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 WG 2021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。2021年は6月に一斉発行が行われた。[*1]

2021年 は、2020年 のIDAST（Identity, AuthN / AuthZ, Security, Trust）と呼ばれるグループ（WGにはなっていない。）でのWebPKIを始めとするトラストに関する議論は落ち着き、情報交換に留まらない議論を求める声はあるものの、新たな議論は行われなかった。moCA WGのco-chairである木村は、引き続き、WebPKIにおけるトラストアンカー関する研究活動と、PKI技術をBGPのセキュリティに適用したRPKI（リソースPKI）の開発と普及に携わっている。

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。2022年1月18日現在、WIDEメンバ総数は894名で、発行されたWIDEメンバ証明書は899。WIDEメンバに対する再発行はまだ行われていない。WIDEサーバ証明書は21のドメイン名に対して発行されている。

第３章　PKIの議論に関わる概況

2020年はHTTPSをフィッシングサイトが増加し、銀行やECサイト、クラウドサービス事業者をかたったフィッシングメールが増加した年であった。昨今のフィッシングサイトはHTTPSでアクセスでき、鍵マークが表示される。ChromeやFirefoxといったWebブラウザでは鍵マークの表示が2018年頃から徐々に簡略化され、サーバのドメイン名が確認された証明書（Domain Validation - DV）とドメイン名の割当先組織の実在性が確認されている証明書（Extende Validation - EV）の違いが分かりにくくなり、WebのPKIという仕組みとして、ユーザのオンラインでのアクセスにおいて「セキュア」かどうかの判断材料になる状況ではなくなりつつある。

PKIのようなグローバルなインターネットにおける通信相手の認証や改ざん検知に関する暗号技術を使った基盤技術への理解は、WIDE研究会やWIDE合宿での議論において、共通認識が得られている状態である。しかし新たな提案が少ない状況や、集合体となる認証局の現実社会での運用上の課題に取り組む議論を行うには、糸口が見出しにくい状況と言える。

＊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