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 2022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プロジェクトにおける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の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年おきに一斉発行されている[*1]。前回の発行は2021年6月であり、2023年はメンバーの追加やユーザの申告に基づく証明書発行の他に一斉発行は行われなかった。

moCAはmoCA WGメンバーによって継続的にメンテナンスされている。moCAで使用しているOpenSSL（バージョン3）がPKCS#12形式のファイルを生成する際に、証明書と私有鍵の暗号化のためにデフォルトでAES256-CBC（CBCモードのAES256）を使用するようになった。そのため、macOSではインポートできないという事象があった。トリプルDES（-descert-legacyオプション）を使用することでこの問題は回避された。

PKIに関する議論としては、moCA WG会合ではないものの、PKIのトラストモデルの改善を目指したポスター発表[*2]が2022年9月のWIDE合宿で行われ、moCAWGメンバーを含めて議論された。

第２章　moCAによる証明書発行の概況

2022年1月15日現在、WIDEメンバ総数は952名で、同数のWIDEメンバ証明書が発行されているほか、利用環境の変更等、メンバからの申告で再発行されたものが21あった。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

ここ2,3年、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サイトやフィッシング詐欺の報告件数が多い状況が続いている[*3]。フィッシングサイトの多くはHTTPSを使っていて、2018年頃からChromeやFirefox、スマートフォンのWebブラウザにおいてHTTPSのマークが簡略化されたこともあって、ユーザのオンラインでのアクセスにおいてPKIを使ったそのマークは、「セキュア」かどうかの判断材料にならなくなってきている。

前述のトラストモデル改善に向けた研究は、この状勢を受けたもので、PKIにおけるRP（Webブラウザなどのサーバ認証を行う役割/プログラム）にユーザが主体となって条件を設けるアプローチを取っている。

＊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。

＊2　Work in progress: Adding confirming requirements on PKI Relying Party, Taiji Kimura, Keio university / JPNIC

＊3　フィッシング対策協議会 | 報告書類 | 月次報告書 より https://www.antiphishing.jp/report/monthly/

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