第 10 章　インターネットの可用性と安全な経路制御の課題

内容

- 運用と安全性との関係の特定
- 運用の柔軟性の確保
- 性能評価

10. インターネットの可用性と安全な経路制御の課題

インターネットにおけるネットワークアプリケーションの可用性の確保の為に安全な経路制御は重要であるが、そのネットワークの運用が実用的な柔軟性を持ち続けることも重要である。

本章では、JPNIC で検討されている経路情報の登録機構や、S-BGP や soBGP を利用した安全な経路制御を実施するに当たり、検討すべき課題について述べる。

10.1. ネットワークの運用と安全性との関係の特定

はじめに挙げられるのがネットワークの運用と S-BGP などの機構によって得られる安全性との関係を特定することが挙げられる。機構が安全性を向上させるものであっても、運用の仕方によって効果を表さないようであれば意味がない。

これには、S-BGP 等の電子認証を使った仕組みについては、電子証明書の発行方法が大きく影響すると考えられる。発行対象が間違っていたり、証明書の検証を行う者が間違った認証局証明書を入手して使用してしまうと、偽の証明書を有効とみなしてしまう、いわゆる「オレオレ証明書」の問題が起こってしまったりする。

2005 年度の本調査研究では、JPNIC の認証局を利用し、ルーティングの安全性向上を図るための「経路情報の登録」と電子証明書を発行するモデルについて、第 17 回 JANOG で発表を行った。しかし会場では特に意見を頂くことはできず、具体的な運用手順が明らかになっていないとコメントのしようがない、という状況であった。事後に行なった ISP へのヒアリングについて 10.4.1 節で述べる。

今後は、実際に S-BGP などの運用ができる環境を構築し、電子認証の手順を明らかにしたり、これによって安全性が高まるポイントをまとめたりすることで、運用手順を明らかにし、安全性との関係についての意見を集約できるようにすることが考えられる。この検証を進める為、JPNIC では実験環境の構築を進めている。本実験環境については 10.4.2 節に掲載した。

10.2. 運用の柔軟性の確保

インターネットが国際的な接続を持つネットワークであるため、経路情報の交換も、国際的な接続を通じて行われている。そのため、日本国外から経路情報を受け取ったり、場合によっては日本国内で JPNIC 以外のインターネットレジストリを通じて割り当てられた IP アドレスを使ったりする必要がある。

しかし JPNIC は日本の NIR（National Internet Registry：国別インターネットレジストリ）であり、日本国内の IP アドレス管理指定事業者に対して IP アドレスの割り振りを行っている。そのため登録情報は日本国内の IP アドレスに関するものとなる。

国外の IP アドレスの使用のようなネットワークの運用の柔軟性は、元来ネットワーク利用者側にある要件であり、インターネットレジストリが制限すべき事項ではない。従って電子認証の導入の際には、ネットワーク利用者側の要件を吸収できるような柔軟性を持たせる必要がある。

現在、この柔軟性については JPNIC IRR 企画策定専門家チームと経路情報の登録機構の検証専門家チームで検討を行っており 10.4.1 節で述べるヒアリングはその一環である。

10.3. 性能評価

S-BGP や soBGP 等で適用されている、暗号技術を使った認証機能は、暗号の処理が必要となり、既存のネットワーク機器の新たな負荷となる。これまで BGP 等の経路情報交換プロトコルではメッセージ認証などの処理は伴わないプロトコルであった為、これらの認証機能についての性能評価が必要となる。

本調査研究では、2006 年度に予定していたこの調査を前倒しし、ルーティングの実験環境を構築して検証を開始した。2005 年度は環境整備を進めている段階であるが、いずれ ISP 等との情報交換に利用できるような実験プラットホームになることが望ましいと考えられる。

10.4. 各課題に対する 2005 年度の取り組み

2005 年度の調査研究を通じて、安全な経路情報交換のための IP アドレス認証の展開にはいくつかの課題が見えてきた。そこで ISP に対するヒアリング等を実施して、課題解決のための取り組みを行なっている。

