

Appendix 1
IP アドレス認証局
認証業務規定 (CP/CPS)
ドラフト版

<添付資料 1 について >

- この資料は、IP アドレス認証局の認証業務規定 (CP/CPS) のドラフト版である。本 CP/CPS 策定の為の検討については本報告書第 5 章で述べる。
 - 本 CP/CPS は RFC3647 のフレームワークに則って記述されている。
 - URL などを含め、公開が行われる前に一部改定されることが想定されている。

目次

| | |
|-------------------------------|----|
| 1. はじめに..... | 1 |
| 1.1. 概要..... | 1 |
| 1.2. 文書の名前と識別..... | 2 |
| 1.3. PKI の関係者..... | 2 |
| 1.4. 証明書の使用方法..... | 4 |
| 1.5. ポリシ管理..... | 5 |
| 1.6. 定義と略語..... | 5 |
| 2. 公開とリポジトリの責任..... | 7 |
| 2.1. リポジトリ..... | 7 |
| 2.2. 証明情報の公開..... | 7 |
| 2.3. 公開の時期又は頻度..... | 8 |
| 2.4. リポジトリへのアクセス管理..... | 8 |
| 3. 識別及び認証..... | 9 |
| 3.1. 名前決定..... | 9 |
| 3.2. 初回の本人性確認..... | 9 |
| 3.3. 鍵更新申請時の本人性確認と認証..... | 11 |
| 3.4. 失効申請時の本人性確認と認証..... | 11 |
| 4. 証明書のライフサイクルに対する運用上の要件..... | 12 |
| 4.1. 証明書申請..... | 12 |
| 4.2. 証明書申請手続..... | 12 |
| 4.3. 証明書発行..... | 13 |
| 4.4. 証明書の受領確認..... | 14 |
| 4.5. 鍵ペアと証明書の用途..... | 14 |
| 4.6. 証明書の更新..... | 15 |
| 4.7. 証明書の鍵更新..... | 15 |
| 4.8. 証明書の変更..... | 16 |
| 4.9. 証明書の失効と一時停止..... | 17 |
| 4.10. 証明書のステータス確認サービス..... | 20 |
| 4.11. 登録の終了..... | 21 |
| 4.12. キーエスクローと鍵回復..... | 21 |
| 5. 設備上、運営上、運用上の管理..... | 22 |
| 5.1. 物理的管理..... | 22 |
| 5.2. 手続的管理..... | 23 |
| 5.3. 人事的管理..... | 25 |
| 5.4. 監査ログの手続..... | 27 |
| 5.5. 記録の保管..... | 29 |
| 5.6. 鍵の切替..... | 30 |
| 5.7. 危殆化及び災害からの復旧..... | 31 |
| 5.8. 認証局又は登録局の終了..... | 32 |
| 6. 技術的セキュリティ管理..... | 33 |
| 6.1. 鍵ペアの生成及びインストール..... | 33 |

| | |
|-------------------------------|----|
| 6.2. 私有鍵の保護及び暗号モジュール技術の管理 | 34 |
| 6.3. その他の鍵ペア管理 | 36 |
| 6.4. 活性化データ | 36 |
| 6.5. コンピュータのセキュリティ管理 | 37 |
| 6.6. ライフサイクルの技術上の管理 | 37 |
| 6.7. ネットワークセキュリティ管理 | 38 |
| 6.8. タイムスタンプ | 38 |
| 7. 証明書と、証明書失効リスト及びOCSPのプロファイル | 39 |
| 7.1. 証明書のプロファイル | 39 |
| 7.2. 証明書失効リストのプロファイル | 43 |
| 7.3. OCSP プロファイル | 44 |
| 8. 準拠性監査とその他の評価 | 45 |
| 8.1. 評価の頻度又は評価が行われる場合 | 45 |
| 8.2. 評価人の身元又は資格 | 45 |
| 8.3. 評価人と評価されるエンティティとの関係 | 45 |
| 8.4. 評価で扱われる事項 | 45 |
| 8.5. 不備の結果としてとられる処置 | 46 |
| 8.6. 評価結果の情報交換 | 46 |
| 9. 他の業務上の問題及び法的問題 | 47 |
| 9.1. 料金 | 47 |
| 9.2. 財務的責任 | 47 |
| 9.3. 情報の秘密性 | 47 |
| 9.4. 個人情報のプライバシー保護 | 48 |
| 9.5. 知的財産権 | 49 |
| 9.6. 表明保証 | 49 |
| 9.7. 保証の制限 | 51 |
| 9.8. 責任の制限 | 51 |
| 9.9. 補償 | 51 |
| 9.10. 有効期間と終了 | 52 |
| 9.11. 関係者間の個別通知と連絡 | 52 |
| 9.12. 改訂 | 52 |
| 9.13. 紛争解決手続 | 53 |
| 9.14. 準拠法 | 53 |
| 9.15. 適用法の遵守 | 53 |
| 9.16. 雑則 | 53 |

1. はじめに

1.1. 概要

本 CP/CPS は、社団法人 日本ネットワークインフォメーションセンター（以下、JPNIC と呼ぶ）と IP アドレス管理指定事業者等との間における、IP アドレス及び AS 番号に関する各種管理業務に用いる証明書を発行する JPNIC IP アドレス認証局（以下、本認証局と呼ぶ）の認証業務に関する運用規則を定める。

本認証局は、本 CP/CPS に基づき、IP アドレス管理指定事業者に所属し、各種申請処理業務を行う者（以下、ホストマスタと呼ぶ）等に証明書を発行する等の認証サービスを提供する。また、安全な通信を実現するため、レジストリシステムの各種サーバに対してサーバ証明書を発行する。

本 CP/CPS の構成は、IETF PKIX が提唱する RFC3647「証明書ポリシーと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework）」に準拠している。

本認証局は、CP（証明書ポリシー）及び CPS（認証実施規程）をそれぞれ独立したものとせず、本 CP/CPS として証明書ポリシー及び運用規程を定めるものとする。

JPNIC は、認証業務の提供にあたり、自らのポリシー、証明書所有者及び証明書検証者の義務等を、本 CP/CPS、証明書所有者同意書によって包括的に定める。なお、本 CP/CPS と証明書所有者同意書の内容に齟齬がある場合は、証明書所有者同意書が優先して適用されるものとする。

本 CP/CPS は、証明書所有者及び証明書検証者がいつでも閲覧できるように JPNIC のホームページ上（URI は決定後に記述される）に公開する。

(1)CP/CPS

CP/CPS は、証明書の目的、適用範囲、証明書プロファイル、本人認証方法及び証明書所有者の鍵管理並びに認証業務に関わる一般的な規定を記述した文書である。本 CP/CPS は、必要に応じて証明書所有者同意書を参照する。

(2)証明書所有者同意書

証明書所有者同意書は、認証サービスの内容や証明書所有者の義務等、証明書所有者と JPNIC 間における、認証サービス利用上の諸規則を記述した文書である。

1.2. 文書の名前と識別

本 CP/CPS の正式名称は「JPNIC IP アドレス認証局 認証業務規程」という。

JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。

表 1-1 JPNIC 及び JPNIC IP アドレス認証局に関連するオブジェクト識別子

| オブジェクト | オブジェクト識別子 |
|----------------------------------|--|
| 社団法人 日本ネットワークインフォメーションセンター | 1.2.392.00200175 |
| JPNIC IP アドレス認証局 認証業務規程 (CP/CPS) | 1.2.392.00200175.2 (OID は決定後に記述される) |
| EE 証明書ポリシー | 1.2.392.00200175.2 (OID は決定後に記述される) |

