JPRS サーバー証明書発行サービス ACME 対応版

Certbot ご利用マニュアル

Version 1.5

株式会社日本レジストリサービス（JPRS）

目次

更新履歴 2

1　本資料について 3

2　事前準備 4

3　初回の証明書発行を行う 5

4　証明書の更新を行う 9

5　その他必要時にのみ行う作業（強制更新、失効） 13

6　参考情報 15

更新履歴

日付	Version	
2021/11/10	1.0	初版リリース
2021/12/08	1.1	失効申請に関するオプションの修正
2022/01/17	1.2	自動更新設定に関する注意事項の追加
2022/03/02	1.3	dry run の挙動に関する修正、注意事項の追加 その他、表現に関する修正
2022/04/11	1.4	OCSP に関する注記書きを更新
2022/12/15	1.5	key-type オプションに関する記載の追加

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、Certbot（サートボット）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 Certbot について

Certbot は米国の非営利法人である電子フロンティア財団（Electronic Frontier Foundation: EFF）が開発・公開している、オープンソースの ACME クライアントの一つです。Certbot は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。

- ✓ root 権限でコマンドを実行できるものとします。
- ✓ OS の設定については、本資料の対象外とします。
- ✓ Certbot のパッケージ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 Certbot 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 Certbot 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：https://certbot.eff.org/docs/install.html

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。

※ 認証情報の有効期間は、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」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。

※　本作業の際、Certbot の開発元である Electronic Frontier Foundation に対し自分のメールアドレスを送信するかの確認メッセージが出力されますが、送信は必須ではありません。送信が行われなくとも、本サービスをご利用いただけます。

■例：

```
# certbot register -m 'mail@example.jp' --agree-tos --eab-kid
'NUtfiBgcWr9oGCWmF8PQd2d499T7WrgqsnkxIOAPASE' --eab-hmac-key
'Shn8-aYwhUw0esMLnqJL_o9Fg_BszfAgrRJjOtGQGGY' --server
'https://acme.amecert.jprs.jp/DV/getDirectory'
```

※「#」はプロンプトであり、入力は不要です。

※ 緑文字は実行環境により異なります。

「Account registered.」メッセージが表示されれば、ACME アカウントの発行は完了です。

■ACME アカウントに関連する Certbot のサブコマンド・オプション（一部）：

サブコマンド	説明
register	ACME アカウントを作成します。

オプション	必須／任意	説明
-m 'MAIL'	任意	ACME アカウントに設定するメールアドレスを指定します。（コマンドラインでのオプション指定は任意ですが、指定しない場合にはインタラクティブに入力を求められます）
--agree-tos	任意	JPRS の利用規約に同意します。（コマンドラインでのオプション指定は任意ですが、指定しない場合にはインタラクティブに入力を求められます）
--eab-kid 'KID'	**必須**	ACME アカウントの認証情報を指定します。（MAC 鍵識別子）
--eab-hmac-key 'HMAC-KEY'	**必須**	ACME アカウントの認証情報を指定します。（MAC 鍵）
--server 'SERVER'	**必須**	申請先のサーバーホストを指定します。以下の固定値を入力してください。'https://acme.amecert.jprs.jp/DV/getDirectory'

3.2 サーバー証明書を発行・設定する

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し、Apache Web サーバーに証明書を設定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。

■例：

```
#certbot run --apache -d example.com, www.example.com --key-type rsa
--server 'https://acme.amecert.jprs.jp/DV/getDirectory'
```

複数の FQDN を指定する場合、example.jp,www.example.jp のようにコンマで区切って指定します。複数の FQDN を指定することで、それらの FQDN が SAN（そのサーバー証明書を設定・使用するドメイン名）に記載された、1 枚の証明書が発行されます。

> ご注意
> ※ この状況において指定した FQDN の一つを利用終了した場合、その証明書自体が失効され、結果として他の FQDN が使用中であった場合も、指定したすべての FQDN の証明書が無効となることにご注意ください。
> 当該状況を回避するため、複数の FQDN を指定する場合、同じ利用期間を持つ FQDN とすることを推奨します。

「Successfully received certificate.」メッセージが表示されれば、証明書の発行は完了です。

発行された証明書は通常、以下のディレクトリで確認できます。

証明書 ：/etc/letsencrypt/live/${FQDN}/fullchain.pem

秘密鍵 ：/etc/letsencrypt/live/${FQDN}/privkey.pem

※　${FQDN} は、証明書を設定する Web サーバーの FQDN を示します。

※　/etc/letsencrypt は、Certbot がデフォルト設定で生成するディレクトリです。

■証明書発行に関連する Certbot のサブコマンド・オプション（一部）：

サブコマンド	説明
run	証明書の発行・更新・Web サーバーへのインストールを行います。

オプション	必須／任意	説明
-d	**必須**	証明書を発行する FQDN を指定します。カンマで区切ることで複数指定が可能です。
--apache	任意	apache プラグインを利用して、証明書の発行とインストールを自動化します。 利用する認証方法はファイル認証となります。
--key-type	Certbot 2.0.0 以降は必須	rsa を指定します。 ※Certbot 2.0.0 以降、指定しない場合申請エラーになります。

ご注意

※ ワイルドカード証明書はファイル認証では発行できません。DNS 認証をご利用ください。

※ DNS 認証では、証明書の発行対象となる FQDN のゾーンを管理する権威 DNS サーバーに、ドメイン名利用権確認用の認証文字列が記載された TXT レコードを所定の方式で設定・更新する必要があります。そのため、DNS 認証を利用して証明書の発行・更新を自動化する（TXT レコードの設定・更新を自動化する）場合、ご利用の DNS プロバイダーが ACME クライアントとの API 連携に対応している必要があります。詳細につきましては、ご利用中の DNS プロバイダーにご確認ください。

