



Cisco AnyConnect Secure Mobility Client Apple iOS 向けリリース 4.7.x リリースノート

[Apple iOS 向け AnyConnect リリースノート](#) 2

改訂：2019年8月5日

Apple iOS 向け AnyConnect リリース ノート

Apple iOS モバイル デバイス 向け AnyConnect

AnyConnect Secure Mobility Client により、リモート ユーザは Cisco ASA 5500 シリーズへのセキュアな VPN 接続を確立できます。このクライアントは、エンタープライズ ネットワークへのシームレスかつセキュアなリモート アクセスを提供し、インストールしたアプリケーションがエンタープライズ ネットワークに直接接続されているかのように通信を行えるようにします。AnyConnect は、IPv4 または IPv6 トンネルを介した IPv4 および IPv6 リソースへの接続をサポートします。

AnyConnect Secure Mobility Client と適応型セキュリティ アプライアンス (ASA) 5500 の管理者向けに作成されたこのドキュメントは、『Cisco AnyConnect Mobile Platforms 管理者 ガイド リリース 4.6』を補足するとともに、Apple iOS デバイス上で動作する AnyConnect のリリースに固有の情報を提供します。

AnyConnect アプリケーションは、Apple iTunes App Store でのみ入手できます。シスコでは、AnyConnect モバイル アプリケーションを配布していません。また、ASA からモバイル アプリケーションを展開することもできません。このモバイル リリースがサポートされている間は、ASA からデスクトップ デバイス用の他の AnyConnect リリースを展開することが可能です。

AnyConnect Mobile のサポート ポリシー

シスコでは、現在 App Store で入手可能な AnyConnect バージョンをサポートしていますが、修正プログラムと拡張機能は、最新のリリース バージョンでのみ提供されます。

AnyConnect のライセンス

ASA ヘッドエンドに接続するには、AnyConnect 4.x Plus または Apex ライセンスが必要ですが、トライアル ライセンスも用意されています。詳細については、『Cisco AnyConnect 発注ガイド』を参照してください。

最新のエンドユーザライセンス契約についてはシスコエンドユーザライセンス契約、AnyConnect Secure Mobility Client リリース 4.x、を参照してください。

オープンソース ライセンス通知については、以下を参照してください。Cisco AnyConnect Secure Mobility Client で使用されているモバイル向けオープンソース ソフトウェア リリース 4.x

TestFlight による Cisco AnyConnect のベータ テスト

TestFlight でのリリース前のテストには、AnyConnect のベータ ビルドを利用します。TestFlight でのテストに参加するには、<https://testflight.apple.com/join/NOQLSq2c> の手順に従います。

この TestFlight のリンクで後からオプトアウトすることも可能です。オプトアウトしたら、ベータ ビルドをアンインストールして最新のベータ版ではない AnyConnect を再インストールする必要があります。

ベータ テスト中に問題が見つかった場合は、シスコ (ac-mobile-feedback@cisco.com) に電子メールで速やかに報告してください。Cisco Technical Assistance Center (TAC) は、AnyConnect のベータ版で見つかった問題には対処しません。

Apple iOS で利用可能な AnyConnect のバージョン

Cisco AnyConnect for Apple iOS は、現在複数のバージョンで利用可能です。

• Cisco AnyConnect

Cisco AnyConnect は、Apple iOS で利用可能な最新の推奨バージョンです。常に最新の Apple iOS のバグ修正を受けられるように、最新バージョンにアップグレードしてください。

このバージョンは、Apple iOS 10.3 以降でを使用することを推奨します。このバージョンは、iOS が提供する新しい拡張フレームワークを使用して、VPN とそのすべての機能を実装しています。アプリケーション単位 VPN トンネリングは AnyConnect 4.0.07x 以降で完全にサポートされている機能であり、新しい拡張フレームワークでは TCP と UDP の両方のアプリケーションをサポートできます。今後も、新しい Cisco AnyConnect バージョンが、すべての拡張機能とバグ修正を含む唯一のバージョンとなります。番号は、4.0.07x 以降となります。

• Cisco レガシー AnyConnect

レガシー AnyConnect 4.0.05x は、11.x. を超える iOS ではサポートされていません。iOS の以降のバージョンとの互換性を確保するには、App Store で使用可能な最新の AnyConnect アプリケーションをインストールします。

