第5章 レジストリシステムにおける認証システム

内容

- レジストリシステムにおける認証機能
  - レジストリシステムの構成
  - 情報モデルとセキュリティモデル
  - PKI を用いた認証機能
  - レジストリデータベースの応用

5. レジストリシステムにおける認証システム

ネットワーク資源の割り振り及び割り当ての情報は、インターネットレジストリの「レジストリシステム」とよばれるシステムで管理される。レジストリシステムは、ネットワーク資源だけでなくインターネットレジストリがネットワーク利用者の登録情報も管理している。インターネットにおける正しい資源利用の信頼性を向上させるためには、レジストリシステムにおける登録情報（レジストリデータ）の確実な扱いが必要になる。

本章では、レジストリシステムにおけるレジストリデータの確実な取り扱いのために、既存のレジストリシステムにどのような機能を持たせるべきかについて述べる。レジストリデータの信頼性はレジストリシステムの認証機能と、インターネットのような分散環境で信頼性を検証する機能の二つで実現される。従って本章ではレジストリシステムだけでなく、信頼性を検証するユーザ環境についても述べる。更にこれらの機能を利用することで実現可能な応用方法について述べる。

5.1. NIR におけるレジストリシステム

NIR は国別のインターネットレジストリであるため、ネットワーク資源の割り振り及び割り当ては当該国に存在するネットワーク利用組織を対象にして行われる。日本の NIR である JPNIC は、ネットワーク資源を割り振った組織の情報を日本における存在証明書類に基づいて確認する。この登録情報はネットワーク資源の管理のために使用される。またネットワーク利用組織の情報は運用上に必要となる相互の連絡などに使われるため、一部が公開される。

JPNIC における、レジストリシステムとそれに関わる組織の概要を図 30 に示す。

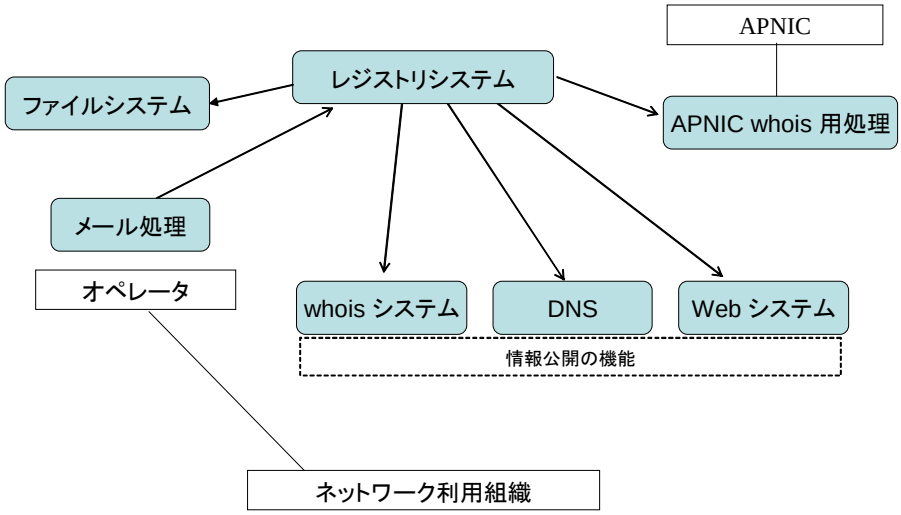

図 30　レジストリシステムに関わる組織とシステム

JPNIC はネットワーク資源の割り当て及び割り振りと同時に、ネットワーク利用組織をレジストリデータベースに登録する。登録情報は、ネットワーク利用組織から電子メールを通じて送られ、オペレーターが対応する。レジストリシステムに入力された登録情報の一部は whois システムなど情報公開の機能をを使って公開され、ネットワークの運用やネットワーク利用組織の相互の連絡等に用いられる。

5.2. レジストリシステムの構成

JPNIC で管理されるネットワーク資源は IP アドレスと AS 番号である。AS 番号は「IRR（Internet Routing Registry)」とよばれるシステムでも管理されているが、これはネットワークの運用の為の情報共有が主な目的であり、ネットワーク資源の管理が目的ではない。

本研究ではネットワーク資源、特に IP アドレスの割り当ての確実性に注目するため、IP レジストリシステムに注目する。IP レジストリシステムの概要を図 31 に示す。

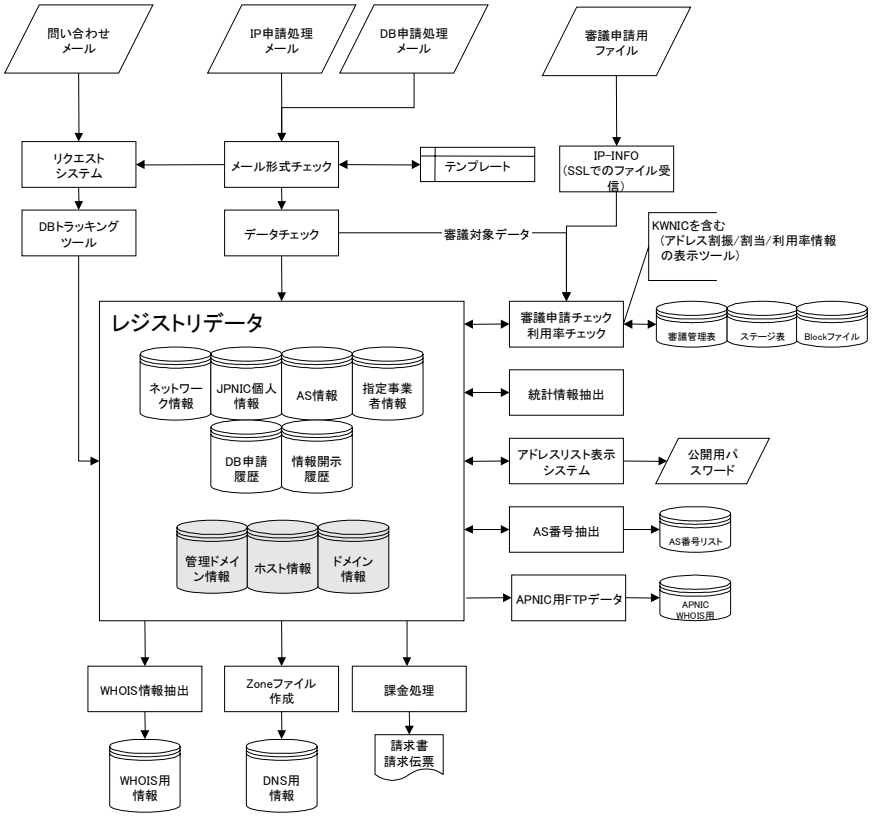

図 31　IP レジストリステム概要図

IP レジストリシステムの主要な処理は中央の四角で囲われたレジストリデータの扱いである。多くの RIR では、whois システムが、レジストリシステムとは別のシステムに位置付けられているが、ここでは後に述べるメッセージ認証機能を考慮するためレジストリシステムの情報公開機能に位置付ける。

