CertCentral API活用方法の解説資料

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. サーバ証明書(OV/EV)の申請 :page 11
   3.1 ワークフロー概要 :page 11
   3.2 サーバ証明書(OV/EV) の申請 :page 16
   3.3 ドメイン名利用権確認(DCV) :page 33
   3.4 組織およびドメイン名の管理 :page 41
4. サーバ証明書(DV)の申請 :page 50
   4.1 ワークフロー概要 :page 50
   4.2 サーバ証明書(DV)の申請 :page 55
5. オーダー管理、リクエスト管理 :page 69
   5.1 オーダー管理 :page 69
   5.2 (OV/EV証明書のみ)リクエスト管理 :page 77
6. 発行された証明書の取得 :page 82
7. 再発行、複製、失効等の証明書管理 :page 88
8. プラン・証明書の有効期間・更新案内メールについて :page 97

1. はじめに

はじめに

- 当資料は CertCentral Partner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 Partner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 Partner利用ガイド(コンソール編)
    - URL：https://www.digicert.co.jp/sid-partner/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/EV証明書およびDV証明書の両方を取り扱う
  - 「都度認証」(各証明書申請のタイミングでDCVを実施する)方式を中心に扱う
    (不特定多数のエンドユーザの申請を扱うためOV/EV証明書の「事前認証」方式は参考との位置づけ)

    ＜「都度認証」方式とは？＞： 各証明書申請のタイミングで組織情報およびドメイン名を登録し、その都度、組織認証ならびにDCV(ドメイン名利用権確認)を実施する方式

    ＜(参考)「事前認証」＞ 証明書申請に先立ってアカウント内に組織情報およびドメイン名を登録し、組織認証ならびにDCV(ドメイン名利用権確認)を事前に済ませておくことで、その認証履歴の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方式

変更履歴

Ver.	公開日	変更点	変更箇所
~0.9	2020/8/5	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. サーバ証明書(OV/EV)の申請]「複数年プラン」について追記、DCVメール(日本語)文面など、多数改訂	Page 11-49
		[4. サーバ証明書(DV)の申請]「複数年プラン」について追記など、多数改訂	Page 50-68
		[5. オーダー管理、リクエスト管理] 「複数年プラン」について追記	Page 70
		[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 82-87
		[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 87-96
		[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 97-101

※ 変更点、変更箇所を表すセクション番号やページ数は改訂当時のものです。セクション番号やページ数は必要に応じて順次変更される場合があります。

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

※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

ルート1
(全ての
ユーザー)

トップ画面

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

ルート2
(管理者
専用)

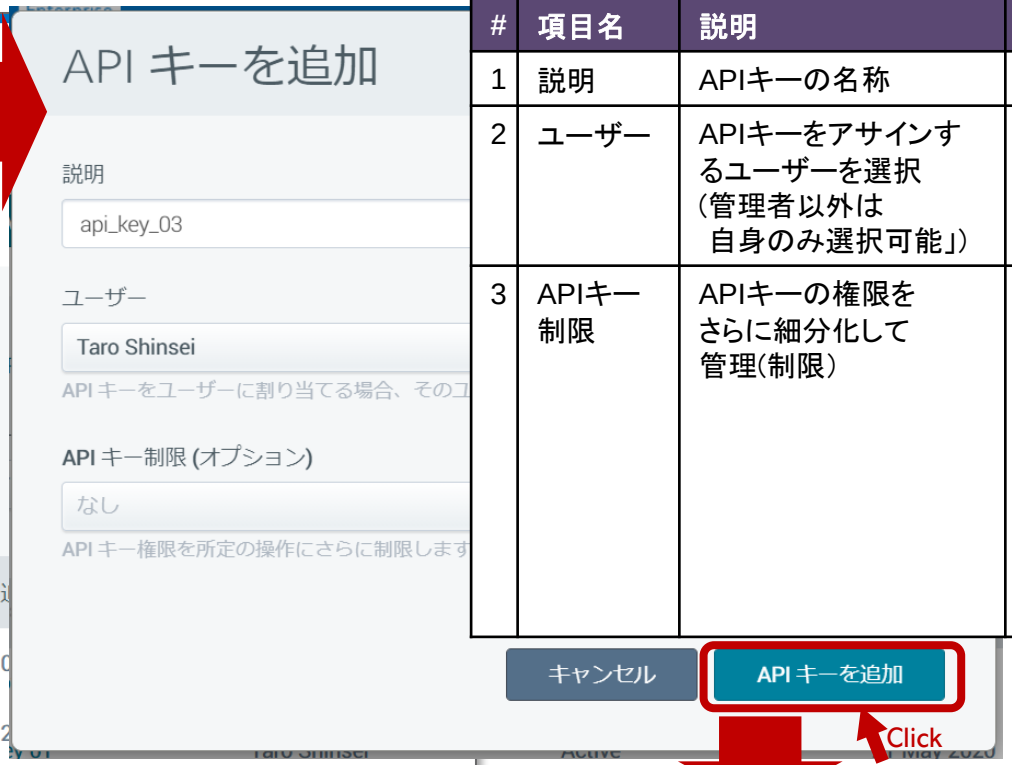
トップ画面

APIキー管理画面

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キーの追加(作成)・確認

■「APIキー」管理画面



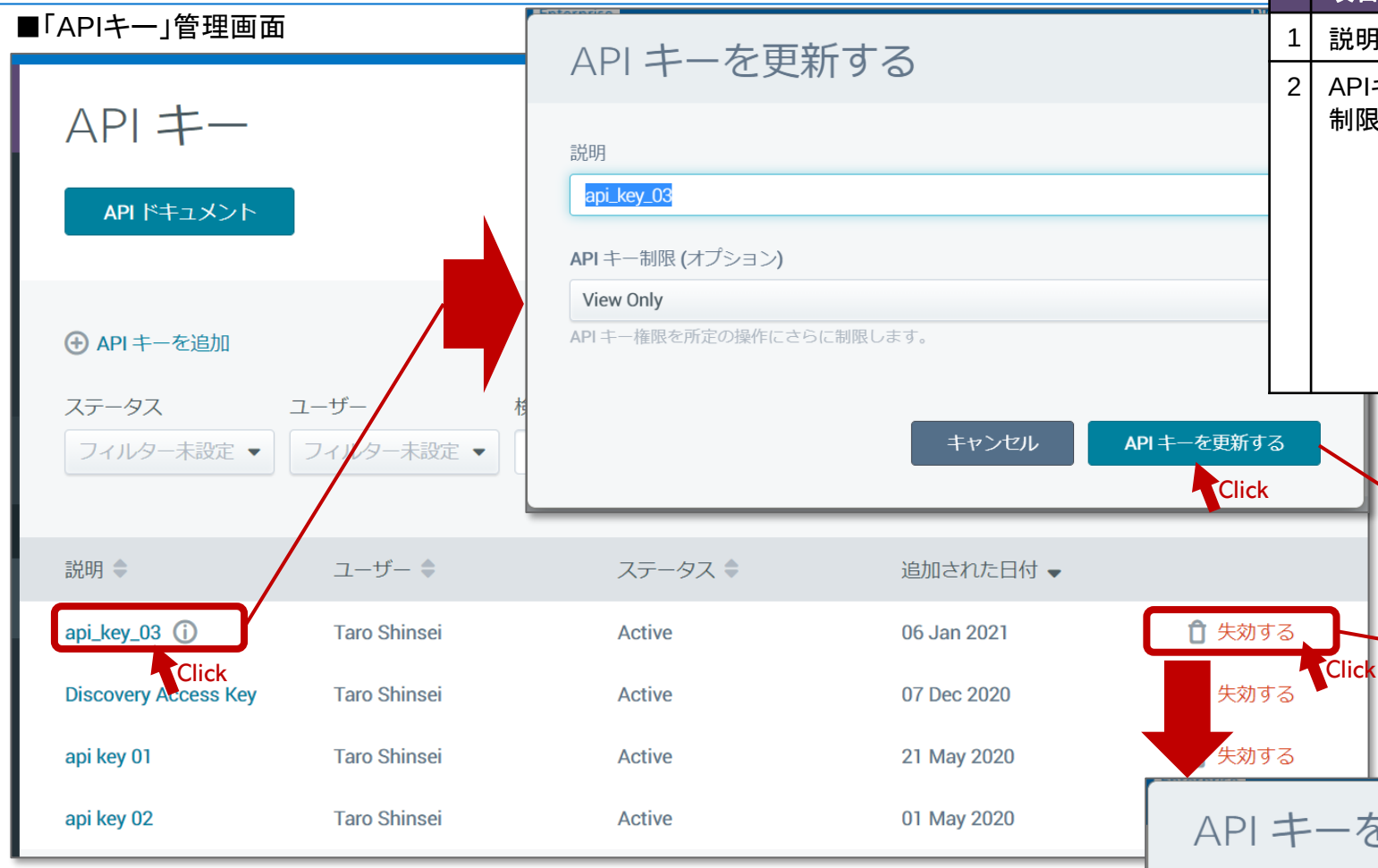
■APIキー追加(作成)時の入力/選択項目

#	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)	「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

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。

APIキーの更新・無効化

■「APIキー」管理画面



■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出来ます。

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

3. サーバ証明書(OV/EV)の申請

~ 3.1 ワークフロー概要 ~

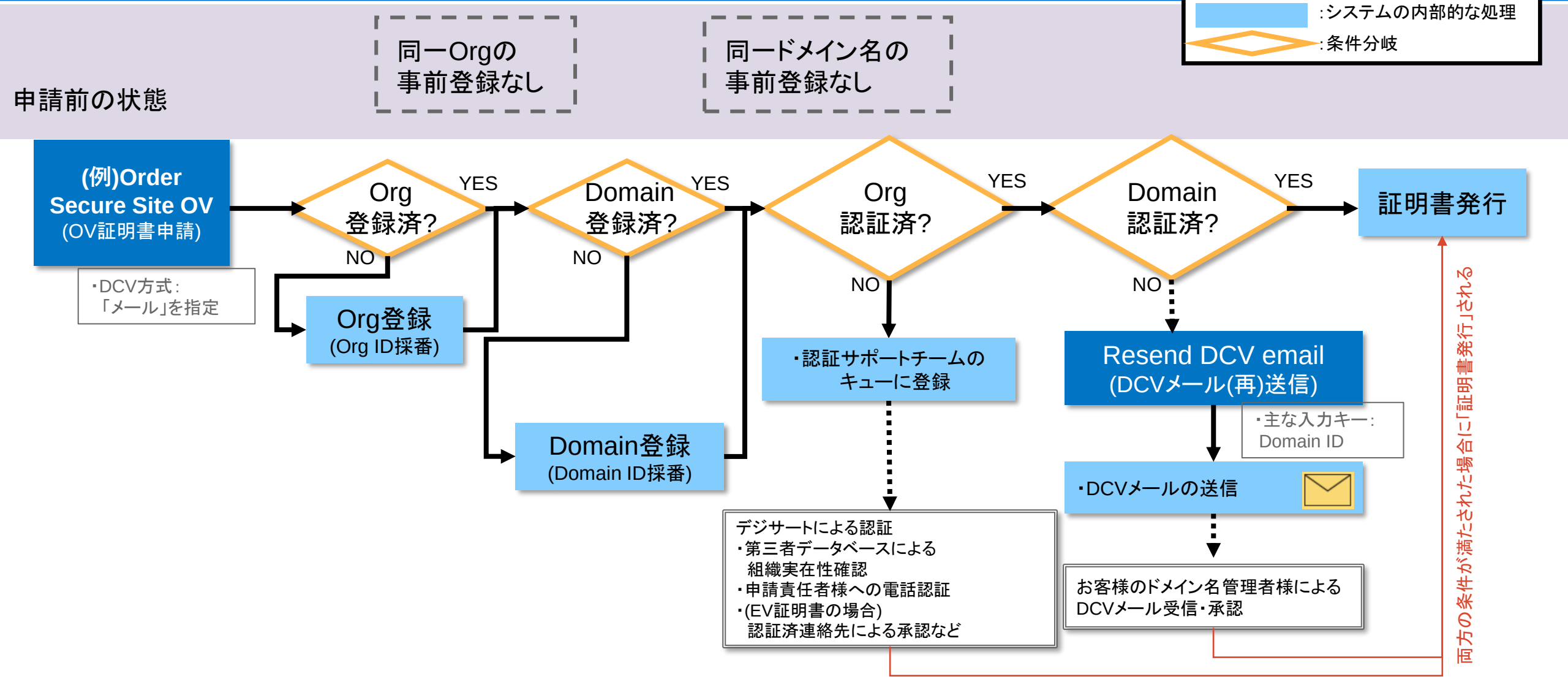
CertCentral APIによるOV/EV証明書の申請ワークフロー概要
(「都度認証」方式、DCV方式：メール認証の場合)

タスク概要		内容	CertCentral API		エンドユーザ企業	
			API	備考	申請責任者	ドメイン名管理者
エンドユーザ様からの申請受付・確認		・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて) 申請責任者様の確認、事前調整 ・(必要に応じて)ドメイン名管理者の確認、事前調整	特にAPI操作不要		N/A	N/A
証明書の申請		・APIを通じてプランのお申込み(証明書を申請) ・レスポンスでorg_id、domain_idを取得	(例)Order Secure Site OV	セクション 3.2 参照	N/A	N/A
申請レビュー・承認		(アカウント単位の設定で省略可) ・管理者が申請内容を確認し、承認または却下	Update request status	省略	N/A	N/A
認証	オーダーの認証情報確認	・オーダー認証ステータスを確認 ・オーダーに紐づくorg_id、domain_idを(再)確認	Validation status	セクション 3.2 参照	N/A	N/A
認証	組織(Org)認証	・デジサートにて認証を開始(第三者データベースによる組織実在性確認、申請責任者様への電話認証など) ・(EV証明書の場合)認証済連絡先による承認など	-		認証へのご対応	N/A
認証	ドメイン利用権確認(DCV)	・ DCVメール宛先の選択・(再)送信	Resend DCV email		N/A	DCVメール受信・承認
認証	ステータス確認	・個別オーダのステータス(発行済か否か)をチェック	Order Info	セクション 5 参照	N/A	N/A
認証	ステータス確認	・指定した時間内にステータスが変更したオーダーを検索 (例:30分以内に「発行済」となったオーダー)	Status change list		N/A	N/A
証明書の取得		・発行された証明書を形式を指定して取得(ダウンロード)	Download certificate	セクション 6 参照	N/A	N/A

