2017 年 8 月 16 日
ジェイサート株式会社

お客様各位

DNS CAA レコード検証機能の実装につきまして

DNS Certification Authority Authorization（以下「CAA」）とは、ドメイン名の所有者・管理者が、DNS サーバを用いて、自らが所有・管理するドメイン名に対して SSL/TLS 証明書の発行を受け入れる認証局をあらかじめ特定できるようにする仕組みです。

DNS に CAA レコードを新たに追加指定することで、自らが所有・管理するドメイン名に対して、 **悪意ある第三者が「なりすまし」サイトへの利用を目的に、認証手続きの甘い認証局（あるいは中間認証局）を利用する等により、存在すべきでない証明書が発行されるリスク（2017 年の旧シマンテック社による Google 偽（ニセ）サイトへの証明書の"誤"発行が好例）を低減する**ものです。

【参考】
https://jp.godaddy.com/help/caa-ssl-27227
https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/setup-caa.html

2017 年 8 月 17 日（米国時間）以降、弊社を介して申請頂いたスターフィールド& Go Daddy 両用 SSL/TLS サーバ証明書に対しては、米国認証局が当該申請を受領時にお客様の DNS ゾーンファイル内の CAA レコードを確認し【注】、

1）CAA レコードがデフォルト値（未登録）、あるいは
2）CAA レコードとして " starfieldtech.com " あるいは " godaddy.com " と登録されている。

IN CAA 0 issue "starfieldtech.com"
IN CAA 0 issue "godaddy.com"

上記いずれかの場合に限り、証明書発行プロセスを継続します。（上記に該当しないレコード登録が確認されました場合には、ご申請をお受け出来ません。）

【注】 DNS ゾーンファイル内 CAA レコードは、
1. https://caatest.co.uk/
2. https://www.ssllabs.com/ssltest/

等外部ツールにて視認できます。

なお、CAA レコード確認プロセスの新設による、ご申請手順や、サーバへの証明書インストール手順、またはクライアント端末への影響は一切ございません。

以上