2015/05/13 第 109 回理事会
資料 8-2

JPNIC プライマリルート認証局 CPS 案
(Certification Practice Statement)

Version 1.2

一般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

改訂履歴

版数	改訂日	内容
1.0	2009 年 5 月 15 日	初版作成
1.1	2011 年 12 月 16 日	署名アルゴリズム(SHA-256)の追加 認証局名称(S2)の追加
1.2	2015 年 5 月 13 日	署名アルゴリズム(SHA-1)の削除 認証局名称(S1)の削除

目次

1. はじめに（Introduction）

1.1. 概要（Overview）

JPNIC プライマリルート認証局（以下、本認証局と呼ぶ）は、JPNIC が行なう認証サービスにおいて最上位に位置する認証局であり、下位認証局他に対して発行した電子証明書の正当性を JPNIC が証明する目的で運営されるものである。

JPNIC は、JPNIC の認証サービスを利用する者他に対して本認証局が行う業務の信頼性や安全性を示すため、本認証局の業務実施に関わる方針と、その方針の適用方法をまとめた JPNIC プライマリルート認証局 CPS（Certification Practice Statement）（以下、本 CPS と呼ぶ）を策定する。本認証局は、本 CPS に則って運用される。

JPNIC における本認証局の運営、および本 CPS の策定は、JPNIC プライマリルート認証局運営規程に則って行なわれる。

本 CPS は、IETF において策定された RFC3647[1]に基づいて構成される。また、本 CPS には CP（Certificate Policies ― 証明書ポリシ）が記述される。

1.2. 文書の名前と識別（Document Name and Identification）

本 CPS の名称とオブジェクト識別子[2]を表 1-1 に示す。

表 1-1　名称とオブジェクト識別子

CPS の名称（日本語）	JPNIC プライマリルート認証局 CPS
CPS の名称（英語）	JPNIC Primary Root Certification Authority CPS
オブジェクト識別子	1.2.392.00200175.2.0

1.3. 関係者（PKI Participants）

本認証局に関わる主体と役割を表 1-2 に示す。

[1] RFC3647, “Certificate Policy and Certification Practices Statement Framework”（証明書ポリシと認証実践の枠組み）

[2] 登録機関（ISO、ITU-T）に登録された国際的に一意となる値。国内では電子商取引推進センターと総務省が登録業務を行っている。

表 1-2　本認証局に関わる主体と役割

名称	略称	役割、説明
証明書申請者		本認証局に対して、証明書の発行申請を行う主体を表す。
証明書所有者	所有者	本認証局により証明書の発行を受けた主体を表す。本 CPS では、JPNIC の下位認証局をいう。
証明書検証者	検証者	本認証局の証明書を用いて、電子証明書等の検証を行い、その結果に依拠して行動する主体を表す。
JPNIC プライマリルート認証局発行局	発行局	JPNIC プライマリルート認証局発行業務をつかさどる主体を表す。登録局より依頼された証明書の発行を行う。 認証局の内、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する。
JPNIC プライマリルート認証局登録局	登録局	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主体をあらわす。
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機能を表す。
JPNIC 下位認証局	下位認証局	JPNIC プライマリルート認証局により証明書の発行を受ける認証局、下位認証局を表す。
JPNIC 認証局		JPNIC が運営を行う認証局の総称。JPNIC プライマリルート認証局、JPNIC で運営される下位認証局で構成される。
下位認証局証明書		JPNIC プライマリルート認証局が、下位認証局に対して発行する証明書を表す。
JPNIC プライマリルート認証局認証局運用責任者	認証局運用責任者	下位認証局の設置を運営委員会に発議する。認証局運用責任者は、運営委員会によって指名される。
JPNIC プライマリルート認証局運用担当者	認証局運用担当者	登録局（RA）を管理し運用する者。証明書発行、失効の登録作業を行う。また認証局システムを運用管理する。

1.4. 証明書の使用方法（Certificate Usage）

1.4.1. 適切な証明書の使用

本 CPS に基づき発行される下位認証局証明書は、当該認証局の発行する公開鍵証明書の検証のために使われるものとする。

1.5. 組織内の CPS 管理（Policy Administration）

1.5.1. 文書を管理する組織及び連絡担当者

一般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　セキュリティ事業担当

電子メールアドレス：ca-query at nic.ad.jp

at を@に置き換えること。

受付時間は、JPNIC 事務局の問い合わせ受付時間に準ずる。

1.5.2. 承認手続き

本 CPS の承認は、別途定められた JPNIC プライマリルート認証局運営規程に則って行なわれる。

1.5.3. 改訂手続

本認証局は、証明書ポリシ及びその保証、義務に著しい影響を与えない範囲で、本 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 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。