レガシー AnyConnect は Apple iOS 6.0 以降をサポートするバージョンで、今後しばらくの間 App Store で利用可能です。このバージョンは時間をかけて段階的に廃止されますが、最新の推奨バージョンへの移行が容易になるように現在も利用可能です。

レガシー AnyConnect アプリの Per App VPN トンネリング機能は、TAC サポートを受けません。Per App VPN の使用を希望されるお客様は、新しいバージョンに移行する必要があります。

レガシー AnyConnect は、重要なセキュリティ上の問題に関する更新のみがなされます。このリリースには、4.0.05x という番号が使用され続けます。

Cisco AnyConnect と Legacy AnyConnect は、異なるアプリ ID を持つ異なるアプリです。次に例を示します。

- AnyConnect 4.0.07x (およびそれ以降) で新しい拡張フレームワークを使用すると、レガシー AnyConnect 4.0.05x : AnyConnect の動作が次のように変更されます。AnyConnect は、スプリット包含ネットワークにない場合でも、トンネル DNS サーバのトラフィックがトンネリングされると見なします。
- AnyConnect アプリケーションを 4.0.05x 以前のバージョンから AnyConnect 4.0.07x または 4.6.x にアップグレードすることはできません。Cisco AnyConnect 4.0.07x (または 4.6.x) は別のアプリケーションで、別の名前とアイコンを使用してインストールされています。
- AnyConnect の異なるバージョンは、モバイルデバイスに共存できますが、これはシスコではサポートされません。両方のバージョンの AnyConnect がインストールされている状況で接続しようとする、予期せぬ動作が発生する恐れがあります。デバイスにインストールされている AnyConnect アプリは 1 つだけで、デバイスと環境に適したバージョンであるようにしてください。
- Legacy AnyConnect バージョン 4.0.05069 以前のリリースを使用してインポートされた証明書は、新しい AnyConnect アプリケーションのリリース 4.0.07072 ではアクセスおよび使用ができません。MDM で導入された証明書は、両方のアプリ バージョンでアクセスおよび使用ができます。
- 証明書やプロファイルなどの、Legacy AnyConnect アプリにインポートされたアプリ データは、新しいバージョンに更新する場合、削除する必要があります。そうしないと、システムの VPN 設定で引き続き表示されます。Legacy AnyConnect アプリをアンインストールする前にアプリ データを削除します。

- 現在の MDM プロファイルでは、新しいアプリはトリガーされません。EMM ベンダーは、VPNType (VPN)、VPNSubType (com.cisco.anyconnect)、および ProviderType (パケットトンネル) をサポートする必要があります。AnyConnect は新しいフレームワークで ISE にアクセスできなくなるため、ISE と統合させるには UniqueIdentifier を AnyConnect に渡せる必要があります。設定方法については、EMM ベンダーにお問い合わせください。カスタム VPN タイプが必要な場合もあれば、リリース時にはサポートされていない場合もあります。

AnyConnect 4.0.07x 以降で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x からの動作が次のように変更されます。

- ヘッドエンドに送信されたデバイス ID は、新しいバージョンでは UDID ではなく、初期設定へのリセット後には、同じデバイスで作成されたバックアップからデバイスが復元されない限り、デバイス ID が異なるものになります。
- MDM で導入された証明書だけでなく、AnyConnect で利用可能ないずれかの方法 (SCEP、UI 使用 - 手動で、URI ハンドラ) を使用してインポートされた証明書も使用できます。AnyConnect の新しいバージョンでは、電子メールまたはこれらの識別されたもの以外のメカニズムを使用してインポートした証明書を使用できなくなりました。
- UI を使用して接続エントリーを作成する際には、表示された iOS セキュリティ メッセージを受け入れる必要があります。
- AnyConnect VPN プロファイルからダウンロードしたホストエントリーと同じ名前のユーザが作成したエントリーは、アクティブであれば切断されるまで名前の変更されません。また、ダウンロードされたホスト接続エントリーは、接続が維持されている間ではなく、接続が解除された後に UI に表示されます。
- AnyConnect では、split-include ネットワークではない場合でもトンネル DNS サーバのトラフィックがトンネル化されると見なされます。