10.4.1. 経路情報の登録機構に関するヒアリングについて

2006 年の 2 月頃、JPNIC で検討している「経路情報の登録機構」に関するヒアリングを行った。経路情報の登録機構とは、JPNIC から IP アドレスの割り振りを受けている IP 指定事業者から AS 番号管理者に対して IP アドレスの利用を認可（authorization）する仕組みである。本機構は、AS 番号や IP アドレスを詐称してインターネットの接続性に混乱をきたす「経路ハイジャック」を防ぐ為の基礎的な仕組みとなりうる。第 17 回 JANOG での発表の際には、本機構の意義を理解していた参加者はあったものの、ISP にとっての具体的な利点や課題を調査するまでには至らなかった。その為改めて個別にヒアリングを行った。

ヒアリングは日本国内で ISP 事業を行なっている大手 4 社に対して行った。ヒアリングの際に「経路情報の登録機構」に関する説明を行い、その機構の有効性や導入の影響について意見収集を行った。

○「経路情報の登録機構」の有効性（ポジティブな意見）

- 本機構の有効性については下記に示す回答が得られた。
- 経路情報の第三者による検証は楽になる。
- 他の AS の情報を経路情報からチェックできる。
- トラブルが発生したときの他の経路から連絡先の妥当性が担保される。
- 人的な経路の設定ミスを発見できる。

本機構は JPNIC の登録情報のデータベースであるので、経路ハイジャックを防ぐ仕組みにするには利用スキームが必要だという意見があった。

経路情報の登録機構は、JPNIC における不正登録を防ぐ仕組みであり、これだけで経路ハイジャックを防げる仕組みではない。登録データを利用してネットワークの運用に反映する仕組みが必要だという意見だと思われる。

○「経路情報の登録機構」に対するネガティブな意見

- 登録されている情報が Up-to-date に更新されておらず、信頼性がない。

これは本機構というよりは、データの更新の問題だと捉えることができる。本機構の効率的な利用には、登録情報の新鮮さが重要だという認識があることがわかった。

○prefix filter の利用に関する意見

prefix filter とは IP アドレスのプリフィックスを指定して不本意な IP パケットの転送を防ぐフィルタリングの方法である。多くの ISP で使われている他のフィルタリングの方法には AS path filter がある。本機構は IP アドレスの認可を行なうものであるため、本機構の利点は prefix filter の設定において、偽装登録されたアドレスを使うことが防げる点にある。ISP における prefix filter の利用状況についての意見を以下に示す。

- 国内では prefix filter よりも AS path filter を利用していることが多いと思われる。
- AS path filter では Origin AS のチェック（IP アドレスのプリフィックスを広告している AS 番号の組み合わせのチェック）ができないので、ピア（経路交換と IP パケット転送上の接続）の相手によっては、問題だという認識はある。

○本機構の運用における業務のオーバーヘッドについて

本機構を使うと、IP アドレスを割り振られた者が経路情報の広告をおこなう者に認可を行う必要がある。このことで認可されていない、本来広告されるべきでない IP アドレスが不正に登録されそうになったときに、そのことが検出される仕組みである。しかしこれまでこのような認可行為は明示的になっておらず、例えば RADB では登録される IP アドレスが正しく割り振られたものであるのかどうかのチェックは行われていない。

認可行為が ISP の業務で新たに発生するオーバーヘッドになるとするとどのようなものか、意見収集を行った。

- 運用段階では必要なオーバーヘッドだと考えられる。
- 初期登録の段階では大きなオーバーヘッドがある。

- カスタマーの AS 番号や IP アドレスの登録にオーバーヘッドがある。

特に注目すべき点は三番目のカスタマーの登録である。ISP 事業者によっては接続先の AS 情報の登録を代行しているケースがあり、また海外との接続を行っている場合などに接続先の IP アドレスを自社の AS から広告する必要がある。IP アドレスに対する AS 番号の変更は少ないと言われているが、コネクション・バイ・ボーイング[1]のように AS 番号の変化が起こるサービスが現れている。本機構の登録業務が、BGP の使われ方の実態に合った形で実現できることが望ましいと考えられる。

○ユーザ・インターフェースについて

本機構のユーザは IP アドレスの割り振りを受ける IP アドレス指定事業者等と AS のネットワークの運用を行っている組織（以下、AS 運用組織と呼ぶ）である。IP アドレスの登録業務が主に Web インターフェースを通じて行われているため、本機構も同様に Web インターフェースがよいかどうかについて意見収集を行った。

