第13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 2016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。

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。前回は2015年6月に行われたために2016年には行われなかった。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無料のサーバ証明書を利用できるLet's Encryptが利用されているものがあり、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２章　moCAによる証明書発行の概況

執筆現在、電子証明書が発行されるWIDEメンバ総数は932名で、moCAに発行された有効なWIDEメンバ証明書は952である。(WIDEメンバ証明書は、一人のユーザに対して複数の有効な証明書が存在する。発行対象のユニーク数とWIDEメンバの数とは一致しない)

2017年1月5日現在の有効なWIDEサーバ証明書は52である。

第３章　電子証明書にかかわる動向 - CT Log

Certificate Transparency(CT) Logは、Google社によって提案された仕組みで[19, 20]、認証局による証明書発行や失効を公開されたLogサーバに記録する事でその透明性を高めることを目的としたものである。サーバ証明書の過去の更新などの処理の結果を確認できる他、ある証明書が不適切に発行されたサーバ証明書かどうかを確認するためにも使われている。IETF TRANS WGで標準化活動が行われており、CTはRFC6962になっている。CTは、Let's Encryptを通じて発行されたサーバ証明書でも使われておりWIDEプロジェクトでも使われていることになる。証明書チェーンや仕様についてはLet's EncryptのChain of Trust[21]が詳しい。

CT LogはWebページを通じて閲覧することができる[4]ため、証明書の発行や更新の手順を調べるためにも使われ始めている。外部に公開されていないサーバのホスト名が露呈してしまう問題が指摘されており、IETF TRANS WGでは対策が検討されている。

Webブラウザにおいては、逐次CT Logをチェックしてユーザへの表示を変える動きがある。これは同一のドメイン名を持つWebサーバの証明書が他の未知の認証局によって発行されているような場合、いわば不正な証明書を発見するのに役立つ一方で、証明書を発行する認証局や証明書を使うサーバ管理者には、業務の手続きやCT Logサーバ等の監視対象が増えるなど、運用負荷が高まる可能性が

ある。

WIDEプロジェクトにおけるサーバは、利用者が限定されたものであると言えるため、不正証明書が発行されるリスクは高まっていないと考えられるが、今後、Webブラウザの実装状況やユーザへの警告の必要性などを踏まえて、CT Logにまつわる動向を見ておくことが重要であると考えられる。

第４章　リソースPKI（RPKI）

国内のIPアドレスに関してJPNICが試験提供を行っているRPKIは、利用者が微増傾向を続けている[5]。WIDEプロジェクトに割り当てられたIPアドレスにもリソース証明書が発行されており、経路広告元のASを示すデータであるROAが作成されていることから、異なるASによる誤った経路広告を検知し、BGPルータでその経路情報の扱いを決められる状況である。

RPKIの仕様策定を行っているIETF SIDR WGではROAを使ったOrigin Validation（経路広告元の確認）の他にAS Path Validation（ASパスの確認）の仕様は既に固まってきており米国NISTのBGP-SRx[6]における対応など、実装が出始めている。

第５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