CertCentral APIによるOV/EV証明書の申請ワークフロー概要
(「都度認証」方式、DCV方式：ファイル認証/DNS認証の場合)

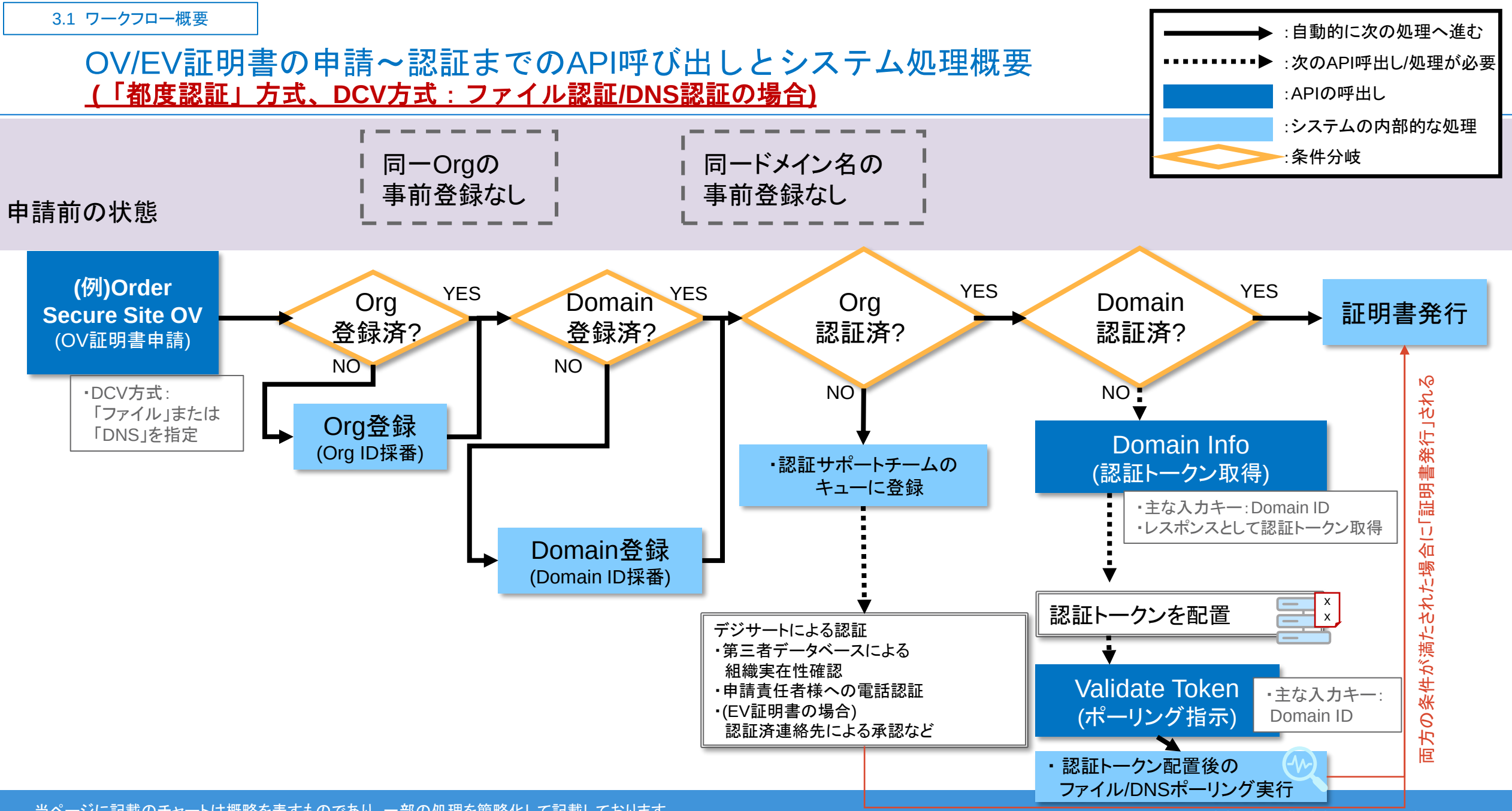
タスク概要		内容	CertCentral API		エンドユーザ企業	
			API	備考	申請責任者	ドメイン名管理者
エンドユーザ様からの申請受付・確認		・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて) 申請責任者様の確認、事前調整	特にAPI操作不要		N/A	N/A
証明書の申請		・APIを通じてプランのお申込み(証明書を申請) ・レスポンスでorg_id、domain_idを取得	(例)Order Secure Site OV	セクション 3.2 参照	N/A	N/A
申請レビュー・承認		(アカウント単位の設定で省略可) ・管理者が申請内容を確認し、承認または却下	Update request status	省略	N/A	N/A
認証	オーダーの認証情報確認	・オーダー認証ステータスを確認 ・オーダーに紐づくorg_id、domain_idを(再)確認	Validation status	セクション 3.2 参照	N/A	N/A
認証	組織(Org)認証	・デジサートにて認証を開始(第三者データベースによる組織実在性確認、申請責任者様への電話認証など) ・(EV証明書の場合)認証済連絡先による承認など	-		認証へのご対応	N/A
認証	ドメイン利用権確認(DCV)	・認証トークンの取得・配置	Domain Info		N/A	N/A
認証	ドメイン利用権確認(DCV)	・ファイル/DNS認証のための(再)ポーリング指示	Check DCV(OV/EV)			
認証	ステータス確認	・個別オーダのステータス(発行済か否か)をチェック	Order Info	セクション 5 参照	N/A	N/A
認証	ステータス確認	・指定した時間内にステータスが変更したオーダーを検索 (例:30分以内に「発行済」となったオーダー)	Status change list			
証明書の取得		・発行された証明書を形式を指定して取得(ダウンロード)	Download certificate	セクション 6 参照	N/A	N/A

OV/EV証明書の申請～認証までのAPI呼び出しとシステム処理概要
(「都度認証」方式、DCV方式：メール認証の場合)



当ページに記載のチャートは概略を表すものであり、一部の処理を簡略化して記載しております。
セキュリティ、コンプライアンスの理由から上記に記載がない、追加の確認などが必要となるケースがあります。ご理解・ご了承ください。

OV/EV証明書の申請～認証までのAPI呼び出しとシステム処理概要
(「都度認証」方式、DCV方式：ファイル認証/DNS認証の場合)



当ページに記載のチャートは概略を表すものであり、一部の処理を簡略化して記載しております。
セキュリティ、コンプライアンスの理由から上記に記載がない、追加の確認などが必要となるケースがあります。ご理解・ご了承ください。

3. サーバ証明書(OV/EV)の申請

~ 3.2 サーバ証明書(OV/EV)の申請 ~

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)

```
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		
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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

[別紙] product_id(製品識別子)一覧

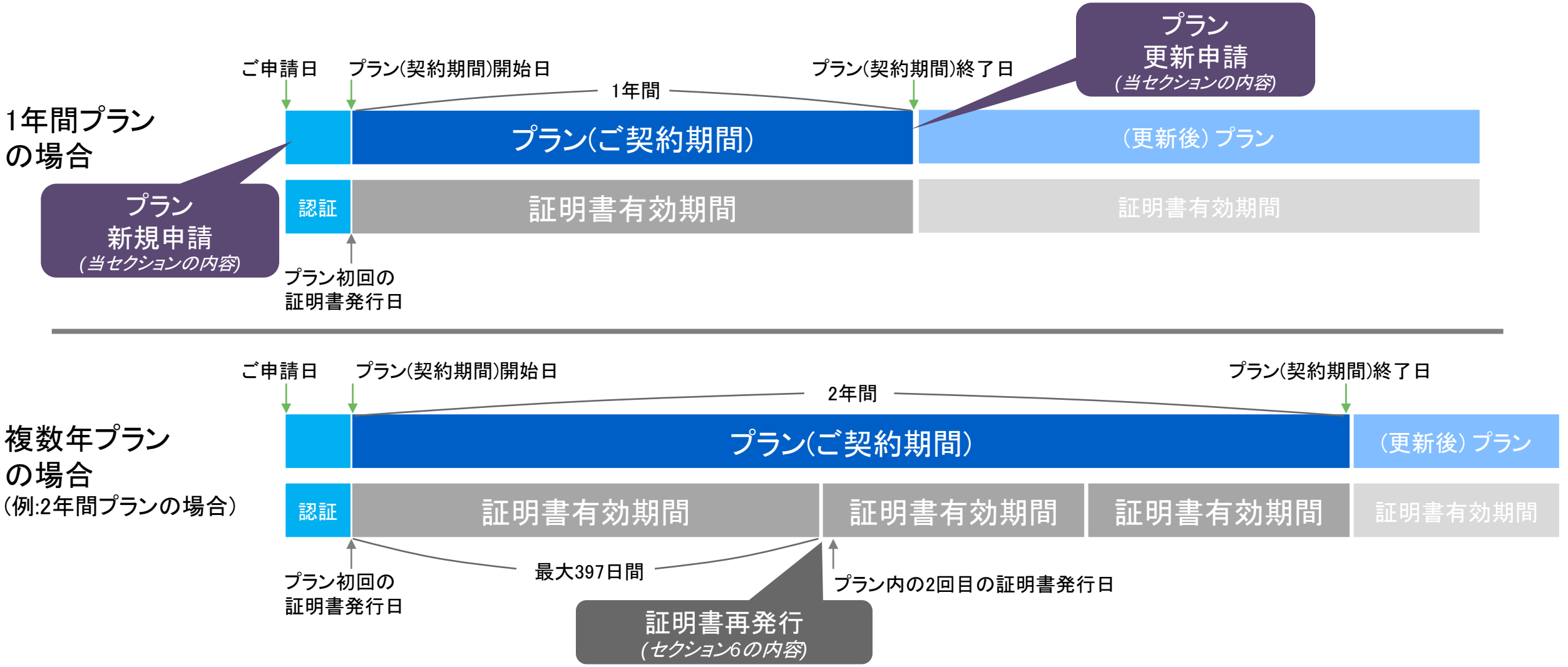
```
POST  https://www.digicert.com/services/v2/order/certificate/{{product_id}}
```

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	
	スタンダード・サーバID EV	Basic EV	ssl_ev_basic	
	ジオトラスト トゥルービジネスID with EV	GeoTrust TrueBusiness ID EV	ssl_ev_geotrust_truebizid	
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	
	スタンダード・サーバID	Basic OV	ssl_basic	
	ジオトラスト トゥルービジネスID	GeoTrust TrueBusiness ID OV	ssl_geotrust_truebizid	

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	・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。
複数年プラン(2年間~6年間)	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	・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 〇プランの期間:order_validity .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。 〇証明書の有効期間:certificate.cert_validity .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。

[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きます
・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

・「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きます
・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■>/ ＞

Order Secure Site OV ： セキュア・サーバIDの新規申請 (続き)

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
証明書申請について組織(Org)とドメイン(Domain)の(事前)認証が完了していない場合

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

