CertCentral Partner 簡易マニュアル

最終更新日：2021年 12月 16日
デジサート・ジャパン合同会社

目次

© 2021 DigiCert – All Rights Reserved

1. はじめに

はじめに

- 当資料は CertCentral を用いてデジサートの証明書を申請、発行、または管理（再発行、失効などを含む）いただくために、パートナー様ならびにユーザー様に対して、補足的なガイダンスを提供するものです。
- 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)
- 当版では特に以下のシナリオを中心として解説いたします。
  - OV/EV証明書およびDV証明書の両方を取り扱う
  - 「都度認証」(各証明書申請のタイミングでDCVを実施する)方式を中心に扱う
    (不特定多数のエンドユーザの申請を扱うためOV/EV証明書の「事前認証」方式は参考との位置づけ)
- 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。
- 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。
  表示言語の切換えについては次ページを参照ください。

© 2021 DigiCert – All Rights Reserved

変更履歴

Ver.	公開日	変更点	変更箇所
~0.9	2020/9/23	省略	-
1.0	2020/11/16	[1. はじめに] 「CertCentralへログイン」「変更履歴」ページを追加	Page 5-6
		[2.3 ドメイン名利用権確認(DCV)] DCVメールのタイトル、文面変更を反映	Page 31, 34
		[5. 発行された証明書の取得] 証明書発行時点の証明書ファイル形式の詳細を追記	Page 75-78
		[7. プラン・証明書の有効期間、更新案内メールについて] プランおよび証明書の有効期間の詳細を追記	Page 89-92
		[9.4 ゲストアクセス] セクションを追加	Page 124-129
		[10.1 サイトシール] 画面およびシールデザイン変更を反映	Page 131-135
		その他誤記修正	-
1.1	2021/1/25	[9.3 ゲストアクセス]および[9.4 ゲストURL] 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 119-131
1.2	2021/3/16	[2.2 OV/EV証明書の申請]、[2.4 （参考）組織およびドメイン名の管理]および[8.ユーザー管理] 担当者/ユーザー情報の入力欄ラベル「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 21, 41, 43, 99
1.3	2021/8/3	各証明書の有効期間について	Page 89-92
1.4	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 31,35,145,146

※ 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。

© 2021 DigiCert – All Rights Reserved

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。

© 2021 DigiCert – All Rights Reserved

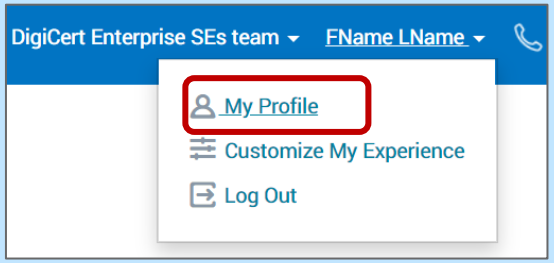
CertCentralを日本語でご利用いただくための各種設定について

区分	設定方法

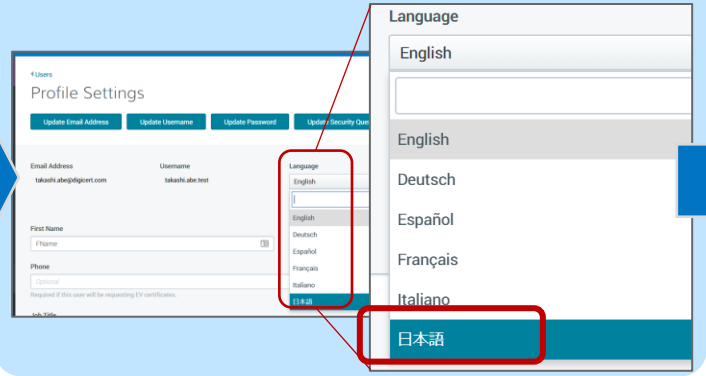
画面表示言語

■CertCentralの画面表示言語を英語→日本語へ切り替える手順

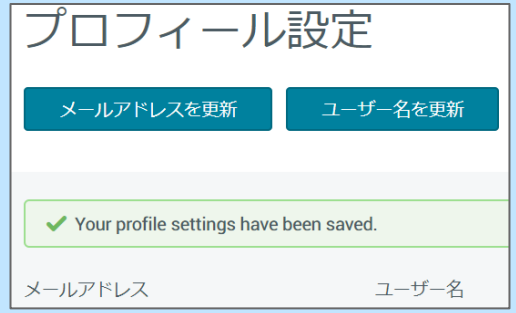
STEP 1：画面右上部の「My Profile」をクリックして「Profile Setting」画面を開きます



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

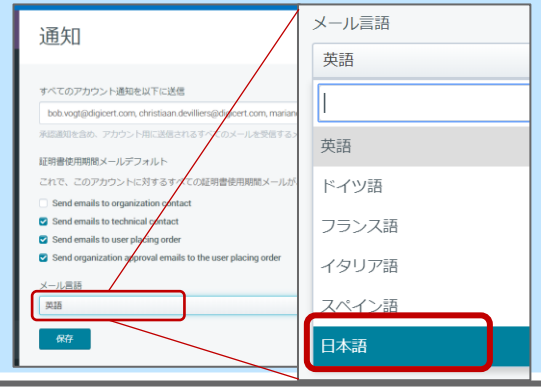


メール言語

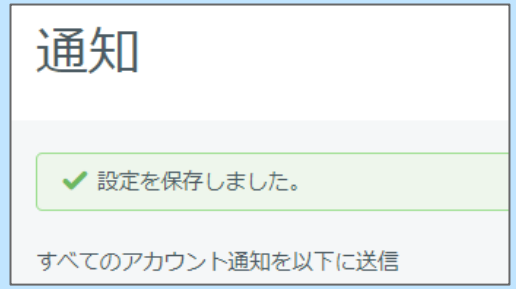
■CertCentralから配信されるメール（※DCVメールを除く）の画面を英語→日本語へ切り替える手順

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



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。

© 2021 DigiCert – All Rights Reserved

2. OV/EV証明書の申請

~ 2.1 ワークフロー概要 ~

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

タスク概要		内容	CertCentral		エンドユーザ企業	
			メニュー操作	備考	申請責任者	ドメイン名管理者
事前準備		・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて) 申請責任者様の確認、事前調整 ・(必要に応じて)ドメイン名管理者の確認、事前調整	(特にメニュー操作不要)		N/A	N/A
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)	[証明書の申請]	セクション 2.2 参照	N/A	N/A
申請レビュー・承認		(アカウント単位の設定で省略可) ・管理者が申請内容を確認し、承認または却下	[証明書]→ [証明書申請の一覧]	省略	N/A	N/A
認証	オーダー詳細確認	・オーダーの認証ステータスを確認	[証明書]→[オーダー] →[オーダー詳細]	セクション 4 参照	N/A	N/A
	組織(Org)認証	・デジサートにて認証を開始(第三者データベースによる組織実在性確認、申請責任者様への電話認証など)	(特にメニュー操作不要)		認証へのご対応	N/A
	ドメイン利用権確認(DCV)	・ DCVメールの送信指示	[証明書]→[オーダー] →[オーダー詳細]		N/A	DCVメール受信
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]→[オーダー] →[オーダー詳細]	セクション 5 参照	N/A	N/A

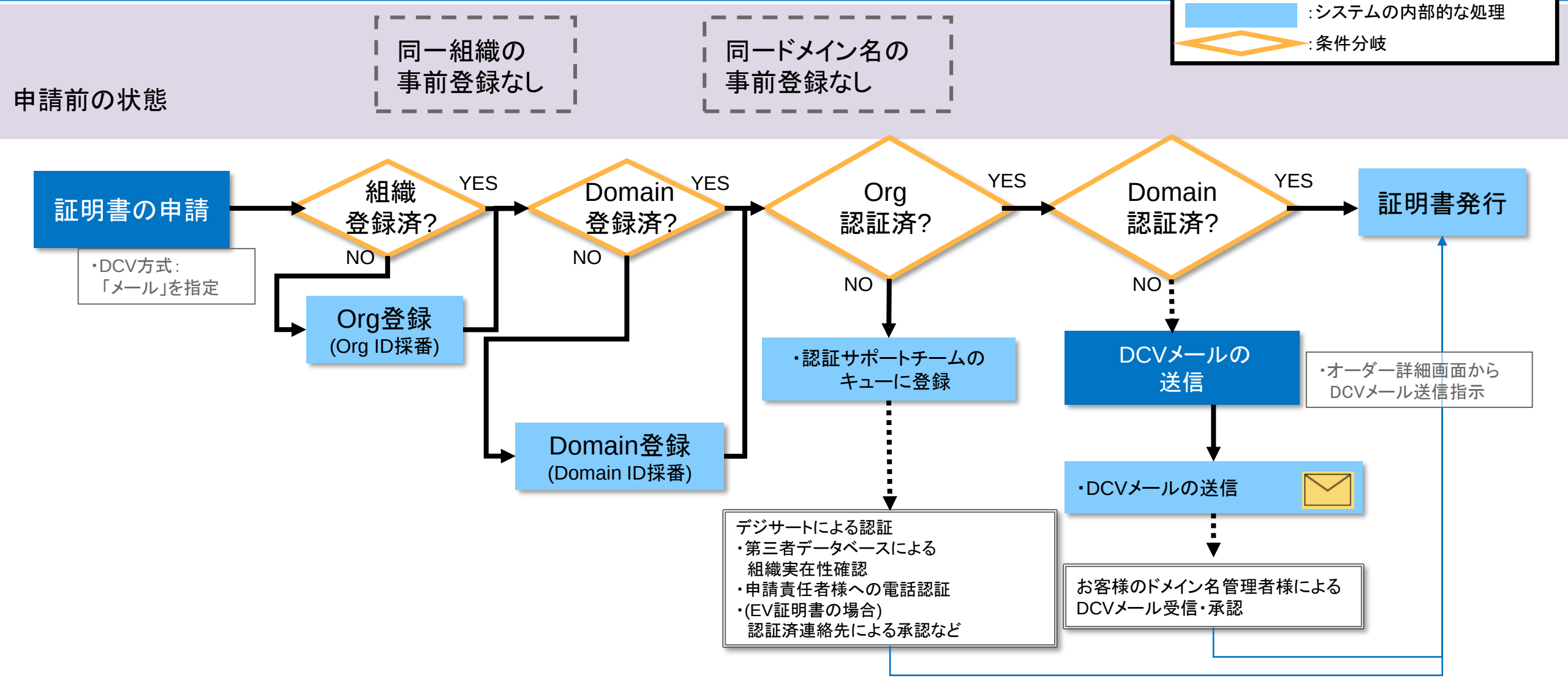
© 2021 DigiCert – All Rights Reserved

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

タスク概要		内容	CertCentral		エンドユーザ企業	
			メニュー操作	備考	申請責任者	ドメイン名管理者
事前準備		・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて) 申請責任者様の確認、事前調整	(特にメニュー操作不要)		N/A	N/A
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)	**[証明書の申請]**	セクション 2.2 参照	N/A	N/A
申請レビュー・承認		(アカウント単位の設定で省略可) ・管理者が申請内容を確認し、承認または却下	**[証明書]→[証明書申請の一覧]**	省略	N/A	N/A
認証	オーダー詳細確認	・オーダーの認証ステータスを確認	**[証明書]→[オーダー]→[オーダー詳細]**	セクション 4 参照	N/A	N/A
認証	組織(Org)認証	・デジサートにて認証を開始(第三者データベースによる組織実在性確認、申請責任者様への電話認証など)	**(特にメニュー操作不要)**		認証へのご対応	N/A
認証	ドメイン利用権確認(DCV)	・認証トークンの取得・配置 ・ファイル/DNS認証のための(再)ポーリング指示	**[証明書]→[オーダー]→[オーダー詳細]**		N/A	N/A
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]→[オーダー]→[オーダー詳細]**	セクション 5 参照	N/A	N/A

© 2021 DigiCert – All Rights Reserved

OV/EV証明書の申請～認証までのご申請手続きとシステム処理概要
(「都度認証」方式、DCV方式：メール認証の場合)



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

© 2021 DigiCert – All Rights Reserved

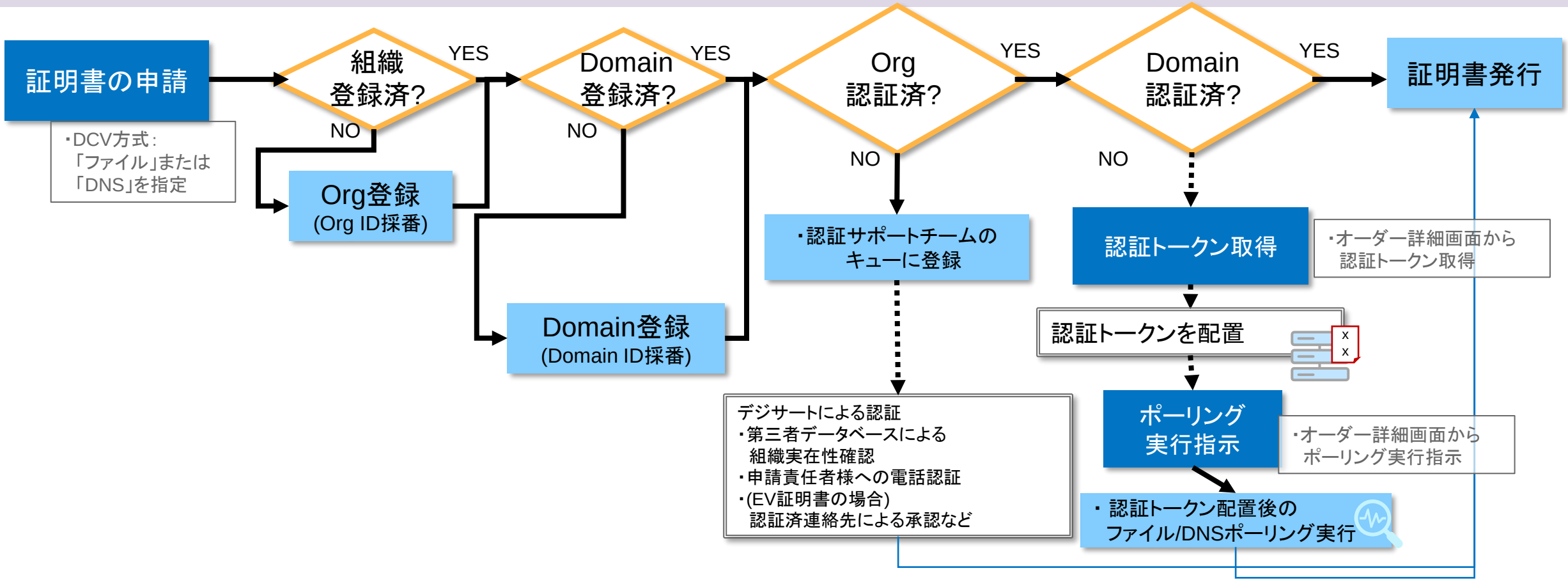
OV/EV証明書の申請～認証までのご申請手続きとシステム処理概要
(「都度認証」方式、DCV方式：ファイル認証/DNS認証の場合)

: 自動的に次の処理へ進む
: 次の手続きが必要
: CertCentralでのご申請手続き
: システムの内部的な処理
: 条件分岐

申請前の状態

同一組織の
事前登録なし

同一ドメイン名の
事前登録なし



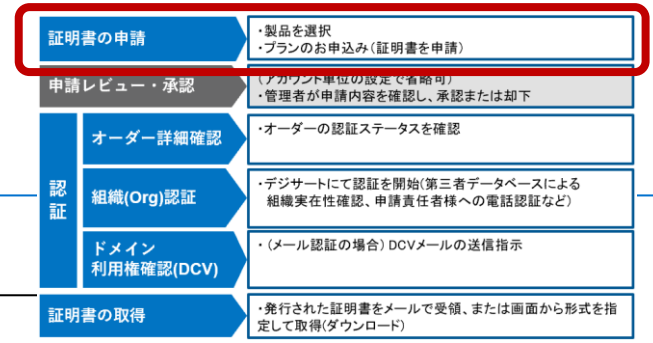
当ページに記載のチャートは概略を表すものであり、一部の処理を簡略化して記載しております。
セキュリティ、コンプライアンスの理由から上記に記載がない、追加の確認などが必要となるケースがあります。ご理解・ご了承ください。

© 2021 DigiCert – All Rights Reserved

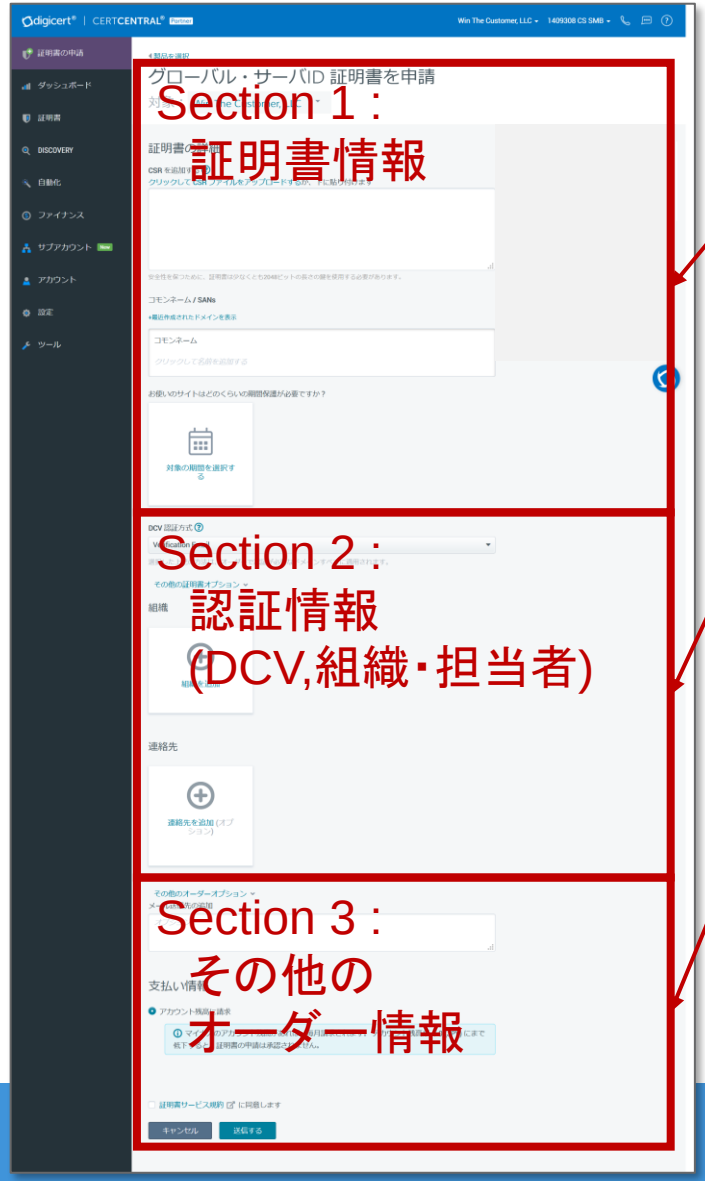
2. OV/EV証明書の申請

~ 2.2 OV/EV証明書の申請 ~

OV/EV証明書の申請画面（新規申請/更新申請 共通）



■「証明書の申請」メニューからOV/EV証明書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

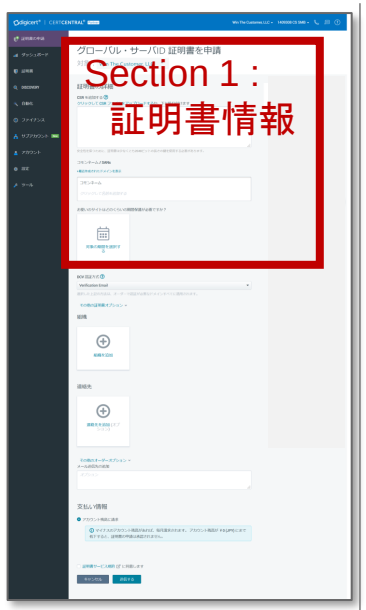
次ページ以降で詳細な入力方法をガイドします。

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 新規申請 Section 1：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」



製品を選択
グローバル・サーバID 証明書を申請
対象： -- Container 01

証明書の詳細

CSR を追加する
クリックして CSR ファイルをアップロードするか、下に貼り付けます

```
-----BEGIN CERTIFICATE REQUEST-----
MIICxjCCAa4CAQAwgYAxCzAJBgNVBAYTAlVTMR0wGwYDV00DExRkZW1vMjAxOTEx
LmFwcGZ3LmS1dDEeMBwGA1UECgwVV2luIFRoZSBDdXN0b21lciwgTExDMR0wEgYD
V0QLDAtFbmdpbmVlcmluZzENMAsGA1UEC80EVXRhaDENMAsGA1UEBx0ETGVoaTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALXcOccStKtGAoL3b0HHqLW+
no9ISiFfT1IlZ4MHh+lkNhes5A9WA5IvNmYYEbBMgJfqTH68BimnCSdUKlXfwhG
pjic2yJ3a6zvkRPr8lhT8HIpoFtmEFzkA/4BIZF64e+e/9pmE1/Xdzw1uqzOjgeN
4fgd7sU0To50ket0qwG+GEbk+jsv/xAXATOF/RJxp4I8HRbJvPkE4MoVRoCY8Uu3
Zmz1W1D+HS90cvyD42VF+E3az58m3bnnT37s/K1WpgYFPY2AJFo9mZsyPaWX59Vd
5apzJlhzlt9s8jcCmdleUlirMk2OvYSjB106SkaIRhPFs9amfwWrqU/tLr1JF1EC
AwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQBGDx056blvB5ArAOmvmtqYOwrXHNbT
ztoqAnBP088q4ciu8FMdn5gdWdkPe2hZO4/ABtvjBHelF+G0Yfy4aDU8lMezRAxo
```

安全性を保つために、証明書は少なくとも2048ビットの長さの鍵を使用する必要があります。

コモンネーム / SANs

+最近作成されたドメインを表示

コモンネーム
www.example.com

SANs
example.com

クリックして名前を追加する

お使いのサイトはどのくらいの期間保護が必要ですか？

対象の期間を選択する

■【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て証明書を申請す場合は
クリックして表示されるプルダウンリストから選択してください。

■【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。
・SANs欄の入力数量には上限がある場合があります(※1)。
・SANs入力される値により費用が変動します(※2)。

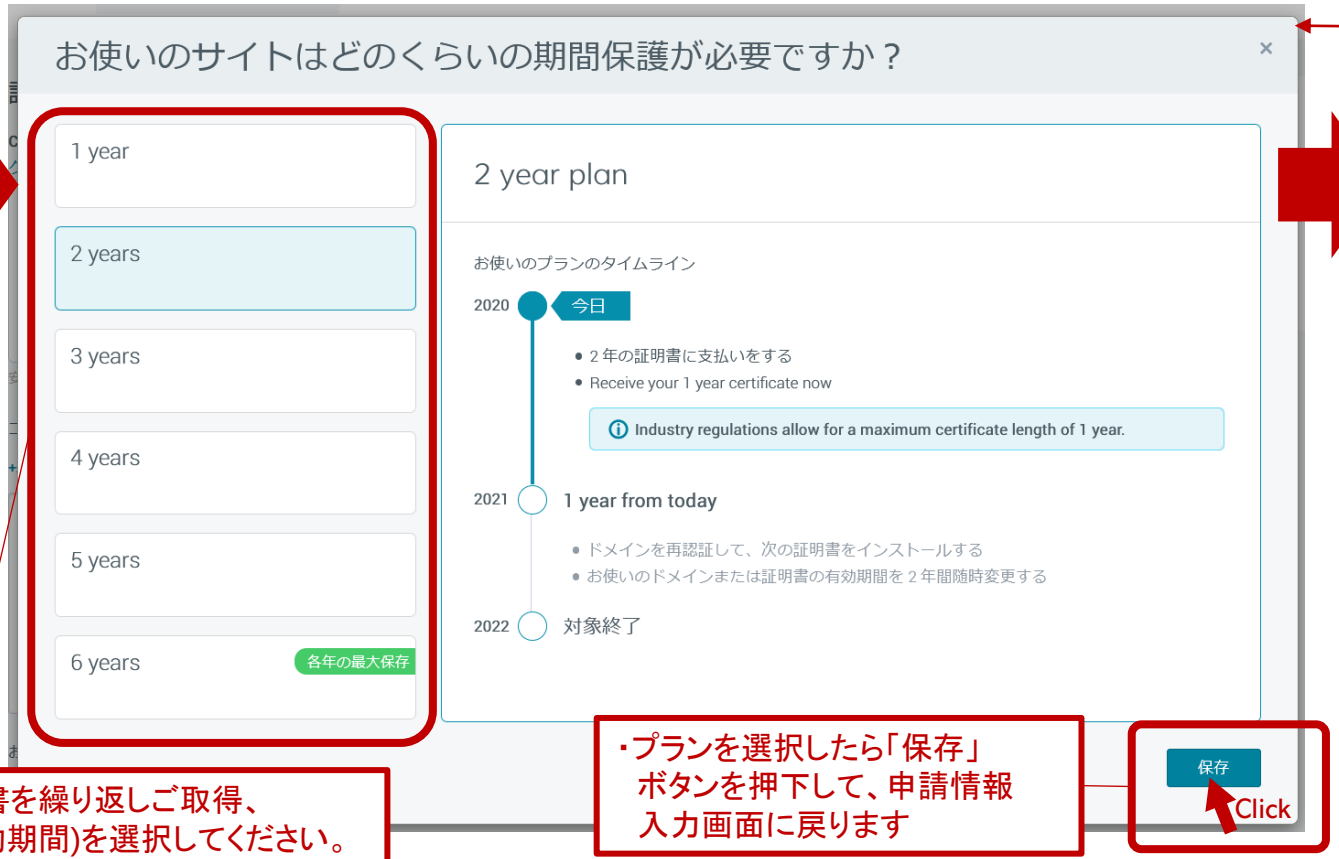
■【必須】期間：
・ご申請いただくプラン(証明書を繰り返しご取得、継続してご利用
いただけるご契約期間)を、1年間~6年間からご選択ください
・プラン選択後、プランの初回にご取得いただく証明書の有効期間
を選択・指定いただけます(最大397日間、※3)。
→詳細は次ページ[補足 プランの選択]をご参照ください

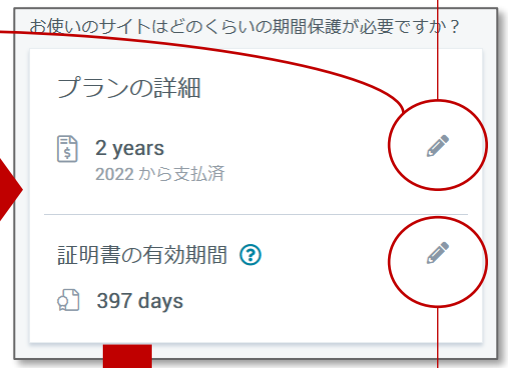
※1：通常は最大255のSANsを入力可能です。また【バウチャー】を用いた申請時には、バウチャー生成時に指定した上限が設定されますのでご注意ください。
※2：FAQ「(OV/EV証明書用)Subject Alternative Names（サブジェクトの別名）」について」https://knowledge.digicert.com/ja/jp/solution/SO27318.html
※3：【バウチャー】を用いた申請時にはプランの期間は自動的に設定されます

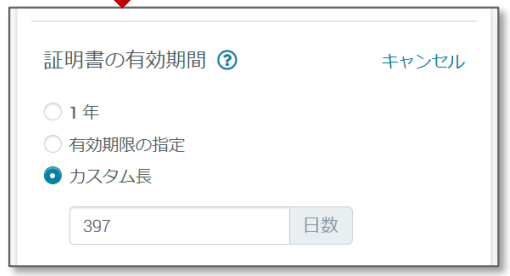
© 2021 DigiCert – All Rights Reserved

補足 プラン(契約期間)の選択

■「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)







・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

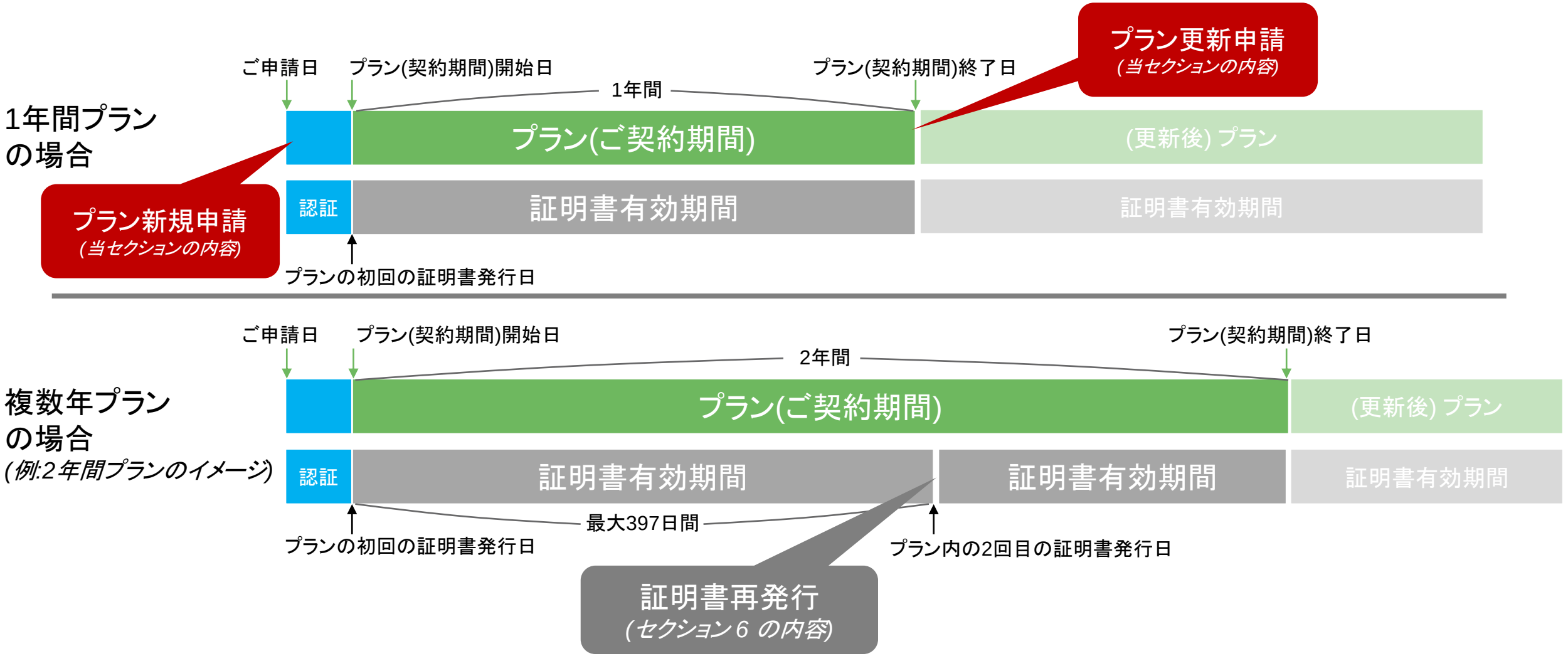
このアイコンをクリックするとプラン選択ウィンドウが再度開きます

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など詳細については *セクション7「証明書の有効期間」*を参照ください

© 2021 DigiCert – All Rights Reserved

補足 プランと証明書の「有効期間」、「更新」および「再発行」

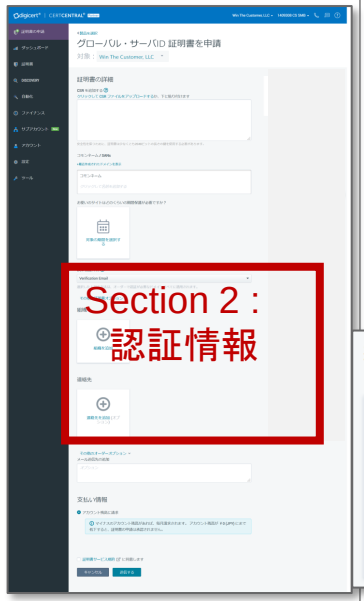


© 2021 DigiCert – All Rights Reserved

新規申請 Section 2 (OV証明書の場合) : 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

