CertCentral Enterprise 簡易マニュアル

最終更新日：2022年 10月 5日
デジサート・ジャパン合同会社

目次

1. はじめに

はじめに

- 当資料は CertCentral Enterpriseを用いてデジサートのSSL/TLSサーバ証明書、コードサイニング証明書を申請、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
- デジサートが提供するCertCentralのご活用方法の全体像ならびに各種機能の詳細については、以下の文書を併せて参照ください
  - DigiCert documentation (ご活用方法の全体像、CertCentralの各種機能詳細)
    - URL : https://docs.digicert.com/ja/ (日本語版) または https://docs.digicert.com/ (英語版)
- 当資料では**「事前認証」方式**を中心に解説いたします。
  - **「事前認証」方式とは：**個別の証明書申請に**先立って**お客様のCertCentral Enterpriseのアカウント内に組織情報およびドメイン名情報を登録し、認証を完了させる方式を指します。認証履歴の有効期間内(およそ1年間)はこれを再利用することで、個別の証明書の申請から発行までのリードタイムを短縮することが可能です
- 当資料内の画面イメージは、表示言語として「日本語」選択時のものを採用しています
  - 表示言語については当セクション内「CertCentralを日本語でご利用いただくための各種設定について」参照
- 当資料内の画面のデザインや文言等の詳細は予告なく変更される場合があります

変更履歴

Ver.	公開日	変更点	変更箇所
~0.9	2020/11/11	省略	-
1.0	2020/11/16	[1.はじめに]「変更履歴」ページを追加	Page 5
		[9.1. サイトシール]画面およびシールデザイン変更を反映	Page 95-99
1.1	2021/1/5	・コードサイニング証明書、EVコードサイニングおよびプライベートSSL証明書製品の申請手順等を追記 ・これに伴いセクション構成を改訂	全体
		[2.3 ドメイン名利用権確認(DCV)] DCVメール(日本語)のタイトル、文面変更を反映	Page 22, 24
		[3.1 サーバ証明書(OV/EV)の申請]において「複数年プラン」の申請手順等を追記	Page 29-41
		[4.オーダー・証明書一覧管理およびレポート]に「TIPS : オーダーレポート(CSV形式)が文字化けしてしまう」追加	Page 61
		[9.1 ゲストURL] 多言語対応等に伴う改訂 (画面イメージ最新化、説明の詳細化等)	Page 103-105
1.2	2021/1/21	[9.1 ゲストURL] 機能拡充等に伴う改訂	Page 100-106
		[9.2 ゲストアクセス] 多言語対応、機能拡充等に伴う改訂 (画面イメージ最新化、説明の詳細化等)	Page 107-114
1.3	2021/2/9	[3.2 プライベートSSLの申請] [5.2 中間証明書・証明書階層構造について] プライベートSSLに関する説明を詳細化	Page 45, 79
1.4	2021/3/16	[2.2 組織(Organization)の事前認証] [8.ユーザー管理] 担当者/ユーザー情報の入力欄「部署名および組織名」変更に伴う画面イメージや入力例等の改訂	Page 14, 100
1.5	2021/8/3	各証明書の有効期間について	Page 90-93
1.6	2021/12/16	ファイル認証注意事項追記、レポートライブラリ機能、カスタムEメール機能 追加	Page 22,135,139
1.7	2022/5/20	ドメインロック機能、ドメイン一括再認証機能 追加	Page 28-30
1.8	2022/10/5	ドメイン一括再認証機能にDNS-TXT, DNS-CNAME方式を追加 [4. オーダー・証明書の一覧管理およびレポート] オーダ詳細ページ デザイン変更を反映	Page 28-29 Page 66-68

※ 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。

CertCentralへログイン

■CertCentral サインイン画面URL(日本語):
https://www.digicert.com/account/login.php?lang=ja

■CertCentralへのログイン画面

ユーザー名、パスワードを入力してください。
ログインする企業アカウントは、ユーザー名によって自動的に特定されます

TIPS 1：ユーザー名を忘れた場合
「ユーザー名を忘れましたか？」のリンクをクリックしてください。
ユーザーアカウント作成時に登録したメールアドレスにユーザー名を通知します。

TIPS 2：パスワードを忘れ　　た場合
「パスワードを忘れましたか？」のリンクをクリックしてください。
ユーザーアカウント作成時に登録したメールアドレス、「秘密の質問」を使って
パスワードを再設定いただくことが可能です。

TIPS 3：アカウントロックがかかった場合
複数回ユーザー名およびパスワードを間違えた場合、アカウントロックがかかる場合があります。解除についてはデジサートのテクニカルサポートまでお問合せください。

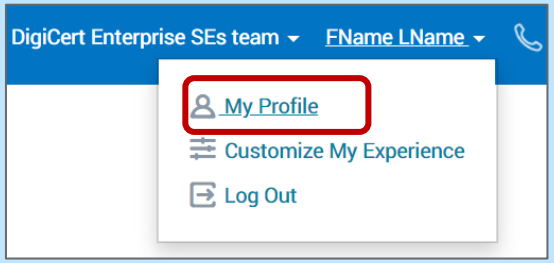
CertCentralを日本語でご利用いただくための各種設定について

区分	設定方法

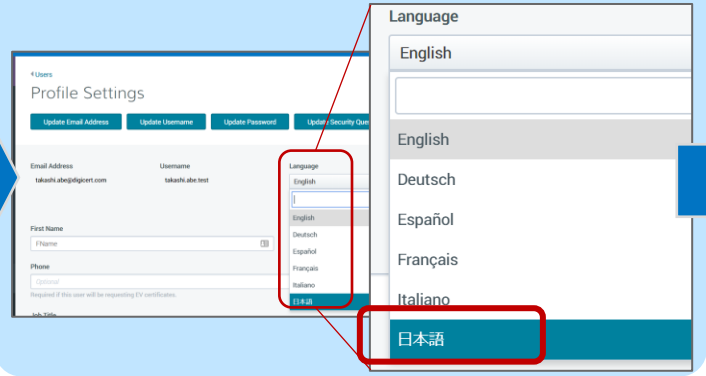
画面表示言語

■CertCentralの画面表示言語を英語→日本語へ切り替える手順

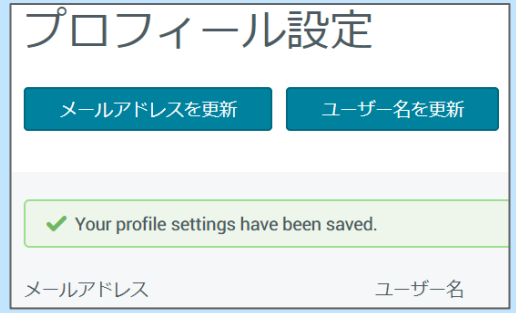
STEP 1：画面右上部の「My Profile」をクリックして「Profile Setting」画面を開きます



STEP 2：画面右側の「Language」プルダウンリストから「日本語」を選択します



STEP 3：下のようなメッセージが表示され、画面の表示文言が日本語に切り替われば完了です

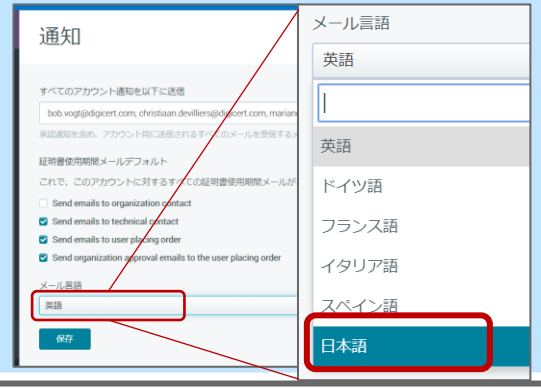


メール言語

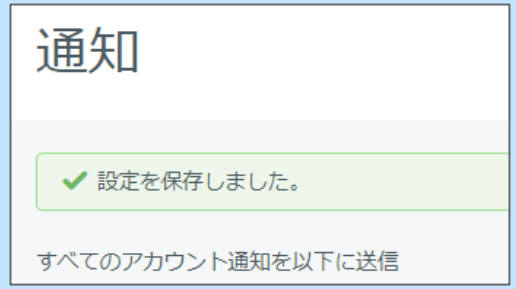
■CertCentralから配信されるメール（※DCVメールを除く）の画面を英語→日本語へ切り替える手順

STEP 1：画面左メニューの「設定」から「通知」クリックして「通知」画面を開きます

STEP 2：画面下部の「メール言語」プルダウンリストから「日本語」を選択します（注1）



STEP 3：下のようなメッセージが表示されれば完了です



注1：[保存]ボタンを押下いただく前に画面上部の[すべてのアカウント通知を以下に送信]にメールアドレスを登録ください。
同欄にメールアドレスが未登録の場合、設定を保存できません。この欄に設定いただいたメールアドレスには、アカウント内で発行された証明書の発行通知や証明書更新案内メールなどが配信されます。複数のメールアドレスを指定する時は、カンマで区切って入力ください。

2. 事前認証（組織およびドメイン名の管理）

~ 2.1 ワークフロー ~

製品カテゴリー別 ワークフロー

■ワークフロー概要

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

	製品カテゴリ	SSL/TLSサーバ証明書			コードサイニング証明書	
		OV (企業認証)	EV (Extended Validation)	Private SSL (プライベートSSL)	CS (企業認証)	EVCS (Extended Validation)
	具体的な製品名の例	セキュア・サーバID	セキュア・サーバID EV	Private SSL OV	コードサイニング証明書	EVコードサイニング証明書
「組織」の事前認証	組織 (Organization) の事前認証	必要 →セクション2.2				
	認証済連絡先 (Verified Contact) の事前認証	不要	必要 →セクション2.3	不要	必要 →セクション2.3	必要 →セクション2.3
ドメインの事前認証	ドメイン名の事前認証	必要 (DCV方式をメール認証、ファイル認証、DNS認証から選択) →セクション2.4			不要	

デジサートによる「組織」の事前認証 概要

■「組織」の事前認証における「担当者」の種類と役割
・CertCentral Enterpriseにおける事前認証の段階では、**「申請責任者」**および**「認証済連絡先」**を決定いただきます。
・各担当者は同一の方に兼任いただくことも可能です。

	役割
申請責任者 (Organization Contact)	・CertCentral Enterprise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。 ・CertCentral Enterpriseに登録する1つの「組織」に対して1名を紐づけてアサインいただきます(必須、変更可能)
技術責任者 (Technical Contact)	・申請責任者(Organization Contact)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。 ・（「組織」の事前認証時ではなく）証明書申請時に、「組織」に紐づける形でご登録いただきます。
認証済連絡先 (Verified Contact)	・**EV SSL証明書**、**コードサイニング証明書**および**EVコードサイニング証明書**について、これらの製品カテゴリごとに申請団体を代表してCertCentral Enterpriseでの申請を承認する権限を持つ方としてアサインいただきます ・CertCentral Enterpriseに登録する1つの「組織」に対して1名または複数名を紐づけてアサインいただきます(変更可能) ・組織の認証申請時にデジサートより電話認証（在籍および権限の確認など）させていただきます ・認証済連絡先の方は、**証明書申請の都度**、申請を承認いただきます(詳細後述)

*1：[CCE] 各担当者（連絡先）の役割について：https://knowledge.digicert.com/ja/jp/solution/SO280058.html

*2：電話認証の詳細については以下Knowledge Baseを参照ください。
[CCE]電話認証の手順について（SSL証明書/EV SSL証明書）：https://knowledge.digicert.com/ja/jp/solution/SO280056.html
[CCE]電話認証の手順について（コードサイニング証明書）：https://knowledge.digicert.com/ja/jp/solution/SO280057.html

2. 事前認証（組織およびドメイン名の管理）

~ 2.2 組織(Organization)の事前認証 ~

組織(Organization)の管理

■「証明書」→「組織」メニュー選択時

・メイン画面の左ペインメニューから、
「証明書」→「組織」を選択してください。

・登録された組織の一覧が表　　示されます。
(初期状態では、アカウント作成時に入力いただいた
組織名のみが表示されています)

・新しい申請団体に対して証明書を申請する場合の事前認証を行う場合：
→**「新しい組織」**ボタンを押下して組織情報を登録いただけます。

・登録済の申請団体に対して認証申請を行う場合：
→一覧に表示された組織を選択して**「組織詳細/認証申請」**画面に
進んで、組織情報を管理いただけます。

組織(Organization)の管理 – 新しい組織の登録 (1/2:組織の詳細)

■「新しい組織」の登録画面

■組織情報の入力項目の説明・入力/選択例

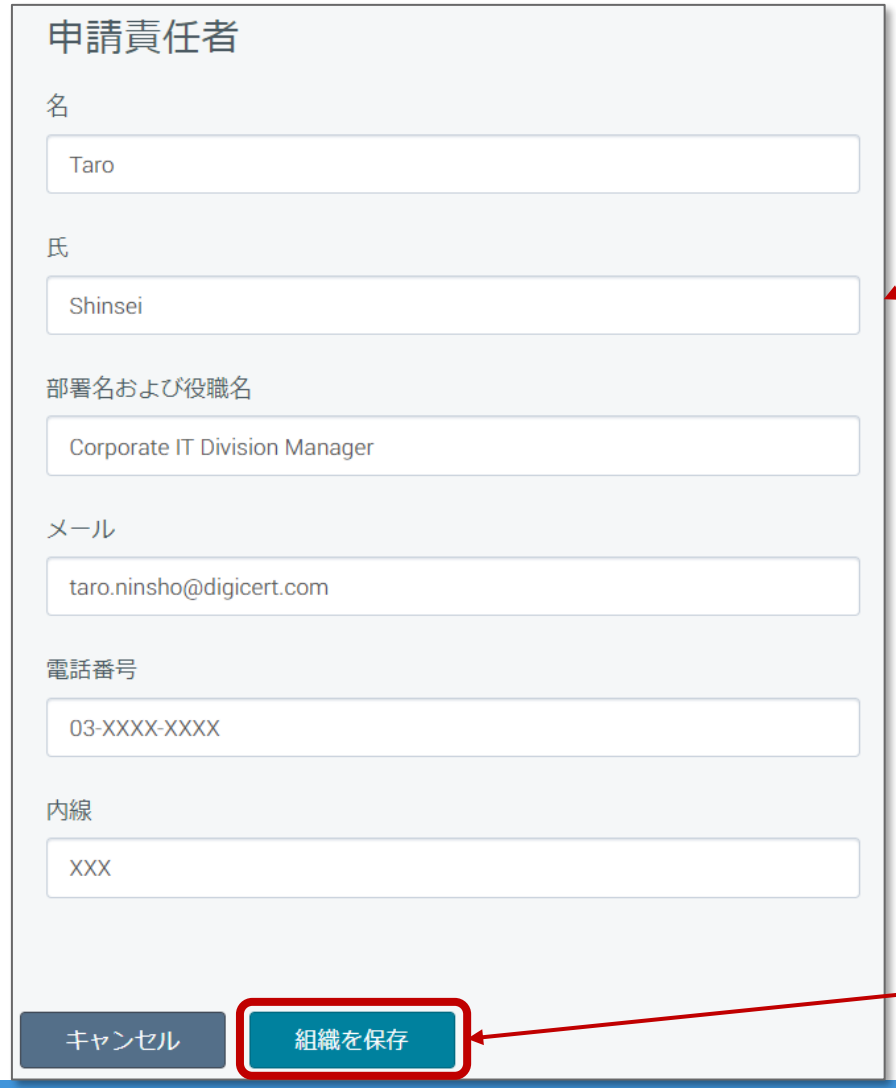
項目名	概要	入力/選択例
正式名称	【証明書のSubject O】 申請団体の正式名称 (日本語、英語いずれも可)	・<日本語組織名の場合>: デジサート・ジャパン合同会社 ・<英語組織名の場合>: DigiCert Japan G.K.
一般名称	<入力不要>	
組織の電話番号	申請団体の電話番号	03-XXXX-XXXX
国	【証明書のSubject C】 「Japan」を選択	Japan
住所1	申請団体所在地・市区町村より下のレベル(番地等)	例1 : 6-10-1 Ginza 例2 : 580-16 Horikawa-cho
住所2	<入力不要>	
市町村名	【証明書のSubject L】 申請団体所在地・市区町村名	例1 : Chuo-ku 例2 : Kawasaki-shi
State / Province / Region	【証明書のSubject S】 申請団体所在地・都道府県名	例1 : Tokyo 例2 : Kanagawa
Zip / Postal Code	申請団体所在地・郵便番号	104-0061

その他のパターンの記入例については以下のFAQを併せてご参照ください。
https://knowledge.digicert.com/ja/jp/solution/SO22977.html

※ 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りますので、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。

組織(Organization)の管理 – 新しい組織の登録 (2/2:申請責任者)

■「新しい組織」の登録画面



■申請責任者の入力項目の説明・入力/選択例

項目名	概要	入力例
名	申請責任者氏名の名	Taro (※1)
氏	申請責任者氏名の氏	Ninsho (※1)
部署名および役職名	申請責任者氏名の部署名および役職名	Corporate IT Division Manager (※1)
メール	申請責任者氏名の電子メールアドレス	taro.ninsho@digicert.com
電話番号	申請責任者氏名の電話番号	03-XXXX-XXXX
内線	【任意】申請責任者氏名の内線番号	XXX

	役割
申請責任者 (Organization Contact)	・CertCentral Enterpriseで発行する証明書の発行対象となる組織(Subject O)を代表する担当者 ・CertCentral Enterpriseに登録する「組織」に対して1名を紐づけてアサインいただきます(必須、変更可能) ・組織の認証申請時にデジサートより電話認証（在籍および権限の確認など）させていただきます(認証履歴はその有効期間内(およそ1年間)は再利用されます)

以上で入力は終了です。「組織を保存」ボタンを押下してください。
続けて認証申請(電話認証などの認証の開始リクエスト)を行う場合は、
「証明書」→「組織」メニューから「組織詳細/認証申請」画面へ進んでください。

※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。

組織(Organization)の管理 – 認証申請：認証タイプの選択

■「組織詳細/認証申請」画面

・表示された組織情報詳細画面下部の「組織認証の申請」欄で、
必要な認証タイプ(OV, EV, CSなど(*))を選択してください。

*1：ご注意ください：ご契約条件によって表示される認証タイプが左の画面と異なる場合があります。区分については[2.1 ワークフロー]を参照ください。ご契約条件の詳細はデジサートの営業担当者にお問合せください

・【「EV」、「CS」または「EVCS」を含む場合】
「連絡先を追加」をクリックして「認証済連絡先」(Verified Contact)」を追加します
次セクションのガイドに従って入力してください

・必要な項目の入力が終了したら**「認証申請」**ボタンを押下してください。
→弊社側で入力いただいた組織(Org)情報の事前認証を開始いたします。
事前認証した組織(Org)を用いたドメイン名の事前認証、証明書申請は、
組織(Org)の事前認証が完了した後に進めていただけるようになります

2. 事前認証（組織およびドメイン名の管理）

~ 2.3 認証済連絡先(Verified Contact) ~

認証済連絡先の役割と（証明書申請の都度）オペレーションのパターン

■「認証済連絡先」の役割（再掲）

認証済連絡先 (Verified Contact)	・**EV SSL証明書**、**コードサイニング証明書**および**EVコードサイニング証明書**について、 CertCentral Enterpriseで申請団体を代表してこれらの証明書の発行を承認する権限を持つ方 ・CertCentral Enterpriseに登録する組織に対して1名または複数名を紐づけてアサインいただきます（変更可能） ・組織の認証申請時にデジサートより電話認証（在籍および権限の確認など）させていただきます ・認証済連絡先の方は、**証明書申請の都度**、申請を承認いただきます（詳細後述）

■証明書申請の都度「認証済連絡先」の方が担う役割

	条件1：アカウント設定	条件2：証明書申請の条件	CertCentral Enterpriseの動作
パターン1【推奨】	[認証済連絡先]がCertCentral Enterpriseのユーザー**である**場合	[認証済連絡先]**自身**(※)がCertCentralにログインして証明書を申請した場合 ※ Administrator/Manager権限の場合	証明書が発行されます（追加の操作は不要）
パターン2		[認証済連絡先]**以外**のCertCentralユーザーが証明書を申請した場合	アカウントの管理者(Administrator/Manager権限を持つユーザ)に宛てて証明書申請の承認が必要なことを通知するメールが送信されます。[認証済連絡先]ユーザーがCertCentralにログインし、証明書申請を承認いただくと、証明書が発行されます。
パターン3	[認証済連絡先]がCertCentral Enterpriseのユーザー**ではない**場合	-	デジサートの認証担当者が申請内容を確認後、[認証済連絡先]に宛てて証明書申請の【承認申請メール(※1)】が配信されます。 メールを受信した[認証済連絡先]の方が承認操作を完了させると、証明書が発行されます。

もっと詳しく：[FAQ]EV SSL/コードサイン/EVコードサイン証明書の申請・発行承認について：https://knowledge.digicert.com/ja/jp/solution/SO23322.html

※ [認証済連絡先]自身のアカウントユーザーがAdministrator/Manager権限を持つこと、またアカウント設定「設定」→「選択設定」→「詳細設定」→「承認手順」メニューにおける証明書申請後の 「申請レビュー・承認」プロセスが「(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)」または「常に1ステップ承認」であること。「申請レビュー・承認」の詳細は「3.1 サーバ証明書(OV/EV)の申請」を参照

パターン1【推奨】 組織(Organization)の管理 – 「認証済連絡先」の追加

■「認証済連絡先」の追加手順 (前ページ パターン1の場合)

*1：ご注意ください：お客様のアカウントの設定によって「新しい連絡先」が表示されない場合があります。
「新しい連絡先」を表示させるには、Administrator権限を持ったユーザが「設定」→「選択設定」
メニューを開き、「詳細設定」→「有効な連絡先」セクションで、「DigiCert アカウントに未登録の
ユーザーを有効な認証連絡先として使用」というラベルのチェックボックスをONにして
「設定を保存」を押下してください。

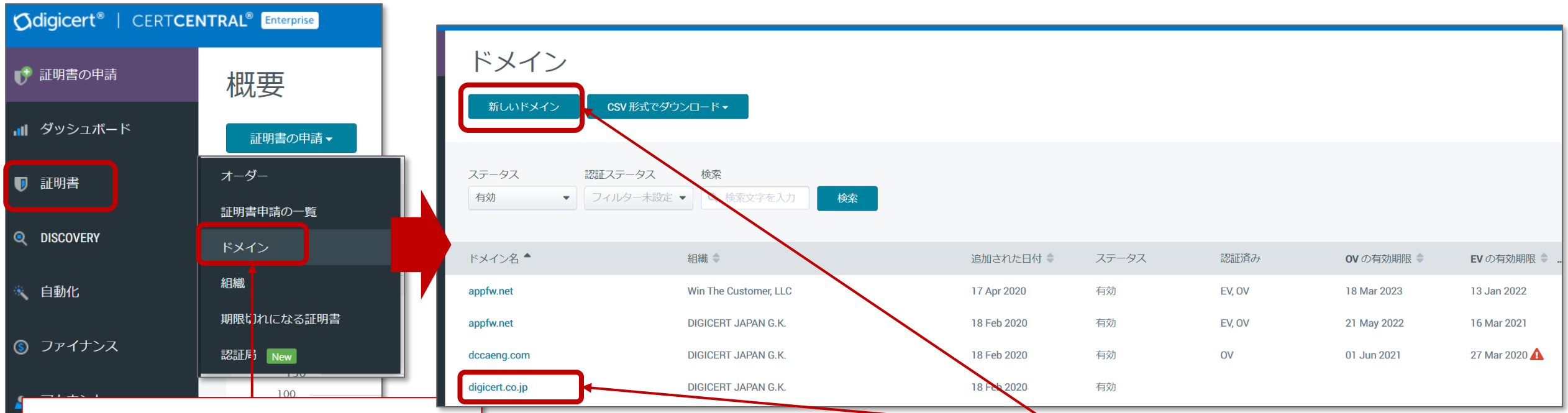
・[認証済連絡先]が承認(/申請)する証明書カテゴリを選択してください
EV：EV SSL証明書
CS：コードサイニング証明書
EV CS：EVコードサイニング証明書
・「認証申請」ボタンを押下して申請を確定させてください

2. 事前認証（組織およびドメイン名の管理）

~ 2.4 ドメイン名の事前認証 ~

ドメイン名(Domain)の管理 – 新しいドメイン名の登録 (1/2)

■「証明書」→「ドメイン」メニュー選択時



・メイン画面の左ペインメニューから、
「証明書」→「ドメイン」を選択してください。

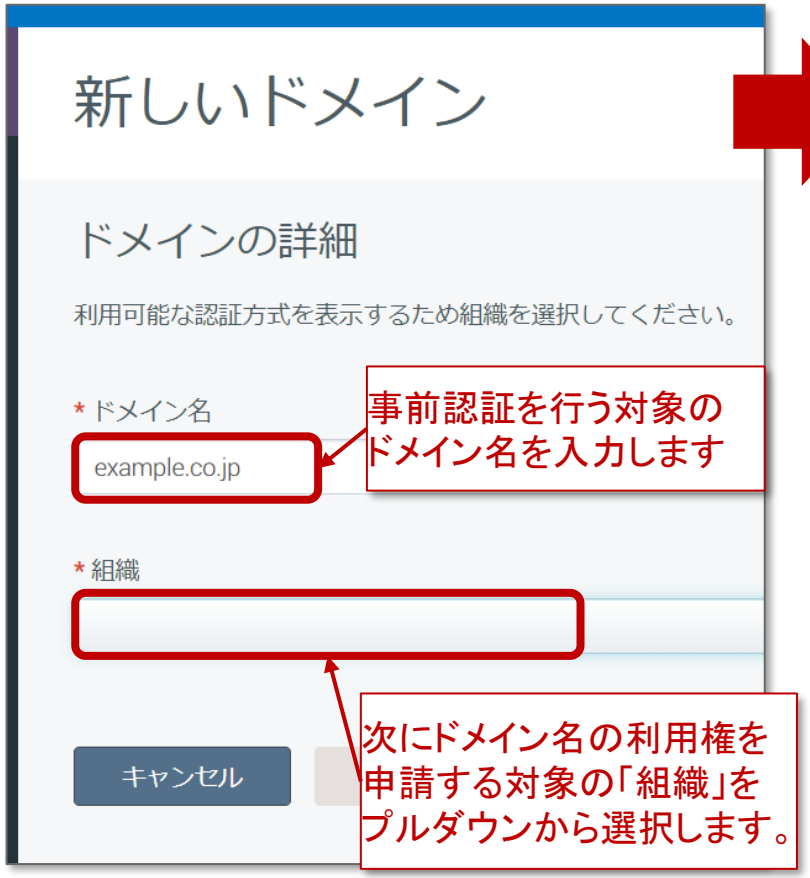
登録されたドメイン名の一覧画面が表示されます(初期状態では空欄)

・新しいドメイン名の登録および事前認証(DCV)を行う場合:
→「新しいドメイン」ボタンを押下してください。

・登録済のドメイン名に対して再認証(DCV)申請を行う場合:
→一覧に表示されたドメイン名を選択して「ドメイン詳細/認証申請」画面に進んでください。

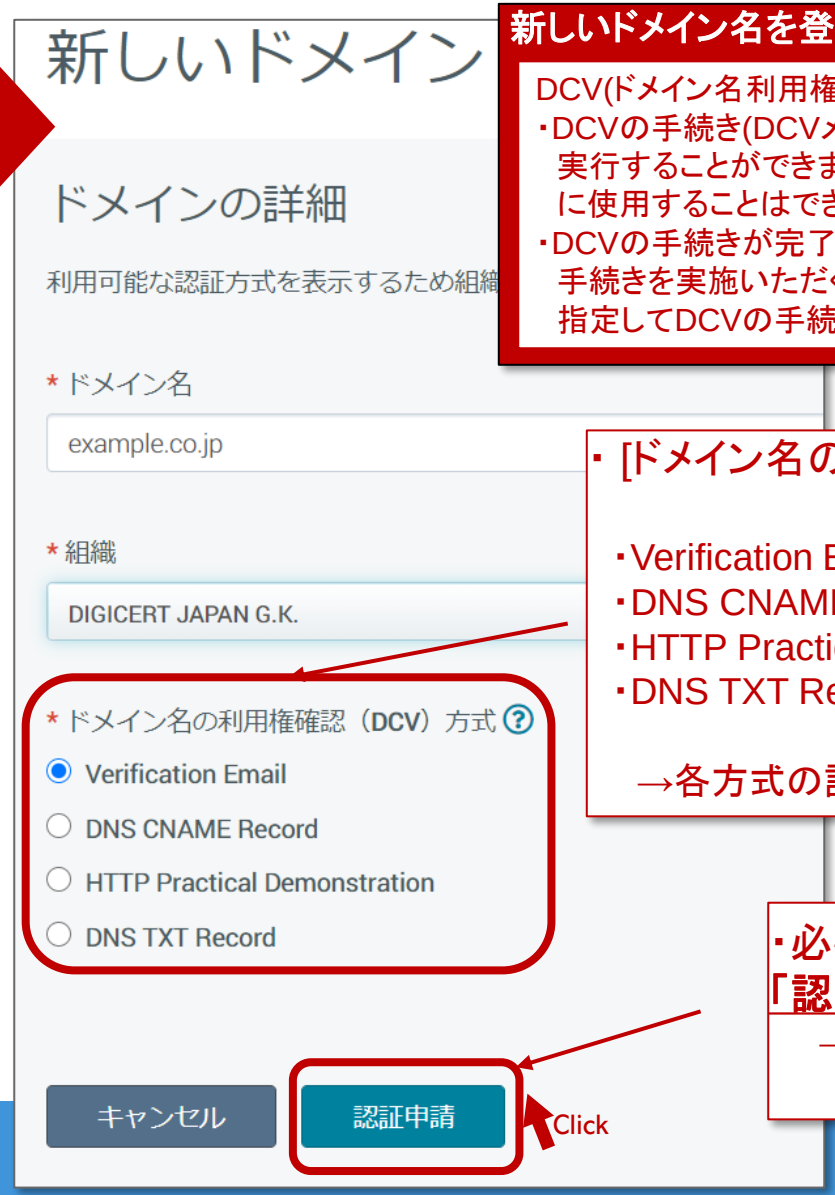
ドメイン名(Domain)の管理 – 新しいドメイン名の登録 (2/2)

■「新しいドメイン」画面



事前認証を行う対象のドメイン名を入力します

次にドメイン名の利用権を申請する対象の「組織」をプルダウンから選択します。



新しいドメイン名を登録する際は、以下の点について留意ください

DCV(ドメイン名利用権確認)の有効性は対象の「組織」との組合せで管理されます
- DCVの手続き(DCVメールの送受信やファイル認証等)は「組織」の認証完了前でも実行することができますが、「組織」の認証が完了するまでドメイン名を証明書発行に使用することはできません
- DCVの手続きが完了した後に「組織」の名称が変更となった場合、再度DCVの手続きを実施いただくことが必要となる場合があります。認証完了済の「組織」を指定してDCVの手続きを開始いただくことを推奨いたします。

- [ドメイン名の利用権確認(DCV)方式]を選択してください
  - Verification Email：メール認証
  - DNS CNAME Record：DNS認証(CNAME RRを利用)
  - HTTP Practical Demonstration： ファイル認証
  - DNS TXT Record：DNS認証(TXT RRを利用)

  →各方式の詳細は**次ページ**を参照ください。

- 必要項目の選択が終了したら**「認証申請」**ボタンを押下してください。
  →デジサート側で入力いただいた情報を元にドメイン名の利用権確認を開始いたします。

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	内容
メール認証	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] ■送信元アドレス：no-reply@digitalcertvalidation.com
ファイル認証	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。ワイルドカードではご利用いただけません。 ■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	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	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

各DCV方式の詳細 – 「メール認証」の場合 (1/2)

■(「事前認証」の場合)DCVメールの送信先

例1：登録/認証申請ドメイン名=「example.com」の場合

→DCVメールの配信先は常に右の通りとなります。

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

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

→DCVメールのデフォルトの配信先は常に右の通りとなります。

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

（参考）ドメイン詳細画面のイメージ

※1：DCVメールの「再送」について
DCVが「承認待ち(Pending)」状態にある場合、CertCentral上のドメイン詳細画面
（「証明書」→「ドメイン」→一覧に表示されるドメイン名をクリックして開く画面）の下部の
「メールを再送する」リンクをクリックいただくことで、上記と同一のDCVメールを再送いただくことが可能です。

※2：DCVメール送信先の変更のについて
確認対象のドメイン名がサブドメイン名を含む場合に、サブドメイン名を含まないメールアドレスを利用すること
(例：上記例2の場合にDCVメールを admin@example.com に送信する)を希望の場合は、お手数ですが、
弊社認証サポートチームまでアカウント番号、ドメイン名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 (2/2)

■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]
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(※2)> 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(※1)

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

各DCV方式の詳細 – 「ファイル認証」の場合

■ファイル認証用「ランダムな認証トークン」の取得・利用方法

〇STEP 1 : ドメイン名の登録時に、[ドメイン名の利用権確認(DCV)方式]として「HTTP Practical Demonstration(ファイル認証)」を選択します

〇STEP 2 : 認証トークンの取得

登録後に表示されるドメイン詳細画面の下部に、以下のように認証トークン情報(※1)および配置URLが表示されます

〇STEP 3 : 認証トークンファイルの作成および配置

ランダムな認証トークンを含んだファイル（テキストエディタ等で作成）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、配置します(配置URL：STEP 2で取得した配置URL)

〇STEP 4 : 認証トークンファイルのチェック

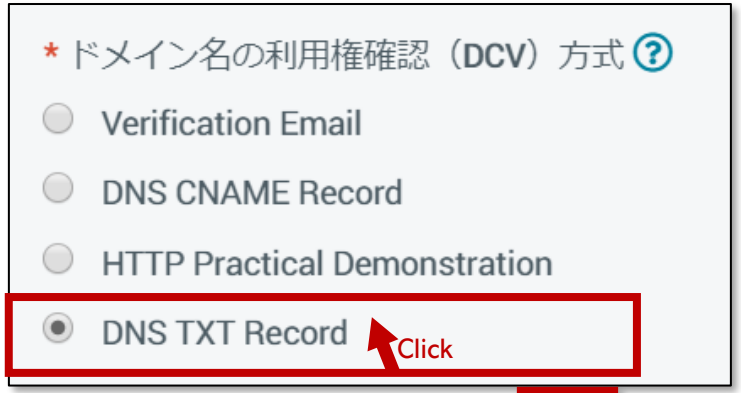
同画面内の「HTTPトークンを確認する」ボタンを押下すると、デジサートが規定の場所に正しく認証トークンファイルが配置されているか確認します。
確認が成功すると、DCVプロセスは完了です

※1 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。ワイルドカードドメインにはご利用いただけません。またマルチドメインを利用する場合は各FQDN毎に認証を実施いただく必要があります。

各DCV方式の詳細 – 「DNS TXT認証」の場合

■DNS TXT認証用「ランダムな認証トークン」の取得・利用方法

〇STEP 1 : ドメイン名の登録時に、[ドメイン名の利用権確認(DCV)方式]として「DNS TXT Record(DNS TXT認証)」を選択します

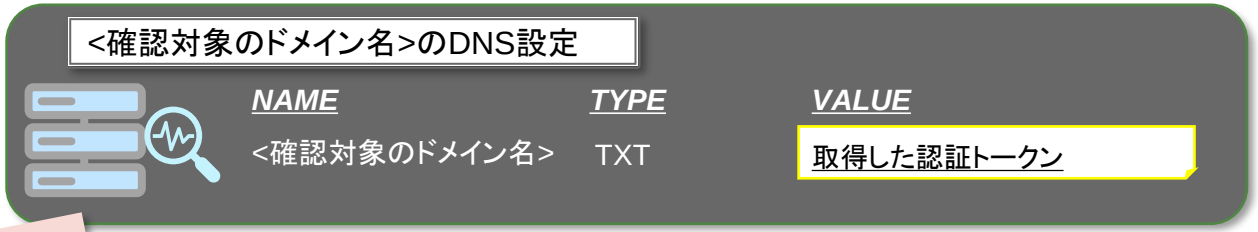


〇STEP 2 : 認証トークンの取得

登録後に表示されるドメイン詳細画面の下部に、以下のように認証トークン情報(※1)およびDNS TXTリソースレコード設定イメージが表示されます

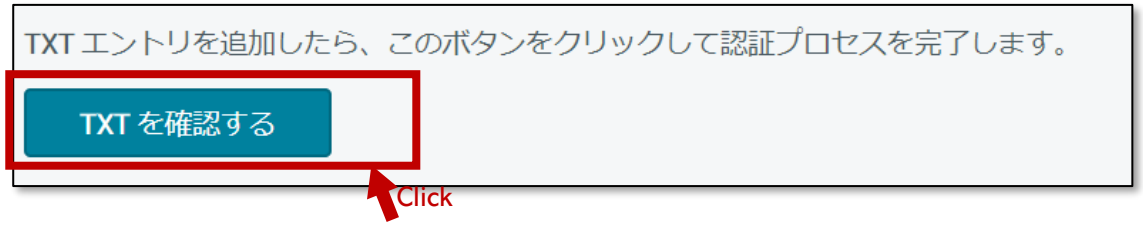
〇STEP 3 : 認証用DNS TXTリソースレコードの設定

STEP 2で取得したランダムな認証トークン情報を値(Value)として、確認対象のドメイン名のDNS TXTレコードを設定します。



〇STEP 4 : DNS TXT リソースレコードのチェック

同画面内の「TXTを確認する」ボタンを押下すると、デジサートが規定の方法でDNS TXTリソースレコードに正しく認証トークンが設定されているか確認します。
確認が成功すると、DCVプロセスは完了です

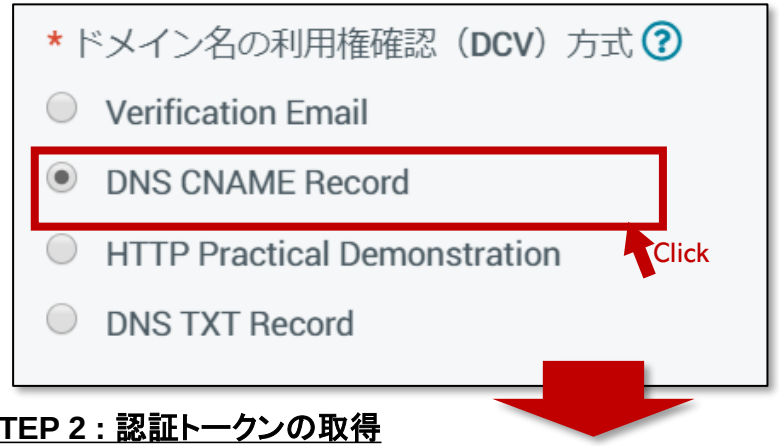


※1 当ページに記載されているトークンはサンプルであり、実際にはご利用いただけませんのでご注意ください
認証トークンの有効期間は30日間となります。一度使用した認証トークンは再利用できません。

各DCV方式の詳細 – 「DNS CNAME認証」の場合

■DNS CNAME認証用「ランダムな認証トークン」の取得・利用方法

〇STEP 1 : ドメイン名の登録時に、[ドメイン名の利用権確認(DCV)方式]として「DNS CNAME Record(DNS CNAME認証)」を選択します

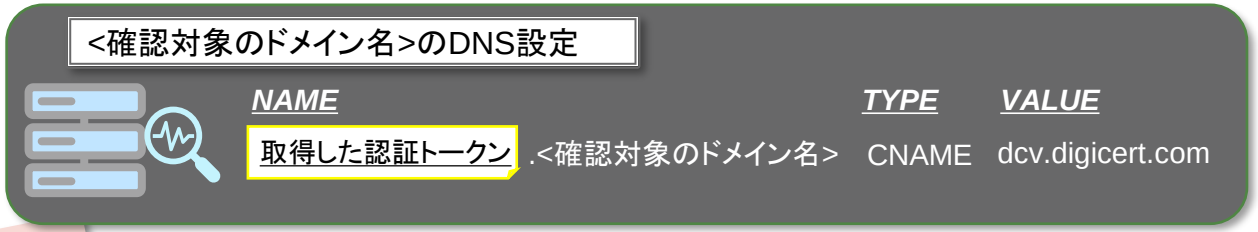


〇STEP 2 : 認証トークンの取得

登録後に表示されるドメイン詳細画面の下部に、以下のように認証トークン情報(※1)およびDNS CNAMEリソースレコード設定イメージが表示されます

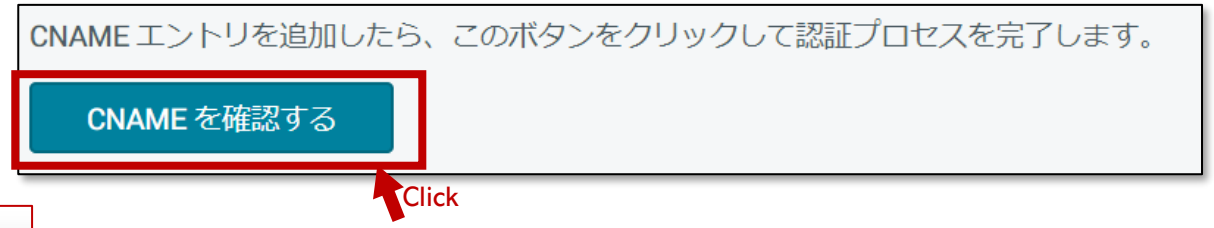
〇STEP 3 : 認証用DNS CNAMEリソースレコードの設定

STEP 2で取得したランダムな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



〇STEP 4 : DNS CNAMEリソースレコードのチェック

同画面内の「CNAMEを確認する」ボタンを押下すると、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正しく設定されているか確認します。
確認が成功すると、DCVプロセスは完了です