1.3. PKI の関係者

1.3.1. 認証局、登録局、所有者及び検証者

本認証局が発行する証明書の流通するコミュニティの PKI 関係者には、表 1-2 に示す登場者が含まれる。

表 1-2 コミュニティに関する登場者と役割

| 登場者 | 略称 | 役割、説明 |
|--------------|--------|---|
| ホストマスタ | | IP アドレス及び AS 番号の割当て・返却等のレジストリ業務を行う者 |
| サーバ | | レジストリ業務に用いる JPNIC 内のサーバのうち、証明書が発行されるもの |
| ホストマスタ証明書 | | ホストマスタに対して発行される証明書 |
| サーバ証明書 | | JPNIC の各種サーバに対して発行される証明書 |
| LRA 管理者証明書 | | 本認証局の認証業務に必要な運用用証明書の一つ。ホストマスタへの証明書発行時の LRA 管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。 |
| エンドエンティティ | EE | 証明書の発行対象である、ホストマスタ及び各種サーバの総称 |
| エンドエンティティ証明書 | EE 証明書 | ホストマスタ証明書及びサーバ証明書の総称 |

| 登場者 | 略称 | 役割、説明 |
|------------------|----------|---|
| 証明書申請者 | 申請者 | EE 証明書を申請中の者 |
| 証明書所有者 | 所有者 | 証明書発行申請を行い、自ら鍵を生成し、認証局により証明書を発行される主体をあらわす。本 CP/CPS では、EE 証明書を所有している者又はサーバの管理者となる。 |
| 証明書検証者 | 検証者 | 証明書を受け取る者で、その証明書を用いて検証することにより、その証明書及び/又はデジタル署名に依拠して行動する者 |
| JPNIC 発行局 | JPNIC IA | JPNIC ルート認証局内の発行局及び JPNIC IP アドレス認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC IP アドレス認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。 認証局 (CA) の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。 |
| JPNIC 登録局 | JPNIC RA | 証明書発行の証明書申請者の本人を確認し、主として登録業務・失効業務をつかさどる組織。証明書の所有者の本人確認と認証に責任を持っている。 |
| 運営委員会 | | JPNIC の理事により構成される会議であり、JPNIC 認証局の運営方針の決定等を行う。運営委員会は、JPNIC の定款・規程に従って運営される。 |
| 認証局管理者 | CAO | 認証局サーバ、ディレクトリサーバ等認証局システムの運用管理をする者。 |
| 登録局管理者 | RAO | 登録局 (RA) を管理し運営する者。証明書発行、失効の登録作業を行う。 |
| リポジトリ | | 認証局が署名した証明書及び CRL 等を格納し公表するデータベース。 |
| JPNIC ルート認証局 | | JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局 (IP アドレス認証局) の証明書に電子署名を行う。 |
| JPNIC IP アドレス認証局 | | JPNIC が運営を行う IP アドレスの管理業務に関連する証明書の発行を行う認証局。JPNIC IP アドレス認証局証明書は、JPNIC ルート認証局により電子署名される。 |

| 登場者 | 略称 | 役割、説明 |
|------------|---------|---|
| JPNIC 認証局 | | JPNIC が運営を行う認証局の総称。JPNIC ルート認証局、JPNIC IP アドレス認証局、JPNIC 登録局及びリポジトリから構成される。 |
| ローカル登録局 | LRA | 証明書を発行する組織とは異なる組織若しくは団体であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が LRA となる。 |
| ローカル登録局責任者 | LRA 責任者 | IP アドレス管理指定事業者の中における、LRA 業務の責任者。LRA 管理者の任命・解任を行う。 |
| ローカル登録局管理者 | LRA 管理者 | IP アドレス管理指定事業者の中で、ホストマスタのメンバー管理と認証及びホストマスタ証明書の発行申請操作を行う。 |

1.4. 証明書の使用方法

1.4.1. 適切な証明書の使用

本 CP/CPS に基づき発行される証明書は、JPNIC の行う IP アドレス管理業務における各種の申請及び連絡等を目的として、レジストリシステムにおけるユーザ認証及びメッセージ認証のために使われるものとする。

1.4.2. 禁止される証明書の使用

本 CP/CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものであり、電子商取引での利用に意図されているものでも、認められているものでもない。また JPNIC は、IP アドレス管理指定事業者のホストマスタ相互間での証明書の使用を制限するものではないが、本使用に対して、なんら責任を負うものではない。

1.4.3. 証明書の相互運用性

JPNIC 認証局は、他の認証局と相互認証を行うことがあるものとする。

1.5. ポリシ管理

1.5.1. 文書を管理する組織及び連絡担当者

本 CP/CPS を管理する組織及び問い合わせ先を次に定める。

社団法人 日本ネットワークインフォメーションセンター

受付時間：月～金（年未年始 / 祝祭日は除く） 10:00～18:00

電子メールアドレス：（電子メールアドレスは決定後に記述される）

1.5.2. CP/CPS のポリシ適合性を決定する者

本 CP/CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会と呼ぶ）が行う。

1.5.3. CP/CPS 承認手続

本 CP/CPS の改訂は、運営委員会により承認を受けた後に公表されるものとする。

1.6. 定義と略語

本 CP/CPS にて使用される用語は、表 1-3 に示すとおりである。

表 1-3 用語

| 用語 | 略称 | 説明 |
|-------|-----|---|
| 電子証明書 | 証明書 | ある公開鍵を、記載されたものが保有することを証明する電子的文書。認証局が電子署名を施すことで、その正当性が保証される。本 CP/CPS では、特に断らない限りホストマスタ証明書、サーバ証明書及び運用用証明書を総称して「証明書」と呼ぶ。 |
| 認証局 | CA | 証明書の発行・更新・失効、認証局等私有鍵の生成・保護及び証明書申請者の登録を行う機関。本 CP/CPS 内で、単に認証局という場合は証明書の発行業務及び登録業務を含む。 |

| 用語 | 略称 | 説明 |
|--|-----|--|
| RFC 3647 (Request For Comments 3647) | | 認証局 や PKI のための CP/CPS の執筆者を支援するフレームワーク。 |
| オブジェクト識別子 (Object Identifier) | OID | 世界で一意となる値を登録機関 (ISO、ITU) に登録した識別子。PKI で使うアルゴリズム、証明書内に格納する名前 (subject) のタイプ (Country 名等の属性) 等は、オブジェクト識別子として登録されているものが使用される。 |
| X.509 | | ITU-T が定めた証明書及び証明書失効リストのフォーマット。X.509 v3 では、任意の情報を保有するための拡張領域が追加された。 |
| 公開鍵 | | 公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵。 |
| 私有鍵 | | 公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。 |
| 証明書発行要求 (Certificate Signing Request) | CSR | 証明書を発行する際のもとなるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。 |
| CRL (Certificate Revocation List) | | 証明書の有効期間中に、認証局私有鍵の危殆化等の事由により失効された EE 証明書及び運用用証明書の失効リスト。 |
| PIN (Personal Identification Number) | | 個人を識別するための情報。 |

2. 公開とリポジトリの責任

2.1. リポジトリ

本認証局を含む JPNIC 認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理を行う。システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくはホームページ上で公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。

