第3章 RIR の認証局の状況

内容

- 地域インターネットレジストリ（RIR）の認証局と証明書を使ったサービス
  - APNIC
    1. ユーザ証明書の扱い
    2. MyAPNIC
  - RIPE NCC
    1. ユーザ証明書の扱い
    2. LIR Portal
  - ARIN における議論

3. RIR の認証局の状況

3.1. はじめに

アジア太平洋地域の地域インターネットレジストリ（RIR：Regional Internet Registry）である APNIC（Asia Pacific Network Information Centre）や、ヨーロッパ地域の RIR である RIPE NCC（Réseaux IP Européens Network Coordination Centre）では、既に認証局が構築されている。これらの認証局は、各種申請の関連業務におけるクライアント認証で使われる電子証明書（以下、証明書という）の発行に利用されている。

本調査研究では、これらの認証局と証明書の利用方法について調査を行うとともに、APNIC、RIPE NCC の技術担当者との意見交換を実施した。これらの RIR の認証局の動向は、JPNIC における認証業務との連携に大きく影響するため、本章では特に APNIC と RIPE NCC の認証業務と証明書の利用について重点的に述べる。アメリカ地域の RIR である ARIN（American Registry for Internet Numbers）については、進行中である議論や動向について述べる。

従来、各 RIR においてはレジストリデータ編集の際に MAIL-FROM を用いた認証を実施していたが、かねてより強度面での脆弱さが指摘されており、CRYPT-PW、MD5、そして PGPKEY と、より強度の高い認証方式が随時、採用されてきた。

これらの認証方式として表 3-1 の方式が定義され、採用されている。

表 3-1 APNIC における mntner オブジェクトの認証方式[1]

認証方法	概要
NONE	保護されない。
MAIL-FROM	電子メールアドレスによるもの。きわめて弱い保護といえる。
CRYPT-PW	UNIX crypt 方式の暗号化パスワード。パスワード文字列長が 8 文字のため、強力とはいえない。
MD5	UNIX md5 方式の暗号化パスワード。パスワード文字列長が 65 文字に拡張され、CRYPT-PW よりも強力といえる。
PGPKEY	公開鍵証明書を示す署名識別子。公開鍵暗号による保護を提供する。

CRYPT-PW と MD5 は、ユーザパスワードを、DES 暗号を基にした Unix crypt 関数及び一方向ハッシュ関数である md5 で暗号化したものをレジストリデータに登録するものである。このことで安全性を向上させることが出来る。しかし、問題は残っ

[1] Authentication options for maintainer objects
http://www.apnic.net/db/ref/attributes/mntner/auth-mntner.html

ている。

- ユーザから RIR へ転送されるパスワードは平文で記入されるため、盗聴によりパスワードが流出する危険性がある
- 暗号化されたパスワードが whois 経由で公開されるため、パスワードが解析される危険性がある

CRYPT-PW のパスワードは 8 文字という制限があるため、現代の計算機能力を持ってすれば十分に推測可能といわれている。MD5 では、より長いパスワードが利用できるため、総当り攻撃でパスワードを推測することは困難といえる。しかし、通信経路として電子メールを使っているため、パスワード盗聴の危険性は依然として残る。

PGPKEY を使った場合には、これらの問題は解決する。更新データを含んだメッセージを事前に登録した PGPKEY を使って電子署名することで、メッセージ作成者の認証を行うとともに完全性の保証が可能となる。

現在提供されている認証方式の強度の関係は表 3-2 のように示される。

表 3-2 認証方式の強度比較

方式	強度	理由
NONE	無し	検証が行なわれない
MAIL-FROM	脆弱	なりすましの危険性がある
CRYPT-PW	弱	パスワード長が短く推測可能
MD5	中	転送中のパスワードに盗聴の危険性がある
PGPKEY	高	認証と完全性を提供できる

PGPKEY を用いることで強度的には十分な認証が実施できると考えられる。しかし、PGP は元々、個人が暗号化や電子署名を行うために開発されたものである。whois データベースの更新を電子メール経由で行う場合には十分とはいえ、拡張性、応用性を考えると難しい面がある。

ここ数年の間、各 RIR では、PGP よりも拡張性に富む PKI ベースの認証システムの配備を進めている。以降では、APNIC、RIPE NCC、ARIN における認証業務の動向について述べる。

3.2. RIR における認証局の活用

認証対象に証明書を発行し、検証を行うのが典型的な活用方法である。

本節では、PKI の活用の概要を概念的な手順で説明する。次に APNIC や RIPE NCC の認証局の活用について述べる。最後に、PKI（Public-Key Infrastructure、公開鍵基盤）の導入が進みつつある ARIN で認証方式の PKI の適性についての議論を紹介する。

3.2.1. PKI 活用の概要

PKI を利用した認証処理は、証明書の検証を通じて認証を行う検証者が、認証局（Certificate Authority、以下、CA と呼ぶ）を信頼することによってはじめて実現する。認証対象である EE は、CA から発行された証明書を検証者に提示し、検証者が EE の証明書の検証を行う。従って検証者が認証結果にもとづいてアクセス制御を実施することが出来る状況は、下記のような手順で構築される。

- 検証者による認証局の信頼
- EE による CA 証明書の組み込み
- EE による証明書の組み込み
- ユーザ（EE）管理
- 証明書の検証
  - サーバ証明書（EE が検証者となる）
  - クライアント証明書

3.2.1.1. 検証者による CA の信頼

検証者は CA の運用を兼ねているので RIR における、この手順は既に実施されている。

3.2.1.2. EE による CA 証明書の組み込み

暗号通信（SSL/TLS）を利用する場合、クライアントはサーバによる認証を受ける前に、サーバ認証を行う。その際に、サーバの提示する証明書を検証する必要があるため、CA 証明書が必要になる。EE が CA 証明書を組み込むには、検証者として CA を信頼する必要がある。この CA 証明書の組み込みと信頼の手順は、上記に述べた検証者によるものと同様である。

3.2.1.3. EE による証明書の組み込み

EE が認証手続きを受けるためには、検証者が信用する CA から証明書パスを辿る

ことができる証明書を発行されている必要がある。この手順は、EE による CA への証明書の要求と、CA による承認および発行、EE による証明書の組み込みといったもとなる。

3.2.1.4. ユーザ（EE）管理

サービスの提供者がユーザ認証に証明書を使う場合、証明書の管理すなわちユーザの管理が必要となる。クライアント証明書を使ったユーザの管理では、ユーザアカウントの無効化は証明書の失効によって行なわれる。しかし、一つのユーザアカウントに対し、複数の証明書を発行するようなモデルの場合、ユーザと証明書を管理するデータベースを用意し、該当するユーザのエントリを無効化するなどの方法となる。

ユーザアカウントが無効化されたことは、適切なタイミングで検証者に伝えられる必要がある。検証時にクライアント証明書の有効期限が切れている場合には、その情報だけでユーザアカウントが無効であることがわかる。しかし、有効期限内にユーザアカウントが無効化された場合は、CRL（Certification Revocation List）や OCSP（Online Certificate Status Protocol）といった失効情報を扱う仕組みが必要となる。

ユーザ管理は、以下のような要素によって、その形態が決まる。

- ユーザの規模
- ユーザの地理的な分散
- ユーザの権限の管理形態

ユーザの任命行為や権限の管理が地理的に分散した組織で行なわれる場合、ユーザの管理を行う管理者が分散している方が効率的な管理を行うことができる。しかし、管理者を分散して配置するとなると、運用のレベルを保つためには監視や監査といったマネジメント上の作業が発生する。

多くのユーザを管理する場合は、ユーザ登録や権限の管理といった処理にかかる負荷も大きくなる。そのため、管理部門を一箇所に集中させるよりは、社会的な権限の管理体系に合わせた構造にする必要がある。

3.2.1.5. 証明書の検証

サービス提供者が、アクセスしてきたユーザに対して、アクセス制御を行うためには、クライアント証明書の検証を行い、クライアントの認証を行う必要がある。

証明書の検証の際には、前述した証明書の失効情報を扱うとともに、アクセス制御の規則を定義したデータベースを扱う。

3.3. APNIC

ここでは、前節で述べた手順の概要に沿って APNIC（Asia Pacific Network Information Centre）における認証局の活用について述べる。

APNIC は、アジア太平洋地域を管轄とする RIR である。APNIC では、1999 年より PKI への取り組みを開始している。

1999 年には要件定義の試みとしての Scoping Project が行なわれ、認証局の運用について必要な機能及び現状の問題点がまとめられた。翌 2000 年には認証運営の試みとして Pilot Project が行なわれ、メンバ登録からオンラインでの証明書要求から発行まで詳細な議論と実証が行なわれた。これらの試験的プロジェクトの成果により、認証運営の環境が整えられたといえる。

