第 2 章　アドレス資源管理における安全性

内容

- アドレス資源管理におけるセキュリティ
  - JPNIC におけるアドレス資源管理の仕組み
  - レジストリデータの保護

2. アドレス資源管理における安全性

2.1. アドレス資源管理におけるセキュリティ

JPNIC のようなインターネットレジストリはアドレス資源管理と呼ばれる業務を行なっている。アドレス資源管理とは、アドレス資源を利用する組織を登録し、アドレス資源の割り振りに関する情報管理を通じて、アドレス資源の健全な利用を図る業務である。

本節では、まずアドレス資源管理に利用されているレジストリデータ（登録情報）について認証と管理権限の観点で述べる。次に申請業務におけるリスクについて述べ、業務データの保護の必要性について述べる。業務データの保護については、アジア太平洋地域の地域インターネットレジストリである APNIC やヨーロッパ地域の地域インターネットレジストリである RIPE NCC で活用されている仕組みについても言及する。

2.1.1. レジストリデータとは

有限であるアドレス資源の割り振り／割り当てを効率的に行なうためには、アドレスがどのように分割されているのかを把握している必要がある。また、アドレスブロックの使用率を調べる、使用されていないアドレスを回収するなどを行なうために、アドレスブロックの使用者は誰かを知る必要がある。

このようなアドレス資源の管理を行なうために維持管理すべきデータは、インターネットレジストリのリポジトリに収められている。このデータをレジストリデータと呼ぶ。レジストリデータには様々なものが存在するが、ここでは四つのデータに着目する。そのデータとは、LIR（Local Internet Registry：ローカルインターネットレジストリ、日本におけるプロバイダを意味する）の情報、ネットワーク情報、AS 情報、割り当て情報である。

2.1.1.1. アドレス資源管理の仕組み

インターネットのアドレス資源管理は、Internet Assigned Numbers Authority（以下、IANA と呼ぶ）機能を実施する非営利法人 Internet Corporation for Assigned Names and Numbers（以下、ICANN と呼ぶ）と、この ICANN／IANA からアドレス資源の割り振りを受けたインターネットレジストリによって行われている。

インターネットレジストリはアドレス資源の割り振り業務の形態に従い、ICANN／IANA を頂点とする木構造を成している。ICANN／IANA は Regional Internet Registry（地域インターネットレジストリ：以下、RIR と呼ぶ）に割り振りを行って

いる。

RIR（Regional Internet Registry：地域インターネットレジストリ）は北米、ラテンアメリカ・カリブ地域、ヨーロッパ地域、アフリカ地域、アジア太平洋地域のそれぞれに存在している。北米にはAmerican Registry for Internet Numbers（以下、ARINと呼ぶ）が、ラテンアメリカ・カリブ地域には Latin America and Caribbean Internet Address Registry（以下、LACNIC と呼ぶ）が、ヨーロッパ地域には Reseaux IP Europeens Network Coordination Centre（以下、RIPE NCC と呼ぶ）が、アフリカ地域には African Network Information Center（以下、AfriNIC）が、アジア太平洋地域の RIR には Asia Pacific Network Information Centre（以下、APNIC）がある。この構造を図 2-1 に示す。

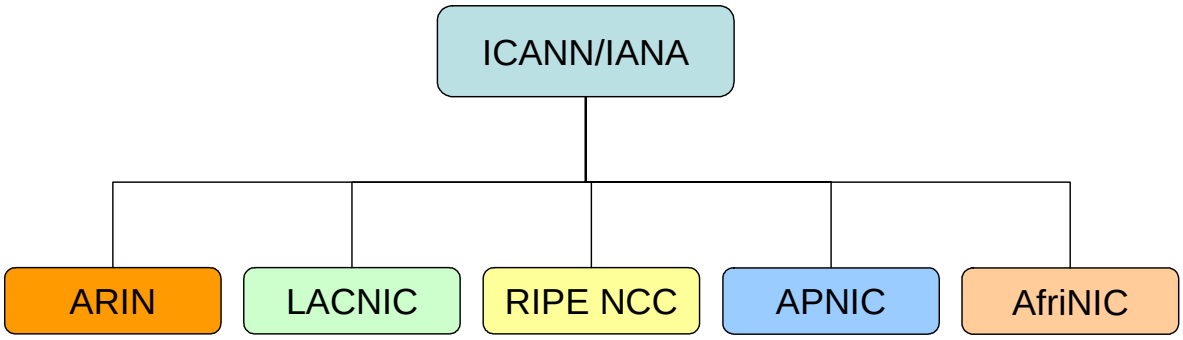

図 2-1 ICANN/IANA と RIR の構造

アドレス資源に関する登録情報は RIR が管理業務を行うが、個々のデータの内容のほとんどは登録主体である LIR などが管理するようになっている。RIR は、NIR や LIR を対象とするメンバーシップ制度を設けており、会費の収入を得ると同時にポリシー策定のための会議を開催したり、教育活動を行ったりしている。

以下で、各 RIR におけるメンバーシップについて述べる。

（1） ARIN におけるメンバーシップ

ARIN では地域内の IP アドレスユーザからの意見を集約する目的でメンバーシップ制度を設けている。ARIN から直接の割り振りを受けている ISP は自動的にメンバーとなる。この場合のメンバーシップ年会費は、更新費用に含まれている。割り振りを受けていない組織または個人の場合には年会費 500 ドルを支払って、申し込みを行う必要がある。この手続きは次の様になる。

（1） 申請フォームに記入する（http://www.arin.net/membership/join.html）
↓
（2）初年度の会費 500 ドルを支払う

メンバーに与えられる権利には次のものがあげられている。

- ARIN のオペレーションについて報告および討議を行うため、年に二度開催される ARIN のメンバー会議への二人分の参加権
- 二年に一度開催される Public Policy Meeting への二人分の参加権（無料分）
- Board of Trustee および Advisory Council メンバーの指名および投票権
- アナウンスおよび討議用メーリングリストへの参加権
- 企業または個人のウェブサイトに ARIN メンバーロゴを表示する権利
- 今後提供されるメンバーシップの享受

（2） RIPE NCC におけるメンバーシップ

RIPE NCC では、アドレス資源を受け取るためには LIR としてメンバーになることが求められる。メンバーは RIPE NCC General Meeting への参加を通じて RIPE NCC の活動とサービスに影響を与えることが出来るとされている。

メンバー加入手続きは次の様になる。

（1） 登録希望者は「RIPE NCC のメンバーとなる手続き[1]」を理解し、記入した申請フォームを new-lir@ripe.net に送信する

↓

（2） RIPE NCC はレジストリファイルを作成し、料金請求書を登録希望者に送付する

↓

（3） 登録希望者は「RIPE NCC におけるローカルインターネットレジストリを構築する手続き」について理解し、契約に合意することを new-lir@ripe.net に送信する

↓

（4） RIPE NCC は構築作業の詳細を登録希望者に電子メールで通知する

[1] Procedure for Becoming a Member of the RIPE NCC（RIPE-257）
http://www.ripe.net/ripe/docs/newlir.html

↓

（5）　登録希望者は「標準 RIPE NCC サービス合意書[2]」の署名済みコピーを提供する

↓

（6）　登録希望者は料金を支払う

↓

（7）　RIPE NCC は、料金と署名済み合意書を受け取った後、登録希望者のサービスレベルが上がったことを通知する

（3） APNIC におけるメンバーシップ

アジア太平洋地域を管理する APNIC では、各国別のアドレス資源管理を National Internet Registry（以下、NIR と呼ぶ）に委譲している。APNIC から割り振り／割り当てを受けている NIR としては、Japan Network Information Center（以下、JPNIC と呼ぶ）、Korean Network Information Center（以下、KRNIC と呼ぶ）、China Internet Network Information Center（以下、CNNIC と呼ぶ）、Taiwan Network Information Center（以下、TWNIC と呼ぶ）、Asosiasi Penyelenggara Jasa Internet Indonesia（以下、APJII と呼ぶ）が存在する。

APNIC ではメンバーに対し、アドレスの割り振り、会議への参加などのサービスを提供している。

メンバーとなる手続きは次のように定められている。

（1）メンバー申込書を申請する

↓

（2）APNIC よりメンバーキットが送られる

↓

（3）メンバーシップ同意書にサインし、メンバー料金を支払う

↓

（4）APNIC は同意書にサインし、コピーを送る

---

[2] The Standard RIPE NCC Service Agreement
http://www.ripe.net/ripe/docs/service-agreement.html

