第 2 章　NIR におけるセキュリティ

内容

- 登録情報の利用上の脅威と保護
  - 登録情報
  - ネットワーク資源に対する脅威
  - 脅威の影響と保護
  - 権限委譲と PKI

2. NIR におけるセキュリティ

2.1. 登録情報利用上の脅威

インターネットレジストリに登録されている情報は様々な場面で利用される。これらの情報に対する操作には、情報の登録、参照、編集といったものがある。

これらの操作手段を提供するシステムに安全性を維持する機能がないと、通信路での不正な改ざん、第三者による不正な書き換え、盗聴などが容易に行われてしまう可能性がある。この状況はインターネットの利用の上で問題が起きる可能があるだけでなく、インターネットレジストリの登録管理業務の意義が問われる状況になりかねない。

ここでは、インターネットレジストリが管理している登録情報の種類とそれぞれに想定される脅威について述べる。

2.1.1. インターネットレジストリの登録情報

インターネットレジストリの登録情報は、ネットワークの管理者に連絡を取る際などに利用される。またネットワーク情報の変更の際にその申請者を認証するために使われたり、インシデントレスポンスのためにネットワーク情報の検索に使われたりする。

登録情報は主に whois システムや WWW を利用して閲覧される。インターネットレジストリが管理する登録情報は大きく分けて以下の４つである。

- IP アドレス空間情報
- 逆引きドメイン情報 (in-addr.arpa.)
- AS 情報
- コンタクト(人物)情報

RIPE NCC や APNIC、LACNIC といった RIR では、登録情報の管理の為に、RIPE で開発された Database Management System が利用されている。このシステムは情報をクラスとして定義し、そのインスタンス（実体）をオブジェクトと呼んでいる。クラスとして定義された情報は、インターネットコミュニティで必要とされている情報を網羅していると考えられるため、ここでは情報クラスについて述べる。

表 7　RIPE データベースシステムの情報クラス

カテゴリ	情報クラス名
IP アドレス空間情報	inetnum, inet6num, inet-rtr
AS 番号情報	as-block, as-set, aut-num
コンタクト(人物)情報	person, role, mntner, key-cert, irt

なお、逆引きドメイン情報は DNS を用いて提供されるので、ここでは詳細は述べない。

- IP アドレス空間情報

このカテゴリに含まれる情報クラスは inetnum, inet6num, inet-rtr である。

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

実際のデータは次のようになる（以下、データは　whois –h whois.ripe.net 193.0.0.203 のもの）。

```
inetnum:      193.0.0.0 - 193.0.1.255
netname:      RIPE-NCC
descr:        RIPE Network Coordination Centre
descr:        Amsterdam, Netherlands
country:      NL
admin-c:      DDL122-RIPE
tech-c:       OPS4-RIPE
status:       ASSIGNED PI
remarks:      used to be two different /24 inetnum objects
remarks:      until 19990305  (ripe-ncc & ripe-meeting)
mnt-by:       RIPE-NCC-MNT
mnt-lower:    RIPE-NCC-MNT
```

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

- AS 番号情報

このカテゴリに分類される情報クラスは as-block, as-set, aut-num がある。

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

aut-num クラスのオブジェクトは、一つかつクリアに定義された外部経路ポリシーを持つ一つかそれ以上のオペレーターにより操作される IP ネットワークのグループを意味する、AS の表現のデータベースである。

このクラスのオブジェクトは経路制御ポリシーを特定するために使われる。aut-num: 属性はこのオブジェクトによってあらわされる AS 番号である。as-name: 属性は AS のシンボリック名である。

- コンタクト(人物)情報

このカテゴリに分類される情報クラスは person, role, mntner, key-cert, irt, がある。

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

irt オブジェクトは CSIRT の連絡先およびセキュリティ情報を表す。アドレス範囲に対するコンピュータやネットワークのインシデントの扱いに責任がある CSIRT を特定するために inetnum または inet6num オブジェクトから参照される。オブジェクトの名前は “IRT-“ で始めなければならない。

key-cert オブジェクトはサーバに格納される公開鍵のデータベースで、mntner オブジェクトの更新を実施する際の認可に使われる。現在は”OpenPGP Message Format[9]”に準拠した鍵だけがサポートされる。

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

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

2.1.2. 登録情報に対する脅威

登録情報はインターネットレジストリに保持されるだけでなく、インターネットに関わるユーザや管理者によって参照される。参照情報の利用に関するリスクは表 8 に示すような脅威および原因によって引き起こされる。

表 8　登録情報に関するリスク

リスク	原因となる行為
不正なデータの保持	なりすまされた登録/更新/削除
	登録途中の書き換え
	古いデータの遺棄
不正なデータの提供	提供途中の書き換え
	なりすまされた情報提供
	提供不能行為
データの流出	権限の無い第三者による盗聴
	情報の露出

以下では、表 8 にあげたリスクが、現実のシステムにどのように現れているのか、について述べる。

調査の対象として、APNIC での IP アドレスの登録に存在する脅威、whois サービスによる情報提供に関わる脅威、JPNIC での IP アドレスの登録と更新に存在する脅威の三つをあげる。

2.1.2.1. APNIC での IP アドレスの登録に存在する脅威

APNIC に IP アドレス登録を要求する手順には、認証情報の登録において機密性を欠いているため、パスワードの盗聴による第三者による不正なアクセス権限の入手を始め、様々な脅威、それから生じるリスクが想定される。

この手続きは以下の手順で実施される[10]。

[10] “APNIC guidelines for IPv4 allocation and assignment requests”, http://ftp.apnic.net/apnic/drafts/apnic-draft-v4-guide.txt

