第59回IETFミーティング参加報告

JNSA研究員　安田　直義

2004年2月29日～3月5日に韓国 ソウル Lotte Hotelにて開催された第59回IETF(Internet Engineering Task Force: http://www.ietf.org/)に、ChallengePKI活動の一環として参加した。IETFは、インターネット上のプロトコルをはじめとする技術標準について議論し決める団体だが、JNSAのChallengePKIでは、2002年7月の横浜で開催された第54回IETF以来参加している。
今回の第59回IETFへの参加は次のような目的を持っていた。

1. 日本より提案しているInternet-Draftである Multi Domain PKI(セコムトラストネット 島岡氏著)の扱いを調整
2. 証明書のUTF8Stringに関しての議論に参加

セコム株式会社 IS研究所
松本　泰、　石垣　陽

セコムトラストネット株式会社
島岡　政基

富士ゼロックス株式会社
稲田　龍、横田　智文、益井　隆徳

NPO 日本ネットワークセキュリティ協会
安田　直義

ソウル Lotte Hotel

概観

IETFでは活動を8つのエリアに分け、各々のエリアにArea Directorを設け、Area Directorの統括の元にWGでの標準化活動を行っている。通常の標準化活動はメールベースで行われるが、年に3回、実際に顔をあわせるオフラインの会議が行われている。この会議は、2回は米国内、1回は米国外で行われる習慣となっているが、今回の韓国での開催は、2002年の第54回横浜に続きアジアでの2回目の開催になる。

今回のIETFのホストにはKorea TelecomとSamsungがなり、協賛としてTIA、ANF、ETRI、KIPA、KISA(Korean Information Security Agency)、KISTI、KRNIC、NCAOSIAなど韓国の官民両サイドでのバックアップがなされていた。また今回、初めての試みとして、IETFに併設してIPv6 Demonstrationが行われていた。

第59回IETFミーティングの参加者は、32カ国から総勢1,545人だった。今回は、韓国での初めての開催のせいか、やはり韓国人の参加が目立ち、参加国別の統計は事務局によると第一位 韓国人 45%、第二位 米国人 22%、第三位 日本人 10%とのことだった。

JNSAが中心となったChallengePKIの活動を中心にIETFを概観してみよう。

セキュリティ関連の活動

ここ数年、セキュリティの確保はインターネットにとり大きな課題となっており、各社は種々の対策/提案を行なってきた。IETFは、標準化を行なう立場で活動を行なっており、多くのプロトコルに関してセキュリティ面での強化を行なってきている。

ここ数年にわたり初日にはSecurity Tutorialが開催され、インターネット・プロトコルに対して必要とされるセキュリティ要件に関しての講義が行われている(後述)。Internet-Draft/RFCに関しては“Security Consideration”の項目が必須となるなどインターネットの標準化に関してセキュリティは必須の要件となっている。

JNSAのChallengePKIのグループも、月曜日の夜に、

PKIX-WGのChairであるSteve Kent氏、Jim Schaard氏と供にRussell Housley氏、Steven Bellovin氏と食事をし、PKIのモデルを今後どうIETFで扱うかに関してディスカッションをした。

PKI関係の活動

Steve Kent氏、Jim Schaard氏、Russell Housley氏、Steven Bellovin氏とのディスカッション

現在、ChallengePKIで作業しているGPKI/PKI関連の活動において、現行のIETFにおけるPKIの利用に関しての標準文書であるRFC 3280では十分ではない事が判明している。特に、PKIのドメインが複数あり、互いに相互認証する場合のモデルに関してきちんとした文書の整備が必要である事がわかっている。

この問題に関して、ChallengePKIグループではセコムトラストネットの島岡氏を中心にしてInternet-Draftsを作成しているが、これの扱いに関して前記のメンバおよびIPA 宮川氏、セコム株式会社 IS研究所 松本氏、JNSA 安田などを交えてディスカッションを行った。

当初、59th IETF開催前にPKIX-WG ChairであるNISTのTim Polk氏（今回は脊椎捻挫のため欠席）およびBBNのSteve Kent氏にInternetにおけるPKIのモデルの話であるのでPKIX-WGのWork Itemとして活動を行なえないかと打診をしてみた。両氏からは、PKIX-WGのミッションは標準化を行なうことであること、IESGよりPKIX-WGは、新たなWork Itemの追加を許されていない事を理由にPKIX-WGでの活動にすることは難しいとのコメントがあり、Security AreaのADであるRussell Housley/Steven Bellovinの両氏に相談すべきと助言された。Russell Housley/Steven Bellovin の両氏は、PKIのモデルに関する記述の不足を認め、Security Areaの新たなWGとして活動を行なう事を提案された。

Stephen Kent氏(左)、Steven Bellovin氏(中央)、Russell Housley氏(右)

左から稲田氏、Jim Schaard 氏、島岡氏、宮川氏(右)

