

---

# デジサートユーザ向け CertCentral簡易ガイド [ドキュメントサイニング証明書]

2025年6月18日更新



# 目次

1. 申請前の準備 : [page 3](#)
2. 証明書の新規申請 : [page 7](#)
3. 証明書の更新申請 : [page 15](#)
4. 証明書の取得 : [page 17](#)
5. 証明書の再発行 : [page 20](#)

申請前の準備

# 証明書の発行まで

## 1 比較検討/お見積り



製品ごとの特長を比較検討し、該当する製品のお見積書を取得してください。

## 2 オンライン申込 & お支払



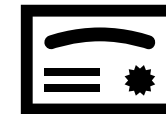
画面の流れに沿って必要事項をご入力ください。また、案内に沿ってお支払いを完了させてください。

## 3 認証 / 証明書の発行通知



お申込み情報を基に認証（発行審査）後、発行のお知らせをEmailで送付します。  
証明書は通常3営業日程で発行されます※。

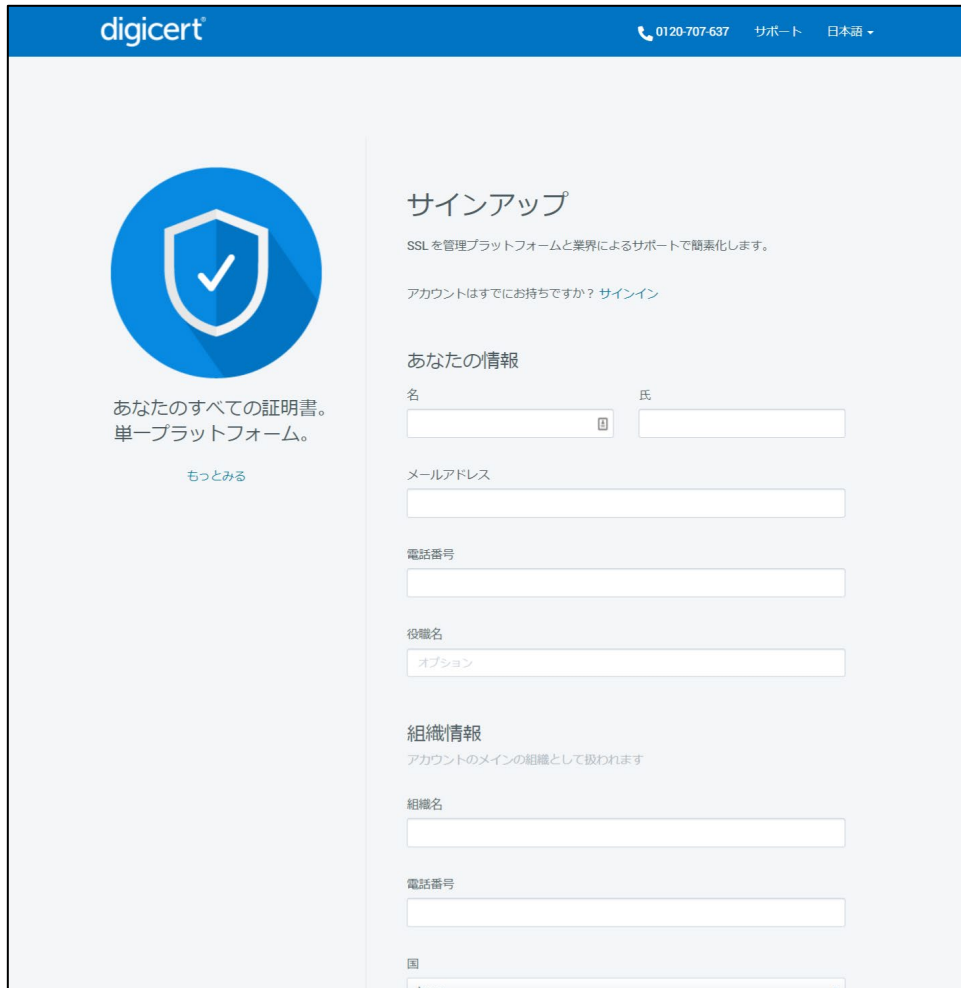
## 4 ドキュメントサイニング証明書のインストール



必要に応じてトークンに証明書のインストールを行い、署名を行うアプリケーションの手順に沿ってデジタル署名します。

※ 問題なくスムーズに認証が進んだ場合になります。お申込み内容によっては3営業日以上の日数を要する場合がございます。

# CertCentral アカウントの作成（オンライン申込）



digicert 0120-707-637 サポート 日本語

**サインアップ**  
SSLを管理プラットフォームと業界によるサポートで簡素化します。

