# ユーザ向け
# CertCentral簡易ガイド

Authentication for Employee/Authentication for Individual対応版
2025年 8月 1日更新

digicert®

# 目次


1. 申請前の準備 : page 3
2. OV組織認証の申請 : page 9
3. プラン/証明書の新規申請
   Authentication for Employee : page 12
4. プラン/証明書の新規申請
   Authentication for Individual : page 19
5. 証明書の取得 : page 26
6. 証明書の取り消し : page 29
7. 再発行申請、または更新 : page 34
8. 更新のお知らせ : page 36

# 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 CSR作成は不要

Authentication for EmployeeまたはAuthentication for Individualを申請する場合、取得時に鍵を生成しますので、CSRの準備は不要です。

## 3 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。証明書の販売代理店からご購入する場合は販売代理店にご連絡ください。

## 4 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５営業日以内で発行されます※。
送信されたメール内の手順に従い処理ください。

## 5 認証用証明書のインストール

メール内の手順に従い、証明書を取得すると、証明書を含むPKCS＃12ファイルを作成します。このファイルを利用環境にインストールしてください。

※ 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５営業日以上の日数を要する場合もございます。

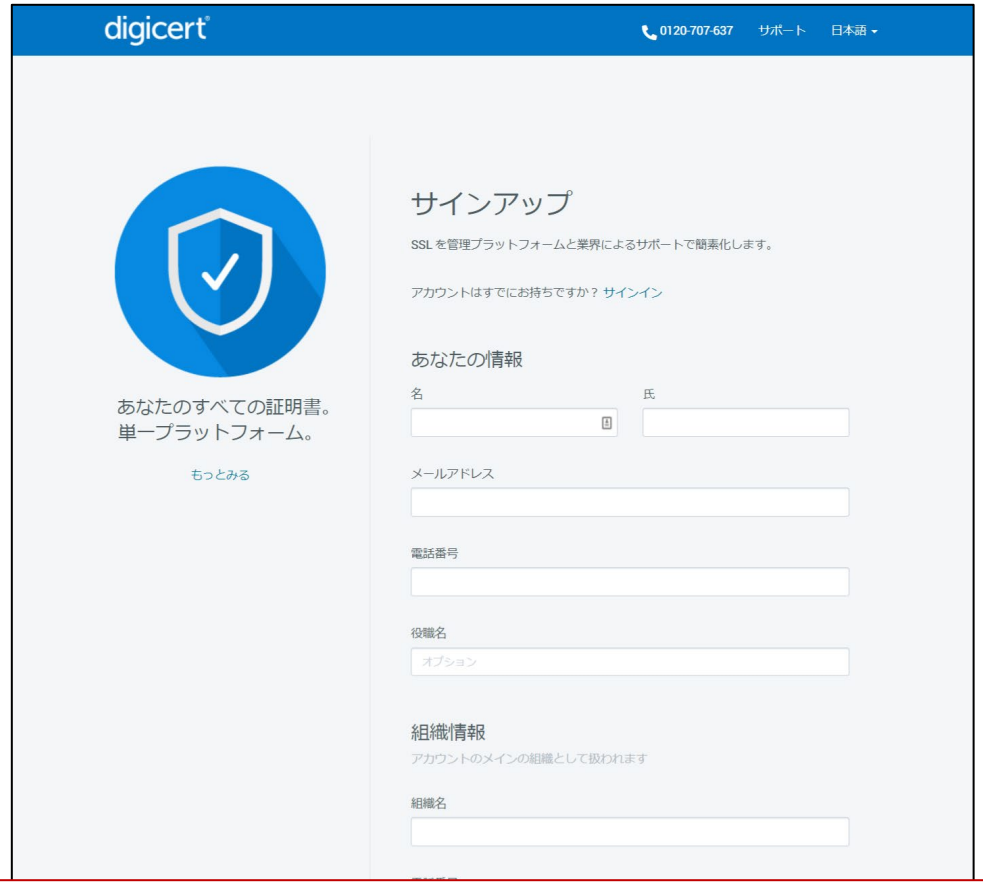
# 製品による申請手順の差異について

- Authentication for IndividualとAuthentication for Employeeでは、証明書に記載される情報に差異があり、認証用証明書として認証要件、発行可能範囲を適用いたします

  - Authentication for Employee
    - 証明書のSubjectにはCNと最大４つのOUを記載することが可能です
    - 組織内個人用の証明書になりますので以下の認証が必要です
      - 組織認証（OV組織認証を使います）
    - 法人登記がされていない等の理由でOV組織認証ができない場合には、本証明書は発行できません

  - Authentication for Individual
    - 証明書のSubjectにはCNと最大４つのOUを記載することが可能です
    - 組織認証は不要です
    - メールアドレスは証明書の記載情報として使用されないため、ドメインの利用権確認（DCV）は不要です
    - 申請を行うと、その時点で即時に証明書を発行いたします

# CertCentral アカウントの作成（オンライン申込）




**「ユーザ名」はCertCentralへのサインイン時に提示いただくIDとなります。「メールアドレス」とは別に指定できますのでログインの際はご注意ください。**

「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 お客様の情報は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組織情報は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

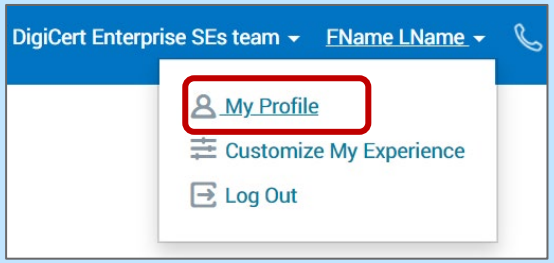
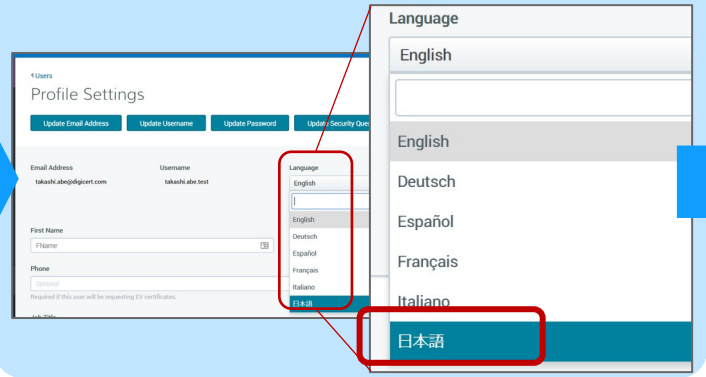
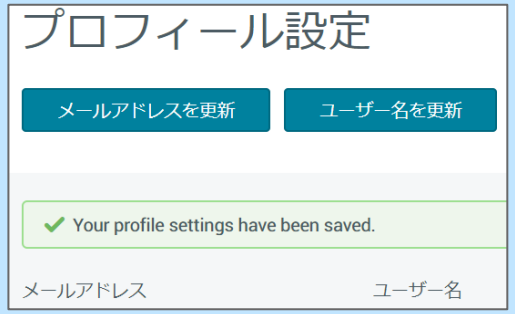
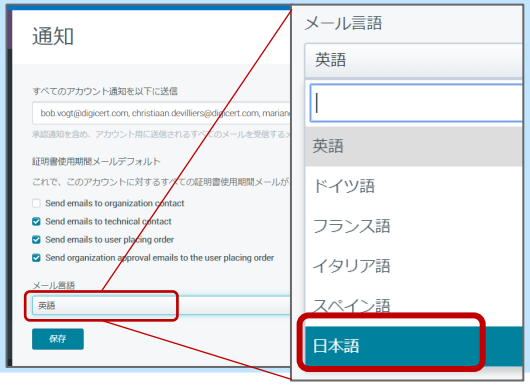
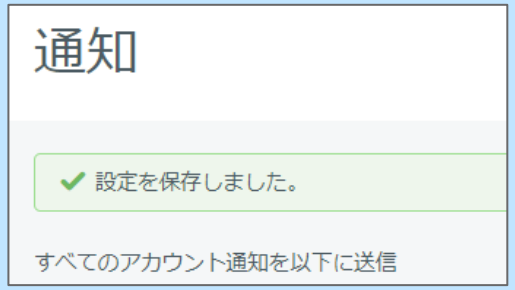
④アカウント情報にはサインインするユーザー名やパスワード、秘密の質問を設定します

