【CertCentral Enterprise 簡易マニュアル 別冊】

[ゲストユーザー]様向け CertCentral利用ガイド

最終更新日：2021年 3月 16日
デジサート・ジャパン合同会社

目次

1. はじめに

はじめに

- 当資料は、[ゲストユーザー]様が、組織の管理者が生成・管理する[固有の申請用URL]を通じてCertCentralにアクセスし、証明書申請等の手続きをいただく手順のガイダンスを提供するものです
  - [ゲストユーザー]とは : CertCentralのユーザーアカウントを持たないが、CertCentralの【ゲストURL】【ゲストアクセス】(詳細後述)機能を利用してデジサートのSSL/TLSサーバ証明書をご申請、取得いただくユーザー様を、当資料では便宜的に[ゲストユーザー]と呼称します。

- [固有の申請用URL]は、組織の管理者によって、以下の機能を用いて提供されます
  - 【ゲストURL(Guest URL)】：証明書新規申請用に用いられる固有の申請用URLを作成、管理する機能
  - 【ゲストアクセス(Guest Access)】：証明書更新申請、再発行・複製・失効申請に用いられる固有の申請用URLを管理する機能

- [固有の申請用URL]は組織の管理者によって管理されるCertCentralのアカウント毎に異なりますのでご注意ください。不明な場合は組織の管理者にお問合せください。

- 当資料内の画面イメージは予告なく変更される場合があります。予めご理解・ご了承ください。

変更履歴

Ver.	公開日	変更点	変更箇所
~0.9	2020/11/1	省略	-
1.0	2020/11/1	[1. はじめに]「変更履歴」ページを追加	Page 5
		[7. ゲストアクセスリンクからサイトシールを取得] セクションを追加	Page 35-39
1.1	2021/1/5	[2. ゲスト URL による証明書新規申請] 多言語対応等に伴う改訂 画面イメージ最新化、説明の詳細化等	Page 9-15
1.2	2021/1/21	[2. ゲスト URL による証明書新規申請] 機能拡充等に伴う改訂 「複数年プラン」の申請手順を追記、画面イメージ最新化等	Page 7-20
		[3. ゲストアクセスによる証明書更新申請] 多言語対応、機能拡充等に伴う改訂 「複数年プラン」の申請手順を追記、画面イメージ最新化等	Page 21-3
		ゲストアクセス機能の証明書管理機能拡充に伴い、[再発行申請][失効申請]等のライフサイクル管理手順を [4. ゲストアクセスによる証明書再発行、複製および失効申請 に統合	Page 33-39
		[5.2 ゲストアクセスから証明書をダウンロード] セクションを追加	Page 46-48
1.3	2021/3/16	[3. ゲストアクセスリンクによる証明書オーダー情報へのアクセス]を分割し独立 これに伴いセクション構成を改訂	Page 21-27
		[8.ゲストアクセスによる証明書製品のその他の機能の利用]セクションを追加	Page 58-64

※ 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。

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

マネージドPKI for SSL

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

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

管理者によるレビュー・承認
→証明書発行、失効完了

CertCentral

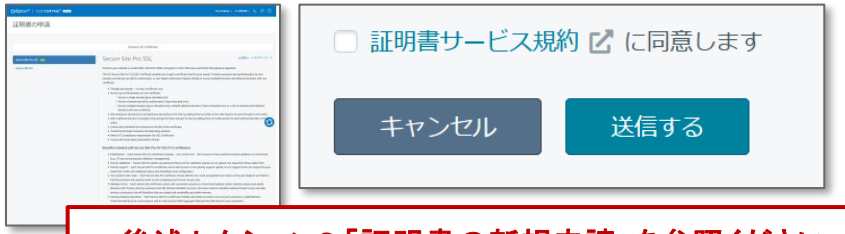
■CertCentral ゲストユーザー向け機能

ゲストユーザー

証明書新規申請

【ゲストURL】

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



→後述セクション2「証明書の新規申請」を参照ください

証明書更新申請／再発行／失効など

【ゲストアクセス】

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

→後述セクション3および4「証明書の更新申請」を参照ください

管理者によるレビュー・承認
→証明書発行、失効完了

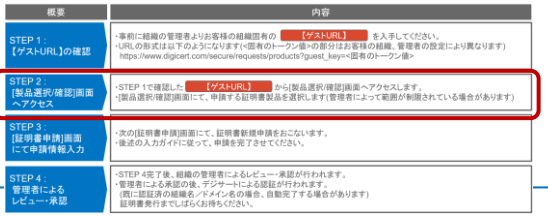
2. ゲストURLによる証明書新規申請

ゲストURLによる証明書新規申請の流れ

[ゲストユーザー]様による、【ゲストURL】機能を用いた証明書新規申請の手順は以下の通りとなります。

概要	内容
STEP 1 : 【ゲストURL】の確認	・事前に組織の管理者よりお客様の組織固有の【ゲストURL】を入手してください。 ・URLの形式は以下のようになります(<固有のトークン値>の部分はお客様の組織、管理者の設定により異なります) https://www.digicert.com/secure/requests/products?guest_key=<固有のトークン値>
STEP 2 : [製品選択/確認]画面 へアクセス	・STEP 1で確認した【ゲストURL】から[製品選択/確認]画面へアクセスします。 ・[製品選択/確認]画面にて、申請する証明書製品を選択します(管理者によって範囲が制限されている場合があります)
STEP 3 : [証明書申請]画面 にて申請情報入力	・次の[証明書申請]画面にて、証明書新規申請をおこないます。 ・後述の入力ガイドに従って、申請を完了させてください。
STEP 4 : 管理者による レビュー・承認	・STEP 3完了後、組織の管理者によるレビュー・承認が行われます。 ・管理者による承認の後、デジサートによる認証が行われます。 (既に認証済の組織名／ドメイン名の場合、自動完了する場合があります) 証明書発行までしばらくお待ちください。

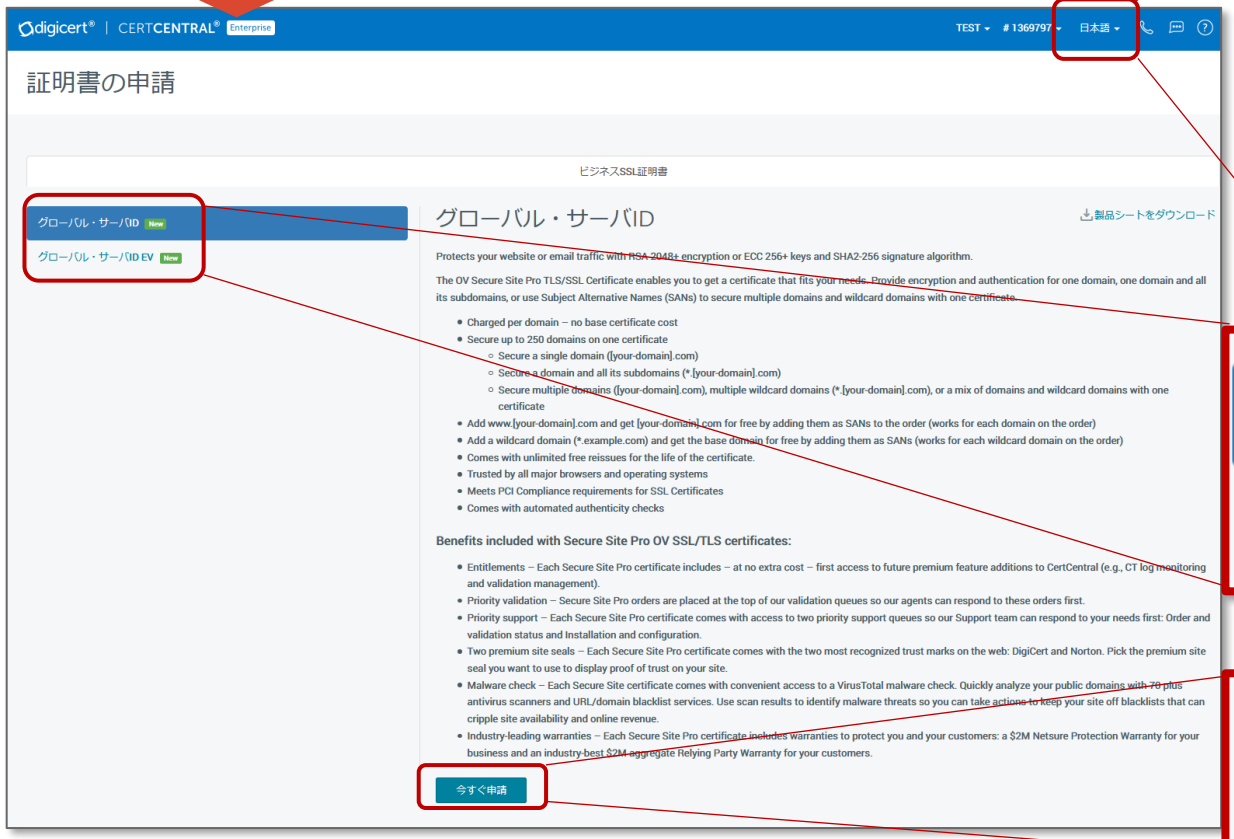
ゲストURL機能の利用 (ゲストURLを用いた証明書申請)

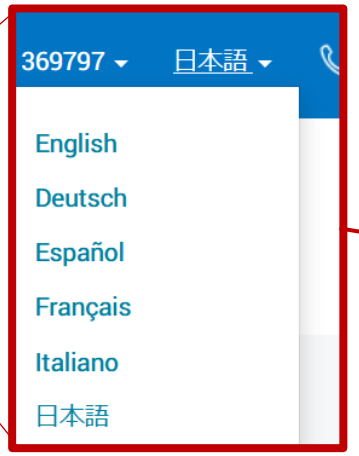


■ゲストURLへのアクセス後の製品選択/確認画面(※1)

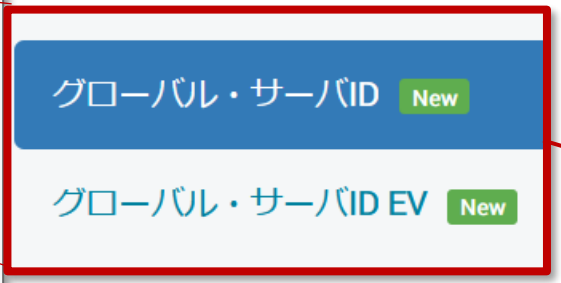
ゲストユーザー

【ゲストURL】

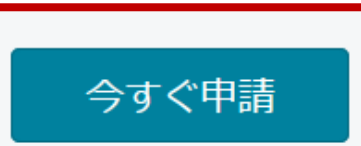




ゲストURLで使用する
画面表示言語を指定します
(管理者によってデフォルトの
言語が指定されています)

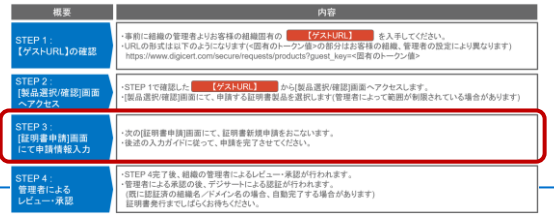


複数の製品が表示されて
いる場合は選択します。



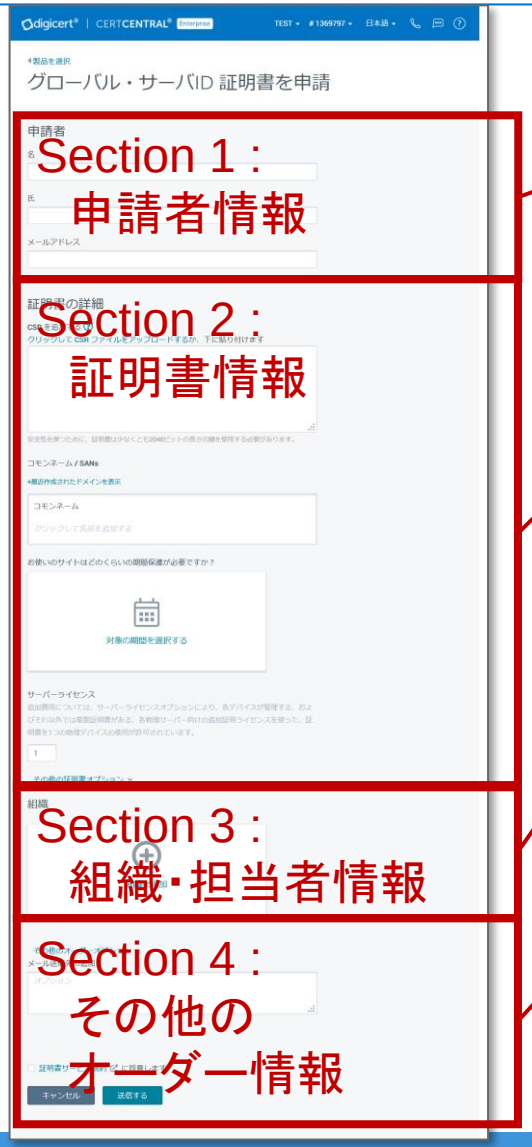
証明書申請画面へ
移動します

ゲストURL機能の利用 (ゲストURLを用いた証明書申請)



■証明書申請画面(※1)

ゲストユーザー



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

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

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)

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

次ページ以降で詳細な入力方法をガイドします。

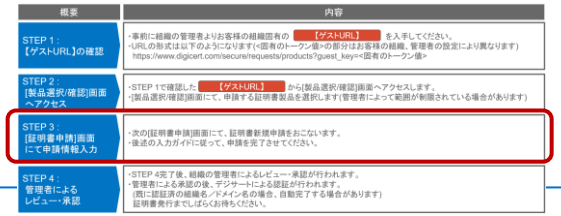
※1：画面表示言語に「日本語」を指定した場合のイメージ
※2：ゲストURLの証明書申請画面では、組織の管理者の設定によって表示が省略されたり、追加で入力が必須となる項目があります。

