



【CertCentral Partner 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 : [page 3](#)
2. ゲストURLによる証明書新規申請 : [page 7](#)
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 : [page 21](#)
4. ゲストアクセスによる証明書更新申請 : [page 28](#)
5. ゲストアクセスによる証明書再発行、複製、失効 : [page 36](#)
6. 証明書の取得 : [page 44](#)
 - 6.1. 発行通知メールから証明書を取得 : [page 44](#)
 - 6.2. ゲストアクセスから証明書をダウンロード : [page 50](#)
7. ゲストアクセスによるサイトシールの取得 : [page 53](#)
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 : [page 58](#)
 - 8.1. マルウェアスキャン : [page 58](#)
 - 8.2. CTログモニタリング : [page 60](#)
 - 8.3. 脆弱性アセスメント : [page 62](#)

1. はじめに

はじめに

- 当資料は、[ゲストユーザー]様が、デジサートの販売代理店の管理者が生成・管理する[固有のURLリンク]を通じてCertCentralにアクセスし、デジサートの証明書を申請、ダウンロードまたはサイトシール掲載用スクリプトを取得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サーバ証明書を申請、ダウンロードしたりサイトシール掲載用スクリプトを取得いただくエンドユーザー様を、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URLリンク]は、販売代理店の管理者によって、以下の機能を用いて提供されます
 - 【ゲストURL(Guest URL)】：証明書新規申請用の固有のURLリンクを作成、管理する機能
 - 【ゲストアクセス(Guest Access)】：証明書のダウンロード、サイトシール掲載用スクリプトの取得用の固有のURLリンクを生成、管理する機能
- [固有のURLリンク]は販売代理店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。不明な場合は販売代理店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 |
|------|-----------|---|------|
| 1.0 | 2021/1/25 | 初版作成 | - |
| 1.1 | 2021/3/16 | 以下のセクションを追加 [2. ゲストURLによる証明書新規申請] [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] [4. ゲストアクセスによる証明書更新申請] [5. ゲストアクセスによる証明書再発行、複製、失効] [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] これに伴いセクション構成を改訂 | - |
| | | | |
| | | | |
| | | | |

(参考) 旧プラットフォームの「Invitation」機能、「End User Portal」機能との比較(イメージ)


旧プラットフォーム

■ (参考) 旧プラットフォームの「Invitation」「User Portal」ページ
URL形式: [https://products.websecurity.digicert.com/...](https://products.websecurity.digicert.com/) / [https://products.geotrust.com/...](https://products.geotrust.com/)

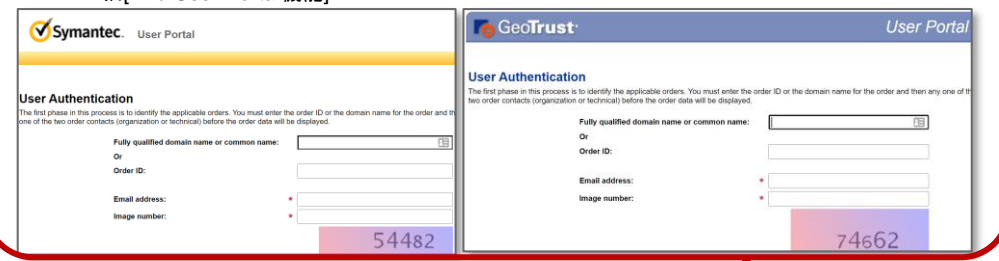
ゲストユーザー (エンドユーザー) → 証明書申請

証明書再発行 / 失効

旧[Quick Invite機能]



旧[End User Portal機能]



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


証明書更新申請 / 再発行 / 失効など

【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

【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「証明書の更新申請」を参照ください

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 | <ul style="list-style-type: none"> ・事前に販売代理店の管理者より固有の 【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>の部分は販売代理店の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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・STEP 3完了後、販売代理店の管理者によるレビュー・承認が行われます。 ・販売代理店の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URL】

グローバル・サーバID **New**

グローバル・サーバID EV **New**

今すぐ申請

369797 日本語

- English
- Deutsch
- Español
- Français
- Italiano
- 日本語

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)

グローバル・サーバID **New**

グローバル・サーバID EV **New**

複数の製品が表示されている場合は選択します。

今すぐ申請

証明書申請画面へ移動します

| 概要 | 内容 |
|---------------------------|---|
| STEP 1: 【ゲストURL】の確認 | <ul style="list-style-type: none"> 事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 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販売代理店の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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> STEP 3完了後、販売代理店の管理者によるレビュー承認が行われます。 販売代理店の管理者による承認の後、デジタルによる認証が行われます。 (既に該証明書の発行者がドメイン名の場合、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)

| 概要 | 内容 |
|----------------------------------|--|
| STEP 1: 【ゲストURL】の確認 | ・事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 ・URLの形式は以下のようになります(「固有のトークン」は販売代理店の管理者の設定により異なります) https://www.digicert.com/secure/requests/products?quest_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、販売代理店の管理者によるレビュー/承認が行われます。 ・販売代理店の管理者による承認の後、デジタルによる認証が行われます。 ・既に該証明書の種別名・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。 |

■証明書申請画面(※1)



申請者情報

証明書情報

組織・担当者情報

その他の
オーダー情報

Section 1 : 以下のような「申請者情報」を入力します。

- ・申請者氏名
- ・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

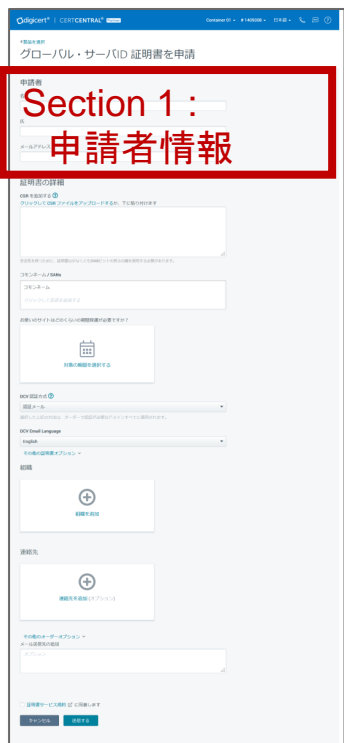
次ページ以降で詳細な入力方法をガイドします。

※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、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、追加で入力が必要となる項目があります。

Section 1 : 申請者情報の入力

■ 証明書申請画面



申請者

名

Taro

氏

Shinsei

メールアドレス

taro.shinsei@digicert.com

■ 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URL】の確認 | <ul style="list-style-type: none"> ・事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 ・URLの形式は以下ようになります(固有のトークン値の部分は販売代理店の管理者により異なります) 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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・STEP 3完了後、販売代理店の管理者によるレビュー承認が行われます。 ・販売代理店の管理者による承認の後、アシサートによる認証が行われます。 ・既に該証明書の種別名・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。 |

■【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。

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)