IP アドレスの割り振りを受ける LIR（ネットワークサービスプロバイダー等）は電子メールを利用して IP アドレスのアドレスブロックの操作（新規割り振り、サイズの変更）を申請する。レジストリシステムはこのメールを処理し、ホストマスターの審議結果に基づいて情報登録等を行う。登録情報が格納されるデータベースは「レジストリデータベース」とよばれる。

5.3. whois システム

whois システムは登録情報のうち、ネットワーク組織のネットワーク管理者が相互に連絡を取り合うための情報を公開するシステムである（図 32）。1.4.3 節ではこの機能

を「登録情報の提供」として述べた。

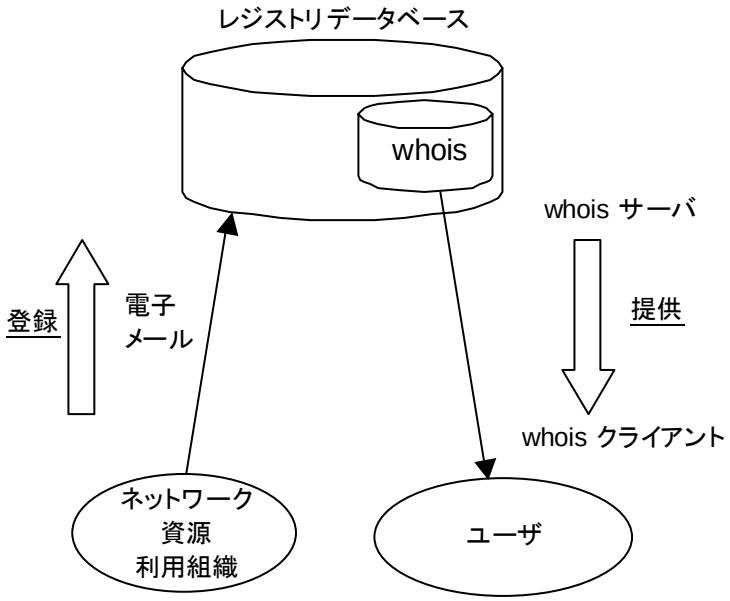

図 32　whois システム

ネットワーク資源を利用する組織が、情報を登録し、その情報を whois システムが提供することで、ネットワーク利用組織の相互連絡の手段を提供している。whois システムは、サーバ-クライアント方式で通信を行うシステムで、ユーザはサーバに格納された情報を検索し、閲覧する。whois システムの構成を図 33 に示す。

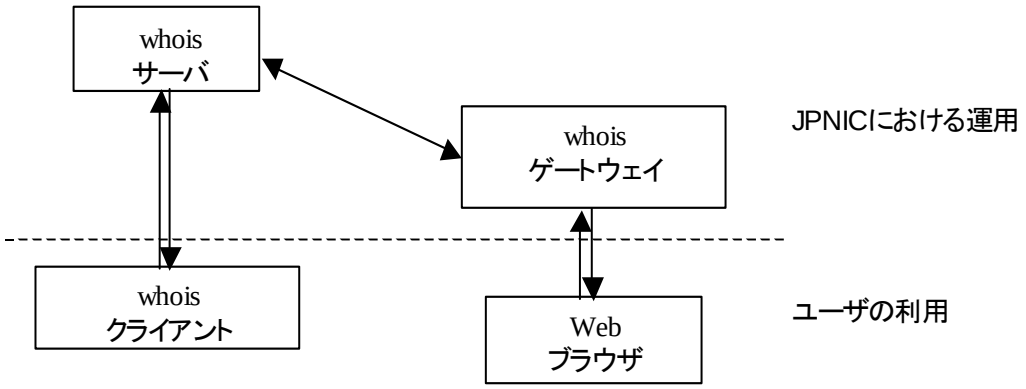

図 33　whois システムの構成

whois システムは、JPNIC における whois サーバとユーザが利用する whois クライアントで構成される。whois サーバは whois ゲートウェイを通じて利用することもできる。

whois システムは、扱われるデータがテキストのみであり、また GUI(Graphical User Interface）の開発環境が現在ほど一般的になっていない時代に開発されたため、多くのクライアントプログラムは CUI（Character User Interface）である。しかし JPNIC では WWW（World Wide Web）インターフェースを提供しており、ユーザは Web ブラウザを使って whois のデータを検索することができる(図 34)。なおこのような Web インターフェースは他の多くのインターネットレジストリでも提供されている。

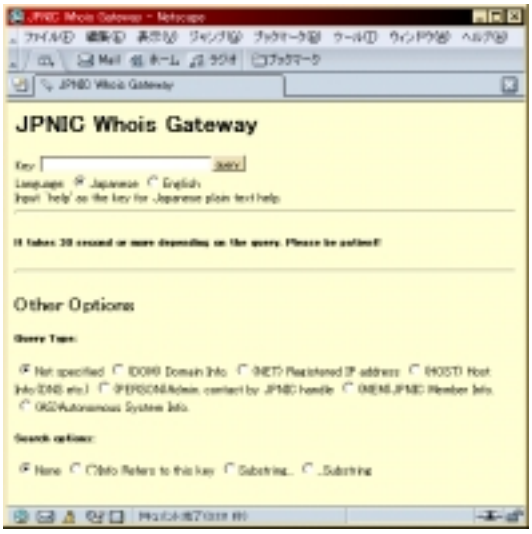

図 34　whois の Web インターフェース

whois の Web インターフェースは、通信プロトコルに HTTP を利用しており、ユーザが検索した結果のデータを転送するプロトコルは、既存の whois クライアントを利用した場合と異なる。https とよばれる TLS を利用した HTTP は、多くの Web ブラウザで利用可能であるため、Web インターフェースの場合には https を利用する構成にすることが可能である。転送プロトコルが異なると安全な通信のための設計に影響がある。

whois システムで扱われる情報は、項目名と値の組み合わせがテキスト形式で表現される。項目名の組み合わせは、データの分類ごとに定義されており、情報を新規に登録する場合、その分類に必要な項目に対応する値を入力する必要がある。

JPNIC の whois システムで扱われる登録情報の分類はレコードの種類の違いとして扱われる。それぞれのレコードのために定義された項目を表 19 に示す。

表 19　whois データのレコードと項目名

レコード名	レコードに含まれる項目名
ネットワーク情報	IPネットワークアドレス、ネットワーク名、組織名、運用責任者、技術連絡担当者、 ネームサーバ、割当年月日、返却年月日、通知アドレス、最終更新
AS情報	AS番号、AS名、組織名、運用責任者、技術連絡担当者、技術連絡担当者 AS-IN、AS-OUT、割当年月日、返却年月日、通知アドレス、最終更新
個人情報	ホスト名、IPアドレス、技術連絡担当者、通知アドレス、最終更新
ホスト情報	JPNICハンドル、氏名、電子メイル、NICハンドル、組織名、 郵便番号、住所、部署、肩書、電話番号、FAX番号、通知アドレス

