第57回IETF参加報告

富士ゼロックス株式会社
稲田　龍

NPO日本ネットワークセキュリティ協会(JNSA)では、PKI相互運用技術WGとChallenge PKIプロジェクトを中心にして、PKI関連の問題を取り上げ、実際に使えるものにするための試行として、問題点の指摘と改善案の提案や議論などを、大元のIETF(Internet Engineering Task Force: http://www.ietf.org/)のPKIX-WGに対して行ってきている。この活動は、Challenge PKI 2001で得られた知見や成果をIETFの場で議論するべく、横浜で2002年7月に開催された第54回IETFミーティングのPKIX-WGで始めてプレゼンを行い、プライベートBOFも開催したことが発端になっている。この後、Challenge PKI 2002の作業を通して、2002年11月のアトランタの第55回IETF、2003年3月のサンフランシスコの第56回IETFとPKIX-WGでの発表を重ねてきた。2003年7月のウィーンで開催された第57回IETFでは、Challenge PKI 2002の派生物として、個人提案の形ではあるがインターネットドラフトの提出を行い、非常に注目された。この報告では、第57回IETFの概要を簡単にご紹介する。
尚、2003年11月にミネアポリスで第58回IETFが開催されており、ここでも先のインターネットドラフトをRFCにするための準備として、主要なメンバーのレビューを行ってもらうことをお願いしたり、内容についてのディスカッションなども個別に進めることができるようになってきている。これらの成果は、2004年3月のソウルで開催される第59回IETFで発表する予定なので、今後のことについては改めてご報告したい。

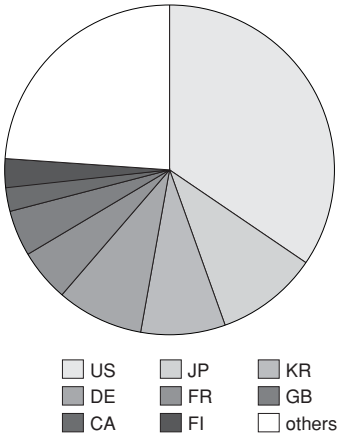
さて、2003年7月13～18日にオーストリアのウィーンのAustria Center Viennaにて開催された第57回IETFミーティングであるが、JNSAは2002年度に情報処理振興事業協会セキュリティセンター（略称：IPA/ISEC http://www.ipa.go.jp/security/）より委託を受けた事業であるChallenge PKI 2002プロジェクトの派生物であるInternet-Draft“Memorandum of Multi Domain PKI interoperability”（セコムトラストネット島岡政基氏著）に関しての島岡氏の発表と議論をPKIX-WGにて行う目的で、下記のメンバーで参加した。（敬称略、順不同）

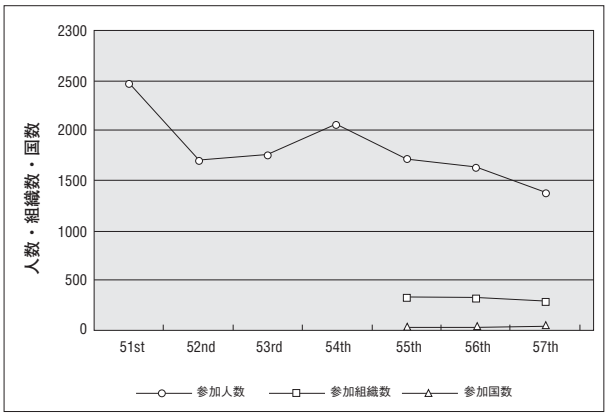
富士ゼロックス株式会社　稲田 龍、横田智文
セコム株式会社　松本 泰、漆島賢二
セコムトラストネット　島岡政基
ディアイティ(JNSA)　安田直義

■IETFの参加者

第57回IETFミーティングの参加者は48カ国から277の組織で、総勢1,331人であった。前回のサンフランシスコでの第56回が1,640名であり、アトランタの大55回が1,706名、横浜の大54回が2,064名、第53回のミネアポリスが1,756名であり、参加者数は減少傾向にある。日本と韓国、ドイツはほぼ同数だったが、米国からの参加者が大幅に減少している。同時テロ以前のロンドンで行われた第51回が2,457人であったことを考えると、米国でのITバブルの崩壊の影響は、いまだ強く残っている事が感じられた。

以下、第57回IETFで直接参加したPKIXでの議論と、関連するWGでのいくつかの議論を紹介する。少し専門的過ぎるかもしれないが、IETFの現場での議論を少しでもお伝えしたいので、いま少しお付き合いいただければ幸いである。





■ IETF/PKIX-WGの方向性

今回のIETFでは、WGチェアのSteve Kent/Time Polk両氏より「IESGの方針を受け、PKIX-WGはこれ以上新しいWorking Itemを増やさない」という方針が事前にアナウンスされた。また、この方針のため、今回のPKIX-WGのAgendaとして下記のような内容があげられている。

> 1.1 WG Focus and Direction [ADs]
>
> The working group has received direction from the IESG that will limit the types of new specifications accepted as PKIX work products.
>
> The ADs will present IESG's expectations for the PKIX WG along with the rationale. (15 min.)

