マネージド PKI Lite
管理者マニュアル

Ver10.0（2024 年 12月版）

GlobalSign by GMO

目次

目次

はじめに

本マニュアルはマネージドPKI Lite を利用する管理者向けの操作説明ドキュメントです。
初回に GS パネルのアカウント・プロファイル・ライセンスなどのお申し込みを完了された後、実際にクライアント証明書を発行するまでには、いくつかの初期設定を行う必要があります。

初期設定の手順は、本マニュアルP5～の「1.マネージド PKI Lite 初期設定」をご参照ください。

大まかな流れは以下の通りです。

①GS パネル（管理画面）へアクセスし、「マネージド PKI」タブに移動
②クライアント証明書を発行するためのライセンスを購入、プロファイルの登録（ライセンス購入申請の承認と、プロファイルの審査をグローバルサインで行います。）
③②の完了後、再度 GS パネルにアクセスし、「マネージド PKI」タブ上で管理者証明書を取得
④取得した管理者証明書で、証明書の管理画面に進む

※本マニュアルは 2024 年 12月時点の仕様を元に作成されています。
以下の仕様が追加されておりますので、ご注意ください。

・証明書の利用用途に応じて、紐づく中間CAを選択いただけます。

用途	中間 CA 証明書
S/MIME 用途	S/MIME BR(Legacy)対応用中間 CA（GlobalSign GCC R6 SMIME CA 2023
アクセス認証用途	アクセス認証用中間 CA(GlobalSign GCC R45 Client Authentication CA 2024) ※2024 年 12 月 9 日以降はこちらの中間から発行されます。
	アクセス認証用中間 CA(GlobalSign GCC R3 PersonalSign 2 CA 2020)

※異なる中間CA証明書より発行した証明書を対象に更新を行うことはできません。

・2024年12月9日以降、証明書のDN（ディスティングイッシュネーム）情報に、新たに以下の項目を追加いたします。
「SurName（名字）」、GivenName（名前）、「Pseudonym（スードニム）」
※個人名用ライセンスを利用して【S/MIME用中間CA】から発行されるクライアント証明書が対象です。
※SurName、GivenName＋SurNameまたはPseudonymのいずれかを設定する必要があります。

・2025年5月26日以降は、SurName、GivenName＋SurNameまたはPseudonymのいずれかが適用されていない証明書は更新および再発行ができかねますのでご注意ください。

・S/MIME BR(Legacy)対応用中間CAを利用するためには下記の条件をすべて満たす必要があります。
① OU フィールドが登録されていない。
② S/MIME BR(Legacy)対応用 E メールドメインが登録されている。
③ OrganizationIdentifier（OID）が登録されている。
※一つでも対応できていない場合は、プロファイル上でS/MIME BR(Legacy)対応用中間CAを選択できません。

また、本マニュアルはGS パネルの「マネージドPKI」タブの画面よりいつでもダウンロードできます。
ご不明点な等ございましたら、下記リンクのお問い合わせフォームよりお気軽にお問い合わせください。

https://jp.globalsign.com/contact/customer/

1.マネージド PKI Lite　初期設定

※こちらでご紹介する手順は、既に GS パネルのアカウントをお持ちの方が、マネージド PKI Lite の利用を開始する手順です。

まだGS パネルのアカウントをお持ちでない方は、以下のお申し込みガイドを参考にお手続きください。お手続き完了後に GS パネルのアカウントが作成されますので、本マニュアルP13～「(初期設定)管理者証明書を取得」へお進みください。

〈マネージド PKI Lite 新規お申し込み (プロファイル申請・ライセンス購入)〉
https://jp.globalsign.com/service/clientcert/order_epki.html

【 ライセンスとは 】
ライセンスとは、クライアント証明書を発行する権利であり、その有効期間は一律 1年間となります。

ライセンスを消費して実際に発行されるクライアント証明書の有効期間とは異なりますのでご注意ください。

【ライセンスの種類について】

■マネージドPKI Lite byGMO 個人名用

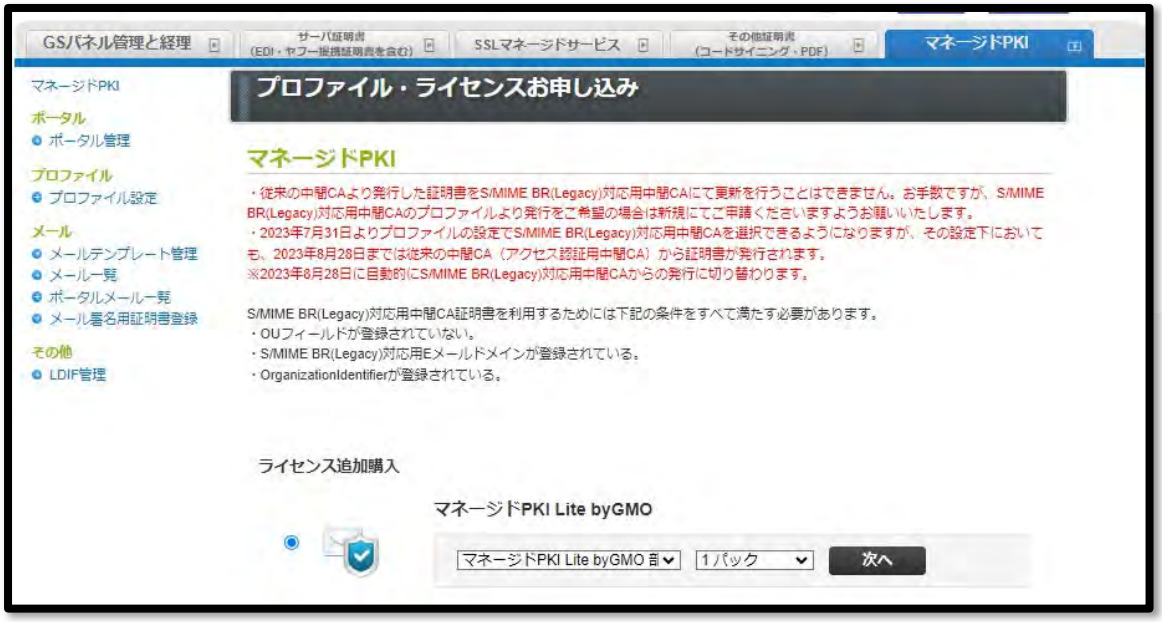
利用用途	説明
アクセス認証の用途で利用する場合	証明書のコモンネーム(CN)に、任意の値を設定可能です。
S/MIME の用途で利用する場合	S/MIME 用証明書のコモンネームとして利用できる値は、以下の通りです。 **①自社および関連会社に属する個人の E メールアドレス** **②SurName** **③SurName + GivenName** **④Pseudonym** ※法人名、または、自社および関連会社に属する部門用メールアドレスを設定する場合は、【マネージド PKI Lite byGMO 法人名用】をお申し込みください。

■マネージドPKI Lite byGMO 法人名用

利用用途	説明
アクセス認証の用途で利用する場合	【マネージド PKI Lite byGMO 個人名用】を選択しなおし、お申込みください。
S/MIME の用途で利用する場合	S/MIME 用証明書のコモンネーム(CN)に**法人名、または、自社および関連会社に属する部門用メールアドレス**を設定可能です。

初期設定①プロファイル・ライセンスお申し込み

1.　GS パネルにログイン後、「マネージドPKI」のタブに移動します。
ライセンス追加購入のラジオボタンをチェックし、ご希望のライセンス数を選択して「次へ」に進みます。
※プロファイル未申請の状態で初回申し込みを行う場合、ライセンスの申し込みとプロファイルの申請は同時に行われます。
プロファイルの申請権限は管理者権限のみのため、管理者権限のユーザ ID でログインして、作業を進めてください。



2. ライセンスを利用して発行する証明書の有効期間を選択し、「次へ」をクリックして進みます。
（キャンペーンコードやクーポンコードをお持ちの方は、こちらの画面で入力し、「適用」ボタンをクリックしてください。）

3.プロファイル情報（発行するクライアント証明書に記載される内容）を登録します。

証明書をS/MIMEの用途で利用する場合は、「S/MIME BR(Legacy)対応用中間 CA」を選択し、「organizationIdentifier」の項目を入力してください。
※S/MIME を利用する場合は必須となります。

証明書をアクセス認証の用途で利用する場合は、「アクセス認証用中間 CA」を選択し、「BaseDN」の項目にチェックを入れ、「組織名（O）」と「部署名（OU）」に値を入力してください。
「次へ」をクリックして進みます。

【 BaseDN とは】
BaseDN の項目にチェックを入れてプロファイル情報を登録すると、「組織名（O）」と「部署名（OU）」の組み合わせを独占し、他のお客様に同じ値を登録させないようにすることができます。
こちらの組み合わせをアクセス認証の設定にお使いいただくことをおすすめします。
※OUを含むことができる「アクセス認証用中間 CA」のプロファイルからのみ利用可能です。

4.お支払い情報を入力し、「次へ」をクリックして進みます。

5. 入力した情報の確認画面が表示されます。
ライセンスの有効期限を理解し、利用規約に同意した上で「次へ」をクリックしてください。
以上で申請は完了です。

2～3営業日でライセンスの承認やプロファイルの審査が完了いたします。
※第三者データベースまたはご提出頂いた電話会社の請求書に記載されている代表電話番号へご連絡を行い、申請者様の在籍確認と連絡先電話番号の確認を行います。
上記確認事項を元に、申請者様へご連絡をし「プロファイル ID」、申請内容を確認させていただきます。

上記が完了したら、次項の「メールドメインの登録」に進みます。
※「S/MIME BR(Legacy)対応用中間 CA」のプロファイルを選択した場合は登録が必須になります。
※プロファイルの審査完了後にメールドメインの登録が可能になります。

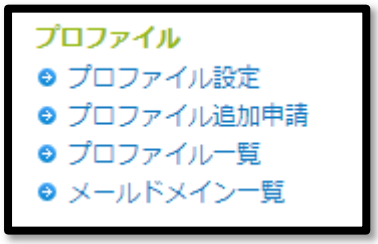
初期設定②メールドメイン情報の登録

「S/MIME BR(Legacy)対応用中間 CA」のプロファイルを使用する場合、メールドメイン情報の登録および審査が必須となり、その審査情報利用期間は397日となります。

以下の条件に該当する場合、以下の手順でメールドメイン情報の登録をしてください。

・S/MIME 利用の場合
・「アクセス認証用中間 CA」のプロファイルから、管理者一括申請の証明書にメールアドレスを登録したい場合
※追加登録は随時可能です。

1. マネージドPKI のタブから「プロファイル設定」を選択し、「次へ」進みます。



2. メールドメインを設定するプロファイルを選択し、「次へ」進みます。

3. メールドメイン情報の「設定」ボタンを選択し、「次へ」進みます。

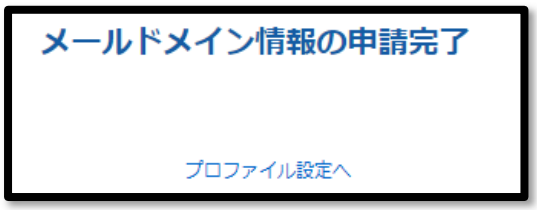
4.任意のメールドメイン情報を入力後、「S/MIME を利用します。メールドメインの有効期間は 397 日となり、継続利用のためにはドメインの再認証が必要であることを了承します。」を選択し、「次へ」進みます。
※アクセス認証用中間 CA 利用のお客様は「SMIME は利用しませんが…」を選択することで、再審査をせずに継続して利用することができます。

5.メールドメイン認証方法選択の画面に移ります。
メール認証・DNS 認証・ページ認証いずれかの対応可能な認証方法を選択してください。

利用可能な認証方法を選択し、「次へ」をクリックして進みます。

6. 登録内容に問題がないことを確認し、「次へ」をクリックして進みます。

7. 以上でメールドメイン情報の登録は完了です。



申請完了後、2～3営業日以内を目処に弊社審査部門よりメールにてご連絡いたします。
認証方法によってメールの From アドレスが異なります。
下記をご参照ください。

認証方法	From	説明
メール認証	approval@globalsign.com	例：globalsign.com でメール認証をした場合、mail.globalsign.com 等でも利用できます。
DNS 認証	vetting-jp@globalsign.com	例：globalsign.com で DNS 認証をした場合、mail.globalsign.com 等でも利用できます。
ページ認証	vetting-jp@globalsign.com	例：globalsign.com でページ認証をした場合、mail.globalsign.com 等では利用できません。 ページ認証の場合は、サブドメインを含む FQDN 単位で登録し、認証する必要があります。

8. 登録を行ったメールドメインは左サイドメニューのメールドメイン一覧にて確認する事ができます。

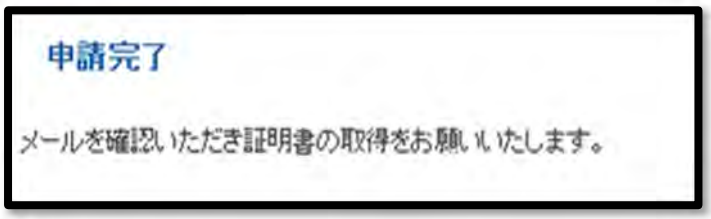
初期設定③管理者証明書を取得

【管理者証明書を取得】
GS パネル内のクライアント証明書を管理する画面にアクセスするための専用のクライアント証明書です。
グローバルサインから無償で提供しているため、管理者証明書の発行にライセンスは消費しません。

1.GS パネルにログインし、「マネージドPKI」タブ内の「証明書管理」をクリックします。

2.管理者証明書を取得する際に必要となるパスワードを設定します。
半角英数混在8文字以上の値を2回入力し、「次へ」をクリックします。

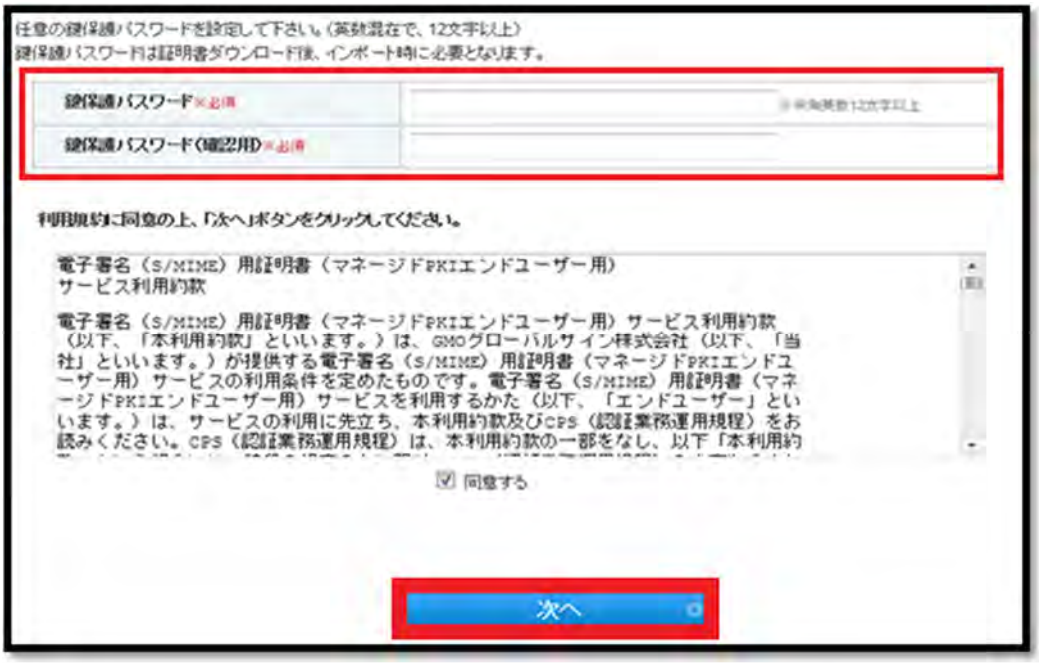
3.「申請完了」と表示されれば、申請は完了です。



4.ユーザ情報に登録されているメールアドレス宛てに送信されるメールを確認し、メール内に記載されている証明書取得メールへアクセスします。

5. 2.で登録した証明書取得用パスワードを入力し、「次へ」進みます。
※証明書取得用 PW は 256 文字以内で設定してください。

6.後ほどダウンロードする証明書ファイル（PKCS12 ファイル）にかけるパスワードを設定します。
半角英数混在の12文字以上の値を2回入力し、利用規約に同意の上、「次へ」をクリックします。



7.「証明書ダウンロード」ボタンをクリックし、証明書ファイルを任意の場所へ保存します。

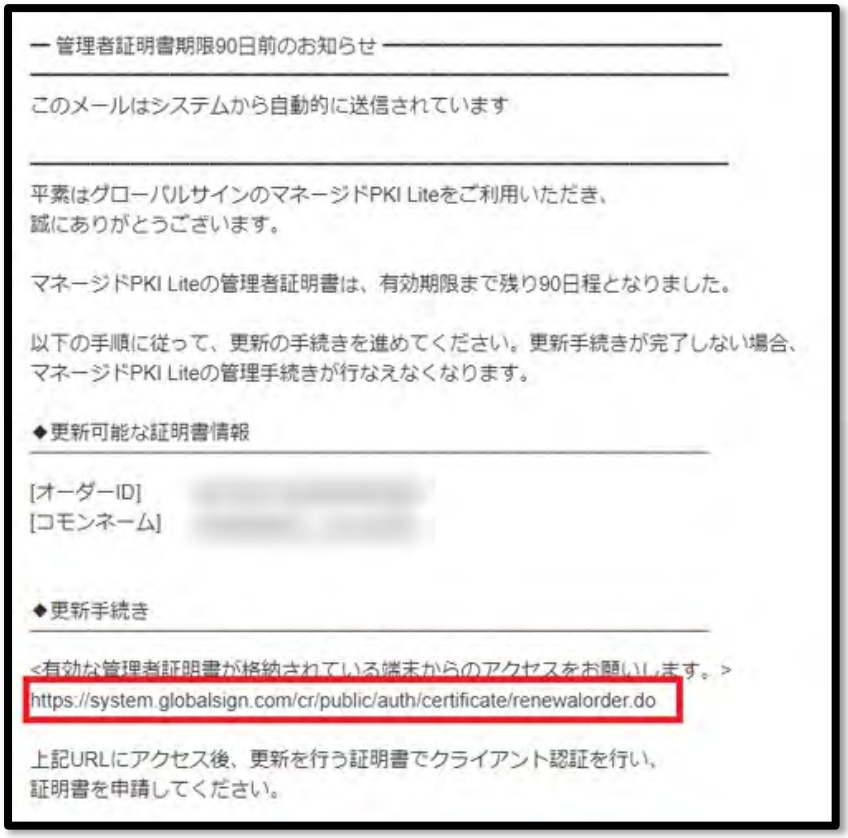
8.お使いの端末やブラウザ等の環境に合った方法で、保存した証明書ファイルを用いて証明書ストアへ証明書のインストールを行います。
※証明書のインストール方法につきましては、P58～をご確認くださいませ。