※ Certbot には主な DNS プロバイダーとの API 連携に対応したプラグインが用意されています。詳細は Certbot 公式の Web サイト(*)をご確認ください。

(*)https://certbot.eff.org/docs/using.html#dns-plugins

4 証明書の更新を行う

4.1 更新を行う

Certbot renew コマンドを実行し、サーバー証明書を更新します。

このコマンドは、証明書の有効期間が 30 日以上残っている場合は更新がスキップされ、30 日未満である場合に更新を実行します。

```
#certbot renew
```

ご注意

※ Certbot のオプションである ‘--dry-run’ は本サービスでは正常に動作しないため、利用しないようお願いします。

4.2 自動更新設定を行う

‘renew’コマンドを定期的に実行するように設定することで、証明書の更新を自動化できます。

以下の例では、証明書の更新を自動化し Apache の設定ファイルを再読み込みする場合の設定を、cron に記述したものを示しています。

■例：

```
sudo crontab -l -u root
0 0,12 * * * certbot renew --deploy-hook "sleep 10m;systemctl reload httpd"
```

ご注意

※ ご利用の環境・インストール方法によって、Certbot が自動更新用のサンプルファイルを生成する場合があります。本記載例は、サンプルファイルを利用しない場合の手順となります。

※ 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。上記の例では Linux の sleep コマンドにより、10 分の待機時間を設定しています。

✓ （必要時）更新の設定を確認する

証明書の更新の際は設定ファイルに記述された、発行時に指定したオプションを利用して申請を行います。変更が必要な場合、設定ファイルを修正してください。
設定ファイルは通常、以下のディレクトリに格納されます。

/etc/letsencrypt/renewal/${FQDN}.conf

※　${FQDN}は、証明書を設定するWebサーバーのFQDNを示します。

また、この設定ファイルの”renew_before_expiry”の値を変更することで、‘renew’コマンドで更新を実行する証明書の有効期限を変更することができます。
以下の例では、”renew_before_expiry”を91日にすることで、必ず’renew’コマンドで証明書が更新されるようにした場合の設定を示しています。

※　以下は例示用の設定であり、本運用における設定は推奨されません。
　　更新申請の挙動確認などにご利用ください。

■例：

```
/etc/letsencrypt/renewal/${FQDN}.conf
renew_before_expiry = 91 days
version =
archive_dir = /etc/letsencrypt/archive/${FQDN}
cert = /etc/letsencrypt/live/${FQDN}/cert.pem
privkey = /etc/letsencrypt/live/${FQDN}/privkey.pem
chain = /etc/letsencrypt/live/${FQDN}/chain.pem
fullchain = /etc/letsencrypt/live/${FQDN}/fullchain.pem

# Options and defaults used in the renewal process
[renewalparams]
account =
server = https://acme.amecert.jprs.jp/DV/getDirectory
authenticator =
```


5 その他必要時にのみ行う作業（強制更新、失効）

5.1 強制的に更新を行う

'-- force-renewal'オプションを指定することで、証明書の有効期間が 30 日以上残っている場合も、証明書を強制的に更新できます。緊急に証明書の入れ替えが必要になったなどの場合に、本オプションを指定してください。

※ 大量の証明書発行が継続して行われた場合、サーバー側で申請を制限する場合があります。

■例：

```
#certbot renew --force-renewal
```

■証明書更新に関連する Certbot のサブコマンド・オプション（一部）：

サブコマンド	説明
renew	以前に発行した有効期間満了が近い証明書（デフォルトでは 30 日未満）を全て更新します。

オプション	必須／任意	説明
--force-renewal	任意	証明書の有効期限に関わらず、すぐに証明書の更新を行います。
-- deploy-hook 'コマンド'	任意	個々の証明書の更新が行われた場合にのみ、指定したコマンドが 1 度だけ実行されます。更新が行われなかった場合は実行されません。
-- post-hook 'コマンド'	任意	全ての証明書の更新申請が終わった後、指定したコマンドが 1 度だけ実行されます。更新申請が行われなかった場合は実行されません。

5.2 （必要時）証明書を失効する

秘密鍵の危殆化など、証明書を失効する必要が生じた場合、次のコマンドを実行することで証明書を失効できます。

■例：

```
# certbot revoke --cert-path /etc/letsencrypt/live/example.com/cert.pem --server 'https://acme.amecert.jprs.jp/DV/getDirectory'
```

「Congratulations! You have successfully revoked the certificate that was located at サーバー証明書ファイル（.pem）のフルパス 」メッセージが表示されれば、証明書の失効は完了です。

■証明書失効に関連する Certbot のサブコマンド・オプション（一部）：

サブコマンド	説明
revoke	発行した証明書を失効します。

オプション	必須／任意	説明
-- cert-path サーバー証明書ファイル（.pem）のフルパス	任意	サブコマンドを実行する対象となるサーバー証明書ファイルを指定します。
--server 'SERVER'	**必須**	申請先のサーバーホストを指定します。以下の固定値を入力してください。 'https://acme.amecert.jprs.jp/DV/getDirectory'

6 参考情報

6.1 Certbot 公式 - all-instructions

様々な環境に Certbot のインストール・証明書の設定方法が記載されています。

https://certbot.eff.org/all-instructions/

6.2 Certbot 公式 - ユーザーガイド

Certbot を利用する際の詳細説明（利用可能なサブコマンド・オプションの一覧など）が記載されています。

https://certbot.eff.org/docs/using.html

6.3 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

