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iPhoneでのIPsec認証設定

Ver.1.0

2011 年 4 月

目次

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・iPhone用の構成プロファイルを利用して、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1.7）
  ※以後、「Gléas」と記載します
- iPhone4 （iOS 4.2.1）
  ※以後、「iPhone」と記載します
  ※IPsecクライアントはiOS標準のものを利用します
  ※2011年4月現在、シスコシステムズ社ではiOS 2.x / 3.xのみの動作確認となっています

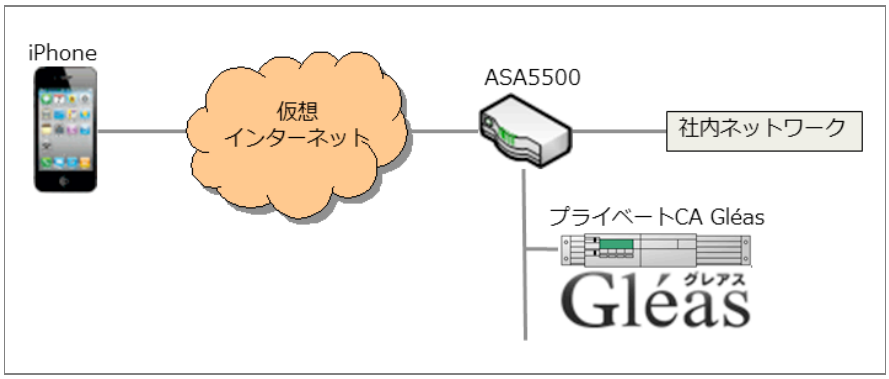
以下については、本書では説明を割愛します。

- 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
- iPhone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

1. 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、IPsecを終端する
2. 有効なクライアント証明書を持つiPhoneだけがIPsec接続を行うことができる
3. 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

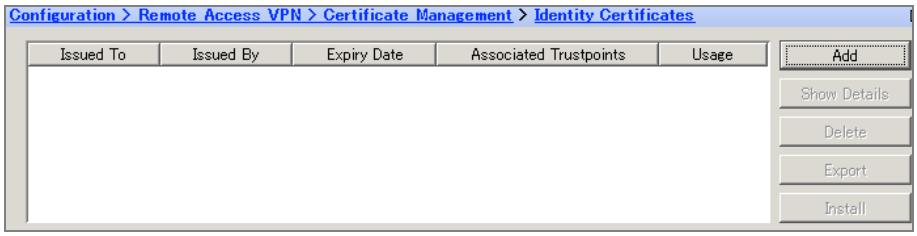
2. ASA5500（ASDM）の設定

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。

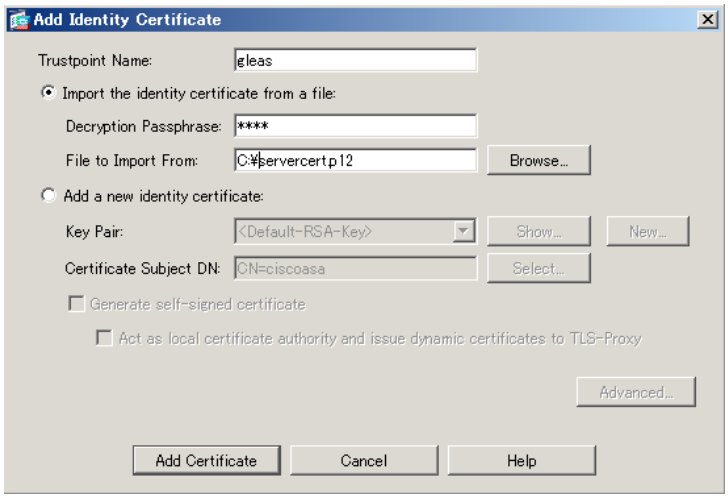
本手順を行う前にあらかじめ Gléas よりサーバ証明書をファイル形式（PKCS#12 ファイル）でダウンロードしておきます。