※サインインした後、作成したCertCentralアカウントへ複数のユーザーを追加登録することが可能です

⑤ Authentication for～をご利用の場合、アカウントの開設後、開設した組織名とアカウント番号を添えて弊社サポートまでご連絡ください

※デジサート側で製品追加の設定作業が必要です

# 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<br>STEP 1 : 画面右上部の 「My Profile」から「Profile Setting」をクリック<br>  <br>STEP 2 : 画面右側の「Language」プルダウンリストから 「日本語」を選択<br>  <br>STEP 3 : 下のようなメッセージが表示されれば完了です<br>  |
| 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<br>STEP 1 : 画面左メニューの 「設定」から「通知」クリック<br> <br>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<br>  <br>STEP 3 : 下のようなメッセージが表示されれば完了です<br>  |

# よくあるご質問について

- 以下をご参照ください

証明書申請時の組織情報入力とデジサートによる組織認証について
https://knowledge.digicert.com/jp/solution/organization-validation-process

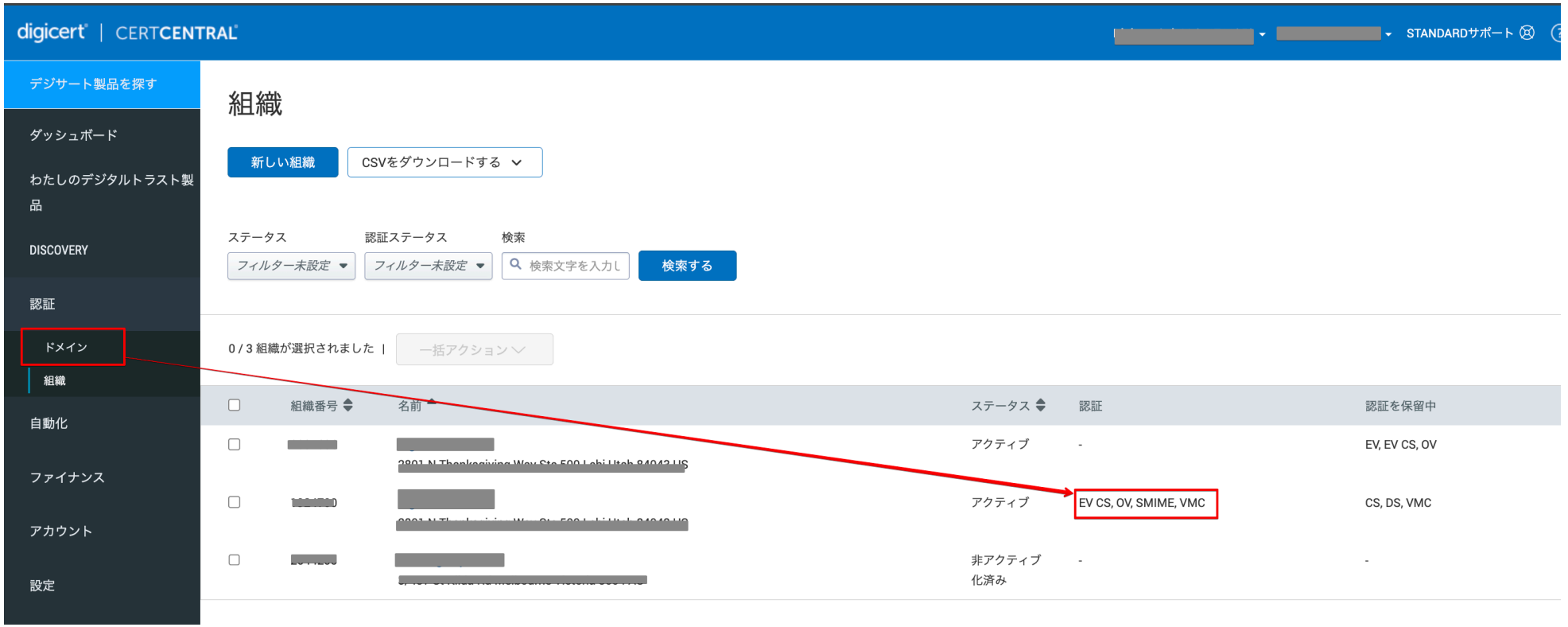
[CertCentral]二要素認証設定について

https://knowledge.digicert.com/jp/general-information/certcentral-two-factor-authentication

# OV組織認証の申請

# 組織認証

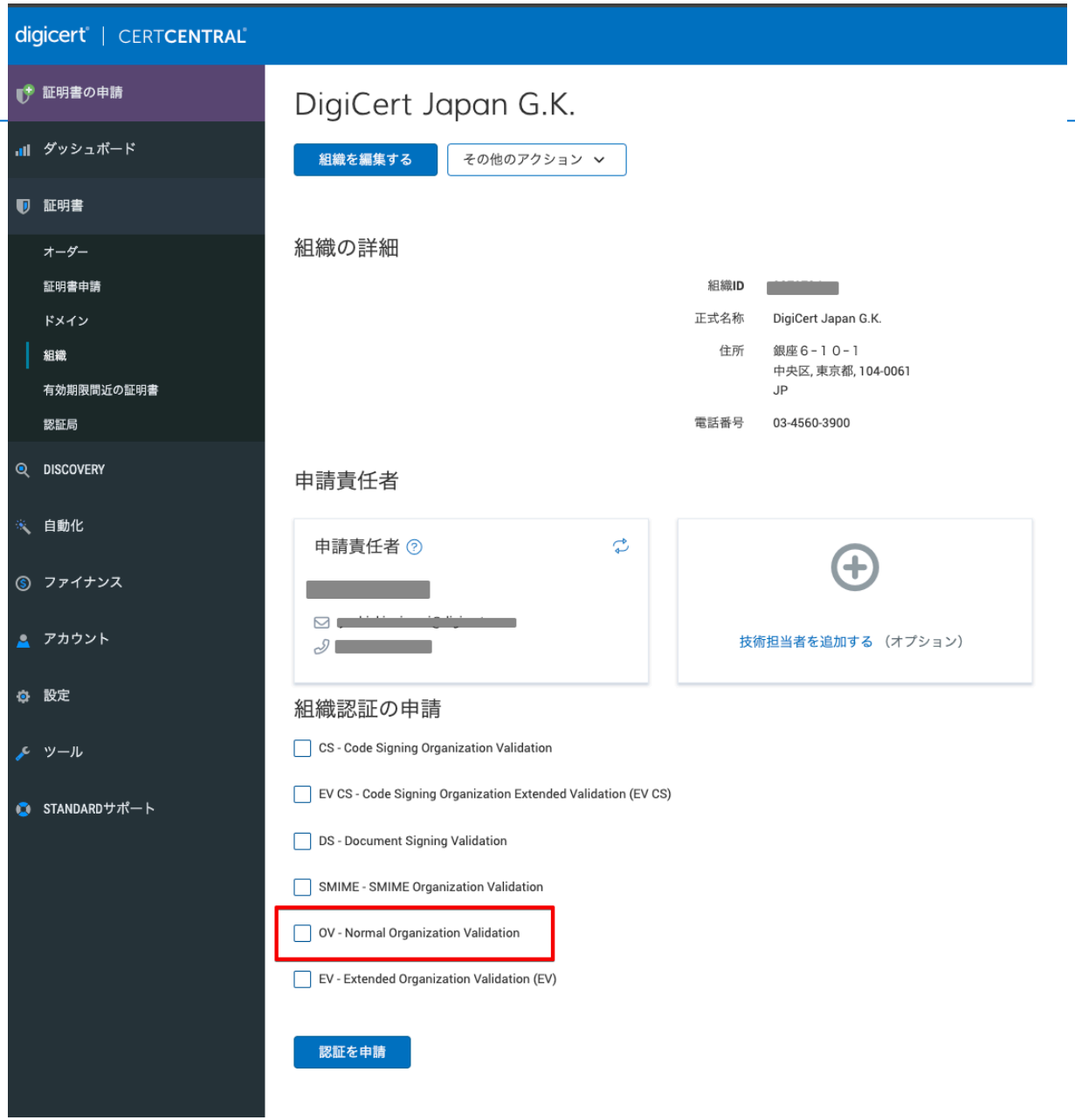
- CertCentralにログイン後、左のメニューから「組織」をクリックしてください
- すでに登録されている組織を表示します。以下のエリアに「**OV**」の記載があれば、OV組織認証が完了しています。完了していない場合、次ページの申請が必要です



