経済産業省受託調査研究

電子認証フレームワークのあり方に関する調査報告書

2006 年 3 月

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

電子認証フレームワークの
あり方に関する
調査報告書

2006 年 3 月

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

はじめに

インターネットの普及に伴い、電子認証の重要性は大きくなってきた。ネットバブルと呼ばれる 2000 年以降の ICT の発展に伴い、インターネットを使った様々なサービスで電子認証が実施されている。金融機関が実施しているインターネット・バンキング・サービスでは、様々な趣向を凝らしたユーザ認証システムが採用され、ユーザの預金口座を保護する取り組みが行われている。日本政府が実施している電子政府の電子申請システムでは、PKI（Public-Key Infrastructure）を使った電子認証が採用されている。掲示板システムの発展型であるブログの多くでも、パスワードを使ったユーザ認証が行われている。

電子認証とは、ユーザ認証システムのようにアクセスしようとする者（以下、アクセス者と呼ぶ)、もしくはアクセスする先の本人性を確認する技術やその行為を総称したものである。電子認証の対象はユーザである場合があれば、サーバである場合もある。本人でない者による不正なアクセスを防ぐセキュリティを実現する為の仕組みである。コンピューターシステムが持つセキュリティ機能には、大きく分けると対策的アプローチを取るものと構築的アプローチを取るものの二種類がある。前者は不正アクセス等があった後に取られる事後策であるのに対し、後者は不正アクセスが起こらないようにする仕組みを作る事前策である。電子認証は後者の構築的アプローチを取るものだと言える。

2002 年以降、インターネットの IP アドレスを管理している「インターネットレジストリ」でも電子認証の強化策が実施され始めた。2003 年にはアジア太平洋地域の RIR（Regional Internet Registry：地域インターネットレジストリ）である APNIC が、2004 年には主に北米地域の RIR である ARIN や主にヨーロッパ地域の RIPE NCC が、それぞれ認証局を構築し、電子証明書を使った電子認証を実施している。JPNIC でも 2002 年度より調査研究を開始し、2004 年度に認証局の運用を開始した。

しかし、電子認証の技術を適切な利用には様々な要素の検討が必要となる。近年問題になっている「オレオレ証明書」や「オレオレ認証局」がそのいい例であろう。オレオレ証明書とは、ユーザが証明書の信頼性を確認する手段が提供されていないにも関わらずオンライン・サービスで使われ、ユーザがその場で信頼する設定をすることが促されるような自己署名証明書を意味する。事前にその証明書の正しさを確認できないため、本当の通信相手なのか、なりすまし行為が行われているのかが区別できない。オレオレ認証局はオレオレ証明書を認証局証明書として発行されたもので、ユーザが一度その証明書をユーザ環境に組み込んでしまうと、それ以降その認証局が発行したあらゆる証明書を有効だと見なしてしまう可能性がある。

他に、認証結果についてユーザに適切な警告や通知を行なうようなユーザ環境の検討が必要である。PKI を使った電子認証を使うと、暗号アルゴリズムや一方向性ハッシュアルゴリズムを破らなければ、成りすましやメッセージの改ざん行為は理論的に

難しい。しかしユーザの初期設定や注意を促すダイアログボックスの部分が悪用されると、いとも簡単になりすましやメッセージの改ざんができるようになってしまう。

電子認証の適切な利用のためのノウハウが欠乏していることは、IETF（Internet Engineering Task Force）の SAAG（セキュリティエリアのミーティング）や JNSA（日本ネットワークセキュリティ協会)の PKI 相互運用 WG においても度々議題に挙がってきた。電子認証技術の標準化は進んでいるものの、その最良の適用方法をまとめた BCP（Best Current Practice：最良と考えられる実践的知識）のドキュメント化は進んでいないという指摘に対してどのようにアプローチすべきかという課題である。

本調査研究では、「電子認証フレームワーク」という仕組みの検討を通じてこの問題に取り組むこととした。電子認証フレームワークは、電子認証に関わる各種ノウハウをドキュメント化し、参加者のコンセンサスと専門家のレビュを通じて、標準技術的なノウハウの集約を図る枠組みである。日本国内で主体的に技術的な知識の集約を図ることで、これまで主に予め標準化されている技術を利用するだけの状況にある電子認証の分野において、セキュリティ文化の向上やより高度なセキュリティ技術の研究開発を促すという狙いもある。

本調査研究は 2005 年度から 2008 年度の 3 年度の計画で取り組むものである。1 年目である 2005 年度は､「電子認証フレームワークのあり方に関する調査研究」と題し、電子認証の専門家の意見集約を図り、既存の電子認証に関わるガイドライン・ドキュメントの基本的な調査を行った。来年度は実際にノウハウとなるドキュメントを試験的に策定し、レビュのプロセスに関する調査研究を進める予定である。一方、電子認証の実践的な取り組みを並行して実施している。「IP アドレス認証の展開」と題し、2004 年度までに構築した JPNIC の認証局を使って、IP アドレス管理指定事業者（JPNIC から IP アドレスの割り振りを受けている通信事業者）の電子認証や、BGP（Border Gateway Protocol）における電子認証の適用に取り組む。これらの電子認証は、ユーザの所属性の認証やサーバ間の認証である。

電子認証というと自然人の厳密な認証に目が向けられがちであるが、インターネットにおける電子認証の需要は、この仮名的な認証の方が需要が高いと考えられる。なぜなら、社会システムの一部として実装されているネットワーク・アプリケーションの多くは、ユーザを戸籍上実在する人間として捉えるよりも、会社組織への所属や、支払能力を持つこと、他システムに予め登録されていること、といった属性の検証に重点が置かれている為である。電子認証フレームワークは、電子認証の種類に応じてノウハウのドキュメント化を行うことで、分野ごとに適用しやすいノウハウの蓄積を行うことができる仕組みであることが望ましい。従って、JPNIC の実施しつつある電子認証もひとつの事例となることが望ましい。

電子認証の技術の多くは、米国またはヨーロッパにおいて発展してきたものである。日本国内では暗号技術の研究では先進的な取り組みが行われているものの、PKI のような電子認証の概念を規定する技術の発展の例を見ない。日本において開発が進むアプリケーション・サービスは、日本独自の側面で、電子認証に対する要求事項があるはずである。日本国内における科学技術の発展を考える場合、既に確立された概念に則った、既存の技術を利用するだけでなく、主体的な概念形成と技術開発に取り組むことが望ましいと考えられる。

電子認証は、他のセキュリティの技術と同様に「利便性と安全性のシーソー」になりがちとなる技術だと言われている。これは安全性を向上させるには利便性を犠牲にしなければならず、利便性を向上させるには安全性を犠牲にしなければならないという社会的・学術的な通念である。しかし電子認証適用の社会的な影響を踏まえた、実践的なノウハウに基づいて構築されたシステムには、必ずしもこの通念が当てはまらないと思われる。非接触 IC カードを使った自動改札機や社員証システムは、そのよい例である。電子認証の利用によって、むしろ利便性が向上し、その一連の認証の上で新たなサービスが適用できる応用的な基盤となっている。

日本における電子認証はどのような形で普及するべきなのか。電子署名法などの電子署名に関する法整備や SSL/TLS のサーバ証明書の普及が進みつつある現在、この疑問に答える為の取り組みを開始し、利便性と安全性を共に確保した、安心できるネットワーク社会の発展が本調査研究の目指すところである。

目次

第 1 章　調査研究の背景と位置づけ

内容
- 調査研究の背景
- 調査研究の実施内容
- 調査研究の成果物

本報告書の章立て

1. 調査研究の背景と位置づけ

本章では、「電子認証フレームワークの在り方に関する調査研究」の背景と、2004 年度までに行われた IP アドレス認証局に関する調査研究との位置づけについて述べる。また本報告書の章立てについて述べる。

1.1. 調査研究の背景

当センターでは、2002 年度から 2004 年度にかけて「IP アドレス認証局」の構築に取り組んできた。IP アドレス認証局は IP アドレスというアドレス資源の管理を、国際的な連携を図りつつセキュアにするための認証局である。認証局というと、しばしば、認証の機能を一手に担うような総合的な仕組みだと思われてしまわれることがある。しかし認証局は、端的にいえば電子証明書を発行する機能でしかない。電子証明書を使って何をどのように認証するか、ということは電子証明書を使ったシステムを構築する側に任されているのである。従って、認証局がインターネットのアドレス資源（IP アドレス等）のセキュアな管理にどう生かされてくるのかは、認証局を構築、運用し、電子証明書の用途を詳細に検討する必要がある。

2004 年度までに行われた調査研究は、JPNIC におけるこの認証局の役割を明らかにする為の調査研究であった。電子証明書が誰にどのように使われるのか、それによって何がセキュアになるのか、といったことを組み立てていく作業である。2002 年度から 2004 年度の活動の結果、電子証明書を使ったユーザ認証用と、その電子証明書を発行する仕組みの構築の必要性が明らかになってきた。そこで CPS（Certificate Practice Statement：認証業務規程）の検討を行った。その結果、JPNIC に IP アドレスの情報登録を行う「IP アドレス管理指定事業者」の認証を強化し、日本国内の IP アドレスに関する登録情報の正当性を向上させる取り組みを行うこととなった。更に JPNIC で運用される複数の認証局の役割が決まり、その一部が実験的に稼動し始めた。JPNIC の認証局の構築に当たっては、CPS(Certificate Practice Statement - 認証業務規程)の策定や記述例のまとめを通じてノウハウが蓄積されてきた。

2005 年度は「電子認証フレームワーク」と「IP アドレス認証の展開」というタイトルで調査研究に取り組んだ。「電子認証フレームワーク」は、電子認証技術の適切な普及を図るための調査研究である。認証局を実現するための技術である PKI(Public-Key Infrastructure)は、データフォーマットや処理方法の策定は進んでいるものの、広く普及していない。PKI でないパスワードベースの電子認証は、フィッ

シングサイトによるパスワードの盗用や通信路の盗聴等、安全性が危惧されているにも関わらず多くのシステムで使われ続けている。この原因は、PKI に比べてパスワードシステムは見かけ上の使い方がわかりやすく、システム構築や初期のユーザ教育が容易であるためだと考えられる。しかし既存の多くの利用法は、システム構築を行うものの知識や意識レベルによるところが大きく、実際には安全でないこともある。すなわち安全な利用方法のノウハウを明文化して、多くの技術者に理解されやすい状態にしておくことが望ましい。いわばノウハウのデファクト・スタンダードである。この標準的で多くの技術者に確認されたノウハウをいかにドキュメント化して残していくか、その共通認識の形成の場はどんなものであるべきなのかがポイントとなる。このノウハウがあれば、パスワードを使った認証システムを安全に運用しやすくなるだけでなく、パスワードよりも安全にしやすい PKI の、適切な普及を図ることができる。

「IP アドレス認証の展開」は JPNIC の認証局の役割を発展させ、登録情報に基づく認証を具体的なアプリケーションに発展させる調査研究である。JPNIC で取り扱っている登録情報のほとんどは IP アドレスに関連付けられた情報である。IP アドレスは Web サーバや企業や家庭のパソコンを始め、電話網や家電など、様々な機器で使われており、用途が広がりつつある。IP アドレスの登録情報を使うと、これらの機器の識別やネットワークとしての所属性を調べられるため、登録情報を基にした電子認証を通じて通信の信頼性を高めることの意義は大きい。

本調査研究の初年度である 2005 年度は主にインターネットのルーティングの安全性向上を図るための電子認証に取り組んだ。インターネットにおけるルーティングは、インターネットの IP パケットの伝送網を支える最も重要な仕組みである。インターネットを利用する全てのアプリケーションに共通して利用される、基盤的な仕組みである。ルーティングの安全性の向上を図らずに、インターネットアプリケーションの可用性向上を図ることは考えにくい。しかしインターネットのような分散環境におけるルーティングは、中央集権的な役割を設けず、各ネットワークの自律的な運用を原則としている。この状況で、ルーティングを安全にするために JPNIC の認証局が提供する電子認証をどのように適用するのかがポイントとなる。

2005 年度は 3 年度計画の初年度であるため、調査研究の方向性を探ることに多くの時間を費やした。本報告書では、調査研究の過程で見出されてきた「電子認証フレームワークのあり方」や「IP アドレス認証の展開のあり方」を様々な情報交換や検討の経緯を交えて報告したい。

1.2. 調査研究の実施内容

本調査研究は、二つのテーマについて取り組む。どちらのテーマも国際会議を通じた情報交換と、専門家による検討を重ねて実施することとなった。

電子認証フレームワークに関する調査研究では、PKI の専門家で、かつ IETF 等の標準的なドキュメント策定の会議に詳しいメンバーでチームを構成して、現在の電子認証の普及に必要な仕組み（フレームワーク）に関する議論を繰り返して行った。その結果、電子認証の適用に関するベストプラクティス・ドキュメントが必要であることが分かってきた。ベストプラクティスとは、IETF で使われている用語である Best Current Practice の意味を示している。これは現在わかっている最善の実践方法という意味で、技術を利用または運用するにあたって判明している、いわばノウハウである。またこのノウハウとして現在必要とされているものを調査するため、電子認証の「保証レベル」やドキュメント策定プロセスに関する基本調査を実施した。

IP アドレス認証の展開に関する調査研究では、IETF 等国際会議を通じた情報交換や JANOG(Japan Network Operator's Group)での意見収集、ISP へのヒアリング等を実施した。その結果、IP アドレス認証の展開の仕組みとして許可リストと呼ばれる仕組みを提案することとなった。この仕組みは、インターネットにおける経路制御（ルーティング）のセキュア化のため、IP アドレスと AS 番号（Autonomous System 番号）の正当な組み合わせを作り出していくためのものである。

1.3. 調査研究の成果物

本調査研究は、IP アドレス認証の展開のあり方、および電子認証フレームワークのあり方を明らかにする調査研究であり調査検討の結果が成果物となる。本報告書では、検討のために使用した発表資料を始め関連性が強い技術標準、ガイドラインに関する基本調査資料などを交えて調査結果を報告する。

1.4. 本報告書の章立て

本報告書の章立てについて述べる。第 2 章では本調査研究のテーマのひとつである電子認証フレームワークの意義と IP アドレス認証局との関係について述べる。第 3 章では IETF における電子認証技術とドキュメント策定プロセスの動向について報告する。IETF では参加者主体のプロトコル策定活動を行っており、電子認証フレームワークのガイドライン策定プロセスを構築するに当たって参考になる活動である。第 4 章では電子認証フレームワークの要件を検討するにあたって調査した、電子認証の運用に関するドキュメントやその策定プロセスについて述べる。第 5 章では第 4 章の調査結果を受け、電子認証フレームワークの在り方について述べる。第 6 章では IP アドレス認証局とその認証の展開について概説する。第 7 章では、IP アドレス認証の展開を行う分野であるインターネットのアドレス資源管理と経路情報の現状について述べる。第 8 章で経路情報におけるセキュリティの現状について述べ、第 9 章で主に電子認証技術を利用した不正利用排除の仕組みについて述べる。第 10 章ではインターネットの可用性維持の為の、安全な経路情報の交換の課題について述べる。第 11 章では本調査研究をまとめ、今後の活動の方向性について述べる。

第 2 章　電子認証フレームワークに関する調査研究について

内容

- PKI と利用上のノウハウ
- 電子認証の普及と BCP
- 電子認証フレームワークとは
- 電子認証に関するガイドライン等の状況

ほか

2. 電子認証フレームワークに関する調査研究について

2.1. 調査研究の背景

近年、インターネットは情報インフラとして認知されるようになっている。日本におけるインターネットの普及は 1990 年代に遡るが、その中で World Wide Web（以下、Web と呼ぶ）の普及は大きな原動力であった。2005 年現在、携帯電話を使って Web の閲覧をしたり電子メールをやりとりしたりできることは、もはや常識と言えるだろう。Web や電子メールはインターネットで使われているアプリケーションの一部に過ぎないが、これらを使って提供されるサービスは数多い。Web や電子メールはこれまで物理的な媒体で実現してきた広告やダイレクトメールを非常に高い費用対効果で代替するツールであるだけでなく、インターネットの双方向性を生かしたサービスを提供するプラットホームでもある。Web を使ったアプリケーションサービスは、しばしば「Web アプリケーション」と呼ばれる。

Web アプリケーションの発展は、特に商用 Web サイトに見ることができる。まず目に留まるのは広告であろう。ユーザが過去にアクセスした商品の情報を元に関連する商品を表示したり、他のユーザの購買履歴を元に、ユーザに「おすすめ」したりする。ユーザが商品に関する情報交換をするための掲示板が設置されていて、そこに書き込まれた商品レビューに対する評価の仕組みもある。様々な商品検討の材料が提供される上に、商品の購入は非常に簡単である。一般的に「カート」と呼ばれる仕組みで、一度クレジットカード情報等の支払い情報と商品の送付先の住所を登録しておけば、商品を選択して「購入」をクリックするだけで購入できてしまう。あとは商品が届くのを待つだけである。購入後は、商品の配送状況が電子メールで通知されたり、ユーザの好みを考慮した関連商品の広告が届いたりする。

小売の商用 Web サイトの他にも、Web アプリケーションによる各種サービス提供が行われるようになってきた。政府が取り組んでいる電子申請や電子入札、教育機関における資料の閲覧サービス、医療機関等で構築されている「Web ポータル」は、その構造上、ほぼ全て Web アプリケーションの仕組みが使われていると言える。民間企業の、顧客に対する各種申し込み等を含めると、企業や個人にとって日常的な活動に密着したサービスが Web アプリケーションで提供されつつあると言える。しかし、ユーザの利便性が高まる一方、これは非常に危険な状況ができつつあるとも言える。最もわかりやすい問題は、ID の盗用である。ID とはユーザを識別するためにコンピューター・システムがユーザを識別する為に割り当てる番号や記号のことで、対面で確認のできないインターネット越しのユーザを識別するために使われる。ID は、本来ユ

ーザ本人だけに使われるべきものであるが、もし他のユーザを別のユーザの ID を利用できてしまうと問題が起こる。前述した小売の商用 Web サイトの場合には、自分が注文していない商品が他人に勝手に注文されてしまったり、商品の届け先が変更されていて、支払いを負わされてしまったりすることが考えられる。企業活動で使われる ID の盗用が起きると被害は更に大きくなると考えられる。ID を盗用されたユーザが被害を受けるだけでなく、システムを提供しているサービス会社側でも発生した損害の賠償責任が問われ、信用の失墜も起こる。ID の盗用が起こるとユーザ側にもサービス提供者側にもメリットはない。Web アプリケーションの普及によって、日常的な活動が他人になり変わられてしまう危険性が大きくなる。

ID の盗用は人的な要素が大きく影響するため、完全に防止することは難しい。例えばパスワードが他人に知られた時に、ユーザ自身が気づくことは不可能であろう。しかし ID の盗用をより困難にし、盗用が起こった場合に追跡調査ができるようにするような対策を講じることはできる。例えばオンラインで本人を確認する「認証」を行うとき、パスワードだけでなく IC カードも使うようにすれば、ユーザはその IC カードが盗まれたことに気づいた時点で、その ID が悪用されないように利用を一旦停止するなどの対処ができる。また、そもそも偽の ID の発行が行われたような場合でも、その登録の記録が残っていれば何が原因であったのかを後になってから調べ、責任の所在を明らかにすることができる。

電子認証の技術は、IDの盗用のような被害を防止する対策となる技術である。パスワードも電子認証技術の一種で特定の情報を「知っていることによる認証」である。その他にICカードなどの認証トークンを用いた「物を持つことによる認証」、指紋や虹彩などユーザの「特徴による認証」などの分類がある[1]。電子認証の技術は、しばしば暗号技術の発展の一環として捉えられることがある。例えば、暗号技術の発展によって元々のメッセージを解読することが難しくなり、従ってメッセージを送った本人になりすますことが難しくなる、といった捉え方である。しかし実際にその暗号技術を使ってシステムを運用させるにはいくつかの落とし穴がある。例えば、暗号化に使われた暗号鍵のデータは、本人しか知らない情報かどうかが確認されていないかも知れない。また元々本人だと思われていた人が実は本人でなかった時、その間違いの原因を突き止めて再発を防ぐ対策が取られているか、といったことである。

これらのことから、認証技術の利用には認証技術そのものの他に、適切に運用していくためのノウハウのようなものが必要であると考えられる。Web アプリケーション

[1] 「Network Security: Private Communication in a Public World」、Charlie Kaufman、Radia Perlman、Mike Speciner、ISBN: 0130614661

の多くで使われているパスワードを上記の暗号鍵に置き換えると、多くの落とし穴が考えられる。アクセスしているユーザが本物かどうか、その判断にはどのようなチェックが行われたのかといった点である。このようなノウハウに則って運用されなければ認証技術はその効果をほとんど発揮しない。Web サーバの認証で使われている電子証明書の技術である PKI も同様のことが言える。

2.2. PKI と利用上のノウハウ

PKI は ITU-T の X.500 ディレクトリサービスの為の認証技術で、X.509 で勧告され標準化された技術である。X.509 の初版である 1988 年版には、既に認証情報の失効（ID の失効）の情報を伝達する仕組みが入っている。パスワードシステムに比べると処理は複雑であるものの、様々な利用場面が考えられる基盤の概念を規定している。1990 年代に入ると IETF で RFC（Request for Comments）としても策定された。現行の RFC3280 では電子証明書の検証方法の詳細がより明確になるなどしている。PKI は基盤的な技術で、特定のアプリケーションに特化した電子認証のために考慮されたものではない。そのため同一の認証情報、PKI の場合には「電子証明書」を、複数のアプリケーションで利用できるため応用性が高い。例えば複数の Web サーバにアクセスするときに一度認証手続きを踏むだけで複数のサーバにログインできる「Single Sign On」の実現に利用できる。

しかし電子証明書の発行手続きにもノウハウが必要である。PKI を使った認証では、認証手続きを受けるもの、例えばユーザは、実際に認証手続きを受ける前に電子証明書を発行してもらっておく必要がある。もし実際とは異なるユーザに電子証明書が発行されてしまうと、それ以降、本来のユーザになりすませることになってしまい認証の意味がない。電子証明書を身分証明書だと捉えると、その運用には新たな観点が必要となる。現実社会における身分証明書は発行に必要な手続きの種類は少なく、例えば日本国内のパスポートであれば、ほぼ一定の確からしさは推測できる。しかし PKI の「サーバ証明書」の場合は状況が違ってくる。サーバ証明書を発行する電子認証サービスは多数存在しており、運営主体も様々で、各々が独自の発行手続きを取っている。するとユーザにとっては見た目が同じサーバ証明書でも、確からしさは様々であるはずである。

すなわち、ユーザが証明書の信頼の程度を識別できるような指針が必要だと考えられる。PKI のような高度な認証技術を多くのユーザに普及することを考えると、このような指針や認証技術の運用ノウハウは、オープンなドキュメントとしてまとめられる必要があると考えられる。

2.3. 電子認証の普及と BCP

日本における PKI の利用に関しては、電子署名の分野について 2001 年に「電子署名及び認証業務に関する法律」が施行されて以降、関連の手続き等に対する常識的な想定事項が作られつつある。それに対し、電子認証の分野ではガイドラインなど実践の規範となるべきドキュメントがない状態にある。Web における SSL/TLS の証明書を用いた認証は一般にも普及しつつあるが、これに反してフィッシング詐欺などの脅威は高まりつつある。電子認証の技術が適切に利用されれば、サーバのなりすまし行為が直接的な被害の原因であるフィッシングを防止できると考えられる。電子認証の技術は、Web ブラウザに実装されていてもそれがこれらの不正行為を防げるような方法では利用されていないのが現状である。

電子認証サービスに関する利用・運用の指針やガイドラインがないことは、リスクに応じた対策を講じることを困難にしているとも言える。ユーザはリスクが高い場合と低い場合とを区別することが難しく、リスクが高い場合でも個人情報を入力してしまったりする。これでは電子認証の技術を利用する意味が薄れてしまい、今後の電子認証の普及を阻害する要因ともなりかねない。

一方、これまで IETF 内の PKIX WG において PKI の基本的なプロファイルやプロトコルの策定が行われてきている。しかし PKI の利用場面では、もはや基本的なプロファイルだけでは足りず、「有効で目安となる使い方」の情報が必要とされている。この Best Current Practice はほとんど蓄積されておらず、PKI を利用してシステムを構築している SI 業者や開発者において短期的な開発方法が用いられるなど、PKI の利点を生かしきれていない状況がある。そこで、この PKI に関する「有効で目安となる使い方」をまとめるべく、民間組織が策定活動に参加して業界での Best Current Practice を策定し、ガイドラインとしてとりまとめることが期待されている。

2.4. 電子認証フレームワークとは

電子認証フレームワークとは、「有効で目安となる使い方」を民間組織が中心となって業界での Best Current Practice を策定する仕組みである。2004 年度、IP アドレス認証局の調査研究を行っている際に、認証技術の専門家による議論の中で必要性が明らかになってきたもので、認証技術の適切な普及に欠けている部分であると考えられている。この仕組みの具体的なあり方は本調査研究を通じて明らかにしていくが、これまでに判明している状況の中では、例えるならば IETF の Best Current Practice 版だと考えられている。

電子認証の技術の利用には、各業界に共通の基盤的要素と業界やアプリケーション毎の応用的要素がある。各々の要素に対して「有効で目安となる使い方」を集約することで、業界に共通のノウハウ、または該当業界におけるデファクトスタンダードとなるノウハウがドキュメント化されることが考えられる。その為には、IETF におけるプロトコルの標準化活動と同様に、民間組織によって主体的な活動を行い、利用場面やアプリケーションに即したガイドラインを迅速に策定していく必要がある。

すなわち電子認証フレームワークは、民間組織における電子認証の適切な利用を促進するための枠組みである。

2.5. 電子認証に関するガイドライン等の状況

電子認証の利用や運用に関するノウハウをドキュメント化していくことを考えるにあたり、内容やその策定仕組みとしてどのようなものが必要になってくるのか、という点がポイントになる。ここでは既に明らかになっているガイドライン等の策定に関わる状況について述べる。

（1） 民間で利用できるガイドライン・ドキュメントの欠如

はじめに挙げられる点は、政府機関における電子認証のガイドライン・ドキュメントが国内外において整備されつつある中で、民間サービスで利用できるものが存在しないことである。現在、日本で電子認証に関して利用できる適切なガイドライン・ドキュメントが存在しない。具体的な状況としては以下に示す。

- 米国では e-Authentication Guidance で定められた 4 段階のレベルのレファレンスがある、日本では同様のレベル付けはない。
- 監査基準を一種のガイドラインとして捉えると、WebTrust for CA などが該当するドキュメントとして挙げられる。しかし CP（Certificate Policy – 証明書ポリシ）を規定していなかったり、現在の要求水準からは不足と思われる項目が少なくなかったりする。
- 現状では日本国内で提供されている電子認証サービスおいて、セキュリティに関する保証レベルを評価することができない。認証業務の安全性レベルは、電子認証サービス毎に独自に設定されるもので、ユーザがサービスごとの安全性レベルを比較するにはエンドユーザにはわかりくい CPS を読んだり、認証局の監査報告書を見たりする必要がある。そのため、ユーザは費用の高いサービスがセキュリティも高いと認知されるなど、実態に即したサービスの評価がなされていない。

（2） 脅威の高度化

電子認証におけるセキュリティ上の脅威としては、以下の状況が認められる。

- Web における SSL/TLS の安全な利用については、検証できない証明書を信用しないなどの普及啓発が進みつつあるが、正式な証明書を用いたフィッシングサイトが出現するなど、電子認証の利用に際して利用者に求められる知識も高度化しつつあり、適切な利用を阻害する原因となりかねない。

（3） 日本の認証に固有の条件

上記(1)(2)の状況に加え、ガイドライン・ドキュメントを策定する活動を行う場合、日本では以下のような事情を考慮する必要がある。欧米で規定されたものをそのまま適用できない。

- 人を対象とした認証の場合、欧米諸国では個人名での認証のみを考えればよいのに対し、日本では個人名のほかに、役職名による認証を行う場合がある。これは特に法人などを対象とした認証サービスを行う場合には欠くことのできない条件となる。

2.6. 日本におけるこれまでの取組み

電子認証を対象としたガイドライン・ドキュメントに関連するこれまでの取組みとして、以下の事例が挙げられる。

（1） 認証局運用ガイドライン（電子商取引実証推進協議会（ECOM））

1.1.1.3(2)で示したように、ISO（International Organization for Standardization）や IETF 等で検討されている電子認証もしくは認証局に係わる各種のガイドラインの内容や、ECOM（Next Generation Electronic Commerce Promotion Council of Japan）内で認証局の実験を行ったプロジェクト等からの意見をもとに 1998 年 10 月に策定されたガイドラインである。

（2） 保健医療福祉分野PKI認証局 証明書ポリシ（厚生労働省）[2]

保健医療福祉分野においてサービス提供者及びサービス利用者への署名用公開鍵証明書を発行する「保健医療福祉分野 PKI 認証局」による証明書発行（失効も含む）に

[2] 保健医療福祉分野PKI認証局 証明書ポリシ
http://www-bm.mhlw.go.jp/shingi/2005/04/dl/s0401-1a.pdf

関してその適用範囲、セキュリティ基準、審査基準等の一連の規則を定めるものである。厚生労働省における医療情報ネットワーク基盤検討会での審議を経て、2005 年 4 月に策定された。引き続き、公開鍵基盤認証局の整備と運営に関する専門家会合での検討が続けられている。

（3） 時刻認証基盤ガイドライン（タイムビジネス推進協議会）[3]

これまで時刻の証拠能力の担保に関してはその重要性に反して指針が存在しなかったことを問題意識として、政府・地方公共団体におけるタイムスタンプの利用に焦点を置いて 2003 年 3 月に策定された。タイムスタンプに関するガイドラインとして利用側における要件、提供側における技術基準、運用基準等を規定している。

（4） 電子認証ポリシーガイドライン（日本 PKI フォーラム）

現在、日本PKIフォーラムの相互運用技術検討部会ポリシーサブワーキンググループにおいて検討が進められている。電子認証に必要とされるセキュリティレベル、信用レベル等について国内及び海外の調査を実施し、事業化において必要とされる電子認証のポリシについて検討することが予定されている。[4]

2.7. 電子認証フレームワークに期待されること

電子認証フレームワークは諸外国のガイドラインと異なり、民間組織に利用されることを想定する。民間組織による電子認証を踏まえて、電子認証フレームワークに期待されるニーズを以下に挙げる。

（1） 電子認証の適用用途からのニーズ

電子認証フレームワークの適用が望まれている用途としては、以下が挙げられる。

- ユーザ認証
  民間組織内、または組織間のユーザ認証の保証レベルを明らかにし、企業間取引において利用できるようなユーザ認証の制度面の整備が必要とされている。大学間のユーザ認証の連携や、医療分野における認証の連携、企業間取引の際に有効とみなされるユーザ認証の保証レベルなどである。

[3] タイムビジネス推進協議会, 時刻認証基盤ガイドライン, 2003.3.
[4] 日本PKIフォーラム 2005 年度活動計画
http://www.japanpkiforum.jp/info/plan/2005/pl_sougo.htm

- IP アドレス認証
  JPNIC において取り組んでいる IP アドレス認証局は、日本国内の ISP の業務管理者や業務担当者の認証を行うための電子証明書の発行を行っている。この電子証明書は必ずしも自然人を対象としたものではない。ユーザが対象組織に所属していることを確認したり、個人の匿名性を確保しつつ不正発見時の追跡を可能にしたりすることを目的としている。いわゆる「三文判 PKI」の一種と考えられる電子認証である。このような電子認証は既存のユーザ認証システムに組み込みやすく、電子認証の適切な利用を促進しうるものだが、業界内でのデファクトとしての認知が欠如しているなど制度面での整備が必要となる分野である。
- サーバ認証
  サーバを対象とした認証についてはこれまでも行われているが、その認証の保証レベルや業界における認知については上記の IP アドレス認証と同様、あいまいである。一様に Web ブラウザの「鍵マーク」が表示されることで一部の業界ではよしとされている面があるが、実際にはこれはサーバの成りすましをユーザに気づかせることができない、間違った認識である。電子認証の保証レベルなど、業界内での整備が必要である。
- 法人の役職名による認証
  日本の法人においては幅広く行われている承認形態でありながら、欧米にはない慣習である。社内や特定の取引関係グループの内部など、これまでも限られた範囲内での認証サービスにおいては、役職名による認証の有効範囲を内部的に決定することで実現されてきたケースも多いが、電子認証サービスの普及に際しては、より普遍的な規範となるべきものが求められる。

（2） 電子認証フレームワークの仕様に関するニーズ

一方、フレームワークが提供すべき仕様に関するニーズとしては、これまで示してきたように日本国内では電子認証サービスの比較において、セキュリティに関する保証レベルを評価することができないことから、以下のバリエーションに応じた電子認証サービスを提供するためのフレームワークを用意することが求められていると考えられる。

- 電子認証に関係する役割の整理
  電子認証の技術を利用するには、サービス提供者とサービス利用者の他に、認証サービス事業者や監査人等の関係組織がある。またアプリケーションベンダーは出荷時に、特定の認証局を信頼する設定にしておくことが多い。その他に、実際に電子認証の設計を行うのが、システム・インテグレーターやソリューション・ベンダーと呼ばれる業者であることが多い。電子認証の適用にあたって関係組織の整理を行う必要がある。
- 保証レベル
  民間組織における認証の安全レベルは、特定の基準に則って形成されるよりも、

サービスに必要な最低限のものとして設定されると考えられる。従って、諸外国の政府のガイドラインのようにすべてが準拠性を要することが適するとは考えにくい。業界に共通する部分は準拠性を以って適切な普及を図りつつ、業界毎の部分は各業界のセキュリティ文化の向上を図りつつ規定する必要がある。

2.8. 電子認証フレームワークのあり方に関する調査事項

電子認証フレームワークのあり方に関して調査研究を実施するにあたり、「電子認証の運用に関するドキュメントに関する基本調査」と「電子認証の技術とドキュメント策定プロセスに関する調査」を行った。

電子認証の運用に関するドキュメントに関しては、既存の電子認証の運用に関わるガイドライン・ドキュメントについての基本調査を行った。本調査では、ガイドラインと捉えられる既存のドキュメントについて諸外国及び日本国内の状況を踏まえて調査を行った。

電子認証の技術とドキュメント策定プロセスに関しては、電子認証技術である PKI のプロトコル策定動向について、IETF のミーティングに参加し調査を行った。また IETF においてドキュメント策定プロセスの見直しに関わる活動が始まっているため、関連 WG に参加し動向を調査した。

次章では、電子認証技術である PKI の国際動向について述べ、その状況を受けて行ったこれらの基本調査については第 3 章で述べる。

第 3 章　IETF における電子認証とドキュメント策定プロセスの動向

内容

- IETF における動向調査について
- 電子認証の技術に関する動向
- 経路制御技術に関する国際動向
- ドキュメント策定プロセスの動向
- 2005 年度の IETF の動向

3. IETF における電子認証とドキュメント策定プロセスの動向

本章では、IETF（Internet Engineering Task Force）における電子認証技術の動向とドキュメント策定プロセスの動向について述べる。はじめに IETF に着目することの意味について述べ、次に動向について簡潔にまとめる。最後に実際に参加して調査を行った IETF ごとの報告をまとめる。

3.1. IETF における動向調査について

IETF はインターネットで使われるプロトコルの仕様を議論し、主にその仕様の文書化を行っている任意団体である。IETF は年に 3 回行われる会議の名称でもある。この会議は、運用や開発に関わる研究者や開発者が個人として参加し、実際の実装と運用に基づいた"業界標準"としての仕様を決めているという特徴を持つ。現在インターネットで使われているプロトコルのほとんどが IETF によってドキュメント化され、その仕様が普及していることから、ネットワーク技術者に限らず情報セキュリティの研究者等、様々なエンジニアの関心を集めている。この IETF において策定されたドキュメントは主に RFC(Request for Comments)と呼ばれ IETF の Web ページを通じて公開されている。

IETF では基本的にワーキンググループ（以下、WG と呼ぶ）でプロトコルの策定活動が行われる。WG 毎にメーリングリスト（以下、ML と呼ぶ）が設置され、年間で 3 回行われるミーティング以外では、ML で議論が行われている。WG の ML は参加者に制限はなく、料金の徴収もない（ただし、IETF のミーティングは 2006 年 3 月現在、550 ドルの参加費用の支払いが必要である）。

IETF におけるプロトコル策定活動は、ML での議論の知識さえあれば誰でも参加することができる。しかし参加者は当該 WG で扱われている技術について専門的な知識を持っていることを前提として議論が進められる。従って技術を解説するようなプレゼンテーションや勉強目的の会合はほとんどなく、参加者自身が勉強をして IETF に臨む必要がある。WG 活動の状況によって議論の方向性が変わるため、当該 WG の関連する技術とプロトコル策定状況に関しての知識も要する。

IETF の大きな特徴は、参加者が主体となって積極的にプロトコル策定を行っていくことにある。前述のように参加者自身が勉強してくる状況では、プロトコル策定の

主要なメンバーには必然的にその分野のエキスパートが集まることになる。よく理解していない参加者は本質的な議論に実質的に参加できず、プロトコル自身は技術的に優れたものになりやすい。一方で専門的になりすぎてプロトコルの実装が難しくなり、利用場面が限定的になってくることもある。これらは ITU-T や JIS などの標準化活動には見られない特徴である。

本調査研究では IETF 特有の活動に着目し、電子認証技術の PKI（Public-Key Infrastructure）に関する動向と、プロトコル策定プロセスの動向について調査を行った。

3.2. 電子認証の技術に関する動向

2005 年度、最も大きな電子認証の技術に関する動向として「一方向性ハッシュ関数の弱体化」について述べる。

一方向性ハッシュ関数は、入力データに対して逆算の難しい演算処理を何度も行い、一定の長さの値を出力する計算処理（関数）である。この一方向性ハッシュ関数の SHA-1 が、新たに発見された攻撃方法によって、本来備えているはずの性質を保てなくなり、SHA-1 を使ったセキュリティの機能の弱体化を招いてしまうこととなった。

SHA-1 は X.509 形式の電子証明書で使われている。今回弱体化した一意性の確保ができなくなると、偽装された電子証明書を正しいものと判断してしまう恐れがある。なお SHA-1 以外では MD5 を使えるが、MD5 も同様の弱体化が既に起こっている。従ってこれらの一方向性ハッシュ関数を利用したプロトコルの全てが、その関数に頼っていたセキュリティの機能を維持できなくなる。電子証明書の他に S/MIME や OCSP などがある。

IETFでは、HASH BoFを開催してIETFにおける標準化活動における対策を検討し、またIRTFにCFRG（Crypto Forum Research Group）を設置して継続的な議論を行っている。HASH BoFでは、米国のNIST（National Institute of Standards and Technology）が主催しているCryptographic Hash Function Workshop[1]で行われた議論の結果を受けて、IETFにおいてもSHA-2 シリーズへの移行が提案されている。また長期的には特定の関数に依存しない仕組みを検討することも提案されている。

これらの対策によって、今回の SHA-1 の弱体化の影響を減らすことができるが、対策の実施にはいくつか課題がある。まず既存の SHA-1 しか対応していないソフトウェアから、SHA-２等の新たな関数に対応したソフトウェアへの移行プランである。

[1] Cryptographic Hash Function Workshop
http://www.csrc.nist.gov/pki/HashWorkshop/index.html

SHA-1 を利用しているソフトウェアは、認証局で使われているなど、簡単に入れ替えることが難しい可能性がある。また有効期限を長く設定し、すでに発行されている認証局証明書をどのように扱うか、という対処方法が明らかになっていない課題もある。今後、議論が進められることで、移行プランや新たなプロトコルのための枠組み作りが行われていくと考えられる。

3.3. 経路制御技術に関する国際動向

2005 年度の経路制御技術に関する動向として、SIDR（Secure Inter-Domain Routing）と IRR の議論について述べる。

SIDR は、セキュアなドメイン間ルーティングの経路情報交換プロトコルの策定を行う為の WG である。経路情報交換プロトコルは、インターネットの接続性を維持するために、通信経路に関する情報を交換するプロトコルで、その安全性の確保は重要な課題になっている。これまで、RPSEC（Routing Protocol Security）WG において、セキュアな経路情報交換プロトコルの安全要件をドキュメント化する活動が行われてきていたが、新たなプロトコルを使ってセキュアな経路情報交換を実現する活動には至っていなかった。

SIDR では主に、S-BGP や soBGP といった認証機能を持つプロトコルを扱い、RIR の認証局との連携を視野に標準化を進めていく模様である。SIDR WG は 2006 年 3 月の第 65 回 IETF において新たに設置された。第 64 回 IETF ではそのための BoF が開かれ、趣意の確認や執筆をサポートするメンバーの募集が行われている。

IETF における IRR に関する議論は、第 64 回 IETF の CRISP WG と Technical Plenary で行われた。この議論は、IRR のようなルーティングに関する情報の原本となるデータの信頼性向上は、どのように図られるべきか、というものである。

現在多くの登録数を持つ代表的な IRR に、Merit 社が運用する RADB がある。しかしこれらの IRR はインターネットレジストリが保持している IP アドレスの割り振り情報との整合性は確認されておらず、実際には割り照られていないアドレスが登録され、インターネットで使われている可能性がある。この問題に対し、JPNIC の IRR 企画策定専門家チームでは、インターネットレジストリによる IRR の運用を提案し、登録情報の整合性を保つために使うことができる CRISP の RREG 書式の提案を行ってきた。

しかし CRISP WG では、第 64 回 IETF で開かれた WG セッションで、RREG 書式はルーティングの登録情報という大きな論点があり、WG のスコープを超えているという判断がなされた。また同じ第 64 回 IETF の Technical Plenary のオープン・マイクロホン（参加者が自由に発言できる時間）では、IRR が RIR と同様のツリー構造を持つことの妥当性について議論された。この話題は多くの参加者の関心を集め多く

の意見が寄せられた。中でもインターネットレジストリにおける IRR の運用が、IP アドレスの管理がルーティングに関与すべきでないという原則に反するという意見は強い。また RADB のようにルーティングのコミュニティで利用されているサービスが、RIR や NIR とは別であることに疑問を持っていない様子の意見も多く見受けられた。

この話題は、アプリケーション・エリアのエリアディレクターであるテッド氏の協力を仰ぐことができる見込みから、プロトコル策定の方向性にまで議論が到達することができれば BoF を開催できる可能性がある。しかし JPNIC のようにインターネットレジストリとある程度の登録数のある IRR が同一の組織で運用されている状況は、他の地域については理解されにくく、IRR の信頼性確保という根本的な課題の取り組み方を具体的に示していく必要があると考えられる。

3.4. ドキュメント策定プロセスの動向

IETF におけるドキュメント策定プロセスの動向について、PESCI（Process Evolution Committee of the IETF）と TECHSPEC BoF について述べる。

PESCI は IETF のプロトコル策定プロセスを評価するため、IETF チェアの Brian Carpenter 氏によって結成された委員である。第 64 回 IETF で初めての BoF が開催された。PESCI BoF では、策定プロセスの変更の際に留意されるべきプリンシパル（原則のようなもの）の考え方について紹介され、議論が行われた。プリンシパルは、意味的に原則となるべきものと、プロトコル策定の作業上の原則となるものなどに分かれると考えられている。

PESCI は今後、BoF の議論を受けて Committee のメンバーを中心に論点の整理を進め、プロセス変更の要点やゴールを明らかにしていく予定になっている。

TECHSPEC BoF は、第 64 回 IETF で開かれた BoF で、IAB が中心となって IETF のドキュメント化プロセスに対する要求事項を整理するために行われた。この BoF では、具体的な要求事項として編集（editor）のタイミングを早め、著者へのフィードバックをなるべく早い段階でできるようにする改善点が挙げられた。

IETF におけるプロトコル策定プロセスは、これまで大きな変更はされず運用されてきた。近年、ドキュメントの数の増加に伴い、RFC editor（RFC の為の整形や整理を行うグループ）の負荷が高まり、既に IESG の承認が降りているにもかかわらず、RFC として公開されるのが遅れるケースが顕著になってきていた。しかしここ一年は、RFC editor の体制の改善やドキュメント活動に関わるツールの提供などの影響で、状況は改善されつつある。ただしこれまでは、ドキュメント化の作業を進める上での改善が図られてきた。今後は PESCI や TECHSPEC BoF のような見直しの活動を通じて、ドキュメント策定プロセスの意味的な改善が進み効率的で有効性の高いドキュメ

ントが作られやすい環境作りが行われていくと考えられる。

3.5. 2005 年度の IETF の動向

最後に、2005 年度に参加した第 63 回および第 64 回 IETF ミーティングの動向について、ミーティング毎にまとめる。

3.5.1. 第 63 回 IETF の動向

◆第 63 回 IETF の概要

2005 年 7 月 31 日(日)～8 月 5 日(金)、フランスのパリにある Le Palais des Congress de Paris(パレ会議場)で、第 63 回 IETF が開催された。今回のホストは France telecom、協賛は Cisco Systems、Juniper Networks、 Renator の 3 社で、フランスの大手通信企業とネットワーク機器ベンダの大手企業が占めていることになる。

IETF Chair による発表によると今回の IETF の参加登録者数は 1,454 名であった。前回の IETF まで参加人数が減少傾向にあるが、今回は大幅に増加した。近年参加者の間で「IETF の参加者数が減っている」と言われている。そこで実際の傾向を見てみるため、ここ 2 年間の参加登録者数をまとめる。

表：近年（2 年）の IETF の参加人数

開催	参加人数	参加国数	開催地
第 63 回	1,454 名	36 ヶ国	フランス・パリ
第 62 回	1,133 名	28 ヶ国	アメリカ・ミネアポリス
第 61 回	1,311 名	26 ヶ国	アメリカ・ワシントン D.C.
第 60 回	1,460 名	40 ヶ国	アメリカ・サンディエゴ
第 59 回	1,390 名	32 ヶ国	韓国・ソウル
第 58 回	1,233 名	29 ヶ国	アメリカ・ミネアポリス

"Past Meetings of IETF" 発表と各回の IETF の Plenary ミーティングでの IETF Chair の発表をまとめたもの。この発表と Web ページの事後の集計結果が異なることがある。
http://www.ietf.org/meetings/past.meetings.html

1,500 名を毎回越えていた 2000 年頃に比べると少ないが、ここ 2 年間は 1,100 名～1,500 名の間で推移していることがわかる。減少し続けているわけではないようであ

る。一方、人数が多い回は参加国数も多いことから、多様な国から参加している様子が伺える。開催地の気候などが関係しているとも考えられる。

第 63 回の IETF ではチュートリアルを除いて 116 のセッションが開かれた。このうち、WG が結成される前の新しく活動を始める段階の議論を行う BoF は、13 セッションが開かれた。

Plenary(全体会議)は、2 つに分けて行われた。1 つ目は"Operations and Administration Plenary"と呼ばれ、8 月 3 日(水)の夕方に行われた。2 つ目は"Technical Plenary"と呼ばれ、8 月 4 日(木)の夕方に行われた。

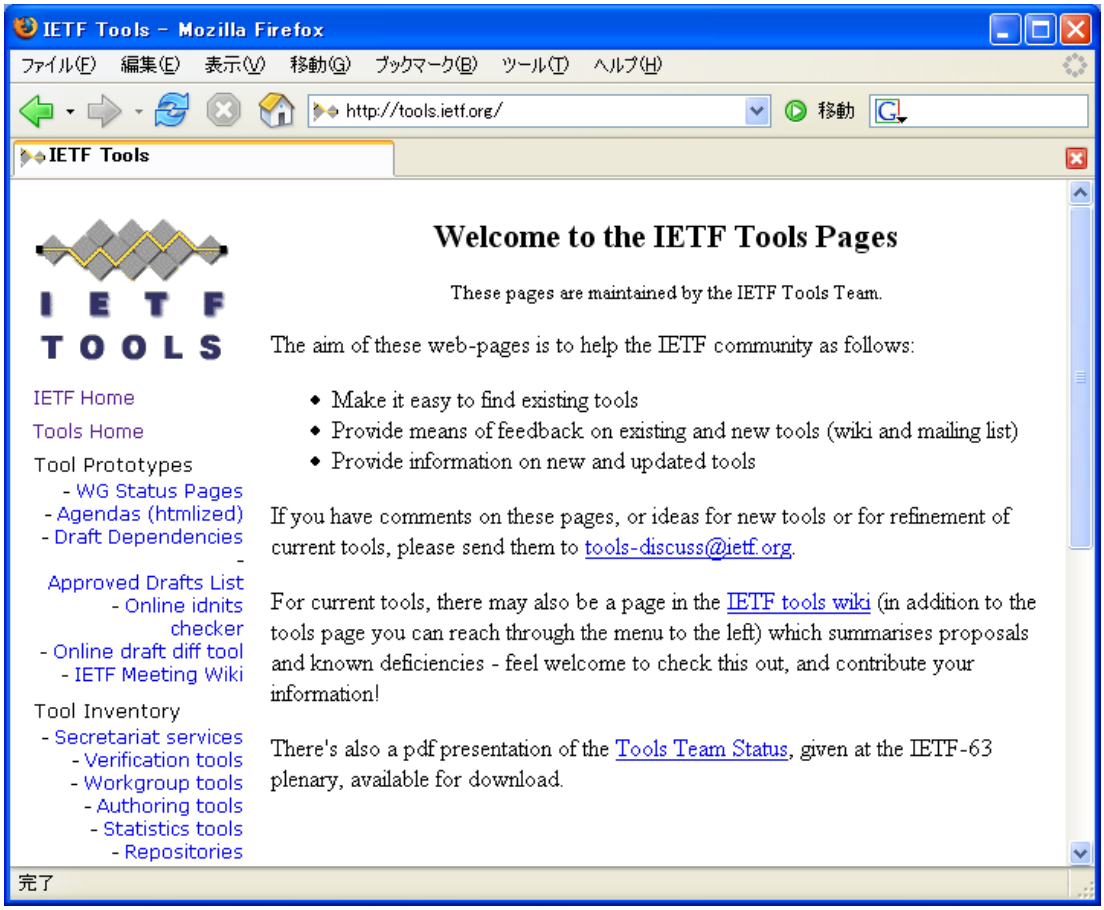
◆Operations and Administration Plenary

Operations and Administration Plenary は、IETF の活動全体の運営に関する報告と議論を扱う全体会議である。この会議では IETF チェアによる IETF ミーティングの参加状況などの概況、ホストであるフランステレコムによるプレゼンテーション、John Postel 賞の発表、IAOC の活動報告、TOOLS チームの活動報告などが行われた。

John Postel 賞はデータ通信のコミュニティで、持続的な技術的貢献をした方や、リーダーシップを発揮した方に送られる賞である。1999 年に故 John Postel 氏に対して贈られて以降、毎年一人ずつ受賞者が選出されてきている。今回は前 JPNIC 理事長である村井純氏に対し、彼のビジョンと先駆者としてのアジア地域におけるインターネット普及活動の推進を称えて贈られた。

IAOC(IETF Administrative Oversight Committee)の活動報告では、メンバ紹介やこれまでに行われたミーティングについて報告された。IAOC は 2004 年の始め頃から行われている、IETF の運営管理体制の再編の活動の一環として作られた委員である。IETF の予算や活動計画、契約などに関する IAD(IETF Administrative Director)の提案に対してレビュを行い、活動の方向性を示す役割を担っている。

TOOLS チームの活動報告では、これまでに開発されたツールの紹介が行われた。TOOLS チームは 2004 年の中頃に当時の IETF チェアである Harald 氏らによって提案されたもので、IETF におけるドキュメント化活動を支援するツールの開発などを行うチームである。開発されたツールは下記の Web ページから利用できる。



図：IETF TOOLS　http://tools.ietf.org/　　Copyright (C) The Internet Society (2005)

IETF Tools の Web ページではドキュメントのステータスや WG のマイルストーンをリアルタイムに表示するツールの他に Internet Draft(以下、I-D と呼ぶ)の書式をチェックするツールなどがある。WG チェアや I-D の著者の助けになりそうなものが多く見られる。

IETF Last Call となっている全ての I-D を表示するツールなどもあり、次に RFC になる I-D を比較的簡単に探せるようになっている。RFC に則ったプログラムの開発を行っている開発者に役立つツールと言える。

◆Technical Plenary

Technical Plenary は IETF の活動のなかで技術的な議論を扱う全体会議である。前エリア・ディレクターの Steve Bellovin 氏によるプレゼンテーションや、IAB の活動報告、IRTF の活動報告などが行われた。

Steve Bellovin 氏のプレゼンテーションでは、"Application Security:Threats and Architecture"と題して、プロトコルのアーキテクチャ(設計上の考え方)に起因するセキュリティ上の問題点とその仕組みが解説された。後半ではセキュアなネットワーク・アプリケーションを設計する為のポイントなどが整理して紹介された。Steven Bellovin 氏のプレゼンテーション資料は下記の Web ページにまとめられている。

"Steven M. Bellovin -- Talks"
http://www.cs.columbia.edu/~smb/talks/

IAB の報告では、IAB で作られているドラフト・ドキュメントの紹介や今年にフォーカスする話題についてプレゼンテーションが行われた。

IAB では、ドメイン名が商標やネットワーク・サービスの存在の推定に使われてしまうことの問題についてまとめたドキュメント(draft-iab-dns-assumptions)や、データリンクの状況がインターネット・アーキテクチャに対して持つ役割に関するドキュメント(draft-iab-link-indications)の編纂が進められている。一方プロトコルのレビュをする立場の人にわかりやすいモデルの記述方法をまとめた"WritingProtocol Models"が RFC4101 になった。IAB では IETF における仕様策定活動に共通するトピックのドキュメント化活動が行われている。IAB のドキュメント活動と現在の活動内容については下記の Web ページにまとめられている。

IAB Documents and Current Activities
http://www.iab.org/documents/index.html

また IAB の概要については下記の Web ページにまとめられている。

About the IAB
http://www.iab.org/about/description.html

今年、IAB では IPv6 の利用の為の実装上のソリューションや、インターネット・エンジニアリングの上で共通の知識となるような"原理"に関するドキュメント、望ましくないトラフィックが起こる可能性を減らしたり、悪影響を小さくしたりするためのツールを提供することを想定した、プロトコルやインフラに関するドキュメントの 3 つにフォーカスして活動するとのことである。

IRTF 報告では、新しく設置される見込みとなっている Research Group の紹介が

行われた。その中で新設が検討されている Internet Congestion Control Research Group としてフォーカスする技術として XCP(eXplicit ControlProtocol)が紹介された。この他の IRTF の Research Group については下記の Web ページにまとめられている。

IRTF Research Groups
http://www.irtf.org/groups

◆電子認証関連の WG

Technical Plenary は、最後に"Town Hall Meeting"と呼ばれる参加者同士の自由討論が行われ、会場の都合で IETF として異例の 19 時半という早い時間に終了した。

第 63 回 IETF では、17 のセキュリティエリアのセッションが開かれた。そのうち 4 セッションが新たに開かれた BoF であった。

今回開かれた BoF は下の 4 つである。

・Hash BoF(One-way Hash Function BoF)
・ALIEN BoF(Anonymous Identifiers BOF)
・MASS BoF(Message Authentication Signature Standards BoF)
・SECMECH BoF(Security Mechanisms BoF)

前回まで BoF が開かれていた BTNS は WG になり、初めての WG セッションとなった。以下では、セキュリティエリアのセッションの電子認証に関わるセッションについてご報告する。

◆One-way Hash Function BoF(ハッシュ関数の脆弱性に関する BoF)

2005 年 8 月 1 日(月)18:15 よりハッシュ関数の脆弱性に関する BoF が開かれた。この BoF は最近発見されたハッシュ関数の脆弱性に対して、どのように対応していくかを議論するための BoF である。話題性のある内容だけに、会場には 150 人程集まり、会場の通路や前方近くに座って参加する人が多数いる程参加者の注目を集めていた。

ハッシュ関数とは、任意の長さのデータに対する演算処理を何度も行い、一定の長さの値を算出する計算処理(関数)のことです。元になるデータが少しでも違うと算出される値が大きく変わる性質を利用して、通信路でデータが改変されていないかどう

かを確認するときなどに使われ、X.509 の電子証明書などで使われている。

ハッシュ関数に関する研究は長年行われてきており、脆弱性を示唆する現象はこれまでにも指摘されてきた。しかし 2004 年中頃から 2005 年にかけて、これまでにないほど影響が大きい研究結果がいくつかの学会で発表された。ハッシュ関数の中に、異なるデータから同じ値が算出されるものがあることが立証されたり、同じ値が算出されるようなデータを探す方法で、効率の良いものが発表されたりしたのである。

IETF で仕様が策定されているセキュリティ関連のプロトコルの中には、MD5 や SHA-1 といった脆弱性が指摘されたハッシュ関数を使っているものが多くある。これらのハッシュ関数の対衝突性(同じ値が算出されるような元の値の探索が難しいという性質)は、実は想定よりも弱いことがわかってきた。

この BoF は、ハッシュ関数の脆弱性に関する現状を把握し、IETF のセキュリティエリアとしてどのように対応していくかを議論するために行われた。BoF の活動趣意やアジェンダについては下記にまとめられている。

□One-way Hash Function BOF (hash)
http://www.ietf.org/ietf/05aug/hash.txt

この BoF では、はじめに米国 NIST(National Institute of Standards and Technology - 米国標準技術研究所)によるワークショップの紹介があった。このワークショップは 2005 年の 10 月 31 日～11 月 1 日に開催が予定されており、既存のハッシュ関数に代わる SHA-256 や SHA-512 といったハッシュ関数の紹介や新しいハッシュ関数への移行方法について議論が行われる予定です。詳しくは下の Web ページにまとめられている。

□CRYPTOGRAPHIC HASH WORKSHOP
http://www.csrc.nist.gov/pki/HashWorkshop/index.html

次に、プロトコルの工夫によって脆弱性を回避する方法がいくつか紹介された。新たなハッシュ関数を開発しその強度を検証するには時間がかかるため、これらの短期的な対策が必要になる。今回プレゼンテーションされたものはいずれも提案の段階で、今後どのような"短期的な対策"と"長期的な対策"が取られていくかは、前述のワークショップでの議論を踏まえて検討されていくと考えられる。BoF で紹介のあったハッシュ関数の現状をまとめた Web ページと今後の議論に使われるメーリングリストの加入方法については、下記にまとめられている。

□Cryptographic Hashes(現状をまとめたページ)
http://www.vpnc.org/hash.html

□ハッシュ関数の脆弱性に関する議論を行うメーリングリストの Web ページ
https://www1.ietf.org/mailman/listinfo/hash

◆PKIX WG

PKIX WG のセッションは、2005 年 8 月 2 日(火)14:00 から行われた。約 60 名の参加で、近年の PKIX WG のセッションとしてはまずますの人数である。はじめにドキュメントステータスの報告が行われた。前回の IETF から今回までの期間に二つのドキュメントが RFC になった。

・Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4055)
・Internet X.509 Public Key Infrastructure Permanent Identifier (RFC 4043)

前者は電子証明書と CRL(失効リスト)で、RSA のアルゴリズムに関連した署名アルゴリズムと鍵共有アルゴリズム、それから一方向性関数の追加について取り決めたものである。後者は Subject 欄などではなく、恒久的な識別子を電子証明書に入れるための拡張である。電子証明書の有効期限が切れるなどして、別の電子証明書が発行されたときでも、同一の識別子を入れておくために使われる。

PKIX WG の議論としては、はじめに"SRV RR"に関するプレゼンテーションがあった。これは_ldap._tcp.domain.com といった DNS の RR(リソースレコード)を使って、電子証明書のデータを格納／取得する方法の提案である。WG としてのドラフト・ドキュメントにはなっておらず、個人のドラフト(draft-santesson-pkix-srvrr-00.txt)として submit されている。これに対し会場からは、DNS のゾーン管理がサーバ証明書の利用を許可するようなモデルで問題がないかを確認する必要がある、といった指摘があった。一方、ML では入手した電子証明書を検証するための信頼の設定について議論されている。

SCVP については、処理能力が低いシン・クライアントでの実装上の問題について議論された。SCVP は電子証明書の検証を、他のサーバに任せて行うためのプロトコ

ルである。今までに上がっている指摘は、複数の認証局証明書を検証するときに、nameConstraints 等の制約をチェックすることが負荷になる点、検証ポリシーと検証アルゴリズムの二つの OID(Object Identifier)が必要になる点の二つである。後者についてポリシーとアルゴリズムをまとめたポリシーOID を設ける提案がなされたが、会場ではまとまらないため、一度個別に議論が行われることになった。

RFC3280bis は、電子証明書と CRL の基本的な扱いを記述するドキュメント RFC3280 の後継となるドキュメントである。RFC3280 には様々な論点が残っており、例えば認証局の鍵を変えるための"Root CA key update"は、RFC2510(CMP)で言及されている古い鍵で新しい証明書に署名をする"new with old"などを組み合わせる手法があるが、改めて記述するようである。この他に keyUsage フィールドに入る nonRepudiation ビットの解釈の仕方をはじめ、6 つほど大きな論点が残っている。

恒例の Liasion Presentation では、ETSI(European Telecommunications Standards Institute)の立場で、Denis Pinkas 氏が CAdES(CMS Advanced Electronic Signature)の紹介が行われた。CAdES は CMS(Cryptographic Message Syntax)を使って長期的に検証可能な電子署名を実現するための書式である。ETSI では XML を使った電子署名の書式である XAdES(XML Advanced Electronic Signatures)を ETSI TS 101 901 と呼ばれるドキュメントにまとめており、これを CMS を使ったものに書き換えるという位置づけのようである。同様のプロトコルに RFC3126 があり、これを更新することを目標としているようである。ドラフト・ドキュメントは下記の URL から入手できる。

□CMS Advanced Electronic Signatures (CAdES)
http://www.ietf.org/internet-drafts/draft-pinkas-smime-cades-01.txt

◆SAAG (Security Area Advisory Group)

SAAG は IETF のセキュリティエリアの全体会議です。各セッションの報告や最近の話題についてのプレゼンテーションや議論が行われている。今回の IETF では 8 月 4 日(木)の 14:00～16:30 開催された。今回行われたプレゼンテーションは、"ITU-T Recommendation X.805"の紹介と"Unicode Security Considerations"の紹介である。

ITU-T Recommendation X.805 は End-to-End の通信を構成するシステムのセキュリティの側面を分類し整理したものである。盗聴やなりすまし、使用不能といった脅威をモデルとして、脅威を避けるための技術要素を分類している。分類は Security Dimensions、Security Layers、Security Planes と呼ばれる三つの観点で行われてい

る。

会場からは、三つの観点の関連性はあるのか、ある脅威に対して適した分類がなされているのか、などの内容の正しさに関する指摘が挙がり、果たしてこの文書が"Recommendation"(勧告)の役割を果たすのかという根本的な疑問が呈される場面があった。

一方、ITU-T のような IETF 以外の会議で、ネットワークのセキュリティがどのように捉えられているのかを知る機会になるという説明があった。この発表は、IETF が議論した結果の"仕様"を決めるミーティングであり、必ずしも IETF における視点だけが正しいわけではないという、控えめな見地に立って行われたようである。IETF における WG 活動とドキュメント活動は長年のノウハウもあって、とても洗練されているが、別の技術標準の状況を知ることによって、また新たな視点を取り込むことができると考えられているようである。

"Unicode Security Considerations(Unicode Technical Report #36)"では、Unicode の利用によって起こる問題点の紹介などが行われた。例えば文字の記述方向が異なる言語を組み合わせて IDN(Internationalized Domain Names)を使って URL を記述すると、URL の途中で右方向に読んだり左方向に読んだりという、使いづらい状況ができてしまう。このような問題に対して、User Agent(Web ブラウザ等)に必要になることなどをまとめたのが Unicode Technical Report #36 である。このドキュメントは下の Web ページで読むことができる。

□Unicode Technical Report #36
Unicode Security Considerations
http://www.unicode.org/reports/tr36/

3.5.2. 第 64 回 IETF の動向

◆第 64 回 IETF の概要

2005 年 11 月 6 日(日)～11 月 11 日(金)、カナダのバンクーバーにある The Westin Bayshore Resort and Marina にて、第 64 回 IETF が開催された。今回のホストは Nortel 社で、スポンサーは BC.NET、Symantec 社、Telus 社の 3 組織である。Symantec 社を除いて、すべてカナダを拠点にしているネットワーク関連の企業や任意団体である。

IETF チェアの発表によると今回の IETF の参加登録者数は 1,291 名であった。前回(第 63 回)の 1,454 名よりは少ないものの、1,100 名から 1,500 名で推移しているここ 2 年間では、まずまずといったところである。この時期の IETF は毎年アメリカ国内で行われてきたが、テロへの警戒の影響でアメリカへの入国手続きが煩雑化している国があり、それらの国からの参加者に配慮して今回はカナダで開催された。参加国は 40 ヶ国と多かったのはその影響だと推測される。

IETF ミーティングは基本的に、初日から始まるチュートリアルと、2 日目以降に行われる WG や BoF のセッション、4 日目や 5 日目に行われる Plenary (全体会議)で構成されている。また IETF には含まれていないがグローバルなインターネットの運用に関する調整を目的とした IEPG (Internet Engineering and Planning Group)ミーティングが、おおむね毎回初日の午前に開かれている。

今回の IETF では 124 の WG や BoF が開かれ、このうち BoF は 14 セッションであった。BoF は、WG が結成される前に活動趣意(チャーター)を決めたり、WG の必要性についてのコンセンサスを確認したりする会議である。

Plenary の一つ目である“ IETF Operations and Administration Plenary ”は 11 月 9 日(水) に、二つ目の“ Technical Plenary ”は 11 月 10 日(木)に開かれた。

◆IETF Operations and Administration Plenary

IETF Operations and Administration Plenary は、IETF の活動全体の運営に関する報告と議論を扱う全体会議である。今回は、IETF チェアの Brian 氏によるチェア報告、ホストを務める Nortel 社によるホスト報告と NOC の運用報告、IAD (IETF Administrative Director)からの報告、RFC Editor 報告、IANA 近況報告、PROTO チームの近況報告などが行われた。

チェア報告ではドキュメント策定状況の報告の他に PESCI (Process Evolution Committee of the IETF)が紹介された。PESCI は IETF におけるドキュメント策定プロセスの見直しを図るため、改善を図るべき範囲を特定し、議論を進めるためのチームである。今回の IETF で初めての BoF が開かれ、策定プロセスを変更するにあたっての考え方を明確にする(明確化されたものは Principles と呼ばれる)議論が行われた。この策定プロセスの見直しについては以下の Web ページにまとめられている。

□ Goals and Principles for IETF Process Evolution

draft-davies-pesci-initial-considerations-00.txt

また続いて、TCP/IP の開発や IETF の創設といった貢献で有名な Vinton G. Cerf 氏と Robert E. Kahn 氏が Presidential Medal of Freedom を受賞したとのニュースが発表された。Presidential Medal of Freedom は米国の市民栄誉賞にあたるようである。

□ The　Presidential Medal of Freedom
http://www.medaloffreedom.com/

IAD (IETF Administrative Director)からの報告では、IETF ミーティング参加費用の値上げのお知らせがあった。ISOC からの補助額は毎年増加しており、2005 年には 100 万ドルを超える見込みがあるものの、RFC Editor の業務増強のための支出増加が見込まれ、参加費用の値上げに踏み切ったようである。2006 年以降に行われる（すなわち第 65 回以降の）IETF のミーティング参加費用は 550 ドルになる模様である。

RFC Editor 報告では、昨年に比べて RFC 化の業務速度が向上しており、ひと月あたりの公開ドキュメント数が投稿される数(30 程度)に近づいているとのことであった。RFC Editor の編集待ちリストは以下の URL で見ることができる。

□ RFC Editor Queue
http://www.rfc-editor.org/queue.html

◆Technical Plenary

Technical Plenary は IETF の活動のなかで技術的な議論を扱う全体会議である。IRTF (Internet Research Task Force)の報告、IRTF の CFRG (Crypto Forum Research Group)のハッシュ関数の問題に関するプレゼンテーション、IAB のチェア報告などが行われた。

IRTF の報告では新設されたリサーチ・グループの紹介とリサーチ・グループの状況報告が行われた。新設されたリサーチ・グループは、Transport Modeling Research Group と Internet Congestion Control Research Group の二つである。

続いて IRTF CFRG のチェアである David McGrew 氏から、SHA-1 や MD5 といった、多くのプロトコルで使われている一方向性ハッシュ関数が脆弱になっている状況と、IETF における対策についての説明があった。対策として SHA-1 や MD5 の利用をやめ、SHA-256 を利用する等の方法があげられていた。移行にかかる期間やアル

ゴリズムの研究と実用化の状況から SHA-2 シリーズの利用の方向性は、ほぼ決まっているという印象を受けた。

最後の IAB のチェア報告では、IAB の役割に照らし合わせた活動報告があった。IAB には IESG や RFC Editor のメンバーの補填(ほてん)のための候補選びや IETF における策定プロセス遂行状況の監視といった役割がある。

□ Charter of the Internet Architecture Board (IAB)
http://www.ietf.org/rfc/rfc2850.txt

今回の IETF では IAB の主導により、TechSpec (Technical Specification) BoF が開かれた。これはドキュメント化の要求事項を見直す活動について議論を行うための BoF である。IETF の WG における議論では、しばしばドキュメント化される技術に対する requirement(要求事項)の整理とレビュが行われる。このプロセスを促進する意味で、現行のドキュメント策定プロセスを見直す必要性が指摘されている。BoF では特に、下記の draft-mankin-pub-req-01 を元に、IETF の現行のドキュメント策定プロセスの中で、編集のタイミングを見直すことについて議論が行われた。

□ Requirements for IETF Technical Publication Service
http://www.ietf.org/internet-drafts/draft-mankin-pub-req-01.txt

Technical Plenary の最後のオープン・マイクロホン(参加者が自由に発言できる時間)では、JPNIC IRR 企画策定専門家チームのメンバーである長橋氏によって IRR (Internet Routing Registry)のあり方に関する議論が行われた。世界各地域の IP レジストリは ICANN/IANA を頂点とする IP アドレスの割り振り構造に従って木構造の関係を持っており、各 IP レジストリにある登録情報の整合性を保ちやすい構造になっている。一方、IRR は IP レジストリのような構造を持たずに運用されており、登録情報の正しさを実質的に担保できるような仕組みはない。

以前より、IRR を IP レジストリで運用し、IP レジストリの割り振り／割り当て情報と照らし合わせて、正しさを確認できるようにするという考え方がある。しかし、ある程度の数のルータ管理者に利用されている IRR と、IP レジストリの両方が一つの組織によって運用されている JPNIC のようなケースは少なく、その効果や実現性が理解されにくい状況があるようである。

Technical Plenary では、インターネットレジストリがルーティングに関与する可能性を高めるような木構造は避けるべきである、IRR は RIR よりも多く必要であり、例

えばヨーロッパ地域では NIR のあるアジア地域のようにはうまくいかない、といった意見が挙げられていた。またオープン・マイクロホンの場ではないが、IETF のプロトコル策定の場だけでなく、ルーティングのコミュニティでの議論が必要だという意見が寄せられていた。

今後、IRR の登録情報に関連したプロトコルの策定と、IRR における登録情報の正当性に着目した議論が活発に行われていくと考えられる。この議論は、本調査研究の「IP アドレス認証の展開」で取り組んでいる「安全案経路制御のための電子認証」の仕組みが大きく関係している。IP アドレスに関する登録情報を使い、IRR に登録された情報との整合性を取る形の電子証明書が発行されると、IRR を補完し、より安全なルーティングが実現する可能性がある。

◆電子認証関連 WG の動向

第 64 回IETFでは、セキュリティエリアのセッションが合計で 18 行われた。このうちBoFはDKIM BoF[2]とEMU BoF[3]の二つである。DKIM BoFによって、2004 年秋のMARID WGのクローズ以降、迷惑メール対策になる技術に関するIETFの活動が再度始まったことになる。また今回のIETFでは、セキュリティエリアではないものの、電子認証に関連したSIDR BoFが開かれた。

本節では、SIDR BoF と PKIX WG、IEPG での AS 番号の枯渇と電子証明書に関する話題などについて報告する。

◆SIDR BoF (Secure Inter-Domain Routing BoF)

---

[2] DKIM BoF (Domain Keys Identified Mail BoF)
迷惑メールなどの中でしばしば行われている発信元メールアドレスのドメイン部分を偽装する行為(スプーフィング)を、電子署名を使って検出できるようにする仕組みについての BoF である。DKIM WG のチャーターでは、現在のスパムをなくすこと自体を目的にするのではなく、安全上の脅威(threats)や要求事項(requirements)をまとめ、また DKIM を使う場合と使わない場合の違いについて分析を行うといったアプローチを取っている。

[3] EMU BoF (EAP Method Update BoF)
PPP や 802.11 等で使われている認証の枠組みである EAP (Extensible Authentication Protocol)方式のドキュメント整備に関する BoF である。EAP 方式を使った認証プロトコルは数多く提案されていますが、RFC になっているものは少なく I-D を元にした実装の相互運用性が確保されていない可能性がある。そこで EAP-TLS(RFC2716)の Proposed Standard 化進めると共に、パスワードなどの方式についてもドキュメント化を進めていくとされている。

これまで RPSEC WG において、インターネットにおけるルーティングの仕組みについて安全上の要件をまとめる作業が行われてきた。

"Generic Threats to Routing Protocols"
draft-ietf-rpsec-routing-threats-07.txt
ルーティング・プロトコルに対する脅威を、原因・可能性・脅威となる挙動・その結果といった形でまとめたもの。

"BGP Security Requirements"
draft-ietf-rpsec-bgpsecrec-03.txt
ルーティング情報の交換プロトコルである BGP(Border Gateway Protocol)を安全にするための要件(requirements)についてまとめたもの。ピア関係や BGP スピーカー同士、交換される経路情報の認証など複数のポイントについてまとめてある。

これらのドキュメントを通じてルーティングの安全性に関する認識が共有できるようになってきたことから、この BoF は論点を先に移して、ドメイン間ルーティングのセキュリティ・アーキテクチャについて議論し、さらに BGP の安全性の機能を定義する、といった活動を行うために開かれた。

この BoF では、まずこの議論とドキュメント化活動が SIDR という新たな WG を設立して行われることの妥当性について議論された。既に RPSEC WG や IDR WG といった WG で、ドメイン間ルーティングのセキュリティについての議論が行われてきたためである。議論の結果、これらの WG では安全上の要件や短期的な解決方法のドキュメント化が行われてきたのに対し、SIDR はドメイン間ルーティングのインフラストラクチャやプロトコルに着目し、経路情報の認証を行う仕組みを検討するという点で独自の趣意を持っていることが確認された。

次に soBGP、S-BGP、psBGP という三つのプロトコルのデザインについて紹介された。これらは経路情報を交換するためのプロトコルである BGP を拡張し、情報源の認証や AS パスの検証といった手続きを通じて、ルーティングの安全性向上が図られたプロトコルである。

soBGP に関するインターネットドラフト(以下、I-D)
・draft-white-sobgp-architecture-01.txt
・draft-ng-sobgp-bgp-extensions-01.txt
・draft-weis-sobgp-certificates-01.txt

S-BGP の情報源
・http://www.net-tech.bbn.com/sbgp/sbgp-index.html

psBGP に関するテクニカルレポート
・http://www.scs.carleton.ca/research/tech_reports/2005/download/TR-05-08.pdf

いずれも IP アドレスと AS 番号の偽装を防ぐために電子証明書が使われており、soBGP と S-BGP では、その電子証明書が IP レジストリで運用される認証局によって発行されることが想定されている。IP アドレスの割り振りを IP レジストリの認証局が証明する(certificate)という意味がある。IP レジストリの認証局が発行した証明書を使うことで、経路情報に含まれている IP アドレスが正当に割り振られたものなのかどうかを判断できるようになる。

BoF では、この証明の基盤に基づく経路情報の認証についての議論を進めることに協力するメンバーがいることが確認された。SIDR WG が設立されると、経路情報の証明データに関するドキュメント活動が行われていくと考えられる。

◆PKIX (Public-Key Infrastructure (X.509)) WG

PKIX WG のセッションは 11 月 7 日(月)の 9 時から行われました。約 45 名の参加で前回の約 60 名よりは減少した。前回の第 63 回 IETF(2005 年 8 月開催)から今回までの期間に、RFC になったドキュメントが三つ、RFC Editor の編集待ちのドキュメントが三つという状況である。

RFC3280 の後継(通称 RFC3280bis)の議論は、ドキュメント改定が進んでいる SCVP (Simple Certificate Validation Protocol)への影響を避けるために一旦停止している。PKIX WG のセッションの後に新たなドラフトの準備が行われるようである。

SCVP の I-D は 21 版となった。SCVP は電子証明書の検証を他のサーバに任せて行うためのプロトコルである。新たに SCVP のサーバが別のサーバからの返答をリレーできるようにするための拡張が行われたりしている。また SHA1 等の一方向ハッシュアルゴリズムの脆弱化を受け、新たなハッシュアルゴリズムに対応できるような書式が盛り込まれることとなった。

2005 年 10 月、米国の NIST (National Institute of Standards and Technology:米

国標準技術研究所)で行われたハッシュ・ワークショップでの議論の結果を受け、OCSP(Online Certificate Status Protocol)における新たなハッシュアルゴリズムへの対応手法について議論が行われた。OCSP はオンラインで失効状況を問い合わせるためのプロトコルで、応答の中で電子署名が使われている。ハッシュアルゴリズムの移行時期には複数の種類のハッシュアルゴリズムが使われることが考えられるため、問い合わせ側(requestor)は応答側(responder)が、どのハッシュアルゴリズムを使うのかを知っている必要がある。今のところ問い合わせ側が応答側に対し、事前に指定する方法が挙げられているが、詳細の検討は今後行われる見込みである。

PKIX WG では、OCSP 以外のプロトコルでも新たなハッシュアルゴリズムに対応する必要性があることが認識されている。なお NIST のワークショップでは、当面 2010 年を目処に SHA-256 というハッシュアルゴリズムへの移行が提案されており、業界全体としての移行プランの検討が始まっている。また SHA-256 の次のハッシュアルゴリズムに関する検討も始まっている。

前回の IETF でプレゼンテーションが行われた draft-ietf-pkix-srvsan は DNS の SRV レコードにあまり依存しない仕様になるようである。このドキュメントは "_ldap._tcp.domain.com"といったドメイン名の SRV レコードを使って証明書データをやり取りする手法を提案したものである。以前は、得られた証明書の中で subjectAltName として指定された文字列と証明書の入手のために使われたドメイン名とが比較されることになっていた。新しい版では、問い合わせ側は予め対象のサーバのドメイン名とサービス名を知っているという前提に立ち、DNS のドメイン名ではなく、問い合わせ側でわかっている文字列(ユーザーに指定されたものなど)と比較をすることになった。ただしこの用法の安全性は再検証される必要があると指摘があった。

◆IEPG における AS 番号の枯渇と電子証明書に関する話題

IEPG (Internet Engineering and Planning Group)は主にインターネットのオペレーションに関して意見交換を行い、調整を行うために IETF の直前に開かれている会合である。

The IEPG
http://www.iepg.org/

第 64 回 IETF の直前に開かれた IEPG ミーティングの中で、RIPE NCC の Henk 氏が AS 番号に関する電子証明書について紹介する場面があった。

RIPE NCCのRIS[4]を使った調査によると、2005 年 8 月 1 日現在、33681 のAS番号が割り当てられていることがわかっている。AS番号として使える番号の総数は 64511 で、まだ残りがあるものの、ひと月に 160 前後の伸びがあり、2013 年から 2024 年の間に枯渇するという予測が立てられている。

枯渇を避ける方法として、AS 番号のビット長を現行の 16 ビットから 32 ビットにする方法と、利用されていない AS 番号を回収する方法の二つが考えられている。前者は、根本的な解決方法でありながらまだ実装がなく、移行プランも立っていない。一方後者は回収した AS 番号が再び使われ始めると AS 番号の一意性が失われてしまうという問題がある。

Henk 氏は後者の問題の対策として、電子証明書を使って AS 番号の利用の証明(certification)を利用する手段について紹介していた。電子証明書を利用すると有効期限を設定したり、有効期限内に失効させたりできるためである。前の利用者の電子証明書が有効かどうかを確認することで AS 番号を再利用してよいかどうかの判断ができると考えられる。

この AS 番号の電子証明書は RIPE NCC の 2006 年活動計画の中に入っている。第 20 回 APNIC ミーティング Routing SIG でも"resource certificate"という考え方が紹介されている。今後、RIR で電子証明書を使った IP アドレスや AS 番号の証明(certification)がさらに検討されていくと考えられる。

[4] RIS: Routing Information Service
http://www.ripe.net/ripencc/pub-services/np/ris-index.html

第 4 章　電子認証の運用に関するドキュメントの現状

内容
- 情報ネットワークやシステムを対象とするドキュメント
- ドキュメントの策定プロセス
- 電子認証に関わる既存ガイドラインの分析
- 調査対象の概要

ほか

4. 電子認証の運用に関するドキュメントの現状

本章では、電子認証に関わるオープンなガイドラインを日本において運用するための要件を明らかにするため、IETF、IP レジストリ及び国内外の政府によるガイドライン・ドキュメントの現状について述べる。はじめに電子認証の分野でガイドラインが求められる背景と必要性について整理するとともに、IETF より提供されるドキュメントのうち、Best Current Practice として扱われるものに着目し、その策定プロセスの分析を行う。次に海外の政府もしくは民間団体によってまとめられた電子認証に関わるガイドラインについて、目的、利用者・利用方法の想定、運用の特徴などについて述べる。

4.1. 情報ネットワークやシステムを対象とするドキュメント

本章では、電子認証に関するフレームワークに関する検討を行うに先立ち、電子認証のような情報ネットワークや情報システムを利用したサービスの構築や運用、利用に関するドキュメントの種類と特徴について概観する。

電子認証に関する構築や運用、利用のために提供されるドキュメントについて、その種類に応じて例を挙げるとともに、どのような経緯で作成されてきたかについて整理する。なお法令、条例等の法的拘束力を有するドキュメントについては、調査対象から除外した。

4.1.1. 各種ガイドライン

文書名に「ガイドライン」を含むドキュメントはこれまでに数多く発行されている。ここではその発行主体によって分類した上でその傾向を示す。

4.1.1.1. 国際機関によるガイドライン

代表例として、OECD（経済協力開発機構）が情報セキュリティと個人情報保護を対象に策定したガイドラインの例を示す。

（1） 情報システム及びネットワークのセキュリティのためのガイドライン（OECD）

1992 年に策定され、2002 年に大規模な改訂が行われた。情報システムとネットワークに関するすべての関係者（参加者）を対象として「セキュリティ文化の醸成」を

目指し、9 つの原則が示されている。[1]

（2） 個人情報保護ガイドライン（OECD）

1980 年に策定された 8 原則からなる。本ドキュメントはガイドラインの位置づけであるが、各国における個人情報保護に関する法制度が本ガイドラインに準拠している場合も多く、影響力が大きいことが特徴である。

（3） Interchange of Data between Administrations (IDA) Authentication Policy（EU）

EU の政府間データ交換委員会（IDA）において、分野別ネットワークとプロジェクトにおける適切な認証メカニズムの構築を目的とした基本ポリシーを定めるものである。保証レベル等の考え方は、1.1.1.2(1)の E-Authentication Guidance と共通する部分が多いが、EU における条件を踏まえて追加されているものもある。

4.1.1.2. 各国政府によるガイドライン

各国政府が策定しているガイドラインの例を示す。ただし、日本以外については電子認証に関するものを中心として扱う。このうち、海外の電子認証に関するガイドラインの事例については次節において詳細な分析を行う。

（1） E-Authentication Guidance for Federal Agencies（米国）

政府内において電子認証に関する一貫したアプローチの保証を実現することを目的として、2003 年 12 月に策定された。電子認証サービスを提供する政府機関におけるリスクアセスメントの実施を定めることにより、サービス利用者としての国民の判断基準を提供している。

（2） Registration and Authentication －e-Government Strategy Framework Policy and Guidelines －（英国）

英国の電子政府が提供する電子認証サービスにおける保証レベルを定めることを目的として 2002 年 9 月に策定された。匿名でのアクセスに関する取扱いが区分されて扱われている点などに特色がある。

[1] OECD情報システム及びネットワークのセキュリティのためのガイドライン
http://www.meti.go.jp/policy/netsecurity/oecd2002.htm

（3） Australian Government Electronic Authentication Framework（オーストラリア）

オーストラリア政府機関を対象とした電子認証フレームワーク（AGAF）において、リスクレベルに対応した認証手段を実施することを目的として 2005 年に策定された。副題として認証とアクセス管理のための「Better practice guide」との標題がつけられている。

（4） Authentication for e-government Best Practice Framework for Authentication（ニュージーランド）

ニュージーランド政府の電子認証サービスにおけるリスク評価の方針と保証レベルの定義を定めたガイドラインとして、2004 年 4 月に策定された。オンライン認証の実装方法についても解説がある。

（5） Evidence of Identity Framework（ニュージーランド）

ニュージーランドの政府機関において高いリスクを伴う情報処理を行う際の高レベルの機密性確保と個人認証の実現を目的として、2004 年 10 月に策定された。リスクの分析に重点が置かれているほか、政府内の事例毎の詳細な説明が添付されている。

（6） 経済産業省による各種基準・ガイドライン（日本）

電子認証フレームワークに関連して政府が定めた法規としては、「電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）」が存在するが、これ以外に直接的に電子認証サービスを対象とする政府によるガイドライン等のドキュメントは存在しない。情報セキュリティに関連する各種基準、ガイドラインの例としては以下の例が挙げられる。

- 情報セキュリティ管理基準（2004 年 10 月策定）
- 電子政府情報セキュリティ管理基準モデル（2004 年 10 月策定）
- 情報セキュリティ監査基準（2004 年 10 月策定）

4.1.1.3. 民間団体によるガイドライン

民間主導で作成されたガイドラインの例を示す。

（1） Trust Framework（米国Electronic Authentication Partnership）[2]

5.1.1.2(1)の E-Authentication Guidance で定められた内容をもとに、政府と民間の連携、ないし民間同士での連携のスキームの確立を目指すもものである。

（2） 認証局運用ガイドライン（電子商取引実証推進協議会（ECOM））[3]

ECOM により、国際標準化機構（ISO）、IETF 等で検討されている認証もしくは認証局に係わる各種のガイドラインの内容や、ECOM 内で認証局の実験を行ったプロジェクト等からの意見をもとに、1998 年 10 月に策定されたガイドラインである。

本ガイドラインは認証局の運用を対象として、以下の特徴を有する。

- 認証局の機能として、登録局機能、リポジトリ機能等も包含した認証管理サービス全体を対象とする要件を規定するなど、汎用性を意識したものとなっている。
- ガイドラインの内容は ISO の TTP（Trusted Third Party）ガイドライン、金融向けの認証管理、IETF/PKIX の認証ポリシーと認証実施フレームワーク等のドラフトにおいて検討されている要件をもとに、セキュアな認証局の運用のために備えるべきものをを洗い出した上で規定されており、国際整合性に配慮している。
- 認証局の用途等をもとに３段階のレベル付けを行っている。具体的は、以下の 3 種類が想定した上で、それぞれのレベルの認証局の要件をマネジメント、業務運用、設備・システムなどの単位で規定している。
  i) 電子メールに対する認証書のような信頼度の保証が比較的低いレベルの認証書を発行する認証局
  ii) 電子商取引において高額ではないが決済の保証をする信頼度中レベルの認証書を発行する認証局
  iii) 下位の認証局に高い信頼度を持った認証書を発行する認証局

[2] Electronic Authentication Partnership Trust Framework
http://eapartnership.org/docs/Trust_Framework_010605_final.pdf
[3] 電子商取引実証推進協議会, 認証局運用ガイドライン(1.0 版), 1998 年 10 月.