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 **Click**

1 year

2 years

3 years

4 years

5 years

6 years

Custom order validity

2 year plan

お使いのプランのタイムライン

2020 今日

- 2年の証明書に支払いをする
- 1年の証明書を受け取る

① 業界の規定により、証明書の有効期間は最大で1年間となります。

2021 本日より1年

- ドメインを再認証して、次の証明書をインストールする
- お使いのドメインまたは証明書の有効期間を2年間随時変更する

2022 対象終了

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。

証明書の有効期間 397 days

証明書の有効期間 ② キャンセル

1年

有効期限の指定

カスタム長

397 日数

保存 **Click**

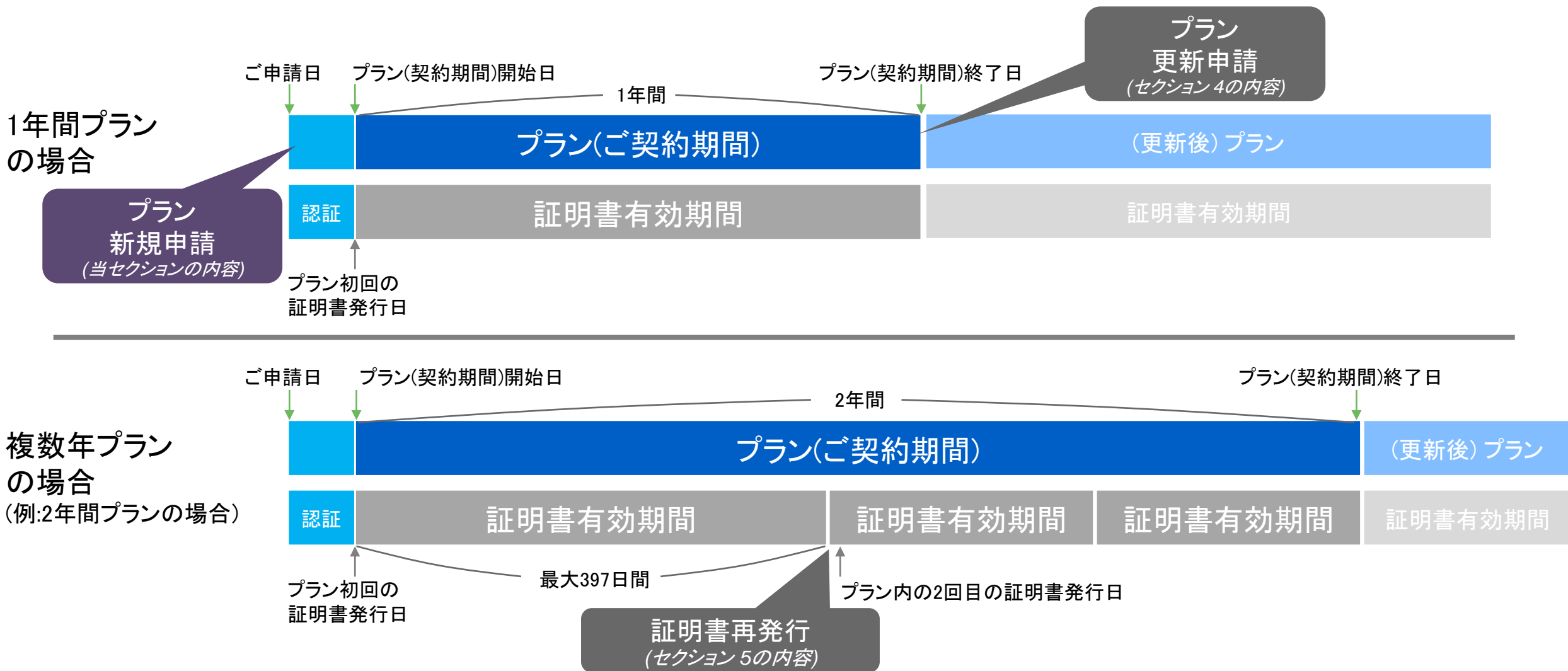
最大6年間まで選択可能

・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

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

補足「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)

■ 証明書申請画面



DCV 認証方式 ?

認証メール

選択した上記の方法は、オーダーで認証が必要なドメインすべてに適用されます。

DCV Email Language

Japanese

その他の証明書オプション ▼

Click

その他の証明書オプション ▼

署名ハッシュ

SHA-256

サーバープラットフォーム

Apache

■ 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URL】の確認 | ・事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 ・URLの形式は以下のようになります(値のトークン値の部分は販売代理店の管理者の指定により異なります) <a href="https://www.digicert.com/secure/requests/products?guest_key=<固有のトークン値>">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: 【発行】画面へアクセス | ・STEP 3完了後、販売代理店の管理者によるレビュー承認が行われます。 ・販売代理店の管理者による承認の後、デジタルによる認証が行われます。 |

■【必須・自動設定あり】ドメイン名利用権確認(DCV)

- ・<既に代理店アカウント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>

■【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。

- ・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販売代理店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)

■証明書申請画面

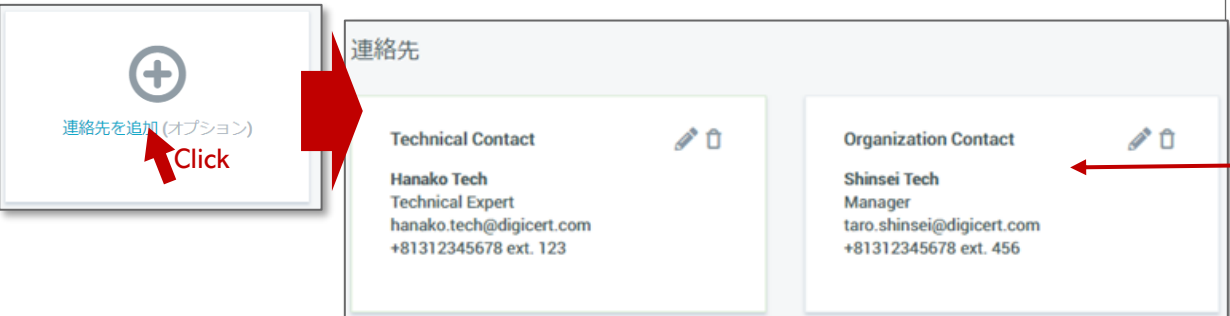


**Section 3 :
組織・担当者
情報**

■組織情報入力欄



■担当者情報入力欄



■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URL】の確認 | <ul style="list-style-type: none"> 事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 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販売代理店の管理者の決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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> STEP 3完了後、販売代理店の管理者によるレビュー承認が行われます。 販売代理店の管理者による承認の後、デジタル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。 |

■【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。

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

| 概要 | 内容 |
|----------------------------|---|
| STEP 1 : 【ゲストURL】の確認 | ・事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 ・URLの形式は以下のようになります(「<固有のトークン>」の部分は販売代理店の管理者の決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、販売代理店の管理者によるレビュー承認が行われます。 ・販売代理店の管理者による承認の後、デジタル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。 |

■証明書申請画面



■組織情報入力欄



組織

組織情報

DIGICERT JAPAN G.K.
EV Validated

6-10-1, Ginza
Chuo-ku, TOKYO, JP, 104-0061

03-4560-3900

■担当者情報入力欄



連絡先

Verified Contact

Jiro EV
IT Director
0312345678 ext. 122
jiro.ev@digicert.com

別の認証済連絡先を追加 (オプション)

Technical Contact

Hanako Tech
Technical Expert
0312345678 ext. 124
hanako.tech@digicert.com

Organization Contact

Taro Shinsei
Manager
0312345678 ext. 123
taro.shinsei@digicert.com

■【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。

OV/EV証明書 新規申請 Section 3 : 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

組織を追加

既存の組織
 新しい組織

① 新しい組織は、証明書を発行が可能になる前に、**認証**される必要があります。

正式名称

一般名称

国

住所1

住所2

市町村名

State

Zip Code

組織の電話番号

■ 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) | <ul style="list-style-type: none"> <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>

OV/EV証明書 新規申請 Section 3 : 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

連絡先を追加

連絡先タイプ
申請責任者

① 申請責任者は、当社から連絡し 組織を認証し、証明書要求を確認します。

既存の連絡先
 新しい連絡先

名
氏

部署名および役職名

メール

電話
内線
オプション

キャンセル 追加

■ 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) | <ul style="list-style-type: none"> 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) | <ul style="list-style-type: none"> 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) | <ul style="list-style-type: none"> 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 |

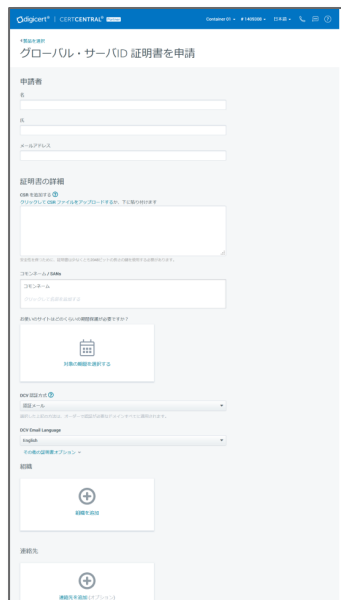
■ 担当者情報の入力項目の説明・入力/選択例

| 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。

Section 4 : その他のオーダー情報入力

■証明書申請画面



Section 4 :
その他の
オーダー情報

■その他のオーダーオプション 入力欄

その他のオーダーオプション ▼

Click

その他のオーダーオプション ▼

管理者への連絡事項

オプション

(証明書には含まれません)

