ICAT NewsLetter Vol,5

認証実用化実験協議会
（財）日本情報処理開発協会内　〒105-0011　東京都港区芝公園3-5-8　☎03-3432-9387

今　号　の　記　事

第40回 IETF会議報告

報告者：稲田　龍（富士ゼロックス㈱）

40th IETFミーティングは、1997年12月7日から14日までアメリカ合衆国ワシントンD.C.で開かれた。

IETF(Internet Engineering Task Force) は、Internet にある技術的な問題を解決するために結成され、現在200を超える WG(Working Group) が活動を行っている。各 WG は、活動の大半をメーリングリストで行っているが、年に3回、いわゆる“オフラインミーティング”を開く。

下の写真は、ミーティングの会場となった Omini Sheraware Hotel の外観である。

今回の IETF の参加者は2000名をついに超えた。下の写真はレジストレーションの様子である。

レジストレーションのデスクの前には長蛇の列が出来ており、報告者はレジストレーションを行うのに30分ほどの時間を費やした。 年々、IETFへの参加者は増えており今後、もっと合理的で早いレジストレーションの仕組みが出来ることを強く望む。

１．概観

今回の IETF では、全体として

・IPv6 への移行
・Security

が多くの場面で目に付いた。

特に IPv6 は、基本となるプロトコルがほぼ完成され、相互運用も実現されてきており 6BONE などを使って全世界レベルでの相互接続実験環境が整備されている。IPv6同士での通信は、問題なく出来るレベルまでになっている。

今後は、従来の Internet Protocol (IPv4) と新しい Internet Protocol (IPv6) 間での移行環境を整えることが課題として上がっていた。そのための手法としていくつかのモデルが提唱され ていた。

この WG では、日本の WIDEプロジェクトのアクティビティが高く評価されていた。

WIDEプロジェクトのアクティビティとして出ていたものは

WIDE 6BONE　：日本国内での6BONE
SOCKS64　：Socks Protocol

による IPv4/IPv6 Gateway などがあげられる。

Securityに関しては、多くの組織が Security の重要性を認識し IETF としても種々の活動を行っている。

特に暗号関連はアメリカ合衆国政府の制作と特許関連の問題はあるが、多くの分野で徐々に問題点はクリアされつつある。

今回の IETF では、RSA Data Security Inc. は、IETF に対して「Secure DNSに関して RSA の特許を使う場合、特許料の請求は行わない」旨の発表があった。 米国でRSA公開鍵暗号の特許が

2000年に切れるので、それまでに多くの Internet の領域で RSA がデファクトスタンダードになるように思索しているようである。

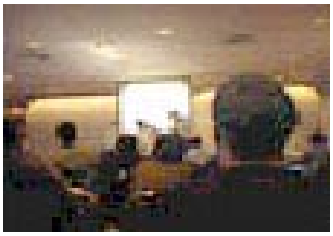
２．IPv6への移行

IPv6 は既に目の前に来ている感じである。日本国内でも昨今 DEC が IPv6評価キットを販売始めたように、主要なルータメーカ/コンピュータメーカの一部は IPv6 の実装を何らかの形で持っているという印象である。IPv6 への移行で問題になるのは、現状の IPv4 の世界のマシンからどう移行するかである。IPv6 自体には、IPv6 のアドレス空間の一部を IPv4 のアドレスに割り当てているので、 IPv6 のアドレス空間に IPv4 のアドレスを持っていたマシンを格納することは出来る。

３．PKIX
（Public-Key Infrastructure(X.509)）

ITU-T X.509 証明書を使った公開鍵暗号方式の証明書を、Internet での認証および暗号鍵の配布に使うための枠組みを議論している WG である。

ミーティングは2回行われた。以下の写真はミーティングの風景を撮ったものである。



今回のミーティングでは、

1. CertificateとCRL(Certificate Revocation List) のプロファイル
2. LDAP WG との連携および要求
3. CMP(Certificate Management Protocol)
4. CRS(Certificate Request Syntax)
5. Time Stamping (TSA) & Notary (NA)
6. OCSP(Online Certification Status Protocol)

についての報告があった。

CertificateとCRL(Certificate Revocation List)のプロファイル

Internet Public Key Infrastructure X.509 Certificate and CRL Prefile として出されている X.509 の証明書のプロファイルについて他のアプリケーションとの整合性をどこまで取るかについての議論が取り交わされた。すでに IESG への提出は終わっているが、いくつかの問題が残っていることが報告された。

1. Name の中の Wildcard をどう扱うか?
2. ASN.1 として1988年版を使うべきか1993年版を使うべきか？
3. キャラクタコードをどうするか？ UTF-8 を使うのか？
4. 鍵の利用条件を証明書内に持つべきか？
5. CRLDistributionPoint を Critical とすべきか否か？

といった問題が残っているとの報告があった。

LDAP WGとの連携および要求

LDPA v2 の Profile は Last call/IESG への提出も終了している。 現在の PKIX は LDAP v2 をベースとしているので新しいものは v3 に入れることにしたとの報告があった。この後必要である、新しいスキームを導入するときに LDAP WG と連携して行うべきであるとの意見がで、採用された。

CMP(Certificate Management Protocol)

キャラクタセットとして何を使うかという問題が残っているとの報告があった。CMP の Internet-Draft は“Internet Public Key Infrastructure Certificate Management Protocols”である。

ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-07.txt

CRS(Certificate Request Syntax)

PKCS7/10との整合性をどうするかという報告があった。

プロポーザルを S/MIME WG へ送り、S/MIME WG のチェアである Schiller氏/Housley氏からは特に反対を受けなかった旨が報告された。 この問題は S/MIME だけに関わる問題ではないことでもあり、一般的な解決を行うには PKIX で 扱うのが良いであろうという判断が行われた。

CRS については、今後も CMP との関係を明確化し RFC とすることが確認された。1998年3月24日付けで、一連の RFC として RSA の PKCS #1/#7/#10が RFC化されたことを付記しておく。

RFC2313 PKCS #1:
RSA Encryption Version 1.5 Version 1.5

ftp://ftp.iij.ad.jp/rfc/rfc2313.txt

RFC2314 PKCS #10:
Certification Request Syntax Version 1.5

ftp://ftp.iij.ad.jp/rfc/rfc2314.txt

RFC2315 PKCS#7:
Cryptographic Message Syntax Version 1.5

ftp://ftp.iij.ad.jp/rfc/rfc2315.txt

Time Stamping (TSA) & Notary (NA)

ICAP で行っているタイムスタンプサービスと同様なことをしようとしていた。

実際に何かを「証明しよう」とするときに「いつのものであるか」を明確に「証明」したいと言う要求はどこにもあるようである。

“Internet-draftsとしてInternet Public Key Infrastructure Pert V:Time Stamp Protocols”が出ている。

ftp://ftp.ietf.org/internet-drafts/
draft-ietf-pkix-ipki5tsp-00.txt

OCSP(Online Certification Status Protocol)

Internet-draft (Internet Public Key Infrastructure Online Certificate Status Protocols – OCSP) の状況を Mike Myers が報告した。 次回の Los Angels のミーティングまでに Last call するつもりであると報告された。

ftp://ftp.ietf.org/internet-drafts/
draft-ietf-pkix-ocsp-02.txt

[お問い合わせ先]

認証実用化実験協議会（*ICAT*）事務局：
財団法人 日本情報処理開発協会
情報セキュリティ対策室 内

〒105-0011 東京都港区芝公園３丁目５番８号
Tel: 03-3432-9387 FAX: 03-3432-9419
E-mail: info@icat.or.jp
URL: http://www.icat.or.jp/