マネージド PKI Lite 管理者マニュアル Ver10.0 (2024 年 12月版)





目次

目次

はじめに	4
1. マネージド PKI Lite 初期設定	5
初期設定①プロファイル・ライセンスお申し込み	
初期設定②メールドメイン情報の登録	
初期設定③管理者証明書を取得	13~14
管理者証明書の更新について	15
管理者証明書取得時のトラブルに関して	
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	17~20
2. クライアント証明書の発行手順について	21
クライアント証明書を新規申請(新規)	21
A:「証明書発行」の申請~発行までの手順	
B:「証明書発行(一括)」の申請~発行までの手順	24~31
C:「証明書発行(管理者一括)」の申請~発行までの手順	
D: ユーザによる申請~発行までの手順	
クライアント証明書の発行手順について(更新)	
クライアント証明書申請時の項目について(新規・更新)	43~45
各申請項目の説明	
3. クライアント証明書の再発行手順について	
A:証明書の再発行を1枚ずつ行う手順	50 ~ 51
B:「証明書再発行(一括)」の再発行申請~再発行までの手順	52 ~ 53
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	54~57
4. クライアント証明書の格納先について	
A:ブラウザの鍵生成機能を用いた証明書の取得手順	
B:PKCS12 形式での証明書の取得手順	61~62
C:CSRを用いた証明書の取得手順	63

5. クライアント証明書の確認・キャンセル・再発行・失効	64~65
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	
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	
6-2. ライセンスの追加購入について	
6-3. ライセンスのキャンセルについて	
7. プロファイルについて	74
7−1. プロファイルの追加登録について	
7-2. プロファイルの更新について	
7-3. プロファイル設定について(オプションの有効化)	
8. ユーザ権限について	
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	
9-2. メールテンプレート管理	
9-3. メールドメイン情報	
9-4. メールドメインの更新について	
9-5. LDIF 管理	
9-6. クライアント証明書のロック解除機能について	101
9-7. 証明書取得用パスワードの確認方法	

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。

 GSパネル(管理画面)へアクセスし、「マネージドPKI」タブに移動
 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。)
 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。

<u>・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。</u>

・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 <mark>法人名、または、自社および関連会</mark> 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。

Con String	ノロノアイル・ノイビノスの中し座の	
ホータル		
ハーダル言理	マネージドPKI	
プロファイル		
プロファイル設定	・従来の中間CAより発行した証明書をS/MIME BR(Legacy)対応用中間CAにて更新を行うことはできません。お手数ですが、S/MIME BD// computing 中間CAのプロフェイルとり発行する希望の現在は新潟にアプ申請くおさいます。FSが取りいたくます	
K-16	prkLegacyJanの時中間はAのノビノアイルなり先行をこ年年以後合され7歳にして一時にたさいなりようの時いいにしょう。 ・2023年7月31日とわプロファイルの設定でSMIME RRI eacyが成広田由間にAを選択であるようになりますが、その設定下において	
メールテンプレート管理	・2020年7月37日よりフロノアイアルの設定でGinning Br(Legacy)7310月中間CAと進伏できるようによりますが、その設定下において も、2023年8月28日までは従来の中間CA(アクセス認証用中間CA)から証明書が発行されます。	
メール一覧	※2023年8月28日に自動的(CS/MIME BR(Legacy)対応用中間CAからの発行に切り替わります。	
ポータルメール一覧		
• メール署名用証明書登録	SMIME BR(Legacy)対応用中間CA証明書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。	
その他	・SIGMINE BR(Learny)所立用Eメールドメインが登録されている。	
o LDIF管理	· OrganizationIdentifierが登録されている。	
	ライセンス追加購入	
	マネージドPKI Lite byGMO	
	○ マネージドPKILite byGMQ 高マ 1パック マ 次本	

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。)

サービス読択 >>> サービスド	浴田田 ≫ DN信服入力 ≫ 支払方法入力 ≫ 確認
ヒス内容の選択 -	マネージドPKI Lite 10 pack
明書年数三之章	 ●1年 ¥108,000 ●2年 ¥205,200 ●3年 ¥298,080
キャンペーンコード	通用 ※キャンペーンをご利用の場合は、キャンペーンコードを入力のうえ、「適用」ボタンを押 してください
アーボンコード	通用 ※クーポンをご利用の場合は、クーポンコードを入力のうえ、「適用」ボタンを押してくだ さい
調 (税达)	¥ 108,000
当者情報入力	
別の方の場合は、こちらから	入力をお願いします。

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。

吉1 〒牧人儿 れる証明書に記載される情報ですので、お	間違いのないようにお願いします。
P間CA証明書	○ S/MIME BR(Legacy)対応用中間CA証明書
	● アクセス認証用中間CA証明書
BaseDN	
圆/地域 = C※必須	日本 - JP 🗸
『道府県 = S 半角英数、または全角(UTF-8)128文字以内	例)Tokyo
5区町村 = L 《半角英数、または全角(UTF-8)128文字以内	(%) Shibuya
日織名 = 〇 ※必須 《半角英数、または全角(UTF-8)64文字以内	例)GlobalSign K.K.
郡智名 = OU ※BaseDnをチェックする場合は必 半角英数、または全角(UTF-8)64文字以内	Ø() Markeling Division
雪名アルゴリズム	 sha256RSA RSASSA-PSS (sha256) こちらを選択した場合は有効期限1年の証明書の申込以外は行えません。
organizationIdentifier(2.5.4.97) SMIMEを利用する場合は 必須となります。	 ● VAT ○ GOV VAT番号を発行した国
	日本 - JP ×
	国税庁法人番号を入力してください

【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。

プロファイル・ライ	センスお申し込み
1.サービス選択	2.完了
サービス選択 ≫ サー	-ビス内容選択 ≫ DN情報入力 ≫ 支払方法入力 ≫ 確認
支払方法情報	
支払方法	◎ 銀行振込(後払い) ※翌月末日までに代金をお振り込みください。
	クレジットカード

カード名義(First name)※ 必須	例)Taro
カード名義(Last name) ※必 須	例)Yamada
カード会社※必須	©VISA ©MasterCard ©JCB ©DC
カード番号※必須	例) 4980123412341234
カード有効期限(MONTH)/ カード有効期限(YEAR)※必 須	例) 01/2005
次回以降もこのクレジットカ ード情報を利用する	副除方法はこちらをご参照ください。
その他情報	
Xモ欄	
	in the second
_	

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。

プロファイル・ライセンスお申し込み	
1. サービス選択	2.第7
サービス通訳 🔉 サービス内容圏	R 🔉 DN情報入力 🧊 支払方法入力 🚿 <mark>磁盤</mark>
き録情報の確認 ライヤンス内容	
サービス名	マネージドPKI Lite byGMO 即門/法人名用 1 pack
証明書年数	1年
キャンベーンコード	
クーボンコード	
金額(税込)	¥ 0.
ディスティングイッシュネーム物	青穀
中間CA証明書	S/MIME BR(Legacy)対応用中間CA症明問
BaseDN	
組織名 = 0	GlobalSign K.K.
部署名 = OU	
市区町村 = L	Shibuya
都適府號 = S	Tokyo
国/地域 = C	日本 - JP
organizationIdentifier(2.5.4.97)	GOVJP
その他情報	

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。

1.サービス選択	2.完了
申し込み完了	
完了	
ユーザロ	
ライセンスID	
プロファイルID	
申請書を印刷す	- 0

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。

組織部署	铭	GlobalSign K.I	C			
部署			-			
-	路					
URL		-				
URL	L(PKCS12 オプション)					

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。

プロファイルID	MP202
組織名	GlobalSign K.K.
部署名	
JRL	
JRL(PKC \$12 オプション)	
ユーザー権限	設定

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。

Cールドメイン情報 SMIMEを利用する場合は登録必須です 一括申請で証明書を発行する場合は、3 なります。詳しくは管理者マニュアルで ールドメイン情報入力	。追加登録は随時可能でございます。S/MIMEを利用しな ペールドメインを登録、認証することで、メールアドレス ご覧ください。	い場合は登録不要ですが、管理者 を証明書に登録することが可能と	
メールドメイン情報 SMIMEを利用する場合は必須となりま す。	globalsign.com		
 S/MIMEを利用し が必要であること? S/MIMEは利用し メールドメインを言 	ルます。メールドメインの有効期間は397日となり、継続 27承します。 ルませんが、管理者一括申請での証明書発行で、メールア 総録します。	利用のためにはドメインの再認証 ドレスを証明書に登録するため、	
登録済みメールドメイン			

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。

1. 9 -E	選択 2.完了	\supset	
DN情報入力	メールドメイン情報入力	※ メールドメイン認証方法選択 ※ 変字	
メール語	証		
メール間 承認作業	証では、ドメイン所有者のみが受 を行っていただきます。	可能と想定されるメールアドレスへ弊社から承認メ	ールを送信し、ドメイン所有者に
WHOISO	メールアドレス		
承認メー 【WHOI WHOIS	ルアドレスは、下記選択肢の中か 登録情報の修正が必要な場合】 報の変更につきましては、お客様	任意のものをご選択ください。 Y容録されたドメイン専業者へお問い合わせくださし	λ.,
O admir	@globalsign.com		
O admin	istrator@globalsign.com aster@globalsign.com		
Opostn	aster@globalsign.com		
Owebn	aster@globalsign.com		
O WHO	ISアドレスを記入してください。		
	-		

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。

		lobalsign.com	メールドメイン情報 S/MIMEを利用する場合は必須となります。
▶間CA証明書 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	なり、継約	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	中間CA証明書
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	Eす。	別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	

7.以上でメールドメイン情報の登録は完了です。

メールドメイン情報の申請完了
プロファイル設定へ

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	<u>vetting-jp@globalsign.com</u>	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。

マネージドPКI	1 11 10 1 15 10	-				
証明書 ● 証明書管理	X-1/1×1 28	UR De la Reize				
 ライセンス ● ライセンス追加購入 ● ライセンス購入履歴 	表示件数 10 ~	p-support se		検索		
プロファイル ● プロファイル設定 ● プロファイル追加申請 ● プロファイルー覧 ● メールドメイン一覧	1 - 10 /11	<1	2次へ>			
ポータル ◎ ポータル管理	プロファイルロ	メールドメイン	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
iOS 証明書	MP202308256191	acccestes.com	承認済み	設定		
● 構成プロファイル設定	MP202308236119	enablesmime com	承認済み		2023-08-25 09:00:00.0	2024-09-25 09:00:00.0
メール	MP202308236119	sample.com	承認済み	設定		

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。

GSパネル管理と経理 🕒	サーバ証明書 (EDI・ヤフー提携証明書を含む) E SSLマネージドサービス E (コードサイニング・PDF) E	マネージドPKI 🗉
マネージドPKI 評問書	ライセンスお申し込み	
 ・ 証明書管理 ライセンス ・ ライセンス追加購入 ・ ライセンス ぶの歴 	マネージドPKI	

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。

管理者証明書取得 証明書取得用パスワードを、8文字以上でご登録 このパスワードは、後間と通信される、管理者証 証明書を取得する際にご入力いただ(必要があ) 管理者証明書取得用メールは、 その他の場合はグローバルサインまでお問い合	4ください。 明春取得用メールより ります。 に通信されます。 わせくだえい。
証明書取得用パスワード:	
証明書取得用パスワード(強認用):	
	次へ =

3.「申請完了」と表示されれば、申請は完了です。

申請完了
メールを確認いただき証明書の取得をお願いいたします。

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。

線保護パスワード×上海	》 采用规则12次学习(上
総保護リスワード(確認用)×20年	
現現りに同意の上、「次へ」ボタンをクリックしてください。	
電子署名(S/MIME)用証明書(マネージドPKIエンドユ サービス利用約款	ーザー用)
電子署名(S/MINE)用証明書(マネージ FPRIIンドユ (以下、「本利用約款」といいます。)は、GMOグロー) 社」といいます。)が提供する電子署名(S/MINE)用約 ーザー用)サービスの利用条件を定めたものです。電子 ージ FPRIIンドユーザー用)サービスを利用するかた います。)は、サービスの利用に先立ち、本利用約款及 読みください。CPS(認証業務運用規程)は、本利用約割	 - ザー用) サービス利用約款 バルサイン様式会社(以下、「当 同書(マネージドPRIエンドユ 響名(S/MIME) 用証明書(マネ (以下、「エンドユーザー」とい DCPS(認証業務運用規程)をお 次の一部をなし、以下「本利用約
্র ছান্ত্র হি	