オーダー特定の更新メッセージ

オプション

■メール送信先の追加 入力欄

メール送信先の追加

taro.shinsei@digicert.com

■規約同意、証明書の申請

証明書サービス規約 に同意します

Click

キャンセル

送信する

Click

■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URL】の確認 | ・事前に販売代理店の管理者より固有の【ゲストURL】を入力してください。 ・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販売代理店の管理者の決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、販売代理店の管理者によるレビュー承認が行われます。 ・販売代理店の管理者による承認の後、デジカ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。 |

■【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。

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。

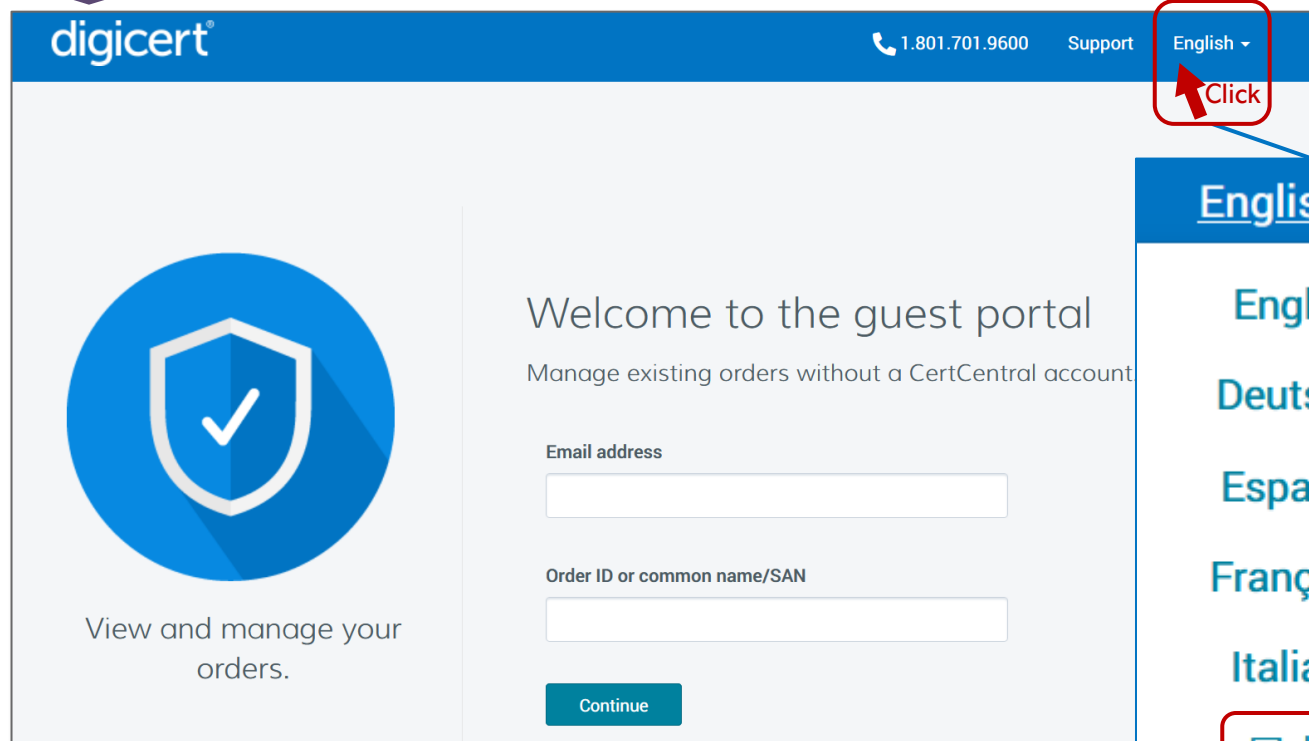
| 概要 | 内容 |
|-----------------------------------|--|
| STEP 1 : 【ゲストアクセスリンク】 の確認 | <ul style="list-style-type: none"> ・事前に販売代理店よりお客様の組織固有の【ゲストアクセスリンク】を入手してください。 ・【ゲストアクセスリンク】の形式は以下のようになります <a href="https://www.digicert.com/account/guest-access/?c=<固有のトークン>">https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分は販売代理店の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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・STEP 4完了後、販売代理店の管理者によるレビュー・承認が行われます。 ・販売代理店の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

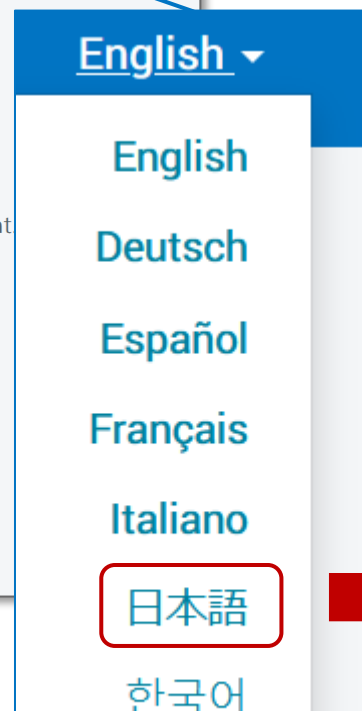
はじめに ~ゲストアクセス機能を「日本語」でご利用いただくために~

【ゲストアクセスリンク】



The screenshot shows the English version of the digicert guest portal. The header includes the digicert logo, a phone number (1.801.701.9600), a 'Support' link, and a language dropdown menu currently set to 'English'. A red box highlights the 'English' dropdown with a red arrow and the word 'Click'. The main content area features a shield icon with a checkmark and the text 'View and manage your orders.' To the right, there is a 'Welcome to the guest portal' message and instructions to 'Manage existing orders without a CertCentral account'. Below this are two input fields: 'Email address' and 'Order ID or common name/SAN', followed by a 'Continue' button.

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。



A vertical dropdown menu for language selection. The options listed are: English, Deutsch, Español, Français, Italiano, 日本語 (highlighted with a red box), and 한국어.



The screenshot shows the Japanese version of the digicert guest portal. The header includes the digicert logo, a phone number (1.801.701.9600), a 'Support' link, and a language dropdown menu currently set to '日本語'. The main content area features a shield icon with a checkmark and the text 'View and manage your orders.' To the right, there is a 'ゲストポータルへようこそ' message and instructions to 'このポータルからCertCentralのオーダーを管理することができます'. Below this are two input fields: 'メールアドレス' and 'オーダーID、またはコモンネーム/SAN', followed by a '続行する' button.

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)

| 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。 (固有のトークン値の部分はお客様の組織、管理者の指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。 確認の入力内容に基いて、申請を完了させてください。 |
| STEP 5: 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、ゲストポータル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は、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。 |

【ゲストアクセスリンク】



ゲストユーザー



オーダー内容の確認と管理

ゲストポータルへようこそ

このポータルからCertCentralのオーダーを管理することができます

メールアドレス

オーダーID、またはコモンネーム/SAN

続行する Click

CertCentralのアカウントをお持ちの方はこちら [サインイン](#)

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

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

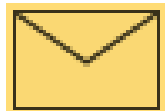
・次の画面へ遷移します
・同時に、[メールアドレス]欄に入力したメールアドレスに「認証コード」が送信されます。



⚠ Cannot access guest portal.

