WIDE moCA(members oriented Certification Authority)における WIDE メンバ証明書管理の状況について

2005 年 1 月 27 日
moCA WG
櫻井三子(mine@ax.jp.nec.com)

概要:
WIDE プロジェクトのセキュリティエリアには、認証インフラの一つである PKI(Public Key Infrastructure)技術の普及を目指し、WIDE プロジェクト内部向け CA の運用実験を行なっているワーキンググループがある。
WIDE プロジェクト内部向け CA である moCA(members oriented CA)は、2004 年から運用フェーズに入った。ここでいう運用フェーズとは、「エンドユーザが証明書をある程度日常的に利用する」段階をさしている。本レポートでは、その運用状況として、証明書発行、再発行、失効について報告する。
moCA はエンドユーザ数 1,000 人未満の CA であり、Windows, UNIX, MacOS などさまざまなブラウザ環境で利用されている点が特徴的である。運用フェーズに入ってみると証明書再発行や失効が月に数件程度の頻度でコンスタントに発生することがわかってきた。証明書の再発行理由の多くは、紛失によるものであり、再発行と同時に失効させるような機能が CA に必要であるといった知見が得られた。
このような運用の積み重ねが、組織ごとのリーズナブルな PKI の運用構築ノウハウにつながり、最終的に PKI の普及へとつながっていくと考え運用データを公開する。

1. はじめに

われわれは、1996 年より CA 運用実験を開始している。証明書の発行といった構築段階については WIDE プロジェクトという組織の特徴を考えながらいくつかの方法で試行錯誤を行なってきた。しかし、PKI の運用上の重要な課題の一つとされている再発行や失効については、証明書が利用されていなければ必要性すら実感しづらく、具体的な検討ができていなかった。
WIDE プロジェクトの研究活動の中で証明書を利用する場面が増えた今、エンドユーザ数 1,000 人未満の CA で、日々の証明書管理の状況を実際のデータで得られるようになった。以下では、moCA という CA の特徴について述べた後、証明書発行、再発行、失効の状況について報告する。

2. WIDE メンバ証明書の運用形態

moCA は、エンドユーザ用証明書とサーバ用証明書の 2 種類を発行している。

エンドユーザ用証明書としては、WIDE メンバ証明書、秘書さん証明書、テンポラリ証明書の3種類がある。以降は、エンドユーザに日常的に使われるWIDEメンバ証明書に絞り、運用形態について述べる。

(ア) WIDE メンバ証明書の使われ方

現状では、Web ページのアクセス時のユーザ認証に使われることが主であるが、暗号メール(S/MIME)に使っているメンバもいる。Web ページの具体例としては、以下がある。

- WIDE メンバ限定のホームページ
- WIDE 研究会合宿の参加申し込みページ
- WIDE 研究会アンケート記入ページ

また、WG メンバ限定のホームページがある場合、必要に応じて、WG メンバであることの認証にも使われている。

(イ) WIDE メンバ証明書の有効期間

1 年間である。その発行サイクルは毎年 6 月中に発行され、翌年の 7 月 1 日まで有効となるように、有効期限をそろえている。

(ウ) WIDE メンバ証明書発行数の規模

WIDE メンバ証明書発行数の規模は、1,000 程度である。

(エ) WIDE メンバ証明書発行方法

CA オペレータが 3 人体制で WIDE メンバの鍵と証明書を発行する。毎年 6 月時点でのWIDEメンバにはメールで一斉に鍵と証明書(PKCS#12 ファイル)の配付を行なう。配付は自動化しており、作業は一人で行なえる。一斉配付後に WIDE メンバに登録された場合は、メンバ登録と同時に、自動的に鍵と証明書を発行し、メールで配付が行なわれるようにしている。

(オ) WIDE メンバ証明書保管方法

WIDE メンバは、メールで配付された鍵と証明書を、PC のハードディスク上にインストールして利用する。そこで、WIDE メンバには、各自での鍵と証明書のバックアップを推奨している。

また、CA オペレータが作成した WIDE メンバ証明書の鍵は証明書配付と同時に削除し、保管しないようにしている。

(カ) WIDE メンバ証明書再発行方法

WIDE メンバが証明書の紛失などにより証明書を使えなくなった場合には、WDE メンバからの申し出にしたがって、CA オペレータが手動で鍵と証明書をあらたに発行しメールで配付する。

