第7章 IP アドレス認証局の応用

内容

- 経路情報の安全性
    1. 今後のシナリオ
- アドレス資源管理の効率化
    1. Web トランザクション
- 商用 ENUM サービスでの適用事例

第7章　IP アドレス認証局の応用

IP アドレス認証局は、インターネットにおける登録情報の安全性向上と登録情報の内容を用いた認証に利用することができる認証局である。当センターではアドレス資源管理に必要となるネットワーク情報（割り振り先の情報、割り当て先の情報）、ホスト情報、AS 情報といった登録情報のデータベースを管理しており、インターネットの自律的な運用を支える役割を担っている。これらの情報の登録は IP 指定事業者を中心として、多くのネットワーク利用組織が行ってきたものである。アドレス資源の一意となる割り振りというインターネットレジストリにおいて、登録情報は登録者自らが集約する役割を持っているモデルはインターネット以外で使われている識別子の管理モデルとは異なり独特なものであろう。

本章では、この独特のモデルによるアドレス資源管理がインターネットの安全な識別（認証）に対してどのようなアプローチが可能であるか、という点に着目し、インターネットレジストリにおける認証局である IP アドレス認証局がどのような応用の方向性を持っているかについて述べる。

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」でも IP アドレス認証局の応用について述べた。2003 年度は新たなネットワークアプリケーションやビジネスモデルの登場といった広い視野で行ったのに対し、本章では具体的に応用可能なプロトコルについて述べる。本章で紹介するプロトコルにおいて IP アドレス認証局が発行する証明書が利用可能になったとしても、2003 年度で述べたようなネットワークアプリケーションがすぐに実現するわけではないが、インターネットにおける安全なアドレス資源の管理とノード間の認証の実現に向けた活動によって生活基盤としてのインターネットを確立し、向上された安全性にのっとった様々なアプリケーション開発が可能になると考えられる。

本章では三つの応用について述べる。一つは IRR における認証局の応用である。もう一つはアドレス資源管理をより効率的に行う Web トランザクションについて述べる。アドレス資源管理における組織間の連携は RIR と NIR の間において行われてきているが、より迅速さや安全さが効果を発揮する連携は NIR と LIR の間であろう。2004 年度にシステム開発の一環として行われた連携の仕組みについて述べる。更に、ENUM の登録における認証局の利用の事例を紹介する。

7.1. インターネットにおける経路情報の安全性

インターネットにおける経路制御はインターネットレジストリにおけるアドレス資源の割り振りと割り当てに則って行われる。経路制御で使われるアドレス資源は IP アドレスと AS（Autonomous System）番号である。

また AS（Autonomous System：自律システム）は、ネットワーク利用組織が経路を管理する上での方針に則って経路制御を行う。この方針の中には、割り振られていないはずのアドレスの経路情報を排除したり、あまりに経路の変動が激しい場合にその情報を伝播しないようにしたりといった、ネットワークの運用上の安全性を考える上で重要な要素が含まれている。

IRR（Internet Routing Registry）は、AS 番号と prefix（経路情報で使われるアドレスブロック）に加え、経路情報の伝播に関する方針を登録することが出来るインターネットレジストリの機能である。

近年当センターにおいて、IRR における経路情報の安全な交換に向けた活動が行われている。

はじめに 2003 年度に当センターの IRR 企画策定専門家チームで検討された IRR とルーティングの安全性に関する記述を紹介する。

2004 年 3 月 31 日に公開された「JPNIC における IRR サービスに関する検討報告書」から該当部分を抜粋する。

6.8　IRR のセキュリティ

IRR におけるセキュリティを考慮するに当たっては、「IRR が果たす役割」を考えます。そして、その役割を満たすために何を守らなくてはならないのかを定義し、対策を打つことで IRR のセキュリティを高めます。

IRR の果たす役割は、実際にインターネット上に流れる経路に対する台帳　としての役割とそれら経路に関する情報の提供という役割があります。これらの役割を言い替えると、前者は「ルーティングのリスクに対する IRR の役割」であり、後者は「安全な情報提供と情報登録を(ユーザに対して)実施させる役割」と言うことができます。そこで今回は、この 2 点についてフォーカスを絞り検討を実施しました。

これまでの検討においては、その多くが情報そのものの信憑性(意味的な正当性)について実施されてきましたが、上記の 2 点にフォーカス絞るため情報そのものよりも手続き的な信憑性(形式的な正当性)に注目しています。この「形式的な正当性」

とは、登録されている内容が正しいかどうかと言うことではなく、登録される際に、その登録者が正しいかどうかという認証の問題と、登録される内容がいかに検証されるべきかを指しています。

この章では、これらの前提条件のもと、ルーティングと IRR の役割、さらにその役割に対する登録情報の正当性について検討した内容について述べ、最後に、登録情報の正当性をどのような仕組みで実現するかについて述べます。

6.8.1 ルーティングと IRR の安全性

IRR の安全性を検討するに当たっては、「IRR の目的は何か」を定義し、その目的を阻害する要素を分析する必要があります。

IRR とは、ルータによる適切なルーティングを助けるための適切な参照情報を提供することが目的です。このため、IRR の安全性を検討するには、この目的が阻害される脅威に対する検討が必要となってきます。

以下は、この定義に準じた形で、検討項目を明らかにするための簡単なリスク分析を行います。分析は、(a)IRR の目的(要件の定義)、(b)目的を達成するために守るべき資源の定義、(c)それら資源に対する脅威の分析の 3 段階で脅威(いわゆる、リスク)を分析します。

(a)IRR の目標とする要件は何か

- *該当経路のルーティングを行うための参考情報の提供*
- *適切な経路情報を入手するための参考情報の提供*
- *適切な範囲で経路情報の交換を行うための参考情報の提供*

(b)IRR が守るべき資源は何か

- *各ルータが持つ正しい経路情報*
- *経路情報の正しい伝達*
- *意図した通りの AS-PATH の伝達*

(c)資源に対する脅威は何か

- *変更された経路情報の伝達*
  - *・意図された変更*
  - *・意図されない変更*

- *根拠のない経路情報の伝達*
- *経路情報の意図通りでない伝達*

経路情報に対する脅威(上記(c)であげた脅威)から守るためには、いかに伝達されてくる経路情報が正しいかを検証する必要があります。しかし、伝達されてくる経路情報は、BGP の Peer を張っているルータが正しいかどうかというような単純な問題ではなく、Origin AS が発行した経路情報が、伝達過程の AS の中で、その AS の意図通りに加工され、複数の経由 AS の意図が正しく盛り込まれ、最終的な AS に伝達されていることを検証する必要があります。

このような検証を実施できるようにするために IRR を利用するには、IRR は、経路情報の元来あるべき内容と、経路情報流入の根拠を調べられるような情報源になっている必要があります。

そして、この場合の IRR の安全上のあり方は、ルータの挙動と IRR の登録情報が密接に関わる場合に限られています。公共的な IRR の場合は、登録情報が AS に対して強い影響を及ぼさないことがあります。例えば、インターネットレジストリの割り振り情報と IRR の登録情報が対応しているべき、といった要件がどれほど強く適用されるべきなのかを検討する必要があります。

一方、IRR の利用者の観点では、登録情報の正当性に対する依存が発生します。これは他者の登録した情報が、どの程度正当なのかがわからなければ参照の意味が薄れてしまうからです。例えば弱い認証方式を利用して情報の登録を行った利用者は、他者の情報の登録に対しても弱い保護しか期待しなくなります。弱い認証方式が破られ、書き換えられている可能性を考慮しながら参照することは、ルータの管理者にとって上記の脅威を避ける手段としては弱いものになります。その結果、メールなどの他の手段を取らざるを得ず、IRR の効力が薄れてしまいます。

これらのことを考えると、IRR に求められる安全性を決める要素には下記のものがあることがわかります。

- *意図通りのルーティングのための安全性の観点*
  IRR の登録情報が AS に及ぼす影響の強さを想定する必要がある

- *IRR の利用者の観点*
  利用者の IRR に対する依存度を想定する必要がある

つまり、プライベートな IRR に比較して公共的な IRR は蓄積される情報の性質から、IRR の登録情報が AS に及ぼす影響の強さは低いと想定した場合、IRR の安全性は、利用者の IRR に対する依存度によって決定されるということになります。また、依存度は、不慮の操作の禁止、悪意のある操作の不可能性、適正な利用を促す仕組み(制約事項)などの対策を打つことで高めることが可能ということになります。

6.8.2 登録情報の安全性

前節までは、IRR とルーティングシステム全体を考慮したうえでの安全性について検討してきました。ここでは、さらにフォーカスを絞って、IRR への情報登録とそこからの情報提供に関する安全性に検討を進めます。

一般に「安全性」と呼ばれる性質の中には、いくつかの要素があります。
ここで、IRR における安全性という観点で考えると、その登録情報が安全に提供されことや、登録情報が正当性、可用性(availablity)を持ったものであるといった点が重視されると考えられます。その他に、機密性の要素も重要な要素の 1 つではありますが、公共的な IRR では、認証情報のような一部の情報を除くと、あまり重視されない要素であると考えています。

本節では、登録情報の正当性を分類し、「形式的な正当性」について述べます。次に、形式的な正当性が失われる場面と原因について述べ、対策を検討します。

IRR における登録情報の正当性は、まず IRR への登録内容が正しいこと、そして、登録や参照手続きの処理が確実であること、この 2 つが両立してはじめて成り立ちます。登録や閲覧手続きが確実であるとは、正しい登録者による登録結果が、その通りに誰もが閲覧できるような状態のことを指します。
ここでは、内容の正しさを「意味的な正当性」と呼び、登録や閲覧手続きの確実性に基づく正当性を、「形式的な正当性」と呼ぶことにします。

形式的な正当性が失われる状況を挙げると、以下のようになります。

- *登録情報自体の正当性が失われる状況*
  - *意図しない変更・削除*

・*災害*
・*サーバ・クライアントのバグ*
・*クライアント・ユーザへのなりすまし行為*

- *登録時の不正*
・*サーバへのなりすまし行為*
・*クライアント・ユーザへのなりすまし行為*

- *利用上の登録情報の正当性が失われる状況*

- *参照時の不正*
・*サーバへのなりすまし行為*
・*伝送路での書き換え(参照時、ミラー時)*

これまで、RPSL では「登録時の不正」に着目し、CRYPT-PW, PGP-KEY と言った認証機能を用意していました。しかし、形式的な正当性という見方をすると、登録者の認証だけでは、「意図しない変更・削除」や「参照時の不正」の対策をとることができません。これらの状況には、登録時以外での登録情報の変化が含まれており、登録者の認証だけでは、検出や回避することはできないためです。

つまり、登録情報の形式的な正当性を確認する仕組みが必要になります。
例えば、登録情報にハッシュ値を付加し、閲覧時に確認するといった方法です。登録者との関連性を保障するため、ハッシュ値に電子署名を加える方法が考えられます。しかし、RPSL ではオブジェクトに電子署名を加える書式は提供されていません。参照のために、Whois プロトコルの代わりに https を利用したとしても、「参照時の不正」や「サーバへのなりすまし行為」を検知することができるだけで、ミラーリングを行っているときの伝送路での書き換えを防ぐことはできません。

今後、形式上の正当性を確保するためには、CRISP や EPP(Extensible Provisioning Protocol)において電子署名を利用した登録情報の保護機能が必要になると考えられます。しかし、そのためには認証情報(署名鍵)の管理や登録の手続きなどを、今後検討する必要があります。

6.8.3 IRR のセキュリティ向上のための今後の対応

IRR のセキュリティを検討するために、いくつかの言葉の定義や IRR における安全性について基本的検討から行いました。

これらの検討の中で、登録情報の形式上の正当性について検討を進めましたが、その一方で、意味的な正当性の向上についてはほとんど検討がされていません。また、IRR に必要な安全性を決める要素として、ルーティングの安全性と IRR の利用者の観点を挙げましたが、これについても、運用者や IRR 情報のミラーリング時の検討が行われていません。さらに、形式的な正当性を確保するためには、登録時の認証ではなく、登録された情報を保護する仕組み(電子署名)を利用する仕組みについて述べましたが、現行の RPSL では電子署名を利用することはできません。

IRR に関するセキュリティの議論は、ルーティングシステムとの関連の中で検討する必要があるため、検討のポイントはルーティングシステム自体へとずれてしまいがちです。今後は、IRR そのもののセキュリティの検討と、ルーティングシステムと関連させたセキュリティの検討に分割すると共に、今回の検討で残されている検討項目をさらに検討していく必要があります。

2004 年度は、この IRR 企画策定専門家チームにおける検討を元に認証局の応用のシナリオを検討した。

7.1.1. 2004 年度に行われた議論とシナリオ

2003 年度の議論を受け、IRR 企画策定専門家チームの 2004 年度の議論では、IRR におけるセキュリティの目標の設定が行われた（図 7-1)。

概要

- **次世代（本来）のIRRのセキュリティ上のゴール**
  - **登録内容を信じて設定できること ⇒ 今回**
    - **考え方：信じて設定（例えば自動設定） ⇒ 楽 ⇒ 利用価値**
    - **仕組み：登録時の認証強化 ⇒ 登録内容のチェック ⇒ 正しい形で提供 ⇒ 機能的に利用**
  - **登録内容を使って相手認証できること ⇒ 将来**
    - **考え方：S-BGP、soBGP で使える ⇒ 経路ハイジャックに対する防衛強化**
    - **仕組み：登録時の認証強化 ⇒ 登録内容のチェック ⇒ 証明書発行 ⇒ 証明書を使ってAS認証**

図 7-1 IRR におけるセキュリティの目標の設定

またこの二つの目標を達成する為に、必要になる仕組みの提案がされた（図 7-2）。

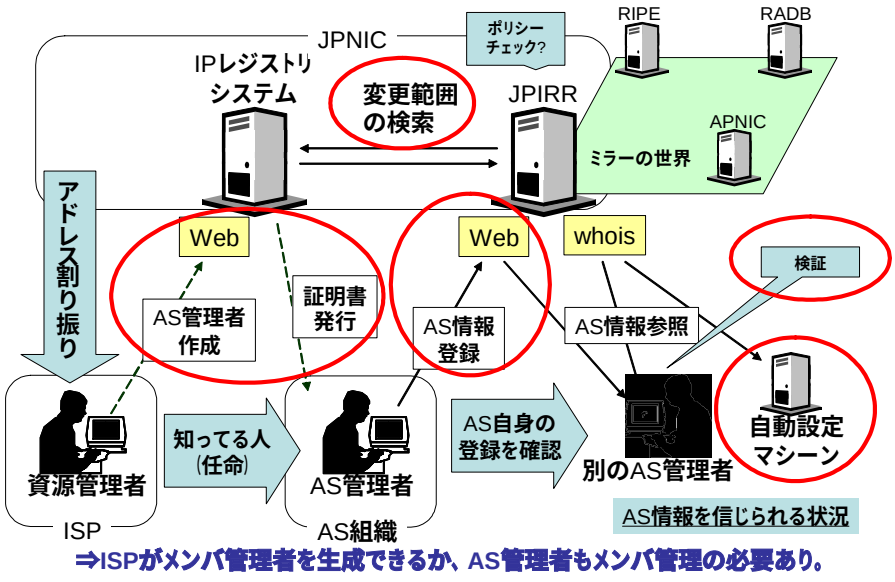

図 7-2 セキュリティの目標を達成するための仕組み

この仕組みは IRR への登録時の認証を強化し、登録情報と登録者の関係をたどれる状況を作ることで、IRR に登録された情報を使ったネットワーク機器の設定を行うことができるというものである。また登録情報に電子署名を付けることで、登録者と登録情報の正当性（改竄がないこと）を検証することが出来るようになるとしている。電子署名であれば他の IRR からミラーの仕組みを使って伝播してきた情報であっても、検証ができるとしている。

登録時の認証強化は Web インターフェースを使うなどすることで、既存のソフトウェアやプロトコルを使って実現する見込みがあるが、IRR の登録情報における電子署名を行う仕組みはこれまでにはなく、実現の為には新たに提案・開発を行っていく必要がある。

7.2. アドレス資源管理の効率化　－Web トランザクション－

本節では、IP レジストリシステムの Web トランザクション機能の目標、運用管理されているデータ及び業務を明らかにし、IP 指定事業者と交換するレジストリデータの安全性確保について述べる。