```
{
   "id": 19188494,
   "organization": {
     "id": "816532"
   },
   "domains": [
      {
      "id": 1738406,
      "name": “new-domain.example.com"
      }
   ],
   "certificate_id": 19947412
}
```

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
organization	(証明書申請時に新規の組織(Org)が登録された場合のみ	**Object**
id	組織(Org)のID	Int
domains	(証明書申請時に新規のドメイン(Domain)が登録された場合のみ (複数の場合は複数回繰り返し)	**Object**
id	ドメイン(Domain)のID	Int
name	ドメイン(Domain)名	
certificate_id	certificate_id (証明書オブジェクトを示す識別子)	Int

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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

Order Secure Site OV ： セキュア・サーバIDの新規申請 (続き)

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

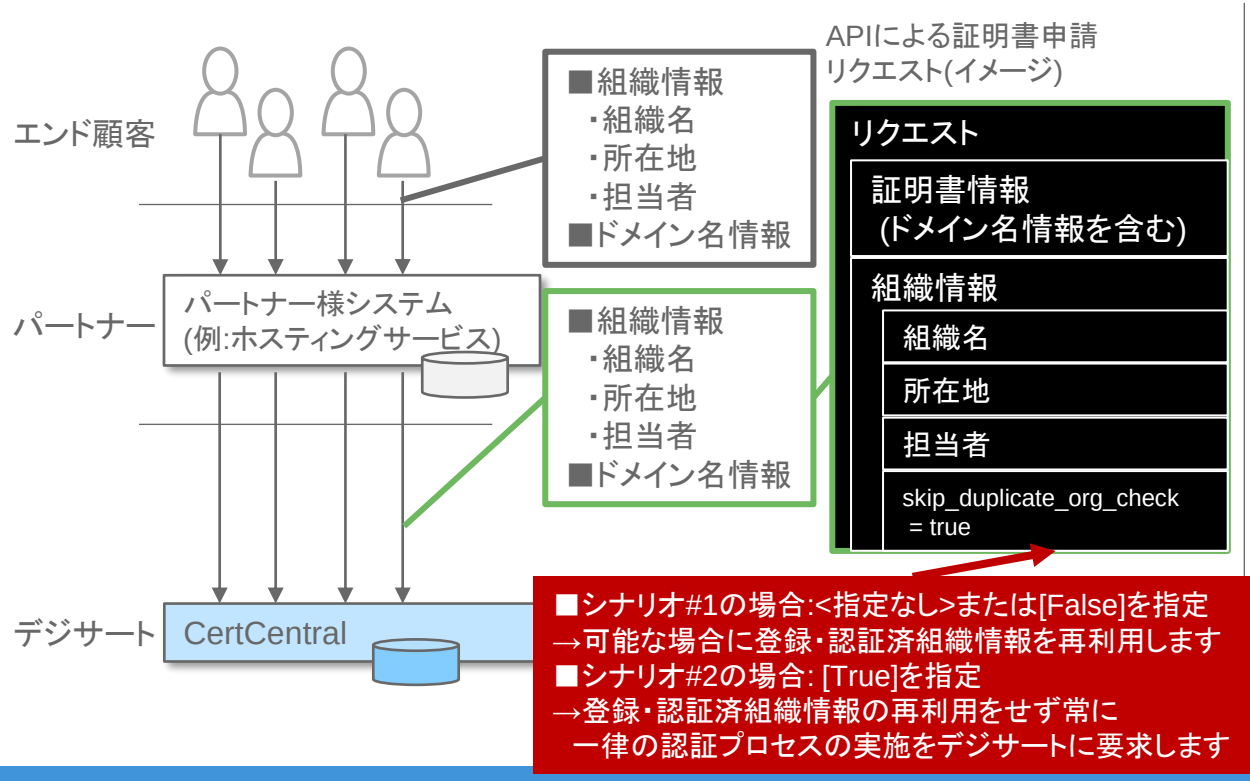
もっと詳しく: https://dev.digicert.com/services-api/orders/order-secure-site-ov/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

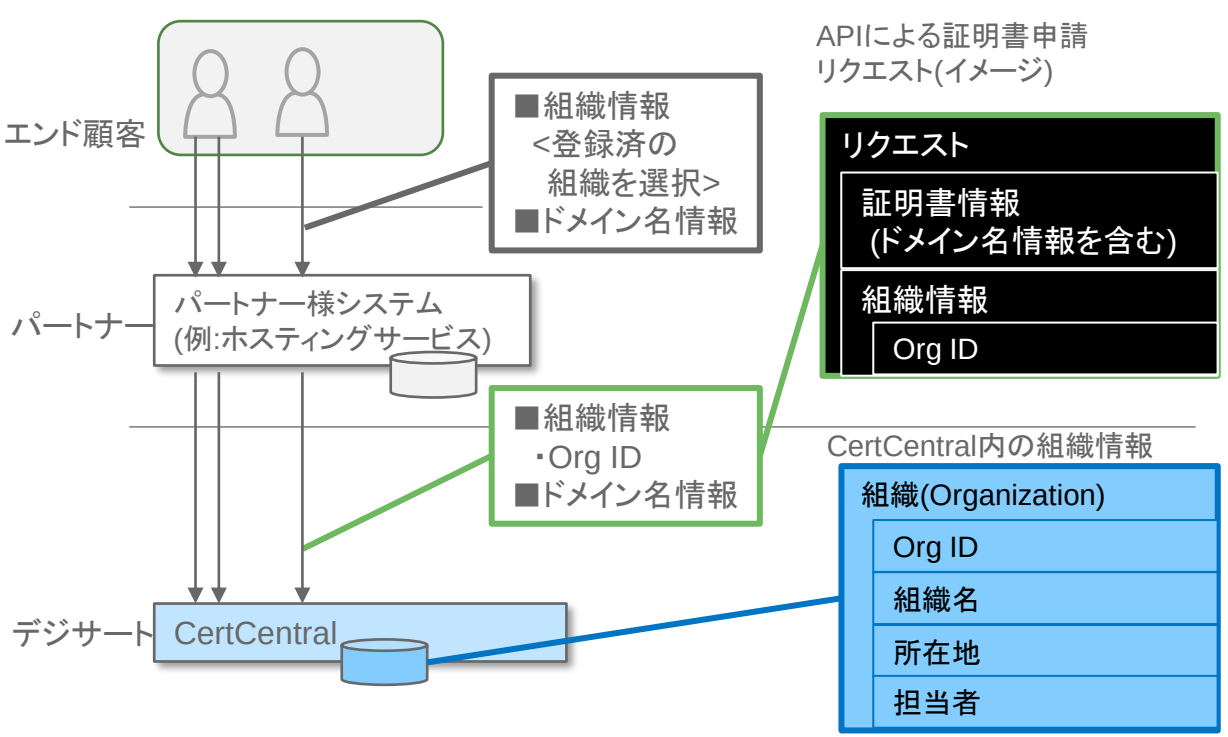
OV/EV証明書の申請における組織情報の再利用について

●CertCentral APIを通じたOV/EV証明書の申請時ににおける登録・認証済の組織情報の再利用要否について、以下のシナリオからご選択いただけます
シナリオ #1. 可能な場合に登録・認証済の組織情報を再利用(*1)をデジサートに許可する形で、不特定多数の組織に対してOV/EV証明書を申請する
シナリオ #2. 登録・認証済の組織情報を再利用せず、不特定多数の組織に対するOV/EV証明書申請時に、常に一律の認証実施をデジサートに要求する
シナリオ #3. 特定の組織情報をパートナー様システム上に登録・管理し、登録・認証済の組織情報を指定してOV/EV証明書を申請する
●上記シナリオ#1-3を併存させることも可能(例：大手エンド顧客には#3を、それ以外の不特定多数のエンド顧客には#1を適用する等)
●それぞれのシナリオにおける証明書申請時の"Organization"オブジェクトの指定方法については以下を参照ください

■シナリオ #1 / #2. 不特定多数の組織/申請団体に対する証明書申請(イメージ)



■シナリオ #3. 登録済の特定組織/申請団体を指定した証明書申請(イメージ)



*1：証明書申請時の組織(Organization)データのうち「組織名(name)」「国名(Country)」「都道府県(State)」および「市区町村(City/Locality)」の全てが登録済組織データと合致した場合、同一の組織(申請団体)に対する証明書申請と見なします。

[別紙] 組織(Org)情報の入力方法 (1/2 組織情報)

■[シナリオ #1 / #2. OV/EV証明書申請時に組織情報を入力する]場合のリクエスト(イメージ)

```
"organization": {
  "name": "OrgName Co., Ltd",
  "address": "6-10-1 Ginza",
  "city": "Chuo-ku",
  "state": "Tokyo",
  "country": "JP",
  "zip": "1040061",
  "telephone": "0312345678",
  "contacts": [
    {
      "contact_type": "organization_contact",
      "first_name": "Taro",
      "last_name": "Shinsei",
      "job_title": "Manager",
      "email": "taro.shinsei@digicert.com",
      "telephone": "81312345678"
    },
    {
      "contact_type": "ev_approver",
      "first_name": "Jiro",
      "last_name": "EV",
      "job_title": "EV Tantou",
      "email": "jiro.ev@digicert.com",
      "telephone": "81312345680"
    }
  ]
}
```

セクション1 組織情報

セクション2 担当者情報

■セクション1：組織情報の入力項目の説明・入力/選択例

フィールド名	項目名(日本語)	概要	入力/選択例
name	正式名称	【証明書のSubject O】 申請団体の正式名称 (日本語、英語いずれも可)	・<日本語組織名の場合>: デジサート・ジャパン合同会社 ・<英語組織名の場合>: DigiCert Japan G.K.
assumed_name	一般名称	<入力不要>	
country	国	【証明書のSubject C】 「Japan」を選択	Japan
address	住所1	申請団体所在地・市区町村より下のレベル（番地等）	例1：6-10-1 Ginza 例2：580-16 Horikawa-cho
address2	住所2	<入力不要>	
city	市町村名	【証明書のSubject L】 申請団体所在地・市区町村	例1：Chuo-ku 例2：Kawasaki-shi
state	State / Province / Region	【証明書のSubject S】 申請団体所在地・都道府県	例1：Tokyo 例2：Kanagawa
zip	Zip / Postal Code	申請団体所在地・郵便番号	104-0061
telephone	組織の電話番号	申請団体の電話番号	03-XXXX-XXXX
skip_duplicate_org_check	(詳細は前ページ参照)	■[False]を指定した場合： →可能な場合に登録・認証済組織情報を再利用します(デフォルト値) ■ [True]を指定した場合： →登録・認証済組織情報の再利用をせず常に一律の認証プロセスの実施をデジサートに要求します	True または False

※ 以下の項目には日本語（ひらがな、カタカナ、漢字）を利用いただくことが可能です ： 正式名称★、住所1、住所2、市町村名★、State(都道府県名)★
ただし上記のうち「★」印の項目はSSL/TLSサーバ証明書に記載され、ウェブサイトを訪問されたエンドユーザ様が鍵マークをクリックした際などに目に触れる項目となますので、お客様のウェブサイトの特性としてグローバル向けにサービスを行うようなケースではアルファベットをご利用いただくことを推奨しております。

[別紙] 組織(Org)情報の入力方法 (2/2 担当者情報)

■[シナリオ #1 / #2. OV/EV証明書申請時に組織情報を入力する]場合のリクエスト(イメージ)

