Apple iOS 用 Cisco AnyConnect セキュア モビリティ クライアント ユーザ ガイド（リリース 4.0.x）

AnyConnect ユーザ ガイド 2

AnyConnect のインストールおよび起動 2

VPN 接続の設定 5

VPN 接続の確立 16

AnyConnect 通知への応答 16

AnyConnect の設定と管理（オプション） 17

AnyConnect のモニタリングとトラブルシューティング 22

Revised: October 10, 2016,

AnyConnect ユーザ ガイド

AnyConnect のインストールおよび起動

AnyConnect の概要

Apple iOS 用 Cisco AnyConnect セキュア モビリティ クライアントは、企業ネットワークへのシームレスかつセキュアなリモートアクセスを実現します。AnyConnect を使用すると、インストールされているアプリケーションで、企業ネットワークに直接接続されているかのように通信できます。AnyConnect は高度なネットワーキング アプリケーションであり、プリファレンスを設定したり、AnyConnect の動作を制御したり、デバイスで管理者が推奨する診断ツールや診断機能を使用したりすることも可能です。

企業で AnyConnect をモバイル デバイス管理ソフトウェアと組み合わせて使用する場合があります。その場合、デバイス管理ルールに、VPN アクセス許可を、承認された一連のアプリケーションに限定するなどの内容が含まれる場合があるため、管理者と協力してデバイス管理ルールに従うようにしてください。組織によっては Apple iOS 向け AnyConnect の使用方法に関するその他のマニュアルがある場合があります。

Apple iOS App Store には、初期インストールとすべてのアップグレード用のアプリケーションが用意されています。Cisco 適応型セキュリティ アプライアンス（ASA）は、VPN へのアクセスを許容するセキュア ゲートウェイですが、モバイル デバイス向け AnyConnect の更新はサポートしません。

ヘルプの表示

AnyConnect では、ヘルプが使用可能な場合には、画面の右下隅に情報アイコンが表示されます。このアイコンをタップし、現在のオプションに関するヘルプ情報を表示します。

または、[バージョン情報（About）] をタップして、このガイドにアクセスできるリンクを表示します。

オープン ソフトウェア ライセンスに関する通知

- 本製品には、OpenSSL Toolkit（http://www.openssl.org/）で使用するために OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。（This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit（http://www.openssl.org/）.）
- 本製品には、Eric Young 氏（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。（This product includes cryptographic software written by Eric Young（eay@cryptsoft.com）.）
- 本製品には、Tim Hudson 氏（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。（This product includes software written by Tim Hudson（tjh@cryptsoft.com）.）

サポートされている Apple iOS デバイス

（注） Per App VPN では、Apple iOS 8.3 以降を使用する必要があります。

デバイス	必要な Apple iOS リリース
iPad Air	7.0 以降
iPad 2	6.0 以降
iPad（第 3 世代）	6.0 以降
iPad（第 4 世代）	6.0 以降
iPad mini	6.0 以降
iPad mini（Retina ディスプレイ）	7.0 以降
iPad-Pro	9.0 以降
iPhone 3GS	6.0 - 6.1.6
iPhone 4	6.0 - 7.1.2
iPhone 4S	6.0 以降
iPhone 5	6.0 以降
iPhone 5C	7.0 以降
iPhone 5S	7.0 以降
iPhone 6	8.0 以降
iPhone 6 Plus	8.0 以降
iPhone 6s	9.0 以降
iPhone 6s Plus	9.0 以降
iPod Touch（第 4 世代）[1]	6.0 - 6.1.6
iPod Touch（第 5 世代）	6.0 以降

[1] AnyConnect は、iPhone 上の場合と同じように iPod Touch 上に表示され、動作します。

Apple iOS AnyConnect アプリケーションのインストール

Cisco AnyConnect Secure Mobility Client for Apple iOS は、Apple App Store からインストールします。

手順

ステップ 1 App Store を開きます。

ステップ 2 [検索（Search）] を選択します。

ステップ 3 検索ボックスに「anyconnect」と入力し、[候補（Suggestions）] リストにある [cisco anyconnect] をタップします。

ステップ 4 [AnyConnect] をタップします。

ステップ 5 [無料（Free）]、[アプリのインストール（INSTALL APP）] の順にタップします。

ステップ 6 [インストール（Install）] を選択します。

Apple iOS での AnyConnect のアップグレード

AnyConnect へのアップグレードは、Apple App Store を使用して管理します。AnyConnect のアップグレードが利用可能であることを示す通知を Apple App Store から受けたら、次の手順に従います。

はじめる前に

デバイスをアップグレードする前に次の手順を実行する必要があります。

- AnyConnect VPN セッションを確立している場合は、セッションを切断します。これに失敗した場合は、新しいバージョンの AnyConnect を使用する前に、AnyConnect はデバイスの再起動を要求します。
- AnyConnect アプリケーションが開いている場合は閉じます。

手順

ステップ 1 iOS のホームページで、[App Store] アイコンをタップします。

ステップ 2 [AnyConnect アップグレード通知（AnyConnect upgrade notice）] をタップします。

ステップ 3 新機能を確認します。

ステップ 4 [更新（Update）] をクリックします。

ステップ 5 [Apple ID パスワード（Apple ID Password）] を入力します。

ステップ 6 [OK] をタップします。

AnyConnect の更新が実行されます。

次の作業

（注） Apple iOS のオンデマンド接続機能が VPN 接続を自動的に行うためにデバイスで使用される場合、AnyConnect アプリを起動し、VPN 接続を確立する必要があります。このようにしないと、次に iOS システムが VPN トンネルを確立しようとするときに、「VPN に接続するにはアプリケーションを起動する必要があります（The VPN Connection requires an application to start up）」というエラー メッセージが表示されます。

