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

SonicWALL （Aventail）でのSSL-VPNにおける

クライアント証明書認証設定

Ver.1.0

2015 年 4 月

目次

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、デル株式会社（デルソニックウォール）のDell Sonicwall AventailでSSL-VPN接続時における認証をおこな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、最終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。

- SSL-VPN装置： Dell Sonicwall Aventail E-Class SRA EX6000（バージョン10.7.1-237）
  ※以後、「Aventail」と記載します
- ドメインコントローラ：Microsoft Windows Server 2012 R2 Standard
  ※以後、「ドメインコントローラ」と記載します
- JS3 プライベートCA Gléas （バージョン1.12）
  ※以後、「Gléas」と記載します
- クライアント（PC）： Microsoft Windows8.1 Pro / Aventail Connect with Smart Tunneling 10.7.1.237
  ※以後、「PC」と記載します
- クライアント（iOS）： iPad（第三世代、iOS 7.1.2）/ SonicWALL Mobile Connect 3.0.10
  ※以後、「iPad」と記載します
- クライアント（Android）: Nexus 7 （2013、Android 4.4.4）/ SonicWALL Mobile Connect 3.1.5
  ※以後、「Android」と記載します

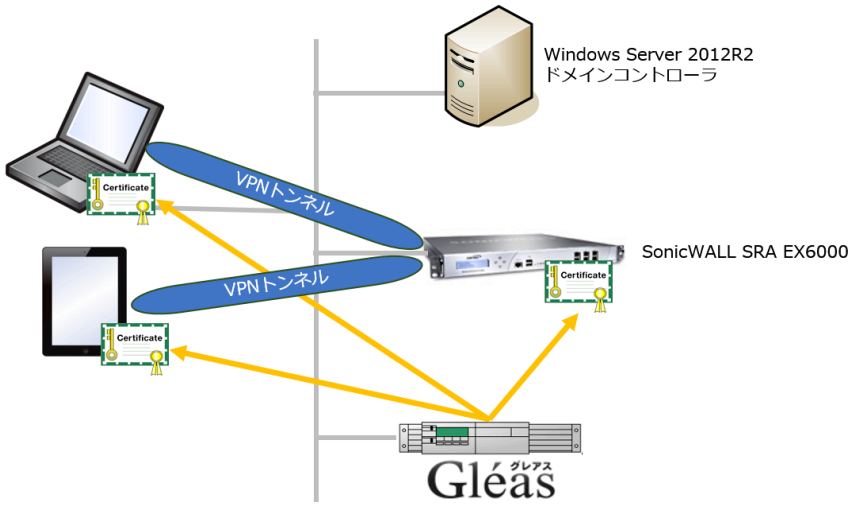
以下については、本書では説明を割愛します。

- Windows ServerやWindowsドメインのセットアップ
- Aventailのネットワーク設定や、SSL-VPN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
- PC・iPad・Androidでのネットワーク設定等の基本設定、クライアントソフトウェアの利用方法

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。



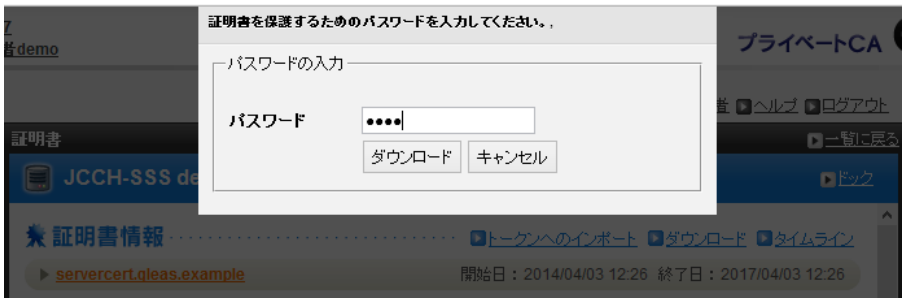
1. Gléasでは、Aventailにサーバ証明書を、PC・iPad・Androidにクライアント証明書を発行する
2. Aventailの認証設定はクライアント証明書と、WindowsドメインのID/パスワードを用いる二因子認証とする

2. Aventailの設定

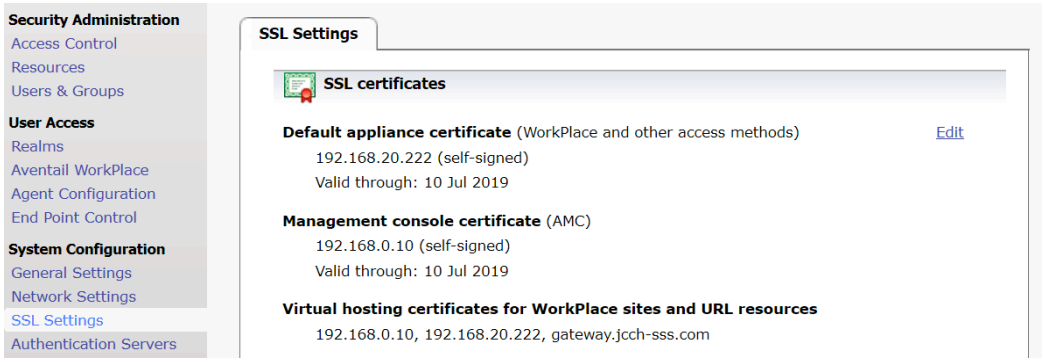
2.1. SSL サーバ証明書のインポート

本手順開始前に、Gléas の管理者画面よりサーバ証明書ファイル（PKCS#12 ファイル）をダウンロードします。
ダウンロードする際に保護パスワードの入力を求められますが、Aventail にインポ