APNIC のメンバーのアドレス資源の割り振り構造を図 2-2 に示す。

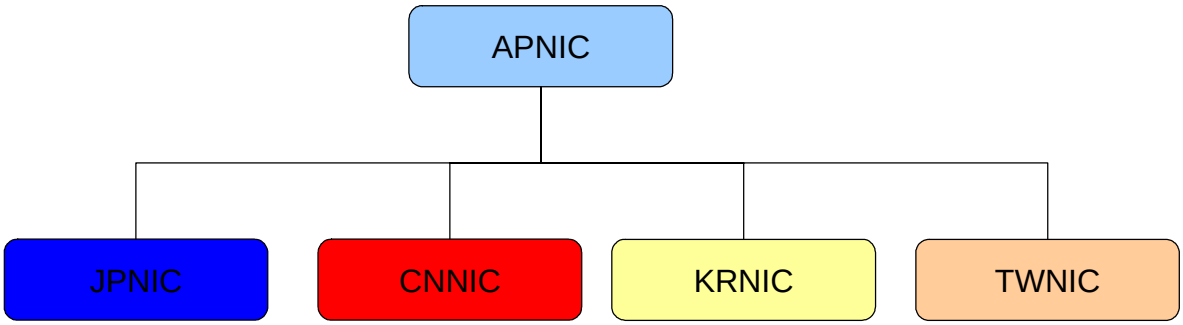

図 2-2 APNIC メンバー

メンバー申し込み申請はウェブから行う（図 2-3）。

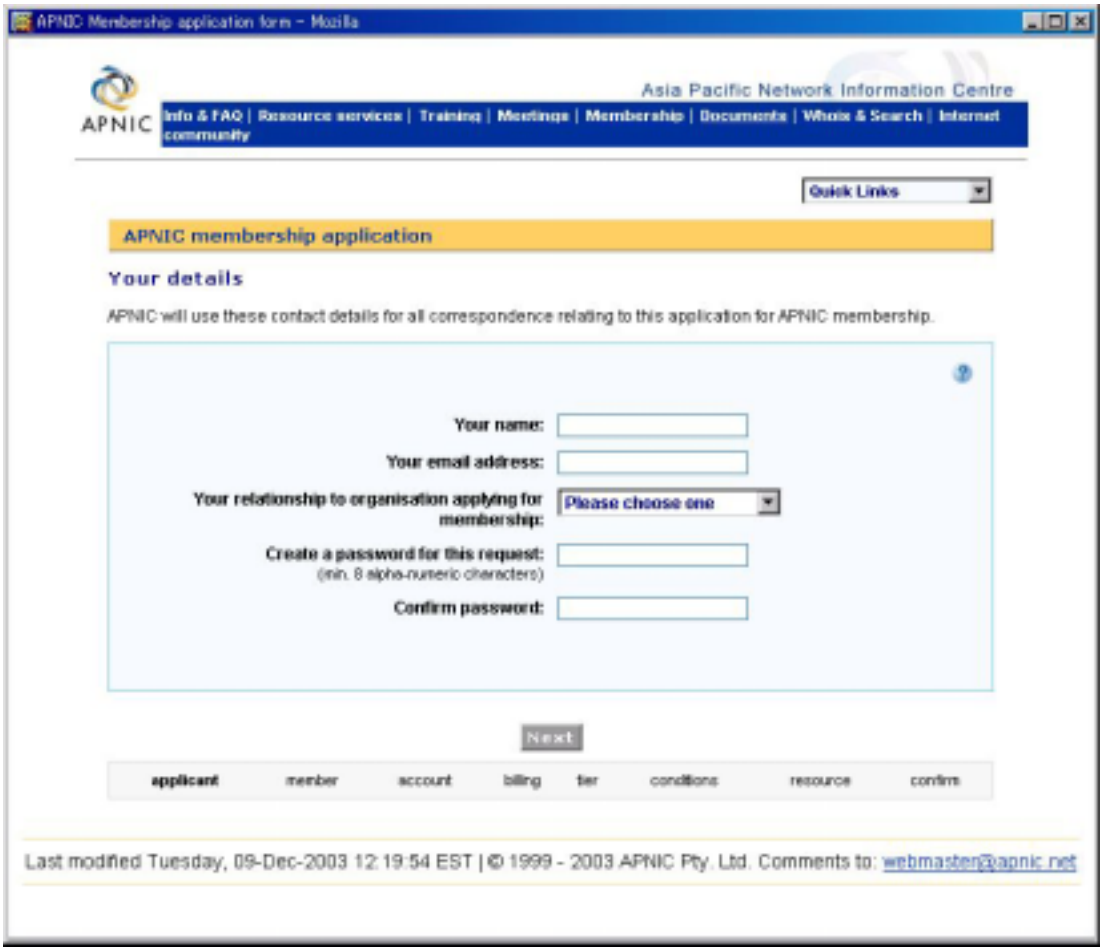

図 2-3 APNIC メンバー申請フォーム

メンバーシップ料金は表 2-1 のように定められている。利用できるアドレス空間の大きさによって年会費が変わる。

表 2-1 APNIC メンバー料金（2004 年 2 月現在）

メンバーシップ	年会費（US$）	IPv4 アドレス空間	IPv6 アドレス空間
Associate	625	None	None
Very small	1,250	/22	/35
Small	2,500	/19 から /22	/32 から /35
Medium	5,000	/16 から /19	/29 から /32
Large	10,000	/13 から /16	/26 から /29
Very large	20,000	/10 から /13	/23 から /26
Extra large	40,000	/10 以上	/23 以上

メンバーの検索フォームが公開されており、Extra large メンバーには、JPNIC、KRNIC、CNNIC、TWNIC など、各国の NIR が登録されている。

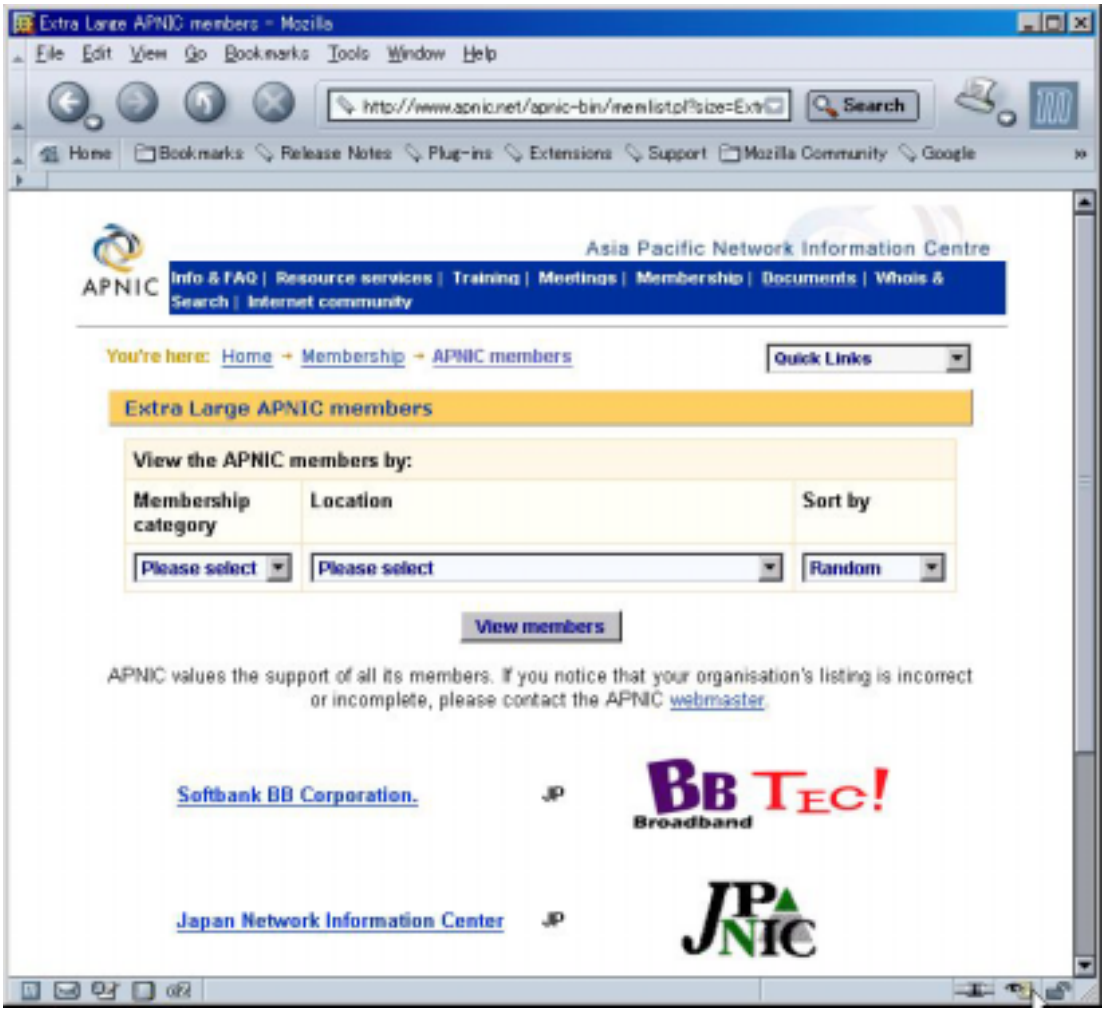

図 2-4 APNIC メンバー検索画面

RIR のメンバーである NIR と LIR は、アドレス資源の管理権限の委譲を受けると共に、そのアドレス資源のサイズに応じた費用を負担する。インターネットレジストリにおける収入は、ポリシー策定、レジストリシステムの運用、審議、教育といった活動費用に当てられ、継続的なアドレス資源の運用の財源に充当される。

インターネットで利用される各種アドレス資源は、論理的識別子であり、管理権限の割り振りによって物品の移動が伴わない。つまりインターネットにおけるアドレス資源の流通は、インターネットレジストリにおける各種手続きによって実現している。インターネットレジストリの活動の本質は、ユーザによる自律的で適切なアドレス資源の利用を目的とした、情報登録および後述する情報公開である。

（4） whois によるデータ公開

レジストリにおけるレジストリデータの公開には whois が用いられる[3]。これはサーバクライアントによる簡易検索を提供するものである。このプロトコルが策定されたのは 1982 年（RFC812 の公開年）のことである。当初は、ARPANET の利用者に関するディレクトリサービスとして、氏名、電話番号、メールアドレスなどを提供していた。

現在では、インターネットレジストリそれぞれが、保有するレジストリデータの公開手法として、whois サーバを運営し、必要に応じて whois クライアントによる問い合わせを受け付けるという方法を採用している。

whois サーバへの問い合わせは、ドメイン及びネットワークに障害が発生した際の連絡先の問い合わせなど、ネットワーク管理上の必要がある場合に行うことになっている。

[3] RFC954 NICNAME/WHOIS
http://www.ietf.org/rfc/rfc0954.txt?number=954

表 2-2 whois による問い合わせの例

```
% whois -h whois.nic.ad.jp www.nic.ad.jp

[ JPNIC & JPRS database provides information on network administration. Its   ]
[ use is restricted to network administration purposes. For further infor-    ]
[ mation, use 'whois -h whois.nic.ad.jp help'. To suppress Japanese output,   ]
[ add'/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.       ]

Domain Information: [ドメイン情報]
a. [ドメイン名]                NIC.AD.JP
e. [そしきめい]                しゃだんほうじん にほんねっとわーくいんふぉめーしょんせんたー
f. [組織名]                    社団法人 日本ネットワークインフォメーションセンター
＜省略＞
```

（5） JPNIC 割り振りの申請、審議、登録、情報公開

自組織のネットワークをインターネットに接続するためには、ネットワークアドレスの割り当て（assignment）を受ける必要がある。この割り当ては JPNIC から割り当て業務を委託されている IP アドレス管理指定事業者に対して申請を行う。

割り当てに先立って、IP アドレス管理指定事業者は JPNIC から管理するアドレスブロックの割り振り（allocation）を受ける。この管理の委託構造は図 2-5 のように表される。

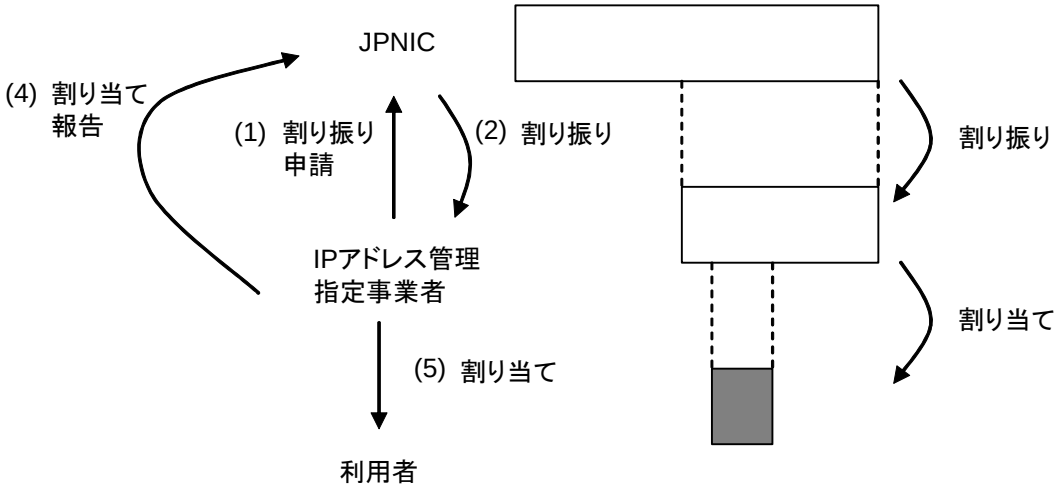

図 2-5 JPNIC における割り振り、割り当て概念図

なお、割り振り、割り当ての定義は表 2-3 のように示される。

表 2-3 割り振り、割り当ての定義

割り振り（Allocation） 　再分配用としてプロバイダ集成可能アドレス空間を IP アドレス管理指定事業者に分配することです。 割り当て（Assignment） 　IP アドレス管理指定事業者が割り振られたアドレス空間の一部または全部を、接続組織のネットワーク利用のために分配することです。また、IP アドレス管理指定事業者が自身のバックボーンネットワークや内部ネットワークとして使うときも割り当てられたアドレス空間と呼びます。 （JPNIC 用語集 http://www.jpnic.jp/ja/tech/glos-wa.html より）

利用者、IP アドレス管理指定事業者、JPNIC の三階層モデルを採用することで管理業務の集約化が図られ、アドレス資源管理の効率化が実現されている。

LIR である IP アドレス管理指定事業者は企業その他法人によって構成され、一般的に ISP（Internet Service Provider：インターネットサービスプロバイダ）と呼ばれる。ISP はインターネットを利用するための各種サービスを提供する。一方、NIR および RIR は、インターネットにおける公共性のあるインフラストラクチャーとして、継続的な運用を推進する役割を持つ。LIR に対するアドレスの割り振りに、審議が行われるのはこのためである。

2.1.1.2. IP アドレス管理指定事業者情報

IP アドレス管理指定事業者とは、IP アドレスの割り当て業務およびそれに付随する業務の一部（以下、IP 割り当て管理業務と呼ぶ）を JPNIC から委託された事業者のことである[4]。

