ICAT NewsLetter Vol,3

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

IETF（Internet Engineering Task Force）とはInternet上のプロトコルをどのようにするか、議論をするTFであり、各カテゴリー毎にWGを作りI-D（Internet-draft）という規格のドラフトを作成する。これが諮問機関のIESG（Internet Engineering Steering Group）でRFC（Request for Comments）として認められると実質上の標準となる。

I. 第38回IETF会議報告

報告者：菊池 浩明（東海大）

期間：1997年4月7日（月）～4月11日（金）
会場：アメリカ〔メンフィス〕 Peabody Hotel

第38回IETFは2000人を超える参加者であった。ホストはFedexで宅配便の封筒を資料入れに配っていた（これをタダで送れるといいのだけども）。会場のPeabody Hotelは歴史を感じさせる重みのあるホテルである。

なぜか毎日午前11時にファンファーレと共にカモがエレベータから赤いカーペットを渡ってロビーの噴水にやってくる。夜ちゃんと帰って行くようである。

1 PKIX

PKIXは4月7日、8日の2つのスロットで行われた。座長の一人の Steve Kent さんはお休みで、VeriSignの Warwic Ford さんが仕切った。アジェンダは主に次のようなものであった。

・PKIX Part1. Profile
・PKIX Part2. Operational Protocol　【New】
・PKIX Part3. Management
・PKIX Part4. Policy
・Web based Certificate and CRL Repository
・New extension: Key Purpose
・Access Description
・Key Storage
・Time Stamping, Notary

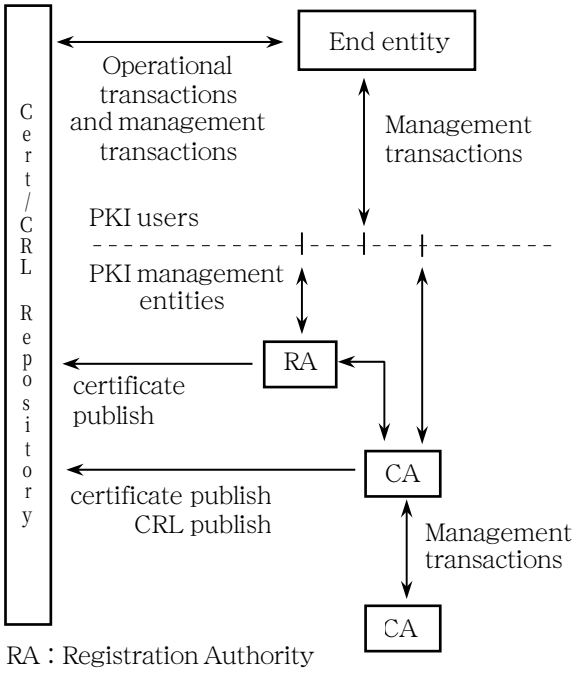

図 1 – Internet PKI Entities
(draft-ietf-pkix-ipki-part1-05.txtより)

1.1 Part 1. Profile

T.Pork（NIST）

４番目のドラフトであり、ほとんど安定してきた。大きな議論もなく、コメントを２週間待った後、Proposed Standard として提出する予定であるとのこと。いわゆる“lastcall”である。ただし、

今回の会議へのI-Dは間に合わなかったので、Webで公開するとのこと。前にアナウンスしたURLからは入手できなかった）。

San Joseでの議論から主な変更点は次のようなものである。

- ・only 2 private extension（caInfoAccessがなくなった？）
- ・不評の sliding window for time encoding（20aa年～20bb年の間、二つの符号化が混在する）は廃止された。
- ・alt name への URI が導入された（証明書を指す）。
- ・CRLdist.point へも URI が導入された。
- ・Online validation serviceのための URI が導入された。
- ・Cylink社の特許が記載された（RSAはまだ触れていない）。
- ・ASN.1の EXPLICIT/IMPLICIT の問題が正された。
- ・KEA の定義が明確にされた。

未解決の問題は次の通り。

○ASN.1 '88版 と '93版があり、どちらを使うべきか？ （これは翌日T.Pork自身は互換性のため'88版を使うべきだという補足があった）

○KEAアルゴリズムそのものについての参考文献Warwickによると、Part1はまず、問題無くRFCとなるだろうとのこと。ただし他のシリーズは、まだ議論が必要である。

