JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局 Gléas ホワイトペーパー

Cato Cloudでのクライアント証明書認証

Ver. 1.0
2021 年 2 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」で発行されたクライアント証明書を利用して、Cato Networks社のクラウド型ネットワークセキュリティ「Cato Cloud」(ケイト クラウド)にてクライアント証明書認証をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- クラウド型リモートアクセスサービス：CATO Cloud
  ※ 以後、「Cato」と記載します
- JS3 プライベート認証局 Gléas （バージョン2.2.5）
  ※ 以後、「Gléas」と記載します
- クライアント：Windows 10 Pro（バージョン1909） / Cato Client (バージョン 2.0.3.1b7852fe)
  ※ 以後、「Windows」と記載します
- クライアント：iPhone 12 Pro（iOS 10.15.6） / Cato Client (バージョン 2.0.3.1b7852fe)
  ※ 以後、「iPhone」と記載します

以下については、本書では説明を割愛します。

- Catoの一般的な設定（Cato Socketの構築、Cato管理画面の操作など）
  ※ 本書はCato Clientからのパスワード認証によるCatoへの接続が可能なことを前提としています
- Gléasでのサーバ・クライアント証明書の発行などの基本操作

これらについては、各製品・サービスのマニュアル・ヘルプをご参照いただくか、各製品を取り扱う販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。

【クライアント証明書のクライアント端末へのインポート】

1. Catoで、リモートポートフォワーディングを設定し、宅内に設置されたGléasのUA（ユーザ画面）に、インターネット経由でアクセス可能にする。
2. クライアント端末は、Cato経由でUAにアクセスし証明書をインポートする。
   なお、iPhoneの場合はOver The Airエンロールメントで証明書を含む構成プロファイルをインポートする。

【Cato Clientでのクライアント証明書によるCatoへのアクセス認証】

1. Cato ClientからCatoにアクセスする。
2. パスワードに加えクライアント証明書認証がおこなわれ、Cato経由で社内やクラウド上のリソースの利用が可能となる。

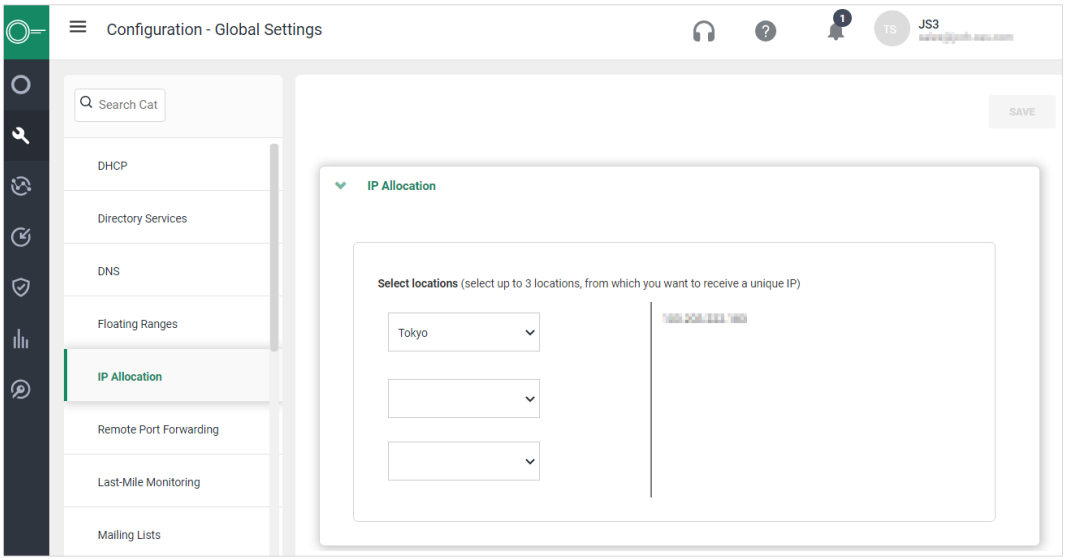
1.4. 本構成における留意事項

- iOS向けCato VPN接続プロファイルの生成機能はGléasのオプション機能となります。詳細は最終項のお問い合わせ先までご連絡ください。
- CatoのVPN接続ではクライアント証明書の失効確認はサポートされておりません。
- 本書の手順で証明書をWindowsインポートするには、OSの管理者権限が必要になります。

