	
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	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシを示す文字列を記載する。（「HPKI-01-*-forNonRepudiation」とする。なお、文字列中の"01"は、本 CP の版数である"第 1.0 版"を示す。また、"*"は CA を唯一に識別できる文字列とする。）
Subject	◎	英数字のみ使用する。（CountryName、SerialNumber は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	○	加入者が医療機関等の管理者の場合は必須。 その場合は医療福祉機関名をローマ字あるいは英語名で OrganizationName に記載し、 OrganizatioUnitName に” Director” の文字列を格納する。
OrganizationUnitName	○	
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。
SubjectPublicKeyInfo	◎	
Algorithm	◎	RSAEncryption とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域（Extensions）参照

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

表 7.1.2　証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subejctKeyIdentifier	◎		FALSE
KeyUsage	◎		TRUE
DigitalSignature	×		-
NonRepudiation	◎		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	×		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△		FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	◎	医療従事者等の資格（hcRole）を記載。	FALSE
AttrType	○	加入者が国家資格保有者及び医療機関等の管理者の場合は必須。その他(患者等)の場合は省略可。	-
AttrValues	○	HCActor の codeDataFreeText に資格名テーブル表 7.1.3 の英表記を UTF8String で設定。subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定する。	-
basicConstraints	×		TRUE
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	◎	DirectoryName あるいは URI で、CRL の配布点を指定する。	FALSE
subjectInfoAccess	×		FALSE
authorityInfoAccess	△		FALSE

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

7.1.10 保健医療福祉分野の属性（hcRole）

(1) サブジェクトディレクトリ属性拡張での hcRole 属性の使用

本ポリシでは、ISO, 17090 で規定した hcRole 属性を下記に示すようにプロファイルして用いることにする。

subjectDirectoryAttributes の attrType には hcRole を表す OID {id-hcpki-at-healthcareactor} を設定する。

attrValue は HCActorData で、HCActor の codedData では codeValueData は用いず、codeDataFreeText を用いる。

本ポリシでは coding scheme reference の OID として ISO coding scheme reference を用いず、本 CP の元で定めた表 7.1.3 の資格名を参照する local coding scheme reference の OID は、{ iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6) national-coding-scheme-reference(2) version(1) }を用いる。資格名は、表 7.1.3 に示すように英語表記を用い UTF8string で設定する。

subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定することができる。

本拡張は、加入者が国家資格保有者及び医療機関等の管理者の場合は必須、その他(患者等)の場合は省略可とする。

削除: TS

削除: IS

削除: 1

表 7.1.3 HPKI 資格名テーブル（codeDataFreeText の定義）

資格名（国家資格）	説明
'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
'Clinical Engineer'	臨床工学技師
'Masseur'	あん摩マッサージ指圧師/はり師/きゅう師
'Dental Hygienist'	歯科衛生士
'Prosthetics & Orthetic'	義肢装具士
'Artificial Limb Fitter'	柔道整復師
'Clinical Laboratory Technician'	衛生検査技師
資格名（医療機関の管理責任者）	説明
'Director of Hospital'	病院長
'Director of Clinic'	診療所院長
'Supervisor of Pharmacy'	管理薬剤師
'Proprietor of Pharmacy'	薬局開設者
'Director'	その他の保健医療福祉機関の管理責任者

注）資格名のワード間の空白は一個の Space (x20)とする。

削除: 'Care Manager'

削除: Director

患者に対して署名付の文書を交付することが多い医療機関等の管理責任者を hcRole だけで識別できるように定めている。

なお、上記 Director の属性を使用する場合は Subject フィールドの OrganizationName 及び OrganizationUnitName は必須で、OrganizationName に保健医療福祉機関名を英語又はローマ字で格納し、OrganizationUnitName に"Director"の文字列を格納する。

