第3章 他のインターネットレジストリの活動

内容

- 認証局とデータベース保護に関する活動
  - APNIC
    1. CA Pilot Project
    2. MyAPNIC
  - RIPE NCC
    1. オブジェクトの保護
    2. WebUpdates
  - RIR の whois システム
  - RIPE Database System

3. 他のインターネットレジストリの活動

本章では、データベース保護と PKI に関連する活動について、他の RIR（地域インターネットレジストリ）が取り組んでいるプロジェクトを概説する。

具体的には APNIC における CA（Certification Authority）プロジェクト、RIPE における WebUpdates および LIR Portal プロジェクトとなる。また、ARIN については分散データベースの取り組みとして提供されている RWhois システムを取り上げる。

このうち APNIC と RIPE は SSL を用いたウェブインターフェースを提供している。中でも APNIC の CA プロジェクトの一環として運用されている MyAPNIC では X.509 形式の公開鍵証明書（以下では証明書とよぶ）をサーバだけでなくクライアントにも発行することでサーバ、クライアント間の相互認証を実現している。証明書ベースのクライアント認証を行なうことで、ウェブアプリケーションによく見られるパスワード認証に比べ、遥かに高い信頼性を与えることを可能としている。

今回取り上げた APNIC、ARIN はともに RIPE の開発するデータベースシステムを採用しており、RPSL（Routing Policy Specification Language）を使用している。

本章の終わりに、この RIPE のデータベースシステムについての概要を述べる。

3.1. APNIC

APNIC は Asia Pacific 地域を管轄とする RIR である。APNIC では 1999 年から PKI に対する取り組みを行なっており、パイロット運用を行なっている。

APNIC は管轄地域の IP アドレス割り振り、割り当てに関する権限を持っている。IP アドレスと、それに関する提供情報の価値というものは極めて高いものであり、APNIC の業務と提供情報を正しく維持し、提供することは、インターネット運用上、重要な役割であると考えられる。

- IP アドレス
- AS 番号
- 逆引き情報
- whois 情報

PKI 導入プロジェクトが開始されたのは、APNIC とメンバーのやりとりが非同期の電子メールによるコミュニケーションで行われていることに対する反省が元になっている。

例として、新たに IP アドレスの割り振りを申請する手続きは図 16 のようになっている[16]。

図 16　APNIC における IP アドレス割り振り申請プロセス

この手続きの間、通信経路およびフォームやメールといった情報そのものに特別な保護対策は施されていない。

また、メンバー登録により PIN（Personal Identification Number – 個人識別番号）が発行され、メンバーの認証は、この PIN により行なわれる。つまり、パスワード認証とほぼ同等程度の安全度しか持たない。

メンバーからも、電子メールの認証とプライバシー、およびウェブサイトの認可についての関心が寄せられ、1999 年から 2000 年にかけての第 8 回、第 9 回および第 10 回目の APNIC Open Policy Meeting では、PKI に関する取り組み開始の発表と議論が行なわれた。

より高度なセキュリティを実装するため、1999 年 10 月から 3 ヶ月かけて、PKI の導入による影響の分析、議論のための論点を提供、PKI に関する意識の向上を目的とした Scoping Project が実施された。

さらに Scoping Project の成果を受け、2000 年 4 月から 5 月にかけて Pilot Project

[16] “APNIC IPv4 ISP Request Form”, http://ftp.apnic.net/apnic/docs/isp-address-request

が実施され、PKI を導入する領域の特定、ソフトウェアと手順の開発のスケジュール、リスク分析が行なわれた。

この成果はレポートにまとめられ公開されている。その中で、PKI 導入の試みに関する目的および利点については次のように述べられている。

- APNIC のリソースの不正使用、改ざんを防ぐ。
- ビジネスをより安全に、より良い方向に変えていく。
- これにより中核となるリソースを更に保護できる。
- メンバーとメンバー情報を管理する必要がある。
- APNIC サービスの安全性について改善さらに効率も改善する。

また、ここ数年間に行なわれた PKI および CA 運用に関するプロジェクトは表 12 のようになっている。

表 12　APNIC における PKI および CA 運用に関するプロジェクト

実施時期	プロジェクト
1999 年	Scoping Project 開始
2000 年	Pilot Project 開始
2001 年	MyAPNIC Project 開始

プロジェクトに関する討論の場として、年に二回開催される APNIC Open Policy Meeting では CA に関する BoF が催されている。

表 13 は同ミーティングでの CA プロジェクトに関する発表のリストである。

表 13　APNIC Open Policy Meeting での CA プロジェクトに関する発表

会合	表題
2000 年 APNIC 10 ブリスベーン	APNIC Certification Authority project
2001 年 APNIC 11 クアラルンプール	CA Scoping Project Report
2001 年 APNIC 12 台北	APNIC MyAPNIC project Use of certificates in routing validation

3.1.1. Scoping Project

このプロジェクトはパイロット実装に先立って、必要な要件を定義するために行なわれた。

結論として、メンバーのセキュリティに大きな利点があること、PKI をサポートする標準の育成が重要であることなどがあげられている。

3.1.2. Pilot Project

証明書の利用により、APNIC のメンバーと顧客のために拡張された安全なサービスを提供するために CA を運用する。このサービスの一部として、APNIC はメンバーに証明書を発行することになる。これが Pilot Project である。

このプロジェクトにおいて、APNIC の CA サービスは次の契約条件のもとに提供される：

- CA サーバシステムは安全な環境で維持され、APNIC 内部ネットワークまたはインターネットに接続されることはない。
- APNIC は、プライベート鍵の生成、データの転送、APNIC により運営される他の安全なシステムといった同様の標準に対しての仲介システムを制御する。
- 署名された鍵ペア生成手続きは、アイデンティティの適切な保証を利用する、これはパスポートや他の公式な写真付のアイデンティティ文書のことである。

- APNIC は、鍵の生成、配布、安全な廃棄が行われることを保証する CA サービスプロセスにおいてリーズナブルな対処を行う。

- APNIC は、提案される CA サービスのステータスの変更、鍵ペアの変更について、証明書所有者と連絡を行う。

- APNIC は、APNIC により発行されるデジタル証明書の利用により生じる、信頼の喪失、またはダメージを許容しない。

- APNIC CA により発行されるデジタル証明書の受領者は、証明書の利用により生じるいかなる種類の損害についても、第三者からのクレームに対して、APNIC に補償を行なう。

3.1.3. APNIC の業務に対する PKI の導入

APNIC の業務に PKI を取り入れることについて Pilot Project が行った提案についてまとめる[17]。この提案は 2000 年当時のものである。

この提案では次の処理について述べられている。

- 新規メンバー登録
  - 書面による登録フォームの処理
  - 鍵と証明書要求の生成
  - オンラインでの証明書要求の処理
  - 証明書利用可能および証明書取得手順の通知
  - 新メンバアカウントの初期化
- 安全なオンライン要求の送信
  - APNIC ウェブベースオンラインサービスの強力な認証
  - オンラインサービス要求の完遂
  - SSL を通じた電子署名および転送
  - APNIC によるオンライン要求の検証
  - APNIC によるオンライン要求の処理
- APNIC メンバアカウントの終了
  - アカウントのクリーンアップ、終了
  - (可能であれば)証明書の廃棄

[17] “APNIC PKI pilot project Report”, https://www.apnic.net/ca/ca-scoping.pdf

この報告で提案されている各種手続きについての詳細を以下で述べる。

- 新規メンバー登録（書面による登録フォームの処理）

新規メンバー登録手続きは図 17 のような流れとなる。RA（Registration Authority）は、CA の機能の一つで、証明書の発行要求を受け付けと登録を行う。

