



【CertCentral Enterprise利用者向け解説資料】

CertCentral API 活用ガイド

最終更新日：2021年2月8日
デジサート・ジャパン合同会社

目次

1. はじめに	: page 3
2. APIキーの作成・管理	: page 6
3. 事前認証(組織およびドメイン名の管理)	: page 11
3.1 ワークフロー	: page 11
3.2 ドメイン名の事前認証と管理	: page 13
4. サーバ証明書(OV/EV)の申請	: page 29
5. オーダー管理、リクエスト管理	: page 41
5.1 (共通)オーダー管理	: page 41
5.2 リクエスト管理	: page 49
6. 発行された証明書の取得	: page 55
7. 再発行、複製、失効等の証明書管理	: page 62
8. プラン・証明書の有効期間・更新案内メールについて	: page 72

1. はじめに

はじめに

- 当資料は CertCentral Enterpriseに付随する API機能(以下「CertCentral API」または「API」)を活用してデジサートのSSL/TLSサーバ証明書を申請、発行および管理（再発行、失効等を含む）いただくためのガイダンスを提供する簡易マニュアルです
- CertCentral Enterpriseのご活用方法の全体像については、以下の文書を併せて参照ください
 - CertCentral Enterprise利用ガイド(コンソール編)
 - URL : https://www.digicert.co.jp/enterprise/certcentral/pdf/certcentral_simple_manual.pdf
 - DigiCert Docs (CertCentral各種機能の詳細マニュアル)
 - URL : <https://docs.digicert.com/ja/> (日本語版) または <https://docs.digicert.com/> (英語版)
- CertCentral APIの詳細機能については、以下の文書を併せて参照ください
 - DigiCert Developer documentation (CertCentral API技術仕様書)
 - URL : <https://dev.digicert.com/ja/> (日本語版) または <https://dev.digicert.com/> (英語版)
- 当版では特に以下のシナリオを中心として解説いたします。
 - OV(企業認証)証明書およびEV(Extended Validation)証明書を対象とする
 - **「事前認証」方式を中心に扱う**
「事前認証」方式とは：個々の証明書申請に先立ってお客様のCertCentral Enterpriseアカウント内に組織情報およびドメイン名を登録し、認証を完了させる方式を指します。認証履歴の有効期間内は(およそ1年間)はこれを再利用することで、個別の証明書の申請から発行までのリードタイムを短縮することが可能です

変更履歴

Ver.	公開日	変更点	変更箇所
~0.9	2020/7/2	省略	-
1.0	2021/2/8	[1.はじめに]「変更履歴」ページを追加	Page 5
		[2. APIキーの作成・管理]セクション追加、これに伴いセクション番号を見直し	Page 6-10
		[3. 事前認証(組織およびドメイン名の管理)] DCVメール(日本語)のタイトル、文面変更を反映など、多数改訂	Page 11-28
		[4. サーバ証明書(OV/EV)の申請]「複数年プラン」申請方法を追記など、多数改訂	Page 29-40
		[5. オーダー管理、リクエスト管理] オーダーステータス状態遷移など説明を詳細化など、多数改訂	Page 41-54
		[6. 発行された証明書の取得] 証明書ファイル形式の詳細を追記など、多数改訂	Page 55-61
		[7. 再発行、複製、失効等の証明書管理]「複数年プラン」再発行申請方法等を追記など、多数改訂	Page 62-71
		[8. プラン・証明書の有効期間、更新案内メールについて]「複数年プラン」について追記など、多数改訂	Page 72-76

2. APIキーの作成・管理

CertCentral APIの概要と「APIキー」

1

RESTful形式のサービスAPIによる柔軟なシステム連携を実現 ※1

・Method: GET POST PUT DELETE

・EndPoint (Base URL): `https://www.digicert.com/services/v2`

・Content-Type: 主にJSON形式

1. Application/json
2. Application/zip
3. Application/xml
4. Image/jpeg(または/png)

・配下で参照/操作可能な
オブジェクト(例)

- ・オーダー(注文単位)
- ・証明書
- ・リクエスト(申請承認リクエスト、失効承認リクエストなど)
- ・組織(Organization)
- ・ドメイン名 など他多数

2

APIキー認証と補完的セキュリティ機能により、利便性と安全性を両立 ※2

・APIキーによるHTTPヘッダベース認証

・CertCentralのユーザ管理の一機能として
コンソール内でAPIキー管理機能を提供

```
curl -X GET \  
  'https://www.digicert.com/services/v2/user' \  
  -H 'Content-Type: application/xml' \  
  -H 'X-DC-DEVKEY: {{api_key}}'
```

・IPアドレス制限の付与により
APIアクセスのセキュリティ強化

IP 制限

セキュリティ強化のため、DigiCertは特定のIPアドレスから

IPアドレスの制限

オン オフ

※1 : もっと詳しく : <https://dev.digicert.com/services-api/>

※2 : もっと詳しく : <https://dev.digicert.com/authentication/>

APIキー管理の概要

■「APIキー」管理画面へのアクセス

トップ画面

ルート1
(全てのユーザー)

プロフィール設定画面

ルート1の場合、自身のユーザーアカウント用のAPIキーのみを管理できます

トップ画面

ルート2
(管理者専用)

ルート2の場合、アカウント内の全てのユーザーのAPIキーを管理できます

APIキー管理画面

説明	ユーザー	ステータス	追加された日付	
Discovery Access Key	Taro Shinsei	Active	07 Dec 2020	失効する
api key 01	Taro Shinsei	Active	21 May 2020	失効する
api key 02	Taro Shinsei	Active	01 May 2020	失効する

APIキーの追加(作成)・確認

■「APIキー」管理画面

API キー

API ドキュメント

+ API キーを追加

ステータス ユーザー 検索

フィルター未設定 フィルター未設定 検索文字を入力 検索

説明	ユーザー	ステータス
Discovery Access Key	Taro Shinsei	Active
api key 01	Taro Shinsei	Active
api key 02	Taro Shinsei	Active

01 May 2020 失効する

■APIキー追加(作成)時の入力/選択項目

#	項目名	説明	入力/選択例
1	説明	APIキーの名称	「api_key_01」
2	ユーザー	APIキーをアサインするユーザーを選択(管理者以外は自身のみ選択可能)	プルダウンから選択
3	APIキー制限	APIキーの権限をさらに細分化して管理(制限)	<p>「なし」: 全ての操作が可能</p> <p>「Orders」: 以下の操作が可能 <オーダー>、<リクエスト> および<証明書></p> <p>「Orders, Domains, Organizations」: 以下の操作が可能 <オーダー>、<リクエスト>、 <証明書>、<組織>および <ドメイン></p> <p>「View Only」: 参照(GET)のみ可能</p>

キャンセル API キーを追加

追加(作成)したAPIキーの値は「1度だけ」表示されます。適切に保管してください。

新しいAPIキー

テキストをクリックしてコピー

<APIキー>

セキュリティ上の理由から、APIキーを再度表示することはできません。

私は、再びAPIキーを見ることができないことを理解しました

APIキーの更新・無効化

■「APIキー」管理画面

The screenshot shows the 'API キー' management page. On the left, there's a sidebar with 'API キー' and 'API キーを追加'. Below it are filters for 'ステータス' and 'ユーザー'. The main area displays a table of API keys:

説明	ユーザー	ステータス	追加された日付
api_key_03 ⓘ	Taro Shinsei	Active	06 Jan 2021
Discovery Access Key	Taro Shinsei	Active	07 Dec 2020
api key 01	Taro Shinsei	Active	21 May 2020
api key 02	Taro Shinsei	Active	01 May 2020

A modal window titled 'API キーを更新する' is open, showing the update form for 'api_key_03'. The form includes a '説明' field with 'api_key_03', an 'API キー制限 (オプション)' dropdown set to 'View Only', and a 'キャンセル' button. A red arrow points from the 'api_key_03 ⓘ' in the table to the modal.

■APIキー更新時の入力/選択項目

#	項目名	説明	入力/選択例
1	説明	APIキーの名称	「api_key_01」
2	APIキー制限	APIキーの権限をさらに細分化して管理(制限)します	「なし」 : 全ての操作が可能 「Orders」 : 以下の操作が可能 <オーダー>、<リクエスト> および<証明書> 「Orders, Domains, Organizations」 : 以下の操作が可能 <オーダー>、<リクエスト>、 <証明書>、<組織>および <ドメイン> 「View Only」 : 参照(GET)のみ可能

※ APIキーをアサインするユーザー、APIキーの値を更新することは出来ません。

APIキーの名称、APIキー制限は適宜更新することができます。

APIキーが不要になった場合は「失効する」を押下して該当のAPIキーを無効化してください



The modal dialog is titled 'API キーを取り消す'. It contains the text: 'API キー "api_key_03" を Taro Shinsei に対して完全に無効にしてもよろしいですか?'. At the bottom, there are two buttons: 'キャンセル' and '失効する'.

3. 事前認証（組織およびドメイン名の管理）

～ 3.1 ワークフロー ～

製品カテゴリー別 ワークフロー

■ ワークフロー概要

・CertCentral Enterpriseでどのような種類の証明書(例:セキュア・サーバIDの場合は「OV(企業認証)のSSL/TLSサーバ証明書」)を申請・発行されるかに拠って、「事前認証」の手順が異なります。以下のチャートを参考に、必要な「事前認証」の範囲を確認してください

製品カテゴリー	SSL/TLSサーバ証明書			コードサインング証明書	
	OV (企業認証)	EV (Extended Validation)	Private SSL (プライベートSSL)	CS (企業認証)	EVCS (Extended Validation)
具体的な製品名の例	セキュア・サーバID	セキュア・サーバID EV	Private SSL OV	コードサインング証明書	EVコードサインング証明書

「組織」の事前認証	組織 (Organization) の事前認証	必要 →CCE利用ガイド(コンソール編)(*1)セクション2.2「組織の事前認証」参照				当文書の対象外
	認証済連絡先 (Verified Contact) の事前認証	不要	必要 → CCE利用ガイド(コンソール編)(*1)セクション2.3 「認証済連絡先」参照	不要	必要 → CCE利用ガイド(コンソール編)(*1)セクション2.3 「認証済連絡先」参照	必要 → CCE利用ガイド(コンソール編)(*1)セクション2.3 「認証済連絡先」参照
ドメインの事前認証	ドメイン名 の事前認証	必要 (DCV方式をメール認証、ファイル認証、DNS認証から選択) →当文書セクション2.2			当文書の対象	不要

*1 : CertCentral Enterprise利用ガイド (コンソール編)

URL : https://www.digicert.co.jp/enterprise/certcentral/pdf/certcentral_simple_manual.pdf

3. 事前認証（組織およびドメイン名の管理）

～ 3.2 ドメイン名の事前認証と管理 ～

Add Domain : ドメイン(Domain)の追加登録

cURLのサンプルコード(*1)

```
curl -X POST \
  https://www.digicert.com/services/v2/domain \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "name": "example.com",
    "organization": {
      "id": 112233
    },
    "validations": [
      {
        "type": "ov"
      },
      {
        "type": "ev"
      }
    ],
    "dcv_method": "email"
  }'
```

Method+Endpoint:

POST https://www.digicert.com/services/v2/domain

リクエスト : 主なパラメータ	説明	データタイプ
name	追加登録するドメイン名	String
organization	Organizationオブジェクト	Object
id	ドメイン名の利用権を表明する対象の組織(証明書申請団体)のOrganization ID	Int
validations	認証タイプ(繰り返し)	Object []
type	認証タイプ(OV, EV)を指定	String
dcv_method	ドメインIDで指定したドメイン名に対するDCV方法 <ul style="list-style-type: none"> email :DCVメールをWhois連絡先/規定のアドレスに送信 http-token : 認証コードを含むファイルをウェブサーバ上に公開 dns-txt-token : DNSのTXTレコードに認証コードを指定 dns-cname-token : DNSのCNAMEレコードに認証コードを指定 	String

もっと詳しく: <https://dev.digicert.com/services-api/domains/add-domain/>

cURLのサンプルコード(*1)

「メール認証(email)」を選択した場合のレスポンス例

```

{
  "id": 123356,
  "validation_emails": {
    "name_scope": "example.com",
    "base_emails": [
      "postmaster@example.com",
      "administrator@example.com",
      "hostmaster@example.com",
      "admin@example.com",
      "webmaster@example.com"
    ],
    "whois_emails": [
      "it@example.com"
    ]
  }
}

```

レスポンス :	説明	データタイプ
id	追加登録したドメイン名に紐づく Domain ID	Int
validation_emails		String
name_scope	ドメインIDに紐づくドメイン名(FQDN)	String
base_emails	「規定ホスト名@確認対象のドメイン名」で構成されるメールアドレス	Object
whois_emails	WHOISに掲載のアドレス	String

もっと詳しく: <https://dev.digicert.com/services-api/domains/add-domain/>

cURLのサンプルコード(*1)

「ファイル認証(http-token)」を選択した場合のレスポンス例

```

1 {
2   "id": 1863015,
3   "dcv_token": {
4     "token": "1ldr959m7p6f11s06k9z23b13szpss7h",
5     "expiration_date": "2020-07-31T18:22:13+00:00",
6     "http_token_url": "http://example.net/.well-known/pki-validation/fileauth.txt"
7   }
8 }

```

「DNS TXT認証(dns-txt-token)」を選択した場合のレスポンス例

```

1 {
2   "id": 1863017,
3   "dcv_token": {
4     "token": "b3x590nrq9d8j02bdpjr9z11s21zxnn1",
5     "expiration_date": "2020-07-31T18:24:34+00:00"
6   }
7 }

```

レスポンス :	説明	データタイプ
id	追加登録したドメイン名に紐づく Domain ID	Int
dcv_token		String
token	(ファイル認証/DNS認証の場合) : 認証トークンの値	String
expiration_date	認証トークンの有効期限 (通常30日間)	String
http_token_url	ファイル認証の場合 : 認証トークンを含むファイルを配置するURL	String

※ 当ページに記載されているトークンはサンプルであり、実際にはご利用いただけませんのでご注意ください
 認証トークンの有効期間は30日間となります。一度使用した認証トークンは再利用できません。

もっと詳しく: <https://dev.digicert.com/services-api/domains/add-domain/>

ドメイン名利用権確認(DCV) – CertCentralで利用可能な方式

- ・パブリックSSL/TLSサーバ証明書を発行するためには、認証プロセスの一環として、SSL/TLSサーバ証明書の申請者または申請団体が証明書を発行する対象のドメイン名に対する所有権／管理権限を持つことを確認する必要があります。この確認のためのプロセスを「ドメイン名利用権確認(DCV)」と呼びます。
- ・CA/ブラウザフォーラムの「Baseline Requirement(パブリックSSL/TLSサーバ証明書のための要件を定めた業界基準)」で認められた複数のDCVの方式のうち、CertCentralでは以下の4種類の方式をサポートしています。
- ・CertCentralではDCVを実施するタイミングとして、証明書申請に先立ってアカウント内でドメイン名を登録し有効期間内は証明書申請に繰り返し再利用可能な状態とする「事前認証」方式(OV/EV証明書のみ対応)、ならびに各証明書申請のタイミングでDCVを実施する「都度認証」方式をサポートしています。
- ・ドメイン名の所有者とSSL/TLSサーバ証明書の申請団体が同一の組織である場合にもDCVが必要となります。
- ・いずれの方式にもご対応いただけない場合は、SSL/TLSサーバ証明書を発行することができませんのでご理解・ご了承ください