アカウントはすでにお持ちですか？ [サインイン](#)

あなたの情報

名  氏

メールアドレス

電話番号

役職名

組織情報  
アカウントのメインの組織として扱われます

組織名

電話番号

国

あなたのすべての証明書。  
単一プラットフォーム。  
[もっとみる](#)

「CertCentral」アカウント作成ページにアクセスしてください

<https://www.digicert.com/account/signup/standard/?lang=ja&currency=JPY>

- ① CertCentralのアカウントをお持ちでない方は上記の申請画面よりアカウント新規作成（無料）してください
- ② 初めに、CertCentralのメイン管理者（Administrator）様となるご担当者様の情報を入力します
- ③ 次に、主にアカウント管理を行う企業・組織の情報を入力します  
※組織情報はサインイン後、追加、削除等が可能です
- ④ 最後に、主にアカウント管理を行う企業・組織の情報を入力します  
※ユーザはサインイン後、追加、削除等が可能です

# CertCentralを日本語でご利用いただくための各種設定について

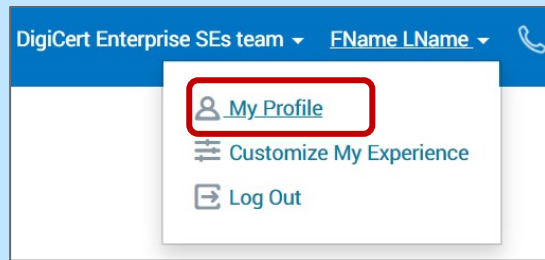
区分

設定方法

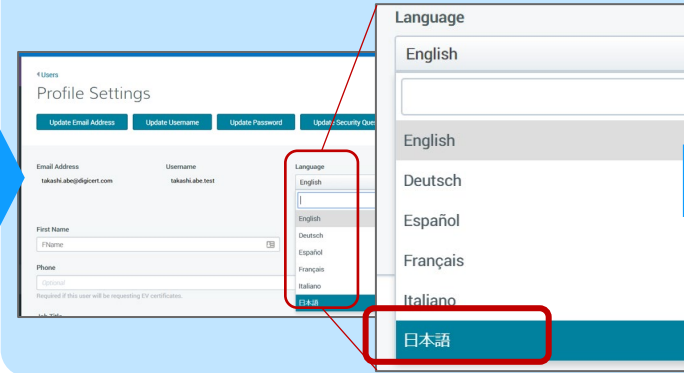
画面表示  
言語

画面表示言語を日本語へ切り替える

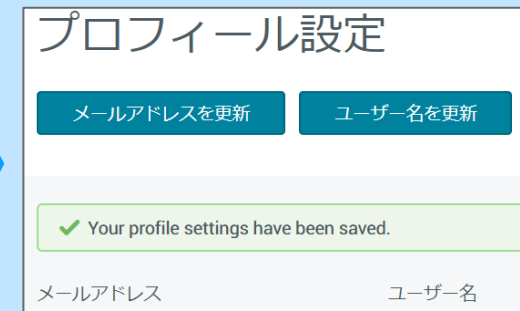
STEP 1: 画面右上部の「My Profile」から「Profile Setting」をクリック