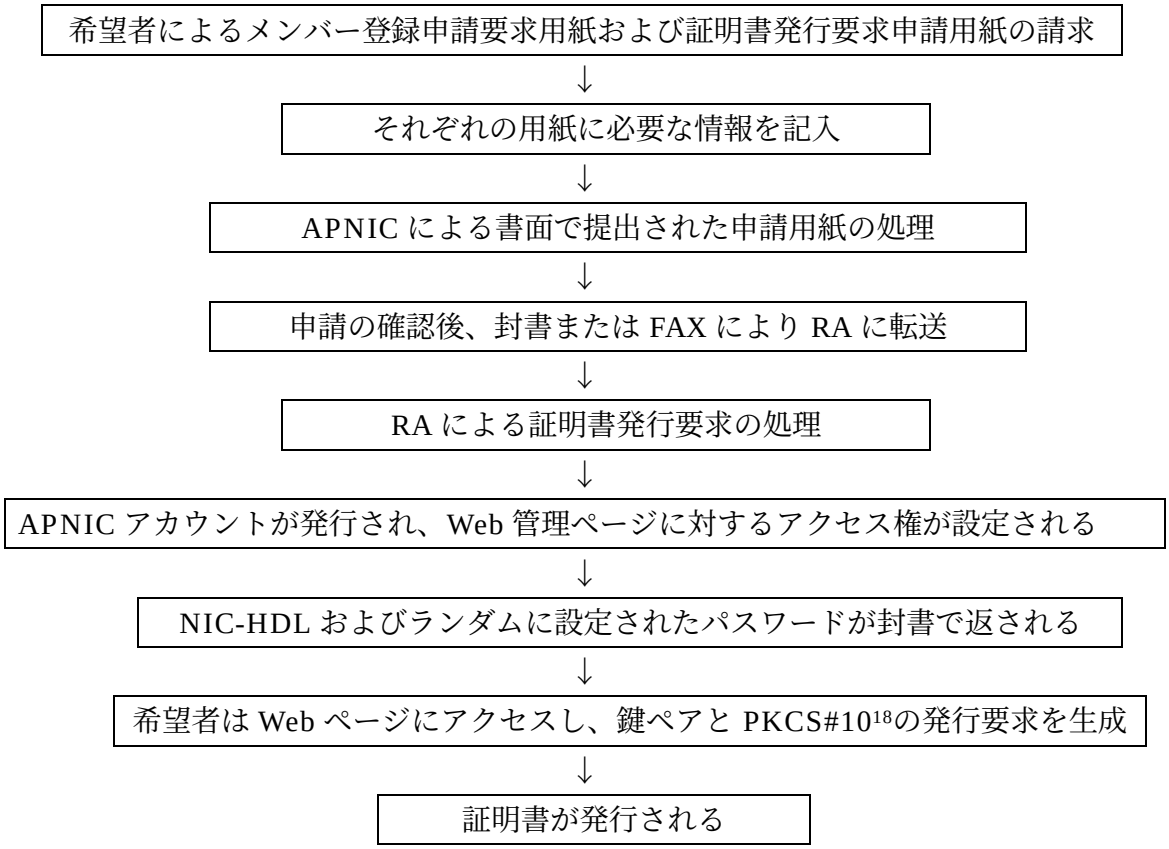
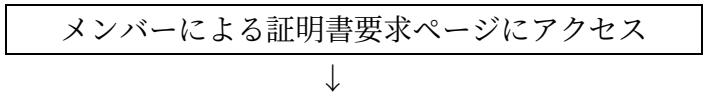


図 17　新規メンバー登録（書面による登録フォームの処理）

ここでは封書を用いてトランザクションが行なわれることになっているが、現在では SSL を用いた Web ケーションによる申請の試みが行なわれている。

- 新規メンバー登録（鍵の生成と証明書要求の処理）

新規メンバー登録手続きのうち、鍵の生成と証明書要求の処理は図 18 のようになる。



[18] PKCS#10, “Certification Request Syntax Standard”, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.ps