表 19 で示した項目はすべて whois システムを使って公開されるものである。「ネットワーク情報」は、IP アドレスのブロックが割り振り又は割り当てられている組織の情報を含んでいる。「AS 情報」は AS 番号がその組織に割り当てられていることを示している。「運用責任者」や「技術連絡担当者」は、これらの情報の書き換えを行うことができるユーザを示していると同時に、ネットワーク利用組織の間で連絡を取る際に利用される。「個人情報」は、「運用責任者」や「技術連絡担当者」に含まれる人物情報のレコードである。「個人情報」に変更があった場合でも、「ネットワーク情報」等を変更せずに「個人情報」のみを変更するだけでよい。「ホスト情報」は DNS サーバの情報を登録するために存在する。各ネットワーク利用組織の DNS サーバは必ず「ホスト情報」として登録されなければならない。DNS における名前解決のための権限の委譲は「ホスト情報」に登録されたホストに対して行われる。

JPNIC における DNS は、主に IP アドレスからホスト名を検索する”逆引き”の利用を想定している。これは JPNIC が IP アドレスを割り振る NIR であり、その割り振られた IP アドレスに基づいて DNS が利用されるためである。

このように、whois システムはネットワーク資源の割り振り及び割り当ての情報そのものを提供しており、ネットワーク利用組織の管理者はその前提の上に運用管理を行う。

5.4. レジストリシステムにおける認証機能

レジストリデータの登録や公開を行うレジストリシステムに、セキュリティ機能を持たせるためには、レジストリデータの信頼性を定義し、また運用上の信頼性の度合いを表す尺度が必要となる。定義内容を満たす手法を実現し、その手法の確実性の度合いを増すことで、レジストリデータの信頼性が向上する。

信頼性の度合いは、レジストリシステムの運用上のセキュリティ要件を、どの程度満たしているかによって測られる。従って運用業務の内容と運用結果が明らかにならなければわからない。信頼性を考慮した運用業務の内容は、セキュリティ要件を予め決めることで決定される。本研究では運用業務の内容を決定する作業を、調査研究の後に行うものに位置付けており、信頼性の度合いについてはここでは言及しない。なお、セキュリティを考慮した運用要件を求める方法と基本調査については４章で述べた。

この節では、レジストリシステムにおけるセキュリティモデルと情報モデルについて述べた上で、認証機能のあり方について述べる。

5.4.1. 情報通信のセキュリティモデル

情報のやり取りが行なわれるエンティティの間のセキュリティは、大きく分けて「トランスポートセキュリティ」と「オブジェクトセキュリティ」の二つのセキュリティモデルに沿って考察される（図 35）。

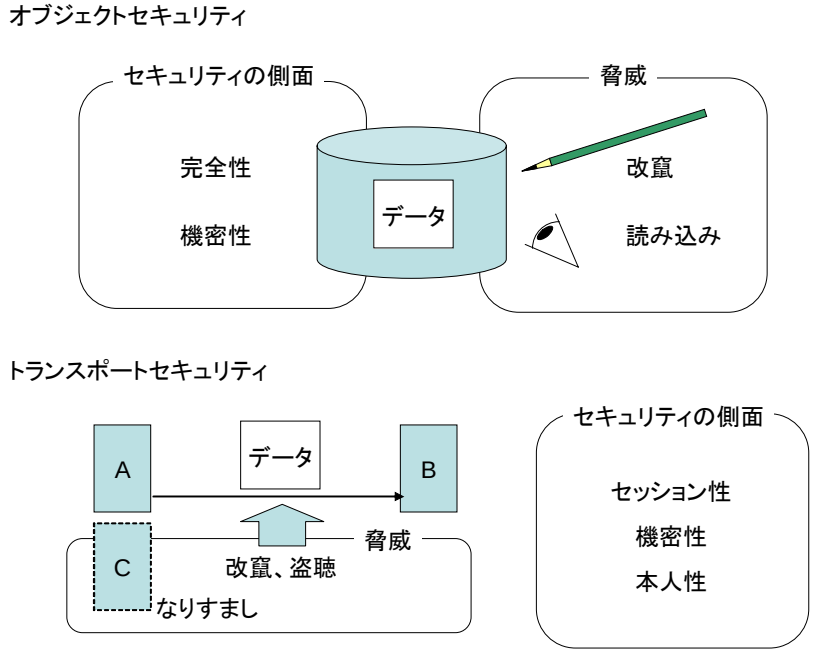

図 35　二つのセキュリティモデル

オブジェクトセキュリティとは、情報の機密性、完全性など、データの状態に注目したモデルである。このモデルでは機密性や完全性を保証する暗号強度などが問題となる。

トランスポートセキュリティとは、二つのエンティティの間でやり取りされる情報をいかに保護するかに注目したモデルである。このモデルでは通信相手の認証、通信相手の特定、メッセージの完全性などが問題となる。

情報は、対象とする情報モデルに応じて適切に適用されなければならない。例えば電子メールのセキュリティプロトコルを考案する際に、トランスポートセキュリティのモデルは適さない。これは保護対象が電子メールのメッセージであるため、個々の通信を保護するモデルでは、次々に転送される電子メールの仕組みにそぐわないからである。

5.4.2. レジストリシステムの情報モデル

レジストリシステムにおける保護対象は、レジストリデータである。レジストリデータには個人情報や組織情報など機密性を要求される情報が含まれていると同時に、whois システムを用いてユーザに開示される情報が含まれている（図 36）。

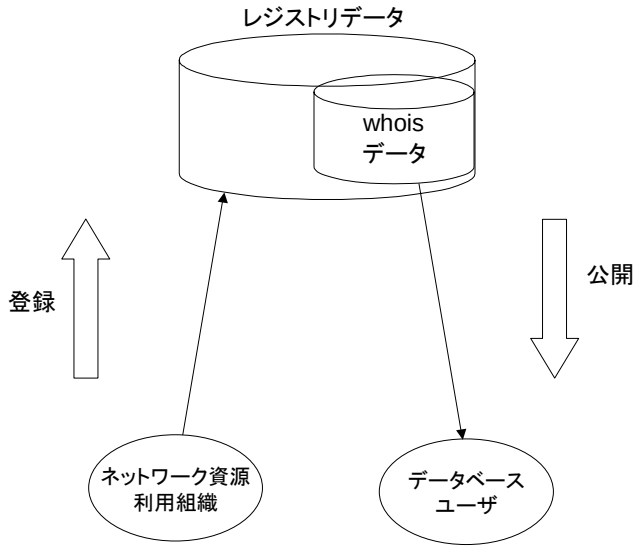

図 36　レジストリデータの情報モデル

１章及び２章で述べたように、レジストリシステムで管理される情報は、委譲された権限の範囲の情報である。この情報は、ネットワークを通じてやり取りされるかどうかに関わらず保護されなければならない。従ってオブジェクトセキュリティのモデルを適用するべきである。