2.2. 証明情報の公開

本認証局を含む JPNIC 認証局は、次の情報を、JPNIC 認証局のリポジトリ上に公開する。

- 自己署名証明書 (JPNIC ルート認証局)
- リンク証明書 (JPNIC ルート認証局)
- 下位認証局証明書 (JPNIC ルート認証局)
- EE 証明書 (JPNIC IP アドレス認証局) *公表時のみ
- CRL (JPNIC ルート認証局、JPNIC IP アドレス認証局)
- CP/CPS (JPNIC ルート認証局、JPNIC IP アドレス認証局)

リポジトリの URI は次のとおりである。

(URI は決定後に記述される)

また、JPNIC が運営する認証局は、フィンガープリントを、リポジトリより SSL/TLS を使用して公開する。フィンガープリントを公開するリポジトリの URI は次のとおりである。

(URI は決定後に記述される)

なお、CP/CPS 及び認証局に関する重要情報は、JPNIC の次に示す URI のホームページにおいても公開される。

(URI は決定後に記述される)

2.3. 公開の時期又は頻度

本認証局を含む JPNIC 認証局が公開する情報について、公開の時期及び頻度は次のとおりである。

- CP/CPS については、改訂の都度、本 CP/CPS 「9.12.2.通知方法及び期間」で定める時期に公表される。
- 自己署名証明書、リンク証明書、下位認証局証明書については、発行及び更新の都度公表される。
- CRL については、発行の都度公表される。発行の頻度は本 CP/CPS 「4.9.7.証明書失効リストの発行頻度」で規定される。
- 認証局に関する重要情報若しくはその他の情報は、JPNIC 認証局の判断により適宜更新が行われる。
- EE 証明書については、発行及び更新の都度公表される。* 公表時のみ

2.4. リポジトリへのアクセス管理

本認証局を含む JPNIC 認証局は、公開情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。証明書所有者及び証明書検証者は、JPNIC が運営する認証局が発行した証明書に関する公開情報を、リポジトリを通じて入手することができる。

3. 識別及び認証

3.1. 名前決定

3.1.1. 名前の種類

証明書発行者の名前と発行対象の名前は、X.500 シリーズ定義の識別名の規定に従って設定する。

3.1.2. 名前が意味を持つことの必要性

証明書に記載される名前は、個人名、組織名及びその個人、組織が管理する機器名をあらわすものである必要がある。

3.1.3. 所有者の匿名性又は仮名性

証明書に記載される名前として匿名又は仮名を使用することはできない。

3.1.4. 種々の名前形式を解釈するための規則

様々な名前の形式を解釈するルールは、X.500 シリーズ定義の識別名の規定に従う。

3.1.5. 名前の一意性

証明書に記載される名前は、本認証局が同一ポリシーのもとで発行する全ての証明書において一意とする。

3.1.6. 商標の認識、認証及び役割

規定しない。

3.2. 初回の本人性確認

3.2.1. 私有鍵の所持を証明する方法

本認証局は、PKCS#10 (Public-Key Cryptography Standards #10) に従った電子署名のされた証明書発行要求の利用、その他本認証局が認めた方法を通じて、ホストマスタ証明書の申請者が私有鍵を所有していることを確認する。

サーバ証明書に関しては、本認証局は、予め規定された方法により証明書申請者が私有鍵を所有していることを確認する。

3.2.2. 組織的本人性の認証

本認証局は、LRA に対して組織若しくは団体の認証を行う。LRA としての認証を受けようとする組織若しくは団体は、登記簿及び代表者の印鑑証明、その他本認証局が必要と認める書類を本認証局に提出し、審査を受けなければならない。

サーバ証明書に関しては、本認証局は、証明書の発行対象となるサーバを運用・管理する組織若しくは団体が、JPNIC 又は JPNIC が認める組織若しくは団体であることを確認する。

3.2.3. 個人的本人性の認証

LRA 管理者は、ホストマスタ証明書発行対象者の発行登録を行う際に、人事情報 DB、雇用契約等本人を特定できる情報を用いて発行対象者の本人確認を行う。また、証明書発行対象者が、LRA 責任者より証明書の発行の許可を受けている者であることを確認する。

サーバ証明書に関しては、本認証局は、証明書の発行を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを、予め規定された方法により確認する。

3.2.4. 確認しない所有者の情報

規定しない。

3.2.5. 権限の正当性確認

本認証局は、LRA 管理者からホストマスタ証明書の申請登録を受付けるにあたって、当該 LRA 管理者の正当性を確認する。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申請時の本人性確認と認証

3.3.1. 通常の鍵更新の本人性確認と認証

本 CP/CPS「3.2.初回の本人性確認」に定める手続と同様とする。

3.3.2. 証明書失効後の鍵更新の本人性確認と認証

本 CP/CPS「3.2.初回の本人性確認」に定める手続と同様とする。

3.4. 失効申請時の本人性確認と認証

LRA 管理者は、ホストマスタから署名付き電子メールによる失効申請を受付けた場合には、その署名を検証する。また署名付き電子メールによらないその他の失効申請の場合は、LRA が事前に定め、本認証局から承認を受けた方法によって申請者の本人確認を確実に行うものとする。

LRA 管理者は、失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

サーバ証明書に関しては、本認証局は、証明書の失効を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを、予め規定された方法により確認する。

4. 証明書のライフサイクルに対する運用上の要件

4.1. 証明書申請

4.1.1. 証明書申請を提出することができる者

ホストマスタ証明書の申請を行うことができる者は、LRA 契約を結んだ IP アドレス管理指定事業者の従業員若しくは LRA が指定した者とする。

サーバ証明書の申請を行うことができる者は、JPNIC の職員若しくは JPNIC が指定した者とする。

4.1.2. 登録手続及び責任

ホストマスタ証明書の申請者は、LRA 管理者により事前に周知された方法に従い、LRA 管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 に従った電子署名のされた証明書発行要求をセキュアなオンライン通信を介して送付する。

サーバ証明書の申請者は、本認証局に対して予め規定された方法により証明書の発行申請を行う。

証明書申請者は証明書を申請するにあたって、次の責任を負うものとする。

- 本 CP/CPS、その他本認証局により開示された文書の内容の承諾
- 証明書申請内容の正確な提示

4.2. 証明書申請手続

4.2.1. 本人性確認と認証機能の実行

ホストマスタ証明書の申請者の本人性確認は LRA 管理者が行う。LRA 管理者は、本 CP/CPS 「3.2.3.個人的本人性の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。LRA 管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。

サーバ証明書の申請者の本人性確認は、本認証局が予め規定された方法により行う。

4.2.2. 証明書申請の承認又は却下

LRA 管理者は、ホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。LRA 管理者は、申請の審査に関して責任を負うものとする。

なお、本認証局は、ホストマスタ証明書の申請登録を行う LRA 管理者の本人性確認を行った後、証明書の発行手続を開始する。

サーバ証明書に関しては、本認証局が申請の諾否を決定する。

4.2.3. 証明書申請の処理時間

LRA 管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。

本認証局は、LRA 管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。

サーバ証明書に関しては、本認証局は、本 CP/CPS「4.1.1.証明書申請を提出することができる者」にて規定した者より発行申請を受理した場合、速やかに証明書の発行を行う。

4.3. 証明書発行

4.3.1. 証明書の発行過程における認証局の行為

本認証局は、LRA 管理者からのホストマスタ証明書の発行申請登録を受付けるにあたって、予め定められた方法により LRA 管理者の本人性確認を行う。本認証局は、申請登録の真正性を確認した後、ホストマスタ証明書の申請者に対し、本 CP/CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。

