

---

# ユーザ向け CertCentral Secure Mail ID 簡易ガイド

Secure Email for Organization 対応版

2025年10月24日更新



# 目次

1. 申請前の準備 : [page 3](#)
2. 事前認証：S/MIME用 組織認証 : [page 9](#)
3. 事前認証：ドメインの利用権確認（DCV） : [page 12](#)
4. Secure Mail IDの新規申請 : [page 17](#)
5. Secure Mail IDの更新申請 : [page 23](#)
6. 証明書の取得 : [page 26](#)
7. 再発行申請 : [page 29](#)
8. お問い合わせ先 : [page 32](#)

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(※)



必要に応じCSRを作成してください。CSRの提出無しで証明書取得時に鍵を生成する方法も可能です。

## 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。  
証明書は平均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 Secure Mail IDのインストール

メール内の手順に従い、証明書を取得します。CSRを提出した場合は生成したサーバへ証明書をインストールしてください。  
CSRの提出をしていない場合は、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。  
PKCS #12ファイルは秘密鍵を含みます。インターネット上へ流出されないよう取り扱いにはご注意ください。

※ 問題なくスムーズに認証が進んだ場合はその限りではありません。お申込み内容によっては5営業日以内もしくはそれ以上の日数を要する場合がございます。

※2025年8月1日よりCertCentralでセキュアメールID製品を提供しています。

# 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

「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 Secure Mail ID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

「ユーザー名」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

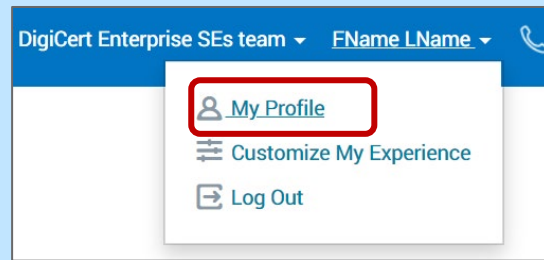
区分

設定方法

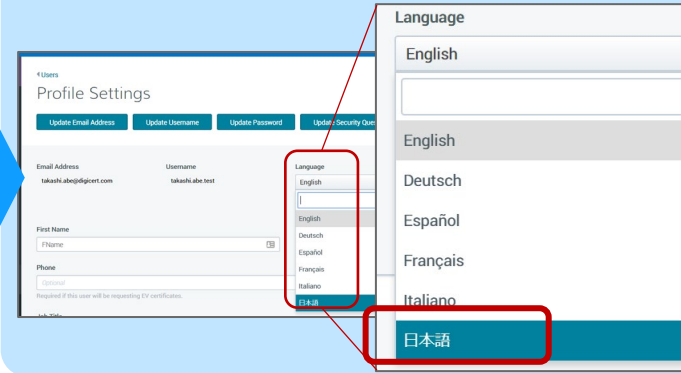
画面表示  
言語

画面表示言語を日本語へ切り替える

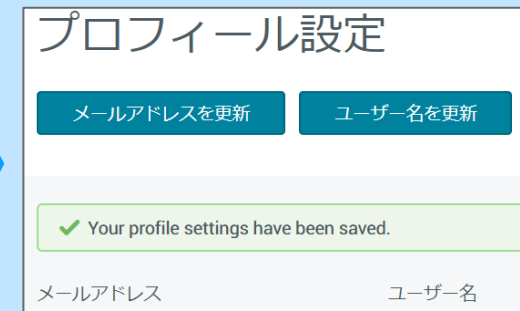
STEP 1 : 画面右上部の「My Profile」から「Profile Setting」をクリック