ゲストポータル – 認証コードの生成 (2/2)

| 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/guestportal-access/your-unique-link (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。 確認の入力内容によって、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、ゲストポータルによる認証が行われます。 (既に認証済の組織名/ドメイン名の場合は、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。



オーダー内容の確認と管理

次のEメールアドレスに送付された認証コードを入力してください:

<前ページで指定されたメールアドレス>

認証コード

↑Paste

サインイン

↑Click

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

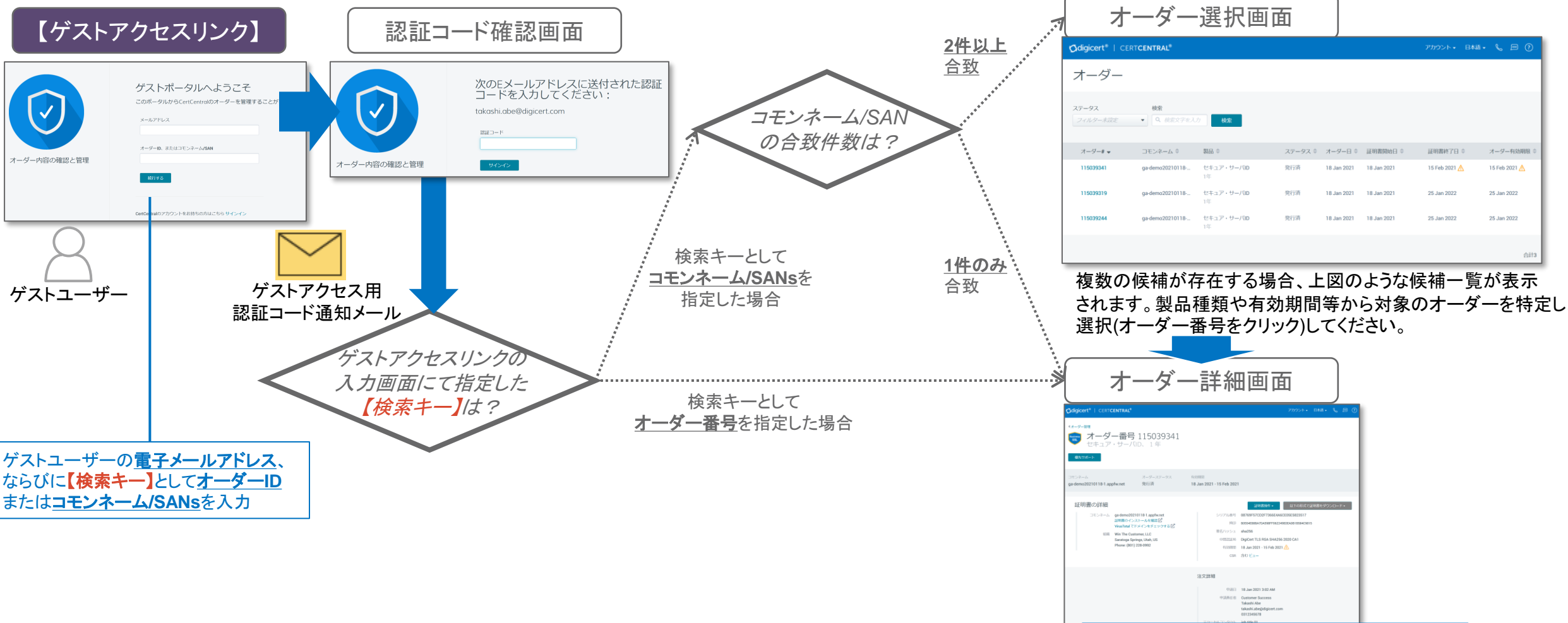
コードの検証が失敗した場合

⚠ Cannot access guest portal.

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。

| 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。 (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。 検索の入力サイズによって、申請を変更できません。 |
| 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、デジタルによる承認が行われます。 (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

次ページを参照ください

オーダー詳細画面

| 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。 (※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。 ・確認の入力内容に基いて、申請を完了させてください。 |
| STEP 5: 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、デジタルによる認証が行われます。 (既に認証済の組織名/ドメイン名の場合は、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。 |

■オーダー詳細画面



digicert | CERTCENTRAL

アカウント 日本語

オーダー管理

Business SSL オーダー番号 124208640
グローバル・サーバID, 1年

優先サポート PQC ツールキット CT ログ監視を有効にする 脆弱性アセスメントを有効にする

コモンネーム: <FQDN> オーダーステータス: 発行済 有効期間: 09 Mar 2021 - 16 Mar 2022

証明書の詳細

コモンネーム: ga-demo202103.vsd.jp
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: <組織情報>

シリアル番号: 0B26AED7B46EBD2B017234B61E69CBDB
拇印: C5ABEA8134843FC9C33D757FB2C61102E5D6B4F6
署名ハッシュ: sha256
中間認証局: DigiCert TLS RSA SHA256 2020 CA1
有効期間: 09 Mar 2021 - 16 Mar 2022
CSR: 含む ビュー

注文詳細

申請日: 09 Mar 2021 4:56 AM
複数年プランの詳細: 1年プラン (08 Mar 2021 - 16 Mar 2022)
自動更新: いいえ
Auto-reissue:
申請責任者: <申請責任者情報>
技術担当者: <技術担当者情報>
管理グループ: Win The Customer, LLC
オーダーステータス: 発行済
プラットフォーム: Apache

■ 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。

Click

証明書操作

- 証明書を再発行
- 証明書を更新
- 複製発行の申請
- 証明書を失効
- サイトシール

| 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 |

※ デジサートまたは販売代理店の指示に沿ってご利用ください(指示が無い場合は、これらのメニューのご利用をお控えください)

以下の形式で証明書をダウンロード

■ 「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 | <ul style="list-style-type: none"> ・事前に販売代理店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 <a href="https://www.digicert.com/account/guest-access/?c=<固有のトークン>">https://www.digicert.com/account/guest-access/?c=<固有のトークン> (<固有のトークン値>の部分は販売代理店の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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・STEP 4完了後、販売代理店の管理者によるレビュー・承認が行われます。 ・販売代理店の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

| 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がお客様の組織固有の【ゲストアクセスリンク】を入力してください。 ・【ゲストアクセスリンク】の形式は以下のとおりです。 https://www.digicert.com/account/guest-access/?pk=<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。 ・認証コードはメールまたは返信される認証コードを参照して、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、デフォルトによる認証が行われます。 ・(西に認証済の組織名/ドメイン名の場合、自動完了する場合があります) 証明書発行までお任せください。 |



ゲストユーザー

■オーダー詳細画面

digicert | CERTCENTRAL

アカウント | 日本語

オーダー管理

オーダー番号 124208640
グローバル・サーバID, 1年

優先サポート | PQC ツールキット | CT ログ監視を有効にする | 脆弱性アセスメントを有効にする

コモンネーム: <FQDN> | オーダースtatus: 発行済 | 有効期間: 09 Mar 2021 - 16 Mar 2022

証明書の詳細

コモンネーム: ga-demo202103.vsdj.jp
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

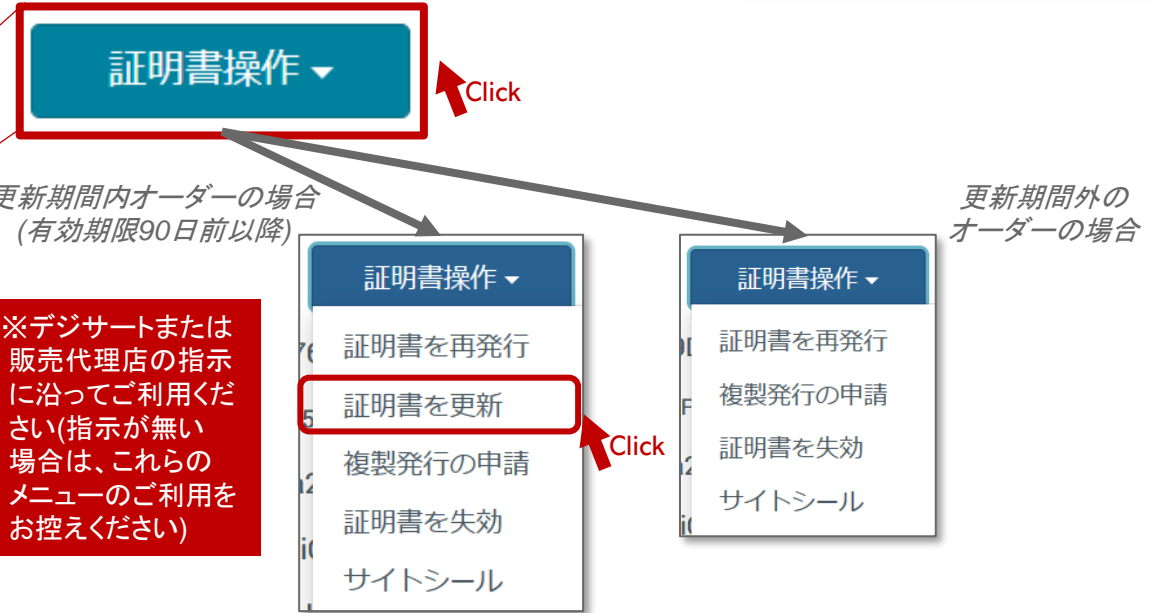
組織: <組織情報>

シリアル番号: 0B26AED7B46EBD2B017234B61E69CBDB
押印: C5ABEA8134843FC9C33D757FB2C61102E5D6B4F6
署名ハッシュ: sha256
中間認証局: DigiCert TLS RSA SHA256 2020 CA1
有効期間: 09 Mar 2021 - 16 Mar 2022
CSR: 含む ビュー