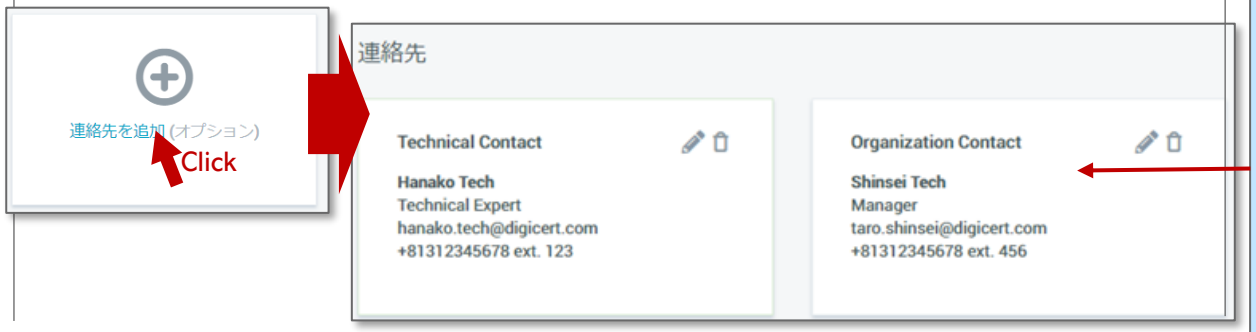
■「申請情報入力画面」



■DCV方式の選択

■組織情報入力欄

■担当者情報入力欄



■【必須】DCV方式の選択
ドメイン名利用権確認(DCV)の方式を以下から選択します。
・メール (Verification Email)
・ファイル (HTTP Practical Demonstration)
・DNS TXT (DNS TXT Record)
・DNS CNAME (DNS CNAME Record)
（各方式の詳細は別紙参照）

■【必須・自動設定あり】組織情報
・証明書に記載する組織(申請団体)情報を入力します
・「組織を追加」→「新しい組織」を選択いただき、組織(申請団体)情報を入力します（入力例は別紙参照）
・過去の証明書申請・発行履歴がある場合、組織名情報や担当者情報が自動設定される場合があります。
・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・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（各担当者の役割や入力例等は別紙参照）
・組織情報の自動設定により、担当者情報も併せて自動設定される場合があります。

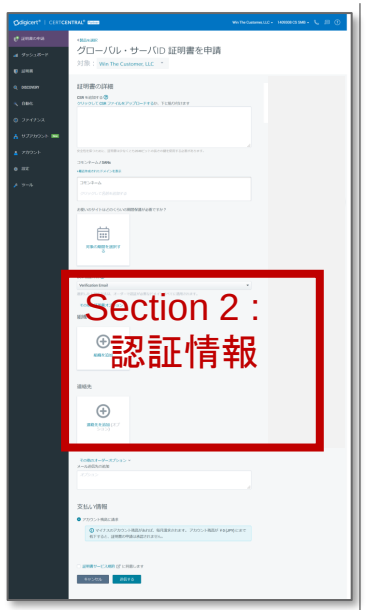
・「申請責任者」欄にダミー情報(「FirstName」「LastName」等)が表示されている場合、右上のゴミ箱マークをクリックして削除し下部の「+Add Organization Contact」リンクから正しい情報を入力してください。

© 2021 DigiCert – All Rights Reserved

新規申請 Section 2 (EV証明書の場合) : 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

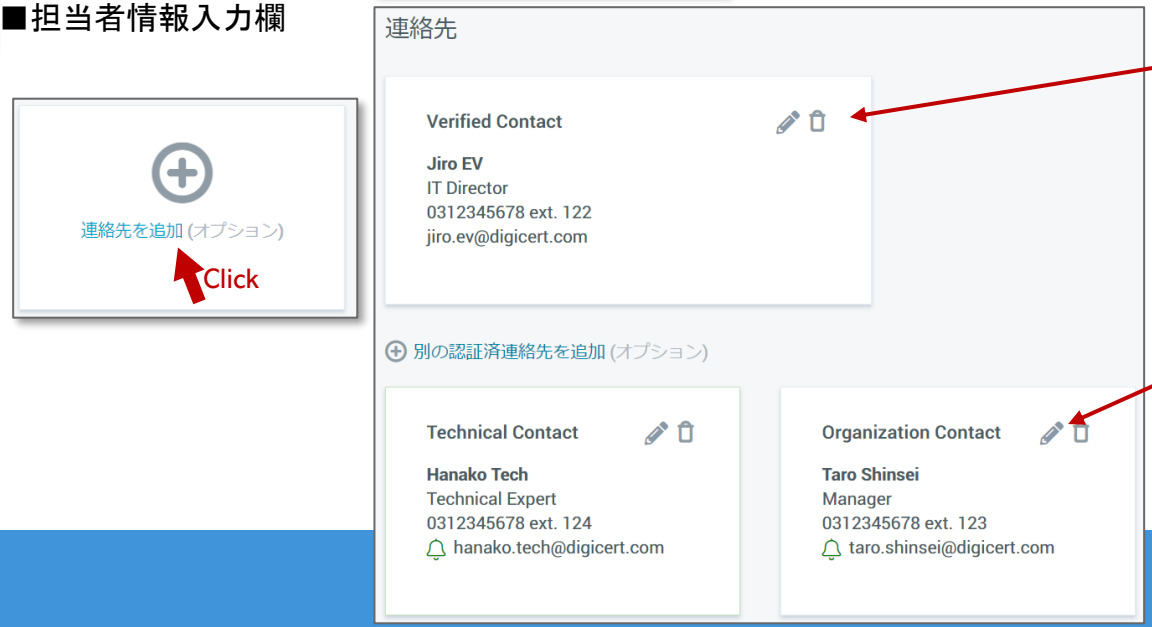
■「申請情報入力画面」



■DCV方式の選択
(OV証明書の場合と同一のため省略)

■組織情報入力欄

■担当者情報入力欄



■【必須】DCV方式の選択
(OV証明書の場合と同一のため省略)

■【必須・自動設定あり】組織情報
・証明書に記載する組織(申請団体)情報を入力します
・「組織を追加」→「新しい組織」を選択いただき、組織(申請団体)情報を入力します(入力例は別紙参照)
・過去の証明書申請・発行履歴がある場合、組織名情報や担当者情報が自動設定される場合があります。
・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・自動設定あり】認証済連絡先(Verified Contact)
・「認証済連絡先」を指定します。
・過去の証明書申請・発行履歴がある場合、組織名情報や担当者情報が自動設定される場合があります。

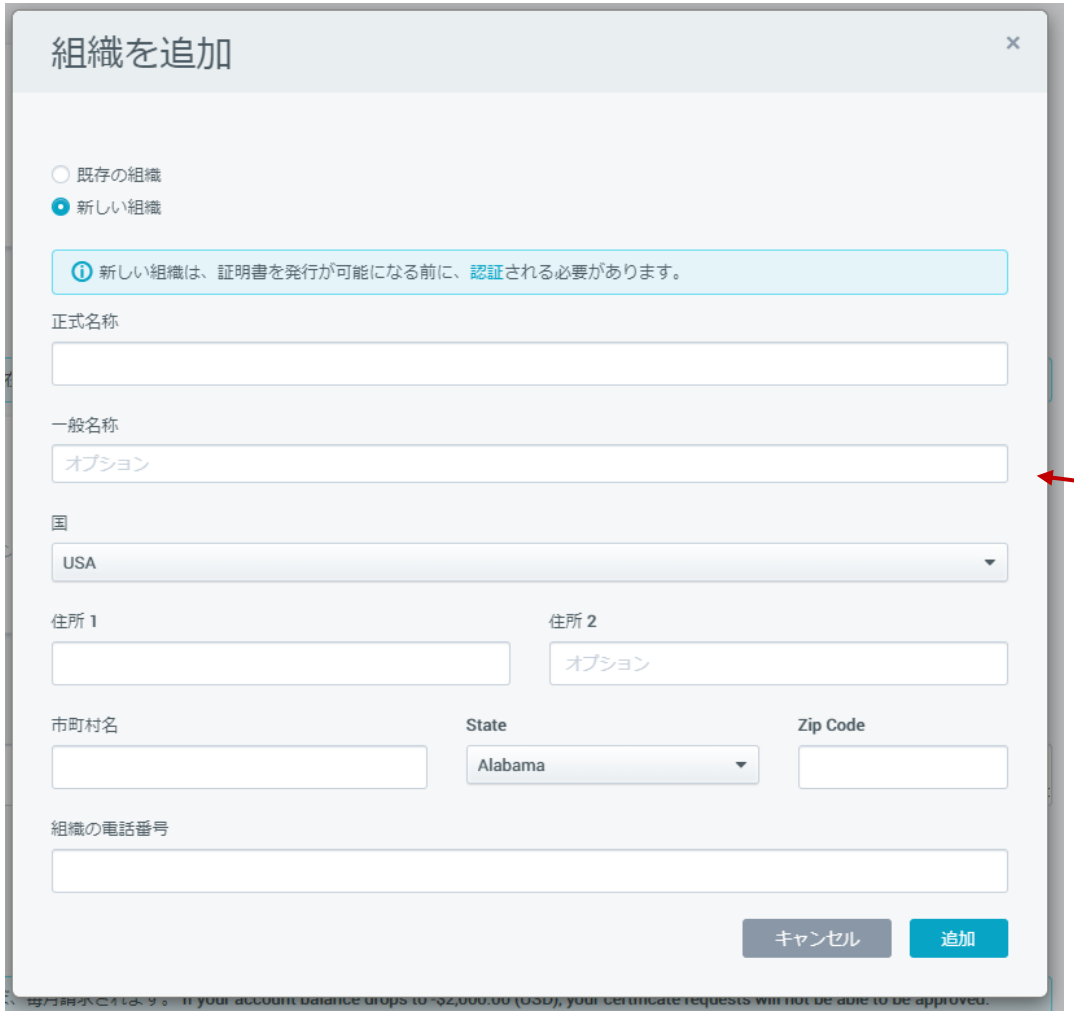
■【必須・自動設定あり】担当者(Contacts)情報
・証明書の申請に関する「技術担当者」「申請責任者」を設定することができます(各担当者の役割や入力例等は別紙参照)
・組織情報の自動設定により、担当者情報も併せて自動設定される場合があります。

・「申請責任者」欄にダミー情報(「FirstName」「LastName」等)が表示されている場合、右上のゴミ箱マークをクリックして削除し下部の「+Add Organization Contact」リンクから正しい情報を入力してください。

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 新規申請 Section 2 : 補足 組織情報の入力例

■新規組織(Org)登録時の組織情報入力例



■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>	
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	【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 Code	申請団体所在地・郵便番号	104-0061
組織の電話番号	申請団体の電話番号	03-4560-3900

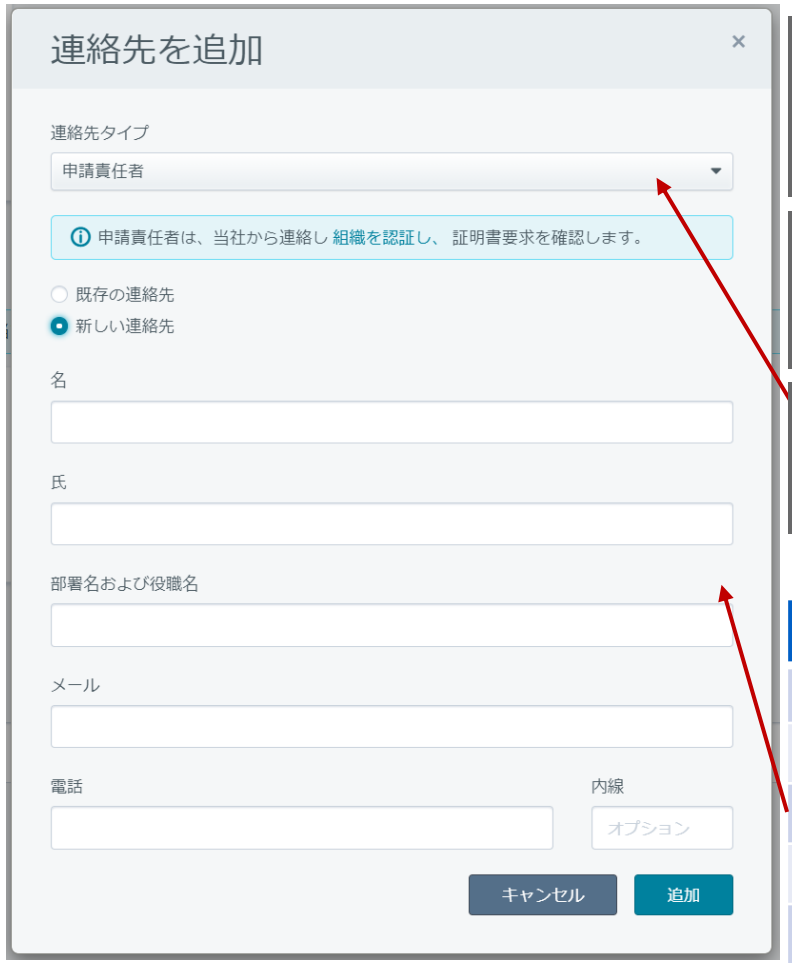
その他のパターンの記入例については以下のFAQを併せてご参照ください。
https://knowledge.digicert.com/ja/jp/solution/SO22977.html

※ 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。

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 新規申請 Section 2 : 補足 担当者情報の入力例

■新規担当者(Contact)登録時の担当者情報入力欄



■OV/EV証明書の新規申請時に入力いただく担当者の種類と役割

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

■担当者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 (※1)
氏	担当者氏名の氏	Nihon (※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	担当者の電子メールアドレス	taro.nihon@digicert.com
電話	担当者の電話番号	03-4560-3900
内線	【任意】担当者の内線番号	123

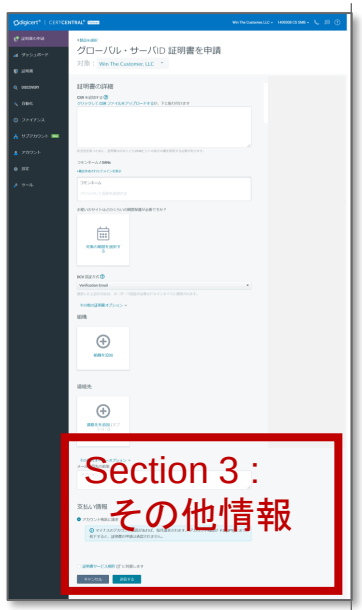
※1 : 該当項目には日本語（ひらがな、カタカナ、漢字）での入力も可能です。

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 新規申請 Section 3 : 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。

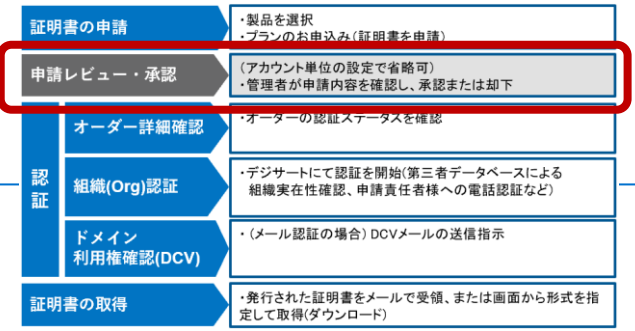
・「メール送信先の追加」: 申請者に加えて、申請関連のメールや更新案内メールの送信先を追加することができます。

■【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。

© 2021 DigiCert – All Rights Reserved

(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)



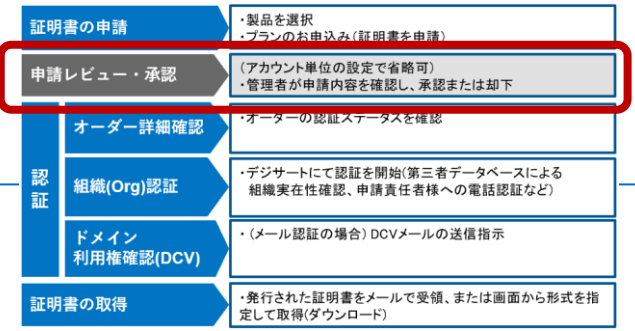
■「設定」→「選択設定」→「詳細設定」→「承認手順」メニューにて、証明書申請後の「申請レビュー・承認」プロセスの有無をアカウント単位で選択いただくことが可能です。
■当設定は任意となります。初期状態(下記表内の最上段)が推奨となります。

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

承認の手順については次ページ参照

© 2021 DigiCert – All Rights Reserved

(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)



■「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]

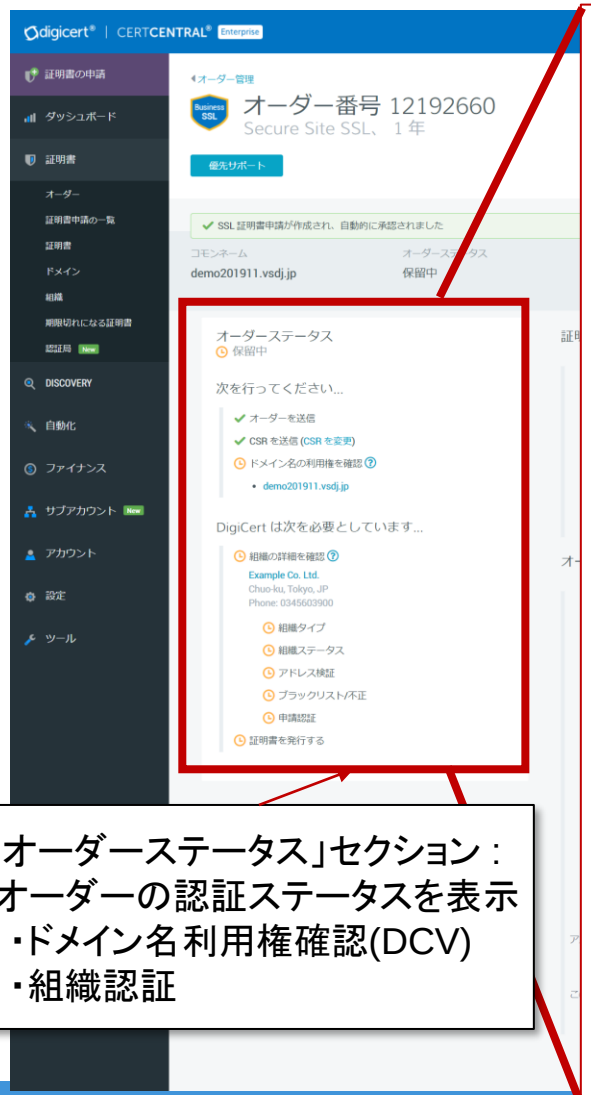
Click

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)

© 2021 DigiCert – All Rights Reserved

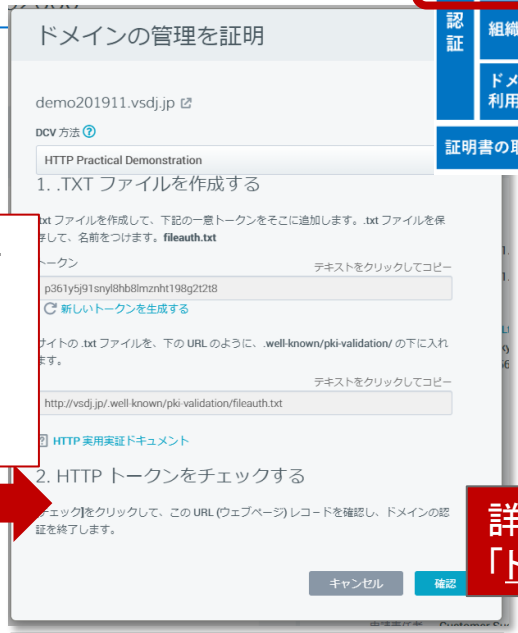
オーダー詳細確認～組織(Org)認証～ドメイン名利用権確認

■「証明書」→「オーダー」メニューからオーダー選択後に表示される「オーダー詳細画面」

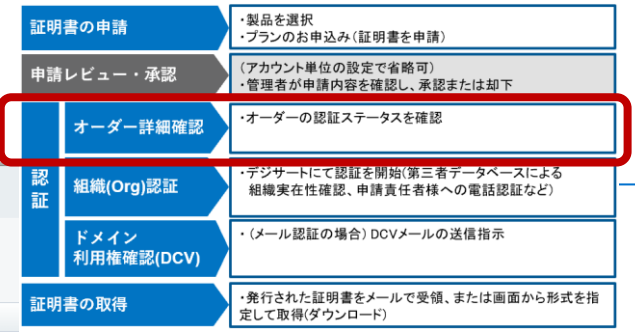


「オーダーステータス」セクション：
オーダーの認証ステータスを表示
・ドメイン名利用権確認(DCV)
・組織認証

■ドメイン名をクリックすると…
・DCV方式確認/変更
・メール配信先確認/(再)送信
・認証コード(Token)確認/
ポーリング実行
が可能な画面を表示



■組織名称をクリックすると
組織情報詳細画面を表示

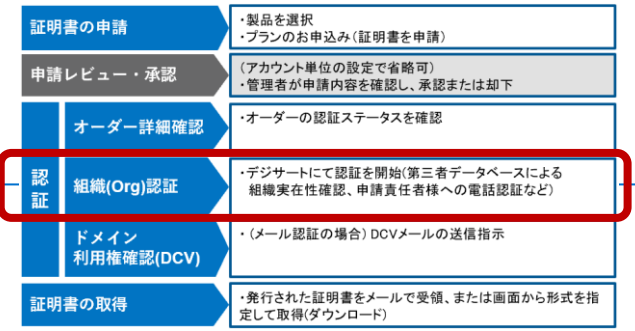


詳細はセクション2.3
「ドメイン名利用権確認」を参照

組織認証の流れ、
デジサートからのご案内内容
については次ページ以降参照

© 2021 DigiCert – All Rights Reserved

(OV証明書の場合) 組織(Org)認証の流れ



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

証明書を申請する組織(申請団体)における「有効(再利用可能)なOV認証履歴」の有無 (*1)

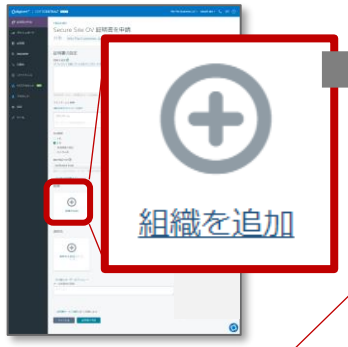
	申請責任者への連絡	技術担当者への連絡
有りの場合	原則として、ご連絡はありません。	
無しの場合	■ご連絡内容： ・**電話認証** (規定のデータベースで確認した組織(申請団体)の電話番号による証明書申請の意思確認 (*2))	■連絡内容： ・**登録内容の確認** ・**書類等のご提出依頼** (いずれも必要な場合のみ、*2)

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

*3：**「新しい組織」**を選択して組織情報を入力し直した場合も、登録済の組織情報と「組織名(name)」「国名(Country)」「都道府県(State)」および「市区町村(City/Locality)」の全ての情報が一致した場合、同一の組織(申請団体)に対する証明書申請と見なします。

*1：OV証明書申請時に「有効(再利用可能)なOV認証履歴」の有無を確認する方法 (*3)

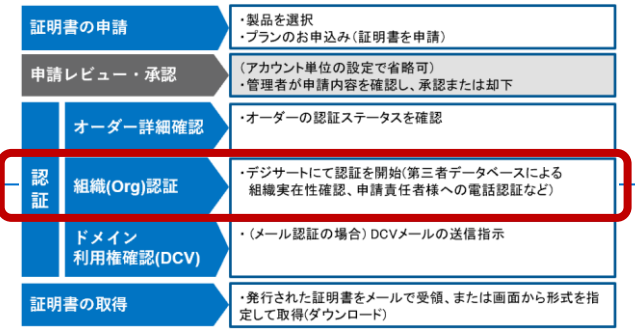
■OV証明書申請画面



「既存の組織」および
「認証未完了組織を非表示にする」
をクリックすると、プルダウン内に「有効(再利用可能)なOV認証履歴」を持つ組織のリストが名称順に表示されます。
対象組織が存在する場合はリストから選択してください。

© 2021 DigiCert – All Rights Reserved

(EV証明書の場合のみ) 追加ステップ「認証済連絡先による承認」



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

追加STEP 1: 認証済連絡先の認証

EV証明書を申請する組織(申請団体)における「認証済連絡先」の有無

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

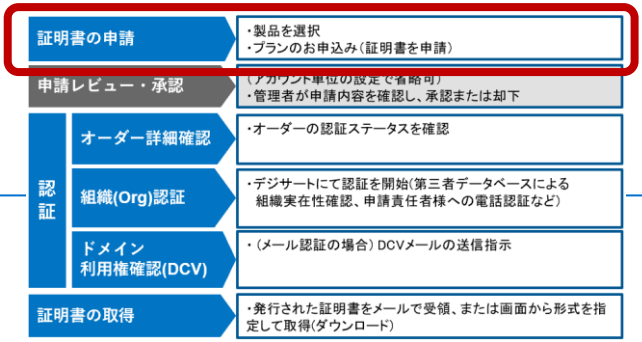
追加STEP 2: (認証済連絡先による)EV証明書申請の承認

EV証明書の申請の都度、認証済連絡先のメールアドレスへ送信される
「承認申請メール」の件名、送信元および本文イメージは以下のようになります

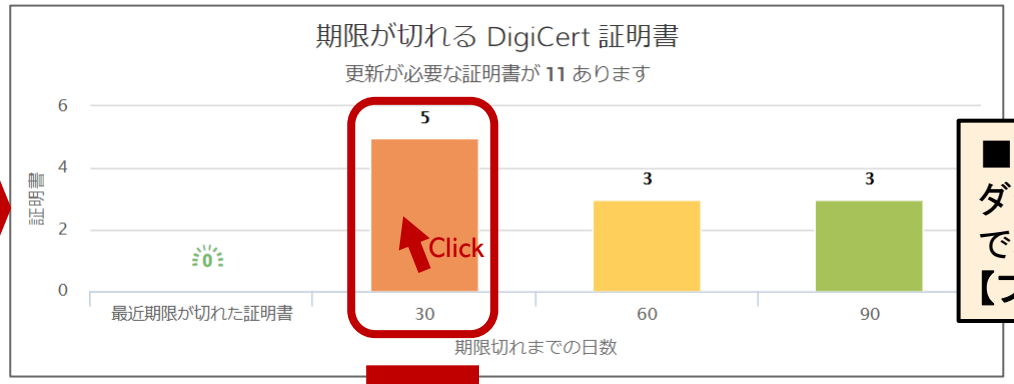
件名	DigiCert 証明書発行に関わる承認確認依頼 オーダー番号（[オーダー番号]、Organization name [組織名]
送信元	DigiCert <admin@digicert.com>
本文イメージ(抜粋)	[<認証済連絡先>氏名] 様 デジサートでは、申請組織 [組織名] 様の証明書の申請を受付けました。 証明書の発行には、本Eメールの宛先となるご担当者様に承認をいただく必要がございます。 以下の承認サイトにアクセスいただき、内容をご確認のうえ承認操作をお願いいたします。: https://www.digicert.com/link/approve-order.php? [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

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 更新申請 STEP 1：更新対象を特定

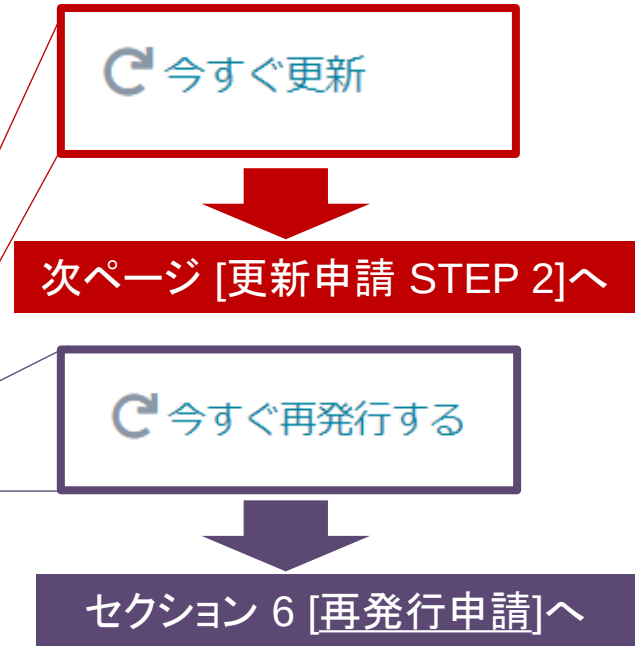


■ダッシュボード内の「期限が切れるDigiCert証明書」から



■「証明書」→「期限切れになる証明書」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**

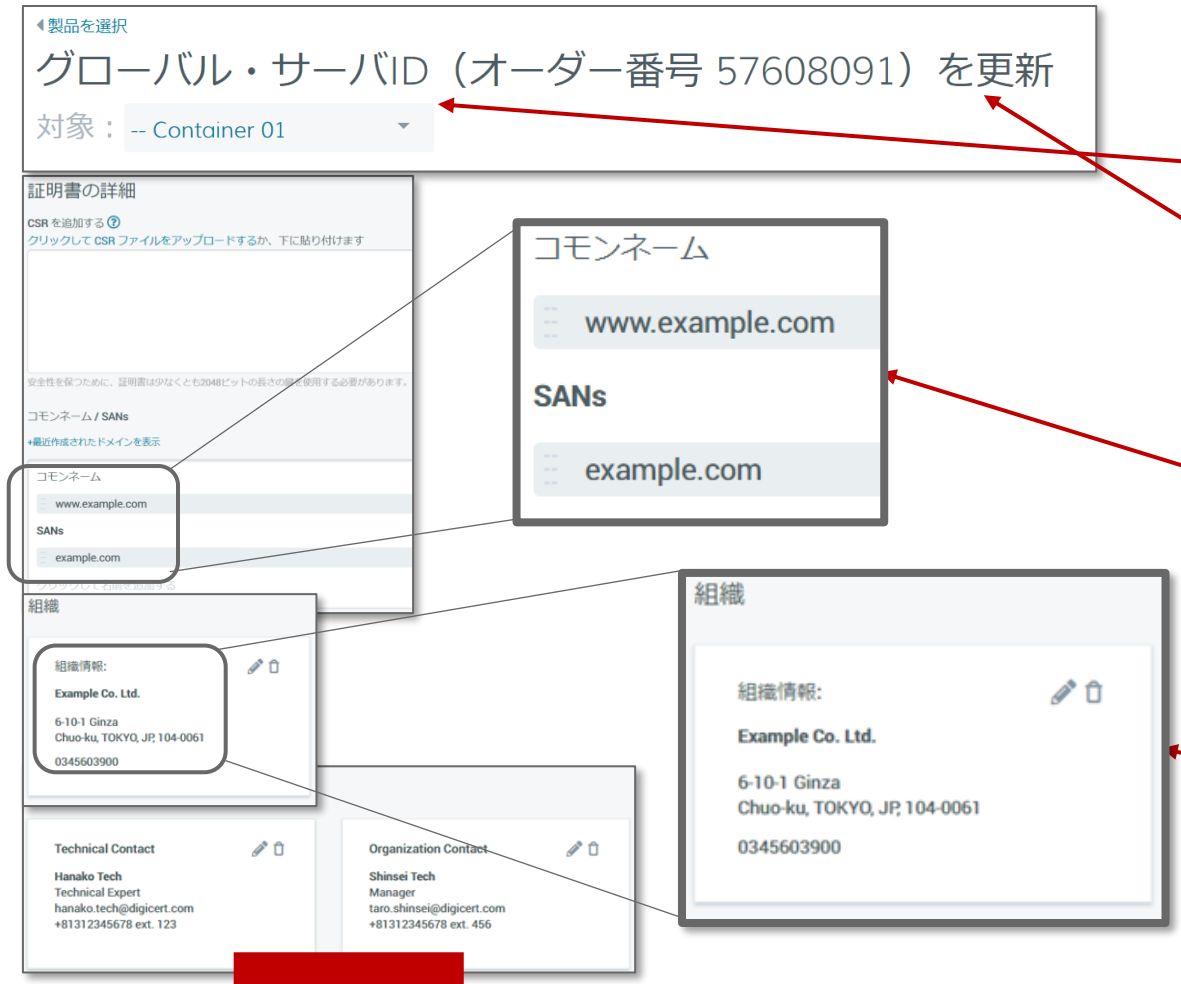


■ポイント2：
「期限切れになる証明書」メニューでは以下の要領でアクション(一覧の右端のリンク文言)が変化します。
・【プラン】が有効期限を迎える場合：**「今すぐ更新」　→　プラン(契約期間)を更新してください**
・【証明書】が有効期限を迎える場合：**「今すぐ再発行する」　→　証明書を再発行してください**

