第4章 RIR の認証局とセキュリティの動向

内容

- APNIC における動向
    1. RFC3779 BoF
    2. MyAPNIC と証明書発行数
- RIPE NCC における動向
    1. 認証局と Database の連携
    2. 今後の方向性に関する情報交換
- ARIN における動向
    1. 証明書の用途
    2. チュートリアルの内容

第4章　RIR の認証局とセキュリティの動向

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」を通じて、各 RIR が、認証局の構築をはじめとする安全性向上の方策を取っていることがわかった。ユーザの管理と認証局を組み合わせ方は RIR によって様々な方法を取っている。またレジストリデータの登録者の考え方が異なっていた。

2004 年度の調査研究では、更に各 RIR の担当者および責任者と直接的にヒアリングを行い、認証局のマネジメントに関する知見の交換を行なった。これらのヒアリングを通じて、レジストリデータの登録者に対する認証を目的とした限定的な認証局であることが判明してきた。また APNIC や RIPE NCC の認証局は、利用が強制されていないにも関わらず証明書発行数が伸びている。逆に JPNIC において検討が進んでいる業務モデル、CP/CPS の策定、レジストリデータの応用の為の認証局について、RIR の認証局の担当者にとっての参考情報として、一定の注目があることがわかった。各 RIR が認証局の構築の模索を行ってきており、参考事例が少ないという経緯が原因として考えられる。

本章では各 RIR のミーティングと各 RIR の認証局担当者と行ったミーティングを通じて得られた認証局と登録情報のセキュリティに関する動向について報告する。

4.1. APNIC における認証局マネジメントの動向

■APNIC CA の動向

APNIC CA は APNIC メンバに使われる証明書を発行している認証局である。証明書は、APNIC とメンバとのメールの保護や MyAPNIC（Web インターフェースを持つ資源管理システム）へのアクセスの保護に使われる。

APNIC CA が発行した証明書の発行数は順調に増加しており、担当者の話によると 2002 年 11 月の運用開始から一年後の 2003 年 11 月には 600 を超え、2004 年 8 月には 1000 を超えているとのことである。

このことから APNIC CA は利用者が順調に増加していることも容易に想像でき、アドレス資源管理の認証用の認証局として成功している事例と見ることができるであろう。そこで第19回APNICミーティングで運用状況と今後の活動方向についてヒアリングを行った。

このヒアリングの為のミーティングは APNIC CA の構築と運用を行っているプロジェクト担当者と個別に行った。このミーティングでの情報交換は非公式に行っているため、必ずしも APNIC の今後の活動を示すものではないが現状と今後の活動方向性の情報を得ることができた。ミーティングの内容を以下に示す。

- APNIC CA の運用状況
  APNIC CA と JPNIC CA の連携可能性があるか。またその場合はどのような形になるか。
  連携を踏まえた crossCertificate の可能性
- CPS のドラフト状況
  APNIC CA が発行した証明書を認証に利用するアプリケーション S-BGP と soBGP における証明書の応用。S-BGP に関するミーティングについての情報。
  IP アドレスを含めた証明書について。
  ルーティングセキュリティへの影響。

このミーティングの結果、以下のような情報交換を行うことができた。

- APNIC CA の運用状況

申請の頻度	一日に 2,3 通
運用場所	オーストラリアのブリスベン
運用に関わる人数	登録（RA）は IP アドレス管理業務を行うホストマスター（10 名）が兼務。認証局自体はプログラマを含め 3 名。
運用体制	システムの運用は 24 時間 365 日。承認と発行業務は通常の業務時間と同じ。登録は午前 7 時から午後 7 時まで。認証局（発行）は午前 9 時から午後 5 時まで。

- 認証局の連携可能性について
  相互認証は運用が簡単ではないので調査が必要と考える。JPNIC 側で調査が進んでいるようであれば情報交換したい。

- CPS のドラフト状況
  特に進展はなく、ドラフトしている状況である。正式なリリースはしていない。

- S-BGP、soBGP に関して
  APNIC にとって潜在的な次のサービスとなるかもしれない。
  RFC3779 に準拠した証明書の管理がポイントになる。階層構造でなければならないので、NRO がルート証明書に署名し、APNIC が NIR 用の証明書に署名するなどというように考えている。サンプル証明書を数ヶ月以内に作成することを考えている。
  第 18 回 APNIC ミーティングで S-BGP の提案者と RIR の認証局関係者を交えたミーティングが予定されていたが、彼の参加ができなくなったため、第 19 回 APNIC ミーティングに延期された。

- その他の特記事項

- APNIC CA 証明書の再発行
  APNIC CA において HSM（Hardware Security Module）の導入が行われた。また認証局証明書の再発行が行われ有効期限が 2014 年 6 月 3 日になった。以前の証明書の有効期限は 3 年間であったが、今回 10 年間の証明書に切り替えられたことになる。

次に第 19 回 APNIC ミーティングの期間中に行われた RFC3779 について述べる。

4.1.1. RFC3779 BoF

RFC3779 は IP アドレスと AS 番号を X.509 形式の電子証明書に含める為の書式を提案した RFC である。またこの RFC ではこの証明書がインターネットレジストリにおける「アドレスブロック利用／管理権限の証明」を行うとされている。（RFC3779 の内容は章末を参照）

APNIC の認証局プロジェクト担当者の呼びかけでこの RFC3779 に関する BoF（Birds of Feather：興味を持つ人が集まる非公式の会議）が開かれた。この BoF のアジェンダを下に示す。

概要：
S-BGP で利用可能な RFC3779 形式の証明書のインターネットレジストリでの運用に関する BoF
日時：
2005 年 2 月 24 日 18:00 から
アジェンダ：
Meeting objective and agenda bashing
Participant introductions
RFC3779 summary
Open discussion
Meeting conclusion
Action plans (if any)

この BoF には IETF セキュリティエリアのエリアディレクターや RIPE NCC の技術統括、APNIC の技術統括と認証局プロジェクト担当者、S-BGP の提案者、各 RIR の会議に参加し活躍している技術研究者といった著名な人物が参加した。

議論に先立ち、APNIC の認証局プロジェクト担当者よりこの BoF での議論の側面が示された。ポリシー、技術、オペレーションの三つである。

ここでいうポリシーとは IP アドレスの管理ポリシーと認証における信頼のポリシーである。RFC3779 の形式の証明書はアドレス資源の割り振り／割り当てに従って発行されるものであり、インターネットレジストリにおける実際の割り振り／割り当てと連動することが必要となる。

技術については、PKI と RFC3779 の形式の証明書の用途に関する議論が行われた。電子証明書は割り振り行為と対応する形で発行されツリー構造が形成される。また明文化はされていないもののこの形式の証明書は S-BGP で利用されることが想定されている。

オペレーションはインターネットレジストリと認証局における運用である。RIR では認証局を立ち上げるプロジェクトが次々に実施されており、既に APNIC、ARIN、RIPE NCC が認証局の運用を行っている。また RIR におけるアドレス資源の階層的な管理が始まる前のアドレスに対する証明書を扱うため、IANA の認証局が必要かどうかを検討する必要がある。

BoF では以下のような議論が行われた。

論点：

- AS Holder とネットワーク管理者の違い
  そのため RFC3779 では S-BGP に言及していない。
- レジストリに対する信用とルーティングシステムの信用の違い
  対応を取る方法（subjectAltName を使うなど）は考えられるが、
  運用上の課題がある。
- 証明書の有効期限
  保障の上では短いほうが望ましいが、ルーティングの混乱を避けるには
  ある程度の長さが必要になる。
- アドレスブロックの切り替え(ERX 等)への対応
  歴史的な経緯で RIR を通さず IANA から直接割り振られているアドレスの証明書など、アドレスの移管や割り振りの変更があった際の影響に対応する必要がある。この点はまだ議論が続いており、メールで継続してやりとりされている。
- IANA による認証局か他の認証局か
  歴史的な経緯のアドレスに対する証明書を扱うには、IANA で認証局を構築することが必要になる。NRO（Number Resource Organization）によって認証局が運用されるという案も挙がっている。
- アドレスの追加割り振りと鍵ペアを再生成
  アドレスの追加割り振りは新たに証明書が発生することを意味する。
  しかし議論の結果、追加割り振りは同じ鍵ペアの保有者に対して行われる

- 認証局の実装方法
  商用認証局を利用するには証明書要求の際に入れ込んでおく必要がある。またオープンソースの認証局のどちらでも、レジストリが拡張フィールドを管理する必要がある。
- 全ての証明書に CA フラグが必要
  RFC3779 の証明書は割り振り先に対する証明書を、上位が発行した証明書の鍵ペアを使って発行する。つまりすべての証明書が認証局の役割を持つ。
  https や S/MIME の用途で発行した証明書では一般的に行われないことであるが、証明書に CA フラグ（認証局証明書であることを示すフラグ）を含める事になる。また拡張フィールドの keyUsage に keyCertSign といった証明書発行を意味するフラグが立てられることが予想される。

