第56回IETFミーティング参加報告書

富士ゼロックス株式会社
稲田　龍

セコムトラストネット
島岡　政基

NPO 日本ネットワークセキュリティ協会
安田　直義

富士ゼロックス情報システム株式会社
増田　健作

2003/3/17-21に米国サンフランシスコのSan Francisco HILTONにて開催された第56回IETF(Internet Engineering Task Force: http://www.ietf.org/)ミーティング にNPO　日本ネットワークセキュリティ協会(略称: JNSA http://www.jnsa.org/)が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JNSA Challenge PKI 2002プロジェクトの報告とその成果物である“Multi Domain PKI Test Suite”のデモンストレーションをPKIX-WGにて行う目的でJNSA安田直義氏、セコムトラストネット島岡政基氏およびFXIS増田健作氏と共に参加したので報告する。

第56回IETFミーティングの参加者は34カ国から325の組織で、総勢1,640人であった。アトランタの第55回IETFミーティングの参加者は34カ国から334の組織で、総勢1,706人であった。横浜の第54回IETFが2,064人、第53回のミネアポリスのIETFが1,756人であった。同時テロ以前のロンドンで行われた第51回IETFが2,457人であったことを考えるとテロの影響と米国におけるITバブルの崩壊の影響と思われる。

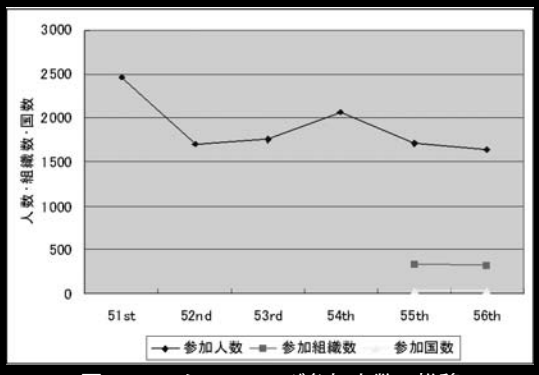

図1 IETFミーティング参加人数の推移

■報告者のPKIX-WGでの発表に関して

報告者である稲田は、アトランタで行われた第55回IETFに引き続きJNSAと共同で行っている「JNSA Challenge PKI 2002」の報告とその成果物である“Multi Domain PKI Test Suite”のデモンストレーションをPKIX-WGで報告した。

写真1 PKI-WGミーティングで報告している稲田(右)

「JNSA Challenge PKI 2002」プロジェクトおよび“Multi Domain PKI Test Suite”は、IPA/ISECの平成14年度「情報セキュリティ関連の調査・開発に関する公募」に対してJNSAが応募し採択された「電子政府情報セキュリティ相互運用支援技術の開発」によるものである。発表内容は、「JNSA Challenge PKI 2002」の概要(図2)と成果物である“Multi Domain PKI Test Suite”のコンセプトと機能概略（図 3)の説明および今後、Multi Domain PKI環境を定義し、テスト環境を作るためのInternet-Draftsを書く事を報告した。

