ICAT NewsLetter Vol,1

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

事　務　局　連　絡

第36回IETF報告

―分岐点に立つセキュリティ基盤の標準化―

インターネットの標準化を進める第36回インターネット技術者会議IETFが，6月24日より5日間カナダのモントリオール，コンベンションセンターにて開催されました．広域環境に広く適用可能な認証盤を提供しようとする本協議会にとって，国際的な相互接続性を図ろうとするIETFの活動は重要です．そこで，同会議に参加した数名の専門家に各々の分野の動向を探ってもらいました．インターネットにけるセキュリティ基盤がどのような形に進んでいくのか，これらのレポートからその姿が浮かび上がってきそうです．

TABLE OF CONTENTS

1. Overview

報告者：菊池浩明（東海大学）

第36回IETFは，6月24日より5日間カナダのモントリオール会議場で開催された．今回はインターネットソサイティ主催のINET96との合同開催であり，どちらの参加者も互いの会議に出席できることが許されている．そのため，総勢3500名の通常より大規模な会議となった．端末室もMac, Windows, Unix入り交じって300台が一室に設定され，相互連絡や資料集めにしばしば活用されていた．何台かPower Pointがインストールされたマシンと OHPシートの入ったプリンタも提供されており，その場で発表の資料を作ることも出来る（私もお世話になった）．

開催国のお国柄か，INETの全てのセッションについてフランス語の同時通訳がサービスされていて，逆に，フランス語でのスピーチも許されていた．ただし，これは残念ながらIETFについては行われなかったINETによるものだが，会場の一階で展示会も開かれていた． TVなどのPressが多く取材に来ていて，カナダでのインターネットの盛り上がりを感じた．日本人も何人か捕まって取材されていた．

会場のモントリオール会議場は地下鉄の駅に併設されており交通の便がよく，夜遅くでも安全に出歩くことが出来た．チャイナタウンや旧市街が近く，食事のバリエーションにも困らない．

2. PKIX（Public-Key Infrastracture with X.509）

報告者：菊池浩明（東海大学）

PKIX WGは，6月25日の午前と午後の第一セッションで開催された．主な議題は次の通り．

1. Introduction
2. ISO X.509 Update
3. PKIX Part 1 (Certificate and CRL Profiles)Review
4. PKIX Part 3 Management Protocols Review
5. DoD Management Protocols
6. Japanese PKI Report
7. ASN.1 Documentation
8. Validity Periods
9. Reference Implementations & Conformance Testing

大きなニュースは３つある．一つは，ISOで進めている公開鍵証明書X.509バージョン3(V3)の仕様がほぼ固まり，名前空間の点においてOSI離れが進んだことである．これに伴い，本WGで標準化しているプロファイルも最終段階に来たが，ここでインターネット独自の証明書拡張が提案されたことが，二つ目のニュースである．そして最後のニュースは，当協議会の活動紹介と開発成果物の一部のデモが行われたことであろうか．以後，各々について報告する．

2.1 ISO X.509 Update

Northan Telcomの Warwick Fordが7月1日に行われた ISO/IECの X.509標準化動向を報告した．

大きな変更点の一つは，criticality-based changes と呼ばれる属性である．（常に）critical，（常に）non critical，（CAの選択により） critical/non criticalの三種類が提供される．この修正に伴って，今までのOIDも更新される点に注意がなされた．

また，識別名の領域に今まではOSIのDN名しか許されていなかったのが，General Name(すなわち，URL，IPアドレス，OIDなど）を置くことが許されるようになった．（思わず拍手がわいた）

Indirect CRLもここで新しく加えられた機能である．これは，あるCAに属するユーザのCRLを他のCAが代理で発行する機能であり， CRLの発行手続きを簡略化する効果がある．しかしながら，ひとつのCRLの中に複数のCAのCRLが混在することになり，どのCAのものなのか識別するための情報が導入されることとなった．他にも "Hold"の機構や差分CRL，名前の厳密なマッチング規則などの修正が行われた．なお最新のドラフトは，ftp://NC-17.MA02.Bull.com/pub/OSIdirectory/Certificatesにある．

