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

初版：2021 年 3 月 26 日

Cisco Secure Client リリース 5 リリースノート

最新バージョンの Cisco Secure Client のダウンロード

始める前に

最新バージョンの Cisco Secure Client をダウンロードするには、Cisco.com に登録されたユーザーである必要があります。

手順

ステップ 1 Cisco Secure Client 製品のサポートページを参照します。

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

ステップ 2 Cisco.com にログインします。

ステップ 3 [ソフトウェアのダウンロード（Download Software）] をクリックします。

ステップ 4 [最新リリース（Latest Releases）] フォルダを展開し、最新リリースをクリックします（まだ選択されていない場合）。

ステップ 5 次のいずれかの方法で Secure Client パッケージをダウンロードします。

- 1 つのパッケージをダウンロードする場合は、ダウンロードするパッケージを見つけて [ダウンロード（Download）] をクリックします。
- 複数のパッケージをダウンロードする場合は、目的のパッケージの横にある [カートに追加（Add to cart）] をクリックし、[ソフトウェアのダウンロード（Download Software）] ページの上部にある [カートのダウンロード（Download cart）] をクリックします。

ステップ 6 メッセージが表示されたら、シスコのライセンス契約書を読んで承認します。

ステップ 7 ダウンロードを保存するローカルディレクトリを選択し、[保存（Save）] をクリックします。

ステップ 8 『Cisco Secure Client Administrator Guide, Release バージョン 5』[英語] を参照します。

Web 展開用の Cisco Secure Client パッケージファイル名

OS	Cisco Secure Client Web 展開パッケージ名
Windows	cisco-secure-client-win-バージョン-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-バージョン-webdeploy-k9.pkg
Linux（64 ビット）*	cisco-secure-client-linux64-バージョン-webdeploy-k9.pkg

* RPM および DEB インストールの Web 展開は、現時のところサポートされていません。

事前展開用の Cisco Secure Client パッケージファイル名

OS	Cisco Secure Client 事前展開パッケージ名
Windows	cisco-secure-client-win-version-predeploy-k9.zip
macOS	cisco-secure-client-macos-version-predeploy-k9.dmg
Linux（64 ビット）	（スクリプトインストーラーの場合） cisco-secure-client-linux64-version-predeploy-k9.tar.gz （RPM インストーラ*の場合） cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tar.gz （DEB インストーラ*の場合）cisco-secure-client-linux64-*version*-predeploy-deb-k9.tar.gz

*RPM および DEB インストーラで提供されるモジュール：VPN、DART

Cisco Secure Client への機能の追加に役立つその他のファイルもダウンロードできます。

Cisco Secure Client 5.0.04032 の新機能

このメンテナンスリリースは、次の機能とサポートの更新を含むものであり、「Cisco Secure Client 5.0.04032 （43 ページ）」に記載されている不具合を修正します。

- Cisco Secure Client ThousandEyes Endpoint Agent モジュールの導入：事前展開パッケージで ThousandEyes Windows インストーラ（.msi）が提供されるようになりました。インストール時に、Secure Client は ThousandEyes モジュールのインストールを検出し、[バージョン情報（About）] ボックスにバージョンを表示できますが、UI タイルは表示されません。この統合により、お客様はアプリケーションの正常性を完全に把握できるため、十分な情報に基づいた意思決定を行い、問題を迅速に解決できます。詳細については、『Cisco Secure Client Administrator Guide』の「Thousand Eyes Integration」を参照してください。ユーザーがモニター対象ネットワーク内から特定の Web サイトにアクセスするときにネットワーク層およびアプリケーション層のパフォーマンスデータを収集する方法の詳細については、『Cisco Secure Client - ThousandEyes Endpoint Agent Module Integration Guide』を参照してください。

- Secure Cloud Analytics との統合（Windows のみ）：Network Visibility Module のデータを、Secure Cloud Analytics の [NVM フロー（NVM Flow）] タブで表示できるようになりました。デフォルトの展開とプロファイルでは、Network Visibility Module はデータを Cisco XDR に送信します。詳細については、『Network Visibility Module in Cisco XDR』を参照してください。マニュアルはこちらから入手できます。
- ARM64 Windows の ISE ポスチャ：ISE は、エンドポイントにネットワークへのアクセスを許可する前に、ポスチャチェックを実行してコンプライアンスステータスを確認できます。

Cisco Secure Client 5.0.03076 の新機能

これは、Windows（Intel）のみで見つかった不具合を解決する Cisco Secure Client メンテナンスリリースです。この不具合は、Windows のみの機能であるネットワーク アクセス マネージャに固有のものです。MacOS および Linux ユーザーには適用されない解決済みの不具合の詳細については、Cisco Secure Client 5.0.03076 （44 ページ） を参照してください。

Cisco Secure Client 5.0.03072 の新機能

これは、次の機能とサポートの更新を含むメンテナンスリリースであり、「Cisco Secure Client 5.0.03072 （44 ページ）」に記載されている不具合を修正します。

- 特定のユーザー補助の変更：不利な立場にある人々に利益をもたらし、デジタル トランスフォーメーションを通じて生産性を向上させるために、特定の Voluntary Product Accessibility Template（VPAT）コンプライアンス基準に取り組みました。
  - ハイコントラストテーマ：[バージョン情報（About）] ダイアログとタイルタイトルの非表示のハイパーリンクを修正しました
  - 最小コントラスト比：タイルサブメニューと DART メニューの説明のテキストの色を調整してコントラストを高めました
  - Windows の一般的なショートカットキー（Tab、Enter、Spacebar）によるキーボードナビゲーション
  - メニューボタンによる高度なウィンドウのナビゲーションと選択（上/下および左/右矢印キーを使用）
  - 詳細ウィンドウから環境設定、バージョン情報、DART ウィンドウへのキーボードアクセス
  - 統計グループを展開および折りたたむための PgUp/PgDn によるキーボードナビゲーション
  - DART および Cisco Secure Client UI のナビゲーションと選択フォーカスの可視性
  - ログ設定のスクリーンリーダーと JAWS アナウンスの不一致を調整

- DART 暗号化メニューのスクリーンリーダーと JAWS アナウンスの不一致を調整
- 名前のラベルに対する適切な JAWS アナウンス

- [デュアルホーム検出（Linux用）（Dual-Home Detection (for Linux)）]：マルチホームエンドポイントが企業のネットワークからパブリックネットワークに切り替わり、企業の個人情報が漏洩しないように、信頼できないインターフェイスを無効にします。プロファイルで Secure Trusted Network Detection を有効にする必要があります。これにより、静的 DNS 設定によって信頼できるネットワークが検出されると、追加のチェックとして HTTPS プローブが構成済みの信頼できるサーバーに送信されます。[信頼されたネットワークで信頼されたサーバー接続のないインターフェイスを無効にする（Disable interfaces without trusted server connectivity while in trusted network）] チェックボックスの詳細については、「Cisco Secure Client Profile Editor, Preferences (Part 2)」を参照してください。