© 2021 DigiCert – All Rights Reserved

OV/EV証明書 更新申請 STEP 2：プラン更新申請情報の入力

■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。

© 2021 DigiCert – All Rights Reserved

2. OV/EV証明書の申請

~ 2.3 ドメイン名利用権確認(DCV) ~

ドメイン名利用権確認(DCV) – OV/EV証明書で利用可能な方式

・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 (OV/EV証明書の場合) または no-reply@geotrust.com (DV証明書の場合)
ファイル認証	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

© 2021 DigiCert – All Rights Reserved

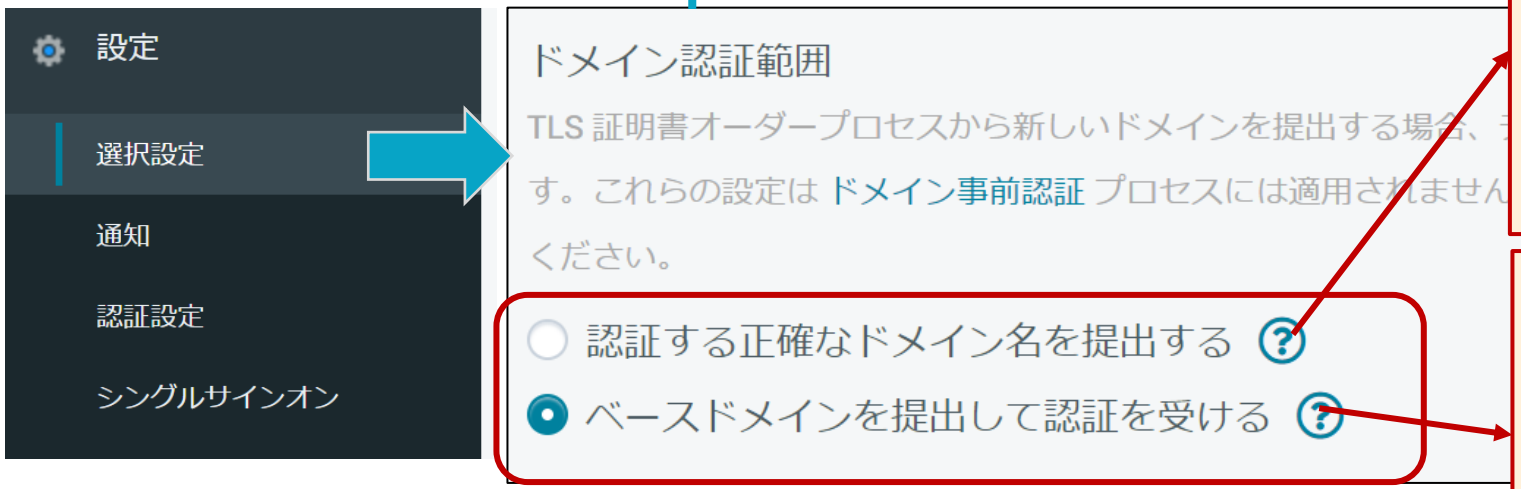
各DCV方式の詳細 – 「メール認証」の場合 (1/3 : 送信先の選択ルール)

■(「都度認証」の場合)OV/EV証明書のDCVメールの送信先は以下の組み合わせによって決定されます。

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

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

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



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

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

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

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

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

© 2021 DigiCert – All Rights Reserved

各DCV方式の詳細 – 「メール認証」の場合 (3/3 : メール文面)

■DCVメール(**OV/EV証明書用**)の概要

→メール件名、送信元および本文イメージは、以下のようになります

件名	[Domain Approval] ドメイン名の利用権確認のお願い: [確認対象のドメイン名(※1)]
送信元	no-reply@digitalcertvalidation.com
本文 イメージ (抜粋)	DigiCert では、DigiCert SSL/TLSサーバ証明書、S/MIME証明書等デジタル証明書の発行前に必要となるドメイン名利用権の確認を実施しております。ご担当者様が、ドメイン名 [確認対象のドメイン名(※1)] の所有者または管理者であることを確認いただいた上で、SSL/TLSサーバ証明書、またはS/MIME証明書に当該ドメイン名を利用することをご承認ください。 下記URLにアクセスしウェブページ上の内容をよくお読みになり、「承認する」のボタンをクリックしてください。（当ウェブページへのリンクの有効期間は30日間です。） https://www.digicert.com/link/dcv-approve/?t=<ランダムな認証トークン(※3)> Click

■DCV承認画面(**OV/EV証明書用**)イメージ

→DCV承認画面(日本語)のイメージは以下のようになります(※2)

※1 : 確認対象のドメイン名は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、申請内容ならびに前ページに記載のアカウント設定によって決定されます。
※2 : 承認画面の表示言語は画面上部の「言語」欄から選択いただき切り替えることが可能です。
※3 : 認証トークンの有効期間は30日間となります。一度使用した認証トークンは再利用できません。DCVメールを紛失した場合はCertCentralから再送いただくことが可能です。

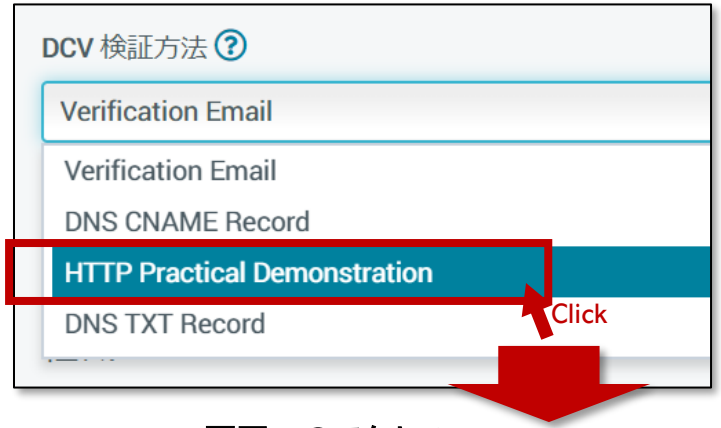
© 2021 DigiCert – All Rights Reserved

OV/EV証明書 各DCV方式の詳細 – 「ファイル認証」の場合

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

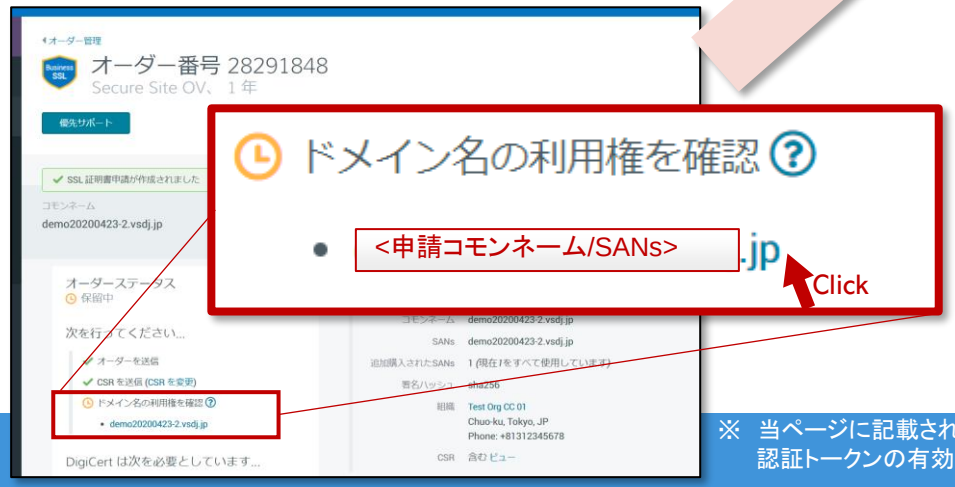
○STEP 1：証明書の申請

申請画面上の「DCV検証方法」欄で「HTTP Practical Demonstration」を選択し、申請を完了します



○STEP 2：DCV画面へのアクセス

申請完了後のオーダー詳細画面上で「ドメイン名の利用権を確認」リンクをクリックします



○STEP 3：認証トークンの入手

DCV画面に認証トークンの値が表示されます。テキストエディタを用いて、この値を含む「fileauth.txt」という名称のテキストファイル（認証トークンファイル）を作成します。

○STEP 4：認証トークンファイルの配置

インターネット経由でアクセス可能なウェブサーバ上の規定の場所に認証トークンファイルを配置し、公開します。

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

取得した認証トークン

※1：<確認対象のドメイン名>はかならず証明書に含む「申請コモンネーム/SANs」すべてに対して個々の認証が必要となります。ワイルドカードをコモンネーム、またはSANsに含む場合は、自動的にDCV Eメールが送付されます。アカウント内「設定」→「選択設定」→「ドメイン認証範囲」の設定は無視されますのでご注意ください。

○例：申請コモンネーム/SANs ＝ sub01.example.comの場合、配置URLは以下となります
→配置URL ＝ http://sub01.example.com/.well-known/pki-validation/fileauth.txt

○STEP 5：認証トークンファイルのチェック

同画面内の「チェックする」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。成功すると、DCVプロセスは完了です

※ 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。

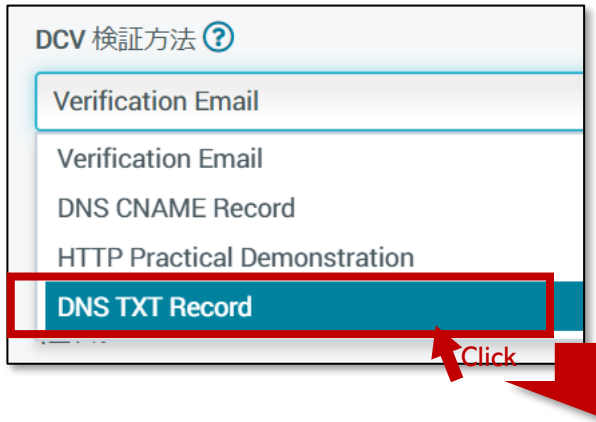
© 2021 DigiCert – All Rights Reserved

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

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

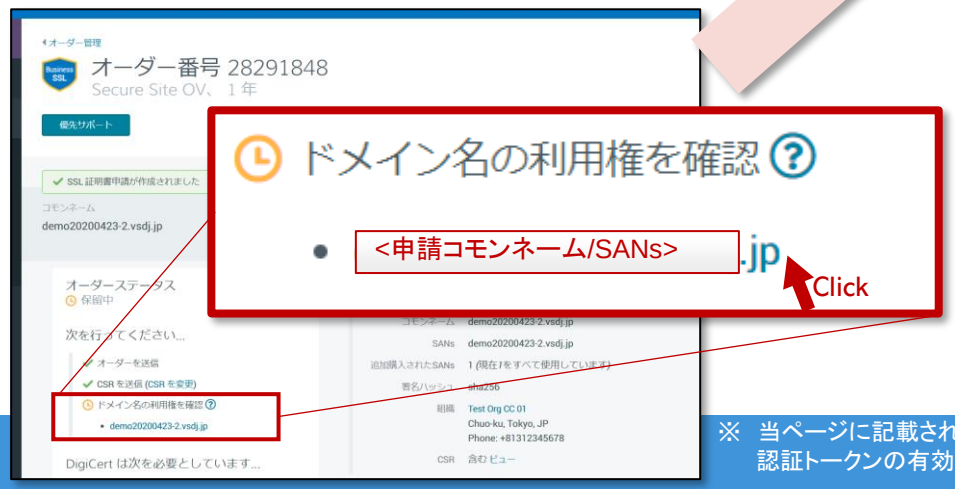
○STEP 1：証明書の申請

申請画面上の「DCV検証方法」欄で「HTTP Practical Demonstration」を選択し、申請を完了します



○STEP 2：DCV画面へのアクセス

申請完了後のオーダー詳細画面上で「ドメイン名の利用権を確認」リンクをクリックします



○STEP 3：認証トークンの入手

DCV画面を開いて画面中央部の「トークン」欄をクリックして、DNS TXTレコードに設定する認証トークンを入手します

○STEP 4：認証トークンの配置

STEP 3で取得した認証トークンを値(Value)として、確認対象のドメイン名のDNS TXTリソースレコードを設定します。

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

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

○STEP 5：認証トークンのチェック

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

※ 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。

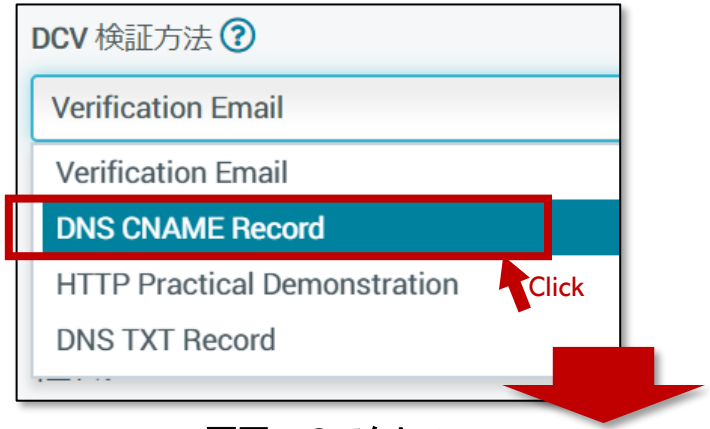
© 2021 DigiCert – All Rights Reserved

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

■DNS CNAME認証用「認証トークン」の取得・利用方法 (**OV/EV証明書のみで選択可**)

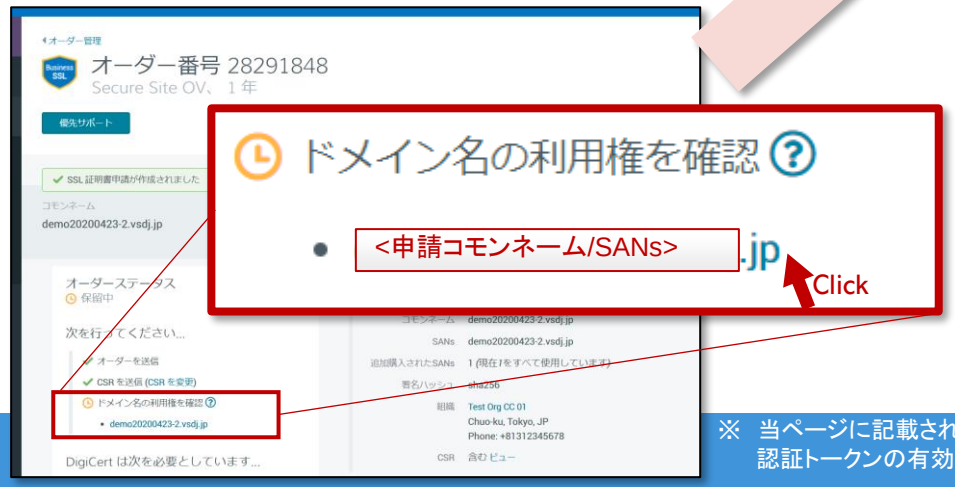
○STEP 1：証明書の申請

申請画面上の「DCV検証方法」欄で「HTTP Practical Demonstration」を選択し、申請を完了します



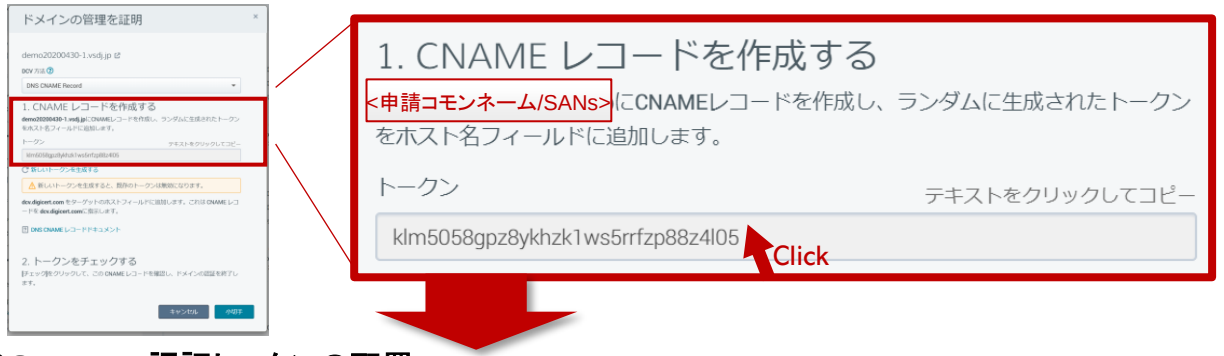
○STEP 2：DCV画面へのアクセス

申請完了後のオーダー詳細画面上で「ドメイン名の利用権を確認」リンクをクリックします



○STEP 3：認証トークンの入手

DCV画面を開いて画面中央部の「トークン」欄をクリックして、DNS CNAMEレコードに設定する認証トークンを入手します



○STEP 4：認証トークンの配置

STEP 3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

NAME	TYPE	VALUE
取得した認証トークン.<確認対象のドメイン名(※1)>	CNAME	dcv.digicert.com

※1：<確認対象のドメイン名>は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、証明書申請内容ならびにアカウント内「設定」→「選択設定」→「ドメイン認証範囲」の設定によって決定されます。

○例：申請コモンネーム/SANs ＝ sub01.example.comの場合、<確認対象のドメイン名>は以下となります
- →「ドメイン認証範囲」＝「Submit base domains for validation」の場合
  - →<確認対象のドメイン名> ＝ example.com
- →「ドメイン認証範囲」＝「認証する正確なドメイン名を提出する」の場合
  - →<確認対象のドメイン名> ＝ sub01.example.com

○STEP 5：認証トークンのチェック

同画面内の「チェックする」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設定されているか確認します。成功すると、DCVプロセスは完了です

※ 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。

© 2021 DigiCert – All Rights Reserved

2. OV/EV証明書の申請

~ 2.4 （参考）組織およびドメイン名の管理 ~

当セクションの内容は、「事前認証」方式を採用する場合の手順となります。

「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 Partner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。

「都度認証」(各証明書申請のタイミングで組織認証/DCVを実施する)方式のみをご利用の場合は、当セクションは
スキップいただけます。

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。

© 2021 DigiCert – All Rights Reserved

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

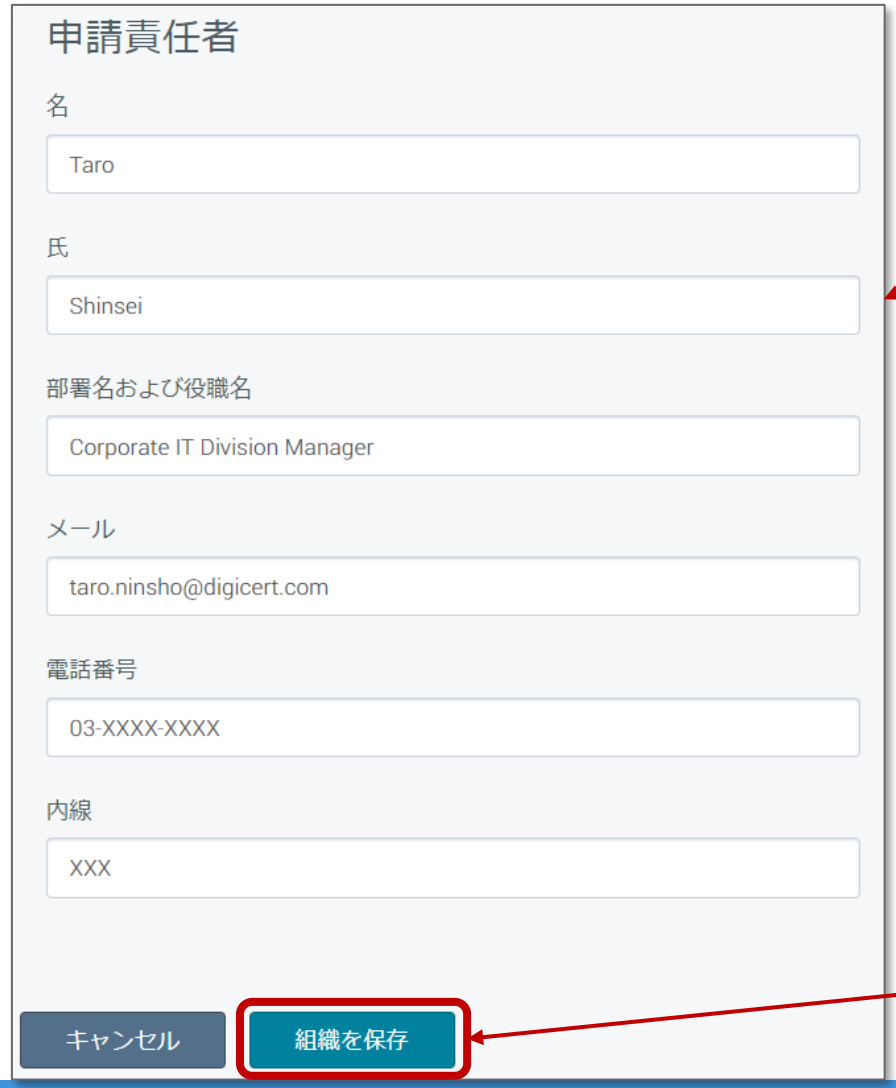
その他のパターンの記入例については以下のFAQを併せてご参照ください。
https://knowledge.digicert.com/ja/jp/solution/SO22977.html

※ 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。

© 2021 DigiCert – All Rights Reserved

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 Partner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 Partner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。

© 2021 DigiCert – All Rights Reserved

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：ご契約条件等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。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

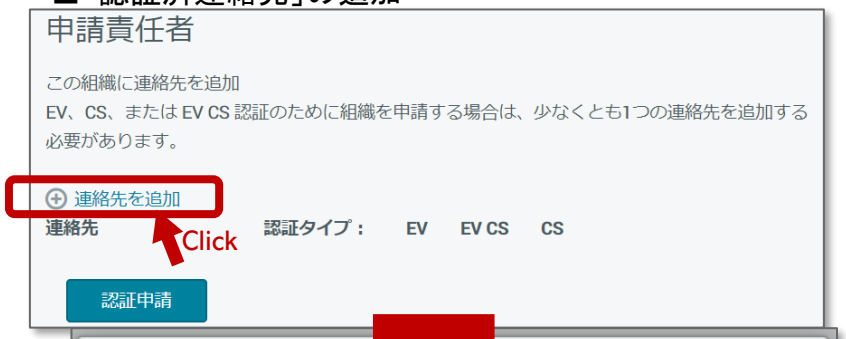
・【「EV」、「CS」または「EVCS」を含む場合】
「連絡先を追加」をクリックして「認証済連絡先」(Verified Contact)」を追加します
次ページのガイドに従って入力してください

・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

© 2021 DigiCert – All Rights Reserved

組織(Organization)の管理 – 「認証済連絡先」の追加

■「認証済連絡先」の追加



■「新しい連絡先」選択時

■認証済連絡先を追加いただく方法

「既存の連絡先」：CertCentralのお客様のアカウントに登録されたユーザーの一覧の中から「認証済連絡先」として認証する担当者を選択します。

「新しい連絡先(*1)」：認証済連絡先をとして認証する担当者の情報を新規に登録します。以下の入力例を参考にして入力してください。

項目名	概要	入力例
名	認証済連絡先として認証する担当者の名	Taro (※1)
氏	同担当者の氏	Shinsei (※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	同担当者の電子メールアドレス	taro.shinsei@example.com
電話番号	同担当者の電話番号	+81-3-XXXX-XXXX
内線	【任意】同担当者の内線番号	XXX

*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。

「追加」ボタンを押下して認証済連絡先の情報を保存してください。

※ 認証済連絡先を有効化するためには前ページのガイドに沿って**「認証申請」**の操作をいただく必要がありますのでご注意ください。

※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。

© 2021 DigiCert – All Rights Reserved

ドメイン名(Domain)の管理 – 新しいドメイン名の登録 (1/3)

■「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。
(初期状態では空欄です)

・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追加の認証(DCV)申請を行う場合：
→一覧に表示された組織を選択して「ドメイン詳細/認証申請」画面に進んでください。

© 2021 DigiCert – All Rights Reserved

ドメイン名(Domain)の管理 – 新しいドメイン名の登録 (2/3)

■「ドメイン詳細/認証申請」画面

・[新しいドメイン]画面の上段の[ドメイン名]欄に、事前認証(DCV)を行う対象のドメイン名を入力してください。

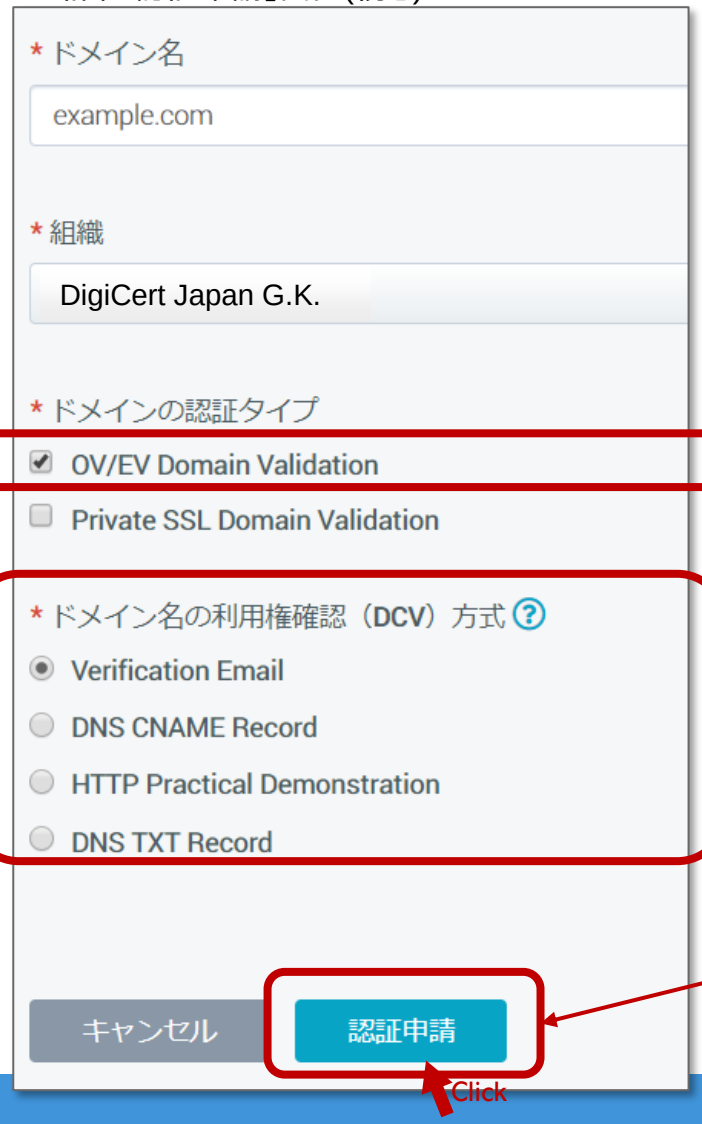
・下段の[組織]欄に、ドメイン名の利用確認(DCV)をおこなう対象の組織名を選択してください。

次ページに進みます

© 2021 DigiCert – All Rights Reserved

ドメイン名(Domain)の管理 – 新しいドメイン名の登録 (3/3)

■「ドメイン詳細/認証申請」画面(続き)



・続けて表示される[ドメインの認証タイプ(OV/EVなど)] を選択してください。
※ CertCentralでは企業認証(OV)およびEV SSL証明書用のDCVは統合され、単一のDCVプロセスで両方の認証をカバーすることができます。

・続けて表示される [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**セクション2.3**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。
→弊社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。

© 2021 DigiCert – All Rights Reserved

3. DV証明書の申請

~ 3.1 ワークフロー概要 ~

CertCentral PartnerにおけるDV証明書の申請ワークフロー概要 (DCV方式：メール認証)

タスク概要	内容	CertCentral		エンドユーザ企業	
		メニュー操作	備考	申請責任者	ドメイン名管理者
事前準備	・CSR生成、ドメイン名利用権確認(DCV)方法の決定 ・(必要に応じて)ドメイン名管理者の確認、事前調整	特にメニュー操作不要		N/A	N/A
証明書の申請	・製品を選択し証明書を申請 ・DCV方法の指定(メール認証) ・DCVメール配信先の指定、メール送信	[証明書の申請]	セクション 3.2 参照	N/A	DCVメール受信・承認
認証 ドメイン利用権確認(DCV)	・(必要に応じて)DCVメールの再送信	[証明書]→[オーダー] →[オーダー詳細]	セクション 3.2 参照	N/A	DCVメール受信・承認
証明書の取得	・発行された証明書を形式を指定して取得(ダウンロード)	[証明書]→[オーダー] →[オーダー詳細]	セクション 5 参照	N/A	N/A

© 2021 DigiCert – All Rights Reserved

CertCentral PartnerにおけるDV証明書の申請ワークフロー概要 (DCV方式：ファイル認証/DNS認証)

タスク概要	内容	CertCentral		エンドユーザ企業	
		メニュー操作	備考	申請責任者	ドメイン名管理者
事前準備	・CSR生成、ドメイン名利用権確認(DCV)方法の決定	特にメニュー操作不要		N/A	N/A
証明書の申請	・製品を選択し証明書を申請 ・DCV方法の指定(ファイル認証/DNS認証)	**[証明書の申請]**	セクション 3.2 参照	N/A	N/A
認証 ドメイン利用権確認(DCV)	・認証トークンの取得・配置 ・ファイル/DNS認証のための(再)ポーリング指示	**[証明書]→[オーダー] →[オーダー詳細]**	セクション 3.2 参照	N/A	N/A
証明書の取得	・発行された証明書を形式を指定して取得(ダウンロード)	**[証明書]→[オーダー] →[オーダー詳細]**	セクション 5 参照	N/A	N/A

© 2021 DigiCert – All Rights Reserved

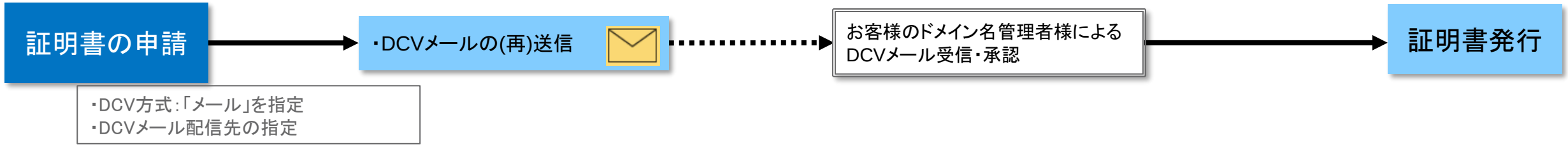
DV証明書の申請～認証までのご申請手続きとシステム処理概要
(DCV方式：メール認証)

: 自動的に次の処理へ進む
: 次の手続きが必要
: CertCentralでのご申請手続き
: システムの内部的な処理
: 条件分岐

申請前の状態

同一Orgの
事前登録なし

同一ドメイン名の
事前登録なし



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

© 2021 DigiCert – All Rights Reserved

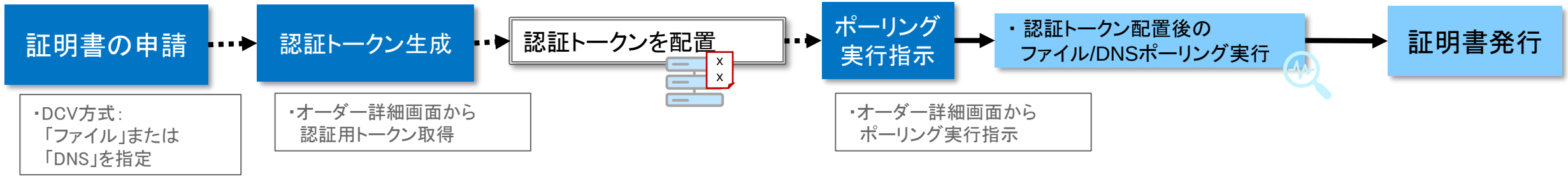
DV証明書の申請～認証までのご申請手続きとシステム処理概要
(DCV方式：ファイル認証/DNS認証)