9.管理者証明書のインストールが完了後、再度 1.の「証明書管理」をクリックしてください。
アクセス認証が開始し、証明書の選択画面が表示されますので、正しい証明書を選択すると、クライアント証明書の発行等の操作ができるようになります。

【管理者証明書の更新について】

ご利用の管理者証明書の有効期限が近づくと、管理者証明書に登録されたメールアドレス宛に以下の更新案内メールが送信されます。
※有効期限 90 日前より送信されます。

1. 更新案内のメール内に記載されたURL に、管理者証明書がインストールされたPC／ブラウザでアクセスしてください。



2. 更新対象の管理者証明書を選択し、クライアント認証を行い、更新のお手続きを進めてください。

【管理者証明書取得時のトラブルに関して】

・管理者証明書の取得がお済みではない場合
GS パネルの「マネージドPKI」タブ内、「証明書管理」へアクセス後、「次へ」ボタンより管理者証明書の再発行画面へとお進みください。
（有効期限が切れた場合でも同様に「次へ」ボタンが表示されます。）

・管理者証明書を既に取得したが、紛失等で管理者証明書を取得しなおしたい場合
GS パネルの「マネージドPKI」タブ内、「証明書管理」へアクセス後、証明書のポップアップが表示されます。
「キャンセル」ボタンをクリック後、上記の画面が表示されますので、「次へ」ボタンより管理者証明書の再発行画面へとお進みください。

＜管理者証明書に関する注意点＞

※2024年8月26日以降、管理者証明書のプロファイル情報が変更されました。
以降は、変更前プロファイルの管理者証明書を利用した認証ができなくなりますので、新しいプロファイルの管理者証明書を新規にて発行してください。

※管理者証明書の再発行や更新に関するメールの送付先アドレスは、後から変更することができます。
GS パネルの「ユーザ管理」から対象のユーザ ID を編集すると、以降に行う再発行や更新に関するメールが、変更後の新たなメールアドレス宛に送信されます。（管理者証明書に登録されているメールアドレスは変更されません。）

※管理者証明書に登録されている CN（＝ユーザ ID）やメールアドレスを変更したい場合、「ユーザ管理」から新たにユーザを追加登録し、そのユーザIDで新たに管理者証明書を取得してください。

※ご利用の端末を変更される場合は、現在利用中の端末で、管理者証明書をエクスポートし、新しい端末にインポートしてご利用ください。

※再発行にて新しい端末で取得し直すことも可能です。

※再発行後は、元の証明書は利用できなくなりますのでご注意ください。

初期設定④プロファイルのセットアップウィザードを設定

ライセンスの購入やプロファイルの認証が完了後、プロファイル セットアップウィザードを利用して、クライアント証明書の発行時に適用される各種オプションを確認、設定することができます。

1.GS パネルにログインし、「マネージドPKI」タブに移動します。
「セットアップウィザード」の項目をクリックしてください。

2.認証済みのプロファイルが表示されていますので、そのまま「次へ」をクリックして進みます。

3.「更新設定」の項目では、発行したクライアント証明書の更新時に、どのような申請や承認フローをとるかという「更新タイプ」を選択します。
お客様の運用にあった更新タイプを選び、「次へ」をクリックして進みます。
※クライアント証明書の更新タイプの詳細につきましては、P43 をご確認ください。

4.「EFS 設定」の項目で「有り」を選択すると、発行される証明書の拡張キー使用法に「暗号化ファイルシステム」が追加されます。
この設定に対応するアプリケーションを使用する方のみ「有り」を選択し、「次へ」をクリックして進みます。

【 EFS（Encrypting File System）】
証明書の拡張キー使用法の項目に「暗号化ファイルシステム（1.3.6.1.4.1.311.10.3.4）」の記載があるものは、Microsoft OS で使用している NTFS 形式のファイルの暗号化に利用することができます。

5.「エクスポート不可設定」の項目で「有り」を選択すると、Windows の機能により、後から秘密鍵をエクスポートできなくなります。
※詳細は P81「秘密鍵のエクスポート不可」をご覧ください。

こちらの機能が必要な方のみ「有り」を選択し、「次へ」をクリックして進みます。

6.「API 設定」の項目では、証明書の申請等に API を利用される方のみ、アクセスを許可する IP アドレスを設定してください。「次へ」進みます。

7.「メールテンプレート設定」の項目では、発行するクライアント証明書関連のメールテンプレートや送信の有無等を編集することができます。
必要な箇所を編集し、「次へ」をクリックしてください。
※各メールテンプレートの詳細は P88～をご覧ください。

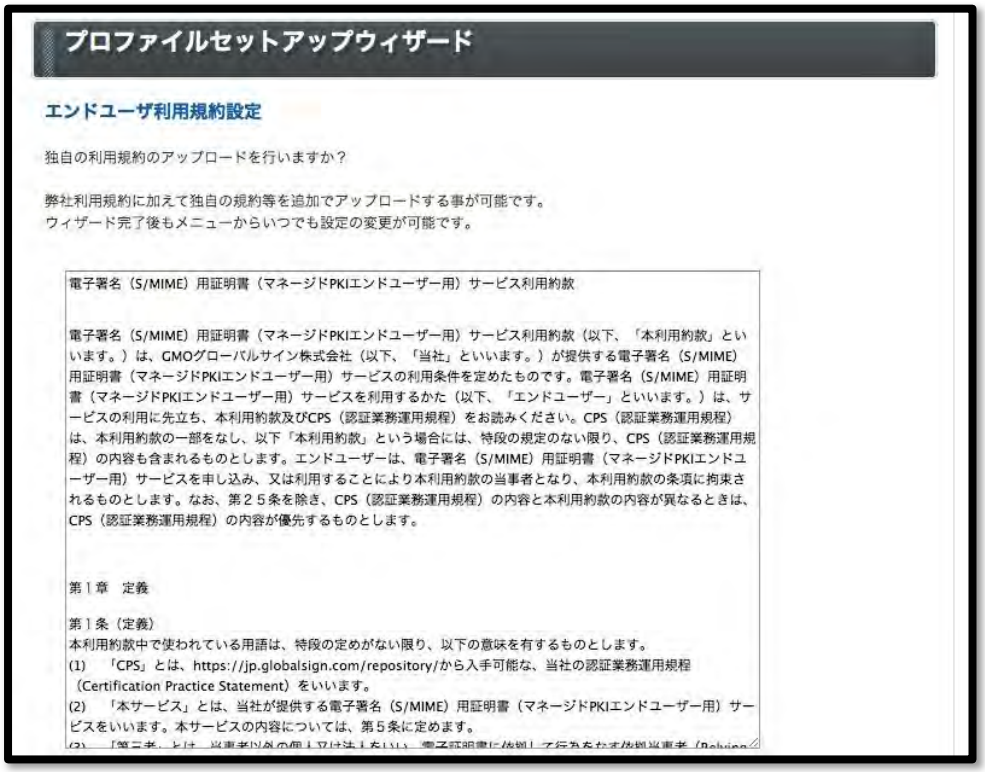
〈メールテンプレート編集時の注意点 〉
※初期設定でそのままご利用いただけるテンプレートになっています。
※テンプレートの編集は可能ではございますが、初期設定で使用されている変数は変更されないことを推奨いたします。
（変数まで変更してしまうと、想定した挙動にならない恐れがあります。）

8.「ポータル画面設定」の項目では、エンドユーザ向けポータル画面のページタイトルやロゴ・フッダー画像を編集することができます。
こちらの対応が必要な方のみ編集を行い、「次へ」をクリックして進みます。
※詳細につきましては、P86～をご覧ください。

9.「エンドユーザ利用規約設定」の項目では、エンドユーザ向けの利用規約に独自の内容を追加でアップロードすることができます。
こちらの対応が必要な方のみ編集を行い、「次へ」をクリックして進みます。

※利用約款をカスタイマイズした場合、弊社標準の利用約款が優先的に表示されますが、GS パネル内で「追加した利用約款をグローバルサインの約款と同時に表示する」にチェックをいれることで、弊社標準の利用約款と、カスタマイズした利用約款の 2 つを表示させることができます。

※利用約款のカスタマイズをしていない場合は、表示の変更はありません。



以上で、プロファイルのセットアップウィザードは完了です。
P80「プロファイル設定」より各設定をご確認ください

2.クライアント証明書の発行手順について

クライアント証明書を発行する方法は、以下の 4 通りです。
各方法別の違いを参考に、お客様の運用に合った方法をお選びください。

A:**「証明書発行」**
→ マネージド PKI Lite の管理者が、個別に申請し、ユーザ向けに証明書取得メールを手配する方法です。
※P22～よりご参照ください。

B:**「証明書発行（一括）」**
→ マネージド PKI Lite の管理者が、CSV ファイルに情報を入力して一括申請し、ユーザ向けに証明書取得メールを手配する方法です。
※P24～よりご参照ください。

C:**「証明書発行（管理者一括）」**
→ マネージド PKI Lite の管理者が、CSV ファイルで一括申請し、証明書の取得もユーザに代わって一括で行う方法です。（後ほどユーザに手動で配布）
※P32～よりご参照ください。

D:**「ユーザによる申請」**
→ 証明書のユーザがポータル画面より申請を行う方法です。
※P41～よりご参照ください。

【参考】クライアント証明書の各発行方法による違い

証明書の申請方法	申請	取得
A:証明書発行	管理者	ユーザ
B:証明書発行（一括）	管理者	ユーザ
C:証明書発行（管理者一括）	管理者	管理者
D:ユーザによる申請	ユーザ	ユーザ

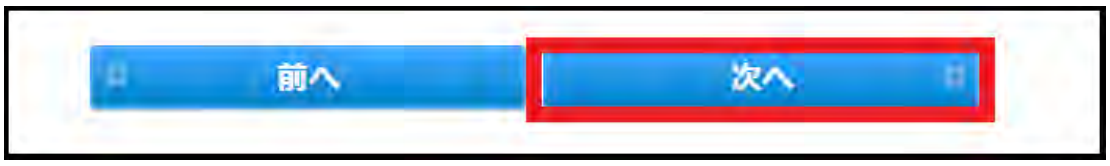
以降で、各申請方法別の詳しい手順をご紹介します。

A:「証明書発行」の申請～発行までの手順

1. GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。
（管理者証明書で認証を行います。）
アクセス後、「証明書発行（一括）」をクリックしてください。

2.発行したい証明書のプロファイル ID・ライセンスを各1つずつ選択し、「次へ」進みます。

3.発行する証明書の情報を入力し、画面下部の「次へ」進みます。
※証明書申請時の項目の詳細については、P42～よりご確認ください。



4.発行する証明書の情報を確認し、画面下部の「完了する」を押し、次へ進みます。

5.申請完了後の画面です。

6. 手順 3 にてご登録のメールアドレス宛に「電子証明書取得のお願い」メールが送信されますので、メールに記載の URL にアクセスし、インストール作業を行ってください。

メールから証明書を取得する方法は、P58「4. クライアント証明書の格納先について」をご確認ください。

※申請した証明書の情報は、P59「5. クライアント証明書を確認・キャンセル・再発行・失効したい」の証明書一覧より確認することができます。

B:「証明書発行（一括）」の申請～発行までの手順

本方法は、管理者が CSV ファイルに情報を入力して一括申請し、ユーザ向けに証明書取得メールを手配する方法です。

＜証明書発行（一括）の申請方法における注意点＞

※2024年12/9以降、個人名用ライセンスを利用してS/MIME用中間CAから発行されるクライアント証明書において、証明書発行（一括）、証明書発行（管理者一括）の際に使用するCSVのCommonNameフィールドの記載方法にも変更があります。

CommonNameフィールドに、TrueまたはONを入力した場合：SANRFC822EmailAddressに指定した値がコピーされます。

CommonNameフィールドに、FalseまたはOFFを入力した場合：DN入力ルールに沿って指定したSurName、GivenName SurName、Pseudonymのいずれかの値がコピーされます。

※CommonNameに利用しない場合でも、CSVには、SurName、GivenName、Pseudonymの各DN項目を含める必要があります。

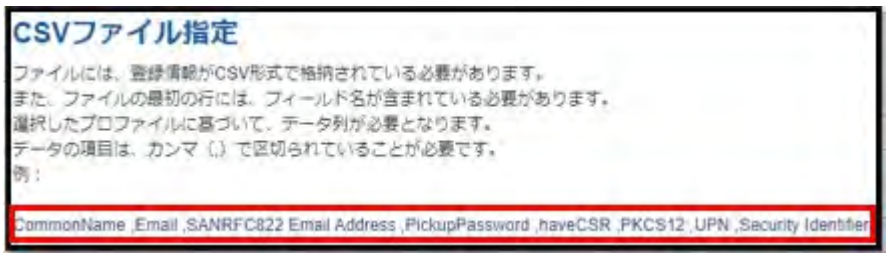
CommonName	DN			CommonName にコピーされる値
	SurName	GivenName	Pseudonym	
True/On	Yamada	Taro		taro.yamada@globalsign.com
False/OFF	Yamada			Yamada
False/OFF	Yamada	Taro		Taro Yamada
False/OFF			abc123	abc123

1.一括申請に必要な CSV ファイルを作成します。入力する項目は以下の通りです。
一行目に項目名を入れて作成してください。
※UPN、SID を使用する場合、値を入力してください。

＜CSV ファイルの作成例＞

＊【S/MIME BR(Legacy)対応用中間 CA】のプロファイルから「.pfx（PKCS#12）としてダウンロードする」を選択した場合、ユーザーの申請時に自動生成された鍵保護パスワードのみ利用できます。

以下の画面にて利用可能な項目を事前に確認することができます。
※図内の赤く囲った青字部分が動的に変化しますので、先頭行の項目確認としてご利用いただけます。



オプションやプロファイルの設定によって、入力項目が異なります。

	A	B	C	D	E	F	
1	CommonName	Email	SANRFC822 Email Address	PickupPassword	haveCSR	PKCS12	UPN
2	A1	sample.globalsign.com	sample.globalsign.com	AUTOGEN	FALSE	TRUE	
3	A2	sample.globalsign.com	sample.globalsign.com	AUTOGEN	FALSE	TRUE	

【アクセス認証用中間 CA にて証明書発行（一括）をご利用の場合】

項目	説明	制限事項
CommonName	コモンネーム	半角英数、または全角（UTF-8）64 文字以内
OrganizationUnit	所属 2	半角英数記号『- ._,+/()』または全角（UTF-8）64 文字以内
OrganizationUnit	所属 3	半角英数記号『- ._,+/()』または全角（UTF-8）64 文字以内
Email Address	メールアドレス 【補足】 Email Address または Contact Email Address のいずれかの入力が必須です。 いずれも連絡先メールアドレスとして、証明書取得メール等が送信されますが、証明書の DN の E にメールアドレス情報追加をご希望の場合は、Email Address の項目をご利用ください。 （双方に異なるメールアドレスを入力した場合は、Email Address の情報で上書きされます。）	半角英数 128 文字以内
SANRFC822 Email Address	証明書申請時に選択できる項目「アクセス認証に E メールアドレスを利用する」について「はい」を選択した場合、証明書内に格納される情報項目のうち、ディスティングイッシュネームの「E メールアドレス」と、「SANRFC822name」の項目に、E メールアドレスの情報が格納されます。	半角英数 128 文字以内
Contact Email Address	連絡用メールアドレス	半角英数字　8 文字～64 文字。 証明書取得用パスワードを自動生成する場合は、"AUTOGEN"を設定。

PickupPassword	証明書取得用パスワード	半角英数字 8 文字～64 文字。
haveCSR	VPN 機器等で CSR を用意している方は、"true" または "on" を設定。	true/on false/off/設定なし
PKCS12	証明書を PKCS12 形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数 128 文字以内
Security Identifier(SID)	セキュリティ識別子	半角英数-（ハイフン）128 文字以内

【S/MIME BR(Legacy)対応用中間 CA にて証明書発行（一括）をご利用の場合】

項目	説明	制限事項
CommonName	コモンネーム ※S/MIME BR(Legacy)対応用中間 CA 選択時は任意の値は設定することができません。 ※利用するライセンスにより、CN に設定できる値が異なります。 ■マネージド PKI Lite byGMO 個人名用のライセンスの場合 **証明書 CN（コモンネーム）として利用できる値は、以下の通りです。** **①自社および関連会社に属する個人の E メールアドレス** **②SurName** **③SurName + GivenName** **④Pseudonym** ■マネージド PKI Lite byGMO 法人名用のライセンスの場合 **法人名、または、自社および関連会社に属する部門用メールアドレスのみ**が登録可能です。	半角英数、または全角（UTF-8）64 文字以内
Email Address	メールアドレス 証明書の DN の E にも追加をご希望の場合は、Email Address にも SANRFC822 Email Address と同じメールアドレスを入力してくださ い。 （異なるメールアドレスを入力した場合は SANRFC822 Email Address の情報で上書きされます。）	半角英数 128 文字以内
SANRFC822 Email Address ※1	S/MIME でのご利用ではメールアドレスのご登録が必要な項目です。 SANRFC822 Email Address は連絡用メールアドレスにもなり、証明書取得メール等が送信されます。 必須項目ですので、必ず入力してください。	Email Address

PickupPassword	証明書取得用パスワード	半角英数字 8 文字～64 文字。 証明書取得用パスワードを自動生成する場合は、 "AUTOGEN"を設定。
haveCSR	VPN 機器等で CSR を用意している方は、"true" または "on" を設定。	true/on false/off/設定なし
PKCS12	証明書を PKCS12 形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数 128 文字以内
Security Identifier(SID)	セキュリティ識別子	半角英数-（ハイフン）128 文字以内
GivenName	名前 ※SurName と組み合わせることでコモンネームとして利用可能です。	半角英数、または全角（UTF-8）31 文字以内
SurName	名字 ※コモンネームとして単体で利用可能です。	半角英数、または全角（UTF-8）31 文字以内
Pseudonym	スードニム ※コモンネームとして単体で利用可能です。 スードニムとは、ユーザ個人に関連付けられた識別子です。 第三者が個人を特定可能なニックネームなどはご利用になれません。 管理者が、当該識別子をもとにユーザ個人を特定できないものもご利用になれません。	半角英数、または全角（UTF-8）64 文字以内