本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。

サーバ証明書に関しては、本認証局は、申請者の本人性確認を行った後、予め規定された方法により証明書の発行を行う。

4.3.2. 認証局の所有者に対する証明書発行通知

本認証局は、証明書発行に必要な 2 種類の情報を生成し、一方を（電子メール若しくは郵送：決定後に記述される）を用いて直接ホストマスター証明書の申請者へ、もう一方を（電子メール若しくは郵送：決定後に記述される）を用いて LRA 管理者経由でホストマスター証明書の申請者へ通知する。

サーバ証明書に関しては、本認証局は、予め規定された方法により申請者に対し発行通知を行う。

4.4. 証明書の受領確認

4.4.1. 証明書の受領確認の行為

本認証局は、ホストマスター証明書の申請者による証明書のダウンロードをもって、証明書の受領を確認する。

サーバ証明書に関しては、本認証局は、予め規定された方法により、証明書の受領を確認する。

なお、証明書の申請者は、証明書ファイルが自身の PKI 環境で利用可能であること、証明書の記載内容が正しいことを確認しなければならない。

4.4.2. 認証局による証明書の公開

本認証局を含む JPNIC 認証局は、本 CP/CPS 「2.2.証明情報の公開」に規定する証明書をリポジトリにて公開する。

4.4.3. 他のエンティティに対する認証局の証明書発行通知

本認証局は、他のエンティティに対して証明書の発行通知を行わない。

4.5. 鍵ペアと証明書の用途

4.5.1. 所有者の私有鍵及び証明書の使用

本 CP/CPS に基づき発行される証明書は、JPNIC と IP アドレス管理指定事業者間での申請等業務に利用することを意図するものであり、電子商取引での利用に意図されているものでも、認められているものでもない。

証明書所有者は、私有鍵及び証明書の使用に関して、次の責任を負うものとする。

- 証明書の記載内容の受領時確認と誤記内容の申告
- 私有鍵の盗難・漏えい・紛失・他者による不正利用等を防ぐことへの十分な注意と管理
- 鍵の危殆化又はその可能性がある場合の速やかな失効申請
- 使用目的の確認及び、その目的内での使用
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

4.5.2. 検証者の公開鍵及び証明書の使用

証明書検証者は、証明書を信頼するにあたって、次の責任を負う。

- 証明書を信頼する時点で、本 CP/CPS の理解と承諾
- 証明書の使用目的と自己の使用目的が合致していることの承諾
- 証明書に行われた電子署名の検証と発行者の確認
- 証明書の有効期間や記載項目の確認
- CRL に基づいて、証明書が失効していないことの確認
- 証明書パス上の全証明書の改ざん、有効期間、失効、使用目的の確認

4.6. 証明書の更新

本認証局では、鍵ペアの更新を伴わない証明書の更新は行わない。証明書を更新する場合は、新たな鍵ペアを生成することとし、本 CP/CPS 「4.7.証明書の鍵更新」に定める手続とする。

4.7. 証明書の鍵更新

4.7.1. 証明書の鍵更新の場合

証明書の鍵更新は、次の場合に行われるものとする。

- 証明書の有効期間が終了する場合
- 鍵の危殆化を理由に証明書が失効された場合

4.7.2. 新しい公開鍵の証明申請を行うことができる者

本 CP/CPS 「4.1.1.証明書申請を提出することができる者」と同様とする。

4.7.3. 証明書の鍵更新申請の処理

本 CP/CPS 「4.2.証明書申請手続」及び「4.3.証明書発行」に定める手続と同様とする。

4.7.4. 所有者に対する新しい証明書の通知

本 CP/CPS 「4.3.2.認証局の所有者に対する証明書発行通知」と同様とする。

4.7.5. 鍵更新された証明書の受領確認の行為

本 CP/CPS 「4.4.1.証明書の受領確認の行為」と同様とする。

4.7.6. 認証局による鍵更新済みの証明書の公開

本 CP/CPS 「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7. 他のエンティティに対する通知

本 CP/CPS 「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8. 証明書の変更

4.8.1. 証明書の変更の場合

証明書の変更は、次の場合に行われるものとする。

- 証明書に含まれる公開鍵以外の情報に変更が生じた場合

4.8.2. 証明書の変更を申請することができる者

本 CP/CPS 「4.7.2.新しい公開鍵の証明申請を行うことができる者」と同様とする。

4.8.3. 変更申請の処理

本 CP/CPS 「4.7.3.証明書の鍵更新申請の処理」と同様とする。

4.8.4. 所有者に対する新しい証明書の通知

本 CP/CPS 「4.7.4.所有者に対する新しい証明書の通知」と同様とする。

4.8.5. 変更された証明書の受領確認の行為

本 CP/CPS 「4.7.5.鍵更新された証明書の受領確認の行為」と同様とする。

4.8.6. 認証局による変更された証明書の公開

本 CP/CPS 「4.7.6.認証局による鍵更新済みの証明書の公開」と同様とする。

4.8.7. 他のエンティティに対する認証局の証明書発行通知

本 CP/CPS 「4.7.7.他のエンティティに対する通知」と同様とする。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の場合

LRA 組織に所属する証明書所有者は、LRA が別途定める基準に基づき、LRA 管理者に証明書の失効申請を行わなければならない。

本認証局は、証明書所有者及び LRA 管理者からの失効申請の他に、次の項目に該当すると認めた場合、ホストマスタ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- 証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者が本 CP/CPS に違反した場合

- 証明書所有者あるいは LRA が、本 CP/CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合
- その他本認証局が失効の必要があると判断した場合

サーバ証明書の証明書所有者は次の項目に該当する場合に本認証局に対し失効申請を行わなければならない。

- サーバの使用を停止する場合
- サーバの私有鍵が危殆化した（又はそのおそれがある）場合

また、本認証局は、証明書所有者からの失効申請のほかに、次の項目に該当すると認められた場合、サーバ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- サーバの私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者が本 CP/CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- その他本認証局が失効の必要があると判断した場合

4.9.2. 証明書失効を申請することができる者

ホストマスタ証明書の失効要求ができる者は、次のとおりである。

- 証明書所有者
- 証明書所有者の法律上の正式な代理人
- 証明書所有者が所属する組織の LRA 責任者、LRA 管理者
- 本認証局

サーバ証明書の失効要求ができるものは、次のとおりである。

- 証明書所有者
- 本認証局

4.9.3. 失効申請手続

LRA 組織に所属する証明書所有者若しくは LRA 責任者は、LRA 組織により定められた手続によって、LRA 管理者に失効申請を行う。LRA 管理者は失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

サーバ証明書の所有者は、本認証局に対し予め規定された方法により失効申請を行う。

なお、「4.4.1.証明書が失効される理由」にて列挙する項目に該当すると本認証局が認めた場合には、本認証局が自身の判断により証明書の失効登録を行うことがある。

4.9.4. 失効申請の猶予期間

証明書の失効要求は、失効すべき事象が発生した場合、可能な限り速やかに行われるものとする。

4.9.5. 認証局が失効申請を処理しなければならない期間

本認証局における証明書の失効処理は、失効申請の受付後、(時間は決定後に記述される) 時間以内に行われる。

4.9.6. 検証者の失効調査の要求

証明書検証者は、本認証局により発行された証明書を信頼し利用するにあたって、最新の CRL を参照し当該証明書の失効処理が行われていないことを確認しなければならない。

