ICAT NewsLetter Vol,2

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

今　号　の　記　事

第37回IETF報告

TABLE OF CONTENTS

１．概要

第37回 IETF は、米国 California 州 San Jose の Fairmont ホテルにおいて 1996年12月9日から13日にかけて開催された。

２．PKIX-WG

報告者：菊池 浩明(東海大学)

PKIX-WGは PKI(Public-Key Infrastructure) X.509 に関するWorkgroupで、12/9(月)の午後のスレッドで行われた。アジェンダは次の通りであった。

・Part 1, status, update (Polk)
・Open group PKIX Architecture
　(Blakely@IBM/X-open)
・MISPEC update
・D-H certificate request message (Solo)
・Part 3 update (Farrell)
・Part 4, Certificate policy (Choknani)

2.1 Part1(Polk@NIST)

MLに流れた最新のドラフトの報告。主にPolkが概要を説明し、もう一人の著者がCRLについて補足を加え、BullのPikersがコメントを行った。主な変更点は次の通り。

・Cert、CRLのいくつかのシンタックスが変更された。 UTC Time の問題、 V3の UTC Time は UTC TimeとGeneralized TimeのCHOICEに置換された。現在から2015年まではUTC Timeを、2005年以降はGeneralized Timeを利用する。これによると2005年から2015年までは両方の表記が混在するため異議が出ていた。この数値は著者の判断によるものであり、厳密な意味はない。
・Part 4に関係する Policy Quantifierが追加された。新規はuser notice、CPS pointerの二つ。
・private extensionに新しく意味付けが行われた。
・CRLに新しく hold の仕様を加えた。
・いくつかのOIDが定義された（今まで未定義だったのが不思議）。RSAはPKCS、DESなどはANSI、KEAはSNN.701と706のものを利用する。
・実装に関するいくつかの要請がまとめられた。それによるとCAは V3 cert、V2 CRLを利用することができ、クライアントはv1、v2、v3 cert、v1、v2 CRLの全てをサポートしなくてはならない。加えてpath validationも対応するべき。拡張は例の９種類を全てサポートするべき。
・CRLのプロファイルも同様な変更が行われた。新しいところではisuring Distribution pointの拡張子が用意されたこと、差分CRLについては相互運用性を考慮して使ってもいいがフルCRLも同時に発行 するべきことが提案された。

2.2 Open group Architecture PKI-WG (Bob Lakley)

本WGに提出されたI-Dの説明。APKI-WG は X-openで行っている活動の一環であり、いくつかのコンピュータメーカから構成されている。このドラ

フトは技術論よりむしろPKIを実現していく上での要請をまとめたものである。詳しい情報はhttp://www.xopen.org/public/tech/security/pki/を参照。

この提案で特徴的なのはセキュリティ機能を分類し、OSIのような階層モデルを構成している点である。証明書に関する機能はLong-time key serviceと呼ぶ層に相当しており、その下に暗号化をサポートする層があり、その上にセキュリティプロトコルが来ている。こうすることにより、例えば輸出規制に関する暗号アルゴリズムの置き換えなども容易に行えると主張している。もうひとつの特徴は、キーエスクローやリカバリに対して肯定的であり、それらをサポートするための層が各層に対して貫くように横にまたがっている点であった。

また、CAに関しては通常のCAの機能をLRA、CAA、CA、PA(Publication Authority)の４つのブロックに分割している。CAAは、VerisignのClass3のように利用者からの要求に対してオペレータを介してオフラインで証明書発行を行うことを考慮して、CAとは別にしており、LRAとCAA間がオフライン、CAAとCAとPAの間がオンラインである。PAは、証明書の配布だけを専門に行うブロックである。

この提案に対して議論が爆発したのはもちろんエスクローであった。本題から脱線してほんとに必要なのか、エスクローとリカバリーの違いは何かに始まって、暗号鍵と認証鍵のどちらをリカバリーするのか（エスクローだと暗号鍵だけだが、リカバリというと認証鍵までを含むもの)。文書を暗号化して格納する鍵と通信に利用する鍵を区別しないでリカバリーするのか、さまざまな質問や提案や嘆きがあげられた。大方は米国政府に反対している。しかし顧客から要求されて仕方なくサポートを考えているという意見もあげられた。

その他には階層モデル自体についても、機能のいくつかは階層を超えて利用されるので、実装と一致しない のではないかという意見も多くあげられた.

