第6章 認証業務規程（CPS）の更新

内容

- 再検討の目的
- コミュニティの定義
- 前提条件の整理
- ギャップの整理

第6章 認証業務規程（CPS）の更新

6.1. CPS の再検討の目的

CPS（Certification Practice Statement：認証業務規程）は、認証局がその業務方針を明文化した文書である。認証局において CPS の公開は任意であり、CPS なくして認証局はありえないかというとそうではないが、商取引や政府認証基盤といった多くのユーザを収容する規模の認証局の多くは CPS を定め公開している状況がある。2002 年度「IP アドレス認証局のあり方に関する調査研究」では日本における特定認証業務のガイドライン、米国およびカナダにおける WebTrust for CA といった認証局の監査基準の調査研究を行ったが、これらの監査はすべて CPS を基にして行われる。

CPS を定め、公開するには大きく分けて二つの意味がある。一つは認証局の運用主体が、その認証局の位置づけや役割、規模といった事項を再認識し業務の適正化を図る基準にするという意味である。もう一つはその認証局が発行した証明書を検証する際の判断基準である。証明書検証者は認証局を「信頼できる第三者」として位置づけ、検証しようとしている証明書の信頼性を測ろうとする。なぜなら証明書の発行自体に信憑性がなければ、認証相手の正しさ（なりすましや偽造行為）を検証するができない為である。

IP アドレス認証局は自然人を認証することを目的としていない為、特定認証業務の業務レベルとは性質が異なる。また WebTrust for CA のような「Web サーバ証明書」の発行を目的としたものでもない。しかしインターネットにおけるアドレス資源の管理を行うインターネットレジストリにおいて実施される認証業務である。本報告書の第 6 章で述べるように、インターネットを使うノードの間での認証に証明書が使われる可能性を持っている。

2003 年度や 2004 年度の IP アドレス認証局に関する報告書で述べてきたように、アドレス資源の信頼性はインターネットの運用の信頼性を左右する要素である。安全な運用を図る為のアドレス資源の元本としての登録情報は、十分に強い方式を使いかつ現実的な運用によって登録者を認証し、登録内容の信頼性向上と公開時の原本性の確保が必要となるであろう。登録情報の公開（whois）はインターネットを利用する多くのユーザに対して意味を持つ。

このような背景を受け、IP アドレス認証局の CPS は 2003 年度よりドラフト作成を開始し、認証業務の定義づけを行ってきた。2004 年度は認証局システムの構築によって、いよいよ証明書検証者に対する信頼の確立が必要になる。しかし 2004 年度に行った認証局の構築活動から、2003 年度にドラフトした CPS から修正が必要になることがわかってきた。例えば認証業務の規模はより簡易になり、認証局システムで利用される機器構成や設備が具体的になってきた。そこで 2004 年度は、具体化してきた認証業務を受けて CPS の全面的な見直しを行った。

CPS の編纂作業は、CPS に関する知識とノウハウが必要になる作業である。本章では当センターで行った CPS の見直しの内容について述べ、IP アドレス認証局の業務規程について述べると共に、多くの認証局で懸案事項となっている CPS を編纂に関する

参考情報となるよう、そのプロセスについて述べる。

6.2. CA とアプリケーション専門家チーム

CPS に関する検討や記述には、認証技術としての PKI に関する知識だけでなく証明書の運用業務や証明書管理の手法といった知識を必要とする。また CPS として記述するための問題点・記述の分解作業が必要である。これらの作業を進める為、当センターでは「専門家チーム」と呼ばれるチームを設立し、CPS の見直し作業を行なった。

CA とアプリケーション専門家チームの活動主旨を以下に示す。

6.2.1. 活動内容

a. メーリングリストにおける意見交換
   CP/CPS 記述上の論点をまとめるための議論を行った。

b. 個別会議の開催
   CP/CPS の検討方針について議論と論点整理を行なう為、個別の会議を行った。
   人数は一名ないし二名の少人数を想定し、12 月から月に二回の開催を想定した。

c. 全体レビュ会議の開催
   ML と個別会議等を通じて明らかになった論点と記述についてレビュを行い
   CP/CPS での記述方法について具体的な検討を行った。1 月と 2 月の二回の開催を想定した。

