DigiCert Consulting Services - DigiCert Japan G.K.

DigiCert CertCentral

Certbot を利用したサーバー証明書自動化

2025-09-03

免責事項

デジサート・ジャパン合同会社は、本書の情報の正確さと完全性を保つべく努力を行っております。ただし、デジサート・ジャパン合同会社は本書に含まれる情報に関して、（明示、黙示、または法律によるものを問わず）いかなる種類の保証も行いません。デジサート・ジャパン合同会社は、本書に含まれる誤り、省略、または記述によって引き起こされるいかなる（直接または間接の）損失または損害についても責任を負わないものとします。

さらに、デジサート・ジャパン合同会社は、本書に記述されている製品またはサービスの適用または使用から生じたいかなる責任も負わず、特に本書に記述されている製品またはサービスが既存または将来の知的所有権を侵害しないという保証を否認します。本書は、本書の読者に対し、本書の内容に従って作成された機器または製品の作成、使用、または販売を行うライセンスを与えるものではありません。最後に、本書に記述されているすべての知的所有権に関するすべての権利と特権は、特許、商標、またはサービス・マークの所有者に属するものであり、それ以外の者は、特許、商標、またはサービス・マークの所有者による明示的な許可、承認、またはライセンスなしにはそのような権利を行使することができません。デジサート・ジャパン合同会社は、本書に含まれるすべての情報を事前の通知なく変更する権利を持ちます。

Table of Contents

1. 本資料について

本資料では、DigiCert CertCentral TLS/SSL Manager（以下、CertCentral）で TLS/SSL 証明書をサードパーティアプリケーションである Certbot を利用して発行する方法について説明します。

1.1 本資料のターゲット

本資料では、下記のユーザーに向けた内容としております。

- TLS/SSL サーバー証明書を利用しているが、自動化が必要な対象機器が少数である
- 対象サーバーが汎用的な Web サーバー等である
- サポート等不要で、単純に TLS/SSL サーバー証明書を自動化する方法が知りたい

1.2 CertCentral について

CertCentral は、幅広いパブリックトラスト製品のリクエストと管理を簡素化し、パブリックトラストの確立と管理の基盤となるソリューションです。

ACME プロトコルに対応しており、TLS/SSL 証明書の発行、更新、失効を行うことができます。

本資料を用いて TLS/SSL 証明書を発行するためには、CertCentral のアカウントおよび契約が必要です。

1.3 ACME について

ACME（Automatic Certificate Management Environment）と呼ばれる証明書の管理を自動化するためのプロトコルで、RFC8555 として発行されています。

ACME を利用するソフトウェアを利用することで、証明書のライフサイクル（発行、更新、失効等）を自動化することができます。

1.4 Certbot について

Certbot は、カリフォルニア州サンフランシスコに拠点を置く 501(c)3 非営利団体である Electronic Frontier Foundation によって作成された、手動で管理される Web サイトで証明書を自動的に使用して HTTPS を有効にするための無料のオープンソースソフトウェアツールです。

1.5 前提条件

本資料は、下記の前提にて記載しております。

- 特権管理者（Linux：root 権限）で実行可能とします
- OS や Web サーバー等の設定については、対象外とします
- Certbot の導入方法は、対象外とします。