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。

- 管理者証明書期限90日前のお知らせ	5
このメールはシステムから自動的に送信されています	
平素はグローバルサインのマネージドPKI Liteをご利用いただき、 戯にありがとうございます。	-
マネージドPKI Liteの管理者証明書は、有効期限まで残り90日程となりました	0
以下の手順に従って、更新の手続きを進めてください。更新手続きが完了した マネージドPKI Liteの管理手続きが行なえなくなります。	い場合、
◆更新可能な証明書情報	
オーダーID] コモンネーム]	
◆更新手続き	
を有効な管理者証明書が格納されている端末からのアクセスをお願いします。 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、 证明書を申請してください。	

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。

ライセンスお申し込み	
マネージドPK	
ブロファイルセットアップウィザード	
プロファイルの各種設定が完了していません。 証明書の申請前に、こちらからプロファイル設定を完了することをおすすめします。 セットアップウィザード	

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。

アイル設定	
プロファイルD	dev4_MP201202030989
制模名(英語)	Global Sign K.K.
即要名(英語)	

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。

プロファイルセッ	トアップウィザード		
更新設定	1		
証明書の更新時に申請や承認の?	フローを必要としますか?		
・手動 ユーザからの申請を管理者が承認 永防後、証明書取得メールがユー ・自動 ユーザからの申請後、すぐに回い (管理者による承認が不更とな) ・クイック 更新定内メールが証明書取得メー (ユーザからの申請と管理者に、 ●更新変内メールは有効期限305	8年る必要があります。 ーザに送信されます。 月敷取得メールがユーザに送信され: ります。) ールになっています。更新旅内メー」 とる承認が不要となります。) 前に1度だけ送信されます。	ます。 しからすぐに証明書が取得でき	а т.
更新タイプ	⊙ ≠8⊖88⊖2	192	
-	tho.	200	

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 DE			5 m
紅田市をファイド語見なの間冷から到底に			
に対象で ノアイ 20年515の7日期でに利用す	こなりますか?		
Encrypted File System オプションを有り この設定に対応するアプリケーションを行 現時点で不明の場合は、そのまま"次へ"お	にすることで、発行される証明書の 使用する際にご利用ください。 溢みください。ウィザード売了後	D拡張キー使用法に「暗可化ファイ) もメニューからいつでも設定の変更	レシステム」が追加されます。 が可能です。
Encrypting File System	Car C 34 9		
(a)	前へ	次へ 0	
2	i		

【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。

プロファイルセットアッ	ブウィザード			
エクスポート不可設定	1			
証明書利用者に、証明書のエクスポート(コ	ピー利用)を許可しますか?			
エクスポート不可オプションを有りにするこ 制限することができます。 こちらのオプションは、Windowsの機能をF また、PKCS12オプションを利用することが	とで、ユーザ端末で証明書を: 用するため、証明書を取得で、 できなくなります。	ミクスポートすることがで ぎるブラウザがInternet Ex	きなくなり、証明 plorerのみに制取さ	着を利用する端末を れます。
秘密種エクスポート不可 Internet Explorer ちみに東定されます。	@mL_mo			
e	#^	次へ		

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。

曲システムからAPIを利用しますか? IPIオプションは、マネージドPKIのAPIを使用する場合に設定いただきます。 プローパルサインのシステムと連携するお客様サーバのPPアドレスをご指定ください。 最終を許可するIPアドレスを制設することで、セキュリティを強化します。 IPIを利用しない場合は、空様のまま次へお進みください。 API IPアドレス API IPアドレス	API設定	
PIオプションは、マネージドPN0のAPIを使用する場合に設定いただきます。 /ローバルサインのシステムと達然するお客様サーバのPPアドレスをご推定ください。 樹を許可するIPアドレスを制取することで、セキュリティを強化します。 PIを利用しない場合は、空僕のまま次へ利加みください。 API IPアドレス AP I 使用時のみに販売されます。	システムからAPIを利用しますか?	
API #アドレス AP 1 使用時 のみに推定されます。	PMオンションは、マネージトPMのAPM パローバルサインのシステムと連携する(聴気を許可するIPアドレスを制設すること PIを利用しない場合は、空積のまま次^	を使用する場合に認定いたださます。 お客様サーバのPPアドレスをご推定ください。 とで、セキュリティを強化します。 へお流みください。
90 90 211.11.148.248.211.11.148.250		

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。

<u>A:「証明書発行」の申請~発行までの手順</u>

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。

 サーバ証明書 (EDI・ヤフー環線証明書を含む)
 その他証明書 (コードサイニング・PDF)
 マネージドPKI

 証明書発行

 ご明書発行(一括)

 証明書発行(管理者一括)

 管理者一括発行履歴

 承認侍ち証明書一覧

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。

1.9-CARR	2.寬7	\geq	
70774888 »	DNSHEAD 39 HEE		
ナービス内容の選択	R		
カファイル			
1077-1NO	BaseON	総構名 (英語)	部署名 (英語)
AP201911291486	無い	and when	and spectra
トイセンス			
H-U7			ライセンス推動
2-64			the second se
● マネージドPHO Lite 監門	法人名用 1年		

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。

目前へ	次へは

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。

個人情報の取り扱いについて	
GMOグローバルサインは、本申し込みにあたりお い適正に管理します。当社規定に関しては、以下の さまは該当べージをご確認下さい。本サービスの申 みなします。	預かりしたお客さまの個人情報を当社規定に従 ページで詳しくご案内しておりますので、お客 込に当たっては、下記の内容に同意したものと
個人情報の取り扱いについて	個人情報保護法にもとづく公表事項
0 前へ	完了するの

5.申請完了後の画面です。

証明書お申し込み		
1.サービス選択	2. 荣了	
申し込み完了		
完了		
オーダーID	MF \$20191202673896	

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 にコピーされろ値		
Commonwanie	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 >

SVフアイル相正 アイルには、登録情報がCSV形式で格納 た、ファイルの最初の行には、フィール 択したプロファイルに基づいて、データ ータの項目は、カンマ(、)で区切られて :	されている必要があります。 ド名が含まれている必要があります。 別が必要となります。 いることが必要です。			
mmonName ,Email ,SANRFC822 Email , te Jones ,kate jones@globalsign.com ,ka nnifer Jones ,Jennifer jones@globalsign.c rorge Jones ,George jones@globalsign.c	Address ,PickupPassword ,haveCSR ,PKCS12 ,UPN ,Security ite.jones@globalsign.com ,9o719ghsa3 ,true ,false ,admin@gli com ,Jennifer.jones@globalsign.com ,9o719ghsa3 ,false ,false om ,George.jones@globalsign.com ,9o719ghsa3 ,false ,true ,a	/ Identifier obalsign.com ,S-1-1-11-0 ,admin@globalsign.com ,S idmin@globalsign.com ,S		
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		
Email Address	s メールアドレス			
SANRFC822 Email Address	Email Address SANRFC822 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 パスワードを目動生成 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		
CSVファイル	ファイルの選択ファイルが選択されていま	きせん アップロード		
メールテンプレート				
「夜田するい いっとゴレートも、空切して	ください	日本語 - JA 🗸		
週用9 のメールテノノレートを選択して		· · · · · · · · · · · · · · · · · · ·		

*【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。

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喜づいて、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 Identif

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。

	А	В	С	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
	コモンネーム	半角英数、または全角(UTF-
CommonName		8) 64 文字以内
OrganizationUnit	所属 2	半角英数記号『,+/()』また
organizationonit		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
	メールアドレス	半角英数 128 文字以内
	【補足】	
	Email Address または Contact Email Address のいずれかの入	
	力が必須です。	
Email Address	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。)	
	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	半角英数 128 文字以内
SANREC822 Email	ドレスを利用する」について「はい」を選択した場合、証明書	
Addross	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	
Address	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。	
	連絡用メールアドレス	半角英数字 8 文字~64 文
Contact Email		字。
Address		証明書取得用パスワードを自
Audress		動生成する場合は、
		"AUTOGEN"を設定。

		1
	証明書取得用パスワード	半角英数字 8 文字~64 文
PickupPassword		字。
have CCD	VPN 機器等で CSR を用意している方は、"true" または "on" を	true/on false/off/設定なし
navecsk	設定。	
	証明書を PKCS12 形式でダウンロードする場合、"true" または	true/on
PRC312	"on" を設定。	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	セキュリティ識別子	半角英数-(ハイフン)128
Identifier(SID)		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。 	半角英数、または全角 (UTF-8)64 文字以内
	 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。 	
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。	Email Address
	必須項目ですので、必ず入力してください。	

	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
PickupPassword		動生成する場合は、
		"AUTOGEN"を設定。
haveCCD	VPN 機器等で CSR を用意している方は、"true" または "on" を	true/on
navecsk	設定。	false/off/設定なし
	証明書を PKCS12 形式でダウンロードする場合、"true" または	true/on
PRCSIZ	"on" を設定。	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	セキュリティ識別子	半角英数-(ハイフン)128 文
Identifier(SID)		字以内
	名前	半角英数、または全角(UTF-
GivenName	※SurName と組み合わせることでコモンネームとして利用可	8) 31 文字以内
	能です。	
SurName	名字	半角英数、または全角(UTF-
Surraine	※コモンネームとして単体で利用可能です。	8) 31 文字以内
	スードニム	半角英数、または全角(UTF-
	※コモンネームとして単体で利用可能です。	8) 64 文字以内
	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。	
Pseudonym	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。	

※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。

サーバ証明書 (EDI・ヤフー提携証明書を含む) ① (コ	その他証明書 ードサイニング・PDF)	⋜⋨ − ジドРКІ	•
証明書			
 ● 証明書発行(一括) 			
 ○ 証明書一覧 ○ 証明書発行(管理者→括) 			
 ● 管理者→括発行履歴 ● 承認待ち証明書→覧 			

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。

1.9-EAB	2.97					
プロファイル選択	>> DNSHEA.71 3> 4823					
ナービス内容の	選択					
077414						
パロファイルロ	BaseON	組織名 (英語)	部署名 (英語)			
IP201911291486	無し	The second secon				
イセンス						
サービス	サービス					
 マネージドPK0 LA 	e 影門/法人名用 1年					

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-1-1-11-0123456789-0123456789-0123456 false ,Jennifer.jones@globalsign.com ,Jennifer.jones@globalsign.com ,9o7t9ghsa3 ,false ,false ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789 false .George.jones@globalsign.com ,George.jones@globalsign.com ,9o7t9ghsa3 ,false ,true ,admin@globalsign.com ,S-1-1-11-0123456789-0

	incers.	DINT-Aven
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。	半角奏数128文字以内
SANRFC822 Email Address	SANRFC822 Email Address	Email Address
PickupPassword	証明直取得用バスワード	半角英数字 8文字~ 64文字,証明書取得用 パスワードを目動生成 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
JPN.	ユーザーブリンシバル名	半角英数128文字以内
curity Identifier	セキュリティ識別子	半角英数- (ハイフン) 128文字以内
livenName	企業RAは申請者個人の身元属性を要付ける証拠 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
iurName	企業RAは申請者個人の身元風性を要付ける証拠 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
seudonym	企業RAは申請者個人の身元属性を実付ける証拠 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) 84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る	ません アップロード
メールテンプレート		
	1++++	FI * 25 1A *