また、WIDE メンバのメールアドレスが変更になった場合には、WIDE メンバ登録情報(WIDE-DB)の更新と同時に、自動的に鍵と証明書をあらたに発行しメールで配付する。

(キ) WIDE メンバ証明書失効方法

WIDE メンバが証明書を使えなくなった場合には、WIDE メンバからの申し出にしたがって、CA オペレータが手動で証明書を失効させる。

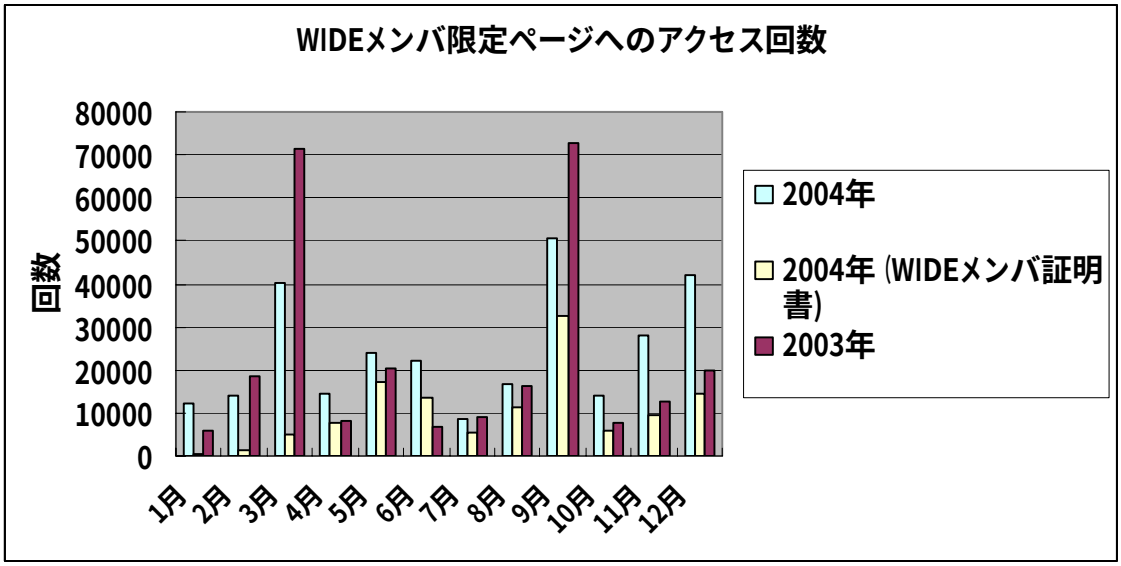
WIDE メンバが WIDE プロジェクトを脱退した場合には、CA オペレータが手動で証明書を失効させる。

失効情報は、Web サーバなど、WIDE メンバを認証する側が入手し、失効した証明書が使われていないかを確認できるようにする必要がある。失効情報の提供手段として、失効情報を CRL(Certificate Revocation List)という形式にまとめて公開する方法があり、moCA では定期的に発行して配付する。

3. WIDE メンバ証明書発行と利用の状況

2004 年 6 月に WIDE メンバ証明書の一斉配付を行なった時の発行数は、767 である。また、6 月以降にメンバ登録した WIDE メンバへの発行数は、2004 年 12 月 31 日現在で 51 である。

次に、WIDE メンバ証明書利用の状況を調べるため、日常的に利用されている WIDE メンバ限定ページへのアクセス回数をグラフ 1 に示す。



グラフ 1: WIDE メンバ限定ページへのアクセス回数

WIDE メンバ限定ページアクセス回数の総数は、2003 年で 269,452 回、2004 年で 287,447 回であり、2003 年と 2004 年とでアクセス傾向の変化は特にない。2004 年 2 月下旬からはWIDE メンバ限定ページへのアクセス時にWIDE メンバ証明書が利用されるようになっている。2004 年の WIDE メンバ証明書による WIDE メンバ限定ページへのアクセス回数の総数は、124,206 回となった。これは、2004 年のアクセス回数総数の約 43%を占めている。

2003 年以前を含め、これまでに WIDE メンバ証明書で Web ページへのアクセスができたと報告されたブラウザを表 1 に、できなかったと報告されたブラウザを表 2 に示す。