  次の制限は、デュアルホーム検出（Linux と macOS の両方）で既知であり、現在対処中です。

  - CSCwf51800：Linux、MacOS：一部のシナリオでデュアルホーム検出が有効になった後、「信頼されたネットワーク上で」UI メッセージが表示されない
  - CSCwf52884：Linux、MacOS：Secure TND プローブで断続的に問題が発生する
  - CSCwf52878：Linux、macOS：ネットワーク設定がすぐに利用できない場合のデュアルホーム検出タイミングの問題

- [VPN セッションタイムアウト時に接続をバイパスする（Bypass Connect Upon VPN Session Timeout）]：信頼できるネットワークポリシーまたは信頼できないネットワークポリシーのいずれかが接続に設定されているときに、VPN セッションがタイムアウトした場合に自動的に発生する接続の再試行をバイパスできます。このチェックボックスは、VPN プロファイルエディタに追加されます（設定パート 2）。

既知の問題：（CSCwf63877）オペレーティングシステムの NetworkManager コンポーネントからの DNS サーバー情報が正しくないため、Red Hat 9.2 で信頼されたネットワーク検出が期待どおりに機能しない。

Cisco Secure Client 5.0.02075 の新機能

このメンテナンスリリースは、次の機能とサポートの更新を含むものであり、「Cisco Secure Client 5.0.02075 （47 ページ）」に記載されている不具合を修正します。

- **UseLocalProfileAsAlternative カスタム属性**：Cisco Secure Firewall ASA で Cisco Secure Client プロファイル（旧名は AnyConnect）を設定せずに、アウトオブバンドで（SCCM、MDM、SecureX Cloud Management などを使用して）プロファイルを配布する場合は、UseLocalProfileAsAlternative カスタム属性を使用できます。このカスタム属性を設定すると、クライアントは設定とプリファレンスに(通常のデフォルトではなく)ローカル（ディスク上）の Cisco Secure Client プロファイルを使用します。詳細については、アドミニストレーション ガイドの「Predeploying Cisco Secure Client」を参照してください。また、

ASDM バージョン 7.19（またはそれ以降）で必要な設定手順については、「Configure Secure Client Custom Attributes in an Internal Group Policy」を参照してください。『Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide』の「Secure Client Custom Attributes」の項には、このカスタム属性などのタイプと名前付きの値が記載されています。

- [EDRインターネットチェックを無効にする（Disable EDR Internet Check）]：リアルタイム転送プロトコルチェック、およびエンドポイントと検出応答（EDR）の定義の確認をスキップする ISE ポスチャ プロファイル エディタ オプション。EDR 製品がインストールされている場合は、システムスキャン中にこのオプションを使用してインターネットの確認を実行できます。
- [デュアルホーム検出（MacOSのみ）（Dual-Home Detection (macOS Only)）]：マルチホームエンドポイントが企業のネットワークからパブリックネットワークに切り替わり、企業の個人情報が漏洩しないように、信頼できないインターフェイスを無効にします。プロファイルで Secure Trusted Network Detection を有効にする必要があります。これにより、静的 DNS 設定によって信頼できるネットワークが検出されると、追加のチェックとして HTTPS プローブが構成済みの信頼できるサーバーに送信されます。[信頼されたネットワークで信頼されたサーバー接続のないインターフェイスを無効にする（Disable interfaces without trusted server connectivity while in trusted network）] チェックボックスの詳細については、「Cisco Secure Client Profile Editor, Preferences (Part 2)」を参照してください。
- Umbrella モジュールの ARM64 サポート。
- WPA3 Enhanced Open（OWE）および WPA3 Personal（SAE）のサポートが、ネットワークアクセス マネージャに追加されました。

既知の問題

（CSCwe92223）Windows arm64：SplitDNSV6 テストで、トンネル外の pcap に遊離 DNS クエリが表示される

Cisco Secure Client 5.0.01242 の新機能

このメンテナンスリリースは、次の機能とサポートの更新を含むものであり、「Cisco Secure Client 5.0.01242 （51 ページ）」に記載されている不具合を修正します。

- ISE ポスチャの基本的なポスチャ CLI（CSCwc98263）：Windows のみの場合、ポスチャ cli.exe オプションが追加されたため、すべての UI プロセスで許可されていた 1 つのクライアントと 1 つのサーバーの通信ではなく、複数のクライアントがポスチャサブシステムに接続してデータを送信できます。
- 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。

ISE ポスチャはまだ TLS 1.3 をサポートしていません。

- Start Before Login は ARM64 ベースの PC 用に Microsoft がサポートしているバージョンの Windows 10 および 11 でサポートされます。
- セキュアクライアントの高速ユーザー切り替え：GUI は、同じデバイスに同時にログインしている複数のユーザーに対して機能します。この Windows 機能は、AnyConnect VPN モジュールを展開していない Cisco Secure Endpoint の導入でのみサポートされます。VPN 展開は、高速ユーザー切り替えの機能を中断します。

既知の問題

CSCwd79171：ネットワーク アクセス モジュール クライアントは、新しい設定ファイルを保存し、newConfigFiles ディレクトリ内の設定の xml データを解析および検証しようとした後にクラッシュすることがあります。サービスはシャットダウン後に再起動するように設定されているため、管理者は気付かない場合があり、無効なメモリアクセスが発生する可能性があります。

CSCwd68113：正しいユーザー名とパスワードが入力されていても、Secure Client VPN AAA 認証が「ログイン失敗（Login Failed）」エラーで失敗することがあります。再起動すると問題が解決し、期待どおりに認証が機能します。

Cisco Secure Client 5.0.00556 の新機能

このリリースでは、当初は Windows サポートのみでリリースされていた Cisco Secure Client（AnyConnect を含む）に macOS および Linux のサポートが追加されています。次の機能とサポート更新を含み、「Cisco Secure Client 5.0.00556 （55 ページ）」に記載されている不具合を修正します。

- 認証後の接続の失敗後に VPN 接続を試行するとハングするという既知の問題（CSCwc56173）が修正されました
- Linux 要件の変更：systemd と libsystemd は Linux の必須パッケージになりました
- Red Hat 9.0 のサポート

次の箇条書きは、Cisco AnyConnect セキュア モビリティ クライアント 4.x リリースとは異なる主要なサポート、命名、および機能の変更を示しています。リリース 5 では、Cisco AnyConnect セキュア モビリティ クライアントの名前が Cisco Secure Client（AnyConnect を含む）に変更されました。