4.1.2. BCP（Best Current Practice）

インターネットで利用される技術の標準化を行う組織である IETF（Internet Engineering Task Force）において策定されるドキュメントの中には、“ Best Current Practice ”と名付けられたカテゴリーに所属する一連の文書がある。これは、インターネット運用における組織や管理に関して現在行われている各種の手続きを文書化したものが中心となっている。「現時点における最良の方法、実践、規範」など直訳的に解釈されるほか、「現状通知」などと訳される場合もある。ドキュメントは主に開発者を対象に書かれているが、ネットワークサービスの提供者を対象としたものもある。

BCP も IETF で扱われる正式文書の総称である RFC（Request For Comments）に属するドキュメントであるが、後の策定プロセスの項で説明するように、RFC のうち“ Standard ”に属するドキュメントがその策定に際して広範なテストと意見の募集を経るのに対し、BCP に属するドキュメントについては、IETF の下部組織である技術専門家グループの IESG（Internet Engineering Steering Group）によるレビューと承認を経るのみで決定される点が異なる。

BCP の定義については、過去には単独の RFC として RFC1818（Best Current Practice）が提供されていたが、現在、RFC1818 は Historic（歴史的）の位置づけとなり、RFC2026（The Internet Standards Process - インターネット標準化手続 - Revision 3）のセクション 5 に規定された内容に基づいて策定されている。RFC2026 も Best Current Practice のカテゴリーに所属する RFC である。

現在 BCP として提供されているドキュメントをカテゴリー別に整理すると、以下のようになる。

（1） ガイドライン、規範的な位置づけのもの

あるプロセスや活動における望ましい規範として IETF が定めるものであり、本調査におけるガイドラインの位置づけの規範となるものである。ここに該当する BCP の例としては以下のようなものがある。

- Recommended Internet Service Provider Security Services and Procedures（RFC 3013, BCP 46）
- IANA Guidelines for IPv4 Multicast Address Assignments（RFC 3171, RFC 51)
- Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")（RFC 3172, RFC 52)
- Guidelines for Evidence Collection and Archiving（RFC 3227, BCP 55）
- Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols（RFC 3470, BCP 70）
- Guidelines for Writing RFC Text on Security Considerations（RFC 3552, BCP 72）

- DNS IPv6 Transport Operational Guidelines（RFC 3901, BCP 91）
- Guidelines for Cryptographic Key Management（RFC 4107, BCP 107）
- Guidelines and Registration Procedures for New URI Schemes（RFC 4395, BCP 115）

（2） 個別事項についてのベストプラクティス

ガイドラインのように一般化するのではなく、個別事項についての対応方法をベストプラクティスとしてまとめたものである。ここに該当する例としては以下のようなものがある。

- Address Allocation for Private Internets（RFC 1918, BCP 5）
- Use of DNS Aliases for Network Services（RFC 2219, BCP 17）
- Classless IN-ADDR.ARPA delegation（RFC 2317, BCP 20）
- Change Process for the Session Initiation Protocol (SIP)（RFC 3427, BCP 67）

（3） 特定のリスクに対する対応のあり方を示すもの

(2)の特殊な例として、特定のリスクへの対処のあり方を示すものがある。ここに該当する BCP の例としては以下のようなものがある。

- Hanging the Default for Directed Broadcasts in Routers（RFC 2644, BCP 34）
- Inappropriate TCP Resets Considered Harmful（RFC 3360, BCP 60）
- Embedding Globally-Routable Internet Addresses Considered Harmful（RFC 4085, BCP 105）

（4） 自らの組織とプロセスに関するもの

BCP の中には、IETF 自らの組織とその活動についての規定を行っているものが存在する。これが BCP に位置づけられるのは、通常の標準文書のようにテストを実施することが適切でなく、かつ内部での承認の必要性を伴うものであることにより、必然的に BCP の扱いで策定せざるを得ないことによる。ここに該当する BCP の例としては以下のようなものがある。

- Guide for Internet Standards Writers（RFC 2360, BCP 22）
- IETF Working Group Guidelines and Procedures（RFC 2418, BCP 25）
- IETF Guidelines for Conduct（RFC 3184, BCP 54）
- Defining the IETF（RFC 3233, BCP 58）
- The IESG and RFC Editor Documents: Procedures（RFC 3932, BCP 92）
- A Model for IETF Process Experiments（RFC 3933, BCP 93）
- Updates to RFC 2418 Regarding the Management of IETF Mailing Lists（RFC

3934, BCP 94）
- A Mission Statement for the IETF（RFC 3935, BCP 95）
- Structure of the IETF Administrative Support Activity (IASA)（RFC 4071, 4371, BCP 101）
- IAB Processes for Management of IETF Liaison Relationships（RFC 4052, BCP 102）
- Procedures for Handling Liaison Statements to and from the IETF（RFC 4053, BCP 103）
- The IETF Administrative Oversight Committee (IAOC) Member Selection Guidelines and Process（RFC 4333, BCP 113）

（5） 知的財産権に関するもの

(4)の特殊な例として、知的財産権に関する扱いを BCP として定めた RFC の例として以下のものがある。

- IETF Rights in Contributions（RFC 3978, BCP 78）
- Intellectual Property Rights in IETF Technology（RFC 3979, BCP 79）

これらを含め、現在 IETF から BCP として公開されているドキュメントの一覧を章末の Appendix 2 に示す。

4.2. ドキュメントの策定プロセス

前項で示した各種のドキュメントについて、その策定プロセスを整理する。

4.2.1. IETF におけるドキュメント策定プロセス

IETFにおける標準的なRFCの策定手順の流れをJPNICが一般向けに公開している資料「What is IETF」[4]ならびに「Introduction to RFC(s)」[5]をもとに図に示す。

プロセス内に位置するドキュメントのステータスとして、以下の種類が定められている。

（1） Internet-draft

Internet-draft は誰でも自由に投稿することができる Working-in-Progress の扱いのドキュメントである。IETF に Internet-draft が投稿されると、FTP サーバおよび Web サーバを通じて 6 か月間公開される。この間に広くインターネット業界に有用な情報を含んでいると判断されると、これを RFC あるいは BCP にするよう IESG に申請が行われる。申請が承認されると、ドキュメントには RFC 番号（あるいは BCP 番号）が割り当てられ、公式に IETF の FTP および Web サーバを通じて恒常的に参照可能なドキュメントとして扱われるようになる。

（2） Standard Track RFC（Proposed Standard、Draft Standard、Standard）

これらはドキュメントが Internet-draft の段階を経て、業界での国際標準とすべく Working Group においてコンセンサスが得られた仕様としてとりまとめられたものである。Proposed、Draft などの種類は、実装や運用のテストの経過段階に応じて定められており、Proposed Standard は複数の組織での独立な実装テストと相互接続性の確認、Draft Standard は実質的かつ広範囲での運用テストがそれぞれ条件となっている。これらの段階を経て Standard の状態になると、RFC の番号とは別に STD 番号が割り振られる。RFC として管理されているドキュメントの中で、STD 番号を有するものは非常に少数であり、Draft Standard の段階の RFC であっても、実質的に国際標準として利用されているものも少なくない。

---

[4] 江崎 浩: What is IETFより第４章「IETFにおける標準化プロセス」
http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section4.html
[5] 宇夫 陽次朗: Introduction to RFC(s)
http://rfc-jp.nic.ad.jp/introduction/

（3） BCP（Best Current Practice）

前述の通り、BCP は IESG による承認を得たドキュメントであるが、標準として扱うに際して実装や運用のテストを経ない点で(2)と異なる。しかしながら標準として利用することを意図していることでは(2)と共通であり、BCP に位置づけられるドキュメントはすでに広く利用されている手続きや規範を扱ったものが多い。STD 番号と同様、BCP 番号が RFC の番号と別に割り振られる。

（4） Experimental RFC

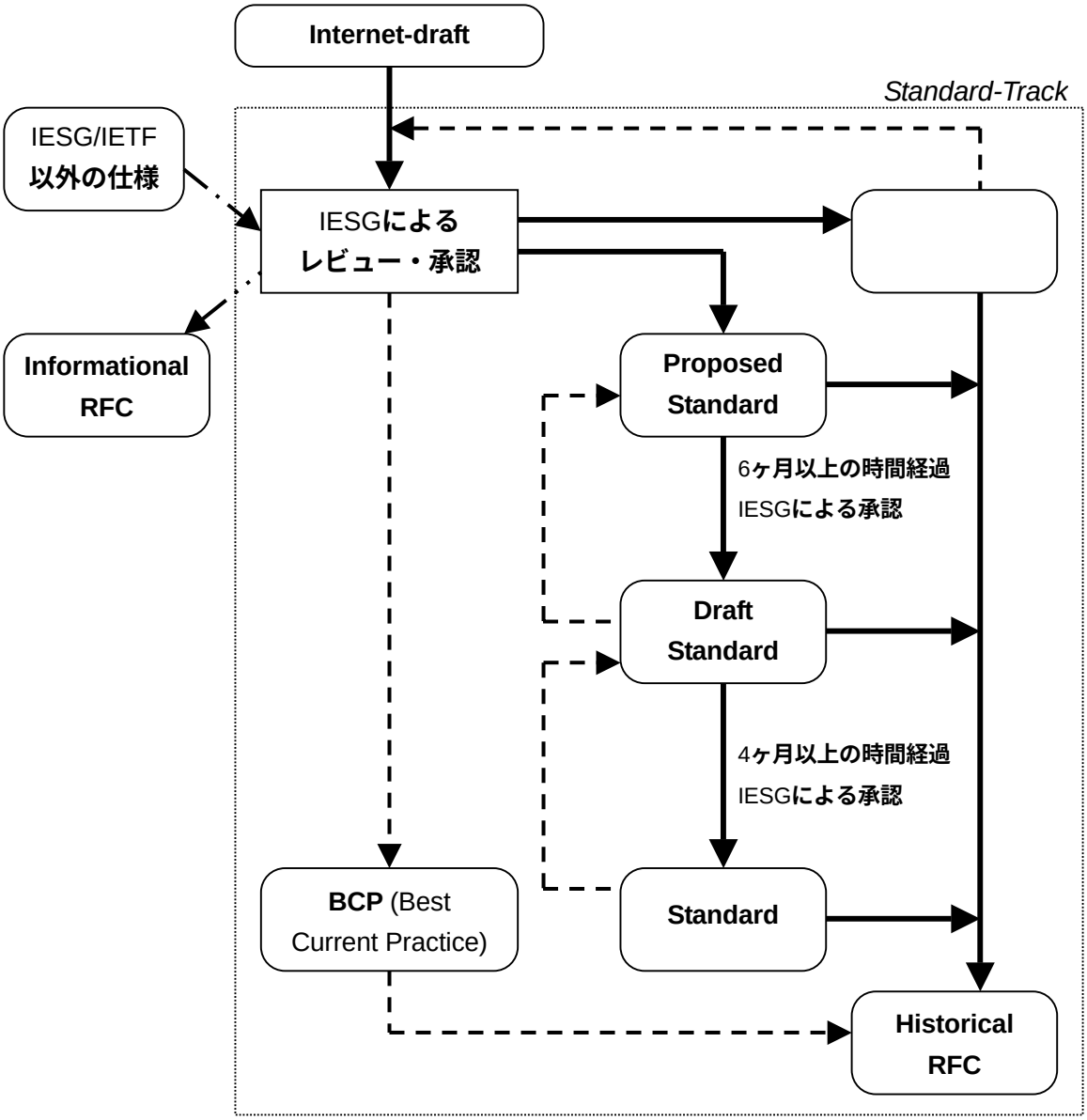
Experimental に分類されるドキュメントには、標準化を目的とせず、研究等における技術仕様を規定したものも含まれる。これは、純粋な研究目的のほか、本来企業独自の仕様であるものをデファクト化することを目的として提供される場合もある。

（5） Informational RFC

Informational に分類されるドキュメントには、標準化は想定していないが、業界にとって有用と判断されるものが含まれる。すなわち、仮に特定の企業などに固有の仕様であっても、それが、標準仕様の議論や策定に有効であると認められる場合には RFC とすることができる。(4)と同様、企業が標準化を待たずに製品展開を行うような場合に、Informational RFC としてその仕様を広く公開することにより、デファクト・スタンダードを確立するための手段として利用されることもある。

（6） Histrorical RFC

かつては標準として利用されていたが、技術の進展や環境の変化などの影響により同一の分野での別の RFC が承認されたことを通じて、現役のドキュメントとして利用されなくなったものは Historical（歴史的）として位置づけられる。



（江崎 浩「What is IETF」[6]挿入図より作成）

図 4−1 IETF における RFC の策定プロセス

[6] 江崎 浩「What is IETF」第４章「IETFにおける標準化プロセス」
http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section4.html

4.2.2. その他の策定プロセス

IETF における策定プロセスの説明を補足する視点から、IP レジストリなど他機関における類似ドキュメントの策定プロセスについて示す。

4.2.2.1. JPNIC における策定プロセス

参考情報として、JPNIC で用いている策定プロセスの例として、IP アドレスポリシーに関する策定プロセスを示す。

ポリシー提案は、以下のステップに基づく議論をもとに、その採用ないし実装が検討される[7]。

（1） ポリシー提案の提出

ポリシー提案が、提案者から JPNIC ポリシーワーキンググループ（以下ではポリシーWG という）に提出される。

（2） APNIC に対する提案の必要性の確認

提出された提案について、APNIC に対しても提案が必要かどうかの確認をポリシーWG が JPNIC と共同で行い、その結果を提案者に連絡する。

（3） ポリシー提案の公開

ポリシーWG は提出されたポリシー提案を、オンサイトフォーラム（会議場に参加者が集合して行う形式のもので、この場合は JPNIC オープンポリシーミーティングが該当する）の開催にあたり、事前に Web もしくはオンラインフォーラム上、あるいはその双方で公開する。

（4） ポリシー提案の議論

オンサイトフォーラムの場で提出したポリシー提案に関する説明を提案者が行い、参加者からの質問に対応する。

[7] JPNICにおけるIPアドレスポリシー策定プロセス
http://www.nic.ad.jp/doc/jpnic-00962.html

（5） コンセンサスの醸成

提出されたポリシー提案に対し、オンサイトフォーラムの参加者の過半数の賛同が得られた場合に、そのポリシー提案はコンセンサスを得たものとされる。このコンセンサスの確認はポリシーWG のチェアによって行われる。このコンセンサスは「1 次コンセンサス」と呼ばれる。

（6） 最終コメント期間

1 次コンセンサスを得たポリシー提案は、オンラインフォーラム上で公開され、最低 2 週間の最終コメント期間を経るものとする。この最終コメント期間は、ポリシーWG のチェアの裁量で延長することができる。

（7） 最終的なコンセンサスの確認

前項の最終コメント期間において本質的な反対がなければ、当該ポリシー提案は最終的なコンセンサスを得たものとされる。この判断は、ポリシーWG のチェアによって行われる。

（8） コンセンサス内容の確認と実装勧告

最終的なコンセンサスを得たポリシー提案について、ポリシーWG によってその内容の妥当性の再評価が行われ、コンセンサスの内容が整理される。その結果をもって、ポリシーWG は JPNIC に対し、当該ポリシー提案の実装勧告を行う。

（9） JPNIC による実装検討

JPNIC では、ポリシーWG からの実装勧告を受け、実務的な面で実装が可能か、採算上問題ないか、APNIC のポリシーに反しないかなどの確認と検討を行う。

（10） JPNIC による承認プロセス

実装勧告に対して JPNIC が実装可否の判断を行い、この結果は JPNIC の理事会の審議を経て最終的に決定される。

（11） JPNIC による結果報告

JPNIC による実装検討の結果が、オープンポリシーフォーラムへ報告される。実装が決定したポリシー提案は、実施日などの調整を行ったうえで施行の運びとなる。

一方、提案者から提出されたポリシー提案が棄却となる条件としては、以下の場合が挙げられている。

- オンサイトフォーラムの場で、参加者の過半数の賛同を得られなかった場合
- オンサイトフォーラムでは参加者の過半数の賛同を得たが、オンラインフォーラムでの最終コメント期間中、最終的なコンセンサスの確認が取れないとポリシーWG のチェアが判断した場合
- 最終的なコンセンサスが確認されたが、その内容が妥当でないとポリシーWG によって判断された場合
- ポリシーWG からの実装勧告に対し、JPNIC が実務的な面、採算上の問題、APNIC とのポリシーとの整合性等の観点から実装することができないと判断した場合
- ポリシー提案の実装が JPNIC だけで決定できず、APNIC に提案する必要があり、その提案が APNIC オープンポリシーミーティングにおいて賛同を得られなかった場合

提出されたポリシー提案が棄却された場合は、ポリシーWG もしくは JPNIC が、オンサイトフォーラムまたはオンラインフォーラム、もしくはその両方で、棄却となった理由について報告を行う。

4.3. 電子認証に関わる既存ガイドライン等の分析

IETF、IP レジストリ、日本政府、諸外国政府及び外郭団体のガイドラインを挙げ、その状況と特徴をまとめる。

4.4. 調査対象の概要

本調査では、以下の観点から各ガイドラインの分析を行う。

本調査の結果は、章末に記載した表 4-1「海外における電子認証に関わる既存ガイドラインの例」に掲載する。

（1） 目的

ガイドライン作成の目的を識別する。

（2） 利用者

ガイドラインを利用するターゲットについて、文書中に記述されている場合はそれを抽出し、そうでない場合は内容から想定を行う。

（3） 利用方法の想定

ガイドラインをどのような場合に利用することを想定しているかについて、検討を行う。

（4） 運用方法

ガイドラインの運用（改定等のメンテナンス、普及・広報活動等）について、関係する情報を整理する。

（5） 特徴

他のガイドラインと比較した特徴的な事項の抽出を行う。

4.5. E-Authentication Guidance for Federal Agencies（米国）

本文書の要約として、以下の事項が示されている。

> This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their e-government authentication needs. Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.

＜引用部の訳文＞

本ガイダンスは、政府機関に対して認証プロセスが適切な保証レベルを提供することを確実にするために、新規および既存の電子的なトランザクションの見直しを要求するものである。

本ガイダンスでは、認証が要求される電子的なトランザクションの為の、本人性保証の 4 つのレベルが規定され、説明されている。また、保証レベルは連邦政府関係機関を代表してクレデンシャル・サービス・プロバイダー（Credential Service Providers: CSPs）を評価するための原則を提供している。本ドキュメントは、政府機関が電子政府認証ニーズを決定することの手助けともなる。政府機関の業務プロセス所有者は、本人保証レベル及びそれらを提供する戦略に対して主要な責務を担う。この責務は、電子認証システムにまで及ぶこととなる。

> Agencies should determine assurance levels using the following steps, described in Section 2.3:
>
> 1. Conduct a risk assessment of the e-government system.
> 2. Map identified risks to the applicable assurance level.
> 3. Select technology based on e-authentication technical guidance.
> 4. Validate that the implemented system has achieved the required assurance level.

5. Periodically reassess the system to determine technology refresh requirements.

＜引用部の訳文＞

政府機関は、本ガイダンスの 2.3 節で説明される、次の手順に従って保証レベルを決定すべきである。

1. 電子政府システムのリスクアセスメントを実施する。
2. 判明しているリスクを該当する保証レベルに位置づける。
3. 電子認証の技術ガイダンスに基づいて技術を選択する。
4. 実装されたシステムが、要求された保証レベルに達しているかを検証する。
5. 定期的にシステムを見直して 技術更新要件を決定する。

4.5.1. 保証レベルの説明

本文書において、保証レベルの説明として以下の事項が示されている。

This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as

1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

The four assurance levels are:

Level 1: Little or no confidence in the asserted identity's validity.

Level 2: Some confidence in the asserted identity's validity.

Level 3: High confidence in the asserted identity's validity.

Level 4: Very high confidence in the asserted identity's validity.

＜引用部の訳文＞

本ガイダンスでは、電子政府のトランザクションのための 4 つの identity 認証保証レベルについて説明をする。利用者が提示した自らを参照する識別子（本文書ではクレデンシャル）についての政府機関の確度で各レベルは述べられている。本文書において、保証は次のように定義される。

1) クレデンシャルが発行された個人の身元をするために立証するために使用される審査プロセスにおける信頼度
2) クレデンシャルを使用する個人が、クレデンシャルを発行された個人であることの信頼度

4 つの保証レベルとは、

レベル１：asserted identity's validity の信頼はほとんどない

レベル２：asserted identity's validity の信頼は若干ある

レベル３：asserted identity's validity の信頼は高い

レベル４：asserted identity's validity の信頼は非常に高い

である。

4.5.2. リスク、潜在的影響、および保証レベル

本文書において、リスク・潜在的影響・保証レベルの説明として以下の事項が示されている

> While, this guidance addresses only those risks associated with authentication errors, NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems,” recommends a general methodology for managing risk in Federal information systems. In addition, other means of risk management, (e.g., network access restrictions, intrusion detection, and event monitoring) may help reduce the need for higher levels of authentication assurance.

＜引用部の訳文＞

本ガイダンスでは、認証エラーに関連するそれらのリスクのみを扱っているが、NIST Special Publication 800-30 の「情報技術システムのためのリスク管理ガイド（Risk Management Guide for Information Technology Systems）」では、連邦情報システムのリスク管理のための一般方法論が推奨されている。そして、リスク管理の他の手段（例えば、ネットワークアクセス制限、侵入検知、モニタリングなど）を用いることにより、さらに高い認証保証レベルの必要性を軽減させることが可能である。

4.5.2.1. 潜在的影響カテゴリー

本文書において、潜在的リスクの説明として以下の事項が示されている。

> To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:
>
> 1) potential harm or impact, and
>
> 2) the likelihood of such harm or impact.

＜引用部の訳文＞

利用者の asserted identity における適切な保証レベルを決定するために、政府機関は潜在的リスクを評価し、その影響が最小に抑えられるための対策を特定しなければならない。潜在的により悪い結果を招く認証エラーは、より高い保証レベルを必要とします。業務プロセス、政策、および技術は、リスク軽減に役立つ可能性がある。認証エラーに起因するリスクは、次の 2 つの要因による作用である。

a) 潜在的な損害または影響

b) 潜在的な損害または影響の見込み

（1） 損害と影響のカテゴリー

損害と影響のカテゴリーには次が含まれる。

- 不便、苦痛、または地位や評判に対する損害
- 経済的損失または政府機関の負担
- 政府機関の計画や公益への損害
- 機密情報の不正発表
- 個人の安全
- 民事または刑事上の違反行為

連邦情報処理規格(FIPS) 199、「連邦政府の情報と情報システムのセキュリティ分類の規格（Standards for Security Categorization of Federal Information and Information Systems)」に記述されている潜在的影響値を使用して、電子的なトランザクションのために要求される保証レベルは、上記のそれぞれのカテゴリーの潜在的影響の評価によって決定される。3 つの潜在的影響の評価とは次の通りである。

・ 低影響

・ 中影響

・ 高影響

（2） 認証エラーの潜在的影響の決定

上記で述べた各カテゴリーにおける潜在的影響の定義付けを行う。

表 4-1　各カテゴリーにおける潜在的影響の定義付け

カテゴリー	低影響	中影響	高影響
不便、苦痛、または地位や評判に対する損害の潜在的影響	最悪の場合、苦痛や当事者の当惑が限定的、短期間の不便さである。	最悪の場合、苦痛や当事者の地位や評判に対する損害が、深刻で短期間または（範囲が）限定的で長期間の不便さである。	苦痛や当事者の地位や評判に対する損害が、重度のまたは深刻な長期間の不便さである（通常は、著しく深刻な影響を伴った状況または多くの人に影響を及ぼす)。
経済的損失の潜在的影響	最悪の場合、当事者に対する重要ではない場合や取るに足りない回復不能な経済的損失であるか、または、重要ではない場合や取るに足りない政府機関の負担である。	最悪の場合、当事者に対する深刻な回復不能な経済的損失であるか、深刻な政府機関の負担である。	当事者に対する重度のまたは壊滅的な回復不能な経済的損失であるか、重度のあるいは壊滅的な政府機関の負担である。

カテゴリー	低影響	中影響	高影響
政府機関の計画や公益への損害の潜在的影響	最悪の場合、組織の運営や資産、あるいは公益への限定的悪影響。限定的悪影響の例： 1) 組織において、かなり（noticeably）限定された効力で主要な機能を遂行できる程度と期間に対する、任務実行能力の低下。 2) 組織の資産や公益への軽度の損害	最悪の場合、組織の運営や資産、あるいは公益への深刻な悪影響。深刻な悪影響の例： 1) 組織において、かなり（sig-nificantly）限定された効力で主要な機能を遂行できる程度と期間に対する、任務実行能力の著しい低下。 2) 組織の資産や公益への多大な損害	組織の運営や資産、あるいは公益への深刻な又は破滅的な悪影響。深刻な又は破滅的な悪影響の例： 1) 組織において、かなり（severe）限定された効力で 1 つ又は複数の主要な機能を遂行できる程度と期間に対する、任務実行能力の重度の低下。 2) 組織の資産や公益への大規模な損害
機密情報の不正発表の潜在的影響	最悪の場合、FIPS PUB 199 に定義されているような機密を、低影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表	最悪の場合、FIPS PUB 199 に定義されているような機密を、中影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表	FIPS PUB 199 に定義されているような機密を、高影響によって、認可されていない当事者へ、個人または米国政府の機微、商業的に機密な情報を限定的に公表
個人の安全の潜在的影響	最悪の場合、医療手当を必要としない軽傷	最悪の場合、医療手当を必要とする、軽傷の中程度のリスクまたは負傷の限定的リスク	重傷または死のリスク

カテゴリー	低影響	中影響	高影響
民事または刑事上の違反行為の潜在的影響	最悪の場合、通常は執行対象とならないような種類の民事または刑事上の違反行為	最悪の場合、執行対象となり得るような種類の民事または刑事上の違反行為	執行プログラムにとって特に重要な民事または刑事上の違反行為

4.5.2.2. 保証レベルの決定

本文書において、保証レベルの決定についての説明として以下の事項が示されている

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

＜引用部の訳文＞

下記の表 4-2 においてリスクアセスメントからの影響プロファイルとそれぞれの保証レベルに関連する影響プロフィールを比較する。要求される保証レベルを決定するために、リスクアセスメントで分析された各カテゴリーに対して、影響プロファイルが潜在的影響と一致または超える最低限のレベルを見つける。

表 4-2　各保証レベルの最大潜在的影響

	保証レベル影響プロファイル			
認証エラーの潜在的影響カテゴリー	1	2	3	4
不便、苦痛、または地位や評判に対する損害	低	中	中	高
経済的損失または政府機関の負担	低	中	中	高
政府機関の計画や公益への損害	N/A	低	中	高
機密情報の不正発表	N/A	低	中	高
個人の安全	N/A	N/A	低	中／高
民事または刑事上の違反行為	N/A	低	中	高

4.5.3. 保証レベルの決定とリスクアセスメントを用いた認証ソリューションの選択

本文書において、リスクアセスメントを利用した保証レベルの決定法と認証ソリューションの選択について説明が述べられている。政府機関は下記で説明する手順に従って、保証レベルを決定する。

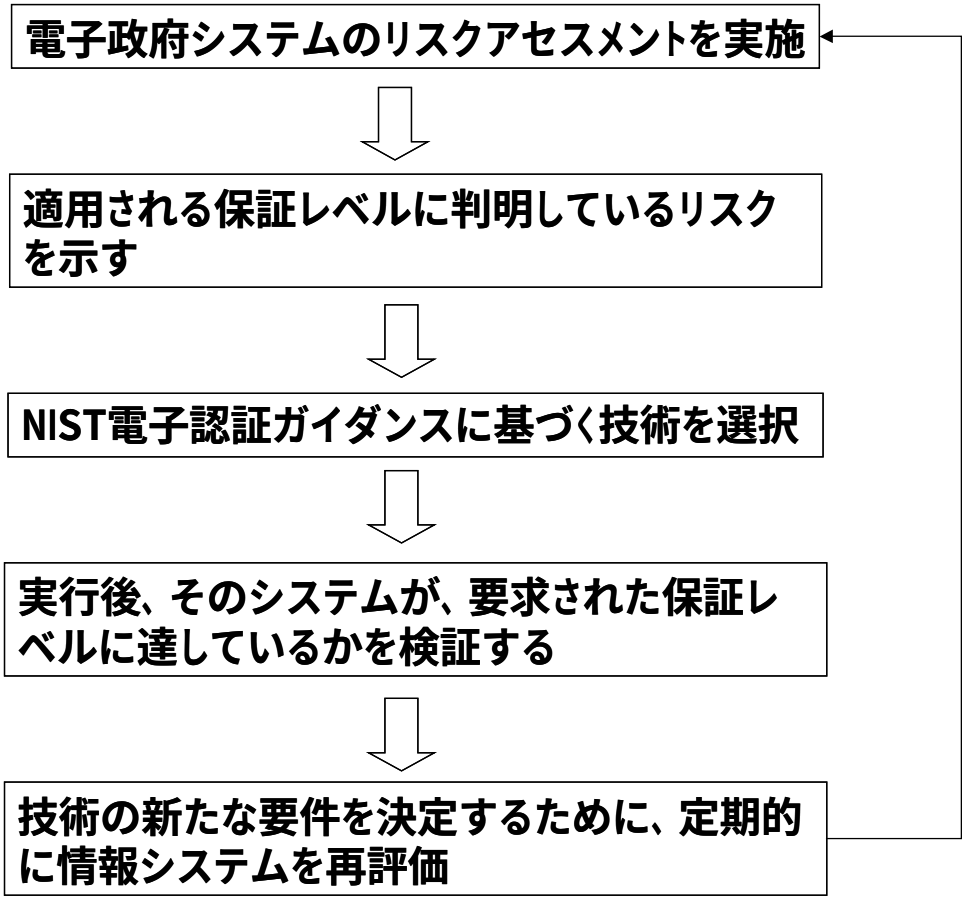


図 4−2　保証レベル決定の手順

手順１：電子政府システムのリスクアセスメントを実施する

Conduct a risk assessment of the e-government system.

Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of OMB's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

Risk analysis is to some extent a subjective process, in which agencies must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. Agencies should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis. Once risks have been identified, there may also be ways to adjust the business process to mitigate particular risks by reducing the likelihood that they will occur (see Step 4).

＜引用部の訳文＞

政府機関がリスクアセスメントを実施するためのガイダンスは、OMB の GPEA ガイダンスのセクション５の A-130 および既存の NIST ガイダンスから入手可能である。リスクアセスメントは、電子政府システムでの identity 認証エラー発生時における、潜在的損害の相対的重大性と（当事者に対する）広範囲の影響の発生見込みを測るものである。

リスク分析はある程度主観的であるので、（この他の原因もあるが）技術的な失敗、維持の悪い第三者、人的ミスなどから生じる損害について政府機関は考慮しなければならない。どんな潜在的損害がビジネスプロセスに関連するかを決定しようとする際に、政府機関は広範囲に可能なシナリオを考慮すべきである。この分析を実施する際には、包括的でないよりも過剰に包括的である方が好ましい。一度リスクが確認されると、そのリスクが発生する可能性を低減させることにより、特定の危険を緩和するようにビジネスプロセスを調整する方法（手順４参照）があるかもしれない。

手順２：判明しているリスクを要求されている保証レベルに対応付ける

Map identified risks to the required assurance level.

The risk assessment should be summarized in terms of the potential impact categories in Section 2.2.

To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

＜引用部の訳文＞

リスクアセスメントは、セクション 2.2 での潜在的影響カテゴリーの観点から要約されるべきである。

所要の保証レベルを決定するためには、認証技術に関係なく、政府機関は最初にトランザクションプロセスにおける固有のリスクについて確認すべきである。そして、政府機関は潜在的影響カテゴリーの結果を認証レベルに結び付け、確認される全ての潜在的影響をカバーする最低の認証レベルを選択すべきである。従って、潜在的影響カテゴリーにおいて、５つがレベル１相当で、１つがレベル２相当である場合には、トランザクションはレベル２の認証を要求する。例えば、医療処理においてユーザの電子 identity/credentials の誤用が大怪我か死の危険を招く場合には、たとえ他の項目の結果が最小限であるとしても、レベル４より下で識別されるリスクプロファイルについても対応付ける必要がある。

手順３：NIST 電子認証ガイダンスに基づく技術を選択する

Select technology based on the NIST e-authentication technical guidance.

After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

＜引用部の訳文＞

保証レベルを決定した後、政府機関は適切な技術的要件を識別し実装するために NIST 電子認証技術ガイダンスを参照すべきである。

手順４：実行後、そのシステムが、要求された保証レベルに達しているかを検証する

After implementation, validate that the information system has operationally achieved the required assurance level.

Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the systems's authentication requirements as part of required security procedures (e.g., certification and accreditation).

＜引用部の訳文＞

実行によっては特定のリスクを生み出したり悪化させたりするので、ユーザから政府機関へのプロセスにおいて要求された保証レベルをシステムが満たしていることを確認する最終確認を行うこと。認証プロセスが（例えば、証明と認可など）要求されたセキュリティ・プロシジャーの一部分としてシステムの認証要件を満たしていることを、政府機関は確認すべきである。

手順５：技術の新たな要件を決定するために、定期的に情報システムを再評価

Periodically reassess the information system to determine technology refresh requirements.

The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

＜引用部の訳文＞

技術の変化または政府機関におけるビジネスプロセスの変化の結果、identity 認証要件が、有効であり続けるのを保証するために、政府機関は定期的に情報システムを再評価しなければならない。年に一度の情報セキュリティ評価要件を設けることは、再評価のための格好の機会である。追加的なリスク緩和処置を用いて、政府機関は identity 信用証明書の保証レベルを調整することができる。identity 信用証明書の要件保証レベルを緩和することは、有効な顧客プールの規模を増大させる可能性がある。しかし政府機関は、（レベルの緩和が）システムによる保証レベルの選択に悪影響を及ぼさないようにする必要がある。

4.5.4. 保証レベルとリスクプロファイル

表 4-3　保証レベルに応じたリスクプロファイル

保証レベル	説明	例
レベル 1	asserted identity において信頼はほとんど又は全くない。例えば、レベル 1 信用証明書は、人々が今後の参考のためにウェブページにブックマークを付けることを許可する。	1. 電子トランザクションにおける個人によるフォームの提出：駐車場の年間利用許可証を申請するときなど。 2. ユーザがカスタマイズすることができる教育省のウェブページ“My.ED.gov”に、ユーザが独自で登録した ID やパスワードを提示して利用するとき。 3. 名前と場所以外の身元情報を要求されないホワイトハウスのオンラインディスカッションに参加するとき。
レベル 2	総じて asserted identity が正確であるという信頼はある。政府機関が初めに identity 特定を必要とする国民に対する広範囲の業務に、レベル 2 信用証明書が使われる。	1. 政府オンライン学習センター（Gov Online Learning Center）へ会員登録するとき。このトランザクションに関する唯一のリスクは、第三者が成績情報にアクセスするときである。この損害が小さいと判断したとき、政府機関はこの保証レベルの認証と決定する。 2. 社会保障ウェブサイトを通じて、受給者は住所変更を行う。支払額や口座の状態、変更履歴公式通知を受益者の記録されている住所に送るので、機密情報の不正発表の中程度リスクを伴う。 3. 銀行口座やプログラム資格、支払情報を政府機関のプログラムクライアントが更新する。紛失や遅延は重大な影響を与えるが、長期

保証レベル	説明	例
		間ではない。個人の経済的損失の潜在的影響は低いが、総計では中程度の影響である。 4. 潜在的に機密な個人クライアント情報へ政府機関職員がアクセスする。制限の少ない状況では、政府機関職員が行う個人的な機密情報へのアクセスは、機密情報の不正発表の中程度の潜在的影響であるが、システムのセキュリティ対策により低影響になる。
レベル 3	レベル 3 は、asserted identity の正確性において高い信頼度を必要とするトランザクションに適している。追加的な identity assertion の規則を適用せず、ウェブサービスへアクセスするために、人々はレベル 3 信用証明書を使用できる。	1. 特許弁理士が、米国特許商標局へ電子的に機密特許情報を提出する。 2. 大きな政府調達のために、供給者が共通役務庁（General Services Administration）の契約担当官と取引を維持する。経済的損失の潜在的影響はかなり（significant）あるが、重度（severe）や破壊的ではないので、レベル 4 は適切でない。 3. インシデントの報告や運用情報の共有、応答活動の調整のために、最初に応答する人は災害管理報告ウェブサイトへアクセスする。 4. 政府機関の職員または契約者が、潜在的に機密な個人クライアント情報へリモートアクセスで接続する場合（連邦政府のアクセス制御されたビルで働いているものとする）。このとき、入手可能な機密個人情報の不正発表は中程度である。

保証レベル	説明	例
レベル 4	レベル 4 は、asserted identity の正確性において非常に高い信頼度を必要とするトランザクションに適している。identity assertion 以上の規則を要求せずに assert identity によって厳しく制限されたウェブの情報資源へアクセスするために、利用者はレベル 4 認証証明書を提示してもよい。	1. 法執行機関の当局者が、捜査当局にある犯罪歴を含むデータベースへアクセスする。不正アクセスは、プライバシー問題を引き起こし、また捜査を危うくする。 2. 復員軍人省の薬剤師が、規制医薬品を調剤する。その薬剤師は、有資格医師が処方する全ての保証を必要とする。薬剤師は、処方を確認して、定められた量で正しい薬を調剤することに関するあらゆる失敗に対して、刑法上責任がある。 3. 政府機関の調査官が、潜在的に機密な個人クライアント情報へリモートアクセスで接続する場合（ノート PC を用いて外部から接続する）。このとき、不正認証による機密個人情報の不正な流出は中程度であるが、ノート PC の脆弱性と安全でないインターネットアクセスにより、総合的なリスクを引き起こす。

4.5.5. リスクの範囲と要素

リスクの範囲と要素に関して、本ガイダンスに以下の事項が示されている。

When determining assurance levels, one element of the necessary risk assessment is the risk of denial (or repudiation) of electronically transmitted information. Section 9c of OMB's GPEA guidance states agencies should plan how to minimize this risk by ensuring user approval of such information. Section 8c of the OMB Procedures and Guidance on Implementing GPEA includes guidance on minimizing the likelihood of repudiation.

OMB's GPEA guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal Agencies on Implementing Electronic Processes" discusses the legal issues surrounding electronic government. Legal and enforcement needs may affect the design of an e-authentication system and may also entail generation and maintenance of certain system management documentation.

＜引用部の訳文＞

保証レベルを決定する際、必要なリスクアセスメントの 1 つに電子的に送信された情報の拒否（または否認）のリスクがある。OMB の GPEA ガイダンスのセクション 9c では、そのような情報のユーザ承認を確実にすることにより、このリスクを最小にする方法を、政府機関は計画すべきであると記載されている。OMB の GPEA 実行に関する手順とガイダンスのセクション 8 には、否認の可能性を最小限にすることのガイダンスを含まれている。

OMB の GPEA ガイダンスでは、identity 認証において、適切に実行された技術は手書きの署名よりも高い信頼度を提供すると記載されている。逆に、電子的なトランザクションは、民事または刑事上の違反行為に関するリスクと損害（そして補償を困難にすること）を増加させる可能性がある。司法省の「電子プロセスの実行にあたっての連邦政府機関のためのガイド」では、電子政府にまつわる法的な問題について論じられている。法律および施行のニーズは、電子認証システムの設計に影響を及ぼす可能性がある。また、あるシステム管理ドキュメントの作成とメンテナンスを必要とする可能性がある。

4.5.6. クレデンシャル・サービス・プロバイダーの信頼評価

クレデンシャル・サービス・プロバイダーの信頼評価に関して、本ガイダンスに以下の事項が示されている。

> Since identity credentials are used to represent one's identity in electronic transactions, it is important to assess the level of confidence in the credential. Credential Service Providers (CSPs) are governmental and non-governmental organizations that issue and sometimes maintain electronic credentials. These organizations must have completed a formal assessment against the assurance levels described in this guidance.
>
> The CSP's issuance and maintenance policy influences its e-authentication process trustworthiness. The E-Authentication Initiative will therefore develop an assessment process for the government to determine the maximum assurance level merited by the CSP. For example, if a CSP follows all process/technology requirements for assurance Level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring assurance Levels 1, 2, or 3.

＜引用部の訳文＞

identity 信用証明書は、電子的なトランザクションにおいて人の識別を行うために使用されるので、信用証明書の信頼レベルの評価することは重要である。クレデンシャル・サービス・プロバイダー（CSP）とは、電子信用証明書を発行し、場合によっては維持を行う政府や非政府機関である。これらの組織は、本ドキュメントに記述してある保証レベルに対して公式な評価を終えていなければならない。

CSP の（電子信用証明書を）発行および維持管理方針は、電子認証プロセスの信頼性に影響を与える。それゆえ、政府機関が CSP によって得られた最大の保証レベルを決定するための評価プロセスを、E-authentication initiative は明らかにする。例えば、もし CSP が保証レベル 3 に要求される全てのプロセスと技術要件に従っているならば、利用者が、保証レベルが 1, 2, 3 を要求するトランザクションにおいて自分自身を認証するために CSP によって付与された信用証明書を利用しても良い。

4.5.7. 電子認証プロセス

電子認証プロセスに関して、本ガイダンスに以下の事項が示されている。

> Each step of the authentication process influences the assurance level chosen. From identity proofing, to issuing credentials, to using the credential in a well-managed secure application, to record keeping and auditing—the step providing the lowest assurance level may compromise the others. Each step in the process should be as strong and robust as the others. Agencies will achieve the highest level of identity assurance through strong identity proofing, a strong credential, and robust management (including a strong archive and audit process). However, the best authentication systems result from well-engineered and tested user and agency software applications. A process currently being developed for enabling authentication across Federal agencies will be published for implementation when complete.

＜引用部の訳文＞

認証プロセスの各ステップは、選択された保証レベルに影響を与える。identity proofing からクレデンシャル発行、適切に管理されたセキュリティ・アプリケーションにおけるクレデンシャルの使用、記録保存および会計監査まで、最も保証レベルの低い手順は、他の手順も危うくする可能性がある。プロセスの各手順は、他の手順と同様に強く頑丈であるべきである。強固な identity proofing、強固なクレデンシャル、（強固なファイル保管庫や監査プロセスを含む）堅固な管理を通じて、政府機関は最高レベルの identity 保証を成し遂げるだろう。しかしながら、最良の認証システムは、優れた技術と、ユーザと政府機関のソフトウェア・アプリケーションのテストによって支えられる。連邦政府機関で横断的に認証を可能とするための現在の開発されているプロセスは、完成次第、実施のために発表される。

4.5.8. 匿名信用証明書の使用

匿名信用証明書の使用に関して、本ガイダンスに以下の事項が示されている。

> Unlike identity authentication, anonymous credentials may be appropriate to use to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Government against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:
>
> - The user is a member of a group; and/or
> - The user is the same person who supplied or created information in the first place; and/or
> - A user is entitled to use a particular pseudonym.
>
> These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and identity credentials. As general matter, anonymous credentials are appropriate for Levels 1 and 2 only.

＜引用部の訳文＞

identity 認証とは異なり、認証が既知の個人識別と関係している必要はないとき、匿名信用証明書は属性を評価するために使用するのが適切だろう。プライバシーを守るために、利用者のプライバシーの権利と誰が政府と通信しているかについて知ることの、必要性のバランスを取るのは重要である。これには、個人がそれが使われると確信した方法だけで情報を使うことを含む。場合によっては匿名性を保つことは、望ましいことがある。その場合、以下のことを認証すれば十分である。

- 利用者はグループのメンバーである。
- 利用者は初めに情報を提供したか作成した人と同一である。
- 利用者は特定の匿名を使用する資格がある。

これらの匿名信用証明書は、アプリケーションを制限し、ケースバイケースで使用される。人によっては、匿名および identity 信用証明書を持っているだろう。一般的

な問題として、匿名信用証明書はレベル 1 か 2 においてのみ相応しい。

4.5.9. 情報共有とプライバシー法

情報共有とプライバシー法に関して、本ガイダンスに以下の事項が示されている。

> When developing authentication processes, agencies must satisfy the requirements for managing security in the collection and storage of information associated with validating user identities. The E-Government Act of 2002, section 208 requires agencies to conduct privacy impact assessments for electronic information systems and collections. This includes performing an assessment when authentication technology is added to an electronic information system accessed by members of the public. For additional information on privacy impact assessments, consult OMB guidance.

＜引用部の訳文＞

認証プロセスを構築するとき、政府機関はユーザアイデンティティの検証に関する情報の収集と保管において、セキュリティを管理するための要件を満たさなければならない。2002 年の電子政府法令においてセクション 208 では、政府機関に電子情報システムと収集のためのプライバシー影響評価を実施することを要求している。これには認証技術が国民によってアクセスされる電子情報システムに追加されるとき、プライバシー影響評価を行うことが含まれている。プライバシー影響評価に関する追加情報については、OMB ガイダンスを参照のこと。

4.5.10. コスト／便益における考慮

コスト／便益における考慮に関して、本ガイダンスに以下の事項が示されている。

> Like any capital purchase, implementing e-authentication requires consideration of the benefit and costs, and thus a cost-benefit analysis is required by the Capital Programming Guide. It is also important to match the required level of assurance against the cost and burden of the business, policy, and technical requirements of the chosen solution.

＜引用部の訳文＞

投資購入と同じように、電子認証を実施するには利益とコストの考慮が必要である。そのため費用便益分析は Capital Programming Guide において必要とされている。更に、選択されたソリューションにおいて、コストやビジネスの負荷、政策および技術的要件に対して必要な保証レベルに合わせることも重要である。

4.6. Registration and Authentication －e-Government Strategy Framework Policy and Guidelines －（英国）

本文書は、電子政府のサービスへのアクセスを求める市民や組織の登録と認証に関するフレームワークのポリシーとガイドラインを示すものである。

4.6.1. 目的

本文書の目的として、以下の事項が示されている。

> This document is intended to set out a number of trust levels for registration and authentication in e-Government transactions.
>
> Current guidance on the use of registration and authentication services in the context of e-Government services is set out in the companion security architecture document.

＜引用部の訳文＞

本書は、電子政府の transaction における登録と認証についての保証レベルを定めることを目的としたである。電子政府サービスに関する登録と認証サービスの利用に関する現行のガイダンスについては、セキュリティアーキテクチャの手引きにおいて示すものとされ、本文書の対象外となっている。

4.6.2. 利用者

本文書の利用者として、以下の事項が示されている。

> This document is aimed at those procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.
>
> In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.
>
> It is also relevant to security authorities that may use this document to assess the suitability of offered solutions and accredit them for operational use.

＜引用部の訳文＞

本ドキュメントは電子政府サービスの入手や提供をするものを対象としている。それには、中央政府省庁、外郭公共団体、地方自治体や、電子政府サービスの提供を担当するその他の地方政府機関等、電子政府サービスの入手や提供をするものも含まれている。また、公的な資産と情報を適切に審査・管理するための責任ある取締機関も含まれる。

そのうえ、政府に代わってサービスを提供・運用を望むサービスプロバイダーや、電子政府を維持させるための機器を提供することを望むものも含まれる。

更に、本ドキュメントは、ソリューションの適合性を評価し、そうしたソリューションの実用を認可するためのセキュリティ機関にも関係がある。

4.6.3. 利用方法の想定

本文書の利用方法の想定として、以下の事項が示されている。

It applies in circumstances where government needs to have trust in the identity (real-world or otherwise) and authority of those it is dealing with to ensure that there is no breach of privacy or confidentiality, theft/misuse of data, or other harm. The framework includes those cases where anonymous or pseudonymous access is acceptable.

Business sponsors must also consider the role of registration, authentication, access control and user access management in the context of government users. The exact requirements may differ from those that relate to clients, since other aspects of security (*eg* physical and procedural) may be applicable.

The applicability of the framework to transactions where government is simply receiving payments *via* electronic media in exchange for the provision of goods, services or information to consumers, for example where a government department wishes to sell goods over the Internet and sets up a website accepting credit card payments, needs to be examined on a case by case basis. It is likely that in these circumstances, good commercial practice should be appropriate.

＜引用部の訳文＞

本ドキュメントが適用する状況は、政府が取引相手の本人性（現実世界またはそれ以外）と権限を信頼し、プライバシーや機密性の侵害、データの盗難／不正使用、その他の危害が存在しないことを確保することが必要な場合である。このフレームワークには、匿名または偽名でのアクセスが認められる場合も含まれる。

ビジネススポンサーは、政府ユーザに関する登録、認証、アクセス制御、ユーザーアクセス管理の役割も考慮しなければならない。セキュリティの他の側面（物理的な面、手順面など）が適用することも考えられるため、ビジネススポンサーに対する厳密な要件はクライアントに関係する要件とは異なりうる。

政府が消費者への財、サービス、または情報の提供の見返りとしての支払いを電子的媒体で受領するだけの取引の場合（たとえば政府省庁がインターネットでの財の販売を希望してクレジットカード決済を引き受けるウェブサイトを設ける場合）は、取引に対するこうしたフレームワークの適用性をケースバイケースで検討する必要がある。そのような状況では、良い商慣行が使用されるべきであると思われる。

4.6.4. 運用方法

特に記述されていない。

4.6.5. 特徴

本フレームワークは、登録や認証が必要である全ての電子政府または電子政府代理との電子取引に適用される。また、中央政府省庁および政府機関は、電子取引に関して本フレームワークを満たさなければならない。その他公共団体については、企業や他の公共団体、公共団体の代理との間で行なわれる取引において、本フレームワークの助言を受け入れることが強く推奨される。

4.7. Australian Government E-Authentication Framework（オーストラリア）

4.7.1. 目的

本文書の目的として、以下の事項が示されている。

> Being able to conduct transactions online provides advantages to businesses and government by enabling around-the-clock services, shorter waiting times, paperless transactions and streamlined processes. However, as online transactions increase in frequency and signifi cance, the risks associated with such transactions can also increase.
>
> To provide a consistent, whole-of-government approach to managing these risks, the Australian Government Information Management Office (AGIMO) of the Department of Finance and Administration has developed the Australian Government e-Authentication Framework (AGAF).

＜引用部の訳文＞

オンラインによる取引を行えるようにすることは、24 時間サービスの実現、待ち時間の短縮、ペーパーレス取引と能率化されたプロセスにより企業と政府に便宜をもたらす。しかしながら、オンライン取引の頻度と重要性が増大すると、そうした取引に関連したリスクもまた増大する。

こうしたリスクを管理するための一貫した政府全体へのアプローチを提供するため、オーストラリア政府の財務管理省情報管理局（AGIMO）はオーストラリア政府認証フレームワークを作成した。

4.7.2. 利用者

本フレームワークの利用者としては、まず政府と企業が対象とされ、個人への拡張が進められている。

（1） 政府と企業

フレームワークの利用により、政府とのオンライン取引における信頼性の強化と取引におけるリスクレベルに応じた電子認証メカニズムとの適合を目指している。本フレームワークで規定するリスクレベルは、記述の米国 OMB によるものと同趣旨の 4 段階となっている。

（2） 政府と個人

個人を対象とするものについては、政府と企業を対象にするフレームワークを拡張

する形で、オーストラリア政府により議論が進められている。

4.7.3. 利用方法の想定

本フレームワークが企業にもたらす利点として、以下の事項が示されている。

Benefits to businesses

The AGAF provides a guide for Australian businesses on how to conduct transactions securely with Australian Government agencies on a wide range of matters and through a wide range of deliverychannels.

This will benefit businesses by enabling:

+ electronic transfer of funds or private information by government

+ around-the-clock services

+ shorter waiting times for services

+ paperless transactions with government, and

+ streamlined processes.

＜引用部の訳文＞

AGAF は、広範囲の流通チャネルを通じた広範囲の状況において、オーストラリアの企業がオーストラリア政府機関と安全な取引を確立する方法のガイドを提供する。

これは以下の事項を可能とすることでビジネスに利点をもたらす。

- 政府による資金やプライベート情報の電子的移送
- 24 時間サービス
- サービスの待ち時間減少
- 政府とのペーパーレス取引
- 能率化されたプロセス

4.7.4. 運用方法

AGAF は以下の原則のもとに運用されることが示されている。

Principles guiding the AGAF

The following principles will guide the selection and implementation of e-authentication approaches:

+ Transparency – e-authentication decisions will be made in an open and understandable manner.

+ Cost-effectiveness – businesses will not have to undergo cumbersome and expensive e-authentication processes for simple or low-risk transactions.

+ Risk management – the selection of e-authentication mechanisms will be guided by the likelihood and impact of identified risks.

+ Consistency – government agencies will apply a consistent approach to selecting e-authentication mechanisms.

+ Trust – the mechanisms used will support online services and be useful and safe.

+ Improved privacy – personal information will be collected only where necessary for the business processes being undertaken.

＜引用部の訳文＞

電子認証のアプローチに関する選択と実装は、以下の原則のもとで定められる：

- 透過性：電子認証における決定は、オープンかつ理解できるような方法でなされる。
- 費用対効果：企業は単純であるかリスクの低い取引のために、扱いにくく高価な電子認証プロセスに耐える必要はない。
- リスクマネジメント：電子認証メカニズムの選択は、起こり得る可能性と識別されたリスクの影響によって定められる。
- 一貫性：政府機関は、電子認証メカニズムの選択に対して一貫した方法を適用する。
- 信頼：使用されるメカニズムは、オンラインサービスをサポートし、便利かつ安全である。
- プライバシー強化：個人情報は、保証されたビジネスプロセスにおいて必要な場合にのみ収集される。

4.7.5. 特徴

本フレームワークの特徴として、政府と企業それぞれに向けて、オンライン取引を行う際に考慮すべき項目のチェックリストを提供していることが挙げられる。

4.8. Authentication for e-government Best Practice Framework for Authentication（ニュージーランド）

リスク評価の方針と信用レベルの定義についてのガイドラインである。また、オンライン認証ソリューションの実装方法について解説している。

4.8.1. 目的

本文書の目的として、以下の事項が示されている。

> The Framework is one of a series of documents related to an all-of-government approach to online authentication and is aimed at providing a guideline for agencies in the area of authentication.

> The Framework provides:
>
> - information on concepts and terminology related to authentication;
> - references to an all-of-government approach and the long-term strategic vision for all-of-government authentication;
> - guidance and advice regarding the issues that need to be addressed through planning and policy work; and
> - information on implementing an online authentication initiative and issues to consider.

＜引用部の訳文＞

本フレームワークは、オンライン認証に関係する全ての政府機関のアプローチに関する一連の資料の 1 つであり、政府機関での認証分野におけるガイドラインを提供することを目的としている。

具体的には、本フレームワークは以下の情報を提供している。

- 認証に関する概念と用語についての情報
- 全ての政府組織へのアプローチ、及び全ての政府組織における電子認証の長期的戦略ビジョンについてのリファレンス
- 計画と方針決定においての取り組むべき問題に関する指針と助言
- オンライン認証 initiative の実行と考慮すべき問題に関する情報

4.8.2. 利用者

オンライン認証プロジェクトの計画に関わる人、または要件決定を行う人を対象としている。特に以下の人を対象としている。

- 政府の認証構想とオンライン認証向け長期戦略目標を高いレベルから俯瞰することを希望する人
- 認証ソリューション案が省庁とクライアントに与える可能性のある効果と方針に関心のある人
- 認証の技術的実現について興味のある読者、計画と構築に関する認証オプションの検討を考える人
- 大規模な IT プロジェクト導入関連の基準と、政府の指示遵守に関心のある人

4.8.3. 利用方法の想定

電子政府サービスの中でも特に認証が必要なサービスを構築する際に利用される。

4.8.4. 運用方法

認証技術と実践の変化、オンライン認証の戦略的方向性に関する政府の意思決定を反映されるため、本フレームワークは定期的に改訂されることに注意すること。

4.8.5. 特徴

電子認証の実装方法について詳細に述べており、また製品やサービス選択に関する助言も含まれている。

本フレームワークでは、省庁が必ず採択すべき基準は指示していない。

4.9. Interchange of Data between Administrations (IDA) Authentication Policy（EU）

4.9.1. 目的

本文書の目的として、以下の事項が示されている。

This document aims at defining the IDA authentication policy, which can serve as a basic policy for establishing the appropriate authentication mechanisms in sectoral networks and in horizontal security-related projects.

Considering the nature of the IDA mission as defined by the European Commission, we believe that the scope of the IDA Authentication Policy shall be limited to the remote authentication of participants in IDA Sectoral Networks (i.e. primarily public servants of the Member State Administrations and the European Institutions) using electronic credentials.

Moreover the above analysis shows that:

- 2 main phases shall be considered in the whole authentication process: the registration phase (i.e. identity proofing + token delivery) and the remote electronic authentication (i.e. proof of possession of the token);
- The registration phase requires a Registration Authority and a Credential Service Provider to be present in one way or another (preferably locally so as to cope with the subsidiarity principle) in the authentication process;
- Several Authentication Assurance Levels shall to be defined;
- Common rules have to be defined and agreed (in particular to achieve the identity proofing of public servants) to encourage mutual recognition within sectoral applications;
- Authentication and authorisation are separate decisions
- Not only individual authentication but also group authentication shall be considered.

＜引用部の訳文＞

本ドキュメントは、IDA（Interchange of Data between Administrations）認証ポリシーの定義を行うことを目的としている。そのポリシーは、部門毎のネットワークや横断的なセキュリティに関するプロジェクトにおいて、適切な認証メカニズムを規定するための基本ポリシーとして役立つものである。

欧州委員会によって定義ていることから、IDA ミッションは IDA 認証ポリシーの対象は電子証明書を用いた IDA Sectoral Network （つまり、主として加盟国の政府やヨーロッパの公共機関の公務員）において、参加者の遠隔認証に限られていると考えられる。

更に、上記の分析は次のものを示す。

- 全体の認証プロセスにおいて、次の 2 つの主なフェーズがある：登録フェーズ（つまり、identity proofing とトークン配送）と遠隔電子認証（つまり、トークン所有の証明）。
- 登録フェーズでは、認証プロセスにおいて何らかの方法（望ましくは、欧州連合における補完性原理を対処する局所的なもの）で、登録局（Registration Authority）とクレデンシャル・サービス・プロバイダーが存在することを必要とする。
- 幾つかの認証保証レベルが定義されるようにすべきである。
- 部門別のアプリケーションにおける、相互の認識（特に、公務員による identity proofing の実現）の為、共通のルールが定義され、合意を得ている必要がある。
- 認証（authentication）と認可（authorisation）は別々に決定する。
- 個人の認証だけでなく、グループ認証も考慮されるべきである。

4.9.1.1. 用語の説明

（1） identity proofing

identity proofing は、正しく関連している(恐らく名前だけの)属性を用いて、identity が実際に実在の人物であることを保証するプロセスである。保証のレベルを上げることは、参加者の identity を保証するための取り組みを増やすことを必要とする。identity proofing を行うエンティティは、Registration Authority (RA)である。

（2） Registration Authority (RA)

Registration Authority (RA)は、通常は紙の証明書の提示やデータベースの記録によって加入者の identity 確認する役割を果たす。RA は順々に CSP へ参加者の identity を保証する。

（3） クレデンシャル・サービス・プロバイダー (CSP)

CSP は、参加者へ認証プロセスにおいて使用されるトークンを登録または与え、トークンと identity を結びつけたり、identity と何かしら使いやすい属性と結びつけたりする必要に応じて証明書を発行する。参加者は、登録の時点でトークンと組になる電子証明書を受け取るか、後ほど必要に応じて証明書を発行してもらう。

常に RA と CSP は結びついている。最も単純で、おそらく最も一般的な場合は、RA と CSP は同一のエンティティで別々の機能を有しているものである。しかしながら、RA は、独立している CSP や複数の異なる CSP の参加者を登録する会社や組織の一部であるかもしれない。従って、ある CSP には不可欠な RA が存在するかもしれないし、複数の独立した RA と結びついているかもしれない。そして、RA もまた複数の CSP と結びついている可能性がある。

（4） sectoral application（SA）

部門別のアプリケーションは、運用や共同利用できる telematic networks を設立することにより、加盟国の政府へ汎ヨーロッパサービスを提供することを目的としたアプリケーションである。

4.9.2. Sectoral Project 認証ポリシーの作成

Sectoral Application[8] Ownersは、次のように認証ポリシーを作成すべきである。基本的な流れは、米国の“ E-Authentication Guidance for Federal Agencies ”と同様である。

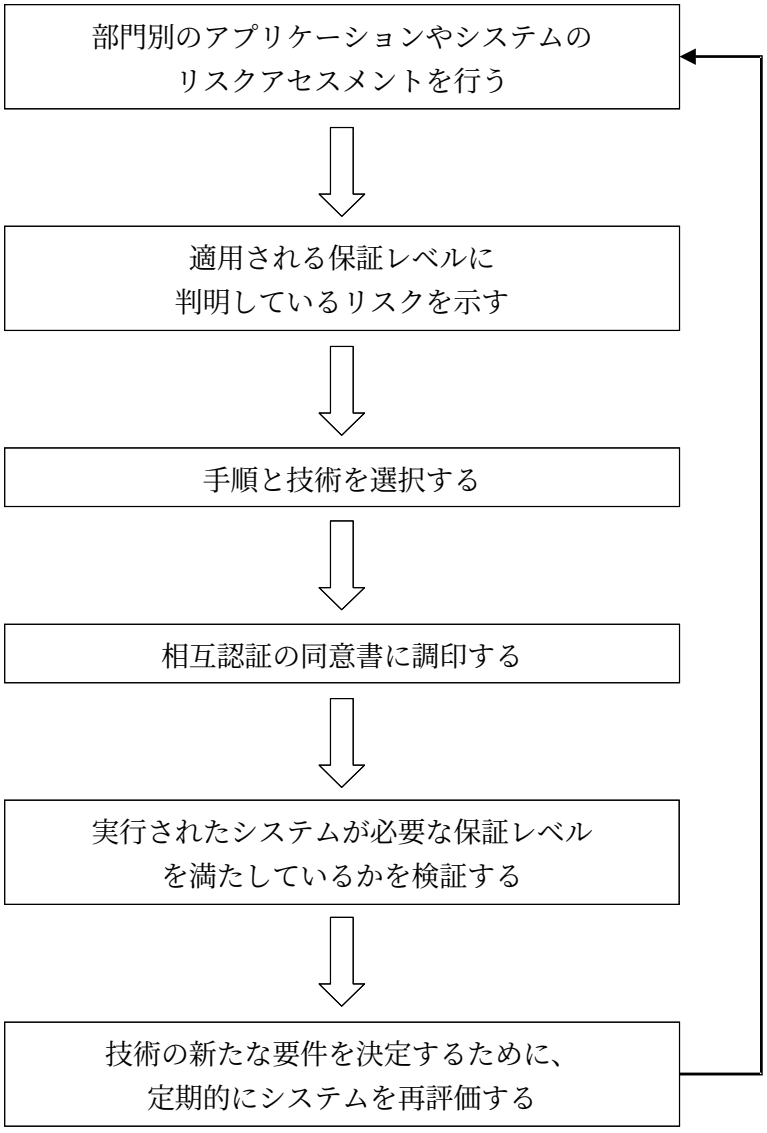


図 4−3 認証ポリシー作成の手順

[8] ここではsectoral applicationを部門別または部門内のアプリケーションと記述する。

ステップ 1：Sectoral Application やシステムのリスクアセスメントを早急に行う

公務員の主張した identity における適切な保証レベルの決定のために、sectoral application Owners は潜在的リスクの評価とそれらの影響を最小にする処置を特定しなければならない。潜在的により悪い結果を及ぼす認証エラーは、より高い保証レベルを必要とする。ビジネスプロセスとポリシー、技術はリスクを低減させることに役立つだろう。

ステップ 2：適用される保証レベルに判明しているリスクを示す

このステップは、全ての確認されたリスクの基準に従って要求される認証保証レベルを定めることにある。表 4.9.3 にあるマトリックスを参照のこと。

ステップ 3：手順と技術を選択する

リスクアセスメントと適用される保証レベルに判明しているリスクを示した後、sectoral application Owners は、適切な技術（つまり、要求する保証レベルの要件で最低限の技術）を選択する。特に、この提案されている IDA 認証ポリシーは、以下の分野における 4 つの各々の保証レベルに対する特定の技術要件について述べられている。

- identity proofing とクレデンシャルの交付を含む登録
- identity を証明するためのトークン
- 遠隔認証メカニズム
- メカニズムの判定

ステップ 4：相互認証の同意書（MRA）に調印する

いったん認証ポリシーが選ばれると、当事者間で MRA に調印しなければならない。1 つの部門内プロジェクトに対して双方での MRA の調印を行うことが膨大な数になることを避けるために、部門内プロジェクトのマネージャーと担当している専門家の委員会／グループの間で、一回の MRA に調印を行うことが望ましい。もし、部門内プロジェクトにそのような専門家の委員会／グループがないならば、欧州委員会と各々関わった加盟国の間で一回の MRA に調印しなければならない。

ステップ 5：実行されたシステムが必要な保証レベルを満たしているかを検証する

複数の実行が特定のリスクを生じさせるか悪化させるので、そのシステムが部門別のアプリケーションを利用するために要求された保証レベルを満たしていることを確認し、最終的な検証を行う。認証プロセスが必要な（例えば certification と authentication の）セキュリティ手順の一部としてシステムの認証要件を満たしていることを、部門別プロジェクトでは確認されなければならない。

ステップ 6：技術の新たな要件を決定するために、定期的にシステムを再評価する

技術の変化や部門内アプリケーションにおけるビジネスプロセスの変化の結果 identity 認証要件が有効であり続けていることを保証するために、sectoral project は定期的に情報システムを再評価しなければならない。年に一度、情報セキュリティの評価要件を設けることは、上記のための格好の機会を与える。部門内プロジェクトでは、追加的なリスク緩和処置を用いて identity 証明書の保証レベルを調整してもよい。identity 証明書の要件保証レベルを緩和することは、使用可能となる顧客対象を増加させるかもしれないが、部門内プロジェクトは、（レベルの緩和が）システムの保証レベルの選択に悪影響を及ぼさないように実施される必要がある。

4.9.3.（Annex）認証保証レベルの定義テンプレート

ここに、本文書の付録にある認証保証レベルの定義テンプレートの 1 つを載せる。表 2 5 ではリスクとして Fictitious real-world identity を記しているが、実際の付録には各リスクに対して同様の定義テンプレートが載せてある。

表 4-4　認証保証レベルの定義テンプレート

リスク	可能性	損害のインパクト				
		非常に高い	高い	中間	低い	極わずか
Fictitious real-world identity	ほとんど確か	（＊）	（＊）	レベル 4	レベル 3	レベル 3
	起こりえる	（＊）	レベル 4	レベル 3	レベル 3	レベル 2
	中程度	レベル 4	レベル 3	レベル 3	レベル 2	レベル 2
	起きそうもない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	滅多にない	レベル 3	レベル 2	レベル 2	レベル 1	レベル 1

（＊）：オープンネットワーク上では遠隔認証は適用できない

4.9.4. 認証ポリシーフレームワーク

ここでは、まず始めに保証レベルを定義し、次に迅速なリスクアセスメントに基づく保証レベルの選択方法を説明する。最後に、各レベルでの登録と電子認証を成し遂げるための手順と技術を示す。

4.9.4.1. 認証保証レベルの定義

（1） 認証保証

本文書では認証保証に関して、以下の事項が示されている。

Note: The authentication assurance describes the Sectoral Application's degree of certainty that the public servant has presented a credential that refers to his identity.

In this context, authentication assurance is defined as

- the degree of confidence in an asserted real-world identity (i.e. identity proofing)
- the degree of confidence in an electronic identity presented to a service provider by means of a credential (i.e. proof of possession)

＜引用文の訳文＞

注意：この認証保証は、公務員による本人性を示すクレデンシャルの提示に対する、部門別のアプリケーションにとっての確実さの度合いを記述している。

ここでは、認証保証は次のように定義される。

- 現実社会で主張されている本人性の信頼の程度（すなわち本人性の証拠）
- クレデンシャルを使ってサービスプロバイダーへ提示された電子的な本人性の信頼の程度（すなわち所有の証明）

（2） レベル

本文書ではレベルに関して、以下の事項が示されている。

Note: Our approach is to consider that authentication assurance levels should be layered according to the severity of the impact of damages that might arise from misappropriation of a person identity.

The more severe the likely consequences are, the more confidence in an asserted identity will be required to engage in a transaction.

We suggest 4 assurance levels to be defined:

- Level 1: .....Minimal Assurance
- Level 2: .....Low Assurance
- Level 3: .....Substantial Assurance
- Level 4: .....High Assurance

＜引用部の訳文＞

注意： person identity の不正流出から生じ得る損害の影響の重大性によって認証保証レベルが階層化されるべきだ、という考えからのアプローチである。

起こりうる結果がより深刻なほど、トランザクションに携わっている主張された本人性についてより多くの信頼が要求される。

4 つの保証レベルを次のように定義する。

- レベル 1：最小の保証
- レベル 2：低い保証
- レベル 3：かなりの保証
- レベル 4：高い保証

（3） 登録と認証の方法へのアプローチ

本文書では登録と認証の方法へのアプローチに関して、以下の事項が示されている。

It should be noted that, for a given transaction, registration and authentication might not possess equal emphasis and thus would attract different levels (i.e. Level 2 registration does not necessarily imply a requirement for Level 2 authentication and so on).

As an example, a transaction such as pseudonymous access to medical testing would need unequal levels of registration and authentication since a real-world identity is not required but strong authentication is needed to ensure that the results are disclosed only to the client possessing the correct electronic identity.

Note: Member State Administrations should allocate each sectoral application to both a registration and authentication level in accordance with the guidance contained in the proposed IDA Authentication Policy.

＜引用部の訳文＞

あるトランザクションにおいて、登録と認証は同等の重要性を持っていないかもしれなく、その結果、異なるレベルを招く（つまり、レベル 2 の登録は必ずしもレベル 2 の認証を必要とするわけではない）ことを注意しなければならない。

例えば偽名などを用いて医療検査へアクセスするトランザクションは、登録及び認証と同等のレベルは必要とされない。なぜなら、現実世界の本人性は要求せず、電子的に正しい本人性を持つ患者にだけ結果を開示することを保証するために強い認証を必要とするからである。

注意：加盟国の政府は提案された IDA 認証ポリシーに含まれるガイダンスに従ってそれぞれの sectoral application を登録と認証レベルへ割り当てるべきである。

4.9.5. リスクマネジメント

sectoral application Owners が受け入れるリスクのレベルは、資産評価やリスクの正しい識別、それらリスクを管理するために利用できる資産提供のレベル、生命・資産・サービスに及ぼす潜在的影響を含む幾つかの要因に依存している。

4.9.5.1. 評価

IDA 認証ポリシーの定義を目的としているため、データの評価のみを対象とする。

本文書では評価に関して、以下の事項が示されている。

> Whatever the nature of the DATA being exchanged over sectoral networks, i.e. CLASSIFIED or UNCLASSIFIED, there is so far no possibility to establish a one-to-one mapping between EC classification levels for information security (as defined by Council Decision [RD8]) and authentication assurance levels. The explanation for this is twofold:
>
> - On one hand, the processing of "unclassified" data over sectoral networks does not necessarily indicate a "low assurance" as far as authentication is concerned;
> - On the other hand, the use of "remote electronic authentication" may reveal not secure enough to process EU-Confidential data (or even more sensitive data), as regard to the impact of damage in case of disclosure, loss, or unauthorised modification of such data (as described in Annex A).

＜引用部の訳文＞

sectoral network 上でやり取りされているデータの性質が何であれ（すなわち CLASSIFIED または UNCLASSIFIED であれ）、（Council Decision [RD8]として定義されている）情報セキュリティのための EC（Electronic Certificate）分類と認証保証レベルの間には 1 対 1 の対応を付ける実現性は今のところない。これについての説明は次の 2 つである。

- 一方では、認証に関する限り、sectoral network 上で『分類されていない』データの処理は必ずしも『低い保証』を示すというわけではない。
- 他方では、（Annex A に記述されている）データの公開または損失、未許可の変更などの場合には損害の影響を考慮して、『遠隔電子認証』の使用は EU 秘密データ（又は更に機密なデータ）の処理においては充分には安全でないと示されるかもしれない。

表 4-5　レベルによるデータ評価の分類

<table>
<tr><td>情報セキュリティに対して EU 分類と認められたもの</td><td colspan="4">認証保証レベル</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td colspan="5">分類された情報</td></tr>
<tr><td>EU 最高機密
（Top-Secret）</td><td colspan="4" rowspan="3">（1）</td></tr>
<tr><td>EU 機密
(Secret)</td></tr>
<tr><td>EU 秘密
(Confidential)</td></tr>
<tr><td>EC 部外秘
（Restricted）</td><td></td><td></td><td>×（2）</td><td>×（2）</td></tr>
<tr><td colspan="5">分類されていない情報</td></tr>
<tr><td>制限されている
（Limited）</td><td>×</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td>内部の
（Internal）</td><td>×</td><td>×</td><td>×</td><td></td></tr>
<tr><td>公開
（Public）</td><td colspan="4">N/A</td></tr>
</table>

（1） 分類された情報に対する認証保証レベルは、Council と Commission Security の規定によって特定されている要件を遵守しなければならない。具体的には、最低でも次を満たすこと。

- そのような機密扱いの情報へのアクセスを必要としている人は、適切な認可を必要とする（EU-Confidential またはそれより上位）
- そのような情報の電子取り扱いを必要とするシステム（特に電子資

格証明書を使用する遠隔認証）は、対応するレベルで『公認されること』を要求する。従って、その公認のための SSRS は、そのようなシステムの認証の観点で規則と状況を正確に定義する。

そういうわけで、現在では IDA 認証ポリシーの範囲外にある。

（2） 適切なリスクアセスメントを受ける

4.9.5.2. リスクによる識別

本文書ではリスクによる識別に関して、以下の事項が示されている。

Risk is normally defined as the chance or likelihood of damage or loss. This definition can be extended to include the impact of damage or loss. That is, it is a function of two separate components, the likelihood that an unwanted incident will occur and the impact that could result from the incident. **Note: Only general risks pertaining to registration and authentication processes and those pertaining to misappropriation of credentials/electronic identity and/or real-world identity are considered here.**

＜引用部の訳文＞

リスクは通常、損害や損失の機会もしくは見込みとして定義される。損害や損失の影響を含むように、この定義を拡張することができる。つまり、望まれていないインシデントが起こりそうな見込みとそのインシデントによる影響という 2 つの別々のコンポーネントの機能である。

注意：登録と認証プロセスに関係する一般的なリスクと、電子および現実の identity 証明書の悪用に関係する一般的なリスクのみここでは考慮されている。

表 4-6　認証エラーに関係するセキュリティリスクの一覧

リスク ID	タイプ	説明
リスク 1	Fictitious real-world identity	クライアントが Fictitious real-world identity に関係する証明書を得る。
リスク 2	False details	偽の情報が実世界の identity に扮いて記録され、それが信頼を得てしまう。
リスク 3	アクセストークンの盗難	証明書を含むアクセストークンがユーザから盗まれるかユーザへ配送中に盗まれるかして、成りすましによってそれを使用される又はユーザの情報を得るためにその後不正使用されること。
リスク 4	実世界での identity（real-world identity）の盗難	本物の実世界での identity は、登録の時点で悪用される。
リスク 5	秘密の認証情報の妨害または暴露	（PIN や個人の署名鍵のような）秘密情報は、証明書を使用したとき送信中に傍受されるか、ユーザまたは第三者の故意・不注意によって露呈してしまう。
リスク 6	信頼されていない端末での秘密の認証情報の記憶	（家庭用またはオフィスの PC、インターネットカフェや公共のキオスクの PC など）信頼されていない端末に秘密情報が記憶される。そのような秘密情報（例えば、端末での暗号機能を実行するために使われる個人の署名鍵や暗証番号）は、ウェブベースのフォームに入れられ、後にキャッシュに保存されるかもしれない。
リスク 7	アクセストークンの権限のない使用	トークンとして発行されたユーザ以外の者によってアクセストークンが使用される。

リスク ID	タイプ	説明
リスク 8	危殆化された証明書の使用	証明書が危殆化した後に使用される。
リスク 9	状況の実質的な変化の後の証明書の使用	本来なら証明書が発行されていないことを意味するくらい状況が変化したところで証明書が使用される。
リスク 10	意図されていない目的での証明書の利用	想定した取引の種類や価値のために発行者が発行した証明書を、準備されていない取引に関して使用される。
リスク 11	正統な理由のない証明書の取り消し	状況の変化や証明書の危殆化などにおいて、誤りか悪意ある報告により証明書が取り消される。
リスク 12	証明書の詐欺的な使用	個人的にか第三者を通じて、所有する証明書が権限の与えられていない取引への使用が試みられる。
リスク 13	ハッカー攻撃	何らかの私利を獲得する目的や EU への迷惑行為、システムへのアクセス拒否、システムへの損傷をもたらすために、敵意ある部外者が Sectoral Application サービスに直接のアクセス権を得るかもしれない。
リスク 14	情報の分散格納	様々な電子政府サービスに集められた情報の断片化のために、クライアントの情報がより危ういリスクとなる。

4.9.5.3. 損害

本文書では損害に関して、以下の事項が示されている。

Every sectoral application owner will be in charge of analysing damages resulting from a breach in the authentication process and assess their impact. To help him in this process, we suggest the possible impact of damages to be chosen among those listed below (Table 3).

＜引用文の訳文＞

全ての部門別アプリケーション所有者は、認証プロセスでの違反から生じる損害を分析し、損害の影響を評価することの責務を負う。このプロセスの手助けのために、以下に記載したリスト表 5‐7 から損害の起こりうる影響を選択することを推奨する。

表 4-7　損害

損害	コメント
完全性の喪失	システムとデータの完全性は、情報が不適当な変更から保護されるという要件について言及している。意図的であるか偶然の行為によってデータや IT システムに許可されていない変更が行なわれると、完全性は喪失する。もしシステムやデータにおける完全性の喪失が修正されないのならば、汚染されたシステムや改竄されたデータの継続的使用は、不正確や詐欺、誤った決定をもたらすかもしれない。また、完全性の侵害は、システムの可用性や機密性に対する攻撃に先立って実行されたものかもしれない。これら全ての理由のために、完全性の喪失は IT システムの保証を低減させることとなる。
可用性の喪失	エンドユーザが基幹 IT システム（mission-critical IT system）を利用できないならば、組織のミッションに影響を及ぼすかもしれない。例えば、システム機能と操作の有効性の損失は、生産的な時間の損失をもたらすかもしれない。その結果、組織のミッションをサポートするシステム機能は、エンドユーザのパフォーマンスを阻害する。
機密性の喪失	システムとデータの機密性は、不正開示からの保護の観点から言及される。機密情報の不正開示における影響は、国家の安全を危険にさらすことからプライバシー保護法データ（個人データ等のプライバシー保護の対象となるデータ）の流出にまで及ぶ。未許可または予期しない、意図的でない流出によって組織存続の上での評価を失う。これは評判の悪化、信憑性の損失や不利な結果、信用の失墜、困惑、または訴訟を伴う。

損害	コメント
個人の安全に対するリスク	情報の不正開示や変更、非可用性は、個人の安全を生死にかかわる危険にさらしめる可能性がある。例えば次の通りである。 ・ 特定個人の住所の不正開示は、政治的・不平・その他の動機であれ、その人に害を加えたいと望んでいる人々に狙われるかもしれない。 ・ （例えば、製造プロセスや交通移動、医療行為などに関わる）情報の不正変更は、設備の誤作動、安全や人々の幸福での悪影響によって誤った決定などを起こしかねない。 ・ （例えば、交通移動や医療行為などに関わる）システムの情報の非可用性は、安全や人々の幸福での悪影響によって決定が遅れたり誤ったりすることをもたらしかねない。
経済的損失	金銭的な取引に直接関わる情報や関係組織の経済的な状態に関する情報が IT システムに格納され処理される。非可用性や破壊と同様に、そのような情報の不正開示と改竄によって経済的損失を被るだろう。例えば、遅延かアクションが無いことによる、株価の低下や詐欺、契約違反による損害である。同時に、非可用性の結果や情報の破壊などは、ユーザへの混乱を招く。そのようなインシデントからの修正または復旧は時間と労力を要する。このようなことは場合によっては重要であり、考慮されなければならない。共通名目を利用するために、復旧のための時間を人月によって計算し、財務費用に換算すべきである。この費用は、組織内で適当な等級/レベルでの人月の正常原価を参照することによって計算されるべきである。

4.9.5.4. Likelihood Determination

本文書では Likelihood Determination に関して、以下の事項が示されている。

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

＜引用文の訳文＞

潜在的脆弱性が関連する脅威環境の構図の範囲内で実行されるかもしれないという可能性を指し示す総合的な見込み評価を導くために、以下の支配的な要因は考慮しなければならない。

- 脅威の原因のモチベーションと脅威ができること
- 脆弱性の本質
- 現在のコントロールの存在と有効性

表 4-8　Likelihood Level

Likelihood Level	Likelihood Definition
ほとんど確か	脅威の原因は、大いに動機付けられていて充分な能力を有している。そして、その脆弱性が実行されることを阻止するコントロールは効果がない。
起こりえる	脅威の原因は、大いに動機付けられていて充分な能力を有している。しかし、その脆弱性が実行されているところはコントロールが効く。
中程度	脅威の原因は、動機付けられていて能力を有している。しかし、その脆弱性が実行されているところはコントロールが効く。
起きそうもない	脅威の原因は、動機付けか能力に欠けている。又は、コントロールによって脆弱性の実行を阻止できるか、少なくともかなり阻止できる。
滅多にない	脅威の原因は、動機付けと能力に欠けている。又は、コントロールによって脆弱性の実行を阻止できる

4.9.5.5. Impact Severity Scaling

表 4-9　Scale ranging of impact severity.

記号	範囲	説明
N	無視できる	損害は通常の操作で対処される
L	低い	損害は、いくらかのサービスの効率または効果を脅すが、内部的に対処することができる
M	中間	損害は、サービスの提供は脅かさないが、加盟国の政府は重大な検査を受けるか機能の方法を換えることを意味する。
H	高い	損害は、サービスの継続的な供給を脅かし、トップレベルのマネジメントか政府の干渉を要する
V	非常に高い	損害は、クライアントと政府に対して重大な問題を引き起こして、主要なサービスの供給を脅かす

4.9.5.6. レベルによるリスクの測定

既存のリスク低減尺度のあるバックグラウンドとは対照的に、リスクの測定は事件の起こりやすさと損害の影響の両方の関係で決定される。

損害の影響、及び起こりやすさは、リスクレベルの決定に対して決定的になってはならない。部門内アプリケーションでの最も大きなリスクは、強烈な影響を持っており、ほぼ間違いなく起きてしまうというものである。逆に、影響を無視でき、また滅多に起きない事件は取るに足らないものと考えられる。滅多に起こらないが強烈な影響を与えるイベントは、重大なリスクであると考えられる。

特定されたリスクを考慮に入れて、Application に必要な認証保証レベルを推測するために部門別アプリケーションの責任者は、効果的なリスクマトリックスの開発が望ましいかも知れない。このプロセスを手助けするために、リスクの測定（MoR: Measure of Risk）から、考慮されたそれぞれのリスクを低減させることを要求するし最小の認証保証レベルへ落とし込むことができる参照マトリックス（表 4-10）を作成した。

表 4-10　リスクの測定／認証保証レベルマトリックス

		損害の影響				
	Likelihood	非常に高い	高い	中間	低い	無視できる
リスク i	ほとんど確か	（＊）	（＊）	レベル 4	レベル 3	レベル 3
	起こりえる	（＊）	レベル 4	レベル 3	レベル 3	レベル 2
	中程度	レベル 4	レベル 3	レベル 3	レベル 2	レベル 2
	起きそうもない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	滅多にない	レベル 3	レベル 3	レベル 2	レベル 2	レベル 1
	ほとんど確か	レベル 3	レベル 2	レベル 2	レベル 1	レベル 1
（＊）オープンネットワーク上では遠隔認証は適用できない						

4.9.6. 登録

本文書では登録に関して、以下の事項が示されている。

> In our approach, levels 1 and 2 recognise the use of anonymous credentials. When anonymous credentials are used to imply membership in a group, the level of proofing should be consistent with the requirements for the identity credential of that level. Explicit requirements for registration processes for anonymous credentials are not specified, as they are unique to the membership criteria for each specific group.
>
> At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on their relationship.

＜引用部の訳文＞

本ポリシーのアプローチでは、レベル 1 と 2 は匿名の証明書の使用を認める。匿名の証明書がグループの会員資格を意味するのに用いられるとき、証明のレベルは identity 証明のために要求されるレベルと一致しているべきである。匿名の証明書のための登録プロセスは明確な用件は特定されておらず、それぞれ特定のグループおいて特有の会員基準に則る。

レベル 2 やそれ以上において、登録に関する記録は、それらの関係によって RA か CSP により保守されるべきである。

4.9.7. 電子認証方法

本文書での POLSECD[RD7]からの引用部分を以下に示す。

Extract from POLSEC [RD7]:

Authentication is generally achieved through one or more of the following methods:

- **Authentication by Knowledge (a.k.a. "Something you know").** This method is based on something the user knows. This could be a password or a Personal Identification Number (PIN). This method is based on the assumption that the value used for authenticating a certain person is only known to that person.
- **Authentication by Ownership (a.k.a. "Something you have").** This method is based on something that the user possesses. This could be, for example, a smart card, hardware token, an identity card or a door key. The method is based on the assumption that it is difficult for an attacker to replicate the object used for authentication, and that users do not allow other persons to use their authentication objects.
- **Authentication by Characteristic (a.k.a. "Something you are").** This method is based on the utilisation of biometrics to recognise one or more unique characteristics of the user, such as the retina pattern and fingerprints. This method is based on the assumption that certain human characteristics can uniquely identify human beings.

＜引用部の訳文＞

POLSEC [RD7]からの引用：

一般に、認証は以下の方法の 1 つ以上を用いて達成される。

知識（"Something you know" の別名でも知られる）による認証。この方法は、ユーザの何かしらの知識に基づいている。これは、パスワードや暗証番号（Personal Identification Number：PIN)）によってなされる。この方法は、" 特定の人を認証するために使用される値は、その人しか知らない値である "という仮定に基づいている。

所有（"Something you have"の別名でも知られる）による認証。この方法は、ユーザの何かしらの所有に基づいている。例えば、スマートカードやハードウェアトークン、ID カード、ドアの鍵などがこれに当たる。この方法は、" 認証のために使用されるものを攻撃者が複製することが困難であり、ユーザはそれら認証のためのものを他人が使用することを許さない " という仮定に基づいている。

特徴（“Something you are” の別名でも知られる）による認証。この方法は、網膜パターンや指紋などのユーザ特有の 1 つ以上の特徴を、バイオメトリックスによる認識を利用することに基づいている。この方法は、“ 特定の人の特徴は、その人を唯一特定することができる ” という仮定に基づいている。

本文書では電子認証方式に関して、以下の事項が示されている。

> In electronic authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for electronic authentication shall include some secret information and it is important to provide security for the token. In fact, the three methods (or “factors”) mentioned above often influence the security provided by tokens. Tokens that incorporate all three factors are stronger than tokens that only incorporate one or two of the factors.

電子認証では、要求者はネットワーク上でシステムやアプリケーションを認証する。従って、電子認証のために使用されるトークンは、何かしらの秘密情報を含んでいるべきであり、トークンによってセキュリティを供給することは重要である。実際、上記で言及されている 3 つの方法（もしくは要素は）は、しばしばトークンによって提供されたセキュリティに影響を及ぼす。3 つの要素全てを取り入れたトークンは、1 つか 2 つの要素しか取り入れていないトークンより強固である。

4.9.7.1. トークンタイプ

本文書ではトークンタイプに関して、以下の事項が示されている。

> In this sense, four types of tokens for authentication are presented below (Table 7). Each type of token incorporates one or more of the methods (something you know, something you have, and something you are.)
>
> **Note: Only electronic tokens are considered here.**

＜引用部の訳文＞

この意味で、認証のための 4 つのタイプのトークンは、下記の表 4-11 で示される。それぞれのタイプのトークンは、（知っていること、持っていること、本人の性質）方法の 1 つかそれ以上を取り入れている。

注意：ここでは電子的なトークンのみを扱っている。

表 4-11　トークンタイプ

トークンタイプ	説明
パスワードまたは PIN トークン	クライアントが自分自身のアイデンティティを認証するために暗記して、使用する秘密の文字列
ワンタイムパスワードデバイストークン	認証のために“ one time ”パスワードを生成するパーソナルハードウェアデバイスである。デバイスは、ある種の不可欠な entry pad や不可欠な（指紋などの）バイオメトリック読み取り機、（USB ポートのような）直接的なインターフェースを持ち合わせているかどうか分からない。 ハードウェアデバイスに保管された対称鍵とワンタイムパスワードを生成するために使われたノンスを組み合わせる為、パスワードは、ブロック暗号かハッシュアルゴリズムを用いて生成されるべきである。ノンスは、日時やデバイスで生成されたカウンター、（デバイスに入力機能があれば）検証者から送られてきたチャレンジでもよい。 ワンタイムパスワードは、通常はデバイスに表示されパスワードとして検証者に手動入力する（デバイスからコンピュータへ直接の電子入力も許可されている）。
ソフト暗号トークン	暗号鍵は、通常はディスクか何か他のメディアに保存されている。認証は、鍵の所有証明と管理によって成される。ソフトトークンは、ユーザしか知らないパスワードから得られた鍵を用いて暗号化されるので、パスワードに関する知識はトークンを使える状態にするために必要である。それぞれの認証はパスワード入力を必要とするべきであり、認証鍵の暗号化されていない複製は認証後に消去されるべきである。
ハード暗号トークン	保護された暗号鍵を含んでいるスマートカード。認証は、そのデバイスの所有を鍵管理の証明によって成される。ハードトークンは、 ・ パスワード入力か認証鍵を有効にするためのバイオメトリックを要求し、 ・ 認証鍵をエクスポートすることができない でなければならない。

（1） レベルによるトークンタイプ

表 4-12　レベルによるトークンタイプ

トークンタイプ	保証レベル			
	1	2	3	4
ハード暗号トークン	×	×	×	×
ソフト暗号トークン	×	×	×	
ワンタイムパスワード デバイストークン	×	×		
パスワードまたは PIN トークン	×			

4.9.7.2. 遠隔認証メカニズム

本文書では遠隔認証メカニズムに関して、以下の事項が示されている。

> **Remote authentication mechanisms are basically the credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be.**

＜引用部の訳文＞

遠隔認証メカニズムは、基本的には、証明書やトークン、要求者が実際に自分自身だと主張する加入者であることを確認する認証プロトコルである。

（1） Authentication Protocols Threat Model

本文書では、Authentication Protocols Threat Model に関して、以下の事項が示されている。

> RAs, CSPs, verifiers and relying parties are ordinarily trustworthy (in the sense of correctly implemented and not deliberately malicious). However, claimants or their systems may not be trustworthy (or else we could simply trust their identity assertions).

＜引用部の訳文＞

通常、RAs、CSPｓ、検証、および relaying parties は信頼できる（正しく実行されていて故意に悪意がないことの意味において)。しかしながら、主張者やそのシステムは信頼できないかもしれない（我々は、identity の主張についてのみ信頼できる)。

（2） レベルによる認証プロトコル

表 4-13 レベルによる認証プロトコルタイプ

許可されたプロトコルタイプ	保証レベル			
	1	2	3	4
秘密鍵 PoP	×	×	×	×
共通鍵 PoP	×	×	×	×
ワンタイム（又は強力な）パスワード PoP	×	×	×	
Tunnelled password PoP	×	×		
Challenge-reply password PoP	×			

PoP: Proof of Possession

（3） レベルによる保護要件

表 4-14　レベルによる保護要件

保護	認証保証レベル			
	1	2	3	4
盗聴者		×	×	×
リプレイ	×	×	×	×
オンライン推測	×	×	×	×
検証者に成りすまし			×	×
中間者攻撃			×	×
セッションハイジャック			×	×

4.9.7.3. Assertion Mechanisms

本文書では、Assertion Mechanisms に関して、以下の事項が示されている。

Assertion mechanisms are used to communicate the results of a remote authentication to other parties.