1.6 表示情報について

本資料は、certbot コマンドを例として記載しています。

コマンドの表記の凡例を下記に示します。

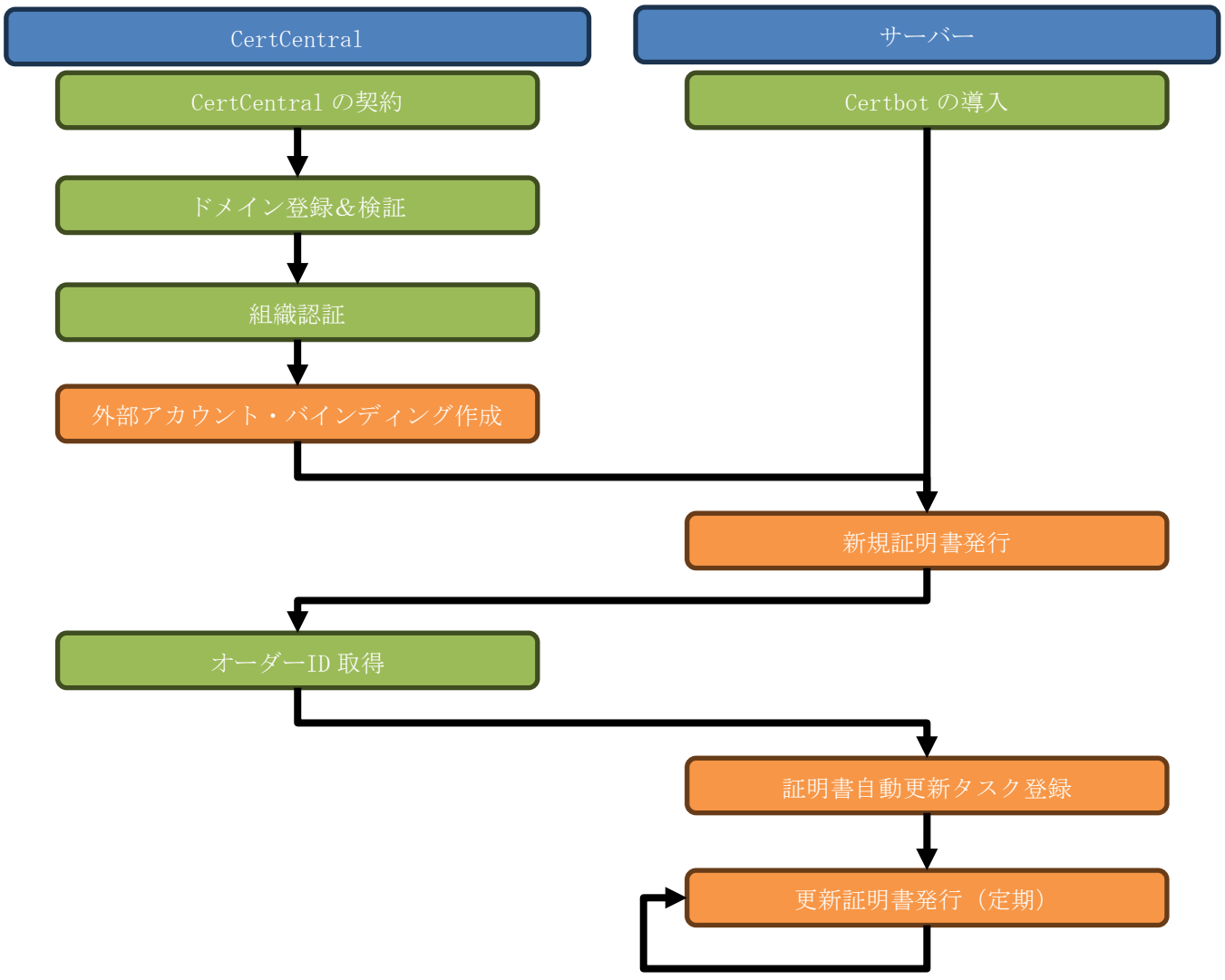
```
# certbot certonly --standalone --non-interactive --force-renewal --config-dir /opt/digicert/certific
ate --server https://one.digicert.com/mpki/api/v1/acme/v2/directory?action=reissue&orderId=123456789
--eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com,test2.example.com
```