2.2 PKIX Part 1 (Certificate and CRL Profiles)Review

SpyrusのRuss HousleyによるPKIX Part 1のドラフトについての提案と議論である．

重要なのは，このドラフトがX.509の拡張のうち13だけをプロファイルとして採用することと，証明書について3つ， CRLについて4つのそれぞれインターネット独自の拡張をしようということである．前者についてはこれまで報告されたものから今回のcriticalなどの属性の拡張が振られただけなのに対し，後者はOSIの枠からはみ出すものである．互換性を保証しないわけで，会場から活発な賛否両論が寄せられた． これらの Internet Extensionは，主にアクセスの方法（information Access)を記述するものであり，ほぼ OIDと GeneralNameの組で構成される．証明書については，Subject,Authority, CAの3種類， CRLについては， Status, Retrival,Policy, Certificateの４種類がこの拡張で与えられる情報である．CAとAuthorityを分けたのは， Indirect CRLをサポートするためである．

ICATで提供しているホームページのCA treeで定義している 1. CA, 2. CA Policy, 3.CA certの情報は，ここでの拡張するべきと提案されているものにそのまま対応しており，アクセス手段の提供を重要視している点で彼らの主張と同意している．

最後に，CharのSteve Kentから，本ドラフトは既に提案の形を整えているので WGメンバーからのMLでのコメントが要請された.

2.3 Japanese PKI Report

ICATのHiroaki Kikuchiによるもの．これまでの日本のPKIに対する取り組みとして，WIDEプロジェクトのFJPEMと，ICATの目的と成果が報告された．これに対して，次に示す質問が挙げられた.

・証明書発行頻度と廃止リストの頻度について
・秘密鍵の生成について
・暗号化アルゴリズムについて
・暗号タスクフォースで計画している暗号化ライブラリについて
・日本における信頼の鎖の大きさの試算について

なお，本WGに関しては次の参考資料がある.

Steve Kentによる議事録
ICAT Demonstaration Trans. (Postscript, 600k)
ICAT Presentation Trans. (Postscript, 3.5M)

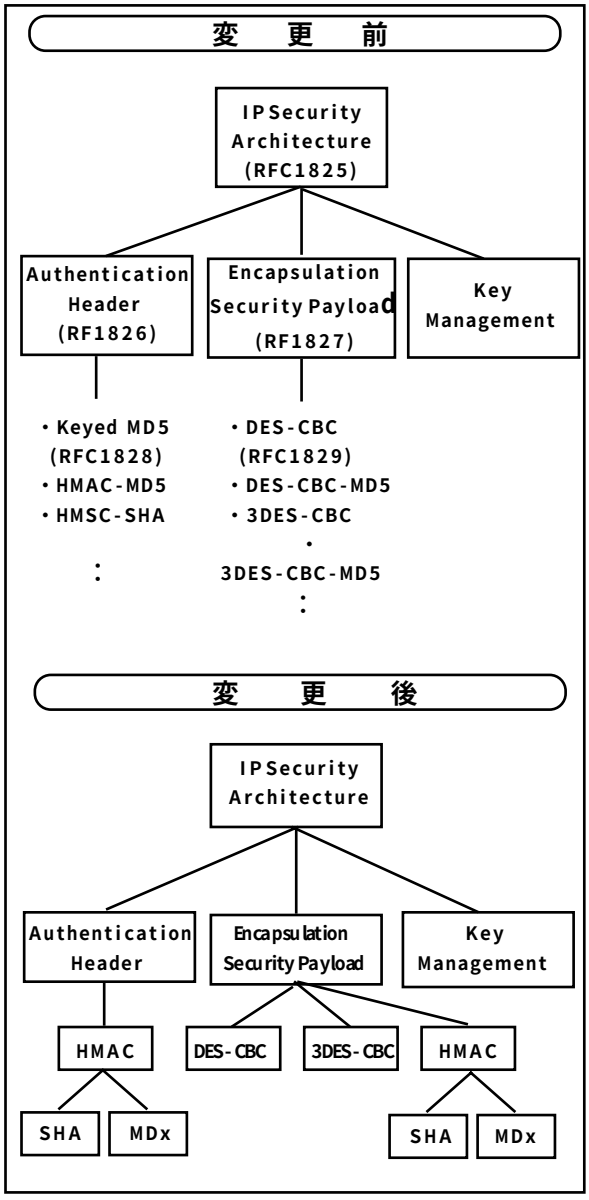
3. IPSEC（1）(IP Security WG)

