

# 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。

#### 目次

1. はじる	めに	4
1.1.	本書について	4
1.2.	本書における環境	4
2. Gléa	s の管理者設定	5
2.1.	UA(ユーザ申込局)設定	5
3. Andr	oid 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。

> UA 申込局 ▶ <u>Gleas Generic UA</u> Gleas デフォルト申込局

[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。

▶基本設定	
🗆 トークンへのインボート	管理するトークン Gemalto .NETカード 💌
□ 証明書ストアへのインポート	証明書ストアの種類 ユーザストア 👤
ダウンロードを許可 ダウンロード可能時間(分) 1	<ul> <li>インポートワンスを利用する</li> <li>登録申請を行わない</li> </ul>
	保存

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。

▶ 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	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	Cisco AnyConnectヘインポート 💌		
AnyConnectの接続名	JS3 Demo VPN		
AnyConnectの接続先URL	https://		
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 GI × +	≡,
●エンドユーザログイン [UA]	
UA ▶ユーザID、パスワードを入力し てログインしてください。	
▶ユーザID galaxy	
▶パスワード	
ログイン	
▶ <u>ユーザID・パスワードを忘れたら…</u>	

#### ログインすると、ユーザ専用ページが表示されます。

図 プライペートCA GI × +			≡,
$\leftrightarrow$ $\rightarrow$ $\times$ 😵 🔒 https://ipad.jcch-sss.com/ua/login/info	*	Q	0
プライベート	CA G	léä	Ŝ UA
サムスン ギャラクシー さんのページ			
ב-#ID		8	galaxy
メール			
AnyConnectの接続設定			
接続名: JS3 Demo VPN	١	/PN設定を	生作成
JCCH-SSS demo CA			
有効期限 2014/08/24		ダウンロ	4 – F
		<b></b>	ヴアウト
(C) 2011 JC	CH Security Solu	tion System	s Co., Ltd.

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、憶えてから[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 Gl	× +	≡,
$\leftrightarrow$ > c 😵	https://ipad.jcch-sss.com/ua/login/info	\star Q 🛛
	プライベー	🗠 Gléåš 💵
サムスン ギャラクシー さんの	ページ	
ユーザID		galaxy
メール		
AnyConnect の接続設定		
接続名: JS3 Demo VPN		VPN設定を作成
JCCH-SSS demo CA		
証明書 PIN: 0052		決定 キャンセル
		ログアウト
	(C) 2011 JG	CCH Security Solution Systems Co., Ltd.

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。

Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this?		
Yes	No	

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。

The server you are trying to access could not be verified by the system. Do you wish to proceed?		
Yes	No	

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。

AnyConnect			
Please enter the password for certificate import.			
Password			
Show password(s).			
ОК	Cancel		

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。

■ プライベートCA GI × +	≡,
$\leftrightarrow$ $\rightarrow$ $\times$ $\textcircled{S}$ $\triangleq$ https://ipad.jcch-sss.com/ua/login/info	★ Q 🛛
プライベート	🛯 🗛 Gléãs 🗠
サムスン ギャラクシー さんのページ	
ユーザID	galaxy
メール	
AnyConnect の接続設定	
接続名: JS3 Demo VPN	VPN設定を作成
JCCH-SSS demo CA	
有効期限 2014/08/24	ダウンロード
	ログアウト
(C) 2011 JC	CH Security Solution Systems Co., Ltd.

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。

۱۱۱،۱۱، AnyConnect CISCO Secure Mobility Client	
AnyConnect VPN No connection selected	
Choose a connection	
JS3 Demo VPN	
Add New VPN Connection	

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。

(1)	
AnyConnect VPN Connected to JS3 Demo VPN	
Choose a connection	
JS3 Demo VPN	
Add New VPN Connection	

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。

Connection Editor	
Description JS3 Demo VPN	۲
Server Address	
Certificate galaxy	

# 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や検証用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