

ACME連携による証明書更新運用のご案内

2026年4月17日

株式会社ブロードバンドセキュリティ
マネジメントサービス本部

1.ACMEプロトコルとは・・・

ACMEプロトコル概要

(Automatic Certificate Management Environment)

【目的】

TLS証明書の発行・更新を自動化し、手動作業や期限切れを防止する

【前提】

証明書の認証局がACME対応をしていること

【処理の流れ】

1.ACMEクライアントがCAへ証明書を要求

2.ドメイン所有確認(チャレンジ)

・HTTP-01:Webサーバに認証ファイルを配置

・DNS-01:DNSにTXTレコードを追加

3.検証成功後、証明書を発行

4.有効期限前に自動更新

弊社にてご提供するチャレンジ種別は「DNS-01チャレンジ」となります

【メリット】

・証明書管理を自動化

・更新忘れによる障害を防止

【まとめ】

証明書をAPIで自動取得・自動更新する仕組み

2.お客様へのご依頼事項

【アクセスキーやプロファイルキーの取得】

ご利用の認証局へアクセスキーとプロフィールキーの取得方法についてご確認をお願いします。
ご取得頂いたアクセスキーとプロフィールキーを弊社にご提供ください。

【DNSレコードの登録】

更新したい証明書のドメイン名にて、以下のCNAMEレコードの登録をお願いします。
初回登録時の1回のみで問題ございません。

※example.com による例

_acme-challenge.example.com. IN CNAME _acme-challenge.example-com.acme.aams.jp.

ドメイン名の「.(ドット)」は「-(ハイフン)」へ変換してください

弊社側のDNSサーバでは以下のような設定を行います。
DNS-01チャレンジのタイミングで弊社側にて都度更新を行います。

_acme-challenge.example-com.acme.aams.jp. IN TXT "xx"

DNS-01チャレンジにて取得したテキストレコードを登録します

3. ACMEによる証明書発行・更新フロー