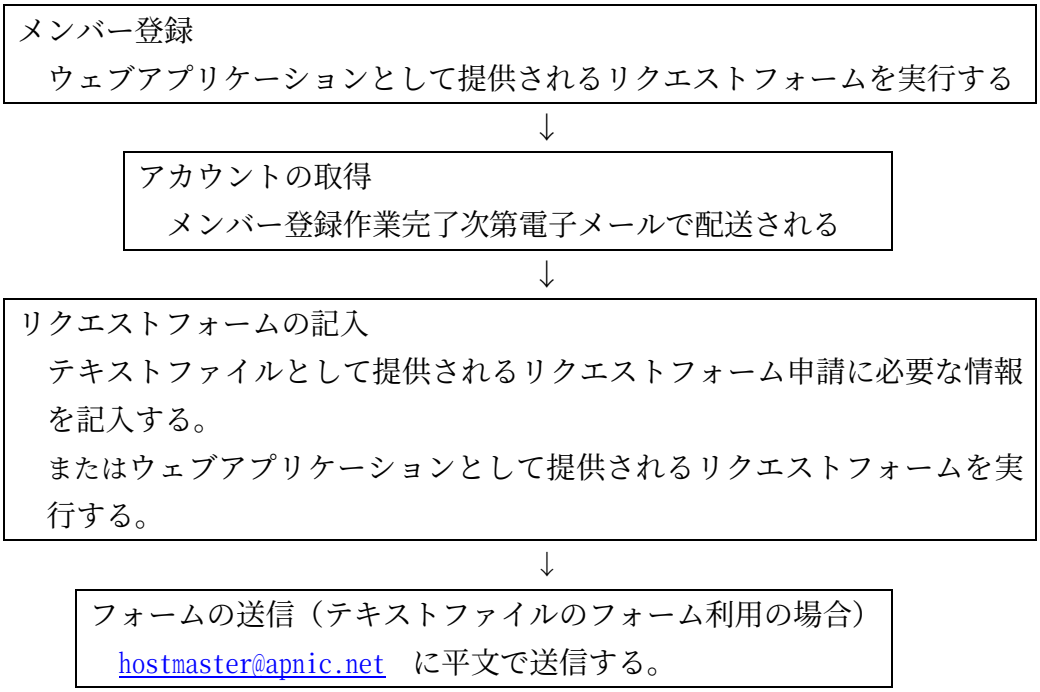


図 4　APNIC における IP アドレス登録プロセス

この手続きのうち、メンバー登録はウェブアプリケーションで行なわれるが、ここでパスワード登録を行うにも関わらず、保護されていないチャンネル経由で通信が行なわれている。

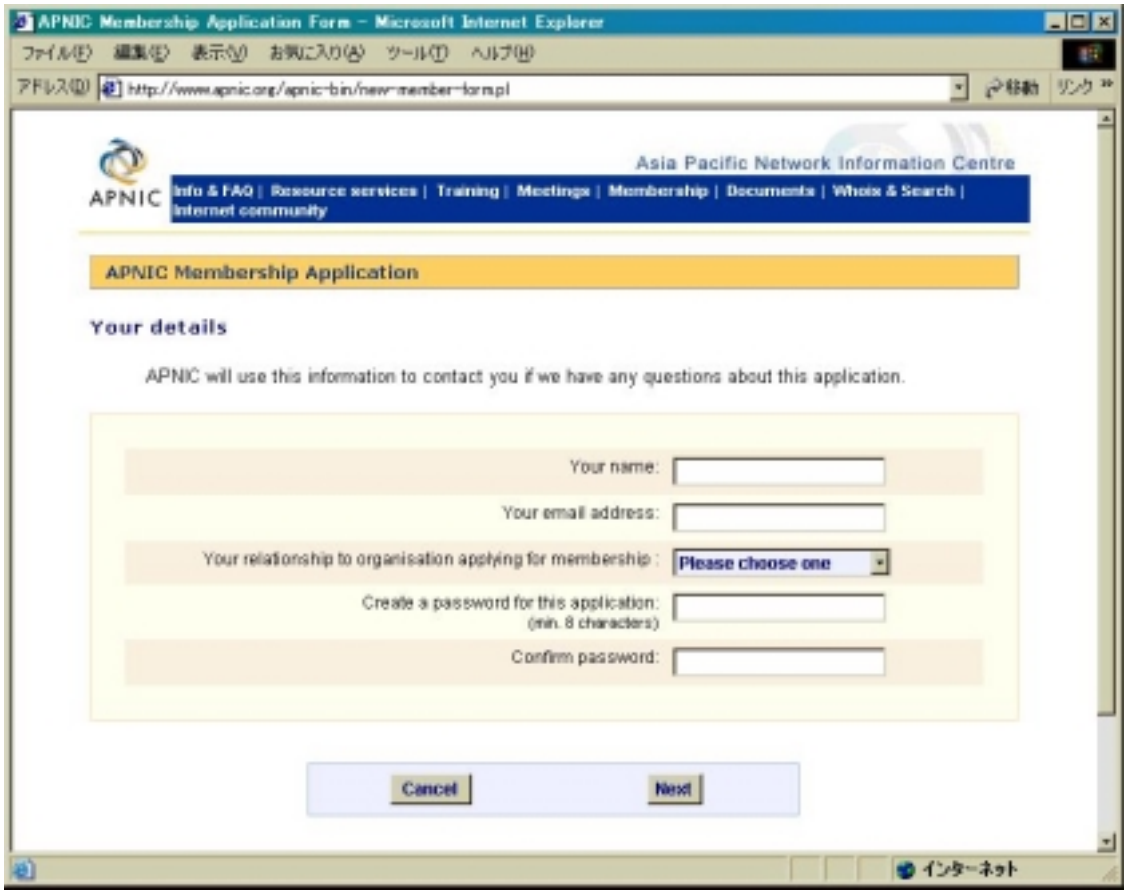


図 5　APNIC のメンバー登録リクエストフォームアプリケーション

APNIC の公開文書である” Policies for IPv4 address space management in the Asia Pacific region[11]”には次の記述があり、機密の保持およびセキュリティに関しての取り組みが行なわれていることがわかる。

セキュリティと機密性 APNIC は会員とその顧客の商業とインフラストラクチャ操作に関連する全ての情報の機密性を保護するためのシステムと業務を維持する。APNIC は全てのスタッフとエージェントの雇用が、そのような情報に関した機密性の明確な条件に基づいて行われることを保証する。 APNIC は APNIC　whois データベースに認可と検証メカニズムを提供する。このメカニズムを適用することは、それぞれのインターネットレジストリとエンドユーザの責任である。

[11] http://www.apnic.net/docs/policy/add-manage-policy.html

ここでは、登録業務に携わる全ての人員が機密性に関して認識を持つこと、システムにはセキュリティに考慮した機能が実装されること、その機能を実行することが宣言されていると考えられる。

しかし、セキュリティはシステムとして完全に機能していなければ意味をなさず、登録時の認証情報の漏えいが、以降のすべての操作における信頼性を損ねる要因となる。

2.1.2.2. whois サービスによる情報提供に関わる脅威

登録情報の利用は whois プロトコルを利用してレジストリデータベースを検索することになる。このプロトコルの仕様は次のようにきわめて単純なものである。

1. サービスホストに TCP ポート 43 で接続する。
2. <CRLF>で終了する一行のコマンド行を送信する。
3. コマンドラインに対応する情報を受け取る。
4. 出力が終わり次第、サーバは終了する。

プロトコル自体には認証、認可、機密性、完全性といったセキュリティ機能の指定はない。このようにセキュリティ機能に乏しいプロトコルを保護するためには、SSL や IPsec などのセキュリティ機能を実装するといったアプローチを取る手法があるが、そのような対策を施した whois サーバを提供しているインターネットレジストリは存在しない。

whois サーバに認証の仕組みがないということは、不正なデータの提供という脅威が存在するということである。この脅威に伴うリスクとして次のシナリオ実現の可能性が発生する。

