Cisco Secure Client モバイルプラットフォームおよび機能ガイド

改訂：2023 年 5 月 24 日

Cisco Secure Client モバイルプラットフォームおよび機能

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。

Kindle での 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。Cisco Secure Client for Kindle は Cisco Secure Client for Android パッケージと機能的に同等です。

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（3.2 を含む）を実行する Samsung デバイスが必要です。NVM の設定には、Cisco 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。

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。

Google Chrome OS でサポートされるデバイス

Google Chromebook での Cisco Secure Client には、Chrome OS 43 以降が必要です。Chrome OS 45 では、安定性と機能拡張を利用することができます。

Google Chromebook 上の Cisco Secure Client は、別のプラットフォームのスタンドアロン Chrome ブラウザからは使用できません。

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いるため、ChromeOS で最適な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。

ユニバーサル Windows プラットフォームのサポート対象デバイス

ユニバーサル Windows プラットフォーム上の Cisco Secure Client は、デスクトップを含むすべての UWP 互換デバイスをサポートします。

Cisco Secure Client モバイルプラットフォームの機能マトリックス

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
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	対応	対応	対応
Cisco VPN プロファイルのサポート（手動インポート）	対応	対応	対応	非対応
Cisco VPN プロファイルのサポート（接続中のインポート）	対応	対応	対応	非対応
MDM 設定の接続エントリ	対応	対応	対応	対応
ユーザー設定の接続エントリ	対応	対応	対応	対応
トンネリング：				
TLS	対応	対応	対応	対応
データグラム TLS（DTLS）	対応	対応	対応	対応*
DTLS v1.2		対応		
IPsec IKEv2 NAT-T	対応	対応	対応	非対応
IKEv2 - raw ESP	対応	非対応	非対応	非対応
Suite B（IPSec のみ）	対応	対応	非対応	非対応
TLS 圧縮	対応	対応（32 ビットデバイスのみ）	非対応	非対応
デッド ピア検出	対応	対応	対応	非対応
トンネル キープアライブ	対応	対応	対応	非対応
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	非対応	非対応	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。	対応（Cisco AnyConnect 4.0.09xxx および iOS 10.3 以降が必要です）	非対応	対応。MDM プロビジョニングのみ
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	非対応	非対応	非対応

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
複数のトンネル	非対応	対応。MDM を設定します。	非対応	非対応
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	対応	対応	対応
スプリット トンネル（スプリットを含む）	対応	対応	対応	対応
ローカル LAN（スプリットを含まない）。	非対応	対応	対応	非対応
Split-DNS	対応。スプリットによる処理を含みます。	対応	非対応	対応
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。	対応	対応。Chrome OS 51 以降と Cisco Secure Client 4.0.0113 以降が必要です。	対応。ユーザーが同じネットワーク上にとどまっており、ネットワーク接続が終了していない場合。
オンデマンド VPN（宛先により起動）	非対応	対応（オンデマンドでApple iOS Connect と互換性があります）	非対応	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	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。	非対応	非対応
キー再生成	対応	対応	対応	非対応
IPv4 パブリック トランスポート	対応	対応	対応	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。	対応	非対応	対応
IPv4 over IPv4 トンネル	対応	対応	対応	対応

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
IPv6 over IPv4 トンネル	対応	対応	非対応	対応
IPv6 over IPv4 トンネル	対応	対応	非対応	対応
IPv6 over IPv6トンネル	対応	対応	非対応	対応
デフォルト ドメイン	対応	対応	対応	対応
DNS サーバーの設定	対応	対応	対応	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。	対応	対応。ASA で設定されたプロキシ PAC URL を使用。	対応。制限付きのサポート
プロキシ例外	対応	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）	非対応	非対応
パブリック側プロキシ サポート	非対応	非対応	非対応	非対応
ログイン前バナー	対応	対応	対応	対応
ログイン後バナー	対応	対応	対応	対応
DSCP の保存	対応	非対応	非対応	非対応
接続と切断：				
VPN ロード バランシング	対応	対応	対応	対応
バックアップ サーバー リスト	対応	対応	対応	非対応
最適ゲートウェイ選択	非対応	非対応	非対応	非対応
認証：				
クライアント証明書の生体認証保護	対応	対応	非対応	非対応
SAML 2.0	対応	対応	対応	非対応
クライアント証明書認証（RSA）	対応	対応	対応	対応
クライアント証明書認証（ECDSA）	対応	対応	対応	対応

