第 XVIII 部

公開鍵証明書を用いた
利用者認証技術

第 18 部
公開鍵証明書を用いた利用者認証技術

第 1 章　moCA WG の 2004 年度の活動概要

1.1 活動概要

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いる。この実験では WIDE メンバに対する証明書の発行・失効・更新を行い、利用環境や利用法に関する情報交換を行っている。

2004 年度はこれまでの運用を振り返る意味で運用手順のドキュメント化を行い、WIDE 内部に公開した。また moCA をより多くの WIDE メンバに使ってもらえるように、WWW サーバの PKI 対応設定例や moCA を応用した（PKI 対応の）プログラム例についてドキュメント化を行い、WIDE 内部に公開した。

- 「moCA におけるサーバ証明書の発行手順（オペレータ用）」
- 「Apache を moCA 対応とするための設定方法について」
- 「moCA 対応プログラムの例」

一方、WIDE メンバ証明書が使われる上で moCA の運用や機能上の改良の必要性が上がってきた。運用の改善のためには証明書の利用用途を反映するための証明書プロファイルの改良や、証明書の配布をお知らせするメールをスパムメールと区別しやすくするための変更が行われた。

機能の改良のためには、CRL を短期間の間隔で定期的に発行する機能が追加された。これは WIDE メンバ証明書の再発行申請にともなう失効が多く発生し、失効情報をよりタイムリーに伝達する必要があると考えられたためである。またほかのメンバの証明書を入手しやすくするため、リポジトリの必要性が挙げられたが、作業が進まず完了しなかった。

今後はこれまでに挙がった改善策を実施する必要がある。なお、機能的な改善のためには、環境構築などを担当できる人手を確保することは課題である。また、WIDE 外での証明書の利用方法の確立などのほか、運用フェーズで取ることができたデータから、認証局運用の知見を得ることが課題である。

1.2 moCA の運用上の改善

1.2.1 証明書プロファイルの改良（keyUsage の変更、CRLv2 への対応）

これまで moCA によって発行された証明書には、鍵用途（keyUsage）として下記のものが設定されていた。

- digitalSignature（電子署名）
- keyEncipherment（鍵の暗号化）
- nonRepudiation（否認防止）
- dataEncipherment（データ暗号化）
- keyAgreement（鍵合意）

このうち nonRepudiation（否認防止）と keyAgreement（鍵合意）は WIDE メンバ証明書では使われることを想定していない。そこで 6 月の一斉配布の機会に合わせ、これらが有効にならない証明書プロファイルに変更した。また CRL に Authority Key Identifier（認証局の鍵の識別値）の拡張フィールドを加えられるよう、CRLv2 に対応した。

1.2.2 配布メールの改良

WIDE メンバ証明書は電子メールを使って配布される。この配布メールがユーザにとって問題になることがあった。1 つは添付ファイルのファイル名である。このファイル名はユーザのメールアドレスを元につけられていた。そのためユーザのメールアドレスに .com が含まれた場合に、配送途中で配布メールがウィルスである疑いをかけられユーザに届かないことがあった。もう 1 つはメールの Subject に “delivery” という文字列が含まれており、これがスパムメールと判断されてしまうことがあった。いずれも文字列の変更等で対処した。

1.2.3 fingerprint の正しさ

moCA では CA 証明書の正しさの検証の利便のため、Web ページに fingerprint を掲載している。こ

の fingerprint が正しいものかの確認の問い合わせがあった。fingerprint は元来、複数の異なるメディアによって伝えられた値を比較することで、証明書データの信憑性を向上させるが、Web ページに複数掲載されている場合にはいずれかが改ざんされた場合に、どれが正しいのか判断しかねる状況になる。そこで掲載箇所を統一した。

なお、実際には fingerprint 値の正しさが確認できればよいという要望であった。

1.2.4 CRL 自動発行

WIDE メンバ証明書は、年間を通じて約 1 割が失効される見込みであることが統計から判明した。とくに 2004 年 3 月は異動の時期であり、失効要求が多く発生した。証明書の失効を証明書検証の結果に反映するには、適切な間隔で CRL を発行し公開しておく必要がある。