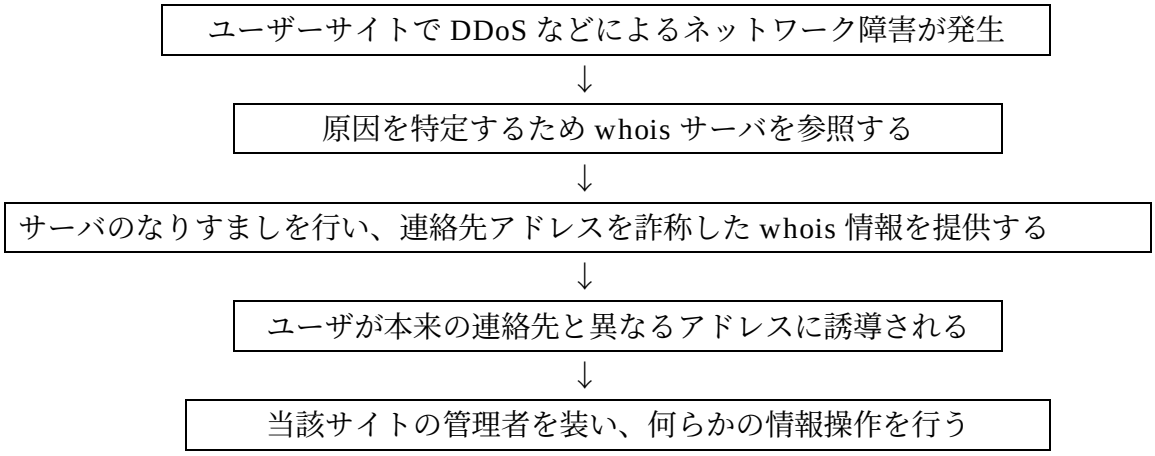


図 6　whois サーバのなりすまし行為

このようにしてなりすまし行為を行い、被害の拡大を図ることが出来る。

また、完全性の保証がないことから、man-in-the-middle 攻撃による情報の不正な書き換えを行うことができる。

また、whois データベース中の情報が現状を反映していないことがあり、情報を参照する価値が無くなっているという問題がある。

このような情報の陳腐化と、その影響は図 7 のように進展していくと考えられる。

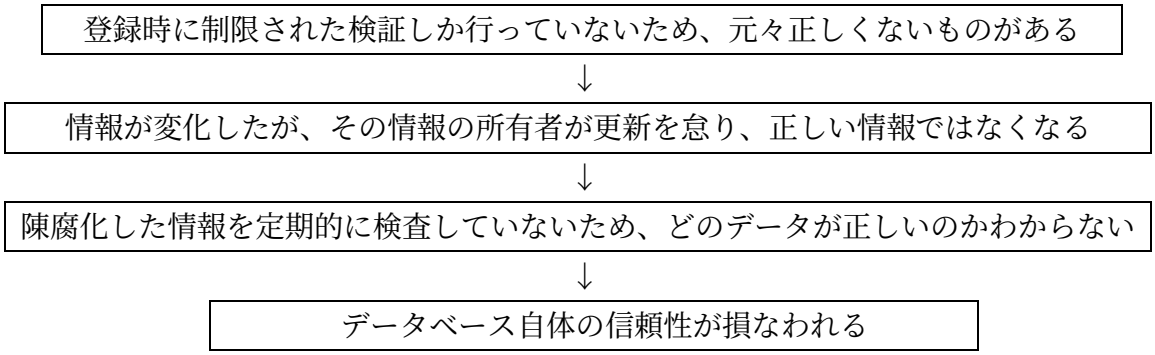
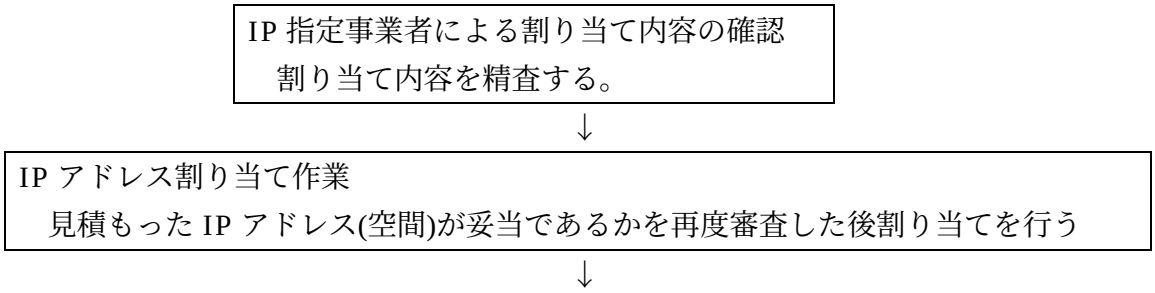


図 7　情報の陳腐化のプロセス

このような状況を放置しておけば、ネットワークの問題解決に使われるべき情報であるにも関わらず、逆に問題を発生させる一因となりかねない。

2.1.2.3. JPNIC での IPv4 アドレスの登録と更新に存在する脅威

JPNIC における IPv4 アドレスの登録手続きは、IP アドレス管理指定事業者(以下では IP 指定事業者とよぶ)からの割り当て報告申請を受け付けることで行われる。この申請手続きについては図 8 のように説明がなされている[12]。



[12] “IP アドレス割り当て報告申請処理について(ユーザネットワーク用)”, http://www.nic.ad.jp/doc/jpnic-00841.html

JPNIC へ割り当て報告申請
　JPNIC へ割り当て申請を行い、JPNIC は申請内容を DB に登録する。

図 8　IP アドレス割り当て報告申請プロセス

アドレス割り当てに関して IP 指定事業者から提出される情報について、JPNIC ではアドレスサイズが規定を超えて大きい場合を除き、特別な審査は行わない。つまり、情報に誤りがあったとしてもデータベースへの登録が行なわれてしまうことになる。

この点について、IP 指定業者が情報確認を行うことを確認するため、割り当て内容の精査について以下の注意が記載されている。

申請者から受け取った内容について記入漏れがないか、記載事項に誤りがないか等について精査してください。申請内容に虚偽がふくまれていないことを確認するのは困難ではありますが、可能な限りこれに努めてください。

登録情報の更新については更なる問題が存在する。ネットワーク資源の割り当てを受けている事業者、または個人による個人情報の変更については、IP 指定事業者を経由することなく、直接 JPNIC に追加・変更申請を行うことになっている。

この手続きは図 9 の手順で行なわれる。

http://www.nic.ad.jp/doc/jpnic-00844.html 中の追加・変更申請フォームの記入
↓
電子メールにより apply@db.nic.ad.jp へと送信
↓
機械的に処理され、データベースに反映される

図 9　登録情報更新プロセス

この手続きには認証手順が含まれないため、第三者が電子メール操作により不正にデータベースの書き換えを行う可能性がある。

この登録と更新に関する問題が、whois サービスで述べたようなデータベースの信頼性を損ね、登録情報の主な利用目的であるネットワーク上の問題解決に悪影響を与える可能性を否定できないと考えられる。

2.1.3. ネットワーク資源に対する脅威

ネットワーク資源は有限であるため、効率的な運用がおこなわれなければインターネットそのものが機能しなくなる危険性をはらんでいる。また、資源の利用に関する規則の遵守は紳士規定に過ぎず、設定ミスばかりでなくとも、意図的に規則を破って不正な情報操作を行うことでネットワークに多大な影響を与える攻撃が存在する。このような事態を引き起こす要因となる脅威には表 9 のものが存在すると考えられる。