6.2.2. 活動スケジュール

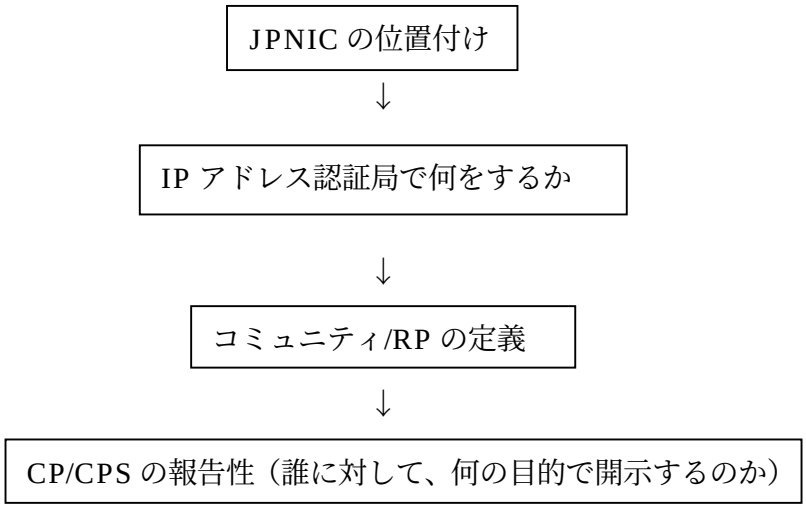
2004 年 12 月　専門家チームを編成し、検討方針の決定と CP/CPS 記述上の論点整理を行った。
2005 年 1 月　論点ごとに記述案をまとめ、全体レビュ会議にかける。そこで課題抽出を行った。
2005 年 2 月　1 月の全体レビュ会議で明らかになった課題に対して行った対策についてレビュを行い、CP/CPS をまとめる為に必要な作業が更にあればその検討を行った。
2005 年 3 月　CP/CPS 文書としてまとめた。

6.2.3. 作業手順

はじめに CPS の記述に取り掛かる前に検討順序を定めた。

6.2.3.1. 検討順序と項目

2003 年度にドラフトした CPS を元に、下記の検討順序のうち前半は概ね明らかになっていた。しかし「IP アドレス認証局で何をするか」には JPNIC による登録者の認証用途に限定するか JPNIC に情報登録を行っている日本のインターネットコミュニティの中でユーザ同士が認証に用いることが出来るようにするのか、という異なる二つの目的が挙がっていた。



CPS では認証用途に限定し RP（Relying Party）等を想定した。RP とは主に証明書検証者を指し、認証局を信用し証明書の信頼性に基づいた行動（認証行為と一連の処理）行う主体のことである。

次に 2003 年度の CPS とのギャップの分析を行った。

1. ギャップの整理
   - 制約条件（コスト等）からのギャップ
   - 方針の変更によるギャップ（RP を特定した等）
2. 前提条件の整理
   - RP、コミュニティ、CPS の目的
   - 制約条件（コスト、体制）
3. 検討課題
   - 論点
   - 各認証局の目的と用途

認証業務の目的や証明書の用途を限定することで、認証局に関わる主体が限定され、前提条件が整理された。

更に検討のスケジュールと重点を置く配分を決める為、既存の CPS の分量と重み付けを調査した。

章立てとページ数	（全体 127 ページ）
はじめに	17 ページ
一般条項	25 ページ
識別と認証	9 ページ
運用上の要件	34 ページ
建物人員設備	20 ページ
技術的なセキュリティ管理	14 ページ
プロファイル	6 ページ
仕様の管理	2 ページ

以下に、これらの検討の内容を述べる。

6.3. IP アドレス認証局の位置づけとコミュニティの定義

2003 年度および 2004 年度の検討の結果、IP アドレス認証局は細分化され役割ごとに異なる認証局を構築するものとした。
主に登録情報の登録者を認証する為の証明書を発行する IP アドレス認証局（認証）について行った検討について述べる。

はじめに JPNIC の役割を明文化する。しかしここでは詳細にせず主体と責任についてのみ記述する。

6.3.1. 認証局における JPNIC の役割

JPNIC は、IP アドレス認証局(認証)の運用主体。
認証の結果とその権限分離に対する責任を持つ。

次に IP アドレス認証局（認証）の業務の種別を検討した。

6.3.2. IP アドレス認証局で何をするか

JPNIC における認証のための証明書発行および失効を行なう。
ここで候補と考えられる認証業務を列挙し RP やコミュニティの違いを検討した。ここでは挙げられた A、B、C の三種類を以下に示す。

A. IP レジストリシステムによる IP 指定事業者(契約管理者、資源管理者、申請者)の認証

IP レジストリシステムは、本人性の確認ができた場合にログインを許可し、本人性に基づく権限の実施を許す。
なお IP レジストリシステムにもアカウントの失効機能がある。

