DNSを用いたドメイン名の管理権限確認を使用する際の注意点

▼この文書について

インターネット上の一部のサービスではDNSの名前解決を利用して、**サービス利用者のドメイン名の管理権限**を確認します。この文書では**その仕組みと、関係者において推奨されるアクション**を解説します。

▼ユースケース

- サーバー証明書の発行（ACMEの**dns-01**、以下を参照）
- Web CDNサービスの提供
- 利用者のドメイン名によるグループウェアサービスの提供

▼確認の仕組み

DNSを用いた管理権限確認では「**チャレンジレスポンス**」の仕組みが広く使われています。

最初に、サービスプロバイダーが**1回限りのシークレットトークン**を作成し、安全な方法でサービス利用者に送ります。サービス利用者は受け取ったトークンを、**自身が管理する権威DNSサーバーに適切な方法で設定**します。

その後、サービスプロバイダーはサービス利用者が設定したデータを**DNSの名前解決**で入手し、自身が送ったトークンとの**一致を確認**します。

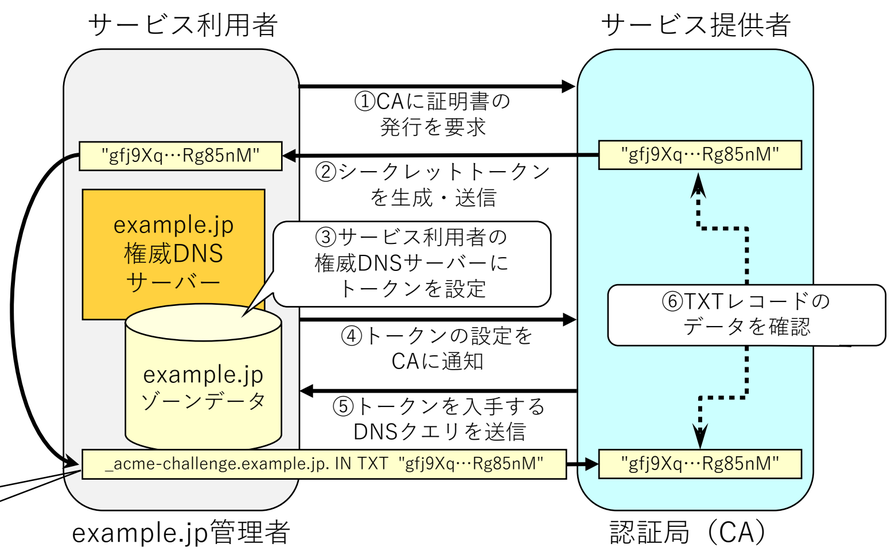

図1: ACMEのdns-01における確認の流れ

dns-01は確認の際、アンダースコアラベル「**_acme-challenge**」を使います。このラベルはIANAにより予約されています。

▼関係者において推奨されるアクション

- **プロトコル開発者**
  - プロトコル・サービス用の**アンダースコアラベルを選び、IANAに登録する**
- **サービス提供者**
  - 確認に使うフルリゾルバーで**DNSSEC検証を有効にする**
- **サービス利用者**
  - 権威DNSサーバーに**DNSSECを適用する**
- **外部DNSサービスプロバイダー**
  - 利用者に**DNSSECサービスを提供**する
  - **既存のゾーンのアンダースコアラベルのサブゾーンを、同じ権威DNSサーバー上に他の利用者が作成できないように設定されている**ことを確認する

▼関連するRFCと標準化の状況

RFC 8552及び8553（BCP222）は、アンダースコアラベルと親ドメイン名の関連付けにおけるDNSレコードタイプの使用範囲を定義し、「**Underscored and Globally Scoped DNS Node Names**」レジストリをIANAに創設しています。

draft-ietf-dnsop-domain-verification-techniquesは、サービスごとの「**_foo-challenge**」、複数の機能ごとの「**_feature1._foo-challenge**」 という形式のラベルを、**TXTレコードと共に使う形式**を推奨しています。この提案は現在、**IETF dnsop WG**で議論されています（現在WG Last Call中）。