表 9　ネットワーク資源に対するリスク

リスク	脅威	原因
ネットワークの飽和	ネットワーク資源の枯渇	不要なネットワーク資源の使用 使用されていないネットワーク資源の申請
通信障害	ネットワーク資源の衝突	割り当てられていないネットワーク資源の使用

以下にこれらの脅威が引き起こすリスクについて記述する。

2.1.3.1. ネットワークの飽和の可能性

インターネットを支える資源のうち、枯渇が問題となっているものの筆頭が IPv4 アドレスである。32 ビット固定長という構造上、最大割り当て数を増やすことができない、RIR へのブロック割り振りの都合上、例えば ARIN に未割り当てアドレスがあったとしても APNIC 管轄の NIR へ割り当てることもできないといった要因から、実際に利用できるアドレス数は理論上のものより少ない。

インターネットが今より小規模であった頃、ある程度の規模を持った企業であれば、クラス B のアドレスブロック（最大で 65534 ホスト）を割り当てられることも珍しくはなかった。現在ではクラス C（最大で 254 ホスト）を割り当てられることも難しい。

このように大きなアドレスブロックを以前に割り当てられた組織に対し、過剰な割り当て分について、自主的に返還することを推進する運動がかつてあった。しかし、割り当てられたアドレスブロックは、将来に備えるといった理由で返還されなかったものもあったと思われる。また割り当てを受けたアドレスブロックが、実際には過多な場合もあると考えられる。

割り振り、割り当て済み IPv4 アドレスは年々増加する一方であり、このままの状態

が続けば、アドレスが枯渇することは間違いない。この対策として IPv6 への移行が始まって久しいが、緩やかな移行が起こるかどうかは予測できず、アドレスブロックの割り当てが安定して行われるかどうかはわからない。

2.1.3.2. ネットワーク資源の衝突による通信障害の可能性

あるネットワーク、ホストが使用する IP アドレスはインターネット接続前に申請し割り当てを受けていなければならないが、実際には、割り当てを受けていなくても接続することは可能であり、通信を行うことが可能である。

これには経路制御がどこで行われるか、その設定をするのは誰であるか、といった条件が存在するが、RIPE NCC が実施している RRCC（Routing Registry Consistency Check Project）によると、実際に流されている経路情報のうち、相当数のものが未登録であることがわかっている[13]。

インターネットの経路制御は AS を単位として自律的に行われている。そのため悪意を持って流される経路情報がインターネット全体に波及することは十分に考えられる。

The "No Questions Asked" Prefix Return Policy[14]で述べられているように、経路表の膨張に伴うインターネットオペレーション負荷の増大を防ぐためには、アドレスの返却と再割り当てにより、経路表の集約を可能とすることが不可欠である。

2.1.4. ネットワーク資源の脅威の影響

ネットワーク資源に対する浪費の意味での脅威は、いずれの原因でも同等である。しかし「割り当てられていないネットワーク資源の使用」は他の行為とは性質が異なる。割り当てられていないネットワーク資源が悪意のあるユーザに使われた場合に、その影響を抑えることが難しい。たとえば、割り当てられていない AS 番号と IP アドレスがテロ組織によって使用された場合、テロ行為の状況を把握すること、テロ行為を引き起こしているパケットの発信元を特定することが難しくなることが考えられる。これは転送経路を次々に変更することが可能であるためである。

---

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

[14] The "No Questions Asked" Prefix Return Policy, http://ftp.apnic.net/apnic/docs/no-questions-policy.txt

経路情報を扱う上での一つの問題が swamp address space と呼ばれるものである。これはインターネットレジストリにとって再割り振りが難しい、細かいブロックの集合を意味し、グローバルには IANA が割り振りを行っていた時代に割り振られたクラス C アドレスブロックを指すことがある。

南カリフォルニア大学情報科学研究所の調査プロジェクト、Procedures for Internet and Enterprise Renumbering の 1996 年当時の swamp address に関する報告書[15]によれば、192/8 のクラス C アドレスを持つ、5980 の組織に連絡をとった結果、1850 の回答があり、1448 が配送に失敗した。返答の内訳は以下の通り。

表 10　swamp address の利用に関する調査

	アドレス空間を返却する	しない
アドレスを使っている	189	1351
アドレスを使っていない	135	23

このように実際に使われてしまっているものについて大多数が返却しないと述べているが、さらに重要なことは 20%以上の組織に連絡がとれないことである。つまり、管理者不在の状態で放置されているということである。

これら古い時代に割り振られたアドレスブロックは RIR による割り振りプロセスを経ていないことから、地理的地域性による、経路表の集約といった配慮を欠いている。場合によっては RIR をまたいで割り振られたものがあり、こういったアドレスに関する経路情報は、どこから流されるのか前提条件をもうけることができないため、エッジルータでブロックすることが出来ず、一つのネットワークだけでは正しいものかどうかの検証も難しいため、結果的に経路表に載ることになってしまう。

つまり、現在管理者不在の swamp address を調査し、それらのアドレスに対する経路情報をインターネットに流すことで、インターネットレジストリに登録せずとも、世界中に通信可能なネットワークを設けることが出来るということになる。

前述の RRCC の調査が、実際に登録されていない多数の経路情報が流通していることを示している。インターネットレジストリのポリシーに従ってネットワークを構築し

[15] “PIER - Procedures for Internet and Enterprise Renumbering”, http://www.isi.edu/div7/pier/)

ている組織が、登録をせずにインターネット接続することは考えにくいため、設定間違いによるもの、もしくは確信犯による行為と考えられる。

このようなアドレスを使って不正行為を行うと、実行者を特定するため、および不正行為をブロックするためには、経路上にあるすべてのネットワーク管理者の協力を仰ぐ必要がある。しかし、実行者が複数のアドレスを使い、それらを渡り歩くことで不正行為を継続したとすると、実行者の追跡はほぼ不可能になり、不正行為を遮断することも困難となり、多くのネットワーク接続が不安定な状況になることが考えられる。

図 10 は、攻撃者が不正な経路を作り出すことで、第三者サイトを経由した攻撃を行っている状況を示している。サービス不能攻撃を行うのであれば、被害者サイトがサービス不能に陥ったことを確認した後、経路の公告を停止することで、追跡の手が及ぶ可能性を減らすことができる。