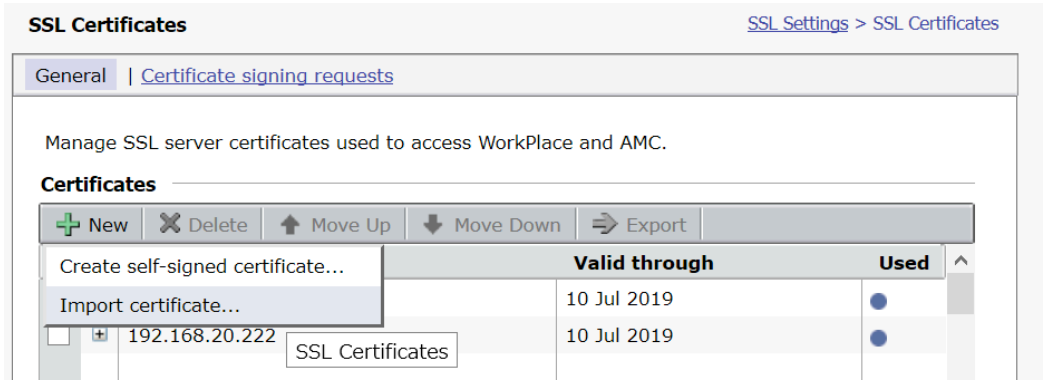
ートする際にこのパスワードが必要となります。



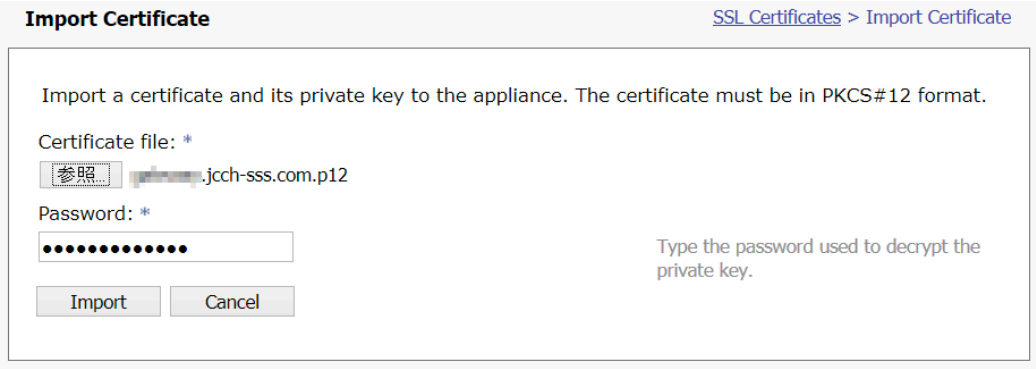
AMC（Aventail 管理コンソール）にログインし、左側メニューSystem Configuratio から[SSL Settings]をクリックします。
中央ペインの Default appliance certificate の右にある[Edit]をクリックします。



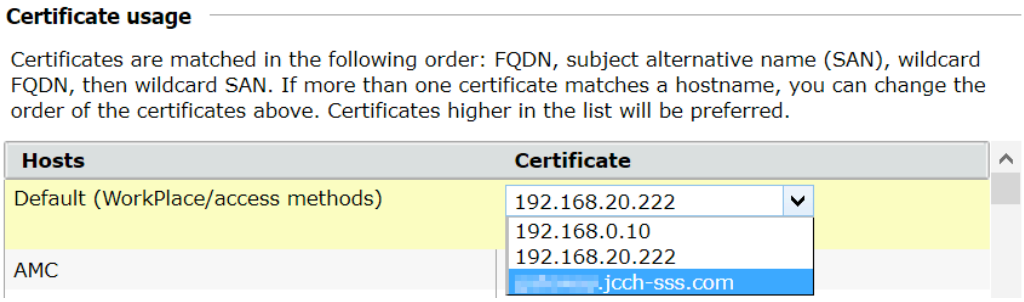
次の画面では[＋New]をクリックし、[Import certificate…]を選びます。
※[Certificate signing requests]を選択し証明書署名リクエスト（CSR）を作成し、Gléas にて証明書発行を行うことも可能です



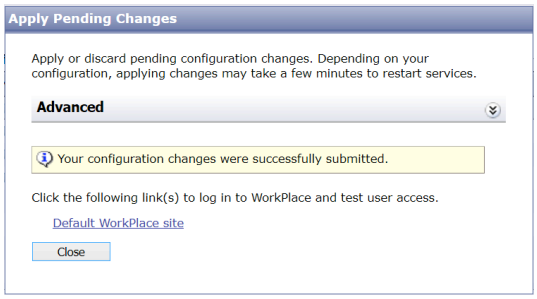
先ほどダウンロードしたファイルの指定及び、保護パスワードを入力します。



もとの画面に戻りインポートした証明書が追加されるので、Certificate Usage に移動し対象のワークプレイスのサーバ証明書をインポートしたものに変更します。



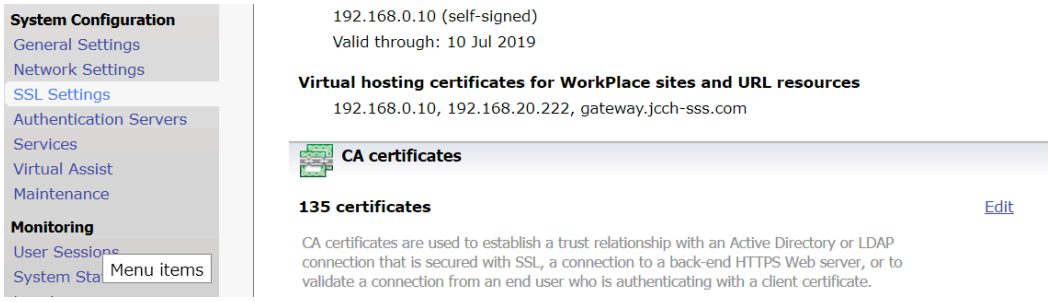
右上の[Pending changes]をクリックすると変更が反映され、対象のワークプレイスにアクセスするとサーバ証明書が変更されていることが確認できます。



