5　建物・関連設備、運用のセキュリティ管理

これらは、ISO 17799-1：2000 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

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、且つ建物構造上、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事。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。

認証設備室への立ち入りは、立ち入り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、立ち入り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、立ち入り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することや、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 手続き的管理

手続き的管理は、ISO 17799:2000 と同等以上の規格に従うものとする。例えば、ISO/IEC17799:2000 の「第 8 章 通信及び運用管理」がこれに相当する。

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事は避けること。

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さ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、登録局システムへのアクセス権限者は、認証局運営責任者により任命されるものとし、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証明書等により、本人しか持ち得ない強固な認証方式を採用する事。

5.2.4 職務分割が必要になる役割

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事。

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、ISO 17799-1:2000 と同等以上の規格に従うものとする。例えば、ISO/IEC17799:2000 の「第 6 章　人的セキュリティ」等がこれに相当する。

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、ISO 17799-1:2000 と同等以上の規格に従うものとする。例えば、ISO/IEC17799:2000 の「第 8 章　通信及び運用管理」、「第 9 章　アクセス制御」、「第 10 章　システムの開発及び保守」、「第 12 章　適合性」等がこれに相当する。

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 度以上の頻度で定期的に精査する。

5.4.3 監査ログを保存する期間

監査ログは、最低 2 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とられ、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、ISO 17799-1:2000 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、ISO/IEC17799:2000 の「第 10 章　システムの開発及び保守」、「第 12 章　適合性」等がこれに相当する。

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。

- 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。

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危殆化の恐れが生じた場合は、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、登録局の持ってい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。なお、登録局は、このような場合に他の登録局に加入者の情報や運営を他の登録局に移管することについて、事前に加入者の同意を得るものとする。

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 鍵の使用目的

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 複数人による私有鍵の管理

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 私有鍵の複数人コントロール」と同じく、複数人によって、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 私有鍵と公開鍵証明書の有効期間

CA 私有鍵の有効期間は 20 年を越えないものとし、その鍵の使用は 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私有鍵の有効期間は 5 年を越えないものとし、その鍵の使用は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

ISO 17799:2000「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。

6.6.2 セキュリティ運用管理

ISO 17799:2000「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。

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

ISO 17799:2000 と同等以上の規格に従うものとする。

例えば、ISO/IEC17799:2000 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。

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。