1. 先頭の「#」はプロンプトのため、入力は不要です。
2. 緑文字は実行環境により入力値が異なります。

1.7 証明書自動化の流れ

証明書を自動化するための流れは、下図の通りです。

オレンジ色の項目：本書内にて説明。緑色の項目：本書の対象外。



2. 事前準備

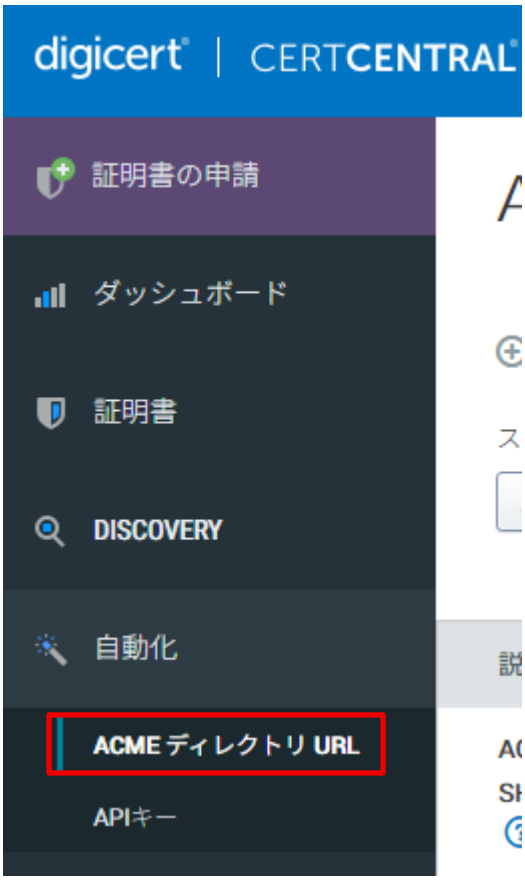
2.1 ACME 外部アカウント バインディング（EAB）の用意

ACME を利用するためには、CertCentral にて外部アカウント バインディング（以下、EAB※）を発行する必要があります。

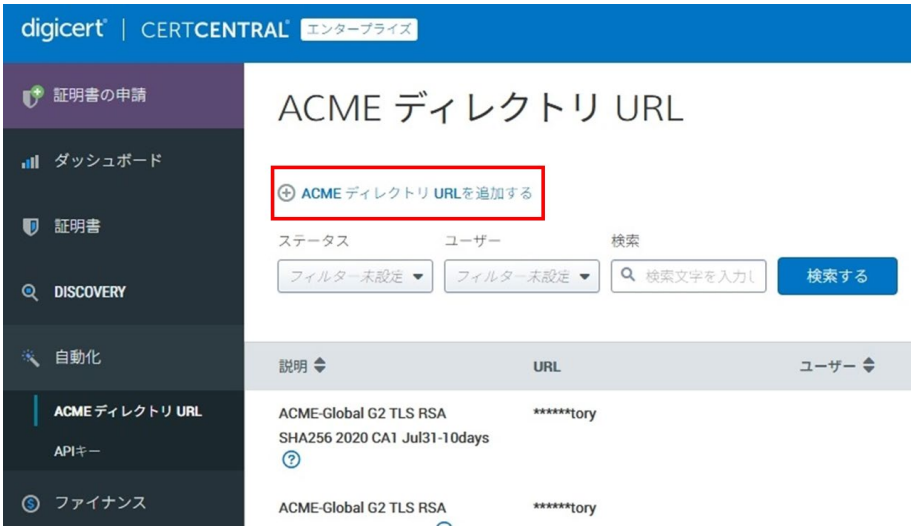
※EAB=External Account Binding

2.1.1 ACME ディレクトリ URL を取得する

CertCentral の左側にあるメニューから「自動化」を選択し、表示される「ACME ディレクトリ URL」を押下します。



「ACME ディレクトリ URL を追加する」を指定します。



ACME ディレクトリ URL を作成するための入力フォームが表示されます。
必要事項をすべて入力いただき、「ACME ディレクトリ URL を追加する」を押下します。
※初期表示は「名前」～「管理グループ」までですが、入力を進めることで表示数が増えます。

「名前」には、CertCentral の画面上で ACME ディレクトリ URL を識別できる任意の名前を入力します。

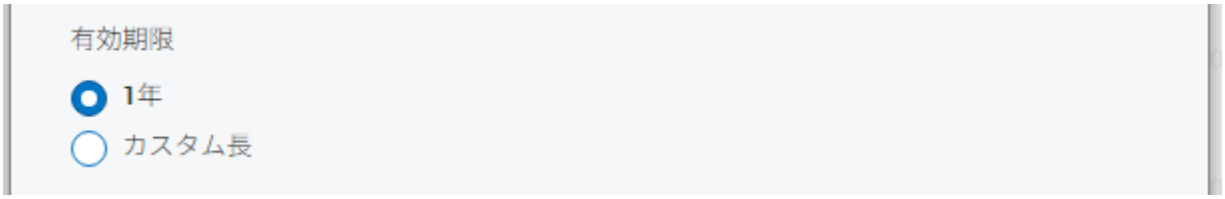
「製品」は、ご契約から購入できる製品がリストアップされます。発行希望の製品を選択してください。

