セコムパスポート for Web シリーズ

ACME_証明書発行手順書
【Certbot 編】

第 2 版
2026 年 1 月 15 日

セコムトラストシステムズ株式会社

目　次

1.　本手順書について 3
2.　EAB の取得 3
3.　証明書発行（初回） 4
3.1.　ドメイン審査方法の確認 4
3.2.　アカウントの発行および証明書の発行 4
3.3.　証明書の確認 6
3.4.　証明書のインストール 6
4.　証明書発行（更新） 7
4.1.　証明書の更新 7
4.2.　証明書自動更新の設定 7
4.3.　証明書の更新可能期間（必要な場合） 8
5.　証明書の再発行 9
6.　証明書の失効 9

1. 本手順書について

ACME を利用して証明書を発行するにあたり、ACME クライアントの一つである Certbot（サートボット）をご利用いただく場合に、証明書発行に必要となる認証情報（以下「EAB」といいます）の設定から証明書発行を行うまでの手順書となります。ACME での証明書発行の流れについてはこちらを参照ください。

ACME クライアントである Certbot は、Certbot の公式サイト　https://certbot.eff.org/　から入手し、サーバー等にインストールしてご利用ください。

本手順書は Linux を利用して、certbot が提供するマニュアルを元に当社で検証を行った方法になり、一部のオプションコマンドを掲載しています。オプションコマンドや詳細な設定については、Certbot が提供する以下ユーザーマニュアル等を参照ください。

redhat Certbot User Guid　：　https://eff-certbot.readthedocs.io/en/stable/using.html

2. EAB の取得

証明書発行に必要な EAB は、審査が完了した後、「契約申込書承諾、および、証明書ダウンロード手続きのご案内」のメールが届きましたら、お客様専用ページからダウンロードができるようになります。

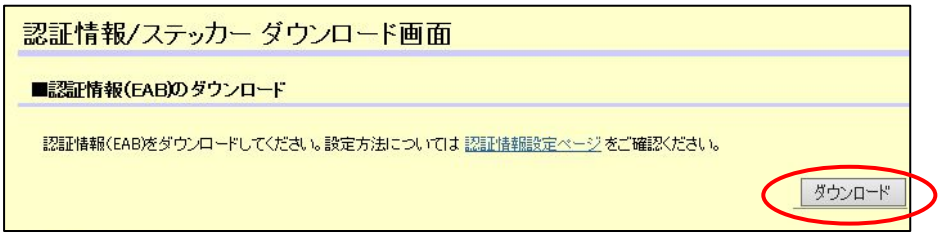
【お客様専用ページへのログインはこちら】
https://www.secomtrust.net/service/pfw/user/login.html

＝＝重要＝＝
EAB はお客様が証明書を発行するための重要な情報となります。管理には十分ご注意ください。

（１）お申込一覧中画面から、ダウンロードする契約の「詳細」ボタンをクリックしてください。

（２）お申込情報詳細画面にある、認証情報（EAB）/ステッカーのダウンロードの「ダウンロードはこちら」をクリックします。

（３）認証情報（EAB）/ステッカーダウンロード画面から、ダウンロードボタンをクリックして EAB をダウンロードしてください。



3. 証明書発行（初回）

3.1. ドメイン審査方法の確認

ACME でサーバー証明書を発行する際にドメイン利用権の確認が行われるため、ドメイン審査方法を選択します。ACME では以下いずれかのドメイン審査方法のご利用が可能です。

■ドメイン審査方法

種類	審査概要
ファイル認証（http-01）※1	指定する URL にランダム値を設定し、その URL にアクセスしてランダム値を確認する審査方法
DNS 認証（dns-01）※2	DNS の TXT レコードにランダム値を設定し、DNS へ問い合わせしてランダム値を確認する審査方法

※1　日本国外からのアクセスを制限されている場合も含め、外部公開されていないサーバーの場合はご利用いただけませんので、ご注意ください。

※2 ドメイン審査を自動化するには事前に DNS プロバイダに対応したプラグインが必要になります。DNS との連携については、DNS 事業者へお問い合わせください。

3.2. アカウントの発行および証明書の発行

初めて証明書を発行する場合、ACME アカウントの発行が必要になりますので、ダウンロードした EAB をご用意ください。

（１）以下のコマンドを実行します。　※コマンドは下部で説明

コマンド例）

certbot --server［サーバーホスト］--eab-hmac-key［MAC 鍵］--eab-kid［MAC 鍵識別子］ -d［コモンネーム］--key-type［暗号］

入力例）

```
[xxxxxx]# certbot --server https://secomtrustacme.com/acme/ --eab-hmac-key
jT7wsDpSs8RmCQjgyABCD123Zencvh4eZJB5QwjUryN6 --eab-kid Abcde9gvkzOU -d
www.example.com --key-type rsa
```