ある組織が IP アドレス管理を行うために IP アドレス管理指定事業者として登録されるには、JPNIC との間に IP アドレス管理指定事業者契約を締結する必要がある。この契約により IP アドレス管理指定事業者となった場合には、IP アドレス管理指定事業者情報がレジストリデータとしてリポジトリに格納され、その一部は公開される。

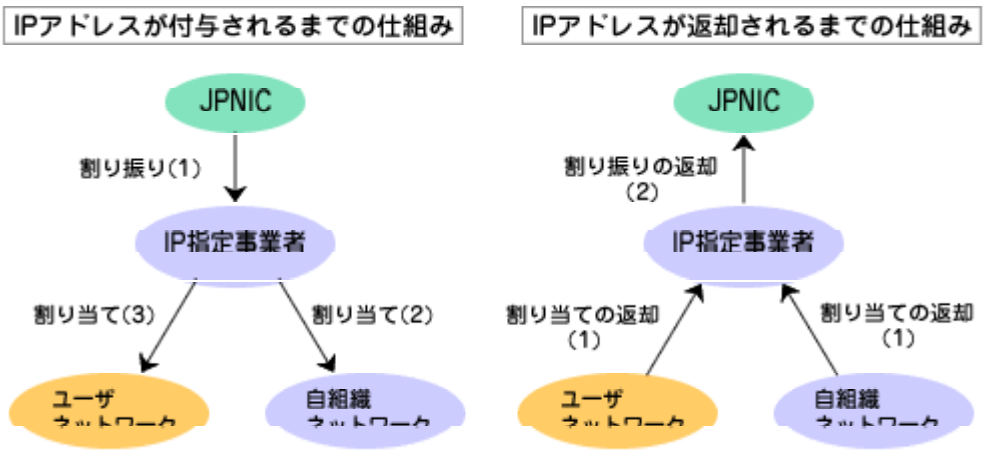

図 2-6 IP アドレス付与／返却の仕組み[5]

公開されるデータを表 2-4 に示す。

[4] IP アドレス管理指定事業者について
http://www.jpnic.jp/ja/ip/member/index.html
[5] IPv4 アドレスの申請
http://www.nic.ad.jp/ja/ip/ipguide.html

表 2-4 IP アドレス管理指定事業者データ

データ項目	概要
指定事業者名	指定事業者の正式名称。JPNIC 会員登録申請の際に登録されたもの。
指定事業者略称	指定事業者を一意に識別するための符号。
管理アドレスブロック	指定事業者が管理しているアドレスブロック
連絡先	電子メールアドレス
住所	一般利用者から指定事業者に関する問合せ等を受けた場合に紹介すべき連絡先
電話番号	同上
ファックス番号	同上

IP 管理指定事業者はインターネットレジストリの管理権限を委譲されているため、インターネットのサービス利用が可能である。RIR と NIR の契約関係と同時に NIR と LIR の契約（登録）関係があることは、アドレス資源の確実性を確保する上で重要である。

インターネットの自律的管理の場面では、アドレスの利用者を特定するために、RIR から NIR、NIR から LIR という風に、それぞれの登録の記録を確認していくことが可能である。

2.1.1.3. ネットワーク情報

JPNIC の技術文書「JPNIC-00820 公開・開示対象情報一覧[6]」によると、ネットワーク情報は次のように定義されている。

> インターネットリソースである IP アドレスを利用しているのがどの組織、 または個人であるかを示すための情報。組織名、または個人名が公開される。 組織、または個人を特定するための住所は、請求により開示される。

公開されるネットワーク情報を表 2-5 に示す。

[6] JPNIC-00820 公開・開示対象情報一覧
http://www.nic.ad.jp/doc/jpnic-00820.html

表 2-5 ネットワーク情報公開データ

データ項目	概要
IP ネットワークアドレス	ネットワークアドレス
ネットワーク名	ネットワークを表す、意味のある任意の文字列
組織名	ネットワークを運用する組織の正式名称
運用責任者	運用に対して責任を負う担当者の JPNIC ハンドル
技術連絡担当者	技術面で責任を負う担当者の JPNIC ハンドル
ネームサーバ	ネットワークアドレスに関するネームサーバ（/24 より大きなアドレスブロックの場合のみ）
通知アドレス	変更登録された場合に通知すべき電子メールアドレス
割り当て年月日	割り当てが行われた年月日
返却年月日	（返却されている場合）返却年月日
最終更新	データが更新された年月日

JPNIC のネットワークアドレスに関して、実際に検索できる情報は表 2-6 のようになる。

表 2-6 JPNIC の公開ネットワーク情報

項目名	データ
a. [IP ネットワークアドレス]	202.12.30.0
b. [ネットワーク名]	JPNICNET
f. [組織名]	社団法人日本ネットワークインフォメーションセンター
g. [Organization]	Japan Network Information Center
m. [運用責任者]	SN3603JP
n. [技術連絡担当者]	HK8068JP
n. [技術連絡担当者]	NM050JP
p. [ネームサーバ]	ns1.nic.ad.jp
p. [ネームサーバ]	ns2.nic.ad.jp
y. [通知アドレス]	system@nic.ad.jp
[割当年月日]	1995/11/17
[返却年月日]	
[最終更新]	2002/08/19 13:08:04 (JST)
	koreeda@nic.ad.jp

ネットワーク情報を検索することで、どの IP アドレスがどの団体によって管理されているのか、（公開されてはいない情報ではあるが）どのように使われているのかがわかる。本質的には、インターネットレジストリによる登録情報の維持と連携によって、アドレスの台帳といえるものが世界規模で構成できるはずである。ただし、インター

ネットの黎明期に行われていたインターネットの利用を促進するための利用といった経緯や、現行業務の証明性、または安全上の理由により、一元的な台帳になる状況は考えにくい。アドレス資源の台帳が、どのような性質の情報を保持し、また公開するべきかであるかを定義することは、本調査研究の課題でもある。

2.1.1.4. AS 情報

AS（Autonomous System：自律システム）は、経路制御の上で運用ポリシーを統一することのできるネットワークの範囲のことである。インターネットで経路情報を交換する AS は ASN（AS Number）と呼ばれる識別番号を持っている。ASN は IP アドレスと同様に世界で一意に行われる必要があり、インターネットレジストリが割り当て業務を行っている。ASN の割り当ての際に登録される情報は AS 情報と呼ばれる。

JPNIC の技術文書「JPNIC-00820 公開・開示対象情報一覧」によると、AS 情報は次のように定義されている。

インターネットリソースである AS 番号を利用しているのがどの組織、 または個人であるかを示すための情報。組織名、または個人名が公開される。 組織、または個人を特定するための住所は、請求により開示される。

公開される AS 情報は表 2-7 のようになる。

表 2-7 AS 情報公開データ

データ項目	
AS 番号	
AS 名	AS につける名称
組織名	ネットワークを運用する組織の正式名称
運用責任者	運用に対して責任を負う担当者の JPNIC ハンドル
技術連絡担当者	技術面で責任を負う担当者の JPNIC ハンドル
AS-IN	外部からの経路情報受け入れに関するポリシー
AS-OUT	外部へ広告する経路情報に関するポリシー
通知アドレス	変更登録された場合に通知すべき電子メールアドレス
割り当て年月日	割り当てが行われた年月日
返却年月日	（返却されている場合）返却年月日
最終更新	データが更新された年月日

表 2-8 は whois データベース上で公開される、JPNIC の所有する AS に関する情報である。

表 2-8 JPNIC 公開 AS 情報

データ項目	
a. [AS 番号]	2515
b. [AS 名]	JPNIC
f. [組織名]	社団法人 日本ネットワークインフォメーションセンター
g. [Organization]	Japan Network Information Center
m. [運用責任者]	SN3603JP
n. [技術連絡担当者]	NM050JP
n. [技術連絡担当者]	HK8068JP
o. [AS-IN]	from AS2500 10 accept ANY
o. [AS-IN]	from AS2497 10 accept ANY
p. [AS-OUT]	to AS2500 announce AS2515
p. [AS-OUT]	to AS2497 announce AS2515
y. [通知アドレス]	system@nic.ad.jp
[割当年月日]	1994/11/21
[返却年月日]	
[最終更新]	2002/08/19 13:08:15 (JST)
	ip-alloc@nic.ad.jp

AS はグローバルインターネットで経路情報を交換する組織の単位である。従って、IP アドレスの割り当てと AS による経路情報の交換に矛盾が生じると、膨大なアドレス資源の不正利用が可能になる。アドレス資源の不正利用は、追跡が不可能な通信ノードの設置を可能にし、広域における通信障害を故意に起こすことが可能な状況を作り出すことがある。

2.1.1.5. 割り当て情報

割り当て情報とは、割り当てられたネットワーク情報である。IP アドレス管理指定事業者が申請者に IP アドレスを割り当てる際には、JPNIC に対して、IP アドレス割り当て報告申請を行う必要が有る。JPNIC では、IP アドレス割り当て報告申請受理後に申請が適正なものであるかの審議を行い、適正であると判断された場合、申請内容をデータベースに記録し、申請を行った IP アドレス管理指定事業者に受理の返答を行う。

これらの情報を元にアドレス資源の管理を行うのがインターネットレジストリである。新たなアドレス資源の割り振りに伴う審議や、ネットワーク情報の公開などの活動は、すべて登録情報に基づいて行われている。すなわち登録情報はアドレス資源管理の元本となる情報である。

2.1.2. レジストリデータの保護

ここでは前節で示されたレジストリデータに関する脅威を明らかにし、保護すべき対象を示す。このために、それぞれのデータについて、発生から利用、消滅の過程を示し、セキュリティ上の問題を明らかにする。

2.1.2.1. 申請業務における認証業務と安全性

レジストリデータは申請とともに発生し、削除申請とともに消滅する。ここでは、申請の概要を示し、安全性の議論を行う。

現状の業務では、データの申請（および更新）は図 2-7 のように行われる。

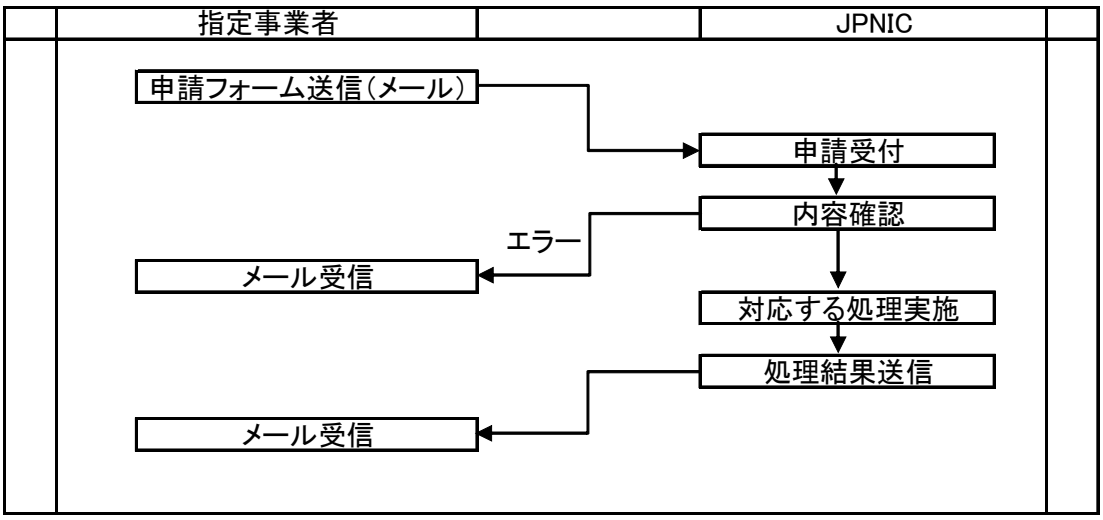

図 2-7 申請処理概要

JPNIC から提供される申請フォーム[7]は電子メールを使って送受信される。電子メールは盗聴や改ざんが可能な情報伝達手段である。保護機能のない電子メールを利用すると、虚偽の申請や不正な申請が行われる恐れがある。そのため JPNIC を含め、多くのインターネットレジストリではパスワードや暗号技術を利用したメールなど、保護機能の実現に取り組んできた。

