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、役割名、および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

証明書には、個人、組織、役割、および機器が特定できる名前であれば、実名を使用する必要はない。

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のもとで発行する全ての EE に対して一意とする。同一 EE に対する証明書の更新が行われた場合、更新前の証明書と名前が重複する場合がある。

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、資源申請者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. 組織の認証

本認証局は、ローカル RA に対して組織若しくは団体の認証を行う。ローカル RA としての認証を受けようとする組織若しくは団体は IP 指定事業者でなければならない。

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. 個人の認証

JPNIC は、契約／資源管理者証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を行うこととする。

契約／資源管理者は、資源申請者証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を責任を持って行うこととする。

JPNIC は、JPNIC 職員向け証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を行うこととする。

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、契約／資源管理者から資源申請者証明書の申請登録を受け付けるにあたって、当該契約／資源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 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 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

JPNIC は、契約／資源管理者証明書に対する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。

契約／資源管理者は、原則として資源申請者証明書に対する失効申請者の本人確認を行い、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。

JPNIC は、JPNIC 職員向け証明書に対する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。