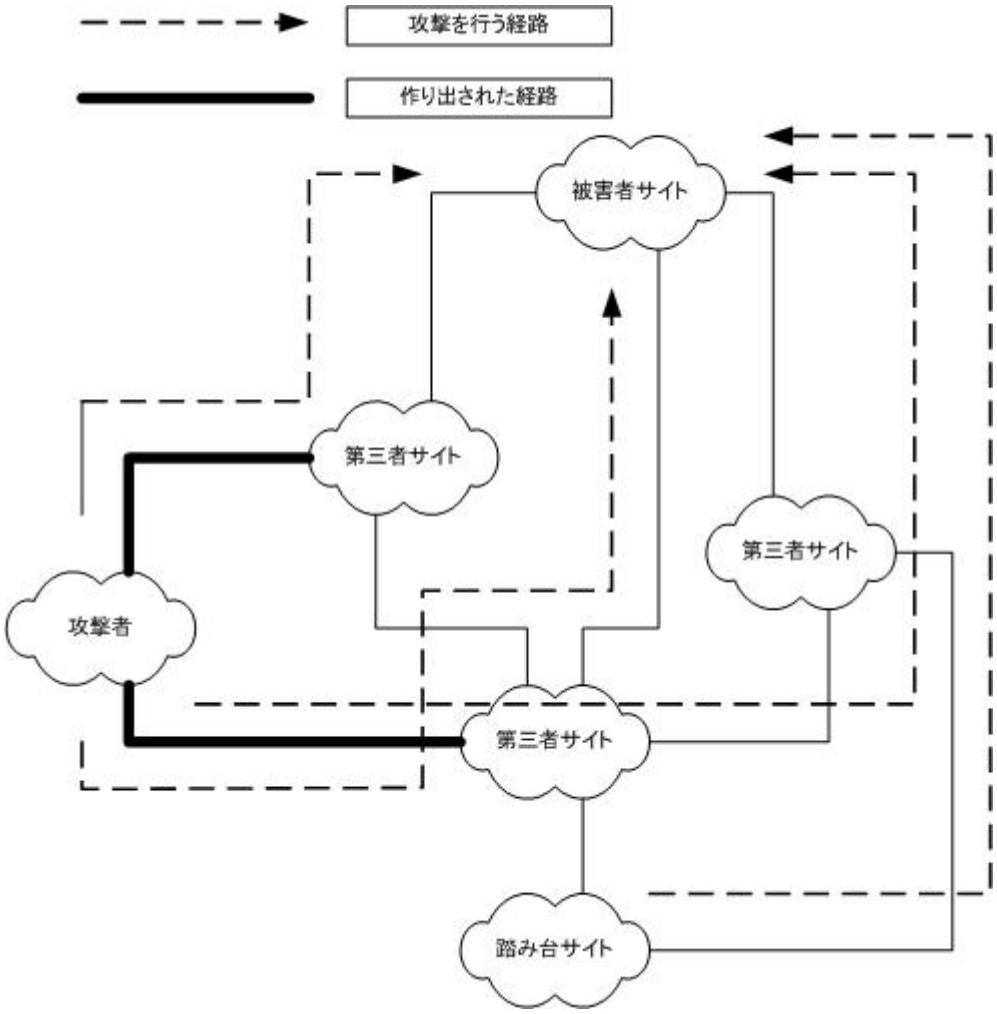


図 10　未登録の経路を利用した攻撃

犯罪組織がネットワーク資源の脅威を利用したこの種の攻撃は実際に発生している。

2003 年 2 月 27 日、RIPE に対する DDoS 攻撃(分散サービス不能攻撃)の影響から、二時間半に渡って、レジストリへのアクセスが不能となった(90%以上のパケットがロスト)。この攻撃は ICMP echo を悪用したもので、DNS、whois、FTP、Web サービスが利用不可能となった。

それぞれのサービスへの攻撃ではなく、大量の ICMP リクエストにより、RIPE の BGP セッションが影響を受け、外部からの通信が正常に行われなくなってしまったのが原因である。

この攻撃は別名 smurf と呼ばれるもので、古典的なものである。攻撃者については

不明とされているが、このような一般によく知られている手法であっても、RIR のネットワークが麻痺状態に陥ったことがわかる。

この事例の場合、RIR ネットワークそのものが孤立した状況に陥ったことで、すべての外部サービスが利用不可能と成った。

BGP ルータのフィルターで攻撃パケットをブロックすることが可能であったなら、サイトがダウンすることも無かったかもしれないが、この件では、攻撃自体検知されたにも関わらず、有効な手立てを打ち出せず、結果的に過剰な負荷によりルータがダウンするという結果となってしまった。

2.2. 登録情報の利用法と脅威の影響

インターネットレジストリの登録情報について想定される利用についてまとめ、これまでに述べた脅威が、その利用にどのような影響を及ぼすのかについて述べる。

2.2.1. 登録情報の利用

ネットワーク情報には IP アドレスのブロックを割り振られた／割り当てられたネットワークの情報のことであり、この情報は JPCERT/CC に代表される CSIRT（Computer Security Incident Response Team) によって、迷惑行為の発信元ネットワークへの連絡先の検索などに使われている。

AS 番号には AS 番号を割り当てられたネットワークの情報が登録されている。間違った経路情報を広告しているネットワークの特定や、ネットワーク管理者による正しい設定内容の検索に使われる。

ドメイン情報にはドメイン名を登録した組織の情報が登録されている。IP アドレスからドメイン名を調べた上で、登録されたドメイン情報が見つかった場合、CSIRT などによる連絡先の検索などに使われる。

組織情報にはデータベースに情報が登録されている組織の情報が登録されている。インシデントレスポンスチームなどによる連絡先の検索などに使われる。

2.2.2. 脅威の影響

登録情報およびレジストリデータベースは、インターネット運営に障害が発生した際のトラブルシューティングに利用されることが多い。つまり危機管理上重要な情報であ

り、インターネットの正常な運営が行われていることを確実なものとするために不可欠の情報といえる。

登録情報に含まれる、連絡先情報が不正な操作により改ざんされ、CSIRT が本来連絡をとるべき管理者に連絡がとれなくなれば、問題の解決に深刻な影響を与えることになる。

2.3. 登録情報/レジストリデータベースの保護

脅威の影響を最小限に抑えるため、情報は不正なアクセスから保護される必要性がある。2.2.2 節で述べた脅威を考慮して、登録情報に求められる性質を挙げる。

- 正確性

  提供する情報が「正しい」こと。正しいというのは提供者が「意図した通り」を意味する

- アクセス管理

  連絡先情報については、パブリックに公開されるべき情報ではあるが、個人情報についてはアクセス制限が要求されることがある

- 安定性

  インシデント解決に利用されることが多いということは、インシデントの発生に左右されることなくサービスが稼働しなくてはならない

- 即時性

  要求された情報が遅延なく提供されること

安定性と即時性についてはレジストリデータベースが配置されるネットワークの保護が必要となる。この保護については、ハードウェア構成に大きく依存するため、本報告書では考察の対象とはしない。

要求される性質のうち、正確性の保証、アクセス管理の実施のため必要な要件を以下に述べる。

・　ユーザ情報

　特定のネットワーク利用組織の登録情報を変更することができるユーザに関する情報のことで、ネットワーク資源の占有や登録情報の不正な書き換えを防ぐため、この情報へのアクセスについては、強力な認証が要求される。

・　認可の実装

　認可とはユーザがある操作を行うことに対する制御を行うことである。たとえば、組織情報のうち、組織名称を変更できるものは管理者のうちでも特定の一人にだけ許可し、組織連絡先電話番号の変更は管理者全員に許可するなどの利用が考えられる。