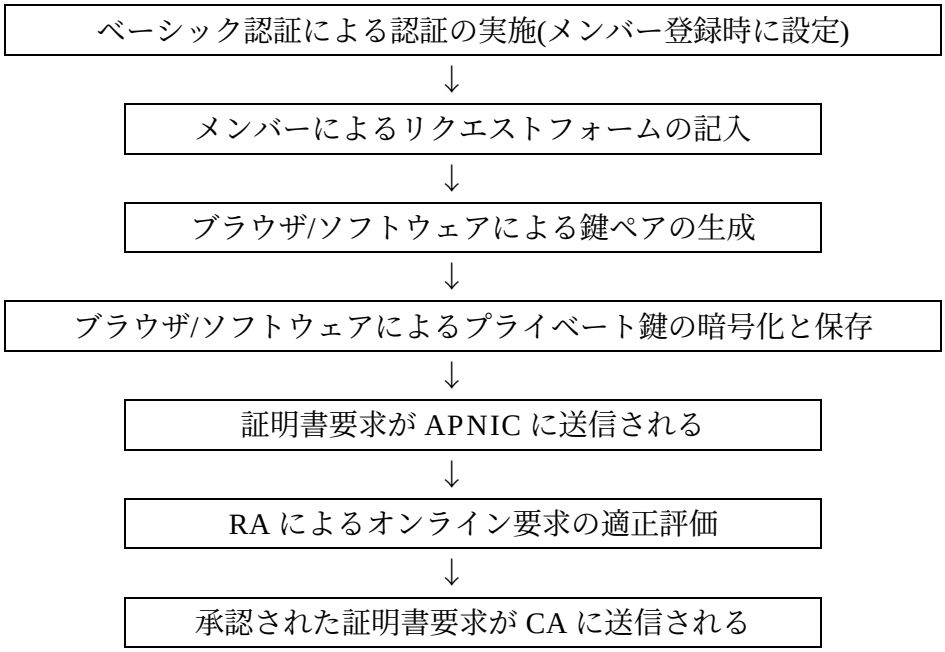


図 18　新規メンバー登録（鍵の生成と証明書要求の処理）

- 新規メンバー登録（新規アカウントの初期化）

新規メンバー登録手続きのうち、新規アカウントの初期化処理は図 19 のようになる。

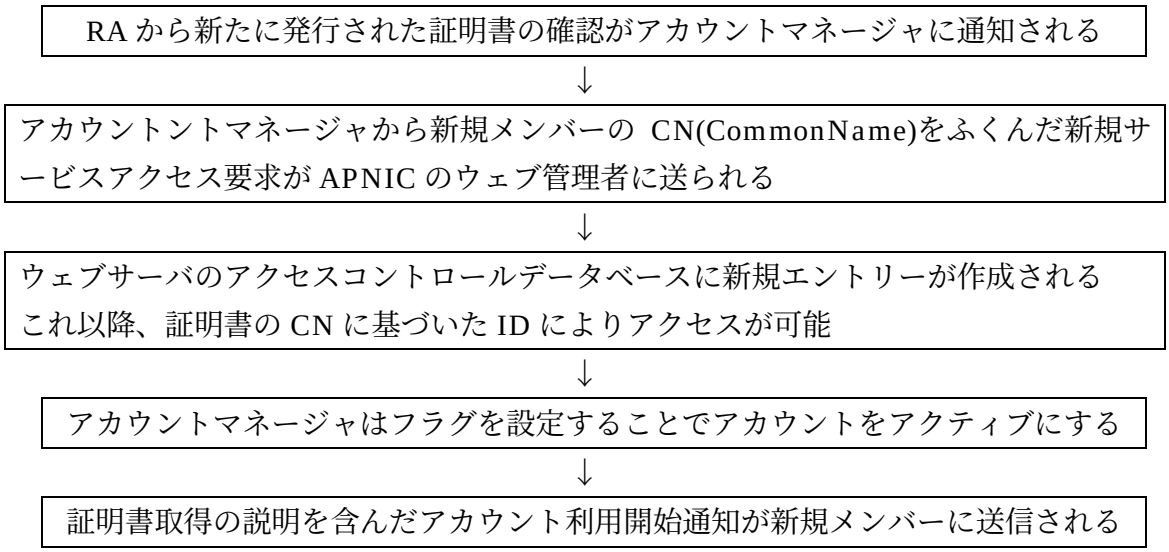


図 19　新規メンバー登録（新規アカウントの初期化）

- 証明書の取得

APNIC CA により生成された証明書は図 20 の手順で取得する。

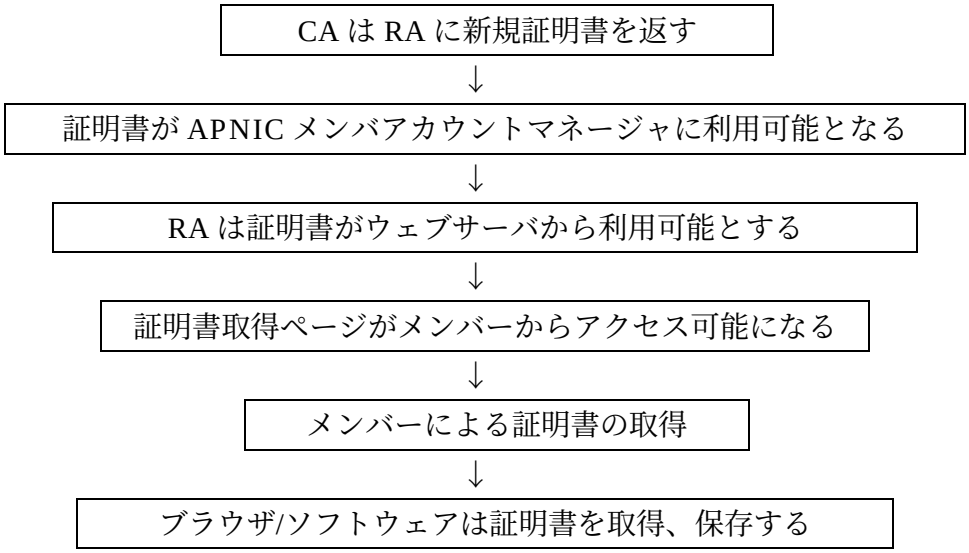
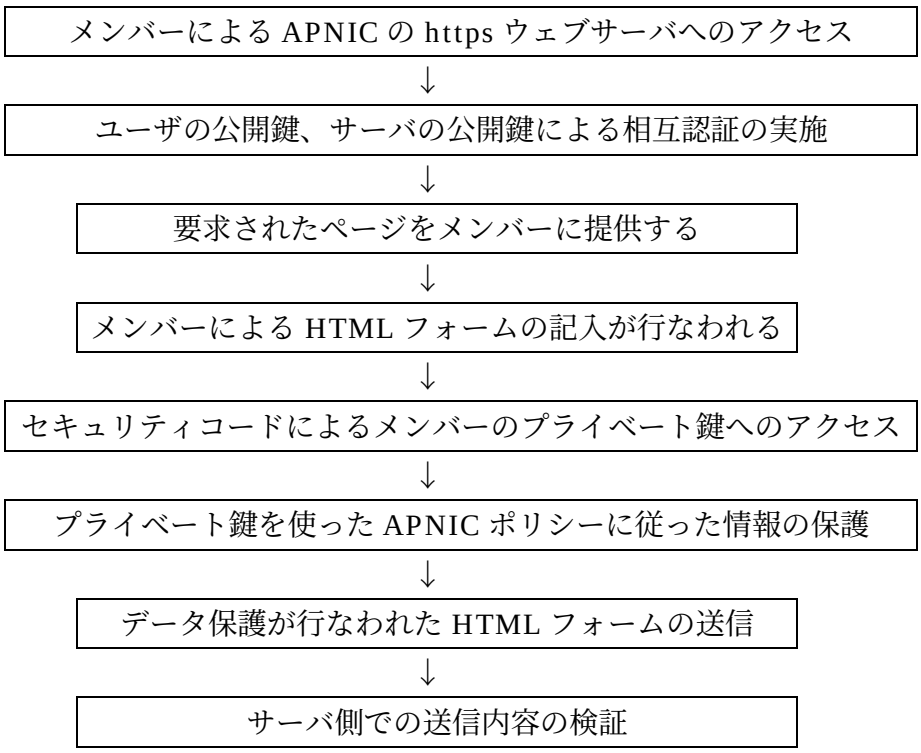


図 20　証明書の取得

この段階でメンバーは APNIC のセキュアオンラインサービスにアクセスするために必要なすべての情報をもつことになる。

- オンラインでのリソース要求

メンバーがプライベート鍵、公開鍵を利用する手順について述べる。



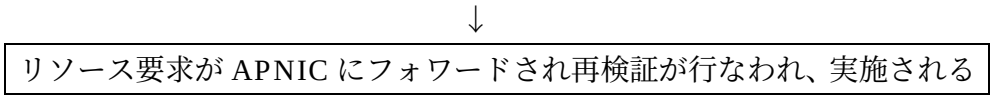


図 21　オンラインでのリソース要求

- オンラインでのリソース要求処理

APNIC の要求処理システムには RT（Request Tracking） システムが実装されている。RT が要求をどのように処理するのかを図 22 に示す。

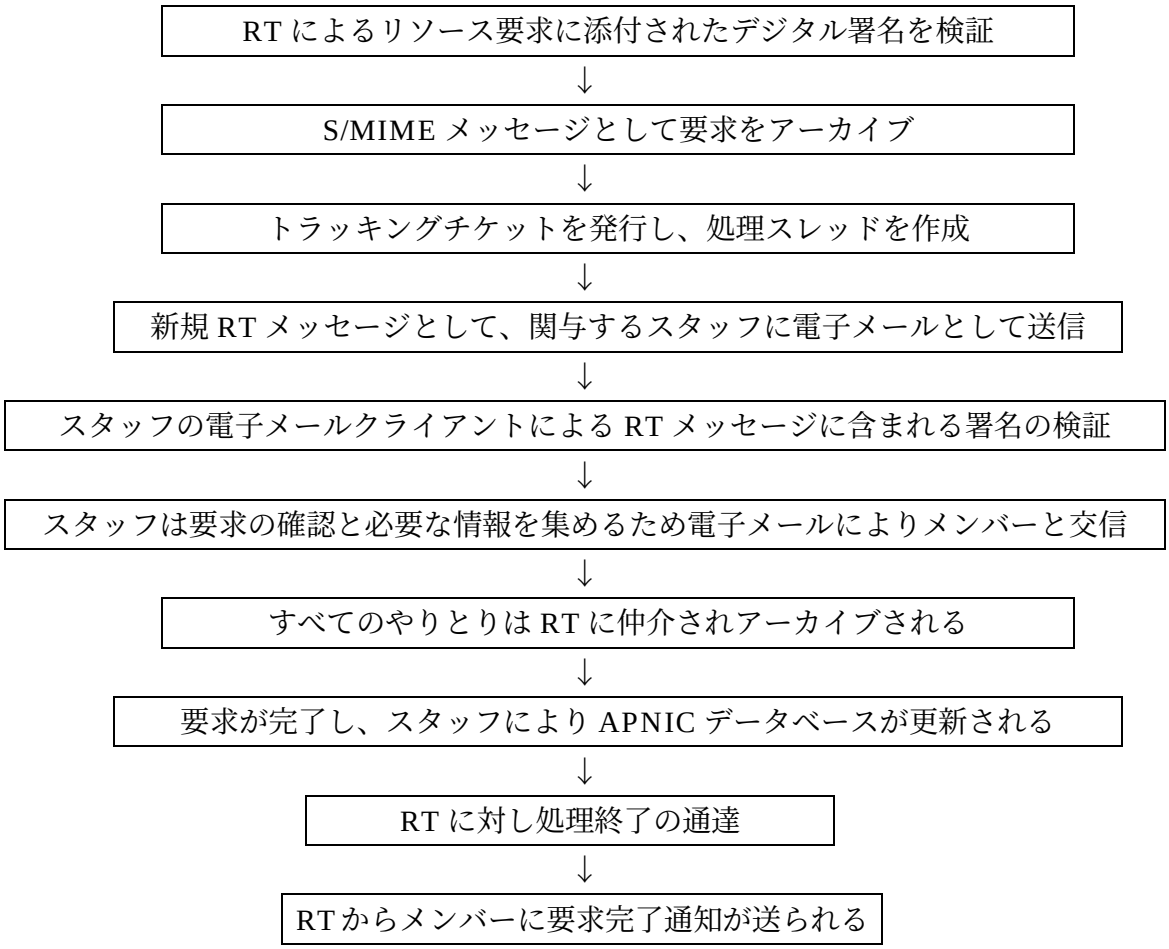
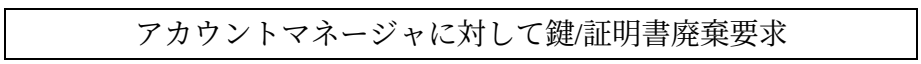