1.2 PKIX Part 2. Operational

S. Boeyen（Notel）

特徴は次の通り

- ・LDAP Profile
- ・FTP Profile
- ・Online Certificate Status Checking（OCSC）
- ・LDAPによる Name、Cert、CRLの読み込みと、emailaddressなどの検索。

FTPは匿名FTPによる配布。".cer", ".crl" という拡張子のファイルに証明書のBERのバイナリを格納したファイルが直接入る。HTTPについての標準化案も含まれているが、この後でリリースされた“*Web based Certificate Repository*”との調整が必要である。

私からの、アドレスによる検索はプライバシ侵害を引き起こす可能性があるのでは？、という指摘に対して、リクエストをLADPに転送するだけでLDAPが責任を取る問題であるというスタンスを表明した。

1.3 PKIX Part3. Management

C. Adams（Nortel）

Stephan Frawelは欠席（ICETELが忙しいのか？）これも30分の遅れでI-Dのcut offdateに間に合わず。

主な変更点は

- ・PKCS#10（certificationRequest）が新設された。
- ・bootstrapping時における PKCS message が用意される。

ことである。

1.4 PKIX Part4. Policy

S. Chokhani（CygnaCom Solutions）

前回の議論を元に、ドラフトの書き換えを図っている。Certificate Policy（ポリシーを定めるための枠組み）とCertification Practice Statement（ポリシーの実例）の違いを強調していた。

主な質問

- ・Pinkersより、既存のドラフトとの関連を明確にすることが要求された。例えば、Part 3で述べられているPublishing Authorityの概念がPart 4には全くないようである。

1.5 Web based Certificate Repository

H. Kikuchi（Tokai Univ）

Firewallを想定し、HTML言語を利用したRepository案。

例としては以下の通りである。

```
(draft-kikuchi-web-cert-repository-00.txより)
   POST IAP/queryType HTTP/1.0
   name1=value1&name2=value2&…&namen=valuen

   HTTP/1.0 200 OK
   Date: Wednesday
   MIME-version:  1.0
   Content-type: text/html

   <HEAD><TITLE>queryType</TITLE></HEAD>
   <BODY>
   <H3> statusCode</H3>
   <H1> statusMessage</H1>
        information
   </BODY>
```

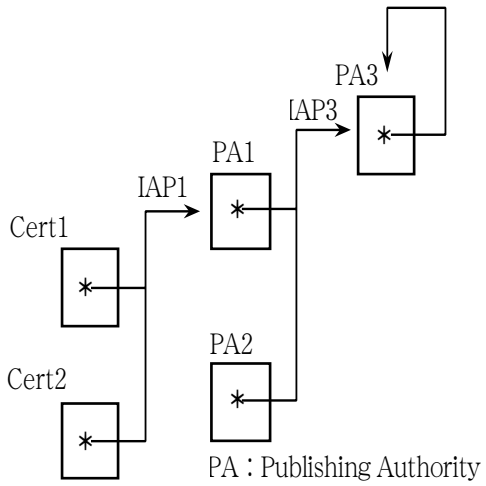

図2：Example of PAs hierarchy

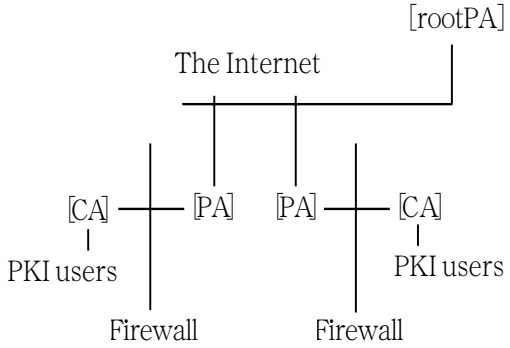

図3：Relationship between PA and CA

詳細は
ftp://ftp.icat.or.jp/pub/interauth/draft-kikuchi-web-cert-repository-00.txt
を参照のこと。使用した発表資料も
ftp://ftp.icat.or.jp/pub/interauth/PKIX97Mem.ppt
に置いてあるので参照のこと。

これに対して次の質問とコメントがあった。

・subject info access が不要ということだが、証明書が破棄された時はどうするか？（Russ, Houslyから）
→Authorityが代わりに配るのでよい。それがPart 1でこの拡張子を導入した理由らしい。