「管理グループ」は、CertCentral に登録されている管理グループから選択します。通常は 1 つの管理グループが作成されています。

「組織」は、CertCentral に登録されている組織情報から選択します。通常は 1 つの組織が作成されています。組織を選択するためには、作成された組織にて組織認証が完了している必要があります。

「複数年のプラン期間」、ご契約されているプランを選択ください。

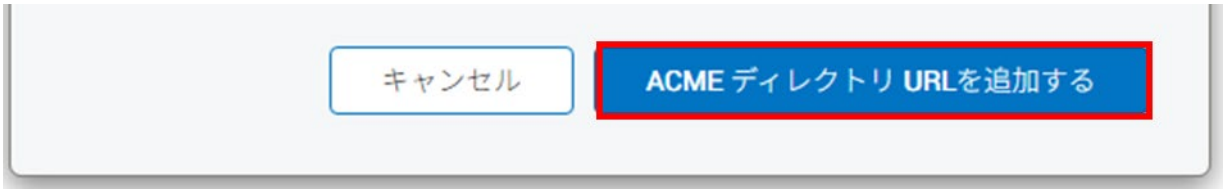
あ



証明書発行時に有効期限を変更する場合にチェックを入れます。通常は不要です。

「中間チェーン」は、発行する証明書の上位の認証局証明書を選択します。ハッシュアルゴリズムや鍵長が異なります。

「ACME ディレクトリ URL を追加する」を押下して URL を作成します。



新しい ACME ディレクトリ URL が生成されます。
「ACME ディレクトリ URL」、「KID」、「HMAC 鍵」をコピーして保管してください。

「すべてをコピーする」を押下することでクリップボードに Certbot で利用できる形式で値を取得できます。
例)

```
--server https://one.digicert.com/mpki/api/v1/acme/v2/directory --eab-kid Q3kufrI87uS6y_vLRiki5riMofakEcr2s_wAchO6oYl --eab-hmac-key 7hepaJechop72coqUm2K1tuneBrusaYl6ha3pud672T5emUz9thlrunEc6lQoQIpdratruDr2FREjIku1uk6DR
```

保管後、「私は、これが再度表示されないことを理解します」を押下して画面を閉じます。
※以後、再度表示して確認することができないことにご注意ください。

3. 新規証明書発行

3.1 サーバー証明書を発行する

サーバー証明書を新たに発行する場合、CertCentral から発行された EAB を付与して、発行対象 FQDN を指定の上で、Certbot コマンドを実行します。

3.1.1 Certbot コマンド例：

```
certbot certonly --standalone --register-unsafely-without-email --non-interactive --force-renewal --config-dir /opt/digicert/certificate --key-type rsa --server https://one.digicert.com/mpki/api/v1/acme/v2/directory?action=reissue&orderId=123456789 --eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com,test2.example.com
```

3.1.2 certonly サブコマンド・オプション

サブコマンド	説明
certonly	証明書を発行します。

必須	オプション	設定値	説明
○	--standalone	なし	スタンドアロン Web サーバーを使用してサーバー証明書を取得します。
×	--register-unsafely-without-email	なし	メールアドレスの登録を不要にします。
×	--non-interactive	なし	ユーザー入力を一切求めずに非対話で実行します。 ※初回起動は、本オプションを指定せずに動作させてください。
○	--domain	FQDN	証明書を取得する FQDN を指定します。 「-domain」オプションを複数指定するか、FQDN のカンマ区切りのリストを指定することでマルチドメイン証明書が発行できます。
○	--eab-kid	EAB_KID	外部アカウントバインディングのキー識別子を指定します
○	--eab-hmac-key	EAB_HMAC_KEY	外部アカウントバインディングの HMAC 鍵を指定します
○	--server	ACME Directory Resource URI	申請先の ACME Directory Resource URI を指定します。