図 22　オンラインでのリソース要求処理

- 証明書廃棄およびアカウントの終了

メンバアカウントの削除および、証明書の廃棄に関する手続きは図 23 のようになっている。



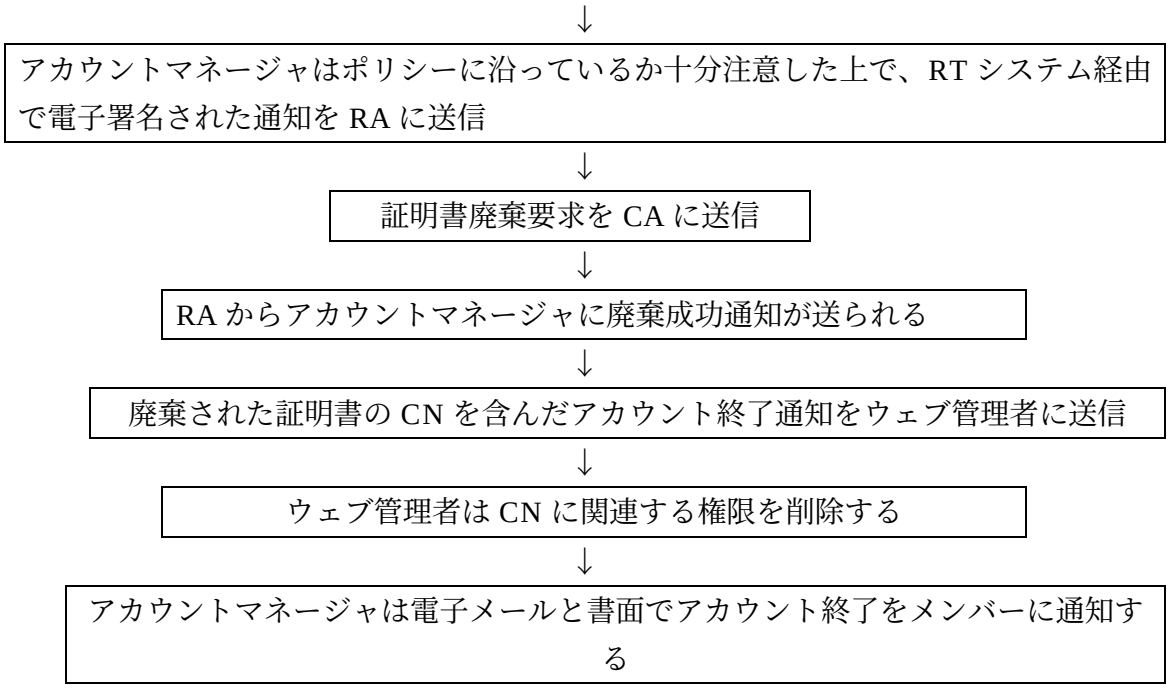


図 23　証明書廃棄およびアカウントの終了

3.1.4. MyAPNIC

MyAPNIC プロジェクトはメンバーに安全なウェブインターフェースを提供し、そのインターフェースを通じた、メンバーの個人情報へのアクセスおよび APNIC サービスの利用を可能とすることを目的としている。このプロジェクトは PKI を利用したもので一連の CA プロジェクトのプロトタイプとして位置付けられている。

プロジェクトの動機となった問題点として次のものがあげられている。

- メンバーが whois 登録情報に関して変更が発生したとしてもデータベースを更新しようとしない。
- 熟練度のギャップが APNIC のホストマスタたちに余計な仕事を作り出している。
- APNIC とメンバー間のセンシティブな情報やりとりがより良い保護機構を要求している。
- 電子メールによるリクエストフォームにはタイプエラーの傾向があり生産性を低下させている。
- メンバシップ価値の向上の試み。

プロジェクトのシステムは図 24 のように構成される。

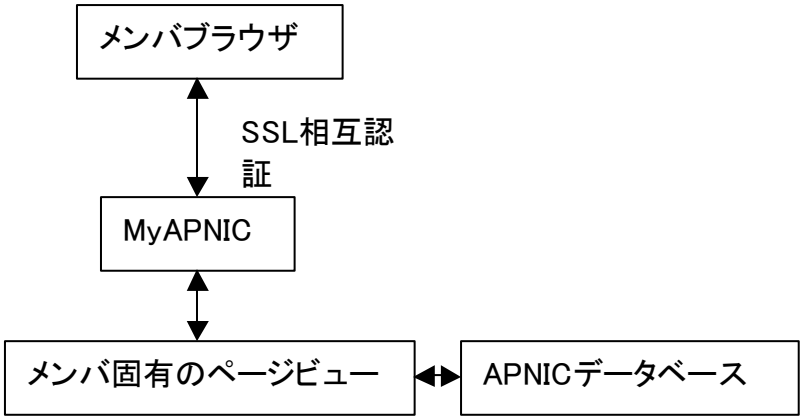


図 24　MyAPNIC の構成

MyAPNIC のコンセプトは次のように表明されている。

- 容易な利用
  - インターネットリソースデータベースの更新を奨励
  - 習熟曲線の短縮
  - シンプル、ユーザは割り当てられた画面だけを見る
  - APNIC がすでに情報を持っていれば予めフォームに入力
- 安全
  - サーバとクライアントの双方が SSL 認証で保護
  - APNIC は trusted CA の役割を果たす
  - 正しいクレデンシャルを持つものだけが情報を見ることが可能(クライアント証明書に束縛)
- 柔軟性
  - メンバーに自身の組織構成に合うユーザベースとオーソリティを設定可能
  - 更なるサービス拡張のプラットフォームを提供

また、機能として次のものが実装される。

- リマインダ
- インターネットリソース管理
- 財政/管理
- 訓練
- セキュリティ

実際のデモ環境では次のものが実装されている[19]。

- 割り当てグラフ

ここではメンバーが割り振られたネットワークごとの割り当て済みアドレスがバーグラフとして表示される。これを参照することで追加割り振り要求を申請する必要があるかどうかを判断することができる。