: 自動的に次の処理へ進む
: 次の手続きが必要
: CertCentralでのご申請手続き
: システムの内部的な処理
: 条件分岐

申請前の状態

同一Orgの
事前登録なし

同一ドメイン名の
事前登録なし



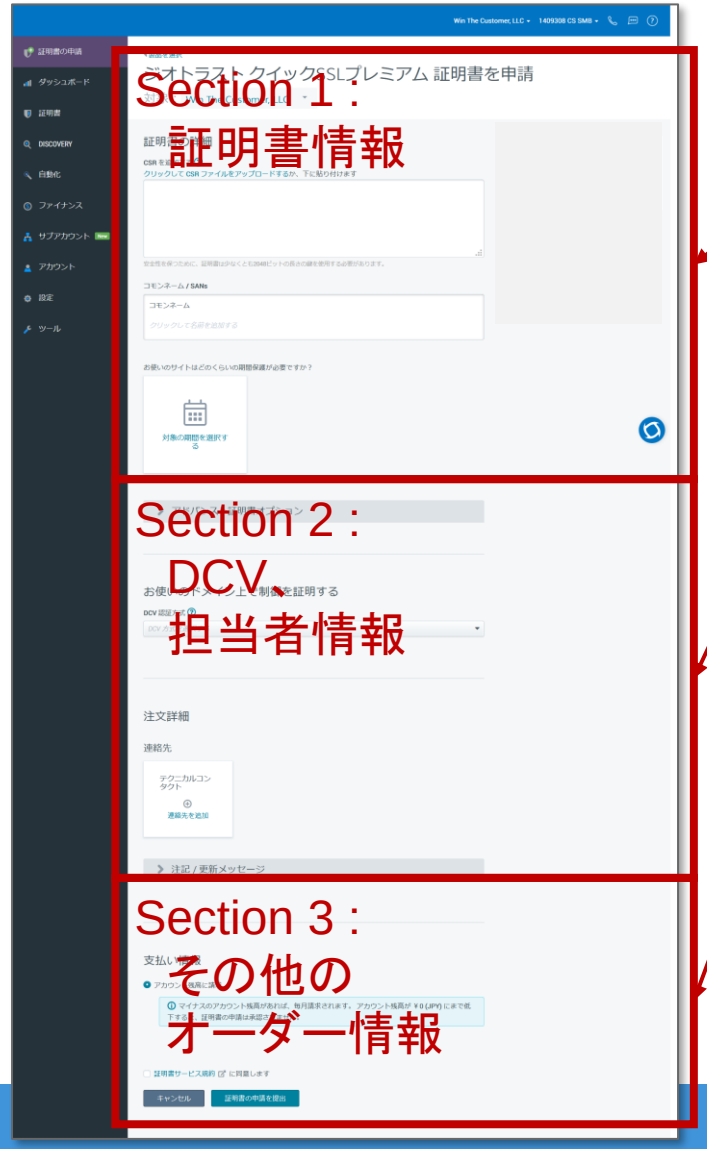
© 2021 DigiCert – All Rights Reserved

3. DV証明書の申請

~ 3.2 DV証明書の申請 ~

DV証明書の申請画面（新規申請/更新申請 共通）

■「証明書の申請」メニューからDV証明書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

Section 2：次にDCV方式の指定、技術担当者情報を入力します。
- ドメイン名利用権確認(DCV)の方式指定
- 技術担当者情報

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

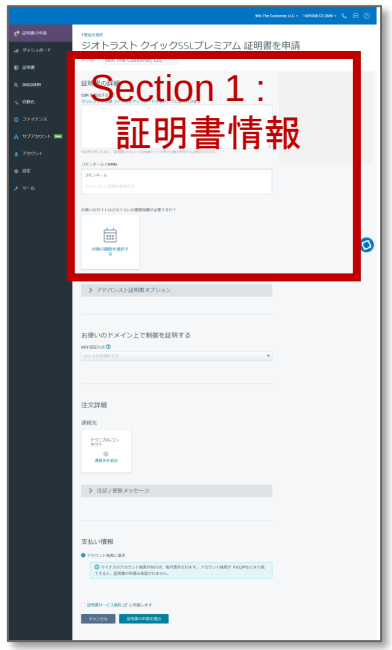
次ページ以降で詳細な入力方法をガイドします。

© 2021 DigiCert – All Rights Reserved

DV証明書 新規申請 Section 1：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て証明書を申請す場合は
クリックして表示されるプルダウンリストから選択してください。

■【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。
・SANs欄の入力数量には上限がある場合があります(※1)。
・SANs入力される値により費用が変動します(※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、1年間~6年間からご選択ください
・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、※3)。
→詳細は page 14 [補足 プランの選択]をご参照ください

※1：通常は最大255のSANsを入力可能です。また【バウチャー】を用いた申請時には、バウチャー生成時に指定した上限が設定されますのでご注意ください。
※2：FAQ「(DV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/SO24206.html
※3：【バウチャー】を用いた申請時にはプランの期間は自動的に設定されます

© 2021 DigiCert – All Rights Reserved

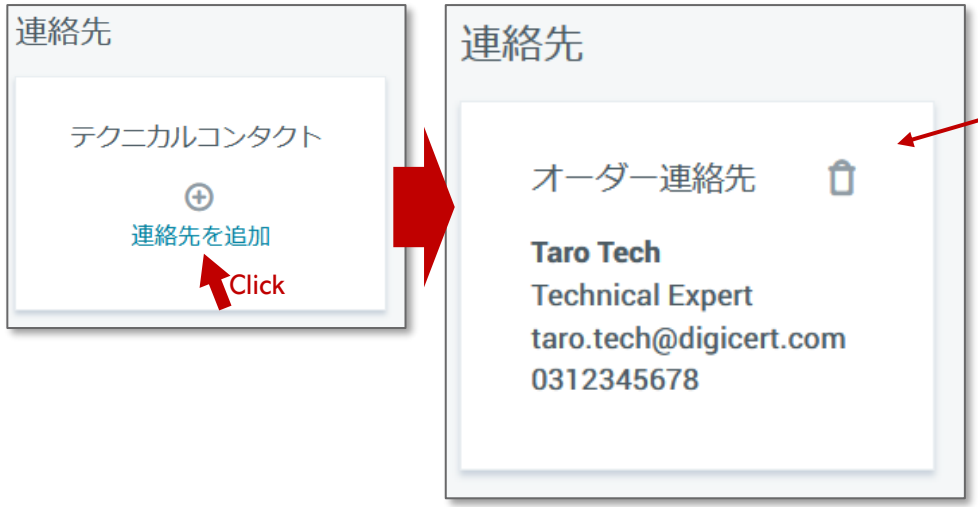
DV証明書 新規申請 Section 2 : DCV、担当者情報の入力

■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」

■DCV方式の選択(「メール」選択時)

■技術担当者情報入力欄



■【必須】DCV方式の選択
ドメイン名利用権確認(DCV)の方式を以下から選択します。
・DNS TXT
・ファイル
・メール
(メールを選択時にはDCVメールの言語を下部に選択されるプルダウンから選択いただけます。日本語のDCVメールをご希望の場合は「Japanese」を選択してください)

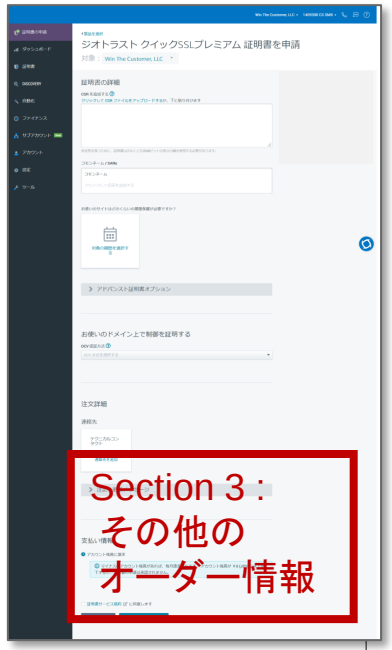
■【任意】オーダー連絡先(技術担当者)情報
・技術担当者情報を入力します。技術担当者には必要に応じてデジサートからご申請に関する連絡を差し上げる場合があります
・オーダー連絡先(技術担当者)を指定しない場合は、申請ユーザーが技術担当者として自動的にアサインされます

© 2021 DigiCert – All Rights Reserved

DV証明書 新規申請 Section 3 : 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。

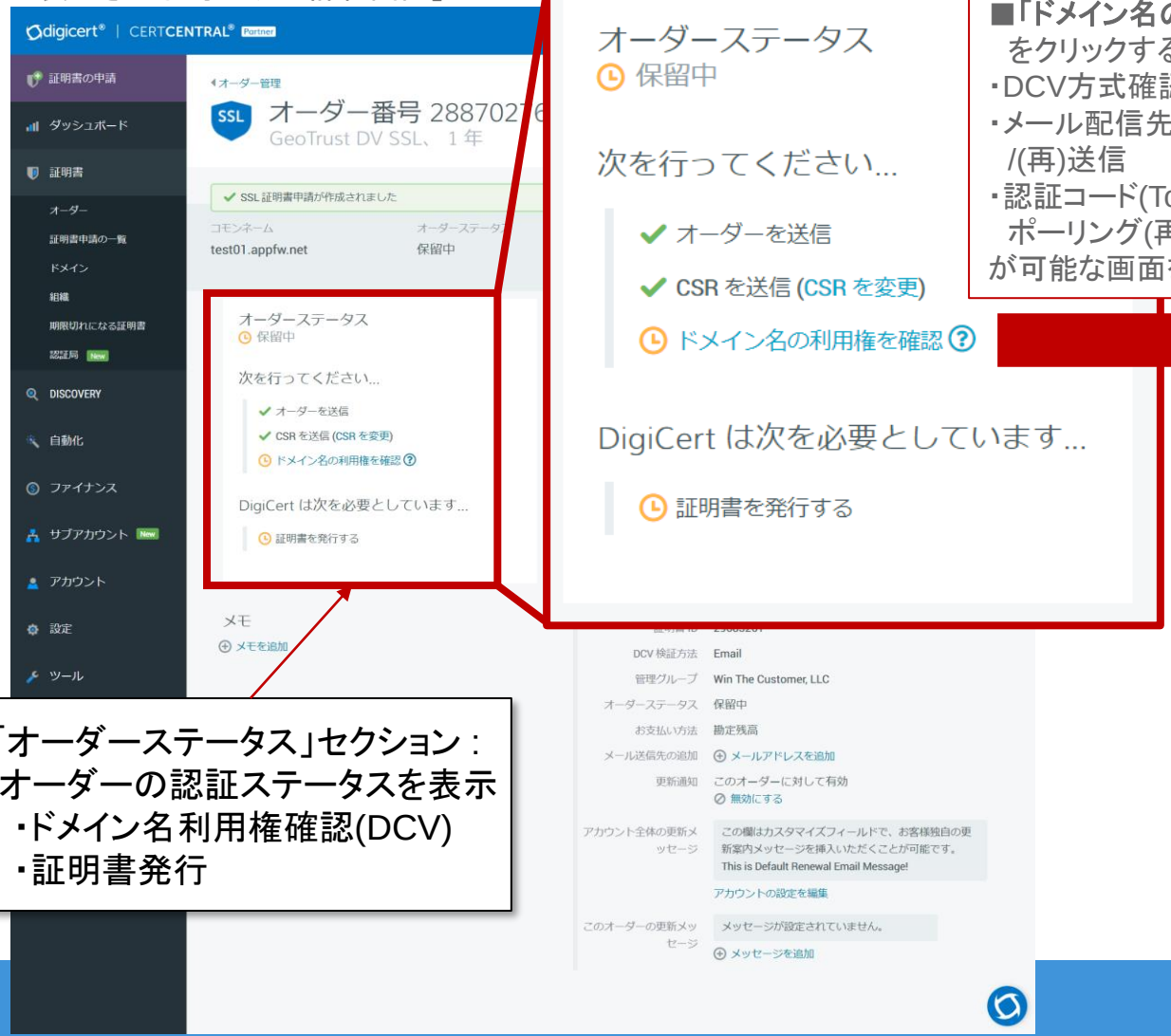
■【必須】証明書サービス規約
リンク先の規約をご確認いただき、チェックボックス=ONにしてください。

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。

© 2021 DigiCert – All Rights Reserved

オーダー詳細確認～ドメイン名利用権確認

■「証明書」→「オーダー」メニューから
DV SSL証明書のオーダー選択後に
表示される「オーダー詳細画面」



■「ドメイン名の利用権を確認」
をクリックすると…
・DCV方式確認/変更
・メール配信先確認、変更、
/(再)送信
・認証コード(Token)確認/
ポーリング(再)実行
が可能な画面を表示

「オーダーステータス」セクション：
オーダーの認証ステータスを表示
・ドメイン名利用権確認(DCV)
・証明書発行

© 2021 DigiCert – All Rights Reserved

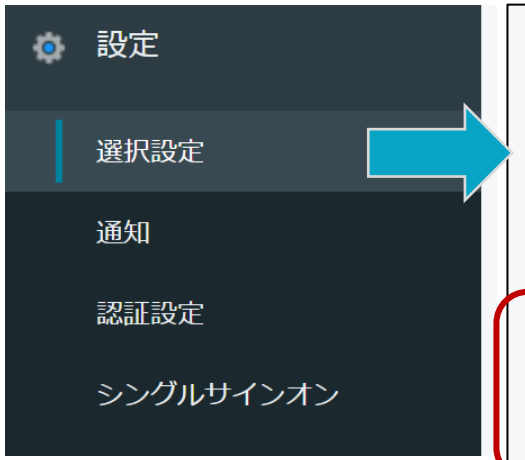
各DCV方式の詳細 – 「メール認証」の場合 (1/3 : 送信先の選択ルール)

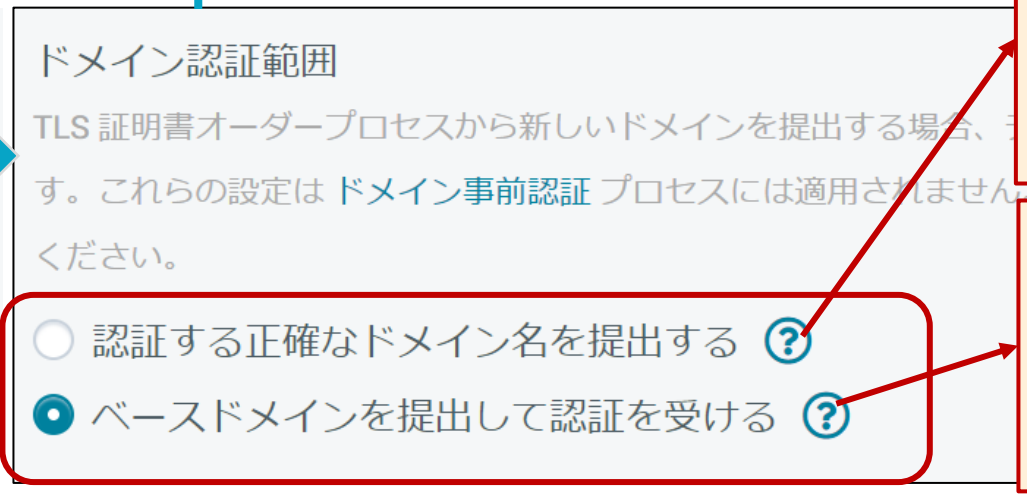
■DV証明書のDCVメールの送信先は以下の組み合わせによって決定されます。

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

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

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





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

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

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

© 2021 DigiCert – All Rights Reserved

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

<table>
<tr><th>アカウント設定</th><th>申請コモンネーム/SANs</th><th>DCVメール仕様 (※1)</th></tr>
<tr><td rowspan="2">A1:「ベースドメインを提出して認証を受ける」
(推奨、デフォルト設定)</td><td>B1: example.com の場合</td><td rowspan="2">DCVメールは以下の全てのメールアドレスに送信されます
区分 / DCVメール宛先
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</td></tr>
<tr><td>B2: sub01.example.com の場合</td></tr>
<tr><td rowspan="2">A2:「認証する正確なドメイン名を提出する」</td><td>B1: example.com の場合</td><td>DCVメールは以下の全てのメールアドレスに送信されます
区分 / DCVメール宛先
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</td></tr>
<tr><td>B2: sub01.example.com の場合</td><td>DCVメールは以下の全てのメールアドレスに送信されます
区分 / DCVメール宛先
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</td></tr>
</table>

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

© 2021 DigiCert – All Rights Reserved

各DCV方式の詳細 – 「メール認証」の場合 (3/3 : メール文面)

■DCVメール(**DV証明書用**)の概要

→メール件名、送信元および本文イメージは、以下のようになります
(証明書申請画面内の「DCV Email Language」において
「Japanese(日本語)」を選択いただいた場合)

件名	[Domain Approval] ドメイン名の利用権確認のお願い: [確認対象のドメイン名(※1)]
送信元	no-reply@geotrust.com
本文 イメージ (抜粋)	デジサートでは、GeoTrustSSL/TLSサーバ証明書、S/MIME証明書等デジタル証明書の発行前に必要となるドメイン名利用権の確認を実施しております。 (中略) ご担当者様が、ドメイン名[確認対象のドメイン名(※1)]の所有者または管理者であることをご確認いただいた上で、SSL/TLSサーバ証明書、またはS/MIME用証明書に当該ドメイン名を利用することをご承認ください。 下記URLにアクセスし、ウェブページ上の内容をよくお読みになり、「承認する」のボタンをクリックしてください。（当ウェブページへのリンクの有効期間は30日間です。）： https://dcv.geotrust.com/link/domain-control-validation/?t=<ランダムな認証トークン(※3)> Click

■DCV承認画面(**DV証明書用**)イメージ

→DCV承認画面(日本語)のイメージは以下のようになります(※3)

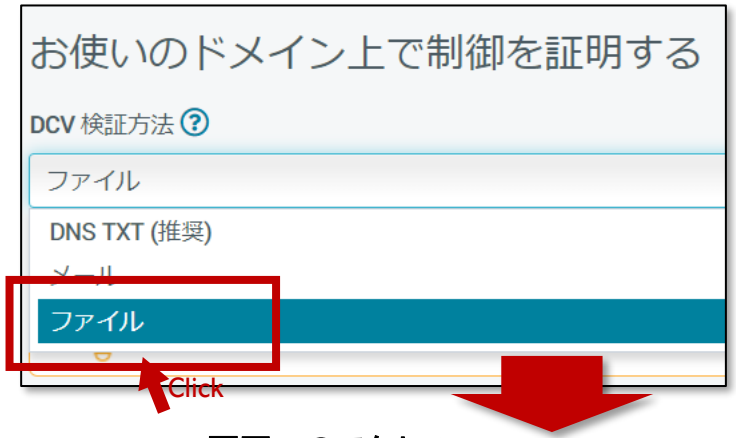
※1 : 確認対象のドメイン名は「申請コモンネーム/SANs」または「ベースドメイン名」のいずれかとなり、申請内容ならびに前ページに記載のアカウント設定によって決定されます。
※2 : 承認画面の表示言語は画面上部の「言語」欄から選択いただき切り替えることが可能です。
※3 : 認証トークンの有効期間は30日間となります。一度使用した認証トークンは再利用できません。DCVメールを紛失した場合はCertCentralから再送いただくことが可能です。

© 2021 DigiCert – All Rights Reserved

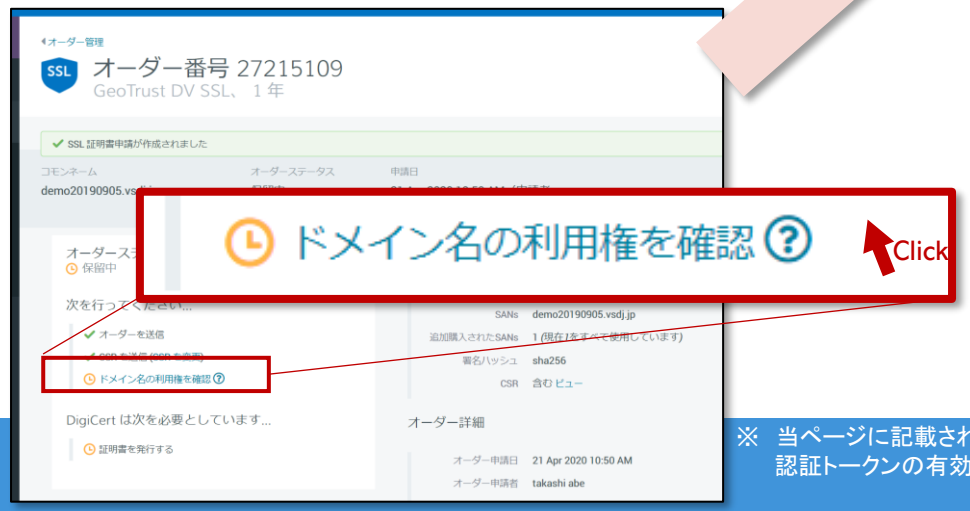
各DCV方式の詳細 – 「ファイル認証」の場合

■ファイル認証用「認証トークン」の取得・利用方法 (DV証明書の場合)

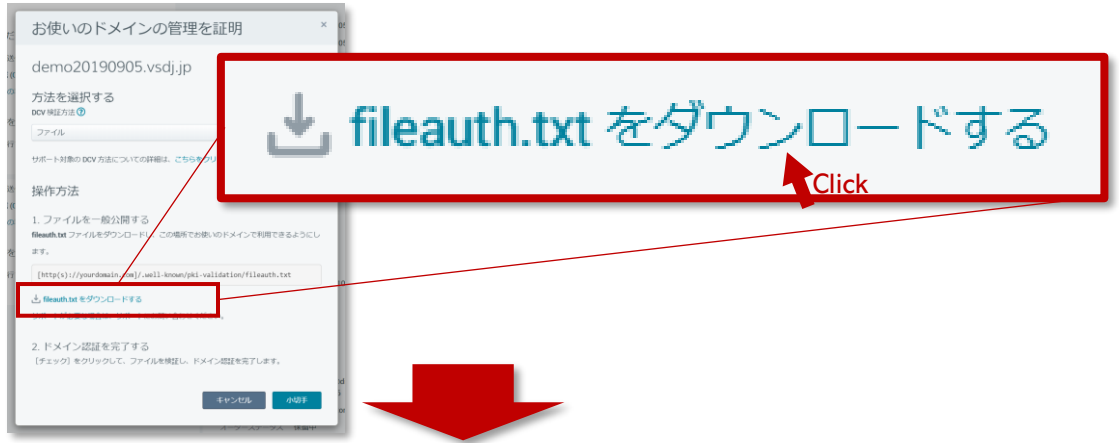
○STEP 1：証明書の申請
申請画面上の「DCV検証方法」欄で「ファイル」を選択し、申請を完了します



○STEP 2：DCV画面へのアクセス
申請完了後のオーダー詳細画面上で
「ドメイン名の利用権を確認」リンクをクリックします



○STEP 3：認証トークンファイルのダウンロード
DCV画面を開いて画面下部の「fileauth.txtをダウンロードする」をクリックして、
ウェブサーバに配置する認証トークンファイルを入手します



○STEP 4：認証トークンファイルの配置
インターネット経由でアクセス可能なウェブサーバ上の規定の場所に、
認証トークンファイルを配置します。

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

取得した
認証トークン

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

○STEP 5：認証トークンファイルのチェック
同画面内の「チェックする」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。成功すると、DCVプロセスは完了です

※ 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。

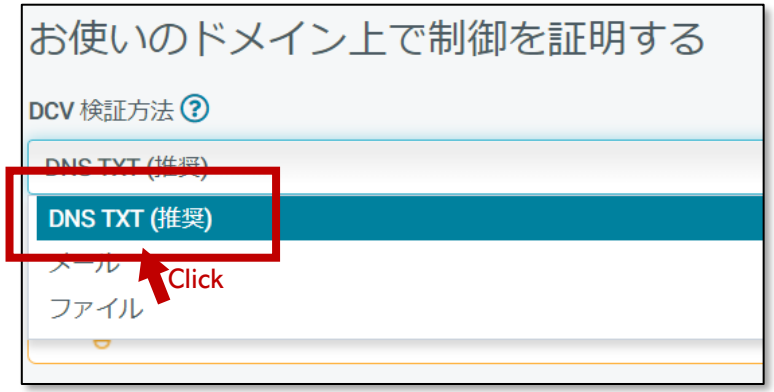
© 2021 DigiCert – All Rights Reserved

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

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

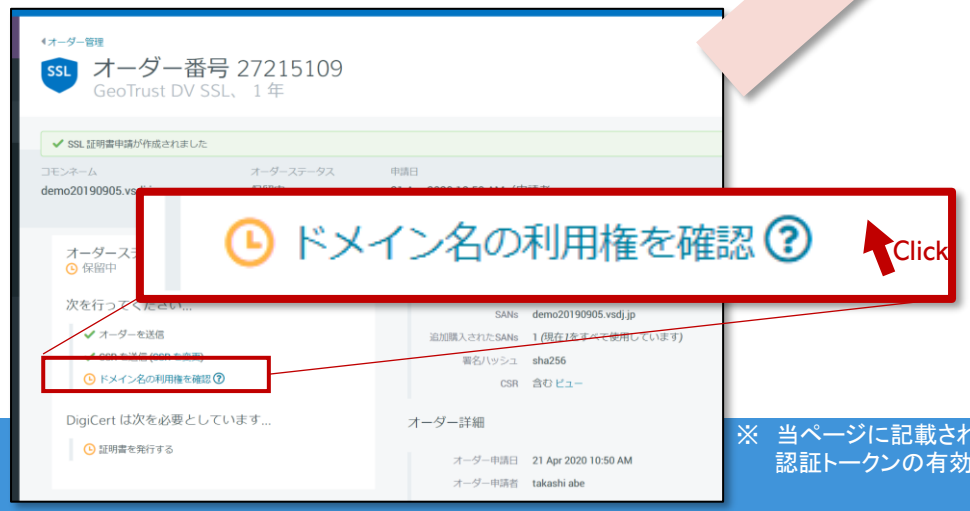
○STEP 1：証明書の申請

申請画面上の「DCV検証方法」欄で「DNS TXT」を選択し、申請を完了します



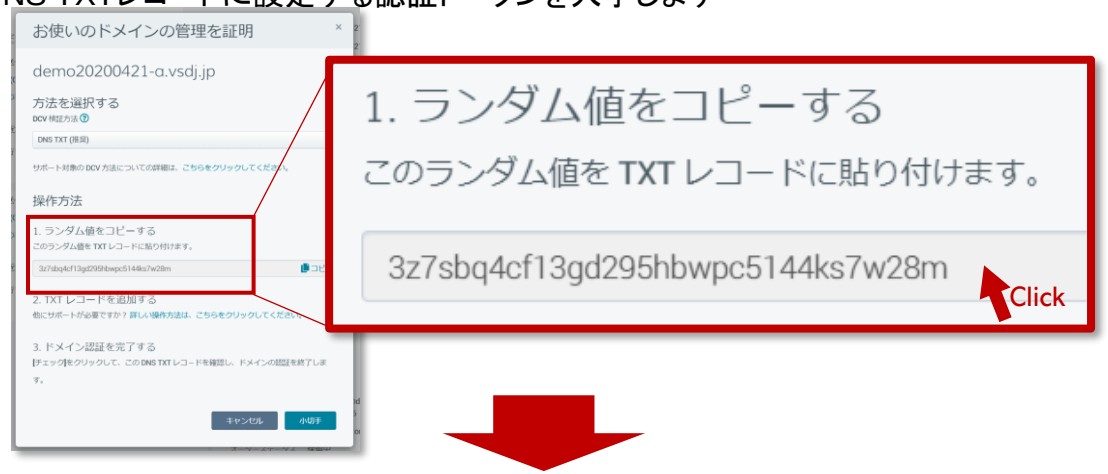
○STEP 2：DCV画面へのアクセス

申請完了後のオーダー詳細画面上で
「ドメイン名の利用権を確認」リンクをクリックします



○STEP 3：認証トークンの入手

DCV画面を開いて画面中央部の「ランダム値をコピーする」をクリックして、
DNS TXTレコードに設定する認証トークンを入手します



○STEP 4：認証トークンの配置

STEP 3で取得した認証トークンを値(Value)として、確認対象のドメイン名のDNS TXT
リソースレコードを設定します。

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

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

○STEP 5：認証トークンのチェック

同画面内の「チェックする」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
レコードに認証トークンが設定されているか確認します。成功すると、DCVプロセスは完了です

※ 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。

© 2021 DigiCert – All Rights Reserved

4. オーダー・証明書ステータス管理

「証明書」メニューの概要

■「証明書」メニュー

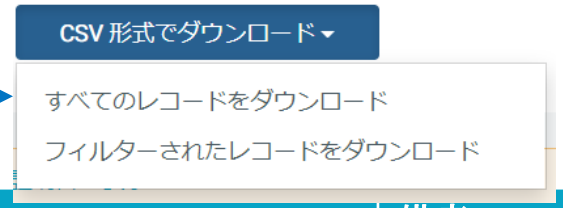
メニュー名称	機能説明	備考
オーダー	・オーダー(証明書注文単位)の一覧表示、検索 ・オーダーレポートの出力 ・(一覧から)オーダー詳細確認・管理(再発行、失効等)	詳細後述
証明書申請の一覧	・「承認待ち」リクエストの一覧表示、検索 (証明書発行リクエスト、失効リクエストなど) ・(一覧から)リクエスト詳細確認・管理(承認／却下)	詳細後述
ドメイン	・アカウントに登録済みの**ドメイン名**の一覧表示、検索 ・(一覧から)ドメイン名の詳細表示(認証有効期間など) ・ドメイン名の管理(追加、認証申請、無効化/(再)有効化)	
組織	・アカウントに登録済み**組織**の一覧表示、検索 ・(一覧から)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。

© 2021 DigiCert – All Rights Reserved

「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*	

© 2021 DigiCert – All Rights Reserved

「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

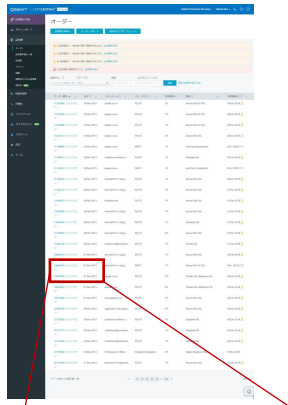
■「高度な検索を表示する」をクリックして表示される検索条件一覧

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）

© 2021 DigiCert – All Rights Reserved

「証明書」→「オーダー」メニューの使い方 (2/2 オーダー詳細確認・管理)

■オーダーー一覧



10864414 クイックビュー

Click

■オーダー詳細画面

・オーダー(証明書申請)に関する詳細情報を確認することができます。
・また、以下の管理機能を利用いただけます。
  ・証明書操作(再発行、失効など)
  ・発行済証明書のダウンロード

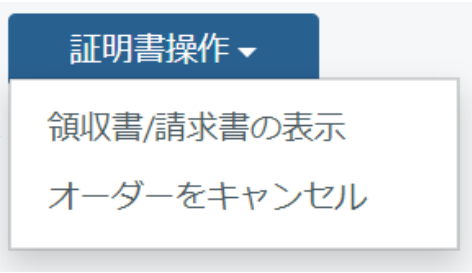
・以下の情報を確認することができます。
  ・オーダーの申請者
  ・オーダーの申請責任者、技術担当者
・また以下の操作が可能です。
  ・メール送信先の追加
  ・更新案内メッセージの編集

© 2021 DigiCert – All Rights Reserved

「証明書」→「オーダー」メニューの使い方 (2/2 オーダー詳細確認・管理)

■オーダー詳細画面

■証明書詳細（**ステータス＝未発行(pending)**の場合）



メニュー	説明
領収書/請求書の表示	***＜利用不可＞***
オーダーをキャンセル	オーダーを（発行前）キャンセル

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証明書の場合)認証済連絡先の確認
- 証明書発行

© 2021 DigiCert – All Rights Reserved

「証明書」→「オーダー」メニューの使い方 (2/2 オーダー詳細確認・管理)

■オーダー詳細画面

Section 1 :
証明書詳細・管理

■証明書詳細（**ステータス＝発行済(issued)**の場合）

証明書の詳細

証明書操作 ▾ | 以下の形式で証明書をダウンロード ▾

コモンネーム <FQDN>
証明書のインストールを確認
VirusTotal でドメインをチェックする
組織 <組織名など 固有の情報>

シリアル番号	0A7BEA3A1B59470EE4CBC77C96F0FD6F
拇印	503448DAACF69B6435F0A36901C8DEB7B4DD574E
署名ハッシュ	sha256
発行認証局	DigiCert SHA2 Secure Server CA
有効期間	30 Jun 2020 - 03 Jul 2020 ⚠
CSR	含む ビュー

