# 第 XVII 部

# 公開鍵証明書を用いた
# 利用者認証技術

# 第 17 部
# 公開鍵証明書を用いた利用者認証技術

## 第 1 章　はじめに

moCA WG では、CA（Certification Authority）の振る舞いや証明書の扱いに注目し、オンライン CA である moCA（members oriented CA）の運用実験を行ってきた。実験では ICAP（ICAT CA Package）を用いたオンライン CA の運用を行い、必要に応じて証明書の発行・失効・更新を行い、また利用環境や用法に関する情報交換を行っている。

2003 年度は 2002 年度に引き続いて、WIDE メンバ証明書とサーバ証明書を発行する運用業務を行った。ただ 6 月末の WIDE メンバ証明書の再発行と、サーバ証明書の更新を除いて、moCA 自身を対象とする実験は行われなかった。

一方で、サーバ証明書の利用場面がこれまでに比べて拡大した。サーバ証明書の発行業務はこれまでにも行っていたが、証明書の内容を利用したアクセスコントロールを実際のサービス運用の為に利用したり、検証者を WIDE メンバに限定しない用途に利用したりする場面が現れた。

本報告では、第 2 章で証明書の利用場面について列挙するとともに、各々の場面で証明書（特にクライアント証明書）を利用した人数や件数について紹介する。第 3 章では、第 2 章で列挙した利用場面の中でも特にインターネットコンファレンス 2003 の参加申し込みにおける事例を、第 4 章では WIDE 合宿の参加申し込みでの活用事例に関する詳細を述べる。第 5 章で moCA の今後の課題について触れ、章末に関連する CA の証明書のフィンガープリントを掲載する。

## 第 2 章　moCA が発行したサーバ証明書の応用

- インターネットコンファレンス 2003 の参加申し込み（2003 年 6 月）
  WIDE メンバ以外の Web のユーザが参加申し込みを行う可能性がある場面である。WIDE メンバ以外のユーザが、WIDE Root CA をトラストポイントにしている状況は想定することができない。そのため、Web ブラウザを用いてアクセスしたときに表示されるダイアログの意味や、フィンガープリントを確認する方法について説明する必要があった。また、単に同一の PKI ドメインを想定できないだけでなく、ユーザのニーズや理解度が予測できないため説明文を工夫する必要があった。申し込みを行った 72 名のうち、https のユーザは 52 名であった。また https のユーザのうち、半数以上が WIDE メンバではなかった。
- 合宿の参加申し込み（2003 年 9 月）
  WIDE メンバ証明書を利用してアクセス者の識別を行う場面である。証明書の内容（WIDE 番号）を利用してアクセス者の識別を行った後、過去に入力されたデータを呼び出すといった入力補助を行う。この利用方法は例年行われてきたもので、現在では、認証時に証明書を持っている人には証明書の提示を求め、証明書を持っていない人にはパスワード入力を求めるという、切り替えが自動的に行われる形で利用されている。今回は、283 名の参加者のうち 262 名が WIDE メンバ証明書を使って申し込みを行い、証明書利用率が 90%以上となった。
- 12 月研究会の記名式アンケートでの活用（2003 年 12 月）
  WIDE メンバ証明書を利用してアクセス者の識別を行う場面である。環境変数を用いて、証明書の内容（WIDE 番号）を CGI のプログラムで

読み込む方法に関する情報交換が行われた。アンケートの回答数 64 件のうち、48 件が WIDE メンバ証明書を使ってアクセスされて回答されたものであった。

- two WG の管理者用情報共有サーバでの利用（2002 年 9 月より）
  two WG における情報共有サーバで、アクセスコントロールのために WIDE メンバ証明書が利用されている。クライアント認証の結果に応じて、ページの内容を切り替える機能やクライアント証明書が利用できない場面でのパスワード方式への切り替えなど、様々な機能が実装されている。WIDE メンバ証明書が利用できる場合には、その内容を利用したアクセスコントロールが行われる。このサーバで、クライアント認証が必須とされた 2002 年 9 月 11 日以降、121 のクライアント証明書が利用されている。なお two WG に登録されているメンバは 137 名であり、多くのメンバが WIDE メンバ証明書を利用していることがわかる。
- $(pg)^3$a WG の WIDE Hour での利用（2003 年 9 月より）
  $(pg)^3$a WG の運用している WIDE Hour のサーバで、アクセス者の識別を行うために WIDE メンバ証明書を利用することができる。運用が開始された 2003 年 9 月の合宿期間から 2003 年 12 月 31 日までに 1058 回のログインが発生しており、このうち 872 回が WIDE メンバ証明書を利用していた。また、ログインしたことのある 166 名のうち 128 名が WIDE メンバ証明書を利用していた。ここでも多くのメンバが WIDE メンバ証明書を利用していることがわかる。

