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
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。	(1)認証設備室には、消防法施行令に規定された自動火災報知機及び消火装置を設置し、消防署等の検査を受け、定期点検を実施していること。 (2)認証設備室を含む区画は、建築基準法に規定する防火区画であること。	消防用設備等検査済証、定期点検検査報告書、建築図面（防火区画が記されているもの）を閲覧し消化装置が設置され、防火区画内に設置されていることを確認する。					
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。	(1)アーカイブデータ、バックアップデータを含む記録媒体は、例えばスマートカード、生体認証、入退室管理簿等により適切な入退室管理が行われた室内の施錠可能な保管庫に保管すること。 (2)記録媒体の搬入出時には、例えば搬入出者、日時等の記録を残し管理することを事務取扱要領等に明確かつ適切に規定する等の措置を講じていること。	CPS、事務取扱要領書、入退室の記録等を閲覧および現地を観察し、記録媒体が適切な入退室管理が行われた室内の施錠可能な保管庫に保管されていること、および適切な搬入出管理が行われていることを確認する。					
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、所定の手続きに基づいて適切に廃棄処理を行う。	(1)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、廃棄の記録、機密度に応じた廃棄方法（溶解・裁断・上書きによる消去等）に係わる手続きを事務取扱要領等に明確かつ適切に規定し、必要な措置を講じていること。 (2)第3者の廃棄業者に廃棄を委託する場合は、委託業者との契約書に機密保持、個人情報保護及び廃棄報告の事項を入れること。	事務取扱要領、委託契約書を閲覧し、適切な廃棄処理および第三者との契約がなされていることを確認する。					
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。	(1)認証サービス等に係わるバックアップ媒体を認証設備室もしくは建築物以外に保管できる場合は、災害等による損傷を避けるため可能な限り分離して保管すること。また、災害発生時の復旧方法について事務取扱要領等で適切に規定し、必要な措置を講じていること。 (2)外部に保管する場合は、その記録媒体の管理に関して、認証設備と同等の管理を実施すること。委託業者に委託する場合は、適切な業者を選定し、契約書等で媒体の取り扱いについて厳格に規定すること。 (3)外部への保管が不可能な場合は、災害等による損傷を極力排除可能なように保管し、その保管方法及び災害発生時の復旧方法について、事務取扱要領等で適切に規定し、必要な措置を講じていること。	(1)(3)事務取扱要領書、委託契約書等を閲覧し、バックアップ媒体が災害等による損傷を避けるため可能な限り分離して保管され、認証設備と同等の管理を実施することされているか、外部への保管が不可能な場合は、災害等による損傷を極力排除可能なように保管されているか確認する。 また、事務取扱要領等を閲覧し、災害発生時の復旧方法について適切に規定し、必要な措置を講じていることを確認する。 (2)事務取扱要領書、委託契約書等を閲覧し、委託業者に委託する場合は、適切な業者を選定し、媒体の取り扱いについて厳格に規定されているか確認する。					
5.2	手続き的管理							
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。	認証業務に従事する者の責任及び権限、指揮命令系統に関して、特定の個人に業務が集中しないよう内部牽制を考慮した上で事務取扱要領等に明確かつ適切に規定し、実施していること。少なくとも「CAシステム管理者」、「登録局管理者」、及び「監査者」は兼任しないこと。	事務取扱要領、指揮命令系統の示された組織体制図を閲覧し、特定の個人に権限が集中していないことを確認する。					
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。	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。 例えば、 CAシステムの私有鍵の生成、管理者・利用者の私有鍵の生成（生成を行う場合）、CAの私有鍵の活性化、CAの機能に関連するソフトウエアの更新等の操作、および高度な安全管理区域への立ち入りが単独の操作者で行えないように必要な人数を定めていること。	CPS、事務取扱要領、指揮命令系統の示された組織体制図等を閲覧し、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
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。	(1)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、その任命方法が定められていること。 (2)システムへのアクセス時(システム機器への操作開始時またはシステム室への入退室等のアクセス時の少なくともいずれかにおいて)の本人確認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定めていること。 (入退出時のみにICカードを用いる場合は操作権限者のみが入退出可能な状態に設定されていること。 また、認証設備室外での登録局システム機器の操作時の本人確認にはICカ ード等のセキュリティデバイスを 採用すること。)	CPS、事務取扱要領書等を閲覧し、重要な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および、本人確認に当たっては操作や入退出等のどこか一箇所以上で本人しか持ち得ない権限者の私有鍵を用いた強固な認証方式を採用していることを確認する。 また、認証設備室外での登録局システム機器の操作時の本人確認にはICカ ード等のセキュリティデバイスを 採用していることを確認する。					