≪マルチドメインでご契約した場合≫

-d［コモンネーム］ の箇に、契約したコモンネームを並べて記載してください。

例）　-d www.example.com –d www2.example.com –d www3.example.com

（２）使用するプラグインを選択します。

出力例）

```
How would you like to authenticate and install certificates?
-------------------------------------------------------------------------------
1: Apache Web Server plugin (apache)
2: Nginx Web Server plugin (nginx)
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
```

（３）メールアドレスを登録します。

出力例）

```
Enter email address or hit Enter to skip.
(Enter 'c' to cancel): test@example.com
```

（４）本サービスの利用規定に同意します。「y」を選択ください。

出力例）

```
-------------------------------------------------------------------------------
Please read the Terms of Service at:
https://repo1.secomtrust.net/spcpp/publicly-trusted-cpcps/
You must agree in order to register with the ACME server. Do you agree?
-------------------------------------------------------------------------------
(Y)es/(N)o: y
```

（５）以下のメッセージが表示された場合、Certbot 提供元（電子フロンティア団体）にメールアドレスの提供可否を選択します。提供する場合は「y」を、拒否する場合は「n」を選択ください。

出力例）

```
-------------------------------------------------------------------------------
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-------------------------------------------------------------------------------
(Y)es/(N)o: n
```

「Successfully received certificate.」が表示されたら、証明書発行は完了です。

■コマンド説明

オプションコマンド	お客様入力値	説明
--server	[サーバーホスト]	証明書発行する認証局のURLを入力（EAB内に記載）
--eab-kid	[MAC鍵識別子]	MAC識別子を入力（EAB内に記載）
--eab-hmac-key	[MAC 鍵]	MAC鍵を入力（EAB内に記載）
-d	[コモンネーム]	証明書に登録するFQDN
--key-type	[暗号]	RSA鍵を指定（EAB内に記載） ※「rsa」指定が必須です。

-m	[メールアドレス]	ACMEアカウントに設定するメールアドレスを入力
--agree-tos	—	本サービスの利用規定に同意
--preferred-challenges	[ドメイン審査方法]	ドメイン審査方法を選択 dns ： DNS認証 http: ファイル認証 ※certbotのバージョン等により、デフォルトでhttpが設定されている場合があります。

※ [ ] 色はコマンド上　必須入力項目です。

＝＝ご注意＝＝

証明書発行を行う際、Apache の場合は Apache プラグイン、nginx の場合は nginx のプラグイン、また cron を利用する場合は cron のインストールが必要です。事前にインストールを行ってください。

3.3. 証明書の確認

発行された証明書は、以下のディレクトリで確認することができます。

証明書 ： /etc/letsencrypt/live/[コモンネーム]/fullchain.pem
秘密鍵 ： /etc/letsencrypt/live/[コモンネーム]/privkey.pem

出力例）

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/www.example.com/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/www.example.com /privkey.pem
This certificate expires on 2026-08-31.
These files will be updated when the certificate renews.
```

※ディレクトリ名はデフォルトで「letsencrypt」となっています。

3.4. 証明書のインストール

証明書の発行は ACME プロトコルで行われますが、インストールにおいてはお客様自身で設定をいただきます。コンフィグファイルを設定いただき、「3.3 証明書の確認」にあるサーバー証明書、中間 CA 証明書、秘密鍵の 3 つのファイルを指定してサービス（またはサーバー）の再起動等を行ってください。

4.　証明書発行（更新）

ACME には、期限切れが近い証明書や失効した証明書に関する情報を取得し、それに基づいて証明書を再発行するべきか、または既存の証明書を使い続けるべきかを判断する機能が備わっています。この仕組みにより、証明書の有効期限が切れる一定期間前から証明書の更新を行うことが可能になります。

4.1.　証明書の更新

renew コマンドを実行することで、既存の証明書を更新することができます。

コマンド例）

certbot renew --apache --server ［サーバーホスト］ --cert-name ［証明書名］ --deploy-hook "systemctl restart httpd"

入力例）