4.9.7. 証明書失効リストの発行頻度

CRL は証明書失効の有無に関わらず、24 時間以内に更新される。証明書の失効が申請された場合は、失効手続が完了した時点で更新される。

4.9.8. 証明書失効リストの発行最大遅延時間

本認証局は、CRL が生成された後、速やかにリポジトリに公開する。

4.9.9. オンラインでの失効/ステータス確認の適用性

OCSP 等のオンラインの失効又はステータスチェックの機能はサポートしない。

4.9.10. オンラインでの失効/ステータス確認を行うための要件

規定しない。

4.9.11. 利用可能な失効通知の他の形式

規定しない。

4.9.12. 鍵更新の危殆化に対する特別要件

本認証局は、本認証局の私有鍵に危殆化又は危殆化のおそれがある場合は、直ちに全ての証明書の失効処理を行い、CRL に登録し、証明書所有者に対してメール等の手段で本認証局の私有鍵の危殆化等の事実と証明書失効の通知を行う。

4.9.13. 証明書の一時的停止の場合

本認証局は、発行した証明書の一時的停止を行わない。

4.10. 証明書のステータス確認サービス

4.10.1. 運用上の特徴

本認証局は、証明書検証者における証明書ステータスの確認手段として、CRL を提供する。CRL へのアクセス要件は、本 CP/CPS 「2.4.リポジトリへのアクセス管理」に規定する。また、CRL の発行頻度及び発行最大遅延時間については、本 CP/CPS 「4.9.7.証明書失効リストの発行頻度」及び「4.9.8.証明書失効リストの発行最大遅延時間」に規定する。

4.10.2. サービスの利用可能性

本 CP/CPS 「2.1.リポジトリ」に規定する。

4.10.3. オプションな仕様

規定しない。

4.11. 登録の終了

証明書所有者が本認証局のサービスの利用登録を終了する場合、本認証局は証明書所有者に対して発行した証明書の全てを失効する。

4.12. キーエスクローと鍵回復

本認証局は私有鍵を第三者に対して寄託しない。

EE は私有鍵を EE 自身で生成及び管理する。

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、電磁界、水害、地震、落雷、空気汚染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い、また監視カメラによる記録を行う。認証設備室への立入には、入室権限を有する複数人が同時に操作する必要がある。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建物及び室には漏水検知器の設置等、防水対策を施して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、別地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 CP/CPS 上信頼される役割を担っている。JPNIC 認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。JPNIC 認証局運営上の役割を表 5-1 に示す。

表 5-1 名称とその役割

| | 役割名称 | 役割の説明 |
|--|-------|--|
| | 運営委員会 | <ul style="list-style-type: none"> ・ 監査報告の確認及び承認 ・ 認証局運営責任者への監査指摘事項対応指示 ・ JPNIC 認証局の運営方針の決定 ・ 証明書ポリシー、運用ポリシー及び運用ポリシー変更の最終承認 ・ 認証局運営責任者の任命・解任等 ・ その他、重要な事項の協議及び決議 |

| | | 役割名称 | 役割の説明 |
|------|-------|-----------|---|
| 運営組織 | 運営組織 | 認証局運営責任者 | <ul style="list-style-type: none"> ・ 認証サービス及び運用組織の統括 ・ 監査指摘事項への対応統括 ・ 運用管理者の任命・解任 ・ システム変更及び運用ポリシー変更の承認 ・ 非常時対応等の指揮、監督 |
| | | 運用管理者 | 運用組織の統括 <ul style="list-style-type: none"> ・ 運用担当者の任命・解任 ・ 運用担当者の教育計画策定及び実施 ・ 運用担当者の入室権限付与 ・ 運用担当者の作業報告確認 ・ 認証局私有鍵の活性化操作、非活性化操作の立会い ・ 非常時の対応指示 ・ 作業報告書、貸出簿等、運用記録の保管・管理等 ・ その他、運用全般の管理 |
| | 運用担当者 | ログ検査者 | <ul style="list-style-type: none"> ・ 監査ログ、入退室ログ等の検査 |
| | | 鍵管理者 | <ul style="list-style-type: none"> ・ キーセレモ二時の認証局鍵生成作業立会い ・ 認証局鍵廃棄時の立会い ・ バックアップ私有鍵の管理 |
| | | セキュリティ管理者 | <ul style="list-style-type: none"> ・ 認証局システムのセキュリティ設定及び変更 ・ キーセレモ二時のRAOの登録、発行 |
| | | 認証局管理者 | <ul style="list-style-type: none"> ・ 認証局サーバ、ディレクトリサーバ等認証局システムの運用管理 |
| | | 登録局管理者 | <ul style="list-style-type: none"> ・ 証明書発行、失効の登録作業 ・ 登録局の管理運営 |
| | | 審査者 | <ul style="list-style-type: none"> ・ LRA 管理者証明書発行申請の受付 ・ 証明書発行に係る審査 ・ 承認者への LRA 管理者証明書の発行依頼 |
| | | 承認者 | <ul style="list-style-type: none"> ・ 審査結果の承認 ・ 発行登録作業の承認 |
| | | | 保守員 |
| | | ベンダー保守員 | <ul style="list-style-type: none"> ・ 各種機器の故障等の対応 |

| | | 役割名称 | 役割の説明 |
|--|---------|------------|---|
| | ローカル登録局 | ローカル登録局 | 証明書を発行する組織とは異なる組織若しくは団体であり、登録局業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が LRA となる。 |
| | | ローカル登録局責任者 | IP アドレス管理指定事業者の中における、LRA 業務の責任者 ・ LRA 管理者の任命及び解任 |
| | | ローカル登録局管理者 | IP アドレス管理指定事業者の中で、ホストマスタのメンバー管理と認証及びホストマスタ証明書の発行申請操作を行う。 |

5.2.2. 職務ごとに必要とされる人数

JPNIC 認証局システムサーバの操作は複数人の CAO によって行う。また、JPNIC 登録局の端末を用いた発行・失効等の操作は複数人の RAO によって行う。

JPNIC 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

JPNIC 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、JPNIC 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

JPNIC 認証局では、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. 経歴の調査手続

JPNIC 認証局業務に係わる要員を採用するにあたって、JPNIC は予め定めた適切な方法を用いてその人物の背景調査を行う。

5.3.3. 研修要件

JPNIC 認証局は、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 JPNIC 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

JPNIC は、JPNIC 認証局運営が損なわれないよう職員の退職又は解任に備えて適切な対策を講ずる。

5.3.6. 認められていない行動に対する制裁

JPNIC は、JPNIC 認証局の運用要員による認可されていない行為に対し、（罰則規定書の名称は決定後に記述される）に従って制裁を与える。

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

JPNIC 認証局は次の文書を運用要員に開示し周知する。

- 本 CP/CPS
- 認証局運用に関する諸規程、手順書、マニュアル、災害復旧計画書等
- 運用要員が遵守しなければならない各種関連規程
- (その他、要員に提供されるべき文書があれば決定後に記述される。)

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
- システムの起動・停止
- データベースの操作
- 権限設定の変更履歴
- 証明書の発行
- 証明書の失効
- CRL の発行
- 監査ログの検証 等

また、次のような認証設備室内のネットワーク機器並びに監視システムについても履歴を記録する。

- 認証設備室への入退室に関する記録
- 認証局設備への不正アクセスに関する記録 等

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、外部記憶媒体に最低 10 年間は保管される。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。監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。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、認証局サーバ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・テクノロジーの導入等、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 CP/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
- 証明書有効期限の変更等、ポリシーの何らかの変更