AnyConnect の起動

手順

iPhone または iPad のホーム画面で AnyConnect のアイコンをタップします。
インストール後またはアップグレード後に初めて AnyConnect を起動する場合、[OK] を選択して AnyConnect を有効にします。この操作により、このアプリでデバイスの仮想プライベート ネットワーク（VPN）機能を拡張することができます。

AnyConnect の [ホーム（Home）] 画面で以下を実行できます。

- [AnyConnect VPN] のオン/オフ スイッチで、VPN 接続を確立したり、終了したりします。
- アクティブな接続を識別し表示する [接続（Connections）] ウィンドウに移動するか、設定されている他の接続エントリから選択します。
- 現在の VPN 接続のステータスとその他の [詳細情報（Details）] を表示します。
- [設定（Settings）]、[診断（Diagnostics）]、および [バージョン情報（About）] ウィンドウに移動します。

VPN 接続の設定

AnyConnect が VPN 接続を確立するには、次の情報が必要となります。

- ネットワークにアクセスするためのセキュア ゲートウェイのアドレス。

  このアドレスは、接続エントリで設定されます。接続エントリは、AnyConnect のホーム画面にリストされます。アクティブな接続エントリは、AnyConnect ホーム画面または [接続（Connections）] リストに示されます。VPN 接続エントリは、デバイス上で手動で設定するか、または社内の管理者によって自動的に設定されます。

- 正常に接続を確立するための認証情報。

  これは、覚えておく必要のあるユーザ名とパスワードの形式となるか、またはデバイスに設定されたデジタル証明書に含められます。一部の VPN 接続では、両方の認証方式が必要になる場合があります。デジタル証明書は、デバイス上で手動で設定するか、またはデバイス管理者によって自動的に設定されます。

管理者の指示に従って AnyConnect クライアントを設定します。明確な指示がない場合は、管理者に問い合わせてください。

接続エントリの設定

接続エントリは、プライベート ネットワークへのアクセスを提供するセキュア ゲートウェイ、およびその他の接続属性を指定します。

すでにデバイスで設定されているエントリを表示するには、AnyConnect のホーム画面から [接続（Connections）] を選択します。複数の接続エントリがリストされることもあります（いくつかは [Per-App VPN] の見出しの下に表示されます）。接続エントリは、次のステータスになっています。

- [有効（Enabled）]：この接続エントリはモバイル デバイス マネージャによって有効にされ、接続に使用できます。
- [アクティブ（Active）]：このマークまたは強調表示された接続エントリは、現在アクティブです。
- [接続済み（Connected）]：この接続エントリは、アクティブなエントリであり、現在接続され、稼動しています。
- [切断済み（Disconnected）]：この接続エントリは、アクティブなエントリですが、現在切断され、稼動していません。

Per-App VPN 接続エントリは、社内のモバイル デバイス マネージャによって設定され、アプリケーションのリストが含まれることがあります。それらには、企業のプライベート ネットワークへのアクセスが許可されているアプリケーションのみが含まれます。

手順

接続エントリは、次の方法でデバイス上で手動または自動で設定されます。

- 手動での設定。

  ネットワークへのセキュア ゲートウェイのアドレスを把握しておく必要があります。このアドレスはセキュア ゲートウェイのドメイン名または IP アドレスであり、所属するグループを指定することもあります。その他の接続属性も設定できます。「手動による接続エントリの追加または変更, （7 ページ）」を参照してください。

- 管理者から提供されたリンクをクリックすることで、自動的に設定されます。

  AnyConnect URI リンクは電子メールに含まれるか、または Web ページで公開されます。このことをデバイスで許可するには、アプリケーション プリファレンスの [外部制御（External Control）] を、[プロンプト（Prompt）] または [有効（Enable）] に設定する必要があります。参照先 AnyConnect の外部使用の制御, （17 ページ）

- 接続エントリを含む AnyConnect クライアント プロファイルをダウンロードするセキュア ゲートウェイに接続した後で、自動的に設定されます。「VPN プロファイルの管理, （19 ページ）」を参照してください。

- 会社のモバイル デバイス管理ソフトウェアによる設定。デバイス管理プロファイルが、デバイスの一般設定下に見つかる場合があります。

手動による接続エントリの追加または変更

はじめる前に

（注） 作成した接続エントリは変更できますが、AnyConnect VPN プロファイルまたは iPhone Configuration Utility mobileconfig からインポートされた接続は完全には編集することはできません。

手順

ステップ 1 AnyConnect のホーム画面で、[接続（Connections）] をタップします。次に、編集する接続を選択するか、[VPN 接続の追加（Add VPN Connection）] を選択します。
基本的な VPN 接続パラメータが表示されます。設定プロセスは、[キャンセル（Cancel）] をタップしていつでもキャンセルできます。接続エントリを保存するには、[保存（Save）] をタップします。

ステップ 2 （任意） [説明（Description）] をタップして、接続エントリの一意の名前を指定します。
この名前は、AnyConnect のホーム画面の接続リストに表示されます。接続リストに収まるように、半角 24 文字以内にすることを推奨します。キーボードのアルファベット、空白文字、数字、記号を使用します。AnyConnect では、ユーザが指定した大文字と小文字が維持されます。

例：Example 1。

ステップ 3 [サーバ アドレス（Server Address）] をタップして、接続する Cisco 適応型セキュリティ アプライアンスのドメイン名、IP アドレス、またはグループ URL を入力します。
例：vpn.example.com。