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。	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(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)の定めがなされ運用されていること。事務取扱要領には操作後の台帳管理やアクセスログによる監査証跡のチェックを含めること。	1)指揮命令系統の示された組織体制図、CPS、事務取扱要領、運用マニュアル、キーセレモニー記録等を閲覧し、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が採用されていることを確認する。 2)作業記録やログ等を閲覧し、複数人によるコントロールで運用していることを確認する。					
5.3	要員管理							
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を理解しているものを配置する。	1)認証局の業務運営に関して信頼される役割を担う者が認証局運営組織の採用基準に基づき採用された職員であることを定めていること。 2)およびCAシステムを直接操作するものはPKIの概要とシステムの操作方法を理解していることを確認してから配置することを定めていること。	CPS、事務取扱要領、組織の採用基準を定めた内規等を閲覧、または、直接面接し質問する等して、認証局の業務運営に関して信頼される役割を担う者がそれらの基準に従って採用され配置されていることを確認する。					
5.3.2	経歴の調査手順 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。	信頼される役割を担う者の決定に際して、対象者の履歴、技能、適格性に関する基準を定めていること。	CPS、事務取扱要領、組織の採用基準を定めた内規等を閲覧し、対象者の履歴、技能、適格性に関する基準を定めてあることを確認する。					
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。	信頼される役割を担う者に対しての業務に必要な教育の基準を定め、また就業開始時およびその後の必要時および定期的な教育実施に関する規定を定めていること。	CPS、事務取扱要領等を閲覧し、業務に必要な教育基準および定期的な教育訓練実施に関する規定を定めていることを確認する。					
5.3.4	再研修の頻度及び要件 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ことを確認する。					
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。	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ことを確認する。					
5.3.6	認められていない行動に対する制裁 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ことを確認する。					
5.3.7	独立した契約者の要件 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
5.3.8	要員へ提供する資料 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ことを確認する。					
5.4	監査ログの取扱い							
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できる。	認証局のイベントログを自動または手動で取得できること。例えば、以下のようなログを取得できること。 ●利用者情報の初期化、証明書のおよび私有鍵の生成、活性化、非活性化、更新、修復、削除等に関する操作 ●CA操作者のパスワード、私有鍵および公開鍵の作成、変更、削除、更新、およびCA操作者としてのログインに関する操作 ●リポジトリを用いている場合はリポジトリへの利用者のアクセスが不成功な場合、およびCAによるリポジトリ書き込みおよび読み取り操作 ●CRL操作に関する記録、セキュリティポリシの変更や評価、CAアプリケーションの起動・終了、データベースのバックアップ、クロス証明書や証明書チェインの確認、属性証明書に関する操作、利用者の更新、DNの変更、データベースやログの操作方法の変更、証明書の取り扱いの変更 ●鍵ペアの生成、格納、検索、活性化、非活性化、保存および破壊に関する操作	1)CPS、事務取扱要領を閲覧し、例示したような取得すべきログを規定してあることを確認する。 2)また、関連ソフトウエアの仕様書を閲覧し、実際に取得できる設計になっていること、およびログを閲覧し実際に取得していることを確認する。					
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。	監査ログは最低3ヶ月に一度検査することが定められ実施されていること。	1)CPS、事務取扱要領等を閲覧し、最低3ヶ月に一度以上検査することが定められていることを確認する。 2)また、運用開始後3ヶ月を経過している場合は、作業記録等を閲覧し、実際に検査していることを確認する。					
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。	監査ログは最低10年間保存することが定められていること。	CPS、事務取扱要領等を閲覧し、監査ログを10年保存することが定められているか確認する。					
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。	監査ログに関するアクセス規則が定められ、技術的もしくは運用的措置による権限管理により、それが保障されるような認証方法が定めれられていること。	CPS、事務取扱要領、関連ソフトウェアの仕様書等を閲覧し、監査ログに関するアクセス規則が定められていることを確認する。					