```
"organization": {
  "name": "OrgName Co., Ltd",
  "address": "6-10-1 Ginza",
  "city": "Chuo-ku",
  "state": "Tokyo",
  "country": "JP",
  "zip": "1040061",
  "telephone": "0312345678",
  "contacts": [
    {
      "contact_type": "organization_contact",
      "first_name": "Taro",
      "last_name": "Shinsei",
      "job_title": "Manager",
      "email": "taro.shinsei@digicert.com",
      "telephone": "81312345678"
    },
    {
      "contact_type": "ev_approver",
      "first_name": "Jiro",
      "last_name": "EV",
      "job_title": "EV Tantou",
      "email": "jiro.ev@digicert.com",
      "telephone": "81312345680"
    }
  ]
}
```

セクション1 組織情報

セクション2 担当者情報

■セクション2：担当者情報の入力項目の説明・入力/選択例

フィールド名	項目名	概要	入力例
contacts			
contact_type	担当者種別	「organization_contact(申請担当者)」、「technical_contact(技術担当者)」または「ev_approver(認証済連絡先)」から選択 (下表参照)	
first_name	名	担当者氏名の名	Taro (※1)
last_name	氏	担当者氏名の氏	Ninsho (※1)
Email	役職名	担当者の役職名	Manager (※1)
job_title	メール	担当者の電子メールアドレス	taro.ninsho@digicert.com
Telephone	電話番号	担当者の電話番号	03-XXXX-XXXX

	役割	必須/任意
申請責任者 (Organization Contact)	・CertCentralで発行する証明書の発行対象となる組織(Subject O)を代表し、証明書を申請する権限を持つ責任者です。	任意 省略した場合、「申請者(APIキー所有者)」を申請責任者として割り当てます
技術担当者 (Technical Contact)	・申請責任者のサポート役となる担当者 ・オーダーの登録内容の確認、書類等のご提出依頼など、認証のために確認事項がある場合の連絡先窓口となります。	任意 省略した場合、申請責任者を連絡先窓口と見做します
認証済連絡先 (Verified Contact)	・申請団体を代表してEV証明書発行を承認する担当者 ・デジサートより在籍および承認権限を確認します ・認証済連絡先は、EV証明書が申請された場合に、その都度、申請を承認いただきます(詳細後述)	EV証明書申請の場合、必須

※1：該当項目には日本語（ひらがな、カタカナ、漢字）での入力も可能です。

[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

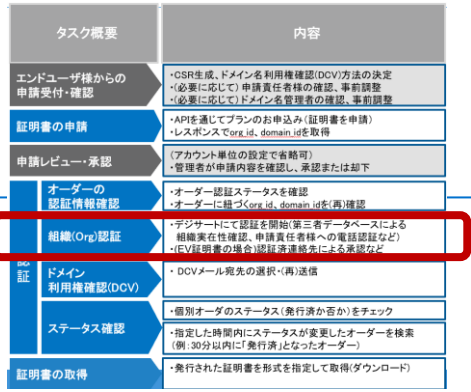
```
{
  "containers": [
    {
      "id": 129626,
      "public_id": <ユニークな値>,
      "name": "Win The Customer, LLC",
      "parent_id": 0,
      "template_id": 5,
      "ekey": <ユニークな値>
      "has_logo": false,
      "is_active": true
    },
```

・List Containersエンドポイントで一覧を確認可能できます
・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

・「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きます
・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■>/ ＞

(OV証明書の場合) 組織(Org)認証の流れ



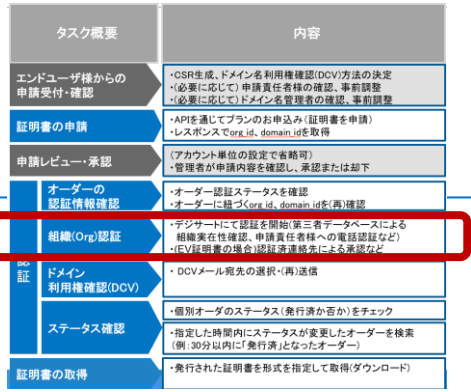
■OV証明書の申請時に必要となる組織(Org)認証の手続きは以下のようになります。
・過去の証明書申請・発行履歴、または「事前認証」の有無によって組織(申請団体)の担当者様へのご連絡の有無や内容が異なりますので、ご注意ください。

証明書を申請する組織(申請団体)における「有効(再利用可能)なOV認証履歴」の有無

	申請責任者への連絡	技術担当者への連絡
有り の場合	原則として、ご連絡はありません。	
無し の場合	■ご連絡内容： ・**電話認証** (規定のデータベースで確認した組織(申請団体)の電話番号による証明書申請の意思確認 (*1)	■連絡内容： ・**登録内容の確認** ・**書類等のご提出依頼** (いずれも必要な場合のみ、*1)

*1：「電話認証」や書類認証の詳細については**「FAQ ： 実施する「認証」の詳細について」**を参照ください
https://knowledge.digicert.com/ja/jp/solution/SO23253

(EV証明書の場合のみ) 追加ステップ「認証済連絡先による承認」



■EV証明書の申請時には、前ページの「組織認証」に加えて、追加ステップとして
「認証済連絡先の認証」および**「(認証済連絡先による)EV証明書申請の承認」**が必要です。
以下をご参照の上、パートナー様におかれましては申請団体の認証済連絡先の担当と
連携の上、ご対応をお願いいたします。

追加STEP 1: 認証済連絡先の認証

EV証明書を申請する組織(申請団体)における「認証済連絡先」の有無

無しの場合	認証済連絡先の認証を行います。 ■ご連絡内容： ・**電話認証** (規定のデータベースで確認した組織(申請団体)の電話番号から認証済連絡先の在籍および権限を確認)
有りの場合	<追加STEP 2に進みます>

追加STEP 2: (認証済連絡先による)EV証明書申請の承認

EV証明書の申請の都度、認証済連絡先のメールアドレスへ送信される
「承認申請メール」の件名、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	DigiCert 証明書発行に関わる承認確認依頼 オーダー番号（[オーダー番号]、Organization name [組織名]
送信元	DigiCert <admin@digicert.com>
本文イメージ(抜粋)	[<認証済連絡先>氏名] 様 デジサートでは、申請組織 [組織名] 様の証明書の申請を受付けました。 証明書の発行には、本Eメールの宛先となるご担当者様に承認をいただく必要がございます。 以下の承認サイトにアクセスいただき、内容をご確認のうえ承認操作をお願いいたします。: https://www.digicert.com/link/approve-order.php? [オーダー固有のトークン]&order_id=[オーダー番号] Click 内容についてご不明な点がございましたら、 DigiCertサポートまでお問い合わせください。 ご対応の程、よろしくお願いいたします。

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が異なってい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い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

OV/EV証明書：プラン/証明書の更新申請

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 years/ days/ custom_expiration_date	【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	-
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 years/ days/ custom_expiration_date	【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	-
renewal_of_order_id	更新元プラン/証明書のオーダーIDを指定	
renewed_thumbprint	更新元プラン/証明書の証明書ハッシュ値	

プラン更新申請の場合、いずれか一方が必須

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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

3. サーバ証明書(OV/EV)の申請

~ 3.3 ドメイン名利用権確認(DCV) ~

[別紙] 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	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。 ■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] (※1) ■送信元アドレス：no-reply@digitalcertvalidation.com (OV/EV証明書の場合) または no-reply@geotrust.com (DV証明書の場合)
ファイル認証	http-token	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。 ■設置場所：http://<確認対象のドメイン名>/.well-known/pki-validation/fileauth.txt
DNS TXT認証	dns-txt-token	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。 ■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	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。 ■設置例：<認証トークン>.<確認対象のドメイン名> CNAME dcv.digicert.com

※1：本資料作成時点で、OV/EV証明書のDCVメールの言語は英語のみとなります。順次「日本語」への対応を予定しております。

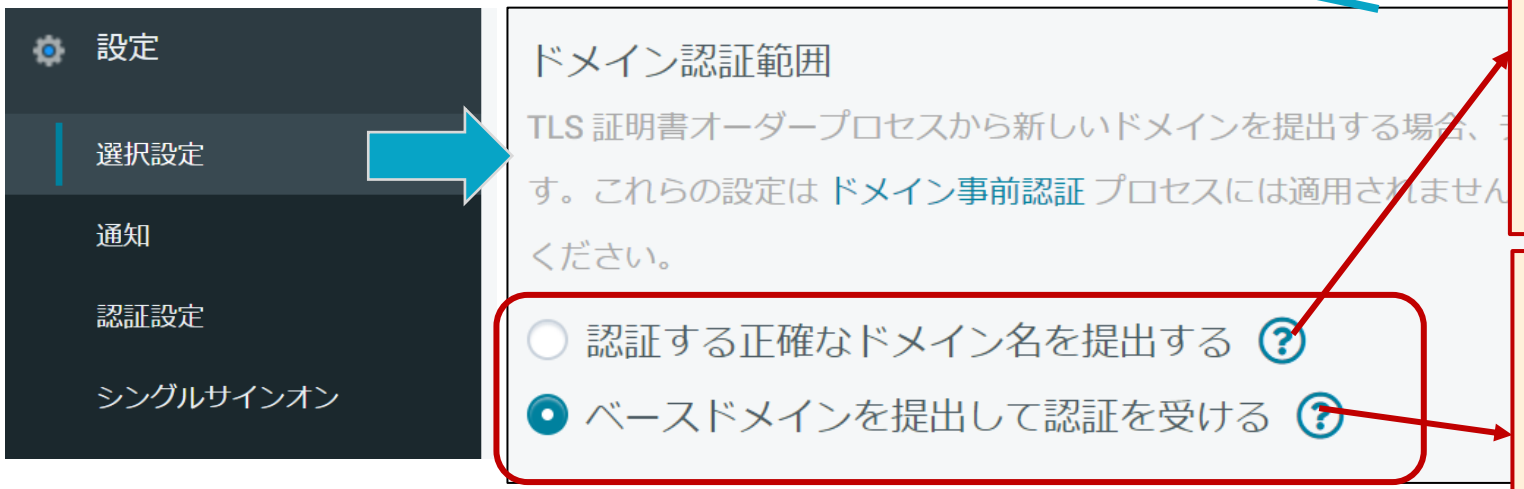
各DCV方式の詳細 – 「メール認証」の場合 (1/3 : 送信先の選択ルール)

■OV/EV証明書のDCVメールの送信先は以下の組み合わせによって決定されます。

A:アカウント設定「ドメイン認証範囲」 ✖ **B:申請コモンネーム/SANs**

CertCentralのメニュー「設定」→「選択設定」→「ドメイン認証範囲」の設定値によって、CertCentralから配信されるDCVメールの宛先のメールアドレスが変化します。
ここでは以下の2つの選択肢による違いを説明します。
A1: **「ベースドメインを提出して認証を受ける」** (推奨、デフォルト設定)
A2: **「認証する正確なドメイン名を提出する」**

証明書申請時のコモンネーム/SANsに指定されるドメイン名の階層構造によって、DCVメールの宛先のバリエーションが変化します。
ここでは以下の2つの例でご説明します。
B1: コモンネーム/SANs＝**example.com** の場合
B2: コモンネーム/SANs＝**sub01.example.com** の場合



「認証する正確なドメイン名を提出する」とは？
例えば申請コモンネーム/SANsが**[sub01.example.com]**の場合、DCVメールによるドメイン名利用権の確認対象は、コモンネーム/SANsと同一のレベル、つまり**[sub01.example.com]**となります。
→アカウント内に登録され、承認後にDCV履歴として再利用可能になるドメイン名は**[sub01.example.com]**となります。
→規定ホスト名(admin@等)によるDCVメール送信先のドメイン名部分(@マークの右側)は、**@sub01.example.com**(申請コモンネーム/SANsのサブドメイン名を含む値)となります。

「ベースドメインを提出して認証を受ける(推奨、デフォルト設定)」とは？
例えば申請コモンネーム/SANsが**[sub01.example.com]**の場合、DCVメールによるドメイン名利用権の確認対象は、コモンネーム/SANsのベースドメイン名部分、つまり**[example.com]**となります。
→アカウント内に登録され、承認後にDCV履歴として再利用可能になるドメイン名は**[example.com]**となります。
→規定ホスト名(admin@等)によるDCVメール送信先のドメイン名部分(@マークの右側)は、**@example.com**(申請コモンネーム/SANsのベースドメイン名部分)となります。

各DCV方式の詳細 – 「メール認証」の場合 (2/3 : 送信先の選択方法)

<table>
<tr><th>アカウント設定</th><th>申請コモンネーム/SANs</th><th>DCVメール仕様 (※1)</th><th>アカウント内に登録され、承認後に
DCV履歴として再利用可能になるドメイン名</th></tr>
<tr><td rowspan="2">A1:「ベースドメインを提出して認証を受ける」
(推奨、デフォルト設定)</td><td>B1: example.com の場合</td><td rowspan="2">DCVメールは以下の全てのメールアドレスに送信されます
<table><tr><th>区分</th><th>DCVメール宛先</th></tr><tr><td>WHOIS
(WHOIS-based Email)</td><td>1. WHOISに掲載されたメールアドレス</td></tr><tr><td>規定ホスト名
(Constructed Email)</td><td>2. admin@example.com
3. administrator@example.com
4. hostmaster@example.com
5. postmaster@example.com
6. webmaster@example.com</td></tr></table></td><td rowspan="2">example.com</td></tr>
<tr><td>B2: sub01.example.com の場合</td></tr>
<tr><td rowspan="2">A2:「認証する正確なドメイン名を提出する」</td><td>B1: example.com の場合</td><td>DCVメールは以下の全てのメールアドレスに送信されます
<table><tr><th>区分</th><th>DCVメール宛先</th></tr><tr><td>WHOIS
(WHOIS-based Email)</td><td>1. WHOISに掲載されたメールアドレス</td></tr><tr><td>規定ホスト名
(Constructed Email)</td><td>2. admin@example.com
3. administrator@example.com
4. hostmaster@example.com
5. postmaster@example.com
6. webmaster@example.com</td></tr></table></td><td>example.com</td></tr>
<tr><td>B2: sub01.example.com の場合</td><td>DCVメールは以下の全てのメールアドレスに送信されます
<table><tr><th>区分</th><th>DCVメール宛先</th></tr><tr><td>WHOIS
(WHOIS-based Email)</td><td>1. WHOISに掲載されたメールアドレス</td></tr><tr><td>規定ホスト名
(Constructed Email)</td><td>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</td></tr></table></td><td>sub01.example.com</td></tr>
</table>

※1 : アカウント設定の指定に対して、オーダー単位で異なるドメイン名の階層のメールアドレスのご利用を希望の場合
(例 : アカウント設定＝「ベースドメイン名」を設定した状態で、特定のオーダーに対してサブドメイン名を含むメールアドレス(例 : admin@sub01.example.com)のご利用を希望の場合)
弊社認証サポートチームまでアカウント番号、オーダー番号等の情報を添えてご依頼ください。

各DCV方式の詳細 – 「メール認証」の場合 (3/3 : メール文面)

■DCVメール(**OV/EV証明書用**)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(※1)]
送信元	no-reply@digitalcertvalidation.com
本文 イメージ (抜粋)	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。 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。） https://www.digicert.com/link/dcv-approve/?t=<ランダムな認証トークン(※3)> Click

■DCV承認画面(**OV/EV証明書用**)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(※2)

※1 : 確認対象のドメイン名は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、申請内容ならびに前ページに記載のアカウント設定によって決定されます。
※2 : 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。
※3 : 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)

○STEP 1：証明書の申請

オーダーリクエスト(例：**Order Secure Site OV**)時のパラメーター
「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/order/certificate/ssl_securesite_flex
```

＋

```
"dcv_method": "http-token",
"technical_contact": {
```

○STEP 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。

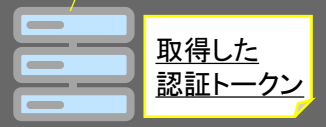
- ドメイン名をキーとする照会(**Domain Info**)のレスポンスで認証トークン取得 → *Page 44-45 参照*
- DCV方式の「変更」(**Change DCV method**)と同時に認証トークン取得 → *Page 46 参照*

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

○STEP 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://<確認対象のドメイン名(※1)>/.well-known/pki-validation/fileauth.txt



取得した認証トークン

※1：<確認対象のドメイン名>は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、証明書申請内容ならびにアカウント内「設定」→「選択設定」→「ドメイン認証範囲」の設定によって決定されます。
○例：申請コモンネーム/SANs ＝ sub01.example.comの場合、配置URLは以下となります
→「ドメイン認証範囲」＝「Submit base domains for validation」の場合
→配置URL ＝ http://example.com/.well-known/pki-validation/fileauth.txt
→「ドメイン認証範囲」＝「認証する正確なドメイン名を提出する」の場合
→配置URL ＝ http://sub01.example.com/.well-known/pki-validation/fileauth.txt

○STEP 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 47 参照*

※ 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。

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**)

○STEP 1：証明書の申請

オーダーリクエスト(例：**Order Secure Site OV**)時のパラメーター
「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/order/certificate/ssl_securesite_flex
```

＋

```
"dcv_method": "dns-txt-token",
"technical_contact": {
```

○STEP 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 44-45 参照*
- DCV方式の「変更」(**Change DCV method**)と同時に認証トークン取得 → *Page 46 参照*

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

○STEP 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*
<確認対象のドメイン名(※1)>	TXT	取得した認証トークン

※1：<確認対象のドメイン名>は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、
証明書申請内容ならびにアカウント内「設定」→「選択設定」→「ドメイン認証範囲」の設定によって
決定されます。
○例：申請コモンネーム/SANs ＝ sub01.example.comの場合、<確認対象のドメイン名>は以下となります
→「ドメイン認証範囲」＝「Submit base domains for validation」の場合
→<確認対象のドメイン名> ＝ example.com
→「ドメイン認証範囲」＝「認証する正確なドメイン名を提出する」の場合
→<確認対象のドメイン名> ＝ sub01.example.com

○STEP 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 47 参照*

※ 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。

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**)

○STEP 1：証明書の申請

オーダーリクエスト(例：**Order Secure Site OV**)時のパラメーター
「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/order/certificate/ssl_securesite_flex
```

```
 payment_method :  balance ,
"dcv_method": "dns-cname-token",
"technical_contact": {
```

○STEP 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 44-45 参照*
- DCV方式の「変更」(**Change DCV method**)と同時に認証トークン取得 → *Page 46 参照*

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

○STEP 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.<確認対象のドメイン名(※1)>	CNAME	dcv.digicert.com

※1：<確認対象のドメイン名>は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、
証明書申請内容ならびにアカウント内「設定」→「選択設定」→「ドメイン認証範囲」の設定によって
決定されます。
○例：申請コモンネーム/SANs ＝ sub01.example.comの場合、<確認対象のドメイン名>は以下となります
→「ドメイン認証範囲」＝「Submit base domains for validation」の場合
→<確認対象のドメイン名> ＝ example.com
→「ドメイン認証範囲」＝「認証する正確なドメイン名を提出する」の場合
→<確認対象のドメイン名> ＝ sub01.example.com

○STEP 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 47 参照*

※ 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。

3. サーバ証明書(OV/EV)の申請

~ 3.4 組織およびドメイン名の管理 ~

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		**dns_name_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/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

（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：組織認証およびドメイン名利用権確認(DCV)が完了しているのに、証明書を申請しても、その後すぐ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