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



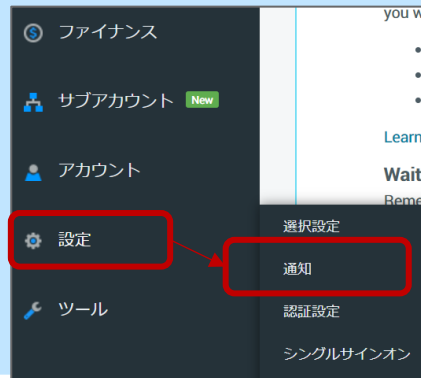
STEP 3 : 下のようなメッセージが表示されれば完了です



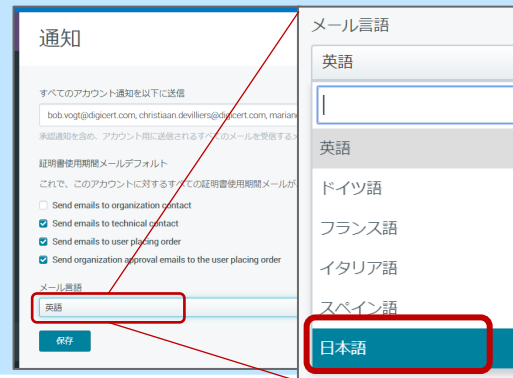
メール  
言語

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

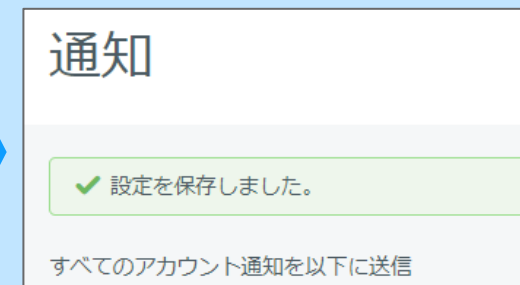
STEP 1 : 画面左メニューの「設定」から「通知」をクリック



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



## 証明書のプロファイルの選択について

- Secure Mail IDの申請では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、2025年7月31日まで提供していたセキュアメールIDと同じ仕様とする場合は、**Multipurpose**をご選択の上、**個人認証 (Personal Authentication)**にチェックを入れて申請してください。

プロファイルの選択	使用目的
Strict (既定値)	個人認証 (Personal Authentication)
<b>Multipurpose</b>	否認防止 (Non-repudiation) データの暗号化 (Data Encryption) <b>個人認証 (Personal Authentication)</b>

※使用目的について

- 否認防止 (Non-repudiation)：データが改ざんされていないことを証明し、データの正当性を証明します
- データ暗号化 (Data encipherment)：データの機密性を保ち、不正アクセスや情報漏洩から保護します
- 個人認証 (Personal Authentication)**：間違いなく本人であることを確認・証明する機能です。本製品においては、S/MIME 証明書を用いて組織を認証します。これにより、メールがその組織から送信されたものであることを証明します。

参考サイト：LegacyプロファイルS/MIME証明書の発行終了のご案内

<https://knowledge.digicert.com/jp/alerts/new-certificate-profile-requirements-for-public-secure-email-smime-certificates>

## よくあるご質問について

---

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>

セキュアメールID申請・認証に関するよくあるご質問

<https://knowledge.digicert.com/jp/general-information/secure-mail-id-authentication-application-faq>

[セキュアメールID]セキュアメールIDについて（申請から発行までの流れ）

<https://knowledge.digicert.com/jp/general-information/secure-email-id>

[セキュアメールID]更新、再発行/再申請、破棄について

<https://knowledge.digicert.com/jp/general-information/secure-mail-id-renewal-reissue-revocation>

[セキュアメールID]CSR 生成 / PKCS#12ファイルの生成 (openssl)

<https://knowledge.digicert.com/jp/tutorials/secure-mail-id-csr-generation-and-pkcs12-conversion-using-openssl>

事前認証：S/MIME用 組織認証

# 組織認証（事前認証）

- Secure Mail IDの申請をするタイミングで組織認証を行う場合は事前認証は不要です。
- Secure Mail IDの申請前に事前認証を実施する必要がある場合はCertCentral左メニュー[証明書]>[組織]より実施してください。
- すでに登録されている組織がある場合は以下のエリアに「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は、次ページの事前認証の申請を行ってください。

digicert® | CERTCENTRAL®

デジサートジャパン ▾ サンプル ▾ STANDARDサポート ⓘ (?)