2. Catoの設定

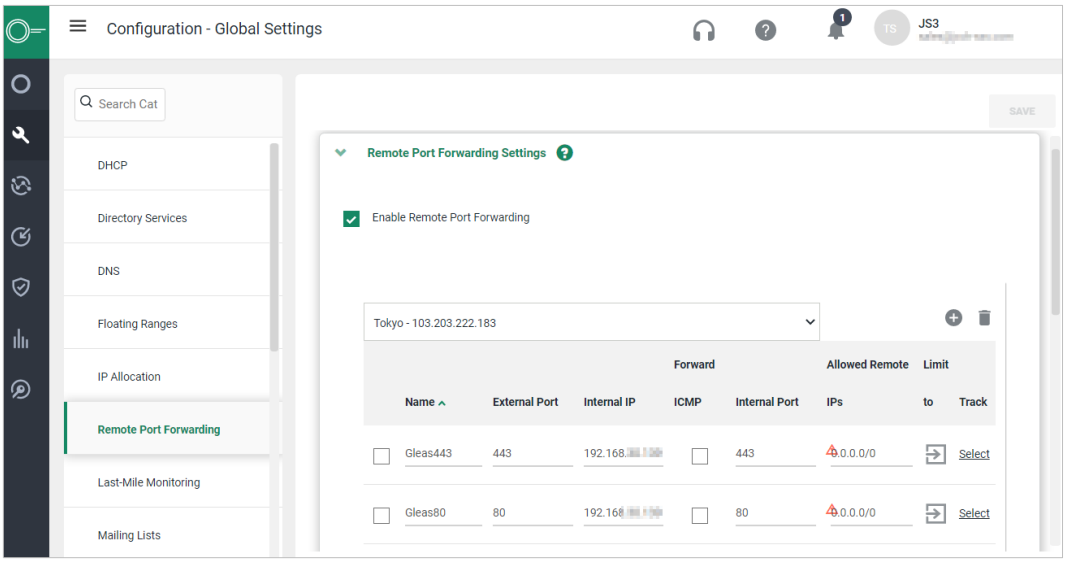
2.1. リモートポートフォワーディングの設定

Cato の Web 管理画面にログインし、以下の操作をおこないます。
Configuration > Global Settings > IP Allocation と進み、Select Locations で[Tokyo]を選択し、東京 POP の IP アドレスを取得します。



Configuration > Global Settings > Remote Port Forwarding より[Enable Remote Port Forwarding]にチェックを入れ、IP Allocation にて取得した IP アドレスを選択し、+ボタンを押下後に以下の情報を入力します（ポートごとに 2 つエントリを作成します）。

- Name： 識別名称を入力
- External Port： 443 と 80
- Internal IP： Gleas の UA に割り当てた IP アドレス
- Internal Port： 443 と 80
- Allowed Remote IPs： 0.0.0.0/0 (アクセス元の IP アドレスが固定できない場合)



また、IP Allocation にて取得した東京の IP アドレスに対し、DNS で名前解決が可能なホスト名（A レコード）を付与しておきます。Gléas の UA に設定する SSL サーバ証明書のサブジェクト代替名（DNS 名）にもこのホスト名を付与する必要があります。

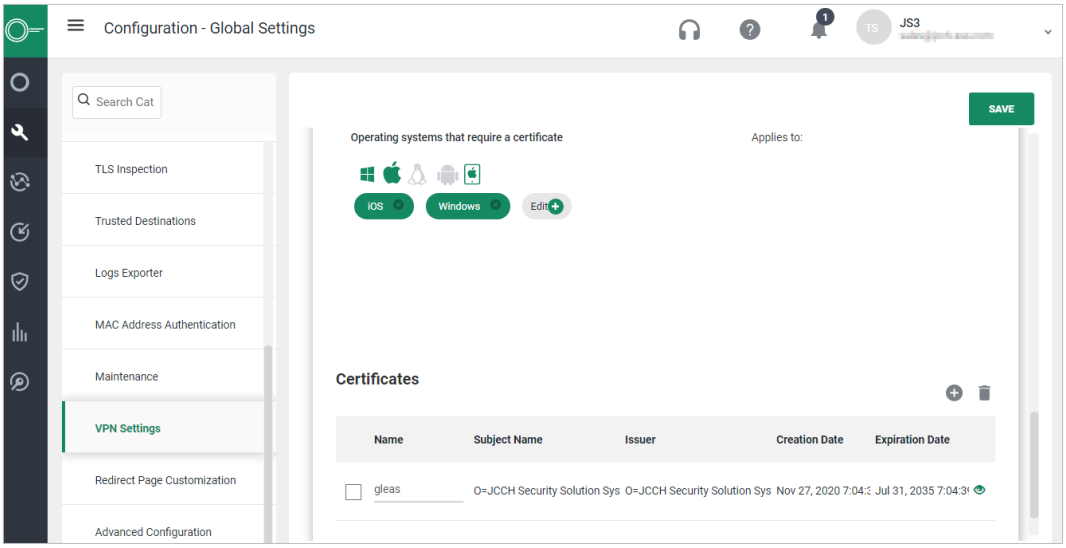
設定が正常におこなわれていれば、付与したホスト名で Gléas の UA に http、あるいは https でアクセスすることが可能です。
（https でアクセスした場合に警告が出現する状態では、OTA エンロールメントに失敗します）