しかしインターネットを通じて使われる通信プロトコルのうちオブジェクトセキュリティを適用としたものは少ない。例えば https や SSH といったプロトコルは、通信相手の認証や、やり取りされるデータの機密性を実現するためのもので、トランスポートセキュリティのモデルが適用されている。whois システムのように即時操作性を提供するサービスを使ってレジストリデータの情報公開機能を実現するには、レジストリシステムにトランスポートセキュリティのモデルを適用し、サービスシステムを設計する必要がある。

5.4.3. レジストリデータのオブジェクトセキュリティ

レジストリシステムで保護すべきデータは、レジストリデータであり、オブジェクトセキュリティのモデルを適用すべきであることは既に述べた。そのデータはインターネットを使った転送および書き換えの際にも保護されていなければならない。ここでいう保護とは、メッセージの機密性と完全性である。

5.4.3.1. メッセージの機密性

レジストリデータには、whois システムを用いて公開されている情報の他にネットワーク利用組織の電話番号など公開されない情報が含まれている。そのため非公開の情報を、インターネットを使って転送したり書き換えたりする必要がある場合に、メッセージの機密性を保持する必要がある。

JPNIC の現行の IP レジストリシステムと管理業務では、レジストリデータの登録及び書き換えのメッセージは電子メールを使ってやりとりされる。このときにデータの機密性は維持されていない。ただし、現行の whois システムでは機密性を要するデータは特定のユーザにしか提供しておらず、提供時の機密性の保持に関する問題を回避している。

5.4.3.2. メッセージの内容証明

委譲された権限とネットワーク資源を示すレジストリデータの内容は、電子的手段を用いて正しさが証明されていなければならない。証明されていない場合、その権限とネットワーク資源の保有を主張する第三者に対して、その真偽を示すことができない。また、登録されたネットワーク利用組織同士がレジストリデータの内容を相互に確認できなければ、自律的な問題解決を行うことはできない。

従って whois システムを使って提供されるデータや、レジストリデータの新規登録及び変更の結果は、その内容が証明されていなければならない。またその内容の証明を、whois システムの利用者が検証できる環境が必要である。

証明書を用いて内容証明を行うには、その保証レベルを予め定義しておくべきである。保証レベルについては 4.5.2.1 節で述べた。

5.4.4. レジストリシステムにおけるトランスポートセキュリティ

レジストリデータの操作（新規作成及び変更、削除）におけるトランスポートセキュリティは、手続きを行うものの本人性と権限の確からしさ、セッションの一貫性の三つの要素によって成り立つ。この三つの要素は、セキュリティプロトコルを設計する際の留意事項のうち、トランスポートセキュリティのモデルに当てはまるものである。これらの要素が IP レジストリシステムにどう関係するかを表 20 に示す。

表 20　IP レジストリシステムにおけるセキュリティ要素

	主体 （本人性の条件）	権限 （権限の確認方法）	セッションの一貫性
アドレス ブロック	LIR	割り振りを受けたアドレスブロックの再割り当て	やり取り中の 電子メール送信者の同一性
	ネットワーク利用組織	割り当てを受けたアドレスブロックの利用	
AS 番号	個人情報が登録された 申請者	対向とpeerを確立する	やり取り中の 電子メール送信者の同一性
個人情報 （登録情報として）	個人情報の申請者	登録申請と 登録情報の変更	やり取り中の 電子メール送信者の同一性

5.4.4.1. 本人性

IP レジストリシステムの申請者による操作要求は電子メールを通じて送られる。申請者の判別は MAIL-FROM とよばれるメールフォーマット[29]のヘッダー”From:”行の文字列を利用する。しかしこの文字列は第三者によって書き換えることが容易であり、あたかも申請者自身から送信された電子メールであるかのようにメッセージを偽造することが可能である。S/MIME といったメッセージ保護の機能を利用すれば、電子メールを利用してもなりすましを防ぐ方法を実現できる。例えば保護範囲の中に本人を示す値を含めておくことによって第三者による偽造を検出し、要求の受け入れを拒否することができる。しかし現行の IP レジストリシステムと、これを使った現行の業務では S/MIME を利用することはできない。RIPE NCC などで利用されている PGP についても、現在は利用することができない。

5.4.4.2. 権限の確からしさ

権限の確からしさはアクセス制御とよばれる処理で確認される。アクセス制御は、検査対象にその権限があるかどうかを判断し、権限があればその行使を許可し、権限がなければアクセスを拒否する処理である。アクセス制御は、アクセス制御規則とよばれる規則に従って実施される。

IP レジストリシステムにおけるアクセス制御は、レジストリデータを書き換えられ

[29] RFC822, “Standard for The Format of ARPA Internet Text Messages”, http://www.ietf.org/rfc/rfc822.txt

るかどうかの判断に用いられる。アクセス制御には、表 21 に示すエンティティと権限の確認方法が適用される。

表 21　アクセス制御の為のエンティティと権限の確認方法

	情報を更新するエンティティ	権限の確認方法
ネットワーク情報	LIRとネットワーク利用組織 （運用責任者及び技術連絡担当者）	MAIL-FROMとLIR情報の比較
AS情報	自律システム （運用責任者及び技術連絡担当者）	MAIL-FROMとAS情報の比較
個人情報	登録者	MAIL-FROMと個人情報の比較
ホスト情報	ホストの管理者 （運用責任者及び技術連絡担当者）	MAIL-FROMとホスト情報の比較

なお、JPNIC におけるレジストリデータの為のアクセス制御は業務の中で実施され、レジストリシステムの処理には含まれていない。

現行のアクセス制御は、先に述べた本人性に基づいて行なわれている。すなわち MAIL-FROM を用いた方法で本人性を確認し、その権限を確認した上で書き換え許可の判断を行なっている。アクセス制御の処理は本人性に依存するため、例え権限の確からしさを業務手続の中で確認したとしてもそれが本来あるべき権限であったかどうかはわからない。

5.4.4.3. セッションの一貫性

セッションの一貫性とは、セッションとよばれる一つの目的を持った通信のまとまりにおいて、やりとりされるメッセージの目的が終始一貫しているという性質である。偽造したメッセージが挿入されたり、通信相手がすりかわったりすることで、メッセージの一貫性が損なわれる。whois システムにおけるにおけるメッセージの一貫性について図 37 に示す。