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。

ウービス488番目 》 CSVファイル描定 》 画 》 構造 CommonName Faceural Xールアドレス - E SANRFC822 Email Address (a) 取用書物信用パスワード(a) CSRを既に持っている PKCS12オブター Ox - ルアドレス @ 低人名 または peudonym Annorogen autogen 0.0	サーL ま の Com のメ・ の頃, pseu のメ・ の気・	ビス内容選択 >> mmonName Required にしたアドレス いたのとい	CSVファイル指定 🍛 🖁 メールアドレス = E	i <mark>()</mark> → #2	SANRFC822 E	mail Address ∞ 2/3					1
CommonName Request メールアドレス = E SANRFC822 Email Address (a) (a) 延明書取個用パスワード (a) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	Com OX- @@ pseu	nmonName Required ールアドレス い人名 または udonym	メールアドレス = E		SANRFC822 E	mail Address⊛@a					1
CommonName Request メールアドレス = E SANRFC822 Email Address (2) 延期書取得用パスワード(2) CSRを提に持っている PKCS12オブシ 〇メールアドレス (9) (日名 素 志は pseudonym (1)	Com Ox- @ pseu Ox- @ g	nmonName Required にールアドレス IL人名 または udonym	メールアドレス=E		SANRFC822 E	mail Address 🖓 🖓		-			1
OX-ルアドレス Itaro yamada@globalsign.com autogen Itaro yamada@globalsign.com OX-ルアドレス Itaro yamada@globalsign.com autogen Itaro yamada@globalsign.com OX-ルアドレス Itaro yamada@globalsign.com autogen Itaro yamada@globalsign.com OX-ルアドレス Itaro yamada@globalsign.com taro yamada@globalsign.com autogen Itaro yamada@globalsign.com Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: St	Ox- © pseu Ox- © (D)	ペールアドレス I人名 または						証明書取得用パスワ	7ード※必須	CSRを既に持っている	5 PKCS12オプショ
●国人名 または pseudonym Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com ○メールアドレス ●国人名 または pseudonym Iaro.yamada@globalsign.com Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com ○メールアドレス ●国人名 または pseudonym Iaro.yamada@globalsign.com Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com ●メールアドレス ●国人名 または pseudonym Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com Iaro.yamada@globalsign.com ●メールアドレス ●国人名 または pseudonym Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com Iaro.yamada@globalsign.com ●メールアドレス ○国人名 または pseudonym Iaro.yamada@globalsign.com autogen Iaro.yamada@globalsign.com Iaro.yamada@globalsi	●個 pseu のメ・	I人名 または Idonym						1	_		
pseudonym Image: state in the constraint of the constrai	pseu 〇メ・ ●個	idonym			taro.yamada@)globalsign.com		autogen		0	
OX-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com taro yamada@globalsign.com autogen □ □ OX-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com taro yamada@globalsign.com autogen □ □ ®MAA2 または pseudonym taro yamada@globalsign.com taro yamada@globalsign.com autogen □ □ ®A-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □ @A-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □ @X-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □ @X-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □ @X-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □ #X-ルアドレス @EdA2 または pseudonym taro yamada@globalsign.com autogen □ □								1.			
●個人名 または taro.yamada@globalsign.com taro.yamada@globalsign.com autogen □ ○メールアドレス ●個人名 または taro.yamada@globalsign.com taro.yamada@globalsign.com autogen □ ●「メールアドレス ●「メールアドレス ●「メールアドレス ●「 □ □ ●「メールアドレス ●「 ●「 ●「 □ □ ●「メールアドレス ●「 ●「 ● □ □ ●「 ●「 ● ● ● ● ● ●「 ●「 ●	06	ールアドレス							-		-
Ox - \UZ PK UZ Iaro yamada@globalsign.com Iaro yamada@globalsign.com Iautogen Iauto	DODU	人名 または	taro.yamada@globalsi	gn.com	taro.yamada@	globalsign.com		autogen			
Image: Second Pick Pick Pick Pick Pick Pick Pick Pick	pseu				_						
mary marked galaxies marked		人名 または	taro vamada@globalsi	an com	taro vamada@	alobalsion com		autogen	- I	D.	
●メールアドレス Itaro yamada@globalsign.com autogen □ □ ●風人名 または □ Itaro yamada@globalsign.com □ □ □ ●風人名 または □ Itaro yamada@globalsign.com □ □ □ □ ●風人名 または □ Itaro yamada@globalsign.com □	pseu	udonym	ano.yumuuuuugjobaloij	gn.oom	turo.y unitudu(giobaloign.com		uutogen	-		
○個人名 または taro.yamada@globalsign.com autogen □ □ ◎メールアドレス ○個人名 または □ □ □ □ ○個人名 または □ □ □ □ □ □ □ ◎メールアドレス □ <td>®×.</td> <td>ールアドレス</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>1</td>	®×.	ールアドレス									1
pseudonym ●メールアドレス ●メールアドレス ● ■ ■ ■ ■ ■ ①個人名 または pseudonym ● ● ■ ■ ■ ■ ■ ●メールアドレス ○個人名 または pseudonym ● ■ ■ ■ ■ ■ ● ● ■ ■ ■ ■ ■ ● ● ■ ■ ■ ■ ● ■ ■ ■ ■ ■ ● ■ ■ ■ ■ ● ■ ■ ■ ■		人名 または	1		taro.yamada@	globalsign.com		autogen			
●メールアドレス 〇風入名または pseudonym Iaro. yamada@globalsign.com autogen □ □ ●メールアドレス 〇風入名または pseudonym Iaro. yamada@globalsign.com autogen □ □ ●メールアドレス 〇風入名または pseudonym Iaro. yamada@globalsign.com autogen □ □ ●メールアドレス ○風入名または pseudonym Iaro. yamada@globalsign.com Iaro. yamada@globalsign.com □ □	pseu	udonym							-		
Olig 人名または pseudonym taro.yamada@globalsign.com lautogen ・シールアドレス Olig 人名または pseudonym taro.yamada@globalsign.com autogen ・レア・ブレート JA	©×.	ールアドレス							_		-
●メールアドレス ○個人名または pseudonym Itaro.yamada@globalsign.com autogen □ ールテンプレート JA		人名 または			taro.yamada@	globalsign.com		autogen			
●メールアトレス ○個人名または pseudonym Itaro.yamada@globalsign.com Iautogen IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	pseu	udonym									
Disk a s/Lik pseudonym JA	OF.	レールアトレス 1.1ターキキル			taro yamada/	alabalsian com		autogon	- T	n.	6
ールテンプレート JA	pseu	udonym			[laio.yamada@	ggiobalsign.com		autogen	5		0
ールテンプレート JA	1.000						1				1
	ールテン	ンプレート	JA								
			前へ		次へ	0					
前へ、次への			100 C								
ロ 前へ 次へ ロ											
0 前へ 次へ 0	_										

無し

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。

完了する

taro.yamada@globalsign.com 357cdb1f

6 taro.yamada@globalsign.com

個人情報の取り扱いについて

個人情報の取り扱いについて

JA

GMのグローバルサインは、本用し込みにあたりお預かりしたお客さまの個人情報を当社境定に従い 通正に簡整します。当社規定に関しては、以下のページで詳しくご案内しておりますので、お客さま は該当ページをご確認下さい。本サービスの申込に当たっては、下記の内容に同意したものどみなし ます。

前へ

メールテンプレート

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 パネルのオーダーー覧より該当の証明書を検索することで、 確認が可能です。

無し

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。

Given

Sur

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。

SVファイル指定		
1アイルには、登録情報がCSV形式で格納 た、ファイルの暴初の行には、フィール 訳したプロファイルに高づいて、データ ータの項目は、カンマ() で区切られて 」:	iされている必要があります。 ド名が含まれている必要があります。 列が必要となります。 こいることが必要です。	
ommonName Email SANRFC822 Email ate Jones kate jones@globalsign.com k ennifer Jones Jennifer jones@globalsign eorge Jones ,George jones@globalsign.	Address, PKCS12 Password, UPN, Security Identif ate.jones@globalsign.com9o7t9ghsa3YZ.admin@ .com.Jennifer.jones@globalsign.com.AUTOGEN.ac com.George.jones@globalsign.com.AUTOGEN.ac	ler Iglobalsign.com ,S-1-1-11-0123456 admin@globalsign.com ,S-1-1-11-0 Imin@globalsign.com ,S-1-1-11-01
		I show when
项目	說明	制限事項
項目 CommonName	説明 コモンネーム	制限事項 半角英数、または全角 (UTF-8) 64文字以内
项目 CommonName Email Address	説明 コモンネーム メールアドレス	制限事項 半角英数、または全角 (UTF-8) 64文字以内 半角英数128文字以内
項目 CommonName Email Address SANRFC822 Email Address	説明 コモンネーム メールアドレス SANRFC822 Email Address	 制限事項 単角英数、または金角 (UTF-8) 64文字以内 半角英数128文字以内 Email Address
项目 CommonName Email Address SANRFC822 Email Address PKCS#12 Password	説明 コモンネーム メールアドレス SANRFC822 Email Address PKCS#12/パスワード	制限事項 単角英数、または全角 (UTF-8) 64文字以内 半角英数128文字以内 Email Address Please use "AUTOGEN"
項目 CommonName Email Address SANRFC822 Email Address PKCS#12 Password UPN	20月 コモンネーム メールアドレス SANRFC822 Email Address PKCS#12/(スワード ユーザーブリンシ/()ル名	制限事項 半角英数、または全角 (UTF-8) 64文字以内 半角英数128文字以内 Email Address Please use "AUTOGEN" 半角英数128文字以内
Implement CommonName Email Address SANRFC822 Email Address PKCS#12 Password UPN Security Identifier	説明 コモンネーム メールアドレス SANRFC822 Email Address PKCS#12/(スワード ユーザープリンシ/いい名 セキュリティ識別子	 制限事項 単角英数、または全角 (UTF-8) 64文字以内 半角英数128文字以内 Email Address Please use "AUTOGEN" 半角英数128文字以内 半角英数128文字以内 半角英数・(ハイフン) 128文字以内
項目 CommonName Email Address SANRFC822 Email Address PKCS#12 Password UPN Security Identifier CSVファイル	 説明 コモンネーム メールアドレス SANRFC822 Email Address PKCS#12/(スワード ユーザーブリンシ/いル名 セキュリティ識別子 ファイルの選択 ファイルが選択 	 制限事項 単角英数、または全角 (UTF-8) 64文字以内 半角英数128文字以内 Email Address Please use "AUTOGEN" 半角英数128文字以内 半角英数128文字以内 半角英数-(ハイフン) 128文字以内 されていません

【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

	メールアドレフ	半角苗粉 128 立空以内
Email Address		十月英载 120 文于以内
	Email Address または Contact Email Address のいうれかの	
	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。)	
	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	半角英数 128 文字以内
	ドレスを利用する」について「はい」を選択した場合、証明	
SANRFC822 Email	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	
Address	ネームの「E メールアドレス」と、「SANRFC822name」の	
	項目に、Fメールアドレスの情報が格納されます。	
	連絡用メールアドレス	半角英数字 8 文字~64 文
Contact Email Address		字。
		- 5° 証明書取得用パスワードを自
		動生成する場合け
		新工成 f る初日は、 "AUTOGEN!"を設定
PickupPassword	証明者取得用ハスリート	十月央奴子 0 又子~04 又子。
haveCSR	VPN 機器等で CSR を用意している方は、"true" または "on"	true/on false/off/設定なし
	を設定。	
PKCS12	証明書を PKCS12 形式でダウンロードする場合、"true" また	true/on
	は "on" を設定。	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	セキュリティ識別子	半角英数-(ハイフン)128 文
Identifier(SID)		今回み

【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
	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。	半角英数、または全角 (UTF-8)64 文字以内
CommonName	 ■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 	
Email Address	スのみが登録可能です。 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	セキュリティ識別子	半角英数-(ハイフン)
-----------------	-----------------------------------	----------------
Identifier(SID)		128 文字以内
	名前	半角英数、または全角
GivenName	※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	(UTF-8)31 文字以内
	t,	
SurNamo	名字	半角英数、または全角
Surname	※コモンネームとして単体で利用可能です。	(UTF-8)31 文字以内
	スードニム	半角英数、または全角
Pseudonym	※コモンネームとして単体で利用可能です。	(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。

