	証明書ポリシ	監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.2.10	私有鍵の破棄方法 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。	(1) CA私有鍵を破棄する場合、物理的に安全な場所(認証局室内等)で、権限を付与された複数人によるコントロール(例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制)によって、安全な方法(例えばトークンへの新しい鍵、ゼロ又はスペースの上書き、トークンの破壊など)で行われていること。 (2) CA鍵ペアの有効期間が終了するとき、そのCA私有鍵の全てのコピーとフラグメントが、破壊されていること。 (3) アクセス可能な状態にある暗号モジュールが永久にサービスから取り除かれるとき、そのモジュールの中に格納されている全ての鍵が消去されていること。 (4) 加入者の私有鍵の破棄手続が、CPS又は加入者が入手可能な文書に明記されている。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CA私有鍵および加入者私有鍵が権限を付与された複数人によるコントロールで安全な方法を用いて破棄されることを確認する。					
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。	暗号モジュールは、FIPS 140-2の適切なセキュリティレベル(CA私有鍵の場合レベル3と同等以上、加入者私有鍵の場合レベル1と同等以上)のものを使用していること。	メーカ取得した認定書、CPSを閲覧し、FIPS 140-2の適切なセキュリティレベルのものを使用していることを確認する。					
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。	認証局は、デジタル署名又は適切なインテグリティコントロールによって改ざんを検証又は防止し、CPSが定める期間、CAが生成した全ての公開鍵(CA、レポジトリ、下位CA、RA、加入者及び他の関係者)をアーカイブしていること。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CPSが定める期間、CAが生成した全ての公開鍵をアーカイブしていることを確認する。					
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。	(1) 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していること。 (2) 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していること。	(1)(2) CPSを閲覧し、私有鍵および公開鍵の有効期間がCPで定める範囲内であることを確認する。					
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。	(1) CA私有鍵の活性化データ(PIN、パスフレーズ、鍵分散の断片など)は、一意で予測不能なものになっていること。 (2) CA私有鍵の活性化データの生成及びインストールは、CPS等に準拠し実施されていること。 (3) 加入者私有鍵の活性化データは、一意で予測不能なものになっていること。 (4) 加入者私有鍵の活性化データの生成及びインストールは、CPS等に準拠し実施されていること。	(1)(3) CPS、PKIソフトウェア概要書、鍵ライフサイクル管理規程などを閲覧し、活性化データが一意で予測不能なものになっていることを確認する。 (2)(4) CPS、運用マニュアル、RAマニュアルなどを閲覧、および、実際の操作を観察し活性化データの生成及びインストールが、CPSに準拠して実施されていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
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。	(1) CA私有鍵の活性化データの取扱い（保管、バックアップ、転送、廃棄など）は、CPSに準拠し、CA私有鍵と同等に安全に保護されていること。 (2) CA（又はRA）が加入者の活性化データを生成している場合、認証局は、私有鍵の活性化データを、加入者に送付した後、完全に廃棄（消磁、破壊、他のデータの上書きなど）し、保管していないこと。 (3) 加入者は、自ら生成した又は認証局から送付された活性化データを安全に保護するよう、CPS、契約書、サービス約款などで義務付けられていること。	(1) CPS、運用マニュアル、RAマニュアルなどを閲覧、CA私有鍵の活性化データが安全に取扱われていることを確認する。 (2) CPS、PKIソフトウェア概要書、鍵ライフサイクル管理規程などを閲覧し、CA（又はRA）が加入者の活性化データを生成している場合、認証局は、私有鍵の活性化データを、加入者に送付した後、完全に廃棄し、保管していないことを確認する。 (3) CPS、契約書、利用約款などでを閲覧し、加入者が自ら生成した又は認証局から送付された活性化データを安全に保護するよう義務付けられていることを確認する。					
6.4.3	活性化データのその他の要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