【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。

()内は保管期間

- 本 CP/CPS、証明書所有者同意書及びその変更に関する記録（その作成又は変更を行ってから 10 年間）
- 認証業務に従事する者の責任及び権限並びに指揮命令系統に関して記載した文書及びその変更に関する記録（その作成又は変更を行ってから 10 年間）
- 証明書の発行、失効時に提出を受ける申請書（該当する証明書の有効期間の満了日から最低 10 年間）
- 証明書申請者の真偽の確認のために提出を受けた書類（該当する証明書の有効期間の満了日から最低 10 年間）
- 証明書の発行、失効申請に対する諾否を決定した者の氏名の記載した書類及び、申請に対して承諾をしなかった場合においてその理由を記載した書類（該当する証明書の有効期間の満了日から最低 10 年間）
- 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（その作成を行ってから 10 年間）
- 監査の実施結果に関する記録及び監査報告書（その作成を行ってから 10 年間）

5.5.2. アーカイブ保持期間

本認証局は、認証局サーバデータベースの履歴及び監査ログファイルの履歴を最低 10 年間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本 CP/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、磁気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、認証局サーバ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、認証局サーバシステム、監査ログとともに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、正確な時刻源から時刻を取得し、NTP (Network Time Protocol) を使用し認証局システムサーバの時刻同期を行ったうえ、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。

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 CP/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 CP/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 CP/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。

- ホストマスタ証明書、サーバ証明書等の失効手続
- 認証局私有鍵の廃棄及び再生成手続
- ホストマスタ証明書、サーバ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 CP/CPS 「4.9」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（日は決定後に記述される）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。

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、安全性の高い暗号化モジュールを含むソフトウェア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

本認証局は EE 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

EE 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、次にあげる 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 認証局は (URI は決定後に記述される) 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 (URI は決定後に記述される) 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 (URI は決定後に記述される) にて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。
- サーバ証明書の管理者には RAO が、ホストマスタには LRA 管理者が本認証局の証明書を手渡しする。

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 と呼ぶ) 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。

ホストマスタ証明書の keyUsage は digitalSignature、keyEncipherment 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。

サーバ証明書の keyUsage は digitalSignature、keyEncipherment のビットを使用する。SSL/TLS サーバ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 CP/CPS 「4.12.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。

EE の私有鍵は EE 自身が私有鍵の生成を行い、EE 自身で格納を行う。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複数名の CAO を必要とする。

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複数名の CAO を必要とし、

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、鍵管理者と複数名の CAO 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つい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。

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。バックアップデータは改ざん防止のため暗号化して保管される。

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。また、CAO によって定期的に変更を行う。

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、複数人の CAO 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。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

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 CP/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。

7. 証明書と、証明書失効リスト及び OCSP のプロファイル

7.1. 証明書のプロファイル

本認証局が発行する証明書は、X.509 証明書フォーマットのバージョン 3 に従う。証明書プロファイルは、表 7-1 のとおりである。

7.1.1. バージョン番号

本認証局が発行する証明書は全て X.509 バージョン 3 証明書フォーマットに従う。

7.1.2. 証明書拡張

本認証局が発行する証明書に使用される拡張領域を次に示す。

7.1.2.1. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.2. subjectKeyIdentifier

当該証明書所有者の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.3. keyUsage

ホストマスタ証明書、サーバ証明書共に digitalSignature と keyEncipherment のみを使用する。この拡張は critical である。

7.1.2.4. certificatePolicies

ホストマスタ証明書、サーバ証明書共に certificatePolicies 拡張を使用する。policyIdentifier の値は本 CP/CPS 「7.1.6.証明書ポリシ OID」、policyQualifiers の値は本 CP/CPS 「7.1.8.ポリシ修飾子の記述と意味」に示す。この拡張は non-critical である。

7.1.2.5. subjectAltName

この拡張はホストマスタ証明書にのみ使用する。rfc822Name として証明書所有者の電子メールアドレスを記述する。この拡張は non-critical である。

7.1.2.6. cRLDistributionPoints

本認証局が発行する CRL の URI を記述する。この拡張は non-critical である。

7.1.3. アルゴリズム OID

本認証局が発行する証明書において使用されるアルゴリズム OID は次の 2 つである。

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- rsaEncryption (1.2.840.113549.1.1.1)

7.1.4. 名前形式

本 CP/CPS 「3.1.1.名前の種類」に従う。

7.1.5. 名前制約

本認証局は、発行する全ての証明書において nameConstraints 拡張を使用しない。

7.1.6. 証明書ポリシー OID

ホストマスタ証明書、サーバ証明書共に本 CP/CPS 「1.2.文書の名前と識別」に定める EE 証明書ポリシーの OID を使用する。

7.1.7. ポリシ制約拡張

本認証局は、発行する全ての証明書において policyConstraints 拡張を使用しない。

7.1.8. ポリシ修飾子の記述と意味

ホストマスタ証明書、サーバ証明書共にポリシ修飾子の値として本 CP/CPS が公開されている URI を使用する。

7.1.9. critical な証明書 certificatePolicies 拡張の処理

本認証局が発行する証明書に含まれる certificatePolicies 拡張は全て non-critical であり、本項の規定を行わない。

表 7-1 JPNIC IP アドレス認証局が発行する証明書プロファイル

| Field | critical flag | ホストマスタ証明書 | サーバ証明書 |
|---------------------------|---------------|--|---|
| version | NA | 2 | 2 |
| serialNumber | NA | non-negative integer | non-negative integer |
| signature | NA | | |
| algorithm | | sha1withRSAEncryption | sha1withRSAEncryption |
| parameters | | null | null |
| issuer | NA | | |
| | | PrintableString* ¹ | PrintableString* ¹ |
| validity | NA | | |
| notBefore | | UTCTime | UTCTime |
| notAfter | | UTCTime notBeforeの時刻より2年後 | UTCTime notBeforeの時刻より2年後 |
| subject | NA | | |
| | | PrintableString* ² | PrintableString* ³ |
| subjectPublicKeyInfo | NA | | |
| algorithm | | rsaEncryption | rsaEncryption |
| parameters | | null | null |
| subjectPublicKey | | ホストマスタ公開鍵のBIT STRING | サーバ公開鍵のBIT STRING |
| authorityKeyIdentifier | n | | |
| keyIdentifier | | JPNIC IPアドレス認証局 公開鍵の160bit SHA-1 ハッシュ値 | JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値 |
| authorityCertIssuer | | 使用しない | 使用しない |
| authorityCertSerialNumber | | 使用しない | 使用しない |
| subjectKeyIdentifier | n | ホストマスタ公開鍵の 160bit SHA-1ハッシュ値 | サーバ公開鍵の160bit SHA-1ハッシュ値 |
| keyUsage | c | | |
| digitalSignature | | 1 | 1 |
| nonRepudiation | | 0 | 0 |
| keyEncipherment | | 1 | 1 |
| certificatePolicies | n | | |
| policyIdentifier | | 本CPのOID | 本CPのOID |
| policyQualifiers | | | |
| policyQualifierId | | CPSUri | CPSUri |
| qualifier | | 本CP/CPSを公開するURI | 本CP/CPSを公開するURI |
| subjectAltName | n | | |
| rfc822Name | | ホストマスタの メールアドレス | 使用しない |
| cRLDistributionPoints | n | | |
| DistributionPoint | | | |
| distributionPoint | | JPNIC IPアドレス認証局が CRLを公開するURI | JPNIC IPアドレス認証局が CRLを公開するURI |
| reasons | | 使用しない | 使用しない |
| cRLIssuer | | 使用しない | 使用しない |