サーバ証明書 (ED)・ヤフー提携証明書を含む)	その他証明書 (コードサイニング・PDF)	⋜⋨ ౼ ジドРКI 💿
 証明書 ● 証明書発行 ● 証明書発行(一括) ● 証明書再発行(一括) ● 証明書一覧 		
 ○ 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.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。

12	-ビス内容の選拔	2		
	10771140	BaseDN	組織名 (英語)	部署名 (英語)
۲	/P201911291485	無し	The second	The second second
i-rt	:>ス			
	サービス			ライセンス残数
۲	マネージドPKI Lite 取得	法人名用 1年		
0	マネージドPKI Lite 個人:	Concernance of Concer		

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。登録債報が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専づいて、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 ,907t9ghsa3 ,true ,false ,admin@globalsign.com ,S-1-11-0123456789-0123456789-0123456 false ,Jennifer jones@globalsign.com ,Jennifer.jones@globalsign.com ,907t9ghsa3 ,false ,false ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789false .George.jones@globalsign.com ,George jones@globalsign.com ,907t9ghsa3 ,false ,true ,admin@globalsign.com ,S-1-1-11-0123456789-0123456789-

44.03	說明	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	証明層取得用バスワード	半角英数字 8文字~ 84文字, 証明書取得用 パスワードを目動生成 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/設定たに、
JPN	ユーザープリンシバル名	半角束数128文字以内
ecurity Identifier	セキュリティ戦別子	半角英数- (八イフン) 128文字以内
livenName	企業RAは申請者個人の身元属性を実付ける証拠 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
iurName	企業RAは申請者個人の身元属性を要付ける証拠 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
seudonym	企業RAは申請客個人の身元属性を実付ける証拠 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る	ません アップロード
メールテンプレート		
	ださい	日本語、A>

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。

No	CommonName Required	メールアドレス = E	SANRFC822 Email Address	証明書取得用パスワード※必須	CSRを既に持っている	PKCS12オプション	-
ĺ	〇メールアドレス ・ 個人名 または pseudonym		taro.yamada@globalsign.com	autogen	Ō.	D	(
2	○メールアドレス ●個人名 または pseudonym	taro.yamada@globalsign.com	taro.yamada@globalsign.com	autogen		٥	C
3	〇メールアドレス ●個人名 または pseudonym	taro.yamada@globalsign.com	taro.yamada@globalsign.com	autogen	<u>a</u>		C
	 ・メールアドレス ○個人名 または pseudonym 		taro.yamada@globalsign.com	autogen	0	D	C
	 ●メールアドレス ○個人名 または pseudonym 		taro.yamada@globalsign.com	autogen	0	D	C
	・ ・ メールアドレス つ個人名 または pseudonym		taro.yamada@globalsign.com	autogen	0	D	C
x-	ルテンプレート	JA					

忍											
D	氏名 = CN	メールアドレス = E	SANRFC822 Email Address	証明書取得用パスワード	CSRを既に持っている	PKCS12オプション	ユーザープリンシバル名	セキュリティ識別子	GivenName	SurName	Pseudonym
T	Given Sur		taro.yamada@globalsign.com	e601666e	無し	無し			Given	Sur	
T	Sur	taro.yamada@globalsign.com	taro.yamada@globalsign.com	e250f1eb	無し	無し				Sur	
T	PSE	taro.yamada@globalsign.com	taro.yamada@globalsign.com	e68b20c1	無し	無し					PSE
T	iaro.yamada@globalsign.com		taro.yamada@globalsign.com	5dfc6134	無し	無し				Sur	
T	iaro.yamada@globalsign.com		taro.yamada@globalsign.com	ffa576d9	無し	無し					PSE
	taro.yamada@globalsign.com		taro.yamada@globalsign.com	357cdb1f	無し	無し			Given	Sur	
個日面	人情報の取り扱いについ MOグローバリンドンは、本甲 Eに管理します。当社規定に開 炭当ページをご確認下さい、オ す。	て し込みにあたりお預かりしたお しては、以下のページで詳しく: 'サービスの申込に当たっては、'	をさまの個人情報を当社規定にな ご案内しておりますので、お客さ 下記の内容に同意したものとみな	乱い 注意 実し							
はま											

6.左部メニューの「管理者ー括発行履歴」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。

マネージドPKI 証明書 ● 証明書発行	PKCS#12一覧画面 ・条件を入力し、検索ボタンを押してください。	
 ● 証明書発行(一括) ● 証明書再発行(一括) 	PKCS#12・オーダーID	
 ○ 証明書一覧 ○ 証明書発行(管理者一) 	プロファイル・オーダーID	
 5 短 第 3 2 5 3 7 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8	ライセンス・オーダーID	
● 目注目 1月光11版座 ● 承訟付り証明書 夏	申請日	例) 2010/11/01
ライセンス ● ライセンス追加購入	発行日	例)2010/11/01
♥ ライセンス購入腹壁	表示件数	
 ノロノアイル ○ プロファイル設定 ○ プロファイル追加申請 	検索 セット	

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。

プロファイル・オーダーID	ライセンス・オーダー・ID	アップロード件数	ダウンロード
MP200907150326	ML200907291832	3	ダウンロード
MP200907150326	ML200907291832	5	ダウンロード

<u>D: ユーザによる申請~発行までの手順</u>

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。



ボー	ータル	
	プロファイルID	MP200905210053
	組織名(英語)	GlobalSign K.K.
	部署名(英語)	sales - authenticated by LRA
	URL	https://system.globalsign.com/cr/public/certificate /order.do?p=a6f6244c92e7b以下省略
	URL(PKCS12オプション)	https://system.globalsign.com/cr/public/certificate /order.do?p=ab5c1232098d7 以下省略

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。

Ā	承認待ち証明書										
		編集	オーダーID	登録タイプ	証明書管理者	サービス名	PKC \$12オプション	コモンネーム	メールアドレス	証明書有効期間	種別
	Ē	續生	MPS201511172833	ポータル		マネージド PKI Lite 部 門/法人名	= 1.	teet	mitsuhiro sugino@globalsign.com	1 年	新相
4	-	NINE AC	MP3201011172000	4. 24		用 100 pack	<i></i>	1631	misuni o.sugiro@giobaisgn.com	14	101 105
	•	編集	MPS201406180243	ボータル		マネージド PKI Lite 部 門/法人名 用 10 pack	無し	test2014	mitsuhiro.sugino@globalsign.com	1年	新規
					キャンセ	zル処理 内	和認処理				

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URLIC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 ト記URLIC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。バ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

国/地域 = C	日本 - JP
組織名 = O ※半角英概、または金角(UTF-8)64文字以内	GlobalSign K.K.
氏名 = CN 2010 ※半角英觀、または全角(UTF-8)64文字以内	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
● 個人名 ○ pseudonym	(名前) 【名字 】 】
8.4555769篇	pseudonym
SAN RFC 822	メールドメインを選択してメールアドレスを入力 ※メールドメインをりストから選択のうえ、アドレスの構善をかの傷に入力してくたさい。 @マークの入力も必要です。 . メールドメインリスト ↓ メールアドレスの確認 メールアドレスを入力してください。
アクセス認証にEメールアドレスを利用す る ® 40分	 ()しいえ ()はい
ユーザープリンシバル名	
セキュリティ識別子	
誕生成オプション	 .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。 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。 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:※※	〔日本語 - JA ✔
証明書取得用バスワードを必須	※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ホタンを押下すると、ランダムなバスワードを自動作体ノセットを行い
	ます。

【アクセス認証用中間 CA】のプロファイルの場合

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	Токуо
市区町村 = L ※半角英歌、または全角(UTF-8)128文字以内	Shibuya
組織名 = O ※半角長数、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※20月	
アクセス認証にEメールアドレスを利用す る ※必須	Oltin
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。 C SR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、こちらをご選択を ださい。 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の通	□日本語 - JA V
証明書取得用パスワード金永道	※半角英数8文字以 パスワード自動生成 パスワード自動生成メタンを押下すると、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) 🖦 🖗 🕮	※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 + 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: 証明書のコモンネーム(CN)に、任意の値を設定可能です。 	Taro Yamada
O(Organization) <mark>※必須</mark>	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) <mark>※必須</mark>	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) <mark>※必須</mark>	「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。	<u>support-</u> 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 <mark>※必須</mark>	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。

<u>・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。</u>

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。

<u>A:証明書の再発行を1枚ずつ行う手順</u>

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。

サーバ証明書 (EDI・ヤフー提携証明書を含む)	その他証明書 (コードサイニング・PDF)	マネージドPKI 💿
<mark>証明書</mark> ● 証明書発行 ● 証明書発行(一括) ● 証明書再発行(一括) 		
 ○ 証明書一覧 ○ 証明書発行(管理者一括) ③ 管理者一括発行履歴 ③ 承認待ち証明書一覧 		

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。

例)MPS2	01207030574かJohn	Smith	0		簡易検索	
申請日 全ての ¹ ブロファ 部署名	 ・ 期間 サービス ・ 全て イルロ ライセ メール 	指定 • F の証明書オ・ シスID シアドレス	列) yyyy/mm/d ーダーステー ▼	d 目 と [全ての証 証明書管 全てのメ	(列) yyyy/mm/dd E明書ステータス E理者 ニールデンプレート 検索	• •
表示件数:	10 •					
1 - 10 /85						
		C	<u>SV出力</u> <1234	456789	LDIF出力 次へ >	
各種申請	オーダーID	組織名	コモンネーム	サービス名	証明書有効期間	メールア
申請	MPS20160331143240	tuika	fxtestsugino	マネージド PKI Lite 部 門/法人名 用 100 pack	1年	mitsuhir
				▽ネージド		

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。

証明書失効申請 証明書保留 キャンセル申し込み 証明書再発行 PKCS#12ダウンロード メール送信一覧

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。

	[L	
目生成オプション	 .pfx (PKCS#12) としてダウンロ 証明書取得時に、証明書、中間CA証 れた.pkファイルとしてダウンロード ドを設定して鍵を保護する必要があい CSRによる発行 HSM等で課を管理するためにCSRで ださい。 Microsoft EdgeのInternet Explo ブラウザ健生成構能を用いて証明書が は、こちらをご選択ください。 	1ードする 明書、秘密鍵が1つにバックージング にします。。ptxファイルは熱しいバスク ります。 申請が必要な場合は、こちらをご送り rer互換モードによる発行 を発行し、USBトークンに格納する場
メールテンプレート×必須	日本語 - JA V	
証明書取得用パスワード=20家	パスワード自動生成 パスワード自動生成	※半角英語(文字以) 5ンダムな/(スワードを目的作成/セットを)
証朝吉取得用バスワード(確認用) ■@編		※參與英語8文字以1
メモ模		
O. 1	ĵΛ.	次へ 🝺

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。

<u>B:「証明書再発行(一括)」の再発行申請~再発行までの手順</u>

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。

SVファイル指定 アイルには、登録債報がCSV形式で格納されていた、ファイルの最初の行には、フィールド名が含い 旅したプロファイルに基づいて、データ列が必要 一タの項目は、カンマ(、)で区切られていること 度につき200件まで申請することができます。 : -ダーID、証明書取得用パスワード PS20200522340049,1w8uj7654	る必要があります。 まれている必要があります。 となります。 が必要です。	
項目名	說明	制限事項
オーダーID	MPS****, MAS****	証明書ステータス発行 済み且つ有効期限あり ※証明書発行(留理者 一括)からの申込は利 用できません
証明書取得用パスワード	管理者がユーザーに通知するパスワード	半角英数8文字以上64 文字以下
CSVファイル	ファイルを選択 選択されていません	アップロード
メールテンプレート		
		日本語 - JA Y