認証対象の種別：

- IP 指定事業者(契約管理者、資源管理者)
  申請者の証明書の発行申請を行うことができる。
- 申請者
  アドレス資源の各種申請を行うことができる。

B. JPNIC 職員による IP 指定事業者(契約管理者、資源管理者、申請者)の認証

JPNIC 職員が IP 指定事業者のメッセージ認証と本人性確認と行なう。電子メールのやりとりの際に用い、暗号化と署名を用いる。認証対象の種別にも用いられる。

C. IP 指定事業者同士による IP 指定事業者(契約管理者、資源管理者、申請者)の認証

「すること」の拡大解釈であり、IP アドレス認証局(認証)は本認証に対する責任を一切持たない。

IP 指定事業者が、メッセージ認証と本人性確認に用いる。電子メールのやりとりの際に用い、暗号化と署名を用いる。認証対象の種別にも用いられる。

更にそれぞれについてコミュニティと RP の定義を行った。

6.3.3. コミュニティ/RP の定義

D. IP レジストリシステムによる IP 指定事業者(契約管理者、資源管理者、申請者)の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員 - RAA
- IP アドレス認証局(認証) 認証局システム
- IP レジストリシステム - RP
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - EE, RA, 申請者の任命
- IP 指定事業者 資源管理者 - EE, RA, 申請者の任命
- IP 指定事業者 申請者 - EE

E. JPNIC 職員による IP して事業者(契約管理者、資源管理者、申請者)の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員 - RP
- IP アドレス認証局(認証) 認証局システム
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - RA, EE, 資源管理者の任命
- IP 指定事業者 資源管理者 - RA, EE, 申請者の任命
- IP 指定事業者 申請者 - EE

F. IP 指定事業者同士による IP 指定事業者(契約管理者、資源管理者、申請者)
の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員
- IP アドレス認証局(認証) 認証局システム
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - RA, EE, RP, 資源管理者の任命
- IP 指定事業者 資源管理者 - RA, EE, RP, 申請者の任命
- IP 指定事業者 申請者 - EE, RP

更に CPS の報告性を文章化した。

6.3.4. CP/CPS の報告性（誰に対して、何の目的で開示するのか）

A. IP 指定事業者と一般に対して、認証用証明書の運用の信頼性を周知

本人性確認手段の運用レベルを一般に示すこと。目的は一般に参照される WHOIS に対する信頼性の向上。また申請者に対する認証強化への安心の提供。

B. 同上 ただし WHOIS は除く。

C. IP 指定事業者に対して、認証用証明書の運用の信頼性を周知

JPNIC における本人性確認手段の運用レベルを一般に示すことで、推測可能な本人性を提供する状況を作ること。

6.4. コミュニティに基づく前提条件の整理

前節の認証業務の候補からコミュニティを記述し比較を行った。

- RP
  業務 A：IP レジストリシステム(JPNIC)
  業務 B：IP レジストリシステム(JPNIC)、JPNIC 職員(JPNIC)
  業務 C：IP 指定事業者
- コミュニティ
  業務 A：
  IP レジストリシステム、契約管理者、資源管理者、申請者、IP 事業部担当者、認証局管理者、証明書管理者、運用責任者、理事会
  業務 B：
  業務 A＋JPNIC 職員
  業務 C：
  契約管理者、資源管理者、申請者、IP 事業部担当者、認証局管理者、証明書管理者、運用責任者、理事会
- CPS の目的
  業務 A：
  申請者の認証レベルを IP 指定事業者と一般に示す。
  間接的に whois の信頼性向上させるため。

  IP レジストリシステムにおける、契約管理者、資源管理者、申請者
  JPNIC 事業部担当者の認証業務を記述
  業務 B：
  登録者の認証強度を IP 指定事業者に示す。
  業務 C：
- 制約条件
  ・コスト
  認証業務は実験の位置づけの為、事業収入はない。
  ・体制
  理事会：理事
  認証局：担当 1、スタッフ 1
  IP 事業部：担当 1
- 各認証局の役割整理

  JPNIC ルート認証局：
  JPNIC のレジストリデータにおける(PKI)認証業務の信頼性を代表し認証業務を代表し、下位認証局を監督する権限を持ち、その証明書を失効することが可能。統一方針に従った管理を適用する。