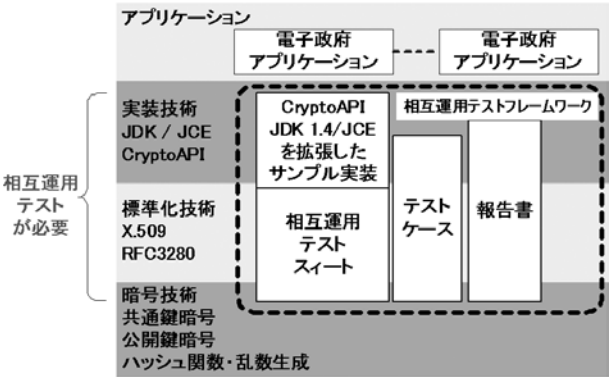

図 2 JNSA Challenge PKI 2002の概要

日本政府は、行政手続きの効率化と国民負担の軽減を目標に、国民と行政機関の間の申請・届出・通知などといった手続きを電子化する「電子政府」の構築を目指している。

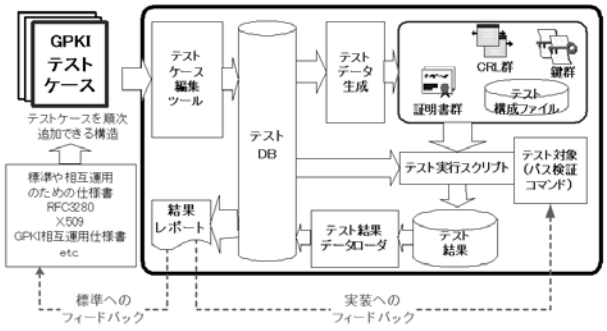

図 3 “Multi Domain PKI Test Suite”の概要

情報流通の基盤として構築されている政府認証基盤(GPKI)では、ブリッジCAモデルと呼ばれる信頼モデルが使用されている。ブリッジCAモデルは、主体者が異なるマルチドメインPKIを実現する手段として柔軟性のあるモデルであるが、その反面、ドメイン間での相互運用性を確保するために高度な技術を要する。

その状況下で、適正なPKIアプリケーションの開発を行うために証明書の失効確認/パス検証を行うテスト環境として“Multi Domain PKI Test Suite”とテストケースを開発した。“Multi Domain PKI Test Suite”はGPKIに限らず、汎用なPKIテスト環境を提供する。

現在、インターネット上ではPKIのアプリケーションが使われているが、複雑なPKIドメインを適用している例は少ない。また、PKIXが出したRFC 3280では、複雑なPKIドメインを使うことも考慮されてはいるが実際に試せる環境は少ない。NISTなどでRFC 3280の相互接続実験は行われているが、テスト環境の構築が難しく手軽にテストすることは難しい。

今回の“Multi Domain PKI Test Suite”は、スタンドアロンで動作し手軽にテスト環境を構築/運用できるようにしたものであり、他に類がない。「JNSA Challenge PKI 2002」の報告書を英訳および“Multi Domain PKI Test Suite”の公開を6月に公開する事を発表した。

写真 2 質問をするSteve Hanna氏

また、この“Multi Domain PKI Test Suite”を作るにあたってMulti Domain PKIの定義がIETFでは文書化されていない事が明らかになった。Multi Domain PKI環境でのテストケースを適正に作成維持していくためには「Multi Domain PKIの定義」を文書化し共通の認識で作成していく必要性を実感したため、「Multi Domain PKIの定義」のInternet-Drafts化を行うことと、テストケースを交換しやすくするためにテストケースデータベースのスキーマの定義をするInternet-Draftsを作成するつもりであると報告した。

発表後のQ&Aでは、Sun Microsystems社のSteve Hanna氏(JAVA JDKのPKI検証ライブラリの作成者)から、発表に使用したスライドがいつ公開されるかという質問があった(スライドはPKIX-WGのチェアには送付済みで、後日、Proceedingsとして公開される予定)。

写真 3 Tim Polk氏と

ミーティング終了後、台湾のPanasonic Taiwan Laboratoriesの周立平氏/陳柏飛氏がコンタクトして来た。彼らもMulti Domain PKI環境でのテストを行うことに苦慮しており、公開の時期と彼らの環境で動くかどうかを気にしていた。

ミーティングの終了後、Tim Polk氏と今後の活動に関しての議論を行った。作成を意図している2つのInternet-Draftsは、WGドキュメントにするかJNSAのパーソナルドキュメントではじめるかに関わらず7月のPKIX-WGでの議論対象にすることも可能であることを確認した。

また、発表後にGlenn Mansfield Keeni氏(Extended Incident Handling(INCH)の主要メンバー)より以下の共同で行える事がないかという趣旨のメールをもらった。

Subject: Todays PKIX Presentation
From: Glenn Mansfield Keeni <glenn@cysols.com>
To: Ryu Inada <Ryu.Inada@fujixerox.co.jp>
Dear Inada-san,
That was good and important work ! What are the plans from now. Let me know if I can help in any way.
We are looking forward to the presentation in Vienna.
Cheers
Glenn