WGの作成は、正道でありIETFにおいて標準化を行う際には必要となることである。IETFのルールでは、まず、BOFを最大3回おこない必要性が認められたらWGとすることになっている。最大3回のBOFにおいて必要性が認められない場合、そのアイテムはIETFで扱うべきものではないと認定されることになる。

ChallengePKIで、IETFの新しいWGを目指して活動するかどうか議論を行なったが、現時点では新たなWGを作ることは地理的、言語的にも荷が重く、できれば中心になって旗を振ってもらえる方がいないか検討して欲しいという希望を伝えるとともに、何らかの方法で個人的なI-DをRFCにすることはできないかを相談した。Russell Housley/Steven Bellovinの両氏は、個人としてRFCを発行することは可能であるが、IESGが認める事が必要であり、そのためにはきちんとした識者によるレビュが必須であるという要件が示され、レビュアとして適切な人間を数名上げていただいた。今回のIETFで行なわれた、OPSECも同様の立場にあるとのことだが、ChallengePKIとしては、この提案を受け、新たなWGを

作らず、識者によるレビュを受けてIESGにBCPとしてRFC化を目指す方針とした。

今後、2004年末にRFC化を目指して下記のような作業を行う予定である。

1. I-Dの改訂
2. PKIX-WGその他関係あるMLに対してアナウンス
3. 議論用のMLの立ち上げとアーカイブの開始
4. 平行して識者へのレビュ依頼
5. 60th IETFにおいてBOFの開催

Public-Key Infrastructure WG

3月1日に行われたPKIX-WGは、Co-Chairであるの NISTのTim Polk氏が脊椎捻挫のためBBNのStephen Kent氏により仕切られ、参加者は約50名程度だった。

WGのミーティングは通常通りにドキュメントステータスより始まり、粛々と議題をこなしていく進行で、議論としては若干低調ではあったが、内容としてはQualified CertificateのRFC化が進み、Proxy CertificateはRFC化が決まるなど多くの面で進展が見られた。それらの中からひとつだけ紹介しておこう。

Subject Identification Methodに関する問題

韓国のKISAのJongwook Park氏と米国NIST Tim Polk氏の連名での報告があった。韓国では既に国民に対して証明書を発行しており、米国も計画があるが、その際に証明書内に格納するプライバシー情報（住所、生年月日、性別、氏名など）をどう証明書内に表現するかが問題になっている。

韓国や米国はこの問題を重要なものとして捉え、特定の方式で暗号化した情報を記載することにより、適切な権限を持った利用者のみに情報が開示される方式を提案している。日本で展開されている公的個人認証サービスに関しても同様な問題を抱えており、日本の場合は、公的個人認証サービスの証明書を利用するのは官側のみと規定し問題がないとしているが、実際には民間でも広く使われそうなので、もっとよく考えなければならないだろう。広く官民で利用できるようにするためには証明書に記載されるプライバシー情報などを適切に扱える仕組みが必要なので、このアプローチは注目される。今回は、現在のI-Dのステータスの報告と、更なる修正が必要との報告が行なわれていた。

その他のセッション

New Comer's Training

2月29日の13:00-14:00に開催された、初めて参加する聴衆のためのガイダンス講座で、今回は初めての試みとして通常の英語でのセッションのほか、韓国語でのセッションも開催されていた。

英語でのセッションは、約120名が参加しIETFの概要と標準化の流れと基本的な考え方として“Rough consensus and running code”が説明された。一言で言えば、「細かなことは気にせず、動くものを（追認して）標準化する」ということであり、ITU-T/ISOなどとは異なる標準化ポリシーの元に「標準化」が進められていることが説明されている。IETFのこのスタンスが、インターネットの急速な発展とdog yearといわれる急速な変化に何とか追従している理由ともなっている。

Editor's Training

2月29日13:00-15:00に開催され、参加者は40名ほどであった。

Editor's Trainingは、Internet-Drafts/RFCを書く人に対してのセッションであり、RFC Editorがどのような観点で「編集」を行いIETFでの標準化文書が作られるかの過程の説明を行う。Editorとしての心得や、どのタイミングでRFC Editorに送るべきかなどが説明された。

Internet-Drafts/RFCを作成する面で役に立つツール類の紹介もあった。Internet-Drafts/RFCは、基本はnroffで作成されているが、XMLにも対応できており、それらのTipsなどの説明があった。

セッションは、多くの質問が寄せられ、当然とはいえ、Internet-Drafts/RFCを書くことがセッション参加者の

主な興味対象であることが感じられた。

紹介されたツール類は、以下のようなものである

1. Text Formatting Tools / http://www.rfc-editor.org/formatting.html
2. xml2rfc / http://www.ietf.org/rfc/rfc2629.txt
3. nroff(groff)
4. Microsoft word template / http://ftp.rfc-editor.org/in-notes/rfc-editor/2-Word.template.rtf
5. LaTeX
6. MIB reference and compilers