表 1: WIDE メンバ証明書で Web ページアクセスができたブラウザ

- **Firefox 1.0 on FreeBSD 5.3R**
- **Firefox 1.0 on FreeBSD 4.10**
- **Firefox 1.0 on NetBSD 2.0**
- **Internet Explorer 6 on WindowsXP SP2**
- **Internet Explorer 6 on WindowsXP SP1**
- **Internet Explorer 6 on WindowsXP**
- **Internet Explorer 5 (128bits) on Windows2000**
- **Internet Explorer 5 (128bits) on WindowsNT**
- **Internet Explorer 5 (128bits) on Windows95**
- **Internet Explorer 5 (56bits) on Windows98**
- **Internet Explorer on WindowsXP SP1**
- **lynx on UNIX**
- **Mozilla 5.0 on MacOSX**
- **Mozilla Firefox 0.8**
- **Mozilla Firebird 0.7.1(日本語化版) on MacOSX 10.3.2 (Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; ja-JP; rv:1.5) Gecko/20031026 Firebird/0.7)**
- **Mozilla Firebird (旧 Phoenix 0.6)**
- **Mozilla 1.5 on MacOSX 10.3.2**
- **Mozilla 1.4b on MacOSX (v10.2)**
- **Mozilla 1.4 on MacOS X v10.2**
- **Mozilla 1.4 on Windows2000**
- **Mozilla 1.3.1 on FreeBSD-5.0**
- **Mozilla 1.4 on FreeBSD 4.8 (+KAME snap)**

- Mozilla Firebird 0.7 on NetBSD 1.6ZG
- Mozilla 1.3.1 on NetBSD-1.6U
- Mozilla 1.3 on NetBSD 1.6U
- Mozilla 1.3.1 on Debian GNU/Linux
- Mozilla 1.0
- Wazilla 1.3 on MacOS X (v10.2)
- Netscape Navigator 7.02 on WindowsXP SP1
- Netscape Navigator 7.1
- Netscape Navigator 7.0
- Netscape Navigator 6.x
- Netscape Navigator 4.x
- Netscape Navigator on MacOSX (例外あり)
- Opera7.23 on WindowsXP
- Opera on Windows
- Opera on MacOSX
- Safari 1.2 on MacOS X
- Sleipnir 1.66 on WindowsXP SP2
- w3m/0.3.2.2-stable-m17n-20021207 on UNIX
- w3m-1.7 on UNIX
- w3m/0.3.2.2-stable-m17n-20021207
- w3m 0.4

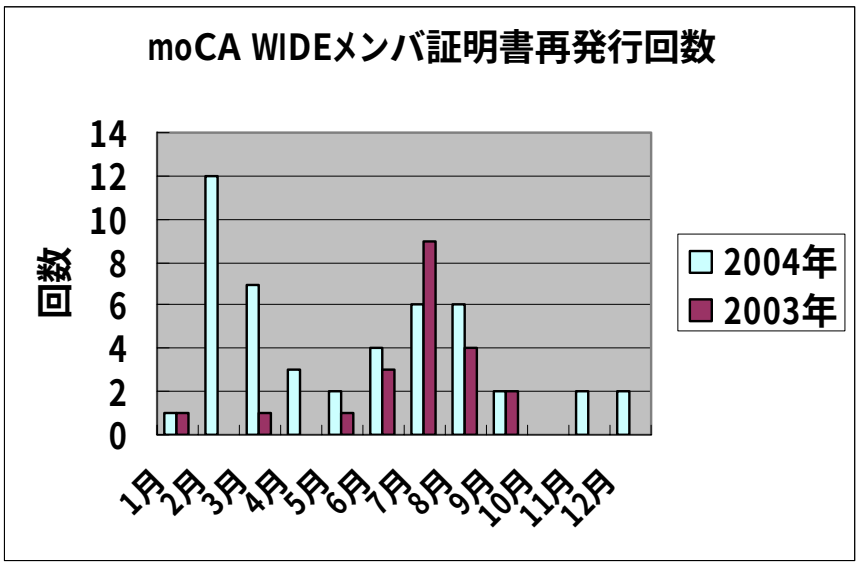
表 2: WIDE メンバ証明書で Web ページアクセスができなかったブラウザ

- Internet Explorer 5.0 on MacOSX
- Internet Explorer 5.1 on MacOSX
- Netscape Navigator 7.0PR1 on MacOSX 10.2
- Safari 1.1(v100.1) on MacOSX 10.3.2
- Safari on MacOSX (2005.01.20)
  「Safari はサーバ"widecamp.e-side.co.jp"にセキュリティ保護された接続を確立できませんでした。」と言われ NG。ただし、https://member.wide.ad.jp/ は OK
- Konqueror 3.14 on Linux(distribution:gentoo, kernel 2.4.22)