・PKIX Part2とは独立に用意されたので、多少冗長なところがある（T. Porkから）。
→いずれ調整したい。

・HTMLがhuman readableという提案だが、それは同意しかねる（T. Porkから）。

・HTML encodingはBERに比べてどのくらいサイズが大きくなるのか？
→まだ計っていない。

1.6 秘密鍵の格納に関して
C. Allen（Consensus Development）

あるアプリに使った秘密鍵を別のアプリで利用するにはどうしたらよいか。この問題に対する標準には次の二つが知られている。

・Microsoft PFX. PKCS#12に基づくバイナリ
・ASCII Armor. PKCS#5,7,8 + Base64 で表現

この標準化についての議論を次で行う。

```
<certstorage-wg@consensus.com>
subject=subscribe
```

1.7 その他

・Time stamping/notaries の活動を、このWGでやるかどうかわからないが、プロトコルを決めたいので希望者はAdamsに知らせてくれとのこと。

・93ASN.1は、互換性を重視するために捨てたい（T. Pork個人的に）。

・CRLの圧縮に関するPart 5のドラフトを考えている。

・それはスマートカードに格納するのにいいのでMLで議論したいとのこと。

・Key Usage は8ビットしかないので様々な利用、例えば、PGP用やPEM用に利用するために次の提案をしたいとのこと。

```
Key Purpose ::=  SEQUENCE OF OID;
```

Key Usageには輸出規制をかけるためにもなくては困るので

```
Key Usage ::=  SEQUENCE {
               KeyUsage       BitString,
               SEQUENCE OF OID Optional
               }
```

多くの同意が選られた。ISOへの提案も同時に行うことにする。

・Access Descriptionに圧縮などのアルゴリズムを入れたいので format という属性を加える提案。デフォルトはPKIX2とすればよい。

II. 第39回IETF会議報告

期間：1997年8月11日（月）～8月15日（金）
会場：ドイツ〔ミュンヘン〕Sheraton Hotel

報告者：北野　博之（ICAT事務局）

IETFは年３回行われており、そのうち１回はアメリカ以外で行うとのこと。今回の開催地ミュンヘンはドイツ北部バイエルン州の州都であり、人口100万人程度ののどかな街である。北はオーストリアと国境を接しており、ザルツブルグとはアウトバーンで結ばれており、夏休みであるのと観光地であるせいか街中にはスーツを着た人は少なかった。緯度的にはニューヨーク、北海道と同じである。着いてみると思っていたよりも暑く、最高気温は連日30℃くらいあった。日差しは強いが、湿度が低いせいか日陰は涼しく、屋内は空調がなくても過ごしやすかった。喉は渇くので炭酸ガス入りミネラルウォータが欠かせない毎日だった。

１．PKIX（Public-key Infrastructure（X.509））

ここはX.509証明書をベースとした公開鍵機構についてのWG。昔はPEMのWGであり、ICATの活動にもっとも近いところである。前回は菊池委員が「PKI:Webベースの証明書とCRLの格納」
ftp://ftp.icat.or.jp/pub/interauth/draft-kikuchi-web-cert-repository-00.txt
について発表したWGでもある。

PKIXの内容は
- Part 1 - Profile
- Part 2 - Operational Protocols
- Part 3 - Management Protocols
- Part 4 - Policy Framework
- Part 5 - Time Stamping
- part 6 - Notary Protocols
- Internet PKI （PKCS #7, #10）
- KEA

でありWGは8月13、14日の2日間に渡って行われた。
PEMのRFCが1421～1424まで連番になっていることを考えると、このようなPart分けも妥当であろう。

1.1 Part1 - X.509 Profile

RFC1421と同様に、ここPart1は以下のPartを構成するための標準と位置づけてある。
X.509v3、X.509v2 CRLの説明から始まり、Subject Name、UCTTimeなどの証明書のField、RSA、DH、DSA等の特許まで記述されている。100ページを越え読み応えがあるが、PKIXに興味がない人でも読んでおきたいドラフトである。
前回のMeetingから若干Reviceされ、Lastcallを出すということであった。