これまで moCA が発行する CRL は、人手によって 1 ヶ月に一度程度の頻度で発行されていた。しかしこれでは失効情報の伝達に大幅な遅れが生じ、また人手であるため、間隔が一定でないという問題があった。そこで CRL をより短期間に自動的に発行されるようにした。具体的には 1 日に一度発行する。

CRL の自動発行は CRL を提供するサーバの運用レベルが、CRL を利用した証明書検証時の結果に直接的に影響する。CRL を提供するサーバが運用を停止していると、証明書を検証するプログラムによって証明書検証に失敗することがあるからである。

しかしこれまでに moCA が定期的な点検以外でダウンしたことが少なかったことから、CRL の自動発行と提供を実施することとした。ただし CRL に含まれる next update の値は 1 ヶ月に据え置きとし、例え CRL を提供できない場合でも、証明書検証プログラムがあらかじめ入手していた CRL を 1 ヶ月間は利用できるようにした。

1.3 moCA 機能上の改良

1.3.1 証明書リポジトリ

S/MIME を使ったメールを利用する場合、暗号化のためにはメールの送信相手の証明書が必要になる。しかし、moCA は WIDE メンバ向けの証明書配布を行っておらず、S/MIME のメールを送信できる相手が限定されてしまう。

そこで moCA に証明書リポジトリの機能を、OpenLDAP を使って提供することが検討された。しかしまだ作業途中のためリポジトリは提供されていない。なお LDAP のリポジトリでは下記の LDIF を使った指定によって格納した証明書データを提供することができる（IETF PKIX WG の活動から、binary: の記述方法がなくなる可能性がある。）。

```
userCertificate;binary:< file:///user_cert.der
```

LDAP を使った基本的なリポジトリの提供ができたあとには、WIDE メンバの情報（証明書にはメールアドレスや WIDE 番号が含まれている）の保護のため、配布範囲を限定するアクセスコントロールが必要になると考えられる。

1.3.2 相互認証証明書

moCA が発行している証明書は WIDE メンバ以外のユーザによって検証されることがある。その際には moCA の証明書（CA 証明書）の有効性が事前に確認されている必要があるが、WIDE メンバでないユーザは WIDE ルート認証局の証明書の有効性を判断できない。

moCA ML には、WIDE メンバ以外のユーザが WIDE メンバ証明書の有効性を確認できるよう、相互認証証明書（crossCertificate）は使えないか、という問い合わせがあった。

WIDE 外の認証局を信頼点とするユーザが WIDE メンバ証明書の有効性を検証するには、その認証局のツリーに含まれている認証局から、WIDE ルート認証局か、moCA に対して相互認証証明書が発行されている必要がある。相互認証証明書は、一般的に認証局の運用内容を確認した上で発行されるため、WIDE の認証局の運用内容がわかる（ポリシーとの比較等）状態が必要になる。

相互認証証明書は、WIDE メンバ証明書の利用範囲を WIDE 外に広げる効率的な方法であるため、moCA WG で実験ができるとよいと思われる。

1.4 話題

2004 年は、WIDE での貢献が期待されるメンバやグループに送られる WIDE 賞を受賞することができ、また WIDE メンバ向け（WIDE confidential）の Web ページの認証方法が、共通パスワードから WIDE メンバ証明書に移行された年である。

2004 年 9 月頃、クライアント認証を行う https を Apache2 で行う際に、POST メソッドが正常に動作

しないことが確認され、WIDE メンバ向けの Web ページで共通パスワードが使われることがあった。しかし 12 月の WIDE 研究会で、この問題を回避するパッチが見つかっている。

```
http://issues.apache.org/bugzilla/
show_bug.cgi?id=12355
```

また WIDE サーバ証明書が WIDE メンバ以外のユーザによって検証されるケースで、その SSL/TLS の説明についての議論が挙がった。

WIDE メンバ以外のユーザが参加を行う Internet Conference の参加申し込み用 Web サーバでは、moCA が発行した WIDE サーバ証明書が使われている。WIDE メンバ以外のユーザに対して WIDE Root CA を信頼点にすることは想定できないため、この Web ページでは証明書の有効性に関する説明を行っている。これに対して証明書の検証方法と SSL/TLS の意味について説明が不十分であるという指摘を受けた。これまで、サーバ証明書の有効性を確認するための適切な手段に関する議論は行われているが、それに加えて一般のユーザに対する適切な説明を提供することが改めて指摘された状況である。