今後どのように議論が進められるかは未定だが、IETF RPSEC WG のメーリングリストの動向を見ると、ルーティングプロトコルの安全性の議論が更に進み証明書の適用方法にまでつながっていく必要があると考えられる。

なお、電子証明書については次回 IETF でも議論が行われる様子であった。

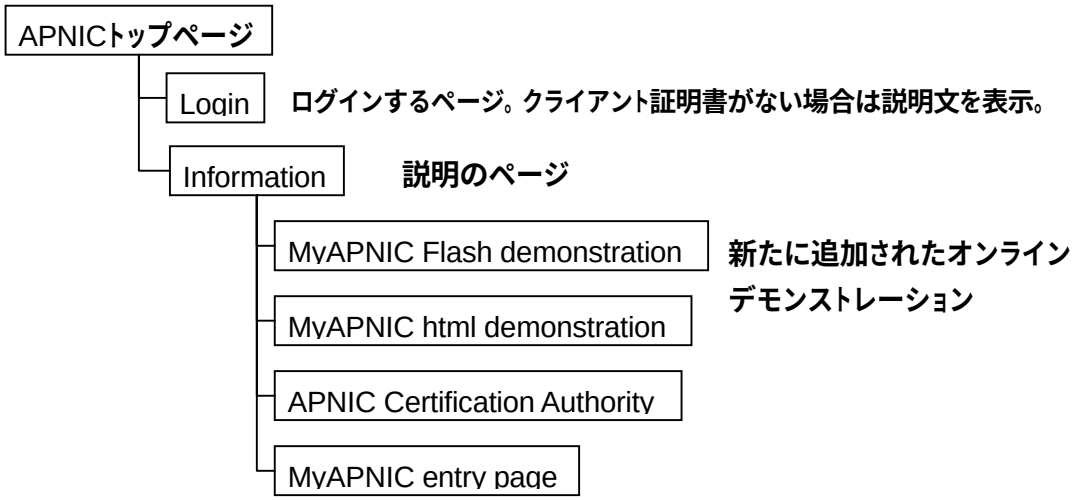
今後は IETF などを通じて議論を進めていくということになった。

4.1.2. MyAPNIC と認証局に関するガイドの充実

APNIC CA が発行する認証用の証明書は MyAPNIC と呼ばれる資源管理の為のシステムで利用されている。MyAPNIC は Web を利用したシステムでアドレス資源の申請等を行うユーザは Web ブラウザを使ってアクセスする。通信には https（SSL/TLS を用いた HTTP）を用い、通信路の暗号化、やり取りされるメッセージの保護、通信相手の認証が行われている。

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」以降、MyAPNIC 自体の主な機能の向上は見られないが、ユーザに対する説明資料は拡充していた。

MyAPNIC に関する Web ページの構造を示す。



今回追加されたデモは認証を含めて MyAPNIC の利用法を三つの部分に分けて説明している。はじめに「セキュリティ」が説明される。https を使った通信路の保護、https を使った相互認証、証明書を使った認証が挙げられている。

次に資源管理の方法、アカウント管理（連絡先、費用）の方法が説明され、最後に選挙のための投票機能の使い方と APNIC が実施しているトレーニング状況の表示方法について説明される。

このように MyAPNIC はクライアント証明書を用いた認証を実施すると共に、その認証結果をアクセスコントロールのために利用している。

[http://www.apnic.net/member/corp-contacts/index.html] 権限の説明

MyAPNIC のセキュリティの機能には、X.509 形式の証明書を使ったクライアント認証だけではなく、ユーザの権限管理がある。MyAPNIC での権限の分類を以下にあげる。

MyAPNIC における権限の分類

* Policy development
* Internet resource management
* Technical issues
* Administration/billing
* Training

なお権限分離の機能は 2003 年度の調査時と変わっていないが、Training の役割に対してトレーニングコースの受講結果を表示する機能が実装されている。

4.1.3. 登録情報のセキュリティの動向

APNIC ミーティングにおける登録情報のセキュリティに関する動向について述べる。

APNIC ミーティングにおける登録情報に関する議論の場は、Database WG である。第 18 回 APNIC ミーティングの Database WG のアジェンダを以下に示す。

第 18 回 APNIC ミーティング Database WG のアジェンダ

Review of action items
Proposal on IPv6 IRR service at APNIC
Privacy of customer assignment records - project update
Protecting historical records in the APNIC Whois Database - project update
Modification of Whois domain object authorisation
RIPE database software update

このうち登録情報のセキュリティに関連する話題は、「Protecting historical records in the APNIC Whois Database - project update」が挙げられる。

「Protecting historical records in the APNIC Whois Database - project update」は RIR によるアドレス資源管理が始まる前の IANA から割り振られたという歴史的経緯を持つアドレスの保護に関するプロジェクト中間報告である。歴史的経緯を持つアドレスの中でハイジャックと呼ばれるのっとり行為が行われており、問題になっている。ハイジャックされた登録情報の一覧を作っている Web サイトが存在している。
http://www.completewhois.com/hijacked/hijacked_qa.htm

なおこの Web ページは 2002 年度の「IP アドレス認証局のあり方に関する調査研究」でも取り上げた。登録情報ののっとり行為は RIR や NIR で階層的に管理しているアドレスよりも歴史的経緯を持つアドレスの方が行われやすいと言われており、APNIC ミーティングでのプレゼンテーションではその傾向を受けたものであると考えられる。ハイジャック自体は歴史的経緯を持つアドレスの登録情報に限られた問題ではない。

このプレゼンテーションでは、歴史的経緯を持つアドレスに対して APNIC のメンテナを用いた管理（一旦登録情報を APNIC の管理下におく）とし、継続して管理を行う場合には一つのメンテナを設けるごとに 100 米ドルを維持料として APNIC に支払うとしている。

第 19 回 APNIC ミーティングでは、登録情報とスパム、認証局に関する議論が行われていた。第 19 回 APNIC ミーティングの概要とスケジュールを次頁に示す。

概要：
2 月 21 日（月）Tutorial
Dynamics of policy process
Spam prevention

2 月 22 日（火）Tutorial
Keynote: Security protocol
Certification Authority
ISP security strategy
Internet governance（一部 ISP security strategy と併催）
APOPS
PGP key signing party（APOPS と併催）
APRICOT opening event

2 月 23 日（水）Policy meetings
APRICOT plenary
IPv6 technical SIG
NIR SIG（IPv6 technical SIG と併催）
Routing SIG
APNIC 19 reception
＃RFC3779 BoF は APNIC19 reception の直前の一時間に行われた。

2 月 24 日（木）Policy meetings
Policy SIG
Database SIG
IX SIG（Database SIG と併催）
DNS operations SIG（IX SIG と併催）
CRISP/EPP BOF
APRICOT closing reception

2 月 25 日（金）Member meeting
APNIC Member Meeting

第 19 回 APNIC ミーティングで行われたセッションのうち、登録情報とネットワーク・セキュリティに関連するものに、2 月 21 日と 2 月 22 日のチュートリアルでスパムメールと認証局に関するプレゼンテーションが挙げられる。また 2 月 23 日に行われた

Database SIG では登録情報の記述言語である RPSLng に関連する APNIC での状況報告が行われた。

2005 年 2 月 21 日のチュートリアルセッションでは「Dynamics of the policy development process」、「Introduction to spam prevention」、「Anti spam activities in Japan」の三つが行われた。最初のものは APNIC におけるポリシー策定プロセスに関するチュートリアルである。二番目と三番目はインターネットにおけるスパムメールの一般的な話題であるが、APNIC や JPNIC といったインターネットレジストリは登録情報の中に、ネットワーク管理者同士が連絡を取り合うことに利用されるコンタクト情報を持っていることから、インターネットレジストリの情報提供機能における課題抽出が可能な話題であると考えられる。

「Anti spam activities in Japan」では最近になって日本で見られるようになった、機械的なフィルタにかかりにくいスパムメールや携帯電話を使ったスパムメール、日本における法制度の動向などについてプレゼンテーションされた。

スパムメールをフィルタする為に、メールで使われているフレーズに基づいた技術が多くのプログラムで使われているが、あたかも人が発信したかのようなスパムメールはこのフィルタにかからない。このような巧妙なスパムメールは増加しつつある。

スパムメールの配送をフィルタする技術には、メールの発信元であるメールサーバの DNS への登録状況を確認する方法や、メールメッセージに含められた署名データを検証する方法がある。このようなネットワークの登録情報を使う場合、その登録情報の正当性が重要性を持つ。現在、アドレス資源の割り振り情報を使ったメッセージ発信元の認証技術は普及していないが、IETF における DNS のゾーン情報を使った技術標準化が進むに伴って今後インターネットレジストリにおける登録情報の管理上の役割が発生する可能性が考えられる。