Relying parties may accept assertions that are:

- Digitally signed by a trusted identity (e.g. the verifier); or
- Obtained directly from a trusted entity using an authentication protocol of the corresponding level or above.

Assertions shall expire after a certain period, defined by level (see …). They should not be accepted afterwards.

＜引用部の訳文＞

Assertion mechanisms は、遠隔認証の結果を他の関係者へ伝えるために使用される。

当てにされた関係者は、次の場合には主張を受け入れるだろう。

- （例えば検証者など）信頼された identity によって電子的に署名された

・ 対応するレベルかそれ以上のレベルの認証プロトコルを通じて信頼されたエンティティから直接受け取る。

レベルによって定められたある期間の後に、Assertions は期限が切れるものとするべきである。その後は、その Assertions を受け入れるべきではない。

表 4-15　レベルによる有効期限

有効期限	保証レベル			
	1	2	3	4
24 時間	×			
12 時間	×	×		
2 時間	×	×	×	
直ちに	×	×	×	×

4.9.8. Common Practice Statement

表 4-16　レベル 1　ポリシー

情報分類	sectoral network 上だけでは分類されていない情報の交換は適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 1 の登録** 1．定義 実世界での identity の流出によって起こり得る損害が「無視できる」または「低い」影響の sectoral application transaction に対しては、レベル 1 の登録は適当である。 この登録レベルは（ウェブメール、オンライン、オークションなど）多くのインターネットアプリケーションで使用頻度が高い。 2．要件 identity 証明や登録事実の記録を保持するといった要件はない。主張者の identity 断言は受け入れられる。e-メールアドレスだけは一義的で検証されなければならない。
登録データの保存期間	**なし**
トークンタイプ	多くの場合、パスワードや PIN トークン しかしリスクアセスメントによれば、以下のものも可能である。 ・ ワンタイムパスワード・デバイス・トークン ・ ソフト暗号トークン ・ ハード暗号トークン

電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	大抵の場合、Challenge-reply password PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ Tunelled password PoP ・ ワンタイム（又は強力な）パスワード PoP ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ リプレイ ・ オンライン推測

表 4-17　レベル 2　ポリシー

情報分類	sectoral network 上だけでは分類されていない情報の交換は適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 2 の登録** 1．定義 実世界での identity の流出によって起こり得る損害が「中間」影響の sectoral application transaction に対しては、レベル 2 の登録は適当である。 レベル 2 登録のほとんどの場合、オンラインですぐに成し遂げることができる。 ２．要件 述べられている登録ポリシーによると、加入者の identity 情報が検証、確認されることを RA が確実にするべきである。identity 情報は、加入者を一意的に特定することができる最低限で完全な正式氏名、他をサポートしている情報を含むべきである。 登録事実の記録は、CSP かその代表によって保存されるべきである。Level 2 証明書のための登録データのために提案された最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれでも）を越えた 5 年である。 もし、RA と CSP が分離していてネットワーク上で交信するのであれば、RA と CSP 間の登録取引全体を含む交信は、承認された方法での暗号的保護と少なくともレベル 2 保証での要件を満たしている認証プロトコルであるべきである。 3．手順 少なくとも、登録手続は次を行う。 (1)　加入者の主張された identity が、機構との認証された進行中のビジネス関係の人であることを確認する。そのために、RA は実世界 identity 証明（例えば、

	国家の ID カード、運転免許証、パスポートなど）の署名済みコピーを要求しなければならない。 (2) 検証された identity と下記の何れかで確認されたものを紐ける形で、証明書やトークンを発行や更新する。 (a)加入者の記録のポータルアドレス（例えば、認証者が記録されているアドレスへ手紙を送る） (b)加入者の電話番号（例えば、記録されている加入者電話番号へ掛ける又は掛けさせるを要求する） (c)記録されたアドレスへ電子メールか他の電子的ビジネスコミュニケーション（例えば、認証者から加入者の電子メールアドレスへ送る）
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 5 年。
トークンタイプ	望ましくは、ワンタイムパスワード・デバイス・トークン しかしリスクアセスメントによれば、以下のものも可能である。 ・ ソフト暗号トークン ・ ハード暗号トークン
電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	たいてい、Tunnelled 又はワンタイムパスワード PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測

表 4-18　レベル 3　ポリシー

情報分類	sectoral network 上での分類されていない情報と EU-RESTRICTED レベルの分類された情報の交換へ適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 3 の登録** 1. 定義 実世界での identity の流出によって起こり得る損害が「高い」影響の sectoral application transaction に対しては、レベル 3 の登録は適当である。 レベル 3 での identity proofing は、RA が加入者の identity の実質証拠を検証することを必要とする。しかし、加入者が登録するために自分で現れることを必ずしも義務づけるというわけではない。一般的に、identity を検証するために用いられた証明書や記録の少なくとも幾つかの実態が、現在でも有効だと確認するということを、レベル 3 での identity proofing は必要とする。それには物理的アドレスや記録にある電話番号の確認も必要とする。 2. 要件 加入者の identity 情報が述べられている登録ポリシーに従って検証・チェックされていることを RA は確認すべきである。identity 情報は少なくとも次のものを含む。 ・ 完全な正式氏名 ・ 誕生の日付と場所（検証されないかもしれないが、集められるべきである） ・ 記録の現在の場所 ・ パスポート番号や社会保険番号、運転免許証番号など、登録プロセスでチェックされた全ての文書の identity 番号 実世界 identity の証拠（例えば、国民 ID カード、運転免許証、パスポートなど）の提示によって identity は検査され

	なければならない。加入者は、組織における自分の活動に関する証拠（例えば、加盟国政府の手紙など）のうち 1 つは提示もしなければならない。 登録の事実に関する記録は、CSP かその代表によって保存されるべきである。Level 3 証明書のための登録データのために提案された最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれでも）を越えた 7 年である。 もし RA と CSP が分離していてネットワーク上で交信するのであれば、レベル 3 以上で要求されるものに合致する認証プロトコルを用いて暗号的に認証し、暗号化では承認された暗号方法を用いて、登録取引全体を行うべきである。 3. 手順 少なくとも、登録手続は次を行う。 (1) 加入者の主張された identity が、現在の個人で、証明書（例えば、加盟国政府の手紙など）の提示によって組織との関係が優良な状態であることを確認する。 (2) 検証された identity と下記のどちらかで確認されたものを紐ける形で、証明書やトークンを発行や更新する。 (a)加入者の記録のポータルアドレス（例えば、認証者が記録されているアドレスへ手紙を送る） (b)加入者の電話番号（例えば、記録されている加入者電話番号へ掛ける又は掛けさせるを要求する）
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 7 年。
トークンタイプ	ソフト暗号トークン しかしリスクアセスメントによれば、次のものも可能である。 ・ ハード暗号トークン

電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	望ましくは、ワンタイムパスワード PoP しかしリスクアセスメントによれば、以下のものも可能である。 ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測 ・ 検証者に成りすまし ・ 中間者攻撃 ・ セッションハイジャック

表 4-19　レベル 4　ポリシー

情報分類	sectoral network 上での分類されていない情報と EU-RESTRICTED レベルの分類された情報の交換へ適用できる
登録フェーズ	
・ identity proofing の手続き ・ ユーザ登録の詳細 ・ トークンと信用証明書の交付	**レベル 4 の登録** 1. 定義 実世界での identity の流出によって起こり得る損害が「非常に高い」影響の sectoral application transaction に対しては、レベル 4 の登録は適当である。 加入者の写真を含む identity 文書と、加入者から撮影された写真や指紋などのバイオメトリックと記録に保存されたもので、対面の identity proofing を必要とするという点で、レベル 4 での identity proofing は異なっている。 トークンの配送も、RA において実際に現れて関連付けられるべきである。このレベルでは、加入者がアプリケーションへ手書きでサインをし、これは違反すれば偽証罪が適用される。 2. 要件 加入者の identity 情報が述べられている登録ポリシーに従って検証・チェックされていることを RA は確認すべきである。 最初のステップとして、加盟国政府の公務員へ信用証明書を発行するために、組織管理から認証された要請が、RA／CSP によって必要とされる。さらに、RA／CSP は加入者によって提供されたバイオメトリックを用いて検証することを必要とする。 取られた方法と加入者の identity を検証するために試験されたあらゆるドキュメントのコピーを含む登録事実の記録は、CSP かその代表によって保守されるべきである。 Level 4 証明書のための登録データのための最小限の保持期間は、証明書の満期または取り消し（より遅いものはどれ

	でも）を越えた 10 年である。 もし RA と CSP が分離していてネットワーク上で交信するのであれば、レベル 4 で要求されるものに合致する認証プロトコルを用いて暗号的に認証し、暗号化では承認された暗号方法を用いて、登録取引全体を行うべきである。 3. 手順 少なくとも、登録手続は次を行う。 （1)　加入者に対するクレデンシャルの発行要求が、組織管理の上で提出されたことを検証する。 （2)　公式の組織人事記録を利用することにより加入者の職業を検証する。 （3)　登録同局の前に、次のプロセスに基づいて対面の検査により加入者の identity を証明する。 （a)identity 証明として､加入者は政府によって発行された識別（例えば、現在のパスポートや運転免許証）または組織の発行した写真つき ID （b)RA は､提示された信用証明書に加入者に結びつくバイオメトリックデータがないか検査する。 （c) 上記(3)(a)で提示された信用証明書が、現在でも通用し合法的だということを RA によって検証されるべきである（例えば、組織発行 ID は有効かどうかが検証される)。通常これは、信用証明書を発行した組織に保存してある人事記録に問い合わせを行うことにより成し遂げられる。 （4)　加入者のバイオメトリック（例えば､写真や指紋）を記録し保存する。 その上、RA は各々の信用証明書を発行するために辿ったプロセスを記録すべきである。プロセス文書と認証要求は次のものを含むべきである。 ・　識別をしている人の identity

	・ CSP によって要求され identity 検証された加入者が署名した宣言書 ・ 加入者の ID や ID の複製による一意的な identity ナンバー ・ 加入者のバイオメトリック ・ 検証の日付と時間 ・ 加入者の手書き署名によって署名され、identity 認証を実行する人の面前で行なわれる identity 宣言書 ・ 受領者と、加入者が手書きで署名をし、identity 認証を実行する人の面前で行なわれたトークン利用者との間での義務に関する協定書
登録データの保存期間	証明書の満期または取り消し（より遅いものはどれでも）を越えた 10 年。
トークンタイプ	ハード暗号トークン
電子認証フェーズ	
PoP (Proof of Possession)のための認証プロトコル	次の何れか ・ 共通鍵 PoP ・ 秘密鍵 PoP
保護実行のために Sectoral Application owner に対する要件	・ 盗聴者 ・ リプレイ ・ オンライン推測 ・ 検証者に成りすまし ・ 中間者攻撃 ・ セッションハイジャック

4.9.9. 利用者

IDA 認証ポリシーの範囲は、電子証明書を用いることにより、IDA Sectoral Networks における関係者間の遠隔認証に限定されるものとする。

4.9.10. 利用方法の想定

Sectoral Project Authentication Policy を作成する、またはこれを利用する際に本ドキュメントの参考を利用する。

4.9.11. 運用方法

特に記されていない。

4.9.12. 特徴

本ドキュメントは、フレームワーク規約 ENTR/01/67-CONSEC の下で準備されたものである。また、本ドキュメントは 2003 年に発表された米国の“ E-Authentication Guidance for Federal Agencies ”を参考に作成されたもので、一部文言などが同一である。

フレームワークの登録段階において、バイオメトリックを使用する記述があるので人の認証のみを扱っている。

4.10. TRUST FRAMEWORK（米国）

4.10.1. 目的

本文書の目的として、以下の事項が示されている。

> Signatories to these business rules agree that these rules govern the use and validation of Electronic Authentication Partnership (EAP) certified credentials, the certification of such credentials and the accreditation of those who assess issuers of such credentials. These business rules are intended to cover use of credentials for purposes of authentication and not specifically for the application of a legal signature, which may be subject to other rules depending upon the parties and transactions involved.

＜引用部の訳文＞

本ビジネス・ルールにおける署名者は、Electronic Authentication Partnership（EAP）証明書付きクレデンシャルの使用とバリデーション（有効性検証)、当該クレデンシャルの証明、及び当該クレデンシャルの発行者のアセスメントを担当する機関の認定に関して、当該ルールに準拠することに同意する。本ビジネス・ルールは、認証を目的とするクレデンシャルの利用を対象としており、当事者および関係取引ににより別のルールが適用され得る特定の法的署名の適用について意図しているわけではない。

4.10.2. 利用者

EAP システムに参加する全ての人々を対象とする。

4.10.3. 利用方法の想定

本文書の利用方法の想定として、以下の事項が示されている。CSP（クレデンシャル・サービス・プロバイダー）が、EAP 認定アセスメント機関によるアセスメントを無事完了することができるために利用する。アセスメントについては、下記の通りである。

The EAP Service Assessment Criteria (SAC) are prepared and maintained by the Electronic Authentication Partnership (EAP) as part of its Trust Framework. These criteria set out the requirements for services and their providers at all assurance levels within the Framework. These criteria focus on the specific requirements for EAP assessment at each assurance level (AL) for the following:

- The general business and organizational conformity of services and their providers,
- The functional conformity of identity proofing services, and
- The functional conformity of credential management services and their providers.

These criteria (at the applicable level) must be complied with by all services that are assessed for certification under the EAP Trust Framework.

＜引用部の訳文＞

EAP Service Assessment Criteria(SAC)は Trust Framework の一部として Electronic Authentication Partnership(EAP)によって作成され、維持される。この基準は、フレームワーク内のすべての保証レベルについて、サービスとプロバイダの要件を規定する。そして、各保証レベル（AL）における EAP アセスメントとして、下記の具体的要件を焦点としている。

- サービス及びサービスプロバイダーのビジネス全般と組織の適合性
- identity proofing services の機能的な適合性
- クレデンシャル管理サービスとそのプロバイダの機能的な適合性

EAP Trust Framework の下で証明用に評価されるすべてのサービスが（該当するレベルで）この基準に従っていなければならない。

4.10.4. 運用方法

本文書の運用方法として、以下の事項が示されている。

Promulgation and Amendment of Business Rules and Other Documents

The EAP shall formalize and may periodically amend these business rules. The EAP shall also formalize and may periodically amend a set of documents governing the accreditation of assessors of EAP CSPs and the certification of EAP credentials. The EAP reserves the right, at its discretion, to formalize and periodically amend such other materials, including policies or guidelines, participation agreements, handbooks or other documents relevant to the EAP. Notice of all amendments shall be given by EAP by electronic mail to the contact person(s) identified by each signatory for such purpose and by posting to the EAP web site. All amendments shall be effective as of the date specified in such notice. If a signatory objects in writing to an amendment within 30 days after notice of the amendment is given by EAP, such objection shall be deemed to be a notice of termina-tion of such signatory's participation in EAP under Section 1.2.

Relying Party, CSP and Assessor Approval

The EAP is responsible for approving participation in the EAP System by relying parties, CSPs and assessors. The EAP shall formalize and may periodically amend requirements for certification of credentials issued by a CSP and the accreditation of assessors of CSPs. The EAP shall formalize, maintain and update as needed an EAP-approved CSP list (EAP CSP list) of certified signatory CSPs. This EAP CSP list shall include, at a minimum, the names of each CSP, the level of assurance for which credentials issued by the CSP have been certified and a URL and other contact information for the CSP.

＜引用部の訳文＞

ビジネス・ルールその他の文書の正式発行と修正

EAP は、このビジネス・ルールを公式化するものとし、これを定期的に修正することができる。また、EAP は、EAP CSP のアセスメント機関の認定及び EAP クレデンシャルの証明に関する一連の文書を公式化するものとし、これを定期的に修正することができる。EAP は、EAP に関連する方針、ガイドライン、参加協定、ハンドブックまたは他の文書を、独自の判断で公式化し定期的に修正する権利を保有する。あ

らゆる修正に関する通知は EAP により、その目的で署名された連絡先への電子メール、ならびに EAP の Web サイトへの掲載により行われる。すべての修正は、当該通知に指定する日付をもって効力を発生する。EAP により修正の通知があった後 30 日以内に署名者がその修正に対して書面により異議を申し立てる場合、当該異議申し立ては本フレームワークのセクション 1.2 に基づき EAP への当該署名者の参加終了の通知であるとみなされる。

信頼当事者、CSP 及びアセスメント機関の承認

EAP は、信頼当事者、CSP 及びアセスメント機関が EPA システムへ参加を承認することに責任を負う。EAP は、CSP の発行するクレデンシャルの証明及び CSP のアセスメント機関認定の要件を公式化するものとし、これを定期的に修正することができる。EAP は、証明済みの署名者 CSP を記載する EAP 承認済み CSP リスト（EAP CSP リスト）を公式化し、維持し、必要に応じて更新する。この EAP CSP リストには、各 CSP の名称、CSP の発行するクレデンシャルが証明された際の保証レベル、及び CSP の URL その他の連絡先情報を最低限記載するものとする。

4.10.5. 特徴

各信頼当事者と CSP は、EAP システムへの参加の前提条件として、このビジネス・ルールによって制約されていることに同意しなければならない。

4.11. EVIDENCE OF IDENTITY FRAMEWORK（ニュージーランド）

本文書には、以下の事項が示されている。

This EOI Framework is a good practice tool for establishing, to a high level of confidence, the identity of individuals who wish to carry out transactions carrying a significant level of identity-related risk with government agencies – such as exchanging sensitive personal information or conducting transactions with financial implications.

It has been developed in response to a number of issues:

- Government agencies currently take different approaches to EOI, which can cause confusion for the individuals concerned, who may be asked to supply different EOI for similar uses.
- The identified need for a robust, consistent and cross-government approach to EOI that will help protect individuals against the theft or fraudulent use of their identities, and prevent the personal and public loss of money through identity fraud.
- The requirement for a robust framework has become increasingly important to the E-Government Unit's work on online identity authentication.
- Identity fraud (whether through establishing false identities or stealing legitimate ones) is increasing and has significant financial and social costs to individuals, businesses and the public.
- Identity fraud is increasingly an international problem, with links between identity fraud and other criminal activity.

＜引用部の訳文＞

本認証（EOI: Evidence Of Identity：以下 EOI と記す）フレームワークは、政府機関と identity 関連のリスク（identity-related risk）の有意水準で取引（例えば、機微な個人情報を交換や、経済的な取引。）を行いたいと思っている個人の identity を高レベルの信頼で確立するためベスト・プラクティス・ツールである。

これは、次のような多くの問題に応じて開発されたものである。

政府機関は現在、関係する個人に対して混乱を引き起こしたり、同様の用途に対して異なる EOI の提供が要求されたりする様々なアプローチの EOI を行なっている。

盗難や identity の不正使用から個人を守る手助けをし、identity 詐欺による個人や公共の金銭的損失を防ぐような、強固で一貫性のある政府横断的な EOI へのアプロー

チが認証には必要である。

強固なフレームワークの要件は、オンライン identity 認証に対する電子政府ユニットの仕事に対してますます重要になってきている。

（誤った identity の確立や合法的なものを盗むことにかかわらず）identity 詐欺は増加し、個人やビジネス、公共へ著しい財政的・社会的損失をもたらしている。

identity 詐欺は、identity 詐欺と他の犯罪行為との関連で、国際問題へと発展している。

The EOI Framework is a good practice tool for establishing, to a high level of confidence, the identity of individuals who wish to carry out transactions that have a significant level of risk with government agencies.

It is important to note that agencies should apply the Framework alongside, and not instead of, other initiatives designed to mitigate the risks associated with identity fraud.

EOI フレームワークは、政府機関と identity 関連のリスク（identity-related risk）の有意水準で取引を行いたいと思っている個人の identity を高レベルの信頼で確立するためベスト・プラクティス・ツールである。

政府機関は、identity 詐欺のリスクを低減されるために設計された他のイニシアチブの替りではなく、それらと並行して本フレームワークを適用すべきであると留意することは重要である。

次の図 4−4 は、EOI フレームワークの一部をなすものである。これは、各コンポーネントについて概説しているもので、それぞれの Objective は高レベルの認証で個人の identity を認めるために必要である。

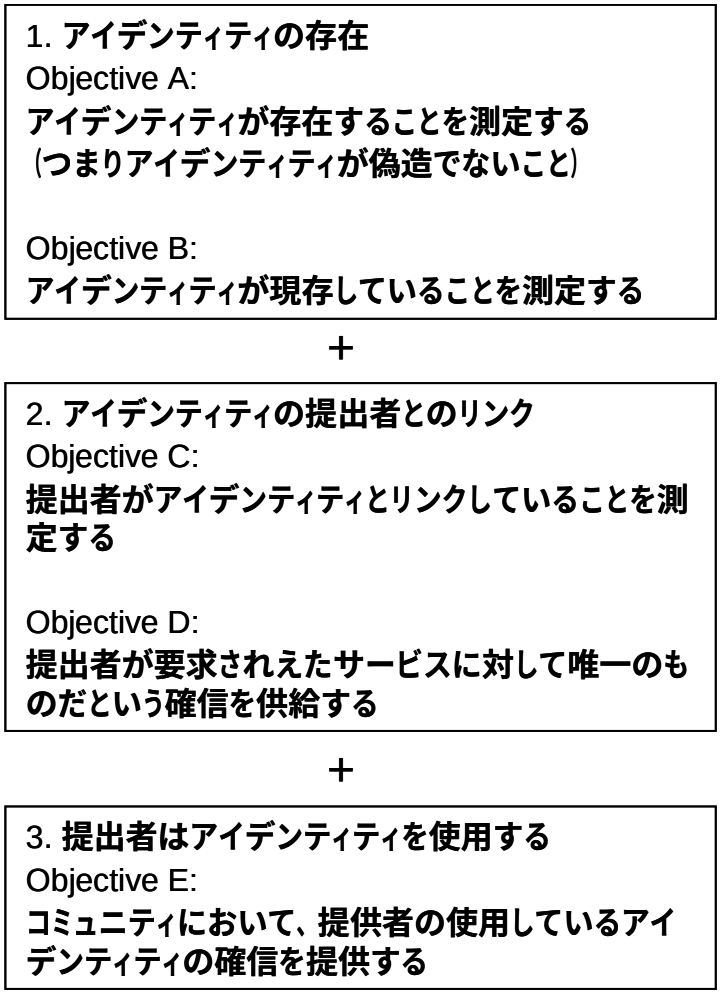


図 4−4　EOI フレームワークの認証コンポーネント

4.11.1. リスク評価と信用レベル

4.11.1.1. リスク評価

全ての取引が EOI での同一のレベルを要求するわけではなく、いくつかは全く要求しない。

取引でのリスクを次の 4 つのカテゴリーに分けることができる（本フレームワークでは最後の 2 つにだけ適用される）

- カテゴリー 0：人が特定されるのを必要としない匿名のサービス/取引
- カテゴリー 1：人が特定されるのを必要としない偽名のサービス/取引、しかし連絡先は必要とする
- カテゴリー 2：人が明確に特定されるのを必要とする認証されたサービス/取引
- カテゴリー 3:人が明確に特定されるのを必要とする検証されたサービス/取引、さらに認証データも検証される

4.11.1.2. 信用レベルの選択

一般的に、

- 信用レベルＡのプロセスは、カテゴリー 2 の取引に適用される
- 信用レベルＢのプロセスは、カテゴリー 3 の取引に適用される

取引が EOI を必要とするかどうか（つまり、その取引がカテゴリー 2 か 3 に一致しているか）を決定することは比較的簡単である。

しかしながら、それに関係する信用レベルを区別することは、より難しい。ある取引がカテゴリー 3（高リスク）取引かどうかを決定する際、政府機関は例えば次のような質問をする。

- 金融リスクの重大なレベルに関わるか？
- 個人の（例えば健康情報など）機密な情報の流出に関わるか？
- 発行している政府機関に取引リスクが含まれるか？（つまり、他の政府機関が発行したドキュメントでの結果を他の取引の identity 認証としての利用／許可する取引に対して、これは適用される）
- 取引は、個人の健康と安全に対してリスクを及ぼすか？（例えば、保護された個人情報の公開が、個人を危険にさらすことに繋がる取引か？）

4.11.2. identity プロセスの認証

本文書では identity プロセスの認証に関して、以下の事項が示されている。

The tables on the following pages provide guidance on the types of EOI that can be used to meet Confidence Levels A and B.

They cover:

- the objective: the desired results of each component of the EOI process;
- the requirement: the evidence required to achieve the objective; and
- the document or process: the physical evidence or procedures that can be used as evidence of the individual's identity according to the relevant Confidence Level. Appendix 3 provides further information on each of the EOI documents and data sources.

Note that any documents specified in the following pages are original or official documents, not photocopies (verified or otherwise).

＜引用部の訳文＞
以下のページ（表 4-20）は、信用レベル A，B に合致するために使用される EOI のタイプについて提供している。
それらは、次のことが網羅されている。

- Objective：EOI プロセスのそれぞれのコンポーネントでの望ましい結果
- 要件：Objective を成し遂げるための認証用件
- ドキュメントやプロセス：適切な信用レベルに関する個人 identity の認証として使用される物理的認証や手続き。Appendix 3 でそれぞれの EOI ドキュメントやデータソースに関する更なる情報を提供している。

以下のページで指定されているどんなドキュメントも（照合したものやその他のものの）コピーではなく、オリジナルで公式なドキュメントであることに注意をする。

表 4-20　Objective A

コンポーネント 1：identity の存在		
Objective A：アイデンティティが存在することを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
その人が生まれていることの認証 **要件：** ・ （出生から現在までの）オリジナルな名前を認証 ・ 誕生日を認証 ・ 出生地を認証 ・ 出身国の認証	**本 Objective を満たすためのオプション：** 完全な出生記録の提示 **and/or** パスポートの提示 **and/or** 銃器取扱いライセンスの提示 **and/or** ニュージーランド市民証明書の提示 **and/or** identity 証明書の提示 **and/or** 難民旅券文書の提示	**本 Objective を満たすためのオプション：** **Either** 個人から同意を得て、主要なデータの管理人へ検証を要求する **or** 完全な出生記録の提示とドキュメントが本物だと検証する **and/or** パスポートの提示とドキュメントが本物だと検証する **and/or** 銃器取扱いライセンスの提示とドキュメントが本物だと検証する **and/or** ニュージーランド市民証明書の提示とドキュメントが本物だと検証する

表 4-21　Objective B

コンポーネント 1：identity の存在		
Objective B：アイデンティティが現存していることを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
その人が死亡していないことを認証	**Objective 2C を満たしている限り、この objective においてプロセスは要求されない**	**本 Objective を満たすためのオプション：** **Either** 信頼された保証人に、主張された identity（つまりサービスに申し込んでいる人）が持ち主の identity かを検証させる **or** 以下の何れかを用いて、現れている人が申請者であることを要求 ・ 信頼された保証人によって写真の検証 ・ パスポート ・ identity の証明書 ・ 難民旅券文書 **or** ニュージーランドの死亡登録を用いて主張された identity が死亡記録に入っていないことを検証する。（海外で死亡した人については、死亡記録の登録は必要はないことを注意すること。）

表 4-22　Objective C

コンポーネント 2：identity の提出者とのリンク		
Objective C：提出者が idnetity とリンクしていることを測定する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
物理的に提出した人が主張された identity とリンクしているかを認証	**本 Objective を満たすためのオプション：** **Either** 信頼された保証人によって検証された人の写真と、申請者 **or** 信頼された保証人によって検証された申請者の写真の提示 **or** パスポートの提示と、サービスへの申請者とパスポートの人が同じであることを保証人が検証（両方） **or** 銃器取扱いライセンスの提示と、サービスへの申請者とライセンスの人が同じであることを保証人が検証（両方） **or** 運転免許証の提示と、サービスへの申請者と運転免許証の人が同じであることを保証人が検証（両方）	**本 Objective を満たすためのオプション：** 認証レベル A の要件と次のプロセス **and** 検証のために申請者と保証人の両方によって提供された詳細を、信頼された保証人に連絡する

表 4-23　Objective D

コンポーネント 2：identity の提出者とのリンク		
Objective D：提出者が要求されたサービスに対して唯一の者だという確信を提供する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
他の人が、サービスへのアクセスのために主張された identity を持っていないことを認証する	**サービス提供機関のデータベースをチェックする**	**サービス提供機関のデータベースをチェックする**

表 4-24　Objective E

コンポーネント 3：提出者は identity を使用する		
Objective E：コミュニティにおいて、提出者の使用している identity の確信を提供する		
要件	ドキュメントやプロセス	
	信用レベル　A	信用レベル　B
コミュニティでの identity の利用を認証する **and** 現在か以前に使用された他の名前が、オリジナルの名前とリンクするかを認証する	もし可能であれば、名前のどのような変更についても公的な認証を提示する（例えば、結婚証明や法的な証明） **and** 次のうち少なくとも 1 つのコミュニティ利用認証の提示 ・ 運転免許証 ・ コミュニティサービスカード ・ 名前・住所・ＩＲＤナンバーがある、ＩＲＤ statement（ＩＲＤ：Inland Revenue Department） ・ 選挙人名簿登録の詳細 ・ 名前と住所の詳細を含む有効的な明細書（例えば、電話や電気） ・ 名前と住所の詳細を含む経済的な明細書 ・ 銀行カード ・ 学生ＩＤや社員ＩＤカード	もし可能であれば、名前のどのような変更についても公的な認証を提示する（例えば、結婚証明や法的な証明） **and** コミュニティでの identity の個人利用について信頼された保証人によって検証ｓれる **and** 次のうち少なくとも 2 つのコミュニティ利用認証の提示 ・ 運転免許証 ・ コミュニティサービスカード ・ 名前・住所・ＩＲＤナンバーがある、ＩＲＤ statement（ＩＲＤ：Inland Revenue Department） ・ 選挙人名簿登録の詳細 ・ 名前と住所の詳細を含む有効的な明細書（例えば、電話や電気）

	ード ・ Steps to Freedom form	・ 名前と住所の詳細を含む明細書 ・ 銀行カード ・ 学生ＩＤや社員ＩＤカード ・ Steps to Freedom form

4.11.3. 目的

本文書の目的として、以下の事項が示されている。

The Framework has been developed for New Zealand's government sector, primarily for agencies to apply when carrying out high-risk transactions with members of the public. It may also be applied to recruitment within agencies where the position being recruited to is of high-risk. Likewise, the Framework could also be helpful to organisations outside the government sector in determining the accuracy, and benefits or limitations of, different government-issued documents (as described in Appendix 3).

＜引用部の訳文＞

本フレームワークは、ニュージーランドの政府部門のために作成されたものであり、主として政府機関が公共のメンバーと高リスクの取引を行う際に適用されるものである。また、新規雇用が高リスクの位置をしめる政府機関での雇用にも適用されるかもしれない。同様にまた、政府部門外の組織が、異なる政府が発行した（Appendix 3 で述べる）文書における利益や制限の正確さを判断する際にも、フレームワークは役立つだろう。

4.11.4. 利用者

本文書の利用者として、以下の事項が示されている。利用対象者は、大多数の人々である。未成年者や認証サービス等へアクセスできない人は除いている。

The vast majority of individuals will be able to meet the EOI requirements, outlined in this Framework.

Exceptions include, for example, minors or people who cannot access the required evidence from their country of origin or where the emergency nature of a particular service makes it inappropriate to require individuals to meet the EOI requirements.

In cases like these, the Framework objectives should still be pursued where possible, but alternative EOI sources will be required. Agencies will need to apply discretion, just as they do currently.

＜引用部の訳文＞

大多数の個人は本フレームワークで概説された EOI 要件を満たしているだろう。

例外は、例えば未成年者や、要求されている証拠のうち出身国から出ているものを得られない人々、または特定のサービスの突発的に事情によって、個人への EOI 要件の適用が不適切な場合である。

これらのような場合でも本フレームワークの目標は可能な場面では追求されるべきだが、代替の EOI の情報源が必要とされるだろう。政府機関は、現在実行しているのと同様の裁量が必要であるだろう。

4.11.5. 利用方法の想定

次の図 4−5 は EOI フレームワークの利用工程である。特定のトランザクションに関して政府機関が本フレームワークを必要としているかどうかを視覚的に案内しているもので、本フレームワークをどのように使用すべきかが記されている。

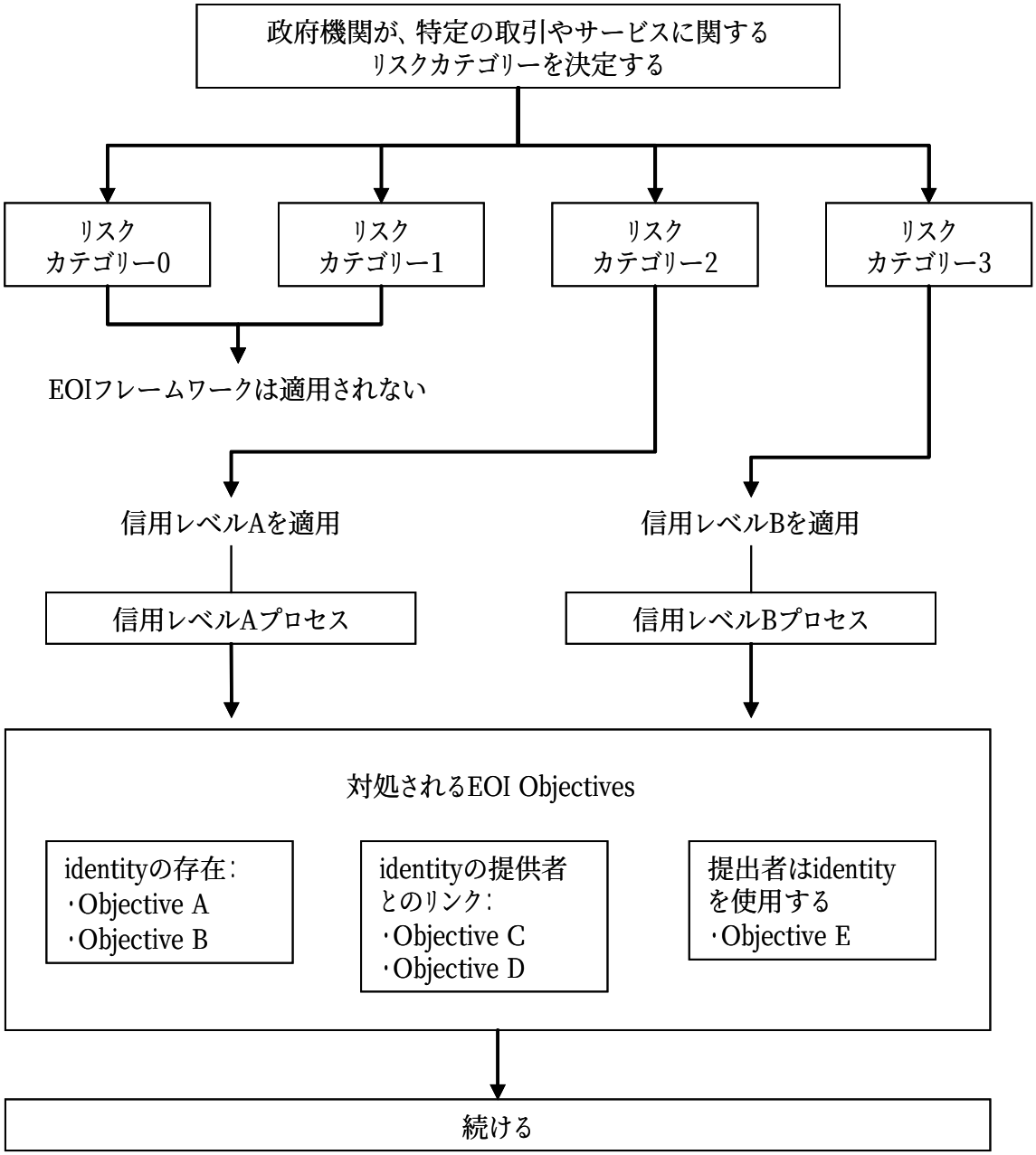


図 4−5　EOI フレームワーク利用工程

4.11.5.1. 本フレームワークの限定

EOI プロセスでも詐欺行為はありうる；結果を保証するものは扱いにくいので、（個人情報の過度な要求や政府機関の実施コストといった）コストは利益よりも優先される。

しかしながらフレームワークの目標を満たすことは、便宜主義的な者が単純な identity 詐欺行為や盗難に陥るリスクを軽減させると考えられる。例えば、信頼された証明書の検証における本フレームワークの要件は、存在しない保証人のサインの偽造のリスクを低減させるだろう。

4.11.5.2. identity ドキュメントの証拠

政府機関が自身の要件としてどの程度の頻度で関連ドキュメントを発行しておくべきかを、本フレームワークが規定しているわけではない。しかしながら、事例としては次のようなものを要求することが挙げられる。

- 現在のドキュメント（法的には、これに対する例外を規定するかもしれないが）
- “ コミュニティ（フレームワークでの Objective 3.E）における identity の使用 ” の証拠のため、（現在の使用を示すために）６ヶ月前までに発行された証拠と（長期に渡って個人により使用された identity と示すために）それ以前に発行された証拠のうち少なくとも１つのソース

もし個人の EOI（例えば、ニュージーランドで発行されなかったドキュメントや評判が傷つけられているドキュメントなど）に確信が持てない又はある個人が信用レベル B の要件を満たすことができないならば、政府機関は注意をし更なる協力的な認証を要求するべきである。

4.11.5.3. identity 情報の証拠管理

本フレームワークが強固な EOI プロセスのための good practice ガイドであるが、本フレームワークは、identity 情報の収集、保存、セキュリティの確保のために必要な内部プロセスについては対象としない。（ただし、Privacy 条例に関わるところは例外とする。）

フレームワークの成功は、EOI プロセスの管理のために効果的な社内手続を政府機関が持ち合わせることにある。弱い繋がりには次のことを含む。

- 内部での詐欺によるリスク
- セキュアでないシステム

- いい加減な処理標準
- いい加減な内部統制
- 最前線のスタッフに対する適切な危機認識トレーニングの不足

identity の潜在的詐欺や盗難を示している EOI を受け取った政府機関は、それらのプロシジャーに従い、適切な当局へ警告を発するべきである。もし、EOI の特定のフォームが変更されたり誤用されたりした場合には、（フレームワークを出した）政府機関は可能な限りアドバイスをするべきである。

4.11.6. 運用方法

上記の本フレームワーク利用方法の想定に含まれる。

4.11.7. 特徴

本フレームワークを作成する際、その他海外の政府電子認証モデルを参照した。それらのモデルをニュージーランドに則した形に変更したものである。

また、認証には住所や名前、運転免許証を必要とするので、基本的には人の認証のみを扱っている。

略称 Appendix

1. 本文中で用いている略称の正式表記

BCP	Best Current Practice
BCP	Business Continuity Plan（業務継続計画）
CA	Certification Authority（認証局）
CP	Certificate Policy（認証局証明書ポリシー）
CPS	Certification Practice Statement（認証業務規定）
CRL	Certificate Revocation List（証明書失効リスト）
CSP	Credential Service Provider
EAP	Electronic Authentication Partnership
EE	End Entity
EOI	Evidence of Identity
GPKI	Governmnent Public Key Infrastructure（政府認証基盤）
IDA	Interchange of Data between Administrations
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
ML	Mailing List（メーリングリスト）
OCSP	Online Certificate Status Protocol
OID	Object ID（オブジェクト ID）
PKI	Public Key Infrastructure（公開鍵基盤）

RA	Registration Authority（登録局）
RFC	Request For Comments
SAC	Service Assessment Criteria
SNS	Social Network Service
SSL	Secure Sockets Layer
WG	Working Group

表 4-1　海外における電子認証に関わる既存ガイドラインの例

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
E-Authentication Guidance for Federal Agencies―（米国）	政府機関における個人認証において適切な保証レベルを提供すること。	連邦政府関係機関	政府機関が本文書に従って保証レベルを決定することを求める。	実施日以降の一定期限内に各機関による保証レベルの設定を規定。	4 段階の保証レベルを規定。個人の身元認証と属性認証を扱うが、サーバ認証等は対象外。
Registration and Authentication ― e-Government Strategy Framework Policy and Guidelines ―（英国）	電子政府の transaction における登録と認証についての保証レベルを定めること。	電子政府サービスの入手や提供をするもの。	政府が取引相手の本人性と権限を信頼し、プライバシーや機密性の侵害、データの盗難／不正使用、その他の危害が存在しないことを確保することが必要な場合。	特に記述されていない。	中央政府省庁および政府機関は、電子取引に関して本フレームワークを満たさなければならない。
Australian Government Electronic Authentication Framework ― （オーストラリア）	政府機関が認証方法について意思決定する場合に、必ず一貫した方法が適用されるようにし、政府機関が取引の際のリスクレベルに対応した認証手段を実施することを保証する。	政府機関と企業。	政府と企業間で認証が必要となる取引において、記載されている手順を参照する。	サービスの増加に伴い、ユーザ認証方法を換え、フレームワークも更新する。	オーストラリア政府の電子認証フレームワークの公開草案であり、この草案に対する意見を募っている。

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
Authentication for e-government Best Practice Framework for Authentication — （ニュージーランド）	政府機関での認証分野におけるガイドラインを提供すること。	オンライン認証プロジェクトの計画に関わる人、または要件決定を行なう人。	電子政府サービスの中でも特に認証が必要なサービスを構築する際に利用される。	認証技術と実践の変化、オンライン認証の戦略的方向性に関する政府の意思決定を反映されるため、本フレームワークは定期的に改訂される。	電子認証の実装方法について詳細に述べており、また製品やサービス選択に関する助言も含まれる。
Interchange of Data between Administrations (IDA) Authentication Policy — （EU）	IDA 認証ポリシーの定義を行なうこと。	IDA Sectoral Network で遠隔認証を必要とするもの	Sectoral Project Authentication Policy を作成する際に利用される。	特になし。	このドキュメントは、フレームワーク規約 ENTR/01/67-CONSEC の下で準備されたもの。また、米国の E-Authentication Guidance for Federal Agencies と似ている部分が多数ある。人の認証のみを扱っている。

海外ガイドライン	目的	利用者	利用方法の想定	運用方法	特徴
TRUST FRAMEWORK —（米国）	Electronic Authentication Partnership（EAP）運用および利用に関するフレームワーク作り。	EAP システムに参加する全ての人々	CSP（クレデンシャル・サービス・プロバイダー）が、EAP 認定アセスメント機関によるアセスメントを無事完了することができるために利用する。	EAP は、このビジネス・ルールを公式化するものとし、これを定期的に修正することができる。	各信頼当事者と CSP は、EAP システムへの参加の前提条件として、このビジネス・ルールによって制約されていることに同意しなければならない。
EVIDENCE OF IDENTITY FRAMEWORK —（ニュージーランド）	政府機関と公共のメンバーが高リスクの取引を行う場合のフレームワークを提供する。	大多数の人々。未成年者や認証サービスへアクセスできない人を除く。			人の認証のみを扱っている。例えば、認証時に写真による検証を行なう等。

2. IETF における Best Current Practice の一覧

表A－1　現在有効なBest Current Practiceの一覧[1]

BCP番号	標題	作成者	発行時期	バイト数	備考
3	Variance for The PPP Compression Control Protocol and The PPP Encryption Control Protocol.	F. Kastenholz.	Feb-96	14347	(Also RFC1915)
4	An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA.	P. Nesser II.	Feb-96	23623	(Also RFC1917)
5	Address Allocation for Private Internets.	Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear.	Feb-96	22270	(Obsoletes RFC1627, RFC1597) (Also RFC1918)
6	Guidelines for creation, selection, and registration of an Autonomous System (AS).	J. Hawkinson, T. Bates.	Mar-96	22073	(Also RFC1930)
7	Implications of Various Address Allocation Policies for Internet Routing.	Y. Rekhter, T. Li.	Oct-96	34717	(Also RFC2008)
8	IRTF Research Group Guidelines and Procedures. A. Weinrib,	J. Postel.	Oct-96	27507	(Also RFC2014)

[1] 本表の内容はRFC Editorより下記にて公開されている 2006 年 2 月 26 日時点の内容に基づく。
BCP INDEX
ftp://ftp.rfc-editor.org/in-notes/bcp-index.txt

BCP番号	標題	作成者	発行時期	バイト数	備考
9	The Internet Standards Process -- Revision 3.	S. Bradner.	Oct-96	86731	(Obsoletes RFC1602, RFC1871) (Updated by RFC3667, RFC3668, RFC3932, RFC3979, RFC3978) (Also RFC2026)
10	IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees.	J. Galvin, Ed..	Jun-04	76395	(Obsoletes RFC2727) (Also RFC3777)
11	The Organizations Involved in the IETF Standards Process.	R. Hovey, S. Bradner.	Oct-96	13865	(Updated by RFC3668, RFC3979) (Also RFC2028)
12	Internet Registry IP Allocation Guidelines. K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg,	J. Postel.	Nov-96	28975	(Obsoletes RFC1466) (Also RFC2050)
13	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures.	N. Freed, J. Klensin.	Dec-05	74243	(Obsoletes RFC2048) (Also RFC4288, RFC4289)
14	Key words for use in RFCs to Indicate Requirement Levels.	S. Bradner.	Mar-97	4723	(Also RFC2119)
15	Deployment of the Internet White Pages Service.	H. Alvestrand, P. Jurg.	Sep-97	31539	(Also RFC2148)
16	Selection and Operation of Secondary DNS Servers.	R. Elz, R. Bush, S. Bradner, M. Patton.	Jul-97	27456	(Also RFC2182)
17	Use of DNS Aliases for Network Services.	M. Hamilton, R. Wright.	Oct-97	17858	(Also RFC2219)
18	IETF Policy on Character Sets and Languages.	H. Alvestrand.	Jan-98	16622	(Also RFC2277)
19	IANA Charset Registration Procedures.	N. Freed, J. Postel.	Oct-00	21615	(Obsoletes RFC2278) (Also RFC2978)

BCP番号	標題	作成者	発行時期	バイト数	備考
20	Classless IN-ADDR.ARPA delegation.	H. Eidnes, G. de Groot, P. Vixie.	Mar-98	17744	(Also RFC2317)
21	Expectations for Computer Security Incident Response.	N. Brownlee, E. Guttman.	Jun-98	86545	(Also RFC2350)
22	Guide for Internet Standards Writers.	G. Scott.	Jun-98	47280	(Also RFC2360)
23	Administratively Scoped IP Multicast.	D. Meyer.	Jul-98	17770	(Also RFC2365)
24	RSVP over ATM Implementation Guidelines.	L. Berger.	Aug-98	15174	(Also RFC2379)
25	IETF Working Group Guidelines and Procedures.	S. Bradner.	Sep-98	62857	(Obsoletes RFC1603) (Updated by RFC3934) (Also RFC2418)
26	Guidelines for Writing an IANA Considerations Section in RFCs.	T. Narten, H. Alvestrand.	Oct-98	25092	(Updated by RFC3692) (Also RFC2434)
27	Advancement of MIB specifications on the IETF Standards Track.	M. O'Dell, H. Alvestrand, B. Wijnen, S. Bradner.	Oct-98	13633	(Also RFC2438)
28	Enhancing TCP Over Satellite Channels using Standard Mechanisms.	M. Allman, D. Glover, L. Sanchez.	Jan-99	47857	(Also RFC2488)
29	Procedure for Defining New DHCP Options.	R. Droms.	Jan-99	10484	(Obsoleted by RFC2939) (Also RFC2489)
30	Anti-Spam Recommendations for SMTP MTAs.	G. Lindberg.	Feb-99	53597	(Also RFC2505)
31	Media Feature Tag Registration Procedure.	K. Holtman, A. Mutz, T. Hardie.	Mar-99	24892	(Also RFC2506)
32	Reserved Top Level DNS Names.	D. Eastlake 3rd, A. Panitz.	Jun-99	8008	(Also RFC2606)
33	URN Namespace Definition Mechanisms.	L. Daigle, D. van Gulik, R. Iannella, P. Falstrom.	Jun-99	26916	(Obsoleted by RFC3406) (Also RFC2611)
34	Changing the Default for Directed Broadcasts in Routers.	D. Senie.	Aug-99	6820	(Updates RFC1812) (Also RFC2644)

BCP番号	標題	作成者	発行時期	バイト数	備考
35	Registration Procedures for URL Scheme Names.	R. Petke, I. King.	Nov-99	19780	(Obsoleted by RFC4395) (Also RFC2717)
36	Guidelines for Writers of RTP Payload Format Specifications.	M. Handley, C. Perkins.	Dec-99	24143	(Also RFC2736)
37	IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers.	S. Bradner, V. Paxson.	Mar-00	18954	(Also RFC2780)
38	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.	P. Ferguson, D. Senie.	May-00	21258	(Obsoletes RFC2267) (Updated by RFC3704) (Also RFC2827)
39	Charter of the Internet Architecture Board (IAB).	Internet Architecture Board, B. Carpenter, Ed..	May-00	15984	(Obsoletes RFC1601) (Also RFC2850)
40	Root Name Server Operational Requirements.	R. Bush, D. Karrenberg, M. Kosters, R. Plzak.	Jun-00	21133	(Obsoletes RFC2010) (Also RFC2870)
41	Congestion Control Principles.	S. Floyd.	Sep-00	43823	(Also RFC2914)
42	Domain Name System (DNS) IANA Considerations.	D. Eastlake 3rd, E. Brunner-Williams, B. Manning.	Sep-00	22454	(Also RFC2929)
43	Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types.	R. Droms.	Sep-00	13631	(Obsoletes RFC2489) (Also RFC2939)
44	Use of HTTP State Management.	K. Moore, N. Freed.	Oct-00	18899	(Also RFC2964)
45	IETF Discussion List Charter.	S. Harris.	Nov-00	5682	(Also RFC3005)
46	Recommended Internet Service Provider Security Services and Procedures.	T. Killalea.	Nov-00	27905	(Also RFC3013)
47	Tags for the Identification of Languages.	H. Alvestrand.	Jan-01	26522	(Obsoletes RFC1766) (Also RFC3066)

BCP番号	標題	作成者	発行時期	バイト数	備考
48	End-to-end Performance Implications of Slow Links.	S. Dawkins, G. Montenegro, M. Kojo, V. Magret.	Jul-01	39942	(Also RFC3150)
49	Delegation of IP6.ARPA.	R. Bush.	Aug-01	5727	(Obsoleted by RFC3596) (Updates RFC2874, RFC2772, RFC2766, RFC2553, RFC1886)(Also RFC3152)
50	End-to-end Performance Implications of Links with Errors.	S. Dawkins, G. Montenegro, M. Kojo, V. Magret, N. Vaidya.	Aug-01	36388	(Also RFC3155)
51	IANA Guidelines for IPv4 Multicast Address Assignments.	Z. Albanna, K. Almeroth, D. Meyer, M. Schipper.	Aug-01	15389	(Also RFC3171)
52	Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa").	G. Huston, Ed..	Sep-01	18097	(Also RFC3172)
53	GLOP Addressing in 233/8.	D. Meyer, P. Lothberg.	Sep-01	8225	(Obsoletes RFC2770) (Also RFC3180)
54	IETF Guidelines for Conduct.	S. Harris.	Oct-01	7413	(Also RFC3184)
55	Guidelines for Evidence Collection and Archiving.	D. Brezinski, T. Killalea.	Feb-02	18468	(Also RFC3227)
56	On the use of HTTP as a Substrate.	K. Moore.	Feb-02	34785	(Also RFC3205)
57	IANA Considerations for IPv4 Internet Group Management Protocol (IGMP).	B. Fenner.	Feb-02	6473	(Also RFC3228)
58	Defining the IETF.	P. Hoffman, S. Bradner.	Feb-02	6401	(Also RFC3233)
59	A Transient Prefix for Identifying Profiles under Development by the Working Groups of the Internet Engineering Task Force.	M. Rose.	Jul-02	7916	(Also RFC3349)

BCP番号	標題	作成者	発行時期	バイト数	備考
60	Inappropriate TCP Resets Considered Harmful.	S. Floyd.	Aug-02	46748	(Also RFC3360)
61	Strong Security Requirements for Internet Engineering Task Force Standard Protocols.	J. Schiller.	Aug-02	16411	(Also RFC3365)
62	Advice to link designers on link Automatic Repeat reQuest (ARQ).	G. Fairhurst, L. Wood.	Aug-02	66097	(Also RFC3366)
63	Session Initiation Protocol for Telephones (SIP-T): Context and Architectures.	A. Vemuri, J. Peterson.	Sep-02	49893	(Also RFC3372)
64	Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP).	K. Zeilenga.	Sep-02	45893	(Also RFC3383)
65	Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures.	M. Mealling.	Oct-02	19469	(Also RFC3405)
66	Uniform Resource Names (URN) Namespace Definition Mechanisms.	L. Daigle, D. van Gulik, R. Iannella, P. Faltstrom.	Oct-02	43707	(Obsoletes RFC2611) (Also RFC3406)
67	Change Process for the Session Initiation Protocol (SIP).	A. Mankin, S. Bradner, R. Mahy, D. Willis, J. Ott, B. Rosen.	Dec-02	26234	(Updated by RFC3968, RFC3969) Also RFC3427)
68	Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update.	W. Townsley.	Dec-02	9135	(Also RFC3438)
69	TCP Performance Implications of Network Path Asymmetry.	H. Balakrishnan, V. Padmanabhan, G. Fairhurst, M. Sooriyabandara.	Dec-02	108839	(Also RFC3449)
70	Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols.	S. Hollenbeck, M. Rose, L. Masinter.	Jan-03	64252	(Also RFC3470)

BCP番号	標題	作成者	発行時期	バイト数	備考
71	TCP over Second (2.5G) and Third (3G) Generation Wireless Networks.	H. Inamura, Ed., G. Montenegro, Ed., R. Ludwig, A. Gurtov, F. Khafizov.	Feb-03	61528	(Also RFC3481)
72	Guidelines for Writing RFC Text on Security Considerations.	E. Rescorla, B. Korver.	Jul-03	110393	(Also RFC3552)
73	An IETF URN Sub-namespace for Registered Protocol Parameters.	M. Mealling, L. Masinter, T. Hardie, G. Klyne.	Jun-03	14815	(Also RFC3553)
74	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.	R. Frye, D. Levi, S. Routhier, B. Wijnen.	Aug-03	115222	(Obsoletes RFC2576) (Also RFC3584)
75	Session Initiation Protocol (SIP) Basic Call Flow Examples.	A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers.	Dec-03	163159	(Also RFC3665)
76	Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows.	A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers.	Dec-03	200478	(Also RFC3666)
77	IETF ISOC Board of Trustee Appointment Procedures.	L. Daigle, Ed., Internet Architecture Board.	Dec-03	13008	(Also RFC3677)
78	IETF Rights in Contributions.	S. Bradner, Ed..	Mar-01-05	43574	(Obsoletes RFC3667) (Updates RFC2026) (Also RFC3978)
79	Intellectual Property Rights in IETF Technology.	S. Bradner, Ed..	Mar-01-05	41366	(Obsoletes RFC3668) (Updates RFC2026, RFC2028) (Also RFC3979)
80	Delegation of E.F.F.3.IP6.ARPA.	R. Bush, R. Fink.	Jan-04	7137	(Also RFC3681)

BCP番号	標題	作成者	発行時期	バイト数	備考
81	The IETF XML Registry.	M. Mealling.	Jan-04	17325	(Also RFC3688)
82	Assigning Experimental and Testing Numbers Considered Useful.	T. Narten.	Jan-04	15054	(Updates RFC2434) (Also RFC3692)
83	A Practice for Revoking Posting Rights to IETF Mailing Lists.	M. Rose.	Mar-04	15698	(Also RFC3683)
84	Ingress Filtering for Multihomed Networks.	F. Baker, P. Savola.	Mar-04	35942	(Updates RFC2827) Also RFC3704)
85	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP).	J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo.	Apr-04	77308	(Also RFC3725)
86	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys.	H. Orman, P. Hoffman.	Apr-04	55939	(Also RFC3766)
87	Use of Interior Gateway Protocol (IGP) Metric as a second MPLS Traffic Engineering (TE) Metric.	F. Le Faucheur, R. Uppili, A. Vedrenne, P. Merckx, T. Telkamp.	May-04	17475	(Also RFC3785)
88	IANA Considerations for the Point-to-Point Protocol (PPP).	V. Schryver.	Jun-04	6321	(Also RFC3818)
89	Advice for Internet Subnetwork Designers.	P. Karn, Ed., C. Bormann, G. Fairhurst, D. Grossman, R. Ludwig, J. Mahdavi, G. Montenegro, J. Touch, L. Wood.	Jul-04	152174	(Also RFC3819)
90	Registration Procedures for Message Header Fields.	G. Klyne, M. Nottingham, J. Mogul.	Sep-04	36231	(Also RFC3864)
91	DNS IPv6 Transport Operational Guidelines.	A. Durand, J. Ihren.	Sep-04	10025	(Also RFC3901)

BCP番号	標題	作成者	発行時期	バイト数	備考
92	The IESG and RFC Editor Documents: Procedures.	H. Alvestrand.	Oct-04	17093	(Updates RFC2026, RFC3710) (Also RFC3932)
93	A Model for IETF Process Experiments.	J. Klensin, S. Dawkins.	Nov-04-04	14409	(Also RFC3933)
94	Updates to RFC 2418 Regarding the Management of IETF Mailing Lists.	M. Wasserman.	Oct-04	8488	(Updates RFC2418) (Also RFC3934)
95	A Mission Statement for the IETF.	H. Alvestrand.	Oct-04	16639	(Also RFC3935)
96	Procedures for Modifying the Resource reSerVation Protocol (RSVP).	K. Kompella, J. Lang.	Oct-04	15314	(Updates RFC3209, RFC2205) (Also RFC3936)
97	Clarifying when Standards Track Documents may Refer Normatively to Documents at a Lower Level.	R. Bush, T. Narten.	Dec-04	12251	(Also RFC3967)
98	The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP).	G. Camarillo.	Dec-04	20615	(Updates RFC3427) (Also RFC3968)
99	The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP).	G. Camarillo.	Dec-04	12119	(Updates RFC3427) (Also RFC3969)
100	Early IANA Allocation of Standards Track Code Points.	K. Kompella, A. Zinin.	Feb-22-05	13706	(Also RFC4020)
101	Structure of the IETF Administrative Support Activity (IASA).	R. Austein, Ed., B. Wijnen, Ed., B. Carpenter, Ed., L. Lynch, Ed..	Jan-06	55589	(Also RFC4071, RFC4371)
102	IAB Processes for Management of IETF Liaison Relationships.	L. Daigle, Ed., Internet Architecture Board.	Apr-25-05	18360	(Also RFC4052)

BCP番号	標題	作成者	発行時期	バイト数	備考
103	Procedures for Handling Liaison Statements to and from the IETF.	S. Trowbridge, S. Bradner, F. Baker.	Apr-25-05	38816	(Also RFC4053)
104	Terminology for Describing Internet Connectivity.	J. Klensin.	May-11-05	24522	(Also RFC4084)
105	Embedding Globally-Routable Internet Addresses Considered Harmful.	D. Plonka.	Jun-05	22656	(Also RFC4085)
106	Randomness Requirements for Security.	D. Eastlake, 3rd, J. Schiller, S. Crocker.	Jun-03-05	114321	(Obsoletes RFC1750) (Also RFC4086)
107	Guidelines for Cryptographic Key Management.	S. Bellovin, R. Housley.	Jun-05	14752	(Also RFC4107)
108	IP Performance Metrics (IPPM) Metrics Registry.	E. Stephan.	Aug-05	23074	(Also RFC4148)
109	Deprecation of "ip6.int"	G. Huston.	Aug-05	5353	(Also RFC4159)
110	Tunneling Multiplexed Compressed RTP (TCRTP).	B. Thompson, T. Koren, D. Wing.	Nov-05	48990	(Also RFC4170)
111	Guidelines for Authors and Reviewers of MIB Documents.	C. Heard, Ed..	Sep-05	102521	(Also RFC4181)
112	Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance.	G. Choudhury, Ed..	Oct-05	34132	(Also RFC4222)
113	The IETF Administrative Oversight Committee (IAOC) Member Selection Guidelines and Process.	G. Huston, Ed., B. Wijnen, Ed..	Dec-05	15396	(Also RFC4333)
114	BGP Communities for Data Collection.	D. Meyer.	Feb-06	26078	(Also RFC4384)
115	Guidelines and Registration Procedures for New URI Schemes.	T. Hansen, T. Hardie, L. Masinter.	Feb-06	31933	(Obsoletes RFC2717, RFC2718) (Also RFC4395)

第 5 章　電子認証フレームワークのあり方

内容

- ガイドラインのターゲット
- ガイドラインの提示すべき内容
- ガイドラインの策定と維持管理のあり方
- ガイドライン策定に際して留意すべき事項

5. 電子認証フレームワークのあり方

本章では前章で示した問題意識のもと、電子認証フレームワークの中での BCP の位置づけにおいて日本国内で策定すべきガイドラインの要件について検討する。

5.1. ガイドラインのターゲット

ガイドラインの外形的要素として、対象、用途、想定利用者などのターゲットについての望ましいあり方について議論する。

5.1.1. ガイドラインの対象

電子署名については法制度が整備されつつある。従って電子認証と同様にガイドラインへのニーズは共に高いと考えられるが、電子署名には PKI の検証者がユーザ側に存在し、信頼性の構造は電子認証に比べて若干複雑である。そこで当面のターゲットは電子署名を除き、ノウハウが溜まりやすい分野を対象とする。

また、電子書名は長期保存についても考慮すべき点が通常の電子認証とは大きく異なり、統一的に扱うことが難しいことから、長期保存についてもターゲットからは除外することが適切と言える。

このほか、ガイドラインの対象とすべきターゲットについて、専門家会合において以下の意見が指摘されている。

- 自然人の領域についてはこれまでに利用されている例が多く、かつ法的な強制の適用が適切でない分野であり、ベストプラクティスに基づくガイドラインを適用することが望ましいと言える。
- レベルの高い保証レベルにおいては、ボトムアップに基づくベストプラクティスといった弱い縛りによるものは運用上の高い水準の確保の誘因にはなりにくく、強制力を持った形での適用が必要ではないか。

5.1.2. ガイドラインの用途

電子認証に関しては、現在 PKI を利用してシステムを構築している SI 業者や開発者が短期的な開発方法を繰り返すなどの結果、システムの構築過程において、ベストプラクティスといえる内容がほとんど蓄積されていない状況にある。これは開発の都度試行錯誤を行うことになるため非効率であるだけでなく、情報セキュリティの確立のために必要な要件が見落とされる可能性が高まるなど、社会基盤としての PKI の確立ならびに発展において望ましいことではない。

そこで、ガイドラインに求められる最も重要な役割は、開発者に向けて「有効で目安となる電子認証基盤の使い方」に関する情報を提示することであると考えられる。

5.1.3. ガイドラインの想定利用者

ガイドラインの想定利用者としては、電子認証フレームワークのステークホルダであればそのすべてが対象となりうる。具体的には以下の利用場面が想定される。

- サービスの調達者：電子認証サービスの機能仕様を検討する際に参照する
- サービス構築者：機能仕様をもとに電子認証機能を実装する際に参照する
- サービス提供者の団体・組織：組織間で利用すべき電子認証サービスのあり方を議論する際に参照する

これらはいずれもガイドラインの適用がふさわしい場面であるが、前項におけるガイドラインの用途を想定した場合、想定利用者としてはサービスの構築者および PKI システムの開発者が中心となることが考えられる。

5.1.4. 電子認証フレームワークにおける策定プロセスの位置づけ

前項におけるニーズに対応するための電子認証フレームワークを構築するためにふさわしい策定プロセスのあり方について検討する。

5.1.4.1. 電子認証フレームワーク策定に係る論点

前述した議論を踏まえ、電子認証フレームワークを策定するにあたって検討すべき論点を以下に示す。

（1）　電子認証フレームワークのターゲット

電子認証フレームワークのターゲットとすべき領域について、JPNIC 専門家チームメンバである松本泰氏のアイデアをもとに、以下の３種類の視点を３次元の軸としてとらえ、現在の電子署名・電子認証のターゲットを立体上に投影したもの（発案した松本氏にちなんで「松本キューブ」と呼ばれている）を示す。

- ｘ軸：認証対象（デバイス、サーバ、自然人（その他 、法人、職権なども想定））
- ｙ軸：サービスの種類（電子署名、電子認証、暗号）
- ｚ軸：レベル（低 ←レベル１・２・３・４→ 高）

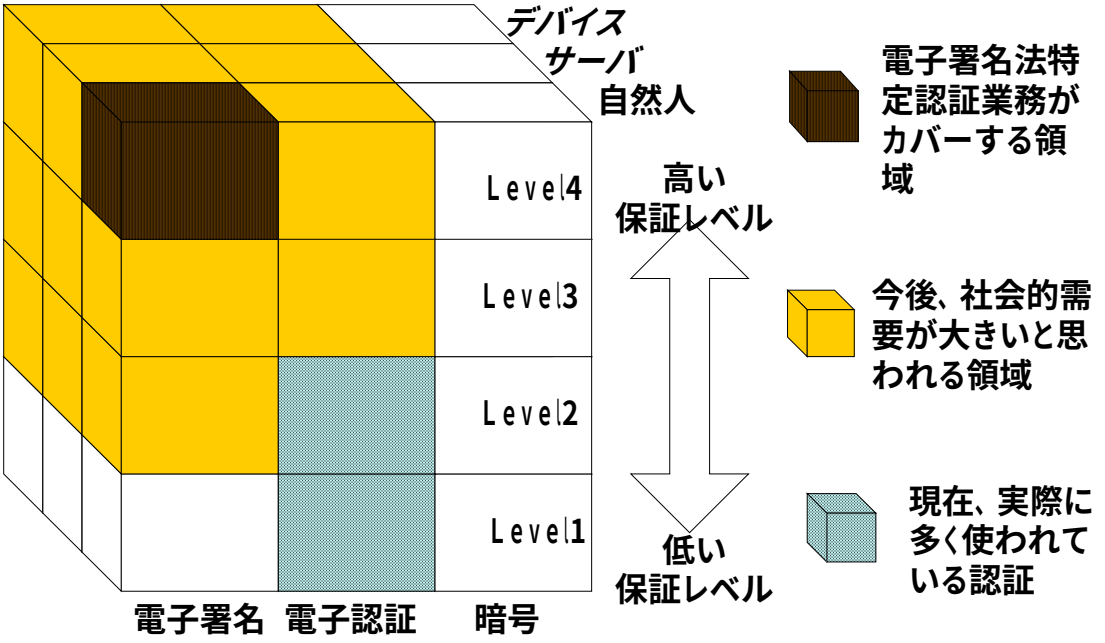


図 5－1　電子認証のターゲットについての図示例（松本キューブ）

この図は現在の電子認証における以下の状況を表象している。

- 電子署名法における特定認証業務でカバーしているのは、電子署名、自然人、レベル４のブロックに相当。
- 現在、実際に多く使われている認証は、電子認証、レベル１～２、自然人のブロックに相当。
- 今後社会的需要が大きいのは、電子署名＋電子認証、レベル２～４、デバイスやサーバの領域と思われる。

（2） 策定主体

電子認証フレームワークの策定主体になるべき組織に対しては、以下の要件が求められる。

- 民間組織であること。これは、民間主導によるフレームワークであることから必須の要件となる。
- 既存の電子認証サービス事業者において、策定主体との関係により事業者間に不公平の生ずることがないこと。

BCP はコンセンサスを基にするため、策定主体となるグループは WG の参加者に相当することになるが、実質的には WG のチェアとなる。

（3） メンテナンス主体

電子認証フレームワークをメンテナンスしていく主体については、策定主体と同一である場合、異なる場合のいずれも想定されるが、要件としては(2)で示したものと同一と考えられる。

5.1.4.2. 電子認証フレームワークを実現させるための策定プロセスのあり方

上述の論点はいずれも重要な課題であり、最適なフレームワークを策定するためには検討すべき事項も多い。ただし、フレームワークを早期に導入、活用したいというニーズも強く、策定に長時間をかけることはこうしたニーズを損ない、電子認証サービスにおける構築・運用コストやリスクの増大を招く恐れがある。

こうした状況において、ここでは電子認証フレームワークを IETF における BCP として位置づけることの可能性について検討する。

（1） BCP（Best Current Practice）としての策定が適切となる条件

IETF において BCP として公開されているドキュメントには、すでに広く利用されている手続きや規範を扱ったものが多く、ドキュメントの実用的な側面が重視されているが、Informational RFC に位置づけられるドキュメントと異なり IESG（Internet Engineering Steering Group）による承認を経ることによる公共的な性質も持ち合わせている。

こうした BCP として策定することが適切となる条件としては、以下の要素が想定される。

- すでに実践に供されている規範、成功事例がある
  BCP は現行の取りうる方策の中で最善であることが前提であるため、電子認証フレームワークで規定される内容はいずれも実践に供され、成功事例といえる成果を得ていることが求められる。
- 内容をあらかじめ最適化することが困難
  最適化することが可能な方策の場合は、BCP という手法をとらなくとも、当初から最適案で合意形成が可能なことが多い。

（2） BCP（Best Current Practice）としての策定することによる利点

BCP として策定することによる利用者への利点としては、以下が挙げられる。

- スピーディーな提供が可能
  既存の実践例をもとにドキュメント化し、関係者の合意を得た上で公開する手続きとなるため、新たに根本から方法を議論する場合と比較して策定に必要な期間が短い。
- 分野を超えた利用が可能
  BCP としての位置づけを与えることで、何らかの分野の中で適用可能な BCP があれば、分野に拘ることなくその成果を相互利用できるメリットを期待することが可能となる。

（3） BCP が成立するための条件

電子認証フレームワークを BCP として策定する方法には(2)で示したような利点がある反面、これを成立させるために以下のような条件を満足させる必要がある。

- 成功事例が存在していること
  BCP は現状におけるベストプラクティスとしての意味づけをもつため、ここに盛り込まれる内容については、これまでの実践において成功を得た事例が存在する必要がある。ただし、これはフレームワークにおいて想定しているターゲットと同一である必要はなく、今回の例であれば海外の同様のドキュメントなどを参考にすることで条件を満たすことも可能である。
- 想定ターゲットとなるフレームワークの利用者が策定プロセスに参加もしくは委任すること
  BCP の公正性、客観性等は策定メンバーの構成と策定プロセスの公開によって保証されることになるため、策定に際しては想定ターゲットとなるフレームワークの利用者が策定プロセスに参加することが望ましい。ただし、利用

者が策定プロセスに参加するために必要な知識を持ち合わせているとは限らないため、策定プロセスへの委任を得ることによっても差し支えない。

5.2. ガイドラインの提示すべき内容

ここでは、前項の対象に向けたガイドラインにおいて、「経験上有効で目安となる使い方」の情報として、具体的に提示すべき内容について検討する。

5.2.1. 開発・構築関連

電子認証サービスの開発・構築の際に有効な BCP として、以下の内容を規定することが想定される。

5.2.1.1. 認証の保証レベル

電子認証サービスにおける保証レベル（assurance level）については、海外ではすでに広く利用されているにもかかわらず日本では GPKI（Government Public Key Infrastructure - 政府認証基盤）などを含めても準拠可能なレベルの規定がなく、ガイドラインで提示する内容の中で最も高いニーズがあると考えられるものの１つである。反面前例がないだけに、ガイドラインにおいてその概念について十分な説明を行うことが必要となる。

保証レベルに関してガイドラインにおいて言及すべき内容を、以下に列挙する。なお、ここでは民間用途を想定し、政府認証基盤における保証レベルの扱いについてはガイドラインで定める内容の対象外とする。

（1） 保証レベルの定義

レベルについては認証対象を限定せずに規定する。段階数については、海外との共通性の観点から、４段階程度に分割することが想定される。

2.2 節において示した通り、米国政府による“ E-Authentication Guidance for Federal Agencies ”における保証レベルの区分は下表のようになっている。

表 5－1　"E-Authentication Guidance for Federal Agencies"が定める保証レベル

レベル	保証の程度	定義
1	最低限の保証	正当性への信頼はほとんどまたは全くない
2	低い保証	正当性に対する若干の信頼がある
3	中程度の保証	正当性への信頼は高い
4	高い保証	正当性への信頼は非常に高い

（2） 認証の対象と保証レベルとの対応

(1)で認証対象を限定せずに保証レベルを規定した上で、本項で認証対象との対応関係を検討することで柔軟な適応性を実現する。認証対象としては、以下を想定する。

- 個人
- サーバ
- 機器に割り当てられた IP アドレス

このうち個人認証については、(1)で示した米国政府のガイダンスでは以下の 2 種類の区分を想定している。

- 身元（identity）認証
- 属性認証（例：退役軍人、米国市民、等）

このほか、個人認証については、扱う情報がセンシティブ情報かどうかでさらに細分化することも考慮の対象となる。

（3） 保証レベル決定のための必要作業と手続き

新たな電子認証サービスにおける保証レベルを決定する手順として、以下の項目についての対応方法を定めることが想定される。

- 電子認証サービスに対するリスク評価（リスクアセスメント）の手続き
- 用いるべきリスク分析手法
- 評価結果と保証レベルとの対応づけに関する合意形成プロセス

（4） 既存の制度と補償レベルの対応関係

電子署名法の要件に準拠したシステムなど、一定の情報セキュリティ要件を満たした場合に、自動的に一定の保証レベルを割り当てることについても、保証レベルの検討とあわせて考慮する必要がある。

5.2.1.2. 電子認証サービスで用いる情報システムの要件と保証レベルとの対応づけ

各保証レベルに対応する、電子認証サービスで用いる情報システムにおいてあるべき要件について、以下の観点から整理する。

（1） 本人確認手段

個人を認証する場合、サービス提供事業者が行う本人確認の確認方法と、保証レベルとの対応を定める。

本人確認手段としては、以下の２種類について検討する必要がある。

- 登録時（対面、確認文書、証明者、等）
- サービス利用時（PIN・パスワード、認証デバイス（IC カード、トークン等）、バイオメトリクス等）

策定内容の参考として、EU の“IDA Authentication Policy”が本人確認手段として定めるトークンの例を示す。

表 5－2　保証レベルに応じたトークンの種類

トークンの種類	保証レベル（○＝使用可能、×＝使用不可）			
	1	2	3	4
ハード暗号トークン（認証を必要とするスマートカード等）	○	○	○	○
ソフト暗号トークン（メディアに保存された暗号鍵等）	○	○	○	×
ワンタイムパスワードデバイストークン	○	○	×	×
パスワードまたは PIN トークン（利用者が暗記した文字列）	○	×	×	×

（2） 認証結果の有効期限

認証に成功した結果を、どの程度の期間有効と認めるかの基準について定める。(1)と同様、EU の“ IDA Authentication Policy ”における有効期限の例を示す。

表 5－3　保証レベルに応じた有効期限

有効期限	保証レベル（○＝使用可能、×＝使用不可）			
	1	2	3	4
24 時間	○	×	×	×
12 時間	○	○	×	×
2 時間	○	○	○	×
直ちに	○	○	○	○

（3） システムにおけるアクセス制御措置

電子認証に関わるシステムで利用するサーバにおけるアクセス制御に関する措置との対応関係を定める。アクセス制御方式としては、以下が想定される。

- OS における強制アクセス制御
- 管理者権限の分割・最少化
- デュアルコントロール（複数の管理者の同席を前提とした制御）

（4） システムを構成する機器における認証取得

認証に関わるシステムの構成製品が取得している情報セキュリティ評価・認証制度（ISO/IEC15408 - Common Criteria）の認証レベルとの対応関係を定める。

5.2.1.3. 電子認証サービスのマネジメントと保証レベルとの対応づけ

各保証レベルに対応する、電子認証サービスのマネジメントにおいてあるべき要件について、以下の観点から整理する。

（1） 情報セキュリティマネジメントシステム（ISMS）

各保証レベルに応じた、電子認証サービスにおける情報セキュリティマネジメントシステム（ISMS）についての要件について定める。

（2） セキュリティ監査の方法

各保証レベルに応じた、情報セキュリティ監査として実施すべき要件について定める。

（3） 失効情報の取得と検証

保証レベルに応じた失効情報の扱いについて規定する。なおこの扱いに関して、すでに保証レベルに基づいた運用を行っている米国の Federal PKI においては、低いレベルにおいては失効情報そのものを扱っていないことを考慮し、本ガイドラインにおいても保証レベルにより失効情報の取り扱いの有無を含めた検討を行うものとする。

5.2.1.4. 電子認証サービスの構成要素毎のベストプラクティス

（1） 信頼点（トラストポイント）

信頼点に関しては、相互認証を円滑に実現するなどの視点から共通の規範をベースに提供されていることが望ましい。そこで、RFC3647、RFC4158 の内容などを考慮しつつ、以下に示す項目について提示することで、信頼点の設定に関する共通化を促すものとする

- 証明書検証者への情報提供方法
- 信頼点の認証局の信頼性担保の仕組み

（2） 登録局（RA）

認証局については、以下の内容が想定される。

- 登録局で行うべき業務の内容
- 保証レベルの区分への対応

（3） 証明書

特殊な証明書についての情報提供を行うことが想定される。

- 職権証明書
- 仮名証明書（欧州で利用）

（4） リポジトリ

認証局などが有するリポジトリの相互利用に関して、その整合性を確保するための複製や連携の方法などについて規定することが考えられる。

（5） ユーザ環境

ガイドラインにおいてユーザ環境について規定すべき項目としては、以下が想定される。

- 鍵ペアの運用環境のあり方
- 失効情報の取得と検証

このうち失効情報についてはエンドユーザにおける対応に関して現状で問題点が多いことから、ガイドラインで規定することが有用と考えられる。

5.2.1.5. 失効情報の取得と検証

失効情報を扱う際に考慮すべき項目として、以下を想定する。

- 失効情報の伝達方法の特徴（OCSP と CRL の違い：データサイズ、伝達時間の長さ等）
- 失効情報の取り扱いの期限
- 失効情報の受付方法（例：ポータルにアクセスすると失効情報がチェックされるなど）

5.2.1.6. 証明書利用者（EE）への情報提供

証明書利用者に対して、以下の項目についての情報提供を行う。

- 信頼点の証明書、検証パス、ポリシーの相互運用
- オブジェクト識別子（OID）とは

- オブジェクト識別子の取り方、管理方法

5.2.1.7. 分野別の要件（保健医療、金融、教育等）

以上の項目のほか、分野別のベストプラクティスとして、以下の各分野についての規定事項を追加することが想定される。

- 保健医療分野
- 金融分野
- 教育分野

こうした分野別の項目は、本来共通にすべきであるが経緯上複数の規範が存在するような場合の打開策としても適用が可能である。

5.2.1.8. コストとの関係

電子認証に関するサービスレベルを決定する際に、構築・運用に要するコストと運用時のリスクについて情報を提供することは有用と考えられる。ただし、分野を特定しない状態で定量的な議論を行うことは困難であることもあり、コストとリスクに関する要因とその相互作用についての指摘にとどまることも想定される。

5.2.2. 運用関連

電子認証サービスを運用もしくは保守していく際の BCP として、以下の内容を規定することが想定される。なお、これらの事項をとりまとめ、運用規程のテンプレートとして提供することも考慮することが望ましい。

5.2.2.1. 失効情報の取扱い

保証レベルの箇所でも言及しているが、失効情報についてはこれまでの認証サービスにおいて適切に扱われてきたとは言えない。ガイドラインにおいては、一定の保証レベル以上で運用する場合、最新の失効情報を反映させることを求めることになる。

5.2.2.2. 危機管理対応

電子認証サービスにおける緊急事態発生時の危機管理（Crisis Management）として

対応すべき対応（緊急時対応、業務継続計画（Business Continuity Plan））について定めるものである。想定される緊急事態の例としては、以下のケースを想定する。

（1） 秘密鍵の漏洩

認証局等において管理している秘密鍵に関する機密性が破られた場合に関係者が行うべき対策とその実施手順を規定する。

（2） 暗号アルゴリズムの危殆化

暗号アルゴリズムそのもの、もしくは認証サービスにおいて利用している実装において欠陥が発見され、認証サービスにおける機密性や完全性が確保されない恐れが生じた場合に講じるべき対策とその実施手順について規定する。

（3） 認証局サーバへの不正アクセス、悪意のソフトウェアの侵入

認証局を運用しているサーバへの不正アクセスやコンピュータウイルス、ワーム等の侵入が発生、ないし発生する恐れがある場合の対策とその実施手順について規定する。

5.2.2.3. 証明書利用者（EE）に必要とされること

これまでは、証明書利用者のうち、いわゆるエンドユーザを対象にセキュリティ確保を目的として何らかの義務を課したりすることは困難とされてきた。ただし、電子認証サービスにおいて一定の保証レベルを確保するためにはすべての参加者が安全管理を行うことが欠かせなくなるため、以下に示すような事項の遵守をもとめることについて規定する。遵守を規定する方法としては、こうした内容について了解した旨を同意書の形式で提供することなどが考えられる。

（同意書の記述項目の例）

- サービス利用に先立って認証局証明書を確認すること
- 秘密として扱うべき情報を漏洩させてはいけないこと

5.3. ガイドラインの策定と維持管理のあり方

これまでの議論をもとに、IETF における BCP の策定プロセスを日本国内で適用した場合の、ガイドラインの策定とその後の維持管理のあり方について検討する。

5.3.1. ガイドラインの策定プロセス

前節で示したように、IETF における BCP ドキュメントの策定プロセスは以下の手順で行われる。ここでは、確認のためそれぞれのプロセスの要旨を示す。

（1） Internet-draft の提出

誰もが自由に投稿できるドキュメントとして、Internet-draft が提出される。

（2） Internet-draft の公開

提出されたドキュメントを、IETF は自らのサーバを通じて６ヶ月間公開する。

（3） 支持に基づく IESG への申請

公開中の意見をもとに、広くインターネット業界に有用な情報を含んでいると判断された場合、BCP にすることについての IESG への申請が行われる。

（4） IESG によるレビュー・承認

申請をもとに、IESG が申請内容をレビューし、BCP とすることが適切と判断された場合は承認の手続きが行われる。

（5） BCP としての登録・公開

申請が承認されると、ドキュメントには RFC 番号（あるいは BCP 番号）が割り当てられ、公式に IETF の FTP および Web サーバを通じて恒常的に参照可能なドキュメントとして扱われるようになる。

これと同様の手続きを経るべく、ガイドラインの策定プロセスとしては以下の手順を想定する。

（1） 民間におけるニーズに基づく趣意の表明

電子認証フレームワークの一環として電子認証に関わるガイドラインを策定する旨の趣意の表明を行う。

（2） 趣意の内容の公開

以下の項目を含んだ趣意を公開し、関係者（ステークホルダ）からのコメントを集める。

- 文書化の目標
- 利用対象者
- 策定作業期間
- レビュ対象者

（3） 趣意に基づく活動の実施

外部からのコメントをもとに、ワーキンググループ等の活動を通じてガイドライン案の作成作業を行う。

（4） ガイドラインの策定

作成されたガイドライン案を公開し、コメントを得た上で承認プロセスを経て策定に至る。

（5） 新たなニーズに基づく更新

運用・マネジメントのプロセスとして、ガイドラインの実施を通じて得られた影響、反応、意見等を踏まえ、ガイドラインの更新プロセスを継続的に実施することになる。

5.3.2. ガイドラインの展開のあり方

ガイドライン策定後の展開として、ある分野を対象とした BCP を電子認証フレームワークを通じて別の分野に適用すべく改良することが想定される。この関係を次図に示す。派生的な BCP について議論する手段としては、直接ワーキンググループ（WG）会合を通じて行うだけでなく、メーリングリストやソーシャルネットワークサービス（SNS）を使って行うことも想定される。

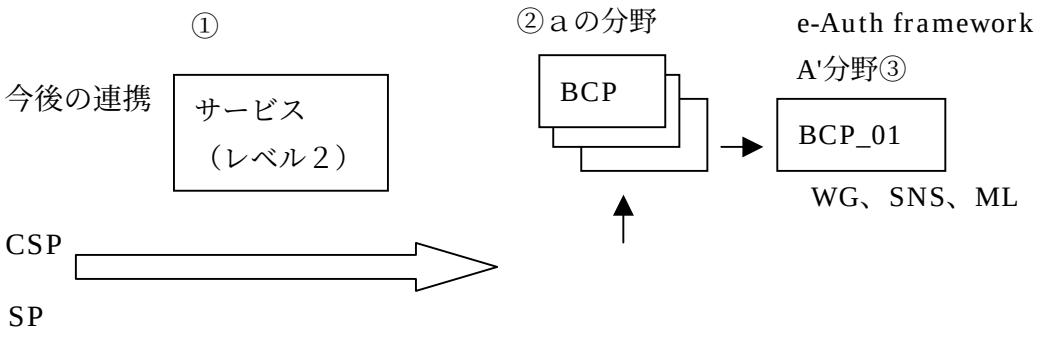


図 5−2　他分野への BCP を通じた連携

5.4. ガイドライン策定に際して留意すべき事項

これまで議論してきたガイドラインが有効に機能する範囲について確認する。

5.4.1. ガイドラインが機能しない条件

日本国内における電子認証分野において、本ガイドラインの適用対象外、もしくは適用対象であっても有効に機能しないと考えられる条件について考察する。

5.4.1.1. ガイドラインの適用対象外となる事例

電子認証サービスのうち、以下の事例については本ガイドラインの適用対象外となるものと考えられる。

（1）　電子認証の仕様や運用に関する規程が独自に定められている分野

分野を限定して、電子認証に関して独自の規程を適用することが定められている場合は、本ガイドラインの適用対象にはなり得ない。現時点においては日本国内においてこうした分野の事例はないが、「保健医療福祉分野 PKI 認証局 証明書ポリシ」が 2005 年に策定されるなど、独自の規程を策定しようとする動きが見られる。

（2）　セキュリティ対策の不十分な認証サービスを許容している分野

当然ながら、本ガイドラインの定める内容を満たすことを前提としない認証サービスにおいては、一部組織が本ガイドラインに準拠しても全体のサービスレベルは本ガイドラインの想定している水準を満たさない。このようなサービスについては本ガイドラインの適用対象外となる。

5.4.1.2. ガイドラインの適用対象であっても有効に機能しない事例

前項とは別に、ガイドラインの適用対処とすることは可能であるが、実際には有効に機能しないと判断される分野の事例を挙げる。

（1）　高度なセキュリティを規定する必要がある分野

通常と比較して極めて高度なセキュリティを要求される分野については、各組織が本ガイドラインに準拠する形で、電子認証サービスにおいて必要なセキュリティを確保す

ることは容易ではない。これは、ベストプラクティスに基づいて要件を定める方式が、高いレベルのセキュリティ要件の規定には適していないことによる。このような条件の場合は、強制力をもった規程を定め、サービスの参加組織にこれを遵守させることが必要となる。

（2） 高度なセキュリティを規定する必要がある分野

ここで対象としているガイドラインは民間主体で策定するものであるが、国をはじめとする行政機関、公的機関において、本ガイドラインに基づいた電子認証サービスの構築、運用を行うことを妨げるものではない。ただし、一般に行政の提供するサービスには行政固有の要件を必要とする場合が多く、電子認証サービスにおいてもそうした要件を行政において独自に規定する場合は、本ガイドラインに準拠しているとみなすことは難しくなる。

このほか、以下の条件が満たされる場合も、行政機関等が独自のガイドラインの策定する動機となり得る。

- ガイドラインの策定主体、策定プロセスが中立的とみなしにくい場合
- 何らかの理由の結果、本ガイドラインの維持・管理が将来的に継続的に行われることへの信頼感が得にくい場合

5.5. まとめ

日本における電子認証サービスにおいては、幅広く利用可能で保証レベルを定めたガイドライン的な役割を担うドキュメントが存在せず、本来必要であるべき安全性が確保されないまま PKI システムの構築が進んでいく恐れがある。

こうした中で、IETF の Best Current Practice の考え方をもとに、電子認証フレームワークの中で「経験上有効で目安となる使い方」をまとめたガイドラインの作成を推進していくことが求められている。

5.6. 今後の展望

電子認証フレームワークにおいてガイドラインを作成していくのに向けて、今後の展望を示す。

5.6.1. 関連機関との連携

日本 PKI フォーラムにおいて、調査で提案しているガイドラインと同様、レベル分けを含む内容をもった電子認証ポリシーガイドライン検討が進められている。電子認証の利用者の視点からは、日本 PKI フォーラムが証明書ポリシー（CP）、JPNIC が認証業務規程（CPS）をそれぞれ策定するイメージがあるとの意見もあり、これらが重複した作業になることを避けるためにも両者の知見を交え、それぞれの立場からベストプラクティスを提示、共有していくことが考えられる。

5.6.2. ガイドラインの構築に向けた取組み

実際にガイドラインを作成するのに際しては、以下のような取組みが考えられる。

（1）　ベストプラクティスの集成

これまでに実施されている電子認証サービスの構築・運用事例のうち、優れた効果を示しているものや利用者・運用者の評価が高いものについて、実施者の協力を得てその構築・運用時に用いたドキュメントやノウハウの収集、整理を行う。

（2） 保証レベル区分の導入の影響に関する調査

今回策定するガイドラインの主たる特徴となる保証レベルについて、導入した場合の影響や事前に考慮しておくべき対策について調査を行うことが望ましい。

（3） 策定プロセスの実施

以上(1)(2)の結果を踏まえ、策定プロセスに則ってガイドラインの検討が行われることになる。

第 6 章　IP アドレス認証の展開に関する調査研究について

内容

- IP アドレス認証局の役割と構成
- 安全な経路制御の為の電子認証

6. IP アドレス認証の展開に関する調査研究について

本章では、2004 年度までに構築された IP アドレス認証局の展開に関して述べる。IP アドレス認証局は JPNIC で構築された認証局の一部で、他の認証局が発行する電子証明書と組み合わせ、また登録情報に基づいた電子証明書の発行を行うことで、様々な展開方法が考えられる。

