第 IX 部

公開鍵証明書を用いた
利用者認証技術

第 9 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 2007 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 ROOT 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。2007 年度は、毎年恒例となっている WIDE メンバ証明書/サーバ証明書の更新を実行し、維持管理を中心に行った。また、ワーキンググループが発足して 10 年が経過したこともあり、これまでに培った CA 運用ノウハウを文書化することについて検討を行い、目次作成までをほぼ完了した。さらに、TWO ワーキンググループでは無線 LAN 利用に関して、CSAW ワーキンググループでは WIDE 内 SNS 利用に関して、WIDE メンバ証明書が認証手段として用いられた。ワーキンググループ発足当初から目指してきた WIDE プロジェクトの認証基盤としての役割をようやく果たせるようになってきた。

下記に、おもな活動について報告する。

- （毎年行われる）証明書の更新
- （2007 年度 3 月合宿にて TWO ワーキンググループと合同で試行した）無線 LAN 接続時の証明書利用

第 2 章　証明書の更新

2.1 更新作業について

2007 年 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。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。

また、サーバ証明書の更新にあたっては、サーバ証明書の申請者が WIDE メンバ証明書を利用してサーバ証明書を更新できる Web インターフェイスを提供する方法をとった。

更新作業にあたっては、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

今回は、従来の方法を維持したため CA プログラムや設定ファイルの変更が最小限となり、更新準備は 2 週間程度と最短であった。

WIDE メンバ証明書の発行数は 816、サーバ証明書の発行数は 28 であった。

2.2 更新時に起きた不具合等について

ここ数年、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、電子メールをプログラムから自動送付するためのメールサーバを送信専用で運用しているためか、受信側でスパムメールと判定されるケースが以前より増えている。一斉配付を実施した後、電子メールが届いていないといった問い合わせがあり、今回は、11 通の再発行を行った。WIDE メンバ証明書の配付方法は確立したとみなしていたが、スパムメールと判定されるケースがさらに増えれば、配付方法を変更する検討が必要になる。

また、Mac OS X の Safari ブラウザへの WIDE メンバ証明書インストールについて、昨年度の CA 鍵対変更時にノウハウを蓄積したつもりでいたが、予想に反して不安定な状況となった。Mac OS X の各ユーザの環境の違いによるためか、同じインストール方法に沿っても、成功する場合と成功しない場合とがあり、解決できなかった。Mac OS X ユーザからの報告によると、Safari ブラウザで利用できる個人証明書は、最初に登録した 1 通のみとのことである。つまり、昨年度の WIDE メンバ証明書が登録されている状態で今年度の WIDE メンバ証明書を追加登録しても有効にならないため、昨年度の WIDE メンバ証明書を削除しなければならないということになる。

第 3 章　無線 LAN 接続時の証明書利用

2007 年 3 月の WIDE 合宿にて、無線 LAN における認証に WIDE メンバ証明書を利用する実験が行われた。この実験は 2006 年 9 月に行われた実験に引き続く二回目のものである。

WIDE 合宿の参加者は多種の OS や、無線 LAN の、サプリカントと呼ばれるクライアントソフトウェアが利用されている。認証方式として WPA-EAP を利用し、EAP-TLS のクライアント認証で、WIDE メンバ証明書を使うことが実用に耐えうるのかどうかの検証が行われた。

- 利用された無線 LAN の認証方式：
  - WPA-Enterprise (802.1x)
- 利用できることが確認された OS：
  - Windows XP
  - MacOS 10.3, 10.4
  - FreeBSD
  - NetBSD
  - Linux
- 利用状況：(回答者：150 人)
  - 利用した：45 人
  - 利用しようとしたが、できなかった：27 人
  - 利用しなかった：63 人
  - 無回答：15 人

WIDE 合宿の一環として行われたアンケート結果、「利用しようとしたが、できなかった」ことの理由は、以下のものがあった。

- 認証を試みていますのメッセージの先に進まず、接続できなかった。
- ESSID がアナウンスされていなかったため、OS 標準のサプリカントでは手動設定しても、基地局が見つからず接続できなかった。

ただし、一度 logout する必要があった、Windows XP ではバージョンが古いドライバの中には WPA2 をサポートしておらず、アップデートが必要である (Windows Update とは異なる)、などのノウハウも寄せられた。他には、思ったより簡単に動いた、WEP をやめてもよい、といった意見も寄せられた。

この実験により、一部の OS やハードウェアで利用できないことがあるものの、OS 標準の機能を利用してクライアント証明書を使った無線 LAN における認証が利用できることが確認できた。

第 4 章　まとめ

2008 年度は CA 運用ノウハウをドキュメントにまとめる活動を中心に行っていくほか、RSA に代わる新しい署名アルゴリズム ECDSA の利用に挑戦し、各種ブラウザの対応状況の調査を実施したい。

付録　フィンガープリントの一覧

1 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

2 フィンガープリント

2008 年 1 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。