2.2. ルート証明書のインポート

本手順前に、Gléas の管理者画面（RA）よりルート証明書をダウンロードします。
※デフォルトのルート証明書は以下 URL よりダウンロード可能です。
http://hostname/crl/ia1.pem

AMC の左側メニューSystem Configuration から[SSL Settings]をクリックし、中峰ペインの CA Certificates の[Edit]をクリックします。



次の画面では[＋New]をクリックし、ダウンロードしたルート証明書をアップロードします。

もとの画面に戻るので、インポートしたルート証明書をクリックします。

Certificate revocation checking で失効確認関連の設定をおこないます。

- [Use Certificate Revocation List (CRL)]にチェック
- [Use this certificate distribution point (CDP)]にチェック

※上記 certificate は、crl の誤りと思われます

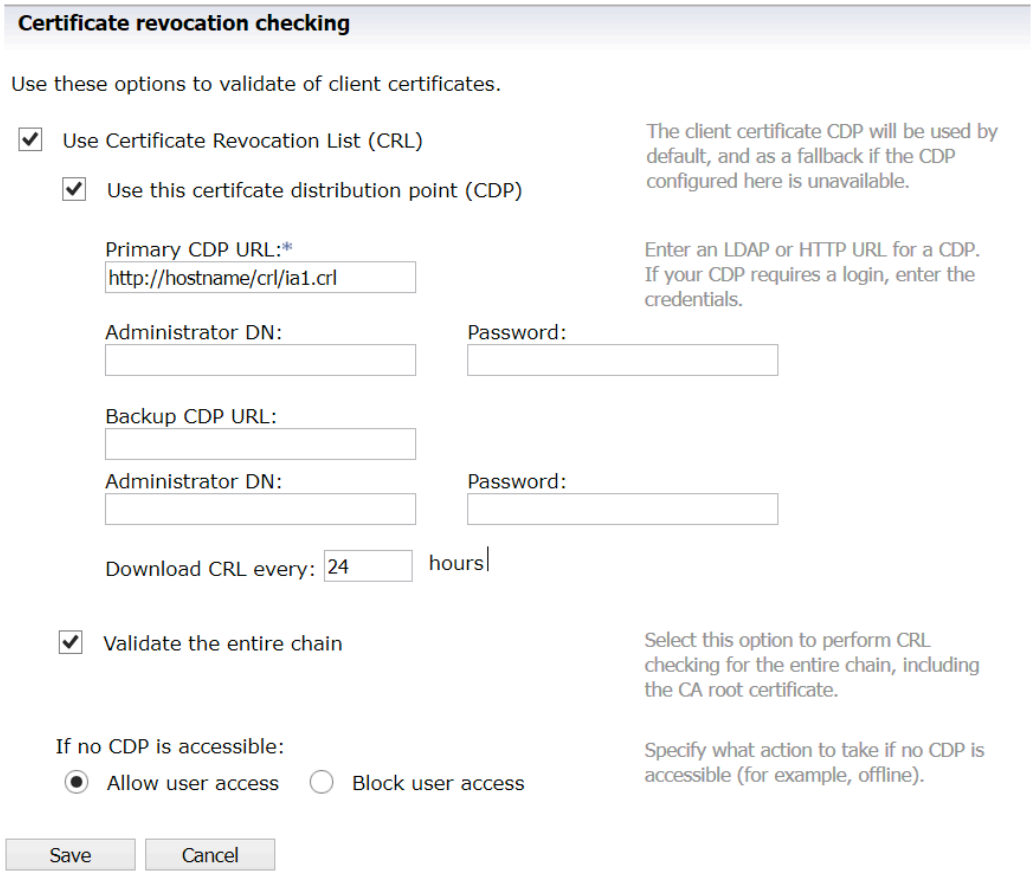
- Primary CDP URL には、CRL 配布ポイントを入力

  ※Gléas のデフォルトの CRL 配布ポイントは以下の通りです

  http://hostname/crl/ia1.crl

  複数の CRL 配布ポイントや、LDAP で CRL を公開しているケースでは Aventail が CRL を入手できるよう適切な設定をおこないます
- Download CRL every: ☐ hours には、失効リストの取得間隔を指定
- If no CDP is accessible には、指定した CDP にアクセスできず失効リストが取得できない場合の認証可否を指定

