CAA レコード設定

- CAAレコードとは
- CAA レコード設定値
- 設定確認方法

CAAレコードとは

CAAは、Certification Authority Authorizationの略になります。
認証局は、CA/Browser Forum の Baseline Requirementsにより2017年9月8日以降、 サーバ証明書発行時にサーバ証明書発行先ドメインのDNSに含まれるCAAレコード確認が必須となりました。
CAAレコードは、意図しない認証局からサーバ証明書の発行を防止するための仕組みになります。

認証局はサーバ証明書を発行する際に発行先ドメインを管理しているDNSサーバーを確認し、その認証局にサーバ証明書の発行を許可しているかどうかを確認します。
もし、CAAレコードで指定した認証局以外の発行が許可されていない場合、それ以外の認証局からサーバ証明書は発行できません。

CAAレコード設定を実施していないドメインの場合は、どの認証局からもサーバ証明書を発行できます。
なお、CAAレコードはDNSサーバに未設定でも問題ありません。意図する認証局のみからサーバ証明書を発行したい場合にのみ設定してください。

CAA レコード設定値

サーバ証明書の発行元認証局を指定したい場合はCAA レコードをDNSサーバに登録します。1つのFQDNに対して複数のCAAレコード登録も可能です。
また、ルートドメインに設定されている場合サブドメインも対象となります

（例）利用機関のドメインが「xxx.ac.jp」で、UPKI電子証明書発行サービスより発行される認証局を指定する場合

- 2020年12月25日以降の発行
  xxx.ac.jp. CAA 0 issue "secomtrust.net"

- 2020年12月24日以前の発行
  xxx.ac.jp. CAA 0 issue "certs.nii.ac.jp"

設定確認方法

CAAレコードはdigコマンドで確認できます。

（例）xxx.ac.jpのCAAレコードを確認する場合
dig caa xxx.ac.jp

結果

;; ANSWER SECTION:
xxx.ac.jp. 86400 IN CAA 0 issue "secomtrust.net"