※1）SANRFC822 Email Address とは、S/MIME 利用のために利用される証明書内のフィールドです。
本項目にメールアドレスが入っていること、【S/MIME BR(Legacy)対応用中間 CA 】が選択されていることが S/MIME 利用の条件です。
【S/MIME BR(Legacy)対応用中間 CA】の場合は、事前にドメイン審査を完了した上で、証明書発行申請時にメールアドレスを入力いただくことで、本項目にもメールアドレスが自動追加されます。

2.GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。（管理者証明書で認証を行います。）
アクセス後、「証明書発行（一括）」をクリックしてください。

3. 発行したい証明書のプロファイル ID・ライセンスを各1つずつ選択し、「次へ」進みます。

4.申請に使用する CSV ファイルを指定します。
「参照」ボタンより 1.で作成したCSV ファイルを選択し、「アップロード」ボタンをクリックします。
完了後、「次へ」をクリックして進みます。

CSVファイル指定

ファイルには、登録情報がCSV形式で格納されている必要があります。
また、ファイルの最初の行には、フィールド名が含まれている必要があります。
選択したプロファイルに基づいて、データ列が必要となります。
データの項目は、カンマ (,) で区切られていることが必要です。
例：

CommonName ,Email ,SANRFC822 Email Address ,PickupPassword ,haveCSR ,PKCS12 ,UPN ,Security Identifier ,GivenName ,SurName ,Pseudonym

true ,kate.jones@globalsign.com ,kate.jones@globalsign.com ,9o7t9ghsa3 ,true ,false ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789-012345
false ,Jennifer.jones@globalsign.com ,Jennifer.jones@globalsign.com ,9o7t9ghsa3 ,false ,false ,admin@globalsign.com ,S-1-1-11-0123456789-012345678
false ,George.jones@globalsign.com ,George.jones@globalsign.com ,9o7t9ghsa3 ,false ,true ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789-

項目	説明	制限事項
CommonName	メールアドレスを利用する場合はTrue/ON。 名前またはPseudonymを利用する場合は False/OFF。 個人名は名前と名字からコピーされます。 PseudonymはPseudonymからコピーされます。	E =True/ON Name or Pseudonym=False/OFF
Email Address	入力値が、「Email Address」≠「SAN RFC822 Email Address」となる場合、「SAN RFC822 Email Address」の値で上書きとなります。	半角英数128文字以内
SANRFC822 Email Address	SANRFC822 Email Address	Email Address
PickupPassword	証明書取得用パスワード	半角英数字　8文字～64文字。証明書取得用パスワードを自動生成する場合 は、"AUTOGEN"を設定。
haveCSR	VPN機器等でCSRを用意している方は、"true"または "on" を設定。	true/on false/off/設定なし
PKCS12	証明書をPKCS12形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数128文字以内
Security Identifier	セキュリティ識別子	半角英数-（ハイフン） 128文字以内
GivenName	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）31文字以内
SurName	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）31文字以内
Pseudonym	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）64文字以内

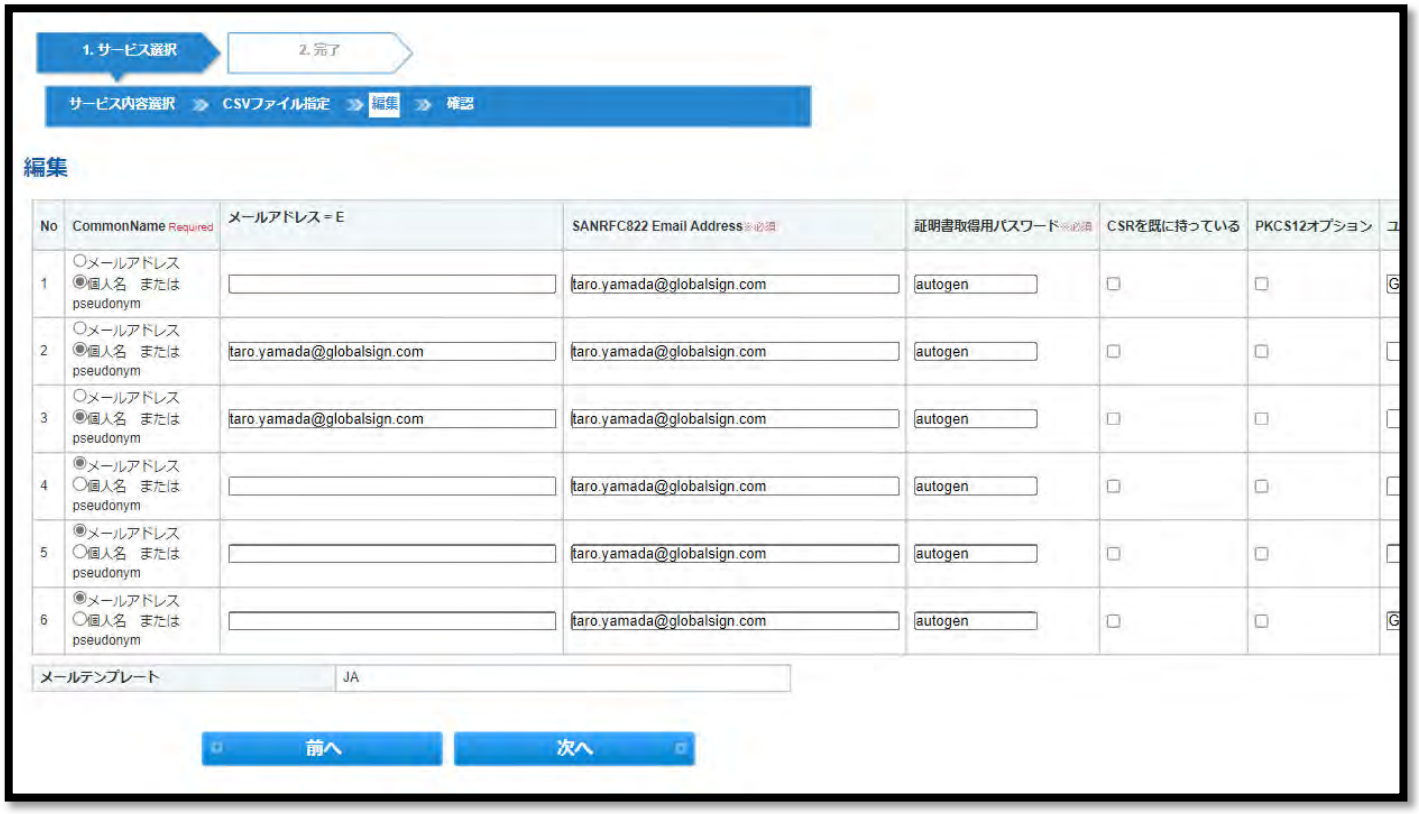
CSVファイル	EPKIPSsmimeSample.csv ファイルの選択　ファイルが選択されていません　アップロード

メールテンプレート	
適用するメールテンプレートを選択してください	日本語 - JA

ご注意：以前「MS SmartCard Logon」と表記していた項目名を、「UPN」に変更いたしました。

前へ　次へ

5.アップロードされたCSV ファイルの確認画面が表示されます。
内容を確認して次へ進めば、登録は完了です。



6.登録したメールアドレス宛てに、証明書取得メールが送信されます。
事前に設定したパスワードをユーザに伝えてください。
※もしパスワードを紛失した場合、GS パネルのオーダー一覧より該当の証明書を検索することで、確認が可能です。

ユーザが証明書を取得する方法は、P58「4. クライアント証明書の格納先について」をご確認ください。

C:「証明書発行（管理者一括）」の申請～発行までの手順

本方法は、管理者が証明書を一括で取得することで、ユーザによる証明書取得の作業負担を削減することができます。
ただし、本方法で発行された証明書は更新が不可となりますのでご注意ください。
有効期限が近くなりましたら、都度新規にて証明書を申請いただきますようお願いいたします。

＜証明書発行（管理者一括）の申請方法における注意点＞
※2024年12/9以降、個人名用ライセンスを利用してS/MIME用中間CAから発行されるクライアント証明書において、証明書発行（一括）、証明書発行（管理者一括）の際に使用するCSVのCommonNameフィールドの記載方法にも変更があります。

CommonNameフィールドに、TrueまたはONを入力した場合：SANRFC822EmailAddressに指定した値がコピーされます。

CommonNameフィールドに、FalseまたはOFFを入力した場合：DN入力ルールに沿って指定したSurName、GivenName SurName、Pseudonymのいずれかの値がコピーされます。

※CommonNameに利用しない場合でも、CSVには、SurName、GivenName、Pseudonymの各DN項目を含める必要があります。

CommonName	DN			CommonName にコピーされる値
	SurName	GivenName	Pseudonym	
True/On				taro.yamada@globalsign.com
False/OFF	Yamada			Yamada
False/OFF	Yamada	Taro		Taro Yamada
False/OFF			abc123	abc123

＊こちらの方法で証明書を申請・発行した場合、GS パネル上で取得できる証明書は PKCS12 形式のみです。

＊【S/MIME BR(Legacy)対応用中間 CA】のプロファイルから「.pfx（PKCS#12）としてダウンロードする」を選択した場合、GS パネル上で自動生成されたパスワードのみ利用可能です。
CSV 利用時は【AUTOGEN】を使用してください。
（半角英数大文字小文字記号含む 17 桁以上）

＊こちらの方法で発行する証明書には、事前にメールドメインの審査を完了しなければ、メールアドレスを記載することができません。（電子メールでの利用、S/MIME としての利用ができなくなります。）
メールドメインの審査については P93～をご参照ください。

＊証明書の有効期限が 30 日前になると、申請者（証明書管理者）宛に期限通知メールが送付されます。
継続利用される場合は、証明書の有効期限が切れる前に再度証明書の申請を行ってください。

「メールテンプレート管理」で送信設定を無効に設定している場合は送付されません。
メールテンプレート管理については P88～をご参照ください。

「更新タイプ」を"クイック"に設定している場合は、期限通知メールは送付されませんのでご注意ください。
更新タイプについては P43をご参照ください。

1.　一括申請に必要な CSV ファイルを作成します。
入力する項目は以下の通りです。一行目に項目名を入れて作成してください。
※プロファイルの設定により、指定する項目に増減があります。

【アクセス認証用中間 CA にて証明書発行（管理者一括）をご利用の場合】

項目	説明	制限事項
CommonName	コモンネーム	半角英数、または全角（UTF-8）64 文字以内
OrganizationUnit	所属 2	半角英数記号『- ._,+/()』または全角（UTF-8）64 文字以内
OrganizationUnit	所属 3	半角英数記号『- ._,+/()』または全角（UTF-8）64 文字以内

Email Address	メールアドレス 【補足】 Email Address または Contact Email Address のいずれかの入力が必須です。 いずれも連絡先メールアドレスとして、証明書取得メール等が送信されますが、証明書の DN の E にメールアドレス情報追加をご希望の場合は、Email Address の項目をご利用ください。 （双方に異なるメールアドレスを入力した場合は、Email Address の情報で上書きされます。）	半角英数 128 文字以内
SANRFC822 Email Address	証明書申請時に選択できる項目「アクセス認証に E メールアドレスを利用する」について「はい」を選択した場合、証明書内に格納される情報項目のうち、ディスティングイッシュネームの「E メールアドレス」と、「SANRFC822name」の項目に、E メールアドレスの情報が格納されます。	半角英数 128 文字以内
Contact Email Address	連絡用メールアドレス	半角英数字　8 文字～64 文字。 証明書取得用パスワードを自動生成する場合は、"AUTOGEN"を設定。
PickupPassword	証明書取得用パスワード	半角英数字 8 文字～64 文字。
haveCSR	VPN 機器等で CSR を用意している方は、"true" または "on" を設定。	true/on　false/off/設定なし
PKCS12	証明書を PKCS12 形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数 128 文字以内
Security Identifier(SID)	セキュリティ識別子	半角英数-（ハイフン）128 文字以内

【S/MIME BR(Legacy)対応用中間 CA にて証明書発行（管理者一括）をご利用の場合】

項目	説明	制限事項
CommonName	コモンネーム ※S/MIME BR(Legacy)対応用中間 CA 選択時は任意の値は設定することができません。 ※利用するライセンスにより、CN に設定できる値が異なります。 ■マネージド PKI Lite byGMO 個人名用のライセンスの場合 **証明書 CN（コモンネーム）として利用できる値は、以下の通りです。** **①自社および関連会社に属する個人の E メールアドレス** **②SurName** **③SurName + GivenName** **④Pseudonym** ■マネージド PKI Lite byGMO 法人名用のライセンスの場合 **法人名、または、自社および関連会社に属する部門用メールアドレスのみ**が登録可能です。	半角英数、または全角（UTF-8）64 文字以内
Email Address	メールアドレス 証明書の DN の E にも追加をご希望の場合は、Email Address にも SANRFC822 Email Address と同じメールアドレスを入力してください。 （異なるメールアドレスを入力した場合は SANRFC822 Email Address の情報で上書きされます。）	半角英数 128 文字以内
SANRFC822 Email Address ※1	S/MIME でのご利用ではメールアドレスのご登録が必要な項目です。 SANRFC822 Email Address は連絡用メールアドレスにもなり、証明書取得メール等が送信されます。 必須項目ですので、必ず入力してください。	Email Address
PickupPassword	証明書取得用パスワード	半角英数字 8 文字～64 文字。 証明書取得用パスワードを自動生成する場合は、"AUTOGEN"を設定。
haveCSR	VPN 機器等で CSR を用意している方は、"true" または "on" を設定。	true/on false/off/設定なし
PKCS12	証明書を PKCS12 形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数 128 文字以内

Security Identifier(SID)	セキュリティ識別子	半角英数-（ハイフン） 128 文字以内
GivenName	名前 ※SurName と組み合わせることでコモンネームとして利用可能です。	半角英数、または全角 （UTF-8）31 文字以内
SurName	名字 ※コモンネームとして単体で利用可能です。	半角英数、または全角 （UTF-8）31 文字以内
Pseudonym	スードニム ※コモンネームとして単体で利用可能です。	半角英数、または全角 （UTF-8）64 文字以内

※1）SANRFC822 Email Address とは、S/MIME 利用のために利用される証明書内のフィールドです。本項目にメールアドレスが入っていること、【S/MIME BR(Legacy)対応用中間 CA 】が選択されていることがS/MIME 利用の条件です。
【S/MIME BR(Legacy)対応用中間 CA】の場合は、事前にドメイン審査を完了した上で、証明書発行申請時にメールアドレスを入力いただくことで、本項目にもメールアドレスが自動追加されます。

2.GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。
（管理者証明書で認証を行います。）
アクセス後、「証明書発行（管理者一括）」をクリックしてください。

3.証明書の発行に利用するプロファイル ID、ライセンスを選択し、「次へ」をクリックして進みます。

4.申請に使用する CSV ファイルを指定します。
「参照」ボタンより 1.で作成したCSV ファイルを選択し、「アップロードボタン」をクリックしてください。
完了後、「次へ」をクリックして進みます。
一回に最大 200 件までアップロードすることが可能です。

CSVファイル指定

ファイルには、登録情報がCSV形式で格納されている必要があります。
また、ファイルの最初の行には、フィールド名が含まれている必要があります。
選択したプロファイルに基づいて、データ列が必要となります。
データの項目は、カンマ (,) で区切られていることが必要です。
例：

CommonName ,Email ,SANRFC822 Email Address ,PickupPassword ,haveCSR ,PKCS12 ,UPN ,Security Identifier ,GivenName ,SurName ,Pseudonym

true ,kate.jones@globalsign.com ,kate.jones@globalsign.com ,9o7t9ghsa3 ,true ,false ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789-012345
false ,Jennifer.jones@globalsign.com ,Jennifer.jones@globalsign.com ,9o7t9ghsa3 ,false ,false ,admin@globalsign.com ,S-1-1-11-0123456789-012345678
false ,George.jones@globalsign.com ,George.jones@globalsign.com ,9o7t9ghsa3 ,false ,true ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789-

項目	説明	制限事項
CommonName	メールアドレスを利用する場合はTrue/ON。 名前またはPseudonymを利用する場合は False/OFF。 個人名は名前と名字からコピーされます。 PseudonymはPseudonymからコピーされます。	E =True/ON Name or Pseudonym=False/OFF
Email Address	入力値が、「Email Address」≠「SAN RFC822 Email Address」となる場合、「SAN RFC822 Email Address」の値で上書きとなります。	半角英数128文字以内
SANRFC822 Email Address	SANRFC822 Email Address	Email Address
PickupPassword	証明書取得用パスワード	半角英数字　8文字～64文字。証明書取得用パスワードを自動生成する場合 は、"AUTOGEN"を設定。
haveCSR	VPN機器等でCSRを用意している方は、"true"または "on" を設定。	true/on false/off/設定なし
PKCS12	証明書をPKCS12形式でダウンロードする場合、"true" または "on" を設定。	true/on false/off/設定なし
UPN	ユーザープリンシパル名	半角英数128文字以内
Security Identifier	セキュリティ識別子	半角英数-（ハイフン）128文字以内
GivenName	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）31文字以内
SurName	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）31文字以内
Pseudonym	企業RAは申請者個人の身元属性を裏付ける証拠を収集し、保持するものとします。	半角英数、または全角（UTF-8）64文字以内