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。	・認証業務用設備に対するアクセスに対する方針（例えば、①職務に対応したアクセス権限付与、②個人識別及び本人確認の方法、③職務分離、④特別なCAオペレーションを遂行するために必要な要員数（n out of m rule））が定められていること。 ・上記アクセス方針は、認証業務用設備に対する不正なアクセス等を防御することに対する対策（具体的には、①個人識別、②本人確認、③権限確認、④アクセスログ取得）を講じていること。 ・認証業務用設備に対するアクセスポイントにおいて、上記アクセス方針に基づく設定が行われていること。 ・CAシステムへのログイン時のプロセスが、本CP「5.2.3 個々の役割に対する本人性確認と認証」で定める方法と同じプロセスにより、ユーザの認証を行っていること。	・認証業務用設備に対して責任を有するものに対する質問により、左記アクセス方針が想定されるリスクに対して十分であると判断している理由等を確認する。 （①CAオペレータのOSアクセス、②DB管理者のDBMSアクセス、RAオペレータのCAアプリケーションアクセスのそれぞれについて、必要に応じCAの構成について確認する） ・認証業務用設備に対する当該電気通信回線へのアクセスに対する方針をレビューし、対策の網羅性、リスクに対する対策強度の十分性を評価する。 ・認証業務用設備に対するアクセスポイントにおいて、左記アクセス方針に従った設定が行われていることを機器等の設定値を閲覧することにより確認する。 ・CAシステムへのログイン時のプロセスが、本CP「5.2.3 個々の役割に対する本人性確認と認証」で定める方法と同じプロセスによりユーザの認証を行っていることを、運用規程等により確認する。					
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。	・コンピュータ機器に対するセキュリティ基準を定めること。 ・コンピュータ機器が、上記セキュリティ基準により適切な客観的な評価者による評価を受けていること。 要件として求められるものではないが、例えば CAソフトウェア及びインターネットファイアウォールに関しては、次に掲げる業界基準があり、セキュリティ基準の設定、セキュリティ対策の参考とすることができる。 ①ITSEC－レベルE2 ②TCSEC－レベルC2 ③CC（ISO15408）－レベルEAL3	・責任者に対し質問あるいは評価報告書等を閲覧し、ISO15408等のセキュリティ基準を参考にし、コンピュータ機器に対する想定されるリスクを軽減するための十分なセキュリティ基準を定めていることを確認する。 ・上記セキュリティ基準を閲覧し、想定されるリスクを軽減するために十分なセキュリティ対策が規定されていることを評価する。 ・評価報告書等を閲覧し、コンピュータ機器が、上記セキュリティ基準に照らして客観的な評価者による評価を受けていることを確認する。 ・評価者に質問、又は評価者の評価能力を示す資料を閲覧することにより、上記評価者が十分な評価能力を有していることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.6.1	システム開発管理 JIS X 5080:2002「第10章　システムの開発及び保守」と同等以上の規格に従うものとする。	・新規システム又は既存システムの改善に対するビジネス要件定義書には、コントロール要件を具体的に記述すること。(10.1.1) ・認証業務用システムの変更の実施を厳しく管理すること。(10.5.1) ・オペレーティングシステムを変更した場合は、認証業務用システムを閲覧し、運用又はセキュリティに影響を与えないかどうかを確認すること。(10.5.2) ・パッケージソフトウェアの変更は、組み込まれたコントロールとインテグリティのプロセスが危殆化する場合やベンダから必要な改定版が得られる場合を除き、極力行わないこと。(10.5.3) ・隠れチャネル及びトロイの木馬が心配される場合には、信頼できるソースからのソフトウェアの購入、コード変更の制限、ソースコードの検査を行うこと。(10.5.4) ・ソフトウェア開発を外部委託する場合には、ライセンス契約、コードの所有権、知的財産権、実施される業務の品質検査、立ち入り監査権、受入検査などについて検討を行うこと。(10.5.5)	・開発・保守管理責任者に質問し、システム開発・保守のための手続きの説明をうけ、統制上の重大なプロセス漏れがないことを確認する。 ・システム開発・保守のための規程・手続書類を閲覧し、想定されるリスクに対して十分な統制活動が組み込まれていることを評価する。 ・システム開発・保守のための申請書等を閲覧し、定められた閲覧・検査・承認が適切に行われていることを確認する。 ・ソフトウェア開発を外部委託する場合の事業者・作業者の選定基準および契約書を閲覧し、想定されるリスクに対して十分な統制活動が組み込まれていることを評価する。					
