

# Gléas<sup>TM</sup> グレアス

さらに便利で使いやすく。進化したプライベート認証局。



Reliability

Flexibility

Manageability

スマート  
デバイスに  
標準対応!

- ✓ 電子証明書のライフサイクル全体の効率的なマネジメント
- ✓ マルチデバイス対応のエンドユーザ向けWEBインターフェース
- ✓ 強力なテンプレート機能による柔軟な証明書属性の管理
- ✓ 多様なアプリケーションでのクライアント証明書認証に対応
- ✓ 業種・規模を問わない企業セキュリティ・プラットフォーム

# さらに便利で使いやすく。

全く新しいプライベート認証局の誕生です。

プライベートCA <sup>グレース</sup> Gléasは、証明書の発行・配布・失効にいたるライフサイクル全体の管理を、高い柔軟性と操作性で実現するために開発された認証局アプリケーション製品です。JCCH・セキュリティ・ソリューション・システムズが、自社で開発・販売することで、お客様からのニーズに対して、迅速かつ柔軟な対応を実現しています。スマートフォンなどのマルチデバイスからのさまざまな利用シーンにおいて、Gléasを利用することにより、証明書を使った相互認証による厳格なセキュリティ・プラットフォームを安全かつ手軽にご利用いただけます。



→ 大規模ユーザへの対応を可能にする、さらに進化した管理機能

## Manageability

- 証明書・アカウント・認証デバイスの統合管理
- 直感的に操作可能なインターフェース
- ユーザ申込画面でアカウント登録を簡略化



認証局を運用する上で管理すべき項目は多岐にわたります。証明書はもちろん証明書を使用するアカウントや証明書を格納する認証デバイスなど、Gléasでは統合された管理インターフェースを提供し、管理者の負担を軽減させます。また、証明書を利用するエンドユーザ自身によるユーザ登録申請や証明書発行申請も画面から簡単に行えるため、申請発行業務を大幅に簡略化できます。

## Reliability

- より安全なハッシュ関数SHA-2に対応
- USBトークンなどの認証デバイスを標準サポート



安全性の高い認証システムを構築するために、GléasではNIST(米国国立標準技術研究所)が推奨するRSA2048bit鍵やハッシュ関数SHA-2などの新しいアルゴリズムをサポートしています。また、Gléasは証明書をより安全に利用するためにUSBトークンやICカードなどのデバイスを標準でサポートしており、証明書をWebブラウザから認証デバイスに格納することができます。

## Flexibility

- テンプレート機能による柔軟なポリシー設定
- 中小規模から大規模まで多彩なシステム環境をサポート



ユーザが認証局に求める機能はさまざまです。認証局の細かな属性や外部リポジトリとの連携などのシステム運用にかかわるルールは、強化されたテンプレートとグループ機能により柔軟に設定することができます。また、Gléasでは機能によりコンポーネントが分割されているため、使用される環境に応じてサーバの台数を増やして増大する負荷を処理することができます。

## → 豊富な対応デバイス

### USBトークン・ICカード

次世代暗号アルゴリズムを採用し、認証機能を搭載したセキュリティ・デバイスです。証明書を安全に格納し、所有と記憶による二因子認証を実現します。

### スマートデバイス

いつでも、どこからでも社内の情報資産にアクセスできるスマートフォンやタブレットなどに証明書を格納することでアクセス時の認証強化が可能となります。

### PC

Microsoft Windowsの証明書ストアやMac OS Xのキーチェーンなどの各OSが提供している証明書格納領域を利用することで認証強化が可能となります。



## 証明書ライフサイクル全体の効率的管理

Gléasは証明書要求の作成から証明書の失効、有効期限切れまでの証明書ライフサイクル全体を管理します。サブジェクト、鍵用途、証明書の発行日時、有効期限など多彩な条件で証明書を検索し、一覧表示する機能も備えているため大量の証明書を効率的に管理することが可能です。同じ操作を保存することで一括して実行可能とするドック機能や検索条件を保存するクイックナビ機能を使用することで、さらに運用業務の効率化を図ることができます。