Section 1：申請者情報の入力

■凡例

・・・必須(入力または選択)

・・・自動設定可または任意

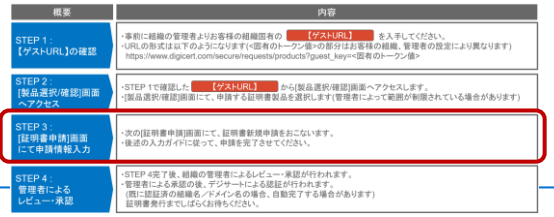


■証明書申請画面

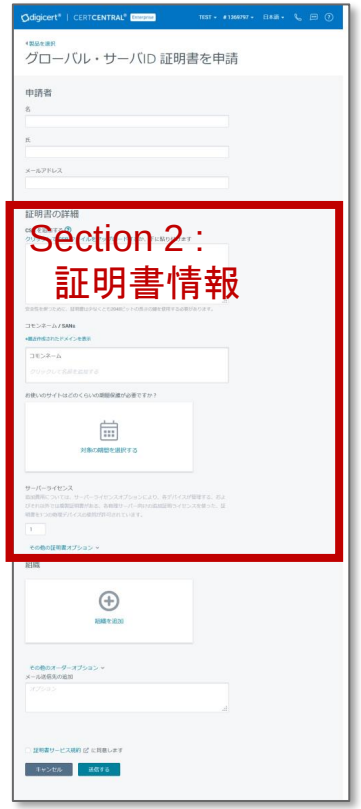
■【必須】申請者情報
名：申請者氏名の「名」を入力ください。
氏：申請者氏名の「氏」を入力ください。
メールアドレス：申請者のメールアドレスを入力ください。

Section 2：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



■証明書申請画面



■【必須】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」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。

注：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

■【必須・自動設定あり】コモンネーム / SANs
・初期状態では更新元証明書と同一のFQDNが設定された状態
・任意の値に上書き可能です。一度当欄を空白にクリアしてから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)が自動設定されます。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。

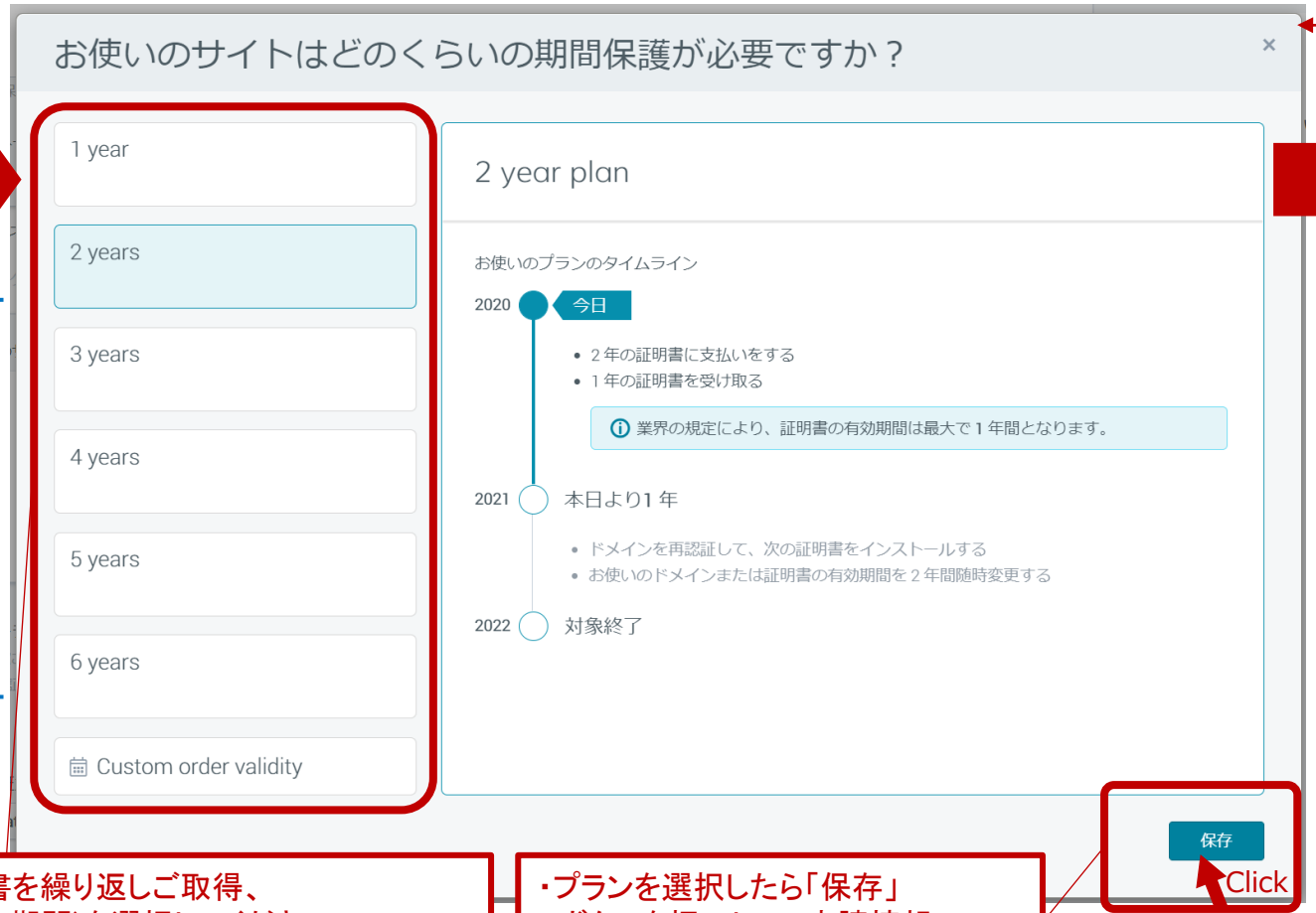
■【必須】期間：
・ご申請いただくプラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択ください
・プラン選択後、プランの初回にご取得いただく証明書の有効期間を選択・指定いただけます(最大397日間)
→詳細は次ページ[補足 プランの選択]をご参照ください

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

補足 プラン(契約期間)の選択

例1：ユニットライセンスを都度ご購入いただいているお客様の場合

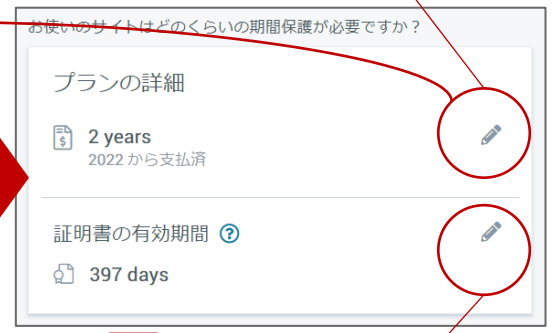
■「プラン(契約期間)」をご選択いただくイメージ（例：2年間有効な複数年プランをご選択いただいた場合）



最大6年間まで
選択可能

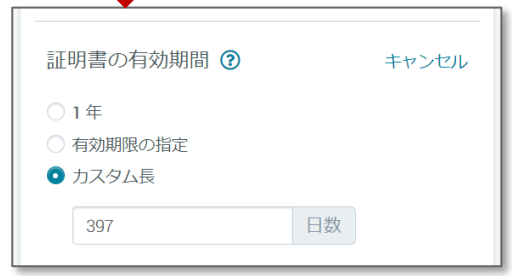
・枠内の選択肢から、プラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択してください。
例:「2 years」=2年間プラン

・プランを選択したら「保存」ボタンを押下して、申請情報入力画面に戻ります



このアイコンをクリックすると
プラン選択ウィンドウが再度
開きます

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



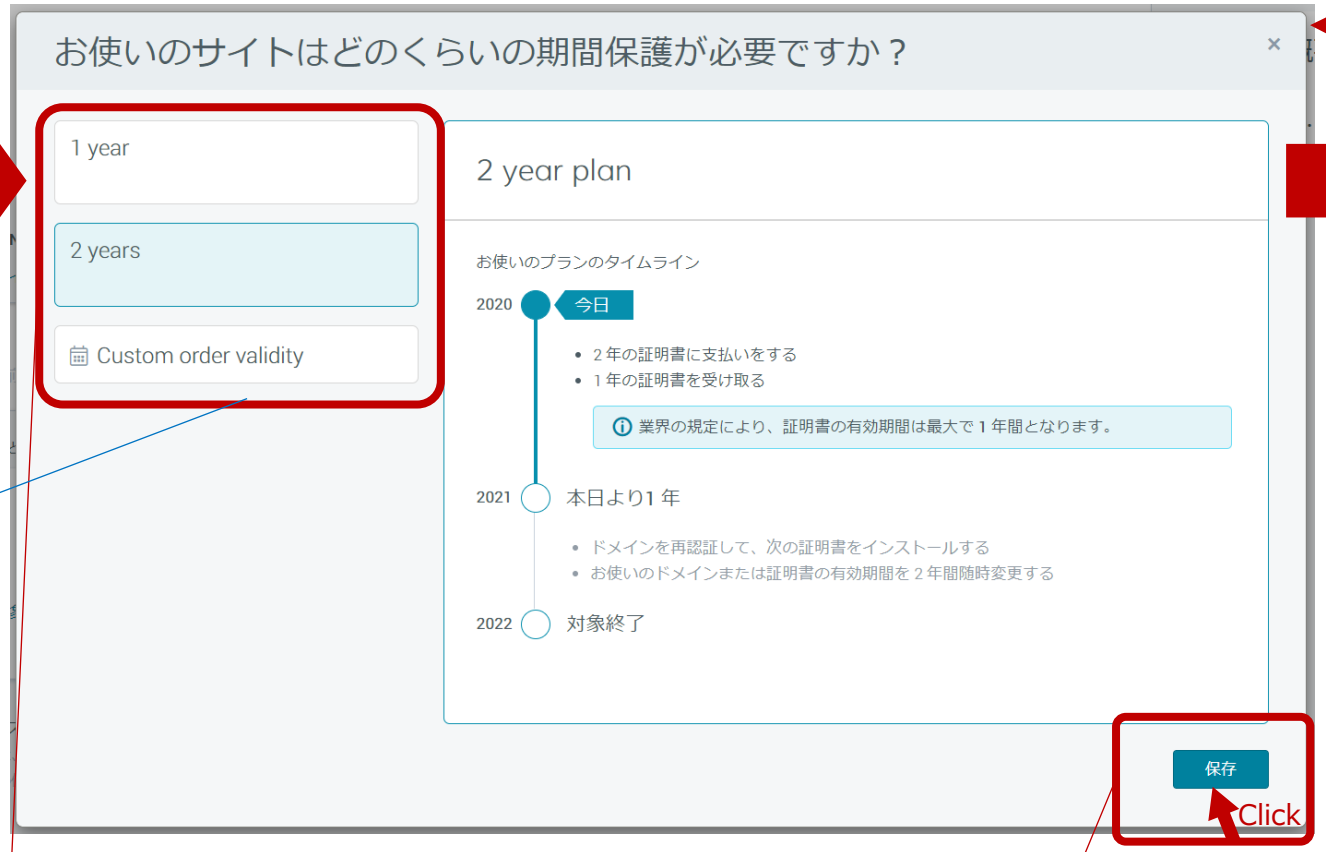
指定によって実際に発行される証明書の有効期間の設定のされ方の詳細については
FAQ(※1)を参照ください

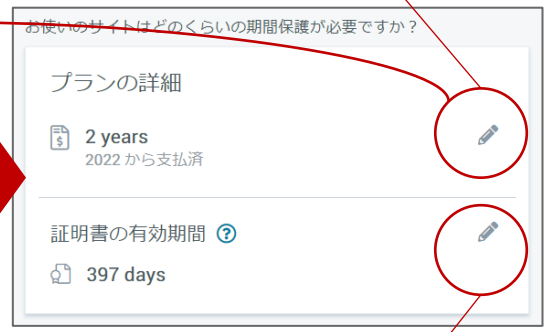
※1：FAQ「サーバ証明書の有効期間について」：https://knowledge.digicert.com/ja/jp/solution/SO22917.html