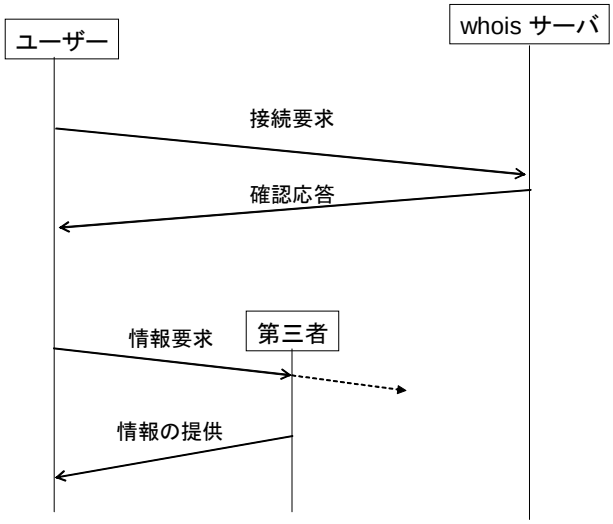

図 37　whois におけるセッションの一貫性

メッセージの一貫性は、予め定義され、保護されたセッション識別子を使用することで保持することができる。セッション識別子とは、セッションごとに別々の識別子を決め、その識別子を含まないあるメッセージがセッション中のものかどうかを確認するためのものである。セッション識別子が偽造されるとメッセージの一貫性が損なわれるため、偽造された場合に、通信相手がそれを検知できる仕組みが必要になる。

現行の IP レジストリシステムでは、ユーザと IP レジストリシステム及びオペレーターは、電子メールを使ってメッセージをやり取りしている。また電子メールの本文にセッション識別子は含まれていない。whois システムは TCP を使っているため、そのセッション管理機能を利用することができる。しかし TCP のセッション識別子は保護されておらず、通信経路上で書き換えることが可能である。TLS のセッション管理機能を用いると安全なセッション管理が実施できるが、whois のクライアントやサーバプログラムで TLS を利用している実装は、これまでには見つかっていない。

従ってレジストリデータは、登録及び変更のセッション中や提供セッション中に偽造することが可能である。どちらのセッションにおいても一貫性が保持される仕組みが必要である。

5.5. PKI を用いた認証機能

レジストリシステムの認証機能に、公開鍵暗号を使った強い認証機能を適用するには、

その認証機能をどの場面で利用するのかが検討課題になる。PKI を用いた認証機能は、この節では 5.4 節で述べた情報モデルとセキュリティモデルに基づき、レジストリシステムに適用するための、PKI を用いた認証機能について述べる。

5.5.1. レジストリデータのメッセージ認証

5.4.3 節で述べたように、レジストリデータは本来オブジェクトセキュリティのモデルを適用すべきである。このモデルの適用し、情報の完全性を検証する環境を実現することで、whois のユーザはレジストリデータの完全性を確認することができる。また転送プロトコルに依存せずに、様々なネットワークサービスで情報提供及び入手を行うことが可能になる。

レジストリデータの完全性は、メッセージ認証機能の付加によって実現することができる。メッセージ認証機能には、データエントリーへの電子署名と、その電子署名を検証する環境の二つが必要になる。

データエントリーへの電子署名は、IP レジストリシステムの処理の中で行われる。電子署名が行なわれたデータエントリーは既存のデータエントリーの扱いと同様にデータベースに格納されることで既存の whois システムを使った情報公開を継続することができる。この構成にすることで、ユーザはこれまで通り Web ブラウザを用いて閲覧することができる（図 38）。

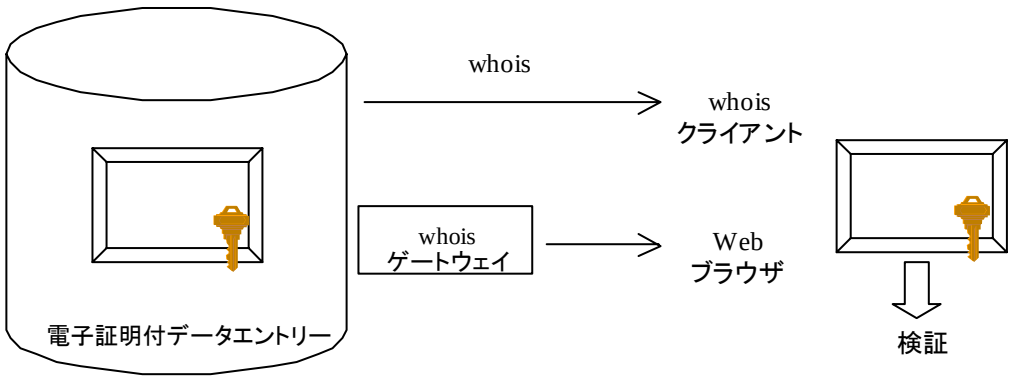

図 38　レジストリデータのメッセージ認証

しかし既存の Web ブラウザや whois クライアントには、電子署名が付加されたデータエントリーの正当性を確認することはできない。これはこれらのクライアントプログ

ラムには、テキスト文字列に対する電子署名の検証機能が実装されていないためである。

メッセージ認証機能をレジストリシステムに適用するには、電子署名が付加されたデータエントリーの転送と、テキストデータへの電子署名を検証できるユーザの環境が必要になる。電子署名はオブジェクトセキュリティのモデルを適用したシステムであり、転送プロトコルを選択する必要はない。しかしユーザの利便性を考慮すると、電子署名が施されたデータオブジェクトを受信し、証明書を用いて検証することができるプログラムが必要となる。この環境を実現するには、既存のクライアントプログラムに変更を行うか、新たなクライアントプログラムの開発が必要となる。

5.5.1.1. メッセージ認証のメッセージフォーマット

多くの RIR では、レジストリデータ（whois データ）の表現言語に RPSL を利用している。RPSL には RPSS（Routing Policy System Security[30]）とよばれる認証と認可を実現するための仕組みがある。しかし RPSL には暗号技術を利用したデータ完全性の保護機能がない。従ってそのままでは分散環境におけるデータの保護と検証のために利用することはできない。今後、RPSL に電子署名の機能を付加するか、構造化された言語にデータを変換して提供する手法が開発される可能性がある。

PKI を利用した、メッセージ認証を実現する既存のメッセージフォーマットには S/MIME や PKCS#7 が存在する。S/MIME は IETF smime WG で提案されたメッセージフォーマットで、任意のデータに電子署名や暗号化を施すことができる。PKCS#7 は S/MIME バージョン 3 より早い 1993 年に RSA Data Security 社によって提案されたメッセージフォーマットで、内容は S/MIME のエンベロープ（電子封筒）とほぼ同じである。

S/MIME や PKCS#7 を用いる場合、任意のデータに対するエンベロープ（電子封筒）を適用することになり、各々のデータの構造が無視される。whois システムでは、しばしば連鎖した検索のようなデータの構造を利用した処理を行うため、構造化されていないデータの扱いは適さない。レジストリデータの構造に対するエンベロープの適用方法について、新たなプロトコルを策定するか、代替手段を用いたメッセージ認証機能を実現する必要がある。

[30] RFC2725, “Routing Policy System Security”, http://www.ietf.org/rfc/rfc2725.txt

5.5.1.2. 実装の際の留意事項

IETF の provreg ワーキンググループでは、whois に代わるプロトコル epp（extensible provisioning protocol）の策定が行われている。レジストリシステムの情報公開機能とユーザ環境の実装の際には、このような新しいプロトコルへの対応等に留意する必要がある。また W3C（World Wide Web Consortium）では XML Signature とよばれる、構造化された拡張可能言語 XML に電子署名を付加するプロトコルが提案されている。今後、構造化されたテキスト表現に対する電子署名を実現するプロトコルが利用される可能性がある。