7.2.1. Web トランザクションの目標

レジストリデータ、中でもアドレス資源の管理において、指定事業者もしくは ISP が行う業務は多岐に渡る。ただし業務によっては年間数件のみの処理が必要な業務から、日常的に発生する業務まで、業務内容により様々である。そこで、今回は指定事業者が ISP の申請を受け、指定事業者が JPNIC へ申請をするという二段構成を検討し、指定事業者と JPNIC の間の連携実現を目指す。

IP アドレス管理業務において、基本となる 3 つの業務を以下に示す。

- IP アドレスの割り振り
  指定事業者からの割り振り申請に対して、IP アドレスの範囲を割り振る(割り振られた IP アドレスの範囲を、アサインメントウィンドウサイズ　以下 ASWS と略す)。
- IP アドレスの割り当て
  指定事業者が、割り振られた IP アドレスを実際に使用する場合に、割り振られたアドレスを割り当てる。
- 追加割り振り申請
  JPNIC から IP アドレスを指定事象者へ割り振り続けると、指定事業者へ割り振ることができるアドレスが不足することがある。その場合に、JPNIC が APNIC から、新しい IP アドレスの範囲を取得する必要がある。

3 つの業務のユースケース図を次頁に示す。

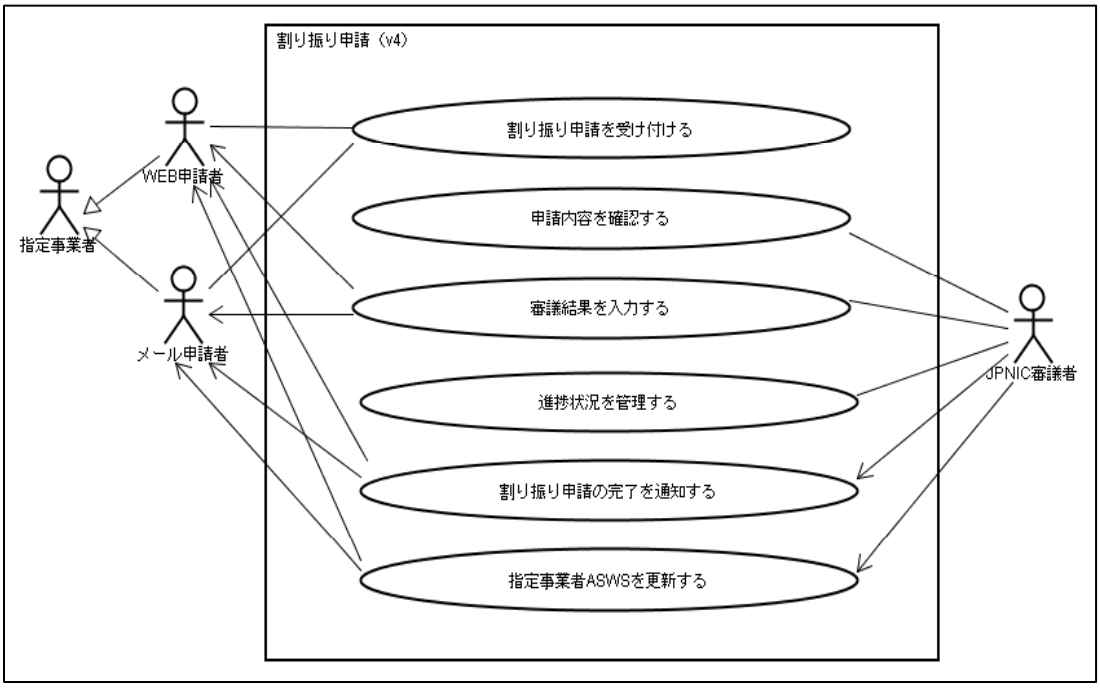

図 7-3　IP アドレス割り振り申請のユースケース図

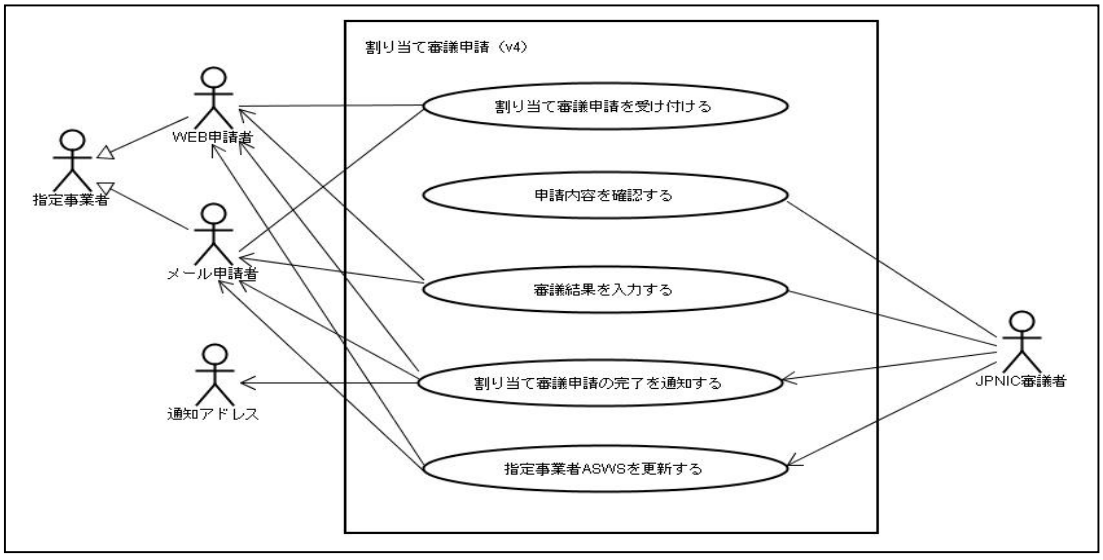

図 7-4　IP アドレス割り当て申請のユースケース図

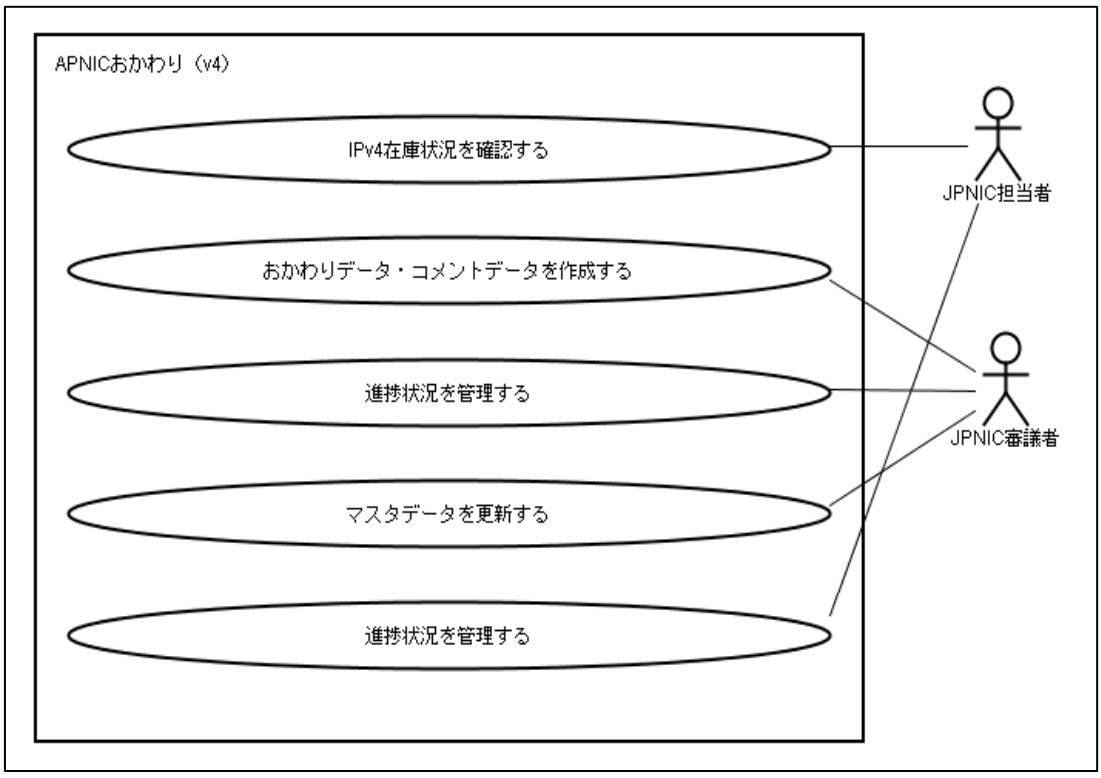

図 7-5　APNIC への追加割り振り申請のユースケース図

そこで、現在日常的にメールにて行われている、IP アドレス割り当て報告時における申請処理について、Web トランザクション方式を用いて処理の迅速化を図り、エンドユーザからの申請に対する指定事業者側の負担軽減を目的とする。

7.2.2. IP レジストリシステムが提供する機能リスト

IP レジストリシステムとは、JPNIC の IP 事業部の業務担当者が IP アドレス及び関連資源提供業務を行うにあたり、必要とする情報の保持、伝達、保守及び公開を行うことを目的としたシステムである。

IP レジストリシステムは、IPv4 アドレスの管理をはじめとする IP アドレス関連資源の管理業務を行う。主な機能は以下の通り。

- 指定事業者から、IP アドレスおよび関連資源の割り振りや返却の申請を受け付け、処理結果を IP レジストリシステムから指定事業者へ通知する。（表 7-1①）
- 指定事業者および指定事業者を含む一般申請者から、AS 番号の割り当て、返却、変更等の申請を受け付け、処理結果を IP レジストリシステムから指定事業者へ通知する（表 7-1②）

- APNIC に対して、共有プールの申請、指定事業者からの IPv6 に関する申請の取次ぎ申請、日本国内の IP アドレス割当報告等を行う（表 7-1③）
- 指定事業者を含めたインターネット利用者に対して、Whois データベース情報および逆引き DNS 情報の公開を行う（表 7-1④）
- 上記の各機能を JPNIC の業務担当者やシステム運用者が運用する（表 7-1⑤）

IP レジストリシステムの利用者、接続システムとの関係イメージを図 7-6 に示す。

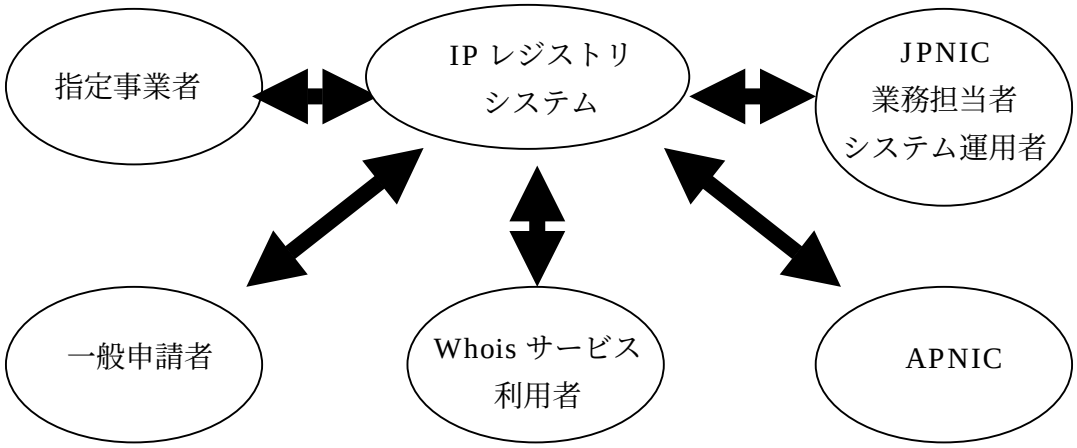

図 7-6　IP レジストリシステムの関係イメージ

IP レジストリシステム内で処理する主な申請業務を、次の表に示す。

表 7-1　主な申請業務一覧

申請名	利用方法			対象者			申請概要
	①	②	③	④	⑤	⑥	
割り振り申請(v4)	○	○		○		○	指定事業者からの割り振り申請を受付け、申請内容について JPNIC 審議を行い、APNIC 共有プールまたは追加割り振り申請のプールから割り振り処理を行う。
割り振り返却申請(v4)	○	○		○		○	指定事業者からの割り振り返却申請を受付け、申請内容について JPNIC 審議を行い、追加割り振り申請のプールへ割り振り返却処理を行う。

APNIC への返却申請	○					○	割り振り返却申請(v4)において、追加割り振り申請のプールへ割り振り返却処理されたアドレスブロックを一定期間エージングし、APNIC 共有プールへ返却処理を行う。
割り当て審議申請(v4)	○	○		○		○	指定事業者からの割り当て審議申請を受付け、申請内容について JPNIC 審議を行い、審議結果を通知する。
割り当て報告申請	○	○		○			指定事業者からの割り当て報告申請を受付け、申請内容について JPNIC 審議を行い、割り当て情報の更新処理を行う。
割り当て・リナンバ報告・返却の取下申請	○			○		○	指定事業者からの割り当て・リナンバ報告・返却の取下申請を受付け、申請の取下処理を行う。
イベント割り当て申請	○			○		○	指定事業者からのイベント割り当て申請を受付け、申請内容について JPNIC 審議を行い、イベント割り当て処理を行う。
割り当て済アドレスの統廃合申請	○			○		○	指定事業者からの割り当て済アドレスの統廃合申請を受付け、申請内容について JPNIC 審議を行い、アドレス統廃合処理を行う。
割り当て IP アドレスの返却申請	○	○		○			指定事業者からの割り当て IP アドレスの返却申請を受付け、割り当て返却処理を行う。
割り当て返却年月日変更申請	○			○			指定事業者からの割り当て返却年月日変更申請を受付け、割り当て返却年月日の更新処理を行う。
ネットワーク記載事項変更申請	○	○		○		○	指定事業者からのネットワーク記載事項変更申請を受付け、申請内容について JPNIC 審議を行い、ネットワーク情報の更新処理を行う。
IP 指定事業者情報変更申請	○	○		○		○	指定事業者からの IP 指定事業者情報変更申請を受付け、申請内容について JPNIC 確認を行い、指定事業者情報の更新処理を行う。
逆引きネームサーバ申請	○	○		○		○	指定事業者からの逆引きネームサーバ申請を受付け、申請内容について JPNIC 審議を行い、逆引き DNS の更新処理を行う。
個人情報申請	○	○		○		○	指定事業者からの個人情報申請を受付け、申請内容について JPNIC 審議を行い、個人情報の更新処理を行う。

AS 割り当て申請	○			○	○	○	指定事業者または一般利用者からの AS 割り当て申請を受付け、申請内容について JPNIC 審議を行い、AS 番号割り当て処理を行う。
AS 返却申請	○	○		○	○	○	指定事業者または一般利用者からの AS 返却申請を受付け、申請内容について JPNIC 審議を行い、AS 番号割り当て返却処理を行う。
AS 情報変更申請	○	○		○	○	○	指定事業者または一般利用者からの AS 情報変更申請を受付け、申請内容について JPNIC 審議を行い、AS 番号情報の更新処理を行う。
指定事業者契約申請	○		○	○	○	○	指定事業者または一般利用者からの指定事業者契約申請を受付け、申請内容について JPNIC 審議を行い、郵送で契約関連書類を取り交わし、契約締結処理と行う。
指定事業者解約申請	○	○	○	○		○	指定事業者からの指定事業者解約申請を受付け、郵送で解約関連書類を取り交わし、申請内容について JPNIC 審議を行い、契約解約処理と行う。
APNIC 向け追加割り振り申請 (v4)	○					○	V4 アドレスブロックが不足した際に、JPNIC 業務担当者が APNIC へ v4 アドレスブロックの割り振り依頼を行う。
APNIC 向け追加割り振り申請(AS)	○					○	AS 番号が不足した際に、JPNIC 業務担当者が APNIC へ AS 番号の割り振り依頼を行う。
V6 割り振り申請取次ぎ	○	○		○		○	指定事業者からの割り振り申請取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ割り振り依頼を行う。
V6 割り振り変更取次ぎ	○	○		○		○	指定事業者からの割り振り申請取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ割り振り情報の更新依頼を行う。
V6 割り振り返却取次ぎ	○	○		○		○	指定事業者からの割り振り返却取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ返却依頼を行う。
V6 割り当て申請取次ぎ	○	○		○			指定事業者からの割り当て申請取次ぎを受付け、APNIC 向けデータベースの更新処理を行う。
特殊用途 PI アドレス割当取次ぎ	○		○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス割り当て取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で契約関連書類を取り交わし、契約締結処理を行う。また、APNIC へ割り当て依頼を行う。