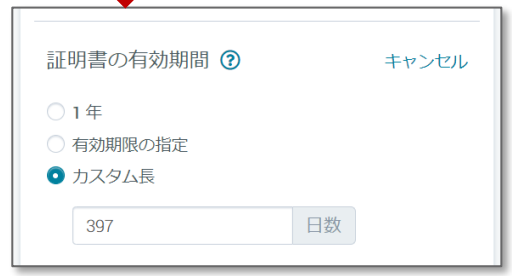
補足 プラン(契約期間)の選択

例2：サブスクリプション契約をご締結いただいているお客様の場合

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







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。

**最大2年間まで
選択可能**

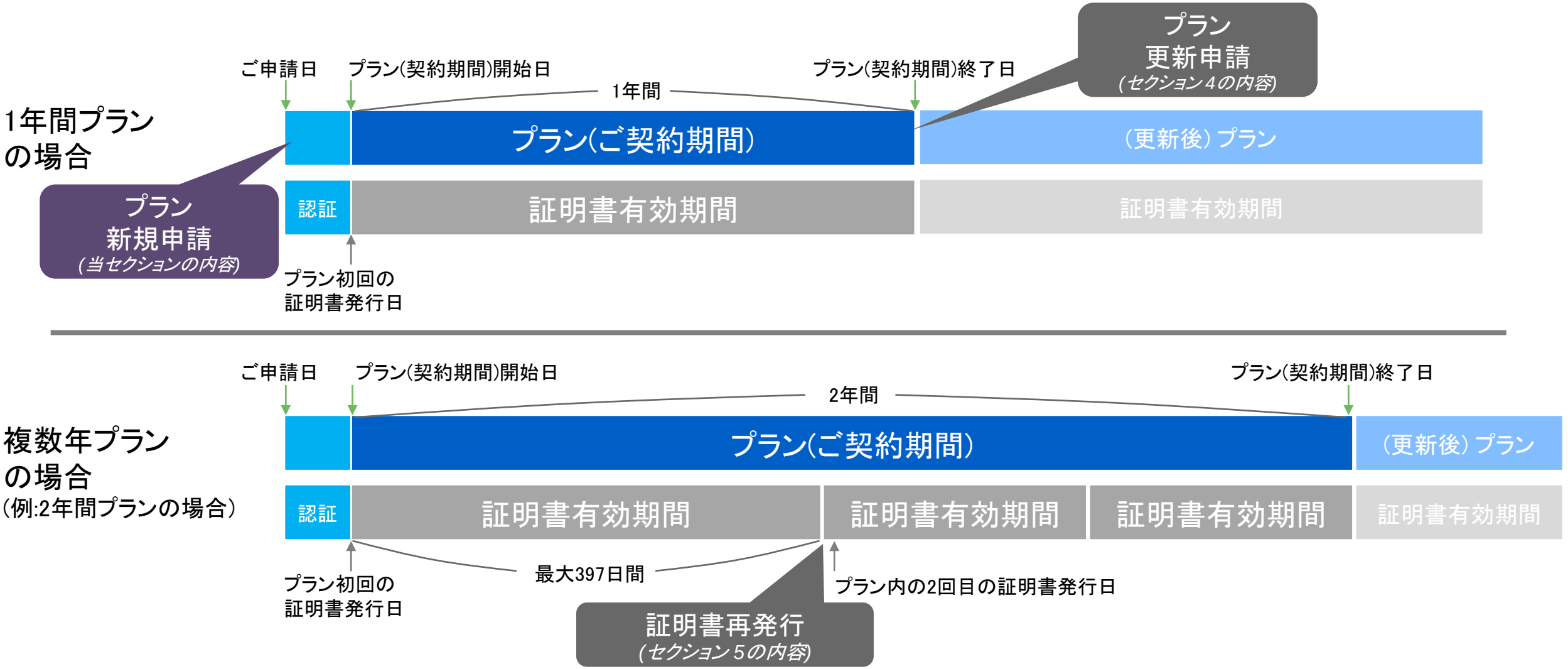
・枠内の選択肢から、プラン(証明書を繰り返しご取得、
継続してご利用いただけるご契約期間)を選択してください。
例:「2 years」=2年間プラン

・プランを選択したら「保存」
ボタンを押下して、申請情報
入力画面に戻ります

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

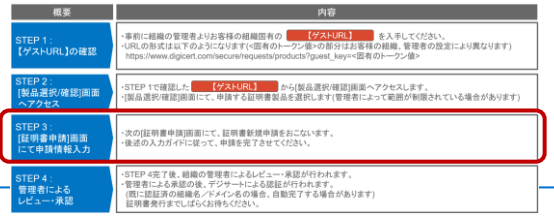
※1：FAQ「サーバ証明書の有効期間について」：https://knowledge.digicert.com/ja/jp/solution/SO22917.html

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



Section 2 : 証明書情報の入力 (続き)

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意



■証明書申請画面

■ドメイン名利用権確認(DCV)

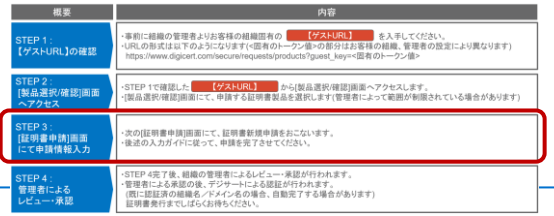
■【アカウント設定によって必須】ドメイン名利用権確認(DCV)
・アカウントの管理者によって非表示に設定されている場合があります
・表示されている場合;
┗<既に登録済かつ認証済のドメイン名>を利用した申請の場合、
設定値は無視されます(DCVメールの送信やファイル認証の
ポーリングは行われません)
┗<新しいドメイン名>を利用した申請の場合、
「DCV認証方式」で選択した方法でドメイン名の利用権を確認します
※1 : 詳細はこちらを参照ください
[DCV] SSL/TLS サーバ証明書のドメイン名の認証(共通)
https://knowledge.digicert.com/ja/jp/solution/SO23241.html
※2:組織のポリシーによって、ゲストURL での証明書申請時に新しい
ドメイン名の追加が許可されている場合にのみ利用します

■【任意】その他の証明書オプション
クリックして追加入力フィールドを表示すると以下の設定が可能です。
・中間チェーン:証明書チェーン(中間証明書とルート証明書の組合せ)を選択します
※組織のアカウント設定によって表示されない場合があります
※製品種類によってご利用いただけるチェーンの種類は異なります(※3,4)
・署名ハッシュ:
お客様のサーバ証明書(End-Entity)に対する署名アルゴリズムを
選択可能です(選択肢:SHA-256(標準), SHA-384, SHA-512)。
・サーバープラットフォーム:
お客様のサーバープラットフォーム環境を選択し、発行通知メールに
添付される証明書ファイル形式を最適化いただけます
※ 発行通知メールの形式は組織の管理者によって指定されます
※ ファイル形式の詳細はセクション「6.1. 発行通知メールから証明書を取得」を
併せて参照ください

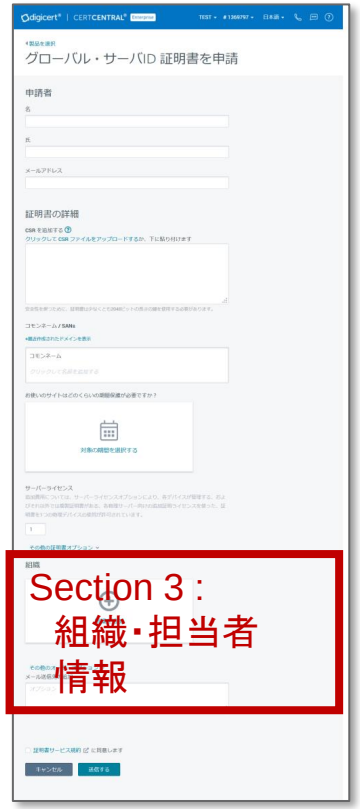
※3 : 各製品ごとにご利用いただける中間証明書とルート証明書の組合せについて : https://knowledge.digicert.com/ja/jp/solution/SOT0006.html
※4 : 中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、
最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら : https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

Section 3 : 組織・担当者情報 (OV証明書の場合)

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意



■証明書申請画面



■組織・担当者情報欄:(自動)入力前の状態

■(自動)入力後の状態

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

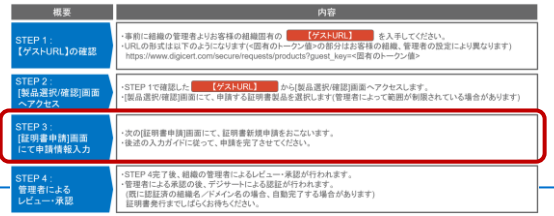
■連絡先 確認・設定欄

■【アカウント設定によって任意】担当者情報 (Contacts)
・アカウントの管理者によって非表示に設定されている場合があります
・表示されている場合、証明書の申請に関する「技術担当者」および「申請責任者」を確認・設定することができます。
・上部の「組織情報」欄に登録・認証済の組織情報が選択・設定された場合、該当の組織情報に紐づいてCertCentralが保持する担当者情報がオーダーの担当者として自動設定されます。

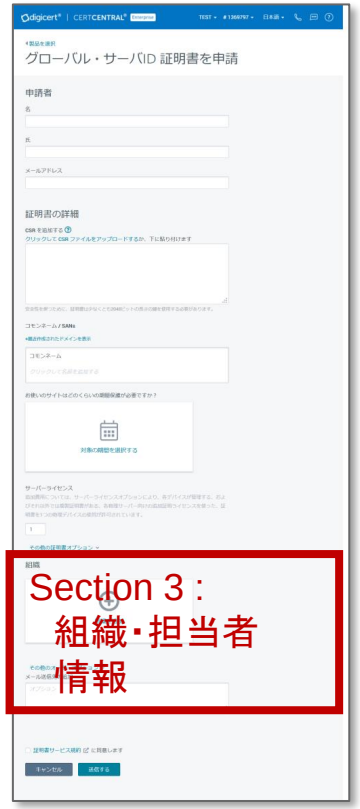
→変更する必要が無い場合はそのまま申請を進めてください。
不明な場合は組織のアカウント管理者にお問合せください

Section 3 : 組織・担当者情報 (EV証明書の場合)

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意



■証明書申請画面

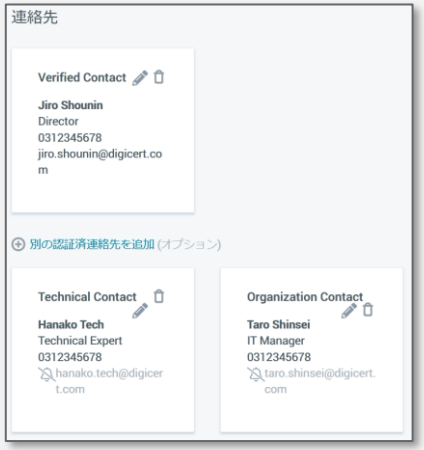


■組織・担当者情報欄:(自動)入力前の状態

■(自動)入力後の状態

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

■連絡先 確認・設定欄

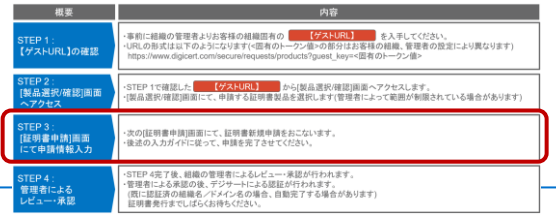


■【アカウント設定によって任意】担当者情報 (Contacts)
・アカウントの管理者によって非表示に設定されている場合があります
・表示されている場合、証明書の申請に関する「認証済連絡先」、「技術担当者」および「申請責任者」を確認・設定することができます。
・上部の「組織情報」欄に登録・認証済の組織情報が選択・設定された場合、該当の組織情報に紐づいてCertCentralが保持する担当者情報がオーダーの担当者として自動設定されます。

→変更する必要が無い場合はそのまま申請を進めてください。
不明な場合は組織のアカウント管理者にお問合せください

Section 4：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



■証明書申請画面

■その他のオーダーオプション 入力欄

■メール送信先の追加 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
クリックして追加入力フィールドを表示すると以下の設定が可能です。
・「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。

■【任意】「メール送信先の追加」:申請者に加えて、申請関連のメールや
更新案内メールの送信先を追加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。「送信する」を
押下して申請を完了させてください。

【ゲストURL】による証明書新規申請について – よくあるご質問 -

Q (ご質問)	A (回答)
証明書を申請する組織名／申請団体名(証明書のSubject Organization)はどのようなものでもよいのですか？	組織のポリシーによって、ゲストURLでの証明書申請時に新しい組織情報の追加が許可されていない場合があります。 証明書申請に利用可能な組織名／申請団体名や、追加の可否については、必要に応じて組織の管理者にご確認ください。
証明書を申請するドメイン名はどのようなものでもよいのですか？	組織のポリシーによって、ゲストURLでの証明書申請時に新しいドメイン名の利用が許可されていない場合があります。 証明書申請に利用可能なドメイン名や、追加の可否については、必要に応じて組織の管理者にご確認ください。
・[DCV 認証方式][DCV Email Language]という項目は何ですか？ ・この項目は入力/選択しなくてよいのですか？	組織のポリシーによって、ゲストURLでの証明書申請時に新しいドメイン名の追加が許可されている場合にのみ利用します。 既に登録済かつ認証済のドメイン名を利用した申請の場合には設定値は無視されます(DCVメールの送信やファイル認証のポーリングは行われません)。
証明書階層構造を選択できる機能はないのですか？	組織の管理者による設定によって設定可能である場合／不可である場合があります。詳細は管理者にご確認ください。
申請画面の最下部に、このガイドには書かれていない、または名称の異なる追加のフィールドがあります。これは何ですか？	組織の管理者によって申請時の入力項目としてカスタムオーダーフィールド（お客様組織独自の追加入力・管理項目）が設定されている場合があります。 追加項目の詳細は管理者にご確認ください。

3. ゲストアクセスリンクによる証明書オーダー情報へのアクセス

（参考）ゲストアクセスリンクによる証明書更新申請の流れ

[ゲストユーザー]様による、【ゲストアクセス】機能を用いた証明書更新申請の手順は以下の通りとなります。

概要	内容
STEP 1 : 【ゲストアクセスリンク】 の確認	・事前に組織の管理者よりお客様の組織固有の【ゲストアクセスリンク】を入手してください。 ・【ゲストアクセスリンク】の形式は以下のようになります https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分はお客様の組織、管理者の設定により異なります)
STEP 2 : オーダーアクセス用 認証コードの取得	・STEP 1で確認した【ゲストアクセスリンク】からオーダーアクセス用の認証コードを取得します。 ・指定したメールアドレスに送信される認証コードを使用して、オーダー詳細画面へアクセスします。
STEP 3 : オーダー詳細画面 にて対象を確認	・オーダー詳細画面で、更新申請を行う対象のオーダー情報を確認します。
STEP 4: [証明書申請]画面 にて申請情報入力	・次の[証明書申請]画面にて、証明書更新申請をおこないます。 ・後述の入力ガイドに従って、申請を完了させてください。
STEP 5 : 管理者による レビュー・承認	・STEP 4完了後、組織の管理者によるレビュー・承認が行われます。 ・管理者による承認の後、デジサートによる認証が行われます。 (既に認証済の組織名／ドメイン名の場合、自動完了する場合があります) 証明書発行までしばらくお待ちください。