多くのインターネットレジストリで取られてきた保護機能は authentication（認証）のスキームと呼ばれ、申請者自身が登録した認証情報（パスワードや暗号鍵）を使って当事者であることを確認する手法が使われてきた。しかし暗号の解読技術や巧妙な業務分析の手法が発展するに従って、より強固なユーザ認証方式が必要になってきた。

[7] http://www.jpnic.jp/ja/doc/validity.html 以下に配置されている

ここでいう強固なユーザ認証方式とは、単に暗号強度の高い方式であるだけでなく登録手続きやユーザ管理といった運用の面でも安全性に配慮した方式を意味している。例えば、Web ベースで申請業務を行うことを考えると、HTTPS を用いてクライアント認証を行うことが可能であるが、転送されるメッセージ（つまり申請）が予め登録されたユーザが作り出したものであるという関連付けをアプリケーションで行う必要がある。

電子メールベースの申請業務上で、認証を行うための現実的な手法として、PGP（Pretty Good Privacy[8]）を使ったメッセージ認証、S/MIME を使ったメッセージ認証などがあげられる。実際に RIPE NCC では PGP を使ったメッセージ認証を取り入れている。

RIPE NCC ではデータベースに RPSL（Routing Policy Specification Language）と呼ばれるルーティングポリシー記述言語を用いている。この言語は ARIN,APNIC においても使われており、RIPE NCC が採用している PGP を用いたメッセージ認証は、他組織においても参考となると考えられる。以下に、そのメッセージ認証について説明を行なう。

（1） RIPE NCC における PGP によるデータ保護

RIPE NCC のレジストリ操作は MIME 形式の電子メールを利用して行われる。この際に MIME の各パートに対し、PGP の署名を行い、データベースに登録する。

まず、データの登録を電子メールベースで行う[9]。コンタクト情報の登録作業は次のようになる。

（1） コンタクト情報登録テンプレートを作成する。
（2） テキストエディタで必須項目を記入する（nic-hdl 属性に「AUTO-1」、source 属性に「TEST」、changed 属性に記入者の電子メールアドレスを記入する（表 2-9））。
（3） 完成したテキストを test-dbm@ripe.net に送信する。
（4） 数分で TEST データベースから登録の可否と新しい nic-hdl が通知される。

[8] PGP Corporation
http://www.pgp.com/

[9] RIPE Database User Manual:Getting Started, 2.3.2 Registering contact information
http://www.ripe.net/ripe/docs/db-start.html

表 2-9 コンタクト情報登録例

データオブジェクト	データ
person	John Smith
Address	Example LTD, High street 12 St. Mery Mead Essex, UK
Phone	+44 1737 892 004
e-mail	John.smith@example.com
nic-hdl	AUTO-1
remarks	******************************
remarks	This object is only an example!
remarks	******************************
Changed	John.smith@example.com
Source	TEST

レジストリデータの操作が許されるオペレータは person オブジェクトのうち、mntner オブジェクトの所有者である。この mntner オブジェクトには、所有者の公開鍵情報を、key-cert オブジェクトとして格納することが許される。

このオブジェクトには、編集作業を認証するための公開鍵が格納される。現在、Open PGP[10] 準拠の鍵だけがサポートされている。

key-cert オブジェクトの構成は表 2-10 のように定義されている

[10] RFC2440 OpenPGP Message Format
http://www.ietf.org/rfc/rfc2440.txt?number=2440

表 2-10 key-cert オブジェクト

データオブジェクト	
key-cert	データベースに格納された公開鍵の識別子。PGPKEY-<ID>の形式で登録される。
method	公開鍵のタイプ。現在は PGP のみが認められる。
owner	公開鍵の所有者
fingerpr	公開鍵証明書のフィンガープリント
certif.	公開鍵（テキスト形式）
remarks	注釈
notify	通知アドレス
mnt-by	このオブジェクトの操作を認証するために使われる mntner オブジェクトの識別子。
changed	オブジェクトの最終更新者と最終更新日。
source	オブジェクトの登録先

key-cert オブジェクトの生成手続きは以下のようになる。

（1） GnuPG（Gnu Privacy Guard[11]） の鍵をファイルにエクスポートする

（2） gpg –list-keys の出力の中から自分の電子メールアドレスに対応するものを探し、Key ID を記録する（この ID に PGPKEY-を加えたものが key-cert ID となる）

（3） 鍵をエクスポートしたファイルをエディタで開き、各行の先頭に certif: を加える

（4） ファイルの先頭に「key-cert: PGPKEY-<自分の KeyID>」を加える

（5） ファイルの終わりに次の各要素を加える（mnt-by: changed: source）

（6） mntner オブジェクトがパスワードで保護されている場合には、パスワード要素を加える

（7） 作成されたファイルを auto-dbm@ripe.net に送信する

ここで作成されたファイル、つまり key-cert オブジェクトの属性は次のようになる。

[11] The GNU Privacy Guard – GnuPG.org
http://www.gnupg.org/

表 2-11 ker-cert 登録データ

データ項目	内容
key-cert	PGPKEY-XXXXXXXX
certif...	------BEGIN PGP PUBLIC KEY BLOCK------
certif...	Version: GnuPG v1.2.2(cygwin)
certif...	mQGiBEAfEesRBCCTD0koyPykQv/lJj4q7eSiZv62qVA794bWmeydTBT5nxNdzoGT
certif.	鍵の内容が続く
certif	-----END PGP PUBLIC KEY BLOCK-----
mnt-by	EXAMPLE-MNT
changed	john.smith@example.com 20020827
source	RIPE

作成された key-cert オブジェクトを mntner オブジェクトに結びつけるためには、mntner オブジェクトに表 2-12 の属性を追加する。

表 2-12 mntner オブジェクトに追加する key-cert ID

auth: PGPKEY-XXXXXXXX

結び付けられた公開鍵で更新するデータを署名する手続きは次のようになる。

（1） 更新データをファイルに保存する

（2） データファイルに署名する（gpg –clearsign データファイル）

（3） 出力ファイルを auto-dbm@ripe.net に送信する。

署名データは表 2-13 のようになる。

表 2-13 署名データ例

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

person: Adam Smith
address: RIPE NCC
address: Singel 258
address: 1016 AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 545 4445
e-mail: adam-example@ripe.net
nic-hdl: AUTO-1
notify: Adam-example@ripe.net
mnt-by: EXAMPLE-MNT
changed: ripe-dbm@ripe.net
source: RIPE
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.2 (Cygwin)