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	
<input type="checkbox"/>	1-7	Ltd. Tokyo JP	アクティブ	OV, SMIME	認証を保留中
<input type="checkbox"/>		Ltd. Tokyo 104-6111 JP	アクティブ	-	SMIME

# 組織認証の申請

1. 既存の組織名をクリック、もしくは組織を追加してください
2. 「組織認証の申請」項目で「SMIME - SMIME Organization Validation」をチェックします
3. 「認証を申請」をクリックします
4. 事前認証を行うために、DigiCert認証サポートまで必ずご連絡ください

送信先： standard.validation.jp@digicert.com

件名： 組織認証依頼（組織ID：XXXXXXXX）

本文： 以下組織の認証を依頼します。  
アカウント番号： XXXXXXXX  
組織ID： XXXXXXXX

### 組織認証の申請

CS - Code Signing Organization Validation

EV CS - Code Signing Organization Extended Validation (EV CS)

DS - Document Signing Validation

SMIME - SMIME Organization Validation

OV - Normal Organization Validation

EV - Extended Organization Validation (EV)

参考サイト：[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>

事前認証：メールアドレスで使用する  
ドメインの利用権確認（DCV）

# ドメイン利用権の確認 (DCV)

- Secure Mail IDはDCVの事前認証を推奨します。
- Secure Mail IDの申請前に事前認証を実施する場合はCertCentral左メニュー[証明書]>[ドメイン]より実施してください。
- すでに登録されているドメインがありDCVが完了していない、もしくは登録がない場合は、次ページの事前認証の申請を行ってください

※Secure Mail IDは申請画面でDCVを選択する箇所がなく自動的にメール認証(Verification Email)として処理され、対象の宛先にメール（英文）が送信されます。そのため事前にDCVを実施し、完了したあとに申請することを推奨しております。

The screenshot shows the CertCentral interface for domain management. The left sidebar has a menu with 'Domains' highlighted. The main content area shows a table of domains with columns for 'Domain Name', 'Organization', 'Added Date', 'DCV Method', 'Verification Status', and 'Verification Validity Period'. One domain is listed with a 'Verification Status' of 'Verification Complete'.

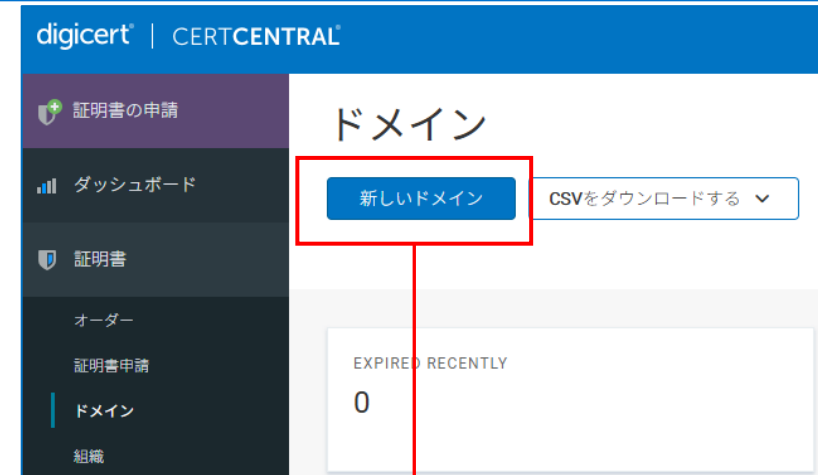
ドメイン名	組織	追加工	DCV方式	認証ステータス	認証有効期間
.....co.jp ドメイン ID: .....	.....Ltd. 組織ID: ..... ..... Tokyo..... ..... JP	2025/1/16	申請承認メール(DCVメール)	認証済み	2026/2/17

# ドメイン利用権の申請（新規）

1. ドメイン利用権の確認を新規で登録する場合は「新しいドメイン」をクリックして登録してください。
2. ドメイン名を入力します
3. 組織は登録済みの組織名から選択します
4. ドメインの利用権の確認方法を指定します
5. 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
6. 「Choose addresses」をクリックして申請します
7. 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>



### 新しいドメイン

ドメインの詳細

ドメイン名  
sample.jp-ex.com

組織  
DigiCert Japan G.K. Organization ID:1168491

ドメイン名利用権の確認 (DCV) 方式 ⓘ

- DNS TXTレコード
- DNS CNAMEレコード
- 申請承認メール
- ファイル認証

DCVメールの言語  
Japanese

キャンセル Choose addresses

# ドメイン利用権の申請（既存の場合）

1. リストされたドメイン名をクリックします
2. 「ドメイン認証有効期限」の期間内である場合はDCVを省略することが可能です
3. 認証期間が切れている場合には改めて「ドメイン名利用権の確認（DCV）方式」でDCVを行う方式を指定し「Submit for validation(認証を申請)」をクリックして申請します
4. 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>

