

プライベートCA Gléas ホワイトペーパー

~Cisco ASA5500~

Androidでのクライアント証明書による

L2TP/IPsec認証設定

Ver.1.0 2011 年 6 月

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

- 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
1.3.	本書における構成	5
2. ASA	5500(ASDM)の設定	5
2.1.	電子証明書のインポート	5
2.2.	IP アドレスプールの作成	9
2.3.	L2TP/IPsec の設定	9
2.4.	暗号マップの設定	11
2.5.	接続プロファイルの変更	12
2.6.	トンネルグループの割当	13
3. Gléa	s の管理者設定	14
3.1.	UA(ユーザ申込局)設定	14
4. Andr	roid の設定	15
4.1.	Gléas の UA からの証明書インポート	15
4.2.	L2TP/IPsec の設定	19
5. 問い	合わせ	20

1. はじめに

1.1. 本書について

本書では、シスコシステムズ合同会社の統合セキュリティアプライアンスである 「ASA5500」シリーズと、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、Android端末にてL2TP/IPsec接続を行う環境を構築する 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。

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。

- Cisco ASA5505 (Version 8.4(1))
 ※以後、「ASA5500」と記載します
 ※設定はAdaptive Security Device Manager (ASDM) を利用して行います。ASDMのバージョンは6.4(1)で行っています
- > JS3 プライベートCA Gléas (バージョン1.8)
 ※以後、「Gléas」と記載します
- > HTC Aria (イー・モバイル S31HT、Android 2.2.1)
 ※以後、「Android」と記載します
 ※L2TP/IPsecクライアントはAndroid標準のものを利用します
 ※シスコシステムズ社では、ASA5500のバージョン8.4(1)以降とAndroid2.1以降にてL2TP/IPsecの接続をサポートするとしています

以下については、本書では説明を割愛します。

- ASA5500の基本的なセットアップ方法
- 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
- 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。

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。



※仮想インターネットの部分は、実際はWifiを利用

- ASA5500はインターネットとLANの境界にゲートウェイとして存在し、 L2TP/IPsecを終端する
- 2. ASA5500及びAndroidはGléasにより発行された証明書を利用する
- 有効なクライアント証明書を持つAndroidだけがVPN接続を行うことができる
- 4. クライアント証明書の失効確認には証明書失効リスト(CRL)を利用する

2. ASA5500 (ASDM)の設定

2.1. 電子証明書のインポート

ASA5500 にサーバ証明書と、今回利用するクライアント証明書のトラストアンカ となるルート認証局をインポートします。

本手順を行う前にあらかじめ Gléas よりサーバ証明書をファイル形式 (PKCS#12 ファイル) でダウンロードしておきます。

ASDM にログインし、上部より[Configuration]ボタンをクリックし、左側ペインの 大メニューより[Remote Access VPN]をクリック、小メニューより[Certificate Management] > [Identity Certificates]を選択します。 その後、右側ペインで[Add]をクリックします。

Co	nfiguration > Re	mote Access VP	N > Certificate Ma	nagement > Identity Certific	<u>ates</u>	
	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Add
						Show Details
						Delete
						Export
						Install

「Add Identity Certificate」ウィンドウが表示されるので、以下を設定します。

- [Trustpoint Name:]には任意の名前を入力
- [Import the identity certificate from a file:]を選択
- [Decryption Passphrase:] には PKCS#12 ファイルのパスワードを入力
- [File to Import From:] には PKCS#12 ファイルへのパスを入力

🔂 Add Identity Certificate			×
Trustpoint Name:	gleas		
Import the identity certif	icate from a file:		
Decryption Passphrase:	****		
File to Import From:	C:¥servercertp12	Browse	
C Add a new identity certif	icate:		
Key Pair:	<default-rsa-key></default-rsa-key>	Show	New
Certificate Subject DN:	CN=ciscoasa	Select	
🗖 Generate self-signed	d certificate		
🗖 Act as local cer	tificate authority and issue dynamic c	ertificates to TLS	i–Proxy
		L	Advanced
Add Certifi	icate Cancel	Help	

