第3章 認証技術とセキュリティに関する国内外の動向

内容

- 技術の標準化動向と国内外での議論
  - IETF
    1. S-BGP の展開に関する議論
    2. 認証技術の実践的な議論
    3. 各回の報告
  - NANOG での話題
  - 国内での議論

第3章 認証技術とセキュリティに関する国内外の動向

3.1. はじめに

認証技術は様々な要素が組み合わった複合的な技術である。認証技術の導入にあたって検討されるべきことは色々と考えられるが、まず技術そのものと技術の運用という二つの大きな側面に分けられるであろう。技術の側面は様々な研究の情勢や国際会議での標準化動向、システム導入の技術検討といった活動がある。運用の側面は技術を利用する組織での運用や業界での運用、ミクロな視点では利用環境が挙げられる。それぞれの組織や業界に合った使い方をしなければ、認証技術はセキュリティの向上を図るどころか、意味のないものになってしまうだろう。

認証局はこの認証技術の二つの側面を考慮する必要がある。インターネットで使われているプロトコルで使われるような形式で証明書を発行できなければ、その証明書の普及はなく認証局の存在意味がなくなってしまう。更に目的とする電子認証に対して、妥当な組織によって認証局が運営されていなければ、ユーザの信頼を得ることが難しく電子認証のレベルの向上を図ることはできない。

本調査研究は NIR における認証局のマネジメントに関する調査研究である。従って NIR における技術と運用の両面に重点を置いた動向調査が必要である。JPNIC における電子認証の技術の要素は、プロトコルの標準化動向であり、運用の要素は他の認証局、特にインターネットレジストリの認証局の動向である。

3.2. 本章の内容

本章では、プロトコルの標準化動向として IETF [1]における認証技術の動向を、インターネットレジストリの認証局に関しては RIR における認証局の動向を中心に報告する。インターネットレジストリのセキュリティが大きく影響を持つグローバル・インターネットのネットワークセキュリティに関して、北米のネットワークオペレータの会議である NANOG から最新の話題について報告する。この他に日本国内における認証技術とネットワークセキュリティに関わる動向を報告する。インターネットレジストリの認証局に関しては、第 4 章でまとめている。

[1] Internet Engineering Task Force
http://www.ietf.org/

なお、ネットワークセキュリティにおける「運用」という言葉は、ネットワークオペレーション（ネットワーク機器等の運用）を指すことがある。本調査研究では基本的に認証技術の運用（認証局や認証サービスの運用）を指すこととする。

3.3. 認証技術(PKI)とネットワークセキュリティに関わる国内外の動向

認証技術で使われている要素技術の多くは、国際的な学術会議（カンファレンス）とオペレータの知見を通じて発展してきた。またインターネットにおける通信の基本となるプロトコルである IP を始め、アプリケーションのプロトコルに至る多くの技術は、国際的な標準化活動の成果でもある。

RFC の公開を行っている IETF は標準化活動のよい例であろう。PKI に関わる RFC である RFC3280、RFC3647、IPsec に関わる RFC2401、SSL/TLS の RFC2246 など、インターネットで使われている電子認証のプロトコルは必ずといっていいほど IETF の標準化プロセスを経ているのが現状である。

電子認証の技術的な最新動向を調査するには IETF のような国際会議の動向を調査するのが早道である。認証技術をはじめ、情報科学の技術は企業の研究所や大学で研究されることが多い。しかし実装されインターネットで本格的に利用されるようになるのは、標準化され文書化されたあとになる。従ってプロトコルの標準化を行うような国際会議は、インターネットで使われている、もしくは将来使われるようになる技術の最新動向を知るのに適している。IETF では、運用に関する知見の集約も早い段階で行われる。インターネットにおけるアドレス資源の管理がその代表的な活動であろう。

3.4. 国際会議について

本調査研究では国内外で開催される国際会議に参加し、直接的な情報交換を図った。

この調査について、ここでは三つの構成に分けて報告する。

一つ目は国際的なプロトコルの標準化と、グローバル・インターネットのオペレーション（技術的な管理運用）である。ここでは IETF と NANOG について述べ、インターネットの技術面と、ネットワーク運用面の動向について報告する。

二つ目は国内の認証技術の動向である。ここでは JNSA の PKI 相互運用技術 WG と WIDE Project にについて述べ、日本の認証技術の普及と技術的な課題について述べる。

三つ目は国内のネットワーク・オペレータの動向である。

ここでは JANOG と JPNIC の IRR 企画策定専門家チームについて述べ、日本のネットワークオペレータが議論を行っているネットワークの最新動向と、グローバル・インターネットにおける経路制御の安全性についての最新動向について述べる。

3.5. プロトコルの標準化とインターネット・セキュリティに関わる国際動向

IETF はインターネットで使われる各種プロトコルの標準化を行っているグループである。ISOC から資金援助を受けて活動しており、RFC と呼ばれる技術文書を公開している。議論の技術的なレベルが高く、文書化されたプロトコルの適用性が高い。従って参加費用はやや高額（約 55000 円）であるが、毎回 1300 名以上の参加者を確保している。参加者のうちの 50%以上がアメリカの企業や大学からの参加であるが、残りの 50%近くは日本、ドイツ、フランス、イギリス、韓国、といった様々な国の企業や大学からの参加者である。政府組織の技術者の参加も多い。

NANOG は北米地域のネットワークオペレータ（技術的な管理運用を行う担当者）を対象にした会議である。主に参加者同士の運用に関わる技術的な情報交換を目的としており、会議は発表形式である。参加者のほとんどがアメリカからで、2004 年 11 月に行われた第 32 回の参加者は 600 名程であった。日本からの参加者は 20 名程であった。

3.5.1. IETF における RIR の技術者との情報交換

IETF はプロトコルの標準化活動を行う会議である性質上、インターネットに関連するベンダ、政府組織等から技術者が一堂に集まる機会である。この機会を利用して、RIR における認証局の状況に関する情報交換を行ったり、JPNIC 認証局の応用技術に関する情報交換を行ったりした。IETF の動向の報告に先立ち、この個別の情報交換について述べる。

3.5.2. S-BGP の展開に関する情報交換

第 60 回および第 61 回 IETF における情報交換において特筆すべきことは、S-BGP に関することであろう。第 60 回 IETF において PKIX WG のドキュメントとして RFC3779 が I-D から RFC になっただけでなく、S-BGP の提案者や APNIC の職員と技術と運用に関する情報交換を行った。本節では、RFC3779 の意義について述べると共に得られた情報を元に今後予想される動きについて述べる。

グローバル・インターネットにおける経路制御のセキュリティは、経路情報が正しいのか、本来想定されたルータによって特定の経路情報が流されているか等の要素がある。その中でレジストリの登録情報に関連することは、経路情報交換における認証と、経路情報とアドレスの割り振り／割り当て情報との整合性である。

RFC3779 [2] は、X.509 形式の電子証明書に IP アドレスと AS 番号を含める拡張フィールドを定義している。この RFC は、拡張フィールドの定義や RIR の認可（authorization）の概念がまとめられたものであるが、このプロトコルの目指していることはグローバル・インターネットにおける経路制御のセキュリティに対して、PKI を用いたアプローチを行っていると言える。

RFC3779 の概要を以下に示す。

■RFC3779 の概要

Abstract

This document defines two X.509 v3 certificate extensions.　The first binds a list of IP address blocks, or prefixes, to the subject of a certificate.
The second binds a list of autonomous system identifiers to the subject of a certificate.
These extensions may be used to convey the authorization of the subject to use the IP addresses and autonomous system identifiers contained in the extensions.

