Cisco AnyConnect Secure Mobility Client Android 向けリリース 4.9.x リリースノート

Android 向け AnyConnect リリースノート

Android モバイル デバイス 向け AnyConnect

AnyConnect Secure Mobility Client により、リモート ユーザーは 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 セキュア モビリティ クライアントと適応型セキュリティアプライアンス（ASA）5500 のシステム管理者向けに作成されたこのドキュメントは、上で動作する AnyConnect のリリースに固有の情報を提供します。Android デバイス

AnyConnect アプリケーションは、入手できます。Amazon.com で使用可能な Kindle パッケージを除き、Google Play でシスコでは、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 ライセンスまたは Apex ライセンスが必要です。トライアルライセンスを使用できます（Cisco AnyConnect Ordering Guide）。

最新のエンドユーザーライセンス契約については、『Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 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。 Open Source Software Used In Cisco AnyConnect Secure Mobility Client Release 4.x for Mobile

Cisco AnyConnect Android ベータ テスト

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。

これらのバージョンを受け取れるようにするには、次の Google Play のリンクでオプトインしてベータ ビルドを受け取ります。
https://play.google.com/apps/testing/com.cisco.anyconnect.vpn.android.avf

この Google Play 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。

Android でサポートされるデバイス

Cisco AnyConnect on Android のフル サポートは、Android 4.0（Ice Cream Sandwich）から最新リリースまでの Android を搭載するデバイスで提供されます。

Android 用の AnyConnect Umbrella モジュールを使用するには、Android 6.0 以降が必要です。

Kindle Fire HD デバイスと新しい Kindle Fire 向けの AnyConnect for Kindle Fire HD を Amazon から入手できます。AnyConnect for Kindle は、AnyConnect for Android パッケージと同じ機能を備えています。

現在のすべての Chromebook では、AnyConnect for Android が公式にサポートされており、ChromeOS で最適な AnyConnect エクスペリエンスを実現するために強く推奨されています。ネイティブ ChromeOS クライアントは、Android アプリケーションを実行できないレガシー Chromebook 専用です。

Per App VPN は、管理型環境および非管理型環境でサポートされています。Samsung KNOX MDM を使用する管理型環境では、Android 4.3 以降で Samsung Knox 2.0 を実行する Samsung デバイスが必要です。非管理型環境で Per App を使用する場合は、一般的な Android のメソッドが使用されます。

Network Visibility Module（NVM）機能に関しては、Android 7.0 以降を必要とする Samsung Knox 2.8 以降（3.3 を含む）を実行する Samsung デバイスが必要です。NVM の設定には、AnyConnect 4.4.3 以降の AnyConnect プロファイル エディタも必要です。それより前のリリースでは、モバイル NVM の設定はサポートされていません。

インストールおよびアップグレードの手順については、Cisco AnyConnect Secure Mobility Client の Android 向けユーザーガイドを参照してください。

Android 用の AnyConnect Umbrella モジュール

リリース 4.8.03645（以降）では、Android 6.0.1 以降のデバイス向けの Cisco AnyConnect Umbrella モジュールが提供されます。この管理対象 Android デバイス用のローミングクライアントは DNS レイヤ保護を提供します。この保護は、ワークプロファイルでカバーされるアプリケーションとブラウジングの両方に拡張されます。

モバイルデバイス管理システム (MDM) は、このクライアントを Android デバイスに展開し、Umbrella 設定を Android デバイスにプッシュするために必要です。サポートされている MDM およびその他の前提条件のリストについては、「Android OS で AnyConnect の Umbrella モジュールを展開するための前提条件」を参照してください。

機能によっては、次のような機能が制限されることがあります。

- アプリケーションごとの VPN は、OS の制限により、Umbrella モジュールでは機能しません。リモートアクセス VPN がアクティブな場合、Umbrella による保護は、VPN トンネルによって代行受信された DNS トラフィックにのみ適用されます。アプリケーションごとの VPN に対してリモートアクセスが設定されている場合は、トンネル化されたアプリケーションの DNS トラフィックに対してのみ、Umbrella による保護が適用されます。
- Umbrella による保護を使用する場合、常時接続 VPN は、ロックダウン（フェールクローズ）オプションとともに使用しないでください。これは、VPN サーバーに到達できない場合にユーザーのインターネットアクセスが停止されるためです。常時接続がオンになっている場合にロックダウン設定をオフにするには、MDM ガイドを参照してください。