DCV方式	dcv_method	内容
メール認証	email	<p>規定のメールアドレス宛に送信されるDCVメールをドメイン名所有者が受信のうえ承認操作をいただくことでドメイン名利用権を確認する方式です。</p> <ul style="list-style-type: none"> ■宛先：WHOISに掲載のアドレスおよび「規定ホスト名@確認対象のドメイン名」で構成されるメールアドレス (詳細は後述) ■件名：[Domain Approval] ドメイン名の利用権確認のお願い: [確認対象のドメイン名] ■送信元アドレス：no-reply@digitalcertvalidation.com
ファイル認証	http-token	<p>CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをインターネット経由でアクセス可能なウェブサーバ上の規定の場所にアップロードしていただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。</p> <ul style="list-style-type: none"> ■設置場所：<a href="http://<確認対象のドメイン名>/.well-known/pki-validation/fileauth.txt">http://<確認対象のドメイン名>/.well-known/pki-validation/fileauth.txt
DNS TXT認証	dns-txt-token	<p>CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをDNS TXTリソースレコードとして登録・公開していただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。</p> <ul style="list-style-type: none"> ■設置例：<確認対象のドメイン名> TXT <認証トークン>
DNS CNAME認証	dns-cname-token	<p>CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをDNS CNAMEリソースレコードとして登録・公開していただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。</p> <ul style="list-style-type: none"> ■設置例：<認証トークン>.<確認対象のドメイン名> CNAME dcv.digicert.com

各DCV方式の詳細 – 「メール認証」の場合 (1/2)

■(「事前認証」の場合)DCVメールの送信先

例1: 登録/認証申請ドメイン名=「example.com」の場合

→DCVメールの配信先は常に右の通りとなります。



区分	DCVメール送信先
WHOIS (WHOIS-based Email)	1.WHOISに掲載されたメールアドレス
規定ホスト名 (Constructed Email)	2. admin@example.com 3. administrator@example.com 4. hostmaster@example.com 5. postmaster@example.com 6. webmaster@example.com

例2: 登録/認証申請ドメイン名=「sub01.example.com」の場合

→DCVメールのデフォルトの配信先は常に右の通りとなります。



区分	DCVメール送信先
WHOIS (WHOIS-based Email)	1.WHOISに掲載されたメールアドレス
規定ホスト名 (Constructed Email)	2. admin@sub01.example.com 3. administrator@sub01.example.com 4. hostmaster@sub01.example.com 5. postmaster@sub01.example.com 6. webmaster@sub01.example.com

■(参考)事前に利用可能なメールアドレス(DCVメール送信先)を確認する方法

Domain emailsのレスポンスから、ドメイン名毎に利用可能なメールアドレス(DCVメール送信先)を事前にご確認いただくことが可能です。

Domain emails: DCVメール送信先アドレス取得



[Page 27 参照](#)

各DCV方式の詳細 – 「メール認証」の場合 (2/2)

■ DCVメール(OV/EV証明書)の概要

→メール件名、送信元および本文イメージは、以下のようになります

件名	[Domain Approval] ドメイン名の利用権確認のお願い: [確認対象のドメイン名]
送信元	no-reply@digitalcertvalidation.com
本文イメージ (抜粋)	<p>DigiCert では、DigiCert SSL/TLSサーバ証明書、S/MIME証明書等デジタル証明書の発行前に必要となるドメイン名利用権の確認を実施しております。ご担当者様が、ドメイン名 [確認対象のドメイン名(※1)] の所有者または管理者であることを確認いただいた上で、SSL/TLSサーバ証明書、またはS/MIME証明書に当該ドメイン名を利用することをご承認ください。</p> <p>下記URLにアクセスしウェブページ上の内容をよくお読みになり、「承認する」のボタンをクリックしてください。(当ウェブページへのリンクの有効期間は30日間です。)</p> <p><a href="https://www.digicert.com/link/dcv-approve/?t=<ランダムな認証トークン(※2)>">https://www.digicert.com/link/dcv-approve/?t=<ランダムな認証トークン(※2)></p> <p style="text-align: center;">↑Click</p>

■ DCV承認画面(OV/EV証明書)イメージ

→DCV承認画面(日本語)のイメージは以下のようになります(※1)

ドメイン名利用権の確認(SSL/TLSサーバ証明書, S/MIME用クライアント証明書)

DigiCertでは、ドメイン名 [確認対象のドメイン名] に対するSSL/TLSサーバ証明書、またはS/MIME用クライアント証明書の発行前に必要となるドメイン名利用権の確認を実施しております。ご担当者様が当該ドメイン名の所有者または管理者であることをご確認いただいた上で、SSL/TLSサーバ証明書、またはS/MIME証明書に当該ドメイン名を利用することを承認いただく場合は、下記のドメイン名利用内容をよくお読みになり、「承認する」ボタンをクリックしてください。ご担当者様の承認をもって、[確認対象のドメイン名] に対するSSL/TLSサーバ証明書、またはS/MIME証明書の発行を可能といたします。

ドメイン名利用内容の詳細

ドメイン名 [確認対象のドメイン名]

申請団体 [確認対象のドメイン名]

ご承認いただく内容

私は、当該ドメイン名の所有者または管理者であることを表明します。デジサートが、末尾に [確認対象のドメイン名] が付くドメイン名(FQDN)のウェブサイトに対しSSL/TLSサーバ証明書を発行すること、または当該ドメインメールアドレスに対してS/MIME用クライアント証明書を発行することに同意します。

- [確認対象のドメイン名] が、申請団体 [確認対象のドメイン名] を代表してこのドメイン名のSSL/TLSサーバ証明書を申請する権限、またはS/MIME用クライアント証明書を当該ドメインメールアドレスに発行する権限を持つことを認めます。
- 申請団体 [確認対象のドメイン名] が、当該ドメイン名ならびにそのサブドメインのSSL/TLSサーバ証明書を取得し使用する権限、または当該ドメインならびにサブドメインのメールアドレス向けにS/MIME用クライアント証明書を取得し使用する権限があることを認めます。
- DigiCertは、[確認対象のドメイン名] が要求するSSL/TLSサーバ証明書に関する以降の発行要求(新規、更新申請を含む)、またはS/MIME用クライアント証明書に関する同様の発行要求に、2801 North Thanksgiving Way, Suite 500, Lehi UT, 84043 USAを住所とするDigiCertの法務部門宛に送付された書面によってこの承認が取り消されるまでの間、この承認内容を適用できるものとします。
- 万が一この承認内容を取り消す場合、または当該ドメイン名を第三者に譲渡する場合はDigiCertに速やかに報告します。
- DigiCertは、ドメイン管理者様宛に送信された再確認メールに関する再確認を定期的実施することがあります。

承認する

万が一この申請に誤りがある場合、またはこの申請を承認し

※1: 承認画面の表示言語は画面上部の「言語」欄から選択いただき切り替えることが可能です。
 ※2: 認証トークンの有効期間は30日間となります。一度使用した認証トークンは再利用できません。
 DCVメールを紛失した場合はCertCentralから再送いただくことが可能です。

各DCV方式の詳細 – 「ファイル認証」の場合

■ファイル認証用「認証トークン」の取得・利用方法 (OV/EV証明書の場合)

OSTEP 1: ドメイン名の登録(Add Domain)時のパラメータ「DCV検証方法(dcv_method)」に「ファイル認証(http-token)」を指定します

POST `https://www.digicert.com/services/v2/domain`



```
"dcv_method": "http-token"
```

OSTEP 2: 認証トークンの入手

Add Domainのレスポンスから、またはDomain Info、Change DCV Methodなど適切なエンドポイントを利用して認証トークンを取得します。

ドメイン名をキーとする照会(Domain Info)のレスポンスで認証トークン取得

[Page 23-24 参照](#)

DCV方式の「変更」(Change DCV method)と同時に認証トークン取得

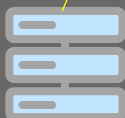
[Page 25 参照](#)

```
"dcv_token": {
  "token": "xqxm71sgry65ssw2sw8pkgnv3b1j313g",
```

OSTEP 3: 認証トークンファイルの配置

認証トークンの値を含む「fileauth.txt」という名称のファイル(認証トークンファイル)を作成し、インターネット経由でアクセス可能なウェブサーバ上の規定の場所に認証トークンファイルを配置し、公開します。

配置URL = `http://<登録・認証対象のドメイン名(※1)>/.well-known/pki-validation/fileauth.txt`



取得した
認証トークン

※1: 例: 登録・認証対象のドメイン名 = `example.com`の場合、配置URLは以下となります
→配置URL = `http://example.com/.well-known/pki-validation/fileauth.txt`

OSTEP 4: 認証トークンファイルのチェック

Check DCV(OV/EV)エンドポイントを利用して、デジサートが規定の場所に正しく認証トークンファイルが配置されているか確認します。成功すると、DCVプロセスは完了です。

Check DCV: 即時ポーリング実行呼出し

[Page 26 参照](#)

各DCV方式の詳細 – DNS認証 (TXTリソースレコードを利用) の場合

■ DNS TXT認証用「認証トークン」の取得・利用方法 (OV/EV証明書の場合)

OSTEP 1: ドメイン名の登録(Add Domain)時のパラメータ「DCV検証方法(dcv_method)」に「DNS TXT認証(dns-txt-token)」を指定します

POST `https://www.digicert.com/services/v2/domain`

`"dcv_method": "dns-txt-token"`

OSTEP 3: 認証トークンの配置

認証トークンを値(Value)として、確認対象のドメイン名のDNS TXTリソースレコードを設定します。

	NAME	TYPE	VALUE
	<登録・認証対象のドメイン名>	TXT	取得した認証トークン

OSTEP 2: 認証トークンの入手

Domain Info、Change DCV Methodなど適切なエンドポイントを利用して認証トークンを取得します。

ドメイン名をキーとする照会(Domain Info)のレスポンスで認証トークン取得

[Page 23-24 参照](#)

DCV方式の「変更」(Change DCV method)と同時に認証トークン取得

[Page 25 参照](#)

```
"dcv_token": {
  "token": "xqxm71sgry65ssw2sw8pkgnv3b1j313g",
```

OSTEP 4: 認証トークンのチェック

Check DCV(OV/EV)エンドポイントを利用して、デジサートが規定の方法でTXTリソースレコードに認証トークンが正しく設定されているか確認します。成功すると、DCVプロセスは完了です。

Check DCV : 即時ポーリング実行呼出し

[Page 26 参照](#)

各DCV方式の詳細 – DNS認証 (CNAMEリソースレコードを利用) の場合

■ DNS CNAME認証用「認証トークン」の取得・利用方法 (OV/EV証明書の場合)

OSTEP 1: ドメイン名の登録(Add Domain)時のパラメータ「DCV検証方法(dcv_method)」に「DNS CNAME認証(dns-cname-token)」を指定します

POST `https://www.digicert.com/services/v2/domain`



```
"dcv_method": "dns-cname-token"
```

OSTEP 3: 認証トークンの配置

認証トークン情報と確認対象のドメイン名を".(ドット)"で連結してDNS CNAMEリソースレコードを作成します。値(Value)には「dcv.digicert.com」を設定します

NAME	TYPE	VALUE
取得した認証トークン.<登録・認証対象のドメイン名>	CNAME	dcv.digicert.com

OSTEP 2: 認証トークンの入手

Domain Info、Change DCV Methodなど適切なエンドポイントを利用して認証トークンを取得します。

ドメイン名をキーとする照会(Domain Info)のレスポンスで認証トークン取得

→ [Page 23-24 参照](#)

DCV方式の「変更」(Change DCV method)と同時に認証トークン取得

→ [Page 25 参照](#)

```
"dcv_token": {
  "token": "xqxm71sgry65ssw2sw8pkgnv3b1j313g",
```

OSTEP 4: 認証トークンのチェック

Check DCV(OV/EV)エンドポイントを利用してデジサートが規定の方法でCNAMEリソースレコードに認証トークンが設定されているか確認します。成功すると、DCVプロセスは完了です

Check DCV : 即時ポーリング実行呼出し

→ [Page 26 参照](#)

Domain Info : ドメイン名情報確認、認証トークンの確認

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}'
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

GET https://www.digicert.com/services/v2/domain/{{domain_id}}

● 200 OK

```
{
  "id": 738687,
  "is_active": true,
  "status": "approved",
  "name": "appfw.net",
  "date_created": "2019-08-30T02:25:08+00:00",
  "organization": {
    "id": 754781,
    "status": "active",
    "name": "Win The Customer, LLC",
    "display_name": "Win The Customer, LLC",
    "is_active": "1"
  },
  "container": {
    "id": 129626,
    "name": "Win The Customer, LLC"
  }
}
```

- ・API Endpointとして指定するURLのうち上記部分にはDomain IDを指定してください。
- ・Domain IDは、以下のようなタイミングでアカウント内で登録されたドメイン名に対して割り振られます。
 - ・明示的にドメイン名を事前登録したタイミング
 - ・(その時点で未登録の新しい)ドメイン名でOV/EV証明書を申請したタイミング
- ・OV/EV証明書のオーダに紐づくドメイン名のdomain_idは、「Validation status」でのレスポンス「dns_name_validations」オブジェクト内の「domain_id」にてご確認いただけます(詳細は別頁)

レスポンス :	説明	データタイプ
status	ドメイン名のステータス (approved, pending)	String
name	ドメインIDに紐づくドメイン名(FQDN)	String
organization	ドメイン名の利用権が確認された(紐づけられた)対象の組織(Org)	Object
id	組織(Org)のID	int
container	ドメイン名が登録された管理グループ	Object
id	管理グループのID	int

もっと詳しく: <https://dev.digicert.com/services-api/domains/domain-info/>

Domain Info : ドメイン名情報確認、認証トークンの確認 (続き)

Domain Info呼出し時に、エンドポイントにパラメータ(“?”以降の文字列)を追記いただくことで、レスポンスデータに追加情報を含めて取得いただくことが可能です。

`include_dcv=true` : 認証トークン(ファイル/DNS認証用)情報

`include_validation=true` : 認証カテゴリ(EV, OVなど)ごとの認証ステータス情報

■ リクエスト例 : パラメータを指定した場合

`https://www.digicert.com/services/v2/domain/{{domain_id}}?include_dcv=true&include_validation=true`

① 認証トークン情報を「含める」と指定

② 認証カテゴリ(EV, OVなど)ごとの認証ステータス情報を「含める」と指定

■ dcv_token (①の指定によって追加される情報) の項目説明

レスポンス :	説明	データタイプ
<code>dcv_token</code>	ドメイン名利用権確認(DCV)オブジェクト	Object
<code>token</code>	認証トークン(ファイル/DNS認証用)の値	String
<code>status</code>	DCVのステータス。例 : 「pending」	String
<code>http_token_url</code>	ファイル認証の場合 : 認証トークンファイルを配置するURL	String