サポートされている Apple iOS デバイス

Cisco AnyConnect 4.0.07x 以降は、最新の推奨バージョンで、Apple iOS 10.3 以降を実行するすべての iPhone、iPad、および iPod Touch デバイスで利用可能です。

デバイスが Apple iOS 10.3 以降をサポートしていない場合は、Apple iOS 6.0 以降を実行するすべての iPhone、iPad、および iPod Touch デバイスで利用可能な **Legacy AnyConnect 4.0.05x** のみが使用できます。レガシー AnyConnect の Per App トンネリングには、Apple iOS 8.3 以降が必要です。



(注) 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 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。Cisco AnyConnect または Legacy 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。



(注) AnyConnect アプリケーションを 4.0.05x 以前のバージョンから AnyConnect 4.0.07x または 4.6.x にアップグレードすることはできません。Cisco AnyConnect 4.0.07x (または 4.6.x) は別のアプリケーションで、別の名前とアイコンを使用してインストールされています。

新しいバージョン 4.0.07xxx をインストールする前に、[Apple iOS で利用可能な AnyConnect のバージョン \(3 ページ\)](#) を参照してください。Legacy AnyConnect アプリ データをすべて削除し、Legacy AnyConnect アプリを削除してから、新しいバージョンをインストールすることを推奨します。

始める前に

デバイスをアップグレードする前に、AnyConnect VPN セッションが確立されている場合はそのセッションを切断し、AnyConnect アプリケーションが開いている場合は閉じる必要があります。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。



(注) これは、Apple Connect-on-Demand 機能を使用していて、4.0.05032 より前の Legacy AnyConnect リリース、または 9.3 より前の Apple iOS リリースを実行している場合にのみ、お使いの環境に適用されます。AnyConnect の更新後に Connect On-Demand VPN トンネルが適切に確立されるようにするには、ユーザが AnyConnect アプリを手動で開始して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。

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。

新機能

Apple iOS モバイル端末向け AnyConnect 4.7.03051 の新機能

このリリースでは、[Apple iOS の AnyConnect 4.7.03051 の解決済みの問題 \(13 ページ\)](#) に記載されている不具合を解決します。

シスコでは、お使いのデバイスが iOS 10 以降をサポートしている場合は、このリリースの AnyConnect にアップグレードし、『Apple iOS での AnyConnect の注意事項と制約事項 (11 ページ)』と『既知の互換性の問題 (12 ページ)』で現在の運用に関する留意事項を確認しておくことをお勧めしています。

Apple iOS モバイル端末向け AnyConnect 4.7.02025 の新機能

このリリースでは、Apple iOS の AnyConnect 4.7.02025 の解決済みの問題 (13 ページ) に記載されている不具合を解決します。

シスコでは、お使いのデバイスが iOS 10 以降をサポートしている場合は、このリリースの AnyConnect にアップグレードし、『Apple iOS での AnyConnect の注意事項と制約事項 (11 ページ)』と『既知の互換性の問題 (12 ページ)』で現在の運用に関する留意事項を確認しておくことをお勧めしています。

Apple iOS モバイル端末向け AnyConnect 4.7.01072 の新機能

このリリースでは、Apple iOS の AnyConnect 4.7.01075 の解決済みの問題 (14 ページ) に記載されている不具合を解決します。

シスコでは、お使いのデバイスが iOS 10 以降をサポートしている場合は、このリリースの AnyConnect にアップグレードし、『Apple iOS での AnyConnect の注意事項と制約事項 (11 ページ)』と『既知の互換性の問題 (12 ページ)』で現在の運用に関する留意事項を確認しておくことをお勧めしています。

Apple iOS モバイル端末向け AnyConnect 4.7.00139 の新機能

この AnyConnect のリリースでは、次の新機能が提供され、『Apple iOS の AnyConnect 4.7.00139 の解決済みの問題 (14 ページ)』に記載されている不具合が解決されます。

- VPN TLS ECDSA クライアント証明書のサポート。
- DTLSv1.2 のサポート。

シスコでは、お使いのデバイスが iOS 10 以降をサポートしている場合は、このリリースの AnyConnect にアップグレードし、『Apple iOS での AnyConnect の注意事項と制約事項 (11 ページ)』と『既知の互換性の問題 (12 ページ)』で現在の運用に関する留意事項を確認しておくことをお勧めしています。