報告者：寺田真敏（日立）

3.1 IP層におけるセキュリティ体系

インターネットにおけるIP層のセキュリティを向上させるため、 RFC(Request ForComments) 1825からRFC1829において、 IP層のセキュリティ体系、メッセージ認証、暗号化方式の標準化が進められてきた(図1 変更前)。今回、メッセージ認証で使用する関数取り扱いの一般化、同じくメッセージ認証におけるリプレイ攻撃対策、暗号化方式での完全性保持情報付加等の方式の改善、多様化から、体系の見直しとこれに伴うRFCの改訂作業が進められることとなった(図1 変更後)。

（図１）



3.2鍵管理方式

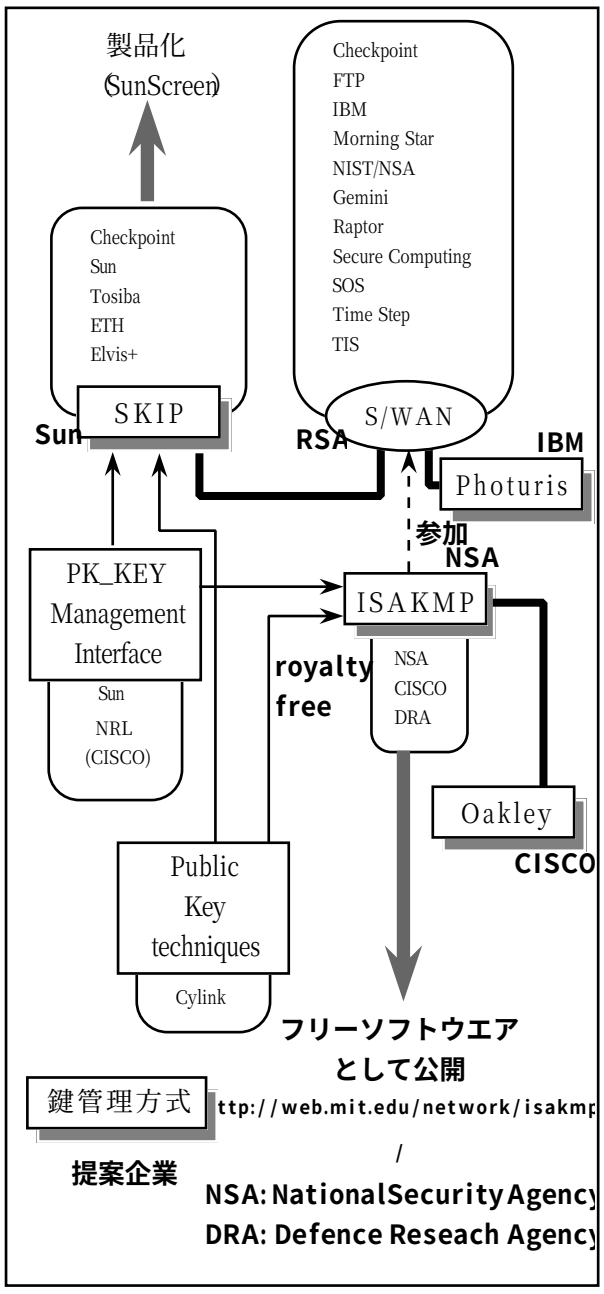
今回のIETF IPSecにおいてもっとも議論の対象となった項目が、 IP層セキュリティにおける鍵管理方式であり、以下の発表が行われた。