## 第 3 章　インターネットコンファレンス 2003 の参加申し込みにおけるサーバ証明書と WIDE メンバ証明書の活用事例

### 概要

インターネットコンファレンス 2003（IC2003）では、moCA の発行するサーバ証明書を利用して HTTPS による参加申し込みを行った。IC2003 では WIDE メンバ以外の人も参加するため、それらの人が moCA の発行するサーバ証明書を利用する際には moCA の認証局を信頼してもらう必要がある。そのため、moCA のポリシーと HTTPS でのアクセスの際に必要となる知識や手順について簡単にまとめ、HTTPS による参加申し込みの前にポリシーを理解し、その上でアクセスするということが理解できる文書を作成した。

### 3.1 IC2003 での参加申し込み

インターネットコンファレンスは WIDE プロジェクトと他 4 団体が主催するインターネット技術に関する会議であり、年 1 回日本国内で開催している。インターネットコンファレンスでは、これまで HTTP による参加申し込みシステムを使用してきたが、IC2003 ではそれに加えて HTTPS による参加申し込みを行うことにした。ただし、HTTPS によるアクセスができない場合のことを考え、HTTPS による参加申し込みのみではなく、従来の HTTP を用いた参加申し込みも準備することとした。

### 3.2 moCA のポリシー

IC2003 の参加者は WIDE メンバだけではなく、主催団体の会員、協賛団体の会員や一般参加者からなる。そのため、WIDE メンバ以外の人が moCA の発行するサーバ証明書を利用する可能性がある。サーバ証明書を利用するにはサーバ証明書を発行している moCA の認証局を信頼する必要があるが、moCA では WIDE メンバ以外にそのポリシーを示すドキュメントがなかったため、moCA のポリシーおよび HTTPS でのアクセスの際に必要となる知識や手順について簡単にまとめた web ページを用意し、HTTPS アクセスの前に周知することにした。

### 3.3 実験結果

IC2003 の web 上での参加申し込み期間は 2003 年 9 月 22 日から 10 月 17 日であった。この期間中に参加申し込みを行った人数は 72 名で、そのうち HTTPS を利用した人数は 52 名であった（表 3.1）。参加申し込みをした人のうち 7 割程度が HTTPS を利用し

**表 3.1.**　参加申し込み人数

| | HTTPS | HTTP | 合計 |
|---|---|---|---|
| WIDE メンバ | 25 | 5 | 30 |
| 非 WIDE メンバ | 27 | 15 | 42 |
| 合　計 | 52 | 20 | 72 |

て申し込みを行っている。WIDE メンバでない人も 27 名が HTTPS を利用して申し込みを行っている。また、moCA のポリシーの書かれた web ページへの期間中の総アクセス数は 83 であった。

### 3.4 考察・今後の課題

今回の参加申し込みでは、HTTPS を利用するか HTTP を利用するかの選択は申し込みをする人に任されていて、HTTPS を利用するメリット等については web 上では特に何も提示しなかった。それでも HTTPS を利用する人のほうが利用しない人より多くなっている。WIDE メンバ以外の人に moCA をアピールする方法として活用できるのではないかと考えられる。

今後の課題として、moCA のポリシーがどれくらい WIDE メンバ以外の人に理解してもらえたかが不明であるので、参加申し込みと同時にアンケートを取るなどして、よりわかり易い文書にしていく努力が必要である。また、今回は WIDE メンバ以外の人が moCA の認証局の証明書を検証する方法についての準備と説明が不十分だったため、その説明を追加する必要がある。

## 第 4 章　合宿申し込みでの moCA 活用事例

昨年度に引き続き今年度も、3 月と 9 月の年 2 回の研究会合宿に向けた参加申し込みにおいて、合宿プログラム委員会の協力を得て WIDE メンバ証明書を利用した申し込み実験を行った。これは、PKI のプロモーションの一環で、証明書による認証の後、WIDE メンバ証明書に記載されている WIDE 番号を利用して、WIDE 番号の手入力を省けるという使い方をアピールする実験である。具体的には、WIDE 番号から過去の合宿参加申し込み情報が自動的に取り出せるようになっており、継続的に合宿に参加している人にとっては申し込み内容の入力の手間が軽減される。

3 月合宿の申し込みでは、認証時に WIDE 共有パスワードか WIDE メンバ証明書かを選択したが、9 月合宿の申し込みでは、WIDE 共有パスワードを利用せず初めて WIDE メンバ証明書を原則利用する（例外的に個別 ID／パスワードの利用が可能な）実験となった。