■IETFにおけるPKIの応用

前回のアトランタで行われた第55回IETFミーティングでも、話題として上げられていたが、PKIをS/MIMEやSSL/TLS以外のアプリケーション/プロトコルでも利用する動きがある。

実際、AAA-WGで決まったDiameterにおいてはデータの交換形式としてCMS(Cryptographic Message Syntax)を用いて暗号化/電子署名が実現されている。
今回のS/MIME-WGのミーティングにおいてもSIPのパケットフォーマットにCMSを使うという動きがある。

PKIの利用範囲が広まりつつある反面、なかなか配備が進まない、技術的に難解であると言う不満が出ている。これらの状況は、ようやくPKIが「インターネットで使える技術」として認知されたということである。

また、今回の「IESG Open Plenary」で正式に発表されたが、Security AreaのDirectorとして長年貢献したMITのJeffrey I. Schiller氏に代わり、元RSA Laboratories(現Virgil Security社)のRussell Housley氏が就任した。Housley氏はRFC 2459/3280の著者の一人でありPKIの第一人者である。この交代は、3年近くPKIX-WGの活動を通じ、PKIの展開を進めていたが、この展開が遅々として進まない反面、OASIS/W3C/EESIなどから続々とPKIに対しての標準の提案とIETFに対しての協調の要請が出ている状況をIESGとしては看破できず、PKIに対してのてこ入れがなされたと報告者は受け取った。前節にも述べたとおり、PKIが「インターネットで使える技術」として認知こともあり、今後の展開が期待される。

■IETFの在り様の変化

IETFは、インターネットの標準の策定を行っているが、昨今、活動範囲が多岐にわたり他組織との間の協調の必要性が高くなっており、IETFが独自に規約/標準を決められなくなりつつある。これは、インターネットが複雑化し多くの団体がその価値を認め利用を始めていることの証明である。

また、IETFの内部にも問題を抱えている。

第一に、IETFの運営資金をどうするかが問題となり

つつある。IETFは、いくつかの資金源を持っているが、多くは年3回のIETFオフラインミーティングの会費で賄っている。ここ数回のオフラインミーティングの参加者が落ち込んでいる状況を考えると楽観は出来ない。実際、過去からの繰越金で運営されている状態であり3年後には資金が枯渇するとの報告があった。また従来、IETFのオフラインミーティングには、スポンサーが付くが(第54回の横浜のIETFでは、富士通がスポンサーとなった)、今回のオフラインミーティングでは初めての試みとしてスポンサーなしでオフラインミーティングが行われた。これは、米国でのIT業界の不況のためスポンサーのなり手がなかったのではないかとも、また、特定のスポンサーの利害にIETFが左右されるのを嫌ったとも考えられる。

第二に、IETFが標準化を行う領域が広く、また細分されておりIETFに参加しているメンバーのレビューが出来なくなりつつある。具体的には、各WGから提出されるInternet-Draftsのレビュー率が低くなり(平均10%程度)、Internet-DraftsとしてIESGが承認できない状況が増えている事が報告されている。これはInternet-Draftsの内容が高度に専門化されてしまい、多くのメンバーは何が書いてあるかが理解できていない状況であるといえる。

■IETFにおけるセキュリティに対する意識

IETFにおいても、セキュリティは大きな問題として取り上げられており、「セキュリティ」はひとつのキーワードとなっている。

具体的には、RFC/Internet-DraftにはSecurity Considerationというセクションが設けられておりRFCの発行に関してArea Director/IESG(Internet Engineering Steering Group)から「セキュリティに関しての考察が甘い」といったコメントがある場合が多い。

IETFの初日である17日には、Security Tutorialが開かれ、Security AreaのArea DirectorであるJeffrey Schiller 氏/Steven Bellovin氏よりProtocolを安全に設計するためのチュートリアルが開かれた。このSecurity Tutorialは昨今のIETFでは毎回開催されている。

