



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CA Gléas ホワイトペーパー

～Cisco ASA5500～

クライアント証明書による Android での AnyConnect 認証設定

Ver.1.0

2011年9月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ 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。

プライベート CA Gléas ホワイトペーパー
Android 版 AnyConnect 設定

目次

1. はじめに	4
1.1. 本書について	4
1.2. 本書における環境	4
2. Gléas の管理者設定	5
2.1. UA (ユーザ申込局) 設定	5
3. Android の設定	6
3.1. Gléas の UA からの証明書インポート	6
3.2. AnyConnect での接続	10
4. 問い合わせ	11

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CA Gléas」で発行したクライアント証明書を利用して、シスコシステムズ合同会社のAndroid向けSSL-VPNクライアントソフトウェア（Cisco AnyConnect）での接続を行う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。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、5項のお問い合わせ先までお気軽にご連絡ください。

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。

- JS3 プライベートCA Gléas （バージョン 1.9）
※以後、「Gléas」と記載します
- Samsung Galaxy Tab 10.1 （Androidバージョン 3.1）
※以後、「Android」と記載します
- Cisco ASA5505 （バージョン 8.4(1)）
※以後、「ASA5500」と記載します
- Cisco AnyConnect for Samsung Devices （バージョン 2.4.7073）
※以後、「AnyConnect」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。

- ASA5500でのSSL-VPN環境のセットアップ
※弊社のWEBサイトでは、ASA5500でのSSL-VPN環境を構築するためのホワイトペーパーを公開しておりますので、構築時の参考にしてください
参考URL：
http://www.jcch-sss.com/images/Cisco_ASA_Gleas_configuration_AnyConnect.pdf
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- Androidでのネットワーク設定等の基本設定、及びAnyConnectソフトウェアのインストール

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

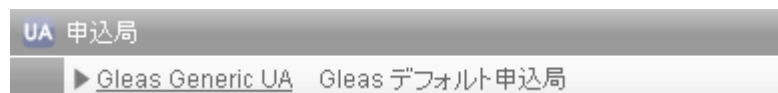
2. Gléasの管理者設定

Gléas で発行済みのクライアント証明書 を AnyConnect にインポートさせるための設定を本章では記載します。

※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

2.1. UA（ユーザ申込局）設定

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、Android用に設定するUA（申込局）をクリックします。



[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。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定

[インポートワンスを利用する]にチェックを入れてこの設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、証明書のダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のAndroidへの証明書のインストールを制限することができます。



設定終了後、[保存]をクリックします。

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]をチェックし、以下の設定を行います。

プライベート CA Gléas ホワイトペーパー Android 版 AnyConnect 設定

▶ Androidの設定

Android 用 UAを利用する

ダウンロードの動作

ログインパスワードで証明書を保護 数字のみの PIN を表示

証明書ダウンロードの種類

AnyConnectの接続名

AnyConnectの接続先URL

保存

- インポート時の証明書保護パスワードの設定
 - [ログインパスワードで証明書を保護]にチェックすると、UAログイン時のパスワードを利用します
 - [数字のみのPINを表示]をチェックすると、インポート時に数字のみのパスワードを画面に表示します
 - どちらにもチェックしないと、インポート時に英数字のパスワードを画面に表示します
- [証明書ダウンロードの種類]は、[Cisco AnyConnectへのインポート]を選択
- [AnyConnectの接続名]には、任意の接続名称を入力
- [AnyConnectの接続先URL]には、Androidデバイスから見たASAの接続先URLを入力

