

ユーザ向け CertCentral簡易ガイド

Secure Email for Individual / Business対応版
2025年 8月 1日更新



目次

1. 申請前の準備 : [page 3](#)
2. S/MIME用の組織認証 : [page 10](#)
3. メールアドレスで使用するドメインの利用権の申請 (DCV) : [page 13](#)
4. プラン/証明書の新規申請
Secure Email for Business : [page 18](#)
5. プラン/証明書の新規申請
Secure Email for Individual : [page 25](#)
6. 証明書の取得、インストール : [page 31](#)
7. 証明書の取り消し : [page 34](#)
8. 再発行申請、または更新 : [page 38](#)
9. 更新のお知らせ : [page 40](#)

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



Secure Email for Individual
またはBusiness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 S/MIME証明書のインストール

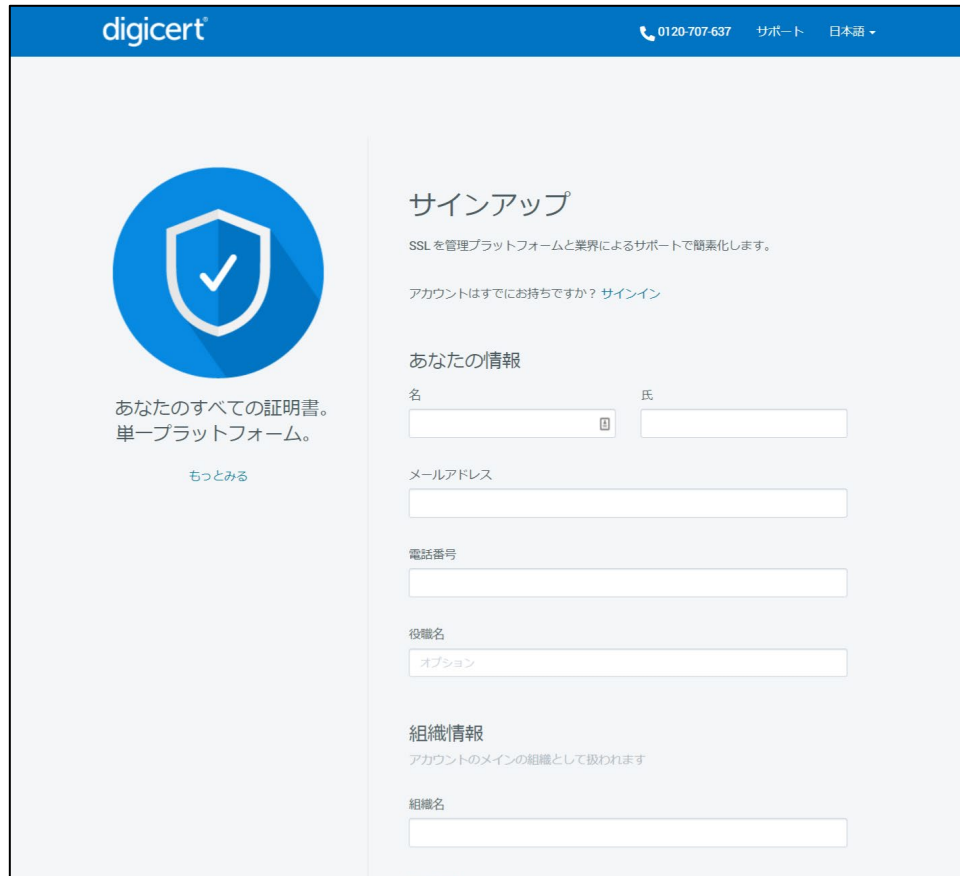
メール内の手順に従い、証明書を取得すると、証明書を含むPKCS #12ファイルを作成します。このファイルを利用環境にインストールしてください。S/MIME用として使う場合には、メーカーにもS/MIME証明書の設定を行なってください。

※ 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

- Secure Email for IndividualとSecure Email for Businessでは、証明書に記載される情報に差異があり、CA Browser フォーラムの定義する複数のS/MIME証明書の定義に合わせて、認証要件、発行可能範囲を適用いたします
 - **Secure Email for Individual**
 - 証明書のSubjectにはEmailアドレスのみを記載しますので、S/MIME用の組織認証は不要です
 - 認証は、メールアドレスへの到達性を持って認証としますので、メールアドレスで使用するドメインの利用権確認は不要です
 - 自組織でのドメインを管理していない場合（例：gmail.comのアドレスなど）には本S/MIME証明書のみが発行可能です
 - 後述する組織認証、ドメイン利用権確認の承認は不要で、そのまま証明書の申請に進んでください
 - **Secure Email for Business**
 - 組織内個人用の証明書になりますので以下の二つの認証が必要です
 - S/MIME用組織認証
 - メールアドレスで使用するドメインの利用権確認(DCV)
 - S/MIME用組織認証では、日本国内の組織であれば、登記が必須となり、未登記の組織への発行はできません
 - その他の理由でS/MIME用の組織認証ができない場合、本証明書の発行はできません

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

「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¤cy=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 Secure Email for ～の製品をご利用の場合、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