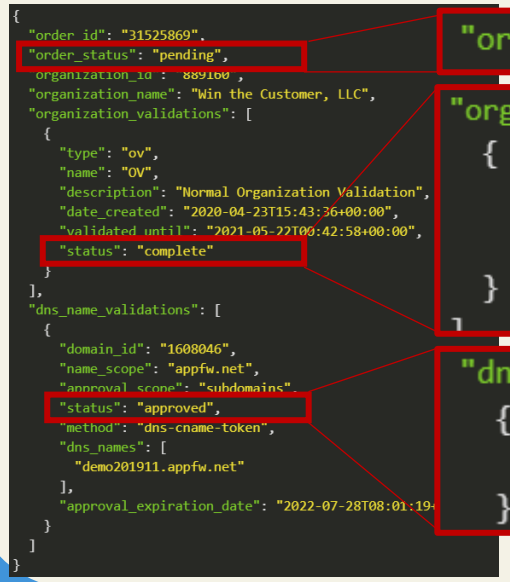
オーダーステータス
証明書最終確認

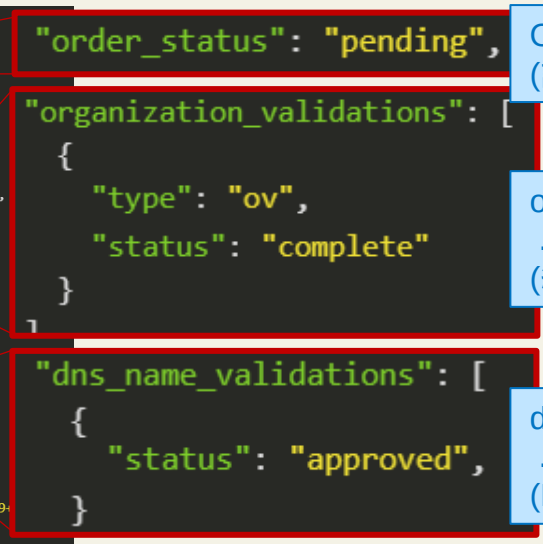
オーダーステータスが「証明書最終確認」と表示されていること

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_status=pending
(証明書は発行待ち)

AND

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

AND

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

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}}

・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）

● 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"
  }
}
```

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

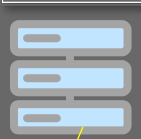
① 認証トークン情報を「含める」と指定

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
dcv_token	ドメイン名利用権確認(DCV)オブジェクト	**Object**
token	認証トークン(ファイル/DNS認証用)の値	String
status	DCVのステータス。例：「pending」	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

「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": "bx4b8g34lq85w84b56kspzxprw366wd9",
    "status": "pending",
    "http_token_url": "http:\/\/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(OV/EV証明書)

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 ・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": "bx4b8g34lq85w84b56kspzxprw366wd9",
    "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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

Check DCV(OV/EV)：即時ポーリング実行

cURLのサンプルコード(*1)

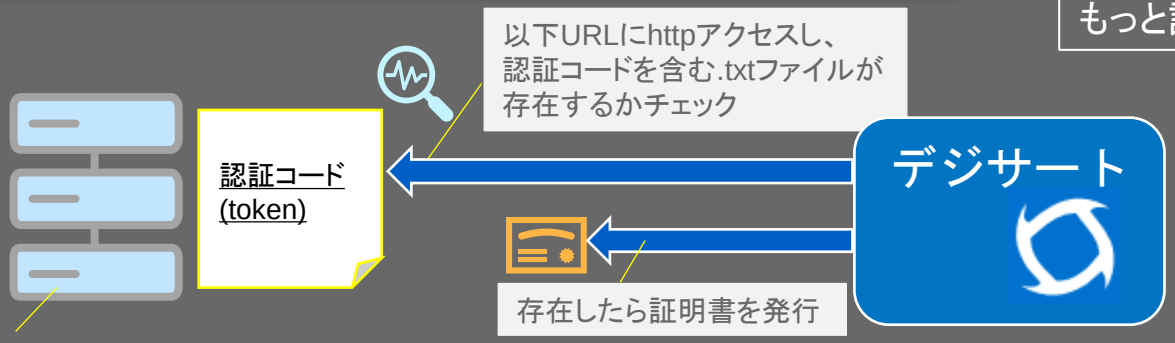
```
curl -X PUT \
  'https://www.digicert.com/services/v2/domain/{{domain_id}}/dcv/validate-token' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}'
```

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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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:

GET 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 **(下記注釈参照ください)**

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

【ご注意ください】上記**シナリオ2(ドメイン名指定)**の結果で返却されるレスポンス内”base_emails”の値は、証明書申請時にDCVメールが送信される宛先と異なる場合があります。
1：【Domain Emailsの{domain_id}パラメーターに**[sub01.example.com]**を設定した場合
→ レスポンス内”base_emails”に含むメールアドレスのドメイン名部分(@マークの右側)は、**常に「sub01.example.com」**(パラメーターとして渡されたFQDN)となります。
2：【オーダーエンドポイントのcommon_nameに**[sub01.example.com]**を設定した場合
→ DCVメールの送信先は、**[アカウント設定]等の複数の要素によって決定**されます。詳しくは以下を参照ください。
OV/EV証明書の場合：セクション 2.3内「DCVメール送信先の選択ルール」 ／ DV証明書の場合：セクション 3.3内「DCVメール送信先の選択ルール」

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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

4. サーバ証明書(DV)証明書の申請

~ 4.1 ワークフロー概要 ~

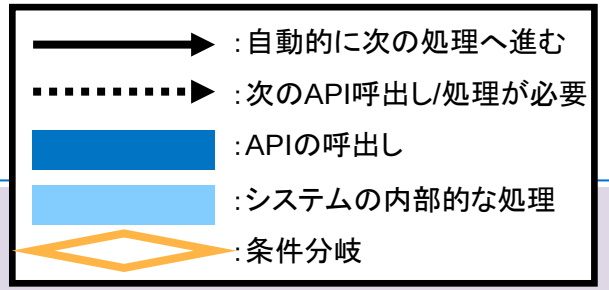
CertCentral APIによるDV証明書の申請ワークフロー概要 (DCV方式：メール認証の場合)

タスク概要		内容	CertCentral API		エンドユーザ企業	
			API	備考	申請責任者	ドメイン名管理者
事前準備		・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて) ドメイン名管理者の確認、事前調整	特にAPI操作不要		N/A	N/A
証明書の申請		・APIを通じて証明書を申請 ・DCVメール配信先の指定、メール送信	(例)Order GeoTrust DV SSL	セクション 4.2 参照	N/A	DCVメール受信・承認
認証	ドメイン利用権確認(DCV)	・(必要に応じて)DCVメールの再送信	DV SSL: Resend emails	セクション 4.2 参照	N/A	DCVメール受信・承認
認証	全般	・個別オーダのステータス(発行済か否か)をチェック	Order Info	OV/EV 証明書と共通	N/A	N/A
認証	全般	・指定した時間内にステータスが変更したオーダーを検索 (例:30分以内に「発行済」となったオーダー)	Status change list		N/A	N/A
証明書の取得		・発行された証明書を形式を指定して取得(ダウンロード)	Download certificate		N/A	N/A

CertCentral APIによるDV証明書の申請ワークフロー概要 (DCV方式：ファイル認証/DNS認証の場合)

タスク概要		内容	CertCentral API		エンドユーザ企業	
			API	備考	申請責任者	ドメイン名管理者
事前準備		・CSR生成、ドメイン名利用権確認(DCV)方法の決定	特にAPI操作不要		N/A	N/A
証明書の申請		・APIを通じて証明書を申請 ・認証トークンの取得	(例)Order GeoTrust DV SSL	セクション 4.2 参照	N/A	N/A
認証	ドメイン利用権確認(DCV)	・認証トークンの取得・配置 ・ファイル/DNS認証のための(再)ポーリング指示	DV SSL: Check DCV	セクション 4.2 参照	N/A	N/A
認証	全般	・個別オーダのステータス（発行済か否か）をチェック	Order Info	OV/EV 証明書と共通	N/A	N/A
認証	全般	・指定した時間内にステータスが変更したオーダーを検索 (例：30分以内に「発行済」となったオーダー)	Status change list		N/A	N/A
証明書の取得		・発行された証明書を形式を指定して取得(ダウンロード)	Download certificate		N/A	N/A

DV証明書の申請～認証までのAPI呼び出しとシステム処理概要
(DCV方式：メール認証の場合)



申請前の状態

同一Orgの
事前登録なし

同一ドメイン名の
事前登録なし

(例) Order
GeoTrust DV SSL
(DV証明書申請)

・DCV方法の指定
・DCVメール配信先の指定

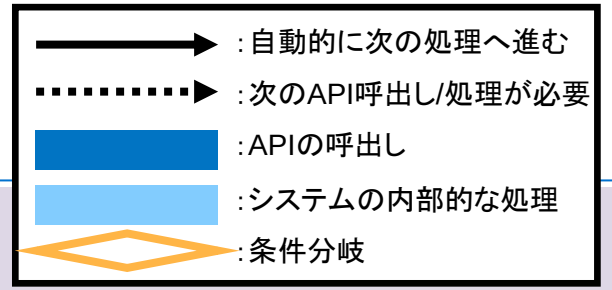
・DCVメールの(再)送信

お客様のドメイン名管理者様による
DCVメール受信・承認

証明書発行

当ページに記載のチャートは概略を表すものであり、一部の処理を簡略化して記載しております。
セキュリティ、コンプライアンスの理由から上記に記載がない、追加の確認などが必要となるケースがあります。ご理解・ご了承ください。

DV証明書の申請～認証までのAPI呼び出しとシステム処理概要
(DCV方式：ファイル認証/DNS認証の場合)



申請前の状態

同一Orgの
事前登録なし

同一ドメイン名の
事前登録なし

(例) Order GeoTrust DV SSL
(DV証明書申請)

・DCV方法の指定
・レスポンスとして認証トークンを取得

認証トークン配置

DV SSL: Check DCV
(Pollingの(再)実行)

・主な入力キー：Order ID

・認証トークン配置後の
ファイル/DNSポーリング実行

証明書発行

当ページに記載のチャートは概略を表すものであり、一部の処理を簡略化して記載しております。
セキュリティ、コンプライアンスの理由から上記に記載がない、追加の確認などが必要となるケースがあります。ご理解・ご了承ください。

4. サーバ証明書(DV)の申請

~ 4.2 サーバ証明書(DV)の申請 ~

DV証明書：プラン/証明書の新規申請

cURLのサンプルコード(*1)

```
curl -X POST \
  'https://www.digicert.com/services/v2/order/certificate/ssl_dv_geotrust_flex' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "certificate": {
        "common_name": "example.com",
        "dns_names": [
            "sub.example.com",
            "log.example.com"
        ],
        "csr": "<csr>",
        "server_platform": {
            "id": 2
        }
    },
    "custom_expiration_date": "",
    "comments": "Message for the approv
    "container": {
        "id": 69748
    },
    "custom_renewal_message": "Renew me
    "skip_approval": true,
    "disable_ct": 0,
    "order_validity": {
      "years": 1
    },
    "custom_fields": [
        {
            "metadata_id": 12,
            "value": "Invoice #12345"
        }
    ],
    "payment_method": "balance",
    "dcv_method": "email",
    "dcv_emails": [
        {
            "dns_name": "example.com",
            "email_domain": "example.com",
            "email": "admin@example.com"
        },
        {
            "dns_name": "sub.example.com",
            "email_domain": "example.com",
            "email": "jim.smith@example.com"
        },
        {
            "dns_name": "log.example.com",
            "email_domain": "example.com",
            "email": "it@example.com"
        }
    ],
    "locale": "en",
    "technical_contact": {
        "first_name": "Jim",
        "last_name": "Smith",
        "telephone": "555-555-5555",
        "job_title": "IT Admin",
        "email": "jim.smith@example.com"
    }
}'
```

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
→ https://dev.digicert.com/glossary/#product-identifiers 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。 CertCentral利用ガイド「5. 発行された証明書の取得」を参照ください	Int
cert_validity years/ days/ custom_expiration_date	【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	-
container	[別紙] container : id (管理グループ/Division) の確認方法 参照	**Object**
dcv_method	[別紙] 各DCV方式の詳細 参照	**Object**
order_validity years/ days/ custom_expiration_date	【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	-
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-geotrust-dv-ssl/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

DV証明書：プラン/証明書の新規申請 (続き)

cURLのサンプルコード(*1)

メール認証の場合
(dcv_method=email)のレスポンス例:

201 Created (email) 201 Created (

```
{
  "id": 6484932,
  "certificate_id": 6079436
}
```

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

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-geotrust-dv-ssl/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

DV証明書：プラン/証明書の新規申請 (続き)

cURLのサンプルコード(*1)

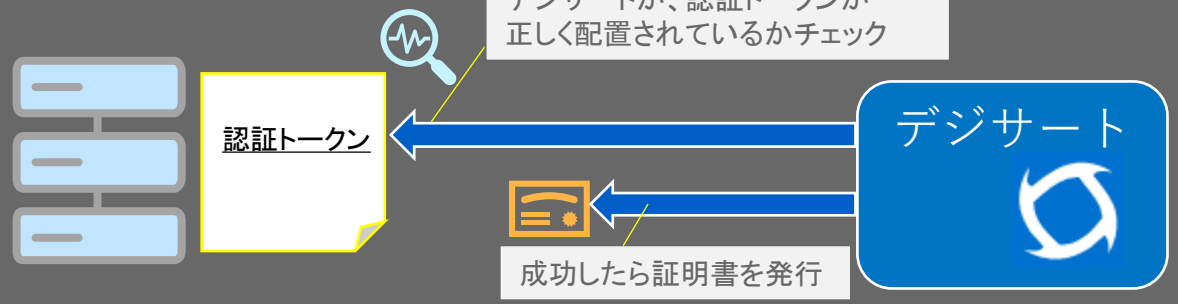
ファイル認証/DNS認証の場合
(dcv_method=http-token)のレスポンス例:

201 Created (email)　201 Created (dns-txt-token or http-token)