このような環境構築の成果を受け、APNIC では、証明書ベースの認証を取り入れた、メンバの所有するデータベースオブジェクトの管理インターフェースとして MyAPNIC というウェブサービスを提供している。

以降で、MyAPNIC における PKI の利用と、認証局の運用について述べる。

3.3.1. 概要

ここでは、認証業務と MyAPNIC におけるアクセスコントロールについて述べる。

APNIC では次の目的を達成するため、独自の認証局(以下、APNIC CA と呼ぶ)を構築している。

- メンバと APNIC 間の電子メール交換を安全にする
- MyAPNIC へのアクセスを安全にする

MyAPNIC は SSL/TLS で保護された通信経路上で情報提供サービスを行なっている。（図 3-1）

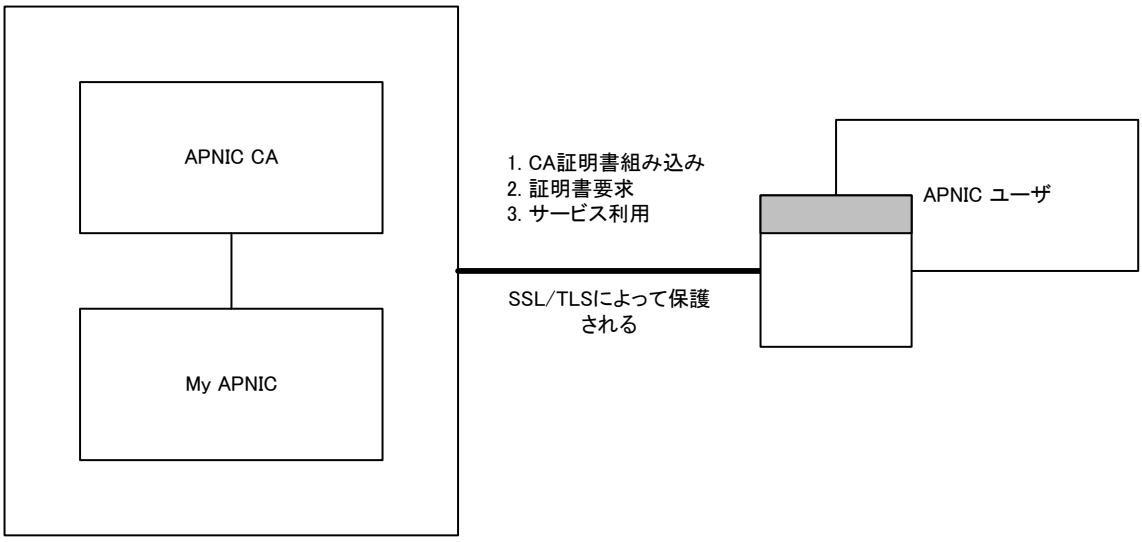

図 3-1 MyAPNIC 概要

以下では、MyAPNIC へのアクセスに用いられる証明書の運用に関して、APNIC CA の業務について述べる。

3.3.2. EE による CA 証明書の組み込み

APNIC ルート CA 証明書のロードおよびオンラインでの証明書要求申請は、ウェブインターフェース（図 3-2）を介して行なわれる。

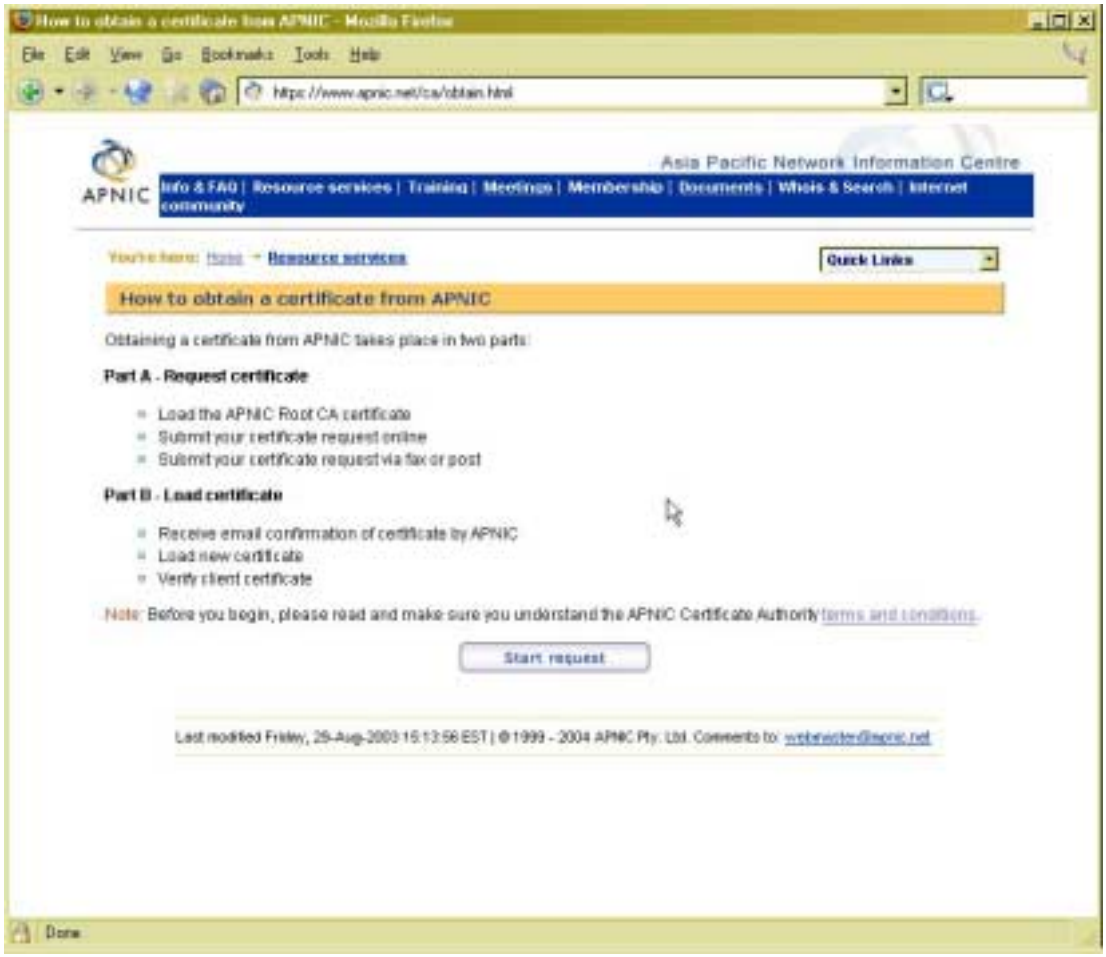

図 3-2 APNIC 認証局発行証明書の手続き[2]

このページ自体は APNIC 認証局の証明書（図 3-3）で保護された形で提供される。この証明書は、インターネットエクスプローラ及び Mozilla といった、通常使われているブラウザの CA 証明書ストアには含まれていないので、アクセス時に証明書が検証できず、受け入れるかどうかをたずねるダイアログが表示される。