2.2. クライアント証明書認証の設定

Gléas よりルート証明書（PEM 形式）をダウンロードしておきます。デフォルトのルート証明書ダウンロード URL は以下の通りです。
http://gleas.example.com/crl/ia1.pem

Cato の Web 管理画面より Global Settings > VPN Settings > Device Authentication で以下の設定をおこないます。

- Operating systems that require a certificate で、証明書認証をおこなう OS を選択
- Certificates の Name にルート CA の識別名称を入力し、[UPLOAD FILE]にて Gléas よりダウンロードしたルート証明書をアップロード



この画面で OS を選択せずルート証明書だけを設定し、代わりに VPN Users > User 名 > Device Authentication で同様に OS を指定することで、特定のユーザだけ証明書を要求するといった設定も可能です。

3. Gléas UAの管理者設定（Windows用）

GléasのUA（申込局）より発行済み証明書をWindowsクライアントにインポートできるよう設定します。

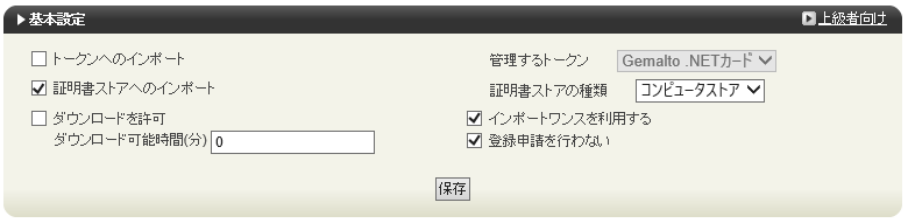
※ 下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[コンピュータストア]を選択
- 証明書のインポートを一度のみに制限する場合、[インポートワンスを利用する]にチェック



設定終了後、[保存]をクリックし設定を保存します。
また、認証デバイス設定の以下項目にチェックがないことを確認します。

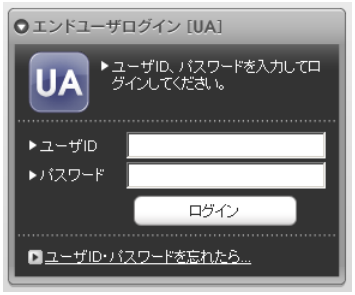
- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

4. クライアントからのアクセス（Windows）

4.1. クライアント証明書のインポート

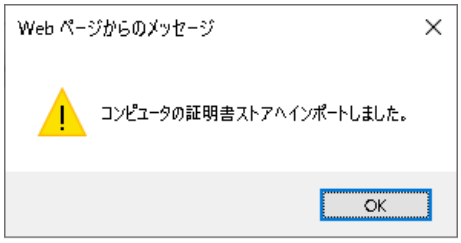
Internet Explorer（IE）を、アイコン右クリックの「管理者として実行」メニューから起動し、2.1項で設定したホストにアクセスします。
Gléas UAのログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

※ UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先までご連絡ください



ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。



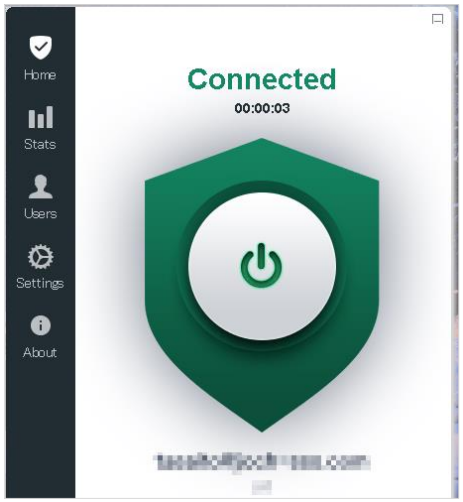
※ 初回ログイン時にはActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了します。また、事前にインターネットオプションにてこのホスト名を「信頼済みサイト」に加えておく必要があります