IP アドレス認証局（認証）
　JPNIC の申請者認証の為の認証局で、JPNIC による IP 指定事業者の認証を目的とする。

IP アドレス認証局（証明）
　JPNIC の登録情報に基づいて証明書を発行し、ユーザ間の認証を目的とする。

業務 A、B、C の比較の結果、主に業務 B を対象とした CPS とすることにした。

6.5. ギャップの整理

RFC3647 のフレームワークを元に、2003 年度にドラフトした CPS とのギャップの整理を行った。この段階では単なる違いの洗い出しではなく、記述方針をできるだけ決めておくこととした。

- 制約条件（コスト等）からのギャップ

  ・(全体)
  当時は運用費用のシミュレーションを行なっておらず、運用内容に大きな幅があった。収入に基づいた運用を考慮し始めること自体が大きなギャップ。
  ・(システム維持費)
  システム維持費用の特定の根拠認証局システムの構築に、維持費用の特段の根拠はなく、最低のコストで External RA を実施するに留めた程度。

あとは個別に記述することにする。

- 方針の変更によるギャップ（RP を特定した等）

  上位概念的な懸案事項
  ・ IP アドレス認証局(認証)をツリーに含めるか
  ⇒ ツリーに入れると ISP の証明書を一般に検証できる状況ができる。
  IP アドレス認証局(認証)の認証業務が、ルート認証局の業務の信頼性に影響を持つことである。RP が異なるため、例えば一般の RP が認証用途の証明書を検証できる必要はない。

  これに対して組み立てたロジックは、ルート認証局はレジストリデータの業務の信頼性を代表する認証局であり、IP アドレス認証局(認証)の業務を監督する権限を持ち、その証明書を失効することが可能である。傘下に置くことによって、統一的な管理を適用する。

  報告書の本文に入るべき内容：
  ルート認証局の存在目的が決まると、ルート認証局の指導に従って IP アドレス認証局(認証)の CPS を見直す可能性がある。

  個別
  ・ ルート認証局の役割候補の列挙（本文）
  ・ IP アドレス認証局(認証)の鍵サイクル
  ⇒ 追加も可能
  ・ "ISP 管理者を（契約管理者、資源管理者）に分ける"等の違い

⇒ プロファイルの列挙。注にて対応。

6.6. RFC2527 に沿った更新の方針

2003 年度の CPS の検討は RFC2527 に沿って行われた為（当時の最新の RFC は RFC2527 であった)、検討内容と照らし合わせた更新案（該当部分のみ記述）を作成した。

- 契約管理者、資源管理者の本人特定 rfc2527:3.1.9

  契約管理者・資源管理者の本人特定方法の候補：

  - 指定事業者契約
  - 業務委託契約
  - 雇用契約書類
  - 電話確認

  既存の業務に従う。

  申請者の本人特定方法の候補：
  - 雇用契約書類
  - メール到達性

  「ホストマスタ業務をする人に発行してください。」と書く。
  CPS にて：「<Name>に入る名前は自然人を確認したものではない」

  発行申請に必要事項の候補：契約印、担当部署名、所在地、連絡先、担当者印、角印＋callback

- 失効時の本人確認方法 rfc2527:3.4

  契約管理者・資源管理者：
  - 指定事業者契約
  - 業務委託契約
  - 雇用契約書類
  - 電話確認

  申請者の本人特定方法の候補：

  - 雇用契約書類
  - メール到達性

失効申請：契約印、部署名 or 申請時の担当者印

運用に関わる事項（後に検討、ルール化）
・fingerprint の確認方法
・ハードウェアトークン送付方法（タンパーシールの使用）

・鍵の切り替え方法 rfc2527:4.7 ⇒ なし

・建物の要件：JPNIC マシンルームの想定に変更 rfc2527:5.1.2

認証設備室：（CA サーバ及び HSM を設置する部屋、以下同じ）
常時施錠とし、許可されたものだけが入室できるように管理する。
常時施錠された設備内で運用される。

入退室管理
"ＲＡシステム設備室"