ステップ 4 [詳細（Advanced）] をタップして、高度な VPN 接続パラメータを設定します。

a) （任意） この接続の [ネットワーク ローミング（Network Roaming）] を設定します。「ネットワーク ローミングの設定」を参照してください。

b) （任意） この接続の [証明書（Certificate）] の使用を設定します。「証明書の使用の設定」を参照してください。

c) （任意） [アプリケーション ルール（App Rules）] を表示します。
デバイスが企業のモバイル デバイス管理ソフトウェアで管理されている場合、プライベート ネットワークへのアクセスが許可されているアプリケーションのリストがここに表示されます。アプリケーションが許可され、インストールされると、ここにリストされます。その他のすべてのアプリケーションのデータ フローは VPN 接続を使用しませんが、データは VPN トンネルの外部で、暗号化しないで送受信されます。

d) （任意） この接続の [オンデマンド接続（Connect on Demand）] を設定します。「オンデマンド接続の設定」を参照してください。

e) （任意） この接続を、SSL ではなく [IPSec を使って接続（Connect with IPsec）] に設定します。「IPsec の設定」を参照してください。

a) [VPN 接続の追加（Add VPN Connection）] をタップして、初期設定ウィンドウに戻ります。

ステップ 5　接続の値を保持するには、[保存（Save）] をタップします。

ネットワーク ローミングの設定

ネットワーク ローミングにより、デバイスが起動してから、または接続タイプ（EDGE（2G）、1xRTT（2G）、3G、Wi-Fi など）を変更してから AnyConnect の再接続にかかる時間が設定されます。ネットワーク ローミングはオンまたはオフにできます。

- [オン（ON）]：（デフォルト）このオプションでは、VPN アクセスが最適化されます。AnyConnect が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定では、アプリケーションは VPN への持続的な接続に依存します。AnyConnect は、再接続にかかる時間を制限しません。
- [オフ（OFF）]：このオプションでは、バッテリ寿命が最適化されます。AnyConnect が接続を失った場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。接続が必要な場合、新しい VPN 接続を開始する必要があります。

はじめる前に

（注）
- ネットワーク ローミングは iOS 8 より前のリリースにのみ適用されます。iOS 8 以降のリリースは、常にネットワーク ローミングがオンであるかのように動作し、成功するまで接続の再確立を試行します。
- このパラメータは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響しません。
- iPhone Configuration Utility によって作成された VPN 設定は、ネットワーク ローミングをサポートしません。iOS 8 以前でネットワーク ローミングが必要な場合、接続エントリを手動または AnyConnect VPN プロファイルで設定する必要があります。

手順

[詳細（Advanced）]接続エントリ設定画面の [ネットワーク ローミング（Network Roaming）] フィールドで [オン（ON）] または [オフ（OFF）] をタップします。

証明書の使用の設定

手順

ステップ 1 [詳細（Advanced）]接続エントリ設定画面で、[証明書（Certificate）] をタップして [証明書の選択（Select Certificate）] 画面を表示します。

ステップ 2 次のいずれかの選択肢をタップします。

- [無効（Disabled）]：（デフォルト）クライアント証明書は認証に使用されません。
- [自動（Automatic）]：AnyConnect によって、認証で使用されるクライアント証明書が自動的に選択されます。この場合、インストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、VPN 接続を確立するたびに実行されます。
- [証明書の名前（Certificate Name）]：デバイスに証明書をインストール済みの場合、この VPN 接続に関連付ける証明書を選択します。

ステップ 3 [詳細（Advanced）] をタップして、詳細設定ウィンドウに戻ります。

オンデマンド接続の設定

他のアプリケーションがネットワーク接続を開始するときに確認されるルールのリストを作成して、オンデマンド接続機能を設定します。ルールに一致した場合、次のいずれかのオンデマンド接続動作が行われます。

- [接続しない（Never Connect）]：このリストのルールに一致したときに、iOS は絶対に VPN 接続の開始を試行しません。このリストのルールは、その他のすべてルールよりも優先されます。

  オンデマンド接続が有効になっている場合、サーバアドレスが AnyConnect によって自動的にこのリストに追加されます。これにより、Web ブラウザでサーバのクライアントレス ポータルへアクセスする場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。
- [必要に応じて接続（Connect if needed）]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続の開始を試行します。
- [常に接続（Always Connect）]：Apple iOS 6 では、iOS はこのリストのルールに一致したときに、常に VPN 接続の開始を試行します。iOS 7.x では [常に接続（Always Connect）] はサポートされません。このリストのルールに一致したときは、[必要に応じて接続（Connect if needed）] ルールとして動作します。以降のリリースでは、[常に接続（Always Connect）] は使用されません。設定済みのルールは [必要に応じて接続（Connect if needed）] リストに移動され、それに応じて動作します。

これらのルールは、ホスト名（host.example.com）、ドメイン（.example.com）、または部分ドメイン（.internal.example.com）のリストで構成されており、IP アドレス（10.0.0.1）を含めることができません。AnyConnect は、各リスト エントリのドメイン名形式について次のような柔軟性があります。

一致	指示	エントリの例	一致する例	一致しない例
完全なドメイン名の一致。	プレフィクス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
トップ レベル ドメインまでの一連の個別サブドメインの完全一致。先頭のドットにより、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