# 組織認証の申請

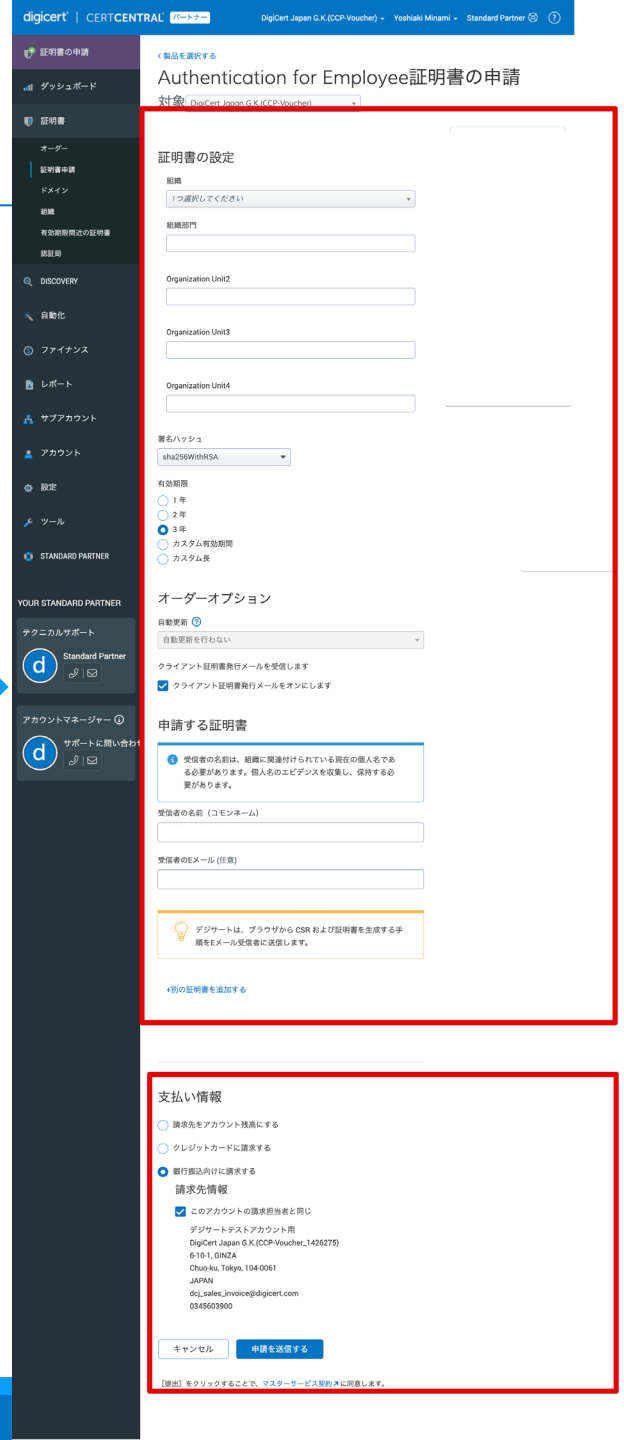
- 既存の組織名をクリックするか、組織を追加してください
- 右の項目でOVの項目「OV – Normal Operation Validation」をチェック
- 「認証を申請」をクリック
- DigiCert認証サポートまでご連絡ください

[事前認証] 組織の認証申請について
https://knowledge.digicert.com/jp/solution/how-to-request-organization-validation



# プラン/証明書の新規申請
# Authentication for Employee

# プラン/証明書の新規申請




Authentication for Employeeを選択してください。

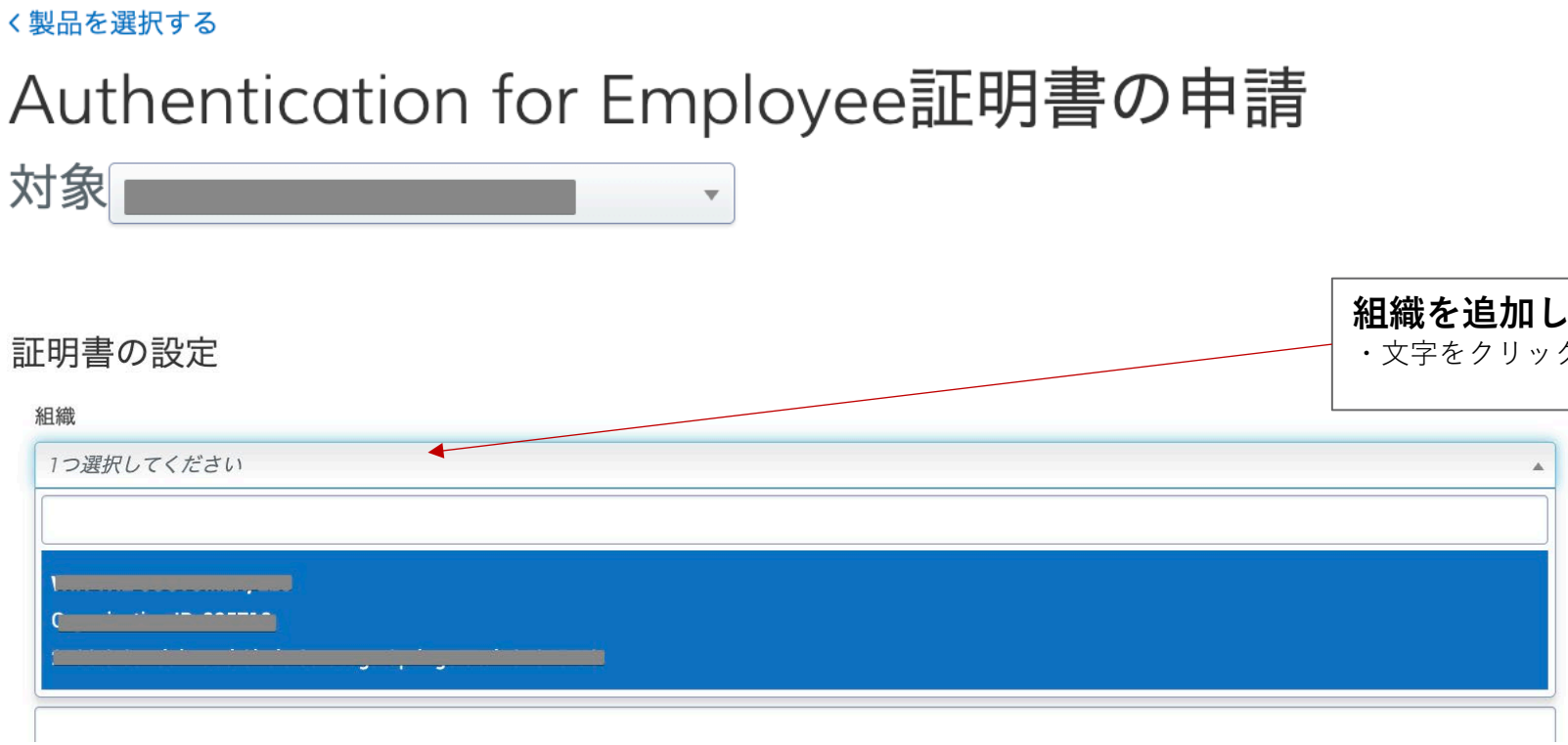
注：バウチャーをご利用の場合は、バウチャー券面に記載のURLからご申請ください。
[CertCentral]バウチャー(クーポン) を利用するうえでの注意点について
https://knowledge.digicert.com/jp/general-information/faq-vouchers