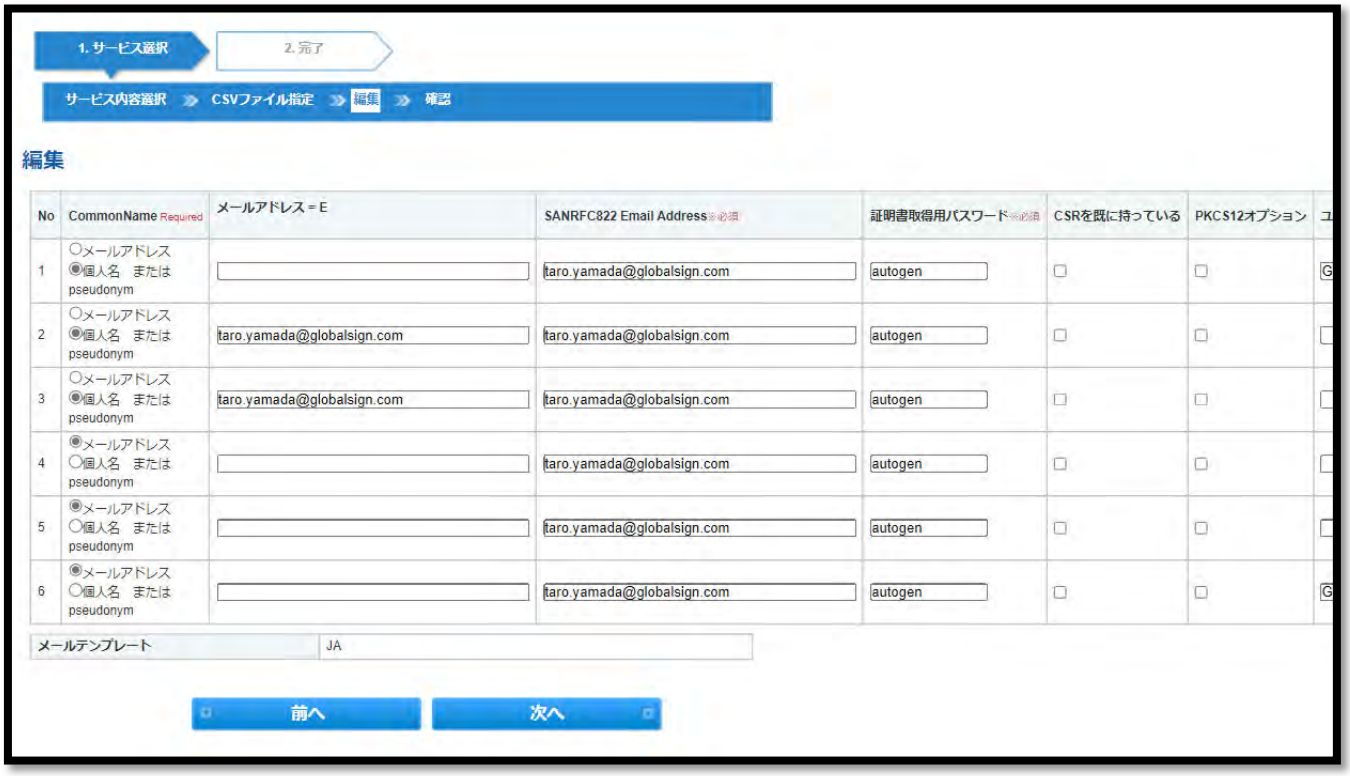
ＣＳＶファイル	EPKIPSsmimeSample.csv ファイルの選択　ファイルが選択されていません　アップロード

メールテンプレート	
適用するメールテンプレートを選択してください	日本語 - JA

ご注意：以前「MS SmartCard Logon」と表記していた項目名を、「UPN」に変更いたしました。

前へ　次へ

5.アップロードされたCSV ファイルの確認画面が表示されます。
こちらの画面で内容の確認や修正をすることができます。
内容を確認して「次へ」をクリックすると、登録は完了です。

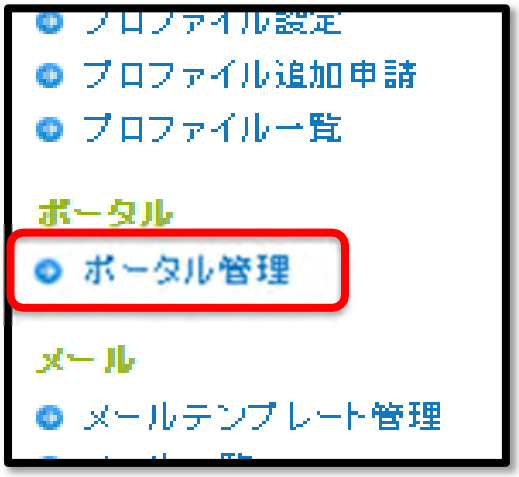


6.左部メニューの「管理者一括発行履歴」に進み、証明書を取得します。
「検索」をクリックし、オーダーの一覧を表示します。

7.一覧内の「ダウンロード」ボタンをクリックすると.zip ファイルで証明書を一括取得することができます。
ボタンがグレー表示の場合は、証明書を作成中ですので時間を置いてから再度お試しください。
※PKCS12 形式のパスワードは、証明書ダウンロード後、インポート時に必要となります。
発行された証明書と一致させてください。

D: ユーザによる申請～発行までの手順

1.マネージドPKI の管理者は、ユーザ（証明書を取得したい人）に、申請用のポータルURL をご案内ください。
URL は、左部メニューの「ポータル管理」より確認することができます。



いずれのリンクとも、ユーザ側で証明書情報の入力が求められますが、それぞれ以下の特徴があります。

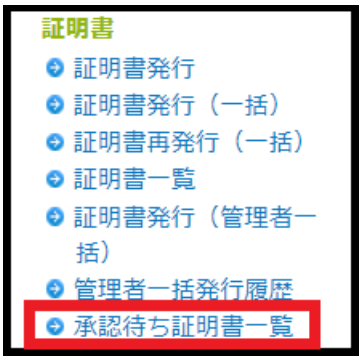
＊「URL」リンクからの申し込みの場合、
→ ユーザが指定する任意の鍵生成オプションを用いて、証明書を配布

＊「URL（PKCS12 オプション）」リンクからの申し込みの場合、
→ PKCS12 形式のファイルで証明書をダウンロード

2.ユーザが案内されたポータル URL にアクセスし、証明書を申請します。
発行したい証明書の情報を入力後、「次へ」ボタンを押し、約款に同意して完了です。
申請時の入力項目の詳細に関しては P46～をご覧ください。

※こちらの申請画面については、「ポータル管理」からヘッダ・フッダ画像や、ページ上部の文言をカスタマイズすることが可能です。
詳しくは P86～をご覧ください。

3.ユーザからの申請が完了すると、管理者にメールで通知がされます。
証明書の発行には管理者による承認が必要です。
GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。（管理者証明書で認証を行います。）



4.管理者は申請された証明書を確認し、承認したい証明書にチェックを入れて、「承認処理」をクリックします。
同様に、キャンセル処理をクリックすると申請はキャンセルされます。

5.確認画面で内容を確認し、「次へ」をクリックすると承認は完了です。
承認後、ユーザへ証明書取得のメールが送信されますので、端末にインストールし、ご利用ください。

証明書を取得する方法は、P58～をご確認ください。

クライアント証明書の発行手順について(更新)

プロファイル設定時に選択いただきました更新タイプによって更新の流れが異なります。
クライアント証明書の更新タイプは以下の3種類から選択できます。

■自動更新無し(デフォルト)
ユーザからの更新申請を管理者(または承認権限を持つユーザ)が承認する必要があります。

■自動更新有り
ユーザからの更新申請後、すぐに証明書取得メールが送信されます。

■クイック更新
証明書の有効期限 30 日前に一度だけ送信される証明書取得メールより、ユーザはすぐに証明書を取得できます。

	ユーザからの更新申請	管理者による承認
自動更新無し	必要	必要
自動更新有り	必要	不要
クイック更新	不要	不要

更新案内メールテンプレートには、初期設定で2種類の更新申請用 URL があります。

お客様の状況に合わせて、どちらの URL から更新するかご選択ください。


◆更新手続き用URL

<有効なクライアント証明書をお持ちの方>
https://system.globalsign.com/cr/public/auth/certificate/renewalorder.do
上記URLにアクセス後、更新を行う証明書でクライアント認証を行い、
証明書を取得してください。

<クライアント証明書をお持ちでない方>
https://system.globalsign.com/cr/public/certificate/renewalorder.do?p=70b9520a25193ec28c
上記URLにアクセス後、前回証明書取得時に使用したパスワードを入力し、
証明書を取得してください。パスワードが不明な場合、取得いただけません。

〈更新対象の証明書がある場合の URL〉

更新用の URL に接続すると、クライアント認証が行われます。

複数の証明書がある場合は、どの証明書を更新するかを選択してください。

〈更新対象の証明書がない場合のURL〉

更新用の URL に接続後、前回証明書を取得した際のパスワードをご入力いただく必要があります。

更新対象の証明書がインストールされていない環境から更新申請をする場合にご利用ください。

上記どちらかの URL に接続後、証明書の申請画面へとお進みください。

クライアント証明書申請時の項目について（新規・更新）

証明書の申請時は以下のようなフォームが表示されますので、必要な箇所を入力し、「次へ」をクリックしてください。
※申請方法、選択されるプロファイルによって、証明書の入力内容は異なります。

それぞれの入力項目の意味は以下の通りです。
【S/MIME BR(Legacy)対応用中間 CA】のプロファイルの場合

【アクセス認証用中間 CA】のプロファイルの場合

証明書情報入力

国/地域 = C	日本 - JP
都道府県 = S ※半角英数、または全角（UTF-8）128文字以内	Tokyo
市区町村 = L ※半角英数、または全角（UTF-8）128文字以内	Shibuya
組織名 = O ※半角英数、または全角（UTF-8）64文字以内	GlobalSign K.K.
部署名 = OU	
氏名 = CN※必須 ※半角英数、または全角（UTF-8）64文字以内	
利用者メールアドレス※必須	
アクセス認証にEメールアドレスを利用する ※必須	◉いいえ 〇はい
ユーザープリンシパル名	
セキュリティ識別子	
鍵生成オプション	◉ .pfx（PKCS#12）としてダウンロードする 証明書取得時に、証明書、中間CA証明書、秘密鍵が1つにパッケージングされた.pfxファイルとしてダウンロードします。.pfxファイルは新しいパスワードを設定して鍵を保護する必要があります。 〇 CSRによる発行 HSM等で鍵を管理するためにCSRで申請が必要な場合は、こちらをご選択ください。 〇 Microsoft EdgeのInternet Explorer互換モードによる発行 ブラウザ鍵生成機能を用いて証明書を発行し、USBトークンに格納します。
メールテンプレート※必須	日本語 - JA
証明書取得用パスワード※必須	※半角英数8文字以上 パスワード自動生成 パスワード自動生成ボタンを押下すると、ランダムなパスワードを自動作成／セットを行います。
証明書取得用パスワード（確認用）※必須	※半角英数8文字以上
メモ欄	

〈証明書申請時の時の注意点 〉

※プロファイル情報の変更や複数のプロファイルにて証明書の発行を行いたい場合は、別途プロファイルを追加登録することで発行可能です。
詳しくは P68 をご参照ください。

※更新の場合、コモンネーム、メールアドレス、OU は変更できません。

※以下の文字はディスティングイッシュネーム情報としてご登録できません。

「$, ¥n, ¥r ,; ,! ,¥u ,0000 ,% ,` ,? ,~」

各申請項目の説明(ポータル画面)

ディスティングイッシュネーム 各項目名	説明	入力例
CN(Common Name)※必須	担当者の氏名が該当いたします。 ※2013 年 1 月 28 日より日本語表示に対応 **※利用する中間 CA とライセンスの組み合わせにより、CN に設定できる値が異なります。** **【 S/MIME BR(Legacy)対応用中間 CA 証明書】** **「マネージド PKI Lite byGMO 個人名用」のライセンスの場合：証明書 CN(コモンネーム)として利用できる値は、以下の通りです。** **①自社および関連会社に属する個人の E メールアドレス** **②SurName** **③SurName + GivenName** **④Pseudonym** **「マネージド PKI Lite byGMO 法人名用」のライセンスの場合：法人名、または、自社および関連会社に属する部門用メールアドレスのみが登録可能です。** **【アクセス認証用中間 CA 証明書】** **「マネージド PKI Lite byGMO 個人名用」のライセンスの場合：証明書のコモンネーム(CN)に、任意の値を設定可能です。** **「マネージド PKI Lite byGMO 法人名用」のライセンスの場合：利用できません。個人名用ライセンスをお申込みください。**	Taro Yamada
O(Organization)※必須	組織の正式名称です。 ※プロファイル情報より自動入力	GlobalSign K.K.
OU(Organization Unit)	組織での部署名です。最大3つまで追加可能です。 ※S/MIME BR(Legacy)対応用中間 CA では設定不可	Sales Dept
L(City or Locality)	組織が置かれている市区町村です。 ※プロファイル情報より自動入力	Shibuya
S(State or Province)	組織が置かれている都道府県です。 ※プロファイル情報より自動入力	Tokyo
C(Country)※必須	国を示す 2 文字の ISO 略語です。 ※プロファイル情報より自動入力	日本-JP

OrganizationIdentifier(2.5.4.97) ※S/MIME BR(Legacy)対応用中間 CA のみ必須	プロファイル申請組織を識別するための情報です。OID の分類には、VAT、GOV、NTR の 3 種類があります。 ※プロファイル情報より自動入力	1011001040181
E(メールアドレス)※必須	**「アクセス認証に E メールアドレスを利用する」**で「はい」を選択した場合は、メールアドレス情報は証明書の DN の E に格納されます。 **【S/MIME BR(Legacy)対応用中間 CA】のプロファイルの場合、メールアドレスは証明書内の「SANRFC822name」フィールドに格納されますが、証明書にメールアドレスを含むには「はい」を選択してください。 ※登録済みのメールドメインリストからドメインを選択する必要があります。** 【アクセス認証用中間 CA】のプロファイルの場合、証明書にメールアドレス情報を格納できますが、 S/MIME 利用はできませんので、ご注意ください。	support-jp@globalsign.com
GivenName	名前 ※SurName と組み合わせることでコモンネームとして利用可能です。	半角英数、または全角（UTF-8）31 文字以内
SurName	名字 ※コモンネームとして単体で利用可能です。	半角英数、または全角（UTF-8）31 文字以内
Pseudonym	スードニム ※コモンネームとして単体で利用可能です。 スードニムとは、ユーザ個人に関連付けられた識別子です。 第三者が個人を特定可能なニックネームなどはご利用になれません。 管理者が、当該識別子をもとにユーザ個人を特定できないものもご利用になれません。	半角英数、または全角（UTF-8）64 文字以内

その他申請時のオプション	説明
ユーザープリンシパル名	ユーザー プリンシパル名 (UPN):マイクロソフト アクティブディレクトリ(AD)の登録名です。 AD へのスマートカードログイン時に証明書を参照します。
セキュリティ識別子(Security Identifier:略称 SID)	セキュリティ識別子(SID):コンピュータまたはドメインコントローラがユーザを識別するために使用する固有の ID 番号です。 Windows コンピューターからコマンド「whoami / user」を使用して生成できます。 **2025 年 2 月 11 日以降、Active Directory 証明書サービスをでクライアント証明書を使用しているユーザーはこの値が必須となります。**
CSR による発行	証明書取得メールのリンク先で CSR 登録フォームに証明書取得時に、CSR と引き換えに、証明書を発行することができます。 VPN 機器等で CSR を用意している方はこちらの項目にチェックをつけてください。
PKCS12 オプション	通常、クライアント証明書を発行する際には、証明書を取得するブラウザの鍵生成機能を利用しますが、こちらの項目にチェックをつけると、グローバルサイン側で秘密鍵や証明書の生成を行い、PKCS12 形式のファイルとしてダウンロードできるようになります。
メールテンプレート **※必須**	オーダーごとに、使用するメールテンプレートを選択することができます。 英語は自動的に内容も翻訳されますが、その他の言語は翻訳されていません。 お客様ご自身にて翻訳いただく必要があります。 ※デフォルトでは日本語が自動的に選択されています。
証明書取得用パスワード ※必須	証明書取得メールを送信して 30 日後に、まだ証明書を取得していないユーザへ取得を促すメールが送信されます。 ※256 文字以内で設定してください。 ※パスワードを紛失した場合、GS パネルのオーダー一覧より該当の証明書を検索し、「編集」をクリック後ページ下部の取得用パスワードより確認できます。 【S/MIME BR(Legacy)対応用中間 CA】のプロファイルから「.pfx(PKCS#12)としてダウンロードする」を選択した場合、GS パネル上で自動生成されたパスワードのみ利用可能です。

3. クライアント証明書の再発行手順について

クライアント証明書を再発行する方法は、以下の 3 通りです。
各申請方法によって再発行手順が異なりますので、証明書発行時の申請方法をご確認ください。

＜証明書の再発行における注意点＞
・有効期限切れ・未発行・失効済み証明書に関しては再発行を行えません。

・2024年12月9日以降、証明書のDN（ディスティングイッシュネーム）情報に、新たに以下の項目を追加いたします。
「SurName（名字）」、GivenName（名前）、「Pseudonym（スードニム）」
※個人名用ライセンスを利用して【S/MIME用中間CA】から発行されるクライアント証明書が対象です。
※SurName、GivenName＋SurNameまたはPseudonymのいずれかを設定する必要があります。

・2025年5月26日以降は、SurName、GivenName＋SurNameまたはPseudonymのいずれかが適用されていない証明書は更新および再発行ができかねますのでご注意ください。

A：**証明書の再発行を 1 枚ずつ行う手順**
→ どちらの申請方法を選択されても、1枚ずつ再発行を行うことは可能です。
詳しくは P51～をご参照ください。

B：**「証明書再発行（一括）」の再発行申請～再発行までの手順**
→ 証明書発行時に「証明書発行（一括）」にて申請した場合のみ利用可能です。
マネージド PKI Lite の管理者が、CSV ファイルに情報を入力して一括申請し、ユーザ向けに証明書取得メールを手配する方法です。
詳しくは P52～をご参照ください。

C：**「証明書発行（管理者一括）」の再発行申請～再発行までの手順**
→「証明書発行（管理者一括）」にて証明書を申請した場合、証明書が発行されてから 30 日間は既存の証明書 zip ファイルがダウンロードできます。
30 日経過するとダウンロードボタンは消え、代わりに証明書再発行のボタンが表示されるようになりますので、発行済みステータスのオーダーID を含んだCSV ファイルをアップロードすることで再発行が行えます。
※200 件を超える一括申請はできません
詳しくは P54～をご参照ください。