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

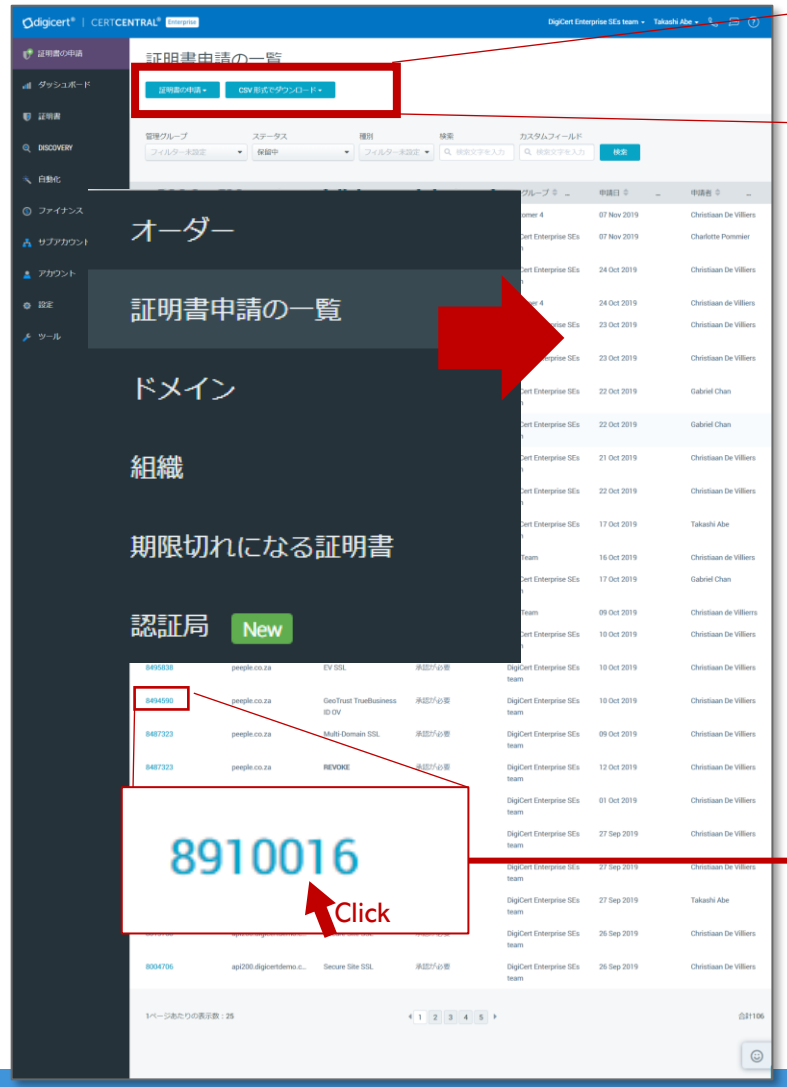
証明書操作 ▾
- 証明書を送信
- 複製発行の申請
- 証明書を再発行
- 証明書を更新
- 証明書を失効
- 領収書/請求書の表示
- サイトシール

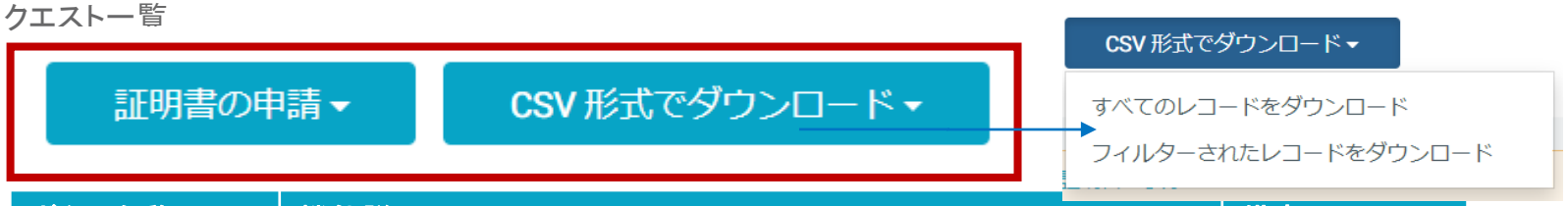
メニュー	説明	備考
証明書を送信	証明書をメールで送信	-
複製発行の申請	証明書の複製(Duplicate)申請画面へ移動	*詳細はセクション 6 を参照*
証明書を再発行	証明書の再発行(Reissue)申請画面へ移動	
証明書を更新	(有効期限の90日前以降の場合のみ) 証明書の更新申請画面へ移動	*詳細はセクション 2.2 を参照*
証明書を失効	証明書の失効申請画面へ移動	*詳細はセクション 6 を参照*
領収書/請求書の表示	*＜利用不可＞*	-
サイトシール	ノートンシール等のサイトシール掲載	*詳細はセクション 10.1 を参照*

© 2021 DigiCert – All Rights Reserved

「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

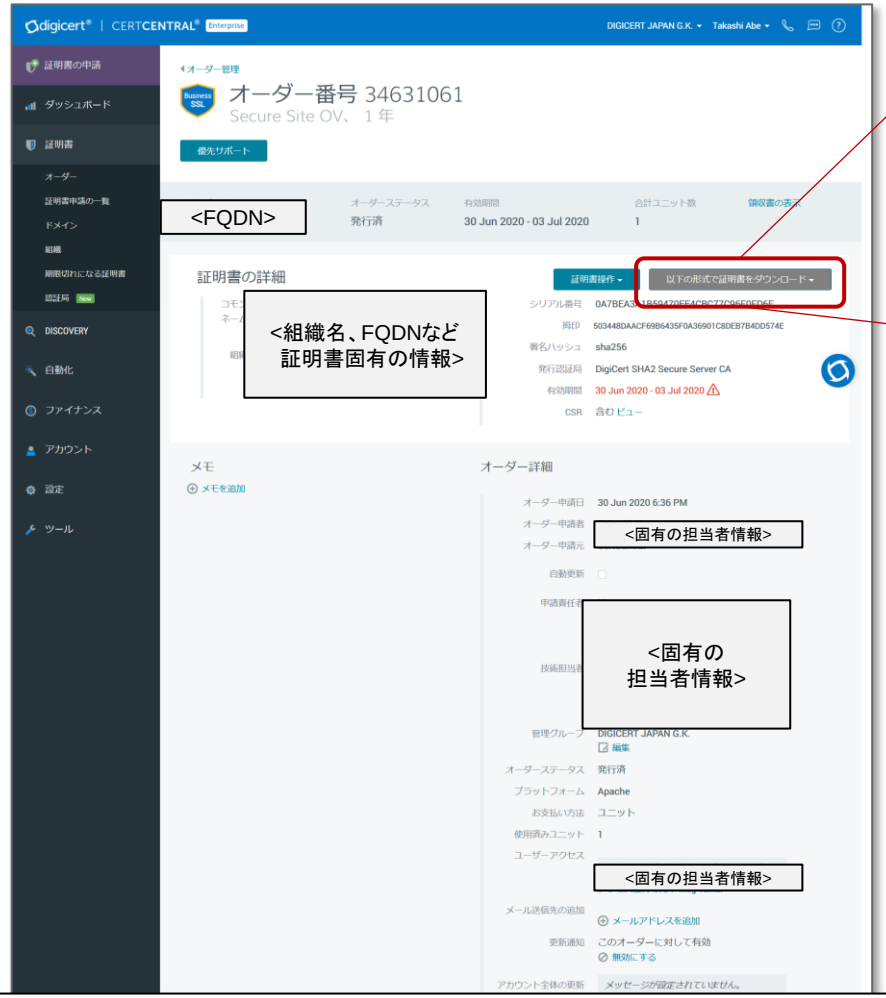
ボタン名称	機能説明	備考
却下	リクエストを却下する	■証明書申請時の「承認」要否について: 【アカウント設定「承認手順」】によって証明書発行リクエストに対する「承認」操作の要否が異なります。 詳細については**セクション2.2 内「アカウント内での申請レビュー・承認について」を参照** ■失効申請時の「承認」要否について: 失効申請の場合は、全ての場合において、管理者による失効リクエストに対する「承認」操作が必要となります。 詳細については**セクション6「失効申請」を参照**
承認	リクエストを承認する	

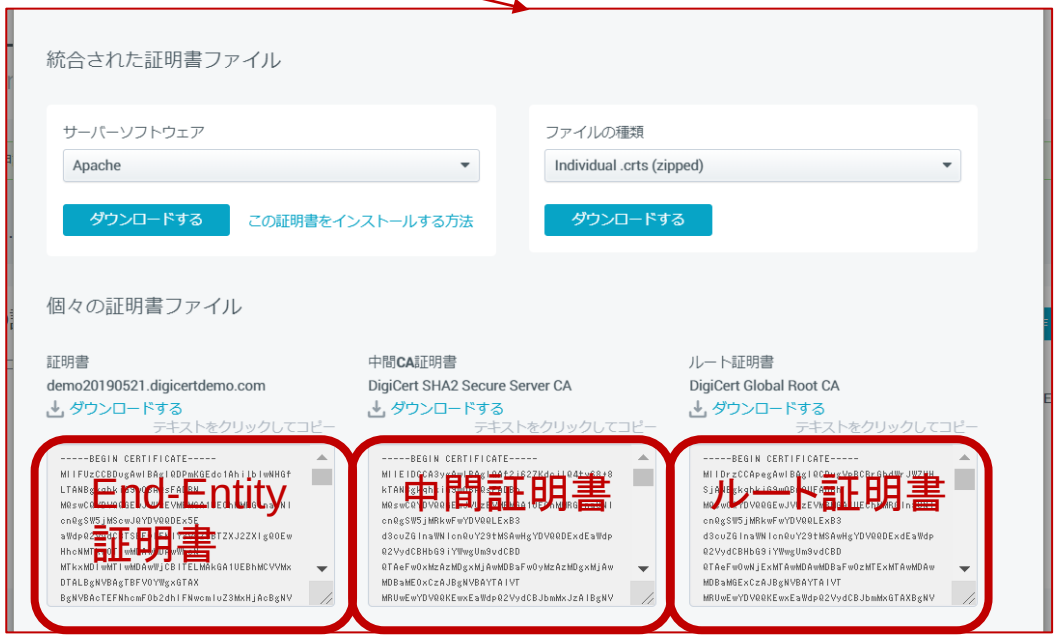
© 2021 DigiCert – All Rights Reserved

5. 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）

■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2.3参照)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3参照)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）

© 2021 DigiCert – All Rights Reserved

発行された証明書の取得（メールを受領）

■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

© 2021 DigiCert – All Rights Reserved

「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

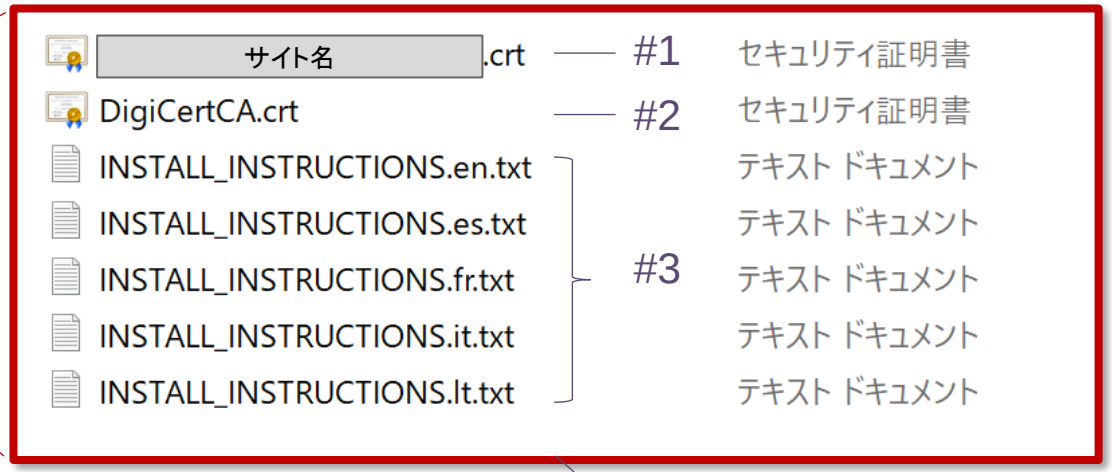
当ページの内容は以下のKnowledgeページの要約となります。上表に記載のないサーバーソフトウェアなど、さらに詳細は以下ページを併せてご参照ください。
・サーバーソフトウェア：https://dev.digicert.com/glossary/#server-platforms (※1:サーバーソフトウェアの一覧はこちらを参照ください)
・ファイル形式について：https://dev.digicert.com/glossary/#certificate-formats (※2:ファイル形式IDの一覧はこちらを参照ください)

© 2021 DigiCert – All Rights Reserved

（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

© 2021 DigiCert – All Rights Reserved

「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

© 2021 DigiCert – All Rights Reserved

（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)

© 2021 DigiCert – All Rights Reserved

6. 再発行、複製、失効等の証明書管理

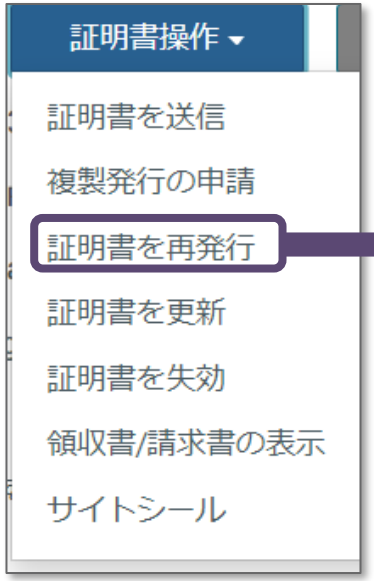
CertCentral における証明書管理ワークフロー概要 (証明書タイプ共通)

タスク概要	内容	CertCentral		エンドユーザ企業	
		メニュー操作	備考	申請責任者	ドメイン名管理者
証明書の再発行	・証明書再発行(Reissue)を申請します ・【複数年プランの場合】証明書有効期間を延長します ・以下の場合、ドメイン利用権確認(DCV)が必要です 【OV/EV証明書の場合】DCV履歴が期限切れの場合のみ 【DV証明書の場合】申請都度、常にDCV実施要 ・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]→[オーダー] →[オーダー詳細] →[証明書操作]**	後述の解説を参照	N/A	(必要な場合) DCVメール 受信・承認
証明書の複製 【※ OV/EV証明書のみ】	・証明書複製(Duplicate)を申請します 【OV/EV証明書の場合のみ】	**[証明書]→[オーダー] →[オーダー詳細] →[証明書操作]**	後述の解説を参照	N/A	N/A
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。 次の管理者による失効申請リクエストの「承認」が必要です。	**[証明書]→[オーダー] →[オーダー詳細] →[証明書操作]**	後述の解説を参照	N/A	N/A
	・失効リクエストの「承認」処理	**[証明書] →[証明書申請の一覧]**			

© 2021 DigiCert – All Rights Reserved

OV/EV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)

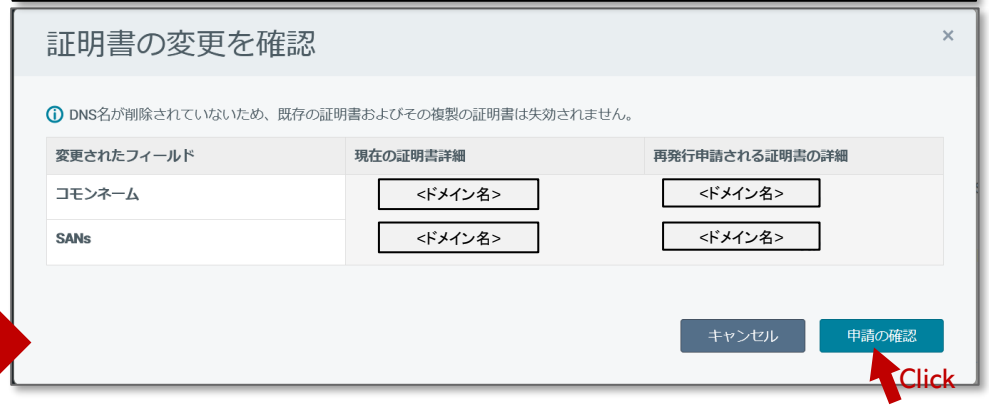
「プランの詳細」で
証明書有効期間を選択・指定します
(詳細は後述の「補足」参照)

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

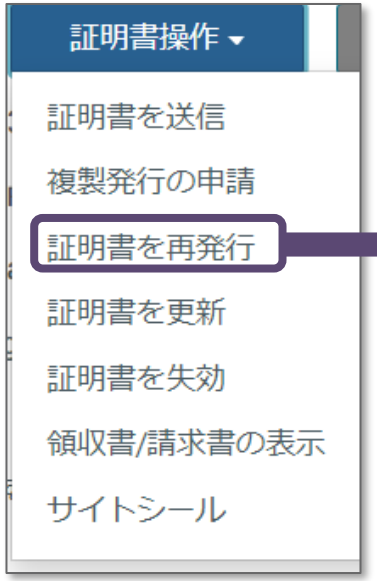
最後に再発行申請内容確認画面が表示されます。
再発行前後の証明書のコモンネーム／SANsの情報を
見比べてご確認いただき、内容に誤りがなければ
「申請の確認」ボタンを押下してください。



© 2021 DigiCert – All Rights Reserved

DV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)

「DCV認証方式」を選択します

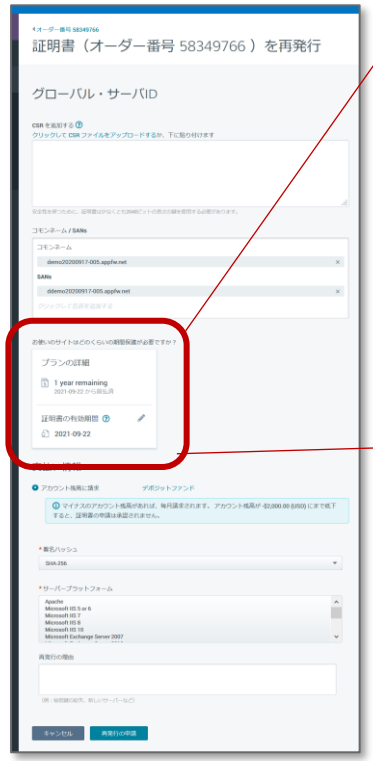
必要に応じて「再発行の理由」
を入力します（任意）

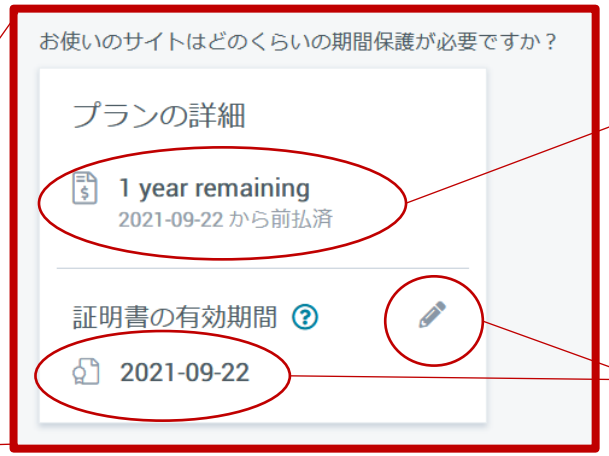
「再発行の申請」ボタンを押下します

© 2021 DigiCert – All Rights Reserved

補足 再発行(Reissue)申請時の「証明書有効期間」について

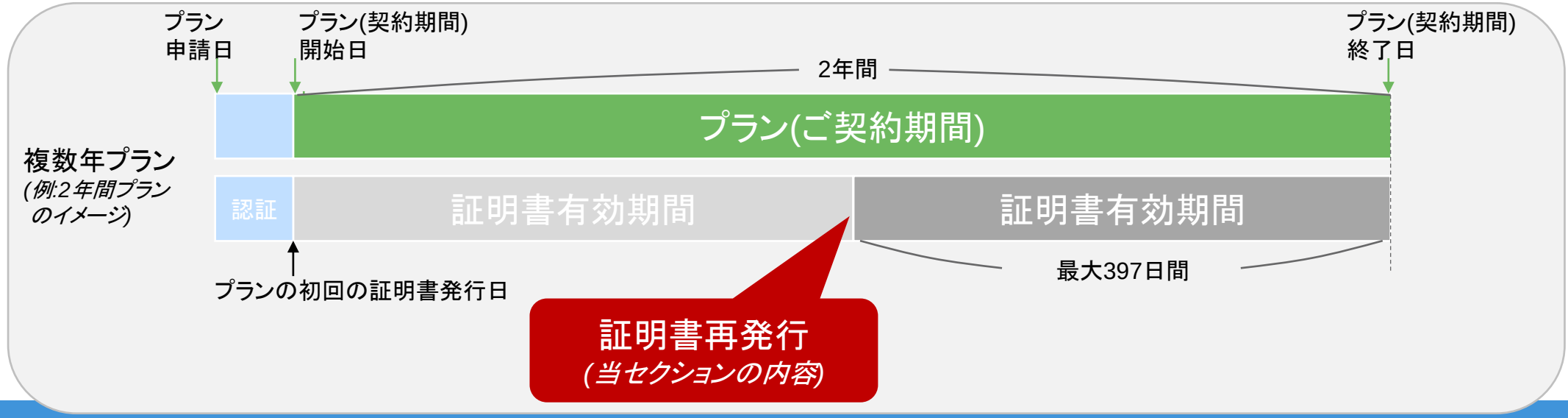
■再発行(Reissue)申請画面





・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。

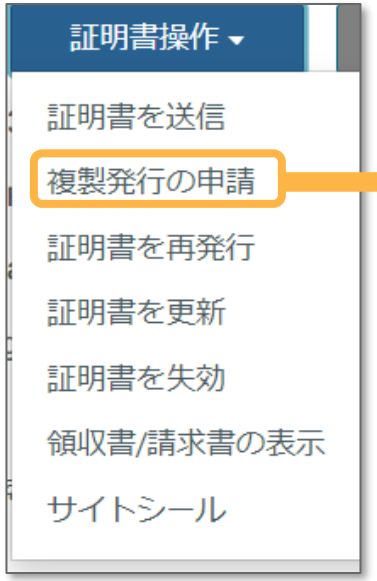
・【証明書の有効期間】の初期設定値は**「プラン(契約期間)終了日」と「397日間」のいずれか早い方**が設定されます
・上部のペンの形のアイコンをクリックすると[証明書の有効期間]を編集いただくことが可能です
・編集後の【証明書の有効期間】の終了日は「プラン(契約期間)終了日」を超えることはできません
・編集後の【証明書の有効期間】は「397日間」を超えることはできません
・再発行申請によってプラン(ご契約期間)を延長することはできません



© 2021 DigiCert – All Rights Reserved

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。

© 2021 DigiCert – All Rights Reserved

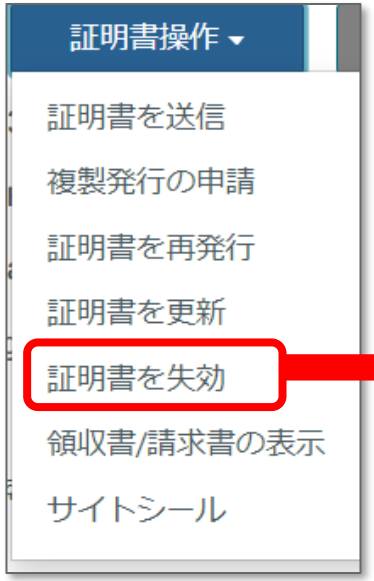
（補足）証明書の「再発行」 と「複製」の違い

	再発行(Reissue)	複製(Duplicate)
対象製品	・OV/EV証明書 ・DV証明書	OV/EV証明書のみ
主な用途	・証明書の更新(有効期間延長) ・コモンネーム／SANsの追加/変更/削除 ・鍵/署名アルゴリズムの変更	鍵/署名アルゴリズムの変更
コモンネーム／SANsの変更	可能（注：下記「費用」を参照）	不可
証明書有効期間終了日の変更	可能（注：指定可能な証明書有効期間終了日の制限について 別紙「再発行(Reissue)申請時の証明書有効期間について」参照	不可
費用	FQDN(SANs)を追加する場合に必要 （注：バウチャーのご利用時など、一部のご契約体系では、 プラン途中でのFQDN(SANs)が不可である場合があります）	・なし
元証明書が失効されるか?	コモンネーム／SANsを変更/削除した場合、 元証明書は48-72時間以内に失効されます	・失効されない

© 2021 DigiCert – All Rights Reserved

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。

© 2021 DigiCert – All Rights Reserved

「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

© 2021 DigiCert – All Rights Reserved

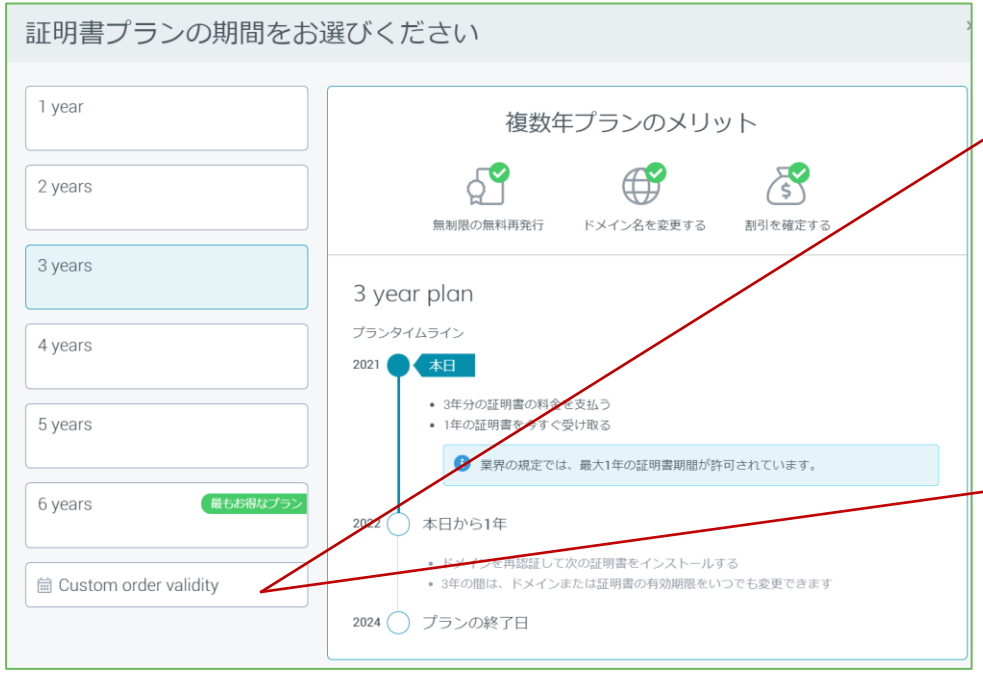
7. プラン・証明書の有効期間、更新案内メールについて

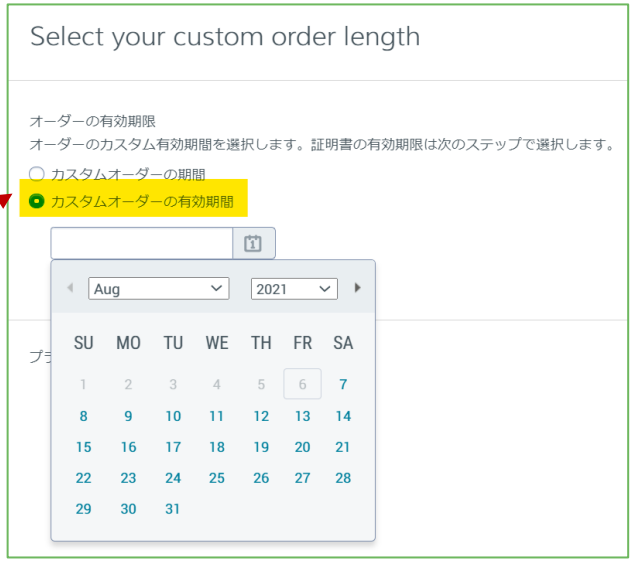
【サーバ証明書(OV/EV共通)】新規・更新申請 - プランおよび証明書の有効期間①

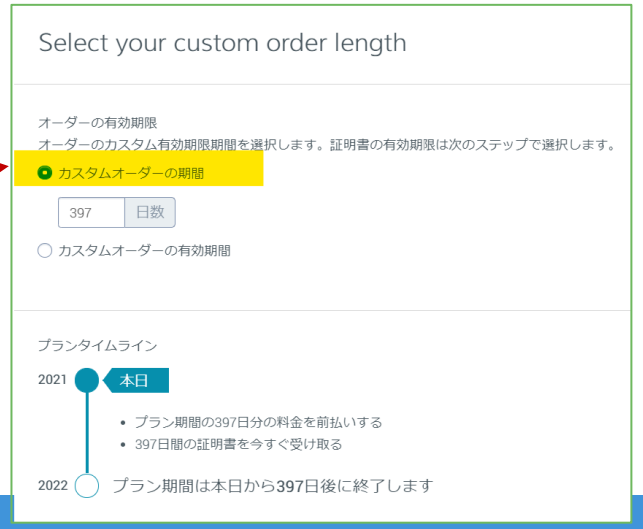
■**サーバ証明書(OV/EV) 新規・更新申請で**設定されるプラン期間および証明書有効期間については以下Knowledgeをご参照ください。

[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。





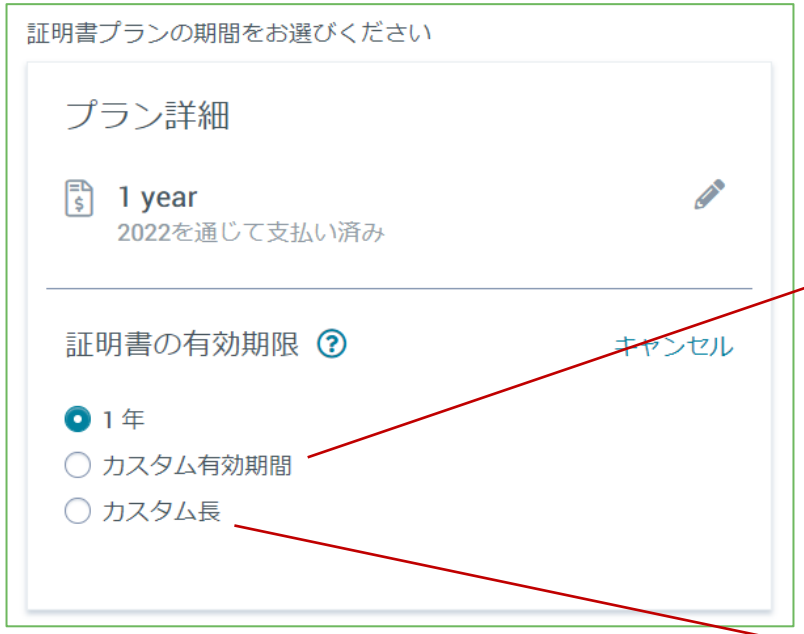


*1：有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります
詳細はこちら：https://docs.digicert.com/ja/manage-certificates/setting-validto-time-certificates/
*2：業界団体CA／ブラウザフォーラムの決議に則り、2020年9月以降にデジサートが発行するパブリック証明書の最大有効期限は最大397日間となります。

© 2021 DigiCert – All Rights Reserved

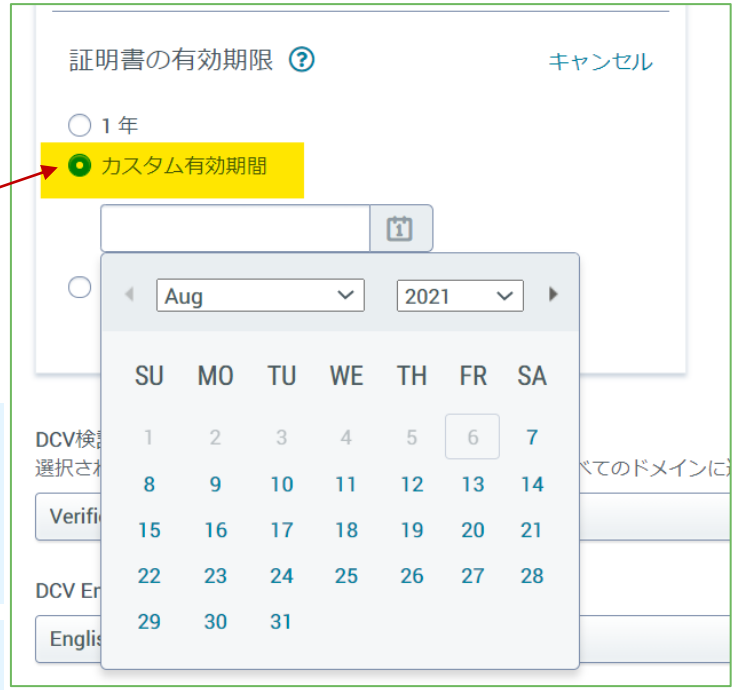
【サーバ証明書(OV/EV共通)】新規・更新申請 - プランおよび証明書の有効期間②

