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

契約／資源管理者証明書の申請を行うことができる者は、IP 指定事業者に所属する者とする。

資源申請者証明書の申請を行うことができる者は、認証された契約／資源管理者とする。

JPNIC 職員向け証明書の申請を行うことができるものは、JPNIC に所属する者とする。

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

契約／資源管理者証明書の申請者は、JPNIC により事前に周知された方法に従い、JPNIC に対して証明書の発行申請を行う。契約／資源管理者は申請書の記載によって役割を確認される。

資源申請者証明書の申請者は、契約／資源管理者により事前に周知された方法に従い、契約／資源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 等の証明書発行要求のデータ形式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。証明書発行要求の電子署名は検証される。

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。

JPNIC 職員向け証明書の申請者は、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 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

契約／資源管理者証明書の申請者の本人性確認は JPNIC の登録局管理者が行う。

資源申請者証明書の申請者の本人性確認は契約／資源管理者が行う。契約／資源管理者は、本 CPS「1.1.1.個人の認証」に基づき、資源申請者証明書の申請者の本人確認を実施する。契約／資源管理者は、資源申請者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。

JPNIC 職員向け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。

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

契約／資源管理者は資源申請者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。契約／資源管理者は申請の審査に関して責任を負うものとする。

JPNIC の登録局管理者は契約／資源管理者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。JPNIC の登録局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、資源申請者証明書の申請登録を行う契約／資源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。

JPNIC 職員向け証明書に関しては、本認証局が申請の諾否を決定する。

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

契約／資源管理者は、資源申請者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。

JPNIC の登録局管理者は契約／資源管理者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、契約／資源管理者又は JPNIC の登録局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。

JPNIC 職員向け証明書に関しては、本認証局は、本 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。

サーバ証明書に関しては、本認証局は、本 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、契約／資源管理者からの資源申請者証明書の発行申請登録を受け付けるにあたって、予め定められた方法により契約／資源管理者の権限確認を行う。また契約／資源管理者証明書の発行申請登録を受け付けるにあたって、予め定められた方法により契約／資源管理者の権限確認を行う。本認証局は、申請登録の真正性を確認した後、資源申請者証明書の申請者に対し、本 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、資源申請者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資源申請者証明書の申請者に対し証明書を発行する。

本認証局は、契約／資源管理者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、オフラインの手段を介して契約／資源管理者証明書の申請者に対し証明書を発行する。

JPNIC 職員向け証明書に関しては、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。

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

契約／資源管理者証明書はオフラインの手段により申請者に対し発行通知を行う。

本認証局は、証明書発行に必要な 2 種類の情報を生成し、二つの異なる方法を用いて契約／資源管理者経由で資源申請者証明書の申請者へ通知する。

JPNIC 職員向け証明書に関しては、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。

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

契約／資源管理者証明書に関してはオフラインの手段を使い受領する。証明書に不具合がある場合は JPNIC へ連絡を行う。配達後一週間後までに連絡がない場合は受領したとみなす。

本認証局は、到達確認のできる方法で契約／資源管理者の証明書を配達する。資源申請者証明書の申請者による証明書のダウンロードし、確認した上で受領するものとする。証明書に不具合がある場合は契約／資源管理者を通じて JPNIC へ連絡を行う。ダウンロード後一週間後までに不具合の連絡がない場合は受領したとみなす。

JPNIC 職員向け証明書に関しては、本認証局は予め規定されたオフラインの手段を使う方法により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

本認証局は、本 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 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る。

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 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 CPS「4.7.証明書の鍵更新」に定める手続とする。

4.6.1. 証明書更新が行われる場合

規定しない。

4.6.2. 証明書の更新を申請することができる者

規定しない。

4.6.3. 証明書の更新申請の処理

規定しない。

4.6.4. 所有者に対する新しい証明書の通知

規定しない。

4.6.5. 更新された証明書の受領確認の行為

規定しない。

4.6.6. 認証局による更新された証明書の公開

規定しない。

4.6.7. 他のエンティティに対する通知

規定しない。

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 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 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 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 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 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 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 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 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 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 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 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 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

資源申請者証明書の証明書所有者は、契約／資源管理者に証明書の失効申請を行わなければならない。

契約／資源管理者証明書の証明書所有者は、JPNIC に証明書の失効申請を行わなければならない。

本認証局は次の項目に該当すると認めた場合、いずれの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
- 証明書所有者あるいはローカル RA が、本 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本認証局は、証明書所有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、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 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

資源申請者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ローカル RA 責任者、契約／資源管理者
- 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

契約／資源管理者は所定の手続きに従って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。

JPNIC は所定の手続きに従って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、失効申請の受領後、5 営業日以内に行われる。

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/ステイタス確認の適用性

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/ステイ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. 証明書の一時停止の場合

本認証局は、発行した証明書の一時停止を行わない。

4.9.14. 証明書の一時停止を申請することができる者

規定しない。

4.9.15. 証明書の一時停止申請手続き

規定しない。

4.9.16. 一時停止を継続することができる期間

規定しない。

4.10. 証明書のステイタス確認サービス

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イ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 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 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 CPS「2.1.リポジトリ」に規定する。

4.10.3. オプショナルな仕様

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。

4.12.1. キーエスクローと鍵回復ポリシ及び実施

規定しない。

4.12.2. セッションキーのカプセル化と鍵回復ポリシ及び実施

規定しない。