5. 設備上、運営上、運用上の管理

5.1. 物理的管理

5.1.1. 立地場所及び構造

本認証局に係わる重要な設備については、火災、水害、地震、落雷その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。

また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5.1.2. 物理的アクセス

本認証局は、認証設備室に関して、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理を行う。本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。

5.1.3. 電源及び空調

本認証局は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電及び電圧・周波数の変動に備えた対策を講ずる。また空調設備に関して、各種使用する機器類に悪影響を与えないよう維持管理を行う。

5.1.4. 水害及び地震対策

本認証局の設備を設置する室は防水対策を施し､浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。

5.1.5. 火災防止及び火災保護対策

本認証局は、設備を防火壁によって区画された防火区画内に設置する。また防火区画内では電源設備や空調設備の防火措置を講じ、火災報知器及び消火設備の設置を行う。

5.1.6. 媒体保管場所

アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、本認証局の設置場所とは別の適切な入退管理が行われた室内の保管庫に保管される。

5.1.7. 廃棄処理

本認証局は、機密扱いとする情報を含む書類・記録媒体について、情報の初期化・裁断等、事前に定められた方法に従い適切に廃棄処理を行う。

5.1.8. 施設外のバックアップ

規定しない。

5.2. 手続的管理

5.2.1. 信頼される役割

証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担う。

5.2.2. 職務ごとに必要とされる人員

認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。

5.2.3. 個々の役割に対する本人性確認と認証

認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。

5.2.4. 職務分割が必要となる役割

権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。

5.3. 人事的管理

5.3.1. 資格、経験及び身分証明の要件

JPNIC は、職員に認証局の役割を任命する際及びその後定期的に、適切な人物審査を実施のうえ、任命を行う。任命の際には守秘義務契約を結び、情報の適切な管理を行う。また日常業務においては、メンタルヘルス、健康管理及び適正な処遇等による継続した人事管理を行う。

5.3.2. 人員配属に関する規定事項

認証局業務に関わる要員を任命するにあたって、業務の遂行上支障が出ない適切な人員を配置する。配属されるものは機密保持及び内部規定の遵守に対する誓約書を提出する。

5.3.3. 研修要件

運用要員の教育を次のように行う。

- 運用要員が役割に就く前に、認証局の運用に必要な教育を実施する。
- 役割に応じた教育・訓練計画を策定し、計画に沿って定期的に教育・訓練を実施する。
- 業務手順に変更がある場合は遅滞なく事務取扱要領の必要箇所を変更し、その変更に関わる教育・訓練を実施する。

5.3.4. 再研修の頻度及び要件

JPNIC は定期的に本認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。

5.3.5. 仕事のローテーションの頻度及び順序

規定しない。

5.3.6. 認められていない行動に対する処罰

JPNICは、本認証局の運用要員による認可されていない行為に対し、予め決められた規程に従って処罰する。

5.3.7. 独立した契約者の要件

JPNIC は、委託契約において委託業務の内容を明確にするとともに、受託者に対して JPNIC の指示の遵守、責任分担、保証、違反時の罰則等について明確にし、かつ受託者と守秘義務契約を結ぶ。また委託後は受託者の業務が適切に行われていることを監督し管理する。

5.3.8. 要員へ提供される資料

運用に必要な文書を運用要員に開示し周知する。

5.4. 監査ログの手続

5.4.1. 記録されるイベントの種類

本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。

認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。

- 認証局の私有鍵の操作に関する記録
- 証明書の発行及び失効等の作業に関する記録
- 失効情報の作成作業に関する記録
- 監査ログの確認に関する記録

また、認証局設備へのアクセスに関する履歴を記録する。

5.4.2. 監査ログを処理する頻度

本認証局は、監査ログ及び関連する記録を定期的に精査する。

5.4.3. 監査ログを保持する期間

監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に一定期間保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。

5.4.4. 監査ログの保護

本認証局は、JPNIC によって認可された人員のみが監査ログファイルにアクセスすることができるようにするために権限者を定め、許可されていない者が閲覧、修正又は削除をすることから保護する。また定期的に監査ログのバックアップを外部記憶媒体に取得し、適切な入退室管理が行われている室内において、施錠可能な保管庫に保管する。