必須	オプション	設定値	説明
×	-force-renewal	なし	要求されたドメインにすでに証明書が存在する場合、有効期限が近いかどうかに関わらず、すぐに更新します。--expand も暗黙的に指定されます。
×	--config-dir	ファイルパス	certbot が使用する設定ディレクトリを指定します。
×	--key-type	アルゴリズム名	「rsa」、「ecdsa」を指定できます。（既定：ecdsa）

※本資料に掲載しているオプションは、一部であり、一例です。certbot コマンドには、他のオプションによる方法もあります。詳細は certbot 公式ドキュメントを参照ください。

3.1.3 複数の FQDN を指定する方法

複数の FQDN を指定する場合、FQDN ごとに「--domain」オプションを指定するか、１つの「--domain」オプションにカンマ区切りで指定します。

例）FQDN ごとに「--domain」オプションを指定する場合：

```
--domain test1.example.com --domain test2.example.com
```

例）１つの「--domain」オプションにカンマ区切りで指定する場合：

```
--domain test1.example.com,test2.example.com
```

3.1.4 発行完了時

下記メッセージが表示されれば、サーバー証明書の発行は完了です。

```
Successfully received certificate.
```

3.1.5 Certbot 初回利用時の規約同意について

Certbot で初めて証明書を発行させる際は、規約に同意する手続きが必要です。

DigiCert Master Service Agreement (https://www.digicert.com/master-services-agreement) をご確認いただき、内容に同意いただける場合は、「Y」を入力してください。

```
[root@digicert dir]# certbot certonly --standalone --register-unsafely-without-email --force-renewal
--config-dir /opt/digicert/certificate --key-type rsa --server https://one.digicert.com/mpki/api/v1/a
cme/v2/directory--eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at:
https://www.digicert.com/master-services-agreement
You must agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
Account registered.
Requesting a certificate for test1.example.com

Successfully received certificate.
Certificate is saved at: /opt/digicert/certificate/live/test1.example.com/fullchain.pem
Key is saved at:         /opt/digicert/certificate/live/test1.example.com/privkey.pem
This certificate expires on 2026-07-17.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

4. 更新証明書発行

4.1 サーバー証明書を更新する

サーバー証明書の有効期限が近づき、証明書を更新する場合は、更新手続きにてサーバー証明書を発行できます。

サーバー証明書を更新させる際に、CertCentral のオーダー番号を指定することで、指定したオーダーのプライマリ証明書を発行させることができます。

4.1.1 Certbot コマンド例：

```
certbot certonly --standalone --register-unsafely-without-email --non-interactive --force-renewal --config-dir /opt/digicert/certificate --key-type rsa --server https://one.digicert.com/mpki/api/v1/acme/v2/directory?action=renew&orderId=123456789 --eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com,test2.example.com
```

4.1.2 certonly サブコマンド・オプション

サブコマンド	説明
certonly	証明書を発行します。

必須	オプション	設定値	説明
○	--standalone	なし	スタンドアロン Web サーバーを使用してサーバー証明書を取得します。
×	--register-unsafely-without-email	なし	メールアドレスの登録を不要にします。
×	--non-interactive	なし	ユーザー入力を一切求めずに非対話で実行します。
○	--domain	FQDN	証明書を取得する FQDN を指定します。 「-domain」オプションを複数指定するか、FQDN のカンマ区切りのリストを指定することでマルチドメイン証明書が発行できます。
○	--eab-kid	EAB_KID	外部アカウントバインディングのキー識別子を指定します
○	--eab-hmac-key	EAB_HMAC_KEY	外部アカウントバインディングの HMAC 鍵を指定します
○	--server	ACME Directory Resource URI	申請先の ACME Directory Resource URI を指定します。

必須	オプション	設定値	説明
×	-force-renewal	なし	要求されたドメインにすでに証明書が存在する場合、有効期限が近いかどうかに関わらず、すぐに更新します。--expand も暗黙的に指定されます。
×	--config-dir	ファイルパス	certbot が使用する設定ディレクトリを指定します。
×	--key-type	アルゴリズム名	「rsa」、「ecdsa」を指定できます。（既定：ecdsa）

※本資料に掲載しているオプションは、一部であり、一例です。certbot コマンドには、他のオプションによる方法もあります。詳細は certbot 公式ドキュメントを参照ください。

4.1.3 --server オプションに追加するクエリ

クエリ	設定値	説明
action	renew	更新を意味する値「renew」を指定します。
orderId	オーダーID	CertCentral で発行されたオーダーID に紐づけます。オーダーID を省略すると、CertCentral が該当するオーダーを自動検出し、紐づけます。

4.1.4 発行完了時

下記メッセージが表示されれば、サーバー証明書の発行は完了です。