6.6.2	セキュリティ運用管理 JIS X 5080:2002「第10章　システムの開発及び保守」、「第11章　事業継続管理」と同等以上の規格に従うものとする。	・認証業務用システムに入力されたデータは、正確で適切であることを確かめるために、その妥当性を確認すること。(10.2.1) ・処理エラーや意図的な行為によるデータの改変を検出するために、システムに妥当性の検査を組み込むこと。(10.2.2) ・メッセージ内容のインテグリティを確保すべきセキュリティ要件がCAシステムに存在する場合には、メッセージ認証の適用を考慮すること(10.2.3) ・認証業務用システムからの出力データについては、格納された情報の処理がシステム状況に応じて正しく、適切に行われたことを確かめるために、妥当性を確認をすること。(10.2.4) ・運用システムへのソフトウェアの導入を管理すること。(10.4.1) ・試験データを保護し、管理すること。(10.4.2) ・プログラムソースライブラリへのアクセスを厳密に管理すること。(10.4.3)	・運用規程、運用手順書を閲覧し、認証業務用システムに入力・処理・出力されるデータが、正確で適切であることを確実するために必要な手順が定められていることを確認する。 ・認証業務用システム上のソフトウェアの実行を管理するための運用規程・運用手順書が整備されていることを確認する。					
		・組織全体を通じて事業継続計画を開発及び保守するための健全な管理プロセスが整っていること。(11.1.1) ・事業継続計画は、業務プロセスの中断を引き起こし得る事象を明確化することから始めること。(11.1.2) ・事業継続に対する全体的なアプローチを決定するために、適切なリスクアセスメントに基づいた戦略計画を立てること。(11.1.2) ・重要な業務プロセスの中断又は破綻の後、必要なタイムフレームで、事業運営を維持又は復旧させるための計画を立てること。(11.1.3)・すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画（ビジネスユニットごとに作成される）に関する共通の枠組みを維持すること。(11.1.4) ・事業継続計画が最新かつ有効であることを確かめるために、定期的に試験すること。(11.1.5) ・事業継続計画の継続的な有効性を確かめるために、定期的な見直し及び更新によって維持すること。(11.1.5)	・認証業務責任者に質問し、認証業務について、事業戦略的な観点から事業継続計画が策定されていることを、確認する。 ・認証業務についての事業継続計画を閲覧し、想定されるリスクに応じて適切な手順であることを評価する。 ・想定されるリスクが適切であることを評価する。 ・認証業務用システムについて、それぞれの業務手続の中断又は障害の後、認証業務の運営を維持又は要求される時間内に復旧させるための計画を策定していることを確認する。 ・上記事業継続計画が有効に機能するための試験結果を閲覧し、計画の有効性を評価する。 ・認証業務運営会議等の議事録等を閲覧に、上記事業継続計画が、試験結果等に基づき適切に改善されていることを評価する。					
6.6.3	ライフサイクルのセキュリティ管理 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.7	ネットワークのセキュリティ管理 JIS X 5080:2002と同等以上の規格に従うものとする。 例えば、JIS X 5080:2002 の「第8章　通信及び運用管理　8.5 ネットワークの管理」、「第9章　アクセス制御　9.4　ネットワークのアクセス制御」等がこれに相当する。	1）ネットワークにおけるセキュリティを実現し、かつ維持するために、次の事項を含む、一連の管理策を実施すること。(8.5.1) ・ネットワーク運用責任とコンピュータ操作作業を分離すること ・遠隔地に所在する設備がある場合、その管理責任および管理手順を確立すること ・公衆ネットワークを通過するデータの機密性および完全性を保護する管理策を確立すること ・ネットワークに接続したシステムを保護するための管理策を確立すること ・必要に応じネットワークサービスの可用性およびネットワークに接続したコンピュータの可用性を維持するための管理策を確立すること	1）ネットワーク管理に関わる手順書等を閲覧し、管理策が定められていることを確認する。 2）責任者に質問あるいは必要により検査し、管理策が実施されていることを確認する。					
		2）内部及び外部のネットワークを介したサービスは制御されることが望ましい。そのために次の事項を含む一連の管理策を実施すること。(9.4) ・ネットワークサービスの利用者には、使用することが特別に許可されたサービスへの直接のアクセスだけを提供すること。その為に個別方針を明確にすること(9.4.1)	1）利用者に使用を許可するネットワークサービスを規定した文書を閲覧し、次の事項が定められていることを確認する。 ・アクセスが許可されるネットワークおよびネットワークサービス ・アクセス許可の手順 ・ネットワーク接続とネットワークサービスへのアクセスを保護するための管理策と管理手順 2）認証局ネットワークの構成情報を閲覧し、利用者が使用できるネットワークサービスが、許可されたサービスのみに限定されていることを確認する。					
		・利用者端末とコンピュータサービスの間の経路は、権限確認されたユーザだけにアクセスを制限すること。(9.4.2) 例えば次のような方法で限定されていること。 ・専用線や専用電話番号の割り当て ・指定された業務システム又はセキュリティゲートウェイへの自動接続 ・選択できる利用者メニューの制限 ・無制限のネットワーク探索の防止 ・(外部の利用者)指定された業務システムとセキュリティゲートウェイの使用 ・セキュリティゲートウェイ(ファイアウォール等)による制御 ・VPNによるアクセス制限	1）認証局システムとネットワークの構成図、経路設計を閲覧し、ユーザーがコンピュータにアクセスする場合の経路は、アクセスが限定されていることを確認する。 2）適用されている方法に応じた、ネットワーク経路制御情報を閲覧し、設計どおりに設定されていることを確認する。					