特殊用途 PI アドレス変更取次ぎ	○		○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス変更取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で変更関連書類を取り交わし、契約更新処理を行う。また、APNIC へ割り当て情報の更新依頼を行う。
特殊用途 PI アドレス解約取次ぎ	○	○	○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス解約取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で解約関連書類を取り交わし、解約処理を行う。また、APNIC へ割り当て情報の更新依頼を行う。
アドレスリスト申請	○		○	○	○	○	指定事業者または一般利用者からのアドレスリスト申請を受付け、申請内容について JPNIC 確認を行い、パスワード発行処理を行う。
情報開示請求申請	○		○	○	○	○	指定事業者または一般利用者からの情報開示請求申請を受付け、申請内容について JPNIC 確認を行い、開示情報リストの作成処理を行う。

利用方法　①：Web　②：メール　③：郵送

対象者　④：指定事業者　⑤一般利用者　⑥：JPNIC 業務担当者

また、表 7-2 にレジストリデータの管理や外部連携等、主な機能を示す。

表 7-2　IP レジストリシステムの主な提供機能

機能区分	機能名	機能概要
資源管理	V4 割り振り管理	割り振り申請(v4)、割り振り返却申請(v4)、APNIC への返却申請、APNIC 向け追加割り振り申請 (v4)、指定事業者契約申請における v4 割り振り管理を行う。
	V4 割り当て管理	割り当て審議申請(v4)、割り当て報告申請(v4)、割り当て・リナンバ報告・返却の取下げ申請、イベント割り当て申請、割り当て済アドレスの統廃合申請、割り当て IP アドレスの返却申請、割り当て返却年月日変更申請における v4 割り当て業務を行う。
	V6 割り振り管理	V6 割り振り申請取次ぎ、v6 割り振り変更取次ぎ、v6 割り振り返却取次ぎにおける v6 割り振り管理を行う。
	V6 割り当て管理	V6 割り当て申請取次ぎにおける v6 割り当て管理を行う。

	AS 割り当て管理	AS 割り当て申請、AS 返却申請、AS 情報変更申請、APNIC 向け追加割り振り申請 (AS)、指定事業者契約申請における AS 割り当て管理を行う。
	特殊用途 PI 割り当て管理	特殊用途 PI アドレス割り当て取次ぎ、特殊用途 PI アドレス変更取次ぎ、特殊用途 PI アドレス解約取次ぎにおける特殊用途 PI 割り当て管理を行う。
	個人情報管理	個人情報申請における個人情報管理を行う。
	ネットワーク情報管理	ネットワーク記載事項変更申請におけるネットワーク情報管理を行う。
	ML リスト管理	日次処理として、ML リストの更新処理を行う。
	IP リスト管理	日次処理として、IP リストの更新処理を行う。
	AS 番号リスト管理	日次処理として、AS 番号リストの更新処理を行う。
	Whois 情報管理	Whois データ更新時に、JPNIC　Whois データベースの更新処理を行う。
契約管理	指定事業者契約管理	指定事業者契約申請における指定事業者契約関連処理を行う。
	指定事業者変更管理	IP 指定事業者情報変更申請における指定事業者変更処理を行う。
	指定事業者解約管理	指定事業者解約申請における指定事業者解約処理を行う。
外部連携	APNIC 連携	APNIC 向け Whois 情報、逆引き DNS 情報を作成し、APNIC データベースへの連携を行う。
	JPRS 連携	JPRS 向け Whois 情報、逆引き DNS 情報を作成し、JPRS データベースへの連携を行う。
Whois	Whois 検索 (Web)	Web ブラウザからの Whois 検索を行う。
	Whosi 検索（Whois クライアント）	Whois クライアントからの Whois 検索を行う。

表 7-1 および表 7-2 に示す通り、IP アドレス管理業務は多岐に渡る。申請業務のほとんどが、メールによる申請と、Web での申請状態確認という位置付けであるため、申請担当者及び JPNIC 業務担当者の双方にとって、効率が悪い。

そこで、メールでの申請ではなく、Web により直接申請が可能なように効率化を図る。従来、メールによる申請担当者の認証は、メールの送信元アドレスを基本としている。Web での申請の場合も、申請担当者の認証が同様に必要となる。Web での認証としては、証明書による認証基盤を利用する。

7.2.3. IP レジストリシステムの構成

まず、現在、IP アドレス管理業務を運用している IP レジストリシステムの構成を明らかにする。続いて、IP レジストリシステム上に、証明書による認証基盤を連携する場合に、どのようなシステム連携で、申請担当者認証を行うのかを明らかにしていく。

IP レジストリシステムの論理ネットワーク構成図を図 7-7 に示す。

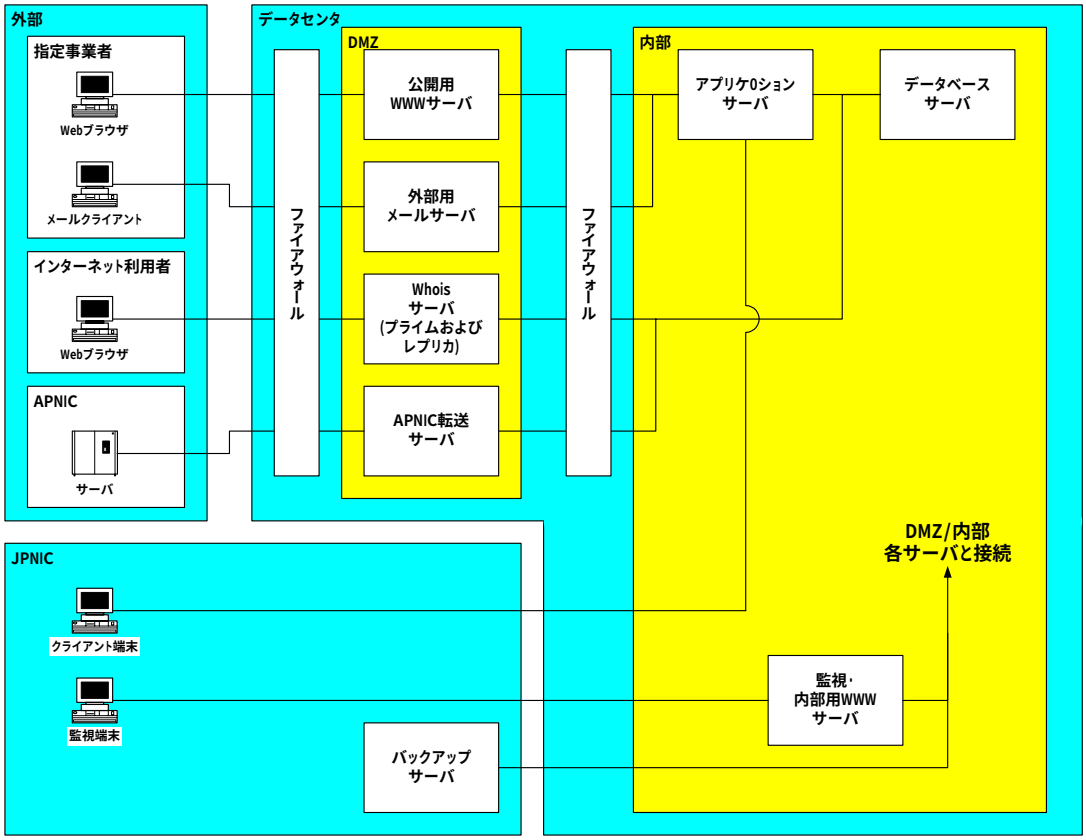

図 7-7　IP レジストリシステムの論理ネットワーク構成図

また、各サーバでの提供機能を表 7-3 に示す。

表 7-3　IP レジストリシステム内サーバの提供機能

サーバ名	提供機能
メールサーバ	・インターネットを経由した指定事業者からのメールによる各種申請の受付け及び応答を行う。
公開用 WWW サーバ	・インターネットを経由した指定事業者からの Web ブラウザによる各種申請等の受付け及び応答を行う。
Whois サーバ(プライム)	・インターネットを経由した一般利用者からの Web ブラウザによる Whois サービスの受付け及び応答を行う。 ・Whois サーバ(レプリカ)との複数構成により、負荷分散と障害時のサービス継続を行う。
Whois サーバ(レプリカ)	・インターネットを経由した一般利用者からの Web ブラウザによる Whois サービスの受付け及び応答を行う。
APNIC 転送サーバ	・APNIC システムとの間で、逆引き DNS データ、Whois データの送受信を行う。
アプリケーションサーバ	・公開用 WWW サーバ、メールサーバからの要求を元に、各種申請を処理する。
データベースサーバ	・主なデータを格納し、アプリケーションサーバからの処理要求を受付ける。
監視・内部用 WWW サーバ	・IP レジストリシステム内の各サーバ及びネットワーク機器の動作状態を監視する。 ・JPNIC 内部用 WWW サーバを兼ね、JPNIC 業務管理者が申請業務を処理する際に利用する。
バックアップサーバ	IP レジストリシステム内の各サーバのデータについて、バックアップを行う。

7.2.4. IP アドレス認証局と IP レジストリシステムとの連携

IP レジストリシステムで表 7-1 及び表 7-2 で示した各種申請を行う際に重要となるのは、申請担当者の認証である。申請担当者を認証するために、IP アドレス認証局システムが IP レジストリシステムと連携してクライアント証明書を発行するまでの処理の流れを、図 7-8 に示す。認証情報の連携は、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”の際に策定したモデルを適用し、設計する。

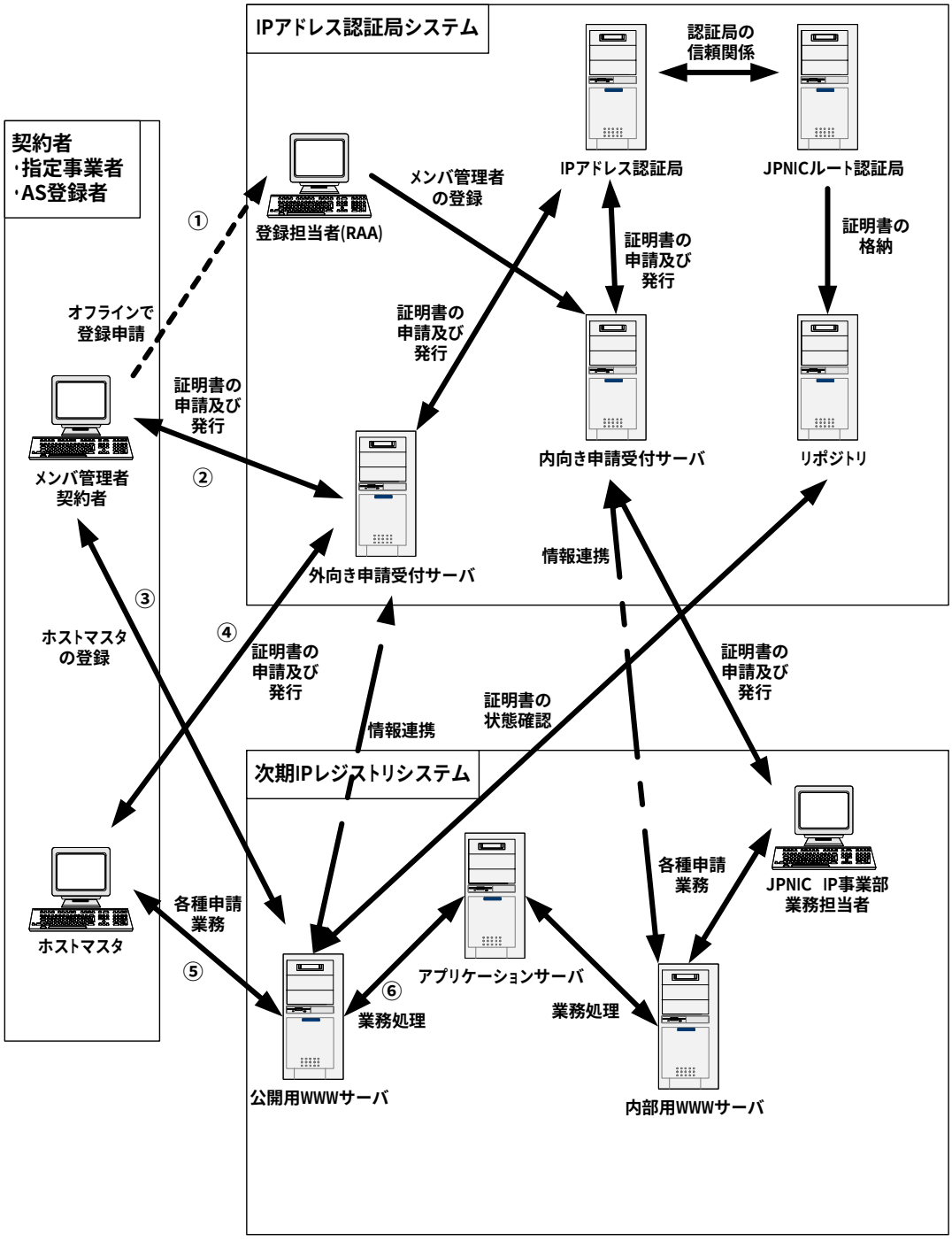

図 7-8　IP レジストリシステムと IP アドレス認証局システムの連携

図 7-8 において、ホストマスタが申請業務を行うまでの流れを、以下に示す。

- ①において、メンバ管理者自身の証明書の発行申請を行う
- ②において、登録担当者から返却された情報を元に外向き申請受付サーバへアクセスし、メンバ管理者が自身の証明書を取得する

- ③において、ホストマスタの情報を登録しておく
- ④において、③で登録された情報でホストマスタが外向き申請受付サーバへアクセスし、ホストマスタ自身の証明書を取得する
- ⑤において、ホストマスタ自身の証明書を使用して公開用 WWW サーバへアクセスし、申請業務を行う
- ⑥において、申請者（すなわちホストマスタ）の権限および申請内容を確認し、処理する

図 7-8 に示すように、IP レジストリシステム上のユーザを IP アドレス認証局システム上で認証するためには、IP レジストリシステムと IP アドレス認証局システムを連携するための設計が必要となる。

IP レジストリシステムと IP アドレス認証局システムそれぞれでユーザが利用する Web ページの遷移及び両システム間でインターフェースしあうデータの流れ(図 7-8 中の外向き申請受付サーバと公開用 WWW サーバ間及び内向き申請受付サーバと内部用 WWW サーバ間の情報連携部分)を詳細化したものを図 7-9 に示す。

外向き申請受付サーバおよび公開用 WWW サーバは、インターネットを介した契約者からのアクセスに利用される。内向き申請受付サーバおよび内部用 WWW サーバは、JPNIC IP 事業部の業務担当者からのアクセスに利用される。

IP レジストリシステムと IP アドレス認証局システム間で連携されるデータは、クライアント証明書を申請するために利用される。クライアント証明書と 1 対 1 に対応する証明書認証 ID は、メンテナーコードというグループに所属する。メンテナーコードとは、操作対象資源と操作権限を持つグループである。

IP レジストリシステム内のデータベースにて保管されているメンテナー及び証明書認証 ID に関するデータを、クライアント証明書への処理の際に IP アドレス認証局システムからの問い合わせに対して適切に回答するインターフェースが、図 7-9 におけるメンテナートランザクション CGI である。このインターフェースにより、IP レジストリシステムと IP アドレス認証局システムの間で、認証のためのデータの連携が実現可能となる。