## ドメイン認証ステータス

ドメイン認証有効期限  
2026/8/16 13:05 JST 

注：業界の変更により、ドメインの有効期間が短くなっています。

## ドメイン名利用権の確認（DCV）方式

- DNS TXT Record
- DNS CNAME Record
- Verification Email
- HTTP Practical Demonstration

認証するドメインを申請し、ドメインの再認証を再開します。

キャンセル

認証を申請

# ドメインの利用権 (DCV) の種類

- ・ 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(Verification Email)	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(HTTP Practical Demonstration)	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： <b>http://&lt;確認対象のドメイン名&gt;/.well-known/pki-validation/fileauth.txt</b>
DNS TXT認証(DNS TXT Record)	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： <b>&lt;確認対象のドメイン名&gt; TXT &lt;認証トークン&gt;</b>
DNS CNAME認証(DNS CNAME Record)	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： <b>&lt;認証トークン&gt;.&lt;確認対象のドメイン名&gt; CNAME dcv.digicert.com</b>

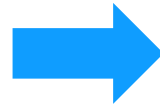
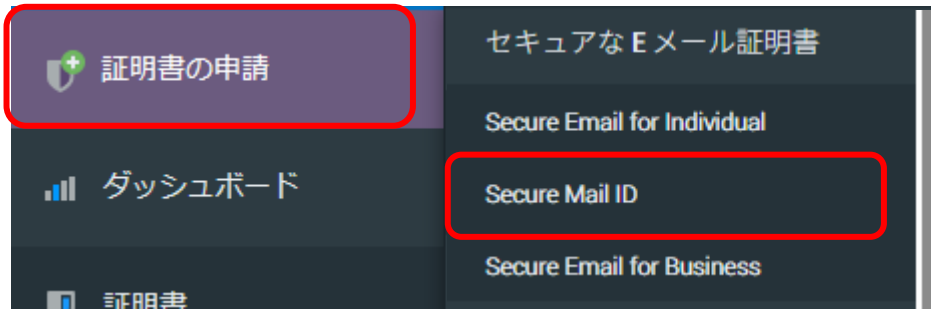
参考サイト：

[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>

# Secure Mail IDの新規申請 (Secure Email for Organization)

# Secure Mail IDの新規申請



証明書の申請情報  
組織申請  
その他のオーダー情報の  
入力が必要です

CertCentral左メニュー「証明書の申請」から  
Secure Mail IDお選びください

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>

# Secure Mail ID 申請：証明書情報の入力

必須

Secure Mail ID証明書を申請する  
対象：デジサート・ジャパン合同会社

証明書の有効期限

- 1年
- 2年
- カスタム有効期間
- カスタム長

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。

※バウチャーには、申請可能な製品、製品の有効期間などの情報があらかじめ登録されています。CertCentralで申請する際にはこれらの登録されている内容がプリセットされた状態から申請を開始します。

必須

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。

組織



組織を追加する

組織を追加する

どの組織名を証明書に表示させますか？

既存の組織

未認証の組織 を非表示にする

テスト株式会社  
(組織ID:1919900)

銀座6-10-1 GINZA SIX8階  
中央区, 東京都, JP: 1040061  
03-4560-3900

デジサート・ジャパン  
合同会社  
(組織ID:1007421)

銀座6-10-1 GINZA SIX8階  
中央区, 東京都, JP: 1040061  
03-4560-3900

DigiCert Japan G.K.  
(組織ID:1168491)

銀座6-10-1 GINZA SIX8階  
中央区, 東京都, JP: 1040061  
03-4560-3900

新しい組織

キャンセル

追加する

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。

※稀に次頁項目のCSRを提出した際、組織情報が複数表示されることがあります。その際はゴミ箱のアイコンマークですべての組織を削除し、「組織を追加する」から正しい組織を選択しなおしてください。

# Secure Mail ID 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

安全性を維持するため、証明書は長さが少なくとも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。

## CSRの生成方法を指定します

必須

・サーバーで生成したCSRを提出もしくは、発行後にブラウザで秘密鍵とCSRを生成し証明書を取得する方法のいずれかを選択してください。

※ CSRの内容と、証明書Eメールアドレスや組織情報、住所の値が異なる場合は、申請時の入力内容が優先され、上書きされます。

※ 「ブラウザからCSRを生成する」でCSRの提出をしない場合は、発行された後、ブラウザで証明書を含む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。PKCS # 12ファイルは秘密鍵を含みますのでインターネット上でのやりとりなどを行わない等、取り扱いにご注意ください。

証明書の詳細

コモンネーム  
組織名またはEメールアドレスを追加

Eメール    **組織**

組織名  
DigiCert Japan G.K.