入力後、[Add Certificate]をクリックします。以下のメッセージが表示されれば完了です。



サーバ証明書が以下のように表示されます。

Configuration > Re	<u>emote Access VP</u>	<u>N > Certificate Ma</u>	<u>inagement</u> > <u>Identity Certi</u>	<u>icates</u>	
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Add
de=COM_de=JC	de=JCCH-SSS_d	21:57:45 JST Feb 2	eleas	General Purno	
			0.000		Show Details
					Delete
					Export
					Install

詳細を見る場合は[Show Details]をクリックします。

また上記操作でルート証明書も同時にインポートされています。

左側ペインより[CA Certificates]を選択すると、インポートされたルート証明書の情報を見ることができます。

<u>C</u>	Sonfiguration > Remote Access VPN > Certificate Management > CA Certificates					
	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Add
	JCCH-SSS demo	dc=JCCH-SSS, d	00:46:45 JST Jan 7	gleas	Signature	
						Edit
						Show Details
						Request CRL
						Delete

詳細を見る場合は[Show Details]をクリックします。

この状態で[Edit]をクリックすると、「Edit Options for CA Certificate」ウィンドウが 開くので、以下設定を行います。

 [Revocation Check]タブで、[Check Certificates for revocation]を選択し、下の ボックスから CRL を Revocation Methods(失効方法の確認方法)として指定 する

It Options for CA Certificate Revocation Check CRI Retrieva	e	vanced
C Do not check certificates for	revocation	
Check certificates for revoca	ition	
Revocation Methods		
Specify the methods used method will be used only i	for revocation checking and their order. If both met f the first one returns error	hods are selected, the second
OCSP	Add>> CRL	Move Up
	< <remove td="" <=""><td>Move Down</td></remove>	Move Down

※[Consider certificate valid if revocation information cannnot be retrieved]をチェックすると、 CRL 取得時にエラーが起こった場合等でも、証明書認証を成功させます

 [CRL Retrieval Policy]タブで、[Use static URLs configured below]にチェックを 入れ、Static Configuration ボックスに CRL を取得する URI を設定します

dit Options for CA Certificate	
Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced	
Use CRL Distribution Point from the certificate	
✓ Use Static URLs configured below	
Static Configuration	
Static URLs:	
	Edit
	Delete
	Move Up
	Move Down

※Gléasの標準のCRLの配布ポイントは以下の通りとなります(httpの場合)

http://Gléas のホスト名或いは IP アドレス/crl/ia1.crl

[Advanced]タブで、CRL optons の[Cache refresh time:]に CRL のキャッシュ時間を入力します(デフォルトでは 60 分)。

Edit Options for CA Certificate	×
Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced	
CRL options	
Specify the certificate revocation list parameters.	
Cache Refresh Time: 60 minutes	
I✓ Enforce next CRL update	
OCSP options	
Specify the Online Certificate Status Protocol (OCSP) parameters.	
Server URL: http://	
Disable nonce extension	
Validation Policy	
Specify the type of client connections that can be validated by this CA.	
C SSL C IPSec 📀 SSL and IPSec	
Other Options	
Accept certificates issued by this CA	
$\overline{oldsymbol{arsigma}}$ Accept certificates issued by the subordinate CAs of this CA	
OK Cancel Help	

※[Enforce next CRL update]にチェックを入れると、有効期限内にある CRL かどうかをチェ ックします。チェックを外すと有効期限を過ぎた CRL でもキャッシュされている間は有効 なものとして扱います(弊社未検証)

※[Validation Policy]では IPsec が含まれるものにしておく必要があります ([IPSec]か[SSL and IPSec])

※[Other Options]では、[Accept certificates issued by this CA]にチェックが入っている必要 があります

完了後、[OK]をクリックすると元の画面に戻ります。

この状態で[Request CRL]をクリックすると、ASA5500 は CRL を即時取得します。 取得時のメッセージにある通り、上部メニューより[Monitoring]をクリックし、左側 ペインより[Propertied] > [CRL]をクリックすると取得した CRL の情報を見ること ができます。

