



iPhone と iPad の配備 仮想プライベートネットワーク



iPhone や iPad では、業界標準の仮想プライベートネットワーク (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にアクセスできます。iOS に内蔵されている VPN クライアントが、Juniper、Cisco、F5 Networks、SonicWALL、Aruba Networks などの他社製アプリケーションを使えば、エンタープライズシステムへの接続も簡単です。

iOS はあらかじめ、Cisco IPsec、L2TP over IPsec、PPTP に対応しています。会社がこのいずれかのプロトコルに対応していれば、特別なネットワーク構成や他社製アプリケーションを用意しなくても、iPhone や iPad から VPN に接続できます。

また、iOS は SSL VPN にも対応するため、Juniper SA シリーズ、Cisco ASA、F5 BIG-IP Edge Gateway SSL VPN サーバへのアクセスも可能となります。Juniper、Cisco、F5 製の VPN クライアントアプリケーションを App Store からダウンロードするだけで、すぐに使い始めることができます。iOS が対応しているほかの VPN プロトコルと同様、SSL VPN の構成には、デバイス上で手動で行う方法と、構成プロファイルを使用する方法があります。

iOS は、IPv6、プロキシサーバ、スプリットトンネリングなどの業界標準のテクノロジーに対応しているため、企業のネットワークに接続する際に VPN の機能を存分に活かすことができます。また、iOS はパスワード、二要素トークン、デジタル証明書など、様々な認証方式に対応します。証明書ベースの認証が使用されている環境で効率的に接続できるよう、iOS には VPN オンデマンド機能が用意されています。この機能により、指定したドメインに接続する際に VPN セッションが自動的に開始されます。

対応しているプロトコルと認証方式

SSL VPN

パスワード、二要素トークン、証明書によるユーザ認証に対応しています。

Cisco IPsec

パスワードと二要素トークンによるユーザ認証、および共有シークレットと証明書によるコンピュータ認証に対応しています。

L2TP over IPsec

MS-CHAP v2 パスワードと二要素トークンによるユーザ認証、および共有シークレットによるコンピュータ認証に対応しています。

PPTP

MS-CHAP v2 パスワードおよび二要素トークンによるユーザ認証に対応しています。

VPN オンデマンド

iOS には、証明書ベースの認証を使用した構成のための、VPN オンデマンド機能が用意されています。VPN オンデマンド機能を使えば、事前に定義されているドメインにアクセスする際に、自動的に接続が確立されるため、ユーザに意識させることなく VPN 接続を行うことができます。

これは iOS の機能の一部なので、特別なサーバ構成は不要です。VPN オンデマンドの構成は、構成プロファイルを使って行うことも、デバイス上で手動で行うこともできます。

VPN オンデマンド機能のオプションは次のとおりです。

常に確立

指定されたドメインと一致するアドレスに対して接続する際に、VPN 接続を開始します。

確立しない

指定されたドメインと一致するアドレスがあっても VPN 接続は開始しません。ただし、すでにアクティブになっている VPN 接続がある場合は、その接続を使用できます。