以上でGléasの設定は完了です。

3. Android の設定

3.1. Gléas の UA からの証明書インポート

Androidの標準ブラウザでGléasのUAサイトにアクセスします。

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。

プライベート CA Gléas ホワイトペーパー
Android 版 AnyConnect 設定



ログインすると、ユーザ専用ページが表示されます。



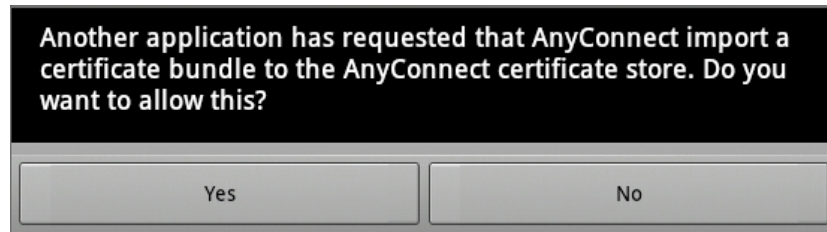
最初にクライアント証明書のインポートをするため[ダウンロード]をタップします。
ログインパスワードで証明書の保護をしない状態では、証明書インポート用のパスワードが表示されますので、覚えてから[決定]をタップします。

※ログインパスワードで証明書の保護を行う設定になっている場合は、この画面は出現しません

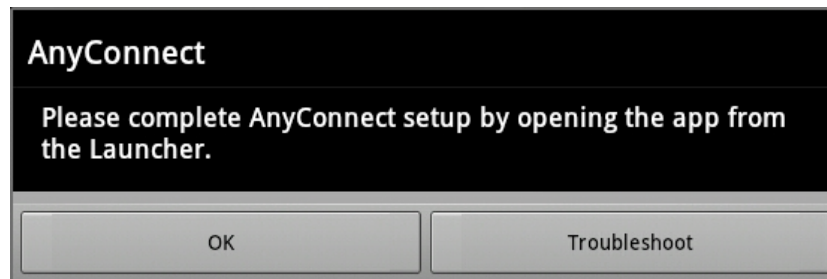
プライベート CA Gléas ホワイトペーパー
Android 版 AnyConnect 設定



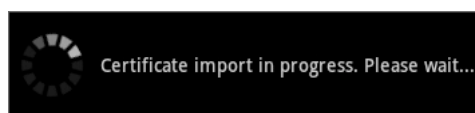
以下のメッセージが表示されますので、[Yes]をタップします。



以下のメッセージが出現する場合は、AnyConnectを一度起動しセットアップを終了させる必要があります。

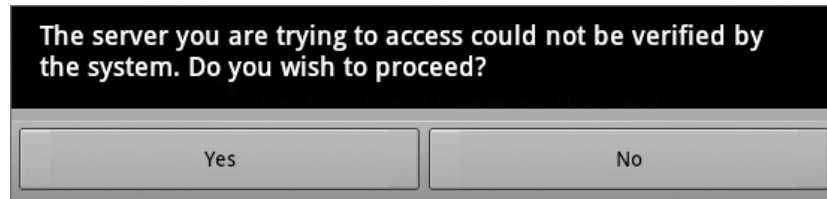


インポートが開始されます。

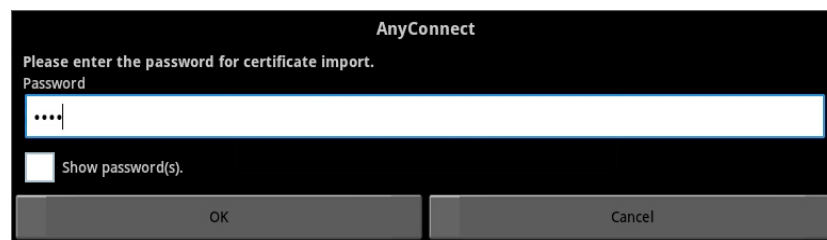


以下のメッセージが表示される場合は、接続しているGléasが正しいものであることを念のため確認したうえで[Yes]をタップします。

プライベート CA Gleás ホワイトペーパー
Android 版 AnyConnect 設定



クライアント証明書の保護パスワードを入力します。
ログインパスワードで証明書の保護をしている状態では、UAログイン用のパスワードを、そうでない場合はユーザ専用ページに表示されたパスワードを入力します。