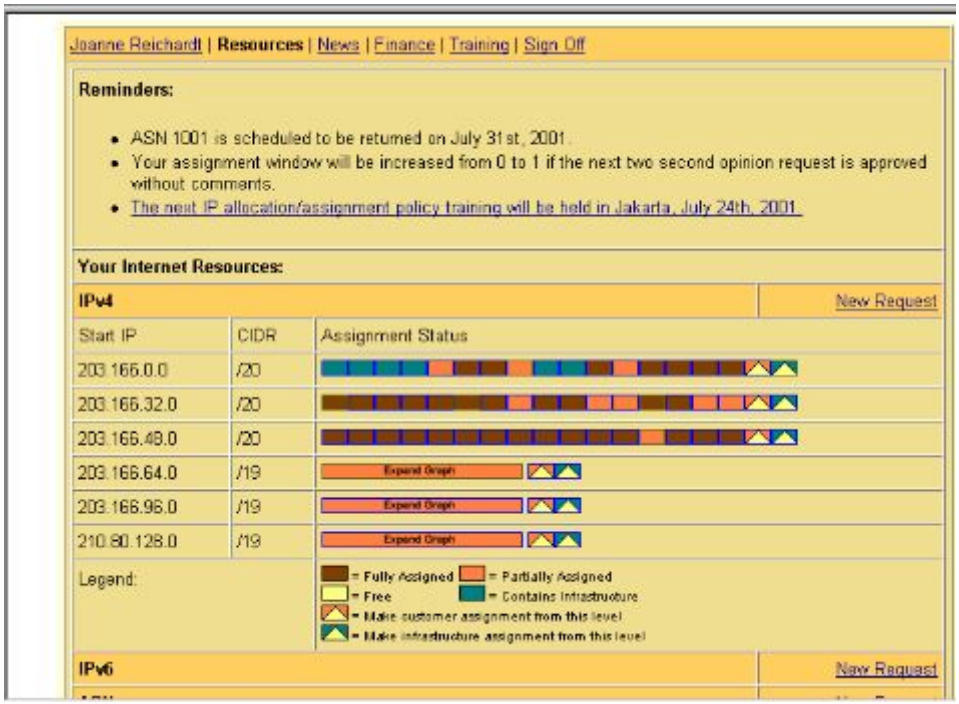


図 25　MyAPNIC 割り当てグラフ

- 割り当て表

ここではメンバーが所有するネットワークごとの割り当て実績に関する情報を表形式で一覧することができる。

[19] http://www.apnic.net/meetings/12/docs/My-APNIC.ppt から抽出

図 26　MyAPNIC 割り当て表

- 割り当て編集

ここでは選択したネットワークに関する情報のうち、ネットワーク名、デバイスの数、サブネットの数、割り当て日時について、オンラインで編集することができる。

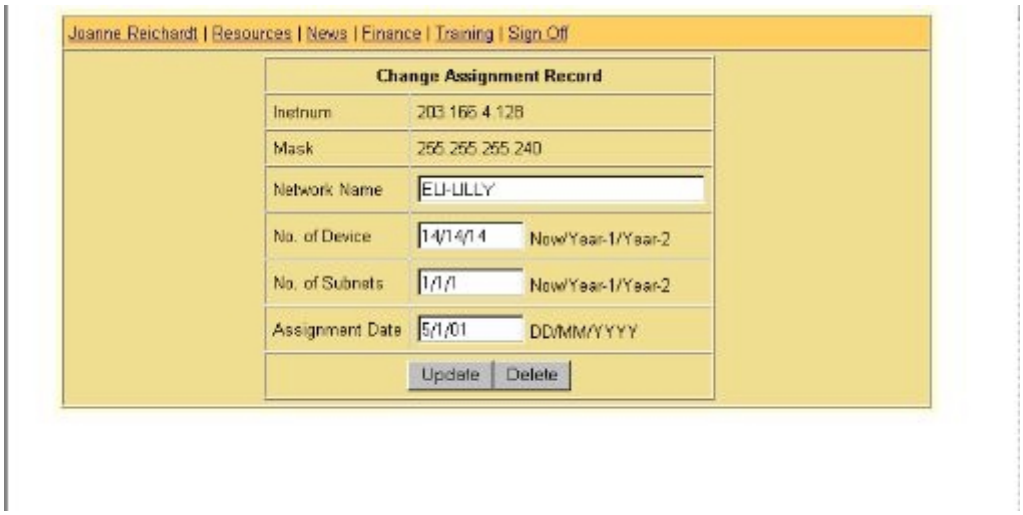


図 27　MyAPNIC 割り当て編集

- 新規割り当て

ここでは所有するネットワーク情報に新規割り当てレコードを登録することができる。その情報は、ネットワークアドレス、ネットワークマスク、ネットワーク名、デバイスの数、サブネットの数、割り当て日時となっている。

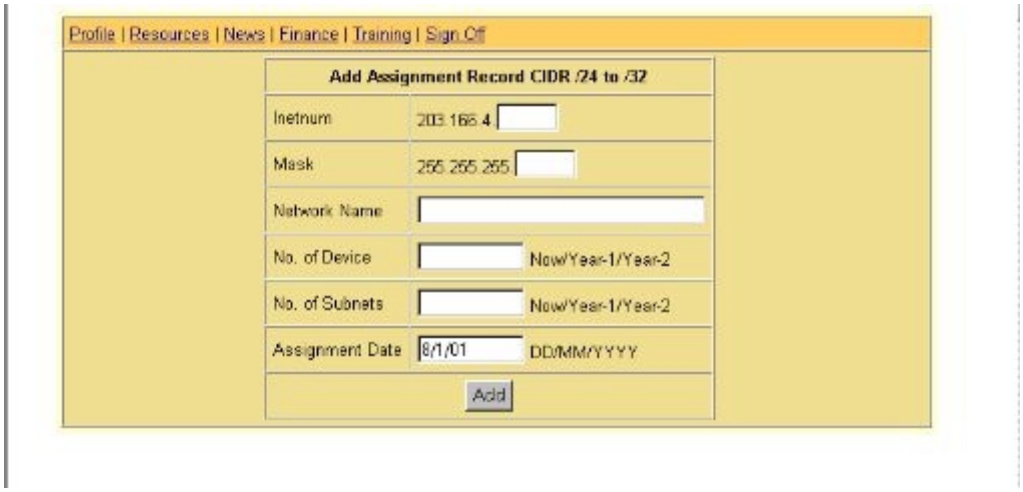


図 28　MyAPNIC 新規割り当て

- プロファイル編集

ここではメンバーのプロファイル情報を編集することができる。その情報は、フルネーム、ポジション、アドレス（都市、州、国、郵便番号）、電話番号、ファックス番号、ホームページ、電子メールアドレスとなっている。