Apple iOS AnyConnect 機能マトリックス

次の機能は、Apple iOS 端末向け AnyConnect でサポートされます。

カテゴリ：機能	Apple iOS
展開および設定：	
アプリケーションストアからのインストールまたはアップグレード	○
Cisco VPN プロファイルのサポート (手動インポート)	○
Cisco VPN プロファイルのサポート (接続中のインポート)	○
MDM 設定の接続エントリ	○

カテゴリ：機能	Apple iOS
ユーザ設定の接続エントリ	○
トンネリング：	
TLS	○
データグラム TLS (DTLS)	○
IPsec IKEv2 NAT-T	○
IKEv2 - raw ESP	いいえ
Suite B (IPSec のみ)	○
TLS 圧縮	あり。32 ビットデバイスのみ
デッドピア検出	○
トンネル キープアライブ	○
複数のアクティブ ネットワーク インターフェイス	いいえ
アプリケーションごとのトンネリング	あり。Cisco AnyConnect 4.0.09xxx および iOS 10.3 以降が必要です。
フルトンネル (OSにより、アプリケーションストアへのトラフィックなど一部のトラフィックで例外が発生する可能性があります)	○
スプリット トンネル (スプリットを含む)	○
ローカル LAN (スプリットを含まない) 。 *	○
Split-DNS	○
自動再接続/ネットワーク ローミング	○
オンデマンド VPN (宛先により起動)	あり。オンデマンドで Apple iOS Connect と互換性があります。
オンデマンド VPN (アプリケーションによって起動)	あり。アプリケーション単位 VPN モードで動作している場合のみ。
キー再生成	○
IPv4 パブリック トランスポート	○
IPv6 パブリック トランスポート	○
IPv4 over IPv4 トンネル	○
IPv6 over IPv4 トンネル	○
IPv6 over IPv4 トンネル	○
IPv6 トンネルを介した IPv6	○

カテゴリ：機能	Apple iOS
デフォルトドメイン	○
DNS サーバの設定	○
プライベート側プロキシサポート	○
プロキシ例外	あり。ただし、ワイルドカードの仕様はサポートされていません。
パブリック側プロキシサポート	いいえ
ログイン前バナー	○
ログイン後バナー	○
DSCP の保存	いいえ
接続と切断：	
VPN ロード バランシング	○
バックアップ サーバ リスト	○
最適ゲートウェイ選択	いいえ
Authentication:	
SAML 2.0	○
クライアント証明書認証	○
オンライン証明書ステータス プロトコル (OCSP)	いいえ
手動によるユーザ証明書の管理	○
手動によるサーバ証明書の管理	○
レガシー SCEP の登録	いいえ
SCEP プロキシの登録	○
自動証明書選択	○
手動による証明書の選択	○
スマートカードのサポート	いいえ
ユーザ名およびパスワード	○
トークン/課題	○
二重認証	○
グループ URL (サーバアドレスで指定)	○
グループの選択 (ドロップダウン選択)	○
ユーザ証明書からのクレデンシャルの事前入力	○

カテゴリ：機能	Apple iOS
パスワードの保存	いいえ
ユーザ インターフェイス：	
スタンドアロン GUI	○
ネイティブ OS GUI	あり。機能制限があります。
API/URI ハンドラ（以下を参照）	○
UI のカスタマイゼーション	いいえ
UI のローカリゼーション	あり。アプリケーションには事前にパッケージ化された言語が含まれています。
ユーザ設定	○
ワンクリック VPN アクセス用のホーム画面のウィジェット	いいえ
AnyConnect に固有のステータス アイコン	いいえ
モバイル ポスチャ： （AnyConnect Identity Extension (ACIDex)）	
シリアル番号または固有 ID のチェック	○
ヘッドエンドと共有される OS および AnyConnect のバージョン	○
AnyConnect NVM のサポート	いいえ
URI の処理：	
接続エントリの追加	○
VPN への接続	○
接続時のクレデンシャルの事前入力	○
VPN の解除	○
証明書のインポート	○
ローカリゼーションデータのインポート	○
XML クライアントプロファイルのインポート	○
URI コマンドの外部（ユーザ）制御	○
レポートおよびトラブルシューティング：	
統計情報（Statistics）	○
ロギング/診断情報（DART）	○