5.4.5	監査ログのバックアップ手順 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。	1)監査ログを定期的にオフラインの記録媒体にバックアップされることが頻度を明記して定められていること。 2)また媒体の保管場所について安全性の確保を含めて定められていること。	CPS、事務取扱要領等を閲覧し、オフライン記録媒体へのバックアップ頻度が明記されていることを確認する。また、当該媒体の保管場所について、不正な閲覧、改ざん、滅失、消去などの脅威に対する安全性が確保されていることを確認する。					
5.4.6	監査ログの収集システム(内部対外部) 規定しない。	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ことを確認する。					
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。	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ことを確認する。					
5.4.8	脆弱性評価 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ことを確認する。					
5.5	記録の保管							

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
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	認証局 は、少なくとも以下の情報をアーカイブすること。 ・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	CPS等関連規定を閲覧し、少なくともCPに定める情報をアーカイブしていることを確認する。					
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。	アーカイブする情報は、記録が作成されてから最低10年間は保存すること。	CPS等関連規定の閲覧および必要に応じ体制および設備を調査することにより、アーカイブする情報が、記録が作成されてから最低10年間は保存されることを確認する。					
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。	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、許可されたもの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、消去から保護されていること。	CPS等関連規定の閲覧および必要に応じ媒体が保管されている設備を調査することにより、アーカイブ情報の収められた媒体が物理的セキュリティによって保護され、許可されたもの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、消去から保護されていることを確認する。					
5.5.4	アーカイブのバックアップ手続 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。					
5.5.5	記録にタイムスタンプをつける要件 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。					
5.5.6	アーカイブ収集システム(内部対外部) 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。					
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。	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。					
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。	1) 認証局は、定期的にCA私有鍵の更新を行うこと。 2) 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こと。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と。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こと。	1) CPS等関連規定を閲覧し、CA私有鍵が定期的に更新されることを確認する。 2) CPS等関連資料およびキーセレモニー等の記録を閲覧し、必要に応じ体制および設備の調査あるいは、HSMの仕様・認証取得等を確認することにより、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CAの私有鍵が生成され、自己証明書が更新されることを確認する。					
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	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・訓練を実施していること。 ・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	CPS等関連規定を閲覧し、CPに上げる脅威に対するする復旧手続を規定しているか確認する。教育履歴簿等および訓練履歴簿等を閲覧し、関係する認証局員全員に適切な教育・訓練を実施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
