



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

～Juniper MAG/SecureAccess～

iOSデバイスでのクライアント証明書による認証設定
(Junos Pulse Mobile編)

Ver.2.0

2011年11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
iOS デバイスでのクライアント証明書による認証設定 (Junos Pulse Mobile 編)

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. MAG/SA の事前設定	5
2.1. 信頼するルート認証局の設定	5
2.2. 認証サーバの設定	6
3. PULSE の設定	7
3.1. ロール (ユーザ権限) の作成	7
3.2. レルム (ユーザ認証) の作成	8
3.3. サインインポリシーの設定	10
4. GLÉAS の管理者設定 (PULSE)	11
4.1. UA (ユーザ申込局) 設定	11
5. IPHONE での構成プロファイル・証明書のインストール	13
5.1. Pulse のインストール	13
5.2. Gléas の UA からのインストール	13
5.3. Pulse の利用	16
6. 問い合わせ	17

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・iOS構成プロファイルを利用して、ジュニパーネットワークス社製SSL-VPN装置「MAG」「SecureAccess」シリーズとiOS用VPNクライアントソフトウェアである「Junos Pulse」を利用してのトンネリング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、6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。

- Juniper Networks SecureAccess DTE (バージョン7.1R3 (build 18671))
 - ※以後、「SA」と記載します
 - ※本書の内容はMAGシリーズでも適用できます
- 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
- iPhone 4 (iOS 5.0)
 - ※以後、「iPhone」と記載します
 - ※本書の内容はiPadにも適用できます
- Junos Pulse (バージョン3.0.0.14217)
 - ※以後、「Pulse」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。

- MAG/SAでのサーバ証明書設定やネットワーク設定、アクセス権限等の設定
- 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
- iOS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。

2. MAG/SAの事前設定

2.1. 信頼するルート認証局の設定

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設定します。

管理者画面左側のメニューより[Configuration] > [Certificates] > [Trusted Client CAs]と進み、右側に表示する[Import CA Certificate...]ボタンをクリックします。



[Import From:]のところで[参照]ボタンを押し、ローカルに保存してあるルート証明書を選択し、[Import Certificate]ボタンをクリックします。

成功すると以下のような画面が現れます。



失効リスト (CRL) を利用したクライアント証明書の失効確認を行う場合は、Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択してください。



ここで一度[Save Setting]をクリックして、設定を保存してください。

その後、同じ設定画面の最下部にある CRL Setting の項目で、[CRL Checking Options...]をクリックします。

CRL Checking Option の設定画面に移動しますので、以下の設定を行います。

- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 配布ポイントとなる URL を入力
※CRL 配布点が複数ある場合は、Backup CDP を設定することも可能

以下は Gléas が http で公開している CRL を取得しに行く場合の設定例となります。

CRL Distribution Points (CDP)

Use:

Specify a HTTP or LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, enter the appropriate credentials as well.

Primary CDP

CDP URL:

HTTP example:
http://server.domain.com:8339/domaincaserver.crl

LDAP example:
ldap://ldap.domain.com:6000/CN=ldap,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com?certificateRevocationList?base?objectclass=CrlDistributionPoint

Admin DN: (LDAP only)

Password: (LDAP only)

また CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定することにより可能です。

以下は CRL の有効期限に関係なく、24 時間毎に CRL を取得しに行く場合の設定例となります。

Options

CRL Download Frequency: hours (1-9999)

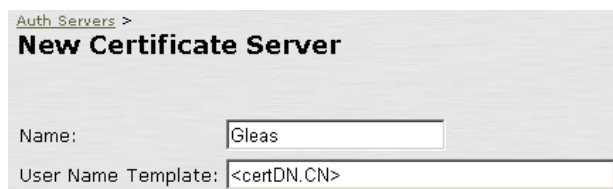
設定終了後、[Save Setting]をクリックして設定を保存してください。

2.2. 認証サーバの設定

左側のメニューから[Auth. Server]をクリックし、右側の画面の[New:]のドロップダウンより[Certificate Server]を選択し、[New Server...]をクリックします。

認証サーバの設定画面に移動するので、以下の設定を行います。

- [Name:]には、一意の認証サーバ名称を入力
- [User Name Template:]にはSAでユーザIDとするものを入力
※証明書サブジェクトCN (Common Name) を利用するケースでは、デフォルトで入っている <certDN.CN> のままにしておきます



