第 X 部

公開鍵証明書を用いた
利用者認証技術

第 10 部
公開鍵証明書を用いた利用者認証技術

第 1 章　moCA ワーキンググループ 2008 年度の活動

moCA ワーキンググループでは CA（Certification Authority）の振る舞いや証明書の扱いに注目し、WIDE プロジェクト内で CA の運用実験を行っている。具体的には、WIDE プロジェクトにおけるルート CA である WIDE ルート CA、WIDE メンバに対する証明書の発行・失効・更新を行う moCA（members oriented CA）の運用を行っている。また、SOI ワーキンググループなど特定のワーキンググループ活動目的に応じて構築された CA を WIDE ROOT CA が認証する活動を行ってきた。これらの活動を通じて、利用環境や利用法に関する情報交換を行っている。

2008 年度は、メンバー専用ページアクセス時の認証が証明書のみになった（共有パスワードと証明書の併用を廃止）。また、WIDE メンバーに対する証明書の発行は例年と同様に行われ、メンバーの利用環境における動作検証が行われた。

2008 年度に初めて起きたイベントとして、Debian 系 OS の特定の環境で生成された鍵が脆弱であることがわかる一件があった。このときには、一度発行された証明書に対する検査が行われた。その一方で、WIDE メンバーへの証明書の配布にあたって、moCA からの電子メールがスパムと判定されてしまうような、例年発生している件への対応や、Mac OS X の Safari でうまくクライアント認証ができない技術的な課題への対応なども行われた。

第 2 章　証明書の更新

2008 年も例年と同様に 6 月に WIDE メンバ証明書およびサーバ証明書の更新を行った。

(1) WIDE メンバ証明書について

WIDE メンバ証明書の更新にあたっては、例年通り、WIDE メンバ全員に電子メールで一斉送付する方法をとった。電子メールは 2 通あり、1 通目は CA 証明書を含めた鍵対（証明書と秘密鍵）を PKCS#12 形式にて、2 通目は PKCS#12 のインポートに必要な情報を送付した。

作業にあたっては、ミスを防ぐために下記に関するチェックリストに沿って進め、約 1 週間で準備が完了した。年 1 回の作業ということで、とくに忘れがちの作業内容を昨年メモ化していたため、昨年よりも効率よく作業を進めることができた。

- 証明書有効期限の設定
- 配付文面やアナウンス文面のチェック
- 複数人への一斉配付テスト

WIDE メンバ証明書の発行数は 837 であり、昨年より 20 ほど増えた。

(2) サーバ証明書について

WIDE サーバ証明書の、2008 年 7 月以降の発行状況を以下に示す。

○ サーバ証明書発行数　37
　※ 同一サーバに対して発行された複数の証明書を含む
○ 発行対象となったサーバの数　28
○ 6 月以前から利用を継続しているサーバの数　24

WIDE サーバ証明書の更新にあたっては、例年通り、サーバ証明書の申請者自身がサーバ証明書を更新できる Web インターフェースを提供した。Web インターフェースの提供に先立ち、ミスを防ぐために以下のチェックを行った。

- 証明書プロファイル
- 発行プログラムの動作確認
- テスト発行したサーバ証明書を使った動作確認

これらの項目は、オペレーターズチェックリストと呼ばれる Web ページにまとめられており、moCA のオペレーターが確認しながら作業ができるようになっている。

(3) 更新時に起きた不具合等について

WIDE メンバ証明書の配付に電子メールを利用する方法をとってきているが、受信側でスパムメールと判定されるケースが今回も発生した。事後ではあったが、対策のため、メールサーバの設定を見直した。原因はメールサーバの envelope from が架空のメールアドレスとなってしまっていたためで、実在のメールアドレスとなるように変更した。なお、証明書が届いていないとの申告による再発行は 2 件であり、過去最少となった。

また、WIDE メンバ証明書を Mac OS X の Safari ブラウザへインストールするケースがここ数年増えている。適宜ノウハウに関して利用者間で情報交換が行われるようになったが、今年になってもなかなか解決手順が明確ではない。さらに、WIDE メンバ証明書の内容が変わったわけではないが、Mac OS X の Safari ブラウザから、合宿申込サーバへ WIDE メンバ証明書でアクセスできなくなる事象が発生した。サーバ側の設定も含めた調査の結果、共有パスワードと証明書を併用できる設定だとアクセスできず、証明書のみを受け付ける設定だとアクセスできることがわかった。

本質的には Mac OS X の Safari ブラウザの問題のようだが、対処としては、合宿申込サーバの設定を変更した。それから、同様に、WIDE メンバ専用ページのサーバ設定も証明書のみを受け付ける設定を行った。共有パスワードと証明書を併用できる設定は 2005 年 1 月から実施し、証明書のみを受け付けるまでの移行措置としてきたが、2008 年に思いがけない事象から 3 年間にわたる移行措置を終了する結果となった。