2005 年 2 月 24 日の Database SIG では RPSLng に関する情報共有のプレゼンテーションが APNIC の技術部門担当者によって行われた。このプレゼンテーションでは IETF における RPSLng に関する標準化と開発の活動 * 、APNIC における IPv6 をサポートした IRR（Internet Routing Registry）IETF CRISP WG における標準化活動 * といった RPSLng に関連した APNIC における活動についての情報共有が図られた。

RPSLng に関する標準化と開発の活動

- IETF における Internet-Draft の新バージョン
  draft-blunk-rpslng-08.txt
- IRR における IPv6 とマルチキャストルーティングのサポート
- Merit におけるプログラム開発
  2004 年 10 月　初バージョン
  2004 年 12 月　RIPE NCC の whois での組み込み
  2005 年第二四半期　IPv6 のルーティングレジストリでの組み込み

CRISP WG における標準化活動

- 2004 年 1 月　利用上の仕様の PS（Proposed Standard）化
- 2004 年 1 月　ドメイン名のスキーマ（dreg）の PS 化
- 2004 年 6 月　IP アドレスのスキーマ（areg）の PS 化

2005 年 2 月のドキュメント化の状況

RFC 発行済み

- RFC3707　CRISP requirements

CRISP（Cross Registry Information Service Protocol）は whois に変わる登録情報の効率のよい閲覧を実現するプロトコルである。このプロトコルには「レジストリの管理化にある情報の適切な特定」「情報伝送と問い合わせ応答のプロトコルの実現」といった機能が必要とされている。

この RFC ではディレクトリサービスの実現や転送プロトコルについて定義している。

- RFC3981　IRIS core protocol
  IRIS（The Internet Registry Information Service）はクライアント・サーバモデルで登録情報の問い合わせ・応答を実現する為のプロトコルである。
  XML（Extensible Markup Language）を用いており、特定の種類の登録情報に依存しない、汎用的な問い合わせ・応答の定義を行っている。
- RFC3982　DREG schema
  IRIS のドメイン名のスキーマを定義する RFC である。
- RFC3983　IRIS over BEEP
  IRIS のやり取りの転送の為に BEEP（Blocks Extensible Exchange Protocol）と呼ばれるトランスポート上のプロトコルで利用するとし、BEEP を定義した RFC である。

Internet-Draft の状況

- Draft-ietf-crisp-iris-areg-09.txt
  アドレス登録情報のスキーマを定義することを目的とした Internet-Draft
- Draft-ietf-crisp-iris-areg-urires-00.txt
  IRIS のアドレスと登録情報のスキーマで使われる URI（Uniformed Resource Identifier）を定義することを目的とした Internet-Draft
- Draft-ietf-crisp-iris-dchk-02.txt
  IRIS のフレームワークを用いてあるドメイン名の存在を確認する簡易なサービスに関する定義を行うことを目的とした Internet-Draft

- Draft-ietf-crisp-iris-lwz-01.txt
  IRIS のための UDP（User Datagram Protocol）を用いたトランスポート（伝送路）の提供の為の定義を行うことを目的とした Internet-Draft

新しい動きについては二つ紹介された。RREG（ルーティング・レジストリのスキーマ)が JPNIC の IRR 企画策定専門家チームによって行われていることと、第 62 回 IETF で RREG に関する議論が行われ、CRISP WG のチャーターの調整が行われることである。

また将来の方向性として CRISP が一方向性の問い合わせ・応答のプロトコルであるのに対し、登録と問い合わせの両方向をサポートするような活動を目指すこと、単一のクライアントで全ての CRISP を使ったレジストリとのやりとりの実現、などが紹介された。詳細は第 20 回 APNIC で示されるとの事であった。

2005 年 2 月 24 日（木）CRISP/EPP BoF が開催された。この BoF は CRISP と EPP（Extensible Provisioning Protocol）に関して、特に IETF CRISP WG の活動の状況について議論を行う BoF である。

この BoF では RREG の標準化と RIR/NIR における取り組みを進めることの必要性や IETF CRISP WG での RREG の扱い方に関して議論が行われた。

インターネットにおける経路情報の正しさを検証する必要性が一部の専門家に指摘されているが、その状況を受けてか、ISP における IRR のサービスが立ち上がりつつある。しかし経路情報の正しさは IP アドレスの割り振り／割り当てと AS 番号の割り当ての正しさに基づいているため JPNIC のようなインターネットレジストリにおける適切な情報公開が肝要になる。APNIC や JPNIC の IRR 企画策定専門家チームでは whois と同様に、登録情報に基づく IRR サービスの提供が、要求されている機能を実現する方法であると考えられている。情報の正確さと規模拡張性の観点から CRISP の利用が重要であるという見方も一致している。

一方、この BoF の APNIC の技術担当者は CRISP WG で RREG を扱うことに関して慎重な態度であった。ルーティングレジストリはアドレスレジストリとは異なるフラットな構造であり、AS のルーティングレジストリにおける登録情報の信頼は歴史的な経緯からインターネットレジストリの構造とは若干異なっている。（例えば米国 Merit による IRR のサービス RADB は、ARIN の役割とは独立している。）

BoF の中で、ルーティングレジストリの機能を RIR や NIR といったインターネットレジストリで検討されることで解決する問題は多くあるという見方が強い。しかし IETF CRISP WG は、このようなモデルの再検討が必要になる可能性に対応できるような長期的なマイルストーンを設けておらず、現在取り組んでいるドメイン名とアドレスのスキーマのドキュメント化を進め当面の目標を達成したいという意図があると感じられた。

Database SIG における RPSLng に関するプレゼンテーションの中で、IETF CRISP WG のチャーターの調整は、必ずしも RREG を含めた目標の拡大であるとは限らない状

況であると考えられた。技術的な観点ではドメイン名のスキーマやアドレスのスキーマと同様に、ルーティングレジストリのスキーマを定義するに留め、サービスや運用方法の取り決めは CRISP WG の活動外とする方法が考えられる。

4.2. RIPE NCC における認証局のマネジメントと登録情報の安全性に関する動向

RIPE NCC では X.509 形式の電子証明書を用いたクライアント認証を既に実施しており、その電子証明書の発行に使われる認証局の運用も実施されている。2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」で述べたように、RIPE NCC では X.509 形式の電子証明書を資源管理の情報を表記する言語 RPSL で記述したデータオブジェクトに組み込む活動を行っている。この活動は既存のアドレス資源管理の手法に新たな認証の機能と加えるという、やり方である。このように書くと特段変わった方法ではないようにも取れるが、例えば APNIC では既存のアドレス資源管理の認証とは分けて管理し、ARIN では既存の認証で使われている識別子を電子証明書に含め、whois などの既存の登録情報には影響させない手法が取られている。

RIPE NCC における認証局のプロジェクトは” Improved Secure Communication System for RIPE NCC Members” * で文書化されている。この文書では PKI の X.509 形式の証明書を使ってコミュニケーションシステムの安全性向上を図るとしている。ただし、認証局の機能を全て満たすようなシステムの提供は目標ではなく、あくまで安全性向上の範囲での構築とされている。そのため認証局に関連するプロジェクトのゴールは認証局の構築を中心としたものではない。

”Improved Secure Communication System for RIPE NCC Members ”で挙げられているゴール

Access to the services and data

The goal in this area is to make communication faster and easier by introducing stronger and more uniform security mechanisms. This will make it easier for the user to maintain and use their security tokens and will allow the seamless use of some of the advanced interfaces (such as web-based interfaces) with strong security support.

Privilege management

The system will provide unified privilege management support for the users. X.509 PKI certificates used in the system as security tokens have intrinsic revocation and expiry mechanisms that, together with support for their maintenance, make the system less vulnerable.

Minimal deployment and maintenance efforts for the users

Based on an industry standard and being well deployed in commercial and open source software, the communication system will require no additional client-side software.