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。

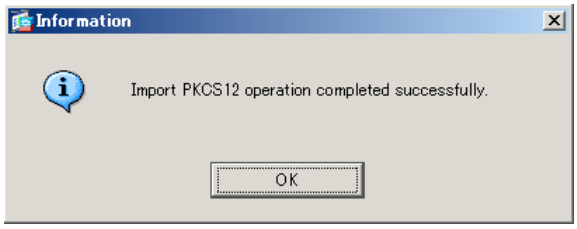


「Add Identity Certificate」ウィンドウが表示されるので、以下を設定します。

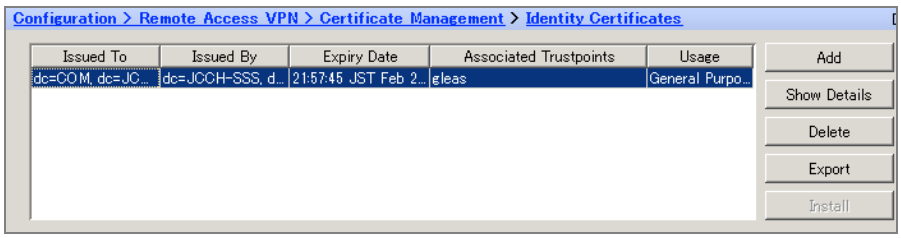
- Trustpoint Name には任意の名前を入力
- [Import the identity certificate from a file:]を選択
- [Decryption Passphrase:] には PKCS#12 ファイルのパスワードを入力
- [File to Import From:] には PKCS#12 ファイルへのパスを入力



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。

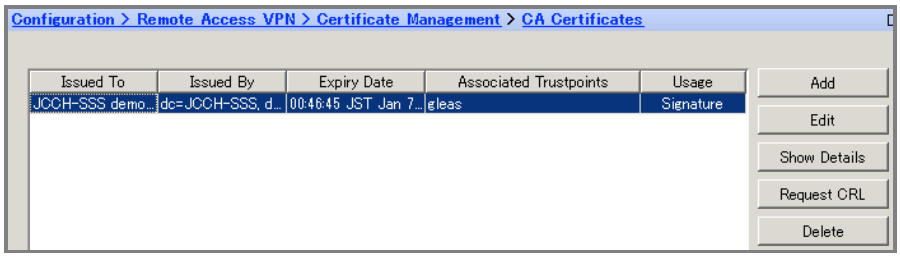


サーバ証明書が以下のように表示されます。



詳細を見る場合は[Show Details]をクリックします。

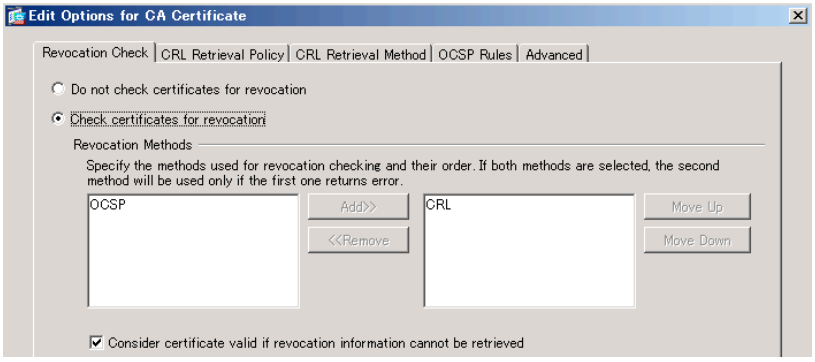
また上記操作でルート証明書も同時にインポートされています。
左側ペインより[CA Certificates]を選択すると、インポートされたルート証明書の情報を見ることができます。