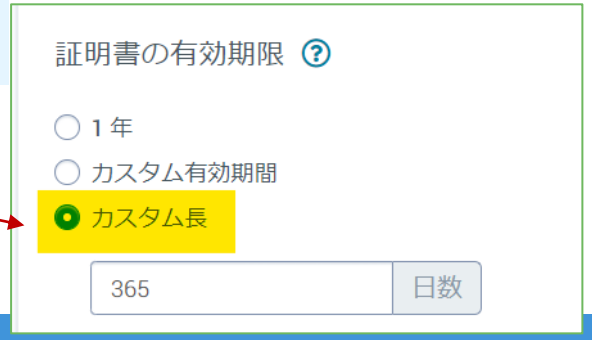
■申請画面のプラン期間を選択後「プランの詳細」の鉛筆マークより、証明書有効期間を日付や日数で指定することも可能です。
※プラン期間を越えた日で設定することはできません。



「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)





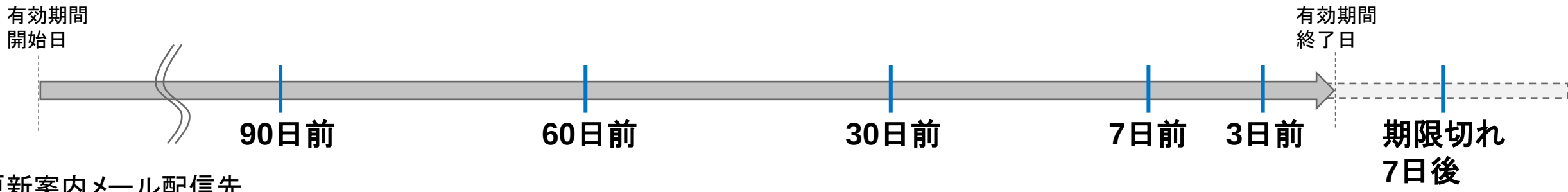
*1 : 有効期間終了日が土曜日、日曜日または年末休暇等にかかる場合、追加で数日間程度を追加で付与する場合があります
詳細はこちら:https://docs.digicert.com/ja/manage-certificates/setting-validto-time-certificates/
*2 : 業界団体CA／ブラウザフォーラムの決議に則り、2020年9月以降にデジサートが発行するパブリック証明書の最大有効期限は最大397日間となります。

© 2021 DigiCert – All Rights Reserved

証明書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

© 2021 DigiCert – All Rights Reserved

証明書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。

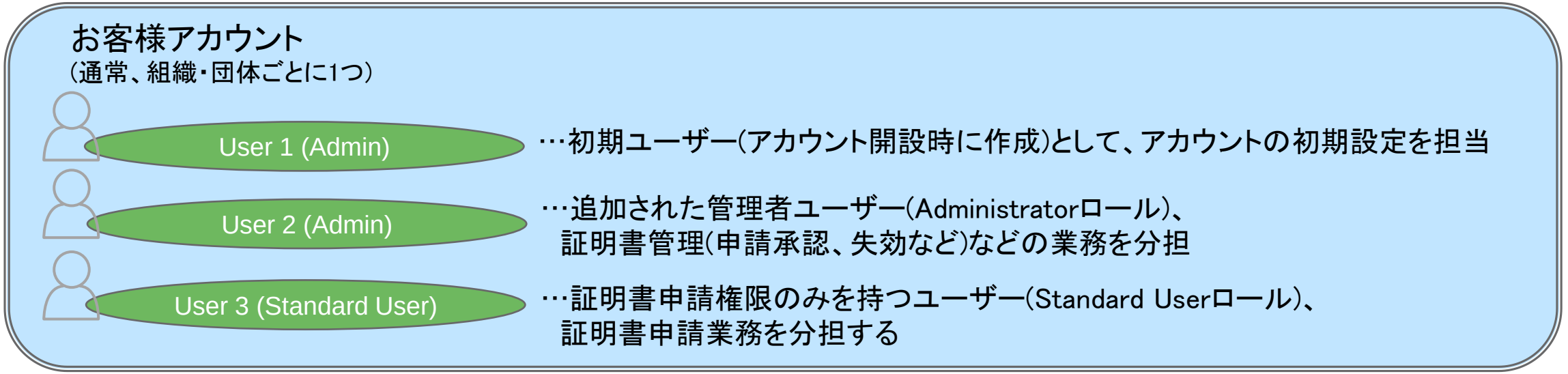
© 2021 DigiCert – All Rights Reserved

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）



© 2021 DigiCert – All Rights Reserved

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)	○	○	○	○	○
・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/

© 2021 DigiCert – All Rights Reserved

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)

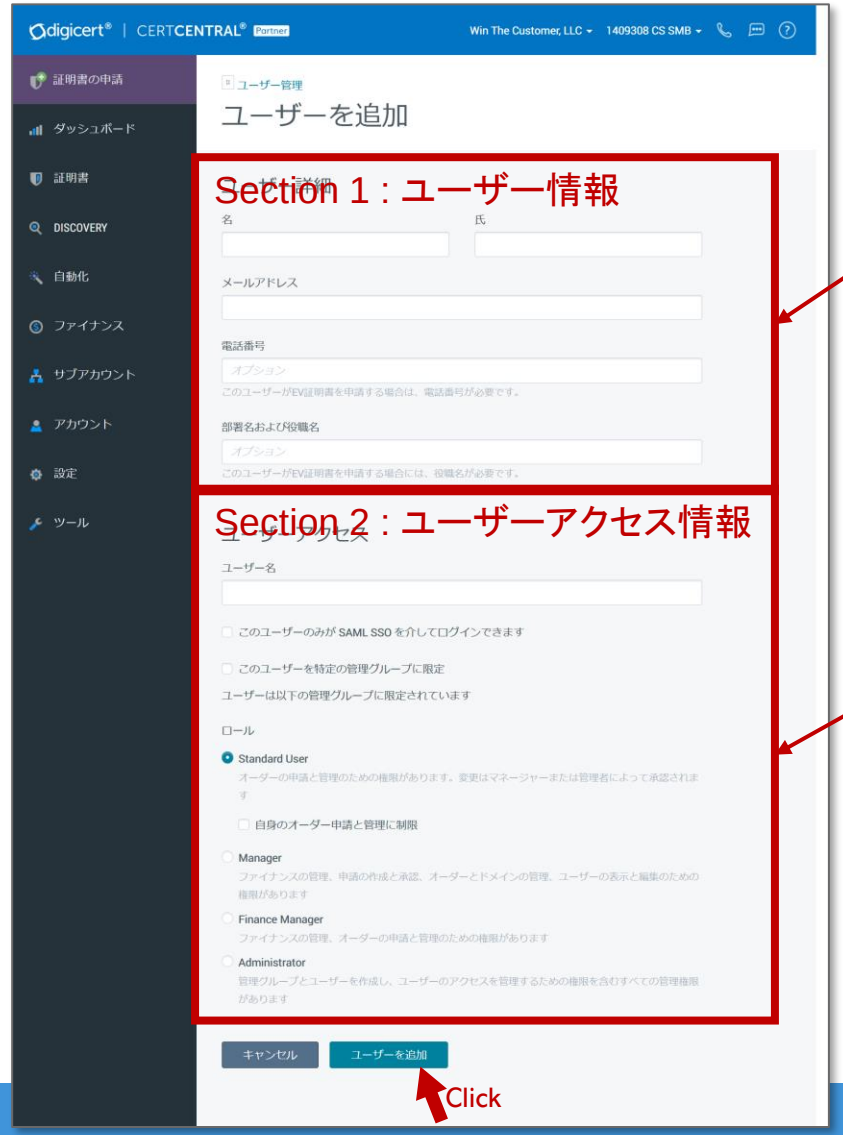
■メニューから「アカウント」→「ユーザー」を選択

■「ユーザーを追加」ボタンを押下してください

© 2021 DigiCert – All Rights Reserved

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。

ert – All Rights Reserved

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。

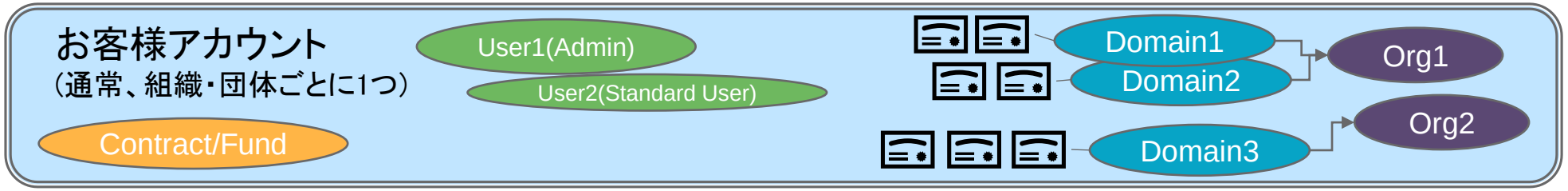
© 2021 DigiCert – All Rights Reserved

9. アカウントアクセス管理

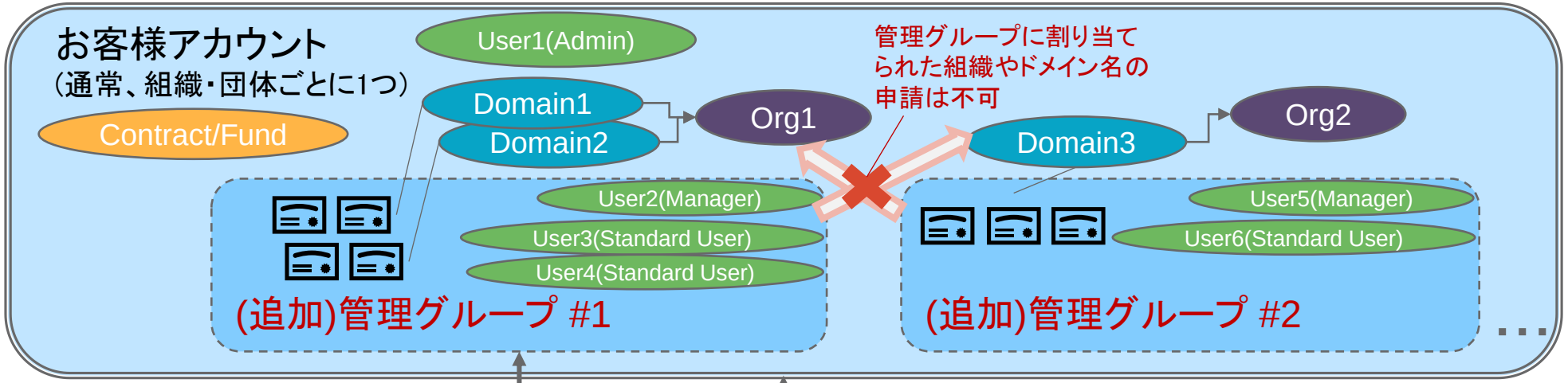
~ 9.1 管理グループ ~

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

© 2021 DigiCert – All Rights Reserved

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）

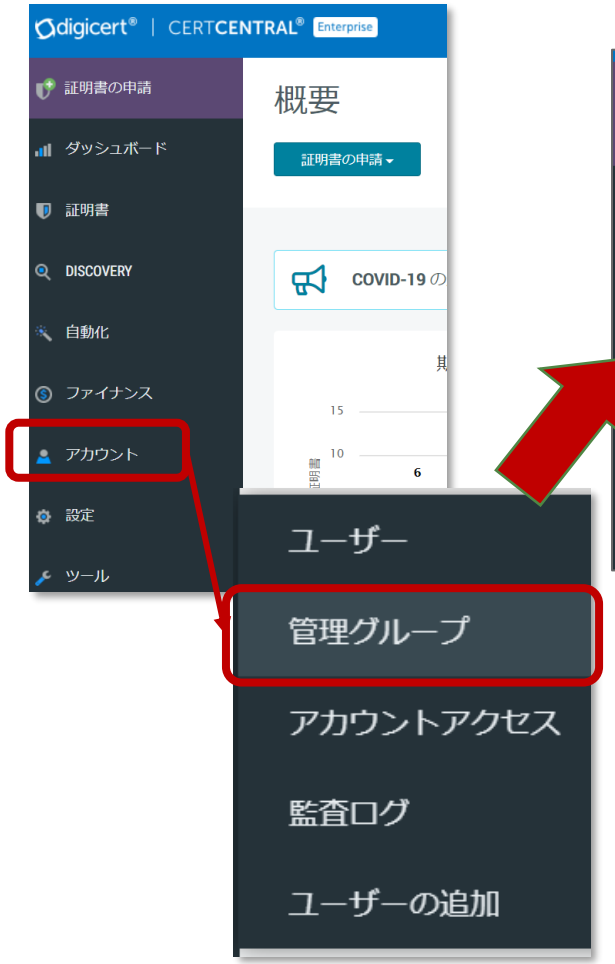
■管理グループ追加(作成)時の入力/選択項目

#	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

© 2021 DigiCert – All Rights Reserved

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）



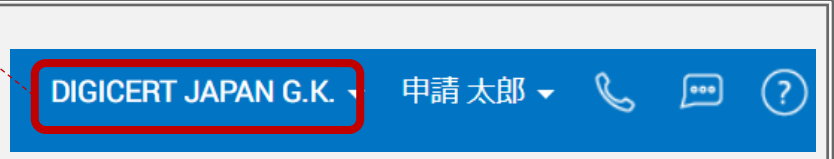
■管理グループ一覧と各機能説明

	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。



© 2021 DigiCert – All Rights Reserved

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/

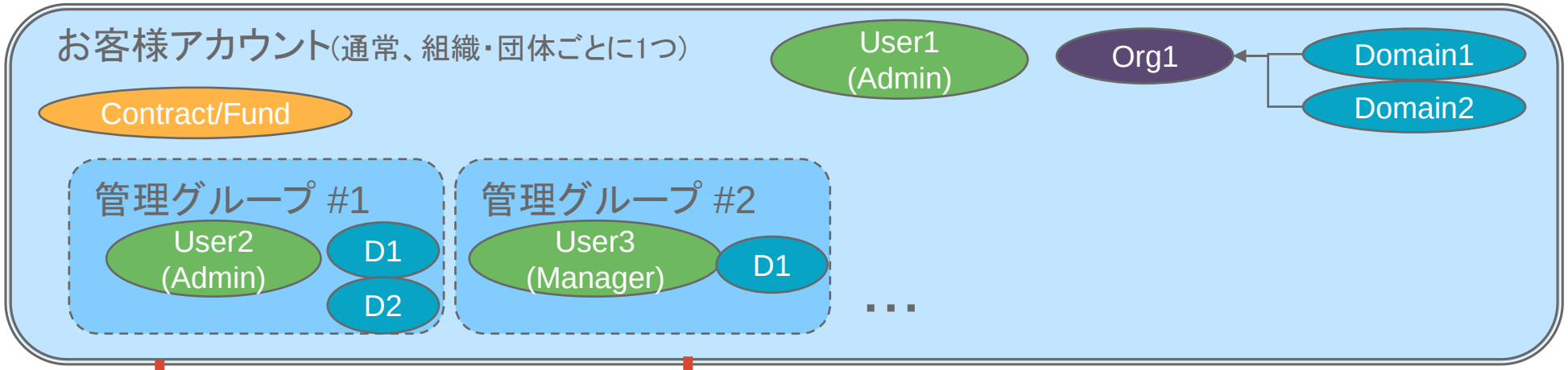
© 2021 DigiCert – All Rights Reserved

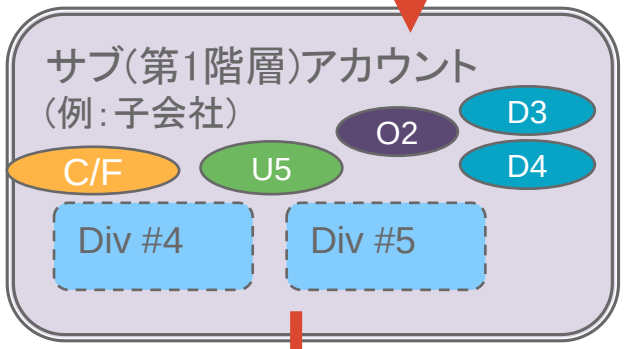
9. アカウントアクセス管理

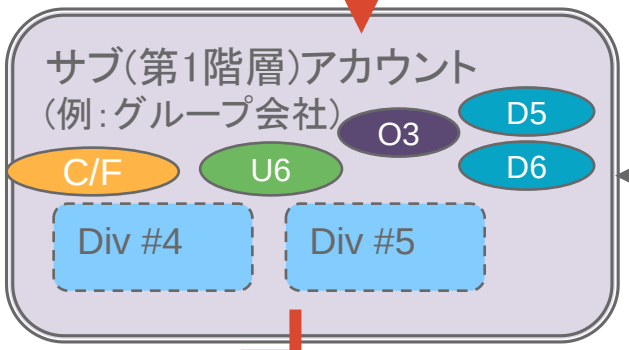
~ 9.2 サブアカウント ~

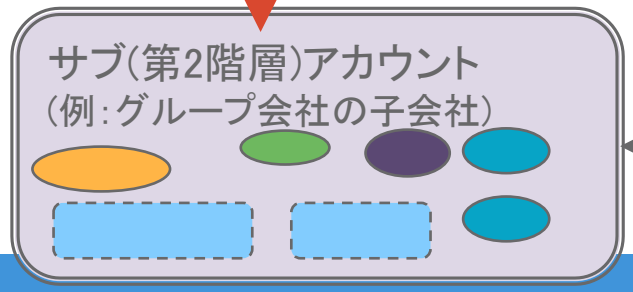
CertCentralの「サブアカウント(Sub Account)」機能をグループ企業や子会社などに適用することで、証明書の価格条件やセキュリティ設定の統合管理を容易にします

「サブアカウント」を活用する場合のイメージ









■親アカウントは、サブアカウントに対して;
- 証明書オーダー状況を確認することができる
- 申請可能な証明書製品範囲指定することができる
- (見た目の)価格条件を設定することができる。

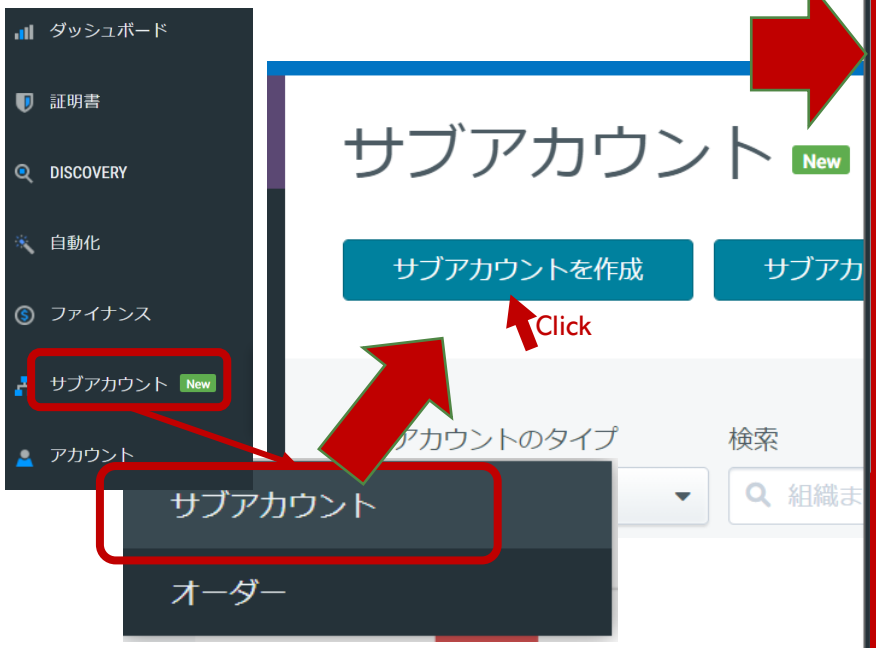
■サブアカウント内で自由に設定・利用可能な機能
- 組織(Org)およびドメイン名の管理
- 証明書申請および管理
- 管理グループ(Division)管理
- ユーザー管理
- (一部親アカウントの設定に拠る)デポジット管理

© 2021 DigiCert – All Rights Reserved

【親アカウント側の作業】 新規サブアカウントを作成する

親

(親)アカウント
管理者



■サブアカウント作成画面

Section 1：以下のような「(サブアカウント)基本情報」を入力します。
・サブアカウントタイプ
・担当アカウントマネージャー

Section 2：次に「サブアカウント管理者情報」を入力します
・サブアカウント管理者の氏名・連絡先
・サブアカウント管理者のメールアドレス・ユーザーID

Section 3：次に「サブアカウント組織情報」を入力します
・サブアカウントを所有・管理する組織の情報

Section 4：最後にサブアカウントで申請可能な製品、価格ならびにご請求に関連する設定を行います。
・サブアカウントで申請可能な製品の設定
・サブアカウントに適用する製品別価格の設定
・請求設定

© 2021 DigiCert – All Rights Reserved

【親アカウント側の作業】新規サブアカウント作成画面 Section 1 : 基本情報

■サブアカウント作成画面

親

■サブアカウントの基本情報設定欄

サブアカウントのタイプ	説明
リテール (Retail)	「エンド顧客」様向けのサブアカウントを作成する場合に選択します。サブアカウントでは対象の「エンド顧客」様自身が証明書の申請・管理を行います。 **(2020年9月時点では特にデジサートからの指定がない限り通常はこちらのみをご利用ください)**
再販業者 (Reseller)	**(2020年9月時点ではこちらは選択不可)**

親アカウント内のユーザーアカウントから、サブアカウントを管理する「アカウントマネージャー(例：パートナー様の営業担当者)」を指定します。

© 2021 DigiCert – All Rights Reserved

【親アカウント側の作業】新規サブアカウント作成画面 Section 2：管理者情報

■サブアカウント作成画面

親

■サブアカウント管理者情報設定欄

・サブアカウント管理者情報を登録します。
ここで登録したメールアドレスには、サブアカウント開設後の最初のユーザー(初期管理者)としてログインしていただくためのセットアップ画面へのリンクが送信されます。以下の説明・入力例を参考にして情報を正しく入力してください

項目名	説明	入力例
名	サブアカウント管理者の名	Taro
氏	サブアカウント管理者の氏	Shinsei
メールアドレス	**サブアカウント管理者の電子メールアドレス**	**sub.admin@example.com**
ユーザー名	サブアカウント管理者がサブアカウントにログインする際に用いるユーザーID **※「メールアドレス」欄の入力値が自動補完されますが、変更可能です。** **※ 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。**	sub.admin.user.id （入力例と同じ値はご利用いただけません）
電話番号	担当者の電話番号	03-XXXX-XXXX
役職名	担当者の役職名	Manager

© 2021 DigiCert – All Rights Reserved

【親アカウント側の作業】新規サブアカウント作成画面 Section 3 : 組織情報

■サブアカウント作成画面

親

■サブアカウントの組織情報設定

・サブアカウントの管理を行う組織情報を登録します。
以下の説明・入力例を参考にして情報を正しく入力してください。

項目名	概要	入力/選択例
組織名	組織の正式名称 (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.
電話番号	組織の電話番号	03-4560-3900
国	「Japan」を選択	Japan
郵便番号	組織の所在地:郵便番号	104-0061
住所	組織の所在地・市区町村より 下のレベル(番地等)(※1)(※2)	例1 : 6-10-1 Ginza 例2 : 580-16 Horikawa-cho
住所 2	<入力不要>	
市町村名	組織の所在地・ 市区町村名(※1)(※2)	例1 : Chuo-ku 例2 : Kawasaki-shi
州/ 都道府県	組織の所在地・ 都道府県名(※1)(※2)	例1 : Tokyo 例2 : Kanagawa

※1 ・入力例は英語で記載していますが、日本語での入力も可能です。
・ここで記入した情報は開設したサブアカウントの「表示上の代表組織名」として用いられますが、必ずしも証明書発行のための認証対象項目にはなりません。
・なお、サブアカウント開設後、ここで記入した組織情報に対してサブアカウントにて「認証申請」をリクエストいただき、証明書発行に用いるようにすることも可能です。この場合は正式な組織情報を入力ください。

※2 住所(申請団体所在地)の都道府県名、市区町村名などの区切り方などについて、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

【親アカウント側の作業】新規サブアカウント作成画面 Section 4：製品・価格・請求設定

■サブアカウント作成画面

親

■サブアカウントの請求設定

製品請求先

証明書オーダーの請求先はどちらですか？

- ○ 請求サブアカウント
- ◉ 請求 Win The Customer, LLC (1409308)
- ☐ サブアカウントの子に強制的にサブアカウントに請求する

サブアカウント支出制限

サブアカウントが制限を超えて支出されるのを防止します。これは、実際の資金ではなく購入額はお客様に請求されます。

- ○ 無制限 – このサブアカウントの支出を制限しない
- ◉ 制限付き – サブアカウントの支出にマイナス残高制限を設定する

1000000

通貨

JPY - Japanese Yen

請求先	説明
請求サブアカウント	(2020年9月時点ではこちらは選択不可)
請求<親アカウント名>	(2020年9月時点では特にデジサートからの指定がない限り通常はこちらのみをご利用ください) サブアカウントで申請・発行された証明書の費用については、デジサートと貴社(パートナー様)との間で合意した条件に基づきデジサートから貴社へご請求させていただきます 注：“サブアカウントの子に強制的に…”にはチェックしないでください

サブアカウント支出制限	説明
無制限	サブアカウント内で上限なく証明書を申請・発行可能とします
制限付き	サブアカウント内で申請・発行可能な証明書の数量に上限を設定するため「サブアカウント支出制限(アカウント残高のマイナス上限値)」を設定します
残高制限	整数値で「サブアカウント支出制限」を指定します。指定値がサブアカウントにおけるアカウント残高のマイナス上限値となります (このアカウント残高は見た目上の資金であり、実際の資金ではありません)

次ページに進みます

© 2021 DigiCert – All Rights Reserved

【親アカウント側の作業】新規サブアカウント作成画面 Section 4 : 製品・価格・請求設定 (続き)

■サブアカウント作成画面

親

■サブアカウントの製品・価格設定欄

	説明
製品別 【ステータス】	サブアカウントにおいて該当製品の申請・発行を許可する場合に「有効」チェックをONにしてください
製品別 【ベース価格】	対象製品に設定する【ベース価格(*1)】を整数値で指定します
製品別 【FQDN価格】	対象製品に設定する【FQDN価格(*1)】を整数値で指定します
製品別 【ワイルドカード価格】	対象製品に設定する【ワイルドカード価格(*1)】を整数値で指定します (EV証明書製品ではワイルドカードを使用しないため指定しない)

*1 :「ベース価格」「FQDN価格」「ワイルドカード価格」については次ページを参照ください。

・全ての入力・選択が完了したら「保存」ボタンを押下してください。

© 2021 DigiCert – All Rights Reserved

（参考）サブアカウントに対する価格設定に関する補足資料

■サブアカウントで申請・取得される証明書にかかる費用は、以下の組み合わせによって算出されます。

ベース価格

各証明書製品のオーダー単位の基礎部分(ベース)の費用を指します。
ベース価格には、通常証明書に含まれるFQDNまたはワイルドカードドメイン名のための価格は含まれていません。
実際の証明書製品のご購入にあたっては、ベース価格に加え、必ず1つ以上の＜FQDN価格またはワイルドカード価格＞を足した費用がかかります。
デジサートが提供する一部製品ではベース価格が「ゼロ円」です。

＋

FQDN価格

単一のFQDN(例:「www.example.com」)をSubject CNおよびSubject Alternative Namesに含む証明書を発行するために必要な費用を指します。
1枚の証明書に複数のFQDNを含む場合、＜FQDN価格＊FQDN数＞をベース価格に足した費用がかかります。

AND / OR

ワイルドカード価格 (WC価格)

単一のワイルドカードドメイン名(例:「*.example.com」)をSubject CNおよびSubject Alternative Namesに含む証明書を発行するために必要な費用を指します。
1枚の証明書に複数のワイルドカードドメイン名を含む場合、
＜ワイルドカード価格＊ワイルドカードドメイン数＞をベース価格に足した費用がかかります。

■デジサートの一部製品の標準販売価格(1年間プラン)を例にした「ベース価格」「FQDN価格」「WC価格」の設定例

ブランド	デジサート				ジオトラスト		
製品(※1)	グローバル・サーバID EV	セキュア・サーバID EV	グローバル・サーバID	セキュア・サーバID	トゥルービジネスID with EV	トゥルービジネスID	クイックSSLプレミアム
ベース価格	¥0	¥0	¥0	¥0	¥42,200	¥22,000	¥11,800
FQDN価格	¥219,000	¥162,000	¥138,000	¥81,000	¥73,000	¥33,000	¥19,500
WC価格	-	-	¥681,000	¥400,000	-	¥116,400	¥104,100

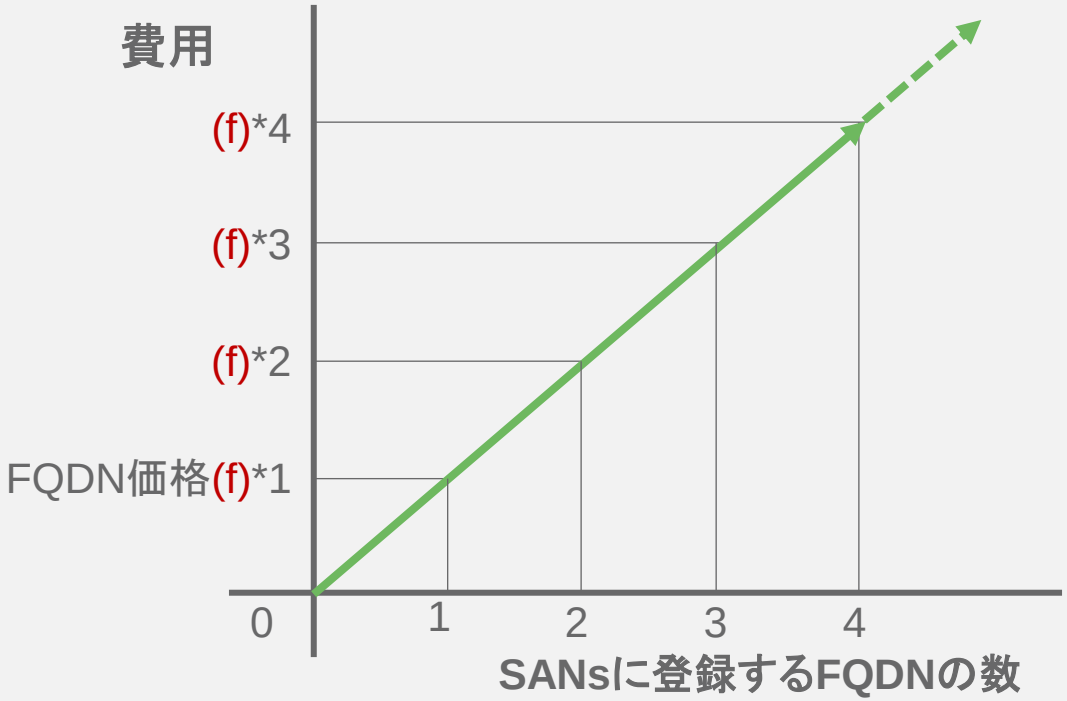
※1：CertCentral Partnerを通じてパートナー様に対して提供可能な全ての製品を網羅するものではございません。また、ここに示す価格は2020年9月時点でのデジサートの一部製品のウェブサイト上での標準販売価格を「サブアカウントに対する製品価格の入力例」として示すものであり、それ以外の目的で掲載するものではございません。デジサートの標準販売価格は今後変更となる場合があります。

© 2021 DigiCert – All Rights Reserved

（参考）サブアカウントへのデジサート セキュア・サーバIDの価格設定と費用計算例

■デジサート セキュア・サーバID

	1年間(JPY)	
ベース価格	¥0	(b)
FQDN価格	¥81,000	(f)
WC価格	¥400,000	(w)



■実際の申請費用計算例 (1年間有効な証明書の場合)

例1

コモンネーム	aaa.example.com	(f)
SANs	aaa.example.com	コモンネームと同一値（デフォルトで設定）
	www.aaa.example.com	無償追加可能なSANs（www.あり／なしの違い）