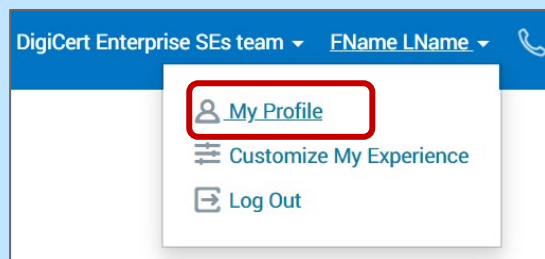
区分

設定方法

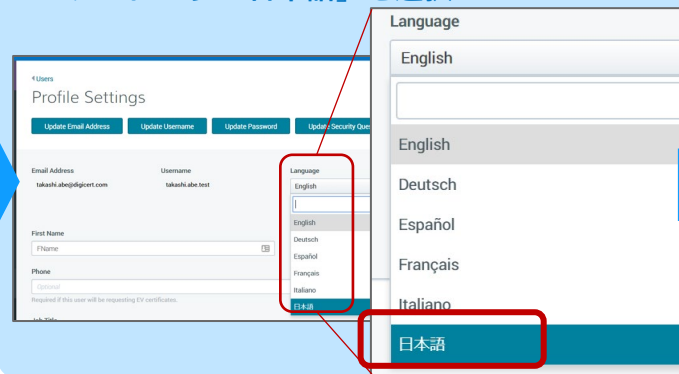
画面表示
言語

画面表示言語を日本語へ切り替える

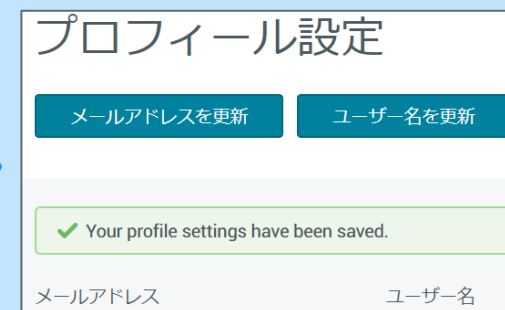
STEP 1: 画面右上部の「My Profile」から「Profile Setting」をクリック



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



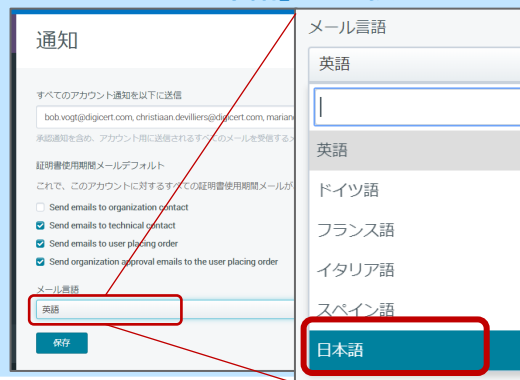
メール
言語

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

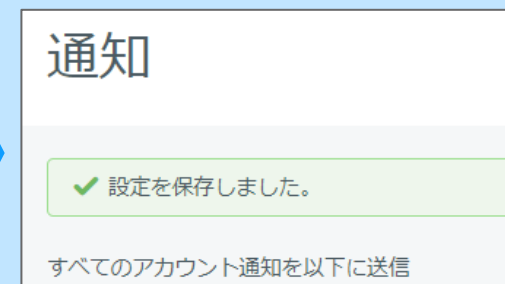
STEP 1: 画面左メニューの「設定」から「通知」をクリック



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



2025年7月追記）証明書のプロファイルの選択について

- Secure Email for Individual、ならびにSecure Email for Businessについて、2025年7月9日（日本時間）より、プロファイルの選択が必要となります。
- ご利用の目的に合わせて、以下のドロップダウンメニューよりプロファイルの選択をお願いいたします。どちらを選択すべきか不明な場合には、MultiPurposeをご選択してください

プロファイルの選択	
Strict（既定値）	PDFの署名にのみ使う場合にはこちらでも利用可能
MultiPurpose	PDFの署名ならびにWebサーバーにログインする場合にはこちらをお使いください。 独立行政法人医薬品医療機器総合機構様のゲートウェイに使用される際には、こちらをご選択ください

- Strictを選択した場合には、後述する個人認証のオプションは設定いたしません

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>

[DCV] ドメイン名の認証 (DCV:Domain Control Validation)について

<https://knowledge.digicert.com/jp/solution/dcv-ssl-smid-domain>

[CertCentral]二要素認証設定について

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

S/MIME用組織認証の申請

組織認証

- Secure Email for Individualの証明書発行では組織認証は不要です
- 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「SMIME」の記載があれば、S/MIME用の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

digicert® | CERTCENTRAL®

デジサートジャパン ▾ サンプル ▾ STANDARDサポート ⓘ (?)

証明書の申請

ダッシュボード

証明書

オーダー

証明書申請

ドメイン

組織

有効期限間近の証明書

認証局

DISCOVERY

ACME ディレクトリ URL

組織

新しい組織 CSVをダウンロードする ▾

ステータス 認証ステータス 検索

アクティブ フィルター未設定 🔍 検索文字を入力し 検索する

0 / 191 組織が選択されました | 一括アクション ▾

☐	組織番号 ▾	名前 ▲	ステータス ▾	認証	認証を保留中
☐	1-7	Ltd. Tokyo JP	アクティブ	OV, SMIME	-
☐		Ltd. Tokyo 104-6111 JP	アクティブ	-	SMIME

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SMIMEの項目「SMIME - SMIME Organization 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>

The screenshot displays the DigiCert CERTCENTRAL web interface. On the left is a dark sidebar with navigation links: 証明書申請, ダッシュボード, 証明書, オーダー, 証明書申請, ドメイン, 組織 (highlighted), 有効期限近い証明書, 認証局, DISCOVERY, 自動化, ファイナンス, アカウント, 設定, ツール, and STANDARDサポート. The main content area has a blue header with the DigiCert logo. Below the header, there's a section for '組織の詳細' (Organization Details) with fields for 組織ID, 正式名称, 住所, and 電話番号. To the right of these fields is a box for '申請責任者' (Applicant) with a search icon and a box for '技術担当者を追加する (オプション)' (Add technical contact (optional)). Below this is the '組織認証の申請' (Organization Validation Application) section, which contains a list of checkboxes: CS - Code Signing Organization Validation, EV CS - Code Signing Organization Extended Validation (EV CS), DS - Document Signing Validation, SMIME - SMIME Organization Validation (checked and highlighted with a red box), OV - Normal Organization Validation, and EV - Extended Organization Validation (EV). At the bottom of this section is a blue button labeled '認証を申請' (Apply for authentication).