2.3 Minimum Interoperability Specifications for PKI Components (MISPC)

NISTの W. Polkによる提案

NISTの CRDA(プロジェクト名)の活動として行われているもの。このグループはATTやBBN、VeriSignなども加わっている官民共同のものである。モントリオールでNSAのMISSIの提案があったが、それとも関わっている。企業ベースで行われているものと、政府の仕様との間で相互接続性を得ることを目的としている.

PKIXと大きく異なる点は次の通りである。

・PKIXは ITUの拡張であり、独自拡張がある。MISPCは部分集合であり、ITU からはみ出すものはない。その代わりに altName 拡張子に独自の意味付けをしている(issuerNameなども含む)。URLの代わりにURI(Uniform Resource Identifier)を採用している。これはURLをより一般化したものであり、リソースの内容を指すことで場所にとらわれないで識別できるものである。
・転送手段としてLDAP(Lightweight Directory Access Protocol)を採用していること、PKIX Part3の部分集合しかサポートしないこと。これは実装と相互接続性を容易にするためである。
・署名アルゴリズムとしてRSA、DSA、それにECDSA(楕円)を採用していること。ECDSAはANSIのOIDを利用している。
・certificate repository を明らかに用意する。基本的にはLDAPだが、FTPなどとの併用も出来るようにする。分散管理を行う。したがって、証明書の配布にはあるアドレスを決めておき、そこから辿れるようにする。CRLもここから入手できる。
・CRLはCA間の連携を図るために採用するが、オンラインの検証を行うCAがあってもよい。

ここでの議論をもとに、３月には改訂版を公開する予定である。NISTからの正式な公開は４月か５月になるとのこと。なお、著者のPolkはPart1の共著でもある。URLは
http://csrc.nist.gov/pki

2.4 Part 3. Certificate Management

S. Farawell と Notel の C. Adomsの提案。主にAdomsが報告していた。以前のドラフトとの変更点は次の通り。

・InfoReqという一般的な情報交換のためのPKImessageが追加された。
・POPO(Proof of possession of private/public key)というフィールドが追加された。これは証明書の再設定などの際、本当にその人が正しい鍵を持っているかを示すものである。具体的には乱数を送り、それに署名してもらうという手順をとる。public keyの場合はその鍵はどれだけのサイズがあるかを知ることができるため、輸出規制などに利用されるものである。
・DHBasedMac(上でのD-H)とPasswdBased Mac という

２種類のアルゴリズム識別子が定義された。秘密共有によるメッセージ検証であり、例えば証明書の登録のときなどに利用することが意図されている。
・エラーメッセージを返すことが追加された。
・転送手段としてSocketBased な方法が提案された。

これらはほぼIDに従っている。ところがFarawellが次の提案を行った。「PKImessageの秘匿性にPKCS7を、証明書の登録に PKCS10を利用してはどうか？」 PKCSの方が広く知られており、既存のプロトコルを使った方が実装もやさしいだろうということである。PKCS7に対しては、多くの賛成(反対は0だった)が得られていたが、PKCS10に関しては、すでに Part3で提案したものと矛盾することになり反対意見も出ていた。

2.5 Part 4 Policy

CygnaCom Solution社の Chokhani による提案。Certificate Policy と Certificate Practice Statement(CPS)の違いなどを詳細に説明していた。前者はポリシーを記述するためのテンプレートであり、後者は個々のサイト毎に異なる詳細を定めたものである。CPSを複数持つことも考慮されている。ポリシーに関する初めてのドラフトである。

次回のIETFでは、Certificate Storageに関するBOFを行うとのこと。場所などはMLでアナウンスされるとのこと。参加希望者は
certstorage-wg@consensus.com まで。

３．IPSEC

報告者：山口 英
(奈良先端科学技術大学院大学)

近年のインターネットの急激な広がりと利用の拡大によって、インターネット環境 におけるセキュリティ保全の重要性が強く認識されるようになった。ネットワーク環境 におけるセキュリティ保全の手法には様々なものがあるが、特にその中でも通信データ の暗号化の実現は多くの問題を解決する。

インターネットにおいては、これまで通信の 暗号化はアプリケーションによるサポートが一般的であったが、IETFでの長期間にわた る活動によって、やっとネットワーク層での暗号化を実現する標準が定められた。IETF のIPSECWGでは、IPデータグラムのデータ領域の暗号化フレームワークであるIPSECと、インターネット環境での鍵交換プロトコルであるISAKMPをそれぞれ標準化した。これにより、インターネットプロトコルにおける基本的な暗号化通信のフレームワークが確立したといえる。