Apple iOS は、次のすべての条件が満たされた場合にのみ、アプリケーションに代わって VPN 接続を確立します。

- VPN 接続がまだ確立されていない。
- アプリケーションでは、IP アドレスではなく、完全修飾ドメイン名を使用することによって宛先を指定する。
- 接続エントリが有効な証明書を使用するように設定され、かつオンデマンド接続が有効になっている。
- AnyConnect がドメイン要求を [接続しない（Never Connect）] リスト内の文字列に一致させることができない。
- 次のどちらかの条件を満たしている。
  - AnyConnect がドメイン要求を [常に接続（Always Connect）] リスト内の文字列と一致させている。
  - DNS ルックアップが失敗して、AnyConnect がドメイン要求を [必要に応じて接続（Connect if needed）] リスト内の文字列と一致させている。

（注） iOS の Connect on Demand 経由で VPN 接続が開始されると、iOS は、トンネルが一定の期間非アクティブである（トンネルを通過するトラフィックがない）場合、そのトンネルを切断します。詳細については、Apple の https://support.apple.com/en-us/HT203743 [英語] にあるマニュアルを参照してください。

はじめる前に

- 接続エントリは、有効な証明書を使用して認証するように設定されている必要があります。詳細については、証明書の使用の設定, （9 ページ）を参照してください。
- 接続エントリは、ユーザが作成したものである必要があります。ユーザは、ASA からダウンロードされた接続プロファイルでオンデマンド接続を設定できません。

手順

ステップ 1 [詳細（Advanced）] 接続エントリ設定画面で、[オンデマンド接続（Connect On Demand）] の横の [オン（ON）] をタップします。

ステップ 2 [ドメイン リスト（Domain List）] をタップします。

ステップ 3 ドメインを追加するには、次のいずれかを実行します。

- [常に接続（Always Connect）]、[接続しない（Never Connect）]、または [必要に応じて接続（Connect if needed）] セクションの下の [ドメインの追加（Add Domain）] をタップして、そのリストにドメイン文字列を追加します。[ドメイン（Domains）] 画面のリストに行が追加され、ドメイン文字列を入力するためのオンスクリーン キーボードが表示されます。
- 画面の上部にある [編集（Edit）] をタップし、ドメイン文字列を追加、編集、または削除します。
  - リスト間でドメイン名を移動するには、ドメイン エントリの右にある 3 本線をタッチして、移動先リストのタイトルの下の領域にエントリをドラッグします。
  - ドメイン名を削除するには、ドメイン名の左の赤い円をタップして、ドメインの右の [削除（Delete）] をタップします。

ステップ 4 [保存（Save）] をタップします。

IPsec の設定

手順

ステップ 1 [詳細（Advanced）] 接続エントリ設定画面で [IPSec を使って接続（Connect with IPsec）] をタップして、この VPN 接続に SSL ではなく IPSec を使用します。
VPN 接続プロトコルに IPsec を選択した場合、[認証（Authentication）] パラメータが表示されます。

ステップ 2 （任意） [認証（Authentication）] をタップし、この IPSec 接続の認証方式を選択します。

- EAP-AnyConnect（デフォルト）
- IKE-RSA
- EAP-GTC

- EAP-MD5
- EAP-MSCHAPv2

ステップ 3 [詳細（Advanced）] をタップして、詳細設定ウィンドウに戻ります。

EAP-GTC、EAP-MD5、またはEAP-MSCHAPv3を認証に使用するように指定している場合、[IKE ID（IKE Identity）] パラメータが表示されます。

ステップ 4 （任意） [IKE ID（IKE Identity）] をタップして、必要なクライアント ID を入力します。これは管理者から提供されます。

接続エントリの削除

この手順では、手動で設定したVPN接続エントリを削除します。VPNセキュア ゲートウェイからインポートした接続エントリを削除する唯一の方法は、接続エントリが含まれているダウンロードした AnyConnect プロファイルを削除する方法です。

手順

ステップ 1 AnyConnect ホーム画面で、VPN 接続エントリの右の詳細表示ボタンをタップします。

ステップ 2 [VPN 接続の削除（Delete VPN Connection）] をタップします。

証明書の設定

証明書について

証明書は、VPN接続の両端（セキュア ゲートウェイまたはサーバとAnyConnectクライアントまたはユーザ）を電子的に識別するために使用されます。サーバ証明書はAnyConnectに対してセキュア ゲートウェイを識別し、ユーザ証明書はセキュア ゲートウェイに対してAnyConnectユーザを識別します。証明書は認証局（CA）から取得されます。また、認証局によって検証されます。

接続を確立する際、AnyConnectは常にセキュア ゲートウェイからのサーバ証明書を待ちます。セキュア ゲートウェイは、AnyConnect からの証明書のみを待ちます（そのように設定されている場合）。VPN 接続を認証するもう 1 つの方法は、AnyConnect ユーザが証明書を手動で入力するのを待つことです。実際、セキュア ゲートウェイは、AnyConnect ユーザをデジタル証明書、手動による証明書の入力、またはその両方で認証するように設定できます。証明書のみによる認証では、ユーザの操作を必要とせずに VPN が接続できます。

セキュア ゲートウェイおよびデバイスに対する証明書の配布および使用については、管理者から指示されます。管理者からの指示に従い、AnyConnect VPN のサーバ証明書とユーザ証明書のインポート、使用、および管理を行います。このマニュアルの証明書および証明書の管理に関連した情報および手順は、ユーザに理解し、参考にしてもらうために提供されています。

AnyConnect は、独自の証明書ストアに認証用のユーザ証明書とサーバ証明書を保存します。AnyConnect 証明書ストアは、[診断（Diagnostics）] > [証明書（Certificates）] 画面から管理します。