設定が終わったら、[Save]をクリックして設定を保存します。



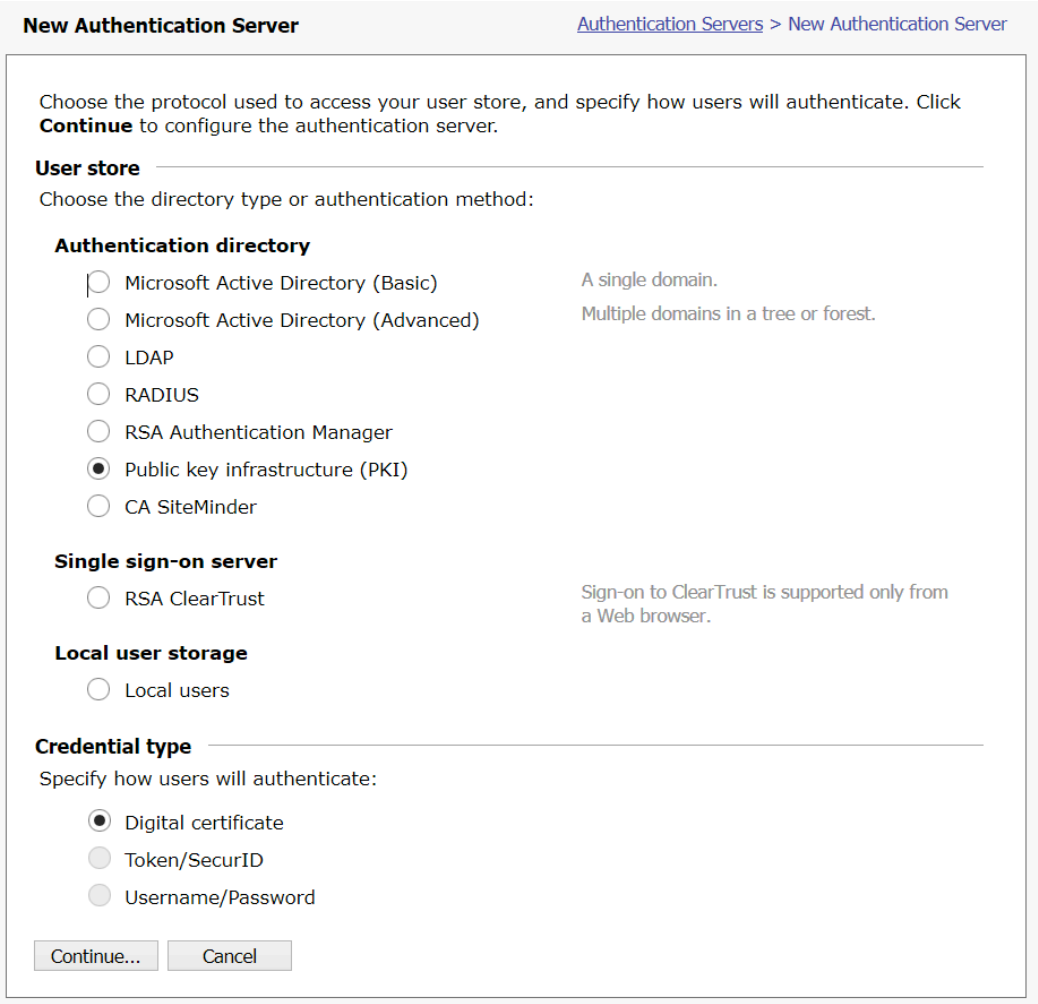
2.3. 認証サーバの設定

左メニューの System Configuration より[Authentication Servers]をクリックし、中央ペインの Authentication Servers の[New…]をクリックします。

以下の通り指定します。

- Authentication Directory では、[Public key infrastructure (PKI)]を選択
- Credential Type では、[Digital Certificate]を選択

