JPNIC 資源管理認証局
認証業務規程
（Certification Practice Statement）

Verions 1.0

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

目次

1. はじめに

1.1. 概要

本 JPNIC 資源管理認証局 認証業務規程（以下、CPS という）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 という）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 資源管理認証局（以下、本認証局という）の認証業務に関する運用規則を定める。

本認証局は、本 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、資源申請者という）等に証明書を発行する等の認証サービスを提供する。本認証局は実験としての位置づけで運用される。

本 CPS の構成は、IETF PKIX WG において標準化されている RFC3647「証明書ポリシ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）及び CPS（認証実施規程）をそれぞれ独立したものとして定めず、本 CPS として証明書ポリシ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、証明書所有者及び証明書検証者の義務等を、本 CPS、証明書所有者同意書によって包括的に定める。なお、本 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Webページ上（http://jpnic-ca.nic.ad.jp/）に公開する。

(1)CPS

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 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 CPS の正式名称は「JPNIC 資源管理認証局 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 資源管理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	1.2.392.200175
JPNIC 資源管理認証局 認証業務規程（CPS）	1.2.392.200175.1.2.1
EE 証明書ポリシ	1.2.392.200175.1.2.1

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 コミュニティに関係する登場者と役割

登場者	略称	役割、説明
資源申請者		IP アドレス及び AS 番号の割当て・返却等の業務を行う者
サーバ		本認証業務に用いる JPNIC のサーバ
資源申請者証明書		資源申請者に対して発行される証明書
契約／資源管理者		資源申請者の任命及び解任、委任等を行う者
契約／資源管理者証明書		本認証局の認証業務に必要な運用用証明書の一つ。資源申請者への証明書発行時の契約／資源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。
JPNIC 職員向け証明書		本認証局の認証業務に必要な運用用証明書の一つ。IP レジストリシステムにおける契約／資源管理者の識別子の管理等の業務を行う JPNIC の職員に対して発行される証明書
エンドエンティティ	EE	証明書の発行対象である、資源申請者、契約／資源管理者、JPNIC 職員の総称
エンドエンティティ証明書	EE 証明書	EE に発行される証明書の総称
証明書申請者	申請者	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 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/又はディジタル署名に依拠して行動する者

登場者	略称	役割、説明
JPNIC 発行局	JPNIC IA	JPNIC ルート認証局内の発行局及び JPNIC 資源管理認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 資源管理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。
担当理事		JPNIC セキュリティ事業の担当理事。JPNIC 認証局の運営方針の決定等を行う。
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（資源管理認証局）の証明書に電子署名を行う。
JPNIC 資源管理認証局		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 資源管理認証局証明書は、JPNIC ルート認証局により電子署名される。
JPNIC 認証局		JPNIC が運営を行う認証局の総称。
ローカル RA		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ローカル RA となる。

登場者	略称	役割、説明
ローカル RA 責任者		IP アドレス管理指定事業者の中における、ローカル RA 業務の責任者。契約／資源管理者の任命・解任を行う。
契約／資源管理者	契約／資源管理者	IP アドレス管理指定事業者の中で、資源申請者のメンバ管理と認証及び資源申請者証明書の発行申請操作を行う。

1.3.2. その他の関係者

規定しない。

1.4. 証明書の使用方法

1.4.1. 適切な証明書の使用

本 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がユーザ及びメッセージを検証する為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 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る。また JPNIC は、IP アドレス管理指定事業者の資源申請者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 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 （年末年始／祝祭日は除く） 10:00～18:00

電子メールアドレス：（ca-query@nic.ad.jp）

1.5.2. CPS のポリシ適合性を決定する者

本 CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の担当理事が行う。

1.5.3. CPS 承認手続

本 CPS の改定は、担当理事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 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 CPS では、特に断らない限り資源申請者証明書、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 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。
RFC 3647（Request For Comments 3647）		認証局 や PKI のための 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。

用語	略称	説明
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。