ユーザ証明書の管理

デジタル証明書を使用してセキュア ゲートウェイへの認証を行うには、ユーザ証明書をインポートし、VPN 用に設定する必要があります。

ユーザ証明書は、管理者からの指示に従い次のいずれかの方法でインポートされます。

- 電子メールに添付された証明書のインポート，（13 ページ）
- ハイパーリンクによる証明書のインポート，（14 ページ）
- 手動での証明書のインポート，（14 ページ）
- セキュア ゲートウェイから提供される証明書のインポート，（15 ページ）

証明書のインポート後、この証明書を特定の接続エントリに関連付けるか、または接続確立中に認証のためにこの証明書を自動的に選択させることができます。「証明書の使用の設定，（9 ページ）」を参照してください。

サーバ証明書の管理

接続の確立中にセキュア ゲートウェイから受信したサーバ証明書は（証明書が有効で信頼できる場合のみ）、そのサーバを AnyConnect に対して自動的に認証します。該当しない場合は、次のようになります。

- 有効であっても信頼できないサーバ証明書は、確認、認可後に、AnyConnect証明書ストアにインポートされます。AnyConnect ストアにサーバ証明書がインポートされると、このデジタル証明書を使用する、そのサーバに対する後続の接続は自動的に受け入れられます。
- 無効な証明書は AnyConnect ストアにインポートできません。現在の接続を完了するために受け入れる以外の用途はありません。ただし、これは推奨されません。

AnyConnect ストア内のサーバ証明書は、認証に必要なくなった場合は削除できます。

電子メールに添付された証明書のインポート

はじめる前に

管理者は、認証に使用する証明書を電子メールで送信する必要があります。

手順

ステップ 1　添付された証明書のアイコンをタップします。

証明書を開いたことが Apple iOS で認識され、インストール ウィザードが開きます。

ステップ 2 [インストール（Install）] をタップします。

ステップ 3 インストール ウィザードの指示に従います。

ステップ 4 プロンプトが表示されたら、証明書の認証コードを入力します。

ステップ 5 [次へ（Next）] をタップします。
Apple iOS で証明書がインストールされます。

ハイパーリンクによる証明書のインポート

はじめる前に

この操作を実行するため、AnyConnect 設定内で [外部制御（External Control）] が [プロンプト（Prompt）] または [有効（Enable）] のいずれかに設定されていることを確認します。詳細については、AnyConnect の外部使用の制御, （17 ページ）を参照してください。

管理者は、ユーザの iOS デバイスにインストールする証明書の場所へのハイパーリンクを提供する必要があります。

手順

ステップ 1 管理者から受け取ったハイパーリンクをタップします。

ステップ 2 プロンプトが表示されたら、証明書の認証コードを入力し、[次へ（Next）] をタップします。
Apple iOS で証明書がインポートされ、証明書の登録メッセージが表示されます。

手動での証明書のインポート

はじめる前に

管理者は、証明書の URL を提供する必要があります。

手順

ステップ 1 AnyConnect ホーム画面で、[診断（Diagnostics）] > [証明書（Certificates）] をタップします。

ステップ 2 [ユーザ（User）] タブをタップします。

ステップ 3 [証明書のインポート（Import Certificate）] をタップして、証明書を手動でインポートします。

ステップ 4 管理者から入手した URL を入力します。

セキュア ゲートウェイから提供される証明書のインポート

はじめる前に

管理者は、SCEP プロトコルを使用して証明書を配布するために設定した接続エントリの名前を提供する必要があります。

手順

ステップ 1 AnyConnect のホーム画面の [接続を選択（Choose a connection）] 領域で、モバイル デバイスに証明書をダウンロードできる接続の名前をタップします。

ステップ 2 AnyConnect の [オン（On）] ボタンをタップします。

ステップ 3 [証明書を取得（Get Certificate）] が表示される場合はこれをタップします。それ以外の場合は、モバイル デバイスに証明書をダウンロードするように設定されているグループを選択します。

ステップ 4 管理者から受け取った認証情報を入力します。

セキュア ゲートウェイによってデバイスに証明書がダウンロードされ、VPN セッションが切断されて、証明書の登録が正常に完了したことを示すメッセージを受け取ります。

ステップ 5 [OK] をタップします。

次の作業

AnyConnect が証明書を自動で使用できるようになりました。ユーザが証明書を特定の接続エントリに割り当てることもできます。詳細については、証明書の使用の設定, （9 ページ）を参照してください。

証明書の表示と削除

手順

ステップ 1 AnyConnect ホーム画面で、[診断（Diagnostics）] > [証明書（Certificates）] をタップします。

ステップ 2 AnyConnect 証明書ストアのユーザ証明書を表示するには、[ユーザ（User）] タブをタップします。[編集（Edit）] をタップして単一の証明書を削除するか、[すべてのユーザ証明書の削除（Delete All User Certificates）] をタップしてすべてのユーザ証明書を削除します。

ステップ 3 AnyConnect 証明書ストアのサーバ証明書を表示するには、[サーバ（Server）] タブをタップします。[編集（Edit）] をタップして単一の証明書を削除するか、[すべてのサーバ証明書の削除（Delete All Server Certificates）] をタップしてすべてのサーバ証明書を削除します。

VPN 接続の確立

はじめる前に

- VPN に接続するには、アクティブな Wi-Fi 接続があるか、またはサービス プロバイダーに接続している必要があります。
- VPN 接続を開始するには、AnyConnect のホーム ウィンドウで [接続を選択（Choose a Connection）] に接続エントリが 1 つ以上リストされている必要があります。
- VPN に接続するには、セキュア ゲートウェイによって想定される認証情報が必要です。

手順

ステップ 1 AnyConnect のホーム画面で、使用する接続エントリをタップします。
AnyConnect で、その接続エントリの横にチェック マークが移動され、実行中のすべての VPN 接続が解除されます。