※1 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。

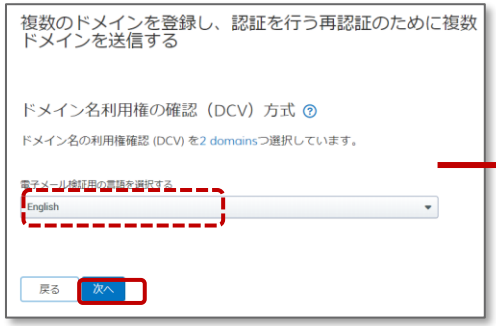
便利な機能：ドメインの再認証 ～ 一括認証機能 ～ (1/2)

登録済みのドメインに対して、まとめて再認証をリクエストすることができます。

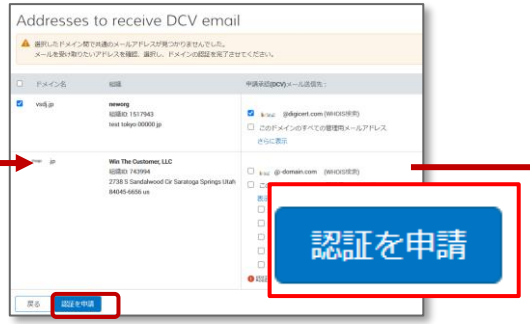
1) 認証を行うドメインを選択(✓)し、**[再認証のためにドメインを送信する]** ボタンを押下します。
2) DCV方式が表示されますので、希望するDCV方式を選択します。選択したDCV方式は、選択したドメイン全てに適用されます。
   - Eメールでの再認証
   - DNC CNAMEレコードでの再認証
   - DNS TXT
3) DCV方式を選択すると、方式毎に次のステップが表示されます。画面に表示される手順に従って再認証のリクエストを行います。なお、現在認証が保留されているドメインに対しても実施することができますが、この操作を行うと過去に発行された認証トークンは無効となり、新しい認証用トークンが適用されます。

便利な機能：ドメインの再認証 ～ 一括認証機能 ～ (2/2)

Eメールによる再認証



1) Eメール言語を選択し**[次へ]**



2)宛先を選択し**[認証を申請]**

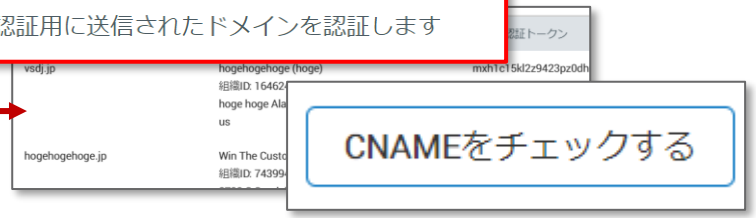
3) DCVメール配信完了

4) メールを受信したドメインオーナーが承認操作を行い認証を完了します

DNC CNAME レコードでの再認証

DNS TXT レコードでの再認証

(※基本的な操作は同じ)



1) 対象ドメインと現在のステータスを確認
[認証のためにドメインを送信する]を押下

2) 対象ドメイン毎の認証トークン取得
- **[CSVをダウンロードする]**･･･ドメイン毎の認証トークンが記載されているCSVファイルを取得
- **[トークンを表示して、再認証用に送信されたドメインを認証します]**･･･認証用トークンを画面上で表示

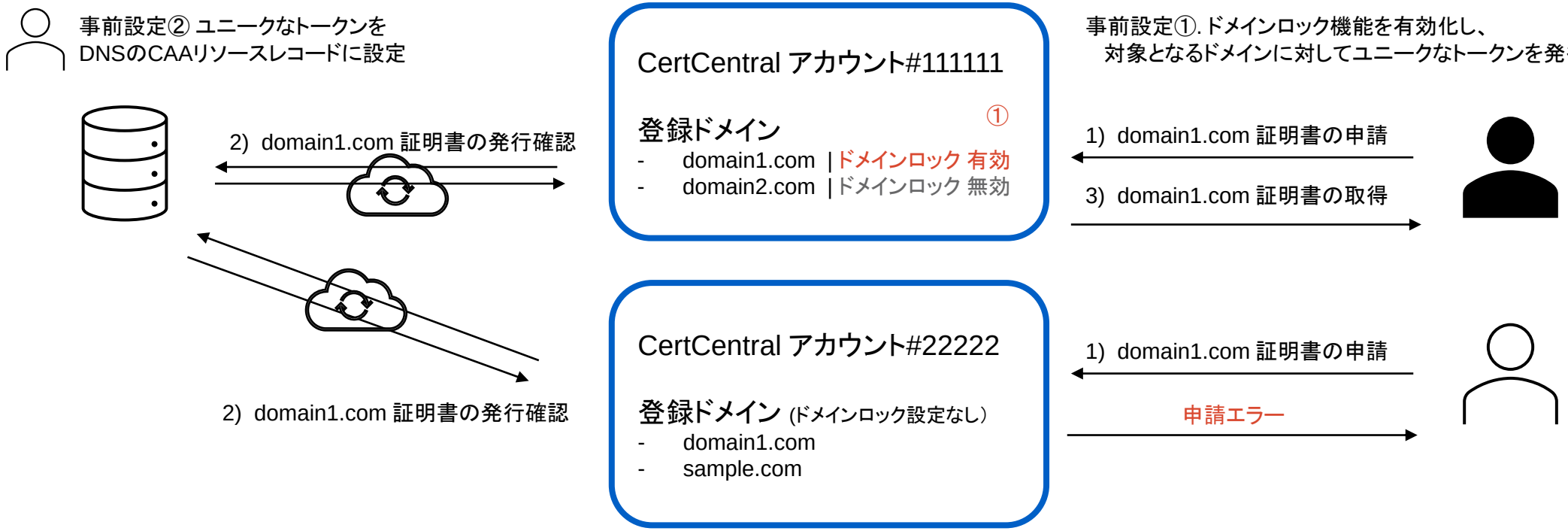
3) 認証用トークンをDNS（CNAME、またはTXT）リソースレコードに設定
4) **[CNAMEをチェックする]** または **[TXTをチェックする]**を押下し、デジサートによる認証を依頼
5) デジサートが設定された認証用トークンを確認し、認証を完了

便利な機能： ドメインロック機能 -ドメインロックとは -(1/2)

ドメインロック機能を利用して、指定するドメインに対して証明書を発行できるCertCentralアカウントを制限することができます。

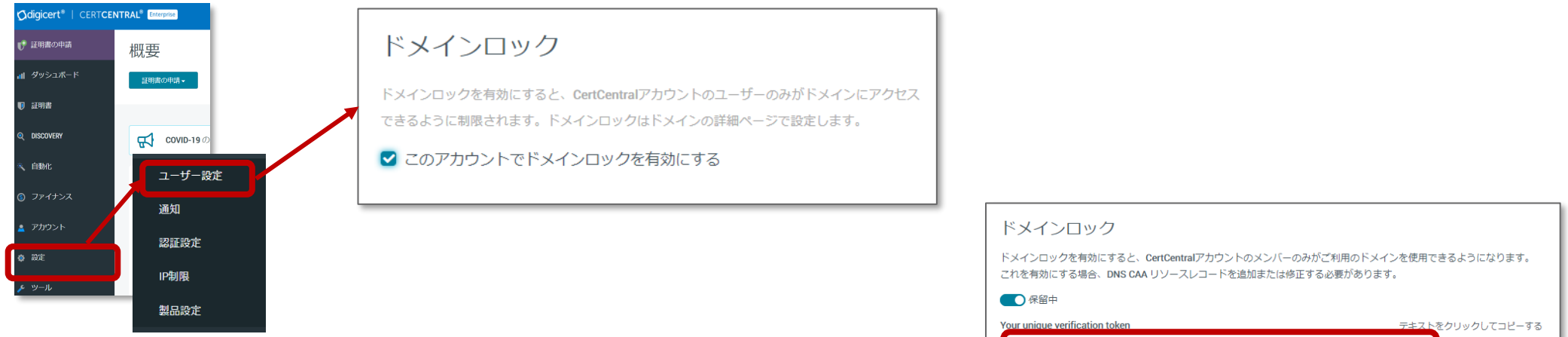
利用例） 複数のCertCentralアカウントから証明書の申請があり発行承認プロセスが煩雑、簡素化したい
自社ドメインに対して発行されるSSL/TLSサーバ証明書を一元管理したい

■ドメインロックの仕組み

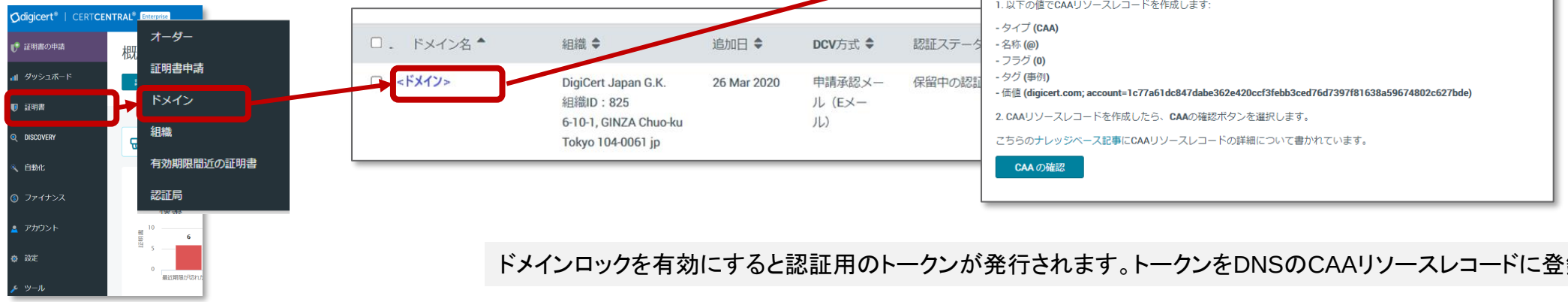


便利な機能： ドメインロック - 設定方法 - (2/2)

■「ドメインロック機能」初期設定： メニュー(「設定」＞「ユーザ設定」詳細設定→ ドメインロックをチェックして有効にします (※1)



■「ドメインロック機能」利用手順： 対象となるドメインを選択して設定します。



ドメインロックを有効にすると認証用のトークンが発行されます。トークンをDNSのCAAリソースレコードに登録します。

3. 証明書の申請

~ 3.1 サーバ証明書(OV/EV)の申請 ~

サーバ証明書(OV/EV)証明書の申請～発行までの流れ

■セクション「2.事前認証」の範囲

製品カテゴリ		SSL/TLSサーバ証明書	
		OV(企業認証)	EV(Extended Validation)
「組織」の事前認証	組織 (Organization)	セクション2.2 参照	
	認証済連絡先 (Verified Contact)	不要	セクション2.3 参照
ドメインの事前認証	ドメイン名	セクション2.4 参照	

■当セクションの範囲

証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
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

■セクション「5.証明書の取得」

証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)

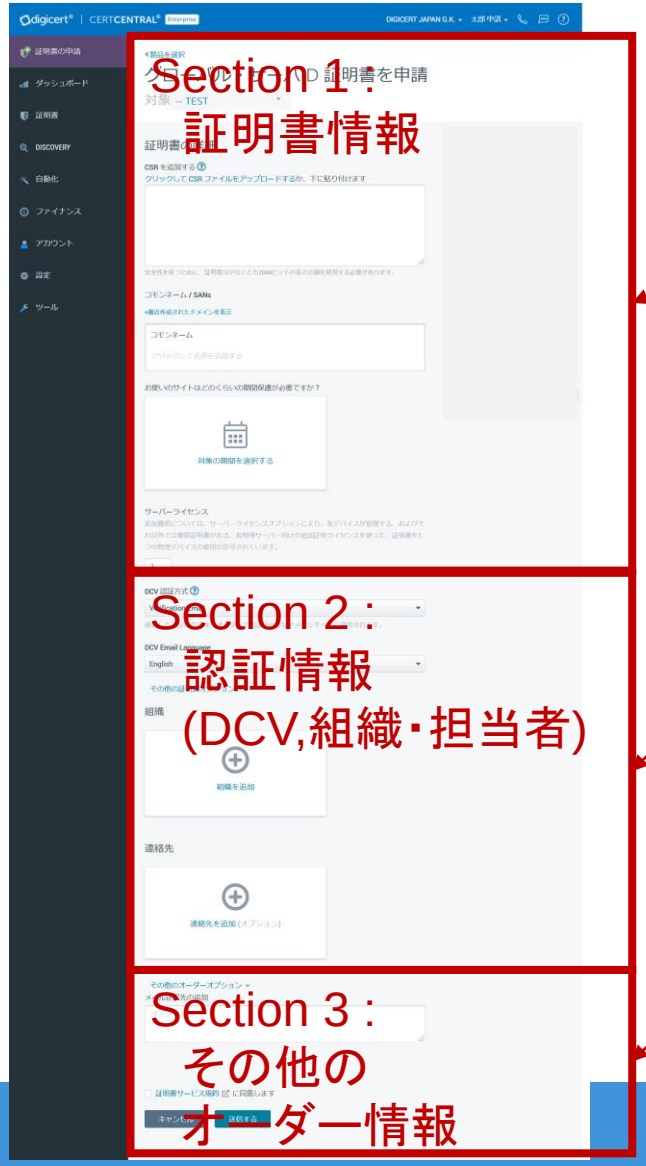
■セクション「6.証明書管理」

証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

サーバ証明書(OV/EV)の申請画面 (新規/更新申請 共通)

証明書の申請	・製品を選択 ・プランのお申込み(証明書を申請)
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■「証明書の申請」メニューからサーバ証明書(OV/EV)製品選択後に表示される「申請情報入力画面」



Section 1：以下のような「証明書情報」を入力します。
- CSR
- コモンネーム／SANsの指定
- プラン(ご契約期間)／証明書有効期間の選択

Section 2：次に以下のような組織・担当者情報、DCVなどのOV/EV証明書の認証に必要な情報を入力します。
- ドメイン名利用権確認(DCV)の方式指定
- 申請団体の組織情報
- 申請責任者／技術担当者
- (EV証明書申請時のみ)認証済連絡先

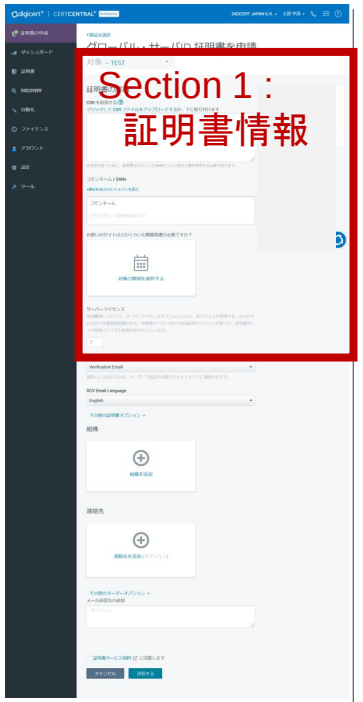
Section 3：最後にその他の情報を入力、利用規約を確認いただきます。
- その他のオーダーオプション
- 証明書サービス利用規約の確認

次ページ以降で詳細な入力方法をガイドします。

新規申請 Section 1 (OV/EV共通) : 証明書情報の入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■【任意】管理グループ(Division)の選択
・デフォルトの管理グループが選択された状態
・特定の(追加)管理グループに紐づけた証明書申請を行う場合にのみ、クリックして表示される一覧から選択してください。
(管理グループについての詳細はセクション 9.3を参照)

■【必須】CSRの設定
・「クリックしてCSRファイルをアップロードする」をクリックしてCSR(テキストファイル形式)をアップロードしていただく、または
・入力欄にクリップボードからCSRを貼り付けてください。

■【必須・自動設定あり】コモンネーム / SAN
・初期状態からCSRを貼り付けた場合、CSRの内容から抽出したコモンネーム(Subject CN)を自動設定します
・任意の値に上書き可能です
・CSRの内容と異なる値を入力した場合、当欄に設定した値が優先して申請に利用されます
・入力欄の下部にSANsに追加したいドメイン名を追記いただくことが可能です(※1)
・SANsの入力数量には上限がある場合があります(※2)

■【必須】期間:
・ご申請いただくプラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択ください
・プラン選択後、プランの初回にご取得いただく証明書の有効期間を選択・指定いただけます(最大397日間)
→詳細は次ページ[補足 プランの選択]をご参照ください

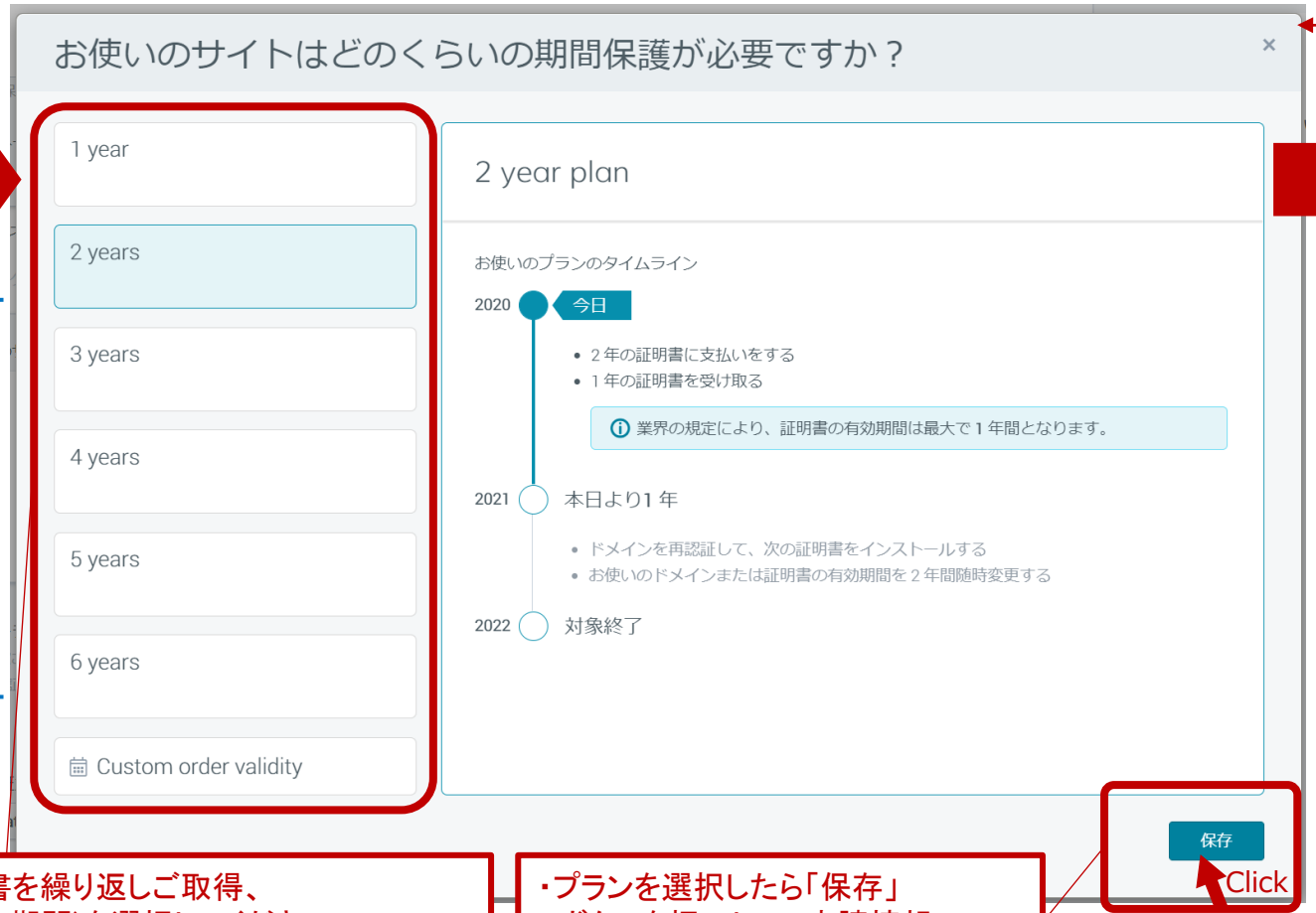
■【必須・自動設定あり】サーバライセンス
SSL/TLSセッションを利用する論理的なSSLサービスコンポーネントが複数ある場合はそのライセンス数を入力してください(デフォルトは1)

※ 1 : SANsについてもっと詳しく:FAQ「(OV/EV証明書用)Subject Alternative Names（サブジェクトの別名）」について」https://knowledge.digicert.com/ja/jp/solution/SO27318.html
※ 2 : 通常は最大250のSANsを入力可能です。

補足 プラン(契約期間)の選択

例1：ユニットライセンスを都度ご購入いただいているお客様の場合

■「プラン(契約期間)」をご選択いただくイメージ（例：2年間有効な複数年プランをご選択いただいた場合）

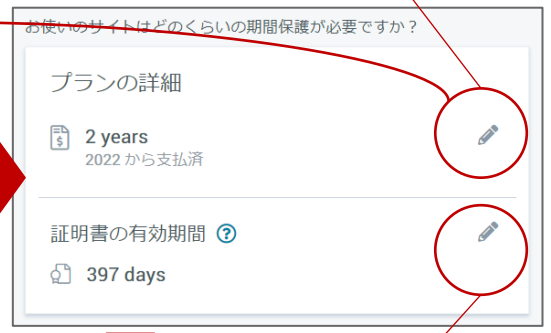


最大6年間まで
選択可能

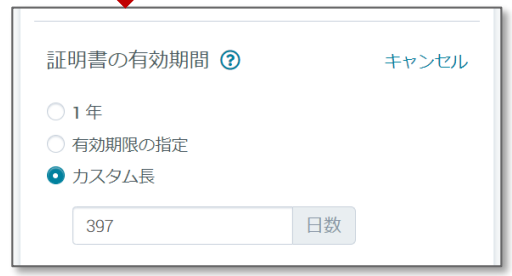
・枠内の選択肢から、プラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択してください。
例:「2 years」=2年間プラン

・プランを選択したら「保存」ボタンを押下して、申請情報入力画面に戻ります

このアイコンをクリックすると
プラン選択ウィンドウが再度
開きます



このアイコンをクリックすると
[証明書の有効期間]を編集
いただくことが可能です。



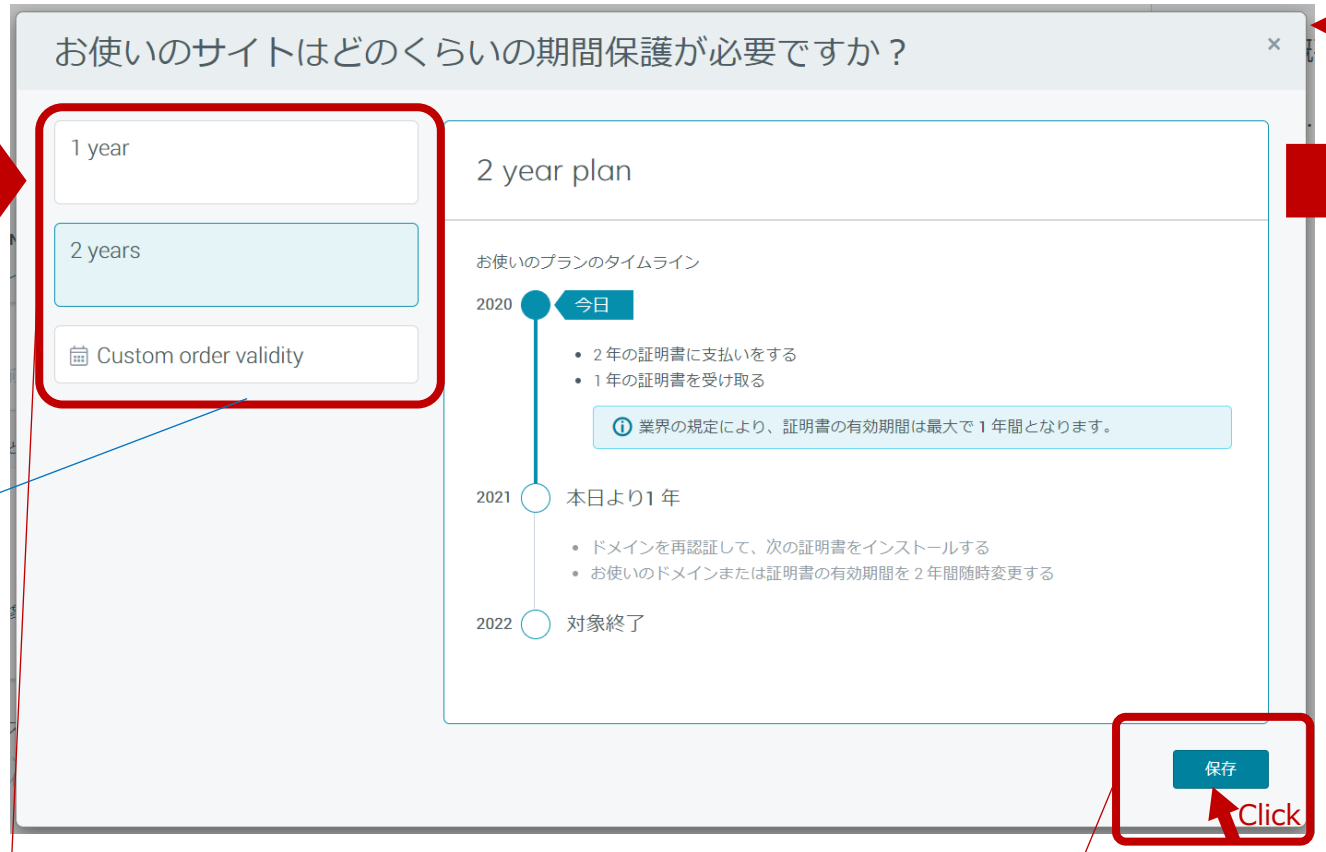
指定によって実際に発行される証明書の有効期間の設定のされ方の詳細については
FAQ(※1)を参照ください

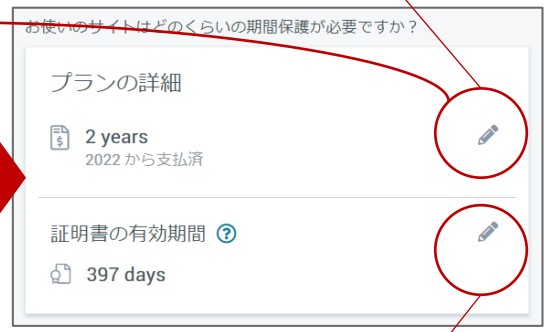
※1：FAQ「サーバ証明書の有効期間について」：https://knowledge.digicert.com/ja/jp/solution/SO22917.html

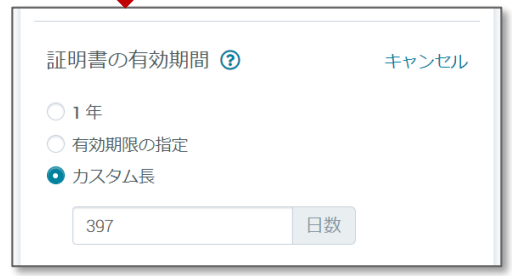
補足 プラン(契約期間)の選択

例2：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

■「プラン(契約期間)」をご選択いただくイメージ（例：2年間有効な複数年プランをご選択いただいた場合）







最大2年間まで選択可能

・枠内の選択肢から、プラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択してください。
例:「2 years」=2年間プラン

・プランを選択したら「保存」ボタンを押下して、申請情報入力画面に戻ります

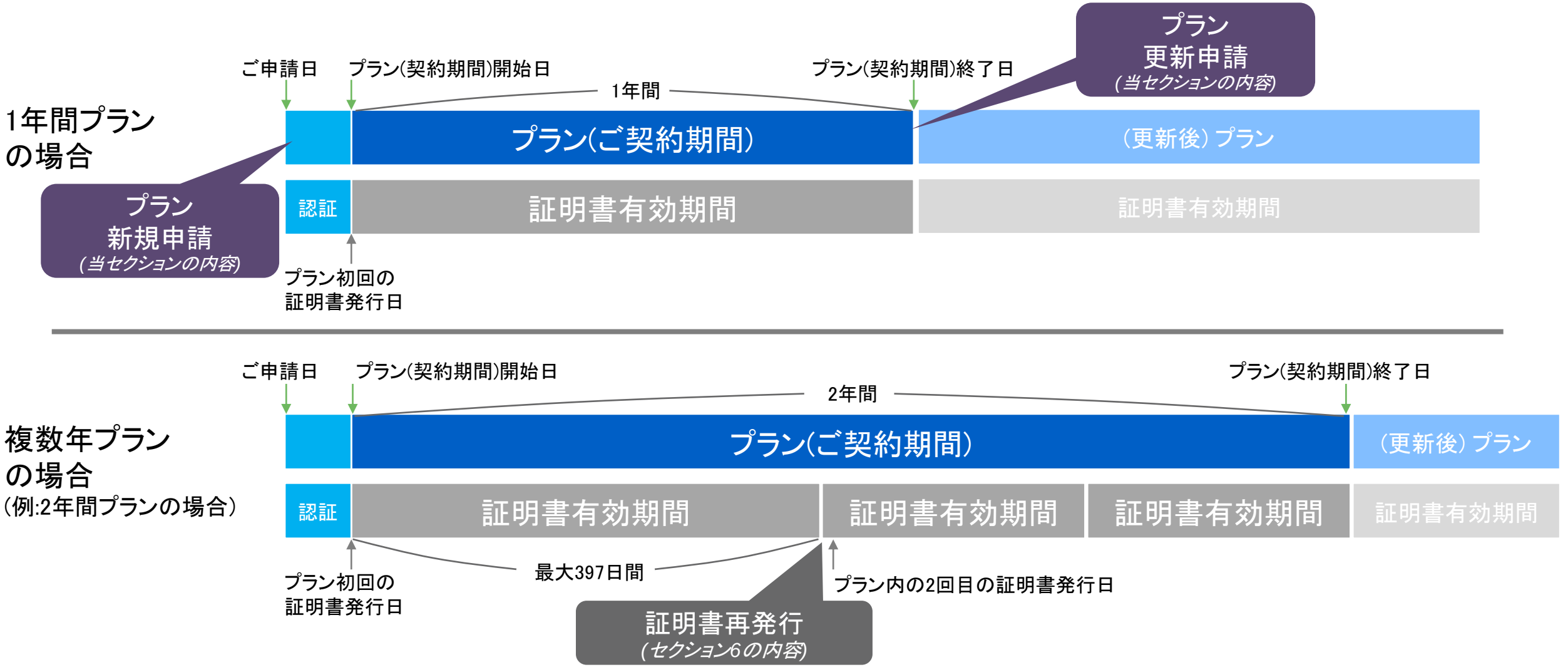
このアイコンをクリックするとプラン選択ウィンドウが再度開きます

このアイコンをクリックすると[証明書の有効期間]を編集いただくことが可能です。

指定によって実際に発行される証明書の有効期間の設定のされ方の詳細については FAQ(※1)を参照ください

※1：FAQ「サーバ証明書の有効期間について」：https://knowledge.digicert.com/ja/jp/solution/SO22917.html

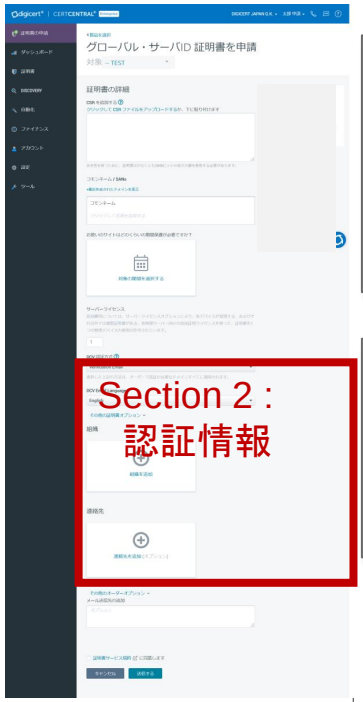
補足 CertCentral Enterprise「複数年プラン」オプション機能のご利用イメージ



新規申請 Section 2 (OVの場合) : 認証情報の入力

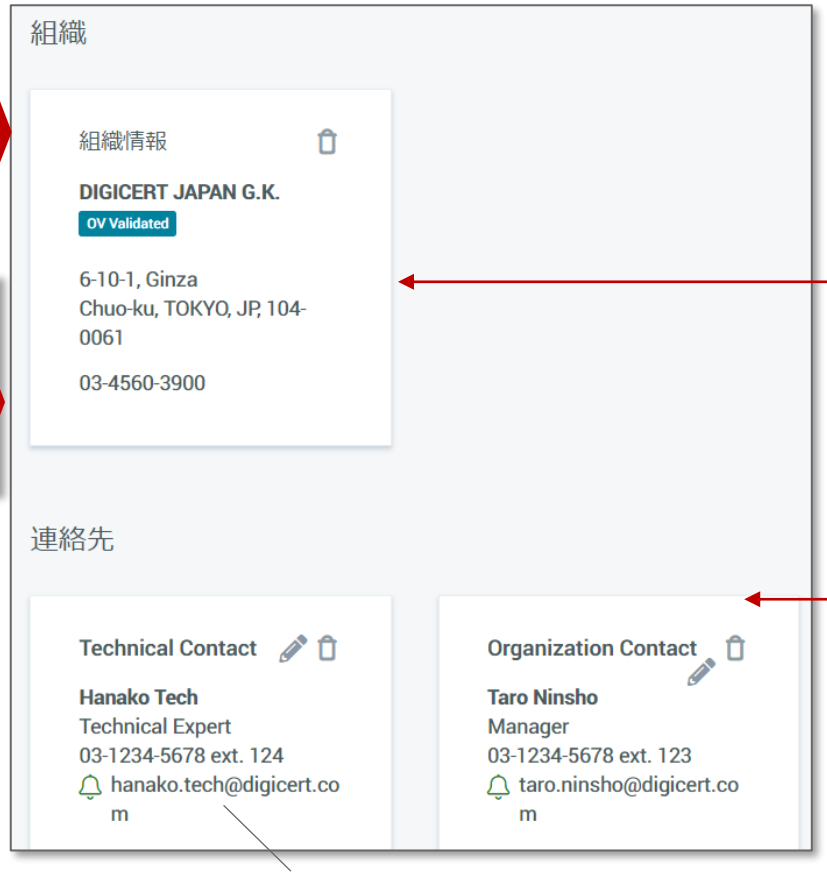
■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■組織・担当者情報欄:(自動)入力前の状態

■(自動)入力後の状態



■【必須・自動設定あり】組織情報
・証明書に記載する組織の情報を入力します。
・事前登録・認証済の組織名がCSRから抽出した組織名(Subject O)と一致した場合は、組織の所在地等の情報を事前登録・認証済の情報から自動設定します。
・「組織を追加」リンクをクリックして表示される選択肢から事前登録・認証済の組織を選択することも可能です。

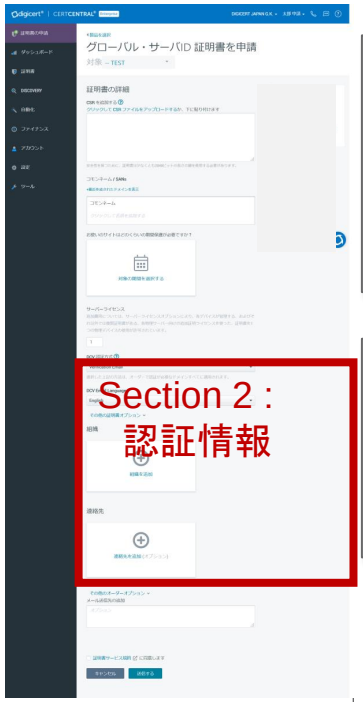
■【任意・自動設定あり】担当者(Contacts)情報
・証明書の申請に関する「技術担当者」「申請責任者」を設定することができます。
※ 各担当者の役割についてはセクション「2.1 ワークフロー」「デジサートによる「組織」の事前認証 概要」を参照ください

・上部の「組織情報」欄に登録・認証済の組織情報が選択・設定された場合、該当の組織情報に紐づいてCertCentralが保持する担当者情報がオーダーの担当者として自動設定されます。

新規申請 Section 2 (EVの場合) : 認証情報の入力

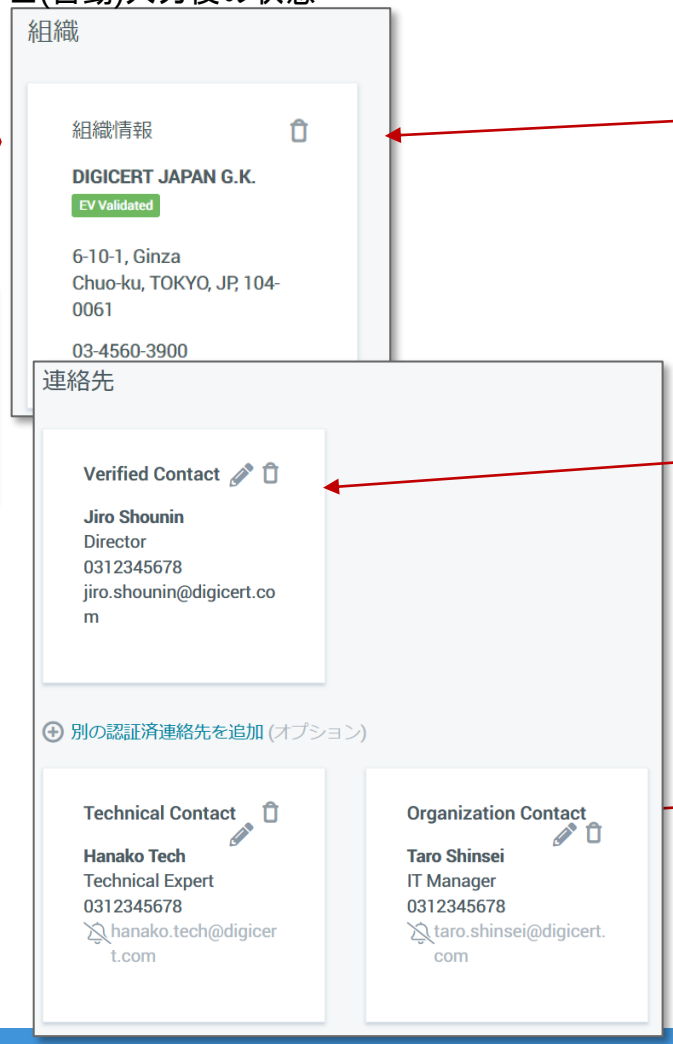
■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■組織・担当者情報欄:(自動)入力前の状態

■(自動)入力後の状態



■【必須・自動設定あり】組織情報
・証明書に記載する組織の情報を入力します。
・事前登録・認証済の組織名がCSRから抽出した組織名(Subject O)と一致した場合は、組織の所在地等の情報を事前登録・認証済の情報から自動設定します。
・「組織を追加」リンクをクリックして表示される選択肢から事前登録・認証済の組織を選択することも可能です。

■【必須・自動設定あり】「認証済連絡先(Verified Contact)」
・EV SSLの承認権限を持つ「認証済連絡先」を指定します。
・当ガイドセクション2.2~2.3に沿って該当の組織情報に対して「認証済連絡先(EV)」の登録・認証が完了し有効化されている場合、自動設定されます。

■【任意・自動設定あり】担当者(Contacts)情報
・証明書の申請に関する「技術担当者」「申請責任者」を設定することができます。
※ 各担当者の役割についてはセクション「2.1 ワークフロー」「デジサートによる「組織」の事前認証 概要」を参照ください

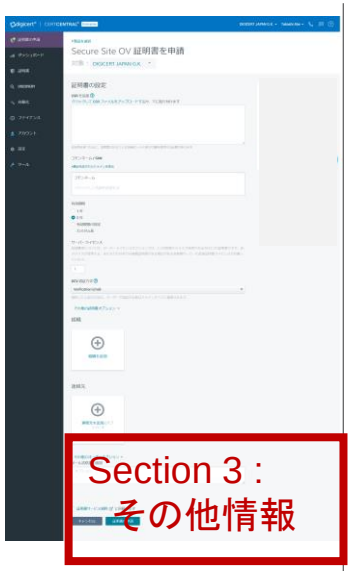
・上部の「組織情報」欄に登録・認証済の組織情報が選択・設定された場合、該当の組織情報に紐づいてCertCentralが保持する担当者情報がオーダーの担当者として自動設定されます。

EV SSL証明書の申請・発行承認についてもっと詳しく : https://knowledge.digicert.com/ja/jp/solution/SO23322.html

新規申請 Section 3 (OV/EV共通) : その他のオーダー情報入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■その他の情報 入力欄

■規約同意、証明書の申請

■【任意】その他のオーダーオプション
以下の詳細設定が可能です。

・「管理者への連絡事項」: 管理者(証明書リクエストの承認者)に対するメッセージを設定できます。

・「オーダーの更新メッセージ」: 有効期間満了前の更新案内に含めるメッセージを設定できます。

・「メール送信先の追加」: 申請者に加えて、申請関連のメールや更新案内メールの送信先を追加することができます。

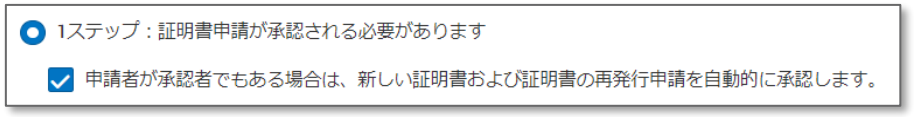
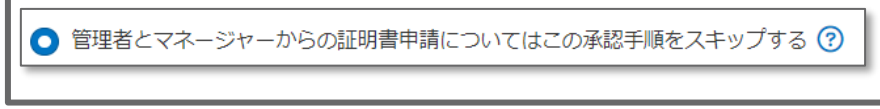
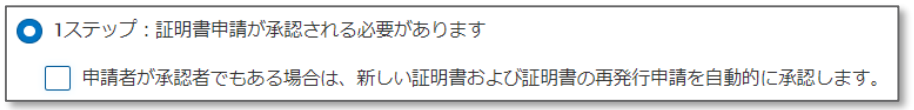
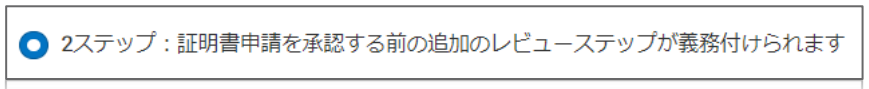
■【必須】証明書サービス規約
リンク先の規約をご確認いただき、チェックボックス=ONにしてください。

