Engineer

ACME

✹ 人の操作なしで証明書を発行するプロトコル

どのようなものか

ACME（Automatic Certificate Management Environment）は、プログラムが認証局へ証明書を要求し、要求した名前を管理していることを証明し、期限切れ前に新しい証明書を取得するためのプロトコルです。途中で、人がフォームに記入したり、確認メールに応答したりすることはありません。2019年3月にRFC 8555として標準化され、多くの人はLet's Encryptという認証局を通して使っています。

クライアントは、どの証明書の鍵とも分けて保持する自身のアカウント鍵を用意し、その鍵ですべての要求に署名します。証明書の取得は、サーバー上の五つのリソースを通ります。

```
newAccount   アカウント鍵を一度だけ登録する
newOrder     証明書の対象とする名前を列挙する
authz        名前ごとの認可に、チャレンジの選択肢を示す
finalize     すべて検証済みになったら証明書署名要求を送る
certificate  発行された証明書チェーンを取得してインストールする
```

チャレンジは、クライアントが名前の管理権限を示す方法です。サーバーがトークンを渡し、クライアントはアカウント鍵のフィンガープリントと結び付け、そのアカウントに固有の証明を作ります。それを、名前を管理する人だけが置ける場所に公開します。重要なチャレンジは三種類です。

- **http-01**は、対象の名前の `/.well-known/acme-challenge/<token>` に、値をファイルとして提供します。認証局の最初の要求は、必ずポート80への平文HTTPで届きます。
- **dns-01**は、その名前の下の `_acme-challenge` のTXTレコードに、値のハッシュを置きます。三つのうち、 `*.example.com` のようなワイルドカードの管理権限を証明できるのは、これだけです。

- **tls-alpn-01**は、2020年2月のRFC 8737で追加され、専用のALPNプロトコルを使うTLSハンドシェイク中に、ポート443で応答します。ポート443を持ち、ポート80を使えないリバースプロキシに適しています。

2025年6月に公開されたRFC 9773は、ACME Renewal Information（ARI）を追加しました。認証局が、発行した各証明書の更新を推奨する期間を公開し、クライアントは推測せずに、その推奨期間を問い合わせます。例えば一斉失効の前に、誰も設定ファイルを編集することなく、認証局が更新を前倒しできます。

概念を判断に生かす

「ACMEとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

証明書を手動で更新し続けられるかは、もはや好みの問題ではありません。日付で条件が決まっています。

CA/Browser Forumは、公に信頼されるすべての認証局が従うルールを定めています。2025年4月に採択したSC-081v3は、2026年3月15日以降に発行する証明書の有効期間を200日以下に制限します。2027年3月15日から100日、2029年3月15日から47日に短縮します。ドメインの管理権限の証明を再利用できる期間も、現在の200日から100日、最終的には10日だけに短縮します。最終段階では、有効期間の三分の二が経過した時点で更新する場合、約一か月ごとに新しい証明書が必要で、ほぼ毎回、新しいチャレンジが必要になります。

Let’s Encryptは、それより先を進んでいます。現在の標準の証明書は90日間有効ですが、2027年2月10日から64日、認可の再利用期間は10日となり、2028年2月16日からは45日、再利用期間は7時間になります。自身の発表で、手動更新は推奨しないと述べています。また、2025年6月4日に期限の通知メールを廃止しており、更新忘れを知らせる安全網もなくなりました。

手動更新を選べないため、ACMEが標準となります。残る判断は、各部分をどこに置くかです。

- **チャレンジ。** ポート80で応答する単一サーバーなら、http-01から簡単に始められます。ワイルドカード、同じ名前の背後にある複数サーバー、インターネットから到達できないホストでは、dns-01の追加設定に価値があります。ポート443を持ち、ポート80を使えないプロキシには、tls-alpn-01が適します。
- **クライアント。** ウェブサーバー内に置く、その横で動かして新しい証明書をインストールするフックを設ける、または別のマシンで検証を集中して行い、証明書をコピーする方法があります。
- **監視するもの。** 更新を行うクライアント自身が故障した場面なので、その外側で、更新されていないことに気付く必要があります。

実際の活用例

当社はDevOpsエンジニアとして、ApacheとNginxの両方がトラフィックを処理するUbuntu Linuxホスト上の、百のDockerアプリケーションから、証明書に関する手作業を取り除きました。各証明書の発行、期限切れ前の更新、デプロイまで、全手順をACMEが行いました。誰かが日付を覚えていることに頼る手順はなくなり、百のアプリケーションすべてで有効な証明書を維持し、手作業も不要になりました。