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。

追加する

追加のEメールアドレス (オプション)

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

必須

・必ず「組織」を選択して下さい。これにより証明書情報に組織名が登録されます。


## 証明書Eメールアドレス

必須


・ Secure Mail IDを利用するEメールアドレスを入力し「追加する」で確定してください。

# Secure Mail ID 申請：追加証明書オプション

✓追加証明書オプション

プロファイルオプション  ←

Multipurpose

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 ←

## 申請する証明書のプロファイルの選択

必須

・ Strict (デフォルト) 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。

・ 2025年7月31日まで提供していたセキュアメールIDと同じ仕様とする場合は、**Multipurpose** をご選択の上、個人認証 (Personal Authentication) にチェックを入れて申請してください。

## 生成する鍵の長さを指定します

・ 「ブラウザからCSRを生成する」を選択した際にこのプルダウンメニューが表示されます。CSRを提出した場合は表示されません。生成される鍵のサイズを指定してください。鍵のサイズは後で変更することはできません。

## 証明書の使用（目的）を指定します

必須

・ 目的に合わせて選択します。不明な場合、2025年7月31日まで提供していたセキュアメールIDと同じ仕様とする場合は「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

## 中間CAおよびRoot CAの指定

・ デフォルトで表示されているキーチェーンのまま変更せず申請してください  
中間CA証明書：DigiCert Assured G2 SMIME RSA4096 SHA384 2024 CA1  
ルート証明書：DigiCert Assured ID Root G2

## 証明書の署名ハッシュ（アルゴリズム）

必須

・ sha256RSAまたはsha384WithRSAなどをご指定ください。

# Secure Mail ID 申請：その他オプション、支払い情報の指定

✓ 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。

## その他のオーダーオプション

- ・「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。
- ・「追加のEメール」：申請者に加えて、申請関連のメールの送信先を追加することができます。追加したすべての宛先に発行通知メールが送信される仕様のため、ご申請完了後に追加することを強くおすすめいたします。申請後、CertCentral左メニュー[証明書]>[オーダー]からオーダー詳細画面で追加/変更/削除することが可能です。

### 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 ←

このアカウントの請求担当者と同じ

テスト  
デジサート・ジャパン合同会社  
銀座6-1-10  
GINZA・SIX 8階  
中央区, 東京都, 1234567  
JAPAN  
@digicert.com  
03-4560-

[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** ←

## 支払い情報

- ・支払い方法を指定します。銀行振込の場合は社名等の情報が不足していないかご確認ください。「このアカウントの請求担当者と同じ」のチェックを外すと入力画面に切り替わりますので請求書に表示する情報をご入力ください。
- ・クレジットカードの場合、即時に課金します。
- ・バウチャーを利用して申請している場合は、支払方法の選択情報は表示されません。