メールアドレスで使用するドメインの利用権の申請
(DCV)

ドメイン利用権の確認 (DCV)

- Secure Email for Individualの証明書発行ではドメイン利用権の確認 (DCV)は不要です
- CertCentralにログイン後、左のメニューから「証明書」>「ドメイン」をクリックしてください
- 登録されているものがあれば、ドメインの一覧が表示されますので、ドメイン名をクリックしてください
- 登録されたものがない、または利用権が確認できてない場合には次ページのドメイン利用権の確認を申請してください

digicert | CERTCENTRAL

デジサートジャパン サンプル STANDARDサポート

ドメイン

新しいドメイン CSVをダウンロードする

ドメインステータス: アクティブ | 認証ステータス: フィルター未設定 | ドメイン認証方法: フィルター未設定 | 組織: Unfiltered | 検索: 検索文字を入力し 検索する

0 / 218 選択されているドメイン | 再認証のためにドメインを送信する | ドメインの削除

	ドメイン名	組織	追加日	DCV方式	認証ステータス	認証有効期間
☐	co.jp ドメイン ID:	Ltd. 組織ID: Tokyo JP	2025/1/16	申請承認メール(DCVメール)	認証済み	2026/2/17

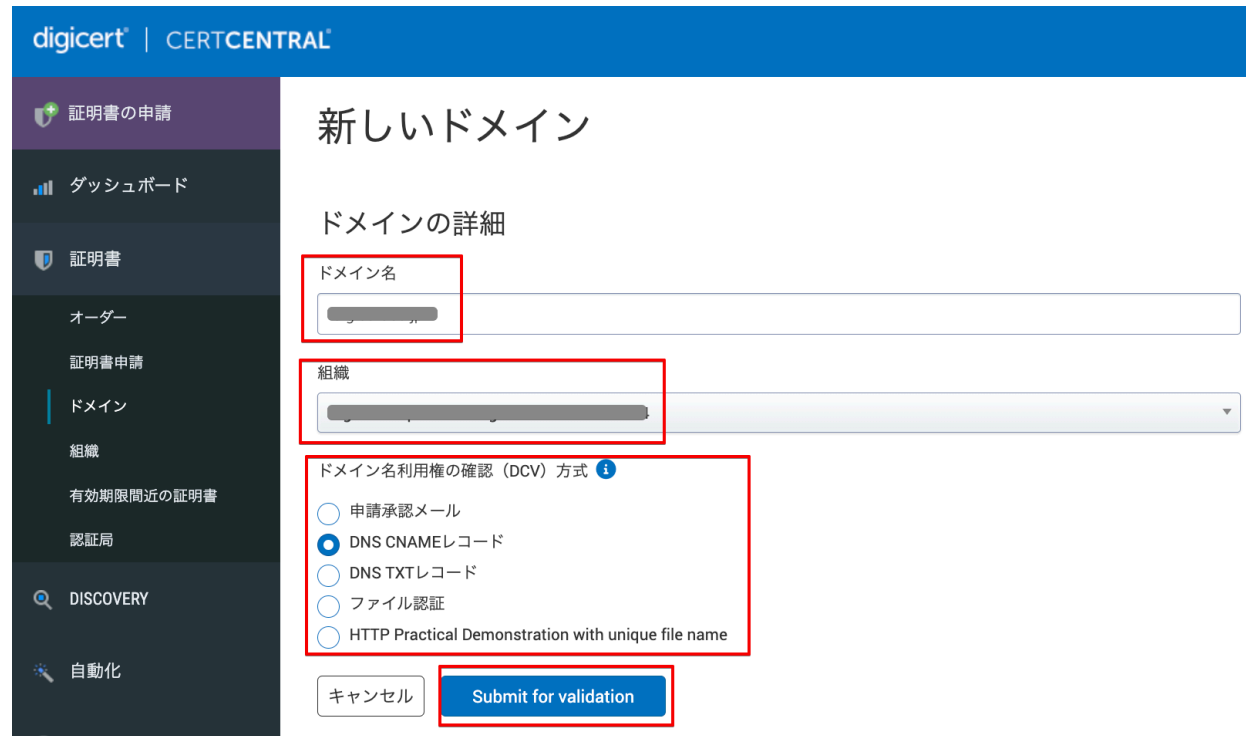
ドメイン利用権の申請（新規）

- ドメイン利用権の確認を新規に申請する場合、「新しいドメイン」をクリックしてください。
- ドメイン名を入力します
- 組織は、登録済みのものから選択できます
- ドメインの利用権の確認方法を指定します
- 申請承認メールを選択した場合は言語を「Japanese」を指定します
- 「Submit for validation(認証を申請)」をクリックして申請します
- 選択したDCV方式で承認をしてください

参考サイト：

[DCV] ドメイン名の認証 (DCV:Domain Control Validation)について

<https://knowledge.digicert.com/jp/solution/dcv-ssl-smid-domain>



ドメイン利用権の申請（既存の場合）

- ・ リストされたドメイン名をクリックします
- ・ 申請期間中であれば、申請内容が表示されます、DigiCertにご連絡いただければ、DCVへの対応の作業を実施ください
- ・ 申請期間が切れている場合には、右のような画面になりますので、改めて利用権の確認を実施する方法を指定
- ・ 「Submit for validation(認証を申請)」をクリックして申請します
- ・ 選択したDCV方式で承認をしてください