```
Successfully received certificate.
```

4.2 サーバー証明書を再発行する

サーバー証明書の有効期限が近づき、同内容のサーバー証明書を発行する場合は、更新ではなく再発行の手続きでサーバー証明書を発行できます。

サーバー証明書を再発行させるケースでは、CertCentral のオーダー番号を指定することで、指定したオーダーに紐づけてサーバー証明書を再発行させることができます。

再発行では、同内容の既存のサーバー証明書を失効させずに対応できます。記載事項を変更した場合、既存のサーバー証明書は、失効されるケースがあるため、ご注意ください。

4.2.1 Certbot コマンド例：

```
certbot certonly --standalone --register-unsafely-without-email --non-interactive --force-renewal --config-dir /opt/digicert/certificate --key-type rsa --server https://one.digicert.com/mpki/api/v1/acme/v2/directory?action=reissue&orderId=123456789 --eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com,test2.example.com
```

4.2.2 certonly サブコマンド・オプション

サブコマンド	説明
certonly	証明書を発行します。

必須	オプション	設定値	説明
○	--standalone	なし	スタンドアロン Web サーバーを使用してサーバー証明書を取得します。
×	--register-unsafely-without-email	なし	メールアドレスの登録を不要にします。
×	--non-interactive	なし	ユーザー入力を一切求めずに非対話で実行します。
○	--domain	FQDN	証明書を取得する FQDN を指定します。 「-domain」オプションを複数指定するか、FQDN のカンマ区切りのリストを指定することでマルチドメイン証明書が発行できます。
○	--eab-kid	EAB_KID	外部アカウントバインディングのキー識別子を指定します
○	--eab-hmac-key	EAB_HMAC_KEY	外部アカウントバインディングの HMAC 鍵を指定します
○	--server	ACME Directory Resource URI	申請先の ACME Directory Resource URI を指定します。

必須	オプション	設定値	説明
×	-force-renewal	なし	要求されたドメインにすでに証明書が存在する場合、有効期限が近いかどうかに関わらず、すぐに更新します。--expand も暗黙的に指定されます。
×	--config-dir	ファイルパス	certbot が使用する設定ディレクトリを指定します。
×	--key-type	アルゴリズム名	「rsa」、「ecdsa」を指定できます。（既定：ecdsa）

※本資料に掲載しているオプションは、一部であり、一例です。certbot コマンドには、他のオプションによる方法もあります。詳細は certbot 公式ドキュメントを参照ください。

4.2.3 --server オプションに追加するクエリ

クエリ	設定値	説明
action	reissue	再発行を意味する値「reissue」を指定します。
orderId	オーダーID	CertCentral で発行されたオーダーID に紐づけます。オーダーID を省略すると、CertCentral が該当するオーダーを自動検出し、紐づけます。

4.2.4 発行完了時

下記メッセージが表示されれば、サーバー証明書の発行は完了です。

```
Successfully received certificate.
```

5. 証明書の失効

5.1 サーバー証明書を失効する

必要に応じて、発行したサーバー証明書を失効させます。

サーバー証明書を失効させるケースは、「サーバー証明書が必要ではなくなった」、「サーバー証明書の秘密鍵の危殆化が判明した」などがあります。

Certbot では、失効用のコマンドを発行することで発行されたサーバー証明書を失効させることができます。

5.1.1 Certbot コマンド例：