ステップ 2 [AnyConnect VPN] の横にある [オン（ON）] をタップします。

ステップ 3 必要に応じて、システム管理者から提供された資格情報を使用してログインします。

ステップ 4 システム管理者から指示があった場合は、[証明書を取得（Get Certificate）] をタップします。

ステップ 5 必要に応じて、[接続（Connect）] をタップします。
セキュア ゲートウェイの設定に応じて、AnyConnect が接続エントリを取得し、それらを [接続（Connections）] リストに追加することがあります。

VPN アイコンがステータス バーに表示され、その VPN は「接続済み（Connected）」として表示されます。

⚠

注意 AnyConnect のホーム画面で別の VPN 接続をタップすると、現在の VPN 接続は切断されます。

AnyConnect 通知への応答

信頼できない VPN サーバ通知への応答

表示される [信頼されていない VPN サーバ（Untrusted VPN Server）] 通知のタイプは、[信頼できない VPN サーバのブロック（Block Untrusted VPN Server）] アプリケーション プリファレンスによって異なります。

- 有効になっている場合、ブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」が表示されます。次のいずれかを選択します。
  - [安全を確保（Keep Me Safe）]：この設定とこのブロッキング動作を保持します。

- [設定の変更（Change Settings）]：ブロッキングをオフにします。

  [信頼できない VPN サーバのブロック（Block Untrusted VPN Server）] を変更したら、VPN 接続を再び開始します。

- 有効になっていない場合、ノンブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」が表示されます。次のいずれかを選択します。
  - 信頼できないサーバへの VPN 接続を中止するには、[キャンセル（Cancel）] を選択します。
  - 信頼できないサーバに接続するには [続行（Continue）] を選択します。このオプションは推奨されません。
  - 証明書の詳細を表示し、今後接続を受け入れて続行するためにサーバ証明書を AnyConnect 証明書ストアにインポートするかどうかを決定するには、[詳細の表示（View Details）] を選択します。

別のアプリケーションへの応答

デバイスを保護するため、AnyConnect は、外部アプリケーションが AnyConnect を使用しようとすると警告します。これは、AnyConnect アプリケーション プリファレンスの [外部制御（External Control）] が [プロンプト（Prompt）] に設定されている場合に生じます。

次のプロンプトに対して [はい（Yes）] をタップするかどうか管理者に確認してください。

- `Another application has requested that AnyConnect create a new connection to host.Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect connect to host.Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect disconnect the current connection.Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store.Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import localization files.Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import profiles.Do you want to allow this? [Yes | No]`

AnyConnect の設定と管理（オプション）

AnyConnect の外部使用の制御

外部制御アプリケーションの設定により、AnyConnect アプリケーションが外部 URI 要求に応答する方法が指定されます。外部要求により、接続エントリの作成、VPN の接続または切断、およびクライアント プロファイル、証明書、またはローカリゼーション ファイルのインポートが行われます。

外部要求は、一般には管理者により電子メールまたは Web ページで提供されます。管理者は、次の値のいずれかを使用するように指示します。

- [有効（Enabled）]：AnyConnect アプリケーションは自動的にすべての URI コマンドを許可します。
- [無効（Disabled）]：AnyConnect アプリケーションは自動的にすべての URI コマンドを拒否します。
- [プロンプト（Prompt）]：AnyConnect アプリケーションは、デバイス上の AnyConnect URI にアクセスするたびプロンプトを表示します。URI 要求を許可または拒否します。詳細については、別のアプリケーションへの応答，（17 ページ）を参照してください。

手順

ステップ 1 AnyConnect アプリケーションで、[設定（Settings）] をタップします。
ステップ 2 [外部制御（External Control）] をタップします。
ステップ 3 [有効（Enabled）]、[無効（Disabled）]、または [プロンプト（Prompt）] をタップします。
ステップ 4 [設定（Settings）] をタップして、[設定（Settings）] 画面に戻ります。

信頼されていないサーバのブロック

このアプリケーション設定は、AnyConnect がセキュア ゲートウェイを識別できない場合に接続をブロックするかどうかを決定します。この保護はデフォルトでは ON です。OFF にできますが、OFF にすることは推奨されません。

AnyConnect はサーバから受信した証明書を使用してそのアイデンティティを確認します。期限切れまたは無効な日付、キーの不正な使用、または名前の不一致が原因で証明書エラーが発生すると、接続がブロックされます。

この設定が ON になっている場合、ブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」により、このセキュリティの脅威が警告されます。

手順

ステップ 1 AnyConnect アプリケーションで、[設定（Settings）] をタップします。
ステップ 2 [信頼されていないサーバをブロック（Block Untrusted Servers）] チェックボックスをタップし、このプリファレンスを有効または無効にします。

FIPS モードの設定

FIPS モードでは、すべての VPN 接続に連邦情報処理標準（FIPS）暗号化アルゴリズムが使用されます。

はじめる前に

ネットワークに接続するためにお使いのモバイル デバイスで FIPS モードを有効にする必要がある場合は、管理者からそのことが通知されます。

手順

ステップ 1 AnyConnect アプリケーションで、[設定（Settings）] をタップします。

ステップ 2 [FIPS モード（FIPS Mode）] チェックボックスをタップし、このプリファレンスを有効または無効にします。

VPN プロファイルの管理

デバイス上の VPN プロファイルの管理は、管理者が指定する手順に基づいて実行します。

AnyConnect VPN クライアント プロファイルは、セキュア ゲートウェイからダウンロードした XML ファイルで、クライアントの動作を指定し、VPN 接続を識別します。VPN クライアント プロファイル内の各接続エントリは、このエンドポイント デバイスにアクセス可能なセキュア ゲートウェイ、およびその他の接続属性、ポリシー、および制約を指定します。デバイスに手動で設定した VPN 接続に加えて、これらの接続エントリが、VPN 接続を開始するときに選択できます。