設定終了後、[Save Change]をクリックして設定を保存してください。

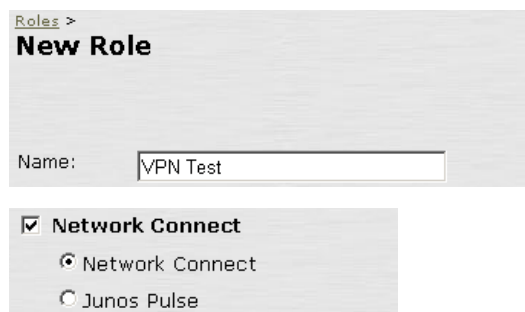
3. Pulseの設定

3.1. ロール（ユーザ権限）の作成

左側のメニューより[User Roles] > [New User Role]をクリックします。

ロールの作成画面に移動しますので、以下の設定を行います。

- [Name:]に一意のロール名称を入力
- [Access features]の欄で、[Network Connect]にチェックを入れ、[Network Connect]を選択
- 必要に応じその他の項目を設定



設定終了後、[Save Change]をクリックして設定を保存してください。

その後に表示される画面上部の[Network Connect]タブを選択し、トンネリングに関する設定を行います。

※ここではクライアントへのIPアドレス割当設定のみを記載します。その他各種設定（アクセスコントロール、接続プロファイル、スプリットトンネル、帯域幅の管理等）については説明を割愛します。ネットワーク環境やポリシーに応じて設定を行ってください

画面最下部の[Connection Profiles]リンクをクリックします。

プライベート CA Gléas ホワイトペーパー iOS デバイスでのクライアント証明書による認証設定 (Junos Pulse Mobile 編)



Network Connect Connection Profiles画面に移動します。[New Profiles]ボタンをクリックし、プロファイルの作成画面に移動しますので以下の設定を行います。

- [Name:]には、一意のルール名称を入力
- IP address assignmentの項目に、クライアントに対するIPアドレスの配布方法を選択（既存のDHCPサーバを利用か、管理者が割り当てるIPアドレスレンジを設定）
- 必要に応じその他の項目を設定

以下はクライアントに対し、10.0.0.1から10.0.0.10までのアドレスを割り当てる設定例となります。

IP address assignment

Specify how IP addresses are assigned to clients.

DHCP servers
Specify the name or IP address for up to 3 DHCP servers

DHCP options
Specify any DHCP options that should be sent to the DHCP Server. Enter the option number, option value, and option value type. Option values can be token replaced values.
Note: Please refer to Admin Guide for more details.

<input type="checkbox"/>	Option Number	Option Value	Option Type	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	String	<input type="button" value="Add"/>

IP address pool
Specify the assignable IP address ranges for this profile, one per line.
Note: Please refer to Admin Guide for details.

Examples:
10.10.1.1-10.10.5.200
10.10.10.10-100
10.10.10.50

設定終了後、[Save Change]をクリックして設定を保存してください。

3.2. レルム（ユーザ認証）の作成

左側のメニューより[User Realms] > [New User Realm]をクリックします。Realm の作成画面に移動しますので、以下の設定を行います。

- [Name:]には、一意のレルム名称を入力
- [Authentication:]には、2.2項で設定した名前ものを選択

- 必要に応じその他の項目を設定

New Authentication Realm

Name: Label to reference this realm

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

設定終了後、[Save Change]をクリックして設定を保存してください。その後、Role Mapping設定画面に移動しますので、[New Rule...]をクリックします。

Role Mapping Rule画面に移動しますので、以下の設定を行います。

- [Rule based on:]には、ドロップダウンメニューより[Username]を選択し、
※[Certificate]を選択した場合、証明書サブジェクトOU等による制御が可能
- [Name:]には、一意のルール名称を入力
- [Rule: If username...]項目にはこのルールを適用するユーザ名を入力
※ワイルドカードの利用 (*) も可能
- [...then assign these roles]項目には、3.1項で作成したルールを選択
- 必要に応じその他の項目を設定

以下は、有効なクライアント証明書が提示された場合、証明書のサブジェクトCN (2.2項でユーザIDとして設定済み) が何であろうと「VPN Test」というロールにマッピングする例です。

User Authentication Realms > VPN user >
Role Mapping Rule

Rule based on: Username [Update]

Name: VPN Rule

Rule: If username...

is * If more than one username should match, enter one username per line. You can use * wildcards.