1.5.4. 通知方法及び期間

本認証局は、変更された CPS をその改訂が有効になる一ヶ月前までにリポジトリ

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。

2. 情報公開とリポジトリ（Publication and Repository Responsibilities）

2.1. 情報公開

本認証局は、次の情報をリポジトリで公開する。

- 自己署名証明書
- 下位認証局証明書
- CRL
- CPS

リポジトリは下記の URL でアクセスできるものとする。

http://jpnic-ca.nic.ad.jp/

また、本認証局の証明書のフィンガープリントは紙面にて公開される。

なお、便宜上、リポジトリより https 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 URL を次に示す。

http://serv.nic.ad.jp/capub/fingerprint.html

2.2. リポジトリ（情報公開機能）

本認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように可能な範囲で維持管理を行う。但し、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に通知なく停止することがある。

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。

- CPS、自己署名証明書、リンク証明書、下位認証局証明書は、改訂の都度、公表される。
- ARL（Authority Revocation List：機関失効リスト）については、本 CPS「4.9.5 機関失効リストの発行頻度」で規定される頻度で公開される。
- 認証局に関する重要情報若しくはその他の情報は、その重要性に応じて適宜更新が行われる。

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制御は行わない。

3. 識別名と認証要件（Identification and Authentication (I&A)）

3.1. 証明書に記載される識別名（Naming）

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証明書において一意とする。

3.2. 初回の本人性確認（Initial Identity Validation）

3.2.1. 証明書申請者の確認

本認証局は、証明書申請者が、下位認証局の組織に関する情報の申請を行うための正当な権限を有していることを確認する。

3.2.2. 私有鍵（private key）の所持の確認

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を利用し、本認証局が認めた方法を通じて、証明書申請者が私有鍵を所有していることを確認する。

3.3. 鍵更新申請時の本人性確認と認証（I&A for Re-key Requests）

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（I&A for Revocation Requests）

本認証局は、証明書の失効申請を受け付けた場合、下位認証局の組織に関して提供された情報をもとに、正当な失効要求であることを確認する。

4. 証明書ライフサイクルにおける認証局運用要件
（Certificate Life-Cycle Operational Requirements）

4.1. 証明書申請（Certificate Application）

4.1.1. 証明書申請を提出することができる者

証明書の発行申請を行うことができる者は、下位認証局の運用責任者とする。

4.1.2. 登録手続の要件

証明書申請者は、証明書を申請するにあたって、本認証局に次の情報を提供するものとする。

- 証明書発行申請書
- 認証局運用責任者による承認を受けていることを示す情報
- CPS
- CSR（Certification Signing Request）

また、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. 証明書申請に関わるプロセス（Certificate Application Processing）

4.2.1. 本人性確認と認証機能の実行

本認証局は、本 CPS「3.2.初回の本人性確認」に基づき、証明書申請者の本人確認及び組織確認を行う。

4.2.2. 証明書申請の承認又は却下

本認証局は、証明書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。申請を受理するにあたっては、認証局運用責任者の承認の確認を行うものとする。

4.3. 証明書発行（Certificate Issuance）

4.3.1. 発行プロセス

本認証局は、証明書申請者から提出された CSR の公開鍵に対し、本 CPS「7.1.証明書プロファイル」に準じた内容で、本認証局の署名を付した証明書を発行する。

4.4. 証明書の受け渡し（Certificate Acceptance）

4.4.1. 認証局による証明書の公開

本認証局に発行された証明書は、本 CPS「2 情報公開とリポジトリ」に規定する証明書をリポジトリにて公開する。

4.4.2. 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（Key Pair and Certificate Usage）

4.5.1. 所有者の私有鍵及び証明書の使用

本認証局が発行する証明書の用途は、証明書の発行対象である組織が提供するサービス又は製品に定められている用途に制限されるものとする。

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
- 利用目的の確認
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

4.5.2. 証明書検証者の要件

証明書検証者の要件を以下に示す。

- 証明書を信頼する時点で、本 CPS の理解
- 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
- 証明書検証

4.6. 証明書の更新（Certificate Renewal）

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」に定める手続をとる。

4.7. 証明書の鍵更新（Certificate Re-key）

4.7.1. 新しい公開鍵を含む証明書申請者の要件

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。

4.8. 証明書の変更（Certificate Modification）

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

4.9. 証明書の失効と一時停止（Certificate Revocation and Suspension）

4.9.1. 証明書失効

証明書所有者は、次の場合に、本認証局に対し証明書の失効申請を行う。

- 証明書記載事項に変更があった場合
- 私有鍵が危殆化、若しくはそのおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