注文詳細

申請日: 09 Mar 2021 4:56 AM
複数年プランの詳細: 1年プラン (08 Mar 2021 - 16 Mar 2022)
自動更新: いいえ
Auto-reissue:
申請責任者: <申請責任者情報>
技術担当者: <技術担当者情報>
管理グループ: Win The Customer, LLC
オーダーステータス: 発行済
プラットフォーム: Apache

■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がIPアドレスの証明書固有の【ゲストアクセスリンク】を入力してください。 【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/?ip=<固有のトークン> (<固有のトークン>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られる認証コードを取得して、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、証明書更新申請をください。 ・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 | ・申請が完了後、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、デジタルサインが完了します。 ・(西暦証明書の組織名/ドメイン名の場合、自動完了する場合があります) ・証明書発行までにお待ちください。 |

更新申請画面

証明書操作 ▾

- 証明書を再発行
- 証明書を更新
- 複製発行の申請
- 証明書を失効
- サイトシール

【ゲストアクセスリンク】



アカウント 日本語

4オーダー#57267885を管理
セキュア・サーバID (オーダー番号 57267885) を更新

Section 1 : 申請者情報

申請者氏名
氏名
メールアドレス

Section 2 : 証明書情報

証明書の詳細
CSR
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
クリックして名前を追加する

共通ネーム / SANs
共通ネーム
demo20200915-api4.appfw.net
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

Section 3 : その他のオーダー情報

その他の証明書オプション
その他の証明書オプション
メール送付先の追加
takaishi@digicert.com

証明書サービス規約 に同意します

キャンセル 送信する

Section 1 : 以下のような「申請者情報」を入力します。

- 申請者氏名
- 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
- 証明書有効期間

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

■更新申請画面

■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が所属組織内の【ゲストアクセスリンク】を入力してください。 ・【ゲストアクセスリンク】の形式は以下のとおりです。 <https://www.digicert.com/account/guest-access/?p=<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。 ・取得したメールアドレスに送られる認証コードを取得し、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、証明書更新申請を行います。 ・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 | ・申請が完了後、組織の管理者によるレビュー画面が稼働します。 ・管理者による承認の後、デジタルによる認証が行われます。 (西に認証済の組織名/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。 |