- Network Access Manager は Cisco Secure Client 5 の一部ですが、SecureX 内の Network Access Manager プロファイルエディタはリリース 5 では使用できません。
- Windows 用 Cisco Secure Client は Cisco Secure Endpoint（旧 AMP for Endpoints）との完全な統合を提供するため、AMP イネーブラは Cisco Secure Client 5 での macOS 専用です。
- 一部の AnyConnect モジュールも、Cisco Secure Client 5 リリースで新しい名前が付けられています。HostScan（VPN Posture）は Secure Firewall Posture に変更されます。ASDM UI では、リモートアクセス VPN ウィンドウでポスチャ（Cisco Secure Firewall 用）として参照されます。同様に、Cisco.com からダウンロードした hostscan.pkg の名前は、secure-firewall-posture-version-k9.pkg に変更されます。
- ドキュメントと ASDM UI で AnyConnect への参照に気付くでしょう。ASDM は Cisco Secure Client 5 プロファイルを設定するために完全にサポートされていますが、現在、これらの参照を新しい Cisco Secure Client 名に変更する予定はありません。Cisco Secure Firewall ASA は、バージョン 9.18 以降では新しい ASA 名になります。
- Umbrella クラウド インフラストラクチャにインストールされたすべての AnyConnect モジュールの自動更新を提供する Umbrella ローミング セキュリティ モジュールの機能は、リリース 5 で削除されました。
- AnyConnect の Apex および Plus ライセンスは、Cisco Secure Client の Premier および Advantage ライセンスに変更されました。

Cisco Secure Client 5.0.00529 の新機能

これはメジャー リリースであり、次の機能とサポート更新を含み、Cisco Secure Client 5.0.00529（56 ページ）に記載されている不具合を解決します。

- 初期の Cisco Secure Client（AnyConnect を含む）リリース 5 は、Windows でのみ使用できます。ドキュメントでは、macOS および Linux 対応の Cisco Secure Client について言及されていますが、この機能はこの初期リリースには適用されません。macOS または Linux で実行している場合は、そのプラットフォームで Cisco Secure Client が正式にリリースされるまで、AnyConnect 4.x リリースのドキュメントを参照してください。Android と iOS には、すでに 5.0 リリースがあります。
- さまざまな言語のデフォルトのローカリゼーションファイル：Cisco Secure Client のインストールには、さまざまな言語のデフォルトのローカリゼーションファイルが含まれています。デバイスで指定されているロケールに従って、表示される言語が決定します。Cisco Secure Client は最適なものを判断するため、言語仕様を使用してから、リージョン仕様を使用します。

- プロファイルエディタでの OpenJDK の使用：Oracle Java 8 以降を使用している場合は、JRE の場所に関する追加のプロンプトなしでプロファイルエディタを起動できます。OpenJDK/JRE（Java 8 以降）を使用している場合、JRE パスの入力を求められる場合があります。一部の OpenJDK バリアントでは、プロファイルエディタの再インストールまたはアップグレード時に JRE/JDK パスを 1 回手動で指定する必要があります。
- ActiveX コントロールは、Cisco Secure Client および Cisco Secure Firewall ポスチャから削除されました。

次の箇条書きは、Cisco AnyConnect セキュア モビリティ クライアント 4.x リリースとは異なる主要なサポート、命名、および機能の変更を示しています。リリース 5 では、Cisco AnyConnect セキュア モビリティ クライアントの名前が Cisco Secure Client（AnyConnect を含む）に変更されました。

- Network Access Manager は Cisco Secure Client 5 の一部ですが、SecureX 内の Network Access Manager プロファイルエディタはリリース 5 では使用できません。
- Windows 用 Cisco Secure Client は Cisco Secure Endpoint（旧 AMP for Endpoints）との完全な統合を提供するため、AMP イネーブラは Cisco Secure Client 5 での macOS 専用です。
- 一部の AnyConnect モジュールも、Cisco Secure Client 5 リリースで新しい名前が付けられています。HostScan（VPN Posture）は Secure Firewall Posture に変更されます。ASDM UI では、リモートアクセス VPN ウィンドウでポスチャ（Cisco Secure Firewall 用）として参照されます。同様に、Cisco.com からダウンロードした hostscan.pkg の名前は、secure-firewall-posture-version-k9.pkg に変更されます。
- ドキュメントと ASDM UI で AnyConnect への参照に気付くでしょう。ASDM は Cisco Secure Client 5 プロファイルを設定するために完全にサポートされていますが、現在、これらの参照を新しい Cisco Secure Client 名に変更する予定はありません。Cisco Secure Firewall ASA は、バージョン 9.18 以降では新しい ASA 名になります。
- Umbrella クラウド インフラストラクチャにインストールされたすべての AnyConnect モジュールの自動更新を提供する Umbrella ローミング セキュリティ モジュールの機能は、リリース 5 で削除されました。
- AnyConnect の Apex および Plus ライセンスは、Cisco Secure Client の Premier および Advantage ライセンスに変更されました。

既知の問題

VPN 接続の試行は、前の認証後の接続の失敗の後、最大 3 分間ハングする場合があります（CSCwc56173）。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.04032 の新機能

Cisco Secure Firewall ポスチャ 5.0.04032 には、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれ、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.04032

（57 ページ） に記載されている不具合が修正されています。詳細については、「Release and Compatibility」の「Secure Firewall Posture Support Charts」[英語] を参照してください。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.03072 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.03072 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれ、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.03072 （57 ページ） に記載されている不具合が修正されています。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.02075 の新機能

Secure Firewall Posture（以前の HostScan）5.0.02075 リリースには、次の機能が含まれており、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.02075 （58 ページ） に記載されている不具合が修正されています。

[Cisco Secure Firewallディスク暗号化（Secure Firewall Disk Encryption）]：Cisco Secure Firewall ポスチャ（以前の HostScan）機能の一部としてエンドポイントにインストールされているディスク暗号化製品をレポートする機能。[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）] > [ポスチャ（Cisco Secure Firewall用）（Posture (for Secure Firewall)）] > [ポスチャ設定（Posture Settings）] > [構成（Configure）] で、ASDM の Advanced Endpoint Asssesment に追加のチェックボックスが追加されます。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.01242 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.01242 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれ、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.01242 （58 ページ） に記載されている不具合が修正されています。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00556 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00556 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00529 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00529 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。

システム要件

ここでは、このリリースの管理要件とエンドポイント要件について説明します。各機能のエンドポイント OS のサポートとライセンス要件については、『Cisco Secure Client Features, Licenses, and OSs』[英語] を参照してください。