「**Access to the services and data**」における「より強固で統合化された認証」は X.509 形式の証明書を、現行の資源管理機構における認証方式の選択手法の中で利用していく方針であることがわかる。また「**Privilege management**」での権限管理は、資源管理のために使われている RPSL を使って行われることがわかる。「**Minimal deployment and maintenance efforts for the users**」は、クライアント側に Web ブラウザ等の多くの環境で利用可能なプログラムを用い、それらの改良や開発が必要ない状況を目標にしていることがわかる。

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」で、RIPE NCC が whois データベースに登録された証明書を認証に利用する方式を採用したことを報告した。この方式では、ユーザが LIRPortal 等の Web のシステムにアクセスしたときに、そこで提示されたクライアント証明書の検証で PKI のパス検証行わない。そこで提示された証明書が whois データベースに事前に格納されていれば認証が成功する方式である。これは RPSL の key-cert クラスと呼ばれるデータ形式で whois データベースに証明書を格納して実現している。

なお、JPNIC における認証局の取り組みは、key-cert クラスを用いた手法を除き、RIPE NCC における「既存の登録情報の扱い方を生かした新しい認証技術の導入」という手法に似ている。JPNIC では既存の登録情報の管理形態を引き継ぎつつ新たな PKI を用いた認証の機構を導入している。

本調査研究では、2004 年度 RIPE ミーティングに参加し、実際に認証局のプロジェクトを進めた技術担当者との個別のミーティングを行った。また他の RIR のミーティングで行われた RIPE NCC の近況報告を入手し、調査を行った。

■RIPE NCC CA の動向

2005 年 2 月に行われた第 19 回 APNIC ミーティングで、RIPE NCC の whois データベースソフトウェアの近況についてプレゼンテーションが行われた。なお RIPE NCC における認証局機能は whois データベースソフトウェアの一環として位置づけられている。

このプレゼンテーションで述べられた認証機能に関する報告を以下に示す。

X.509 Support
- KEY-CERT class changed
- Update mechanisms updated
  - E-mail supports S/MIME
  - webupdates/syncupdates support client SSL certificates

Organization Object Type

NONE Authentication Deprecated

X.509 Support は、X.509 形式の証明書を使った認証に関するデータベースと登録情報の変更機構の改良である。key-cert クラスはユーザが証明書を格納するために使われるデータ構造で、今回の変更で認証方式を指定する method のフィールドで key-cert クラスの識別子を指定する書式が若干変更された。また自動登録の機能が実現された。RIPE NCC の認証局にクライアント証明書を発行してもらった場合に、自動的に key-cert クラスのオブジェクトが登録されるようになった。以前は証明書の発行後にユーザが登録操作を行う必要があり、RIPE NCC の担当者の間では証明書の利用を複雑にする要因と位置づけられていた。

Update mechanism の E-mail supports S/MIME とは、暗号化された電子メールを使った申請の受付が可能になったことである。RIPE NCC の whois データベースは key-cert クラスを使って証明書の格納とアドレス資源の管理権限の管理を一元化しており、LIR（日本の ISP にあたる）は Web を利用するシステムである LIRPortal を使っても、S/MIME を使った電子メールのどちらでも、同じアドレス資源に関する申請／情報変更業務を行うことができる。Webupdates は Web を使ったデータベース操作のインターフェースで、LIR が RPSL で表現されたデータ・オブジェクトを個別に生成／変更する方法で登録情報を変更することができる。このシステムでもクライアント証明書を用いたクライアント認証を利用することになった。

NONE Authentication Deprecated は、認証方式に”none”（なし）が指定されている登録情報の削除に関する活動内容の説明である。認証方式が”none”に指定されており、また管理情報のメンテナが存在しない場合には、その登録情報を変更することができなくなり、新しいメンテナを生成するための連絡先が通知される。認証方式が”none”でメンテナが存在する場合は新たにパスワードが設定される。

次に第 49 回 RIPE ミーティングで行った調査について述べる。

■認証局に関する情報交換

2004 年 9 月 20 日（月）～2004 年 9 月 24 日（金）に行われた第 49 回 RIPE ミーティングで、RIPE NCC の認証技術と whois データベースの技術を担当しているソフトウェア・マネージャーと RIPE NCC の認証局関連の技術担当者を交えて、認証局と登録情報における認証に関する個別のミーティングを行った。

個別ミーティングのアジェンダ（議題）を以下に示す。

認証局に関する個別ミーティングの議題

- JPNIC CA Updates
  CP/CPS ドラフト、プロジェクトに関する意見交換
- CA management model
  認証局システムに関する意見交換
- One big picture
  RIR と NIR における登録情報のセキュリティレベル／アドレス情報に基づく証明基盤
- A Protection mechanism in RPSL
  big picture 実現の為の手法

個別ミーティングでは、はじめに JPNIC の IP アドレス認証局に関する意見交換を行った。

前回情報交換を行った第 46 回 RIPE ミーティングでの個別ミーティング以降、JPNIC では CPS のドラフトと CA プロジェクトの進行等が変わった部分となる。先方が興味を持った点は、CPS の作成にかかる期間である。IP アドレス認証局の CPS のドラフトには約 6 ヶ月かかっている。

CA management model は、2003 年度に行われた IP アドレス認証局のマネジメントに関する調査研究の一環として定義された認証業務のモデルに関する情報交換である。これは External RA（外部 RA）と呼ばれるもので、LIR に所属するユーザ（業務責任者等）がその管理下のユーザアカウント（申請業務を行う業務担当者等）の作成／管理を行うことができる。

このモデルと、このモデルに基づいてドラフトされた CPS に関して情報提供を行い、意見交換を行った。モデルに関しては興味を持って頂いた様子で、特に問題点の指摘はなかった。APNIC や ARIN の認証局で External RA のモデルを採用している例をみないため、同じレジストリの認証機構として受け入れにくいという意見が上がる可能性を考えていたが、特に問題はないことが確認できた。

One big picture は、インターネットレジストリにおける PKI の活用に関する意見交換である。これは JPNIC における IP アドレス認証局の調査研究を通じて練ってきた構想を紹介し、意見を頂くという主旨で行った。これに対し、彼らはこの構想の整理の仕方に興味を持ち、特に登録情報の正当性を確認する（電子署名等の）方式がないという問題意識の共有を行うことができた。その際に、全体の構想を NRO（Number Resource Organization）に持ちかけてはどうか、という意見を頂いた。本調査研究ではそこまで活動を行うことはできなかったが、ICANN をはじめアドレス資源管理の安全性向上の必要性がいくつかの団体から指摘されていることから、インターネットレジストリ全体

の取り組みとして捉えるための活動があると有効であると考えられる。

本構想について意見交換を行った内容を以下に示す。

ここではインターネットレジストリのアドレス資源管理構造に、PKI のツリー構造を当てはめ、割り振り／割り当てに対してアドレス資源の利用権利の証明と、インターネットレジストリが発行した証明書を使ってユーザ間またはホスト間の認証を行うという概念を説明している。

この概念の実現には、登録情報のミラーの機構、証明と検証の機構、登録手続きの安全かの三つが必要であるとしている。

Components

- Good mechanism for mirroring and referring
  - CRISP / RPSL
  - whois?
- Good mechanism for certification and verification
  - We don't have yet.
    - https and server certificate is not suitable for us I think.
- Making registration process secure
  - strong authentication (certificate and PGP)

Japan Network Information Center　17

登録情報のミラーの機構にはRPSLを使ったアドレス資源管理情報の統一的な表現や、CRISP を使った透過的な参照を可能にする検索が必要になる。証明と検証の機構には、まだ適切なものがないがインターネットレジストリが発行している証明書を使い、登録情報に電子署名を施す手法が候補として挙げられる。最後の登録手続きの安全化は、LIR によって実施される登録プロセスに強い認証機構を導入することである。ここでは証明書と PGP を挙げている。

Assuming users

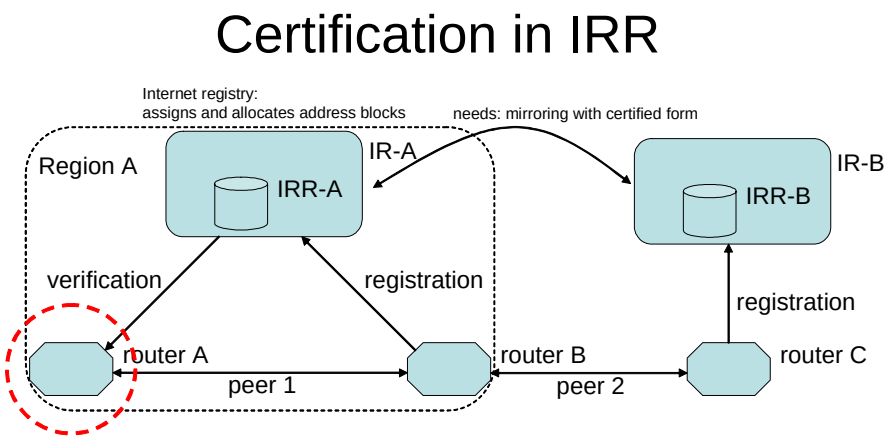
- Users
  - LIRs in World Wide
    - for secure routing in global level
      - e.g. S-BGP, soBGP
  - Service Providers
    - for verifying and controlling access
      - e.g. commercial CA, CDN, small but many IPv6 nodes
  - Incident Response Team

⇒ They all use registered information (objects in RPSL).