以上で申請は終わりです。「証明書の申請」を押下して申請を完了させてください。

(任意)アカウント内での申請レビュー・承認について (1/2 設定)

証明書の申請	・製品を選択 ・プランのお申込み(証明書を申請)
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■「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： 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)		**条件付き自動承認** (承認権限（管理者またはマネージャ）があるユーザーによるレビューをスキップし、デジサートによる申請内容の確認、証明書発行に進みます)	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)
条件付き自動承認			
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

(任意)アカウント内での申請レビュー・承認について (2/2 通知・承認)

証明書の申請	・製品を選択 ・プランのお申込み(証明書を申請)
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■「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]

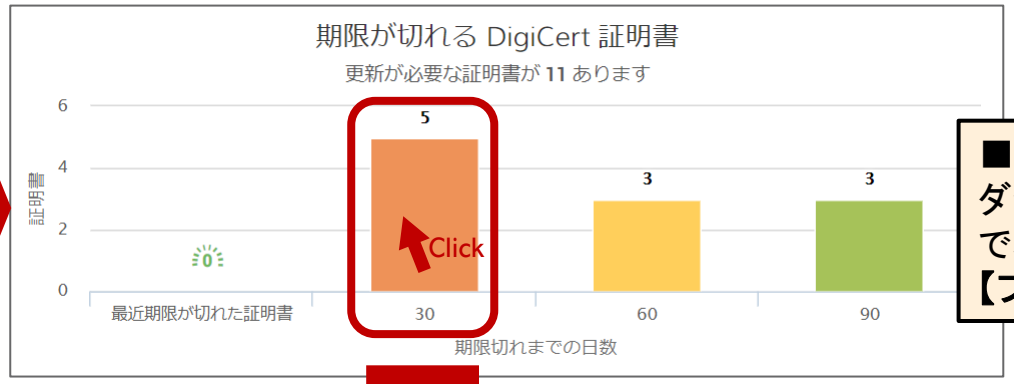
Click

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)

更新申請(OV/EV共通) STEP 1：更新対象を特定

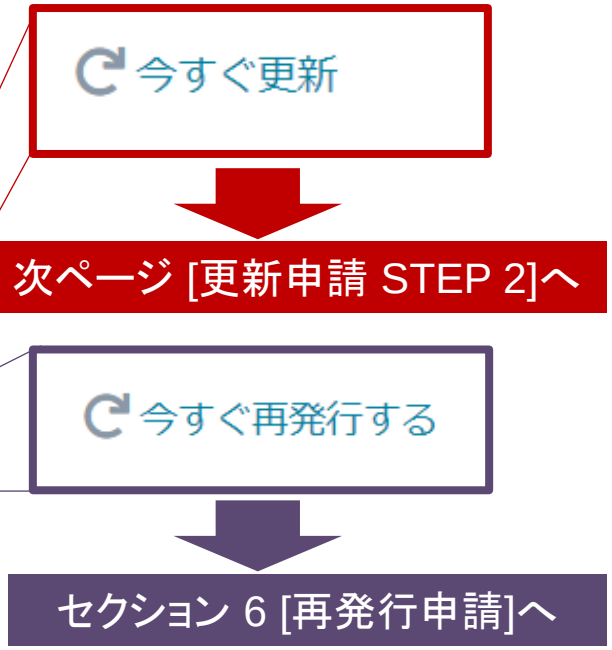
証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
申請レビュー・承認	（アカウント単位の設定で省略可） ・管理者が申請内容を確認し、承認または却下
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得（ダウンロード）
証明書管理	・証明書再発行（証明書の更新） ・証明書の失効

■ダッシュボード内の「期限が切れるDigiCert証明書」から



■ポイント1：
ダッシュボードおよび「期限切れになる証明書」メニューで表示される対象には、間もなく有効期限を迎える**【プラン】と【証明書】の両方を含みます**

■「証明書」→「期限切れになる証明書」から

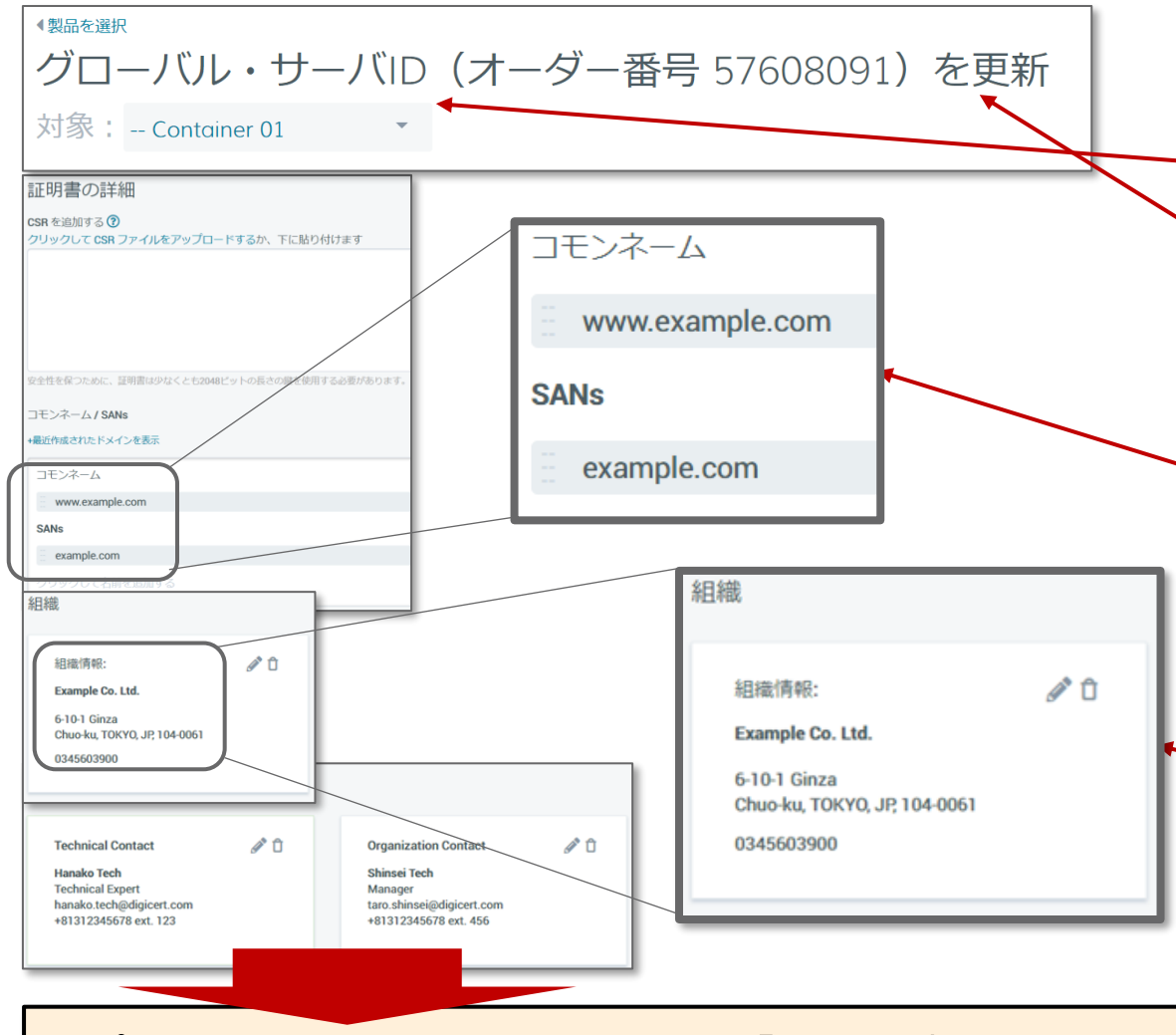


■ポイント2：
「期限切れになる証明書」メニューでは以下の要領でアクション(一覧の右端のリンク文言)が変化します。
・【プラン】が有効期限を迎える場合：**「今すぐ更新」　→　プラン(契約期間)を更新してください**
・【証明書】が有効期限を迎える場合：**「今すぐ再発行する」　→　証明書を再発行してください**

更新申請(OV/EV共通) STEP 2：プラン更新申請情報の入力

証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■前ページ「**今すぐ更新**」等から更新申請を開始した場合の表示例



■**ポイント1**：更新元証明書と同一の製品が選択された状態
（更新申請時の製品変更は**不可**）

■**ポイント2**：更新元証明書のオーダー番号が表示された状態

■**ポイント3**：更新元証明書と同一のFQDNが設定された状態
（更新申請時のコモンネーム(FQDN)変更は**可能**）
・この状態でCSRを入力した場合、CSR内のSubject CN(コモンネーム)が画面上に設定されたコモンネームと異なる場合は、**画面上の当欄に設定された値が優先して申請に利用されます**のでご注意ください。

■**ポイント4**：更新元証明書と同一の組織情報が設定された状態
（更新申請時の組織情報の変更は**可能**）
・この状態でCSRを入力した場合、CSR内のSubject O(組織名)が画面上に設定された組織情報と異なる場合は、**画面上の当欄に設定された値が優先して申請に利用されます**のでご注意ください。

■**ポイント5**：上記以外の入力項目等は「新規申請」時と同一です。必要な情報を入力・選択いただき申請を完了させてください。

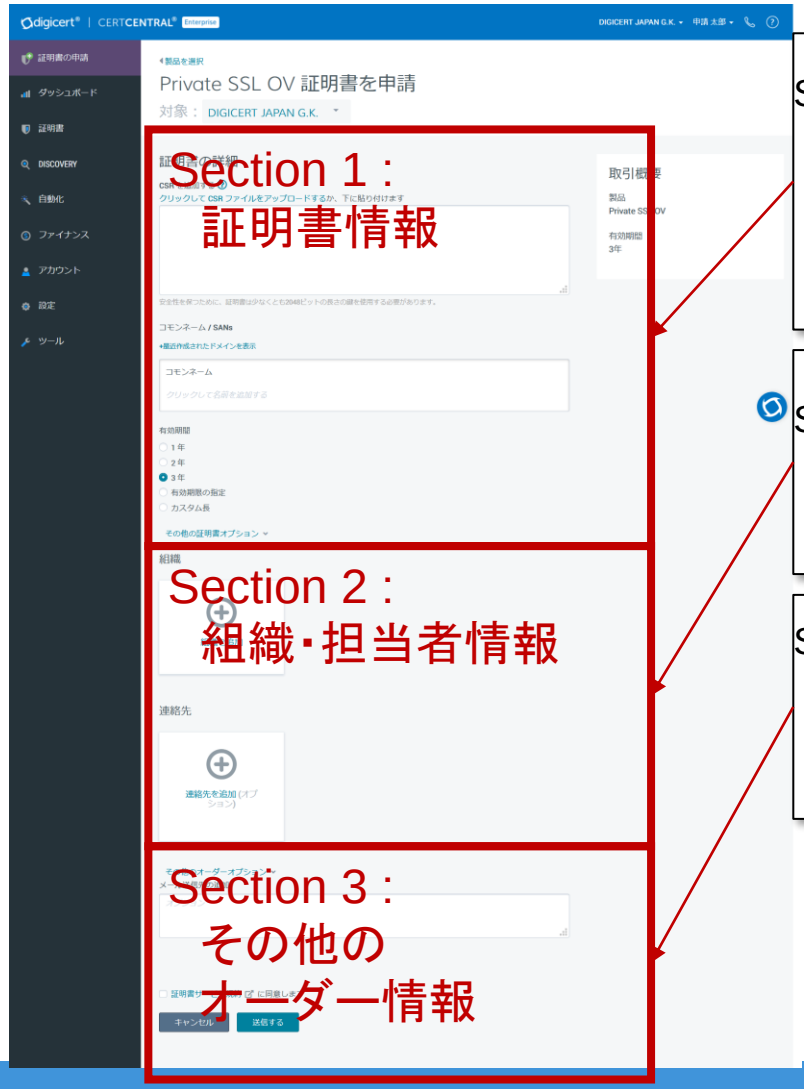
3. 証明書の申請

~ 3.2 プライベートSSL証明書の申請 ~

プライベートSSL証明書の申請 – 申請画面概要

■メニュー内 製品選択

■プライベートSSL申請画面



Section 1 :「証明書情報」を入力します
- CSR
- コモンネーム
- 証明書有効期間
- (任意)階層構造オプション

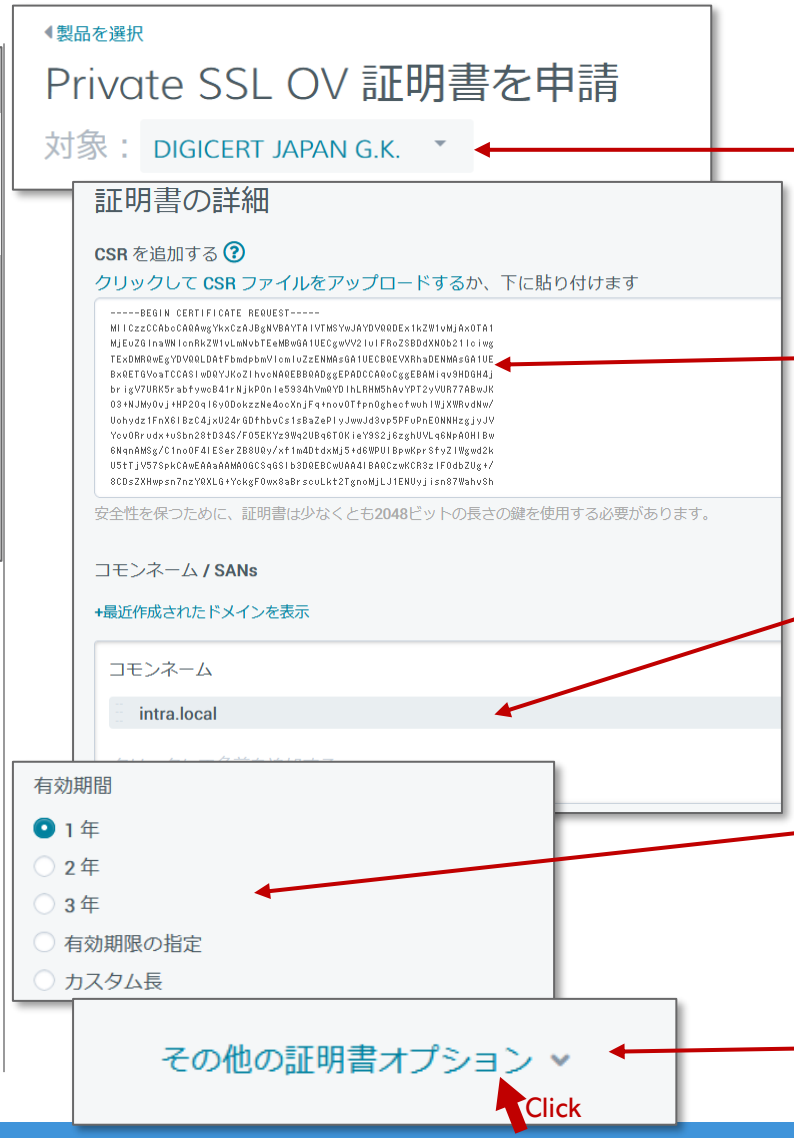
Section 2 : 次に組織・担当者情報を入力します
- 申請団体の組織情報
- 連絡先担当者

Section 3 : 最後にその他の情報を入力、
利用規約を確認いただきます
- その他のオーダーオプション
- 証明書サービス利用規約の確認

プライベートSSLの証明書申請 Section 1 証明書情報入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■【任意】管理グループ(Division)の選択
・デフォルトの管理グループが選択された状態
・特定の(追加)管理グループに紐づけた証明書申請を行う場合にのみ、クリックして表示される一覧から選択してください。
(管理グループについての詳細はセクション 9.3を参照)

■【必須】CSRの設定
・「クリックしてCSRファイルをアップロードする」をクリックしてCSR(テキストファイル形式)をアップロードしていただく、または入力欄にクリップボードからCSRを貼り付けてください。

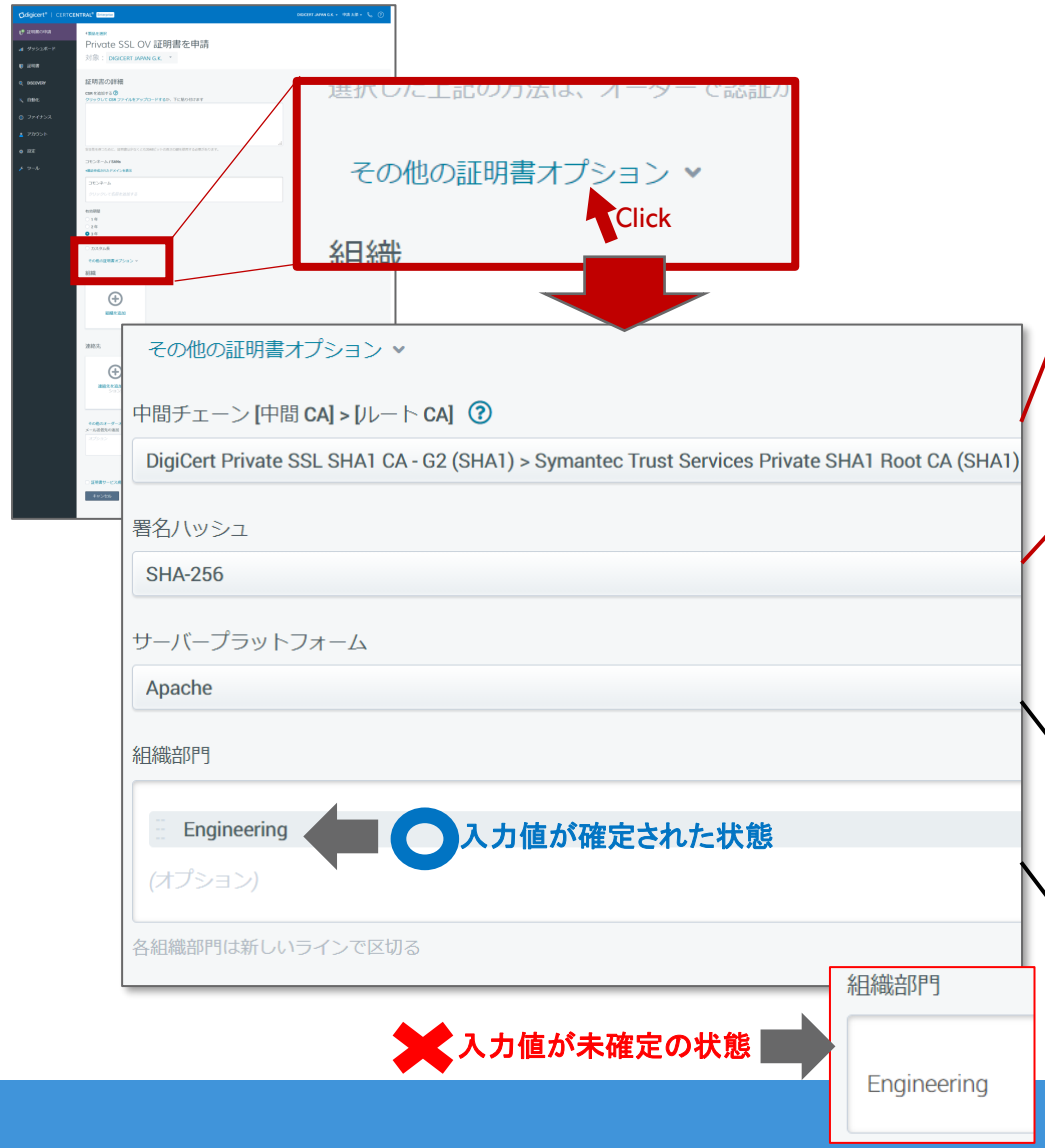
■【必須・自動設定あり】コモンネーム / SAN
・初期状態からCSRを貼り付けた場合、CSRの内容から抽出したコモンネーム(Subject CN)を自動設定します。
・任意の値に上書き可能です。CSRの内容と異なる値を入力した場合、当欄に設定した値が優先して申請に利用されます。

■【必須】有効期間:
以下の選択肢から、証明書の有効期間を選択・設定してください。
・1 年:1年間有効な証明書
・2 年:2年間有効な証明書
・3 年:3年間有効な証明書
・有効期限の設定:有効期間終了日を直接指定(カレンダー方式で指定可)
・カスタム長:有効期間を日数で直接指定(数値で指定可)

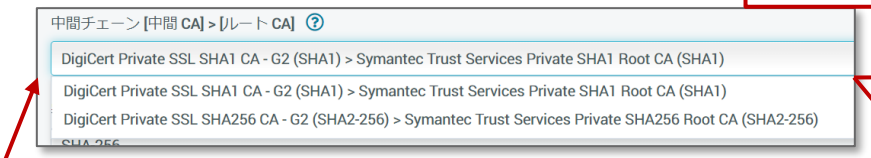
■その他の証明書オプション
※必ずクリックして階層構造オプションや署名アルゴリズムを確認してください
→詳細は次のページを参照ください

補足：プライベートSSLの「その他の証明書オプション」指定について

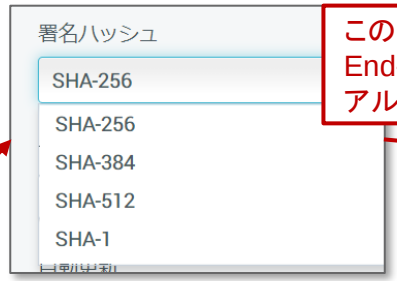
■「申請情報入力画面」



■プライベートSSLの階層オプション
(中間認証局およびルート証明書)選択欄 (※1,2)

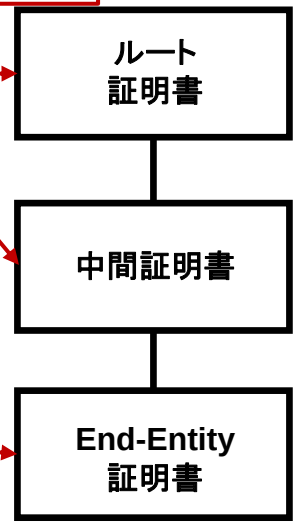


■プライベートSSLの署名ハッシュ
(End-Entityへのデジタル署名の署名アルゴリズム)選択欄 (※2)



このプルダウンで
ルートCA+中間CAを決定

このプルダウンで
End-Entityへの署名
アルゴリズムを決定



※1：お客様とのご契約内容等により選択いただける階層オプションは異なります。プライベートSSL【レガシータイプ】の階層構造は、セクション「5.2 中間証明書・証明書階層構造について」を参照ください
※2：アカウント内メニュー「設定」→「製品設定」から、申請画面に表示する階層オプションおよびデフォルト値、署名ハッシュの設定をカスタマイズ可能です

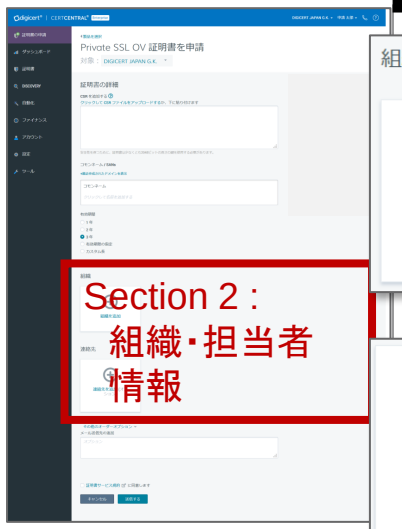
■サーバープラットフォーム：
当欄の選択肢、これによって決定されるファイル形式はパブリックのSSL/TLSサーバ証明書製品と同等となります。詳細はセクション「5.1 発行された証明書の取得」を参照ください

■組織部門(OU)：
証明書のSubject OU(OrganizationalUnitName)に設定する値を指定することができます。
【注意】文字列を入力後、リターンキーを押下して左図のイメージのように入力が確定した状態としてください
(白背景のままの場合(左の赤枠の図)、入力が確定していません)

プライベートSSLの証明書申請 Section 2 組織・担当者情報の入力

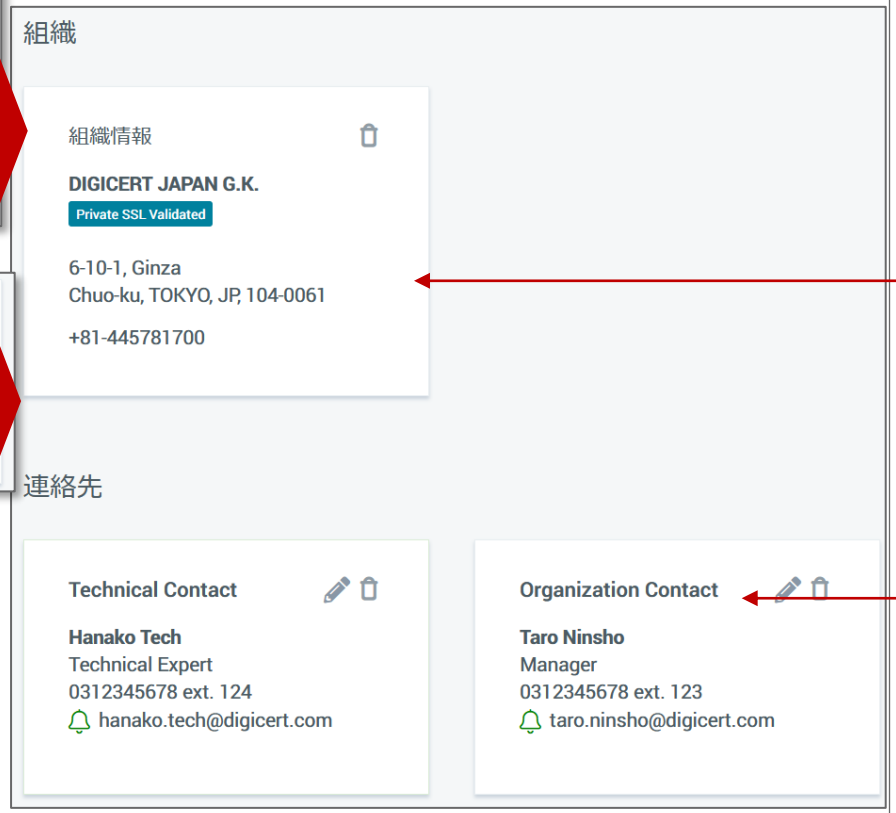
■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■組織・担当者情報欄:(自動)入力前の状態

■(自動)入力後の状態



■【必須・自動設定あり】組織情報
・証明書に記載する組織の情報を入力します。
・事前登録・確認済の組織名がCSRから抽出した組織名(Subject O)と一致した場合は、組織の所在地等の情報を事前登録・確認済の情報から自動設定します。
・「組織を追加」リンクをクリックして表示される選択肢から事前登録・確認済の組織を選択することも可能です。

■【必須・自動設定あり】担当者(Contacts)情報
・証明書の申請に関する「技術担当者」「申請責任者」を設定することができます。
※ 各担当者の役割についてはセクション「2.1 ワークフロー」「デジサートによる「組織」の事前認証 概要」を参照ください

・事前登録済の組織名がCSRから抽出した組織名(Subject O)と一致した場合は、組織の担当者として登録した担当者情報が自動設定されます。

プライベートSSLの証明書申請 Section 3 その他のオーダー情報の入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」

Section 3 :
その他の
オーダー情報

■その他の情報 入力欄

その他のオーダーオプション
メール送信先の追加
オプション
Click

管理者への連絡事項
オプション
(証明書には含まれません)
オーダー特定の更新メッセージ
オプション
メール送信先の追加
オプション

■規約同意、証明書の申請

証明書サービス規約 に同意します
Click
キャンセル
証明書の申請
Click

■【任意】その他のオーダーオプション
以下の詳細設定が可能です。

・「管理者への連絡事項」:管理者(証明書リクエストの承認者)に対するメッセージを設定できます。

・「オーダーの更新メッセージ」:有効期間満了前の更新案内に含めるメッセージを設定できます。

・「メール送信先の追加」:申請者に加えて、申請関連のメールや更新案内メールの送信先を追加することができます。

■【必須】証明書サービス規約
リンク先の規約をご確認いただき、チェックボックス=ONにしてください。

以上で申請は終わりです。「証明書の申請」を押下して申請を完了させてください。

3. 証明書の申請

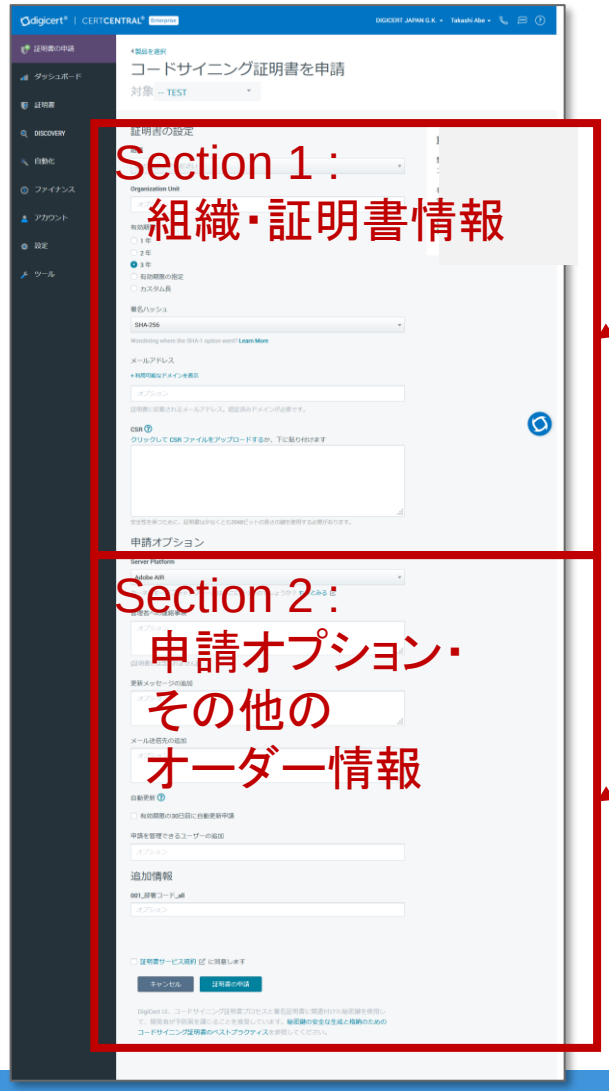
~ 3.3 コードサイニング証明書の申請 ~

コードサイニング証明書の申請 – 申請画面概要

■メニュー内 製品選択

「コードサイニング証明書」を
クリックして、申請を開始

■コードサイニング証明書申請画面



Section 1 :「組織・証明書情報」を入力します
- 組織情報（プルダウンから選択）
- 証明書有効期間
- CSR

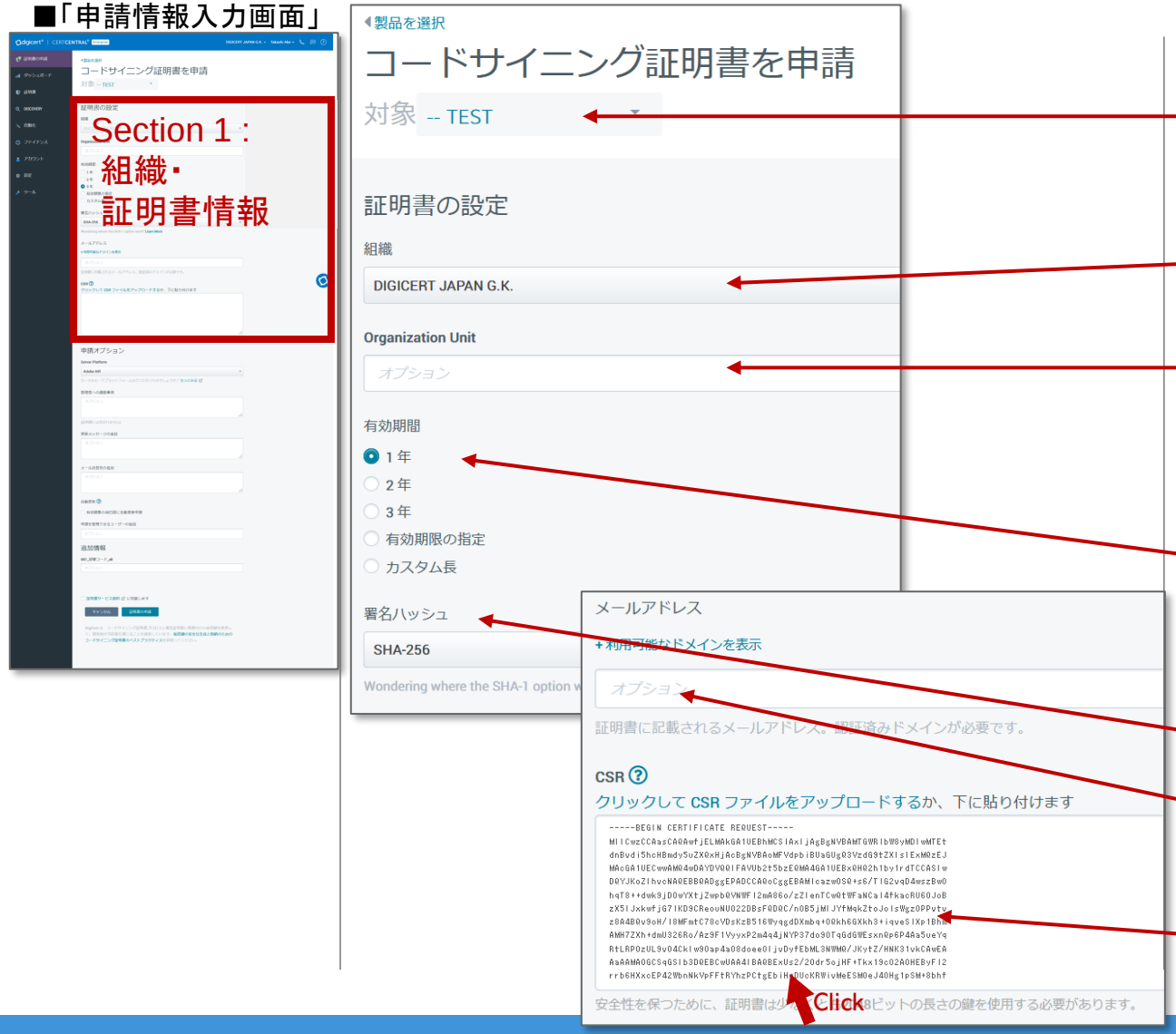
Section 2 : 次に申請オプション情報ならびに
その他のオーダー情報を入力いただき、
利用規約を確認いただきます
- Server Platform(署名対象アプリケーション)
- (任意)メール送信先の追加
- 証明書サービス利用規約

※ : コードサイニング証明書の申請についてもっと詳しく https://docs.digicert.com/ja/manage-certificates/code-signing-certificate/order-code-signing-certificate/

コードサイニング証明書の申請 – Section 1 組織・証明書情報入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■「申請情報入力画面」



■【任意】管理グループ(Division)の選択
・デフォルトの管理グループが選択された状態
・特定の(追加)管理グループに紐づけた証明書申請を行う場合にのみ、
クリックして表示される一覧から選択してください。
(管理グループについての詳細はセクション 9.3を参照)

■【必須】組織の選択
・証明書発行対象の組織(Subject O)をプルダウンから選択してください。

■【任意】Organization Unit:
・部門名等、必要に応じてご記入ください。
入力した内容は認証の対象となり、証明書に反映されます。

■【必須】有効期間:
以下の選択肢から、証明書の有効期間を選択・設定してください。
・1 年:1年間有効な証明書
・2 年:2年間有効な証明書
・3 年:3年間有効な証明書
・有効期限の設定:有効期間終了日を直接指定(カレンダー方式で指定可)
・カスタム長:有効期間を日数で直接指定(数値で指定可)

■【必須・自動入力あり】署名ハッシュ:
(初期状態)「SHA-256」を設定します

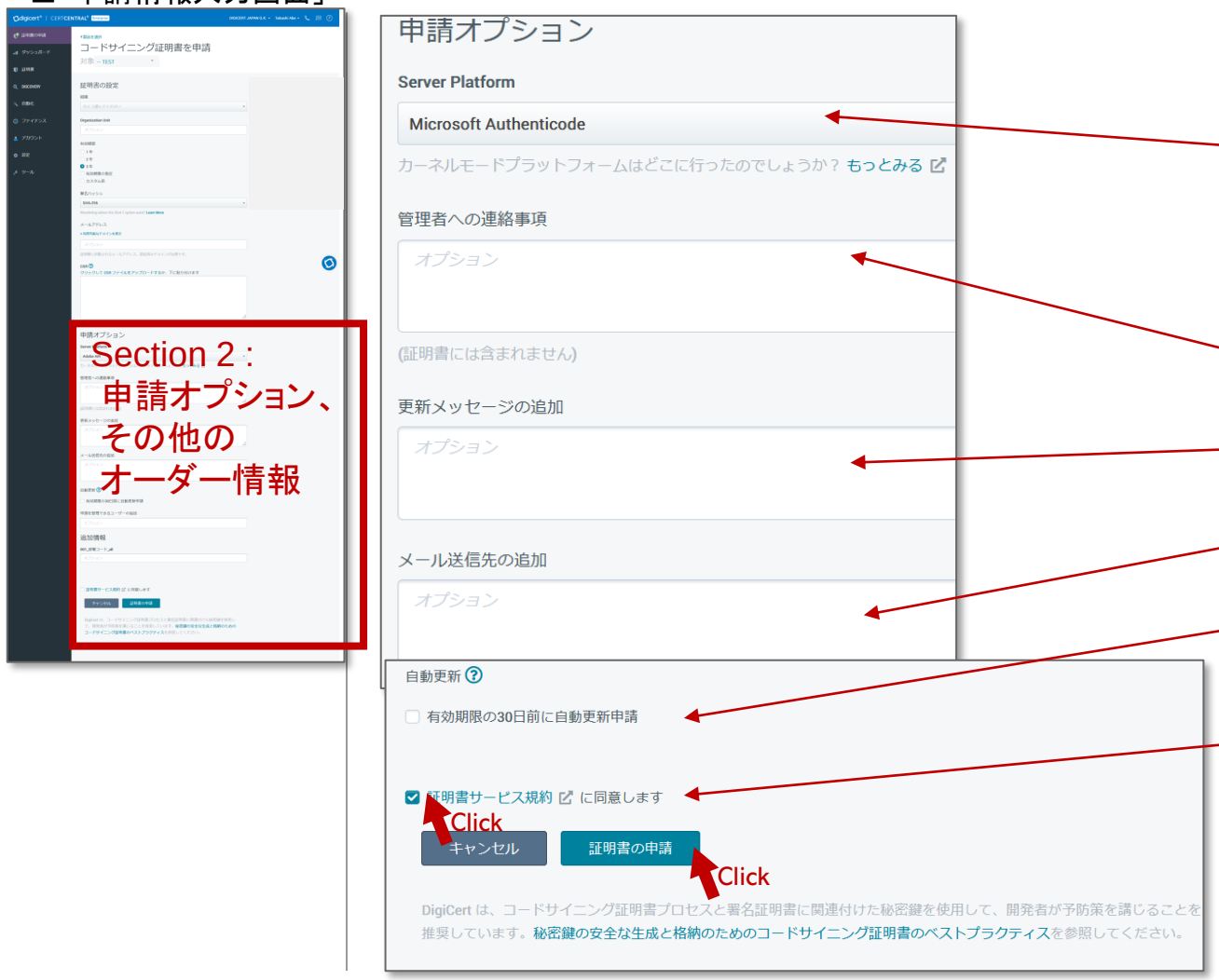
■【使用しません】メールアドレス

■【必須または任意】CSR
・Server Platform =「Sun Java」で申請する場合:**必須**
「クリックしてCSRファイルをアップロードする」をクリックしてCSR(テキストファイル形式)をアップロード、または入力欄にクリップボードからCSRを貼り付けてください。
・Server Platform =「Sun Java」以外で申請する場合:任意

コードサイニング証明書の申請 –
Section 2 申請オプション、その他のオーダー情報

■凡例
- ・・・必須(入力または選択)
- ・・・自動設定可または任意

■「申請情報入力画面」



■【必須】Server Platform(署名対象アプリケーションの種類)
・コードサイニング証明書を利用する署名対象アプリケーションの種類を選択します
（以下、抜粋）
- Adobe Air
- Microsoft Authenticode
- Microsoft Office VBA
- Sun Java
- Other (上記以外の場合)