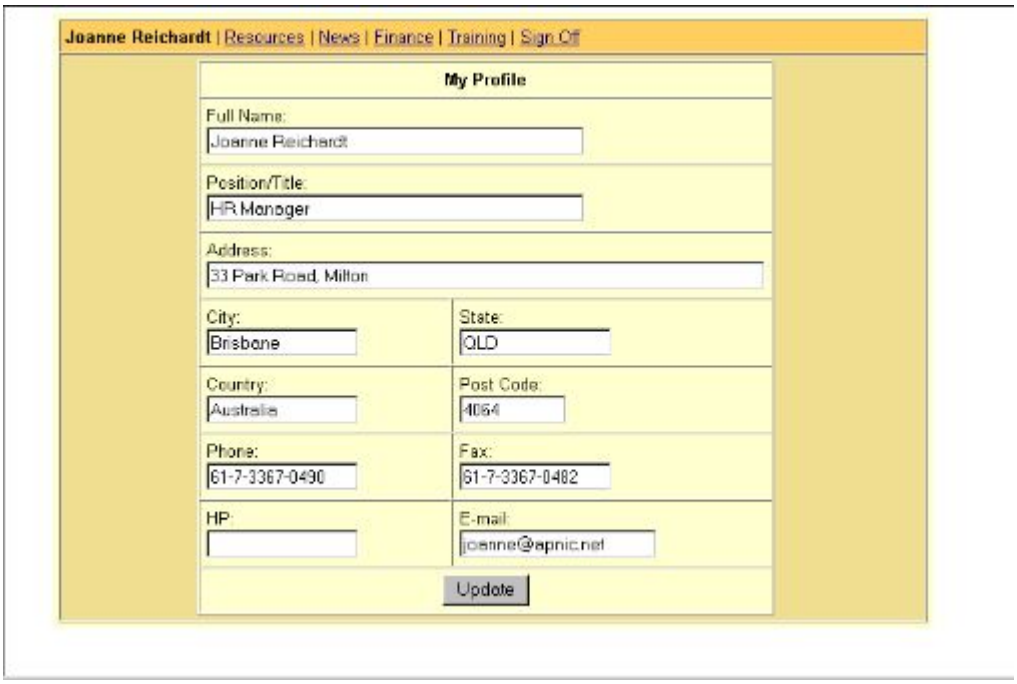


図 29　MyAPNIC プロファイル編集

3.1.5. 今後の展開

APNIC CA プロジェクトの今後の展開に関しては次のような議論が行われている。

- CA 機能の一般化
  - APNIC の証明書を汎用目的で使う
  - 信頼を確保するため APNIC 証明書の強固なポリシー作成と質の高いフレームワークの確立
- 階層的証明
  - APNIC のメンバーが彼ら自身のメンバーや顧客を証明するために、自身の証明書を使う
  - ISP や NIR に利用可能
- 公開鍵証明書
  - アイデンティティの公開鍵にリンクされる証明書（CA が発行）
- 属性証明書
  - アイデンティティの属性にリンクされる証明書（CA または他のオーソリティが発行）
  - 認証のみならず認可情報を提供

（属性証明書は広く採用されてはいない）

3.2. RIPE NCC

RIPE ではデータベースワーキンググループにてセキュリティに関する議論が行なわれている。

1998 年、1999 年とデータベースセキュリティタスクフォースで議論が行なわれていたが、2000 年 2 月の RIPE Meeting 第 35 回以降はワーキンググループに話し合いの場が移された。

2001 年 4 月の同ミーティング第 39 回の会議では PGP でも保護されたオブジェクトが全体の 2%に過ぎないことが報告された。また同じ会議で PGP ライセンスサービスの停止を求める提案がなされた、これは既知の問題のある PGP を使ったライセンスが発行されていること、新しいデータベースが GnuPG を使っていることが理由とされている。

同ミーティング第 42 回の会議では MD5-PW スキームがテストデータベースに導入されたことが報告された。またハッシュパスワードを remarks オブジェクトに埋め込む方式が提案された。

2002 年 9 月の同ミーティング第 43 回では、メインテナの 41%が MD5-PW スキームを利用していることが報告された。この会議では電子メールベースのインタラクションがビギナーには複雑であることから、データベースアクセスにウェブインターフェースを実装することが提案されている。この実装は WebUpdates と呼ばれており、オブジェクトの追加、削除、修正が可能となっている。しかし、パスワード認証のみであること、パスワードがクッキーに保存されることから、この段階ではプロトタイプに過ぎない（このプロトタイプは既に公開されていない）。

3.2.1. オブジェクトの保護

RIPE のデータベースでは、あるオブジェクトが変更されると、そのオブジェクトの所有者であるメインテナに通知されるように設定を行なうことが出来る。また、変更の際に認証を必須とするためにいくつかの認証スキームが設定可能である。この認証スキームを用いるためには以下の手順を実施する。

- mntner オブジェクトに auth:属性を追加
  - NONE、無認証
  - MAIL-FROM、指定した正規表現がメールヘッダの From:に適合することを検

証。容易に成りすましが可能なため推奨されない（すでに使われない）
  - CRYPT-PW、UNIX CRYPT フォーマットによるパスワード検証。パスワードが平文で通信されるため推奨されない
  - MD5-PW、ハッシュパスワード検証。CRYPT-PW よりは良いが強力なものではない。
  - PGPKEY、公開鍵暗号に基づく認証。提供される認証機構中で最も強力
- 認証を要するオブジェクトに mnt-by 属性を追加
- 選択した認証スキームに対するパスワードまたは公開鍵を登録(パスワードの場合は auth: 属性、公開鍵の場合は key-cert: オブジェクトを登録し、auth: 属性には、その ID を登録する)

3.2.2. WebUpdates

現在、WebUpdates は SSL ベースのアプリケーションとして稼動しており、サーバ証明書は米 RSA Security 社によって発行されたものである。このアプリケーションは SSL 経由でも通常の HTTP でもアクセスできる[20]

このインターフェースはサーバ認証のみであり、RIPE 自身での CA 運用もされていない。

RIPE Meeting 第 43 回で WebUpdates の発表が行なわれている。Synchronous Updates and Web Updates in RIPE Database[21]がそれである。

その発表で述べられた現状の更新システムの問題は次のものである。

- 自動化、または管理化の観点から便利なものとはいえない
- 要求の提出と処理に遅れがあり、またどの程度遅れるのかわからない
- ビギナーを悩ませることがある（提出した要求に不備があった場合、エラーメールが送り返され、それに対して再びメールを返して、などしていると効率的でない）
- ほとんどのユーザにとっては電子メールによるインタラクションはなじみの無いものである

そして解決策として次の二つが提案されている。

- 同期した更新の仕組み – syncupdates
- syncupdates に対するウェブインターフェース – WebUpdates

syncupdates が同期するものはいるのは、ユーザが提出した追加、削除、変更要求が

[20] “Web Updates for RIPE Database”, http://www.ripe.net/webupdates/
[21] http://www.ripe.net/ripe/meetings/archive/ripe-43/index.html

直ちに受理されるということであり、実際にデータベースに反映させるのは既存のシステムであるため、処理終了通知は従来どおり電子メールにより送信される。

しかし、インターフェースの時点でデータの不備などは判明するため、以前の電子メールによるやり取りに比べてストレスの少ないものとなることが期待されている。

このシステムの課題としては、ユーザのローカルホスト上にパスワードが格納されるという単純な認証しか行なっていないことから、PGP による認証機構の実装があげられている。

3.2.3. LIR Portal

LIR Portal は、2002 年 9 月からベータテストが開始されたサービスで、LIR による RIPE NCC へのアクセスの増加を受け、ウェブインターフェースを提供することで遅延の減少を目的とするものである。

サポートされる機能には次のものがある。

- LIR コンタクト情報、アドレス情報の閲覧と編集
- 支払い情報の閲覧
- IP および AS リソースの閲覧
- オープンチケット状況の閲覧
- ニュースおよびイベント

このウェブサービスは SSL を通じて提供される。利用するためには、前もって登録を行なう必要がある。

3.2.4. RPSL (Routing Policy Specification Language)

RPSL とは Routing Policy Specification Language [22]で定義されるルーティングポリシー記述言語である。ネットワークオペレータは様々な階層でこの記述を使ってポリシーを定義することができる。

この言語はオブジェクト指向言語として設計されており、オブジェクトがポリシーと管理情報を持つことになる。定義されたオブジェクトは IRR（Internet Routing Registry）に格納される。

---

[22] RFC2280, “Routing Policy Specification Language (RPSL)”, http://www.ietf.org/rfc/rfc2280.txt

表 14 は経路オブジェクトの構造定義を示している。このように RPSL のオブジェクトは（属性、値の概要、値の型）として定義される

表 14　RPSL オブジェクトの例

Attribute	Value	Type
route	<address-prefix>	mandatory, single-valued, class key
origin	<as-number>	mandatory, single-valued, class key
withdrawn	<date>	optional, single-valued
member-of	list of <route-set-names> see Section 5	optional, single-valued
inject	see Section 8	optional, multi-valued
components	see Section 8	optional, single-valued
aggr-bndry	see Section 8	optional, single-valued
aggr-mtd	see Section 8	optional, single-valued
export-comps	see Section 8	optional, single-valued
holes	see Section 8	optional, single-valued