Monit	toring > Properties > CRL		
-ORL-			
01.2	View or clear the CRLs of all or the selected CA certificates.		
	CA Certificate Na		
	View CRL Clear CRL		
	CRL Info:		
	CRL Issuer Name: dc=JCCH-SSS,dc=COM,cn=JCCH-SSS demo CA LastUpdate: 19:10:35 JST Mar 1 2011 NextUpdate: 19:10:35 JST Mar 31 2011 Cached Until: 12:38:37 JST Mar 7 2011 Retrieved from CRL Distribution Point: http:// http:// Size (bytes): 5154 Associated Trustpoints: gleas		

2.2. IP アドレスプールの作成

上部メニューより[Configuration]をクリックします。 左側ペインの大メニューより[Remote Access VPN]をクリックし、小メニューより [Network (Client) Access] > [Address Assignment] > [Address Pools]をクリックしま す。右側ペインで[Add]をクリックします。

「Add IP Pool」ウィンドウが表示されるので、クライアントに割り当てるIPアドレス情報を設定し[OK]をクリックします。

🔂 Add IP Pool			×
Name:	pool-sample		
Starting IP Address:	10.0.0.1		
Ending IP Address:	10.0.0.10		
Subnet Mask:	255.255.255.0	v	
ОК	Cancel Help		

上記はVPNクライアントに対し、10.0.0.1~10/24を割り当てる例です。

2.3. L2TP/IPsec の設定

ここではウィザードを利用して設定を行います。

メニューバーの[Wizard] > [VPN Wizards] > [IPsec (IKEv1) Remote Access VPN Wizard...]をクリックしウィザードを開始します。

薩 VPN Wizard	X
VPN Wizard	IPsec IKEv1 Remote Access Wizard (Step 1 of)
Branch	Use this wizard to configure new new IPsec (IKEV1) remote access VPN tunnels. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate Network	Remote Access
	VPN Tunnel Interface: outside 💌
	✓ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Filmish Cancel Help

以下項目の通り、設定を進めます。

ページ	設定
IPsec IKEv1 Remote Access Wizard	デフォルト設定のまま[Next >]をクリック
(Step 1 of)	
Remote Access Client (Step 2 of)	(1) [Microsoft Windows client using L2TP over IPsec]を
	選択する
	(2) PPP 認証プロトコルは[MS-CHAP-V1]と
	[MS-CHAP-V2]を選択し、[Next >]をクリック
	※弊社環境では上記2つ共に[MS-CHAP]と表示されました
VPN Client Authentication Method and	(1) Authentication Method で[Certificate]を選択し、
Tunneling Group Name (Step 3 of)	[Certificate Name]で 2.1 項で作成した Trustpoint Name
	を選択する
	(2) Tunnel Group にはグループ名(任意)を設定
	上記を設定し、[Next >]をクリック
	※ここで設定したトンネルグループ名が、そのまま接続プロフ
	アイル名にもなります
Client Authentication (Step 4 of)	Authenticate using the local user database を選択し、
	[Next >]をクリック
	※外部ユーザデータを利用する場合は事前に AAA Server
	Group を設定しておき、それを選択
User Accounts (Step 5 of)	ユーザ認証情報(Username と Password)を追加し、
	[Next >]をクリック

	※ここで作成したユーザは自動的に Step 3 で作成したトンネ
	ルグループに割り当てられます
Address Pool (Step 6 of 11)	2.2 項で作成したアドレスプール名を選択し、[Next >]
	をクリック
	※[New]をクリックし、ここでアドレスプールを追加すること
	も可能
Attributes Pushed to Client (Optional)	デフォルト設定のまま[Next >]をクリック
(Step 7 of 11)	※クライアントに割り当てる DNS サーバ・WINS サーバのア
	ドレスやデフォルトのドメイン名の設定は必要に応じ行って
	ください
IKE Policy (Step 8 of 11)	デフォルト設定のまま[Next >]をクリック
	※暗号化・メッセージダイジェスト・DH グループの設定は必
	要に応じ変更してください
	※今回利用した Android では DH グループを 2 にしておく必要
	がありました
IPsec Settng (Step 9 of 11)	デフォルト設定のまま [Next >]をクリック
	※NAT 例外は今回の検証環境では、[Interface:]には内部インタ
	ーフェース(デフォルトでは Internal)を設定し、[Exempt
	Network]にはデフォルトで作成されている[Inside-Network]オ
	ブジェクトを指定しています
	※スプリットトンネルは L2TP/IPsec では利用できません
	※今回利用した Android では、Perfect Forwarding Security
	(PFS)はオフにする必要がありました
Summary (Step 10 of 11)	設定内容を確認し、[Finish]をクリック

