第11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 2019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。

moCA WGで運用されているCAであるmoCAでは、WIDEメンバのためのWIDEメンバ証明書と主にTLSのサーバのためのWIDEサーバ証明書が1年おきに一斉に発行されている。2019年も6月にWIDEメンバ証明書の一斉発行が行われた。

2019年は、昨年に続いてIPアドレス認証局ついて議論が行われた。次の節でmoCAにおける証明書発行の概況を報告したのち、これらの議論について報告する。

第２章　moCAによる証明書発行の概況

WIDEメンバ証明書とWIDEサーバ証明書は1年おきに一斉に発行されている。執筆現在、WIDEメンバ総数は890名で、発行されたWIDEメンバ証明書は907、再発行数は14である（*2）。WIDEサーバ証明書は24のドメイン名に対して発行されている。

第３章　WIDE研究会におけるPKIに関わる議論

○IPアドレス認証局

IPアドレス認証局は、IPアドレスが記載された電子証明書を発行する認証局で、IPを使った通信における通信路の安全性や通信データの安全性を確保するための仕組みである。JPNICでは、公益的な観点でオープンソースのプロジェクトとして検討している。

2019年5月の研究会で下記のような議論が行われた。

（IPアドレス認証局に関する議論）
- IoTのユースケースで「あの電球をつける」といったときにどうするのか
- IPアドレス証明書はオレオレ証明書とはどう違うのか
- 違うデバイスが勝手にIPアドレスを使い始めるとどうなるのか

JPNICでは専門家チームではユースケース（利用場面）を想定した仕組み作りに向けた議論を行っている。デバイス認証とIPアドレス認証の関係を明確にしていく必要がある。

＊1　moCA WGで運用されているCAであるmoCAは、4種類のクライアント証明書を発行している。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合宿等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。サーバ証明書はWIDEサーバ証明書の1種類のみである。
moCAによって発行された証明書は、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サーバなどで使われている。WIDEプロジェクトで使われているサーバの中にはLet's Encrypt を利用しているものがあり、WIDEメンバの間ではWIDEサーバ証明書と使い分けがなされている。

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