1 C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=JPNIC Resource Service Certification Authority

2 C=JP, O=Japan Network Information Center, OU=Internet Resource

Services, OU=Resource Holder, OU= (JPNIC が LRA 組織に一意に割り当てる ID) (LRA 組織名称), CN= (証明書発行対象ホストマスタの氏名をアルファベット表記したもの) + serialNumber= (LRA 組織ごとに一意に管理される ID)

3 C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=Resource Management System, CN= (証明書発行対象サーバの FQDN)

7.2. 証明書失効リストのプロファイル

本認証局が発行する CRL は、X.509CRL フォーマットのバージョン 2 に従う。CRL プロファイルは、表 7-2 のとおりである。

7.2.1. バージョン番号

本認証局が発行する CRL は全て X.509 バージョン 2CRL フォーマットに従う。

7.2.2. CRL 及び CRL エントリ拡張

本認証局は次の 2 つの CRL 拡張を使用し、CRL エントリ拡張は使用しない。

7.2.2.1. cRLNumber

本認証局が発行する CRL において一意となる非負の整数を使用する。

7.2.2.2. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

表 7-2 JPNIC IP アドレス認証局が発行する CRL プロファイル

| Field | critical flag | 証明書失効リスト |
|------------------------|---------------|---|
| version | NA | 1 |
| signature | NA | |
| algorithm | | sha1withRSAEncryption |
| parameters | | null |
| issuer | NA | |
| | | PrintableString ^{*1} |
| thisUpdate | NA | UTCTime |
| nextUpdate | NA | UTCTime thisUpdateより24時間後 |
| revokedCertificates | NA | |
| revokedCertificate | | |
| userCertificate | | 失効された証明書の シリアル番号 |
| revocationDate | | UTCTime 証明書の失効された時刻 |
| crlEntryExtensions | | |
| | | 使用しない |
| crlExtensions | NA | |
| cRLNumber | n | non-negative integer |
| authorityKeyIdentifier | n | JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値 |

1 C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=JPNIC Resource Service Certification Authority

7.3. OCSP プロファイル

OCSP は使用しない。

8. 準拠性監査とその他の評価

8.1. 評価の頻度又は評価が行われる場合

本認証局を含む JPNIC 認証局は、毎年一回以上、認証局運用についての準拠性監査を実施する。また、必要に応じて、不定期な監査を実施する。

8.2. 評価人の身元又は資格

JPNIC は、認証局の準拠性監査を、運営委員会が選定する認証業務に精通した監査者により実施する。

8.3. 評価人と評価されるエンティティとの関係

JPNIC は、本認証局を含む JPNIC 認証局の認証業務に係わる要員以外から監査者を選定する。

8.4. 評価で扱われる事項

本認証局を含む JPNIC 認証局の準拠性監査は、認証局の運営が本 CP/CPS 及び関連する規定を遵守して運営されているかを監査するものである。

主な監査項目は次のとおりである。

- 認証局の業務担当者の業務運用
- 認証局私有鍵の管理
- 証明書のライフサイクル管理
- ソフトウェア、ハードウェア、ネットワーク
- 物理的環境及び設備
- セキュリティ技術の最新動向への対応
- 規定等の妥当性評価

また、運営委員会が必要と認めた場合、運営委員会が指定する監査目的による監査を実施する。

なお、JPNIC は LRA の監査を行う権利を有する。

8.5. 不備の結果としてとられる処置

本認証局を含む JPNIC 認証局は、監査報告書で指摘された事項に対して、運営委員会がその対応を決定する。運営委員会は、指摘事項に関して、セキュリティ技術の最新動向も踏まえ、問題が解決されるまでの対応策も含め、その措置を JPNIC 認証局の運営責任者に指示する。講じられた対応策は、運営委員会に報告され、評価されるとともに、次の監査において確認される。監査において発見された不備等の指摘事項への対応をしない場合は、運営委員会によって予め定められた罰則が課される。

8.6. 評価結果の情報交換

監査結果の報告は監査者から運営委員会に対して行われる。本認証局を含む JPNIC 認証局は、法律に基づく開示要求があった場合以外は、監査結果を外部へ開示しない。

なお、監査報告書については、JPNIC 認証局運営責任者が最低 5 年間保管管理するものとする。

9. 他の業務上の問題及び法的問題

9.1. 料金

本認証局が発行する証明書に関わる発行料金、更新料金、利用料金等は、別途定めるものとし、事前に関係者に周知する。

9.2. 財務的責任

JPNIC は本 CP/CPS に規定した内容を遵守して認証業務を提供し、認証局私有鍵の信頼性を含む認証業務の信頼性の確保を保証する。JPNIC がこの保証に違反して損害賠償を負う場合には、IP アドレス管理指定事業者等との契約における該当条項に従う。

9.3. 情報の秘密性

9.3.1. 秘密情報の範囲

本認証局を含む JPNIC 認証局が保持する情報は、本 CP/CPS 「2.2.証明情報の公開」で公表すると定めた情報、本 CP/CPS の一部として明示的に公表された情報、ホームページで公表している情報、証明書の失効理由及び失効に関するその他の詳細情報を除き、秘密扱いとする。

証明書所有者の私有鍵は、その証明書所有者によって秘密扱いとされる情報とする。

9.3.2. 秘密情報の範囲外の情報

本 CP/CPS で公表すると定めた情報、本 CP/CPS の一部として明示的に公表された情報、ホームページ等で公表している情報、証明書の発行者である認証局情報と失効日時を含む CRL は秘密扱いとしない。その他、次の状況におかれた情報は秘密扱いとしない。

- JPNIC の過失によらず知られるようになった情報
- JPNIC 以外の出所から、機密保持の制限なしに JPNIC に知られるようになった情報
- JPNIC によって独自に開発された情報
- 開示対象の情報に関連する人又は組織により承認を得ている情報

9.3.3. 秘密情報を保護する責任

本認証局を含む JPNIC 認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を開示することができる。また、本認証局を含む JPNIC 認証局で取扱う情報に関して、調停、訴訟、仲裁、その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。更に、本認証局では、LRA 管理者から、LRA 管理者の管理する証明書所有者に関連する情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、LRA 管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、LRA 管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。

JPNIC 認証局は、業務の一部を委託する場合、秘密情報を委託先に開示することができる。ただし、その委託契約においては秘密情報の守秘義務を規定する。

JPNIC 認証局は、前述の場合を除いて秘密情報を開示しない。秘密情報が漏えいした場合、その責任は漏えいした者が負う。

なお、個人情報の保護に関する取扱いは、本 CP/CPS 「9.4.個人情報のプライバシー保護」に定める。

9.4. 個人情報のプライバシー保護

9.4.1. プライバシポリシー

本認証局を含む JPNIC 認証局は個人情報保護の重要性を認識し、個人情報を本 CP/CPS 「9.3.3.秘密情報を保護する責任」と同様に取扱うことに加え、次のポリシーを遵守する。