「認証用のファイル配置」の方法



認証トークン

以下URLでインターネットでアクセスできる状態で、発行された認証トークン(レスポンス中の“token”の値)を含む.txtファイルを配置し、公開してください。

`http://<証明書を申請したFQDN>/.well-known/pki-validation/fileauth.txt`

```
{
  "id": 1408596,
  "is_active": true,
  "status": "pending",
  "name": "digicertdemo3.com",
  "date_created": "2020-03-18T11:01:56+00:00",
  "organization": {
    "id": 847307,
    "status": "active",
    "name": "TEST ORG 20200318-3",
    "display_name": "TEST ORG 20200318-3",
    "is_active": "1"
  },
  "validations": [
    {
      "type": "ov",
      "name": "OV",
      "description": "Normal Organization Validation",
      "status": "pending",
      "dcv_status": "pending"
    },
    {
      "type": "ev",
      "name": "EV",
      "description": "Extended Organization Validation (EV)",
      "status": "pending",
      "dcv_status": "pending"
    }
  ],
  "dcv_method": "http-token",
  "dcv_token": {
    "token": "bx4b8g341q85w84b56kspzxpwr366wd9",
    "status": "pending",
    "http_token_url": "http://www.digicertdemo3.com/.well-known/pki-validation/fileauth.txt"
  },
  "container": {
    "id": 129626,
    "name": "Win The Customer, LLC"
  }
}
```

②の指定によって追加された情報(例)

①の指定によって追加された情報(例)

もっと詳しく: <https://dev.digicert.com/workflows/ov-certificate-lifecycle/>

Change DCV method : DCV方法の変更

cURLのサンプルコード(*1)

```
curl -X PUT \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/method' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "dcv_method": "<dcv_method>"
  }'
```

Method+Endpoint:

PUT https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/method

- API Endpointとして指定するURLのうち上記部分にはDomain IDを指定してください。
- Domain IDは、以下のようなタイミングでアカウント内で登録されたドメイン名に対して割り振られます。
 - 明示的にドメイン名を事前登録したタイミング
 - (その時点で未登録の新しい)ドメイン名でOV/EV証明書を申請したタイミング
- OV/EV証明書のオーダに紐づくドメイン名のdomain_idは、「Validation status」でのレスポンス「dns_name_validations」オブジェクト内の「domain_id」にてご確認いただけます(詳細は別頁)

リクエスト :	説明	データタイプ
dcv_method	ドメインIDで指定したドメイン名に対するDCV方法 <ul style="list-style-type: none"> • email :DCVメールをWhois連絡先/規定のアドレスに送信 • http-token : 認証トークンを含むファイルをウェブサーバ上に公開 • dns-txt-token : DNSのTXTレコードに認証トークンを指定 • dns-cname-token : DNSのCNAMEレコードに認証トークンを指定 	String

もっと詳しく: <https://dev.digicert.com/services-api/domains/change-dcv-method/>

「メール(email)」→「ファイル認証(http-token)」に変更した場合(初回)のレスポンス例

```
{
  "dcv_token": {
    "token": "bx4b8g341q85w84b56kspzprw366wd9",
    "expiration_date": "2020-04-17T17:06:22+00:00",
    "http_token_url": "http://digicertdemo3.com/.well-known/pki-validation/fileauth.txt"
  }
}
```

レスポンス :	説明	データタイプ
token	認証トークン(ファイル/DNS認証用)の値	String
expiration_date	認証トークンの有効期限 (通常30日間)	String
http_token_url	ファイル認証の場合 : 認証トークンファイルを配置するURL	String

Check DCV(OV/EV) : 即時ポーリング実行

cURLのサンプルコード(*1)

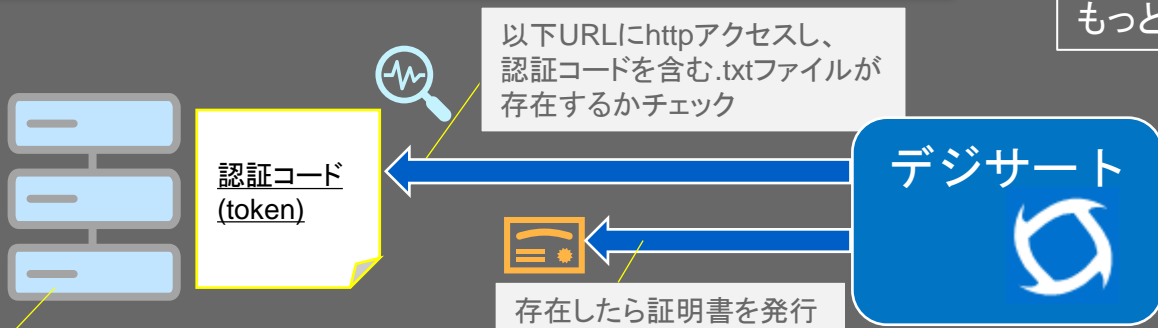
```
curl -X PUT \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/validate-token' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

PUT https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/validate-token

リクエスト : 主なパラメータ	説明	データタイプ
dcv_method	ドメインIDで指定したドメイン名に対するDCV方法を指定 ファイル認証の場合「http-token」を指定	String
token	ポーリング実行を指示する対象の認証コードの値を指定	String

・「認証コード配置済ファイルのポーリング実行」の処理イメージ



もっと詳しく: <https://dev.digicert.com/services-api/domains/ov-ev-ssl-check-dcv/>

Domain emails : DCVメール送信先アドレス取得

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/emails' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

```
● 200 OK
```

```
{
  "name_scope": "sub.digicert.com",
  "base_emails": [
    "admin@sub.digicert.com",
    "webmaster@sub.digicert.com",
    "postmaster@sub.digicert.com",
    "hostmaster@sub.digicert.com",
    "administrator@sub.digicert.com"
  ],
  "whois_emails": [
    "someguy@digicert.com"
  ]
}
```

Method+Endpoint:

- API Endpointとして指定するURLのうち上記部分にはDomain IDまたはFQDNを指定してください。
- Domain IDは、以下のようなタイミングでアカウント内で登録されたドメイン名に対して割り振られます。
 - 明示的にドメイン名を事前登録したタイミング
 - (その時点で未登録の新しい)ドメイン名でOV/EV証明書を申請したタイミング
- OV/EV証明書のオーダに紐づくドメイン名のdomain_idは、「Validation status」でのレスポンス「dns_name_validations」オブジェクト内の「domain_id」にてご確認いただけます(詳細は別頁)

■シナリオ1 : Domain ID(下記青字部分)を指定して、お客様のアカウントに登録済ドメイン名で利用可能なDCVメール送信先アドレスを取得

```
GET https://www.digicert.com/services/v2/domain/585807/dcv/emails
```

■シナリオ2 : FQDN (下記青字部分)を指定して、利用可能なDCVメール送信先アドレスを取得

```
GET https://www.digicert.com/services/v2/domain/example.com/dcv/emails
```

もっと詳しく: <https://dev.digicert.com/services-api/domains/domain-emails/>

Resend DCV emails : DCVメールの(再)送信

cURLのサンプルコード(*1)

```
curl -X PUT \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/emails' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "name_scope": "sub.example.com"
  }'
```

Method+Endpoint:

PUT https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/emails

- API Endpointとして指定するURLのうち上記部分にはDomain IDを指定してください。
- Domain IDは、以下のようなタイミングでアカウント内で登録されたドメイン名に対して割り振られます。
 - 明示的にドメイン名を事前登録したタイミング
 - (その時点で未登録の新しい)ドメイン名でOV/EV証明書を申請したタイミング
- OV/EV証明書のオーダーに紐づくドメイン名のdomain_idは、「Validation status」でのレスポンス「dns_name_validations」オブジェクト内の「domain_id」にてご確認いただけます(詳細は別頁)

リクエスト: 主なパラメータ	説明	データタイプ
name_scope	(任意) ドメインIDに紐づくドメイン名(FQDN)	String

もっと詳しく: <https://dev.digicert.com/services-api/domains/resend-dcv-email/>

4. サーバ証明書(OV/EV)の申請

サーバ証明書(OV/EV)証明書の申請～発行までの流れ

■ セクション「2.事前認証」の範囲		製品カテゴリ	SSL/TLSサーバ証明書	
			OV(企業認証)	EV(Extended Validation)
	「組織」の事前認証	組織 (Organization)	→CCE利用ガイド(コンソール編)(*1) 参照	
		認証済連絡先 (Verified Contact)	不要	→CCE利用ガイド (コンソール編)(*1) 参照
	ドメインの事前認証	ドメイン名	セクション2.2 参照	
■ 当セクションの範囲	証明書の申請	<ul style="list-style-type: none"> ・製品を選択 ・プランのお申込み(証明書を申請) 		
■ セクション「4.2 リクエスト管理」	申請レビュー・承認	(アカウント単位の設定で省略可) <ul style="list-style-type: none"> ・管理者が申請内容を確認し、承認または却下 		
■ セクション「5 証明書の取得」	証明書の取得	<ul style="list-style-type: none"> ・発行された証明書を形式を指定して取得(APIでGET) 		
■ セクション「6 証明書管理」	証明書管理	<ul style="list-style-type: none"> ・証明書再発行(証明書の更新) ・証明書の失効 		

*1 : CertCentral Enterprise利用ガイド (コンソール編)

OV/EV証明書：プラン/証明書の新規申請

cURLのサンプルコード(*1)

Method+Endpoint:

POST https://www.digicert.com/services/v2/order/certificate/{{product_id}}

・APIエンドポイントのURIのうち上記下線部分には、product_id(製品識別子)を指定します
 →[別紙] product_id(製品識別子)一覧 参照

```
curl -X POST \
https://www.digicert.com/services/v2/order/certificate/ssl_ev_basic \
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}' \
-d '{
  "certificate": {
    "common_name": "example.com",
    "dns_names": [
      "sub.example.com",
      "app.example.com"
    ],
    "csr": "<csr>",
    "signature_hash": "sha256",
    "server_platform": {
      "id": 2
    },
    "cert_validity": {
      "custom_expiration_date": "21 DEC 2021"
    }
  },
  "comments": "Certificate for app server.",
  "container": {
    "id": 334455
  },
  "auto_renew": 1,
  "custom_renewal_message": "Keep this renewed.",
  "organization": {
    "id": 123456,
  },
  "order_validity": {
    "custom_expiration_date": "21 DEC 2024"
  },
  "payment_method": "balance"
}'
```

証明書
(certificate)管理グループ
(container)組織
(organization)

リクエスト： 主なパラメータ	説明	データ タイプ
certificate	certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN) ※ 証明書申請には当パラメータの値が利用されます(CSRの値は使用しない)	String
dns_names	コモンネーム(FQDN)と異なる名称のSANsを追加する場合、併せて指定します SANsの入力数量の上限(デフォルト):250	String[]
csr	CSR(Certificate Signing Request)	String
signature_hash	証明書に対する署名に使用するハッシュアルゴリズム(通常"sha256")	String
server_platform	お客様のサーバープラットフォーム環境を選択し、発行通知メールに添付される証明書ファイル形式を最適化いただけます ※ 発行通知メールの形式は組織の管理者によって指定されます。 CCE簡易マニュアル「5.1 発行された証明書の取得」を参照ください	Int
cert_validity	【複数年プランの場合に指定】 [別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照	-
years/ days/ custom_expiration_date		
container	[別紙] container : id (管理グループ/Division) の確認方法 参照	Object
organization	[別紙] 組織(Org)情報の入力方法 参照	Object
order_validity	【複数年プランの場合に指定】 [別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照	-
years/ days/ custom_expiration_date		
validity_years/ validity_days/ custom_expiration_date	【複数年プランでない場合に指定】 [別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照	-

その他のパラメーターの説明など、もっと詳しく:<https://dev.digicert.com/services-api/orders/order-multi-year-plan/>

[別紙] product_id(製品識別子)一覧

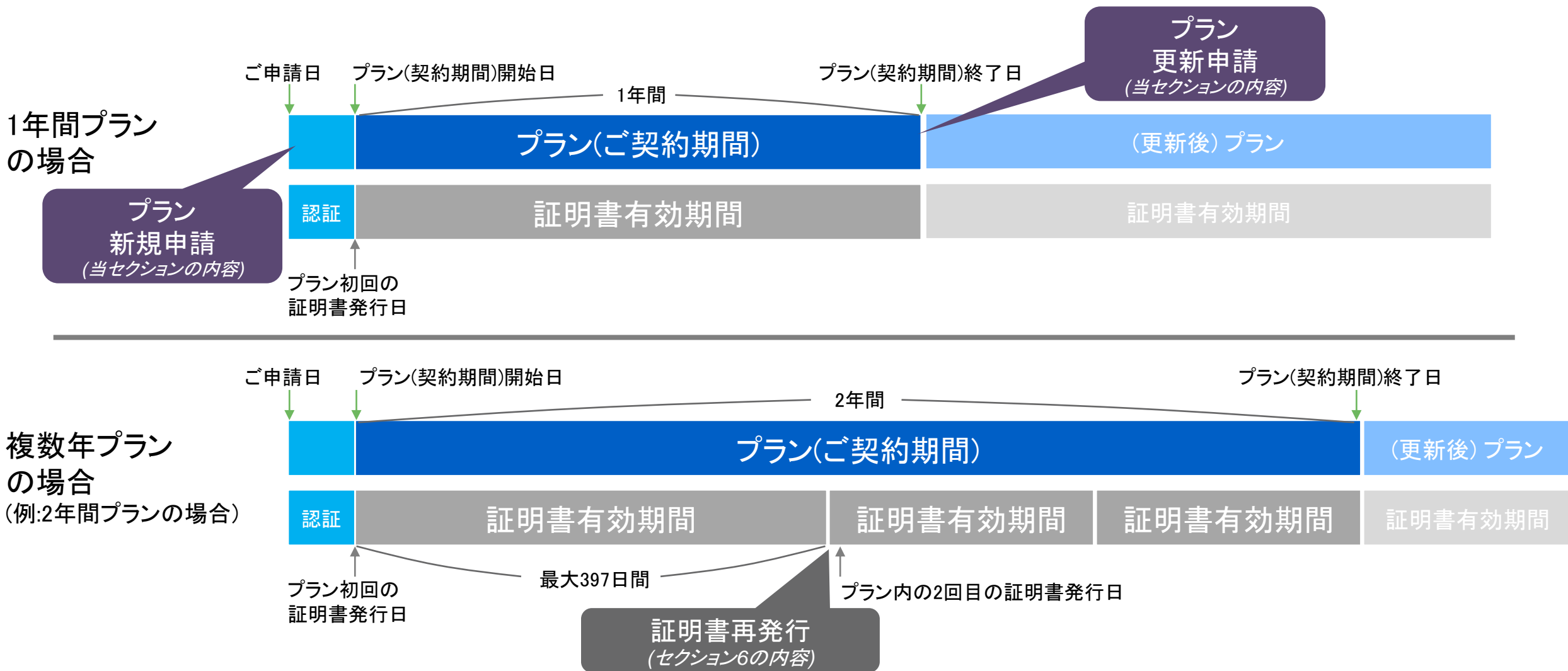
POST https://www.digicert.com/services/v2/order/certificate/{{product_id}}

オーダー系APIエンドポイントをご利用いただく際に、URIの末尾に付与いただくproduct_id(製品識別子)パラメータは、以下表を参考にしてご選択・指定ください

カテゴリー	製品名(日本語名称)	(参考)製品名(英語名称)	product_id (オーダー系エンドポイントに 指定する製品識別子)	備考
Extended Validation (EV)証明書	グローバル・サーバID EV	Secure Site Pro EV SSL	ssl_ev_securesite_pro	
	セキュア・サーバID EV	Secure Site EV	ssl_ev_securesite_flex	
組織認証 (OV)証明書	グローバル・サーバID	Secure Site Pro SSL	ssl_securesite_pro	
	セキュア・サーバID	Secure Site OV	ssl_securesite_flex	
	ジオトラスト トゥルービジネスID	GeoTrust TrueBusiness ID OV	ssl_geotrust_truebizid	
プライベートSSL	プライベート サーバID	Private SSL OV	private_ssl_flex	本文書の対象外
コードサイン証明書	コードサイン証明書	Code Signing Certificate	code_signing	本文書の対象外
	EVコードサイン証明書	EV Code Signing Certificate	code_signing_ev	本文書の対象外

もっと詳しく: <https://dev.digicert.com/glossary/#product-identifiers>

補足 CertCentral Enterprise「複数年プラン」オプション機能のご利用イメージ



[別紙] 複数年プラン(ご契約期間)のリクエストパラメーターについて

契約期間	方式	指定イメージ	指定方法
1年間	旧方式	リクエスト certificate validity_years /validity_days /custom_expiration_date organization	<ul style="list-style-type: none"> ・プラン(ご契約期間)と証明書の有効期間を単一のパラメーターで指定します ・短期的には引き続きご利用いただけますが、今後長期的に「非推奨」扱いとなります。順次新方式への移行をご検討ください。
	新方式	リクエスト certificate cert_validity years /days /custom_expiration_date order_validity years /days /custom_expiration_date validity_years /validity_days /custom_expiration_date organization	<ul style="list-style-type: none"> ・プラン期間と証明書有効期間を異なる複数のパラメーターで指定します <p>○プランの期間:order_validity</p> <ul style="list-style-type: none"> .years : [1~6] 証明書有効期間を年数で指定します。 .days : [1~2190] 証明書有効期間を年数で指定します。 .custom_expiration_date : [dd MMM YYYY形式(例:[09 JUN 2025])] 証明書有効期間終了日を日付形式で指定します。設定する終了日は申請日から起算して2190日以内である必要があります。 <p>○証明書の有効期間:certificate.cert_validity</p> <ul style="list-style-type: none"> .years : [1] 証明書有効期間を年数で指定します。 .days : [1~397] 証明書有効期間を日数で指定します。 .custom_expiration_date : [dd MMM YYYY形式(例:[09 JUN 2021])] 証明書有効期間終了日を日付形式で指定します。設定する終了日は申請日から起算して397日以内である必要があります。
複数年 プラン (2年間 ~6年間)			

[別紙] container : id (管理グループ/Division) の確認方法

- ・container : idはCertCentralのアカウントに紐づけて登録された「管理グループ/Division」に割り振られるIDです。
- ・アカウント開設直後の、追加の管理グループを登録していない状態では、アカウント開設時の組織情報を元に「(親となる)管理グループ」が1つだけ作成されています。
- ・アカウント内の管理グループの一覧および管理グループのIDは以下の通り確認いただけます。

■APIでの管理グループ/Division情報確認方法

Method+Endpoint:

GET <https://www.digicert.com/services/v2/container>