・　完全性の保証

　情報の経路上での改ざんを防ぐためには電子署名などを用いた完全性の保証を行う必要がある。

・　機密性の確保

　機密性が要求される情報については暗号化を施す必要がある。暗号化された情報は管理者のうち許可されたものおよびデータベース管理者にとって複号可能である必要がある。

・　登録情報の検証

　登録される情報のうち、組織情報、個人情報などは、正しくなければ保証する意味がない。オフラインでの情報の検証が必要となる。

　これらの機能を実現することで、正しい情報の維持が可能となり、また正しく伝えることが可能となる。

2.4. インターネットレジストリにおける権限委譲と PKI

　インターネットレジストリの、ネットワーク資源に関する権限の委譲構造は、権限の認可構造でもある。これは TTP（Trusted Third Party – 信頼できる第三者）を利用する認証基盤である PKI（Public-Key Infrastructure）の Authorization（認

可）構造と近似している。本節ではインターネットレジストリにおける権限委譲と PKI について述べる。また第 55 回 IETF（Internet Engineering Task Force）の PKIX ワーキンググループで議論された PKI の利用事例について述べる。

2.4.1. PKI

本調査研究報告書では「認証局」のあり方に関して述べるため、本節では PKI について概説と共に動向について述べる。

PKI（Public-Key Infrastructure）は公開鍵暗号を利用した認証基盤である。基盤技術であるため、PKI という一つの仕組みを、様々な認証の為に利用できる。

PKI では通信相手が本物であるかどうかの確認（認証）に公開鍵証明書（以下、証明書）を利用する。PKI における証明書は、発行者の名前といった情報が記述されており、身分証明書の役割を果たす。身分証明書を、信頼できる第三者（TTP：Trusted Third Party）に発行してもらうことで、その身分証明書を信頼できるようにするのが PKI の特徴である（図 11）。たとえばここでいう身分証明書が運転免許証であるとすると、信頼できる第三者は公安委員会ということになる。

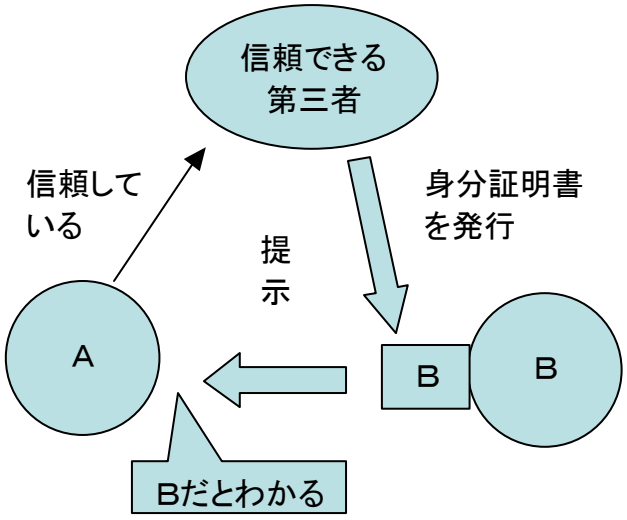


図 11　信頼できる第三者

証明書を利用して相手を認証する際には、証明書が偽造されていないか、その証明書の発行元は信頼がおけるのか、といった確認が行われる。証明書が有効であれば、その証明書の提示を行ったのが正しい相手であることがわかる。そのため初めて通信する相手でも、直接対面することができない通信相手でも認証できる。よって PKI はインタ

ーネットのような通信相手と対面することを前提にできない環境に適している。

以下に PKI の仕組みのうち、X.509 や RFC3280 に基づいた証明書の扱いについて概説する。

2.4.1.1. 証明書の利用

PKI で用いられる証明書は、認証局（CA：Certification Authority）によって発行される。PKI では、この CA が“ 信頼できる第三者 ”にあたる。CA は、いわば身分の証明を行っている機関なので、ユーザに強く信頼されていなければならない。ユーザは、自分が信頼している CA が発行した証明書であれば信じられるということになる。

証明書には身分を証明する内容だけでなく、公開鍵暗号方式で使われる暗号鍵（公開鍵）も含まれている。この暗号鍵は、電子メールの電子署名や Web のサーバやクライアント（ブラウザ）の認証に使うことができる。たとえば電子メールの場合、S/MIME（Secure/Multipurpose Internet Mail Extensions）というプロトコルで、PKI を利用することができる。電子メールでの重要なやりとりでは、送信者は本人に間違いないのか、内容が他人によって書き換えられていないか、といった事が重要になる。PKI を使うと、S/MIME での電子署名が本人のものであるかを確認することができる。また TLS（Transport Layer Security）でも PKI が利用される。Web ブラウザが https（TLS や SSL を使った http）を使って Web サーバと通信を行っているとき、そのことを示す鍵マークが表示される。鍵マークが表示されるまでに、Web サーバと Web ブラウザは証明書の交換を行い相手の証明書を検証するが、この時に PKI が使われる。 PKI は認証情報をアプリケーションとは独立に扱うため、様々なアプリケーションに応用したり、アプリケーションに変更を加えずに PKI の仕組み自体を改良したりできる。

2.4.1.2. 証明書とユーザ

ユーザは CA に証明書を発行してもらい、その証明書をアプリケーションで利用する（図 12）。CA はユーザと同様に証明書を持っており、その証明書に含まれている暗号鍵を使って、発行する証明書に電子署名を施す。ユーザは CA の証明書を参照する事で、検証したい証明書の発行に使われた暗号鍵が、確かにその CA のものであるということを確認できる。

図 13 のように、ユーザはルート CA、もしくはいずれかの CA を信頼し、その CA が発行する証明書は正しいという前提に立って証明書の検証を行う。ユーザが信頼している CA は、そのユーザにとっての“ トラストポイント ”（信頼点）と呼ばれる。トラ