カテゴリ：機能	Apple iOS
認定：	
FIPS 140-2 レベル 1	○

* オペレーティングシステムの実装による ASA の設定に関係なく、iOS デバイスに対してローカル LAN アクセスが有効になります。

適応型セキュリティ アプライアンスの要件

次の機能には、ASA の最小リリースが必要です。



(注) 現在の AnyConnect Mobile リリースでこれらの機能を使用できるかどうかを確認するには、お使いのプラットフォームの機能マトリックスを参照してください。

- SAML 認証機能を使用するには、ASA 9.7.1.24、9.8.2.28、9.9.2.1 以降にアップグレードする必要があります。クライアントとサーバ両方のバージョンが最新であることを確認してください。
- TLS 1.2 を使用するには、ASA 9.3.2 以降にアップグレードする必要があります。
- アプリケーション単位 VPN トンネリング モードを使用するには、ASA 9.3.2 以降にアップグレードする必要があります。
- 次のモバイル機能を使用するには、ASA 9.0 にアップグレードする必要があります。
 - IPsec IKEv2 VPN
 - Suite B 暗号化
 - SCEP プロキシ
 - モバイル ポスチャ
- ASA リリース 8.0(3) および Adaptive Security Device Manager (ASDM) 6.1(3) は、モバイル端末の AnyConnect をサポートする最小リリースです。

その他のシスコ ヘッドエンドのサポート

AnyConnect SSL 接続は、Cisco IOS 15.3(3)M 以降/15.2(4)M 以降でサポートされています。

AnyConnect IKEv2 接続は、Cisco ISR g2 15.2(4)M 以降でサポートされています。

AnyConnect SSL および IKEv2 は、Cisco Firepower Threat Defense リリース 6.2.1 以降でサポートされています。

Apple iOS での AnyConnect の注意事項と制約事項

- AnyConnect の設定は、ユーザ（手動で）または iPhone 設定ユーティリティ（<http://www.apple.com/support/iphone/enterprise/>）によって生成する AnyConnect VPN クライアントプロファイルによって行うか、エンタープライズ モバイルデバイス マネージャを使用して行うことができます。
- Apple iOS デバイスは 1 つの AnyConnect VPN クライアント プロファイルのみサポートします。生成された設定の内容は、必ず最新のプロファイルと一致します。たとえば、ユーザが `vpn.example1.com` に接続してから `vpn.example2.com` に接続すると、`vpn.example2.com` からインポートされた AnyConnect VPN クライアントプロファイルにより、`vpn.example1.com` からインポートされたクライアント プロファイルが置き換えられます。
- このリリースは、トンネル キープアライブ機能をサポートしています。ただし、デバイスのバッテリー寿命は短くなります。アップデート間隔の値を増やすことでこの問題は軽減します。
- **DHE の非互換性**
AnyConnect リリース 4.6 で導入された DHE 暗号サポートにより、ASA 9.2 より前の ASA バージョンで非互換性の問題が発生します。9.2 より前の ASA リリースで DHE 暗号を使用している場合、これらの ASA バージョンで DHE 暗号を無効にする必要があります。

Apple iOS Connect On-Demand の注意事項：

- iOS On-Demand ロジックの結果として自動的に接続され、Disconnect on Suspend（一時停止時に接続解除）が設定されている VPN セッションは、デバイスがスリープすると切断されます。デバイスがスリープ状態から起動すると、必要に応じて On-Demand ロジックが VPN セッションを再接続します。
- AnyConnect は、UI が起動され、VPN 接続が開始されたときにデバイス情報を収集します。そのため、ユーザが iOS の Connect on Demand 機能を使用して最初に接続を行う場合、または OS バージョンなどのデバイス情報が変更された後、AnyConnect がモバイル ポスチャ情報を誤ってレポートする状況が発生します。
- これは、Apple Connect-on-Demand 機能を使用していて、4.0.05032 より前の Legacy AnyConnect リリース、または 9.3 より前の Apple iOS リリースを実行している場合にのみ、お使いの環境に適用されます。AnyConnect の更新後に Connect On-Demand VPN トンネルが適切に確立されるようにするには、ユーザが AnyConnect アプリを手動で開始して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。