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、検証者に情報公開用Webサイト等により通知する。	1) 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うことが規定され、実施体制および設備が整備されていること。 2) また、こうした認証局業務を再開するまでの平均的な目標期間が合理的期間内であらかじめ設定されていること。 3) 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ことが規定され、実施体制および設備が整備されていること。	CPS等関連規定を閲覧すること並びに必要に応じて体制図を閲覧すること及び設備を検査することにより、復旧作業が合理的な時間で速やかに行われること及び障害発生時に加入者、検証者に情報公開用Webサイト等により通知されることを確認する。					
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。	1) CA私有鍵が危殆化又は危殆化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ための体制が確立されていること。 2) さらに、全ての加入者証明書の失効を行い、CRL/ARLを開示し、CA私有鍵を廃棄するための手順および体制が規定され、実施体制及び設備が整備されていること。 3) 更に、原因の追求と再発防止策を講じるための実現可能な手順および体制が規定されていること。 4)危殆化の原因追求のために、認証局業務従事者以外の者が調査する体制をとること。	1) CPS等関連規定を閲覧することにより CA私有鍵が危殆化又は危殆化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ための体制が確立されていることを確認する。 2) さらに、CPS等関連規定を閲覧すること及び必要に応じて設備を検査することにより、全ての加入者証明書の失効を行い、CRL/ARLを開示し、CA私有鍵を廃棄するための手順および体制が規定され、実施体制及び設備が整備されていることを確認する。 3) 4)更に、CPS等関連規定を閲覧し、原因の追求と再発防止策を講じるための実現可能な手順および体制が規定されていることを確認する。					
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。	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、加入者及び検証者に速やかに情報を公開するための手続きが認証局で規定されていること。	CPS等関連規定を閲覧し、必要に応じ設備を検査することにより、通常の業務継続が困難な場合に、加入者及び検証者に速やかに情報を公開するための手続きが規定されていること、					
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。	1) 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方法を手配することが規定され、本規定に基づく体制が整備されていること。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が規定され、本規定に基づく体制が整備されていること。 2) 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ことが規定され、本規定に係る体制が整備されていること。	1) CPS等関連規定 および外部に委託している場合は必要に応じ契約書を閲覧することにより、認証局が運営を停止する場合は、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方法を手配すること及び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が規定され、本規定に基づく体制が整備されていることを確認する。 2) CPS等関連規定および外部に委託している場合は必要に応じ契約書を閲覧することにより、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ことが規定され、本規定に係る体制が整備されていることを確認する。					
6	技術的なセキュリティ管理							
6.1	鍵ペアの生成と実装							

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
6.1.1	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。	(1)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)を用いて適切に生成されていること。 例えば 1) 鍵ペアは、FIPS 140-2の適切なセキュリティレベルの要件(CA私有鍵の場合レベル3と同等以上)を満たす安全な暗号モジュールの中で生成されていること。 2) 鍵ペアの生成に使用される乱数発生器は、FIPS 140-2の適切なセキュリティレベル相当を満たしていること。 3) 鍵ペアの生成に使用される素数発生器は、FIPS 140-2の適切なセキュリティレベル相当を満たしていること。 4) 鍵ペアの生成には、ANSI X9又はISOの標準で規定されている鍵アルゴリズム(例えば、RSA署名つきのSHA1)が使われていること。 (2) 鍵ペアの生成には、複数の立会いのもと、権限付与された者により適切に生成されていること。 例えば 1)権限付与された者による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)により生成されていること。 2) 鍵生成に使われるハードウェア又はソフトウェアのインテグリティ及びハードウェアとソフトウェアのインタフェースが使用前にテストされていること。 3) CAの鍵ペアは、その認証局のPAA(ポリシ承認局)がCPS(認証局運用規定)等を承認した後に、生成されていること。	(1)HSMメーカが取得している認定書等、CPS、運用マニュアル、PKIソフトウェア概要書などを閲覧し、CA鍵ペアが、認証設備室内に設置された専用の暗号モジュール(HSM)を用いて適切に生成されていることを確認する。 (2)CPS、運用マニュアル、組織図、認証局構築スケジュール、議事録、作業記録(作業申請書・指示書・報告書等)などを閲覧し、鍵ペアの生成は、複数の立会いのもと、権限付与された者により適切に生成されていることを確認する。					