Security Tutorial

2/29の15:00-17:00に開催された。参加者は300名程度。満席であり、SUNのRedia Perlman女史が説明した。Redia女史は、ARPの開発者としても知られている人物で、IETFの長老の一人である。

インターネットでなぜ、Securityが重要であるかに関しての説明を、技術的なコンセプト、守るための個別の技術などを平易に、解説しており、特に暗号技術に関しても多くの説明を行っていた。暗号に関しては、「勝手に暗号を作るべきではなく、きちんとレビュを受けたものを使うのが望ましい」というコメントを残していた。セキュリティプロトコルは大変難しいので、全部自分でやるのではなく、複数の人間が共同して行うことが重要とも言っていた。

セッション終了後、Redia女史に「大変有効なセッションなのでスライドをもらえないか」と聞いたところ、後日連絡することを快諾された。その後、このドキュメントはIPAと共同で翻訳され、Webページから公開されている。

Redia Perlman女史(中央)と稲田氏(左)

Security Tutoriaruの会場

http://www.ipa.go.jp/security/ietf/ietfsectut-ja-20040608.pdf

WG Chair Training

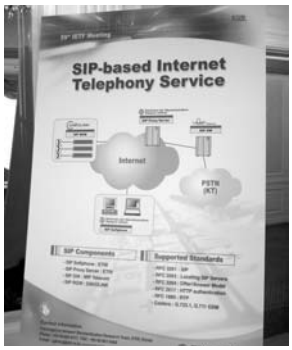
2月29日13:00-15:00に開催。Mararet Wassermanが説明した。

WG Chairになった人、またはこれからなろうとしている人向けに、WG Chairの役割と責任の範囲が解説された。また、WGを公正かつオープンかつ生産的に運用するためのノウハウが紹介された。このセッションはIETF参加者全員が聞くことが出来、特にWGのChairとして指名されていなくても聞くことが可能である。

参加者は、10数名程度と少数であったが、WG運営に必要な作業や情報の紹介は、WGを運営しようとする人々だけでなく、WGに参加して具体的な活動をしていく(例えばI-Dを執筆したりする人々)にとっても非常に有益なセッションだった。

オープン性と公正性を保つための工夫として、オフラインミーティングに参加できない人々に配慮して必ずMLでの確認を求めたり、言語や文化の異なる人々のために、オフラインミーティングでも口頭でのコミュニケーションに頼らず文書を記録として残せるよう注意を促すなど、IETFの本質的な運営ノウハウが非常に興味深かった。

WG Chairとなるべき人々に対して、IETFの基本思想である“Rough Consensus, Running code”を改めて説明するあたり、基本思想の維持徹底を心がける努力を欠かしてないことも窺えた。



SIP利用IPv6電話の説明


SIP利用IPv6電話のデモ

IPv6 Demoについて

今回のIETFは、初めての試みとしてIPv6の製品群のデモンストレーションが同じ会場ホテルの別室で行われた。これはホストである韓国 Korea Telecomの思惑とIETFの思惑が一致したために実現したようである。デモ会場には、SIPを利用したIP電話が置かれ、国際電話を無料でサービスしていた(通話料はKorea Telecom持ちのようである)。デモンストレーションを見る限り、特にIPv4/IPv6の違いを意識せずにアプリケーションを利用できるようである。日本へテスト的に電話をしてみたが、SIP応用のIP電話は、十分に実用に耐える品質を持っているようだ。

現時点ではSIPのパケットに関しては暗号化・電子署名といった伝送路中での盗聴・改竄対策はなされていないが、IETFのSIP関連のWGでは、SIPパケットに対して暗号化・電子署名を行うための議論が進められている。


KEIS6デモの一部

SIPパケットをPKIベースのCMS(Cryptographic Message Syntax)で暗号化·電子署名を行うことが提案されており、比較的早期に暗号化·電子署名が導入されると思われる。

韓国は、国策としてIPv6を推進しており、Seoul市内に大規模なIPv6デモンストレーション場(KEIS6、IETF会場より見学ツアーあり)を用意するなどIPv6の普及を図っている。日本においても国策としてIPv6の発展・普及は行われているが、韓国に比べると迫力に欠ける感じがするのは何故だろうか。

以上、ソウルで開催された第59回IETFのほんのさわりをご紹介した。IETFはやはり一度は行って話を聞いてみる価値があるだろう。一度だけではすまないかもしれない。自分の問題意識を持って、実際に起こった問題や提案を持っていけば、多少言葉が通じなくても歓迎されるのは間違いないだろう。さまざまな問題点を議論し、より良いRFCを作り上げ、世界の多くの開発者や、ひいてはそれを使うユーザが幸せになることが、共通の目的意識だろう。JNSAのChallengePKIプロジェクトも、11月のI-DのRFC化へ向け、更に磨きをかけて行きたい。

より詳しい報告は、別途JNSAのWebページでも掲載する予定なので、そちらも参照していただければ幸いである。