ICAT NewsLetter Vol,7

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42回 IETF会議報告

報告者: 櫻井 三子 （NEC）

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っているIETF（Internet Engineering Task Force）の 定例会議に参加した。IETF への参加は第41回に続き2回目である。

Ｉ．一般動向報告

会議は、1998年8月24日から8月28日の期間、米国シカゴの Sheraton Chicago Hotel & Towers にて開催された。参加者総数は約 2,000 名であり、日本からの参加者は100名程度である。今回も会議期間中は、1時間～2時間半のセッションが1日に4～6 程度というスケジュールであった。

一般動向報告編では、セキュリティエリア全体の動向、およびICAT の活動と最も関連の深い PKIX の話題について報告する。

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8つの WG（Working Group）と2つの BOF（Birds of a Feather）があった。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）。

	TRUSTMGT			
応用系	AFT,STP	OpenPGP	SMIME TLS IPSEC	SECSH
インフラ系	CAT	(SPKI)	PKIX	

図中の略語の意味を以下に示す。

CAT	Common Authentication Technology WG
TLS	Transport Layer Security WG
STP	Secure Transport Proxy BOF
AFT	Authenticated Firewall Traversal WG
SECSH	Secure Shell WG
IPSEC	IP Security Protocol WG
SMIME	Secure MIME （S/MIME） WG
PKIX	Public Key Infrastructure with X.509 WG
TRUSTMGT	Trust Management BOF
OpenPGP	An Open Specification for Pretty Good Privacy WG
（SPKI）	Simple Public Key Infrastructure WG　今回はなし。

今回のセキュリティエリアのセッションでは、IPSEC、TLSをはじめとして、X.509 の定義に基づいた公開鍵暗号のインフラを軸とした技術は収束しはじめ、一段落しつつあるという印象を持った。X.509 の定義に基づいた公開鍵暗号のインフラを決める PKIX についても、今まで1つも RFC になっていなかったが、公開鍵証明書フォーマットの部分を皮切りにいくつかのプロトコルが近日中に RFC となる見込みである。

また、全体的に、認証方式（Authentication）が落ち着きを見せはじめたのに続いて、今度はアクセス権の管理方式（Authorization）をキーワードとした議論が出始め、新たな展開がはじまったと感じた。セキュリティエリアだけではなく、一般エリア（GEN）で AAA（Authentication、Authorization、Accounting） BOF が開催されたことが注目の高さの一端を伺わせる。

暗号アルゴリズムや方式に関わる特許およびライセンス問題については、全て把握しきれないといった問題はあるが、特許やライセンスを保有する企業が、特別な利用目的に限ってライセンスフリーで使用を許可するケースが増えてきた。これは技術が広がる意味で望ましい傾向になってきているといえる。特許やライセンスについて保有企業から見解の出されている件については、IETF の Intellectual Property Rights のページ

にまとめるようにした、とセキュリティエリアディレクタの Jeffrey Schiller氏からアナウンスがあった。LICENSE AGREEMENT の書類等が用意されている。

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

PKIX WGは、X.509 の定義に基づいた公開鍵暗号のインフラをインターネットで利用していくためのプロトコルの定義を行い、議論を行う WG である。PKIX WG のセッションは2つあり、最初のセッションが主に現在の主要なドラフト（Established Projects）について、2回目のセッションが主に新しい話題について、I-Ds（Internet-Drafts） を叩き台とした検討が行われた（実際の発表順は多少異なる）。

・Established Projects:
- （1） PKIX Cert and CRL Profile
- （2） LDAP v2 Schema and Profile
- （3） OCSP
- （4） CMP and CRMF
- （5） CMMF and CMC
- （6） IBM PKIX Software

・New Topics:
- （7） Timestamp Protocol
- （8） Notary Protocol
- （9） Web-based Integrated CA services Protocol、ICAP
- （10） Enhanced CRL Distribution Options
- （11） PKIX Roadmap
- （12） Qualified Certificates

主要なドラフトの状況は、以下のようにかなり収束してきた。

●IESG Last Call
- *（1） の draft-ietf-pkix-ipki-part1-09

●IESG 預り
- *（2） の draft-ietf-pkix-ldapv2-schema-01
- *（4） の draft-ietf-pkix-ipki3cmp-08

●WG Last Call
- *（3） の draft-ietf-pkix-ocsp-05
- *（5） の draft-ietf-pkix-cmmf-02、draft-ietf-pkix-cmc-01
- * draft-ietf-pkix-ipki2opp-07

（1）～（5）までは、変更点を中心とした説明が行われた。

盛り上がった話題は、（2）LDAPv2 の中で CA の証明書を格納する際に、cACertificate attributes と crossCertificatePair attributes のどちらの属性を使うのがよいか、という点であった。セッションでは 6つの場合分けをして Interoperability や Path Development について比較した後、以下の2つの場合に絞りこんだ。IETF後 ML上で投票中である。

