# 第 VIII 部

# 公開鍵証明書を用いた<br>利用者認証技術

# 第 8 部
# 公開鍵証明書を用いた利用者認証技術

## 第 1 章　moCA WG 2010 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 はこの CA の下位 CA である。
- 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。

2010 年は、継続して CA の運用を行い WIDE メンバへの鍵対の提供を行ったほか、WIDE メンバ証明書を UNIX コマンドを使って失効するコマンドの作成や Web ページのデザイン変更などを行った。

## 第 2 章　WIDE メンバへの鍵対の提供

2009 年に moCA が発行する WIDE メンバ証明書の有効期限を変更したため、2010 年は WIDE メンバ証明書の更新作業を行わなかった。

### (1) WIDE メンバ証明書について

2008 年まで、WIDE メンバ証明書の有効期間は 1 年間であり、毎年 WIDE メンバ全員に WIDE メンバ証明書を一斉送付してきた。しかし、Web ブラウザ等の WIDE メンバ証明書をインストールするソフトウェアの設定変更を、毎年行うことは WIDE メンバの負担が大きいという意見をきっかけとして、2009 年 6 月、WIDE メンバ証明書の有効期間を 2 年間とした。

2009 年 6 月の WIDE メンバ証明書一斉配付時の発行数は、841 であった。このうち失効されているものは 19 である（2010 年 12 月現在）。次回の WIDE メンバ証明書の一斉配付は、2011 年 6 月である。

今のところ CRL（Certificate Revocation List―失効された証明書の一覧データ）のサイズは 1 K バイト程度であり、特に不具合は報告されていない。

### (2) WIDE サーバ証明書について

WIDE サーバ証明書は、WIDE メンバが発行を申し込むことができる SSL/TLS 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ことを目的とした WIDE 合宿や WG のサーバで使われている。

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。更新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が有効なサーバ証明書を得られるようになっている。

WIDE サーバ証明書の発行状況を以下に示す。数量は 2009 年 6 月以降に発行されたもので有効なものを数えている。

○ サーバ証明書発行数 31
　※ 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 25
　※ 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 23

## 第 3 章　失効コマンドの作成

認証局ソフトウェアの見直し活動の一環として、WIDE メンバ DB との連携を図るため、UNIX コマ

ンドとして動作する失効プログラムを作成した。これまでは、WIDE メンバ証明書の失効を行うために Web インターフェースを使う必要があった。今後は、WIDE メンバの追加や削除の際に WIDE メンバ証明書を自動的に発行するだけでなく、失効を行うことができる。

## 第 4 章　Web ページのデザイン変更

PKI や moCA に関する情報集約やドキュメント整備の一環として、moCA WG の Web ページのデザイン変更とトップページの英語訳作成を行った。Web ページのデザインは、2009 年に用意されていたものを使用した。この他に、moCA が発行している電子証明書の種類や用途を説明する文書作成などを行った。

## 第 5 章　moCA によって発行された証明書の有効期限の監視

2010 年は、WIDE サーバ証明書の更新を例年のように 6 月に更新作業をできなかった。これは WIDE メンバ証明書の更新作業と同時作業として行っていた WIDE サーバ証明書の更新作業の必要性に気づかなかったためである。そこで、moCA のオペレーターが WIDE サーバ証明書の有効期限が近づいたことに気づくため、two WG の監視サーバを利用した WIDE サーバ証明書の有効期限の監視を開始した。

## 第 6 章　まとめ

2010 年は、moCA を実験から運用に適した形にするための作業が行われた。moCA WG の趣意書ではこれまでに述べた活動の他に、暗号アルゴリズム移行や認証局ソフトウェアの改良が予定されていたが、実施には至らなかった。残った課題は中期的な課題であるが、WIDE において電子証明書が普及している状況を鑑みると今後も継続して活動することが重要である。

## 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

2010 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