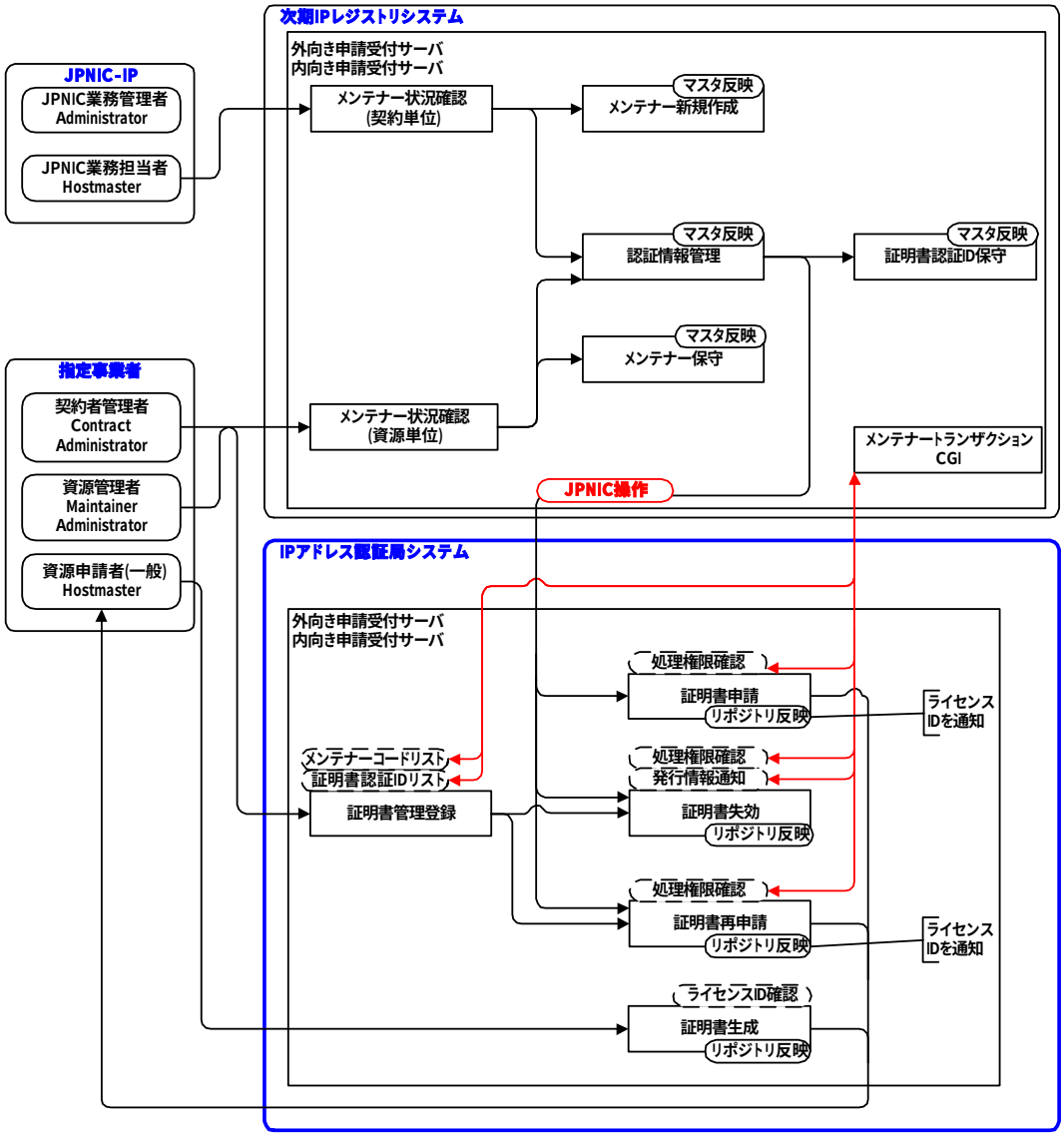

図 7-9　IP レジストリシステムと IP アドレス認証局間のデータの流れ

図 7-9 中において、IP アドレス認証局が IP レジストリシステムにて動作するメンテナートランザクション CGI との通信を行う 4 つのインターフェースについて、表 7-4 に示す。

表 7-4　インターフェース一覧

インターフェース名	処理内容
メンテナーコードリスト取得	証明書に関する処理を行いたいメンテナーを検索するためのインターフェース。 メンテナーコードを直接指定するのみではなく、メンテナーコードが所属している組織や、対応する契約管理番号もしくは資源管理者番号からも検索可能である。
証明書認証 ID リスト取得	特定のメンテナーコードに紐付いている証明書認証 ID のリストを取得するためのインターフェース。
処理権限確認	証明書に関する操作を行う場合、処理対象となる証明書認証 ID が紐付いているメンテナーコードの権限を管理可能か、確認するためのインターフェース。
発行情報通知	証明書に関する操作が完了した場合、操作に関する情報(証明書の発行もしくは失効)を IP レジストリシステムへ通知するためのインターフェース。

表 7-4 に示した 4 つのインターフェースについて、問い合わせ内容、返却値および返却例について、表 7-5 から表 7-14 に示す。

表 7-5　メンテナーコードリスト取得インターフェース

項番	項目名	備考
1	検索区分	1：契約管理番号、2：資源管理者番号、3：資源管理者略称、4：組織名、5：メンテナー検索
2	検索対象	検索したい文字列

表 7-6　メンテナーコードリスト取得インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	メンテナー情報	複数回指定可
3-1	メンテナーコード	検索された情報に紐付いているメンテナーコード
3-2	権限識別子	3-1 で返却するメンテナーコードの権限

3-3	組織名	3-1 で返却するメンテナーコードの所属組織
3-4	メンテナー識別名	3-1 で返却するメンテナーコードの識別名
4	件数	返却するメンテナーコード数

表 7-7　メンテナーコードリスト取得インターフェースへの返り値例

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Tue, 28 Sep 2004 02:15:06 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Tue, 28 Sep 2004 02:09:24 GMT
Content-Length: 101

RET=00
RET_CODE=00000000
MNTNER=MNT-JP000001¥tMNT_AR=4¥tORG_NUM=
Japan Network Infomation Center¥tMNT_NM=山田太郎
MNTNER=MNT-JP000002¥tMNT_AR=5¥tORG_NUM=
Japan Network Infomation Center¥tMNT_NM=佐藤次郎
COUNT=2
```

表 7-8　証明書認証 ID リスト取得インターフェース

項番	項目名	備考
1	メンテナーコード	証明書認証IDのリストを取得したいメンテナーコード

表 7-9　証明書認証 ID リスト取得インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	権限識別子	問い合わせされたメンテナーコードの権限 1：JPNIC 業務管理者、2：JPNIC 業務担当者、3：契約管理者、4：資源管理者、5：資源申請者

4	組織名	問い合わせされたメンテナーコードの所属組織
5	証明書認証 ID	問い合わせされたメンテナーコードに紐付いている証明書認証 ID
6	件数	返却する証明書認証 ID 数

表 7-10　証明書認証 ID リスト取得インターフェースへの返り値例

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Tue, 28 Sep 2004 02:15:06 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Tue, 28 Sep 2004 02:09:24 GMT
Content-Length: 150

RET=00
RET_CODE=00000000
MNT_AR=4
ORG_NUM = Japan Network Infomation Center
CERT_ID=1234567
CERT_ID=2345678
COUNT=2
```

表 7-11　処理権限確認インターフェース

項番	項目名	備考
1	処理者メンテナーコード	証明書の発行を依頼するユーザのメンテナーコード
2	被処理者メンテナーコード	証明書を発行する対象ユーザのメンテナーコード

表 7-12　処理権限確認インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000

表 7-13　発行情報通知インターフェース

項番	項目名	備考
1	メンテナーコード	証明書状態が変更された証明書認証 ID が紐付いているメンテナーコード
2	証明書認証 ID	証明書状態が変更された証明書認証 ID
3	申請状態フラグ	証明書状態 1：発行済み、2：失効済み

表 7-14　発行情報通知インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	メンテナーコード	通知されたメンテナーコード
4	証明書認証 ID	通知された証明書認証 ID

7.2.5. LIR 認証局と IP レジストリシステムとの連携

前節では、申請担当者を認証するためのクライアント証明書を発行及び失効する際の処理の流れを示した。ここでは、申請担当者ではなく指定事業者システムを利用する複数のユーザを仮想的に申請担当者とみなす場合を検討する。

図 7-10 において、指定事業者システムの WWW サーバが、IP レジストリシステムからは一人の申請担当者として見ることができる。すなわち、IP レジストリシステムと関連するクライアント証明書を所有しない複数の申請担当者は、指定事業者システムの WWW サーバに認証を肩代わりしてもらうことにより、認証の通った申請業務を遂行可能となる。

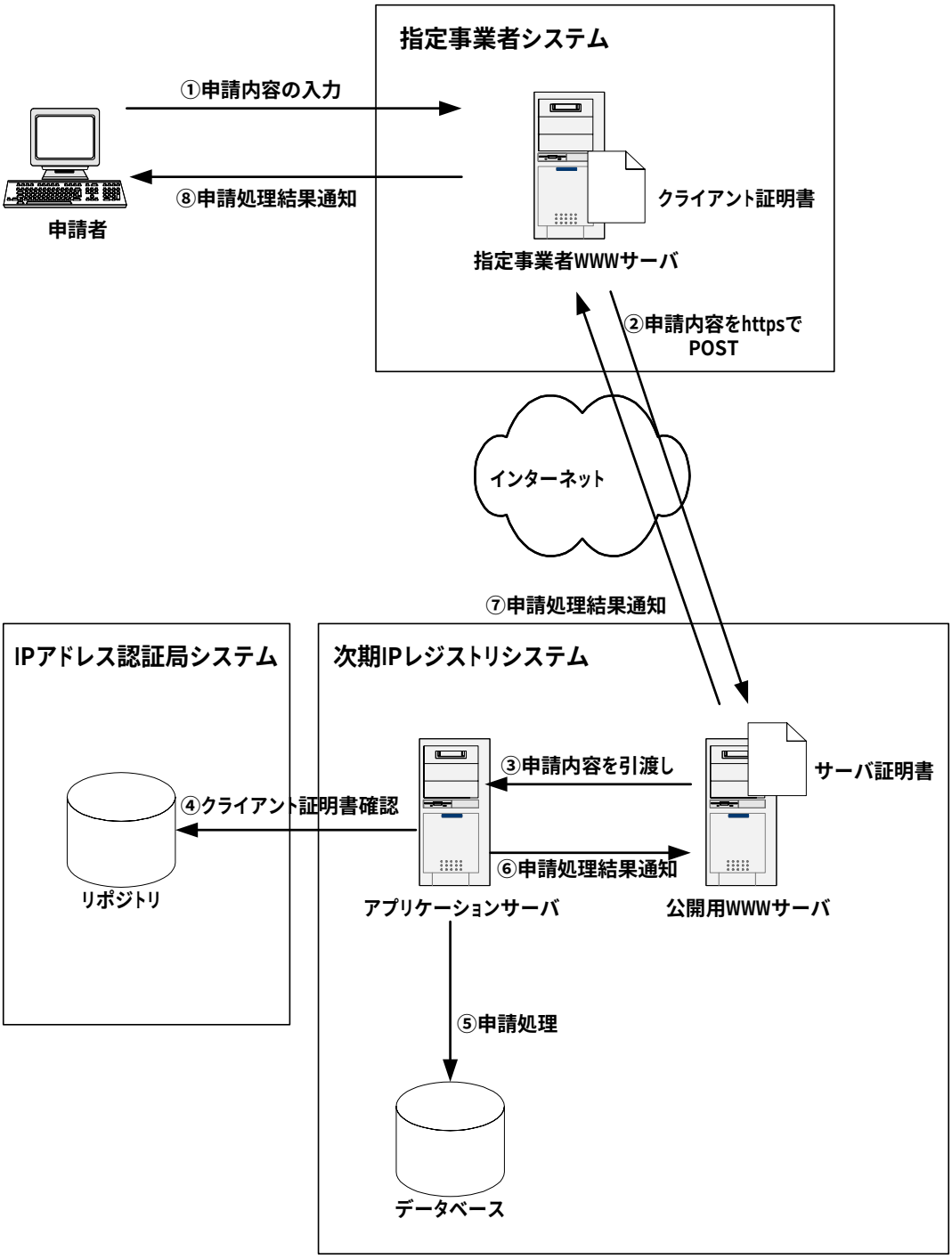

図 7-10　Web トランザクションによる申請の流れ

7.2.6. LIR の認証モデル

https での通信において、通信の暗号化とともにクライアント認証も重要である。ここでは、Web トランザクションによるアクセスと、一般申請者が Web ブラウザでアクセスする際の 2 種類のアクセスについて、クライアント証明書を利用したクライアント認証処理の流れを示す。

まずは Web トランザクションによるアクセスの場合を示す。図 7-10 において、「② 申請内容を https で POST」の部分で、クライアント認証を行う必要がある。トランザクションの流れを以下に示す。(図 7-11 参照)

- 事前に、IP アドレス認証局にて発行したクライアント証明書を https クライアントに組み込んでおく必要がある。
- １、指定事業者 WWW サーバ内の https クライアントが、IP レジストリシステムの公開用 WWW サーバへ https 通信を開始する。
- ２、公開用 WWW サーバが、自身の WWW サーバ証明書を https クライアントに通知し、https クライアントは WWW サーバ証明書を確認する。
- ３、https クライアントが、自身のクライアント証明書を公開用 WWW サーバへ通知し、公開用 WWW サーバはクライアント証明書を確認する。その際に、クライアント証明書の有効期限チェック、IP アドレス認証局のリポジトリ内 CRL のチェックを経て、問題がない場合はクライアント証明書内に格納されているメンテナーコードを取得する。
- ４、メンテナーコードから権限や処理可能な資源情報をデータベースから取得し、申請内容との整合性を確認する。

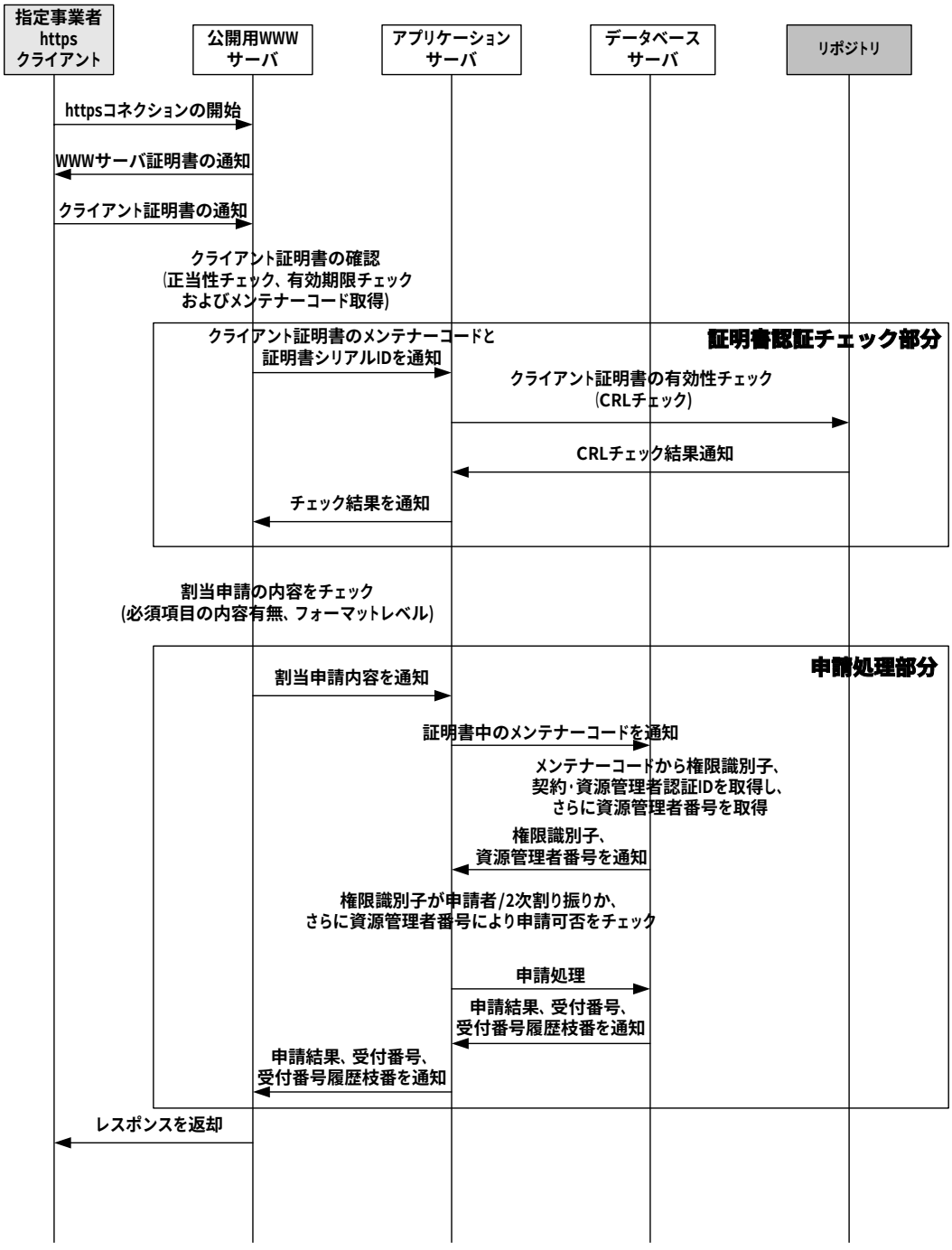

図 7-11　トランザクション処理の流れ

Web トランザクションにおけるクライアント認証と同様に、一般申請者が Web ブラウザを使用して、クライアント証明書による認証により公開用 WWW サーバへアクセスする実装も可能である。