以下では、特に 2003 年 9 月合宿の申し込みに絞って報告する。

WIDE 共有パスワードを利用しないで WIDE メンバ証明書を原則利用するにあたり、考慮すべき点がいくつかあった。

(1) 代理申し込みに対する考慮
(2) WIDE 番号がまだ割り当てられていなくて WIDE メンバ証明書が発行されていない場合に対する考慮

(1) に関しては、合宿参加者の代理で申し込みをする場合があり、秘書業務を行う人など WIDE メンバではない方が合宿申し込みをできるようにする必要があった。このような秘書モデルは現実にはよくあることだが、実際の合宿参加者が WIDE メンバ証明書と秘密鍵を秘書に渡すのではなく、WIDE メンバ証明書よりも有効期限を短くした秘書専用の「秘書さん証明書」を発行して、実質申し込みのみに使える方法を試みることにした。

実際には、3 枚発行された。発行時には、合宿参加者から「秘書さん証明書」の申請を moCA オペレータが受け、合宿参加者に電話等で意思確認を行う予定であったが、合宿参加者と連絡をとるのが難しく、秘書の方をあらかじめ知っている他の方に秘書の本人確認を依頼することもあった。

今回の方法では、秘書が 1 人で何人分もの代理申し込みをするには人数分の「秘書さん証明書」が必要となり不便である。そこで、このようなケースでは例外的に ID／パスワード 1 組を秘書に配付して人数分の申し込みができるようにした。

(2) に関しては、合宿参加申し込みと WIDE メンバ登録がほぼ同時期で、まだ WIDE 番号が割り当てられていない場合があり、従来は仮番号を申し込み時に割り当てて利用していた。WIDE メンバ以外の方が合宿に参加するにあたっては、あらかじめボードの承認が必要となることから、今回は、参加承認が得られた人に対し、有効期限が短く仮番号が記載された「テンポラリ証明書」を発行することにした。

実際には、3 枚発行されたが、テンポラリ証明書が使われる前に、WIDE メンバ証明書の発行が間に合うケースがあり、実際に申し込みに使われたのは 1 枚のみであった。

WIDE メンバ証明書に関しては例年通り 6 月に一

斉配付した他、新規に WIDE メンバが登録されると同時に WIDE メンバ証明書を配付した。6 月の一斉配付後、7 月の合宿参加申し込みまでの間に WIDE メンバ証明書を利用するイベントがあまりなかったこともあり、WIDE メンバ証明書の紛失などによる再発行が 15 件ほどあった。

合宿参加申し込み期間中の moCA オペレーションは、WIDE メンバ証明書、秘書さん証明書、テンポラリ証明書の 3 種類の証明書を発行できる体制を敷いて対応した。表 4.1 に、各種証明書の特徴をまとめる。また、今回の実験に関して、合宿プログラム委員会、合宿参加申し込み受付業務を請け負う株式会社イーサイド、および、moCA WG を含めた全体の役割分担の状況を参考として図 4.1 に示す。

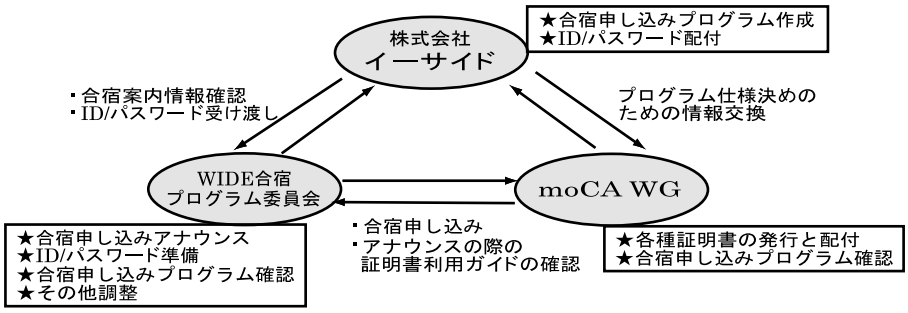


**図 4.1.**　合宿申し込みにおける役割分担

**表 4.1.**　各種証明書の特徴

| | | WIDE メンバ<br>証明書 | 秘書さん<br>証明書 | テンポラリ<br>証明書 |
|---|---|---|---|---|
| 内容 | 有効期限 | 2004 年 6 月末<br>（1 年） | 2003 年 9 月中旬<br>（2 ヶ月） | 2003 年 9 月中旬<br>（2 ヶ月） |
| | Subject.CN | “ WIDE 番号　氏名 ” | “ WIDE 番号　[sec] 氏名 ”<br>↑　　↑<br>合宿参加者の　秘書さんの | “ 仮番号　氏名 ” |
| 申請方法 | | WIDE メンバ登録<br>申請をもって申請<br>とみなす | 合宿参加者が申請 | ボードへの合宿参<br>加申請をもって申<br>請とみなす |
| 発行数 | | 約 750 | 3 | 3 |