詳細を見る場合は[Show Details]をクリックします。

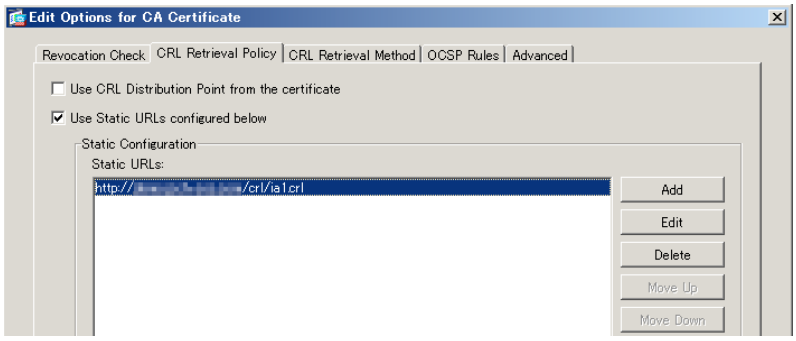
この状態で[Edit]をクリックすると、「Edit Options for CA Certificate」ウィンドウが開くの以下設定を行います。

- [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



※[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

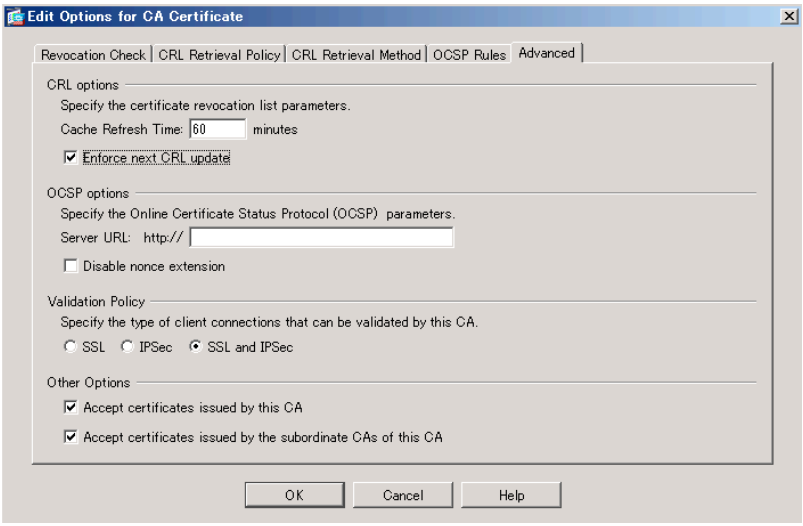
- [CRL Retrieval Policy]タブで、[Use static URLs configured below]にチェックを入れ、Static Configuration ボックスに CRL を取得する URI を設定します



※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）。

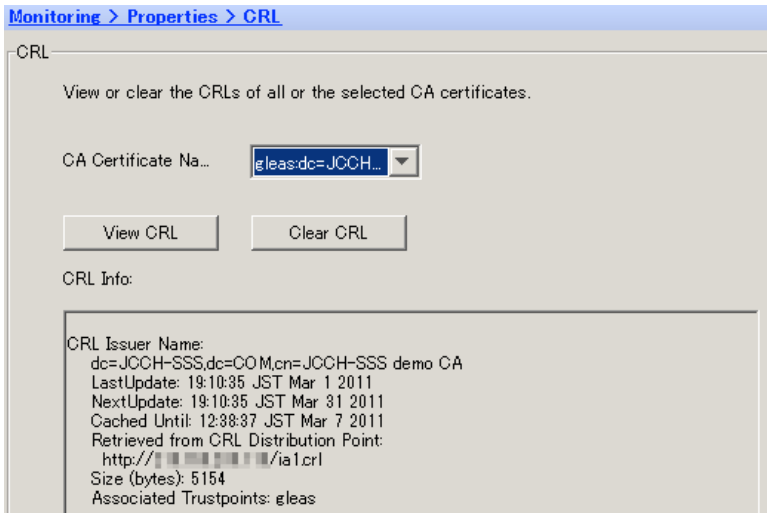


※[Enforce next CRL update]にチェックを入れると、有効期限内にある CRL かどうかをチェックします。チェックを外すと有効期限を過ぎた CRL でもキャッシュされている間は有効なものとして扱います（弊社未検証）