**証明書の申請情報ならびに組織申請**

左メニューより「**証明書の申請**」をクリックしてAuthentication for Employeeをお選びください

**その他のオーダー情報**

# Authentication for Employee 証明書の新規申請：証明書情報の入力




必須

**組織を追加します**

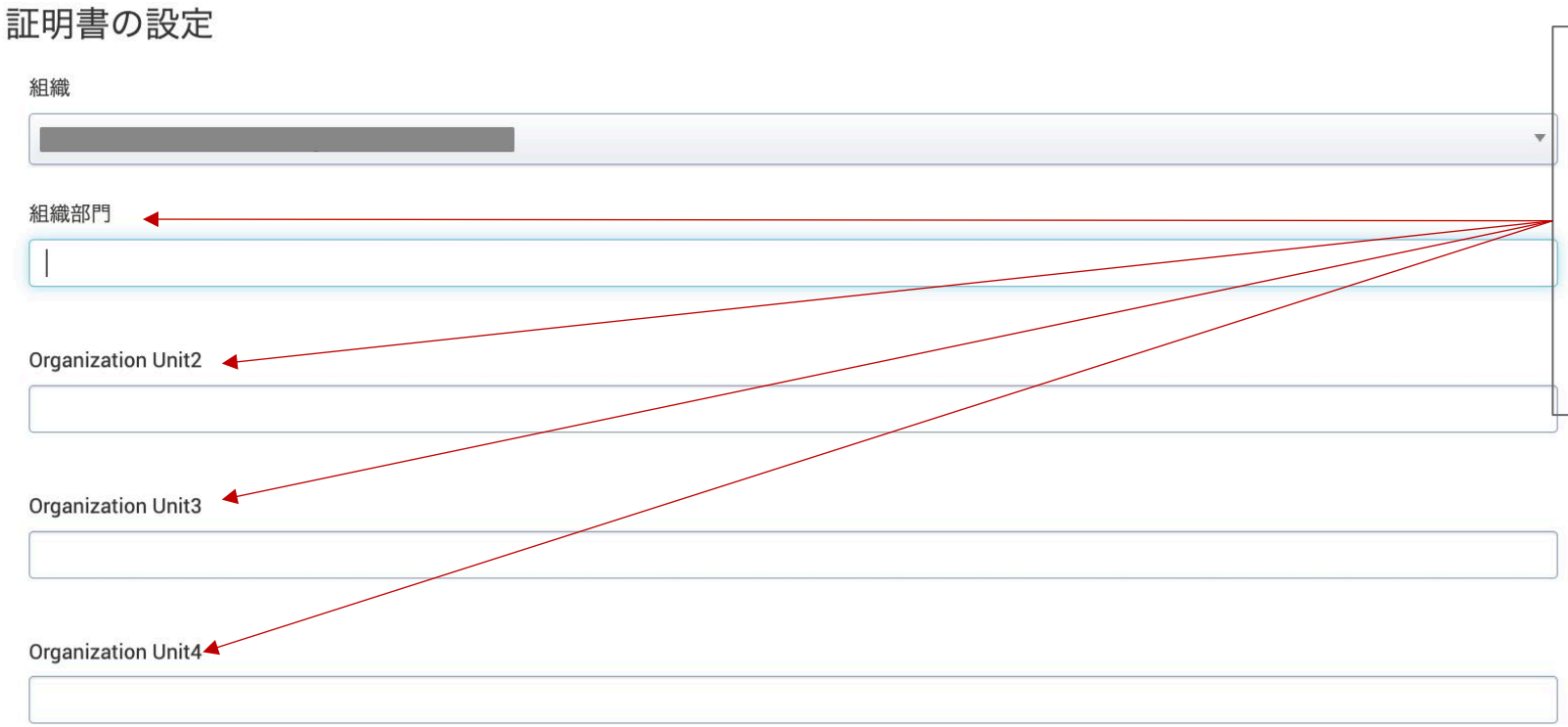
・文字をクリックして、組織を追加してください。

必須

**組織名の追加**

- ここに表示されるのはOV組織認証が完了している組織になりますので、希望の組織が表示されない場合、OV組織認証が完了していません。
- 申請前にOV組織認証を完了してください。（11ページをご参照ください）