```
{
  "id": 6484932,
  "certificate_id": 6079436
  "dcv_random_value": "icru1984rnekfj"
}
```

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
dcv_random_value	（ファイル認証/DNS認証の場合）：認証トークンの値	String

・認証トークン配置後の「ファイル/DNSポーリング」の処理イメージ



もっと詳しく:https://dev.digicert.com/workflows/dv-ssl-certificate-lifecycle/

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-geotrust-dv-ssl/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

各DCV方式の詳細 – 「メール認証」の場合 (1/4 : 送信先の選択ルール)

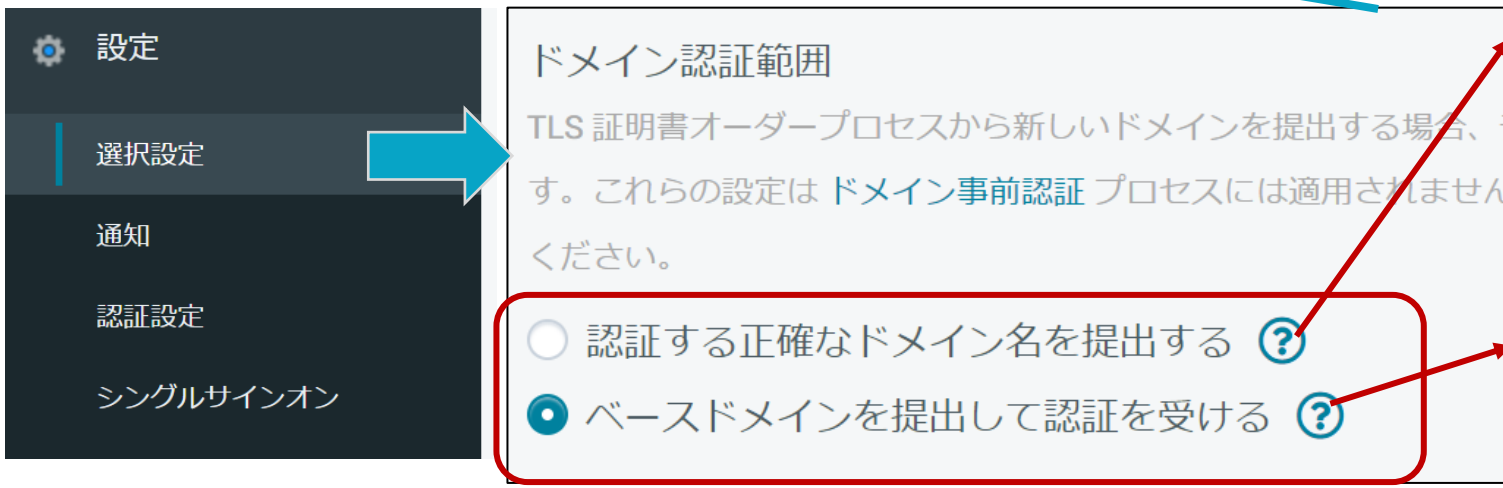
■DV証明書のDCVメールの送信先は以下の組み合わせによって決定されます。

A:アカウント設定「ドメイン認証範囲」 ✖ **B:申請コモンネーム/SANs** ✖ **C:リクエストパラメーター ”dcv_emails”**

CertCentralのメニュー「設定」→「選択設定」→「ドメイン認証範囲」の設定値によって、CertCentralから配信されるDCVメールの宛先のメールアドレスが変化します。
ここでは以下の2つの選択肢による違いを説明します。
A1: **「ベースドメインを提出して認証を受ける」** (推奨、デフォルト設定)
A2: **「認証する正確なドメイン名を提出する」**

証明書申請時のコモンネーム/SANsに指定されるドメイン名の階層構造によって、DCVメールの宛先のバリエーションが変化します。
ここでは以下の2つの例でご説明します。
B1: コモンネーム/SANs＝**example.com** の場合
B2: コモンネーム/SANs＝**sub01.example.com** の場合

AおよびBによって決定されたDCVメール宛先リストの範囲内で宛先を絞り込むことが可能です。
C1: 指定なし＝全ての候補に送信
C2: 指定あり＝パラメータで指定した宛先にのみ送信



「認証する正確なドメイン名を提出する」とは？
申請コモンネーム/SANsが**[sub01.example.com]**の場合、DCVメールによるドメイン名利用権の確認対象は、コモンネーム/SANsと同一のレベル、つまり**[sub01.example.com]**となります。
→規定ホスト名(admin@等)によるDCVメール送信先のドメイン名部分(@マークの右側)は、**@sub01.example.com**(申請コモンネーム/SANsのサブドメイン名を含む値)となります。

「ベースドメインを提出して認証を受ける(推奨、デフォルト設定)」とは？
申請コモンネーム/SANsが**[sub01.example.com]**の場合、DCVメールによるドメイン名利用権の確認対象は、コモンネーム/SANsのベースドメイン名部分、つまり**[example.com]**となります。
→規定ホスト名(admin@等)によるDCVメール送信先のドメイン名部分(@マークの右側)は、**@example.com**(申請コモンネーム/SANsのベースドメイン名部分)となります。

※ : OV/EV証明書と異なり、DV証明書の場合はDCV履歴を再利用いたしません。同一コモンネーム/SANsでのご申請を繰り返す場合でも、申請の度にDCVを実施いただく必要がございます。

各DCV方式の詳細 – 「メール認証」の場合 (2/4 : 送信先の選択方法)

アカウント設定	申請コモンネーム/SANs	リクエストパラメーター指定方法およびDCVメール送信先 (※1)	
		C1: ”dcv_emails” 指定なし	C2: ”dcv_emails” 指定あり
A1:「ベースドメインを提出して認証を受ける」 (推奨、デフォルト設定)	B1: example.com の場合	DCVメールは以下の全てのメールアドレスに送信されます 区分: WHOIS (WHOIS-based Email) → 1. WHOISに掲載されたメールアドレス 区分: 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	“dcv_emails”パラメータの指定により左記の選択肢の範囲内でDCVメールの宛先を絞り込むことが可能です 例 : [admin@example.com] のみにDCVメールを送信する場合 `"dcv_emails": [ { "dns_name": "example.com", "email_domain": "example.com", "email": "admin@example.com" } ],`
	B2: sub01.example.com の場合	DCVメールは以下の全てのメールアドレスに送信されます 区分: WHOIS (WHOIS-based Email) → 1. WHOISに掲載されたメールアドレス 区分: 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	“dcv_emails”パラメータの指定により左記の選択肢の範囲内でDCVメールの宛先を絞り込むことが可能です 例 : [admin@example.com] のみにDCVメールを送信する場合 `"dcv_emails": [ { "dns_name": “sub01.example.com", "email_domain": "example.com", "email": "admin@example.com" } ],`

※1 : アカウント設定の指定に対して、オーダー単位で異なるドメイン名の階層のメールアドレスのご利用を希望の場合
(例 : アカウント設定 =「ベースドメイン名」を設定した状態で、特定のオーダーに対してサブドメイン名を含むメールアドレス(例 : admin@sub01.example.com)のご利用を希望の場合)
弊社認証サポートチームまでアカウント番号、オーダー番号等の情報を添えてご依頼ください。

各DCV方式の詳細 – 「メール認証」の場合 (3/4 : 送信先の選択方法(続き))

アカウント設定	申請コモンネーム/SANs	リクエストパラメーター指定方法およびDCVメール送信先 (※1)	
		C1: ”dcv_emails” 指定なし	C2: ”dcv_emails” 指定あり
A2: 「認証する正確なドメイン名を提出する」	B1: example.com の場合	DCVメールは以下の全てのメールアドレスに送信されます 区分: WHOIS (WHOIS-based Email) → 1. WHOISに掲載されたメールアドレス 区分: 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	“dcv_emails”パラメータの指定により左記の選択肢の範囲内でDCVメールの宛先を絞り込むことが可能です 例 : [admin@example.com] のみにDCVメールを送信する場合
	B2: sub01.example.com の場合	DCVメールは以下の全てのメールアドレスに送信されます 区分: WHOIS (WHOIS-based Email) → 1. WHOISに掲載されたメールアドレス 区分: 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	“dcv_emails”パラメータの指定により左記の選択肢の範囲内でDCVメールの宛先を絞り込むことが可能です 例 : [admin@sub01.example.com] のみにDCVメールを送信する場合

```
"dcv_emails": [
  {
    "dns_name": “example.com",
    "email_domain": "example.com",
    "email": "admin@example.com"
  }
],
```

```
"dcv_emails": [
  {
    "dns_name": “sub01.example.com",
    "email_domain": “sub01.example.com",
    "email": "admin@sub01.example.com"
  }
],
```

※1 : アカウント設定の指定に対して、オーダー単位で異なるドメイン名の階層のメールアドレスのご利用を希望の場合
(例 : アカウント設定 =「ベースドメイン名」を設定した状態で、特定のオーダーに対してサブドメイン名を含むメールアドレス(例 : admin@sub01.example.com)のご利用を希望の場合)
弊社認証サポートチームまでアカウント番号、オーダー番号等の情報を添えてご依頼ください。

各DCV方式の詳細 – 「メール認証」の場合 (4/4：メール文面)

■DCVメール(**DV証明書用**)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
(証明書申請画面内の「DCV Email Language」において
「Japanese(日本語)」を選択いただいた場合)

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(※1)]
送信元	no-reply@geotrust.com
本文 イメージ (抜粋)	デジサートでは、GeoTrustSSL/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。 (中略) 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ご確認いただいた上で、SSL/TLSサーバ証明書、またはS/MIME用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。 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。）： https://dcv.geotrust.com/link/domain-control-validation/?t=<ランダムな認証トークン(※3)> Click

■DCV承認画面(**DV証明書用**)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(※3)

※1：確認対象のドメイン名は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、申請内容ならびに前ページに記載のアカウント設定によって決定されます。
※2：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。
※3：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 (DV証明書の場合)

〇STEP 1：証明書の申請

オーダーリクエスト(例：**Order GeoTrust DV SSL**)時のパラメーター
「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/order/certificate/ssl_dv_geotrust_flex
```

```
"dcv_method": "http-token",
"technical_contact": {
```

〇STEP 2：認証トークンの入手

オーダーリクエストのレスポンスから認証トークンを取得します。

```
{
  "id": 27249419,
  "certificate_id": 28070426,
  "dcv_random_value": "334ssgfjtf71rrtcp0ky3y7qb5bnbj37"
}
```

〇STEP 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://<申請コモンネーム/SANs(※1)>/.well-known/pki-validation/fileauth.txt

取得した認証トークン

※1：DV証明書の場合、ファイル認証における認証トークンファイルの配置先は「申請コモンネーム/SANs」となります。申請コモンネーム/SANsがサブドメイン名を含む場合は、配置先はサブドメイン名を含む上記URLとなります

〇STEP 4：認証トークンファイルのチェック

DV SSL: Check DCV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。

DV SSL: Check DCV：即時ポーリング実行呼出し *Page 67 参照*

※ 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。

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 (**DV証明書の場合**)

〇STEP 1：証明書の申請

オーダーリクエスト(例：**Order GeoTrust DV SSL**)時のパラメーター
「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/order/certificate/ssl_dv_geotrust_flex
```

```
"dcv_method": "dns-txt-token",
"technical_contact": {
```

〇STEP 2：認証トークンの入手

オーダーリクエストのレスポンスから認証トークンを取得します。

```
{
  "id": 27249419,
  "certificate_id": 28070426,
  "dcv_random_value": "334ssgfjtf71rrtcp0ky3y7qb5bnbj37"
}
```

〇STEP 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*
<申請コモンネーム/SANs(※1)>	TXT	取得した認証トークン

※1：DV証明書の場合、DNS TXT認証における認証トークンの設定対象リソースレコードは
「申請コモンネーム/SANs」となります。申請コモンネーム/SANsがサブドメイン名を含む場合は、
サブドメイン名を含むDNS TXTリソースレコードに認証トークンを設定します

〇STEP 4：認証トークンのチェック

DV SSL: Check DCV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。

DV SSL: Check DCV：即時ポーリング実行呼出し *Page 67 参照*

※ 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。

DV証明書：プラン/証明書の更新申請

cURLのサンプルコード(*1)

```
curl -X POST \
  'https://www.digicert.com/services/v2/order/certificate/ssl_dv_geotrust_flex' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
    "certificate": {
        "common_name": "example.com",
        "dns_names": [
            "sub.example.com",
            "log.example.com"
        ],
        "csr": "<csr>",
        "server_platform": {
            "id": 2
        }
    },
    "custom_expiration_date": "",
    "comments": "Message for the approv
    "container": {
        "id": 69748
    },
    "custom_renewal_message": "Renew me
    "skip_approval": true,
    "disable_ct": 0,
    "order_validity": {
      "years": 1
    },
    "custom_fields": [
        {
            "metadata_id": 12,
            "value": "Invoice #12345"
        }
    ],
    "payment_method": "balance",
    "dcv_method": "email",
    "dcv_emails": [
        {
            "dns_name": "example.com",
            "email_domain": "example.com",
            "email": "admin@example.com"
        },
        {
            "dns_name": "sub.example.com",
            "email_domain": "example.com",
            "email": "jim.smith@example.com"
        },
        {
            "dns_name": "log.example.com",
            "email_domain": "example.com",
            "email": "it@example.com"
        }
    ],
    "locale": "en",
    "technical_contact": {
        "first_name": "Jim",
        "last_name": "Smith",
        "telephone": "555-555-5555",
        "job_title": "IT Admin",
        "email": "jim.smith@example.com"
    }
}'
```

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
→ https://dev.digicert.com/glossary/#product-identifiers 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。 CertCentral利用ガイド「5. 発行された証明書の取得」を参照ください	Int
cert_validity years/ days/ custom_expiration_date	【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	-
container	[別紙] container : id (管理グループ/Division) の確認方法 参照	**Object**
dcv_method	[別紙] 各DCV方式の詳細 参照	**Object**
order_validity years/ days/ custom_expiration_date	【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	-
renewal_of_order_id	更新元プラン/証明書のオーダーIDを指定	
renewed_thumbprint	更新元プラン/証明書の証明書ハッシュ値	

プラン更新申請の場合、いずれか一方が必須

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-geotrust-dv-ssl/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

DV SSL: Resend emails：DCVメールの(再)送信 (DV証明書)

cURLのサンプルコード(*1)