(b)

→ (b) + (f)*1 = ¥81,000-

例2

コモンネーム	aaa.example.com	(f)
SANs	aaa.example.com	CN同一
	www.aaa.example.com	無償SANs
	bbb.example.com	(f)
	ccc.example.jp	(f)
	www.ccc.example.jp	
	ddd.example.net	(f)

(b)

→ (b) + (f)*4 = ¥324,000-

例3

コモンネーム	*.aaa.example.com	(w)
SANs	aaa.example.com	無償追加可能なSANs（"*"あり／なしの違い）
	*.example.net	(w)
	ccc.example.jp	(f)

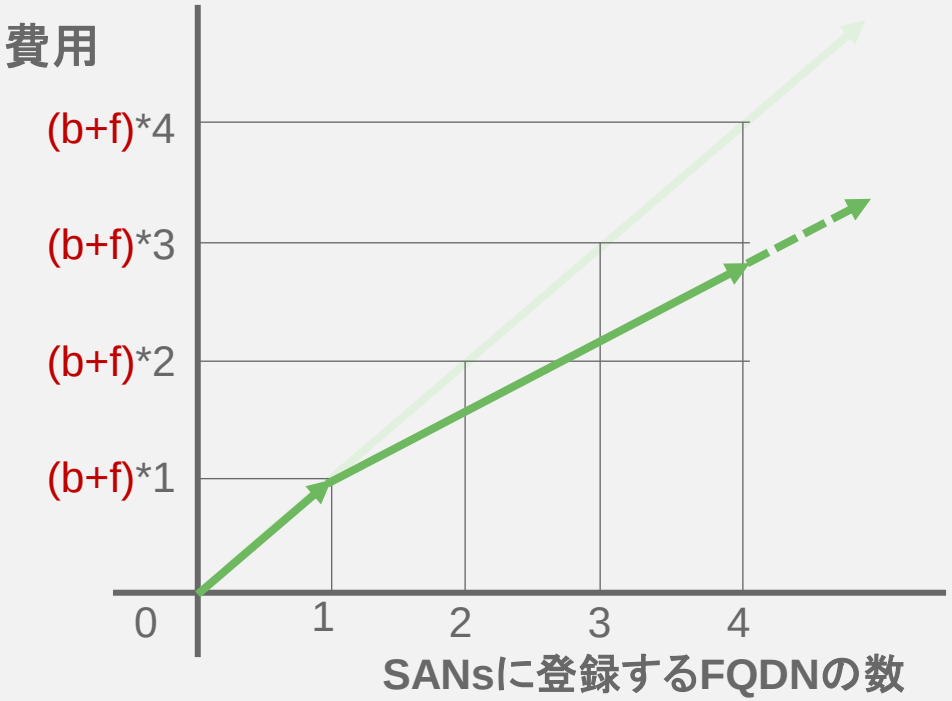
(b)

→ (b) + (f)*1 + (w)*2 = ¥881,000-

（参考）サブアカウントへのジオトラスト クイックSSLプレミアムの価格設定と費用計算例

■ジオトラスト クイックSSLプレミアム

	1年間(JPY)	
ベース価格	¥11,800	(b)
FQDN価格	¥19,500	(f)
WC価格	¥104,100	(w)



■実際の申請費用計算例 (1年間有効な証明書の場合)

例1

コモンネーム	aaa.example.com	(f)
SANs	aaa.example.com	コモンネームと同一値（デフォルトで設定）
	www.aaa.example.com	無償追加可能なSANs（www.あり／なしの違い）

(b)

→ (b) + (f)*1 = ¥31,300-

例2

コモンネーム	aaa.example.com	(f)
SANs	aaa.example.com	CN同一
	www.aaa.example.com	無償SANs
	bbb.example.com	(f)
	ccc.example.jp	(f)
	www.ccc.example.jp	
	ddd.example.net	(f)

(b)

→ (b) + (f)*4 = ¥89,800-

例3

コモンネーム	*.aaa.example.com	(w)
SANs	aaa.example.com	無償追加可能なSANs（“*”あり／なしの違い）
	*.example.net	(w)
	ccc.example.jp	(f)

(b)

→ (b) + (f)*1 + (w)*2 = ¥239,500-

【サブアカウント側の作業】サブアカウント開設案内メール → パスワード設定

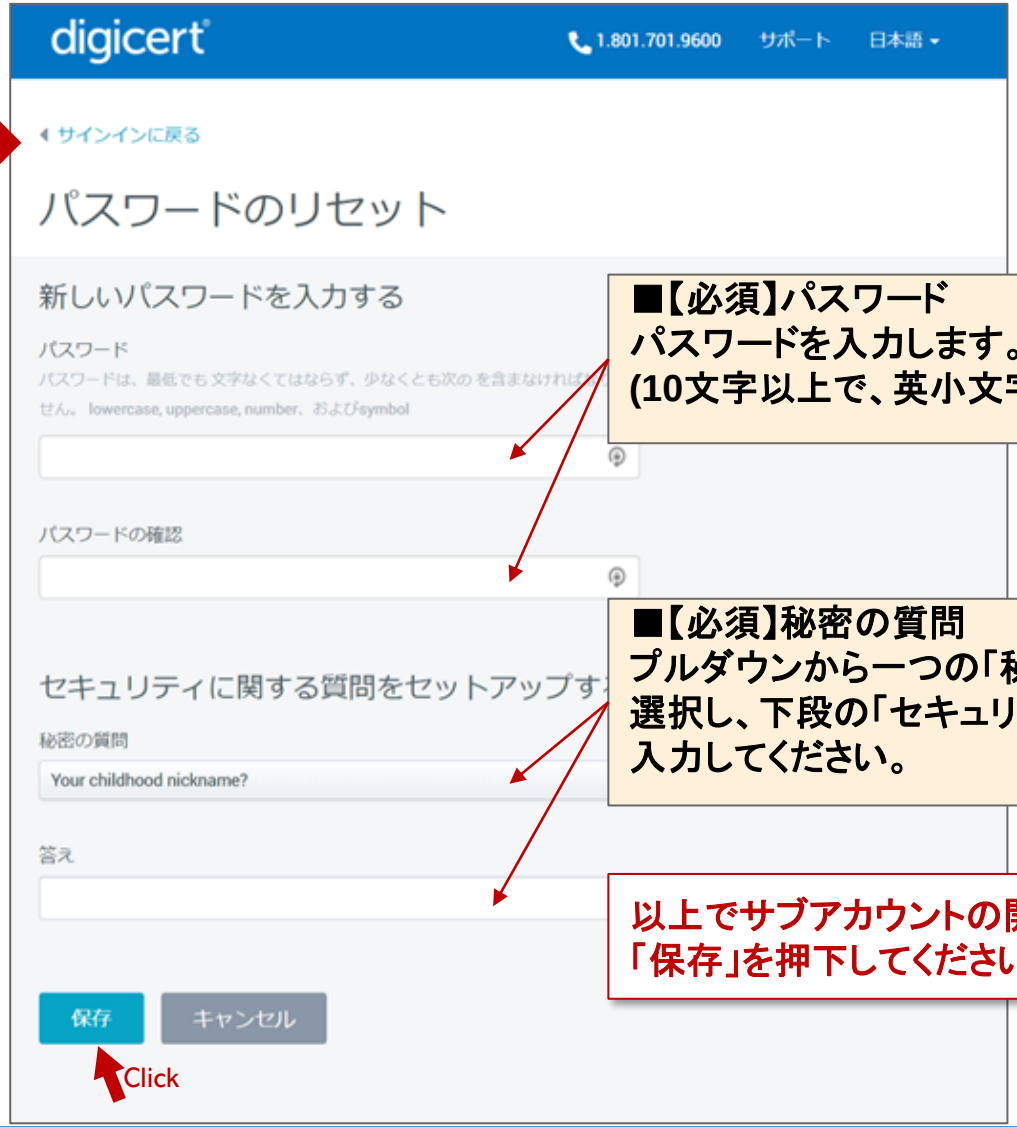
■新規サブアカウント設定画面

URLリンクをクリック

アカウント開設の案内メール

サブアカウント管理者

件名	DigiCert User Account Created - Action Required
送信元	DigiCert <admin@digicert.com>
本文イメージ	[サブアカウント組織名] Your new DigiCert user account has been created. Your username is: [前ステップで入力したサブアカウント管理者のユーザーID] Please complete the process by following the link below to set your password and configure your account. https://www.digicert.com/link/pass.php?t=[お客様固有のトークン情報] <後略>



■【必須】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)

■【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。

以上でサブアカウントの開設作業は終了です。
「保存」を押下してください。

※：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
また、メール本文のイメージは今後変更となる場合があります

© 2021 DigiCert – All Rights Reserved

【サブアカウント側の作業】サブアカウントで出来ること・出来ないこと

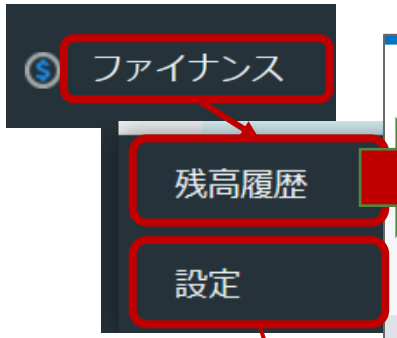
■サブアカウント ログイン画面のイメージ

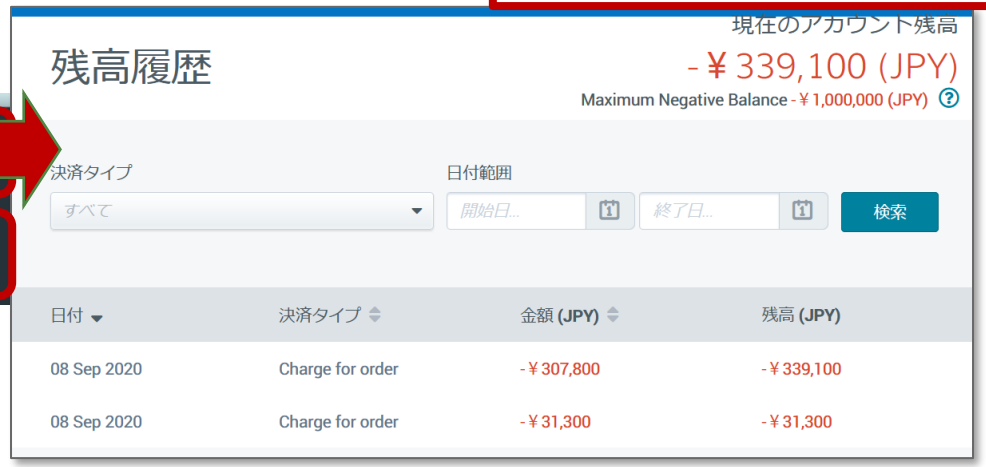
メニュー構成は親アカウントや独立アカウントとほぼ同一

■サブアカウントで申請可能な製品

申請・発行可能な製品範囲は親アカウントによって制限される

■ファイナンスメニューでできること
－「残高履歴」の確認





親アカウントが設定したアカウント残高のマイナス上限値の範囲内でのみ証明書の申請・発行が可能

サブアカウント内で独自にデジサートとの直接の取引（直接購入）は不可

上記以外の「利用可能な機能」の範囲は親アカウント／独立アカウントと同一となります
詳しくは下記URL等に掲載されるエンドユーザー向けの簡易マニュアルなどをご活用ください
https://www.digicert.co.jp/storefront/certcentral/

All Rights Reserved

9. アカウントアクセス管理

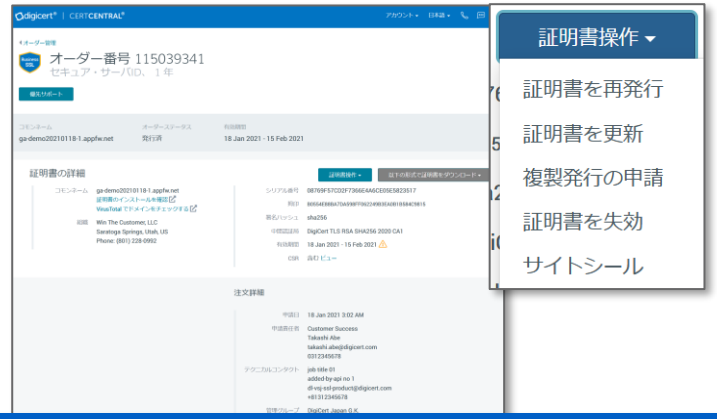
~ 9.3 ゲストアクセス ~

「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エンドユーザーがサイトシールを取得したり、発行済の証明書をダウンロードすることが可能

■「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)

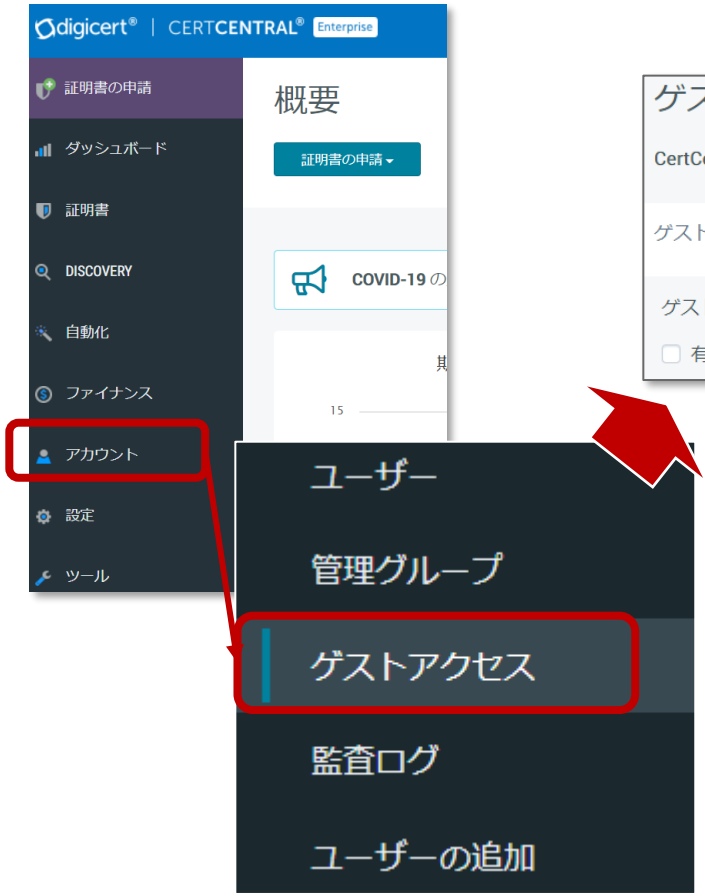


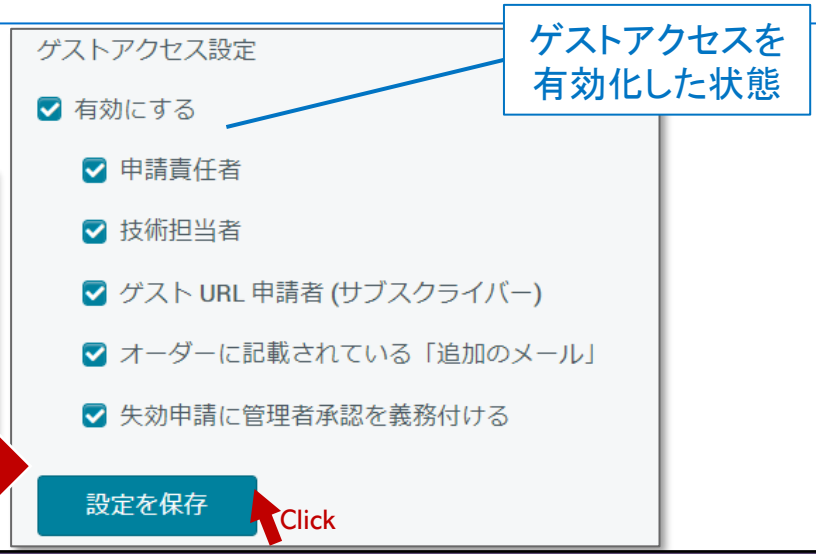
※ 当機能を有効化してご活用いただく場合、ゲストユーザー(エンドユーザー)向けに、サイトシールを取得いただく手順や、
ゲストアクセス機能を通じて証明書ダウンロードいただく手順をまとめた利用ガイドを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から**「ゲストユーザー(エンドユーザー)向け利用ガイド」**をご参照ください。
https://www.digicert.co.jp/sid-partner/certcentral/

© 2021 DigiCert – All Rights Reserved

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】

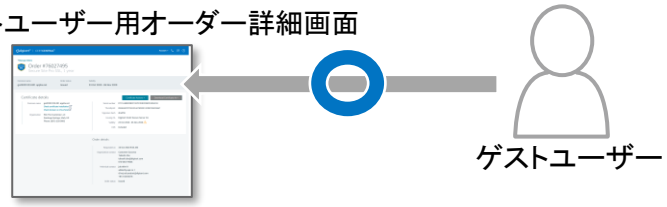
© 2021 DigiCert – All Rights Reserved

ゲストアクセスをオーダー単位で有効化／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)

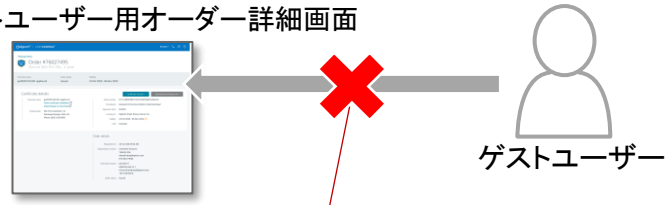
■このオーダーに対してゲストアクセスが「有効化」された状態

■ゲストユーザー用オーダー詳細画面

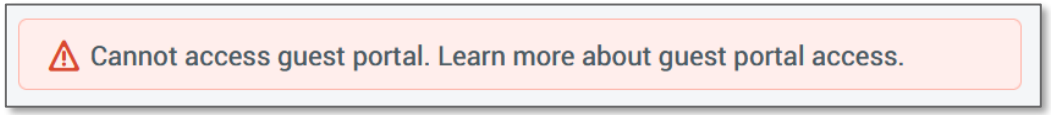


■このオーダーに対するゲストアクセスが「無効」である状態

■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。



© 2021 DigiCert – All Rights Reserved

(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

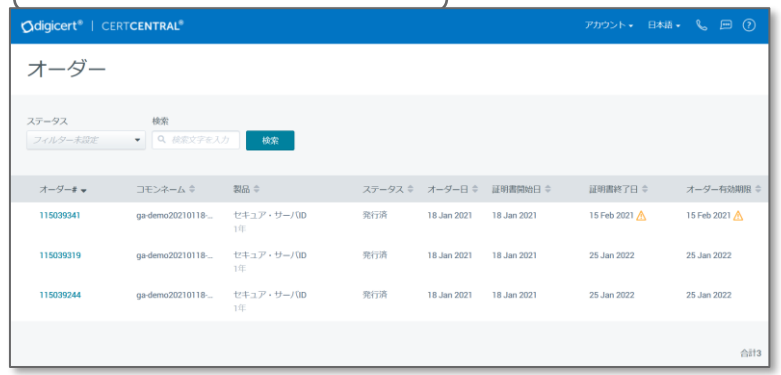
コモンネーム/SANの合致件数は？

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

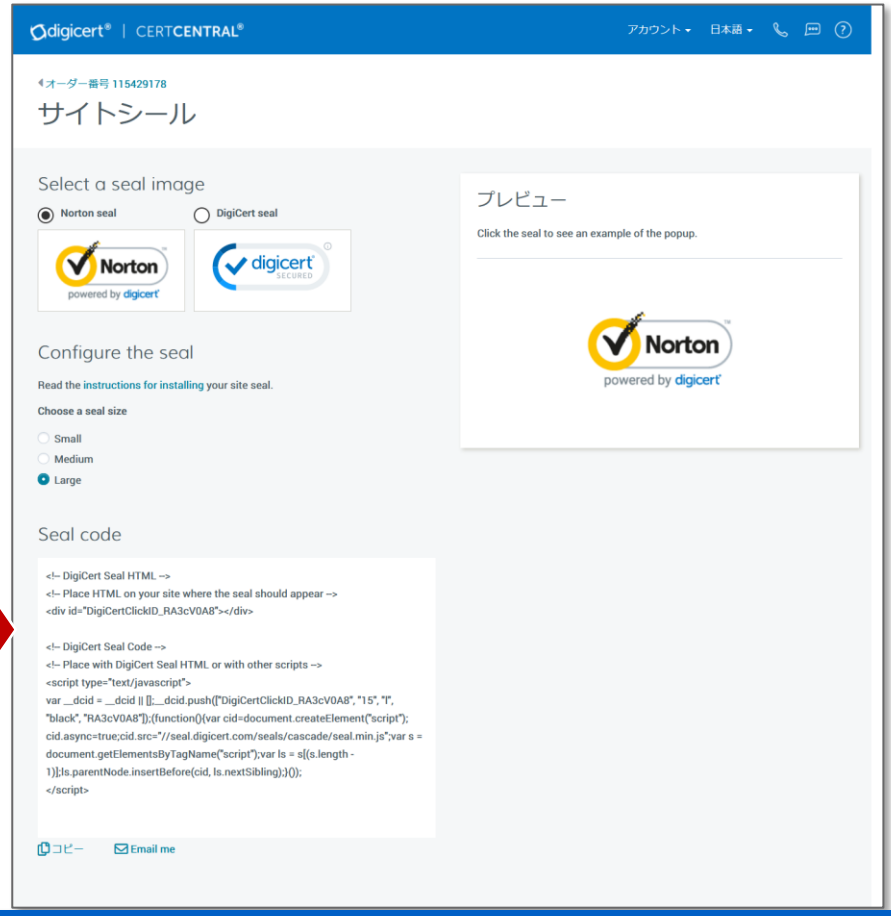
※ 当機能を有効化してご活用いただく場合、ゲストユーザー(エンドユーザー)向けに、サイトシールを取得いただく手順や、
ゲストアクセス機能を通じて証明書ダウンロードいただく手順をまとめた利用ガイドを別紙にて公開しておりますので併せてご活用ください
下記リンクのページ内から**「ゲストユーザー(エンドユーザー)向け利用ガイド」**をご参照ください。
https://www.digicert.co.jp/sid-partner/certcentral/

© 2021 DigiCert – All Rights Reserved

(ゲストユーザー向け) ゲストアクセスリンクを用いたサイトシール掲載用スクリプト生成 (イメージ)

■ゲストユーザー用オーダー詳細画面

■サイトシール生成画面



※ 当機能を有効化してご活用いただく場合、ゲストユーザー(エンドユーザー)向けに、サイトシールを取得いただく手順や、
ゲストアクセス機能を通じて証明書ダウンロードいただく手順をまとめた利用ガイド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(エンドユーザー)向け利用ガイド**」をご参照ください。
https://www.digicert.co.jp/sid-partner/certcentral/

© 2021 DigiCert – All Rights Reserved

【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)
・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？	・ゲストアクセスリンクを有効化した場合、ゲストユーザー(エンドユーザーは)証明書情報の参照や証明書のダウンロード、サイトシールを取得いただくことだけでなく、証明書の更新申請/再発行申請/失効申請をいただける機能も備えております。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。 ・また、該当の証明書オーダーの「申請責任者」「技術担当者」「申請者」「追加メールアドレス」のいずれにも該当しないユーザーは、セキュリティ上の理由から、ゲストアクセス機能でオーダー情報にアクセスいただくことは出来ません。ご理解・ご了承ください。
・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。管理者様は、アクセス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いただくことが可能になります。
・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。

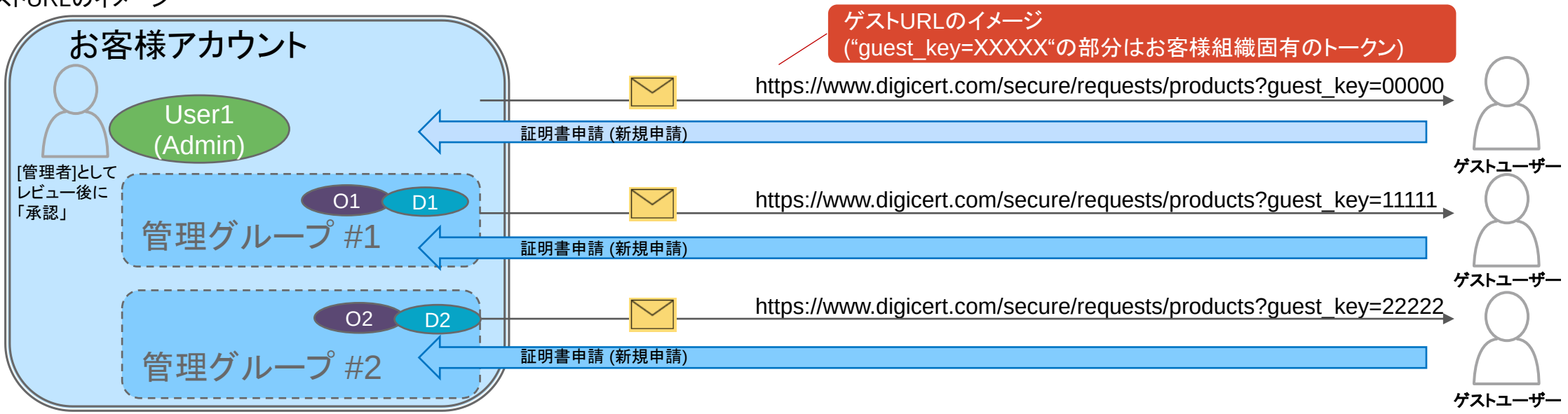
© 2021 DigiCert – All Rights Reserved

9. アカウントアクセス管理

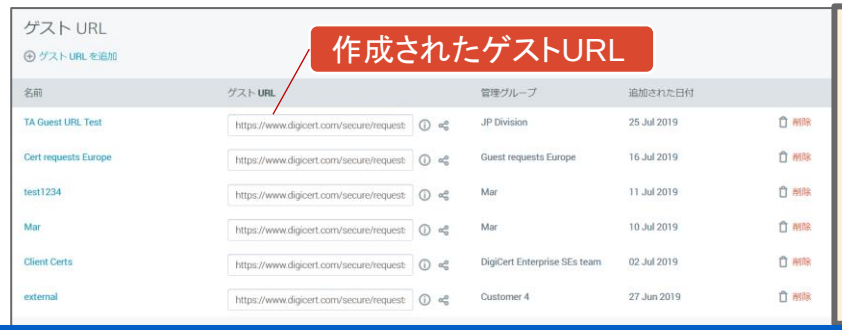
~ 9.4 ゲストURL ~

「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

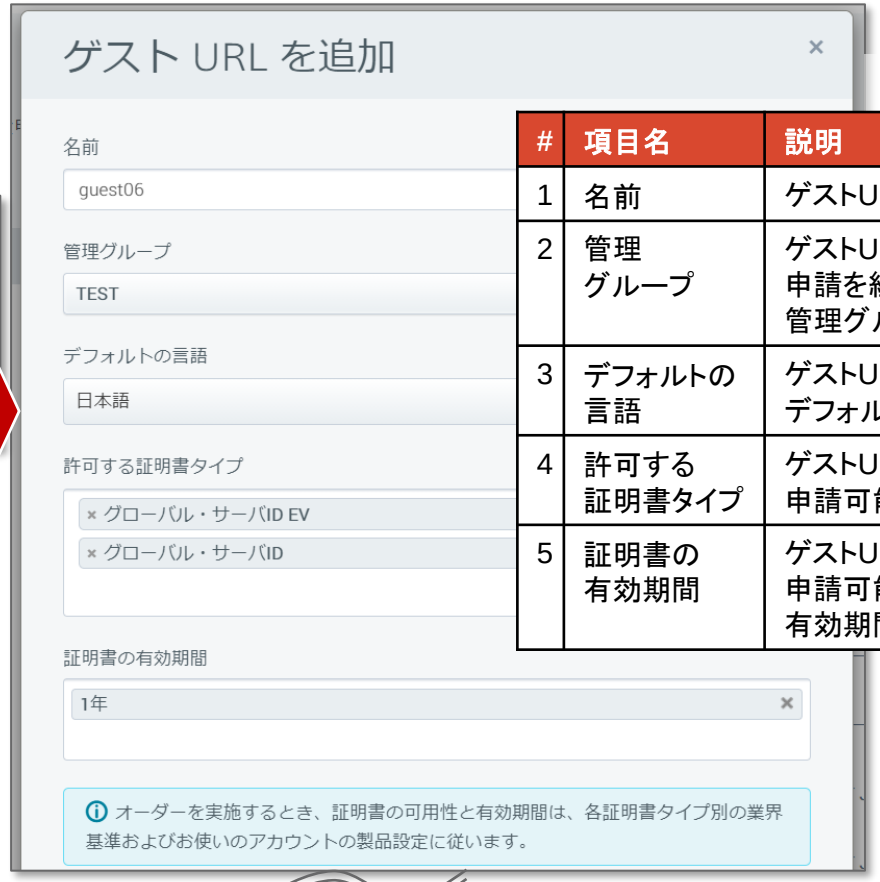
・(申請可能な)製品および証明書有効期間
→各管理グループ(事業部門等に紐づく)ごとに異なる
証明書製品の選択やライフサイクルへ対応

※ 当機能を有効化してご活用いただく場合、ゲストユーザー(エンドユーザー)向けに証明書申請手順をまとめた利用ガイド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(エンドユーザー)向け利用ガイド」**をご参照ください。
https://www.digicert.co.jp/sid-partner/certcentral/

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」

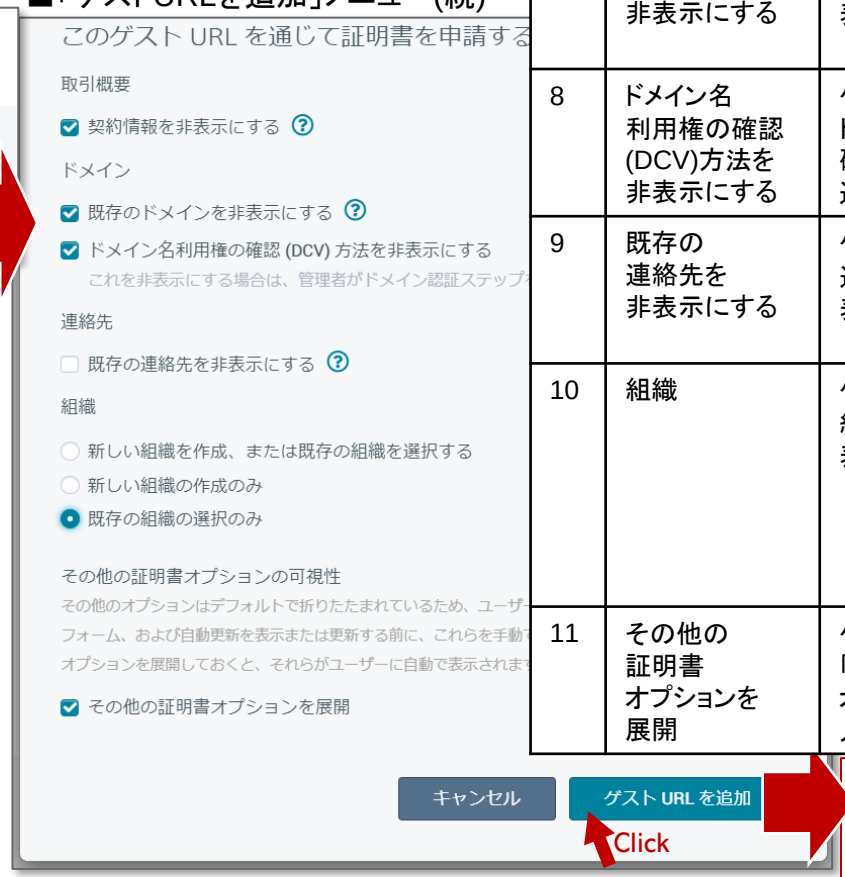
(次のページに続きます)

© 2021 DigiCert – All Rights Reserved

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)

■「ゲストURLを追加」メニュー(続)