5.4.5. 監査ログのバックアップ手続

監査ログは、認証局システムのデータベースとともに、事前に定められた手続に従

い、外部記憶媒体に定期的にバックアップがとられ、それらの媒体は安全な施設に保管される。

5.4.6. 監査ログの収集システム

監査ログの収集機能は認証局システムの一機能として内在しているものとし、セキュリティに関する重要なイベントを監査ログとして収集する。

5.4.7. イベントを起こしたサブジェクトへの通知

本認証局では、監査ログの収集を、イベントを発生させた人、システム又はアプリケーションに対して通知することなく行う。

5.4.8. 脆弱性評価

認証業務において用いるハードウェア及びソフトウェアは、監査ログ検査等によるシステム面及び運用面におけるセキュリティ上の脆弱性評価に加え、最新の実装可能なセキュリティ・テクノロジの導入等、セキュリティ対策の向上を図るものとする。

5.5. 記録の保管

5.5.1. アーカイブ記録の種類

本 CPS「5.4.1.記録されるイベントの種類」に規定する監査ログに加えて、本認証局は次の記録を保存する。

【認証局システムに記録されるイベント】

- 本認証局の署名用鍵ペアの生成
- システムからの証明書所有者の追加及び削除
- 証明書の発行・失効を含めた鍵の変更
- 登録局管理者権限の追加、変更及び削除

【紙媒体又は外部記憶媒体として保存するもの】

本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。

- 本 CPS、証明書所有者同意書及びその変更に関する記録
- 認証業務に従事する者の責任及び権限に関して記載した文書及びその変更に関する記録
- 認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本
- 監査の実施結果に関する記録及び監査報告書

5.5.2. アーカイブ保持期間

本認証局は、認証局システムのデータベースの履歴及び監査ログファイルの履歴を一定期間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本 CPS「5.5.1.アーカイブ記録の種類」に規定する。

5.5.3. アーカイブ保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。本認証局は、アーカイブデータのバックアップを定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した者以外の者がアクセスできないように制限し、温度、湿度等の環境上の脅威から保護された施設に保管する。

5.5.4. アーカイブのバックアップ手続

本認証局は、認証局システムのデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、監査ログも定期的に外部記憶媒体に格納する。

5.5.5. 記録にタイムスタンプを付ける要件

本認証局は、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。ここでいうタイムスタンプとは暗号技術を用いたものではない。

5.5.6. アーカイブ収集システム

認証局サーバデータベース用の履歴収集システムは、認証局サーバシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CPS「5.4.6.監査ログの収集システム」に規定する。

5.5.7. アーカイブの情報を入手し、検証する手続

アーカイブデータは、厳格に管理された区画からアクセス権限者が入手し、外部記録媒体の可読性確認を定期的に行う。また必要に応じ、アーカイブデータの完全性及び機密性の維持に留意し、新しい媒体へ複製を行うとともに、保管期間の過ぎた古い媒体は破棄する。

5.6. 鍵の切替

本認証局の私有鍵は、その有効期間の残りが EE 証明書の最大有効期間よりも短くなる前に、JPNIC はその鍵による新たな EE 証明書の発行を中止し、新たな認証局鍵ペアを本 CPS「6.1. 鍵ペアの生成及びインストール」に定める方法で生成する。新たな公開鍵は JPNIC ルート認証局から証明書の発行を受け、本 CPS「6.1.4.検証者に対する認証局の公開鍵の交付」に定めた方法と同様に配布を行う。

5.7. 危殆化及び災害からの復旧

5.7.1. 事故及び危殆化の取扱手続

認証局私有鍵の危殆化又は危殆化のおそれがある場合、及び災害等により認証業務の中断又は停止につながるような問題が発生した場合、本認証局は予め定められた計画及び手順に従い、認証業務の再開に努める。

5.7.2. コンピュータの資源、ソフトウェア及び/又は、データが破損した場合

JPNIC 認証局は、ハードウェア、ソフトウェア又はデータが破壊された場合、事前に定められた復旧計画に従い、バックアップ用のハードウェア、ソフトウェア及びデータにより、速やかに復旧作業に努める。

5.7.3. エンティティの私有鍵が危殆化した場合の手続

認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。

- 契約／資源管理者証明書、資源申請者証明書、JPNIC 職員向け証明書の失効手続
- 認証局私有鍵の廃棄及び再生成手続
- 契約／資源管理者証明書、資源申請者、JPNIC 職員向け証明書証明書等の再発行手続

また、証明書所有者の私有鍵が危殆化した場合は、本 CPS「4.9.証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。

5.7.4. 災害後の事業継続能力

災害等により JPNIC 認証局の設備が被害を受けた場合は、JPNIC は予備機を確保しバックアップデータを用いて運用の再開に努める。

5.8. 認証局又は登録局の終了

JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ及びアーカイブデータ等の保管組織

及び開示方法を業務終了 14 日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。