■【任意】「管理者への連絡事項」:
管理者（証明書リクエストの承認者）に対するメッセージを設定できます

■【任意】「更新メッセージ追加」:
有効期間満了前の更新案内に含めるメッセージを設定可能です

■【任意】「メール送信先の追加」:
申請者に加えて、申請関連のメールや更新案内メールの送信先を追加できます

■【使用しません】「自動更新」

■【必須】証明書サービス規約
リンク先の規約をご確認いただき、チェックボックス=ONにしてください。

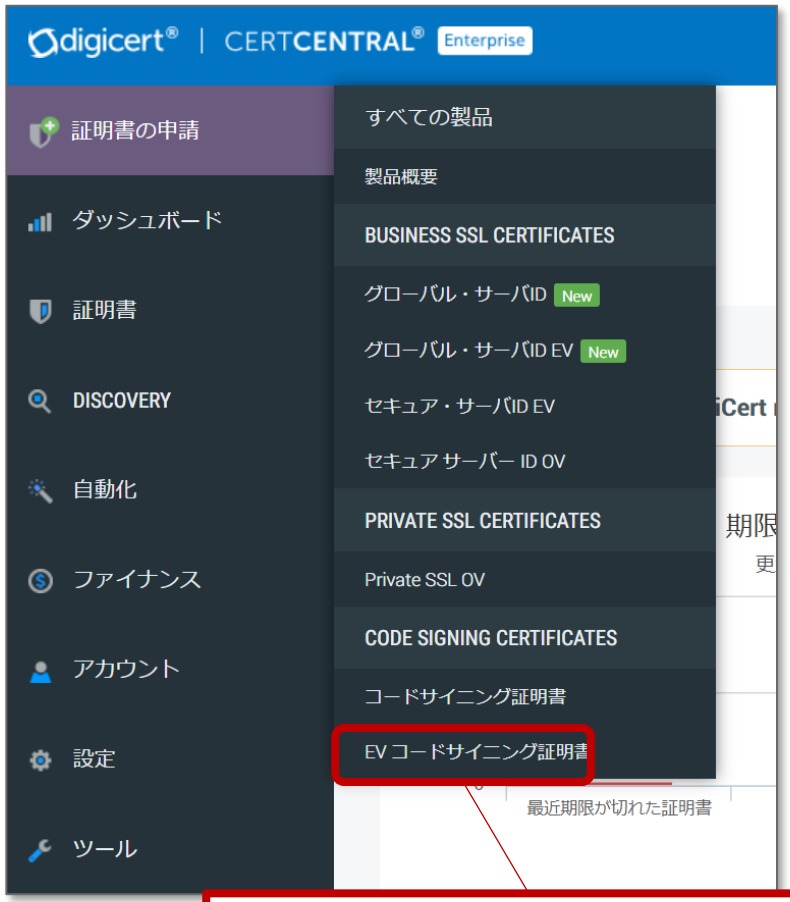
以上で申請は終わりです。
「証明書の申請」を押下して申請を完了させてください。

3. 証明書の申請

~ 3.4 EVコードサイニング証明書の申請 ~

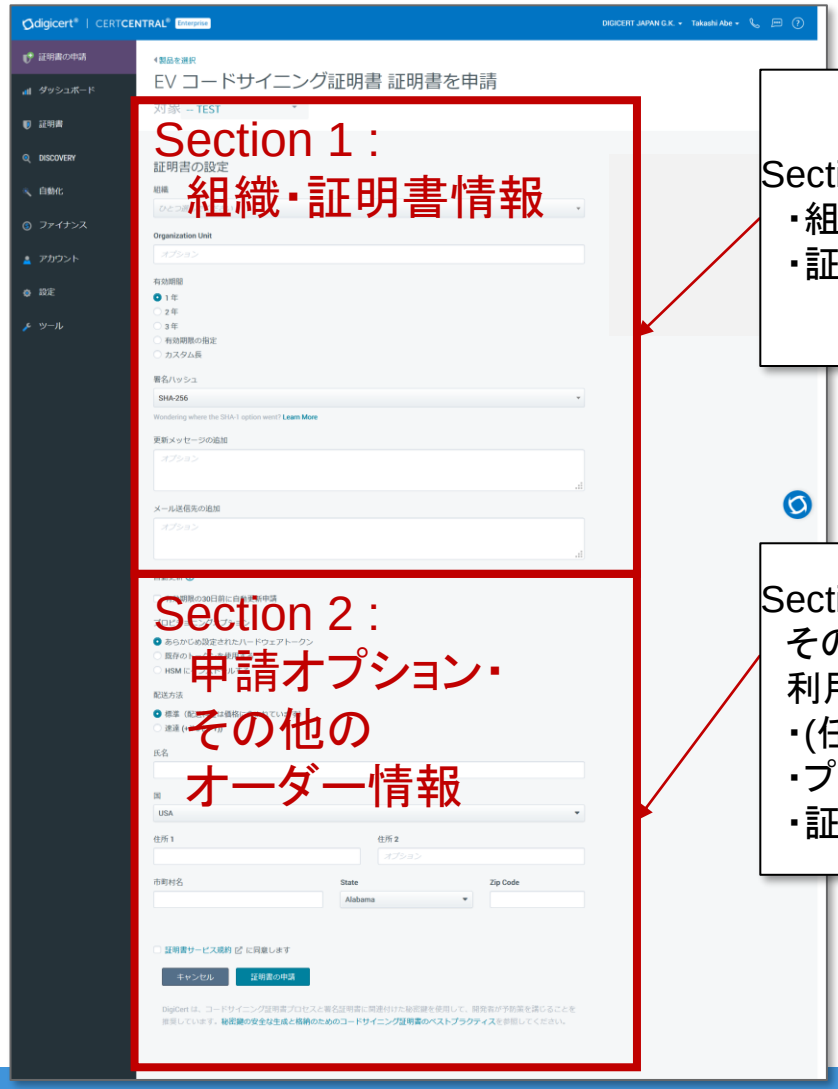
EVコードサイニング証明書の申請 – 申請画面概要

■メニュー内 製品選択



「EVコードサイニング証明書」を
クリックして、申請を開始

■EVコードサイニング証明書申請画面



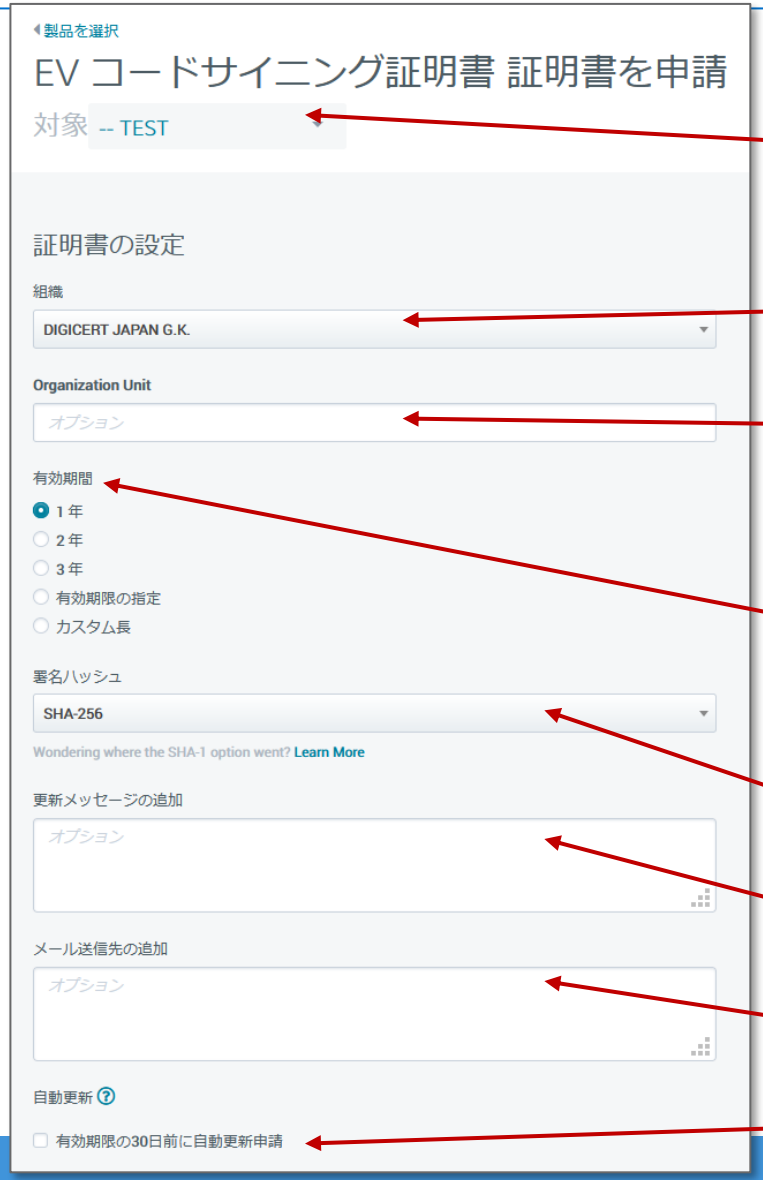
Section 1 :「組織・証明書情報」を入力します
・組織情報（プルダウンから選択）
・証明書有効期間

Section 2 : 次に申請オプション情報ならびに
その他のオーダー情報を入力いただき、
利用規約を確認いただきます
・(任意)メール送信先の追加
・プロビジョニングオプション/配送方法
・証明書サービス利用規約

EVコードサイニング証明書の申請 – Section 1 組織・証明書情報入力

■凡例
- ・・・必須(入力または選択)
- ・・・自動設定可または任意

■「申請情報入力画面」



■【任意】管理グループ(Division)の選択
・デフォルトの管理グループが選択された状態
・特定の(追加)管理グループに紐づけた証明書申請を行う場合にのみ、
クリックして表示される一覧から選択してください。
(管理グループについての詳細はセクション 9.3を参照)

■【必須】組織の選択
・証明書発行対象の組織(Subject O)をプルダウンから選択してください。

■【任意】Organization Unit:
・部門名等、必要に応じてご記入ください。
入力した内容は認証の対象となり、証明書に反映されます。

■【必須】有効期間:
以下の選択肢から、証明書の有効期間を選択・設定してください。
・1 年:1年間有効な証明書
・2 年:2年間有効な証明書
・3 年:3年間有効な証明書
・有効期限の設定:有効期間終了日を直接指定(カレンダー方式で指定可)
・カスタム長:有効期間を日数で直接指定(数値で指定可)

■【必須・自動入力あり】署名ハッシュ:
(初期状態)「SHA-256」を設定します

■【任意】「更新メッセージ追加」:
有効期間満了前の更新案内に含めるメッセージを設定可能です

■【任意】「メール送信先の追加」:
申請者に加えて、申請関連のメールや更新案内メールの送信先を追加できます

■【使用しません】「自動更新」

EVコードサイニング証明書の申請・発行承認についてもっと詳しく : https://knowledge.digicert.com/ja/jp/solution/SO23322.html

EVコードサイニング証明書の申請 – Section 2 申請オプション、その他のオーダー情報

■凡例
- ・・・必須(入力または選択)
- ・・・自動設定可または任意

■「申請情報入力画面」

■【必須・自動設定あり】プロビジョニングオプション
EVコードサイニング証明書をハードウェアトークンに格納する際の証明書をインストールする際のオプションを選択します

証明書を新規に取得する場合など新しいトークンが必要な方は「あらかじめ設定されたハードウェアトークン」を選択してください。トークンの送付先が表示されますので、トークン送付先を指定してください(利用方法は下記注※1)。

証明書を更新する場合などすでにトークンをお持ちの方は「既存のトークンを使用する」、または利用者のHSMにインストールする場合は「HSMにインストールする」を選択し、対象となるプラットフォームを選択します。

■【必須】証明書サービス規約
リンク先の規約をご確認いただき、チェックボックス=ONにしてください。

以上で申請は終わりです。
「証明書の申請」を押下して申請を完了させてください。

※1：【EVコードサイニング証明書】ハードウェアトークンの使用方法についての詳細：https://knowledge.digicert.com/ja/jp/solution/SOT0004.html

4. オーダー・証明書の一覧管理およびレポート

「証明書」メニューの概要

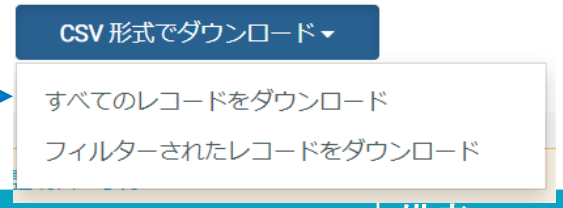
■「証明書」メニュー

メニュー名称	機能説明	備考
オーダー	・オーダー(証明書注文単位)の一覧表示、検索 ・オーダーレポートの出力 ・(一覧から)オーダー詳細確認・管理(再発行、失効等)	詳細後述
証明書申請の一覧	・「承認待ち」リクエストの一覧表示、検索 (証明書発行リクエスト、失効リクエストなど) ・(一覧から)リクエスト詳細確認・管理(承認／却下)	詳細後述
ドメイン	・アカウントに登録済みの**ドメイン名**の一覧表示、検索 ・(一覧から)ドメイン名の詳細表示(認証有効期間など) ・ドメイン名の管理(追加、認証申請、無効化/(再)有効化)	
組織	・アカウントに登録済み**組織**の一覧表示、検索 ・(一覧から)組織の詳細表示(認証有効期間など) ・組織の管理(追加、認証申請、無効化/(再)有効化)	
期限切れになる証明書	・更新対象(有効期限90日前～)証明書の一覧表示 ・(一覧から)更新申請	
認証局	・アカウントで発行可能な証明書用の中間証明書の一覧 ・中間証明書のダウンロード	

次ページ以降で詳細な活用方法をガイドします。

「証明書」→「オーダー」メニューの使い方 (1/2 オーダー一覧)

■「証明書」→「オーダー」メニューから表示するオーダー一覧



ボタン名称	機能説明	備考
証明書の申請	・製品の選択→新規申請を開始	新規申請画面は別項参照
オーダーレポート	・管理グループ(Division)別発行済証明書のレポート	管理グループについては別項参照
CSV形式でダウンロード	■「すべてのレコードをダウンロード」 アカウント内で発行された全てのオーダー情報を含むレポートをCSV形式でダウンロードします。 （「有効期限切れ(expired)」「失効済(revoked)」などを含む） ■「フィルターされたレコードをダウンロード」 画面上で指定されたフィルター条件を適用した状態で、該当するオーダー情報を含むレポートをCSV形式でダウンロードします。 *〇適用可能なフィルター条件の例：* *「証明書ステータス(有効期間内、失効済など)」、「製品種類」、「オーダーID」、「FQDN」、「オーダー申請日(From&To)」など*	

「証明書」→「オーダー」メニューの使い方 (1/2 オーダー一覧 続き)

■「証明書」→「オーダー」メニューから表示するオーダー一覧

■「高度な検索を表示する」をクリックして表示される検索条件一覧

検索項目名（抜粋）	検索条件
ステータス	オーダーのステータスによる絞り込み 「すべて」「発行済」「保留中」「失効」「期限切れ」 「30/60/90日以内に期限切れになる証明書」等を指定可能
検索	以下の検索キーによるオーダーの検索 ・オーダーID ・FQDN(証明書Subjectコモンネームおよび SANsの値を含む)
コモンネーム	証明書Subjectコモンネームによるオーダーの検索
メール	*＜(サーバ証明書では)使用不可＞*
オーダー日	オーダーを作成（申請）した日付範囲による絞り込み （一方のみを指定することも可能）

オーダーレポート(CSV形式)の詳細

■オーダーレポート(「証明書」→「オーダー」メニューから「CSV形式でダウンロード」ボタンを押下して生成するCSVレポート)の項目

位置 (*1)	フィールドのラベル	説明	出力例
1	id	オーダーID (数値,*2)	21382177
2	certificate.id	証明書ID (数値,*2)	22155792
3	certificate.common_name	証明書コモンネーム (FQDN)	test.example.com
4	certificate.dns_names	証明書SANsフィールド (コモンネームおよび追加SANsをカンマで連結)	test.example.com,add.example.jp
5	certificate.valid_from	証明書有効期間開始日 (yyyy-MM-dd形式)	2020-06-05
6	certificate.valid_till	証明書有効期間終了日 (yyyy-MM-dd形式)	2021-07-06
7	certificate.days_remaining	レポート生成時点での証明書有効期間残日数	365
8	certificate.signature_hash	証明書署名アルゴリズム	sha256
9	status	オーダーステータス	pending : 発行待ち(認証中) issued : 発行済/有効 expired : 有効期限切れ rejected : 発行前にキャンセル済 revoked : 発行後に失効済
10	is_renewed	オーダー更新済フラグ	1:更新済、空欄:更新済でない
11	date_created	オーダー作成日時 (ISO8601表記, UTC)	2020-06-05T07:54:55+00:00
12	organization.id	組織(Organization)ID (数値,*2)	583312

位置 (*1)	フィールドのラベル	説明	備考
13	organization.name	組織名称	DIGICERT JAPAN G.K.
14	validity_years	オーダー有効期間(年数)	1:1年間、2:2年間
15	order_valid_till	オーダー有効期間終了日 (yyyy-MM-dd形式)	2021-09-02
16	disable_renewal_notifications	更新案内通知配信有無	1:配信しない、空欄:配信する
17	container.id	管理グループのID (数値,*2)	310681
18	container.name	管理グループ名称	DIGICERT JAPAN G.K.
19	product.name_id	製品ID	ssl_securesite_pro
20	product.name	製品名(画面表記と同一)	Secure Site Pro SSL
21	product.type	製品カテゴリー	ssl_certificate:SSLサーバ証明書 code_signing_certificate: コードサイニング証明書
22	has_duplicates	「複製」された証明書の有無	1:有り、2:無し
23	price	使用済ユニット数 (最大値256)	1
24	product_name_id	No.18と同一	
25	alternative_order_id	(移行データのみ) マネージドPKI for SSLのオーダーID	1562795930
26	number_of_sans	証明書SANsフィールドに含むFQDN/ワイルドカードドメイン名の数 (最大値:256)	2
27	legacy_order_id	No.23と同一	1562795930
28	server_licenses	サーバーライセンス数 (最大値256)	1

*1 : CSV形式レポート内の各レポート項目の位置等は今後変更となる可能性があります。予めご理解・ご了承ください。

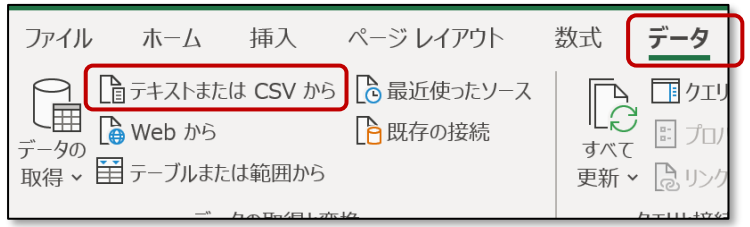
*2 : 数値(Integer)形式のフィールド(例:オーダーID等)は、本資料時点では8桁程度で推移しておりますが、今後最大(十進数で)10桁程度まで増加する可能性があります。
お客様にてCSVデータのシステム取込みをご検討いただく際のデータ設計においては、上記をご勘案いただき余裕をもった実装をご検討ください。

TIPS : オーダーレポート(CSV形式)が文字化けしてしまう

Q	CertCentralのオーダーレポートを開くと日本語(マルチバイト文字)データの文字化けが発生します。回避する方法はありますか？
A	CertCentralのオーダーレポートはUTF-8形式、拡張子=.csvですが、Microsoft Excelでそのまま開くと日本語データの文字化けが発生します。 文字化けを回避して正しいデータを確認するには以下いずれかの方法をお試しください(Windowsの場合)

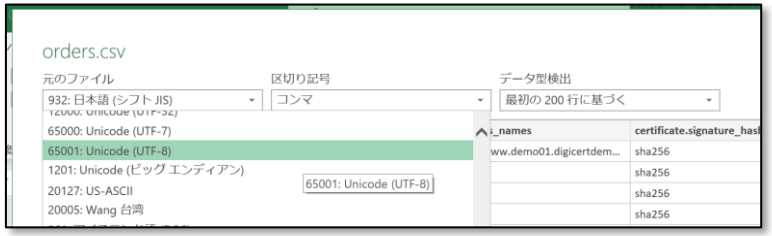
■方法1 : UTF-8形式でCSVファイルを「インポート」する

手順1 : Microsoft Excelを起動し、「データ」メニュー配下の[(テキストまたはCSVから)データの取得]を起動する



手順2 : ダウンロードしたオーダーレポート(CSV形式)を指定して「インポート」する

手順3 : 下図ウィザードの左上部「元のファイル」プルダウンを「日本語 (シフトJIS)」から「Unicode (UTF-8)」に変更する

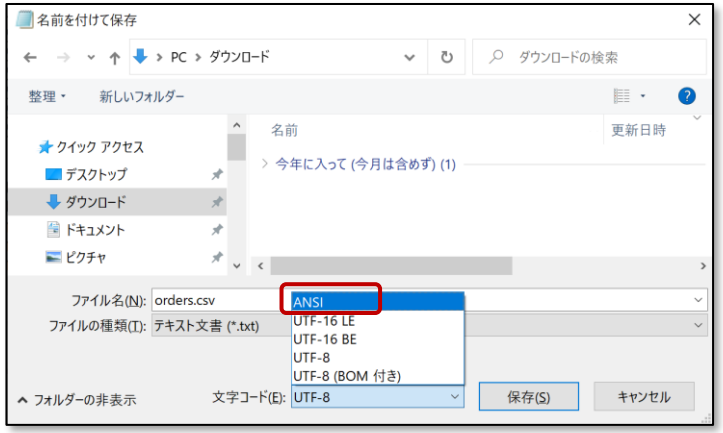


手順4 : 右下部「読み込み」ボタンを押下してインポートを完了すると日本語データの文字化けが解消された状態でレポートを確認いただけます

■方法2 : CSVファイルをANSI/Shift_JISに変換して開く

手順1 : 「メモ帳(Notepad)」でダウンロードしたオーダーレポート(CSV形式)を開く

手順2 : 「ファイル」→「名前を付けて保存」メニューから下図の「名前を付けて保存」ウィンドウを開く

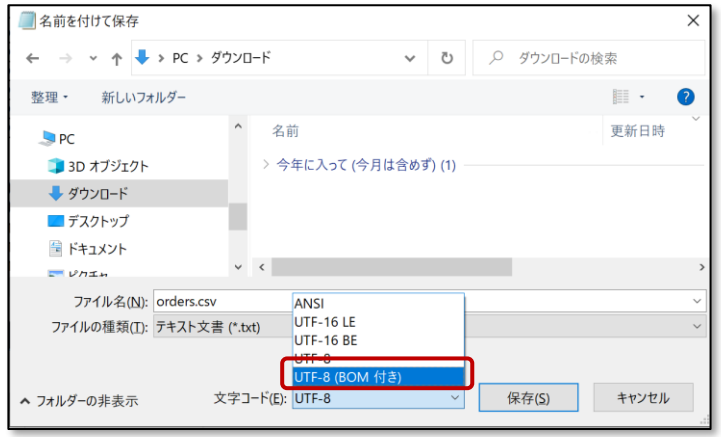


手順3 : 上図の通り「文字コード」に「ANSI」を選択し、ファイルを保存(拡張子=.csv)」する

手順4 : Microsoft Excelでファイルを開くと、日本語データの文字化けが解消した状態でレポートを確認いただけます

■方法3 : CSVファイルにBOMを付与して開く

手順1 ~ 手順2 : 左の方法2に同じ

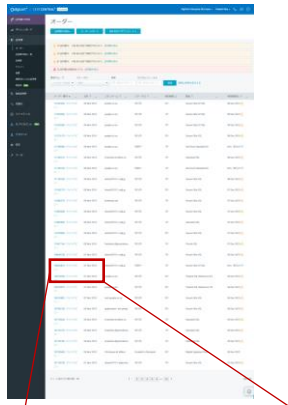


手順3 : 上図の通り「文字コード」に「UTF-8 (BOM付き)」を選択し、ファイルを保存(拡張子=.csv)」する

手順4 : Microsoft Excelでファイルを開くと、日本語データの文字化けが解消した状態でレポートを確認いただけます

「証明書」→「オーダー」メニューの使い方 (2/2 オーダー詳細)

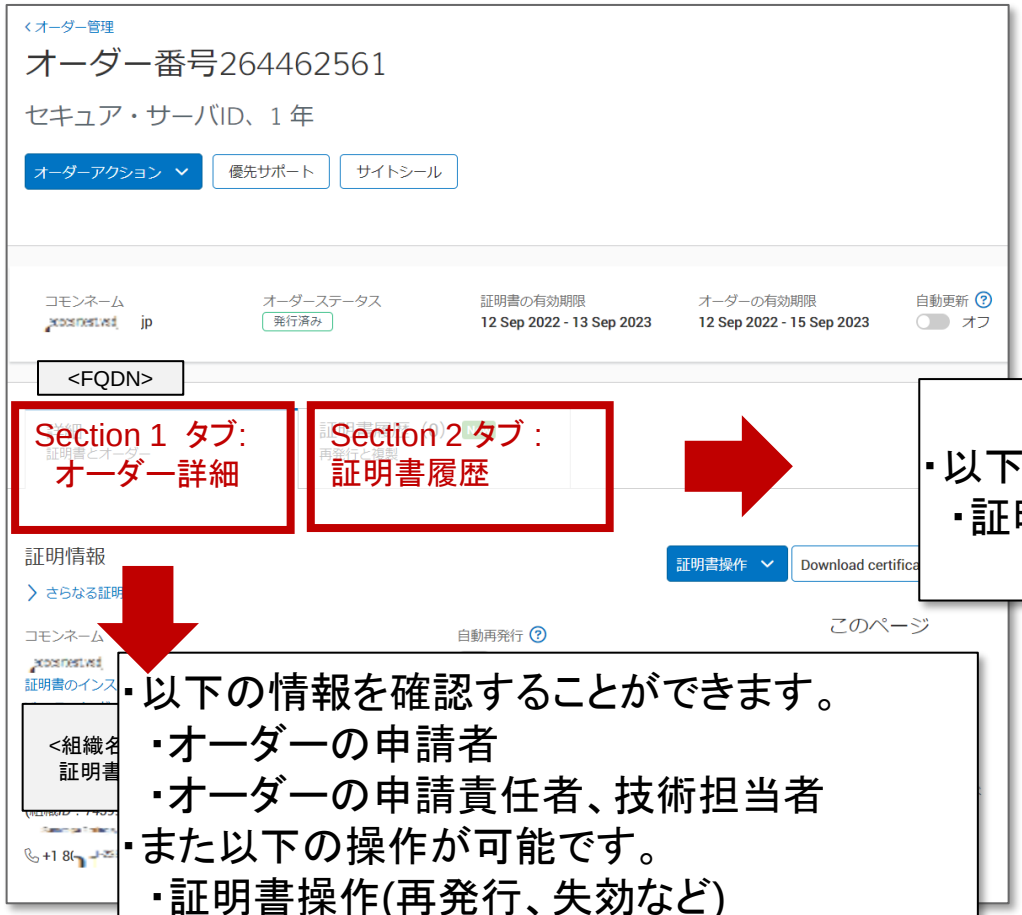
■オーダー一覧



10864414 クイックビュー

Click

■オーダー詳細画面



・以下の管理機能を利用いただけます。
　・証明書再発行履歴の確認

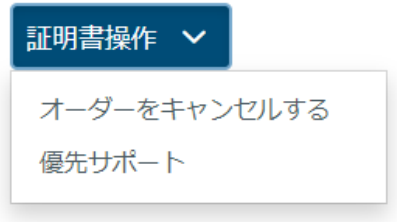
・以下の情報を確認することができます。
　・オーダーの申請者
　・オーダーの申請責任者、技術担当者
・また以下の操作が可能です。
　・証明書操作(再発行、失効など)
　・メール送信先の追加
　・更新案内メッセージの編集

「証明書」→「オーダー」メニューの使い方 (2/2 オーダー詳細)

■オーダー詳細画面

Section 1 タブ:
オーダー詳細

■証明書詳細（**ステータス＝未発行(pending)**の場合）



メニュー	説明
オーダーをキャンセル	オーダーを（発行前）キャンセル
優先サポート	サポートへ問い合わせ

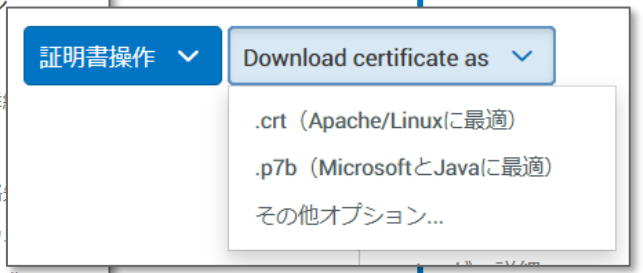
ステータス＝未発行(pending)の場合、以下の
カテゴリごとに完了／未完了の状況が表示されます。
・ドメイン名利用権確認(DCV)
・組織認証(可能な場合、さらに詳細な項目を表示)
・(EV/CS/EVCSの場合)認証済連絡先の確認
・証明書発行

「証明書」→「オーダー」メニューの使い方 (2/2 ステータス・管理)

■オーダー詳細画面

Section 1 タブ:
オーダー詳細

■証明書詳細（**ステータス＝発行済(issued)**の場合）



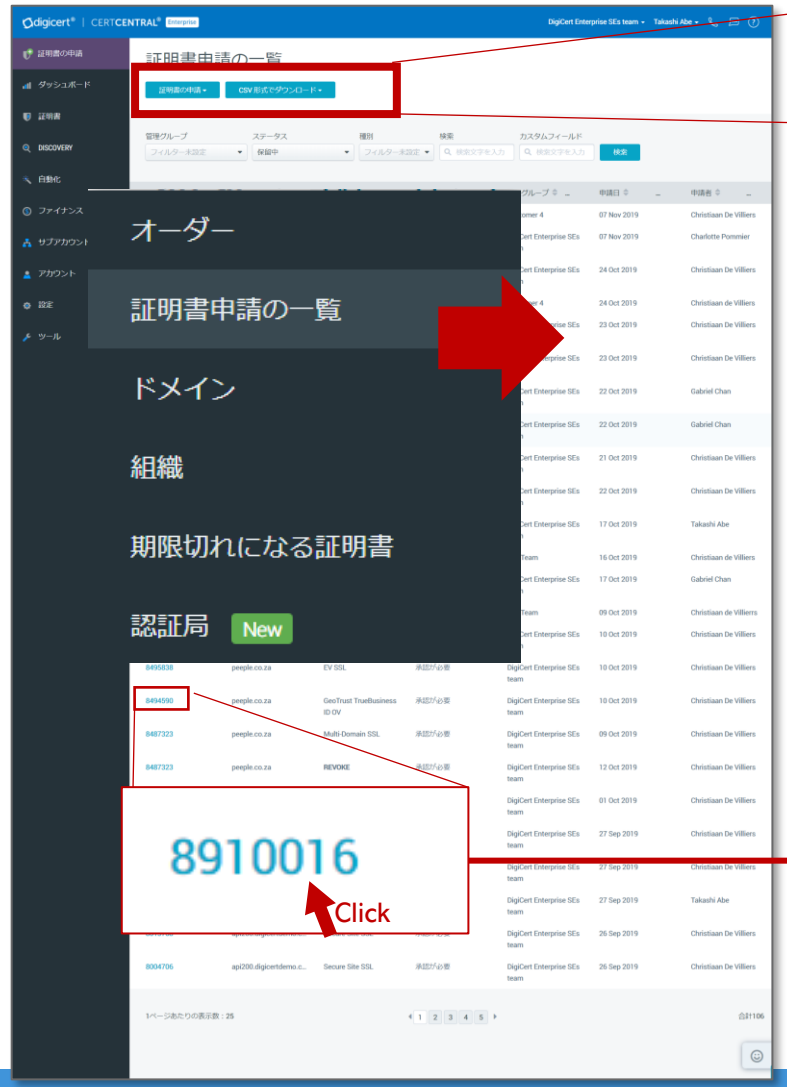
後述の *セクション５「発行された証明書の取得」* を参照ください

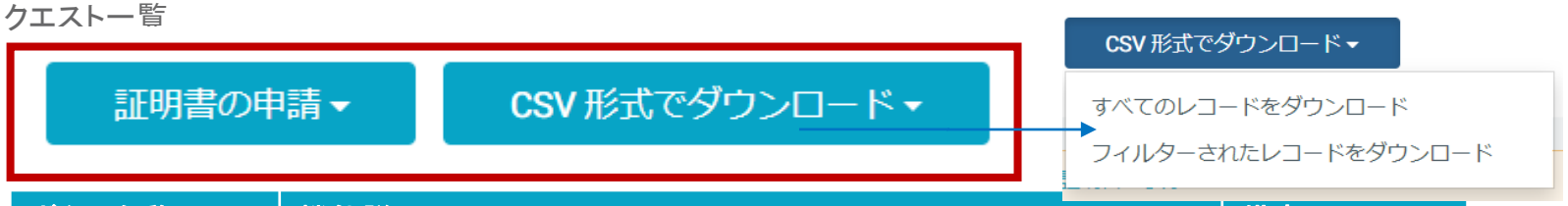
(表示例)

メニュー (例)	説明	備考
証明書を送信	証明書をメールで送信	-
証明書を更新	(有効期限の90日前以降の場合のみ) 証明書の更新申請画面へ移動	*詳細はセクション 3.1 を参照*
複製発行を申請する	証明書の複製(Duplicate)申請画面へ移動	*詳細はセクション 6を参照*
証明書を再発行する	証明書の再発行(Reissue)申請画面へ移動	
すべての証明書を取り消す	証明書の失効申請画面へ移動	*詳細はセクション 6を参照*
サイトシール	ノートンシール等のサイトシール掲載	*詳細はセクション 10.1を参照*

「証明書」→「証明書申請の一覧」メニューの使い方

■「証明書」→「証明書申請の一覧」メニューから表示するリクエスト一覧





ボタン名称	機能説明	備考
証明書の申請	・製品の選択→新規申請を開始	新規申請画面は別項参照
CSV形式でダウンロード	■「すべてのレコードをダウンロード」 アカウント内の全ての「承認待ち」リクエスト(証明書発行リクエスト、失効リクエストなど) 情報を含むレポートをCSV形式でダウンロードします。 ■「フィルターされたレコードをダウンロード」 画面上で指定されたフィルター条件を適用した状態で、該当するリクエスト情報を含むレポートをCSV形式でダウンロードします。	ー

ボタン名称	機能説明	備考
却下	リクエストを却下する	■証明書申請時の「承認」要否について: 【アカウント設定「承認手順」】によって証明書発行リクエストに対する「承認」操作の要否が異なります。 詳細については**セクション3.1 内「アカウント内での申請レビュー・承認について」を参照** ■失効申請時の「承認」要否について: 失効申請の場合は、全ての場合において、管理者による失効リクエストに対する「承認」操作が必要となります。 詳細については**セクション6「失効申請」を参照**
承認	リクエストを承認する	

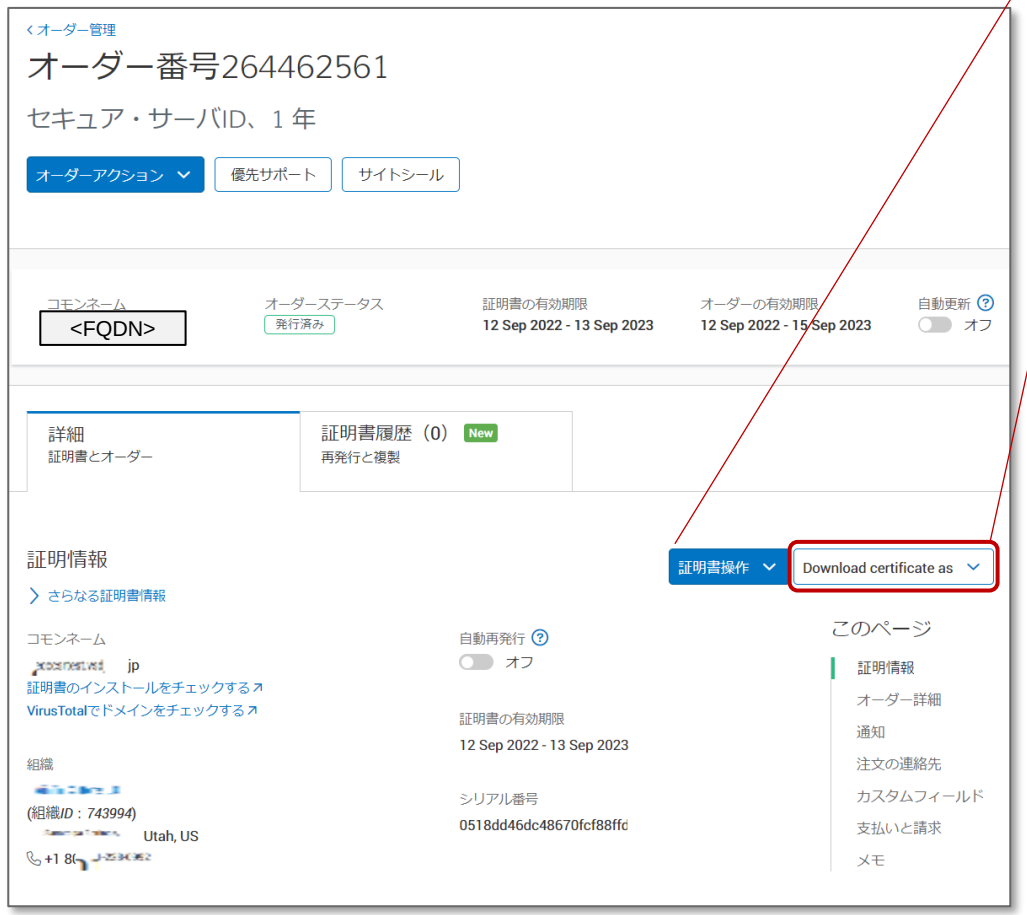
5. 発行された証明書・中間証明書の取得

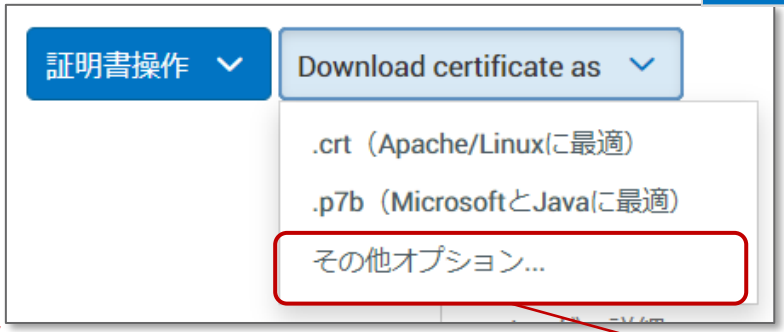
~ 5.1 発行された証明書の取得 ~

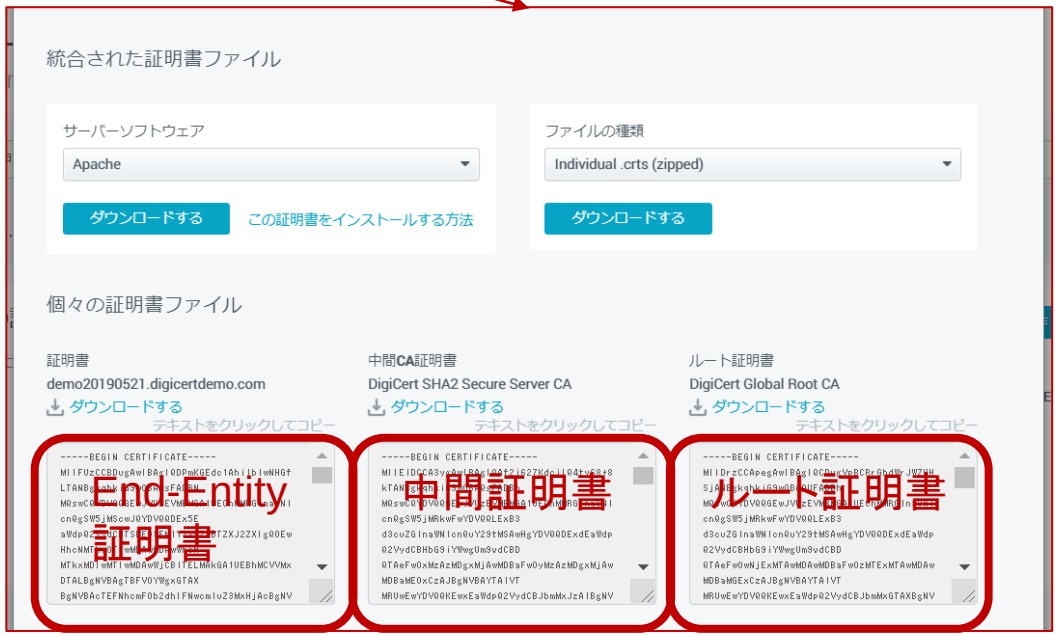
発行された証明書の取得（画面からダウンロード）

証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■証明書発行後のオーダー詳細画面イメージ







■ポイント：お客様の環境（サーバーの種類や配布方式）に応じて複数のフォーマット・ファイル形式から最適なものを選択して証明書をダウンロードいただくことが可能です。

発行された証明書の取得（メールを受領）

証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■発行通知メール配信先

#	配信先	説明	設定
①	[アカウント設定] 「設定」→「通知」→「全通知の送信先」	アカウント単位で任意のメールアドレス(固定)を指定可能 **（複数設定可能）**	アカウントメニュー**「設定」**→**「通知」**にて**「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
②	[オーダー(証明書申請)別パラメータ] User Placing Order/申請者	オーダー(証明書申請)を実行したCertCentralのユーザーアカウントに紐づいたメールアドレス	アカウントメニュー**「設定」**→**「通知」**にて**「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
③	[オーダー(証明書申請)別パラメータ] Organization Contact/申請責任者	オーダー(証明書申請)時に、組織の「Organization Contact/申請責任者」として指定した担当者のメールアドレス	アカウントメニュー**「設定」**→**「通知」**にて**「Send emails to organization contact」**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] Technical Contact/技術担当者	オーダー(証明書申請)時に、組織の「Technical Contact/技術担当者」として指定した担当者のメールアドレス	アカウントメニュー**「設定」**→**「通知」**にて**「Send emails to technical contact」**欄のチェックボックスをONにした場合に配信
⑤	[オーダー(証明書申請)別パラメータ] Additional Emails/メールの追加送信先	オーダー(証明書申請)時に、「メール送信先の追加(Additional Emails)」欄に指定したメールアドレス **（複数設定可能）**	オーダー(証明書申請)時の入力欄**「その他のオーダーオプション」**→**「メール送信先の追加」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

■「設定」→「通知」メニューにおけるメール配信先に関する設定箇所

■証明書申請画面(セクション3.1参照)における「メール送信先の追加」欄
（複数設定可能）

■オーダー詳細画面(セクション4参照)における「メール送信先の追加」欄
（複数設定可能、証明書発行後も追加可能）

発行された証明書の取得（メールを受領）

証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
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
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■発行通知メールのフォーマット

・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。
・お客様の環境（サーバーの種類や配布方式）に応じて複数のフォーマット・ファイル形式から最適なフォーマットを選択していただくことが可能です。