申請者

名
Taro

氏
Shinsei

メールアドレス
taro.shinsei@digicert.com

■【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

■更新申請画面



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-----
MIICcwCCAsCARAwwFjELMkGA1UEBhMCSIAxIjAgBgNVBAMTGW1bW8yMDIwMTEt
dnBvdj1ShoHbmdy5uZkxhZjAgBgNVBAMTGFVud215bzE0MA4GA1UEBxQ0H2h1b1r
dCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMlcazw0S0s6/T1G2vqD4wszBw0
haT8+dwk9jD0wYXtjZwpbQVNF12mAR8o/z1enTCw0tWfaNca14fkacR06Jo8
zXS1Jkxwfj67IKD9CReouWU02ZBsF0D0C/n0B5JMIJYfMkZtoJo1sWgz0PPvtv
z8A4B0v9oH/18Mfmc78oVDSkzB516WYqgdXmbq+00kh6GXkh3+1qve51Xp18hm
AMH7Zxh+dmU326Ro/Az9F1VyyxP2m4q4jNYP37d090Tq6dGWEsxn0p6P4Aa5ueYq
RtL6P0eUL9v04ck1w90ap4a084oea01jvDyFEbML3NIMW/JkytZ/HNK31ukCAwEA
AaAAMQ0CSqGSIb3DQEBCwUAA41BA0BEXUs2/20d75oJHF1Thx19e02A0HEByf12
rrb6HXxcEP42WbnNKVpFFrYhZpCtgEb1HqDUcKRwivMeESM0eJ40Hg1pSMf0bhf
```

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

コモンネーム

<更新元証明書のコモンネーム>

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？

プランの詳細

1 year
2022 から支払済

証明書の有効期間 ?

1 year

■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が所属する組織固有の【ゲストアクセスリンク】を入力してください。 ・※有効期限は以下のとおりです。 https://www.digicert.com/account/invite-access/?p=<固有のトークン> (<固有のトークン>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。 ・取得したURLアドレスに記述される認証コードを使用し、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、証明書更新申請を承ります。 ・後述の入力欄に従って、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で完了後、組織の管理者によるレビュー承認が行われます。 ・管理側になる認証コード、デフォルトによる認証が行われます。 (西: 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) 証明書発行までにお待ちください。 |

■【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

Section 3 : その他のオーダー情報の入力

■更新申請画面

■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がお客様の組織固有の「[ゲストアクセスリンク]」を入力してください。 「[ゲストアクセスリンク]」は以下のURLです。 `https://www.digicert.com/account/agent-access/?m=<固有のトークン>` (固有のトークン>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。 ・取得したURLアドレスに記述される認証コードを使用し、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、証明書更新申請をいたします。 ・後述の入力項目に従って、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 | ・申請が完了した後、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、デフォルトによる認証が行われます。 ・(西: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。 |



その他の証明書オプション

署名ハッシュ
SHA-256

サーバープラットフォーム
Apache

その他のオーダーオプション

管理者への連絡事項
オプション
(証明書には含まれません)

オーダー特定の更新メッセージ
オプション

メール送信先の追加
<更新元証明書の追加メールアドレス>

証明書サービス規約 に同意します

キャンセル 送信する

■【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。

- ・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販売代理店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「5.1. 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

■【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) |
|---|--|
| <ul style="list-style-type: none"> ・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。 | <ul style="list-style-type: none"> ・販売代理店の管理者によって、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。必要に応じて販売代理店の管理者にご確認ください。 |
| <ul style="list-style-type: none"> ・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。 | <ul style="list-style-type: none"> ・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) |
| <ul style="list-style-type: none"> ・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？ | <ul style="list-style-type: none"> ・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、必要に応じて販売代理店の管理者にご確認ください。 |
| <p>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？</p> | <p>販売代理店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(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。追加項目の詳細は販売代理店の管理者にご確認ください。</p> |

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

digicert | CERTCENTRAL

アカウント | 日本語

オーダー管理

Business SSL オーダー番号 124208640
グローバル・サーバID, 1年

優先サポート | PQC ツールキット | CT ログ監視を有効にする | 脆弱性アセスメントを有効にする

コモンネーム: <FQDN> | オーダーステータス: 発行済 | 有効期間: 09 Mar 2021 - 16 Mar 2022

証明書の詳細

コモンネーム: ga-demo202103.vsdj.jp
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

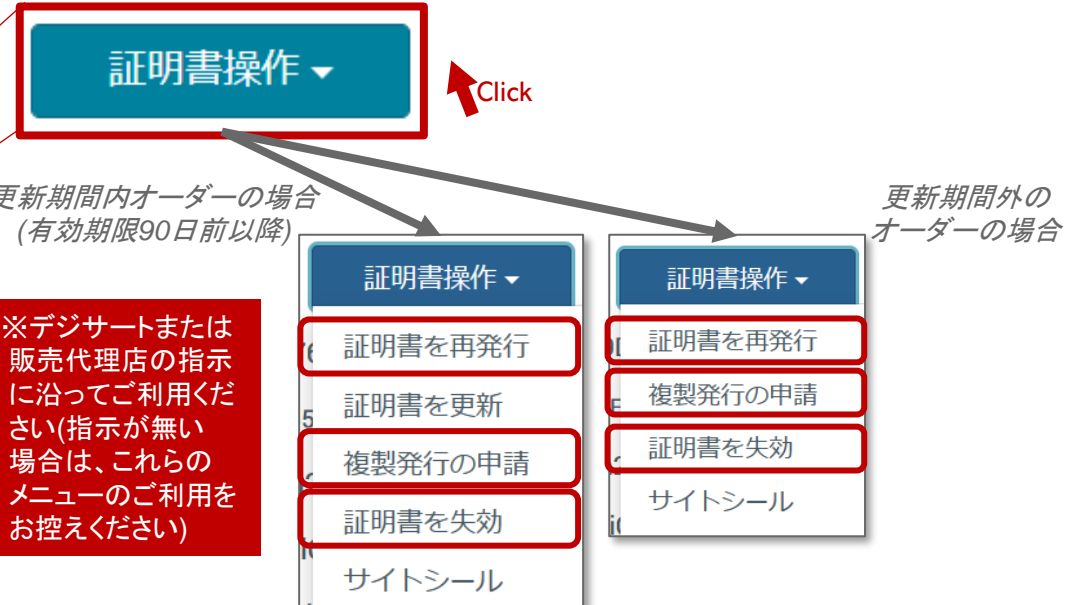
組織: <組織情報>

シリアル番号: 0B26AED7B46EBD2B017234B61E69CBDB
拇印: C5ABEA8134843FC9C33D757FB2C61102E5D6B4F6
署名ハッシュ: sha256
中間認証局: DigiCert TLS RSA SHA256 2020 CA1
有効期間: 09 Mar 2021 - 16 Mar 2022
CSR: 含む ビュー

注文詳細

申請日: 09 Mar 2021 4:56 AM
複数年プランの詳細: 1年プラン (08 Mar 2021 - 16 Mar 2022)
自動更新: いいえ
Auto-reissue:
申請責任者: <申請責任者情報>
技術担当者: <技術担当者情報>
管理グループ: Win The Customer, LLC
オーダーステータス: 発行済
プラットフォーム: Apache

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

証明書操作 ▾

証明書を再発行

複製発行の申請

証明書を失効

サイトシール

【ゲストアクセスリンク】



■再発行(Reissue)申請画面

digicert® | CERTCENTRAL® アカウント 日本語

オーダー番号 115039341

証明書 (オーダー番号 115039341) を再発行

セキュア・サーバID

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

有効性を保つために、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

コモンネーム
ga-demo20210118-1.appfw.net
クリックして名前を追加する

* 中間チェーン (中間 CA) > [ルート CA]
DigiCert TLS RSA SHA256 2020 CA1 (SHA2-256) > DigiCert Global Root CA (SHA1)

* 署名ハッシュ
SHA-256

* サーバープラットフォーム
Apache
Microsoft IIS 5 or 6
Microsoft IIS 7
Microsoft IIS 8
Microsoft IIS 10
Microsoft Exchange Server 2007

再発行の理由
(例: 秘密鍵の紛失、新しいサーバーなど)

キャンセル 再発行の申請

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

Click

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)

■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。