A：証明書の再発行を１枚ずつ行う手順

1.GS パネルにログインし、「マネージドPKI」タブ内の「証明書管理」にアクセスします。
（管理者証明書による認証が行われます。）

アクセス後、「証明書一覧」をクリックしてください。

2.検索画面が表示されますので、確認したい証明書の情報を入力し、「検索」ボタンをクリックします。
表示された候補の「申請」ボタンを押下して次へ進みます。

3. 「申込証明書編集」の一番上か下にある「証明書再発行」をクリックします。
※証明書のステータスによって表示されるボタンは異なります。

4. 再発行される証明書のディスティングイッシュネームを確認し、証明書取得用パスワードを入力し、「次へ」をクリックしてください。
※再発行では、ディスティングイッシュネームの変更はできません。
※証明書発行時に必要となりますのでお忘れにならないようメモをしてください。

5. 再発行される証明書の内容を確認し、「完了する」をクリックすると再発行の申請が完了します。
登録のメールアドレスへ証明書取得メールを送信いたしますので、証明書取得用 URLにアクセスし、証明書の取得を行ってください。
※設定した証明書取得用パスワードを事前にユーザに伝えておく必要があります。

B:「証明書再発行（一括）」の再発行申請～再発行までの手順

1.GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。（管理者証明書で認証を行います。）

アクセス後、「証明書再発行（一括）」をクリックしてください。

2. 申請に使用する CSV ファイルを指定します。
「ファイルを選択」より作成したCSV ファイルを選択し、「アップロード」ボタンをクリックします。
完了後、「次へ」をクリックして進みます。

※「証明書再発行（一括）」にてお申込みいただいた証明書の中で再発行を行う証明書のオーダーID および証明書取得用パスワードを含んだCSV ファイルを作成ください。

3.アップロードされたCSV ファイルの確認画面が表示されます。
内容を確認後、「次へ」お進みください。最終的な内容確認画面が表示されますので、
「完了」をクリックし、再発行申請は完了です。

4.再発行申請完了後、登録のメールアドレス宛てに証明書取得メールを送信いたしますので、証明書取得用 URL にアクセスし、証明書の取得を行ってください。
※設定した証明書取得用パスワードを事前にユーザに伝えておく必要があります。

ユーザが証明書を取得する方法は、P58～をご確認ください。

C:「証明書発行（管理者一括）」の再発行申請～再発行までの手順

1.GS パネルにログインし、「マネージドPKI」タブ内左部メニューの「証明書管理」にアクセスします。（管理者証明書で認証を行います。）

アクセス後、「管理者一括発行履歴」をクリックしてください。

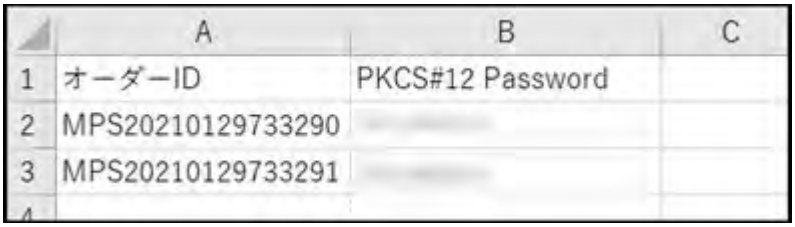
2.「検索」をクリックし、オーダーの一覧を表示します。

3.一覧内の再発行を行いたいオーダーに対して「編集」ボタンをクリック。

PKCS#12・オーダーID	編集	申請日	発行日	オーダー・ステータス
MPB202105190647	編集	2021年05月19日 14:48(GMT+09:00)	2021年05月19日 15:15(GMT+09:00)	発行済み
MPB202105190646	編集	2021年05月19日 14:45(GMT+09:00)	2021年05月19日 14:55(GMT+09:00)	発行済み

4.ページ下部の「CSV 出力」をクリックし、CSV ファイルを取得します。
取得した CSV ファイルの中身を編集し、編集が完了しましたら「再発行 Zipped PKCS#12」をクリックしてください。

※アップロードする CSV ファイルは A 列のオーダーID 以外を削除し、B 列に PKCS#12 Password のみを記載ください。



5. 編集したCSV ファイルを選択後、「アップロード」ボタンをクリックします。

完了後、「次へ」をクリックして進みます。

6.内容を確認の上、「完了する」をクリックすると、登録が完了します。

7.左部メニューの「管理者一括発行履歴」に進み、証明書を取得します。
「検索」をクリックし、オーダーの一覧を表示します。

8.一覧内の「ダウンロード」ボタンをクリックすると.zip ファイルで証明書を一括取得することができます。
ボタンがグレー表示の場合は、証明書を作成中ですので時間を置いてから再度お試しください。
※PKCS12 形式のパスワードは、証明書ダウンロード後、インポート時に必要となります。
発行された証明書と一致させてください。

4. クライアント証明書の格納先について

クライアント証明書の取得は、下記の各種ブラウザ、または携帯端末で行うことができます。
各環境により、証明書の格納場所等が異なりますのでご注意ください。

Windows	・Microsoft Edge	Windows　証明書ストア
	・Chrome	
	・Firefox	FireFox　証明書ストア
Mac	・Chrome ・Safari	Mac キーチェイン
	・Firefox	FireFox 証明書ストア
iOS	・Safari	iOS トラストストア
Android	・Chrome	証明書ストア

次のページから以下の環境における証明書の取得（インストール）手順をご案内します。
お使いの環境の手順をご確認ください。

A：ブラウザの鍵生成機能を用いた証明書の取得手順
→ブラウザの鍵生成機能を利用する場合は Microsoft Edge の Internet Explorer モードをご利用ください。
詳しくは P59～よりご参照ください。

B：PKCS12 形式での証明書の取得手順
→PKCS12 形式で証明書を申請した場合、拡張子が .pfx のファイルとしてダウンロードされます。
詳しくは P60～をご参照ください。
なお、対応可能ブラウザは以下となります。
※2017 年 9 月時点調べ。各開発元の資料に基づいて作成しております。
※アプリケーション提供元にてサポートが終了している場合、正常に動作しない可能性があります。
・Microsoft Internet Explorer 6 SP3 以降 (Windows XP SP3 以降)
・Mozilla Firefox 3.02 以降
・Apple Safari (Mac OS X 10.5 以降)
・Opera 9.50 以降
・Google Chrome
・Microsoft Edge

C：CSR を用いた証明書の取得手順
→詳しくは P63 をご参照ください。

A:ブラウザの鍵生成機能を用いた証明書の取得手順

※2022 年 6 月 16 日(木)に Internet Explorer のサポート終了が終了いたしました。
ブラウザによる鍵生成をご希望の場合は、Microsoft Edge の Internet Explorer モードをご利用ください。

【Microsoft Edge の Internet Explorer モードについて】
https://jp.globalsign.com/support/codesign/config/edge-ie-valid.html

1.件名「電子証明書取得のお願い」のメールに記載されている証明書取得用 URL にアクセスします。
申請時に設定した証明書取得用パスワードを入力して、「次へ」をクリックします。

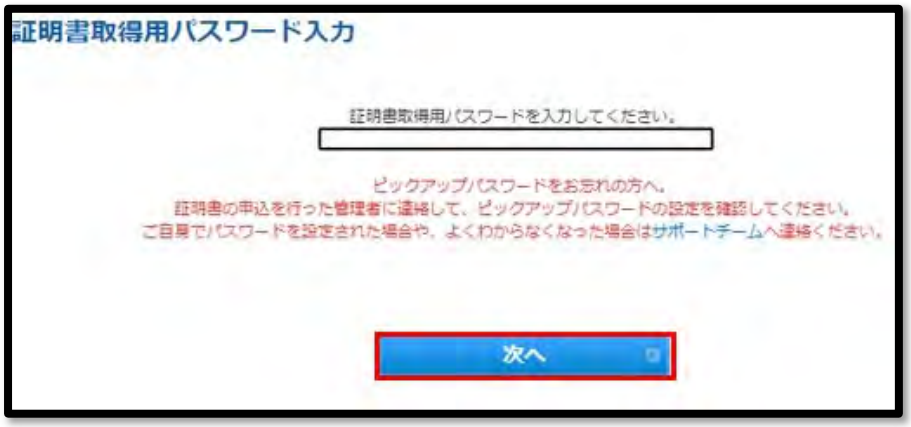
2. ActiveX コントロールの警告や以下の画面が表示された際は、「はい」をクリックします。

3. Windows の証明書ストアに証明書を格納後、証明書のエクスポートをできないようにしたい場合は、上段のチェックボックスのチェックを外し、下段の約款に同意するにチェックをして次へ進みます。
※クライアント証明書のエクスポートを行えなくすることで、証明書を利用する端末を限定することができます。

4.「証明書インストール」をクリックするとインストールが始まります。
※インストールボタンを押すと windows のインポートウィザードが立ち上がります。

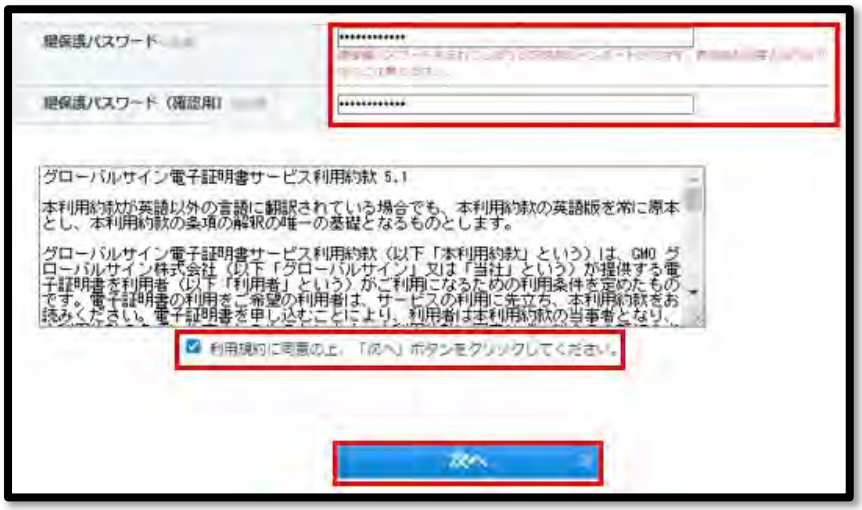
B:PKCS12 形式での証明書の取得手順

1.件名「電子証明書取得のお願い」のメールに記載されている証明書取得用 URL にアクセスします。
申請時に設定した証明書取得用パスワードを入力して、「次へ」をクリックします。

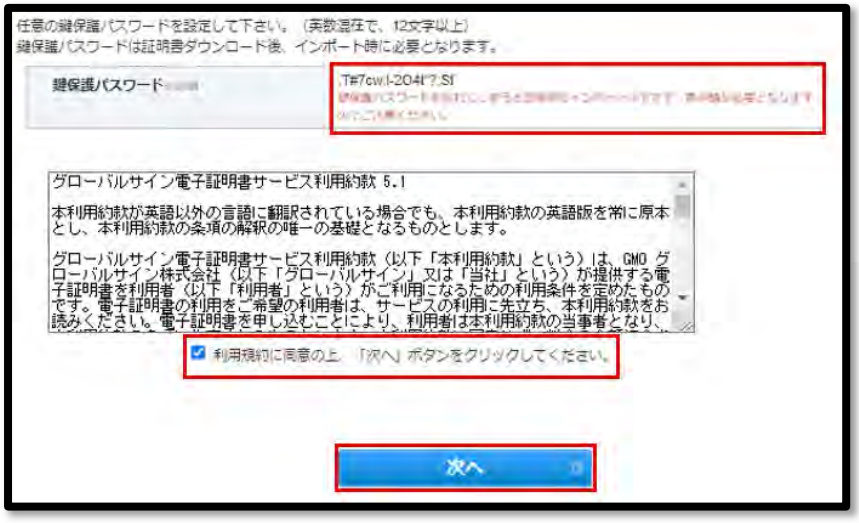


2.鍵保護パスワードを入力して、「次へ」をクリックします。
※インポート時に必要になりますので、大切に保管してください。

・アクセス認証用中間 CA のプロファイルの場合



・S/MIME BR(Legacy)対応用中間 CA のプロファイル
※自動で鍵保護パスワードが生成されます。

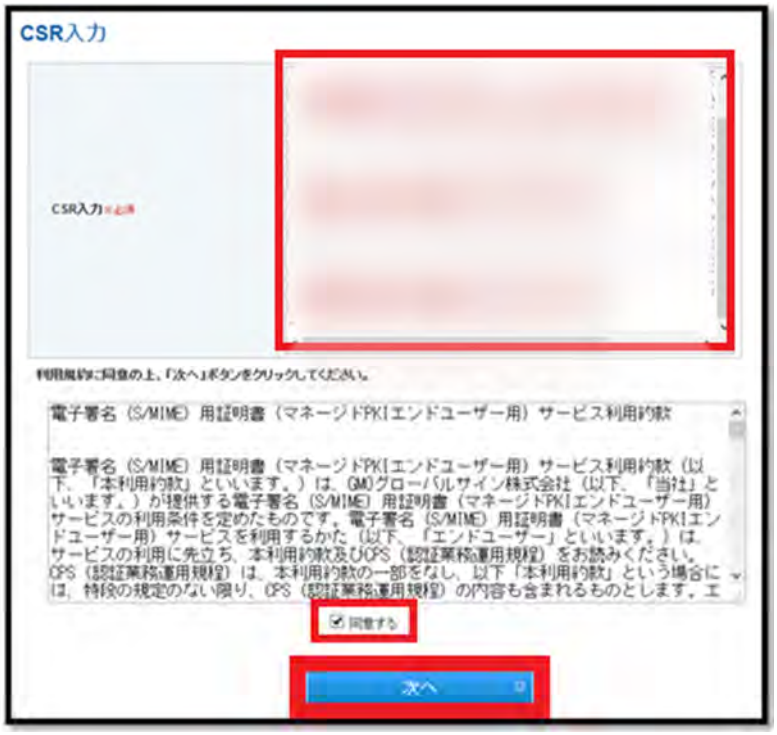


3.証明書を取得します。
ダウンロード画面が表示されますので、ダウンロードいただき、ご利用の環境にインストールを行ってください。

C：CSRを用いた証明書の取得手順

1.件名「電子証明書取得のお願い」のメールに記載されている証明書取得用 URL にアクセスします。
申請時に設定した証明書取得用パスワードを入力して、「次へ」をクリックします。

2. CSR 入力欄に CSR をコピー＆ペーストし、「次へ」をクリックします。



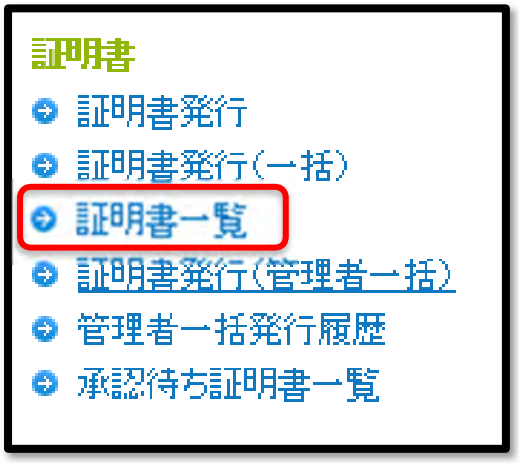
4.「証明書インストール」および「中間証明書 1 インストール」をクリックするとお客様環境にPEM 形式の証明書と中間 CA がダウンロードされますので、CSR を作成した環境にインストールし、ご利用ください。

5.クライアント証明書の確認・キャンセル・再発行・失効

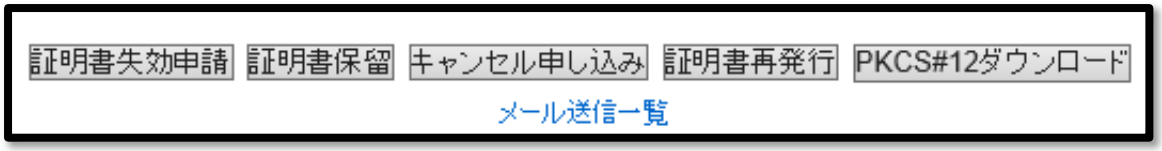
発行したクライアント証明書の内容を確認、キャンセル、再発行、失効をしたい場合は、「証明書一覧」から行うことができます。

1.GS パネルにログインし、「マネージドPKI」タブ内の「証明書管理」にアクセスします。
（管理者証明書による認証が行われます。）

2.進んだ次の画面で、左部メニューから「証明書一覧」をクリックします。



3.検索画面が表示されますので、確認したい証明書の情報を入力し、「検索」ボタンをクリックします。
表示された候補の「申請」ボタンを押下して次へ進みます。



＜各種ボタンの詳細＞

「証明書失効申請」:
証明書の紛失、盗難等で証明書を失効したい場合に利用します。
失効処理を実行すると次回発行される CRL（証明書失効リスト）に情報が反映されます。
※使用したライセンスは戻りません。

「証明書保留」:
証明書を一時的に失効します。
保留状態時には証明書が CRL に反映されます。
解除することで CRL から証明書情報が削除され、保留状態から回復します。

「キャンセル申込」:
証明書発行後 7 日以内であれば本ボタンが表示されます。
キャンセルすることにより消費されたライセンスが元にもどります。

「PKCS#12 ダウンロード」:
申請方法に関わらず、PKCS12 形式で証明書を発行した場合、発行後 30 日間はこのボタンが表示されます。
30 日経過後(31 日後)までダウンロードされなかった際は、ダウンロードボタンが自動的に削除されます。
何らかの理由で、証明書取得メールから取得されたPKCS#12 ファイルを紛失してしまった場合でも、30 日間以内であればこちらのボタンから再取得が可能です。

「証明書再発行」:
発行済みの証明書の再発行が可能です。
発行される証明書の情報や有効期限は、前回の証明書と同一になります。

「PKCS#12 証明書再発行」:
証明書発行（管理者一括）の申請方法にて証明書を発行してから 30 日経過後、こちらのボタンが表示され、PKCS#12 ファイルを再発行できるようになります。
※30 日間以内に証明書を再発行したい場合、「キャンセル申込」から発行済みの証明書をキャンセルし、再度申請から行ってください。