Umbrella 完全機能セットの説明については、「Umbrella Module for AnyConnect (Android OS)」を参照してください。

Android での Umbrella のライセンス要件

Android 用の AnyConnect Umbrella モジュールは、AnyConnect ライセンスの有無にかかわらず有効にできます。AnyConnect ソフトウェアライセンスの詳細については、『Cisco AnyConnect Ordering Guide』を参照してください。管理者は、トライアル版の AnyConnect Apex（ASA）ライセンスを http://www.cisco.com/go/license から入手できます。Android で AnyConnect を利用するには、Cisco Adaptive Security Appliance（ASA）ブートイメージ 8.0(4) 以降が必要です。ライセンスに関する質問と評価用ライセンスについては、ac-temp-license-request@cisco.com にお問い合わせください。その際、Cisco ASA から実行した **show version** コマンドの出力のコピーを提供してください。

AnyConnect 上の Umbrella モジュールには Umbrella ライセンスが必要です。詳細については、https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-package-comparison-2 をクリックしてください。

Android OS で AnyConnect の Umbrella モジュールを展開するための前提条件

展開の前提条件：

（注） AnyConnect は、MDM で作成されたワークプロファイル内のアプリとブラウザから生成されたトラフィックをモニタし、それに応じて閲覧をブロックまたは許可します。アプリケーションやブラウザによってワークプロファイルの外部で生成されたトラフィックはモニタされません。

- ソフトウェアを展開し、Umbrella設定をモバイルデバイスにプッシュするためのモバイルデバイス管理システム（MDM）。現在テスト済みのバージョンは、Mobile Iron、Meraki、VMWare Workspace 1（AirWatch）、または Microsoft Intune です。
- Android OS バージョン 6.0.1 以降を搭載した Android（Samsung/Google Pixel）モバイルデバイス。
- DNS ポリシーの設定、登録済みAndroidデバイスの管理、およびレポートのためのUmbrellaライセンス。
- 機能を有効にするための Umbrella 組織 ID。
- 信頼ネットワーク検出（TND）の場合：
  - Umbrella モジュールは、HTTPS が有効な仮想アプライアンス（VA）を検出すると、それ自身を非アクティブにします。ただし、VA が HTTPS をサポートしていない場合は、Umbrella モジュールが動作を続行します。
  - umbrella_va_fqdns 内のすべての VA FQDN を有効にする必要があります。

新機能

Android モバイルデバイス向け AnyConnect 4.9.06048 の新機能

このバージョンの Android 向け AnyConnect はメンテナンスリリースで、VPN 関連の問題が発生することはありません。

Android モバイルデバイス向け AnyConnect 4.9.06039 の新機能

このバージョンの Android 向け AnyConnect には、次の機能およびサポートの更新が含まれます。

- NVM で DTLS を介してコレクタに安全にデータを送信するかどうかを決定する機能。
- ASA の新しい未リリースバージョンに接続する際の DTLS セッションの障害に対処するために、CiscoSSL ライブラリが更新されました。

Android モバイルデバイス向け AnyConnect 4.9.04035 の新機能

Android 向け AnyConnect のこのバージョンでは、VPN 接続用のサーバー名識別（SNI）のサポートが追加されています。

Android モバイルデバイス向け AnyConnect 4.9.00576 の新機能

このバージョンの Android 向け AnyConnect には、VPN 関連の問題はありません。

Android モバイルデバイス向け AnyConnect 4.9.00564 の新機能

このバージョンの Android 向け AnyConnect では、Android 向け AnyConnect 4.9.00564 で解決済みの問題 （15 ページ）に記載されている不具合が解消されます。

Android モバイルデバイス向け AnyConnect 4.9.00548 の新機能

このバージョンの Android 向け AnyConnect では、次の機能およびサポートの更新が提供されます。

- OpenSSL（Cisco SSL）ライブラリの更新
- SSL VPN の場合、AnyConnect は TLS と DTLS の両方からの暗号スイート、DHE-RSA-AES256-SHA と DES-CBC3-SHA をサポートしなくなりました。
- IKEv2/IPsec については、AnyConnect は次のアルゴリズムをサポートしなくなりました。
  - 暗号化アルゴリズム：DES と 3DES
  - 疑似ランダム関数（PRF）アルゴリズム：MD5
  - 整合性アルゴリズム：MD5
  - Diffie-Hellman（DH）グループ：2、5、14、24
- Umbrella ユーザー ID のサポートが追加されました。管理対象デバイスが Umbrella ダッシュボードに表示され、特定のデバイスまたはすべてのデバイスにポリシーを個別に適用できます。詳細については、『Cisco Umbrella Module v1.1 for AnyConnect for Android OS』を参照してください。