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

以上で申請は終わりです。

# Secure Mail IDの更新申請 (Secure Email for Organization)

# Secure Mail IDの更新申請

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

ACME ディレクトリ URL

有効期限間近の証明書

レポート

更新通知

フィルター未設定

検索する

30日以内に有効期限が切れる

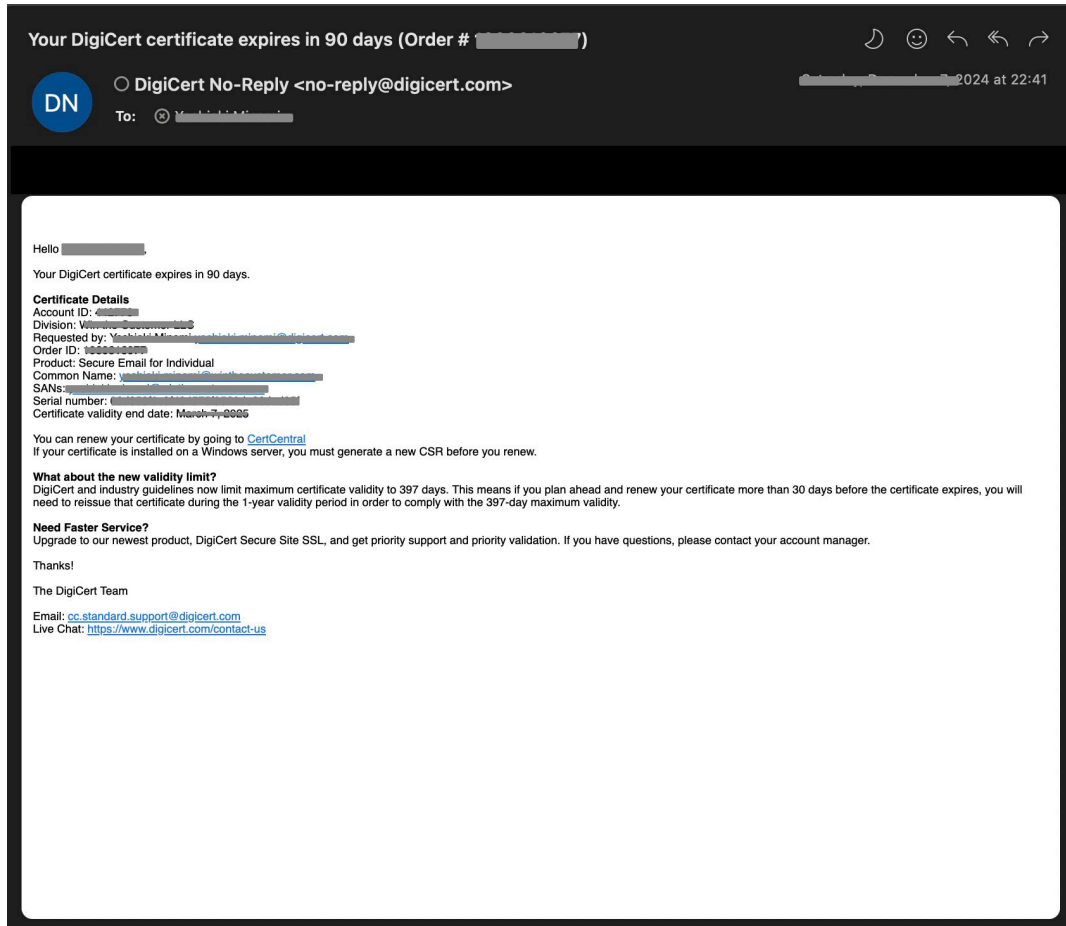
オーダー番号	コモンネーム	期限切れ予定日	オーダー有効期限切れ	製品	有効期限	更新通知
クイックビュー		2025/7/19	2025/7/19	Secure Mail ID	2年	今すぐ更新する
クイックビュー		2025/7/31	2025/7/31	Secure Mail ID	2年	今すぐ更新する
クイックビュー		2025/8/4	2025/8/4	Secure Mail ID	2年	今すぐ更新する

CertCentral左メニュー「**有効期限間近の証明書**」から「今すぐ更新する」の文字をクリックして更新申請を開始してください。

更新申請手順は**新規申請手順の19ページ**以降をご参照ください。

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>

# 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>

- 更新申請はオーダー有効期限日90日前から行えます
- 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、組織認証およびDCVの再認証が必要になります