5.5.2. レジストリシステムにおける認証システム

第三章で述べたように、他のインターネットレジストリでは Web インターフェースによるレジストリデータの書き換え等のサービスが提供されている。APNIC の MyAPNIC のように、クライアントに対しても強い認証が実施され始めている。NIR は LIR によって登録されている情報を公開するため、LIR による情報登録や更新といった機能を実現する必要がある。

5.5.2.1. 相互認証

ユーザにレジストリデータの登録や更新のサービスを提供する場合、ユーザのなりましやサーバのなりすまし、通信経路でのデータの改ざんや破棄といった脅威が存在する。これを防ぐには、暗号技術を利用したセキュリティプロトコルを利用する必要がある。

ユーザ及びサーバのなりすましを防ぐには、相互認証を行うことができるプロトコルを利用する必要がある。相互認証とは、ユーザがサーバを認証すると同時にサーバがユーザを認証する仕組みである。PKI を用いて相互認証を実現するには、予め信頼する認証局の証明書を入手しておき、認証対象が提示した証明書を検証する必要がある。

サーバがユーザを認証するには、サーバ（サーバ管理者）が信頼する認証局が、ユーザの証明書を発行しておく必要がある。またユーザは、その証明書をクライアントソフトウェアに組み込んでおき、サーバにアクセスした際にそれを利用できなければならない。

サーバによるユーザ認証を実施するには、LIR の登録情報を更新する必要があるユーザが、証明書を利用できる環境が必要である。また鍵ペアと証明書の扱いに関して第４章 4.4.6 節の事項、すなわち鍵の安全性と用途に関して留意する必要がある。

ユーザがサーバを認証するには、ユーザが信頼する認証局がサーバの証明書を発行している必要がある。そのためには少なくともレジストリデータを編集する必要があるユーザの全員が信頼する認証局が存在し、その証明書がユーザの環境になければならない。

5.5.2.2. ユーザーインターフェースとプロトコル

インターネットを通じてレジストリデータの登録や更新の機能を実現するには、5.4.1 節で述べたトランスポートセキュリティのモデルを適用するか、ユーザの申請内容をオブジェクトセキュリティのモデルで保護するという、二つの方法が考えられる。APNIC の MyAPNIC や RIPE NCC の LIR Portal といった Web インターフェースを使った登録や更新の機能が実装されている状況は、LIR による手続きの簡便化の要求が存在することを意味している。これは、ユーザの申請内容を保護する方法は、そのデータ（電子メール）のやり取りに時間がかかり、また申請書類の書式に間違いがある場合などに再送の必要があるなど、やりとりに必要となるオーバーヘッドが大きい。一方、Web インターフェースでは書式に間違いがある場合に、すぐにエラーをユーザに知らせることができ、また再申請の際に一度入力された情報を入力フォームに表示しておくことで、ユーザに再入力を要求する必要がない。

HTTP を使ったシステムを構築する場合、トランスポートセキュリティのモデルを適用した https か、HTTP にて転送される MIME オブジェクトにオブジェクトセキュリティのモデルを適用したプロトコルを利用する方法が挙げられる。しかし後者の形式のプロトコルは未だ実装されておらず、S/MIME オブジェクトを HTTP で転送するといった手法は一般的ではない。前者の https を使う方法は、多くの Web ブラウザに PKI を利用する機能が実装されていることから、より実用的である。

https の利用の際には、5.4.4.3 節で述べた一貫性の保証が重要課題となる。これは一つの目的に対して複数の TCP コネクション及び TLS コネクションを利用する必要があるためである。この問題に対して、多くの Web ページでは cookie を用いてアプリケーションのためのセッション管理機能を実現している。しかしユーザ環境に保存された cookie のデータの扱いを誤ると、NIR が管理していない Web サーバにそのデータが転送される可能性がある。この問題は CSS（Cross-Site Scripting）問題の一つである。セッションの管理機能については、慎重に設計される必要がある。

またユーザ環境に組み込まれている認証局の証明書が、NIR の認証局だけであることは想定しにくい。このことは多くの認証局ベンダが発行している証明書が、ユーザ環境では有効であると表示される状況を作り出す。従ってある NIR と同名のサーバ証明書が、いずれかの認証局によって発行された場合、ユーザはその証明書を提示したサー

バを誤って認証してしまう。ユーザの証明書に対する誤認を防ぐ仕組みが必要である。

5.5.3. 分散環境でレジストリデータを検証する環境

インターネットレジストリにおける登録を、分散環境（インターネットのようなネットワーク環境）で検証する環境について述べる。

5.5.3.1. インターネットレジストリの証明書

1 章で述べたように、CIDR ブロックの割り振りは ICANN、RIR、NIR、LIR のどのレベルでも行われる。あるネットワーク資源の割り振りを示す証明書を検証しようとした場合、その証明書を発行した認証局の証明書が正当であり有効であることを確認できなければならない。インターネットレジストリ全体のネットワーク資源の管理構造に PKI を利用する場合、いずれのインターネットレジストリの認証局が発行した証明書であっても、ある信頼点に基づいて検証できなければならない。すなわち信頼のチェインがインターネットレジストリの認証局の間で一貫性を持っている必要がある。

この報告書では NIR における認証局のあり方について注目しているが、インターネットにおけるネットワーク資源の確認方法に PKI を利用する場面を考えると、他のインターネットレジストリにおける認証局との連携の仕方について検討する必要がある。他の認証局との連携の際には、第 4 章で述べた保証レベルを検討しなおすなど新たな課題がある。

5.5.3.2. 検証環境における証明書

whois システムのユーザが、レジストリデータの証明内容を電子的に検証するには、ユーザ環境に、電子署名を検証するための証明書が必要となる。第２章で述べたように NIR の提供するレジストリデータの内容は、NIR によって証明される。従って NIR の認証局の証明書がユーザ環境に組み込まれている必要がある。またユーザの信頼する認証局の証明書を使って、NIR の認証局が発行した証明書の正当性を確認できる状況が必要である。そのためには、NIR の認証局の証明書を予め whois のユーザに配布しておくか、ユーザが信頼している認証局によって NIR の認証局の証明書を発行しておくという二つの方法が考えられる。

第１章で述べた NIR の権限の構造を、証明書のツリー構造になぞらえると、ICANN によってルート認証局が運用され、RIR に証明書を発行する構造が考えられる。この場合、RIR は更に NIR に証明書を発行することになる。しかし第３章で述べた調査結果から、インターネットレジストリ間で証明書を発行している例はない。また JPNIC は

IP アドレスの割り振り対象を確認する際に、APNIC の審査基準を用いるだけでなく、日本国における存在証明を利用している。この方法はインターネットレジストリに共通したものではなく、JPNIC のポリシーによるものである。従って JPNIC が、あるエンティティに発行した証明書は、JPNIC の認証局を信頼していなければ正しさを検証することができない。これはユーザにとって JPNIC の認証局が信頼点である必要がある。

