

合宿申し込みでの moCA 活用事例

2004 年 8 月 27 日

初版 2004 年 1 月 5 日

moCA WG

櫻井三子

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、秘書が一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/パスワード一

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「テンポラリー証明書」を発行することにした。

実際には、3 枚発行されたが、テンポラリー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、テンポラリー証明書の 3 種類の証明書を発行できる体制を敷いて対応した。表 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 1 に示す。

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 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。

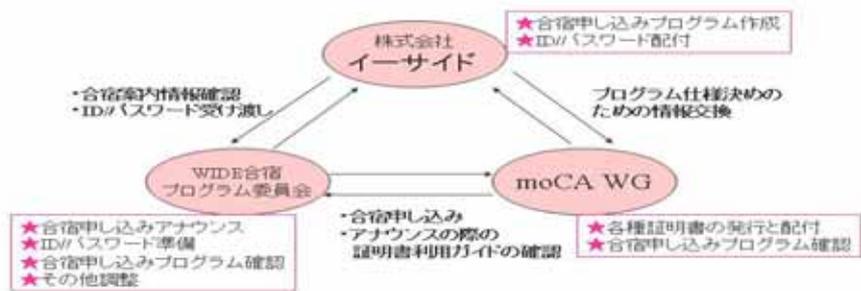


図 1. 合宿申し込みにおける役割分担

表 1 各種証明書の特徴

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

表 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
 - MacOSX (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 + Mozilla1.3.1
 - Phoenix 0.6
- chrome://pipcki/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

Copyright Notice

Copyright (C) WIDE Project (2004). All Rights Reserved.