- 事前に、IP アドレス認証局にて発行したクライアント証明書を Web ブラウザに組み込んでおく必要がある。
- １、Web ブラウザにより公開用 WWW サーバへ https を使用してアクセスする。
- ２、公開用 WWW サーバが、自身の WWW サーバ証明書を Web ブラウザに通知し、Web ブラウザは WWW サーバ証明書を確認する。
- ３、Web ブラウザが、組み込まれているクライアント証明書を公開用 WWW サーバへ通知し、公開用 WWW サーバはクライアント証明書を確認する。その際に、クライアント証明書の有効期限チェック、IP アドレス認証局のリポジトリ内 CRL のチェックを経て、問題がない場合はクライアント証明書内に格納されているメンテナーコードを取得する。
- ４、メンテナーコードから権限や処理可能な資源情報をデータベースから取得し、権限に対応した Web ページを Web ブラウザへ返す。

7.2.7. 運用上の問題点と課題

クライアント証明書による認証は、アクセス元を特定する手段として有効であるが、クライアント証明書の管理に慎重になる必要がある。本節では、クライアント証明書の運用上の問題点と課題について述べる。

まず、指定事業者への証明書提供(運用管理部分)に関する問題点と課題について検討する。

クライアント証明書を利用した認証システムにおいては、クライアント証明書の管理に注意する必要がある。

証明書は、有効期限を設定して発行される。一般的には、クライアント証明書の有効期限は１年間である。発行から１年間経過した場合、そのクライアント証明書は無効となり、認証に使用できない。よって、クライアント証明書の再発行、引渡し、設定を考慮すると、有効期限が切れる１ヶ月前程度を目安とし、更新処理を行う必要がある。クライアント証明書を利用するすべての指定事業者に対して、同じタイミングでクライアント証明書を発行するならば、更新処理も同じタイミングで可能だが、契約時期が異なる場合はクライアント証明書の発行タイミングも異なることとなり、指定事業者毎に異なるタイミングで更新処理を行う必要がある。

クライアント証明書自体の管理も厳重に行う必要がある。現在の不正アクセス、個人情報漏洩問題と関連し、以下のような問題点がある。

- クライアント証明書が組み込まれているモバイル PC を盗難され、不正アクセスされてしまう。
- クライアント証明書のファイルが不正に複製され、外部に漏洩し、不正アク

セスされてしまう。

- また、有事の際の対処としては、機能面と業務面の 2 つの方向からの対処が挙げられる。まずは機能面での対処について、以下に示す。
- 不正アクセスに使用されたユーザのアカウントを、IP レジストリシステム側で無効とする。IP アドレス認証局システム側でクライアント証明書として正当なものと認識されたとしても、IP レジストリシステム側のアカウントが無効となっている場合は、ログインおよび申請業務を不可とする。
- 不正アクセスに使用されたユーザのクライアント証明書を、IP アドレス認証局システム側で失効扱いとする。IP レジストリシステム側での認証の際に、CRL に挙がっているクライアント証明書からのアクセスを拒否する。
- 業務面での対処としては、以下が挙げられる。
- クライアント証明書を組み込んだ PC の厳重管理。
- クライアント証明書を組み込んだ PC が盗難された場合の、クライアント証明書失効処理の明確化。
- 日常的な、クライアント証明書によるアクセス及び申請内容の確認。
- クライアント証明書を利用する PC の IP アドレス管理。
- 管理者のクライアント証明書に対して、責任を集中させることによる不正の抑止。(申請担当者の不正によるペナルティを、申請担当者の管理者も負わせることによる、指定事業者内での抑止効果を目的とする)

次に、提供業務の拡張に関する問題点と課題について検討する。6.4.6.5 において、IP アドレス割当申請業務について、メールによる申請を Web トランザクション化することによる申請業務の円滑化を図った。さらなる申請業務の円滑化を拡大することを目的とし、別の申請業務を Web トランザクション化する場合、各申請業務を実施可能な権限が問題となる。Web トランザクションを処理する指定事業者側 WWW サーバに組み込むクライアント証明書を、どの権限のメンテナーコードで発行するか、考慮する必要がある。

表 7-15　主な業務毎の処理実施可否について

主な業務名称	契約管理者	資源管理者	資源申請者
指定事業者 契約関連	○	×	×
資源管理情報関連	○	○	×
資源の割り振り 申請	×	×	○
資源の割り当て 報告	×	×	○

表 7-15 にて、権限によって可能な業務が分けられていることを示す。この場合、指定事業者 WWW サーバに組み込んでいるクライアント証明書のメンテナーの権限によっては、申請を受理できない。契約管理者の権限を持つメンテナーコードのクライアント証明書を使用すると、資源管理者や資源申請者が行う業務については、権限が合わず、申請ができない。(図 7-12 参照)

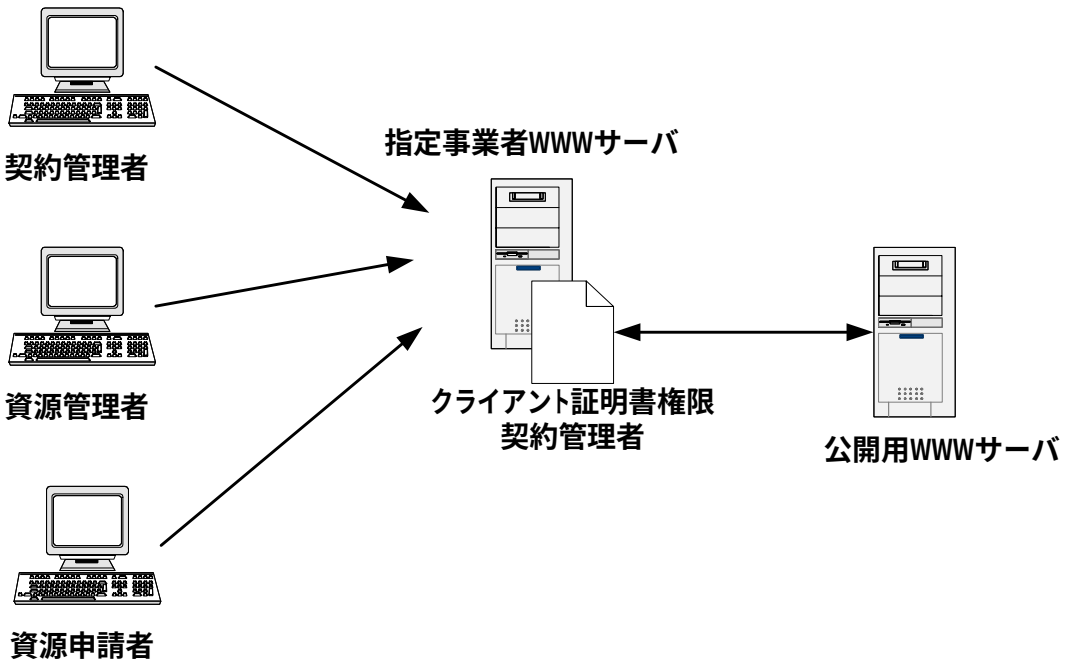

図 7-12　クライアント証明書の権限を共有した場合

よって、Web トランザクションで対応する申請業務を拡張する場合は、図 7-12 のように、申請業務を実施可能な権限毎に WWW サーバを分け、公開用 WWW サーバに申

請情報を POST するクライアントを分けることが考えられる。もしくは、クライアント証明書を、契約管理者用、資源管理者用、資源申請者用それぞれを WWW サーバに入れておき、申請内容によって、使用するクライアント証明書を分けることも考えられる。(図 7-13 参照)

ただしその場合でも、利用者から指定事業者 WWW サーバへの認証に、ユーザ ID とパスワードを使用する場合は、不正アクセスによる権限のなりすましが発生した場合、意図しないユーザからの申請が通ってしまうことが発生する。可能な限り、利用者と指定事業者 WWW サーバの間についても、クライアント証明書による認証を施すべきであると考える。

サーバ構成として単純にする場合は、使用するクライアント証明書毎に Web サーバを分離する方法も考えられる。(図 7-14 参照)

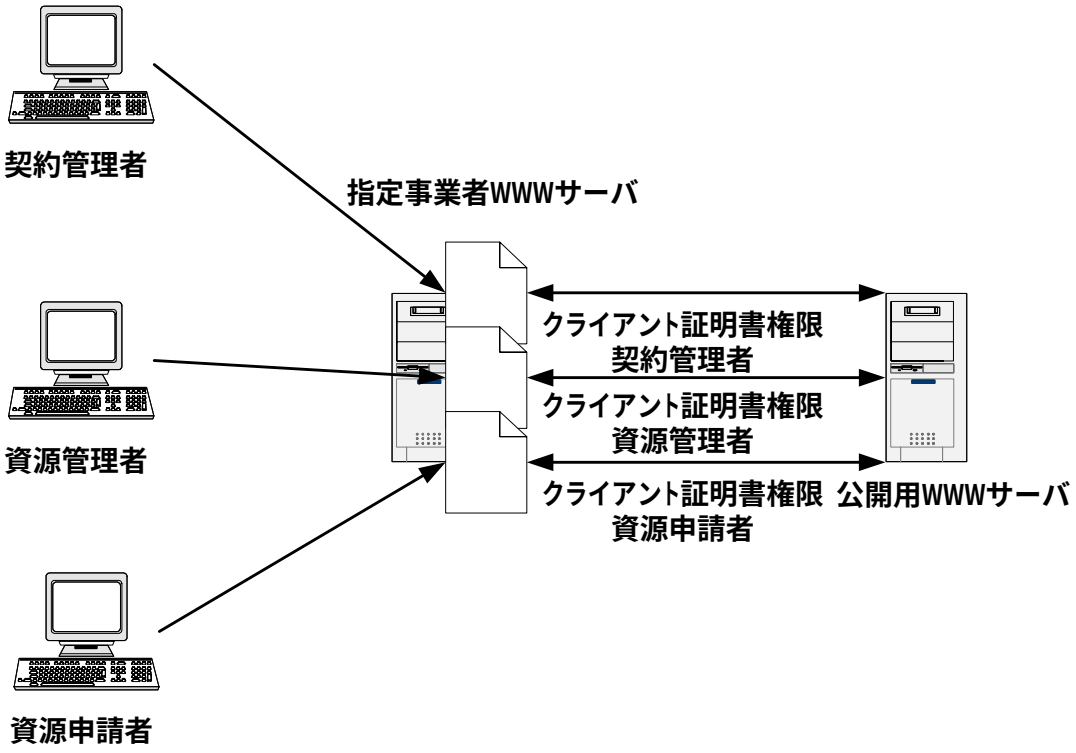

図 7-13　クライアント証明書の権限を分離する手段１

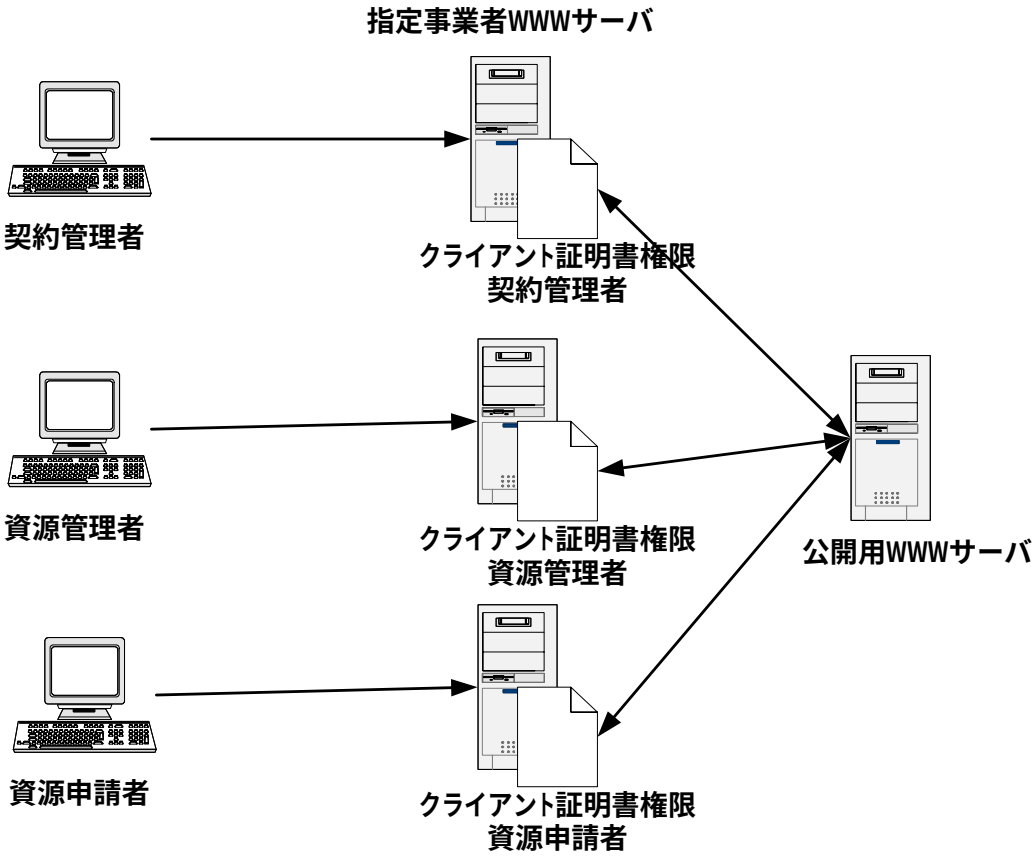

図 7-14　クライアント証明書の権限を分離する手段２

7.3. 商用 ENUM サービスの登録情報管理における適用事例

ENUM（tElephone NUmber Mapping）は、電話番号をインターネット上のアドレスやサービスと対応づけ、アクセスの手段として利用する仕組みである。日本でも 2003 年 9 月より、任意団体「ENUM トライアルジャパン」によって接続の実証実験が続けられている。

この ENUM について、2004 年 12 月にオーストリアが世界で最初の ”商用サービス” を生み出すことに成功した。ENUM はそのサービスの特性上、強固な本人認証がレジストリ・レジストラ業務の中で不可欠である。そのためオーストリアでは、認証局を通じて証明書を発行するモデルを実践している。ここでは、レジストリ(レジストラ)の行う登録管理業務の中で、実際にトークンを使用している事例として、このオーストリアの ENUM サービスの概略を紹介する。

7.3.1. ENUM とは

まず、ENUM の概略を述べる。

ENUM とは、電話番号を用いて、インターネット上のサービスで使われるアドレスを識別する仕組みである。まず、電話番号をドメイン名の形（e164.arpa）に変換し、それを DNS（Domain Name System）で、文字や数字そして特殊記号から成る通常のインターネットアドレス(メールアドレスや Web サイトの URL、SIP アドレス等)である相手の URI（Uniform Resource Identifiers）と対応づける。それによりその URI で指定されたアプリケーション、たとえば IP ネットワーク上の電話やメール、FAX などに接続することが可能となり、異なる通信サービスを 1 つの番号で利用することができる。