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



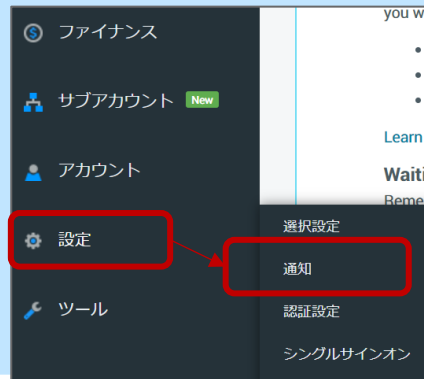
STEP 3: 下のようなメッセージが表示されれば完了です



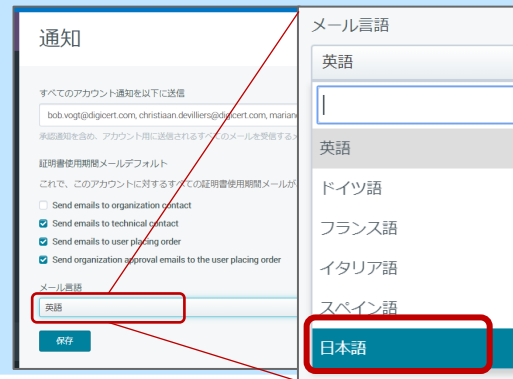
メール  
言語

配信されるメール（※DCVメールを除く）を日本語へ切り替える

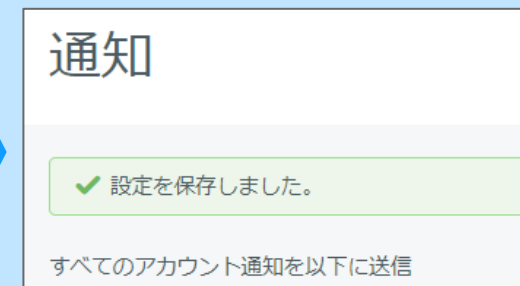
STEP 1: 画面左メニューの「設定」から「通知」をクリックし「通知」をクリック



STEP 2: 画面下部の「メール言語」プルダウンリストから「日本語」を選択



STEP 3: 下のようなメッセージが表示されれば完了です



証明書の新規申請  
ドキュメントサイニング証明書

# 証明書の新規申請：ドキュメントサイニング証明書

Section 1: 証明書情報

Section 2: トークン配送オプション

Section 3: 証明書発行先情報

左メニューより「**証明書の申請**」をクリックして製品をお選びください

2025年3月20日より以下新製品へ変更となりました。Adobe Acrobat、DocuSign、Microsoft Office、OpenOffice およびLibreOffice のドキュメントへの署名に利用することができます。

新製品	旧来の製品
<a href="#">Document Signing for Individual (ドキュメントサイニング証明書 個人)</a>	Document Signing - Individual (500/2000)
<a href="#">Document Signing for Business - Employee</a> ※SubjectのCommonNameに個人名を格納します	Document Signing - Organization (2000/5000)
<a href="#">Document Signing for Business - Group</a> ※SubjectのCommonNameに組織名を格納します	Document Signing - Organization (2000/5000)

注：バウチャーをご利用の場合は、バウチャー券面に記載のURLから、ご申請ください。

[CertCentral]バウチャー(クーポン)を利用するうえでの注意点について  
<https://knowledge.digicert.com/jp/general-information/faq-vouchers>

# 証明書の申請：証明書年数の選択

## Document Signing for Business - Group証明書を申請する

対象：デジサート・ジャパン合同会社

### 証明書の設定

証明書の有効性 ←

- 1年
- 2年
- 3年
- カスタム有効期間
- カスタム長

### 有効期間

- ・証明書に必要な有効期間を選択します（1年～3年）
- ※有効期間の指定で証明書の終了日の指定、カスタム長で発行日から何日間の指定をすることが可能です。

必須

# 証明書の申請：プロビジョニング方法

必須

## プロビジョニングオプション

- DigiCert提供のハードウェアトークン (¥ 20,000 (JPY), non-refundable)
- 既存のトークンを使用する
- HSMにインストールする

配送先住所

受取人のフルネーム

国

住所1

住所2 (任意)

例: "Suite #"

市町村名

State / Province /  
Region

Zip / Postal  
Code

## プロビジョニングオプション

ドキュメントサイニング証明書をハードウェアトークンに格納する際のオプションを選択します。  
※証明書を新規に取得する場合やお手元にトークンがない場合など、新しいトークンが必要な方は「DigiCert提供のハードウェアトークン」を選択してください。