RFC3779 の電子証明書の利用を想定している S-BGP は、1980 年代より研究が進んでいたプロトコルであったが、2001 年以降、アドレス資源の割り当てを行うインターネットレジストリで認証局が立ち上がり始めたことで、やっと普及の方法を検討できる段階になった。

S-BGP とグローバル・インターネットにおけるセキュリティについては、RPSEC WG [3] でドキュメント化の活動が進んでいる。グローバル・インターネットで経路情報の交換に使われている BGP のセキュリティにとって、AS パスの正しさが大きな意味を持つ。経路情報はルータ間をバケツリレー方式で転送されるため、集約やフィルタを行いやすくネットワークを拡張しやすい。しかし同時に情報が間違っていてもその間違いがどこで起こったか特定することが難しい。従って、既知であるかもしくは正しいことが分かっている伝播順序 AS パスであるかどうか、または経路情報の出所が正しいの

[2] X.509 Extensions for IP Addresses and AS Identifiers
http://www.ietf.org/rfc/rfc3779.txt

[3] RPSEC WG
http://www.ietf.org/html.charters/rpsec-charter.html

か、といった判断が各ネットワークの管理者に必要になる。

RPSEC WG のメーリングリストでは、改めて経路の安全性の要件をまとめなおしており、今後のバックボーン・インターネットにおける安全性の確保の仕方、ひいてはインターネットレジストリの業務のあり方に影響してくると考えられている。

なお、第 60 回 IETF では RFC3779 で言及されているインターネットレジストリの重要性や、IP アドレス認証局の応用に位置づけられる点等について S-BGP の提案者と意見交換を行った。

この情報交換でわかったことは、既に APNIC CA において検討が進められており、次回の APNIC ミーティングにおいて RFC3779 に関するミーティングが予定されていることであった。RIR における運用面の検討がまさに始められた状況と言える。

また電子証明書の適用手法について興味深い意見があった。はじめに認証用の証明書を運用し、次に登録情報を証明する証明書を運用する手法がよいとのことである。これは当センターにおける IP アドレス認証局の適用方法と同じである。レジストリにおける登録情報のセキュリティは、登録、公開の行為におけるセキュリティ機構を整備することによって一連の業務の安全性が向上すると考えている。まず登録時の認証強化を行い、暗号技術を使った強い認証のもとに登録された情報を証明（authorization の証明）していくという順序になる。

なお、JPNIC の IP アドレス認証局は、前者の認証を IP アドレス認証局(認証)が、後者の証明を IP アドレス認証局(証明)がそれぞれ役割を担うとしている。

3.5.3. APNIC CA における RFC3779 に関する検討

第 61 回 IETF のセッション後に APNIC CA の運用を行っている担当者と意見交換を行った。ここでおこなった意見交換では技術と運用の両面が話題になった。

技術面の話題は RFC3779 に則った証明書の発行が可能な環境についてである。APNIC ではオープンソースソフトウェアを使った認証局のシステムを運用しており、この対応の為の改良を行っているようであった。JPNIC の IP アドレス認証局は RFC3779 に対応した証明書を GUI（Graphical User Interface）を使って発行することができる。これは割り振り、割り当ての証明を行うことができる点で、意味的にレジストリ業務の安全性向上を望むことができるが、しかし技術的な観点では、アプリケーションの整備が必要であり、今後の大きな課題である。

また割り振り／割り当て業務との連携が必要となる。

運用面の課題は、共有プール化に伴うアドレスブロックの証明性である。アジア太平洋地域の NIR において、割り振りの為のアドレスブロック（プール）は共有プールと呼ばれる。これは APNIC が管理するプールとして扱われるため、アジア太平洋地域の

NIR は自らが管理するプールを予め固定的に持つことがない。

これは、全体的にアドレスブロックの連続的な割り振りをしやすくする効果があると同時に、各 NIR の立場では割り振り行為自体の正当性を保障することが難しい状況であると考えられる。

RFC3779 に準拠した証明書は各レジストリの割り振りを証明する意味を持つため、共有プールから割り振りを行っている NIR にとってこの証明書の発行業務はどれほどの保障性を持つのかが判断しにくい。なお DNS サーバの登録権限が NIR にあることで、運用上の正当性は NIR が管理する状況ではある。

一方ユーザネットワークの立場ではアドレスの一意性だけでなく、割り振り／割り当て情報、連絡先情報の維持がレジストリに期待される。その直接のやりとりのある NIR は、ユーザネットワークと LIR にとってのアドレス管理業務における信頼点である。今後 RFC3779 の証明書を使うアプリケーションが現れるに従って、信頼点の置き方を含めて適切な運用方法を検討していく必要があるであろう。

APNIC 担当者は APNIC における発行に意欲を示しているが、割り振りと整合性を持った証明書を適切な信頼点をもって運用できるか、など認証技術の運用に関しては今後の課題になると思われる。

3.5.4. IETF における認証技術の実践的な議論

近年の IETF において標準化活動の対象となっている認証技術は、Kerberos と PKI である。Kerberos は元々MIT Athena Project [4] で開発されたものだが RFC1510 が出されたり、スウェーデン王立技術研究所(KTH)で eBones を元に作られた Heimdal が配布されて以降、IETF KRB-WG を中心に多くの技術者によって拡張がなされている。一方 PKI は、W3C における XML 署名に関連する標準化 [5]、OASIS における PKI TC [6] といった活動はあるものの、IETF PKIX WG における標準化活動が最も先行しており、またその為に議論の結果の影響は大きい。

しかし IETF PKIX WG は PKI における証明書の書式と適切な処理に注目した WG であり、アプリケーションにおける適用を目的とした議論を行う WG ではない [7]。

---

[4] Kerberos: The Network Authentication Protocol
http://web.mit.edu/kerberos/

[5] W3C Technical Reports and Publications
http://www.w3c.org/TR/

[6] OASIS Public Key Infrastructure (PKI) TC
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pki

[7] Public-Key Infrastructure (X.509) (pkix) Charter

本調査研究の期間に参加したここ二年間の IETF PKIX WG の活動は、クローズ（WG の終了）に向けた活動を行っており、新たな話題が WG のトピックに入ることに対してとても慎重になっている。これまでは PKI を適用したアプリケーションに関する議論は PKIX WG で議論することができた状況であるが、今後はますます難しくなるであろう。

