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

初版：2023 年 10 月 11 日

最終更新：2023 年 10 月 11 日

Apple iOS モバイルデバイス 向け Cisco Secure Client

iOS モバイルデバイス向け Cisco Secure Client（AnyConnect を含む）は、リモートの iOS 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。

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、Apple iOS デバイス上で動作する Secure Client のリリースに固有の情報が記載されています。

Cisco Secure Client アプリケーションは、Apple iTunes App Store でのみ入手できます。 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』[英語] を参照してください。

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。

TestFlight による Cisco Secure Client のベータテスト

TestFlight での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。TestFlight でのテストに参加するには、https://testflight.apple.com/join/N0QLSq2c 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、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。

Apple iOS 向けの Cisco Secure Client バージョン

Cisco Secure Client 5 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。Per-App VPN トンネリングは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、すべての機能強化とバグ修正は、Cisco Secure Client 5 バージョンの一部として提供されます。

Apple iOS 対応デバイス

最新の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な最新の推奨バージョンは **Cisco Secure Client 5** です。

（注） iPod Touch 上の Cisco Secure Client は、iPhone 上と同様に表示され、動作します。

Apple iOS での Cisco Secure Client のアップグレード

Cisco Secure Client へのアップグレードは、Apple App Store を使用して管理されます。Cisco Secure Client のアップグレードが利用可能なことを示す通知を Apple App Store から受信したら、次の手順に従います。

（注） 新しいバージョンをインストールする前に、Apple iOS 向けの Cisco Secure Client バージョン（2 ページ）を参照してください。

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セッションを切断し、Cisco Secure Client 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。この手順を実行しなかった場合、Cisco Secure Client の新しいバージョンを使用する前に、デバイスを再起動する必要があります。

手順

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

ステップ 2 [Cisco Secure Clientアップグレード通知（Cisco Secure Client 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（OK）] をタップします。

Cisco Secure Client の更新が実行されます。

新機能

iOS モバイルリリース向け Cisco Secure Client 5.0.02602 の新機能

Cisco Secure Client のこのメンテナンスリリースでは、必要な更新を提供しています。

iOS モバイルリリース向け Cisco Secure Client 5.0.01256 の新機能

Cisco Secure Client のこのメンテナンスリリースでは、Apple iOS 用 Cisco Secure Client 5.0.01256 で解決された問題 （11 ページ） に記載されているバグ修正を提供しています。

iOS モバイルリリース向け Cisco Secure Client 5.0.01241 の新機能

Cisco Secure Client のこのメンテナンスリリースには、次の新機能が含まれており、Apple iOS 用 Cisco Secure Client 5.0.00246 で解決された問題 （11 ページ） に記載されているバグ修正が含まれています。

- VPN 接続を暗号化するための TLS バージョン 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。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。

- ベンダーデータを介して VPN xml プロファイルをインポートする機能

既知の問題：

CSCwd93529：VPN ショートカットへの iOS Siri 接続が動作していない

CSCwc01260：AnyConnect 接続を数日間実行した後、原因不明の切断が生じることがある

iOS モバイルリリース向け Cisco Secure Client 5.0.00246 の新機能

Cisco Secure Client のこのメンテナンスリリースでは、Apple iOS 用 Cisco Secure Client 5.0.00246 で解決された問題 （11 ページ） に記載されているバグ修正を提供しています。

iOS モバイルリリース向け Cisco Secure Client 5.0.00230 の新機能

5.0.00230 バージョンでは、iOS 用の新しい Cisco Secure Client（AnyConnect を含む）が導入されています。

Apple iOS Cisco Secure Client 機能マトリックス

次の機能は、Apple iOS デバイス向け Cisco Secure Client でサポートされています。

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	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：	

カテゴリ：機能	Apple iOS
TLS	対応
TLS 1.3	対応
データグラム TLS（DTLS）	対応
IPsec IKEv2 NAT-T	対応
IKEv2 - raw ESP	非対応
Suite B（IPSec のみ）	対応
TLS 圧縮	対応（32 ビットデバイスのみ）
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（Cisco Secure Client 4.0.09xxx および iOS 10.3 以降が必要）
フルトンネル（OS は、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に対して例外を発生させる可能性がある）	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
自動再接続/ネットワークローミング	対応
オンデマンド VPN（宛先により起動）	対応（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）	対応（アプリケーションごとの VPN モードでのみ動作する場合）。
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
IPv4 over IPv4 トンネル	対応
IPv6 over IPv4 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