参考サイト：

[DCV] ドメイン名の認証 (DCV:Domain Control Validation)について

<https://knowledge.digicert.com/jp/solution/dcv-ssl-smid-domain>

The screenshot shows the DigiCert domain management interface. At the top, there is a dropdown menu labeled 'ドメインのアクション' (Domain Actions) with a downward arrow. Below this, there is a table with two columns: 'ドメイン認証ステータス' (Domain Authentication Status) and 'DCV方式' (DCV Method). The table is currently empty. Below the table, there is a section titled 'ドメインの詳細' (Domain Details). This section contains the following information: 'ドメイン ID' (Domain ID) is 5000000000000000, 'ドメイン名' (Domain Name) is example.com, '組織名' (Organization Name) is Example Organization, and '追加日' (Add Date) is 2025/1/3. Below this, there is a section titled 'ドメインロック' (Domain Lock). This section contains a toggle switch labeled '無効' (Invalid) and a note: 'ドメインロック機能を有効にすると、CertCentralアカウントユーザのみがドメインを使用できるようになります。これを有効にする場合、DNS CAA リソースレコードを追加または修正する必要があります。' (When you enable the domain lock feature, only CertCentral account users can use the domain. When you enable this, you may need to add or modify DNS CAA resource records.) Below this, there is a section titled 'ドメイン名利用権の確認 (DCV) 方式' (Domain Name Usage Confirmation (DCV) Method). This section contains five radio buttons: 'Verification Email', 'DNS CNAME Record' (selected), 'DNS TXT Record', 'HTTP Practical Demonstration', and 'HTTP Practical Demonstration with unique file name'. Below this, there are two buttons: 'キャンセル' (Cancel) and '認証を申請' (Apply for Authentication).

ドメインの利用権の確認

- ・ご申請後、ご連絡を頂きましたらご申請内容に応じて認証プロセスを開始します
- ・認証のひとつである「**ドメイン名利用権確認(DCV)※**」は、ご申請時に選択した内容にそって手続きをすすめ、認証を完了してください

※S/MIMEのメールアドレスで使用するドメインについて、証明書の申請者または申請団体が証明書を発行する対象のドメイン名に対する所有権／管理権限を持つことを確認するためのプロセス

CertCentralでご選択可能なDCV方式

DCV方式	内容	補足
メール 認証	規定のメールアドレス宛に送信されるDCVメールをドメイン名所有者が受信のうえ承認操作をいただくことでドメイン名利用権を確認する方式です。	宛先：「規定ホスト名@確認対象のドメイン名」で構成されるメールアドレス、またはDNS TXTに指定したメールアドレス
ファイル 認証	CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをインターネット経由でアクセス可能なウェブサーバ上の規定の場所にアップロードしていただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。	設置場所： http://<確認対象のドメイン名>/.well-known/pki-validation/fileauth.txt
DNS TXT 認証	CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをDNS TXTリソースレコードとして登録・公開していただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。	設置例： <確認対象のドメイン名> TXT <認証トークン>
DNS CNAME 認証	CertCentralの画面またはAPIを通じて弊社が提供するランダムな認証トークンをDNS CNAMEリソースレコードとして登録・公開していただき、弊社がこれを確認することによりドメイン名利用権を確認する方式です。	設置例： <認証トークン>.<確認対象のドメイン名> CNAME dcv.digicert.com

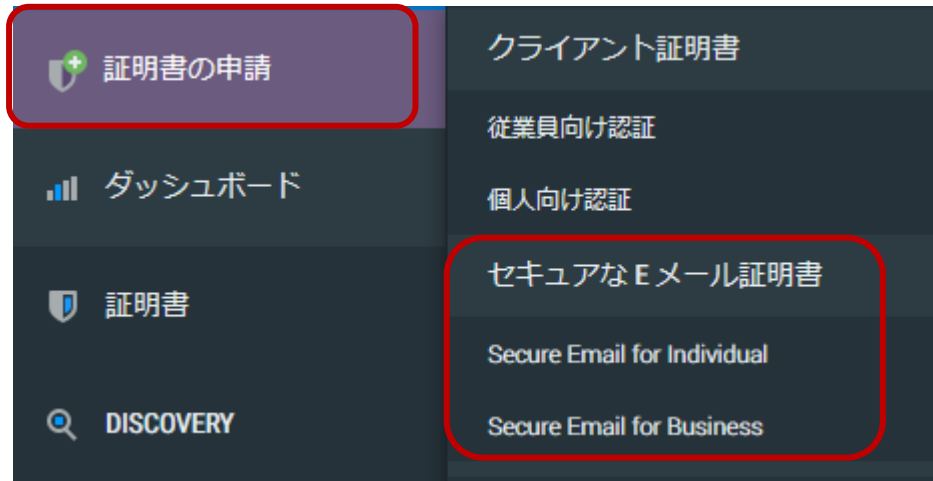
参考サイト：

[DCV] ドメイン名の認証 (DCV:Domain Control Validation)について

<https://knowledge.digicert.com/jp/solution/dcv-ssl-smid-domain>

プラン/証明書の新規申請
Secure Email for Business

プラン/証明書の新規申請



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>

The screenshot shows the 'Secure Email for Business' application page. The page is titled 'Secure Email for Business 証明書を申請する' and '対象: DigiCert Japan G.K.'. It includes sections for 'プロフィールオプション' (Profile Options), '証明書の有効期限' (Certificate Validity Period), '組織' (Organization), 'CSRを追加' (Add CSR), '証明書の詳細' (Certificate Details), and '支払い情報' (Payment Information). The '支払い情報' section is highlighted with a red box, showing options for payment method and billing information.