※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします

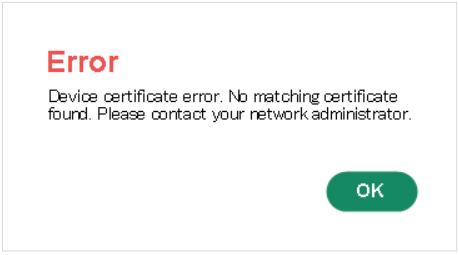
インポートワンスを有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートをおこなうことはできません。

4.2. Cato へのアクセス

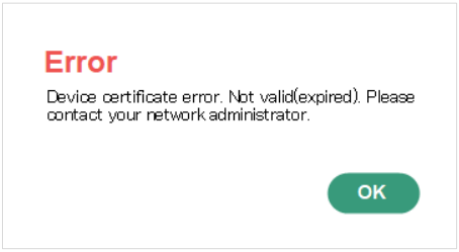
Cato Clientでアカウント（テナントID)、ユーザ名、パスワードが設定された状態で接続すると、証明書認証がバックグラウンドでおこなわれてCatoに接続された状態になります。



証明書がない状態でアクセスすると以下のメッセージが出現します。



証明書の有効期限を過ぎている場合は以下のメッセージが出現します。。



5. Gléas UAの管理者設定（iOS用）

GléasのUA（申込局）より発行済み証明書をiPhoneにインポートできるよう設定します。
※　下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA（申込局）をクリックします。
申込局詳細画面が開くので、認証デバイス情報のiPhone/iPadの設定までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

画面レイアウト

- [iPhone用レイアウトを利用する]をチェック

OTA(Over-the-air)

- [OTAエンロールメントを使用する]にチェック
- [接続するiOSデバイスを認証する]にチェックを入れると、事前に端末識別情報を登録したiOSデバイス以外は証明書を入手することができなくなります。本機能の詳細は最終項の問い合わせ先までお問い合わせください。
- [OTA用SCEP URL]に、2.1項で設定したホスト名とSCEP用URL（/scep）を入力
- [OTA認証局]に、OTAエンロールメント用の証明書を発行するCAを指定

iPhone構成プロファイル基本設定

- [名前]、[識別子]に任意の文字を入力（必須項目）

SCEPの設定

- [SCEP URL]に、2.1項で設定したホスト名とSCEP用URL（/scep）を入力
- [SCEP 認証局]に、Catoの認証に使うクライアント証明書を発行するCAを指定

Cato Clientの設定

- アカウントに、Catoのアカウント（テナントID）を入力

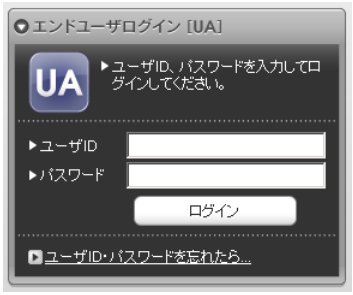
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