件名	[コモンネーム] 証明書発行のお知らせ		
送信元	DigiCert <admin@digicert.com>		
アカウント設定	■「設定」メニュー下「証明書フォーマット」＝「添付ファイル」選択時 証明書の配布方式 (●) 添付ファイル ( ) プレーンテキスト ( ) ダウンロードリンク	■「設定」メニュー下「証明書フォーマット」＝「プレーンテキスト」選択時 証明書の配布方式 ( ) 添付ファイル (●) プレーンテキスト ( ) ダウンロードリンク	■「設定」メニュー下「証明書フォーマット」＝「ダウンロードリンク」選択時 証明書の配布方式 ( ) 添付ファイル ( ) プレーンテキスト (●) ダウンロードリンク
本文イメージ(日本語選択時、抜粋)	[アカウント代表組織名] [申請者(User Placing Order)氏名] 様 [ドメイン名]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 本メールに新しい証明書を添付しています。	[アカウント代表組織名] [申請者(User Placing Order)メールアドレス] 様 [コモンネーム]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 証明書: [End-Entity証明書データ(BASE64形式)] 中間CA証明書: [中間CA証明書データ(BASE64形式)]	[アカウント代表組織名] [申請者(User Placing Order)メールアドレス] 様 [ドメイン名]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 証明書は以下のURLからダウンロードいただけます。 [証明書ダウンロードURL]

※：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

発行通知メールや、発行通知メールに含まれる証明書ファイルについては、以下の弊社FAQページも併せて参照ください。
[CertCental]サーバ証明書 インストール手順 https://knowledge.digicert.com/ja/jp/solution/SOT0002.html

「添付ファイル」形式：[サーバーソフトウェア]別 証明書ファイル形式

■（証明書フォーマット＝添付ファイルの場合）発行通知メールに添付される証明書ファイル形式は、証明書申請時に指定するサーバープラットフォーム/サーバーソフトウェアの指定によって、以下のいずれかの形式となります。

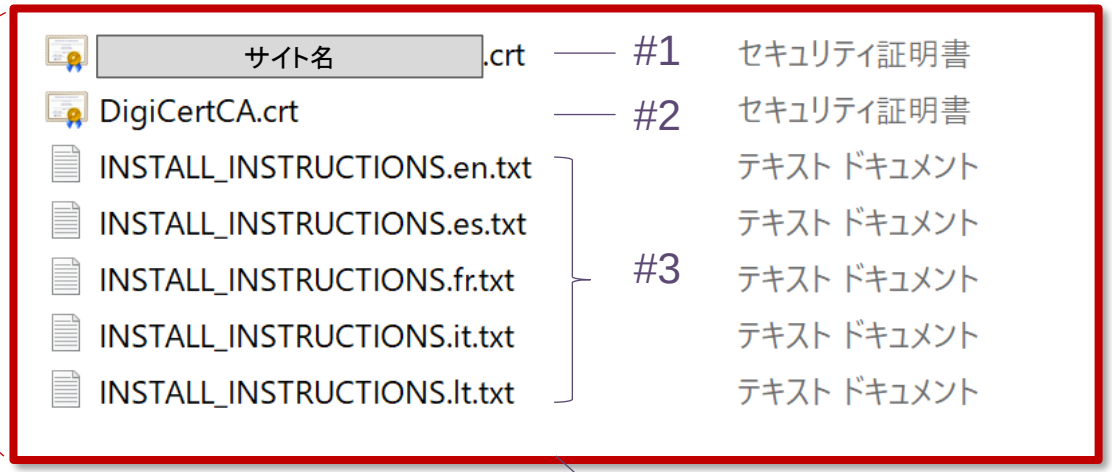
No	サーバーソフトウェア (※1)	ファイル形式ID (※2)	ファイル形式/拡張子	ファイルに含まれる内容
1	Apache(デフォルト)、Citrix Access Gateway 5.x and higher、cPanel、F5 Big-IP、他	apache (デフォルト)	ZIP圧縮ファイル/.zip	-エンドエンティティ証明書(.crt) -中間証明書(.crt)
2	Barracuda、Cisco、Citrix Access Essentials、Juniper、“OTHER”、他	default	ZIP圧縮ファイル/.zip	-エンドエンティティ証明書(.crt) -中間証明書(.crt) -ルート証明書(.crt)
3	IBM HTTP Server	default_cer	ZIP圧縮ファイル/.zip	-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	Microsoft Exchange Server 2016、Microsoft IIS 10、Microsoft Lync Server 2010、Microsoft Office Communications Server 2007、他	cer	PKCS#7形式証明書ファイル/.cer	-エンドエンティティ証明書 -中間証明書 -ルート証明書
5	BEA Weblogic 8 & 9、Java Web Server (Javasoft / Sun)、Microsoft OCS R2、Tomcat、他	p7b	PKCS#7形式証明書ファイル/.p7b	-エンドエンティティ証明書 -中間証明書 -ルート証明書
6	Bea Weblogic 7 and older、Qmail	pem_all	PEM形式証明書ファイル/.pem	-エンドエンティティ証明書 -中間証明書 -ルート証明書
7	nginx、Citrix Access Gateway 4.x、Citrix (Other)	pem_noroot	PEM形式証明書ファイル/.pem	-エンドエンティティ証明書 -中間証明書

当ページの内容は以下のKnowledgeページの要約となります。上表に記載のないサーバーソフトウェアなど、さらに詳細は以下ページを併せてご参照ください。
・サーバーソフトウェア：https://dev.digicert.com/glossary/#server-platforms (※1:サーバーソフトウェアの一覧はこちらを参照ください)
・ファイル形式について：https://dev.digicert.com/glossary/#certificate-formats (※2:ファイル形式IDの一覧はこちらを参照ください)

（参考）添付ファイルに含まれる証明書の形式 (サーバプラットフォーム=Apacheを選択(デフォルト)いただいた場合)

■発行通知メール(イメージ)

■ZIPファイルを展開した状態(イメージ)



No	圧縮ファイル内のファイル名	内容	備考
#1	<サイト名>.crt	今回申請・発行された お客様のEnd-Entity証明書	-
#2	DigiCertCA.crt	中間CA証明書(※1)	お客様のEnd-Entity証明書と併せて サーバーにインストールしてください(※1)。
#3	INSTALL_INSTRUCTIONS.<言語名>.txt	インストール手順書	当資料作成時点では、発行通知メールの添付ファイルに 含まれるこれらの手順書は日本語に未対応です。 ご不便をおかけし申し訳ございません。 サーバへのインストール手順について不明点がありましたら 当社テクニカルサポートへお問合せください。

※1：中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、添付されている最新の中間証明書をサーバにインストールいただけますようお願いいたします。詳細はこちら：https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

「ダウンロードリンク」形式：証明書ダウンロードページ

■（証明書フォーマット＝ダウンロードリンクの場合）ダウンロードURLをクリックして開く証明書ダウンロードページは以下のようになります

■発行通知メール(イメージ)

サイト名 証明書発行のお知らせ

D DigiCert <admin@digicert.com>
宛先 <受信者>

[アカウント代表組織名]

[申請者(User Placing Order)メールアドレス] 様

[ドメイン名]の証明書申請が承認されました。
証明書のオーダー番号は[オーダー番号]です。

証明書は以下のURLからダウンロードいただけます
[証明書ダウンロードURL]

Click

■[証明書ダウンロードURL]をクリックして開いた証明書ダウンロードページ (イメージ)

※1：中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、当画面で取得いただける最新の中間証明書をサーバにインストールいただけますようお願いいたします。詳細はこちら：https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

（参考）[ファイルの種類]別 証明書ファイル形式

No	ファイルの種類	ファイル形式ID (※1)	ファイル形式/拡張子	ファイルに含まれる内容
1	Individual .crts (zipped) (デフォルト)	default	ZIP圧縮ファイル(.zip)	-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	A P7B bundle of all the certs in a .p7b file	p7b	PKCS#7形式証明書ファイル/.p7b	-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	A P7B bundle of all the certs with a .cer extension	cer	PKCS#7形式証明書ファイル/.cer	-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	Separate primary and intermediate .crt files (zipped)	apache	ZIP圧縮ファイル(.zip)	-エンドエンティティ証明書(.crt) -中間証明書(.crt)
5	A single .pem file containing all the certs	pem_all	PEM形式証明書ファイル/.pem	-エンドエンティティ証明書 -中間証明書 -ルート証明書
6	A single .pem file containing only the end entity certificate	pem_nointermediate	PEM形式証明書ファイル/.pem	-エンドエンティティ証明書
7	A single .pem file containing all the certs except for the root	pem_noroot	PEM形式証明書ファイル/.pem	-エンドエンティティ証明書 -中間証明書
8	Individual .crt files with a .cer extension (zipped)	default_cer	ZIP圧縮ファイル/.zip	-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	Individual .crt files with a .pem extension (zipped)	default_pem	ZIP圧縮ファイル/.zip	-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)

5. 発行された証明書・中間証明書の取得

~ 5.2 中間証明書・証明書階層構造について ~

サーバ証明書(OV/EV)製品の階層構造図 (標準)

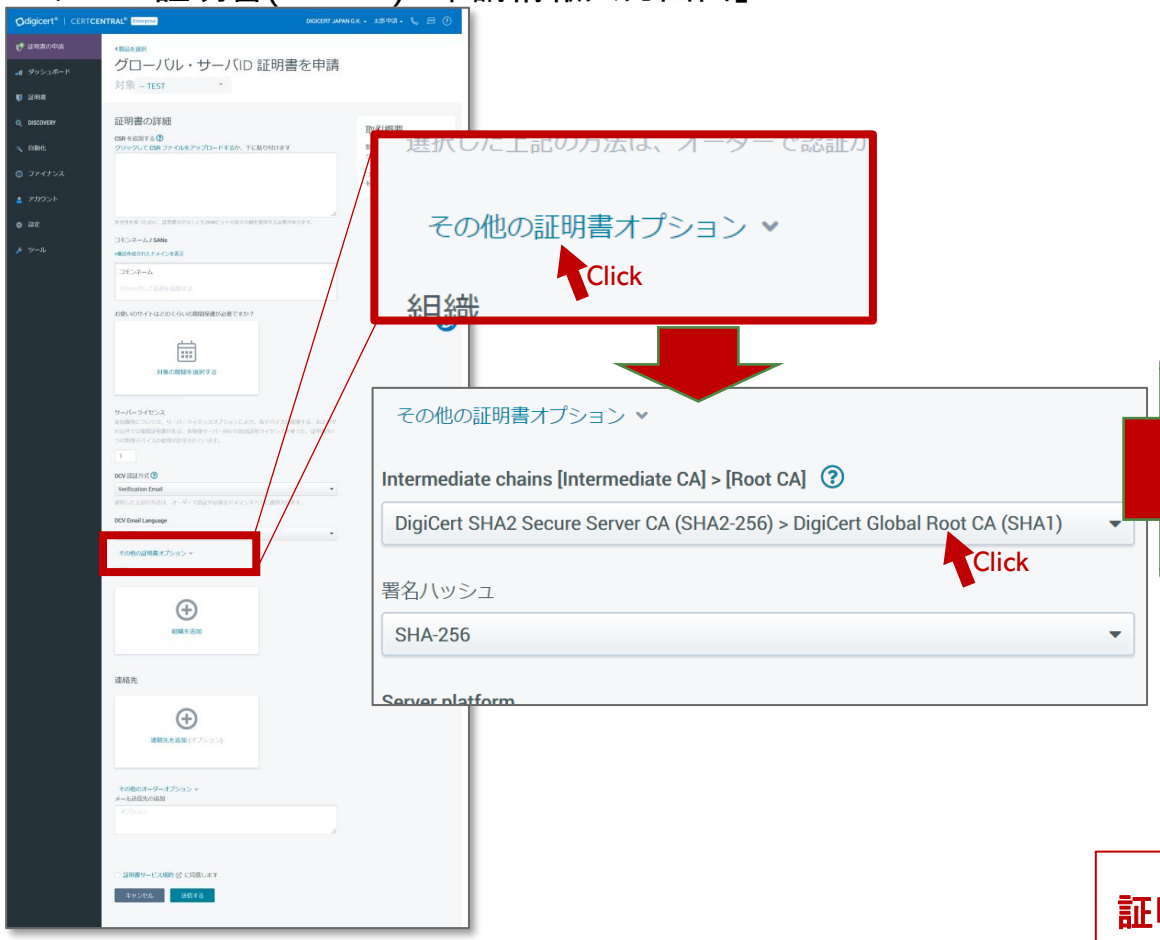
■凡例
1.証明書Subjectの名称
2.公開鍵暗号方式および鍵長
3.デジタル署名
4.有効期限 (GMT)
5.シリアル番号

	グローバル・サーバID (Secure Site Pro SSL) セキュア・サーバID (Secure Site OV)	グローバル・サーバID EV (Secure Site Pro EV SSL) セキュア・サーバID EV (Secure Site EV)
ルート証明書	1. DigiCert Global Root CA 2. RSA2048bit 3. sha1withRSA 4. 2031年11月10日 5. 083be056904246b1a1756ac95991c74a	1. DigiCert High Assurance EV Root CA 2. RSA2048bit 3. sha1withRSA 4. 2031年11月10日 5. 02ac5c266a0b409b8f0b79f2ae462577
ブラウザ/端末側に搭載 *(ブラウザ/端末と通信する)* *サーバ側に設定*		
中間証明書 (※1)	1. DigiCert TLS RSA SHA256 2020 CA1 2. RSA2048bit 3. sha256withRSA 4. 2030年9月23日 5. 0a3508d55c292b017df8ad65c00ff7e4	1. DigiCert SHA2 Extended Validation Server CA 2. RSA2048bit 3. sha256withRSA 4. 2028年10月22日 5. 0c79a944b08c11952092615fe26b1d83
End-Entity 証明書	1. <お客様のウェブサイトのFQDN> 2. <申請時に提出するCSRに含む公開鍵> 3. <申請時に指定する署名ハッシュ(デフォルト:SHA-256)> 4. <申請時に指定する証明書有効期間> 5. <発行都度ユニークなシリアル番号を適用>	1. <お客様のウェブサイトのFQDN> 2. <申請時に提出するCSRに含む公開鍵> 3. <申請時に指定する署名ハッシュ(デフォルト:SHA-256)> 4. <申請時に指定する証明書有効期間> 5. <発行都度ユニークなシリアル番号を適用>

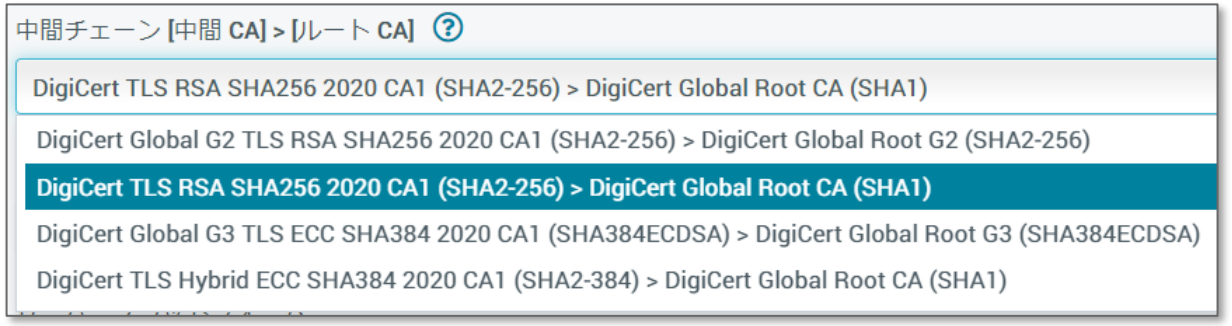
※1：中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、
最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら：https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

サーバ証明書(OV/EV)申請時の階層変更オプション(※1)の指定方法

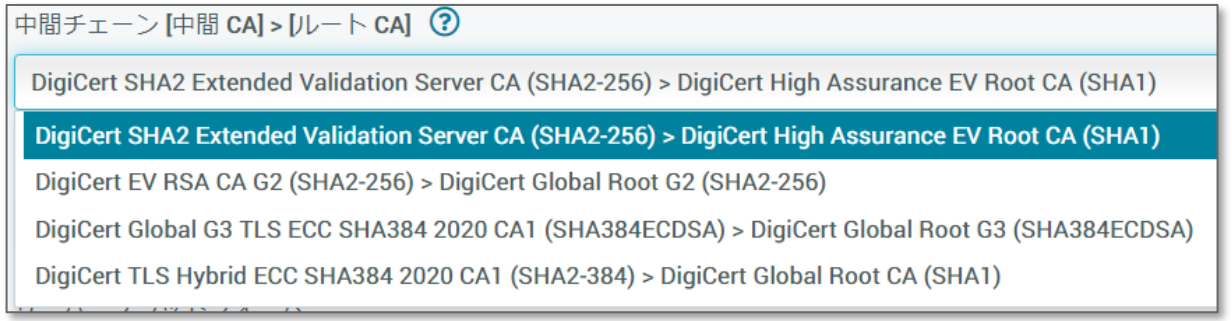
■サーバ証明書(OV/EV)「申請情報入力画面」



■OV証明書の場合の階層オプション選択欄 (※1)



■EV証明書の場合の階層オプション選択欄 (※1)



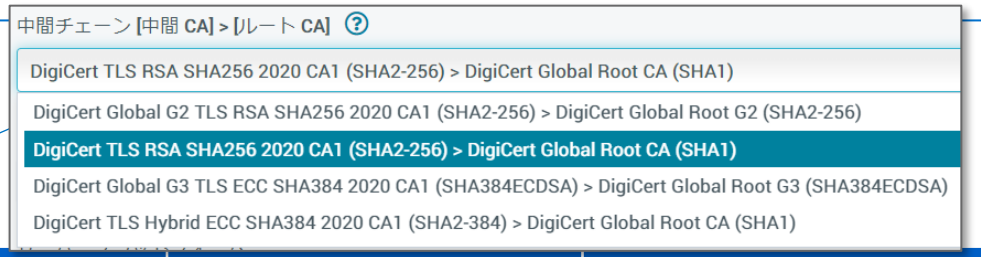
証明書カテゴリや製品種類により選択いただける階層オプションは異なります。
選択可能な階層オプションの詳細については以降のページを参照ください。

※1：「階層変更オプション」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。

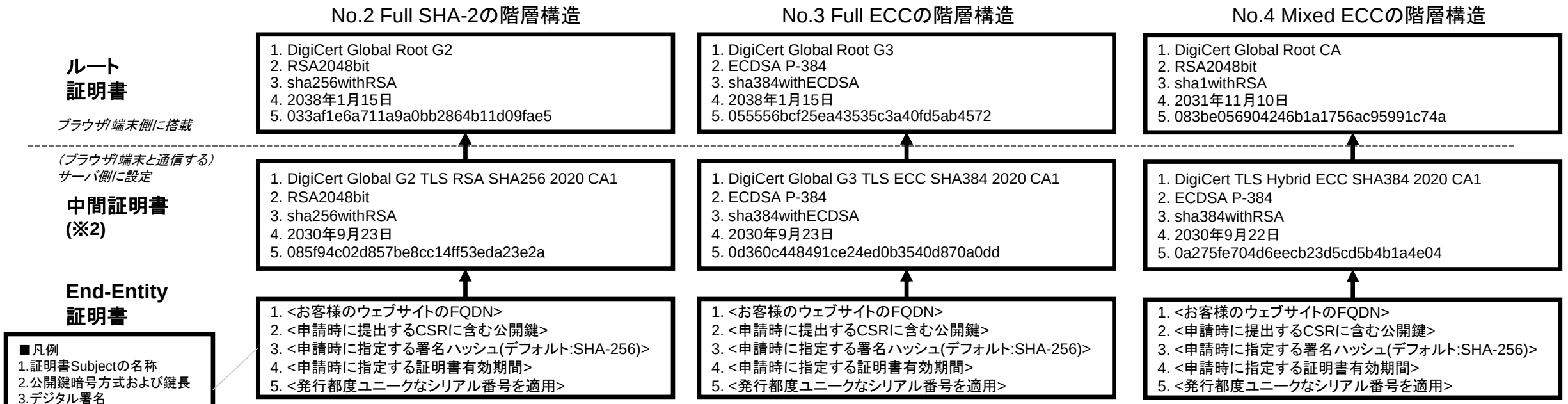
【階層変更オプション(※1)機能を利用した場合】1/2 サーバ証明書(OV)の階層構造図

■対象製品:
・グローバル・サーバID (Secure Site Pro SSL)
・セキュア・サーバID (Secure Site OV)

■OV証明書申請画面
「その他の証明書オプション」内
階層オプション選択欄(※1)



No.	プルダウンの選択肢	通称	ルート (鍵/自己署名)	中間 (鍵/署名)
1	DigiCert TLS RSA SHA256 2020 CA1 (SHA2-256) > DigiCert Global Root CA (SHA1)	**標準** / Mixed SHA-2	RSA2048 / SHA-1	RSA2048 / SHA-256
2	DigiCert Global G2 TLS RSA SHA256 2020 CA1 (SHA2-256) > DigiCert Global Root G2 (SHA2-256)	Full SHA-2	RSA2048 / SHA-256	RSA2048 / SHA-256
3	DigiCert Global G3 TLS ECC SHA384 2020 CA1 (SHA384ECDSA) > DigiCert Global Root G3 (SHA384ECDSA)	Full ECC	ECDSA P384 / SHA-384ECDSA	ECDSA P384 / SHA-384ECDSA
4	DigiCert TLS Hybrid ECC SHA384 2020 CA1 (SHA2-384) > DigiCert Global Root CA (SHA1)	Mixed ECC	RSA2048 / SHA-1	ECC P384 / SHA-384

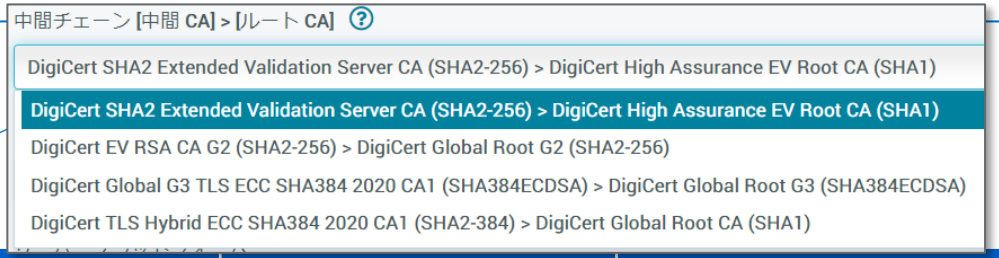


※1:「階層変更オプション」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。
※2:中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら:https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

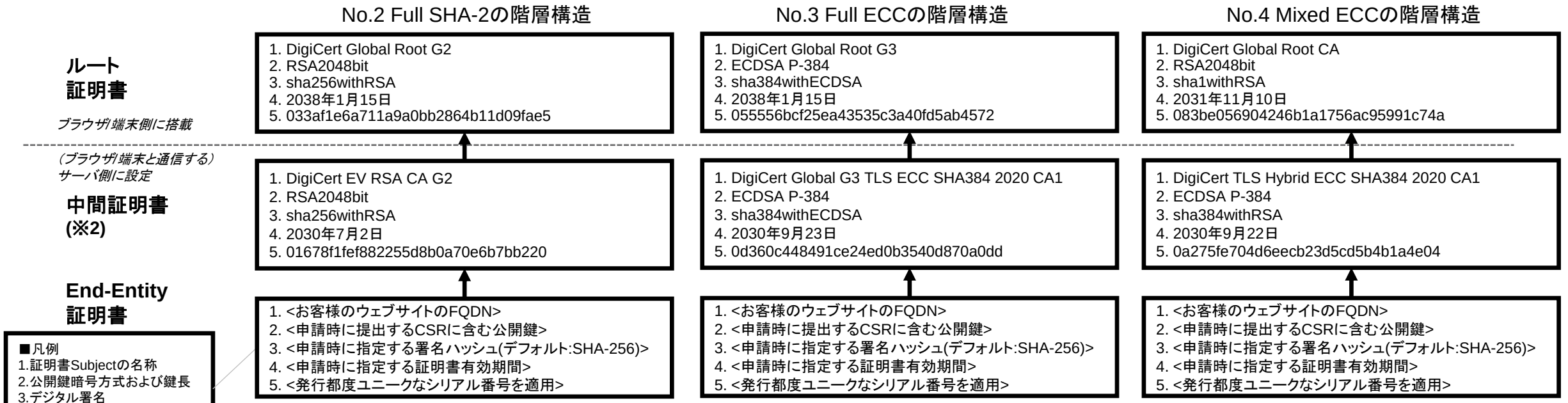
【階層変更オプション(※1)機能を利用した場合】2/2 サーバ証明書(EV)の階層構造図

■対象製品:
・グローバル・サーバID EV(Secure Site Pro EV SSL)
・セキュア・サーバID EV(Secure Site EV)

■EV証明書申請画面
「その他の証明書オプション」内
階層オプション選択欄(※1)

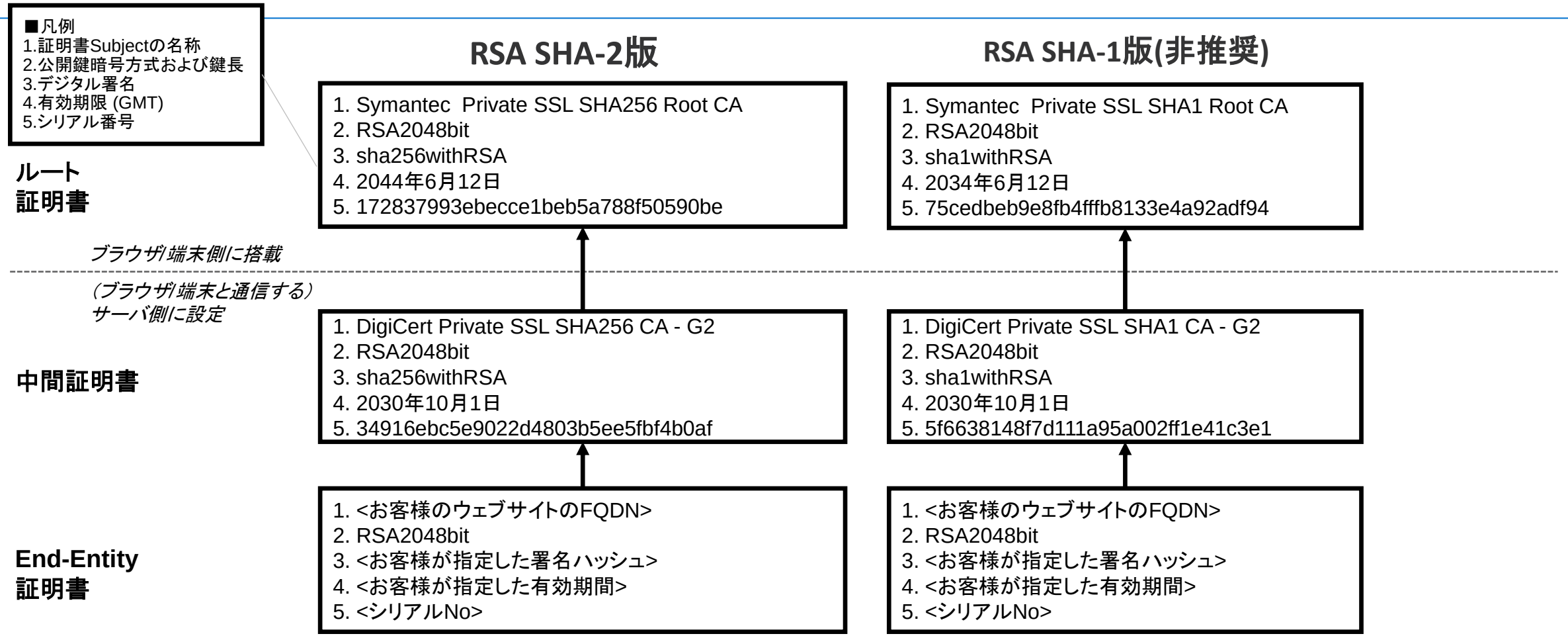


No.	プルダウンの選択肢	通称	ルート (鍵/自己署名)	中間 (鍵/署名)
1	DigiCert SHA2 Extended Validation Server CA (SHA2-256) > DigiCert High Assurance EV Root CA (SHA1)	**標準** / Mixed SHA-2	RSA2048 / SHA-1	RSA2048 / SHA-256
2	DigiCert EV RSA CA G2 (SHA2-256) > DigiCert Global Root G2 (SHA2-256)	Full SHA-2	RSA2048 / SHA-256	RSA2048 / SHA-256
3	DigiCert Global G3 TLS ECC SHA384 2020 CA1 (SHA384ECDSA) > DigiCert Global Root G3 (SHA384ECDSA)	Full ECC	ECDSA P384 / SHA-384ECDSA	ECDSA P384 / SHA-384ECDSA
4	DigiCert TLS Hybrid ECC SHA384 2020 CA1 (SHA2-384) > DigiCert High Assurance EV Root CA (SHA1)	Mixed ECC	RSA2048 / SHA-1	ECC P384 / SHA-384



※1:「階層変更オプション」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。
※2:中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら:https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

プライベートSSL【レガシータイプ】の階層構造図



※ このページの情報はデジサートのプライベートSSL【レガシータイプ】に関するものであり、プライベートSSL【独自認証局タイプ】で個別のお客様にご提供する情報とは異なるものです。
プライベートSSL【独自認証局タイプ】については弊社営業担当までお問合せください。
※ 中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールしてください。
※ プライベートSSL【レガシータイプ】用のクロスルート証明書は以下のKnowledge Baseから取得いただけます。
[CertCentral] プライベートSSLの階層構造について – ルート証明書／中間CA証明書／クロスルート証明書：https://knowledge.digicert.com/ja/jp/solution/SOT0007.html

コードサイニング証明書製品の階層構造図

■凡例
1.証明書Subjectの名称
2.公開鍵暗号方式および鍵長
3.デジタル署名
4.有効期限 (GMT)
5.シリアル番号

【共通】コードサイニング証明書 (Code Signing)/EV コードサイニング証明書 (EV Code Signing)

ルート証明書

1. DigiCert Global Root G4
2. RSA 4096bit
3. sha 384 withRSA
4. 2038年1月15日
5. 059b1b579e8e2132e23907bda777755c

アプリケーションプラットフォーム/署名検証ツール側に搭載

署名ツールに設定して使用

中間証明書 (※1)

1. DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
2. RSA 4096bit
3. sha 384 withRSA
4. 2036年4月29日
5. 08ad40b260d29c4c9f5ecda9bd93aed9

End-Entity 証明書

1. <お客様の組織名称>
2. <申請時に提出するCSRに含む公開鍵>
3. <申請時に指定する署名ハッシュ(デフォルト:SHA-256)>
4. <申請時に指定する証明書有効期間>
5. <発行都度ユニークなシリアル番号を適用>

※1 : コードサイニング証明書には「階層変更オプション」機能はございません。

6. 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

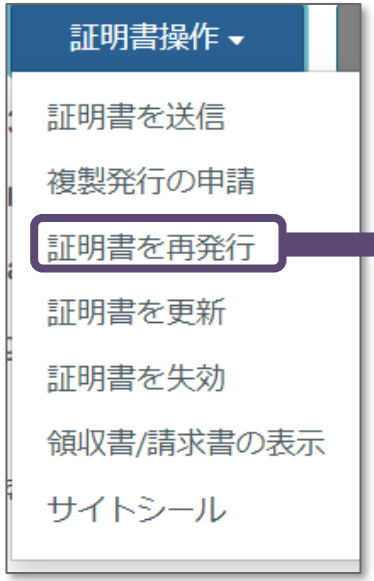
証明書の申請	・製品を選択 ・プランのお申込み（証明書を申請）
申請レビュー・承認	（アカウント単位の設定で省略可） ・管理者が申請内容を確認し、承認または却下
証明書の取得	・発行された証明書をメールで受領、または画面から形式を指定して取得(ダウンロード)
証明書管理	・証明書再発行(証明書の更新) ・証明書の失効

■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：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

サーバ証明書の「再発行(Reissue)申請」

■「証明書操作」メニュー
（例：オーダー詳細画面）



■再発行(Reissue)申請画面

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：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

注2：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、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）

以下の必須項目を入力します
・CSR (注1)
・コモンネーム／SANs (注2)

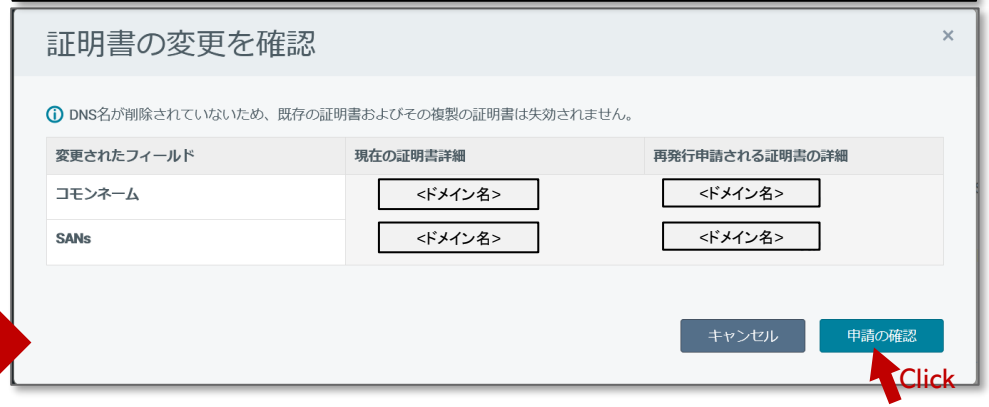
「プランの詳細」で
証明書有効期間を選択・指定します
(詳細は後述の「補足」参照)

必要に応じて「再発行の理由」
を入力します（任意）

「再発行の申請」ボタンを押下します

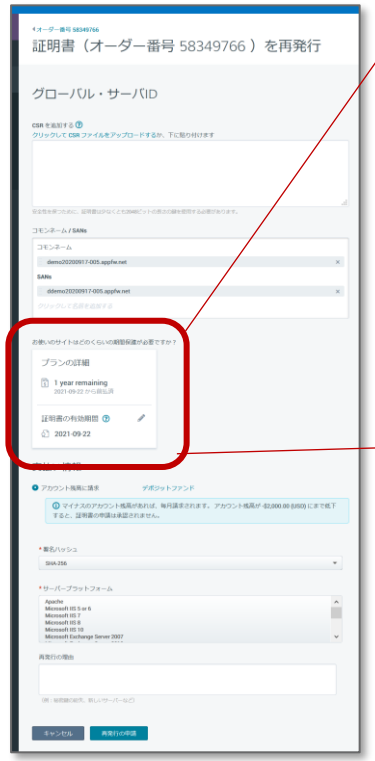
■再発行(Reissue)申請内容確認画面

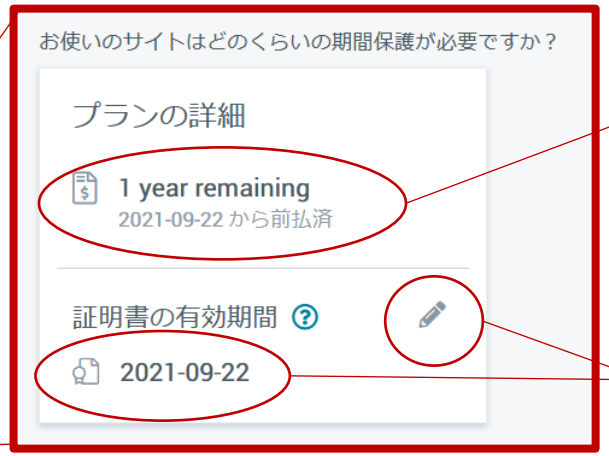
最後に再発行申請内容確認画面が表示されます。
再発行前後の証明書のコモンネーム／SANsの情報を
見比べてご確認いただき、内容に誤りがなければ
「申請の確認」ボタンを押下してください。



補足 再発行(Reissue)申請時の「証明書有効期間」について

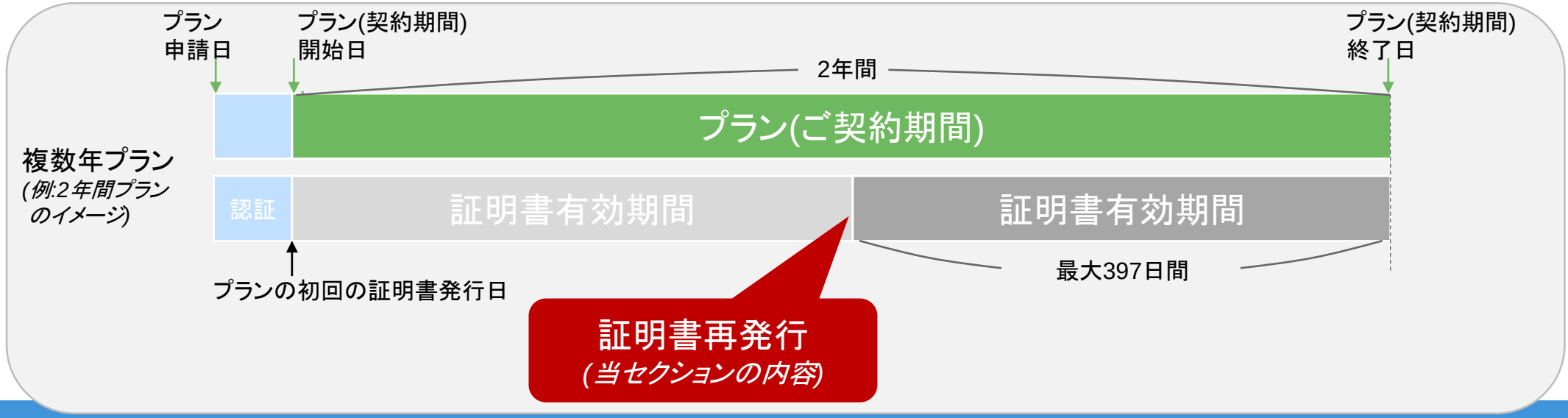
■再発行(Reissue)申請画面





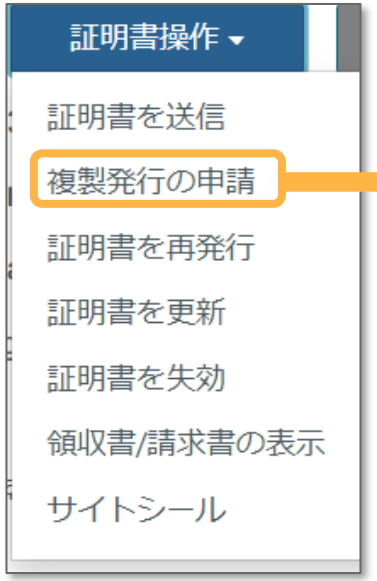
・上段はプラン(ご契約期間)の凡その残り期間を表示します。
・下段は「プラン(契約期間)終了日」を指します。

・【証明書の有効期間】の初期設定値は**「プラン(契約期間)終了日」と「397日間」のいずれか早い方**が設定されます
・上部のペンの形のアイコンをクリックすると[証明書の有効期間]を編集いただくことが可能です
・編集後の【証明書の有効期間】の終了日は「プラン(契約期間)終了日」を超えることはできません
・編集後の【証明書の有効期間】は「397日間」を超えることはできません
・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



サーバ証明書の「複製(Duplicate)申請」

■「証明書操作」メニュー
（例：オーダー詳細画面）



■複製(Duplicate)申請画面

複製申請に必要な以下の情報を入力してください。
・CSR
・署名ハッシュアルゴリズム

必要に応じて「複製発行の理由」を入力します（任意）

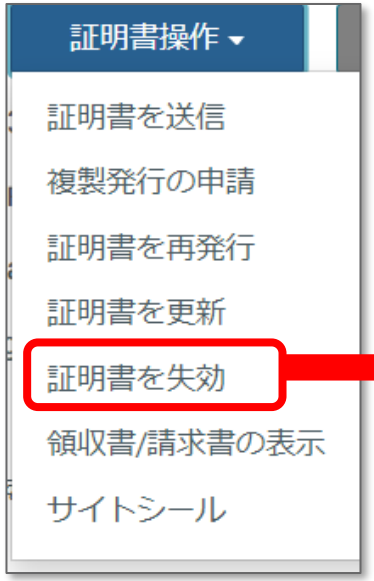
最後に「複製発行の申請」ボタンを押下します。
これで複製発行の申請は完了です。

（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)を追加した場合、以下の式でユニットを消費 **消費ユニット数 ＝ 残プラン年数 x 追加したSANsの数量** （お客様のご契約内容によって実際の費用については異なる場合があります）	・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

証明書の「失効(Revoke)申請」

■「証明書操作」メニュー
（例：オーダー詳細画面）



■失効(Revoke)申請画面

「失効の理由」を入力してください。
（例：「証明書が必要なくなったため」「証明書の秘密鍵が漏洩したため」等）

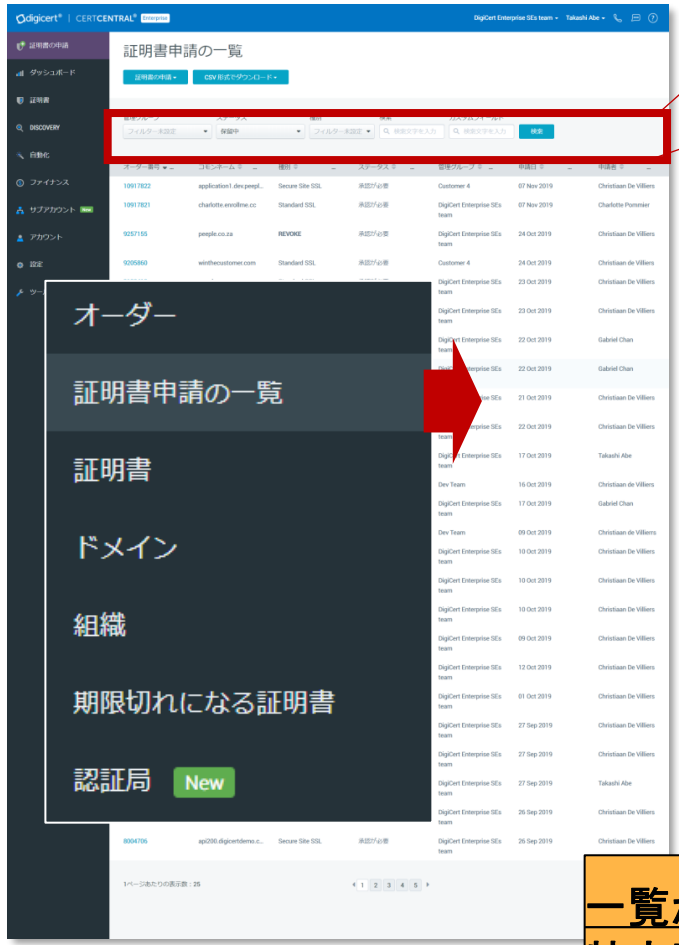
「失効の理由」は管理者による承認（次ページ）時にレビューされ、またシステムに記録されます。

