JPRS サーバー証明書発行サービス ACME 対応版

acme.sh ご利用マニュアル

Version 1.1

株式会社日本レジストリサービス（JPRS）

目次

更新履歴

日付	Version	
2024/03/21	1.0	初版リリース
2024/04/11	1.1	誤植の修正

1 本資料について

本資料では、JPRS サーバー証明書発行サービス ACME 対応版（以下、本サービス）でご利用可能な ACME クライアントの一つである、acme.sh のご利用方法について説明します。

1.1 ACME について

ACME（アクミー）は、Automatic Certificate Management Environment（自動証明書管理環境）に由来する、証明書の管理を自動化するためのプロトコル（取り決め）です。証明書の管理者が ACME に対応することで、サーバー証明書をほぼ全自動で管理できます。

ACME に対応する場合、ACME のサービスを利用するためのソフトウェアである、ACME クライアントを使用できます。

1.2 acme.sh について

acme.sh は UNIX ベースのシェルスクリプトです。無償で利用可能です。

1.3 本資料における前提条件について

本資料は、以下の前提条件で記述しています。

- ✓ CentOS7 及び Apache2.4.6 をご利用中のものとします。
- ✓ OS の設定については、本資料の対象外とします。
- ✓ acme.sh のインストール方法については、本資料の対象外とします。
- ✓ ワイルドカード証明書を含む、DNS 認証（dns-01）を利用したサーバー証明書の発行・更新につきましては、ご利用中の DNS プロバイダーとの連携に対応したプラグインが必要となるため、本資料の対象外とします。恐れ入りますが、DNS 認証プラグインの利用方法につきましては、ご利用者様にてご確認ください。

2 事前準備

2.1 acme.sh のインストール

以下の参考 URL に記載された公式ドキュメント等をご参照のうえ、ご利用の環境に acme.sh をインストールしてください。

なお、インストール方法については本資料では扱いませんので、予めご了承ください。

参考 How to install https://github.com/acmesh-official/acme.sh/wiki/How-to-install

2.2 指定事業者を経由した本サービスの利用申し込み

本サービスのご利用には、指定事業者を経由した申し込みが必要になります。

お手続き方法等は、指定事業者により異なります。申し込みやお手続きなどの詳細につきましては、ご利用の指定事業者にお問い合わせください。

2.3 ACME アカウントの発行に必要な EAB 認証情報の受領

本サービスのご利用には、EAB（認証情報）が必要です。

ご利用の指定事業者から EAB（認証情報）を受け取ってください。

※ EAB（認証情報）の有効期間は、EAB 認証情報の発行から 14 日間です。
この期間内に、手順 3.1「ACME アカウントの発行する」を行ってください。

※ EAB（認証情報）の有効期間が終了した場合や、EAB（認証情報）を失くした場合には、指定事業者へ EAB（認証情報）の発行を依頼してください。

3 初回の証明書発行を行う

3.1 ACME アカウントを発行する

本サービスを利用するための ACME アカウントの発行が必要になります。ご利用中の指定事業者から受領した EAB（認証情報）をご用意ください。
なお、ACME アカウント発行にあたり、JPRS からの緊急連絡を受信するメールアドレスの登録が必要になります。

EAB（認証情報）を利用し、ACME アカウントを発行します。

・--server（必須）: JPRS の ACME サーバーを接続先に指定します。
・--register-account（必須）: ACME アカウント（EAB 認証情報）を登録します。
・--eab-kid（必須）: 指定事業者から受領した MAC 鍵識別子を入力します。
・--eab-hmac-key（必須）: 指定事業者から受領した MAC 鍵を入力します。
・--accountemail（必須）: JPRS からの緊急連絡を受信するメールアドレスを登録します。

```
$acme.sh --server https://acme.amecert.jprs.jp/DV/getDirectory --register-account --eab-kid AbAA5CL8vlEg6hMysInnIMk8_8ARMfe7URnm8 --eab-hmac-key uo_JAOUM06AfZ3Smv-Xbf3NyDpaQa4G9_7XI --accountemail info@jprs.jp
```