・SKIP(Simple Key-Management For Internet Protocols) Updata Tom Markson(Sun)
・ISAKMP (NSA)
・Oakley status Hilarie Ormun
・The resolution of ISAKMP with Oakley D.Harkins
・Comments on Oakley Peter Williams
・Comments on Oakley
－isakmp Hugo Krowczyk

現在、鍵管理方式としてSKIP,Photuris,ISAKMP

(Oakley:ISAKMPのCISCO版)の3方式が提案されているが(図2)、標準化の対象はSKIP,ISAKMPに絞られつつある。発表はSKIP,ISAKMPの良さを互いに強調することに終始し、 IPSec参加者の議論の対象は、 IETFでの標準化がすなわちインターネット標準となることから、鍵管理方式がどのように決着するか(SKIP/ISAKMP/折衷案?)に向けられた。最終的に、この場では今後の方向性は示されなかった。

（図２）



鍵管理方式の方向性については、後日開催されたsaag(Open Security Area DirectorateMeeting BOF)において、 SKIP, ISAKMPが相互に協調しながらIPSecにおける鍵管理方式の確立を進めていくこととなった(9月に最終的な方向性が決定される模様である)。

なお、実装面ではSKIPが先行しているが、規格としての汎用性はISAKMPが優位である(ISAKMPは、TLS(Transport Layer Security WG)における鍵管理方式としても提案されている)。また、ISAKMPの提案元であるNSAは ISAKMPの枠組みの中でKey Escrow機構の取り扱いをも考えている模様で,インターネット上の暗号技術における主導権獲得が見え隠れしている.

4. IPSEC（2）(IP Security WG)

報告者：室田真男（東芝）

IPSEC-WGは 2つのセッションが行なわれ，1つのセッションが鍵管理プロトコルに関する議論にあてられた.

現在 IPSEC-WGからは，SKIP(Sun社), ISAKMP(NSA)， Oakley(Arizona 大)， ISAKMPwith Oakley(CISCO社)の4方式が提案されている．このうち，ISAKMPと Oakleyは統合化が進み，実質的には SKIP(Sun社)と ISAKMP/Oakley(CISCO社)の２方式．なお，Photuris(Qualcom社)は，前回(3月)のIETF会合後 IPSEC-WGからは，はずれている.

まず，各方式の概要と実装状況の簡単な紹介があった．以下に実装状況をまとめる.

SKIP(draft-ietf-ipsec-skip-06.txt)
by Ashar Azis(Sun)

IETF前に SKIP Developers Workshopを開催し，相互接続実験を行なった． 5ヶ国から5つの独立な実装(SUN社， 東芝， イスラエルCheckpoint社，チューリッヒ工科大学，ロシアElvis+社)が参加.
http://skip.incog.com/ISAKMP(draft-ietf-ipsec-isakmp-05.txt) by Douglas Maughan(NSA) 現在の実装は，CISCO社，Defence Research Agency(UK)の2つ.
Softwarerelease用 Webサイトは，
http://web.mit.edu/network/isakmpOakley(draft-ietf-ipsec-oakley-01.txt) by Hilarie

Orman(Univ. of Arizona) ISAKMPとの統合作業がほぼ完成した．実装はアナウンスされていない．
ISAKMPwithOakley(draft-ietf-ipsec-isakmp-oakley-00.txt) D.Harkins

(CISCO)
ソースコードが，
http://www.cisco.com/public/library/isakmp/から得られる．

その後，IPSEC-WGとして，一つの方式に決定するか，複数の方式を標準としデファクト化はマーケットに委ねるかの議論が行なわれたが，会場での挙手によるアンケート結果や議論はほぼ半々に別れ，結論は出なかった．結局，翌日のSAAG-BOFにおいて，エリアディレクタから，各方式の著者が共同作業することに合意したこと，そのdeadlineを 9月1日とすることが，アナウンスされた．