インポートに成功すると、以下のメッセージが少しの間表示されます。

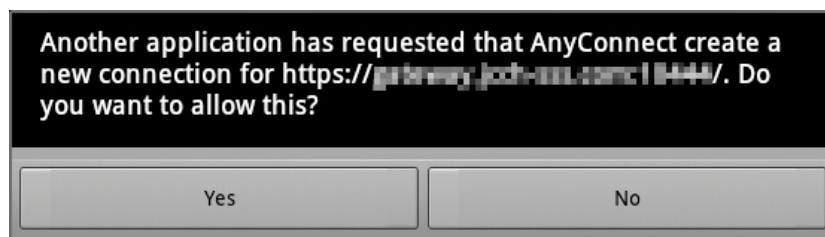
The certificate bundle has been successfully imported.

以上で、クライアント証明書のインポートは終了です。

AnyConnectの画面が表示されている場合は標準ブラウザを開きユーザ専用ページに戻り、接続先情報をAnyConnectにインポートするために[VPN設定を作成]をタップします。



その後、以下のメッセージが出現しますので[Yes]をタップすると接続先情報がAnyConnectにインポートされます。



成功すると以下のメッセージが短い間表示されます。

Successfully created a new VPN connection.

終了後、ユーザ専用ページに戻り[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、クライアント証明書のインポートは終了です。

なお、インポートロックを有効にしている場合、ダウンロードした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表示に変わり、以後のダウンロードは一切不可能となります。

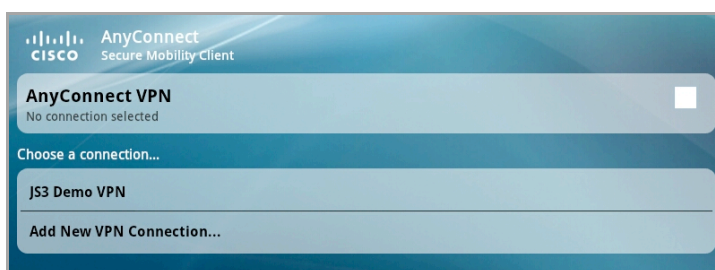


3.2. AnyConnect での接続

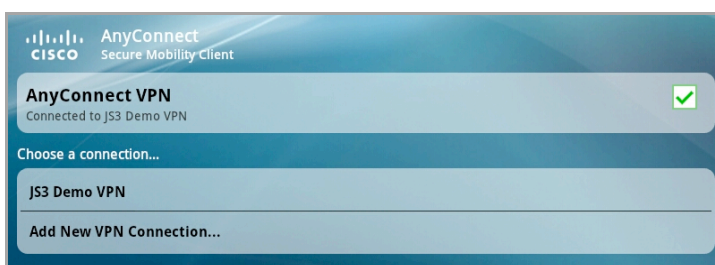
AnyConnectを起動するとインポート済みの設定が既に反映されています。

3.1項の手順でインポートを行っていただければ、インポートした証明書を利用して認証をするようになっています。ASAでクライアント証明書による認証設定がなされていれば、そのまま接続が可能です。

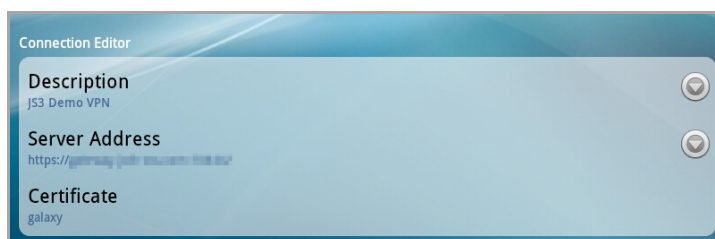
プライベート CA Gléas ホワイトペーパー Android 版 AnyConnect 設定



VPN接続に成功すると、「Connected to [Gléasで設定したAnyConnectの接続名]」と表示されます。



設定を見ると、Gléasの管理者画面で設定したものが反映されていることが分かります。



4. 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。

■Gléasや検証明の証明書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

Tel: 050-3821-2195

Mail: sales@jcch-sss.com