カテゴリ：機能	Apple iOS
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	対応
プロキシ例外	対応（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	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	非対応
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：	
YubiKey	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）	非対応
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
レガシー SCEP の登録	非対応
SCEP プロキシの登録	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

カテゴリ：機能	Apple iOS
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	対応（機能制限があります）
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	非対応
Cisco Secure Client に固有のステータスアイコン	非対応
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 Network Visibility Module のサポート	非対応
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

カテゴリ：機能	Apple iOS
ロギング/診断情報（DART）	対応
認定：	
FIPS 140-2 レベル 1	対応

* オペレーティングシステムの実装による Cisco Secure Firewall 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。

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。

Apple iOS での Cisco Secure Client の注意事項と制約事項

- （iOS 14.0.x 以上）：トンネル DNS サーバーがスプリット DNS ドメイン名を指定せずに設定されている場合、トンネル DNS サーバーでアドレスを解決できなくても、デバイスのパブリック DNS サーバーにフォールバックしません。iOS の変更により、この異なる動作が発生しました。

- （iOS 14.0.x のみ）CSCvv50495：ネットワークの変更後、ネットワークを移行、またはネットワークを一時停止して再開すると、トラフィックが停止します。VPN接続を無効にしてから再度有効にすると、再開できます。この問題は、iOS 14.1 では修正されています。
- CSCvs82209：SCEP経由でインポートされ、アクセスに生体認証を要求するクライアント証明書にアクセスしている場合、iOS 13.3.1 以降では「有効な証明書が見つかりません」というエラーが発生します。 iOS 13.3.1 では、アクセスに生体認証（TouchID/FaceID/パスコード）を要求するセキュリティプロパティを持つ SCEP インポート済み証明書を使用する Cisco Secure Client ネットワーク拡張機能が削除されました。この変更に対応するようにクライアントを再設計できるようになるまでは、生体認証オプションを使用せずにSCEPを使用して証明書を展開します。
- Cisco Secure Client は、ユーザーが手動で設定するか、iPhone 設定ユーティリティ（Mac App Store で入手可能）を使用して生成する Cisco Secure Client VPN プロファイルを使用して、またはエンタープライズ モバイル デバイス マネージャを使用して設定できます。
- Apple iOS デバイスは 1 つの Cisco Secure Client VPN 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、ユーザーが 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 Cisco Secure Client VPN プロファイルにより、vpn.example1.com からインポートされた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が、デバイスのバッテリ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：導入された DHE 暗号サポートにより、9.2 より前の Cisco Secure Firewall 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は、それらの Cisco Secure Firewall ASA バージョンで DHE 暗号を無効にする必要があります。

  DHE 暗号サポートの導入により、9.2 より前の Cisco Secure Firewall 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は、それらの Cisco Secure Firewall 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。
- Cisco Secure Client 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、ユーザーが iOS の Connect On-Demand 機能を使用して初めて接続を確立する場合、またはデバイス情報（OS バージョンなど）が変更された場合、Cisco Secure Client がモバイルポスチャ情報を誤ってレポートすることがあります。

既知の互換性の問題

- 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）、Cisco Secure Firewall 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）。

- Cisco Secure Client UI が開いたままの状態で、UI と内部の Cisco Secure Client 拡張機能の間のプロセス間通信（IPC）を iOS が誤って切断した場合、すべての 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 Cisco Secure Client 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 Cisco Secure Firewall ASA によってクライアントにプッシュされたときに、Cisco Secure Client 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。

- 管理対象の Per-App 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ーが作成した（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。Apple 社は、これが想定されている動作であることを確認しています。

暗号化のサポート

次の安全性の低い暗号スイートは削除されました。

- SSL VPN の場合、Cisco Secure Client 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 の場合、Cisco Secure Client 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

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 [英語] 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。

Apple iOS 用 Cisco Secure Client 5.0.01256 で解決された問題

ID	見出し
CSCwd94735	ベンダーデータが正しく設定されていない場合、AnyConnect VPN がクラッシュする
CSCwe49458	ISE は AnyConnect VPN を使用して Apple M1 デバイスを正しく識別しない

Apple iOS 用 Cisco Secure Client 5.0.01241 で解決された問題

ID	見出し
CSCwd68196	M1/M2 macOS Ventura 上の AnyConnect iOS アプリが接続時にハングする

Apple iOS 用 Cisco Secure Client 5.0.00246 で解決された問題

ID	見出し
CSCwc01260	iOS 15：オンデマンドでトリガーされた VPN を確立できない

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。