その他のトピックスを以下に簡単に示す．

IPsec Architecture Documents
by Ran Atkinson(CISCO)

現在，RFC1825-1827の revise版がInternet-Draftになっているが，6ヶ月後にDraft Standardに，1年後に Full Standardにする予定であることを発表．RFC1828,1829は，Historicとする．

Open Work Items
by Stephan Kent

現在のRFCでは，AHと ESPの組合わせは非常にフレキシブルにできるようになっているが，組合わせ方法を規定して実装を容易にしようというコンセンサスが得られた．

IPsec and Firewalls
by Michael Richardson(Milkyway Networks)

いかにして Firewallを越えてエンドホスト間でAuthenticationされた通信をするかということについてのドラフト紹介
(draft-richardson-ipsec-aft-00.txt)．

S/WAN Status by Brett Howard(RSA)
S/WANは，RSA社が行なっている IPSEC相互接続試験のためのフォーラム．
現在11社が参加している．S/WANへの参加呼び掛けが行なわれた．S/WANの詳細は，http://www.rsa.com/rsa/SWAN/を参照．

Near Term Deployment by John Gilmore
DNS Key Distritution，Key management，IPSEC packet processing，IBM PCベースのCryptowall(Gateway/Firewall)のソフトウェアを，フリーソフトとして今年の夏に公開するとアナウンス．

5. TLS WG（Transport LayerSecurity）

報告者：山口英（奈良先端科学技術大学）

TLS WGは、前回（1996年3月）との間に設立された新しいワーキンググループである。このワーキンググループの名前からは、TCPあるいはUDPなどの既存のトランスポート層プロトコルに対してセキュリティ機能を付加する方法を議論するワーキンググループのように思えるが、実際にはTCPやUDPには変更せずに、トンランスポート層の直上に付加されるセキュリティ層を考え、その層で実現されるべき機能とプロトコルを標準化するものである。これは、ネットスケープ社などが展開しているSSLや、マイクロソフト社が展開を進めているPCTなどの、トランスポート層の直上に用意されるセキュリティ層が幾つかマーケットに登場してきたために、その標準化を行おうとする気運が高まり、このワーキンググループが結成されたのである。

今回のミーティングでは、今後の活動方針と全体のデザインが報告された。このワーキンググループでは、 1996年末までに標準化作業を完了させることを目標としている。今回の会議では、現在マーケットに出回っている幾つかのプロダクトの中で、SSL Ver. 3.0をベースにして標準化を進めていく方針が発表された。 SSLは現在マーケットで広く使われており、これに現在のPCT独自の機能を持たせるようにした方が、標準化作業後のマーケットへの標準の浸透がすばやく行える事を期待していることから、このような方針になったのである。このため、標準化作業としては、現在のSSL Ver. 3.0に対して幾つかの拡張を行うことになる。この拡張について幾つかの議論があった。

それ以外に関連する発表としてSSH (Secure Shell: 詳細はhttp://www.ssh.fiを参照)と、IPSEC WGが開発している鍵管理機構でのプロトコル ISAKMPについての発表が行われた。

このようなワーキンググループができプロトコルの標準化が行われる事で、現在SSLや PCTを用いているセキュリティアプリケーションの相互操作性が増し、インターネットのセキュリティ保全を考えた場合により良い状況になると考えられる。

6. RSVP (Resource Reservation Setup Protocol WG)

報告者：塩野崎敦（ソニーCSL）

rsvp WGのミーティングは，6月24日の夜と26日の午後のセッションに開催された．今回は，RSVP Version 1のドラフトの完成も間近になってきたということから，各ドラフトの進行状況の報告，および Version 2の発展方法に関する議論が行われた．したがって，細かい技術的な話は少なかった．取り上げられた主なテーマを以下に示す．