Japan Network Information Center 18

ここでは本構想で構築される認証基盤のユーザを想定している。まず全世界の LIR が挙げられる。これはグローバル・インターネットにおける安全なルーティングの実現には、インターネットレジストリの登録情報である割り振り／割り当て情報が必要になるためである。ルーティング情報をやり取りするプロトコルの安全性向上に関しては、S-BGP や soBGP を利用するという例を挙げている。

更に、登録情報に関する証明と検証の例を、IRR を使って説明を行った。なお、この機構はまだ標準化等は一切されておらず、本調査研究の一環で構想として練られただけの状態である。（次頁図）



ここでは RIR や NIR で運用されている IRR が、登録情報のミラーリングを行っている状況を前提としている。IRR-A に互いの登録情報を持つ router A と router B は、互いの流す経路情報の正当性を IRR-A を使って確認することができる。しかし IRR-B に登録されている router C が流す経路情報の正しさを検証するには IRR-B から IRR-A にミラーリングされた情報を検証することになる。ミラーリング（情報のコピー）が行われる状況で、その情報に改ざんがないか、登録者が誰であるかといった検証を行うことが必要になる。

次頁の図は、IRR の登録情報における登録者が意図しない変更（unintended）の場合わけを行っている。

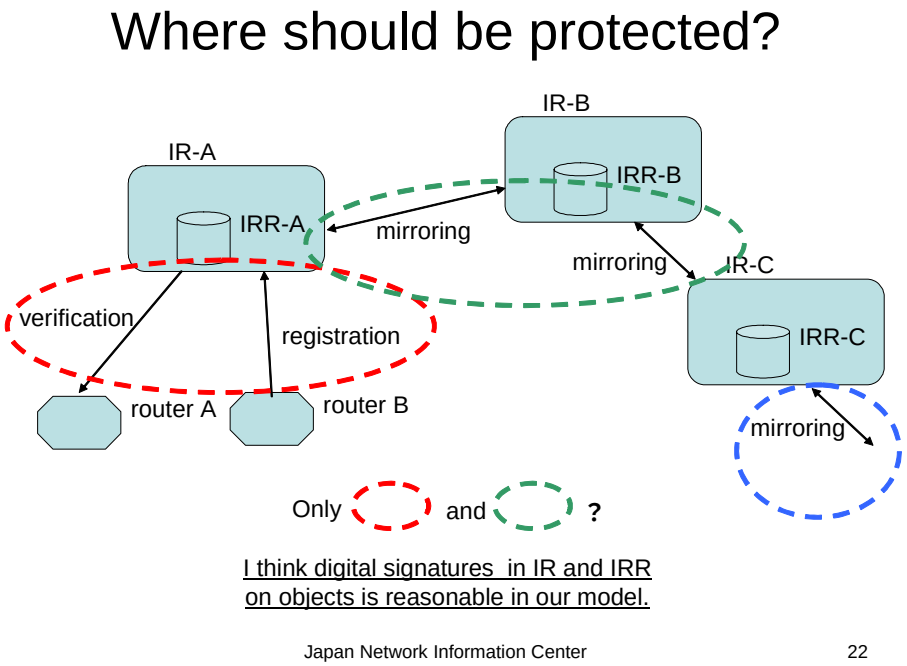
Unintended modifications

- Registered data it self
  - deletes, modifications in DB
    - Disasters
    - Dugs in servers/clients
    - Impersonation for legitimate users
- Unintended modifications on transferring data
  - spoofing (servers, clients)
  - man-in-the-middle attack
  - modifying in mirroring

⇒ We should have a mechanism which can let us know these modifications.

Japan Network Information Center 21

サーバの成りすまし（spoofing)、マン・イン・ザ・ミドル攻撃、ミラーリングされた情報の改ざんがあるような状況では、サーバ認証やクライアント認証ではメッセージの正当性を守ることはできない。従って少なくともメッセージが元々の状態から変更されていることが検出できる仕組みが必要になる（次頁の図)。



この情報共有の後、この同じ構想もしくは同じ問題意識を持つことと、それぞれの問題解決を行う準備を行うことについて呼びかけた。彼らは、このモデルは単一のレジストリが取り組む問題でないと考え、NRO で提案することを進めてくれた。

2005 年度の本調査研究ではそこまで活動を行うことができなかったが、今後 NRO 等を通じた包括的な取り組みが可能であればより効率的に各 RIR がセキュリティに関するプロジェクトを推進できるのではないかと考えられる。

■RIPE NCC の認証局の証明書発行数

第 49 回 RIPE ミーティングの個別ミーティングの後、RIPE NCC の認証局の運用状況について質問を行った。特にクライアント証明書の発行数をたずねたところ、調査して頂いた上で回答を頂くことができた。2004 年 10 月現在 766 のクライアント証明書が失効されずに有効な状態であるとのことである。

■第 49 回 RIPE ミーティングのアジェンダに見るネットワークセキュリティの動向

RIPE ミーティングには European Operators Forum（略称 EOF）と呼ばれるオペレータの情報交換の場が設けられている。EOF は各 RIPE ミーティングの主に初日に行われ、ネットワーク運用の近況報告や話題提供が行われている。

第 49 回 RIPE ミーティングの EOF のアジェンダを以下に示す。

Monday, 20 September 2004
16:00 - 17:30 The Peering Simulation Game
Tuesday, 21 September 2004
09:00 - 10.30 Core Network SecurityTutorial
11.00 - 12.30 Core Network Security Tutorial (continued), Discussion

「The Peering Simulation Game」は参加者が ISP となり、ISP のピア（ISP 同士の一対一の接続）や IX の形成を通じてネットワークの形成を体験するゲームである。小規模な ISP が大規模な（提供地域の多い）ISP とピアを形成すると莫大な費用がかかるため、早期に協力して IX を形成するほうが全体の提供範囲を広げやすいといった状況を体験することができる。

「Core Network Security Tutorial」はサービスプロバイダのコア・ネットワークにおけるセキュリティに関するチュートリアルである。コア・ネットワークはユーザのコピューターが接続されるネットワークからの不正な通信を想定した ACL（Access Control List）の設定が必要になる。また意図どおりのルーティングを維持するために、経路情報を交換するプロトコルの安全性をいかに確保するかが課題となる。

ミーティング全体では、Anti-SPAM をはじめ Database、RIPE NCC Services でスパムに関する議論が活発に行われた。RIPE NCC におけるスパムの議論は、主に登録情報を利用したスパムメールを阻止する観点で行われている。特に第 49 回の Database のセッションでは、whois の検索結果において連絡先のメールアドレスを表示することがスパム防止の観点でよくない、という問題意識を確認した上で、いかに連絡先情報の提供を行うべきか、という議論が行われた。

連絡先情報は、whois を使ってだれもが調べることができ、またネットワークの不具合に対応する目的の連絡先であることから、スパムが発生したときの連絡先に使われやすい。しかしアドレス資源の管理とスパム対応とは必ずしも同じ連絡先ではない。ネットワーク管理の観点ではネットワーク運用に関わる重要なメールがスパム対応のメールにうまってしまっては意味がない。

Anti-SPAM WG のセッションでは、下記の提案が既に受け入れられていることが確認された。

A. IRT-object に abuse-mail を含めること、PGP 等の認証の必須条件なくすこと。
もしくは新しい似た働きを持つオブジェクトを導入すること。
B. whois のデフォルトの動作において abuse のメールアドレスを表示し、
そのアドレスが一つであるならばその他のアドレスを表示しないこと

更にネットワーク情報（inetnum, inet6num, route の各オブジェクト）の検索結果に含まれていたメールアドレスをデフォルトでは表示しないこと、person オブジェクトや role オブジェクトには abuse-email というフィールドを設け、表示される連絡先がスパム対応の目的であることを明示するという提案がなされた。

■第 49 回 RIPE ミーティング全体を通じて

本節では第 49 回 RIPE ミーティングのこれまでに述べた以外の話題を含め全体について述べる。

○概要

第 49 回 RIPE ミーティングは 2004 年 9 月 20 日(月)～9 月 24 日(金)、イギリスのマンチェスターで行われた。RIPE ミーティングは、ヨーロッパ地域のレジストリである RIPE NCC が定期的に開催しているミーティングで、アドレスポリシーを始め、レジストリシステムや IPv6、Routing 等について議論が行われる。

Working Group Agenda
http://www.ripe.net/ripe/meetings/ripe-49/agendas/index.html

■RIPE NCC スタッフとの個別ミーティング

2004 年 9 月 21 日(火) 9:00 から 1 時間 40 分にわたり、RIPE NCC の認証局関連業務の担当者と個別のミーティングを行った。

このミーティングは、RIR の認証局に関する情報交換とネットワーク・セキュリティの為のレジストリの役割について議論することを目的としたものである。認証局に関する情報交換は、第 46 回 RIPE ミーティングの際のミーティングで行ったことがあるため、今回はそれ以降の活動の情報交換が主な話題となった。今回はそれに加えて、インターネットレジストリによる証明基盤の構築に関して話し合った。