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
Secure Email for
Businessをお選びくだ
さい

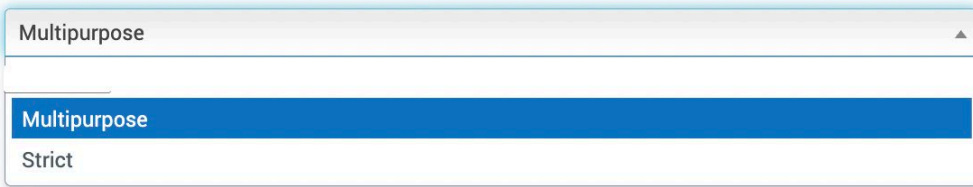
その他のオーダー情報

Secure Email for Business証明書の新規申請：証明書情報の入力

Secure Email for Business証明書を申請する

対象： 

プロフィールオプション 



A dropdown menu with a light blue header and a white body. The header contains the text "Multipurpose" and a small upward-pointing triangle. The body contains two options: "Multipurpose" (highlighted in blue) and "Strict".

 2 年

証明書の有効期限 

☐ 1 年

☒ 2 年

自動更新 

☐ 有効期限日の30日前にオーダーを自動更新する

申請する証明書のプロフィールの選択

- ・ StrictかMultiPurposeを選択します。
- ・ どちらを選択するか不明な場合にはMultiPurposeを選択してください。

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。

必須

Secure Email for Business 証明書の新規申請：証明書情報の入力

組織



組織を追加します

・アイコンをクリックして、組織を追加してください。

必須

A screenshot of a dialog box titled '組織を追加する' (Add Organization). It contains the question 'どの組織名を証明書に表示させますか？' (Which organization name do you want to display on the certificate?). There are two radio buttons: '既存の組織' (Existing Organization) and '新しい組織' (New Organization). Under '既存の組織', there is a checkbox '未認証の組織 ? を非表示にする' (Hide unauthenticated organizations ?) and a list of organization names with a corresponding icon. A red arrow points from the '未認証の組織 ? を非表示にする' checkbox to the '組織名の追加' (Add Organization Name) instruction box. Another red arrow points from the '新しい組織' radio button to the '組織名の追加' instruction box. At the bottom, there are 'キャンセル' (Cancel) and '追加する' (Add) buttons.

組織名の追加

・すでに登録している（既定値では未認証のものを含む）組織名から選択するか、新しい組織名を登録して追加することができます

組織の認証が終了するまでは証明書は発行されません。

必須

Secure Email for Business 証明書の新規申請：証明書情報の入力

CSR を追加 ②

CSR に関するサポートが必要ですか？ [?](#)

✓ ブラウザから CSR を生成する

← CSR を持っています

💡 CSR の追加をしてください。オーダーに CSR がいない場合、デジサートは、ブラウザで CSR および証明書を生成する手順をEメール受信者に送信します。

証明書の詳細

コモンネーム

Eメール

名前

受信者の名前またはEメールアドレスを追加

ⓘ 受信者の名前は、組織に関連付けられている現在の個人名である必要があります。
個人名のエビデンスを収集し、保持する必要があります。

受信者の名前 ←

名

姓

受信者のEメールアドレス

自組織で所有／管理されているドメインのEメールアドレスのみを含めてください。

追加のEメールアドレス (オプション) ←

...

m



追加する

証明書のコモンネームに表示したい受信者のEメールアドレスを入力またはドラッグしてください。

CSRの生成方法を指定します

・ 個人用証明書であるので、ブラウザでCSRを生成するを選択してください。

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

証明書のサブジェクト情報の指定

・ メールアドレスを入力して、「追加」ボタンをクリックしてください。この指定のメールアドレスのドメインについて、ドメイン利用権が確認できている必要があります。

必須

Secure Email for Business 証明書の新規申請：追加オプション

追加証明書オプション

証明書キーサイズ ②

RSA 2048

生成する鍵の長さを指定します

・長く利用される証明書の場合、RSAは3072bit以上を推奨します

必須

証明書の使用

複数目的使用 - Eメールの署名と暗号化

追加の証明書使用目的

☐ 否認防止

☐ データの暗号化

☒ 個人認証

証明書の使用（目的）を指定します

・目的に合わせて選択します、不明な場合には「複数目的使用-Eメールの署名と暗号化」を選択し、「個人認証（ClientAuth）」をチェックしてください

必須

☐ Eメール署名のみ

☐ Eメール暗号化のみ

中間CAおよびRoot CAの指定

・PDFに署名をする場合や厚生労働省のオンラインで利用される場合は申請の際、「[DigiCert G1 SMIME RSA4096 SHA384 2025 CA1 \(SHA2-384\) > DigiCert Global Root CA \(SHA1\)](#)」であることを確認ください。

※ドロップダウンリストに表示されない場合は[テクニカルサポート](#)までメールでご連絡ください。

必須

中間チェーン。[中間CA] > [ルートCA] ②

DigiCert Assured G2 SMIME RSA4096 SHA384 2024 CA1 (SHA2-384) > DigiCert Assured ID Root G2 (SHA2-256)

中間チェーン。[中間CA] > [ルートCA] ②

DigiCert G1 SMIME RSA4096 SHA384 2025 CA1 (SHA2-384) > DigiCert Global Root CA (SHA1)