トークンの送付先が表示されますので、トークン送付先を指定してください。

※「DigiCert提供のハードウェアトークン」をご購入いただいた場合は返金及び返品不可となります。

※ハードウェアトークンとHSMは、FIPS 140 レベル 2、Common Criteria EAL 4+、または同等のものである必要があります。

企業認証コードサイニング証明書における秘密鍵の格納に関する要件

<https://knowledge.digicert.com/jp/general-information/new-private-key-storage-requirement-for-standard-code-signing-certificates>

※証明書を更新する場合などすでにトークンをお持ちの方は「既存のトークンを使用する」を選択してください。

※HSMにインストールする場合は「HSMにインストールする」を選択してください。

- DigiCert提供のハードウェアトークン (¥ 20,000 (JPY), non-refundable)
- 既存のトークンを使用する
- HSMにインストールする

プラットフォーム

SafeNet eToken 5110 FIPS (ECC ONLY)

上記のボックスには、承認済みハードウェアトークンのいずれかがリストされている必要があります。リストにないデバイスに証明書をインストールすることはできません。承認済みトークンがない場合は、事前設定されたハードウェアトークンを配送するオプションを選択してください。ご質問がごある場合は、DigiCert サポートまでお問い合わせください。

- DigiCert提供のハードウェアトークン (¥ 20,000 (JPY), non-refundable)
- 既存のトークンを使用する
- HSMにインストールする

コモンライテリア EAL4+ 標準またはFIPS 140-2 level 2 HSM デバイスが必要です。準拠するHSMがない場合は、別のプロビジョニング方法を選択してください。ご質問がごある場合は、デジサートまでお問い合わせください。

秘密鍵はCommon Criteria EAL4+標準またはFIPS 140-2レベル2 HSMで生成されましたか?

- はい
- いいえ

CSRを追加する

CSRをアップロード、またはここに貼り付けてください。コードサイニング証明書は、安全性を保つために最低3072ビットの長さのRSA鍵を使用する必要があります。

お使いの CSR はヘッダから始まり、  
"-----BEGIN CERTIFICATE REQUEST-----" フッタ "-----END CERTIFICATE REQUEST-----" で終わります。

# 証明書の申請：証明書情報の入力

組織



組織を追加する

## 組織

・「組織を追加する」をクリックし、証明書情報に記載される「組織」を選択します。ラジオボタン「既存の組織」で登録済の組織情報、もしくは「新しい組織」から新たに登録の上、組織を確定してください。組織が有効であれば、認証済み、認証保留中のステータスにかかわらずご申請いただけます。

必須

## ▼ 証明書の詳細オプション

鍵のタイプとサイズ: ?

RSA 2048

署名ハッシュ: ?

sha256WithRSA

証明書の使用

複数用途の文書署名

Adobe PDF、Microsoft 文書、その他の文書の署名向けに推奨されています。

文書署名 - 互換性

デジサートの以前の製品と一致する証明書が必要な場合 (文書署名 - 組織/個人)

否認防止のキーの使用を追加

発行元認証局

中間チェーンです。 [中間CA] > [ルートCA] ?

DigiCert Assured ID G2 Multi Doc Signing RSA4096 SHA384 2023 CA1 (SHA2-384) > DigiCert Assured ID Root G2 (SHA2-256)

## 証明書の詳細オプション

以下の詳細設定が可能です。

- ・「**鍵のタイプとサイズ**」：必要に応じてご選択ください。
- ・「**署名ハッシュ**」：必要に応じてご選択ください。
- ・「**証明書の使用**」：複数用途の文書署名で利用する際はデフォルトのままご申請ください。旧製品で提供していたチェーンをご利用されたい場合は[文書署名 - 互換性]をご選択ください。
  - ※発行元認証局  
複数用途の文書署名：  
DigiCert Assured ID G2 Multi Doc Signing RSA4096 SHA384 2024 CA1(SHA2-384) > DigiCert Assured ID Root G2(SHA-256)
  - 文書署名 - 互換性：  
DigiCert Document Signing CA(SHA-256) > DigiCert Assured ID Root CA(SHA1)
- ・「**否認防止キーの使用を追加する**」：証明書に「否認防止 (Non-Repudiation)」キーの使用を追加する場合は、このオプションを選択します。