```
curl -X PUT \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/resend-emails' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
  "domain_approval_emails": [
    {
      "domain": "example.com",
      "email": "someone@example.com"
    },
    {
      "domain": "example2.com",
      "email": "someone@example2.com"
    }
  ],
  "locale": "en"
}'
```

Method+Endpoint:

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

・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、DV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
domain_approval_emails	(メール認証を指定した場合)DCVメール配信先のアドレスを指定 ※ 単一または複数のアドレスを指定可能。設定しない場合は候補となる全てのメールアドレスにDCVメールを配信する。	String
locale	DCVメールの文面の言語を選択：「jp(日本語)」を指定してください。	String

もっと詳しく:https://dev.digicert.com/services-api/orders/dv-ssl-resend-emails/

*1:当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

DV SSL: Check DCV：即時ポーリング実行 (DV証明書)

cURLのサンプルコード(*1)

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

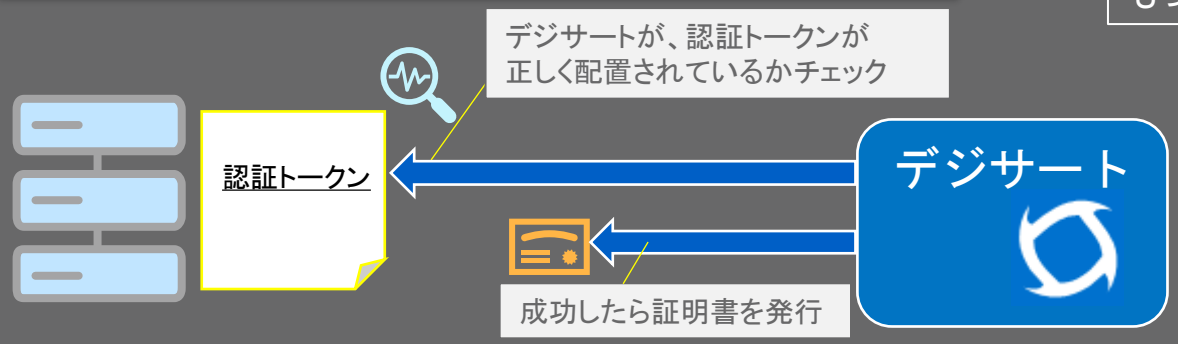
Method+Endpoint:

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

・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、DV証明書を申請したタイミングで割り振られます。

もっと詳しく：https://dev.digicert.com/services-api/orders/dv-ssl-check-dcv/

・認証トークン配置後の「ファイル/DNSポーリング」の処理イメージ



もっと詳しく：https://dev.digicert.com/workflows/dv-ssl-certificate-lifecycle/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

DV SSL: Change DCV method：DCV方法の変更 (DV証明書)

cURLのサンプルコード(*1)

```
curl -X PUT \
  'https://www.digicert.com/services/v2/order/certificate/{{order_id}}/dcv-method' \
  -H 'Content-Type: application/json' \
  -H 'X-DC-DEVKEY: {{api_key}}' \
  -d '{
  "dcv_method": "email"
}'
```

Method+Endpoint:

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

・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、DV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
dcv_method	ドメインIDで指定したドメイン名に対するDCV方法 ・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/orders/dv-ssl-change-dcv-method/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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：

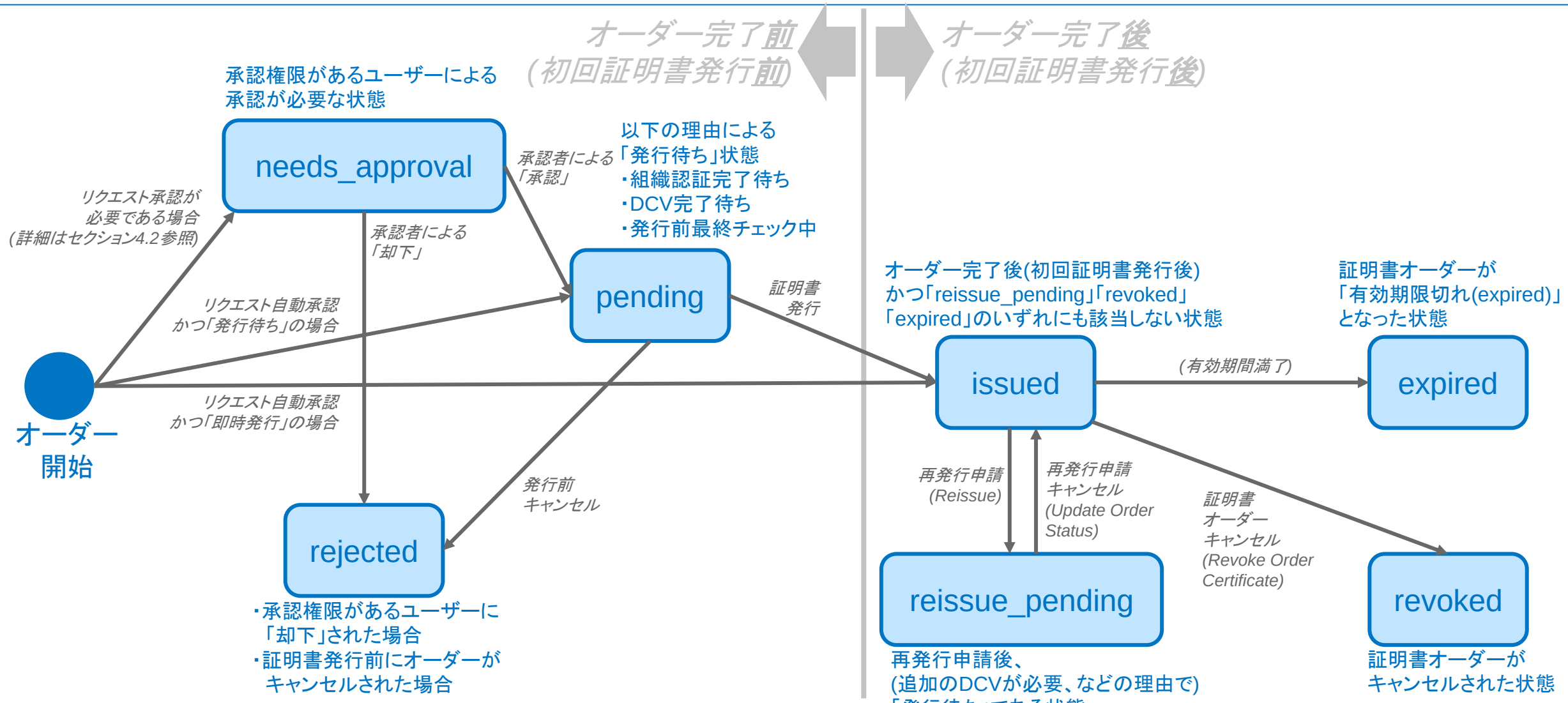

```
{
 "id": 115429178,
 "certificate": {
  "id": 116470545,
  "thumbprint": "(省略)",
  "serial_number": "(省略)",
  "common_name": "demo.appfw.net",
  "dns_names": [
   "demo.appfw.net"
  ],
  "date_created": "2021-01-20T02:30:12+00:00",
  "valid_from": "2021-01-20",
  "valid_till": "2022-01-23",
  "days_remaining": 359,
  "cert_validity": {
   "years": 1
  },
  "csr": "<csr>",
  "organi"zation": {
   "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

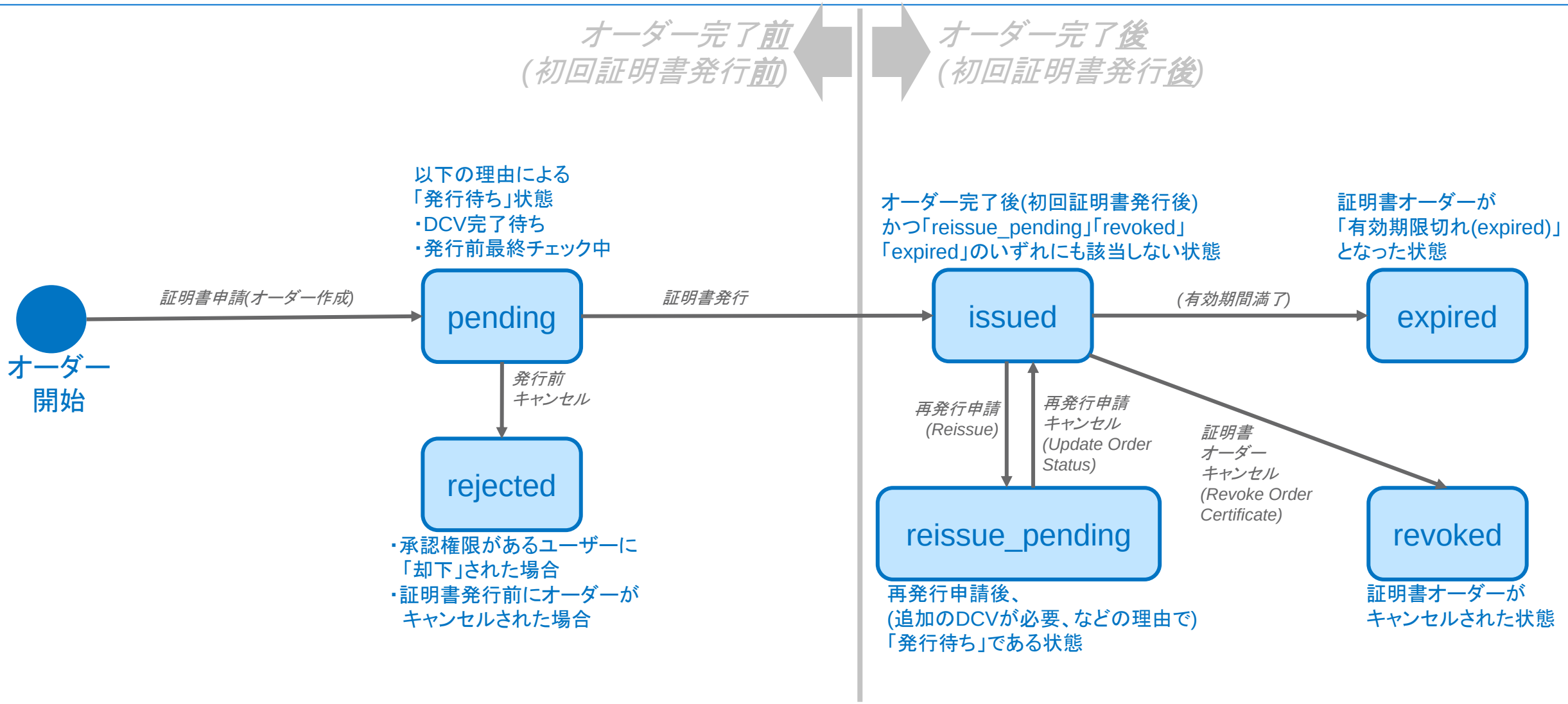
もっと詳しく:https://dev.digicert.com/services-api/orders/order-info/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

（OV/EV証明書の場合）オーダーのステータス状態遷移



（DV証明書の場合）オーダーのステータス状態遷移



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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

(ご参考) List Ordersで利用可能なフィルター覧

■「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
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

「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
該当オーダー覧を取得する場合に指定

■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

Status change list：指定した時間内にステータスが変更したオーダーを検索

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 ・pending : 認証中・未発行 ・issued : 証明書発行済 ・canceled : キャンセル済	String

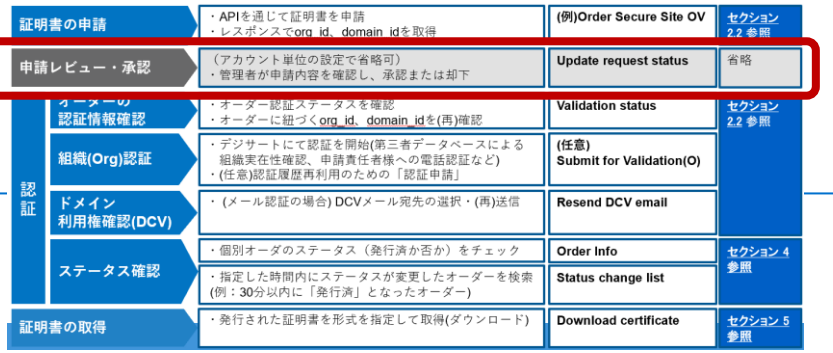
もっと詳しく: https://dev.digicert.com/services-api/orders/status-change-list/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

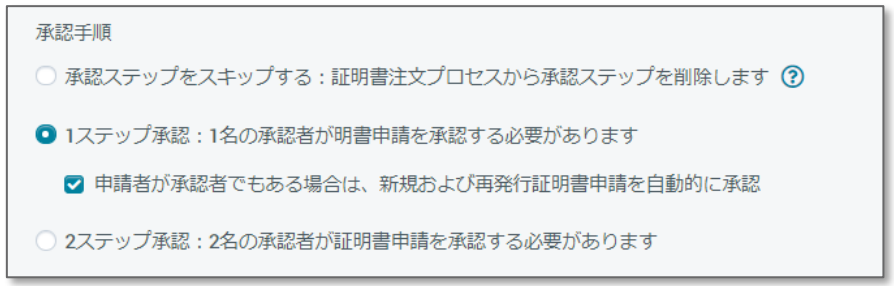
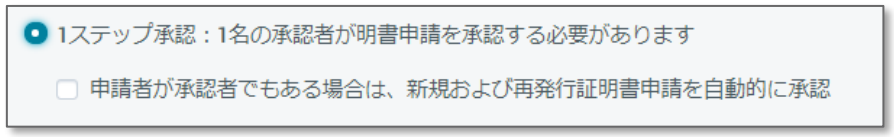
5. オーダー管理、リクエスト管理

~ 5.2 （OV/EV証明書のみ）リクエスト管理 ~

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)		**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		**自動的に承認**	
常に1ステップ承認		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		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)	証明書が申請されました。 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] 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]

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)

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	・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	・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/

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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": "Epigyne 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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

6. 発行された証明書の取得

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

cURLのサンプルコード(*1)

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

Method+Endpoint:

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

・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。

レスポンス例：
(format_type=pem_noroot)

End-Entity証明書
(PEM形式)

