



iPhone と VPN



VPN プロトコル

- Cisco IPsec
- L2TP/IPsec
- PPTP

認証方式

- パスワード(MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- 証明書 (PKCS1, PKCS12)
- 秘密共有

iPhoneなら現在最も使用されている技術標準VPNプロトコルを使用して企業のプライベートネットワークに安全性の高いアクセスをすることが可能です。iPhone 2.0ソフトウェアは、IPsecによるCiscoIPSecやL2TP、およびPPTPをサポートしています。御社の装備に使用されているプロトコルがこれら3つのうちのいずれかであれば、iPhoneとVPNとを接続するにあたり、ネットワーク設定の変更をしたり他のアプリケーションを追加したりする必要は一切ありません。

CiscoIPSecが装備されていれば、技術標準規格x.509に基づくデジタル証明書(PKCS1, PKCS12)による認証が可能になるというメリットがあります。2因子トークンによる認証を実現するため、iPhoneはRSA SecurIDとCRYPTOCARDの両方をサポートしています。ユーザは、PINとトークンから生成された使い捨てパスワードとをiPhoneに入力して、VPNとの接続を確立します。

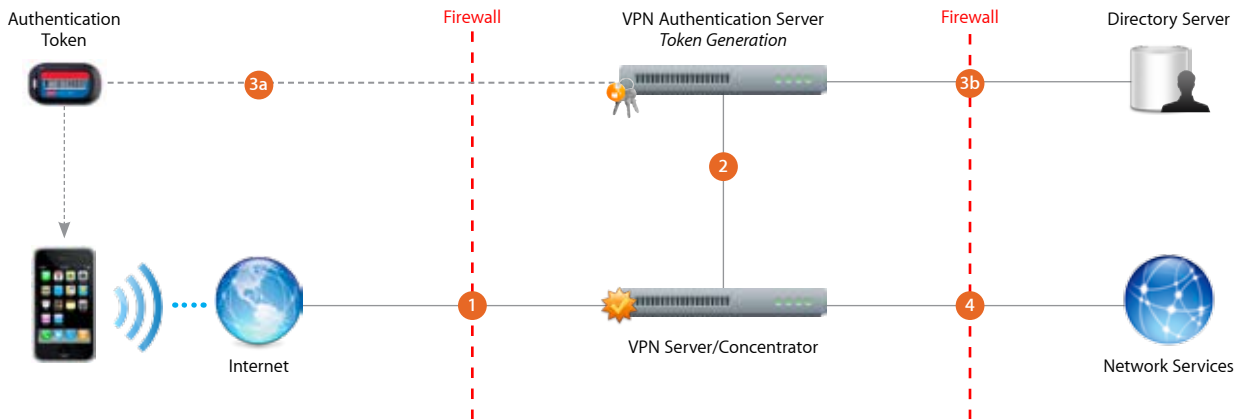
iPhoneは、IPsec規格のCiscoIPSecおよびL2TPによる秘密共有認証方式をサポートしています。また、iPhoneは、最もベーシックなユーザネームとパスワードによる認証を行うためのMS-CHAPv2もサポートしています。認証方式に関係なく、あらかじめVPNに指定されている設定は、iPhoneの設定プロフィールまたはダイレクトリ入力によってユーザに分配されます。

VPN 設定

- iPhoneは現在最も使われているVPNネットワークと一体化されているので、最低限の設定をするだけでiPhoneからネットワークへのアクセスが可能です。装備導入にあたりまず必要なことは、iPhoneがVPNのプロトコルおよび認証方式に対応しているかを確認することです。
- 御社のVPN コンソントレーターと既存標準の適応性を確認します。また、RADIUS及びVPN認証サーバまでの認証パスをチェックして、iPhoneにサポートされている標準が既存のシステムで有効かどうかを確認することを推奨します。
- 証明書による認証方式を利用する場合は、デバイスをサポートすると同時に、公開鍵インフラが鍵供給プロセスによるユーザ証明書に対応する形で設定されていることを確認します。
- 証明書形式および認証サーバとの適合性を検証します。iPhoneはPKCS1 (.cer, .crt, .der) とPKCS12 (.p12, .pfx) をサポートしています。
- 御社のソリューションプロバイダに対して、ソフトウェアおよび装備に最新のセキュリティパッチやファームウェアがアップデートされているかを確認します。
- Cisco IPsecのプロトコルおよび仕様に関する詳細情報はこちらをご覧ください：www.cisco.com

VPN 展開シナリオ

この例は、典型的なVPNのサーバやコンセントレーターおよび企業ネットワークサービスへのアクセスを制御するVPN認証サーバの展開を表示しています。



- 1 iPhoneからネットワークサービスへのアクセスを要求してきます(通常はPPP接続を介して)。
- 2 要求を受け取ったVPNサーバやコンセントレーターは、これを認証サーバに伝達します。
- 3a 2因子トークン環境にある認証サーバでは、鍵サーバと同期されたトークン鍵が生成されます。証明書やパスワード方式が使用されている場合は、ユーザのバリデーションに基づいて認証作業が行われます。
- 3b ユーザの認証が完了すると、認証サーバはグループネットワーク アクセス ポリシーにおけるユーザの正当性を認証します。
- 4 ユーザとグループポリシーの適合性が立証されるとVPNサーバはユーザに対してネットワークサービスに通じるトンネル経由の暗号化されたアクセス(通常、IPSecを介して)を供給します。