任意

# 証明書の申請：証明書情報の入力

## ※ドキュメントサイニング証明書 個人証明書(Document Signing for Individual)と Document Signing for Business – Employee の場合のみ



### サブジェクトの個人を追加する

**i** 対象となる個人の氏名は、貴社組織に関連する個人の現在の氏名でなければなりません。個人の氏名を証明する証拠を収集し、保管しなければなりません。

名(下の名)  
ミドルネームとイニシャルを含めることもできます。"Dr." (博士) のような肩書きや接頭辞は含めないでください。

姓  
"Sr." や "III" などの世代接尾辞を含めることができます。

部署名および役職名(任意)

国コード  電話番号

国

Eメール

### 証明書の詳細

証明書に登録されるサブジェクトの個人を認証する必要があります。

- ・「名」「姓」：名前と氏名を入力してください
- ・「部署名および役職名(任意)」：必要に応じてご入力ください。
- ・「国コード」：日本の「+81 Japan」を選択してください。
- ・「電話番号」：半角数字で入力してください。
- ・「国」：「Japan」を選択してください。
- ・「Eメール」：証明書で利用するEメールアドレスを入力してください。

必須

# 証明書の申請：その他のオーダー情報入力

## ✓その他のオーダーオプション

追加の更新メッセージ (任意)

追加のEメール (任意)

これらのアドレスには、証明書発行、証明書有効期限切れ、オーダー有効期限切れの通知が届きます。アドレスはカンマで区切るか、別の行にしてください。

## その他オーダーオプション

任意

- ・「追加の更新メッセージ」：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。
- ・「追加のEメール」：証明書発行通知メール、更新案内メールの宛先を追加することができます。

## 支払い情報

クレジットカードに請求する

銀行振込向けに請求する

請求先情報

## 支払い情報

必須

「クレジットカードへの請求」または「銀行振込への請求」のいずれかを選択し、必要項目を入力します。銀行振込場合は、請求書の宛名情報をご確認ください。

※バウチャーをご利用いただいている場合は、バウチャー番号が表示されます。

規約同意、証明書の申請

キャンセル

証明書申請を送信する

Click

Click

【提出】をクリックすることで、マスターサービス契約  に同意します。

## 証明書サービス規約

必須

リンク先の「マスターサービス契約」をご確認いただき、「申請を送信」をクリックしてください。

以上で申請は終わりです。次項の手順に沿ってご請求金額をお支払いください。

# 証明書の申請：お支払い

決済手段「**銀行振込**」の場合は、証明書発行後にご申請いただいたオーダーのご請求書をダウンロードし、請求書に記載の期日までにお支払いを完了させてください。

- ① 左メニューの「**証明書**」>「**オーダー**」> 該当[**オーダー番号**]をクリック
- ② 申請詳細画面にある「請求と支払いの詳細情報」から「**請求書をダウンロードする**」をクリック

請求と支払いの詳細情報

支払い方法	請求書	合計価格
銀行振込	<b>請求書をダウンロードする</b>	¥ 121,000 (JPY)

請求書をダウンロードを押下すると、請求書のプレビューと合わせて、PDFにてダウンロードができます。請求書の内容に沿ってお支払いください。

**注：バウチャーをご利用の場合は、右図の請求書は表示されません。**  
[CertCentral]バウチャー(クーポン)を利用するうえでの注意点について  
<https://knowledge.digicert.com/jp/general-information/faq-vouchers>

## ご請求書サンプル

請求書

digicert® デジサート・ジャパン合同会社  
〒104-0061 東京都中央区銀座6-10-1  
TEL: 03-4560-3971  
FAX: 03-6256-0881  
登録番号: T8010001078218

請求書番号: [ ]  
発行日: 2023/10/26

登録番号(インボイス制度)

請求先 [ ]  
合計 ¥ 34,430  
お支払い期日: 2023/11/30

支払条件	支払期日	オーダー番号
Net 30 EOM	2023/11/30	[ ]

