第12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 WG 2011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。

2011年は、東日本大震災の影響で起きた障害を受けてmoCAの認証局ソフトをOpenSSLベースに移行した。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　OpenSSLへの移行とサーバの仮想化

2011年、moCAでは、認証局のソフトウェアをICAT Certification Authority Package（ICAP）からOpenSSLを使うスクリプトに変更した。更にWIDEクラウドを用いた仮想サーバに移行することで、継続運用しやすい形となった。

東日本大震災の影響でmoCAが設置されたNOCで停電が起き、従来の動作環境が、継続的な運用に対して大きな課題となった。ICAPの動作環境が限られていたため、ハードウェア障害が発生した際に復旧しにくかったのである。two WGメンバの尽力によって従来の動作環境に戻ったが、認証局ソフトウェアを切り替え、更に仮想サーバに移行することで、障害から復旧しやすくなった。

第３章　WIDEメンバ証明書

2011年の一斉配布は6月22日に行われた。このとき、889通発行された。前回の2009年6月は841通発行されており、48通増加した。次回の一斉配布は2013年6月を予定している。

第４章　WIDEサーバ証明書

WIDEサーバ証明書の更新は6月27日に行われた。このとき、23通（23サーバ）発行された。前回の更新が行われた2010年6月には23通発行されており、横ばいである。

WIDEサーバ証明書の発行後、設定ファイルを戻していなかったために、WIDEメンバ証明書がWIDEサーバ証明書の証明書プロファイルで発行されるミスが発生した。その後、個別にWIDEメンバ証明書が発行され、設定ファイルを別にするなどの再発防止策が取られた。

第５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