2.4. 暗号マップの設定

上部メニューより[Configuration]をクリックします。 左側ペインの大メニューより[Remote Access VPN]をクリックし、小メニューより [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps]を展開します。 右側ペインより[Add]をクリックし、デフォルト設定に対し以下の設定変更を行いま す。

- [Policy Type:]を[dynamic]に変更
- [IKE v1 IPsec Proposal]に[TRANS_ESP_3DES_SHA](先程のウィザードにより 自動的にトランスフォームセットに追加されています)を指定

プライベート CA Gléas ホワイトペーパー
~Cisco ASA5500~
Android でのクライアント証明書による L2TP/IPsec 認証設定

Create IPsec Rule	x
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside Policy Type: dynamic Priority: 1	
IPsec Proposals (Transform Sets)	
IKE v1 IPsec Proposal: TRANS_ESP_3DES_SHA	
IKE v2 IPsec Proposal: Select	
Peer Settings - Optional for Dynamic Crypto Map Entries	
The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may	
specify up to 10 redundant peers.	
IP Address of Peer to Be Added:	
Add 22	
Remove Move Down	
Enable Perfect Forwarding Secrecy	
Diffie-Hellman Group:	

[OK]をクリックして完了後、[Apply]をクリックし設定を反映します。

2.5. 接続プロファイルの変更

上部メニューより[Configuration]をクリックします。

左側ペインの大メニューより[Remote Access VPN]をクリックし、小メニューより [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles]を展開します。 右側ペインの[Connection Profiles]欄に 2.3 で作成したプロファイルがあるので、 [Edit]をクリックし、以下設定変更を行います。

- ・ 左側ペインで[Advanced] > [IPsec]を展開し、右側ペインの[Certificate Settings]
 の[IKE Peer ID Validation:]を[Do not check]に変更
- [IKE Keepalives]で[Disable keepalives]を選択

🚰 Edit IPsec Remote Acc	ess Connection Profile: 12tp	
Basic H-Advanced General Client Addressing	Certificate Settings Send certificate chain: 「Enable IKE Peer ID Validation: Do not check	
Authentication Authorization Accounting ⊕r <mark>IPsec</mark>	IKE Keepalive © Disable keepalives C Marine keepalives	
PPP	Confidence Interval: seconds Retry Interval: seconds	
	C Headend will never initiate keepalive monitoring	

[OK]をクリックして完了後、[Apply]をクリックし設定を反映します。

2.6. トンネルグループの割当

上部メニューより[Configuration]をクリックします。 左側ペインの大メニューより[Remote Access VPN]をクリックし、小メニューより [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Policy]を展開します。

右側ペインの[Default to Connection Profile:]にチェックが入っていることを確認し、 2.3項のStep 3で設定した接続プロファイル名を選択します。

<u>Configuration > Remote Access VPN > Network (Client) Access</u> > <u>Advanced</u> > <u>IPsec</u> > <u>Certificate to</u> <u>Connection Profile Maps</u> > <u>Policy</u>	
Configure the policy for certificate group matching. The device processes the policies in the order listed below until it finds a match.	
Use the configured rules to match a certificate to a Connection Profile	
Use the certificate OU field to determine the Connection Profile	
Use the IKE identity to determine the Connection Profile	
Use the peer IP address to determine the Connection Profile	
☑ Default to Connection Profile: js3test	

なお、以下の通りクライアント証明書を利用した接続プロファイルの割当設定も可 能です。

[Use the configured rules to match a certificate to a Connection Profile]にチェックした場合は、証明書の記述条件により接続プロファイルを決めることが可能です。