## 充実したアカウント管理

ユーザやコンピュータ、サーバなどの証明書を発行する対象を、アカウントとして統一的に管理します。アカウントはグループに参加することで用途に応じて分類・管理することができます。所属できるグループの数には制限がないので、複雑な構造の組織にも対応が可能です。また、アカウント情報は、CSV形式のファイルやLDAP、ActiveDirectoryなどを利用したインポートにも対応しています。さらにCSV形式のファイルでは証明書発行やアカウント削除などの一括処理も可能です。

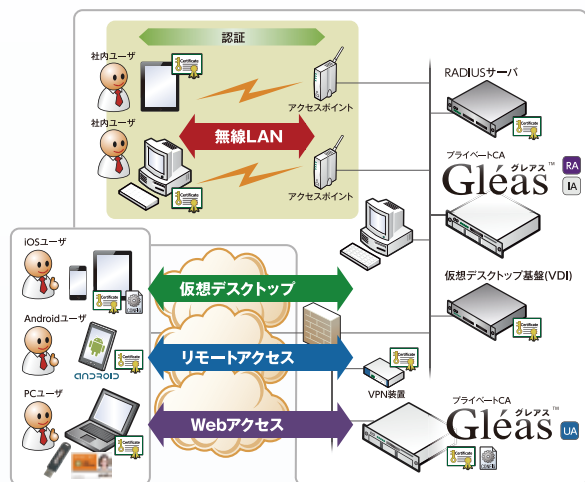
## マルチデバイスへの証明書配布機能

証明書配布機能は、管理者があらかじめ設定した証明書格納領域に専用のウェブ画面からファイルを介さず、証明書を直接インポートできます。そのため管理・配布に関わる運用業務の効率化、ユーザの安全かつ簡単な利用を実現し、トータルオペレーションコストの削減に大きく貢献します。また、証明書が複数の端末にインポートされるのを防ぐPC用のインポートワンス機能、iOSの設定情報をまとめた構成プロファイルへの対応など、各デバイスの特性に応じた機能も充実しています。

## 強力なテンプレート機能

証明書のサブジェクトや鍵長、有効期限などの内容およびそのポリシーを「テンプレート」により管理します。グループにテンプレートを設定することで、グループごとに異なるポリシーの証明書を発行できます。さらに、テンプレートを組み合わせることで企業ポリシーに合わせた証明書の発行と管理の自動化を実現しています。

## → クライアント証明書による認証強化ソリューション



## → 柔軟な管理・運用を可能にする3つの管理概念

Gléasでは、3種類のインターフェースを用いた管理概念を採用し、柔軟な管理・運用を実現しています。たとえば、登録局 (RA)・発行局 (IA) に対して別の管理者をたてる運用や、発行局 (IA) を自動化してひとりの管理者で運用することなどが可能です。

