JPNIC プライマリルート認証局 CPS の制定および JPNIC プライマリルート認証局の設置について

インターネット推進部

■1. 概要

JPNIC プライマリルート認証局運営規定第 7 条第 2 項の定めに従い、JPNIC プライマリルート認証局 CPS の制定をお諮りする。また本 CPS 案に基づく JPNIC プライマリルート認証局の設置をお諮りする。

はじめに JPNIC プライマリルート認証局の概要を示し、次に本認証局の設置に必要な CPS（Certification Practice Statement）案を示す。

■2. JPNIC プライマリルート認証局の概要

JPNIC プライマリルート認証局（以下、本認証局と呼ぶ）は JPNIC が行う認証サービスにおいて最上位の認証局である(図 1)。

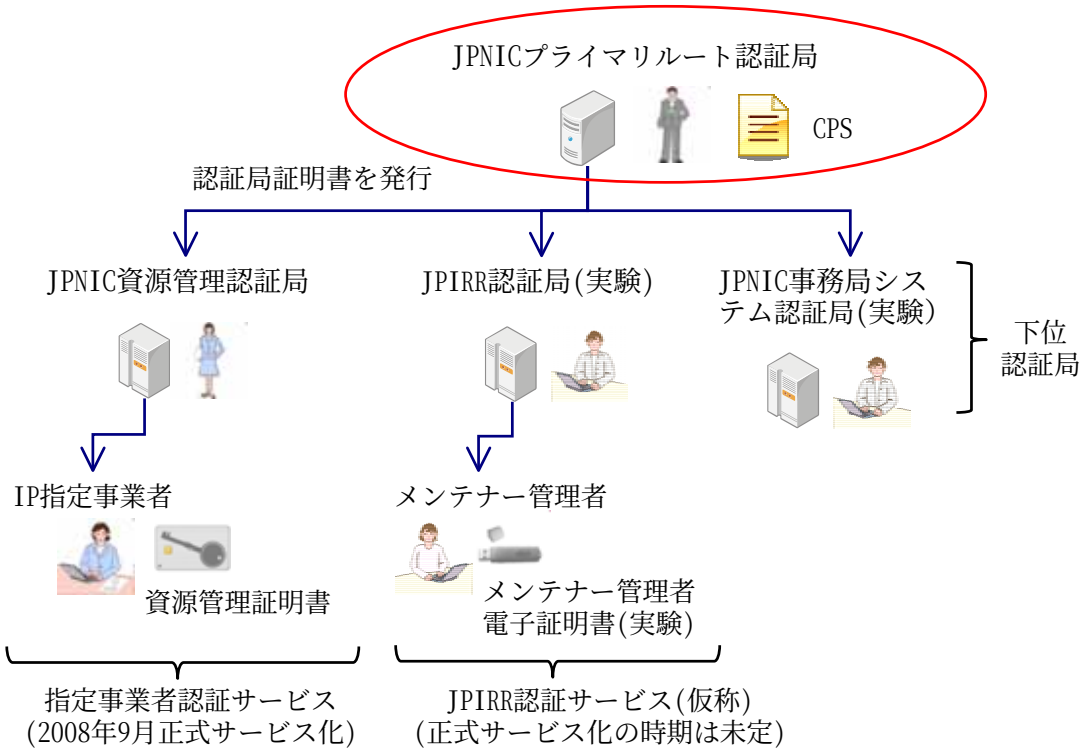

図 1　最上位の認証局である JPNIC プライマリルート認証局

図 1 の左下に示した「指定事業者認証サービス」は 2008 年 9 月に正式サービスを開始した。JPNIC プライマリルート認証局の設置は、現在実験を行っている他の認証サービスを正式サービス化するために是非とも必要である。指定事業者認証サービスのみの場合でも、JPNIC プライマリルート認証局が設置されていることが望ましい。

■3. JPNIC プライマリルート認証局 CPS 案

JPNICプライマリルート認証局運営規程第 7 条第 2 項の定めに従い、JPNICプライマリルート認証局運営委員会（以下、運営委員会と呼ぶ）にてCPS案を作成した[1]。CPS案の章立てを以下に示す。認証局運営委員会は、本認証局の運用の要件と運用の実態を確認した上で、各章の記述内容を確認した(表 1)。

表 1　JPNIC プライマリルート認証局 CPS 案の内容

CPS の各章	内容
1.概要 （認証局の名称や目的の説明）	本認証局は、JPNIC が、下位認証局に対して発行した電子証明書の正当性を証明する目的で運営される。
2.情報公開とリポジトリ （文書とデータ公開機能の説明）	本認証局の CPS は Web で公開される。認証局証明書(電子データ)も Web で公開する。
3.識別名と認証要件 （証明書に記載される ID や証明書申請者に対する確認事項）	本認証局は、下位認証局が私有鍵を確かに有することを確認する。
4.証明書ライフサイクルにおける認証局運用要件 （発行・失効・有効期限切れの各手続の要件）	本認証局は JPNIC の下位認証局に証明書を発行する。発行申請を行うことができるのは、下位認証局の運用責任者である。
5.設備上、運用上の管理 （設備が備える要件や運用で実施すること）	私有鍵を保管する施錠された室は、火災や地震から守られ、権限を有する者以外はアクセスできない。私有鍵の操作は記録される。
6.技術的セキュリティ管理 （暗号技術やシステム）	認証局の鍵は、危殆化の可能性が低いアルゴリズムで、かつ破ることが難しい程度に十分なビット長を持つ。私有鍵は封入されて保管される。
7.証明書と証明書失効リスト （証明書の形式や記述事項）	本認証局の認証局は、下位認証局よりも長い期間、有効である。本認証局自体の証明書の有効期限を 20 年とし、本認証局が発行する証明書の有効期限を 10 年とする。
8.監査とその他の評価 （監査が行われる事項）	本章の内容は規定しない。
9.他の業務上の問題及び法的問題 （料金、個人情報の保護、保証内容など）	料金、個人情報の保護などは本認証局の対象とする業務に含まれない。本章の内容は規定しない。

※特に注意すべきものを太枠で示す。太枠外は認証局の一般的な記述である。太枠外の 1 章から 4 章、及び 7 章には認証局の目的や技術情報を記述した。運用の実態は 5 章と 6 章に記述した。8 章と 9 章の内容は規定しないものとした。

■4. JPNIC プライマリルート認証局の設置

JPNIC プライマリルート認証局運営規定の第 5 条第 1 項の定めに従い、3 項で述べた CPS を定め、JPNIC プライマリルート認証局の設置をお諮りする。

以上

[1] JPNIC プライマリルート認証局運営委員会　開催日時
第 1 回　2009 年 4 月 24 日(金) 13:40～14:30
第 2 回　2009 年 5 月 1 日(金) 14:20～15:00