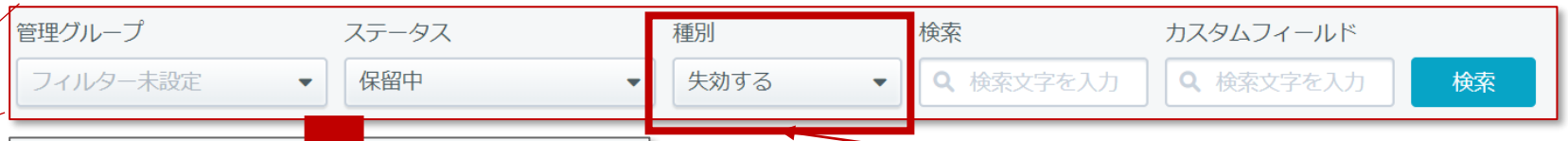
「失効申請」ボタンを押下してください。

※ この時点では失効処理は完了していません。管理者による失効申請リクエストの承認が必要となります。詳細は次ページをご参照ください。

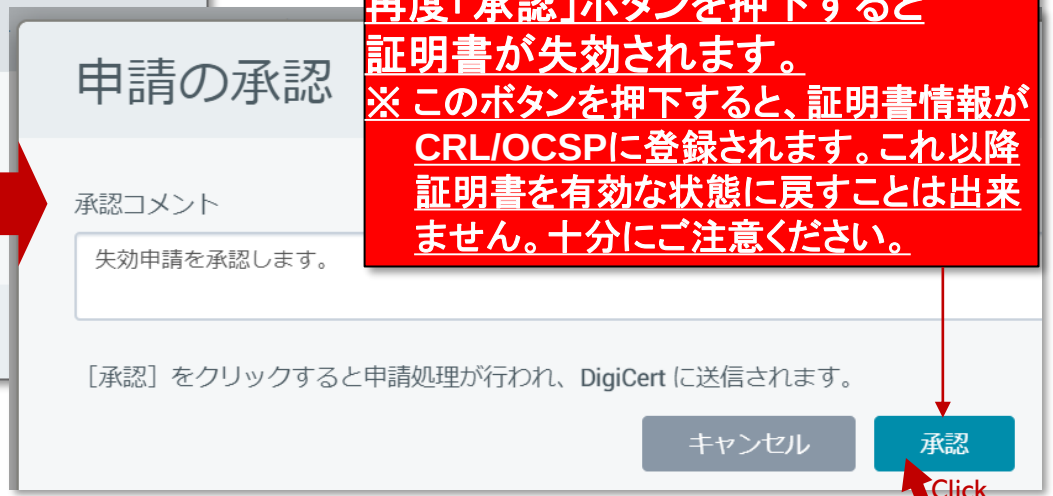
「失効申請」リクエストの特定、レビューおよび「承認」処理

■「証明書」→「証明書申請の一覧」メニューから「失効申請リクエスト」を特定





種別に「失効する」を選択いただき
「検索」ボタンを押下いただくと、
「失効申請」リクエストが一覧表示されます。



最後に「承認コメント」を残して
再度「承認」ボタンを押下すると
証明書が失効されます。
※ このボタンを押下すると、証明書情報が CRL/OCSPに登録されます。これ以降証明書を有効な状態に戻すことは出来ません。十分にご注意ください。

一覧から失効する対象のオーダを
特定してください。右ペインに証明書情報、
申請者による「失効の理由」が表示さます。
ご確認の上、失効してよいと判断された
場合は「承認」ボタンを押下してください。

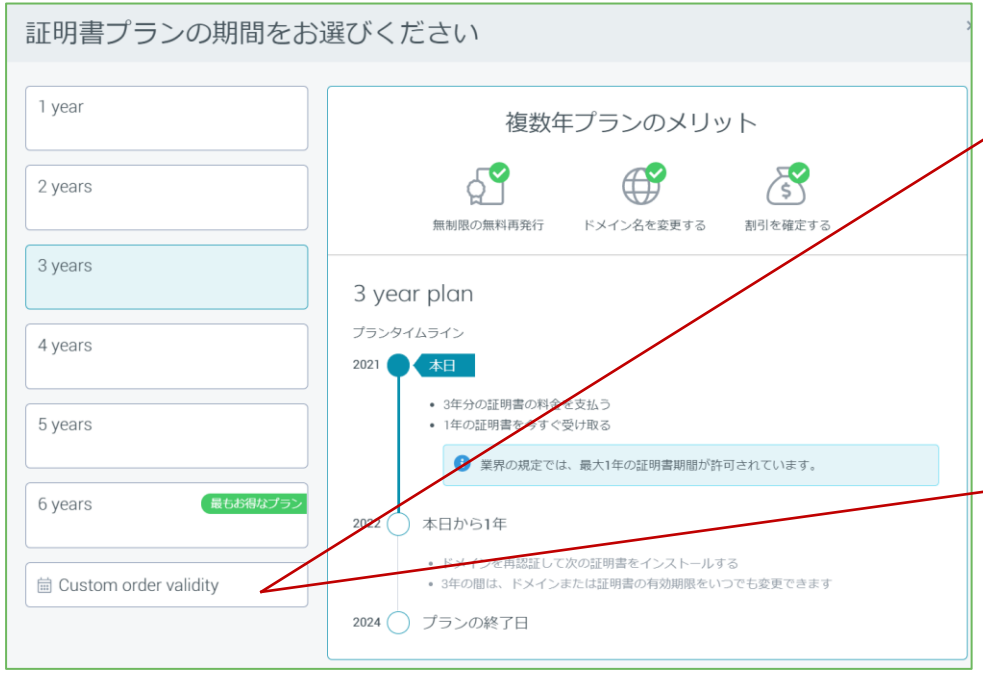
7. プラン・証明書の有効期間、更新案内メールについて

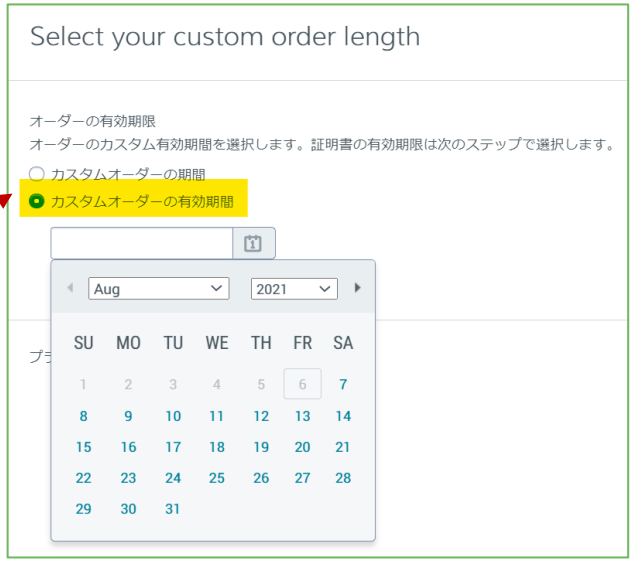
【サーバ証明書(OV/EV/プライベートSSL共通)】新規・更新申請 - プランおよび証明書の有効期間①

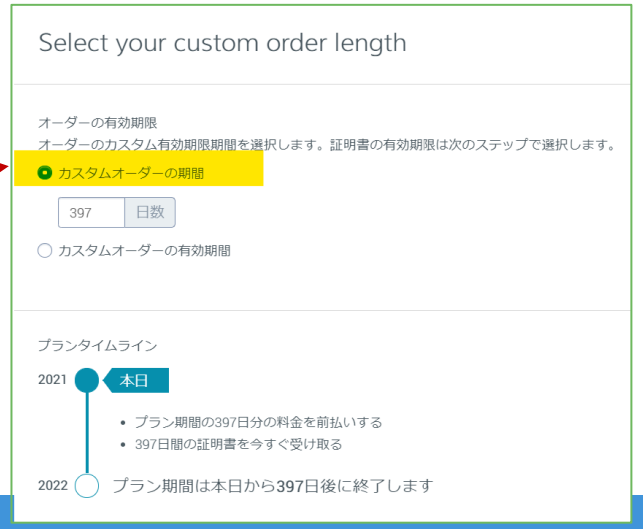
■**サーバ証明書(OV/EV) 新規・更新申請で**設定されるプラン期間および証明書有効期間については以下Knowledgeをご参照ください。

[CertCentral]SSL/TLSサーバ証明書の有効期間設定について
https://knowledge.digicert.com/ja/jp/solution/SO22917.html

■**申請画面の「プラン期間を選択する」でプラン期間を選択・指定することが可能です。**
「Custom order validity」よりプラン期間を日付や日数で指定することも可能です。



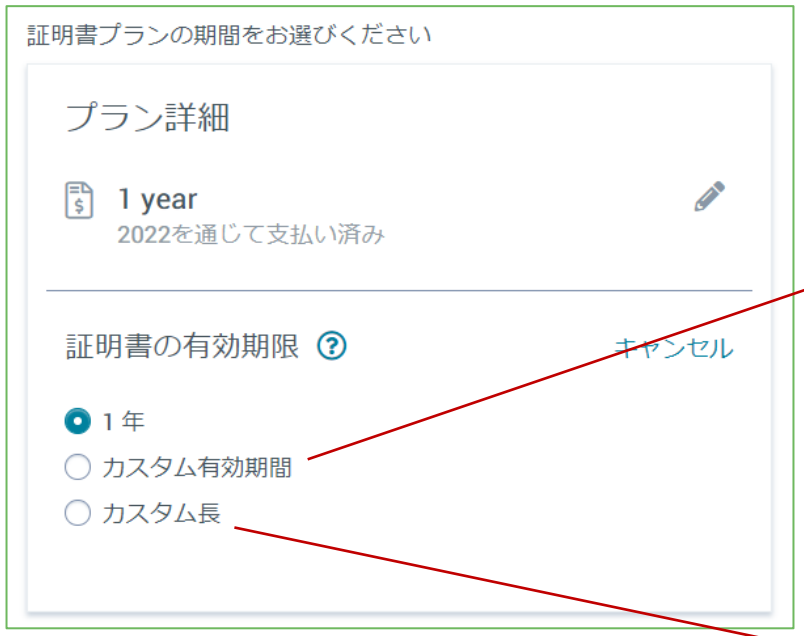




*1：有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります
詳細はこちら：https://docs.digicert.com/ja/manage-certificates/setting-validto-time-certificates/
*2：業界団体CA／ブラウザフォーラムの決議に則り、2020年9月以降にデジサートが発行するパブリック証明書の最大有効期限は最大397日間となります。

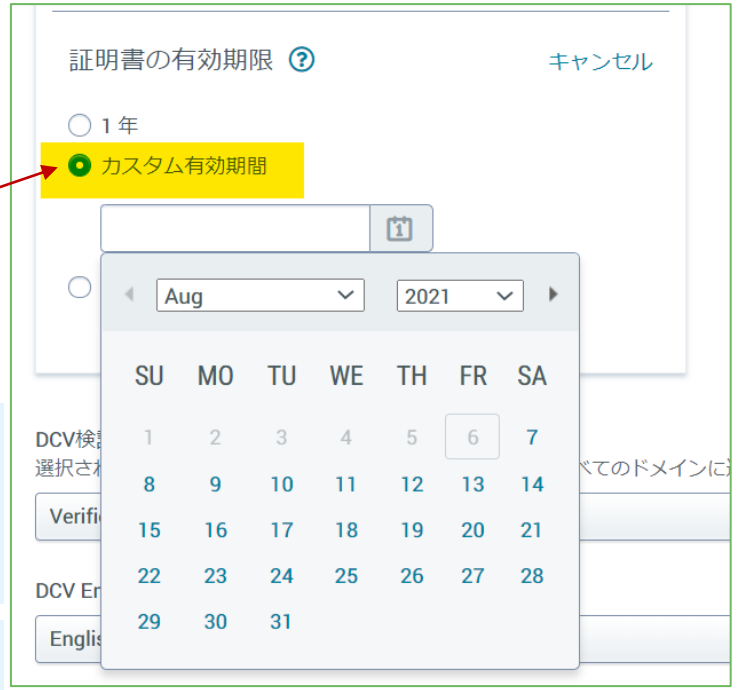
【サーバ証明書(OV/EV/プライベートSSL共通)】新規・更新申請 - プランおよび証明書の有効期間②

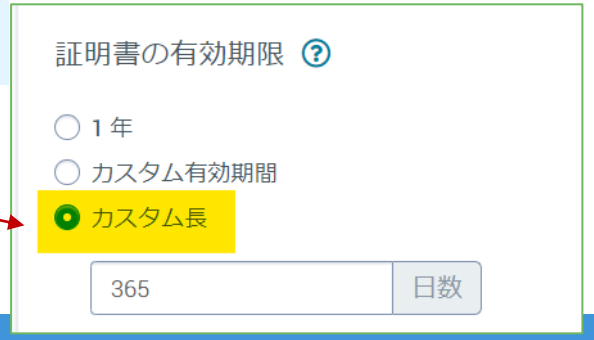
■申請画面のプラン期間を選択後「プランの詳細」の鉛筆マークより、証明書有効期間を日付や日数で指定することも可能です。
※プラン期間を越えた日で設定することはできません。



「カスタム有効期間」
日付形式で有効期間終了日を指定
(カレンダーから選択可)
最大値:申請日から365日後

「カスタム長」
整数値で有効期間(日数)を指定
最大値:397日間(*2)





*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/ja/manage-certificates/setting-validto-time-certificates/
*2 : 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。

【コードサイニング証明書/EVコードサイニング証明書】証明書の有効期間について

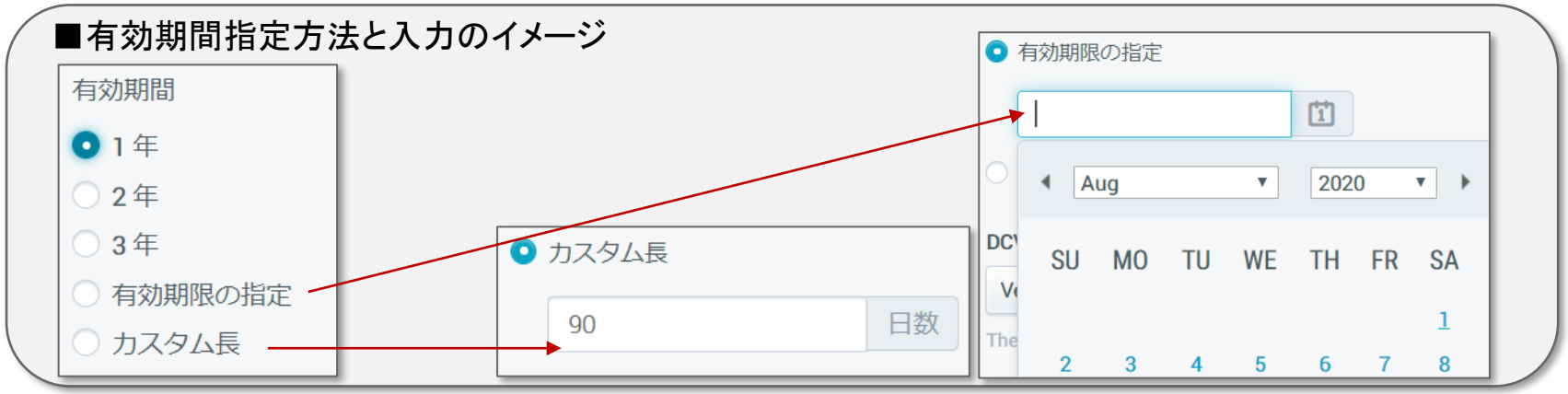
■コードサイニング証明書/EVコードサイニング証明書/プライベートSSLの **新規・更新申請** で設定される証明書有効期間については以下Knowledgeをご参照ください。

コードサイニング証明書の有効期間はどのように設定されますか
https://knowledge.digicert.com/ja/jp/solution/SO23071.html

■申請画面の「プランの詳細」で証明書有効期間を選択・指定することが可能です。

有効期間 選択肢	指定した値	証明書の有効期間	備考
有効期限の指定	日付形式で有効期間終了日を指定 (カレンダーから選択可) (例 : “2021-08-01”)	発行日(有効期間開始日) ～ 指定した日付(有効期間終了日)	「申請～発行までにかかった日数」に関わらず、有効期間終了日には「当欄に指定した日付」が設定されます。 (有効期間は「当欄に指定した日付」－「発行日」となります)
カスタム長	整数値で有効期間(日数)を指定 (例 : “300”)	指定した日数 (最大1,095日)	「申請～発行までにかかった日数」に関わらず、有効期間は当欄に指定した期間となります。 (有効期間終了日には、「発行日」＋「当欄に指定した日数」が設定されます)。

■有効期間指定方法と入力のイメージ

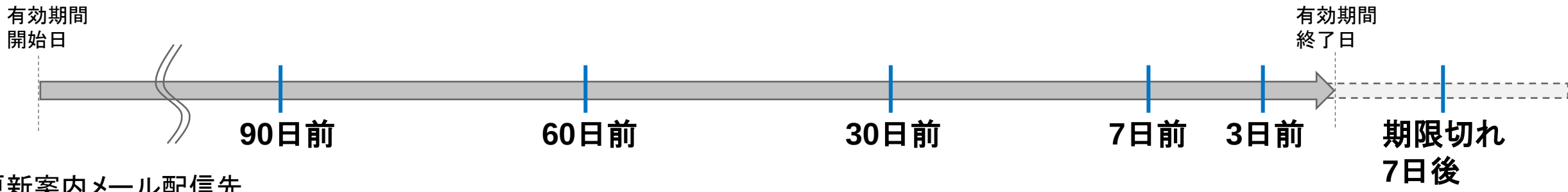


*1 : 有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります
https://docs.digicert.com/ja/manage-certificates/setting-validto-time-certificates/

更新案内メールについて (1/2 メール配信タイミング・配信先)

■更新案内メール配信タイミング

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



■更新案内メール配信先

#	配信先	説明	設定
1	[アカウント設定] 「更新申請通知の送付先」	アカウント単位で任意のメールアドレス(固定)を指定可能 **(複数設定可能)**	アカウントメニュー**「設定」**→**「選択設定」**にて **「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] 「設定」→「通知」→「全通知の送信先」	アカウント単位で任意のメールアドレス(固定)を指定可能 **(複数設定可能)**	アカウントメニュー**「設定」**→**「通知」**にて **「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] User Placing Order/申請者	オーダー(証明書申請)を実行したCertCentralの ユーザーアカウントに紐づいたメールアドレス	アカウントメニュー**「設定」**→**「通知」**にて **「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] Additional Emails/メールの追加送信先	オーダー(証明書申請)時に、「メール送信先の 追加(Additional Emails)」欄に指定したメールアドレス **(複数設定可能)**	オーダー(証明書申請)時の入力欄**「その他のオーダーオプション」**→ **「メール送信先の追加」欄**にメールアドレスを設定した場合、 このアドレスに対して配信

更新案内メールについて (2/2 メールテンプレート)

■更新案内メールのサンプル

→更新案内メール件名、送信元および本文イメージは、以下のようになります

件名	[重要]証明書更新のご案内 N日間 (オーダー番号 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)]

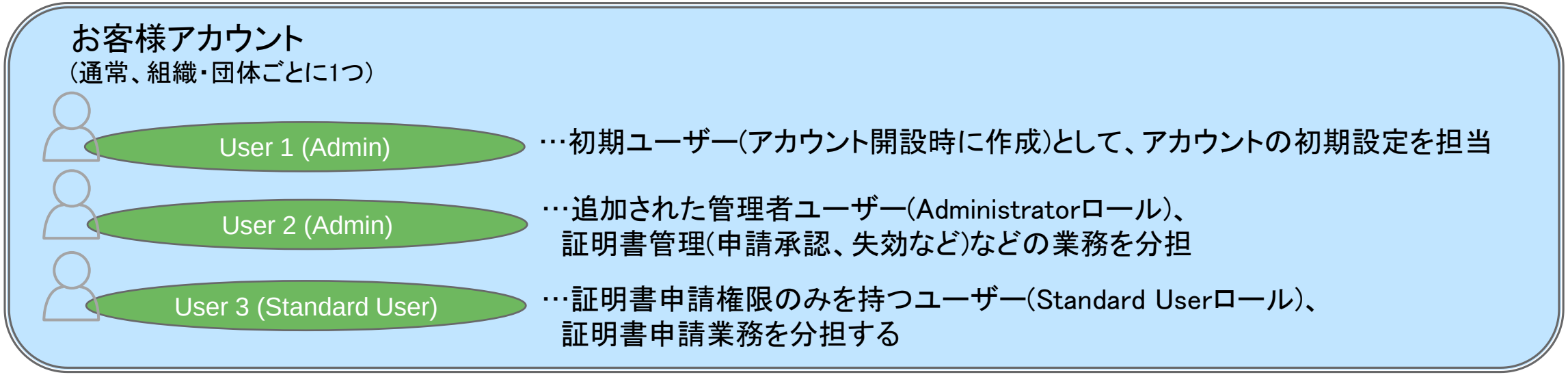
※：上記本文イメージ内に “[“および “]” で囲んだ範囲はお客様固有の申請情報等が記載されます
*1：アカウントメニュー「設定」→「選択設定」内の「証明書の更新設定」セクション下の「既定の更新メッセージ」に設定したテキストが埋め込まれます。

8. ユーザー管理

柔軟なユーザー管理機能 ～証明書管理業務の負荷やリスクを適切に管理～

- CertCentralのアカウントを開設した直後の初期状態は、単一の初期ユーザーのみが存在する状態です。
- 初期ユーザーが他のユーザーを「追加」いただくことで、アカウント内で複数の担当者様によって証明書管理業務を分担いただくことが可能となります。
  - 例1：証明書申請権限のみを持つユーザー(Standard Userロール)を追加し、証明書の申請業務を分担する
  - 例2：管理権限を持つユーザー(Administratorロール)を追加し、証明書管理(申請承認、失効など)業務を分担する
- 登録いただけるユーザー数に上限はございません。
- ユーザ追加の手順ならびに権限(ロール)設定の詳細については以降のページをご参照ください。

■CertCentralアカウント内でユーザーを追加した状態（イメージ）



業務上の必要性に応じて適切な権限(ロール)を付与してください

■CertCentralのユーザー権限 (特定の管理グループにアサインされていないユーザーアカウント)

機能／操作 (*1)	Administrator	Finance Manager	Manager	Standard User	Limited User
・証明書申請 (新規/更新、再発行、失効などのリクエスト) ・申請履歴の参照(自己の申請分)	○	○ （但し新規、失効のみ）	○	○	○
・申請履歴の参照(他ユーザの申請分を含む)	○	○	○	○	
・証明書申請の承認、却下 (*2) ・Discoveryダッシュボードの参照(証明書、エンドポイント脆弱性) ・Discovery管理(センサーの配置、スキャンの実行など) ・ユーザアカウント管理(追加(Adminのみ)、編集、削除) ・ドメイン名管理(追加、認証リクエスト) ・監査ログの参照、監査ログイベント通知の管理	○		○ （ユーザ追加除く）		
・アカウント価格/コントラクト、残高履歴、支出レポート等の確認 ・デポジットファンド、クレジットカードの管理	○	○	○		
・組織(Organization)管理(追加、変更) ・管理グループ(Division)管理(追加、変更) ・セキュリティ設定(認証設定/SSO/IPアクセス制限など) ・製品設定(管理グループ、権限ごとに申請可能な製品を制限可) ・APIキー管理(一覧参照、他ユーザへの発行、削除)	○				

*1 : 画面操作およびAPI操作に共通。尚、自らのユーザアカウントに対するAPIキーの発行は権限に関わらず可能
*2 : 一部製品(EV SSL証明書、コードサイニング証明書)の承認には、上述の権限に加えて追加権限(Subrole)の設定が必要
もっと詳しく(英語資料) : https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/

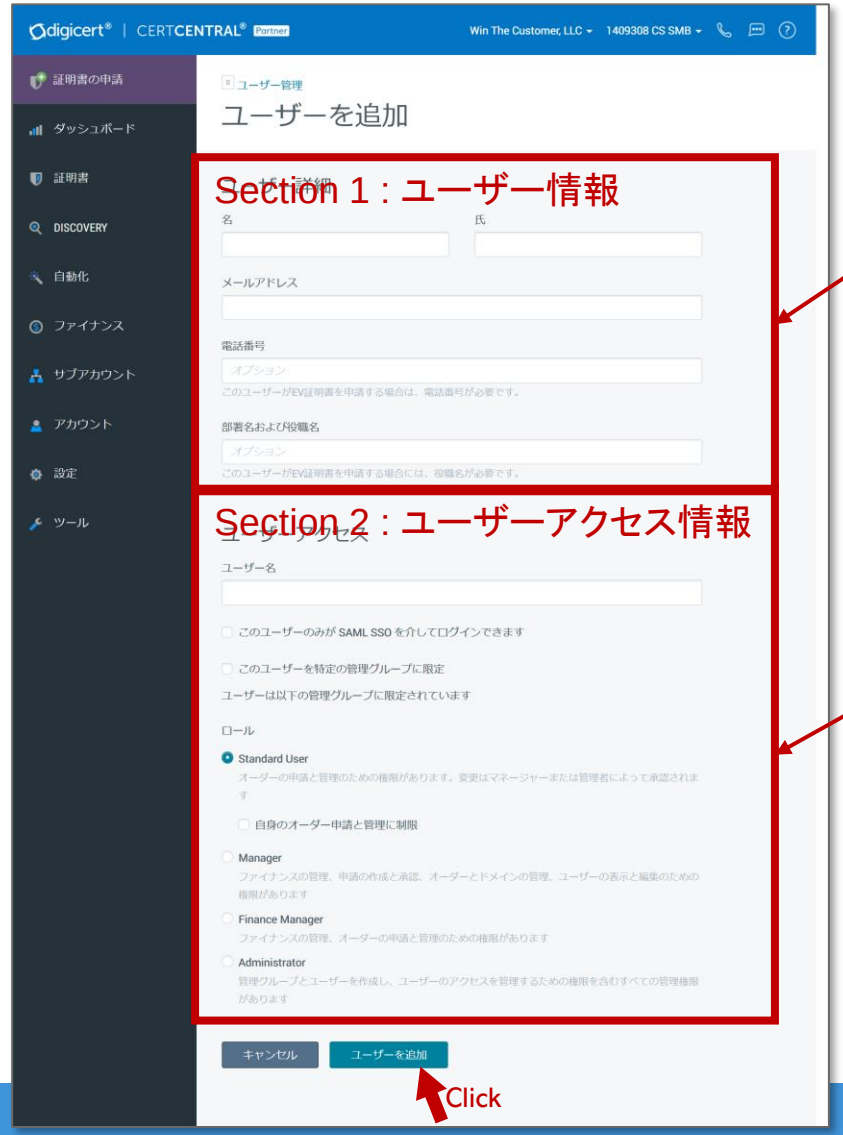
ユーザー追加手順 (1/3 : 既存のユーザーが異なる新規ユーザーを追加登録するシナリオ)

■メニューから「アカウント」→「ユーザー」を選択

■「ユーザーを追加」ボタンを押下してください

ユーザー追加手順 (2/3 : 既存のユーザーが異なる新規ユーザーを追加登録するシナリオ)

■ユーザー追加申請画面



■Section 1: ユーザー情報の入力項目の説明・入力/選択例

項目名	概要	入力例
名	担当者氏名の名	Taro
氏	担当者氏名の氏	Tantou
メールアドレス	担当者の電子メールアドレス ※ このアドレスにパスワードを設定するための手順が記載されたメールが届きます	taro.tantou@digicert.com
電話番号	担当者の電話番号	03-4560-3900
部署名および役職名	担当者の部署名および役職名	Corporate IT Division Manager

■Section 2: ユーザーアクセス情報の入力項目の説明・入力/選択例

項目名	概要	入力例
ユーザー名	アカウントにログインするユーザー名(User ID)を入力してください。 ※ 画面上部のSection1で入力した「メールアドレス」が入力補完されますが、変更が可能です	user01 ※ 上記の入力例はそのまま使用いただくことはできません。入力したユーザー名が他のユーザーによって既に使われている場合、「ユーザー名は利用できません。」というエラーメッセージが表示されます。この場合は別のユーザー名を指定してください
役割	作成するユーザーの権限(役割)を選択 ※別紙ユーザー権限一覧を参照	Standard User

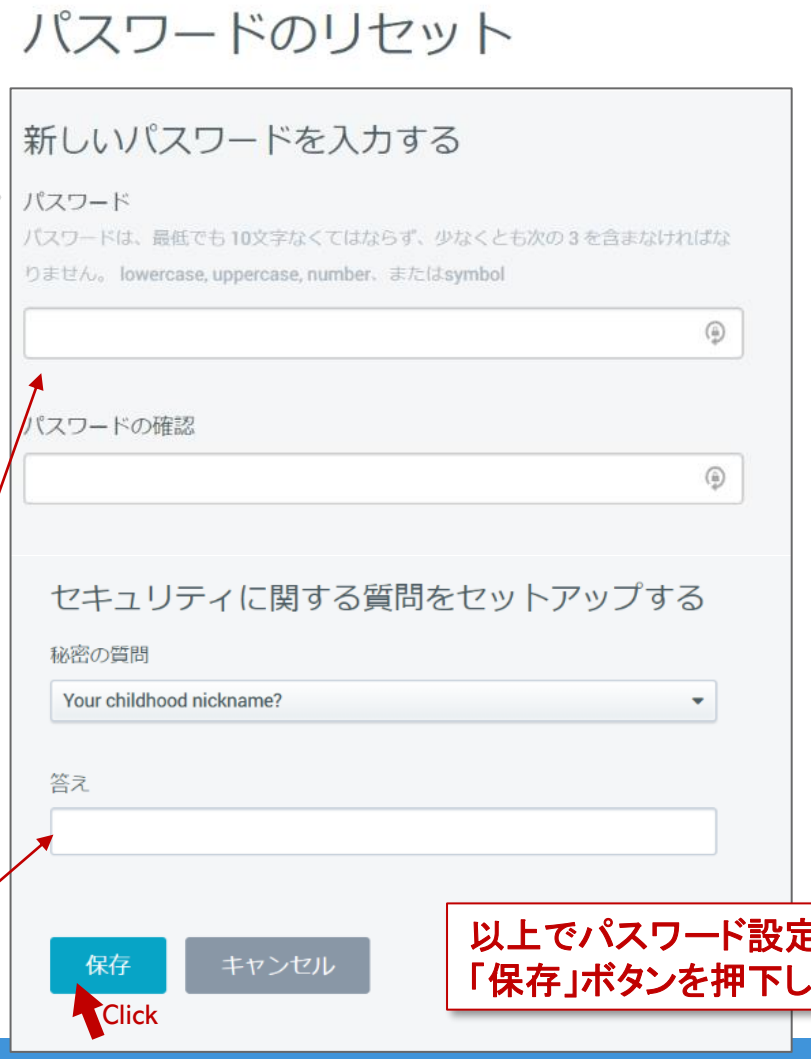
以上で追加申請は終わりです。
「ユーザーを追加」ボタンを押下してください。

ユーザー追加手順 (3/3 : 追加されるユーザー側のパスワード設定作業)

■パスワード設定案内メール（イメージ）

■メール件名
(英語の場合)DigiCert User Account Created - Action Required
■メール送信元
DigiCert <admin@digicert.com>
■メール本文に含まれるURLリンク
https://www.digicert.com/link/pass.php?<お客様特有のキー>

■パスワード設定画面



以上でパスワード設定は終わりです。
「保存」ボタンを押下してください。

■パスワード設定画面の入力項目の説明

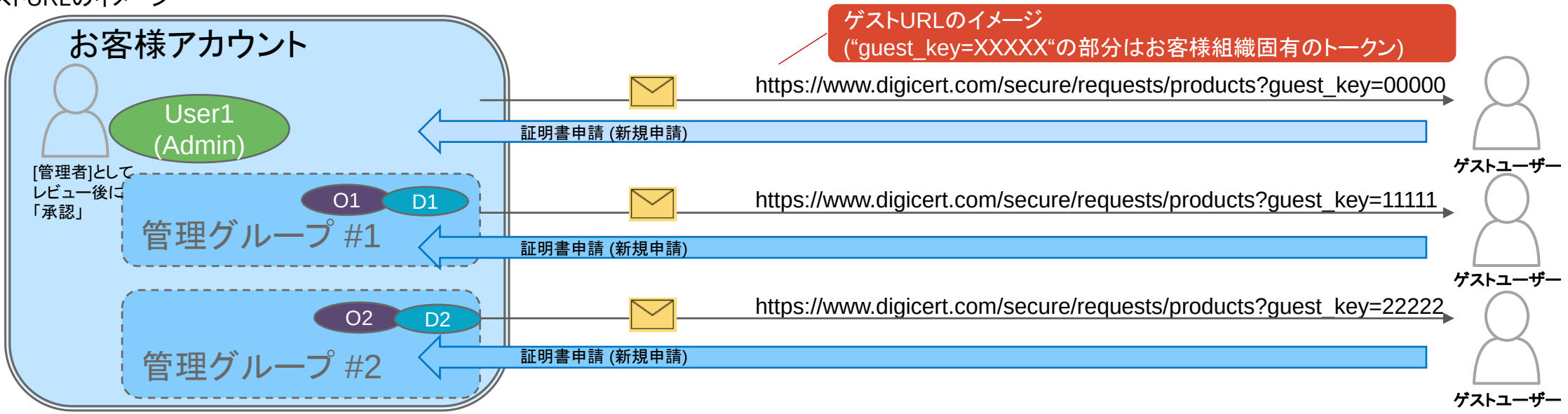
項目名	概要
パスワード	パスワードを入力します。 (10文字以上で、英小文字/英大文字/数字/記号から3種類以上を利用)
秘密の質問	■【必須】秘密の質問 プルダウンから一つの「秘密の質問(Security Question)」を選択し、下段の「セキュリティ回答(Security Answer)」欄に回答を入力してください。

9. アカウントアクセス管理

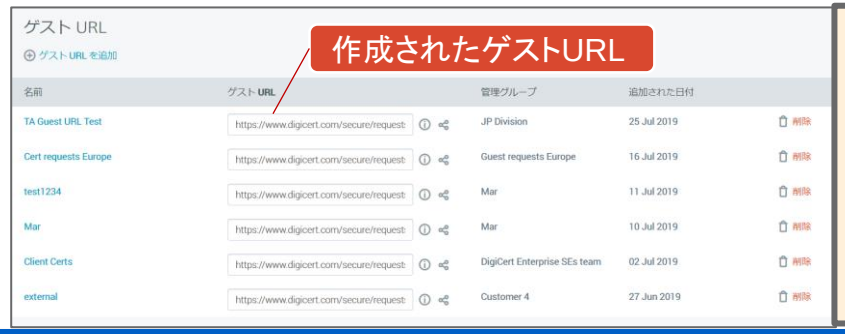
~ 9.1 ゲストURL ~

「ゲストURL」機能を用いることで、ユーザーアカウントを持っていない申請者が新しい証明書をリクエスト（新規申請）することが可能（発行にはアカウントユーザによる承認が必要）

■ゲストURLのイメージ



■(管理者向け)ゲストURL管理画面（イメージ）



各Guest URLには以下の属性を付与することが可能

- **管理グループ(Division)**
  - →証明書発行対象の組織(Org)、ドメイン(Domain)との紐づけ
  - →ライセンス(デポジットファンド)との紐づけ
- **(申請可能な)製品および証明書有効期間**
  - →各管理グループ(事業部門等に紐づく)ごとに異なる証明書製品の選択やライフサイクルへ対応

※ お客様組織内のゲストユーザー様向けに、ゲストURLを用いた申請マニュアルを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から「ゲストユーザー向けCertCentral申請マニュアル」をご参照ください。
https://www.digicert.co.jp/enterprise/certcentral/

（参考） 旧マネージドPKI for SSLの申請者ページ(Subscriber Pages)との比較(イメージ)

マネージドPKI for SSL

■（参考）マネージドPKI for SSLの申請者ページ(Subscriber Pages)トップページ

URL形式：https://certmanager.websecurity.digicert.com/mcelp/enroll/index?jur_hash=<固有のトークン値>

管理者によるレビュー・承認
→証明書発行、失効完了

CertCentral

■CertCentral ゲストユーザー向け機能

ゲストユーザー

【ゲストURL】

URL形式：https://www.digicert.com/secure/requests/products?guest_key=<固有のトークン値>

証明書
新規申請

当セクションで説明の内容
→(必要に応じて)新規申請用リンクとしてゲストユーザーへ配布

【ゲストアクセス】

URL形式：https://www.digicert.com/account/guest-access/?c=<固有のトークン値>

証明書
更新申請
／再発行
／失効など

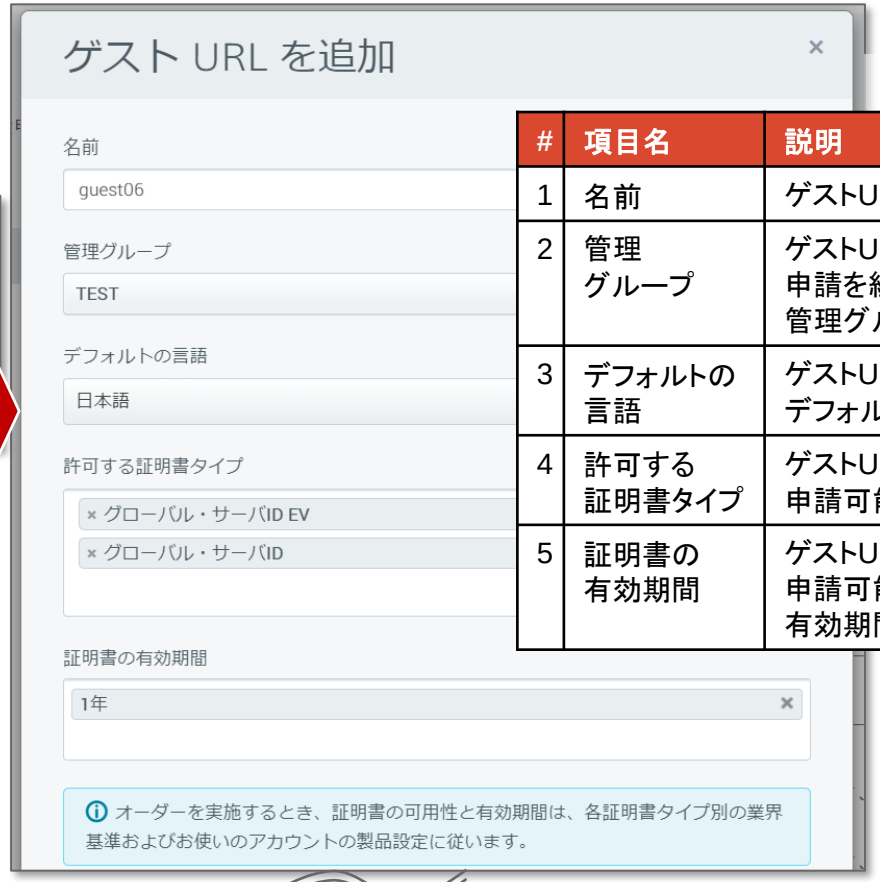
次セクションで説明の内容
→(必要に応じて)更新申請用リンクとしてゲストユーザーへ配布

管理者によるレビュー・承認
→証明書発行、失効完了

ゲストURL機能の管理 - ゲストURLの追加(作成) – 1/2

■「ゲストアクセス」メニュー(「アカウント」メニュー配下)

■「ゲストURLを追加」メニュー



(次のページに続きます)

