ICAT NewsLetter Vol,6

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41回 IETF会議報告

報告者: 櫻井 三子 （日本電気㈱）

よりよいインターネットアーキテクチャ、より円滑な運用を目指し、主に技術標準化活動を行なっている IETF（Internet Engineering Task Force）の定例会議に初めて参加した。

IETF の活動単位には、ルーティング、セキュリティなど技術分野によって大まかに分類されたエリアと、各エリア内で個々の技術を検討するワーキンググループ（WG）とがある。各 WG は通常はメーリングリストを利用して活動を行ない、年3回開催される定例会議で Internet-Drafts（I-D）を叩き台として RFC 化に向けて議論する。定例会議では、WG 以外に単発の会議もあり、そこから新しい WG に発展することもある。

今回の会議は、1998年3月29日から4月3日の期間、米国ロサンゼルスの Westin Bonaventure Hotel にて開催された（このホテルはガラスばりの円柱形の建物からなっていてユニークである。『007』など映画のロケによく使われるというのも納得できる）。

参加者総数は 1,600名強であり、日本からの参加者は100名程度である。会議期間中は、1時間～2時間半のセッションが1日に4～6 程度開かれる。各セッションにつき6～7の会議が並行して行なわれることから、一会議あたり 200～300名が集まるという計算になる。

このような、組織を越え国を越えた、大人数による会議では、単に技術的な観点の議論だけではなく、企業の戦略、特許問題、（セキュリティ関連では特に）輸出規制問題などが複雑に絡み合ってくるということが肌で感じられた。

1. セキュリティエリア全体の動向

今回の会議では、セキュリティエリアのセッションは9つあった。

これらはセキュリティインフラとその応用という観点から以下のように分類できる（IPSEC は PKIX を利用することから、あえて応用系に入れた）。

応用系		OPENPGP	SMIME TLS IPSEC		
ｲﾝﾌﾗ系	CAT	SPKI	PKIX	OTP	CIDF

図中の略語の意味を以下に示す。

CAT	Common Authentication Technology WG
SPKI	Simplle Public Key Infrastracture WG
PKIX	Public Key Infrastracture （X.509） WG
OTP	One Time Password WG
CIDF	Common Intrusion Detection Framework WG
IPSEC	IP Security WG
TLS	Transport Level Security WG
SMIME	Secure MIME （S/MIME） WG
OPENPGP	Open PGP WG

PKIX は、ITU-T X.509 の定義に基づいた公開鍵暗号のインフラ関連のプロトコルについて議論している WG であり、ICAT の活動内容とも関連が深い。この PKIX を軸として、特に CA および CA が発行する証明書をインターネットで利用していくための議論が多かったといえる。

特に、IPsec が求めるCA についてのプレゼンテーションが IPSEC、PKIX の両セッションで行なわれたり、S/MIME の観点から PKIX のドラフトへの変更要求が出されるなど、WG 間でクロスオーバー的な議論も見られた。CA に関係する技術が Proposed Standard という位置付けの RFC化に向けて最終調整段階にあることが伺える。

また、全体を通じて使用する公開鍵暗号アルゴリズムが、現在製品によく使われている RSA から、特許が切れたため無条件に利用可能となった Diffie-Hellman に定着しつつあることや、特許はあるがより強度の高い楕円曲線暗号に対する注目が高まってきていることがわかった。TLS のセッションでは、楕円曲線暗号を使うための枠組みを決めるなど具体的な動きが見られた。

2. PKIX （Public-Key Infrastructure （X.509） WG）

PKIX WG のセッションは2回行われ、主に以下の内容が検討された。

PKIX WG の I-D はまだ RFC になっていないため、とにかく問題のないところから早く RFC 化していくという意向が伝えられた。

（1） Certificate and CRL profile
（2） LDAP profile and schema
（3） OCSP （Online Certificate Status Protocol）
（4） CRMF （Certificate Request Message Format）
（5） CMMF （Certificate Management Message Format）
（6） CMC （Certificate Management Messages over CMS*）
（7） TSP （Time Stamp Protocol）
（8） IPsec PKI Requirements
（9） Implementation Notes （by Microsoft）

* CMS：Cryptographic Message Syntax
S/MIME WG が出しているI-D

（1） Certificate and CRL profile

I-D の変更点についての説明が中心であった。変更点は主に以下である。

- 証明書に含める文字コードとして UTF8 を追加
- Certificate path validation に関して、現時点だけでなく過去の時点の有効性を含めることを追加
- SubjectAltName に“＊”などのワイルドカード文字使用を禁止
- RSAwithSHA1 の oid を追加
- Diffie-Hellman の processing syntax を追加

このドラフトは、Proposed Standard RFC とすることが強く望まれているが、いくつか特許に抵触する可能性のある部分については削除し、別ドキュメントにするという方針が確認された。例えば、X.509 V3 の拡張フィールドとして定義されている CRLDistributionPoints では、CRL の入手先を証明書に記入し必要に応じて取りに行くというアイディアが CRL の管理に関する特許に抵触するとのことである。これについては、特許を持っている Entrust 社が1998年4月23日付けで royalty-free license にすると発表し、関係者は安堵したところである。

http://www.entrust.com/news/1998/04_23_98.htm

（2） LDAP

LDAP v2 は Standard Track には乗れず、Informational Track になったことが報告された。今後、PKIX と LDAP との連携は、LDAP v3 の議論が落ち着くまでペンディングすることとなった。