製品	コモンネーム	取引年月日	数量	金額
[ ]	[ ]	2023/10/26	1	¥ 31,300

取引年月日

小計	¥ 31,300
消費税	¥ 3,130
合計	¥ 34,430
支払額	¥ 0
請求金額	¥ 34,430

消費税額/ご請求額

備考

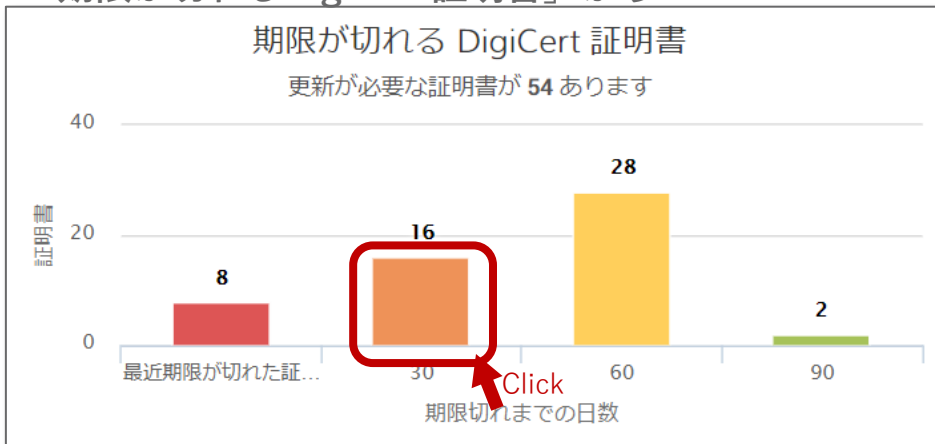
振込先情報  
銀行: 三井住友銀行  
支店(支店番号): ツバキ支店(879)  
口座種別: 当座預金  
口座番号: [ ]  
口座名義: デジサートジャパン(ド)  
\*お振込み手数料は貴社負担でお願いいたします。

お振込み先情報

証明書の更新申請  
ドキュメントサイニング証明書

# 証明書の更新申請：更新元証明書を選択

ダッシュボード内の「期限が切れるDigiCert証明書」から



注：バウチャーをご利用の場合は、バウチャー券面に記載の更新専用URLをクリックし、更新元オーダーを指定してください

「証明書」 → 「有効期限間近の証明書」 から 「今すぐ更新する」

今後30日以内に期限切れになる証明書

オーダー番号	コモンネーム	有効期限日:	製品	有効期間	更新通知	
オーダー番号   クイックビュー	コモンネーム	28 Aug 2019	Document Signing	1年	<input checked="" type="checkbox"/>	今すぐ更新
オーダー番号   クイックビュー	コモンネーム	29 Aug 2019	Document Signing	3年	<input checked="" type="checkbox"/>	今すぐ更新

「今すぐ更新する」をクリックした後は9ページ目以降「新規申請」と同一です。前のセクションをご参照の上、必要な情報を入力・選択いただき申請を完了させてください。

証明書の取得

# 発行された証明書の取得

## — デジサートから発送されたUSBトークンの利用開始 ① —

- ・申請時にプロビジョニングオプションで「あらかじめ設定されたハードウェアトークン」を選択した場合、認証が終わりましたら弊社より認証済住所へUSBトークンを送付いたします。USBトークンの出荷されますと、弊社から下記のEメールが配信されます。
- ・USBのハードウェアトークンが到着しましたら、CertCentralにサインインし、ハードウェアトークンの初期化パスワードを取得します。なお、初期化パスワードの取得は1回のみ表示されるため、必ずお忘れにならないようお願いいたします。

