セコムパスポート for Web シリーズ

ACME_証明書発行手順書

【Lego 編】

第 1 版

2025 年 11 月 17 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

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 Lego（レゴ）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 Lego は、Lego の公式サイト　https://go-acme.github.io/lego/
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、Lego 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、Lego が提供する公式ガイド等を参照ください。

Usage　：　https://go-acme.github.io/lego/usage/cli/index.html

2. EAB の取得

2.1. EAB のダウンロード

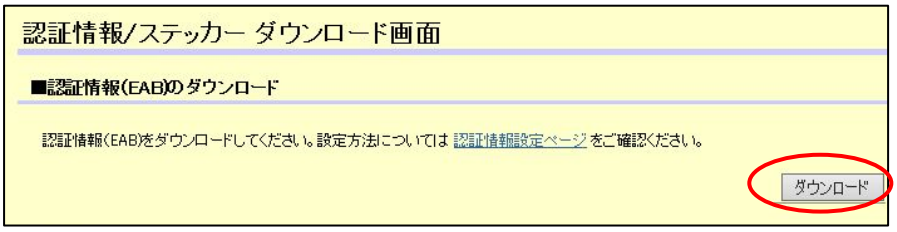
証明書発行に必要な EAB は、審査が完了した後、「契約申込書承諾、および、証明書ダウンロード手続きのご案内」のメールが届きましたら、お客様専用ページからダウンロードができるようになります。

【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）証明書/ステッカーダウンロード画面から、各ダウンロードボタンをクリックしてダウンロードしてください。

2.2. EAB の内容確認

EAB ファイルには、certbot で使用するコマンドが記入されています。本手順とコマンドが異なりますので、以下の［サーバーホスト］［MAC 鍵］［MAC 鍵識別子］の 3 つを抜き出して設定してください。

≪EAB ファイルの中身≫

sudo 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 rsa

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します。証明書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ください。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	お客様サーバーにランダム値のファイルを配置し、そのサーバーにアクセス（問い合わせ）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。
また使用方法の詳細については公式ガイドをご確認ください。

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）run 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）

lego -s［サーバーホスト］--eab --hmac［MAC 鍵］--kid［MAC 鍵識別子］-d［コモンネーム］-m［メールアドレス］--http --key-type［暗号］run

入力例）

```
[xxxxxx]# lego -s https://secomtrustacme.com/acme/ --eab --hmac
1aMIni2bcdefgJQFZUfTVSAxndrp3AlExSy4Sv5W6ic --kid UoRVx1AaBBCC -d
www.example.com -m test@example.com --http --key-type rsa2048 run
```

≪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）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 review the TOS at https://repo1.secomtrust.net/spcpp/publicly-trusted-cpcps/
Do you accept the TOS? Y/n
```

「Your account credentials have been saved in your configuration directory at "/.lego/accounts".」が表示されたらアカウントの登録は完了となり、
また「Server responded with a certificate.」まで表示されたら証明書の発行も完了となります。

■コマンド説明

オプションコマンド	お客様入力値	説明
-s	［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	—	外部アカウントと紐づけして使用
--hmac	［MAC 鍵］	MAC鍵を入力（EAB内に記載）
--kid	［MAC鍵識別子］	MAC識別子を入力（EAB内に記載）
-d	［コモンネーム］	証明書に登録するFQDN
-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
--http --dns	— ［プロバイダ名］	http-01チャレンジを指定する場合 dns-01チャレンジを指定する場合 ※対応プロバイダはlego dnshelpコマンドで確認可能
--key-type	［暗号］	RSA鍵を指定 ※「RSA 2048bit」指定が必須です。
--path	［ディレクトリ］	証明書保存先を指定
--pfx	—	PFX形式で出力（IISで利用する場合に指定）
--pfx.pass	［パスワード］	PFX形式で出力する場合に設定するパスワード

		入力例）'password'

※ [ ] 色はコマンド上 必須入力項目です。http か dns はいずれかが必須です。

3.3. 証明書の確認

発行された証明書がデフォルトでは .lego/certificates ディレクトリに保存されます。certificates ディレクトリへ移動し、証明書および秘密鍵が生成されたかどうか確認できます。

出力例）

```
[xxxxxxx certificates]# ls
www.example.com.crt  www.example.com.issuer.crt  www.example.com.json
www.example.com.key
```

「.crt」・・・サーバー証明書、 「.issuer.crt」・・・中間 CA 証明書、 「.key」・・・秘密鍵
「.json」・・・ドメイン名と証明書 URL（参考情報）

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等を設定いただき、「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

Lego では証明書有効期限の 30 日前からが更新可能な期間となります。renew コマンドを実行して証明書を更新します。

コマンド例）

lego -s [サーバーホスト] -d [コモンネーム] -m [メールアドレス] --key-type [暗号] --http renew

入力例）

