Cisco Secure Client（AnyConnect を含む）Android 用リリース 5 リリースノート

初版：2023 年 8 月 10 日

最終更新：2023 年 8 月 10 日

Android モバイルデバイス 向け Cisco Secure Client

Android モバイルデバイス向け Cisco Secure Client（AnyConnect を含む）は、リモートの Android および ChromeOS ユーザーに、Cisco Secure Firewall ASA およびその他のシスコがサポートするヘッドエンドデバイスへのセキュアな VPN 接続を提供します。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は、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できます。Cisco Secure Client 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。管理者は、追加機能のために Network Visibility Module（NVM）と Cisco Umbrella 機能を設定することもできます。

Cisco Secure Client および Cisco Secure Firewall ASA のシステム管理者向けに作成されたこのドキュメントには、上で動作する Secure Client のリリースに固有の情報が記載されています。
Android デバイス

Cisco Secure Client アプリケーションは、入手できます。Google Play（Amazon.com で使用可能な Kindle パッケージを除く）。 Cisco Secure Firewall ASA からモバイルアプリを展開することはできません。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 Cisco Secure Client リリースを展開できます。

Cisco Secure Client のモバイルサポートポリシー

シスコでは、現在 App Store で入手可能な Cisco Secure Client 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。

Cisco Secure Client のライセンス

Cisco Secure Firewall ASA ヘッドエンドに接続するには、Advantage または Premier 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 Secure Client Ordering Guide。

最新のエンドユーザーライセンス契約書については、Cisco End User License Agreement、Cisco Secure Client [英語] 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、『Open Source Software Used in Cisco Secure Client for Mobile』 [英語] を参照してください。

Cisco Secure Client Android ベータ版のテスト

リリース前のテストには、Cisco Secure Client 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、ベータ版ではない最新の Cisco Secure Client 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、Cisco Secure Client 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

Androidでの Cisco Secure Client のフルサポートは、Android 4.0（Ice Cream Sandwich）から最新の Android リリースを搭載するデバイスで提供されます。

Android 用の Cisco Secure Client 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 用の Cisco Secure Client は、Amazon から Kindle Fire HD デバイスおよび新しい Kindle Fire 用に入手できます。Secure Client for Kindle は Secure Client for Android パッケージと機能的に同等です。

現在のすべての Chromebook では、Cisco Secure Client for Android が公式にサポートされており、ChromeOS で最適な Cisco Secure Client 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、Secure Client 4.4.3 以降の Cisco Secure Client 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。

Cisco Secure Client for Android 用の Umbrella モジュール

リリース 4.8.03645（以降）では、Cisco Secure Client for Android 6.0.1 以降のデバイス用の Cisco Umbrella モジュールが Android から提供されます。この管理対象および管理対象外 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 Cisco Secure Client 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

Cisco Secure Client for Android 用の Umbrella モジュールは、ライセンスの有無にかかわらず有効にできます。Secure Clientソフトウェアライセンスの詳細については、Cisco Secure Client 発生ガイド [英語] を参照してください。管理者用の Premier トライアルライセンスは、http://www.cisco.com/go/license から入手できます。Android for Secure Client には、Cisco Secure Firewall ASA 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 Secure Firewall 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。

Cisco Secure Client 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 Cisco Secure Client の Umbrella モジュールを展開するための前提条件

（注） Cisco Secure Client 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

Cisco Secure Client 5.0.03085 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンでは、Cisco Secure Client 5.0.03085 for Android で解決済みの問題 （14 ページ）に記載されているバグが解決されています。

Cisco Secure Client 5.0.03084 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンでは、Cisco Secure Client 5.0.03084 for Android で解決済みの問題 （14 ページ）に記載されているバグが解決されています。

Cisco Secure Client 5.0.02078 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンには、次の機能とサポートの更新が含まれ、Cisco Secure Client 5.0.02078 for Android で解決済みの問題 （15 ページ）に記載されているバグが解決されています。

- 暗号化された DNS 要求を送信するときに Cisco Umbrella リゾルバと通信するための追加ポート（53 および 5353）のサポート。現在の 443 ポートに障害が発生すると、新しいポートがチェックされ、変更が加えられた新しいポート用の新しいソケットチャネルが作成されます（CSCwe69440）。
- Android 4.2 より前のバージョンを実行しているデバイスでのアップグレードはサポートされていません。
- VPN の接続と切断の Android クイック設定タイルのサポートは追加されると、デフォルトで有効になります。
- MDM 設定で利用可能な機能拡張：
  - Android でユーザーが新しい VPN 接続を作成できる、またはできないようにする
  - 信頼されていないサーバーをブロック

既知の問題：Android SDK 31 への移行とその OS の制限の結果、Cisco Secure Client アプリケーションには、Cisco Umbrella Protection サービスを実行するための Android の「アラームとリマインダ」権限が必要です。管理対象と管理対象外の両方の Android 展開で、この権限を無効にすることを選択したユーザーは、アプリケーションが動作を停止する可能性があります。