iD8DBQeAMb6kOSlVyjdJy2cRAtIGAJ9tBvs43L7YUbb9asWWccI7CLS2JQCeM5gR
pZkDih+FApJqYa38dSy+oF4=
=nv9y
-----END PGP SIGNATURE-----
```

つまり、公開鍵によるデータ編集者の認証と完全性を提供することが目的であり、経路の機密は提供されない。

2.1.2.2. ネットワーク情報、AS 情報、割り当て情報

登録情報の一部は whois サービスを利用してインターネット上で公開される。登録情報の確実性を向上させるため、認証、暗号化、完全性の検証、可用性の保証などといった安全上の対策の強化が求められている。

安全上の脅威が、レジストリデータのうち、ネットワーク情報、AS 情報、割り当て情報に与えるリスクについて述べる。

始めにこれらの情報に共通のリスクを述べ、後に個々の情報に関するリスクを述べる。

（1）　アドレス資源運用管理の阻害

インターネットが健全に運用されるためにアドレス資源の適正な管理が求められている[12]。このアドレス資源の管理が阻害された場合に考えられるリスクを表 2-14 にあげる。

表 2-14 アドレス資源運用管理上のリスク

問題	リスク
アドレス資源の利用状況の把握不可能	アドレスの枯渇 偏ったアドレス利用の発生(ネットワーク/ISP 的偏り) 地域レベルでのアドレス資源管理負荷の増大
追跡不可能な通信ノードのなりすまし	登録されたネットワーク利用組織と異なる組織の利用による連絡と原因追跡の不能状況の発生 不能となるサービスで発生する損害
特定不可能なアドレス資源の不正利用(将来的に IRR との連動があるケース)	割り当てられていないアドレスブロックの利用によるネットワークの不正利用 不正利用によって阻害されたサービスで発生する損害

（2）　自律的運用の阻害

JPNIC では、独自のポリシーに基づいてリポジトリ業務を運営している。データベース公開についても例外ではなく、公共の資源として、正しく活用されるための努力を行なっている[13]。

しかし、不正な手法によるデータベースの改ざん、成りすましなどにより、自律的運用のための適切な連絡活動が阻害される危険性がある。適切な連絡活動ができないと、DNS サーバの設定などの運用が阻害されたり、不正アクセスの対応に大きな遅れが発生したりする。表 2-15 に、そのリスクをまとめる。

12 IPv4 アドレスの審議について
http://www.nic.ad.jp/ja/ip/eval.html
13 JPNIC データベースの情報公開について
http://www.nic.ad.jp/ja/db/dbpi/index.html

表 2-15 自律的運用の阻害におけるリスク

問題	リスク
不本意な連絡活動の発生（DNS の運用、不正アクセス）	登録された組織の信頼性･社会的地位の劣化 登録情報の目的外利用(書き換えによる営利用途等) 本来業務の阻害による間接的被害 紛争等直接経費

（3） DNS の運用阻害

DNS はインターネットを支える重要な基盤技術である。JPNIC では、IP アドレスからホストネームを引くための逆引きネームサーバを運用している。データの改ざんなどにより､誤ったレコードの提供が引き起こすリスクについて表 2-16 にまとめる。

表 2-16 DNS 運用阻害のリスク

問題	リスク
逆引きネームサーバの運用阻害 （ISP と APNIC,JPNIC の DNS サーバで、間違ったレコードが提供される）	多様な他のサービスに使われる DNS サーバの運用に障害をきたす。 メールの配送に支障 SSL 等の利用に支障 クレームケース:本来業務の阻害による間接的被害 クレームケース：紛争等直接経費

以下では情報別のリスクについて議論する。

（4） ネットワーク情報

ネットワーク情報とは 2.1.1.3 で述べたように、IP アドレスを使用している組織、個人に関する情報である。この情報の利用目的には次のものがあげられる。

- 割り振り／割り当て済みアドレスの確認
- ネットワークトラブルの解決
- 登録情報の確認

IR が管理するネットワークブロックについて効率的な割り振り／割り当てを行うためには、使われているブロックの分布状況を正確に把握していなければならない。

このためにネットワーク情報が使われている。

盗聴が行われた場合のリスクについては、公開情報であるため、特段のものはないと考えられる。

なりすましが行われた場合､つまり whois サーバが偽のサーバに代わられた場合と、改ざんが行われた場合とは、意図的な情報が渡されるという点で同じ状況と考えられる。さらに、サービス不能攻撃が行われた場合を考えると、必要なときに正しいデータを参照できないことになる。このことから考えられるリスクを以下にあげる。

ネットワーク情報の割り振り／割り当て要求を行う全てのサービス事業者が、ネットワーク情報の提供に関して、ある程度の障害時間を見込んでいるのであれば、短時間のサービス不能状態は許容できるといえるが、その保証は無く、ネットワーク情報提供サービスの中断が長い時間にわたった場合の影響は大きいと考えられる。

ネットワークトラブルが発生した場合、つまり、あるホストから不正なパケットが送られた、あるネットワークが到達不能となったなどの際に、トラブル解決の糸口として、運用責任者及び技術責任者に電子メールまたは電話などで連絡をとる必要性がある。この際に、ネットワーク情報中のコンタクト情報を用いる。

なりすまし及び改ざんが行われた場合、存在しない連絡先が示される場合と、別の連絡先が示される場合が考えられる。前者の場合、問題の発生しているネットワーク側の対処が自発的に行われるまでトラブルが解決しないため、ネットワークの切断という自体に発展する恐れがある。後者の場合、第三者にトラブル情報を公開してしまう危険性がある。

盗聴が行われた場合のリスクについては、ネットワーク情報の検索及び提供そのこと自体に機密性は無いので、特段の問題は無いと考えられる。しかし、ネットワークトラブル情報には機密情報が含まれる可能性が高いので、コンタクト先とのやりとりには注意が必要となる。

サービス不能攻撃が行われた場合、これは改ざんが行われ、トラブル発生元と連絡が取れない状態と同じことになる。

運用責任者及び技術責任者は自分たちが利用しているネットワークに関する情報が whois で正しく提供されていることを確認し、間違いがあればただちに訂正する、また変更があればただちに変更申請を行うことが求められている。このためには whois を用いて登録情報の確認を定期的に行う必要がある。

（5） AS 情報

AS 情報とは 2.1.1.4 で述べたように、AS を使用している組織、個人に関する情報

である。「JPNIC における AS 番号割り当てに関するポリシ[14]」によれば、この情報の利用目的には次のものがあげられる。

- 一意性の保証（割り当ておよび割り振られた AS 番号空間が世界でただひとつしかないことを保証する）
- 登録（一意性を保証するとともに、トラブル時の参照情報として利用するため）
- 効率的な利用（限られた資源を効率的に利用するため）
- 公平性（いかなる要因に左右されることなく公平に適用されるべきである）

AS 番号自体は運用ポリシーを持ったネットワークのかたまりを識別するためにつけら、BGP（Border Gateway Protocol、AS 同士で経路情報を交換するための外部経路制御プロトコルの一種）を利用して他の AS へ経路制御する際に用いられる。

もし、他 AS の所有する AS 番号を詐称したとしたら、経路情報に本来の状態との齟齬が生じることとなり、正常な経路制御が行えない可能性がある。また、割り振られたが割り当てられていない AS 番号、割り振られていない AS 番号を勝手に使い、経路情報を広告したらどうなるだろうか。これは接続する先の AS の運用状況にもよるが、将来、その AS 番号の正当な所有者が現れた際に混乱の元となるだろう。

実際に、このような割り当てが行われていないはずの AS 番号を含んだ経路情報が広告されていることが観測されている[15]。

AS 番号を用いた経路制御は、インターネットの中核技術の一つである。AS 番号を正しく管理、運営するためには、成りすまし、改ざんの脅威を取り除かなければならない。

AS 情報の登録と公開を行う機能である IRR（Internet Routing Registry）の役割は大きいため、今後、安全性について検討が進められると考えられる。