```
{
  "containers": [
    {
      "id": 129626,
      "public_id": <ユニークな値>,
      "name": "Win The Customer, LLC",
      "parent_id": 0,
      "template_id": 5,
      "ekey": <ユニークな値>,
      "has_logo": false,
      "is_active": true
    }
  ],
}
```

- ・List Containersエンドポイントで一覧を確認可能です
- ・管理グループID(container:idに相当)は、List Containersのレスポンスから対象の管理グループオブジェクト内の"id"を参照ください。
- ・「親となる初期管理グループ」の場合、parent_id=0と表示されます。

■(参考)CertCentralの画面での管理グループ/Division情報確認方法

The screenshot shows the CertCentral interface. On the left, the 'アカウント' (Account) menu is highlighted with a red box. A sub-menu is open, showing '管理グループ' (Management Groups) also highlighted with a red box. On the right, the '管理グループ' (Management Groups) page is displayed. It has three buttons: '新しい管理グループ' (New Management Group), '無効な管理グループ' (Inactive Management Group), and '自身の管理グループ' (My Management Group), with the last one highlighted by a red box. Below the buttons, there is a red box containing the text '<管理グループ/Division名>'. At the bottom, the browser address bar shows the URL 'https://www.digicert.com/secure/divisions/129626', with a red box around the ID '129626' and a red arrow pointing to it from the text 'Container : id'.

- ・「アカウント」→「管理グループ」メニューから一覧を確認可能です
- ・個別の管理グループのID(container:idに相当)は、同メニューから管理グループをクリック、または「自身の管理グループ」をクリックしてください。
→管理グループ詳細画面のURLの以下の部分が「管理グループID(container : id)に該当します。
< <https://www.digicert.com/secure/divisions/<■ここが管理グループIDに該当します■>> >

cURLのサンプルコード(*1)



アカウント内での「申請レビュー・承認」を無効にしている、かつ
組織(Org)およびドメイン(Domain)の(事前)認証が完了していて証明書が即時発行された場合

● 201 (one-step) ● 201 (two-step) ● 201 (auto) ● 201 (skip) ● 201 (immediate)

```
{
  "id": 112233,
  "certificate_id": 113,
  "certificate_chain": [
    {
      "subject_common_name": "example.com",
      "pem": "<pem_certificate>"
    },
    {
      "subject_common_name": "DigiCert SHA2 Secure Server CA",
      "pem": "<pem_certificate>"
    },
    {
      "subject_common_name": "DigiCert Global Root CA",
      "pem": "<pem_certificate>"
    }
  ]
}
```

レスポンス： 主なフィールド	説明	データタイプ
id	order_id (オーダーID)	Int
certificate_id	certificate_id (証明書オブジェクトを示す識別子)	Int
certificate_chain		-
subject_common_name	End-Entity証明書：Subjectコモンネーム	String
pem	End-Entity証明書：PEM形式の証明書データ	String
subject_common_name	中間認証局証明書：Subjectコモンネーム	String
pem	中間認証局証明書：PEM形式の証明書データ	String
subject_common_name	ルート認証局証明書：Subjectコモンネーム	String
pem	ルート認証局証明書：PEM形式の証明書データ	String

もっと詳しく：<https://dev.digicert.com/services-api/orders/order-secure-site-ov/>

プラン更新申請について (プラン新規申請とプラン更新申請の共通点、相違点)

- 「プラン新規申請」と「プラン更新申請」では、共通の[Order*]エンドポイントを用います。

```
POST https://www.digicert.com/services/v2/order/certificate/{{product_id}}
```

- リクエストパラメータに以下のいずれかの識別子を指定いただくことで、弊社システム側で「プラン新規申請」または「プラン更新申請」のいずれかを判定します
 - renewal_of_order_id**: 「更新元プラン/証明書」のオーダーIDを指定、または
 - renewed_thumbprint**: 「更新元プラン/証明書」のハッシュ値
 - 上記のいずれも指定がない場合は「プラン新規申請」と判定
- 「更新元プラン/証明書」は、お客様のアカウント(APIキーを保有するユーザが所属するお客様アカウント)内のオーダー情報として管理されているものである必要があります
 - 他のアカウントで発行された証明書のオーダーID/ハッシュ値を指定した場合はエラーとなります
- プラン更新申請時に更新元と異なるFQDN(Subject CN, SANs)を指定可
 - 更新前後でFQDNが異なっても残有効期間を引き継ぐことが可能
- 【API限定機能】プラン更新申請時に、更新元と異なる証明書製品を指定可
 - 更新前後で製品種類が異なっても残有効期間を引き継ぐことが可能
- 【API限定機能】更新元のプラン有効期間残日数に関わらずプラン更新申請は可能
 - 残日数によって引き継がれる有効期間の算出方法については後述

cURLのサンプルコード(*1)

```
curl -X POST \
https://www.digicert.com/services/v2/order/certificate/ssl_ev_basic \
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}' \
-d '{
  "certificate": {
    "common_name": "example.com",
    "dns_names": [
      "sub.example.com",
      "app.example.com"
    ],
    "csr": "<csr>",
    "signature_hash": "sha256",
    "server_platform": {
      "id": 2
    },
    "cert_validity": {
      "custom_expiration_date": "21 DEC 2021"
    }
  },
  "comments": "Certificate for app server.",
  "container": {
    "id": 334455
  },
  "auto_renew": 1,
  "custom_renewal_message": "Keep this renewed.",
  "organization": {
    "id": 123456,
  },
  "order_validity": {
    "custom_expiration_date": "21 DEC 2024"
  },
  "payment_method": "balance"
}'
```

証明書
(certificate)管理グループ
(container)組織
(organization)

Method+Endpoint:

POST https://www.digicert.com/services/v2/order/certificate/{{product_id}}

・APIエンドポイントのURIのうち上記下線部分には、product_id(製品識別子)を指定します
→[別紙] product_id(製品識別子)一覧 参照

リクエスト： 主なパラメータ	説明	データ タイプ
certificate	certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN) ※ 証明書申請には当パラメータの値が利用されます(CSRの値は使用しない)	String
dns_names	コモンネーム(FQDN)と異なる名称のSANsを追加する場合、併せて指定します SANsの入力数量の上限(デフォルト):250	String[]
csr	CSR(Certificate Signing Request)	String
signature_hash	証明書に対する署名に使用するハッシュアルゴリズム(通常"sha256")	String
server_platform	お客様のサーバープラットフォーム環境を選択し、発行通知メールに添付される証明書ファイル形式を最適化いただけます ※ 発行通知メールの形式は組織の管理者によって指定されます。 CCE簡易マニュアル「5.1 発行された証明書の取得」を参照ください	Int
cert_validity	【複数年プランの場合に指定】 [別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照	-
years/ days/ custom_expiration_date		
container	[別紙] container : id (管理グループ/Division) の確認方法 参照	Object
organization	[別紙] 組織(Org)情報の入力方法 参照	Object
order_validity	【複数年プランの場合に指定】 [別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照	-
years/ days/ custom_expiration_date		
renewal_of_order_id	更新元プラン/証明書のオーダーIDを指定	} プラン更新申請の場合、 いずれか一方が必須
renewed_thumbprint	更新元プラン/証明書の証明書ハッシュ値	

その他のパラメーターの説明など、もっと詳しく:<https://dev.digicert.com/services-api/orders/order-multi-year-plan/>

Additional emails : オーダーの通知メール送信先を追加

cURLのサンプルコード(*1)

```
curl -X PUT \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/additional-emails' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "additional_emails": [
      "jill.valentine@example.com",
      "leon.kennedy@example.com"
    ]
  }'
```

Method+Endpoint:

PUT https://www.digicert.com/services/v2/order/certificate/{{order_id}}/additional-emails

リクエスト: 主なパラメータ	説明	データタイプ
additional_emails	メールアドレス [繰り返し項目]	String []

Additional Emailsを利用して追加したメールアドレスで受信いただける証明書ライフサイクルイベントは以下の通りです。

- ・証明書の発行(発行通知メール)
- ・証明書のライフサイクル管理(再発行、失効等)
- ・証明書の更新案内メール

もっと詳しく: <https://dev.digicert.com/services-api/orders/additional-emails/>

(補足) 組織認証/DCVが完了しているのに証明書が発行されない場合

Q: セクション2.2 [事前認証]で組織認証とDCV(ドメイン名利用権確認)が完了しているのに、条件を満たす証明書を申請しても、その後即時には証明書が発行されない場合があるのは何故ですか？

A: デジサート CertCentralでは不適切な証明書の発行(例:フィッシングサイトへの発行)を回避・防止するために、一般的な組織認証とDCV(ドメイン名利用権確認)に加えて、追加の複数の手段で証明書申請に対する確認を行っております。組織認証とDCVが完了しているにも関わらず申請から30分以上経っても証明書が発行されない場合は、**当社認証サポートチームまでオーダー番号を添えて、該当の申請のステータスについてお問合せください。**

(参考)「組織認証とドメイン名認証が完了しているにも関わらず証明書が発行されていない」状態の見分け方

■ 画面で見分ける方法: オーダー詳細画面

オーダーステータス
証明書最終確認

オーダーステータスが「証明書最終確認」と表示されていること

OR

「証明書を発行する」以外の確認項目に全てチェックマーク(完了マーク)がついていること

■ APIで見分ける方法: Validation Statusエンドポイント

```
{
  "order_id": "31525869",
  "order_status": "pending",
  "organization_id": 889100,
  "organization_name": "Win the Customer, LLC",
  "organization_validations": [
    {
      "type": "ov",
      "name": "OV",
      "description": "Normal Organization Validation",
      "date_created": "2020-04-23T15:43:36+00:00",
      "validated_until": "2021-05-22T00:42:58+00:00",
      "status": "complete"
    }
  ],
  "dns_name_validations": [
    {
      "domain_id": "1608046",
      "name_scope": "appfw.net",
      "approval_scope": "subdomains",
      "status": "approved",
      "method": "dns-cname-token",
      "dns_names": [
        "demo201911.appfw.net"
      ],
      "approval_expiration_date": "2022-07-28T08:01:19"
    }
  ]
}
```

"order_status": "pending",

Order_status=pending
(証明書は発行待ち)

"organization_validations": [

AND

{
 "type": "ov",
 "status": "complete"

organization_validations
.status=complete
(組織認証が完了した状態)

AND

"dns_name_validations": [
 {
 "status": "approved",
 "method": "dns-cname-token",
 "dns_names": [
 "demo201911.appfw.net"],
 "approval_expiration_date": "2022-07-28T08:01:19" }
]

dns_name_validations
.status=complete
(DCVが完了した状態)

5. オーダー管理、リクエスト管理

~ 5.1 オーダー管理 ~

Order Info : 個別オーダーのステータスをチェック

cURLのサンプルコード(*1)

```
curl -X GET \
https://www.digicert.com/services/v2/order/certificate/{{order_id}}\
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

```
GET https://www.digicert.com/services/v2/order/certificate/{{order_id}}
```