4. WIDE メンバ証明書再発行の状況

2004 年の証明書再発行総数は、47 であった。2004 年、および、2003 年の月ごとの

証明書再発行数をグラフ 2 に示す。また、WIDE プロジェクトや moCA に関連した行事について図 1 に示す。



グラフ 2: WIDE メンバ証明書再発行回数

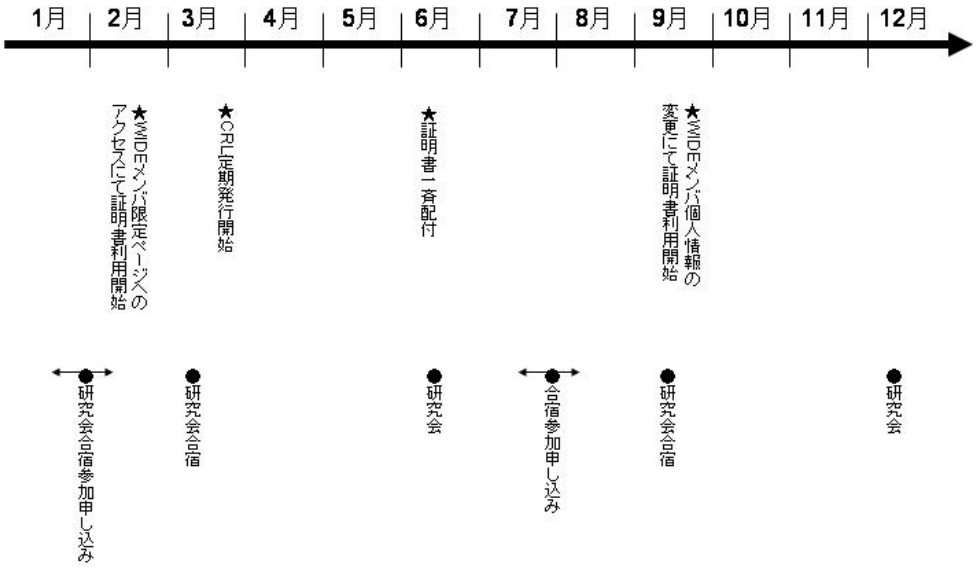


図 1: WIDE プロジェクトおよび moCA 関連の行事(2004 年)

グラフ 2 と図 1 を照らし合わせると、年 2 回の研究会合宿参加申し込みの期間中に再発行が多くなっていることがわかる。2003 年 3 月の研究会合宿参加申し込みでは、証明書再発行数が多くないが、これは、まだ申し込み時に WIDE 共有パスワードを利用できるようになっており、証明書の利用自体が少なかったためである。2004 年 2 月には特に証明書再発行数が多くなっているが、WIDE メンバ限定ページのアクセス時に証明書を利用する環境が整えられたことが影響していると思われる。その後は、コンスタントに証明書再発行が発生している。

証明書再発行の理由については、以下のケースがあった。

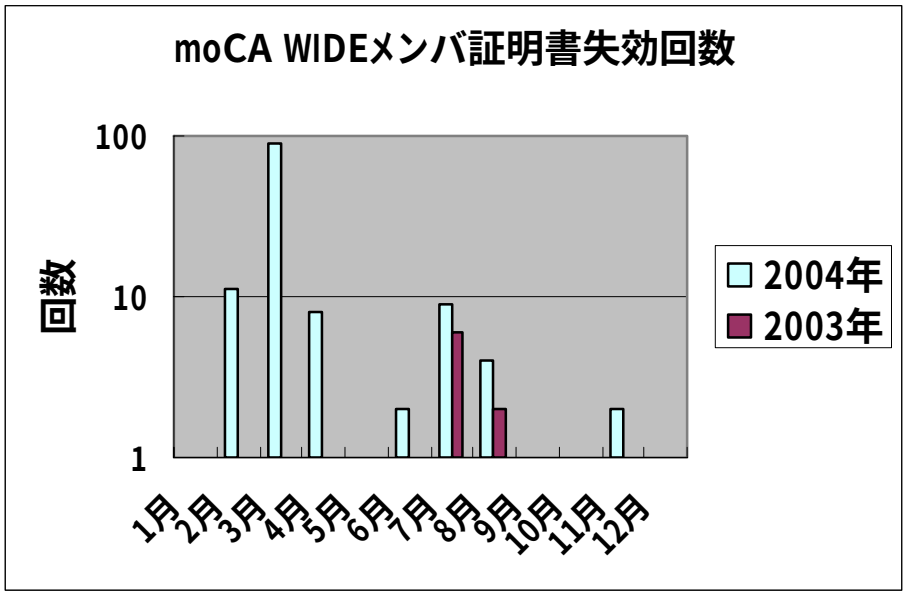
- PC のハードディスク故障により証明書を紛失した
- 証明書配付メールがスパムと間違えられて処理され、届かなかった
- 新規 PC に入れ替えた際に、鍵のバックアップが見つからなかった
- 鍵が必要になった場面で、手元になかった
- 登録しているメールアドレスが変わった