```
certbot revoke --config-dir /opt/digicert/certificate --server https://one.digicert.com/mpki/api/v1/acme/v2/directory --eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -cert-path /opt/digicert/certificate/test.example.com --reason cessationofoperation
```

5.1.2 revoke サブコマンド・オプション

サブコマンド	説明
revoke	証明書を失効します。

必須	オプション	設定値	説明
○	--server	ACME Directory Resource URI	申請先の ACME Directory Resource URI を指定します。
○	--eab-kid	EAB_KID	外部アカウントバインディングのキー識別子を指定します
○	--eab-hmac-key	EAB_HMAC_KEY	外部アカウントバインディングの HMAC 鍵を指定します
○	--cert-name	証明書コモンネーム	失効させるサーバー証明書のコモンネームを指定します。「--cert-path」と排他利用
○	--cert-path	証明書ファイルパス	失効させるサーバー証明書のファイルパスを指定します。「--cert-name」と排他利用
×	--reason	失効理由	任意（既定：unspecified） 失効理由を指定します。 unspecified keycompromise affiliationchanged supersededs cessationofoperation

必須	オプション	設定値	説明
×	--config-dir	ファイルパス	certbot が使用する設定ディレクトリを指定します。

※本資料に掲載しているオプションは、一部であり、一例です。certbot コマンドには、他のオプションによる方法もあります。詳細は certbot 公式ドキュメントを参照ください。

5.1.3 失効完了時

下記メッセージが表示されれば、サーバー証明書の失効は完了です。

```
You have successfully revoked the certificate that was located at ファイルパス.
```

6. ジョブ管理システムを利用した運用例

6.1 Linux cron を利用した自動運用

Linux 標準で利用可能な cron を利用した自動運用について説明します。

6.1.1 cron 編集コマンド呼び出し：

```
crontab -e
```

6.1.2 cron 編集内容：

```
[minute] [hour] [day] [month] [day of week] [command]
```

項番	項目	説明
1	minute	実行する分を 0-59 までの任意の整数で指定します
2	hour	実行する時間を 0-23 までの任意の整数で指定します
3	day	実行する日を 1-31 までの任意の整数で指定します
4	month	実行する月を 1-12 までの任意の整数で指定します
5	day of week	実行する曜日を 0-7 までの任意の整数で指定します（0 と 7 は日曜日） 0=日，1=月，2=火，3=水，4=木，5=金，6=土，7=日 または、曜日を表す英語名でも指定可能です sun，mon，tue，wed，thu，fri，sat
6	command	実行するコマンドを指定します

項番	項目	説明
1	アスタリスク(/*)	すべての有効な値を指定できます。 [day]にアスタリスク(*)を指定すると毎日実行されます
2	ハイフン(-)	範囲を指定します。 1-3 の場合、1,2,3 を指定ことになります。
3	カンマ(,)	一覧を指定します。指定した整数すべてが対象となります。 1,4,7 の場合、指定した３つの整数を指定したことになります。
4	スラッシュ(/)	ステップ値を指定します。範囲の後に「/」がある場合、その範囲で指定した整数値をスキップします。[minute]で 0-59/3 の場合、0-59 分の間で 3 分ごとに実行されます。
5	ハッシュ記号(#)	コメント行

6.1.3 cron 設定例：

毎月１日午前２時３０分頃に実行する。

```
# [minute] [hour] [day] [month] [day of week] [command]

30 2 1 * * /cert-renewal.sh > /dev/null
```

6.1.3.1 cert-renewal.sh：

```
#!/bin/sh

/usr/bin/certbot certonly --standalone --register-unsafely-without-email --non-interactive --force-renewal --config-dir /opt/digicert/certificate --key-type rsa --server https://one.digicert.com/mpki/api/v1/acme/v2/directory?action=renew&orderId=123456789 --eab-kid AAAAAAAAAAA --eab-hmac-key AAAAAAAAAA -d test1.example.com,test2.example.com
```

7. 参考情報

7.1 Certbot 公式

https://certbot.eff.org/

7.2 Certbot 公式 (ユーザーガイド)

https://eff-certbot.readthedocs.io/en/latest/using.html

7.3 RFC8555 Automatic Certificate Management Environment (ACME)

https://datatracker.ietf.org/doc/html/rfc8555/

7.4 CertCentral

https://www.digicert.com/secure/

7.5 CertCentral Documentation

https://docs.digicert.com/en/certcentral.html