IETF に参加している日本の PKI の専門家の中には、影響力の大きい IETF PKIX WG の中で今後実用的な議論がしにくくなると、標準化された技術に基づく適用の議論をする場が少なくなるという状況に危機感を持っている人が多い。PKI を利用するアプリケーションには、https を使う World Wide Web やグループウェア、Windows におけるログオン等が現れているものの、依然限られている状況がある。

同様の危機感は日本の PKI の専門家だけでなく、IETF 参加者の多くにも共通しており第 60 回 IETF の SAAG(Open Security Area Directorate) のセッション [8]でも議論が行われていた。第 60 回 IETF の SAAG では、会場から認証技術と deployment（利用・展開）に関して次のような議論が起こっている。

- PKI の deployment
  PKI の deployment について、広範囲で、かつ工学的な取り組みが必要である。その為には組織的な導入活動が必要である。
- 認証の仕組みの透過性
  ネットワークにアクセスする仕組みとの透過的な関連性が必要である。

PKIX WG が、新たな実践面での話題を扱いにくくなっており、ネットワーク・プロトコルでの認証技術の利用といった実践的な話題を扱う場が、より多く必要になっている状況がうかがわれた。

この他に、各参加者より下のような意見が挙がっていた。

第 60 回 IETF SAAG で各参加者から出された意見

- 組織的な意図は複雑だが、一斉の導入はやっている事例がある。
- BCP(Best Current Practice)を出すべき。

IETF では他に EasyCert [9] というグループが作られて議論されているが、これまでに具体的な利用に向けた対策は挙がってきていない。

---

http://www.ietf.org/html.charters/pkix-charter.html

[8] 61th SAAG minutes
http://www1.ietf.org/proceedings_new/04nov/saag.html

[9] Easy-to-User Certificate
http://www1.ietf.org/proceedings_new/04nov/easycert.html

第 61 回 IETF の EasyCert BoF では、成功している事例から今後 IETF においてどのような活動ができるのかを見出すという主旨で、事例紹介が行われた。

この BoF の主旨は、PKI の成功した導入事例から使いやすい要素を洗い出し、IETF としてできる活動を明らかにする、というものである。

いずれの事例紹介でも話題になったのは、失効方法（CRL を使っているか）と証明書管理モデルの妥当性である。

これらの事例紹介に対し、会場から出る意見は多く、活発に議論が行なわれた。しかし IETF でできる活動の方向性を見出すまでの議論には発展しなかった。

今後はより多くの事例を集め、PKI のガイドブックとなる Informational RFC を作ることを目指す、ということになったが、IETF 参加者の中で利用性に関する意見をあげる人が多いことから、今後もこの認証技術の実践に関する議論が行われることが予想される。

以降、2004 年度に参加した IETF ごとにまとめる。

3.6. 第 60 回 IETF

調査研究の一環として参加した第 60 回 IETF について報告する。

■会議の概要

2004 年 8 月 1 日(日)～2004 年 8 月 6 日(金)、アメリカ合衆国のカリフォルニア州・サンディエゴにある Sheraton San Diego Hotel & Marina で第 60 回 IETF が開かれた。

IETF チェアの発表によると、今回の IETF における参加登録の人数は 1511 名(8 月 4 日現在)だったようである。第 59 回(韓国・ソウルにて開催)の 1255 名、第 58 回(アメリカ・ミネアポリスにて開催)の 1233 名、第 57 回(オーストリア・ウィーンにて開催)の 1304 名に比べて増加している。参加者の国籍は、最も参加人数が多かったのはアメリカで、次いで日本、韓国、ドイツ、フランスと続いていた。合計で 40 ヶ国からの参加があった。

今回の IETF では、120 以上のセッションが開かれ、その中で 11 の BoF が開かれた。前回と同様に、Plenary(全体会議)は IETF Business Meeting と IETF Planning Meeting の二つに分かれて行われた。

■IETF Business Meeting

IETF Bussiness Meeting では、今回の IETF でのネットワークに関する報告、RFC Editor からの報告、IANA による報告、IESG による報告、IESG のプロセスチーム

(PROTO)の紹介、WSIS における議論の紹介、IAB からの報告が行われた。

RFC Editor からの報告では、2004 年 4 月 7 日は RFC1 が発行されてから丁度 35 周年であることや、RFC2223 の記述に代わる新たな著作権表示と知的所有権に関するアナウンスがあった。下記の Web ページにまとめられている。

RFC Copyrights
http://www.rfc-editor.org/copyright.html

IESG からは PROTO チームに関する報告があった。PROTO チームとは、AD（エリアディレクター）のドキュメントプロセスの一部を担うグループで、2004 年 1 月に結成されている。PROTO チームに関する詳細は下記の Web ページにまとめられている。

IESG Process and Tools (PROTO) Team
http://www.mip4.org/proto/
WSIS：http://www.nic.ad.jp/ja/tech/glos-kz.html#03-wsis
IAB：http://www.nic.ad.jp/ja/tech/glos-ij.html#02-IAB

■IETF Planning Meeting

IETF Planning Meeting では、IRTF[10]の ASRG[11]から SPAM の現状と対策に関するプレゼンテーションと、IAB による Security workshop に関する報告、IETF の新たなドキュメント体制チームのステータスレポート、IETF の管理組織に関するステータスレポートが行われた。

ASRG のプレゼンテーションでは、SPAM メールが、必要なメールよりも多く配送されている現状や対策、関連するプロトコルの標準化活動を行っている MARID WG[12]の紹介が行われた。

IAB の Security workshop に関する報告では、CERT に報告されるインシデント数の増加や金銭や規模といった脅威の変化、SSH や VPN といった技術の適用場面の特徴、Peer-to-Peer のセキュリティや DDoS、フィッシング（銀行などの Web サーバと似たような発信元（ドメイン名）のメールを使った詐欺行為）といった未対策の分野の遍歴などが紹介された。

---

[10] IRTF：http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section3.html
[11] ASRG：Anti-Spam Research Group　http://asrg.sp.am/
[12] MARID WG：MTA AuthorizationRecords in DNS WG
MARID WG はライセンスと他技術に関する議論の結果、クローズとなった。

IETF の新たなドキュメント体制チームについては、General AD の Harald Alvestrand 氏よりステータスレポートが行われた。第 59 回 IETF の頃から始まった、ドキュメント化プロセスの効率化は ICAR[13]、NEWTRK[14]、PROTO、EDU といったチーム（一部 WG）によって進められており、それぞれの人数や活動内容のドキュメント化が進んでいるといった報告が行われた。

最後に IETF の運用組織（Administrative Group）に関して、ドキュメント化が進行中である旨の報告、コンサルタントの Carl Malamud 氏の紹介、Administrative Group がどのように ISOC[15]と関連していくかについてのプレゼンテーションが行われた。