また、マルチテナント機能により、1台の認証局に複数の組織における管理を、その各運用単位毎に実現することも可能です。

**UA ユーザ申込局**  
User-Application Authority

証明書ユーザが自らのユーザ登録の申請や証明書の発行要求、ダウンロードなどの管理作業を行います。

**RA 登録局**  
Registration Authority

アカウント (ユーザなど証明書発行対象) の登録、証明書テンプレートの設計、グループの設計、発行局への証明書発行・失効・一時停止の指示などを行います。

**IA 発行局**  
Issuing Authority

登録局からの依頼により、証明書の発行・失効・一時停止を実行します。認証局証明書の鍵の管理や失効リストの発行も行います。

エディション	スターター・エディション	スタンダード・エディション	エンタープライズ・エディション
ライセンス数(オンプレミス)		100~50,000	1,000~
ライセンス数(クラウド)	50・100		
<b>発行可能な証明書</b>			
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	○	○
下位認証局証明書		○	○
<b>証明書用途</b>			
Webサイト認証	○	○	○
SSL-VPN認証	○	○	○
IPsec認証	○	○	○
無線LAN認証	○	○	○
スマートカードログオン		○	○
ドメインコントローラ		○	○
ファイル暗号化		○	○
メール暗号化(S/MIME)		○	○
電子署名		○	○
<b>管理</b>			
登録局(RA)	○	○	○
発行局(IA)		○	○
証明書配布(UA)	○	○	○
証明書申請		○	○
アカウント検索	○	○	○
証明書検索	○	○	○
認証デバイス管理	○	○	○
グループ管理		○	○
管理者数	1	2~	2~
証明書発行承認		○	○
構成プロファイル(iOS)	○	○	○
モバイルデバイス管理(iOS)		○	○
カスタムテンプレート作成		○	○
CSVエクスポート	○	○	○
CSV一括インポート		○	○
外部LDAP/AD手動インポート		○	○
外部LDAP/AD認証連携		○	○
マルチテナント		△	○
パブリックルート署名		△	○
バックアップ	クラウド	内部(外部△)	内部・外部
IDM連携		△	○
証明書更新猶予期間	○	○	○
証明書発行通知メール		△	○
<b>証明書配布(UA)</b>			
構成プロファイル(iOS)	○※2	○	○
構成プロファイル(カスタマイズ)		△	○
端末認証(iOS)		○	○
インポートワンス(PC)	○	○	○
インポートロック	○	○	○
SSLアクセラレータ対応		△	○
Windows証明書ストア(ユーザストア)	○	○	○
Windows証明書ストア(コンピュータ)	○	○	○
証明書更新機能(iOS)		○	○
USBトークン/ICカード	○	○	○
一般ユーザ権限でのインポート	○	○	○
英語版UA	○	○	○
PKCS#12	○	○	○

※1 標準でサーバ証明書のライセンスが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 NTTドコモオリジナル証明書対応の機種となります。 ※6 対応予定(2012年3月現在)

	スターター・エディション	スタンダード・エディション	エンタープライズ・エディション
<b>システム構成</b>			
Linux	○	○	○
Solaris 10			○
クラスターリング		△※2	○
LDAP証明書リポジトリ		○	○
LDAPアプリケーション		△	○
失効情報伝播:LDAP		○	○
:HTTP	○	○	○
外部LDAP/ADエクスポート		△	○
IA専用サーバ			△
UA専用サーバ		△	△
サードパーティUA			△
パブリックサーバ証明書		○	○
HSMサポート ※3		△	△
インターフェースカスタマイズ		△	△
SNMP		○	○
簡易RADIUS		○	○
上位認証局		○	○
OCSP専用サーバ		△	△
<b>暗号関連</b>			
RSA1024~8192bit	○	○	○
SHA-2	○	○	○
全体CRL	○	○	○
区分CRL		○	○
OCSPレスポンス		○	○
PKCS#10証明書要求		○	○
SCEP		○	○
CRL手動更新	○	○	○
失効後のCRL即時更新		○	○
<b>証明書格納先(※4)</b>			
USBトークン/ICカード	○	○	○
・Gemalto .NETシリーズ	○	○	○
・SafeNet eTokenシリーズ	○	○	○
・デバイス初期化	○	○	○
・暗号鍵ペア生成	○	○	○
iOSデバイス	○	○	○
・暗号鍵ペア生成	○	○	○
Android	○	○	○
携帯電話(※5)	○	○	○
Windows Phone(※6)	○	○	○
Windows CE	△	△	△
Windowsの証明書ストア	○	○	○
Mac OS Xのキーチェーン(※6)	○	○	○

→ 製品仕様 Specifications

※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	2GB~
内蔵HDD	SATAまたはSAS HDD2本(RAID1)

※クラウド仕様

メモリ	1GB~
ディスク	30GB以上
NIC	グローバルIPアドレス 1個以上

記載内容は2012年3月現在のものです。製品仕様および価格は予告なく変更することがあります。最新の仕様はJS3のWebサイト(<http://www.jcch-sss.com/>)をご確認ください。

●Microsoft Corporationのガイドラインに従って画面写真を掲載しています。 ●This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)  
 ●This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)... ●Android is a trademark of Google Inc.

**js<sup>3</sup> JCCH・セキュリティ・ソリューション・システムズ**

Tel. **03-5615-1020** Fax. **03-5604-1563**  
 〒116-0014 東京都荒川区東日暮里5-52-2 神谷ビル7F  
 URL.[www.jcch-sss.com](http://www.jcch-sss.com) e-mail.[sales@jcch-sss.com](mailto:sales@jcch-sss.com)

●仕様・デザインは予告なく変更することがあります。ご了承下さい。  
 ●本文中に記載されている商品名、および社名はそれぞれ各社の商標、または登録商標です。

お問い合わせ先