また、IETFの会期の終わり近くに「Open Security Area Directorate」があり、IETFおよびインターネットにおけるセキュリティのあり方の議論と現状の報告が行われる。

今回の「Open Security Area Directorate」では、PKIが話題となっていた。PKIは、3年にわたって展開を行おうとしているが、うまく展開できていないのはなぜであるかが話題となっている。

IETFミーティングではターミナルルームと無線LANでのネットワークコネクティビティを提供しており、すべてのコンファレンスルームでインターネットへ自由に接続できる。前回のIETFミーティングでは、IETF主催者側より「無線LANにおいてパケットの盗聴の可能性があるのでSSL/SSH/IPsecなど暗号化を行うこと」という注意が流れている。今回のIETFでは、IETFのWeb上(http://www.ietf.org/meetings/netinfo.html)に以下の注意が載せてある。

> Security Warning
>
> Please note that using 802.11 without additional encryption is not private. In particular, do not use protocols with cleartext passwords, such as telnet or non-APOP POP3. Instead, use encrypted protocols such as SSH, SSL or IPsec. It is well-known that people may be sniffing packets on the network. There should be no expectation of privacy when using unencrypted protocols on the IETF-56 network.

EAPで無線LANの認証とセキュリティに関しての議論がなされている一方で、この様にある意味では無防備なネットワーク環境が用意されているところにIETFのひとつの側面が現れている。インターネットは、自由なネットワークアクセス環境を提供する。その上で自己を守るための枠組みを作り、それを利用するか否かは利用者が決めるべきであるという考えである。

■IETFのネットワーク環境とターミナルルーム

IETFでは、インターネットの利用を行うためターミナルルームが用意されているが、ここ数回のIETFにおいて通例となっている無線LAN(IEEE 802.11b)によるネッ

写真 4 ターミナルルーム 左側: 入り口/右側: 全景

トワークアクセスが提供されており、会場およびその周辺では自由にネットワークアクセスを行うことが出来た。そのためか、今回のターミナルルームはいつものターミナルルームに比べ狭く感じた(写真 4右)。
会場となったホテルのロビーおよびバーにおいてもこの無線LANを使うことが出来たためロビーのそこかしこでノートPCを持った参加メンバーがインターネットに接続していた。また、ロビー/バーで食事を取りながら打ち合わせをする姿も多く見られた。(写真5)

写真 5 ホテルのロビーにて

ターミナルルームはSUN Microsystemsが運営をしており、SUN RAYを持ち込んでいた。SUN RAYを使うために、SMART CARDが配られており、このCARDには固有のUIDが書き込まれており、ユーザ毎のSUN RAYの設定情報を呼び出すのに使われているとの事であった。(写真6)

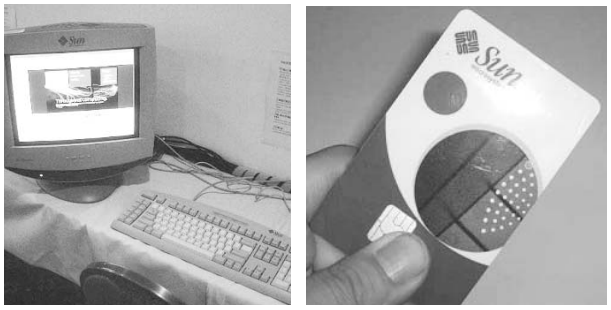

写真 6 SUNRAY(上)とSMART CARD(下)

IETFも転換期を迎えているのかもしれないが、次に引き受ける組織もまだ見えていない。ただ、参加しているメンバーは組織が変わっても相変わらず一緒に作業するチームになることは間違いないだろう。このような意味では、組織ではなく、知識の集約であることが理解できる。このような「場」にきちんと参加し、実体のあるデータや意見を出し、ディスカッションを行うことが重要であろう。日本でこのような活動ができるようになってきたのは喜ばしいことであるし、JNSAが協力できていることはすばらしいことだと思う。今後とも各位のご協力を賜れば幸いである。