1. cACertificate はドメイン内の CA から発行された CA の証明書や自己署名証明書を格納するのに利用する。crossCertificatePair の forward element にはドメイン外の CA から発行された証明書を格納し、reverse element にはドメイン外に対して発行した証明書を格納するのに利用する。

2. cACertificate はドメイン内の CA から発行された CA の証明書や自己署名証明書を格納するのに利用する。crossCertificatePair の forward element にはある CA に対して発行された全ての証明書を格納し、reverse element にはある CA が発行した全ての CA の証明書を格納するのに利用する（つまり、cACertificate は crossCertificatePair の部分集合になる）。

（6） では、IBM が PKIX のフリーウェアを出した（もしくは出す寸前）というアナウンスがあった。CMP、LDAP、CRMF などに対応し、C++ で書かれているとのこと。

http://www.imc.org/imc-pfl/

に ML の案内が書かれている。

（7）、（8） は、内容に関しての議論ではなく、今後も PKIX WG で議論するのが妥当かどうか、APP エリアにすべきかといった議論が行われた。結果としては、圧倒的多数で今までどおり PKIX WG で議論することに決まった。

（9）では、日本の ICAT （認証実用化実験協議会）の成果の1つをまとめる意味で筆者他が書いた I-Dの紹介について、筆者が発表した。内容はアプリケーションが CA を利用するための典型的なサービス（証明書発行、証明書や CRL の入手、証明書の有効性確認など）を Webベースで提供するためのプロトコルの提案である。発表の詳細は ICAT 関連活動編で述べる。

（10）は、CRL のための拡張フィールドの追加提案。例えば、1つのCRLサイズを小さくするために、CRL をシリアル番号の範囲ごとに分けて発行したり（10,000番までの CRL、20,000番までの CRL etc.）、証明書の Subject の文字列パターンごとに分けて発行するために範囲指定フィールドを設けようとするものである。
draft-ietf-pkix-ocdp-01 を参照。

（11）は、PKIX のドキュメントが増えて複雑になってきたため、全体を概観し、実装のアドバイスを含めた形で informational document としてロードマップを示す、という話。まだ I-D としては登録されていない。

（12）は、国際間でもディジタル署名の確認を合法的に行えるようにするための枠組を作ろう、という提案。スウェーデンの SEIS では、Proposed Standard profile for digital ID Certificate があるそうで、この活動を参考に PKIX の Certificate Profile にもう少し細かい制限をつけたり、ポリシをまとめていきたい、とのことである。印象としては、受けがよく、これから前向きに検討が進みそうである。

3. 所感

（1） PKIXの実装
今まで、PKIX の Sample Implementation がなく全体が見えにくかったが、ロードマップが出てきたり、IBM によるフリーソフトが出たことで、PKIX のメインプロトコルの実装が加速するのではないかと思う。しかし、どちらかというと CA 運用会社が中心となっている PKIX に関して、なぜ IBM 社が出てきたのかという背景はわからない（他の人に伺ってみたところ、IBM 社の（TV の CM でもやっている）e-businessの方針と関連があるのでは、という答えが返ってきてなんとなくわかった気がしているところである）。

（2） PKIXの発音
PKI は「ぴーけいあい」だがPKIX は「ぴーきぃくす」（「ぴー」にアクセント）と発音していた。前回 IETF に参加したときには気づかなかった。

（3） IPSEC、TLS、他のプロトコルの使い分け
IPSEC、TLS、SOCKS、SECSH などのセキュリティ関連プロトコルの使い分けや線引きについてはよく聞かれることである。IETF の各セッションでも少しはこの話題が出るが、あまり深い議論になることはなく、ひとまずそれぞれ独立に RFC にしてまとめていきましょう、となる。やはり、サービスを提供する側がある程度考えていく他なさそうである。

Ⅱ. ICAT 関連活動

今回の IETF に向けて、ICAT 広域認証技術TF（Task Force）の成果の1つである CA 運用パッケージ（ICAP）とアプリケーションプログラム（PEPOP）との連携プロトコルを I-D としてまとめる作業を行った。タイトルは、"Web-based Integrated CA services Protocol, ICAP" であり、ファイル名は "draft-sakurai-pkix-icap-00.txt" である。IETF の PKIX WG セッションにてこの I-Dの提案内容を発表してきたので、標準化活動の舞台裏という観点から報告する。