Cisco AnyConnect と Legacy AnyConnect は、異なるアプリ ID を持つ異なるアプリです。次に例を示します。

- AnyConnect アプリを、レガシー 4.0.05x 以前のバージョンから新しい 4.6.x バージョンにアップグレードすることはできません。Cisco AnyConnect 4.6x は別のアプリで、別の名前とアイコンを使用してインストールされています。
- AnyConnect の異なるバージョンは、モバイルデバイスに共存できますが、これはシスコではサポートされません。両方のバージョンの AnyConnect がインストールされている状況で接続しようとする、予期せぬ動作が発生する恐れがあります。デバイスにインストールされている AnyConnect アプリは 1 つだけで、デバイスと環境に適したバージョンであるようにしてください。

- Legacy AnyConnect バージョン 4.0.05069 以前のリリースを使用してインポートされた証明書は、新しい AnyConnect アプリケーションのリリース 4.0.07072 ではアクセスおよび使用ができません。MDM で導入された証明書は、両方のアプリ バージョンでアクセスおよび使用ができます。
- 証明書やプロファイルなどの、Legacy AnyConnect アプリにインポートされたアプリ データは、新しいバージョンに更新する場合、削除する必要があります。そうしないと、システムの VPN 設定で引き続き表示されます。Legacy AnyConnect アプリをアンインストールする前にアプリ データを削除します。
- 現在の MDM プロファイルでは、新しいアプリはトリガーされません。EMM ベンダーは、VPNType (VPN)、VPNSubType (com.cisco.anyconnect)、および ProviderType (パケットトンネル) をサポートする必要があります。AnyConnect は新しいフレームワークで ISE にアクセスできなくなるため、ISE と統合させるには UniqueIdentifier を AnyConnect に渡せる必要があります。設定方法については、EMM ベンダーにお問い合わせください。カスタム VPN タイプが必要な場合もあれば、リリース時にはサポートされていない場合もあります。

AnyConnect 4.6.x 以降で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x からの動作が次のように変更されます。

- ヘッドエンドに送信されたデバイス ID は、新しいバージョンでは UDID ではなく、初期設定へのリセット後には、同じデバイスで作成されたバックアップからデバイスが復元されない限り、デバイス ID が異なるものになります。
- MDM で導入された証明書だけでなく、AnyConnect で利用可能ないずれかの方法 (SCEP、UI 使用 - 手動で、URI ハンドラ) を使用してインポートされた証明書も使用できます。AnyConnect の新しいバージョンでは、電子メールまたはこれらの識別されたもの以外のメカニズムを使用してインポートした証明書を使用できなくなりました。
- UI を使用して接続エントリーを作成する際には、表示された iOS セキュリティ メッセージを受け入れる必要があります。
- AnyConnect VPN プロファイルからダウンロードしたホストエントリーと同じ名前のユーザが作成したエントリーは、アクティブであれば切断されるまで名前の変更されません。また、ダウンロードされたホスト接続エントリーは、接続が維持されている間ではなく、接続が解除された後に UI に表示されます。

既知の互換性の問題

AnyConnect 4.7. xxxxx

- スプリット除外設定で IPv6 のみをトンネリングする場合 (IPv4 アドレスが割り当てられていない場合)、ASA ヘッドエンドへのスプリット トンネリングは機能しません。

除外リスト エントリーを除き、すべてのトラフィックをトンネリングする必要がありますが、スプリット除外リストは適用されません。すべての IPv6 トラフィックは除外されます。詳細については、「CSCvb80768 : IPv6 Split Exclude & IPv4 DropAll がトンネルからのすべての v6 トラフィックを除外」を参照してください。(レーダー 29623849)。

- AnyConnect UI が開いたままの状態、iOS が UI と内部の AnyConnect 拡張機能の間のプロセス間通信 (IPC) を誤って切断した場合、UI アクティビティはエラーまたは不正な応答により失敗します。

これを回復するには、IPCを再確立するAnyConnect UIを閉じてから再起動する必要があります。UIが閉じられたときに予期しないIPC切断が発生した場合、次回UIを開くときに、再確立されます。詳細については、「CSCvb95722：失敗して一時停止状態になります（レーダー 29313229）」を参照してください。