※[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

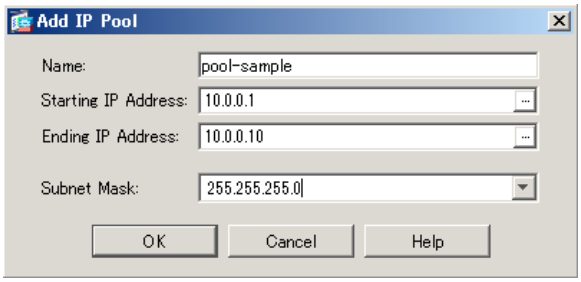
完了後、[OK]をクリックすると元の画面に戻ります。
この状態で[Request CRL]をクリックすると、ASA5500 は CRL を即時取得します。
取得時のメッセージにある通り、上部メニューより[Monitoring]をクリックし、左側ペインより[Propertied] > [CRL]をクリックすると取得した CRL の情報を見ることができます。



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。

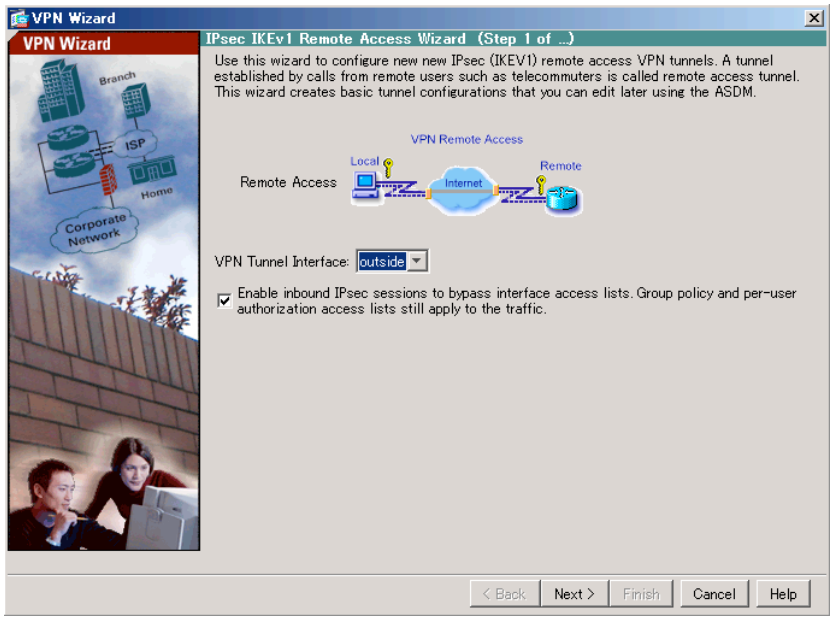


上記はVPNクライアントに対し、10.0.0.1～10/24を割り当てる例です。

2.3. IPsec の設定

ここではウィザードを利用してセットアップを行います。

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。



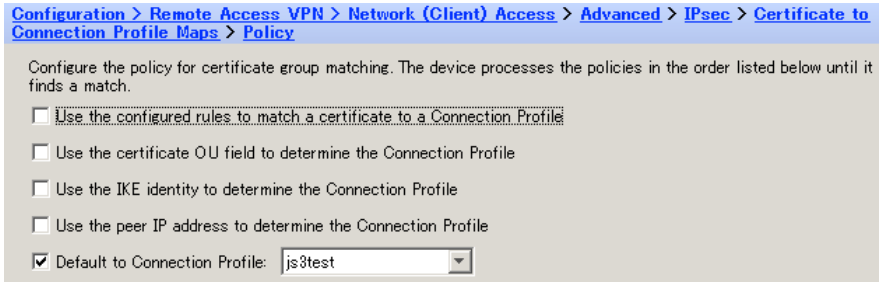
ページ	設定
IPsec IKEv1 Remote Access Wizard (Step 1 of…)	デフォルト設定のまま[Next >]をクリック
Remote Access Client (Step 2 of…)	[Cisco VPN Client, Release 3.X or Higher, or other Easy VPN Remote product]を選択し、[Next >]をクリック
VPN Client Authentication Method and Tunneling Group Name (Step 3 of…)	(1) Authentication Method で[Certificate]を選択し、[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ァ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) (Step 7 of 11)	デフォルト設定のまま[Next >]をクリック ※クライアントに設定する 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行ってください
IPsec Settng (Step 9 of 11)	デフォルト設定のまま [Next >]をクリック ※NAT 例外やスプリットトンネル、Perfect Forwarding Security (PFS)の設定は必要に応じ行ってください
Summary (Step 10 of 11)	設定内容を確認し、[Finish]をクリック