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
SAML + クライアント証明書要求	対応	対応	非対応	非対応
証明書の取消確認	オンライン証明書ステータス プロトコル（OCSP）	iOS バージョンに応じて、OCSP または CRL（証明書失効リスト）のいずれか	非対応	非対応
手動によるユーザー証明書の管理	対応	対応	対応。Chrome デバイスの機能を使用。	対応
手動によるサーバー証明書の管理	対応	対応	対応	対応
レガシー SCEP の登録：廃止	非対応	非対応	非対応	非対応
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	対応	非対応	非対応
自動証明書選択	対応	対応	非対応	対応
手動による証明書の選択	対応	対応	対応	非対応
スマート カードのサポート	非対応	非対応	非対応	非対応
ユーザー名およびパスワード	対応	対応	対応	対応
トークン/課題	対応	対応	対応	対応
二重認証	対応	対応	対応	対応
グループ URL（サーバー アドレスで指定）	対応	対応	対応	対応
グループの選択（ドロップダウン選択）	対応	対応	対応	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	対応	対応	対応
パスワードの保存	非対応	非対応	非対応	非対応
Umbrella ユーザー ID	対応	非対応	非対応	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	対応	対応（機能制限があります）	対応（機能制限があります）
ネイティブ OS GUI	非対応	対応（機能制限があります）	対応（機能制限があります）	対応

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
API/URI ハンドラ（以下を参照）	対応	対応	非対応	非対応
UI のカスタマイゼーション	非対応	非対応	非対応	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）	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）	非対応	非対応
ユーザー設定	対応	対応	対応	部分的に対応
Cisco Secure Client に固有のステータスアイコン	オプション	非対応	非対応	非対応
ダークモード	非対応	対応	非対応	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	対応	非対応	非対応
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	対応	対応	対応
Siri のサポート	非対応	対応	非対応	非対応
Cisco Secure Client Network Visibility Module 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。	非対応	非対応	非対応
NVM フローのエクスポートを制限する機能	対応	非対応	非対応	非対応
DTLS を介してコレクタに安全にデータを送信する機能	対応	非対応	非対応	非対応
URI の処理：				
QR コードのスキャン	対応	非対応	非対応	非対応
接続エントリの追加	対応	対応	非対応	非対応
VPN への接続	対応	対応	非対応	非対応

カテゴリ：機能	Android	Apple iOS	Chrome	ユニバーサル Windows プラットフォーム
接続時のクレデンシャルの事前入力	対応	対応	非対応	非対応
VPN の解除	対応	対応	非対応	非対応
証明書のインポート	対応	対応	非対応	非対応
ローカリゼーションデータのインポート	対応	対応	非対応	非対応
XML クライアント プロファイルのインポート	対応	対応	非対応	非対応
URI コマンドの外部（ユーザー）制御	対応	対応	非対応	非対応
レポートおよびトラブルシューティング：				
統計	対応	対応	対応	非対応
ロギング/診断情報（DART）	対応	対応	対応	対応。Field Medic アプリケーションが必要
認定：				
FIPS 140-2 レベル 1	対応	対応	非対応	非対応

（注） Cisco Secure Client on Android に PAC プロキシ構成を展開する前に、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。

UWP での DTLS のサポートについては、Cisco Secure Client（AnyConnect を含む）のリリースノート、ユニバーサル Windows プラットフォームのリリース 5 で既知のいくつかの制限を参照してください。

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

Apple iOS デバイスにおける VPN 接続の使用方法については、Apple から詳細情報を入手できます。

- https://developer.apple.com/library/ios/search/?q=vpn+server+configuration
- https://support.apple.com/guide/deployment/vpn-settings-overview-dep2d2adb35d

【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/

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。