Android での Google に関する既知の問題

Android OS での Google による制限により、Umbrella AnyConnect モジュールを有効にすると、Google Play ストアでのアプリのダウンロードが失敗する場合があります。この問題を回避するには、Umbrella モジュールを有効にする前にアプリをダウンロードします。Google は Android OS「Q」でこの動作を修正しました。詳細については、「Google Issue Tracker」を参照してください。

Android 向け AnyConnect の機能マトリックス

次の表に Cisco AnyConnect on Android でサポートされるリモート アクセス機能を示します。

カテゴリ：機能	Android VPN
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	対応

カテゴリ：機能	Android VPN
Cisco VPN プロファイルのサポート（手動インポート）	対応
Cisco VPN プロファイルのサポート（接続中のインポート）	対応
MDM 設定の接続エントリ	対応
ユーザー設定の接続エントリ	対応
トンネリング：	
TLS	対応
データグラム TLS（DTLS）	対応
IPsec IKEv2 NAT-T	対応
IKEv2 - raw ESP	対応
Suite B（IPSec のみ）	対応
TLS 圧縮	対応
デッド ピア検出	対応
トンネル キープアライブ	対応
複数のアクティブ ネットワーク インターフェイス	非対応
アプリケーションごとのトンネリング	対応。Android 5.0 以上または Samsung Knox。
アプリケーションごとのトンネリング（許可されていないアプリケーションモード）	対応
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）	対応
スプリット トンネル（スプリットを含む）	対応
ローカル LAN（スプリットを含まない）。	非対応
Split-DNS	対応。スプリットによる処理を含みます。
自動再接続/ネットワーク ローミング	対応。自動再接続プロファイルの指定にかかわらず、ユーザーが 3G と WiFi ネットワークの間を移動するときに、AnyConnect Mobile は VPN を常に維持します。
オンデマンド VPN（宛先により起動）	非対応
オンデマンド VPN（アプリケーションによって起動）	非対応
キー再生成	対応
IPv4 パブリック トランスポート	対応

カテゴリ：機能	Android VPN
IPv6 パブリック トランスポート	対応。Android 5.0 以降が必要です。
IPv4 over IPv4 トンネル	対応
IPv4 over IPv6 トンネル	対応
IPv6 over IPv4 トンネル	対応
IPv6 over IPv6トンネル	対応
デフォルト ドメイン	対応
DNS サーバーの設定	対応
プライベート側プロキシ サポート	Android 10 の直接プロキシモードのみをサポートします。
プロキシ例外	非対応
パブリック側プロキシ サポート	非対応
ログイン前バナー	対応
ログイン後バナー	対応
DSCP の保存	対応
接続と切断：	
VPN ロード バランシング	対応
バックアップ サーバー リスト	対応
最適ゲートウェイ選択	非対応
認証：	
Touch ID	非対応
SAML 2.0	対応
クライアント証明書認証	対応
オンライン証明書ステータス プロトコル（OCSP）	対応
手動によるユーザー証明書の管理	対応
手動によるサーバー証明書の管理	対応
SCEP レガシー登録（お使いのプラットフォームを確認してください）	対応
SCEP プロキシ登録（お使いのプラットフォームを確認してください）	対応
自動証明書選択	対応
手動による証明書の選択	対応

カテゴリ：機能	Android VPN
スマート カードのサポート	非対応
ユーザー名およびパスワード	対応
トークン/課題	対応
二重認証	対応
グループ URL（サーバー アドレスで指定）	対応
グループの選択（ドロップダウン選択）	対応
ユーザー証明書からのクレデンシャルの事前入力	対応
パスワードの保存	非対応
ユーザー インターフェイス：	
スタンドアロン GUI	対応
ネイティブ OS GUI	非対応
API/URI ハンドラ（以下を参照）	対応
UI のカスタマイゼーション	非対応
UI のローカリゼーション	対応（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）
ユーザー設定	対応
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	対応
AnyConnect に固有のステータス アイコン	オプション
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	対応
ヘッドエンドと共有される OS および AnyConnect のバージョン	対応
AnyConnect NVM のサポート	対応。Samsung Knox と MDM に関して特定の要件があります。
URI の処理：	
接続エントリの追加	対応
VPN への接続	対応
接続時のクレデンシャルの事前入力	対応