2.4. トンネルグループの割当

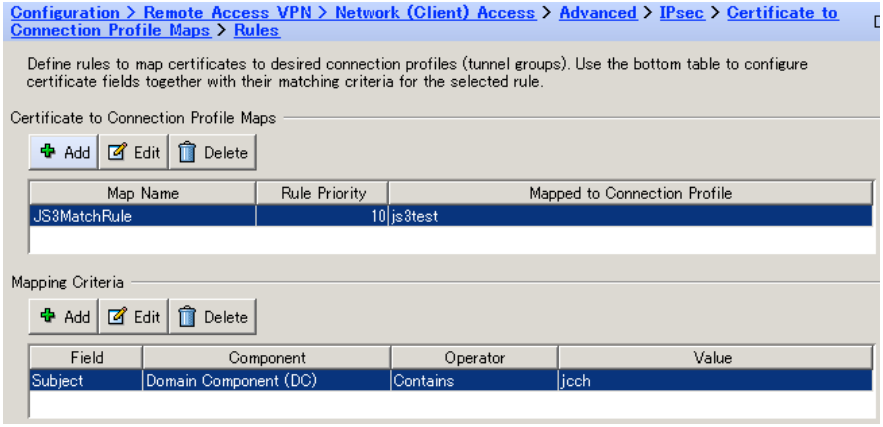
上部メニューより[Configuration]をクリックします。
左側ペインの大メニューより[Remote Access VPN]をクリックし、小メニューより[Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Policy]を展開します。

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。



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。



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含む Cisco IPsec 接続設定（構成プロファイル）を iPhone にインポートす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

※構成プロファイルでの VPN 接続設定は Gléas ではオプションとなっております。詳しくは弊社営業担当までお問い合わせください

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、iPhone用となるUA（申込局）をクリックします。

上記の場合は、iPhone用UAと記載のあるものをクリックします。

[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、構成プロファイル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iPhoneへの構成プロファイルのインストールを制限することができます。

[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。
- [iPhone用レイアウトを利用する]をチェック
- iPhone OS 3を利用しているユーザがいる場合は[ログインパスワードで証明書を保護]をチェック
  iPhone OS 3では構成プロファイルのインストール時に証明書のインポート用パスワードを求められますが、ここをチェックすることにより、UAへのログインパスワードを利用できます。
- [iPhone構成プロファイル基本設定]の各項目を入力
  ※[名前]、[識別子]は必須項目となります
  ※[削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPhoneユーザの誤操作等による構成プロファイルの削除を防止できます）

[IPsec の設定]まで移動し、以下設定を行います。

- [IPsec 接続名]には、任意の名称を入力
- [IPsec サーバホスト名]には、接続先のASA5500のホスト名（或いはIPアドレス）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。

4. iPhone での構成プロファイル・証明書のインストール

4.1. Gléas の UA からのインストール

iPhoneのブラウザ（Safari）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、その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、構成プロファイルのダウンロードを開始します。

※インポートロックを有効にしている場合は、この時点からカウントが開始されます

ダウンロードが終了すると、自動的にプロファイル画面に遷移するので、[インストール]をタップします。

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可能ですので、必要に応じ確認してください。

以下のようなルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります。

※iPhone OS 3の場合は、この前にクライアント証明書の保護パスワードを要求される画面が出現するので、UAログインに利用したパスワードを入力してください

インストール完了画面になりますので、[完了]をタップしてください。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。
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。

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]をタップ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」という表記に変わり、以後のダウンロードは一切不可能となります。

4.2. Cisco IPsec の利用

インストールした構成プロファイルにより、アクセス先ASA5500の設定や、認証に利用するクライアント証明書やユーザIDは既にiPhoneにインストールされていますので、VPNアクセスが可能となっています。

クライアント証明書によるセキュアな接続をお試しください。

構成プロファイルで設定された内容

VPN接続を行ったところ

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