2005 年度の調査研究では、インターネットにおける経路情報交換のプロトコルである BGP の安全な運用に着目し、調査研究を行った。

本章ははじめに IP アドレス認証の考え方と IP アドレス認証局の構成について述べ、次に BGP の安全な運用のために考えられる電子認証の利用方法について紹介する。

6.1. 概要

「IP アドレス認証」とは 2004 年度までに JPNIC で構築が進められた IP アドレス認証局を使った電子認証を意味する言葉である。特に IP アドレスが入った電子証明書を意味しているわけではない。

JPNIC の「IP アドレス認証局」は主に二つの考え方に則って構想が検討された。一つは登録情報の正当性確保である。これは JPNIC に情報登録を行う IP アドレス管理指定事業者に対して電子認証技術を使った認証を行い、不正な情報登録を防ぐという考え方である。この認証強化によって JPNIC が WHOIS サービス等で提供する情報の信頼性が向上するだけでなく、IP アドレス管理指定事業者に割り振られたアドレス資源の情報が、第三者によって不正に書き換えられ、ISP 事業に支障が出ることを防ぐというメリットが考えられる。もう一つの考え方は、登録情報に基づく電子認証の提供である。正当な手続きを踏んで登録された情報は、登録されたユーザやサーバの間の認証に使うことができる有効な情報源になると考えられる。そこで登録情報に基づいて電子証明書の発行を行えば、登録された者同士が SSL や IPsec などの暗号プロトコルを利用するためにその電子証明書を利用することができるようになる。

この二つの考え方は、電子認証の導入における二つの段階でもある。一つ目は JPNIC による登録者の認証であるため、認証する者は必ず JPNIC となる。認証に使われる電子証明書の検証を行う者が JPNIC 自身であるため、電子証明書に入れる内容や保証のレベルを決定しやすい。また電子証明書の発行を行う認証局の信頼性について、外部から担保されるための体制を整える必要がなく、運用を開始しやすい。二つ目は、JPNIC

でない証明書ユーザ同士の認証である。証明書ユーザにとって JPNIC が第三者となるため、PKI の本来の適用方法に近い。発行される電子証明書はユーザの利用環境や、ユーザの挙動を想定して設計される必要がある。また証明書ユーザに対して認証局の信頼性を示す必要がある。JPNIC の認証業務の信頼性は、一つ目の情報登録のための認証が基本となる。

2004 年度までに行われた調査研究では、一つ目の役割を持つ認証局として「IP アドレス認証局（認証）」が、二つ目の役割を持つ認証局として「IP アドレス認証局（証明）」が構築された。

6.2. IP アドレス認証局の役割と構成

JPNIC の認証局である IP アドレス認証局の構成を図 6-1 に示す。

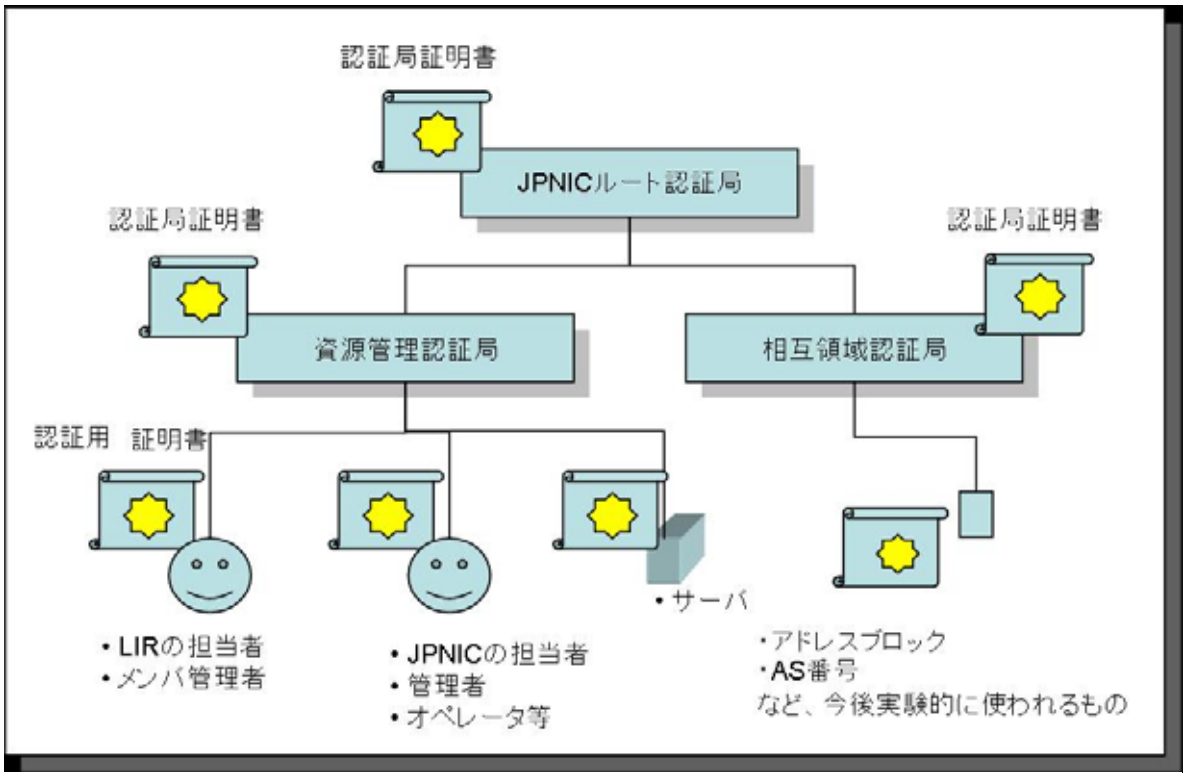


図 6-1　JPNIC の認証局の構成

JPNIC の認証局の中で、すべての認証局の上位認証局となるのが「JPNIC ルート認証局」である。この認証局は、JPNIC における認証業務の信頼点（Trust Point）を提供するためにあり、証明書の検証を行う者は必ずこの「JPNIC ルート認証局」の証明

書を正しい方法で入手する必要がある。2005 年の時点の、この認証局の CN（Common Name）は「JPNIC Primary Root Certification Authority S1」である。

「IP アドレス認証局（認証）」は「資源管理認証局」として示されている。この認証局は、登録情報の正当性向上のための PKI を使った認証機能の提供を目的としている。2005 年の時点のこの認証局の CN は「JPNIC Resource Service Certification Authority」である。

「IP アドレス認証局（証明）」は「相互領域認証局」として示されている。この認証局は、登録情報に基づいた電子証明書の発行を行い、アドレスブロック、AS 番号等における電子認証ために設置されている。2005 年の時点の CN は「JPNIC Interauth Certification Authority」である。

前節で述べた二つの段階は、「資源管理認証局」の構築と「相互領域認証局」の構築の二つにそれぞれ当てはまる。

6.3. 安全な経路制御のための電子認証

JPNIC における登録情報は、主に IP アドレスに関する情報である。この登録情報は、IANA を頂点とするインターネットレジストリの階層構造に則って割り振られた IP アドレスに関するもので、IP アドレスの一意性や地域性を正しく反映したものとなる。一方、IP アドレス管理指定事業者に対する割り振り情報は、インターネットの経路情報に対する原本となる情報であり非常に重要な意味を持つ。インターネットでは、原則的として、この割り振られた IP アドレスの範囲に則って経路情報が決定されているためである。そこで 2005 年度は経路情報の交換を安全に行うための電子認証に注目し、調査研究を行った。

インターネットにおける経路情報の交換は、自律分散システムの技術が使われており、専門的な分野である。また経路情報を交換するシステムは、1970 年代より運用されており歴史が長い。従ってこの分野における電子認証の適用には、経路情報の交換（ルーティング）における歴史的背景や常識的な運用形態に関する理解が必要となる。

そこで次章以降には、ルーティングの分野の専門家に協力を得て、基本的な技術情報から近年の動向にかけて重点的に情報をまとめた。

第 7 章　アドレス資源管理と経路情報の現状

内容

- インターネット経路制御
- BGP-4
- 最新経路情報
- アドレス資源管理と経路
- インターネットルーティングレジストリ

ほか

7. アドレス資源管理と経路情報の現状

本章では、本調査を実施する上で基礎となる情報を解説する。特に、IP アドレスの資源管理方法やインターネットの経路制御の本調査報告書執筆時点における現状についてまとめると共に、本調査で必要となる基礎知識について解説する。

本章では、まずインターネットにおける経路制御の考え方と経路制御方式について解説し、インターネット全体における経路制御を行うための経路制御プロトコルである BGP-4 について、簡単な方式の説明と動向について解説すると共に、現状の経路制御の実態を報告する。

次に、IP アドレス資源の管理方式について解説する。IP アドレスの資源管理と管理されている IP アドレスがインターネットでどのように経路制御されるかについての関連性について解説する。

次に、インターネット経路制御における問題点を整理し、その実態について報告する。

最後に、これら問題点に着眼し、インターネット経路制御を行う上で、本調査の核となる「インターネット・ルーティング・レジストリ」および「IP レジストリシステム」について解説する。

7.1. インターネット経路制御

本節では、インターネットの経路制御について、最初に基礎的な部分を解説し、次に経路制御を実施する上での単位となる経路制御単位(Routing Domain)について解説する。

最後に、会社単位などの組織内での経路制御方式とインターネット全体の経路制御方式の違いを明らかにし、そこで使われている実際の経路制御プロトコルについて解説する。

7.1.1. 経路制御基礎

インターネット上を流れる一連のデータは、パケットといわれるデータ単位に分割され、送信元から送信先にインターネット網上を利用して送信される。このとき、それぞれのパケットには、「送信元アドレス」と「送信先アドレス」が記録されており、インターネット網を構成する「ルータ」は、「送信先アドレス」よって送信先のデータ回線を選択し、目的の送信先端末までパケットを送り届ける。このときの「ルータ」は、電話回線における「交換機」に相当する装置と考えて良い。

この様子を図 7-1 に示す。

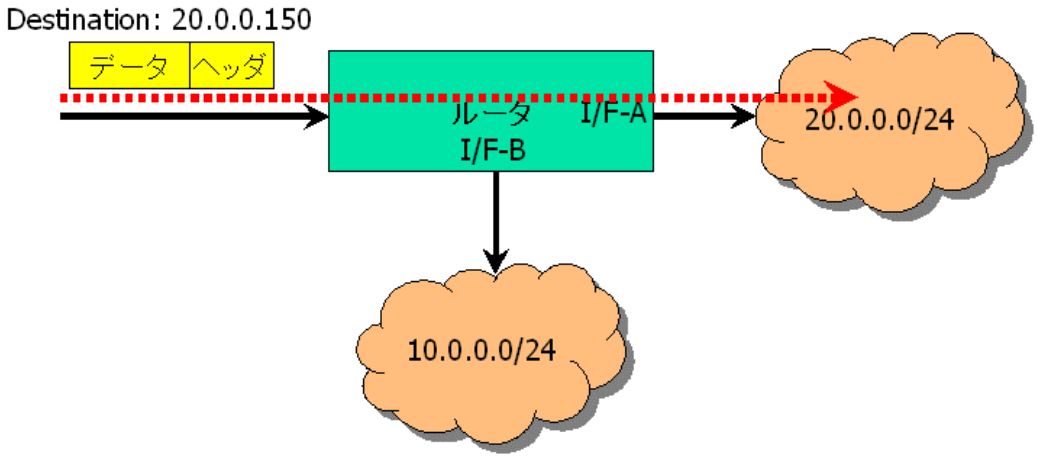


図 7-1　ルータの基本的パケット転送の様子

ルータでは、受信したパケットを、そのパケットの目的地に向かう最良の回線を選択し、その回線にパケットを送信する責務を負っている。この送信回線の選択には、「経路表」といわれる、送信先のリストを使って行われる。実際には、ルータは送信先アドレスの固まりである

プレフィックスとそのプレフィックスに該当するパケットを受信した際の最良の転送先ルータアドレスが書かれた「経路表(Routing Table)」と言われるデータベースを持ち、ルータではこのデータベースに従って経路の選択が行われる。これらの選択は通過するルータで何度も実施されて、パケットは送信先の端末まで送信される。この通過していくパケットの道筋を「経路」という。この様子を図 7-2 に示す。

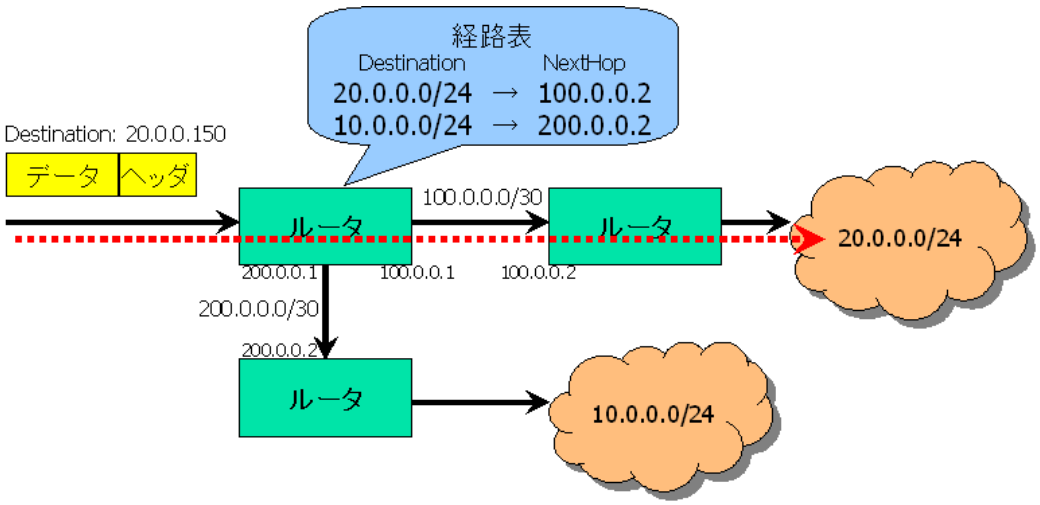


図 7-2 経路表によるパケット転送先の選択

以下に、経路制御の概念についてまとめる。

- 経路
  - パケットが送信元から送信先に向けて転送されてゆく「道筋（パス）」である。

- 経路表
  - 受信したパケットの送信先(Destination)アドレスに向けて、そのパケットを転送する次のルータのアドレスを示したデータベースである。

基本的な経路制御では、この経路表は人の手によって作成され、個々のルータに設定されることによって動作する。しかし、人の手による作業では、管理対象のネットワークが大規模になるにつれ、これらの設定が煩雑になるほか、ネットワークの機器や回線に問題が発生した場合に、人の手を介して対策を講じる必要があり、安定したネットワーク運用に問題が出ることが考えられる。このため、これらの経路表の作成を自動化し、ネットワーク障害が発生した場合にでも、図 7-3 に示すように、障害のポイントを自動的に迂回するような機能を持たせる必要がある。これらの機能を実現する手法として「動的経路制御プロトコル」を利用

する。一方、前者の人の手によって経路表を設定することを、固定的にルータに経路表を設定することから「静的経路制御」と呼んでいる。

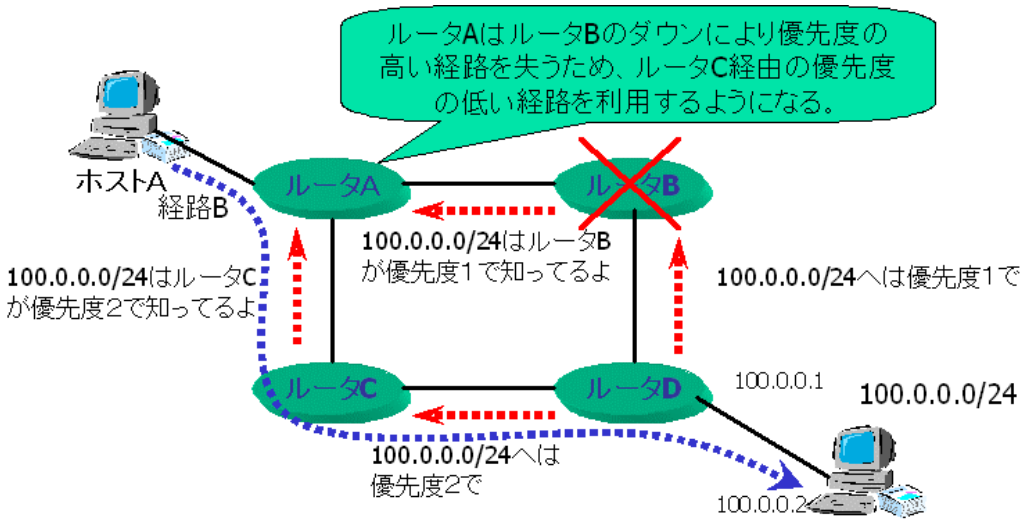


図 7-3　ルータダウンによる迂回の例

経路制御の一般的な特徴は、送信先のネットワークがどこに（どの回線）につながっているかという情報によって送信先を判断している。これは、動的経路制御においても基本的に同じである。具体的には、動的経路制御では、自分が接続しているネットワークの情報を他のルータに伝えるという手段によって、ネットワークの接続情報を構成していく。つまり、あるルータが接続しているネットワークの情報を他のルータに通知し、それをさらにその先のルータに伝搬することで実現するのである。これをデータの流れに置き換えると、データパケットが送信先に向かって送信されていくのに対し、ネットワークの情報である経路情報は、概念的に送信先から送信元に向かって情報が流れていくということになる。

動的経路制御を行う上で、インターネットを安定的に保つというさらに重要な機能を得ることができる。先ほども述べたように、ネットワーク障害の発生している箇所を迂回するという機能である。たとえば、送信元の端末から送信先の端末の間に、複数の経路が存在するような場合に動的経路制御を用いたとする。このような場合、動的経路制御では、これら複数の経路のうち、送信元と送信先の間を結ぶ最良の経路を選択し、その経路を使ってデータを送受信する。そして、万が一最良の経路に問題が発生した場合でも、もう一つある迂回の経路を用いてパケットを送受信するように経路を自動的に選択することが可能になる。

7.1.2. 経路制御ドメイン

経路制御の基本的な考え方は、「7.1.1 経路制御基礎」で解説した。しかし、ここで解説した動的経路制御を大規模なネットワークで実施するには、経路情報が大きくなり過ぎてルータがかえって不安定に可能性があるほか、管理するネットワークが複数の部署や会社にまたがることで、単一の方針によって管理できないなどいくつかの問題が生じてくる。

そこで、動的経路制御では、経路制御できる範囲を分割して管理することで、このような問題を避けるようにすることができる。

この経路制御できる範囲を「経路制御ドメイン(Routing Domain)」と呼ぶ。

また、この経路制御ドメインの範囲内のことを、「イントラ・ドメイン」と呼び、この経路制御ドメイン間を接続することを「インター・ドメイン」と呼ぶ。この様子を図 7-4 に示す。

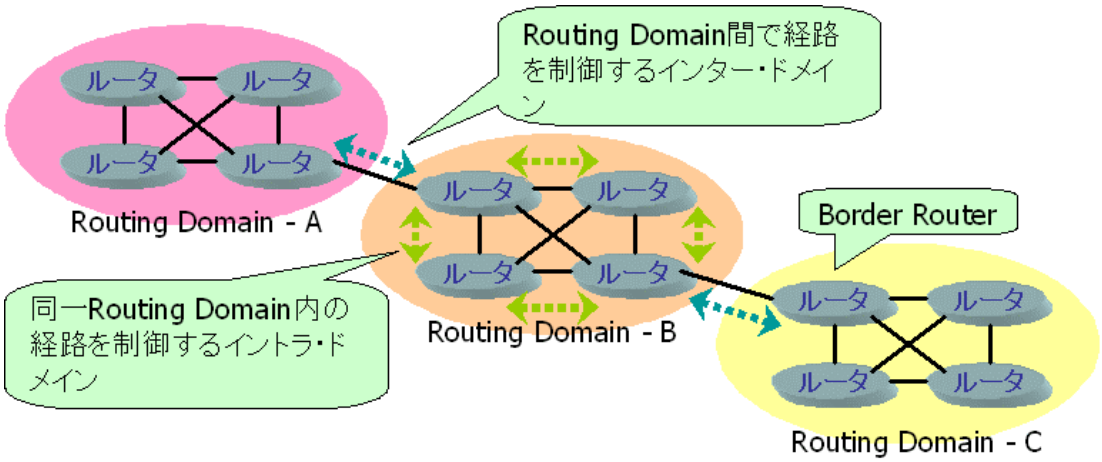


図 7-4　イントラ・ドメインとインター・ドメイン

動的経路制御では、イントラ・ドメインでは一般的に1つの経路制御プロトコルによって動的経路制御を実施する。一方、インター・ドメインでは、同一、または異なる経路制御プロトコル間で互いの経路制御ドメインの経路情報を交換しながら、イントラ・ドメインとインター・ドメインの間の連携を保つ。つまり、インター・ドメインの経路制御で交換される経路情報は、他の経路制御ドメインから受け取った経路情報も伝搬することもでき、これによって、複数の経路制御ドメインを跨いで経路情報を伝搬させることが可能になる。経路情報が複数の経路制御ドメインに行き渡ることができれば、パケットは、複数の経路制御ドメインを跨いで送信可能になると言える。

7.1.3. IGP と EGP

経路制御ドメインは、最小の経路制御の単位となるが、インターネットという膨大なネットワークで経路制御を行うことを考えると、さらに大きな単位での経路制御を行う必要がある。その経路制御単位が「自律システム（Autonomous System）」であり、一般的に「AS」と略して呼ばれものとなる。

ASは、会社やISPなど比較的大規模な単位で構成されるが、その単位毎に一定の経路制御のポリシ（方針）を持って運用されることが前提とされている。一方、AS の内部では、前節で述べたとおり、1つ以上の制御ドメインによって管理されることになる。

AS というような大きな単位間での経路制御プロトコルを「EGP(Exterior Gateway Protocol)」といい、AS内部で利用される経路制御プロトコルを「IGP(Interior Gateway Protocol)」という。この様子を図 7-5 に示す。

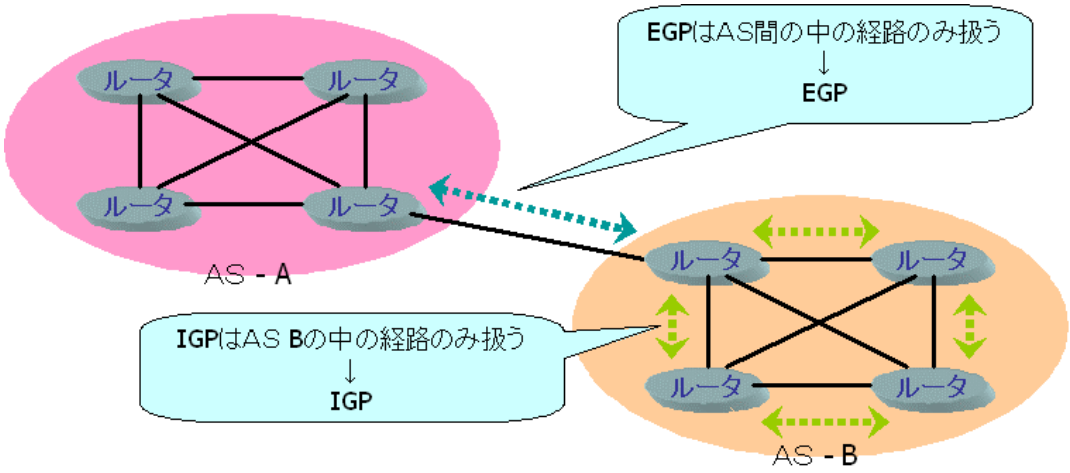


図 7-5 IGP と EGP の違い

IGP と EGP では、経路制御プロトコルの概念が大きく異なる。IGP では、会社や ISP などの組織内部で機敏な制御が可能となるようにサブネット単位での経路制御を基本としている。一方、EGP では、組織単位での経路制御を念頭に置くため、AS という単位で経路制御が行われる。つまり、EGP では、概念的に1つの AS が 1 つのルータのような扱いで経路制御が実施されている。以降の節において、IGP と EGP についてそれぞれ簡単に解説する。

7.1.4. IGP

IGP は、主に AS 内部で経路制御を行うための経路制御プロトコルである。IGP には、主に、RIP、OSPF、IS-IS などのプロトコルが多く使われている。小規模のネットワークでは、RIP が多く使われ、比較的大きなネットワークでは、OSPF がよく使われている。IS-IS は、OSPF と同様の考え方で作られているプロトコルだが、OSPF に比べ早期に作られ、米国などでは未だに多く利用されている。

本節では、以下に RIP と OSPF についてその特徴を整理する。

- RIP (Routing Information Protocol)

  経路制御プロトコルの中で最も単純なプロトコルであり、「距離ベクトル(Distance Vector)型」プロトコルとして、RFC1058[1]にまとめられている。

  初期バージョンの RIP では、アドレスクラス毎の経路制御しかできなかったため、RIP Version2.0 で VLSM(Variable Length Subnet Mask)に対応した。

  RIP での経路制御は、「メトリック（Metric）」といわれる送信先ネットワークまでのルータの数、つまり、送信先ネットワークまでの距離によって制御する。しかし、この Metric の値は最大で 16 までしか対応しておらず、16 台以上のルータを越えた経路制御はできない仕組みになっており、それ以上の大規模なネットワークでは利用できない。

- OSPF (Open Shortest Path First)

  現在 IGP として最もポピュラーなプロトコルであり、「リンク状態(Link State)型」プロトコルとして、RFC2328[2]にまとめられている。現在のバージョンは 2。

  経路制御は、コスト(Cost)という単位を用いて行い、回線毎にコストが設定され、通信端点間の総コストによって最良の経路を選択して、パケットの送信を行っている。

  OSPF では、大規模なネットワークを効率良く管理できるようにするために、複数の

[1] Routing Information Protocol(RFC1058)
http://www.ietf.org/rfc/rfc1058.txt
[2] OSPF Version 2(RFC2328)
http://www.ietf.org/rfc/rfc2328.txt

「エリア」という経路制御ドメインを設定できることが一つの特徴である。

7.1.5. EGP

EGP は先にも解説したように、主に AS 間での経路制御プロトコルとして用いられている。EGP は、現在のところ RFC4271[3]にまとめられている BGP-4(Border Gateway Protocol Version.4)が実質的に唯一の物として利用されている。

BGP-4 は、「パスベクタ(Path Vector)型」のプロトコルで、AS までのパス（経路）とその距離によって最良の経路を判断している。

BGP-4 は、インターネット全体という大規模なネットワークを効率よく経路制御できるように設計されている。このため、経路制御用のパラメータとして、内部で利用できるものや、AS 間で情報を伝搬して利用できる物など複数の経路判断基準を持ち合わせている。このようなことから、BGP-4 は高い拡張性と高いスケーラビリティを持ち合わせたプロトコルといえる。

一方で、柔軟過ぎる構造のためこのプロトコルの利用者とも言えるネットワーク運用者にゆだねられる部分も多く、現在の様な高度なセキュリティが要求されるネットワークにおいていくつかの問題点が出はじめている。

次節において、これらの問題点を正しく把握するために、BGP-4 の動作について解説する。

[3] A Border Gateway Protocol 4 (BGP-4) (RFC4271)
http://www.ietf.org/rfc/rfc4271.txt

7.2. BGP-4

本章では、本調査の主たる目的であるインターネット全体の経路情報に直接関係のある、インターネット全体の経路制御を実質的に行っている、BGP-4(Border Gateway Protocol Version 4)について解説する。

最初に BGP-4 の概要について解説し、BGP-4 というプロトコルがどのように作られているかについて解説する。

次に、このプロトコルを用いて、インターネットでは、どのような経路制御が行われているかについて解説する。

最後に、BGP-4 に関して IETF で行われている最新の議論、および BGP-4 に関連して採択されているプロトコルのうち現在のインターネットに大きな影響を持つものについてリストし、解説する。

7.2.1. BGP-4 とは

BGP-4 は、「7.1.5 EGP」の節でも述べたように、パスベクタ(Path Vector)型の経路制御プロトコルであり、主に AS 間での経路制御を行うためのプロトコルとして開発され、現在は RFC4271 としてまとめられている。

BGP-4 の最大の特徴は、経路を制御する単位を概念的に AS という単位で管理することにある。つまり、AS というネットワークの管理主体の方針に従って AS という単位で経路制御を行うことで、その AS の内部で行われている細かい経路制御などに一切関知することなくインターネット全体として経路制御を可能にしている。

このような BGP-4 には、いくつかのバージョンが存在し、現在は Version4 となっている。このプロトコルの前には Version3 が利用されていた。Version3 と Version4 の違いは、CIDR(Classless Inter-Domain Routing)をサポートしていることであり、それ以外の違いはほとんどない。

また、BGP-4 はインターネット全体という大きなネットワークを管理可能にするために、IGP の様な範囲の限られたネットワークを管理するプロトコルとは、以下の様な点が異なる。

- TCP を用いたプロトコル

　通常、経路制御プロトコルは、IP レイヤ、つまり IP アドレスを用いて通信を行うための情報を交換するプロトコルであるため、経路制御プロトコル自身は IP アドレスを用いた通信ではなく、その下位層の通信手段を用いて隣接するルータと直接情報を交換して経路情報のやりとりを行うことが多い。

　しかし、BGP では、隣接する AS の情報を送受信し、AS 間でどのような宛先のパケットを交換すべきかという情報を交換し、それに従ってパケットを転送することを目的としている。このため、IP レイヤとしては、隣接する AS と接続性を持っていることが前提であり、その上で互いの AS の経路情報を交換するため、IGP の様に下位層を用いた通信を行う必要がない。むしろ、BGP にとっては、隣接の AS の BGP ルータと信頼性のある通信セッションを持ち、常に互いの情報を交換できる環境を維持する必要がある。

　BGP では、これらの要件を満たすために IP レイヤ上の TCP によるコネクションによって通信を行うように設計されている。

- 差分のみの広告

　RIP などのように比較的小規模な経路制御プロトコルは、扱うネットワークの情報も少ないため一定時間毎に各ルータが持つ経路情報をすべて交換することで各ルータが持つ経路情報を最新の状態に維持している。

　しかし、経路制御プロトコルが大規模なネットワークに対応した場合、その経路制御プロトコルが取り扱う情報が膨大となり、すべての経路情報をいちいち交換していたのでは効率が良くない。そこで、BGP のような大規模なネットワークを扱うことのできる経路制御プロトコルは、通信相手のルータに対して更新された差分の経路情報を送付することで、全体の経路情報を最新の状態に維持するように設計されている。

- パスベクタ型の採用

　BGP は、パスベクタ型プロトコルであることは何度も述べてきた。パスベクタ型プロトコルの特徴は、どのような AS を経由して経路情報が到達したかを示す経路（パス）に主眼をおいて経路制御されるところにある。

パスに主眼を置くことで、経路情報が AS を経由してゆく段階で、同一の AS を何度も通過するような「ループ」という状態を検出することができ、このような不要な経路を排除することができる。さらに、経路情報の受信場所から、その経路情報の発信元までいくつの AS を経由してきたかという、概念的な距離も知ることができる。BGP-4 では、ここであげた情報も利用して最良の経路の選択をするすることが可能である。

このような、AS の連続によって表された経路を「AS パス」とよび、この AS パスに関連づけられた情報を「パス属性」とよび、BGP の経路制御に用いられる。

7.2.2. BGP-4 のプロトコル概要

BGP-4 は、TCP/IP 上で動作する経路制御プロトコルである。この経路制御プロトコルでは、前節でも述べたように BGP のコネクション(BGP セッション)を通じてお互いが持つ経路情報を、それぞれが望む属性(Attribute)を付与して相手側に広告(Announce)することによって経路情報を交換する。この様子を図 7-6 に示す。

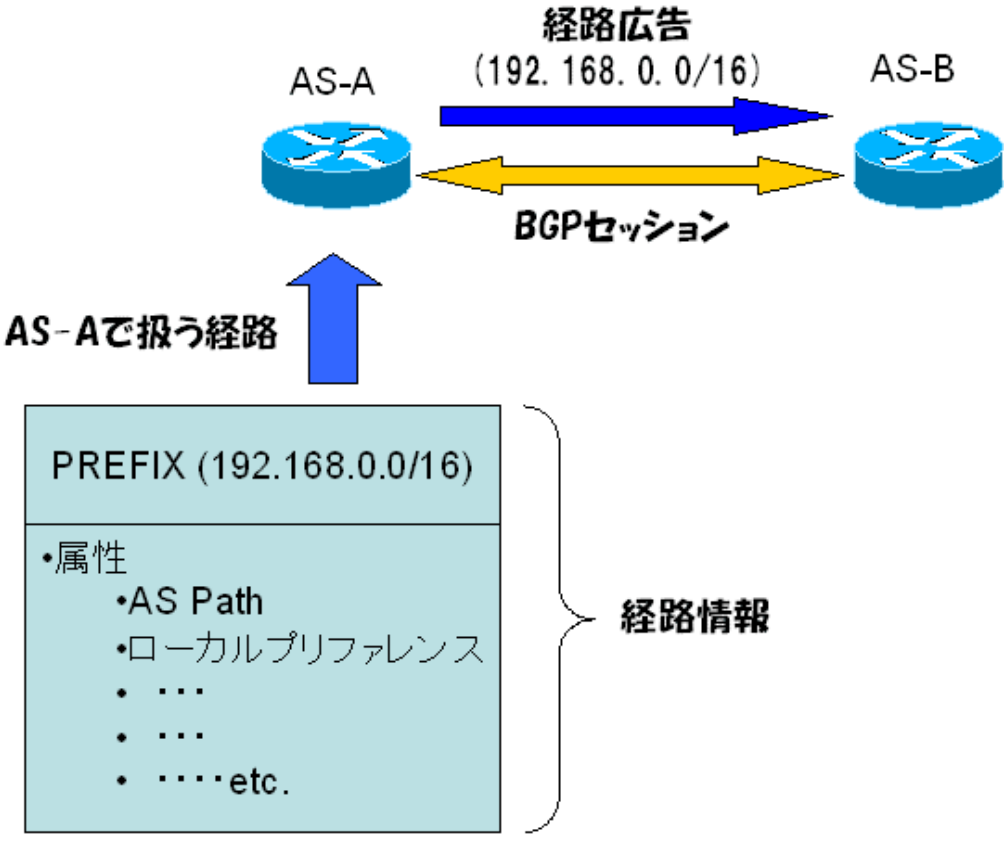


図 7-6 経路の構成とその広告

このため、BGP-4 ではお互いの状態を確実に把握するため、以下の 4 種類のメッセージを用いて互いの状態は管理している。

- OPEN

  待ち受け状態の BGP ルータに対してこのメッセージを送信することで、BGP の接続を開始する通知を行うと共に、互いの BGP ルータのサポートしている機能に関する情報を交換し、接続条件を互いのルータ間で交渉するために用いられるメッセージである。

- UPDATE

  経路情報の追加、削除、更新などの経路の更新情報を相手側に伝えるために用いるメッセージである。

- KEEPALIVE

  BGP-4 では、更新情報を接続相手に伝えるように設計されているため、経路の更新がなければ、メッセージの送信自体が発生しないことになる。このため、BGP セッションが確実に動作していることを確認するために、このメッセージを一定間隔毎に送付し、互いの BGP ルータが動作中であることを確認する設計となっている。

  この KEEPALIVE メッセージは、BGP ルータで持つ HOLD TIMER というタイマの三分の一の時間間隔で送信し、最短で 1 秒の間隔に設定可能である。HOLD TIMER は、KEEPALIVE メッセージの到着を最長で何秒間待つかを設定するタイマで、最低で 3 秒の値をとる。RFC4271 に推奨されているデフォルトの値は 180 秒であることから、KEEPALIVE メッセージの推奨送信間隔は、その三分の一の 60 秒となる。

  HOLD TIMER は、UPDATE メッセージ、または KEEPALIVE メッセージのいずれかを受信することで初期化されるが、HOLD TIMER が超過した場合は、その BGP セッションが正しく動作していない、または、どちらかの BGP ルータが正しく動作していないと判断し、その BGP セッションを破棄し、BGP 接続を切断する仕組みになっている。

- NOTIFICATION

　BGP-4 では、OPEN メッセージで正しくお互いの接続条件が満たされない場合や HOLD TIMER が超過した場合など、いくつかの状況において BGP セッションを維持できない、または確立できない場合がある。

　このような場合、BGP では、NOTIFICATION メッセージを相手側に送信し、エラー内容を通知すると共に、BGP セッションを切断するように設計されている。

BGP-4 では、これら4つのメッセージを使って BGP セッションを以下の 6 つの状態のいずれかにあることを管理している。

- IDLE

　BGP が動作していない状態を示している。

- ACTIVE

　BGP が動作している状態を示すが、BGP セッションの確立動作をしているわけではなく、BGP セッション接続先ルータとの TCP 接続受信待ち状態であることを示している。

- CONNECT

　OPEN メッセージの送受信前の TCP セッションの接続動作を実施中である状態を示している。

- OPEN SENT

　TCP セッションが確立し、OPEN メッセージを接続相手に送信した状態を示している。

- OPEN CONFIRM

　BGP の接続相手から OPEN メッセージを受信し、その動作条件を確認し、送信元の BGP ルータに対して確認の OPEN メッセージを送信し、その確認中の状態を示し

ている。

- ESTABLISHED

お互いの BGP の接続状態が確認でき、BGP セッションが正しく確立されている状態を示している。

BGP による経路情報の送受信は、この ESTABLISHED の状態に遷移した後に行われる。

BGP-4では、これらのメッセージを利用し状態の管理を行い、BGPセッションを正しく起動する。起動された BGP セッションは、ESTABLISHED 状態となり、経路情報の交換がUPDATE メッセージを用いて行われる。

これらの状態の遷移図を図 7-7 に示す。

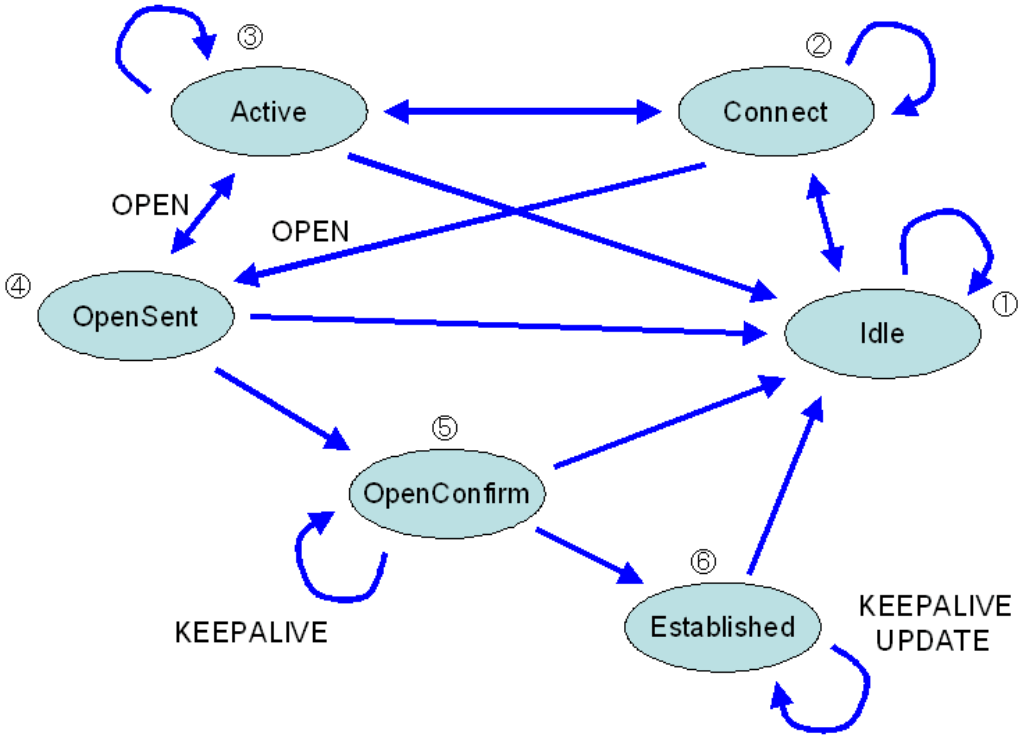


図 7-7 BGP の状態遷移図

UPDATE メッセージには、図 7-8 に示すように、パス属性、NLRI(Network Layer

Reachability Information)、および Withdrawn Routes の3種類の情報によって構成されている。

NLRI は、更新する経路の情報であり、送信元 BGP ルータが該当するネットワークに対する到達性情報を知っているということを受信側 BGP ルータに伝えてきている。この NLRI に対するパスの情報はパス属性によって与えられる。一方、Withdrawn Routes は、送信元 BGP ルータで該当する経路を失ったことを受信側 BGP ルータに伝える役割がある。

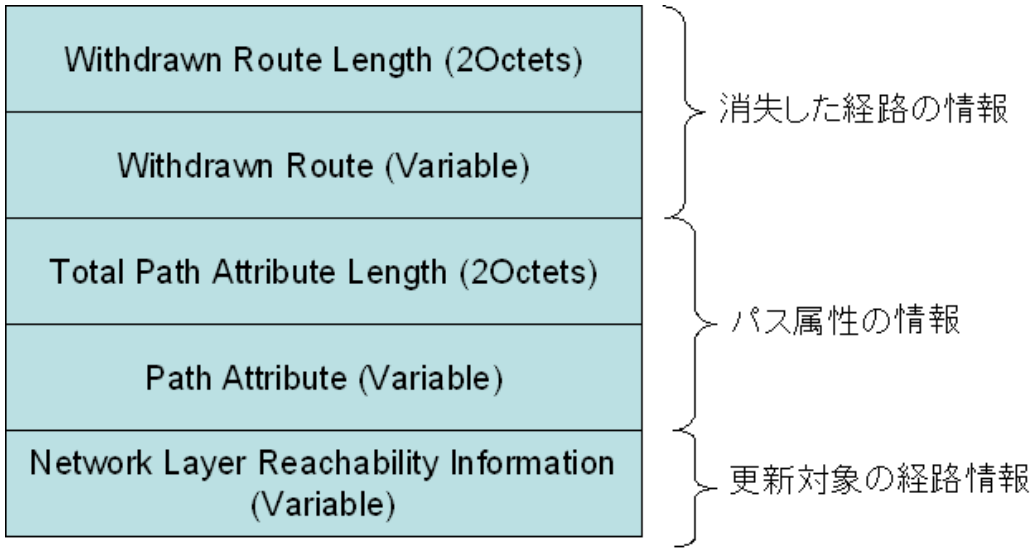


図 7-8 BGP Update メッセージのフォーマット

BGP-4 では、この UPDATE メッセージを用いて経路情報を交換し、最良の経路（パス）を選択している。次節に、BGP-4 による経路制御について解説する。

7.2.3. BGP-4 の経路制御方式

BGP は、AS 間で経路情報を交換するためのプロトコルであるが、AS の内部では他の AS から受け取った経路を自分の AS の中の他の BGP ルータに伝える必要もあるため、AS の内部でも BGP の接続を行うのが通例である。

このような AS 内部の BGP 接続を「IBGP（Internal BGP）接続」といい、通常の AS 間の接続を「EBGP(External BGP)接続」という。この様子を図 7-9 に示す。

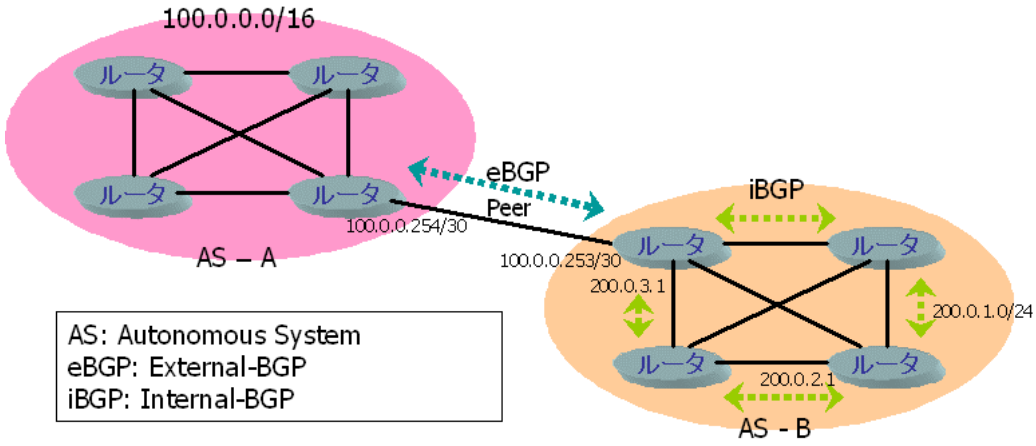


図 7-9 iBGP と eBGP

IBGP と EBGP では、プロトコル的な動作はほとんど変わらないが、唯一違う動作として、IBGP 接続から受信した経路情報を他の IBGP 接続へ転送しないという動作をする。このため、EBGP 接続から受信した経路は直接 BGP で受信した経路を必要とするルータに IBGP 接続で伝える必要がある。このため、通常では AS の内部にあるすべての BGP ルータ同士フルメッシュで IBGP 接続を設定しなくてはならない。

IBGP のフルメッシュによる接続によって AS 内部のすべての BGP ルータで、その AS から他の AS に向かう経路情報を共有することができる。しかし、複数の外部接続を持つ AS の場合、ある AS に向かう経路情報を複数の EBGP 接続から受信することがよくあるため、AS の内部には2つ以上の同一の AS に対する経路が存在することになる。このような場合、AS の内部でどちらの経路を選択するかを決める必要がある。

「7.1.5 EGP」でも述べたとおり、BGP では大規模なネットワークを柔軟に制御できるパス属性といわれる選択パラメータを持っている。以下に、BGP で標準的に利用できる代表的なパス属性について列挙する。

- Origin

  Origin は、何によってその経路が作られたかを示している。この属性の内容は基本的に変更せずに他のルータに伝搬する必要がある。

  Origin の値は、IGP、EGP、Incomplete のいずれかを採る。

- AS Path

  AS Path は、該当する経路情報が通過した AS の番号を列挙している。つまり、一番先頭に経路情報の発信元 AS が記録され、経路情報を伝搬した AS 番号が付加され、最後に自分の AS 番号が記録される形となる。

- Next Hop

  Next Hop は、該当する経路情報へ向かうパケットは、どの IP アドレスへ転送すればよいかを示している。

  EBGP から受信したばかりの経路情報の場合は、隣接するルータの IP アドレスが付与されるのが一般的である。しかし、IBGP 経由で受信した経路情報の場合、自分のルータに直接関係の無い、他のルータの IP アドレスである場合が多く、BGP ルータは、該当する経路情報でパケットの転送をする場合には、BGP の Next Hop アドレスの情報に従って IGP の経路情報を用いてパケットを転送しなくてはならない。

  このため、多くの場合、IBGP に経路情報を転送する場合はこの Next Hop 属性の値は変更されずに転送される。

- MED(Multi-Exit Discriminator)

  MED は、ある AS に対して直接的な接続を 2 つ以上持っている場合に、どの EBGP 接続を優先させるかという意志を接続先 AS に伝える為の属性として用いられる。

  最近の運用では、トラフィックの制御を緻密におこなうため MED などの外的要因によってトラフィックが変動しないように MED 属性を無視するような設定をしている場合が多いため、MED によってトラフィックの制御を行うような場合は、接続先の AS とあらかじめ調整が必要になるケースが多い。

- Local Preference

　Local Preference もパケットの転送先の優先順位を決めるためのパラメータである。主に AS 内部で利用するためのパラメータとして実装されている。

　たとえば、ある EBGP 接続で受信した経路情報を他の EBGP 接続でも受信していたとする。このとき、意図的にどちらかの接続の情報を優先させたい場合、つまり優先させた経路情報を受信している BGP ルータを利用してパケットを他の AS に転送したい場合に、このパラメータを利用して優先的に転送するように設定することができるのである。

　このパラメータの値は、経路情報とともに他のルータに転送してはいけない属性となっているため、基本的に他の AS には転送されない。

さて、BGP ではこれらのパス属性などを使って 1 つの転送先に向かう複数の経路情報からより良い経路情報を選択しなくてはならない。この選択基準は、ルータメーカによって若干の違いがあるが、多くの場合は同じ基準が採用されている。以下に、シスコシステムズ社製のルータで採用されている、経路選択基準を示す。なお、原文のまま引用しており、必要と思われる場合には、括弧内に解説を加えてある。（参照：インターネット・ルーティング・アーキテクチャー）

1) ネクストホップが到達できないときには、その経路は無視される。

2) 大きなウエイト(Weight)を持つパスを優先する。（Weight は、Cisco 独自のパラメータである。）

3) ウエイトが同じときには、大きなローカル優先度(Local Preference)を持つ経路を優先する。

4) 同じローカル優先度を持つときには、ローカルに生成された経路を優先する。

5) ローカル優先度が同じときには、短い AS パスを持つ経路を優先する。

6) AS パスの長さが同じときには、低い起源タイプ(Origin)を持つ経路を優先する。
(IGP < EGP < Incomplete の関係にある。つまり IGP が一番優先される。)

7) 起源タイプが同じときには、低い MED を持つ経路を優先する。
同じ MED を持つときには、次の方法で経路を優先する。外部（EBGP）は、コンフェデレーション外部経路よりも優先され、コンフェデレーション外部経路は内部(IBGP)よりも優先される。（コンフェデレーションは、BGP の拡張によって AS の内部をさらに複数の AS に分割することで、より大きなネットワークを管理しやすくするものである。次節にて解説する。）

8) 前記の条件がすべて同じときには、最も近い IGP 近隣ルータ経由で到達可能な経路を優先する。すなわち、その宛先に到達するのに AS 内で最短の内部パスを採る経路を優先する。

9) 内部パスが同じときには、BGP のルータ ID が決め手となる。最も低いルータ ID を持つ BGP ルータから来る経路が優先される。ルータ ID は通常、そのルータにおける最も大きな IP アドレスか、ループバック（仮想）アドレスである。ルータ ID は、実装に固有なものである。

このような優先される経路の選択は、AS の内外を問わずすべての BGP ルータで行われている。

一般的には、AS 内部では、先ほども説明したようにフルメッシュで IBGP 接続を行うため、優先される経路の情報は共有されており、AS の内部で優先される経路情報は複数あるうちの1つに選択されるが、IBGP 接続の接続先を操作したり、Local Preference の値を適宜操作したりするなどして、AS 内部の所々で選択する経路を変えることもでる。

BGP の経路制御に関する設定や運用が本報告書の主眼ではないため、詳しくは触れないが、BGP はここまでに説明したパス属性や BGP 接続を恣意的に操作するなどして非常にスケーラブルかつ柔軟な運用ができるよう設計されている。

7.2.4. 関連プロトコル

BGP に関する情報は、先にも述べたとおり RFC4271 にまとめられている。RFC4271 は、2006 年 1 月に発行された最新の RFC であり、その前には、RFC1771[4]として発行されていたものである。

[4] A Border Gateway Protocol 4 (BGP-4) (RFC1771)
http://www.ietf.org/rfc/rfc1771.txt

RFC1771 と RFC4271 の違いは、RFC4271 の Appendix. A にまとめられている。以下にその引用を日本語化したものを記載する。

Appendix. A RFC1771 との比較

RFC1771 との比較において、編集上の変更は数多くある。（ここに記載するには多すぎる。）

以下に技術的変更点を列挙する。

- TCP MD5[RFC2385 [5]]、BGP Route Reflectors[RFC2796 [6]]、BGP Confederations[RFC3065[7]]、BGP Route Refresh[RFC2918[8]]といったような機能の利用方法を反映し変更した。

- AGGREGATOR 属性の BGP Identifier の利用方法を明確にした。

- BGP ルータが Peer から受け付けるプレフィックスの上限を制限する手順

- AS 間のトラフィックエンジニアリングの為に AS_PATH 属性にある自 AS のもう一つの事象を BGP ルータの機能として含むようにした。

- NEXT_HOP タイプを明確にした。

- ATOMIC_AGGREGATE 属性の利用法を明確にした。

- 直接的な Next Hop 間の関係と NEXT_HOP パス属性で定義される Next Hop について記述した。

- Tie-Breaking 手順について明記した。

---

[5] Protection of BGP Session via the TCP MD5 Signature Option (RFC2385)
http://www.ietf.org/rfc/rfc2385.txt

[6] BGP Route Reflection – An Alternative to Full Mesh IBGP (RFC2796)
http://www.ietf.org/rfc/rfc2796.txt

[7] Autonomous System Confederations for BGP (RFC3065)
http://www.ietf.org/rfc/rfc3065.txt

[8] Route Refresh Capability for BGP-4 (RFC2918)
http://www.ietf.org/rfc/rfc2918.txt

- 経路広告の頻度について明記した。

- オプションパラメータ Type1(Authentication Information)については、推奨しないこととした。

- UPDATE メッセージエラーのサブコード 7 番 (AS Routing Loop) は、推奨しないこととした。

- OPEN メッセージエラーのサブコード 5 番 (Authentication Failure) は、推奨しないこととした。

- マーカーフィールドを認証の為に使うことを推奨しないこととした。

- TCP MD5 認証の実装を必須とした。

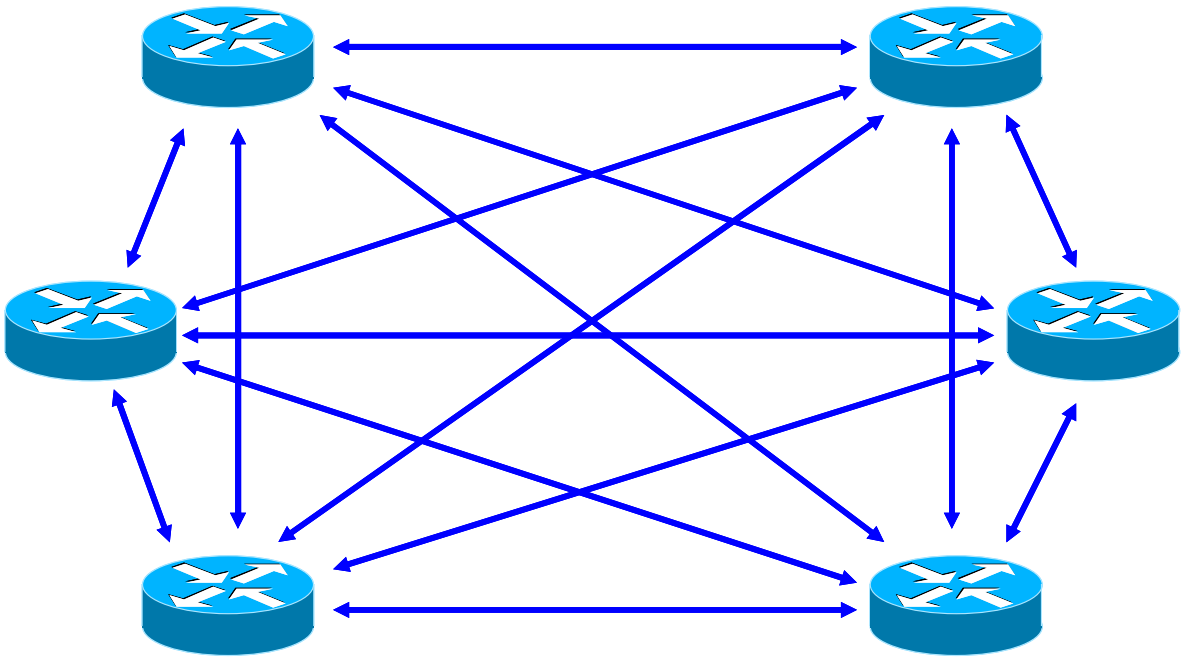
- BGP の FSM を明確にした。

この 2 つの RFC の間に大きな変更はなく、RFC1771 発行以降に発生したいくつかの修正などを反映したような作りになっているだけである。中でも、AS_Path 属性に関する修正が大きな物な修正の一つとしてあげられるが、これもシスコ社製ルータでは古くから実装されているもので、実際の運用現場では既にその機能が標準となっており、今回の RFC はこれに合わせた形になっている。

しかし、BGP はこれら基本的な機能だけでなく、変更点の第一項目で挙げられているような様々な拡張によって、より充実した機能を利用できるようになる。以下に、関連する機能、RFC のなかから重要な物を選択し、簡単な解説を加える。

■ BGP Route Reflection – An Alternative to Full Mesh IBGP (RFC2796)

IBGP 接続は、IBGP 接続経由で受信した経路は他の IBGP 接続に再広告しないため、EBGP で受信した経路は IBGP 接続を用いて AS 内のすべての BGP ルータに直接広告をしなくてはならない。このため、IBGP 接続は、フルメッシュで BGP 接続を行うこととなる。フルメッシュで IBGP 接続を行うと図 7-10 に示すように IBGP 接続が膨大な数となる。このため、大規模なネットワークで BGP を運用する場合には、ルータの性能などが問題となるケースがある。



BGPのフルメッシュのPeer数は、n×(n-1)の式に沿って増加する。
図の場合、n=6なので、6×(6-1)=30のPeer数となる。

図 7-10　フルメッシュによる IBGP 接続数の問題

このような問題を解消するために、ネットワーク内部をいくつかの「クラスタ」と言われるドメインを作り、その中に Route Reflector というそのクラスタのなかで経路制御を中核的に行うルータを設置し、他のルータは Route Reflector に対して IBGP を接続することで、IBGP 接続の数を減らすことが可能となる。

図 7-11 に Route Reflector を使った構成例を示す。

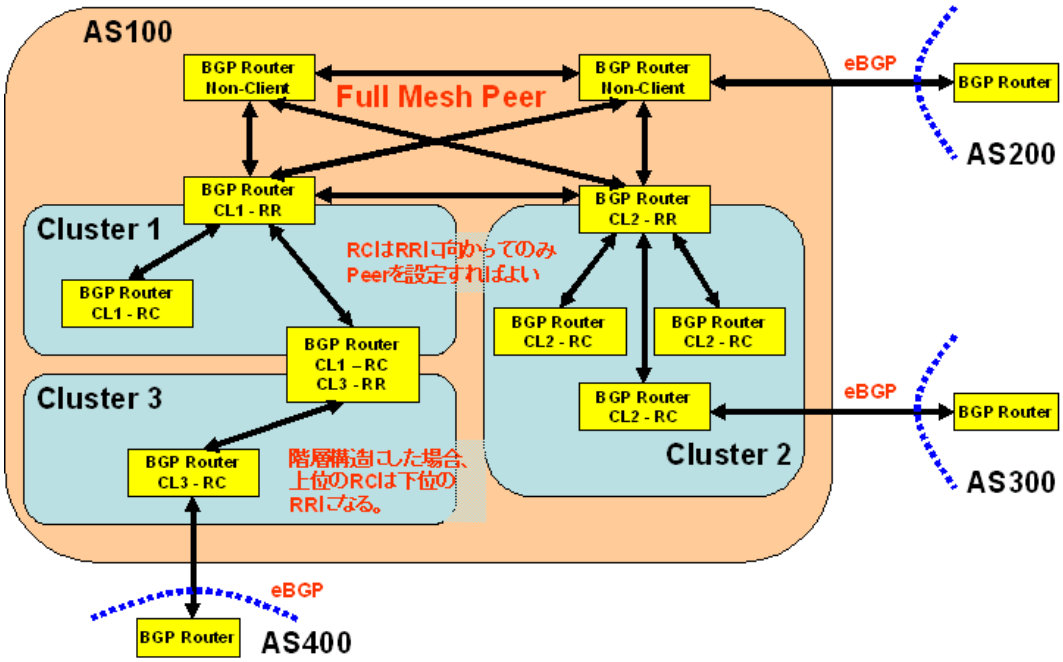


図 7-11　Route Reflector

Route Reflector となったルータは、IBGP で Route Reflector Client から接続されるが、通常の IBGP 接続とは異なり、一部の非転送なパス属性と共に Route Reflector Client から受信した経路を他の Route Reflector Client とクラスタに属さない IBGP ルータに経路情報を転送する処理を行う。

■ Autonomous System Confederations for BGP (RFC3065)

BGP Confederation という手法は、上記の Route Reflector よりも以前に考案された手法で結果的な効果として IBGP の数を減らすという結果を得ることができる。

BGP Confederation を利用した構成例を図 7-12 に示す。

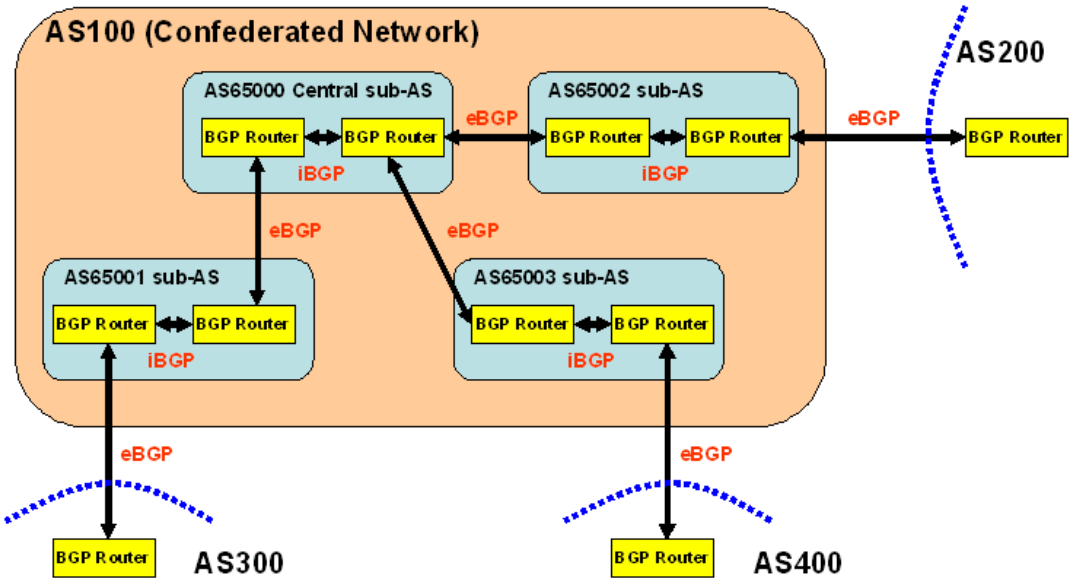


図 7-12　BGP Confederation

しかし、BGP Confederation の考え方は、Route Reflector とは異なり、AS 内部を複数の Sub-AS という AS に分割し、その Sub-AS のなかで独立した経路制御を実施することを推奨している。つまり、外部の AS から見れば通常の AS に見えるが、内部は、複数の AS があたかも小規模のインターネットのように BGP で接続されている状況といえる。これは、IBGP の接続数を減らすという単純な効果だけでなく、非常に大きな AS の場合は、各部署での経路制御ポリシを十分に反映させる方法として採用できるなどの効果もある。

■ Protection of BGP Sessions via the TCP MD5 Signature Option (RFC2385)

この RFC では、TCP の Extension を用いた BGP に対するセキュリティの拡張について記述されている。TCP のオプションでは、TCP セグメントに RFC1321[9]で規定される MD5 Digest を運ぶように設計されている。通常の TCP を利用した BGP セッションでは、何の暗号化もされていないことから、万が一の場合、BGP セッション自体を詐称されるなどの危険性があるが、この TCP MD5 認証方式を使うことで、その危険性から幾分か解消される。

■ Multiprotocol Extensions for BGP-4 (RFC2858[10])

この拡張は、BGP を IPv4 の経路制御だけではなく、ありとあらゆるネットワークアドレスや ID を転送する為の手段として利用できるようにした物である。

たとえば、IPv6 に対応した BGP は「BGP4+」と記されることが良くあるが、実体は、この Multiprotocol Extension を用い、アドレスファミリとして IPv6 を使っているに過ぎない。

このほか、この拡張は MPLS を用いて VPN を構築する際に、ラベルや MAC アドレスを転送するためにも利用することができる。

9 The MD5 Message-Digest Algorithm (RFC1321)
http://www.ietf.org/rfc/rfc1321.txt
10 Multiprotocol Extensions for BGP-4 (RFC2858)
http://www.ietf.org/rfc/rfc2858.txt

7.3. 最新経路情報

本節では、インターネットで実際に流れている経路情報について解説する。

最初に、インターネット全体で取り扱われている経路情報である「フルルート」の経路数の推移を紹介するとともに、フルルートの実態について解説する。以降、この情報を基本として、インターネットルーティングレジストリやインターネットレジストリからの割り振り状況との比較、1つの経路情報が複数の AS から広告される Multi-Origin Prefix の現状について、具体的な数字を挙げながら解説してゆく。

7.3.1. フルルートに関する状況

本節では、インターネットに流れている経路の実態について解説する。

なお、本節で利用する各種情報は特に断りが無い限り、株式会社インテック・ネットコアで取得したフルルートの情報を、経路情報を分析する独自のツールによって解析した 2006 年 1 月 26 日時点の結果を利用して紹介する。

図 7-13 にフルルートの経路数推移を示す。

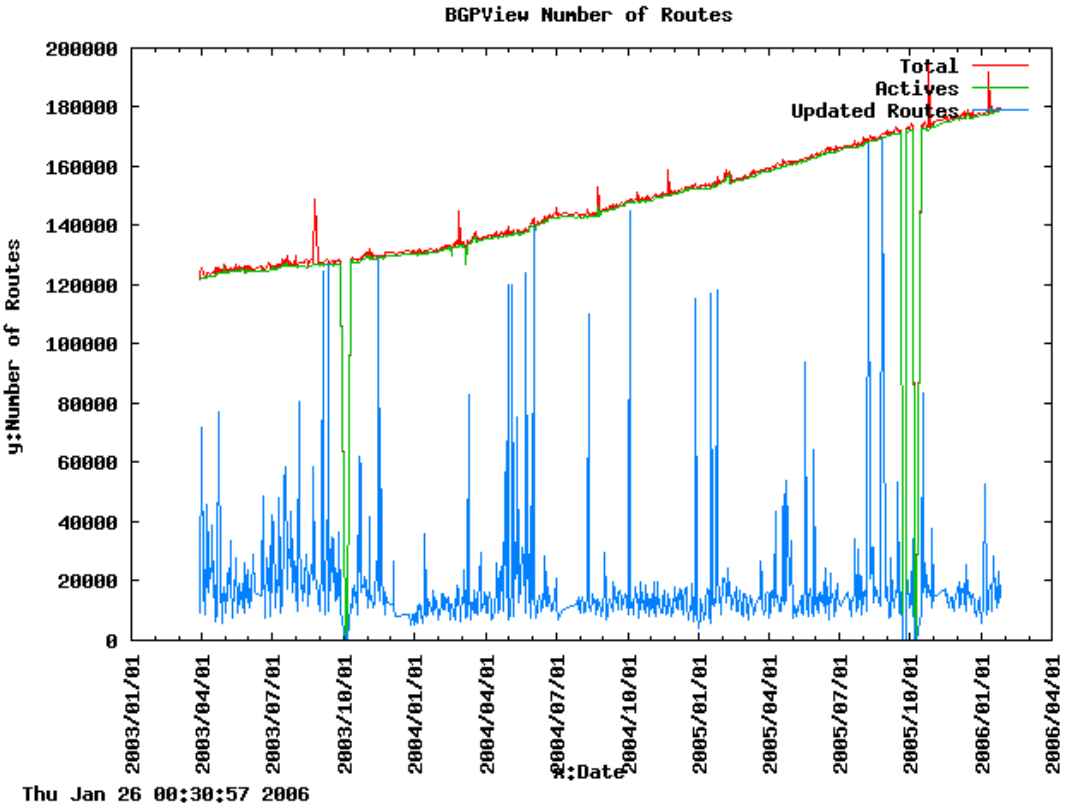


図 7-13 フルルートの経路数推移

グラフは、2003 年 4 月からの推移を示している。グラフでは、上部のなだらかな傾斜の線がフルルートの経路数を、下部の変化が激しい線がフルルートの中で 24 時間以内に更新が行われた経路数を示している。

フルルートの経路数は、グラフ作成当初の 2003 年 4 月において約 12 万経路程度だったが、グラフ作成時点の 2006 年 1 月の段階では約 18 万経路と 3 年間で約 6 万経路も増加していることがわかる。また、グラフの曲線から経路数は単調に増加傾向にあるのではなく、指数関数的に増加していることも推測できる。

一方、24 時間以内の更新される経路数の範囲は、測定開始当初からほとんど変化が無く、約 1 万から 2 万経路程度であることがわかる。

そこで、1日の経路更新数の推移を図 7-14 に示す。

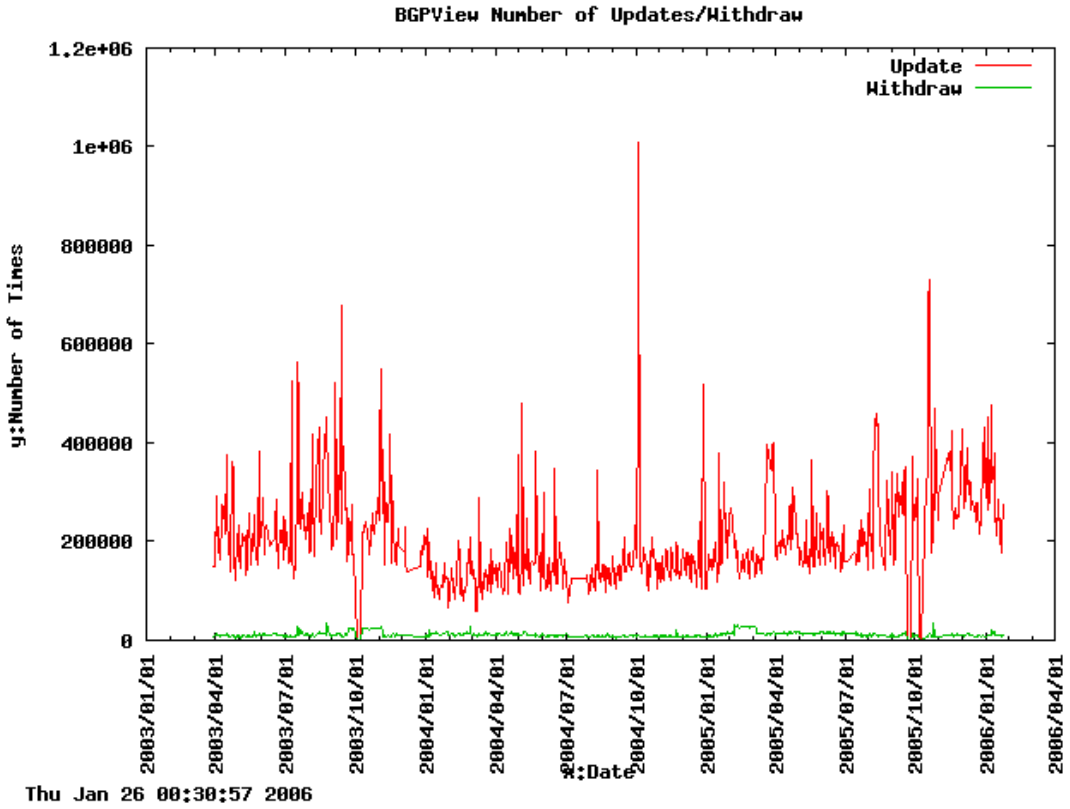


図 7-14 1 日の経路の更新回数の推移

この図では、経路更新数は 2003 年から現在に至るまで多少の変動はあるものの全体で約 2 万回の更新が行われ大きな変化が見られないことがわかる。

そこで、さらにこの更新される経路の内訳をプレフィックス長別に見たものを図 7-15 に示す。

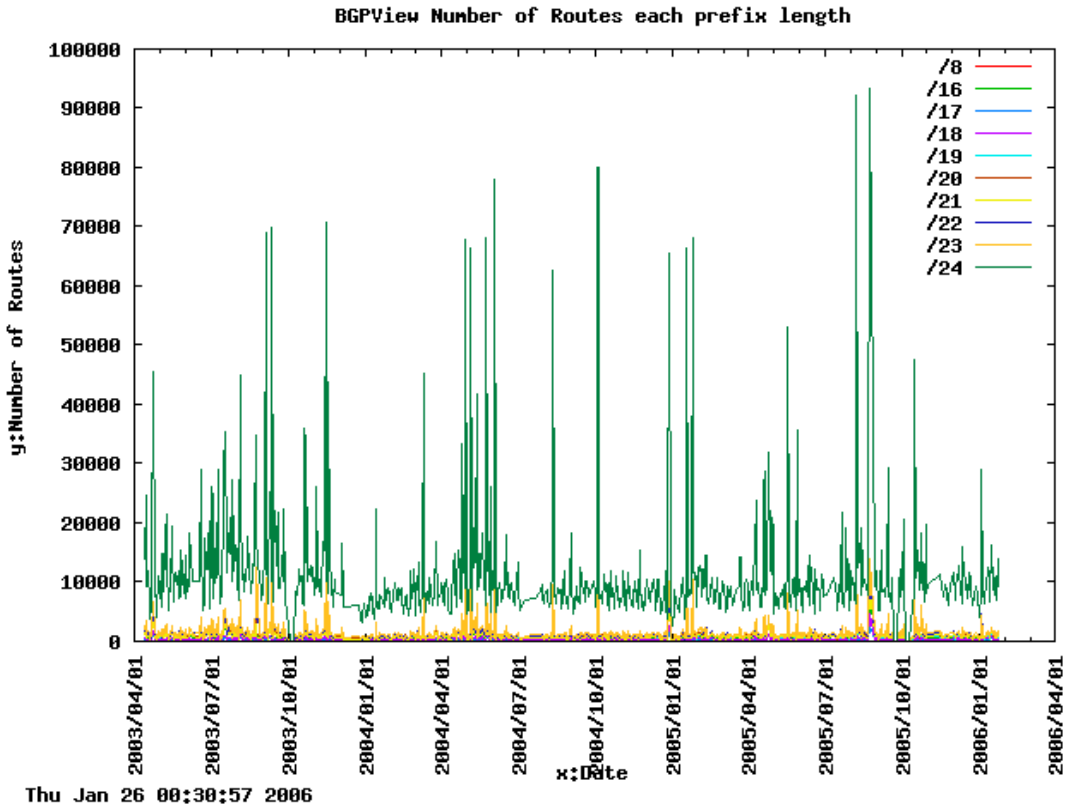


図 7-15 プレフィックス長別の経路更新数の推移

この図では、/24 の更新数を緑色で示しており、その数が他のプレフィックス長の更新回数よりも多く、約 1 万回から 1 万 5 千回で推移しており、その数に長期にわたってあまり変動が無いことがわかる。

つまり、経路数は指数関数的に増加傾向にあるが、そのなかで更新される経路のほぼ大半が/24 の経路であることがわかり、かつ、その更新回数は数年にわたって変化が無いことがわかる。

さて、一方でその経路を流す組織数を AS 単位で見た数、つまり Origin AS の数の推移を図 7-16 に示す。

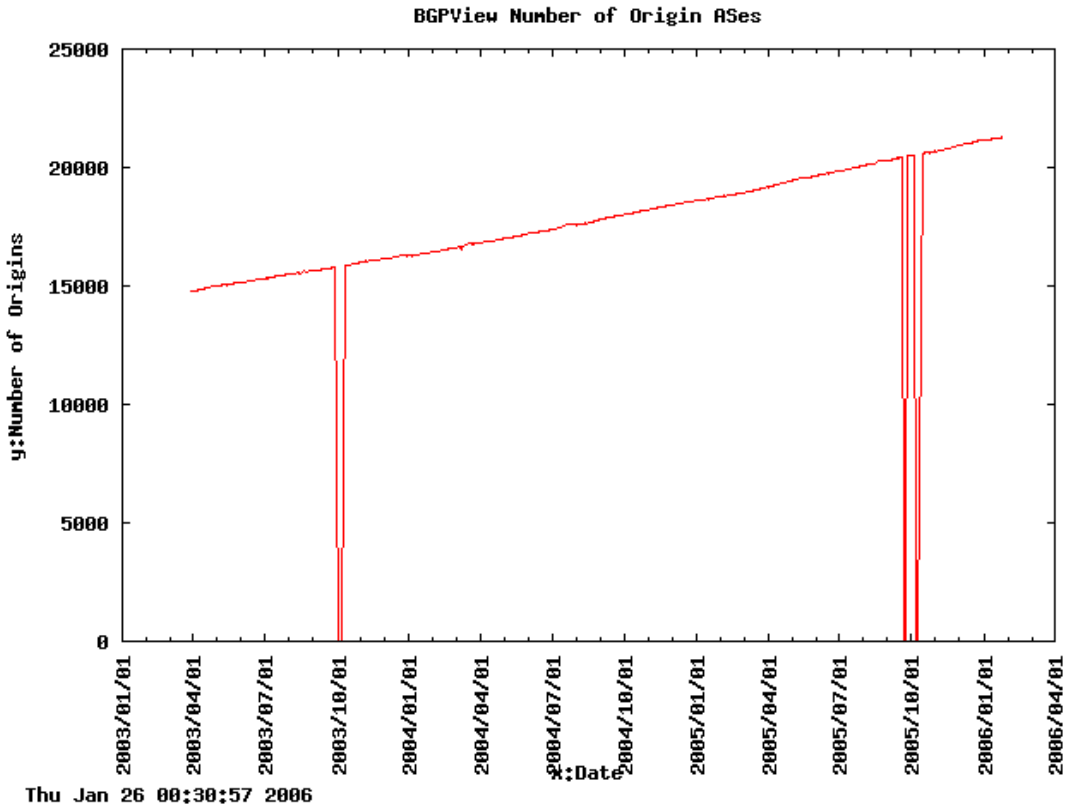


図 7-16 Origin AS 数の推移

図中に2箇所ほど 0 に落ち込んでいるところがあるが、これはデータの取得が失敗している部分であり無視できる。この図によると、2003 年の段階では約 15000 の AS が経路を広告していることがわかり、その数は 2006 年の段階で約 20000 にまで増加している。つまり、3年間で約 5000 の AS が新たにインターネットに接続し、経路の広告を開始したことになる。

この増加傾向と経路数を比較するために、一つの AS が広告する経路数の平均値の推移を図 7-17 に示す。

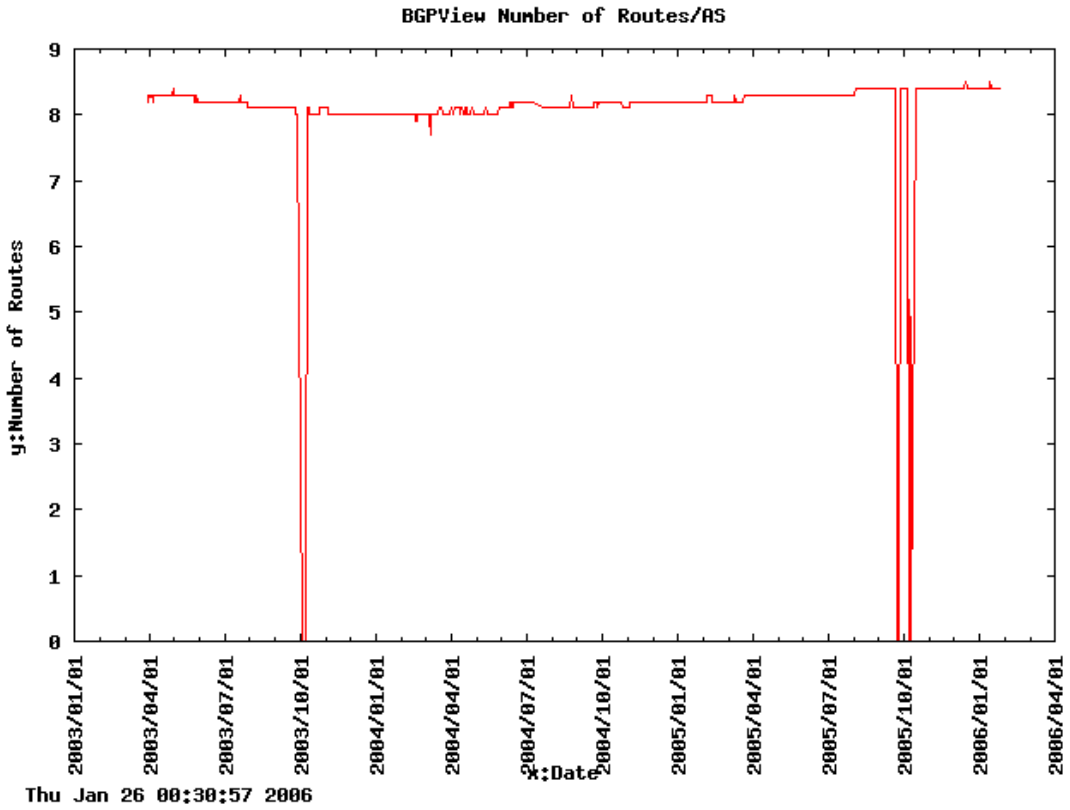


図 7-17 1AS あたりの経路広告数の平均値の推移

図のとおり経路数、Origin AS 数ともに増加傾向にはあるものの、1AS あたりが広告する経路数の推移は約 8 から 9 経路とその数に大きな変化が無いことがわかる。

これらのフルルートとその経路の内容が示す状況として、経路数や AS 数については、増加傾向にあるが、各 AS が取り扱う経路数については、2003 年以降大きな変化は見られないこと。そして、インターネット全体で日々更新される経路数についてもプレフィックス長が/24 のものが多く更新されるものの、更新数は 2003 年以降それほど大きく変化がなく、経路更新という観点から見たインターネットの安定性ついては、大きな変化が見られないことが理解できる。

7.3.2. パンチングホール経路の実態

前節では、流れている経路数そのものに注目してデータを見てきた。本節では、流れている経路の重なり具合を見ることにする。

あるネットワークまでの経路を表す経路情報は一つのネットワークに対して 1 つの経路情報があれば、基本的に問題がない。しかし、インターネットに流れるトラフィックをきめ細かく制御したり、接続事業者の運用上の方針などにより1つのネットワークに向かう経路を分割するなどして複数流したりすることがある。特に、192.168.0.0/16 という経路に 192.168.1.0/24 という重ね合った経路を流した場合に 192.168.1.0/24 は 192.168.0.0/16 のパンチングホールな経路ということができる。

経路制御上、このようなパンチングホール経路は正しく運用されている場合がほとんどだが、経路制御の特徴である Prefix 長[11]が長いほど優先させるという最長一致の原則を逆手にとり、Prefix 長の長い経路を故意にインターネットに流し、経路を横取りするケースもある。

ここでは、悪意のあるなしにかかわらずこの様なパンチングホールの経路がどれくらいあるのかを図 7-18 に示す。

11 本章では他の用語との関係をわかりやすくするため、「プリフィクス」を「Prefix」と表記する。

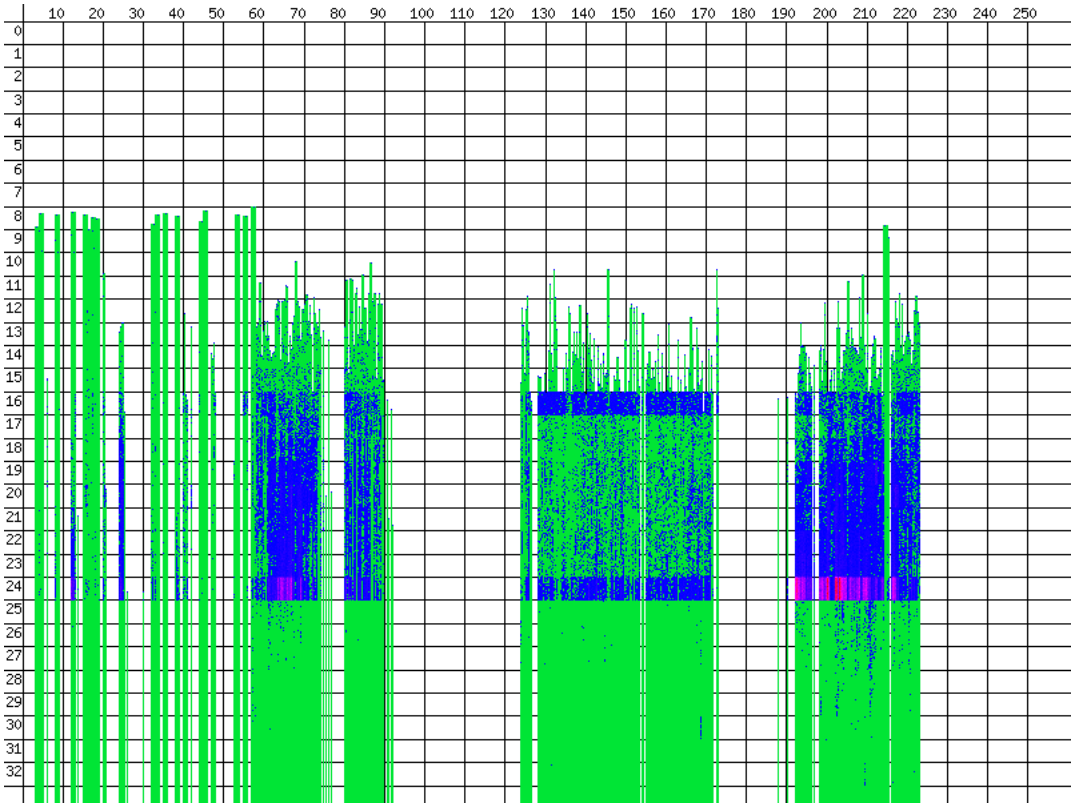


図 7-18　パンチングホール経路の状態

この図は、http://micho.mimora.com/routegraph/に紹介されている大久保氏が作成した経路を図化するツールを用いて描画している。

この図は、1つの経路が1つの点で描画され、横軸にIPアドレスの第一オクテットが表現され縦軸がカバーされるPrefix長となっている。また、1つの点は緑が基本で、複数の重なり合った経路があるほど、青や紫など色が濃くなってくように表現されている。

この図をみると 192/8 当たりに/24 の経路密度が多くなっていることが解る。このほか、青色のところが、ある経路に対するパンチングホールだと考えると、インターネットに流れている経路の広範囲にわたってパンチングホール経路が広告されていることが解る。

このようなパンチングホールが、意図的に正しく流されているのであれば全く問題はない。しかし、悪意を持って流された場合には問題となるが、この様なパンチングホール経路が正しいかどうかを判定することは通常非常に難しいと言える。

7.4. アドレス資源管理と経路

本節では、アドレス資源がどのように管理されているかについて解説する。

最初に、IP アドレスが同様な組織によってどういう形態で管理されているかを解説する。次に、その管理方針の考え方、その歴史について報告し、日本独自で持つ特殊方針の歴史についても言及する。

最後に、IP アドレスの管理と実際にその IP アドレスが経路情報という形でネットワーク運用の現場でどのように使われているか、そしてどのような乖離があるのかについて解説する。

7.4.1. アドレス資源管理の構造

IP アドレスは、IPv4 の場合、32 ビットの数値で表現可能な有限な資源として管理されている。インターネットの資源、つまり、インターネットで利用されるドメインや番号は、ICANN[12] (図 7-19) によって中心的に管理されており、その下部組織や管理を委譲された組織、そしてそれらの関係組織によってより細かい管理と運用がなされている。

特に番号関係については、ICANN の下部組織である IANA[13]にその管理がゆだねられている。

[12] Internet Corporation for Assigned Names and Numbers の略であり、民間の非営利団体です。(http://www.icann.org/)
[13] Internet Assigned Numbers Authority の略。

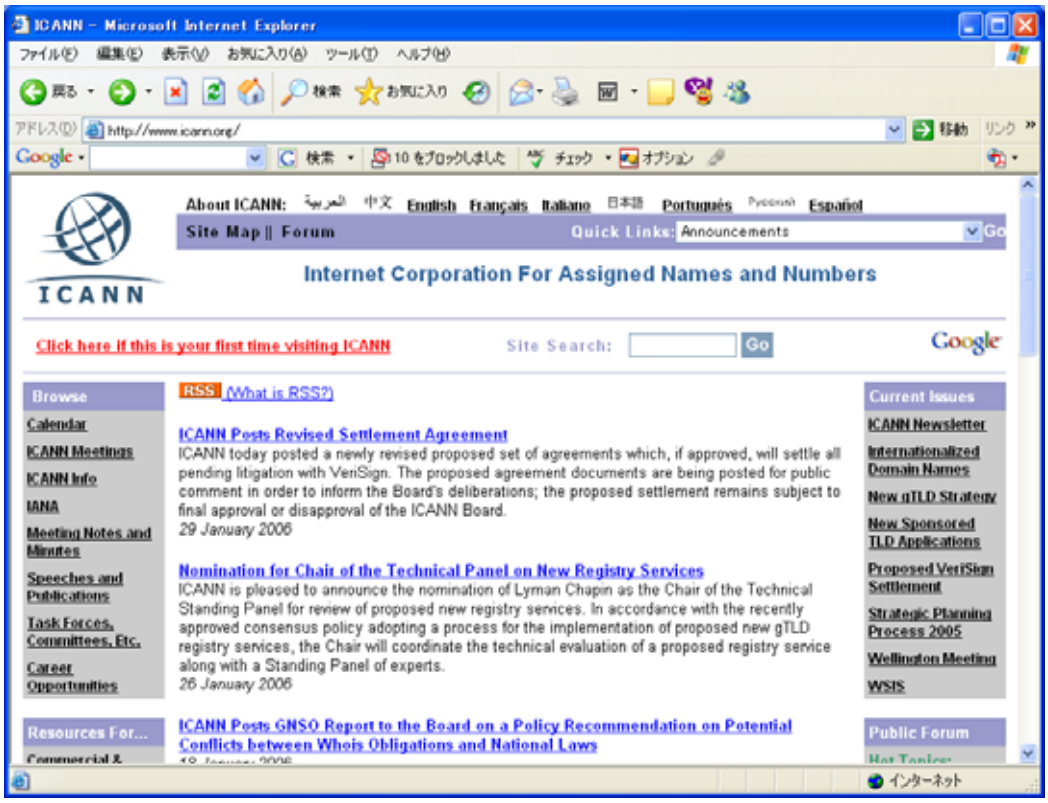


図 7-19 ICANN のホームページ

IANA では、/8 単位で IP アドレスの管理、つまり IP アドレスの上位 8 ビットだけを識別子として管理しており、それ以上の細かい管理は地域レジストリ(Regional Internet Registry : RIR)によって管理されている。