カテゴリ：機能	Android VPN
VPN の解除	対応
証明書のインポート	対応
ローカリゼーション データのインポート	対応
XML クライアント プロファイルのインポート	対応
URI コマンドの外部（ユーザー）制御	対応
レポートおよびトラブルシューティング：	
統計	対応
ロギング/診断情報（DART）	対応
認定：	
FIPS 140-2 レベル 1	対応

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ー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。

Android での AnyConnect の注意事項と制約事項

- ASA は、AnyConnect for Android のディストリビューションと更新プログラムを提供しません。Google Play から入手できます。最新バージョンの APK（パッケージ）ファイルも Cisco.com に掲載されています。
- AnyConnect for Android は Network Visibility Module と Umbrella のみサポートし、他の AnyConnect モジュールはサポートしていません。
- Android デバイスでは 1 つの AnyConnect プロファイル（ヘッドエンドから受信した最後のプロファイル）だけがサポートされます。ただし、プロファイルは複数の接続エントリで構成できます。
- ユーザが、サポートされていないデバイスに AnyConnect をインストールしようとすると、「`Installation Error: Unknown reason -8`」というポップアップ メッセージが表示されます。これは Android OS により生成されるメッセージです。
- ユーザがホーム スクリーンに AnyConnect ウィジェットを表示している場合、[起動時に開く（Launch at startup）] 設定に関わらず AnyConnect サービスが自動的に開始されます（ただし接続は確立されません）。
- AnyConnect for Android では、クライアント証明書からの事前入力を使用する場合に、拡張 ASCII 文字のために UTF-8 文字エンコードが必要です。事前入力機能を使用する場合は、クライアント証明書が UTF-8 でなければなりません（KB-890772 および KB-888180 の説明を参照）。
- AnyConnect は、EDGE の固有の性質およびその他の早期無線テクノロジーによって EDGE 接続上の VPN トラフィックを送受信する場合、ボイスコールをブロックします。
- いくつかのよく知られているファイル圧縮ユーティリティでは、[AnyConnect ログ送信（AnyConnect Send Log）] ボタンを使用してパッケージされたログ バンドルを圧縮解除できません。回避策として、AnyConnect ログ ファイルの圧縮解除には Windows および MacOS のネイティブユーティリティを使用してください。
- 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。

Google Play ストアの Android

シスコでは、すべてのユーザーに、Google Play ストアで入手できる Android リリースの最新バージョンを使用することを強くお勧めします。さらに、.apk バージョンは、最新バージョン用のもののみ Cisco.com で入手できます。Google Play ストアを利用できない場合、AnyConnect ソフトウェア ダウンロード ページにアクセスできる管理者は、このバージョンを入手できます。

既知の互換性の問題

- Android 10 の VPN トンネルで接続の問題が発生している場合は、Android 10 のプライベート DNS 機能を無効にしてみてください。
- パブリック インターフェイスとプライベート インターフェイスにおける IPv6。

  IPv6 は、AnyConnect 4.05015 以降を使用するプライベートおよびパブリック トランスポートの両方でサポートされており、Android 5 以降で対応しています。この組み合わせにより、IPv6 トンネルを介した IPv4 および IPv6 トンネルを介した IPv6 が可能になります。

  以前のバージョンの AnyConnect と Android リリースで従来から使用できたトンネル設定（IPv4 トンネルを介した IPv4 および IPv4 トンネルを介した IPv6）も引き続き使用できます。

  

  注 Android に存在する既知の問題（Issue #65572）が原因で、IPv6 over IPv4 は Android 4.4 上で機能しません。Android 5 以降を使用する必要があります。

- バッテリ セーバーおよび AnyConnect：
  - Android 5.0 では、デバイスでのバックグラウンド ネットワーク接続をブロックするバッテリ セーバー機能が導入されました。バッテリ セーバーを有効にした場合、AnyConnect がバックグラウンドで実行されると、一時停止状態に移行します。Android 5.0 でこれを回避するには、デバイス設定でバッテリ セーバーをオフにすることができます（[設定（Settings）] -> [バッテリ（Battery）] -> [バッテリ セーバー（Battery saver）] または通知バーから）。
  - Android 6.0+ では、AnyConnect がバッテリセーバーが原因で一時停止状態に移行する場合、AnyConnect の部分をバッテリセーバーモードから許可リストに登録するオプションを選択できるポップアップが表示されます。AnyConnect の部分を許可リストに登録すると、バックグラウンドで実行する AnyConnect の機能に影響を与えずにバッテリを節約できます。
  - バッテリセーバーが原因で AnyConnect が一時停止した場合、バッテリセーバーをオフにするか AnyConnect を許可リストに追加するかに関係なく、AnyConnect を一時停止状態から戻すには手動で再起動する必要があります。