6. クライアントからのアクセス（iPhone）

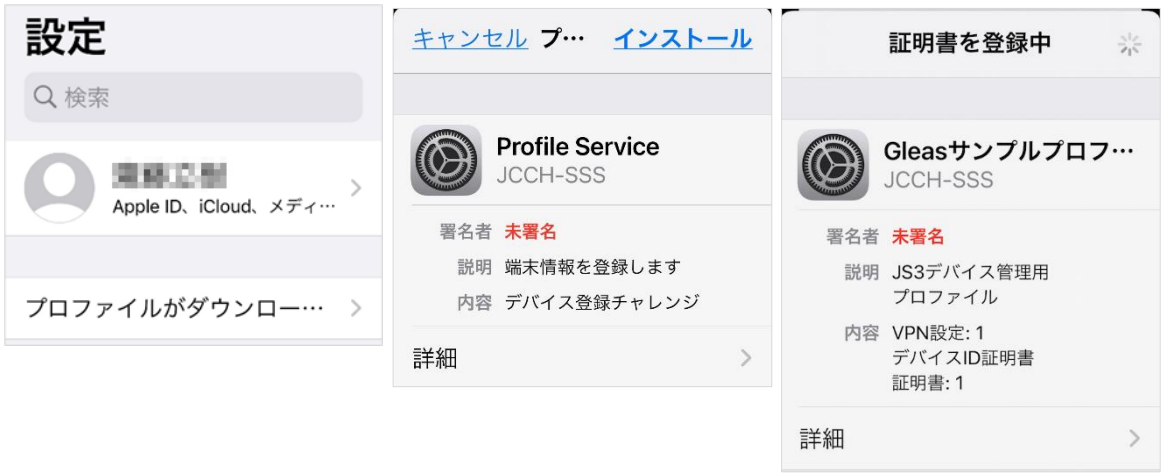
6.1. クライアント証明書のインポート

iPhoneのブラウザ（Safari）で、2.1項で設定したホストにアクセスします。
Gléas UAのログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、そのユーザ専用ページが表示されるので、[証明書要求]をタップし、構成プロファイルのダウンロードをおこないます。

画面の表示にしたがい設定アプリを開くと、プロファイルがダウンロードされた旨が表示されるので、インストールをおこないます。



問題なく進むと、インストールが完了した旨が表示されます。

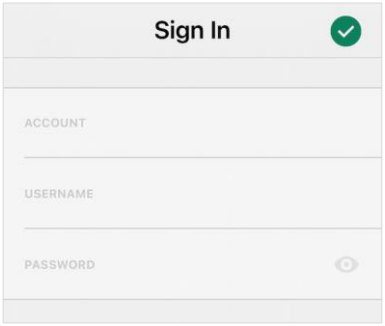
なお、[詳細]をタップすると、インストールされる証明書情報を見ることができます。必要に応じて確認してください。

Safariに戻り、[ログアウト]をタップしてUAからログアウトします。
以上で、iPhoneでの構成プロファイルのインストールは終了です。

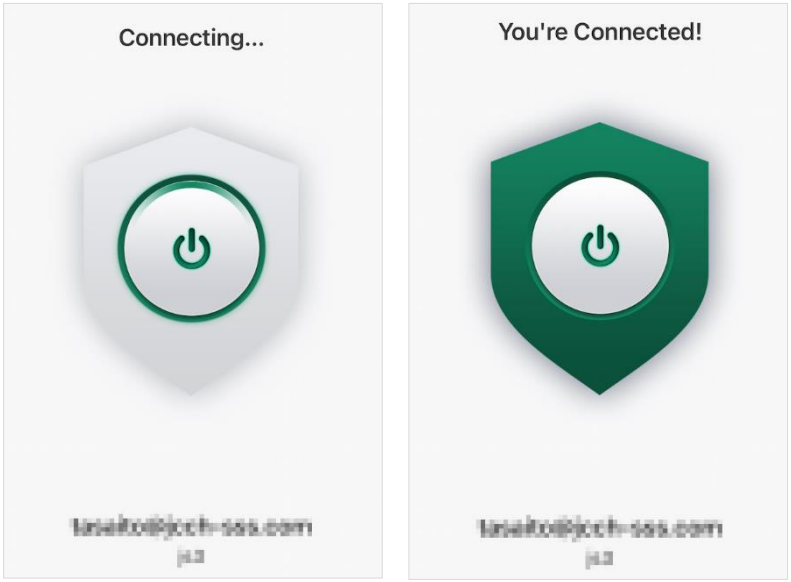
6.2. Cato へのアクセス

Cato Clientアプリを起動してアカウントの追加をおこないます。

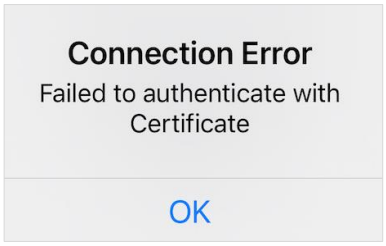
※ すでにアカウント設定がされている場合は、Edit User 画面で[Clear Credential]をタップして再度設定をする必要があるようです



その後、接続をするとバックグラウンドで証明書とパスワード認証をおこない、Cato へ接続します。



なお、有効な証明書がない場合はログインに失敗します。



7. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Cato Cloudに関するお問い合わせ
マクニカネットワークス株式会社
Mail:　cato-seles@cs.macnica.net

■Gléasや本検証内容に関するお問い合わせ
株式会社JCCH・セキュリティ・ソリューション・システムズ
営業本部
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com