■認証技術と PKI に関連する WG 活動

■PKIX（Public-Key Infrastructure (X.509)）WG[16]

PKIX WG は 8 月 4 日(水)の午前に行われた。参加者は 100 名ほどで、前回の約 50 名から比べると大幅に増えている。ただし各ドキュメントに特化した議論がほとんどであるためか、途中退席される方が見受けられた。

PKIX WG は第 57 回 IETF 以降終息に向け、既存のトピックのドキュメント化を中心に議論を進めている。最初にドキュメントステータスの発表が行われた。前回の IETF 以降から今回の IETF までに、下記の RFC が発行された。

RFC 3739　"Qualified Certificates Profile"
RFC 3770　"Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN"
RFC 3779　"X.509 Extensions for IP Addresses and AS Identiers"
RFC 3820　"Internet X.500 Public Key Infrastructure Proxy Certificate Profile"

この他に四つの Internet-Draft（以下、I-D）が IESG に承認され、10 の I-D が AD または WG のレビュー中の状態である。

次に、提案された WG のマイルストーンが提示された。このスケジュールによると 2005 年の春までに、RFC3279 と RFC3280 の更新、テキスト文字列の処理、OCSPv2

[13] ICAR：Improved Cross-Area Review
[14] NEWTRK：New IETF Standards Track Discussion
http://www.ietf.org/html.charters/newtrk-charter.html
[15] ISOC：http://www.nic.ad.jp/ja/tech/glos-ij.html#02-ISOC
[16] PKIX WG
http://www.ietf.org/html.charters/pkix-charter.html

の拡張に関する活動を完了する予定になっている。

続いて、ドラフト・ドキュメントに関する議論が行われた。今回の議論では LDAP[17] 関連、文字列比較ルール、RFC3280 の更新、証明書検証プロトコルの SCVP といった話題があった。

LDAP に関しては、LDAP スキーマとエントリの記述方法に関するプレゼンテーションがあった。LDAP スキーマは、エントリの DIT（Directory Index Tree）構造と OpenLDAP（http://www.openldap.org）バージョン 2.2.1 に設定が含まれていることが発表されていた。正式に組み込まれるのは OpenLDAP 側のレビューの後であるとのことである。

文字列比較ルールについては、UTF8String といった文字データの種別の違いを超えた比較ルールの必要性や DC コンポーネントに対するルールなど、既存のルールとの使い分けなどについて議論が行われていた。

最後に、恒例のリエゾンによるプレゼンテーションとして、韓国の KISA（Korea Information Security Agency）の研究員から PKI の為のユーザインターフェースの要件に関するプレゼンテーションと、IKEv2（Internet Key Exchange version 2）から OCSP（Online Certificate Status Protocol）を効率よく利用するためのメッセージ交換方法について Mike Myers 氏によるプレゼンテーションが行われた。

■PKI4IPSEC（Profiling Use of PKI in IPSEC）WG

2004 年 5 月に、IKE で使われる証明書プロファイルに関する提案 draft-ietf-ipsec-pki-profile-04 が、WG で扱われるドキュメントの位置づけになり、draft-ietf-pki4ipsec-ikecert-profile-00 に改訂され、さらに-01 に更新された。そのため、多くの変更点がプレゼンテーションされた。

変更があった点は、IKE における IP アドレスペイロードの書式と検証方針、一度検証された証明書の扱いや、CERTREQ ペイロードに含めていた識別名（DN）が鍵情報になるなど、多岐にわたっている。また-00 から-01 での更新では、証明書の鍵用途拡張のフィールドがある場合の解釈方法や、認証局が拡張の鍵用途拡張フィールドを加えないなど、PKIX WG の仕様を深く解釈したうえでの提案がなされていた。

また証明書管理の要求事項をまとめた draft-bonatti-pki4ipsec-profile-reqts-01 を PKI4IPSEC WG で扱うことになり、今後、議論が進められるようである。

■MASS（Message Authentication Signature Standards）BoF

MASS BoF は、8 月 5 日(木)の午前に開かれた。定員 100 名弱の部屋には入りきれないほどの人数が参加したため、大きな部屋に移動して行われるという一幕があった。

[17] LDAP：http://www.nic.ad.jp/ja/tech/glos-kz.html#03-ldap

MASS BoF で提案している WG は、MARID WG で扱っている認証用途の DNS レコードを利用して、メールメッセージを認証できるようにするという目的を持っている。SPAM 等のメールで使われるような著名なドメイン名と類似するドメイン名をかたった場合に、判別ができるという効果を狙っている。

この BoF では、WG のゴールやチャーターが始めに提示され、次に DomainKey と呼ばれる認証の為に使われる鍵の使い方や、DomainKey を使ったメールメッセージ、MTA signature と呼ばれる署名に関するプレゼンテーションがあった。

しかし、会場からはフィッシングにおいて根本的な解決にならない、S/MIME との違いは何か、といった厳しい意見が出された。

■SAAG （Open Security Area Directorate：セキュリティエリア全体会議）

今回の SAAG では認証技術の適用に関する議論が行われた。議事録を下記に示す。

SAAG Minutes, August 2004

There were working group and BoF reports from PERM, SASL, KRBWG, INCH, PKIX, SMIME, LTANS, MOBIKE, PKI4IPSEC, ENROLL, MSEC, KITTEN, ISMS, and MASS. See the individual WG's minutes for details.

Joe Touch gave a talk on Anonymous IPsec (draft-touch-anonsec-00.txt). (Slides attached.)

Jordi Palet spoke on IPv6 Distributed Security; again, see the slides. (draft-palet-v6ops-ipv6security-01.txt)

Ian Bryant proposed work on exploit reporting.

During the open mike session, the primary topic of discussion was the difficulty of using certificates and PKI. A mailing list was created (https://www.machshav.com/mailman/listinfo.cgi/easycert) for discussion of this topic; the aim is to work towards an EASYCERT BoF in Washington. The goal of that BoF is to explore what the IETF can do to help with that problem. During the SAAG meeting, we heard of some success stories. The hard parts seemed to be at the political layer; success came when there was an already-existing authentication infrastructure that could be leveraged to issue certificates.