左ペインより[Rules]を展開し、右ペインで条件を設定します。

	onfiguration > Remote Acc onnection Profile Maps > F	<u>ess VPN > Netwo</u> <u>lules</u>	rk (Client) Access >	<u>Advanced</u> > <u>IPsec</u> > <u>Certificate to</u>
	Define rules to map certificate: certificate fields together with	s to desired connecti their matching criteri	on profiles (tunnel group: a for the selected rule.	s). Use the bottom table to configure
Ce	Certificate to Connection Profile Maps			
	🖶 Add 🗹 Edit 📋 Delete			
	Map Name	Rule Priority	Rule Priority Mapped to Connection Profile	
	JS3MatchRule	10 js3test		
Ma	apping Criteria			
	🕈 Add 🗹 Edit 📋 Delet	•		
	Field C	omponent	Operator	Value
	Subject Domain Comp	onent (DC)	Contains	jech

上記はクライアント証明書のサブジェクトDC(domainComponent)に「jcch」という文字列が含まれる場合には、js3testという接続プロファイルにマッチングする例です。

[Use the certificate OU field to determine the Connection Profile]をチェックした場合 は、クライアント証明書のOU(organizatioinUnit)と接続プロファイル名とをマッ チングします。

以上で、ASA5500の設定は完了です。[Apply]をクリックして変更をrunning-config に書き込んでください。

3. Gléasの管理者設定

Gléas で発行済みのクライアント証明書を Android 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

3.1. 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	
□ トークンへのインポート	管理するトークン Gemalto NETカード 💌
□ 証明書ストアへのインボート	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) 	 インポートワンスを利用する 登録申請を行わない
	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、[保存]をクリックします。

▶ Androidの設定		
🔽 Android 用 UAを利用する		
	保存	

以上でGléasの設定は完了です。

4. Android の設定

4.1. 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。



ログインすると、ユーザ専用ページが表示されるので、[ダウンロード]をタップします。



プライベートCA (Gléå's 🛛
Android 太郎 さんのべ	ページ
ユーザID	android
メールアドレス	
Cloud Gleas CA	
有効期限 2012/05/11	ダウンロード
	ログアウト
(C) 2011 JCCH Security	y Solution Systems Co., Ltd

画面に証明書のPINが表示されるので、[決定]をタップします。



[PKCS12キーストアから抽出]と表示されるので、先の画面に表示されたPINを入力 します。





[証明書の名前を指定する]と表示されるので、任意の名前を指定します。



初めて「認証情報ストレージ」(Androidのキーストア)にアクセスする場合は、認 証情報ストレージをアクティベートするパスワードの設定を求められますので、画 面の説明に従いパスワードを設定します。

※ここで設定するパスワードはAndroid起動後、認証情報ストレージへの初回アクセス時に入力を 求められます

セキュリティ 画面のロック解除
● パスワードの設定
新しいパスワード:
/ 新しいパスワードの確認:
e de la constante de
OK キャンセル
安全な認証情報の使用

証明書の認証情報ストレージへのインポートが行われます。

プライベートCA 🤇	Gléå 🖾
Android 太郎 さんのペ	ージ
ユーザID	android
メール	
Cloud Gleas CA	
有効期限 2012/05/11	ダウンロード
	ログアウト
androidがインストールさ	されています。
(C) 2011 JCCH Security	Solution Systems Co., Ltd.

終了後、[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、Androidでの証明書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。



Gléås 🛛
ページ
android
ダウンロード済み
ログアウト
rity Colution Systems Co. 1td

4.2. L2TP/IPsec の設定

Androidのホーム画面で[設定] > [無線とネットワーク] > [VPN設定] > [VPNの追加] > [L2TP/IPSec CRT VPN]をタップし、以下を設定します。

- [VPN名]には、任意の名前を設定
- [VPNサーバの設定]には、アクセス先ASA5500のホスト名を設定
- [証明書を設定する]には、4.1でインポートした証明書を選択
- [CA証明書を設定する]には、4.1でインポートした証明書を選択



以上で、設定は終了です。

作成したVPN設定をタップして、ユーザID・パスワードの入力をし、接続を行って ください。

バックグラウンドでASA5500とAndroidとの間で証明書認証が行われます。



接続が行われると以下の通り「接続されています」と表示されます。



5. 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