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。	(1) CA(又はRA)によって生成された私有鍵を加入者に送付するときは、次のいずれかの方法よって、送付が安全に行われていること。 IETF RFC 2510「証明書管理プロトコル」に準拠した方法で伝送するか、 同様に安全な方法、例えば a. 適切な身元確認を行い、対面で手渡す。 b. 秘密鍵を含むトークンを不正開封防止機能を使用した郵便で送る。 c. SSLセッションの中で伝送する。 (2) CAが加入者の代わりに鍵ペアを生成したとき、その鍵ペアが加入者に引き渡されたなら、CAは、いかなる私有鍵のコピーも保持していないこと。	(1) CPS、運用マニュアル、RAマニュアルを閲覧し、生成された私有鍵を安全に加入者に送付していることを確認する。 (2)CPS、CAシステム概要書、PKIシステム概要書、運用マニュアルなどを閲覧し、鍵ペアが加入者に引き渡された後、CAは、いかなる私有鍵のコピーも保持していないことを確認する。					
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。	加入者によって生成された公開鍵を認証局に送付するときは、次のいずれかの方法によって、送付が安全に行われていること。 IETF RFC 2510「証明書管理プロトコル」に準拠した方法で伝送するか、 同様に安全な方法、例えば a. 適切な身元確認を行い、対面で手渡す。 b. 秘密鍵を含むトークンを不正開封防止機能を使用した郵便で送る。 c. SSLセッションの中で伝送する。B123	CPS、運用マニュアル、RAマニュアルを閲覧し、加入者によって生成された公開鍵が認証局に安全に送付されていることを確認する。					
6.1.4	検証者へのCA公開鍵の送付 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。	(1) CAの公開鍵は、検証者によるダウンロードを可能とするため、本CPとともに、CAのWebサイトで公開されていること。 (2) CAの公開鍵は、定期的に交換(又は再生成)されている、又はされることになっていること。	(1) CPSおよびWebサイトを閲覧し、CAの公開鍵が、検証者によるダウンロードを可能とするため、本CPとともに、CAのWebサイトで公開されていることを確認する。 (2) CPS、運用マニュアルなどを閲覧し、CAの公開鍵が、定期的に交換(又は再生成)されることに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
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。	(1) RSAアルゴリズムを使用する場合、CAの鍵サイズは、2,046ビット以上となっていること。 (2) RSA以外のアルゴリズム使用する場合、CAの鍵サイズは、前項と同等以上のセキュリティ強度となる鍵サイズを使用していること。 (3) RSAアルゴリズムを使用する場合、加入者の鍵サイズは、1,024ビット以上となっていること。 (4) RSA以外のアルゴリズム使用する場合、加入者の鍵サイズは、前項と同等以上のセキュリティ強度となる鍵サイズを使用していること。	(1)(2)(3)(4) CPS、CAシステム概要書、PKIソフトウェア概要書などを閲覧し、CAの鍵サイズおよび加入者の鍵サイズが指定の値になっていることを確認する。					
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。	(1) 公開鍵パラメータは、FIPS 140-2の適切なセキュリティレベルの要件相当を満たす暗号モジュールの中で生成されていること。 (2) 公開鍵パラメータの品質検査が、FIPS 140-2の適切なセキュリティレベルの要件相当を満たす暗号モジュールの中で行われていること。	(1)(2) メーカが取得している認定書、CPS等を閲覧し、公開鍵パラメータ生成および品質管理が信頼できる暗号モジュールで行われていることを確認する。					
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。	(1) 鍵ペアは、個人、国家資格所有者、医療機関等の管理者などに発行された証明書が、本人と公開鍵が一意に関連することを証明する単一の目的（署名と検証）のためにのみ利用されていること。 (2) CAの鍵は、keyCertSignとcRLSignのビットを使用していること。 (3) 加入者の鍵は、nonRepudiationのビットを使用していること。	(1)(2)(3) CP、CPSを閲覧し、KeyusageがCPの指定どおりになっていることを確認する。					
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。	(1) CA私有鍵を格納する暗号モジュールは、FIPS 140-2のセキュリティレベル3と同等以上の規格に準拠していること。 (2) 加入者私有鍵を格納する暗号モジュールは、FIPS 140-2のセキュリティレベル1と同等以上の規格に準拠していること。	(1)(2) メーカが取得している認定書、CPS等を閲覧し、私有鍵を格納する暗号モジュールがCA私有鍵の場合はFIPS 140-2のセキュリティレベル3および加入者私有鍵の場合はFIPS 140-2のセキュリティレベル1と同等以上の規格に準拠していることを確認する。					
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。	CA私有鍵の取り扱い（生成、活性化、非活性化、バックアップ、リカバリ、格納、搬送、破棄など）は、物理的に安全な環境で運用管理者と複数人の権限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）によって私有鍵の管理が行われていること。	CPS、運用マニュアル、操作マニュアル、業務記録等を閲覧し、物理的に安全な環境で運用管理者と権限付与された複数人によるコントロールによって私有鍵の管理が行われていることを確認する。					