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。

編集		
No	オーダーID	証明書取得用バスワード
1	MPS20210526741163	and a second sec
メールテンプレート	AL	
	前へ	次へ

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。

<u>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</u>

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。

サーバ証明書 (EDI-ヤフー提携証明書を含む)	その他証明書 (コードサイニング・PDF)	マネージドPKI 🗉
 証明書発行 ● 証明書発行(一括) ● 証明書再発行(一括) ● 証明書一覧 ● 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 		

2.「検索」をクリックし、オーダーの一覧を表示します。

PKCS#12一覧画面				
・条件を入力し、検索ボタンを押してください。				
PKCS#12・オーダーID				
プロファイル・オーダーID				
ライセンス・オーダーID				
申請日	例) 2010/11/01			
発行日	例) 2010/11/01			
表示件数	10 🗸			
検索 リセット				

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。

PKC S#12・オーターID サービス名 証明書年数 プロファイル・オーダーID ライセンス・オーダーID PKC S#12・オーダー ・ステータス 申請日 発行日 アップロード件数		MPB202007290562 マネージドPKI Lite byGMO 無制限 1 年 MP201805171166 ML202003162052 発行済み 2020年07月30日 08:32(GMT+09:00)									
						2020年07月30日 08-39(GMT+09-00) 2					
									発行件数		1
						オーダーロ	メールアドレス	コモンネーム	部署名	証明書オーダーステータス	証明書ステータス
										再発行済み	発行済み
										発行済み	発行済み

※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。

1	A	В	С
1	オーダーID	PKCS#12 Password	
2	MPS20210129733290	-	
3	MPS20210129733291		
4			

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。

S構されている必要があります。 -ルド名が含まれている必要があります。 - 今列が必要となります。 1ていることが必要です。	
民朝	制限事项
MPStree	証明書ステータス第17 済み目つ有効増限あり ※証明書発行(管理者 一括)からの申込は利 用できません。
PKCS#12/C2/7- H	半角英数字 12文字~ 117文字。
ファイルを選択 目択されていません	アップロード
	_
前へ 次へ	1.0
	 協されている必要があります。 小ド名が含まれている必要があります。 ウ別が必要となります。 1ていることが必要です。 取明 MPS**** PKCS#12/12ワード ファイルを選択 取えされていません 前へ 次へ

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。

オーダーロ	PKCS#12 パスワード×20月 半均美部子 12文字〜117文字
MPS20210129733290	
MPS20210129733291	
	オーダーID MPS20210129733290 MPS20210129733291

管理	者一括再発行 画面	
		管理者一括再発行 完了
	PKCS#12 オーダーID	MPB202105270648
這再更	I明書の再発行には時間が掛かります。 1発行された証明書は管理者一括発行履歴から該当の 2得してください。)PKCS#12・オーダーIDをクリックし、リンク先のダウンロードボタンから

7. 左部メニューの「管理者ー括発行履歴」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。

マネージドPKI 証明書 © 証明書発行	PKCS#12一覧画面 ・条件を入力し、検索ボタンを押してください。	
 ● 証明書発行(一括) ● 証明書再発行(一括) 	PKCS#12・オーダーID	
 ○ 証明書一覧 ○ 証明書発行(管理者一) 	プロファイル・オーダーID	
 ▲ 第日来一任祭行房屋 	ライセンス・オーダーID	
● 自吐日 10元17版正 ● 承認付り証明者一見	申請日	例) 2010/11/01
ライセンス ● ライセンス追加購入	発行日	例) 2010/11/01
♥ ライセンス購入限定	表示件数	10 ~
 プロファイル設定 プロファイル追加申請 	検索レント	

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。

プロファイル・オーダーID	ライセンス・オーダー・ID	アップロード件数	ダウンロード
MP200907150326	ML200907291832	3	ダウンロード
MP200907150326	ML200907291832	5	ダウンロード

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。

	•Microsoft Edge	Windows 証明書ストア
Windows	Chrome	
	• Firefox	FireFox 証明書ストア
	Chrome	Mac キーチェイン
Mac	• Safari	
	• 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

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

<u>A:ブラウザの鍵生成機能を用いた証明書の取得手順</u>

※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。

証明書取得用パスワード入力	
正明書取得用 エア明の場合は正	取るロードを入力してください。
	<u>**</u>

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。

	図 証明書をエクスポート可能にする場合は、チェックを入れてくだれ、
暗号化プロバイダ 憲法書	Microsoft Enhanced Cryptographic Provider v1.0 •
電子著名 (5/MINE) 用証明	1巻(マネージドPRIエンドユーザー用)サービス利用約款
電子署名(5/NINE)用計9	9巻(マネージドaxtエンドユーザー用)サービス利用約款(以下、「本利
第1章 定義	
第1巻 (定義) 本利用約款中で使われてい	も用語は、特段の定めがない限り、以下の意味を有するものとします。

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。

正明書取得用バスワー	-ド入力
	証明書取得用パスワードを入力してください。
証明書の甲込 ご自身でパスワー	ビックアップパスワードをお忘れの方へ。 しを行った管理者に遠絡して、ビックアップパスワードの設定を確認してください。 - ドを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください
	次へ 🗉

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

提保護パスワード	
隠保護パスワード (確認用)	
グローバルサイン電子証明書サービ	又利用約款 5.1 -
本利用約款が英語以外の言語に翻訳 とし、本利用約款の奏項の解釈の唯	されている場合でも、本利用約款の英語版を常に原本 一の基礎となるものとします。
グローバルサイン電子調明書サービ ローバルサイン株式会社(以下「グ	ス利用約款(以下「本利用約款」という)は、GMO ラ モーバルサイン」又は「当社」という)が提供する電
十部明書で利用者(以上「利用者」 です。電子証明書の利用をご希望の 読みください。電子証明書を申し込	という)がこれ用になっための利用は条件を運動にもの。 利用者は、サービスの利用に先立ち、本利用約款をあっ むことにより、利用者は本利用約款の当事者となり、
利用規約に同	夏の上、「広へ」ボタンモクリックしてください。
	200
	444 N

・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。

避保護パスワード	T#7ewi-2041?.SI
グローバルサイン電子証明書サ 本利用約款が英語以外の言語に とし、本利用約款の条項の解釈 グローバルサイン株式会社(以下 子証明書を利用者(以下「利用 です。電子証明書の利用をご希言 読みください。電子証明書を甲	ービス利用約款 5.1 翻訳されている場合でも、本利用約款の英語版を常に原本 の唯一の基礎となるものとします。 ービス利用約款(以下「本利用約款」という)は、GMO グ 「グローバルサイン」又は「当社」という)が提供する電 皆」という)がご利用になるための利用条件を定めたもの 型の利用者は、サービスの利用に去す去、本利用約款をあ し込むことにより、利用者は本利用約款の当事者となり、
☑ 利用現約	こ同意の上、「沢へ」ボタンをクリックしてください。

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。



<u>C:CSRを用いた証明書の取得手順</u>

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。

証明書取得用パスワード入	カ
	証明書取得用パスワードを入力してください。
	*不明の場合は証明書管理者にお問い合わせください。
	No.

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。

CSR入力	-
CSR入力=	
利用規模に同意の上、「次へ」ボタン	使りりったしてくだめい。
電子署名(S/MIME)用證	明書(マネージドPKIエンドユーザー用)サービス利用的数
電子署名(S/MIME)用証 下、「本利用約款」とい しいます。)が提供する サービスの利用条件を定 ドユーザー用)サービス サービスの利用に先立ち (PS (認知業務運用規程) は、特徴の規定のない限	明書(マネージドPK エンドユーザー用)サービス利用約款(以 (ます、)は、GM)グローバ(ルサイン株式会社(以下、「当社」と 電子署名(SAUME)用証明書(マネージドPK エンドユーザー用) めたものです。電子署名(SAUME)用証明書(マネージドPK エン を利用するかた(以下、「エンドユーザー」といいます。)は、 本利用約款及びOS(認証業務運用規制)をお読みください、 は、本利用約款の一部をなし、以下(本利用約款)という場合に、 り、OS(認証業務運用規制)の内容も含まれるものとします。エ 図 回答する

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。

例)MPS2012070305	74かJohn Smith		簡易検索				
 申請日 全てのサービス ブロファイルID 部署名 	 ▼ 期間指定 ▼ ◆ ての証明書: ライセンスID メールアドレス] 例) yyyy/mm/d オーダーステー▼	 ▲ ての証 証明書管 全てのメ 	例) yyyy/mm/dd 四月書ステータス 四里者 ニールテンプレート 検索	▼ ▼		
表示件数: 10 ▼							
1 - 10 /85							
		CSV出力		LDIF出力			
		< 1 2 3 4	120183	(次// >			
各種申請 オーダーID	組織名	コモンネーム	サービス名	証明書有効期間	メールア		
申請 MPS201603	331143240 tuika	fxtestsugino	マネージド PKI Lite 部 門/法人名 用 100 pack	1年	mitsuhir		
4			マネージド				



<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「証明書ー括キャンセル・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。

キャンセル可能な証明書 矢効可能な証明書 表示件数: 10 ▼ - 10 / 15 - 10 / 15 - 24 C 選択 - 24 C 選択 - 24 C 選択 - 24 C 選択 - 25 C 単一 1 年 Sample@globalsign.com PAI	何)MPS2	101207030574か John	Smith		詳細検索			
表示件数: 10 ▼ -10 /15 -12 次へ > 全て選択 <u>各種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証</u> MPS20230823534381 GlobalSign A10 投GMO 1年 sample@globalsign.com PA		++	マンセル可能な	証明書 失	「効可能な証明	明書		
-10/15 <12次へ> 全て選択 <u>各種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明</u> 「MPS20230823534381 GlobalSign K.K. A10 byGMO 1年 sample@globalsign.com PAF	表示件数:	10 🗸						
タイン マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マ	- 10 /15							
Set 2 次へ> 全て選択 各種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明 □ MPS20230823534381 GlobalSign K.K. A10 ジGMO 1年 sample@globalsign.com PAF								
全て選択 名種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明 MPS20230823534381 K.K. A10 byGMO 1年 sample@globalsign.com PAF MPS20230823534381 K.K. ゴーム ゴーム ゴーム ゴーム ジーム アスホージド PKI Lite byGMO ゴーム <l< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></l<>								
全て選択 各種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明 MPS20230823534381 GlobalSign K.K. A10 ジGMOAT 1年 sample@globalsign.com PAF				< 1	2次へ>			
各種申請 オーターID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明 MPS20230823534381 GlobalSign K.K. A10 マネージド PKI Lite byGMO 1年 sample@globalsign.com PAF				< 1	2次へ>			
各種申請 オーダーID 組織名 コモンネーム サービス名 証明書有効期間 メールアドレス 証明 □ MPS20230823534381 GlobalSign K.K. A10 マネージド PKI Lite byGMO 1年 sample@globalsign.com PAF				< 1	2次へ>			
マネージド PKI Lite MPS20230823534381 K.K. A10 byGMO 1年 sample@globalsign.com PAF	全て選択			<1	2次へ>			
	全て選択各種申請	オーダール	組織名	<1 >−×<∋⊂	2 次へ > サービス名	証明書有効期間	メールアドレス	証明
	全て選択 各種申請 □	オーダーID MPS20230823534381	組織名 GlobalSign K.K.	<1 ⊐モンネーム A10	2 次へ > サービス名 マネージド PKI Lite byGMO 1,000 pack	証明書有効期間 1年	メールアドレス sample@globalsign.com	証 PAF

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。

全て選択					
各種申請	オーダーID	組織名	コモンネーム	サービス名	証明書有
•	MPS20230823534381	GlobalSign K.K.	A10	マネージド PKI Lite byGMO 1,000 pack	1年
	MPS20230823534380	GlobalSign K.K.	A9	マネージド PKI Lite byGMO 1,000 pack	1年
	MPS20230823534379	GlobalSign K.K.	A8	マネージド PKI Lite byGMO 1,000 pack	1年
	MPS20230823534378	GlobalSign K.K.	A7	マネージド PKI Lite byGMO 1,000 pack	1年
	MPS20230823534377	GlobalSign K.K.	A6	マネージド PKI Lite byGMO 1,000 pack	1年
	MPS20230823534376	GlobalSign K.K.	A5	マネージド PKI Lite byGMO 1,000 pack	1年