当セクションの範囲

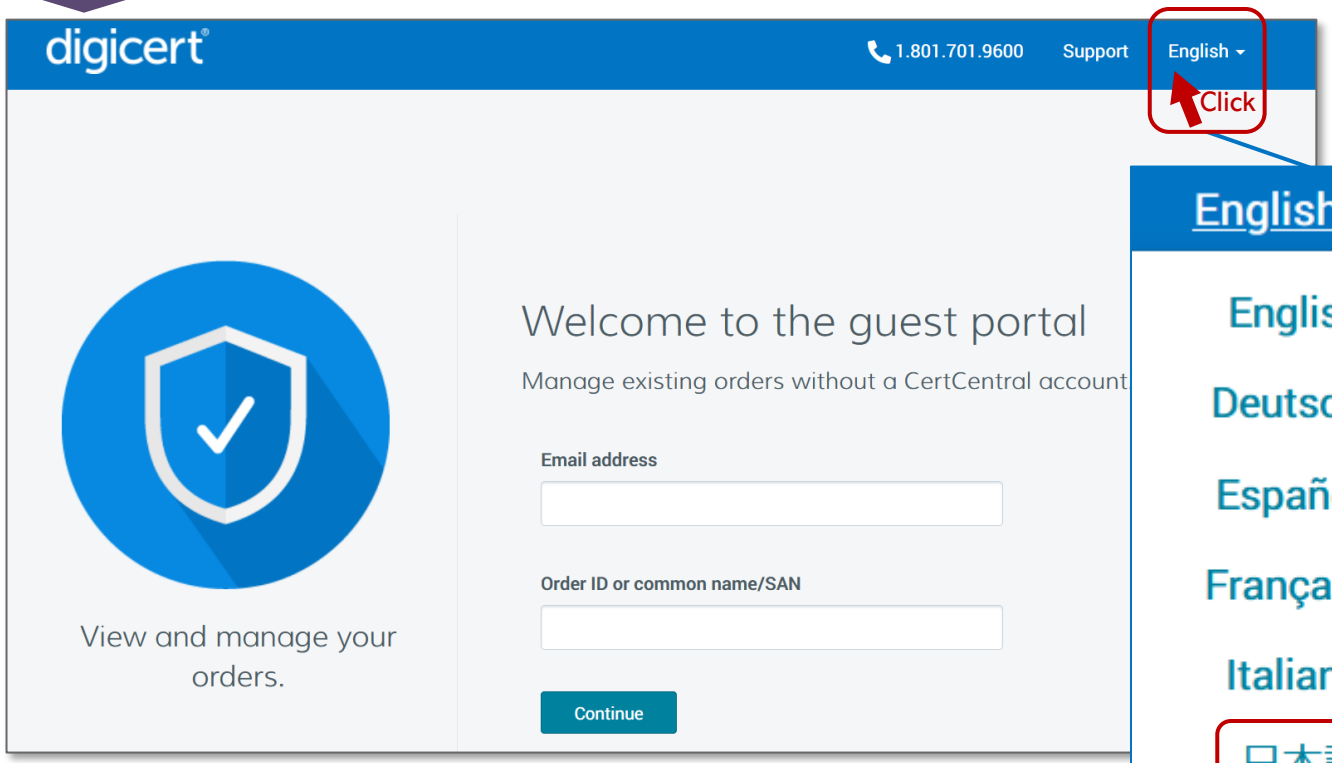
次セクションの範囲

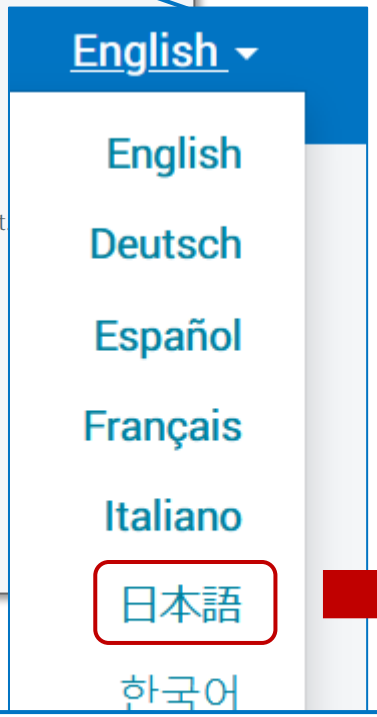
はじめに ~ゲストアクセス機能を「日本語」でご利用いただくために~

【ゲストアクセスリンク】

ゲストユーザー

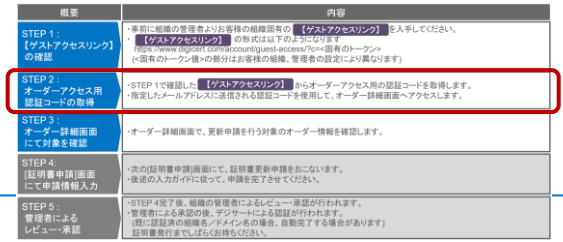
ゲストアクセスリンクからご利用いただく
各種機能を日本語画面でご利用いただくために、
言語選択リンクをクリックして、「日本語」を選択
してください。





以降のガイドは「日本語」を選択いただいた場合の画面イメージでご説明します

ゲストポータル – 認証コードの生成 (1/2)



【ゲストアクセスリンク】

ゲストユーザー

ゲストユーザーのメールアドレスを入力してください。

【重要】ゲストアクセス機能を利用いただくためには、入力したメールアドレスと、検索対象の証明書オーダーの属性情報のうち以下のいずれかの項目値とが合致する必要があります。

- Organization Contact(申請責任者)のメールアドレス
- Technical Contact(技術担当者)のメールアドレス
- Subscriber(申請者)のメールアドレス
- Additional Emails(追加のメールアドレス)

※ 証明書オーダーの担当者が、前任から引き継がれたなどのケースで変更となった場合、組織の管理者によってCertCentralの証明書オーダー情報のうち担当者のメールアドレス(Additional Emails)を上書きしていただくことで、ゲストアクセスが可能になります。詳細は組織の管理者にお問合せください。

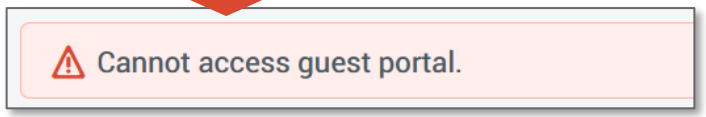
ゲストアクセス機能により更新申請を行う対象を特定するための検索キーとして**「オーダーID」**または**「コモンネーム/SAN」**の値を入力します。

対象オーダーが存在し、ゲストアクセスが許可されている場合

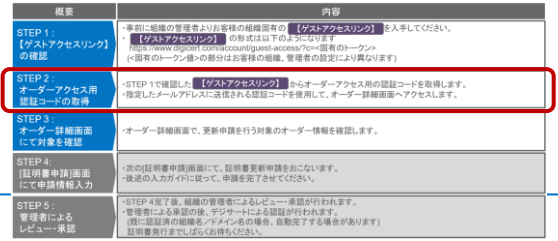
- 次の画面へ遷移します
- 同時に、[メールアドレス]欄に入力したメールアドレスに「認証コード」が送信されます。

ゲストアクセス用
認証コード通知メール

対象オーダーが存在しない場合、または管理者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



ゲストポータル – 認証コードの生成 (2/2)



ゲストアクセス用
認証コード通知メール

ゲストユーザー

画面は
自動遷移

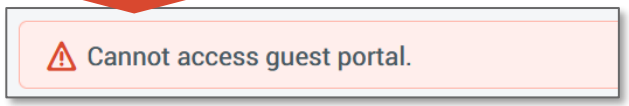
件名	DigiCert アクセスの認証コード
送信元	DigiCert <admin@digicert.com>
本文 イメージ (抜粋)	[お客様アカウント代表組織名]についてDigiCertゲストポータルへのアクセスのリクエストを受け取りました。 ゲストポータルにこのコードを入力し、オーダーにアクセスしてください。 [認証コード] Copy このコードとゲストポータルアクセスの有効時間は 2 時間です。この DigiCert アカウントへのアクセスへのリクエストを行った覚えがない場合、support@digicert.com に連絡の上、承認していない要請について報告してください。

ゲストアクセス用認証コード通知メールに含まれる[認証コード]を次の認証コード入力画面に入力して「サインイン」ボタンを押下します。

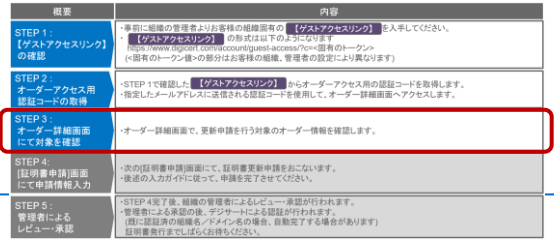
コードの検証が成功した場合

次の画面へ遷移します

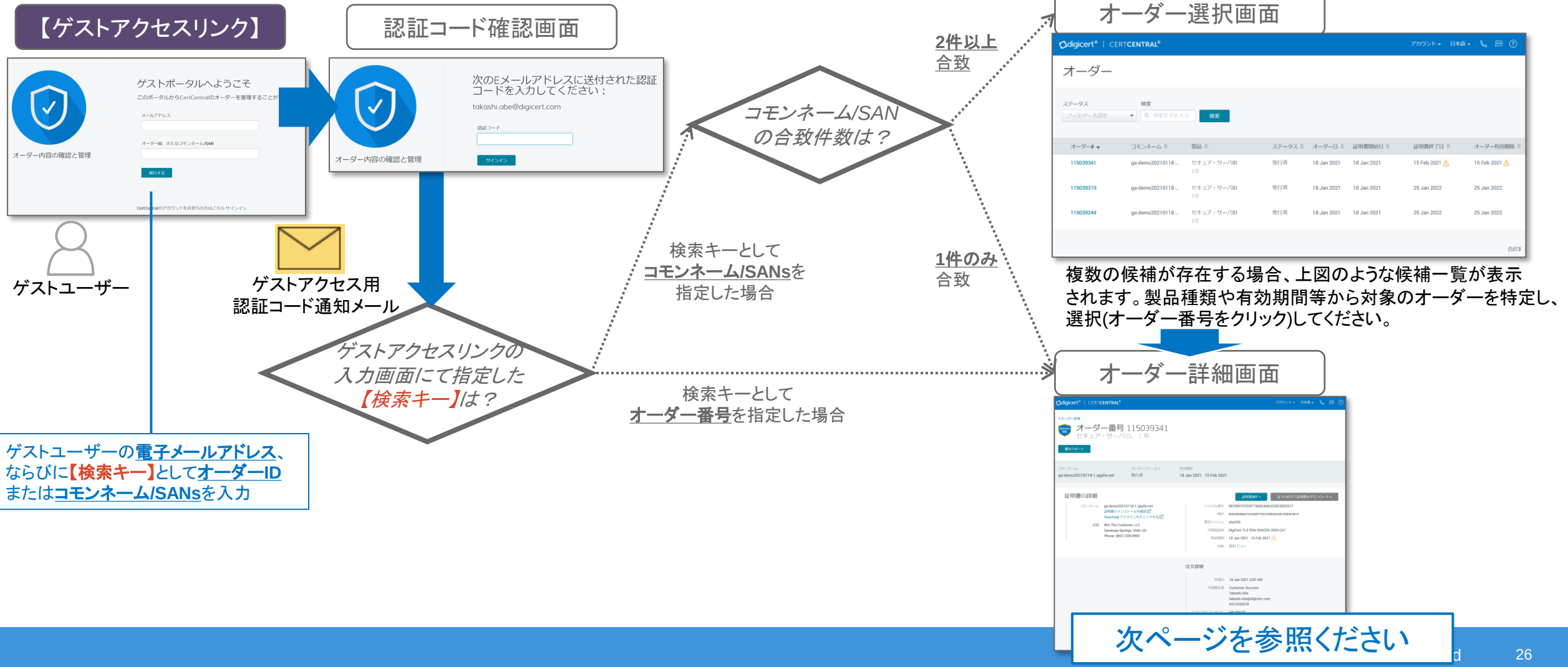
コードの検証が失敗した場合



オーダー詳細画面までの画面遷移



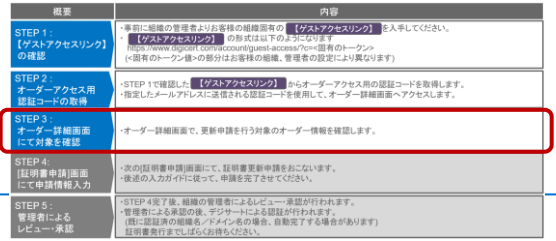
ゲストアクセスリンクの入力画面にて指定した検索キーの種類と、検索の結果合致した件数等の条件により画面遷移は以下のように異なります。



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。

次ページを参照ください

オーダー詳細画面



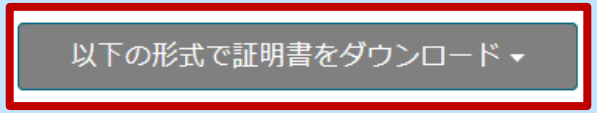
■オーダー詳細画面

ゲストユーザー

■証明書製品のその他機能へのリンク
当ページ上部に表示される各ボタンを押下することで、ビジネス証明書カテゴリのSSL/TLSサーバ証明書製品に付加された追加機能をご利用いただくことが可能です
→***セクション８「ゲストアクセスによる証明書製品のその他の機能の利用」を参照***

■「証明書操作」ボタンを押下すると、配下のメニューからサイトシールのダウンロードをいただくことが可能です。
必要に応じて証明書の更新、再発行、失効などの証明書ライフサイクル管理の操作が可能です。

メニュー	説明
証明書を再発行	→***セクション５を参照***
証明書を更新	→***セクション４を参照***
複製発行の申請	→***セクション５を参照***
証明書を失効	→***セクション５を参照***
サイトシール	→***セクション７を参照***



■「以下の形式で証明書をダウンロード」ボタンを押下すると
発行済の証明書をダウンロードいただけます。
→***セクション6.2「ゲストアクセスから証明書をダウンロード」を参照***