ストポイントはユーザによって異なる。

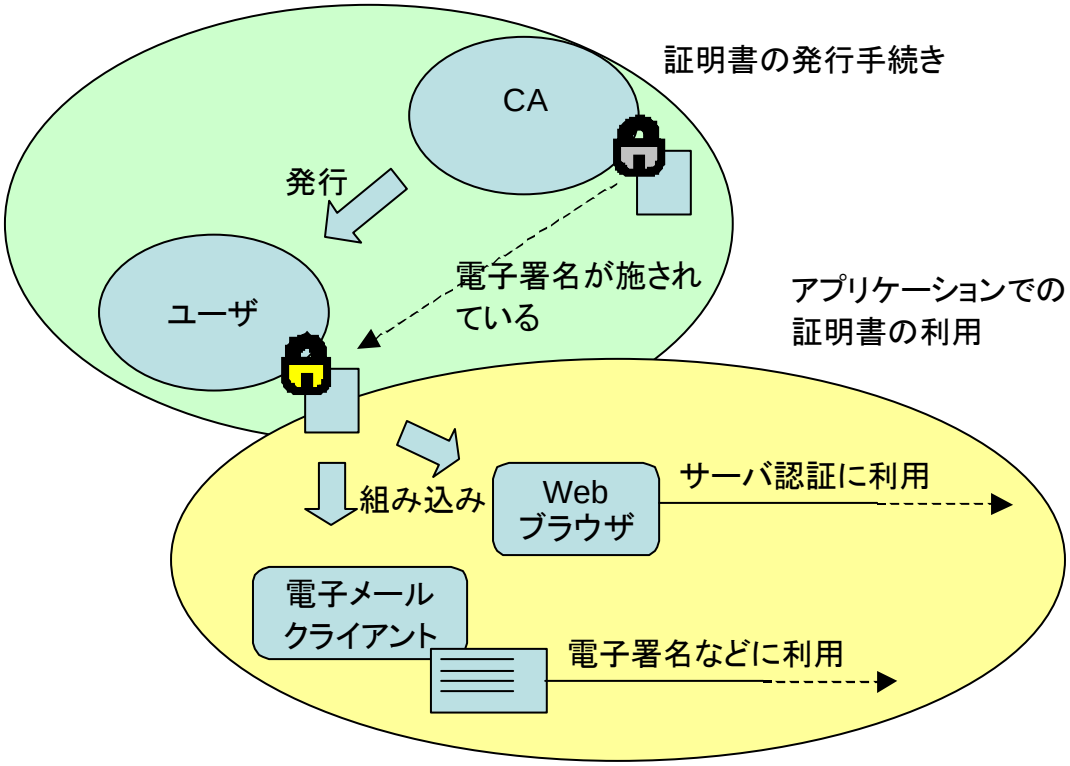


図 12　証明書の発行と利用

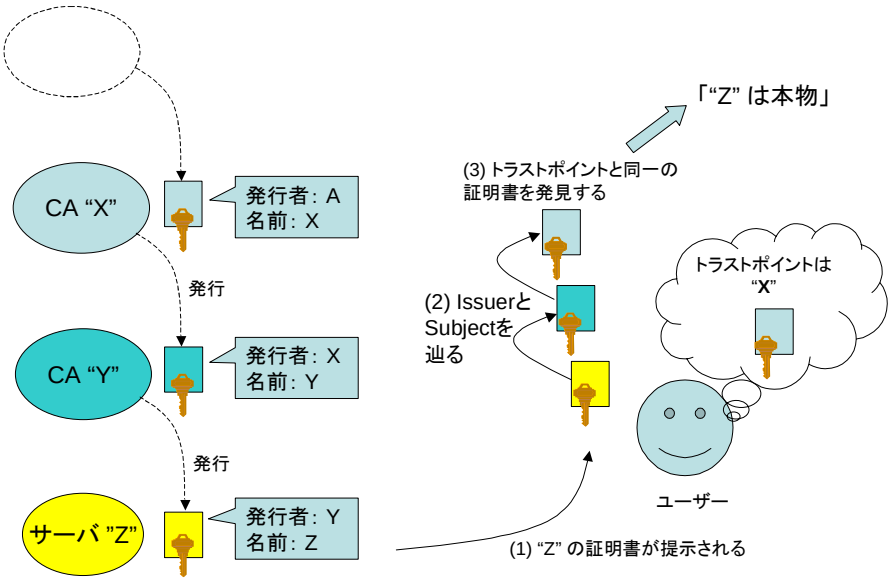


図 13　トラストポイント

2.4.1.3. 証明書の内容

証明書には図 14 のような内容が記述されている。

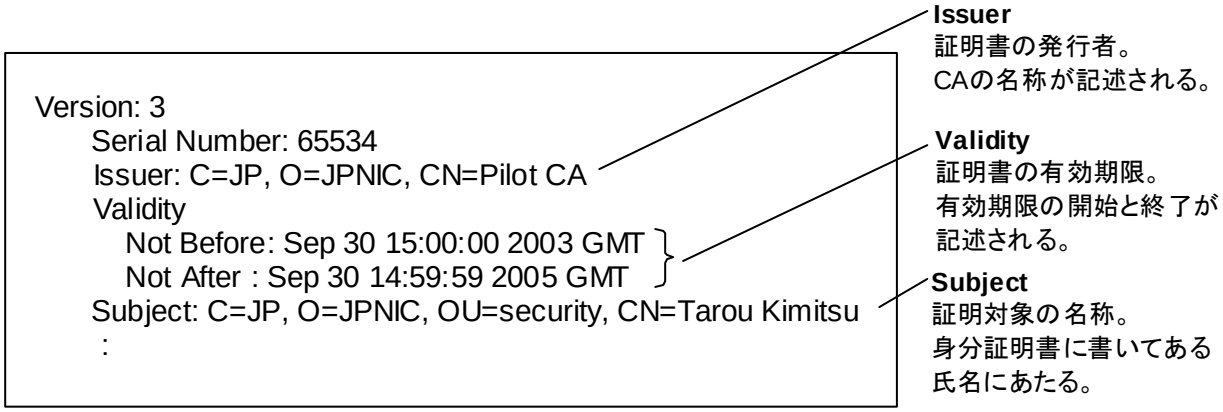


図 14　証明書の例

Subject や Issuer に記述されている名称は、識別名（DN: Distinguished Name）と呼ばれる。表 11 に DN の要素と意味を示す。

要素	意味
C（Country）	国名
O（Organization）	組織名
OU（Organizational Unit）	部門名
CN（Common Name）	一般名

表 11　X.509 形式の証明書で使われる識別名（DN）の要素

この他に、証明書には公開鍵データや CA による署名のデータ、用途などの情報が記述されている。これらのフィールド（項目名と値）は、検証の際に参照される。

2.4.1.4. 証明書の検証

証明書の検証には、二つの側面がある。

一つ目は証明書チェイン（証明書の連鎖）である。証明書チェインとは、検証したい

証明書からトラストポイントもしくはルート CA の証明書までの一連の証明書が連鎖している状態のことである。各々の証明書に電子署名されており、それぞれの電子署名を検証できる公開鍵は、発行者である CA の証明書（以下、CA 証明書）に含まれている。認証したい相手の証明書を検証するには、一連の証明書を次々に検証していく必要がある。

二つ目の側面は、証明内容を受け入れられるかどうかである。証明書には、証明対象の名称や証明書の用途、証明書のポリシー（の識別子）が含まれている。たとえば対象を限定して検証を行いたい場合、Subject の比較を行う。JPNIC という組織に属しているものだけを認証したいとき、Subject に“C=JP, O=JPNIC”が含まれているかどうかを確認する。たとえ証明書の連鎖が成立していても、Subject が想定したものと異なる場合、認証は成立しないことになる。Subject 以外に、受け入れられる用途かどうか、受け入れられるポリシーかどうかといった検査を行う。これらの二つの側面で検査し問題がなければ、認証が成立したことになる。

次に上記で説明した側面をふまえ、証明書の検証手順について説明する。証明書の検証手順には、いくつかの方法が提案されている。ここでは認証対象の証明書から上位の CA に向かって証明書を辿っていく方法を説明する。はじめに認証対象の証明書から上位の CA に向けて証明書のチェインを構築する。この処理はパス構築と呼ばれる。

- Issuer の値（発行者の名称）を元に CA 証明書を入手。
- CA 証明書の Issuer の値を元に、その CA 証明書を発行した CA の証明書を入手。
- CA 証明書入手を繰り返しトラストポイントの CA 証明書に辿り着いたかどうか判断。