クライアント証明書の一括キャンセル・失効機能について

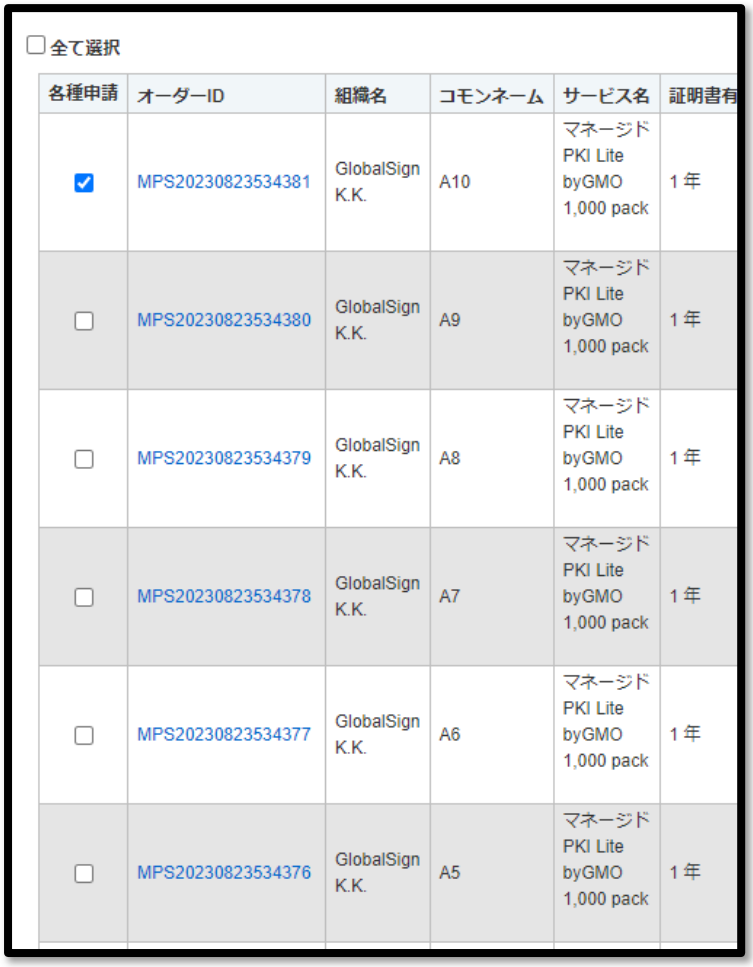
発行したクライアント証明書を一括でキャンセル、失効することができます。

1.GS パネルにログインし、「マネージドPKI」タブ内の「証明書管理」にアクセスします。
（管理者証明書による認証が行われます。）

2.進んだ次の画面で、左部メニューから「証明書一括キャンセル・失効」をクリックします。

3.検索画面が表示されますので、「キャンセル可能な証明書」または「失効可能な証明書」を選択し、ボタンをクリックします。

4.検索結果一覧より、左のチェックボックスにチェックを入れ、
ページ下部の「キャンセル申し込み」または「証明書失効申請」をクリックします。



5.選択した証明書を確認し、完了をクリックします。

6. ライセンスについて

6-1. ライセンスの残数や有効期限の確認方法

1. GS パネルにログイン後、「マネージド PKI」のタブをクリックし、左メニューのライセンス管理より「ライセンス購入履歴」を選択してください。

2. ライセンス ID などご希望の条件を指定し、「検索」をクリックしてください。
（条件の指定を行わない場合、すべてのライセンスの購入履歴が表示されます。）

3. 表示された検索結果画面の「ライセンス有効終了日」の項目にて、有効期限を確認することができます。
より詳細な情報を確認したい場合は、各ライセンス ID をクリックしてお進みください。

また、同じ項目内の「ライセンス未使用数」から、残数を確認することができます。
有効期限を迎えると、残数に関わらず使用することができなくなりますのでご注意ください。
もし、ライセンスが不足している場合は、「ライセンス追加購入」より必要な分だけ購入ください。

6-2. ライセンスの追加購入について

マネージドPKI のライセンス数が不足した場合や種類の異なるライセンスが必要な場合は、追加でライセンスを購入することができます。
※ライセンスとはクライアント証明書を発行する権利であり、その有効期間は一律1年間となります。
ライセンスを消費して実際に発行されるクライアント証明書の有効期間とは異なりますのでご注意ください。
※証明書の利用用途によって、購入するライセンスを選択できます。
下記の表を参照の上、ライセンスを購入してください。

【ライセンスの種類について】

■マネージドPKI Lite byGMO 個人名用

利用用途	説明
アクセス認証の用途で利用する場合	証明書のコモンネーム（CN）に、任意の値を設定可能です。
S/MIME の用途で利用する場合	S/MIME 用証明書のコモンネームとして利用できる値は、以下の通りです。 **①自社および関連会社に属する個人の E メールアドレス** **②SurName** **③SurName + GivenName** **④Pseudonym** ※法人名、または、自社および関連会社に属する部門用メールアドレスを設定する場合は、【マネージド PKI Lite byGMO 法人名用】をお申し込みください。

■マネージドPKI Lite byGMO 法人名用

利用用途	説明
アクセス認証の用途で利用する場合	【マネージド PKI Lite byGMO 個人名用】を選択しなおし、お申込みください。
S/MIME の用途で利用する場合	S/MIME 用証明書のコモンネーム（CN）に**法人名、または、自社および関連会社に属する部門用メールアドレス**を設定可能です。

1. GS パネルにログイン後、「マネージドPKI」のタブに移動してください。左メニューのライセンス管理より、「ライセンス追加購入」を選択して進みます。

2.必要なライセンス数を選択して「次へ」をクリックしてください。

3.証明書年数を選択してください。
キャンペーンコードやクーポンコードをお持ちであれば、そちらも入力してください。
技術担当者を設定する場合は、「技術担当者情報入力」をクリックし、次画面で必要事項を入力してください。
「次へ」をクリックして進みます。

4. 次画面で決済方法に関する必要事項をご入力のうえ、ライセンスの購入手続きを完了してください。
決済方法で前払いをご選択の場合、グローバルサインにて入金を確認後にライセンスが使用可能となります。

6-3. ライセンスのキャンセルについて

グローバルサインの電子証明書サービスは、7日間の完全返金保証が付いています。
ライセンス有効開始日を含めて7日以内に、キャンセルのお手続きが完了した場合には、全額を返金いたします。
※銀行振込にてご返金を行う場合、振込手数料はお客様負担となります。予めご了承ください。

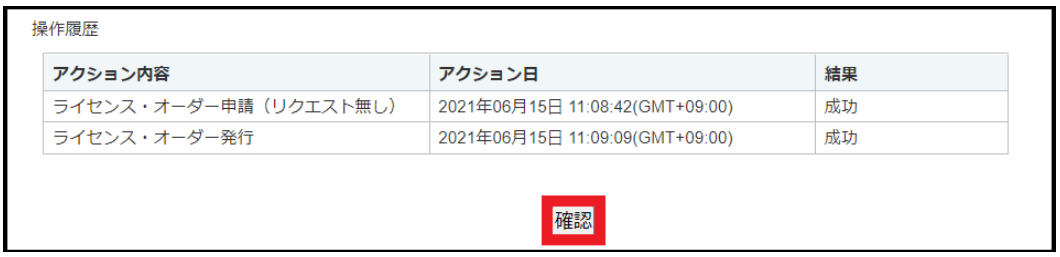
1.GS パネルにログイン後、「マネージド PKI」のタブをクリックし、左メニューのライセンス管理より「ライセンス購入履歴」を選択してください。

2. ライセンス ID などご希望の条件を指定し、「検索」をクリックしてください。
（条件の指定を行わない場合、すべてのライセンスの購入履歴が表示されます。）

3.ライセンス一覧が表示されますので、該当のライセンスの「編集」ボタンをクリックしてください。
次画面でライセンスの詳細が表示されます。

4. ライセンスの詳細画面が表示されます。
画面一番下の「キャンセル申し込み」をクリックし画面に従ってキャンセルを完了してください。
※ライセンス有効開始日より 7 日以降経過したお申し込みは、キャンセル可能期間を過ぎてしまったため、「キャンセル申し込み」のボタンは表示されずキャンセルを行うことはできません。

5.内容確認画面では何も入力をせず画面一番下の確認をクリックし、次の画面で内容を確認の上「完了」をクリックすると、キャンセル申し込みが完了となります。
※振込方法によって赤枠箇所が表示されますが、何も入力せずにお進みください。



7. プロファイルについて

7-1. プロファイルの追加登録について

グローバルサインのマネージドPKI は、部署名や住所の異なる複数のプロファイルを登録することができます。

※契約者情報の組織名と同一の組織名でプロファイルの追加登録を行ってください。

※部署名（OU）は【S/MIME BR(Legacy)対応用中間 CA】では利用できません。

※プロファイルの登録情報に変更がある場合は、新規でのプロファイルの申し込みが必要です。

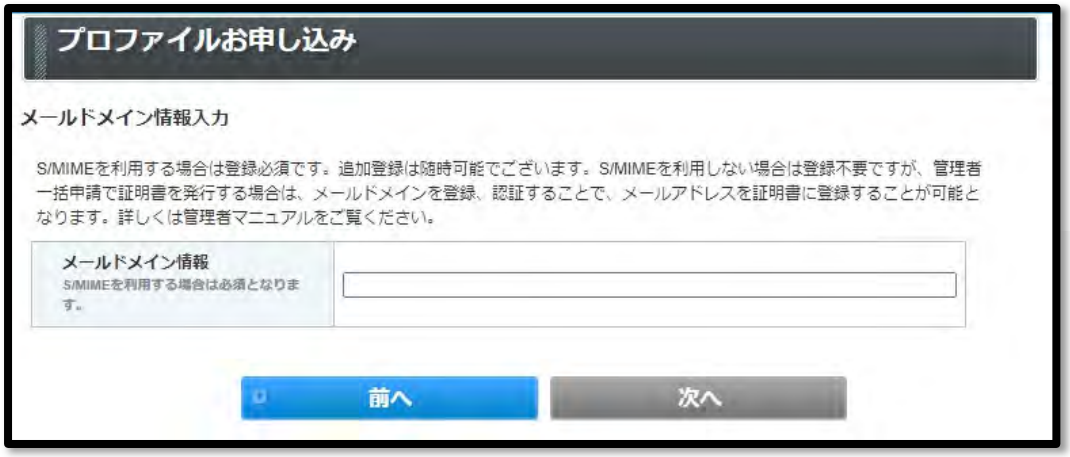
※プロファイル情報に変更の必要があることが判明した場合、その時点でプロファイルが使用停止されます。

1. GS パネルにログイン後、「マネージドPKI」のタブをクリックして移動します。
左メニューのプロファイル管理より「プロファイル追加申請」をクリックしてください。

2. 次画面の証明書情報入力でプロファイルに登録する情報を入力し、「次へ」をクリックしてください。

※「組織名 = O」には契約者情報と同一の組織名を入力してください。

3. メールドメイン情報を設定する場合はご入力の上、「次へ」をクリック押してください。
※S/MIME を利用する場合は登録必須です。
※追加登録は随時可能です。

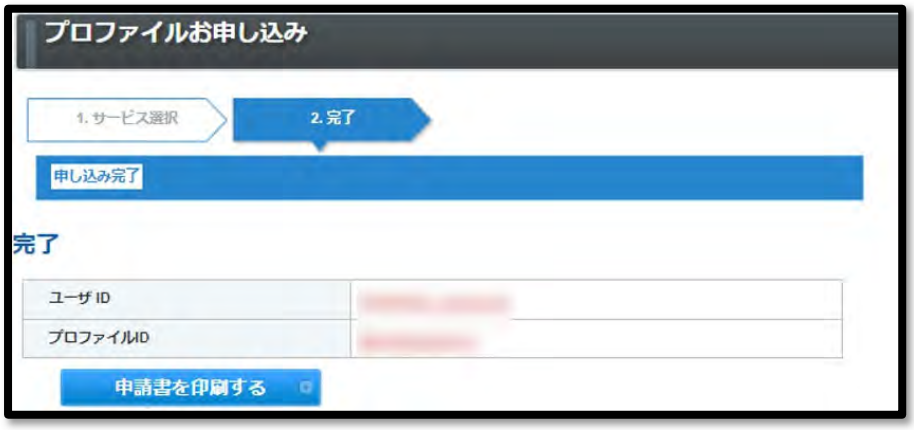


4.メールドメイン認証方法選択の画面に移ります。
メール認証・DNS 認証いずれかの対応可能な認証方法を選択してください。

利用可能な認証方法を選択し、「次へ」をクリックして進みます。

5.登録内容に問題がないことを確認し、「次へ」をクリックして進みます。

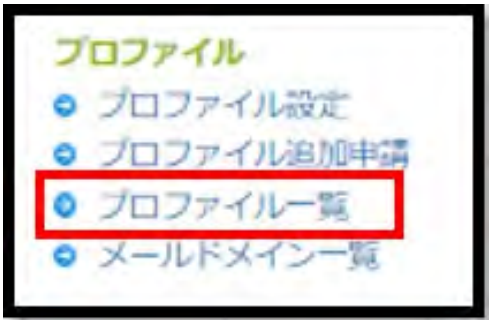
6.以上でプロファイルの追加申請は完了です。



7-2. プロファイルの更新について

【プロファイルの更新における注意点】
・2023 年 4 月 24 日以降に新規で作成されたプロファイルの利用可能期間は、審査完了後 824 日です。
・2023 年 4 月 23 日以前に新規で作成し、2023 年 4 月 24 日以降再審査を行っていない場合は対象外となります。
・プロファイルの登録情報に変更がある場合は、新規でのプロファイルの申し込みが必要です。
※更新申請後、プロファイル情報に変更の必要があることが判明した場合、その時点でプロファイルが使用停止されます。
・プロファイルをお申し込みいただく場合は、GS パネルの管理者情報が最新である必要があります。
・プロファイルの有効期限終了日を超えてしまうと、該当のプロファイルに紐づく証明書自体の発行が行えません。※発行済みの証明書には影響はないです。
・プロファイル審査の更新は有効期限終了日の 90 日前から実施してください。
※更新案内メールは 90 日前から送付されます。

1. GS パネルにログイン後、「マネージドPKI」のタブに移動します。
左メニューのプロファイルから「プロファイル一覧」をクリックして進みます。



2.更新ボタンが表示されているプロファイルを選択し、「更新ボタン」をクリックして進みます。

3.プロファイル情報を確認し、約款に同意後、「次へ」ボタンをクリックして進みます。

4.プロファイルの更新お申込みが完了しました。
※プロファイル審査は、通常 3～4 営業日ほどかかります。

5.「プロファイル一覧」から該当のプロファイルの更新が完了していることを確認できます。

7-3. プロファイル設定について(オプションの有効化)

GS パネルよりプロファイルの設定を変更することができます。
発行する証明書の署名アルゴリズム、EFS(Encrypting File System)対応、MS SmartCard Logon 対応、証明書の更新タイプ、秘密鍵のエクスポート不可、API 申請時の IP アドレスの設定が可能です。
設定手順は以下になります。

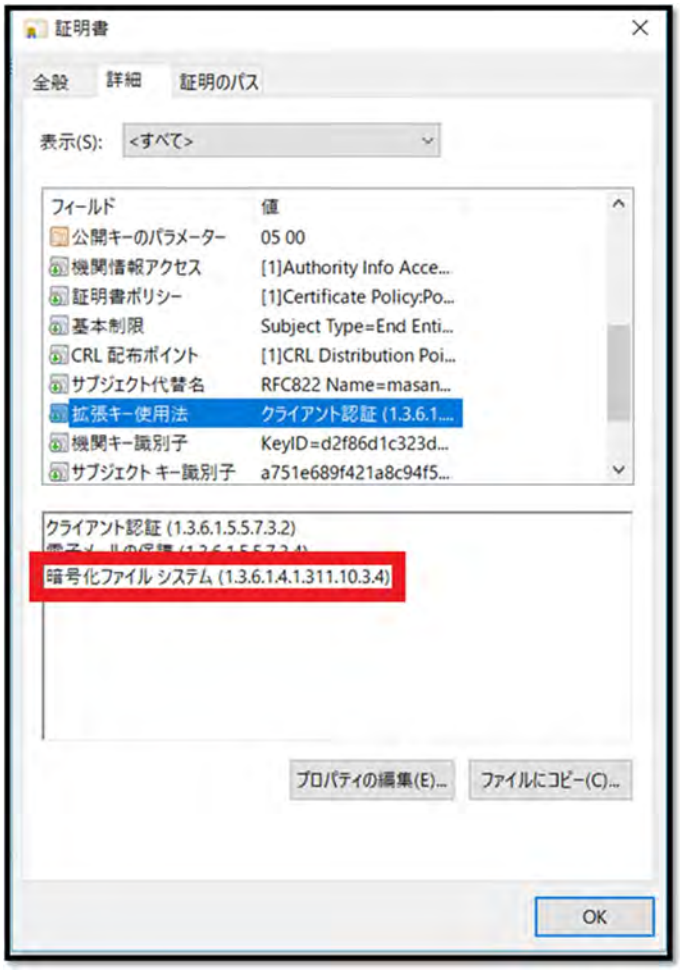
1. GS パネルにログイン後、「マネージドPKI」のタブに移動します。左メニューのプロファイルから「プロファイル設定」をクリックして進みます。

2. プロファイルを選択し、「次へ」ボタンでプロファイル設定画面に移動します。こちらで各設定を変更後、「次へ」ボタンで確認画面に進み、再度「次へ」ボタンをクリックして完了します。

＜各オプションについて＞

「署名アルゴリズム」:
選択したプロファイル情報を利用して発行する証明書の署名ハッシュアルゴリズムを設定します。
デフォルトでは「sha256 RSA」が選択されていますが、ドイツ政府エネルギー関連機関とメールの送受信を行われる方は「RSASSA-PSS（sha256）」をご選択ください。