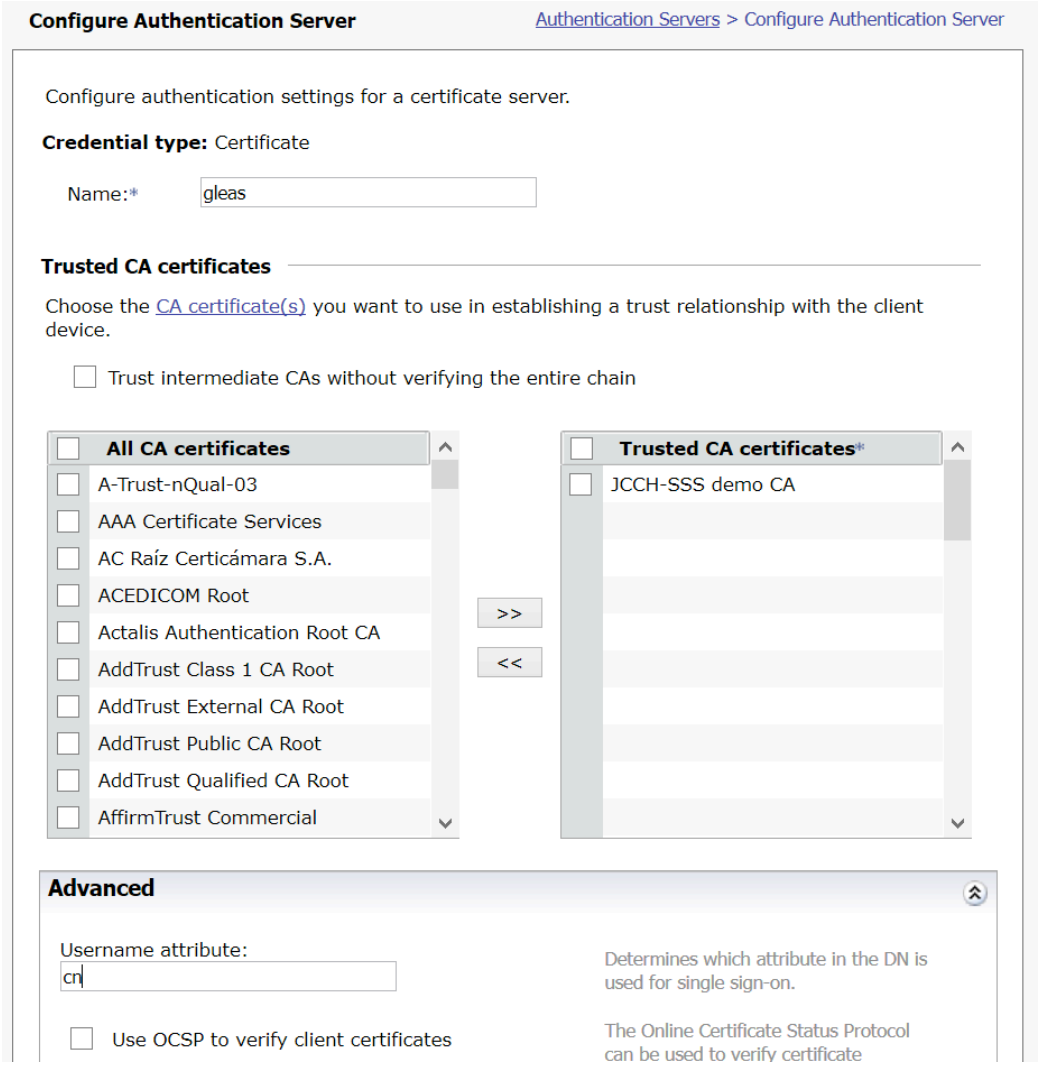
[Continue]をクリックします。



次の画面では以下を設定します。

- Name には、任意の認証サーバ名称を入力
- Trusted CA certificates には、先ほどインポートしたルート証明書を指定
- Advanced を展開し Username Attribute:に[cn]を指定すると、Gléas のアカウント名を Aventail のログインユーザとして扱うことが可能になります

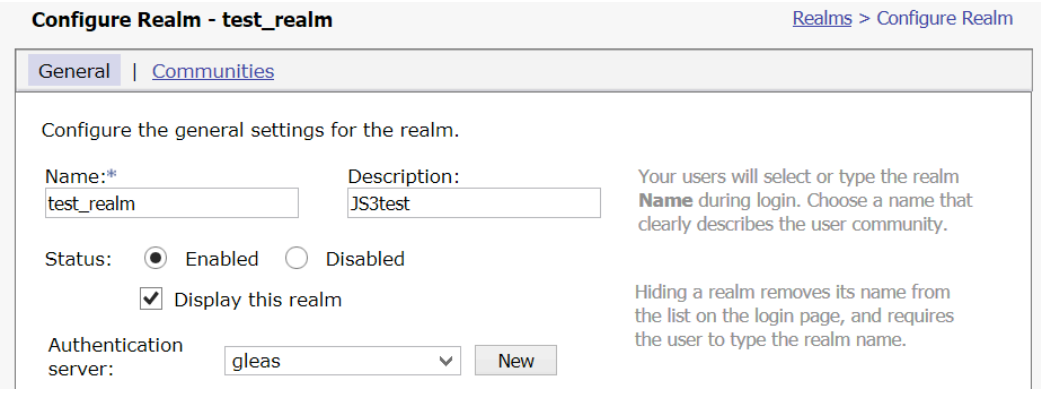
※ Aventail では失効確認手段として OCSP をサポートしています。今回弊社では OCSP の検証をしておりませんが、利用を希望される場合は弊社までお問い合わせください。



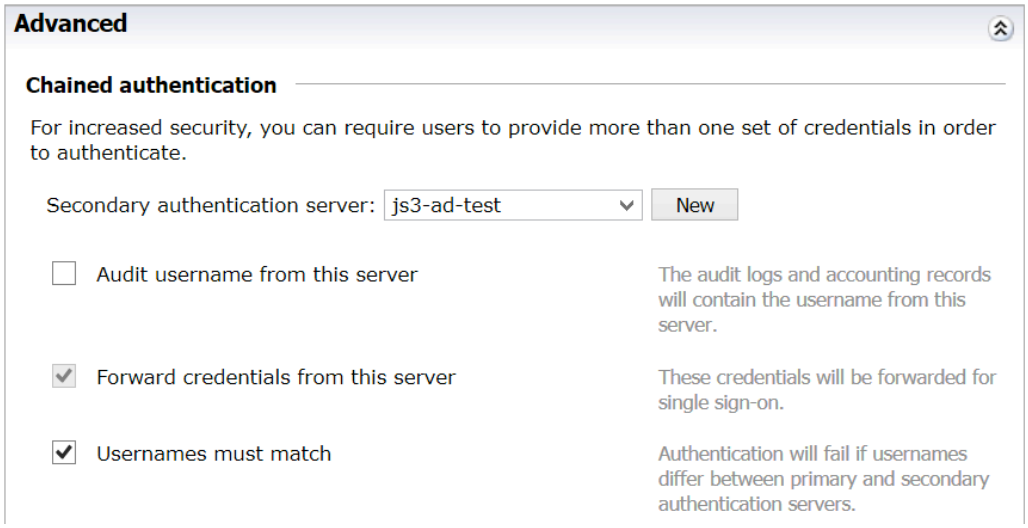
同じメニューで Active Directory の認証サーバ設定もおこないますが、本書では詳細説明を割愛します。

2.4. レルムへのマッピング

左メニューの User Access より[Realm]をクリックし、認証設定を適用するレルムをクリックします。（あるいは新規にレルムを作成します）
Authentication Server に 2.3 項で設定した認証サーバを指定します。