（60th SAAG minutes）
http://www.ietf.org/proceedings/04aug/205.htm

IETF の SAAG では、会場から認証技術と deployment に関して以下のような議論が起こっていた。

- PKI の広範囲で工学的な deployment が必要。それには組織的な導入活動が必要。
- 認証の仕組みとネットワークアクセスのユーザにとっての透過的な関連の必要性。

PKIX WG が、新たな実践面でのトピックを扱いにくくなっており、ネットワーク・プロトコルでの認証技術の利用といった実践的な話題を扱う場が、より多く必要になっている状況がうかがわれた。

セッションの最後には、エリアディレクターより、次回の IETF で実践的なトピックを扱う BoF が開催されることが示唆された。今後、認証技術の deployment に関する議論は、注目を集めることが予想される。

3.7. 第 61 回 IETF

■概要

2004 年 11 月 7 日(日)～2004 年 11 月 12 日(金)、アメリカ合衆国のワシントン D.C. にある Hilton Washington ホテルで第 61 回 IETF が開催された。

第 61 回の参加登録は 26 ヶ国から 1314 名が行ない、前回よりも参加国数、登録人数共に少ない状況であった。しかし IETF チェアの発表資料によると日本からの参加者はアメリカに次いで多く、全参加者の一割以上を占めていたようである。参加者のうち 50%以上を占めるのはアメリカ、次いで日本、韓国、ドイツ、フランスの順とのことであった。国際的な技術標準化の活動の場でこれほど多くの日本人が参加していることは大変素晴らしいことである。

■プレナリー（全体会議）

今回の IETF では、通常二回に分けて行なわれる Plenary(全体会議)が一回にまとめて行なわれた。RFC の発行前の編集を行なっている RFC Editor からは、2001 年には月に 20 程度の文書の編集依頼が来ていたが、2003 年以降は平均 28 に増加していることや XML を使った原稿が増えていること、新しい Word 用のテンプレート[18]に対する

[18] RFC Templates and Info. (Joe Touch 氏のページの一部)
http://www.isi.edu/touch/tools/

コメントを募集していることなどが発表されていた。IANA からは、コード番号やパラメータといった IANA の判断が関連する Internet-Draft(以下、I-D)の状況を見られる Web ページの紹介があった。http://www.iana.org/reporting-and-stats/で見ることができる。

IESG からは AD(Area Director)による I-D の処理状況で、第 60 回までの増加傾向から一転し、第 60 回 IETF から第 61 回 IETF の間はドキュメントの処理(レビュー)依頼件数が減少したことなどが発表された。この統計は主に AD のレビューを支援する PROTO チーム[19] の評価のために取られているそうである。IAB からは第 60 回 IETF で説明があった IETF の運営構造の再編成[20] についての現状報告がありた。ISOC の活動として IAB や IESG をサポートし、また IETF 運営の費用管理を行なう、IASA(IETF Administrative Support Activity)モデルについての RFC(BCP)が作られるようである。

■認証と PKI に関連した WG と BoF

PKIX、BTNS BoF、EasyCert BoF について報告する。

■PKIX

第 61 回 IETF における PKIX WG は 11 月 10 日(水)の午後 1 時から行なわれた。参加者は 60 名程であった。はじめにドキュメントステータスの確認が行なわれた。今回の IETF までに、RFC3874 "A 224-bit One-way Hash Function: SHA-224"が発行された。

以下の三つの I-D は IESG によって承認され、RFC Editor の編集待ちの状態にある。
"Additional Algorithms and Identifiers for RSA Cryptography"
draft-ietf-pkix-rsa-pkalgs-03.txt
"Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)"
draft-ietf-pkix-rfc2510bis-09.txt
"Internet X.509 Public Key Infrastructure Permanent Identifier"
draft-ietf-pkix-pi-11.txt
Certification Path Building を始めとする 6 つの I-D が AD によるフォローかコメントを待っている状態である。SCVP の第 16 版は WG Last Call がかけられた。

---

[19] Workgroup Chair Document Shepherding
draft-ietf-proto-wgchair-doc-shepherding-01.txt

[20] IETF AdminRest Homepage
http://www.alvestrand.no/ietf/adminrest/

今回のセッションではSCVPの16版(draft-ietf-pkix-scvp-16.txt)、RFC3280の改良、CRL の発行者を特定するための拡張フィールド(AIA)、CRL の検証ルール、証明書とCRL を格納する LDAP のスキーマ、簡易版の OCSP、ECC アルゴリズム識別子など、多くのプレゼンテーションが行なわれた。ここでは大きな動きのあった、SCVP と CRL の拡張フィールドについて紹介する。

SCVP の 16 版は、CA 証明書のフルサポートを始め、15 版から様々な機能追加や文書の変更があった。基本的な記述作業は一段落したようで、あとは ASN.1 の記述が正しいかを確認することが指摘されていた。

CRL 発行者を特定する仕組みについては、前回の IETF 以降に ML で必要性が指摘されていた。今回の提案は認証局と鍵を特定できるよう、CRL の拡張フィールドである Authority Information Access を使うことである。新しい作業項目ではあるが、短いドキュメントなので気にせず ML に投稿しては、というアドバイスが出されていた。

リエゾンによるプレゼンテーションは、韓国 KISA の研究員の方によって"User Interface Requirements for PKIX"と題して行なわれた。証明書を扱う GUI の要件について紹介するため、SSL/TLS に加えてオンライン取引に使用するといったデモが行なわれた。

WGチェアのTim氏によると、LDAPスキーマ関連のドキュメントやRFC 3279/3280の改良は2005年の春までに完了させる予定だそうである。PKIX WG のクローズに向け、ラストスパートをかけている様子である。

■EasyCert BoF

EasyCert BoF は、前回の IETF のセキュリティエリア会議(SAAG)で挙がった"PKIの利用が広まらない状況を踏まえて実践的な議論を進めるべき"という指摘を受け、エリアディレクターの Steve Bellovin 氏、Russ Housley 氏がチェアとなって開かれた。180 名近い参加者がいて、会場の部屋は超満員となった。

この BoF の主旨は、PKI の成功した導入事例から使いやすい要素を洗い出し、IETFとしてできる活動を明らかにする、というものである。BoF では MIT の Jeffley Shiller 氏、Johnson&Johnson の Robert Stahl 氏によって 2 つの事例が紹介がされた。

MIT では、学生と教職員の認証に PKI を利用していて、Web のクライアント認証の為の証明書を発行しているそうである。CRL はあえて発行せず、アカウントの無効化はサーバアプリケーションで対応、Kerberos のアカウントと連携しているようである。

Johnson&Johnson は、職員の認証に利用しているようで、大規模な導入の事例として紹介されているようである。上長による承認を経て証明書が発行されるモデルを採用しており、ハードウェアトークンを利用しているとのことであった。また大規模な事例として、Robert 氏に続いて DoD（米国防総省）の方が口頭で DoD PKI の紹介を行っていた。

いずれの事例紹介でも話題になったのは、失効方法（CRL を使っているか）と証明書管理モデルの妥当性である。DoD を除くどの事例でも、証明書は基本的に認証用に用いており、CRL に頼らず、サービスシステム側で認証用のデータベースを持っていた。ちなみに DoD で発行している CRL は 40 メガバイトにもなるそうである。

これらの事例紹介に対し、会場から出る意見は多く、活発に議論が行なわれた。PKI を簡単にする観点については、ISP が証明書を発行してはどうか、PKI の導入スケールを下げて考えるべき、フォーマットが複雑なのが問題、といった意見が挙がった。IETF としてできる活動については、色々な場面で使えるような証明書発行のブートストラッピング（初期立ち上げ）のプロトコルを標準化してはどうか、アカウントを管理するデータベースの議論が必要なのでは、といった意見が出ていた。この他に認証時にどのクライアント証明書を使うべきなのか戸惑う、といった意見があり、TLS WG へのフィードバックになるといったコメントが返されていた。しかし IETF でできる活動の方向性を見出すまでの議論には発展しなかった。

