ACMEサーバにおけるDV証明書発行時のDomain Validationの強化方式

須賀 祐治[1,a)]

Enhanced Domain Validation methods in issuing DV certificates by ACME servers

Yuji Suga[1,a)]

X.509 証明書は，公開鍵とその所有者の関係を保証するデータフォーマットであり，サーバもしくはクライアントの公開鍵を安全に提示するために，SSL/TLS などのセキュアプロトコルにおいて広く利用されている．公開鍵証明書は階層的に発行されており，証明書の発行者を順に辿ってトラストアンカーであるルート証明書に行き着くことで，当該証明書に格納される公開鍵を信用する PKI（ Public Key Infrastructure）の仕組みを利用する．SSL/TLS サーバに対しては商用の CA サービスで販売されており，DV 証明書はドメイン名所有者かどうかの確認のみを行い，現実世界における組織の実在性確認を行うものではなく，デジタル世界で確認処理を完結して発行される証明書である．

Let's Encrypt プロジェクト [1] は，この DV 証明書を無償で自動発行する目的で設立され，2015 年 12 月初旬には，広くサービス利用が可能になった．この自動証明書発行サービスを提供するにあたり，プロジェクト独自のプロトコルを利用せず，IETF ACME WG で策定されている ACME（Automated Certificate Management Environment）プロトコル [2] に準拠したものを利用している．

Let's Encrypt プロジェクトでは、後述する ACME プロトコルを用いた参照実装が提供されている。ACME クライアント（証明書発行依頼を行うユーザ）は Let's Encrypt client を用い、ACME サーバ（Let's Encrypt プロジェクトが運営する CA）と通信することにより、証明書の発行、再発行、失効依頼などの処理を行うことができる。その中で、ドメイン名の保有者かどうかを確認する Domain Validation と呼ばれるいくつかの方式が提供されており，ドメイン保有者であることの確認方法として、ACME サーバ（CA）からのチャレンジに対して、(1) DNS レコードを制御する方法、(2) HTTP サーバの Web ページを記載する方法、(3) SNI（Server Name Indication）を利用する方式も実装が対応している．

ACME は JSON 形式でやり取りするサーバ・クライアント間のプロトコルで，基本的には、ACME サーバは HTTPS サーバとして振る舞い、ACME メッセージは HTTPS で保護される。ACME サーバは CA 側で証明書発行を受け付けるサーバで、ACME クライアントは証明書発行依頼を行うユーザであり、Web サーバやメールサーバなど、サーバ証明書を必要とするサーバでクライアントソフトを動作させることを想定している。

HTTPS を通してクライアントからサーバに送信されるすべての ACME メッセージは JWS（JSON Web Signature）を用いてクライアントにより署名が付与される。この処理により、正しいクライアントからのメッセージであることを、サーバが検証可能となる。この仕組みを提供するためには、クライアントは証明書発行依頼などの前に、自身の公開鍵を ACME サーバに登録する作業が必要となる。具体的には JSON Web Key 形式の鍵データがメールアドレスや電話番号を格納する contact 情報と共にサーバに送付される。このとき、署名に用いられる公開鍵は、サーバ証明書で用いられる公開鍵とは異なり、登録時に使用される Account Key Pair と呼ばれる別の鍵であり，この登録時に利用された 1 つの鍵で、複数の FQDN（Fully-Qualified Domain Name）に対して証明書の発行依頼を行うことができるように設計されている。本稿は，この登録作業に着目して Domain Validation を強化する方式を提案する．

[1] 株式会社インターネットイニシアティブ
[a)] suga@iij.ad.jp

参考文献

[1] Let's Encrypt, https://letsencrypt.org/about/
[2] IETF, "Automated Certificate Management Environment（acme） - Documents", https://datatracker.ietf.org/wg/acme/documents/