（注） AnyConnect は、デバイス上で一度に 1 つの VPN プロファイルのみを維持します。

手順

ステップ 1 AnyConnect のホームページから、[診断（Diagnostics）] > [プロファイル（Profile）] をタップします。

ステップ 2 次のいずれかを選択します。

- [プロファイルのインポート（Import Profile）] : インポートする VPN プロファイルの URL を指定します。
- [プロファイルの削除（Delete Profile）] : デバイスから現在の VPN プロファイルを削除します。

  （注） 同じ ASA のドメイン、IP アドレス、またはグループ URL に再接続すると、AnyConnect によって VPN プロファイルがリロードされ、セキュリティ ポリシーが再度適用されます。
- [プロファイルの表示（Show Profile）] : デバイス上の現在の VPN プロファイルを表示または非表示にします。

ローカリゼーションの管理

インストール済みローカリゼーション データの表示

AnyConnect をインストールすると、デバイスで指定されているロケールがパッケージに含まれている言語変換に一致する場合には、モバイルデバイスがローカライズされます。AnyConnectパッケージには、次の言語変換が含まれます。

- カナダ フランス語（fr-ca）
- 中国語（台湾）（zh-tw）
- チェコ語（cs-cz）
- オランダ語（nl-nl）
- フランス語（fr-fr）
- ドイツ語（de-de）
- ハンガリー語（hu-hu）
- イタリア語（it-it）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- 中南米スペイン語（es-co）
- ポーランド語（pl-pl）
- ポルトガル語（ブラジル）（pt-br）
- ロシア語（ru-ru）
- 簡体字中国語（zh-cn）
- スペイン語（es-es）

インストールされる言語は、[設定（Settings）] > [一般（General）] > [国際（International）] > [言語（Language）] で指定されているロケールによって決定されます。AnyConnect の UI とメッセージは、AnyConnect を起動するとすぐに変換されます。

AnyConnect は最適なものを判断するために、言語仕様、地域仕様の順に使用します。たとえば、インストール後にロケール設定をスイス フランス語（fr-ch）にすると、カナダ フランス語（fr-ca）表示になります。

手順

ステップ 1 AnyConnect アプリケーションで、[診断（Diagnostics）] > [ローカリゼーション（Localization）] をタップします。

ステップ 2 モバイル デバイスにインストールされたローカリゼーション ファイルのリストを表示します。

示されている言語が、現在 AnyConnect で使用されています。

ローカリゼーション データのインポート

インストール後に、AnyConnect パッケージでサポートされていない言語のローカリゼーション データを、次のようにしてインポートします。

- 管理者によって提供され、ローカリゼーションデータをインポートするように定義されたハイパーリンクをクリックします。

  管理者は、クリックするとローカリゼーション データがインポートされるハイパーリンクを、電子メールまたは Web ページで提供できます。この方法では、AnyConnect の設定および管理を簡素化するため、管理者に提供されている機能である AnyConnect URI ハンドラを使用します。

  （注） AnyConnect設定内で外部制御を[プロンプト（Prompt）]または[有効（Enable）]に設定して、この AnyConnect アクティビティを許可する必要があります。この設定方法については、AnyConnect の外部使用の制御, （17 ページ）を参照してください。

- VPN接続時にダウンロード可能なローカリゼーションデータを提供するように管理者が設定したセキュア ゲートウェイに接続します。

  この方法を使用する場合には、管理者が適切な VPN 接続情報を提供するか、または XML プロファイル内に事前定義された接続エントリを提供します。VPN 接続時に、ローカリゼーション データがデバイスにダウンロードされ、ただちに有効になります。

- [AnyConnect ローカリゼーション管理アクティビティ（AnyConnect Localization Management Activity）]画面の[ローカリゼーションのインポート（Import Localization）]オプションを使用して手動でインポートされます。

手順

ステップ 1 AnyConnect アプリケーションで、[診断（Diagnostics）]>[ローカリゼーション（Localization）]をタップします。

ステップ 2 [ローカリゼーションのインポート（Import Localization）]をタップします。

ステップ 3 セキュア ゲートウェイのアドレスとロケールを指定します。

ロケールは ISO 639-1 によって指定され、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。

このローカリゼーションデータは、事前にパッケージ化されてインストールされたローカリゼーション データの代わりに使用されます。

ローカリゼーション データの復元

手順

ステップ 1 AnyConnect アプリケーションで、[診断（Diagnostics）] > [ローカリゼーション（Localization）] をタップします。

ステップ 2 [ローカリゼーションの復元（Restore Localization）] をタップします。

AnyConnect パッケージから事前ロードされたローカリゼーションデータの使用を復元し、インポートされたローカリゼーション データをすべて削除します。

復元される言語は、[設定（Settings）] > [一般（General）] > [国際（International）] > [言語（Language）] で指定されているデバイスのロケールに基づいて選択されます。