1.5 課題

moCA の機能と運用に関する改善点は、2004 年に取り組んだもの以外にも残っている。証明書のバックアップ方法をユーザに周知したり、OCSP レスポンダの提供に関する検討などである。また moCA の運用フェーズにあたって、その上で実施できた運用実験のデータや試行錯誤から、認証局運用の知見を見出していくことが課題であると考えられる。

第 2 章　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

概要

WIDE Project 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」段階を指している。本章では、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。

2.1 はじめに

我々は、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 Project 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ってきた。しかし、PKI の運用上の重要な課題の 1 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 Project 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。

2.2 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・合宿の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）の配付を行う。配付は自動化しており、作業は 1 人で行える。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、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鍵と証明書を新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新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 Project 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。

2.3 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図 2.1 に示す。

WIDE メンバ限定ページアクセス回数の総数は、

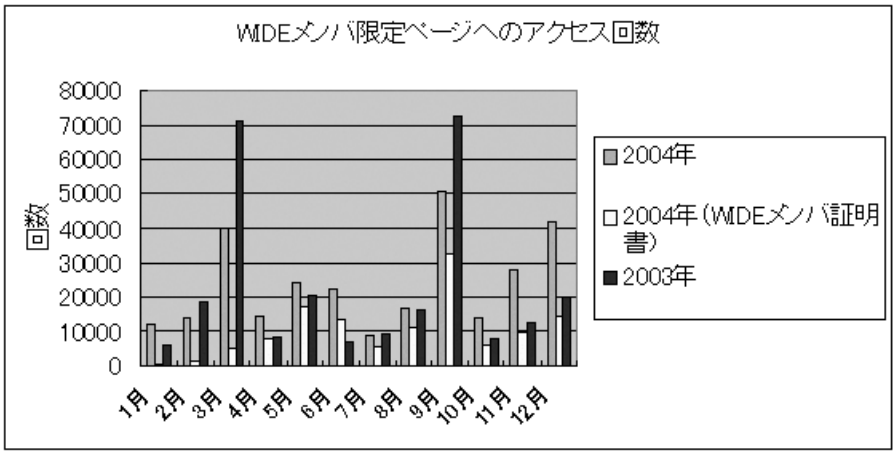

図 2.1.　WIDE メンバ限定ページへのアクセス回数

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2.1に、できなかったと報告されたブラウザを表2.2に示す。

表2.1. 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 (128 bits) on Windows2000
- Internet Explorer 5 (128 bits) on WindowsNT
- Internet Explorer 5 (128 bits) on Windows95
- Internet Explorer 5 (56 bits) 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 2.2.　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)

2.4 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図 2.2 に示す。また、WIDE Project や moCA に関連した行事について図 2.3 に示す。