（6） 割り当て情報

割り当て情報とは 2.1.1.5 で述べたように、割り当てられたネットワーク情報である。

この情報に関するリスクはネットワーク情報と同じものになると考えられる。

---

[14] JPNIC における AS 番号割り当てに関するポリシ
http://www.nic.ad.jp/doc/jpnic-00890.html

[15] General Routing Registry Consistency Check Report
http://rrcc.ripe.net/RRCC_general_report.html

2.1.2.3. 提供する際（whois）と安全性

レジストリデータの提供手段として使われるプロトコルは RFC954 NICNAME/WHOIS で策定されている whois プロトコルである。

このプロトコルは単純な検索を実現するもので、TCP コネクション確立後、クライアントから検索文字列が送信され、サーバはこれをキーとした検索結果を送り返す、といったものとなっている。

このプロトコルでは、認証、機密、完全性といったセキュリティ機能が提供されていない。

whois データ、特にネットワークの運用担当者、技術連絡担当者の正確性は、ネットワークインシデント解決に重要なデータである。正しいサーバから正しいデータを受け取る必要があるが、これを脅かすリスクとして次のようなものが考えられる。

（1） なりすまし

whois クライアントはサーバを認証する機能を持たないため、whois サーバが本来のものであるのかどうかを判断することができない。

例えば whois サーバがドメインネームで指定された場合、DNS データの改ざんにより不正なサーバへクライアントが誘導されるリスクが存在する。また、一部のクライアントではデフォルトの　whois サーバが埋め込まれており、ソースコード改ざんにより、不正サーバへ誘導されるリスクが存在する。

なりすましを防止するためには、サーバ認証を実施しなければならない。なお、そのためには認証に必要な鍵の配布などの仕組みが必要になる。

（2） 盗聴

一般に whois でやりとりされるデータは公開データであり、機密性は無い。このために盗聴による情報漏えいのリスクは無いと考えられる。

（3） データ改ざん

転送経路が保護されていないため、第三者中継によるデータ改ざんのリスクが存在する。データ改ざんを防止するためには、元のデータに署名を行う方策が有効である。

（4） サービス不能攻撃

サービス不能攻撃によるリスクは、サービスのリアルタイム性が重要であるほど高いものとなる。whois サービスを参照する他のサービスにはリアルタイムと言うほど

の高い頻度で問い合わせを行うものは無いと考えられるが、whois のデータ登録件数は、数十万、数百万といったオーダーに達するため、データの参照自体は常に行われていると考えられる。

それらの参照に対する whois サーバの遅延がどれほどの影響を与えるのか、正確に判断することは難しい。しかし、本来の whois の機能が失われないためにはサービス不能攻撃に対する十分な対処が必要である。

JPNIC の whois サーバは、一定時間に一定量以上のアクセスがあると該当のクライアントに対しての返答を遅らせる仕組みが導入されている。またサーバのクラスタリング等の対策方法もある。

2.1.2.4. 申請業務におけるデータ保護

レジストリデータは申請とともに発生し、削除もしくは解約申請とともに消滅する。ここでは以下にあげる主要な申請業務について、現行業務を抽象化した手続きフローを図示し、業務手続きにおける問題点を明らかにする。

- IP アドレス割り振り申請
- 割り当て報告申請
- 個人情報登録/変更
- 指定事業者契約/解約
- ネットワーク記載事項変更申請
- IP 指定事業者情報変更申請

ここでは申請業務における安全性をいくつかの典型的な攻撃を想定して検討を行う。典型的な攻撃とは、なりすまし、盗聴、改ざん、サービス不能攻撃である。電子メールを利用したアドレス資源管理の申請業務において考えられるリスクについて以下に述べる。なお JPNIC ではパスワードや PGP を利用した保護機能を実現しつつある。

なりすましの例として、IP アドレス管理指定事業者のふりをして不正に IP アドレス割り振りの申請を行ったとする。割り振られたアドレスブロックは IP アドレス管理指定事業者によって管理されないため、（不正な）利用状況について把握することができない。そのアドレスブロックで問題が発生したとしても、連絡先がわからない。実際には、不正に割り振られたアドレスブロックを運用することは困難であるため、実用上の特別な問題が発生する可能性は高くはないが、そのアドレスブロックは再利用困難であり、アドレス資源の損失となる。

申請情報の盗聴のリスクは、送信される情報の機密性による。申請情報の中には whois を使って公開されない情報が含まれており、本来公開されるべきでない情報が漏洩する危険性がある。JPNIC では IP アドレスの割り振り審議の際に、ネットワー

クプランと呼ばれるネットワークの詳細情報を利用する。ネットワークノードの数を予測するため、顧客の統計に関する情報が必要になったりネットワークトポロジーがわかる情報が審議のために必要になったりする。IP アドレス管理指定事業者にとっての情報漏えいが、申請情報の機密性に関するリスクである。

サービス不能攻撃については、リアルタイム性が求められる情報については、リスクが存在する。しかし、週に一度の変更、月に一度の変更が行われればよい情報などでは、リスクは存在しつつも大きいものとはいえない。

一般に、脅威から生じるリスクの重大性は、リスクの大きさに蓋然性（possibility）を乗じたものとして評価される。リスク対策には相応のコストが要求されるため、制約の中で対策可能なリスクに重点的に対処し、大きなリスクであっても蓋然性が極めて低いものについては、たとえば保険などでリスクを転化することで、制約の範疇に収めることが考えられる。

以下に個別の申請業務の概要を示し、現状の体系の中で考えられるリスクを指摘する。

（1） IP アドレス割り振り申請

この手続きは、IP アドレス管理指定事業者が、新規の IP アドレスブロックの割り振りを JPNIC に申請するためのものである。

現行業務は図 2-8 のように示される。

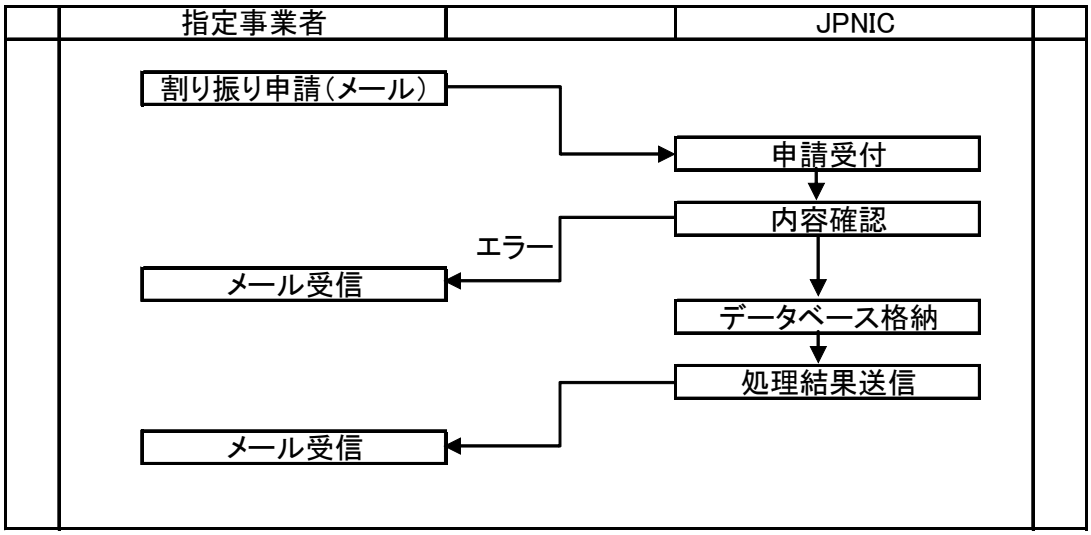

図 2-8 IP アドレス割り振り申請手続きフロー

（1） IP アドレス管理指定事業者から電子メールにて割り振り申請が送られる
（2） JPNIC では申請内容を確認し、問題があればエラーをメールで通知する
（3） 問題が無ければ申請を受理し、データベースにデータを格納する
（4） 処理の結果をメールで申請者に送信する

割り振り申請フォームに記載される内容は表 2-17 のようになっている[16]。

表 2-17 割り振り申請フォーム

番号	項目名	概要
a.	会員略称	申請を行なう IP アドレス管理指定事業者の会員略称。
b.	接続性	どのようにインターネット接続を行なうのかを表す数字。Internet eXchange（相互接続点：以下、IX）経由、ISP 経由、それ以外などの接続形態が示されている。
c.	接続先	接続先が IX または ISP の場合、その事業者名。IP アドレス管理指定事業者の場合は会員略称を記載する。
d.	Addr-3mo	3ヵ月後の IP アドレス管理指定事業者の累計割り当て済みアドレス空間に関する予測値。
e.	Addr-6mo	6ヵ月後の IP アドレス管理指定事業者の累計割り当て済みアドレス空間に関する予測値。
B.	Network-plan	IP アドレス管理指定事業者自身が構築するインフラネットワークで、今後 1 年間で新規に構築するネットワークの詳細情報。
D.	Old-network	IP アドレス管理指定事業者自身が構築するインフラネットワークとして割り当てられたアドレスで構築している、現在のネットワークの構成。

割り振り申請業務において、考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により割り振りに支障を来たし、指定事業者のアドレスブロックが一時的に枯渇し、申請者に対する割り当てが行えない。

（2） IP アドレス割り当て報告申請