**表 4.2.**　実験中に WIDE メンバ証明書が使えると確認できたブラウザの一覧

- Win XP SP1 + IE6
- Win XP SP1 + Netscape 7.02
- Win 2000 + Mozilla 1.4
- w3m/0.3.2.2-stable-m17n-20021207
- w3m 0.4
- MacOS X (v10.2) + Wazilla 1.3
- MacOS X (v10.2) + Mozilla 1.4b
- NetBSD 1.6U + Mozilla 1.3
- NetBSD 1.6U + mozilla 1.3.1
- FreeBSD 5.0RELEASE + Mozilla 1.3.1
- FreeBSD 4.8 (+KAME snap) + Mozilla 1.4
- Debian GNU/Linux + Mozilla 1.3.1
- Phoenix 0.6
  chrome://pippki/content/pref-certs.xul にアクセスするとユーザ証明書を取り込める
- Netscape 7.1

WIDE メンバ証明書が使えない環境から合宿参加申し込みを行うことも想定して、例外的に個別のID／パスワード配付も行えるようにしたが、結果としてパスワード配付件数は 19 であり、合宿参加者約 280 名のうち 90%以上が証明書を使って申し込みを行った。WIDE メンバは様々な OS やブラウザを利用しているが、MacOS を含め、多くの環境のブラウザで証明書対応が安定してきたということが証明書利用の増加に影響していると思われる（表 4.2）。今後も、合宿申し込みでの証明書利用を継続し、定例化してゆきたい。

## 第 5 章　証明書の利用場面拡大と moCA の今後の課題

様々な場面で、クライアント証明書（WIDE メンバ証明書）の利用者数が増えている一方、moCA としての課題も挙がってきている。

WIDE メンバ証明書の有効性を即時に判断できるようにするには、CRL の即時発行を始めとする運用体制の改善が必要である。また認証技術をより高度に活用するためには、証明内容の参照に留まらずに発展した実験活動が必要である。これらは前回の合宿において挙げられた課題であるが、未だ実現できていない。いずれも moCA WG にとって急務である事項なので、早急に取り組む必要がある。

また今後は、moCA が発行した証明書の、より正確な利用者数がわかるような準備があることが望ましいと考えられる。これには証明書利用者に対する、統計情報収集への協力の働きかけなどが考えられる。

## 付録　CA 鍵のフィンガープリント一覧

### 概要

商用ルート CA では最初からブラウザにルート CA 証明書が登録されているが、実験用ルート CA ではユーザがインストールする必要がある。CA 鍵のフィンガープリントは、CA 証明書をインストールする際に、CA を信用するかどうかを判断するために必要な確認情報として使われる。

フィンガープリントの確認は、ブラウザの CA 証明書表示機能、または、CA 証明書を PEM 形式で保存した後 OpenSSL コマンドを実行することによりできる。

フィンガープリントの計算方法には SHA1 と MD5 の 2 種類があるため、後述する一覧では 2 種類の値を記述しておく。しかし、どちらか一方を確認するだけで十分である。なお、Windows の証明書の表示では SHA1 の値が表示され、Netscape では MD5 が、Mozilla の場合は SHA1 と MD5 の両方が表示される。

### フィンガープリント一覧

以下に、2004 年 1 月現在の各 CA 鍵のフィンガープリントを示す。

WIDE ROOT CA

SHA1 フィンガープリント
3560 185D 83DC CBB7 0EBB 45AD 1E9B F529 A816 0562

MD5 フィンガープリント
2B:68:BD:1B:26:28:2A:AC:CF:F3:45:90:1D:6C:2A:9C

moCA

SHA1 フィンガープリント
487E 16E1 746E 5C16 8A7D C55D DE80 37E8 9241 7FA3

MD5 フィンガープリント
17:FD:D2:8A:C2:36:5D:0E:0B:A7:69:BC:9D:7F:E6:97

SOI CA

SHA1 フィンガープリント
0A92 34A8 B589 C835 6101 3151 CBC6 4F18 1ACE 6D4D

MD5 フィンガープリント
7B:23:02:D1:76:37:44:81:76:35:DA:8A:51:BF:B5:48

AI3 CA

SHA1 フィンガープリント
0AE8 76F5 7240 BA67 99B9 A200 C94C 1650 FBB5 29F0

MD5 フィンガープリント
19:89:C9:CF:D5:E1:8F:E1:65:51:92:72:A2:49:96:0F