署名ハッシュ

sha256WithRSA

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

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

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

☒ このアカウントの請求担当者と同じ



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。

必須

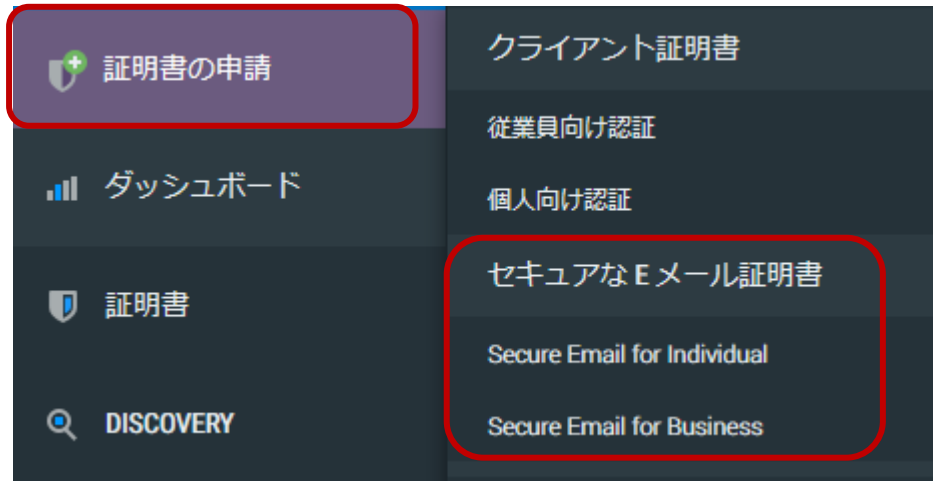
[提出] をクリックすることで、[マスターサービス契約](#) に同意します。

キャンセル

申請を送信

プラン/証明書の新規申請
Secure Email for Individual

プラン/証明書の新規申請



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>

digicert | CERTCENTRAL

証明書申請

ダッシュボード

証明書

オーダー

証明書申請

ドメイン

組織

有効期限間近の証明書

認証局

DISCOVERY

自動化

ファイナンス

アカウント

設定

ツール

STANDARDサポート

Secure Email for Individual証明書を申請する
対象：[]

プロフィールオプション ⓘ

Sprint

証明書の有効期限

1年

2年

自動更新 ⓘ

有効期限日の30日前にオーダーを自動更新する

CSRを追加 ⓘ
CSRに関するサポートが必要ですか? ⓘ

ブラウザからCSRを生成する

✓ CSRを持っています

安全な鍵を使用するため、証明書は長さ少なくとも2048ビットの鍵を使用する必要があります。
サポートされているアルゴリズムとキーの長さ
↓
CSRをアップロードするか、ここにCSRを貼り付けてください。

Eメール証明書

コンモネーム（Eメール）

追加する

追加の受信者Eメールアドレス（複数可）

追加する

証明書のコンモネームに表示したい受信者のメールアドレスを入力またはドラッグしてください。

> 追加証明書オプション

> その他のオーダーオプション

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

☒ このアカウントの請求担当者と同じ

Yoshiaki Minami
Digicert Japan G.K.
郵便 6-1 0-1
中央区 東京都 104-0001
JAPAN
yoshiaki.minami@digicert.com
818091879002

[提出] をクリックすることで、マスターサービス契約 A に同意します。

キャンセル

申請を送信

トランザクションサマリー
製品
Secure Email for Individual
有効期限
2年
申請コスト
• 基本価格:
¥18,800 (JPY)
見込み税額:
¥1,880 (JPY)
合計
¥20,680 (JPY)

1

d

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
Secure Email for Individual
をお選びください

その他のオーダー情報

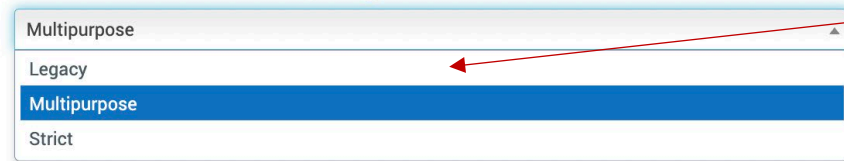
Secure Email for Individual 証明書の新規申請：証明書情報の入力

必須

Secure Email for Individual証明書を申請する

対象： 

プロフィールオプション 



☒ 2年

自動更新 

☐ 有効期限日の30日前にオーダーを自動更新する

申請する証明書のプロフィールの選択

- ・ StrictかMultiPurposeを選択します。
- ・ どちらを選択するか不明な場合にはMultiPurposeを選択してください。

必須

証明書の有効期限 

☐ 1年

☒ 2年

自動更新 

☐ 有効期限日の30日前にオーダーを自動更新する

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。

Secure Email for Individual 証明書の新規申請：証明書情報の入力

CSR を追加 ?

CSR に関するサポートが必要ですか？

✓ ブラウザから CSR を生成する

CSR を持っています



CSR の追加をしてください。オーダーに CSR がない場合、デジサートは、ブラウザで CSR および証明書を生成する手順をEメール受信者に送信します。

CSRの生成方法を指定します

・ 個人用証明書であるので、ブラウザでCSRを生成するを選択してください。

必須

Eメール証明書

コモンネーム (Eメール)

t.com

追加の受信者Eメールアドレス (複数可)

追加する

証明書のコモンネームに表示したい受信者のEメールアドレスを入力またはドラッグしてください。

証明書のサブジェクト情報の指定

・ メールアドレスを入力して、「追加」ボタンをクリックしてください。この指定のメールアドレスのドメインについて、ドメイン利用権が確認できている必要があります。

必須

Secure Email for Individual 証明書の新規申請：追加オプション

追加証明書オプション

証明書キーサイズ ?