4. ゲストアクセスによる証明書更新申請

（参考）ゲストアクセスリンクによる証明書更新申請の流れ

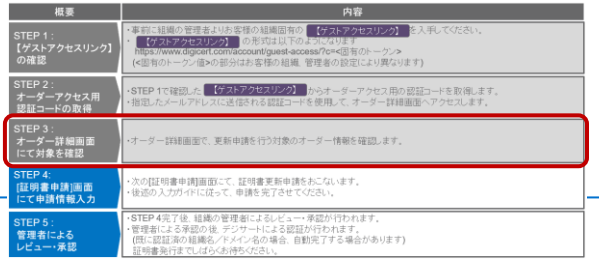
[ゲストユーザー]様による、【ゲストアクセス】機能を用いた証明書更新申請の手順は以下の通りとなります。

概要	内容
STEP 1 : 【ゲストアクセスリンク】 の確認	・事前に組織の管理者よりお客様の組織固有の【ゲストアクセスリンク】を入手してください。 ・【ゲストアクセスリンク】の形式は以下のようになります https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分はお客様の組織、管理者の設定により異なります)
STEP 2 : オーダーアクセス用 認証コードの取得	・STEP 1で確認した【ゲストアクセスリンク】からオーダーアクセス用の認証コードを取得します。 ・指定したメールアドレスに送信される認証コードを使用して、オーダー詳細画面へアクセスします。
STEP 3 : オーダー詳細画面 にて対象を確認	・オーダー詳細画面で、更新申請を行う対象のオーダー情報を確認します。
STEP 4: [証明書申請]画面 にて申請情報入力	・次の[証明書申請]画面にて、証明書更新申請をおこないます。 ・後述の入力ガイドに従って、申請を完了させてください。
STEP 5 : 管理者による レビュー・承認	・STEP 4完了後、組織の管理者によるレビュー・承認が行われます。 ・管理者による承認の後、デジサートによる認証が行われます。 (既に認証済の組織名／ドメイン名の場合、自動完了する場合があります) 証明書発行までしばらくお待ちください。

前セクションの範囲

当セクションの範囲

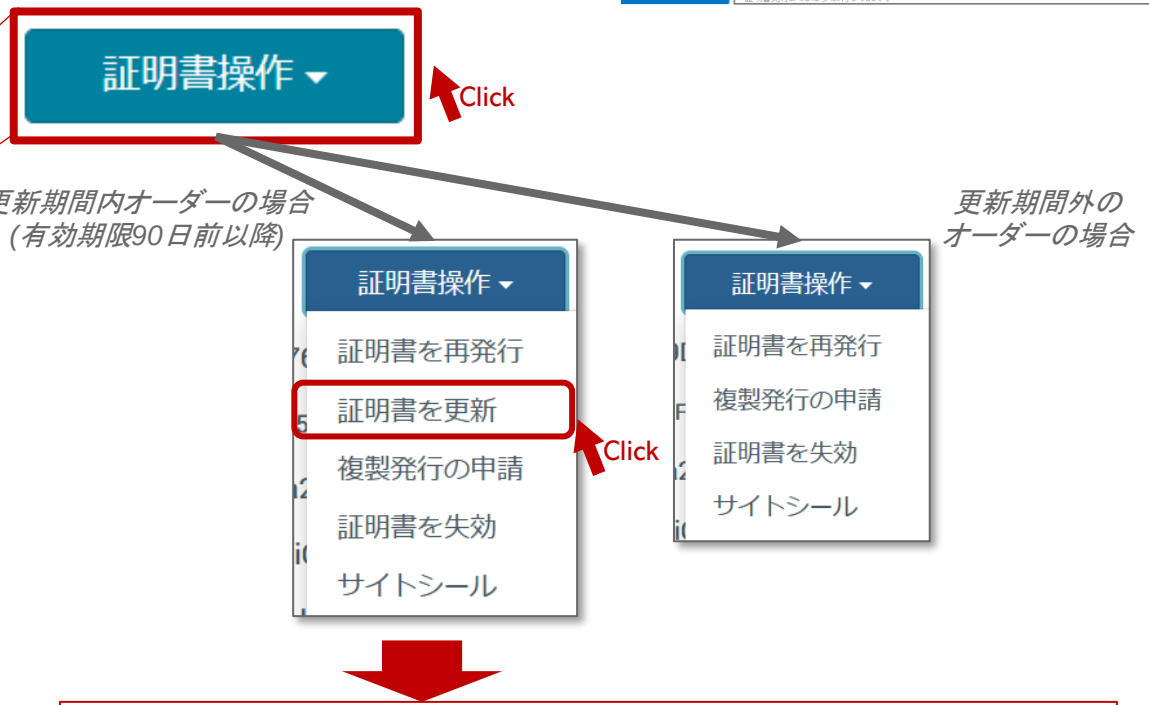
オーダー詳細画面から更新申請を開始する流れ



■オーダー詳細画面

ゲストユーザー

■証明書操作



「証明書を更新」ボタンを押下して、次の[証明書申請]画面にて証明書更新申請をおこないます。

後述の入力ガイドに従って、申請ください。

更新申請画面 – 概要

概要	内容
STEP 1：【ゲストアクセスリンク】の確認	・事前に組織の管理者よりお客様の組織固有の【ゲストアクセスリンク】を入手してください。 ・【ゲストアクセスリンク】の形式は以下のようになります。 https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分はお客様の組織・管理者の設定により異なります)
STEP 2：オーダーアクセス用認証コードの取得	・STEP 1で確認した【ゲストアクセスリンク】からオーダーアクセス用の認証コードを取得します。 ・指定したメールアドレスに送信される認証コードを使用して、オーダー詳細画面へアクセスします。
STEP 3：オーダー詳細画面にて対象を確認	・オーダー詳細画面で、更新申請を行う対象のオーダー情報を確認します。
STEP 4：[証明書申請]画面にて申請情報入力	・次の[証明書申請]画面にて、証明書更新申請をおこないます。 ・後述の入力ガイドに従って、申請を完了させてください。
STEP 5：管理者によるレビュー・承認	・STEP 4完了後、組織の管理者によるレビュー・承認が行われます。 ・管理者による承認の後、デジサートによる認証が行われます。 (既に認証済の組織名／ドメイン名の場合、自動完了する場合があります) 証明書発行までしばらくお待ちください。

■更新申請画面

【ゲストアクセスリンク】

ゲストユーザー

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

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

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

次ページ以降で詳細な入力方法をガイドします。

Section 1：申請者情報の入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

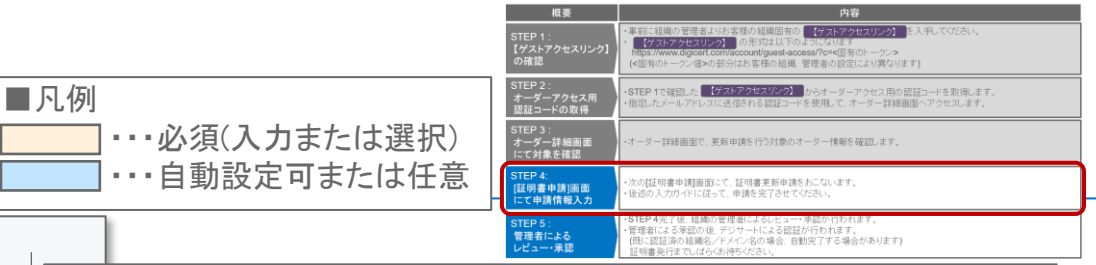
概要	内容
STEP 1：【ゲストアクセスリンク】の確認	・事前に組織の管理者よりお客様の組織固有の【ゲストアクセスリンク】を入手してください。 ・【ゲストアクセスリンク】の形式は以下のようになります。 https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分はお客様の組織・管理者の設定により異なります)
STEP 2：オーダーアクセス用認証コードの取得	・STEP 1で確認した【ゲストアクセスリンク】からオーダーアクセス用の認証コードを取得します。 ・指定したメールアドレスに送信される認証コードを使用して、オーダー詳細画面へアクセスします。
STEP 3：オーダー詳細画面にて対象を確認	・オーダー詳細画面で、更新申請を行う対象のオーダー情報を確認します。
STEP 4：[証明書申請]画面にて申請情報入力	・次の[証明書申請]画面にて、証明書更新申請をおこないます。 ・後述の入力ガイドに従って、申請を完了させてください。
STEP 5：管理者によるレビュー・承認	・STEP 4完了後、組織の管理者によるレビュー・承認が行われます。 ・管理者による承認の後、デジサートによる認証が行われます。 (既に認証済の組織名/ドメイン名の場合、自動完了する場合があります) ・証明書発行までしばらくお待ちください。

■更新申請画面

■【必須】申請者情報
名：申請者氏名の「名」を入力ください。
氏：申請者氏名の「氏」を入力ください。
メールアドレス：申請者のメールアドレスを入力ください。

Section 2：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



■更新申請画面

■【必須】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」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。

注：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

■【必須・自動設定あり】コモンネーム / SANs
・初期状態では更新元証明書と同一のFQDNが設定された状態
・任意の値に上書き可能です。一度当欄を空白にクリアしてから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)が自動設定されます。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】期間：
・ご申請いただくプラン(証明書を繰り返しご取得、継続してご利用いただけるご契約期間)を選択ください
・プラン選択後、プランの初回にご取得いただく証明書の有効期間を選択・指定いただけます(最大397日間)
→詳細は前セクションの[補足 プランの選択]をご参照ください

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

Section 3 : その他のオーダー情報の入力

■凡例
・・・必須(入力または選択)
・・・自動設定可または任意

■更新申請画面

■【任意】その他の証明書オプション
クリックして追加入力フィールドを表示すると以下の設定が可能です。
・中間チェーン:証明書チェーン(中間証明書とルート証明書の組合せ)を選択します
※組織のアカウント設定によって表示されない場合があります
※製品種類によってご利用いただけるチェーンの種類は異なります(※1,2)
・署名ハッシュ:
お客様のサーバ証明書(End-Entity)に対する署名アルゴリズムを選択可能です(選択肢:SHA-256(標準), SHA-384, SHA-512)。
・サーバープラットフォーム:
お客様のサーバープラットフォーム環境を選択し、発行通知メールに添付される証明書ファイル形式を最適化いただけます
※ 発行通知メールの形式は組織の管理者によって指定されます
※ ファイル形式の詳細は「6. 発行された証明書の取得」を参照ください

■【任意】その他のオーダーオプション
クリックして追加入力フィールドを表示すると以下の設定が可能です。
・「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。

■【任意】「メール送信先の追加」:申請者に加えて、申請関連のメールや更新案内メールの送信先を追加することができます。
※ 初期状態では更新元証明書と同一の値が設定された状態

■【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。

以上で更新申請の入力は終わりです。
「送信する」を押下して申請を完了させてください。

※1 : 各製品ごとにご利用いただける中間証明書とルート証明書の組合せについて:https://knowledge.digicert.com/ja/jp/solution/SOT0006.html
※2 : 中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら:https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

【ゲストアクセス】による証明書更新申請について – よくあるご質問 -

Q (ご質問)	A (回答)
・ゲストアクセスリンクによる検索時にエラーが発生します。 ・ゲストアクセスリンクによる検索がうまくヒットしません。 ・認証コードが取得できません。	・組織の管理者によって、ゲストアクセスが一時的に無効化されていたり、有効ではあるがゲストアクセス可能な証明書オーダーが限定されている場合があります。 ・お客様の証明書オーダーに対して「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による検索時に「対象が存在しない」旨のエラーが発生します。必要に応じて組織の管理者にご確認ください。
・電子メールで取得した認証コードを入力したらエラーが発生します。	・認証コードを正確にコピーして入力してください。 (前後にスペースなど不要な文字が付いていないかご確認ください)
・証明書の更新申請時にコモンネーム/SANsを変更することができるのですか？	・ゲストアクセスによる更新申請時にコモンネーム/SANsを変更いただくことは可能ですが、組織のポリシーによって、ゲストアクセスによる証明書申請時に新しいドメイン名の利用が許可されていない場合があります。 ・証明書申請に利用可能なドメイン名や、追加の可否については、必要に応じて組織の管理者にご確認ください。
申請画面の最下部に、このガイドには書かれていない、または名称の異なる追加のフィールドがあります。これは何ですか？	組織の管理者によって申請時の入力項目として**カスタムオーダーフィールド**（お客様組織独自の追加入力・管理項目）が設定されている場合があります。追加項目の詳細は管理者にご確認ください。

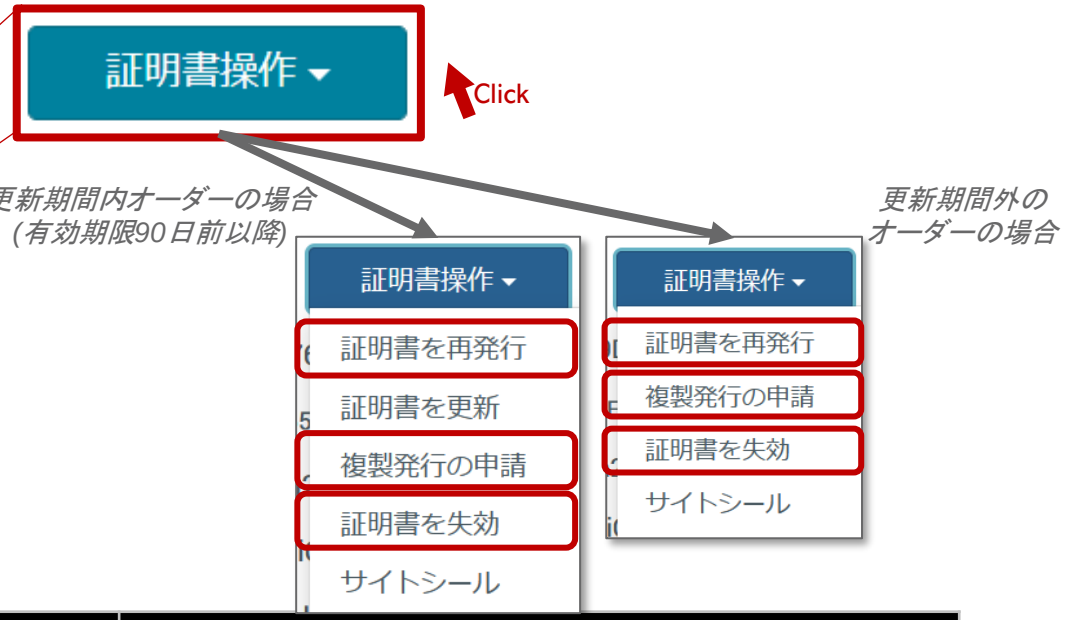
5. ゲストアクセスによる証明書再発行、複製および失効

オーダー詳細画面から証明書再発行、複製および失効を申請する流れ

ゲストユーザー

■オーダー詳細画面

■証明書操作



メニュー	説明
証明書を再発行	証明書再発行申請画面へ移動 →*当セクションの内容。次ページ参照ください。*
証明書を更新	(有効期限の90日前以降の場合のみ)更新申請画面へ移動 →*セクション4を参照*
複製発行の申請	証明書の複製発行申請画面へ移動 →*当セクションの内容。次ページ参照ください。*
証明書を失効	証明書失効申請画面へ移動 →*当セクションの内容。次ページ参照ください。*
サイトシール	「サイトシール」ページへ移動 →*セクション7を参照*