1.2 Part 2 - Operational Protocols

CA-ユーザー間、CA-CA間でのデータのやり取りのプロトコルを議論するパートである。オペレーションのプロトコルとしてLDAP以外にもHTTP、E-mailも念頭に置くということ、Reviceされた PKCS#7と#10を使用するとのことであった。９月に出てきたI-D
draft-ietf-pkix-opp-ftp-http-00.txt
を見てみると、署名された証明書とCRLのファイル名をそれぞれ "anyone.cer"、"any.crl"とし、DER（Distinguished encoding rule）でエンコードして
{f, ht}tp://ftp.your.org/pki/id48.cer
{f, ht}tp://ftp.your.org/pki/id48.no42.crl
などしてファイルとして置くだけのようである。
本筋のI-Dである
draft-ietf-pkix-ipki2opp-04.txt
ではLDAPのプロトコルに則った追加、変更、検索等を実現しようとしている。
これら２つのI-Dでは菊池委員が示したI-Dのように証明書発行要求、破棄要求、有効性確認等の細かいオペレーションについては記載されていない。

1.3 Part 3 - Management Protocols

Reviceされた（される）PKCS#7と#10を使い、PKCS#10をPCKS#7で包んで証明書発行要求をするとのこと。
あと、キーリカバリーをサポートするとのこと。

1.4 Internet PKI

PKCS#7と#10をReviceするとのこと。どうもDSA/DH用に書き換えたいようである。

1.5 総括

最後にChairのKent氏と IETF Security AreaのDirectorであるJeffrey Schiller氏から総括のコメントがあった。PKIXのdefaultのアルゴリズムをDiffie-Hellman（DH）とDSAにしようというものであった。３．に書いてあるTLSやS/MIMEの話を見ると、IETFは特許の絡んだInternet-draft（I-D）を出させないスタンスのようである。

２．OPENPGP

PGPのBOF（Birds of Feather）。
しきりにMailing Listの宣伝をしていた。
http://www.imc.org/ietf-open-pgp/
を参照とのこと。

このセッションで話されていたことは主にBOFからWGへ昇格する際に必要なCharter（憲章）の承認であった。

【Charter】
1. Create a specification that permits encrypting and/or authenticating MIME data.
2. Defines a format for the MIME data, the algorithms that must be used for interoperability, certificate structure.
3. Make NO technical compromises based on any government or legisrative policies.
4. Allows for limited backward compatibility with previous released version.
5. Any required algorithms with be strong, freely available and "unencumbered", other algorithm allowed.
6. Interoperability using "strong" algorithms with the ability to negotiate and communicate at any key length is permissible since the pgp certificate must be obtained in advance.

３と６が強調されていたようであるが．．．

BOFではCharter作成に関係なくいろいろな質問が出ていた。PGPはプロトコルではなくシステムであるということ。だからSSLやS/MIMEやFirewallの認証などの利用は考えていないとのことであった。また、PGP Ver.5.xではElGamalをサポートするとのこと。楽しみにしていた
○X.509への対応
○楕円曲線暗号の対応
がAgendaで示されたが、これらの詳細がなかったのが残念であった。

後日、参加者にPGP社からポスターが送られてきた。このポスターにはX.509や楕円曲線暗号などポスター全体が暗号、認証関係のGlossaryになっており重宝している。

３．TLSとS/MIME

今回はTLSのWGとS/MIMEのBOFのセッションがなかった。S/MIMEの方は
・S/MIMEの商標
・RSAのパテント
の障害があるからである。４月のMemphisでのIETFでは
・WG憲章の作成
・RC2のアルゴリズム公開
を要求され、これに従ったそうだ。しかし、今回IETFはRSA自体のパテントまでをも開放を要求してきた。IETFが終わって9月に入り、S/MIMEのMailing ListではRSA社と別グループがDH/DSAをdefaultとし、RSA/RC2はオプションという案を出してきた。11/7にI-Dが出され、WG設立まで至った。

TLSの方も暗号アルゴリズムのパテントの問題で７月からもめているようで、これが原因でミュンヘンでの開催が中止になったようである。さらに、９月に入ってNetscape社のSSL自体のパテントが成立し、これもIETFとの火種になっているようである。

４．番外編

今年度ICATでは昨年度の「統合暗号システムにおける基盤技術の研究開発」の成果物である楕円曲線暗号、国産ハッシュ等を実装中であり、これらを用いた証明書の作成、実験的認証局の立ち上げを進めている。
X.509の証明書を作成するためにPCKS#1に習って証明書を作成する場合、署名対象データをハッシュした値の前にアルゴリズム固有のオブジェクト識別子（Object Identifier, OID）を挿入しなければならない。この方法ではハッシュのビット長と署名アルゴリズムの鍵長が近い場合、問題が生じることがわかった。すなわち160ビットのハッシュを使用した場合には署名対象データが約300ビットと倍近くになり、160ビットの楕円曲線暗号では署名できない問題が今回のIETF開催の１週間前に浮上してきた。
解決方法として鍵長が短い場合には、署名対象データ（OID＋ハッシュした署名情報）をもう一度ハッシュしてデータ長を署名アルゴリズムの鍵長に収めるという案を早急に作成した。
詳細はProposalの原文
ftp://ftp.icat.or.jp/pub/documents/proposal-icat-short-key-cert-00.txt
を参照のこと。

このようにICAT案を作成したものの、セッションで発表するのに必要なInternet draftの提出期限（cut off date）には間に合わなかった。
Proposalという形で急遽喋りたいとChair（座長）のSteve Kent氏とコンタクトするが、ICATのProposalは

○発表する時間がない。
○X.509やPKCSのフレームワークの問題や、それらのGenericな問題ではなく、別々のOIDを持った署名アルゴリズムとハッシュの組み合わせの問題である。これら２つの組み合わせを一つのOIDで表せられれば署名対象データにハッシュのOIDを付加する必要はなくなる。楕円曲線暗号と同様に鍵長の短いDSAを利用したDSAwithSHA-1では問題無く署名ができている。

との理由でRejectされた。しかし、

○Chairとコンタクトし、Chairに現在のICATの活動を説明できた
○ProposalをI-Dへするための貴重なコメントをもらえた

ことで、今後の活動に十分な資料となった。

鈴木裕信委員が8月末のCRYPTO97[1]で同じProposalの配布を行った。CRYPTO97では配布を置くテーブルがあり、150部のリーフが会場に来ていた人の手に渡った。9月末になり、公開鍵の仕様を決めているIEEE P1363 WG[2]のChairであるBurt Kaliski氏からメールでコメントを頂いた。コメントの内容は

○Kent氏と同じ意見で、署名アルゴリズムにハッシュを一緒に使い、これらを組み合わせたOIDを設定すれば問題は回避できる。
○IEEE P1363とANSI X9.62[3]でもDSA同様の手法を使った楕円曲線暗号の署名方法が提案された。

ということであった。

５．おまけ

写真を撮って来られなくて申し訳ないのですが、Kent氏はハリソン・フォード似のイギリス英語を話すかっこいいおじさんでした。しかもゆっくりと喋ってくれて優しい紳士という感じを受けました。一方、Schiller氏は対照的にスーパーマリオ似の陽気でアメリカ英語を話す人でした（しかもかなり早口）。

今回私はB5サイズのPanasonicのLet's note AL-N2T515J5を持っていったのですが、外国で売られてないらしく、４、５人から話し掛けられました。3000ドルぐらいだと言うと、輸入したいと皆言っていました。ドイツへ行く直前にキーボードが壊れたのもあって、帰国後Panasonicに英語キーボードがあるか確認したところ、きっぱりないと言われました。未だにHome Keyは外れたままです。

６．感想

IETFの議論自体はMailing listで話されていることがほとんどで、会場ではHDの最終確認とインタラクティブな議論のために集まっているようである。
初めてIETFに参加した私としては

○男の人はほとんどひげをはやしており、Ｔシャツに短パンであった。
○平気で会場の床や廊下に座っている人が多い（私も座りましたが）。
○柱のコンセントに平気で突っ込み、電気泥棒を働いている。
○WGでの発表はプロジェクターではなくOHPで、しかもその場で手書きで説明する人も多い。
○やたら話し掛けられる。

という状況はカルチャーショックでした。

《注釈》

1）雑誌 "Journal of Cryptology"を刊行しているIACR(International Association for Cryptologic Research)が開催している暗号に関するカンファレンス。

http://www.iacr.org/

2） IEEE(Institute of Electrical and Electronics Engineers)で公開鍵暗号の標準を決めているWG。ChairはRSA社のBurt Kaliski氏が勤めている。

http://stdsbbs.ieee.org/groups/1363/

3） ANSI(American National Standards Institute)でECDSA (Elliptic Curve Digital Signature Algorithm)の標準を決めているWG。

http://www.ansi.org/

III. 暗号関連ニュース

今年は暗号に関するニュースが目白押しでした。ミュンヘンのIETFミーティング前後にIETF、RSA社、PGP社が関係する特許絡みのニュースが多くありました。アメリカでDiffie-Hellman（DH）の特許が9月に切れたせいもあって、S/MIMEやSSLの問題、PGPがDHを採用したことが発端になっているようです。

次に暗号解読の話です。１月のRSAカンファレンスでRSA社がコンテストを主催していたのですが、ビット数の少ない暗号は次々と破られてきました。これらはすべてアメリカ政府が行っている輸出規制に反対するデモでしょう。アメリカはこういうパフォーマンスが得意ですね。

【暗号関連トピックス】

6/20	56ビットDESが破られる。
6/24	Netscapeが128ビット暗号鍵対応ソフトの輸出許可を取得
6/25	Microsoftが128ビット暗号鍵対応ソフトの輸出許可を取得
7/ 4	独でマルチメディア法が成立 電子署名の法的有効性を認める
7/ 5	RSA社暗号化技術「RC2」をIETFに提出
7/12	56bitDES、パソコンで解読される
7/15	ベリサイン、128ビット暗号IDの発行許可を取得
7/23	日本RSA SET対応暗号ソフトを韓国ソウル銀行等に供与
8/11	大蔵省、オンライン・バンキングを規制する“機械化通達”を廃止
8/28	IETFがRSA社に暗号技術の特許公開を要求
9/ 3	FBI長官が「暗号技術は政府の管理下におくべき」との見解を示す仏内務相、暗号規制の緩和方針を示唆
9/ 5	暗号化ソフトの規制強化提案に米主要IT企業が反発 イリノイ大Bernstein氏、暗号輸出の裁判で勝訴
9/10	Microsoft社オンライン・バンキング用暗号ソフトを配布
9/11	S/MIMEでDSA/DHをデフォルトとする案浮上
9/15	米政府、暗号に関する国際的取り決め違反として非難される 日本法制審議会が“電子メール盗聴捜査”などの合法化を答申
9/17	米でNetscape社のSSLの特許成立
9/18	RSA社PKCS#1、#7、#10をIntrnet-draft化 Security Dynamics、128ビット暗号化ツールの輸出許可を取得
9/23	RSA社S/MIMEのInternet-draft Revice
9/24	米下院委員会、キーエスクローを盛り込んだ暗号法修正案を否決
9/25	RSA S/MIMEの登録商標を放棄
9/26	通産省の暗号製品の輸出規制緩和政策発表
10/ 1	富士通など3社が電子認証の専門サービス会社を設立
10/ 2	PGP社 ビジネス向けキーエスクロー暗号製品を発表
10/ 7	RSA社 スプーフィング対策ソフトを無償提供
10/10	Bruce Schneier氏S/MIMEの40ビットRC2を解読するスクリーン・セーバーを公開
10/13	EC報告書 米国暗号政策を拒否
10/19	RSA社 S/MIME I-D Revice提出
10/22	56ビット RC5破られる RSA社 PKCS #1、#7、#10 I-D Revice
10/27	仏、暗号の40ビットまでの使用制限を解除へ RSA社128ビット暗号製品の輸出許可取得
11/ 7	DH/DSAをデフォルトのアルゴリズムとしたS/MIMEのI-D提出 IETF Security AreaにS/MIME-WG設立

事務局連絡

―第２回 平成９年度定 例研究会を開 催いたします。

日時：1998年2月4日（水）10:00～16:00（予定）

会場：機械振興会館 地下２階ホール

参加手続、プログラム等の詳細は別途ご連絡いたします。

―以 下の報 告書を 製本中で す。会 員には 製本でき次第発送いたします。

「広域認証基盤技術の設計と実装」

「暗号アルゴリズムの設計と実装」

「米国暗号関連の特許登録情報」

「暗号・認証技術の研究開発に関する動向調査」

[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/