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、証明書の失効処理を行う。

- 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
- 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

証明書の失効要求ができる者は、次に示す。

- 証明書所有者
- 本認証局
- その他 JPNIC が指定した者

4.9.3. 失効申請手続

証明書の失効申請を行う者は、証明書失効に関する必要な情報をオフラインにて提出することにより、本認証局に証明書の失効申請を行う。

なお、本認証局が自身の判断により証明書の失効を行うことがある。

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. 機関失効リストの発行頻度

ARL は証明書失効の有無にかかわらず、一定期間で更新を行う。更新頻度は規程しないが、証明書失効がない場合は 1 年を目処とする。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。

4.9.6. 機関失効リストの発行最大遅延時間

本認証局は、ARL が生成された後、速やかにリポジトリに公開する。

4.9.7. 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提供しない。

4.9.8. 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、証明書所有者に対して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。

4.9.9. 証明書の一時停止

本認証局は、発行した証明書の一時停止を行わない。

4.9.10. 証明書ステータス情報の提供（Certificate Status Services）

本認証局は、証明書の有効性の確認手段として 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。

5. 設備上、運用上の管理（Facility, Management, and Operational Controls）

5.1. 物理的管理（Physical Security Controls）

5.1.1. 立地場所及び構造

本認証局に係わる重要な設備は、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。また本認証局は、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、適切な入退室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。

5.2. 手続的管理（Procedural Controls）

5.2.1. 役割

JPNIC プライマリルート認証局運営規程に則って行なわれる。本認証局に関わる役割を表 5-1 に示す。

表 5-1 名称とその役割

役割名称	役割の説明
認証局運用責任者	・ 認証サービス及び運用組織の統括 ・ 運用担当者の任命・解任 ・ 非常時対応等の指揮、監督
運用担当者	・ 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 ・ 証明書発行、失効の登録作業 ・ 登録局の管理運用 ・ 運用記録の保管・管理等 ・ その他、運用全般の管理
鍵管理者	・ 鍵保管設備による私有鍵の管理 ・ 認証局鍵廃棄時の立会い ・ バックアップ私有鍵の管理

5.3. 業務におけるセキュリティ制御

認証局設備の保守、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。

5.4. 運用に携わる者のセキュリティ管理（Personnel Controls）

5.4.1. 資格、経験及び身分証明の要件

本認証局の運用に携わる者は、JPNIC 職員に限られる。

5.5. 監査ログの手続（Audit Logging Procedure）

5.5.1. 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記録として、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
- 証明書の発行
- 証明書の失効
- ARL の発行　　等

5.5.2. 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。

5.6. 記録の保管（Records Archival）

5.6.1. アーカイブ

本 CPS「5.5.1.記録されるイベントの種類」に規定する記録に加えて、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の記録を維持、管理する。

- 本 CPS 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
- 証明書の発行、失効時に提出を受ける申請書
- 証明書申請者の真偽を確認するために提出を受けた書類
- 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
- 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

5.7. 危殆化及び災害からの復旧（Compromise and Disaster Recovery）

5.7.1. 事故及び危殆化の取扱手続

本認証局の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. コンピューター資源の破損

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. 私有鍵が危殆化した場合の手続き

本認証局の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。

- 下位認証局証明書等の失効手続
- 私有鍵の廃棄及び再生成手続
- 下位認証局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。

6. 技術的セキュリティ管理（Technical Security Controls）

6.1. 鍵ペアの生成及びインストール（Key Pair Generation and Installation）

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、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 JPNIC 下位認証局の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

JPNIC 下位認証局の公開鍵は、本 CPS「3.2.1 証明書申請者の確認」に定める手続により検証され、その受渡しはオフラインで行う。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の公開鍵の配布は、本認証局の登録局管理者が、下位認証局証明書の管理者に対して、手渡しによって行う。検証者に対する本認証局の公開鍵の配布は、安全かつ確実な手段により行う。

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。

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、規定しない。

6.1.7. 鍵用途の目的

本認証局の私有鍵は、発行する証明書及び CRL への署名に使用する。証明書の *keyUsage* は *keyCertSign*、*cRLSign* のビットを使用する。

6.2. 私有鍵の保護及び暗号モジュール技術の管理（Private Key Protection and Cryptographic Module Engineering Controls）

6.2.1. 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。

6.2.2. 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行われる。

6.2.3. 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場合には、私有鍵の格納されたメディア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関しても同様の手続によって破棄する。