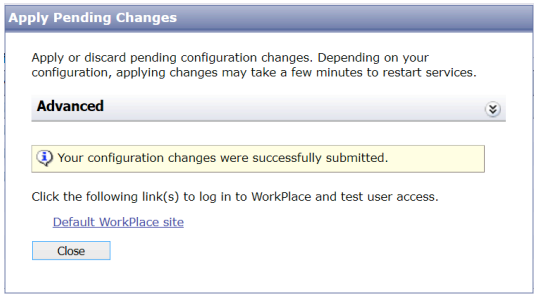


Advanced を展開し、Second authentication server: に Active Directory の設定をおこなった認証サーバを指定します。
[Usernames must match]にチェックをいれると、Gléas のアカウント名（クライアント証明書のサブジェクト cn 値）と、ログインユーザ名の一致を確認するようにできます(2.3 項の通り Username Attribute に cn を設定しておく必要があります)。



保存すると、以下のようなレルムが表示されます。

右上の[Pending changes]をクリックして、設定変更を反映します。



3. Gléasの管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をiPadにインポートできるよう設定します。

※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、設定を行う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。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

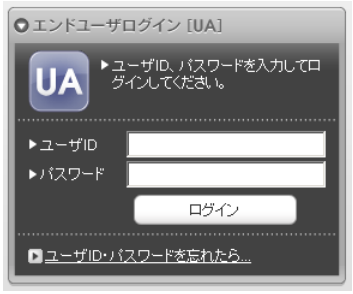
設定終了後、[保存]をクリックし設定を保存します。

各項目の入力が終わったら、 [保存]をクリックします。

4. PC からの接続操作

4.1. クライアント証明書のインポート

Internet Explorer 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ます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

4.2. Aventail へのアクセス（Aventail Connect）

クライアントソフトAventail Connectで接続すると、4.1項でインポートした証明書が選択可能になっていますので、選択して[接続(C)]をクリックします。

ActiveDirectoryによるパスワード認証を経てVPN接続が確立されます。
（Gléasのアカウントと同一のユーザ名を入力しないとエラーになります）

証明書がない状態でアクセスすると、証明書を選択することができず先に進むことができません。

失効された証明書でアクセスすると、以下の通りエラーとなります。

5. Gléasの管理者設定（iPad）

GléasのUA（申込局）より発行済み証明書をiPadにインポートできるよう設定します。

※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

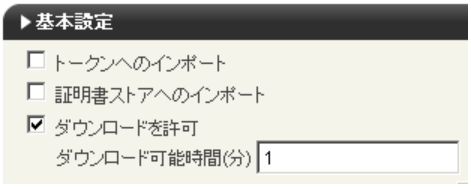
5.1. UA（ユーザ申込局）設定

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、設定を行う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
  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。

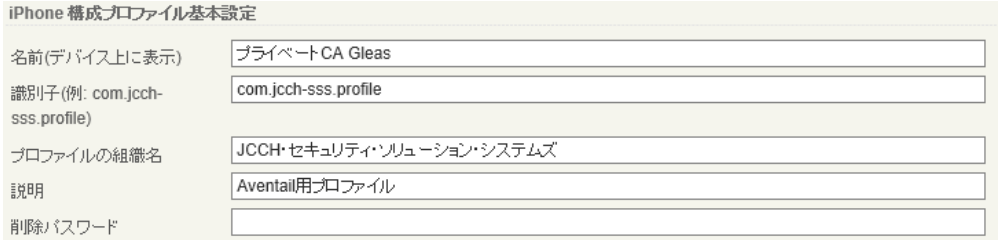
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

iPhone構成プロファイル基本設定

- [名前]、[識別子]、[プロファイルの組織名]に任意の文字を入力（必須項目）
- [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）



設定が終わったら、 [保存]をクリックします。

5. iPad からの接続操作

5.1. 構成プロファイルのインストール

iPad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、[構成プロファイルのダウンロード]をタップし、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

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。

インストール途中に、以下のような確認画面が現れますので、その説明内容を確認したうえで[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Gléasのルート認証局証明書になります。

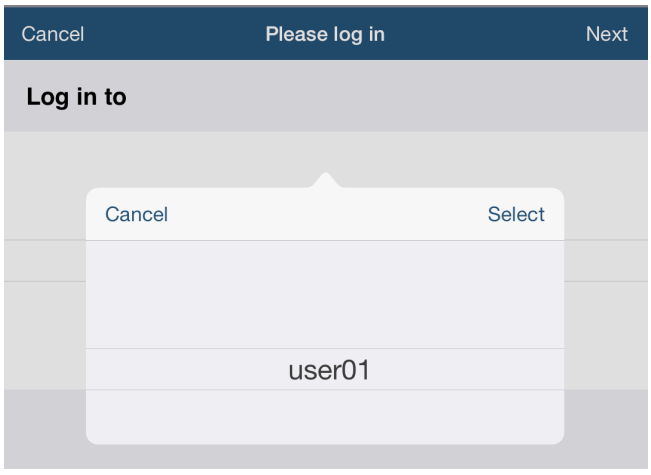
インストール完了と表示されたら[完了]をタップします。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。
以上で、iPadでの構成プロファイルのインストールは終了です。

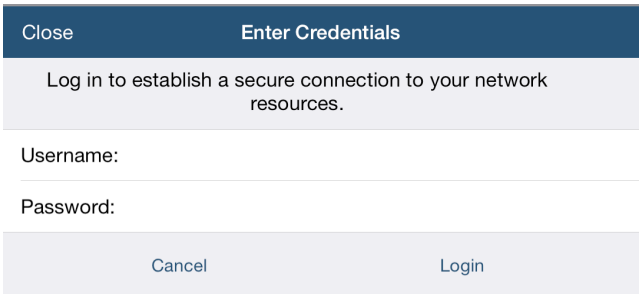
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可能となります。