[2] How to obtain a certificate from APNIC
https://www.apnic.net/ca/obtain.html

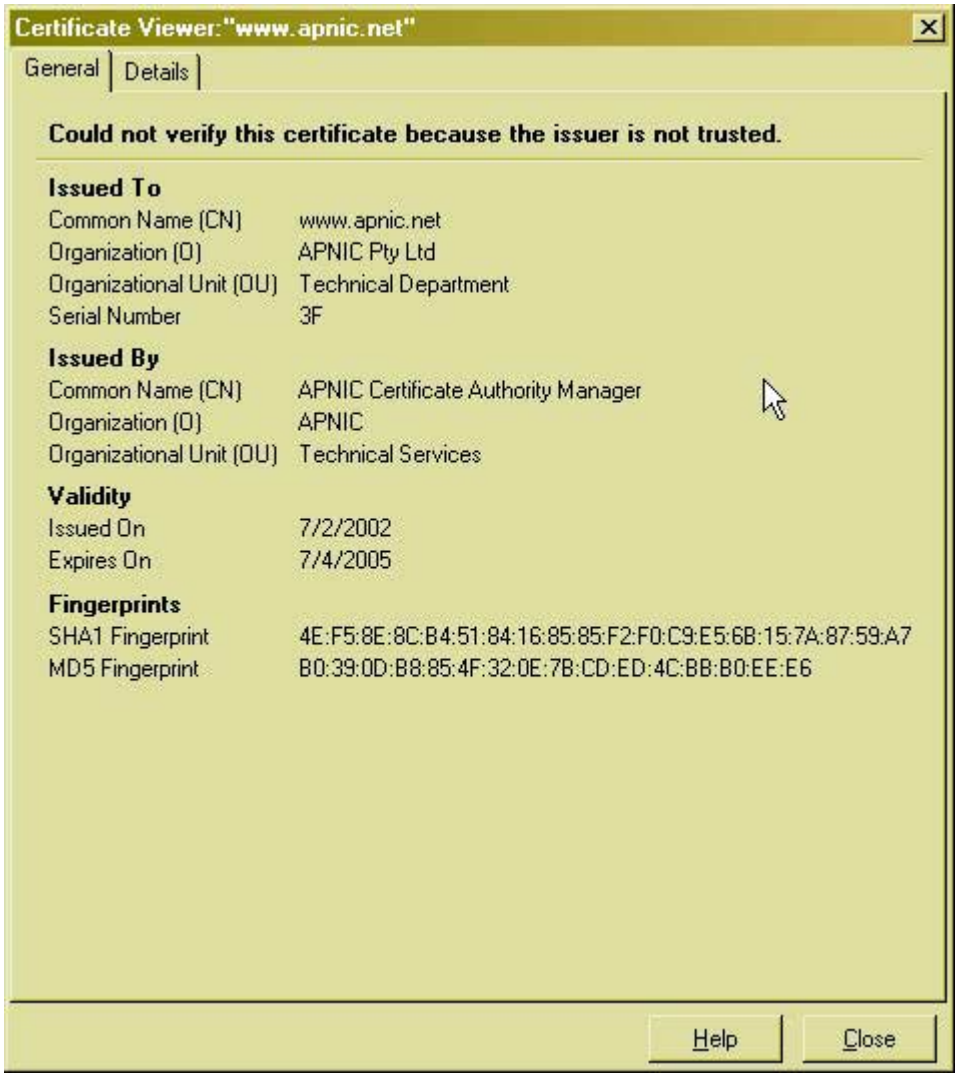

図 3-3 www.apnic.net サイトのサーバ証明書

手続きを進めると、APNIC CA 証明書をロードすることになる（図 3-4）。ここでウェブサイトの識別について、この CA を信頼することにして受け入れると、以降、APNIC ルート CA の発行する証明書が検証できるようになる。

図 3-4 APNIC CA 証明書のロード（Mozilla Firefox での実行結果）

証明書が格納されたことはブラウザから確認できる（図 3-5）。

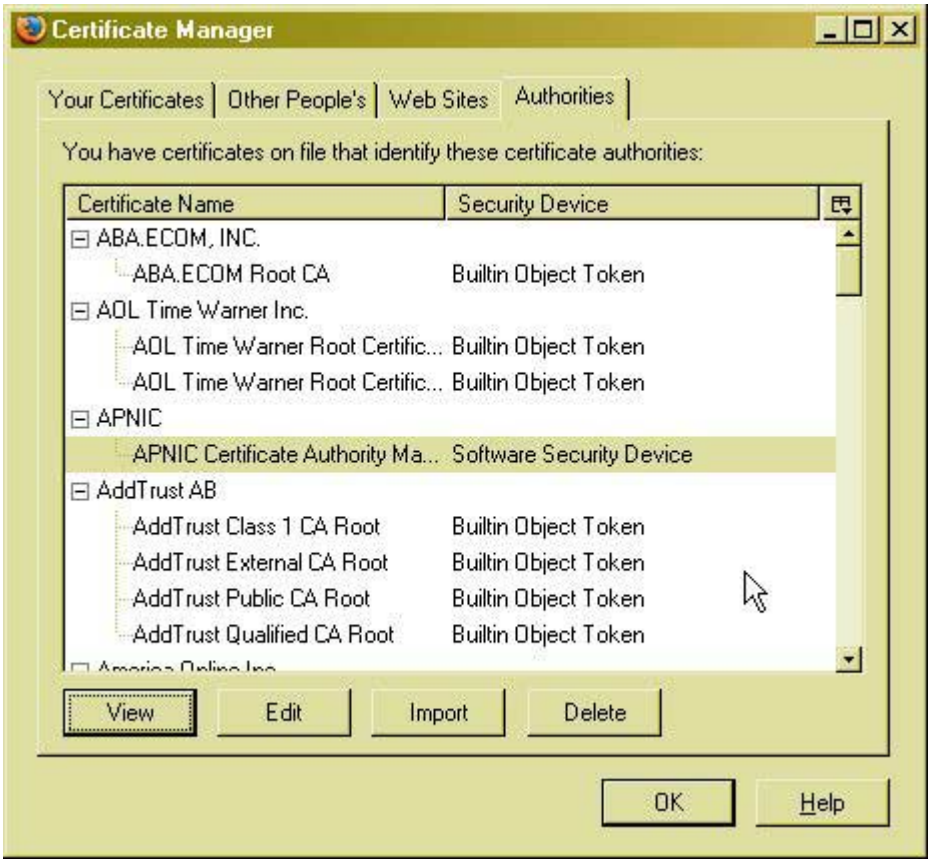

図 3-5 APNIC CA 証明書を受け入れたことの確認（Mozilla Firefox）

続けて個人証明書の発行手続きを行う。

3.3.3. EE による証明書の組み込み

ブラウザに APNIC ルート CA 証明書を組み込んだ後は、その証明書で保護された APNIC CA サイトにアクセスし、オンラインでの証明書要求申請を行う（図 3-6）。

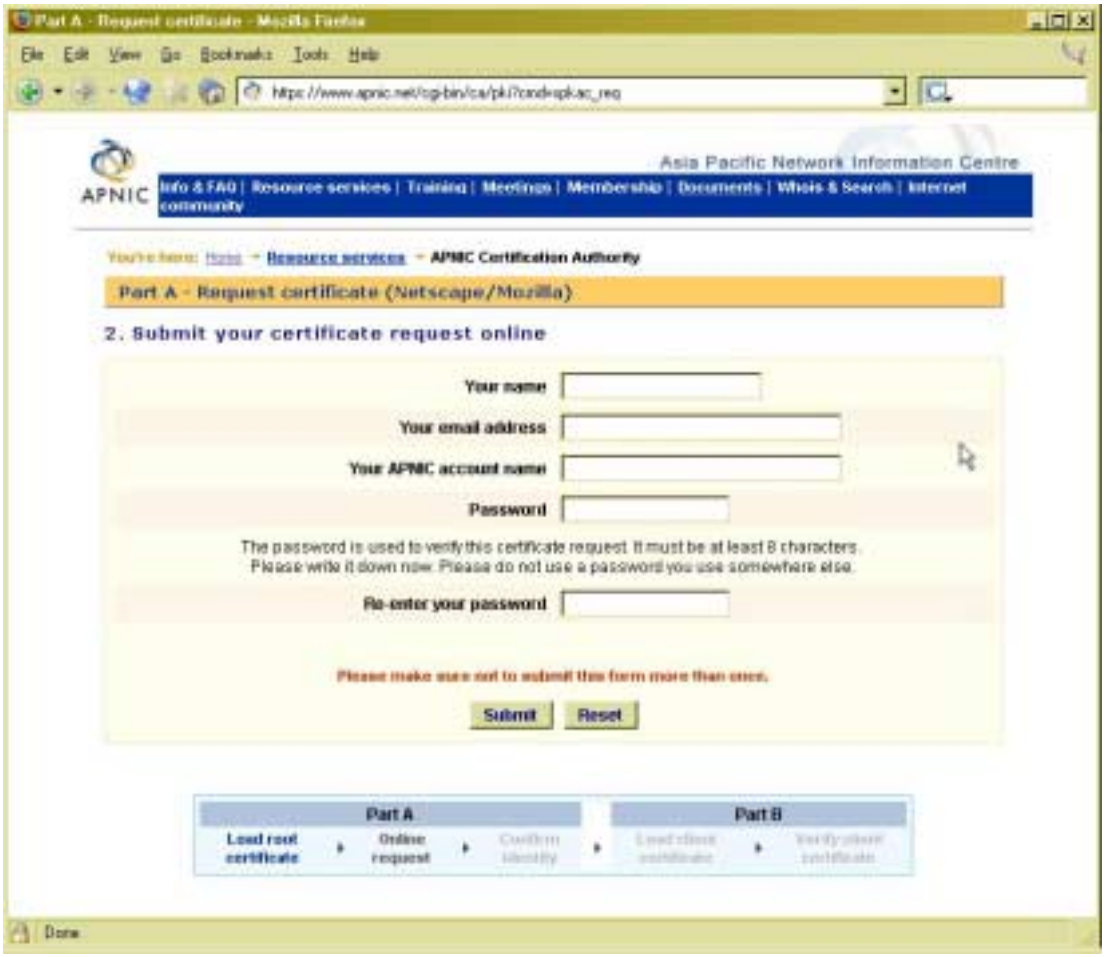

図 3-6 オンラインでの証明書要求申請

オンラインでの申請が終わりしだい、引き続き、オンラインでの申請と本人を結びつけるために、FAX または郵送で表 3-3 の内容を記載した要求申請を行う[3]。

[3] APNIC Certificate Request Form
https://www.apnic.net/ca/apnic-crf.pdf

表 3-3 紙ベースでの証明書要求申請記入内容

項目	内容
Identification document	パスポートなど写真の入った ID 文書のコピー（フォームに貼り付けるか別紙として添付する）
Your full name	オンライン申請に記入したフルネーム
Your email address	オンライン申請に記入した電子メールアドレス
The name of organization	所属する組織名
APNIC account name	APNIC アカウント名
Passwd	オンライン申請に記入したパスワード