シスコは、他の VPN サードパーティクライアントとの互換性を保証できません。

Cisco Secure Client プロファイルエディタの変更

プロファイルエディタを起動する前に、Java（バージョン 8 以降）をインストールする必要があります。Cisco Secure Client プロファイルエディタは、OpenJDKだけでなく Oracle Java もサポートしています。特定の OpenJDK ビルドでは、JRE のパスを特定できなければ、プロファイルエディタの起動に失敗することがあります。インストール済みの JRE のパスに移動すると、プロファイルエディタを正しく起動するように求められます。

Cisco Secure Client の ISE 要件

- **警告**：

  非互換性警告：2.0 以降を実行している Identity Services Engine（ISE）のお客様は、次に進む前にこちらをお読みください。

  ISE RADIUS はリリース 2.0 以降 TLS 1.2 をサポートしてきましたが、CSCvm03681 により追跡される TLS 1.2 を使用した EAP-FAST の ISE 導入に不具合が見つかりました。この不具合は、ISE の 2.4p5 リリースで修正されました。この修正は、ISE のサポートされているリリース用の今後のホット パッチで提供されます。

  上記のリリースより前の TLS 1.2 をサポートする ISE リリースの EAP-FAST を使用して、ネットワーク アクセス マネージャ 4.7（以降）が認証に使用される場合、認証は失敗し、エンドポイントはネットワークにアクセスできません。

- ISE 2.6（以降）と Cisco Secure Client 4.7MR1（以降）では、有線および VPN フローで IPv6 非リダイレクトフロー（ステージ 2 検出を使用）がサポートされます。
- Cisco Secure Client のテンポラル エージェント フローは、ネットワークトポロジに基づいて IPv6 ネットワークで機能します。ISE は、ネットワークインターフェイス（eth0/eth1 など）で IPv6 を設定する複数の方法をサポートしています。
- ISE ポスチャフローに関する IPv6 ネットワークには、（IPv6）ISE ポスチャ検出が特定のタイプのネットワークアダプタ（Microsoft Teredo 仮想アダプタなど）のために無限ループに陥る（CSCvo36890）という制限があります。
- ISE 2.0 は、Cisco Secure Client ソフトウェアをエンドポイントに展開し、Cisco Secure Client 4.0 以降の新しい ISE ポスチャモジュールを使用してそのエンドポイントをポスチャできる最小リリースです。

- ISE 2.0 は Cisco Secure Client リリース 4.0 以降だけを展開できます。Cisco Secure Client の旧リリースは、ASA から Web 展開するか、SMS で事前展開するか、手動で展開する必要があります。
- Cisco Secure Client ISE ポスチャモジュールをインストールまたは更新する場合、ASA で設定されたパッケージとモジュールは、ISE で設定されたものと同じである必要があります。VPN は、他のモジュールのアップグレード時に常にアップグレードされますが、トンネルがアクティブな場合、ISE からの VPN モジュールのアップグレードは許可されません。

ISE ライセンス要件

ISE ヘッドエンドから Cisco Secure Client を展開し、ISE ポスチャモジュールを使用するには、ISE 管理ノードに Cisco ISE Premier ライセンスが必要です。ISE ライセンスの詳細については、『Cisco Identity Services Engine Admin Guide』[英語] の「*Cisco ISE Licenses*」の章を参照してください。

Cisco Secure Client 用の Cisco Secure Firewall ASA の要件

特定の機能に関する最小 ASA/ASDM リリース要件

- Cisco Secure Client VPN SAML 外部ブラウザを使用するには、Cisco Secure Firewall ASA 9.17.x（またはそれ以降）と ASDM 7.17.x（またはそれ以降）にアップグレードする必要があります。そのバージョンと Cisco Secure Client バージョン 5 を使用すると、VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO2、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、認証の選択肢をさらに加えることができます。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、Secure Client が Secure Client の組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。
- DTLSv1.2 を使用するには、Cisco Secure Firewall ASA 9.10.1 以降と ASDM 7.10.1 以降にアップグレードする必要があります。

（注） DTLSv1.2 は、5506-X、5508-X、および 5516-X を除くすべての Cisco Secure Firewall ASA モデルでサポートされており、ASA がクライアントとしてではなくサーバーとしてのみ機能している場合に適用されます。DTLS 1.2 は、現在のすべての TLS/DTLS 暗号方式と大きな Cookie サイズに加えて、追加の暗号方式をサポートしています。

- 管理 VPN トンネルを使用するには、ASDM 7.10.1 にアップグレードする必要があります。

- Network Visibility Module を使用するには、ASDM 7.5.1 にアップグレードする必要があります。
- AMP イネーブラを使用するには、ASDM 7.4.2 にアップグレードする必要があります。

（注） Cisco Secure Client リリース 5.0 には、AMP イネーブラは含まれていません。

- TLS 1.2 を使用するには、Cisco Secure Firewall ASA 9.3(2) にアップグレードする必要があります。
- 次の機能を使用する場合は、Cisco Secure Firewall ASA 9.2(1) にアップグレードする必要があります。
  - VPN を介した ISE ポスチャ
  - Cisco Secure Client の ISE 展開
  - ASA での認可変更（CoA）は、このバージョン以降でサポートされています。
- 次の機能を使用する場合は、Cisco Secure Firewall ASA 9.0 にアップグレードする必要があります。
  - IPv6 のサポート
  - シスコの次世代暗号化「Suite-B」セキュリティ
  - ダイナミック スプリット トンネリング（カスタム属性）
  - Cisco Secure Client 遅延アップグレード
  - 管理 VPN トンネル（カスタム属性）
- 次を実行する場合は、Cisco Secure Firewall ASA 8.4(1) 以降を使用する必要があります。
  - IKEv2 の使用。
  - ASDM による非 VPN クライアントプロファイル（ネットワーク アクセス マネージャなど）の編集。
  - ファイアウォールルールの展開。常時接続 VPN を展開するときは、スプリットトンネリングを有効にして、ローカル印刷デバイスとテザーモバイルデバイスへのネットワークアクセスを制限するファイアウォールルールを設定する必要がある場合があります。
  - 認定された VPN ユーザーを常時接続 VPN 展開から除外するダイナミック アクセス ポリシーまたはグループポリシーの設定。
  - Cisco Secure Client セッションが隔離されているときに Cisco Secure Client GUI にメッセージを表示するダイナミック アクセス ポリシーの設定。