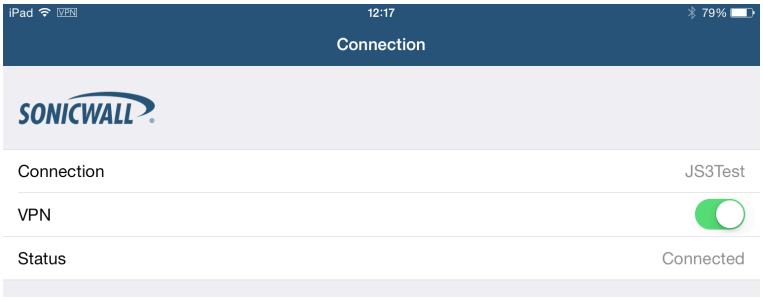
5.2. Aventail へのアクセス

クライアントアプリMobile ConnectでAventailに接続します。
レルムを選択したのちに以下の画面が出現するので、5.1項でインポートした証明書であることを確認し、[Select]をタップします。

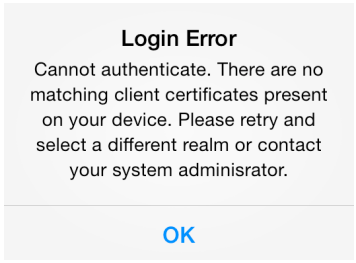


ActiveDirectoryによるパスワード認証を経てVPN接続が確立されます。
（Gléasのアカウントと同一のユーザ名を入力しないとエラーになります）
Statusの欄がConnectedになり、右上に VPN と表示されます。

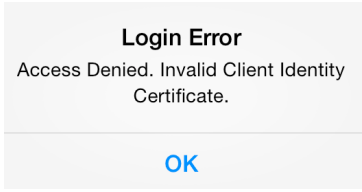




証明書がない状態でアクセスすると、以下のエラーとなります。

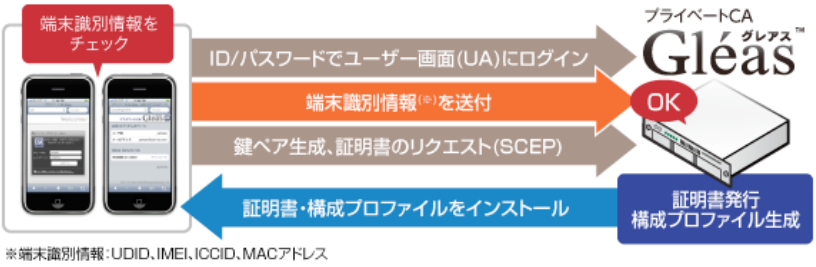


失効された証明書でアクセスすると、以下の通りエラーとなります。



5.3. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air（OTA）エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。
OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。



詳細は最終項のお問い合わせ先までお問い合わせください。

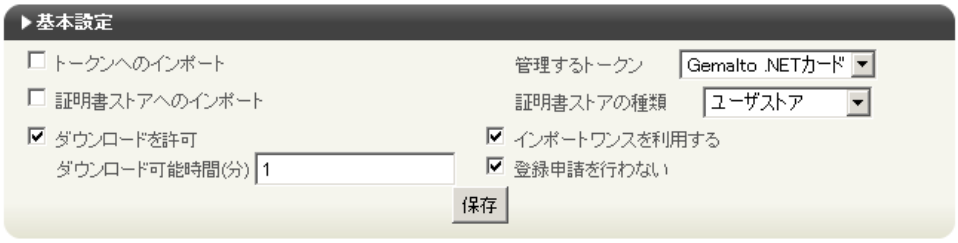
6. Gléas の管理者操作（Android）

6.1. 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。

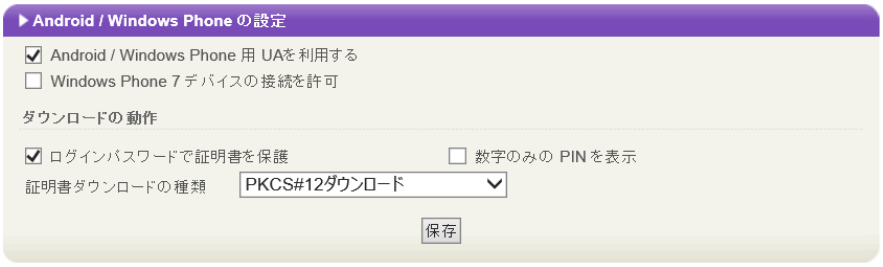
- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定
  [インポートワンスを利用する]にチェックを入れてこの設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、証明書のダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のAndroidへの証明書のインストールを制限することができます。



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 / Windows Phone の設定]までスクロールし、[Android / Windows Phone 用 UAを 利用する]をチェックし、以下の操作をおこないます。

