プライベート認証局 Gléas

安全・確実な電子証明書配布

クラウドサービス
リモートアクセス
Wi-Fi
IoT
多要素認証

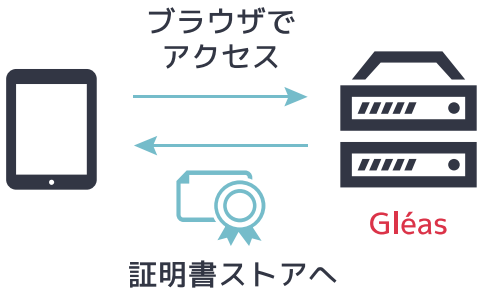
株式会社JCCH・セキュリティ・ソリューション・システムズ

証明書発行だけでは十分ではない
安全・確実に配布してこそ証明書認証の価値がある

安全・確実な電子証明書配布

プライベート認証局 Gléas（グレアス）は、電子証明書の発行・管理のための専用アプライアンスです。証明書を安全に、確実に、管理下のデバイスだけに配布できるよう、Gléas は設計されています。

Gléas からデバイスへ証明書を配布する方法で最も採用されているのが、ブラウザを使う方法です。デバイスのブラウザで Gléas のユーザ用ウェブ画面にアクセスし、OS の証明書ストアに証明書を直接インポートします。



この方法だと証明書がファイルとしてデバイスに残らず、エクスポートもできない設定でインポートされるため、他のデバイスに証明書をコピーされることはありません。

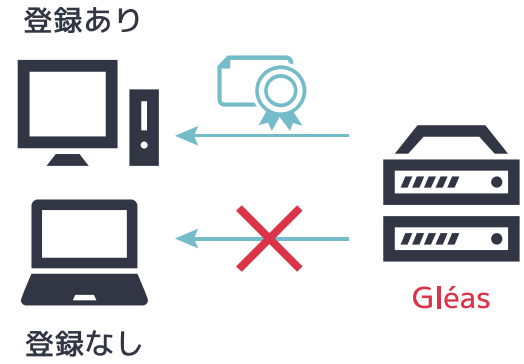
複数デバイスへのインポート制限

Gléas には、個々の電子証明書の証明書ストアへのインポートを 1 回に制限する「インポートワンス機能」があります。この機能を有効にすると、1 枚の証明書が複数のデバイスへインポートされるのを防ぐことができます。

