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 2020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。前回は2019年6月に行われ[*1]、今年は一斉発行は行われなかった。

2020年は、これまでmoCA WGで行われていた、PKIのトラストアンカーに関する議論が他の議論のテーマに位置づけられ、IDAST（Identity, AuthN / AuthZ, Security, Trust）と呼ばれるようになった。この名前をつけたWGの設立を視野に入れた議論が行われた。moCA WGのco-chairである木村は、PKIにおけるトラストアンカーについての研究活動と、PKI技術をBGPのセキュリティに役立てることのできるRPKI（リソースPKI）の開発と普及に取り組んでいる。

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。2021年1月14日現在、WIDEメンバ総数は885名で、発行されたWIDEメンバ証明書の数は、再発行等の理由で一人に対して複数発行されたものを含めて932である[*2]。

第３章　WIDE研究会におけるPKIに関わる議論

2019年までにmoCA WGで報告されてきたように、Webにおいて利用されるPKI（WebPKIと呼ぶ）は、CAにおけるインシデントの発生やWebブラウザにおける実装の変化によって、Webにおけるリスクや安全性をエンドユーザに示す技術としての位置づけが変化しつつある。

2020年6月の研究会では、moCA WGとは別にIDAST WG（仮称）を設立することを視野に、WebPKIにおけるトラスト構造の変化を一つのテーマに含めて議論された。

論点を簡単に紹介する。

- **Identityとidentifierのアーキテクチャ**
  ID基盤として利用できる技術にOpenID ConnectやPKIがある。運用を含めた課題には、Identityの失効処理をいかに適切に行うか、IdPの振るまいをいかに可視化するか、認可を認証といかに整理して実現するか、といったものがある。

＊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。

＊2　WIDEサーバ証明書は25のドメイン名に対して発行されている。

- **トラストアンカー**
  Webブラウザに見られるように、プリインストールされたトラストアンカーは、その中の一部にインシデントが起きるだけで、すべてのユーザに影響してしまうような構造になっている。プリインストールという位置づけの在り方を含めた議論である。

今後、トラストに関する議論は、moCA WGではなくIDASTを扱うグループで行われる可能性がある。

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