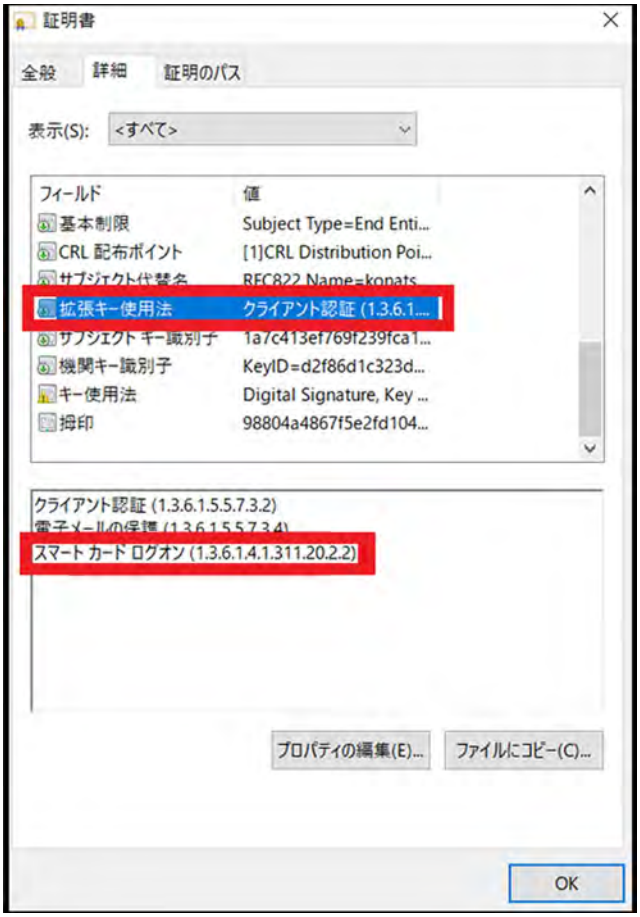
「Encrypting File System」:
有りを選択する事で発行される証明書の拡張キー使用法に「暗号化ファイル システム」が追加されます。
マイクロソフト OS で使用しているNTFS 形式のファイルの暗号化に証明書を利用できるようになります。



「証明書の更新タイプ」:
お選びいただく更新タイプによって、更新の流れが異なります。
詳細につきましては、P43～をご参照ください。

「プロファイル更新メール」:
プロファイルの有効期限 90 日前から送付されるメールの有無を切り替えることができます。

「MS SmartCard Logon」:
有りを選択する事で証明書の拡張キー使用法に「スマート カード ログオン」が追加されます。

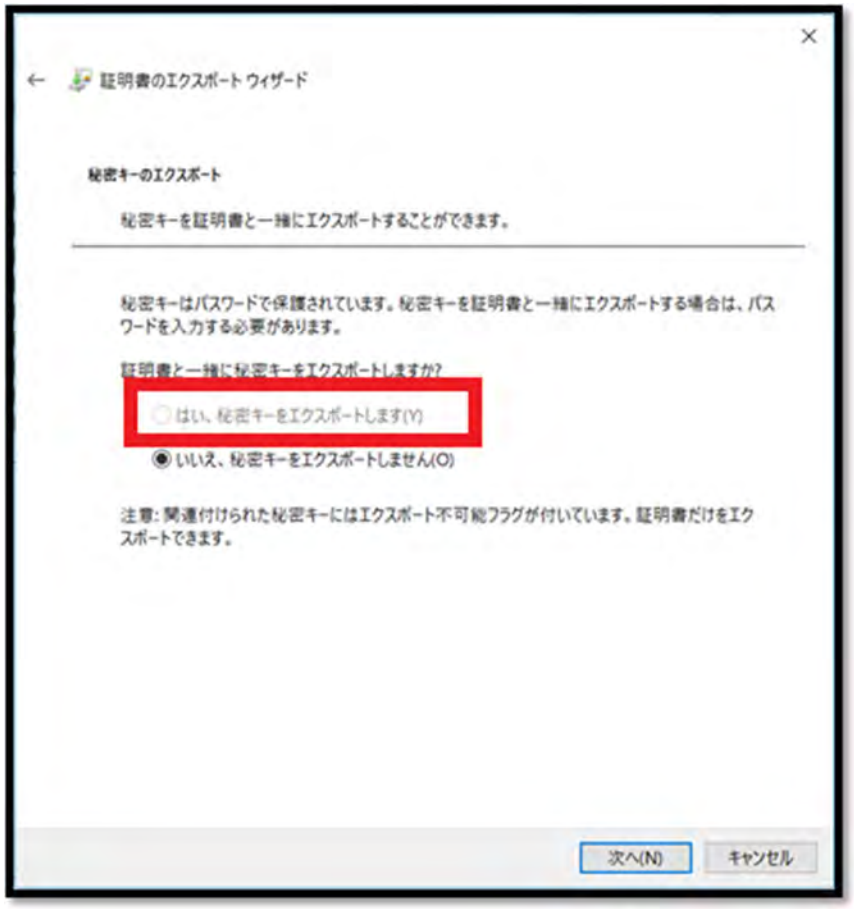


「秘密鍵のエクスポート不可」:
取得した証明書がデフォルト(Windows の機能により)でエクスポートすることができなくなります。
これにより証明書を利用する端末を制限することが可能になります。

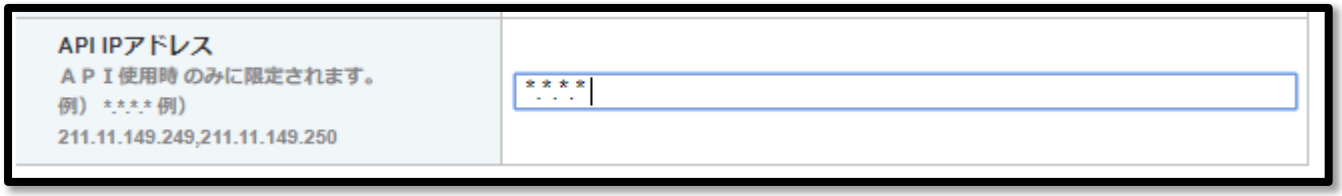
注意)本設定を有効にした場合 Firefox 等の Microsoft Edge の Internet Explorer モード以外で証明書を取得しようとすると以下の図が表示され、クライアント証明書のインストールが行えません。
またPKCS12 形式の証明書取得ができなくなります。

本機能によって取得した証明書をエクスポートした際の画面

*秘密鍵付のエクスポートがグレーアウトして不可になります。



「API 申請時の IP アドレスの設定」:
API の利用時にアクセスを許可する IP アドレスを設定します。
空欄の場合は全てをブロックします。



8. ユーザ権限について

マネージドPKI の管理者として操作できる範囲は、ユーザ権限によって異なります。
詳細は以下の表を参照してください。

	管理者	マネージャー	担当者
証明書管理			
証明書発行	○	○	※1
証明書発行(一括)	○	○	※1
証明書一覧	○	○	※2
証明書発行(管理者一括)	○	○	
管理者一括発行履歴	○	○	
承認待ち証明書一覧	○	○	※3
ライセンス管理			
ライセンス追加購入	○	※4	※4
ライセンス購入履歴	○	○	○
プロファイル管理			
プロファイル設定	○	○	
プロファイル追加申請	○		
プロファイル一覧	○	○	○
メールドメイン一覧	○	○	○
ポータル			
ポータル管理	○	○	
メール			
メールテンプレート管理	○	○	
メール一覧	○	○	
ポータルメール一覧	○	○	
その他			
Action log	○	○	
LDIF 管理	○	○	

※1 “証明書申請”権限付与時：証明書発行(管理者一括)以外の証明書申請
が可能となります。

※2 “証明書失効”権限付与時：証明書一覧にて、証明書の失効作業を行うことができます。

※3 “承認権限”付与時　　：承認待ち証明書一覧にて、承認作業を行う事ができます。

※4 “まとめ買い購入・マネージドPKI ライセンス購入権限”付与時：ライセンス追加購入ができます。
権限の付与は、[GS パネル管理と経理]タブの[ユーザ管理]から行う事が出来ます。

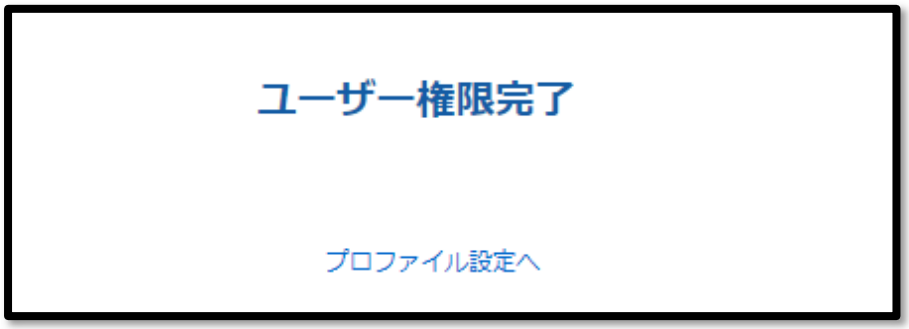
担当者権限のユーザの場合に表示されている※1、※2、※3は、プロファイルごとに「ユーザー権限」
から権限を付与することができます。

ユーザー権限の付与は、【プロファイル設定】から行うことができます。
1.[マネージドPKI]タブから、プロファイル設定を選択してください。

2.ユーザー権限の[設定]ボタンを押してください。

3.権限を付与したいユーザー・権限の範囲を選択してください。

4.内容を確認後、ユーザー権限の付与を完了させます。

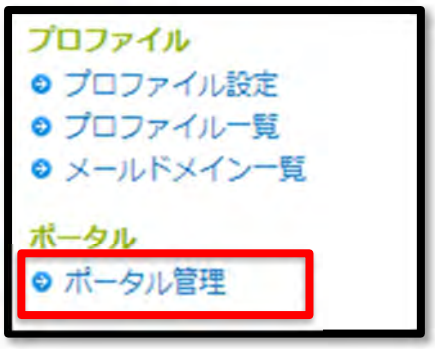


9. その他機能について

9-1. ポータル画面のカスタマイズ

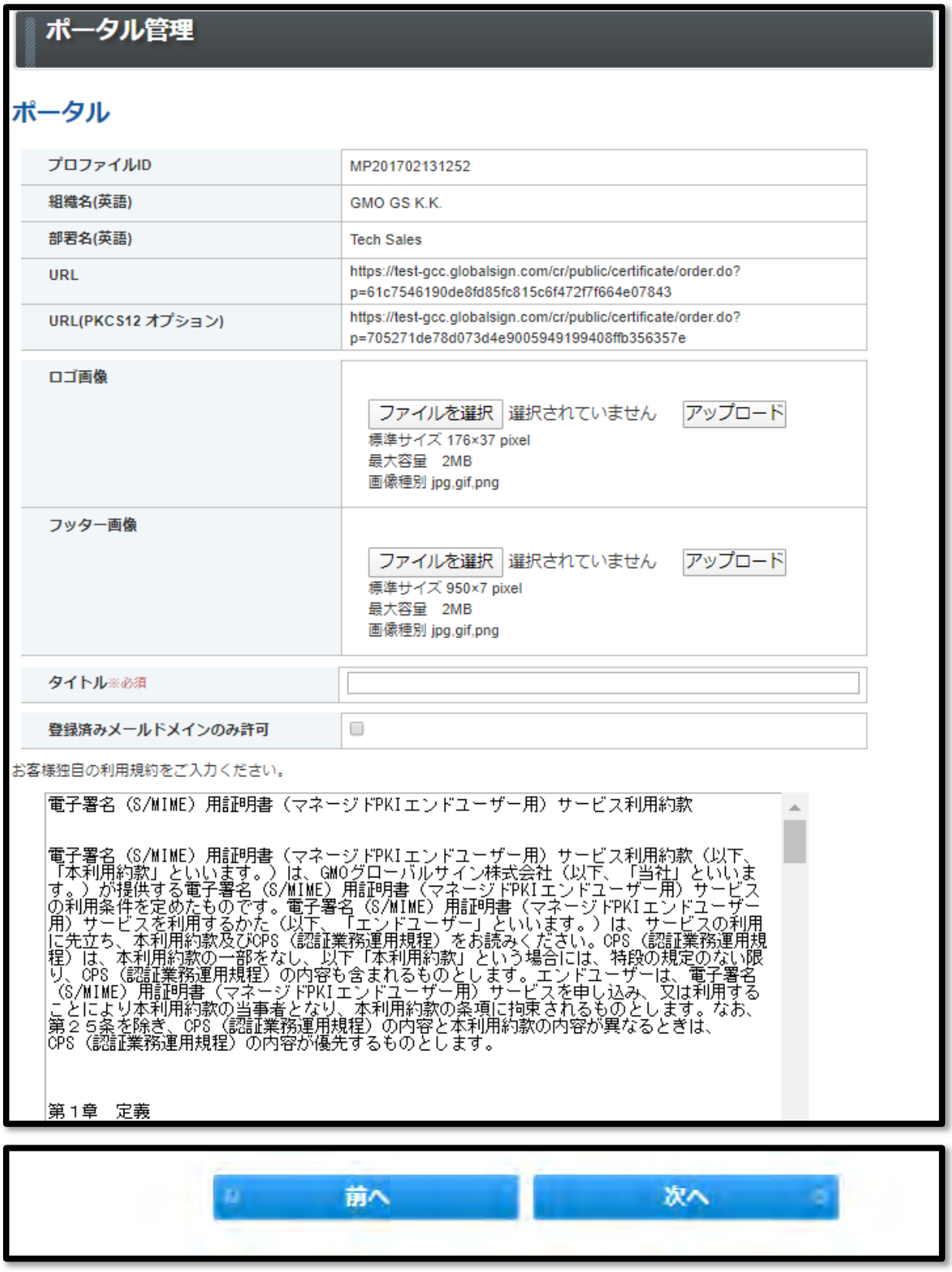
以下手順にてユーザ向けサイトのロゴ等をカスタマイズが可能です。

1.「ポータル管理」を開きます。



2. プロファイルの内容が表示されます。次へをクリックしてください。

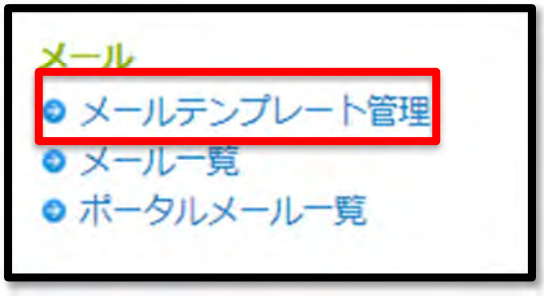
3. ページの上部、フッターに表示させたい画像をアップロード、タイトルを入力して次へ進みます。
登録済みメールドメインがある場合に登録済みメールドメインのみ許可のボックスにチェックをいれると本資料「9-3. メールドメイン情報」の項目で紹介を行う、登録済みドメイン以外のメールアドレスは受け付けなくなります。
また、自社の利用規約が有る場合は追加で表示する事も可能です。
内容を確認し、「次へ」をクリックします。
ユーザにポータル URL を告知し、ご利用ください。



9-2. メールテンプレート管理

メールテンプレート管理では、主に以下の作業を行うことができます。
・自動送信されるメールの内容の編集
・多言語対応（言語ごとのテンプレートの設定）

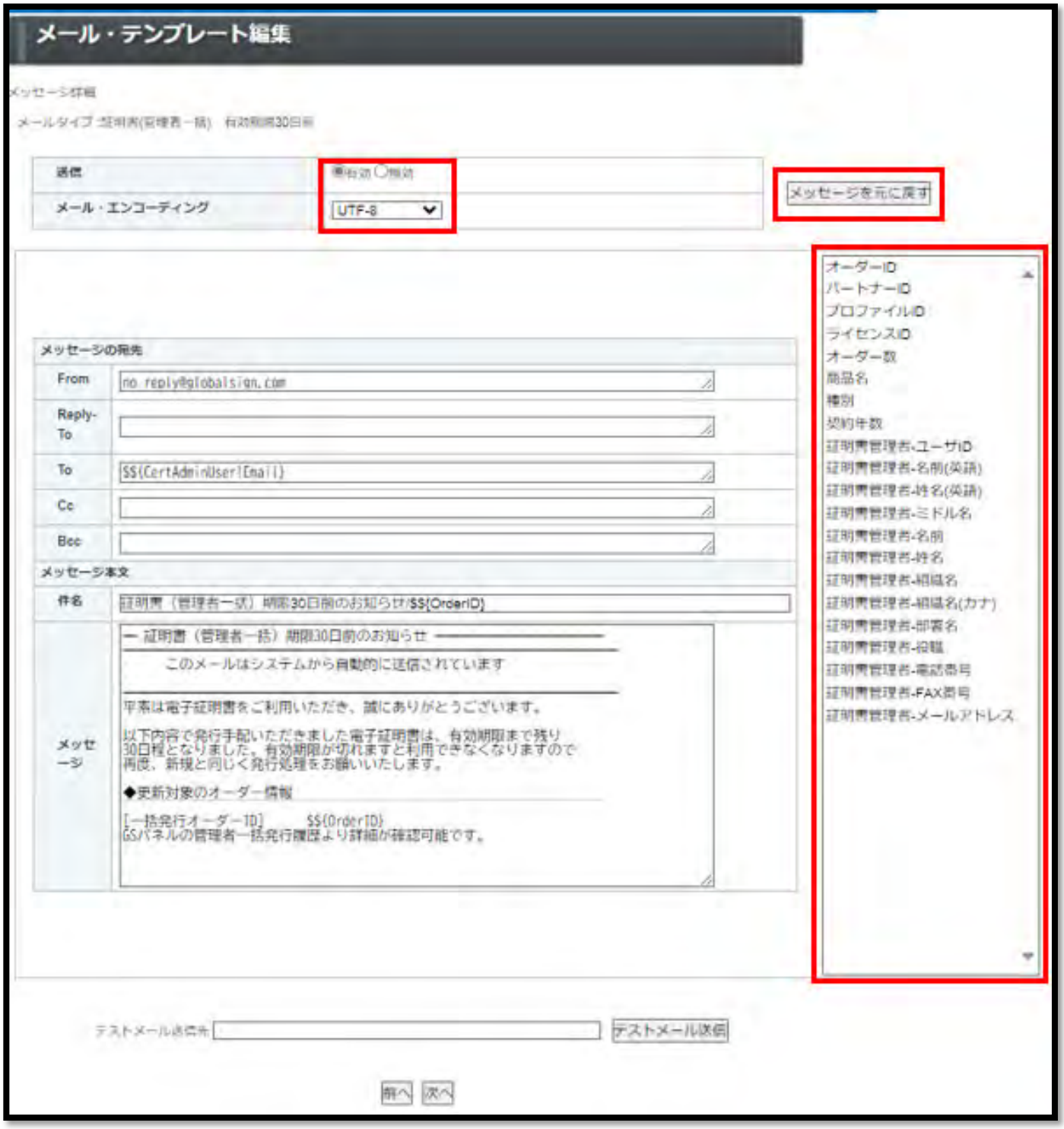
1. GS パネルにログインし、「メールテンプレート管理」をクリックします。



2. 日本語、英語は標準の文面が記載済みですが、その他の言語についてはお客様自身で修正を行い、送信設定を有効にする必要があります。

※メールテンプレート言語は証明書の申請時（新規・更新）に選択・変更が可能です。
※メール内容を編集した場合、以降に送信されるメールが編集後の内容となります。

3. 選択済言語の各メールタイプの編集ボタンを押して、編集を行います。
※詳しいメールタイプについてはP91～をご参照ください。



・メールを送信する場合は、有効にチェックを入れます。
・メール・エンコーディングを UTF-8 もしくは ISO-2022-J より選択します。
UTF-8 を選択することで使用できる文字数が増えますが、ISO-2022-J に比べ、対応する環境が減ることになります。
ISO-2022-J を選択することで、対応する環境は増えますが、一部、海外の言語等は使用できなくなります。
・「メッセージを元に戻す」のボタンを押すと、メールテンプレートが初期状態に戻ります。