AnyConnect の削除

手順

ステップ 1 AnyConnect のホームページから、[診断（Diagnostics）] > [プロファイル（Profile）] をタップします。

ステップ 2 [プロファイルの削除（Delete Profile）] をタップします。

ステップ 3 デバイスのホーム画面に戻ります。

ステップ 4 AnyConnect をフォルダに入れた場合は、そのフォルダを開きます。

ステップ 5 （X）アイコンが AnyConnect アイコンの上に表示されるまで、AnyConnect アイコンをタップしたままにします。

ステップ 6 削除アイコンをタップします。

AnyConnect のモニタリングとトラブルシューティング

AnyConnect のバージョンおよびライセンスの表示

手順

AnyConnect のホーム画面で [バージョン情報（About）] をタップします。

次の作業

[バージョン情報（About）] ウィンドウでリンクをタップして、このガイドの最新バージョンを開きます。

AnyConnect 統計情報の表示

VPN 接続が存在する場合、AnyConnect では統計情報を記録します。

手順

AnyConnect ホーム画面で、[詳細（Details）] > [統計情報（Statistics）] をタップします。

詳細な統計情報には次の値が含まれます。

- [セキュア ルート（Secure Routes）]：通信相手が 0.0.0.0 かつサブネット マスクが 0.0.0.0 のエントリは、すべての VPN トラフィックが暗号化され、VPN 接続を通して送受信されることを意味します。
- [保護されていないルート（Non-Secure Routes）]：[セキュア ルート（Secure Routes）] の下に 0.0.0.0/0.0.0.0 が存在する場合のみ表示されます。VPN セキュア ゲートウェイが決定したとおりに、暗号化された接続から除外されるトラフィック宛先です。

システム情報の表示

手順

AnyConnect ホーム画面で、[診断（Diagnostics）] > [システム情報（System Information）] をタップします。

ログ メッセージの表示と管理

デバイス リソースに対する不要な負荷を避けるために、AnyConnectのデフォルトではメッセージをログ記録しません。トラブルシューティングの場合のみログを有効にしてください。

手順

ステップ 1 AnyConnect のホーム画面で [診断（Diagnostics）] をタップします。

ステップ 2 [VPN デバッグ ログ（VPN Debug Logs）] をオンにして、ロギングを有効にします。

ステップ 3 [ログ（Logs）] をタップします。

ステップ 4 次のいずれかを選択します。

- [メッセージ（Messages）]：ログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [サービス（Service）]：サービス デバッグ ログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [アプリ（App）]：アプリケーション デバッグ ログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [ログのクリア（Clear Logs）]：すべてのログ メッセージが削除されます。

- [診断（Diagnostics）]：[診断（Diagnostics）] 画面に戻ります。

ログ メッセージの送信

はじめる前に

お使いのデバイスに電子メールアカウントが設定されている必要があります。また、[VPNデバッグ ログ（VPN Debug Logs）] を [オン（ON）] に設定しておく必要があります。

手順

ステップ 1 AnyConnect ホーム画面で、[診断（Diagnostics）] > [電子メール ログ（Email Logs）] をタップします。

ステップ 2 問題とその問題を再現する手順を記述し、[送信（Send）] をタップします。

ステップ 3 ログを [管理者（Administrator）] に送信するか、[シスコ（Cisco）] に送信するかを選択し、電子メール アプリケーションを使用して、そのメッセージを送ります。

Apple iOS の一般的な問題

このトピックでは、一般的な問題に対する解決策を説明します。これらの解決策を試みても問題が解決しない場合は、所属する組織の IT サポート部門に問い合わせてください。

一部の接続プロファイルで編集と削除ができません。

AnyConnect 接続プロファイルにインポートしたホスト エントリに影響するポリシーが、システム管理者によって設定されています。これらのプロファイルを削除するには、[診断（Diagnostics）] > [プロファイル（Profile）] > [プロファイル データのクリア（Clear Profile Data）] の順にタップします。

設定を保存または編集しようとするとエラーが発生します。

オペレーティング システムの既知の問題が原因です。Appleは、この問題の解決に取り組んでいます。回避策として、アプリケーションの再起動を試してください。

接続タイムアウトおよび未解決ホスト。

インターネット接続の問題、携帯電話の信号レベルが低い、およびネットワークの輻輳などが原因で、タイムアウトや未解決ホストエラーを引き起こすことがよくあります。LANを利用できる場合は、デバイスのSettingsアプリケーションを使用し、最初にLANとの接続の確立を試してください。タイムアウトになったときに、何度か再試行することで、成功することがよくあります。

デバイスがスリープから復帰したときに VPN 接続が再確立されません。

VPN 接続エントリで [ネットワーク ローミング（Network Roaming）] を有効にします。ネットワーク ローミングを有効にしても問題が解決されない場合は、EDGE（2G）、1xRTT（2G）、3G、または Wi-Fi 接続を確認します。

（注） この問題は、ユーザが所属する組織での VPN の設定に基づく動作である場合があります。

証明書ベースの認証が機能しません。

該当する証明書を以前は使用できた場合、証明書の有効性と期限を確認します。接続に対して適切な証明書を使用しているかどうかをシステム管理者に確認します。

Apple iOS Connect On Demand 機能が動作しない、または接続できません。

その接続で、[接続しない（Never Connect）] リスト内に競合する規則がないかどうかを確認します。その接続に [必要に応じて接続（Connect if needed）] 規則が存在する場合は、[常に接続（Always Connect）] 規則に置き換えます。

AnyConnect は接続を確立できませんでしたが、エラー メッセージが表示されません。

メッセージは、AnyConnect アプリケーションが開かれている場合にのみ表示されます。

Cisco AnyConnect というプロファイルがありますが削除できません。

アプリケーションの再起動を試してください。

AnyConnect アプリケーションを削除しても、Apple iOS の VPN 設定に VPN 設定が表示されます。

これらのプロファイルを削除し、AnyConnect を再インストールするには、[診断（Diagnostics）] > [プロファイル（Profile）] > [プロファイル データのクリア（Clear Profile Data）] の順にタップします。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2016年5月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp