SCIS'97 The 1997 Symposium on
Cryptography and Information Security
Fukuoka, Japan, January 29-February 1, 1997
The Institute of Electronics,
Information and Communication Engineers

オンライン証明書発行局パッケージ(ICAP)の実装と評価

Development and Estimation of Web-based Online Certification Authority, ICAP

服部 裕之[†] 櫻井 三子[‡] 小林 良至[*] 菊池 浩明[**]

Hiroyuki Hattori Mine Sakurai Ryoji Kobayashi Hiroaki Kikuchi

[†]明治大学 情報科学センター [‡]日本電気株式会社 ネットワーキング技術研究所
[*]アスキーネット株式会社 ソリューション事業推進部 [**]東海大学 工学部 電気工学科

〒214 神奈川県川崎市多摩区東三田 1-1-1

Meiji University , Information Science Center

1-1-1, Higashi-mita, Tama-ku, Kawasaki, Kanagawa, JAPAN

あらまし

従来のオフラインによる証明書発行方式における問題に触れ、これを解決する、本人認証作業をオンラインで行なうことによって発行手続きを簡略化するモデルを提案する。

そして、このモデルにおける前提条件および問題点をあきらかにした上で、オンライン証明書発行を実現する発行局ソフトウェア -ICAP- の開発について紹介する。

abstract

This paper describes problems of an off-line certification issuing, and propose a solution of an on-line certification issuing method which can cut down the process of the user's authentification.

This paper also shows the Web-based online certification authority software, ICAP.

1　はじめに

近年の電子商取り引きなどへの関心が高まる中、広域認証技術、とりわけ証明書発行局 [1]（以下単に「発行局」と記する）および発行局構築のためのソフトウェアの必要性が増している。

発行局を構築する為のソフトウェアは、すでにいくつか存在しており、実際の運用に用いられているが、その際に問題となっているのが証明書を発行する時の本人認証の手間である。

一般に発行局では、申請者からの依頼を受けて証明書を発行する際、直接対面による方法などで本人の確認を行なっている。つまり、証明書を発行する際の事務的作業量が決して少なくはなく、組織内で発行局を立ち上げる際の障壁となっていた。

そこで本稿では、オンラインによる証明書の発行を実現することにより、従来よりも証明書の発行手続きを簡略化するモデルを提案する。

さらに、提案したモデルを発行局パッケージ (ICAP) の機能として実装した結果について、検討をおこなう。

2　発行局の課題

2.1　証明書発行手続き

最初に、証明書の発行手続きを明確にするために、証明書の発行を希望する者（証明書申請者）が実際に証明書を入手するまでの手順を図 1 に示す。

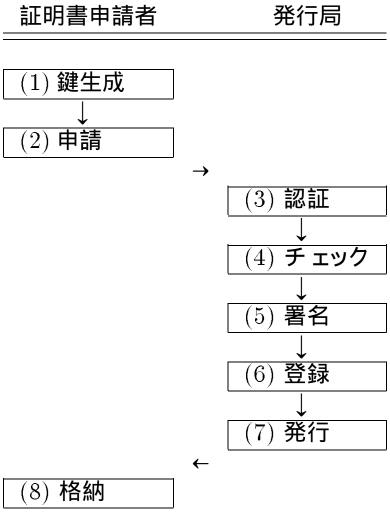


図 1 :証明書の発行手続き

図 1 の説明:

1. 鍵生成　申請者は自分自身が使用する秘密鍵および公開鍵を生成する。
2. 申請　申請者は (1) で生成した公開鍵に対する証明書の発行を、発行局に申請する。
3. 認証　発行局は申請者の認証をおこなう。
4. チェック　2 重申請、あるいは同姓同名などによる DN (Distinguished Name) の重複検査を行なう。
5. 署名　発行局の秘密鍵で署名を行い、証明書を作成する。
6. 登録　作成した証明書を、証明書管理のためのデータベースに登録する。
7. 発行　証明書を申請者に返却する。
8. 格納　申請者は、発行された証明書を自分自身が使用しているシステムに格納する。

図 1 の手続き (3) における本人の確認方法は、証明書の有効性・信ぴょう性と大いに関連する為、発行局のポリシーによってさまざまな手法が取り得る [2]。

たとえば、ノルウェーの教育研究用ネットワークである UNINETT の場合、下位の発行局が証明書を発行する際は、申請する本人自身が発行局を訪れ、パスポートや運転免許証等を提示することによって、認証が行なわれている [3]。

また、WIDE プロジェクトの発行局は、認証のレベルを 2 つに分けている [4]。一つは、低信頼発行局が発行するペルソナ証明書 (Persona Certificate) で、暗号化を考慮していない通常の電子メイルを用いて発行している。もう一つは、公証局が発行する証明書で、これは本人の確認をきちんと行なう「公証人」を媒介人として証明書を発行している。

2.2　証明書発行手続きの問題点

証明書発行手続きにおいて重要な点は、如何に、確実に、証明書の申請者が本人であるかどうかを確認することである。

その為に、UNINETT 発行局 や WIDE 公証局の場合、証明書の申請者は自らを証明する書類を携えて発行局に行く必要があった。

しかし、これには次のような問題がある。

- 発行局の負担
    - 発行申請件数が増えてくると、それに伴って発行事務に関する作業量が増大する。
- 申請者の不便
    - 証明書を入手する際の本人確認が、対面による方法のため、申請者にとっては煩わしい。
    - 発行局側では、人手作業による認証作業の為、窓口の受け付け時間に制限が設けられることが考えられる。この場合は、証明書発行までに時間を要する場合が考えられる。

3 証明書発行手続きの簡略化の提案

ここで、証明書の発行を希望する利用者のコンピュータ利用環境について、たとえば、大学の計算センターの利用者が、証明書の発行を希望するケースを想定してみる。

通常、大学の計算センターを利用する為には、事前に利用登録が必要である。利用登録を行なうことができる資格者は、多くの場合、大学の構成員、もしくはそれに準じた者であるようだ。そして利用登録者には、コンピュータを利用するためのアカウントとして、「ログイン名」と「パスワード」が発行される。

大学の計算センターにおける利用登録の手順を図2に例示する。

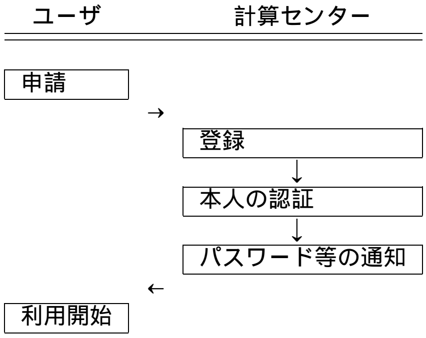


図 2 ：利用登録の流れ（例）

つまり計算センターの利用者には、「ログイン名」「パスワード」のような、コンピュータを利用する際の識別情報が与えられており、しかも利用登録を行なった時点で、本人の認証が行なわれているとみなすことができる。

ここで仮に、発行局が計算センターの利用者の識別情報を認証に利用することができるならば、証明書発行時に、再度、前述のような人手による本人認証作業を行なう必然性は少なくなる。

もう一度、図1の証明書発行手続きのモデルを眺めてみる。

図1において、手続き「(3) 認証」~「(7) 発行」は、発行局側の作業であるが、「(3) 認証」の際、計算センターの識別情報、たとえば「ログイン名」と「パスワード」を利用できるであろう。そして、識別情報によって本人の認証を行なうのであれば、発行局側の処理は自動化が可能であり、「オンラインによる証明書発行」を実現することができる。これにより、証明書発行に要する発行局側の作業を、大いに軽減することができる。

オフラインによる証明書発行手続きと、オンラインによる証明書発行手続きの概要を、図3および図4に示す。

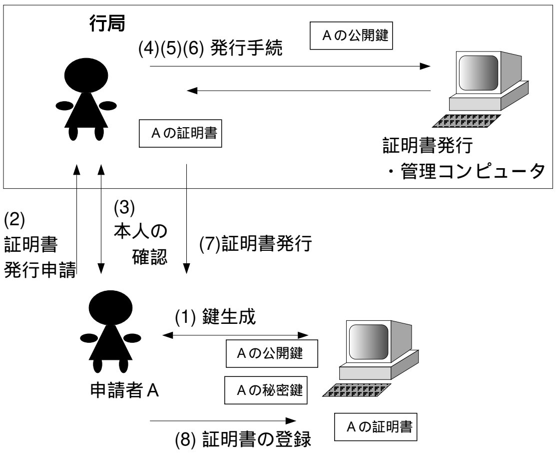


図 3 ：従来の証明書発行手続き（オフライン）

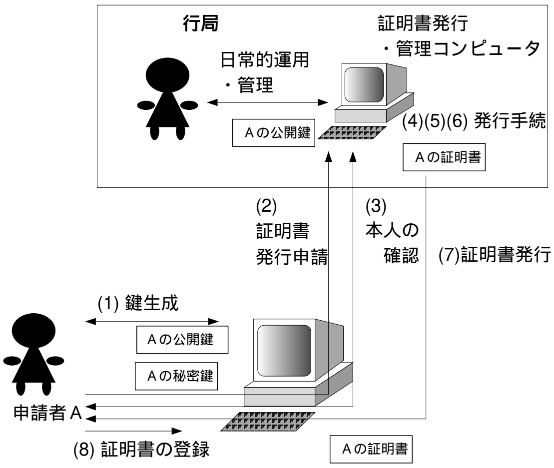


図 4 ：オンラインによる証明書発行手続き

以上の検討をふまえ、オンラインによる証明書の発行を実現する為の前提条件を、明らかにする。

- 前提条件 **1**

1. 証明書の発行を希望する者は、どこかの組織や機関（たとえば計算センター）に秘密の識別情報（たとえばパスワード）を登録済みである。
2. 発行局は、証明書発行を希望する者の識別情報を、事前に入手することができる。

ところで、オンライン認証を行なう際には、申請者の識別情報がネットワーク上を流れることになる。

識別情報には、

- （通常の）パスワード
- ワンタイム・パスワード
- チャレンジ / レスポンス

などを用いることが考えられるが、通常のパスワードを用いる場合は、ネットワーク上を流れる情報に対する盗聴対策が必要となる。その場合は、オンラインによる証明書発行を実現する為の前提条件に、次の条件も加える必要がある。

- 前提条件 **2**

1. 証明書申請者が使用するコンピュータと発行局間の通信は、盗聴への対策を講じている。

4 ICAP の開発

前節までの検討をふまえ、筆者らは、証明書の発行をオンラインで行なう機能をもつ発行局ソフトウェア– ICAP (ICAT Certification Authority Package) – を開発した[1]。

ICAP とは RFC1422 に記載されている発行局を実際に立ちあげ、運用するためのソフトウェアパッケージの名称である。

4.1 特徴

ICAP には以下の特徴がある。

- オンラインによる証明書発行機能
- オンラインによる証明書有効性の確認機能
- オンラインによる証明廃棄機能
  - 証明書の発行を希望する利用者は、オンラインで証明書の発行、有効性の確認、および廃棄が可能である。
- 簡単なインストール

---

[1] ICAP は `http://www.icat.or.jp` より入手可能である。

  - ICAP は簡単にインストールできるよう、(1) インストールスクリプトの充実、(2) バイナリ形式での配布 を行なっている。これにより ICAP のインストールには、面倒な「make」等は不要である。

- 簡単操作
  - 証明書発行に関するほとんどの操作は、Web ブラウザから行なうことができる。

4.2 システム構成

ICAP は、WWW サーバ上で動作する CGI プログラム、および CGI プログラムから起動されるいくつかのプログラムから構成される（図 5）。

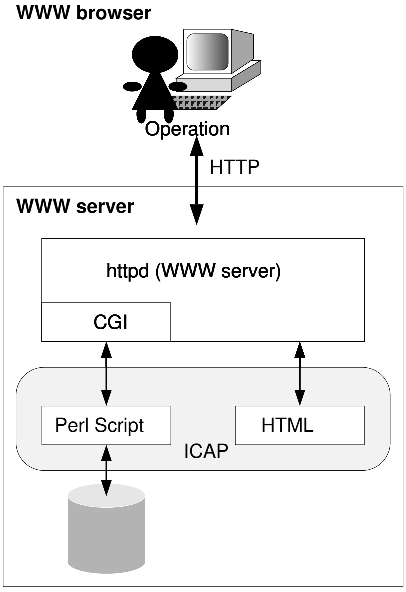


図 5: **ICAP のシステム構成**

4.3 動作環境

ICAP の動作環境は、次の通りである。

- 対象システム
  - SunOS4.1.X
- 必須ソフトウェア
  - **WWW サーバ**

    NSCA httpd または Apache
  - **Web ブラウザ**

    netscape navigator ,

    Internet Explore 等
  - インタプリタ

    Perl 4.036 以上

* WWW サーバと Web ブラウザについては、SSL(Secure Socket Layer) [6] のような暗号通信路を用いたアクセスが可能であることが望ましい。

4.4 操作とメニュー

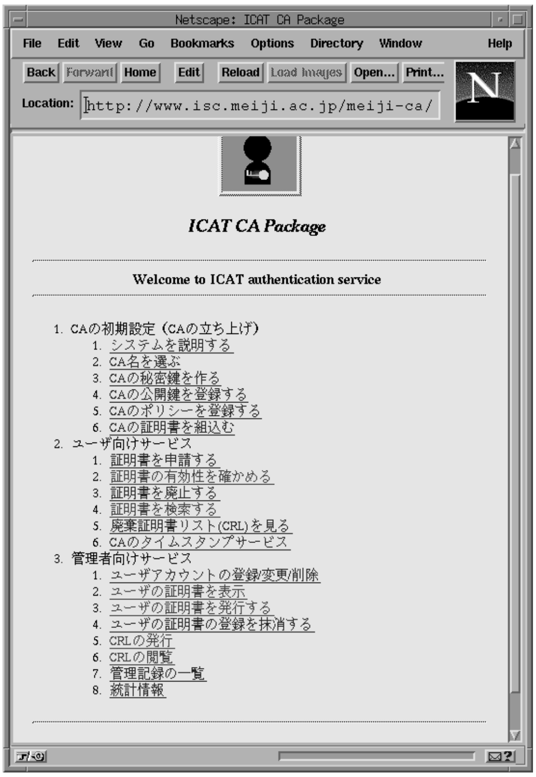
ICAP の操作は、Web ブラウザを用いてネットワークを経由して行なう。ICAP は発行局の管理者向けのメニューページと、一般利用者向けのメニューページを用意している（図 6）。管理者向けメニューページは、パスワード認証によって有資格者以外の者によるアクセスを制限している。

ICAP のメニューを以下に示す。

1. 一般ユーザ向けサービス
   - (a) 証明書を申請する
   - (b) 証明書の有効性を確かめる
   - (c) 証明書を廃止する
   - (d) 証明書を検索する
   - (e) 廃棄証明書リスト (CRL [2]) を見る
   - (f) CA のタイムスタンプサービス
2. 管理者向けサービス
   - (a) ユーザアカウントの登録/変更/削除
   - (b) ユーザの証明書を表示
   - (c) ユーザの証明書を発行する
   - (d) ユーザの証明書の登録を抹消する
   - (e) CRL の発行
   - (f) CRL の閲覧
   - (g) 管理記録の一覧
   - (h) 統計情報

---

[2] Certificate Revocation Lists



ICAT CA Package

Welcome to ICAT authentication service

1. CAの初期設定（CAの立ち上げ）
    1. システムを説明する
    2. CA名を選ぶ
    3. CAの秘密鍵を作る
    4. CAの公開鍵を登録する
    5. CAのポリシーを登録する
    6. CAの証明書を組込む
2. ユーザ向けサービス
    1. 証明書を申請する
    2. 証明書の有効性を確かめる
    3. 証明書を廃止する
    4. 証明書を検索する
    5. 廃棄証明書リスト(CRL)を見る
    6. CAのタイムスタンプサービス
3. 管理者向けサービス
    1. ユーザアカウントの登録/変更/削除
    2. ユーザの証明書を表示
    3. ユーザの証明書を発行する
    4. ユーザの証明書の登録を抹消する
    5. CRLの発行
    6. CRLの閲覧
    7. 管理記録の一覧
    8. 統計情報

図 6 ：ICAP 管理者向けメニュー

5 ICAP を用いた発行局の立ち上げ

ICAP はいずれかの PCA[3]の下位にあたる発行局での利用を念頭においている。本節では、IPRA[4]が証明書を発行した日本で最初の実験的 PCA である ICAT (Initiatives for Computer Authetication Technology- 認証実用化実験協議会-) PCA の下位に、ICAP を用いて新たに発行局を立ちあげる際の手順を紹介する。

1. 新規発行局
    (a) ICAP の入手
    (b) ICAP のインストール
    (c) 鍵生成
        発行局自身の鍵を生成
    (d) 発行局自身の証明書の申請
        公開鍵を ICAT PCA に送付、証明書の申請を行なう。
2. ICAT PCA
    (a) 発行局運用者の認証
        現在のところ、ICAT 側から電話を使ったコールバックを行なうことにより発行局の運用者の認証を行なっている。
    (b) 証明書を発行
        発行局の公開鍵に署名、証明書を発行する。
3. 新規発行局
    (a) 証明書のインストール
    (b) 発行局の運用開始

ICAT PCA は、1996 年 2 月に IPRA から証明書が発行された。そして、1997 年 1 月現在、ICAT およびその参加組織は、ICAP を用いて図 7 に示す証明書発行局の階層構造を実現している[5]。

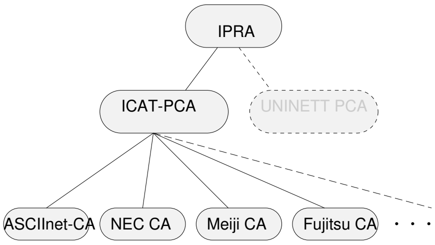


図 7 ：発行局の階層構造

6 ICAP を用いたオンライン証明書発行

証明書の発行を希望する者が、オンラインで証明書の発行申請を行なう手順を紹介する。

前提として、証明書申請者は計算センター等にアカウント登録を事前に行なっており、そのアカウント情報は発行局も保持している必要がある。

1. 発行局
    (a) 申請予定者のアカウント情報を登録する

---

[3] Policy Certification Authority

[4] Internet Policy Registration Authority

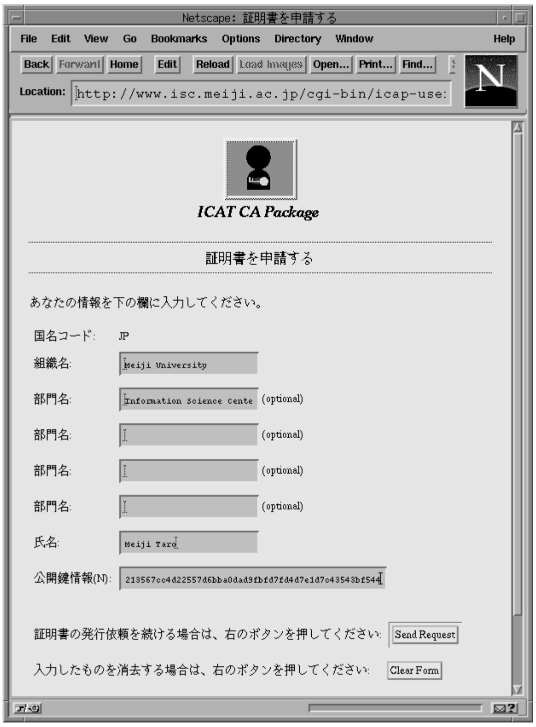
[5] ICAT PCA の下位には、14 の発行局が存在している。

    ICAP が認証で用いるパスワードファイルは、SunOS4.x が参照するパスワードファイル (`/etc/passwd` や NIS passwd マップ) と同一フォーマットである。

2. 申請者
    - (a) 秘密鍵と公開鍵を生成。
    - (b) Web ブラウザを用いて発行局のホームページへ接続。
    - (c) 「証明書を申請する」というメニューを選択。
    - (d) 「公開鍵情報 (N)」欄に、(a) で作成した申請者自身の公開鍵を入力する (図 9)。同時に証明書の DN も指定する。
    - (e) 自分のログイン名およびパスワードを入力する。
3. 発行局
    - (a) パスワードのチェック。
    - (b) 申請フォームのチェック。
    - (c) 証明書の発行。
4. 申請者
    - (a) 証明書の格納。

ICAP は、一般ユーザが証明書の申請を行なう際に、パスワードによって申請者本人の認証を行なう。従って、申請者のパスワードがネットワーク上を流れてしまう為、第 3 者がネットワークを盗聴することによってセキュリティ上の問題が発生する可能性がある。これを回避する為に、Web ブラウザと ICAP 間の通信は、極力、SSL による暗号通信路を用いて行なう (図 8)。

図 8: ユーザ~ICAP 間の暗号通信路



Location: http://www.isc.meiji.ac.jp/cgi-bin/icap-use:

証明書を申請する

あなたの情報を下の欄に入力してください。

国名コード: JP
組織名: Meiji University
部門名: Information Science Cente (optional)
部門名: (optional)
部門名: (optional)
部門名: (optional)
氏名: Meiji Taro
公開鍵情報(N): 213567cc4d22557d6bba0dad9fbfd7fd4d7e1d7c43543bf544

証明書の発行依頼を続ける場合は、右のボタンを押してください: Send Request

入力したものを消去する場合は、右のボタンを押してください: Clear Form

図 9 : ICAP を用いた証明書の発行

7 考察

7.1 認証作業量

オンライン証明書発行方式は、オフライン方式に比べ、発行局側では、証明書発行時の認証作業をオフラインで行なわずに済むという利点がある。

もっともこれは、証明書を発行する時点での作業についてであり、その前提として、申請者本人に対するアカウント発行時の認証作業は、依然として存在する (図 10)。

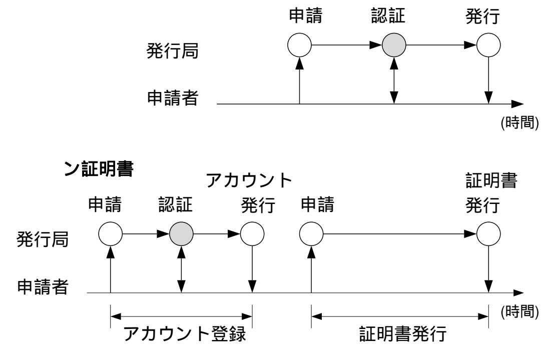


図 10 : 認証作業の比較

仮に証明書の発行局と、アカウントの発行を行なう組織が同一であり、発行局がアカウント情報を入手できるのであれば、発行局を新たに立ちあげる際の作業量の増加はあまり無いものと思われる。

しかしながら、これらの組織がまったく別々のものであり、発行局でアカウント情報を入手できないのであるのならば、オフライン証明書発行方式に比較し、作業量の減少は期待できない。

7.2　安全性

7.2.1　本人認証の確実性

オフラインによる証明書発行方式において、本人であるかどうかの確実性は、対面で認証した際に決まる。

これに対し、オンラインによる証明書発行方式は、

- アカウントを発行する際の本人認証の確実性
- パスワードの確実性

により決定される。ここでパスワードの確実性とは、証明書発行時に申請者が入力したパスワードそのものが、第3者によるものではなく、正しく本人のものであるかどうかを意味している。

オンライン証明書発行方式において、本人であるかどうかの確実性は、この2つの要素が共に確実であるかどうかによって決まる。従って、オンライン証明書発行方式は、オフライン証明書発行方式よりも安全性において劣るといえよう。

さて、それではオンライン証明書発行方式において、安全性を向上するにはどうすればよいであろうか ?

根本的な対策ではないが、認証の際に、パスワード以外の情報を、補助的に用いることによって、安全性を向上できるものと思われる。

たとえば証明書を発行する際に、DNの情報として、本人の本名、生年月日、電話番号等の入力も求めるようにする。そして証明書を発行する時は、パスワードによる認証ばかりでなく、これらの情報も認証のためのキーに用いるようにする。

大学の計算センターで発行局を運用する場合、ICAPが学籍データベースや個人情報データベースと連係することにより、このような認証時の補強も可能であると考えられる。

7.2.2　オンライン発行局システムの安全性

ICAPはオンラインで証明書を発行するという特徴を持っているが、それゆえに、ネットワークを用いたセキュリティ的脅威についても考慮する必要がある。

- 識別情報の盗聴
  - 証明書申請者と、発行局間のネットワークを盗聴することによって、証明書を発行する際の識別情報が洩れる危険性がある。これについての対策は、暗号通信路を用いてオンライン発行を行なうことが考えられる。
  - 申請者がproxyサーバを経由して証明書の発行を行なう場合は、proxyサーバ上で識別情報が盗聴される恐れがある。従って申請者は、proxyサーバを経由せずに証明書の発行を行う方がよい。
- 発行局への不正アクセス
  - ICAPが稼働しているコンピュータ自身に対する不正アクセス。たとえば、サーバプログラムなどのセキュリティホールを利用した不正アクセスなどが考えられる。従って発行局側は、常に最新のセキュリティ情報に注意をはらい、適切な対策を施す必要がある。
- なりすまし発行局
  - インターネットにおけるコンピュータの攻撃方法の一つに、denial-of-service attackがある[7]。これは、ネットワークを経由して特定のコンピュータを利用不可能にしてしまう攻撃である。仮に発行局がこの攻撃を受け、停止してしまった場合、その間を利用して、他のコンピュータが、発行局になりすましをするという攻撃が考えられる。この攻撃への対策は、SSL等を用いてサーバクライアント間の認証機能を持たせ、なりすましを困難にすることなどが考えられる。

