第 VII 部

公開鍵証明書を用いた
利用者認証技術

第 7 部
公開鍵証明書を用いた利用者認証技術

第 1 章　moCA WG 2009 年度の活動

moCA WG 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 WG である。利用環境や利用法に関する情報交換も行われている。moCA WG で運用されている認証局を以下に示す。

- WIDE ROOT CA
  WIDE プロジェクトにおけるトラストアンカーを提供する目的で設置されたルート CA である。次の moCA の他に SOI WG 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 もこの CA の下位 CA である。WIDE ROOT CA のフィンガープリント[1]を「付録　フィンガープリントの一覧」に載せる。
- moCA (members oriented CA)
  WIDE メンバの電子証明書である「WIDE メンバ証明書」を発行する他、WIDE プロジェクト内で使われるサーバ証明書の「WIDE サーバ証明書」の発行を行う。

2009 年は、継続して CA の運用を行ったほか、WIDE メンバ証明書の有効期限の変更や moCA の Web ページのデザイン変更準備作業などが行われた。

第 2 章　証明書の更新

例年と同様に 2009 年も 6 月に WIDE メンバ証明書と WIDE サーバ証明書の更新を行った。

WIDE メンバ証明書の更新は、既存のユーザに対して新たに鍵ペアを生成し、有効期限を新しくした証明書を配布する形で行われた。WIDE サーバ証明書は、基本的に既存のサーバ証明書の鍵ペアを生成せず、有効期限を伸ばした証明書を発行する形で行われた。

(1) WIDE メンバ証明書について

例年は、WIDE メンバ証明書は有効期間を 1 年間として、WIDE メンバ全員に電子メールで一斉送付する方法をとってきた。しかし、毎年 WIDE メンバ証明書を Web ブラウザに設定するのは、WIDE メンバの負担が大きいという意見をきっかけとして、WIDE メンバ証明書の有効期間を 2 年間とした。

今まで有効期間を 1 年間としてきた背景としては、毎年、学生メンバが卒業を機に WIDE の活動を一旦完了とするケースが相当数あることを考慮して、有効期間を短くして有効期間内の失効の手間を軽くする狙いがあった。このような背景のもと、WIDE メンバ証明書の有効期間を 2 年間とした場合の懸念事項としては、有効期間内に証明書を紛失する頻度が高まり、証明書の失効リスト（CRL）のサイズが大きくなることが挙げられた。BoF やワーキンググループで議論をした結果、今回は WIDE メンバ証明書を利用する WIDE メンバの負担を減らす方向で有効期間を 2 年間とし、CRL のサイズがどの程度大きくなるか、実際に試した結果によって再検討することとした。もともと、学生メンバの卒業によるメンバシップ失効については、あくまで学生メンバの意思によって発生するものであり、卒業と同時にメンバシップを失効する運用とはしていない。したがって、WIDE メンバ証明書の失効手続きの負担が大きく増すわけではないと予想している。

2009 年 6 月の WIDE メンバ証明書一斉配付時の発行数は、841 である。2009 年 6 月以降の WIDE メンバ証明書の失効数は 6 である（2009 年 12 月 7 日現在）。次回の WIDE メンバ証明書の一斉配付は、2011 年 6 月となる。それまでの間は、WIDE メンバの失効と WIDE メンバ証明書の失効との関係の考察に重点を置く。

1　補足：フィンガープリント
WIDE ROOT CA を基点とする CA のツリー構造の中で発行されている「WIDE メンバ証明書」などを利用するためには、Web ブラウザなどを使ってフィンガープリントの値を確認し、WIDE ROOT CA の正しい電子証明書データを入手する必要がある。

(2) WIDE サーバ証明書について

WIDE サーバ証明書は、WIDE メンバであれば発行を申し込むことができる SSL/TLS サーバのサーバ証明書である。WIDE サーバ証明書は主に WIDE メンバがアクセスする WG のサーバ等で使われている。

WIDE サーバ証明書は、新規発行は随時受け付けられており、更新は毎年 6 月に行われている。ここで言う更新とは鍵ペアの変更を行わずに有効期限を更新した証明書を発行することで、WIDE サーバ証明書の利用者（“WIDE サーバ証明書の管理者” と呼ばれる）が各自更新用の Web ページにアクセスして行う。

2009 年 7 月以降の WIDE サーバ証明書の発行状況を以下に示す。

○ サーバ証明書発行数 24
　※ 同一サーバに対して発行された複数の証明書を含む
○ ホスト数 22
　※ 同一サーバは 1 と数える
○ 6 月以前から利用を継続しているサーバの数 21

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、一定のレベルの登録業務が行われるようにした。

(3) moCA Web ページのデザイン変更について

WIDE では証明書を使った環境に関する情報交換が適宜行われている。その情報交換の活性化や古いドキュメントの整理を目的として、moCA の Web ページの変更作業が進められた。

ドラフト作成作業は完了したが、英語版のページを提供するかどうかなどの詳細な作業が残っており 2009 年 12 月 11 日時点で公開には至っていない。今後作業を進め Web ページ更新を図りたい。なお、2009 年 WIDE 春合宿に行われた “cool webside design ワークショップ” が活用されたことを述べておく。

第 3 章　まとめ

WIDE サーバ証明書は、WIDE メンバ専用ページの他に WIDE wiki や two サーバ、CSAW（Collaboration Support Architecture for WIDE-community）、WIDE 合宿の参加登録や、WIDE 合宿における無線 LAN 等、他 WG の活動において利用されている。

2008 年に引き続き、moCA WG メンバを中心として、WIDE における電子証明書の利用環境に関する動作検証や情報交換が行われた。これは電子証明書の利用者に対するサポートに生かされた。

付録　フィンガープリントの一覧

概要

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

フィンガープリント

2009 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 ROOT CA 02

sha1 フィンガープリント

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

md5 フィンガープリント

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。

以上