```
[xxxxxx]# certbot renew --apache --server https://secomtrustacme.com/acme/ --cert-name www.example.com --deploy-hook "systemctl restart httpd"
```

■コマンド説明

オプションコマンド	お客様入力値	説明
--server	［サーバーホスト］	証明書発行する認証局のURLを入力（EAB内に記載）
--cert-name	［証明書名］	certbotが管理している証明書名。 「certbot certificates」コマンドを実行することで確認できます。（デフォルト：ドメイン名）
--apache	―	サーバーを選択 Apacheを指定 ※nginxの場合は --nginx
--deploy-hook	"systemctl restart httpd"	サービスの再起動 ※nginxの場合は"systemctl restart nginx"

※ □ 色はコマンド上　必須入力項目です。

4.2.　証明書自動更新の設定

4.1 の Renew コマンドで証明書を更新することができますが、このコマンドを定期的に実行することで、証明書の更新を自動化することができます。自動化する方法としては、certbot に備わっている ertbot.timer や、Linux であれば cron を使用する方法などがあります。

以下の例はcronを使用して証明書の自動更新を行い、さらにApacheの設定ファイルを再読み込みする場合の設定をcronに記述したものです。

入力例

```
[xxxxxx]# crontab -e
* 1 * * * sudo certbot renew --apache --server https://secomtrustacme.com/acme/ --
cert-name www.example.com --deploy-hook "systemctl restart httpd"
```

＝＝契約更新時のご注意点＝＝

契約更新のご申請は早めに行ってください。

証明書は契約の有効期限内でご利用いただけるものであり、契約成立後に EAB の利用期間が更新されることで、継続して有効な証明書としてご利用いただけます。

契約成立（審査完了）が前契約の有効期限切れ当日となった場合、証明書の自動更新が間に合わない可能性があります。

（例えば、当日の ACME クライアントで設定された cron の実行時刻までに更新が完了せず、前の証明書がそのまま設定されている状態になることがあります。この場合、証明書が期限切れとなり、次回の自動更新時刻までの間、ブラウザで警告が表示されます。）

契約の有効期限切れ当日に契約が成立した場合は、手動で証明書発行およびインストールを行う必要がありますので、ご注意ください。

4.3. 証明書の更新可能期間（必要な場合）

Certbot 4.0.0 では、証明書の有効期間の 3 分の 2 を経過した後に更新が可能になり、Certbot 4.0.0 より前のバージョンでは、有効期限の 30 日前から更新が可能になります。自動更新の設定をされた場合、この更新可能期間に入ると証明書の自動更新が実行されます。

更新可能期間は設定ファイルで変更することが可能であり、設定ファイルはデフォルトで以下のディレクトリに格納されています。

/etc/letsencrypt/renewal/[コモンネーム].conf

この設定ファイルにある“renew_before_expiry”の値を変更することで、証明書の自動更新開始時期を変更することもできます。

例）有効期限の 15 日前から更新する場合

renew_before_expiry = 15 days

※このコマンドは証明書ごとに個別に適用されます。また手動更新の際は参照されません。

5. 証明書の再発行

証明書の有効期間が30日以上残っている場合でも、証明書を強制的に更新（証明書再発行）することができます。秘密鍵や証明書の入れ替えが必要になった場合には、再発行を行ってください。

コマンド例）

certbot renew --force-renewal --server［サーバーホスト］--cert-name［証明書名］

入力例）

```
[xxxxxx]# certbot renew --force-renewal --server https://secomtrustacme.com/acme/ --cert-name www.example.com
```

■コマンド説明

オプションコマンド	お客様入力値	説明
--server	［サーバーホスト］	証明書発行する認証局のURLを入力（EAB内に記載）
--force-renewal	—	強制的に更新を実行
--cert-name	［証明書名］	certbotが管理している証明書名。 「certbot certificates」コマンドを実行することで確認できます。（デフォルト：ドメイン名）
--cert-path		証明書を特定（同一FQDNで複数ある場合等に指定）

※ □ 色はコマンド上　必須入力項目です。

6. 証明書の失効

revoke コマンドを実行して、証明書を失効します。該当する失効理由を選択して、証明書を失効してください。

コマンド例）

certbot revoke --server［サーバーホスト］--cert-name［コモンネーム］--reason［失効理由］

入力例）

```
[xxxxxx]# certbot revoke --server https://secomtrustacme.com/acme/ --cert-name www.example.com --reason superseded
```

■コマンド説明

オプションコマンド	お客様入力値	説明
--server	［サーバーホスト］	証明書発行する認証局のURLを入力（EAB内に記載）

--cert-name	[コモンネーム]	失効する証明書のFQDNを入力
--reason	[失効理由]	失効理由を入力（※1）
--cert-path		証明書を特定（同一FQDNで複数ある場合等に指定）

※ [ ] 色はコマンド上　必須入力項目です。

（※1）失効理由は以下より選択してください。

#0：unspecified（その他）

#1：keyCompromise（秘密鍵の危殆化）

#3：affiliationChanged（証明書の記載情報変更）

#4：superseded（証明書の入れ替え）

#5：cessationOfOperation（ウェブサイトの閉鎖またはドメインの所有/管理の終了）