8 他の発行局パッケージとの比較

ICAP と他の発行局パッケージとの比較を図 11 に示す。

9 まとめ

オンラインによる証明書発行は、発行局側の証明書発行作業を軽減することができるが、本人確認の際の確実性については、発行申請者自身の持つ識別情報の信頼性に依存している。

従って、ログイン名とパスワードを識別情報に利用する場合、発行申請者自身のパスワード管理に問題がある場合は、証明書の信頼性そのものが低くなってしまう。

しかしながら、企業内のイントラネットや、大学計算機センターなど、証明書の発行対象者に対する身元確認が、既に行なわれている場合においては、本稿で述べたオンラインによる証明書発行方式は、組織全体の業務量を増やすことなく提供可能であるため、非常に有効である。

10 謝辞

本研究にあたり、有益な意見を戴いた認証実用化実験協議会、広域認証技術タスクフォースのメンバに感謝いたします。

参考文献

[1] S.Kent: “*Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*”, Internet Request for Comments 1422 (1993) (available from ftp://ds.internic.net/rfc/rfc1422.txt)

[2] S.Farrell: “*Internet Public Key Infrastructure PART III:Certificate Management Protocols*”, Internet Draft (1996) (available from ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki3cmp-01.txt)

[3] N.Berge: “*UNINETT PCA Policy Statements*”, Internet Request for Comments 1875 (1995) (available from http://www.uninett.no/pca/rfc1875.txt)

[4] 菊池 浩明, 黒田 康嗣: “暗号メール *PEM:*公証人申請による証明書発行方式”, (1993) (available from ftp://sh.wide.ad.jp/WIDE/free-ware/fjpem/fjpem-1.2.tar.gz)

[5] 櫻井 三子, 服部 裕之, 小林 良至, 菊池 浩明: “証明書発行局間の証明書情報共有機構の設計”, SCIS97 (1997)

[6] A.Freier: “*The SSL Protocol Version 3.0*”, Internet Draft (1996) (available from ftp://ds.internic.net/internet-drafts/ draft-ietf-tls-ssl-vertion3-00.txt)

[7] “*UDP Port Denial-of-Service Attack*”, CERT Advisory CA-96.01 (1996) (available from ftp://info.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial)

[8] 山崎 直洋, 菊池 浩明, 中西 祥八朗: “暗号化サーバによる電子メールのプライバシ強化の提案”, SCIS97 (1997)

	SecuDE(4.4)	SSLeay(0.6.5)	ICAP(1.0b)
開発国	ドイツ	オーストラリア	日本
利用条件	無償	無償 (商利用可能)	無償
配布形式	ソースプログラム (5.0a はバイナリ)	ソースプログラム	ソース＆バイナリプログラム
動作プラットフォーム	UNIX, Windows, DOS	UNIX, Windows, DOS	UNIX(SunOS)
ユーザインタフェース	コマンドライン、専用 X クライアント	コマンドライン	Web ブラウザ
証明書のバージョン	X.509v1 (5.0a は v3)	X.509v3	X.509v1 (1.0 は v3)
証明書要求インタフェース	端末のコマンドライン, GUI	端末のコマンドライン	Web ブラウザ
証明書の署名アルゴリズム	md2withRSAEncryption md5withRSAEncryption shawithRSAEncryption ..	md5withRSAEncryption md2withRSAEncryption shawithRSAEncryption ..	md2withRSAEncryption
対応アプリケーション	PEM	SSLhttpd, SSLtelnet, SSLftp	PEMCAT, FJPEM, Apache+SSL, PEPOP[8]
実働状況	UNINETT PCA および下位 CA で使用中	?	ICAT PCA および下位 CA で使用中
入手先	http://www.darmstadt.gmd.de/secude/	http://www.psy.uq.oz.au/ftp/Crypto	http://www.icat.or.jp/pages/p6.html

図 11 ：ICAP と他の発行局パッケージとの比較