このミーティングを通じて、類似する問題に取り組んでいることや、問題解決の際に共通に重点をおいた点などを相互に確認することができた。また JPNIC にて構想中のアドレス資源に基づく証明基盤について、NRO で提案してはどうかといったアドバイスを頂くことができた。

第 49 回 RIPE ミーティングでは、各 WG セッションにおけるレジストリのセキュリティに関連する話題についての情報収集を行った。

■Opening Plenary, RIPE NCC Services

開催の挨拶の後、RIPE ミーティングのコスト、RIPE NCC からの Update、WG からの話題の紹介が行われた。

RIPE NCC からの Update の中では、IANA への大きな IPv6 アドレスブロックの割り振り（承認）、AfriNIC への業務移転、レジストリシステムの LIRPortal の Organization オブジェクトの追加などが報告された。また新しいプロジェクトである AS 番号に関する Web インターフェースである myASN を始め、X.509 証明書の LIRPortal での扱いの変更、IRRToolsSet の ISC への移管、k ルートサーバの IPv6 対応などがプレゼンテーションされた。

X.509 証明書の LIRPortal での扱いの変更については、第 46 回 RIPE ミーティングで提案された方式が LIRPortal で実施されたとの報告があった。この方式は RIPE NCC の CA 以外の CA から発行された証明書であっても Database に登録することで認証に利用されるというものである。

■WG セッション

今回の RIPE ミーティングでは、WG セッションは概ね 2 つが平行して行われた。以下に各 WG セッションの概要とポイントを簡潔に報告する。

○Routing WG

Routing WG は 9/21 16:00 と 9/22 11:00 の二回セッションが開かれた。最初のセッションは EOF で行われたチュートリアルに関する議論と BGP を使ったマルチホームの陥りやすいミス、日本の NICT（情報通信研究機構）の研究員の方による経路情報の不安定性をモニタするツールの紹介が行われた。

○EIX WG

EIX はヨーロッパの IX 運営に関する WG である。はじめに、各 IX（AMSIX、DE-CIX、LINX、LoNAP、MIX、Netnod、NIX.CZ、VIX、XchangePoint、NAP ofthe Americas）による近況報告が行われた。

このセッションの最後には KIX(Korean Internet eXchange)による報告が行われていた。参考事例としてのプレゼンテーションのようである。会場からは ISP 事業はあるのか、韓国国内 IX との関係などの質問が挙がっていた。

○IPv6 WG

IPv6 WG は、IPv6 に関わる各種話題を扱う WG である。このセッションでは

Global IPv6 routing table status、v6 traffic volume に関する話題、大きな IPv6 アドレスブロックの割り振りに関する話題、IPv6 アドレスの割り当てに関する話題などがアジェンダに挙がっていた。

セッションの後半では、IETF で提案されている IPv6 を使ったマルチホームの新しい手法の紹介が行われていた。

○Anti-SPAM WG

Anti-SPAM WG は、RIPE NCC のコミュニケーションサービス（RIPE NCC の提供する ML や whois）において SPAM メールを抑止する方針・方法について議論を行う WG である。

今回のセッションでは、"Database WG に対する要望事項(Request to Database WG)"がまとめられた。その内容を要約すると以下のようになる。

- アドレスの割り振りにおける abuse contact の利用可能性の向上に対してなるべく早くアクションを起こすこと。

既に提案されている方法で受け入れられるもの：

A. IRT-object に abuse-mail を含めること、PGP 等の認証の必須条件をなくすこと。もしくは新しい似た働きを持つオブジェクトを導入すること。
B. whois のデフォルトの動作において abuse のメールアドレスを表示し、そのアドレスが一つであるならばその他のアドレスを表示しないこと

この他に、LINX によって出されている BCP の update[ube]の紹介、IETF で提案されている MARID や PRA、SPF といった手法の紹介などが行われた。

[ube] New LINX BCP v2.0
http://www.linx.net/noncore/bcp/ube-bcp-v2_0.html

○Database WG

Database WG は RIPE NCC のレジストリシステムと whois や RPSL に関する議論を行う WG である。このセッションは以下のアジェンダに沿って進められた。

1. DB Operational Update
2. ERX Report [196/8, 198/8]
3. IRRToolSet software maintenance

4. Routing Registry Courses
5. CRISP Update
6. IRT / Abuse-c roundup

セキュリティ事業に特に関連のあるセッションであるため、それぞれの話題について報告する。

1. DB Operational Update

   RIPE NCC における Database の運用報告である。統計上の大きな動きとして、inet6num(IPv6 アドレスブロックの割り振り情報)が 7400 あり、年間で 100%以上の伸び率(倍増以上)であること、そのうち 85%が割り当て済みであることなどが紹介された。また統計資料が公開された。

   その他に、whois サーバの性能向上の為、問い合わせ／参照のみのサーバを増加させてロードバランスを行い、update 等の操作を行うためのサーバをバックエンドの扱いとすることなどが紹介された。

   RIPE NCC のデータベースで使われているメンテナーオブジェクトのセキュリティモデルが変更されるとの報告があった。現在はだれでもこのオブジェクトを作成することができる。ハイジャックを防ぐため、セキュリティモデルを変更し、認証方式の mail-from や none を削除すること、mnt-lower フィールドをデフォルトでは mnt-by にするとのことであった。

   その他に、"AUTO-" を使った参照がすべて行われるようになったこと、認証方式を指定する auth のオブジェクトからそれを含む検索（逆の検索）ができるようになったこと、PGP の fingerprint を格納する fingerpr 欄が検索できるようになったことといった変更があった。

   各プロジェクトの進行についての報告も行われた。

   ・RPSLng

   今までは対応していなかった RPSLng に対応したこと、IETF の Internet-Draft が RFC Editor の編集待ちになったこと（すなわち IESG の承認は既にあり、RFC になることが決まっている）などが報告された。

   ・rERX 及び Afritrans

   ERX および Afiritrans（AfriNIC へのアドレスブロックの移転）を進めるプロジェクトの説明。

・KEY-CERT/MNTNER LIR Portal Integration

第 46 回 RIPE ミーティングで提案された、X.509 証明書のデータベースへの登録手続きの改善に関する報告。これまでは証明書の発行とデータベースへの登録が別の手順で利便性が低かった。（登録数が少ない(担当者によると 20 程度)のはことため、という見解であった）新たに導入された方法では、RIPE NCC の認証局を使って証明書を発行すると、自動的に key-cert オブジェクトが生成される。

2. ERX Report

〜 Early Registration TransferStage 3 -“ Class C ” space 〜

ERX の進行状況の報告である。AS 番号の移管は 2002 年 8 月に始まり、IPv4 アドレスの移管は 2002 年 12 月に始まっている。2004 年 4 月までにいわゆるクラス B は、48 (/8) が移管されており、いわゆるクラス C は 196/8 と 198/8 が 2004 年 7 月に開始、合計で 1964 が移管されている。

いわゆるクラス C の移管は、192/8, 196/8 & 198/8 であと 3000 以上が残っている。これらの移管を進める "Stage 3" では、メールの送信の必要がない Web のシステムを使い、レスポンスを早くするとのことである。このシステムやプロジェクトについては[erx-ip]および[db-erx]から資料を入手することができる。

[erx-ip] Project Web Page

http://www.ripe.net/db/erx/erx-ip/

[db-erx] Project Outline

http://www.ripe.net/ripe/meetings/archive/ripe-44/presentations/ripe44-db-erx/

3. IRRToolSet software maintenance

whois のプログラムセットである IRRToolSet は、もともと ISI によって開発されたもので（当時 RAToolSet と呼ばれていた）RIPE NCC に移管されたものであった。しかしソフトウェアの質の向上とソースコードの公開の為、ISC に移管しオープンソースプロジェクトとして進めることになった。

この移管は既に進んでおり、ソースコードのリポジトリ、ML、Web などの移動は終わっているとの事である。またこの機会に RPSLng への対応、各種バグフィックス、パッチの適用、gcc 3.x でのコンパイル対応などを済ませたとの報告があった。

4. Routing Registry Courses

IRR の利用法の説明会の実施報告である。2004 年には 16 回行われた。2005 年は、ドイツ、スペイン、ロシア、オランダ、イギリス、フランスで開催される予定である。資料などは[training-rr]から入手することができる。

[training-rr] Material & Info
http://www.ripe.net/training/rr/

5. CRISP Update

IETF で標準化作業が進んでいる CRISP(Cross-Registry Information Service Protocol)に関する状況報告が資料に沿って行われた。概要は以下の通りである。

・IETF CRISP WG の紹介
・whois に代わるもので、構造化されている
・IRIS の紹介
・whois と IRIS の違い
　－mntner, irt オブジェクトの情報がない
　－import:, export: といった経路情報がない
・VeriSign のリファレンス実装を使ったプロトタイプなどの今後の活動。