- (1) 管理責任者をおき、個人情報の適切な管理を行う。
- (2) 個人情報を収集する場合、収集目的を知らせたうえで、必要な範囲の情報のみを適法かつ公正な手段で収集する。
- (3) 証明書所有者から提出を受けた個人情報は、次の目的にのみ使用する。
 - IP アドレス管理業務の潤滑な運用を行うため
 - 証明書における、認証サービス上の責任を果たすため
 - その他認証業務に関連した目的のため
- (4) 証明書所有者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、

当該業務委託先に対し本書と同等の条件を義務付けるものとする。

- (5) 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざん及び漏えい等から保護するよう努める。
- (6) 証明書所有者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、証明書所有者自身であることが JPNIC 認証局において確認できた場合に限り、JPNIC 認証局において保管している証明書所有者の個人情報を本人に開示する。また、証明書所有者の個人情報に誤りや変更がある場合には、証明書所有者からの申出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。証明書所有者は JPNIC 認証局に開示を求める場合、JPNIC 認証局により定められた方法により申請を行うものとする。
- (7) JPNIC 認証局は、認証業務に従事する職員に対して個人情報保護の教育啓蒙活動を実施する。
- (8) 証明書所有者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護方針を適宜見直し、改善を行う。

9.5. 知的財産権

別段の合意がなされない限り、知的財産権の扱いは次に従うものとする。

- JPNIC 認証局の発行した証明書、CRL は JPNIC に帰属する財産とする
- 本 CP/CPS は JPNIC に帰属する財産とする
- JPNIC 認証局の私有鍵及び公開鍵は JPNIC に帰属する財産とする
- JPNIC 認証局から貸与されたソフトウェア、ハードウェア、その他文書、情報等は JPNIC に帰属する財産とする

9.6. 表明保証

9.6.1. 発行局の表明保証

JPNIC 発行局は、JPNIC 発行局の業務を遂行するにあたり次の義務を負う。

- JPNIC 発行局の証明書署名鍵のセキュアな生成・管理
- (本 CP/CPS、証明書所有者同意書、証明書検証者同意書、JPNIC ルート認証局の自己署名証明書・自己発行証明書、CRL) の値を (SHA-1 (仮のアルゴリズム)) で変換した値の公開

- JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理
- JPNIC 発行局のシステム稼働の監視・運用
- CRL の発行・公表
- リポジトリの維持管理
- JPNIC の判断によって EE 証明書を失効させた場合の当該証明書の所有者への通知
- 本 CP/CPS に従った受付時間内の問合せ受付

9.6.2. 登録局の表明保証

JPNIC 登録局は、JPNIC 登録局の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請における JPNIC 発行局への正確な情報伝達
- 証明書失効申請における JPNIC 発行局への運用時間中の速やかな情報伝達

9.6.3. ローカル登録局の表明保証

LRA は、LRA 業務を遂行するにあたり次の義務を負う。

- 申請書類上の証明書所有者と証明書申請者が同一であることの検証
- JPNIC 登録局への正確な申請情報の伝達
- 証明書使用におけるホストマスタの教育
- 正当な証明書申請者への確実な証明書配布
- 証明書失効の妥当性の確認
- その他、JPNIC との契約に準拠した運用の厳守

9.6.4. 所有者の表明保証

証明書所有者は、証明書所有にあたり次の義務を負う。

- 本 CP/CPS 及び本認証局が提示するその他の文書（文書名は決定後に記述される）の理解と承諾
- 本 CP/CPS 「4.5.1.所有者の私有鍵及び証明書の使用」に規定する義務

9.6.5. 検証者の表明保証

証明書検証者は、本 CP/CPS 「4.5.2.検証者の公開鍵及び証明書の使用」に規定する義務を負う。

9.6.6. 他の関係者の表明保証

規定しない。

9.7. 保証の制限

JPNIC は、本 CP/CPS 「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害、派生的損害に対する責任を負わない。

9.8. 責任の制限

本 CP/CPS 「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」の内容に関し、次の場合には JPNIC は責任を負わないものとする。

- JPNIC に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- LRA 又は証明書所有者が自己の義務の履行を怠ったために生じた損害
- LRA 又は証明書所有者の端末のソフトウェアの瑕疵、不具合その他の動作自体によって生じた損害
- JPNIC の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- JPNIC の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、認証局業務の停止に起因する一切の損害
- 証明書発行申請における本人認証手続等の LRA が行った業務に起因する損害

9.9. 補償

本認証局が発行する証明書を申請、受領、信託した時点で、証明書所有者及び証明書検証者には、JPNIC に対する損害賠償責任及び保護責任が発生する。当該責任の対象となる事象には、各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行のうち、証明書申請時に証明書申請者が本認証局に最新かつ正確な情報を提供しなかったことに起因するもの又は各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような証明書所有者及び証明書検証者の行為、怠慢な行為、各種行為、履行遅滞、不履行等が含

まれる。

9.10. 有効期間と終了

9.10.1. 有効期間

本 CP/CPS、契約書及び協定等の文書は、正当な承認手続にて発行されてから正当な承認手続にて改訂されるまで有効とする。

9.10.2. 終了

本 CP/CPS、契約書、協定等の文書全部又は一部、若しくは特定の関係者に対して規定されている条項が無効になった場合、その該当部分は終了とする。

9.10.3. 終了の効果と効果継続

本認証局は、本 CP/CPS、契約書、協定等に変更又は終了が発生する場合においても、合意事項に責任を持ち続けることに最善を尽くすものとする。

9.11. 関係者間の個別通知と連絡

規定しない。

9.12. 改訂

9.12.1. 改訂手続

本認証局は、証明書ポリシー及びその保証、義務に著しい影響を与えない範囲での本 CP/CPS 変更の必要性が生じた場合、証明書所有者又は証明書検証者に事前の承諾なしに、随時、本 CP/CPS を変更することができる。なお、改訂の通知から改訂が有効になるまでの期間に改訂に対する異議の申出がない場合は、改訂に対する合意が得られたものとする。改訂に対し合意できない関係者においては、即時に本認証局から発行された証明書の使用を中止するものとする。

9.12.2. 通知方法及び期間

本認証局は、変更された CP/CPS をその改訂が有効になる（期間は決定後に記述される）前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知を行うものとする。

9.12.3. オブジェクト識別子の変更されなければならない場合

規定しない。

9.13. 紛争解決手続

本認証局が発行する証明書に関わる紛争について、JPNIC に対して、訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、JPNIC に対して事前にその旨を通知するものとする。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とすることに、全ての当事者は合意するものとする。また、本 CP/CPS、契約書にて定められていない事項やこれらの文書の解釈に関し疑義が生じた場合は、各当事者はその課題を解決するために誠意を持って協議するものとする。

9.14. 準拠法

本認証局を含む JPNIC 認証局、証明書所有者及び証明書検証者の所在地に関わらず、本 CP/CPS の解釈、有効性及び本認証局の証明書発行に関わる紛争については、日本国の法令が適用される。

9.15. 適用法の遵守

本認証局は、国内における各種輸出規制を遵守し、暗号ハードウェア及びソフトウェアを取扱うものとする。

9.16. 雑則

9.16.1. 完全合意条項

本 CP/CPS、契約書又は協定等における合意事項は、これらが改訂又は終了されない限り他の全ての合意事項より優先される。

9.16.2. 権利譲渡条項

規定しない。

9.16.3. 分離条項

本 CP/CPS、証明書所有者同意書及び本認証局より示す協定等において、その一部の条項が無効であったとしても、当該文書に記述された他の条項は有効に存続するものとする。

9.16.4. 強制執行条項

規定しない。