≪ 巻末の付録USBメモリに詳細版を収録 ≫

第15部

公開鍵証明書を用いた利用者認証技術（概要版）

木村 泰司

第１章　moCA WG2013年の活動

moCA WGはCA(Certificate Authority)の振る舞いや証明書の扱いに注目し、WIDEプロジェクトでCAの運用実験を行っているWGである。

2013年は、WIDE Root CAやmoCAといった認証局証明書とユーザやサーバの電子証明書にハッシュアルゴリズムSHA-2を導入するため、WIDE Root CAの鍵生成を行う“キーセレモニー”を実施した。また2年おきに行っているWIDEメンバ証明書とWIDEサーバ証明書の一斉発行を、SHA-2を使った新しい認証局を使って行った。

第２章　WIDE Root CAのキーセレモニー

キーセレモニーとは、暗号技術を用いた認証局等の運用を始めるために、適切な手順を踏んで鍵の生成を行う手続きである。moCA WGでは、WIDE研究会で使われている電子証明書にハッシュアルゴリズムであるSHA-2を導入するため、このアルゴリズムを使う新たな認証局WIDE Root CA 03を立ち上げた。新たな認証局の立ち上げには公開鍵暗号の鍵ペアの生成が必要となる。そのためのキーセレモニーを、2013年5月のWIDE研究会(東京大学 柏キャンパスにて開催)で行った。

第３章　WIDEにおける証明書発行の概況

WIDE研究会では4種類のクライアント証明書が発行されている。WIDEメンバに発行されるWIDEメンバ証明書、WIDEメンバの秘書さんに発行される秘書さん証明書、一時的にWIDE合宿に参加するゲスト向けのテンポラリ証明書、WIDE合宿の事務局業務を行うためのWIDE事務局証明書である。12月31日現在、WIDEメンバ984名全員にWIDEメンバ証明書が発行されている。一斉発行が行われた6月25日以降の再発行の数は25である。

SSL/TLSのWebサーバで使われているWIDEサーバ証明書は2013年12月31日現在、35発行されている。認証局証明書は、ルート認証局であるWIDEルート認証局によって2つの下位認証局証明書が発行されている。

第４章　WIDE Root CA 03フィンガープリント

sha1フィンガープリント

42:75:7B:24:E3:BB:DB:AB:9E:D7:FE:32:D1:27:18:58:EE:3E:81:66

md5フィンガープリント

D2:6E:5A:CE:96:E3:DC:FE:63:D8:B2:01:55:BD:40:D2