RSA 2048

証明書の使用

複数目的使用 - Eメールの署名と暗号化

追加の証明書使用目的

☐ 否認防止

☐ データの暗号化

☒ 個人認証

☐ Eメール署名のみ

☐ Eメール暗号化のみ

中間チェーン。[中間CA] > [ルートCA] ?

DigiCert Assured G2 SMIME RSA4096 SHA384 2024 CA1 (SHA2-384) > DigiCert Assured ID Root G2 (SHA2-256)

署名ハッシュ

sha256WithRSA

生成する鍵の長さを指定します

・長く利用される証明書の場合、RSAは3072bit以上を推奨します

必須

証明書の使用（目的）を指定します

・目的に合わせて選択します、不明な場合には「複数目的使用-Eメールの署名と暗号化」を選択し、「個人認証（ClientAuth）」をチェックしてください

必須

中間CAおよびRoot CAの指定

・PDFに署名をする場合は申請の際、「[DigiCert G1 SMIME RSA4096 SHA384 2025 CA1\(SHA2-384\) > DigiCert Global Root CA \(SHA1\)](#)」であることを確認ください。

※ドロップダウンリストに上記が表示されない場合には[テクニカルサポート](#)までメールでご連絡ください。

必須

中間チェーン。[中間CA] > [ルートCA] ?

DigiCert G1 SMIME RSA4096 SHA384 2025 CA1 (SHA2-384) > DigiCert Global Root CA (SHA1)

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

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

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

☒ このアカウントの請求担当者と同じ



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。

必須

「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。

キャンセル

申請を送信

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ファイルを作成します
 - 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

Create Your DigiCert Secure Email for Business Certificate

送信元

DigiCert <admin@digicert.com>

本文

(抜粋)

Create your DigiCert Personal ID Certificate now by going to:

https://www.digicert.com/link/pid-install.php?token=cctzgkppy7*****

Thank you

DigiCert Team

- 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

証明書の生成 デジサート

技術的なサポートや修正については、管理者にご連絡ください。

① お持ちの Secure Email for Business 証明書の有効期限は発行日から 1 年です。この証明書を生成するか、組織管理者に連絡して新しい電子メールを要求する期限は、[] までです。

デジサートの Secure Email for Business 証明書詳細

名前: []

Eメールアドレス: []

組織: []

証明書パスワード:

12 to 72 characters long and must contain 3 of the following: lowercase letter, uppercase letter, number, and symbol.

パスワードの確認:

☐ 次の文書を読み、内容に同意します マスターサービス契約

証明書を生成する

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。
- S/MIME証明書として、メーカーに設定をする場合には、メーカーの設定画面から証明書を設定してください
- 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

CSVをダウンロードする ▼

組織  製品 オークラスステータス 検索 検索する

> 高度な検索を表示する ☐ 完全に一致が無効 

オーダー	証明書名	証明書ステータス	証明書有効期限	製品	アクション
	Yoshiaki Minami	発行済み	2024/12/18 - 2025/12/18	Secure Email for Business	詳細を表示 
	Yoshiaki Minami	失効済み	2024/12/18 - 2025/12/19		
1078061552 	YOSHIAKI MINAMI	発行済み	2024/12/2 - 2025/12/3		
1078060000 	Yoshimasa Minami	却下済み	-		

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消す」を選択します

証明書アクション

新しい証明書を要求
同一ドメインの新しい証明書を要求することで無料で再発行できます。

すべての証明書を取消す
再発行や重複を含む、このオーダーに含まれるすべての証明書が失効します

Secure Email for Business

証明書の取り消し

< オーダー番号1101406004

オーダー番号 [] の証明書の失効を申請する Secure Email for Business

この証明書を失効させたい理由は？

運用停止 - 証明書に関連するドメインまたはメールアドレスを私が使用または管理しなくなった、または証明書を使用しなくなった。



Need to report a compromised key?