このように、オンラインでの申請とオフラインでの申請を組み合わせることで、本人同一性の検証を行う手続きとなっている。

検証確認後は電子メールにより個人証明書の入手方法が指示される。各人は、指示に沿って、自らの環境に個人証明書を組み込むことになる。

3.3.4. ユーザ（EE）管理

APNIC CA では、RA と IA の機能を分散させることは行なってはいない。3.3.3 で述べたように、本人確認は APNIC CA 自身で行うことになる。

3.3.5. 提供されるサービス

MyAPNIC を通じて図 3-7 のサービスが提供される。

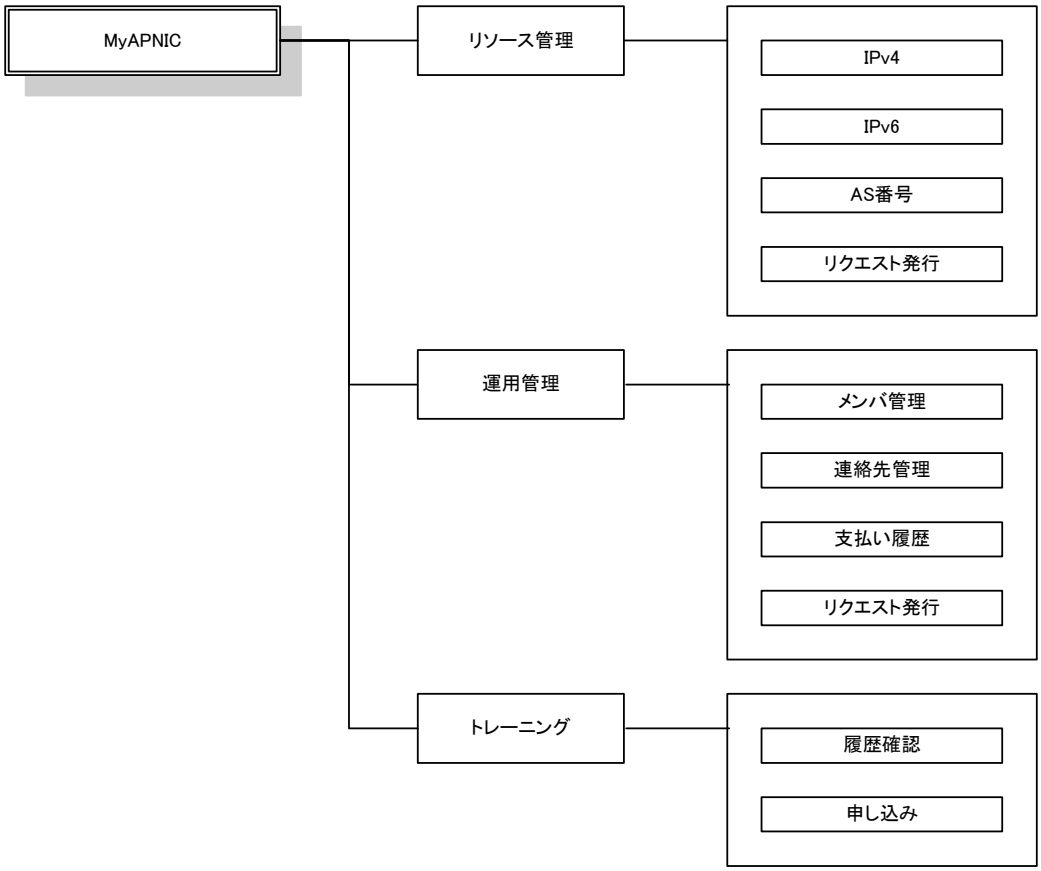

図 3-7 MyAPNIC 機能一覧

以下で、それぞれのサービスの概要を述べる。

（1） リソースマネジメント

リソースマネジメント機能では表 3-4 の機能を提供している。

表 3-4 MyAPNIC リソースマネジメント機能

機能名	機能
IPv4	保有するアドレスブロック、およびその利用率（割り当て状況）の閲覧
IPv6	同上
AS 番号	使用する AS 番号のリストと情報の閲覧
リクエスト発行	IPv4 アドレスリソース、IPv6 アドレスリソース、AS 番号に関して、APNIC ホストマスタに対する要求事項を送信し、チケット番号を受け取る機能

実際の Web インターフェースは図 3-8 のようになる（デモンストレーション）。

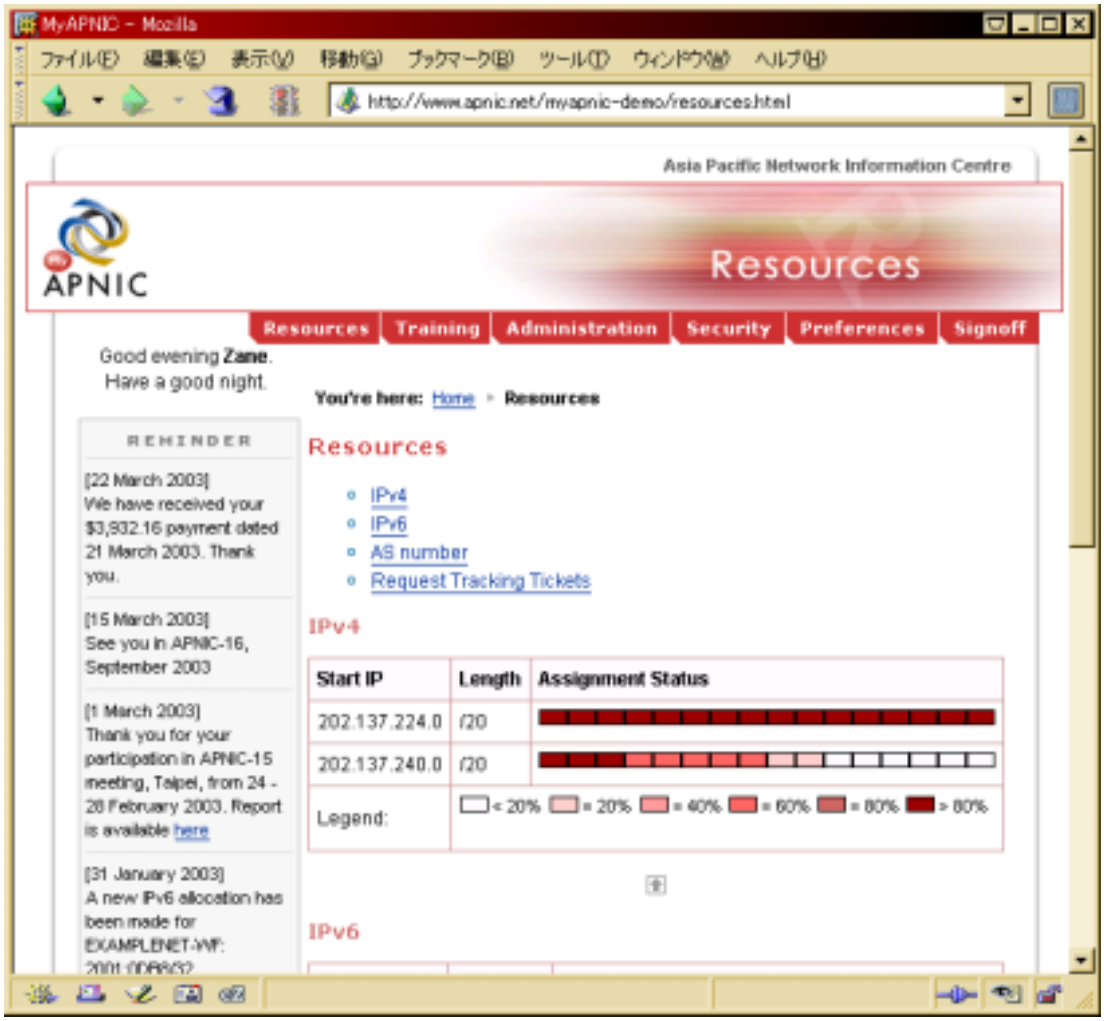

図 3-8 MyAPNIC リソース管理画面

（2） 運用管理

運用管理機能では表 3-5 の情報を管理できる。

表 3-5 MyAPNIC アカウント管理機能

機能名	機能
メンバ管理	アカウントのメンバ情報の詳細を編集することができる
連絡先管理	ホストマスタ、技術担当者、運用担当者などを追加、削除、編集することができる
支払い履歴	APNIC に対する支払い履歴を閲覧することができる
リクエスト発行	（admin@apnic.net 宛ということだが、このペインに現れる情報に関する質問、要求ということだろうか）