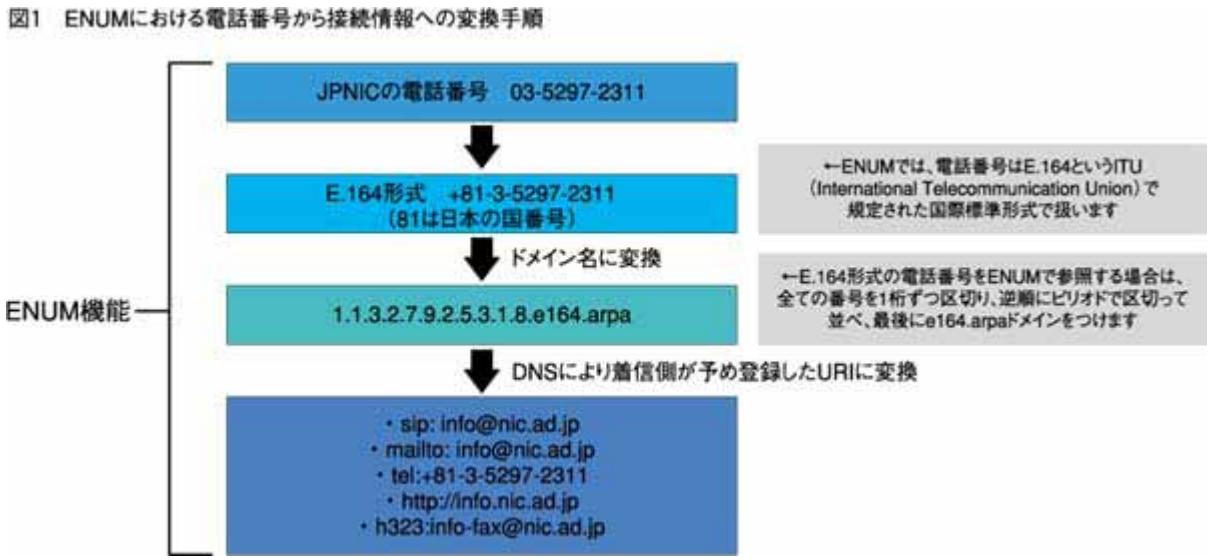

図 7-15　ENUM における電話番号から接続情報への変換手順

電話番号（E.164 番号）は、国際接続を考慮して、国際的な階層構造のもと管理されている。世界中でユニークであり、数字だけを用いていて各国の言語に依存していないという特性があるため、ENUM は世界に跨るグローバルなコミュニケーション構造の基礎としては大変高いポテンシャルを持っているといえる。

このような背景から、ENUM の実際に導入に向けて、国別でトライアルを進めるところが増えている。トライアル用のドメイン空間である「e164.arpa」は、IETF の IAB(Internet Architecture Board)からの委託を受け、RIPE NCC（Reseaux IP Europeens Network Coordination Centre）が管理運用を行っている。トライアルを行う際には、この Tier0 のレジストリである RIPE NCC に申請する必要がある。

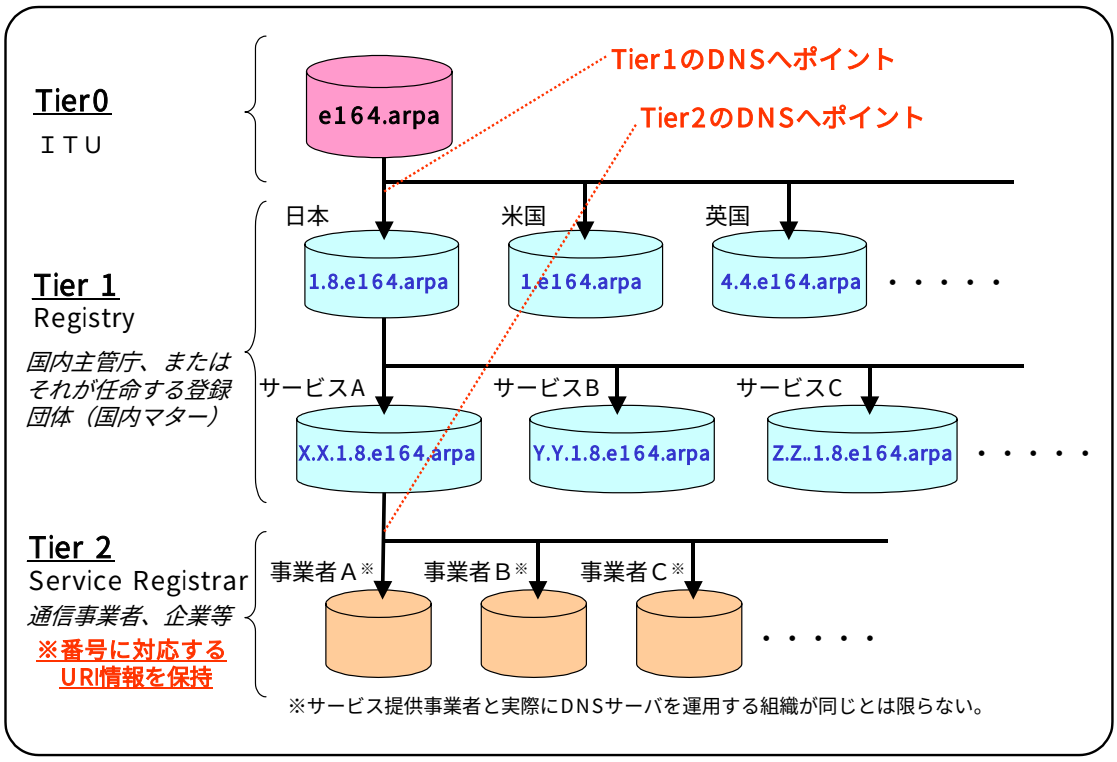

図 7-16　ENUM　DNS サーバの階層構造[1]

また、ENUM の導入に向けた技術の標準化に関しては、IETF（Internet Engineering Task Force）と ITU-T （International Telecommunication Union Telecommunication Standardization Sector ：国際電気通信連合の電気通信標準化部門）が共同で行っている。IETF は主に技術の標準化を行っており、ITU-T では管理基準の議論を行っている。

7.3.2. なぜ ENUM には強固な認証が必要か

ENUM は、存在する番号と適正な URI が結びついて初めてその機能を果たすものである。そのためには ENUM ドメイン名を登録申請した者が保持する電話番号が、本当にその人に属している(その人自身が使用している)という同一性を証明しなくてはならない。この定義ミスがあった場合、インターネットからの呼が ENUM を通じてルーティングされた際に適切でない人に接続されてしまう。そのため、ENUM ドメイン名の登録管理業務の中において、いかなる登録、変更、あるいは削除の作業の際に認証が不可欠となる。

1　総務省「IP ネットワーク技術に関する研究会 報告書」2002 年 2 月
http://www.soumu.go.jp/s-news/2002/020222_3.html
より抜粋

7.3.3. オーストリアでの商用 ENUM サービスの状況について

7.3.3.1. オーストリアでの ENUM 普及の背景と登録モデル

オーストリアは、1998 年の通信法改正により開放された通信市場をもち、欧州で最も競争力を備えた通信市場の一つとなっている。中・東欧市場を視野に入れてオーストリアをハブとして活動する企業が多いということ、また電気通信分野が完全に自由化されたことにより各種サービスが豊富になり、改善され、結果として料金が安くなったことが理由として挙げられる。こうした背景から、オーストリアでは携帯電話や DSL の普及率も非常に高く、これらの充実したインフラを利用しての利便性が高いアプリケーションが生まれる土壌が肥沃である。

ENUM については標準化団体の一つである ITU-T の本部に近いヨーロッパ地域でトライアルの準備が積極的に進められたという経緯もあり、RIPE NCC や ETSI(European Telecommunications Standards Institute：欧州通信規格協会)、CENTR (Council of European National Top Level Domain Registries)等の場を中心として ENUM の技術に関する議論や共同実験プロジェクトが盛んに行なわれたが、その中でアプリケーションに強いオーストリアは ENUM 先進国として ENUM に関するチュートリアルやトライアルを行い、また Asterisk[2]への ENUM 機能の実装もサポートにも積極的に取り組みに指導的な役割を果たしていた。RIPE　NCC からの受けるトライアル用ドメイン名空間のデリゲーション(3.4.e164.arpe)についても 2002 年 6 月と、世界で 4 番目という早さで取得している。

オーストリアで、この 3.4.e164.arpe についてのデリゲーションを受けて 3.4.e164.arpa ドメイン名ホルダーであり運用責任者となっているのは RTR 有限会社 (Rundfunk und Telekom Regulierungs-GmbH：放送テレコム規制有限会社) [3]である。nic.at(nic.at Internet Verwaltungs- und Betriebsgesellschaft m. b. H.：nic.at インターネット管理有限会社)[4] を始めとした関連組織を中心とした 2 年あまりのトライアル期間を経て、RTR は 2004 年 8 月 24 日に enum.at 有限会社[5]との間でレジストリ契約を

---

[2] Linux で動く、IP PBX ソフトウェアのこと

[3] 1997 年に設立のテレコム・コントロール有限会社(Telekom-Control GmbH)を統合して 2001 年 4 月 1 日に設立された通信産業の独立した規制機関。http://www.rtr.at/web.nsf 日本での規制当局。規制関連機関は、総務省と社団法人電波産業会である。

[4] オーストリアのトップレベルドメイン名".at"の登録管理業務を行う ccTLD レジストリ。

[5] 正式名称 enum.at 有限会社。http://www.enum.at/ 非営利財団 Internetprivatstiftung Austria (ipa：インターネット個人財団オーストリア)の 100%の子会社で、at、.co.at、.or.at

締結し、2007 年末まで Tier1 レジストリ業務を enum.at に委託、enum.at が 3.4.e164.arpa の ENUM ゾーンの管理を行う事となった。enum.at が行う事が可能である ENUM ドメイン名配布の範囲・条件などは RTR とのレジストリ契約で規定されている。enum.at は、ENUM ドメイン名の登録管理業務にかかる申請(登録・変更・削除)の手順等を決め、レジストラインターフェースを作成し、国の ENUM-TLD の下にゾーンのネームサーバを運用することが主な業務となる。この enum.at のもと、商用サービスの ENUM ドメインの登録は、2004 年 12 月 6 日から可能となり、トライアルからの転換は、2004 年 12 月 9 日の 12 時に実施された。

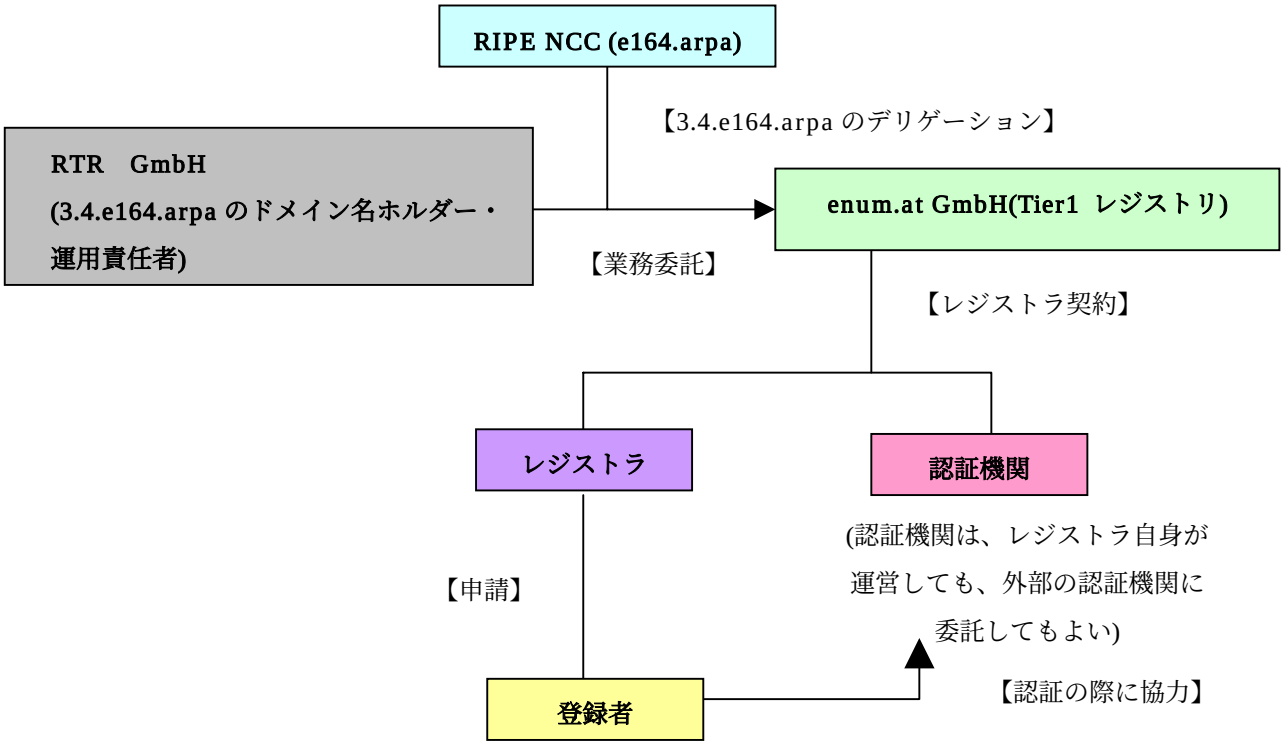

図 7-17　オーストリア ENUM の管理構造

等オーストリアのドメイン名の登録管理に責任を負うレジストリである nic.at の関連会社である。nic.at のマネージャでもある Robert Schischka が、enum.at の管理を引き継いでいる。

7.3.3.2. 各機関の役割と契約関係について

関連プレイヤーとの契約関係を、以下に図示し、整理する。[6]

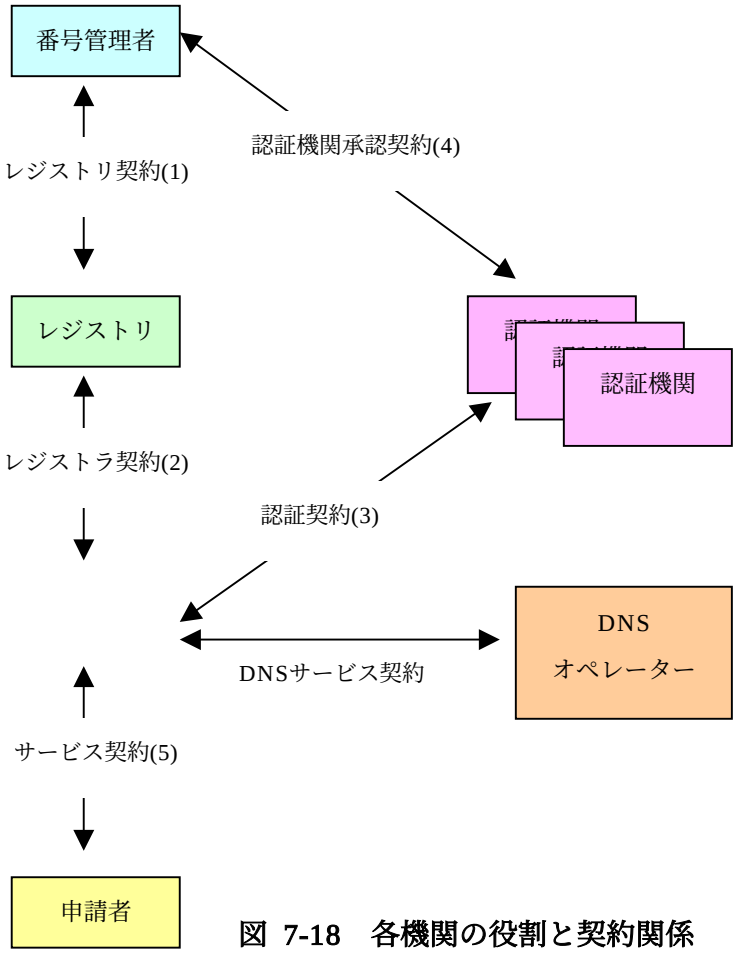

図 7-18　各機関の役割と契約関係

(1) レジストリはレジストリオペレーションについて番号管理者との契約を締結する。

(2) 各レジストラは、番号を割り当てることができるレジストリとレジストラ契約を締結する。

(3) 各レジストラは、レジストラのための認証トークンの作成にあたっては少なくとも最低一つの認証機関と認証契約を締結する。レジストラは、認証機関といかなる契約も存在しない場合においては、組織内の認証機関を利用することも