・カーソルの場所に、右赤枠内から選択した項目をクリックすることで変数が挿入されます。
デフォルトの状態で必要な変数はセットされていますので顧客特有の場合を除いて追加の必要はありません。
・From(メール送信元)やメッセージのフィールドは変数以外にも、文字列(E-Mail アドレス等)を記述し設定することができます。
※ご利用のメーラによっては送付元または受信先のメールドメインと異なるメールドメインに変更されている場合、迷惑メール対策としてメールが正常に送受信できない場合がございます。
その場合は、お手数ですがメールアドレスは「no_reply@globalsign.com」を設定いただきますようお願いいたします。

編集例：no_reply@globalsign.comより送付されたメールへの返信がReply toに設定されたメールアドレス宛に送付されるよう設定しています
ご希望のメールアドレスを返信先としてご登録されたい場合は、「Reply-To」を利用してください。

To(メール宛先)の値に (カンマ) ,任意のメールアドレスを加えることで、変数以外にも任意のメールアドレスが記載されます。
Cc、Bcc の欄にも、同様に修正、追加が可能です。

メールアドレスの記入欄に誤って第三者のアドレスが記載された場合、第三者によって証明書の取得等が行われる可能性があります。
もし誤って送信してしまったメールアドレスから証明書を取得されてしまった場合、直ちに P65～に記載されている失効作業を行ってください。

編集した内容で、テスト送信することが可能です。
メールアドレスを入力し、「テストメール送信」をクリック押します。
テストメール送信では To、Cc、Bcc の内容は反映されません。
編集内容を保存する場合は、「次へ」をクリックし、変更内容を確認後に「完了」をクリックしてください。

各メールタイプの意味は以下の通りです。

証明書(管理者一括) 有効期限 30 日前
管理者一括にて発行された証明書の有効期限 30 日前に管理者宛てに送信されます。
キャンセル完了
管理者によって証明書がキャンセルされた場合に送信されます。
証明書取得(インバイト)
管理者がユーザの証明書を申請後、証明書の取得を促すメールが送信されます。
証明書取得(ポータル)
ユーザがポータル画面から証明書を申請後、管理者がオーダーを承認すると、証明書の取得を促すメールが送信されます。
証明書取得 (クイック更新)
更新の種別をクイック更新にしている場合の証明書取得メールです。 通常の証明書取得と同様に当該メールにて証明書取得が可能になります。 更新元証明書の有効期限 30 日前に一度のみ送信されます。
証明書取得(再発行)
再発行の際の証明書取得メールになります。
証明書取得期限通知 (15 日後)
証明書取得メールを送信して 15 日後に、まだ証明書を取得していないユーザへ取得を促すメールが送信されます。
証明書取得期限通知 (30 日後)
証明書取得メールを送信して 30 日後に、まだ証明書を取得していないユーザへ取得を促すメールが送信されます。
証明書取得期限切れ自動キャンセル
31 日目に証明書取得期限が切れて、証明書が自動的にキャンセルされた場合に送信されます。
証明書発行完了
ユーザにて証明書の取得が完了すると送信されます。
PKCS12 証明書発行完了
PKCS12 形式の証明書の取得が完了すると送信されます。
非承認キャンセル
ユーザによるポータルからの申請を管理者が「非承認」とするとキャンセル通知が送信されます。
ポータル申請受付
ユーザよりポータルから申請があった際に、管理者へ送信されます。
証明書再発行完了
ユーザにて証明書の取得(再発行)が完了すると送信されます。
PKCS12 証明書再発行完了
PKCS12 形式の証明書の取得(再発行)が完了すると送信されます。

証明書 有効期限切れ
発行済み証明書の有効期限の日に送信されます。 証明書 有効期限◯日後、◯日前
証明書 有効期限◯日後、◯日前
発行済み証明書の有効期限の前後に、それを知らせるメールが送信されます。
失効完了
管理者によって証明書が失効された際に送信されます。
保留完了
管理者によって証明書が保留された際に送信されます。
保留解除完了
管理者によって証明書の保留が解除された際に送信されます。

9-3. メールドメイン情報

【アクセス認証用中間 CA】で、E メールを含んだ証明書を証明書発行（管理者一括）で発行する場合、または【S/MIME BR(Legacy)対応用中間 CA】のプロファイルから証明書を発行するに事前に E メールドメインの登録が必須です。

1.[マネージドPKI]タブから、プロファイル設定を選択してください。
2.設定をクリックします。

3.事前審査を行いたいメールドメインを登録し、「次へ」をクリックして、申請を完了してください。

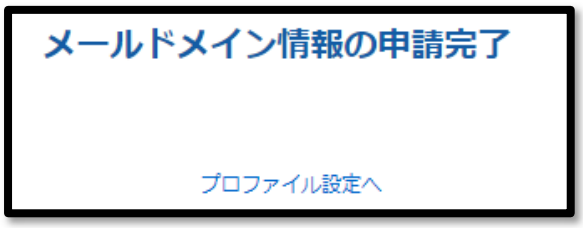
4.任意のメールドメイン情報を入力後、「S/MIME を利用します。メールドメインの有効期間は 397 日となり、継続利用のためにはドメインの再認証が必要であることを了承します。」を選択し、「次へ」進みます。
※アクセス認証用中間 CA 利用のお客様は「SMIME は利用しませんが…」を選択することで、再審査をせずに継続して利用することができます。

5.メールドメイン認証方法選択の画面に移ります。
メール認証・DNS 認証・ページ認証いずれかの対応可能な認証方法を選択してください。

利用可能な認証方法を選択し、「次へ」をクリックして進みます。

6. 登録内容に問題がないことを確認し、「次へ」をクリックして進みます。

7. 以上でメールドメイン情報の登録は完了です。



申請完了後、2～3営業日以内を目処に弊社審査部門よりメールにてご連絡いたします。
認証方法によってメールの From アドレスが異なります。
下記をご参照ください。

認証方法	From	説明
メール認証	approval@globalsign.com	例：globalsign.com でメール認証をした場合、mail.globalsign.com 等でも利用できます。
DNS 認証	vetting-jp@globalsign.com	例：globalsign.com で DNS 認証をした場合、mail.globalsign.com 等でも利用できます。
ページ認証	vetting-jp@globalsign.com	例：globalsign.com でページ認証をした場合、mail.globalsign.com 等では利用できません。 ページ認証の場合は、サブドメインを含む FQDN 単位で登録し、認証する必要があります。

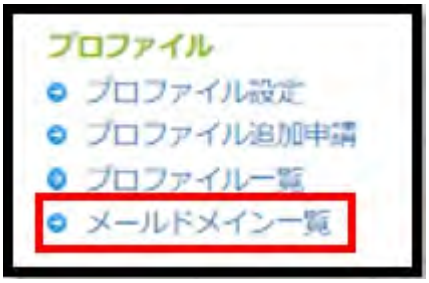
8. 登録を行ったメールドメインは左サイドメニューのメールドメイン一覧にて確認する事ができます。

9-4. メールドメインの更新について

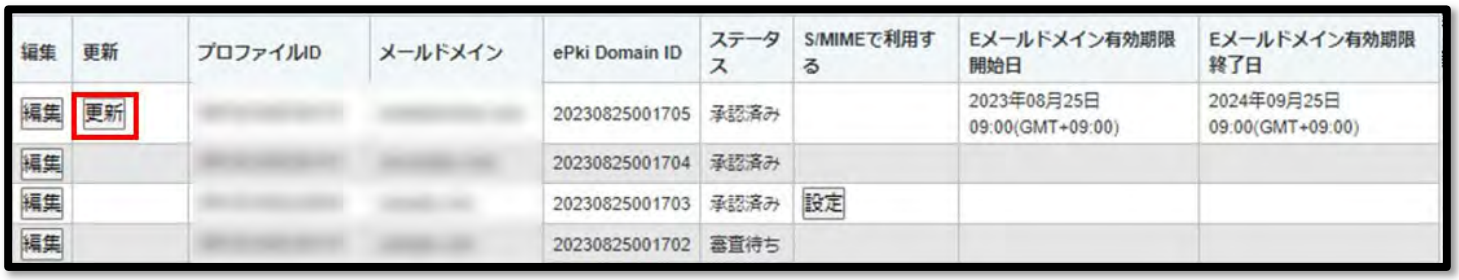
【メールドメイン更新時の注意点】

・「S/MIME を利用します。」を選択しているドメインの審査情報利用期間は 397 日です。
・メールドメインの有効期限終了日を超えてしまうと該当のメールドメインに紐づく証明書自体の発行が行えません。
・「S/MIME を利用します。」を選択していない場合は対象外です。
・ドメイン認証は、通常 2～3 営業日ほどかかります。
・ドメイン審査の更新は有効期限終了日の 90 日前から実施してください。
・更新案内メールは 90 日前から送付されます。
・登録可能なメールドメインは自社および関連会社のもののみとなります。
・複数プロファイルがある場合は、同一ドメインであってもプロファイル毎に登録が必要です。

1.[マネージドPKI]タブから、「メールドメイン一覧」を選択してください。



2. 更新対象のメールドメインを選択し、「更新ボタン」をクリックして、
進んでください。



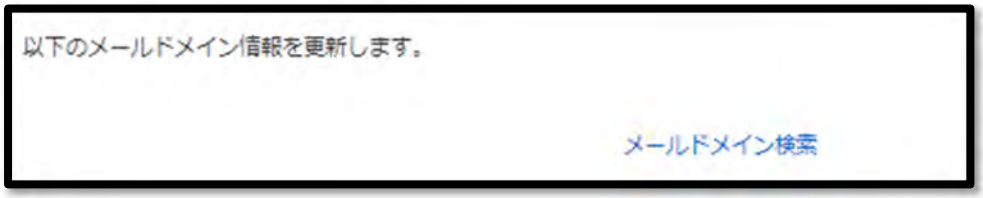
編集	更新	プロファイルID	メールドメイン	ePki Domain ID	ステータス	S/MIMEで利用する	Eメールドメイン有効期限開始日	Eメールドメイン有効期限終了日
編集	更新			20230825001705	承認済み		2023年08月25日 09:00(GMT+09:00)	2024年09月25日 09:00(GMT+09:00)
編集				20230825001704	承認済み			
編集				20230825001703	承認済み	設定		
編集				20230825001702	審査待ち			

3.メールドメイン認証方法選択の画面に移ります。
メール認証・DNS 認証・ページ認証いずれかの対応可能な認証方法を選択してください。
※ドメインの登録時または更新時にメール認証か DNS 認証を選択した場合、次回更新時にページ認証は選べません。
※認証方法を変更したい場合は弊社（support-jp@globalsign.com）までお問い合わせください。

利用可能な認証方法を選択し、「次へ」をクリックして進みます。

4.更新内容に問題がないことを確認し、「次へ」をクリックして進みます。

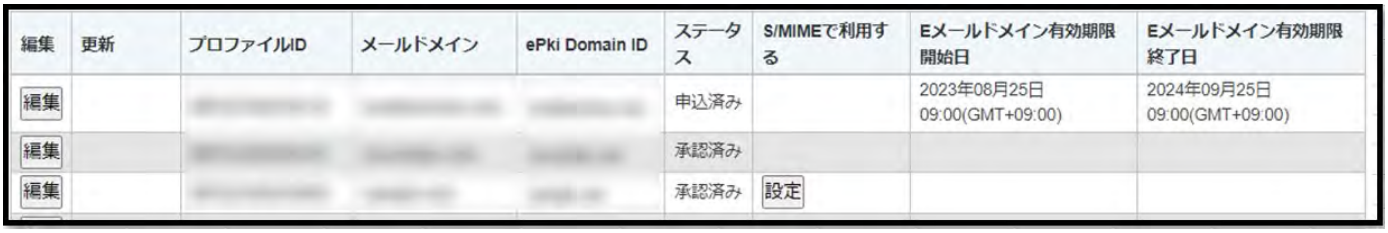
5.以上でメールドメイン情報の更新は完了です。



申請完了後、2～3営業日以内を目処に弊社審査部門よりメールにてご連絡いたします。
認証方法によってメールの From アドレスが異なります。
下記をご参照ください。

認証方法	From	説明
メール認証	approval@globalsign.com	例：globalsign.com でメール認証をした場合、mail.globalsign.com 等でも利用できます。
DNS 認証	vetting-jp@globalsign.com	例：globalsign.com で DNS 認証をした場合、mail.globalsign.com 等でも利用できます。
ページ認証	vetting-jp@globalsign.com	例：globalsign.com でページ認証をした場合、mail.globalsign.com 等では利用できません。 ページ認証の場合は、サブドメインを含む FQDN 単位で登録し、認証する必要があります。

6.更新を行ったメールドメインは左サイドメニューの「メールドメイン一覧」から確認する事ができます。



9-5. LDIF 管理

証明書情報を LDIF 形式でエクスポートすることができます。
自社ディレクトリサーバ等に一括して発行済み証明書を登録することができます。

LDIF フォーマットのカスタマイズ
1.GS パネルにログイン後、「マネージドPKI」－「LDIF 管理」を選択します。

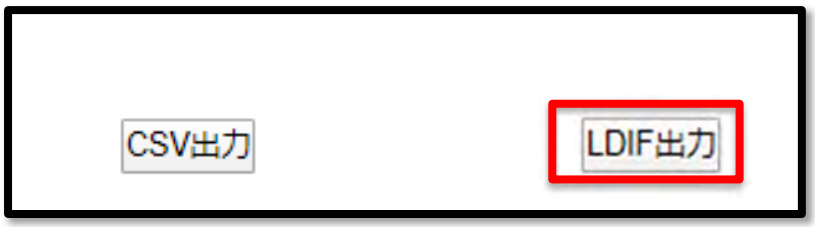
2.こちらの画面でテンプレートを編集します。
設定後、「次へ」ボタンで確認画面へ進み、「完了」ボタンで決定します。

LDIF ファイルのダウンロード方法

GS パネルにログイン後、「マネージド PKI」－「証明書一覧」を選択します。

検索条件を入力後、「検索」ボタンを押します。
（全てを対象にする場合は、「検索」ボタンのみを押してください。）

エクスポート対象の証明書情報が表示されたら「LDIF 出力」をクリックします。
しばらくするとファイルのダウンロードが始まります。

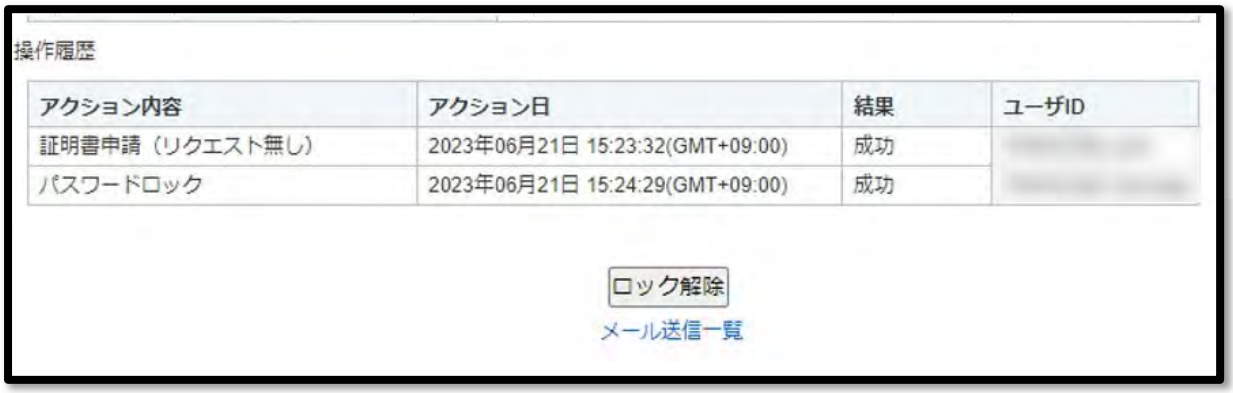


9-6. クライアント証明書のロック解除機能について

クライアント証明書の取得時のパスワードを規定回数(10 回)間違えた場合、証明書の取得がロックされ、しばらく操作が不可になります。

ユーザからお問い合わせが入った場合は、以下いずれかの対応を実施いただくことで再度 URL から取得が可能です。

・ロック発生から 30 分後、再度ユーザに取得をしてもらう。
・証明書の管理者が「証明書一覧」からロック解除を押す。

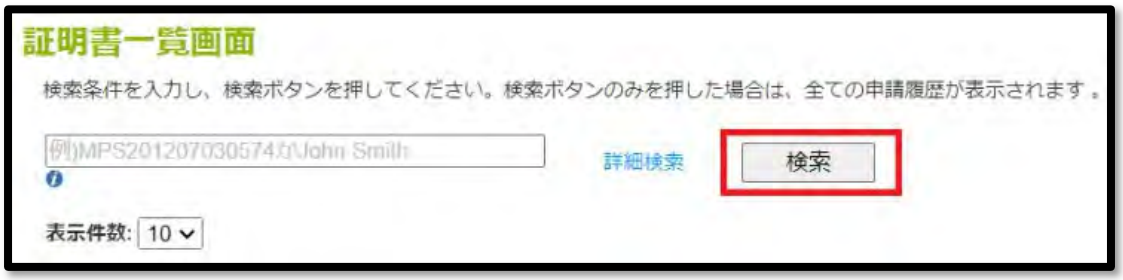


9-7. 証明書取得用パスワードの確認方法

1.GS パネルにログインし、「マネージドPKI」タブを開きます。

2.「証明書一覧」をクリックします。

3. ご希望の証明書を検索します。



4. 該当証明書の「申請」ボタンをクリックします。

5.「証明書取得用パスワード」欄にて確認可能です。

GMO グローバルサイン株式会社
〒150-0043 東京都渋谷区道玄坂 1-2-3 渋谷フクラス
TEL : 03-6370-6500 https://jp.globalsign.com