実際のウェブインターフェースは図 3-9 のようになる。

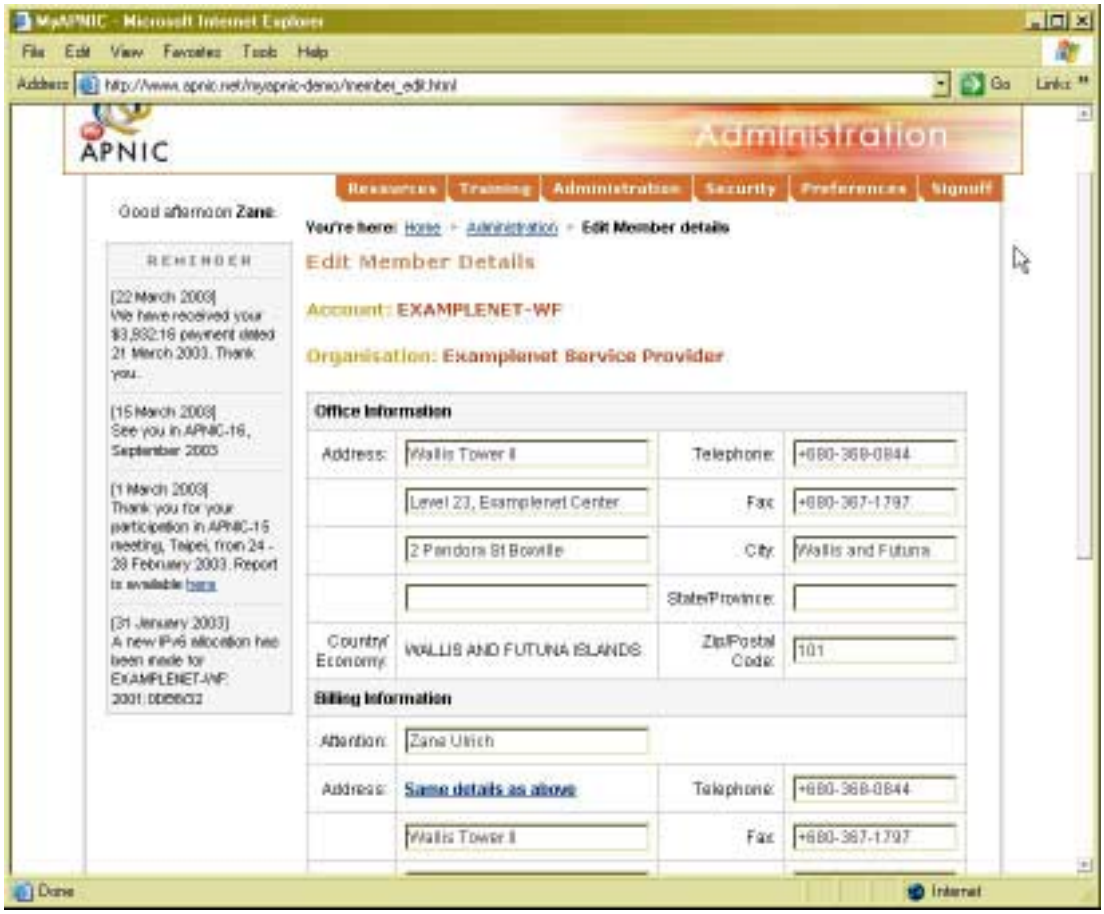

図 3-9 MyAPNIC 運用管理画面（メンバ管理）

（http://www.apnic.net/myapnic-demo/member_edit.html）

（3）　トレーニング

トレーニング機能では、表 3-6 の機能を提供している。

表 3-6 MyAPNIC トレーニング機能

機能名	機能
履歴確認	メンバの APNIC 年次総会、トレーニングなどへの参加履歴を閲覧することができる
申し込み	トレーニングの申し込みを行うことができる

実際の画面は図 3-10 のようになる。

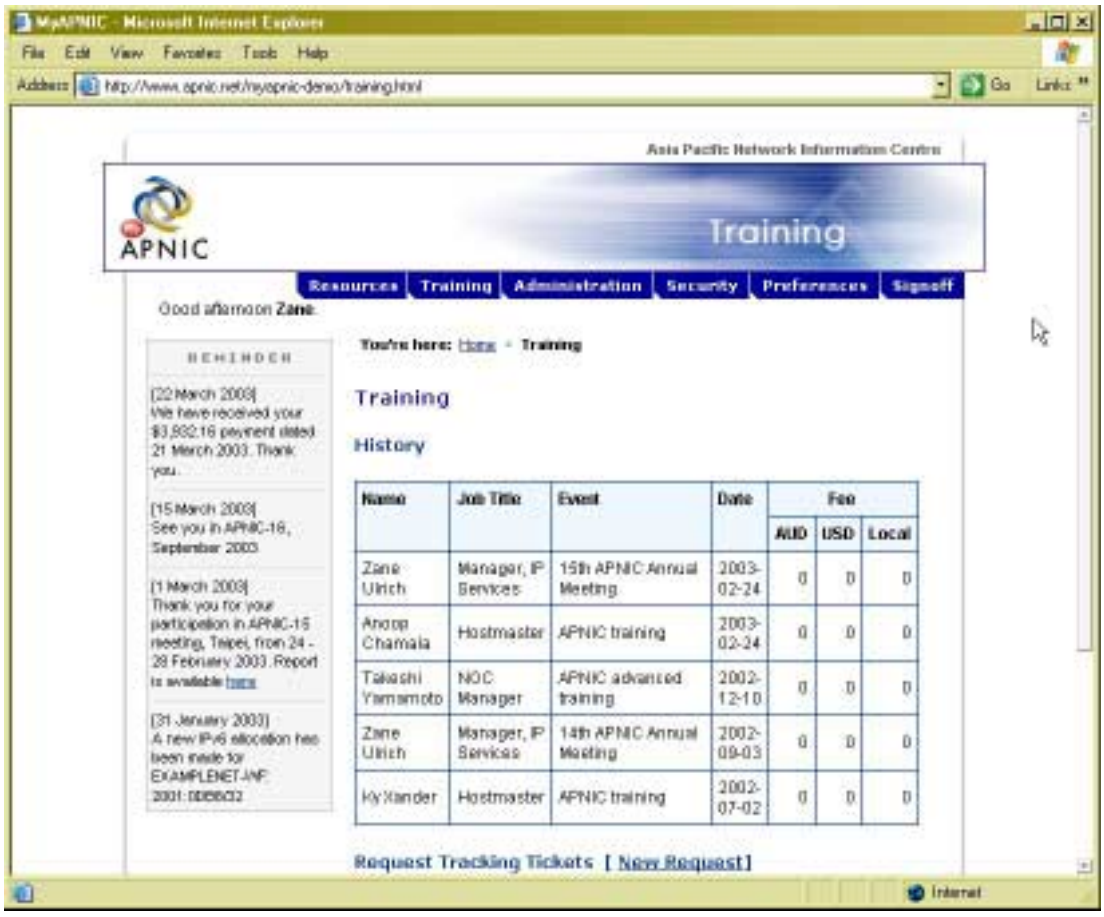

図 3-10 MyAPNIC トレーニング機能

（http://www.apnic.net/myapnic-demo/training.html）

3.3.6. 証明書の利用

ここではMyAPNICにおけるクライアント証明書を利用したアクセスコントロールについて述べる。すでに述べたようにMyAPNICでは、メンバに対し、様々な情報へのインターフェースを提供している。

これらの情報は極めてプライバシーが高いものであり、組織のメンバだからといって開示できるものばかりではない。このため、MyAPNICではメンバごとに権限を指定できるシステムを提供している。

図 3-11 は、MyAPNIC のデモンストレーション中のセキュリティ設定ページである。ここでチェックがつけられている項目は、対応するユーザ及びユーザの個人証明書が提示される際に、MyAPNIC 中で表示される情報を示している。

