第14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 WG2014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プロジェクトでCAの運用実験を行っているWGである。

2014年は、2013年6月に導入したSHA-2を使ったWIDEメンバ証明書やWIDEサーバ証明書を継続的に提供した。2013年6月にWIDEメンバ証明書の一斉発行を行っており、有効期限は2年間であるため2014年に一斉発行は行っていない。

本報告書の執筆現在、WIDE moCAによって発行されている有効なクライアント証明書は1,098であり、サーバ証明書は55である。WIDEメンバ証明書はWIDE研究会やWIDE合宿の申し込みなどのユーザ認証やS/MIMEを使った電子メールで使われており、WIDEサーバ証明書はSSL/TLSを使うWebサーバのほか、テレビ会議システムなどで使われている。

第２章　電子証明書とSHA-2

2014年の後半、Chrome、FirefoxといったWebブラウザで、SHA-1やMD5といった古いハッシュアルゴリズムが使われた電子証明書について、ユーザに警告を表示し、将来的に利用を停止する計画が発表され、修正が行われている[16,17]。なおWindows OSについては2013年11月の段階で方針が公表されていた[18]。また、EV SSL等の商用認証局の認証業務について基準を設けているCA/Browserフォーラムでは、いわゆるパブリック認証局が準拠すべき要件"Baseline Requirements"において、署名のためにSHA-1を使った電子証明書の利用を停止するスケジュールが示されている[19]。

電子証明書におけるSHA-2利用は、WebブラウザやOpenSSLなどの電子証明書を扱うプログラムがSHA-2に対応しているかどうかといった実装上の課題と共に、既に発行されていてまだ有効期限の範囲にあるSHA-1などの電子証明書からどのように移行していくかという運用課題でもある。moCA WGでは電子証明書を並行運用することによって起こる課題に直面することを極力避けるため、2013年に一斉に切り替える方策を取った。2014年末現在、WIDE moCA WGで扱われているすべての電子証明書ではSHA-2が使われており、Webブラウザの修正に対して必要な作業や不具合が発生することはないと考えている。

今後、SHA-2への移行と同様に、楕円曲線を使った電子証明書の導入のような実装上の課題が出てくることが予測される。moCA WGとしても適時調査を行いたい。

第３章　WIDEにおける証明書発行の概況

WIDEメンバ証明書は2013年に一斉発行されており、有効期限は2年間である。そのため2014年は、一斉発行は行われなわれず、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が行われた。

執筆現在、電子証明書が発行されるWIDEメンバ総数は923名で、moCAに発行された有効なクライアント証明書は、WIDEメンバ証明書・WIDE秘書さん証明書・WIDEテンポラリ証明書を含めて合計1,098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、2014年は一斉配布は行われなかった。2015年1月6日現在の有効なWIDEサーバ証明書は55である。

第４章　WIDE Root CA 03フィンガープリント

WIDEプロジェクトにおける電子証明書のトラストアンカーを提供するために運用されている認証局の証明書「WIDE Root CA 03」のフィンガープリントを以下に示す。

SHA-256フィンガープリント

3B:CB:EC:C3:6C:96:ED:D5:A2:98:81:19:C4:C6:F0:4B:DE:AB:43:63:48:D3:7B:05:F9:36:5F:1C:AF:B4:0F:8C

SHA-1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