5.選択した証明書を確認し、完了をクリックします。

No	オーダーロ	組織名	コモンネーム	サービ ス名	証明書有効期間	メールアドレス	証明書管理者	ライセンスル	プロファイルD
1	MPS20230823534381	GlobalSign K.K.	A10	マネー ジド PKI Lite byGMO 1,000 pack	1 年	sample@globalsign.com	PAR60328_masanobu	ML202211248722	MP202308226094
2	MPS20230823534380	GlobalSign K.K.	A9	マネー ジド PKI Lite byGMO 1,000 pack	1 年	sample@globalsign.com	PAR60328_masanobu	ML202211248722	MP202308226094

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。)

GSパネル管理と経理	 サーバ証明書 (EDI・ヤフー提携証明書を含む) SSLマネー 	ジドサービス 🗉 🤅	その他証明書 コードサイニング・PDF)	マネージドPKI
マネージドPKI 証明書 ● 証明書管理	ライセンス一覧画面 検索条件を入力し、検索ボタンを押してください。	。検索ボタンのみを押した場	合は、全ての申請履歴が表示	示されます。
ライセンス ● ライセンス追加購入 ● ライセンス購入履歴	例) ML201207030574かPAR12345_acme ② 表示件数: 10 ~	詳細検索	検索	

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。

ライ た 検索条	マンス一覧画 件を入力し、検索ボタ	国 タンを押してください。検索ボタンの	Dみを押した場合は、	全ての申請履	歴が表示され	まず 。				
0 表示件 1-7/7	L 201 207030574329 裁: 10 〜	AART2345_lucine	< 1 >	索						
編集	ライセンスID	コーポレートID(契約者ユーザID)	申請日	サービス名	証明書年数	ライセンスステータス	ライセンス有効開始日	ライセンス有効終了日	ライセンス数合計	ライセンス未使用数
編集	ML202106082330	PAR	2021年06月08日 18:48(GMT+09:00)	マネージド PKI Lite byGMO 10 pack	1年	ライセンス発行	2021年06月08日 18:49(GMT+09:00)	2022年06月09日 18:49(GMT+09:00)	11	11

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。 <u>6-2. ライセンスの追加購入について</u>

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。

ービス内容の選択		
イセンス追加購入		
বর	トージドPKI Lite byGMG	
	マネージドPKI Lite byGMO	
	 アクセス認証のご利用用途 	このままマネージドPKI Lite byGMO 個人名用をお申込みください。
	■S/MIMEのご利用用途	証明書CNに、個人名、または、自社および関連会社に属する個人のメールアドレスのみが登録可能です。 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の登録をご希望の場合は、

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。							
ライセンス内容選択 ≫ 支払方法入力 サービス内容の選択 - マネー ※S/MIMEのご利用用途では、証明書CNは個人名 法人名、または、自社および関連会社に属する音 「法人名用ライセンス」をお申し込みください。	▶ 確認 -ジドPKI Lite byGMO 1 pack A、または、自社および関連会社に属する個人のメールアドレスのみが登録可能です。 門用メールアドレスの登録をご希望の場合、本ライセンスでは証明書発行ができかねますため、						
証明書年数※必須	 ●1年 ¥0 ○2年 ¥0 ○4年 ¥0 ○短期 ¥0 						
キャンペーンコード							
クーボンコード							
金額(税込)	¥ 0						
技術担当者情報入力 契約者と別の方の場合は、ごちらから入力をお 技術担当者とは、証明書の申請を行う申請手続き 契約者組織と異なる組織に属する方をご登録いた	<mark>いします。</mark> #担当者を意味します。 -だくこともできます。 前へ 次へ 0						

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。

1. サービス選択	2. 完了
ライセンス内容選択 🧊 支払	方法入力 >>> 確認
方法情報	
支払方法	 ○ 銀行振込(後払い) ※翌月未日までに代金をお振り込みください。
	○ クレジットカード
その他情報	O クレジットカード

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。

証明書○ 証明書管理	ライt 検索条	2ンス一覧画 件を入力し、検索ボタ	面 タンを押してください。検索ボタンの	のみを押した場合は、	全ての申請履	歴が
 ライセンス ライセンス追加購入 ライセンス購入履歴 プロファイル プロファイル設定 プロファイル追加申請 プロファイルー覧 メールドメイン一覧 	例) M 0 表示件 1 - 7 /7	L201207030574かり 数: 10 〜	PAR12345_acme	¥細検索 枝 < 1 >	索	
ポータル ◎ ポータル管理	編集	ライセンスID	コーポレートID(契約者ユーザID)	申請日	サービス名	100
iOS 証明書 ◎ 構成プロファイル設定 メール	編集	ML202106082330	PAR44158_testdayo3	2021年06月08日 18:48(GMT+09:00)	マネージド PKI Lite byGMO 10 pack	1
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。

攅	操作履歷							
	アクション内容	アクション日	結果					
	ライセンス・オーダー申請(リクエスト無し)	2021年06月08日 18:48:10(GMT+09:00)	成功					
	ライセンス・オーダー発行	2021年06月08日 18:49:09(GMT+09:00)	成功					
		確認 キャンセル申し込み メール送信一覧						

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。

ライセンス編集	
銀行名	
支店名	
口座種別	
口座番号	
口座名義人	
ライセンスID	ML202106152332
サービス	マネージドPKI Lite byGMO 10 pack
証明書年数	1年
ライセンス数合計	11
ライセンス未使用数	11
ライセンス ステータス	ライセンス発行
ライセンスタイプ	通常
申請日	2021年06月15日 11:08(GMT+09:00)
発注日	2021年06月15日 11:09(GMT+09:00)
ライセンス有効開始日	2021年06月15日 11:09(GMT+09:00)

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。 ライセンス編集

アクション内容	アクション日	結果
ライセンス・オーダー申請(リクエスト無し)	2021年06月15日 11:08:42(GMT+09:00)	成功
ライヤンス・オーダー発行	2021年06月15日 11:09:09(GMT+09:00)	成功

7. プロファイルについて

<u>7-1. プロファイルの追加登録について</u>

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。

GSパネル管理と経理	サーバ証明書 (EDI・ヤフー提携証明書を含	む) 🛛 SSLマネーシ	ドサービス 🔳	その他証明書 (コードサイニング・PDF)	マネージド	PKI 📼
<u>マネージドPKI</u>	ライセンスお	申し込み				
証明書 ● 証明書管理 ライセンス ● ライセンス追加購入	マネージドPKI					
 ● ライセンス購入履歴 プロファイル ● プロファイル設定 ● プロファイル追加申請 ● プロファイル追加申請 ● プロファイルに 	ライセンス一覧	フロファイル設定	マシンク	メールテンプレート管理		

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。

れる証明書に記載される情報ですので、お	間違いのないようにお願いします。
a間CA証明書	 S/MIME BR(Legacy)対応用中間CA証明書 アクセス認証用中間CA証明書
aseDN	
圓/地域 = C≫必须	[日本 - JP ▼]
7道府県 = S 半角英数、または全角(UTF-8)128文字以内	Tokyo 例)Tokyo
5 区町村 = L 半角茣酘、または全角(UTF-8)128文字以内	Shibuya #0. Shibuya
目織名 = O ※必須 半角英数、または金角(UTF-8)64文字以内	GlobalSign K.K.
「著名 = OU※BaseDnをチェックする場合は必 I 半角英数、または全角(UTF-8)64文字以内	(ii) Marketing Descion
名アルゴリズム	 sha256RSA RSASSA-PSS (sha256) こちらを選択した場合は有効期限1年の証明書の申込以外は行えません。
rganizationIdentifier(2.5.4.97) MIMEを利用する場合は 消となります。	○ VAT ● GOV ※法人番号が指定されている申請組織の場合はVATをご選択ください □ □ 本 - JP

※「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。

ታ			_
。追加登録は随時可能でご (ールドメインを登録、認識 ご覧ください。	ざいます。S/MIMEを利 Eすることで、メールア	用しない場合は登録不 ドレスを証明書に登録	、要ですが、管理者 することが可能と
[
前へ	, w	2	
	 追加登録は随時可能でご ・ールドメインを登録、認識 ご覧ください。 前へ 	・ 追加登録は随時可能でございます。S/MIMEを利/ ニールドメインを登録、認証することで、メールア にご覧ください。	・追加登録は随時可能でございます。S/MIMEを利用しない場合は登録不 ールドメインを登録、認証することで、メールアドレスを証明書に登録 ご覧ください。

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。

プロファイルお申し込み	
1. サービス選択 2. 完了	
DN搭載入力 »> メールドメイン搭載入力 >> メールドメイン	認証方法選択 🤉 確認
メール認証	
メール認証では、ドメイン所有者のみが受信可能と想定される。 承認作業を行っていただきます。	メールアドレスへ弊社から承認メールを送信し、ドメイン所有者に
WHOISのメールアドレス	
 梁認メールアドレスは、下記選択肢の中から任意のものをご選択(WHOIS音録)情報の修正が必要な場合) WHOIS音録)情報の修正が必要な場合) WHOIS情報の変更につきましては、お客様が登録されたドメイ admini@globalsign.com administrator@globalsign.com postmaster@globalsign.com webmaster@globalsign.com webmaster@globalsign.com WHOISアドレスを記入してください。 WHOISアドレスを記入してください。 <td>Rください。 ン事業者へお問い合わせください。</td>	Rください。 ン事業者へお問い合わせください。
ページ認証	
ページ認証では、グローバルサインから提供されたドメイン審	音コードをドメインの特定のディレクトリのテキストファイル内に

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。

DN情報入力 » メールドメイン情報	入力 » メールドメイン認証方法選択 » 確認						
登録情報の確認							
中間CA証明書	S/MIME BR(Legacy)対応用中間CA証明書						
BaseDN							
組織名 = 0	GlobalSign K.K.						
部署名 = OU							
都道府県 = S	Токуо						
市区町村 = L	Shibuya						
国/地域 = C	日本 - JP						
organizationIdentifier(2.5.4.97)	GOVJP						
メールドメイン情報	globalsign.com						

6.以上でプロファイルの追加申請は完了です。

プロファイルお申し	<u>ኦ</u> ዎ	
1.サービス選択	2.完了	
申し込み完了		3
7-#fin		
ว้อวราเมอ		
申請書を印刷する	a a	

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「プロファイルー覧」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。

プロファイル更新お明	起み	
1.サービス選択	2.常了	
録情報を確認 嚪CA証明書	S/MIME BR(Legacy)对応用中間(CA証明書	
aseDN	無し	
1織名=0	GlobalSign K.K.	
1織名 = O 「曙名 = OU	GlobalSign K.K.	
11歳名 = 0 1階名 = 0U 50箇府県 = S	GlobalSign K.K.	
1職名 = O 「隋名 = OU 」 」 」 」 」 」 」 」 日 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇	GlobalSign K.K.	
1職名 = O 「曜名 = OU 防迫府県 = S 河区町村 = L 1/地域 = C	GlobalSign K.K.	