JPNIC 下位認証局の私有鍵は、当該認証局自身で確実に破棄するものとする。

6.2.4. 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（Other Aspects of Key Pair Management）

6.3.1. 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 20 年、私有鍵の有効期間は 10 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。

6.4. 活性化データ（Activation Data）

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。また定期的に変更を行う。

6.4.3. 活性化データの他の考慮点

活性化データは、JPNIC において別途定められるセキュリティ管理手順に則って行われる。

6.5. コンピューターのセキュリティ管理（Computer Security Controls）

6.5.1. 特定のコンピューターのセキュリティに関する技術的要件

システムに対して行われた重要な操作については、全て記録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。

6.5.2. セキュリティ運用管理

本認証局のセキュリティ運用管理は、JPNIC において別途定められるセキュリティ管理手順に則って行われる。

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。

7. 証明書と機関失効リスト（Certificate, ARL Profiles）

7.1. 証明書のプロファイル（Certificate Profile）

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。本認証局は、使用するアルゴリズムを移行するため、証明書プロファイルが異なる複数の証明書を発行する。これらは識別名の末尾につけた「S」＋番号で識別する。証明書プロファイルを、表 7-1 に示す。

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*[3]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

本認証局が発行する証明書は全て *keyCertSign* と *cRLSign* のみを使用する。この拡張は *critical* である。

[3] non-critical - 証明書検証時、当該フィールドを解釈できない場合でも処理を継続することを示すフラグの値

7.1.2.4. certificatePolicies

下位認証局証明書は *certificatePolicies* 拡張を使用する。*policyIdentifier* の値は本 CPS「7.1.6.証明書ポリシ OID」、*policyQualifiers* の値は本 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。

自己署名証明書は *certificatePolicies* 拡張を使用しない。

7.1.2.5. cRLDistributionPoints

下位認証局証明書及びリンク証明書は、*cRLDistributionPoints* 拡張を使用する。*distributionPoint* として、本認証局が発行する CRL の URL 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（オブジェクト識別子）

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 を以下に示す。

- *sha256WithRSAEncryption*（1.2.840.113549.1.1.11）
- *rsaEncryption*（1.2.840.113549.1.1.1）

7.1.4. 名前形式

本 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 OID

下位認証局証明書は、本 CPS「1.2.文書の名前と識別」に定める下位認証局証明書ポリシの 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

下位認証局証明書は、ポリシ修飾子の値として本 CPS が公開されている URI を使用する。

7.1.9. 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 プライマリルート認証局が発行する証明書プロファイル

Field	critical flag	下位認証局 証明書	JPNICプライマリルート 認証局証明書
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha256WithRSAEncryption	sha256WithRSAEncryption
parameters		null	null
issuer	NA	PrintableString*2	PrintableString*2
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime notBeforeの時刻より10年後	UTCTime notBeforeの時刻より20年後
subject	NA	PrintableString*1	PrintableString*2
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		JPNIC 下位認証局 公開鍵のBIT STRING	JPNICプライマリルート認証局 公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNICプライマリルート認証局 公開鍵の160bit	JPNICプライマリルート認証局 公開鍵の160bit
authorityCertIssuer		使用しない	使用しない
authorityCertSerialNumber		使用しない	使用しない
subjectKeyIdentifier	n	JPNIC 下位認証局 公開鍵のハッシュ値	JPNICプライマリルート認証局 公開鍵のハッシュ値
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		本CPのOID	使用しない
policyQualifiers			
policyQualifierId		CPSUri	使用しない
qualifier		本CP/CPSを公開するURL	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		CRLを公開するURI	使用しない
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

*1　JPNIC 下位認証局の識別名

*2　値は C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 とする。

7.2. 機関失効リストのプロファイル（ARL Profile）

本認証局が発行する ARL（Authority Revocation List : 機関失効リスト）は、X.509 CRL フォーマットのバージョン 2 に従う。CRL プロファイルを、表 7-2 に示す。

7.2.1. バージョン番号

本認証局が発行する ARL 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

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

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 プライマリルート認証局が発行する ARL プロファイル

Field	critical flag	証明書失効リスト
version	NA	1
signature	NA	
algorithm		sha256WithRSAEncryption
parameters		null
issuer	NA	PrintableString*1
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより1年後
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 ルート認証局 公開鍵の160bit

*1 値は C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 とする。

8. 準拠性監査とその他の評価 (Comliance Audit and Other Assessment)

規定しない。

9. 他の業務上の問題及び法的問題 (Other Business and Legal Matters)

規定しない。