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。	(1) CA私有鍵は、法律によって必要とされる場合を除き、第三者に預託されていないこと。 (2) CA私有鍵が第三者に預託されている場合、当事者間の賠償責任と救済手段を規定した契約が存在すること。 (3) CA私有鍵が第三者に預託されている場合、預託されたCA私有鍵のコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていること。 (4) 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、第三者に預託されていないこと。	(1) (4)CPSを閲覧し、CA私有鍵および加入者の私有鍵が、法律によって必要とされる場合を除き、第三者に預託されていないこととなっていることを確認する。 (2)CPS、契約書を閲覧し、預託された場合、賠償責任と救済手段を規定した契約が存在することを確認する。 (3)CPS、契約書を閲覧し、預託された場合、預託されたCA私有鍵のコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従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
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。	(1) CA私有鍵が暗号モジュールからエクスポートされて、バックアップのために安全なストレージに移転される場合、権限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、次のいずれかを含む安全な鍵管理スキームでCA私有鍵をエクスポートしていること。 a. CA私有鍵の関する情報を暗号文として b. CA私有鍵の関する情報又は所有を分散し、暗号化されたフラグメントとして c. 鍵転送デバイスのような別の安全な暗号モジュールの中で (2) CA私有鍵のバックアップコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていること。 (3) CA私有鍵のリカバリは、権限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、バックアッププロセスと同じスキームで実施されていること。	(1)(3) CPS、CAシステム概要書、PKIソフトウェア概要書、運用マニュアルなどを閲覧し、権限付与された複数人によるコントロールでCA私有鍵をエクスポートおよびリカバリーされることを確認する。 (2) CPS、運用マニュアルを閲覧し、CA私有鍵のバックアップコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていることを確認する。					
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。	CAは、加入者の私有鍵をアーカイブしないポリシに準拠している。	CPSを閲覧し、加入者の私有鍵をアーカイブしないポリシに準拠していることを確認する。					
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。	1）CA私有鍵は、安全に格納すること。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こと。 2）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こと。	CPS、CAシステム概要書、PKIソフトウェア概要書、運用マニュアルなどを閲覧し、CA私有鍵が安全に格納されていること、また、外部へのバックアップや外部からのリストアの場合、セキュアチャネルを通じて行っていることを確認する。					
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。	鍵ペアは、それが使用されるのと同じ暗号モジュールの中で生成されている、又は、それが生成された暗号モジュールから使用されるデバイスへ次のような方法によって、直接投入されていること。 a. IETF RFC 2510「証明書管理プロトコル」 又は同様に安全な方法、例えば b. 2Key-3DESで転送した後、デバイス内で安全に復号	CPS、HSM概要書、運用マニュアル、CAシステム概要書、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、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、私有鍵が加入者の暗号モジュールに安全に入力されること確認する。					
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。	CA私有鍵の活性化は、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）によって行われていること。	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、CA私有鍵の活性化は、物理的に安全な場所認証局室内）で、権限を付与された複数人によるコントロールによって行われていることを確認する。					
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。	CA私有鍵の非活性化は、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）によって行われていること。	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、CA私有鍵の非活性化が、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によって行われていることを確認する。					