### 証明書発行後 Eメールのご案内

件名	ハードウェアトークン出荷のご案内：オーダー番号
送信元	DigiCert <admin@digicert.com>
本文 (日本語 選択時、 抜粋)	<p>ご申請製品 xTSuDdvgWW のハードウェアトークンを出荷いたしました。</p> <p>次のリンクより、配送状況を追跡いただけます。 <a href="#">Links</a></p> <p>配送物が国内各地域のセンターに到着した後は、国際的な配送状況追跡をご利用いただけない場合もありますこと、ご了承ください。</p> <p>トークンを受領されましたら、CertCentralのアカウントにログインしてデバイスのパスワードを確認してください。 <a href="#">CertCentralログイン</a></p> <p>トークンへの初回アクセスの後、パスワードを変更してご利用ください。</p>

お手続き手順はこちらをご参照ください

How to Activate Your Document Signing Token (CertCentral)

<https://www.digicert.com/kb/document-signing/secure-token-setup.htm>

※英語のサイトとなりますのでご不便である場合にはブラウザの翻訳機能などをご活用ください。

# 発行された証明書の取得

## -既存のトークンへのインストール ②-

- ・申請時にプロビジョニングオプションで「既存のトークンを使用する」を選択された場合、認証が終わりましたら弊社から下記のEメールが配信されます。
- ・CertCentralにサインインし、ハードウェアトークンの初期パスワードを取得の上、トークンに証明書をインストールします。

### 証明書発行後 Eメールでのご案内

件名	Document Signing 証明書発行のお知らせ
送信元	DigiCert <admin@digicert.com>
本文 (日本語 選択時、 抜粋)	<p>ご申請製品 xTSuDdvgWWが発行されました。ハードウェアトークンで証明書を作成する準備が整っております。</p> <p>お手持ちのハードウェアトークンをご利用になる場合は、こちらのリンクを使用して初期化プロセスをダウンロードしてください。 <a href="#">Links</a></p> <p>インストーラを実行後、このオーダーの初期化コードを入力する必要があります。</p> <p>初期化コードは、下記リンクにアクセスすDigiCertアカウントにログインしてご取得ください。 <a href="#">CertCentralログイン</a></p>

お手続き手順はこちらをご参照ください

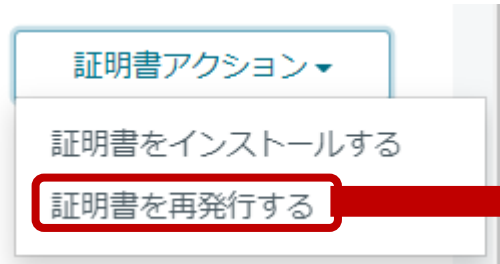
既存トークンへのインストール手順

<https://knowledge.digicert.com/jp/general-information/set-up-your-digicert-provided-etoken>

※EV/OVコードサイング証明書のトークンへのインストール手順 (DigiCert Hardware Certificate Installer) と手順は同じです。

証明書の再発行

# 証明書の再発行(Reissue)申請



◀オーダー番号 131052971

## オーダー番号 131052971 の証明書を再発行する

### Document Signing for Business - Group証明書

すべてのデジサート証明書は無制限で無料再発行できます。

再発行の理由

(例: 秘密鍵の紛失、新しいサーバなど)

キャンセル 再発行を要求する

必要に応じて  
「再発行の理由」  
を入力します (任意)

最後に再発行申請内容確認画面が表示  
されます。  
再発行前後の証明書情報詳細を見比べ  
てご確認いただき、内容に誤りがなけ  
れば「再発行の申請」  
ボタンを押下します。

- ① 左メニューの「証明書」  
「オーダー」 >  
該当[オーダー番号]をクリック
- ② 「証明書操作」 >  
「証明書を再発行」をクリック
- ③ ドキュメントサイニング証明書  
申請時指定した方に証明書再発  
行の承認メールが届きます。
- ④ 発行後のお手続き手順は17ペー  
ジ以降の「証明書の取得」をご  
参照ください

Click



その他ご不明な点があれば下記の  
サポートサイトをご覧ください

**CertCentral**に関するよくあるお問合せ

<https://knowledge.digicert.com/jp/solution/certcentral-qa-general>

**DigiCert Documentation**

<https://docs.digicert.com/ja/>

サポート窓口(申請方法など技術な内容)

<https://www.digicert.com/jp/support>

受付時間：土日祝日および年末年始を除く 平日 9:30 - 17:30