このプレゼンテーションの発表者は、IETF CRISP WG において IP アドレスを AS 番号の書式の提案を行っている。この資料は CRISP と whois の違いを理解する上でわかりやすい。

6. IRT / Abuse-c roundup

データベースにおける IRT オブジェクト／abuse-c の追加に関する議論が紹介された。いくつかの選択肢が紹介されたため、事後に発表者に意見を聞いてみると、mail-abuse の追加が現実的だという見解であった。

○DNS

DNS WG では、RIPE NCC に関連する DNS の話題（登録情報や AAAA レコード等）についての議論を行っている。WG セッションでは、IETF レポートとして DNSEXT WG および DNSOP WG の報告、MARID、CRISP（ドメイン名）の状況報告が行われた。その他には k ルートサーバに関する報告、SiteFinder に関する報告、BIND に関する報告などが行われていた。

○ENUM

ENUM WG は ENUM に関する各種の話題を扱う WG である。各国の ENUM プロジェクトの状況をまとめたり、ENUM 利用に関する報告を行うフォーラムを開催したりしている。今回のセッションでは集められた質問集に関する議論（ここではインフラストラクチャ ENUM は扱わない）やスウェーデンとイギリスで行われたプレゼンテーションの紹介が行われた。

○RIPE NCC Services

RIPE NCC Services WG は、RIPE NCC の提供するサービスについて包括的に扱う WG である。今回は RIPE NCC の提供する ML における Anti-SPAM の観測や、RIPE NCC の会計に関する方針、トレーニングに関する報告が行われた。

RIPE NCC の会計報告では、2004 年度までの収入構造と評価方針と 2005 年度以降の変更とそれに伴う料金の変更などが説明された。

○Address Policy

Address Policy WG のセッションでは、RIPE NCC および ICANN ASO AC の報告のほかに、ポリシー策定プロセスに関する議論と、IPv6 の初期割り振り、IPv6 の IANA から RIR への割り振りの方針などに関するプレゼンテーションが行われた。また whois への登録の必要性とプライバシーに関する議論が行われた。

4.3. ARIN における認証局マネジメントの動向

ARIN（American Registry of Internet Numbers）における認証局のマネジメントの動向に関する情報収集の為、第 14 回 ARIN ミーティングに参加し、また認証局の担当者と個別のミーティング（ヒアリング）を行った。

■ARIN CA の動向

ARIN CA の目的はアドレス資源に関する申請者の、ARIN による認証を実現することとしている。ユーザ同士の認証を想定しておらず、また ARIN が用意した Web サーバ等の申請者による認証（サーバ認証）を想定していない。公開されている CPS によると https を使ったクライアント認証も想定していない模様である。
第 14 回 ARIN ミーティングは、この認証局を用いた申請業務の方法に関するチュートリアルが行われた。

はじめに ARIN の認証局に関して Web 等を通じて調査した認証業務の内容を述べる。

○ARIN における証明書

POC *1 の認証を行うための証明書である。POC とは Point of Contact の略で、RSA (Registration Services Agreement) に合意した組織が予め登録している Admin(管理責任者)もしくは Tech(技術担当者)の POC であるユーザが利用することができる。

POC Template:
http://www.arin.net/library/templates/poc.txt

ARIN が登録している POC アカウントには、複数のユーザが利用可能である role アカウントと個々のユーザに対する個別アカウントの二種類がある。証明書の発行対象となるのは、個別アカウントとして登録された Admin POC といずれの種類の Tech POC である。

○証明書発行対象の認証

証明書の発行要求を出すユーザに対して、三種類の情報の提示を求め、有効性が確認できた場合に証明書の発行を行っている。三種類の情報とは政府によって発行された個人証明と組織の証明、組織と個人の関係を証明する情報である。

○証明書の用途

証明書は、申請書であるメールに対する電子署名に用いることができる。ARIN では、現在これ以外の用途を想定していない。申請書における電子署名によって、

転送中のメールに対する改変や本物であること(genuine)を確認できるものとしている。

○申請方法

Web ページ http://ca.arin.net/request/ にアクセスし Web ブラウザの証明書申請機能を用いて申請を行う。Web ブラウザを利用しない場合には Web ページから入手できる CERT-REQUEST 書式を使って申請を行う。その場合には OpenSSL 等を利用して、ユーザ自身が CSR (Certificate Signing Request) を生成する。

申請に利用できる Web ブラウザについては、テストされた Web ブラウザという形で情報提供がされている。テストされたブラウザは Internet Explorer と Mozilla である。Opera も利用可能だが、証明書を扱う機能はまだ不十分であり推奨されていない。w3m の利用も可能であるという記述がされている。

○証明書の入手

証明書の発行が行われると、Web 経由か電子メールで入手することができるようになる。

○証明書の共有

role アカウント間で証明書を共用してもよいが、role アカウントに含まれる個別アカウントに対する証明書発行も行う。それぞれリクエストに対する署名が複数の人によってできてしまうというリスクと、最初の証明書保持者が残りの証明書リクエストフォームに署名する必要があるという欠点が説明されている。

○証明書の利用に先立つ ARIN CA 証明書の登録

証明書の配布のあと、MUA(Mail User Agent - メールソフト)への組み込みに先立って、ARIN CA 証明書の組み込みをする必要がある。

FAQ では、Internet Explorer と Netscape など、証明書リポジトリを共有していて、Web ブラウザへの証明書の CA 証明書の組み込みによって、メールソフトでのユーザの証明書の利用が可能になるものについての説明がある。しかし証明書とメールソフトの利用方法などの個別の説明は、多種のメールソフトが存在するという理由で、行われていない。

○申請書類を生成するスクリプトの利用

多くのユーザが申請書類の生成にスクリプトを使っているようで、スクリプトを使って電子署名を利用する方法についての説明が提供されようとしている。ただし現在は例示のタイトルがあるものの、文書自体はまだ提供されていない。

○MAIL-FROM の共用

FAQ によると、一度証明書の利用に移行したユーザは MAIL-FROM による申請書の送信はできなくなる。

○証明書について

有効期限は 2 年間。ARIN では有効期限が近くなると更新をメールで知らせるとしている。

○証明書の更新

有効な証明書を使って署名された更新の申請が行われた場合、再度書類を用いた本人確認を行う必要はない。なお証明書の有効期限が切れ、かつ証明書の更新が行われていない場合にも MAIL-FROM を利用できるようにはならない。

○証明書の紛失

証明書を紛失した場合には、ヘルプデスクに連絡することになっている。ヘルプデスクはメールに加え電話による問い合わせにも対応している。

○認証局の鍵更新

CA 証明書の EE への配布によって、証明書の秘密鍵の危殆化の影響を最小化するため、ARIN CA は 6 ヶ月おきに鍵生成を行う。CA 証明書は 3 年間の有効期限を持っているため、最大で 6 つの CA 証明書が存在することになる。

EE 証明書は 6 ヶ月おきに異なる CA 証明書から発行されることになるが、CA 証明書の危殆化の影響（再発行対象の証明書数）は最大で 6 分の 1 になる。

参考文献：
Certificate Cryptographic Authentication at ARIN - FAQ
http://www.arin.net/CA/ca_faq.html

■ARIN の認証局担当者のヒアリング

第 14 回 ARIN ミーティングの期間中、認証局構築の担当者と個別のミーティングを行うことができた。

ヒアリングの内容と結果を以下に述べる。

ヒアリング内容は大きく 4 つに分類される。

○ARIN PKI

認証局自体に関する質問である。認証局には、証明書の発行に関わる認証業務とそのためのシステムという二つの側面を持っていると考えられる。またポリシーの公表による責任分解／問題対応の方針を明らかにするという活動も関連する。

CPS の記述内容を元に ARI CA の特徴のある点､運用の内容についてヒアリングを行った。質問内容を以下に示す。

認証業務の運用人員について

RA(hostmaster) 1 名、他に発行担当者と技術者がいる。管理者は他のシステムと共用で、特定の人員ではない。

認証局の証明書をサイクルする手法について

CA の秘密鍵の危殆化の影響を最小化するための方法。CPS 4.7 の記述に詳しい。

CA 証明書の配布

CA の信頼性に依存して証明書の検証を行う Relying Party が ARIN だけである､という設計に従い､CA 証明書を EE 側で検証する必要はない｡Relying Party については CPS への記述されている。

ユーザ自身の登録に関する安全性の提供の意味はなく、ARIN 側からユーザの認証を強化し、ARIN 側にとっての安全性向上のみを目的としている。

認証局システムについて

基本的にオープンソースソフトウェアを用いている。申請などのメールを受け付けるメールと､認証局の連携のためのソフトウェアは ARIN 内部で開発されたプログラムを用いている。