- スプリット DNS は、Android 4.4 デバイスでは機能しません。また、Samsung 製の Android 5.x デバイスでも機能しません。Samsung デバイスの場合、唯一の回避策は、スプリット DNS を無効にしてグループに接続することです。その他のデバイスでは、Android 5.x にアップグレードして、この問題の修正を入手する必要があります。

  これは、Android 4.4 に存在する既知の問題（ Issue #64819）によるもので、Android 5.x で修正されましたが、Samsung 製の Android 5.x デバイスには組み込まれませんでした。

- Android 5.x のバグ（Google Issue #85758、Cisco Issue # CSCus38925）が原因で、AnyConnect アプリケーションを Recent Apps 画面から閉じると、正しく動作しない場合があります。正常な動作を復元するには、AnyConnect を [設定（Settings）] で停止してから、再起動します。

- Samsung モバイル デバイスでは、[設定（Settings）] > [Wi-Fi] > [スマート ネットワーク スイッチ（Smart network switch）] で、安定したインターネット接続を維持するために Wi-Fi から LTE に切り替えることができます（Wi-Fi 接続が最適でない場合）。この場合も、アクティブな VPN トンネルが一時停止し、再接続します。何度も繰り返し再接続することになるため、この機能を無効にすることをお勧めします。

- 複数のアクティブ ユーザーをサポートする Android 5.0（Lollipop）で、VPN 接続はデバイス上のすべてのユーザーではなく、単一のユーザーのデータのみをトンネルします。バックグラウンド データ フローが暗号化されずに発生する可能性があります。

- Android 4.3.1 のバグ（Google Issue #62073）が原因で、AnyConnect ICS+ パッケージを使用するユーザーは、非完全修飾ドメイン名を入力できません。たとえば、「internalhost」と入力できずに、「internalhost.company.com」と入力する必要があります。

- Android 4.3 への HTC One 上の AT&T ファームウェアのアップデート（ソフトウェア バージョン：3.17.502.3）は、「HTC AnyConnect」をサポートしていません。お客様は「AnyConnect HTC」をアンインストールし、「AnyConnect ICS+」をインストールする必要があります（HTC AnyConnect は、3.22.1540.1 ソフトウェア バージョンのインターナショナル エディションでは機能します）。デバイスのソフトウェア バージョンは、[設定（Settings）] > [端末情報（About）] > [ソフトウェア情報（Software information）] > [ソフトウェア番号（Software number）] で確認します。

- 管理者が Android トンネルの MTU を 1280 以下に設定した場合に VPN 接続が失敗するという Google Issue #70916 が、Android 5.0（Lollipop）で解決されたことをご報告します。次の問題情報は、参考のために提供します。

  Android 4.4.3 でのバグの再発のため（Google Issue #70916、Cisco CSCup24172）、管理者が Android トンネルの MTU を 1280 以下に設定した場合に、VPN 接続が失敗します。この問題はすでに Google に報告されています。Android 4.4.3 で再発したバグを修正するには、新しいバージョンの OS が必要になります。この問題を回避するには、ヘッドエンドの管理者はトンネル MTU を 1280 より小さい値に設定しないようにします。

  問題が発生すると、エンド ユーザーに「System configuration settings could not be applied.A VPN connection will not be established」というメッセージが表示され、AnyConnect のデバッグ ログで以下が報告されます。

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling
```

```
 client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark
 rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()

File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult
AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- Android 4.4（KitKat）のバグ Google Issue #61948（AnyConnect ユーザーが VPN 接続で大量のパケット損失を経験する/タイムアウトが発生する）が Google の Android 4.4.1 のリリース（Google がソフトウェアアップデートを介して一部のデバイスに配布を開始しました）で解決されたことをご報告します。次の問題情報は、参考のために提供します。

  Android 4.4 のバグ（Issue #61948、Cisco サポートの更新 [英語] も参照してください）が原因で、AnyConnect ユーザーは VPN 接続で大量のパケット損失を経験します。これは、Android 4.4 で AnyConnect ICS+ を実行する Google Nexus 5 で確認されています。ユーザーは、特定のネットワーク リソースにアクセスしようとすると、タイムアウトを経験します。また、ASA ログには、「大きいパケット 1420 バイト（しきい値 1405 バイト）を送信（Transmitting large packet 1420 (threshold 1405)）」のようなテキストの syslog メッセージが表示されます。