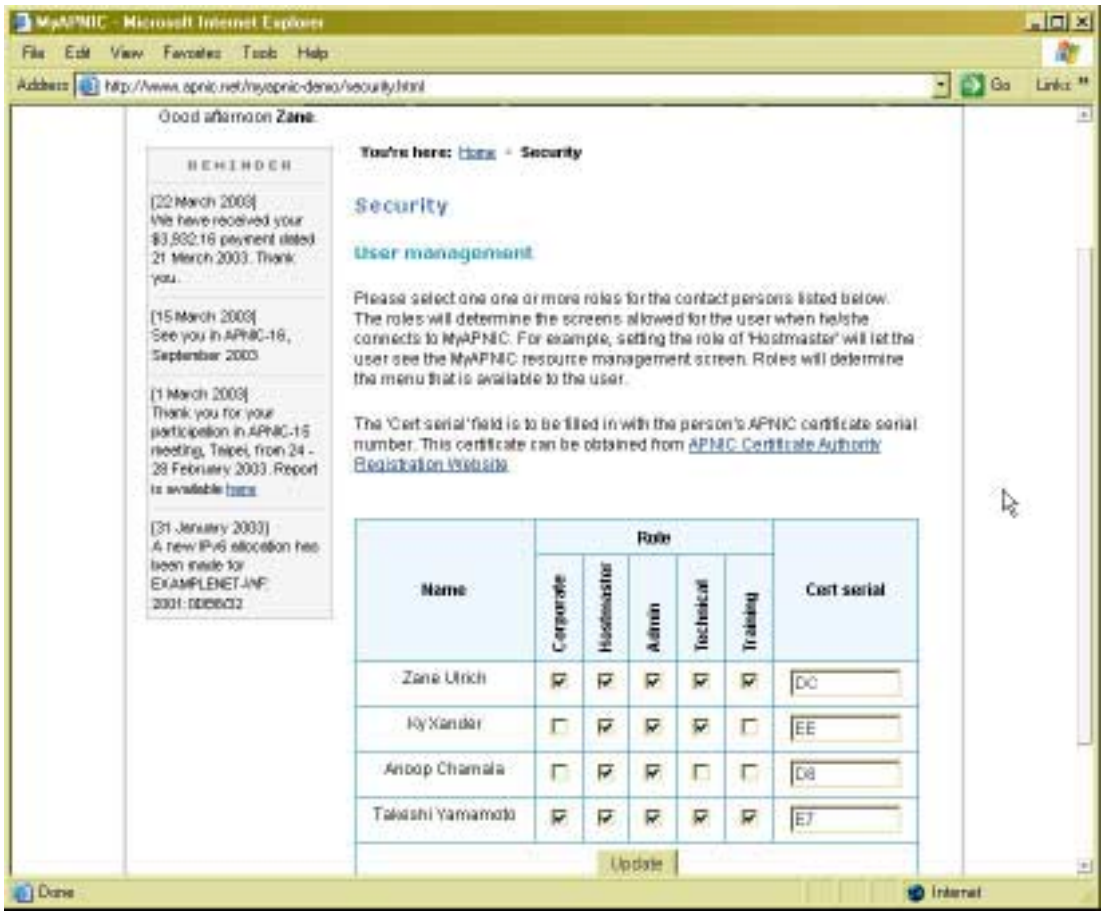

図 3-11 MyAPNIC におけるユーザアクセス権限管理

（http://www.apnic.net/myapnic-demo/security.html）

3.3.7. APNIC CA の今後

APNIC では、認証局を利用した登録情報の保護と活用について、MyAPNIC だけに留まらない検討を行なっている。APNIC の認証局の運用および技術担当者とヒアリングを行なった結果、以下のような利用方法を検討していることが判明した。

- soBGP（secure origin BGP）で使われる証明書[4]
- RIR と NIR における階層的な資源管理を踏まえたメッセージ認証の基盤構築

これらは実現可能性を検討している段階の様子ではあるが、特に soBGP の経路情報の保護を目的とする証明書は、その発行主体がインターネットレジストリであることで登録情報との同期が取りやすいというメリットがある。これはアドレスブロックの割り振り情報は、インターネットレジストリが一次情報源となると考えられるためである。

[4] Secure Origin BGP (soBGP) Certificates
http://www.ietf.org/internet-drafts/draft-weis-sobgp-certificates-01.txt

3.4. RIPE NCC

RIPE NCC（Réseaux IP Européens Network Coordination Centre）では、RIPE NCC の提供するサービスに対するインターフェースとして、SSL による保護されたウェブサイトを提供している[5]。このサイトでのサービスを LIR Portal と呼ぶ（図 3-12）。

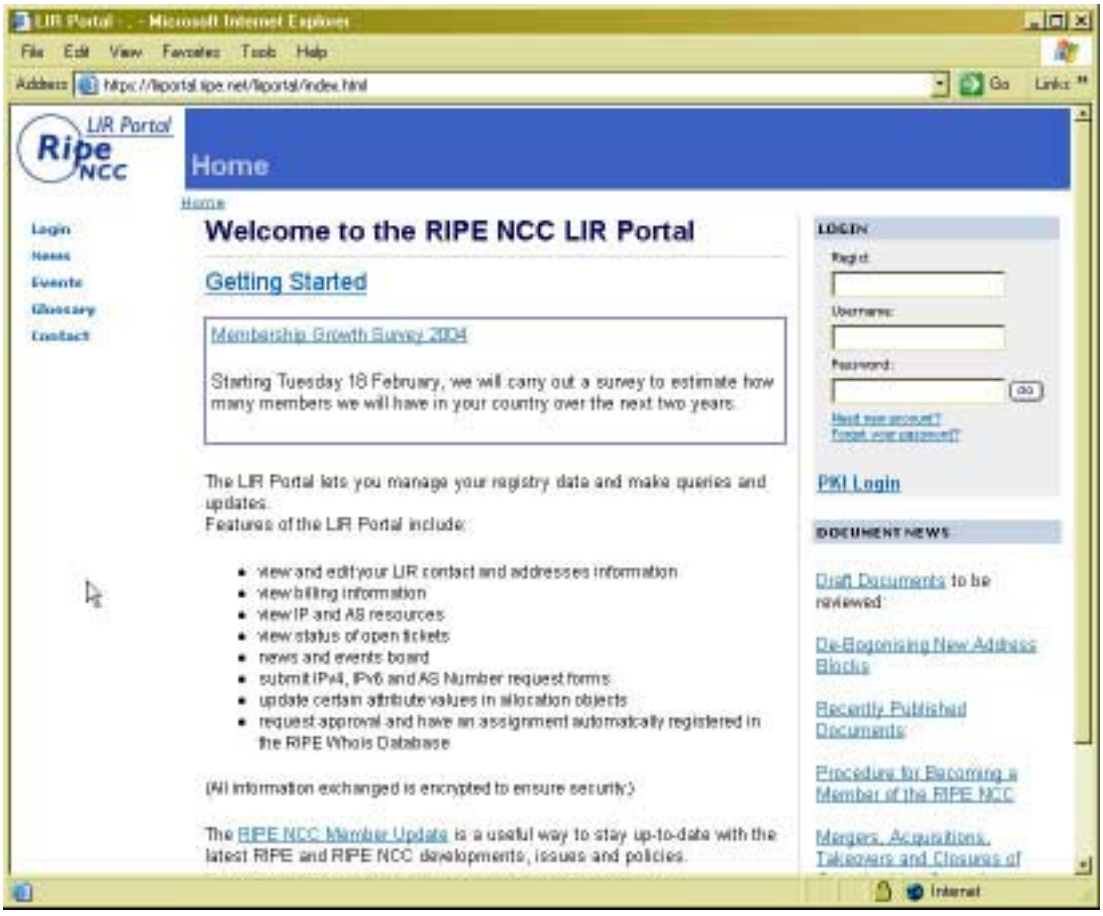

図 3-12 LIR Portal トップページ

LIR Portal では、次の各機能が実装されている。

- LIR の連絡先及び住所情報の閲覧及び編集
- 課金情報の閲覧

[5] LIR Portal
https://lirportal.ripe.net/lirportal/index.html

- IP 及び AS リソースの閲覧
- 開かれているチケット状況の閲覧
- ニュース及びイベント情報
- IPv4、IPv6 および AS 番号要求申請の提出
- 割り振りオブジェクトの属性値の更新
- 要求認可と RIPE Whois データベース中での自動的に登録された割り当て

この LIR Portal では、ウェブインターフェースによるユーザ名/パスワード認証に加え、証明書を使ったクライアント認証をサポートしている。

ここでは、クライアント認証のために発行されるクライアント証明書と認証局について説明を行う。

3.4.1. 概要

2003 年 5 月 12 日から 16 日にかけてスペインバルセロナで開催された RIPE45 でのプレゼンテーション「Improved Secure Communication System for RIPE NCC Members / Tiago Rodrigues Antao[6]」によると、RIPE NCC では、以下の目的を達成するため、安全な通信システムを実装することとなっている。

- RIPE NCC サービスへの、使いやすく、高速なインタラクション
- 統合された強力なセキュリティメカニズム
- 特権/クレデンシャル管理の支援
- ユーザにとって低い、配置及び維持コスト
- LIR にとって選択的
- 標準（X.509 PKI）のサポート

この提案では、RIPE NCC における PKI の実装は図 3-13 ように示されている。

[6] Improved Secure Communication System for RIPE NCC Members
http://www.ripe.net/ripe/meetings/ripe-45/presentations/ripe45-lir-pki/