- 4.3x から 4.6.x への Secure Firewall ポスチャ 移行を実行するには、ASDM 7.9.2 以降が必要です。

Cisco Secure Firewall ASA のメモリ要件

注意 Cisco Secure Client を使用するすべての Cisco Secure Firewall ASA モデルに推奨される最小フラッシュメモリは 512 MB です。これにより、ASA で複数のエンドポイント オペレーティング システムをホストし、ロギングとデバッグを有効にすることができます。

Cisco Secure Firewall ASA のフラッシュサイズの制限（最大 128 MB）により、Cisco Secure Client パッケージの一部の置換は、このモデルにロードできません。Cisco Secure Client を正常にロードするには、使用可能なフラッシュに収まるまでパッケージのサイズを小さくする必要があります（OS を減らす、Secure Firewall ポスチャ をなくすなど）。

Cisco Secure Client のインストールまたはアップグレードを続行する前に、使用可能なスペースを確認してください。これを行うには、次のいずれかの方法を使用できます。

- CLI：**show memory** コマンドを入力します。

```
asa3# show memory
Free memory:       304701712 bytes (57%)
Used memory:       232169200 bytes (43%)
-------------     ----------------
Total memory:      536870912 bytes (100%)
```

- ASDM：[Tools] > [File Management] を選択します。[ファイル管理（File Management）] ウィンドウにフラッシュスペースが表示されます。

Cisco Secure Firewall ASA にデフォルトの内部フラッシュメモリサイズかデフォルトの DRAM サイズ（キャッシュメモリ用）だけがある場合、ASA 上で複数の Cisco Secure Client パッケージを保存およびロードすると、問題が発生することがあります。フラッシュメモリにパッケージファイルを保持するために十分な容量がある場合でも、クライアントイメージの unzip とロードのときに Cisco Secure Firewall ASA のキャッシュメモリが不足する場合があります。ASA のメモリ要件と ASA のメモリアップグレードの詳細については、Cisco ASA の最新のリリースノートを参照してください。

Secure Firewall ポスチャ

Cisco Secure Client 5.0.x は、Secure Firewall Posture 5.0.x（またはそれ以降）を**使用する必要があります**。

（注） Cisco Secure Client 5.0.x は、互換性のないバージョンの HostScan と使用すると、VPN 接続を確立しません。したがって、Cisco Secure Client 5.0.x エンドポイントでの HostScan 4.x の使用はサポートされていません。

現在 **HostScan 4.3.x 以前**を使用している場合は、HostScan の新しいバージョンにアップグレードする前に、1 回限りの HostScan の移行を**実行する必要があります**。この移行の詳細については、『AnyConnect HostScan Migration 4.3.x to 4.6.x and Later』を参照してください。

また、Secure Firewall ポスチャ と ISE ポスチャの併用は推奨されません。2 つの異なるポスチャエージェントを実行する場合、予期しない結果が発生します。

Cisco Secure Firewall ポスチャモジュール（旧 HostScan）により、Cisco Secure Client は、Cisco Secure Firewall ASA のホストにインストールされているオペレーティングシステム、マルウェア対策、およびファイアウォールの各ソフトウェアを識別できます。

Start Before Login（SBL）および Secure Firewall ポスチャ を使用する場合、SBL は事前ログインであるため、完全な Secure Firewall ポスチャ 機能を実現するには、Cisco Secure Client 事前展開モジュールをエンドポイントにインストールする必要があります。

Secure Firewall Posture（独自のソフトウェアパッケージとして入手可能）は、新しいオペレーティングシステム、マルウェア対策、およびファイアウォール ソフトウェアの情報で定期的に更新されます。最新バージョンの Secure Firewall Posture（Cisco Secure Client のバージョンと同じ）を実行することをお勧めします。

Secure Firewall ポスチャ マルウェア対策およびファイアウォール サポート チャートは、Cisco.com で入手できます。

ISE ポスチャ準拠モジュール

（CSCwa91572）互換性と展開の容易さを実現するには、Cisco Secure Client バージョン 5.0.01242 以降で次のコンプライアンスモジュールを使用する必要があります（Windows バージョン 4.3.2755、macOS バージョン 4.3.2379、および Linux バージョン 4.3.2063）。また、すでにリリースされているコンプライアンスモジュールは、Cisco Secure Client バージョン 5.0.01242（およびそれ以降）のビルドではサポートされていません。

（CSCvy53730-Windows のみ）AnyConnect 4.9.06037 の時点では、ISE からコンプライアンスモジュールを更新できません。この変更により、AnyConnect 4.9.06037（およびそれ以降）と Cisco Secure Client 5（5.0.01242 まで）にはバージョン 4.3.1634.6145 以降のコンプライアンスモジュールが必要です。

ISE ポスチャ準拠モジュールには、ISE ポスチャでサポートされているマルウェア対策とファイアウォールのリストが含まれています。Secure Firewall ポスチャ のリストはベンダー別に編成されていますが、ISE ポスチャのリストは製品タイプ別に編成されています。ヘッドエンド（ISE または Cisco Secure Firewall ASA）のバージョン番号がエンドポイントのバージョンよりも大きい場合は、OPSWAT が更新されます。これらのアップグレードは必須であり、エンドユーザーの介入なしで自動的に実行されます。

ライブラリ（zip ファイル）内の個別のファイルは、OPSWAT, Inc. によってデジタル署名され、ライブラリ自体はシスコの証明書によって署名されたコードである単一の自己解凍実行可能ファイルとしてパッケージ化されています。詳細については、ISE コンプライアンスモジュールを参照してください。

Cisco Secure Client における iOS のサポート

シスコでは、セキュアゲートウェイとして機能する iOS リリース 15.1(2)T への AnyConnect VPN アクセスをサポートしています。 ただし、iOS リリース 15.1(2)T は現在、次の Cisco Secure Client 機能をサポートしていません。

- ログイン後の VPN 常時接続
- 接続障害ポリシー
- ローカル プリンタおよびテザーデバイスへのアクセスを提供するクライアント ファイアウォール
- 最適ゲートウェイ選択
- 検疫
- Cisco Secure Client プロファイルエディタ
- DTLSv1.2

AnyConnect VPN に関する IOS サポートのその他の制限については、「Features Not Supported on the Cisco IOS SSL VPN」[英語] を参照してください。

その他の IOS 機能のサポート情報については、http://www.cisco.com/go/fn [英語] を参照してください。

Cisco Secure Client がサポートするオペレーティングシステム

次の表に、サポートされている最小バージョンを示します。*8.x* などとは対照的に、特定のバージョンが示されているのは、特定のバージョンのみがサポートされているためです。たとえば、ISE ポスチャは Red Hat 8.0 ではサポートされていませんが、Red Hat 8.1 以降ではサポートされており、そのように記載しています。