  Google が Android 4.4 用の修正を作成するまで、VPN 管理者は sysopt connection tcpmss <mss size> を設定することにより、ASA 上の TCP 接続のための最大セグメント サイズを一時的に小さくすることができます。このパラメータのデフォルトは 1380 バイトです。ASA ログに表示される値の差に応じてこの値を小さくします。上記の例では、差は 15 バイトです。値を 1365 未満にする必要があります。この値を小さくすると、大きなパケットを送信する接続済みの VPN ユーザーのパフォーマンスに悪影響を及ぼします。

- AnyConnect for Android で、464xlat と呼ばれる IPv6 移行メカニズムを使用してモバイル ネットワークに接続すると、接続の問題が生じる場合があります。影響を受けることが確認されているデバイスには、T-Mobile US ネットワークに接続している Samsung Galaxy Note III LTE があります。このデバイスは、デフォルトで IPv6 モバイル ネットワーク接続のみを使用します。接続を試行すると、デバイスを再起動するまで、モバイル接続が失われることがあります。

この問題を防止するには、AnyConnect ICS+ アプリケーションを使用し、IPv4 ネットワーク接続を取得するか、Wi-Fi ネットワークを使用して接続するようにデバイス設定を変更します。T-Mobile USA ネットワークに接続している Samsung Galaxy Note III LTE の場合、T-Mobile によって提供されている手順 [英語] に従って、デバイスのアクセス ポイント名（APN）を設定します（[APN プロトコル（APN Protocol）] が [IPv4] に設定されていることを確認します）。

- VPN 内のプライベート IP アドレスの範囲がクライアント デバイスの外部インターフェイスの範囲とオーバーラップすると、AnyConnect ICS+ パッケージに問題が発生することがあります。このルートのオーバーラップが発生すると、ユーザーは VPN に正常に接続できますが、実際には何にもアクセスできません。この問題は、NAT（ネットワーク アドレス変換）を使用し、アドレスを 10.0.0.0 ～ 10.255.255.255 の範囲内に割り当てている携帯電話ネットワークで確認されています。またこの問題は、AnyConnect で Android VPN フレームワークのルート制御が制限されていると発生します。ベンダー固有の Android パッケージに完全なルーティング制御があると、このようなシナリオではより良く機能する場合があります。
- Android 4.0（ICS）を実行する Asus タブレットで、TUN ドライバが失われることがあります。これにより、AVF AnyConnect が失敗します。
- Android セキュリティ ルールによって、VPN 接続がアップ状態の間、デバイスのマルチメディア メッセージング サービス（MMS）メッセージの送受信が阻止されます。ほとんどのデバイスとサービス プロバイダでは、VPN 接続がアップ状態の間に MMS メッセージを送信しようとすると通知が表示されます。Android では VPN に接続していないときにメッセージの送受信が許可されます。
- Google Isssue 41037 が原因で、クリップボードからテキストを貼り付けるときに、テキストの前にスペースが挿入されます。AnyConnect では、ワンタイム パスワードなどのテキストをコピーする場合は、ユーザーがこの不要な空白文字を削除する必要があります。

未解決および解決済みの AnyConnect の問題

Cisco Bug Search Tool 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。Bug Search Tool 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://Cisco.com で登録を行ってください。

デスクトップリリースノート（https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/release/notes/release-notes-anyconnect-4-10.html）で定義されている一部のクロスプラットフォームのバグは、モバイルリリースに適用される場合があります。修正済みとして報告されたバグは、AnyConnect のリリース番号が大きいすべてのオペレーティング システム プラットフォーム（モバイル オペレーティング システムを含む）で使用可能になります。vpn、core、nvm、およびクロスプラットフォームに適用される同様のコンポーネントのバグは、後続のモバイルリリースでは重複しません。たとえば、iOS リリース 4.9.00512 では、デスクトップリリース 4.9.00086 で解決された vpn コンポーネントのバグは表示されません。iOS バージョンが、バグが修正されたと報告されたリリースバージョンよりも大きいからです。

Android 向け AnyConnect 4.9.00564 で解決済みの問題

ID	見出し
CSCvv71547	Android 向け AnyConnect 4.9 で OCSP チェックが機能しない

AnyConnect Mobile の関連ドキュメント

詳細については、次のドキュメントを参照してください。

- AnyConnect Release Notes
- AnyConnect Administrator Guides
- Cisco ASA シリーズ ドキュメント一覧

【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。

【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。