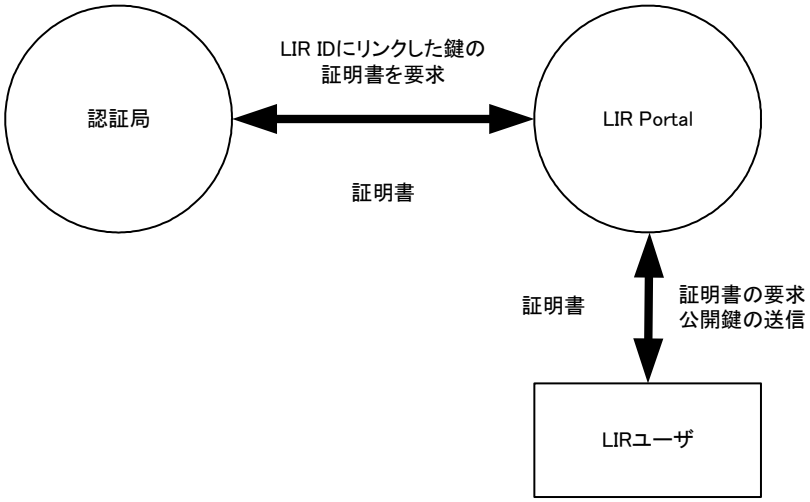

図 3-13 証明書管理サイクル[7]

以下では、RIPE NCC における PKI の活用として、LIR Portal の詳細について述べる。

3.4.2. EE による CA 証明書の組み込み

LIR Portal のサーバ証明書は、ブラウザの配布イメージに組み込まれている認証局から発行されたものであるため、明示的な組み込みは不要である。

3.4.3. EE による証明書の組み込み

ここでは LIR Portal におけるクライアント証明書の取得手順について述べる。クライアント証明書の発行に際して、本人性の確認などを行うために RA が配置される。LIR Portal では、PMS（Privilege Management System）と呼ばれる権限管理システムを導入している（図 3-14）。このシステムでは、RIPE NCC より、各 LIR に管理者権限を持つ証明書が一枚発行される。各 LIR では、この証明書を用いて、ユーザに対する証明書を発行することになる。この形態により、RA を分散配置させることが出来ている。

以下に、LIR 管理者アカウントの作成と、LIR ユーザアカウントの作成について述べる。

---

[7] certificate management cycle
http://www.ripe.net/ripe/meetings/ripe-45/presentations/ripe45-lir-pki/page9.htm

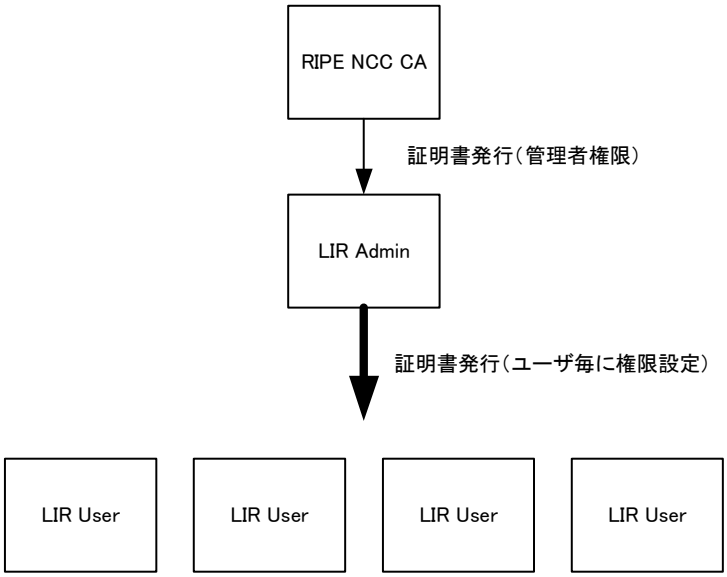

図 3-14 RIPE NCC PMS

3.4.3.1. 管理者アカウントのパスワード設定

各 LIR は管理者ユーザを一つ持つ。このアカウントはユーザアカウントを作成し、その権限を設定および修正することのできるアカウントである（その他のこと、レジストリ情報の閲覧などは出来ない）。

まず、このアカウントのパスワードを設定し、ユーザアカウントの生成を行う。この手続きは三段階に構成される。

- RegID（レジストリ識別子）、LIR への電子メールアドレスおよび FAX 番号を提供しなければならない。これは請求書を発行するために必要となる。
- LIR Portal[8]からこれらの情報が申請されると、LIR は「Fax Confirmation Number」と「E-mail Confirmation URL」が記載されたファックスを受け取ることになる。
- 「E-mail Confirmation URL」に示される URL で「Fax Confirmation Number」を与える。これによりアカウントが有効になる。

これ以降は、選択したパスワードを使って LIR Portal にログインできる。

[8] Member Services
https://lirportal.ripe.net/lirportal/activation/activation_request.html

3.4.3.2. ユーザアカウントの生成

ユーザ証明書の RA は LIR 管理者が務める。このため、LIR 管理者は、ユーザ証明書の発行及び廃棄に関する承認について責任を負うことになる。

3.4.4. ユーザ（EE）管理

前述の PMS を通じて、RA 機能の分散（階層化）が図られている（図 3-15）。RIPE NCC が RA として承認及び本人確認を行うのは LIR 辺り、一名と限られており、ユーザ証明書の発行及び管理負荷は、各 LIR に分散できる。

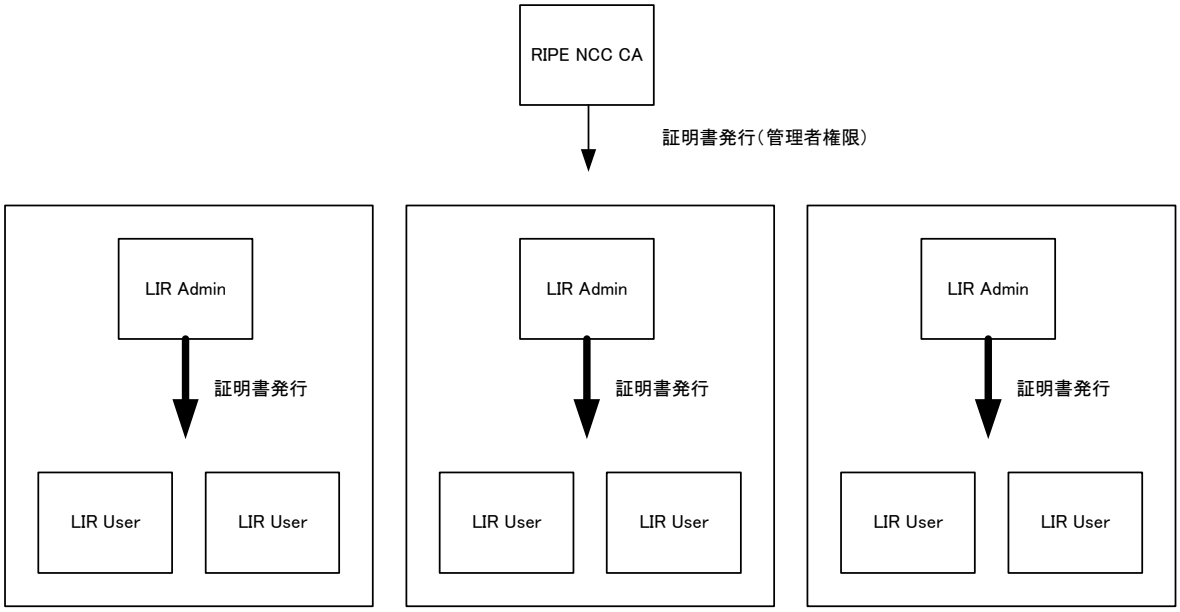

図 3-15 PMS による RA 機能の分散

各 LIR 管理者は RIPE NCC CA と安全な通信経路上で証明書発行依頼を行うことになる。

3.4.5. 認証局の利用

レジストリシステムにアクセスする通信経路には、LIR Portal だけでなく、電子メール経由のアクセスも依然として可能である。RIPE NCC では、RIPE NCC のホストマスタから LIR に送られる電子メールを安全にするため、次の選択肢から、任意のものを選択可能としている。

- PGP 署名つき電子メール（デフォルト）
- PGP 暗号電子メール
- X.509 署名の利用
- X.509 暗号の利用（LIR の公開鍵で暗号化）

また、特別に機密性の高いデータを含んだデータ通信を行う場合など、必要に応じて、より安全な通信方法を選ぶことが出来る。

3.4.6. RIPE NCC の認証局の今後

X.509 PKI インフラストラクチャの構築は、LIR と RIPE NCC サービスとの認証機構にとどまらず､サービス間の統合のためにも使われる｡この統合は主に LIR Portal を通じて行なわれると考えられる。

以下に、X.509 PKI の今後の利用可能性として、RIPE データベース、リバースデリゲーションについて述べる。

3.4.6.1. RIPE　データベースへの応用

RIPE データベースは X.509 PKI に基づいた新しい認証機構が利用可能になる。

最初の段階では、LIR Portal によって発行された証明書だけが、RIPE データベースに受け入れられる。このことは LIR ユーザでなければ、この新しい認証機構を利用することができないことを意味する。