- Web インターフェースだと状態管理などが必要で、かつリストの参照業務との相互運用性が悪い。メールベースが良い。

上記の意見は AS のネットワーク管理者の意見である。IRR で使われている RPSL がルータの設定内容を生成しやすい形式であるのと同様に、本機構の入出力もテキスト形式で、書式の決まったものであることが望ましいことがわかる。一方 IP アドレス割り振りを受け、認可を行う立場では IP レジストリシステムと統一した Web インターフェースが望ましいと考えられる。

○JPNIC 以外のレジストリから割り振られた IP アドレスの扱い

本機構は基本的に JPNIC から割り振られる IP アドレスを対象としている。これは IP アドレスの割り振り情報の情報源として JPNIC の IP レジストリシステムを利用しているためである。しかし、AS 運用組織によっては APNIC から割り振られた IP アドレスを利用している場合がある。

複数の ISP 事業者から、IP アドレスをも扱えるようにする必要性の指摘があった。その際には、JPNIC にて代行登録をし、正当性は APNIC 等の whois を用いて検証する方法があげられた。

○その他の意見

収集された意見のうち、上記に分類されないものを以下に示す。

---

[1] コネクション・バイ・ボーイング
http://www.boeing.jp/businessunits/j_cbb.html

- 本機構の実現性については、有意性を確認できるようなアプリケーションをプロトタイプシステムとして構築し、提示する必要がある。
- 本機構および IRR の普及には、説明の為のより多くの機会を設けることが重要である
- 本機構の効率的な稼動の為にも、IRR の普及は重要である。
- 本機構の導入プランの検討が必要である。
- 本機構以外の登録情報の正当性向上策
  - JPIRR がルートサーバ（route server）[2]と連携し、経路情報の受信者が比較できる仕組み。
  - JPIRR に登録されている情報と流れている経路との比較ができる仕組み。
  - ガーベージコレクション：登録された情報の一定期間後の清掃の仕組み。

ヒアリングの結果から、今後は本機構のプロトタイプシステムを構築し仕様の公開を通じて、仕様の詳細化を図ることが必要であると思われる。また本機構の仕組みだけでなく、移行プラン等についての検討も必要であることがわかる。

10.4.2. ルーティングの安全性検証を行う為の実験について

JPNIC では、ルーティングの安全性向上を図る機構の効果や運用可能性について検証するため、実験環境の構築を進めている。2005 年度は JPNIC IRR 企画策定専門家チーム・メンバーおよび奈良先端科学技術大学院大学の専門家の協力の下、実験環境の検討と一部の構築を進めた。本節では 2005 年度の段階で想定された実験と実験環境について述べる。また今後の取り組みの方向性について述べる。

〇実験の目的

本実験の目的は、ルーティングにおける安全対策の新たな技術を試験的に運用することを通じて技術の検証をすると共に、効果が高い技術の実用性のある運用形態

[2] BGP などの経路情報交換プロトコルを使って、経路情報を提供するサーバ。このサーバとピア接続すると、そこで提供している情報を受け取ることができる。

を検証することにある。

実験を通じて得られた検証結果は、安全対策の運用形態作りに役立てると共に、ISP 等との情報共有を図る。

〇実験の方法

本実験は、安全対策となる技術を実際に運用することを通じて検証を行なうため、ルーティングのできる環境を構築し、その環境の中での技術検証、観測等を行なう方法で実施する。専門化との意見交換の結果、まず下記の点についての技術検証が必要であると考えられる。

- ルーティング・セキュリティにかかわる脅威の確認
- Secure BGP の利用検証
- Secure BGP のルータ運用への影響

これらを何段階かのフェーズに分けて実施する。これらの他の技術についても可能な限り取り入れ、検証項目を挙げて確認作業を行なっていく。

〇実験環境のネットワーク構成

実験環境のネットワークは、検証内容に応じて段階的に構成を変化または拡張していく。はじめに、経路情報の伝播の際に起こる脅威を確認するためのフェーズの、ネットワーク構成を図 10-1 に示す。