RIR は、管轄地域が分かれており、現在のところ ARIN(American Registry for Internet Numbers)、RIPE NCC(Réseaux IP Européens Network Coordination Center)、APNIC(Asia Pacific Network Information Center)、LACNIC(Latin American and Caribbean Network Information Center)、AfriNIC(African Network Information Center)の5つの RIR が存在する。

アドレス資源は、これらIANAとRIRを中心に階層的な構造を用いて管理しており、その階層図を図 7-20 に示す。

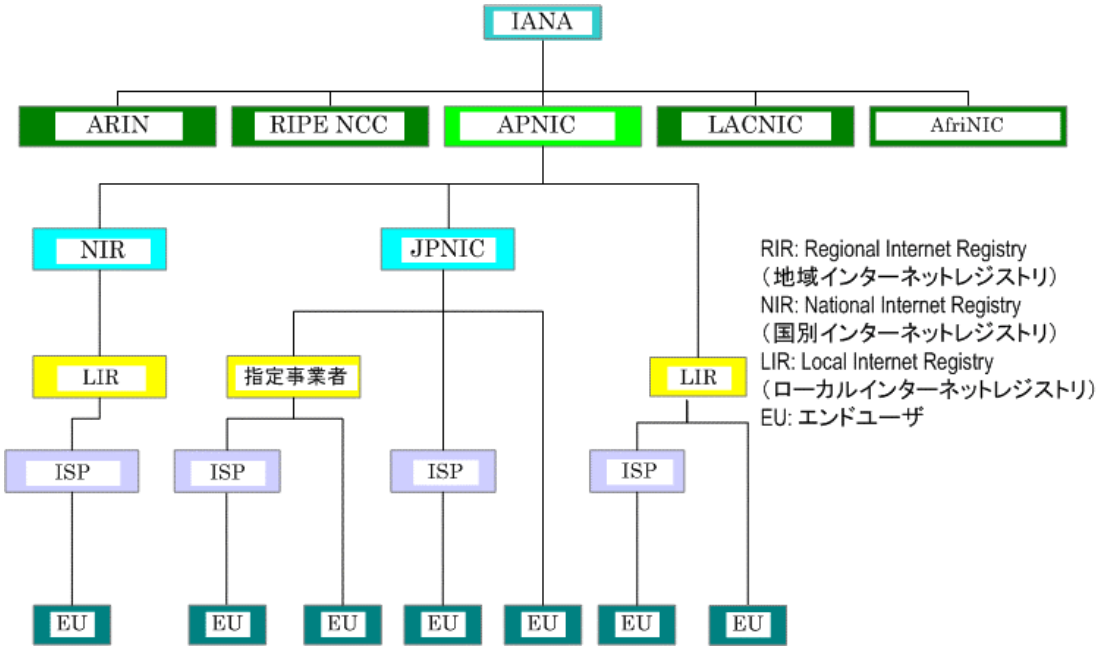


図 7-20　インターネットレジストリの階層構造

この図のように、IANA から RIR のアドレス資源管理は委譲され、そこから LIR と呼ばれる Local Internet Registry にさらに委譲され、最終的に ISP やエンドユーザーにアドレス資源が割り当てられ、世界中で唯一の IP アドレスとして利用することができるように管理されている。

ただし、APNIC および LACNIC においては、地域の中に多数の国が異なる文化を持ち成り立っている地域として、国別のインターネットレジストリである NIR(National Internet Registry)という、もう一つの中間階層が存在している。JPNIC もこの NIR に当たる。

NIR では、基本的に RIR の定めるルールに則った運用が求められているが、国毎に異なる特殊な事情を勘案し、より地域に根ざした方針を策定するための調整が行われている。

7.4.2. IP アドレス管理ポリシの考え方

前節では、アドレス資源管理機構の階層構造について述べた。これらの各 RIR では、アドレス資源を公平かつ効率的に分配するために、アドレス管理ポリシを策定している。

アドレス管理ポリシでは、アドレス資源を公平かつ効率的に分配すると同時に、各地域での特殊事情を勘案して策定されているが、それぞれの RIR が策定するアドレス管理ポリシの基本方針が異なると、地域格差が生まれたり、公平さが失われたりする可能性がある。そこで、IETF では、RFC2050[14]にて、このアドレス管理ポリシを作成するにあたって3つの目標を定めている。

以下に、ここで定める3つの目標について記載する。

(1) 節約

グローバルに一意なインターネットアドレス空間を、それらのアドレス空間を利用して運用されている ISP やエンドユーザーの必要に応じて、公平に分配すること。

アドレス空間をより長く利用できるようにするために、アドレス空間の先取りをさせないようにする。

(2) 経路制御適応性

グローバルに一意なインターネットアドレスを階層的に分配することで、それらのアドレスの経路制御的スケーラビリティが保たれる。インターネット内の経路制御が正しく動作するためには、このようなスケーラビリティが必要である。

ただし、IPv4 アドレスが割り当てられたからといって、経路制御に対する適応性が保証されるわけではない。

14 INTERNET REGISTRY IP ALLOCATION GUIDELINE (RFC2050)
http://www.ietf.org/rfc/rfc2050.txt

(3) 登録

> アドレス空間の割り振りや割り当てを記録する公的レジストリの提供。これは、アドレスの一意性を保証し、インターネットのトラブル対策のあらゆる場面で必要な情報を提供する。

また、この RFC ではこの目標に続いて以下の様にも記載されている。

> 上記の目標は、インターネットコミュニティ全体で満たされるべきものである。ただし、「節約」と「経路制御適応性」は対立しがちな目標であるという点に注意すべきである。さらに、上記の目標は時として個々のエンドユーザーまたはインターネットサービスプロバイダの利益に反する場合がある。したがって、個々のケースに応じて状況を注意深く分析し、判断して、適切な折衷案を見いだす必要がある。

このように、RFC2050 では、基本的な管理方針をガイドラインと示し、各 RIR がそれにそって地域ごとのアドレス管理ポリシを策定して運用できるようにしている。これにより、時代の変化によるニーズを吸収し、アドレスポリシを変更しながら長期にわたって共通の目標に向かって、アドレス資源の管理を行うことができるようになっている。

7.4.3. IP アドレス管理ポリシの変遷

インターネットが米国政府の強力な財政的援助を受けて発展していた 1990 年代初頭までは、NIC といえば世界で唯一の”The NIC”（SRI-NIC、あるいはその後身の nic.ddn.mil）を指していた。The NIC は、アドレスの取得やネームサーバーへの登録など、全世界からの申請を一手に引き受けて処理していた。

しかし、インターネットの急速な発展によって、この集中管理型の NIC 構造に変化が生じてきた。NIC に階層構造をもたせて、グローバルな The NIC から地域的な NIC への管理業務の分散化が図られるようになったからである。具体的には、従来 The NIC が各組織に対して直接割り当てていた IP アドレスをブロック化し、割当て業務を地域ごとの NIC に委任するようになった。この措置には、IP アドレスの地域的なまとまりを重視した CIDR という新しい経路制御技術の導入に対応する意味もあった。

1992 年 4 月には、ヨーロッパ地域を統括する RIPE（Réseaux IP Européens）の NCC（Network Coordination Center）が発足した。さらに 1993 年 4 月、The NIC は InterNIC として新たなスタートを切った。現在、InterNIC はグローバル NIC としての役割を引き継ぐととも

に、北米および周辺地域の NIC としても機能し、RIPE NCC などと協調しながらサービスを実施している。

このような状況のなかで、1993 年 1 月にホノルルで開催された APCCIRN（Asia-Pacific Coordinating Committee for International Research Networking：アジア・太平洋地域国際研究ネットワーク調整委員会）会議において、アジア・太平洋地域の NIC にあたる APNIC 設立に向けた調査・実験が提案された。APCCIRN の参加各国のあいだでも、このような地域的 NIC の発足を望む声が多かったため、APNIC の実験プロジェクトが開始されることになった。1993 年 8 月にサンフランシスコで開かれた APCCIRN 会議では、実験プロジェクトの期間を 1993 年 9 月～1994 年 6 月と定め、実験プロジェクトに関する報告を同会議でおこなうことが確認されている。

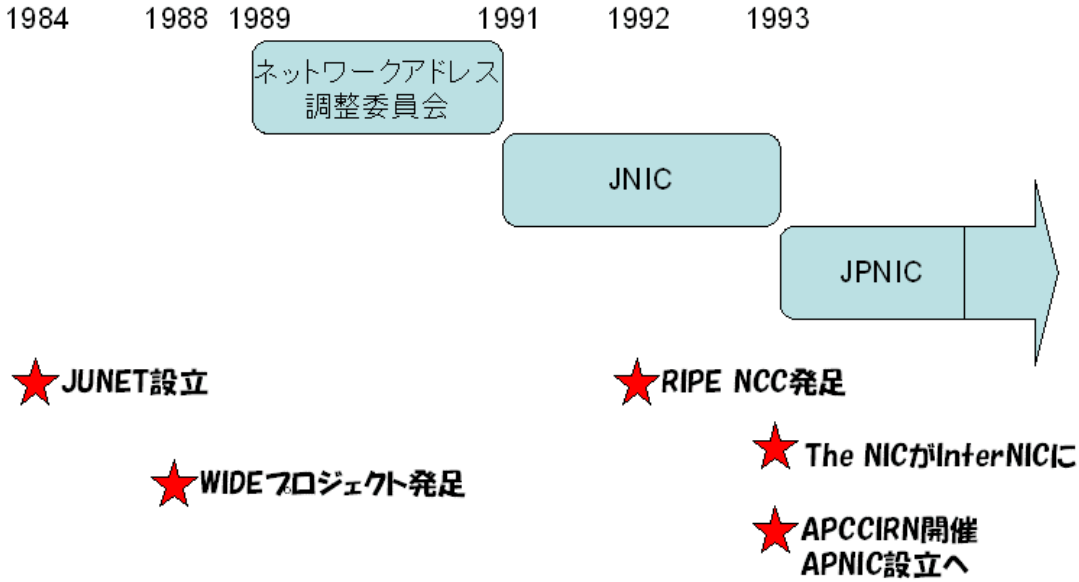


図 7-21 IR の歴史と出来事

APNIC は世界のレジストリの中でどのように位置づけられるかについては、図 7-20 に NIC の階層構造で示したとおりである。

地域インターネットレジストリの基盤が整備された当初、世界を北米、ヨーロッパ、アジア・太平洋を中心とする 3 つの地域に分け、それぞれを代表する地域 NIC（National Internet Registry）を設ける方向で議論が進められた。

この構想にもとづいて APNIC が正式に発足し、日本の国内 NIC（図 7-20 では National

Internet Registry) である JPNIC は、APNIC の下で相互に協力や支援をおこないながら機能していくことになったのである。そこで、JPNIC では、APNIC 実験プロジェクトに対し JPNIC 運営資金の 10%を上限として資金/資源を供与することとし、APNIC の発足に可能なかぎり協力する旨、合意され APNIC が設立されたのである。

その後、地域レジストリには、アフリカを担当する AfriNIC、ラテンアメリカを担当する LACNIC がさらに設立され、現在の 5RIR 体制として活動している。この様子を図 7-22 に示す。

図中にあるように、LACNIC は、主に ARIN の担当地域だったラテンアメリカ地域の管理を引き継ぐ形で新設され、同様に AfriNIC は、主に RIPE NCC が担当だったアフリカ地域の管理を引き継ぐ形で新設されたのである。図中では、ARIN が明確に ARIN と LACNIC に、RIPE NCC が RIPE NCC と AfriNIC に分割されたように表現されているが、実際には、多少の地域のずれがあることを付け加えておく。

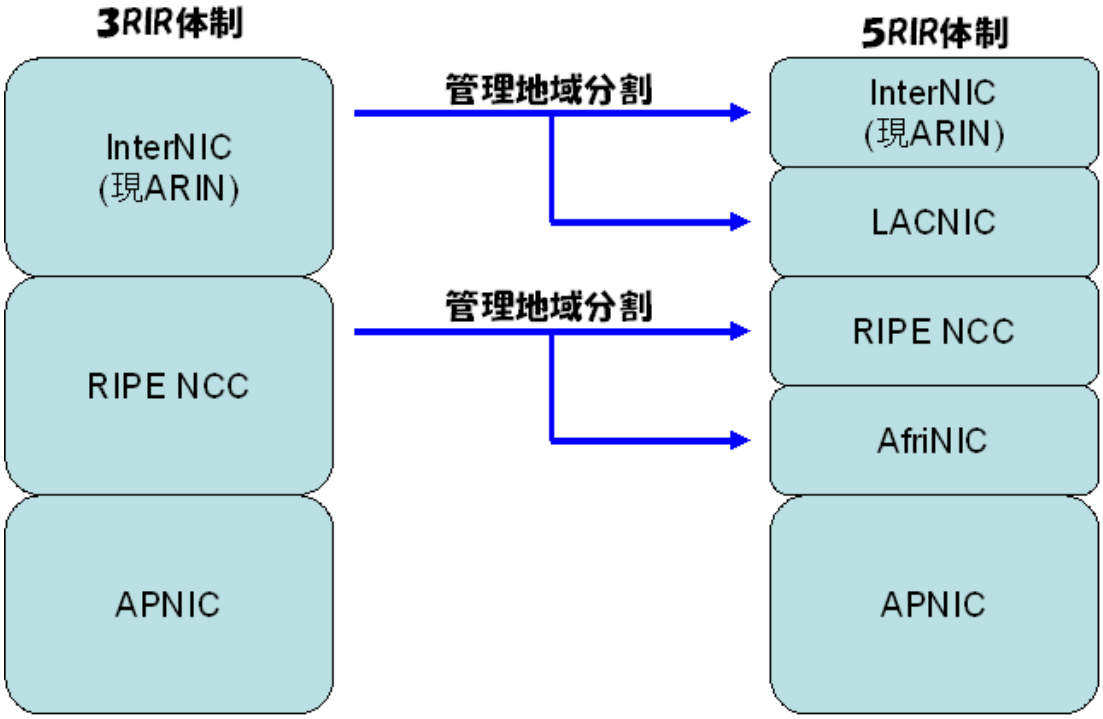


図 7-22　3RIR 体制から 5RIR 体制へ

一方、日本では、1984 年の JUNET 設立がその発端となる。JUNET は、東大、東工大、慶大を結んだ研究用のネットワークで、当時は UUCP をベースとして行われていた。その後、

1988 年に WIDE プロジェクトが開始され、日本でのインターネットの研究に加速がかかった。1989 年には、本格的にアドレスの管理を行うための「ネットワークアドレス調整委員会」が設置され、日本でのアドレスの管理が始まった。

その後、JNIC が 1991 年に発足し、アドレスの管理がネットワークアドレス調整委員会から引き継がれた。

さらに、インターネットの利用が加速され、1993 年には、JNIC は日本におけるサービスをより拡充するため、ネットワークプロジェクトを会員とする任意団体である JPNIC へとその姿を変え、その後社団法人化され、現在の形となっている。

図 7-21 に関連する出来事をまとめておく。

7.4.4. ローカルレジストリの特殊ルール

IP レジストリは、現在世界を5つの地域に分け、各地域に RIR を設置してアドレスの管理活動を行っている。そもそも、アドレスの割り振りなどにはインターネットの利用状況なども勘案した地域的な考慮が必要であり、それらの地域に依存する事柄は各地域レジストリの管理ポリシで吸収している。

特に、アジア太平洋地域の場合は、国数も多くまた経済状況もまちまちであり、APNIC における一つの運用ポリシで行うよりもさらに国別の考慮を行った国別レジストリが必要とされ、国によっては JPNIC の様な国別レジストリが APNIC のさらに下位層のレジストリとして活動をしている。

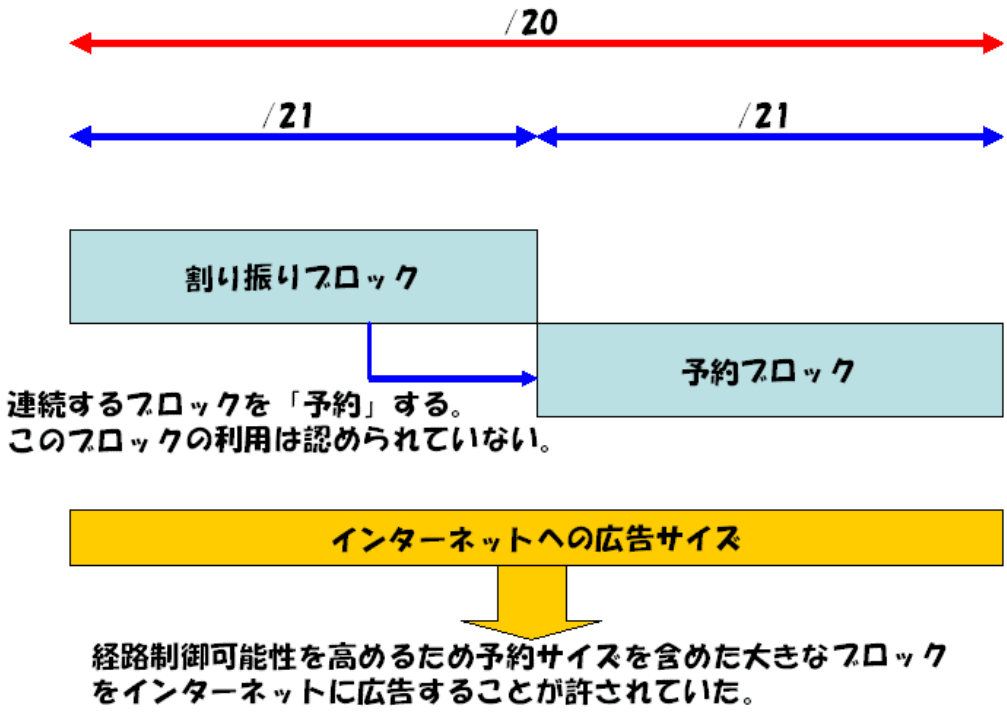


図 7-23　予約割り振り

これらのレジストリでは、RFC2050 や APNIC などの管理ポリシ、そしてインターネットの運用状況なども勘案しながら、地域に適切なローカルポリシの策定を行いる。日本の場合には、過去に「予約割り振り」というローカルルールが存在していた。予約割り振りについては図 7-23 に示しておく。

JPNIC が発足した当初は、まだ日本のインターネットは聡明期で、現在のように大規模な ISP が少なかった。さらに、レジストリからの最小割り振り単位は/20 などの比較的大きなものだったため、アドレスを割り振ってしまうとかなりの量が利用されずに死蔵されるのではないかとの懸念があった。さらに、当時のインターネットの経路制御では、細かい経路は経路フィルタで排除する等の措置も執られており、細かいアドレスを割り振り、経路制御性に問題が発生することも考えられた。そこで、JPNIC では、アドレスを割り振る際に、APNIC で定める最小割り振り単位のブロックを「予約」として扱い、その中から、/21 などの細かいアドレスブロックを割り振っていたのである。これが、予約割り振りが実施されていた経緯である。

その後、日本のインターネットも発展し、アドレスの需要も伸び、さらに、APNIC での最小割り振り単位もさらに小さくなったことから、この「予約割り振り」という制度は廃止されたのである。

7.4.5. 割り振り済みアドレスと経路情報

IP アドレスが ISP 等に割り振られ、それらすべてのアドレスが利用されるのが、アドレスを利用する最大効率である。しかし、経路制御性を考慮したり、ISP がサービスを続けてゆくためにあらかじめ取得するアドレスなどを考慮したりすると割り振ったすべてのアドレスを利用することは大変困難である。

本節では、割り振ったアドレスが実際どれくらいの割合で利用されているかを、インターネットに流れている経路から探ってゆく。

まずは、割り当て・割り振り済みブロックに対す経路情報カバー率について表 7-1 に示す。表中の「調査 prefix 数」は、レジストリから割り振られた「数」で、Prefix 長を考慮しないブロック数を表す。「(/24 にすると)」は、Prefix Length の長さが/24 のものとして換算した数を表す。

表 7-1 割り当て・割り振り済みブロックの経路広告カバー率

	PA		PI	
調査prefix数	1,937	100.00%	2,906	100.00%
(/24にすると)	134,140	100.00%	151,414	100.00%
exact matchのprefix数	1,060	54.72%	931	32.94%
(/24にすると)	100,508	74.93%	93,957	62.05%
広告されているprefixを/24にすると	130,446	97.25%	95,551	63.11%
広告されてないprefixを/24にすると	3,694	2.75%	55,863	36.89%

(JPNIC “経路情報の登録機構の検証”専門家チーム・メンバー 吉田友哉氏の資料より)

表の中では、カバー率を示すために PI と PA の二つに分けている。これは、インターネットレジストリが割り振り・割り当てを行っているアドレスには大きく、Provider Aggregatable(PA)と Provider Independent(PI)の 2 種類があるためである。グローバルにユニークな IP アドレスであるという点については基本的な特性に違いはないが、PA は ISP 等のさらに下位層のエンドユーザーに対してアドレスを割り当て、それらを集約 (Aggregate) する役割を担っているアドレスブロックであり、PI はそれら集約の役割を担わずに直接エンドユーザレベルに対して割り当てるためのブロックをさしている。

現在では、レジストリから割り振られるアドレスのほとんどが PA であるが、歴史的な理由や、特殊な用途のために PI が割り当てられているケースがある。特に、CIDR 以前に割り振られたアドレスを歴史的 PI とよび、特別に扱うケースもある。このため、PI は割り振られたネットワークでの実際のアドレス需要を適切に判断しなくて良い時代に割り振られているケースのものが多く、実際の利用率も低くなっていることが理解できる。

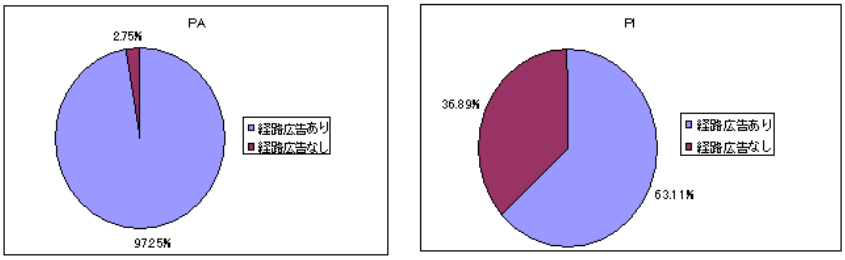
この PI、PA という前提を含めて表を再び解説する。

レジストリから割り振られるアドレスは、特に PA では ISP で集約可能な比較的大きなアドレスブロックになっている。理想的には、この割り振られたサイズそのままをインターネットに経路情報として広告することが望ましく、これにより経路数の爆発が抑制されることが期待できる。

このとき、すでに割り振ったブロック数は、PA で 1937、PI で 2906 となる。これに対し、割り振りブロックサイズがそのまま経路情報として流れているケースは、PA で 1060、PI で 931 であり、PA ですら 54%にしか及ばない。しかし、/24 換算で見た場合、PA で 75%、PI でも 62%とカバー率は高くなる。これは、多くの割り振りブロックが、割り振られたサイズそのままでインターネットに経路広告されているわけではなく、経路制御の都合などで、分割して広告されているという状況が推測できる。

PA と PI の比較についてさらに細かく対比したものを図 7-24 に示す。

- PA
  - ほぼ経路広告されている
  - 経路広告が無いアドレスは、現在広告準備中のものも含まれているので、経路広告ありの比率は実際にはこれ以上になるかもしれない
- PI
  - 6割程度しか広告されていない
  - Exact match で広告されているprefixの経路広告割合が62.05%で、全体の広告率（＝63.11%）に近い≒広告 or 未広告の結果になっている（後述の結果詳細を参照）



(JPNIC “経路情報の登録機構の検証”専門家チーム･メンバー　吉田友哉氏の資料より)

図 7-24　PA と PI の経路広告カバー率の比較

図にもあるように PA は、インターネットレジストリによってアドレスの利用効率を十分に考えられ運用されているブロックであるため、非常に利用効率が高いことが解る。一方、PI は利用効率が良くないことが解る。

注意したいのは、今回のこの評価はあくまでインターネットに流れている経路情報に対して、レジストリが割り振ったアドレスを重ね合わせたにすぎないということである。IP アドレスは、グローバルに一意性を保証して割り振り･割り当てを行うもので、本来、グローバルな経路表にそのアドレスを載せることが目的ではない。

実際には、インターネットに対する接続性を持たないが、多くの顧客を抱えるネットワークでは、プライベートアドレスの重複を避けるなどの目的で、一意性を確保する必要があり、レジストリからグローバルアドレスが割り振られているケースもある。このようなアドレスは、今回の調査のなかでは「未使用」に分類されてしまう。このため、PA、PIの利用率は、実際にはもう少し高くなると考えられることを付け加えておく。

7.4.6. レジストリによる割り振りと経路情報の溝

本章では、アドレスという資源の管理について述べ、それらのアドレスがインターネットの運用の現場に経路情報としてどのように扱われているかについて述べてきた。

本章で明らかにしたことは、アドレスの割り振りポリシは、時代背景と共に様々な変遷を遂げてきたこと、そして、それら割り振られたアドレスは、その時々で最大のパフォーマンスを出すようにアドレス割り振り・割り当てポリシを運用する現場で利用されてきたことである。

この割り振りポリシとその運用は、RFC2050 で扱われているように、効率的な割り振りと経路制御可能性という面でしばしば対立しがちである（図 7-25）。その背景を表しているのが 7.4.5 節で解説した割り振りブロックと経路情報の対比である。

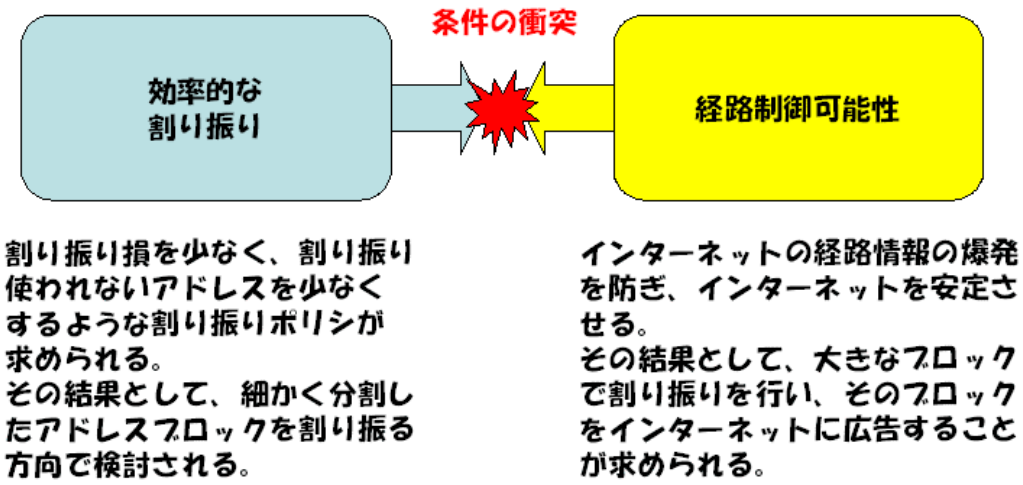


図 7-25　アドレスポリシの衝突する考え方

たとえば、レジストリのアドレス割り振りの運用現場では、割り振り効率を上げるために、/24 単位での割り振りが実際に行われていたのである。アドレスを割り振るという現場での運用は、この判断は非常に正しい判断だと言えるだろう、一方、経路制御と言う観点からは、/24 を 3 個と割り振られた場合には、/23+/24 という 2 つの経路として広告しなくてはならなくなるのである。逆転の発想で言えば、このような割り振りが行われていたために、割り振りサイズがそのままインターネットに広告できないという事態を引き起こしたのだともいえるのである。

現時点では、経路制御可能性とアドレスの割り振りの効率の両方が融和され、このようなことが少なくなってきているが、割り振り効率と経路制御可能性という2つの異なる目的を、同一のポリシのなかで運用することは困難といえ、異なるポリシの中で調和のとれた運用を行うような調整が今後も必要となっていくだろう。

7.5. インターネット経路制御の問題点

IP アドレスは、レジストリによって管理され適切な手続きによって ISP などの IP アドレス利用者に割り振られる。この手続きによってISPはグローバルユニークなIPアドレスを利用可能になり、このグローバルユニークな IP アドレスを利用してインターネット接続を行い様々なサービスが行われている。

割り振られた IP アドレスは、最初に BGP を利用して世界中に自分に割り振られたアドレスがインターネットに接続したことを広告する。BGP に対するアドレスの広告は、先にも述べたように経路広告といい、通常インターネットの接続サービスを提供する ISP 等に接続して、その ISP 経由で行われている。広告された経路は接続先 ISP を通じて世界中に伝搬しゆくのである。

しかし、この経路の伝搬には様々な問題がある。本節では、これらの問題点について解説し、現状での問題の解決方法について触れてゆく。

7.5.1. BGP 運用の根本的問題

先ほどの述べたように、インターネットに広告した経路は BGP を利用して世界中に広告される。これは、BGP を利用して世界中に点在する AS に伝搬してゆくことによって行われている。

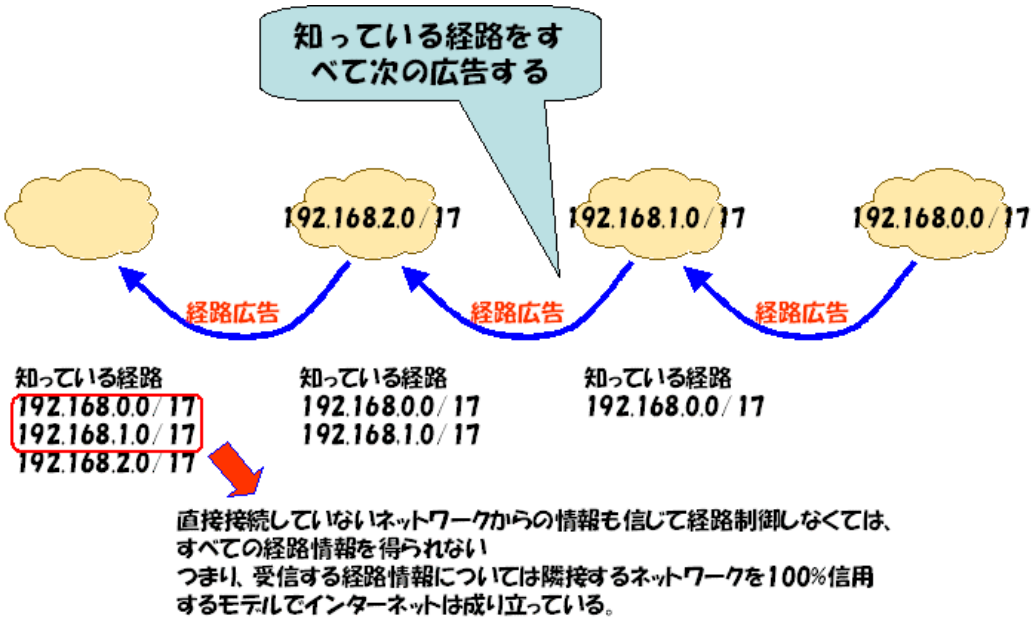


図 7-26　BGP の隣接ネットワーク信用モデル

そこで、いったん BGP での経路広告はどのように行われているかに戻って考えてみることにする。

BGP の経路広告は、異なる AS 間で BGP 接続を通じて、自分のネットワークが転送可能である転送先のアドレス情報を経路情報として、接続相手に広告するということである。一方、経路を受ける側は、自分が転送しようとしているパケットの転送先を他の AS から広告された経路情報によってのみ解決して転送してゆくことになる。この様子を図 7-26 に示す。

ここで問題となるのが、「他の AS から広告された経路情報のみによって解決」されるということである。BGP の世界では、この「他から広告された経路情報」をさらに他の AS に自分が転送可能なアドレス情報として広告するということを繰り返して経路情報が伝搬してゆくのである。これは、必ずしも自分が受信した経路情報が隣接する直近の AS、つまり自分の AS と直接接続している AS が広告した経路情報が必ず到達可能であるということを保証していないのである。

性善説に基づいて BGP の世界を考えた場合、つまり、経路の広告主 (Origin) は必ず正しい経路情報を広告し、経路を転送する途中の AS ではその情報に広告主に到達不可能となるような不正な変更を加えずに経路を転送するという場合には、現在の BGP のモデルでは何ら問題なく動作する。

しかし、これを性悪説で考えた場合には、いくつかの問題が生じてくる。考えられる状況を以下に列挙する。

(1) 広告主は、自分が割り振られている以外の経路情報を広告する。

先にも述べたように自分が経路情報として広告可能な経路情報は、自分がインターネットレジストリから直接割り振られたアドレス、もしくは、その管理権限があるアドレスに対する経路情報と考えるのが妥当である。

しかし、何らかの理由により、自分が管理すべき経路情報以外の情報をインターネットに流すことによって、未使用のアドレス空間を不正に利用したり、他の AS が利用中のアドレスを利用したりすることができるのである。

特に、他の AS が利用中のアドレスに対する経路情報が、関係のない AS から不正に広告された場合には、利用者が目的のネットワークにアクセスできなかったり、場合によっては犯罪に利用されたりする可能性もある。

この様子を図 7-27 に示す。

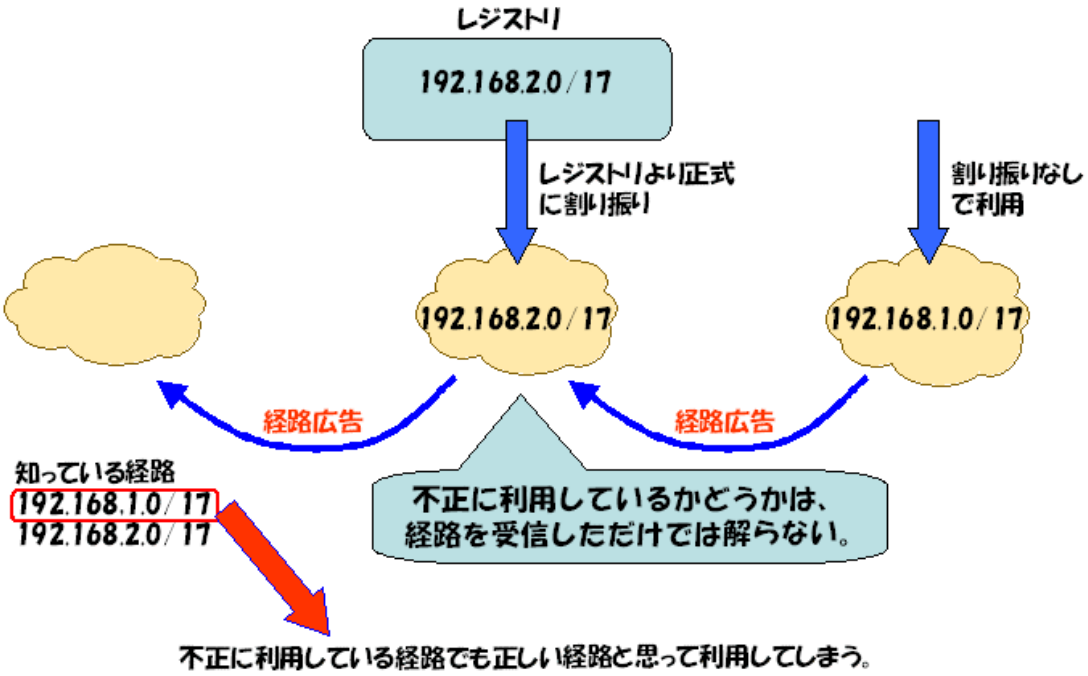


図 7-27　割り振られていないアドレスを利用する例

(2) 経路転送する途中の AS が、広告主を偽るような経路情報の改ざんをする。

BGP は、自分がパケットを転送可能なネットワークの情報を他の AS に経路情報という形で伝えるものあり、この繰り返しによって経路を世界中に転送している。つまり、ある AS に到達する自分の AS の経路情報は、複数の AS をまたがって転送されていることになる。

しかし、悪意を持ってこの転送を行うと、自分が受け取った経路情報を不正に改ざんして、他の AS に転送してしまうことが可能となる。この場合も(1)と同様な被害を考えることができる。

この事象に関する詳しい説明は、7.5.2.2 節で解説する。

(3) 意図的にインターネットを乱すためにある AS が経路情報を不正に流出する。

BGP 接続をしている AS は、自分を広告主としてしまえば事実上どのような経路情報もインターネットに広告可能である。しかし、ルータは制限のあるメモリ量、制限のある CPU 資源などを持った機器で構成され、不用意に大量の経路情報を送り込んだりすれば、これらの資源は使い尽くされ機器が停止してしまう可能性がある。

現在のインターネットの経路情報は、フルルートで約18万経路です。これに対して5万経路や10万経路という大量な経路情報を送り込めば、インターネットを構成するルータなどの機器資源は使い尽くされ一部で機器の停止などが考えられ、ひいてはインターネット全体の混乱を及ぼしかない。

この様子を図 7-28 に示す。

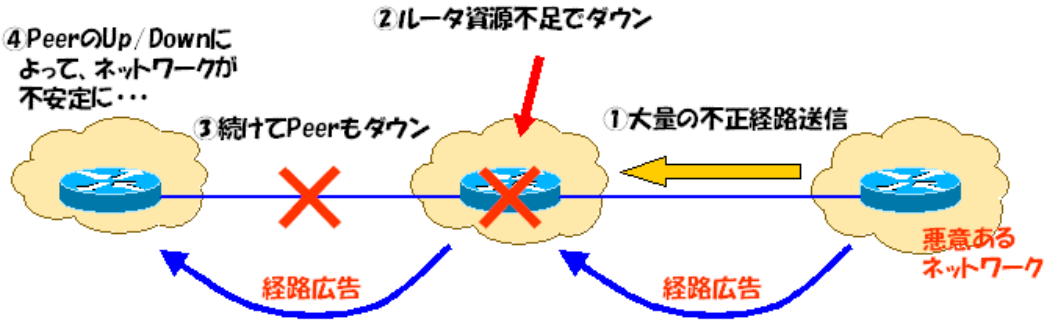


図 7-28　大量経路送信が原因でネットワークが不安定に

これらの例は、悪意こそないと考えられるが、運用上のミスなどによって酷似するケースのトラブルが過去に発生しており、今後深刻な事態に繋がる可能性がある。

特に、(1)や(2)で述べたような経路情報のなりすましや改ざんは、フィッシング詐欺などにつながりやすく今後のインターネットの安全性を考えるうえでは、非常に重要な問題である。

これらの問題の原点は、BGP は性善説に則り、接続先である隣接 AS からの情報を完全に信用するモデルで考案されたプロトコルであると言うところにある。

最近では、本節であげたような問題が指摘されているため、いくつかの問題回避策が考えられ実践されている。

以降に、悪意のあるなしにかかわらず、BGP を利用した経路伝搬の仕組みの中で運用上問題となる点について、より具体的に解説し、その後、回避手段などについて解説する。

7.5.2. 発生する可能性が高い問題

前節では、BGP が隣接 AS を信用するモデルで考案されたたためにいくつかの問題が発生する可能性があることを述べた。

本節では、この発生する問題のうち、比較的よく観測されるものと、悪意性の高い事例について取り上げ解説する。

7.5.2.1. 設定ミスによる影響

BGP は、隣接 AS から広告される経路情報を信用して経路制御を行う。これは、設定が正しく行われている場合、そして、悪意のない正しい情報が登録されている場合には、一切の問題が発生しない。

しかし、ルータなどの設定は基本的に人が行うものであること、そして、機器はしばしば誤動作を起こすものであることを考えると、ネットワークの運用者に悪意が全く無くても、正しくない経路情報がインターネットに流れ、一部のネットワークに問題が発生する、または、インターネット全体に及ぶ問題に発展する可能性すらある。

たとえば、ある内部経路が数万経路ほどある比較的大きなネットワークがあったとする。通常、IGP で扱う内部経路は、BGP のような経路制御プロトコルには転送しない。これは、IGP の様な細かい経路がインターネット全体にとって重要ではないことやインターネット全体の経路情報を減らすという意味もあるからである。

しかし、ルータの設定では、比較的簡単に IGP の経路情報を BGP の経路情報として広告するということが出来てしまうのである。(このような設定用のコマンドが用意されているのは、実際にそのような運用形態もあるからである。) 仮に、このルータの設定が間違えて実行されてしまった場合には、IGP に流れている数万経路がインターネットに流れてしまうのである。

現在のフルルートは約18万経路である。一方、ルータで管理可能な BGP の経路数は、ルータのメーカや性能に相当依存するが、通常25万経路程度のものもあり、これに IGP から8万経路も流れれば、合計が26万経路となり、ルータは BGP の経路情報が扱えなくなる。このとき、ルータは、経路情報を受け取るのをやめるか、リブートをするかのどちらかの動作をとることが多い。

リブートした場合は、そのルータが接続していた他の AS との接続が途絶え、再接続時に再度フルルートが交換され、場合によっては、ここでのトラブルと元となっている 26 万経路の一部も転送される可能性もある。この経路情報が他の隣接 AS に転送され、そこのルータの資源が足りなかった場合には、また同じような状況が発生し、トラブルはどんどん広がってゆくと言うことになる。

このトラブルは、数年前に実際に米国で発生している事例である。単純にルータの設定のミスだったことが解っているが、インターネットにとっては相当大きなトラブルだったと言って過言ではない。

このようにトラブルが連鎖してゆくことを「障害連鎖」といい、総務省の次世代 IP インフラ研究会[15]（図 7-29）の議論のなかでも取り上げられ、対策が必要であると議論されている。

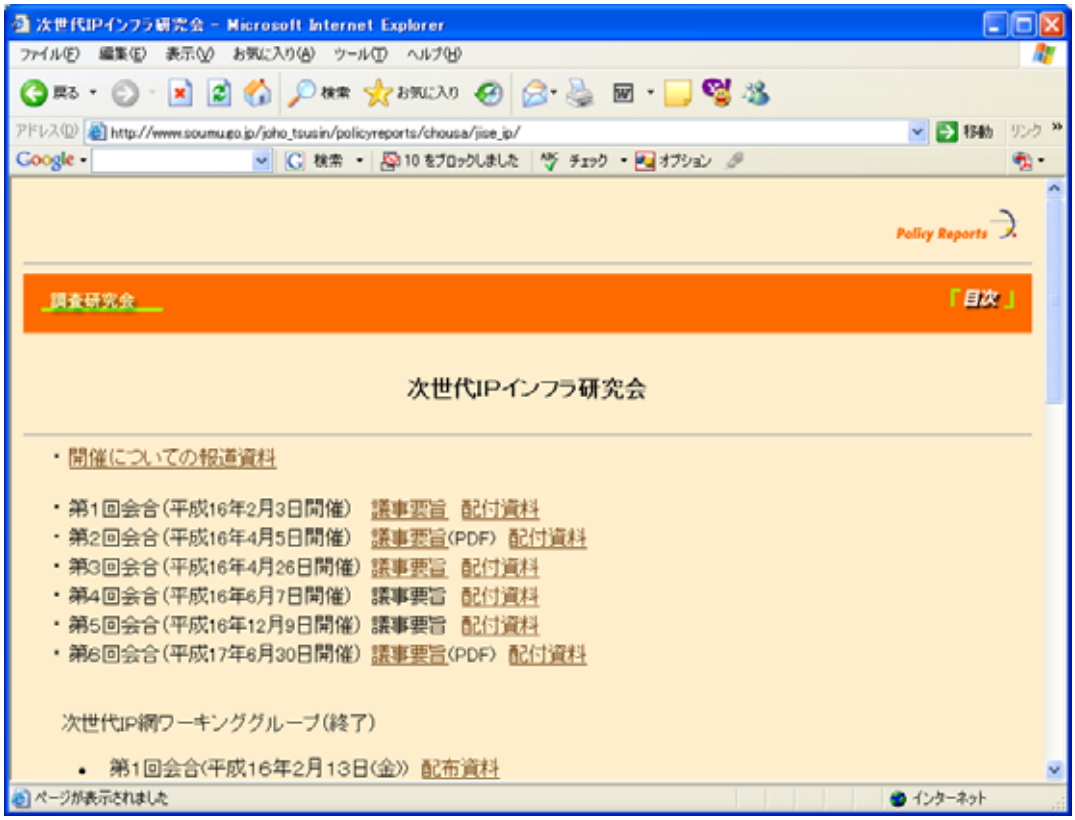


図 7-29　次世代 IP インフラ研究会のホームページ

[15] 次世代 IP インフラ研究会、次世代 IP 網ワーキンググループ（第 3 回会合）（平成 16 年 3 月 10 日開催）にて取り上げられた。
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/040310_3.html

この数万経路が流出するというトラブルは比較的極端な例ではあるが、細かいものでは、広告する経路自体の設定をミスしてしまうと言う例も以外と多く聞かれている。

たとえば、192.168.0.0/16 という経路を設定するところを、192.169.0.0/16 と設定してしまった場合などである。もちろん、ここであげた経路は単なる例だが、設定された例では、第二オクテットが1だけ違っている。広告主は、192.168.0.0/16 の割り振りを受けて、正しく広告しているつもりなのだが、実際には 192.169.0.0/16 がインターネットに広告されることになる。これにより、正しく 192.169.0.0/16 の割り振りを受けている AS は、インターネットの一部からのアクセスが不能になってしまうのである。

このように、経路情報の広告、そしてその伝搬には、単純な設定ミスで思いもよらぬトラブルを引き起こすことが解っている。このようなトラブルが無いように適切な回避策を講じておく必要がある。

7.5.2.2. 経路ハイジャック

もう一つの重要な問題として経路ハイジャックの問題がある。経路ハイジャックとは、現在利用中のネットワークに対する経路情報と同等、もしくは対象ネットワークの乗っ取りたい一部の経路情報をインターネットに広告し、正しく利用しているネットワークへの到達性を奪ったり、悪用するために正しいネットワークへのアクセスを横取りしたりすることを言いう。

乗っ取られた場合の状況として、正規な経路情報と同等もしくは、そのネットワークに含まれる経路情報がインターネットに広告されるため、それが悪意を持っているのか、単なる設定ミスであるのかについては見分けづらい。経路ハイジャックといった場合には、一般的に悪意を持ってこれらの行為を意図的に行っている場合を指す。

この経路ハイジャックは、BGP や経路制御方法の落とし穴をついて行われる。経路制御は、基本的に「Longest Match の原則」がある。経路情報は、Prefix と Prefix Length という2つの情報によって構成されるが、同一の Prefix が存在する場合には、Prefix Length がより長いもの(細かい経路)が優先されるという原則のことである。この Longest Match の原則が経路ハイジャックを行うため手法になるのである。

この様子を図 7-30 に示す。

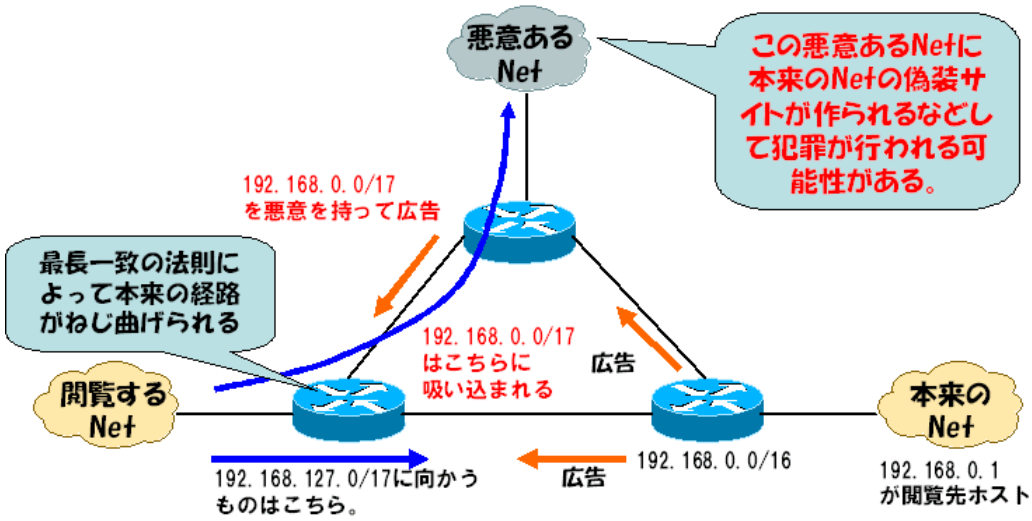


図 7-30　経路ハイジャックの手法

たとえば、AS-X が 192.168.0.0/16 という経路をインターネットに広告していたとする。このときの Prefix は 192.168.0.0 で Prefix Length は 16 である。これに対して悪意をもった AS-Z が、192.168.0.0./17 という経路をインターネットに広告した場合、Prefix は 192.168.0.0 で同じでだが、Prefix Length は 16 と 17 で、悪意を持った AS-Z の方がより長く、経路制御の特性上 AS-Z が優先すべき経路情報として扱われてしまうのである。AS-Z としては、この優先される経路情報を用いて、通常 AS-X に向かうトラフィックを横取りし、場合によってはフィッシング詐欺のためのサーバを立ちあげるなども考えられるのである。

このような例は、最近になって見られるようになってきた。自分のネットワークの経路情報を安全に伝える、また、不正な経路を受け取らないようにするための運用手段の確立、というものが必要になってきていると言える。

7.5.3. BGP 運用による問題回避手段と実情

本節では、前節までに述べた BGP が持つ問題について、現時点での運用上の対策について述べる。

7.5.3.1. 問題回避手段

前節で述べたような問題が発生する原因は、以下の 2 つの点から発生している。

- 広告元 AS が意図しない経路情報を広告している。

- 経路情報の受信時に広告元が意図している経路情報以外の経路情報を受け取っている。

逆に言えば、これらの意図しない経路情報を広告したり受信したりしなければ、経路情報は安定するということが言える。

多くのルータでは、送受信する経路情報を制限するための経路フィルタの機能が実装されており、これを利用して意図しない経路情報を遮断することができる。経路フィルタには、以下の様な種類がある。

(1) AS パスフィルタ

ASパスフィルタは、経路情報がどのようなASによって伝搬されてきたかを示しているBGPの経路情報の属性に含まれているAS Pathによって受信経路をフィルタするものである。

このフィルタでは、経由するASや、どのＡＳを通過してきたかという情報によって、その経路情報を受信するかどうかを決定する。たとえば、広告元のＡＳ番号が1で、その経路情報がＡＳ2と3の両方を経由してＡＳ4に到達しているような場合、ＡＳ4では、ＡＳ2経由の物だけを受信する、というような操作が可能になるのである。

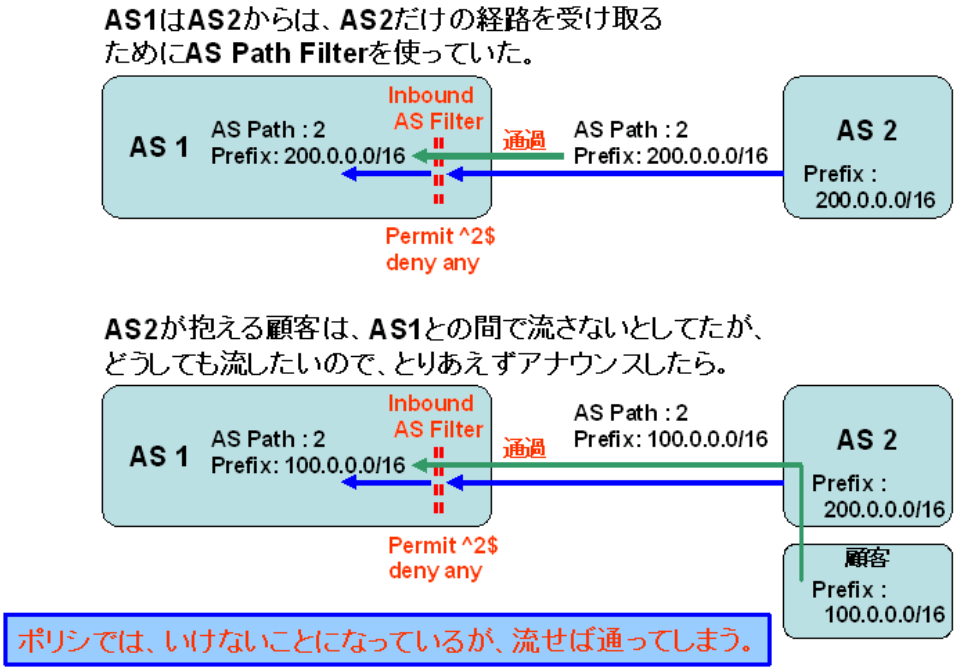


図 7-31　AS Path Filter の例

AS パスフィルタの動作の例について図 7-31 に示す。

一方、AS パスフィルタは、その AS 番号によってのみフィルタされるため、AS パスフィルタによって定義された条件だけを満たせば、実際に送られてくる Prefix の情報が不正な物であっても防げないという弱点もある。

(2) Prefix フィルタ

Prefix フィルタは、受信する経路の Prefix 情報に条件を設けることで経路情報をフィルタするものである。Prefix フィルタは、Prefix と Prefix Length の 2 つの情報によって 1 つの Prefix フィルタを構成する。また、Prefix Length は、多くの場合、設定した長さより「より長い」、「より短い」または「同じ」などの条件を付けることが可能で、Prefix に対して柔軟なフィルタを提供している場合が多い。

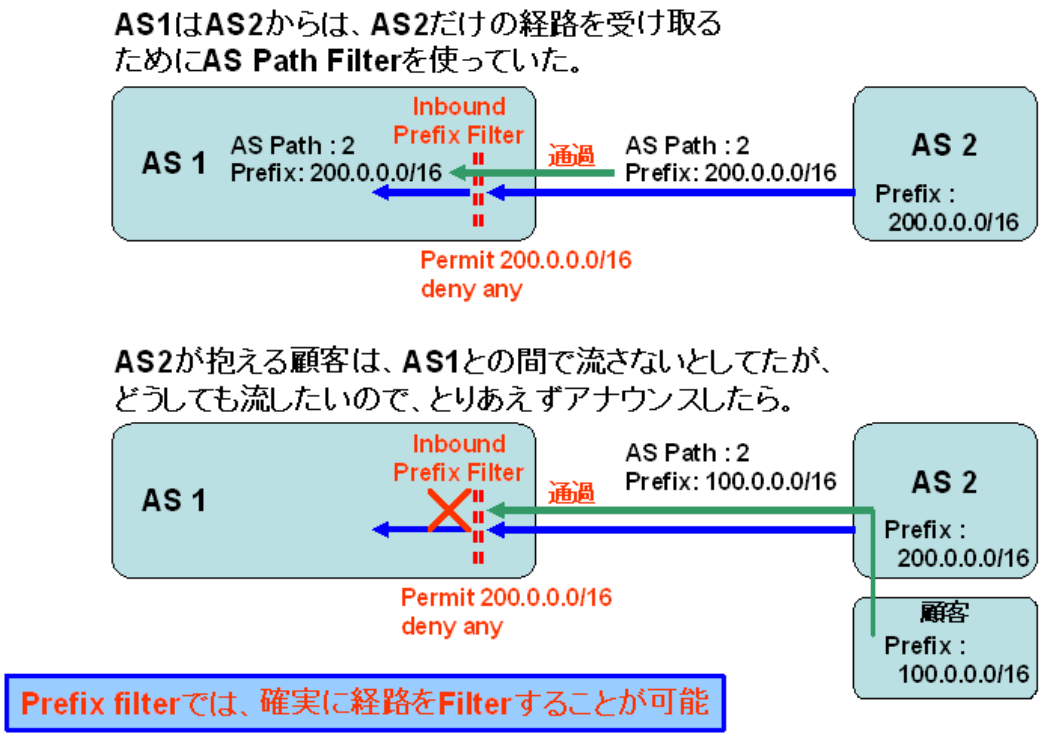


図 7-32 Prefix Filter の例

これは、経路情報として 192.168.0.0/16 とインターネットに広告されてしまっている場合でも、経路制御を行いやすくするために、192.168.0.0/17 と 192.168.128.0/17 の2つの経路情報に分割してインターネットに広告する場合などがあり、このような場合でも「/16 より長い物は受け付ける」と言うように設定することで、ある程度範囲を持ったフィルタの設定をすることが可能になるからである。

Prefix フィルタの動作の例について図 7-32 に示す。

一方、Prefix フィルタは、Prefix 情報をすべて網羅した設定を必要とするため、設定する情報が膨大になり、それによって管理も煩雑になり、設定ミスを引き起こす原因にもなりかねない。また、Prefix 情報が正しければ、経路情報を受け付けてしまうことから、意図しない AS から経路情報が広告されていても、問題なく受け取ってしまう可能性がある。

このように先に挙げた問題を解決する為の「経路フィルタ」という手段は、運用上の手法で対策は可能である。しかし、各フィルタの項目で挙げたように、どちらかのフィルタだけでは、

問題を完全に解決できず、これらのフィルタを複合的に利用することが不可欠である。

さらに、これらの情報を取得する手段についても問題がある。BGP の接続は、ISP から BGP の接続を購入するケース、IX 等に接続して他の ISP と相互接続するケースなどがある。IX に接続するケースは通常「対等ピア」と呼ばれ、お互いの AS の情報とその顧客の AS の情報を交換するにとどまる場合が多い。このため交換する経路情報が比較的少なく、メールなどで広告予定の経路情報を AS パスや Prefix の情報であらかじめ交換し、フィルタを設定しておくことで十分な対策が可能である。しかし、このようなことが可能なのは、実際には対等ピアの数が少なく、BGP の顧客も少ない場合である。これらの数が多くなってきた場合には、現実的にすべてに対してフィルタを設定することは難しくなり、何らかの自動的なフィルタ設定手段を講じるか、網羅的に対応可能なフィルタを考案して設定しておくなどの対応をするしかなく、対応策が機能としては存在していても現実的には設定が難しい状況と言える。

7.5.3.2. 現実的な対応例

前節では、フィルタの手法について述べた。このなかで、それらの手法を利用して細かく設定して、危険を回避することは、フィルタの設定量などの問題で現実的ではないと述べた。

そこで、本節では、現実的な範囲として実際に行われているフィルタの例について紹介する。

(1) IX での AS パスフィルタ

主に日本の IX で行われている。基本的に広告される Prefix に問題がある場合には完全に防ぎきれない AS パスフィルタであるが、IX で行う「対応ピア」は、通常 IX に接続しているもの同士である一定の合意を行い、場合によってはそれを書面で交換するなどの手続きを行って BGP 接続を行っている。また、IX で交換される経路情報は、隣接ASとその AS の顧客の情報を交換するというのが一般的で、交換する経路情報自体がASの管理の範疇であるため、そもそも安定した経路であると言える。そこで、IX での BGP 接続では、隣接 AS が管理している AS に限定することを目的に AS パスフィルタのみで対応しているケースが多いようである。

但し、IX にて AS パスフィルタを多用するケースは、日本における特徴的な運用方法で、米国などでは、そもそもフィルタをしないケースや、Prefix フィルタで行うことが多いようである。

(2) Prefix Length によるフィルタ

Prefix フィルタの一種になるが、特に Prefix Length に注目してフィルタを行う場合を指している。このモデルのフィルタには、より大きな Prefix をフィルタする場合とより細かい Prefix をフィルタするという二つのケースがある。

✧　より大きな Prefix をフィルタする

レジストリから ISP 等にアドレスを割り振る際に経路制御可能性を考慮し、「最小割り振りサイズ」というのが決められている。これは、経路情報が細かくなりすぎて経路数の爆発を防ぐために、ある程度大きな量を ISP に割り振ることで、インターネットに流れる経路情報の細分化を防ぐ為に決められているものである。

この最小割り振りサイズは、/8 単位で決められており、IANA のページや RIR のページで参照することができる。

この情報を利用すれば、意図的に分割して経路情報として流す場合を除けば、大幅に細かい経路情報としてインターネットに流れてくることは考えにくいため、この値を基準にフィルタをすることが可能となるのである。

✧　より細かい Prefix をフィルタする

BGP に流される経路情報は、先にも述べたようにレジストリからの最小割り振りサイズに大きく左右される。一方、この最小割り振りサイズは、CIDR が実施された後に考案された物で、それ以前の物は、クラスフルな割り当てが行われ、結果的にクラスフルな単位での経路情報がインターネットに広告されていたのである。

特にクラス C のアドレスは、/24 という経路情報として出現し、BGP の経路情報としては比較的細かい値となるが、この/24 に相当する経路情報は、今なお経路情報全体の約半数を占めているのである。

そこで、/24 という経路を一つの基準にして、インターネットに広告する経路情報としては、それ以上細かい経路は流さないようにという無言のルールが存在しており、このルールに従ってフィルタをしているケースが多いようである。

(3) その他最低限のフィルタ

最後にその他最低限実施すべきフィルタについて整理する。

このような最低限のフィルタは、JANOG（日本ネットワーク・オペレーターズ・グループ）で議論され、ドリーム・トレイン・インターネットの馬渡氏や株式会社インターネット総合研究所の平尾氏らの提案によって、JANOG の第 16 回ミーティングにて議論され、採択されている。[16]

16 本報告書執筆時点の 2006 年 2 月 9 日の時点では、JANOG のホームページにはまだ掲載されていないようである。詳しくは、議論を行った Inter-domain Routing Security Workshop のホームページから参照できる。(http://www.bugest.net/irs/)

7.6. インターネットルーティングレジストリ

本節では、インターネットルーティングレジストリ（以降、IRR）に関するさまざまな状況および実態について報告する。

最初に、IRR の歴史について解説し、IRR が開発された背景について報告する。次に、現在の国際、およびアジア太平洋での IRR の実態について報告する。次に、これら IRR が現時点で期待されている機能などについて解説し、さらに IRR の現状について報告する。最後に、これらの現状を踏まえ、実際の IRR が利用されている実態について報告する。

7.6.1. IRR の歴史

IRR を研究していた有名なプロジェクトの一つに米国の Merit、University of Southern California Information Sciences Institute(ISI)、Cisco Systems、University of Michigan とその関係者によって提供された Routing Arbiter Project(以下、RA プロジェクト)がある。

RA プロジェクトは、Route Server、Network Management System、Routing Arbiter Database(RADB)、 Routing Engineering Team の 4 つのプロジェクトで構成されていた。この RA プロジェクトは、NAP[17]での経路交換において、NAP 上でフルメッシュの BGP Peer をするのではなく、Route Server を使って、単一の Peer を Route Server に接続することで、BGP の経路情報の交換をスムーズに行うことを目的としていた。この Route Server には、データベースに蓄積された経路情報とポリシ情報を利用して、BGP Peer 間の経路制御を実装する機能があり、ここで利用するデータベースが RADB であり、IRR である。

RADB に蓄積されるポリシ情報は、RIPE-181 という形式で記述されていた。RIPE-181 形式は、ヨーロッパにある RIPE NCC によって開発されたもので、その原型は、1980 年後半に NSFNET のバックボーンルータを設定するために利用されていた PRDB(Policy Routing Database)である。PRDB は、この RADB と RIPE-181 の出現によって、1995 年までに置き換えられている。

[17] NAP(Network Access Point)：現在の IX(インターネットエクスチェンジ)に類似したもの

その後、IRR の記述言語である RIPE-181 はいくつかの拡張をされながら利用されてきたが、1999 年 6 月に RFC2622[18]として RPSL(Routing Policy Specification Language)が定義されると、Merit を初めとするいくつかの IRR サーバ提供者は、すぐさまこれに対応し、現在では、RPSL を利用することが標準となっているのである。

一方で、IRR サービスの状況も変化してきている。RA プロジェクトの発足に合わせる形で、NAP や ISP などでも IRR サービスを提供する動きがあった。1999 年までは、IRR サーバソフトウェアも十分なものがなく、実際にサービスを提供していたのは、RADB、RIPE、Cable & Wireless（旧 MCI）、ANS、CAnet の 5 か所のみだった。この中でも RADB はデータ量などから見ても世界最大のデータベースとなっていた。しかし、Merit は 1999 年後半に、RADB を有料化すると宣言し、同時に、IRRd という IRR サーバソフトウェアの提供を無償で開始すると発表したのである。

現在の IRR のホームページを図 7-33 に示す。

[18] Routing Policy Specification Language (RPSL) (RFC2622)
http://www.ietf.org/rfc/rfc2622.txt

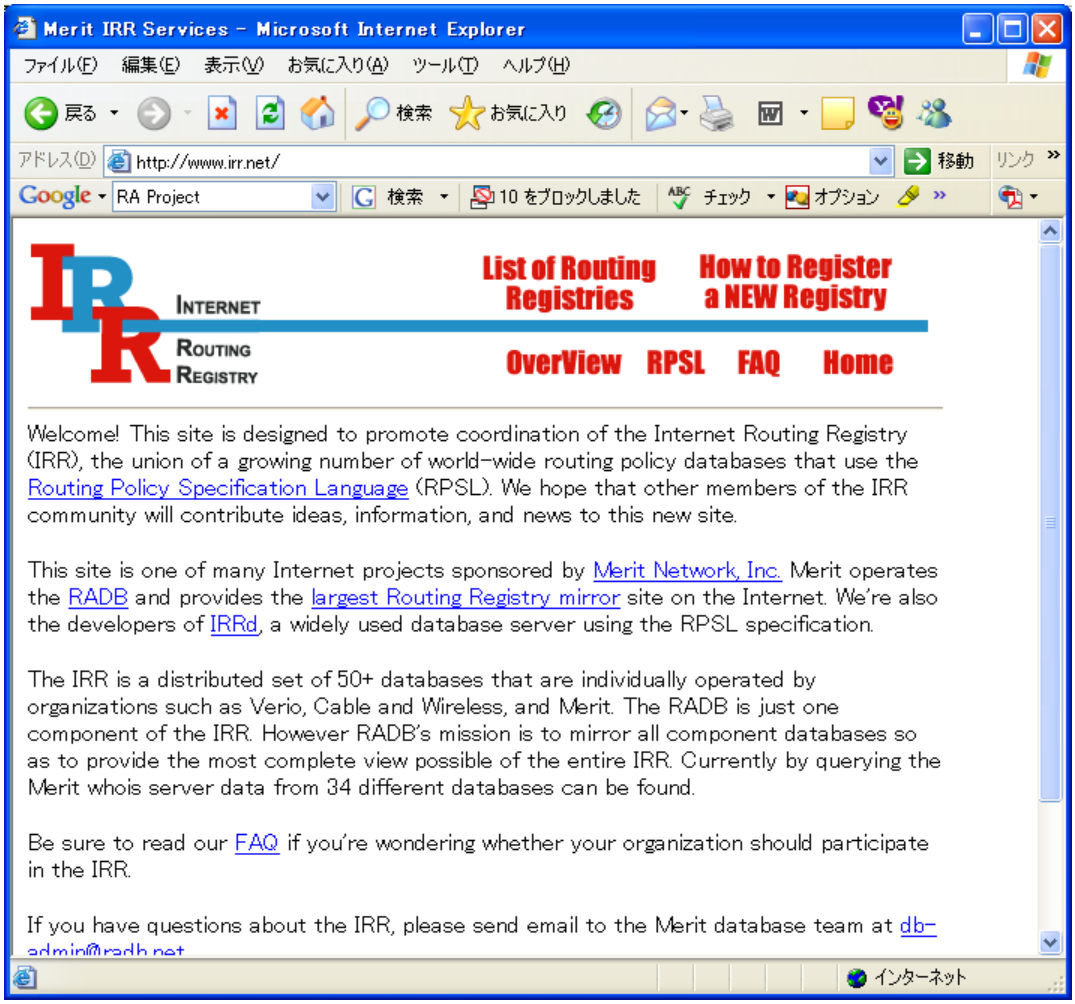


図 7-33 IRR のホームページ

IRRd は、IRR の情報を簡単に扱うことができ、かつ他の IRR とのミラーリングもサポートし、小規模向けには非常に強力なソフトウェアであった。このため、IRR を必要とする ISP などは、IRRd を用いて IRR サービスを独自に行い、そのデータを RADB とミラーするという手法を取り始めたのである。これにより、先にあげた 5 か所の IRR に多く集まっていたデータは徐々に分散化していったのである。

IRR のミラーリングの仕組みでは、ミラーリング先から他のミラーリング先へとデータを転送することは行わないため、今までのように RADB をミラーし、そのデータベースからルータへポリシを実装することが難しくなった。

この段階において、日本でも IRR の周辺事情に関する議論が盛り上がり、JPNIC が 2000 年に開催した IRR 研究会へとつながったのである。

現在、この活動は JPNIC が提供する IRR サービスである JPIRR に結びつき、試験サービスを行うに至った。JPIRR のホームページを図 7-34 に示す。

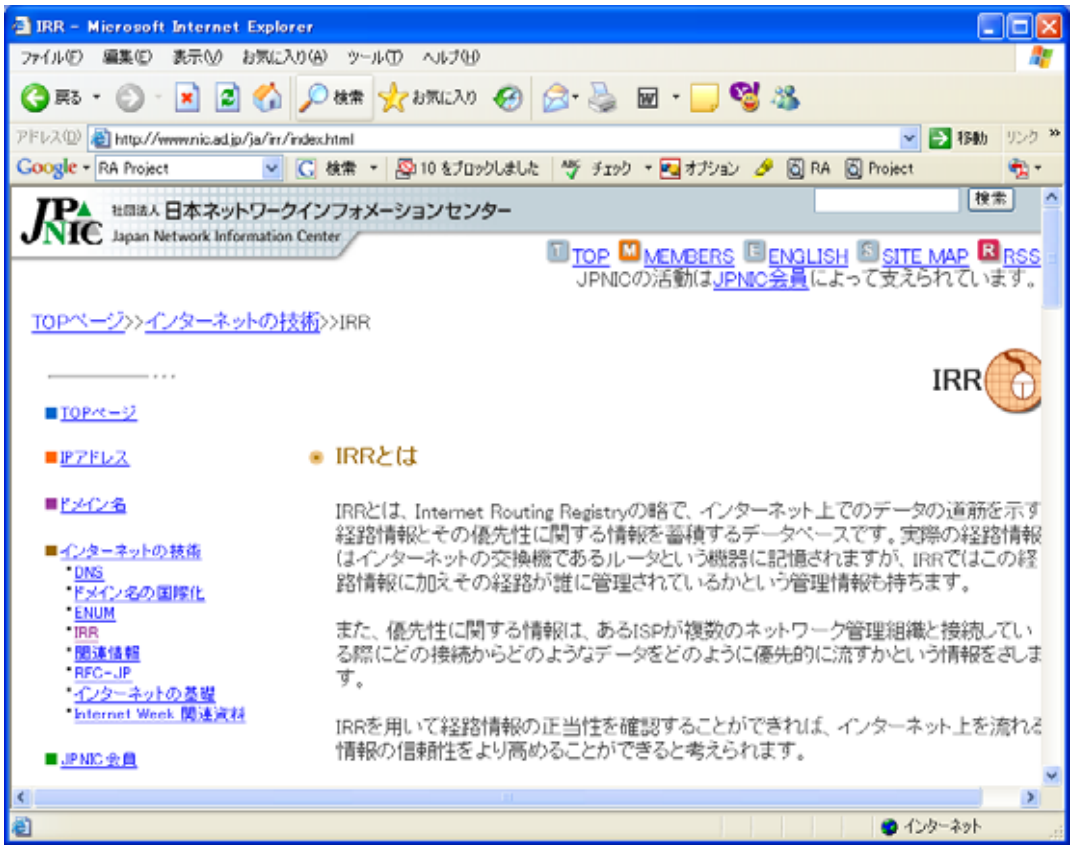


図 7-34 JPIRR のホームページ

7.6.2. 国際的な IRR の利用状況

国際的には、IRR のコミュニティは現在も Merit が運営する RADB を中心と考えて問題ない。Merit の有料化以降、Merit が配布する IRRd を用いて独自に IRR サーバを運営する ISP が数多くいるが、その多くは、RADB とミラーリングを実施しており、その数は、38[19]を越える。このため、RADB から直接検索を実施するのであれば、現在もなお、多くの IRR の情報を取得することが可能である。

[19] 2006 年 1 月 26 日時点で RADB のホームページ(http://www.radb.net/reports.html)にて公開されているミラーリングリストより。ただし、RIPE などが入っていないことから実際にも多数の IRR がミラーされていると思われる。

RADB のホームページを図 7-35 に示す。

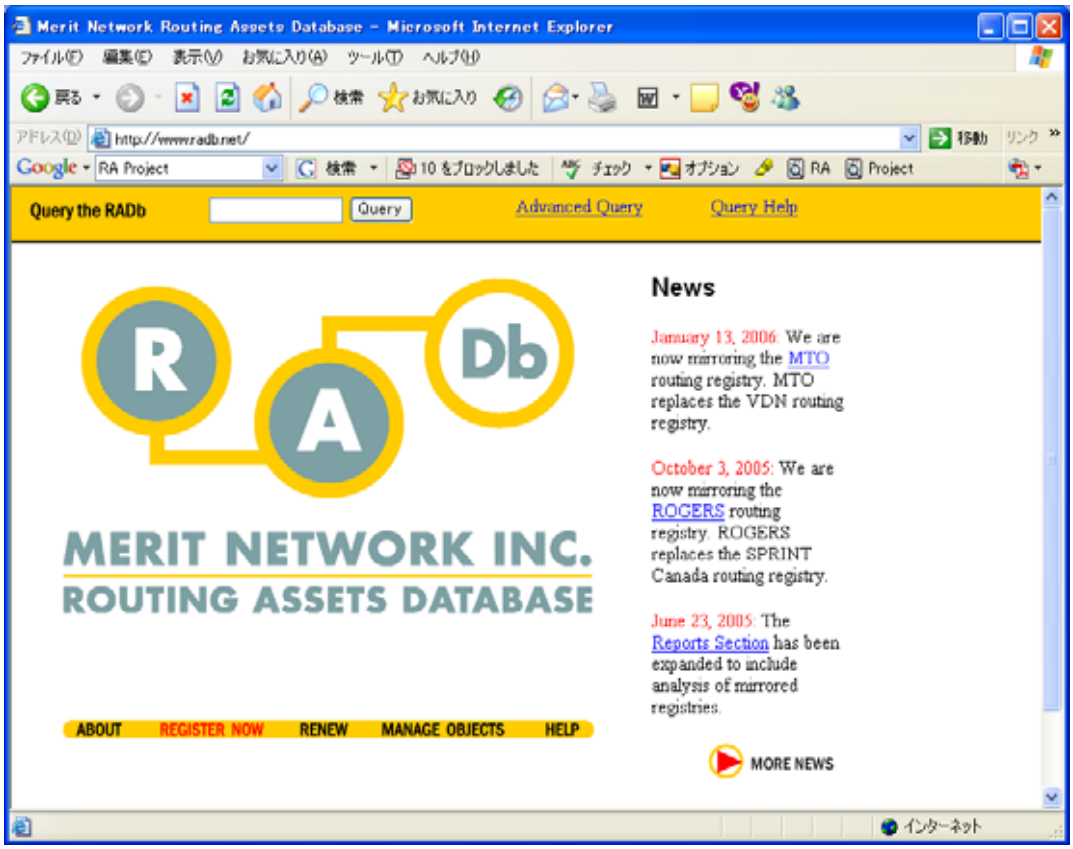


図 7-35 RADB のホームページ

一方で、インターネットレジストリで IRR の機能をサポートする動きもある。この動きは、米国のネットワーク運用グループである NANOG が開催するミーティングである NANOG22(2001 年 5 月開催)において、JPNIC IRR 企画策定専門家チームのメンバーが IRR とインターネットレジストリが持つ Whois データベースの連携によって IRR のデータがより信頼性の高いものになるという提案を行い、それに賛同する形で始まったものである。

この流れを受け、アジア太平洋地域を中心に活動する APNIC は、2002 年より RIPE NCC の Whois システムを採用し、同時に IRR のサービスも始めている。

ヨーロッパを中心に活動を行う RIPE NCC は、独自のデータベースを開発し利用している経緯もあり、古くから、IRR とインターネットレジストリが持つ Whois データベースが統合されたシステムで運用が行われてきたのである。

北米を中心に活動する ARIN(American Registry for Internet Numbers)では、Merit が大きな IRR である RADB を運営していることから、実験的に IRR を運営するにとどまり、積極的な運用は行っていない。

このように、IRR の共通のデータは、RIR(Regional Internet Registry:地域インターネットレジストリ)を中心にデータの統合化が進んできている[20]。しかし、各 ISP、特にトランジットサービスを行うような比較的大規模な ISP においては、現在もなお、独自に IRR サービスを実施しているところも少なくない。

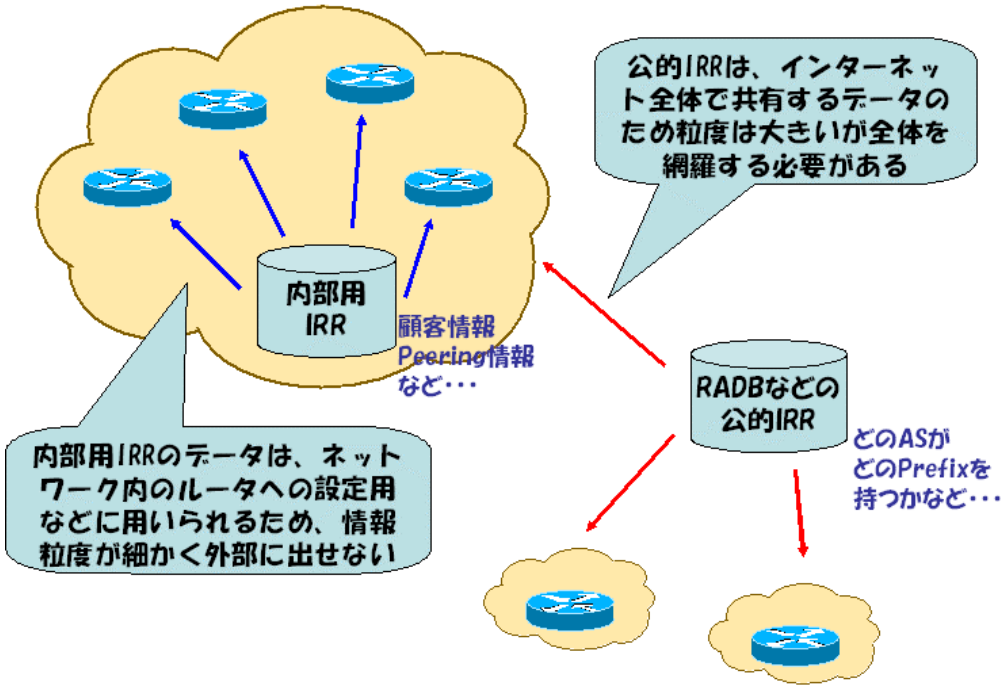


図 7-36 IRR の運用形態によって情報の特性が異なる

この 2 つの運用のされ方には、データの内容に大きな違いがあることがわかってきている。この様子を図 7-36 に示す。

先に説明した、RIR が運用する IRR データについては、より一般的な情報、つまり、AS 番号と Prefix、そしてそれらがグループ化された情報と運用者情報などが入り、経路の優先性情報や Peering 情報などの細かい情報はほとんど含まれていない。その一方で、各 ISP が運用するような IRR では、顧客の Peering 情報が扱われているケースも見受けられる。

[20] 北米では、いまもって RADB が中心的に利用されている。

このように ISP が独自に IRR を運用する背景には、BGP ルータの Prefix フィルタを自動生成するなど運用負荷の軽減や自 AS が管理すべき経路情報の安全な蓄積などという目的があるのである。

RIR が運用するような IRR でも、ごく一般的な情報はあるため Prefix フィルタ程度であれば自動生成が可能である。しかし、ISP が独自に運用する IRR などでは、これに加え、マルチホーム Peering の優先性情報などの細かい情報も扱うことで、より高度な運用負荷軽減を狙っているのが現実と言える。

7.6.3. アジア太平洋地域における IRR の利用状況

アジア太平洋地域における IRR の活動は APNIC を中心に行われている。先の第 22 回 NANOG ミーティングの動きや第 10 回 APNIC オープンポリシーミーティングでの JPNIC IRR 企画策定専門家チームからのインターネットレジストリによる IRR 実施の提案などを受けて、APNIC では 2001 年より IRR サービスを開始したのである。

この動きを経て、APNIC 管轄地域では、APNIC の IRR データベースが利用されるケースが増えてきたのである。

ISP 独自での IRR サービスの運用については、国際的な流れと変わることはないが、全体の数として APNIC 管轄地域では、大規模な ISP も少ないことからその数は多くない。

APNIC 管轄地域において比較的大きな動きがある地域は日本と韓国と言えるだろう。韓国は、先の APNIC の流れを受け、KRNIC(Korea Network Information Center)が中心に IRR サービスの検討プロジェクトが立ち上がっており、サービス開始に向けた検討が進んでいる。日本では、公共の IRR サービスとして現在 JPNIC が実施している JPIRR 試験サービスがあるが、民間・研究団体としては NTT や SINET なども IRR を運用していることがわかっている。

これら APNIC 管轄地域の IRR については、IRR の普及度などの面から、公共の IRR として運用されているものは APNIC の持つ IRR のみであり、JPNIC および KRNIC はいまだ実験段階、その他は ISP 独自となっている状況である。

7.6.4. IRR に期待される機能

ここまで IRR の歴史と世界・アジア地域での議論の状況について報告してきた。これらの

議論の中で、当初 IRR が特定の範囲、特に IX 接続業者間などの限られた範囲内でのみ利用されることを前提として進んできた物が、昨今では実際にインターネット上を流れてくる経路情報を確かめる手段としての価値が高まってきていることが解る。そこで本節では、これらの議論の中での IRR に登録される情報の種類と、それら情報がインターネット上に流れる経路情報の確認手段としての役割について、さらに詳しく報告する。

7.6.4.1. IRR で取り扱うデータの種別

IRR の利用形態はその利用者によって様々である。ある IRR では、特定のインターネットエクスチェンジポイント(IX)の経路交換ポリシを表現するケースや、特定の ISP の顧客の経路情報を管理するケースなどに使われていることが知られている。一方で、IRR のデータはインターネット全体の経路情報が蓄積されていると考えることができ、どの ISP がどのような Prefix や AS の塊で、経路をインターネット上に広告しているのかという、非常に一般的な情報の参照元としても利用されている。

これら 2 つの利用方法は、IRR に登録されるデータの粒度や参照元などが大きく異なるため、同じポリシでデータを取り扱うことは、Peering 情報などの守秘義務もあり、現実的ではない。JPNIC IRR 企画策定専門家チームが主催した会合などでも同様な議論が行われたほか、APNIC や RIPE NCC が主催するミーティングの経路制御関連の専門ワーキンググループ（Routing-WG）の議論でも同じような意見が寄せられている。

これらを整理すると、特定の部分で利用するデータとインターネット全体で利用するデータという 2 つの性質の異なる IRR データをプライベートデータとパブリックデータに分類することができる。

以下では、プライベートデータとパブリックデータの定義について明示する。

◯プライベートデータ

主に、特定の IX への参加者や特定の ISP の顧客向けに提供され、そのコミュニティに閉じて利用される IRR に登録されるデータを指す。これらのプライベートデータには、特定のコミュニティ内で閉じることが必要とされている情報が含まれていることが考えられ、他の IRR との情報の交換には、守秘義務協定など一定の制限を設けて実施するか、または一切の情報交換を実施しないなどの措置が必要である。

具体的には、特定の BGP Peer に対する Local Preference の値、AS-PATH や Prefix

の情報と、それらをどの BGP Peer にどういう優先度で広告するかという情報、およびどういう優先度で受信するかという情報が含まれていることが考えられる。これらの情報を使うことで、特定のコミュニティにおいてきめの細かい経路フィルタなどを自動的に生成することが可能になりうる。

○パブリックデータ

不特定多数からの参照を前提とし、インターネットの経路情報全体を参照できることを目的に運用される IRR に登録されるデータを指す。登録される情報は、インターネットレジストリから割り振られ、実際にインターネットに広告されている経路が登録されるもので、BGP 運用者がインターネットに対して広告する可能性のある経路とその Origin AS の情報などが登録されるほか、トラブル発生時のコンタクト先に関する情報の蓄積などに利用されることが期待されている。

パブリックデータは、インターネットに広告されている全ての経路情報が参照可能であるため、広告されている経路が正しいものであるかどうかを確認することができる点と、プライベートデータのような細かい優先性情報などは、付加的に登録可能、つまりオプションとしての情報であるという点が、重要なポイントとなっている。

もちろん、全ての経路情報に関連するデータが蓄積されるべきものであるため、フルルートに対する適切な Prefix フィルタが実施できるレベルの情報である必要がある。

これら 2 つの情報は、完全に分離して管理されるべきである。プライベートデータは、特定のコミュニティによって管理され、パブリックデータはインターネットレジストリのような公共的な機関によって管理されるべきである。しかし、これら 2 つのデータは時に相互に補完して形成されるべきである。例えば、特定のコミュニティにおいて蓄積されるプライベートデータは、そのコミュニティ内部で利用される情報のみが蓄積されたからである。それ以外の情報はパブリックデータとして蓄積されているデータによって補完されることで、必要な部分は細かく、それ以外の部分については粗く、全ての情報が参照できるようになる。

逆に、プライベートデータから細かい優先性情報などの守秘義務に抵触するような情報をそぎ落とし、パブリックデータに加工することで、パブリックデータを蓄積する IRR に流用することが可能になる。

現時点での IRR の仕組みには、このようなプライベートデータとパブリックデータの分類は存在していない。しかし、将来的に IRR の相互連携モデルが確立した時には、IRR の各オブ

ジェクト、さらには RPSL の各フィールド単位で、パブリック・プライベートなどの属性をもつことで、より信憑性の高い IRR 環境の構築が可能となるだろう。

7.6.4.2. 経路の台帳としての IRR

IRR で取り扱うデータは大きく分類して、「パブリックデータ」と「プライベートデータ」の 2 種類があることを、前節までに説明した。

プライベートデータには、経路の優先性情報などインターネットの運用上、重要な情報が含まれている。このような情報は、企業内や特定のコミュニティの中だけで利用され、外部に流出させないように運用される。その一方、パブリックデータは、プライベートデータをより一般的にし、特定のコミュニティ以外で参照可能な情報となる。

インターネットの運用上、優先性情報といった、より細かい情報を得ることで、運用の煩雑さが改善されることが期待できると考えられている。公共的な団体で実施する IRR では、特定のコミュニティに依存するプライベートデータではなく、広くデータを参照できるパブリックデータが求められている。このため、公的な IRR のサービスを実施する際の判断基準として、パブリックデータをインターネットの運用にどのように生かせるかという点が、一つのポイントとなると考えられる。

これまでの IRR の歴史の中で、この「パブリック」な IRR に近いものが RADB と言えるだろう。IRR が分散化する前の段階における RADB の利用方法を考察することで、パブリックデータの価値が見えてくることが考えられる。

IRR が分散化する前の段階では、RADB は CAnet や MCI をはじめとする他の IRR と比べて、非常に多くのデータを蓄積していた。この段階で、RADB のユーザは主に以下のような利用を行っていた。

1) 経路情報の Prefix や AS-PATH を利用した、フィルタリングの基礎情報の生成
2) 特定の Prefix に対するコンタクト情報の検索
3) 不審経路の確認

当時は、RADB と MCI の IRR を参照することでインターネットのほとんどの経路が参照できたことから、日本の ISP も RADB に自 AS の経路情報を登録しなければ、インターネット上で経路がフィルタされてしまうという懸念があった。

また、ISP の顧客が BGP によって接続する場合には、ISP が RADB への登録を代行してきたため、実質的に RADB を参照すればインターネットの経路情報はほとんど解決可能だと思われていたのである[21]。

もちろんこの段階では、米国の大手の ISP などに、不用意に Prefix や AS のフィルタがされてしまうことを避けるために登録されていたため、経路の優先性情報などの細かい情報はほとんど含まれていなかったのである。

このような環境が功を奏して、インターネットに接続されているネットワークの Prefix や AS に関する情報、コンタクト情報が容易に取得可能になっていたのである。また、このようなインターネットの経路情報が十分集まっているデータベースは、実際にルータで受けている経路の確認のためにも使われていた。

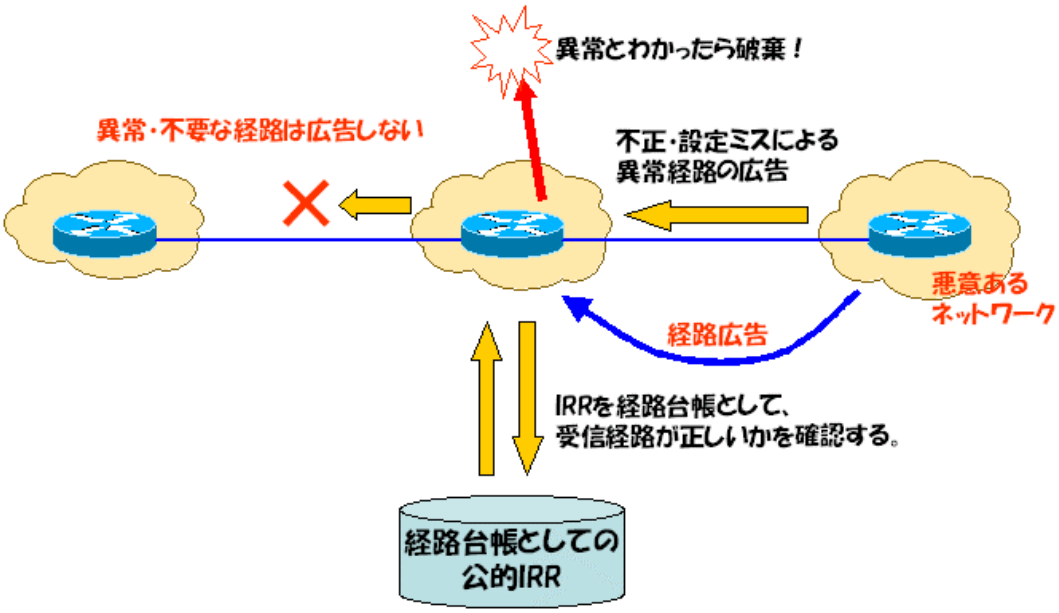


図 7-37　経路台帳として IRR の役割の例

インターネットのルータの運用は、一部自動化されている部分もあるが、多くの場合、人手によって行われている。これは同時にミスを引き起こす原因でもあり、ミスオペレーションなどによって、時として他の AS の Prefix や自分が割り当てられていない AS 番号の経路などをインターネットに流してしまうということがある。もちろん、このほかにも、悪意をもって他の ISP