中間CA証明書
(PEM形式)

```
-----BEGIN CERTIFICATE-----
MIIFTDCCBDSgAwIBAgIQAgUCYKwU/yjB9bPPYn+eRDANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMDExMDkwMDAwMDBa
Fw0yMDEyMDcyMzU5NTlaMHAxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzEQ
MA4GA1UEBxMHQ2h1by1rdTEcMBoGA1UEChMTRElHSUNFUlQgSkFQQU4gRy5LLjEh
MB8GA1UEAxMYYWYyMDIwMTEwNi0wMDUuYXBwZncubmV0MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnjq3WI1juZGpj9L4ONhxGL9przusrDwgJjTuUUVx
4F5kPHkgXhQGcLmewa2FJOelXWvM9plGRjfEdkEdahFzKBonvLWbUOxzcoK411GL
qX1Nvu8p0i6oFI1YE2pCVwoDvjXvw6+U/KC
V9BQ+8KL8c0/X3PSH1NbwGCs0sKDh/C6HOb
YsVX7eyvQXTfY+OOEmUEeHVR0QlGHFY9FyY
pu1TSIjd8y+FrPUurnHJA3YrLu8glLaWLN8
HwYDVR0jBBgwFoAUt2ui6qiqhIx56rTaD5i
70UHDOo41D9FaYFjxcEIMCMGA1UdEQQcMBq
Lm5ldDAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0
BwMCMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh
bS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjB
Y3JsNC5kaWdpY2VydC5jb20vRGlnaUNlcnR
bDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATA
L3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBme
JAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmR
AoY7aHR0cDovL2NhY2VydHMuZGlnaWNlcnQ
MjU2MjAyMENBMS5jcnQwDAYDVR0TAQH/BAI
NDNoI8zzngaIDJ1iD5zmV+LJiMgRRGekEa2
KfUbV2LECnNCUTqxJMMvvey1y4e54gmOBF4
Y0ufC/Uwww7/ourV+q0MYAOcCb0ywLQenuh
7TtbJzV14qUPzLLb5w6XRpZAw05omh4W7vv
Luw+gCTcE1dFaEuLVAbKutA5KCKbhxgxIoP
oViWtija9ybE2lNuwXGqlw==
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMyMzU5NTlaME8xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERpZ2lDZXJ0IFRMUyBS
U0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6a
qXodgojlEVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddn
g9/n00tnTCJRpt8OmRDtV1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuW
raKImxW8oHzf6VGo1bDtN+I2tIJLYrVJmuzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGB
Afr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkDKa77SU+kFbnO8lwZV21r
eacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYEFLdrouqo
qoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFV
MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
EgYDVR0TAQH/BAgwBgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGG
GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2Nh
Y2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNydDB7BgNV
HR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vRGlnaUNlcnRH
bG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYG
Z4EMAQIBMAgGBmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHer
t3onPa679n/gWlbJhKrKW3EX3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNj
OSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Zu2XHFq8hVt1hBcnpj5h232sb0HIM
ULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe50gG66sSmvKvhMNb
g0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4ZxuYRiH
as6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI
8ks5T1KESaZMkE4f97Q=
-----END CERTIFICATE-----
```

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(formart_type)一覧 参照	String

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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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}}'
```

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。

レスポンス例：
(format_type=pem_noroot)

End-Entity証明書
(PEM形式)

中間CA証明書
(PEM形式)

```
-----BEGIN CERTIFICATE-----
MIIFTDCCBDSgAwIBAgIQAgUCYKwU/yjB9bPPYn+eRDANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMDExMDkwMDAwMDBa
Fw0yMDEyMDcyMzU5NTlaMHAxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzEQ
MA4GA1UEBxMHQ2h1by1rdTEcMBoGA1UEChMTRElHSUNFUlQgSkFQQU4gRy5LLjEh
MB8GA1UEAxMYYWwYyMDIwMTEwNi0wMDUuYXBwZncubmV0MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnjq3WI1juZGpj9L4ONhxGL9przusrDwgJjTuUUVx
4F5kPHkgXhQGcLmewa2FJOelXWvM9plGRjfEdkEdahFzKBonvLWbUOxzcoK411GL
qX1Nvu8p0i6oFI1YE2pCVwoDvjXvw6+U/KC
V9BQ+8KL8c0/X3PSH1NbwGCs0sKDh/C6HOb
YsVX7eyvQXTfY+OOEmUEeHVR0QlGHFY9FyY
pu1TSIjd8y+FrPUurnHJA3YrLu8gllaWLN8
HwYDVR0jBBgwFoAUt2ui6qiqhIx56rTaD5i
70UHDOo41D9FaYFjxcEIMCMGA1UdEQQcMBq
Lm5ldDAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0
BwMCMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh
bS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBl
Y3JsNC5kaWdpY2VydC5jb20vRGlnaUNlcnR
bDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATA
L3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBme
JAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmR
AoY7aHR0cDovL2NhY2VydHMuZGlnaWNlcnQ
MjU2MjAyMENBMS5jcnQwDAYDVR0TAQH/BAI
NDNoI8zzngaIDJ1iD5zmV+LJiMgRRGekEa2
KfUbV2LECnNCUTqxJMMvvey1y4e54gmOBF4
Y0ufC/Uwww7/ourV+q0MYAOcCb0ywLQenuh
7TtbJzV14qUPzLLb5w6XRpZAw05omh4W7vv
Luw+gCTcE1dFaEuLVAbKutA5KCKbhxgxIoP
oViWtija9ybE2lNuwXGqlw==
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMyMzU5NTlaME8xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERpZ2lDZXJ0IFRMUyBS
U0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6a
qXodgojlEVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddn
g9/n00tnTCJRpt8OmRDtV1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuW
raKImxW8oHzf6VGo1bDtN+I2tIJLYrVJmuzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGB
Afr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkDKa77SU+kFbnO8lwZV21r
eacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYEFLdrouqo
qoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFV
MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
EgYDVR0TAQH/BAgwBgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGG
GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2Nh
Y2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNydDB7BgNV
HR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vRGlnaUNlcnRH
bG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYG
Z4EMAQIBMAgGBmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHer
t3onPa679n/gWlbJhKrKW3EX3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNj
OSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Zu2XHFq8hVt1hBcnpj5h232sb0HIM
ULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe50gG66sSmvKvhMNb
g0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4ZxuYRiH
as6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI
8ks5T1KESaZMkE4f97Q=
-----END CERTIFICATE-----
```

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(formart_type)一覧 参照	String

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

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

[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)

List Reissue : (単一オーダー内の)再発行した証明書一覧の取得

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/order/certificate/{{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

・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"
    }
  ]
}
```


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)オーダの場合) 証明書有効期間残日数	Int

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

List Duplicate : (単一オーダー内の)複製発行した証明書一覧の取得

cURLのサンプルコード(*1)

```
curl -X GET \
  'https://www.digicert.com/services/v2/order/certificate/{{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

・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。

レスポンス例:


```
{
  "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.dig
        "csr_url": "http://www.digicer
      },
      "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:
      "csr": "<csr>",
      "server_platform": {
        "id": 45,
        "name": "nginx",
        "install_url": "http://www.di
        "csr_url": "http://www.digicer
      },
      "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-certific
        "csr_url": "http://www.digicert.com/csr-creation-ngi
      },
      "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)オーダの場合) 証明書有効期間残日数	Int

*1: 当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

7. 再発行、複製、失効等の証明書管理

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	・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	【サーバ証明書(OV/EV)のみ】 ・証明書複製(Duplicate)を申請します
証明書の失効	・証明書失効(Revoke)の申請 ※ 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】 [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	-
years/ days/ custom_expiration_date		

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

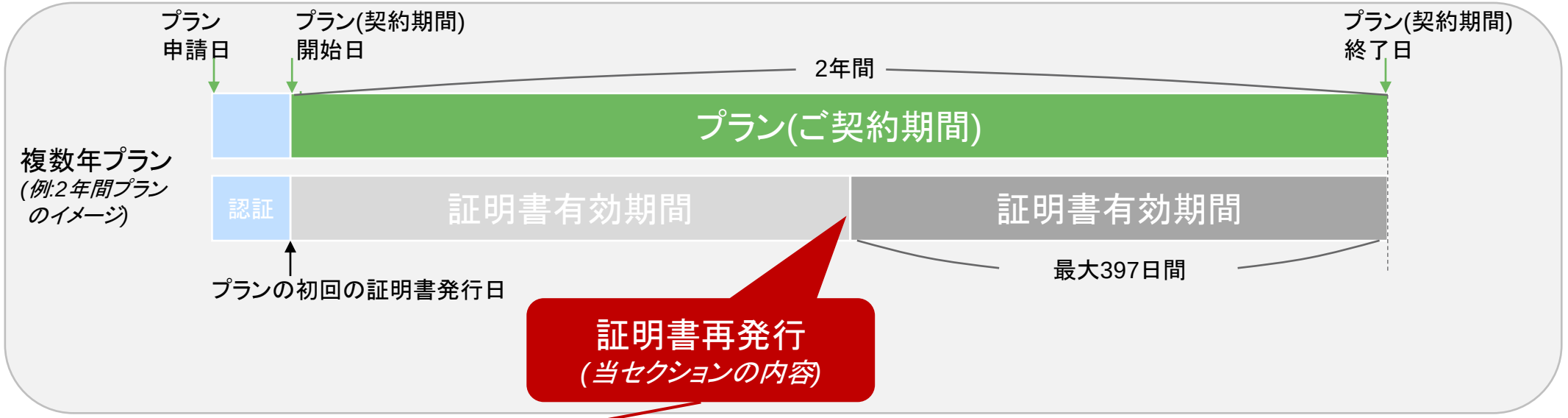
再発行申請を開始する前に、以下の注意事項をよくご確認ください。

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/

*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

（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	・サーバ証明書(OV/EV) ・サーバ証明書(プライベートSSL) ・コードサイニング証明書/EVコードサイニング証明書	・サーバ証明書(OV/EV)のみ
主な用途	・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	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)を追加する場合に必要 （注：バウチャーのご利用時など、一部のご契約体系では、 プラン途中でのFQDN(SANs)が不可である場合があります）	・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	・失効されない

Revoke order certificates：証明書の失効(オーダ/プラン単位)

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」がを必要とする ※ 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

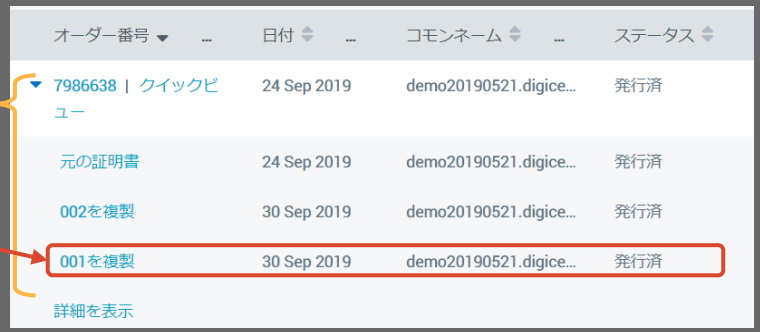
もっと詳しく：https://dev.digicert.com/services-api/orders/revoke-order-certificates/

■ 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



*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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」がを必要とする ※ 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/

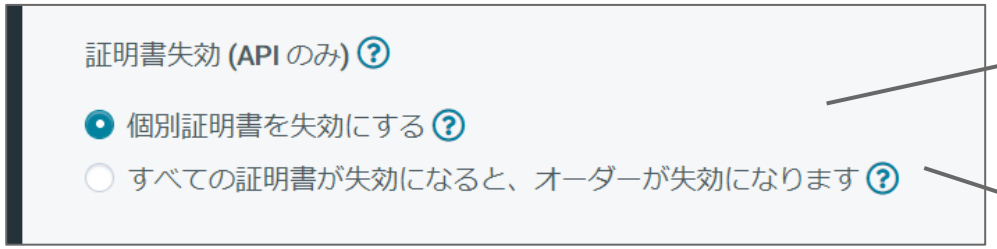
*1：当社は本サンプルコードを用いてデモ用途での動作確認を行っておりますが、お客様に対して、本サンプルコードの品質および機能がお客様の使用目的に適合することの保証を行いません。 また、本サンプルコードによりお客様または第三者に如何なる損害が生じた場合でも、一切の責任を負わないものとします。

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



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. 証明書の有効期間・更新案内通知について

【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 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)
		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。

【サーバ証明書(DV)】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(DV) 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	366日間
		2	730日間
		3~6	365*[指定した年数]
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	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	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	366日間
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(*1)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(*1)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 : 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(DV)】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(DV) 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	366日間	**左列のベース期間(新規申請時と同等)に、更新前証明書の残有効期間日数を加算します**	366 ~ 456日間
		2	730日間		730 ~ 820日間
		3~6	365*[指定した年数]		(a) + [0~90]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]と同一、ただし最大値:397日間(*1)
days	<新規申請時と同様>		
custom_expiration_date	<新規申請時と同様>		

*1 : 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。

更新案内通知について (1/2 メールテンプレート)

■更新案内通知メールのサンプル

→更新案内通知メール件名、送信元および本文イメージは、以下のようになります

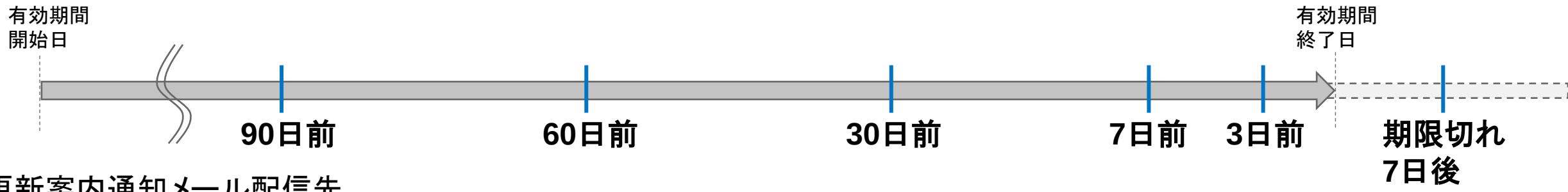
件名	[重要]証明書更新のご案内 N日間 (オーダー番号 XXXXXXXX)
送信元	DigiCert <admin@digicert.com>
本文 イメージ (抜粋)	[証明書の申請者 氏名] 様 弊社サービスをご利用いただき誠にありがとうございます。現在ご利用の証明書の有効期間は、残りN日間となりました。有効期間が切れる前に証明書の更新申請をいただきますようお願いいたします。 証明書詳細 ご申請者：[証明書の申請者 氏名] コモンネーム: [証明書のSubject CN] [オーダー詳細画面へのURL(ログイン要)]にアクセスして証明書を更新ください。 更新のお手続き 事前に証明書を更新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。 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/ 管理者からのメモ: [*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)]

※：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。

更新案内通知について (2/2 メール配信タイミング・配信先)

■更新案内通知メール配信タイミング

更新案内通知メールは、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



■更新案内通知メール配信先

#	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	アカウントメニュー**「設定」**→**「選択設定」**にて **「証明書の更新設定」**セクション内**「更新申請通知の送付先」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] 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	アカウントメニュー**「設定」**→**「通知」**にて **「すべてのアカウント通知を以下に送信」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] 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 **「Send emails to user placing order」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] 追加メールアドレス	登録済オーダーに対して**Additional Emails**エンドポイントを利用して追加指定したメールアドレス	登録済オーダー(証明書申請)に対して**Additional Emails**エンドポイントを利用してメールアドレスを追加指定した場合、このアドレスに対して配信