$の表示は、ご利用の環境により異なります。また、この部分の入力は不要です。

以下のメッセージが表示されましたら、ACME アカウントの発行は完了です。

```
Create account key ok.
Registering account: https://acme.amecert.jprs.jp/DV/getDirectory
Registered
ACCOUNT_THUMBPRINT='7cVRvemCjrikbp-V9yweMB6Iqgj4BBJYRQI'
```


3.2 サーバー証明書を発行する

本サービスではサーバー証明書発行時のドメイン名利用権の確認方法として、ACME のファイル認証（http-01）または DNS 認証（dns-01）を利用できます。

本マニュアルではファイル認証を利用する場合の例を記載します。

> ご注意
>
> ※ DNS 認証を利用する場合、ご利用中の DNS プロバイダーとの連携に対応したプラグインが必要になります。DNS 認証用のプラグインの利用方法につきましては、恐れ入りますがご利用者様にてご確認ください。

ファイル認証を利用してサーバー証明書を発行する例を以下に示します。

・--server（必須）：JPRS の ACME サーバーを接続先に指定します。

・--issue（必須）：サーバー証明書を発行します。

・-k 2048（必須）：鍵長を 2048 ビットに指定します。

・-w：ドキュメントルートを指定します。

```
acme.sh --server https://acme.amecert.jprs.jp/DV/getDirectory --issue -d
example.jp -k 2048 -w /var/www/html
```

以下のメッセージが表示されましたら、サーバー証明書の発行は完了です。

```
Create account key ok.
Registering account: https://acme.amecert.jprs.jp/DV/getDirectory
Registered
ACCOUNT_THUMBPRINT='FiS1akdnQkesz0StKfrEVmE¥1hiJex0ZU'
./acme.sh --server https://acme.amecert.jprs.jp/DV/getDirectory --issue -d
example.jp -k 2048 -w /var/www/html
Using CA: https://acme.amecert.jprs.jp/DV/getDirectory
Creating domain key
The domain key is here: /root/.acme.sh/example.jp/example.jp.key
Single domain='example.jp'
```



```
Getting domain auth token for each domain
Getting webroot for domain='example.jp'
Verifying: example.jp
Processing, The CA is processing your order, please just wait. (1/30)
Success
Verify finished, start to sign.
Lets finalize the order.
Le_OrderFinalize='https://acme.amecert.jprs.jp/finalizeOrder/NkJJJoaU1yaHJybA'
Order status is processing, lets sleep and retry.
Polling order status: https://acme.amecert.jprs.jp/order/NkJJJoaU1yaHJybA
Order status is processing, lets sleep and retry.
Polling order status: https://acme.amecert.jprs.jp/order/ NkJJJoaU1yaHJybA
Order status is processing, lets sleep and retry.
Polling order status: https://acme.amecert.jprs.jp/order/ NkJJJoaU1yaHJybA
Downloading cert.
Le_LinkCert='https://acme.amecert.jprs.jp/getCert/ NkJJJoaU1yaHJybA'
Cert success.
-----BEGIN CERTIFICATE-----
～証明書情報～
-----END CERTIFICATE-----
Your cert is in: /root/.acme.sh/example.jp.jp/example.jp.cer
Your cert key is in: /root/.acme.sh/example.jp/example.jp.key
The intermediate CA cert is in: /root/.acme.sh/example.jp/ca.cer
And the full chain certs is there: /root/.acme.sh/example.jp/fullchain.cer
```

ご注意

現時点における本サービスの仕様により、証明書の発行から OCSP（証明書のステータス情報をオンラインで提供するプロトコル）サーバーへの情報登録までに、最大 10 分程度のタイムラグが存在します。

これにより、アクセス時に OCSP の情報を確認する一部 Web ブラウザーにおいて、OCSP に関するエラーメッセージが表示される場合があります。当社では Firefox ブラウザーにおいて、この状況を確認しています。