21 実際は他の IRR も合わせて参照しなければ解決は不可能であった。

の経路を流し、インターネットを混乱させるということもある。

このような場合、RADB はその膨大なデータ量から、その経路は意図されてインターネットに広告されているのかを確認をするための台帳としての役割も果たしたのである。

このような IRR の利用例を図 7-37 に示す。

現時点での IRR のデータ、特に RADB などのパブリックデータは、IRR の分散化や長期間に渡ってデータが未更新となることなどによって、以前ほどの効果は得られていない。しかし、パブリックデータとして、インターネットの経路情報の台帳となるほどのデータが参照できるようになれば、運用上、非常に有用なデータベースとなることには間違いないであろう。

7.6.5. IRR の稼働実態

現在、世界中で稼働している IRR は大量に存在している。そのほとんどは ISP 内部の私的利用のものである。一方で、公的に利用されている IRR も複数ある。

以下に、私的･公的を問わず世界的に有名な IRR について列挙し、その特徴について解説する。

- RADB

  米国の Merit によって運営されている IRR である。7.6.1 項でも触れたように、RA プロジェクトの実験のために作られた IRR であるが、その後も世界的に利用され、現在では世界最多のオブジェクトが登録されている。

  また、Merit では、IRRd という簡単に IRR サーバを構築できるソフトウェアを配布しており、これを利用して多くの ISP が独自の IRR を構築し、さらにそれらは、RADB とミラーを行っているため、数多くの IRR とミラーを行っている。

  このため、RADB は IRR の代名詞として利用される場合が多く、IRR を用いて経路フィルタを実施する場合でも、現状では RADB に登録することが標準になっているのが現実である。

- RIPE-DB

RIPE によって運営されている IRR である。IRR のソフトウェアとして RIPE-DB という RIPE 独自に開発した IRR ソフトウェアを利用している。この IRR ソフトウェアは、RIPE がインターネットレジストリの WHOIS データベース用に開発したものを IRR もサポートするように拡張したもので、現在でも WHOIS データベースと IRR データベースが共存する形で利用されている。

また、RIPE-DB は IRR に経路情報広告ポリシを記述する言語である RPSL の原点ともなる RIPR-181 をいち早くサポートした IRR でもあり、Merit が開発した IRR ソフトウェアと同じ程度の歴史を持つ IRR といえる。

RIPE-DB は、レジストリが運営する IRR としては最初の IRR で、レジストリが利用する WHOIS データベース、そして IRR データベースの基本ソフトウェアとして広く利用されている。

- APNIC

APNIC によって運営されている IRR である。APNIC は、WHOIS データベースとして RIPE-DB を利用している。このため、IRR をサポートすることは、単純に IRR の機能を有効にするだけで利用できるため、APNIC ミーティングにて、APNIC による IRR の運営がリクエストされてから、IRR のサービスを始めるまでにそう時間がかからなかった。むしろ APNIC では、IRR で参照可能なデータベースを広範囲に広げるために、数多くの IRR とミラーを行うような努力を行い、その結果、レジストリが運用する公的な IRR としては、RADB に次いで多くのオブジェクトの検索が可能となっている。

このため、APNIC は現在、アジア太平洋地域の公的 IRR の中心的存在として運営されている。

- Verio

NTT/Verio が運営する IRR である。主に、顧客の経路情報を登録し NTT/Verio との接続ポイントで不正な経路が混入しないようにフィルタをしたり、確認したりするための参照先データベースとして構築された、私的な IRR である。

NTT/Verio では、この独自の IRR だけでなく、RADB ともミラーを行っており、RADB と NTT/Verio に登録されたデータを中心に経路のフィルタを作成し運用を行っている。

- SINET

  SINET[22]は、日本の学術情報ネットワークで、主に大学などに対してインターネットの接続サービスを行っている組織である。ただし、公式なサービスとしてIRRサービスは提供していないようである。

- JPIRR

  JPNIC が実験的に運営している IRR である。インターネットレジストリが運営する IRR によって IRR に登録する情報内容の正確性の向上と正しい情報が登録されることによって経路情報を確認するための台帳として IRR が機能出来る可能性について研究･開発を行っている。

  JPIRR では、主に JPNIC の IP アドレス管理指定事業者に対してサービスを行っているが、広く IRR の価値を理解してもらうことを目的に、現在のところ IP アドレス管理指定事業者に限らずサービスを提供している。

  2006 年中には、正式サービスへの展開を検討しており、より安定したサービスを展開予定である。

7.6.6. IRR 利用の実態

これら IRR に登録された情報は、インターネットに流れる経路の台帳として利用されることが期待されている。具体的な利用方法としては、IRR に登録されている情報を元にルータに設定する経路情報を生成したり、BGP で受信している経路を確認する手段として利用したりする。このほか、新しい利用方法としてルータの経路制御ソフトウェアに受信経路を IRR で確認する機構を実装し、経路情報の受信とほぼ同時に経路情報の真偽を確認するようなことも考えられている。

以下に、これらの IRR の利用手法の代表的なものと現在考えられている IRR の利用手法について解説する。

---

22 学術情報ネットワークは、国立情報研究所の運営するネットワークである。（http://www.sinet.ad.jp/）

(1) IRR を用いた経路フィルタの生成

IRR には、AS がインターネットに流す経路情報が登録されている。そこで、この情報を利用して自 AS が受信する経路情報をフィルタして、不正な経路情報を受信することを防ぐことができる。

フィルタの生成ツールとして IRRToolSet (図 7-38) が有名である。IRRToolSet は ISI[23] が開発した IRR を検索してその情報からルータに設定するフィルタなどを生成するツールである。フィルタを生成するだけでなく、IRR を利用する上で必要な文法チェックツールなどのパッケージである。

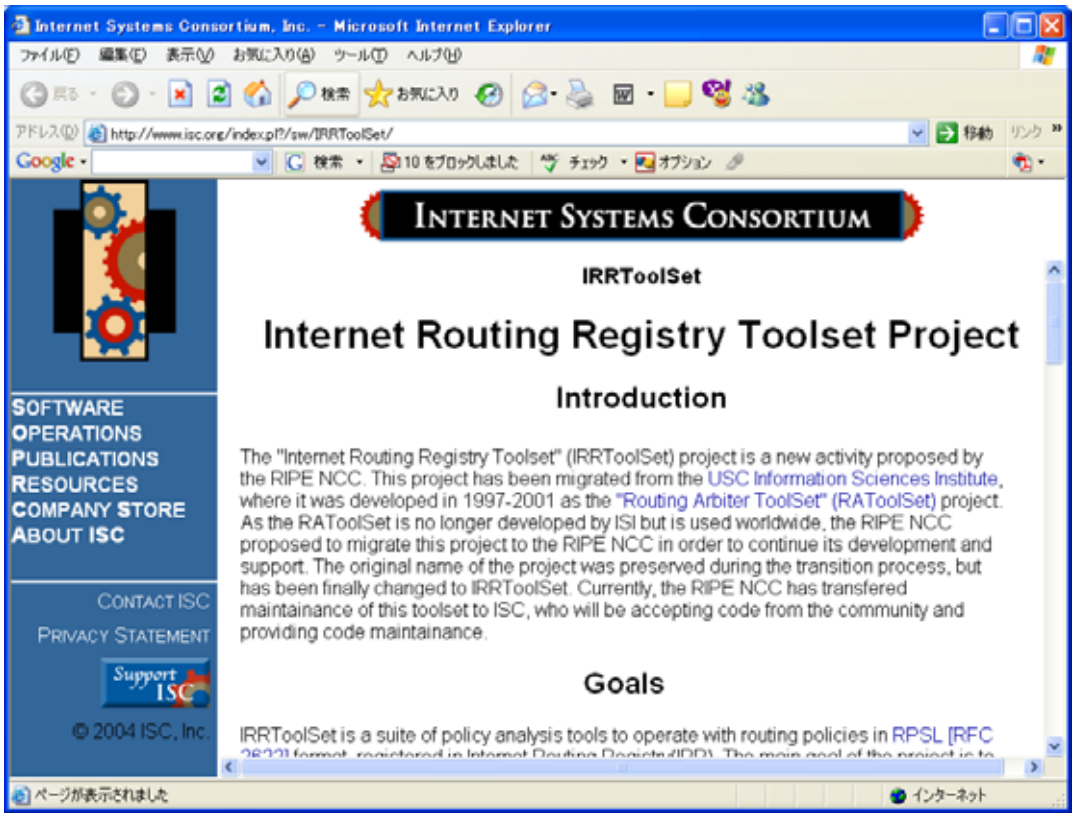


図 7-38 IRRToolSet のホームページ

一般的には、自 AS が接続する AS の情報から、その接続先 AS が接続相手に広告する情報を検索し、その情報から経路フィルタを生成する。この IRR を利用した機構が

[23] The University of Southern California Information Sciences Institute

無い場合に経路フィルタを生成するときには、接続先相手と広告する経路をメールなどで交換し、それをフィルタとして加工し利用することができる。この場合、接続相手の広告経路に追加･削除･変更が生じた場合に、その都度その更新を相手に通知し、フィルタを変更してもらう必要があり、比較的大きな AS の場合、接続 AS も多く、フィルタ更新作業だけでも相当な作業量となる可能性がある。IRR を用いてこれらの経路情報を交換することで、これらの情報のやりとりを簡素化できるだけでなく、フィルタの生成作業も簡素化することが出来るようになることが期待できる。

(2) IRR を用いた自動的な経路情報確認機構

先にも述べたように IRR には、ある AS が広告しようとしている経路情報が登録されている。この情報を利用すれば、経路を受信した時点で、その AS が意図的に広告しているかどうかを判断することができる。この特性を利用し、確認する機構をルータに実装した研究がある。

この研究は、2001 年に東京大学の長橋賢吾氏が「An Integrity Check for the Conflict Origin AS Prefixes in the Inter-domain Routing」という論文にまとめたもので、受信した経路を IRR に問い合わせ、その経路が登録されており、広告元 AS が正しいかなどのチェックを行う機構を経路制御ソフトウェア上に実装し、経路の受信段階で受信経路が広告元 AS によって意図的に広告されているかについて IRR を通して確認するための機構である。

論文発表段階では、IRR に登録されている情報がインターネット上に広告されている経路情報がすべて登録されていないことや、IRR に登録されている情報が正しくないなどの問題があり、有効性に疑問が呈されたが、正しい情報が登録されている IRR ができれば、経路情報のフィルタをダイナミックに行うことが出来る一つの解決策と言えるだろう。

7.6.7. IRR がもたらす影響

前節までに IRR の情報を元にフィルタを生成する手法などについて述べてきた。実際にこれらの手法を利用してフィルタを生成しているという確たる説明はどこの ISP も行っていない。

しかし、実際に IRR から経路情報を削除してしまった場合のトラブル、そして、複数の IRR が乱立し、連携が不十分な状態であるがために、経路制御上の問題が発生しているケース

がいくつか報告されている。

ある例では、AS に関連する情報を RADB に登録していたが、何らかの原因で RADB からオブジェクトが削除された。これにより、上流 AS が接続している他の AS の入り口で当該 AS の経路情報がフィルタで排除され、インターネットの広範囲にわたって接続性を失うトラブルが発生したのである。

そこで接続性の回復の手段として、当該 AS は日本の実験サービスである JPIRR にオブジェクトの登録をおこなった。しかし、これでも状況は改善できなかった。

これは、フィルタをしている AS が IRR オブジェクトの登録先 IRR が RADB または該当 AS が運営する私的 IRR のいずれかに登録しなくてはならないという制限があったためである。

非常に似た例が、JANOG16[24]において、NPO 法人北海道地域ネットワーク協議会の河合氏によって紹介されている。

IRR へのオブジェクト登録には、しばしばこのような誤解が生じている。IRR は、現在多く立ち上がっているが、それぞれの IRR に自身の IRR データベースへの登録を示すために、管理元の IRR の名称がすべてのオブジェクトに「Source」として記されている。IRR のミラーはこの「Source」毎に行われるため、「RADB にオブジェクトを登録」といった場合は、この「Source」が RADB になっていることが求められており、whois.radb.net を検索ホストとして検索が可能かどうかは問題ではないのである。図 7-39 にこの様子を示す。

[24] 日本ネットワーク・オペレーターズ・グループによる第 16 回目のミーティングで、2005 年 7 月 28 日～29 日に福岡で開催された。(http://www.janog.gr.jp/meeting/janog16/)

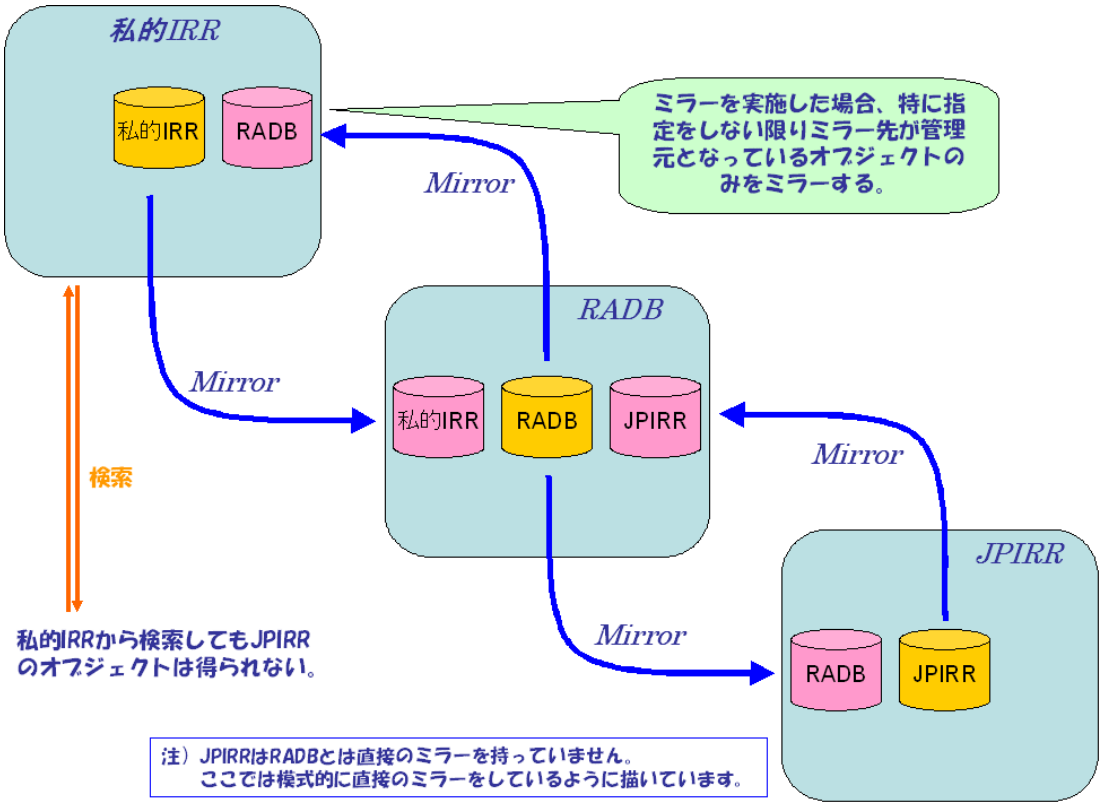


図 7-39 IRR のミラー構造

つまり、今回フィルタしていた AS は、自身の私的 IRR と RADB をミラーしており、私的 IRR で検索可能なオブジェクトを用いてフィルタを生成していたと考えられる。このような状況では、RADB で JPIRR のオブジェクトが検索できたとしても私的 IRR で検索ができないため問題が解決できないのである。

この問題を解決するためには、IRR システム全体としてミラーリングの手法などについて根本的に検討し直さなければならない。

最後に、この節で取り上げた問題を整理する。

(1) IRR への経路登録が無い場合、自 AS とは直接関係の無い AS において、経路がフィルタで排除される可能性があり、潜在的にインターネット全体に対して自 AS が広告した経路が正しく伝わらない可能性がある。

(2) RADB からオブジェクトの検索ができれば問題が解決するわけではなく、ミラーリングシステムを根本的に見直す必要がある。

7.7. IP レジストリシステム

本節では、JPNIC や APNIC などの IP レジストリ[25]が利用する IP レジストリシステムに関して解説を行う。

最初に、IP レジストリが運営する IP レジストリステムにはどのような役割があるのかを解説する。次に、IP レジストリシステムに登録される情報の特徴について解説する。

7.7.1. IP レジストリシステムの役割

IP レジストリは、7.4 節で解説したとおり IANA を頂点として、5つの地域レジストリを中心として、世界的に共通の IP アドレスの空間を管理し、IP アドレスを必要とする組織などに適切に割り当て、その一意性を保証する組織である。

IP レジストリシステムは、これらの IP レジストリが果たすべき役割を補助し、効率よく IP アドレスを管理するためのシステムである。

通常 IP レジストリといった場合、IP アドレスの管理のための階層構造に従い、ネットワーク接続事業などを行うローカルレジストリ（LIR）までを含むが、ここでは、この LIR を含まず、国別レジストリ、または地域レジストリにおける IP レジストリシステムに絞って解説を進めることとする。

この IP レジストリシステムには、IP アドレスを管理し、インターネットの世界を効率よく運用できることをサポートするために、以下の様な役割が実装されている。

(1) 管理すべきアドレス空間を把握する
(2) 利用中のアドレス空間を把握する
(3) アドレスを必要な人に必要なだけ効率よく割り当てる
(4) インターネット運用上必要な情報を公開する
(5) 公開すべき情報を最新に維持する

実際には、IP レジストリの職員が自ら作業するところも多くあるが、IP レジストリシステムとし

[25] ここでは IP レジストリと表記するが、前節までのインターネットレジストリと同義である。

て以上のような役割がある。以下に個々の役割について解説する。

(1) 管理すべきアドレス空間を把握する

IP レジストリが管理するアドレス空間は、IANA を頂点に管理するアドレス空間を必要に応じて地域レジストリに割り振りを行っている。また、APNIC 地域では、さらに国別レジストリが存在し、管理するアドレス空間はさらに国別レジストリへとその管理を委託している。

これら IP レジストリによるアドレス空間の管理では、IP アドレスの一意性を保つために適切に管理する必要があり、各レジストリがどのアドレス空間の管理が委譲されているのかをしっかり把握して管理しなくてはならないのである。

IP レジストリでは、このようなレジストリで管理しているアドレス空間を把握するような実装が必要なのである。

(2) 利用中のアドレス空間を把握する

IP レジストリでは、上記によって委譲されたアドレス空間をアドレスの利用者に対して、割り振り・割り当てを行う。通常、利用者をローカルレジストリとエンドユーザーに分けて考え、ローカルレジストリに対しては、ローカルレジストリがさらにエンドユーザーにアドレスの割り当てを行うことから、アドレスの「割り振り」と呼ぶ。

地域・国別レジストリでは、これら LIR やエンドユーザーに割り振り・割り当てたアドレス空間を管理し、二重に割り振り・割り当てを行わないようにしなくてはならない。

IP レジストリシステムでは、アドレス空間が二重に割り振り・割り当てを行わないような管理を行うための実装が必要なのである。

(3) アドレスを必要な人に必要なだけ効率よく割り当てる

IP アドレスは、インターネットを利用するための公共の資源として考えられる。このため、IP アドレスは、必要とする人に必要なだけ適切に割り当てる必要がある。適切な割り当てについては、先にも解説したように RFC2050 や各レジストリが定めているアドレスの割り振り・割り当てポリシに従って行われなくてはならない。

この割り振り・割り当てには、この「適切さ」を諮る仕組みがあり、IP アドレスの割り振り・割り当てルールが作成されており、このルールに従って実際お割り振り・割り当てが行われることになる。

通常、この割り振り・割り当ては、「申請」→「審査」→「割り振り・割り当て」の流れがあり、この申請の受理や、審査、審査結果の管理を補助するためのシステムが IP レジストリシステムに求められる。

(4) インターネット運用上必要な情報を公開する

RFC2050 でも記載されているとおり、割り振り・割り当てが行われたアドレス空間は、公開される必要がある。

広大なインターネットにおいて、あるネットワークが他のネットワークまでの到達性を確保するためには、複数のネットワークを跨いで接続されるが、多くの場合、直接接続しているネットワーク以外のネットワークの情報は知ることができない。しかし、インターネットの運用においては、離れたネットワークからの経路広告やパケット送受信が自分のネットワークに何らかの影響を及ぼす可能性があり、場合によっては、当該ネットワークに連絡をする必要が発生する。

このように、インターネットの安定運用を目指す上では、自ネットワークと直接接続性を持たないネットワークのコンタクト情報などの情報を知る必要性があり、IP レジストリシステムには、割り振り・割り当ての情報を元に、ネットワークに対するコンタクト情報など運用上必要な情報を適切に公開する責務がある。

IP レジストリステムには、このような割り振り・割り当てを行ったアドレス空間に対する運用上必要な情報を公開するための実装が必要なのである。

(5) 公開すべき情報を最新に維持する

上記によって公開される情報は、運用上最新のものでなくては役に立たない。IP レジストリシステムには、公開情報を最新の情報に維持するための仕組みが必要なのである。

IP レジストリシステムに登録されている情報で且つ運用上必要な情報は、通常

ネットワークの運用者へのコンタクト情報などである。多くのレジストリシステムでは、これらのコンタクト情報は、ネットワーク利用者自身によって変更が可能である。しかし、ネットワーク利用者自身によって更新可能であるということは、更新にあたって、更新者がネットワーク利用者自身であるかどうかを判断する必要であることを意味する。

そこで、IP レジストリシステムでは、これら情報を更新するものが、更新者として適切であるかどうかを判断するための仕組みが必要となるのである。

7.7.2. IP レジストリシステムに登録される情報

7.7.1 節では、IP レジストリシステムに必要な機能について解説した。これらの機能は、先にも述べたように IP アドレスの割り振り・割り当てを適切に行うために必要な機能である。

本節では、IP アドレスの割り振り・割り当てを適切に行うために IP レジストリシステムに登録されるべき情報について整理する。

IP レジストリシステムに登録されるべき基本的な情報は以下の 3 つである。

(1) 上位レジストリからの割り振り情報
(2) 下位レジストリへの割り振り情報
(3) アドレスの割り当て情報

上位レジストリからの割り振り情報の場合、JPNIC の場合は APNIC からの割り振り情報、APNIC の場合は IANA からの割り振り情報となる。

下位レジストリへの割り振り情報は、JPNIC の場合は LIR への割り振りに関する情報となり、割り振り先のコンタクト情報やすでに割り振りを行ったアドレス空間の管理、そして、割り振った時に適切に割り振ったかどうかを示すネットワークに関する情報となる。また、LIR では割り振られた空間をエンドユーザーに割り当てる作業を実際に行うため、この割り当てが実際にどの程度行われているか、つまり、割り振った空間のなかでの割り当てた量を管理しなくてはならない。

アドレスの割り当て情報は、どのアドレス空間をどの利用者が利用しているかを登録する。

これらを整理したものを表 7-2 に示す。

表 7-2 IP レジストリへの登録情報

上位レジストリからの割り振り情報	● 割り振り元レジストリ情報 ● 割り振りアドレス情報 ➢ 開始アドレス ➢ 終了アドレス
下位レジストリへの割り振り情報	● 割り振り先レジストリ情報 ● 割り振りアドレス情報 ➢ 開始アドレス ➢ 終了アドレス ● 割り振り済み空間情報 ➢ 割り振り時のネットワーク情報 ● 割り振り済み空間の利用情報
アドレスの割り当て情報	● 割当先情報 ➢ コンタクト情報など ● 割り当てアドレス情報 ➢ 開始アドレス ➢ 終了アドレス

第 8 章　経路制御におけるセキュリティの現状

内容

- 経路交換の問題点とその原因
- 経路情報保全に関する提案・活動等

8. 経路制御におけるセキュリティの現状

本章では、前章までの問題点などをふまえ、経路制御を行う上でのセキュリティの現状と実体について整理する。

最初に、経路交換を行にあたって、第１層や第2層で発生するセキュリティ上の問題点について整理する。その後、さらに上位層での問題点について整理し、最後に、経路情報保全に関する活動等についてまとめる。

8.1. 経路交換の問題点とその原因

経路交換を行う際には、データ伝送上 (第 1 層、第 2 層) の問題、セッションハイジャックや DoS (Denial of Services) の様なシステムの脆弱性を突いた攻撃、経路情報の信憑性の問題、そして経路情報の増大に関る問題等が上げられる。

本節では、これらの問題点について整理する。

8.1.1. データ伝送上の問題点

ここでは、通常、通信事業者がサービス行っているデータ伝送上の問題点のうち、主に第 1 層および第 2 層に関して述べる。

第 1 層／第 2 層の問題点としては、事故によるファイバ等の物理線の切断や通信機器障害により発生する通信障害、設備管理の不備等による第 3 者の故意による通信設備の破壊／不正アクセスによる不正情報の混入、盗聴等による情報の不正取得等がある。さらに通信上の情報が盗まれることで、より上位層への攻撃を容易にする可能性も増大する。

例えば、通信線は通常ビル内の 1 部屋(MDF 室と呼ぶ)に一度集められ管理／運営されることが多く、この集中管理部屋から各部屋へ再分配される。つまり、一度に数社の人間が MDF 室に入室する可能性がある。この時、さらに第 3 者が入室しても識別は困難である。この第 3 者が通信事設備に対して何らかの不正行為を行う可能性は排除できない。

もう一例としては、特定のエリアにおける Ethernet 環境下では仕様上、ある特殊なアドレスを送信先としてデータを送信すると、エリア内の全て機器はデータを受信して送信元に結果を送り返さなければならない。このとき送信元のアドレスが詐称されていたり、その応答が大量に発生し、応答トラフィックが増大した場合にエリア内での通信障害が起きたりする可能性が高く、さらには、どのような通信サービスを行っているかなどの基本的な情報が盗まれる可能性が大きくなる。

このような事象が発生する原因としては、データ伝送線やデータ伝送機器に対して保護が十分でない場合や、それら機器の管理が徹底されていない状況が考えられる。

データ伝送を行う上での物理的、運用上の様々なリスクを軽減するために ISO27001 等を利用する取り組みがなされている。この取り組みのなかでは、組織における資産の統一的、且つ、一定の基準を持った管理／運用ポリシが必要であり、その管理／運用ポリシを実行している事で、事故が起きたとしても迅速な対処が可能である。また、ポリシを持った運用を行っていることを対外的に示す事ができ、データ伝送提供者、利用者双方に利益につながる。

8.1.2. システムの脆弱性を突いた攻撃

ここでは、サービス・プロバイダの設備となるシステムの問題点として第 3 層から上位層に関して述べる。

第 3 層から上位層は、通信における付加価値サービスの提供を行うサービス・プロバイダや企業内で利用されるケースが多く見られる。現在は、インターネット・プロトコル(以降、IP)の利用が一般的である。IP の仕様は公開されており誰でも自由に参照／利用が可能である。しかし、自由であるが故に悪意のある攻撃者に弱点を突かれるケースもある。現時点では、攻撃によるリスクより利用者が受ける恩恵の方が大きいため、様々なリスク軽減措置を整えた上で IP が利用されている。

IP は、第 1／2 層の通信サービスを介して通信対象者同士が直接データ交換可能な仕組みを提供しているが、この時、通信相手の特定が問題になる。机の隣どうしで通信をする場合には通信機器も通信する人も見て確認できるが、遠距離になると難しい。特に、機器間の通信は設定が容易である IP アドレスを用いて行われるので、知らない間に通信相手が変わっていたと言うことが起こる可能性がある。通信相手が変わっているにもかかわらずそれを知る方法がないとすると、送信者は知らない間に秘密情報を送ってしまう場合があり、それに気づくのが遅れたり、最悪の場合気づかずにより大きい損害発生させたりする可能性がある。

また、IP を利用して通信を行うソフトウェアの弱点を突いて、悪意あるデータが送られた場合、IP を介して受け取ったソフトウェアが停止したり、ソフトウェアを介して重要な情報が盗まれたり、最初にあったソフトウェアが不正なソフトウェアに上書され他組織への攻撃に利用されたりする可能性がある。

最大の原因は、通信相手の特定を IP アドレスに頼っているのにも関わらず、その通信相手が本来の通信相手なのか詐称をしている第三者なのかの確認が困難であることである。

通信相手を確認する方法は様々な取り組みがなされており、利用方法により様々な方法が普及している。一例としては、IPsec を用いた接続先の認証や PKI を利用した接続先の検証などが挙げられる。これら仕組みは、接続先の検証のみではなく他の機能も含まれており適材適所で利用されており、様々な認証機能の仕組みが実現可能である。

8.1.3. 経路情報の信憑性の問題点

本節では、広域でかつ複数の組織が相互接続する環境で、IP 通信を行う場合に利用されている経路交換システム内で扱われる経路情報に関わる問題点に関して述べる。

事故／故意に関わらず、不正な経路情報が経路交換システムへ混入することにより、サービス提供者は提供サービスが正常に提供出来なかったり、サービス利用者が悪意あるサイトへ誘導され、さらに大きい被害に拡大したりする可能性がある。経路交換システムに関してはすでに本調査の前半にて既に述べられているが、経路交換システムで半自動的に受信した経路情報を経路交換システム自身で自動検証する枠組みは現時点では無い。

不正経路による偽サーバへの誘導を図 8-1 に示す。

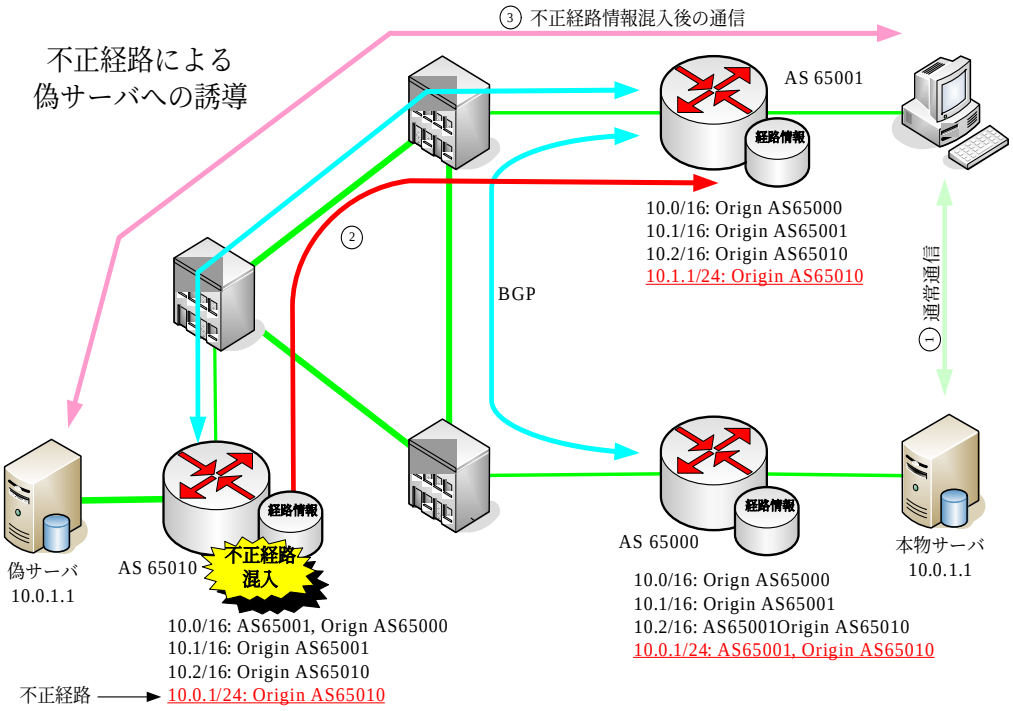


図 8-1　不正経路による偽サーバのへの誘導

しかしながら、不正経路の経路制御システムへの混入は現実問題として起きており、経路情報の保護の必要性が有る事は認識され様々な議論がなされている。このようななか、本調査では soBGP と S-BGP について次章にて述べる。

不正経路情報の排除に関する現実に行われている取り組みとしては、本調査で述べている IRR を利用する方法である。この方法では、IRR に登録されている情報を信用する事で経路制御機器に対して適切なフィルタを設定し、明らかに不正な経路を除外する。しかし、IRR を用いた「登録→フィルタ作成→機器」への設定にはある程度の時間が必要でありトラブルや緊急時の経路変更に対応するのは難しい側面もある。

BGP で現在行われている MD5 による保護は、隣接した機器間で交換される情報の信憑性は確認可能であるが、MD5 へ入力された情報に対する信憑性の有無に関して検証する物ではない。つまり、BGP-MD5 の目的は接続機器間における接続先の確認と通信情報の検証である。

8.1.4. 経路情報の増大に関わる問題

IP 接続組織が多くなるとともに経路情報も大きくなる。本節では、経路情報が大きくなったときにもたらされる問題点に関して述べる。

経路情報が多くなってくると、その情報を処理するための経路制御装置の CPU やメモリ等の容量拡大が必要になり、さらに経路情報に変動が生じたと時その変動を処理するために必要な時間が多く必要となる。また、データ伝送回線に占める経路交換に有する占有率が上がる等の問題がある。

原因は、経路制御機器の誤設定や IP を利用したビジネスの拡大等が考えられる。

経路情報の増大に関しては、現在ほぼ適切な時期に各ルータメーカーなどが CPU やメモリの増強等に対応した機器を発売するなどして対応が行われており、IPv4 の経路制御に関しては相当な対応がされている。しかしながら IPv4→IPv6 移行期や IPv6 普及期に入った時には、更なる経路数の増加が見込まれ、それに伴う更なる設備投資の必要性が考えられる。

8.2. 経路情報保全に関する提案･活動等

問題を解決するための技術や運用による一時対処的なものまで様々な領域で色々な活動が行われているが、IRR にみられる様な経路交換システムとは別のデータベースを利用する事で現行システムに対しての変更を限りなく少なくする取り組みと、soBGP や S-BGP にみられる様な経路交換システムに新たに機能を加えることで経路情報を守る方法と大きく 2 種類の方向性がある。IRR の取り組みに関しては、先に述べた。また、soBGP および S-BGP に関しては第 9 章にて記述する。

第 9 章　経路情報交換における不正利用排除

内容

- RFC3779 の概要
- soBGP の概要とモデル
- S-BGP の概要とモデル

9. 経路情報交換における不正利用排除

本章では、経路交換を行う場合に事故／故意にかかわらず不正な経路情報が混入することによって起こりえるリスクに対しどのようなアプローチがあり、そのアプローチがどのように問題を解決するかを述べる。

構成は、大きく以下の3つに分れている。

- PKI の枠組みを利用して経路情報（IP アドレスブロックと AS 番号）を電子証明書[RFC3280[1]]へ対応するための拡張について
- soBGP を用いた経路交換システムに関して
- S-BGP を用いた経路交換システムに関して

soBGP、S-BGP 両システムとも目的は Origin AS、IP アドレスブロックの検証と AS PATH の検証である。両システムは目的が同じであるが、アプローチ方法が異なる。

soBGP は証明書情報の交換を BGP 経由で行うアプローチを取り、S-BGP は BGP 以外の手段を用いて証明書の交換を行うアプローチをとっている。

[1] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC3280)
http://www.ietf.org/rfc/rfc3280.txt

9.1. RFC3779 の概要

[RFC3779[2]]は、現在 PKI で利用されている X.509v3 証明書[RFC3280]の拡張領域に対して以下に示す 2 種類の情報を定義した RFC である。

- IP アドレス情報
- AS 番号情報

IP アドレス情報用証明書を作成する時には、「アドレスファミリー」「通信方法」と「IP アドレスブロック」もしくは「IP アドレス・プリフィクス」が入り、AS 番号情報用証明書を作成する際には「AS 番号」もしくは「AS 番号ブロック」が入る。

証明書は、IANA/RIR/LIR や「割り振り組織」として認可された権威ある組織が署名する事により、入手した「IP アドレスブロック」や「AS 番号」が正当な手段により取得され、提供された事が検証可能になる。

本 RFC で定義された情報を利用する主な利用例としては、BGP 等の経路制御プロトコルが上げられるが、他組織から経路制御プロトコル経由で渡された「IP アドレスブロック」や「AS 番号」が正当な情報であるかの検証や、IRR に登録されている情報の信憑性の確認する、と言った利用法が考えられる。

9.1.1. IP アドレス情報用拡張の概要

IP アドレス情報を証明書内で認識する為に利用される extnID は「iso(1).identified-organization(3).dod(6).internet(1).security(5).mechanisms(5).pkix(7).id-pe(1).id-pe-ipAddrBlocks(7)」=「1.3.6.1.5.5.7.1.7」で定義済みである。

「IP アドレスブロック」を情報として証明書に入れる場合は 2 つ方法が用意されている。

[2] X.509 Extensions for IP Address and AS Identifiers (RFC3779)
http://www.ietf.org/rfc/rfc3280.txt

一つは「プリフィクス長」を指定する方法、もう一つは IP アドレスブロックを最小アドレスと最大アドレスの範囲を指定する方法である。

- プリフィクス長による指定 ： 10.0.32/20
- 最小アドレスと最大アドレスの範囲を指定： min 10.2.48.0, max 10.2.64.255

図 9-1 に IP アドレスブロック「129.0.68/22」の符号化例を示す。IPv6 アドレスの符号化においても考え方は同様である。

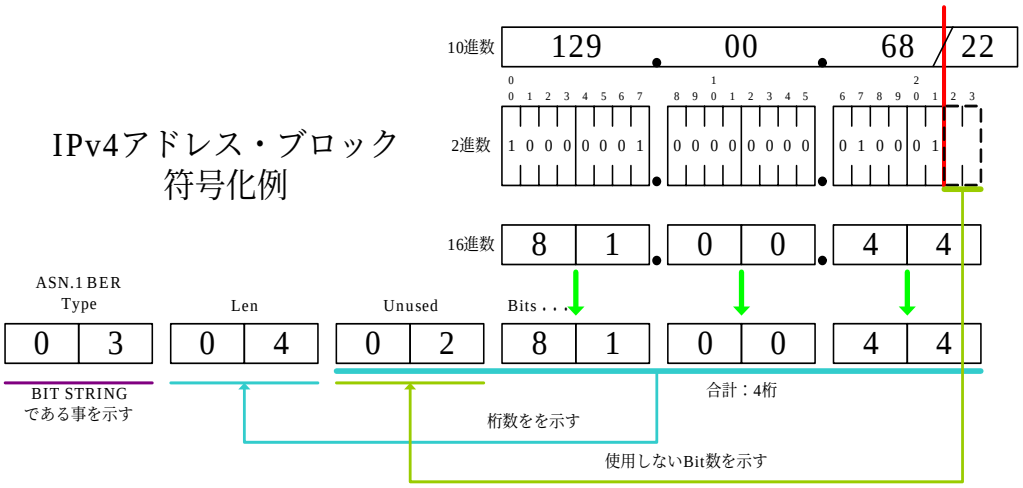


図 9-1　IPv4 アドレスブロック符号化例

その他情報として、「アドレスファミリー　→　IPv4/IPv6」「通信方法　→　Unicast/Multicast」があり、上記「IP アドレスブロック」と合わせて証明書が作成される。

IP アドレスブロック符号化全体例を図 9-2 に示す。

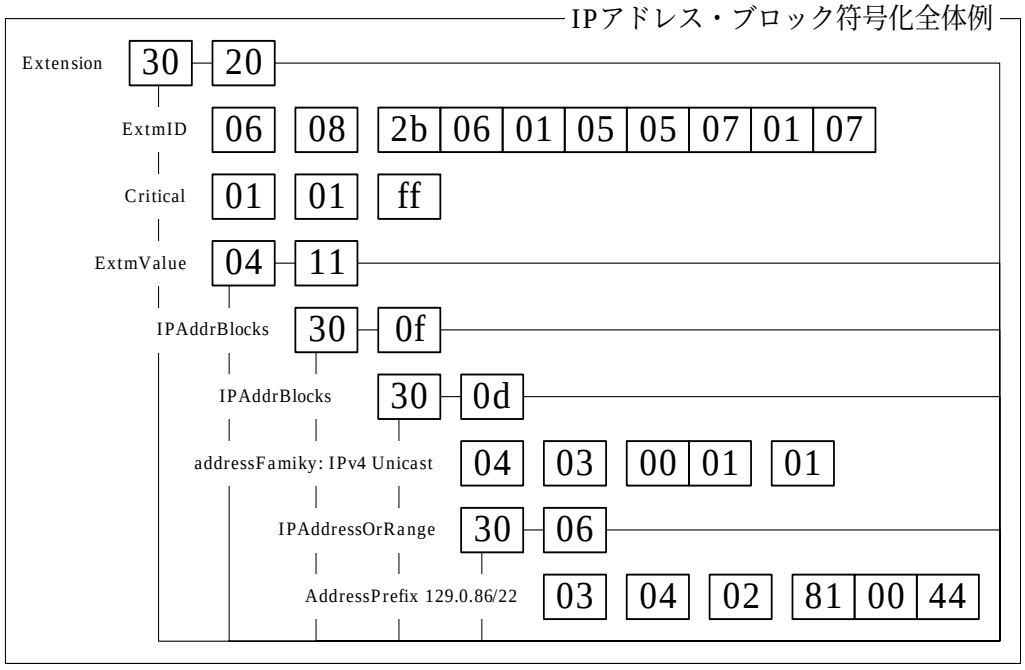


図 9-2　IPv4 アドレスブロック符号化 全体例

9.1.2. AS 番号情報用拡張の概要

AS 番号情報用を証明書内で認識するために利用される extnID は、「iso(1).identified-organization(3).dod(6).internet(1).security(5).mechanisms(5).pkix(7).id-pe(1).id-pe-autonomousSysIds(8)」=「1.3.6.1.5.5.7.1.8」で定義済みである。

「AS 番号」を情報として証明書に入れる場合は 2 つ方法が用意されている。一つは、「AS 番号」を指定する方法、もう一つは AS 番号を最小 AS 番号と最大 AS 番号を範囲で指定する方法である。

- AS 番号による指定 ： 135
- 最小 AS 番号と最大 AS 番号を範囲で指定： min 3000, max 3999

図 9-3 に AS 番号「6434」の符号化例を示し、AS 番号全体例は図 9-4 に示す。

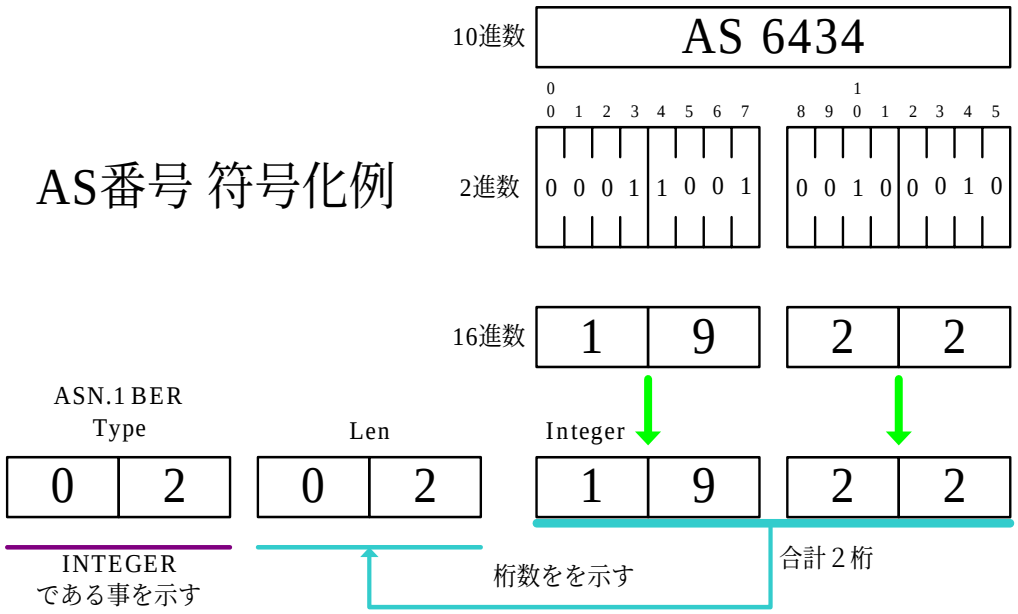


図 9-3　AS 番号符号化例

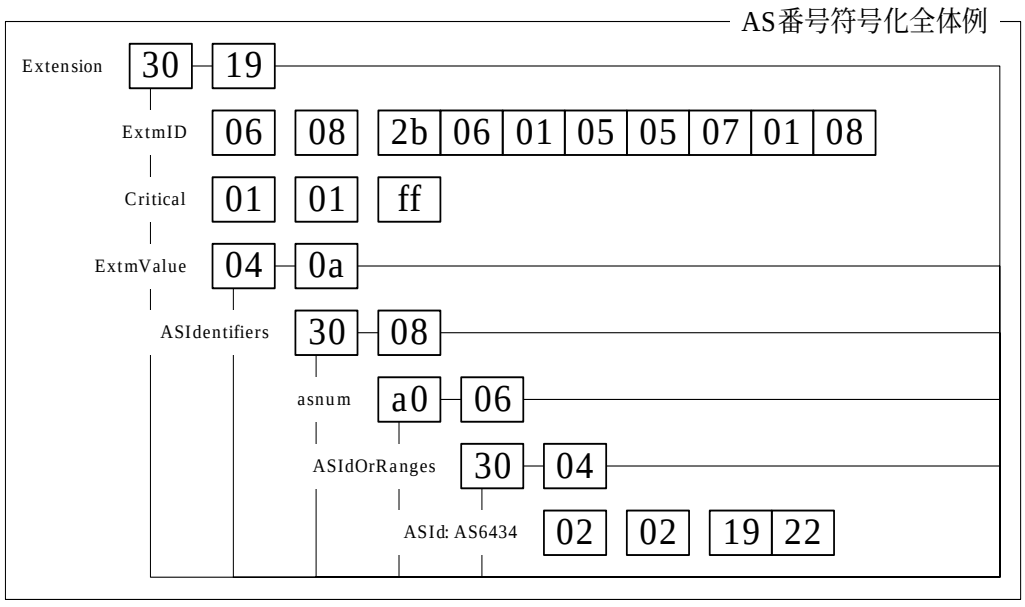


図 9-4　AS 番号符号化 全体例

以上、IP アドレスブロックと AS 番号の 2 種類のうちいずれかを利用し証明書が作成される。

9.2. soBGP の概要とモデル

本節では、経路情報を保護するための提案である soBGP につて、その概要と JPNIC で運用が考えられている IP アドレス証明書システムと JPIRR システムとの連携モデルについて述べる。

9.2.1. soBGP の概要

soBGP の目的は、不正経路情報の発見、除去を自動化する事である。実現方法として、経路生成者が経路情報に対して署名し、作成した証明書を BGP セキュリティ・メッセージで配布する。受取者は受信した証明書を検証する事により、経路情報の真偽を確認する事が可能となり、偽情報を除去する為の情報として利用する事が出来る。証明書の配布→受信→署名検証→証明書の登録／偽情報の排除を自動化する為の提案である。

soBGP で定義されている証明書に含まれる経路情報は主に「AS 番号」「IP アドレス情報」「隣接トランジット AS 番号」「隣接非トランジット AS 番号」がある。定義外の情報に関して検証する手段は提供されない。

9.2.1.1. BGP への拡張

soBGP では、証明書を交換する為に BGP[RFC4271]を拡張し実装される。一つは、隣接する機器同士で[RFC2842[3]]を利用した機能確認を行う（capability code は未決である）機能、二つ目は、BGP で証明書を配布する機能である。証明書配布機能を拡張する為に BGP タイプ・コード（BGP Type Code は未決である）を追加しセキュリティ・メッセージを定義する。

機能確認では、接続先機器が soBGP を利用可能であるかの確認を行い、その結果により soBGP の動作を決定できる仕組みを運用者に提供する。簡単な動作例としては、「接続された機器が soBGP 利用を拒否した時、BGP セッションを停止する」といった運用が可能

[3] Capabilities Advertisement with BGP-4 (RFC2842)
http://www.ietf.org/rfc/rfc2842.txt

になる。この様な接続機器同士の機能確認の仕組みは BGP→soBGP 移行期間には必要な機能である。

新たに定義された BGP タイプ･コードを利用した BGP メッセージ(セキュリティ･メッセージ)では、soBGP の動作を決定するオプションや証明書の送受信などを行うために利用する。簡単な動作としては、「証明書を受信した機器は、証明書を検証し自身の管理テーブルへ登録する。検証出来ない証明書は捨てられると共に経路情報も経路テーブルから削除する」といった動作である。

セキュリティ･メッセージ･フォーマットを図 9-5 に示す。

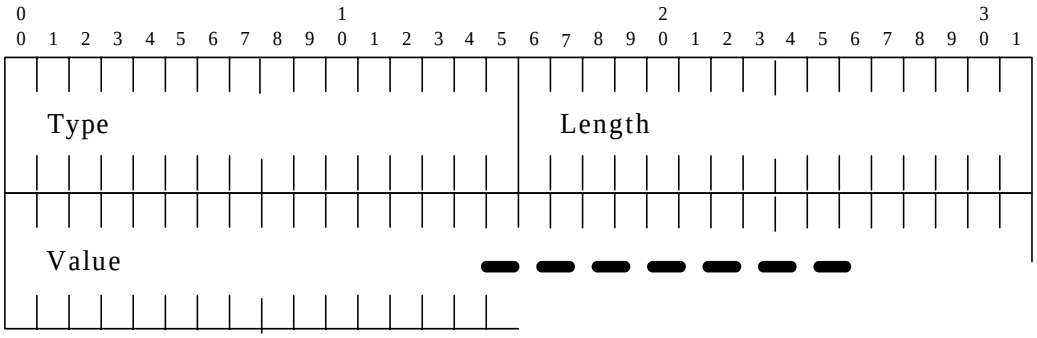


図 9-5　セキュリティ･メッセージ･フォーマット

Type は Value フィールドのデータ種別を示し、Length は Value フィールドのサイズを示す。この様なフォーマットは、TLV (Type,Length,Value) と呼ばれており、本調査でも TLV を利用する。Value フィールドには「SECURITY Option」「Request」「Cluster List」定義されている。

(1) SECURITY Option

本データは、機能確認が行われた後、最初に隣接した機器間で交換が行われる。目的は機器間でのセキュリティ･メッセージをどの様に受け取るかを接続先に伝える事である。

本オプションは、BGP セッション開始時に一度交換され、オプション変更をする

際には BGP セッションのリセットが必要である。

SECURITY Option TLV フォーマットを図 9-6 に示す。

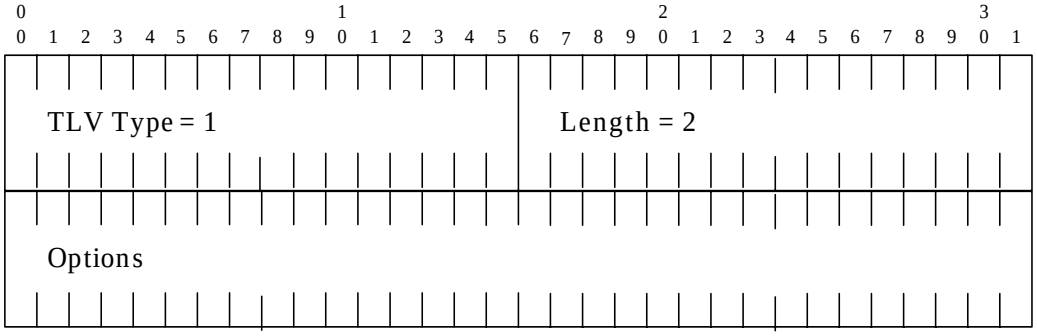


図 9-6　SECURITY Option TLV フォーマット

Option 部分は各ビット単位で意味を表す。

Bit0 の役割は、接続先機器へ経路情報(NLRI)を先に送るのか、証明書→NLRI の順で送るのかを指示する為に利用する。前者の場合には経路収束時間は現状と同等程度であるが、一定期間不正な経路が経路テーブルへ入り込む可能性がある（Routing Information Base(RIB)の更新は行われない）。後者の場合はすべての経路情報を検査した後、経路テーブルへ登録されるため、前者より経路テーブルの更新時間が長く必要である。

Bit1 と Bit2 は既に検証を終えた経路情報について、セキュリティ情報を再検証せずに処理される事を接続先機器へ伝える。Bit1 がセットされている場合は検証済み経路情報が接続先へ送られる事を示しており、Bit2 がセットされている場合は検証済み経路情報を送る事を接続先へ要求し、自身では再検証を行わない事を示している。

Bit1 と Bit2 は iBGP で利用する事で再検証にかかるリソースを軽減されることになるが、eBGP で利用すると不正な経路情報の検証ができない可能性がある為、利用は禁止されている。

⑵ Request TLV

Request TLV は、特定の証明書を指定し接続先に対して要求する。

Request TLV フォーマットを図 9-7 に示す。

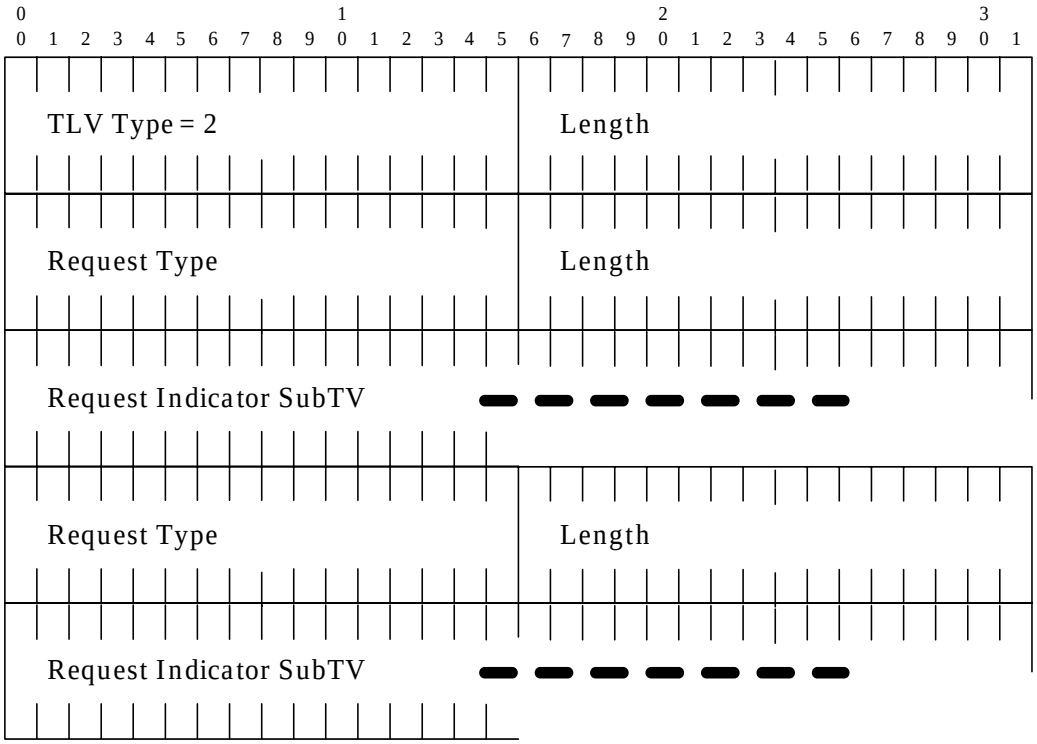


図 9-7　Request TLV フォーマット

Request TLV は、「Request Indicator」で示された条件で「Request Type」で示されている証明書に関して接続先に対して証明書を送る様に要求する。

- 「Request Indicator」にマッチする「EntityCerts」
- 「Request Indicator」にマッチする「ASPolicyCerts」
- 「Request Indicator」にマッチする「PrefixPolicyCerts」
- 「Request Indicator」にマッチするあらゆる証明書

「Request Indicator」には、「割り当て済み/Origin AS 番号」、「署名者/AS 割り当て組織 AS 番号」、「IPv4 アドレス」、「IPv6 アドレス」、「開始シリアル番号」そして「終了シリアル番号」の 6 種類が現在定義されている。

⑶ Cluster List TLV

Cluster List TLV は、受けた経路を Refrect(iBGP で利用される Route Refection と似た動作)して転送する場合に利用し、ClusterID には Reflect した BGP ルータ ID を示す。

Cluster List TLV フォーマットを図 9-8 に示す。

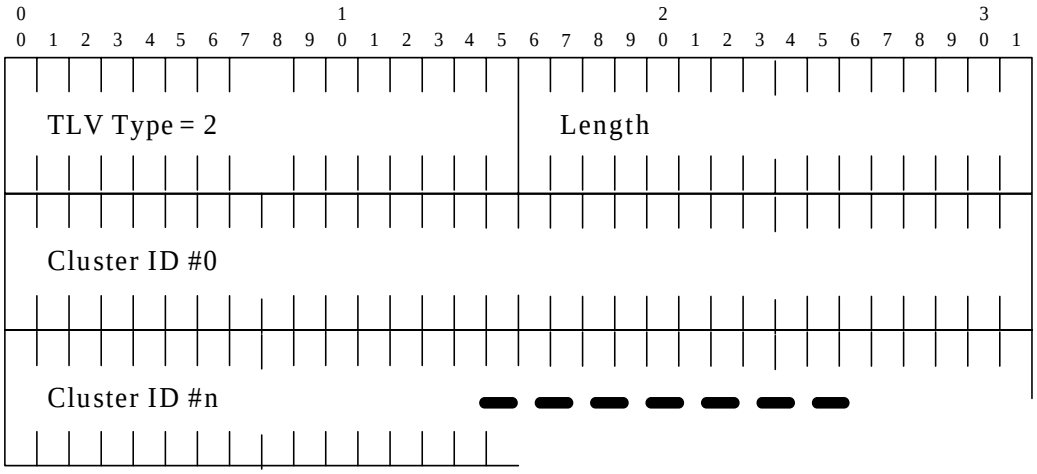


図 9-8　Clister List TLV フォーマット

BGP Refection を利用する BGP ルータは、受け取った BGP セキュリティ・メッセージに ClusterList TLV が定義されているかを確認する必要がある。すでに Cluster List に自身の ID が存在するときには、本メッセージを削除する。自身の ID が存在しないときには追加し、ClusterList TLV が存在しないときには、自身で生成し、追加する。

9.2.1.2. soBGP の情報信頼モデル

soBGP は、公開鍵基盤(PKI)の枠組みを用いて証明書の信頼性を確保する。検証方法は[RFC3280]に従い行われる。

soBGP で基本となる証明書(EntityCert：後述)を Verisign や RIR 等の AS 運用管理組織から信頼されている第 3 組織が運営する認証局を用いて署名する事により、証明書の信頼性を確保し、EntityCert の対となる PrivateKey によりさらに別の証明書に対し署名する事が可能である。検証者は証明書内の認証局名とその署名を確認しながら自身が信用する認証局の署名まで繰り返し確認を行い、自身が信用する認証局が署名までたどり着けない場合には、その証明書は不正に作成されたものであると判断し関わる情報は全て破棄し、CRL や有効期限についても確認が行われ失効している証明書に関しても破棄する。

9.2.1.3. soBGP で利用する証明書

soBGP で利用される証明書は、Entity Certificate(EntityCert)、Authorization Certificate(AuthCert)、Policy Certificate(PolicyCert)の3種類がある。

- EntityCert → AS 運用組織と証明書内の公開鍵が検証可能
- AuthCert → AS が広告する IP アドレスブロック(Origin)である事が検証可能
- PolicyCert →ASPolicyCert と PrefixPolicyCert の2種類あり、前者は AS に関連したポリシ、後者は IP アドレスブロックに関連したポリシが検証可能

⑴ EntityCert に関して

EntityCert は、AS が利用している公開鍵(PublicKey)を配布する為に利用され、AS 番号と公開鍵(PublicKey)が含まれる。 EntityCert に含まれる公開鍵は、AS が発行する様々な証明書を署名する際に利用する秘密鍵(PrivateKey)に対応する公開鍵である。

EntityCert のフォーマットは[RFC3280]で定義され、「AS 番号」は[RFC3779]を

利用し、証明書への署名は[RFC3279[4]]で定義されているsha1withRSAEncryptionを利用する。

EntityCert作成には、EntityCert発行申請者（AS運用組織）がPublicKey/PrivateKeyペアを作成後、AS番号を含んだEntityCert CSRを作成する。作成したEntityCert CSRを証明書発行者（認証局）へ送付する。

EntityCert CSRを受け取った認証局は内容を検証し、情報が正規なものであか検証した後、EntityCert CSRに署名しEntityCertを作成する。作成したEntityCertをAS運用組織へ返送する。

AS運用組織は受け取ったEntityCertを[RFC3280]に基づき検証、問題無ければEntityCertの広告／配布を開始する。

この時点でAS運用組織はEntityCertと対になるPrivateKeyを用いて他の証明書に対して署名可能となる。

soBGPでは、EntityCertをシステム内で一意に識別する為にCertificateSerialNumberとIssuerAltNameを利用する。このフィールドは必ず証明書に含まれていなければならない。

EntityCertの配布法は複数ある。

[4] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC3279)
http://www.ietf.org/rfc/rfc2842.txt

- AS 運用者自身が運用している公開レジストリ若しくは一般に信用されている IP レジストリシステム等に登録し参照者が必要なときに取得する方法
- ネットワークを利用せずに、郵送などの手段を利用する方法
- soBGP で BGP 新たに定義されたセキュリティ・メッセージを利用する方法

初めの2種類に関しては、全てのAS運用者が新しいEntityCertを取得→検証→設定するのに時間必要である為、実際に経路を広告した時、受信側で広告した経路用 EntityCert の検証終了していない可能性がある(つまり経路が破棄される)。最後のセキュリティ・メッセージを利用した場合は、経路制御機器にて即座にその経路に関する EntityCert の検証が可能である。しかし、この方法では、経路制御機器やその他リソースに対して経路交換/検証処理にかかる割合がより大きくなる、また物理回線に占める経路交換情報の比率が上がる事になる(利用者の利用可能帯域が下がる)。

EntityCert を受け取った組織は、[RFC3280]に従い証明書を発行した認証局の署名、有効期限、認証局が発行している CRL も含めて検証を行う。問題が無ければ、EntityCert 内の AS 番号と PublicKey を経路制御機器内に保存し、AS 番号にマッチした組織から広告されたセキュリティ・メッセージ内の経路情報に関して PublicKey を利用した検証準備が出来た事になる。

検証する際に自組織が信頼している第3者機関認証局の証明書も EntityCert(RootEntityCert)として登録し広告しなければならないが、RootEntityCert は自己署名されている為、自動検証は不可能である。RootEntityCert のみは人手により検証され、経路制御機器へ設定する。この時、RootEntityCert が多すぎると運用付加(主に経路制御機器への登録作業)が増大する。また、各組織が独自の判断で第3者機関認証局を選択すると認証局ポリシの違いから不正な経路が紛れ込む可能性も大きくなる。そこで、IANA/RIR/LIR 等の一般的に認知されている権威ある組織が作成した EntityCert を soBGP で利用する場合の最上位の RootEntityCert として定義し手動で登録することにより運用負荷や認証局ポリシの違いから起こりうるリスクの軽減等が可能である。

EntityCert 交換概要を図 9-9 に示す。

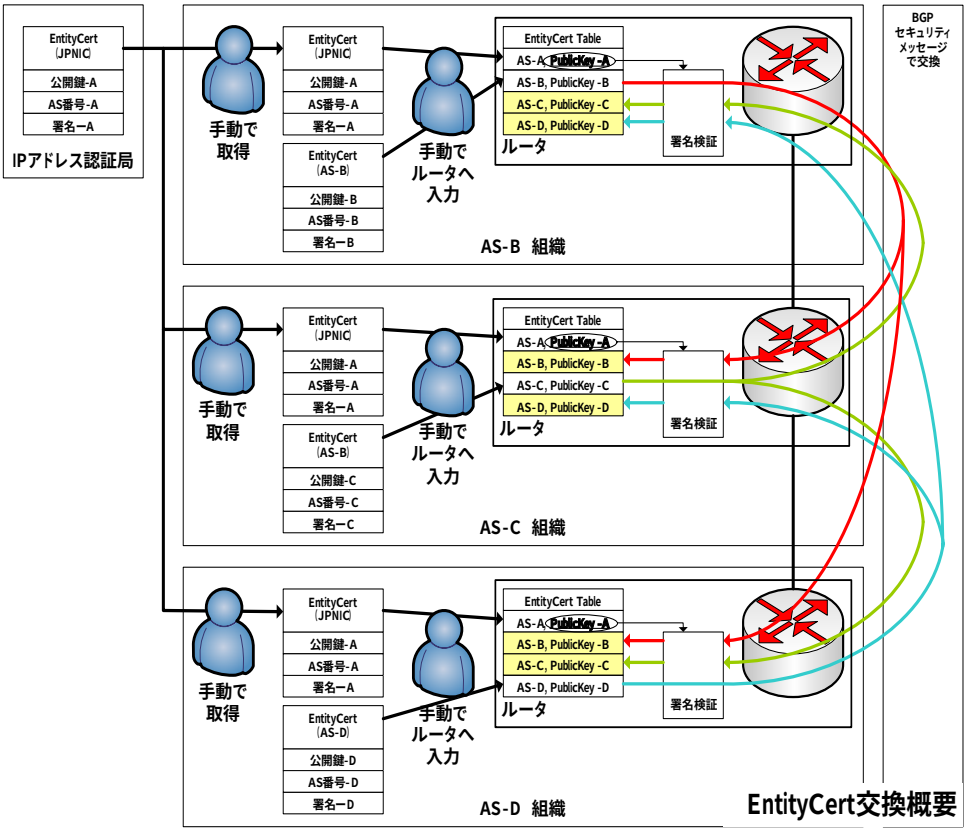


図 9-9　EntityCert を交換する際の概要

EntityCert 証明書は様々な理由で失効するが、有効期限を検査する為に経路制御機器では時刻同期をする必要がある。また、破棄ﾘｽﾄ(CRL)の配布は ASPolicyCert(後述)にて行う。

CRL により EntityCert が失効した時は、失効した EntityCert で検証した情報は全て破棄しなければならない。証明書の有効期限が満了した時には、有効期限が切れる前の証明書で利用した PublicKey/PrivateKey と新しい有効期限で作成された EntityCert が配布された場合には AuthCert と PolicyCert は継続して利用が可能である。しかし、有効期限満了後まったく新しい EntityCert(PrivateKey/PublicKey の再利用はしない)の場合には古い EntityCert で検証した経路情報は破棄しなければならない。

⑵ AuthCert に関して

AuthCert は、AS 運用者が自身を Origin とする IP アドレスブロックであることを証明する為に利用する。自 AS 番号、広告する IP アドレスブロック、IP アドレスブロックを割り振った AS 番号(上位の AS 番号や RIR 等)と IP アドレスの割り振り/割り当てを行った組織の署名が含まれる。

AuthCert を作成するには、後述する署名 TLV 以外の TLV をまとめた後、[RFC3279]で定義されている方法で署名を生成し、署名 TLV を作成する。利用した TLV と署名 TLV を合わせて AuthCert としてセキュリティ・メッセージで広告する。この時、署名に用いられる PrivateKey は IP アドレスブロックを割り当てた組織の EntityCert PublicKey と対となっている物を利用する。AuthCert は、割り当て側が全て作成しても、各々が必要な箇所を埋めても問題は無い。最終的に署名 TLV を作成するのは割り当て側組織である。

AuthCert は、自身を広告する事も可能であるが、後述する PrefixPolicyCert に埋め込まれ、各組織へ配布する形態が考えられている。

AuthCert(PrefixPolicyCert)配送の概略を図 9-10 に示す。

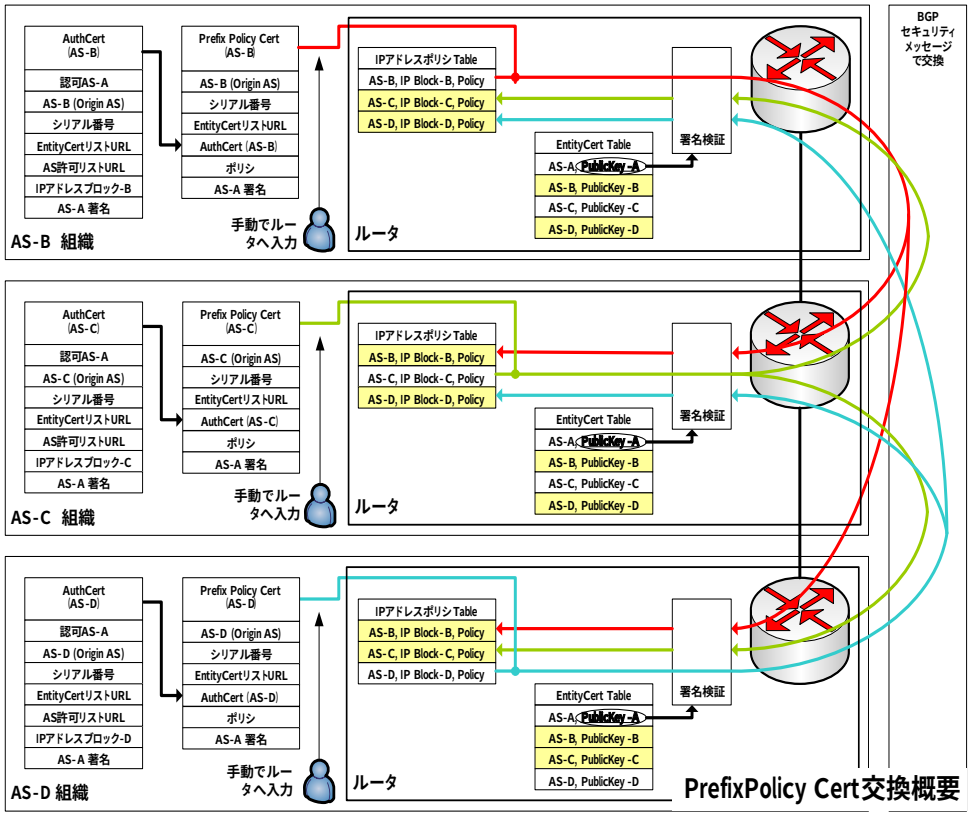


図 9-10　AuthCert 配布の概要

AuthCert の検証には、署名した組織の EntityCert を検証者が持っていなければならない。EntityCert が無い場合は AuthCert を破棄する。EntityCert を取得／検証後、AuthCert の再取得／再検証を行う。EntityCert を検証者が持っている場合には、その中にある PublicKey を利用して AuthCert を検証し、問題が無ければさらに AuthCert 破棄リストを確認し、破棄されていなければ、AuthCert の Address Prefix TLV にある Prefix と Authorized Originator TLV にある AS 番号を利用することが可能である。もし、自己署名された AuthCert を受信したときには注意が必要である。慎重に確認し、個別に判断を下さなければならない。

AuthCert を破棄するためには 3 つの方法がある。一つ目は署名した EntityCert を破棄する。この場合は、個別の IP アドレスブロックの破棄は出来ない。残り 2 つの方法では、IP アドレスブロック別に破棄可能な方法である。二つ目は、AuthCert 用の破棄リストを作成し、この破棄リストを「Authorizing AS Validation List Uniform Resource Locator」で示す。三つ目は、ASPolicyCert(後述)内にある「Authorization Certificate Validity List」を利用する。

AuthCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-11 に示す。

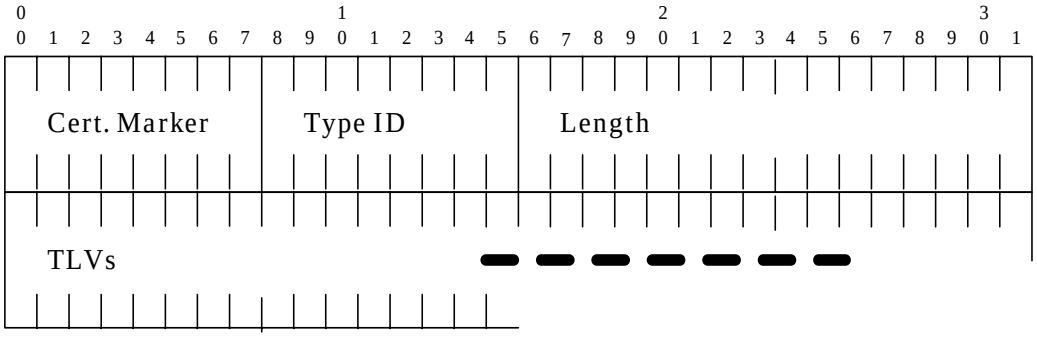


図 9-11　AuthCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)である。Type Id はメッセージ・タイプを示し、AuthCert の場合は「1」を指定する事が規定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Authorizing AS」、「Authorized Originator」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「Authorizing AS Validation List Uniform Resource Locator」、「Address Prefix」そして「Signature」の7種類がある。

「Authorizing AS」TLV は、IP アドレス割り振り／割り当て組織の AS 番号を表す。

Authorizing AS TLV フォーマットを図 9-12 に示す。

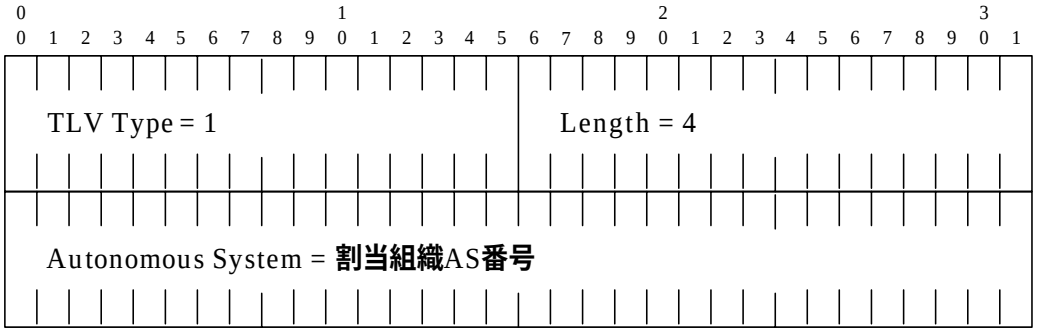


図 9-12　Authorizing AS TLV のフォーマット

「Authorized Originator」TLV は、IP アドレス割り振り／割り当て組織より IP アドレスを割り振り／割り当てられた運用者の AS 番号を表す。

Authorized Originator TLV フォーマットを図 9-13 に示す。

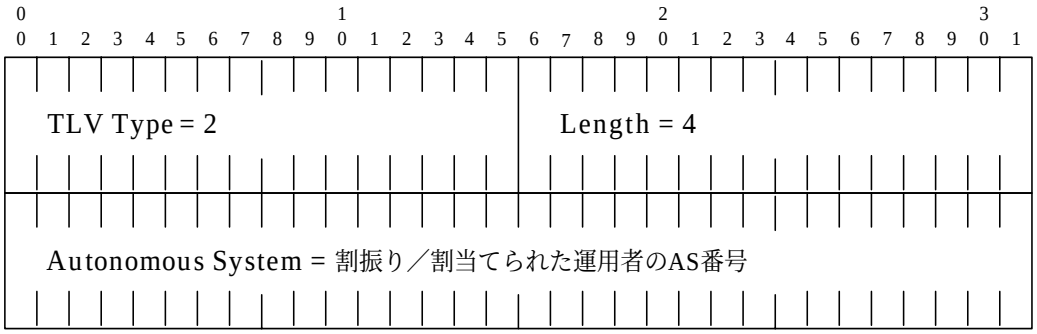


図 9-13　Authorized Originator のフォーマット

「Serial Number」TLV は、IP アドレス割り当て組織により管理され設定する。

Serial Number TLV フォーマットを図 9-14 に示す。

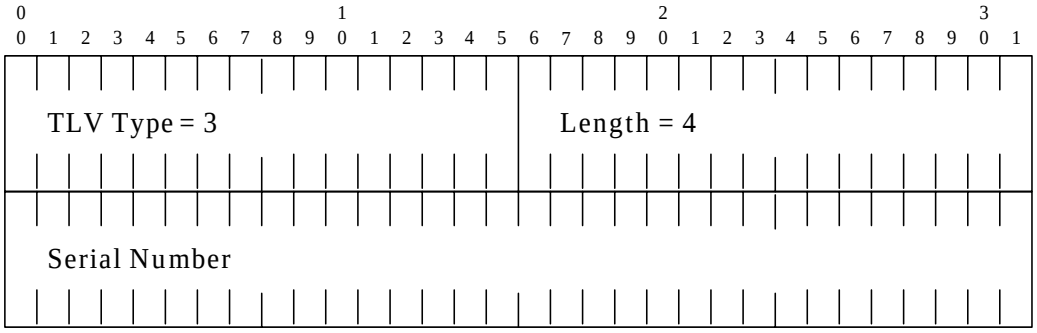


図 9-14　Serial Number TLV のフォーマット

「Authorizing AS EntityCert Uniform Resource Locator」TLV は、IP アドレス割り振り／割り当て組織の最も新しい EntityCert の配布場所を表す URL である。本 TLV は、AuthCert を受け取った機器に既に EntityCert が存在するときには、利用されない可能性や必要無い物として広告しない事もある。

Authorizing AS EntityCert Uniform Resource Locator TLV フォーマットを図 9-15 に示す。

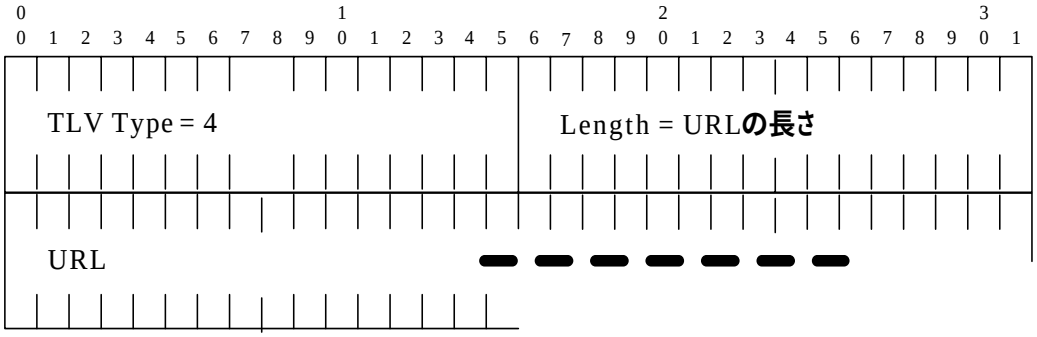


図 9-15　Authorizing AS EntityCert Uniform Resource Lcator TLV フォーマット

「Authorizing AS Validation List Uniform Resource Locator」TLV は、AuthCert の有効／無効を表す最新リストの配布場所を示す URL である。内容は、有効 IP アドレスブロックと無効 IP アドレスブロックを区別できるような形で構成される(ASPolicyCert を参照)。この TLV は、ポリシによっては利用されない可能性がる。また、必要ない物として広告されない可能性もある。

Authorizing AS Validation List Uniform Resource Locator TLV フォーマットを図 9-16 に示す。

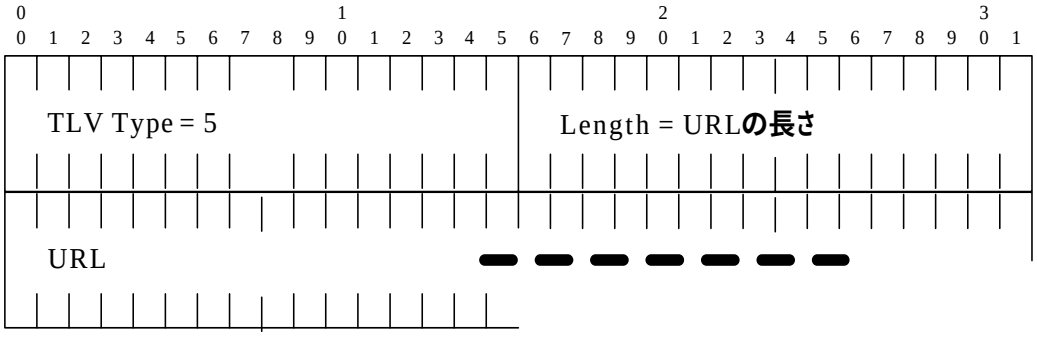


図 9-16　Authorizing AS Validation List Uniform Resource Locator TLV フォーマット

「Address Prefix」TLV は、IP アドレス割り振り組織から割り当てられた IP アドレスブロックを表す。「Address Family Identifier」には、[IANA-AFI[5]]にある値を指定し、「Subsequent AFI」には[IANA-SAFI[6]]にある値を指定する。また「NLRI Data」には[RFC2858]セクション 4 にある形式で IP アドレス・プリフィクスを指定する。

Address Prefix TLV フォーマットを図 9-17 に示す。

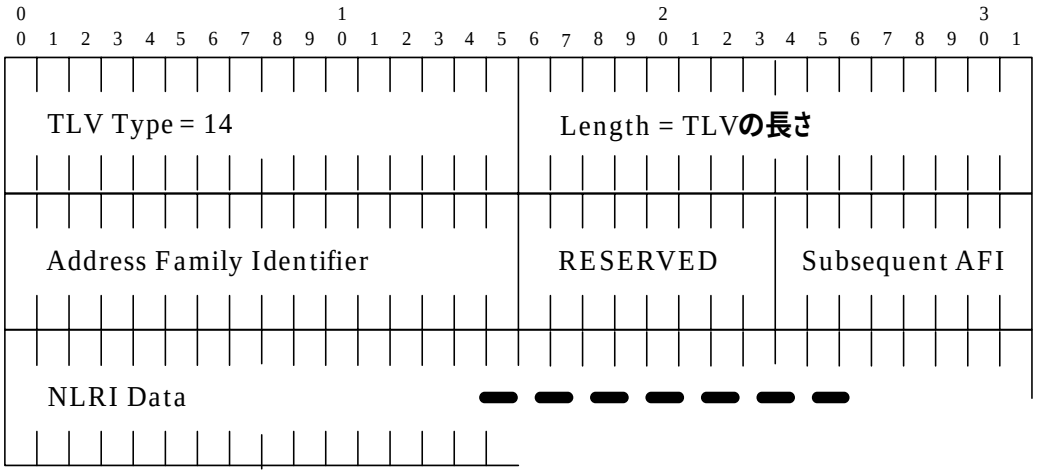


図 9-17　Address Prefix TLV のフォーマット

[5] http://www.iana.org/assignments/address-family-numbers
[6] http://www.iana.org/assignments/safi-namespace

「Signature」TLV は、AuthCert の署名が入る。「Signature Type」には署名アリゴリズムを示し、現在は1のみが定義されている。

Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表す。

「Number of Issuers」は、後に続く割り振り／割り当て組織の組織数を表し、もし Number of Issuers>1 である時は各組織で作られた EntityCert の PublicKey は同じでなければならない。つまり、異なる 2 つ以上の EntityCert PrivateKey で一つの AuthCert を署名することはできない。

「Entity Certificate Issuer Autonomous System」は割り振り組織の AS 番号が入り、「Entity Certificate Serial Number」には割り当て組織の EntityCert に利用したシリアル番号が入る。

「Signature」は Signature Type で生成した署名が入る。

Signature TLV フォーマットを図 9-18 に示す。

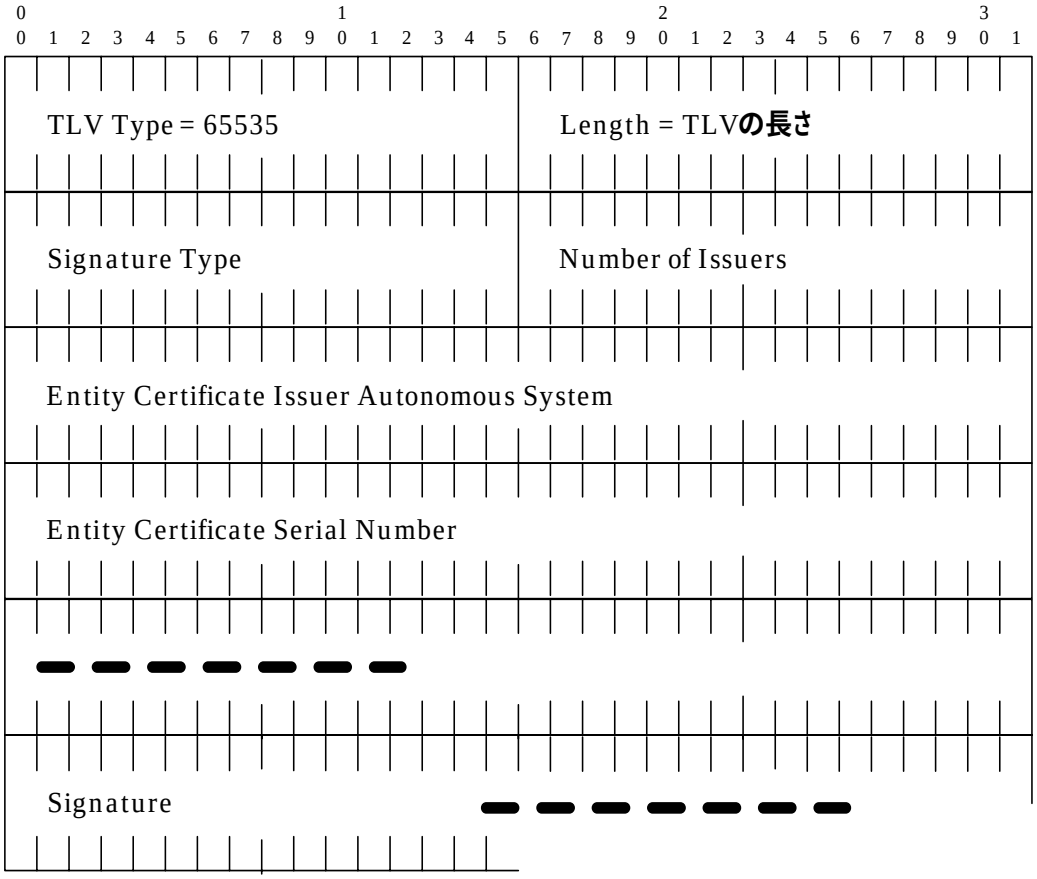


図 9-18　Signature TLV フォーマット

⑶ PrefixPolicyCert に関して

PrefixPolicyCert は、IP アドレスブロックの最大プリフィクス長や AS_PATH の確認の有無等、Origin AS が指定したポリシを証明するために利用する。IP アドレスブロックの Origin AS 番号、AuthCert、ポリシ、署名が含まれる。

PrefixPolicyCert CSR は、IP アドレスブロックの Origin AS 組織が作成する。

PrefixPolicyCert 作成には、署名 TLV 以外の TLV をまとめた後、[RFC3279] で定義されている方法で署名を生成し、署名 TLV を作成する。利用した TLV と署名 TLV を合わせて PrefixPolicyCert としてセキュリティ・メッセージで広告する。この時、署名に用いられる PrivateKey は IP アドレス割り振り／割り当て組織 AS

の EntityCert PublicKey と対になる物である。

PrefixPolicyCert の検証には大きく 2 つのステップがある。これは、PrefixPolicyCert が AuthCert を内包している為である。初めに PrefixPolicyCert に付いている署名の検証、次に PrefixPolicyCert に内包されている AuthCert に付いている署名の検証を行う。双方とも EntityCert を検証者が持っていなければならない。もしどちらか一方の EntityCert が無い場合でも PrefixPolicyCert は破棄され、正規の EntityCert を取得後、再検証を行う。EntityCert を検証者が持っている場合には、EntityCert PublicKey を利用して署名を検証し、問題ない場合に AuthCert 内にある IP アドレスブロックが PrefixPolicyCert 内にあるポリシの範囲で利用可能である。署名が自己署名であった場合には慎重に確認したうえで個別に判断を下さなければならない。

PrefixPolicyCert を破棄する(もしくは有効にしない)ためには 2 つの方法がある。一つ目は EntityCert を破棄することにより署名検証不可にする。もう一つは PrefixPolicyCert 個別に破棄が可能で ASPolicyCert(後述)にある「Prefix Policy Certificate Validity List」TLV を利用する。この TLV で破棄が指定された PrefixPolicyCert は破棄されなければならない。

PrefixPolicyCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-19 に示す。

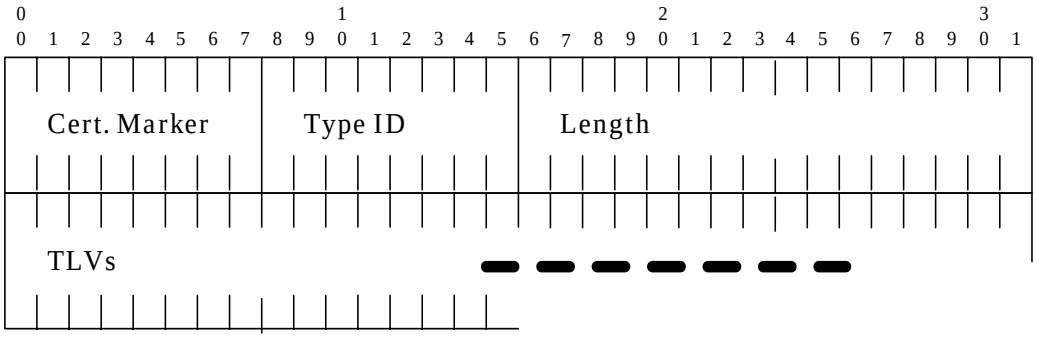


図 9-19　PrefixPolicyCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)、Type Id はメッセージのタイプを表し、PrefixPolicyCert の場合は「2」を指定することが規

