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 2015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、1年おきにWIDEメンバのクライアント証明書を発行している。SHA-2への移行のために2013年に現在の認証局証明書を作成してから2年経ち、新しいmoCAの鍵ペアを使って初めてWIDEメンバ証明書の一斉発行が行われた。WIDEメンバ証明書は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サーバのほか、テレビ会議システムなどで使われている。

第２章　ワイルドカード証明書

ワイルドカード証明書を運用するに際してどういう課題があるか、という実験とサーバにおける証明書管理の負荷軽減のため、CN=*.wide.ad.jpのサーバ証明書を商用認証局から取得した。ボードおよびTWO WGのサーバで使われている。このサーバ証明書の有効期限は2016年3月14日であり、しかも値上がりしているため継続しない方向性である。

第３章　Let's Encryptと新たな証明書検証の仕組み

WIDE研究会では、一般的なサーバ証明書管理と同様に、更新などの管理の負荷軽減が課題として位置づけられている。そこで無料でかつ管理の負荷軽減減が見込まれる仕組みであるLet's EncryptがmoCA WGでも注目された。

Let's Encryptは、Internet Security Research Group (ISRG)で取り組まれている仕組みで、発行される証明書は無料であり、またサーバ証明書の申請や更新手続きを自動的に行うプログラムをインストールするだけで、有効な証明書が維持されるようになっている。サーバ証明書の申請や更新の仕組みは、IETFのAutomated Certificate Management Environment (acme) WGで検討されている。まだ使われるプロトコルはRFCになっていないものの、IETF93でWGに採用された。

IETF の Public Notary Transparency (TRANS) WG では、認証局における不正証明書発行の事件を受けて、Certificate Transparencyと呼ばれる仕組みが検討されている。各認証局が発行前の証明書をCTログサーバと呼ばれるサーバに記録してゆき、それを使ってWebブラウザなどで疑わしい証明書を検知する用途が考えられている。Google Chromeには既に実装されており、他のWebブラウザでも使われるようになる可能性がある。

Let's Encryptでは、このCT対応の他、Domain Validation証明書やExtended Validation証明書への対応も検討されている。今後の動向が注目される。

第４章　RPKI

IPアドレスやAS番号といった番号資源を証明するPKIであるリソースPKI(RPKI)の試験提供が2015年3月にJPNICで開始された。WIDEでは、moCA WGで何度か議題に挙げられ、ポスターセッションなどでルーティングセキュ

リティへの効果などがディスカッションされた。WIDEプロジェクトでも利用を開始しており、Route Origin Authorization (ROA)オブジェクトの発行が行われている。

ROAはIPアドレスのプレフィックスに対して、その経路広告を行うAS番号を示すために作られるデータで、グローバルなインターネットで頻発しているBGPの不正な経路情報の広告を検知することができる。CiscoやJuniperといった大手ルータベンダーによる対応も行われており、今後、ROAを作成することでどの程度セキュアなルーティングに役立てることができるのか、対応ルータを使ったBGPの運用がどうなっていくのかなどの注目すべき技術課題がある。WIDEプロジェクトでも新たなPKI技術の応用の一つとして、ルーティングアーキテクチャやセキュリティについてディスカッションを行っていきたい。

リソースPKI(RPKI), JPNIC
https://www.nic.ad.jp/ja/rpki/

第５章　WIDEにおけ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957名で、moCAに発行された有効なクライアント証明書は、WIDEメンバ証明書・WIDEボードの秘書さん向けの証明書を含めて合計971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)

2015年1月6日現在の有効なWIDEサーバ証明書は52である。

第６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

MD5フィンガープリント
D2:6E:5A:CE:96:E3:DC:FE:63:D8:B2:01:55:BD:40:D2

第７章　参考資料

[1] "Let's Encrypt" https://letsencrypt.org/
[2] RPKIシステムの試験提供開始のお知らせ, 2015年３月３日, JPNIC https://www.nic.ad.jp/ja/topics/2015/20150303-01.html