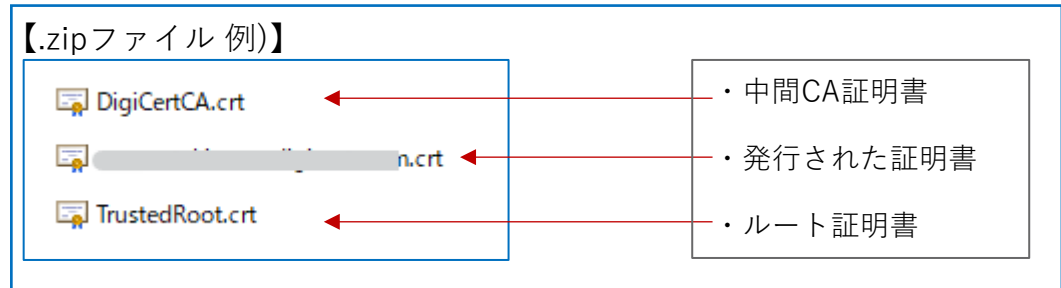
証明書の取得

# CSRを提出した申請の場合：発行された証明書の取得

- ・認証が終わりましたら証明書が発行され、メールで証明書の発行をお知らせするメールが配信されます。メールに添付されている.zipファイルから証明書を取得します。**※発行通知メールは、申請者および申請時に設定した追加のEメール(任意)宛へ自動配信されます。**
- ・CertCentralのオーダーからも証明書をダウンロードすることが可能です。お客様の環境に応じて、PKC#7 (.p7bファイル)、または個々の証明書(.crtファイル)形式から最適なフォーマットを選択してダウンロードしてください。
- ・メールサーバもしくはメーラーに証明書を設定してください

## 申請者宛 メール 例)

件名	XX証明書のEメールアドレスXX 向けの 証明書
送信元	DigiCert <admin@digicert.com>
本文 (日本語 選択時、 抜粋)	<p>XX証明書のEメールアドレスXX 向けの 証明書が承認されました。 この証明書の DigiCert オーダー番号は XXXXXXXXXX です。</p> <p>証明書の詳細 アカウント番号: XXXXXXXX 管理グループ: XXXXXXXXXXXXXXXX 製品: Secure Mail ID シリアル番号: XXXXXXXXXXXXXXXXXXXX コモンネーム: XXXXXXXXXXXXXXXX 有効期間 or 有効年数: 1 証明書の有効期限開始日: 2025-XX-XX 証明書の有効期限終了日: 2026-XX-XX 発行者名: /C=US/O=DigiCert, Inc./CN=DigiCert Assured G2 SMIME RSA4096 SHA384 2024 CA1</p> <p>この E メールに添付されている新しい証明書をご確認ください。.</p> <p>オンライン証明書インストール手順は以下でご覧いただけます。 <a href="http://www.digicert.com/ssl-certificate-installation.htm">www.digicert.com/ssl-certificate-installation.htm</a></p> <p>FAQ: [CertCentral] 発行通知の添付ファイルについて <a href="https://knowledge.digicert.com/ja/jp/solution/SOT0015.html">https://knowledge.digicert.com/ja/jp/solution/SOT0015.html</a></p> <p>ありがとうございました</p> <p>DigiCert チーム</p>



- ・発行された証明書発行通知メールの添付ファイルが社内のセキュリティポリシー等により削除され受信ができない場合は、CertCentralのオーダー画面からご取得いただくことが可能です。発行通知メールの証明書とCertCentralからダウンロードする証明書は同じ証明書です。
- ・発行通知メールの証明書取得方法を添付ファイルではなく別の方法で取得する方法を設定することが可能です。CertCentral左メニュー[設定]>[通知]から「高度な通知設定」を展開し、「証明書ダウンロードのデフォルト」の箇所デフォルト設定となっている「添付ファイル」から「ダウンロードリンク」へ変更することをおすすめします。

※システム変更等により、サンプルと件名及び本文の表記が異なる場合があります。

# 「ブラウザからCSRを生成する」を選択した場合：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を開きインストール用の証明書パスワードを設定すると、ブラウザ内で秘密鍵を生成しPKCS#12ファイルを作成します
  - 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
  - 生成したPKCS#12ファイルをダブルクリックして設定した証明書パスワードを入力し、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 Secure Mail ID 証明書の承認が完了しました
送信元	DigiCert <admin@digicert.com>
本文 (抜粋)	XXXXXXXXXXXX 様 デジサート 組織用証明書（Secure Mail ID）が承認されました。 次のURLにアクセスし、お早めにデジサート 組織用証明書を取得してください： <a href="https://www.digicert.com/link/pid-install.php?token=XXXXXXXXXXXXXXXX">https://www.digicert.com/link/pid-install.php?token=XXXXXXXXXXXXXXXX</a>

- 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
- ※システム変更等により、サンプルと件名及び本文の表記が異なる場合があります