必要に応じて確立

DNS ルックアップが失敗した場合にのみ、指定されたドメインと一致するアドレスに対して接続する際に、VPN 接続を開始します。

VPN 設定

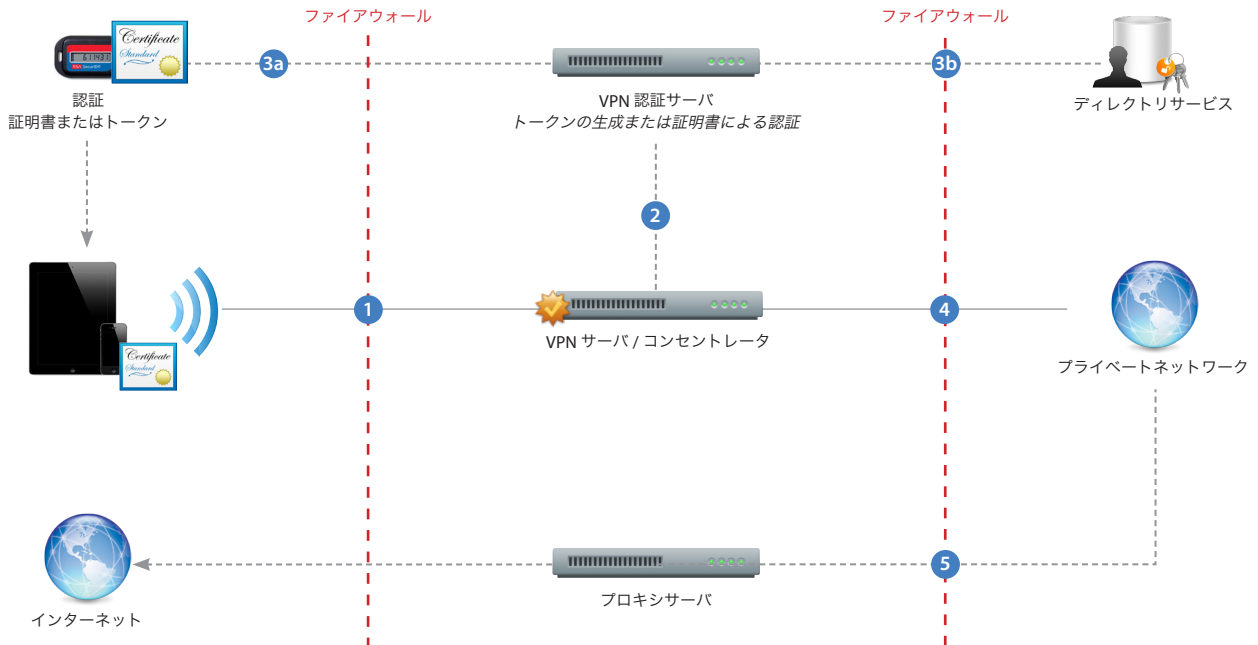
- iOS は既存の多くの VPN ネットワークと互換性があり、構成は最小限で済みます。配備の準備をする際には、企業の既存の VPN プロトコルと認証方式に iOS が対応しているかどうかを確認することをお勧めします。
- iOS が対応している規格が、実際の環境で有効になっていることを確認するために、認証サーバへの認証経路を確認することをお勧めします。
- 証明書ベースの認証を計画している場合は、公開鍵インフラストラクチャをその鍵配布プロセスでデバイスベースおよびユーザベースの証明書をサポートするように構成されていることを確認します。
- URL 固有のプロキシ設定を構成するには、PAC ファイルを基本 VPN 設定でアクセスできるウェブサーバ上に置いて、MIME タイプを `application/x-ns-proxy-autoconfig` に指定します。

プロキシ設定

すべての構成に対して単一の VPN プロキシを指定することもできます。すべての接続に単一のプロキシを構成するには、「手動」設定を使用し、必要に応じてアドレス、ポート、認証方法を指定します。PAC または WPAD を使用して自動プロキシ構成ファイルを指定するには、「自動」設定を使用します。PACS の場合は、PACS ファイルの URL を指定します。WPAD の場合は、iPhone や iPad が DHCP および DNS に適切な設定を照会します。

配備シナリオ

VPN サーバまたはコンセントレータと、企業のネットワークサービスへのアクセスを制御する認証サーバを含む典型的な構成例を示します。



- 1 iPhone や iPad は、ネットワークサービスへのアクセスをリクエストします。
- 2 VPN サーバまたはコンセントレータは、受信したリクエストを認証サーバに渡します。
- 3 二要素トークンの環境では、認証サーバは、キーサーバによって時刻同期されたトークンキー発行を管理します。証明書による認証方式を採用している場合、認証に先立って固有名証明書をインストールしておく必要があります。パスワード方式が採用されている場合、ユーザの確認を経て認証プロセスが続行されます。
- 4 ユーザが認証されたら、認証サーバは、ユーザとグループのポリシーを検証します。
- 5 ユーザとグループのポリシーの検証が完了すると、VPN サーバにより、トンネリングおよび暗号化されたネットワークサービスへのアクセスが提供されます。
- 6 プロキシサーバを使用している場合、iPhone や iPad はプロキシサーバにアクセスすることによりファイアウォールの外の情報にアクセスします。