第16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 2024年の活動

moCA WGはCA（Certificate 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TLSのサーバ等のための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2023年6月であり、2024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。

2024年はmoCA WGの会合は開催されなかった。

第２章　moCAによる証明書発行の概況

2025年1月12日現在、WIDEメンバ総数は1,031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9あった。従来WIDEメンバの管理するサーバについて発行されてきたWIDEサーバ証明書は現在発行されていない。

第３章　PKIに関わる動向

2023年から2024年3月にかけて総務省の事業でRPKI（リソースPKI）に関する実証実験[*2]が行われた。RPKIはIPアドレス等のアドレス資源（リソース）の分配をPKIの電子証明書を用いて証明し、BGPの経路情報の正しさを確認する等に応用される認証基盤である。2024年11月にはJPNICからRPKIガイドラインが公開された[*3]。

IPアドレス等の分配を行うレジストリから発行される"リソース証明書"を使って署名検証のできるROA（Route Origination Authrozation）は、徐々に発行数を増加させており、国内のIPアドレスに対するBGP経路のカバー率は2022年頃に50%程であったものが2024年には70%を超えた。国内の大手IX事業者にいくつかではROAの検証結果をBGPルータに伝える役割を持つ"RPKIキャッシュサーバ"の提供等、RPKIに関わる活動が行われている[*4] [*5]。

WIDE合宿およびWIDEメンバーが構築に関わるイベント等のネットワークにおいてROAを使ったBGP経路の検証が行われつつある。今後はROAを使ったオリジンASを確認する技術に加えて、ASPA（Autonomous System Provider Authorization）を使ったASパスの検証についても導入に向けた動きがあると予想される。

＊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　ISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査、総務省

＊3　RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン - JPNIC、https://www.nic.ad.jp/ja/rpki/guideline/

＊4　MF RPKIプロジェクト、https://www.mfeed.ad.jp/rpki/whatisrpki.html

＊5　BBIX RPKI活動、https://www.bbix.net/rpki/

現在のmoCA WGはWIDEメンバーのユーザ認証に使われる電子証明書の発行を担っているが、かつては権限の証明や属性の証明等、多様なPKIの利用技術について議論されていた。PKIの応用は、細分化もしくはスマートフォンにおけるアプリ等の利用場面の変化に合わせた詳細化が起きており、IoTデバイスにおけるコードやデバイス認証（IETFにおけるSUIT・TEEP・RATSの関連する仕組み）、他のユーザ認証等、今後もこの流れは起きていくと考えられる。

第４章　WIDE Root CA 04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 04」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
0E:DF:6A:78:2D:27:57:8B:0F:97:BC:EE:C9:19:5B:71:
CC:66:96:76:51:66:4A:29:FB:CF:5C:B1:7E:28:38:27

SHA-1フィンガープリント
99:0E:EE:06:0A:0B:B2:89:81:6E:6C:94:C1:6E:B9:10:F
A:11:8E:AC