		・遠隔地からの利用者のアクセスには、認証を行うこと。(9.4.3) 認証方法は例えば以下によること。 ・暗号に基づく技術 ・ハードウェアトークン ・チャレンジレスポンス	1）認証局ネットワークの構成図を閲覧し、認証局への遠隔接続の有無を確認する。 2）遠隔接続がある場合、接続時の認証方法を記載した文書を閲覧し、認証が行われていることを確認する。 3）遠隔接続時の認証に関わるコンピュータの設定情報を閲覧し、遠隔接続時に認証が行われるよう設定されていることを確認する。 4）遠隔接続の手順を観察し、規定どおりの認証が行われることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
		・遠隔コンピュータシステムへの接続は、身元確認されること。(9.4.4)	認証局のシステム構成図、およびネットワークの構成図を閲覧し、遠隔コンピュータシステムへの接続の有無を確認する。 遠隔コンピュータへの接続がある場合、接続時の認証方法を記載した文書を閲覧し、前項のような方法で認証が行われているか確認する。 接続時の認証に関わる遠隔コンピュータの設定情報を閲覧し、規定どおりの認証が行われる設定となっていることを確認する。遠隔コンピュータへの接続手順を観察し、設定どおりに認証されているか確認する。					
		・遠隔診断ポートへのアクセスは、セキュリティを保つように制御されること。(9.4.5)	手順書等を閲覧し、遠隔診断ポートへのアクセスは、適切な管理のもとに行われるよう、手順が定められていることを確認する。 設備を視察し、遠隔診断ポートへのアクセスが、安全に管理されているか確認する。					
		・情報サービス、利用者及び情報システムのグループを分割するためのネットワークセグメンテーションの導入を考慮すること。(9.4.6)	認証局のネットワーク構成図を閲覧し、認証局ネットワークが、他のネットワークから物理的あるいは論理的に、分割されていることを確認する。 設備を視察し、物理構成が、構成図と一致していることを確認する。 ネットワーク構成情報を閲覧し、論理構成が構成図と一致していることを確認する。					
		・予め定義されたテーブルやルールに基づくゲートウェイでのトラフィックのフィルタリングなど、ネットワーク接続の制限は、業務用ソフトウェアのアクセスポリシと要件に基づくこと。(9.4.7)	認証局に関わる業務用ソフトウェアのアクセス制御方針を閲覧し、利用者が利用可能なサービスが限定されていることを確認する。 ネットワークの構成情報を閲覧し、アクセス制御方針に基づき、利用できるサービスを制限するよう設定されていることを確認する。					
		・共有ネットワークは、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするためのルーティング制御（ソースとデスティネーションのアドレスをチェックする機能）を組み込むこと。(9.4.8)	1）共有ネットワークを使用している場合、ネットワークの経路制御の方法を記載した資料を閲覧し、発信元および宛先アドレスの自動的検査による経路制御が適用されているか確認する。 2）ネットワークの構成情報を閲覧し、経路制御について設定されていることを確認する。					
		・公衆または私設のネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティ属性に関する明細な記述を常備し、個別方針と齟齬がないことを評価すること。(9.4.9)	認証局が使用する全てのネットワークサービスについて、セキュリティの特質を説明した資料やセキュリティ評価報告書等を閲覧し、個別方針と齟齬がないことを評価していることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
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。	認証設備で使用するコンピュータは、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。 例えばNTPサービスやGPS、電波時計等による時刻同期を行うこと。 その選択にあたり、ビジネス要件に基づいて、タイムソースの信頼性、許容時差、調時方法を明確に定め、認証局システムの主要な機器の時刻を調節すること。	1）設計書、手順書等を閲覧し、時刻同期が行われていること、およびその方式を選択するにあたり評価が行われていることを確認する。 2）運用記録等を閲覧し、設計どおりに時刻同期が行われていることを確認する。					
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）により認証局ごとに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。	1) 証明書はX.500識別名（Distinguished Name、以下DNという）により認証局ごとに一意に識別される体系とすること。 2) 発行される電子証明書のプロファイルの内、基本領域のプロファイルはCP中の表7.1.1に従い、拡張領域のプロファイルは表7.1.2に従うこと。 3) なお、IssuerのDNは他の認証局と重ならないことについてHPKI認証局専門家会議による確認をうけ、CPS及びその他開示文書に記載することと。	1) CPS等関連規程を閲覧し証明書はX.500識別名（Distinguished Name、以下DNという）により認証局ごとに一意に識別される体系となっていることを確認する。 2) CPS等関連規程および証明書のサンプルデータを閲覧し、電子証明書のプロファイルの内、基本領域のプロファイルはCP中の表7.1.1に従い、拡張領域のプロファイルは表7.1.2に従っていることを確認する。 3) CPS等関連規定を閲覧し、IssuerのDNは他の認証局と重ならないことについてHPKI認証局専門家会議による確認をうけ、CPS及びその他開示文書に記載していることを確認する。					