今後はより多くの事例を集め、PKI のガイドブックとなる Informational RFC を作ることを目指す、ということになり、この作業は IAB の Eric 氏が担当することになった。

EasyCert は、ML での議論も平行して行なわれていた。EasyCert ML に関する情報は"Easycert -- Easy-to-Use Certificates"にてまとめられている。

■その他

今回の IETF のセキュリティエリア会議(SAAG)で、Steven Bellovin 氏がエリアディレクターを引退することが発表され、後任には MIT の Sam Hartman 氏が着任することになった。

IETF はプロトコルの標準化活動を行う団体であるが、議論の中で運用面／利用面の意見が重要なフィードバックとなる。特に PKI の議論に関して、利用経験のある日本の技術者や研究者が標準化活動に参加することで、RFC に知見を盛り込み、利用性向上を図る活動の牽引力になると考えられる。

3.8. NANOG

3.8.1. 概要

NANOG は「The North American Network Operator's Group」の略でバックボーン・ネットワークや企業ネットワークに関連する技術情報の普及や、協調運用のための議論や教育を目的とした会議である。米国の非営利団体である Merit Network 社により、会議が年に三回行われている。このミーティングは主に米国とカナダの ISP を対象としているが、1985 年に始まった NFS-NET の運用上の会議から派生した歴史を持ち、それゆえ実践的で専門的な技術に関する議論が行われることが多い。

本調査研究ではアドレス資源管理の安全性がルーティングや DNS の管理といった ISP やバックボーン・ネットワークの安全性に影響することを踏まえて、NANOG においてどのような話題が扱われているかの調査を行った。

2004 年 10 月 17 日～19 日に開かれた第 32 回 NANOG に参加したところ、"BGP Multihoming Techniques", "Options for Blackhole and Discard Routing", "ISP Security Toolkits"といったバックボーン・ネットワークのセキュリティに関するアジェンダが多く、ネットワークオペレータが可用性（availability）を含めたネットワークセキュリティに高い関心を持っていることが伺えた。

NANOG32 のアジェンダにある話題は大手 ISP にとって先進的な話題であり、日本の ISP においても十分に有用な内容である。日本におけるネットワークセキュリティに関するセミナーは数多いが、特にバックボーン・セキュリティに関して、NANOG32 のような実践的な技術的な知識共有の場は依然少ない状況である。日本でディペンダブル（依存可能な）・インターネットを目標とする活動が見られるように、インターネットのネットワーク運用の側面からの普及・啓発活動が今後ますます重要になると思われる。

NANOG に関する詳細は下記の Web ページを参照されたい。

About NANOG
http://www.nanog.org/about.html

3.8.2. 第 32 回 NANOG における話題

第 32 回 NANOG では、企業や ISP におけるバックボーン・ネットワークの安全性

に関する話題が多く扱われていた。第 32 回 NANOG のアジェンダの中で、ネットワークセキュリティに関するものについて述べる。

Sunday Tutorials
1:30 - 3:00　BGP Multihoming Techniques
1:30 - 3:00　Options for Blackhole and Discard Routing
3:00 - 3:30　Coffee break
3:30 - 5:00　BGP Multihoming Techniques (cont'd.)
3:30 - 5:00　Internet Number Resource Management and Administration
5:00 - 7:00　AOL WELCOME RECEPTION !
7:30 - 8:15　ISP Security Toolkits
7:30 - 9:00　IPv6 Deployment and Case Studies

2004 年 10 月 17 日(日)の初日に行われたチュートリアルの中では、"BGP Multihoming Techniques"、"Options for Blackhole and Discard Routing"、"ISP Security Toolkits"が特に関連するであろう。

"BGP Multihoming Techniques"は、インターネットにおける経路交換の上で複数の上流接続を持つための具体的な設定方法を解説したものである。複数の上流接続を持つことによって、一つの回線が使えなくなった場合でも他の回線にトラフィックを振り替えることができ、ネットワークの可用性を上げることができる。

"Options for Blackhole and Discard Routing"は、ネットワークの利用不能攻撃（DoS）に対してよく知られている Blackhole ルーティングと Discard ルーティングを活用するための話題である。ネットワークの利用不能攻撃は、大量のパケットを特定の相手の送信することによって回線容量やルータの処理能力を限界に近づけ、本来の利用を妨げる攻撃である。このチュートリアルでは Blackhole ルーティングや Discard ルーティングを活用して、利用不能攻撃を意図したパケットをできるだけ発信源に近い場所で遮ったり、自組織のコンピュータから利用不能攻撃のパケットが発生した場合に他組織に迷惑がかからないようにしたりする方法が解説されていた。

次に一般セッションについて述べる。一般セッションはチュートリアルと異なり、技術の解説など自由な形式で行われる。以下に一般セッションのアジェンダを示す。

Monday General Session(Grand Ballroom)

8:00-9:00 a.m. Continental Breakfast, Grand Ballroom Foyer
9:00 a.m. Welcome, Introductions
9:20 a.m. Good Engineering Practice as it Applies to Unlicensed Wireless Networks
10:05 a.m. 802.1X: Deployment Experiences and Obstacles to Widespread Adoption
10:35 a.m. BREAK
11:05 a.m. Extension of Multi-Service Networks Dave Siegel, Global Crossing
11:35 a.m. Network Design to Support Very High-Capacity Streaming and Caching Infrastructures
12:00 p.m. LUNCH (on your own)
2:00 p.m. Botnets John Kristoff, Northwestern University
2:45 p.m. What Will Stop Spam? Charles Stiles, AOL
3:05 p.m. Optical Switching, a Great Tool in Platform Migration at AMS-IX
3:35 p.m. BREAK
4:05 p.m. Research Forum
Sizing Router Buffers

Performing BGP Experiments on a Semi-Realistic Internet Environment
Guido Appenzeller, Stanford University

Monday Evening BOFs +
Key Signing Party

7:30 - 9 p.m. ISP Security and NSP-SEC BOF VII (Grand Ballroom)
9 - 9:30 p.m. PGP Key Signing Party
9 - 10:30 p.m. Optimizing Operational Input to ARIN: What Is Needed and How Do We Get It?