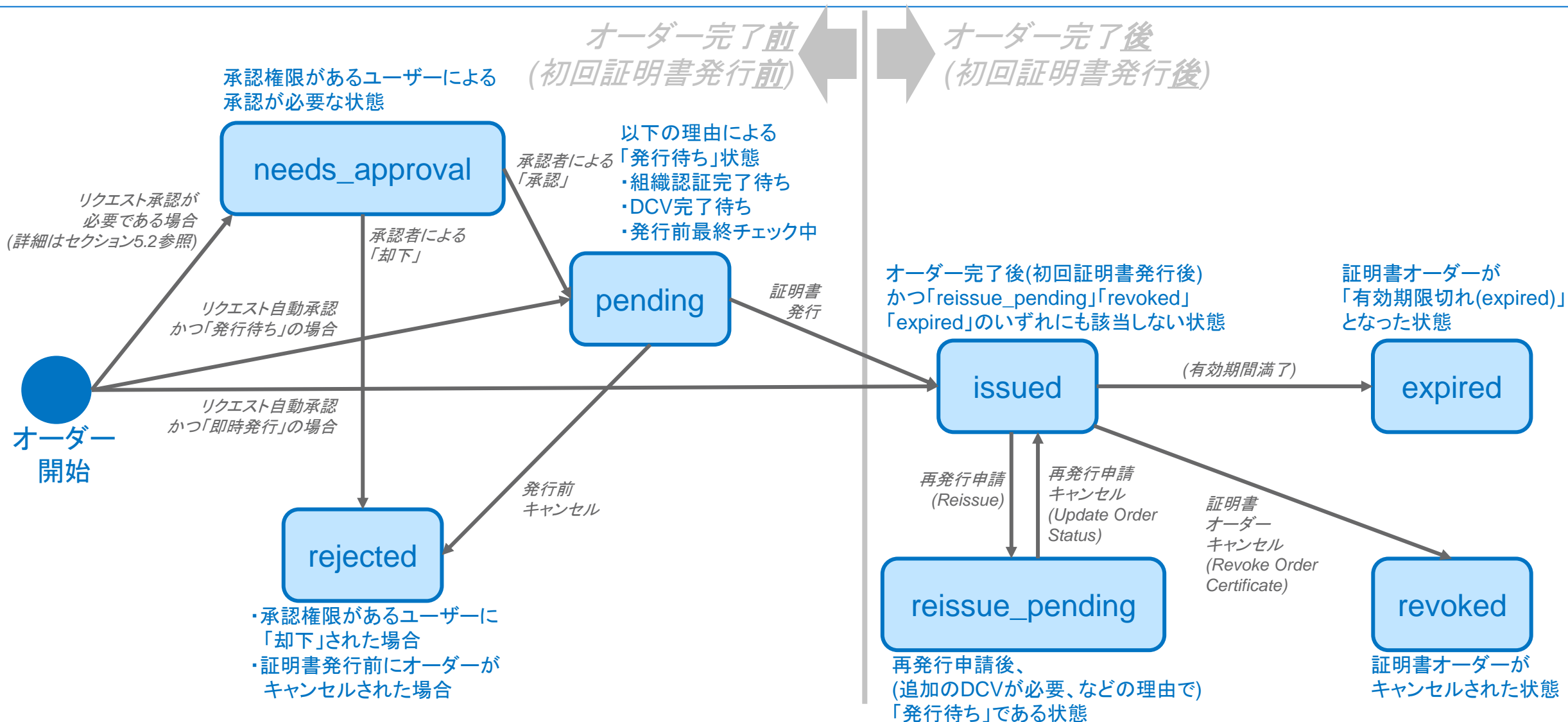
レスポンス例:

```
{
  "id": 115429178,
  "certificate": {
    "id": 116470545,
    "thumbprint": "(省略)",
    "serial_number": "(省略)",
    "common_name": "demo.appfw.net",
    "dns_names": [
      "demo.appfw.net"
    ]
  },
  "date_created": "2021-01-20T02:30:12+00:00",
  "valid_from": "2021-01-20",
  "valid_till": "2022-01-23",
  "days_remaining": 359,
  "cert_validity": {
    "years": 1
  },
  "csr": "<csr>",
  "organization": {
    "id": 754781
  },
  "server_platform": {
    "id": 2,
    "name": "Apache",
    "install_url": "(省略)",
    "csr_url": "(省略)",
    "best_format": "apache"
  },
  "signature_hash": "sha256",
  "key_size": 2048,
  "ca_cert": {
    "id": "39786C15468D713F",
    "name": "DigiCert TLS RSA SHA256 2020 CA1"
  },
  "user_id": 0,
  "receipt_id": "109678649",
  "purchased_dns_names": "1",
  "purchased_wildcard_names": "0"
},
  "status": "issued",
  "is_renewal": false,
  "is_renewed": false,
  "date_created": "2021-01-20T02:30:12+00:00",
  "organization": {
    "id": 754781,
    "name": "Win The Customer, LLC",
    "display_name": "Win The Customer, LLC",
    "is_active": true,
    "city": "Saratoga Springs",
    "state": "Utah",
    "country": "us",
    "telephone": "(801) 228-0992"
  },
  "validity_years": 1,
  "order_validity": {
    "years": 1
  },
  "order_valid_from": "2021-01-19",
  "order_valid_till": "2022-01-24",
  "disable_renewal_notifications": false,
  "auto_renew": 0,
  "container": {
    "id": 259346,
    "name": "Container 01",
    "is_active": true
  },
  "product": {
    "name_id": "ssl_securesite_pro",
    "name": "Secure Site Pro SSL",
    "type": "ssl_certificate",
    "validation_type": "ov",
    "validation_name": "OV",
    "validation_description": "Normal Organization Validation",
    "csr_required": true
  },
  "organization_contact": {
    "first_name": "Guest",
    "last_name": "User",
    "name": "Guest User"
  },
  "technical_contact": {
    "first_name": "abc",
    "last_name": "def",
    "email": "a@a.com",
    "job_title": "manager",
    "telephone": "03-12354-456",
    "name": "abc def"
  },
  "user": {
    "id": 0
  },
  "purchased_dns_names": 1,
  "requests": [
    {
      "id": 11203371,
      "date": "2021-01-20T02:29:08+00:00",
      "type": "new_request",
      "status": "approved"
    }
  ],
  "receipt_id": 109678649,
  "cs_provisioning_method": "none",
  "public_id": "(省略)",
  "additional_emails": [
    "taro.ninsho@digicert.com"
  ],
  "allow_duplicates": true,
  "is_out_of_contract": true,
  "payment_method": "balance",
  "product_name_id": "ssl_securesite_pro",
  "disable_issuance_email": false,
  "disable_ct": true,
  "dcv_method": "email",
  "server_licenses": 1,
  "is_guest_access_enabled": true,
  "is_multi_year_plan": "1",
  "has_pending_request": false
}
```

レスポンス : 主なフィールド	説明	データ タイプ
certificate	Certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN)	String
dns_names	コモンネーム(FQDN)と異なる名称のSANsを追加する場合、併せて指定します	String []
csr	CSR(Certificate Signing Request)	String
signature_hash	証明書に対する署名に使用するハッシュアルゴリズム(通常"sha256")	String
valid_till	(証明書発行済(issued)オーダーの場合) 証明書の有効期間終了日	String
days_remaining	(証明書発行済(issued)オーダーの場合) 証明書有効期間残日数	Int
cert_validity	申請情報 - 証明書有効期間	Object
years/ days/ custom_expiration_date	([別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照)	-
validity_years	申請情報 - 【複数年プランでない場合に指定】有効期間	Int
order_validity	申請情報 - プラン有効期間	Object
years/ days/ custom_expiration_date	([別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照)	-
status	[別紙] オーダーのステータス状態遷移 参照	String
is_renewal	当オーダーが更新申請か否か	boolean
is_renewed	当オーダーの証明書が既に更新されたか否か	boolean
container	管理グループ/Divisionの情報	Object
organization	組織(Org)情報	Object
organization_contact	Organization Contact(申請責任者)情報 (詳細は page17参照)	Object
technical_contact	Technical Contact(申請責任者)情報 (詳細は page17参照)	Object
is_multi_year_plan	複数年プランの場合:1、複数年プランでない場合:なし(フィールドが返却されない)	String
user	証明書オーダーを申請したCertCentralのユーザー情報	Object

もっと詳しく: <https://dev.digicert.com/services-api/orders/order-info/>

(OV/EV証明書の場合) オーダーのステータス状態遷移



Validation Status : オーダーの認証情報を確認

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/validation'
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

```
GET https://www.digicert.com/services/v2/order/certificate/{{order_id}}/validation
```

レスポンス例:

```
{
  "order_id": "112211",
  "order_status": "issued",
  "organization_id": "12345",
  "organization_name": "Example Organization",
  "organization_validations": [
    {
      "dns_name_validations": [
        {
          "domain_id": "1234",
          "name_scope": "example.com",
          "approval_scope": "subdomains",
          "status": "approved",
          "method": "email",
          "dns_names": [
            "sub.example.com"
          ],
          "approval_expiration_date": "2020-09-11T16:27:39+00:00"
        }
      ]
    }
  ]
}
```

レスポンス : 主なフィールド	説明	データタイプ
order_id	order_id (オーダーID)	String
order_status	オーダーのステータス 例 : 「認証中・未発行」の場合「pending」	String
organization_id	組織(Org)のID	String
organization_name	組織(Org)の名称(正式名称)	String
organization_validations	Organization_validationオブジェクト	Object
type	認証タイプ(OV, EV)を指定	String
validated_until	組織(Org)認証履歴の有効期限	String
dns_name_validations	Organization_validationオブジェクト	Object
domain_id	domain_id(ドメインのID)	String
status	ドメイン名利用権確認(DCV)のステータス (approved, pending)	String

もっと詳しく: <https://dev.digicert.com/services-api/orders/validation-status/>

List orders : オーダー一覧の取得

cURLのサンプルコード(*1)

```
curl -X GET \
  https://www.digicert.com/services/v2/order/certificate \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

```
GET https://www.digicert.com/services/v2/order/certificate
```

レスポンス例:

```
{
  "orders": [
    {
      "id": 123457,
      "certificate": {
        "id": 105,
        "common_name": "example.org",
        "dns_names": [
          "sub.example.org"
        ],
        "valid_till": "2020-04-30",
        "days_remaining": 289,
        "signature_hash": "sha256"
      },
      "status": "issued",
      "is_renewed": false,
      "date_created": "2019-04-30T18:02:50+00:00",
      "organization": [],
      "validity_years": 1,
      "container": {
        "id": 14,
        "name": "CertCentral"
      },
      "product": {
        "name_id": "ssl_dv_geotrust",
        "name": "GeoTrust Standard DV",
        "type": "dv_ssl_certificate"
      },
      "has_duplicates": false,
      "product_name_id": "ssl_dv_geotrust"
    }
  ]
}
```

レスポンス : 主なフィールド	説明	データタイプ
id	オーダーID	Int
certificate	Certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN) ※ 複数のSANを登録する場合、併せて"dns_names"を設定	String
valid_till	(証明書発行済(issued)オーダーの場合) 証明書の有効期間終了日	String
days_remaining	(証明書発行済(issued)オーダーの場合) 証明書有効期間残日数	
status	オーダーのステータス (pending : 認証中・未発行等) [別紙] オーダーのステータス状態遷移 参照	string

もっと詳しく: <https://dev.digicert.com/services-api/orders/list-orders/>

List orders : オーダー一覧の取得 (フィルタ機能を用いた場合)

List orders(オーダー一覧の取得)呼出し時に、エンドポイントにフィルタ用のパラメータ(“?”以降の文字列)を追記いただくことで、指定した条件を満たすオーダー情報のみを取得したり、一覧を取得する順次を変更するためのフィルタ機能を活用いただくことが可能です。

■シナリオ1 : 指定した証明書コモンネーム(FQDN)と合致する証明書発行済の全オーダーを取得 (ソートキー:有効期間終了日(降順))

```
https://www.digicert.com/services/v2/order/certificate?filters[search]=www.digicert.com&filters[status]=issued&sort=-date_valid_till
```

①証明書コモンネーム(FQDN)として「www.digicertdemo.com」(完全一致)を指定

②オーダーのステータスとして発行済(issued)を指定を指定

③ソートキーとして有効期間終了日、順序として降順(新→古)を指定
※ フィールド名の前に“+”を指定することで昇順、“-”を指定することで降順を表します。

■シナリオ2 : 指定したベースドメイン名配下のコモンネーム(FQDN)で「セキュア・サーバID(Secure Site)」のオーダーを取得

```
https://www.digicert.com/services/v2/order/certificate?filters[search]=%digicert.com&filters[product_name_id]=ssl_securesite
```

①証明書コモンネーム(FQDN)として「digicert.com」、または配下のサブドメインをコモンネームに持つ証明書(例: sub1.digicert.comやsub2.sub1.digicert.comを含む)を指定

②製品種類として「セキュア・サーバID」を指定
※ 値には製品種類を表す「Product Identifier(製品識別子)」を指定してください。Product Identifierの一覧はこちら:
<https://dev.digicert.com/glossary/#product-identifiers>

■List Orders(オーダー一覧参照)等におけるフィルタ機能(*1)についてもっと詳しく:
<https://dev.digicert.com/services-api/#url-query-strings>

(ご参考) List Ordersで利用可能なフィルター一覧

■「絞り込み」のためのパラメータ

```

container_id=
organization_id=
user_id=
filters[date_created]=
  =2017-05-10+00:00:00...2017-05-11+23:59:59
  >2017-01-01
filters[valid_till]
  =2017-05-10+00:00:00...2017-05-11+23:59:59
  <2017-05-11
filters[status]=
  issued
  pending
  processing
  reissue_pending
  reissue_processing
  revoked
  rejected
filters[email]=
filters[search]=
  %mydomain.com
  %12345678
filters[common_name]=
  %mydomain.com
filters[product_name_id]=ssl_plus

```

「発行済かつ有効期間内」を絞り込み条件として
該当オーダー一覧を取得する場合に指定

ドメイン名/FQDNを絞り込み条件として
該当オーダー一覧を取得する場合に指定
("%"を用いた後方一致検索も可能)

「製品種類」を絞り込み条件として
該当オーダー一覧を取得する場合に指定

Multiple params can be passed in using array identifiers, like so:

```

filters[product_name_id][0]=ssl_plus&filters[product_name_id][1]=ssl_multi_domain&filters[product_name_id][2]=ssl_wildcard
Parameter values should be one of the "products.name_id" values from GET /product

```

■ソートのためのパラメータ、他

```

limit=25
  (Max 1000)
offset=0
sort=
  +order_id
  -order_id
  +date_created
  -date_created
  +common_name
  -common_name
  +status
  -status
  +validity_years
  -validity_years
  +product_name
  -product_name
  +date_valid_till
  -date_valid_till

```

「有効期間終了日」をソート(並び替え)キーとして
利用する場合に指定

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/order/certificate/status-changes?minutes=10'
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

GET https://www.digicert.com/services/v2/order/certificate/status-changes

レスポンス例:

```
{
  "orders": [
    {
      "order_id": 265,
      "certificate_id": 112233,
      "status": "issued"
    },
    {
      "order_id": 264,
      "certificate_id": 112232,
      "status": "canceled"
    },
    {
      "order_id": 263,
      "certificate_id": 112231,
      "status": "issued"
    },
    {
      "order_id": 262,
      "certificate_id": 112230,
      "status": "rejected"
    }
  ]
}
```

リクエスト : 主なパラメータ	説明	データタイプ
minutes	検索範囲を「分」単位で指定	Int

レスポンス : 主なフィールド	説明	データタイプ
order_id	order_id (オーダーID)	Int
certificate_id	certificate_id (証明書オブジェクトを示す識別子)	Int
status	現在(当リクエスト呼び出した時点)のオーダーのステータス <ul style="list-style-type: none"> pending : 認証中・未発行 issued : 証明書発行済 canceled : キャンセル済 	String

もっと詳しく: <https://dev.digicert.com/services-api/orders/status-change-list/>

5. オーダー管理、リクエスト管理

~ 5.2 リクエスト管理 ~

サーバ証明書(OV/EV)証明書の申請～発行までの流れ

■ セクション「2.事前認証」の範囲		製品カテゴリ	SSL/TLSサーバ証明書	
			OV(企業認証)	EV(Extended Validation)
	「組織」の事前認証	組織 (Organization)	→CCE利用ガイド(コンソール編)(*1) 参照	
		認証済連絡先 (Verified Contact)	不要	→CCE利用ガイド (コンソール編)(*1) 参照
	ドメインの事前認証	ドメイン名	セクション2.2 参照	
■ セクション「3 証明書の申請」	証明書の申請	<ul style="list-style-type: none"> ・製品を選択 ・プランのお申込み(証明書を申請) 		
■ 当セクションの範囲	申請レビュー・承認	(アカウント単位の設定で省略可) <ul style="list-style-type: none"> ・管理者が申請内容を確認し、承認または却下 		
■ セクション「5 証明書の取得」	証明書の取得	<ul style="list-style-type: none"> ・発行された証明書を形式を指定して取得(APIでGET) 		
■ セクション「6 証明書管理」	証明書管理	<ul style="list-style-type: none"> ・証明書再発行(証明書の更新) ・証明書の失効 		

*1 : CertCentral Enterprise利用ガイド (コンソール編)

アカウント内での申請レビュー・承認について (1/3 アカウント設定)

- 「設定」→「選択設定」→「詳細設定」→「承認手順」メニューにて、証明書申請後の「申請レビュー・承認」プロセスの有無をアカウント単位で選択いただくことが可能です。
- 当設定は任意となります。初期状態(下記表内の最上段)が推奨となります。

アカウント設定		CertCentralの挙動	
パターン	設定イメージ	承認権限があるユーザーによる申請時 (Administrator等, ※1)	承認権限がないユーザーによる申請時 (Standard User等, ※1)
(初期状態) 1ステップ承認： 申請者が承認権限を持つ場合は自動承認(レビューをスキップ)	承認手順 <input type="radio"/> 承認ステップをスキップする：証明書注文プロセスから承認ステップを削除します ⓘ <input checked="" type="radio"/> 1ステップ承認：1名の承認者が明書申請を承認する必要があります <input checked="" type="checkbox"/> 申請者が承認者でもある場合は、新規および再発行証明書申請を自動的に承認 <input type="radio"/> 2ステップ承認：2名の承認者が証明書申請を承認する必要があります	自動的に承認 (承認権限があるユーザーによるレビューをスキップし、デジサートによる組織認証およびドメイン利用権確認を開始します)	1名の承認権限があるユーザーによる承認が必要 (承認要求メール配信)
常に自動承認	<input checked="" type="radio"/> 承認ステップをスキップする：証明書注文プロセスから承認ステップを削除します ⓘ	自動的に承認	
常に1ステップ承認	<input checked="" type="radio"/> 1ステップ承認：1名の承認者が明書申請を承認する必要があります <input type="checkbox"/> 申請者が承認者でもある場合は、新規および再発行証明書申請を自動的に承認		1名の承認権限があるユーザーによる承認が必要
常に2ステップ承認	<input checked="" type="radio"/> 2ステップ承認：2名の承認者が証明書申請を承認する必要があります	2名の異なる承認権限があるユーザーによる承認が必要	

承認の手順については次ページ参照

アカウント内での申請レビュー・承認について (2/3 メール・GUIでのレビュー・承認)

- 「承認が必要」な証明書申請がある場合、承認権限があるユーザーに対して承認を要求するメールが配信されます。CertCentralにログイン後、ダッシュボード上の「承認が必要な証明書申請」リンクなどから、対象の申請を確認して承認してください。

承認リクエストメール通知

→メール件名、送信元および本文イメージは、以下のようになります

件名	証明書申請 : [コモンネーム]
送信元	DigiCert <admin@digicert.com>
本文イメージ (抜粋)	<p>証明書が申請されました。</p> <p>コモンネーム: [コモンネーム] SANs: [SANs] 有効期間 (年) : [有効期間の年数] 申請者情報: [申請者の氏名およびメールアドレス]</p> <p>下記CertCentralにアクセスして、申請内容を確認の上ご承認ください。 https://www.digicert.com/secure/requests/[リクエスト番号]</p>

Click

承認画面 (承認権限を持つユーザー(Administrator等)がログインした状態)

The screenshot shows the CertCentral dashboard with a notification for 16 pending certificate requests. A red box highlights the notification, which is then shown in a larger view with a '承認' (Approve) button highlighted in a red box.

16 証明書申請

承認

アカウント内での申請レビュー・承認について (3/3 APIでのレビュー・承認)

APIでの「レビュー」 : *Request Info*

Method+Endpoint:

GET https://www.digicert.com/services/v2/request/{{request_id}}

cURLのサンプルコード(*1)

```
curl -X GET \
  https://www.digicert.com/services/v2/request/{{request_id}} \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

レスポンス : 主なフィールド	説明	データ タイプ
id	リクエスト(承認要求) ID	Int
type	リクエストタイプ (例 : new_request:証明書発行申請、revoke:証明書失効要求)	String
status	<ul style="list-style-type: none"> needs_approval : [1ステップ承認の場合] 承認待ち submitted : [2ステップ承認の場合] リクエスト後、第一の承認待ち pending : [2ステップ承認の場合] 第一の承認後、第二の承認待ち 	String
requester	リクエスト作成者の情報	Object
reviewer	[1ステップ承認の場合] <使用しません> [2ステップ承認の場合] 第一の承認者	Object
processor	[1ステップ承認の場合] 承認者 [2ステップ承認の場合] 第二の承認者	Object

もっと詳しく: <https://dev.digicert.com/services-api/requests/request-info/>

APIでの「承認」 : *Update Request Status*

Method+Endpoint:

PUT https://www.digicert.com/services/v2/request/{{request_id}}/status

cURLのサンプルコード(*1)

```
curl -X PUT \
  https://www.digicert.com/services/v2/request/{{request_id}}/status \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "status": "approved",
    "processor_comment": "Your request is approved."
  }'
```

リクエスト : 主なパラメータ	説明	データ タイプ
status	<ul style="list-style-type: none"> approved : 承認 ([2段階承認の場合] 2段階目承認完了) pending : [2段階承認の場合] 1段階目承認(レビュー)完了 rejected : 却下 	String
processor_comment	(任意)リクエスト処理に関するコメント (Request Infoを用いて別途確認することが可能)	String

もっと詳しく: <https://dev.digicert.com/services-api/requests/update-request-status/>

List Request : アカウント内での申請(Request)一覧の取得

cURLのサンプルコード(*1)

```
curl -X GET \
  https://www.digicert.com/services/v2/request \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

Method+Endpoint:

```
GET https://www.digicert.com/services/v2/request
```

レスポンス例:

```
{
  "requests": [
    {
      "id": 198,
      "date": "2018-10-16T20:05:28+00:00",
      "type": "new_request",
      "status": "pending",
      "requester": {
        "id": 14,
        "first_name": "John",
        "last_name": "Smith",
        "email": "john.smith@digicert.com"
      },
      "order": {
        "id": 12345678,
        "certificate": {
          "common_name": "example.com"
        },
        "organization": {
          "id": 112233,
          "name": "Epiygne Unwieldiness llc"
        },
        "container": {
          "id": 5,
          "name": "History Department"
        },
        "product": {
          "name_id": "ssl_plus",
          "name": "Standard SSL",
          "type": "ssl_certificate"
        }
      }
    },
    ...
  ],
  "page": {
    "total": 14,
    "limit": 0,
    "offset": 0
  }
}
```

レスポンス : 主なフィールド	説明	データ タイプ
requests	Request(申請)オブジェクト	Object []
id	申請(Request)ID	Int
status	証明書のステータス pending : レビュー・承認待ち approved : 承認済 rejected : 却下済	String
requester	申請者情報	Object
order	オーダー情報 : 証明書発行や失効等の対象となる証明書オーダー情報	Object
id	order_id (オーダーID)	Int
common_name	証明書発行対象のコモンネーム(FQDN)	String

6. 発行された証明書の取得

サーバ証明書(OV/EV)証明書の申請～発行までの流れ

■ セクション「2.事前認証」の範囲		製品カテゴリ	SSL/TLSサーバ証明書	
			OV(企業認証)	EV(Extended Validation)
	「組織」の事前認証	組織 (Organization)	→CCE利用ガイド(コンソール編)(*1) 参照	
		認証済連絡先 (Verified Contact)	不要	→CCE利用ガイド(コンソール編)(*1) 参照
	ドメインの事前認証	ドメイン名	セクション2.2 参照	
■ セクション「3 証明書の申請」	証明書の申請	<ul style="list-style-type: none"> ・製品を選択 ・プランのお申込み(証明書を申請) 		
■ セクション「4.2 リクエスト管理」	申請レビュー・承認	(アカウント単位の設定で省略可) <ul style="list-style-type: none"> ・管理者が申請内容を確認し、承認または却下 		
■ 当セクションの範囲	証明書の取得	<ul style="list-style-type: none"> ・発行された証明書を形式を指定して取得(APIでGET) 		
■ セクション「6 証明書管理」	証明書管理	<ul style="list-style-type: none"> ・証明書再発行(証明書の更新) ・証明書の失効 		

*1 : CertCentral Enterprise利用ガイド (コンソール編)

Download certificate : 発行された証明書をダウンロード(key:certificate_id)

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/certificate/{{certificate_id}}/download/format/{{format_type}}' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

レスポンス例:
(format_type=pem_noroot)

```
1 -----BEGIN CERTIFICATE-----
2 MIIFTDCCBDSgAwIBAgIQAGUCYKwU/yjB9bPPYn+eRDANBqkqhkiG9w0BAQsFADBP
3 MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGR1aUN1cnQgSW5jMSkwJwYDVQQDEyBE
4 aWdpQ2VydCBUTmFmYyYyMDIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIw
5 Fw0yMDEyMDcyMzU0NTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIw
6 MA4GA1UEBxMHQ2h1by1rdTEcMBoGA1UEChMTRRE1HSUNFU1QgSkFQQ2VydCBHbG9i
7 MB8GA1UEAxMYMDEyMDcyMzU0NTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIwMTIw
8 AQEFAAOCAQ8AMIIBCgKCAQEAAnjq3WI1juZGp9L40NhxGL9przusrDwg7JTuUUVx
9 4F5kPHkGhQ6cLmewa2FJOe1XWvM9p1GRJfEdkEdahFzKBonvLWbU0XzcoK411GL
10 qX1Nvu8p0i6oFI1YE2pCVwoDvjXv6+U/KC
11 V9BQ+8KL8c0/X3PSH1NbwGCS0sKDh/C6H0b
12 YsVX7eyvQXTfY+00EmUEeHVR0Q1GHFY9FY
13 pu1TSIjd8y+FrPuurnHJA3YrLu8glLwLNs
14 HwYDVR0jBBgwFoAUT2ui6qi qhIx56rTaD5i
15 70UHO0o4lD9FaYfjxcEIMCMGA1UdEQQcMBQ
16 Lm51dA0BgNVHQ8BAf8EBAMCBAwHQYDVRO
17 BwMCMIGLBgNVHR8EGYmGwYwPqA8oDqGOGH
18 bs9EaWdpQ2VydFRMU1JTQVNIQTII1njIwMjBj
19 Y3J1sNC5kaWdpY2VydC5jb2V0VRG1naUN1cnR
20 bDBM8GNVHSAERTBDMDCGCGCSAGG/WwBATA
21 L3d3dy5kaWdpY2VydC5jb2V0V1BTMAGGBMe
22 JAYIKwYBBQHMAGGGH0dHA6L9y9v3NwLmR
23 AoY7AHR0cDovL2NhY2VydHMUzG1naUN1cnQ
24 MjU2MjAyMENBMS5jcnQwDAYDVROTAQH/BAI
25 NDNoI8zZngAIDJ1dD5zmlV+LjMgRRGeKEa2
26 KfUbV2LEcnCUTqxJMMvvey1y4e54gm0BF4
27 Y0ufc/Uwwm7/ourV+q0MYAocCb0ywlQenuh
28 7TtbJzV14qUPzLLb5w6XRpZAw05omh4w7Vv
29 Luw+gCTc1dFaEuLAbkUtA5CKbhxgkIoP
30 oViwtiJa9yE21NuWxGq1w==
31 -----END CERTIFICATE-----
```

End-Entity証明書
(PEM形式)

中間CA証明書
(PEM形式)

Method+Endpoint:

```
GET https://www.digicert.com/services/v2/certificate/{{certificate_id}}/download/format/{{format_type}}
```

- ・API Endpointとして指定するURLのうち上記部分にはcertificate_idを指定してください。
- ・certificate_idはOrder Info, List Reissue, List Duplicate等にて参照・取得いただけます。

リクエスト: 主なパラメータ	説明	データ タイプ
format_type	証明書ファイル形式のフォーマットを指定 例: 「pem_noroot」: End-Entity証明書および中間証明書を含むPEM形式 詳細は [別紙] 証明書ファイル形式(format_type)一覧 参照	String

もっと詳しく: <https://dev.digicert.com/services-api/certificates/download-certificate-format/>

[別紙] 証明書ファイル形式(formart_type)一覧

No	ファイル形式ID (※1)	Content-Type	内容	ファイルに含まれる内容
1	default	application/zip	個別のルート、中間、およびエンドエンティティ証明書ファイルを含む、ZIP アーカイブ。	-エンドエンティティ証明書(.crt) -中間証明書(.crt) -ルート証明書(.crt)
2	p7b	application/x-pkcs7-certificates	ルート、中間およびエンドエンティティ証明書を含むシングル P7B バンドルファイル。	-エンドエンティティ証明書(.crt) -中間証明書(.crt) -ルート証明書(.crt)
3	cer	application/x-pkcs7-certificates	ルート、中間およびエンドエンティティ証明書を含むシングル P7B バンドルファイル。	-エンドエンティティ証明書(.cer) -中間証明書(.cer) -ルート証明書(.cer)
4	apache	application/zip	個別の中間およびエンドエンティティ証明書ファイルを含む、ZIP アーカイブ。	-エンドエンティティ証明書(.crt) -中間証明書(.crt)
5	pem_all	application/x-pem-file	ルート、中間およびエンドエンティティ証明書エントリを含む、単一 PEM バンドル。	-エンドエンティティ証明書 -中間証明書 -ルート証明書
6	pem_nointermediate	application/x-pem-file	エンドエンティティ証明書エントリのみを含む、単一 PEM ファイル。	-エンドエンティティ証明書
7	pem_noroot	application/x-pem-file	中間およびエンドエンティティ証明書エントリを含む、単一 PEM バンドル。	-エンドエンティティ証明書 -中間証明書
8	default_cer	application/zip	個別のルート、中間、およびエンドエンティティ証明書ファイルを含む、ZIP アーカイブ。	-エンドエンティティ証明書(.cer) -中間証明書(.cer) -ルート証明書(.cer)
9	default_pem	application/zip	個別のルート、中間、およびエンドエンティティ証明書ファイルを含む、ZIP アーカイブ。	-エンドエンティティ証明書(.pem) -中間証明書(.pem) -ルート証明書(.pem)

当ページの内容は以下のKnowledgeページの要約となります。

・ファイル形式について : <https://dev.digicert.com/glossary/#certificate-formats> (※1:ファイル形式IDの一覧はこちらを参照ください)

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/reissue' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

```
GET https://www.digicert.com/services/v2/order/certificate/{{order_id}}/reissue
```

レスポンス例:

```
{
  "certificates": [
    {
      "id": 12345,
      "thumbprint": "<thumbprint>",
      "serial_number": "<serial_number>",
      "common_name": "example.com",
      "dns_names": [
        "yourexample.com",
        "anotherexample.com",
        "*.myexample.com"
      ],
      "status": "issued",
      "date_created": "2019-04-08T17:33:26+00:00",
      "valid_till": "2020-04-08",
      "days_remaining": 267,
      "csr": "<csr>",
      "key_size": 2048,
      "user_id": 1576,
      "email": "logan.nelson@example.com",
      "firstname": "Logan",
      "lastname": "Nelson",
      "receipt_id": "1234",
      "purchased_dns_names": "2",
      "purchased_wildcard_names": "1"
    }
  ],
}
```

```
{
  "id": 23456,
  "common_name": "anewdomain.com",
  "dns_names": [
    "anewdomain.com"
  ],
  "status": "rejected",
  "date_created": "2018-11-14T19:57:09+00:00",
  "csr": "<csr>",
  "key_size": 2048,
  "user_id": 1576,
  "email": "logan.nelson@example.com",
  "firstname": "Logan",
  "lastname": "Nelson"
},
{
  "id": 34567,
  "common_name": "example.net",
  "dns_names": [
    "example.net"
  ],
  "status": "pending",
  "date_created": "2018-11-15T22:41:43+00:00",
  "csr": "<csr>",
  "key_size": 2048,
  "user_id": 1576,
  "email": "logan.nelson@example.com",
  "firstname": "Logan",
  "lastname": "Nelson"
}
]
```

・API Endpointとして指定するURLのうち上記部分にはorder_idを指定してください。

レスポンス: 主なフィールド	説明	データ タイプ
certificate	Certificateオブジェクト	Object []
id	証明書ID	Int
status	証明書のステータス issued : 証明書発行済 pending : 再発行待ち(認証中、承認待ち等) rejected : 却下された状態	String
serial_number	(証明書発行済(issued)の場合) 証明書のシリアル番号	String
common_name	証明書発行対象のコモンネーム(FQDN)	String
dns_names	証明書発行対象のSANs	String []
valid_till	(証明書発行済(issued)の場合) 証明書の有効期間終了日	String
days_remaining	(証明書発行済(issued)オーダーの場合) 証明書有効期間残日数	Int

cURLのサンプルコード(*1)

```
curl -X GET \
'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/duplicate' \
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}'
```

```
GET https://www.digicert.com/services/v2/order/certificate/{{order_id}}/duplicate
```

レスポンス例:

・API Endpointとして指定するURLのうち上記部分にはorder_idを指定してください。

```
{
  "certificates": [
    {
      "id": 12345,
      "thumbprint": "<thumbprint>",
      "serial_number": "<serial_number>",
      "common_name": "example.com",
      "dns_names": [
        "sub.example.com"
      ],
      "status": "approved",
      "date_created": "2016-03-25T21:01:40:00:00",
      "valid_from": "2016-03-23",
      "valid_till": "2019-03-28",
      "days_remaining": 111,
      "csr": "<csr>",
      "server_platform": {
        "id": 45,
        "name": "nginx",
        "install_url": "http://www.digicert.com/ssl-certification-creation-nginx",
        "csr_url": "http://www.digicert.com/csr-creation-nginx"
      },
      "signature_hash": "sha256",
      "key_size": 2048,
      "ca_cert_id": "1005",
      "sub_id": "111",
      "public_id": "<public_id>",
      "archived": "0",
      "user_id": 2,
      "firstname": "Jan",
      "lastname": "Sport"
    },
    {
      "id": 23456,
      "common_name": "anewdomain.com",
      "dns_names": [
        "sub.anewdomain.com"
      ],
      "status": "rejected",
      "date_created": "2018-11-14T19:00:00",
      "csr": "<csr>",
      "server_platform": {
        "id": 45,
        "name": "nginx",
        "install_url": "http://www.digicert.com/ssl-certification-creation-nginx",
        "csr_url": "http://www.digicert.com/csr-creation-nginx"
      },
      "signature_hash": "sha256",
      "key_size": 2048,
      "ca_cert_id": "1005",
      "sub_id": "112",
      "public_id": "<public_id>",
      "archived": "0",
      "user_id": 5,
      "firstname": "John",
      "lastname": "Someone"
    },
    {
      "id": 34567,
      "common_name": "example.net",
      "dns_names": [
        "sub.example.net"
      ],
      "status": "pending",
      "date_created": "2018-11-15T22:41:43+00:00",
      "csr": "<csr>",
      "server_platform": {
        "id": 45,
        "name": "nginx",
        "install_url": "http://www.digicert.com/ssl-certification-creation-nginx",
        "csr_url": "http://www.digicert.com/csr-creation-nginx"
      },
      "signature_hash": "sha256",
      "key_size": 2048,
      "ca_cert_id": "1005",
      "sub_id": "113",
      "public_id": "<public_id>",
      "archived": "0",
      "user_id": 12,
      "firstname": "Jill",
      "lastname": "Valentine"
    }
  ]
}
```

レスポンス : 主なフィールド	説明	データ タイプ
certificate	Certificateオブジェクト	Object []
id	証明書ID	Int
status	証明書のステータス issued : 証明書発行済 pending : 再発行待ち(認証中、承認待ち等) rejected : 却下された状態	String
serial_number	(証明書発行済(issued)の場合) 証明書のシリアル番号	String
common_name	証明書発行対象のコモンネーム(FQDN)	String
dns_names	証明書発行対象のSANs	String []
valid_till	(証明書発行済(issued)の場合) 証明書の有効期間終了日	String
days_remaining	(証明書発行済(issued)オーダーの場合) 証明書有効期間残日数	Int

7. 再発行、複製、失効等の証明書管理

サーバ証明書(OV/EV)証明書の申請～発行までの流れ

■ セクション「2.事前認証」の範囲		製品カテゴリ	SSL/TLSサーバ証明書	
			OV(企業認証)	EV(Extended Validation)
	「組織」の事前認証	組織 (Organization)	→CCE利用ガイド(コンソール編)(*1) 参照	
	ドメインの事前認証	認証済連絡先 (Verified Contact)	不要	→CCE利用ガイド(コンソール編)(*1) 参照
		ドメイン名	セクション2.2 参照	
■ セクション「3 証明書の申請」	証明書の申請	<ul style="list-style-type: none"> ・製品を選択 ・プランのお申込み(証明書を申請) 		
■ セクション「4.2 リクエスト管理」	申請レビュー・承認	(アカウント単位の設定で省略可) <ul style="list-style-type: none"> ・管理者が申請内容を確認し、承認または却下 		
■ セクション「5 証明書の取得」	証明書の取得	<ul style="list-style-type: none"> ・発行された証明書を形式を指定して取得(APIでGET) 		
■ 当セクションの範囲	証明書管理	<ul style="list-style-type: none"> ・証明書再発行(証明書の更新) ・証明書の失効 		

*1 : CertCentral Enterprise利用ガイド (コンソール編)

再発行、複製、失効等の証明書管理 概要

■当セクションの範囲

証明書の再発行	<ul style="list-style-type: none">・証明書再発行(Reissue)を申請します・【複数年プラン】選択時:プランの期間内で、証明書有効期間を延長(最大397日間)します・ドメイン名の事前認証履歴が期限切れの場合、ドメイン利用権確認(DCV)が必要です・コモンネーム/SANsを変更/削除した場合、元証明書は48-72時間以内に失効されます。ご注意ください。
証明書の複製	<p>【サーバ証明書(OV/EV)のみ】</p> <ul style="list-style-type: none">・証明書複製(Duplicate)を申請します
証明書の失効	<ul style="list-style-type: none">・証明書失効(Revoke)の申請<ul style="list-style-type: none">※ 失効申請が完了しても、証明書失効処理は完了しません→完了させるためには管理者による失効申請リクエストの「承認」が必要・失効リクエストの「承認」処理

Reissue certificate : 証明書の再発行

cURLのサンプルコード(*1)

```
curl -X PUT ¥
'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/reissue'
-H 'Content-Type: application/json' ¥
-H 'X-DC-DEVKEY: {{api_key}}' ¥
-d '{
"certificate": {
  "common_name": "example.com",
  "dns_names": [
    "sub.example.com"
  ],
  "csr": "<csr>",
  "server_platform": {
    "id": 2
  },
  "cert_validity": {
    "days": 60
  },
  "signature_hash": "sha256"
}
}'
```

Method+Endpoint:

POST https://www.digicert.com/services/v2/order/certificate/{{order_id}}/reissue

・API Endpointとして指定するURLのうち上記部分にはorder_idを指定してください。

リクエスト : 主なパラメータ	説明	データ タイプ
certificate	certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN) ※ 証明書申請には当パラメータの値が利用されます(CSRの値は使用しない) ※ 再発行元の証明書から変更が可能 (※注1)	String
dns_names	コモンネーム(FQDN)と異なる名称のSANsを追加する場合、併せて指定します ※ SANsの入力数量の上限(デフォルト): 250 ※ 再発行元の証明書から変更/追加/削除が可能 (※注1)	String[]
csr	CSR(Certificate Signing Request) (※注2)	String
signature_hash	証明書に対する署名に使用するハッシュアルゴリズム(通常"sha256")	String
server_platform	<新規/更新申請時と同様>	Int
cert_validity	【複数年プランの場合に指定】	
years/ days/ custom_expiration_date	[別紙] 複数年プラン(ご契約期間)リクエストパラメーターについて 参照 併せて、再発行申請時に指定可能な有効期限については次ページ参照	-

もっと詳しく: <https://dev.digicert.com/services-api/orders/reissue-certificate/>

再発行申請を開始する前に、以下の注意事項をよくご確認ください。

注1 : コモンネーム/SANsについて

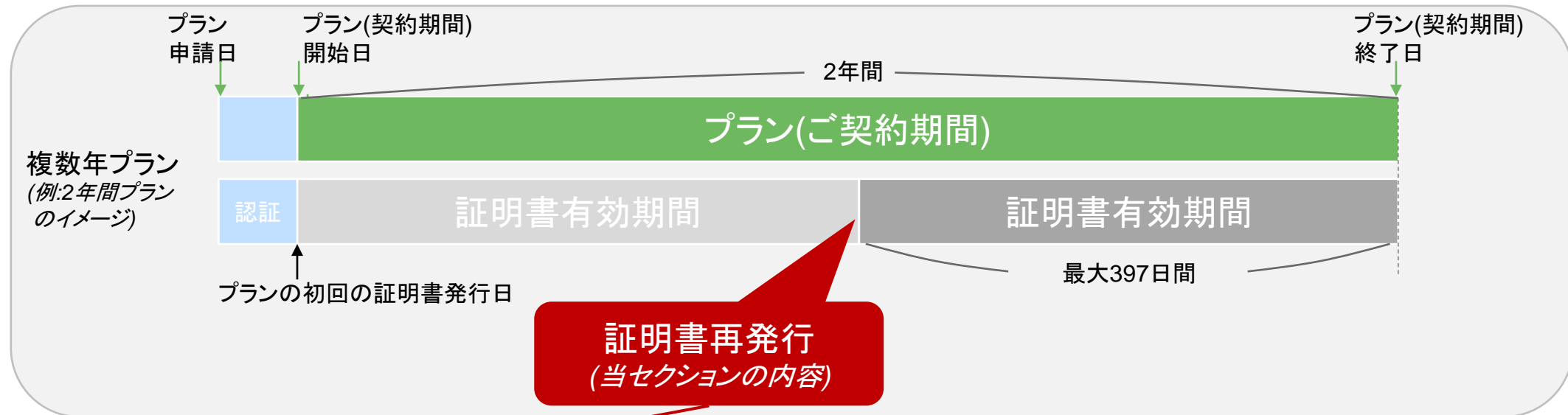
再発行申請時に、再発行前の証明書に含まれていたコモンネーム/SANsを変更したり一部を削除した場合、再発行完了後から48~72時間以内に元証明書が失効されます。ウェブサイトのFQDN変更のタイミングで証明書を再発行する場合等は十分ご注意ください。(全てのコモンネーム/SANsに変更がない場合、または追加のみの場合は、元証明書は失効されません)

注2 : CSRについて

セキュリティ観点でのベストプラクティスとして、証明書再発行いただく際には、以前に作成したCSRを再利用せず、新しく生成し直したCSRを利用いただくことを推奨します

補足 複数年プランの場合 - 再発行(Reissue)申請時の「証明書有効期間」について

■ 複数年プランの場合 再発行申請時の有効期間のイメージ



- 【証明書の有効期間】の最大値は「プラン(契約期間)終了日までの日数」または「397日間」のいずれか早い方となります。
- <cert_validity>オブジェクトを用いて【証明書の有効期間】を設定する場合、以下の点にご注意ください。
- ・cert_validity:years を用いる場合、プラン残期間が370日間以上ある場合に限り、「1」を指定可能
 - ・cert_validity:days を用いる場合、プラン終了日までの残日数を指定可能(最大「397」)
 - ・cert_validity:custom_expiration_date を用いる場合、プラン終了日と同日またはそれ以前の日付を指定可能(最大397日後)
- ※ 再発行申請によってプラン(ご契約期間)を延長することはできません

Duplicate certificate : 証明書の複製発行

cURLのサンプルコード(*1)

```
curl -X POST \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/duplicate' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "certificate": {
      "common_name": "example.com",
      "dns_names": [
        "sub.example.com"
      ],
      "csr": "<csr>",
      "server_platform": {
        "id": 45
      },
      "signature_hash": "sha256"
    }
  }'
```

Method+Endpoint:

POST https://www.digicert.com/services/v2/order/certificate/{{order_id}}/duplicate

- API Endpointとして指定するURLのうち上記部分にはorder_idを指定してください。
- Order IDは、証明書を申請したタイミングで割り振られます。

リクエスト : 主なパラメータ	説明	データ タイプ
certificate	certificateオブジェクト	Object
common_name	証明書発行対象のコモンネーム(FQDN) ※ 証明書申請には当パラメータの値が利用されます(CSRの値は使用しない) ※ 複製発行元の証明書からの変更は不可	String
dns_names	コモンネーム(FQDN)と異なる名称のSANsを追加する場合、併せて指定します SANsの入力数量の上限(デフォルト):250 ※ 複製発行元の証明書からの変更/追加/削除は不可	String[]
csr	CSR(Certificate Signing Request)	String
signature_hash	証明書に対する署名に使用するハッシュアルゴリズム(通常"sha256")	String
server_platform	<新規/更新申請時と同様>	Int

もっと詳しく: <https://dev.digicert.com/services-api/orders/duplicate-certificate/>

(補足) 証明書の「再発行」と「複製」の違い

	再発行(Reissue)	複製(Duplicate)
対象製品	<ul style="list-style-type: none"> ・サーバ証明書(OV/EV) ・サーバ証明書(プライベートSSL) ・コードサイン証明書/EVコードサイン証明書 	<ul style="list-style-type: none"> ・サーバ証明書(OV/EV)のみ
主な用途	<ul style="list-style-type: none"> ・証明書の更新(有効期間延長) ・コモンネーム/SANsの追加/変更/削除 ・鍵/署名アルゴリズムの変更 	<ul style="list-style-type: none"> 鍵/署名アルゴリズムの変更
コモンネーム/SANsの変更	可能 (注: 下記「費用」を参照)	不可
証明書有効期間終了日の変更	可能 (注: 指定可能な証明書有効期間終了日の制限について別紙「再発行(Reissue)申請時の証明書有効期間について」参照)	不可
費用	FQDN(SANs)を追加した場合、以下の式でユニットを消費 $\text{消費ユニット数} = \text{残プラン年数} \times \text{追加したSANsの数量}$ (お客様のご契約内容によって実際の費用については異なる場合があります)	<ul style="list-style-type: none"> ・なし
元証明書が失効されるか?	コモンネーム/SANsを変更/削除した場合、 元証明書は48-72時間以内に失効される	<ul style="list-style-type: none"> ・失効されない

cURLのサンプルコード(*1)