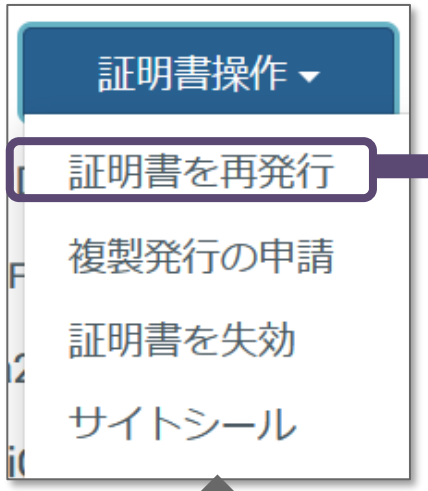
再発行、複製、失効等の証明書管理 概要

■当セクションの範囲

証明書の再発行	・証明書再発行(Reissue)を申請します ・【複数年プラン】選択時：証明書有効期間を延長(最大397日間)します ・ドメイン名の事前認証履歴が期限切れの場合、ドメイン利用権確認(DCV)が必要です ・コモンネーム／SANsを変更/削除した場合、元証明書は 48-72時間以内に失効されます。ご注意ください。
証明書の複製	【サーバ証明書(OV/EV)のみ】 ・証明書複製(Duplicate)を申請します
証明書の失効	・証明書失効(Revoke)の申請 ※ 失効申請が完了しても、証明書失効処理は完了しません →完了させるためには管理者による失効申請リクエストの「承認」が必要 ・失効リクエストの「承認」処理

ゲストアクセスによる証明書再発行申請

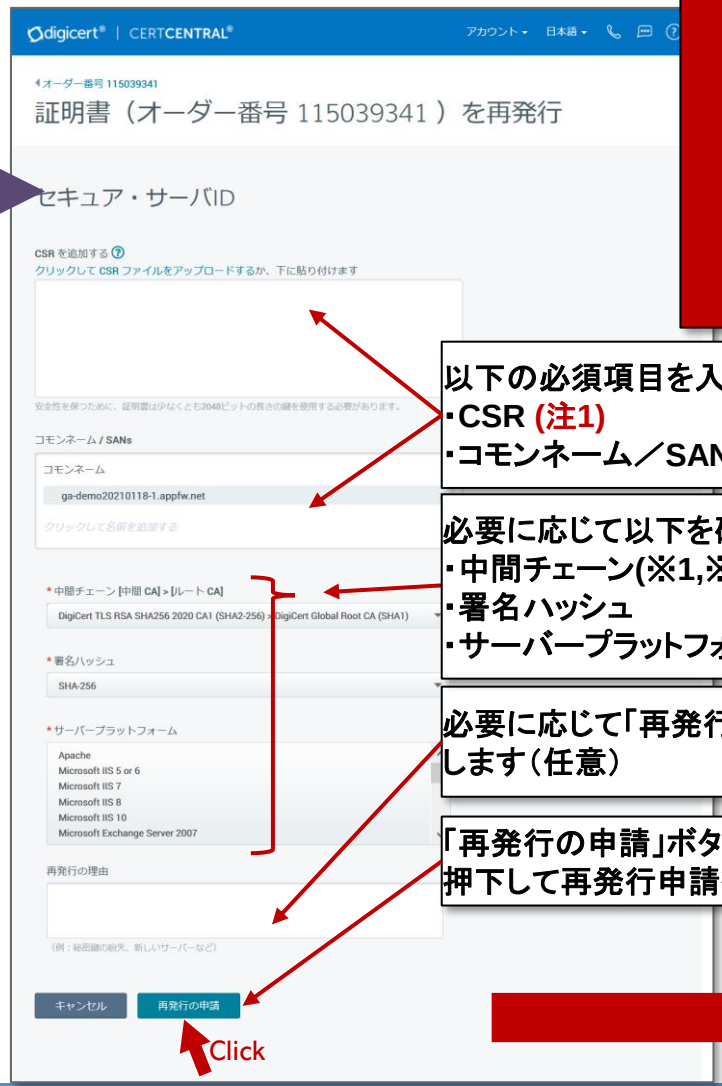
■「証明書操作」メニュー



【ゲストアクセスリンク】

ゲストユーザー

■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、再発行元の証明書に含まれていたコモンネーム／SANsを変更したり一部を削除した場合、再発行完了後から48~72時間以内に元の証明書が**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、再発行元の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)

必要に応じて以下を確認・変更します
・中間チェーン(※1,※2)
・署名ハッシュ
・サーバープラットフォーム

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」ボタンを押下して再発行申請を完了します

■再発行(Reissue)申請内容確認画面

最後に再発行申請内容確認(Confirm Certificate Changes)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「Confirm Request」を押下して申請を確定させてください。

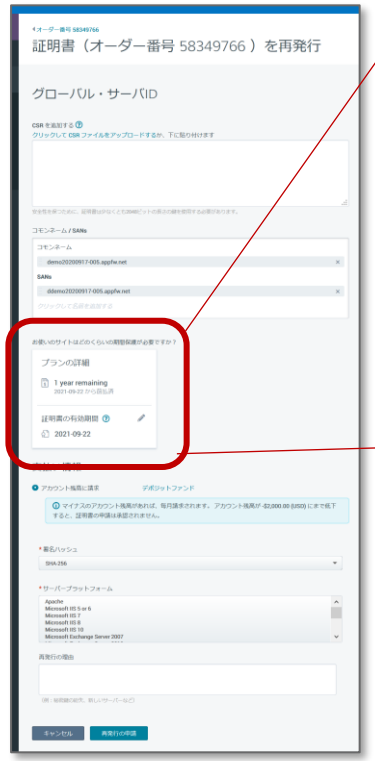
現在(再発行前)のコモンネーム/SANs

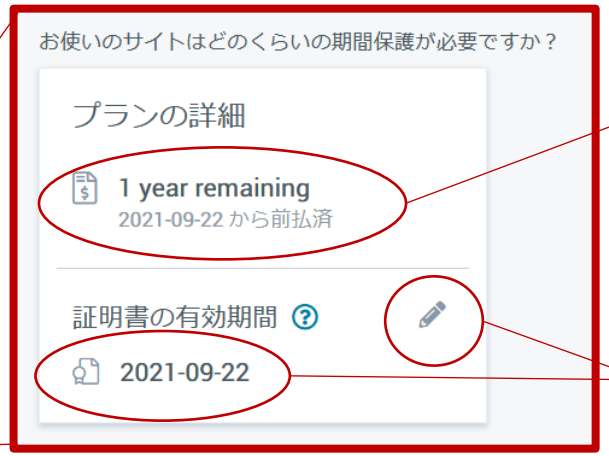
今回申請したコモンネーム/SANs

※1：中間チェーン欄は組織のアカウント設定によって表示されない場合があります。各製品ごとにご利用いただける中間証明書とルート証明書の組合せについて：https://knowledge.digicert.com/ja/jp/solution/SOT0006.html
※2：中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら：https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

補足 再発行(Reissue)申請時の「証明書有効期間」について

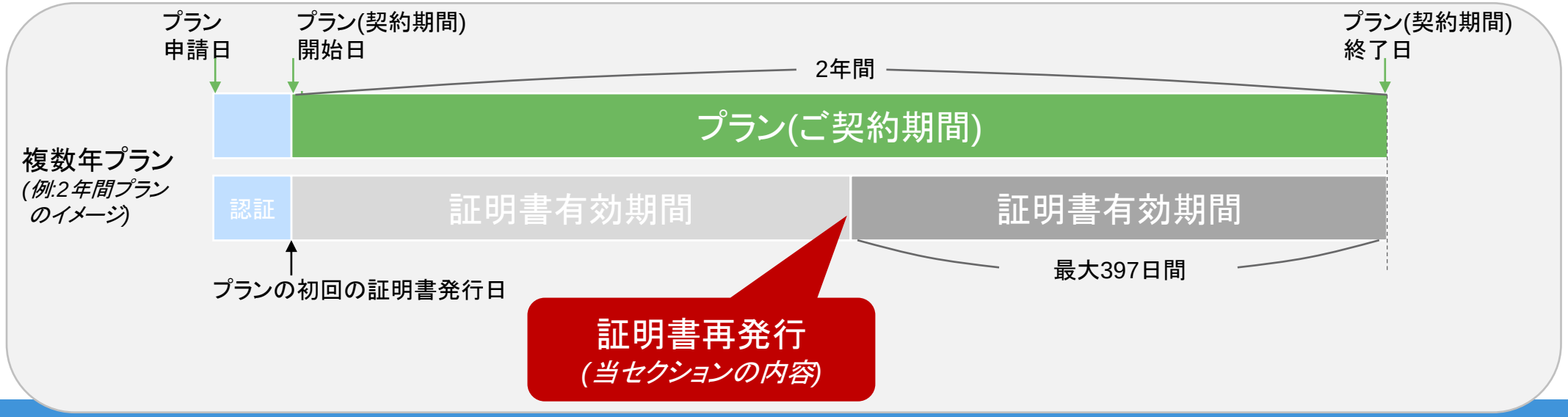
■再発行(Reissue)申請画面





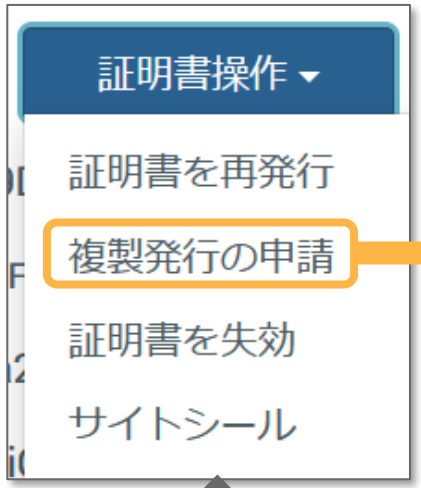
・上段はプラン(ご契約期間)の凡その残り期間を表示します。
・下段は「プラン(契約期間)終了日」を指します。

・【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



ゲストアクセスによる証明書複製申請

■「証明書操作」メニュー



【ゲストアクセスリンク】

ゲストユーザー

■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

対象のオーダーのコモンネームを確認ください

必要に応じて以下を確認・変更します
・中間チェーン(※1,※2)
・署名ハッシュ
・サーバープラットフォーム

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。

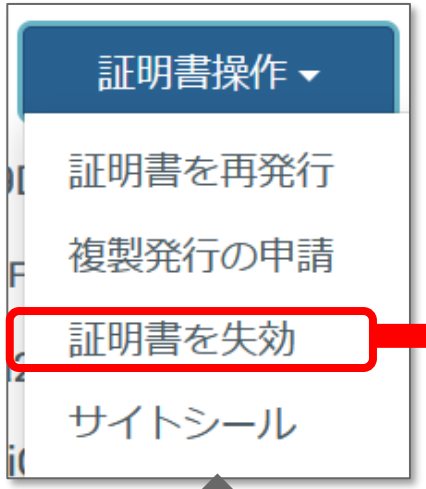
※1：中間チェーン欄は組織のアカウント設定によって表示されない場合があります。各製品ごとにご利用いただける中間証明書とルート証明書の組合せについて：https://knowledge.digicert.com/ja/jp/solution/SOT0006.html
※2：中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら：https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

（補足）証明書の「再発行」と「複製」の違い

	再発行(Reissue)	複製(Duplicate)
対象製品	・サーバ証明書(OV/EV) ・サーバ証明書(プライベートSSL) ・コードサイニング証明書/EVコードサイニング証明書	・サーバ証明書(OV/EV)のみ
主な用途	・証明書の更新(有効期間延長) ・コモンネーム/SANsの追加/変更/削除 ・鍵/署名アルゴリズムの変更	鍵/署名アルゴリズムの変更
コモンネーム／SANsの変更	可能（注：下記「費用」を参照）	不可
証明書有効期間終了日の変更	可能（注：指定可能な証明書有効期間終了日の制限について 別紙「再発行(Reissue)申請時の証明書有効期間について」参照	不可
費用	FQDN(SANs)を追加した場合、以下の式でユニットを消費 **消費ユニット数 ＝ 残プラン年数 x 追加したSANsの数量** （お客様のご契約内容によって実際の費用については異なる場合があります）	・なし
元証明書が失効されるか?	コモンネーム／SANsを変更/削除した場合、 元証明書は48-72時間以内に失効される	・失効されない

ゲストアクセスから証明書失効を申請する手順

■「証明書操作」メニュー



【ゲストアクセスリンク】

ゲストユーザー

■失効(Revoke)申請画面

「失効の理由」欄に**失効申請の理由**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時にレビューされ、またCertCentralに記録されます。