# Authentication for Employee 証明書の新規申請：証明書情報の入力




**組織部門（OU）を追加します（オプション）**

・希望する情報を入力します

・最大で４つのOUフィールドを証明書に記載することができます。

・OUフィールドはPrintableStringまたはUTF8Stringのテキストを最大64Byte指定することができます。

# Authentication for Employee 証明書の新規申請：証明書情報の入力

必須

**証明書の署名アルゴリズム**
・sha256RSAまたはsha384WithRSAなどをご指定ください。

必須

**申請する証明書の有効期限**
・希望する有効期限を指定します、これにより価格が決定します。

# Authentication for Employee 証明書の新規申請：証明書情報の入力

**クライアント証明書発行メール**

・以下が申請画面に表示されている場合にはチェックしてください

クライアント証明書発行メールを受信します

☑ クライアント証明書発行メールをオンにします

必須

**証明書のサブジェクト情報の指定**

・名、姓のそれぞれに英字で氏名を入力してください。

必須

**証明書の発行処理のために使うメールアドレスの指定**

・メールアドレスを入力してください。
・このメールアドレスは証明書には記載しませんが、証明書取得プロセスで使用しますので、入力してください。

必須

**CSRの生成方法の選択**

・Authentication for Employeeでは、申請時にブラウザで鍵を生成しますので、「ブラウザからCSRを生成する」を選択してください。

# Secure Email for Business証明書の新規申請：支払い情報の指定

必須

**支払い情報**
・支払い情報を指定します。クレジットカードの場合、即時に課金します。

必須

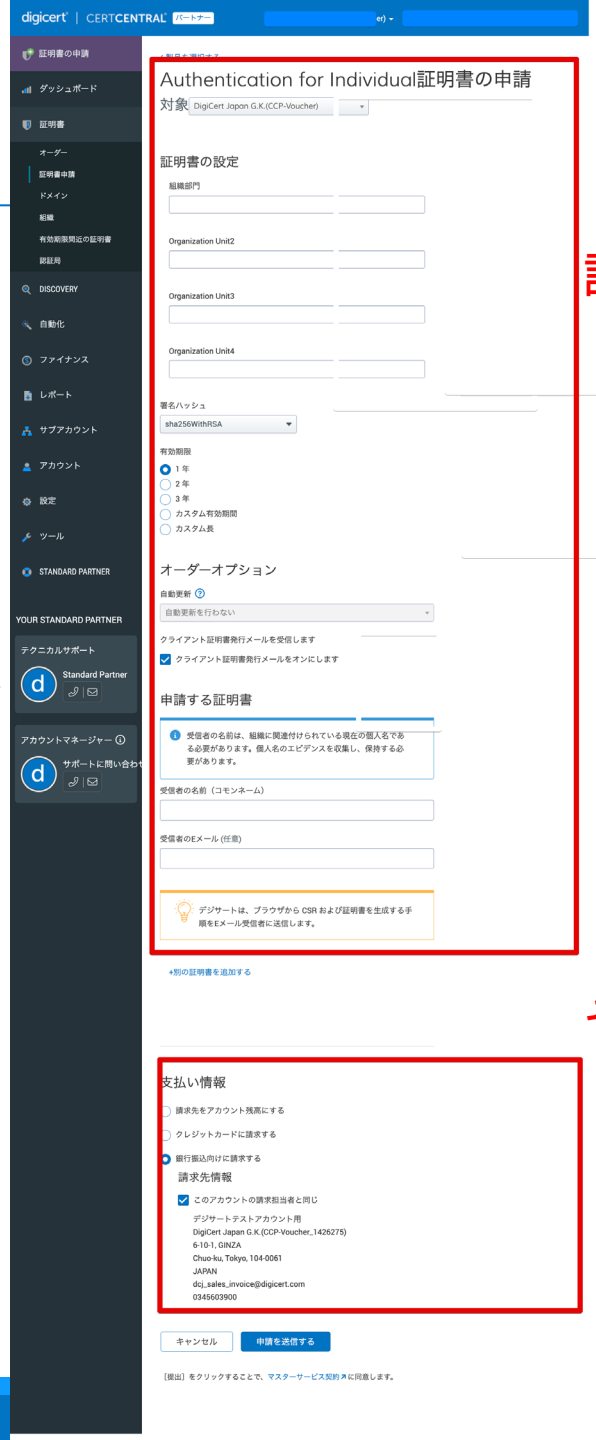
**申請完了**
・「申請を送信」ボタンを押下し申請を完了させてください。

# プラン/証明書の新規申請
# Authentication for Individual

# プラン/証明書の新規申請

Authentication for Individualを選択してください。

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

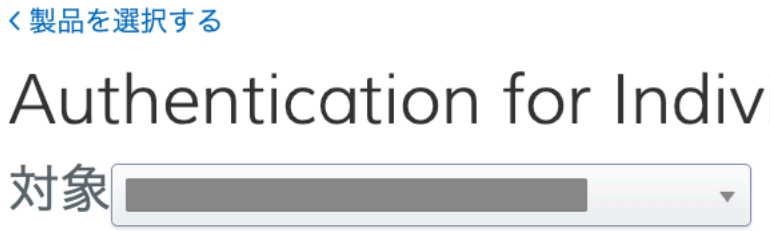



**証明書の申請情報**

左メニューより「**証明書の申請**」をクリックして Authentication for Individualをお選びください

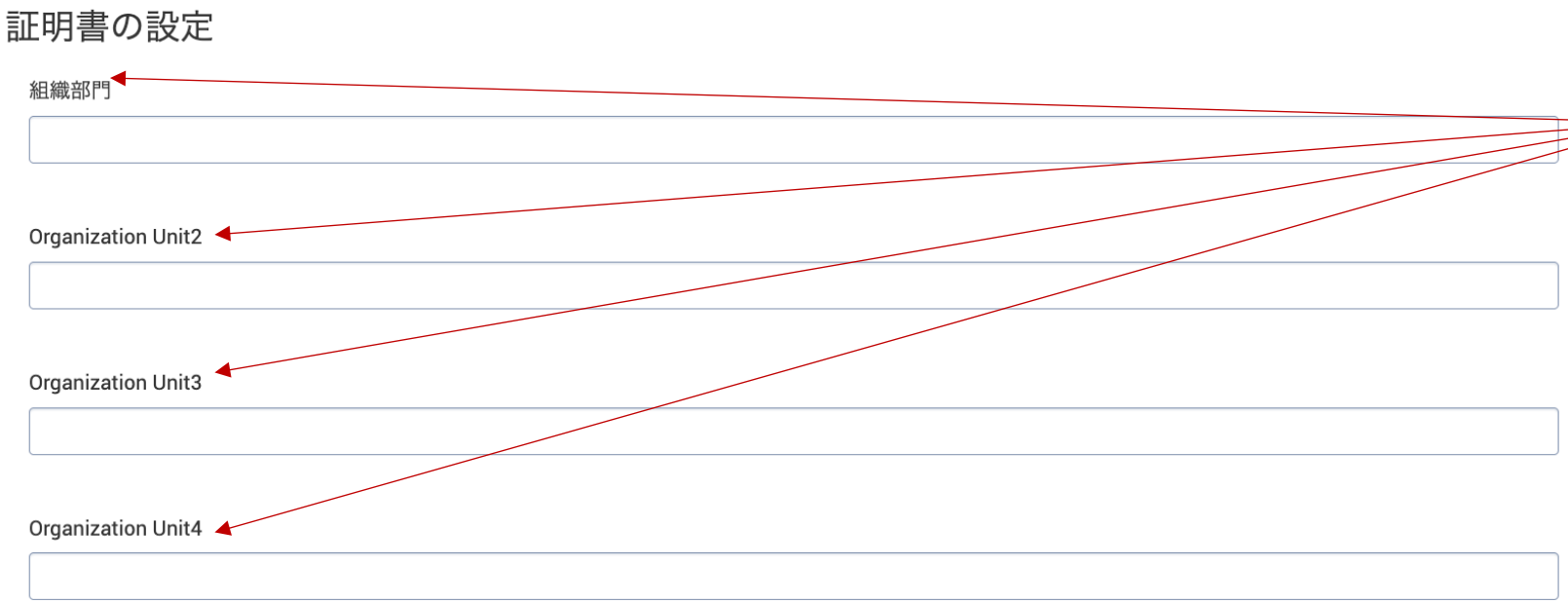
**その他のオーダー情報**

# Authentication for Individual 証明書の新規申請：証明書情報の入力




- 本証明書は組織情報を入力することができません。
- OV組織認証は不要です

# Authentication for Individual 証明書の新規申請：証明書情報の入力



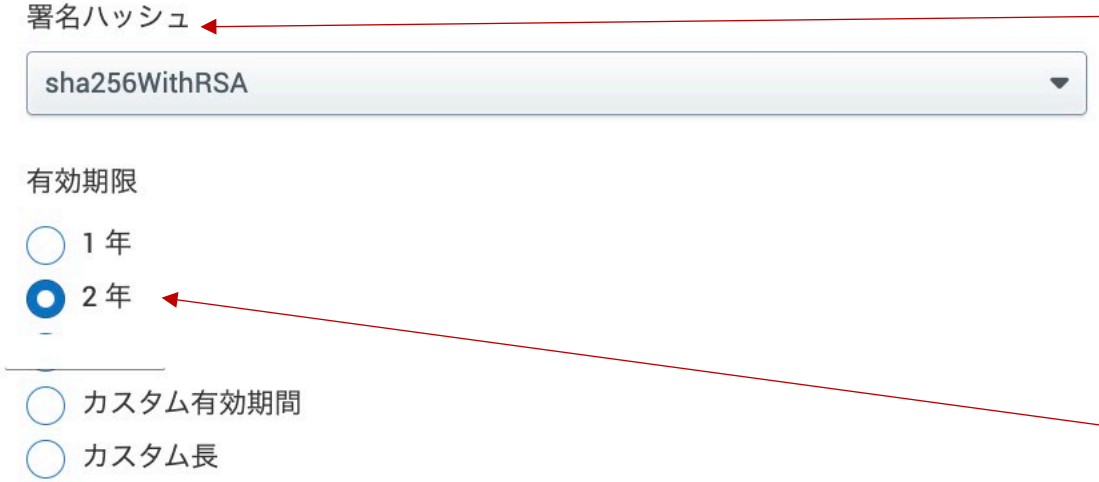

**組織部門（OU）を追加します（オプション）**

・希望する情報を入力します

・最大で４つのOUフィールドを証明書に記載することができます。

・OUフィールドはPrintableStringまたはUTF8Stringのテキストを最大64Byte指定することができます。

# Authentication for Individual 証明書の新規申請：証明書情報の入力




必須

**証明書の署名アルゴリズム**
・sha256RSAまたはsha384WithRSAなどをご指定ください。