図 2.2 と図 2.3 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

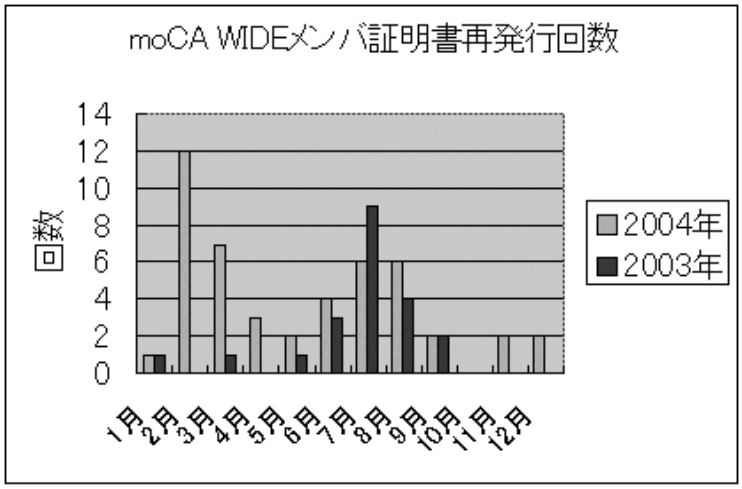

図 2.2.　WIDE メンバ証明書再発行回数

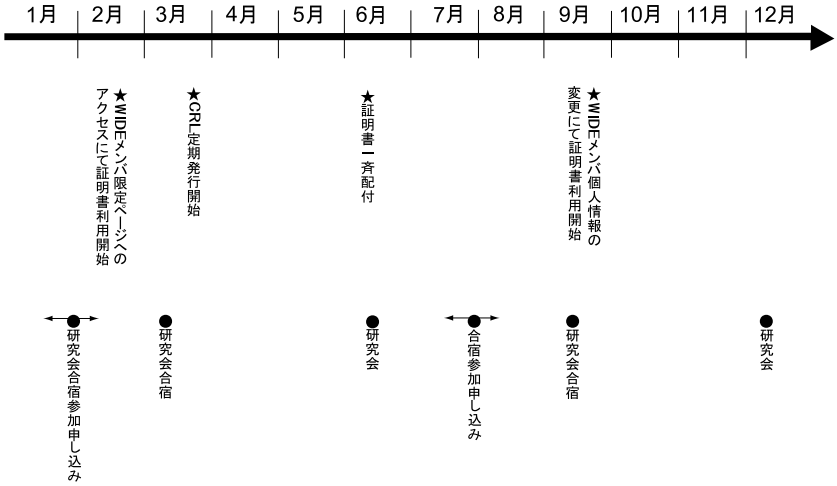

図 2.3.　WIDE Project および moCA 関連の行事（2004 年）

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。

2.5 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失効回数を図2.4に示す。

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 Projectの脱退メンバの失効処理を行ったためである。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うようにしている。図2.2と図2.4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 Project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われていない。

2.6 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

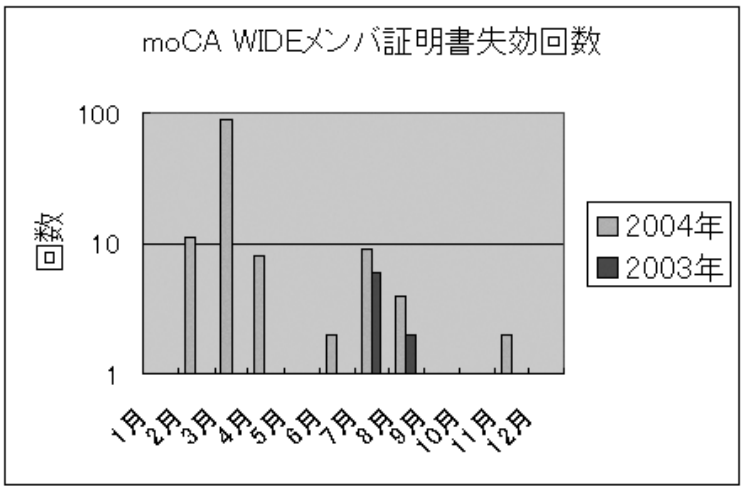

図2.4. WIDEメンバ証明書失効回数

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。

2.7 おわりに

本章では、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。

付録　CA 鍵のフィンガープリント一覧

概要

PKI は公開鍵を使った認証技術である。PKI を利用した認証は、公開鍵を使って作成された電子署名を検証することで行われるため、その公開鍵が正しく検証者に渡っていなければならない。WIDE の各認証局が発行した証明書を検証するには、検証を行うもの（検証者）が各認証局の証明書を原本と違わないように保持している必要がある。

moCA では、moCA 対応のサーバ（クライアント認証を有効にした SSL 等のサーバ）を認証したり、WIDE メンバ同士が電子メールのやり取りを行って相手を認証したりすることを証明書の利用場面として想定している。したがって WIDE メンバは検証者であり、また moCA 対応のサーバも検証者である。

ここでは、WIDE における証明書の検証者があらかじめ入手した認証局の証明書を検証することができるようにフィンガープリントをまとめる。Web ブラウザの CA 証明書表示機能、または認証局の証明書を PEM 形式で保存し、OpenSSL を利用して表示する機能を使って、保持している証明書が原本と相違のないかどうかを確認することができる。

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。その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、どちらか一方を使って確認するだけでよい。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、2005 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