第 3 章　Debian 系 Linux で生成された鍵への対応

2008 年 5 月 13 日、Debian 系の OS で動作する OpenSSL 0.9.8c-1 から 0.9.8g-9 を使って鍵生成を行うと、リモートからのブルートフォース攻撃によって暗号鍵が予測できる脆弱性についての発表があった。

Vulnerability Summary for CVE-2008-0166
`http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0166`

moCA ワーキンググループでは証明書リポジトリを検索し、該当するサーバ証明書の管理者に通知し、再発行などの対応を行った。該当したサーバは 3 あった。証明書リポジトリの検索にあたっては、dowkd 0.9.4 を利用した。

Index of /project/extra/dowkd
`http://security.debian.org/project/extra/dowkd/`

なお、WIDE メンバ証明書はすべて認証局のサーバで生成されるため、この脆弱性は該当しないが、念のために同ツールを使って調査を行った。その結果、予測通り、該当した鍵は見つけられなかった。

第 4 章　証明書の利用環境（iPod touch）

WIDE 合宿中、WIDE メンバ証明書が iPod touch 2.0.2 にインポートできることが WIDE メンバによって確認された。メールに添付された PKCS#12 形式のファイルを開くことで、インポートすることができた。また iPod touch の Safari を使って WIDE メンバー専用ページにアクセスできることが確認された。

第 5 章　まとめ

メンバー専用ページアクセス時の認証に証明書を利用する提案を行ったのは 2002 年 5 月のことで、2005 年 1 月時点で証明書利用率が 40%、2005 年 2 月以降にサーバ設定の工夫により証明書利用率が約 80%となっていた。メンバー専用ページへのアクセス頻度が低い方からは、敷居が高すぎるとの意見があり、100%達成に向けた策を講じることができていなかったが、6 年の歳月を経て、ようやく 100%に至った。

WIDE サーバ証明書は 6 年前の 2002 年には 25 のサーバに対する証明書が発行されていた。以降、30 前後で推移しており、2008 年度、執筆時点（2009 年 2 月 9 日現在）では 28 のサーバに対する証明書が発行されている。WIDE メンバー専用ページの他に WIDE

wiki や two サーバ、CSAW（Collaboration Support Architecture for WIDE-community）、WIDE 合宿における無線 LAN 等、他ワーキンググループの活動や WIDE 合宿において利用されている。

WIDE における証明書の主な用途は、TLS/SSL におけるサーバ認証とクライアント認証であり、この状況は 6 年前と大きく変わっていない。その一方で、証明書の利用環境は OS のバージョンアップや証明書対応機器の増加にともない、常に変化してきた。ワーキンググループメンバーによる各々の利用環境に対する動作検証は、継続的に行われており、この活動は WIDE における証明書を使った認証環境を支えていると言える。

今後は、moCA の情報提供をより充実させていくことが必要とされていると考えられる。とくに、証明書インストールの手間のためにメンバー専用ページアクセスが減らないよう、証明書発行やインストールのために提供すべき情報を整理しなおしたい。

また、Debian 系 OS における脆弱性のように、PKI 技術の運用について最新動向に留意していく必要もある。暗号アルゴリズムの移行問題についても視野に入れた活動をしていきたい。

付録　フィンガープリントの一覧

本章では WIDE ルート CA の適切な利用のため、CA 証明書のフィンガープリントを記述したものである。このフィンガープリントは WIDE ルート CA の運用管理者によって正しさが確認されたもので、ユーザ環境に保存された WIDE ルート CA の証明書データが、オリジナルの証明書データと同一のものであるかどうかを確認するために使われる。

WIDE ルート CA の証明書を入手し、フィンガープリントを確認することは重要である。フィンガープリントの確認が行われていない WIDE ルート CA の証明書を使ってしまうと、間違った証明書が正しいものだとみなされてしまい、https や S/MIME などの証明書を使った認証処理において、なりすまし行為が行われてしまう危険性が高い。その場合にはすぐにその CA 証明書の利用をやめ、正しい CA 証明書を入手しなおすことをお勧めする。WIDE ルート CA の証明書の入手元である URL を以下に示す。

WIDE ルート CA（名称：WIDE ROOT CA 02）の証明書
`http://www.wide.ad.jp/ca/wideroot-cacert_4096.cer`

2008 年 12 月現在の WIDE ルート CA の証明書のフィンガープリントを以下に示す。フィンガープリントは数字の 0〜9 とアルファベットの A〜F までを組み合わせた文字列である。表示を行うソフトウェアによって文字列の間にコロンやスペースが入れられたり逆に省略されたりすることがあるが、その違いは無視してよく、文字列が合っていることを確認すればよい。

WIDE ルート CA（名称：WIDE ROOT CA 02）のフィンガープリント

sha1 の値
4C:57:B2:D5:6B:94:C2:5F:F2:CA:4A:D1:A8:3D:A4:C0:6F:EE:5C:2C

md5 の値
D2:2E:63:73:4A:DC:B6:93:33:0E:A8:09:6F:53:A3:72

sha1 と md5 の両方の値を使って確認することをお勧めする。