必須

**申請する証明書の有効期限**
・希望する有効期限を指定します、これにより価格が決定します。

# Authentication for Individual 証明書の新規申請：証明書情報の入力

## クライアント証明書発行メール

・以下が申請画面に表示されている場合にはチェックしてください

クライアント証明書発行メールを受信します

☑ クライアント証明書発行メールをオンにします

必須

## 証明書のサブジェクト情報の指定

・名、姓のそれぞれに英字で氏名を入力してください。

必須

## 証明書の発行処理のために使うメールアドレスの指定

・メールアドレスを入力してください。
・このメールアドレスは証明書には記載しませんが、証明書取得プロセスで使用しますので、入力してください。

必須

## CSRの生成方法の選択

・Authentication for Individualでは、申請時にブラウザで鍵を生成しますので、「ブラウザからCSRを生成する」を選択してください。

# Authentication for Individual 証明書の新規申請：支払い情報の指定

必須

**支払い情報**
・支払い情報を指定します。クレジットカードの場合、即時に課金します。

必須

**申請完了**
・「申請を送信」ボタンを押下し申請を完了させてください。

# 証明書の取得

# 証明書の発行・取得

- 認証が完了した後メールで、証明書取得用のURLが送信されます
- 当該URLをクリックし、以下のように証明書を取得ください
  - クリックしたURLを開くブラウザ内で、秘密鍵を生成し、指定のパスワードでPKCS#12ファイルを生成します
  - 生成したPKCS#12ファイルをダブルクリックしてローカルの環境にインストールしてください
- 上記の処理は一度しかできません、一回クリックしたURLを再度クリックしても、証明書は発行できません

## メールを受信

| | |
|---|---|
| 件名 | デジサート Authentication for Employee 証明書の承認が完了しました |
| 送信元 | DigiCert <admin@digicert.com> |
| 本文<br>（抜粋） | **デジサート 個人用証明書（Authentication for Employee）が承認されました。**<br><br>**次のURLにアクセスし、お早めにデジサート 個人用証明書を取得してください：**<br><br>https://www.digicert.com/link/pid-install.php?token=**********xx8 |

- 上記のリンクをクリックしブラウザで開くことで、証明書の取得ができます

## ブラウザで証明書を取得

1. 証明書パスワード（12文字以上72文字以内、大文字小文字、数字、シンボル）を入力
   ※利用環境へインストールする際に必要となります。必ず忘れないようにしてください。
2. マスターサービス契約書に同意する（チェックを追加）
3. 「証明書を生成する」をクリック

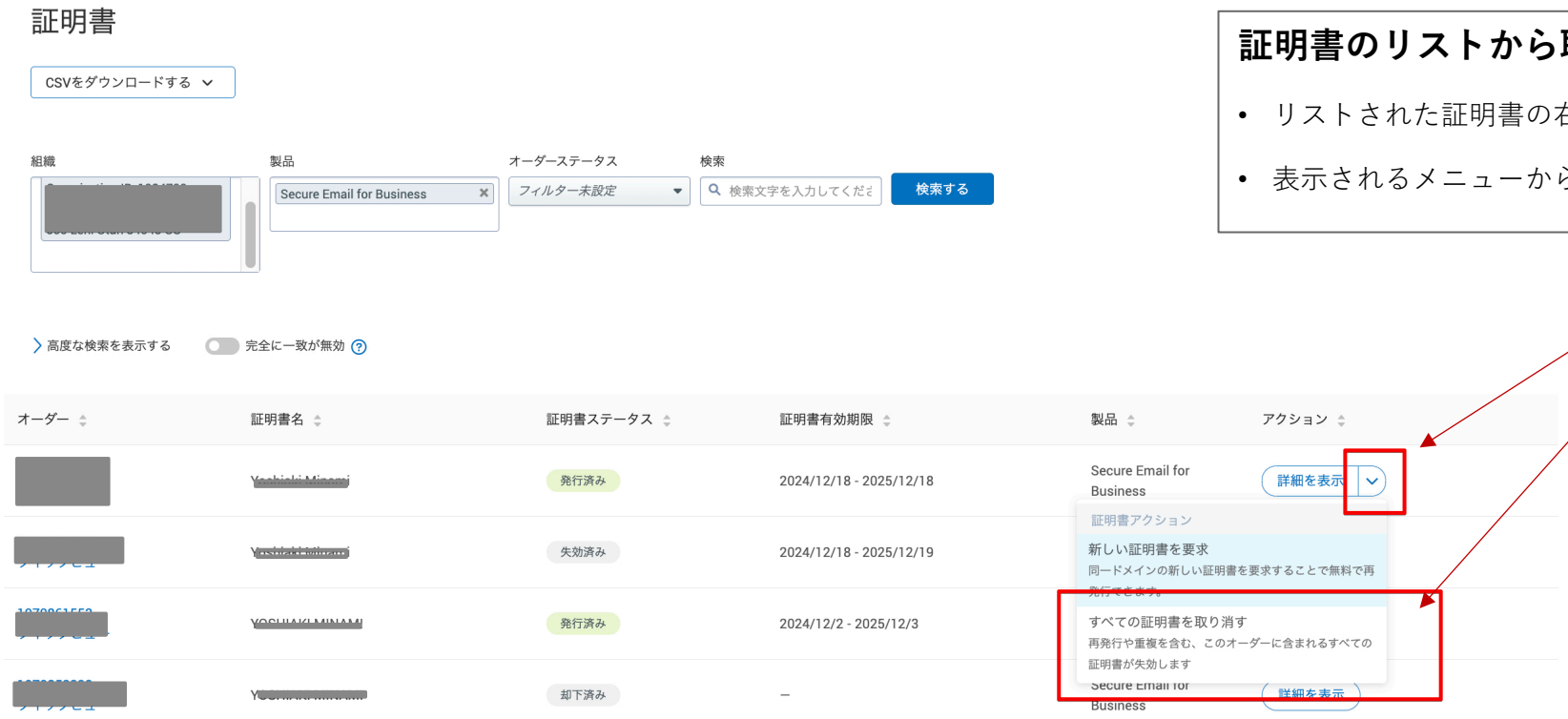
# 証明書のインストール

- 証明書および秘密鍵を含む証明書のPKCS#12ファイルが、ブラウザのダウンロードエリアにダウンロードされます
- PKCS#12ファイルをダブルクリックして証明書のインポートウィザードの指示にしたがってインポートを行います。当該ファイルのパスワードは入力画面で入力したパスワードになります。
- インポート後、発行通知メールが送信（添付ファイル付き：Zipファイル）が送信されますが、破棄いただいても問題ございません。
  - TrustedRoot.crt（ルート証明書）
  - DigiCertCA.crt（中間CA証明書）
  - sample_example_com.crt（発行された証明書）