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。

プロファイル更新お	申込み		
1.9-E38R	2.第了		_
7			
		元」 一覧へ	

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。

GSパネル管理と経理	サーバ証明書 (EDI・ヤフー提携証明書を含	iむ) 🖻 SSLマネージ	ジドサービス 🖻	その他証明書 (コードサイニング・PDF)	マネージドPKI	
マネージドPKI	ライセンスお	申し込み				
 証明書管理 						
 ライセンス ライセンス追加購入 ライセンス購入履歴 	マネーン PPK					
ブロファイル プロファイル設定			23			
 ● フロファイル一覧 ● メールドメイン一覧 	ライセンス一覧	プロファイル設定	ポータル管理	メールテンプレート管理		- 1

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。

プロファイルID			
自織名	GlobalSign K.K.2		
部署名			
URL	https://stg-gcc.globalsign.com/cr/public/certificate/order.do? p=e3b64b611cd90c8f920b4a3ec23e2312c184c6c3 https://stg-gcc.globalsign.com/cr/public/certificate/order.do? p=c2705e4de0e9a09f56b8bc770c9b4df9dd1517fa		
URL(PKCS12オプション)			
ユーザー権限	設定		
メールドメイン情報	設定		
中間CA	S/MIME BR(Legacy)対応用中間CA証明書 アクセス認証用中間CA証明書		
著名アルゴリズム	 ・ ・ ・		
Encrypting File System	● 無し〇 有 り		
MS SmartCard Logon	●無し○有り		
自動更新	 ● 無し ○ 有り ○ クイック 		
秘密鍵エクスポート不可 nternet Explorer のみに限定されます。	〇年し〇有り		
プロファイル更新メール	○送信しない◉送信する		
API IPアドレス API I型用目 のみに意定されます。 用) **** 例)	E		

<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。

			>
全般	詳細証明のパ	え	
表示(S):	<すべて>	~	
フィール	ド キーのパラメーター	値 05 00	^
圖機関 圖証明 圖其本	情報アクセス 書ポリシー	[1]Authority Info Acce [1]Certificate Policy:Po Subject Type=End Enti	
の CRL 同サプシ	配布ポイント ジェクト代替名	[1]CRL Distribution Poi RFC822 Name=masan	
 	キー使用法 キー識別子 バェクト キー識別子	クライアント認証 (1.3.6.1 KeyID=d2f86d1c323d a751e689f421a8c94f5	~
クライアン	小認証 (1.3.6.1.5.	5.7.3.2)	
10000	11 - 10 - 14	C C 7 2 4)	
暗号化了	ファイル システム (1.3	3.6.1.4.1.311.10.3.4)	
暗号化力	ックパンティンファ ファイル システム (1.3	3.6.1.4.1.311.10.3.4)	
暗号化了	ッパンテレンテム (1.3	3.6.1.4.1.311.10.3.4)	
曜号化2	ッパンテレンテム (1.3	3.6.1.4.1.311.10.3.4) プロパティの編集(E)	ファイルにコピー(C)

「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。

全般 詳細 証明のパス 表示(S): <すべて> フィールド 値 國基本制限 Subject Type=End Enti GCRL 配布ポイント [1]CRL Distribution Poi サナジェクト代替名 REC822 Name=konats 「拡張キー使用法 クライアント認証(1.3.6.1) ③サブシェクト ギー取別子 1a7c413ef769t239fca1 ③機関キー取別子 KeyID=d2f86d1c323d デー使用法 Digital Signature, Key	全般 詳細 証明のパス 表示(S): <すべて> フィールド 値 画 基本制限 Subject Type=End Enti 面 CRL 配布ポイント [1]CRL Distribution Poi 面 サブジロクト代替を REC822 Name=konats 面 地グジェクト代替を REC822 Name=konats 面 地グジェクト代替を REC822 Name=konats 面 地グジェクト代替を REC822 Name=konats 面 地グラジェクト キー取別子 1a7c413ef769f239fca1 面 機関キー取別子 KeyID=d2f86d1c323d 面 キー使用法 Digital Signature, Key 面 印印 98804a4867f5e2fd104
表示(S): <すべて> ~ フィールド 値 画 基本制限 Subject Type=End Enti 回 CRL 配布ポイント [1]CRL Distribution Poi 回 サブジロクト代替A BFC822 Name=konats 回 拡張キー使用法 クライアント認証 (1.3.6.1 回 サブシロクトキー取別子 1a7c413ef769f239fca1 回 機関キー取別子 KeyID=d2f86d1c323d 副 キー使用法 Digital Signature, Key	表示(S): <すべて> フィールド 値 画基本制限 Subject Type=End Enti @ CRL 配布ポイント [1]CRL Distribution Poi @ サブジェクト代替名 RFC822 Name=konats <u>気 拡張キー使用法 クライアント認証 (13.6.1</u> @ サブシェクト キー識別子 1a7c413ef769f239fca1 @ 機関キー識別子 KeyID=d2f86d1c323d ■ キー使用法 Digital Signature, Key 拇印 98804a4867f5e2fd104
フィールド 値 ^ 園 基本制限 Subject Type=End Enti ^ 窗 CRL 配布ポイント [1]CRL Distribution Poi ^ 窗 サブジェクト代替名 REC822 Name=konats ^ ፴ 切フジェクト キー蹴別子 1a7c413ef769f239fca1 ^ 窗 機関キー識別子 KeyID=d2f86d1c323d _ 副 キー使用法 Digital Signature, Key ^	フィールド 値 ^ 回 基本制限 Subject Type=End Enti 窗 CRL 配布ポイント [1]CRL Distribution Poi 窗 Tアジロクト代替名 REC822 Name=konats 図 サブジロクト代替名 REC822 Name=konats 図 地域県キー使用法 クライアント認証(1.3.6.1) 図 サブシロクト ギー販別子 KeyID=d2f86d1c323d 副 キー使用法 Digital Signature, Key 図 拇印 98804a4867f5e2fd104
回り(アイアンド)を合く 内トのアント認証(1.3.61) 回切フジェクトキー識別子 1a7c413ef769f239fca1 回機関キー識別子 KeyID=d2f86d1c323d 記キー使用法 Digital Signature, Key	回り/2/12/11 日日/2/13/01/E=000015 回 拡張キー使用法 クライアント認証(1.3.6.1) ④ サブシェクト キー販別子 1a7c413ef769f239fca1 ◎ 機関キー販別子 KeyID=d2f86d1c323d ■キー使用法 Digital Signature, Key ◎ 拇印 98804a4867f5e2fd104
 ・・ 取別子 1a7c413ef769f239fca1 ・ ・ ・ ・<td>(回) サブシェクトキー取別子 1a7c413ef769f239fca1 (回) 機関キー取別子 KeyID=d2f86d1c323d (回) キー使用法 Digital Signature, Key (回) 拇印 98804a4867f5e2fd104</td>	(回) サブシェクトキー取別子 1a7c413ef769f239fca1 (回) 機関キー取別子 KeyID=d2f86d1c323d (回) キー使用法 Digital Signature, Key (回) 拇印 98804a4867f5e2fd104
□ 操印 98804a4867f5e2fd104	~

「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。

対応のプラウザです。 I Eのみ限定です。

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。

APIIPアドレス API使用時のみに限定されます。 例) ****(例) 211.11.149.249,211.11.149.250

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	0	0	※ 1
証明書発行(一括)	0	0	※ 1
証明書一覧	0	0	※2
証明書発行(管理者一括)	0	0	
管理者一括発行履歴	0	0	
承認待ち証明書一覧	0	0	※ 3
ライセンス管理			
ライセンス追加購入	0	※4	※4
ライセンス購入履歴	0	0	0
プロファイル管理			
プロファイル設定	0	0	
プロファイル追加申請	0		
プロファイル一覧	0	0	0
メールドメイン一覧	0	0	0
ポータル			
ポータル管理	0	0	
メール			
メールテンプレート管理	0	0	
メール一覧	0	0	
ポータルメール一覧	0	0	
その他			
Action log	0	0	
LDIF 管理	0	0	

※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。

ロファイルID	MP201709111334
織名(英語)	Sample Corp
署名(英語)	Evaluation Div.
RL	https://test-gcc.globalsign.com/cr/public/certificate/order.do? p=0ecd87f04394b71955e231568061381eb87abb7b
L(PKC\$12 オプション)	https://test-gcc.globalsign.com/cr/public/certificate/order.do? p=c198d010bbd1512b2cd748d0d429c72081e43d65

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。

			つーtf権限	
ユーザーID	ユーザー名	証明書申請	承認権限	証明書失效
		0	0	0
				0
		0		
		0		
		0		
		0		0
		0		
		0		0
				0

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

<u>9-1. ポータル画面のカスタマイズ</u>

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。

ポー	ータル	
	プロファイルID	MP200905210053
	組織名(英語)	GlobalSign K.K.
	部署名(英語)	sales - authenticated by LRA
	URL	https://system.globalsign.com/cr/public/certificate /order.do?p=a6f6244c92e7b 以下省略
	URL(PKCS12オプション)	https://system.globalsign.com/cr/public/certificate /order.do?p=ab5c1232098d7 以下省略

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。

ポータル管理	
ポータル	
プロファイルID	MP201702131252
組織名(英語)	GMO GS K.K.
部署名(英語)	Tech Sales
URL	https://test-gcc.globalsign.com/cr/public/certificate/order.do? p=61c7546190de8fd85fc815c6f472f7f664e07843
URL(PKC\$12 オプション)	https://test-gcc.globalsign.com/cr/public/certificate/order.do? p=705271de78d073d4e9005949199408ffb356357e
ロゴ画像	ファイルを選択 選択されていません アップロード 標準サイズ 176×37 pixel 最大容量 2MB 画像種別 jpg,gif,png
フッター画像	ファイルを選択 選択されていません アップロード 標準サイズ 950×7 pixel 最大容量 2MB 画像種別 jpg,gif,png
タイトル※必須	
登録済みメールドメインのみ許可	
お客様独自の利用規約をご入力ください。	·
電子署名(S/MIME)用証明書(マネー 「本利用約款」といいます。)は、GM す。)が提供する電子署名(S/MIME) の利用条件を定めたものです。電子署 用)サービスを利用するかた(以下、 に先立ち、本利用約款の一部をなし、以 り、CPS(認証業務運用規程)の内容 (S/MIME)用証明書(マネージドPKI ことにより本利用約款の当事者となり 第25条を除き、CPS(認証業務運用規 CPS(認証業務運用規程)の内容が優多	ジドPKIエンドユーザー用)サービス利用約款 ジドPKIエンドユーザー用)サービス利用約款(以下、 0グローバルサイン株式会社(以下、「当社」といいま 用証明書(マネージドPKIエンドユーザー用)サービス 名(S/MIME)用証明書(マネージドPKIエンドユーザー 「エンドユーザー」といいます。)は、サービスの利用 第落運用規程)をお読みください。CPS(認証業務運用規 下「本利用約款」という場合には、特段の規定のない限 ら含まれるものとします。エンドユーザーは、電子署名 エンドユーザー用)サービスを申し込み、又は利用する 、本利用約款の条項に拘束されるものとします。なお、 規程)の内容と本利用約款の内容が異なるとぎは、
第1章 定義	
	前へ次へ

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・テンプレート編集				
メール内容を変更するには「編集」ボタンをクリックし メールの件名/宛先/メッセージ本文を編集することが	てください。 できます。			
有効/無効設定:「有効」を選択するとメールが送信さ 送信が不要な場合には、「無効」を選択してください。	れます。			
日本語 - JA (既定值)				
オランダ語 - NL				
アイスランド語-IS				
サモア語 - SM				
英語 - EN				
アイルランド語 - GA				
テンプレート言語を追加				
選択されたテンプレート言語:英語 - EN			1	
メールタイプ (送信タイミング・種類)	送信	コンテンツ		
証明書(管理者一括) 有効期限30日前	有効	編集		
キャンセル完了	有効	編集		
証明書取得(インバイト)	有効	編集		