証明書の更新と Web サーバーへの読み込みの間に所定の待機時間を設定することで、エラーの発生を回避できます。

3.3 サーバー証明書を更新する

Acme.sh は、インストール時に Cron ジョブを登録するため、手動での更新作業は不要です。

4 参考情報

4.1 acme.sh 公式サイト

サーバー証明書のインストール・証明書の設定方法は公式サイトをご確認ください。

https://github.com/acmesh-official/acme.sh

4.2 ACME 対応版サービス - エラーの種別と発生条件

本サービスで出力するエラーの種別と発生条件は次の通りです。

エラー種別	HTTP ステータスコード	メッセージ文(英語)	発生条件
accountDoesNotExist	400	The request specified an account that does not exist	指定されたアカウントが存在しない場合
alreadyRevoked	400	The request specified a certificate to be revoked that has already been revoked: [%s]	失効対象の証明書が既に失効されている場合
badCSR	400	The CSR is unacceptable	CSR が受け付けられない場合(鍵長が短すぎるなど)
badNonce	400	The client sent an unacceptable anti-replay nonce	受理不能なノンスを受信した場合
badPublicKey	400	The JWS was signed by a public key the server does not support	アカウント公開鍵の情報に問題がある場合
badRevocationReason	400	The revocation reason provided is not allowed by the server: [%s]	送信された失効理由がサーバー側で許可されていない場合
badSignatureAlgorithm	400	The JWS was signed with an algorithm the server does not support: [%s]	サーバーがサポートしないアルゴリズムで JWS が署名されている場合
caa	403	CAA records forbid the CA from issuing a certificate	CAA レコードにより証明書の発行が許可されていない場合
connection	400	The server could not connect to validation target : [%s]	FQDN の審査対象のサーバーに接続できない場合
externalAccountRequired	400	The request must include a value for the externalAccountBinding field	リクエストに externalAccountBinding(*)が存在しない場合 (*)認証情報(MAC 鍵識別子・MAC 鍵)
invalidContact	400	A contact URL for an account was invalid: [%s]	コンタクトの URL の形式が不正である場合
malformed	400	The request information is invalid	必須項目チェックや形式チェックなどのリクエスト不正である場合
malformed	400	Unable to create account	EAB アカウントが不正である場合

malformed	400	The contact information is invalid:	・コンタクトメールアドレスが 7 件以上設定されている、もしくは、0 件である場合 ・コンタクトメールアドレスが重複して設定されている場合
malformed	400	Please agree to the term of service.	利用規約に同意していない場合
malformed	400	The FQDN is invalid: [%s]	発行できない FQDN である場合
malformed	400	Validity period of application has been expired	オーダーオブジェクトの有効期限切れの場合
malformed	400	Unable to accept order	オーダーオブジェクトのステータスが不正である場合
malformed	400	Validity period of application has been expired	認可オブジェクトが有効期限切れである場合
malformed	400	Unable to accept order	認可オブジェクトのステータスが不正である場合
malformed	400	The certificate does not exist: [%s]	失効対象の証明書が存在しない場合
malformed	405	The HTTP method is invalid: [%s]	リクエスト不正：許容されていない HTTP Method である場合
malformed	415	The content-type is invalid: [%s]	リクエスト不正：許容されていない ContentType である場合
orderNotReady	403	The request attempted to finalize an order that is not ready to be finalized	finalize の準備ができていない order に対して finalize した場合
rejectedIdentifier	400	The server will not issue certificates for the identifier	対象の識別子に対してサーバーが証明書を発行しない場合
serverInternal	500	The server experienced an internal error	サーバーで内部エラーが発生した場合
unauthorized	401	The client lacks sufficient authorization	ACME アカウントのステータスが不正である場合
unsupportedContact	400	A contact URL for an account used an unsupported protocol scheme: [%s]	コンタクト URL がサポートしないスキームである場合
unsupportedIdentifier	400	An identifier is of an unsupported type	識別子がサポートされていない場合

※[%s] や [%d] には、エラーの要因となった具体的な値が出力されます