■(続き)ゲストURL追加(作成)時の入力/選択項目

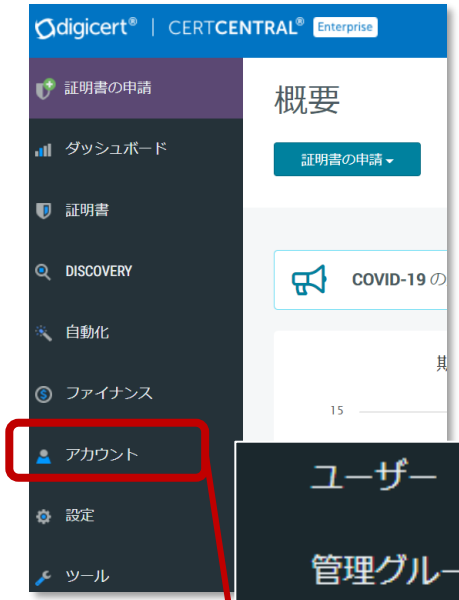
#	項目名	説明	入力/選択例
6	契約情報を 非表示にする	ゲストURLにおける 取引概要欄の 表示設定	チェックボックスON:【推奨】 取引概要欄を隠す(表示しない) チェックボックスOFF: 取引概要を隠さない(表示する)
7	既存の ドメインを 非表示にする	ゲストURLにおける 登録済ドメイン名の 表示設定	チェックボックスON:【推奨】 登録済ドメイン名を隠す(表示しない) チェックボックスOFF: 登録済ドメイン名を隠さない(表示する)
8	ドメイン名 利用権の確認 (DCV)方法を 非表示にする	ゲストURLにおける ドメイン名利用権 確認(DCV)方法 選択欄の表示設定	チェックボックスON: DCV方法選択欄を隠す(表示しない) チェックボックスOFF:【推奨】 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:【推奨】 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: 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

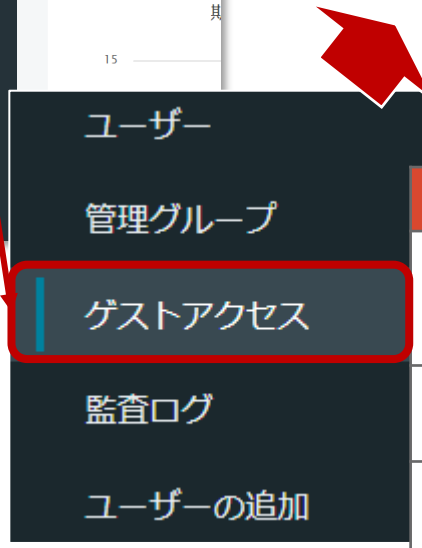
「ゲストURLを追加」を押下します。
次ページへ進んでください

© 2021 DigiCert – All Rights Reserved

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)

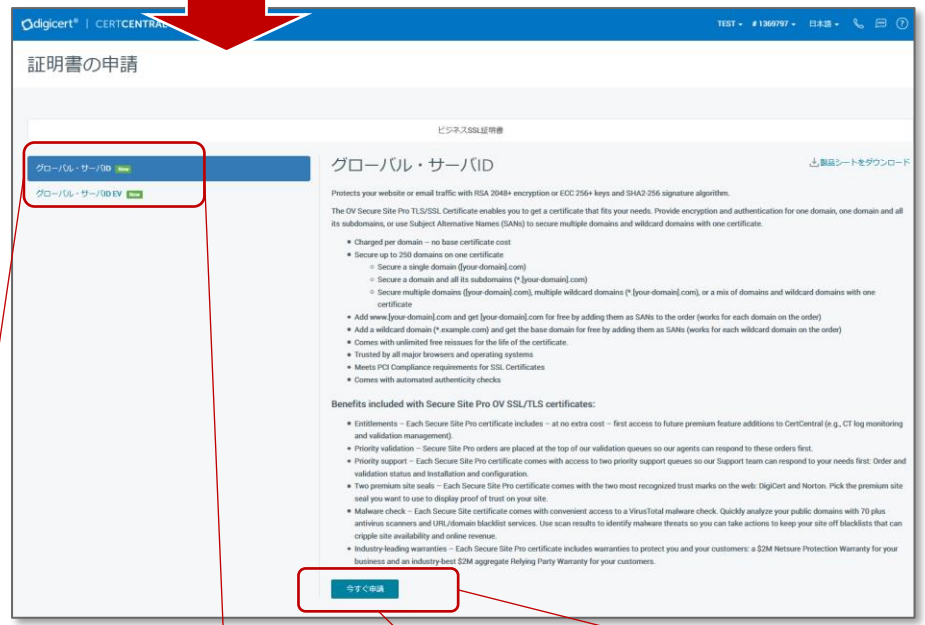
© 2021 DigiCert – All Rights Reserved

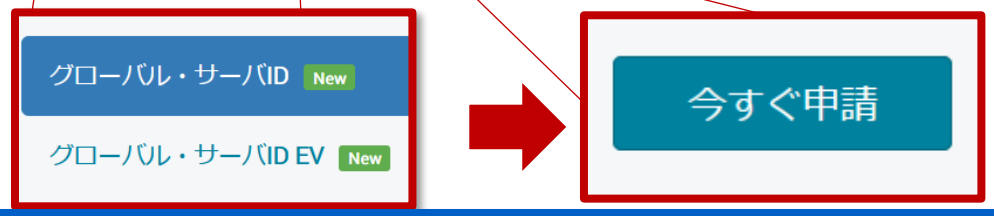
(ゲストユーザー向け) ゲストURLを用いた証明書申請のイメージ

■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

※ 当機能を有効化してご活用いただく場合、ゲストユーザー(エンドユーザー)向けに証明書申請手順をまとめた利用ガイド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(エンドユーザー)向け利用ガイド」をご参照ください。
https://www.digicert.co.jp/sid-partner/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、販売代理店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。

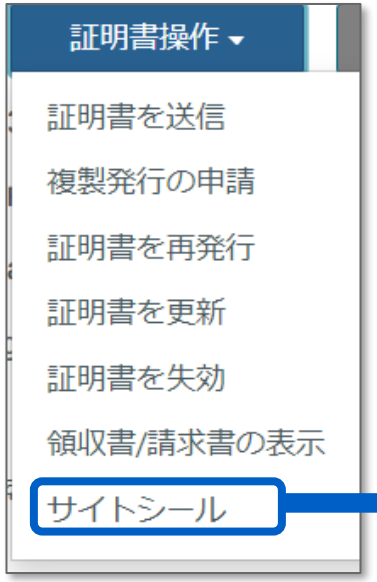
© 2021 DigiCert – All Rights Reserved

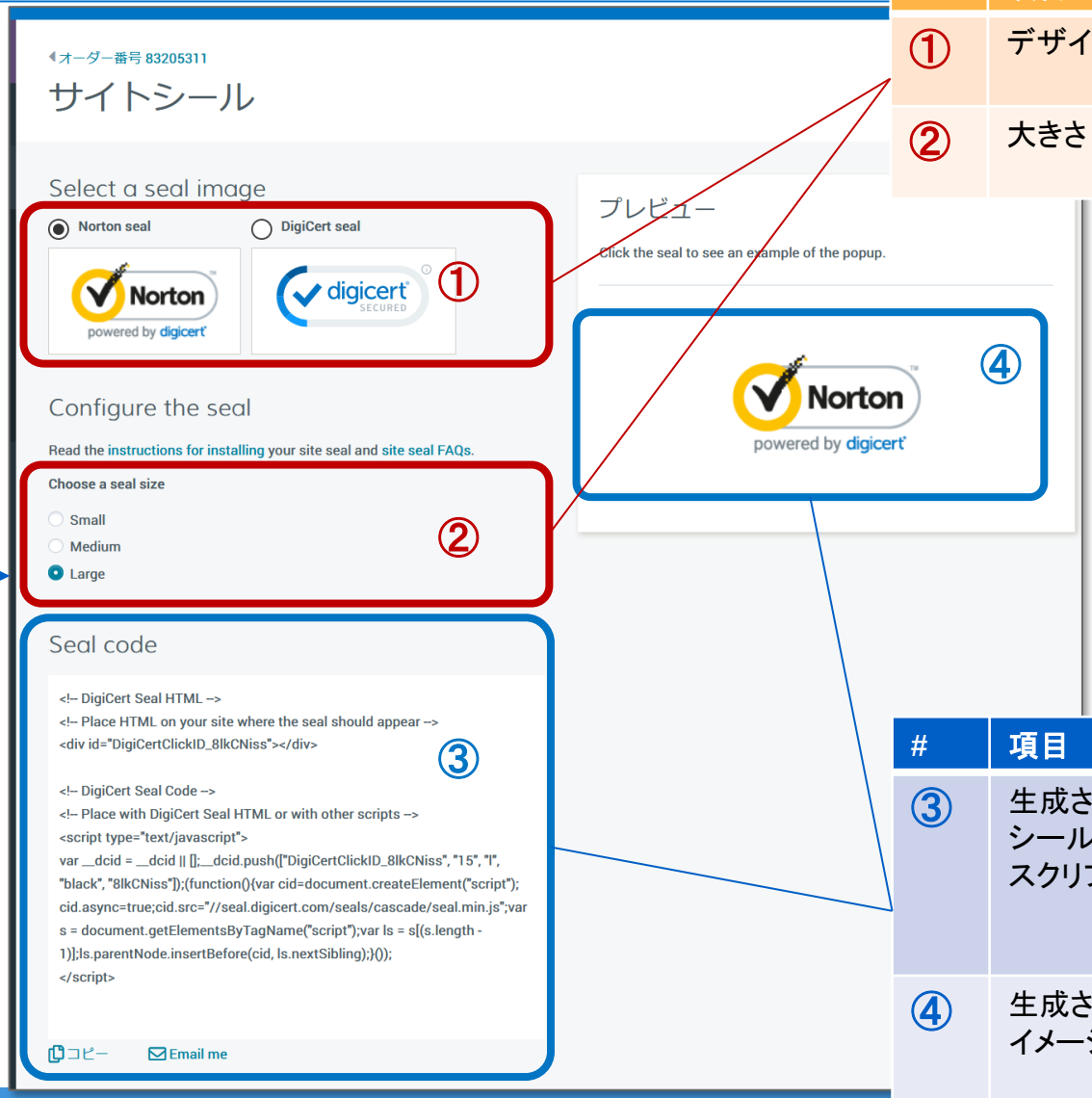
10.その他の証明書製品の機能

~ 10.1 サイトシール ~

「サイトシール」ページ

■「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

© 2021 DigiCert – All Rights Reserved

ブランド/製品別 サイトシール デザイン一覧 (2020年11月時点)

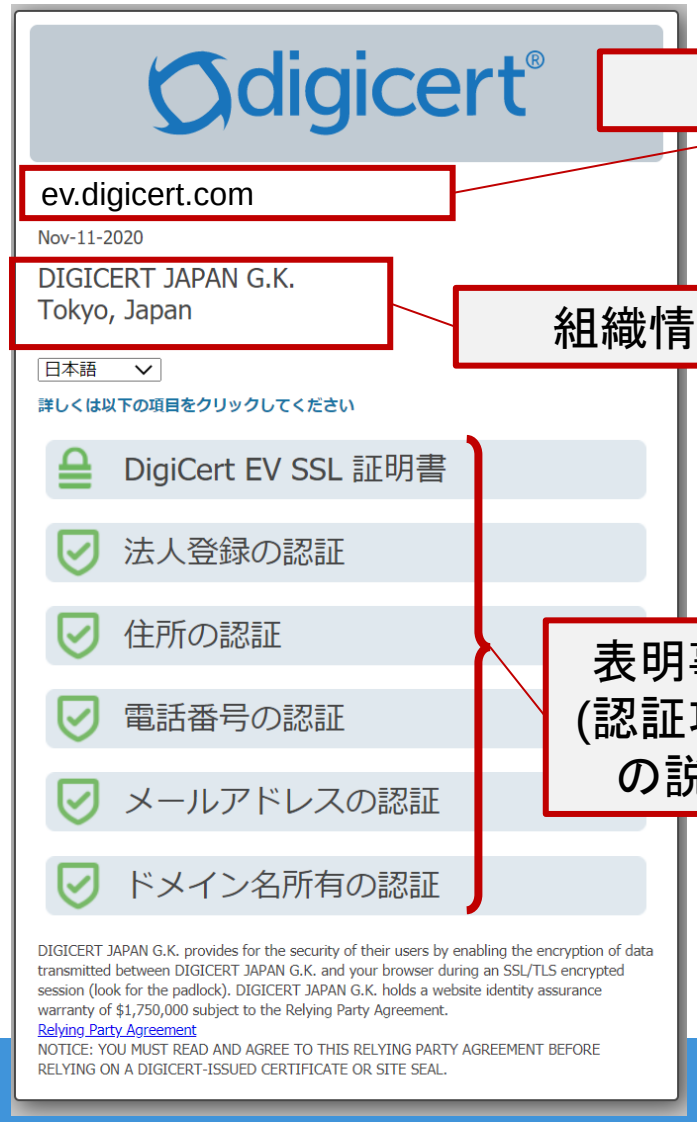
CertCentral 日本語製品名称	英語製品名称	シールデザイン	シール掲載用 HTML/JavaScript
グローバル・サーバID EV	Secure Site Pro SSL EV	以下2種類のデザインから選択可能 (推奨) Norton powered by digicert / digicert SECURED	CertCentralのオーダー詳細画面～「証明書操作」メニュー配下の「サイトシール」ページより、シール掲載用HTML/JavaScriptを入手いただけます。 (詳細は後述)
グローバル・サーバID	Secure Site Pro SSL		
セキュア・サーバID EV	Secure Site EV		
セキュア・サーバID	Secure Site OV		
スタンダード・サーバID EV	Basic EV	digicert SECURED	当製品のサイトシール用HTML/JavaScriptコードは、弊社テクニカルサポートを通じてご提供させていただいております。ご要望のお客様は弊社テクニカルサポートへご連絡ください。
スタンダード・サーバID	Basic OV		
ジオトラスト トゥルービジネスID with EV	GeoTrust TrueBusiness ID EV	GeoTrust SECURED powered by digicert	CertCentralのオーダー詳細画面～「証明書操作」メニュー配下の「サイトシール」ページより、シール掲載用HTML/JavaScriptを入手いただけます。 (詳細は後述)
ジオトラスト トゥルービジネスID	GeoTrust TrueBusiness ID OV		
ジオトラスト クイックSSLプレミアム	GeoTrust DV SSL		

※ シールのデザインや証明書製品との対応については今後変更される場合があります。

© 2021 DigiCert – All Rights Reserved

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)

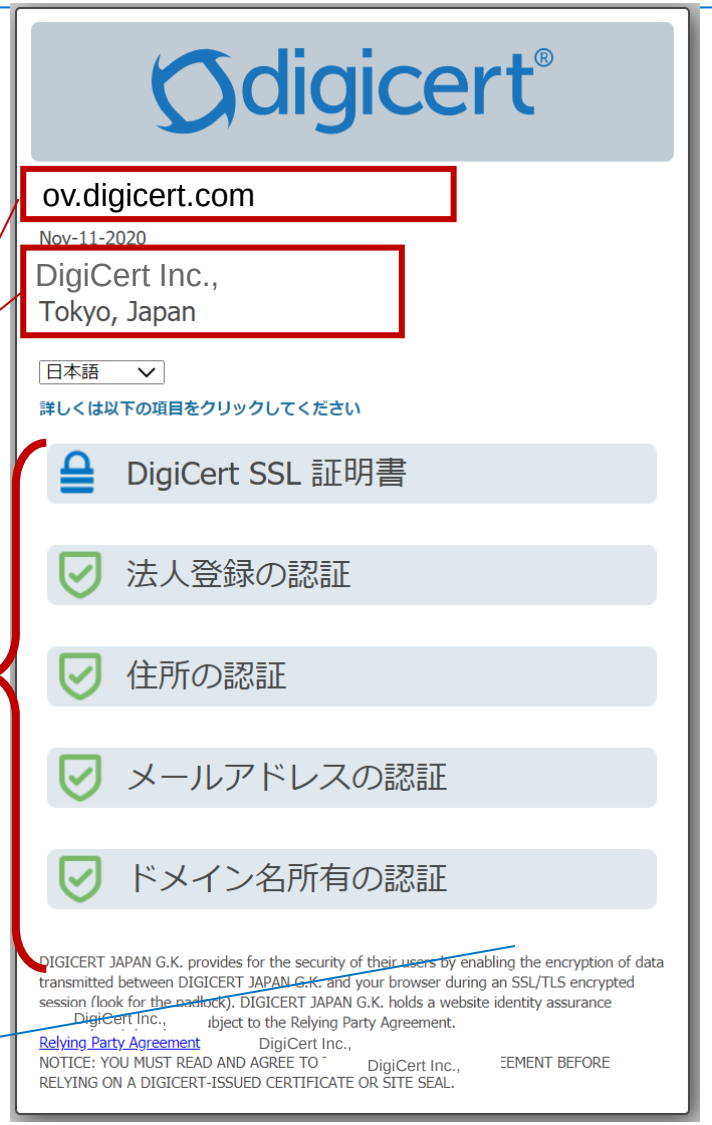
■(**DV証明書の場合**)サイトシール
スプラッシュページ(イメージ)

© 2021 DigiCert – All Rights Reserved

（参考）旧スプラッシュページとの比較

■(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

© 2021 DigiCert – All Rights Reserved

「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>
```

© 2021 DigiCert – All Rights Reserved

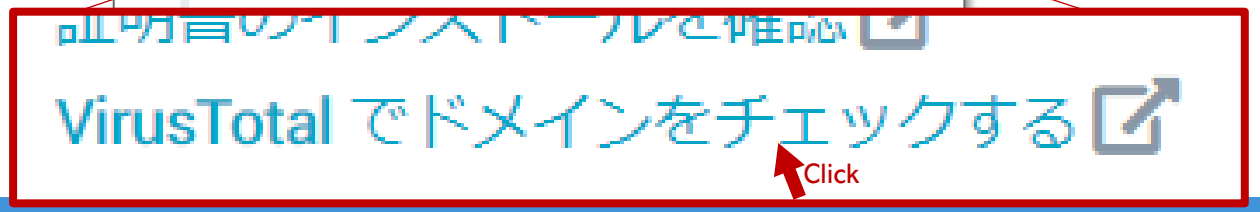
10. その他の証明書製品の機能

~ 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/

© 2021 DigiCert – All Rights Reserved

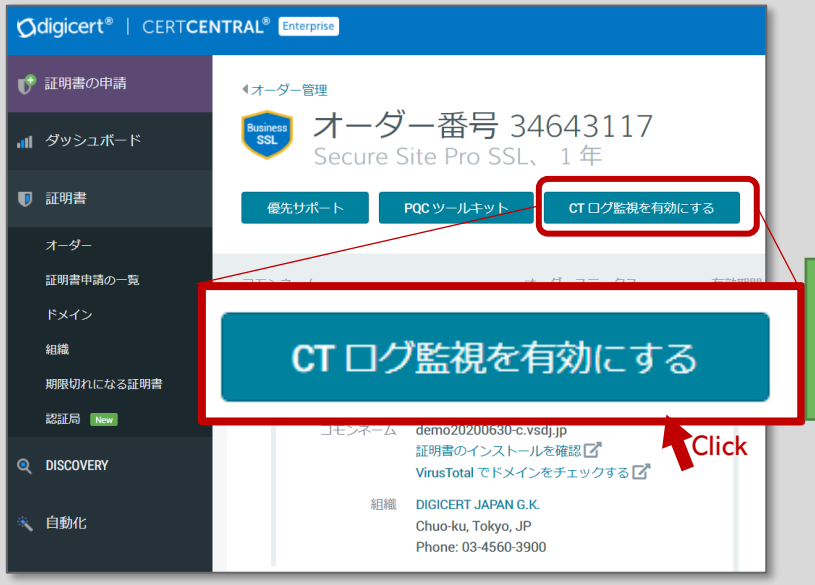
10. その他の証明書製品の機能

~ 10.3 CTログモニタリング ~

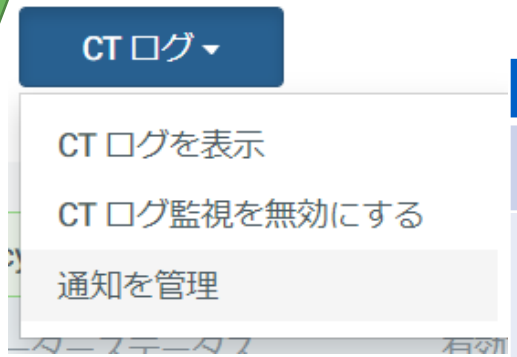
CTログモニタリング機能の有効化

■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/

© 2021 DigiCert – All Rights Reserved

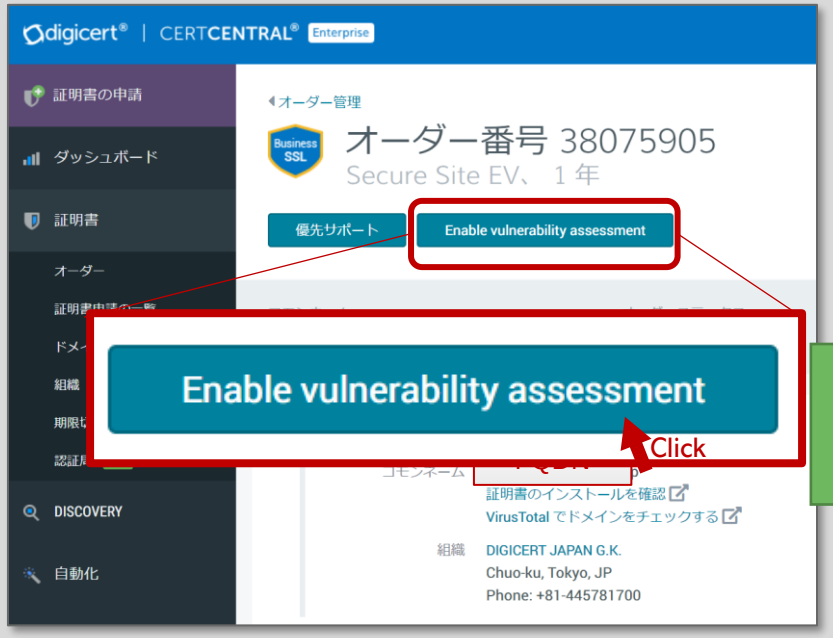
10.その他の証明書製品の機能

~ 10.4 脆弱性アセスメント ~

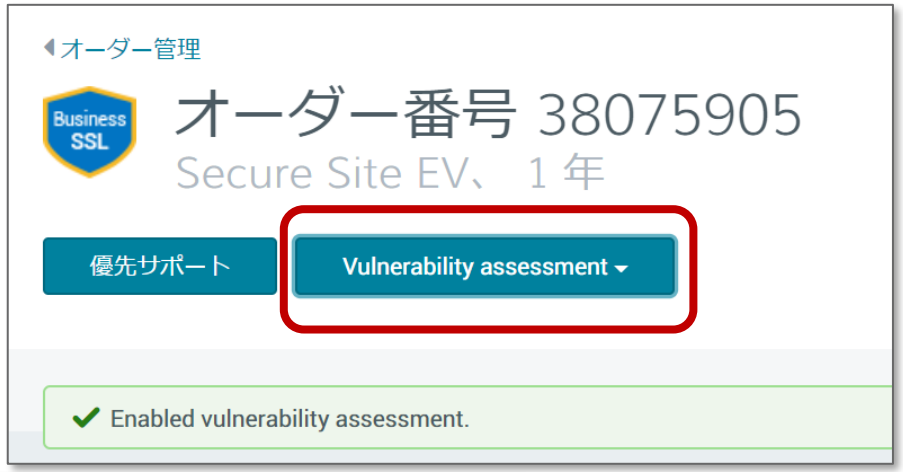
脆弱性アセスメント(Vulnerability Assessment)機能の有効化

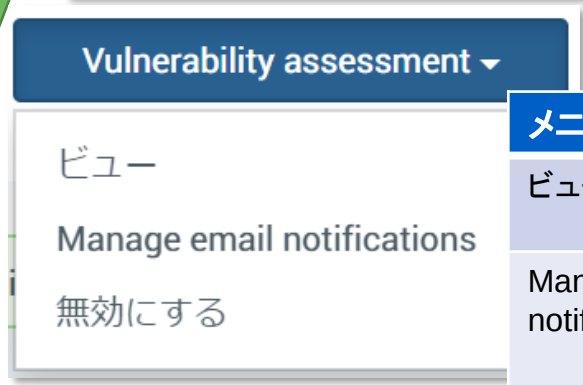
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■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

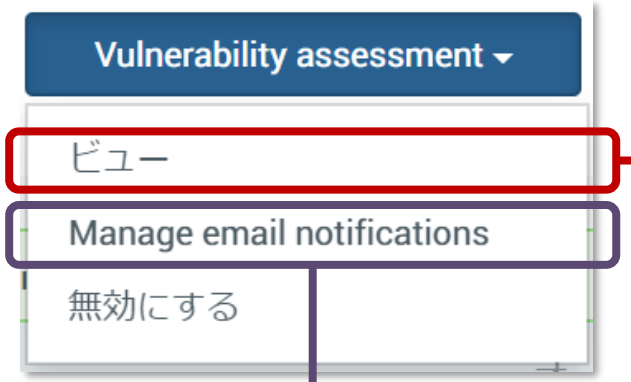
※1：脆弱性アセスメントの活用方法についてもっと詳しく：https://docs.digicert.com/ja/certificate-tools/vulnerability-assessment-service/

© 2021 DigiCert – All Rights Reserved

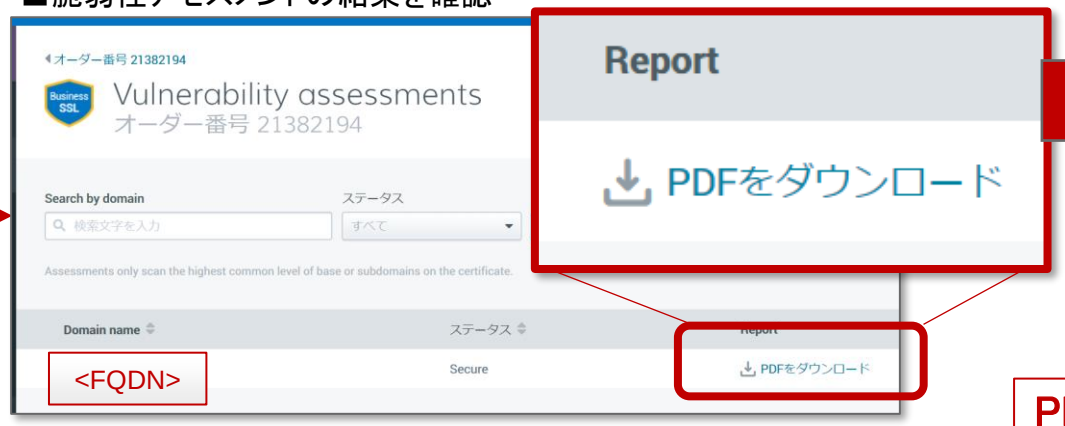
脆弱性アセスメント(Vulnerability Assessment)機能の管理

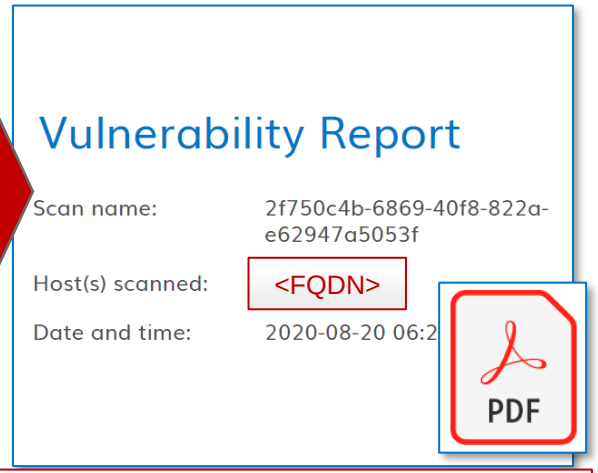
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

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



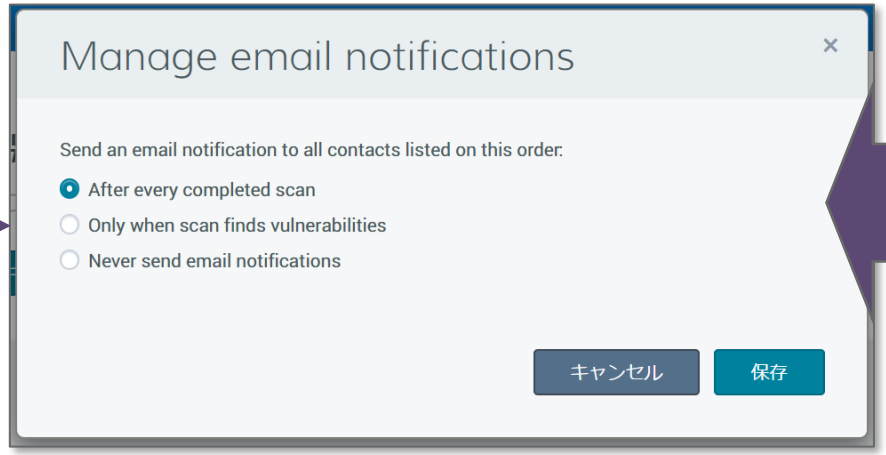
■脆弱性アセスメントの結果を確認





**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/

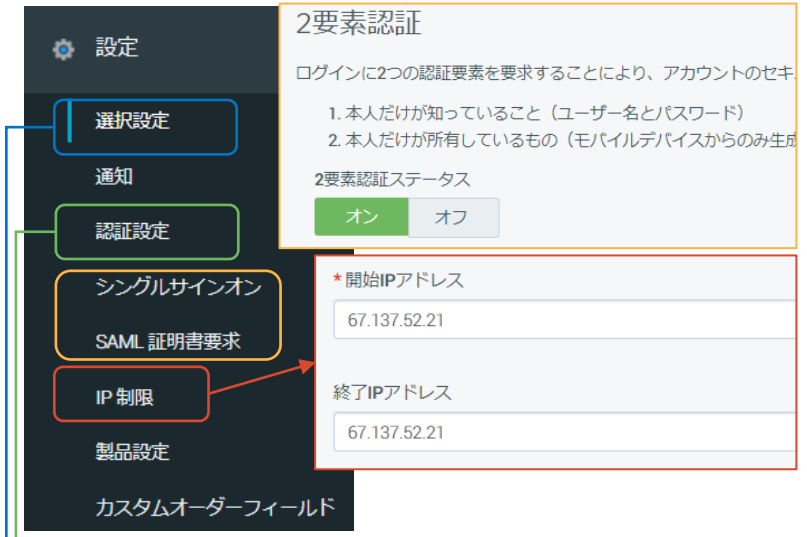
© 2021 DigiCert – All Rights Reserved

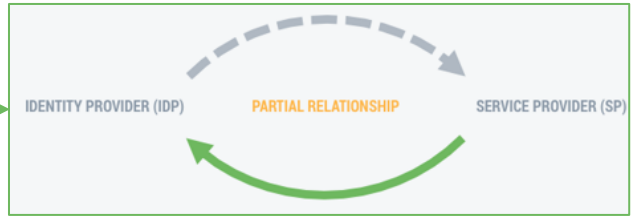
11. その他の管理機能・TIPS

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



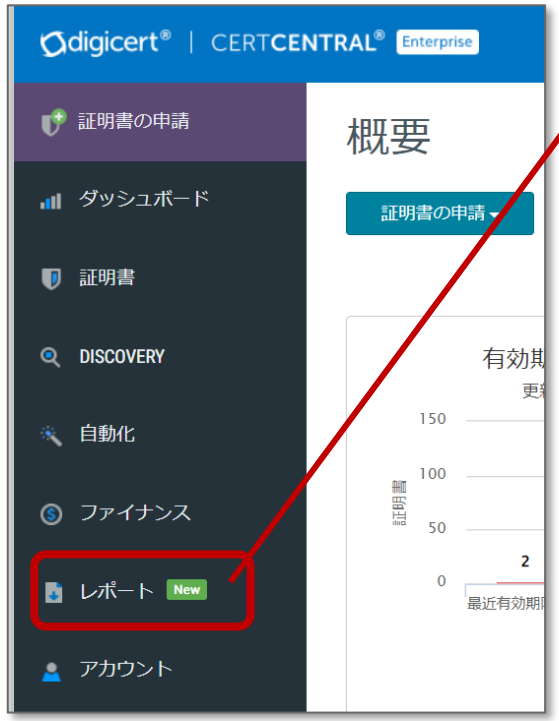


当ページに記載の画面イメージ等は、今後変更となる可能性があります。ご理解・ご了承ください。

© 2021 DigiCert – All Rights Reserved

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。