Cisco Secure Client 5.0.01253 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンでは、Android SDK 31 を対象とするように Cisco Umbrella 機能がアップグレードされ、Cisco Secure Client 5.0.01253 for Android で解決済みの問題 （15 ページ）に記載されているバグが解決されています。

Cisco Secure Client 5.0.01251 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンには、次の機能とサポートの更新が含まれ、Cisco Secure Client 5.0.01251 for Android で解決済みの問題 （15 ページ）に記載されているバグが解決されています。

- VPN 接続を暗号化するための TLS 1.3 のサポート。次の追加の暗号スイートが含まれる：TLS_AES_128_GCM_SHA256 および TLS_AES_256_GCM_SHA384。

（注） セキュアクライアント TLS 1.3 接続には、TLS 1.3 をサポートするセキュアゲートウェイも必要です。Cisco Secure Firewall ASA のリリース 9.19(1) では、このサポートが利用できます。接続は、ヘッドエンドがサポートする TLS バージョンにフォールバックします。

DTLS 1.3 はまだサポートされていません。

UI のトンネル統計では、データトンネルプロトコルが表示されます。したがって、DTLS がネゴシエートされている場合、最初の TLS 接続が TLS 1.3 であっても、DTLS が表示されます。

- 生体認証が有効になっている証明書を使用している場合、ヘッドエンドが証明書を受け入れられなくなったことを示すエラーメッセージが表示されます。証明書を削除して再インポートする必要があります。

Cisco Secure Client 5.0.00247 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンでは、Cisco Secure Client 5.0.00247 for Android で解決済みの問題 （16 ページ）に記載されているバグが解決されています。

Cisco Secure Client 5.0.00238 for Android Mobile リリースの新機能

Android 向け Cisco Secure Client のこのバージョンには、次の機能が含まれ、Cisco Secure Client 5.0.00238 for Android で解決済みの問題 （16 ページ）に記載されているバグが解決されています。未解決の問題はCisco Secure Client 5.0.00238 for Android で未解決の問題 （16 ページ）に記載されています。

- スプリット除外トンネリングのサポート

（注） スプリット除外構成には、100 未満の IPv4 ルートと 20 未満の IPv6 ルートが含まれている必要があります。

- ダークテーマ

次の Android Mobile リリースでは、medium ウィジェットは廃止されます。

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 Cisco Secure Client モジュールを有効にすると、Google Play ストアでのアプリケーション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ケーション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 Cisco Secure Client の機能マトリックス

次の表に、Cisco Secure Client 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
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

カテゴリ：機能	Android VPN
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）。	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 Wi-Fi ネットワークの間を移動する際、Cisco Secure Client 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
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 以降の直接プロキシをサポートします。Android 11 以降の PAC プロキシをサポートします。次の（注）を参照してください。
プロキシ例外	対応
パブリック側プロキシ サポート	非対応

カテゴリ：機能	Android VPN
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
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

カテゴリ：機能	Android VPN
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
Cisco Secure Client 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 Cisco Secure Client のバージョン	対応
Cisco Secure Client ネットワーク可視性モジュールのサポート	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
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

* スプリット除外構成には、100 未満の IPv4 ルートと 20 未満の IPv6 ルートが含まれている必要があります。

（注） Cisco Secure Client on Android に PAC プロキシ設定を展開する前に、アプリケーションが PAC プロキシと互換性があることを確認してください。

Cisco Secure Firewall ASA の要件

次の機能を使用するには、Cisco Secure Firewall ASA の最小リリースが必要です。

（注） 現在の Cisco Secure Client モバイルリリースにおけるこれらの機能の可用性については、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：Cisco Secure Firewall ASA 9.7.1.24、9.8.2.28、9.9.2.1 以降。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 1.3：Secure Firewall ASA 9.19.1 以降。
- TLS 1.2：Cisco Secure Firewall ASA 9.3.2 以降。
- Per-App VPN トンネリングモード：Cisco Secure Firewall ASA 9.3.2 以降。
- IPsec IKEv2 VPN、Suite B 暗号化、SCEP プロキシ、またはモバイルポスチャ：Cisco Secure Firewall ASA 9.0。