## 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.

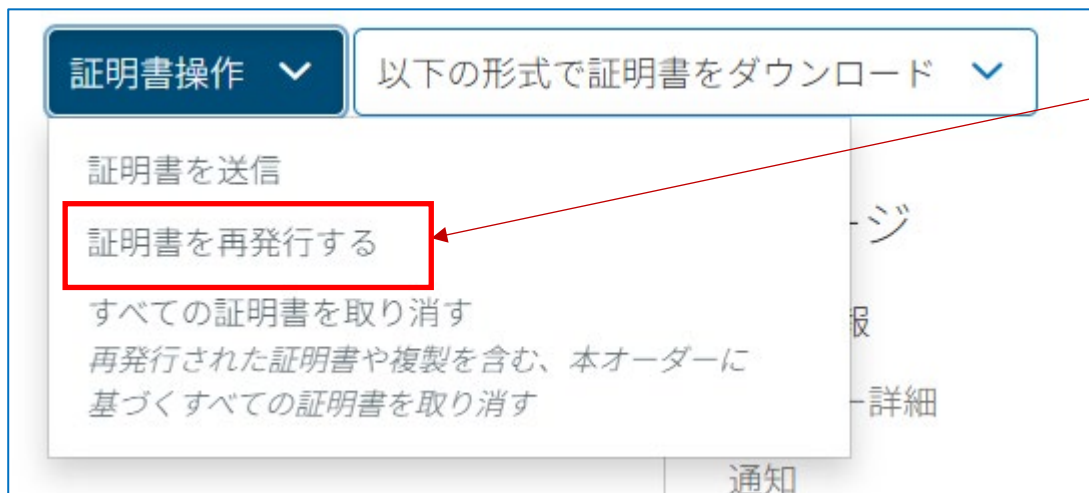
パスワードの確認: [ ]

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](#)

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
- ※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）

再発行申請

# 証明書の再発行



1. CertCentral左メニュー[証明書]>[オーダー]から該当のオーダー番号を選択します
2. [証明書操作]のプルダウンメニューから「証明書を再発行する」を選択します
3. 再発行申請画面で必要な情報を入力し「申請を送信」します

※再発行では以下申請（証明書）情報の変更が可能です。

- CSRの変更
- 証明書の取得方法の変更
- 証明書Eメールアドレスの変更
- プロファイルオプションの変更
- 証明書の使用の変更
- 署名ハッシュ（アルゴリズム）の変更

※社名・組織/団体名が変更になった場合は新規申請が必要です。再発行申請で組織名を変更することはできません。新組織名での証明書は、登記完了後に取得可能となります。

4. 再発行申請が完了し発行済となった後、再発行元の証明書は「失効保留」となり、72時間後に失効（Revoke）されますのでご注意ください

参考サイト：[セキュアメールID]更新、再発行/再申請、破棄について

<https://knowledge.digicert.com/jp/general-information/secure-mail-id-renewal-reissue-revocation>

# 2025年7月31日以前に取得したセキュアメールIDの再発行依頼方法

## DigiCert : セキュアメールID再発行 申請入力フォーム

[必須] のマークのある項目は必須項目です。必ずご記入下さい。

### 申請基本情報

元証明書の受付番号	必須	<input type="text"/>
※オーダー番号や申請管理番号が不明な場合は、コモンネーム等証明書情報をご記入ください。		
再発行理由	必須	<input type="text"/>
(例) 秘密鍵の変更 ※証明書サブジェクト名を変更する場合は、新規申込みとなります。		
製品		セキュアメールID
再発行証明書の有効期限	必須	<input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日

### 証明書申請情報

CSR	必須	<input type="text"/>
-----	----	----------------------

旧セキュアメールID 再発行申請フォームにアクセスします

<https://updates.digicert.com/smidreissue>

専用フォームからご申請ください。申請内容確認後、弊社より再発行のお手続きを行います。なお、証明書サブジェクトに記載される申請団体名の変更が必要となる場合の再発行はお受けできません。CertCentral上から新規申請をしてください。

### 申請基本情報

#### 元証明書の受付番号

・現在ご利用のセキュアメールIDのリクエスト番号やオーダー番号、コモンネーム等証明書を特定できる情報を記入します。

#### 再発行理由

・再発行理由を明記してください。

#### 再発行証明書の有効期間

・現在ご利用のセキュアメールIDの証明書有効期間終了日をご記入ください。

### 証明書申請情報、申請責任者情報、技術担当者情報

・必須項目をすべてご記入ください。  
最後に利用規約にチェックし、「申請する」を押下します。

弊社にて申請内容確認後に、証明書の再発行手続きを進めます。



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

## 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](mailto: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](mailto: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