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。	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。	CPS等関連規程および証明書のサンプルデータを閲覧し、証明書が、X509 Version 3 フォーマット証明書形式により作成されていることを確認する。					
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。	発行される電子証明書の拡張領域のプロファイルはCP中の表7.1.2に従うこと。 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項の定めに従うこと。	CPS等関連規程および証明書のサンプルデータを閲覧し、発行される電子証明書の拡張領域のプロファイルはCP中の表7.1.2に従っていること、および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項の定めに従っていることを確認する。					
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。 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)	基本領域のSignatureアルゴリズムは以下のものを採用すること。 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を採用すること。 RSAEncryption (1.2.840.113549.1.1.1)	CPS等関連規程および証明書のサンプルデータを閲覧し、SignatureおよびsubjectPublicKeyInfoアルゴリズムがCPで示すものを採用していることを確認する。					
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。	IssureとSubjectの名称の形式はCPの表7.1.1に示すプロファイルの規定に従うこと。	CPS等関連規程および証明書のサンプルデータを閲覧し、IssureとSubjectの名前の形式がCPの表7.1.1に示すプロファイルの規定に従っていることを確認する。					
7.1.5	名称制約 用いない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
7.1.6	CPオブジェクト識別子 別途規定する。	HPKI署名用証明明書ポリシのOIDは1.2.392.100495.1.5.1.1.3.1とすること	CPS等関連規程および証明書のサンプルデータを閲覧し、OIDが1.2.392.100495.1.5.1.1.3.1であることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
7.1.7	ポリシ制約拡張 使用しない。	ポリシ制約のための拡張は使用しないこと。	CPS等関連規程および証明書のサンプルデータ閲覧し、ポリシ制約のための拡張は使用していないことを確認する。					
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。	CPSを参照するURLを証明書ポリシーへ付加する場合はその旨CPS等で明確にすること。	CPSを参照するURLを証明書ポリシーへ付加している場合はCPS等関連規程および証明書のサンプルデータ閲覧し、URLが付加されていることをことを確認する。					
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。	認証局は証明書ポリシーとしてCPの規定するOIDを格納すること。	CPS等関連規程および証明書のサンプルデータを閲覧し、証明書ポリシーとしてCPの規定するOIDを格納していることを確認する。					
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 以下省略	subjectDirectoryAttributesのattrTypeにはhcRoleを表すOID {1 0 17090 0 1} を設定すること。 coding scheme referenceのOIDとしては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{'1 2 392 100495 1 6 1 1}を用いること。 資格名は、CPの表7.1.3に示す英語表記を用いUTF8stringで設定すること。 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(愚者等)の場合は省略可とする。	CPS等関連規程および証明書のサンプルデータを閲覧し、HCActorDataがCPで規定するフォーマットに従っていることを確認する。					