なお、再発行の多くの理由は、証明書を紛失した、である。

現状、再発行依頼を受けてから再発行までにかかる時間は、1 営業日以内である。

5. WIDE メンバ証明書失効の状況

2004 年の証明書失効総数は、128 であった。2004 年、および、2003 年の月ごとの証明書再発行数をグラフ 3 に示す。



グラフ 3: WIDE メンバ証明書失効回数

2003 年は、研究会合宿参加申し込み期間に証明書再発行を依頼したとき以外には証

明書失効が行なわれていない。2004 年 3 月は、証明書失効が多数発生している。これは、WIDE プロジェクトの脱退メンバの失効処理を行なったためである。また、2004 年 3 月までは、証明書再発行と同時に証明書失効を行なうかどうかを運用として明確に決めていなかったこともあり、失効したりしなかったりという状況になっていた。2004 年 4 月以降は、証明書再発行と同時に証明書失効を行なうようにしている。グラフ 2 と 3 とを比較すると、2004 年 3 月以降の失効は、再発行がコンスタントに発生しているのと同期してコンスタントになってきている。しかし、再発行と失効の作業が自動的に連動するようにはしておらず、CA オペレータが失効作業を忘れてしまい、何日も遅れることがあった。

CRL は、2004 年 3 月より毎日発行して Web サーバ上で公開し始めた。一部の S/MIME 環境では CRL による失効確認が必須となっている、という報告を得ている。しかし、WIDE プロジェクトで Web サーバとしてよく使われている Apache+mod_ssl の環境では、Web サーバ管理者が手動で CRL を取得して設定しなければならない点で手間がかかるためか、現状では CRL を利用した失効確認は特に行なわれていない。

6. 考察

WIDE メンバがさまざまな OS 環境を利用しているという特徴に対し、WIDE メンバ証明書も Windows, UNIX, MacOS などさまざまなブラウザ環境で利用されている。これは、PKCS#12 ファイルをハードディスクにインストールする方式が功を奏していると思われる。

ただし、エンドユーザの PC のハードディスクに鍵をインストールして利用する方法では、エンドユーザが鍵を紛失しやすく、実際にコンスタントに証明書再発行が発生している。したがって、定常的かつ迅速に証明書の再発行を行なえる運用体制が必要である。再発行の理由の多くは、鍵の紛失によるものであることから、証明書の再発行と失効を連動させる機能を追加するべきである。

日常的に利用される WIDE メンバ限定ページへのアクセスのうち、約 43%は WIDE メンバ証明書を使ったアクセスとなったが、少しずつ利用率が下がってきている。これは、潜在的にはもっと鍵を紛失している可能性が考えられ、再発行申請をわかりやすくすることや、継続して WIDE メンバ証明書を利用すると便利なページを増やしアピールすることが必要である。

7. おわりに

本レポートでは、運用フェーズ 1 年目の CA 運用状況について報告した。

証明書発行、再発行、失効といった証明書のライフサイクルについて一通り運用を経験し、運用のさらなる効率化や作業ミスを防ぐべきことなどが見えてきた。

CRL を利用した失効確認や、OCSP(Online Certificate Status Protocol)のような CRL

以外の方法による失効確認をしやすい環境を作ることについては、今後の課題である。同時に、失効された証明書が Web ページへのアクセスに使われてしまう可能性について、実際の失効理由と照らし合わせて検討し、失効管理の適切なレベルを見極めたい。

謝辞

PKI の普及という目標を理解してくださり、長期にわたる運用実験に参加してくださっている WIDE プロジェクトの皆様に深く感謝いたします。広く普及しているかはさておき、PKI の導入自体は珍しいことではありません。しかし、実際に使われている環境の中で運用データを得ながら、研究報告としてそれらのデータを使える機会は、WIDE プロジェクト以外では考えられないと思います。