しかしながら、暗号化通信が一般的になるにはまだまだ多くの問題が残されている。一つが、暗号方式にどのような機構を採用するかという点である。特に暗 号通信に関しては多くの国々において規制が存在しており、国毎に異なる規制と、国際的な通信基盤であるインターネットとの整合性をどのように確保するか考える必要が出てくるであろう。

もう一つの問題が、暗号化通信と認証機構との連携をどのように確保 するかという点である。この問題に関してはまだまだアプリケーションに依存する点が しばらくは多いと思われるが、安全性の高い通信基盤を考えた場合、2つの機構の連携を どのように行うかは十分に検討されなければならない。このようなことから、プロトコル の標準化は終了したが、まだまだ多くの研究開発が必要である。

４．S/MIME BOF

報告者：菊池 浩明(東海大学)

座長はRSADSI のJeff XXX（S/MIMEのIDの作者）。実証の状況説明からS/MIMEの紹介が行われた。新しい試みとして EDIへの適用やMessage Reciptsの提案を行い、最後に自由なスタイルでデモが行われた。発表は特に新規性は感じられなかったが、それより質疑応答が激しくて興味深かった。私が感じた範囲では、このBOFの意味は、今更S/MIMEを紹介することではなく、S/MIMEのMIME/TYPEにある ”X-”を早く取って欲しいことらしい。面白かった質問や気がついたことを次にあげる。

・相互接続性テストはすでに３回行われており、数社から集まったもののうち、相互接続性があったものについてだけ４社が報告されている。最も安定していたのは、Netscapeと Deming社のものである。
・PKCS-10は必須なのか？ そんなことはなく、他の方法を使うことは許されるだろう。
・証明書を検索したり入手スタイルする方法はディレクトリシステムを使う。
・x-pkix7-signatureは “ detached signature ”と呼ぶらしい。
・S/MIMEはPKCS7の部分集合であり、実装を容易にするためのprofileである。
・S/MIMEでは証明書を省略することが許されており、X.509に縛られているわけではない。

こうして狭い会場に立ち見が出るほど盛り上がっ

てBOFは終了した．これがstandard trackに乗るかどうかはまだわからない．

５．PGP/MIME　BOF

報告者：歌代和正
(株式会社ｲﾝﾀｰﾈｯﾄｲﾆｼｱﾃｨﾌﾞ)

まず、Charles Breed から PGP/MIME の状況に関する報告があった。この中で彼は、PGP/MIME の標準化が必要であること、そのために IETF のワーキンググループを構成することが要求されることなどについて述べた。ミーティング に先だって RFC 2015 - MIME Security with Pretty Good Privacy (PGP) がリリースされており、これを元にして IETF の標準化のプロセスを開始するために、ワーキンググループを構成することが提案された。

続いて、著者である Michael Elkins から、RFC 2015 の概要が説明された。 彼は、インターネットのメールシステムに PGP を採り入れるための標準が必要であることを説き、先にリリースされている RFC1847 - "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted" と PGP の関係について説明した。

Elkins 氏による概要に続いて、RFC 2015 に関して、セクションを一つ一つ追う形で議論が行われた。細かい言葉遣いも含め詳細に意見が交わされたが、特に焦点となったのは認証に使われるアルゴリズムに関することで、MD5 と SHA-1 をどのように扱うかということについて、一応の結論が得られた。また、 認証を行うためのテキストを正規化する手続きについて、日本語処理に関する問題点の指摘が、奈良先端科学技術大学院大学の山本和彦氏から行われた。彼は、いわゆる新 JIS と旧 JIS の異なるコードが混在して利用される日本の状況に ついて説明し、メールの送受信の過程でコードが変更されても正しく認証を行うためには、特殊な正規化が必要であることについて主張した。

その後は、現在存在する PGP/MIME の実装に関するデモンストレーションが行われた。この中には Raph Lavien の "Premail"、Michael Elkins による "MUTT" に加えて山本氏の "MEW" の実装が含まれる。この他、EPPI と PGPClick という実装の紹介があった。

今後の方向性としては、PGP/MIME ワーキンググループを構成し、IETF による 標準化を目指すことで合意が得られ、1997年半ばを目標に標準化に向けての動きが本格化することになる。

事務局連絡

ー報告書配布のお知らせ

- **「暗号アルゴリズムの設計と実装」（５月）**
- **「米国暗号関連の特許登録情報」（５月）**
- **「暗号・認証技術の研究開発に関する動向調査」（６月）**

お問い合わせ先

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）
〒105　東京都港区芝公園３丁目５番８号
機械振興会館内
TEL: 03-3432-9387　FAX: 03-3432-9419
E-mail: info@icat.or.jp
URL: http://www.icat.or.jp