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。	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に従うこと。 基本領域のプロファイルはCPの表7.2.1に従うこと。	CPS等関連規程およびCRLのサンプルデータを閲覧し、CRLの形式がX.509CRLフォーマット形式のバージョン2に従っていること、および基本領域のプロファイルはCPの表7.2.1にしたがっていることを確認する。					
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。 以下省略	CRLエントリの拡張領域のプロファイルは、CPの表7.2.2に従うこと。また、CRL拡張領域のプロファイルは、CPの表7.2.3に従うこと。	CPS等関連規程およびCRLのサンプルデータを閲覧し、CRLエントリの拡張領域のプロファイルは、CPの表7.2.2に従うこと、および、CRL拡張領域のプロファイルは、CPの表7.2.3に従うことを確認する。					
7.3	OCSPプロファイル							
7.3.1	バージョン番号 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
7.3.2	OCSP拡張領域 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
8	準拠性監査とその他の評価							
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。	認証局の準拠性監査は、1年以下の間隔で設定すること。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、直ちに監査を実施すること。	CPS等関連規定を閲覧し、準拠性監査が、1年より長くない間隔で行うことになっていることを確認する。また、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こととなっていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
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。	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こと。	1) 外部機関の発行した資格証明書、または監査者の所属する組織の長が監査者の能力を証明した書類を閲覧し、監査者が適切な能力を有していることを確認する。 2) 内部監査の場合は組織図の閲覧により、監査者が認証局から独立していることを確認する。					
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。	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こと。監査者は、被監査者に対しての特別な利害関係を持たないこと。	内部監査の場合は組織図の閲覧により、監査者が認証局から独立していることを確認する。CPS等関連規定により外部監査の場合は認証局と独立しているとみなす。また、認証局代表者の誓約書により利害関係のないことを確認する。					
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。	監査は、本CP及び関連するCPSへの準拠性をカバーすること。	CPS等関連規定および監査報告書を閲覧し、本CP及び関連するCPSへの準拠性をカバーすること確認する。					
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。	認証局は、認証局代表者は改善指摘事項に関する評価を行い、必要な改善を実施すること。	CPS等関連規定を閲覧し、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ことになっていることを確認する。					
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。	(1) 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、HPKI認証局専門家会議に直ちに通知すること。 (2) その場合、認証局は、HPKI認証局専門家会議の意見を参考とし、必要に応じて、加入者及び検証者に通知すること。	CPS等関連規定を閲覧し、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場合は、加入者及び検証者及びHPKI認証局専門家会議に直ちに通知することとなっていることを確認する。					
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。	CPとして監査目標項目なし。						
9.1.1	証明書の発行又は更新料 規定しない。	CPとして監査目標項目なし。						
9.1.2	証明書へのアクセス料金 規定しない。	CPとして監査目標項目なし。						
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。	CPとして監査目標項目なし。						
9.1.4	その他のサービスに対する料金 規定しない。	CPとして監査目標項目なし。						
9.1.5	払い戻し指針 規定しない。	CPとして監査目標項目なし。						