・必要とされる人数 rfc2527:5.2.2

認証局システムサーバ ⇒ CA サーバ

キーセレモニーをはじめとする特に重要な業務については複数人
での実施する。特に重要な業務：キーセレモニー

－認証局 2 名（うち一名スタッフさん）
－IP 事業部 受付 1 ないし 2 名
－技術部 システム管理者 1 名

・5.3.8 要員に必要とされるべき文書
どこまで用意できるか（業務マニュアル）

「認証業務に必要となる文書を用意する。」でよい。

－業務手順書、書式、災害復旧計画書（新たな作成が必要とされている）
－操作マニュアル

・6.1.1 鍵ペアの生成主体
キーセレモニーどうするか検討

－キーセレモニー
　実験的な位置づけになりそうなので事務局内

FIPS-140-2level2 の認定の機器を利用し、複数人の立会いの元、
生成する。

・6.1.2 利用者への私有鍵の送付方法

－契約管理者・資源管理者：認証局で安全な方法で JPNIC で生成送付する。
　削除する（安全な削除方法をルール化）。
　配送されるトークンの保管場所

－申請者は申請者側で生成するので規定しない。

・6.1.9 鍵の使用目的
S/MIME を書いてしまってよいか。

・6.2.2 複数人による秘密鍵の管理
HSM の利用上、可能か確認
　－人員
　　「複数の要員」等とする。

・6.2.4 私有鍵のバックアップ
手順の確認
　－複数の CAO
　⇒CAO といわずに、「複数の要員」とする。

・6.2.7 私有鍵の活性化方法
複数の CAO が可能か確認
　－同上
　⇒CAO といわずに、「複数の要員」とする。

・6.5.1 信頼されるコンピューティング基本コンセプト
複数の CAO が可能か確認
　－同上
　⇒CAO といわずに、「複数の要員」とする。

・8.3 承認手続き
認証局の運営に関する承認主体

－運営委員会
⇒承認は必要

6.7. RFC3647 に沿った CP/CPS の更新案

最後に 2003 年度の CPS を記述に利用した RFC3647 のフレームワークに沿って、ギャップを整理しなおし記述方針を決定した。

●用語の変更
IP アドレス認証局 ⇒ IP アドレス認証局(認証)
LRA ⇒ メンバ管理者
＃契約管理者、資源管理者のことをさすが、CPS では総称する

●認証用認証局とすることの影響（リポジトリ-CRL,CPS のみ公開の影響）
2.1 リポジトリ
2.2. 証明情報の公開
2.3. 公開の時期又は頻度
2.4. リポジトリへのアクセス管理
3.4. 失効申請時の本人性確認と認証
4.5.2. 検証者の公開鍵及び証明書の使用
⇒「本認証局における証明書検証者は JPNIC 自身であるため規定しない」
でもよい。
6.1.4. 検証者に対する認証局の公開鍵の交付
⇒認証局証明書は公開

●LRA 契約という概念をなくすこと
4.1.1. 証明書申請を提出することができる者
＃単に認証されたメンバ管理者という扱いとする。
⇒「申請者」はメンバ管理者かホストマスタかわかりにくい。
また、ホストマスタが申請することにせず、メンバ管理者が
割り当てることにすれば、シンプルかつ実情に合う。

●認証局システムの開発内容の影響
4.1.2. 登録手続及び責任
⇒署名検証しているかＮＥＣに確認
4.3.1. 証明書の発行過程における認証局の行為
⇒IP 指定事業者からメンバ管理者としての任命を受けていることを
確認する。

●メンバ管理者はセンター発行であることの影響

4.3.2. 認証局の所有者に対する証明書発行通知
4.4.1. 証明書の受領確認の行為
⇒到達確認のできる方法で郵送する。
「PKI 環境」はわかりにくい。「証明書ファイルが自身の環境で利用できることを確認する。」などに。

●運用予定の設備
5. 設備上、運営上、運用上の管理
⇒「高層部に設置する」などにしてあまり書かない方法がある。
⇒防火区画は多くの建物で設置されている（天井に達する仕切り壁等）為、建築の設計書を確認する。消化設備を設置する。

●現実の運用体制（人数と部署）
5.2. 手続的管理
⇒JPNIC では CA 秘密鍵管理など特に重要な業務については、権限を分離している。権限分離の表は載せない。
5.4. 監査ログの手続
「必要な監査ログとして、本認証局が必要と認めた監査ログを取得する。」具体的には書かない。
5.5. 記録の保管
5.4.2. 監査ログを処理する頻度
⇒精査するとできるか。
5.4.3. 監査ログを保持する期間
⇒「規定の期間を保管する。」
5.4.3. 監査ログを保持する期間
⇒改ざん検出までは書かない。外部媒体へのバックアップの際に電子署名する方が効率的か。
「コンピュータの中にある間は、権限のないものがアクセスすることは難しいため」「バックアップ媒体へのタンパーシール」
6.1. 鍵ペアの生成及びインストール
⇒センター発行の分を記述

6.8. 更新された認証業務規程（CPS）

前節までに述べた更新案に基づき、CPS の更新を行った。更新された CPS を本報告書の Appendix.1 として添付する。また前年度の CPS との違いをまとめた表を Appendix.2 として添付する。