6. 技術的セキュリティ管理

6.1. 鍵ペアの生成及びインストール

6.1.1. 鍵ペアの生成

本認証局の鍵ペアの生成は鍵管理者立会いのもと、複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、FIPS140-1 レベル 3 の暗号化モジュールを使用して行われる。

契約／資源管理者証明書及び JPNIC 職員向け証明書の鍵ペアの生成は、FIPS140-2 レベル 3 の暗号化モジュールを使用して行われる。

6.1.2. 所有者に対する私有鍵の交付

契約／資源管理者証明書及び JPNIC 職員向け証明書の鍵ペアの生成は、本認証局において暗号化モジュール内で行われる。生成された鍵ペアは暗号化モジュールを含むハードウェアトークンを使って申請者に交付される。

本認証局は資源申請者証明書の鍵ペアの作成を行わないため、本項の規定を行わない。

6.1.3. 証明書発行者に対する公開鍵の交付

資源申請者証明書の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルを本認証局へ送付することで行われる。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の証明書の配布は、次の 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。

- JPNIC 認証局の Web ページにて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。証明書検証者は同ページより本認証局の証明書をダウンロードして使用することとする。証明書検証者はダウンロードした本認証局の証明書のフィンガープリントとインターネットを使わない方法で公開されてい

るフィンガープリントを比較し、一致していることを確認する。
- 資源申請者には契約／資源管理者が本認証局の証明書を渡すものとする。

6.1.5. 鍵サイズ

本認証局は 2048 ビットの RSA 鍵ペアを使用する。EE については、1024 ビット以上の RSA 鍵ペアを使用することを義務とする。

6.1.6. 公開鍵のパラメータの生成及び品質検査

本認証局の鍵ペアを生成するための公開鍵パラメータは、鍵ペア生成に使用される安全性の高い暗号化モジュールを含むソフトウェアに実装された乱数生成モジュール（以下、RNG という）を用いて生成される。

公開鍵パラメータの品質検査については、特に規定しない。

6.1.7. 鍵用途の目的

本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書及び CRL の発行にのみ使用する。

契約／資源管理者証明書、資源申請者証明書、JPNIC 職員向け証明書の keyUsage は digitalSignature、keyEncipherment、dataencipherment のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用するものとする。

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

規定しない。

6.2.2. 私有鍵の複数人管理

本認証局の私有鍵の管理は、複数の CAO に権限を付与することによって行う。2名以上の CAO が揃わなければ本認証局の私有鍵を操作することはできない。

6.2.3. 私有鍵のエスクロー

本 CPS「4.1.2.キーエスクローと鍵回復」に規定する。

6.2.4. 私有鍵のバックアップ

本認証局の私有鍵は、予め定める外部記憶媒体にバックアップされる。バックアップ作成時も鍵管理者の立会いと複数名の CAO を必要とする。

本認証局は、そのバックアップを予め定める保管場所に保管する。

なお、本認証局は、EE の私有鍵のバックアップを行わない。

6.2.5. 私有鍵のアーカイブ

本認証局の私有鍵のアーカイブは行わない。

EE の私有鍵についても同様にアーカイブは行わない。

6.2.6. 私有鍵の暗号モジュールへの又は暗号モジュールからの転送

本認証局の私有鍵は、安全性の高い暗号化モジュールを含むソフトウェアで生成され、他のハードウェア及びソフトウェア等が介入することはない。

6.2.7. 暗号モジュールへの私有鍵の格納

本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。

資源申請者の私有鍵は資源申請者自身が私有鍵の生成を行い、資源申請者自身で格納を行う。契約／資源管理者及び JPNIC 職員向けの秘密鍵は JPNIC において、安全性の高い暗号化モジュール内で生成、格納される。ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。

6.2.8. 私有鍵の活性化方法

本認証局の私有鍵の活性化は、認証設備室内において行われる。

EE の私有鍵に関しては、規定しない。

6.2.9. 私有鍵の非活性化方法

本認証局の私有鍵の非活性化は、認証設備室内において、操作をする者とその監視をする者とに分かれて行われる。

EE の私有鍵に関しては、規定しない。

6.2.10. 私有鍵の破棄方法

本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者によって、私有鍵の格納されたハードディスクを完全に初期化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によって破棄する。

EE の私有鍵は、EE 自身で確実に破棄するものとする。契約／資源管理者の秘密鍵は基本的に JPNIC において破棄するものとする。ただし、紛失等の場合はこの限りではない。

6.2.11. 暗号モジュールの評価

規定しない。

6.3. その他の鍵ペア管理

6.3.1. 公開鍵のアーカイブ

本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。

6.3.2. 証明書の運用上の期間及び鍵ペアの使用期間

本認証局の証明書の有効期間は 10 年、私有鍵の有効期間は 8 年とする。本認証局は私有鍵の有効期限前に鍵ペアの更新を行う。

EE 証明書の有効期間は 2 年とする。私有鍵は復号を行う場合においてのみ、2 年を超える使用を認めるものとする。

6.4. 活性化データ

6.4.1. 活性化データの生成及び設定

本認証局の私有鍵に対するものを含め、本認証局で使用される PIN やパスワードは、英大文字、英小文字、数字を全て含む 8 文字以上の長さのものとする。

6.4.2. 活性化データの保護

本認証局で使用される PIN やパスワードについては、封印されたうえで運用管理者による管理のもと保管される。

6.4.3. 活性化データの他の考慮点

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

本認証局のサーバシステムに関わる業務は、原則として複数人の CAO によって行われる。ただし、ハードウェア障害時等に発生する専門的な知識を必要とする作業については、CAO の立会いのもとで保守員によって行うものとする。システムに対して行われた重要な操作については、全てログが残るよう設定する。システムにアクセスするための全てのパスワードについては、適切な管理を行う。本認証局のサーバシステムについては、常時リソース監視を行い、システムの異常や不正運用を検知した場合には、速やかに適切な対策を実施する。

6.5.2. コンピュータセキュリティ評価

本認証局は使用する全てのソフトウェア、ハードウェアに対して事前に運用テストを行い、信頼性の確認を行う。

6.6. ライフサイクルの技術上の管理

6.6.1. システム開発管理

システムの品質及びセキュリティを保つために、開発時における各工程の管理、導入前の評価等を実施する。

6.6.2. セキュリティ運用管理

システムのセキュリティ管理として、入退室管理、教育を含む要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のシステム的なセキュリティ対策、セキュリティ対策ソフトウェアの適時更新等を実施する。

6.6.3. ライフサイクルのセキュリティ管理

規定された管理方法により、システムが管理されているかの評価を行う。

本認証局のシステムに対して、セキュリティに関する情報収集を行い、最新の動向を考慮し、適切な評価及び改善を行う。

6.7. ネットワークセキュリティ管理

本認証局の存在するネットワークにはファイアウォールを使用し、ファイアウォール外からのアクセスについては必要最低限のプロトコルに制限する。またアクセス可能なホストも限定する。

6.8. タイムスタンプ

タイムスタンプの使用に関する要件は、本 CPS「5.5.5.記録にタイムスタンプを付ける要件」に規定する。