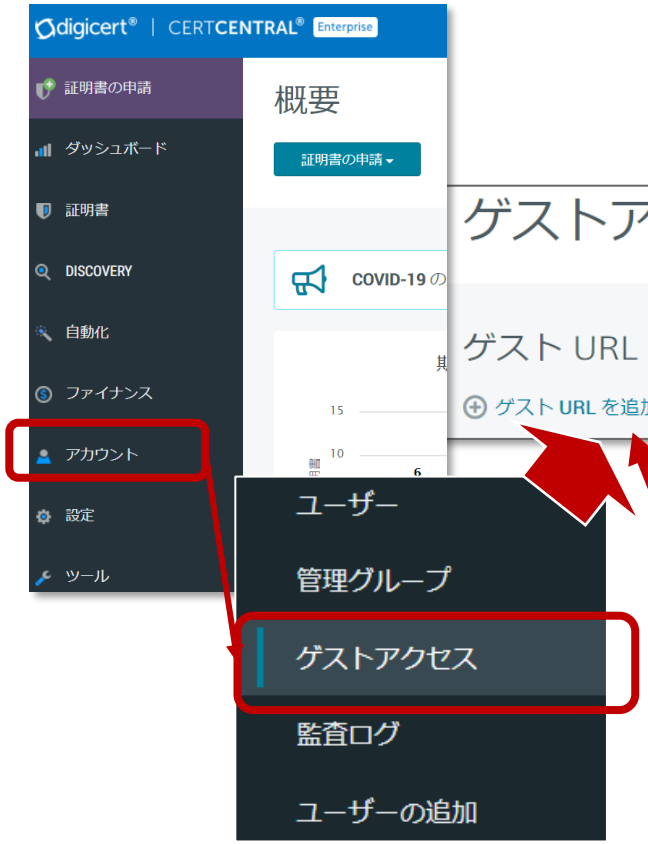
■ゲストURL追加(作成)時の入力/選択項目

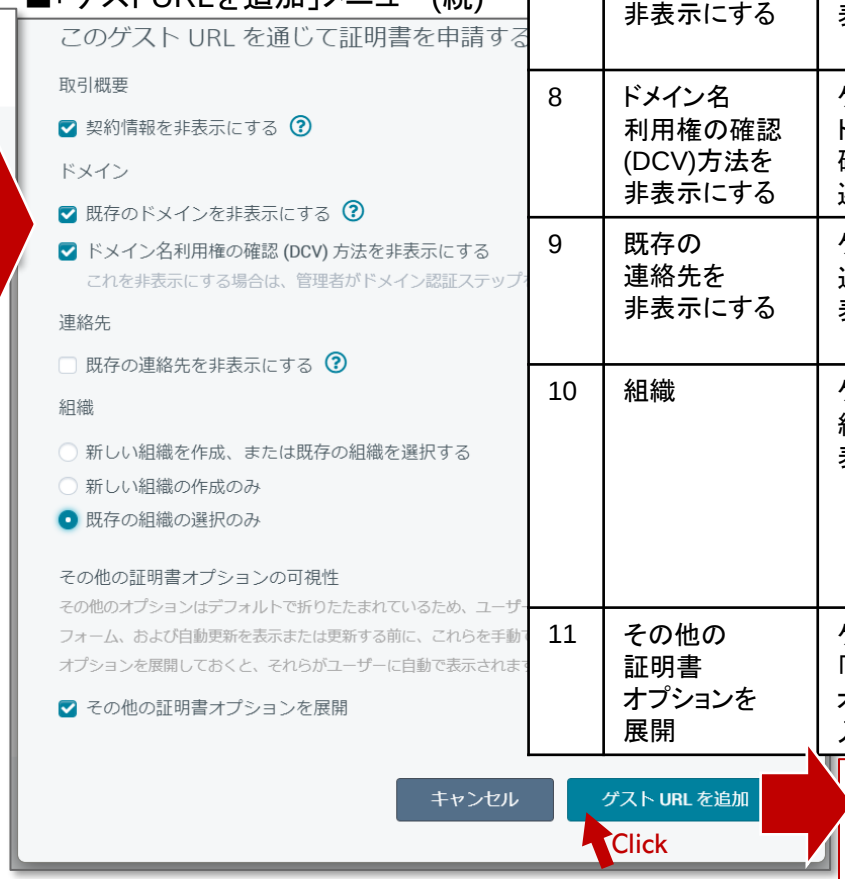
#	項目名	説明	入力/選択例
1	名前	ゲストURLの名称	例:「部署001用 ゲストURL」
2	管理 グループ	ゲストURLの 申請を紐づける 管理グループ	・一覧から選択 ・デフォルトではアカウント開設時に作成された (親となる)管理グループが選択された状態
3	デフォルトの 言語	ゲストURLにおける デフォルト表示言語	「日本語」
4	許可する 証明書タイプ	ゲストURLを用いて 申請可能な製品	例:「セキュア・サーバID」
5	証明書の 有効期間	ゲストURLを用いて 申請可能な証明書 有効期間	例:「1年」

(次のページに続きます)

ゲストURL機能の管理 - ゲストURLの追加(作成) – 2/2

■「ゲストアクセス」メニュー(「アカウント」メニュー配下)





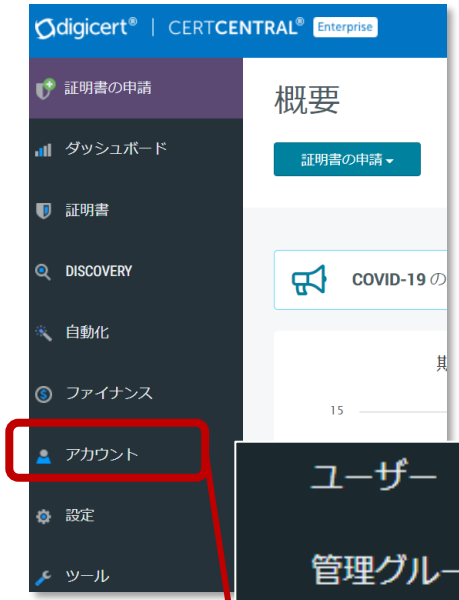
■(続き)ゲストURL追加(作成)時の入力/選択項目

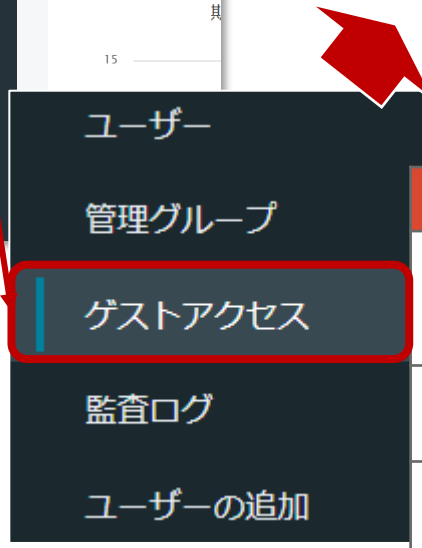
#	項目名	説明	入力/選択例
6	契約情報を 非表示にする	ゲストURLにおける 取引概要欄の 表示設定	チェックボックス**ON**:**【推奨】** 取引概要欄を隠す(表示しない) チェックボックス**OFF**: 取引概要を隠さない(表示する)
7	既存の ドメインを 非表示にする	ゲストURLにおける 登録済ドメイン名の 表示設定	チェックボックス**ON**:**【推奨】** 登録済ドメイン名を隠す(表示しない) チェックボックス**OFF**: 登録済ドメイン名を隠さない(表示する)
8	ドメイン名 利用権の確認 (DCV)方法を 非表示にする	ゲストURLにおける ドメイン名利用権 確認(DCV)方法 選択欄の表示設定	チェックボックス**ON**:**【推奨】** DCV方法選択欄を隠す(表示しない) チェックボックス**OFF**: DCV方法選択欄を隠さない(表示する)
9	既存の 連絡先を 非表示にする	ゲストURLにおける 連絡先(担当者情報) 表示設定	チェックボックス**ON**:**【推奨】** 連絡先(担当者情報)を隠す(表示しない) チェックボックス**OFF**: 連絡先(担当者情報)を隠さない(表示する)
10	組織	ゲストURLにおける 組織情報の 表示/登録設定	・**新しい組織を作成、または既存の組織を選択**: 申請時に組織追加登録を選択可能にする ・**新しい組織の作成のみ**: 申請時に常に組織を追加登録させる ・**既存の組織の選択のみ**:**【推奨】** 申請者に組織の追加登録を許可しない (登録済の組織のみを使用させる)
11	その他の 証明書 オプションを 展開	ゲストURLにおける 「その他の証明書 オプション」表示・ 入力設定	チェックボックス**ON**: 「その他の証明書オプション」を予め展開する チェックボックス**OFF**: 「その他の証明書オプション」を予め展開しない

「ゲストURLを追加」を押下します。
次ページへ進んでください

ゲストURL機能の管理 - ゲストURLの編集、削除

■「アカウントアクセス」メニュー（「アカウント」メニュー配下）





■ゲストURL一覧と各機能説明

	機能	説明
①	ゲストURLを参照・共有する	ゲストURLの全体を表示します。また指定した宛先にゲストURLを電子メールで送付します。
②	ゲストURLのプロパティを参照する	「製品」「有効期間」などのゲストURLのプロパティを参照します。
③	ゲストURLのプロパティを編集する	「製品」「有効期間」などのゲストURLのプロパティを編集します。
④	ゲストURLを削除する	ゲストURLを削除します。削除したゲストURLは利用できなくなります。

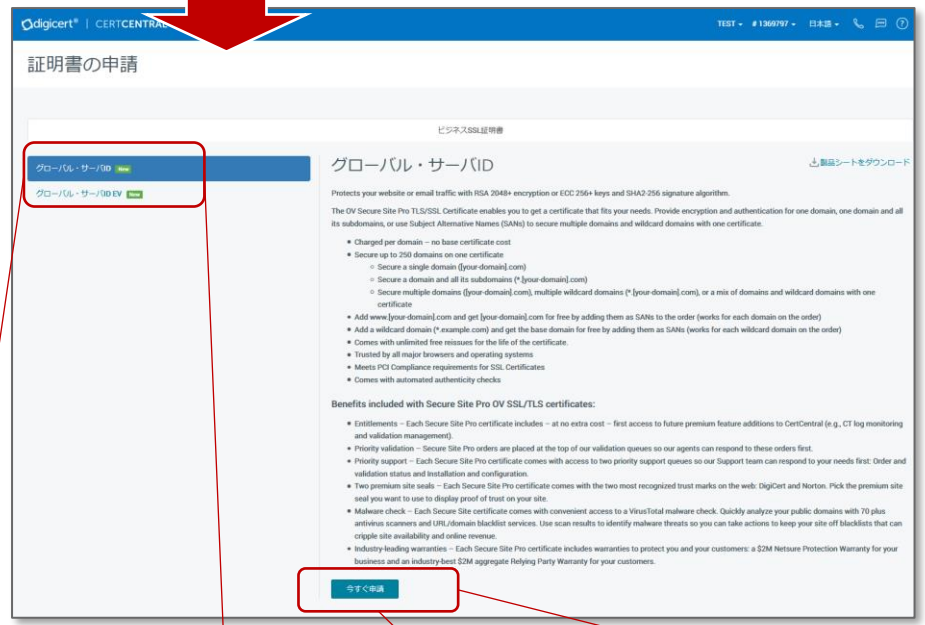
■ゲストURL参照・共有(①)

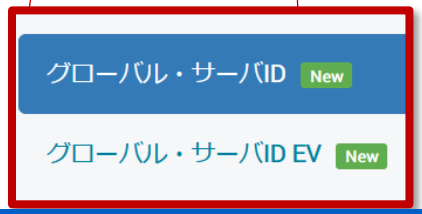
(ゲストユーザー向け) ゲストURLを用いた証明書申請のイメージ

■ゲストURLへのアクセス後の製品選択画面(※1)

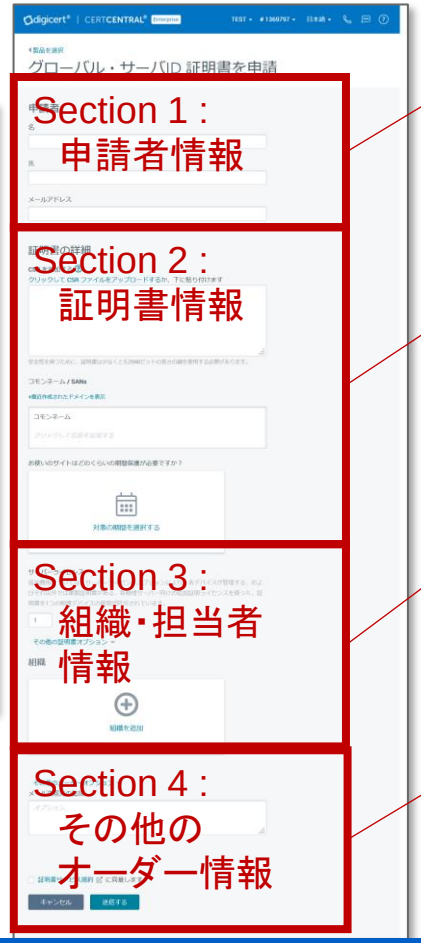
ゲストユーザー

作成されたゲストURL





■左記画面で製品選択後に「今すぐ申請」を押下して開かれる証明書申請画面(※1)



Section 1 : 以下のような「申請者情報」を入力します。
- 申請者氏名
- 申請者のメールアドレス

ゲストURL独自の入力項目

Section 2 : 次に以下のような「証明書情報」を入力します。
- CSR
- コモンネーム／SANs
- プラン(ご契約期間)／証明書有効期間の選択
- ドメイン名利用権確認(DCV)の方式指定(※2)
- その他の証明書オプション

CertCentralの新規申請時と同様

Section 3 : 次に以下のような「組織・担当者情報」を入力します。
- 申請団体の組織情報
- 申請責任者／技術担当者(※2)

CertCentralの新規申請時と同様

Section 4 : 最後に以下のようなその他のオーダー情報を入力し、利用規約を確認いただきます
- その他のオーダーオプション
- (管理者による指定)カスタムオーダーフィールド(※2)
- 証明書サービス利用規約の確認

CertCentralの新規申請時と同様

※ お客様組織内のゲストユーザー様向けに、ゲストURLを用いた申請マニュアルを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から「**ゲストユーザー向けCertCentral申請マニュアル**」をご参照ください。
https://www.digicert.co.jp/enterprise/certcentral/

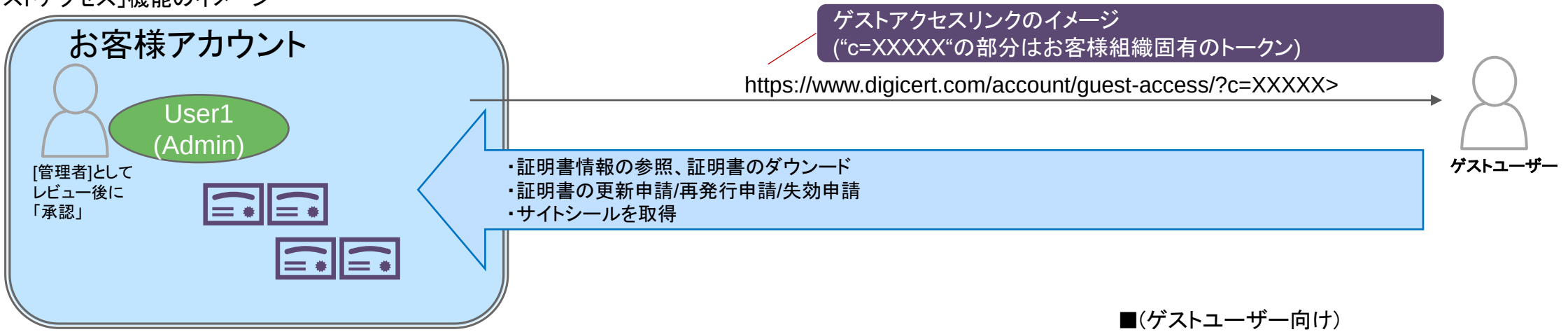
※1 : 管理者によって「Default language」に「日本語」を選択した場合のイメージ
※2 : ゲストURLの証明書申請画面では、組織の管理者の設定によって表示が省略されたり、追加で入力が必須となる項目があります。

9. アカウントアクセス管理

~ 9.2 ゲストアクセス ~

「ゲストアクセス」機能を用いることで、ユーザーアカウントを持っていない申請者が発行済の証明書を更新、再発行または失効することが可能（発行にはアカウントユーザによる承認が必要）

■「ゲストアクセス」機能のイメージ



■(管理者向け)ゲストアクセス管理画面(イメージ)

■(ゲストユーザー向け)
オーダー詳細画面および証明書操作メニュー(イメージ)

※ お客様組織内のゲストユーザー様向けに、ゲストアクセス機能を用いた申請マニュアルを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から「**ゲストユーザー向けCertCentral申請マニュアル**」をご参照ください。
https://www.digicert.co.jp/enterprise/certcentral/

（参考） 旧マネージドPKI for SSLの申請者ページ(Subscriber Pages)との比較(イメージ)

マネージドPKI for SSL

■（参考）マネージドPKI for SSLの申請者ページ(Subscriber Pages)トップページ

URL形式：https://certmanager.websecurity.digicert.com/mcelp/enroll/index?jur_hash=<固有のトークン値>

管理者によるレビュー・承認
→証明書発行、失効完了

CertCentral

■CertCentral ゲストユーザー向け機能

ゲストユーザー

証明書
新規申請

【ゲストURL】

URL形式：https://www.digicert.com/secure/requests/products?guest_key=<固有のトークン値>

前セクションで説明の内容
→(必要に応じて)新規申請用リンクとしてゲストユーザーへ配布

証明書
更新申請
／再発行
／失効など

【ゲストアクセス】

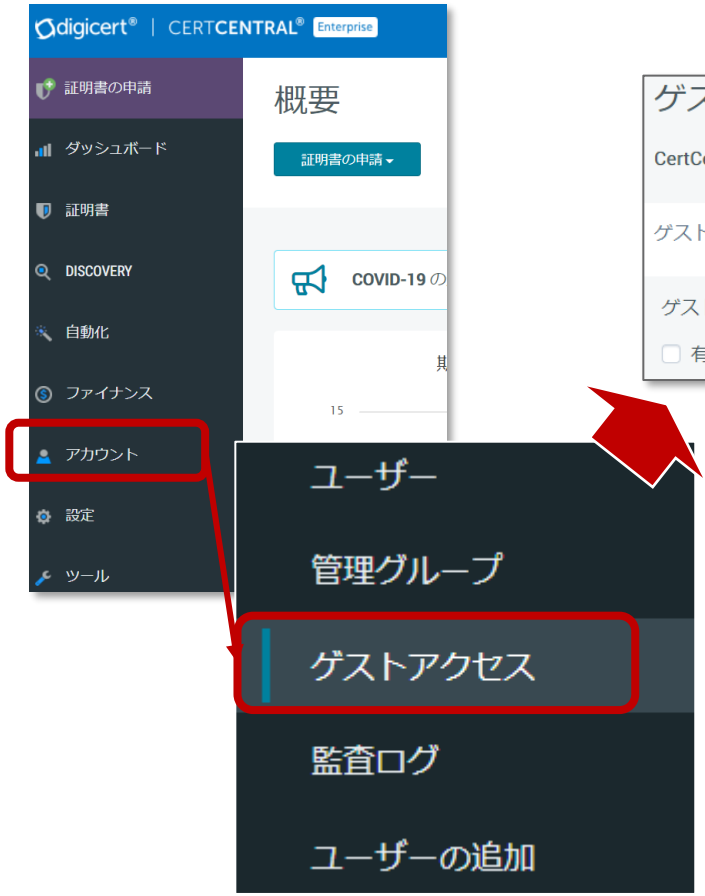
URL形式：https://www.digicert.com/account/guest-access/?c=<固有のトークン値>

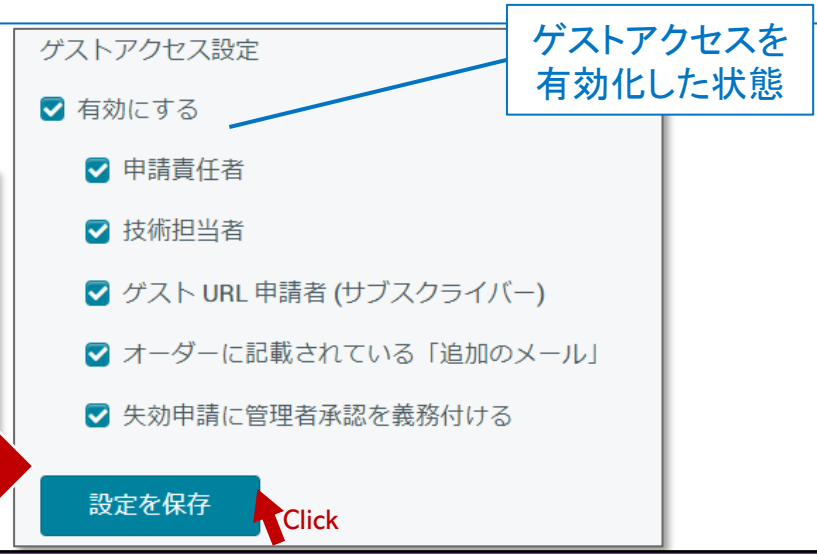
当セクションで説明の内容
→(必要に応じて)更新申請用リンクとしてゲストユーザーへ配布

管理者によるレビュー・承認
→証明書発行、失効完了

ゲストアクセスをアカウント単位で有効化／無効化する

■「ゲストアクセス」メニュー（「アカウント」メニュー配下）





■ゲストアクセスに関する設定項目

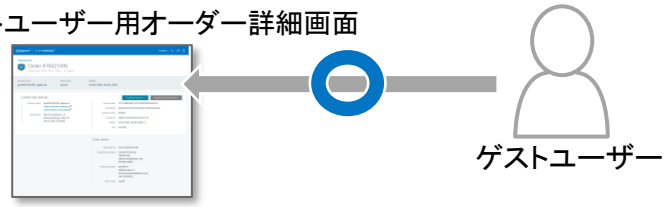
#	項目名	説明
1	有効にする	ゲストアクセスリンクを有効化し、ゲストユーザーに対してゲストアクセスリンクによるオーダー情報へのアクセスを許可する。 (初期状態では**全てのオーダー**に対してゲストアクセスが**許可された状態**になる (オーダー単位でゲストアクセスを無効化(次ページ参照)された場合を除く))
2	申請責任者	オーダーの申請責任者(Organization Contact)にアクセスを許可する
3	技術担当者	オーダーの技術担当者(Technical Contact)にアクセスを許可する
4	ゲストURL申請者(Subscriber)	ゲストURL/ゲストアクセスのオーダーの申請者(Subscriber)にアクセスを許可する
5	オーダーの「追加のメール」	オーダーの追加メールアドレス(Additional Emails)所有者にアクセスを許可する
6	失効申請に管理者承認を義務づける	ゲストアクセスリンクからの失効リクエストについて管理者の承認を必須とする 【ゲストアクセスリンクを有効とする場合、チェックボックスONを推奨】

ゲストアクセスをオーダー単位での有効化／無効化する

■オーダー詳細画面(証明書発行後かつアカウント単位でゲストアクセス有効化された状態)

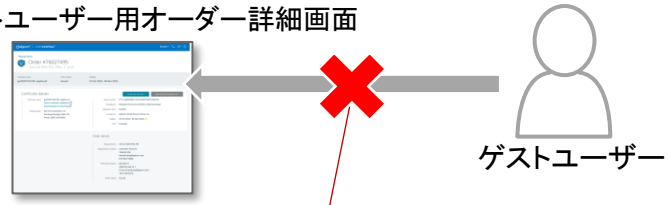
■このオーダーに対してゲストアクセスが「有効化」された状態

■ゲストユーザー用オーダー詳細画面

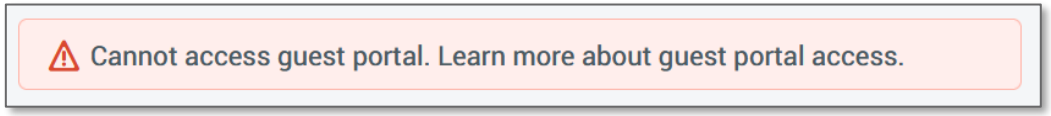


■このオーダーに対するゲストアクセスが「無効」である状態

■ゲストユーザー用オーダー詳細画面



管理者(Administrator権限を持つCertCentralユーザー)によって該当のオーダーに対するゲストアクセスが有効化されていない場合、ゲストアクセスリンク利用時、ゲストユーザーに対して下図のようなエラーメッセージが表示されます。



(ゲストユーザー向け) ゲストアクセスリンクを用いた証明書オーダー情報へのアクセス(イメージ)

【ゲストアクセスリンク】

ゲストユーザー

ゲストユーザーの**電子メールアドレス**、ならびに**【検索キー】**として**オーダーID**または**コモンネーム/SANs**を入力

ゲストアクセス用
認証コード通知メール

認証コード確認画面

ゲストアクセスリンクの入力画面にて指定した【検索キー】は？

検索キーとして
コモンネーム/SANsを
指定した場合

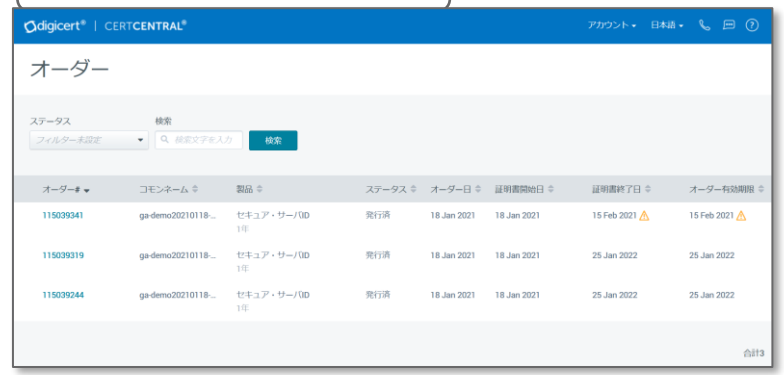
コモンネーム/SANの合致件数は？

2件以上
合致

1件のみ
合致

検索キーとして
オーダー番号を指定した場合

オーダー選択画面



複数の候補が存在する場合、上図のような候補一覧が表示されます。製品種類や有効期間等から対象のオーダーを特定し、選択(オーダー番号をクリック)してください。

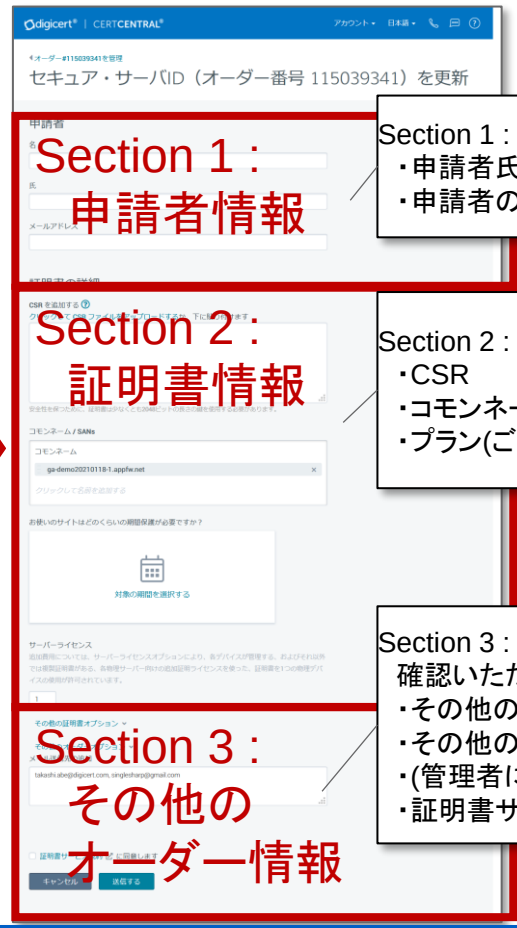
オーダー詳細画面

※ お客様組織内のゲストユーザー様向けに、ゲストアクセス機能を用いた申請マニュアルを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から**「ゲストユーザー向けCertCentral申請マニュアル」**をご参照ください。
https://www.digicert.co.jp/enterprise/certcentral/

(ゲストユーザー向け) ゲストアクセスリンクを用いた更新申請(イメージ)

■ゲストユーザー用オーダー詳細画面

■更新申請画面



Section 1：以下のような「申請者情報」を入力します。
・申請者氏名
・申請者のメールアドレス

Section 2：以下のような「証明書情報」を入力します。
・CSR
・コモンネーム／SANs
・プラン(ご契約期間)／証明書有効期間の選択

Section 3：最後にその他の情報を入力、利用規約を確認いただきます。
・その他の証明書オプション
・その他のオーダーオプション
・(管理者による指定)カスタムオーダーフィールド
・証明書サービス利用規約の確認

※ お客様組織内のゲストユーザー様向けに、ゲストアクセス機能を用いた申請マニュアルを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から「**ゲストユーザー向けCertCentral申請マニュアル**」をご参照ください。
https://www.digicert.co.jp/enterprise/certcentral/

【ゲストアクセス】機能について – よくあるご質問 -

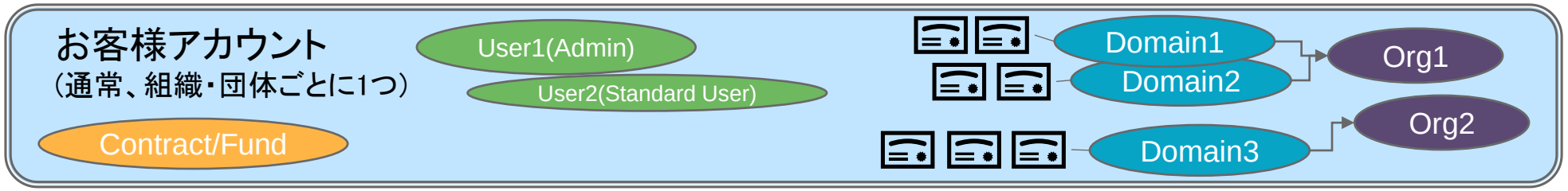
Q (ご質問)	A (回答)
・管理者(AdministratorまたはManager権限を持つCertCentralユーザー)は、ゲストユーザーによる更新申請/再発行申請/失効申請をレビュー・承認する必要がありますか？ ・管理者の意図しない申請や、失効が行われることが懸念されますが、大丈夫ですか？	・ゲストアクセス機能によるゲストユーザーの各種申請は、常に管理者によってレビュー・承認される必要があります。 ・管理者によるレビュー・承認なしに証明書が発行されたり、失効されることはありません。
・ゲストアクセスリンクを有効化すると、証明書オーダー情報に誰でもアクセスできてしまうのですか？ ・何故認証コードが必要なのですか？	・ゲストアクセスでは証明書オーダー情報の確認や証明書申請だけでなく、再発行申請や失効申請を行うことが可能です。意図しない証明書の失効はウェブサーバへの通信ができなくなるなどのインシデントにつながる恐れがあります。 ・CertCentralのゲストアクセス機能では、メールアドレスと認証コードを用いた確認プロセスによって、管理者のポリシーによって許可されたゲストユーザーのみが証明書オーダー情報へのアクセス、各種申請が出来るようにしています。
・昨年の証明書の担当者(ゲストユーザー)が変更となりました。証明書オーダーの[追加メールアドレス(Additional Email)]には昨年の担当者のメールアドレスが付与されています。このままでは新しい担当者(ゲストユーザー)が証明書オーダー情報にアクセスして更新申請することができません。どのようにすればよいですか？	・管理者様にオーダーの[追加メールアドレス(Additional Email)]フィールドを更新いただくことを推奨します。更新対象の証明書オーダーに対して、新しい担当者のメールアドレスを[追加メールアドレス]に上書きいただくことが可能です。これにより新しい担当者がゲストアクセス機能より該当の証明書オーダーにアクセスして、更新申請を行っていただくことが可能になります。
・組織内の申請者が多数であるため管理負荷が高まることが懸念されます。どのようにすればよいでしょう？	以下の複数の対応策の一つまたは複数を組み合わせるなどご検討いただければ幸いです。 案1：申請者は必要に応じてオフラインで管理者にアクセス許可を求め、管理者が[追加メールアドレス]を適宜設定することによって、アクセスを許可するプロセスを含めた運用をご検討いただく 案2：申請者にCertCentralのユーザーアカウントを[権限=Standard User/Limited User]でご取得いただく 案3：申請者は必要に応じてオフラインで管理者に証明書取得を依頼し、CertCentralの管理者(または別のユーザー)がCertCentralにログインをして証明書を取得いただく

9. アカウントアクセス管理

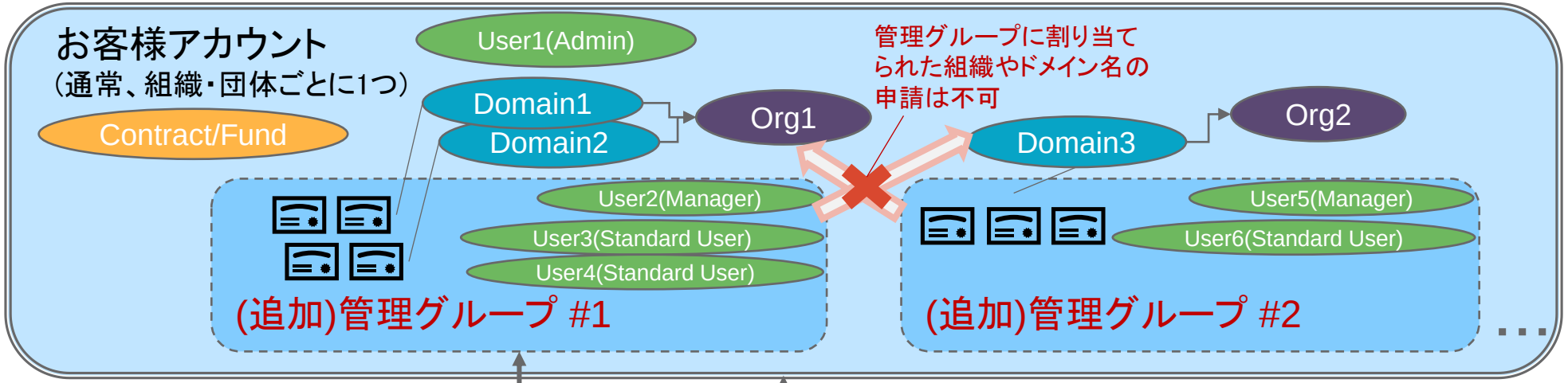
~ 9.3 管理グループ ~

CertCentralの「管理グループ(Division)」機能を活用いただくことで、例えば事業部門ごとに証明書を申請可能な「ユーザー」や「ドメイン名」を制限するなど、緻密な管理が可能です

アカウント開設直後の状態
(追加の管理グループを登録していない状態)



追加の管理グループを活用する場合のイメージ



■管理グループの属性として指定可能
- 管理グループで証明書管理が可能なユーザー
- 管理グループで証明書申請可能な組織(Org)
- 管理グループで証明書申請可能なドメイン名(Domain)

■アカウント設定で管理グループごとに以下「割り当て」が可能
- ユーザー(全Div、単一Divまたは複数Divにアサイン可能)
- 利用可能な製品種類および有効期間(1年/2年など)
- デポジット残高(Fund)
- ゲストURL

管理グループの管理 (1/2 管理グループの追加)

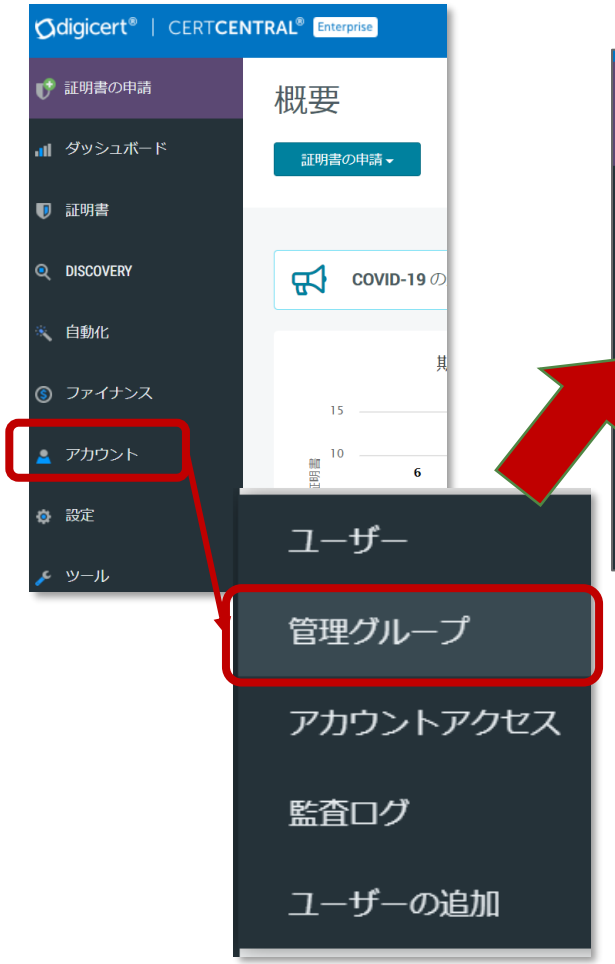
■「アカウントアクセス」メニュー（「アカウント」メニュー配下）

■管理グループ追加(作成)時の入力/選択項目

#	項目名	説明	入力/選択例
1	名前	管理グループの名前	「管理グループ001」
2	説明	管理グループの説明	「部署001用の管理グループ」（任意の文字列）
3	更新申請通知の送付先	管理グループ固有の更新案内メール送信先	「renewal-digicert@example.com」
4	この管理グループに限定されているユーザー	操作可能な範囲を該当の管理グループに限定するユーザー	＜アカウントに登録されたユーザーアカウントのリストから選択＞
5	自動更新ユーザー	「自動更新」機能利用時のデフォルト申請者	（推奨：未指定状態としてください）
6	証明書申請が可能な対象（組織）	該当管理グループで扱う登録済の組織を限定する場合に指定	・「すべての組織」「特定の組織」から選択 ・「特定の組織」選択時は登録済の組織のリストから対象を指定
7	証明書申請が可能な対象（ドメイン）	該当管理グループで扱う登録済のドメイン名を限定する場合に指定	・「すべてのドメイン」「特定のドメイン」から選択 ・「特定のドメイン名」選択時は登録済のドメイン名のリストから対象組織を登録

管理グループの管理 (2/2 管理グループの編集・削除)

■「アカウントアクセス」メニュー（「アカウント」メニュー配下）



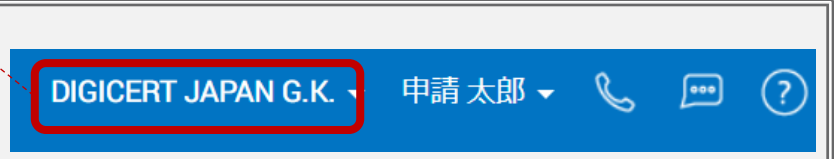
■管理グループ一覧と各機能説明

	項目	説明
[A]	無効な管理グループ	無効化された管理グループを表示
[B]	自身の管理グループ	操作ユーザー自身が所属する管理グループを表示

	項目	説明	備考
①	(親となる) 管理グループ	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(*1)	画面上の管理グループ名をクリックすると管理グループに対して以下の編集(抜粋)が可能です。 ・管理グループ名の変更(*1) ・管理グループの無効化/有効化 ・(前ページ手順で設定した)各種設定項目の変更
②	(追加) 管理グループ	前ページ手順で追加した「(追加)管理グループ」	

TIPS

*1 : CertCentralの画面右上部の組織名称は「(親となる)管理グループ」の名称が表示されます。この値を変更したい場合は、同メニューから「(親となる)管理グループ」の名称を変更してください。



ユーザーの権限をさらに緻密に管理する場合 ～ユーザーを特定の管理グループへアサイン～

■CertCentralのユーザー権限 (特定の管理グループにアサインされたユーザーアカウント)

機能／操作 (*1)	Administrator	Finance Manager	Manager	Standard User	Limited User
・証明書申請 (新規/更新、再発行、失効などのリクエスト) ・申請履歴の参照(自己の申請分)	● （自身が属する管理グループの分のみ、以下同じ）	●	●	●	●
・申請履歴の参照(他ユーザの申請分を含む)	●	●	●	●	
・証明書申請の承認、却下 (*2) ・Discoveryダッシュボードの参照(証明書、エンドポイント脆弱性) ・Discovery管理(センサーの配置、スキャンの実行など) ・ユーザアカウント管理(追加(Adminのみ)、編集、削除) ~~・ドメイン名管理(追加、認証リクエスト)~~ ~~・監査ログの参照、監査ログイベント通知の管理~~	●		● （ユーザ追加除く）		
・アカウント価格/コントラクト、残高履歴、支出レポート等の確認 ・デポジットファンド、クレジットカードの管理	●	●	●		
~~・組織(Organization)管理(追加、変更)~~ ・管理グループ(Division)管理(組織/ドメインのアサイン不可など、一部制限あり) ・セキュリティ設定(IPアドレス制限は不可、SSO設定は可など、一部制限あり) ・製品設定(管理グループ、権限ごとに申請可能な製品を制限可) ・APIキー管理(一覧参照、他ユーザへの発行、削除)	●				

*1 : 画面操作およびAPI操作に共通。尚、自らのユーザアカウントに対するAPIキーの発行は権限に関わらず可能
*2 : 一部製品(EV SSL証明書、コードサイニング証明書)の承認には、上述の権限に加えて追加権限(Subrole)の設定が必要
もっと詳しく(英語資料) : https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/

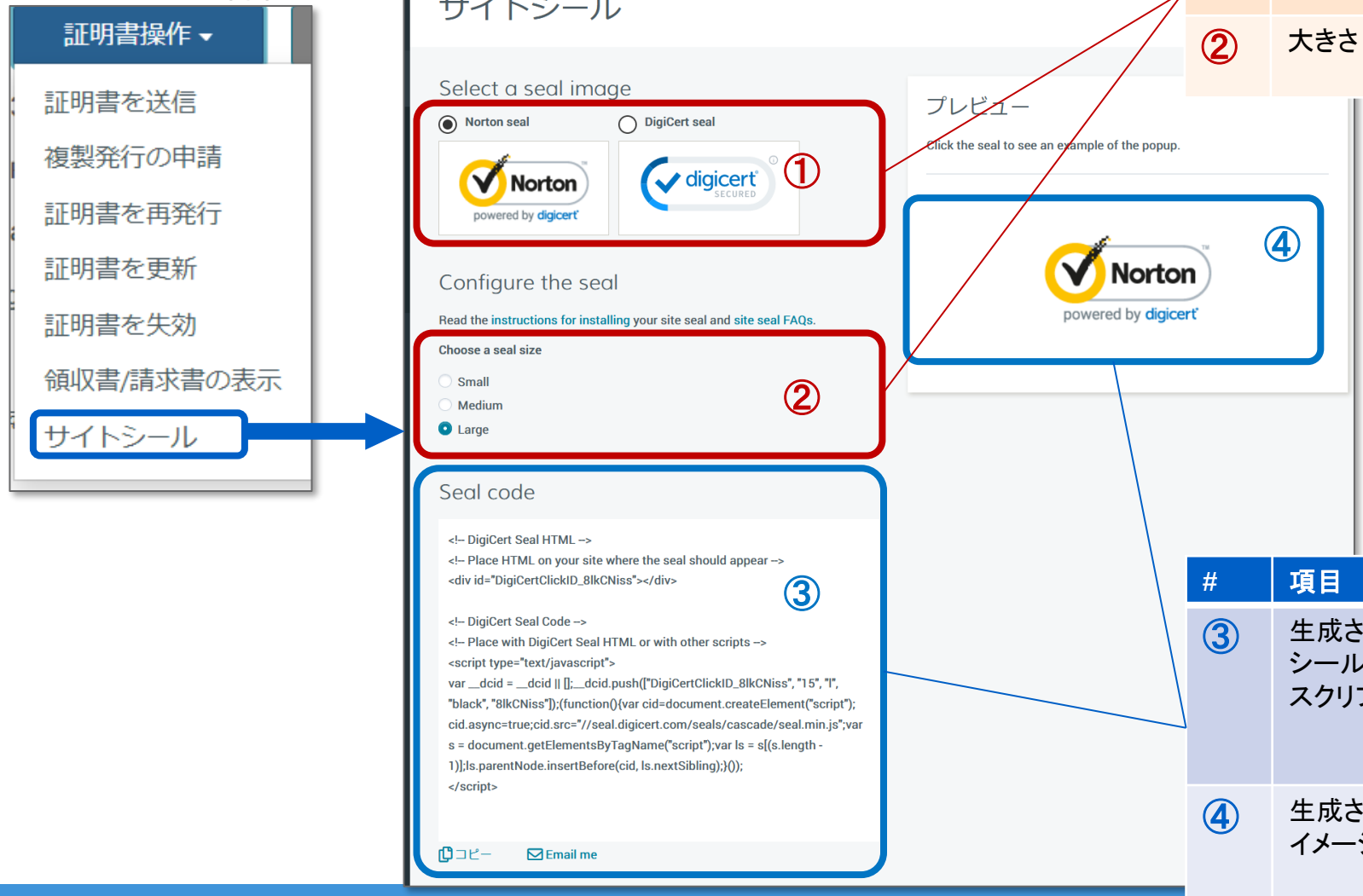
10. 証明書製品のその他の機能

~ 10.1 サイトシール ~

「サイトシール」ページ

■対象製品
・セキュア・サーバID
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■「証明書操作」メニュー
（例：オーダー詳細画面）