# 証明書の取り消し

# 証明書の取り消し

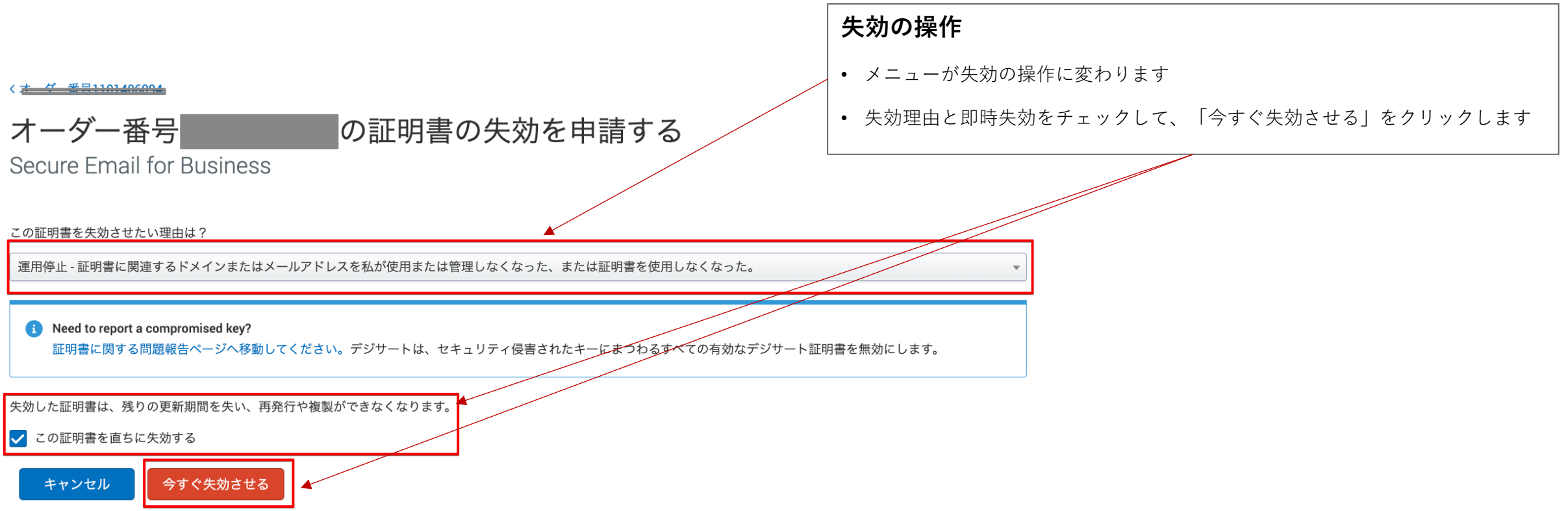
- テスト証明書の場合、発行日から30日以内に「必ず」以下の証明書の取り消しを行なってください
- 上記が行われない場合、証明書の課金を実施します
- 左のメニューから証明書を選択します