```
curl -X PUT \
'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/revoke' \
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}' \
-d '{
"comments": "I no longer need this cert.",
"skip_approval": true
}'
```

Method+Endpoint:

PUT

https://www.digicert.com/services/v2/order/certificate/{{order_id}}/revoke

・API Endpointとして指定するURLのうち上記部分にはorder_idを指定してください。

リクエスト : 主なパラメータ	説明	データ タイプ
comment	失効理由についてのコメント(例: 利用停止、秘密鍵の危殆化など)	String
skip_approval	True : 管理者による追加の「承認処理」をスキップし強制的に失効を完了させる False (未指定の場合はFalse): 失効処理を完了させるために、管理者による追加の「承認処理」が必要とする ※ 管理者による追加の「承認処理」はCertCentralの画面をご利用いただくか、当資料セクション5.2「Update Request Status」エンドポイントを活用ください。	Boolean

レスポンス : 主なフィールド	説明	データ タイプ
id	request_id (リクエストID)	Int
type	リクエストの種類(例: 失効リクエストの場合「revoke」)	String
status	リクエストのステータス(例: 失効リクエスト直後の場合「pending」)	String

もっと詳しく: <https://dev.digicert.com/services-api/orders/revoke-order-certificates/>

■ ご注意ください

・「**Revoke order certificates**」(当ページの内容): オーダ(プラン)単位の失効(無効化)をリクエストする要求。単一のオーダ(プラン)配下に複数の証明書が存在する場合、それら全ての証明書に対する失効およびプランの無効化がリクエストされます

・「**Revoke certificates**」(次ページの内容): 証明書単位の失効をリクエストする要求。単一のオーダ(プラン)配下に複数の証明書が存在する場合に、その中の単一の証明書に対して失効がリクエストされます

■ 単一のオーダ(プラン)に対して、複数の証明書を発行したイメージ

オーダー番号	日付	コモンネーム	ステータス
7986638 クイックビュー	24 Sep 2019	demo20190521.digice...	発行済
元の証明書	24 Sep 2019	demo20190521.digice...	発行済
002を複製	30 Sep 2019	demo20190521.digice...	発行済
001を複製	30 Sep 2019	demo20190521.digice...	発行済


詳細を表示

Revoke certificates : 証明書の失効(証明書単位)

cURLのサンプルコード(*1)

```
curl -X PUT \
'https://www.digicert.com/services/v2/certificate/{{certificate_id}}/revoke' \
-H 'Content-Type: application/json' \
-H 'X-DC-DEVKEY: {{api_key}}' \
-d '{
  "comments": "I no longer need this cert.",
  "skip_approval": true
}'
```

Method+Endpoint:



PUT https://www.digicert.com/services/v2/certificate/{{certificate_id}}/revoke

- API Endpointとして指定するURLのうち上記部分にはcertificate_idを指定してください。
- certificate_idはOrder Info, List Reissue, List Duplicate等にて参照・取得いただけます。

リクエスト : 主なパラメータ	説明	データタイプ
comment	失効理由についてのコメント(例: 利用停止、秘密鍵の危殆化など)	String
skip_approval	True: 管理者による追加の「承認処理」をスキップし強制的に失効を完了させる False (未指定の場合はFalse): 失効処理を完了させるために、管理者による追加の「承認処理」が必要とする ※ 管理者による追加の「承認処理」はCertCentralの画面をご利用いただくか、当資料セクション5.2「Update Request Status」エンドポイントを活用ください。	Boolean

レスポンス : 主なフィールド	説明	データタイプ
id	request_id (リクエストID)	Int
type	リクエストの種類(例: 失効リクエストの場合「revoke」)	String
status	リクエストのステータス(例: 失効リクエスト直後の場合「pending」)	String

もっと詳しく: <https://dev.digicert.com/services-api/certificates/revoke-certificate/>

補足 Revoke Certificateによるオーダ(プラン)の状態遷移について

- ・デフォルトの状態(下記アカウント設定[証明書失効(APIのみ)]が[個別証明書を失効にする]が選択された状態)の場合、前ページの「Revoke Certificate」エンドポイントを使用して、単一のオーダ(プラン)内の証明書を全て失効しても、オーダ(プラン)は「有効」状態のまま存置されます。この時、Reissueエンドポイントを用いて、同オーダ(プラン)内で追加で証明書を申請、発行および取得いただくことが可能です。
- ・単一のオーダ(プラン)内の証明書を全て失効した時にオーダー(プラン)が自動的に無効化されることを希望される場合は、下記アカウント設定[証明書失効(APIのみ)]について[全ての証明書が失効になると、オーダーが失効になります]を選択・保存してください。

■ [設定]->[選択設定]->[詳細設定]配下の[証明書失効]メニュー

証明書失効 (APIのみ) ?

個別証明書を失効にする ?

すべての証明書が失効になると、オーダーが失効になります ?

アカウント設定 [証明書失効(APIのみ)] 選択肢	Revoke Certificateの結果
個別証明書を失効にする (Revoke individual certificates)	単一のオーダ(プラン)内の証明書を全て失効しても オーダ(プラン)は「有効」状態のまま存置されます
すべての証明書が失効になると、 オーダーが失効になります (Revoke order when all certificates are revoked)	単一のオーダ(プラン)内の証明書を全て失効した時に オーダー(プラン)が自動的に無効化されます

8. プラン・証明書の有効期間、更新案内メールについて

【サーバ証明書(OV/EV)】新規プラン申請 - プランおよび証明書の有効期間

■サーバ証明書(OV/EV) 新規プラン申請の場合 - パラメーター指定方法によって設定されるプラン期間および証明書有効期間

プラン有効期間指定方法	必須/任意(優先順位)	指定値	付与されるプラン有効期間
order_validity	必須	-	-
years	-	1	370日間 (*1)
		2	735日間 (*1)
		3~6 (*2)	370 + (365*[指定した年数-1])
days	任意 (指定した場合yearsより優先)	プラン有効期間を日数で指定 最大値:2190 (*2)	指定した日数
custom_expiration_date	任意 (指定した場合yearsおよびdaysより優先)	[dd MMM YYYY]形式(例:[09 JUN 2021])で 有効期間終了日を指定 最大値:申請日から2190日後 (*2)	発行日(有効期間開始日) ~ 指定した日付(有効期間終了日)

証明書有効期間指定方法	必須/任意(優先順位)	指定値	付与される証明書有効期間
cert_validity	必須	-	-
years	-	1	370日間 (*1)
days	任意 (指定した場合yearsより優先)	証明書有効期間を日数で指定 最大値:プラン終了日までの日数または397(*3)のいずれか小さい方	指定した日数
custom_expiration_date	任意 (指定した場合yearsおよびdaysより優先)	[dd MMM YYYY]形式(例:[09 JUN 2021])で 有効期間終了日を指定 最大値:プラン終了日または397日後(*3)のいずれか早い方	発行日(有効期間開始日) ~ 指定した日付(有効期間終了日)

*1: 有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります

詳細はこちら: <https://docs.digicert.com/manage-certificates/setting-validto-time-certificates/#weekend-and-us-holiday-certificate-expiration-date-adjustments>

*2: ご契約内容によってご申請いただける最大のプラン期間は異なります。サブスクリプション契約をご締結いただいているお客様の場合は最大2年間となります。

*3: 業界団体CA/ブラウザフォーラムの決議に則り、2020年9月以降にデジサートが発行するパブリック証明書の最大有効期限は最大397日間となります。

【サーバ証明書(OV/EV)】 プラン更新 - プランおよび証明書の有効期間

■サーバ証明書(OV/EV)プラン更新申請の場合 - パラメーター指定方法によって設定されるプラン期間および証明書有効期間

プラン有効期間指定方法	必須/任意 (優先順位)	指定値	付与されるプラン有効期間												
			ベース期間 (a)	引き継ぎ分の加算期間 (b)	合計 (a+b)										
order_validity	必須	-	-	-	-										
years	-	1	370日間 (*1)	左列のベース期間(新規申請時と同等)に、以下の条件・計算式で算出される日数を加算します <table border="1" data-bbox="1375 514 2038 856"> <thead> <tr> <th>更新前プランの 残有効期間日数</th> <th>加算される日数</th> </tr> </thead> <tbody> <tr> <td>0以下(期限切れ)</td> <td>0</td> </tr> <tr> <td>1~30</td> <td>[残日数]x2 (=2~60)</td> </tr> <tr> <td>31~89</td> <td>30+[残日数] (=61~119)</td> </tr> <tr> <td>90</td> <td>120</td> </tr> </tbody> </table>	更新前プランの 残有効期間日数	加算される日数	0以下(期限切れ)	0	1~30	[残日数]x2 (=2~60)	31~89	30+[残日数] (=61~119)	90	120	370 ~ 490日間 (*1)
		更新前プランの 残有効期間日数	加算される日数												
		0以下(期限切れ)	0												
		1~30	[残日数]x2 (=2~60)												
31~89	30+[残日数] (=61~119)														
90	120														
2	735日間 (*1)	735 ~ 855日間 (*1)													
3~6 (*2)	370 + (365*[指定した年数-1])	(a) + [0~120]日間													
days	<新規申請時と同様>														
custom_expiration_date	<新規申請時と同様>														

証明書有効期間指定方法	必須/任意(優先順位)	指定値	付与される証明書有効期間
cert_validity	必須	-	-
years	-	1	上記プラン期間に[years:1]指定時と同一、ただし 最大値:397日間(*3)
days	<新規申請時と同様>		
custom_expiration_date	<新規申請時と同様>		

*1: 有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります

詳細はこちら: <https://docs.digicert.com/manage-certificates/setting-validto-time-certificates/#weekend-and-us-holiday-certificate-expiration-date-adjustments>

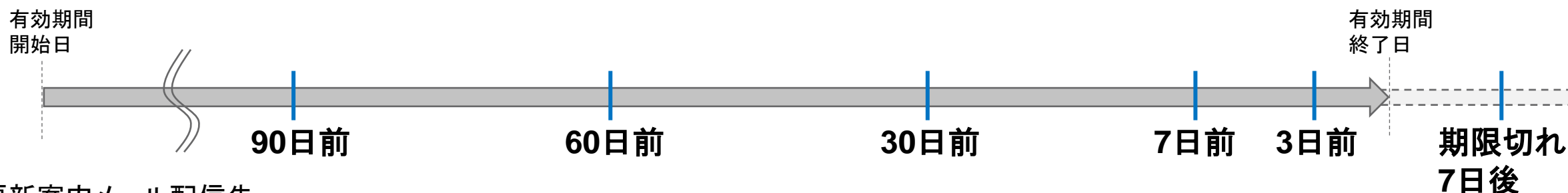
*2: ご契約内容によってご申請いただける最大のプラン期間は異なります。サブスクリプション契約をご締結いただいているお客様の場合は最大2年間となります。

*3: 業界団体CA/ブラウザフォーラムの決議に則り、2020年9月以降にデジサートが発行するパブリック証明書の最大有効期限は最大397日間となります。

更新案内メールについて (1/2 メール配信タイミング・配信先)

■更新案内メール配信タイミング

更新案内メールは、以下図中の6回のタイミングで配信されます(標準設定の場合)
尚、アカウントメニュー「設定」→「選択設定」にて一部または全部のタイミングについてON/OFFを選択可能



■更新案内メール配信先

#	配信先	説明	設定
1	[アカウント設定] 「更新申請通知の送付先」	アカウント単位で任意のメールアドレス(固定)を指定可能 (複数設定可能)	アカウントメニュー「設定」→「選択設定」にて 「 <u>証明書の更新設定</u> 」セクション内「 <u>更新申請通知の送付先</u> 」欄 にメールアドレスを設定した場合、このアドレスに対して配信
2	[アカウント設定] 「設定」→「通知」→「全通知の送信先」	アカウント単位で任意のメールアドレス(固定)を指定可能 (複数設定可能)	アカウントメニュー「設定」→「通知」にて 「 <u>すべてのアカウント通知を以下に送信</u> 」欄にメールアドレスを 設定した場合、このアドレスに対して配信
3	[オーダー(証明書申請)別パラメータ] User Placing Order/申請者	オーダー(証明書申請)を実行したCertCentralの ユーザーアカウントに紐づいたメールアドレス	アカウントメニュー「設定」→「通知」にて 「 <u>Send emails to user placing order</u> 」欄のチェックボックスを ONにした場合に配信
4	[オーダー(証明書申請)別パラメータ] Additional Emails/メールの追加送信先	オーダー(証明書申請)時に、「メール送信先の 追加(Additional Emails)」欄に指定したメールアドレス (複数設定可能)	オーダー(証明書申請)時の入力欄「 <u>その他のオーダーオプション</u> 」→ 「 <u>メール送信先の追加</u> 」欄にメールアドレスを設定した場合、 このアドレスに対して配信

更新案内メールについて (2/2 メールテンプレート)

■ 更新案内メールのサンプル

→更新案内メール件名、送信元および本文イメージは、以下のようになります

件名	[重要]証明書更新のご案内 N日間 (オーダー番号 XXXXXXXXX)
送信元	DigiCert <admin@digicert.com>
本文 イメージ (抜粋)	<p>[証明書の申請者 氏名] 様</p> <p>弊社サービスをご利用いただき誠にありがとうございます。現在ご利用の証明書の有効期間は、残りN日間となりました。有効期間が切れる前に証明書の更新申請をいただきますようお願いいたします。</p> <p>証明書詳細</p> <p>ご申請者：[証明書の申請者 氏名] コモンネーム：[証明書のSubject CN] [オーダー詳細画面へのURL(ログイン要)]にアクセスして証明書を更新ください。</p> <p>更新のお手続き</p> <p>事前に証明書を更新いただくことにより、現在の証明書の残日数を新しい証明書に追加して発行いたします。費用は発生しません。無駄なくご利用いただけますので是非お早めにご申請ください。また、証明書をWindowsサーバにインストールしている場合には、更新する前にCSRを新しく生成してください。</p> <p>お客様が管理者の場合には、アカウントの通知設定で更新通知をカスタマイズすることが可能です。ご活用ください。 https://www.digicert.com/secure/preferences/</p> <p>管理者からのメモ：</p> <p>[*1：アカウント設定:カスタム更新案内通知(既定の更新メッセージ)]</p>

※：上記本文イメージ内に“[”および“]”で囲んだ範囲はお客様固有の申請情報等が記載されます

*1：アカウントメニュー「設定」→「選択設定」内の「証明書の更新設定」セクション下の「既定の更新メッセージ」に設定したテキストが埋め込まれます。