※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・	エンコーディング	●時効 ○無対 UTF-8 ▼	メッセージを市に	展明
			オーダーID パートナーI プロファイバ	0
ッセージ	の発先		オーダー取	
From	no reply@globalsign.com		商品名	
Reply- To	L		之	ちューザロ
To	[SS{CertAdminUser!Enail}		2	昌-名削(英語)
Ce		2 建明青草理:	自-414名(948冊) 首-ミドル名	
Bec		延期 責管理:	西-名前	
ッセージ	孝文	証明書提得 証明書管理:	证明實管理者-相違名	
件名	証明層(管理者一括)期間30日前のお知らせ/\$\${OrderiD}		超期實管理	8-組織名(カナ)
	- 征明書 (管理者一話) 期限30日	前のお知らせ	証明書管理:	哲-印雾名 哲-役職
	このメールはシステムから	自動的に送信されています	紅羽東管理	台-電話番号
		き、誠にありがとうございます。	延利幣給現:	哲-FAX衛号 F-Xールアドレ
メッセージ	以下内容で発行手配いただきまし7 第日程となりました。有効期限が 再度、新規と同じく発行処理をお問	た電子証明書は、有効期限まで残り 初れますと利用できなくなりますので 働いいたします。		
	◆更新対象のオーダー情報			
	[一括発行オーダー物] \$\$(0) (GSパネルの管理者一括発行履歴より	der1D} J詳細が確認可能です。		
	in the second second			

・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「<u>no_reply@globalsign.com</u>」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。

メッセージ	D宛先
From	no reply@globalsign.com
Reply- To	sample@gmail.com

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。

テストメール送信先	info@globalsign.co.jp	テストメール送信
	前へ〕次へ	

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 有効期限〇日後、〇日前

証明書 有効期限〇日後、〇日前

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。

<u>9-3.メールドメイン情報</u>

【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。

イセンス	プロファイル設定	
 ライセンス追加購入 ライセンス購入履歴 	プロファイルID	MP202308226094
077414	組織名	GlobalSign K.K.
プロファイル設定 フロファイル追加申請	部署名	
プロファイル一覧 メールドメイン一覧	URL	
ペータル → ポータル管理	URL(PKCS12 オプション)	The same areas in the second s
DS 証明書	ユーザー権限	設定
●構成プロファイル設定	メールドメイン情報	設定
 メールテンプレート管理 メール一覧 	中間CA	● SIMIME BR(Legacy)対応用中間CA証明書 ○ アクセス認証用中間CA証明書
 ホータルメール一覧 の値 アクションログ マクジョンログ 	署名アルゴリズム	 sha256RSA RSASSA-PSS (sha256) ごちらを進択した場合は有効期間1年の証明書の申込以外は行えません。
LDIF 昌庄	Encrypting File System	●無し〇有り
ePKI Administrator Guide	MS SmartCard Logon	 ●無し〇有り
	自動更新	 ● 無し ○ 有り ○ クイック
	移密鍵エクスポート不可 Internet Explorer のみに確定されます。	●無し○有り
	API IPアドレス API 使用時のみに描述されます。 例)****例) 211.11.149.249.211.11.149.250	(*.*.*.

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。

マネージドPKI	メールドメイン情報	
証明書 ◎ 証明書管理		
 ライセンス違加購入 ● ライセンス違加購入 ● ライセンス満入履歴 プロファイル ● プロファイル段定 ● プロファイル追加申請 ● プロファイル追加申請 ● ブロファイル・見 ● メールドメイン一見 ● ニークド 	メールドメイン情報 SMIMEを利用する場合は登録必須です。追加登録は随時可能でございます。SMIMEを利 ー活申請で証明書を発行する場合は、メールドメインを登録、認証することで、メールア なります。詳しくは管理者マニュアルをご覧ください。 メールドメイン情報入力 メールドメイン情報 SMMMEを利用する場合は必須となりま SMMMEを利用する場合は必須となりま	用しない場合は登録不要ですが、管理者 ドレスを証明書に登録することが可能と
 ・ ボータル管理 ・ 構成プロファイル設定 ×ール ・ メールテンブレート管理 ・ メールー复 ・ ボータルメール一覧 	 ● SIMIMEを利用します。メールドメインの有効期間は397日となり、 が必要であることを了承します。 ○ SIMIMEは利用しませんが、管理者一括申請での証明書発行で、メールドメインを登録します。 登録済みメールドメイン 	総統利用のためにはドメインの再認証 ールアドレスを証明書に登録するため、
その他	メールドメイン(大文字小文字の区別はありません)	ステータス
 アクションログ LDIF管理 	globalsign.com	承認済み
リソース ● ePKI Administrator Guide	2 前へ 2	en e

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。

メールドメイン情報		
S/MIMEを利用する場合は登録必須です 一括申請で証明書を発行する場合は なります。詳しくは管理者マニュアル	7、追加登録は協時可能でございます。SMIMEを利用した メールドメインを登録、認証することで、メールアドレフ をご覧ください。	はい場合は登録不要ですが、管理者 えを証明書に登録することが可能と
メールドメイン情報入力		
メールドメイン情報 SMMMEを利用する場合は必須となりま す。	sample.com	
 SIMIMEを利用 が必要であること: SIMIMEは利用 メールドメインを! 	します。メールドメインの有効期間は397日となり、総統 を了承します。 しませんが、管理者一括申請での証明書発行で、メールフ 登録します。	利用のためにはドメインの専惑証 ?ドレスを証明書に登録するため、
 SIMIMEを利用 が必要であること: SIMIMEは利用 メールドメインを! 登録済みメールドメイン メールドメイン 	します。メールドメインの有効期間は397日となり、総統 を了承します。 しませんが、管理者一括申請での証明書発行で、メールフ 登録します。 > (大文字小文字の区別はありません)	利用のためにはドメインの専惑証 アドレスを証明書に登録するため。 ステータス

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。

プロファイルお申し込み
1.サービス選択 2.完了
DN情報入力 >>> メールドメイン情報入力 >>> メールドメイン認証方法選択 >>> 確認
メール認証
メール認証では、ドメイン所有者のみが受信可能と想定されるメールアドレスへ弊社から承認メールを送信し、ドメイン所有者に 承認作業を行っていただきます。
WHOISのメールアドレス
 承認メールアドレスは、下記選択該の中から任意のものをご選択ください。 [WHOIS登録情報の修正が必要な場合】 WHOIS情報の変更につきましては、お客様が登録されたドメイン享美者へお問い合わせください。 admin@globalsign.com administrator@globalsign.com postmaster@globalsign.com webmaster@globalsign.com WHOISアドレスを記入してください。
ページ認証
ページ認証では、グローバルサインから提供されたドメイン審査コードをドメインの特定のディレクトリのテキストファイル内に

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。

中間CA証明書 S/MIMEを利用します。メールドメイン 利用のためにはドメインの再認証が必要	D有効期間は397日となり、継続 であることを了承します。

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。

GSバネル管理と経理	 サーバ証料書 (EDI - ヤフー度換証明書を含) 	n) 🗉 SSLマネージドサービス	その他証明書 (コードサイニング・PDF	, 🗉 🔽 र*-	ジドPKI 🖃		
マネージドPKI 単単書	メールドメイン核	续					
0 証明書管理	PDZMIN		全ステータス	~			
ライセンス		2.2		検索			
 ライセンス追加購入 ライセンス購入職歴 	表示件数 10 ~						
プロファイル ● プロファイル設定 ● プロファイル設加申請 ● プロファイル	1 - 10 / 14	~	12次へ>				
ポータル © ボータル管理	プロファイルD	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
ios aniz	MP202308256191	gssup.work	20230921001758	審査待ち			
● 構成プロファイル設定	MP202308256191	acccestes.com	20230825001704	承認済み			
<u>и-х</u>	MP202308236119	enablesmime.com	20230825001705	承認済み		2023-08-25 09:00:00.0	2024-09-25 09:00:00.0

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	プロファイルロ	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		des automation of		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。

プロファイルお申し	込み
1.サービス選択	2.元7
DN情報入力 » メールド	メイン情報入力 » メールドメイン認証方法選択 » 確認
メール認証	
メール認証では、ドメイ: 承認作業を行っていただ?	ッ所有者のみが受信可能と想定されるメールアドレスへ弊社から承認メールを送信し、ドメイン所有者に きます。
WHOISのメールアドレ	2
 季認メールアドレスは、 (WHOIS遭録)首級の修正 WHOIS遭報の変更(こつき) admin@globalsign.cor administrator@globalsig postmaster@globalsig webmaster@globalsig WHOISアドレスを記。) 	F記選択版の中から任意のものをご選択ください。 が必要な場合】 ましては、お客様が登録されたドメイン事業者へお問い合わせください。 1 gn.com n.com 1.com 1.com
ページ認証	
ページ認証では、グロー	いしサインから提供されたドメイン審査コードをドメインの特定のディレクトリのテキストファイル内に

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。

プロファイルロ	
ePKI Domain ID	and a second sec
メールドメイン	enablesmime.com
Approval Type	DNSIZE

5.以上でメールドメイン情報の更新は完了です。

以下のメールドメイン情報を更新します。		
	メールドメイン検索	1

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「メールドメインー覧」から確認する事ができます。

編集	更新	プロファイルロ	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					申込済み		2023年08月25日 09:00(GMT+09:00)	2024年09月25日 09:00(GMT+09:00)
編集		and the second second			承認済み			
編集				angle on	承認済み	設定		

<u>9-5. LDIF 管理</u>

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。

テンプレート	メッセージを元に戻す	オーダーID DN-コモンネーム DN-組織名(英語) DN-部署名 DN-部署名
NY9-	#LDIF made by GlobalSign GOC	DN-国コート DN-都道府県 DN-市区町村 DN-メールアドレス 証明書-有効期限開始日 証明書-有効期限終了日
メッセー ラ	Hn: CN=\$\${Dn!CommonName},CN=Users,DC=edit here changetype: modify replace: userCertificate userCertificate:: \$\${Certificate!Pem} -	証明書-シリアルNo 証明書-PEM 証明書-PKCS7 メモ iFilterインストール用UR iFilter証明書再取得用UR iFilter更新手続き用URL
フッター		<u>a</u>

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。

CSV出力	LDIF出力

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。

● パスワードリトライの上限回数 10を超過しました E明書取得用パスワード入力 正明書取得用パスワードを入力してください。 ビックアップパスワードをお忘れの方へ。 正明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	アスワードリトライの上限回数 10を超過しました E明書取得用パスワード入力 証明書取得用パスワードを入力してください。 ビックアップパスワードをお忘れの方へ。 ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。		
正明書取得用パスワード入力 証明書取得用パスワードを入力してください。 ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	正明書取得用パスワード入力 証明書取得用パスワードを入力してください。 ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	● バスワードリトライの上限回数 10を超過しました	
証明書取得用バスワードを入力してください。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	証明書取得用バスワードを入力してください。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	正明書取得用パスワード入力	
ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	証明書取得用パスワードを入力してください。	
		ビックアップパスワードをお忘れの方へ。 証明書の申込を行った管理者に連絡して、ビックアップパスワードの設定を確認してください。 ご自身でパスワードを設定された場合や、よくわからなくなった場合はサポートチームへ連絡ください。	

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。

アクション内容	アクション日	結果	ユーザロ
証明書申請(リクエスト無し)	2023年06月21日 15:23:32(GMT+09:00)	成功	
パスワードロック	2023年06月21日 15:24:29(GMT+09:00)	50 17	

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。

サーバ証明書 (EDI-ヤフー提携証明書を含む)	その他証明書 (コードサイニング・PDF)		マネージドPKI
		-	

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。

証明書一覧画面	1 3 470 A		1.1.1.1.1.1.1
検索条件を入力し、検索ボタンを押してください。	検索ボタンのみを押した場	合は、全ての申	青履歴が表示されます。
例)MPS201207030574均(John Smith 0	詳細検索	検索	
表示件数: 10 🗸			

4. 該当証明書の「申請」ボタンをクリックします。

各種申請	オーダーID	組織名	コモンネーム	サービス名	証明書有实
申請	MPS201007141864	GlobalSign K.K.	Yamada Taro	マネージド PKI Lite 1.000 pack	1年

5.「証明書取得用パスワード」欄にて確認可能です。

メモ欄		
証明書取得用バスワード	example 1234	
Encrypting File System	無し	
MS SmartCard Logon	無し	
ユーザープリンシバル名		



〒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

(C) GMO GlobalSign K.K. All Rights Reserved.