RPSL の目的は、実際にルータで利用される経路情報に加え、管理情報をデータベースとして提供することにある。

3.3. ARIN

ARIN は RPSL によるデータベースを管理しており、その保護の仕組みも RIPE と同様のものである。ARIN には RIPE のデータベースワーキンググループと同様の組織としてデータベース実装ワーキンググループが機能しており、1999 年 4 月の会合でデータベース保護について話されている。

3.3.1. RWhois

RWhois は ARIN により開発されている分散型の whois サービスのことである。従来の whois サーバは中央集権的データベースを持っている。これに対し RWhois では階層的でスケール可能なやり方でデータベースを保持する。RWhois については Referral Whois (RWhois) Protocol V1.5 [23]に詳細が述べられている。

[23] RFC2167, “Referral Whois (RWhois) Protocol V1.5”,

これは一種のディレクトリサービスと位置付けられ、whois のコンセプトを階層的に拡張したものといえる。インターネットをまたいでリソースを発見するための効率的なプロトコルを目指しており、分散データベースである DNS システムを参考にしている。

ある RWhois サーバに対する問い合わせが解決されなかった場合、サーバは、答えを知っているサーバに近いところにあると考えられるサーバへと、クエリを再配送する。これは DNS の再帰問い合わせのメカニズムである。

現状の問題として、分散データベースであるにも関わらず、RWhois サーバを稼動させているインターネットレジストリが少ないため、本来のメリットが生かせないことがあげられる。

しかし、ネットワーク資源の今後の更なる増加を考えると RWhois のような分散データベースの重要性は増すと考えられる。

3.4. RIR の whois システム

ここでは RIR における情報提供サービスである whois システムの外部インターフェースと提供される情報について解説を行なう。システムは ARIN の提供するものと RIPE の提供するものの二つが存在する。APNIC、LACNIC については共に RIPE の開発しているシステムを用いている。

whois サービスは一般に公開されているサービスであるため、提供される情報について知ることは、サービスに必要な保護についての考察を行なう上で重要であると考えられる。

特に組織情報、個人情報には、住所、電話番号といったプライベートな情報が含まれることから、第三者による不正な改ざんから保護すること、また特定の情報についてはビジネス上の観点からアクセス制限を施すことが必要となることも考えられる。

3.4.1. ARIN

ARIN の Whois サービスは ARIN に登録されたリソースのコンタクトおよび登録情報を検索するためのメカニズムを提供する。ARIN のデータベースは IP アドレス、AS 番号、それらのリソースに関連する組織または顧客そして関連するポイントオブコンタ

---

http://www.ietf.org/rfc/rfc2167.txt

クト（POC）を含む。ARIN の Whois はドメイン関連情報、また軍関係の情報を持つことは無い。

実際に www.arin.net 192.149.252.17 のデータを検索すると表 15、表 16、表 17 の出力が得られる。

- Organization Information

表 15　ARIN の whois 出力（組織情報）

OrgName:	American Registry for Internet Numbers
OrgID:	ARIN
Address:	3635 Concorde Parkway, Suite 200
City:	Chantilly
StateProv:	VA
PostalCode:	20151
Country:	US

- Network Address Space Information

表 16　ARIN の whois 出力（ネットワークアドレス空間情報）

NetRange:	192.149.252.0 - 192.149.252.255
CIDR:	192.149.252.0/24
NetName:	ARIN-NET
NetHandle:	NET-192-149-252-0-1
Parent:	NET-192-0-0-0-0
NetType:	Direct Assignment
NameServer:	RS1.ARIN.NET
NameServer:	NS.NETSOL.COM
NameServer:	RIP.PSG.COM
Comment:	
RegDate:	1997-11-05
Updated:	2002-04-05

- Contact Information

表 17　ARIN の whois 出力（コンタクト情報）

```
TechHandle: IP-FIX-ARIN
TechName:   ARIN IP Team
TechPhone:  +1-703-227-0660
TechEmail:  hostmaster@arin.net
OrgTechHandle: IP-FIX-ARIN
OrgTechName:   ARIN IP Team
OrgTechPhone:  +1-703-227-0660
OrgTechEmail:  hostmaster@arin.net
OrgNOCHandle: ARINN-ARIN
OrgNOCName:   ARIN NOC
OrgNOCPhone:  +1-703-227-9840
OrgNOCEmail:  noc@arin.net
```

情報の非公開については “Instructions for Executing ARINs Non-Disclosure Agreement” [24]に詳細が記載されている。ここには ARIN に送信した情報のうち、組織にとってプロプライエタリな情報について非開示契約を ARIN と組織の間に結ぶ際の手続きについて書かれている。

プロプライエタリな情報とは次のようなものと定義され、またそれに限定される。

- ネットワークエンジニアリング計画(次のものを含む、サブネット、ホスト数、サブネット辺りのホスト数)
- ネットワーク配備計画（それぞれのサブネットの主要なマイルストーンを含む）
- 申請者によって作成されたネットワークトポロジー図(一般に公開されたものを含まない)
- 申請者が、無制限な開示、コンペティティブな利用に対抗して保護するこ

[24] “Instructions for Executing ARINs Non-Disclosure Agreement”, http://www.arin.net/library/agreements/nda.pdf

とを希望するその他の情報(この NDA に従って提出されたと互いに合意し、ARIN に提出された際にプロプライエタリであると明確に特定されたもの)

その情報がプロプライエタリであることを明示するために、申請書類ではボールドフェイスで記入されることになっている。

3.4.2. RIPE

RIPE Network Management Database の要素として IP アドレス情報が格納されている。

www.ripe.net 193.0.0.203 を検索すると次の出力が得られる。

```
netnum:        193.0.0.0 - 193.0.1.255
netname:       RIPE-NCC
descr:         RIPE Network Coordination Centre
descr:         Amsterdam, Netherlands
country:       NL
admin-c:       DDL122-RIPE
tech-c:        OPS4-RIPE
status:        ASSIGNED PI
remarks:       used to be two different /24 inetnum objects
remarks:       until 19990305  (ripe-ncc & ripe-meeting)
mnt-by:        RIPE-NCC-MNT
mnt-lower:     RIPE-NCC-MNT
changed:       orange@ripe.net 19960815
changed:       GeertJan.deGroot@ripe.net 19970110
changed:       mir@ripe.net 19970506
changed:       ripe-dbm@ripe.net 19970819
changed:       wilhelm@ripe.net 19990305
changed:       inaddr@ripe.net 19990705
changed:       hostmaster@ripe.net 20010119
changed:       hostmaster@ripe.net 20020410
source:        RIPE
```

3.5. RIPE Database System

RIPE データベースは RPSL を用いている。RPSL はインターネット経路情報レジストリに高度なセキュリティを提供する認可メカニズムを提供する、Routing Policy System Security (RPSS) を実装している。

RIPE ネットワーク管理データベースは IP アドレス空間割り当てと割り振り、経路制御ポリシー、逆引き委譲に関する情報を含むものである。

RIPE データベースの情報はインターネットの公共に提供されるものであるが、著作権は RIPE が所有する。

3.5.1. データベースオブジェクト

RIPE ネットワーク管理データベースは以下のレコードを含む：

- IP アドレス空間の割り当てと割り振り
- ドメイン名 (in-addr.arpa.)
- 経路制御ポリシー情報
- コンタクト情報

データベース中のレコードはオブジェクトと呼ばれる。これには表 18 のものがある。

表 18　データベース中のオブジェクトリスト

Object type (Class name)	短縮形	説明
As-block	Ak	リポジトリに付与された AS 番号の範囲を示す
As-set	As	Aut-num オブジェクトの集合
aut-num	An	データベース中の AS を示す。
domain	Dn	(正引き、逆引き) ドメイン登録
filter-set	Fs	フィルターにマッチする経路の集合
inet6num	i6	IPv6 アドレス空間の割り当て割り振り情報
inetnum	In	IPv4 アドレス空間の割り当て割り振り情報
inet-rtr	Ir	Represents a router in the database.