新しい認証方法のサポートは､X.509 識別名を示す auth: 属性を追加するオプションによって行なわれる｡発行された証明書のコピーを key-cert オブジェクトに加える必要はない。

LIR ユーザはこの新しい認証を電子メールと webupdates の双方で用いることが可能となる。このことで、RIPE データベースの更新は、パスワードによる現在の認証よりも安全になるといえる。

3.4.6.2. Reverse Delegation

LIR は、リバースデリゲーション情報に対するいかなる変更も、X.509PKI によって認証されなければならないことを宣言することが可能となる。つまり、LIR からのすべての要求は、承認されるために署名されなければならないことを意味する。

さらに加えて､リバースデリゲーション情報の修正は LIR Portal においてもサポートされることになる。LIR Portal に対して適用される認証と暗号と同じものがリバー

スデリゲーションにも適用されると考えられている。

3.5. ARIN

ARIN（American Registry for Internet Numbers）では、よりよい認証方式の検討が行なわれ始めている。現段階では、PKI 配備に向けてのベータテストを行なっている段階であり、他 RIR のように、証明書組み込み、ユーザ管理といった具体的な手順については検討の段階である。このため、この節では、ここ数年における ARIN での認証に関する検討状況、および今後の計画について記述する。

3.5.1. 2002 年 ARIN X Open Policy Meeting における発表

2002 年開催された ARIN X Open Policy Meeting での Cathy Murphy 氏によるプレゼンテーション「Next Steps for the ARIN Registration Database[9]」では、認証メカニズムとして次のものが提案されていた。

- PGP 証明書の利用
- X.509 証明書の利用
- Login/SSL パスワードの利用

また、拡張された認証を必要としているプロジェクトとして次のものがあげられている。

- Web ベースのメンバーサイト
- Routing Registry 経路認証

3.5.2. 2003 年 ARIN XI Open Policy Meeting における発表

2003 年に開催された ARIN XI Open Policy Meeting での Tim Christensen 氏によるプレゼンテーション「Authentication[10]」では、最初に実装する認証方式として X.509 証明書をあげている（PGP や MD5 といった認証方式は将来の拡張）。

この理由としては次のものなどがあげられている。

- Public Policy Meeting での議論から証明書が良いという評価を得た
- PGP は公開鍵サーバが必要になる
- 他 RIR の実装を鑑みて

---

[9] ARIN X Public Policy Meeting Minutes
http://www.arin.net/library/minutes/ARIN_X/ppm.html

[10] ARIN XI Public Policy Meeting Minutes
http://www.arin.net/library/minutes/ARIN_XI/ppm_minutes_day2.html

また、X.509 証明書の用途として以下のものがあげられている。

- 電子メールテンプレートの保護（認証、暗号化）
- ウェブトランザクションの認証
- ARIN によって生成されたデータの認証

認証方式として、制御、セキュリティ、活用性のバランスが最も優れているとされている。

3.5.3. 2003 年 ARIN XII Open Policy Meeting における発表

2003 年に開催された ARIN XII Open Policy Meeting での Tim Christensen 氏によるプレゼンテーション「Cryptographic Authentication[11]」では、ARIN における暗号を利用した認証の現状について述べられている。

目標としては次のものが挙げられている。

- 受け取る電子メールの正当性の改善
- データベースの完全性の改善
- 送信される電子メールの認証の改善

要求事項としては次のものが挙げられている。

- 送信者アイデンティティの検証
- 内容が改ざんされないことを確実にする
- 顧客信頼性の改善
- 受託責任のデモンストレーション
- 適用可能な IETF RFC の遵守
- 産業の事業継続計画の追従
- 将来の拡張性

現在のプロジェクトのスコープについては次のものが挙げられている。

- テンプレートベースでの登録を安全にする
- ARIN CA の確立
  - 手続きの識別
  - ワークフローの定義
- アウトバウンド通信を安全にする
  - 電子メールの返答

[11] ARIN XII Public Policy Meeting Minute, Day 1
http://www.arin.net/library/minutes/ARIN_XII/ppm_minutes_day1.html#11

- 証明書

今後の展開として、配備及び実装への道筋が示されている。

POC（Point Of Contact）は証明書署名要求（CSR）を作成する
↓
POC は ARIN に CSR を送信する
↓
ARIN は CSR の内容を検証する
↓
ARIN は証明書を生成、データベースの更新を行ない、証明書を POC に送信する
↓
POC はテンプレートの署名に証明書を用いる
↓
ARIN は POC によって申請されたテンプレートを認証する
↓
POC は認証証明書を維持する

配備に向けてのベータテストの実施項目として次のものがあげられている。

- 識別プロセス
- テスト環境の構築
- 変更プロセスの提示
  - CSR（証明書署名要求）生成
  - ARIN 認証局の稼動
  - 署名テンプレート認可及び拒否
  - 認証失敗に対する対処

今後のタイムラインとして次のものが示されている。

- 要求事項と必要条件の確立
- 必要条件の達成
- オプションの調査
- 現存する RIR の実装の理解
- ユースケースの識別
- テストベッドの確立
- 最初に配備する手法の選択
- 変更プロセスの策定

- ベータコミュニティの形成とテスト
- 配備
- 他の手法の実装
- Mail-From の廃止

この発表が行なわれた時点では、ベータテストの第一フェーズの実施中で、ユーザによる証明書署名要求の生成と ARIN が証明書を発行することなどを評価している。

次回、ARIN XIII では、「Using X.509 Authentication with ARIN's Database」と名づけられたワークショップが開催される予定となっており、オンラインで証明書を要求するプロセスの概要が提示される予定となっている。

3.6. まとめ

APNIC や RIPE NCC では、認証局を運用すると共に、資源管理システムの認証に証明書を利用することが可能になっている。証明書の用途は Web を使った申請などに使われる https だけでなく、暗号を利用した電子メール S/MIME の活用も開始している（RIPE NCC）。サービスと認証用途の証明書は、今後活用されていくと考えられる。ヒアリングの結果、経路情報のプロトコルである BGP での情報の保護にも使う考えを持っていることもわかった。

APNIC は APNIC CA を運用し、MyAPNIC と呼ばれる Web サービスを提供している。MyAPNIC はバージョンアップを重ねており、資源管理機能はまだ実装されていないものの、Executive Council 選挙の機能や連絡先情報の変更などに対応している。APNIC CA はスタンドアローンで運用されており、ユーザが証明書を Web ブラウザに組み込む形で運用されている。CP/CPS の公開などは行なわれていない。RIPE NCC は、データベースシステムにおける証明書の活用に力を入れている。暗号を用いた認証機能では PGP が主流であったが、同様の方法で PKI を使った S/MIME が利用可能になりつつある。登録情報データベースに X.509 形式の証明書を組み込む書式も提案され、実装が進んでいる。ARIN では、証明書を利用した認証に関する議論が進んでいる段階である。ARIN の次回のミーティングでは認証機能に関するワークショップが開催される予定であり、関心の高さを伺うことができる。しかし IP アドレスといったアドレス資源ではなく、ドメイン名を基本とする証明書を利用する可能性がある。

RIR における認証局の状況の中で、JPNIC の認証局に関連することは、証明書の用途・RIR におけるデータ交換と認証方法・認証業務のレベルの 3 点であると考えられる。

- 証明書の用途
  証明書には認証用か署名用かという違いがある。RIR との連携の観点から JPNIC の認証局でも比較的運用しやすい認証用の証明書から始めるのが適切だと考えられるが、第 4 章で述べる認証基盤や RIR のデータ認証を踏まえると署名用の証明書も検討する必要があると考えられる。

- RIR とのデータ交換
  RIR においてアドレス資源の不正／浪費的な利用に関する問題が議論されることがあるが、RIR 間でのデータ同期を含めた全体的な議論は少ない。レジストリの間で登録情報を交換すると、世界規模でアドレス資源管理の情報を検証できるようになるが、その為には電子署名付きのデータがやりとりできる状態になる必要がある。EPP/CRISP といった、登録情報を扱うプロトコルの調査研究が必要となる。

・ 認証業務のレベル

　限られた相手の認証用の証明書を発行するのが RIR における認証局の状況であるが、世界規模で署名を検証するような認証局の場合は、よりセキュリティレベルの高い認証局が必要なる。RIR では認証用の証明書を発行するシンプルな構成であるが、JPNIC の認証局は認証情報の応用も検討しており、インターネットにおける基盤的な認証基盤を目標としているため、CP/CPS の策定から認証局ソフトウェアの活用など、よりセキュリティレベルの高い運用を目指す。

本調査研究で目標としているデータ認証が可能になる状況は、RIR の認証局やレジストリシステム、および認証業務と関連している。従って、今後継続して RIR の認証局について調査研究を行うとともに、IETF におけるレジストリ関連のプロトコルの策定状況の調査が必要と考えられる。