定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Originating Autonomous System」、「Serial Number」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「AuthCert」、「Policies」、「SubTVs」そして「Signature」の 8 種類がある。

「Originating Autonomous System」TLV は Origin AS 番号を表す。

Originating Autonomous System TLV フォーマットを図 9-20 に示す。

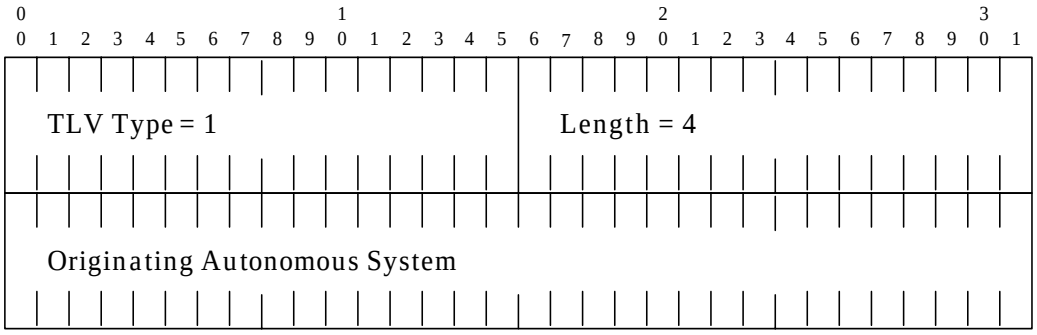


図 9-20　Originating Autonomous System TLV フォーマット

「Serial Number」TLV は、PrefixPolicyCert のシリアル番号を表す。

Serial Number TLV フォーマットを図 9-21 に示す。

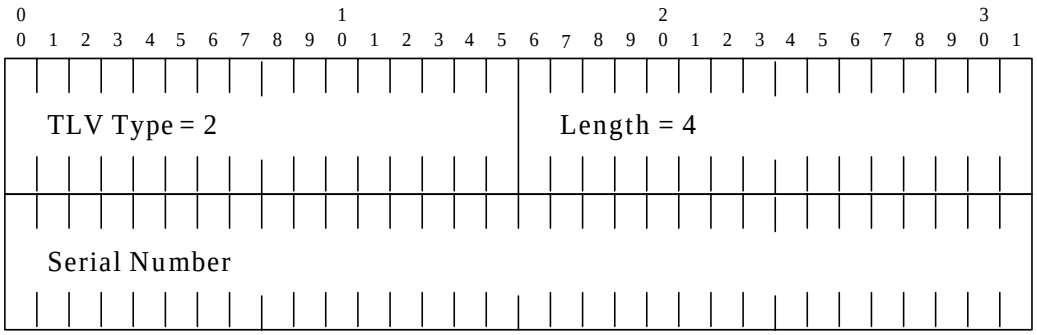


図 9-21　Serial Number TLV フォーマット

「Authorizing AS EntityCerts Uniform Resource Locator」TLV は、IP アドレス割り振り／割り当て組織の最も新しい EntityCert の配布場所を表す URL である。本 TLV は、PrefixPolicyCert を受信した機器に既に EntityCert が存在する時には、利用されない可能性、必要ないものとして広告されない可能性がある。

Authorizing AS EntityCerts Uniform Resource Locator TLV フォーマットを図 9-22 に示す。

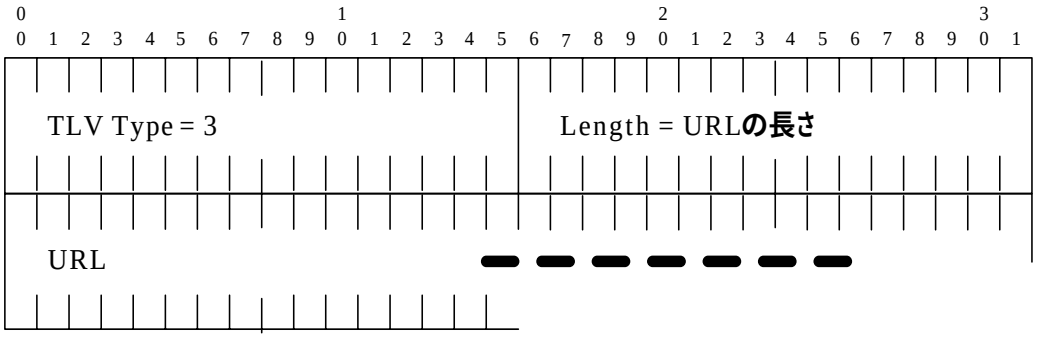


図 9-22 Authorizing AS EntityCerts Uniform Resource Locator TLV フォーマット

「AuthCert」TLV は、AuthCert がそのまま埋め込まれる。PrefixPolicyCert でポリシを示したい IP アドレスブロックに該当する AuthCert が入る。

AuthCert TLV フォーマットを図 9-23 にしめします。

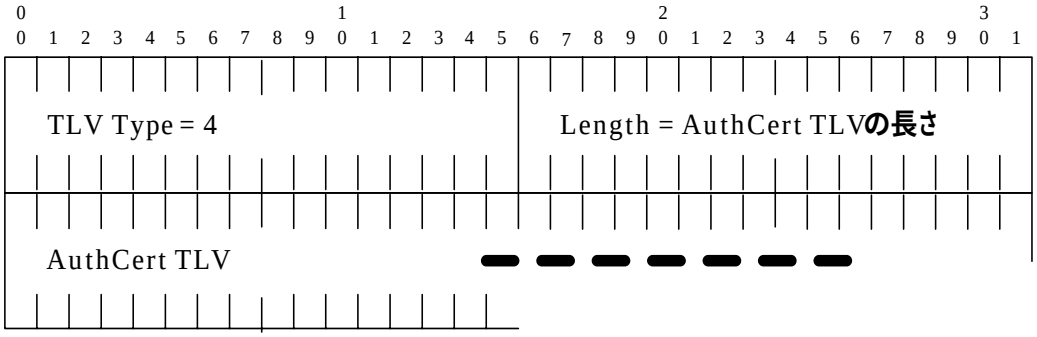


図 9-23　AuthCert TLV フォーマット

「Policies」TLV は、AuthCert 内で示されている IP アドレスブロックに対するポリシを指定する。Option はビット・フィールドで各々のビットをセットすることでポリシを指定し、SubTV(後述)によりポリシの拡張を行う。

Policies TLV フォーマットを図 9-24 に示す。

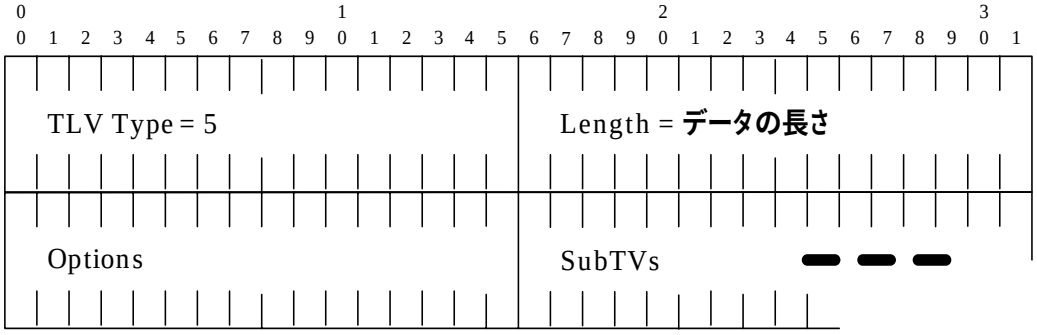


図 9-24　Policies TLV フォーマット

「Options」の Bit0 がセットされた場合、AS_PATH が検証できない経路情報に関しては利用すべきでないことを表し、Bit1 がセットされた場合 AS_PATH の 2 番目の AS に関する情報が検証できない場合には、この AS にかかわる経路情報は利用すべきでないことを表す。他のビットに関しては未定義となっているが将来利用される予定である。

「SubTVs」は、AuthCert 内で示されている IP アドレスブロックに対してオプション・ポリシを指定する。TV Type によりオプションを指定し、必要なパラメータをデータ部に記述する。現在は、3 種類のタイプが定義されている。

SubTVs フォーマットは図 9-25 に示す。

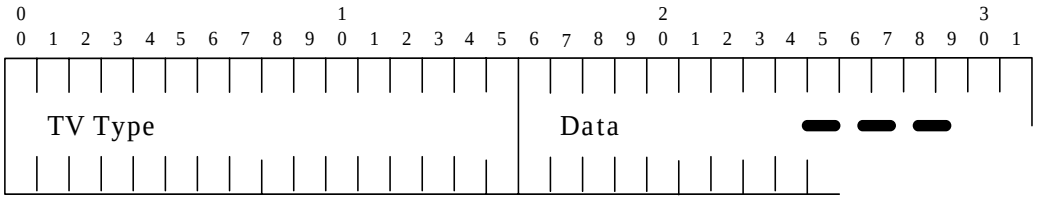


図 9-25　SubTVs フォーマット

TV Type が 1 の時は、AuthCert 内の全ての IP アドレスブロックに関して、Data 部に示された AS 番号が AS_PATH に含まれる事を必要とし、TV Type が 2 の時には、AuthCert 内のいずれかの IP アドレスブロックに関して、Data 部に示された AS 番号が AS_PATH に含まれる事を必要とする。TV Type が3の時には、Data には AuthCert 内にある IP アドレスブロックで利用可能な最大 Prefix 長を示す。

「Signature」TLV は、PrefixPolicyCert 証明書の署名である。「Signature Type」には署名アルゴリズムが入り現在は1のみが定義されている。Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表し、「Number of Issuers」は後に続く割り振り／割り当て組織の組織数を示す。Number of Issuers > 1 である時は、各組織で作られた EntityCert PublicKey は同じでなければならない。つまり異なる 2 つ以上の EntityCert で一つの PrefixPolicyCert を署名することは出来ない。「Entity Certificate Issuer Autonomous System」は割り振り／割り当て組織の AS 番号、「Entity Certificate Serial Number」には割り振り／割り当て組織の EntityCert に利用したシリアル番号、「Signature」は Signature Type で生成した署名が入る。

Signature TLV フォーマットを図 9-26 に示す。

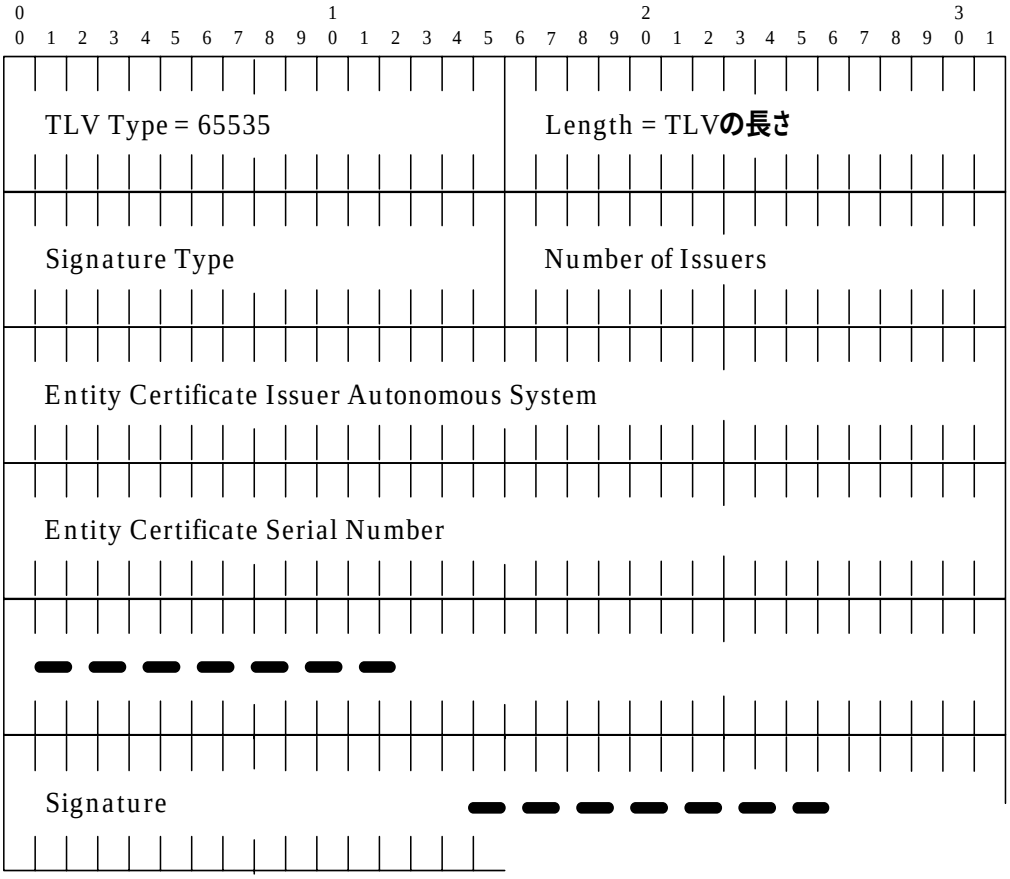


図 9-26　Signature TLV フォーマット

⑷ ASPolicyCert に関して

ASPolicyCert は、隣接組織の AS 番号等、組織単位のポリシを証明するために利用する。トランジット AS リスト、非トランジット AS リストや「Authorization Certificate Validity List」等が含まれる。

ASPolicyCert 作成には署名 TLV 以外の TLV をまとめた後、[RFC3279]で定義されている方法で署名を生成し、署名 TLV を作成、利用した TLV と署名 TLV を合わせて ASPolicyCert としてセキュリティ・メッセージで広告する。署名に用いられる PrivateKey は自 AS 用の EntityCert PublicKey で検証可能な PrivateKey である。ASPolicyCert は Origin AS 組織が作成する。

ASPolicyCert TLV と署名 TLV をまとめ、セキュリティ・メッセージで各組織へ配布される。概略を図 9-27 に示す。

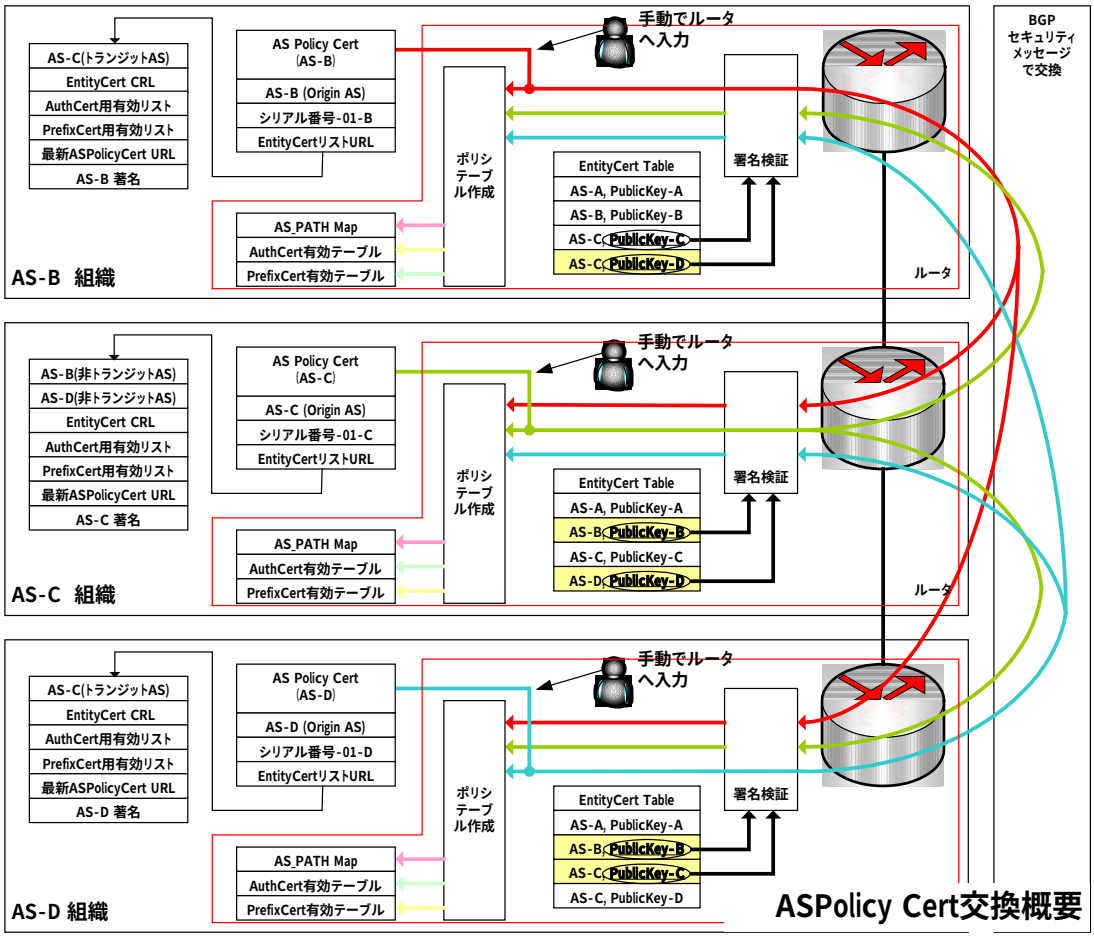


図 9-27　ASPolicyCert 配布概略

ASPolicyCert の検証には、署名した組織の EntityCert を検証者が取得していなければならない。EntityCert が無い時には、ASPolicyCert を信用してはならない。EntityCert を取得後、再検証を行う。EntityCert PublicKey を利用して ASPolicyCert を検証し問題なければ、さらに EntityCert の CRL を確認後、ASPolicyCert 内にある情報（隣接 AS リストや Validation List 等）が利用可能である。自己署名された ASPolicyCert を受信した場合には注意が必要である。慎重に確認したうえで個別判断を下さなければならない。

ASPolicyCert は、一度登録されると署名検証に必要な EntityCert を破棄する以外の方法では自動で破棄されることはない。AS が存在し相互接続されている

環境では必ず広告される。ポリシの変更をする時には内容を変更し署名した新しい ASPolicyCert を広告することで ASPolicyCert は上書きされる。

ASPolicyCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-28 に示す。

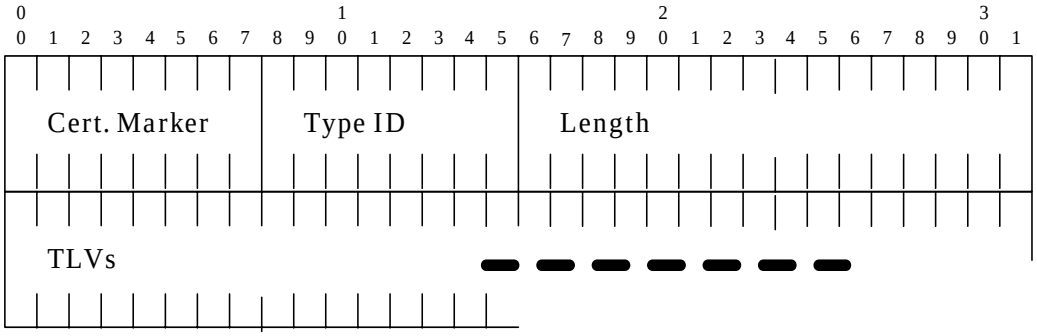


図 9-28　ASPolicyCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)、Type ID はメッセージ・タイプを表し、ASPolicyCert の場合は「3」を指定することが規定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Originating Autonomous System」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「Attached Transit Autonomous Systems」、「Attached Non-transit Autonomous Systems」、「Revoked Entity Certificate List」、「Authorization Certificate Validity List(With Validity Ranges)」、「Prefix Policy Certificate Validity List(With Validity Ranges)」、「Most Recent AS Policy Certificate Uniform Resource Locator」そして「Signature」の11種類がある。

「Originating Autonomous System」TLV は Origin AS 番号を表す。

Originating Autonomous System TLV フォーマットを図 9-29 に示す。

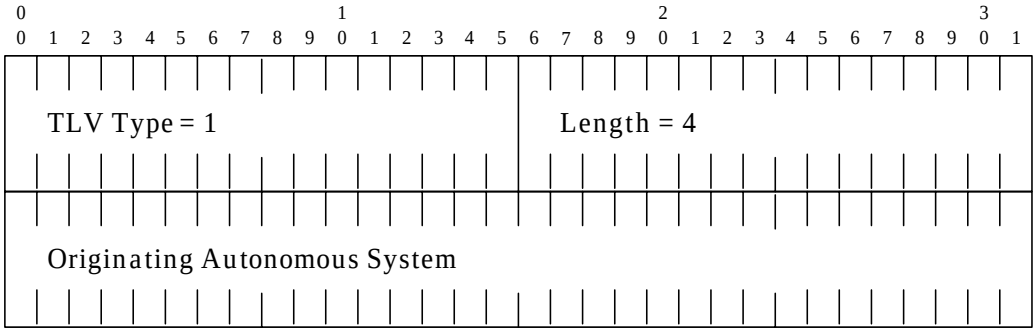


図 9-29　Originating Autonomous System TLV フォーマット

「Serial Number」TLV は署名者により管理され設定される。

Serial Number TLV フォーマットを図 9-30 に示す。

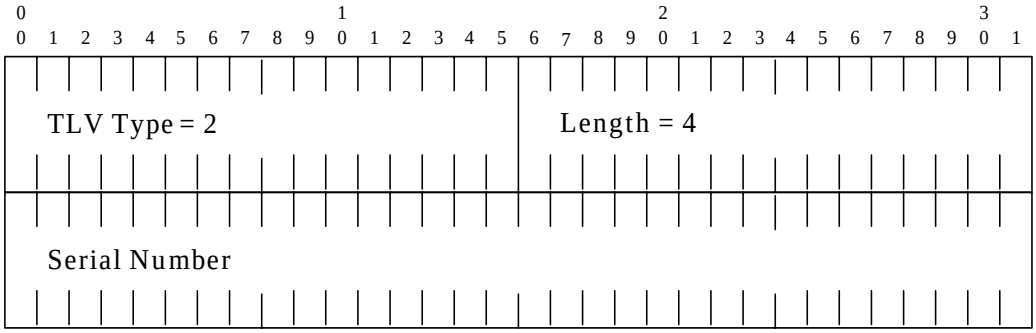


図 9-30　Serial Number TLV フォーマット

「Authorizing AS EntityCert Uniform Resource Locator」TLV は、署名した EntityCert の配布場所を示す URL である。この TLV は、ASPolicyCert を受信した機器に既に EntityCert が存在する場合は、利用されない可能性がある、必要無い物として本 TLV は広告しない可能性もある。

Authorizing AS EntityCert Uniform Resource Locator TLV フォーマットを図 9-31 に示す。

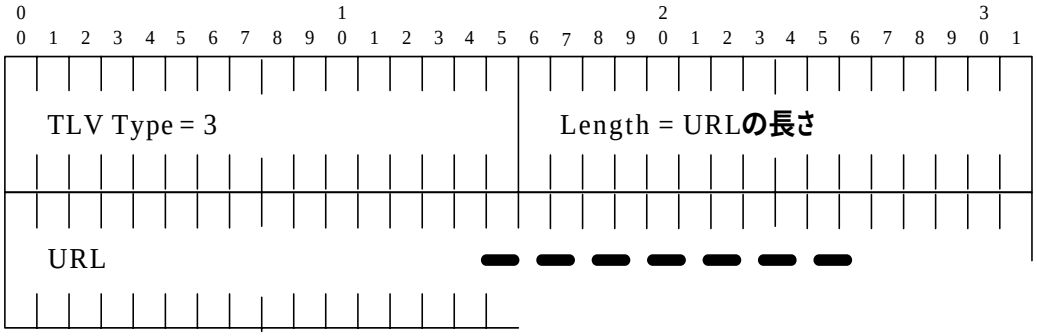


図 9-31　Authorizing AS EntityCert Uniform Resource Locator TLV フォーマット

「Attached Transit Autonomous Systems」TLV は、自組織と接続されているトランジット AS を表す。自組織が複数のトランジット AS が接続されている場合には、本 TLV は一つのセキュリティ・メッセージ内複数現れる。「Address Family Identifier」には[IANA-AFI]にある値を指定,「Subsequent AFI」には[IANA-SAFI]ある値を指定,「Autonomous Systems」には自組織に接続されているトランジット AS を指定する。

Attached Transit Autonomous Systems TLV フォーマットを図 9-32 に示す。

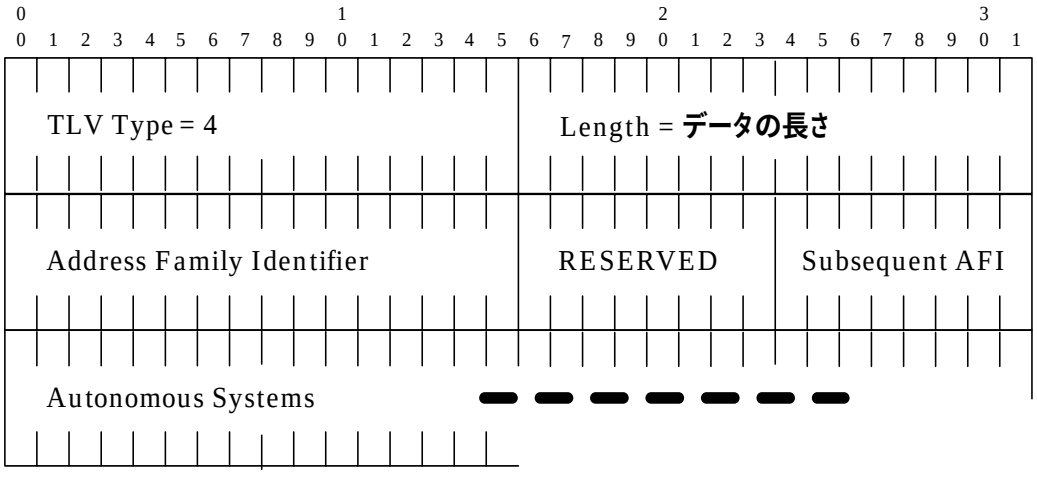


図 9-32　Attached Transit Autonomous Systems TLV フォーマット

「Attached Non-transit Autonomous Systems」TLV は、自組織と接続されている非トランジット AS を表す。自組織が複数の非トランジット AS が接続されている

場合には、本 TLV は一つのセキュリティ・メッセージ内複数現れる。「Address Family Identifier」には、[IANA-AFI]にある値を指定、「Subsequent AFI」には[IANA-SAFI]にある値を指定、「Autonomous Systems」には自組織に接続されている非トランジット AS を指定する。

Attached Non-transit Autonomous Systems TLV フォーマットを図 9-33 に示す。

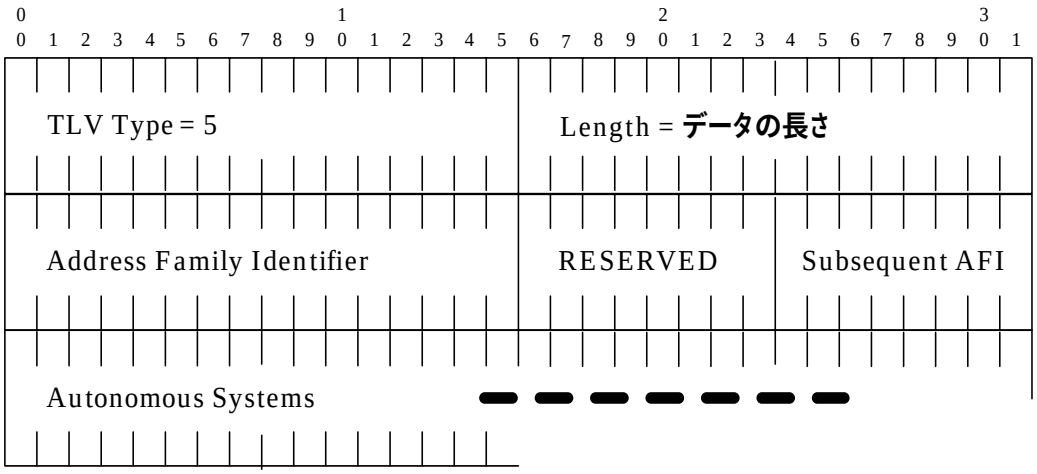


図 9-33　Attached Non-transit Autonomous Systems TLV フォーマット

「Revoked Entity Certificate List」TLV は、自組織の EntityCert 破棄証明書リストを表し、フォーマットは[RFC3280]に定義されている破棄証明書を利用する。

Revoked Entity Certificat List TLV のフォーマットを図 9-34 に示す。

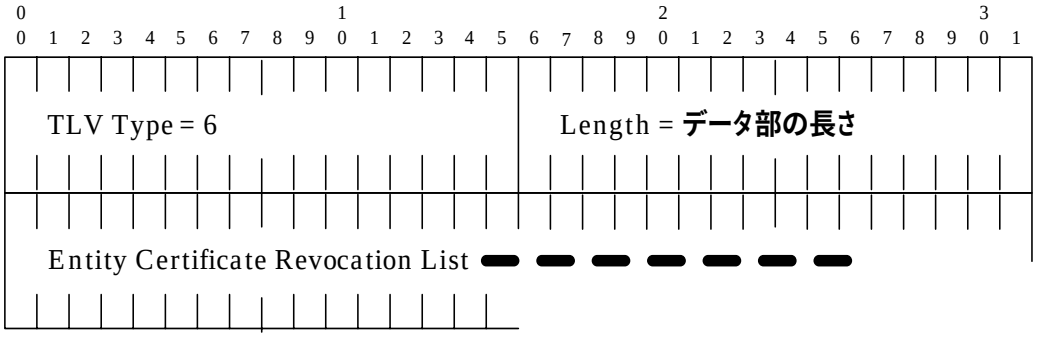


図 9-34　Revoked Entity Certificat List TLV フォーマット

「Authorization Certificate Validity List」TLV は、Origin AS が作成した AuthCert 証明書に対して「Validity Ranges」SubTV に指定されたシリアル番号の証明書が有効か無効かを示す。無効を示された AuthCert は削除されなければならない。

Authorization Certificate Validity List TLV のフォーマットを図 9-35 に示す。

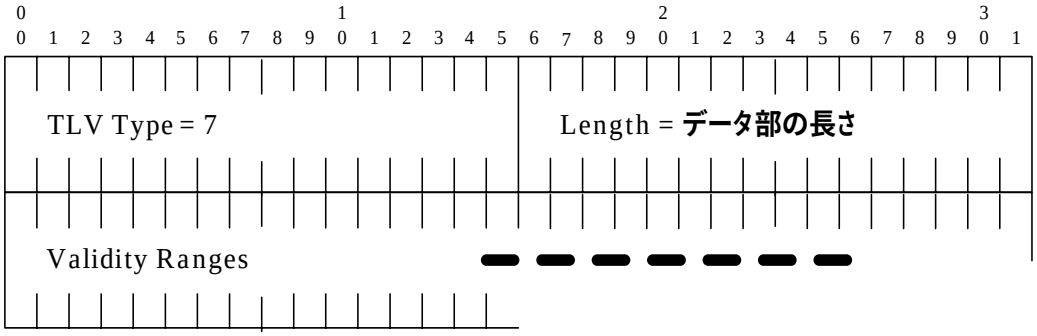


図 9-35　Authorization Certificate Validity List TLV フォーマット

「Validity Ranges」SubTV は、シリアル番号の範囲を指定して有効／無効を示す。「SubTV Type」へは有効／無効を指定し、「Size of Range」へは範囲を指定する。また、「Lowest Authorization Serial Number」へは最小のシリアル番号を指定する。

この SubTV は「Prefix Policy Certificate Validity List」TLV でも利用する。

Validity Ranges SubTV のフォーマットを図 9-36 に示す。

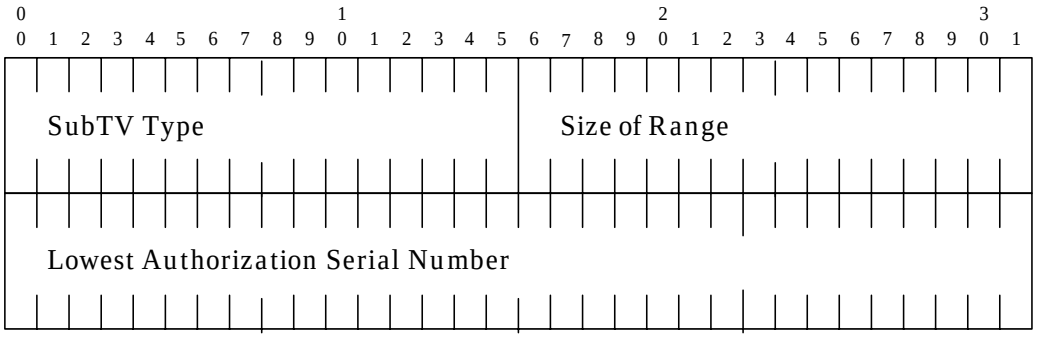


図 9-36　Validity Ranges SubTV フォーマット

「Prefix Policy Certificate Validity List」TLV は、Origin AS が作成した PrefixPolicyCert に対して「Validity Ranges」SubTV に指定されたシリアル番号の証明書が有効か無効かを示す。無効を示された PrefixPolicyCert は削除されなければならない。

Prefix Policy Certificate Validity List TLV のフォーマットを図 9-37 に示す。

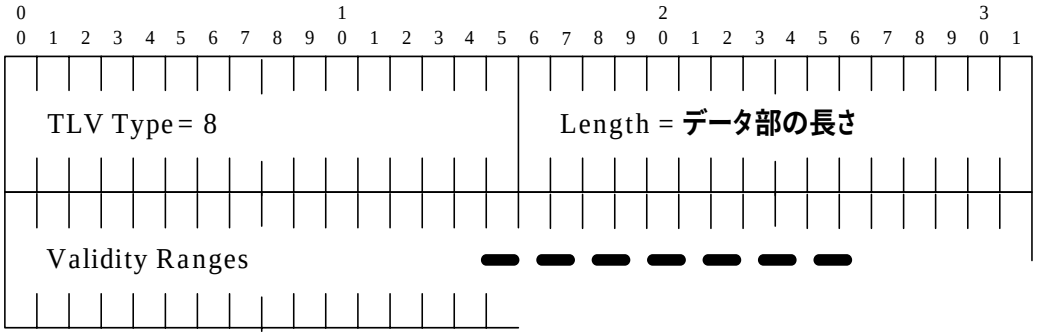


図 9-37　Prefix Policy Certificate Validity List」TLV フォーマット

「Most Recent AS Policy Certificate Uniform Resource Locator」TLV は、Origin AS が作成した最新の ASPolicyCert がある配布場所の URL を示す。

Most Recent AS Policy Certificate Uniform Resource Locator TLV のフォーマットを図 9-38 に示す。

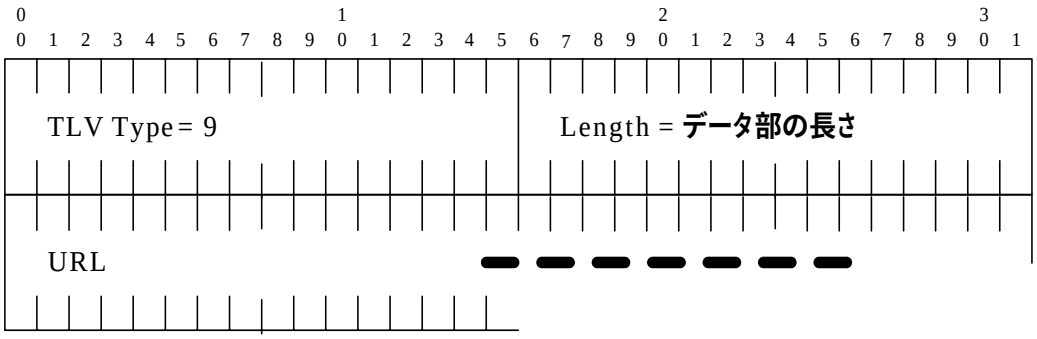


図 9-38　Most Recent AS Policy Certificate Uniform Resource Locator TLV フォーマット

「Signature」TLV は、ASPolicyCert の署名である。「Signature Type」には署名アルゴリズムが入り現在は 1 のみが定義されている。Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表し、「Number of Issuers」は署名組織の数を示す。もし Number of Issuers > 1 である時には各組織で作られた EntityCert の PublicKey は同じでなければならない。つま

り、異なる 2 つ以上の EntityCert で一つの ASPolicyCert を署名することは出来ない。「Entity Certificate Issuer Autonomous System」は Origin AS の AS 番号が入り、「Entity Certificate Serial Number」には Origin AS の EntityCert に利用したシリアル番号が入る。「Signature」は Signature Type で生成した署名が入る。

Signature TLV のフォーマットを図 9-39 に示す。

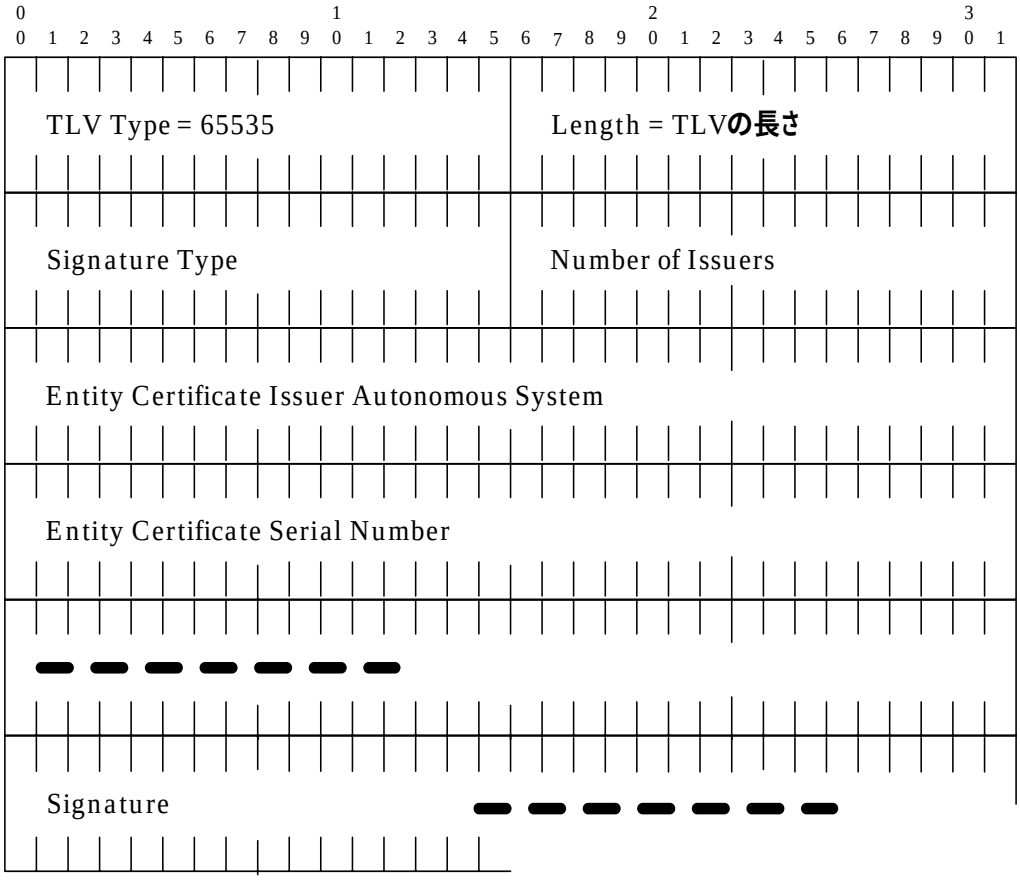


図 9-39　Signature TLV フォーマット

⑸ 各証明書の関係図

各証明書の関係図を図 9-40 に示す。

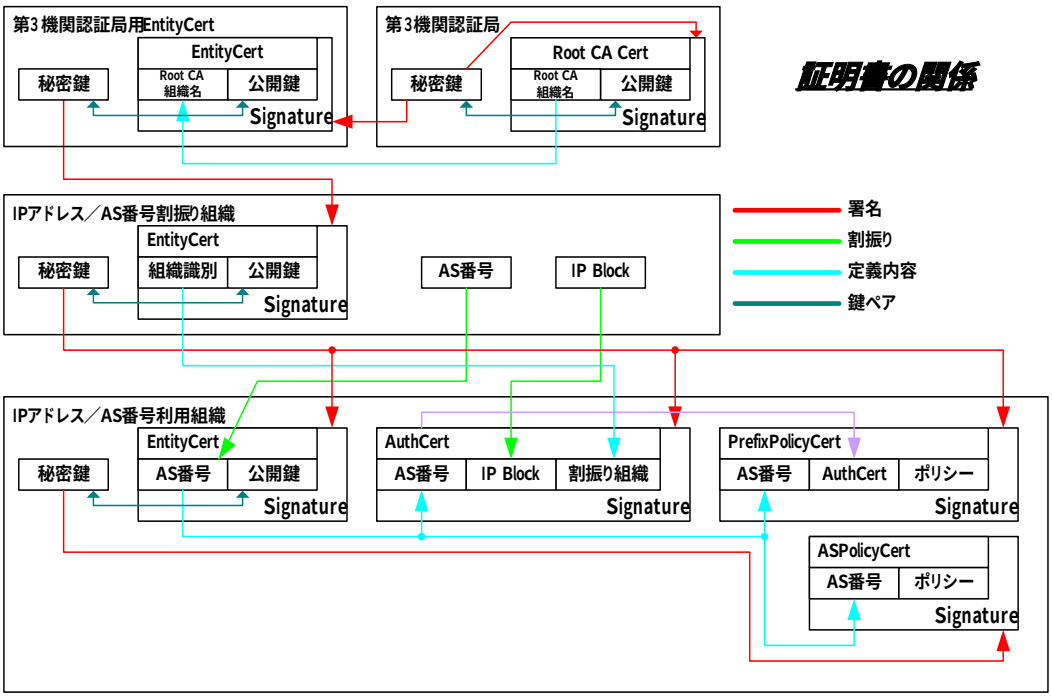


図 9-40　各証明書の関係図

9.2.1.4. 署名の確認

各署名の確認は、図 9-40「証明書の関係」の Signature の矢印を逆向きにたどり、最終的には第 3 機関の認証局の CA にたどり着き終わる。ただし、常に第 3 機関の認証局の CA で確認することは行っていない、なぜなら第 3 機関の認証局の CA まで確認するには人手を介さなければできないからである。自動化するには初めに手動で信用した EntityCert 内の情報を soBGP システムに手動で登録しておき、soBGP ではこの情報を Root して扱うことにより署名の確認が自動化される。

9.2.1.5. soBGP 動作の概略

soBGP 動作概要を図 9-41 に示す。

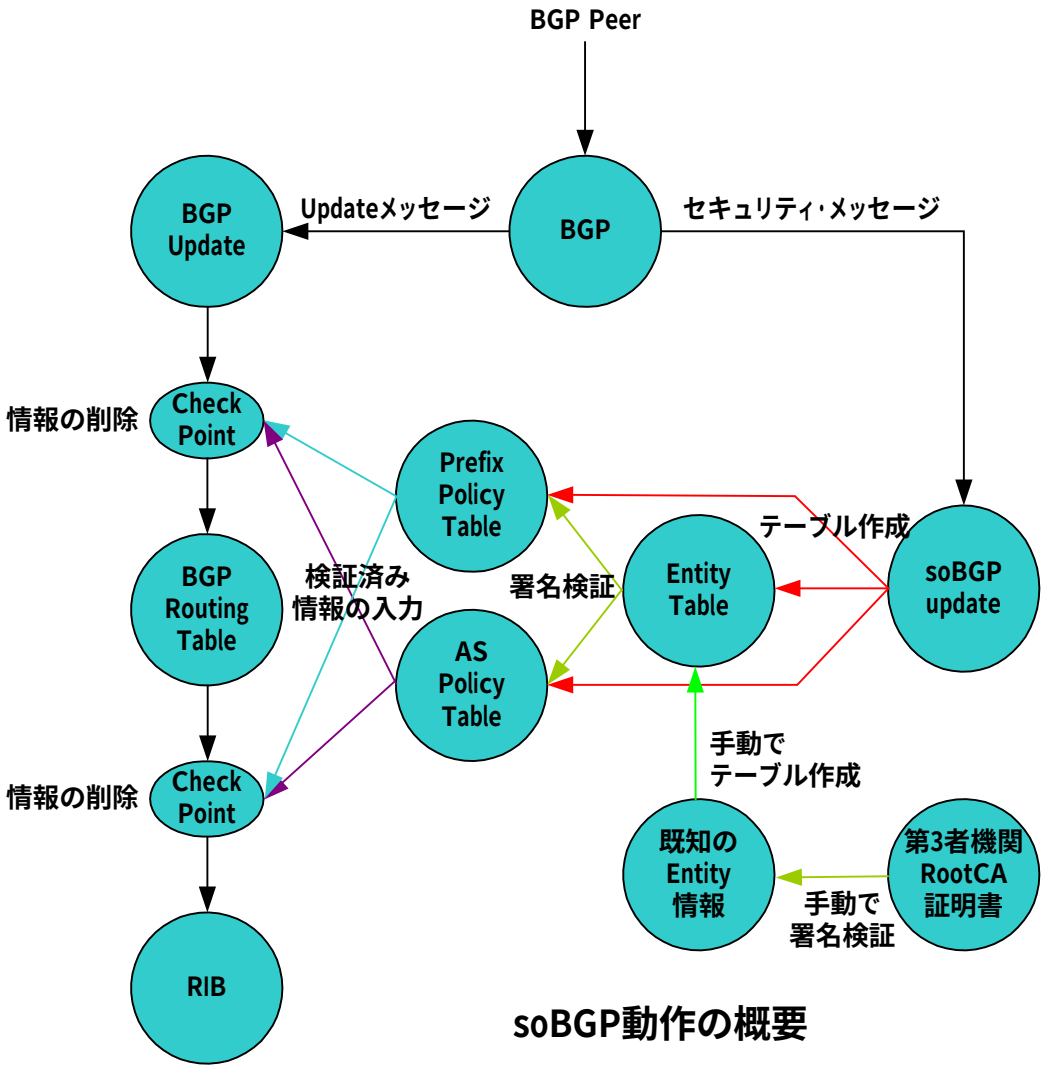


図 9-41　soBGP 動作概要

soBGP を開始する際には、既知の EntityCert(本書では RootEntityCert と呼ぶ)を取得し第 3 者機関の CA 証明書で署名の検証を行い問題がなければルータへ手動で入力しテーブルを作成する。主なデータは{Serial 番号、AS 番号、PublicKey}である。

次に、BGP Peer 間で Capability 確認を行い双方で動作可能であれば、セキュリティ・メッセージの交換を開始する。最初に交換されるセキュリティ・メッセージである Security Option を交換し、図中のどちらの Checkpoint を利用するかを決定する。BGP Routing Table 以前の Checkpoint で経路情報の確認を行う際にはすべての経路情報に関する証明書がないと Routing Table に追加されない。つまり、Routing Table 作成に時間がそれなりにかかる。BGP Routing Table 後の Checkpoint を選択した場合には、Routing Table の構

築には既存の状態と変わらないが、実際の RIB へのインストールは証明書の検証後ということになる。前者は正常な証明書がないものは Routing Table に載らないので経路情報として確認することができない、その代わり Routing Table に費やすリソースは減る。後者は正常な証明書がなくても Routing Table にのるので経路情報を確認することが可能である。その経路情報を見ながら手動で例外を作成することも可能となる。しかしルータのリソースは必要である。

次は EntityCert、PrefixPolicyCert、ASPolicyCert を受信して、到着順に署名の確認を行う。もし、必要な証明書が無い時には、その都度 BGP Peer へリクエストし必要な証明取得を試みた後、再度検証を行う。もし、検証に必要な証明書が取得できないときにはその受信した Cert は破棄される。署名の確認の取れた PrefixPolicyCert と ASPolicyCert のポリシは Checkpoint へ渡され、経路情報への確認を行い問題なければ利用を開始する。しかし、問題があった経路情報に関しては破棄される。

Checkpoint での検証例としては、ASPolicyCert が持つトランジット AS リストと非トランジット AS リストから AS 接続図を作成し、この接続図を基にして AS_PATH の検証が可能である。また、PrefixPolicyCert が持つ最大 Prefix Length では Origin AS が意図していない長さの Prefix を持った経路情報の検証が可能である。

9.2.2. IP アドレス証明書システムと JPIRR の連携モデル

本節では、JPNIC で現在運用されている IP アドレス証明書システムと JPIRR と soBGP の連携について述べる。

IP アドレス証明書システムは、JPNIC が IP アドレスブロックや AS 番号をサービス・プロバイダへ割り振りを行う際に自動的に IP アドレス情報を含んだ証明書を作成するシステムの事である。詳細は、JPNIC 資料を参照、JPIRR は前章を参照。

連携モデルを作る前に証明書に署名する際に利用される PrivateKey の保護について述べておく必要がある。soBGP の利用をするということは、すべての AS 運用者が同じセキュリティレベルにあることが要求される。これは、AS 運用者が PrivateKey を利用した署名行為を行うからである。PrivateKey が一つでも漏洩しそのまま放置されると情報を詐称する事が可能となり soBGP を利用する意味がなくなる。soBGP システム全体を保護するためにも PrivateKey を保護するための統一ポリシを作成し運用者全体が統一した PrivateKey の運

用を行うことが必要である。

ただし、各組織で PrivateKey の適切な運用を行うためには、設備投資、人的リソースの増大等いろいろな面で各組織に負担がかかる。つまりは、soBGP 導入に関して積極的になれない要素となる。各組織の運用、設備投資を最小限に抑えた形で PrivateKey 運用ポリシとシステムを構築することが重要である。

9.2.2.1. soBGP における JPNIC の役割

図 9-40「証明書の関係」にて主な役割は定義されている。「IP アドレス／AS 番号割振り組織」が JPNIC に当たるが、自身が割り振った情報に対しての署名処理と認証局の運用／管理ポリシの作成が主な役割となる。

9.2.2.2. 連携システム概要

ここでは JPNIC で現行動いている IP レジストリシステムと soBGP で必要とされる証明書システムの連携をまとめる。

連携システムの目的は正確な情報(IP レジストリシステムに登録されている情報)を元に EntityCert 証明書や署名した TLV を Secure な環境下で効率よく作成し、Routing システムへ渡す事、Routing システムからの証明書や署名確認の問い合わせに対して迅速に応答する事である。

連携システムは、IP アドレス認証局、IP アドレス証明書システム、AS 内証明書システム、AS 内認証局が soBGP に関わる証明書や署名つき TLV を作成するために必要となる。また、JPIRR への情報を提供することにより JPIRR に登録されている情報の検証を行う事も考えられる。本調査では、認証局としてのポリシを述べる事はしないが、本調査にある連携システムでは、全ての認証局運営組織は同じセキュリティレベルが定義されているポリシを共通で利用し認証局運用する事がセキュリティ上重要である。理由は、署名されたデータは Routing システム介して全ての組織に広告されるためである。これは、経路制御システムで署名つき TLV を交換している組織は全て同一セキュリティドメインであるといえる。

連携システム概略図を図 9-42 に示す。

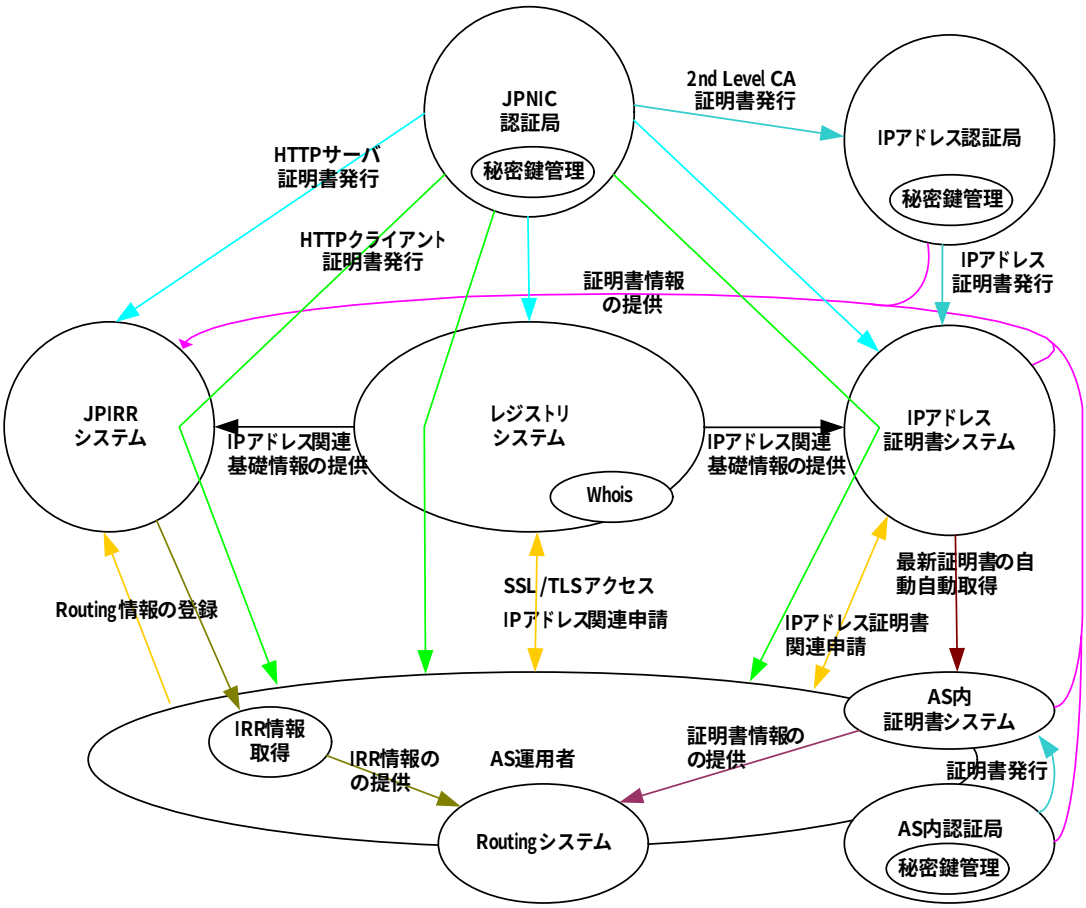


図 9-42　連携システム概略図

⑴ IP アドレス認証局

IP アドレス認証局は、JPNIC にて管理／運用され、その機能は JPNIC が割り振り／割り当てを行った IP アドレスブロックや AS 番号等の情報を含む CSR (EntityCert)や TLV 群(AuthCert, PrefixPolicyCert)への署名である。

⑵ IP アドレス証明書システム

IP アドレス証明書システムは、JPNIC にて管理／運用され、その主な機能は

AS 運用者の認証処理、AS 運用者からの証明書もしくは TLV 群への署名要求を受け付け、IP アドレス認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリシステムへ配布することも考えられる。

⑶ AS 内証明書システム

AS 内証明書システムは、各 AS 運用者により管理／運用され、その主な機能は AS 番号等を含む CSR(EntityCert)や自身が再割り振り／割り当てを行った IP アドレスブロック情報を含む TLV 群(AuthCert, PrefixPolicyCert, ASPolicyCert)の作成と下位組織からの署名申請を受け、AS 内認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリ・システムへ配布することも考えられる。

⑷ AS 内認証局

AS 内認証局は、各 AS 運用者により管理／運営され、その機能は AS 番号等の情報を含む CSR (EntityCert)や TLV 群(AuthCert, PrefixPolicyCert)への署名である。

9.2.2.3. soBGP 初期設定概要

利用を開始する際に必要なのは、基本となる最上位 EntityCert 証明書(RootEntityCert)を作成することである。RootEntityCert を作成するのに適当と思われるのは、RIR 等の権威ある機関で、ここでは JPNIC が RootEntityCert を作成し運用すると仮定し、第 3 認証局としては JPNIC 認証局／JPNIC IP アドレス認証局を利用する。

新たに RootEntityCert を作成するに当たり、JPNIC は RootEntityCert で利用する PublicKey/PrivateKey のペアを作成し[RFC3280]に準拠した CSR を作成、AS 番号は[RFC3779]に準拠して拡張領域に定義する。CSR には新たに作成した PublicKey を含め JPNIC IP アドレス認証局の PrivateKey で署名し、証明書(RootEntityCert)として発行し、一般公開する。

AS 運用者は公開された RootEntityCert を入手し、JPNIC IP アドレス認証局が発行している CA 証明書にて RootEntityCert が改竄されていないか署名の検証を行う。問題無ければ RootEntityCert 内の SubjectAltName、シリアル番号、AS 番号、PublicKey をルータへ設定する。

これで、soBGP を利用するための準備が整ったことになる。

9.2.2.4. 自 AS で利用する EntityCert 作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後 EntityCert CSR を作成し IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。受け取った IP アドレス証明書システムは、レジストリシステム等を利用して CSR の内容を確認、問題無ければ IP アドレス認証局へ CSR を転送し、IP アドレス認証局の PrivateKey にて署名された証明書が返信されるのを待つ。返信された証明書はそのまま申請者へ送信される。

証明書を受信した AS 内証明書システムは EntityCert をセキュリティ・メッセージにてルータへ広告する。この時、受信したルータは RootEntityCert を利用して送られてきた EntityCert の署名を確認問題が無ければ SubjectAltName、シリアル番号、AS 番号、PublicKey を自身のテーブルに登録する。

この時点でルータ内の EntityCert テーブルには、RootEntityCert と自身の EntityCert の 2 つが登録されていることになる。

対となる PrivateKey は AS 内認証局にて管理し、AS 内証明書システムの要求にしたがい必要な署名を行ために利用する。

EntityCert 作成手順概要を図 9-43 に示す。

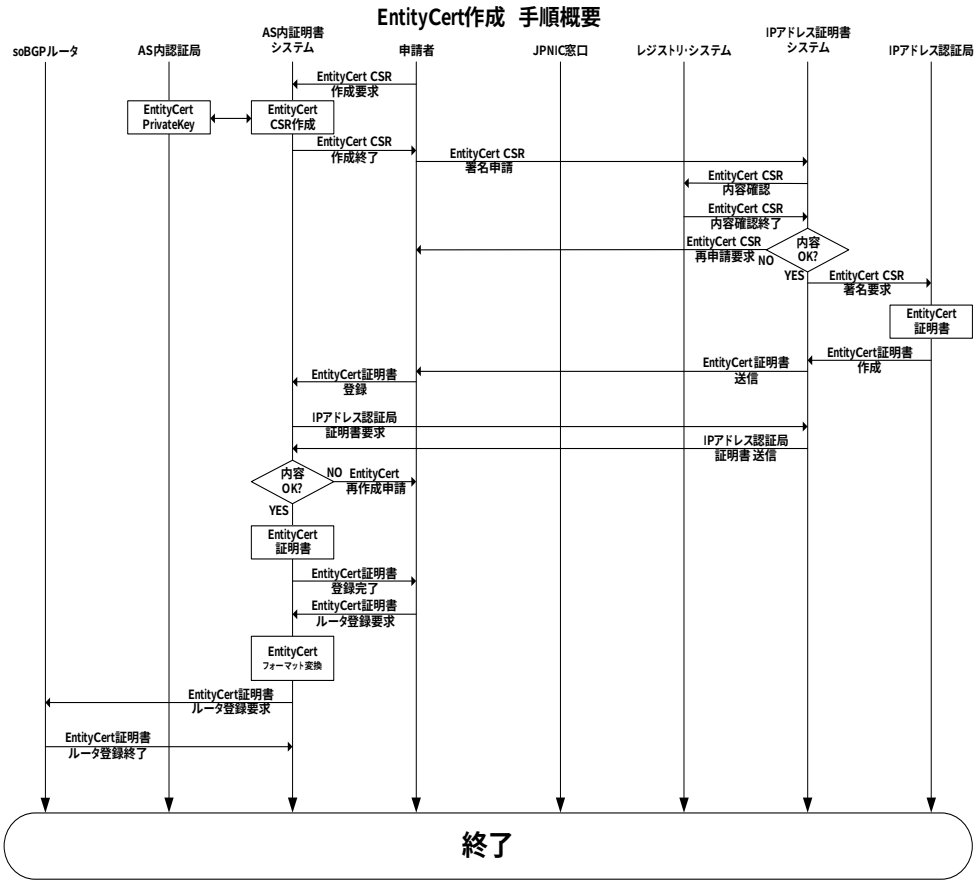


図 9-43　EntityCert 作成手順概要

9.2.2.5. 自 AS 用の PrefixPolicyCert 作成概要

AS 内証明システムに JPNIC から割振りを受けた IP アドレスブロックをデータに持つ AuthCert TLV を作成するように指示をだす。作成された TLV を IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。IP アドレス証明書システムは TLV の内容をレジストリシステム等で確認を行い問題が無ければ、IP アドレス認証局に対して TLV を送信し、受け取った認証局は署名し、IP アドレス証明書システムへ返送される。署名つき TLV 受け取った IP アドレス証明書システムは、AS 内証明システムへ返送する。署名つき TLV を受け取った AS 内証明システムは署名を確認し、問題が無ければ次に PrefixPolicyCert TLV を作成し再度 AuthCert と同様なプロセスをたどり署名つき PrefixPolicyCert TLV をセキュリティ・メッセージにてルータへ広告する。

受け取ったルータは TLV 内の署名フィールドにある署名した EntityCert もしくは

RootEntityCert にて検証を行い問題が無ければ、AuthCert を取り出し AuthCert の署名を確認し問題が無ければ、PrefixPolicy テーブルに TLV 内の情報を追加する。

AuthCert(AC)TLV & PrefixPolicyCert(PP)TLV 作成手順概要を図 9-44 に示す。

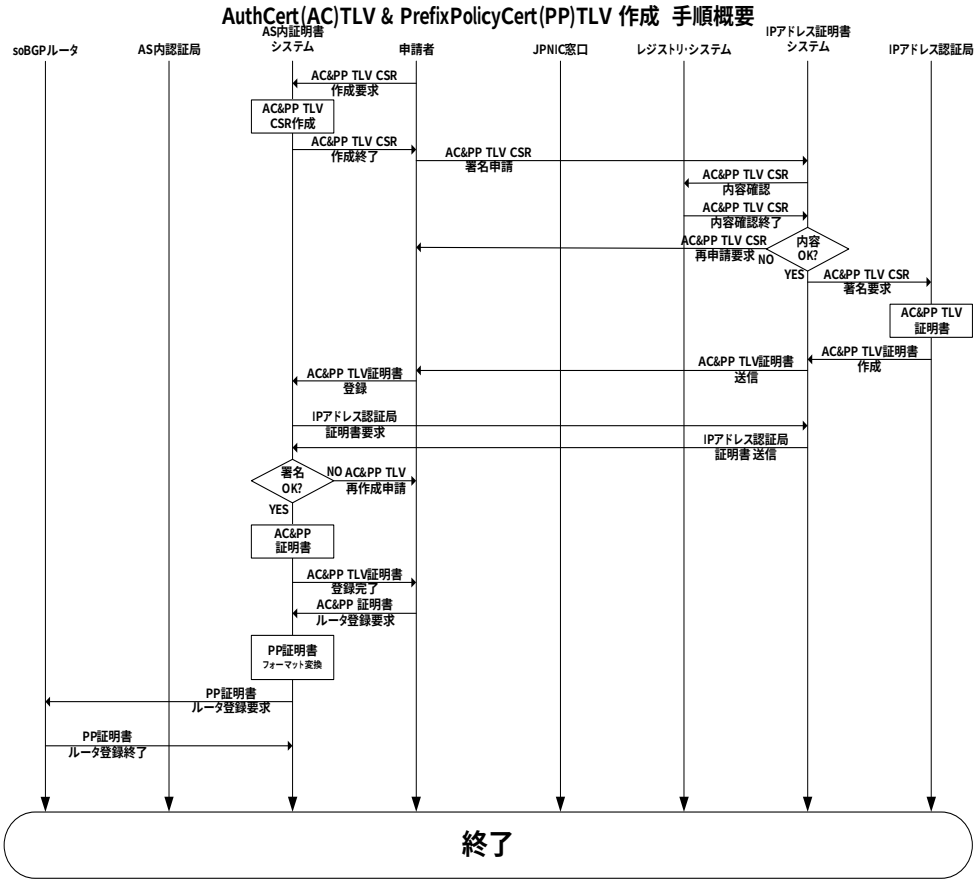


図 9-44　AuthCert(AC)TLV & PrefixPolicyCert(PP)TLV 作成手順概要

9.2.2.6. 自 AS 用の ASPolicyCert 作成概要

AS 内証明システムに ASPolicyCert TLV 作成の指示を出す。作成された TLV を自 AS 認証局へ送信し、認証局で署名後 AS 内証明システムに返信する。受け取った AS 内証明システムは署名を検証後、問題が無ければセキュリティ・メッセージを利用してルータへ ASPolicyCert を広告する。

受け取ったルータは EntityCert で署名を検証し問題が無ければ ASPolicy テーブルへ TLV 内の情報を追加する。

AS policy(AP)TLV 作成手順概要を図 9-45 に示す。

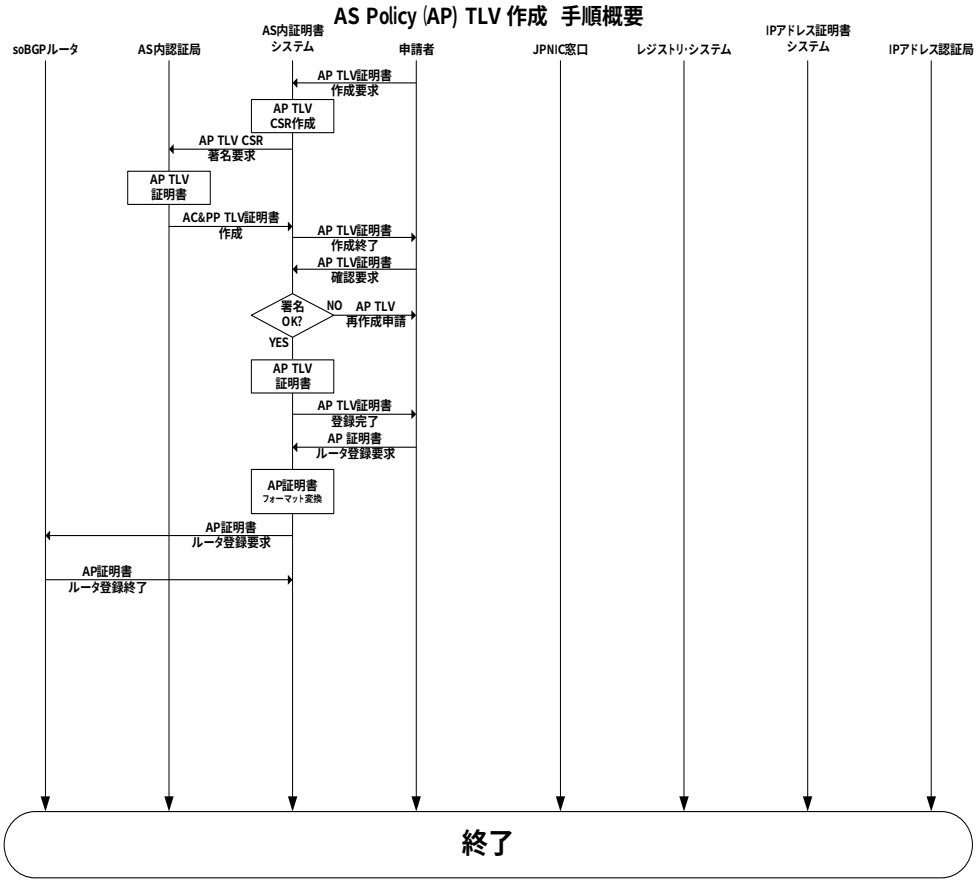


図 9-45　AS policy(AP)TLV 作成手順概要

この時点でルータには、RootEntityCert、EntityCert、PrefixPolicyCert、ASPolicyCert の情報が追加されている。この状態で BGP Update で送られてきた経路情報を Checkpoint で確認可能な状態になったことになる。

9.2.2.7. EntityCert の破棄について

署名検証後は、必ず CRL の検証を行う。EntityCert の破棄については EntityCert 内の URL を参照し最新の CRL を取得後行われ、破棄が確認された EntityCert に関してはテーブルから削除される。

9.2.2.8. PrefixPolicy＆AuthCert の破棄について

特定の PrefixPolicy や AuthCert の破棄を行う場合には ASPolicyCert 内に定義される各々の Validity List を確認して破棄マークがとなっている物に関して PrefixPolicy テーブルから削除が行われる。

9.2.3. その他

すでに記述したが、soBGP の TLV のフォーマットには URL が入るフィールドが有る。これは外部の証明書リポジトリをアクセスするために利用されるが、現時点では仕様が明確になっていないので今回は記述しない。

以上で連携システムの概略に関しての説明を終える。次節では、soBGP とは別なアプローチで経路情報の保護を行う仕組みを提供する S-BGP に関して述べる。

9.3. S-BGP の概要とモデル

本節では、経路交換システムを保護するため提案である S-BGP について、その概要と JPNIC で運用が考えられている IP アドレス証明書システムと JPIRR システムとの連携モデルについて述べる。

9.3.1. S-BGP 概要

S-BGP の目的は不正経路情報の発見、除去を自動化する事にある。実現方法としては、新たに定義する BGP Path Attribute を利用して RA 証明書(後述)を組織間で交換し、受信した証明書を検証することにより経路情報の真偽を確認することが可能となり、偽情報を除去する事が実現する。証明書の配布→受信→署名検証→証明書の登録／偽情報の排除までを S-BGP の枠組みで自動化する。

S-BGP で問題なのは、証明書情報を BGP とは別な仕組みで交換され、その交換方法には時間がかかることである、つまり新たに交換したい IP アドレスブロックに関して様々な前処理をし、証明書情報を全ての運用者に配り終わった後で広告を開始しないと新たに広告した IP アドレスブロックは破棄されてしまう可能性がある。

S-BGP では、BGP セッション開始前の接続先の確認と通信路の保護もその枠組みの中に含まれ、IPsec を利用するように定義されている。

S-BGP 概略を図 9-46 で示す。

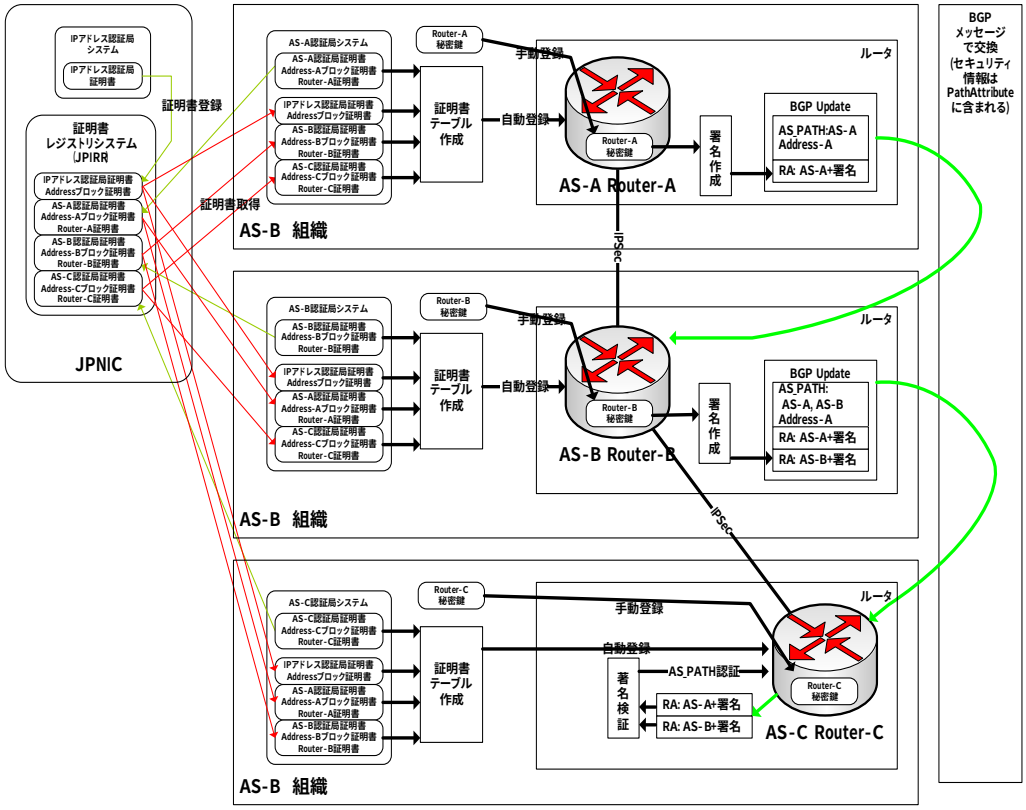


図 9-46　S-BGP 概略図

9.3.1.1. BGP Path Attribute について

BGP Update の最大長は、4096 バイトである。新たに定義する Path Attribute を利用するにしてもこの制限を超える事は出来ない。S-BGP の証明書情報はこの大きさに収まるサイズにしなくてはならない。

Path Attribute には、Route Attestations(後述)と Address Attestations(後述)を含んでいる。

BGP Path Attribue のエンコーディングを図 9-47 で示す。

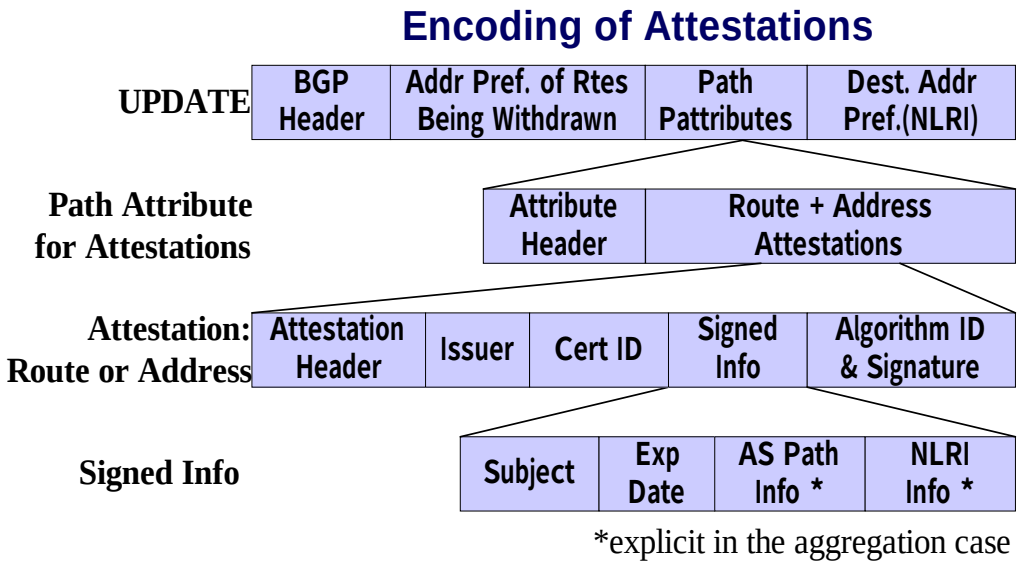


図 9-47　BGP Path Attribue のエンコーディング

実際の Address もしくは Route Attestation メッセージ･フォーマットを図 9-48 に示す。

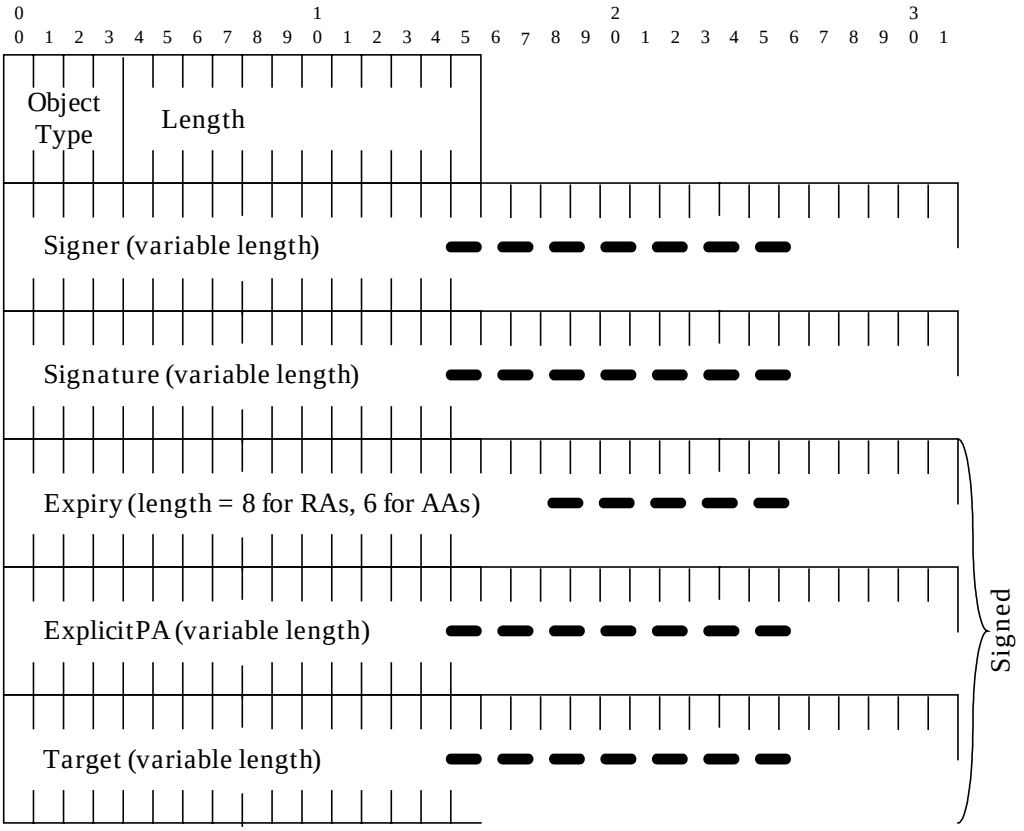


図 9-48　Address もしくは Route Attestation フォーマット

メッセージの基本は Part Code+Length であり、Code は 4 ビット、Length は 12 ビットとなり、合計 16 ビット(2 オクテット)となる。

Part Code と Length のフォーマットを図 9-49 に示す。

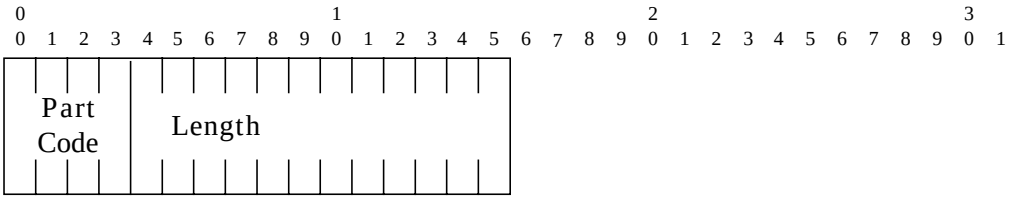


図 9-49　Part Code と Length のフォーマット

⑴ Object Type

証明したい情報の種別を示される。Code が 8 の時の種別は、「Route Attestation(RA)」、Code が9の時の種別は「Address Attestation(AA)」、Code が 14 の時は続くデータは「Extract File Authenticator」を示す。

Object Type のフォーマットを図 9-50 に示す。

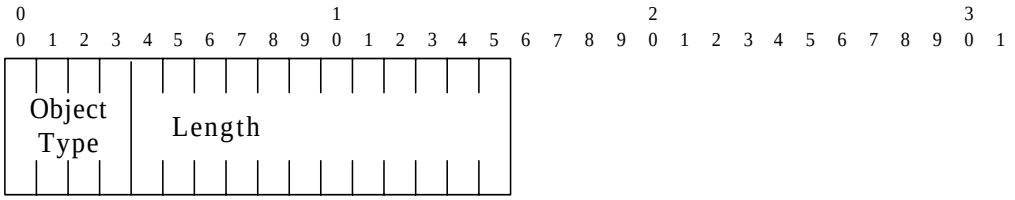


図 9-50　Object Type フォーマット

⑵ Signer

署名の際に利用したデータが示される。利用 Code は1、SignerLength には SignerData の長さ+2 オクテット、AFI は[IANA-AFI]にある値を指定する。SignerData には AFI に対応した情報を入れる。

Signer のフォーマットを図 9-51 に示す。

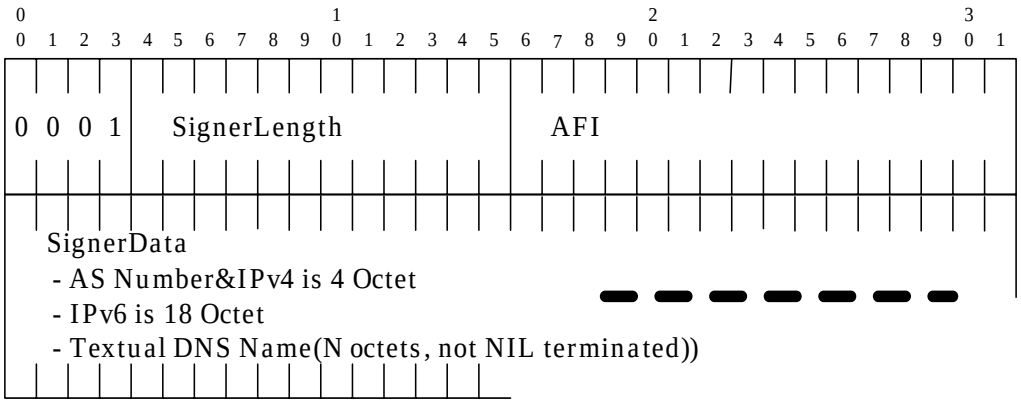


図 9-51　Signer のフォーマット

⑶ Signature

SignerData を基にした署名が示される。Code は 2、SignatureLength はデータの長さ、Signature Algorithm ID(SigAlgID)は署名を作成したときの方法が表され、[IANA-SAN]に有る値をとる。現在は、3(DSA/SHA1[RFC2536[7]、DSA、SHA-1])を使用する。KeyId は複数の認証局により SignerData が署名されたときに、どの認証局かを判別するために利用され、KeyId に対応する証明書内の項目は SubjectKeyIdentifier を利用する。CoverageLen は CoverageMask の長さを指定する。Object Type が AA の場合には CoverageLen は 0 になる。Object Type が RA の時 CoverageMask を利用し署名したときの PATH 属性の状態を記録する。

Signature は SigAlgID で指定された方法で作成された署名が入る。

Signature のフォーマットを図 9-52 に示す。

[7] DSA KEYs and SIGs in the Domain Name System (DNS) (RFC2536)
http://www.ietf.org/rfc/rfc2536.txt

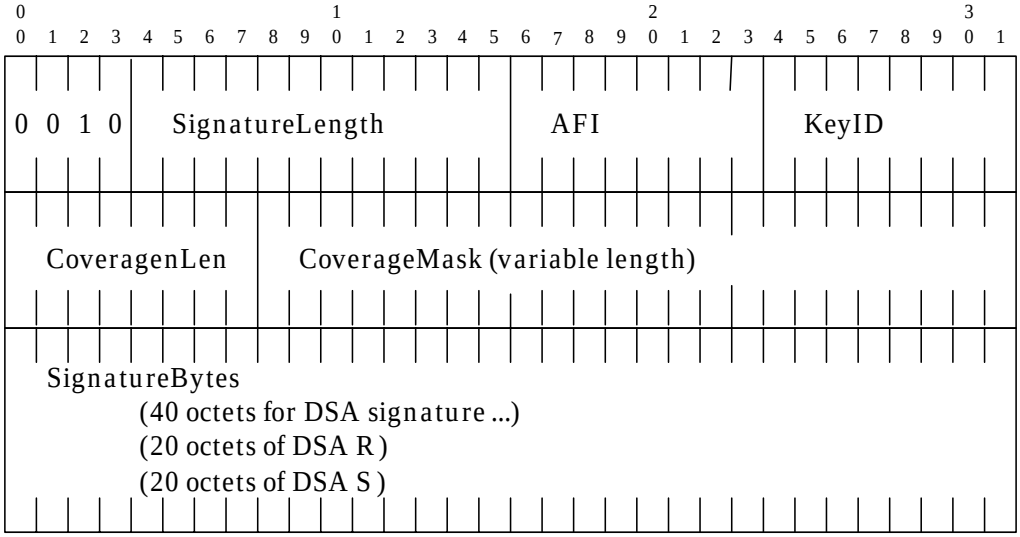
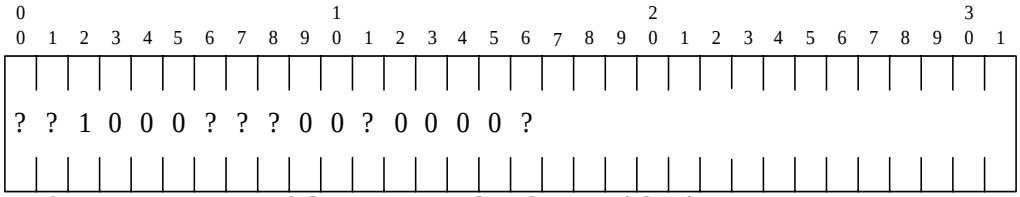


図 9-52　Signature のフォーマット



0: NLRI or MP_REACH_NLRI; 1: ORIGIN; 2: AS PATH;
6: ATOMIC AGGREGATE; 7: AGGREGATOR; 8: COMMUNITIES
11: DPA; 16: EXTENDED COMMUNITY; ... (others to be defined)

図 9-53　CoverageMask フォーマット

⑷ Expiry

証明書の有効期限が示される。Code は 3、ExpiryLength は、データの長さを表し Object Type が AA の時は 4、RA の時は 6 である。Year には西暦を、Month には月を Day には日を入れる。RA の時には A ビットと RASC がさらに必要になる。A ビットは Route の集約が行われた事を表し、RASC は集約が行われた個数を示す。

Expiry のフォーマットを図 9-54 に示す。

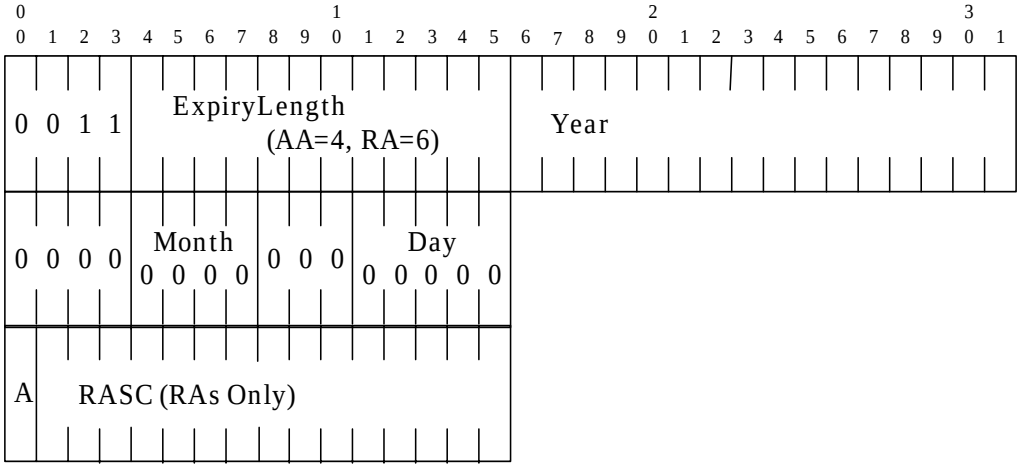


図 9-54　Expiry フォーマット

⑸ ExplicitPA

AS 組織では、複数の下位組織からの IP アドレスブロックを集約し一つの大きい IP アドレスブロックと新たな Path Attribute を広告するケースがある。集約以前の Path Attribute を保存する際に利用される。Code は 4、ExplicitPALength はデータの長さを表す。

ExplicitPA のフォーマットを図 9-55 に示す。

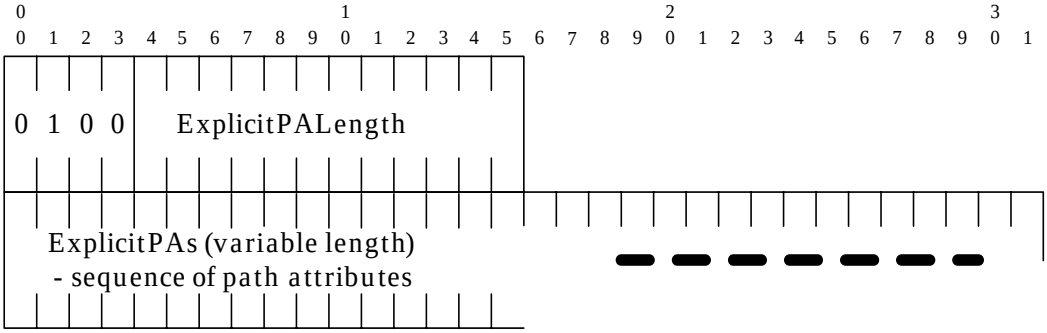


図 9-55　ExplicitPA のフォーマット

IP アドレス Prefix は、対照となる IP アドレスブロックが表される。AddressFamilyIndicator は [IANA-AFI] を利用し、SAFI へは [IANA-SAFI][RFC2858]を利用する。もし、RA 用であれば MaxPrefixLen は 0 がセットされる。AA 用であるときには受信した IP アドレスブロックに関して受け入れ可能な Prefix の最大長を設定する。もし、この Prefix 最大長を超えた IP アドレスブロックを受信した際には、その IP アドレスブロックは破棄される。