- ドラフトの状況
- 実装の状況
- 新しいWGチャータについて
- RSVP Version 2 について

まず RSVP Version 1を proposed standardにするためにはセキュリティのサポートが必要であることが指摘され，RSVPスペック，MD5 Integrity Objectスペック，RSVPIPsecスペックの3つがIESGにパッケージとして近々提出されることが報告された．

各組織の RSVPの実装状況の報告も行われた．Bay，CISCO，IBM，Intel，Sunからの報告があり，組織によっては早くても今年の9月には製品化される予定がたてられている．ISIからは RSVPスペックの ID12をベースにした 4.0a4というリリースが現在配布されている．

ドラフトの現状報告としては，MIB関係，および診断メッセージの発表が行われた．また，RSVP Version 1が完成しつつあるので， WGとしてはここで新たなチャータを作成する必要があると合意され，更に診断メッセージ，トネリングサポート，アクセス制御機構およびフレームワーク，RSVP Version 2のドラフトを作成し承認されるまでのスケジュールがたてられた．また，先行予約(近い将来のために資源予約を今行うこと)の概念もチャータの中に含むべきか議論されたが，決定はされなかった．

二日目のセッションでは，Version 2で取り上げるべき機能について議論された．具体的な提案などの話は少なく項目が列挙されただけだったが，簡単にまとめると，まずIPv6サポートに関しては，router alertドラフトの更新，フローラベルの使い方，RSVPチェックサムの取り扱い，ドキュメントの構成 (IPv6用の RSVPを別の文書にすること)などが挙げられた．また通信経路の最大 MTUの決定方法，セッショングループ，モービリティ，トネリング，QOSPFと RSVPとの関係，アクセス制御およびアカウンティングなどについても議論が行われた．特に，アクセス制御およびアカウンティングに関しては，ローカルポリシモジュール(LPM)を導入して取り扱う．LPMのドラフトは，3つに分割され，今後は RSVPに必要な拡張に関するドキュメントに重点がおかれる．拡張には，Reservation Reportという新たな RSVPメッセージの追加，またRSVPとポリシとのインタフェースの規定などが挙げられている．

7. ION (Internetworking over NBMA (Non Broadcast Multiple Access) WG

報告者：塩野崎敦(ソニーCSL)

Internetworking over NBMA (Non Broadcast Multiple Access) WGは， 6月24日の午後に1回と25日の午後に2回と合計3つのセッションで開催された． ion WGは，同じような問題を解決するために活動してきた ipatm WGと rolc WGを合併させ，新たに作成された WGである．今回が始めての集まりで，最初のセッションでは，現状の報告，NHRP， RFCの更新などが取り上げられ，第2セッションでは IPv6，第3セッションではマルチキャストに関する議論が行われた．

最初のミーティングでは，NHRP Rev 8の報告，および Rev 9に向けて必要な変更点，サーバキャッ

シュ同期プロトコル(SCSP)，RFC1577の更新，IP用のATMシグナリングサポート(RFC1755アップデートにUNI4.0を導入すること)などが取り上げられた．

第2のセッションでは，IPv6 over NBMAの発表が主に3つ行われ， ATMにおける IPv6のリンクの定義，IPv6 neighbor discoveryの実現，NHRPとの統合に関する議論が行われた．結論としては，3つのドラフトは細かい所に相違があるだけで，基本的には似ている提案なので，今後は1つのドラフトにまとめられる方向に決まった．

最後のセッションでは，MARSにおいて複数のマルチキャストサーバを導入する方法の提案が発表され， これを耐故障性，およびロードシェアリングに応用する方法についても議論が行われた．また，MARSと SCSP同一の枠組で利用する方法に関する発表も行われた．非ATM NBMAネットワークにおいて MARSを利用する方法に関する議論も行われ，これは新たなionのチャータ作成のために利用されるかもしれない．MARS MIBに関する発表も行われた．最後に，マルチキャストのスケーラビリティに関する問題について議論が行われた．