```
[xxxxxx]# lego -s https://secomtrustacme.com/acme/ -d www.example.com -m
test@example.com --key-type rsa2048 --http renew
```

■コマンド説明

オプションコマンド	お客様入力値	説明
-s	[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）
-d	[コモンネーム]	証明書に登録するFQDN
-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
--http	—	http-01チャレンジを指定する場合
--dns	[プロバイダ名]	dns-01チャレンジを指定する場合 ※対応プロバイダはlego dnshelpコマンドで確認可能
--key-type	[暗号]	RSA鍵を指定 ※「RSA 2048bit」指定が必須です。
--path	[ディレクトリ]	証明書保存先（新規発行時にパスを指定した場合renewでも必要）

※ 色はコマンド上　必須入力項目です。http か dns はいずれかが必須です。

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。自動化の方法としては、スケジューラ（例：Windows タスクスケジューラや Linux の cron）を使用する方法があります。以下は、証明書の更新を自動化し、更新後にサービスの設定を再読み込みする例となります。
※サンプルのため適宜読み替えて使用してください。

入力例）

Linux環境の例（Apacheの場合）

```
[xxxxxx]# crontab -e
* 1 * * * sudo lego -s https://secomtrustacme.com/acme/ -d www.example.com -m
test@example.com --http --key-type rsa2048 renew --renew-hook "systemctl restart
httpd"？
```

Windows 環境の例(IIS を使用している場合)

```
・スクリプトを作成(C:¥scripts¥sample.ps1 として保存)
& "[lego.exe のフルパス]" -s https://secomtrust-acme.com/acme/ -d www.example.com --key-type rsa2048 -m test@jrce.com --http.webroot C:¥inetpub¥wwwroot --path C:/lego --pfx --pfx.pass 'YourPassword' --http renew --days 999 -renew-hook "powershell -Command Import-PfxCertificate -FilePath 'C:¥lego¥certificates¥www.example.com.pfx' -CertStoreLocation Cert:¥LocalMachine¥My -Password (ConvertTo-SecureString 'YourPassword' -AsPlainText -Force);(Get-WebBinding -Name '[Web サイトの名称]' -Protocol https).AddSslCertificate((Get-ChildItem Cert:¥LocalMachine¥My | Sort-Object NotAfter -Descending | Select-Object -First 1).Thumbprint, 'My')"
・Powershell にて以下を実行
PS C:¥Windows¥system32>
$Action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument '-ExecutionPolicy Bypass -File "C:¥scripts¥sample.ps1"'
$Trigger = New-ScheduledTaskTrigger -Monthly -DaysOfMonth 1 -At 4:00AM
$Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType ServiceAccount -RunLevel Highest
Register-ScheduledTask -TaskName "[タスクの名称]" -Action $Action -Trigger $Trigger -Principal
$Principal

＊参考（登録したタスクの削除） Unregister-ScheduledTask -TaskName "[タスクの名称]" -Confirm:$false
```

＝＝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）

自動更新の設定をされた場合、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が、4.1 の更新コマンドに「--days」オプションを追加することで、更新可能期間を指定することも可能です。

≪参考≫有効期限が切れる 10 日前から証明書を更新したい場合

```
[xxxxxx]#  lego  -s  https://secomtrustacme.com/acme/  -d  www.example.com  -m
test@example.com --key-type rsa2048 --http renew --days 10
```

※証明書有効期限が 10 日以上ある場合は、証明書更新はされません。

■コマンド説明

オプションコマンド	お客様入力値	説明
--days	[残日数]	残り日数を指定 ※証明書の残り日数が[残日数]以下の場合に、強制的に更新させます。

5. 証明書の再発行（強制更新）

証明書の有効期間が 30 日以上残っている場合でも、4.証明書更新 に記載した「--days」オプションを使用することで証明書を再発行（強制更新）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）

lego -s [サーバーホスト] -d [コモンネーム] -m [メールアドレス] --key-type [暗号] --http renew -days [残日数]

入力例）

```
[xxxxxx]#  lego  -s  https://secomtrustacme.com/acme/  -d  www.example.com  -m
test@example.com --key-type rsa2048 --http renew --days 45
```

この場合、証明書有効期限が 45 日以下の場合には、強制的に証明書更新されます。

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。

コマンド例）

lego -s [サーバーホスト] -d [コモンネーム] -m [メールアドレス] --reason [失効理由] revoke

入力例）

```
[xxxxxx]#  lego  -s  https://secomtrustacme.com/acme/  -d  www.example.com  -m
test@example.com --reason 5 revoke
```

■コマンド説明

オプションコマンド	お客様入力値	説明
-s	[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）
-d	[コモンネーム]	証明書に登録するFQDN
-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
--path	[ディレクトリ]	証明書保存先（新規発行時にパスの指定した場合は必要）
--reason	[失効理由]	失効理由を数字で入力（※1）

※ [ ] 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）