削除: 病院長、診療所院長、管理薬剤師、薬局開設者

削除: 4

(2) HPKI hcRole 属性プロファイル

本 HPKI の CP では、ISO TS 17090 に定められた hcRole 属性の ASN.1 表記を以下のようにプロファイルする。

```
hcRole ATTRIBUTE : := {
   WITH SYNTAX                  HCActorData
   EQUALITY MATCHING RULE       hcActorMatch
   SUBSTRINGS MATCHING RULE     hcActorSubstringsMatch
   ID                           id-hcpki-at-healthcareactor}

-- Assignment of object identifier values
-- The following values are assigned in this Technical Specification:
   id-hcpki OBJECT IDENTIFIER :: = {iso (1) standard (0) hcpki (17090)}
   id-hcpki-at OBJECT IDENTIFIER :: = {id-hcpki 0 }
   id-hcpki-at-healthcareactor OBJECT IDENTIFIER :: = {id-hcpki-at 1}
   id-hcpki-cd OBJECT IDENTIFIER :: = {id-hcpki 1}
-- Following values are defined in Japanese HPKI CP:
   id-jhpki OBJECT IDENTIFIER :: =
                    {iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1)}
   id-jhpki-cdata OBJECT IDENTIFIER :: = { id-jhpki 6 1 1 }

-- Definition of data types:
HCActorData :: = SET OF HCActor

HCActor :: = SEQUENCE {
   codedData [0] CodedData,
   regionalHCActorData [1] SEQUENCE OF RegionalData OPTICNAL } -- Note1 (Do not use)

CodedData :: = SET {
   codingSchemeReference [0] OBJECT IDENTIFIER,
   -- Contains the ISO coding scheme Reference
   -- or local coding scheme reference achieving ISO or national registration.
   -- Local coding scheme reference in Japanese HPKI is id-jhpki-cdata (defined above)
   -- In this profile, use this OID: Note 2
   -- At least ONE of the following SHALL be present
   codeDataValue [1] NumericString OPTIONAL, -- Note 3 (Do not use)
   codeDataFreeText [2] DirectoryString } -- Note 4

RegionalData :: = SEQUENCE { } -- Do not define in Japanese HPKI CP
```


Note1： HCActor の regionalHcActorData は、本 CP では使用しない。

Note2： 日本の HPKI CP で定めた local coding scheme reference の OID は、id-jhpki-cdata {iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6) national-coding-scheme-reference(2) version(1)} とする。この OID は、表 7.1.3 の資格名を参照する。

Note3： 本 CP では CodedData の codeDataValue は用いない。

Note4： 本 CP では、codeDataFreeText としての DirecroryString には表 7.1.3 に規定した 'Medical Doctor' などの英語表記の資格名を用いる。また、DirecroryString は UTF8String でエンコードしたものを使う。マッチングルールはバイナリーマッチングによる。

削除: 1

＜参考＞

以下に、hcRole を含めた X.509 SubjectDirectoryAttributes 拡張を DER エンコードしたデータの ASN.1 構造をダンプした例を示す。

Medical Doctor の例

```
No Type Len Value
-----------------------------------------------------------------------
  0 30   61: SEQUENCE {-- SubjectDirectoryAttributes ext.extnValue contents
  2 06    3:   OBJECT IDENTIFIER subjectDirectoryAttributes (2 5 29 9)
  7 04   54:   OCTET STRING, encapsulates {
  9 30   52:     SEQUENCE {-- SubjectDirectoryAttributes
 11 30   50:       SEQUENCE {-- Attribute::hcRoleAttribute
 13 06    6:         OBJECT IDENTIFIER '1 0 17090 0 1'  -- OID::type
 21 31   40:         SET {-- SET of AttributeValue::values
 23 31   38:           SET {-- AttributeValue::HCActorData
 25 30   36:             SEQUENCE {-- HCActor
 27 A0   34:               [0] {-- HCActor
 29 31   32:                 SET {-- CodedData
 31 A0   12:                   [0] {-- codingSchemeReference: local coding scheme
 33 06   10:                     OBJECT IDENTIFIER '1 2 392 100495 1 6 1 1'
        :                     }
 45 A2   16:                   [2] {-- codeDataFreeText
 47 0C   14:                     UTF8String 'Medical Doctor'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
        :         }
        :       }
        :     }
        :   }
```

"--"以降はコメント

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 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。

基本領域のプロファイルは表 7.2.1 に示す。

7.2.2 CRL と CRL エントリ拡張領域

CRL エントリの拡張領域のプロファイルは、以下の表 7.2.2 の通りとする。CRL 拡張領域のプロファイルは、以下の表 7.2.3 の通りとする。

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

表 7.2.1 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 7.1.1 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	◎	c=JP(固定)とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシを示す文字列を記載する。
ThisUpdata	◎	
NextUpdate	◎	
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（crlEntryExtentions）参照
CrlExtentions	◎	拡張領域（crlExtensions）参照