証明書の変更を確認

① DNS名が削除されていないため、既存の証明書およびその複製の証明書は失効されません。

| 変更されたフィールド | 現在の証明書詳細 | 再発行申請される証明書の詳細 |
|------------|-----------------------------|-----------------------------|
| コモンネーム | ga-demo20210118-1.appfw.net | ga-demo20210118-1.appfw.net |
| SANs | ga-demo20210118-1.appfw.net | ga-demo20210118-1.appfw.net |

キャンセル 申請の確認

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

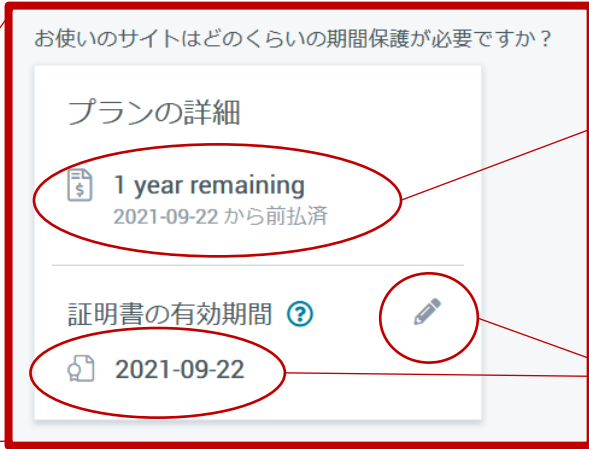
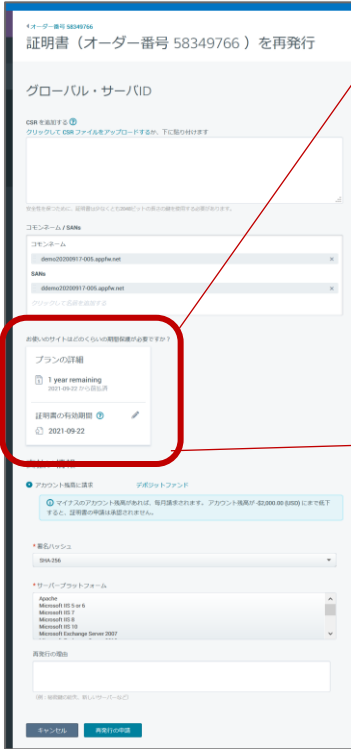
Click

※1: 中間チェーン欄は販売代理店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>

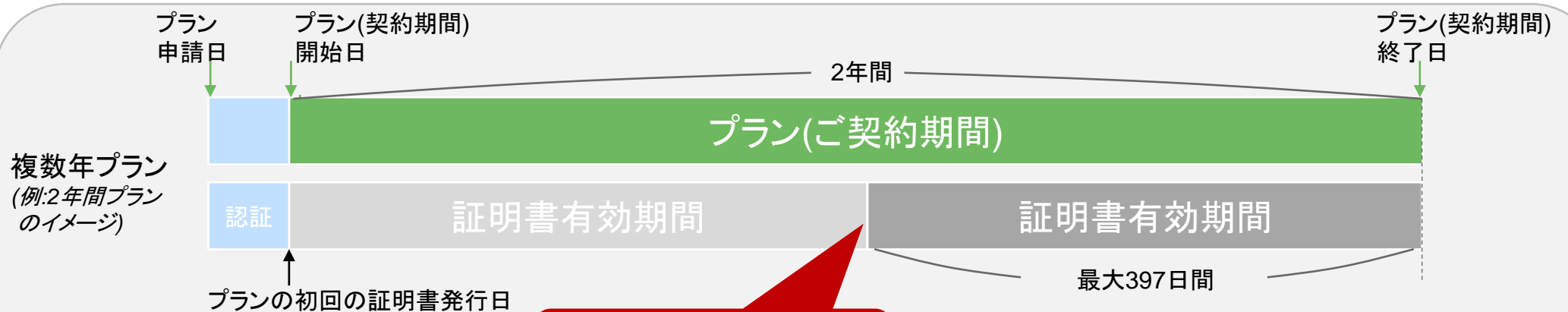
補足 再発行(Reissue)申請時の「証明書有効期間」について

■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。

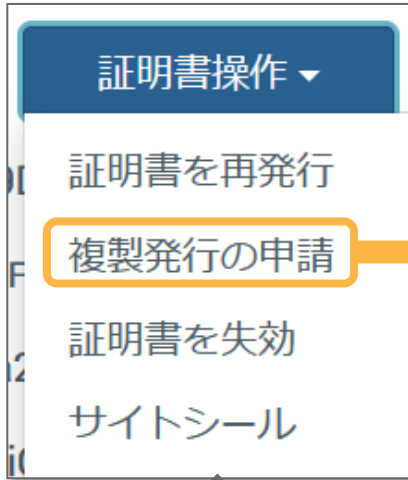
- ・【証明書の有効期間】の初期設定値は「プラン(契約期間)終了日」と「397日間」のいずれか早い方が設定されます
- ・上部のペンの形のアイコンをクリックすると[証明書の有効期間]を編集いただくことが可能です
- ・編集後の【証明書の有効期間】の終了日は「プラン(契約期間)終了日」を超えることはできません
- ・編集後の【証明書の有効期間】は「397日間」を超えることはできません
- ・再発行申請によってプラン(ご契約期間)を延長することはできません



証明書再発行
(当セクションの内容)

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】



■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。

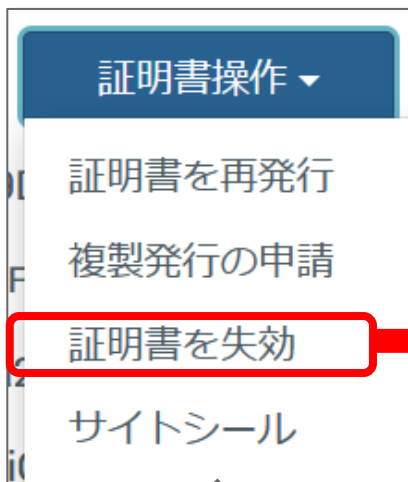
※1 : 中間チェーン欄は販売代理店のアカウント設定によって表示されない場合があります。各製品ごとにご利用いただける中間証明書とルート証明書の組合せについて : <https://knowledge.digicert.com/ja/jp/solution/SOT0006.html>
 ※2 : 中間証明書は定期的に変更されます。新しい(End-Entity)証明書を取得された場合はその都度、以前に利用した中間証明書を再利用せず、最新の中間証明書を取得しインストールいただけますようお願いいたします。詳細はこちら : <https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html>

(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 | <ul style="list-style-type: none"> ・サーバ証明書(OV/EV) ・サーバ証明書(DV) ・コードサイン証明書/EVコードサイン証明書 | <ul style="list-style-type: none"> ・サーバ証明書(OV/EV)のみ |
| 主な用途 | <ul style="list-style-type: none"> ・証明書の更新(有効期間延長) ・コモンネーム/SANsの追加/変更/削除 ・鍵/署名アルゴリズムの変更 | <ul style="list-style-type: none"> 鍵/署名アルゴリズムの変更 |
| コモンネーム/SANsの変更 | 可能 (注: 下記「費用」を参照) | 不可 |
| 証明書有効期間終了日の変更 | 可能 (注: 指定可能な証明書有効期間終了日の制限について別紙「再発行(Reissue)申請時の証明書有効期間について」参照) | 不可 |
| 費用 | <p>FQDN(SANs)を追加した場合、以下の式で費用を計算</p> <p>残プラン年数 x 追加したSANsの数量 x 追加SANs単価</p> <p>(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。詳細は販売代理店にお問合せください)</p> | <ul style="list-style-type: none"> ・なし |
| 元証明書が失効されるか? | <p>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</p> | <ul style="list-style-type: none"> ・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」は販売代理店の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。販売代理店の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。必要に応じて販売代理店の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) | <p>[アカウント代表組織名]</p> <p>[申請者(User Placing Order)氏名] 様</p> <p>[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。</p> <p>本メールに新しい証明書を添付しています。</p> | <p>[アカウント代表組織名]</p> <p>[申請者(User Placing Order)メールアドレス] 様</p> <p>[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。</p> <p>証明書: [End-Entity証明書データ (BASE64形式)]</p> <p>中間CA証明書: [中間CA証明書データ (BASE64形式)]</p> |

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

「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(.cert) -中間証明書(.cert) |
| 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(.cert) -中間証明書(.cert) -ルート証明書(.cert) |
| 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。

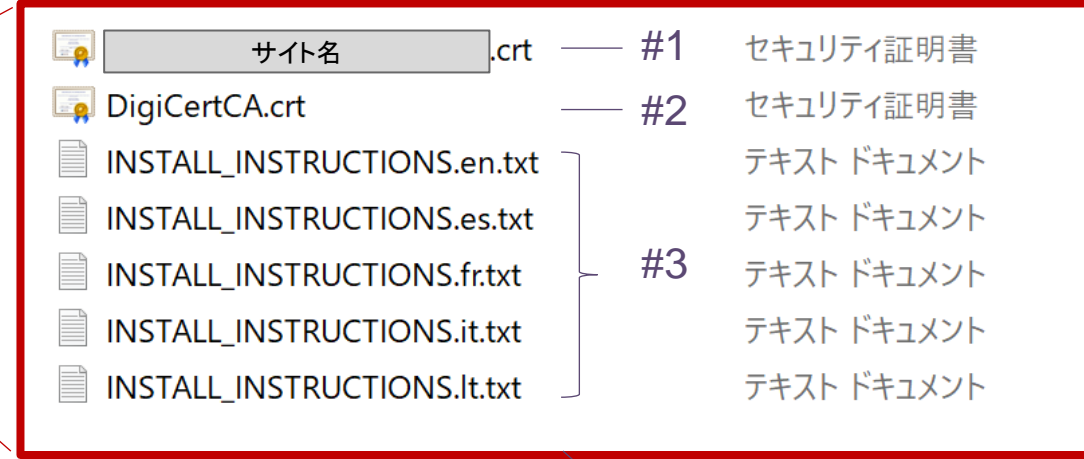
- ・サーバーソフトウェア：<https://dev.digicert.com/glossary/#server-platforms> (※1:サーバーソフトウェアの一覧はこちらを参照ください)
- ・ファイル形式について：<https://dev.digicert.com/glossary/#certificate-formats> (※2:ファイル形式IDの一覧はこちらを参照ください)

(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>.cert | 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。サーバー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ー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)



■ [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)

(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 .crt (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

オーダー番号 124208640
グローバル・サーバID, 1年

優先サポート | PQC ツールキット | CT ログ監視を有効にする | 脆弱性アセスメントを有効にする

コモンネーム: <FQDN> | オーダースtatus: 発行済 | 有効期間: 09 Mar 2021 - 16 Mar 2022

証明書の詳細

コモンネーム: ga-demo202103.vsdj.jp
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: <組織情報>

シリアル番号: 0B26AED7B46EBD2B017234B61E69CBDB
拇印: C5ABEA8134843FC9C33D757FB2C61102E5D684F6
署名ハッシュ: sha256
中間認証局: DigiCert TLS RSA SHA256 2020 CA1
有効期間: 09 Mar 2021 - 16 Mar 2022
CSR: 含む ビュー

注文詳細

申請日: 09 Mar 2021 4:56 AM
複数年プランの詳細: 1年プラン (08 Mar 2021 - 16 Mar 2022)
自動更新: いいえ
Auto-reissue:
申請責任者: <申請責任者情報>
技術担当者: <技術担当者情報>
管理グループ: Win The Customer, LLC
オーダーステータス: 発行済
プラットフォーム: Apache

■証明書をダウンロード

以下の形式で証明書をダウンロード ▾ Click

↓

以下の形式で証明書をダウンロード ▾

- .crt (Apache / Linuxに最適)
- .p7b (MicrosoftとJavaに最適)
- その他オプション...

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> | |

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

■ オーダー詳細画面

ゲストユーザー

オーダー管理

オーダー番号 124208640
グローバル・サーバID, 1年

優先サポート PQC ツールキット CT ログ監視を有効にする 脆弱性アセスメントを有効にする

共通ネーム: <FQDN> オーダーステータス: 発行済 有効期間: 09 Mar 2021 - 16 Mar 2022

証明書の詳細

証明書操作

以下形式で証明書をダウンロード

共通ネーム: ga-demo202103.vsdj.jp
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: <組織情報>

シリアル番号: 0B26AED7B46EBD2B017234B61E69CBDB
拇印: C5ABEA8134843FC9C33D757FB2C61102E5D684F6
署名ハッシュ: sha256
中間認証局: DigiCert TLS RSA SHA256 2020 CA1
有効期間: 09 Mar 2021 - 16 Mar 2022
CSR: 含む ビュー

注文詳細

申請日: 09 Mar 2021 4:56 AM