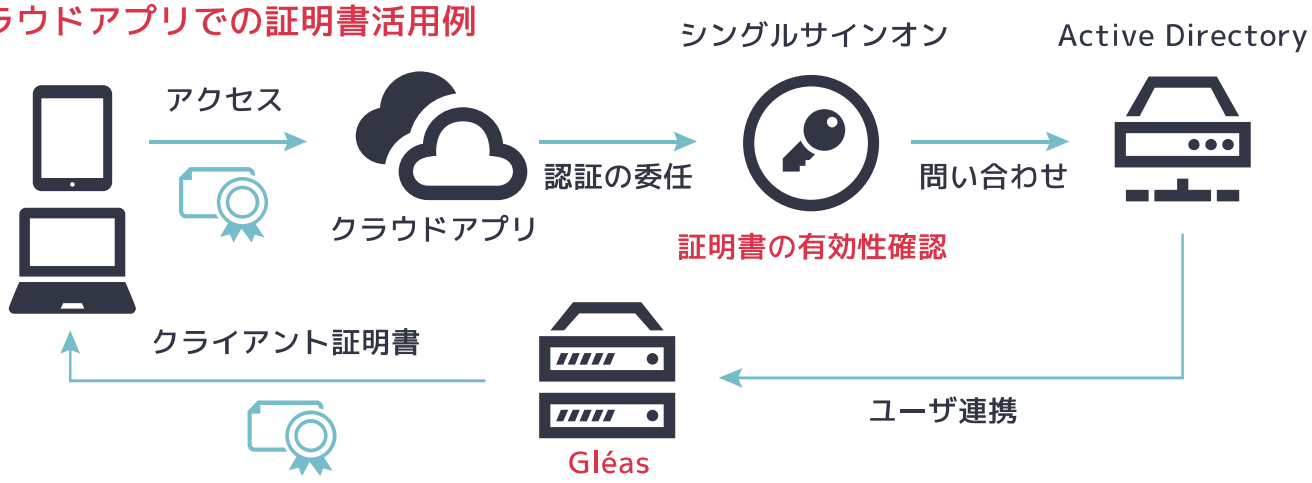
証明書インポート可能なデバイスの限定

Gléas は、証明書を取得できるデバイスの端末識別情報をあらかじめ登録しておくことで、登録外のデバイスへの証明書インポートを防ぐことができます。

これらの機能の組み合わせによって、Gléas は管理側が意図するデバイスへのみ、証明書を配布できます。

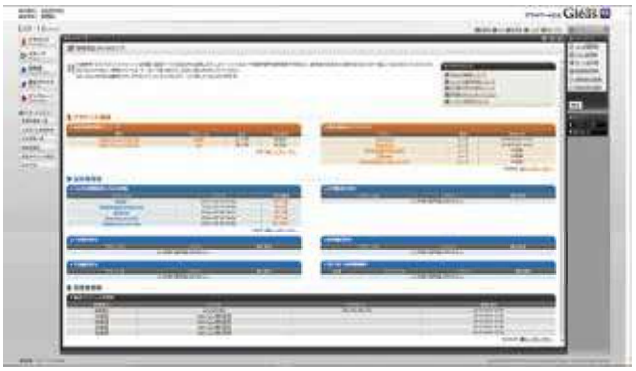


クラウドアプリでの証明書活用例



運用担当の経験によらない
適切な証明書管理を実現

柔軟で適切な証明書管理



Gléas は、証明書の要求・発行・失効・有効期限切れまでのライフサイクルを管理します。

証明書の状態(有効 / 失効 / 期限切れ / 停止中)や日付(作成日 / 終了日 / 失効日)、インポート状況など、複数の条件で証明書を検索し、一覧表示・一括操作できます。

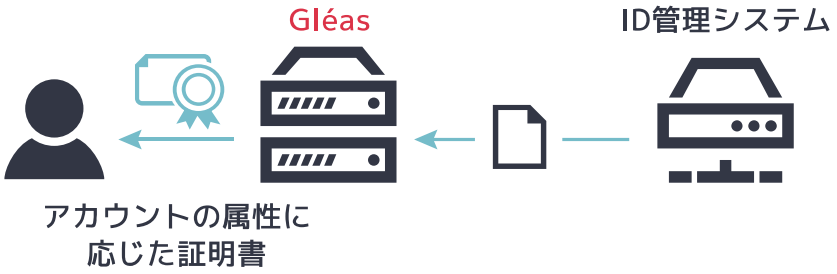
証明書は、アカウントが所属するグループに適用されたテンプレートによって属性や有効期限が設定されます。アカウント / グループ / テンプレートは任意の紐づけが可能で、上限はありません。

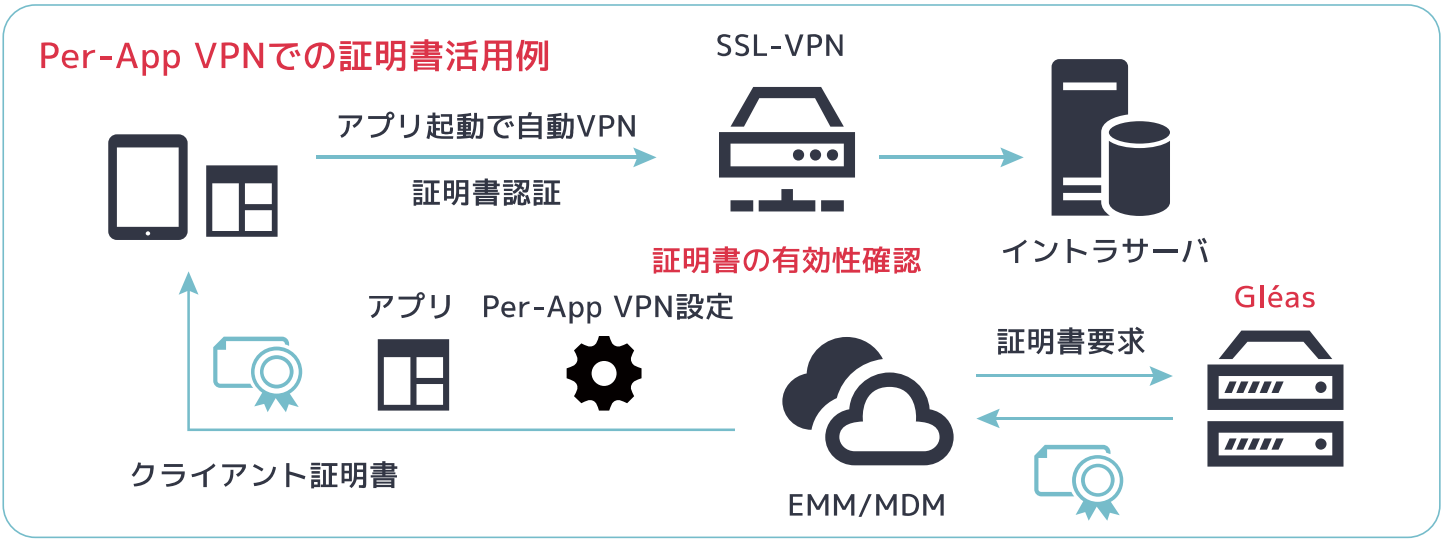
これらは適切な運用ができるように、導入時のコンサルティングに合わせて設定されます。また管理者による設定変更・追加も可能です。