これは、PKIX-WGが本来はインターネットにおけるX.509証明書を利用するための基盤技術を決めるためのWGであるにも限らず、ここ数年、PKIを利用したアプリケーションの必要性を受け、セキュリティエリアをはみ出した活動をしており、そのためにPKIの標準化および配備が遅々として進まない事を打開するためのIESGからの指示と受け取れる。

実際、IETFの他のWGにおいて認証およびセキュリティの仕組みとしてPKIを採用する例が増えておりそれらのWGでの議論とPKIX-WGでの議論が重複/対立を避けたと考えられる。

今回のPKIX-WGで、このAgendaをうけ、Security AreaのArea DirectorであるRuss Housley氏が上記の説明を行った。具体的にどういう活動を行うべきかに関してHousley氏は明言を避けたが、今後、PKIX-WGはこの方針を受けて活動を行うためPKIのインターネットにおける標準化活動は

1. PKIの利用に関しての基盤技術の確立（RFC3280の後継、証明書検証のための枠組み）
2. PKIを応用したプロトコル/アプリケーションの開発

の二つの流れにわかれ1をPKIX-WGが引き続き行い、2を他のWG/新設WGが行うモデルになると考えられる。

この状況は、数年前のIPv6 WGの状況に似ている。IPv6 WGもIPv6の基本プロトコルを制定後、運用、配備、ルーティングなど複数のWGを生み、IPv6の開発および配備を進めてきた。おそらくIESGの意図もIPv6と同様にPKIが基本部分の制定は終了し、今後、本格的な普及に向けた活動を行うことを意図したことと考えられる。

ミーティング終了後、チェアであるSteve Kent氏よりこの部分に関して以下の議事録がPKIX-WGのMLに投稿されている。

> WG Focus and Direction - Russ Housley
>
> The working group has received direction from the IESG that will limit the types of new specifications accepted as PKIX work products. Thus the WG is not accepting new work items.
>
> New WGs will be formed, as needed, to address PKI issues, or individual drafts can be submitted and subject to IETF-wide last call if the work described in them is mature and non-controversial. [no slides]

実際、現在のPKIX-WGでは、PKIの新たな利用に関してのInternet-Draftsも活発に投稿されており、これらの議論が活発になされれば新たなBOF/WGが形成されていく事は想像に難くない。次回、次々回のIETFにおいてPKIX-WGの活動および他のWG/BOFの動きをより注意深く観察し、今後のインターネットにおけるPKI利用の方向性を見定める事が重要と考えられる。

■ PKIX-WGでのInternet-Draftの発表

今回のIETF/PKIX-WGで、JNSAとIPA/ISECの名前で、セコムトラストネットの島岡政基氏がInternet-Draftの発表を行った。島岡氏は、JNSA Challenge PKI 2001/2002の中心人物の一人でありテストケース/テスト環境の設計、報告書の作成などを報告者と共に精力的に行ってきた。

JNSA Challenge PKI 2001/2002の活動を通じ、またアジアPKIフォーラムでの活動において島岡氏はいわゆるMulti Domain PKIに関しての定義が曖昧であり不要な誤解、理解の不足により相互接続性が阻害されていると感じた。そのため、いわゆるMulti Domain PKIに関しての状況を整理しまとめたInternet-Draft“Memorandum of Multi Domain PKI interoperability”を執筆した。
当初は、PKIX-WGのチェアであるSteve Kent氏（BBN Net）およびTim Polk氏（NIST）と相談の上、WG Draftとして公開する予定であったがIESGの方針によりPKIX-WGは、これ以上、Work Itemsを増やさない方針であるとのTim Polk氏の助言により島岡氏個人のPersonal Draftとして公開する事となった[1]。

Tim Polk氏との事前協議により、今回のPKIX-WGにて10分間の時間をもらい、島岡氏がこのInternet-draftを書く背景の説明と内容の説明を行い今後の予定などを発表した。

Title	: Memorandum for multi-domain PKI Interoperability
Author(s)	: M. Shimaoka
Filename	: draft-shimaoka-multidomain-pki-00.txt
Pages	: 16
Date	: June 2003

[1] PKI-WGの活動の方向性に関しては前節の「IETF/PKIX-WGの方向性」を参照のこと。

発表は、好意的に受け入れられた。特にTim Polk氏からは「非常によくまとまった発表であり、今後のRFC3280の後継のRFCに対しても反映したい」というコメントを付けていただいた。事実上、最大限の賛辞であり島岡氏のInternet-Draftが高く評価されたと感じた。おそらく、PKIX-WGがNo more New Work Itemの状態でなければ、文句なくWG DraftとしてPKIX-WGで（おそらくBCPもしくはInformational）RFCとして制定される道をとったものと思われる。

■ パス構築／パス検証に関して

PKIX-WGミーティング終了後、パス構築／パス検証に関してのInternet-Draftsを書いたMatt Cooper氏（Orion Security/draft-ietf-pkix-certpathbuild-00.txtの作者）と意見交換を行った。この意見交換ではMulti Domain PKIに関してのパス構築／パス検証に関しての扱い方と簡単な議論を行い、Matt Cooper氏と協力する事を約束した。後日、Matt Cooper氏と島岡氏でメールをやり取りし、より詳細なレビューを行っている。