2004 年 10 月 18 日(月)と 19 日(火)は、一般セッションである。17 日(日)のチュートリアルと異なり、発表者だけでなく参加者がディスカッションに参加する形で行われる。

一般セッションの中で特に注目を集めていたのは"What Will Stop Spam?"である。第 60 回 IETF で話題となった、スパム・メールの転送を防止するために使われる

SenderID,SPF,DomainKeys を利用しても防ぎきれない状況を解説し、今後どのような技術によってスパム・メールを減らすことができるのか、という議論であった。しかしまだ具体的な方策を見出すことは難しく、別途議論の場を設けて検討を進めていく、という段階である様子であった。

NANOG ミーティングにおけるセキュリティの話題

NANOG ミーティングのこれまでのアジェンダを見ても、今回は特にバックボーン・ネットワークのセキュリティに関連する話題が多い。1990 年代後半から 2001 年年頃は、インターネットでの不正アクセス行為に対しては、ファイアウォールが一定の効果を上げていると考えられていた。しかし近年の不正アクセスはネットワークの内外から大量のトラフィックを送りつける使用不能攻撃であったり、ウィルスやスパム・メールを活用し内部から攻撃したりするものになりつつある。インターネットの家庭への普及が手伝って、これらの不正アクセスの対策は多様な側面を持ってきた。

NANOG ミーティングに参加していると、まずこのようなバックボーンとしてのインターネットのセキュリティに関する意見交換の場が、日本ではまだまだ限られているということを再認識した。日本はブロードバンド・ネットワークの一般家庭への普及が進んでいる世界でも有数の国であり、バックボーン・ネットワークのセキュリティは今後ますます重要になる。また家庭用のネットワークでありながらネットワークの回線容量が大きいことから、前述したネットワークの使用不能攻撃が甚大な被害を発生しうる。

インターネットはネットワーク同士が自律的に問題解決を行って運営されているネットワークの集合体である。その自律的な問題解決の為の相互連絡手段を提供している立場であるインターネットレジストリが、今後どのような役割を果たすべきなのか、オペレータとの意見交換を進めて行うことが必要になってくるであろう。

3.9. 認証技術に関わる国内動向

3.9.1. JNSA における調査研究と取り組み

日本ネットワークセキュリティ協会(JNSA)はネットワークセキュリティに関連するベンダ、システムインテグレータ、インターネットプロバイダといったベンダを中心に、ネットワークセキュリティの社会へのアピール、諸問題の解決といった活動を行う特定非営利活動法人（NPO）である。

政策部会、技術部会等の部会に分かれて活動しており、その内容は調査、実験、勉強会等多岐にわたっている。

JNSA 技術部会の PKI 相互運用技術 WG は、PKI の必要性のアピールと問題解決を目的としており、2004 年度は勉強目的で開催された。

これまでに行われた三回の勉強会では、IETF の標準化動向、運用技術、法制度の三つが主な話題であった。

JNSA の勉強会の議論のテーマとして挙げられるキーワードは「マルチドメイン PKI」「ミドルウェア」「PKI の知見蓄積」であろう。

「マルチドメイン PKI」は JNSA の勉強会の中で中心的な考え方である。IETF の PKIX WG は PKI のフォーマットや証明書の処理方法といった、基本的な技術を対象としている WG である。「マルチドメイン PKI」は現実社会の複数の認証のドメイン（範囲）が存在する環境に、電子的な認証を導入するのに適しているモデルであると考えられている。

「ミドルウェア」と「PKI の知見蓄積」は、普及の段階の議論の中で互いに近い関係している。IETF PKIX WG で進められているような証明書の処理方法だけでなく、運用に必要となる技術（運用技術）の議論を進めることで、認証技術の知見蓄積を進めるという考え方である。ミドルウェアとして捉えることで、アプリケーション開発や基盤機能構築が容易になる状況を想定している。このミドルウェアの概念を図示したものが次頁の表 * である。

法制度については e-文書法の議論が多かった。アプリケーションの課題や電子文書の継続性の課題などが主な話題である。

＊ ミドルウェアの二つの側面

	技術	運用
上位層	アプリケーション	制度、業務形態に合った運用
中間層	セキュリティ ミドルウェア（API）	セキュリティ・インフラの運用
下位層	ネットワーク等の インフラ、API	セキュリティ以外の基本機能

セキュリティ・ミドルウェア(API)の取り組みによって、アプリケーションに対する複雑なセキュリティの要求を吸収し、より簡単で安全なアプリケーションの開発が期待できる。一方、運用面のセキュリティ・インフラは、未開拓の領域である。

本調査研究の IP アドレス認証局は、セキュリティ・インフラの運用に対する取り組みと言える。第 2 回の会合で IP アドレス認証局に関する発表の時間を頂いたところ、様々な方面から意見を頂くことができた。

第 2 回 PKI 相互運用技術 WG で頂いた IP アドレス認証局の応用に関する意見

- IP アドレスに地域の属性を関連づけ、リージョンコードや ISP の識別、地域網の構築が可能になるのではないか。
- AS 番号の証明書を発行することでネットワークの単位で相互の認証ができるようになる。
- POS システムで IP アドレスを利用し、各店舗の無線 POS の一元管理に利用することはできないか。
- IP トレースバックの際に参照するルータの証明書
- IP アドレスに関連づいた情報を使った動的なフィルタ

また進め方として「漠然と利用可能性を挙げるのではなく何をどう認証するのかを考えるべきである。ISP 等のサービスプロバイダを含めた議論が必要ではないか」という意見を頂いた。

前年度の調査研究では IP アドレス認証局の応用可能性を調査したが、今後の構想を念頭に置いた活動には、認証対象や運用方法といった、具体的な検討を行っていく必要があると考えられる。

3.10. JANOG

JANOG(JApan Network Opetators' Group)はインターネットの技術的事項やオペレーションに関する議論、検討、紹介等を行っているグループである。参加は自由に行うことができ、通常はメーリングリストを使った情報交換を行い、一年に三回程度ミーティングを行っている。運営委員会が設置されて運営されているが、インターネットに接続されるバックボーン・ネットワークの運用を有志で行ってきた人の集まりといった、技術者特有のフランクな雰囲気を持つグループである。

IRS(Interdomain Routing Security Workshop)は JANOG のメーリングリストで呼びかけられ、開催された中規模の会議である。IRS も有志によって開催された。

2004 年 7 月 7 日に行われた IRS では下記のアジェンダで情報交換が行われた。

IRS のアジェンダ（http://www.bugest.net/irs/docs_20040707/ より）

- Interdomain Routing Security(IRS) とは？
- IRS の動向
  Control Plane　　---　GTSM、BTSH ほか
  （Forwarding Plane　---　ACL、RPF ほか）
  （Management Plane　---　AAA、Management Port Separation ほか）
  soBGP の motivation と Implementation/Deployment 想定
- TCP Vulnerability 対策について

IRS では経路情報交換における認証だけに注目しているわけではないが、7 月 7 日以降、JANOG のメンバの間では BGP において認証の強化を行った soBGP、S-BGP の議論が活発に行われた。

日本のインターネット・バックボーンの強化を考えると、経路情報の交換のセキュリティは大きな課題である。現在は各 ISP の自助努力によってネットワークの安定性／安全性の確保が図られているが、日本のインターネット全体の安定性／安全性向上の為には、ISP の間でセキュリティの整備が進めることが必要になると考えられる。