その他のシスコ ヘッドエンドのサポート

Cisco Secure Client 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。

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

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

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、Cisco Secure Client 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、Cisco Secure Client 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 Cisco Secure Client と Android リリースで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 Cisco Secure Client：
  - 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すると、Cisco Secure Client はバックグラウンドで実行している場合、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 以降では、バッテリセーバーが原因で Cisco Secure Client が一時停止状態に移行すると、Cisco Secure Client 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。Cisco Secure Client 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 Cisco Secure Client が一時停止した場合、バッテリセーバーをオフにするか、Secure Client を許可リストに追加するかに関係なく、Cisco Secure Client 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）により、Secure Client アプリケーションを [最近利用したアプリケーション（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、[設定（Settings）] で Secure Client を終了してから、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）により、Cisco Secure Client 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」とは入力できず、「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 Cisco Secure Client」をサポートしていません。お客様は「HTC Cisco Secure Client」をアンインストールし、「Cisco Secure Client ICS+」をインストールする必要があります（HTC Secure Client 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 未満に設定した場合に 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ために、ヘッドエンドの管理者はトンネル MTU を 1280 未満に設定しないでください。

  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、Secure Client のデバッグ ログに以下の内容が表示されます。

```
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（Secure Client 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）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）により、Secure Client ユーザーは VPN 接続で大量のパケット損失を経験します。この問題は、Android 4.4 で Secure Client 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、Cisco Secure Firewall 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 syslog メッセージが表示されます。

  Google 社が 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、Cisco Secure Firewall ASA 上の TCP 接続の最大セグメントサイズを一時的に小さくできます。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。

- Cisco Secure Client 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。

  この問題を防ぐには、Cisco Secure Client 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、Cisco Secure Client 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。この問題は、Cisco Secure Client 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。失われると、AVF Cisco Secure Client 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 Issue 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。Cisco Secure Client 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、ユーザーが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 Cisco Secure Client 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、Cisco Secure Client 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。プラットフォームに適用される、vpn、core、nvm、および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。iOS バージョンの番号が、バグが修正済みと報告されたリリースバージョンよりも大きい場合、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。

Cisco Secure Client 5.0.03085 for Android で解決済みの問題

ID	見出し
CSCwh50136	Secure Client が証明書のインポートに失敗する

Cisco Secure Client 5.0.03084 for Android で解決済みの問題

ID	見出し
CSCwd15758	デバイスのメモリ不足後に Android の常時オンの再試行メカニズムが機能しない

ID	見出し
CSCwf111486	常時オンが有効になっている場合、Android でキーチェーン証明書のインポートが失敗する
CSCwf49544	ChromeOS 上の AnyConnect Android アプリケーションがクライアント証明書エラーで認証に失敗する
CSCwf86725（Cisco Umbrella）	CSC 5.0：ポート 53 での暗号化されていない DNS の送信のサポートの追加
CSCwf88091	スプリット DNS 設定を使用して接続しようとすると、アプリケーションがクラッシュする

Cisco Secure Client 5.0.02078 for Android で解決済みの問題

ID	見出し
CSCwe44665	ENH：Android の管理対象設定キーに信頼できないサーバーのブロック機能を追加
CSCwe60126	AnyConnect が SAML 経由で Meraki MX に接続できない
CSCwe67925	ENH：Android AnyConnect ユーザーが新しい接続を作成可能
CSCwe69440	CSC 5.0：Cisco Umbrella Android クライアントのポート 53 および 5353 のサポートの追加

Cisco Secure Client 5.0.01253 for Android で解決済みの問題

ID	見出し
CSCwe41637	Android：5.0.01251 へのアップグレード後の「VPNServiceへのバインドに失敗しました（Failed to Bind to VPNService）」
CSCwe42138	Android：5.0.01251 でレガシー VPN sdk が機能しない

Cisco Secure Client 5.0.01251 for Android で解決済みの問題

ID	見出し
CSCwd86009	GUI を再度開いたときに、Android の管理対象設定を確認する必要がある

Cisco Secure Client 5.0.00247 for Android で解決済みの問題

ID	見出し
CSCwb57297	Medium ウィジェットのコンポーネントが欠落し、動作に一貫性がない（サポートを削除）
CSCwb90260	[ロギングシステム（Logging System）] タブで IP とルート情報を利用できない（Android 11 以降）
CSCwc04300	MobileIron Core を使用した Cisco Secure Client Android の VPN の設定が失敗する
CSCwc24658	アイドルタイムアウトによる切断後に、Android の常時稼働で自動再接続されない
CSCwc53813	フォーカスが失われると SSO 外部ブラウザが閉じる

Cisco Secure Client 5.0.00238 for Android で解決済みの問題

ID	見出し
CSCwb64589	IPv6 対応の携帯電話ネットワークと IPv4 Wi-Fi 間の Android 再接続における AnyConnect 4.10 の遅延
CSCwb70409	Android：UI 設定を追加して PAC プロキシの動作をカスタマイズ

Cisco Secure Client 5.0.00238 for Android で未解決の問題

ID	見出し
CSCwb90260	[ロギングシステム（Logging System）] タブで IP とルート情報を利用できない（Android 11 以降）

Cisco Secure Client 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。

- Cisco Secure Client Release Notes
- Cisco Secure Client Administrator Guides
- Cisco Secure Firewall ASA ドキュメントのランディングページ

翻訳について
このドキュメントは、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。