5.6. 認証機能を持つレジストリシステム

PKI を用いた認証機能をレジストリシステムに組み込むと、メッセージ認証、ユーザ認証を行った上でのレジストリデータの書き換えなどが実施できるようになる。本節では、前節の認証機能をレジストリシステムに組み込んだ場合のシステムの概要を示す。

5.6.1. whois におけるクライアント認証とメッセージ認証

PKI と whois を組み合わせた使ったユーザ認証に基づくレジストリデータの変更とメッセージ認証の概念図を図 39 に示す。

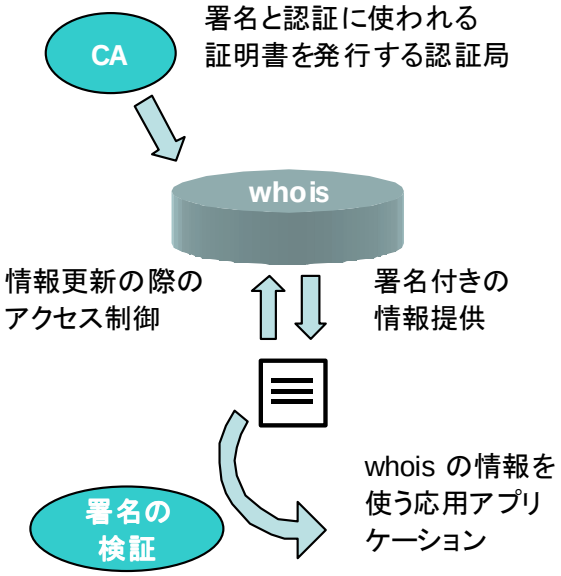

図 39　whois における認証

中央の白い四角が登録情報で、この情報が whois に登録される際に認証とアクセス制御が行われる。また whois は登録された情報の出所を確認できる手段をもって提供し、ユーザは登録情報が確かに JPNIC の whois によって提供されていることを確認することができる。この方法には、オブジェクトセキュリティのモデルを適用し、レジス

トリデータに電子署名を付加する方法と、トランスポートセキュリティのモデルを適用し、ユーザがサーバ認証を行った上で、情報を確認する方法の二つが考えられる。図 39 では前者の電子署名を示している。5.5.1.2 節で述べたように、情報の提供方法を実装する際に、利用する転送プロトコルと表現プロトコルを検討する必要がある。https クライアントとなる様々な Web ブラウザが実装されている状況を考えると、はじめに https を利用した相互認証を段階的に実現し、同時にメッセージ認証を行う環境を整えておくといった手順が考えられる。

whois を利用して、レジストリデータ書き換えの為のクライアント（ユーザ）認証と whois で公開される情報のメッセージ認証機能を提供する仕組みの構成図を図 40 に示す。

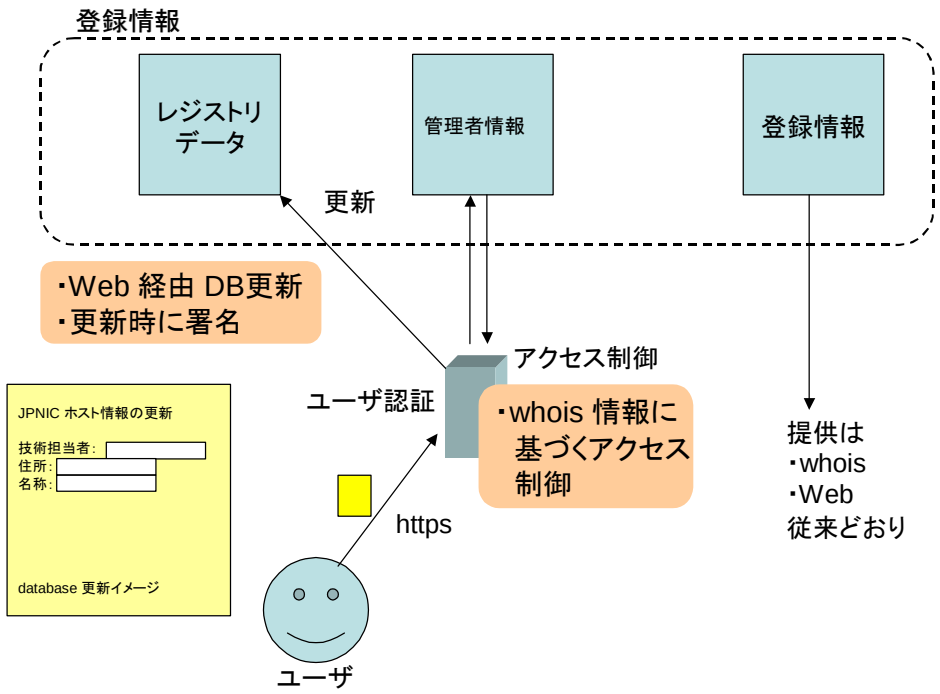

図 40 whois におけるユーザ認証とメッセージ認証

レジストリデータを書き換えようとするユーザは、ユーザ認証を受け、更に書き換える情報に対応してアクセス制御が行われる。特定のレジストリデータの書き換え権限が認められたユーザは、書き換えを実施し、レジストリデータを更新する。なおこの動作はユーザの操作だけで完結するものと、オペレーターの承認といった操作を要するものが存在する。またユーザ認証に https のクライアント認証のみを使うだけでなく、

S/MIME などオブジェクトセキュリティのモデルを適用した方法も考えられる。その場合には、ユーザが記述する申請形式の差異を吸収する仕組みが必要と考えられる。

登録されたレジストリデータは従来と同じ方法すなわち whois および Web を使って公開される。この提供方法を変更しないとすると、クライアントソフトウェアの変更は必要ない。ただし、メッセージ認証機能を実現するには、クライアントソフトウェアの検証機能の開発が必要になる。

また ARIN で利用されている RWhois のように、一元化された whois のインターフェースに対応するためには、登録情報の提供機能に付加的なソフトウェアの開発が必要となる。

5.7. レジストリデータベースの応用

5.5 節で述べた、レジストリデータのメッセージ認証機能を実現すると、ネットワーク資源の割り振り／割り当ての情報の正当性を示すことができる。この機能は、同時に登録されたネットワーク利用組織と特定の識別子（IP アドレス）の関係を結びつける根拠となる。この性質を応用すると、様々なネットワーク資源に関する証明を行うことができる。本節では、内容が証明されたレジストリデータベースの応用について述べ、更に応用例を紹介する。