表 *1 : Windows*

Windows のバージョン	VPN	Network Access Manager	Secure Firewall ポスチャ	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック	ネットワーク可視性モジュール	AMP イネーブラ	Umbrella ローミングセキュリティ	Secure Endpoint Agent
Windows 11（64 ビット）と現在 Microsoft がサポートしているバージョンの Windows 10 x86（32 ビット）および x64（64 ビット）	対応	対応	対応	対応	対応	対応	対応	非対応	対応	対応
ARM64 ベースの PC 用に Microsoft がサポートしているバージョンの Windows 10、Windows 11	対応	非対応	対応	対応	対応	対応	対応	×	対応	非対応

表 *2 : macOS*

macOS のバージョン	VPN	Network Access Manager	Secure Firewall ポスチャ	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック	ネットワーク可視性モジュール	AMP イネーブラ	Umbrella ローミングセキュリティ	Secure Endpoint Agent
MacOS 13 Ventura、macOS 12 Monterey、および macOS 11 Big Sur	対応	非対応	対応	対応	対応	対応	対応	対応	対応	MacOS 10.10 以降

表 *3 : Linux*

Linux のバージョン	VPN	Secure Firewall ポスチャ	ネットワーク可視性モジュール	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック
Red Hat	9.x および 8.x	9.x および 8.x	9.x および 8.x	9.x および 8.1（およびそれ以降）	対応	対応
Ubuntu	22.04 および 20.04	22.04 および 20.04	22.04 および 20.04	22.04 および 20.04	対応	対応
SUSE（SLES）	制限付きのサポート。ISE ポスチャのインストールにのみ使用	未サポート	未サポート	12.3（以降のバージョン）および 15.0（以降のバージョン）	対応	対応

Cisco Secure Client における Microsoft Windows のサポート

Windows の要件

- Pentium クラス以上のプロセッサ。
- 100 MB のハードディスク容量。
- Microsoft インストーラバージョン 3.1。
- 以前の Windows リリースから Windows 8.1 にアップグレードするには、Cisco Secure Client をアンインストールし、Windows のアップグレードが完了した後に再インストールする必要があります。
- Windows XP からそれ以降の Windows リリースにアップグレードする場合は、アップグレード時に Cisco Secure Client 仮想アダプタが保存されないため、クリーンインストールが必要です。Cisco Secure Client を手動でアンインストールし、Windows をアップグレードしてから手動で（または WebLaunch を介して）Cisco Secure Client を再インストールしてください。

- WebLaunch で Cisco Secure Client を起動するには、32 ビットバージョンの Firefox 3.0 以降を使用し、ActiveX を有効にするか Sun JRE 1.4 以降をインストールする必要があります。
- Windows 8 または 8.1 を使用する場合は ASDM バージョン 7.02 以降が必要です。

Windows の制約事項

- リリース 4.10.03104 より前の AnyConnect では、Windows ADVERTISE インストーラアクションはサポートされていませんでした（CSCvw79615）。リリース 4.10.03104 以降では、下位バージョンの AnyConnect を使用している場合に Windows ADVERTISE とともに正常にアップグレードするための修正が提供されています。ただし、AnyConnect バージョン 4.10.02086 以前（4.10.03104 以降ではなく）がアドバタイズされている場合は、今後のアップグレードが失敗する可能性があることに留意してください。
- Cisco Secure Client は、Windows RT ではサポートされません。このオペレーティングシステムでは、この機能を実装するための API が提供されません。シスコでは、この問題に関して Microsoft にオープンな要求を行っています。この機能をご希望の場合は、Microsoft に連絡して関心があることを表明してください。
- 他のサードパーティ製品と Windows 8 には互換性がないため、Cisco Secure Client はワイヤレスネットワーク経由で VPN 接続を確立できません。以下に、この問題の 2 つの例を示します。
  - Wireshark と共に配布されている WinPcap サービス「Remote Packet Capture Protocol v.0 (experimental)」は、Windows 8 をサポートしていません。

    この問題を回避するには、Wireshark をアンインストールするか WinPcap サービスを無効にして Windows 8 コンピュータを再起動し、Cisco Secure Client の接続を再試行します。
  - Windows 8 をサポートしない古いワイヤレスカードまたはワイヤレスカードドライバは、Cisco Secure Client による VPN 接続の確立を妨げます。

    この問題を回避するには、Windows 8 コンピュータが Windows 8 をサポートする最新のワイヤレス ネットワーク カードまたはドライバを備えていることを確認してください。
- Cisco Secure Client は、Windows 8 に導入されている Metro デザイン言語と呼ばれる新しい UI フレームワークと統合されません。ただし、Cisco Secure Client は Windows 8 においてデスクトップモードで動作します。
- HP Protect Tools は、Windows 8.x 上の Cisco Secure Client と連動しません。
- スタンバイをサポートするシステムでネットワーク アクセス マネージャを使用する場合は、デフォルトの Windows 8.x アソシエーションタイマー値（5 秒）を使用することをお勧めします。Windows でのスキャンリストの表示が予想より短い場合は、ドライバがネットワークスキャンを完了してスキャンリストに入力できるように、アソシエーションタイマーの値を増やしてください。

Windows での注意事項

- クライアントシステム上のドライバが、お使いの Windows のバージョンでサポートされていることを確認してください。サポートされていないドライバは、断続的な接続上の問題を発生させる可能性があります。
- ネットワーク アクセス マネージャについては、Microsoft KB 2743127 に記載されているレジストリ修正がクライアントデスクトップに適用されていないかぎり、マシンパスワードを使用するマシン認証が Windows 8 または 10/Server 2012 では機能しません。この修正には、DWORD 値 LsaAllowReturningUnencryptedSecrets を HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa レジストリキーに追加し、この値を 1 に設定することが含まれます。

  （マシンパスワードではなく）マシン証明書を使用したマシン認証では変更は不要であり、より安全なオプションです。マシンパスワードは暗号化されていない形式でアクセスできるため、Microsoft は特別なキーが必要になるように OS を変更しました。ネットワーク アクセス マネージャはオペレーティングシステムと Active Directory サーバー間で確立されたパスワードを認識できず、上記のキーを設定することによってのみパスワードを取得できます。この変更により、Local Security Authority（LSA）が Cisco Network Access Manager などのクライアントにマシンパスワードを提供できるようになります。