複数年プランの詳細: 1年プラン (08 Mar 2021 - 16 Mar 2022)
自動更新: いいえ
Auto-reissue:
申請責任者: <申請責任者情報>
技術担当者: <技術担当者情報>
管理グループ: Win The Customer, LLC
オーダーステータス: 発行済
プラットフォーム: Apache

■ 証明書操作

証明書操作

更新期間内オーダーの場合 (有効期限90日前以降)

更新期間外のオーダーの場合

- 証明書を再発行
- 証明書を更新
- 複製発行の申請
- 証明書を失効
- サイトシール

| 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。 |

Order ID: 115429178

サイトシール

Select a seal image

Norton seal DigiCert seal

①

Configure the seal

Read the instructions for installing your site seal.

Choose a seal size

Small
 Medium
 Large

②

Seal code

③

④

プレビュー

Click the seal to see an example of the popup.

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)

ev.digicert.com
Nov-11-2020
DIGICERT JAPAN G.K.
Tokyo, Japan

日本語

詳しくは以下の項目をクリックしてください

- DigiCert EV SSL 証明書
- 法人登録の認証
- 住所の認証
- 電話番号の認証
- メールアドレスの認証
- ドメイン名所有の認証

DIGICERT JAPAN G.K. provides for the security of their users by enabling the encryption of data transmitted between DIGICERT JAPAN G.K. and your browser during an SSL/TLS encrypted session (look for the padlock). DIGICERT JAPAN G.K. holds a website identity assurance warranty of \$1,750,000 subject to the Relying Party Agreement.
[Relying Party Agreement](#)
NOTICE: YOU MUST READ AND AGREE TO THIS RELYING PARTY AGREEMENT BEFORE RELYING ON A DIGICERT-ISSUED CERTIFICATE OR SITE SEAL.

■(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)

ov.digicert.com
Nov-11-2020
DIGICERT JAPAN G.K.
Tokyo, Japan

日本語

詳しくは以下の項目をクリックしてください

- DigiCert SSL 証明書
- 法人登録の認証
- 住所の認証
- メールアドレスの認証
- ドメイン名所有の認証

DIGICERT JAPAN G.K. provides for the security of their users by enabling the encryption of data transmitted between DIGICERT JAPAN G.K. and your browser during an SSL/TLS encrypted session (look for the padlock). DIGICERT JAPAN G.K. holds a website identity assurance warranty of \$1,750,000 subject to the Relying Party Agreement.
[Relying Party Agreement](#)
NOTICE: YOU MUST READ AND AGREE TO THIS RELYING PARTY AGREEMENT BEFORE RELYING ON A DIGICERT-ISSUED CERTIFICATE OR SITE SEAL.

FQDN

組織情報

表明事項
(認証項目)
の説明

「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タルの 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_TSD09sC1"></div>

<!-- DigiCert Seal Code -->
<!-- Place with DigiCert Seal HTML or with other scripts -->
<script type="text/javascript">
var __dcid = __dcid || [];__dcid.push(["DigiCertClickID_TSD09sC1", "15", "1", "black", "TSD09sC1"]);(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

■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)

■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)

←オーダー管理

Business SSL

オーダー番号 34631061
Secure Site OV、1年

優先サポート

| コモンネーム | オーダーステータス | 有効期限 |
|------------------------|-----------|------|
| demo20200630-b <ドメイン名> | 発行済 | 30 |

証明書の詳細

| | | |
|--------|------------------------|-------------------------|
| コモンネーム | demo20200630-b <ドメイン名> | 証明書のインストールを確認 |
| 組織 | DIGICERT JAPAN G.K. | VirusTotal でドメインをチェックする |

CertCentralの外部へリンク

VIRUSTOTAL

1 / 64

One engine detected this URL

<ドメイン名情報>

<ドメイン名情報>

Community Score

DETECTION DETAILS COMMUNITY

| | |
|-------------------|----------|
| BitDefender | Phishing |
| AegisLab WebGuard | Clean |

VirusTotal でドメインをチェックする

Click

■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

■初期状態 (CTログモニタリングが有効化されていない)

digicert® | CERTCENTRAL® Enterprise

証明書管理

ダッシュボード

証明書

オーダー

証明書申請の一覧

ドメイン

組織

期限切れになる証明書

認証局 New

DISCOVERY

自動化

オーダー管理

オーダー番号 34643117
Secure Site Pro SSL、1年

優先サポート PQC ツールキット CTログ監視を有効にする

CTログ監視を有効にする

Click

ドメイン: demo20200630-c.vsdj.jp
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: DIGICERT JAPAN G.K.
Chuo-ku, Tokyo, JP
Phone: 03-4560-3900

■CTログモニタリングが有効化された状態

Business SSL

オーダー番号 34643117
Secure Site Pro SSL、1年

優先サポート PQC ツールキット CTログ

✓ このオーダーについて Certificate Transparency ログ監視が正常に有効になりました。

CTログ

CTログを表示

CTログ監視を無効にする

通知を管理

| 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) |

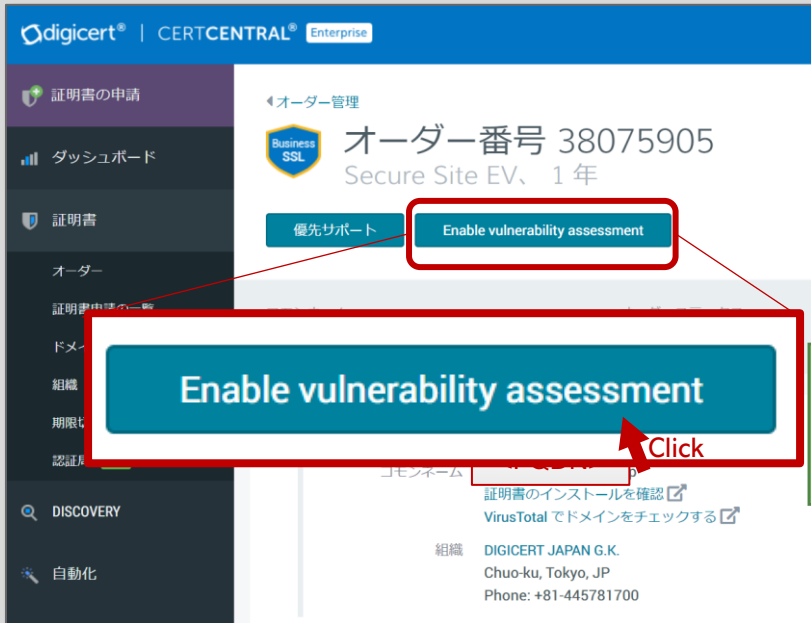
8. ゲストアクセスによる証明書製品のその他の機能の利用

～ 8.3 脆弱性アセスメント～

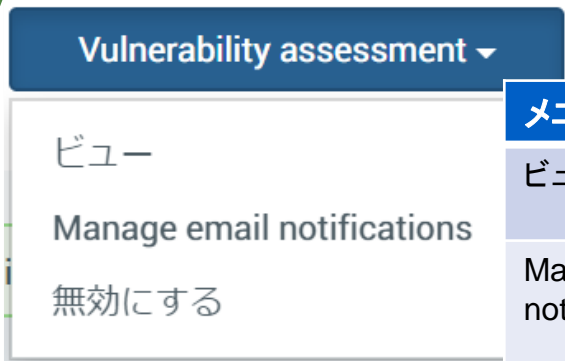
■対象製品
 ・セキュア・サーバID EV
 ・グローバル・サーバID
 ・グローバル・サーバID EV

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

■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 |

■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

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

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

Vulnerability assessment ▾

- ビュー
- Manage email notifications
- 無効にする

■脆弱性アセスメントの結果を確認

Order No. 21382194

Business SSL Vulnerability assessments
 Order No. 21382194

Search by domain: ステータス:

Assessments only scan the highest common level of base or subdomains on the certificate.

| Domain name | ステータス |
|-------------|--------|
| <FQDN> | Secure |

Report

PDFをダウンロード

Vulnerability Report

Scan name: 2f750c4b-6869-40f8-822a-e62947a5053f

Host(s) scanned: <FQDN>

Date and time: 2020-08-20 06:2

PDF

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

Manage email notifications

Send an email notification to all contacts listed on this order:

- After every completed scan
- Only when scan finds vulnerabilities
- Never send email notifications

キャンセル 保存

| 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 |