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。

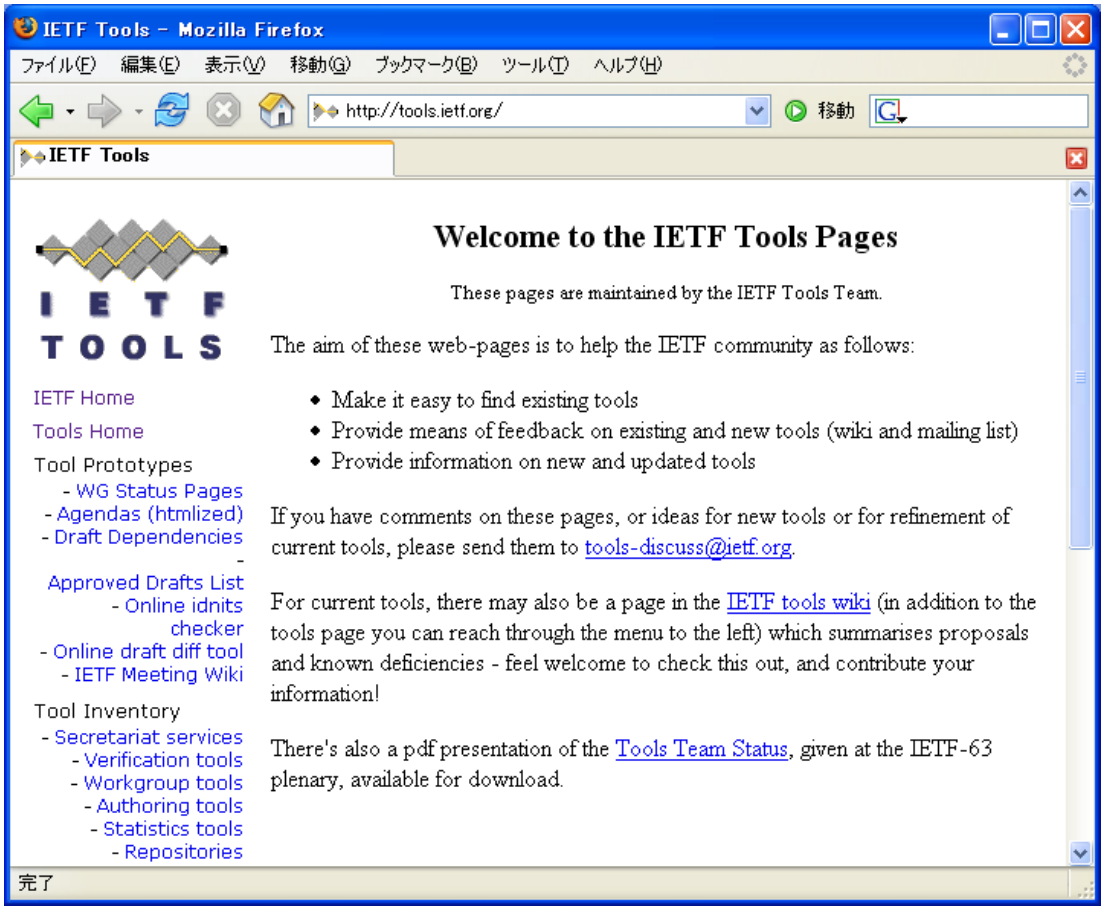
◆Operations and Administration Plenary

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