- オンデマンド接続の場合は、更新されたVPN接続プロファイルがASAによってクライアントにプッシュされたときに、AnyConnect UIを開く必要があります。UIが開かれていない場合、更新されたプロファイルは同期されないため、変更は使用されません。

残念ながら、新しいプロファイルを同期するためにUIを開くことをユーザーに示すことはありません（Legacy AnyConnectと同様）。したがって、更新された接続エントリが使用されない可能性があります。現時点では回避策はありません。詳細については、「CSCvc35923：オンデマンドACを使用すると、更新された接続プロファイル（レーダー 30173053）を同期するためにACを開く必要があることをユーザに通知できません。」を参照してください。

- 管理対象のアプリケーションごとの設定では、アプリケーショントラフィックは、アプリケーションごとに設定され、不適切なタイミングでユーザが作成した（管理対象外の）VPN接続を通過します。

詳細については、「CSCvc36024：アプリケーション別：アプリケーションは、非PAVフルトンネル（レーダー 29513803）を介してトラフィックを渡すことができます。」を参照してください。

未解決および解決済みのAnyConnectの問題

Cisco バグ検索ツール<https://tools.cisco.com/bugsearch/>には、このリリースで未解決および解決済みの次の問題に関する詳細情報が含まれています。バグ検索ツールにアクセスするには、シスコアカウントが必要です。シスコアカウントをお持ちでない場合は、<https://tools.cisco.com/RPF/register/register.do>で登録を行ってください。

Apple iOS のAnyConnect 4.7.03051 の解決済みの問題

ID	見出し
CSCvo90908	証明書の有効期限のしきい値警告が表示されない
CSCvp58245	SAML認証に失敗すると、[グループ選択（group selection）]ページが開くが、[ブラウザを開く（Open Browser）]ボタンが機能しない

Apple iOS のAnyConnect 4.7.02025 の解決済みの問題

ID	見出し
CSCvo51294	11 インチ iPad Pro で AnyConnect がフルスクリーンで実行されない
CSCvn79145	クリーンアップログの保存/拡張機能の回復
CSCvo68322	iPad におけるマルチタスキング機能の導入
CSCvn54093	表示項目がアクセシビリティテキスト設定の変更によって重複する可能性がある
CSCvo79007	[VPN 詳細（VPN detail）]ページにロードされたパターンイメージは、イメージビューを完全にカバーしていない

ID	見出し
CSCvo83166	AnyConnect iOS のクリーンアップが終了時にクラッシュする

Apple iOS の AnyConnect 4.7.01075 の解決済みの問題

ID	見出し
CSCvn79065	既存の設定を更新する前に別のアクティブ VPN 設定を選択すると、AnyConnect アプリケーションがクラッシュする
CSCvn79145	クリーンアップ ログの保存/拡張機能の回復
CSCvn79766	AnyConnect の著作権を2019に更新
CSCvn76993	iOS クライアントがスリープ/ウェイク時にクラッシュを確認する
CSCvo20866	より多くのネットワーク拡張ロギングのクリーンアップ
CSCvo36249	[検疫 (quarantine)]ダイアログで[切断 (Disconnect)]を選択すると、ステータスが [接続 (connected)]と表示され、すべてのトラフィックがブロックされる

Apple iOS の AnyConnect 4.7.00139 の解決済みの問題

ID	見出し
CSCvm12157	SVC メッセージ : 17/ERROR : 再接続してエラーから回復します。

AnyConnect Apple iOS の未解決の問題

ID	見出し
CSCuz38311	AAAA 応答が遅い場合の iOS 4.0.05032/5036 低速接続の確立
CSCuz39092	iOS : 4.0.05036 Clarify Drop All Traffic text
CSCvb31542	iOS : 内部 CRL を使用したアプリケーション単位の SafariDom 内部サイトにエラー R #28176408 が発生する
CSCuy41307	AnyConnect 接続ステータスが同期されていない
CSCuy99092	[ios] IPSec トラフィックを通過させるには、tungrp で MTU を1380以下にする必要があります

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2019 Cisco Systems, Inc. All rights reserved.

【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。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10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。



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>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>