8. Intserv (Integrated Services) WG

報告者：塩野崎敦(ソニーCSL)

intserv WGは，6月26日の午後に開催された．intservでも，proposed standardとして用意しているドラフトスペックを近々 RFCにするためIESGに提出する予定である．そこで今後は，既存の proposed standardの実装経験などを活かし，レビューされるまで新たな standard-trackサービスを提案することは休止する方向であることが明らかにされた．

その後は，各ドラフトスペックの簡単な状況説明が行われ，更に再構成されたGeneral Parametersのドキュメントに関する議論が行われた．現存するテーマの議論は以上で終了した．

最後に，新たに committed rate serviceの提案が発表された． Commited rate serviceとは，経路上の各ネットワーク要素が必ず要求された最低限の転送レトを提供することを約束(committ)するというサービスである．基本的には guaranteedとcontrolled-loadの中間に当たるサービスであり，指定した TSpecの値を越えることなく，バーストトラヒックを流す必要のないアプリケーションを対象にしている．しかし，発表後の議論では既存のサービスとの違いが明白ではないことが指摘され，結局結論はでなかった．

会場となったモントリオールコンベンションセンター

公開鍵証明書発行局パッケージおよび，メッセージ暗号化署名ツール公開のお知らせ

認証実用化実験協議会(ICAT)では，インターネットにおける認証基盤を構築する試みとして，認証ソフトウェアを開発しました．今後，これらを元に認証技術の実証実験に移る計画です．これらはフリーソフトとして公開します。ご自由にお試しください．

インターネットに初めての個人認証を提供しようとする実証実験に参加してみませんか？

1. ICAPとは何か？

ICAT Certification Authority Package， すなわち，公開鍵証明書を発行する発行局(CA)を立ち上げるてためのパッケージソフトです．例えば，商用ネットワークプロバイダや大学などの学術組織などの管理者によって運用されることを想定しています．

ICAPはWebベースのインターフェースが特徴的で，CAの立ち上げから，管理者による手動

の証明書発行，ユーザによる自動の証明書発行までをWebブラウザから行うことが出来ます．

証明書形式はX.509V1，暗号化アルゴリズムはRSAを，証明書登録形式はRFC-1424を用いています．

2. PEMCATとは何か？

RFC-1421, 1422, 1423で標準化されている暗号化電子メールの形式Privacy Enhanced Mail (PEM)に従ってメッセージの暗号化や電子署名を行うツールです．ただし，本バージョンには電子メールソフトへのインターフェースは含みません．
Windows, Macintoshの標準的なGUIを採用しています．

暗号化にはDESとRSAを，電子署名にはMD5とRSAを用いています．

3. 入手方法

・PEMCAT V1.2 Macintosh版(68K, PPC)
・PEMCAT V1.2 Windows95版
・ICAP V1.0b (SunOS 4.1x版)

※上記ソフトウエアの使用条件（ファイル名は'Copyright'）をご利用される前に参照して下さい．

※ これらのソフトはいずれも，ICATホームページの研究開発成果のページ
http://www.icat.or.jp/pages/p6.html
よりFTP出来ます．バグ，バージョンアップなどの情報は，引き続きこのページより行いますので注意していてください．

※また，ICAPのデモンストレーションを行うパイロットCAが，
http://www.icat.or.jp/pilot-ca
で試験運用しております．ここでは，PEMCATのユーザ向に試験用の証明書を発行しております．

4. 問い合わせ先

広域認証タスクフォース： interauth@icat.or.jp

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: 03-3432-9389
E-mail: icat-adm@icat.or.jp

事務局連絡

―定例研究会のお知らせ

平成8年11月26，27日機械振興会館（地下3階会議室）にて，下記の定例研究会を開催します。参加手続，プログラム等の詳細は別途ご連絡致します。

暗号技術に関するワークショップ
「暗号アルゴリズムの設計と評価」

―ＩＣＡＴホームページのお知らせ

ホームページのデザインが変わりました。内容も大幅に追加されています。ご参照ください。

http：//www.icat.or.jp