[6] 「ENUM Registry system specification」８ページより

できる。

(4) 各認証機関は、確認ポリシーについて番号管理者との契約を持つ、それに基づいて処理する。

(5) 各レジストラは、顧客(申請者)の代理で申請する事について申請者との間でサービス契約を締結している。

(6) 申請者に番号割り当てサービスをしようとする各レジストラは、番号範囲ホルダーとの契約を締結する。(オーストリア:+43 780番号)

以上がプレーヤー間の契約であるが、それにより以下の2点が明らかになる事を特記したい。

(7) レジストリには、申請者と締結するいかなる契約もない

(8) レジストリには認証機関と締結する契約はない(レジストリ⇔番号管理者⇔認証機関　のラインとなる)

但し、これに加え、例えば「+43 780」(後述するENUM専用番号)の登録の際にはこれ以外の他の契約関係も加わるかもしれないとされている。

また「レジストラ契約」を結ぼうとする ENUM 登録のレジストラ要件については、下記が課せられている。

(1) enum.atとレジストラ契約を締結する必要あり

(2) 申請者の委任を受けて登録等の申請を行う

(3) レジストラは、番号認証の責任を持つ。この場合、認証機関についてはレジストラ自身で運営しても、外部の認証機関に委託してもよい。が、

(4) 認証方法については enum.at の承認を得なければならず、また、enum.atに対する責任はいかなる場合もレジストラが持つ

また、enum.at と結ぶレジストラ契約では主として下記が規定されている。

(1) 営業規則を持っていること

(2) 従業員教育をすること

(3) EPP[7]登録とホスティングについての技術的基盤を有すること

(4) 銀行口座を有すること

(5) 申請者の意思がたえず優先されること

(6) 瑕疵のあるデリゲーションを行った場合、デリゲーションや番号空間利用の一時停止や禁止を行うことがある

2005 年 3 月現在、このレジストラ契約を締結しているレジストラはインスブリュックに本拠地を置く SI である nemox.net Steiner und Würtenberger OEG[8]、nic.at GmbH、ウイーンの ISP である Silver Server GmbH[9]の 3 社となっている。なお、nemox.net Steiner und Würtenberger OEG については、オーストリアで始めての ENUM レジストラであると同時に、認証局の役割も持っており、nic.at と認証契約を締結し認証業務を請け負っている。

また、認証機関については下記が要件とされている。[10]

(1) 認証情報は、鍵つきの証明書(Token)でやりとりすること

(2) 認証方法を開示すること

(3) 定められた番号空間の認証のみを行うこと

(4) 全てのレジストラにサービスを提供することも出来る

尚、申請者(ENUM 利用者)は、番号の適正使用のために、認証の際には認証機関に協力することとされている

---

[7] Extensible Provisioning Protocol の略で RFC3730 に規定されているレジストリデータの登録・更新のためのプロトコル。ドメイン名レジストリは複数のレジストラに対して、自組織データベースにアクセスさせなければならなく、また、単一のレジストラから複数のレジストリへのアクセス要求も出てきた中、 ドメイン名レジストリ・レジストラ間通信のためのプロトコルとして Network Solutions 社（現在は VeriSign 社に買収されている）によって開発された NSI RRP が存在したが、これでは登録者情報のやりとりはできなかったためそれに替わるものとして EPP が開発された。

[8] nemox.net Steiner und Würtenberger OEG　http://nemox.net/index.html

[9] Silver Server GmbH　http://www.sil.at/

[10] 詳細については、enum.at が発行している認証についての考え方ガイドライン「Identifizierung und Validierung für ENUM IN ÖSTERREICH」がある
http://enum.nic.at/documents/AETP/Permanent_Documents/Drafts/0032-ENUM_Validierung_v_1.0.doc

7.3.4. ENUM に登録出来る番号空間について

ENUM に登録出来る番号空間は下記のとおりであり、それ以外の番号空間の登録は基本的に不可となっている。

(1) 地域別番号

(2) プライベート網用番号(05)

(3) モバイル用番号(06)

(4) 地域に左右されない固定網(0720)

(5) ENUM用番号(0780)

(6) フリーダイアル用番号(0800)

(5)の ENUM 用の番号空間である「0780」は、RTR が ENUM を利用したコンバージェントサービスのために導入した空間であり、この空間下では申請者はその番号が誰にも割り当てられていない場合には好きな番号を選ぶことができる。つまり、ENUM 用の番号である 0780 以外の空間では、その電話番号の存在が適切に認証されて初めて ENUM ドメインが割り当てられるが、0780 に関しては、番号と ENUM ドメイン名を同時に割り当てるという形式をとる。0780 の登録は、通常のドメイン名の登録手順・方法に非常に似ている。但し、デリゲーションには期限が存在する。

7.3.4.1. 課金体系

レジストラへの課金は、その時点でデリゲーションされているドメイン名の数をベースに月ごとに計算する事となる。500 ドメイン名までは、250 ユーロ/月が最低課金料金[11]で、それ以上は、数に応じた表の単価を、数にかけた料金(ドメイン数×単価)としている。

[11] 但し、契約して最初の半年は、最低課金料金(250 ユーロ)の 50%引きを実施

ドメイン数	1 ドメイン辺りの値段(ユーロ/1 ヶ月辺り)
0 -　 500	0,5　ユーロ
501 -　2500	0,45 ユーロ
2501 - 10000	0,4　ユーロ
10001 - 50000	0,35 ユーロ
＞50000	0,25 ユーロ

表 7-16 レジストラへの課金

例:　392 ドメインの場合　→　500 ×　0,5 ユーロ = 250 ユーロ(1 ヶ月辺り)
4612 ドメインの場合　→　500 × 0,5 ユーロ + 2000 x 0,45 ユーロ + 2112 ×　　0,4 ユーロ = 1994,8 ユーロ(1 ヶ月辺り)　となる。

7.3.5. ENUM レジストリシステムの要求事項について

enum.at が、2005 年 1 月 3 日に Ver1.1 を発行した「ENUM Registry system specification」を元に、このレジストリシステムの要求事項と登録手順を述べる。

7.3.5.1. 登録手順について

どの番号空間の利用するかによって、登録手順は多少異なってくるが、ここでは、代表的な例として、地理的識別要素をもった電話番号についての登録手順についての概要を述べる。[12]

[12] 「ENUM Registry system specification」13 ページ～16 ページより
なお、ENUM 専用番号 0780 については 9～12 ページに、SMS を利用した携帯用の番号については 16～17 ページに記載されている。

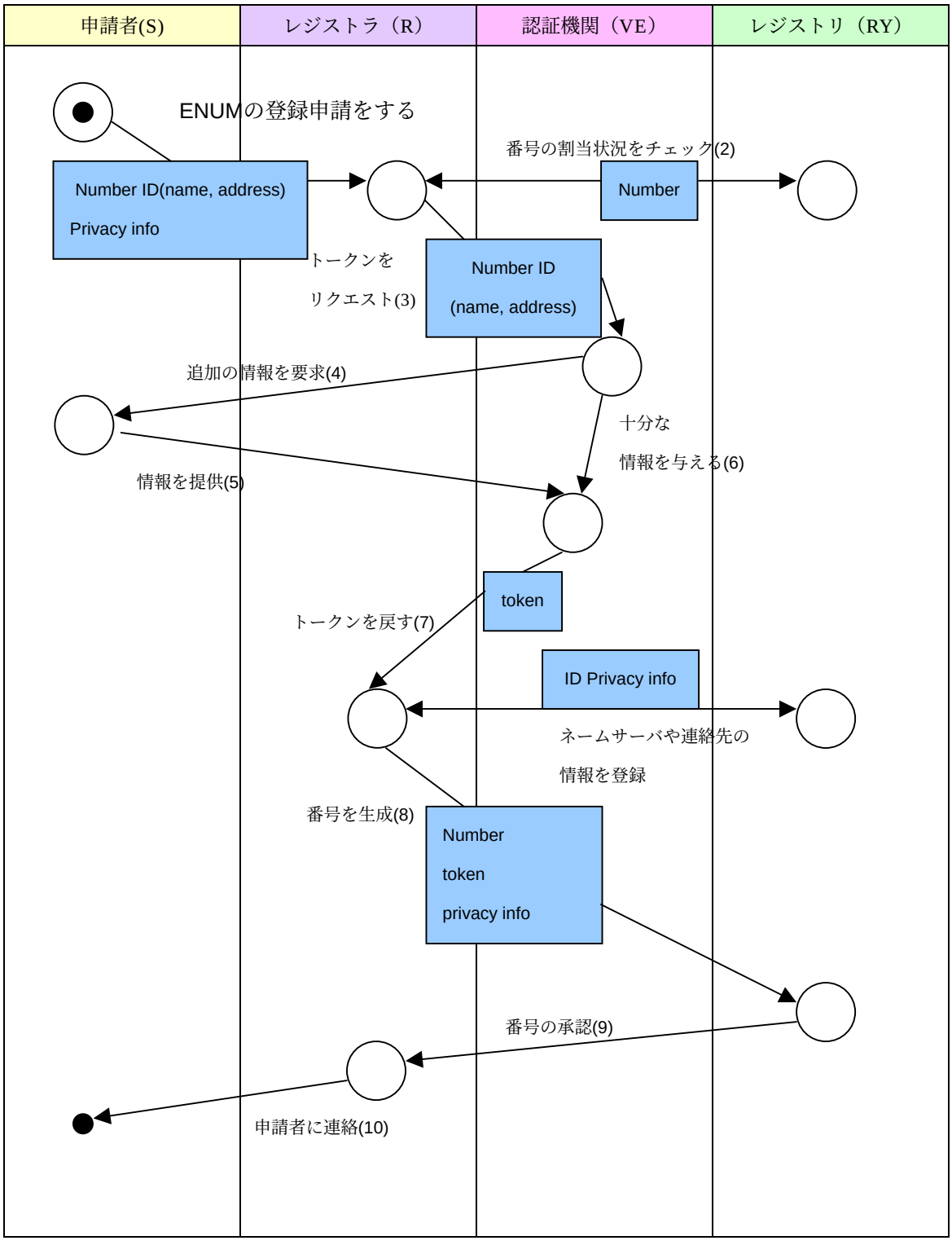

図 7-19　地理的識別要素をもった電話番号についての登録手順

(1)現存する地理的識別性を持った番号のためのENUM 申請者(S)は、レジストラ（R）にサービスを申請する。申請者は申請者認証に必要な情報を提供する

S -> R: Name: Joe User

S -> R: Address: Karlsplatz 1/9, A-1010 Wien

S -> R: Number: +43 1 234234

S -> R: email: joe.user@nic.at

S -> R: validation information (請求書のコピー, IDのコピー等)

(2)レジストラ（R）はレジストリ（RY）と共にその番号がENUMですでに割り当てられていないかどうかをチェックする(万一そのようなことがあれば、CREATENUMBER(番号作成申請)でなくTRANSFERNUMBER(番号移転申請)をしてもらうよう申請者と交渉する必要があるため)。このチェックは、問題の番号がそもそも有効かどうか、ログイン画面の将来のバージョンでは確認する事ができるようになる予定である。

R -> RY: +43 1 234234 available?

RY -> R: +43 1 234234 NOTFOUND – no number resource found

(3)レジストラ（R）は認証機関(VE)を選びその認証機関が必要とする情報を手渡す。この情報にはその認証機関の認証ポリシーに従った文書も含まれる事とする。

R -> VE: number: +43 1 234234

R -> VE: numberholder: Joe User, Karsplatz 1/9, A-1010 Wien

R -> VE: email: joe.user@nic.at

(4)認証機関(VE)は、申請者(S)に追加情報を要求したり、あるいは確認することが可能である。例えば申請とされる電話番号についての最も最近の請求書のコピーを V 申請者に送って欲しいと頼むというようなことである。

VE -> S: email: please fax invoice for +43 1 234234

(1) 申請者(S)は認証機関(VE)からの要求事項に応える。

S -> VE: receives email, faxes invoice

(2) 上記の 4.や 5.の手続きの際、レジストラ（R）が認証機関（VE）に対して認証に必要とされる十分な情報を提供した場合においては、認証機関が

申請者（S）に直接コンタクトすることなくして認証が終了する事もある。(例えばレジストラが電話番号の最新の請求書のコピーを認証機関に提供した場合など)。

(3) 上記の通り認証が成功したら、認証機関がサインした Token をレジストラに返す。

VE -> R: valid, signed token, containing:
VE -> R: number: +43 1 234234
VE -> R: firstname: Joe
VE -> R: lastname: User
VE -> R: creation date: 2004-06-21
VE -> R: expiration data: 2004-12-21

(4) レジストラは、申請者が例えば電話帳ディレクトリのために提供するようなデータのサブセットを含んだ新しいコンタクト・オブジェクトの作成をレジストリに依頼しレジストリはをれを作成する。[13]

R -> RY: CREATECONTACT
R -> RY: type=person
R -> RY: firstname: Joe
R -> RY: lastname: User
R -> RY: email: joe.user@nic.at
RY -> R: contact successfully created, new roid „JU1234“

(5) レジストラは、たった今作成された番号保持者のコンタクトオブジェクトを参照して、番号を割り当てる。コマンドには認証機関から受け取った認証トークンが含まれる。

R -> RY: CREATENUMBER
R -> RY: number: +43 1 234234
R -> RY: numberholder: JU1234
R -> RY: nameserverset: NSSET1234
R -> RY: token: ...
RY -> R: create number OK

(6) レジストラは、申請者に ENUM ドメインの登録が終了した事を伝える。

[13] nameserverset（必要なら)の作成はここでは示されていないが、コンタクトを作成した際の前後になると考えられている。

申請者は、構成データ等を受け取ることもある。

R -> S: Ok, ENUM domain created, here's your account information

R -> S: And now, hand us over your money.