5.7.1. IP アドレスに基づく実在性の証明

NIR によるネットワーク資源の割り振り／割り当てといった情報の登録は、登録されたネットワーク利用組織に対する権限の委譲を示すものが存在する。第１章で述べたようにアサインメントウィンドウ等がその例である。一方この情報は、あるアサインメントウィンドウが実際にどの組織に割り振られているのかを示す情報でもある。つまり特定の IP アドレスの範囲に対して、そこに含まれる IP アドレスを割り当てる権限を持つ組織が存在するのか、またあるとするとその組織はどのような組織であるのか、という情報を示す。JPNIC によるアサインメントウィンドウの割り振り対象は、登記簿謄本等書類の検査に基づいて実在性が確認されている。従って IP アドレスを元にして、その IP アドレスを利用する組織や、割り振る権限を持つ組織を特定することができる。

ネットワーク利用組織が利用することができるネットワーク資源には、IP アドレスの他に AS 番号、ホスト（登録されたもの）、ドメイン名といったものがある。これらの登録情報についても、アサインメントウィンドウの情報と同様に関連する組織の情報を確認することができれば、ネットワーク資源に関するレジストリデータを利用した確

実なネットワークを構築することができる。例えば、IP アドレスの割り当てが証明されている組織とのみ経路交換の peer を確立する経路交換や VPN の構築などが挙げられる。更に、レジストリデータを認証基盤として応用し開発を進めると、公衆交換電話網のゲートウェイを認証した上で接続する安全な IP 電話、予め登録されたメーカーに作られたインターネット家電の認証等、様々な分野への適用が考えられる。また登録情報の重要性を民間組織であるかネットワーク管理組織かといったレベル分けをすることで、利便性と運用の安全性のバランスを取り、分野に応じた安全な認証基盤の構築を視野に入れることができる。

5.7.2. 応用例

本節では、内容が証明されるレジストリデータを応用し、各分野で開発を進めることで考えられる応用の可能性を示す。これらの応用例は、本調査報告書で示す認証局が実現した上に、各種サービスのための開発が進んだ際に実現する可能性があるもので、必ずしも NIR における認証局がこれらを目標として運用されるわけではない。

5.7.2.1. ゲートウェイの証明書

インターネットに接続したネットワーク組織では、インターネットを通じて接続を受け付けるためゲートウェイを構築することがある。ユーザは重要なサービスを利用するためにゲートウェイを利用する際には、そのゲートウェイを認証し、接続を試みる。

既存の多くのゲートウェイの認証対象はアプリケーションゲートウェイであり、正当性が確認されるべき主体はサービス提供者であった。しかし、IPsec を使った通信サービスの提供や IP 電話で利用される公衆交換網ゲートウェイなど、認証対象の主体がネットワーク資源を持つ主体と同一である、もしくはネットワーク資源の利用権限をもつ主体である考えられる状況が存在する。ネットワークサービスを提供する主体が、然るべきネットワーク資源を持つことをユーザが確認できれば、ゲートウェイに対して、より確実な認証を行うことができる（図 41）。

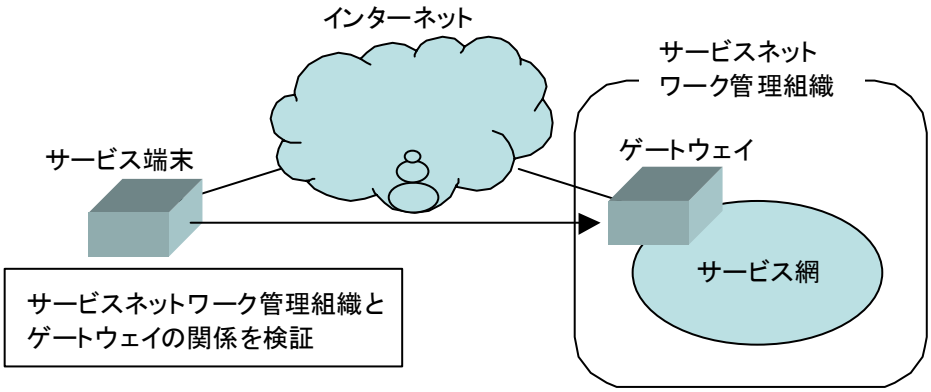

図 41　ゲートウェイの認証

5.7.2.2. 認証局の証明書

インターネットを利用する通信サービスで PKI を利用していると、新たな認証局をトラストポイント（信頼点）に加える場面が存在する。また認証局が発行する失効情報をいち早く入手しなければならない場面がある。

原理的な PKI の利用方法に従うと、認証局の信憑性を確認する手段として、インターネットを利用しない方法が順当である。しかしオフラインの方法では情報が古かったり入手方法自体が不明であったりする。これまでは、ユーザのトラストポイントの扱いについては基本操作に留めておき、トラストポイントの追加の方法を実現したソフトウェアはほとんど見られなかった。そのためユーザはデフォルトで組み込まれている認証局をトラストポイントに設定せざるを得ず、認証のたびに証明書ツリーを確認しない限り、認証対象の妥当性や認証局の保証内容などを無視して PKI を利用することになる。

ある証明書の正当性を確認する手段には、証明書ツリーを利用して検証する方法の他に、トラストポイントの追加手順を利用する方法がある。すなわち信頼する認証局の情報を入手し、その認証局が発行している証明書の fingerprint などの情報と、別の方法で入手した証明書が同一であるかどうかを確認する方法である。

レジストリシステムの情報公開機能で認証局の fingerprint を扱うことができれば、上で述べた「別の方法」の一つを提供できる可能性があると考えられる。または証明書リポジトリとして機能し、ネットワーク利用組織と認証局の相互の利用を促進する役割が考えられる。

5.7.2.3. ネットワーク利用組織をまたぐ認証

PKI を使った証明書の検証環境には、証明書のトポロジーに従った認証の範囲が存在する。この範囲は PKI ドメインと呼ばれる。異なる PKI ドメインと相互に認証を行うためには、相互認証証明書を発行することで証明書のトポロジーを確証するか、トラストポイントを追加する必要がある。

相互認証証明書の発行先の信頼性や、新たなトラストポイントの信頼性を確認する際に、証明書に関する情報を含むレジストリデータを利用することで、信頼のレベルを測ることができる可能性がある。NIR は組織の実在性の確認とネットワーク資源に関する審議を行っているため、特定のネットワーク資源と、特定の認証局の組み合わせが申請された通りであることを証明することができる。ユーザはその組み合わせの証明に基づき、異なるネットワークに属するエンティティの認証に応用することが考えられる。

5.8. まとめ

本章では、NIR における認証局を構築する際に、ネットワーク資源を管理するレジストリステムに、どのような認証システムを適用することができるかについて述べた。その際に、IP レジストリシステムの情報モデルとセキュリティモデルを元に、モデルとしてのセキュリティ要件について述べた。

レジストリシステムにおける認証システムは、データベースの保護の為のユーザ認証と、データエントリーの内容を証明するためのメッセージ認証の機能を持つ必要がある。これらの機能を実現するために、ユーザ環境と規模拡張性を考慮して PKI を適用する場合の、ユーザ環境や認証システムの要件について述べた。

またネットワーク資源の割り当てや割り振りといった内容が証明される機能を、認証基盤として応用することについて述べた。更にその応用例を紹介した。