...then assign these roles

Available Roles: Selected Roles: VPN Test

設定終了後、[Save Change]をクリックして設定を保存してください。

3.3. サインインポリシーの設定

左側のメニューから[Signing-in] > [Sign-in Policies]をクリックし、右側の画面のUser URLsの[*/] (ユーザ用のデフォルトページ) をクリックします。

その後、当該ログインページの設定画面に移動するので、[Authentication realm]の項目で以下を設定します。

- [User picks from a list of authentication realms]を選択
- [Available Realm]ボックスにある3.2で作成したレルムを、[Selected Realm]ボックスに移動

Authentication realm

Specify how to select an authentication realm when signing in.

User types the realm name
The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Available realms: Selected realms: VPN user

Move Up
Move Down

設定終了後、[Save Change]をクリックして設定を保存してください。

4. Gléasの管理者設定 (Pulse)

Gléas で、発行済みのクライアント証明書を含む Pulse 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

※Pulse 用の構成プロファイル生成機能は Gléas ではオプションとなります。詳細は弊社営業までお問い合わせください

4.1. 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。

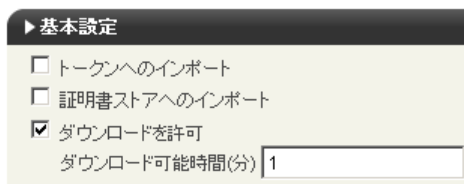


上記の場合は、iPhone用UAと記載のあるものをクリックします。

[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

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な情報を入力する画面が展開されるので、以下設

プライベート CA Gléas ホワイトペーパー
iOS デバイスでのクライアント証明書による認証設定 (Junos Pulse Mobile 編)

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)。なおここでパスワードを設定した場合でも、Pulseアプリケーション上からパスワードの入力なしに接続設定を削除することは可能なので、注意が必要です

認証デバイス情報

The screenshot shows the configuration page for iPhone/iPad settings. It includes a purple header with the title 'iPhone / iPadの設定'. Below the header, there are several sections with checkboxes and input fields:

- iPhone/iPad 用 UAを利用する
- 画面レイアウト**
- iPhone 用レイアウトを使用する
- ログインパスワードで証明書を保護
- iPhone 構成プロファイル基本設定**
- 名前(デバイス上に表示): JS3 demo profile
- 識別子(例: com.jcch-sss.profile): com.jcch-sss.demo-profile
- プロファイルの組織名: JCCH・セキュリティ・ソリューション・システムズ
- 説明: JS3 のデモ用プロファイル(Pulse)
- 削除パスワード: (empty field)

さらに[Juniper SSL-VPNの設定]項目に以下を設定します。

- [SSL-VPN接続名]に、任意の接続名を入力
- [SecureAccessホスト名]に、接続先SAのホスト名 (或いはIPアドレス) を入力
- [オンデマンド接続先]に、自動接続のトリガとなる文字列 (ドメイン名など) を入力 (任意入力項目)

The screenshot shows the configuration page for Juniper SSL-VPN settings. It includes a header with the title 'Juniper SSL-VPNの設定'. Below the header, there are three input fields:

- SSL-VPN 接続名: JS3 Remote
- SecureAccess ホスト名: (blurred)
- オンデマンド接続先: jcch-sss.local

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。

5. iPhone での構成プロファイル・証明書のインストール

5.1. Pulse のインストール

iOS デバイスで Pulse を利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールを行ってください。

本書では Pulse のインストール方法については割愛します。

5.2. 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、GléasのRAで設定したユーザ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、この時点から設定時間 (分) のカウントが開始されます

プライベート CA Gléas ホワイトペーパー
iOS デバイスでのクライアント証明書による認証設定 (Junos Pulse Mobile 編)



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、必要に応じ確認します。



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ます。

※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。

プライベート CA Gléas ホワイトペーパー
iOS デバイスでのクライアント証明書による認証設定（Junos Pulse Mobile 編）

※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ます



インストール完了画面になりますので、[完了]をタップします。



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。

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。



5.3. Pulse 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SAの設定や、認証に利用するクライアント証明書は既にiPhoneにインストールされていますので、Pulseアプリケーションによるアクセスが可能となっています。

※インポートした内容がPulseに反映されていない場合は、Pulseを再起動します



構成プロファイルによって設定されたPulseの接続設定は以下のようになっています。



6. 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。

■MAG/SAに関するお問い合わせ先

ジュニパーネットワークス株式会社

URL : otoiawase@juniper.net

■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