この申請は、IP アドレス管理指定事業者が、IP アドレス利用者にアドレスブロッ

[16] IP アドレス管理指定事業者の IP アドレス割り振り／返却申請フォーム
http://www.nic.ad.jp/doc/jpnic-00865.html

クを割り当てる際に、事前の審査を受けることを目的として、「IP アドレス割り当て報告申請フォーム(ユーザネットワーク用)」を JPNIC に提出する。

IP アドレス割り当て報告申請は、表 2-18 のように定義される。

表 2-18 IP アドレス割り当て報告申請

JPNIC から委託を受けた CIDR ブロック内の IP アドレスの割り当てを行ったときは、JPNIC データベースへの登録が必要となります。割り当て報告申請により、割り当てに関する情報は「ネットワーク情報」として JPNIC データベースへ登録されます。IP アドレス割り当て報告申請は、IP アドレス管理指定事業者ネットワーク用とユーザネットワーク用で必要な項目が異なります。（http://www.nic.ad.jp/ja/ip/ipguide-m.html）

この申請フォームには、割り当てを行うネットワーク情報と、そのネットワークに関する連絡先個人情報を記入する。

現行業務は図 2-9 のように示される。

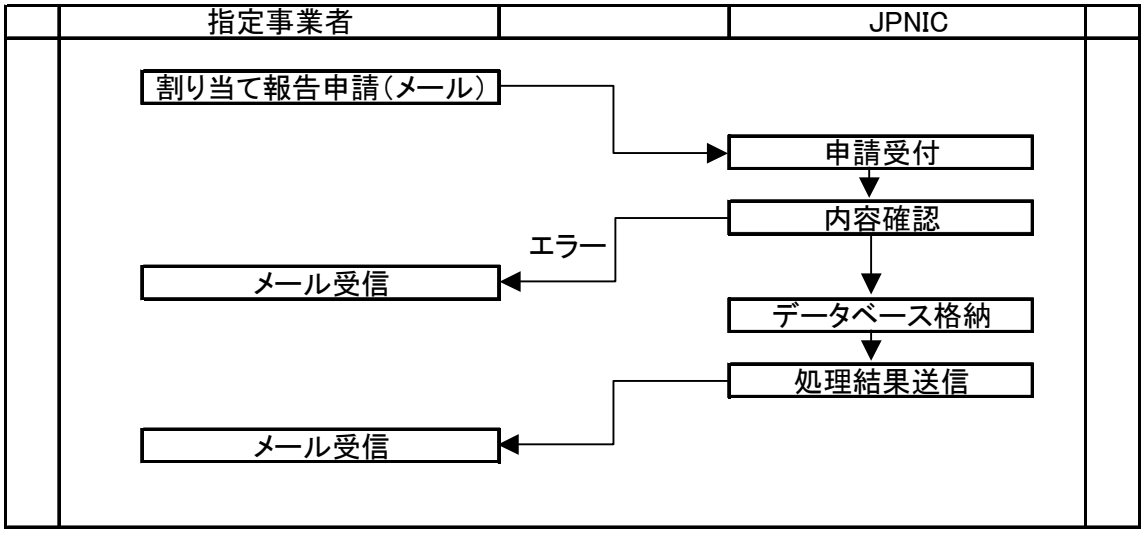

図 2-9 IP アドレス割り当て報告申請フロー

割り当て報告申請フォームに記載される内容は表 2-19 のようになっている[17]。

[17] IP アドレス割り当て報告申請フォーム(ユーザネットワーク用)
http://www.nic.ad.jp/doc/jpnic-00889.html

表 2-19 割り当て報告申請フォーム

番号	項目名	概要
a.	IP ネットワークアドレス	割り当てを行う IP ネットワークアドレス
b.	ネットワーク名	ネットワークを表す任意の文字列。
c.	組織名	ネットワークを運用する会社、組織などの正式名称
H	郵便番号	組織が所在する住所の郵便番
i.	住所	組織が所在する住所
m.	運用責任者	割り当てられる IP アドレスを使用する組織の責任者の JPNIC ハンドル。
n.	技術連絡担当者	割り当てられる IP アドレスを使用するネットワークに関する技術的、事務的などの全般的な問い合わせに対応する人の JPNIC ハンドル。
p.	ネームサーバ	/24 より大きなネットワークで、逆引きサーバの指定を行なう場合に記述する。詳しくは「ドメインネームサーバの設定手続きについて（http://www.nic.ad.jp/doc/jpnic-00886.html）」を参照。
y.	通知アドレス	ネットワーク情報が変更登録された場合に、通知すべき電子メールアドレス。
B.	Network-plan	新規に構築するネットワークの詳細情報をサブネット毎に記入する。
D.	Old-network	現在、割り当てを受けているアドレスで構築しているネットワークの構成をサブネット毎に記入する。
E.	審議番号	審議依頼を行ったネットワークに対する割り当て時のみ、審議申請の際に承認された審議番号を記入する。
F.	会員略称	IP アドレス管理指定事業者である場合には、JPNIC 会員情報の a.[会員略称]を記入する。

割り当て報告業務において考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい（住所などの個人情報を含んでいる）
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により割り当て報告に支障を来たし、逆引きネームサーバが登録されない

（3） 個人情報登録／変更

この申請は担当者の情報を登録または変更する手続きである。担当者の情報は、JPNIC ハンドルという識別子を利用している。

現行業務は図 2-10 のように示される。

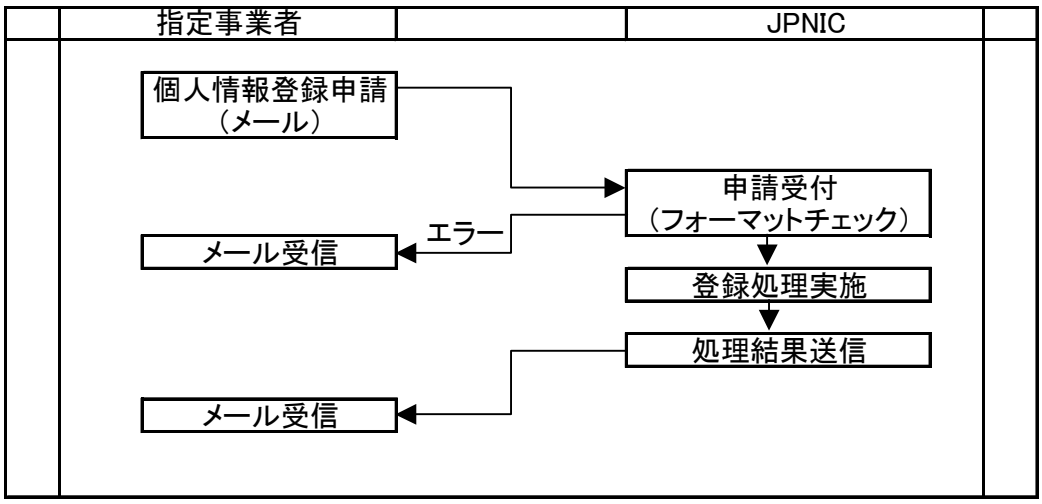

図 2-10 個人情報登録申請手続きフロー

同様に、個人情報変更に関する現行業務は図 2-11 として示される。

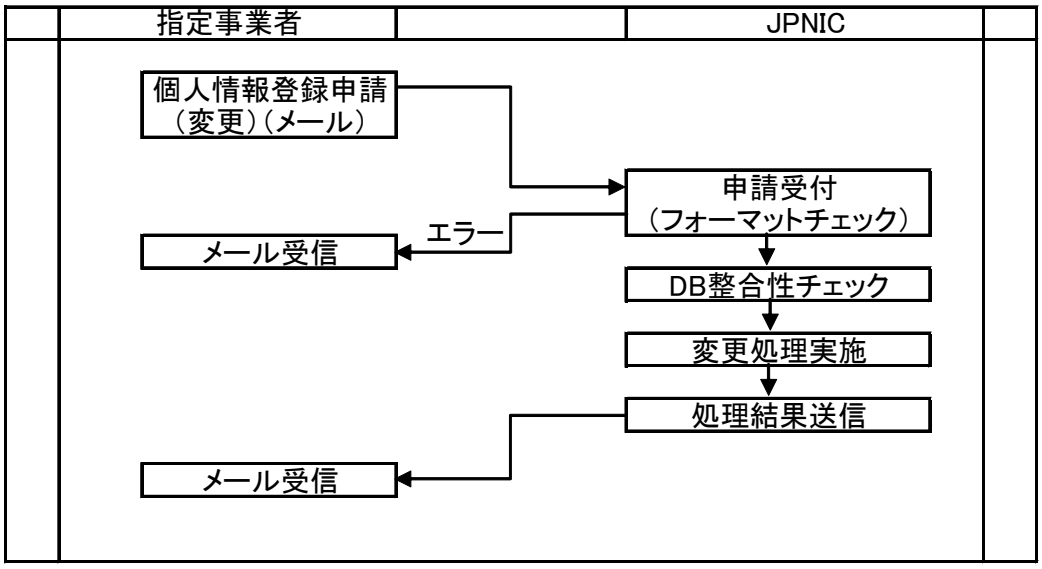

図 2-11 個人情報変更申請手続きフロー

申請フォームに記載される内容は表 2-20 のようになっている[18]。

表 2-20 個人情報登録申請フォーム

番号	項目名	概要
a.	JPNIC ハンドル	すでにデータベースに登録されている場合にはその JPNIC ハンドル、登録されていない場合には任意の数字
b.	氏名	登録する個人名
c.	Last, First	氏名のローマ字表記
d.	電子メイル	登録する個人の電子メールアドレス
f.	組織名	個人が所属する組織の正式名称
g.	Organization	組織名の英語表記
h.	郵便番号	登録する個人が所属する組織住所の郵便番号
i.	住所	登録する個人が所属する組織住所
j.	Address	住所の英語表記
k.	部署	登録する個人が所属する組織中における部署名
l.	Division	部署の英語表記
m.	肩書き	登録する個人が所属する組織中における役職名
n.	Title	肩書きの英語表記
o.	電話番号	登録する個人が所属する組織の電話番号
p.	FAX 番号	登録する個人が所属する組織の FAX 番号
y.	通知アドレス	登録する個人情報が変更された時に通知する電子メールアドレス

個人情報登録申請業務において考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な情報変更
- 電子メールアドレス、電話番号、FAX 番号など、連絡に必要な情報を改ざんすることで、サイトに問題が行った際に、運用責任者、技術連絡担当者に連絡をすることができないようにする。

（4） 指定事業者契約／解約

IP アドレス割り当てを行うためには、JPNIC との間に IP アドレス管理指定事業者

[18] JPNIC データベース 登録・変更ガイド：一般向け
http://www.nic.ad.jp/doc/jpnic-00869.html

契約を締結し、IP アドレス管理指定事業者とならなければならない。

この契約作業は図 2-12 のように実施される。

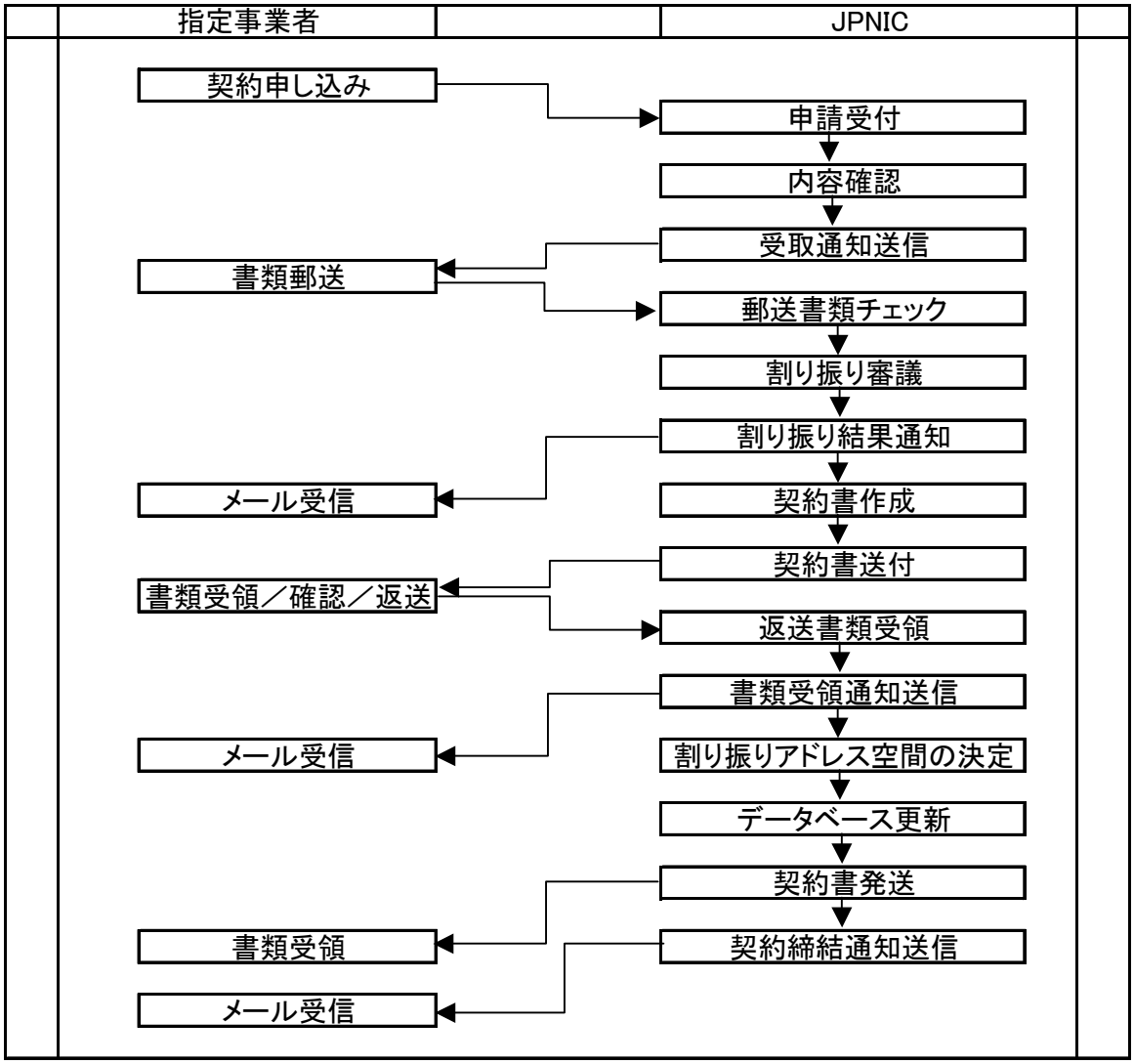

図 2-12 IP アドレス管理指定事業者契約フロー

提出書類として、表 2-21 の書類が指定されている[19]。

[19] IP アドレス管理指定事業者について
http://www.nic.ad.jp/doc/jpnic-00883.html

表 2-21 IP アドレス管理指定事業者契約提出書類

書類	提出方法
IP アドレス管理指定事業者契約申込書	電子メール
[JPNIC 会員情報](指定事業者情報)初期登録情報	電子メール
ネットワークの運用規約あるいはそれと同等のもの	電子メール
接続先確認フォーム	電子メール
初期割り振り要件確認フォーム	電子メール
法人の登記簿謄本	書面
代表者印の印鑑証明書	書面

IP アドレス管理指定事業者と JPNIC のやり取りは、郵便及び平文の電子メールで行なわれる。他の申請業務と異なっているのは、機密性（プライバシー）を有する重要な情報については書面での申請となっており、書面と電子メールを比較することで、なりすまし、改ざんなどの脅威を防止することができる点にある。

このため、考えられるリスクは次のものとなる。

- 電子メール伝達経路の盗聴による情報漏えい（初期登録情報には、申請手続き担当者電子メールアドレスなどの非公開データが含まれる）

（5） ネットワーク記載事項変更申請

ネットワーク記載事項の変更申請は「ネットワーク情報記載事項変更申請について」[20]にて示されるように、「IP アドレス割り当て後にネットワーク名、組織名、住所、運用責任者を変更する」行為である。

この操作の手続きは図 2-13 として示される。

[20] ネットワーク情報記載事項変更申請について
http://www.jpnic.jp/doc/jpnic-00407.html

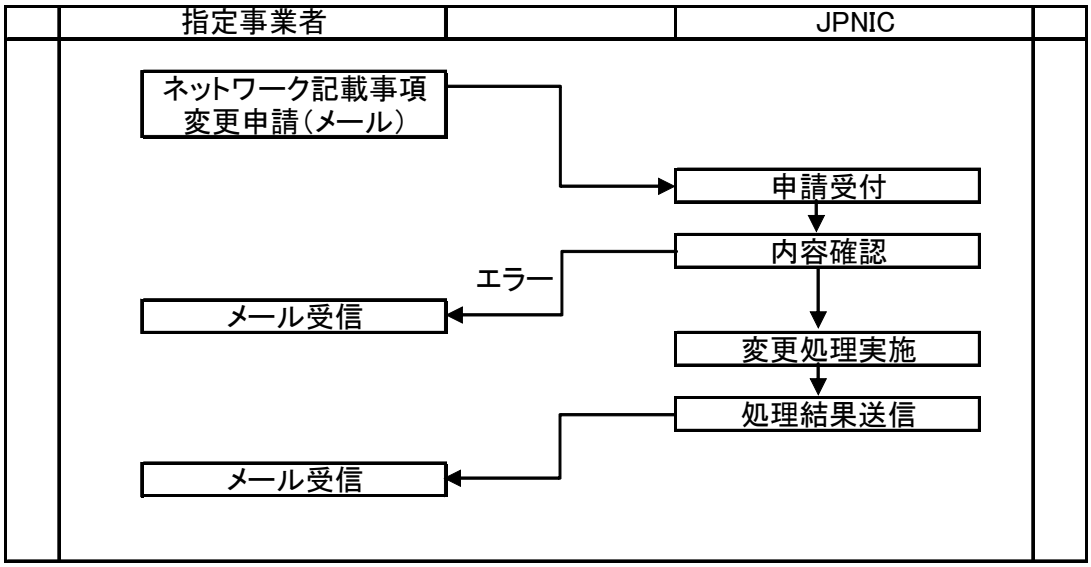

図 2-13 ネットワーク記載事項変更フロー

申請を行うフォームの記入例として表 2-22 が示される[21]

表 2-22 ネットワーク記載事項変更申請記入例