- [ログインパスワードで証明書を保護]にチェック
- [証明書ダウンロードの種類]：[PKCS#12ダウンロード]を選択



以上でGléasの設定は完了です。

7. Android からの接続操作

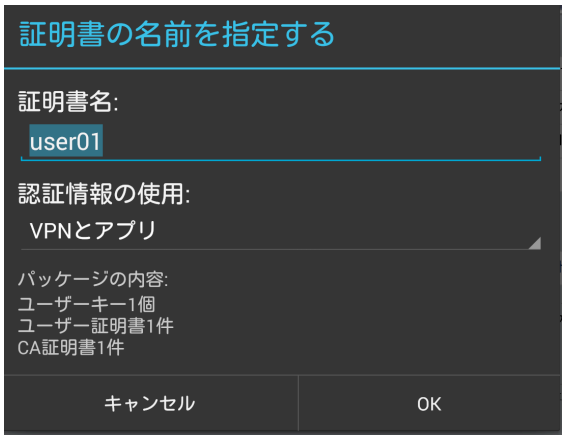
7.1. Gléas の UA からの証明書インポート

Chrome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。

証明書の保護パスワードの入力を促されるので、ログインパスワードと同じものを入力します。

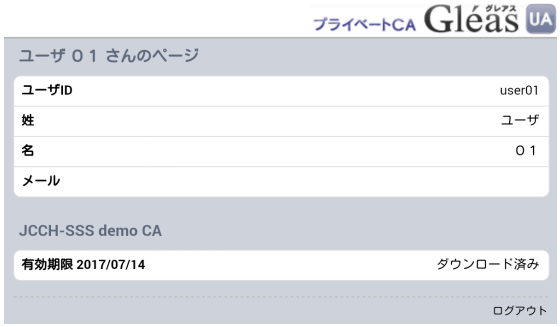
「証明書名」は、Gléasのアカウント名が入っています。
「認証情報の使用」は、[VPNとアプリ]を選択し、[OK]をタップします。



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。

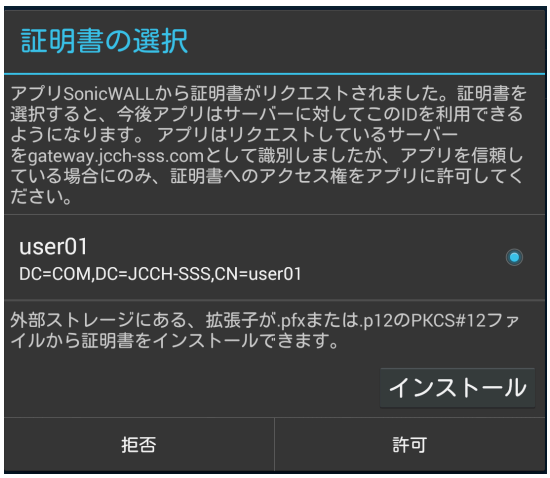
終了後、[ログアウト]をタップしてUAからログアウトします。
以上で、Androidでの証明書インポートは終了です。

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。

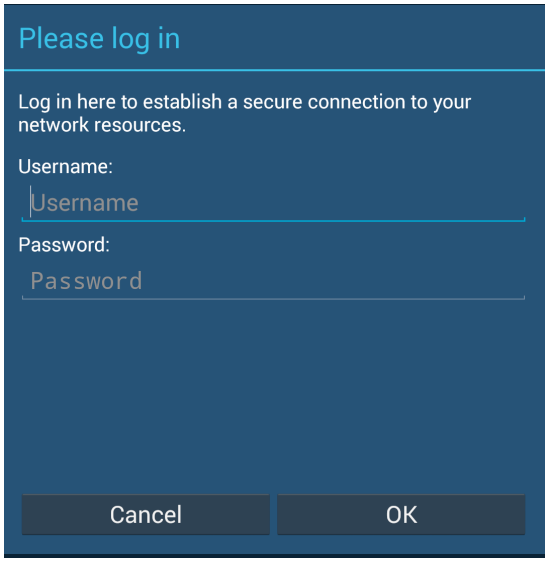


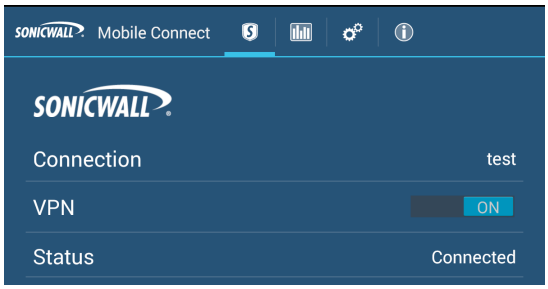
7.2. Aventail へのアクセス

クライアントアプリMobile ConnectでAventailに接続します。
レルムを選択したのちに以下の画面が出現するので、7.1項でインポートした証明書であることを確認し、[Select]をタップします。

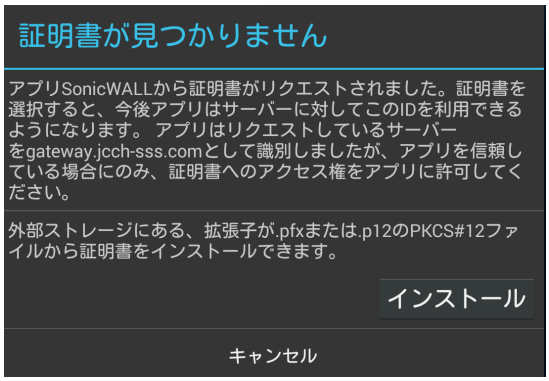


ActiveDirectoryによるパスワード認証を経てVPN接続が確立されます。
（Gléasのアカウントと同一のユーザ名を入力しないとエラーになります）
Statusの欄がConnectedになり、画面左上に鍵マークが表示されます。

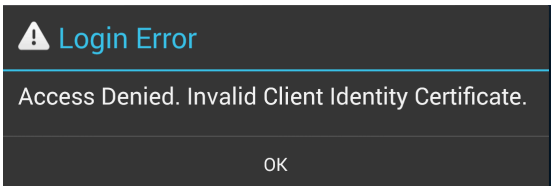




証明書がない状態でアクセスすると、以下のエラーとなります。



失効された証明書でアクセスすると、以下の通りエラーとなります。



8. 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

■Aventail製品に関するお問い合わせ

デル・ソフトウェア株式会社　セキュリティ事業本部

Mail:　Japan_sales@sonicwall.com