デプロイは、その重要性を見落としやすい手順です。ApacheとNginxは、起動または再読み込み時に証明書を読み、そのコピーを提供し続けます。新しいファイルを書くだけのクライアントでは、訪問者から見えるものは何も更新されません。両者が同じサーバー群で動く場合は、新しい証明書が届いた後、それぞれの再読み込みが必要です。

自社サイトでは、クライアントをウェブサーバーに含める、別の構成を使っています。Caddy自体がLet's Encryptからサイトの証明書を更新します。CaddyはACMEに標準対応し、別のツールが不要なため、忘れる可能性のあるデプロイ手順がありません。

問題が起きるところ

ブラウザーでは正常に開けるのに、チャレンジが時間切れか404になります。 http-01の要求はポート80に届き、その経路のどこかに問題があります。443だけを開けるファイアウォールやクラウドのセキュリティグループ、80・443以外へ移すリダイレクト、トークンを受け取っていないサーバーへ送るロードバランサーなどです。Let's Encryptは、最大十回、かつこの二つのポートへのリダイレクトだけをたどります。ポート80を開け、すべてのバックエンドまたは共有ストレージからチャレンジのパスを提供し、ポート80を使えない場合はdns-01に切り替えます。

ウェブサーバー上のDNS API鍵が、ゾーン全体を書き換えられます。 ワイルドカードにはdns-01が必要なので、クライアントはTXTレコードを作る手段が必要です。最も簡単に取得できる認証情報は、アカウントが所有するすべてのレコードを変更できるものであることが少なくありません。ウェブサーバーに侵入されると、メールも他のすべての名前も転送され得ます。事業者が提供する場合は `_acme-challenge` レコードだけに限定した認証情報を使う、CNAMEで `_acme-challenge` をチャレンジ専用のゾーンへ向ける、または別のマシンで検証して証明書をコピーします。DNS変更の反映には時間がかかるため、チャレンジの準備完了を認証局へ伝える前に、最大一時間ほど待つ必要がある場合もあります。

再デプロイ後の新しいコンテナーに証明書がありません。 各コンテナーが起動時に証明書を要求し、自身のファイルシステムにだけ保持すると、再起動のたびに再要求します。再デプロイが多かったり、一度に多数を起動したりすると、認証局のレート制限で追加の注文が拒否されます。RFC 8555は、このエラーに `rateLimited` という名前を付けています。Let's Encryptは、最悪の場合、どのインスタンスも証明書を得られないと警告しています。証明書と鍵を永続ストレージに保持し、新しいインスタンスは、注文前に、そこにある有効な証明書を使います。

更新タイマーが固定されているため、有効期間の短縮後に期限切れになります。 例えば90日証明書に合わせ、60日ごとに更新するジョブです。64日証明書では余裕が四日、45日証明書では、タイマーの起動より約二週間前に期限が切れます。RFC 9773は、固定間隔を、認証局が有効期間を変更する妨げとなる習慣の一つに挙げています。クライアントが対応する場合はARIを有効にします。Let's Encryptは、少なくとも一日二回確認し、安全策として有効期間の三分の一が残る時点で更新することを勧めています。

クライアントは成功と報告しても、訪問者には古い証明書が見えます。 新しいファイルはディスクにありますが、ウェブサーバーへ再読み込みを指示していないか、フックが複数のうち一台だけを再読み込みしています。古い証明書は期限まで使われ続けます。クライアントのデプロイフックから再読み込みし、ファイルではなく、外部から実際に提供中の証明書を監視します。

```
openssl s_client -connect example.com:443 -servername example.com \
    </dev/null 2>/dev/null | openssl x509 -noout -enddate
```

参考資料

- RFC 8555：Automatic Certificate Management Environment（ACME）：アカウント、注文、認可、http-01とdns-01のチャレンジを規定します。
- RFC 9773：ACME Renewal Information（ARI）拡張：認証局が各証明書の更新を推奨する期間を規定します。
- RFC 8737：ACME TLS Application-Layer Protocol Negotiation（ALPN）チャレンジ拡張：すべてポート443で応答するtls-alpn-01を規定します。
- チャレンジの種類：Let's Encrypt自身が、三種類とその制限を比較しています。
- 証明書の有効期間を45日に短縮：Let's Encryptの短縮日程と、更新に関する助言です。
- SC-081v3の投票：200日、100日、47日の制限を定める、CA/Browser Forumの投票です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「ACMEとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/acme/