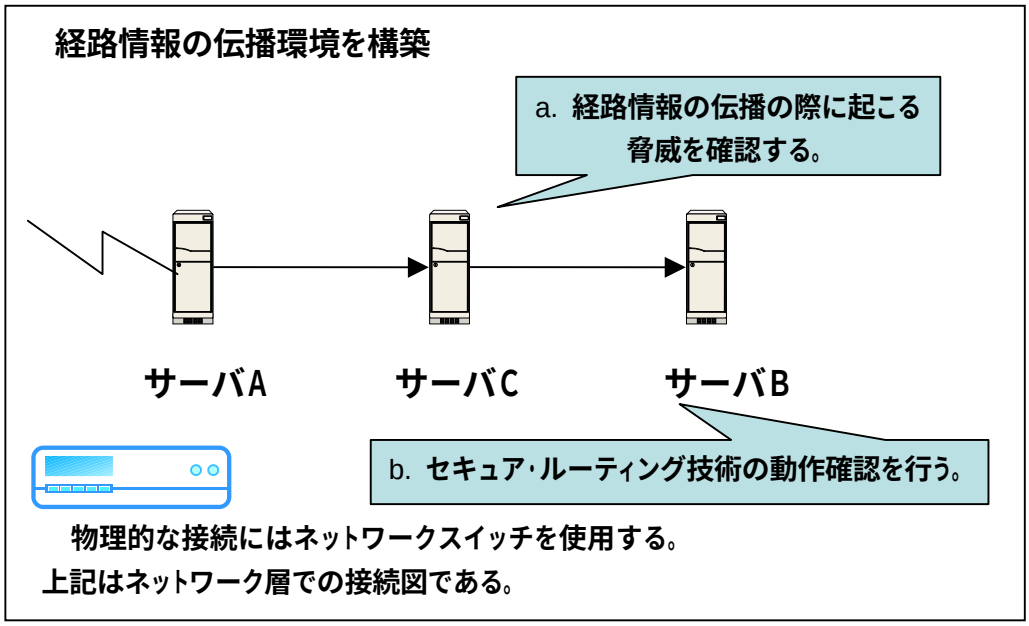

図 10-1 フェーズ１のネットワーク構成

各サーバはルータの役割を持ち、経路情報の交換をインターネットで行なわれているのと同様に行なう。次に不正な経路情報の伝播とその観測を行う環境を構築する。サーバ A とサーバ B でセキュアなルーティングを行う為、図中のサーバの他にリポジトリ／情報サーバを設ける。またサーバ A とサーバ C の間、およびサーバ C とサーバ B の間の観測を行うサーバを設ける（フェーズ２）。フェーズ２の環境構築と実験は、2006 年度に行なう予定である。

○実験の実施状況

現在一部のサーバが稼動しており、経路情報を交換するための環境構築を継続して実施している段階である。なお、環境構築に当たってセキュアなルーティングに関する技術情報の収集を行なった。その情報源を下記に示す。

- Secure BGP Project (S-BGP)
  http://www.ir.bbn.com/sbgp/
- soBGP
  ftp://ftp-eng.cisco.com/sobgp/index.html
- 経路制御の安全性向上 S-BGP/soBGP (Interdomain Routing Security Workshop)
  http://www.bugest.net/irs/docs_20041015/1.soBGP_vs_S-BGP_byTOYAMA.pdf

他に第 9 章で述べた JPNIC の登録情報の応用手法についても検討している。

○実験の今後の方向性

まず本実験はフェーズ１およびフェーズ２の検証を進めることが基本となる。この他に考えられる実験の方向性を以下に挙げる。

- 日本国内の ISP および IX との実験
  インターネットにおけるセキュアなルーティングの実現には最終的に日本国内外の ISP によってセキュアなプロトコルが運用される必要がある。ISP のサービス継続性の面から検討できるよう、調整を図り連携して進めることが考えられる。

- APNIC および RIR との認証の連携
  インターネットにおけるルーティングは国内の ISP に閉じたものではなく、アジア太平洋地域を始め、国際的に行なわれている。国際的な ISP 間の接続においてセキュアなルーティングには、国際的な認証の連携が必要となる。そのため APNIC と認証の連携を行うことで、IP アドレスの管理体系と整合性のある形の信頼モデル構築を図ることが考えられる。

なお 2006 年 3 月現在、2006 年度に実施する見込みとなっている、電子認証フレームワークに関する調査研究の中に位置付けられる調査研究に「インターネットにおける不正登録排除の為の認証基盤に関わる調査研究」がある。本実験はこの調査研究の一環として継続する予定である。