次にそれぞれの証明書の証明内容を検査する。

- CA 証明書に含まれている公開鍵で、認証対象の証明書の電子署名を検証。
- 名称、有効期限、鍵の用途が受け入れられるかどうかを検査。
- 証明書が失効していないかを検査。

証明書の失効とは、CA がその証明書の効力が失われたと認識し宣言することである。証明書の失効の理由には、証明内容の変更や暗号鍵（秘密鍵）の紛失などがある。証明書が失効されているかどうかは CA によって発行される CRL（Certificate Revocation List（失効された証明書のリスト））を使って調べることができる。

証明書の検証をネットワークアプリケーションに組み込むと、そのアプリケーションの認証の手順は以下のようになる。

- 認証処理のはじめに証明書を交換。
- 次に相手が提示した証明書を検証。
- CRL の入手などを適宜行い、証明書の最新の状態を確認。
- 証明書が有効である場合、認証できたと判断しアプリケーションのサービスを開始。

このように、証明書の扱いは認証システムとは独立した仕組みであり、認証システムを構築する際には、通信プロトコル等と組み合わせて利用される。

2.4.2. 第 55 回 IETF PKIX ワーキンググループにおける議論

PKI に関する技術動向の一環として、PKI のプロトコル策定活動を行っている IETF（Internet Engineering Task Force）の PKIX（Public-Key Infrastructure (X.509)）ワーキンググループに参加した。米国アトランタで行われたこの会議では、X.509 形式の証明書の検証プロトコルや証明書の値の利用に関する議論が行われた。本節では、利用に関する議論について紹介する。

このセッションでは以下のようなプロトコルに関するドキュメントが紹介され、議論された。

- DPV/DPD（Delegated Path Validation and Delegated Path Discovery Protocol）
- SCVP（Simple Certificate Validation Protocol）

また証明書のフィールド（項目と値）の利用に関して以下のような提案が紹介され、議論された。

- Proxy Certificates
- LDAP Schema
- Attribute Certificate
- Certificate Warranty Extension
- Logotypes in X.509 Certificates

更に、証明書の利用法に関する紹介が行われた。

- SIM（Subject Identification Method）

SIM は、証明書の拡張フィールドに個人を識別する番号を格納する方式である。この方式は、subjectAltName 拡張フィールドに、一方向性関数を利用した値を格納することで、プライバシーの保護と、予め識別子を知っている検証者によるユーザの識別を可能にする。

証明書のフィールドに格納する値は、PKI を使った認証システムの実装によって扱い方が異なる場合がある。特にフィールドに格納された値からユーザを識別する方法については、プロトコルの提案の範囲を外れている。SIM は、一方向性関数の利用等を通じて、格納された値の利用法の開発に積極的に取り組んでいると考えられる。

本調査研究が想定している認証局でも、証明書に格納する値の議論が必要になると考えられる。今後も、SIM のような積極的な取り組みの動向をみていく必要がある。

なおセッションの最後に、日本ネットワークセキュリティ協会による相互運用に関する実験 ChallengePKI 2002 と ChallengePKI 2003 について紹介された。

2.4.3. インターネットレジストリと Authorization（認可）

インターネットレジストリは、上位インターネットレジストリから下位インターネットレジストリに、ネットワーク資源の割り振りに関する権限を委譲する構造を持つ。一方、認証局が発行する証明書には、認証の他にその証明書で示されている属性を証明するという意味がある。属性には、認証局であるかどうか（証明書を発行できるかどうか）、暗号鍵をどのような用途に使うことができるか、といった情報が含まれている。属性として表される値の中に、そのエンティティが利用または割り当てを行うことができるネットワーク資源を表現することができれば、ネットワーク資源の管理に関する権限の委譲を表現することができる（図 15）。

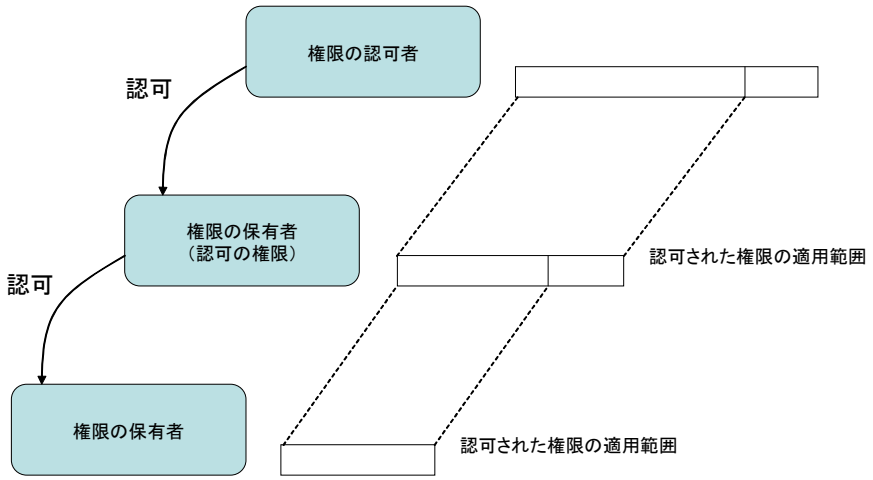


図 15　認可された権限の範囲

しかしこのモデルは、権限の委譲と認可を同等と考えた場合のもので、ネットワーク資源の割り振りに関する権限が「認可」のモデルと一致するかどうかについては議論の余地が大きい。これはネットワーク資源の管理が、合意されたポリシーにもとづいて行われるためで、一義的な「権限の認可」にもとづいていないからである。

またネットワーク資源が証明書で表現されるかどうかについても議論と開発の余地がある。ネットワーク資源の割り振りを検証可能な表現形式で扱ったプロトコルや手法は、日本の NIR や４つの RIR において利用されたことがなく、一般的な概念ではないと考えられる。また PKI の適用に関しては、証明書のフィールドの扱いと、ネットワーク資源の表現方法についての議論が必要である。

2.5. まとめ

インターネットレジストリが提供するサービスおよび保持する情報に関する脅威には次のものなどが存在する。

- 登録情報に関する不正なデータの保持、提供
- ネットワーク資源の浪費、無効化
- データベースサービスへの攻撃

これらが問題となることは、現状の情報提供サービス実装のセキュリティ機能が乏しいことに多くの原因がある。インターネットで広く利用されている SSL（もしくは TLS）は、セッションに機密性と完全性を持たせるプロトコルで、接続先が意図した相手であることを保証するものではない。

また、登録されている情報自体が現状を反映していないという報告が RIR の会合では繰り返されていることなどを考慮すると、登録情報を扱うシステムは次のセキュリティ機能を実装することが急務といえる。

- 正確性
- アクセス管理
- 安定性
- 即時性

データベースの情報を確実なものとし、更新が速やかに行なわれ、安定した情報提供を行い、不正アクセスから保護するということになる。

セキュリティ機能の実装に PKI を使うことが考えられるが、そのためには認証局が重要な検討事項となる。

RIR の試みとしては APNIC の CA パイロットプロジェクトが挙げられる。その詳細については第 3 章で述べる。