運用方法は、hostmaster である RA が USB ドングル（鍵ペアと X.509 証明書を格納できるハードウェアトークン）を用いて鍵生成を行い、認証局の運用担当者に渡す、認証局の運用担当者はそれに格納された証明書への署名を行う。つまり認証局側ではメンバかどうかの確認などは行わない。このモデルは APNIC CA の運用モデルを参考にしたとのことであった。

○データベース

電子証明書を既存の業務の認証や電子署名に用いる場合、既存の業務システムと

の連携が必要になる。認証局は既存の業務システムのユーザ管理とは独立して運用されるため、二つのシステムを如何に連携するか、がポイントになる。

主に二つのシステムの設計の中で留意した点についてインタビューを行った。

質問内容を以下に示す。

ユーザ数の上限について

ユーザ数の上限に関する想定は行っていない。理論的には上限値はない。

認可機構について。RPSL を利用しているか。

RPSL のような認可機構は持っていない。RPSL には組織の概念がないが、ARIN では組織を基準にした認可構造を持っており、メンバである組織に関係付けられたユーザ(POC)の特定を元に権限が検証される。

◯ユーザの認証

電子証明書の発行対象であるユーザの認証方法は、認証業務の強度に影響する。またユーザ数の見込みは、認証局システムと業務運用の継続性に影響する。ARIN CA の設計の上でユーザについての想定についてインタビューを行った。またチュートリアル（後述）の内容が充実していたため、ユーザ教育についての質問を行った。質問内容を以下に示す。

ユーザの登録について

CPS には 3 種類の書類が必要であるという記述ある。具体的な書類の内容は明らかにせず、メンバ組織の歴史的な信頼性に基づいて適宜選択されるとのことであった。アドレス資源の多くを管理しており、長期間メンバである組織のユーザの登録は、そうではない組織のユーザの登録よりも簡易かつ少ない確認によって行うとしている。

証明書とユーザに関する予測

新規プロジェクトであるため、事前に規模の想定を行った。説明会を通じて興味を持つユーザがどれくらいいるかの検討を行ってきた、との事であった。

ユーザの教育と証明書ユーザの確保について

ユーザの教育と、証明書ユーザの増加に関する既存の計画についての質問である。これに対し、メンバミーティングでの認証局プロジェクトについて説明を行ったり興味を持つユーザに対するダイレクトメールで連絡を行ったりしたとのことであった。

議論を重ね、ユーザにとってできる限りシンプルな利用法になるように留意した

とのことである。

○実験的な活動

インターネット・レジストリにおける PKI の利用は、アドレス資源の登録内容に応じた認証基盤の構築にも繋がる活動と捉えることができる。APNIC, RIPE NCC における、PKI を用いた BGP の安全化の検討と同様に、ARIN において実験的な活動が行われているかについてインタビューを行った。質問内容を以下に示す。

soBGP や S-BGP といった新しいプロトコルに関連するプロジェクトについて

この認証局に関連しては、実験的なプロジェクトの活動はないとのことであった。この認証局は ARIN によるメンバの認証のみを目的としており、他の用途は禁止している。従ってメンバ同士の認証を伴う BGP での利用はできない。またもしそのようなプロジェクトを実施するにしても、この認証局を利用せず別の認証局を必要とするとのことであった。

○インタビュー結果を受けて

ARIN 認証局の大きな特徴は、やはり証明書の用途の限定であろう。ARIN 側のユーザ認証であること、電子メールのメッセージを使った認証であることの二つである。これによって CA 証明書のユーザへの確実な配布の手段を検討する必要がなくなる。一方、ユーザの登録情報に対する信頼性、実態としての ARIN が設置するサーバやメッセージの電子的な認証は、今の段階では達せられていない。情報登録必要な認証はレジストリによる登録者の認証だけでよいのか、やや疑問に残る点はある。

JPNIC の認証局システムの設計と導入に関して参考になった点は、特に運用面である。証明書の用途をシステムの認証に限定する方針にすることで CA 証明書の配布の問題が少なくなる点である。これはメッセージ認証（S/MIME 利用）を利用目的としている為に実現できると考えられる。Web サーバの場合には man in the middle 攻撃を避ける意味で相互認証を想定する必要がある。

■登録情報におけるセキュリティの動向

次に第 14 回 ARIN ミーティングの期間中に行われたチュートリアルについて述べる。このチュートリアルは「暗号技術を用いた認証のチュートリアル」と題して ARIN の認証局担当者自身によって行われた。

チュートリアルの資料は

http://www.arin.net/library/minutes/ARIN_XIV/tut.html

より入手できる。

このチュートリアルは利用者を対象にしており、具体的な利用方法を説明することを

目的としている様子であった。概要を以下に示す。

暗号技術を用いた認証のチュートリアル概要

- X.509 を使った保護機能
- 証明書の要求方法
- 識別処理とプライバシーについて
- 証明書のインストール方法と mail-from の利用停止
- ARIN 宛のメールへの電子署名

このプレゼンテーションによると、ARIN におけるテンプレート（申請書式）におけるユーザの認証は mail-from を用いており、より安全な方法に切り替えること、その方法として X.509 形式の証明書を用いることが始めに説明されている。

ARIN ではユーザによる証明書の入手の為の Web ページを用意しており、ユーザは Web ブラウザを用いて鍵の生成と証明書の申請、組み込みを行うことができる。一度証明書を使った認証に切り替えると mail-from は基本的に利用できなくなる、という説明があった。

4.4. まとめ

本節では、今回調査を行った RIR における認証局のマネジメントのポイントについて述べる。

4.4.1. APNIC CA

APNIC CA はメンバの認証用の証明書を発行することを目的とした認証局である。証明書の申請には申請書と写真付きの身分証明書を必要とする。申請書には予め登録されたメンテナの情報を記述する必要がある。発行される証明書は Web ブラウザで利用することができるクライアント証明書である。MyAPNIC と呼ばれる各種申請業務を行うことができる Web インターフェースが用意されており、この MyAPNIC へのログインに利用することができる。

APNIC CA はオープンソースソフトウェアを用いており、またできるだけシンプルな構成で運用している。クライアント証明書の登録業務は、IP 業務のユーザ登録業務と兼ねており、認証局部門とは独立している。認証局部門は証明書管理と認証局システムの運用に専念できる体制となっている。

2003 年度の調査以降、証明書発行数の順調な増加、CA の増強（HSM 導入、鍵ペアの作り直し）、RFC3779 に関する取り組み、説明資料の充実といった動きが見られた。今後も RFC3779 に関連して S-BGP 等の新たな取り組みを行う模様である。

4.4.2. RIPE NCC

RIPE NCC の認証局は、LIR の認証用の証明書を発行することを目的とした認証局である。証明書の申請には組織 ID とパスワードを必要とし、パスワードを知っている LIR の ID 管理者が証明書申請を行うことができる。証明書は各種申請業務における電子メールの暗号化に使われ、また LIRPortal、WebUpdates といった Web インターフェースを利用する際のクライアント認証にも用いることができる。証明書と既存のユーザ情報（person オブジェクト、role オブジェクト）との組み合わせを RPSL（Routing Policy Specification Language）を用いており、既存の資源管理情報との統一的な扱いを実現している。データベースには RIPE NCC の認証局以外から発行されたクライアント証明書を登録することもでき、その証明書を使った各種申請業務を可能にしている。

RIPE NCC における認証局はオープンソースソフトウェアを用いており、RPSL ベースのデータベースと連携するための開発、Web インターフェースとの連携といった開発が行われている。

2003 年度の調査以降の動向として、LIRPortal の証明書発行と RPSL のデータベースの連携により、証明書発行数が大幅に増加した点、電子メール（S/MIME）を用いた各種申請業務が挙げられる。

担当者のレベルでは S-BGP 等の新たな証明書の用途に興味を示しているが証明書の新たな用途に関する RIPE ミーティングでの議論はまだ行われていない。

4.4.3. ARIN

ARIN の認証局は、メンバの認証用の証明書を発行することを目的とした認証局である。証明書の申請には本人確認書類が必要とされているが、詳細は明らかにされていない。Web インターフェースを使って証明書の申請を行うとしている。資源管理情報との関連付けは、POC（Point of Contacts：連絡先）の識別子を用いている。各種申請を行うユーザの ARIN による認証を S/MIME の電子署名を用いて実現することが目的である。従って申請業務の為の Web インターフェースが使われることは今の時点では想定されていない。

認証局システムにはオープンソースソフトウェアが使われており、POC との関連性を確認する機能等を除いて大きな開発を行わずに運用されている。CA 証明書を複数発行し、CA の秘密鍵の危殆化に対応するとしている。

2003 年度の調査以降の動向には、メンバ全体への告知およびチュートリアルの実施、CPS の公開が挙げられる。CPS は必要最低限の記述に留められており、特に「POC に対応する証明書所有者の ARIN による認証」の主旨を明文化する目的で記述されたと考えられる。