≪ 巻末の付録USBメモリに資料を収録 ≫

第16部

公開鍵証明書を用いた利用者認証技術

木村泰司

第１章　moCA WG2012年の活動

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。

2012年は、WIDE Root CAやmoCAの認証局証明書およびユーザやサーバの電子証明書におけるハッシュアルゴリズムSHA-2の導入に向けて、Webブラウザやサーバにおける新たな電子証明書の利用実験を行った。また、例年通りCAの運用を継続しWIDEメンバへの鍵対の提供を行った。

第２章　SHA-2の導入テスト

商用認証局等において進められている電子証明書でのSHA-2の利用は、Webサーバや無線LAN基地局における電子証明書を用いたサーバ認証やクライアント認証に影響する。SHA-2の導入にはWIDEプロジェクトにおける新たな認証局証明書の発行と、すべてのサーバ証明書・クライアント証明書の再発行が必要になる。ユーザによる証明書の利用を考えると、入れ替えは一度にとどめ、似た名前の異なる認証局証明書を配布しなおさないことが望ましい。

moCA WGでは、2012年3月、2012年9月の二回のWIDE合宿の前後に、新たな複数のハッシュアルゴリズムおよび鍵長を組み合わせた電子証明書の実験的な利用を行い、利用できる環境を確認した。その結果、複数のWebブラウザおよびWebサーバでSHA-2の電子証明書を利用できる状態であり、またスマートフォンの一部でも問題ないことが確認された。2013年に予定されている証明書の一斉発行のタイミングでSHA-2の電子証明書に移行していくことが考えられる。

第３章　WIDEメンバ証明書/WIDEサーバ証明書の概況

WIDEメンバ証明書は2011年に一斉配布されており、有効期限は2年間である。そのため2012年は、一斉配布は行わず、新規のWIDEメンバに対する発行とユーザからの依頼に基づく再発行のみが行われた。

2012年12月15日現在、moCAに発行されている有効なクライアント証明書は、WIDEメンバ証明書・秘書さん証明書を含めて合計1,062で、このうちの再発行の数は85である。（WIDEメンバ証明書は、ユーザの確認が取れない限り失効を行わないため、一人のユーザに対して複数の有効な証明書が存在する。発行対象のユニーク数とWIDEメンバの数とは一致しない）

WIDEサーバ証明書は、WIDEメンバ証明書と同様のサイクルで発行されており、2012年は一斉配布は行われなかった。WIDEメンバ証明書とは異なりユーザからの依頼に基づく再発行は1件のみであった。2012年12月15日現在の有効なWIDEサーバ証明書は36である。

第４章　WIDE Root CA 02フィンガープリント

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