Prefix Encoding のフォーマットを図 9-56 で示す。

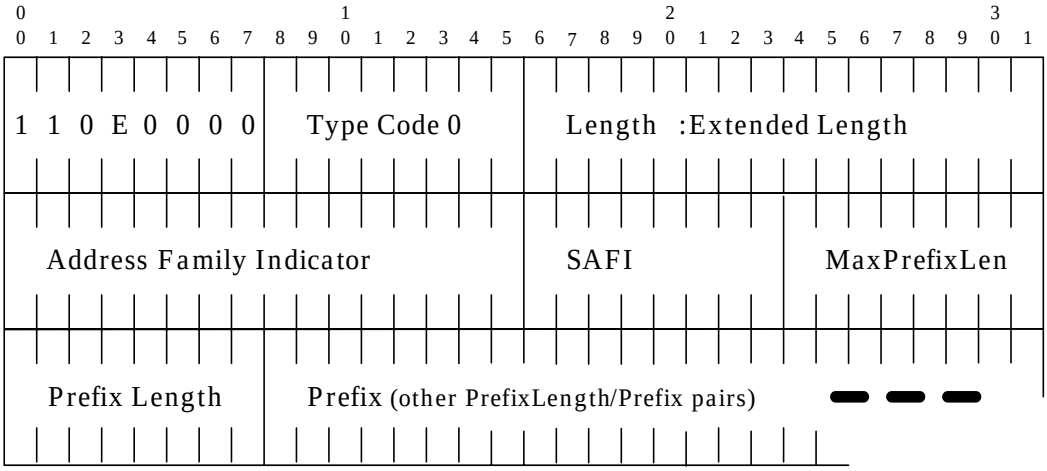


図 9-56　Prefix Encoding のフォーマット

(1) Target

メッセージが RA の時には、AS_PATH に追加した AS 番号を示し、AA の時には IP アドレスブロックの Origin AS を示している。Code は 5、TargetLength にはデータの長さ、AFI は AS 番号を示す 18 ([IANA-AFI]を利用) を指定する。その後一つ以上の AS 番号が続く。

Target Part のフォーマットを図 9-57 に示す。

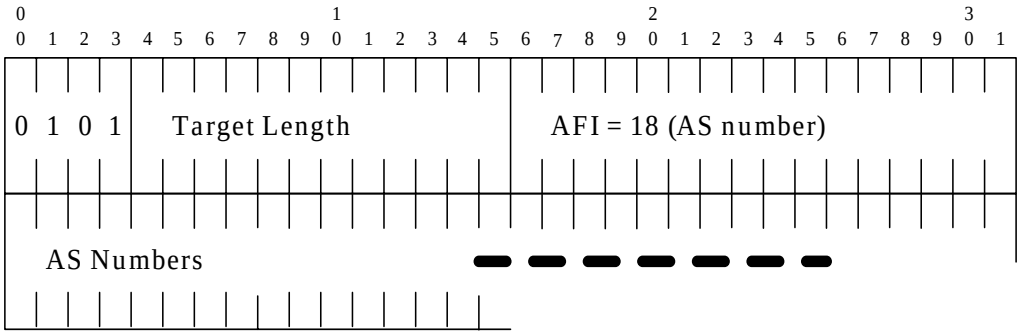


図 9-57　Target Part のフォーマット

9.3.1.2. S-BGP の情報信頼モデル

S-BGP は、公開鍵基盤(PKI)の枠組みを用いて、利用する証明書の信頼性を確保する。実際の確認方法に関しては RFC3280 に従い、証明書の参照先には証明書レジストリ(後述)を利用する。

S-BGP は、IANA 認証局の Root 証明書を全ての AS 運用組織が信用することで成り立つ。また、各組織の認証局のセキュリティ運用ポリシは IANA 認証局と同等もしくは、より厳しいものでなくてはならない。セキュリティポリシが IANA 認証局のものより下回る場合秘密鍵漏洩等の事故による重大な事故が起こる可能性が増大する。

9.3.1.3. S-BGP で利用する証明書

S-BGP で利用される証明書は、「運用組織の CA 証明書」、「RouterID-CA 証明書」、「Address Attestations」そして「Route Attestation」の 4 種類ある。

⑴ Address Attestations に関して

Address Attestations は、Origin AS と IP アドレスブロックを示し、自組織で作成する。

Address Attestations を作成するには、[RFC3280]を利用して証明書基本フォーマットを作成、[RFC3779]を利用して「AS 番号」と「IP アドレスブロック」を拡張領域へ書き込む。証明書は 、[IANA-SAN[8]]にある 3 番(SHA-1/DSA)を使用し、運用組織の CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑵ Route Attestation に関して

Route Attestation は自組織が AS_PATH に自 AS を追加したことを示し、自組織で作成する。

Route Attestations を作成するには、BGP Path Attribute の Object Type=3 に沿ってデータを構築し[IANA-SAN]にある 3 番(SHA-1/DSA)を使用し機器用の RouterID-CA の PrivateKey を利用して署名を作成し「Signature」フィールドへ埋め込む。出来たデータを Path Attribute に追加して BGP Update を再構築し Next Hop AS へ送信する。

各 AS 単位で同様な動作を行い、AS_PATH に AS を追加すると共に RA を追加する。最終的にあて先 AS 番号を持つ経路交換機器が受け取った時に RA の署名を順に検証することで AS_PATH が正しい事を証明出来る。

受信した Origin AS 番号と IP アドレス・プリフィクスに関しては AA を用いて検証する事で正しい事を証明する。

この 2 つの検証結果が良好な場合に限り経路情報は改竄されていないといえる。

8 SIG (0) ALGORITHM NUMBERS
http://www.iana.org/assignments/sig-alg-numbers

⑶ RouterID-CA 証明書に関して

RouterID-CA 証明書は経路制御機器で署名した RA 証明書を検証するために利用し、AS_PATH に AS 番号を追加する経路制御機器で作成する。この証明書は単一 AS にひとつとは限らない、複数の経路制御機器が AS_PATH へ AS 番号を追加する可能性がある時には複数の RouterID-CA 証明書を作成し、どの機器で AS 番号を AS_PATH へ追加したかを検証可能にすることが必要である。

RouterID-CA 証明書を作成するには、[RFC3280]を利用して証明書基本フォーマットを作成、[RFC3779]を利用して「AS 番号」を拡張領域へ書き込む。証明書は [IANA-SAN] にある 3 番(SHA-1/DSA)を使用し、運用組織の CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑷ 運用組織のＣA証明書に関して

運用組織の CA 証明書は自組織が AS を運用していることを示し、自組織で CSR を作成する。

運用組織の CA 証明書を作成するには、RFC3280 を利用して証明書基本フォーマットを作成、RFC3779 を利用して「AS 番号」と「IP アドレスブロック」を拡張領域へ書き込む。証明書は [IANA-SAN]にある 3 番(SHA-1/DSA)を使用し、上位の割り振り／割り当て組織 CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑸ 各証明書の関係図

各証明書の関係を図 9-58 に示す。

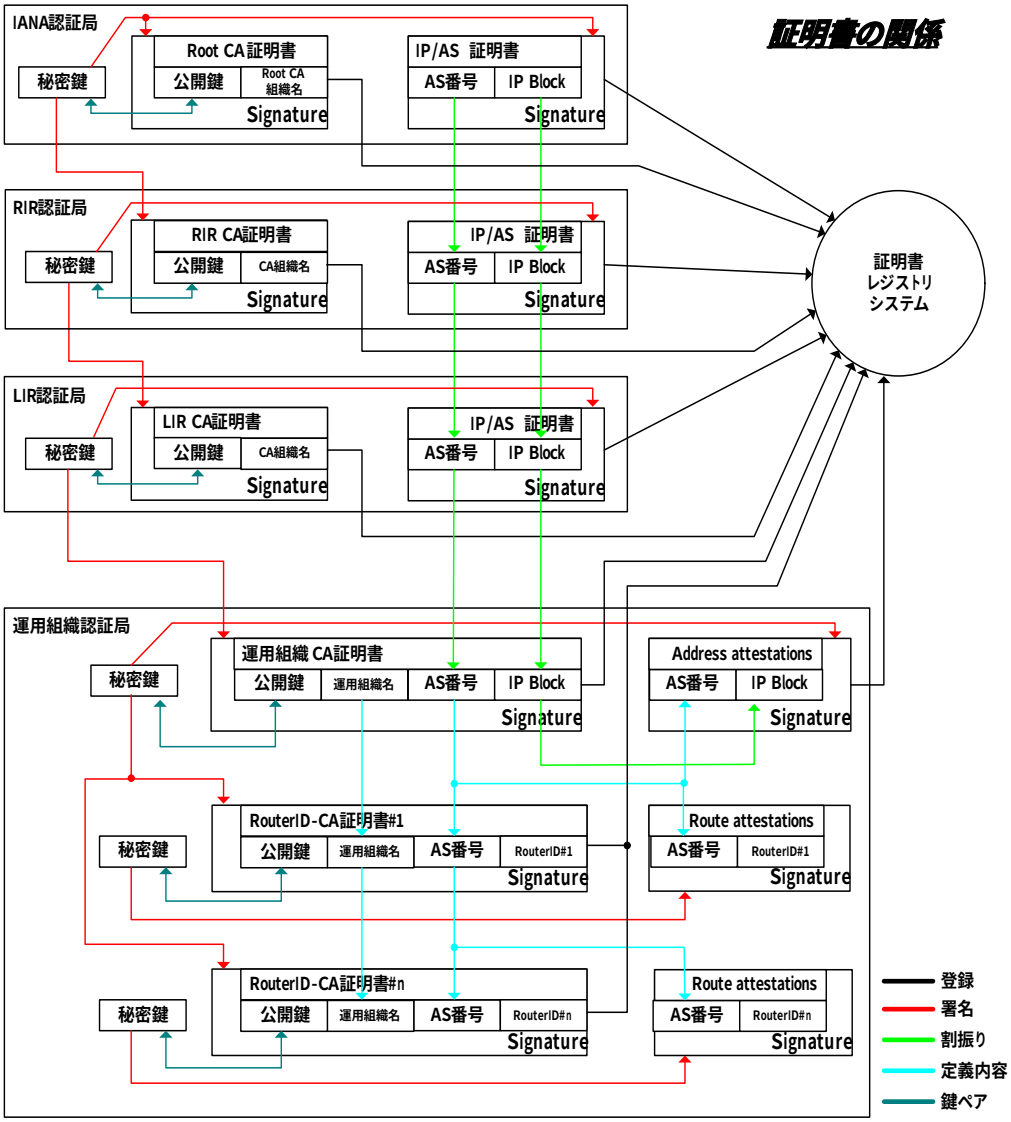


図 9-58 各証明書の関係

9.3.1.4. 署名の確認

各署名の確認は、「証明書の関係」図の Signature の矢印を逆向きにたどり、最終的には IANA 認証局の CA 証明書にたどり着き終わる。

9.3.1.5. S-BGP 動作の概略

S-BGP の動作概要を図 9-59 に示す。

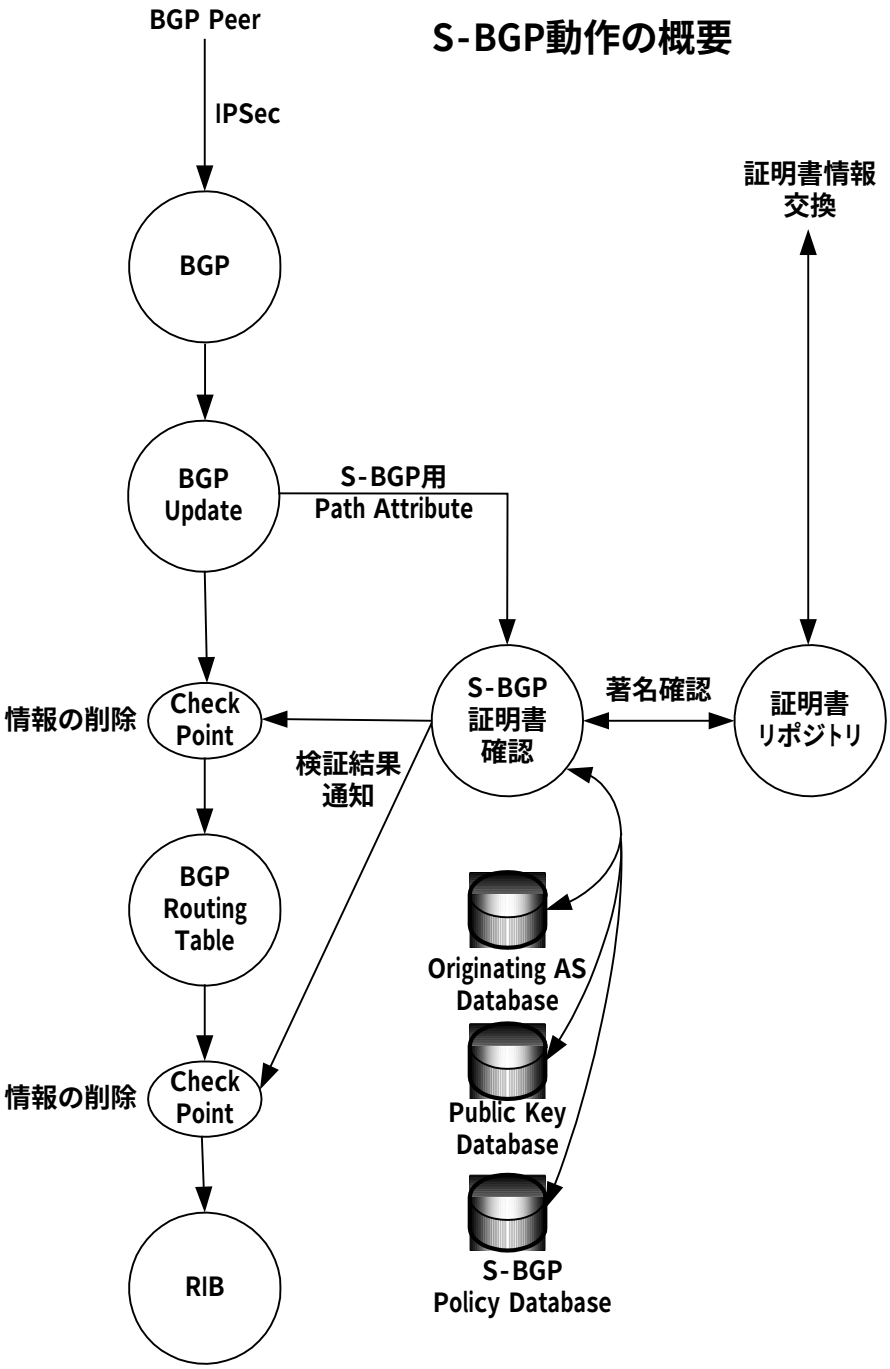


図 9-59　S-BGP の動作概要

S-BGP システムでは、初めに自組織の証明書情報と証明書破棄ﾘｽﾄ(CRL)の公開と他組織の証明書情報と CRL を取得し、取得した証明書情報から 3 種類の Database を作成する。一つ目は、「Originating AS Database」、この Database は「Address Attestations」証明書を検証後、証明書内から Origin AS 番号と IP アドレス Prefix を取り出して作成する。二つ目は「Public Key Database」、この Database は様々な証明書から作成され、証明書検証後の証明書内に有る AS 番号もしくは運用組織と PublicKey を取り出して作成する。三つ目は、「S-BGP Policy Database」、この Database は AS を運用する上でのﾎﾟﾘｼをまとめた物である。この 3 種類のデータを整形し経路交換機器へ設定する。証明書情報に関する処理が終了した後、S-BGP で利用する通信路の確立処理を行う。

経路交換機器間で IPsec-ESP [RFC2406[9]]にて接続先の認証した後暗号化通信を開始する。

BGP セッションが確立し、経路交換が開始されると、「Route Attestation」を含んだ BGP Update を受け取とった経路交換機器は自身の AS 番号を AS_PATH へ追加すると共に RA を Path Attribute へ追加して次の AS へ転送する。宛先となっている AS が BGP Update を受け取ると全ての RA 情報を検証し問題なければ、ルーティングテーブルへ登録する。

Origin AS と IP アドレス Prefix の確認は BGP Update で受け取った Origin AS と IP アドレス Prefix を「Address Attestations」内にある情報と比較し同じであれば経路情報は正常であることを表す。

9.3.2. IP アドレス証明書システムと JPIRR の連携モデル

本節では、JPNIC で現在運用されている IP アドレス証明書システムと JPIRR と S-BGP の連携について述べる。

IP アドレス証明書システムは、JPNIC が IP アドレスブロックや AS 番号をサービス･プロバイダへ割り振りを行う際に自動的に証明書を作成するシステムの事である。

[9] IP Encapsulating Security Payload (ESP) (RFC2406)
http://www.ietf.org/rfc/rfc2536.txt

連携モデルを作る前に証明書に署名する際に利用される PrivateKey の保護について述べておく必要がある。S-BGP の利用をするということは、すべての AS 運用者が同じセキュリティレベルにあることが要求される。これは AS 運用者が PrivateKey を利用した署名活動を行うからである。PrivateKey が一つでも漏洩しそのまま放置されると情報を詐称する事が可能となり S-BGP を利用する意味がなくなる。S-BGP システム全体を保護するためにも PrivateKey を保護するための統一ポリシを作成し運用者全体が統一した PrivateKey の運用を行うことが必要である。

ただし、各組織で PrivateKey の適切な運用を行うためには、設備投資、人的リソースの増大等いろいろな面で各組織に負担がかかる。つまりは、S-BGP 導入に関して後ろ向きの要素となる。各組織の運用,設備投資を最小限に抑えた形で PrivateKey 運用ポリシとシステムを構築することが重要である。

9.3.2.1. S-BGP における JPNIC の役割

図 9-58「証明書の関係」にて主な役割は定義されている。「IP アドレス／AS 番号割振り組織」が JPNIC に当たるが、自身が割り振った情報に対しての署名処理と認証局の運用／管理ポリシの作成が主な役割となる。

9.3.2.2. 連携システム概要

ここでは、JPNIC で現行稼動している IP レジストリシステムと S-BGP で必要とされる証明書システムの連携をまとめる。

連携システムの目的は正確な情報（IP レジストリシステムに登録されている情報）を元に運用組織で利用する証明書を Secure な環境下で効率よく作成し経路制御システムや証明書レジストリ・システムへ提供する事を目的としている。

連携システムは、IP アドレス認証局、IP アドレス証明書システム、AS 内証明書システム、AS 内認証局が S-BGP に関わる証明者、AA や RA を作成するために必要となる。また、JPIRR へ情報を提供する事により JPIRR に登録されている情報の検証を行うことも考えられる。本調査では認証局としてのポリシを述べる事はしないが、本連携システムでは全ての認証局運営組織は同じセキュリティレベルが定義されているポリシを共通で利用し認証局

運用する事がセキュリティ上重要である。理由は署名されたデータは Routing システムや証明書レジストリを介して全ての組織に広告されるためである。これは、システムで署名つき TLV を交換している組織は全て同一セキュリティドメインであるといえる。

連携システム概略を図 9-60 に示す。

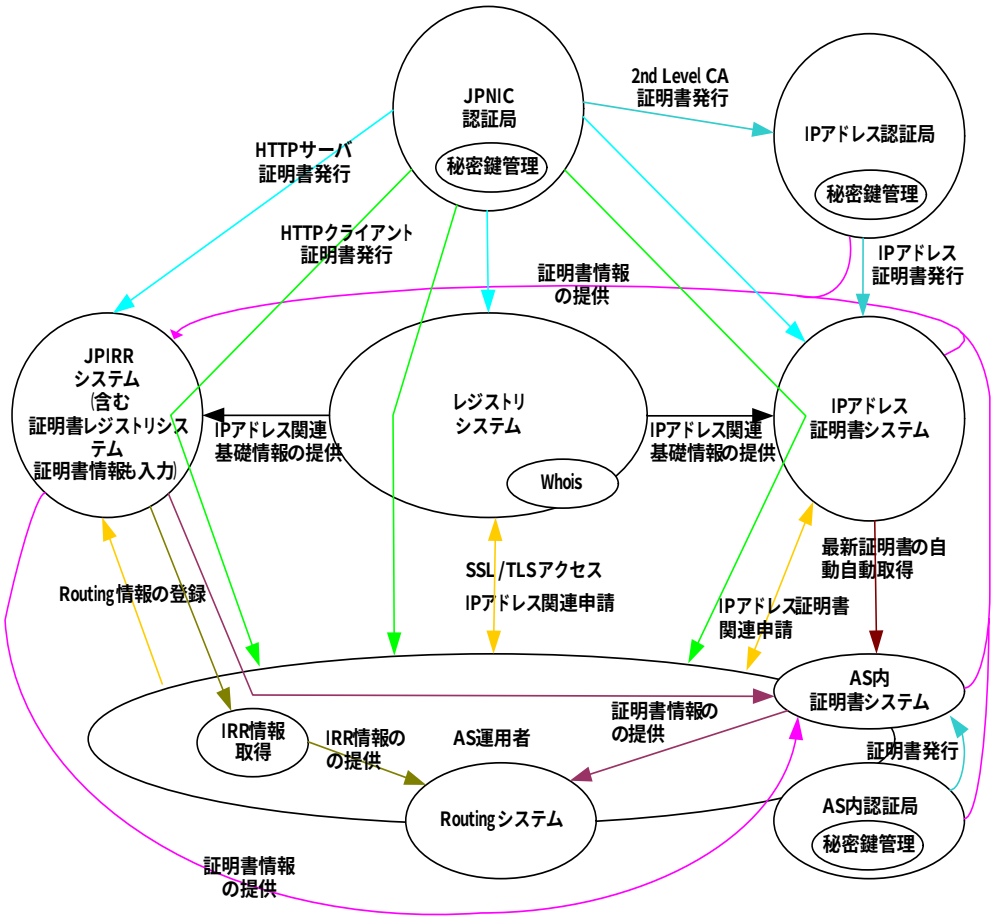


図 9-60　連携システム概略図

(1) 証明書レジストリ・システム

証明書レジストリ・システムは、S-BGP で利用する必要情報と公開鍵を公開するためのシステムである。公開する証明書の種類は、運用組織の CA 証明書, RouterID-CA#n 証明書, Address Attestations 等があげられる。

⑵ IP アドレス認証局

IP アドレス認証局は、JPNIC にて管理／運用され、その機能は JPNIC が割り振りを行った IP アドレスブロックや AS 番号等の情報を含む CSR (運用組織の CA 用)への署名である。

⑶ IP アドレス証明書システム

IP アドレス証明書システムは、JPNIC にて管理／運用され、その主な機能は AS 運用者の認証処理、AS 運用者からの証明書への署名要求を受け付け、IP アドレス認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリ・システムへ配布することも考えられる。

⑷ AS 内証明システム

AS 内証明書システムは、各 AS 運用者により管理／運用され、その主な機能は AS 番号等を含む CSR や自身が再割り振りを行った IP アドレスブロック情報を含む CSR の作成と下位組織からの署名申請を受け、AS 内認証局への橋渡しを行い、署名された物を申請組織へ返送する。また作成された署名物は必要であれば JPIRR 等の他レジストリ・システムへ配布することも考えられる。

⑸ AS 内認証局

AS 内認証局は各 AS 運用者により管理／運営され、その機能は AS 番号等の情報を含む CSR や署名の必要なデータへの署名である。

9.3.2.3. S-BGP 初期設定概要

利用を開始する際に必要なのは、自身の AS を証明する証明書(組織証明書)を作ることである。この証明書は IANA/RIR 等の権威ある機関で署名する。ここでは JPNIC が IANA/RIR の代わりとして署名を行うと仮定し、JPNIC 認証局／JPNIC IP アドレス認証局を利用する。

9.3.2.4. 自 AS で利用する組織証明書作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後、組織 CSR を作成し IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。受け取った IP アドレス証明書システムはレジストリシステム等を利用して CSR の内容を確認し、問題が無ければ IP アドレス認証局へ CSR を転送し、IP アドレス認証局の PrivateKey にて署名された証明書が返信されるのを待つ。返信された証明書は、そのまま申請者へ送信される。

証明書を受信した AS 内証明書システムは、組織証明書を検証後、証明書レジストリシステムへ登録すると共にルータ用のフォーマットに変更してルータへ設定する。

対となる PrivateKey は、AS 内認証局にて管理し、AS 内証明書システムの要求に従い必要な署名を行ために利用する。

組織証明書作成手順概要を図 9-61 に示す。

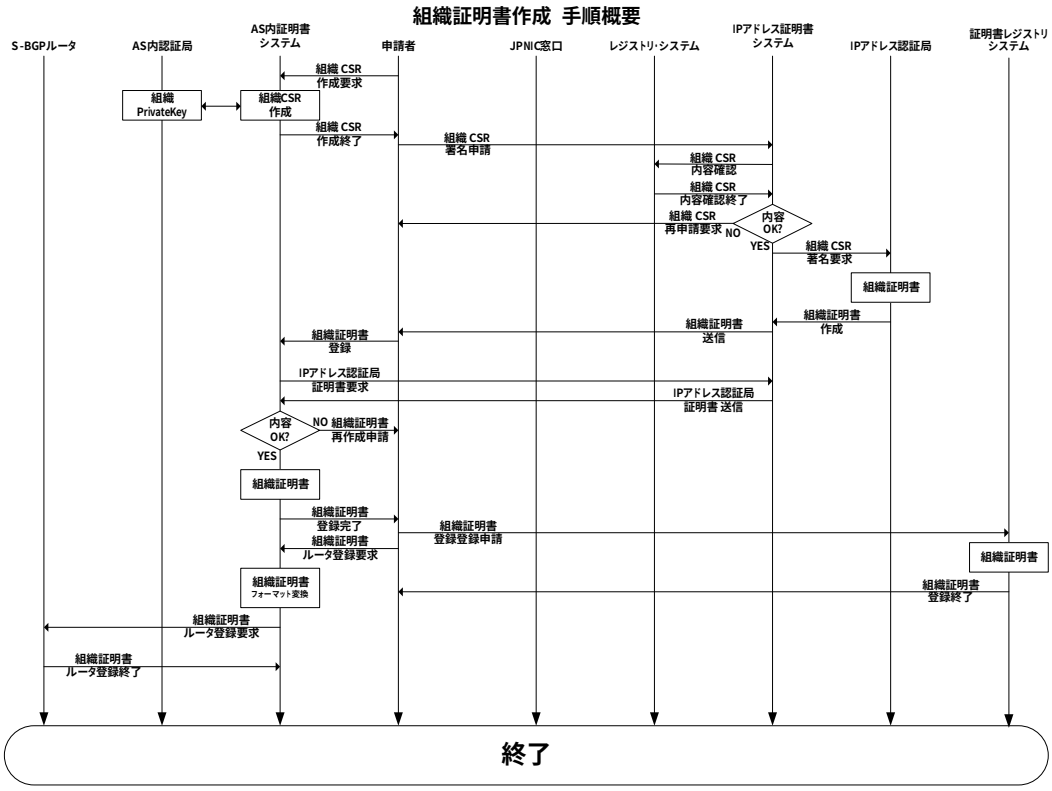


図 9-61　組織証明書作成手順概要

9.3.2.5. Address Attestations (AAs)証明書作成概要

AS内証明書システムにJPNICから割り振りを受けた、IPアドレスブロックをデータに持つAA CSRを作成するように指示を出す。また、AS内認証局に対して今作成したCSRを署名するように指示を出す。受け取った認証局は署名後、AA 証明書としてAS内証明書システムへ返送する。受け取ったAS内システムは著名を確認後問題なければ、証明書レジストリシステムへ登録すると共に、フォーマットをルータ用に変換後、ルータを設定する。

Address Attestations(AA)証明書作成手順概要を図 9-62 に示す

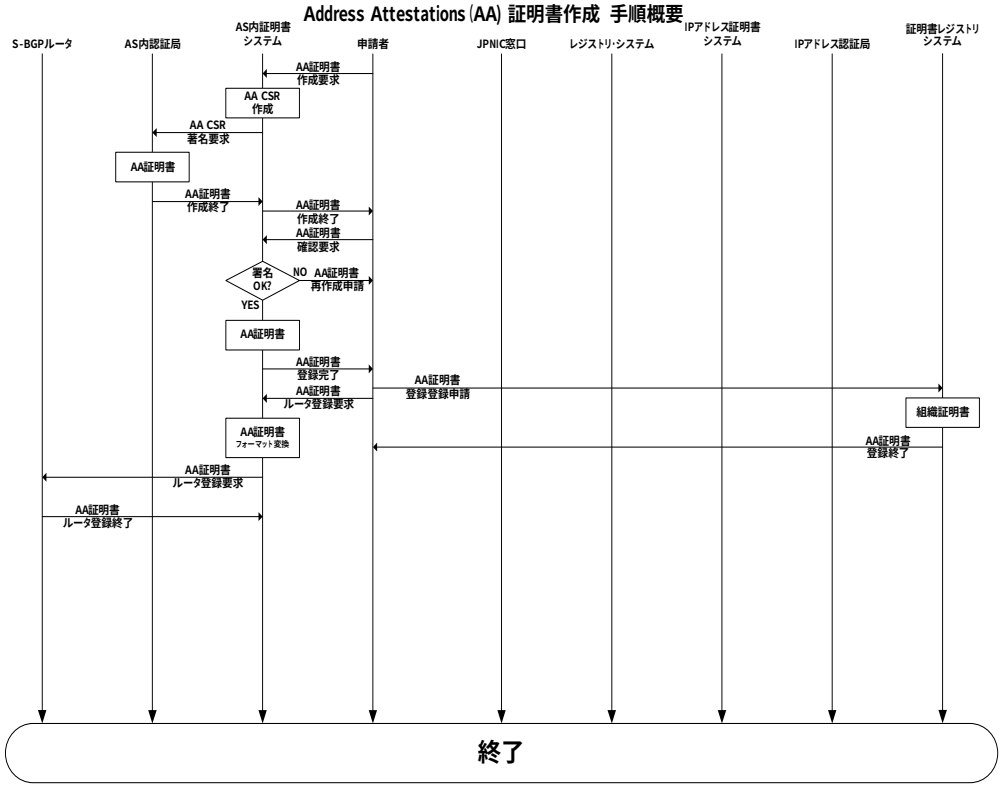


図 9-62　Address Attestations(AA)証明書作成手順概要

9.3.2.6. Route Attestations (RAs)証明書作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後、RA CSR を作成し AS 内証明書システムへ AS 内認証局の署名を申請する。受け取った AS 内認証局は CSR を自身の PrivateKey にて署名し AS 内証明書システムへ RA 証明書として返送する。AS 内証明書システムは返送されて来た RA 証明書の署名を確認し問題がなければ証明書レジストリへ登録する。

次に AS 内証明書システムは RA 秘密鍵をルータへ転送し、ルータ自身が RA を作成できるように設定する。

Route Attestations(RA)証明書作成手順概要を図 9-63 に示す。

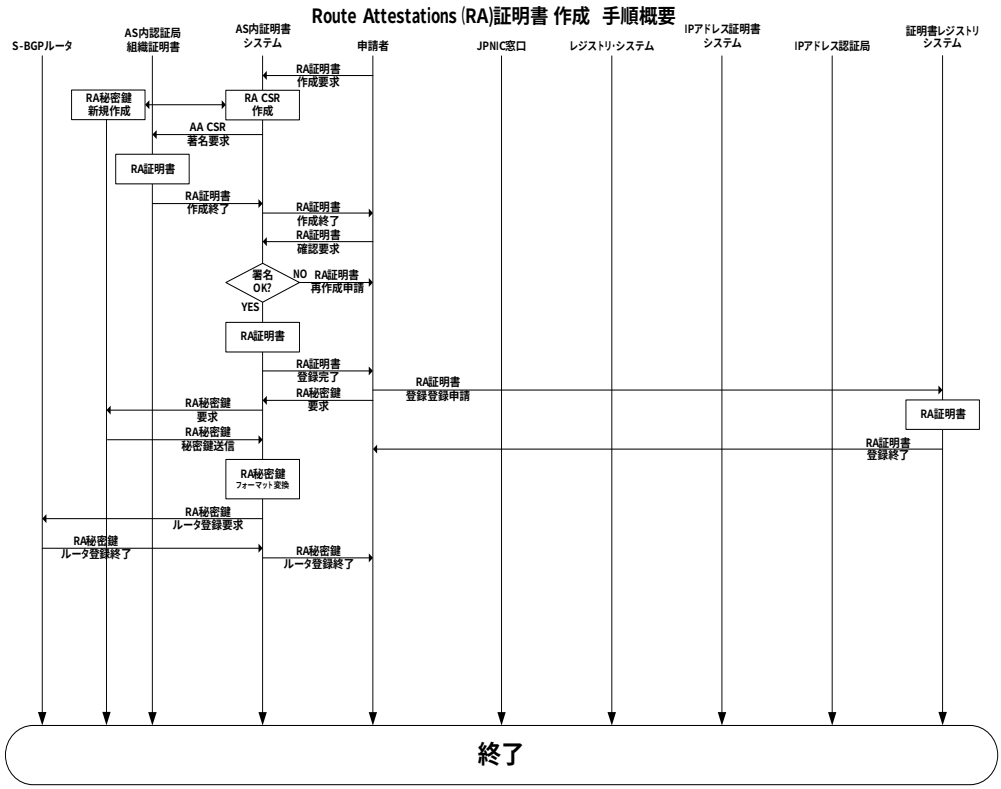


図 9-63　Route Attestations(RA)証明書作成手順概要

この時点でルータには、組織証明書テーブル、AA 証明書テーブル、RA 秘密鍵の情報が追加されたことになる。この状態で BGP Update で送られてきた経路情報が Checkpoint で確認可能な状態になったことになる。

9.3.2.7. 各種証明書の破棄について

署名検証後は必ず CRL の検証を行う。証明書の破棄については証明書内の URL を参照し最新の CRL を取得後行われるか、証明書レジストリ・システムから CRL を取得したものが利用される。破棄が確認された証明書に関してはテーブルから削除するように AS 内証明書システムがルータへ指示を出す。

以上で連携システムの概略に関しての説明を終える。

9.4. 考察とまとめ

本章では、インターネットの経路制御において経路情報を登録する登録機構であるインターネット・ルーティング・レジストリに着目し、経路制御の安全性と、インターネット・ルーティング・レジストリに登録される情報の正確性、信憑性、信頼性の向上について解説、検討、および考察を行った。

この調査の結果では、近年のインターネットに広告される経路数は増加の一途であり、減少する見込みはない。一方で、インターネットに経路を広告する方法は BGP-4 が開発された当初より劇的な変化はなく、開発当初は問題が無かったものでも、現時点のような広範囲にインターネットが普及した状態では、経路制御にセキュリティ的にいくつかの問題があることが明らかになった。

このような問題を解決するための手段としては、経路制御の運用上、経路フィルタをするなどが現時点では最良であるが、厳しい経路フィルタはそれ相応の運用の手間が必要であり、多少セキュリティ的には問題があっても運用上妥当な手間で実施できるレベルにセキュリティレベルと落として運用しているのが実情である。

そこで、本調査研究では、IP レジストリにおける IP アドレス証明書基盤として、「IP レジストリシステムと IRR システムの連携とその認証・承認の強化による IRR 登録情報の正確性・信憑性・信頼性の向上」というアプローチと「soBGP/S-BGP という提案されている新プロトコルの具体的な運用モデルの考察」について調査・検討・考察を行った。

この調査・検討・考察の結果、IP レジストリシステムと IRR システムの連携、および IP アドレス証明書を用いた認証システムを導入することにより、IRR に登録される情報の正確性・信憑性を向上させるのに有効であることが明らかとなった。

また、soBGP/S-BGP は、現時点では現状の運用に若干の問題はあるものの、プロトコルそのものの効果としては、インターネットに流れる経路情報を正しく保つのに効果があることがわかった。

しかし、ここで有効と明らかになったシステムは、いずれもインターネット全体で普及した段階で有効となるものである。つまり、日本国内のみの様な一部の地域、もしくは閉域で利

用しても、それらの領域のみの情報に対してのみ有効なのである。

現状の経路制御のセキュリティを考えると、何らかの対策が必要であることは明らかであり、これらの対策はインターネットに接続しているコミュニティ全体で実施していく必要がある。本調査では、インターネットの経路制御のセキュリティ向上に対する有効な手段を考察し検討しており、この調査報告書で記載されているような機構をインターネットレジストリで導入することの、早急に検討する必要があると考えられる。

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。

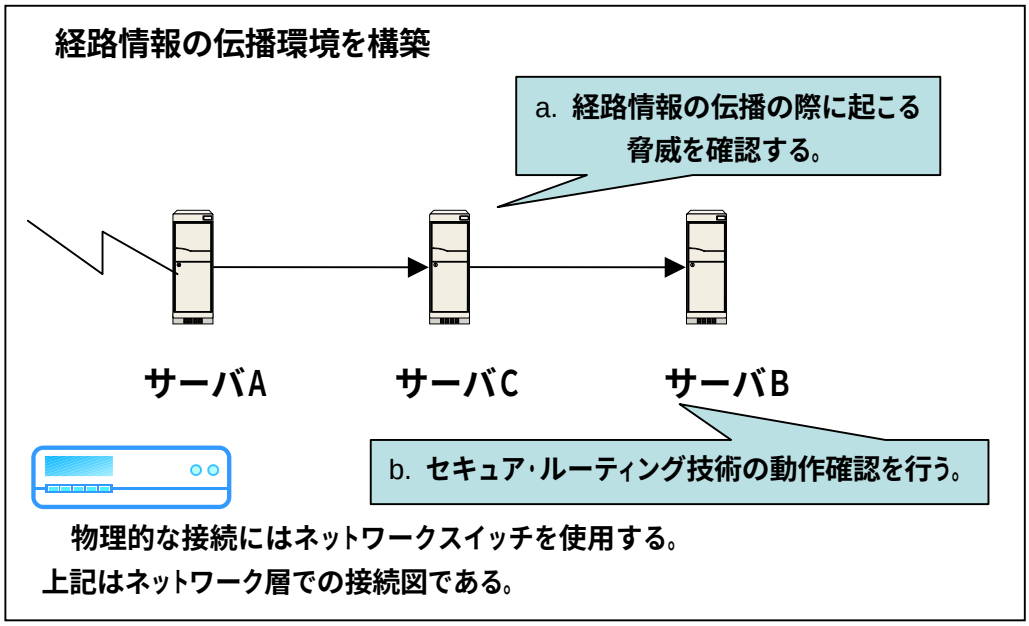


図 10-1 フェーズ１のネットワーク構成

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。

第 11 章　まとめ

内容

- 各章のまとめ

11. まとめ

本章では、本報告書の各章の内容をまとめる。

第 1 章「調査研究の背景と位置づけ」

本調査研究は 2004 年度までに行われた IP アドレス認証局の展開と、電子認証のノウハウとなるガイドライン策定の仕組み「電子認証フレームワーク」に関するものである。

調査研究の一環として、2004 年度までに構築した認証局を運用し、そのノウハウを電子認証フレームワークの中で利用していく。また IP アドレス認証の電子認証フレームワークにおける位置づけを明らかにすることも目指す。

第 2 章「電子認証フレームワークに関する調査研究について」

インターネットの普及と Web アプリケーションを使った身近なサービス提供によって、ID 盗用の問題が大きくなりつつある。

多くの金融機関や商用 Web サイトにおけるユーザ認証はパスワードが使われている。しかしその運用方法は提供者に任され、一定のノウハウが蓄積された状態ではない。PKI（Public-Key Infrastructure）のように電子証明書の仕組みを運用するには、PKI に共通するノウハウや、適用分野ごとに考えられるノウハウを蓄積し、利用していく必要がある。

本調査研究ではノウハウをガイドライン・ドキュメントとして策定し、蓄積している仕組みを「電子認証フレームワーク」と名づけ、その在り方について調査研究を行った。

第 3 章「IETF における電子認証とドキュメント策定プロセスの動向」

IETF（Internet Engineering Task Force）における、電子認証技術に関するプロトコル策定動向やプロトコル策定プロセスに関する動向を報告する。

IETF では、PKI の利用に関する BCP（Best Current Practice）と呼ばれるドキ

ュメントの必要性が指摘されている。これは PKI の技術をより適切に利用するために、技術そのものではなく利用方法に着目したドキュメントである。PKIX WG は PKI の技術自体に関するプロトコルの策定を目標としている為、BCP に関する情報集約や議論のできる場が少ない状況がある。

一方、IETF ではプロトコル策定プロセスを見直す動きがある。ドキュメント化のプロセスを見直し、既存のフローの効率化を図る活動とともに、プロセスの見直しの目的を明らかにし、策定されるドキュメントの質を維持する活動も始まっている。

また経路情報交換の安全性確保のために新たな WG、SIDR（Secure Inter-Domain Routing）が設立された。この WG は、インターネットにおける経路情報交換プロトコルで認証機能を実装している S-BGP や soBGP を中心に、安全な経路制御を図る仕組みの策定を目指すものである。

第 4 章「電子認証の運用に関するドキュメントの現状」

電子認証の運用に関する国内外のドキュメントについて基本調査を行った。特に共通する部分や電子認証の「保証レベル」に関するもので、認証の種別や確からしさに基づくレベル分けを示している。

日本国内においても日本 PKI フォーラムのポリシーWG において、基準となる「保証レベル」や利用方法に関する活動が行われている。

第 5 章「電子認証フレームワークの在り方」

本調査研究の一環として、PKI の専門的な知識を有しており、かつ IETF のドキュメント策定に明るい専門家によるチームを設立した。このチームではガイドライン・ドキュメントを策定する活動に関する要件について議論し、要件事項の集約を図ったものである。その結果、策定によって有用なガイドラインとなるいくつかの内容が明らかになった。その中には前節で述べた「保証レベル」が含まれている。また策定プロセスに関して、策定されたものに準拠しやすいような要件の抽出も行われた。

第 6 章「IP アドレス認証の展開に関する調査研究について」

電子認証フレームワークに関する調査研究と関連して、IP アドレス認証局を利用した認証の展開に関する調査研究を行った。IP アドレス認証局を使って実現できる電子認証は、自然人の認証と異なり、サーバやアドレスの割当先となる。これらの認証を電子認証フレームワークの中で一つの分野として位置づけ、具体的な展開を図る。

本調査研究では JPNIC の登録情報を利用して、インターネットにおける経路情報交換のプロトコルで電子認証を行う仕組みについて取り組む。

第 7 章「アドレス資源管理と経路情報の現状」

経路情報交換の仕組みの基本的な概念の解説を行う。IP アドレスの管理を行うインターネットレジストリを始め、BGP-4 やインターネットで広告されている経路情報の傾向について解説する。

第 8 章「経路制御におけるセキュリティの現状」

経路制御において交換されている情報は、必ずしも IP アドレスの割り振り情報と一貫性が保たれていない。そのため、経路ハイジャックなどの不正行為が可能である状況であり、その影響は大きい。構造上、ISP で提供しているインターネットの接続性を大規模な範囲で失わせるほどの影響が出る可能性がある。

第 9 章「経路情報交換における不正利用排除」

JPNIC の認証局を利用して、S-BGP 等の電子認証を実現するための仕組みを考察した。BGP における認証の考え方を踏まえた仕組みを紹介した。

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」

インターネットを使うネットワークアプリケーションの可用性を確保するためには、安全な経路制御を行うことが重要である。一方、既存の柔軟なネットワーク管理を維持することも必要である。前章で紹介した電子認証を運用することを考える際に必要となる検証事項をまとめた。また課題事項に関して取り組んだ、ヒアリングと実験環境の構築について述べる。

Appendix I「RFC3779 日本語訳」

S-BGP で利用される電子証明書の書式を規定した RFC3779 の日本語訳を掲載する。

Appendix 1

RFC3779 日本語訳

<Appendix 1 について >

- この資料は、IETF において策定された RFC3779　を日本語に翻訳したものです。
  - 内容の理解を図るために翻訳されたもので、内容確認には原文をご利用下さい。
  - 日本語訳は本調査研究の一環として作成されたものです。日本語訳に関するお問い合わせは著者に行なわないで下さい。

Network Working Group　　C. Lynn
Request for Comments: 3779　　S. Kent
Category: Standards Track　　K. Seo
BBN Technologies
June 2004

IP アドレスおよび AS 識別子のための X.509 の拡張

本文書の位置づけ

本文書はインターネットコミュニティのためのインターネット標準化過程プロトコルを定義し、改良のための議論と提案を求めている。本プロトコルの標準化の段階および状態については「Internet Official プロトコル Standard」(STD 1)の最新版を参照してほしい。本文書の配布は制限されない。

著作権表示

要約

本文書は、2 つの X.509 v3 証明書拡張を定義する。最初のものは IP アドレスブロックのリスト、またはプリフィックスを証明書のサブジェクトに結合するものである。2 番目のものは、自律システム識別子のリストを証明書のサブジェクトに結合するものである。これらの拡張は､拡張領域内に含まれる IP アドレスおよび自律システム識別子をサブジェクトが使用することを認証するために使用することができる。

目次

1. はじめに

本文書は、一連の IP アドレスおよび自律システム識別子の使用権の、IANA から地域インターネットレジストリ(RIR)を通じてインターネットサービスプロバイダ(ISP)およびユーザ組織への以上を認証する、2 つの X.509 v3 証明書拡張を定義する。最初のものは、IP アドレスブロック(しばしば IP アドレスプリフィックスと表される)を、証明書のサブジェクト(秘密鍵の保有者)に結合するものである。2 番目のものは、自律システム(AS)識別子のリストを証明書のサブジェクト(秘密鍵の保有者)に結合するものである。証明書の発行者は、一連の IP アドレスブロックおよび AS 識別子の管理権を証明書のサブジェクトに移譲する(「割り振る」)権威を持つエンティティ(たとえば IANA、地域インターネットレジ

ストリ、または ISP) である。これらの証明書は、一連の IP アドレスプリフィックスおよび AS 識別子の使用権を確認する、スケーラブルな手段を提供する。これらは、Secure BGP [S-BGP]などのルーティングプロトコルがルーティング情報の正当性や正確さを確認したり、インターネットルーティングレジストリが受信するデータを確認したりするために使用することができる。

セクション 2 および 3 は、この使用で定義され、従わなければならない(MUST)拡張領域のエンコーディングに関するいくつかの規則を指定する。これらのエンコーディング規則は、以下の目的で使用される。最初に、これらは拡張領域の値の固有のエンコーディングに帰着する。2 つの拡張領域のインスタンスは、オクテットごとに等しいかどうかを比較することができる。第 2 に、これらは、情報を最小サイズでエンコーディングすることができる。第 3 に、これらの規則によって、依存者が証明書パス検証を行うときに、ワンパスアルゴリズムを使うことができる。特に、依存者は複数の境界の場合(隣接、重複、または包含)を扱うために、情報をソートしたりサブセットチェックアルゴリズムの中に余分なコードを実装したりする必要がない。

1.1. 用語

読者は「インターネット X.509 公開鍵基盤 証明書と証明書失効リスト(CRL)のプロファイル」[RFC3280]、「インターネットプロトコル」[RFC791]、「インターネットプロトコルバージョン 6(IPv6)のアドレス体系」[RFC3513]、「インターネットレジストリにおける IP 割り振りのガイドライン」[RFC2050]、および関係する地域インターネットレジストリアドレス管理ポリシードキュメントに記載されている用語および概念を熟知しているものとみなされる。重要な用語には、以下のものが含まれる。

割り振り - リソースの管理権の、中間組織への移譲([RFC2050]参照)。

割り当て - リソースの管理権の、エンドユーザ組織への移譲管理権([RFC2050]参照)。

自律システム (AS) - 1 つの管理ポリシーで単独の技術的管理下にあり、1 つまたは複数の内部ゲートウェイプロトコルとメトリックを使用して自律システム内のパケットのルーティング方法を決定し、外部ゲートウェイプロトコルを使用して他の自律システムへのパケットのルーティングの方法を決定する、ルーターの集合。

自律システム番号 - 自律システムを識別する 32 ビットの数字。

委任- IP アドレスブロックまたは AS 識別子の管理権(すなわち使用権)を、証明書をエンティティに発行することによって委任すること。

第 1 オクテット- DER エンコードされたビット文字列の値の最初のオクテット[X.690]。

IP v4 アドレス- 「.」で区切られた 4 個の 0～255 の範囲の十進数としてあらわされる 32 ビットの識別子。10.5.0.5 は IPv4 アドレスの例である。

IP v6 アドレス- 「:」で区切られた 8 個の 0～ffff の範囲の 16 進数として表される 128 ビットの識別子。2001:0:200:3:0:0:0:1 は IPv6 アドレスの例である。:0: フィールドの文字列は「::」に置き換えてもよいため、2001:0:200:3::1 は直前の例と同じアドレスを表す([RFC3513]参照)。

プリフィックス あるアドレスの初期ビットのいくつかで構成されるビット文字列。アドレスの後ろに「/」および初期ビットの個数が続くものとしてあらわされる。10.5.0.0/16 および 2001:0:200:3:0:0:0:0/64(または 2001:0:200:3::/64)プリフィックスの例である。プリフィックスは、下位のゼロフィールドを省略することによって短縮されることが多いが、示された数のイニシャルビットを含むのに十分なフィールドがあるべきである。10.5/16 および 2001:0:200:3/64 は、短縮されたプリフィックスの例である。

地域インターネットレジストリ (RIR) - IP アドレスおよび AS 識別子の管理を地域内で行うことを IANA に承認された団体。本文書の作成の時点では、AfriNIC、APNIC、ARIN、LACNIC、および RIPE NCC がある。

使用権 - IP アドレスプリフィックスに関しては、インターネット全体でプリフィックスの通知を発信することができる AS を指定することを承認されていること。自律システム識別子に関しては、その自律システム識別子を使って他のネットワークオペレータに自分自

身を特定するネットワークを運営することを承認されていること。

後続オクテット - DER エンコードされたビット文字列の値の 2 番目から最後までのオクテット[X.690]。

トラストアンカー - 証明書パス検証を行うときに信頼する証明書([RFC3280]参照)。

本文書中の「MUST（しなければならない)」「MUST NOT（してはならない)」「REQUIRED（要求される)」「SHALL（すべきである)」「SHALL NOT（すべきでない)」「SHOULD（したほうがよい)」「SHOULD NOT（しないほうがよい)」「RECOMMENDED（推奨される)」「MAY（してもよい)」「OPTIONAL（選択できる)」というキーワード群は、[RFC2119]での記述のとおりに解釈される。

2. IP アドレス委任拡張領域

この拡張は、IP アドレスをエンディティに属する公開鍵に結合することによって、それらのアドレスの割り振りをおこなう。

2.1. コンテキスト

IP アドレス空間は現在、名目上 IANA をルートとするが RIR によって管理される階層によって管理されている。IANA は IP アドレス空間を RIR に割り振り、RIR は次に IP アドレス空間をインターネットサービスプロバイダ(ISP)に割り振り、ISP は IP アドレス空間を下流のプロバイダ、顧客などに割り振る。RIR はまた、エンドエンティティである組織、すなわち他の組織に空間を移譲しない組織に IP アドレス空間を割り当てることもできる。(割り振りおよび割り当てのプロセスについては、[RFC2050]および関連する RIR ポリシードキュメントを参照。)

IP アドレス委任拡張は、IP アドレスブロックが適切に委任されること、すなわちエンティティが IP アドレス空間を使用または再割り振りすることを承認することを検証できるようにすることを目的とする。したがって、IP アドレス空間を割り振るための既存の管理の枠組みの固有の権威性を利用することは意味がある。上記のセクション 1 で説明したように、これはこのセクションで説明する拡張領域を持つ証明書を発行することによって達成される。この拡張領域内の情報を使用する 1 方法の例としては、ある組織が特定の IP アドレスブロックへの経路を通知する BGP UPDATE を発信することを承認されていることを確認するために、あるエンティティがこの情報を使用するというものがある。[RFC1771]、[S-BGP]などを参照。

2.1.1. IP アドレスまたはプリフィックスのエンコーディング

IP アドレスには、IPv4 および IPv6 の 2 つの系統がある。

IPv4 アドレスとは、「.」で区切られた 4 個の 0～255 の範囲の十進数としてあらわされる 32 ビットの数字である。10.5.0.5 は IPv4 アドレスの例である。

IPv6 アドレスとは、「:」で区切られた 8 個の 0～ffff の範囲の 16 進数として表される 128 ビットの数字。2001:0:200:3:0:0:0:1 は IPv6 アドレスの例である。IPv6 アドレスはしばしば、値が 0 である隣接するフィールドを持つ。このような 0 フィールドのグループは、2 個のセミコロン("::")によって短縮することができる。したがって前の例は、2001:0:200:3::1 と表すことができる。

アドレスプリフィックスとは、最上ビットが同じである 2^k 個の連続したアドレスの集合である。たとえば、10.5.0.0～10.5.1.255 の 512 個の IPv4 アドレスの集合は、上位 23 ビットがすべて同じである。このアドレスの集合は、スラッシュ("/")と定数であるビットの数を集合内の最下位アドレスに付加することによって表される。例の集合のプリフィックスは 10.5.0.0/23 で、2^(32-23) = 2^9 個のアドレスが含まれる。2001:0:200:0:0:0:0:0 ～ 2001:0:3ff:ffff:ffff:ffff:ffff:ffff(2^89 個のアドレス)の集合は、

2001:0:200:0:0:0:0:0/39 または同等に 2001:0:200::/39 とあらわされる。プリフィックスは、最下位のゼロフィールドを省略することによって短縮してもよいが、示された 数の定数ビットを含むのに十分なフィールドがあるべきである。例の IPv4 プリフィックスを省略した形式は、10.5.0/23 であり、IPv6 プリフィックスのものは 2001:0:200/39 である。

IP アドレスまたはプリフィックスは、IP アドレス委任拡張領域内では、定数最上位ビットを含む DER エンコードされた ASN.1 ビット文字列としてエンコードされる。ビット文字列の DER エンコーディングはビット文字列タイプ(0x03)、それに続く値オクテットの数(のエンコード)、それに続く値で構成される[X.690] を思い出すこと。値は、最後の値オクテット内で未使用のビット数を指定する「第 1 オクテット」と、それに続くビット文字列を含む「後続オクテット」で構成される。(IP アドレスについては、長さのエンコーディングは単に長さである。)

単独のアドレスの場合は、すべてのビットは定数であるため、IPv4 アドレスのビット文字列には 32 ビットある。アドレス 10.5.0.4 の DER エンコーディング内の後続オクテットは 0x0a 0x05 0x00 0x04 である。最終オクテットのすべてのビットが使用されるため、第 1 オクテットは 0x00 である。したがって、DER エンコードされたビット文字列内のオクテットは以下のとおりである。

```
タイプ 長さ 未使用ビット ...
0x03 0x05   0x00   0x0a 0x05 0x00 0x04
```

同様に、プリフィックス 10.5.0/23 の DER エンコーディングは以下のとおりである。

```
タイプ 長さ 未使用ビット ...
0x03 0x04   0x01   0x0a 0x05 0x00
```


この場合、3 個の後続オクテットには 24 ビットが含まれるが、プリフィックスは 23

個しか使用していないため､最終オクテット内に未使用のビットが１つある｡したがって､第１オクテットは１である(DER では､すべての未使用ビットがゼロビットにセットされなければならない(MUST))｡

IPv6 アドレス 2001:0:200:3:0:0:0:1 の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x11   0x00   0x20 0x01 0x00 0x00 0x02 0x00 0x00 0x03
                   0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01
```

プリフィックス 2001:0:200/39 は最終オクテットに未使用ビットを 1 つ含むが、その DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x01   0x20 0x01 0x00 0x00 0x02
```

2.1.2. IP アドレスの範囲のエンコーディング

任意の隣接する IP アドレス範囲は隣接するプリフィックスの集合で表現できるが、最下位アドレスと最上位アドレスを含むシーケンスとして範囲をエンコードすることによって、より簡潔な表現が得られる。ここで各アドレスはビット文字列としてエンコードされる。シーケンス内では、範囲内の最下位アドレスを表すビット文字列は、アドレスからすべての最下位ゼロビットを取り除くことで形成され、範囲内の最上位アドレスを表すビット文字列は、すべての最下位 1 ビットを取り除くことで形成される。DER ビット文字列エンコーディングでは、最終オクテット内のすべての未使用ビットがゼロビットにセットされなければならない(MUST)｡プリフィックスは､常に範囲として表現することができるが、範囲は常にプリフィックスとして表現することはできないことに注意。

プリフィックス 10.5.0/23 で表現されるアドレスは、10.5.0.0～10.5.1.255 である。最下位アドレスは 16 個のゼロビットで終わるが取り除かれている。結果の 16 ビット文字列の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x03   0x00   0x0a 0x05
```

最上位アドレスは 9 個の 1 ビットで終わるが取り除かれている。結果の 23 ビット文字

列の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x04   0x01   0x0a 0x05 0x00
```


プリフィックス 2001:0:200/39 は、最下位アドレス(2001:0:200::)の DER-エンコーディングが以下のとおりであるような範囲としてエンコードできる。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x01   0x20 0x01 0x00 0x00 0x02
```

最上位アドレス(2001:0:3ff:ffff:ffff:ffff:ffff:ffff)は、90 個の最下位 1 ビットを取り除くと 38 ビット文字列となり、以下のようにエンコードされる。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x02   0x20 0x01 0x00 0x00 0x00
```

特殊な場合として、すべての IP アドレスブロック、すなわちすべてゼロビットのプリフィックスは、長さオクテットが 1、第 1 オクテットがゼロ、後続オクテットなしで DER エンコードしなければならない(MUST)。

```
タイプ 長さ 未使用ビット ...
0x03 0x01   0x00
```

IP アドレスに関しては、一連のゼロビットは意味を持つことに注意。たとえば、以下

の 10.64/12 の DER エンコーディング。

```
タイプ 長さ 未使用ビット ...
0x03 0x03  0x04  0x0a 0x40
```

は、10.64.0/20 の DER エンコーディングとは異なる。

```
タイプ 長さ 未使用ビット ...
0x03 0x04  0x04  0x0a 0x40 0x00
```

2.2. 仕様

2.2.1. OID

この拡張の OID は、id-pe-ipAddrBlocks である。

```
id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }
```

ここで [RFC3280] は以下のように定義する。

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```


2.2.2. クリティカリティ

この拡張は、クリティカルであるものとする(SHOULD)。この拡張の目的とする用途は、拡張領域で指定される IP アドレスのブロックの使用権を暗示することである。CA は拡張

をクリティカルとマークして、証明書が発行された目的のために依存者が証明書を利用するためには、拡張領域の意味を理解しなければならない(MUST)という注意を伝える。個の拡張領域を含む証明書を使用する、新規作成されたアプリケーションは、この拡張を認識するものと期待される。

2.2.3. 文法

```
id-pe-ipAddrBlocks      OBJECT IDENTIFIER ::= { id-pe 7 }

IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE {    -- AFI & オプション SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }

IPAddressRange      ::= SEQUENCE {
   min                  IPAddress,
   max                  IPAddress }

IPAddress           ::= BIT STRING
```

2.2.3.1. タイプ IPAddrBlocks

IPAddrBlocks タイプは、IPAddressFamily タイプのシーケンスである。

2.2.3.2. タイプ IPAddressFamily

IPAddressFamily タイプは、addressFamily および ipAddressChoice 要素を含むシーケンスである。

2.2.3.3. 要素 addressFamily

addressFamily 要素は、2 オクテットのアドレスファミリ識別子(AFI)をネットワークバイトオーダーで含み、オプションで 1 オクテットの後続アドレスファミリ識別子(SAFI)がそれに続くオクテット文字列である。AFI および SAFI はそれぞれ[IANA-AFI]および[IANA-SAFI]で指定される。

特定の AFI とオプションの SAFI に対して、承認が与えられていない場合は、IPAddrBlocks シーケンス内の AFI/SAFI に対して、IPAddressFamily メンバーがあってはならない(MUST NOT)。

AFI と SAFI の固有の組み合わせに対して、IPAddressFamily シーケンスは 1 だけでなくてはならない(MUST)。各シーケンスは、addressFamily の値で昇順に並んでいなくてはならない(MUST) (オクテットは符号なしの量として扱う)。SAFI のない addressFamily は、SAFI を含むものより前に置かなければならない(MUST)。IPv4 と IPv6 の両方のアドレスが指定された場合は、IPv4 アドレスを IPv6 アドレスより前に置かなければならない(MUST)(IPv4 AFI の 0001 は IPv6 AFI の 0002 より小さいため)。

2.2.3.4. 要素 ipAddressChoice およびタイプ IPAddressChoice

ipAddressChoice 要素のタイプは IPAddressChoice である。IpAddressChoice タイプは inherit または addressesOrRanges 要素のいずれかの CHOICE である。

2.2.3.5. 要素 inherit

IPAddressChoice CHOICE に inherit 要素が含まれている場合は、指定された AFI およびオプションの SAFI に対する承認された IP アドレスの集合が、addressesOrRanges 要素

を含む IPAddressChoice を含む証明書が見つかるまで、再帰的に発行者の証明書、または発行者の発行者の証明書からとられる。

2.2.3.6. 要素 addressesOrRanges

addressesOrRanges 要素は IPAddressOrRange タイプのシーケンスである。addressPrefix および addressRange 要素は、以下のバイナリ表現を用いてソートしなければならない(MUST)。

<範囲内の最下位 IP アドレス> | <プリフィックスの長さ>

ここで"|" は連結を表す。この表現内のオクテット(a.b.c.d | IPv4 の長さ または s:t:u:v:w:x:y:z | IPv6 の長さ)は、DER エンコードされたビット文字列値のオクテットではないことに注意。たとえば、以下の 2 つの addressPrefix があるとする。

IP アドレス	長さ	DER エンコーディング			
		タイプ	長さ	未使用ビット...	
10.32.0.0	12	03	03	04	0a 20
10.64.0.0	16	03	03	00	0a 40

32 は 64 より小さいため、プリフィックス 10.32.0.0/12 は、プリフィックス 10.64.0.0/16 より前にこなければならない(MUST)。一方、DER ビット文字列でソートされるとすると、未使用ビットオクテットは逆の順序でソートされるため、順序は逆になる。拡張領域内の IPAddressOrRange choice のペアは、重複してはならない(MUST NOT)。隣接するアドレスプリフィックスまたは範囲は単独の範囲または、可能であれば常に、単独のプリフィックスに組み合わせなければならない(MUST)。

2.2.3.7. タイプ IPAddressOrRange

IPAddressOrRange タイプは、addressPrefix(IP プリフィックスまたはアドレス)または addressRange (IP アドレス範囲)要素の CHOICE である。

この仕様では、プリフィックスとしてエンコードできるアドレス範囲は、IPAddress 要素(ビット文字列)を用いてエンコードしなければならず(MUST)、プリフィックスとしてエンコードできない範囲は IPAddressRange(2 つのビット文字列を含むシーケンス)を用いてエンコードしなければならない(MUST)。以下の擬似コードは、所定のアドレス範囲のエンコードを選択する方法を説明するものである。

```
LET  N = 範囲の最下位および最上位アドレス内の、一致する最上位ビットの数
IF 最下位アドレスに残っているすべてのビットがゼロビット
 AND 最上位アドレスに残っているすべてのビットが 1 ビット
THEN 範囲は N ビット IP アドレスとしてエンコードしなければならない(MUST)
ELSE 範囲 IPAddressRange としてエンコードしなければならない(MUST)
```

2.2.3.8. 要素 addressPrefix およびタイプ IPAddress

addressPrefix 要素は IPAddress タイプである。IPAddress タイプはアドレスの最上位(左側の)N ビットが定数であり、残りのビット(IPv4 では 32-N ビット、IPv6 では 128-N ビット)がゼロまたは 1 のいずれかであるような IP アドレスの範囲を定義する。たとえば、IPv4 プリフィックス 10.64/12 はアドレス 10.64.0.0～10.79.255.255 に対応し、10.64/11 は 10.64.0.0～10.95.255.255 に対応する。IPv6 プリフィックス 2001:0:2/48 はアドレス 2001:0:2::～2001:0:2:ffff:ffff:ffff:ffff:ffff を表す。

IP アドレスプリフィックスは、ビット文字列としてエンコードされる。ビット文字列の DER エンコーディングは、文字列の第 1 オクテットを使って、最終後続オクテットのうちのいくつが未使用であるかを指定する。

DER エンコーディングでは、これらの未使用ビットがゼロビットにセットされなければ

ならない(MUST)と指定している。

例:

```
          128.0.0.0         = 1000 0000.0000 0000.0000 0000.0000 0000
        ～ 143.255 255 255 = 1000 1111.1111 1111.1111 1111.1111 1111
      エンコードするビット文字列 = 1000
                        タイプ 長さ 未使用ビット...
  エンコーディング = 0x03 0x02   0x04   0x80
```

2.2.3.9. 要素 addressRange およびタイプ IPAddressRange

addressRange 要素はタイプ IPAddressRange である。IPAddressRange タイプは、最小(要素 min)と最大(要素 max)の IP アドレスを含むシーケンスで構成される。各 IP アドレスはビット文字列としてエンコードされる。IPAddressRange 内の最小アドレスの意味論的解釈は、指定されていないすべてのビット(完全な長さの IP アドレスに関して)がゼロビットであるということである。IPAddressRange 内の最大アドレスの意味論的解釈は、指定されていないすべてのビット(完全な長さの IP アドレスに関して)が 1 ビットであるということである。最小アドレスのビット文字列は、最小アドレスからすべての最下位ゼロビットを取り除くことで得られる。最大アドレスのビット文字列は、最大アドレスからすべての最下位 1 ビットを取り除くことで得られる。

例:

```
          129.64.0.0         = 1000 0001.0100 0000.0000 0000.0000 0000
        to 143.255.255.255   = 1000 1111.1111 1111.1111 1111.1111 1111
         最小ビット文字列 = 1000 0001.01
         最大ビット文字列 = 1000
  エンコーディング = シーケンス {
              タイプ 長さ 未使用ビット ...
      min     0x03 0x03   0x06   0x81        0x40
      max     0x03 0x02   0x04   0x80
            }
```

証明書パス検証を行うときに IP アドレスブロックの比較を簡素化するために、最大 IP アドレスは値が 1 であるビットを少なくとも 1 つ含んでいなければならない(MUST)。すなわち、後続オクテットは省略されたりすべてゼロであったりしてはならない。

2.3. IP アドレス委任拡張領域証明書パス検証

IP アドレス委任拡張領域を含む証明書の証明書パス検証には、追加の処理が必要である。パス内の各証明書が検証されるときに、その証明書の IP アドレス委任拡張領域内の IP アドレスが発行者の証明書の IP アドレス委任拡張領域内の IP アドレスに含まれていなければならない(MUST)。そうなっていない場合は、検証は失敗しなければならない(MUST)。

証明書パス検証のトラストアンカーである証明書または IP アドレス委任拡張領域を含む証明書、およびパス上のすべての証明書は、それぞれ IP アドレス委任拡張領域を含まなければならない(MUST)。許されるアドレス範囲の初期集合は、トラストアンカー証明書からとられる。

3. 自律システム識別子委任拡張領域

この拡張領域は、自律システム(AS)識別子をエンティティに属する公開鍵に結合することによって、その AS 識別子のエンティティへの割り振りを行う。

3.1. コンテキスト

AS 識別子委任は現在、名目上 IANA をルートとするが RIR によって管理される階層によって管理されている。IANA は AS 識別子を RIR に割り振り、RIR は次に AS 識別子をエンドエンティティである組織、すなわち他の組織に AS 識別子を移譲しない組織に AS 識別子を割り当てる。AS 識別子委任拡張領域は、AS 識別子が適切に委任されること、すなわちエンティティがこれらの AS 識別子を使用することを承認することを検証できるようにすることを目的とする。したがって、AS 識別子を管理するため既存の枠組みの固有の権威性を利用することは意味がある。上記のセクション 1 で説明したように、これはこのセクションで説明する拡張領域を持つ証明書を発行することによって達成される。この拡張領域内の情報を使用する 1 方法の例としては、あるエンティティが、ある組織が AS 識別子で指定さ

れる AS を管理する承認を得ているかどうかを確認するために、この領域を使用することがある。AS 識別子の割り振りを表すためにこの拡張領域を使用することは、AS 識別子が管理される手続きや、AS がいつ使われるべきかを変更することを意図するものではない。[RFC1930]参照。

3.2. 仕様

3.2.1. OID

この拡張の OID は、id-pe-autonomousSysIds である。

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }
```

ここで [RFC3280] は以下のように定義する。

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```


3.2.2. クリティカリティ

この拡張は、クリティカルであるものとする(SHOULD)。この拡張の目的とする用途は、拡張領域内の AS 識別子の使用権を暗示することである。CA は拡張をクリティカルとマークして、証明書が発行された目的のために依存者が証明書を利用するためには、拡張領域の意味を理解しなければならない(MUST)という注意を伝える。個の拡張領域を含む証明書を使用する、新規作成されたアプリケーションは、この拡張を認識するものと期待される。

3.2.3. 文法

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

ASIdentifiers       ::= SEQUENCE {
    asnum               [0] EXPLICIT ASIdentifierChoice OPTIONAL,
    rdi                 [1] EXPLICIT ASIdentifierChoice OPTIONAL}

ASIdentifierChoice  ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   asIdsOrRanges        SEQUENCE OF ASIdOrRange }

ASIdOrRange         ::= CHOICE {
    id                  ASId,
    range               ASRange }

ASRange             ::= SEQUENCE {
    min                 ASId,
    max                 ASId }

ASId                ::= INTEGER
```

3.2.3.1. タイプ ASIdentifiers

ASIdentifiers タイプは 1 つまたはそれ以上の形式の自律システム識別子(AS 番号(asnum 要素内)またはルーティングドメイン識別子(rdi 要素内))を含むシーケンスである。ASIdentifiers タイプに複数の形式の識別子が含まれている場合は、asnum エントリは rdi エントリより前に置かれなければならない(MUST)。AS 番号は BGP によって使用され、ルーティングドメイン識別子は IDRP ないに指定される[RFC1142]。

3.2.3.2. 要素 asnum、rdi、およびタイプ ASIdentifierChoice

asnum および rdi 要素は、どちらもタイプ ASIdentifierChoice である。ASIdentifierChoice タイプは inherit または asIdsOrRanges 要素の CHOICE である。

3.2.3.3. 要素 inherit

ASIdentifierChoice に inherit 要素が含まれている場合、承認された識別子の集合は、asIdsOrRanges 要素を含む ASIdentifierChoice を含む証明書が見つかるまで、再帰的に発行者の証明書、または発行者の発行者の証明書からとられる。特定の形式の AS 識別子に対して承認が与えられていない場合は、対応する asnum/rdi メンバーが ASIdentifiers シーケンスないにあってはならない(MUST NOT)。

3.2.3.4. 要素 asIdsOrRanges

asIdsOrRanges 要素は、ASIdOrRange タイプのシーケンスである。asIdsOrRanges シーケンス内の項目のペアは、重複してはならない(MUST NOT)。任意の隣接する一連の AS 識別子は、可能であれば常に単独の範囲に組み合わせなければならない(MUST)。asIdsOrRanges 要素内の AS 識別子は、数値の増える順にソートされなければならない(MUST)。

3.2.3.5. タイプ ASIdOrRange

ASIdOrRange タイプは単独の整数(ASId)または単独のシーケンス(ASRange)の CHOICE である。

3.2.3.6. 要素 id

id 要素はタイプ ASId を持つ。

3.2.3.7. 要素 range

range 要素はタイプ ASRange を持つ。

3.2.3.8. タイプ ASRange

ASRange タイプは min および max 要素からなるシーケンスで、AS 識別子の値の範囲を指定するために使用される。

3.2.3.9. 要素 min および max

min および max 要素はタイプ ASId を持つ。min 要素は、範囲内の最小の AS 識別子を指定するために使用され、max 要素は範囲内の最大の AS 識別子の値を指定する。

3.2.3.10. タイプ ASId

ASId タイプは INTEGER である。

3.3. 自律システム識別子委任拡張領域証明書パス検証

自律システム識別子委任拡張領域を含む証明書の証明書パス検証には、追加の処理が必要である。パス内の各証明書が検証されるときに、その証明書の自律システム識別子委任拡張領域内の AS 識別子が発行者の証明書の自律システム識別子委任拡張領域に含まれていなければならない(MUST)。 そうなっていない場合は、検証は失敗しなければならない(MUST)。自律システム識別子委任拡張領域を含む証明書の証明書パス検証のトラストアンカーである証明書および、パス上のすべての証明書は、それぞれ自律システム識別子委任拡張領域を含まなければならない(MUST)。許される AS 識別子の初期集合は、トラストアンカー証明書からとられる。

4. セキュリティ上の配慮

本仕様は 2 つの X.509 拡張を説明する。X.509 証明書はデジタル署名されるため、追加のインテグリティサービスは不要である。これらの拡張領域を持つ証明書は、秘密にする必要はなく、これらの証明書に対する無制限の匿名によるアクセスは、セキュリティ上の問題を生じない。

しかし､本仕様の範囲外のセキュリティ要素が証明書ユーザに提供される保証に影響する。このセクションは、実装者、管理者、およびユーザが考慮すべき重要な問題を強調する。

これらの拡張は承認情報、すなわち IP アドレスまたは AS 識別子の使用権を表す。これらは、BGP のセキュアバージョン[S-BGP]をサポートするために開発されたが、他のコンテキストで利用することもできる。セキュア BGP のコンテキストでは、これらの拡張領域を含む証明書は可能性として機能する。証明書は、秘密鍵の保有者(サブジェクト)が拡張領域に現される IP アドレスまたは AS 識別子を使用することを承認されていることを主張する。この機能モデルの結果として、一般的な PKI の慣習とは異なり、サブジェクトフィールドは概してセキュリティ目的とは関係ない。

5. 謝辞

著者は、Charles Gardiner、Russ Housley、James Manger、および Jim Schaad の本仕様への貢献に対し感謝の意を表します。

付録 A -- ASN.1 モジュール

この標準的付録は、準拠 PKI コンポーネントによって使用される IP アドレスおよび AS 識別子拡張領域について ASN.1 文法で説明する。

```
IPAddrAndASCertExtn { iso(1) identified-organization(3) dod(6)
```

```
        internet(1) security(5) mechanisms(5) pkix(7) mod(0)
        id-mod-ip-addr-and-as-ident(30) }
    DEFINITIONS EXPLICIT TAGS ::=
BEGIN
     -- Copyright (C) インターネットソサエティ (2004)--
     -- 本 ASN.1 モジュールの本バージョンは、RFC 3779 の一部である。   --
     -- 完全な法律上の表示については、RFC 自身を参照のこと。          --

-- すべてエキスポート --

IMPORTS

-- PKIX 固有の OID およびアーク --
    id-pe FROM PKIX1Explicit88 { iso(1) identified-organization(3)
              dod(6) internet(1) security(5) mechanisms(5) pkix(7)
              id-mod(0) id-pkix1-explicit(18) };

-- IP アドレス委任拡張領域 OID --

id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }

-- IP アドレス委任拡張領域文法 --

IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE { -- AFI とオプションの SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }
```

```
   IPAddressRange      ::= SEQUENCE {
      min                 IPAddress,
      max                 IPAddress }

   IPAddress           ::= BIT STRING
```



```
   -- 自律システム識別子委任拡張領域 OID --

   id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

   -- 自律システム識別子委任拡張領域文法 --

   ASIdentifiers       ::= SEQUENCE  {
       asnum               [0] ASIdentifierChoice OPTIONAL,
       rdi                 [1] ASIdentifierChoice OPTIONAL }

   ASIdentifierChoice  ::= CHOICE {
      inherit              NULL, -- 発行者から継承 --
      asIdsOrRanges        SEQUENCE  OF ASIdOrRange }

   ASIdOrRange         ::= CHOICE {
       id                  ASId,
       range               ASRange }

   ASRange             ::= SEQUENCE  {
       min                 ASId,
       max                 ASId }
```

```
ASId                ::= INTEGER

END
```

付録 B -- IP アドレス委任拡張領域の例

以下の IPv4 ユニキャストアドレスプリフィックスを指定する、重要な X.509 v3 証明書拡張

1) 10.0.32/20 すなわち 10.0.32.0～10.0.47.255
2) 10.0.64/24 すなわち 10.0.64.0～10.0.64.255
3) 10.1/16 すなわち 10.1.0.0 ～10.1.255.255
4) 10.2.48/20 すなわち 10.2.48.0～10.2.63.255
5) 10.2.64/24 すなわち 10.2.64.0～10.2.64.255
6) 10.3/16 すなわち 10.3.0.0 ～10.3.255.255、および
7) 発行者の証明書からすべての IPv6 アドレスを継承

は、以下のとおり(16 進):

```
30 46                       Extension {
   06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
   01 01 ff                   critical
   04 37                      extnValue {
      30 35                     IPAddrBlocks {
         30 2b                    IPAddressFamily {
            04 03 0001  01         addressFamily: IPv4 Unicast
                                    ipAddressChoice
            30 24                     addressesOrRanges {
```

```
                                    IPAddressOrRange
        03 04 04 0a0020              addressPrefix10.0.32/20
                                    IPAddressOrRange
        03 04 00 0a0040              addressPrefix10.0.64/24
                                    IPAddressOrRange
        03 03 00 0a01                addressPrefix   10.1/16
                                    IPAddressOrRange
        30 0c                        addressRange {
           03 04 04 0a0230              min         10.2.48.0
           03 04 00 0a0240              max         10.2.64.255
                                      } --addressRange
                                    IPAddressOrRange
        03 03 00 0a03                addressPrefix   10.3/16
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
  30 06                         IPAddressFamily {
     04 02 0002                  addressFamily: IPv6
                                   ipAddressChoice
     05 00                           inherit from issuer
                                } -- IPAddressFamily
                              } -- IPAddrBlocks
                            } -- extnValue
                          } -- Extension
```

この例は、プリフィックスと範囲がどのようにソートされるかを示す。

+ プリフィックス1の未使用ビット(4)がプリフィックス2の未使用ビット(0)より大きくても、プリフィックス 1 はプリフィックス 2 より前に置かれなければならない(MUST)。

+ プリフィックス 2 のビット文字列エンコーディングのオクテット数(4)がプリフィックス 3 のビット文字列エンコーディングのオクテット数(3)より大きくても、プリフィックス 2 はプリフィックス 3 より前に置かれなければならない(MUST)。

+ プリフィックス 4 と 5 は隣接している(アドレスの範囲 10.2.48.0～10.2.64.255 を表す)ので、1 つの範囲に組み合わせなければならない(MUST)(範囲は単独のプリフィックス

によってエンコードできないため)。

+ 範囲の max 要素内 6 個の連続するゼロビットが、値の意味論的解釈にとって重要であることに注意(すべての未使用ビットは、ゼロでなく 1 と解釈されるため)。min 要素内の 4 個の連続するゼロビット(したがって、min 要素のエンコーディング内の(4)個の未使用ビット)は重要ではなく、取り除かなくてはならない(MUST)。(DER エンコーディングでは、最後の後続オクテット内の未使用ビットはすべてゼロにセットしなくてはならない(MUST))。

+ プリフィックス 4 と 5 で形成される範囲は、範囲の SEQUENCE タグ(30)がプリフィックス 6 のエンコードに使用されるビット文字列(03)のタグより大きくても、プリフィックス 6 より前に置かれなければならない(MUST)。

+ IPv4 のアドレスファミリ識別子(0001)は IPv6 の識別子(0002)より小さいので、IPv4 情報は IPv6 情報より前に置かれなければならない(MUST)。

IPv6 プリフィックス 2001:0:2/48 および IPv4 プリフィックス 10/8 と 172.16/12 を指定し、すべての IPv4 マルチキャストアドレスを発行者の証明書から継承する拡張領域は、以下のとおり(16 進):

```
   30 3d                       Extension {
      06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
      01 01 ff                   critical
      04 2e                      extnValue {
         30 2c                     IPAddrBlocks {
            30 10                    IPAddressFamily {
               04 03 0001 01          addressFamily: IPv4 Unicast
                                       ipAddressChoice
               30 09                     addressesOrRanges {
```

```
                                    IPAddressOrRange
          03 02 00 0a                addressPrefix   10/8
                                    IPAddressOrRange
          03 03 04 b010              addressPrefix   172.16/12
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
    30 07                       IPAddressFamily {
       04 03 0001 02             addressFamily: IPv4 Multicast
                                  ipAddressChoice
       05 00                        inherit from issuer
                                } -- IPAddressFamily
    30 0f                       IPAddressFamily {
       04 02 0002                addressFamily: IPv6
                                  ipAddressChoice
       30 09                        addressesOrRanges {
                                      IPAddressOrRange
          03 07 00 200100000002       addressPrefix  2001:0:2/47
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
                              } -- IPAddrBlocks
                            } -- extnValue
                             } -- Extension
```


付録 C -- AS 識別子委任拡張領域の例

AS 番号 135、3000～3999、5001 を指定し、すべてのルーティングドメイン識別子を発行者の証明書から継承する拡張領域は以下のとおり(16 進)

```
   30 2b                        Extension {
```

```
06 08 2b06010505070108      extnID        1.3.6.1.5.5.7.1.8
01 01 ff                    critical
04 1c                       extnValue {
   30 1a                      ASIdentifiers {
      a0 14                     asnum
                                  ASIdentifierChoice
         30 12                      asIdsOrRanges {
                                      ASIdOrRange
            02 02 0087                  ASId
                                      ASIdOrRange
            30 08                       ASRange {
               02 02 0bb8                 min
               02 02 0f9f                 max
                                        } -- ASRange
                                      ASIdOrRange
            02 02 1389                  ASId

                                    } -- asIdsOrRanges
                                  } -- asnum
      a1 02                       rdi {
                                    ASIdentifierChoice
         05 00                        inherit from issuer
                                  } -- rdi
                                } -- ASIdentifiers
                              } -- extnValue
                            } -- Extension
```

付録 D -- X.509 属性証明書の使用

この付録では、属性証明書 ([RFC3281]で指定されるように、AC) を、地域インターネットレジストリ(RIR)からエンドユーザ組織へIPアドレスブロックまたはAS識別子の使用権を伝えるために使用するという提案に起因する問題について議論する。

AS 識別子と IP アドレスブロックの 2 つのリソースは、現在異なる方法で管理されている。AS 識別子の使用権を持つすべての組織は、その承認を RIR から直接受ける。IP アドレスブ

ロックの使用権を持つ組織は、その承認を直接 RIR から、または間接的にたとえば下流のサービスプロバイダから受け、その下流のサービスプロバイダは別のサービスプロバイダから承認をうけ、サービスプロバイダは RIR から承認を受ける。

将来 AS 識別子が再割り振りされるかもしれないので、メカニズムは 3 レベルの階層に依存すべきではないことに注意。

RFC 3281 のセクション 1 で、承認情報を伝える拡張領域を持つ公開鍵証明書(PKC)を使用するよりも AC を使用するほうが望ましい理由が 2 つ述べられている。

「承認情報は、PKC 拡張領域におくことも、別の属性証明書(AC)におくこともできる。承認情報を PKC に置くことは、通常 2 つの理由で望ましくない。第 1 に、承認情報は、アイデンティティと公開鍵の結合とは異なる寿命を持つことがよくある。商人情報が PKC 拡張領域におかれると、一般的な結果として PKC の使用可能な寿命が短縮される。第 2 に、PKC の発行者は通常、承認情報に関する権威を持たない。この結果、PKC の発行者は権威をもつものから承認情報を得るという余分のステップを踏まなければならない。」

「これらの理由により、承認情報は PKC とは独立させるほうがよいことが多い。しかし、承認情報はアイデンティティに結合する必要もある。AC はこの結合を提供する。それは単に、デジタル署名(または保証)されたアイデンティティと属性の集合である。」

IP アドレスと AS 識別子の承認の場合、これらの理由は当てはまらない。第 1 に、公開鍵証明書は承認のためだけに発行されるので、証明書の寿命は承認の寿命に正確に対応し、それは発行者と承認を受けるエンティティとの間の契約関係に結びついていることが多い。サブジェクト名と発行者名は証明書パス検証の間に連鎖のために使用されるだけであり、物理的なエンティティに対応する必要はない。PKC 内のサブジェクト名は、実際に発行 CA によってランダムに割り当てられ、リソースの保有者に制限つきの匿名性を与えてもよい。第 2 に、証明書の階層は、証明書の発行者が承認情報に関する権威を持つように構築されている。

したがって、上に引用した最初の段落は AS 番号と IP アドレスブロックの割り振りの場合には当てはまらない。リソースはアイデンティティではなく PKC 内の公開鍵に対応する秘密鍵の保有者に結合されているため、2 番目に引用した段落の要点は当てはまらない。

RFC 3281 は、それに準拠する属性証明書が満たさなければならないいくつかの要件を指定している。S-BGP に関係して、より重要な要件は以下のとおりである。

1 セクション 1 から: 「本仕様では、AC 連鎖の使用は推奨されない(NOT RECOMMEND)。その他の(将来的な)仕様は、AC 連鎖の仕様を扱うかもしれない。」

IANA から RIR へ、RIR から ISP へ、ISP から DSP への割り振りおよびエンド組織への割り当てには、少なくとも IP アドレスブロックに関しては連鎖の仕様が必要である。上位者の AC をどのように見つけ、それをどのように処理するかについての説明が提供されなければならない。本文書の読者は、連鎖を避けることができるような方法を提案することを奨励される。

2 セクション 4.2.9 から: 「セクション 4.3 はこのプロファイルとともに用いてもよい(MAY)拡張領域および、それらがクリティカルとマーク付けされるかどうかを定義する。他のクリティカルな拡張領域が使用される場合、AC はこのプロファイルに準拠しない。しかし、他のクリティカルでない拡張領域が使用される場合、AC はこのプロファイルに準拠する。」

これは、本仕様で定義される委任拡張領域(クリティカルである)が、単純に AC におくことはできないということを意味する。クリティカルとマーク付けされていなければ使用できるが、意図される用途では、思いもよらぬアプリケーションによって拡張領域を含む証明書がアイデンティティ証明書として使用されることがないように、クリティカルであることが必要である。

3 セクション 4.5 から: 「AC の発行者は、PKC の発行者でもあることはできない(MUST

NOT)。つまり、AC の発行者は同時に CA でもあることはできない。」

これは、各 AC の発行者が、AC 保有者の公開鍵を含む PKC を発行するために、独立した CA を必要とすることを意味する。AC の発行者は保有者の PKC を発行することができず、PKC の発行者は AC に署名することができない。したがって、PKI 内の各エンティティは、CA のほかに AC 発行者を運営する必要がある。PKC が使用された場合に比べて、属性証明書のサポートを処理するために、2 倍の数の証明書発行者と CRL が必要になる。単独の目的で証明書を発行する発行者が 2 つあると、不整合が生じる可能性もある。

RFC 3281 の AC モデルは、AC 保有者属性または承認を実証したいときに、保有者が AC を AC 検証者に提示するということを含意する。本文書で定義される拡張領域の意図する用途では、AC 検証者(NOC)と AC の発行者(すべての RIR および NOC)との間の直接の相互作用はない。

主張される使用権の対象への署名があれば、「AC 検証者」は AC の保有者の PKC を見つけることができるが、サブジェクトの AC を見つける直接的な方法はない。

4 セクション 5 から: 「4. AC の発行者は、(設定またはその他の方法によって)AC の発行者として直接信用されなければならない(MUST) 。」

これは、IP アドレスブロックの使用権の場合には事実ではない。IP アドレスブロックは階層を通じて割り振られる。AC の証明書パス検証には、委任階層を上って連鎖をたどる必要がある。各依存者(NOC)が他のすべての NOC を「信用」するように設定しなければならないことは適切ではなく、このような「信用」は、提案されたセキュリティメカニズムが回避するように設計されている失敗に帰する。何千もの個々の信用される ISP ごとの AC の発行者ではなく、信頼されるルートを持つ単独の PKI が使用される。

AC を適切に検証するために必要な作業の量は、本文書で定義される証明書拡張領域

を PKC に置くメカニズムの場合よりも多い。AC に加えて、検証されるべき証明書は 2 倍になる。AC をサポートするために必要な管理負荷が著しく増加する可能性がある。

参考文献

引用規格

[IANA-AFI] http://www.iana.org/assignments/address-family-numbers.

[IANA-SAFI] http://www.iana.org/assignments/safi-namespace.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[X.690] ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, "Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

参考情報

[RFC791] Postel, J., "Internet Protocol -- DARPA Internet Program Protocol Specification", RFC 791, September 1981.

[RFC1142] D. Oran, Ed., "OSI IS-IS Intra-domain Routing Protocol", RFC 1142, February 1990.

[RFC1771] Rekhter, Y. and T. Li, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC2050] Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D. and J. Postel, "Internet Registry IP Allocation Guidelines", BCP 12, RFC 2050, November 1996.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[RFC3281] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[S-BGP] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," IEEE JSAC Special Issue on Network Security, April 2000.

執筆者の連絡先

Charles Lynn

BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3367
EMail: CLynn@BBN.Com

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3988
EMail: Kent@BBN.Com

Karen Seo
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3152
EMail: KSeo@BBN.Com

完全な著作権表示

知的所有権

IETF は、本文書で説明される技術の実装または使用に関連すると主張する知的財産権またはその他の権利の正当性または範囲または、そのような権利に基づくライセンスが利用できるまたはできない範囲に関して、特定の立場をとらない。また、IETF はそのような権利を特定するための独立した努力を行ったと主張するものでもない。RFC 文書内の権利に関する手続きについての情報は、BCP 78 および BCP 79 に見られる。

IETF 事務局に行われた IPR 開示、利用可能になったライセンスの保証、またはこのような所有権の一般的ライセンスまたは使用許可を得るために、本仕様の実施者またはユーザによって試みられた結果は、IETF オンライン IPR レポジトリ http://www.ietf.org/ipr で

入手することができます。

IETF は、本標準を実装するために必要になるかもしれない技術をカバーする可能性のある著作権、特許または特許申請、またはその他の所有権を、利害関係者が知らせることを推奨する。情報は IETF ietf-ipr@ietf.org に送信してください。

謝辞

RFC エディターの職務に関する財政援助は現在インターネットソサエティによって提供されている。