1. 背景

I-D は公開される期間が6ヵ月となっており、更新する場合はその6ヵ月の間に行うことになっている。実は、広域認証技術TFからは、今回の I-D の原型である "Web-based Certificate and CRL Repository" を1997年3月に提出しているが、更新しないまま公開期間が過ぎて振り出しに戻ってしまったという背景がある。今回の I-D は、実装する過程で最初の I-D に改良を加え内容をまとめたものであるが、タイトルやファイル名については最初の I-D の更新という形ではなく、新規に付け直さなければならなかった。
I-D には、WG ドラフト（draft-ietf-WG名 ではじまる I-D）とパーソナルドラフト（draft-個人名 ではじまる I-D）との2種類があるが、ドラフトを RFC とする近道は、まず WG ドラフトとしてから WG内で議論しまとめていくことである。しかし、あるドラフトがどのようなプロセスを経て WG ドラフトとして認められるのかは不明であったため、PKIX WG チェアに問い合わせたが、結局回答を得られないまま、パーソナルドラフトとして7月末に提出した。

2. PKIX WG セッションでの発表

提出した I-D の内容を 実際にIETF会議で発表

させてもらえるかどうかは、WG の状況に大きく依存する。PKIX WG のセッションは2時間半のセッションが2つ予定されており、チェアに発表希望を伝えたところ2つめのセッションで 10 分間もらえることになった（WG ドラフトの数が多いので無理かと思ったが意外にも大丈夫であった）。今回の目標は、標準化の過程に1歩近づくために「まず WG ドラフトとすることの合意を得る」と決めて臨んだ。発表資料は

http://www.icat.or.jp/presentation/PKIX98Aug

にある。

結果的にいうと、今回は ICAP を紹介しドラフトを読んでもらえるように宣伝してきた、というニュアンスにとどまり、議論には至らなかった。

現在、PKIX WGでは主要なプロトコルが収束しつつある状況である。これらのプロトコルではトランスポートを特定せず、またデータフォーマットは ASN.1 により厳密に定義されている。ICAP を提案することによって、証明書の発行、証明書やCRL の入手、証明書の有効性確認といった CA の典型的なサービスを全て HTTP 上で、しかも ASN.1 を極力使わない単純なフォーマットで提供するコンパクトなプロトコルに対してどのような反応が得られるかを期待したのだが、その場では反応が得られなかった。

ICAP の実装がある、と話したことに対しては、何人かが興味を示し、worldwide downloadable かどうかと質問された。現在の実装はすぐに worldwide に公開できる状況ではないため、積極的に宣伝できなかったことが非常に残念である。

Webベースのプロトコルは他にもあり、整理する必要があるのでは、というコメントがあった。これは次節とも大いに関係がある。

3. WebCAP 著者とのローカルミーティング

現在、ICAP と非常に似たプロトコルとして、WebCAP が提案されている。ICAP の I-D を提出する直前から、著者の Surendra Reddy氏とのやりとりをはじめたところ、両I-D のマージの可能性について関心を示してきた。

Reddy氏も IETF に参加していたため、会場で1時間程度のローカルミーティングを行った。ミーティングでは、主に両I-D の違いを確認した。大きな違いは、データフォーマット（ICAP は text/plain、WebCAP は XML）だけであるが、両者ともに譲れない点であることもわかった。CA 間連携の方式は、若干の違いがあるものの、基本的には ICAP が提案している referral モデルに賛成とのことであった。

両I-D をマージするかどうかについては結論が出なかったが、今後も電子メールで意見交換を続けることになった。

4. 今後に向けて

本気で標準化に持って行こうと思ったら、IETF の前準備が勝負であると痛感した。IETF に行く前に充分に作戦を練って長期的、かつ組織的に動かないと活動を進めるのは難しい。

ICAP の場合、活動母体である ICAT の活動の終了により、標準化活動としてICAT から内容を提案しつづけることは難しい状況になるが、逆に ICAT に閉じることなく、よりオープンに議論できる状況になるともいえる。名前も内容も非常に似た WebCAP については、I-D を出すまでは対抗案として意識していたが、PKIX 全体の中では、ICAP 支持案と捉えて一緒にまとめていく方が有利かもしれない（英語で議論することに関しても）。ただし、WebCAP とマージする場合には、現在の ICAP の実装とは切り離して考えることになるだろう。

今後どうするにしろ、今回の I-D は、ICAT に集まった技術者間の交流がなければまとまらなかった。この場をお借りして、ICAT 関係者各位に改めて感謝の意を表したい。

事務局連絡

会員サービス等の事務局業務は、1998年9月30日の解散をもって終了させていただきます。なお、研究開発した成果を普及するために、引き続き、当協議会実験諮問委員会の委員長を務めてきた、奈良先端科学技術大学院大学の山口助教授の研究室へサーバを移し、この３年間に蓄積したノウハウを、引き続き広く一般利用者に対して提供していく所存でおります。今後ともどうぞよろしくお願いいたします（技術情報を提供してきたドメイン：icat.or.jp、wwwサーバ：www.icat.or.jp の変更はありません）。