削除: SHA-1WithRSAEncryption

表 7.2.2　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	×		FALSE
InvalidityDate	×		FALSE
CertificateIssure	×		TRUE

表 7.2.3　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
IssuerAltName	△		FALSE
CRLNumber	◎		FALSE
DeltaCRLIndicator	×		TRUE
IssueingDistributionPoint	○	分割 CRL を用いる場合は必須	TRUE
FreshesCRL	×		FALSE

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

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。本 CP に従って証明書を発行する認証局は、本 CP の要件に完全に従っているということを検証者、加入者及び HPKI 認証局専門家会議が満足する形で確立するものとする。

8.1　監査頻度

認証局の準拠性監査は、1 年以下の間隔で行われるものとする。但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施するものとする。

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部門から独立した、適切な能力を有する監査者に定期監査を委託するものとする。

8.3　監査者と被監査者の関係

監査者は、認証局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 及び関連する 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、認証局代表者の指示のもと、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

各種の料金については、本 CP に従い運用される認証局が設定するものとし、本 CP では規定しない。

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

本CPに従い運用される認証局は、その継続的な運営に必要とされる十分な財務的基盤を維持しなくてはならない。

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 業務情報の秘密保護

9.3.1 秘密情報の範囲

本CPに従う認証局が保持する個人及び組織の情報は、証明書、CRL 、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。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。

加入者の私有鍵は、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、本CP 「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

証明書及びCRL 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。

- 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

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洩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、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洩した場合、その責は漏洩した者が負う。

9.4 個人情報のプライバシー保護

9.4.1 プライバシーポリシ

認証局における個人情報の取り扱いについては、各認証局の CPS で特定される「プライバシーポリシ」を適用するものとする。

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洩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

個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。

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。

・ 加入者証明書：認証局に帰属する財産である
・ 加入者の私有鍵：私有鍵は、その保存方法又は保存媒体の所有者に関わらず、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
・ 加入者の公開鍵：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
・ CPS：認証局に帰属する財産（著作権を含む）である
・ 本CP：「HPKI認証局専門家会議」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及び認証局の定める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の要件と認証局の定めるCPS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、CP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。
・ 本CP「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。
・ 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。
・ 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、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。

- 証明書発行にあたり、申請内容の真偽の確認を確実に行い、確認の結果を認証局に対して保証すること。
- 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。
- 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、本CP「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

本CPに則り運営される認証局の加入者は、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、認証局の定める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、認証局の定めるCPSに従って速やかに届け出ること。

5. 利用規定の遵守責任
   加入者は、本CP及び認証局で加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。

9.6.4 検証者の表明保証

本CPに則り運営される認証局の検証者は以下の責任を果たすものとする。

1. 利用規定の遵守責任
   検証者は、本CP及び認証局で検証者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。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
   - 証明書の有効期限が切れていないこと
   - 証明書が失効していないこと
   - 証明書の記載事項が、本CP「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HPKIの規定に一致していること
     ・hcRole及びkeyUsageのnonRepudiation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、本CP「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、本CP「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、本CP「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

本CPに規定された責任を果たさなかったことに起因して、認証局がサービスの加入者に対して損害を与えた場合、認証局で定める金額を上限として損害を賠償する。

ただし、認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、又は予見の有無を問わず、特別損害については、いかなる場合でも一切の責任を負わない。

また、加入者は認証局が発行する証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。

9.10　本ポリシの有効期間と終了

9.10.1　有効期間

本CP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の終了まで有効であるものとする。

9.10.2　終了

本CP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、FAX番号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の改訂を行う場合は、改訂に先立ち、本CP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が改訂された場合、情報公開用Webサイト等を通じて、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 の変更があった場合には、本 CP 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 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
- 本人性、国家資格の確認方法の厳密さに重要な影響を及ぼす変更がされたとき

9.13 紛争解決手続

証明書の発行主体である、各認証局の CPS において定める。

9.14 準拠法

本 CP 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 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 は、本 CP 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

関係者は、本 CP に定める権利義務を担保に供することができない。また、次の場合

を除き、第三者に譲渡することができない。

- 認証局が登録局に本 CP に定める業務の委託を行うとき
- 本 CP に則った認証局の移管又は譲渡を行うとき

9.16.3 分離条項

本 CP 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定に読み替える。

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、本 CP「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 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 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 の方針に同意し責任を持ち続けるものとする。