（注） マシン認証では、ユーザーがログインする前にクライアントデスクトップをネットワークに対して認証できます。その間、管理者は、このクライアントマシンに対してスケジュールされた管理タスクを実行できます。RADIUS サーバーが特定のクライアントに関してユーザーとマシンの両方を認証できる EAP チェーン機能にもマシン認証が必要です。これにより、企業資産が特定され、適切なアクセスポリシーが適用されます。たとえば、それが個人資産（PC/ラップトップ/タブレット）である場合、企業のログイン情報が使用されると、エンドポイントはマシン認証に失敗しますが、ユーザー認証は成功し、ユーザーのネットワーク接続に適切なネットワークアクセス制限が適用されます。

- Windows 8 では、[環境設定（Preferences）] > [VPN] > [統計（Statistics）] タブの [統計のエクスポート（Export Stats）] ボタンをクリックすると、ファイルがデスクトップに保存されます。他のバージョンの Windows では、ユーザーは、ファイルを保存する場所を尋ねられます。
- AnyConnect VPN は、WWAN アダプタを介して Windows と連動する 3G/4G/5G データカードと互換性があります。

Cisco Secure Client における Linux のサポート

Linux の要件

- GUI セッション（SSH など）を使用しない VPN CLI の使用はサポートされていません。
- インストールするには管理者権限が必要です。
- x86 命令セット
- 64 ビットプロセッサ
- 100 MB のハードディスク容量
- Linux カーネルでの TUN のサポート
- libnss3 (NSS 証明書ストアを使用している場合のみ)
- libstdc++ 6.0.19（GLIBCXX_3.4.19）以降
- iptables 1.4.21 以降
- NetworkManager 1.0.6 以降
- zlib（SSL deflate 圧縮をサポートするため）
- glib 2.36 以降
- polkit 0.105 以降
- gtk 3.8 以降
- systemd
- webkitgtk+ 2.10 以降（Cisco Secure Client 組み込みブラウザアプリケーションを使用する場合にのみ必要）
- libnm（libnm.so または libnm-glib.so）：Network Visibility Module を使用する場合にのみ必要

Cisco Secure Client における macOS のサポート

macOS の要件

- Cisco Secure Client には、50 MB のハードディスク容量が必要です。
- macOS で正しく動作させるには、Cisco Secure Client の最小ディスプレイ解像度を 1,024 X 640 ピクセルに設定する必要があります。

macOS での注意事項

macOS 用の Cisco Secure Client 4.8（以降）が認証され、インストーラ ディスク イメージ（dmg）がステープルされました。

Cisco Secure Client のライセンス

最新のエンドユーザーライセンス契約書については、『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』[英語] を参照してください

ISE ヘッドエンドから Cisco Secure Client を展開し、ISE ポスチャモジュールを使用するには、ISE 管理ノードに Cisco ISE Premier ライセンスが必要です。ISE ライセンスの詳細については、『Cisco Identity Services Engine 』[英語] の「*Cisco ISE Licenses*」の章を参照してください。

Cisco Secure Firewall ASA ヘッドエンドから Cisco Secure Client を展開して VPN と Secure Firewall ポスチャ モジュールを使用するには、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も使用できます。『Cisco Secure Client Ordering Guide』[英語] を参照してください。

Advantage および Premier ライセンスの概要と各機能で使用されるライセンスの説明については、『Cisco Secure Client Features, Licenses, and OSs』[英語] を参照してください。

Cisco Secure Client のインストールの概要

Cisco Secure Client の展開は、Cisco Secure Client と関連ファイルのインストール、設定、アップグレードを意味します。Cisco Secure Client は、次の方法によってリモート ユーザに展開できます。

- 事前展開：新規インストールとアップグレードは、エンドユーザによって、または社内のソフトウェア管理システム（SMS）を使用して実行されます。
- Web 展開：Cisco Secure Client パッケージは、ヘッドエンド（Cisco Secure Firewall ASA または ISE サーバー）にロードされます。ユーザが Cisco Secure Firewall ASA または ISE に接続すると、Cisco Secure Client がクライアントに展開されます。
  - 新規インストールの場合、ユーザーはヘッドエンドに接続して Cisco Secure Client をダウンロードします。クライアントは、手動でインストールするか、または自動（Web 起動）でインストールされます。
  - アップデートは、Secure Client がすでにインストールされているシステムで Cisco Secure Client を実行すること、またはユーザーを Cisco Secure Firewall ASA クライアントレスポータルに誘導することによって行われます。
- SecureX クラウド管理：SecureX UI の [展開の管理（Deployment Management）] ページにある [ネットワークインストーラ（Network Installer）] ボタンをクリックします。これにより、インストーラの実行可能ファイルがダウンロードされます。有効にする Secure Client オプション（Start Before Login、診断およびレポートツール、Cisco Secure Firewall ポスチャ、Network Visibility Module、Secure Umbrella、ISE ポスチャ、ネットワーク アクセス マネージャなど）も選択できます。

Cisco Secure Client を展開するときに、追加機能を有効にするオプションモジュールや VPN などの機能を設定するクライアントプロファイルを含めることができます。次の点を考慮してください。

- Cisco Secure Client モジュールおよびプロファイルはすべて事前展開できます。事前展開時には、モジュールのインストール手順やその他の詳細に特に注意する必要があります。
- VPN ポスチャモジュールによって使用されるカスタマー エクスペリエンス フィードバック モジュールと Secure Firewall ポスチャ パッケージは、ISE から Web 展開できません。
- ISE ポスチャモジュールによって使用されるコンプライアンスモジュールは、Cisco Secure Firewall ASA から Web 展開できません。

（注） 新しい Cisco Secure Client パッケージにアップグレードする場合は、必ずローカリゼーション MST ファイルを CCO の最新リリースで更新してください。

64 ビット Windows で Web ベースのインストールに失敗する場合がある

この問題は、Windows 8 上の Internet Explorer バージョン 10 および 11 に該当します。

Windows レジストリエントリ HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth が 0 に設定されている場合、Cisco Secure Client の Web 展開時に Active X で問題が発生します。

詳細については、http://support.microsoft.com/kb/2716529 を参照してください。

解決策は次のとおりです。

- 32 ビットバージョンの Internet Explorer を実行します。
- レジストリエントリを 0 以外の値に編集するか、レジストリからその値を削除します。

（注） Windows 8 では、Windows のスタート画面から Internet Explorer を起動すると 64 ビットバージョンが実行されます。デスクトップから起動すると 32 ビットバージョンが実行されます。

Cisco Secure Client サポートポリシー

シスコでは、最新の バージョン 5 リリースに基づいてのみ 5.x の修正と拡張機能を提供しています。TAC サポートは、Cisco Secure Client バージョン 5 のリリースバージョンを実行するアクティブな Cisco Secure Client バージョン 5 の契約期間を持つすべてのユーザーが利用できます。古いソフトウェアバージョンで問題が発生した場合は、現在のメンテナンスリリースで問題を解決できるかどうかの確認を求められることがあります。