```
------------------------------------------------------------------------
# CHANGE TEMPLATE V 1.1 #
Current Network Information: [ネットワーク情報]
a. [IP ネットワークアドレス]      192.0.1.0/25
b. [ネットワーク名]               ABC-DUP-NET
f. [組織名]                       学術広帯域ネット協議会
g. [Organization]                 Academic Broadband Conference
h. [郵便番号]
i. [住所]
j. [Address]
m. [運用責任者]                   ABOOOJP
n. [技術連絡担当者]               ABOOOJP
p. [ネームサーバ]
y. [通知アドレス]                 ichiro@abc.ne.jp
```

[21] ネットワーク情報記載事項変更申請フォーム
http://www.jpnic.jp/doc/jpnic-00417.html

```
Network Information: [ネットワーク情報]
b. [ネットワーク名]
f. [組織名]
g. [Organization]
h. [郵便番号]                    101-0047
i. [住所]                        東京都　千代田区　内神田 2-3-4
j. [Address]                     2-3-4, Uchikanda, Chiyoda-ku,
                                 Tokyo 101-0047, Japan
m. [運用責任者]

[変更理由]

本社移転に伴う住所変更のため。

[備考]
------------------------------------------------------------------------
```

ネットワーク記載事項変更申請の申請業務については、次のリスクが考えられる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により情報変更に支障を来たし、サイトに問題が行った際に、運用責任者、技術連絡担当者に連絡をすることができない

（6） IP アドレス管理指定事業者情報変更申請

この手続きについては「指定事業者情報登録ガイド[22]」に詳細が記載されている。指定事業者情報については、変更する情報種類によって申請方法が分かれている。

会員名、運用組織名、運用責任者名が変更される場合には、届出書類を作成し、名称の変更を証明する登記簿謄本等を同封した上、書面のまま JPNIC に送信する。

それ以外の情報の変更については電子メールでの変更申請が行われる。

この手続きは図 2-14 のように示される。

[22] 指定事業者情報登録ガイド
http://www.jpnic.jp/doc/jpnic-00861.html

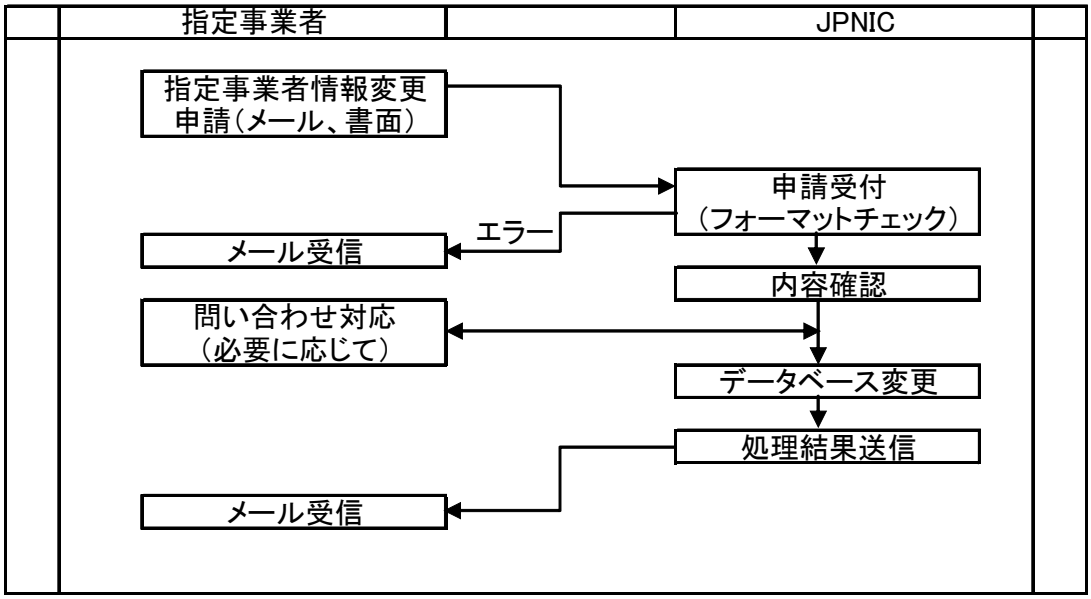

図 2-14 IP アドレス管理指定事業者情報変更申請フロー

書面での変更申請事項は郵送方法に依存した安全性になる。電子メールで変更申請される情報は表 2-23 のものとなる。

表 2-23 IP アドレス管理指定事業者情報のうち電子メールで変更申請される情報

番号	項目名	概要
a.	会員略称	指定事業者略称のこと。指定事業者を一意に識別するための符号として用いる。
g.	郵便番号	一般利用者から指定事業者に関する問い合わせを受けた場合に紹介すべき連絡先
h.	住所	同上
k.	FAX 番号	同上
l.	電子メイル連絡先	
m.	URL	指定事業者に関する情報を掲載する WWW ページの URL（RFC1738 形式）
o.	技術連絡窓口	指定事業者の技術担当者の電子メールアドレス 複数人の場合にはメーリングリストを作成することが望まれる
p.	事務連絡窓口	指定事業者の事務担当者の電子メールアドレス
q.	経理連絡窓口	指定事業者の経理担当者の電子メールアドレス
t.	DB 登録	JPNIC に対して指定事業者として申請手続きを行う担当者の電子メールアドレス
y.	通知アドレス	この情報が変更された場合に通知すべき電子メールアドレス
I.	技術連絡担当者	技術連絡担当者一名の電子メールアドレス
J.	事務連絡担当者	事務連絡担当者一名の電子メールアドレス
K.	経理担当者	経理連絡担当者一名の電子メールアドレス

これらの情報については以下のリスクが考えられる。

- 電子メール伝達経路の盗聴による情報漏えい（住所などの個人情報を含んでいる）
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な連絡担当者の変更

2.1.2.5. レジストリ間データ交換時のデータ保護

ここでは RIPE NCC と APNIC がリポジトリデータベースの同期に用いているスキームの概要を示し、安全上の問題について考察する。

はじめに RIPE NCC が用いている NRTM（Near Real Time Mirroring）について示し、次に APNIC におけるデータ同期スキームを示す。最後に whois を代替する目的で開発されている CRISP（Cross Registry Information Service Protocol）の概観

について示す。

（1） RIPE NCC における whois データベース同期スキーム（NRTM）

RIPE NCC では、レジストリ間 whois データベース同期スキームとして、NRTM が使われている[23]。RIPE NCC データベースのミラーサイトに参加するためには、NRTM によるデータベースを実施する必要がある。

NRTM は、差分更新により、データ転送量を減らす目的で作成された。その手法は、データ更新（追加、削除）のたびにシーケンス番号をインクリメントし、データ同期要求の際には、前回同期した際のシーケンス番号から、現在のシーケンス番号の間に実施された変更操作を転送するというものである。図 2-15 に、この概念が表される。

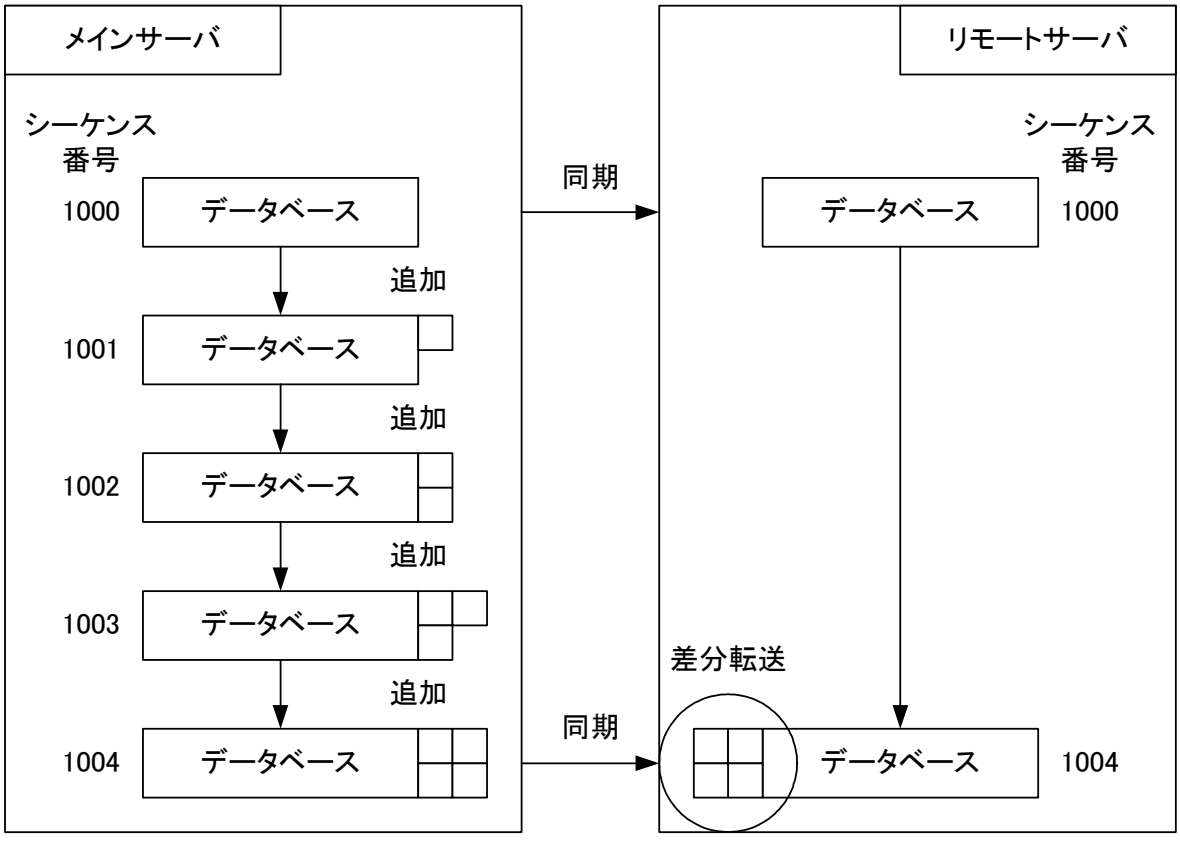

図 2-15 NRTM における差分更新概念

[23] ripe-252 RIPE Database Reference Manual
http://www.ripe.net/ripe/docs/databaseref-manual.html

NRTM では、ミラーサイトからの要求に応じて、マスターサイトからデータが送られる、プル方式を採用している。RIPE NCC のデータベースに対し、シーケンス番号 1539595 から 1539597 までのデータ転送を要求するメッセージは表 2-24 のように表される。

表 2-24 NRTM メッセージサンプル

```
%START Version: 2 RIPE:1539595-1539597
ADD

＜データオブジェクト＞

DELETE

＜データオブジェクト＞

%END RIPE
```

このプロトコル自身ではセキュリティ機能は用意されていない。このため、次のリスクが考えられる。

表 2-25 NRTM で考えられるリスク

セキュリティ機能	考えられるリスク
認証の欠如	なりすましによる認められていないミラーサイトによるデータベースの取得
機密性の欠如	データベース中のデータが、すべて無制限に公開されているわけではないため、第三者への情報漏洩が発生する
完全性の欠如	データ転送過程における改ざんの発生
可用性の欠如	過負荷によりマスターサイトがダウンする危険性がある

特に問題といえるのは第三者中継によるデータ改ざんである。NRTM では、差分方式をとっているため、いったん改ざんされたレコードの正当性が検証される機会は、プロトコル上は存在しない。このため、改ざんされたレコードが提供されつづける可能性がある。

この問題を回避するためには、データに電子署名を行う、保護されたチャンネル上で転送を実施するなどの解決策が考えられる。RIPE NCC のデータベースでは、PGP によるユーザ認証を実施しているので、この鍵を使って電子署名を実現することが考えられる。しかし、NRTM を実施している主体は RIPE NCC と他のインターネット

レジストリであり、電子署名を実施する主体のデータ所有者（ISP や EE など）に電子署名を強制する権限は無いものと考えられる。

このため、実際には転送チャンネルを保護することになるであろう。SSH や SSL/TLS といった暗号通信プロトコルを用いるのがコスト的にも適していると考えられる。ホスト同士が個別に認証を行う場合、互いの公開鍵を安全に交換することが必要になる。ミラーサイトの数が多くなった場合には PKI（Public-Key Infrastructure、公開鍵基盤）の導入を検討することになると考えられる。

（2） APNIC におけるデータ同期スキーム

APNIC では各 NIR との間で DNS の逆引きゾーンデータファイルと whois データベースを同期させている。

DNS の逆引きゾーンファイルは、それぞれの NIR の ftp サイトに次のようなディレクトリとファイルを用意することで公開されることが定められている[24]。

- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>
- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>.md5
- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>.asc

実際に、APNIC の管理する逆引きゾーンファイルは ftp://ftp.apnic.net/pub/zones 以下で匿名 FTP を通じて提供されている。表 2-26 は、その一つの例である。

表 2-26 ftp://ftp.apnic.net/pub/zones/202-APNIC

```
$ORIGIN .
$TTL 172800
15.0.202.in-addr.arpa.   IN      NS      dme2.mpr.wa.gov.au.
15.0.202.in-addr.arpa.   IN      NS      karri.bs.wa.gov.au.

32.0.202.in-addr.arpa.   IN      NS      kirsty.paradise.net.nz.
32.0.202.in-addr.arpa.   IN      NS      rachel.paradise.net.nz.

33.0.202.in-addr.arpa.   IN      NS      kirsty.paradise.net.nz.
33.0.202.in-addr.arpa.   IN      NS      rachel.paradise.net.nz.
```

[24] Operational policies for National Internet Registries in the APNIC region
http://www.apnic.net/docs/policy/operational-policies-nirs.html

```
（省略）

30.12.202.in-addr.arpa.  IN      NS      ns1.nic.ad.jp.
30.12.202.in-addr.arpa.  IN      NS      ns2.nic.ad.jp.

（省略）

APNIC.202.in-addr.arpa.  IN      TXT     "Generated at 2004-03-10 06:16:57Z with
35975 NS records."
```

このデータに対する署名ファイルは表 2-27 として公開されている。

表 2-27 ftp://ftp.apnic.net/pub/zones/202-APNIC.asc

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iEYEABECAAYFAkB0stoACgkQyzQvAdFSThSC0ACfYVW30Z0FsnZfs6+Ln4wsi+CE
rloAn26KcRc+gQAkt5yPaApqT81ZnLY3
=H+Nc
-----END PGP SIGNATURE-----
```

さらにデータに対するチェックサムが表 2-28 として公開されている。

表 2-28 ftp://ftp.apnic.net/pub/zones/141-APNIC.md5

```
MD5 (202-APNIC) = c967be9d4d8029a41e399a8a32503f41
```

このようにデータと電子署名が提供された場合、署名を検証することで作成者の正当性とともにデータの改ざんを発見することが出来る。

この場合、RIPE NCC で述べたように公開鍵を交換し合う必要がある。データを交換し合う IR の数が多くなると、鍵管理の負荷が急激に大きくなる。このため、PKI を構築することで、結果として負荷低減に寄与することとなる。

（3） CRISP のデータ認証方法

レジストリデータの公開手段として whois があることはすでに述べた。whois は単純な検索をサポートしているが、レジストリデータの数が膨大なものとなっている

現状、whois を代替する形の高度な検索プロトコルとして、Cross Registry Information Service Protocol （以下、CRISP と呼ぶ）が提案されている[25]。

このプロトコルは、分散環境への適合、情報ごとの参照権限設定、匿名アクセスからの登録者情報の保護、コンピュータで解析可能な検索・回答フォーマット規定などを実現することを目標においている。

現在は、2004 年 2 月に、「Cross Registry Internet Service Protocol (CRISP) Requirements」が RFC3707 として公開された段階にある。この RFC は、インターネットレジストリに焦点をあてたものとなっている。

今後の拡張として、クライアント認証の導入があげられているが、現時点では認証方式の指定は無く、将来の拡張に備えることだけが示されている（表 2-29）。

表 2-29 RFC3070 4. Feature Requirements より

4.1.　クライアント認証 サービスにアクセスする主体は、認証を目的として、サーバにクレデンシャルを受け渡すメカニズムを提供されなくてはならない。プロトコルは多くの認証タイプを採用でき、将来の認証タイプの拡張を受け入れるメカニズムを提供しなくてはならない。

[25] Cross Registry Information Service Protocol (crisp)
http://www.ietf.org/html.charters/crisp-charter.html

2.2. まとめ

本章では、インターネットレジストリにおけるアドレス資源管理の業務について述べ、申請データの内容、地域インターネットレジストリ（RIR）におけるメンバー、データ保護の仕組みについて述べた。アドレス資源管理における安全性は登録データの正当性が最も重要となる。そのために、申請業務におけるクライアント認証やインターネットレジストリ間の同期におけるデータ認証が必要になると考えられる。

RIR と NIR の連携したアドレス資源管理の機構によって、国際的なアドレス資源の正当性確保が可能になることもわかる。この状況を利用した認証基盤については、第 4 章で述べる。

本章で言及した RIR における認証の機能は、認証局を利用した認証システムでも実現されつつある。RIR の認証局に関しては次の第 3 章で述べる。