■ IPv6アドレスの利用法に関して

IAB Open Plenaryにて、IPv6アドレスの利用に関して興味深い提言がなされた。

IPv6のアドレス体系は、IPv4アドレスでの反省の元に、以下の3つのアドレスを持っている。

1. Global Address
2. Site Local Address
3. Link Local Address

これらのアドレスはアドレススコープという概念の元にまとめられたものであり、各々、インターネット全体から見える、サイト(組織)内でのみ見える、ホスト内でのみ見えるというアドレス体系となっている。この「アドレススコープ」という概念は、IPv4に後付で取り入れられたいわゆるプライベートアドレス/グローバルアドレスの概念を整理/拡張したものである。

これらの「アドレススコープ」をどう使い分けていくべきであるかに関して、IABから以下のような提言がなされた。

1. Global Addressは、対外的なWeb Server/Mail Server/ルータ等全世界から見える必要があるサーバに割り当てる。
2. Site Local Addressは、組織内のデータ共有サーバやプリンタなど対外的に見せる必要はないが組織内では見える必要があるサーバに割り当てる。
3. Link Local Addressは、複数のインターフェイスを持つ場合で特定のインターフェイスに対してルーティングを行いたいなどといった場合に割り当てる。

IPv6対応の製品群は、家電などにも用いられるためセキュリティに対して種々の仕組みを持っており、このアドレススコープという概念もルーティング情報

の圧縮のためという側面と、「見せるべきもののみを見せる」という観点でセキュリティといえる(もちろん、この機能だけでは十二分でない事は明らかではある)。

稲田の所属する富士ゼロックスでも、コピー/プリンタのネットワーク接続を進めており、IPv6化も当然考えねばならない。そのときに、このアドレススコープに対しての対応と接続のために適したアドレススコープを選択できる機能は必須となる。

たとえば、SOHOオフィスなので使う場合は、SOHOオフィス内ではアドレスはSite Local Addressのみで運用されるかもしれない。その場合でもきちんと動作するコピー/プリンタが要求される。

また、単なるプリントエンジンとしてホストに接続する場合はLink Local Addressでの接続が要求されるであろう。等々、きちんとしたIPv6のアドレス体系/プロトコルの理解が要求される[2]。

■ NISTのS/MIME Test Suiteに関して

S/MIME WGのセッションにおいて、NISTのTim Polk氏がNISTで開発しているS/MIME Test Suiteに関して発表を行った。このTest Suiteは、特定のメールアドレスに対してS/MIMEメッセージを送るとそのS/MIMEメッセージの妥当性、正当性を評価しレポートするもののようである。

S/MIME WGの終了後、Tim Polk氏とNIST版S/MIME Test Suiteの構成と日本語に対するサポートの状況を問い合わせたところ、できる限りのサポートをしていただけることとのことであった。Tim Polk氏より、7/21の週にリマインダーとして具体的な依頼事項を記述したメールがほしいとのことであったので次のようなメールを送った。

問い合わせを行った内容は、

1. このTest Suiteのソースコードが公開される予定があるか?
2. 公開されるのなら、ソースコードを変更しChallenge PKI 2002の成果物であるGPKI Test Suiteに同梱して配布してかまわないか?

の2点である。

JNSAは第55回IETF、第56回IETFのPKIX-WGにてChallenge PKI 2001/2002の発表を行っており、Tim Polk氏にはその成果物としてGPKI Test Suiteを公開した事を報告してある。また http://www.jnsa.org/mpki/にてChallenge PKI Projectの成果物を公開している事を知らせてある。これらに関してもTim Polk氏は高く評価してくれている。

■ Challenge PKIへのお誘い

さて、紙数も尽きてきたので、まだまだお伝えしたいことはあるが、標準を作る話の常としてかなり専門的な議論となっているので、Challenge PKI Projectとしての第57回IETFでの議論はこのくらいで終えておこう。この後、2003年11月のミネアポリスでの第58回IETFでは、冒頭で述べたように更に中核人物との連携が実現できた。このような準備ができたので、2004年3月ソウルで開催される第59回IETFでは、Internet-DraftのRFC化を更に進める予定で準備している。

また、2003年11月末にIPA/ISECの課題として報告書を作成している、タイムスタンププロトコルに関する報告書と、アプリケーションAPIに関する報告書の成果を加えて、更にPKIの実運用環境で必要とされる技術標準を考えていきたいと考えている。もしご興味とアイデアをお持ちであれば、ぜひご連絡いただきたい。より広い知見を集められればより良いものになると思うので、ご指導ご協力を賜れるようお願いしたい。

[2] IPv6のアドレスは、通常はNeighbor Discovery Protocolと呼ばれるプロトコルでDHCPのようにアドレス情報を取得する。その際に、悪意のあるNeighborより妨害情報をもらわないようにするための枠組みもSEND(SEecurely Neighbor Discovery) WGで議論されPKI技術の導入も検討されている。