外部システム連携

Gléas は ID 管理システムなどの外部システムと連携ができます。外部システムからの送信データによって Gléas にアカウントが作成され、属性情報に応じてアカウントはグループに所属します。

グループに適用されるテンプレートによって、証明書用途や有効期限など異なるポリシーを持つ電子証明書を、アカウントに対して発行できます。
ID 管理システムにより削除されたアカウントに発行された証明書を失効させることもできます。





機能一覧

○：標準装備　△：オプション

エディション	スターター	スタンダード
発行できる証明書		
ライセンス数	200	100～50,000
クライアント証明書	○	○
コンピュータ証明書	○	○
サーバ証明書	○※1	○
下位証局証明書		○
証明書用途		
ウェブサイト認証	○	○
SSL-VPN認証	○	○
IPsec認証		○
無線LAN認証 (EAP-TLS)	○	○
スマートカードログオン		○
ドメインコントローラ		○
Kerberos認証		○
ファイル暗号化		○
メール暗号化 (S/MIME)		○
電子署名		○
管理		
登録局 (RA)	○	○
発行局 (IA)	○※2	○
証明書配布 (UA)	○	○
アカウント検索	○	○
証明書検索	○	○
CSVインポート・エクスポート	○	○
外部LDAP/AD手動インポート		○
外部システム連携API		○
認証デバイス管理	○	○
モバイルデバイス管理 (iOS)		○
グループ管理		○
カスタムテンプレート作成		○
管理者数	1	2～
管理権限カスタマイズ		△
デュアルコントロール		○
証明書発行ワークフロー		○
CRL手動更新	○	○
CRLリアルタイム更新		○
マルチテナント		○
証明書発行通知メール		○
証明書配布 (UA)		
構成プロファイル (iOS)	○※2	○
構成プロファイルカスタマイズ		△
無線LANプロファイル	○※2	○
端末認証	○	○
インポートワンス	○※2	○
インポートロック	○	○
セルフサービス (内部DB)		○
セルフサービス(外部ディレクトリ連携)		△
証明書更新 (iOS)		○
証明書インポートアプリ (macOS/Android)		○
PKCS#12ファイルダウンロード	○	○
外部LDAP/AD認証連携		○
パブリックサーバ証明書利用		○
英語版UA	○	○
インターフェースカスタマイズ		△

エディション	スターター	スタンダード
システム構成		
オンプレミス		○
クラウド	○	○
クラスタリング		△
UA専用サーバ		△
LDAP証明書レポジトリ		○
LDAPレプリケーション		△
外部LDAP/ADエクスポート		△
HSMサポート ※3		△
上位認証局へのチェーン		○
SNMP		○
Syslog		○
RSA (2048bit以上)	○	○
ECC	○※2	○
SHA-2	○	○
SCEP		○
全体CRL	○	○
区分CRL		○
失効情報公開 (LDAP)		○
失効情報公開 (HTTP)	○	○
OCSPレスポンダ		○
証明書インポート対象 ※4		
Windows	○	○
iOS	○	○
iOSでの鍵ペア生成		○
macOS	○※2	○
Android	○	○
Windows 10 Mobile	○	○
Gemalto ID Primeシリーズ	○※5	○
SafeNet eTokenシリーズ	○※5	○
USBトークン/ICカードの初期化	○	○
USBトークン/ICカードでの鍵ペア生成		○

ハードウェア仕様

サーバ形状	ラックマウント型 (1Uまたは2U)
プロセッサ	x86 CPU
メモリ	8GB～
内蔵HDD	SAS HDD (RAID5)

クラウド仕様

メモリ	8GB～
ディスク	300GB以上
NIC	グローバルIPアドレス 2個以上

※1　標準でサーバ証明書用のライセンスが1付属します。
※2　一部機能が制限されます。
※3　弊社検証済み機種のみ
※4　証明書格納：PKCS#11、Microsoft CryptoAPI、PC/SC
※5　管理者画面でのインポートのみ

●記載内容は2018年11月現在のものです。仕様およびデザインは予告なく変更することがあります。最新の仕様は https://www.gleas.jp をご確認ください。

株式会社JCCH・セキュリティ・ソリューション・システムズ
050-3821-2195　www.gleas.jp　sales@jcch-sss.com
〒116-0014 東京都荒川区東日暮里5-52-2 神谷ビル7F

お問い合わせ先

2018.11