「失効申請」ボタンを押下して失効申請を確定ください。

※ 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。必要に応じて管理者に別途ご連絡ください。

6. 証明書の取得

~6.1 発行通知メールから証明書を取得~

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。
・組織の管理者の設定によって、メール本文のフォーマットならびに証明書ファイルの形式が異なります。

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>		
管理者によるアカウント設定(イメージ)	■「添付ファイル」方式 	■「プレーンテキスト」方式 	■「ダウンロードリンク」方式 
本文イメージ(日本語選択時、抜粋)	[アカウント代表組織名] [申請者(User Placing Order)氏名] 様 [ドメイン名]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 本メールに新しい証明書を添付しています。	[アカウント代表組織名] [申請者(User Placing Order)メールアドレス] 様 [コモンネーム]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 証明書: [End-Entity証明書データ(BASE64形式)] 中間CA証明書: [中間CA証明書データ(BASE64形式)]	[アカウント代表組織名] [申請者(User Placing Order)メールアドレス] 様 [ドメイン名]の証明書申請が承認されました。 証明書のオーダー番号は[オーダー番号]です。 証明書は以下のURLからダウンロードいただけます。 [証明書ダウンロードURL]

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

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

「添付ファイル」形式：[サーバーソフトウェア]別 証明書ファイル形式

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

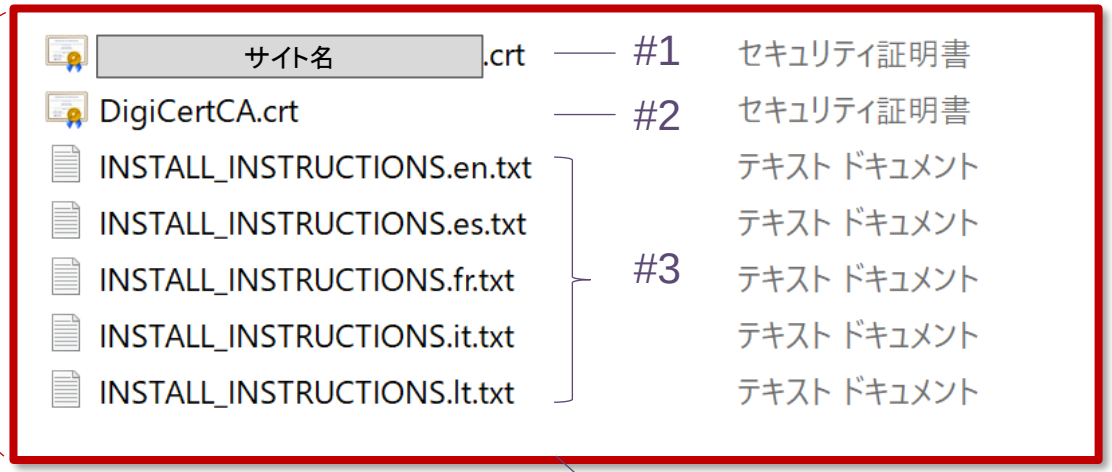
No	サーバーソフトウェア (※1)	ファイル形式ID (※2)	ファイル形式/拡張子	ファイルに含まれる内容
1	Apache(デフォルト)、Citrix Access Gateway 5.x and higher、cPanel、F5 Big-IP、他	apache (デフォルト)	ZIP圧縮ファイル/.zip	-エンドエンティティ証明書(.crt) -中間証明書(.crt)
2	Barracuda、Cisco、Citrix Access Essentials、Juniper、“OTHER”、他	default	ZIP圧縮ファイル/.zip	-エンドエンティティ証明書(.crt) -中間証明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

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

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

■発行通知メール(イメージ)

■ZIPファイルを展開した状態(イメージ)



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

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

「ダウンロードリンク」形式：証明書ダウンロードページ

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

■発行通知メール(イメージ)

サイト名 証明書発行のお知らせ

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

[アカウント代表組織名]

[申請者(User Placing Order)メールアドレス] 様

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

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

Click

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

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

（参考）[ファイルの種類]別 証明書ファイル形式

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

当ページの内容は以下のKnowledgeページの要約となります。
・ファイル形式について：https://dev.digicert.com/glossary/#certificate-formats (※1:ファイル形式IDの一覧はこちらを参照ください)

6. 証明書の取得

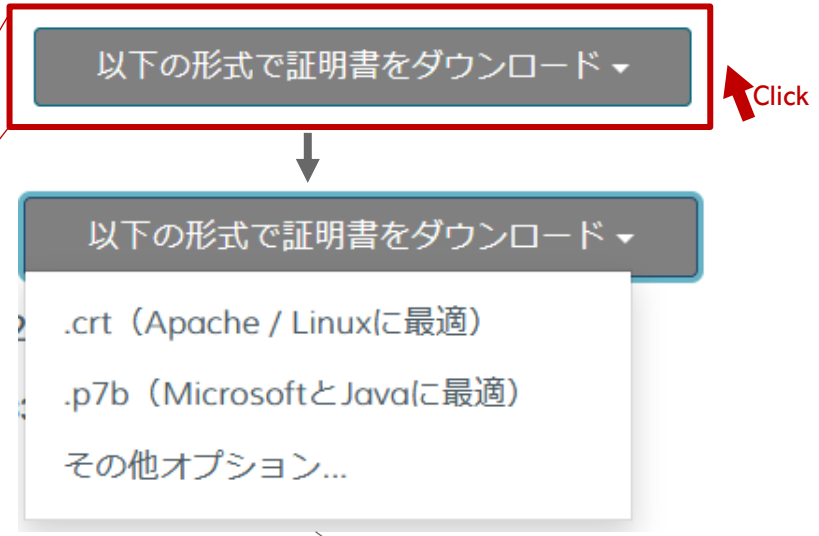
~6.2 ゲストアクセスから証明書をダウンロード~

オーダー詳細画面と証明書のダウンロード

■オーダー詳細画面

ゲストユーザー

■証明書をダウンロード



オーダー詳細画面で対象のオーダー情報を確認し、正しければ「証明書をダウンロード」を押下して証明書にアクセスします

メニュー	ファイル形式/拡張子	ファイルに含まれる内容
.crt (Apache / Linuxに最適)	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)
.p7b (MicrosoftとJavaに最適)	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
その他オプション…	<次ページ参照>	

「その他オプション」選択時の証明書ファイル形式の選択方法

■「その他オプション」を選択

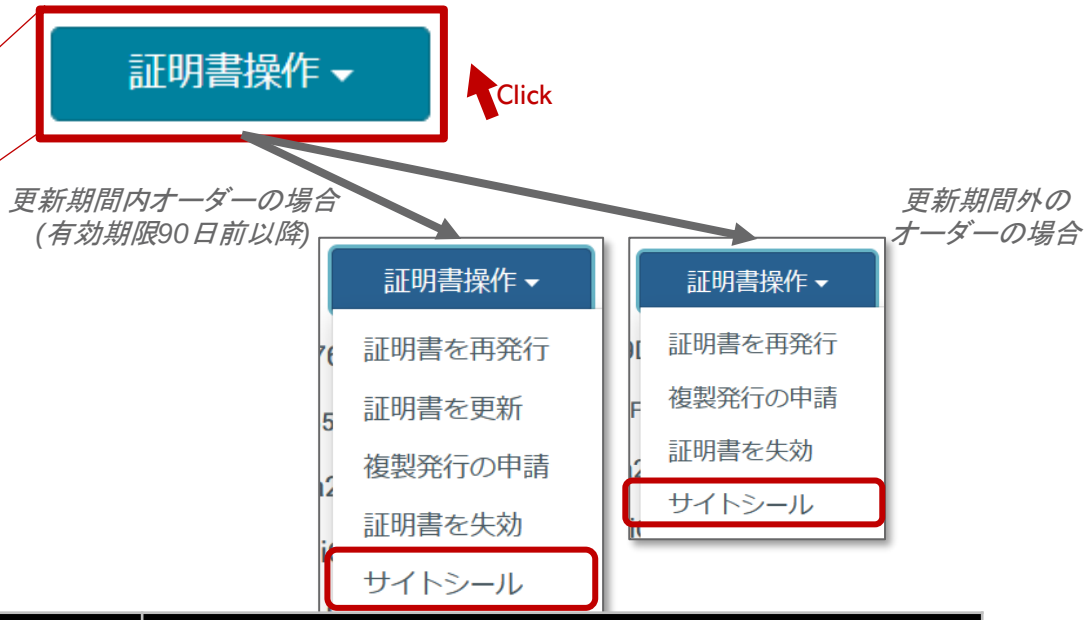
7. ゲストアクセスによるサイトシールの取得

オーダー詳細画面からサイトシールを取得する流れ

ゲストユーザー

■オーダー詳細画面

■証明書操作



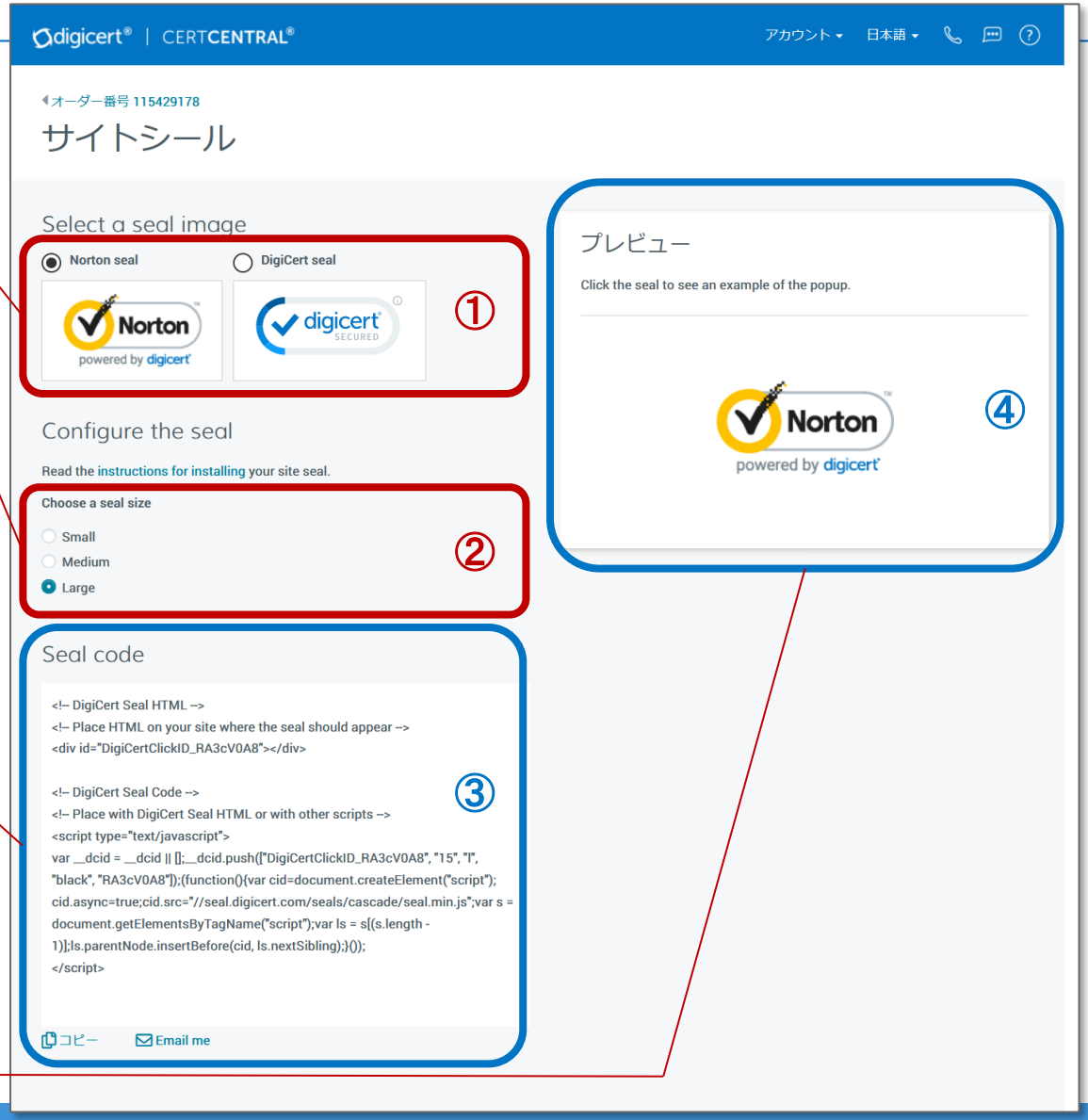
メニュー	説明
証明書を再発行	証明書再発行申請画面へ移動 →***セクション5を参照***
証明書を更新	(有効期限の90日前以降の場合のみ)更新申請画面へ移動 →***セクション4を参照***
複製発行の申請	証明書の複製発行申請画面へ移動 →***セクション5を参照***
証明書を失効	証明書失効申請画面へ移動 →***セクション5を参照***
サイトシール	「サイトシール」ページへ移動 →***当セクションの内容。次ページ参照ください。***