（3）OCSP

OCSP は個々の証明書の状態（有効かどうか）を問い合わせるプロトコルであり、ICAT では VA（Validation Authority）と呼んで議論してきた内容に近い。

証明書の有効性を判定する材料は主に CRL であるが、CA がサーバとなるのか、それ以外のエンティティがサーバとなるのかによって、証明書の有効性を判定する精度が変わってくる。ミーティ

ングでは、証明書が有効かどうかを確認するプロセスについて、以下の議論があった。

・CRL に載っていないからといって即有効と判定しきれない場合どのように応答するか
・有効性判定結果のキャッシュをするか、するなら判定時にどう扱うか
・証明書を一意に識別するには何が適当か（CertID の定義）（CA名に公開鍵のハッシュ値を加えるか、あるいはCA名と公開鍵に対してハッシュを取るか）

証明書の有効性判定プロセスは、まだまだ議論が必要な部分である。CertID の定義については、CA名とシリアル番号に証明書のハッシュを加えるという S/MIME WG との食い違いが見られたが結論は出なかった。

（4）CRMF,（5）CMMF,（6）CMC

これらは証明書の発行要求や廃棄要求など、PKIに関連するデータ形式を定義している。

例えば、証明書の発行要求については、現在多くの実装で使われている PKCS#10 をベースにした形式と、新しい形式の両方の定義が行なわれているが、1つの文書にまとめて入っていない点がわかりにくいとか、なぜ2つ定義するのか、といった議論がされていた。

（7）TSP

Time Stamp Protocol と Notary Protocol との違いは何かといった質問や、Time Stamp Protocol 自体が特許に引っかかるので調べた方がよいといった意見があり、内容より特許に関する議論の方が多かった。

（8）IPsec

IPsec で使う鍵を交換するためのプロトコル IKE（Internet Key Exchange、ISAKMP/Oakley の新名称）において Diffie-Hellman の鍵とホストの対応を保証するために CA を今すぐ使いたいとのこと。そのための検討事項について発表が行なわれた。

詳細は、

ftp://module-one.tillerman.nu/pub/draft-thayer-ipsec-pki-00.txt

より入手可能で、I-D として提出する予定とのこと。ポイントは以下のとおり。

・ 証明書の Subject にホスト名を入れる場合にどのようなデータ形式がよいか
・ ルート CA が信用できるかどうかを判断する材料として、各 CA の管轄するホストの範囲を証明書に入れたい。そのデータは、DNS 形式がよいか、RFC822 形式がよいか、IPアドレス範囲を示す CIDR 表記がよいか

（9）Implementation Notes

Microsoft の人が証明書の有効性を確認するプロセスを明確にするため、CA の証明書に SubjectKeyIdentifier を必須とするような提案を行なった。しかし、SubjectKeyIdentifier を一意に決める方式を定義するのは困難であり、反対意見が多かった。

3．所感

（1） 楕円曲線暗号について

PKIX のセッション中、偶然にも Certicom社の人と隣合わせた。Certicom社といえば，米国標準や ISO 標準に楕円曲線暗号を積極的に提案しているところである。そこで、楕円曲線暗号をサポートした CA を開発しているかどうか聞いたところ、PKIX のドラフトに従うつもりで開発途中とのことであった。

これを聞いて、ICAT で楕円曲線暗号をサポートした CA を開発して実験を行なったことは世界的に見てもやや先行しているように感じた（1998年4月下旬には、Certicom社と Xcert社が契約を結び、Xcert社の製品にCerticom社の楕円曲線暗号が組み込まれる予定との発表があった）。

（2） PKIX と ICAT

過去の ICAT News Letter にある通り、ICATの広域認証技術研究タスクフォースでは今までに、HTTP をベースとした CA Management Protocol を I-D として提案し PKIX セッションで発表した。

また、楕円曲線暗号を利用した署名に関して気づいた問題点をメモにして、IETF 会場にて PKIX WG の議長である Stephen Kent 氏にコンタクトをとったこともある。

今回の会議では残念ながら、PKIX に対して具体的な働きかけができなかったが、挨拶をかねて

Stephen Kent 氏に話しかけてみた（本当にハリソンフォードにそっくり！）。ICAT の成果をどのような形で発表していくのがよいか検討中と話したところ、 Web を利用して PKIX に情報提供してはどうかと助言をいただき、実験結果の報告についてなどは、PKIX のセッションの利用も可能とのことである。

ICAT 全体がまとめの段階にある中で、PKIX に対して何らかの働きかけを行なっていきたいと思う。

事務局連絡

―第２回平成 １０年度定 例研究会の開　催を予定しております。

日時：1998年10月14日（水）

会場：機械振興会館にて

参加手続、プログラム等の詳細は別途ご連絡いたします。

［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/