7.3.5.2. レジストリシステムインターフェース

レジストリとの連携のためには、次の図のように、インターフェースが提供されている。[14]

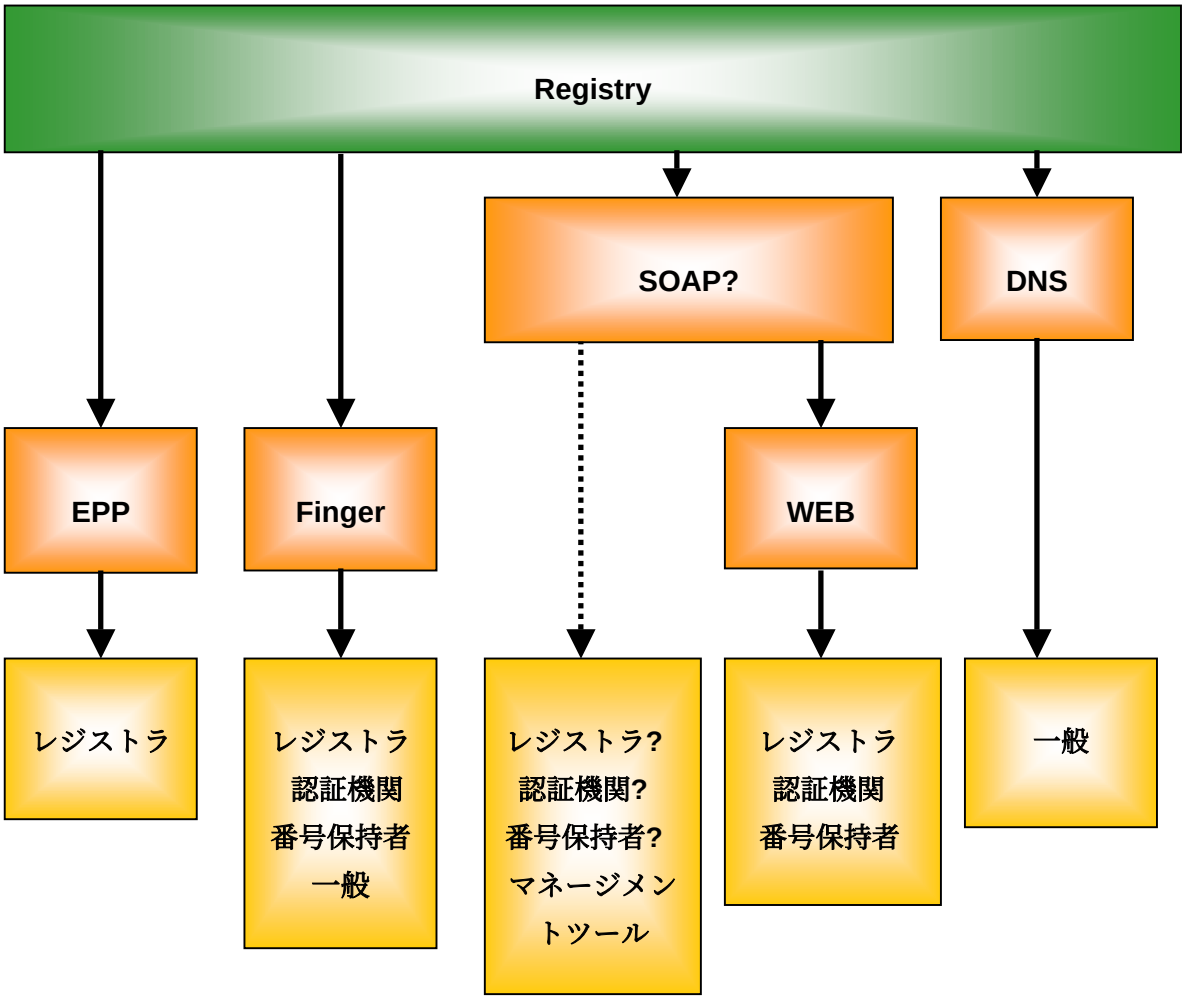

図 7-20　レジストリシステムインターフェース

[14] 図 7-20 の中の DNS のインターフェースは、パブリック ENUM ツリーが管理される場合にのみ適用される。プライベート/キャリア ENUM アプリケーションで、DNS へのアクセスは、あるクライアントに制限されたり、もしくはいかなる DNS も、そもそも使われない可能性もある。

7.3.5.3. サーバポリシー15

ここでは、あるトランザクションが成功したのかそうでないのかを定義するレジストリサーバに適用するルールである、ENUM管理サーバのポリシーについて述べる。但し、ポリシーは、ある処理で運ばれるデータやレジストリ・データベースの状況に依存しているため、時とともに変わる可能性があるものである。

（1） 権限の定義

トランザクションは、サーバによって許される場合と許されない場合があるが、一つのトランザクションを有効に進めるには、真正性を証明されたクライアントによって、以下にあげる許可がされる必要がある。また許可に加えて、処理にはすべてのポリシーがクリアされている事が必要とされる。

(1) クライアントに対して許されるトランザクションのタイプ　：
クライアント(レジストラ)は、問題の処理を許されなくてはいけない。それは、クライアントトランザクションタイプを制限するのに有用である(例えば不払いの場合の新しい番号は付与しない)
(2) クライアントに対して許される番号の種類　：
クライアントは、ある種類の番号だけに制限されることがある。例えば、モバイル・オペレーターは、モバイル番号だけの割り当てを許される。これは非番号トランザクションには適用されない。
(3) 認証機関に対して許される番号の種類　：
認証機関は、自分達が取り扱っている種類の番号のみを扱う事ができる。その種の彼(それ)らが出す番号で制限することができる。モバイル・オペレーターは、例えばモバイル番号だけの認証を許される。
(4) トークン証明書に対して許されるトランザクションタイプ　：
トークンにサインするために使われた証明書は、トークンをサポートするトランザクションのサブセットに制限されていることができる。
(CREATENUMBER、RENEWNUMBER、TRANSFERNUMBER)

（2） ポリシーの依存関係

ポリシーは、以下のものに依存するとされ、ポリシーを通した、ある処理の流れは、

15 「ENUM Registry system specification」63 ページ～64 ページより

次の図の通りとなる。

(1) 番号(番号型エンジン経由で番号から抽出された)の種類

(2) レジストラID

(3) 認証機関

(4) 処理型

(5) オブジェクト(フラグ)の状態

(6) リンクされたり関係付けられたオブジェクトの状態(およびそれらのフラグ)

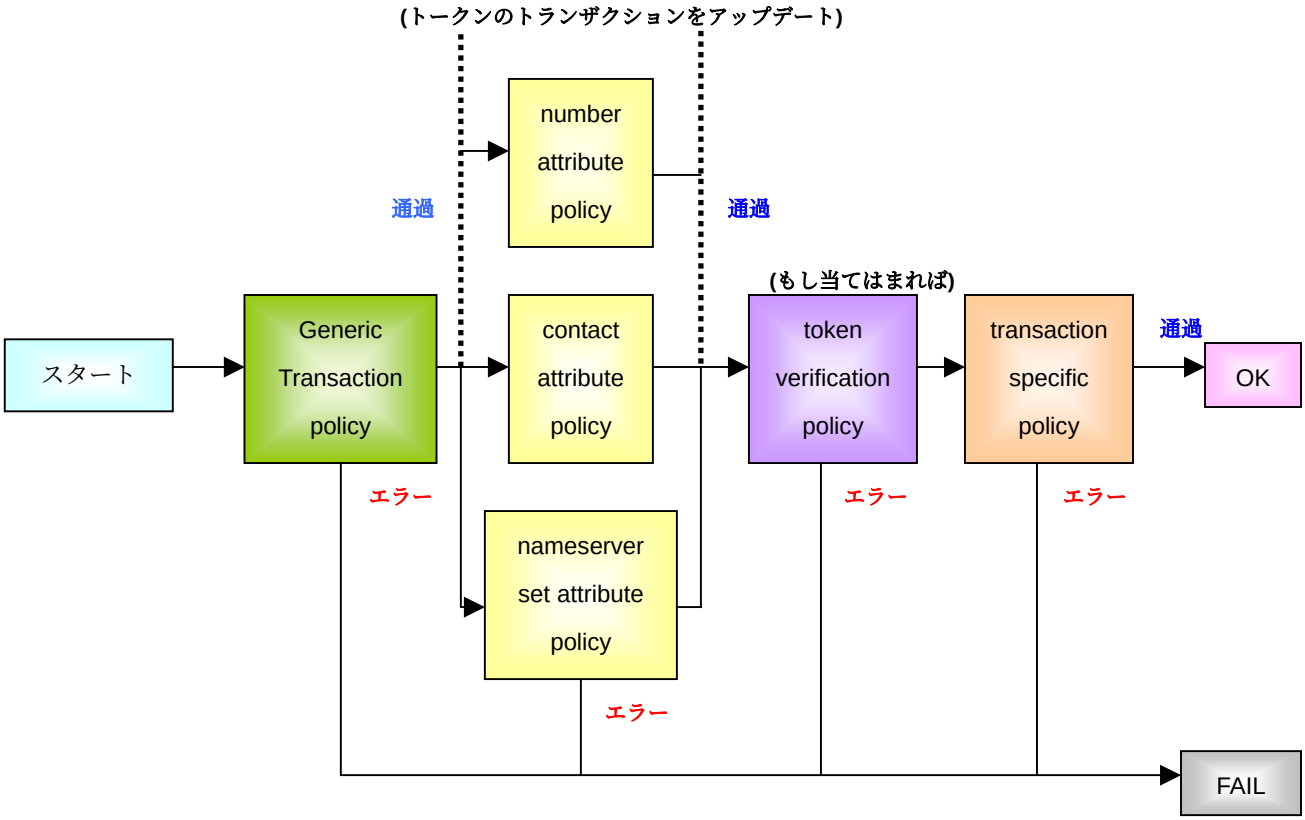

図 7-21　ポリシーの関係

7.3.5.4. 認証[16]

認証のプロセスは、ENUM 登録インフラの基礎的な概念だ。ある番号の認証をするということは、ENUM ドメインの保持者がその番号保持者と完全に一致することを明らかにするということである。これは ENUM 経由の通信が、PSTN(Public Switched Telephone Networks：公衆交換電話網)経由でルーティングされた通信と同じエンティティに届くということを確実にする必要があるということでもある。

何度も述べているが、認証の手順に関しては、特別の役割である「認証機関」のみが実行することができるものである。認証機関はレジストラに対して、あるトランザクションは番号保持者によってオーソライズされたので進める事ができると主張することができる。

ENUM で使われる認証の種類には、まず「最初の認証」と「再認証」の二つがあるが、ここでは「最初の認証」のやり方と考え方について述べる。

「最初の認証」では、一つの番号があるレジストラと認証機関の組み合わせによって割り当てられるということが要求される。または、以前に有効とされた番号が、再割り当てられることも要求される。従って、最初の認証では、以下 3 つのプロセスが必要となる。

(1) 「デリゲーションにあたり番号保持者の同意を確かめる」
これには二つの方法がある。

(a)本人確認→使用権の確認→その後権限付与・・・利便性とセキュリティの間のトレードオフに応じて、これらの3つの要素(三ステップ)がENUM申請手続きの際に組み込まれることが必要となる。

I：Authentication(本人確認) :
このステップは、カスタマーの同一性を確立する。ENUMユーザとなる人の住所と名前を確認する。これには、例えばIDカードやクレジットカードあるいは他の暗号のトークン等を使って行われる。
Ⅱ：Right-to-Use(使用権の確認)　:
第2のステップとして、その番号とその人に関係があることを確認する。

16 「ENUM Registry system specification」67 ページ～72 ページより

これは例えば電話帳を検索したり、請求書のコピーなどを使って行われる。
Ⅲ：Authorization(権限付与)　：
最終のステップは、このレジストラから付与されるENUMドメイン名を、本当に申請者が欲しているかを確かめる事だ。

(b)番号ホルダーによる直接承認・・・時には、番号ホルダーを識別することのプロセスを飛ばすことは、可能である。例えば、SMSハンドシェイクが認証リクエストを承認した場合には、認証機関はその携帯電話の所有者の同一性を確認することを必要としない。

(2) トークンを生成

上記(1)のプロセスが終了したらトークンが生成される。トークンには、選ばれた認証方法に応じて要求されたデータは少なくとも含まれなくてはいけない。トークンにいれられたデータは、番号保持者について追加で調べられたデータなしでも再認証を許される。

(3) トークンにサイン

トークンは、認証機関がレジストリに渡し、そしてそれは、対象のトランザクションおよび種類の番号の参加資格を得る証明書でサインされる必要がある。

7.3.5.5. 証明書管理について

いままでで記述された認証の仕組みの中では、証明書管理プロセスも要求している。証明書管理は、認証トークン(認証機関)の署名者と署名(レジストリ)を確かめる組織の間で必要となるものである。

レジストリは、それぞれの認証機関の証明書リストを管理する。認証機関は「アウトオブバンド」プロセス経由でこのリストに証明書を追加したり削除したりする可能性がある。レジストリは、例えばパブリックCA、プライベートCA、自己サイン証明書等々どんな形式であろうと認証機関が発行した証明書が有効でサインされたX.509証明書だ

という条件で受け取ることとなっている。

ある認証機関の現在有効な証明書のリストは、認証トークンの検証のために有効と見なされる。検証に利用される証明書は、検証プロセスの際には有効でなくてはいけないとされる。

また、認証機関は、特定のトランザクションにおいてトークンの正当性を制限するかもしれないとされている。制限はトークンがサインされた証明書に基づき、ある証明書の制限は、証明書がレジストリによってインストールされるときに、伝えられる必要がある。認証機関は、証明書をCREATENUMER・RENEWNUMBER・TRANSFERNUMBERの1つ以上の処理に制限することもある。

ある証明書の制限というものは変えることができない。認証機関は、追加の証明書を多かれ少なかれトークンが望まれるときに提供する必要がある。制限の目的において、例えばちょうど + 43780番号の作成のため等に、ライトウエイトな認証機関を運営する事ができる。また一つの認証機関は、この数種の番号のためのトークンだけを作る事ができると、制限される事がある。

7.3.5.6. 汎用的なトークン検証プロセス

レジストリによって受け取られたいくらかのトークンは、以下のトークン検証プロセスをパスしなくてはいけない。汎用的なトークンへの検証への追加の要求は、トークンを含む処理・リクエストに依存することを適用するかもしれない。処理詳細ポリシーは、これでより多くの詳細を含む。汎用的トークン検証をパスするために、トークンは、以下の要求を果たさなくてはいけない。

(1) トークンは、書式が正しくなくてはいけない。(分解して解釈できること「paseable」)

(2) トークンのシグネチャは、含まれた証明書に対して有効にしなくてはいけない。

(3) 含まれた証明書は、レジストリのアクティブな証明書のデータベースの中で見つけられなくてはいけない。

(4) 証明書の使い方の制約がトークンを含む処理を許さなくてはいけない

(5) レジストリ・データベースで見つけられた証明書に連合させられた認証機関ID(VE-ID)は、トークンの認証機関ID(VE-ID)の属性につり合わなくてはいけない。

(6) トークンに含まれる番号は、レジストリに知られている番号の一種に地図にマップされなくてはいけない。

(7) 証明書に関連付けられた認証機関ID(VE-ID)は、番号種類のトークンを作り出すことが許される。

(8) トークンの有効期限のタイムスタンプは、それが処理されている時以降でなければならない。

(9) トークンの作られたタイムスタンプは、有効期限のあとであってはならない。

(10) トークンの認証機関ID(VE-ID)との認証シリアルは、レジストリ・データベースでユユニークでなくてはいけない。

7.3.6. まとめ

これまでに述べたとおり、オーストリアではじまったこの商用 ENUM サービスの登録情報管理では、(1)レジストリと独立した認証局を運営していること、(2)「レジストリ‐レジストラ‐認証機関‐申請者」で業務のフローを定義していること、(3)認証局と独立したレジストリが、認証のためにトークンを利用している事などが特徴として挙げられる。

(1)のレジストリと独立した認証局の運営により、レジストリにおける認証業務のコストを下げることだけでなく、既存の認証局の参入を可能にするモデルであると考えられる。(2)では単に認証局を利用した認証を実現するだけでなく登録のスキームを定義し、その中で認証機関が果たす役割を定義している。(1)と(2)を可能にする為に仕組みが(3)のトークンであろう。トークンは電子証明書ではなく、署名つきの認証子の意味で、電子証明書を使った相手の認証だけでなく、登録できる番号の種類といった付随する情報を持っている。

この応用は EPP とトークンの技術によってレジストリにおける認証の実現した事例である。レジストリ・レジストラ間およびレジストリ間の連携のプロトコルが開発され普及するに従って、この事例のような応用例が今後も現れてくる状況になると考えられる。インターネットレジストリの場合には whois に置き換わる CRISP の開発により認証スキームを新たに定義し、実現していく必要性が現れると考えられる。

7.4. 認証局の応用と IP アドレス認証局の役割

IP アドレス認証局は、JPNIC ルート認証局のサブ CA として、IP アドレス認証局（認証）と IP アドレス認証局（証明）の二つの種類を持つとして構築を行った。前者の IP アドレス認証局（認証）はメンテナー認証局とも呼ばれ、アドレス資源管理に関わる情報登録を行う者の認証を行うことを目的とした認証局である。後者の IP アドレス認証局（証明）は相互領域認証局とも呼ばれ、登録情報の内容に基づいた証明書の発行により証明書の利用者が相互認証を行えるような状況を目標とする認証局である。

様々なネットワークサービスやインフラとしてのインターネットを支える要素として電子認証を考えると、IP アドレス認証局（証明）は応用性が広いと考えられる。本章で述べる経路情報の安全性の向上に当たっては、IP アドレス認証局（証明）が利用されることが想定できる。一方、ネットワークサービスのアドレス資源管理の多様化に伴って安全性や効率性の向上を図る要素として電子認証を考えると、IP アドレス認証局（認証）が利用されることが想定できる。本章で紹介する Web トランザクションや ENUM の事例はこれに分類されるであろう。

このように IP アドレス認証局は、それぞれの認証業務にあわせて細分化され、役割を持っていくことが考えられる。特に IP アドレス認証局（証明）は、更に下位認証局を持つ等して、様々な電子認証のテストベッドとして活用され、本章で述べた以外の応用についても検討されていくことが考えられる。