今回の IRS でアジェンダにあがった手法が普及していく場合、認証は何を元にして行うかといった、セキュリティの運用の重要性が増してくると考えられる。

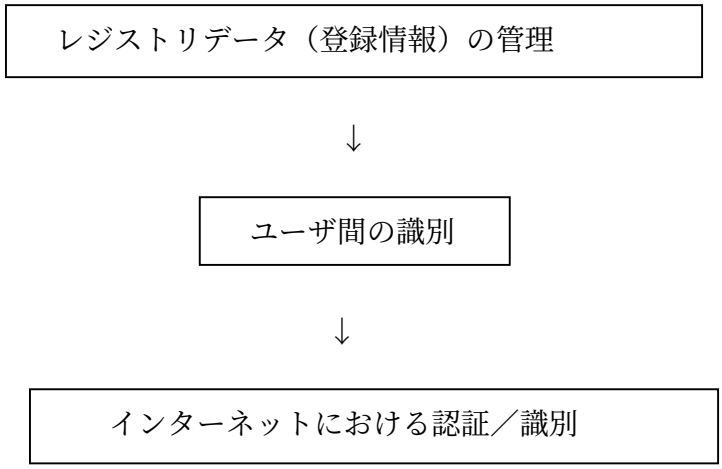
その中で、アドレス資源の管理を行うインターネットレジストリの役割は大きな意味を持つであろう。

3.11. IP アドレス認証局の技術的検討の方向性

IP アドレス認証局は、アドレス資源の登録に関わる認証強化と登録情報の証明の役割を持つが、国内外の技術動向を調査研究するに従って、その意味と技術的な検討の方向性が具体化してきた。

インターネットレジストリが管理しているレジストリデータは、ネットワーク利用組織の IP アドレスと AS 番号の台帳と考えることができる。インターネットに接続しているネットワーク利用組織は、IP アドレスで通信相手を識別する。認証を行う際にもドメイン名だけではなく IP アドレスに変換した結果を元に通信相手を調査するといったこともおこなわれている。

つまりインターネットレジストリは、レジストリデータの情報登録と公開を通じて、ユーザ間の識別手段を提供しているのである(下図)。



IP アドレスを用いた「インターネットにおける認証／識別」は、ユーザ・インターフェースに現れる「認証／識別」ではないが（一般的にユーザに覚えやすいドメイン名が使われるであろう)、DNS で調べることができるドメイン名と異なり、経路制御に直接影響している。これは IP アドレスを成りすますと、即座に通信相手や本来の IP アドレスを持つネットワーク・インターフェースが到達不能になり、成りすましたまま通信を行うことが困難であったり、すぐに気づかれてしまったりする性質がある。

将来的に、BGP における認証をはじめ、逆引きネームサーバを使ったメールサーバの識別（スパムの防止)、通信相手のネットワークの識別、ISP の識別といった、重要な識別にレジストリデータが使われることを想定することができる。

インターネットレジストリは、登録情報である IP アドレスや AS 番号をユーザ間の認証に使えるような技術的検討を進めることで、インターネットの安定性／安全性の向上に資することが可能であると考えられる。

3.12. JPNIC IRR 企画策定専門家チーム

前章で述べたインターネットレジストリの登録情報の応用例として、IRR(Internet Routing Registry)が挙げられる。whois と同様にコマンドラインや Web で登録情報を検索するインターフェースが実装されている。IRR は、経路情報に関する情報の登録・公開機能であり、インターネット・バックボーンに接続されるルータの管理者によって利用されることが想定されている。

JPNIC では IRR 企画策定専門家チームを通じて、IRR のサービスをより広範囲で利用性、安全性の高い機能に高める検討が進められている。広範囲とは RIR の IRR との連携によって、世界中の経路情報の登録情報を検索できることを意味する。この連携はミラーと呼ばれデータを交換する機構を使って行われる。

利便性については IRR に登録された情報をルータの設定に反映したり、経路情報の齟齬を検出することができたりする為の研究や調査が行われている。

広範囲でかつ利便性の高い経路情報の登録情報を提供することで、ユーザネットワークを収容しバックボーンに接続するルータが、インターネット全体に対して矛盾なく経路情報の交換ができる状況を実現することが可能になる。

JPNIC の IRR 企画策定専門家チームでは 2004 年度からセキュリティに関する調査が本格化し、認証局を用いた安全性向上、AS 間のメッセージ認証、IRR の提供情報の信頼性向上などが検討されている。詳細は本報告書第 7 章にて述べる。

3.13. 認証技術(PKI)の動向から見た適切な普及の課題について

PKI は IP アドレス認証局の中心的な役割を果たす技術である。IETF における PKI の標準化活動は現在も続いており、また Mozilla や Internet Explorer をはじめ多くのプログラムは PKI の一部しか実装していないという現状がある。PKI の実用化自体が課題となっている IETF SAAG における議論に見られるように、この状況の要因として利用／運用のための知見が十分に揃っていないことが挙げられる。普及が進まないために利用の知見が蓄積されにくいという悪循環の状況なのである。

JNSA 等の国内での多くの議論の中では、この悪循環を打開する方法は二つの方針があると考えられている。一つは簡単に認証技術を使える状況、つまりユーザが認証技術自体を意識することなく利用している状況を目指すという強制的な普及の方法である。もう一つ既存の制度の中に認証技術を取り入れ、現行業務の安全性向上を目指す方法である。前者は Mozilla や Internet Explorer、Opera といった Web ブラウザが SSL や証明書処理の機能を持つことに見られるように、技術の普及が進んでいると見ることができる。一方、後者は各業界における業務との折り合いが必要であり、現在は進んでいない。個人情報保護のために電子認証技術を採用する動きがあるのは後者の手法に分類されるであろう。

今後、認証技術の適切な普及は、既存の制度に対して適合する形で認証技術を適用していくことが肝要であると考える。国内における「認証」という行為は、各事業や業務における信頼点（事務局や執行役員、企業における代表など）の元に行われていると考えられるであろう。これをインターネットを使った電子認証に落とし込むに当たって、Web ブラウザに組み込まれた認証局証明書が適切かどうか、検討を要するであろう。

本調査研究はその検討の一つの事例として考えられる。本調査研究はインターネットレジストリにおける認証局に関する調査研究であるが、本質的には認証技術をアドレス資源管理の業界でどのように適用していくか、という点が主題となった。前年度の調査研究の結果、レジストリにおける認証業務に適合するモデルは外部に登録主体を持つモデルとなった。これはレジストリ内での認証局と IP 業務部分の分離、外部 RA（Registration Authority）を用いた IP 指定事業者自身による証明書管理という、既存の IP 業務との親和性を意識したものである。またレジストリにおける認証局は、RIR との相互連携を視野に入れておかねばならない。また今後実施されていくと考えられるバックボーン・ネットワークのセキュリティの為に、最新の技術を使った証明書の扱いを検討する必要があった。