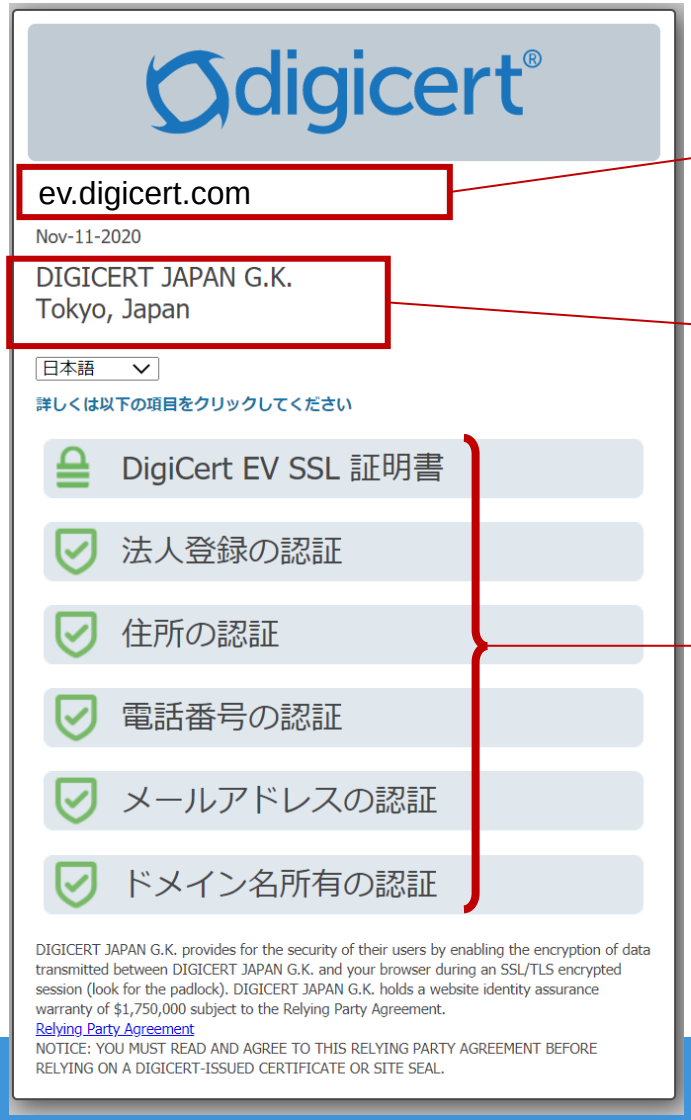
#	項目	内容
①	デザイン	表示されている選択肢から、ご希望のシールのデザインを選択してください。
②	大きさ	以下の選択肢から最適なシールの大きさを選択してください small : 小 ／ standard : 中 ／ large : 大

#	項目	内容
③	生成されたシールスクリプト	①、②の指定に基づいてシールスクリプト(HTML/JavaScriptコード)が生成されます。 生成したスクリプトをメールで送信することも可能です。 インストラクション(※1)に従ってお客様のウェブページに掲載してください。
④	生成されたイメージ	①、②の指定に基づいてシールイメージが生成されます。 またクリックいただくとサンプルのスプラッシュページをご確認いただけます。

※1 シール掲載方法(当資料作成時点では英語のみ)：https://www.digicert.com/kb/ssl-support/site-seal-installation.htm

スプラッシュページのデザイン（イメージ）

■(**EV証明書の場合**)サイトシール
スプラッシュページ(イメージ)



FQDN

組織情報

表明事項
(認証項目)
の説明

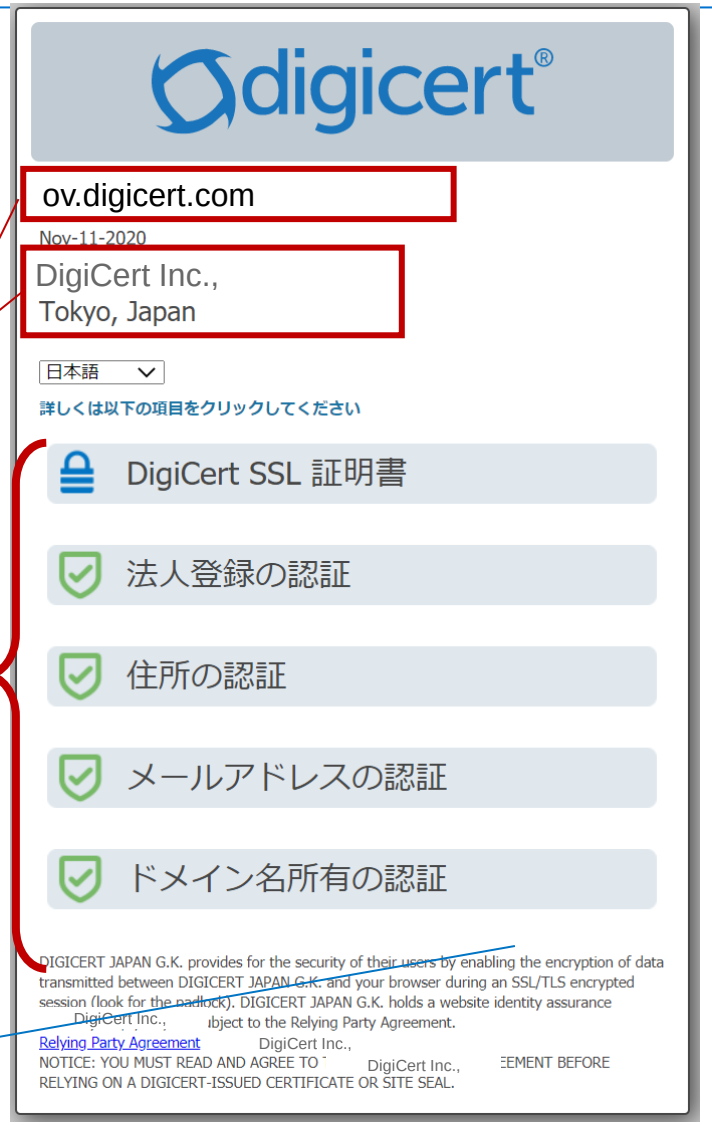
■(**OV証明書の場合**)サイトシール
スプラッシュページ(イメージ)

（参考）旧スプラッシュページとの比較

Norton powered by digicert™ Click

■(参考) 旧スプラッシュページ

■CertCentral版
サイトシール
(**OV証明書の場合**)
スプラッシュページ
(イメージ)



組織情報

FQDN

表明事項
(認証項目)
の説明

各項目(灰色のタイトル部分)を
クリックいただくことで表明事項
(認証項目)をご確認いただけます

「サイトシール」に関するQ&A

#	カテゴリ	Q	A
1	概要	旧シールスクリプト(例えば旧シマンテック社のウェブサイトで生成したシールスクリプト)はいつまで利用することが可能ですか？ (以下イメージ参照)	旧シールスクリプトを利用したシールを継続してご利用いただける期限は、CertCentral移行前の旧プラットフォームで該当のウェブサイト(FQDN)に対して発行した証明書の有効期限、または2021年4月23日の早い方までとなります。 **[CertCentral] シールスクリプトの変更について** https://knowledge.digicert.com/ja/jp/solution/SOT0013.html 期限を迎えると旧スクリプトは無効となり、シールは表示されなくなります。 継続してサイトシールをご利用いただくためにはCertCentralで該当のウェブサイトに対する証明書を申請・発行いただいた後に、シールスクリプトを生成いただき、お客様のウェブページ上のスクリプトを更新していただけますようお願いいたします。
2	インストール	CertCentralで生成したシールスクリプトのインストール方法を詳しく教えてください。	以下のインストラクションをご活用ください。 **[CertCentral] サイトシールのインストール** https://knowledge.digicert.com/ja/jp/solution/SOT0001.html
3	概要	CertCentralでは証明書を更新する都度、シールスクリプトを生成してウェブページに貼りなおさなければならないのですか？	CertCentralで発行した証明書に対して一度生成したシールスクリプト(HTML/JavaScriptコード)は、該当のオーダーを更新いただいた場合は、同一のシールスクリプトを更新後も継続して利用いただくことが可能です。 何らかの理由で「新規申請」扱いで証明書を取得された場合は、同一FQDN上のウェブサイトであっても、以前のシールスクリプトを使いまわすことはできませんのでご注意ください。

■(参考) 旧シールスクリプトのイメージ (※1)

```
<table width="135" border="0" cellpadding="2" cellspacing="0" title="クリックして確認 - このサイトでは、安全な e コマースと機密性の高い通信のためにデジサートの SSL サーバ証明書を選択しています。"><tr><td width="135" align="center" valign="top"><script type="text/javascript" src="https://seal.websecurity.norton.com/getseal?host_name=www.digicert.com&amp;size=M&amp;use_flash=NO&amp;use_transparent=No&amp;lang=ja"></script><br /><a href="https://www.websecurity.digicert.com/ja/jp/security-topics/what-is-ssl-tls-https" target="_blank"  style="color:#000000; text-decoration:none; font:bold 10px verdana,sans-serif; letter-spacing:.5px;text-align:center; margin:0px; padding:0px;">SSL/TLS サーバ証明書とは</a></td></tr></table>
```

※1：旧シールスクリプトの生成ページ：https://www.websecurity.digicert.com/ja/jp/install-norton-seal

■新シールスクリプトのイメージ

Seal code

```
<!-- DigiCert Seal HTML -->
<!-- Place HTML on your site where the seal should appear -->
<div id="DigiCertClickID_TSDO9sC1"></div>

<!-- DigiCert Seal Code -->
<!-- Place with DigiCert Seal HTML or with other scripts -->
<script type="text/javascript">
var __dcid = __dcid || [];__dcid.push(["DigiCertClickID_TSDO9sC1", "15", "l", "black", "TSDO9sC1"]);(function(){var cid=document.createElement("script");cid.async=true;cid.src="//seal.digicert.com/seals/cascade/seal.min.js";var s = document.getElementsByTagName("script");var ls = s[(s.length - 1)];ls.parentNode.insertBefore(cid, ls.nextSibling);}());
</script>
```

10.その他の証明書製品機能

~ 10.2 マルウェアスキャン ~

マルウェアスキャン結果を確認する

■対象製品
・セキュア・サーバID
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■オーダー詳細画面（製品：セキュア・サーバID、ステータス：発行後）

CertCentralの
外部へリンク

■スキャン結果確認画面(VirusTotal.com社のウェブサイトへ移動して確認)

■VirusTotal.comとは？
・対象ドメイン（ウェブサイト）がマルウェア（悪意のあるソフトウェアやコード）等によって侵害されている可能性があるサイトとみなされているかどうかを判定し報告するサービスを提供する、デジサートのテクノロジーパートナー。
・判定には70以上のウェブスキャナ、アンチウィルスベンダおよびユーザコミュニティ、ならびにファイルやURLの分析ツールから収集されたデータを活用
・既知の悪意あるシグネチャだけでなく最新の脅威への識別を含め幅広く網羅
→対象ドメイン（ウェブサイト）に対する客観的で偏りのない判定を得ることが可能

※1：マルウェアスキャン機能の活用方法についてもっと詳しく:
https://docs.digicert.com/ja/manage-certificates/access-your-secure-site-certificate-benefits/access-secure-site-malware-check/

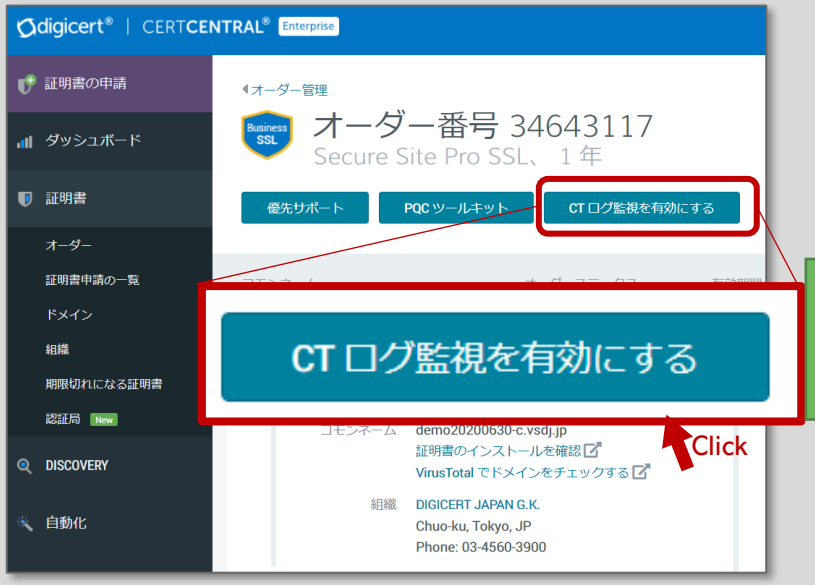
10.その他の証明書製品機能

~ 10.3 CTログモニタリング ~

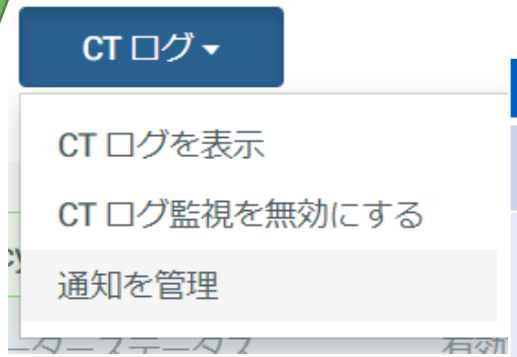
CTログモニタリング機能の有効化

■対象製品
・グローバル・サーバID
・グローバル・サーバID EV

■初期状態
（CTログモニタリングが
有効化されていない）



■CTログモニタリングが
有効化された状態



メニュー	説明
CTログを表示	証明書をメールで送信 (※1)
CTログ監視を無効にする	CTログモニタリング機能を無効化
通知を管理	CTログ登録を発見した際の通知を管理 (※1)

※1：CTログモニタリングの活用方法についてもっと詳しく：https://docs.digicert.com/ja/certificate-tools/ct-log-monitoring-service/

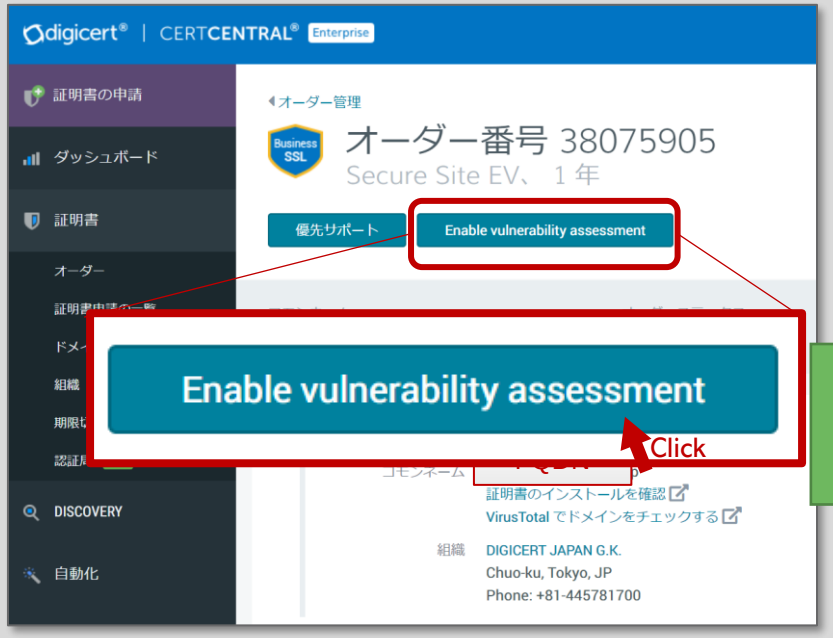
10.その他の証明書製品機能

~ 10.4 脆弱性アセスメント ~

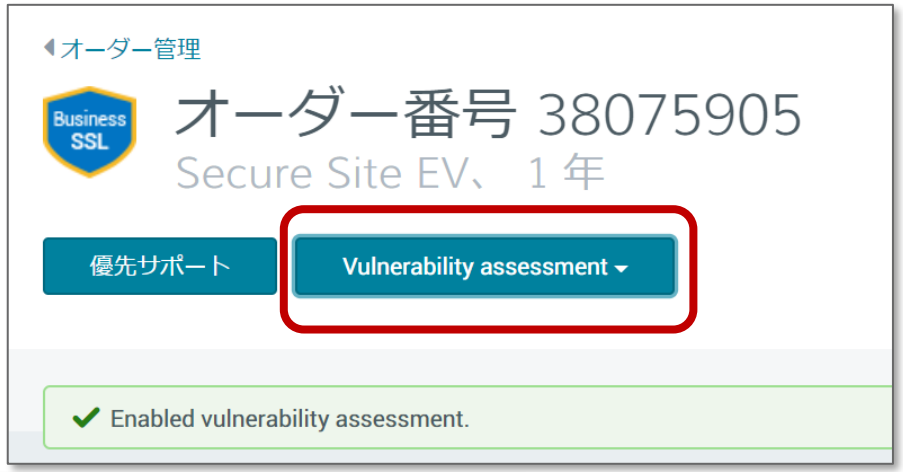
脆弱性アセスメント(Vulnerability Assessment)機能の有効化

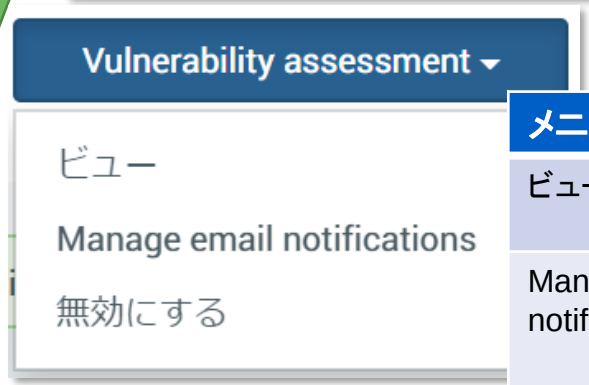
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■初期状態
（脆弱性アセスメントが有効化されていない）



■脆弱性アセスメントが
有効化された状態





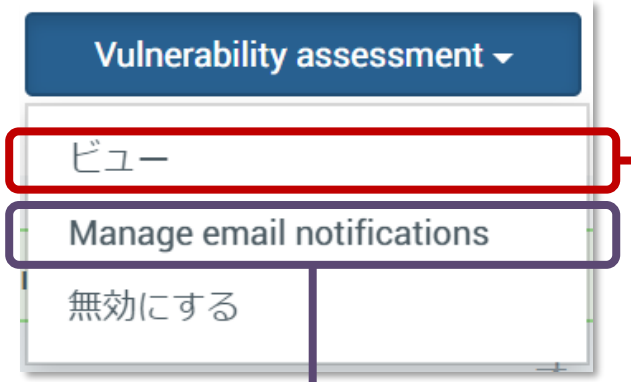
メニュー	説明
ビュー	脆弱性アセスメントの結果レポートを確認 →詳細は次ページ
Manage email notification	脆弱性アセスメントが脆弱性やその可能性を発見した際の通知を管理 →詳細は次ページ
無効にする	脆弱性アセスメント機能を無効化します

※1：脆弱性アセスメントの活用方法についてもっと詳しく：https://docs.digicert.com/ja/certificate-tools/vulnerability-assessment-service/

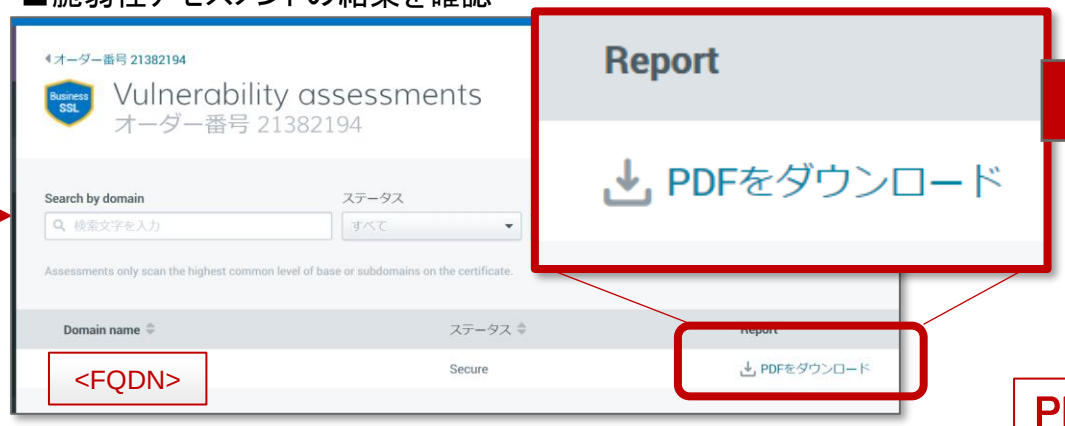
脆弱性アセスメント(Vulnerability Assessment)機能の管理

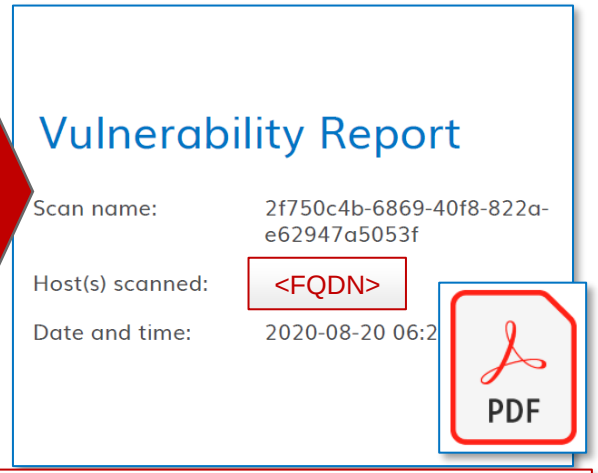
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■Vulnerability Assessmentボタン押下時に表示されるメニュー



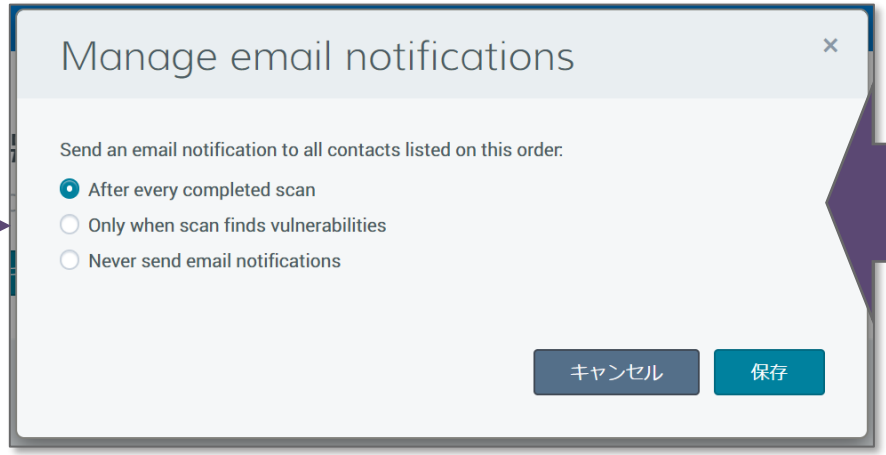
■脆弱性アセスメントの結果を確認





**PDFファイル形式で
脆弱性アセスメント結果レポートを
ダウンロードいただけます。**

■脆弱性アセスメントが脆弱性やその可能性を発見した際の通知を管理



設定	説明
After every completed scan	脆弱性アセスメントのスキャン実施ごとに結果を通知
Only when scan finds vulnerabilities	脆弱性アセスメントのスキャン実施の結果、脆弱性が発見された場合にのみ結果を通知
Never send email notifications	脆弱性アセスメントに関する一切の通知を無効化する

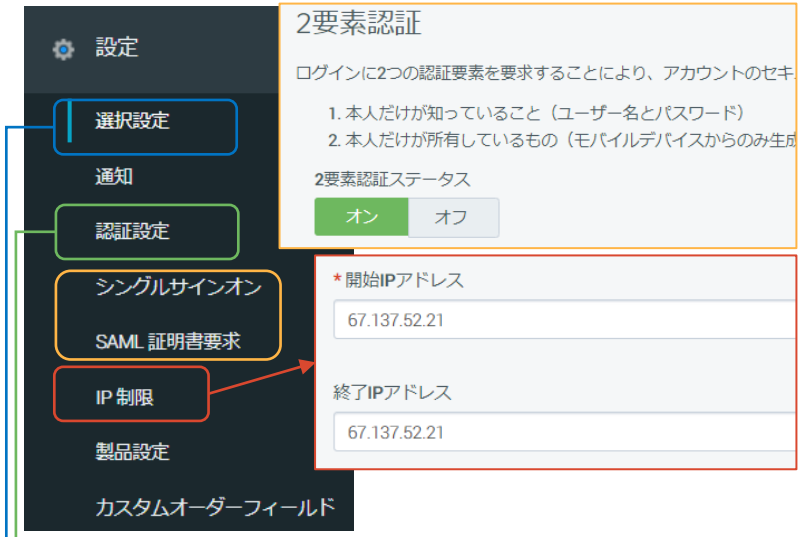
※1：脆弱性アセスメントの活用方法についてもっと詳しく：https://docs.digicert.com/ja/certificate-tools/vulnerability-assessment-service/

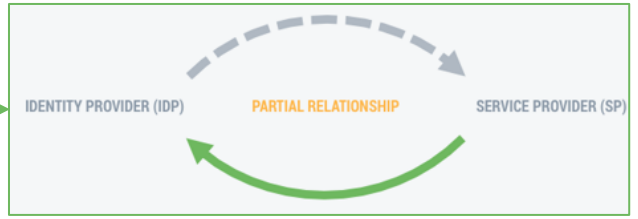
11. その他の管理機能・TIPS

セキュリティレベルを落とさずに、SSOやAPI連携によってお客様の証明書管理業務を効率化できます。
また、お客様のポリシーやプロセスに合わせて、2FA、IPアドレス制限や多段承認プロセスも利用可能です。

テーマ	機能	用途・メリット
セキュリティ強化／ポリシー適用	多要素認証 (2FA)	・クライアント証明書を利用可能 ・OTP：TOTP(Time-Based One-Time Password)対応 ■対応アプリケーション例 -Google Authenticator -Authy -Duo Mobile
	IPアドレス制限	・以下のそれぞれの粒度で制限可能 -アカウント単位 -ユーザー単位(コンソール/API) -ゲストURL
	多段承認プロセス	アカウント内の管理者(Admin権限を持つユーザ)による追加承認プロセスについて以下から選択可能； -「必要としない」 -「1回必要とする」 -「2回必要とする」 (例:事業部およびIT部門マネージャの承認を必要とする、など)
ID連携	SSO／SAML連携	・SAML2.0に対応 ・ADなどお客様のIdPとのフェデレーションによりCertCentralへのログインを簡易に ・CertCentral上でSAML証明書を管理可能

イメージ

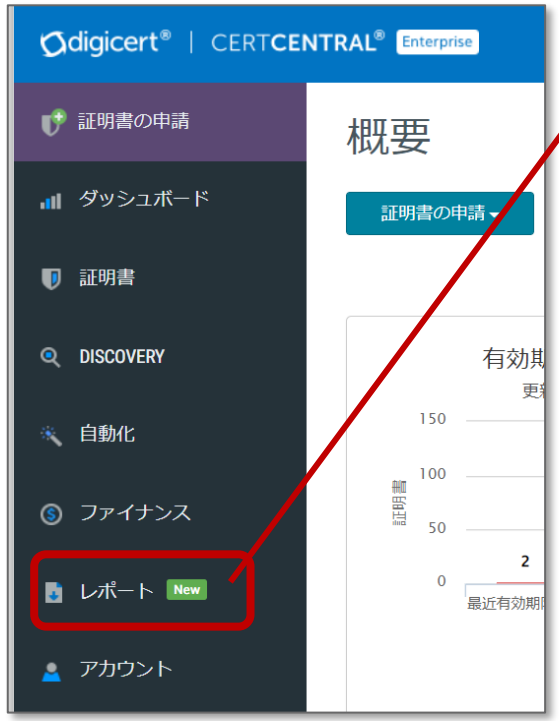




当ページに記載の画面イメージ等は、今後変更となる可能性があります。ご理解・ご了承ください。

レポートライブラリ機能：詳細レポートの出力

■「レポート」メニュー



各種カテゴリの詳細情報を指定してレポートをカスタマイズして生成できる管理者向けの機能です。

■取得可能なレポートの種類 ※1

カテゴリ	説明	頻度	ファイル形式
オーダー	オーダの有効期間や製品名に加えて、再発行されたすべての証明書情報、担当者、支払い情報等オーダに紐づく詳細な情報を取得します。	都度、毎週、毎月	CSV, JSON, Excel
残高履歴	アカウント残高の有効期間や、トランザクション履歴、利用金額、残高などの詳細抽出します。	都度、毎週、毎月	CSV, JSON, Excel
FQDN	製品毎に、コモンネームまたはSANsに含まれるユニークなFQDN数、またはワイルドカードドメイン数をサマリー、および一覧にして出力します。	都度、毎週、毎月	Excel
ドメイン	アカウントに登録されているドメイン名、ドメインに紐づく組織情報、認証ステータス、および認証有効期間を取得します。定期的にレポートを出力して期限切れ間近のドメイン名を管理します。	都度、毎週、毎月	CSV, JSON, Excel
監査ログ	アカウントで行われたユーザーのアクティビティの履歴を出力します。	都度、毎週、毎月	CSV, JSON, Excel
組織	アカウントに登録されている組織情報、認証ステータス、および認証有効期間を取得します。	都度、毎週、毎月	CSV, JSON, Excel

生成されたレポートは、CertCentralからダウンロードいただけます。レポートのダウンロード可能な期間は生成日から90日間です、以降自動的に消去されます。

※1 ご契約内容によりご利用いただけるレポートの種類が異なります。

カスタムオーダーフィールド機能：(1/3 フィールドの定義・登録)

■「カスタムオーダーフィールド」メニュー（「設定」メニュー配下、**※1**）

■カスタムオーダーフィールドの登録

#	カテゴリ	説明	入力/選択例
1	ラベル	カスタムオーダー フィールドのラベル(名前)	◆入力例: 「組織コード」「予算コード」等
2	入力 タイプ	カスタムオーダー フィールドの入力規則	・「すべて」:通常のテキスト入力 （英数字および日本語入力可） ・「テキスト」:TextArea形式 （英数字および日本語入力可） ・整数:整数のみ入力可 ・メールアドレス: 単一メールアドレスのみ入力可 ・メールアドレス リスト: 複数メールアドレス入力可
3	必須 フラグ	当フィールドの入力を オーダー(証明書申請)毎に 必須とするか否かを 指定するフラグ	ON:入力必須 OFF:必須でない(任意項目)

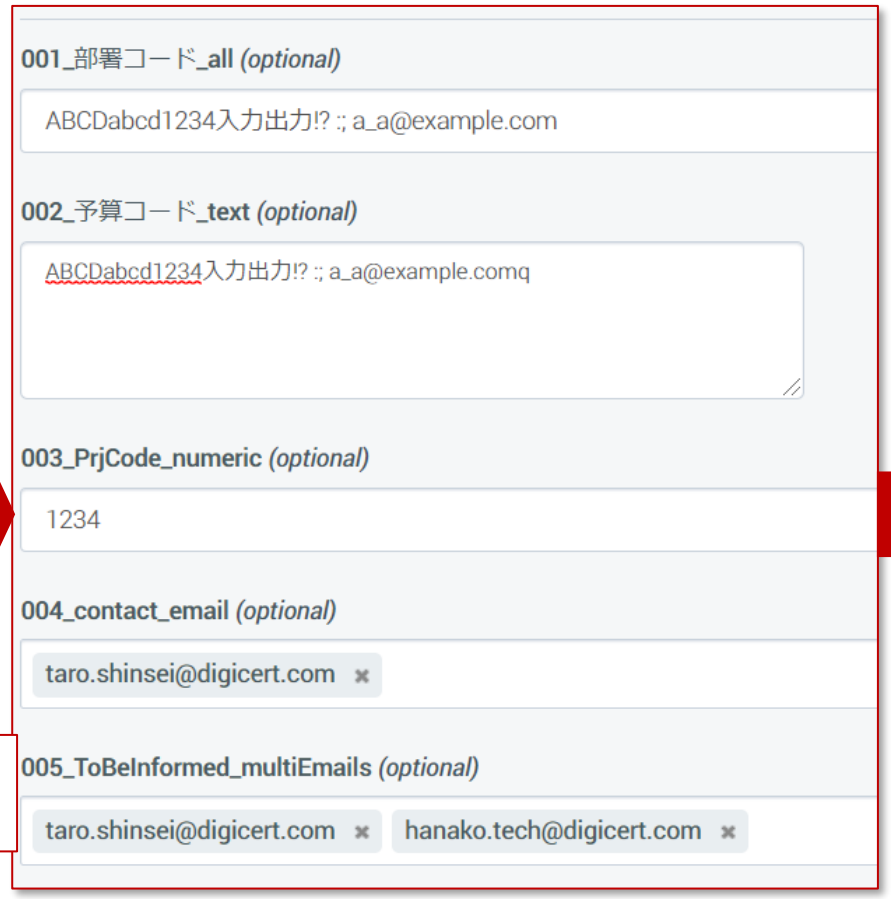
■（参考）登録済カスタムオーダーフィールドの一覧

ラベル	入力タイプ	オーダーフォームの使用	
001_部署コード_all	すべて	オプション	無効化
002_予算コード_text	テキスト	オプション	無効化
003_PrjCode_numeric	整数	オプション	無効化
004_contact_email	メールアドレス	オプション	無効化
005_ToBeInformed_multiEmails	メールアドレス リスト	オプション	無効化

※1：「カスタムオーダーフィールド」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。

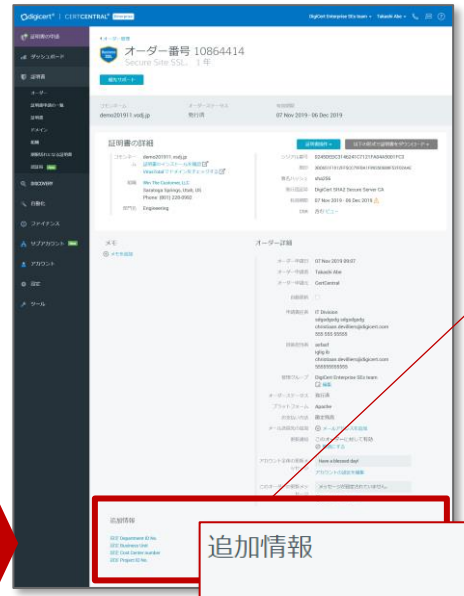
カスタムオーダーフィールド機能： (2/3 フィールドの入力・参照)

■証明書申請画面における「カスタムオーダーフィールド」の入力例（Secure Site OVの場合、※1）

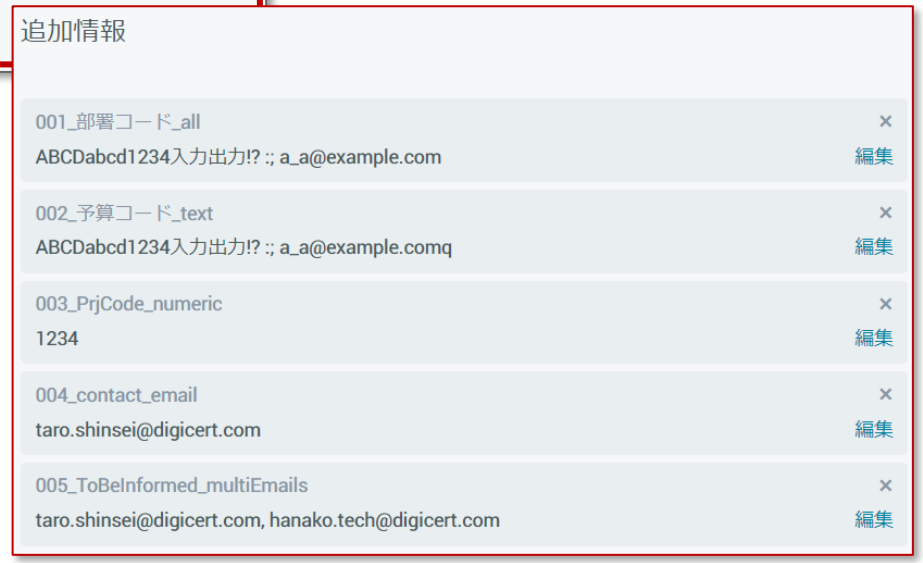


カスタムオーダーフィールド入力欄は
Section 3「その他のオーダー情報」
の最上部に表示されます

■オーダー詳細画面における「カスタムオーダーフィールド」の表示例（※1）



オーダー時に入力された
カスタムオーダーフィールドの
値は、オーダー詳細画面の
最下部でご確認いただけます
(随時編集可能)



※1：「カスタムオーダーフィールド」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。

カスタムオーダーフィールド機能： (3/3 オーダーレポートへの出力)

■オーダーレポート(「証明書」→「オーダー」メニューから「CSV形式でダウンロード」ボタンを押下して生成するCSVレポート)の項目への出力例
(前ページまでの設定例にそって5つのカスタムオーダーフィールドを設定した場合の例)

位置(*1)	フィールドのラベル(*2)	説明		出力例
1 ~ 28	セクション 4.「オーダー・証明書ステータス管理」内の「オーダーレポート(CSV形式)の詳細」を参照ください			
29	custom_fields.0.metadata_id	1つめのカスタムオーダーフィールド	ID (デジサートにて採番)	676
30	custom_fields.0.label		ラベル(名前)	001_部署コード_all
31	custom_fields.0.value		値	Value – 001
32	custom_fields.1.metadata_id	2つめのカスタムオーダーフィールド	ID (デジサートにて採番)	677
33	custom_fields.1.label		ラベル(名前)	002_予算コード_text
34	custom_fields.1.value		値	Value - 002
35	custom_fields.2.metadata_id	3つめのカスタムオーダーフィールド	ID (デジサートにて採番)	678
36	custom_fields.2.label		ラベル(名前)	003_PrjCode_numeric
37	custom_fields.2.value		値	3
38	custom_fields.3.metadata_id	4つめのカスタムオーダーフィールド	ID (デジサートにて採番)	679
39	custom_fields.3.label		ラベル(名前)	004_contact_email
40	custom_fields.3.value		値	004@example.com
41	custom_fields.4.metadata_id	5つめのカスタムオーダーフィールド	ID (デジサートにて採番)	680
42	custom_fields.4.label		ラベル(名前)	005_ToBeInformed_multiEmails
43	custom_fields.4.value		値	005a@example.com,005b@example.com

*1：CSV形式レポート内の各レポート項目の位置等は今後変更となる可能性があります。予めご理解・ご了承ください。
*2：以下、カスタムオーダーフィールドをさらに追加した場合、フィールドのラベルは「custom_fields.X…」のXの部分が1ずつ順に加算された文字列となります。

カスタムEメールテンプレート機能：

■「カスタムEメールテンプレート」メニュー（「設定」＞「通知」メニュー配下 ※1）

■カスタマイズ可能なEメールテンプレートの種類 (対象製品：SSL/TLサーバ証明書のみ)

#	カテゴリ	説明
1	申請完了メール	ユーザーがオーダーを発注したことを管理者に通知します。
2	承認通知メール	管理者がオーダーを承認したことを申請者に通知します。
3	却下通知メール	管理者がオーダーを却下したことを申請者に通知します。
4	有効期限切れ間近通知メール	オーダーの更新が間もなく必要になることを指定されたユーザーに通知します。
5	有効期限切れ 通知メール	デフォルトオーダーの有効期限が切れており、今すぐ更新する必要があることを指定されたユーザーに通知します。
6	複数年プラン：再発行のご案内 （有効期限切れ間近）	複数年プランの証明書を再発行する必要があることを指定されたユーザーに通知します。
7	複数年プラン：再発行のご案内 （有効期限切れ）	複数年プランの証明書の有効期限が切れており、今すぐ再発行する必要があることを指定されたユーザーに通知します。

※1：「カスタムEメールテンプレート」機能はデフォルト設定ではOFFとなっております。同機能のご利用をご希望の場合は担当営業までお問合せください。