「サイトシール」ページ

■オーダー詳細画面の「サイトシール」メニュー

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

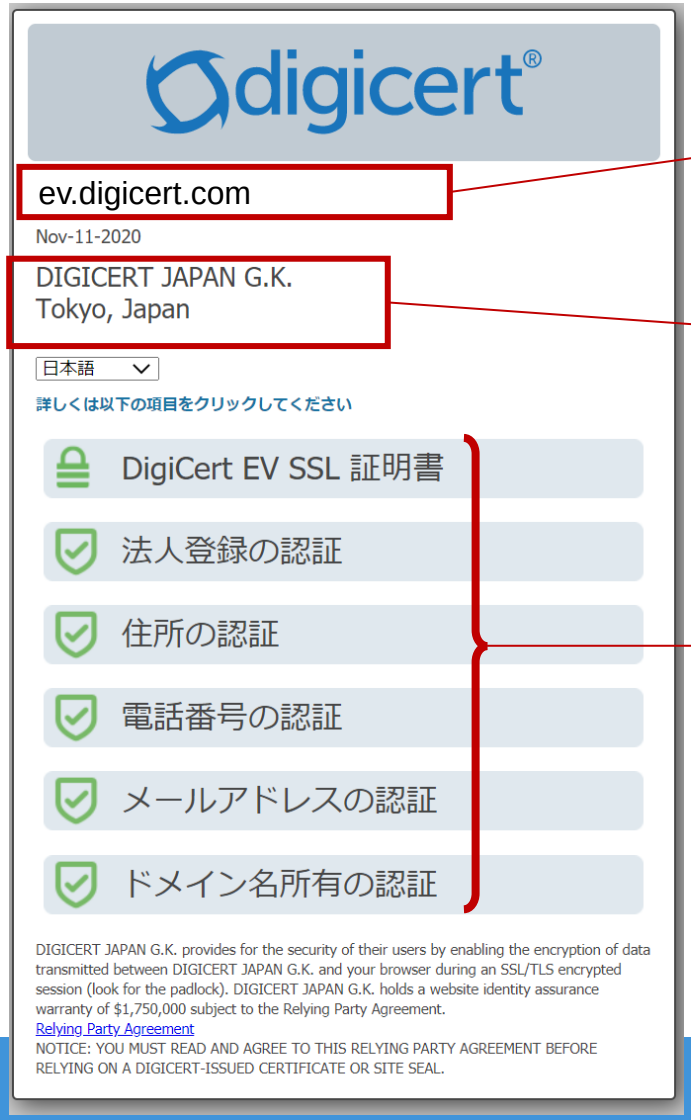
#	項目	内容
③	生成されたシールスクリプト	①、②の指定に基づいてシールスクリプト(HTML/JavaScriptコード)が生成されます。 生成したスクリプトをメールで送信することも可能です。 インストラクション(※1)に従ってお客様のウェブページに掲載してください。
④	生成されたイメージ	①、②の指定に基づいてシールイメージが生成されます。 またクリックいただくとサンプルのスプラッシュページをご確認いただけます。



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

スプラッシュページのデザイン（イメージ）

■(**EV証明書の場合**)サイトシール
スプラッシュページ(イメージ)



FQDN

組織情報

表明事項
(認証項目)
の説明

■(**OV証明書の場合**)サイトシール
スプラッシュページ(イメージ)

「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>
```

8. ゲストアクセスによる証明書製品のその他の機能の利用

~ 8.1 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/

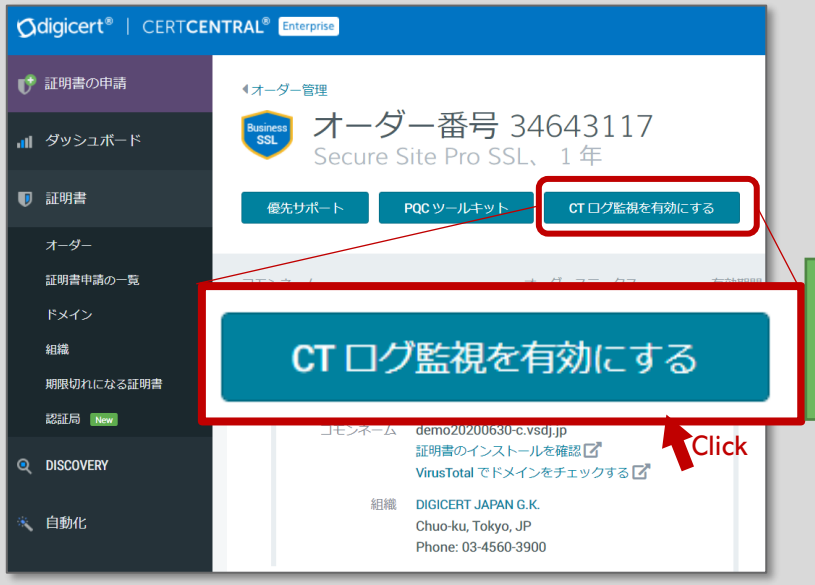
8. ゲストアクセスによる証明書製品のその他の機能の利用

~ 8.2 CTログモニタリング ~

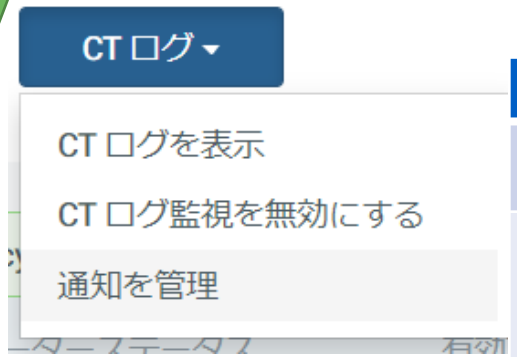
CTログモニタリング機能の有効化

■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/

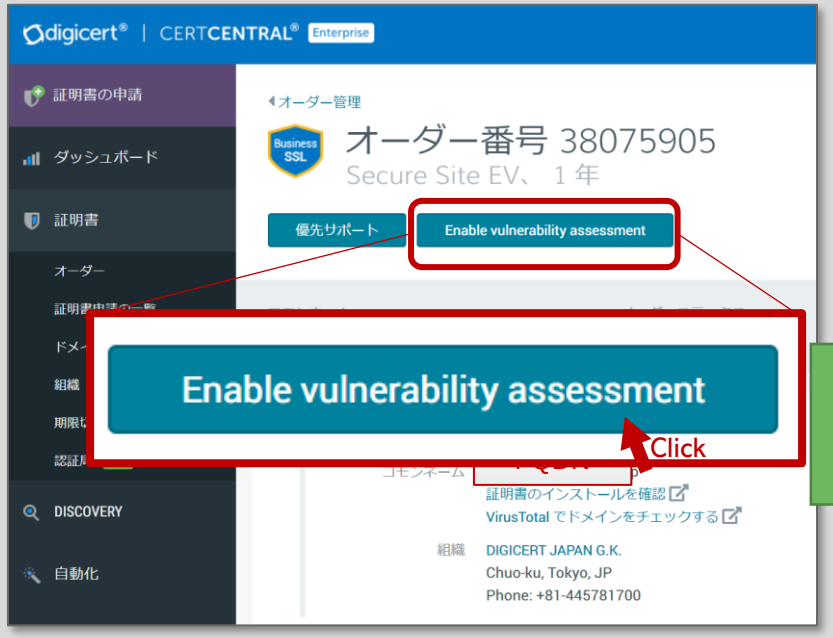
8. ゲストアクセスによる証明書製品のその他の機能の利用

~ 8.3 脆弱性アセスメント ~

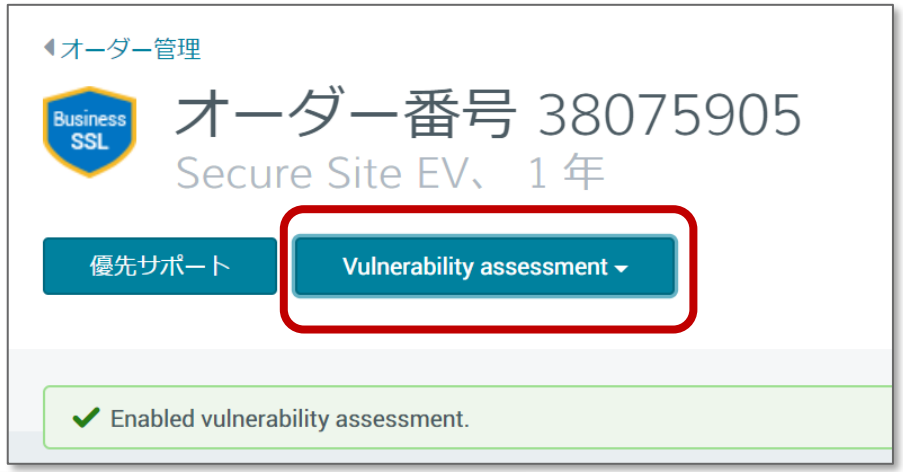
脆弱性アセスメント(Vulnerability Assessment)機能の有効化

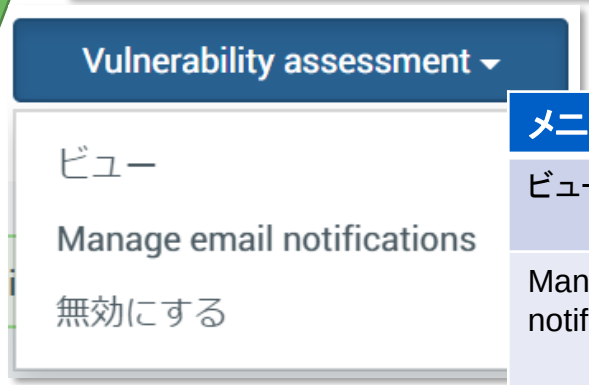
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

■初期状態
（脆弱性アセスメントが有効化されていない）



■脆弱性アセスメントが
有効化された状態





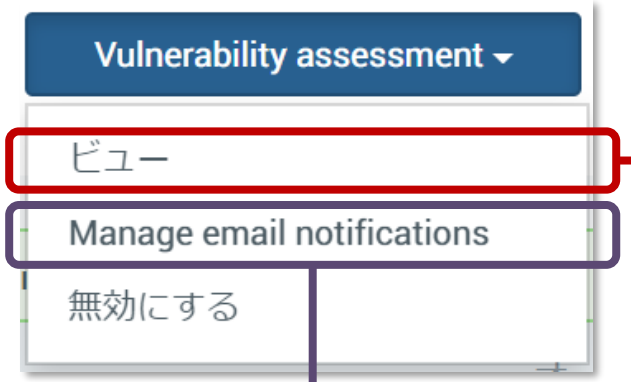
メニュー	説明
ビュー	脆弱性アセスメントの結果レポートを確認 →詳細は次ページ
Manage email notification	脆弱性アセスメントが脆弱性やその可能性を発見した際の通知を管理 →詳細は次ページ
無効にする	脆弱性アセスメント機能を無効化します

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

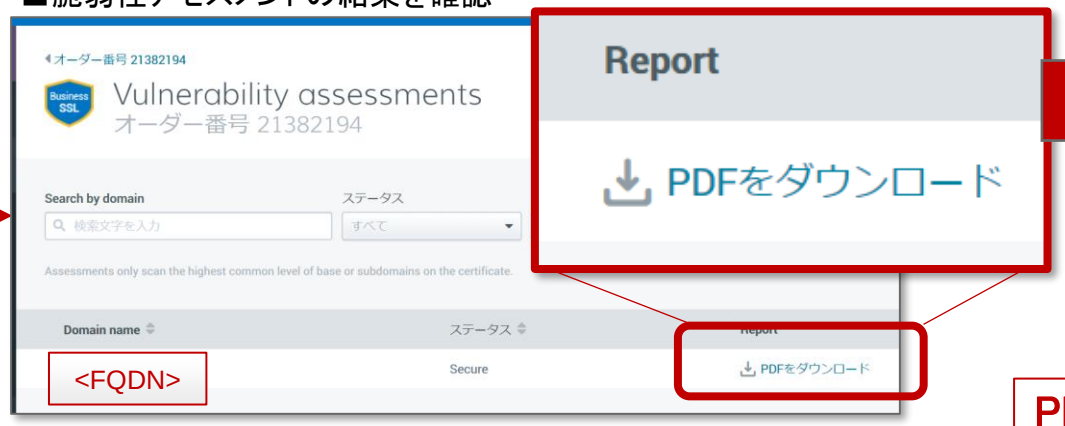
脆弱性アセスメント(Vulnerability Assessment)機能の管理

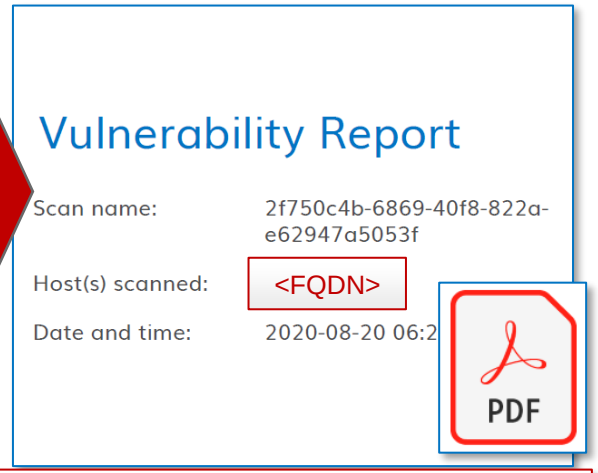
■対象製品
・セキュア・サーバID EV
・グローバル・サーバID
・グローバル・サーバID EV

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



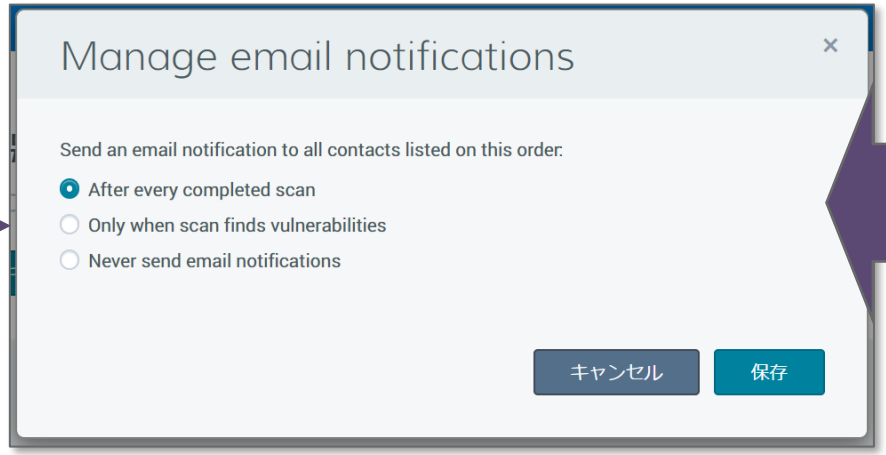
■脆弱性アセスメントの結果を確認





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

■脆弱性アセスメントが脆弱性やその可能性を発見した際の通知を管理



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

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