**証明書のリストから取り消し**

- リストされた証明書の右のメニューから「下矢印マーク」をクリックします
- 表示されるメニューから「すべての証明書を取り消す」を選択します

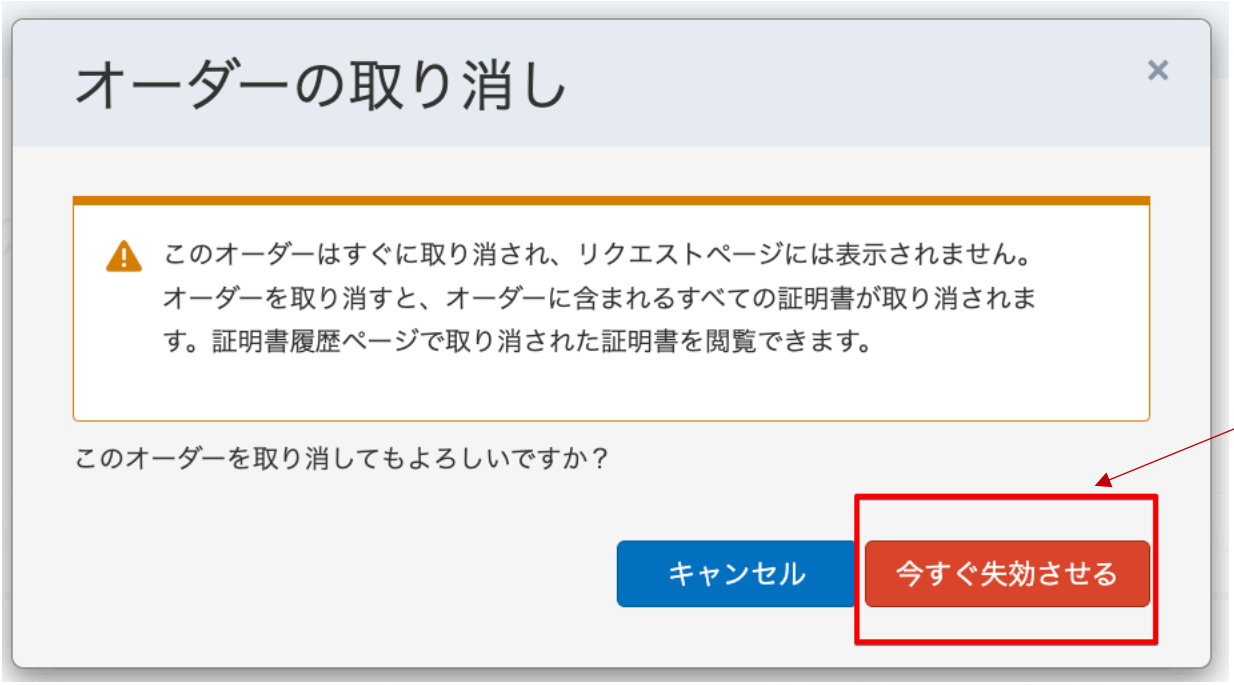
# 証明書の取り消し




**失効の操作**

- メニューが失効の操作に変わります
- 失効理由と即時失効をチェックして、「今すぐ失効させる」をクリックします

# 証明書の取り消し




**失効の操作**

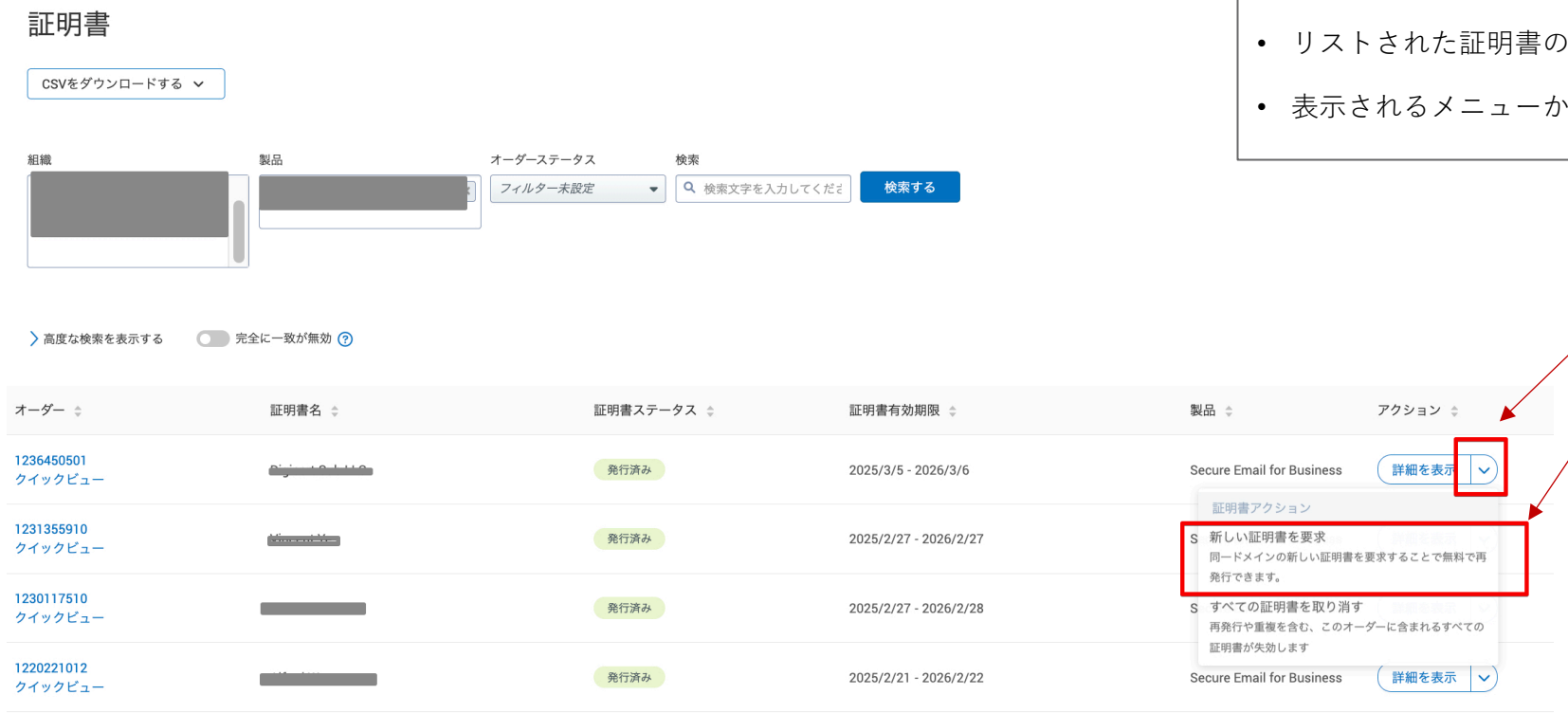
- 「今すぐ失効させる」をクリックします

- 次の画面で、証明書が失効したことを確認ください。

# 再発行申請、または証明書の更新

# 証明書の再発行、または更新

- 左のメニューから証明書を選択します
- 次のページからは新規の申請と同じ入力項目となります

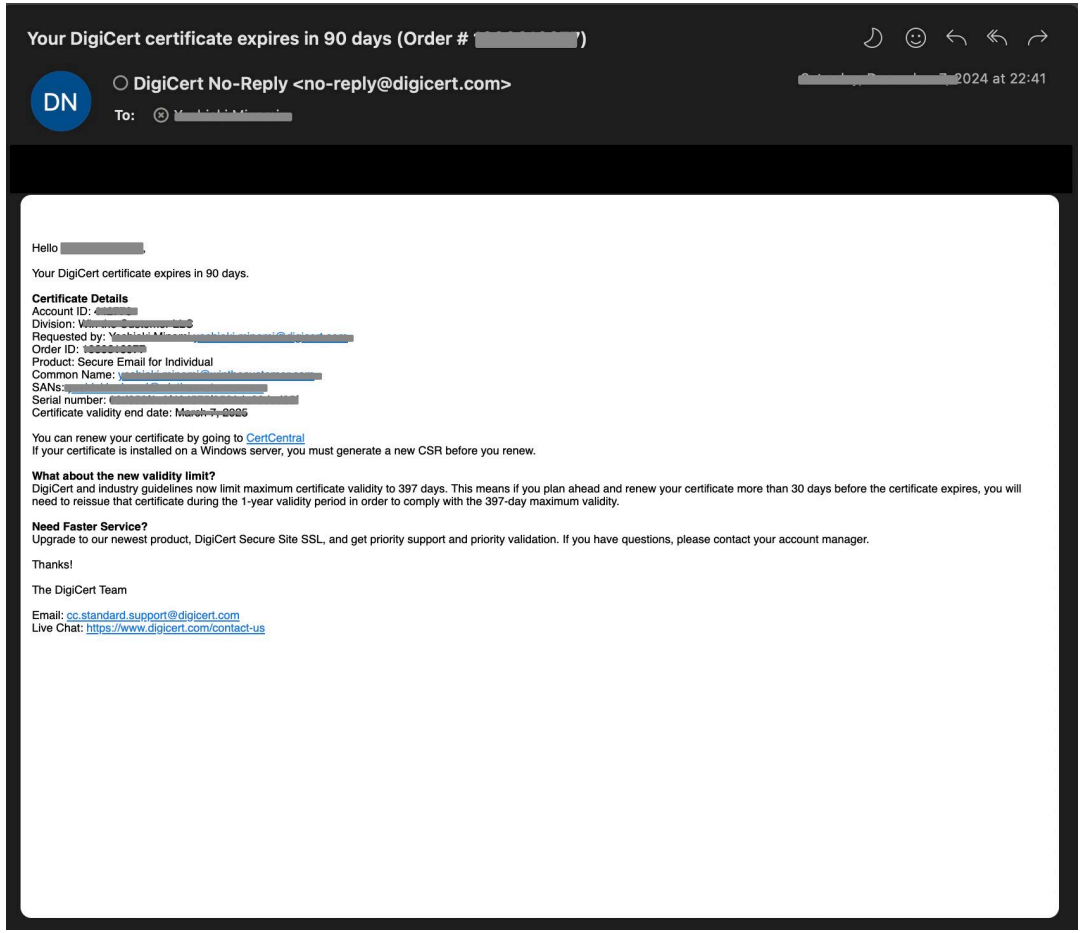



**証明書のリストから「新しい証明書を要求」を選択**

- リストされた証明書の右のメニューから「下矢印マーク」をクリックします
- 表示されるメニューから「新しい証明書を要求」を選択します

# 更新のお知らせ

# 更新のお知らせ


Your DigiCert certificate expires in 90 days (Order # [redacted])

DN

DigiCert No-Reply <no-reply@digicert.com>

To: [redacted]

[redacted] 2024 at 22:41

Hello [redacted].

Your DigiCert certificate expires in 90 days.

**Certificate Details**
Account ID: [redacted]
Division: [redacted]
Requested by: [redacted]
Order ID: [redacted]
Product: Secure Email for Individual
Common Name: [redacted]
SANs: [redacted]
Serial number: [redacted]
Certificate validity end date: March 7, 2025

You can renew your certificate by going to CertCentral
If your certificate is installed on a Windows server, you must generate a new CSR before you renew.

**What about the new validity limit?**
DigiCert and industry guidelines now limit maximum certificate validity to 397 days. This means if you plan ahead and renew your certificate more than 30 days before the certificate expires, you will need to reissue that certificate during the 1-year validity period in order to comply with the 397-day maximum validity.

**Need Faster Service?**
Upgrade to our newest product, DigiCert Secure Site SSL, and get priority support and priority validation. If you have questions, please contact your account manager.

Thanks!

The DigiCert Team

Email: cc.standard.support@digicert.com
Live Chat: https://www.digicert.com/contact-us

- 証明書の有効期限が近づくと、更新されていない場合、90、60、30、7、3日前、有効期限から7日後のそれぞれに有効期限が近づいていることをお知らせするメールが、申請時に使用したメールアドレスに送付されます

  参考サイト：[CertCentral] 更新案内メールについて
  https://knowledge.digicert.com/jp/general-information/configure-certificate-renewal-notifications

- CertCentralにログインをして、証明書の再発行、更新のページに記載の手順にて、新しい証明書を申請してください
- 申請時に組織認証が切れている場合には、合わせて組織認証の再申請が必要になります

digicert®

# 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

## DigiCert Documentation

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

## サポート窓口

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

**テクニカルサポート**
Email：cc.standard.support.jp@digicert.com
電話：03-4578-1368（自動音声ガイダンス2）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

**認証に関するお問い合わせ**
Email：standard.validation.jp@digicert.com
電話：03-4578-1368（自動音声ガイダンス1）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30