irt	It	CSIRT のコンタクト、認証情報
key-cert	Kc	メンテナオブジェクトの更新の際に認証に利用される公開鍵証明書
mntner	Mt	メインテナによって保護されるオブジェクトに対する操作（生成、削除、修正）に対して要求される認証情報を特定する
peering-set	Ps	Peering の集合
person	Pn	技術または管理コンタクトの情報
role	Ro	技術または管理コンタクトの情報だが、人間により実行される役割を記述する
route	Rt	インターネットに広報される経路
route-set	Rs	経路の集合
rtr-set	Is	ルータの集合

各オブジェクトには標準テンプレートが用意される。

- as-block

as-block オブジェクトは AS 番号のレンジを委譲するために必要である。このオブジェクトは as-block: 属性によって特定される範囲内の ant-num オブジェクトの生成のための認可に使われる。

```
as-block:       [mandatory]  [single]     [primary/lookup key]
descr:          [optional]   [multiple]   [ ]
remarks:        [optional]   [multiple]   [ ]
tech-c:         [mandatory]  [multiple]   [inverse key]
admin-c:        [mandatory]  [multiple]   [inverse key]
notify:         [optional]   [multiple]   [inverse key]
mnt-lower:      [optional]   [multiple]   [inverse key]
mnt-by:         [mandatory]  [multiple]   [inverse key]
changed:        [mandatory]  [multiple]   [ ]
source:         [mandatory]  [single]     [ ]
```

- inetnum

inetnum オブジェクトは IPv4 アドレス空間の割り当て割り振り情報を含む。

```
inetnum:        [mandatory]  [single]     [primary/lookup key]
```

netname:	[mandatory]	[single]	[lookup key]
descr:	[mandatory]	[multiple]	[ ]
country:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
rev-srv:	[optional]	[multiple]	[inverse key]
status:	[mandatory]	[single]	[ ]
remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
mnt-lower:	[optional]	[multiple]	[inverse key]
mnt-routes:	[optional]	[multiple]	[inverse key]
mnt-irt:	[optional]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- inet-rtr

ルータは inet-rtr クラスで特定される。inet-rtr: 属性はルータを表す妥当な DNS 名である。alias 属性が提示されたならば、それはルータのカノニカル DNS 名である。local-as: 属性は、このルータによって所有もしくは操作される AS の AS 番号を特定する。

inet-rtr:	[mandatory]	[single]	[primary/lookup key]
descr:	[mandatory]	[multiple]	[ ]
alias:	[optional]	[multiple]	[ ]
local-as:	[mandatory]	[single]	[inverse key]
ifaddr:	[mandatory]	[multiple]	[lookup key]
peer:	[optional]	[multiple]	[ ]
member-of:	[optional]	[multiple]	[inverse key]
remarks:	[optional]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- irt

irt オブジェクトは CSIRT のコンタクトおよびセキュリティ情報を表す。アドレスレンジに対するコンピュータおよびネットワークインシデントのハンドリングに責任ある CSIRT を特定するために inetnum または inet6num オブジェクトから参照される。Irt の名前は “IRT-“ で始めなければならない。

irt:	[mandatory]	[single]	[primary/lookup key]
address:	[mandatory]	[multiple]	[ ]
phone:	[optional]	[multiple]	[ ]
fax-no:	[optional]	[multiple]	[ ]
e-mail:	[mandatory]	[multiple]	[lookup key]
signature:	[mandatory]	[multiple]	[ ]
encryption:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
auth:	[mandatory]	[multiple]	[ ]
remarks:	[optional]	[multiple]	[ ]
irt-nfy:	[optional]	[multiple]	[inverse key]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- key-cert

key-cert オブジェクトはサーバに格納される公開鍵のデータベースで、mntner オブジェクトの更新を実施する際の認可に使われる。現在は”OpenPGP Message Format[25]”に準拠した鍵だけがサポートされる。

key-cert:	[mandatory]	[single]	[primary/lookup key]
method:	[generated]	[single]	[ ]
owner:	[generated]	[multiple]	[ ]
fingerpr:	[generated]	[single]	[ ]
certif:	[mandatory]	[multiple]	[ ]

[25] RFC2440, “OpenPGP Message Format”, http://www.ietf.org/rfc/rfc2440.txt

remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- mntner

RIPE データベース中のオブジェクトは mntner オブジェクトを使うことで保護される。このオブジェクトは、生成、削除、修正に必要な認証情報を特定する。このオブジェクトは自動的には生成されず、手動操作によって RIPE データベース管理業務に転送される。

mntner:	[mandatory]	[single]	[primary/lookup key]
descr:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[optional]	[multiple]	[inverse key]
upd-to:	[mandatory]	[multiple]	[inverse key]
mnt-nfy:	[optional]	[multiple]	[inverse key]
auth:	[mandatory]	[multiple]	[ ]
remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
referral-by:	[mandatory]	[single]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- person

このオブジェクトは技術または管理コンタクトに関する情報を含む。いったんオブジェクトが生成されると、person: 属性を変更することはできない。

person:	[mandatory]	[single]	[lookup key]
address:	[mandatory]	[multiple]	[ ]
phone:	[mandatory]	[multiple]	[ ]
fax-no:	[optional]	[multiple]	[ ]
e-mail:	[optional]	[multiple]	[lookup key]
nic-hdl:	[mandatory]	[single]	[primary/lookup key]

remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[optional]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

3.5.2. Queries in the RIPE Database

データベースへの問い合わせは whois プロトコルクライアントを介して行われる。

新しく導入されたメカニズムは、問い合わせの結果を自動的に追跡し、RIPE データベースからのコンタクト情報の取り寄せを制限する機能である。広告などのデータとしての検索を制限するのが目的である。

サーバのレスポンスには一般的な規則がある：

- % サインで始まる出力はレスポンスコードから情報メッセージである。コメントは%サインの後に空白が一つあり、サーバメッセージは%サインのすぐ後に始まる。
- 空行はオブジェクトのデリミタである。
- 二つの空行はサーバレスポンスの終了を意味する。
- レファラルメカニズムを使っている場合、レファラルサーバの出力は修正なしにクライアントに送られる。

3.6. まとめ

RIR のデータベースはいずれも RPSL を用いている。しかし、そのオブジェクトの保護に関しては意見が異なっている。

RIPE NCC では、PGP を使った認証を推奨してはいるものの、PGP になれていないユーザの存在、環境によっては利用上の問題があることなどから、オブジェクトごとに認証に関する選択権を与えていて、必要としないのであれば認証なしで操作できるオブジェクトも多く存在しているという現状となっている。

また、ユーザ管理インターフェースとして WebUpdates を配置しているが、これはサーバ認証を SSL で提供しているのみで、必要でなければ通常の HTTP でもアクセスできるなど、基本的にユーザが必要とするセキュリティを選択して用いればよいという考えに基づいているとものと考えられる。

これに対し、APNIC の CA プロジェクトは証明書の発行を担うことで、PKI の強力な認証機能をユーザに提供するという高い目標を持ったものである。CA の運営に関する課題は多いが、PKI の認証トポロジーと規模拡張性を考えると、今後の応用が期待できる。

ARIN は RWhois の開発を通じて、従来の whois サービスを大きく拡張するスキームを提唱している。DNS に倣った分散データベースサービスである RWhois には、今のところ認証やデータ保護に関する機能が乏しいが、セキュリティ拡張は随時行われていくものと期待される。

いずれの RIR も地域性による制限もあると思われ、データ保護に関するアプローチは異なっているが、保護をどれだけ機能させることができるのかについてはユーザの選択に任されている。

MyAPNIC プロジェクトでは、ユーザの PKI に対する意識の向上を目的の一つに挙げており、ユーザの利便性と安全性に対する検討が行われたことがうかがえる。