証明書に関する問題報告ページへ移動してください。デジサートは、セキュリティ侵害されたキーにまつわるすべての有効なデジサート証明書を無効にします。

失効した証明書は、残りの更新期間を失い、再発行や複製ができなくなります。

☒ この証明書を直ちに失効する

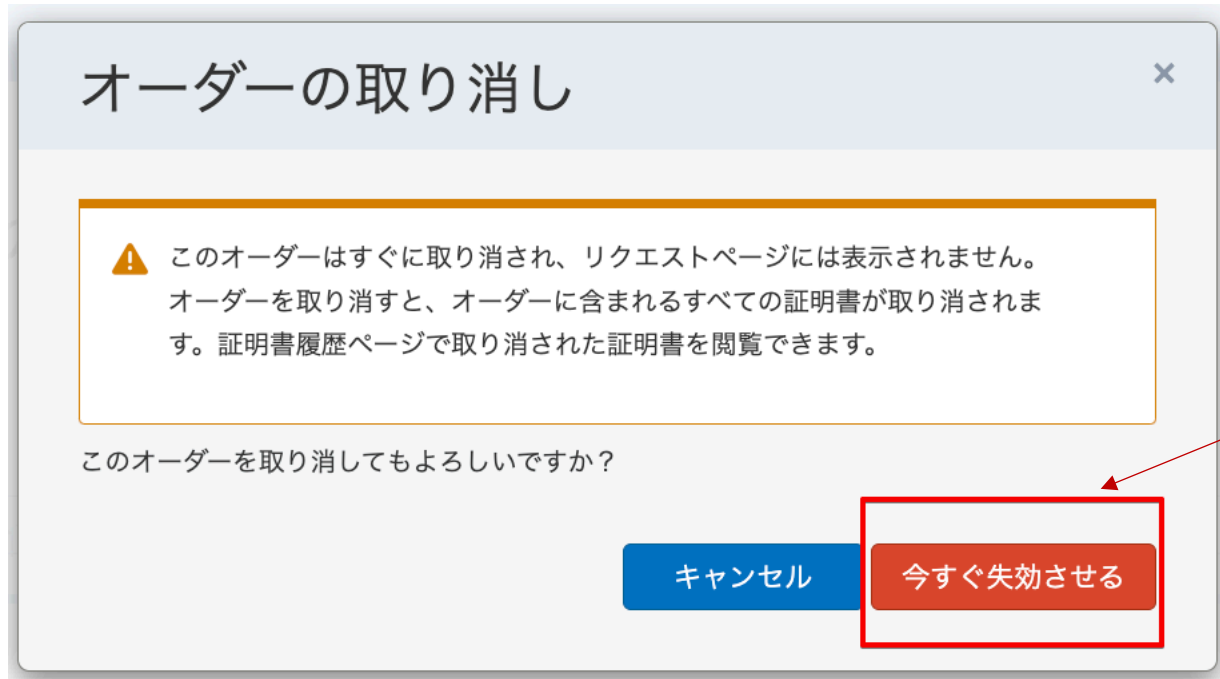
キャンセル

今すぐ失効させる

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
- 証明書の再発行において、証明書記載事項の変更は、初回証明書発行後30日以内のみサポートいたします

証明書

CSVをダウンロードする ▼

組織 製品 オーダーステータス 検索

フィルター未設定

> 高度な検索を表示する ☐ 完全に一致が無効 ☐

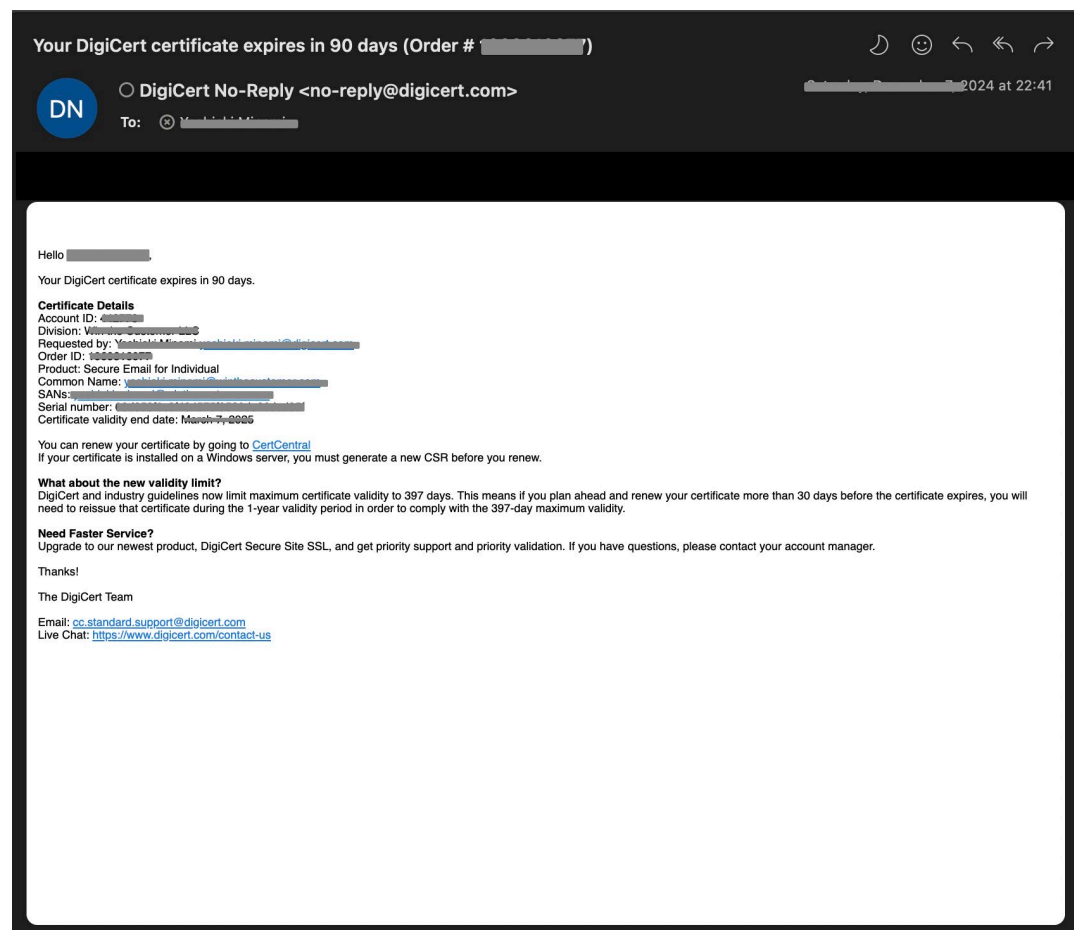
オーダー	証明書名	証明書ステータス	証明書有効期限	製品	アクション
1236450501 クイックビュー		発行済み	2025/3/5 - 2026/3/6	Secure Email for Business	詳細を表示
1231355910 クイックビュー		発行済み	2025/2/27 - 2026/2/27	証明書アクション	詳細を表示
1230117510 クイックビュー		発行済み	2025/2/27 - 2026/2/28	S 新しい証明書を要求 同一ドメインの新しい証明書を要求することで無料で再発行できます。	詳細を表示
1220221012 クイックビュー		発行済み	2025/2/21 - 2026/2/22	S すべての証明書を取消 再発行や重複を含む、このオーダーに含まれるすべての証明書が失効します	詳細を表示

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



- 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
- 申請時に組織認証およびDCVの有効期限が切れている場合には、合わせて組織認証およびDCVの再申請が必要になります



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