Software Center へのアクセスは、最新の修正が適用された Cisco Secure Client バージョン 5 バージョンに制限されます。展開する予定のバージョンが将来もダウンロードできることを保証できないため、展開用にすべてのイメージをダウンロードすることをお勧めします。

注意事項と制約事項

Windows ARM64 の既知の問題

Windows ARM64 の既知の問題は次のとおりです。

- CSCwd81735：Cisco Secure Firewall ASA で Cisco Secure Firewall ポスチャ（以前の HostScan）が有効になっていて、Secure Client と同じ 5.0 バージョンを実行している場合、障害が発生する可能性がある。ただし、Secure Client UI にはステータスメッセージもエラーも表示されない。クライアントは引き続き正常に機能しており、[接続（Connect）] をクリックすると応答するが、ステータスメッセージには何も表示されない。
- CSCwd71408：ASA は、スクリプトを機能させるために、Cisco Secure Client バイナリファイルのカスタマイズのサポートを追加する必要がある。
- ISE ポスチャサービスを使用できない。csc_ise_agent を手動で再起動すると、サービスを復元できる。
- Java の ARM64 バージョンがサポートされていない。X86 または X64 バージョンのみサポートされる。
- ARM64 プラットフォームの Network Visibility Module の場合、モジュール名とモジュールハッシュが、SVCHost プロセス用に生成されたフローで報告されない。

VPN ヘッドエンドの DNS ロードバランシングがサポートされない

AnyConnect は、組み込みブラウザの SAML 認証を使用した DNS ロードバランシングをサポートしています。Secure Firewall ASA、Secure Firewall Threat Defense、またはその他のヘッドエンドと外部ブラウザまたはネイティブブラウザを使用すると、VPN ヘッドエンドの DNS ロードバランシングはサポートされません。これは、オペレーティングシステムの制限により、Cisco Secure Client が必要な基本条件を制御する機能が制限されるためです。

同時 VPN セッションはサポートされない

AnyConnect VPN は、他のクライアント VPN（ユニバーサル Windows プラットフォーム用の Cisco Secure Client のようなシスコソフトウェア、またはサードパーティの VPN のいずれか）と同時にアクティブにできません。

macOS 13 の既知の問題

現時点では、macOS 13 の Continuity Camera はアクティブな VPN 接続中は機能していません。

macOS 12.x での DNS（名前解決）が失敗することがある

macOS 12.x で Cisco Secure Client を実行している場合、DNS（名前解決）が失われ、復元のために再起動が必要になる場合があります。この問題の原因は macOS のバグとして特定されており、macOS 12.3（FB9803355）で解決されています。

Windows のローカルグループポリシーの DNS 設定は無視される

グローバル DNS 設定の Searchlist と UseDomainNameDevolution は、VPN 接続の DNS サフィックス検索リストを作成するために Cisco Secure Client で使用されます。ローカルグループポリシーを使用して設定されたオーバーライドはすべて無視されます。

ルート CA と Firefox NSS ストアの競合（Linux のみ）

ルート認証局（CA）が公的に信頼されている場合、その CA はすでにファイル証明書ストアにあります。ただし、シスコではファイル証明書ストアでの OCSP チェックのみをサポートしているため、Firefox NSS ストアが同時に有効になっていると、OCSP チェックがバイパスされる可能性があります。こうしたバイパスを防ぐには、ローカルポリシーファイルで ExcludeFirefoxNSSCertStore を *true* に設定して Firefox NSS ストアを無効にします。

TND との自動 VPI 接続の開始（CSCvz02896）

信頼ネットワーク検出を使用している場合、システムルートテーブルにデフォルトルートが含まれていなければ、TND ポリシーに従って自動 VPN 接続が開始されないことがあります。

Linux での AnyConnect 4.10 アップグレードの失敗（4.9.01095 よりも前の AnyConnect バージョンのみ）

Web 展開を使用して 4.9.01095 より前のバージョンから AnyConnect または HostScan 4.10 にアップグレードすると、エラーが発生する可能性があります。バージョン 4.9.01095 よりも前の AnyConnect にはシステム CA ストアを解析する能力がなく、ユーザーのプロファイルディレクトリで正しい NSS 証明書ストアのパスを特定できないため、アップグレードが失敗します。4.9.01095 より前のリリースから AnyConnect 4.10 にアップグレードする場合は、エンドポイントで AnyConnect をアップグレードする前に、ルート証明書（DigiCertAssuredIDRootCA.pem）を /opt/.cisco/certificates/ca にコピーします。

Ubuntu 20 で NVM のインストールが失敗する

（カーネルバージョンが 5.4 の）Ubuntu 20.04 を使用している場合は、AnyConnect 4.8 以降を使用する必要があります。そうしないと Network Visibility Module のインストールに失敗します。

ローカルおよびネットワークのプロキシの非互換性

ローカルやネットワークのプロキシ（Web HTTP/HTTPS インスペクションや復号の機能を含む、Fiddler、Charles Proxy、またはサードパーティ製マルウェア対策/セキュリティソフトウェ

アなどのソフトウェア/セキュリティ アプリケーション）は、Cisco Secure Client と互換性がありません。

Linux での Web 展開ワークフローの制限事項

Linux で Web 展開を行う場合は、次の 2 つの制限事項を考慮してください。

- Ubuntu NetworkManager の接続確認機能を使用すると、インターネットにアクセスできるかどうかを定期的にテストできます。接続確認には独自のプロンプトがあるため、インターネット接続のないネットワークが検出された場合は、ネットワーク ログオン ウィンドウを表示できます。ブラウザウィンドウに関連付けられておらず、ダウンロード機能がないネットワークプロンプトを回避するには、Ubuntu 17 以降で接続確認を無効にする必要があります。無効にすることで、ユーザーは ISE ベースの Cisco Secure Client Web 展開用にブラウザを使用して ISE ポータルからファイルをダウンロードできます。
- Linux エンドポイントに Web 展開を行う前に、xhost+ コマンドを使用してアクセス制御を無効にする必要があります。xhost は、デフォルトで制限されているエンドポイントで端末を実行しているリモートホストのアクセスを制御します。アクセス制御を無効にしないと、Cisco Secure Client Web 展開は失敗します。

AnyConnect 4.9.01xxx へのアップグレード後にクライアントの最初の自動再接続が失敗する（Linux のみ）

CSCvu65566 の修正とそのデバイス ID 計算の変更により、Linux の特定の展開（特に LVM を使用する展開）では、ヘッドエンドから 4.9.01xxx 以降に更新した直後に 1 回限りの接続試行エラーが発生します。AnyConnect 4.8 以降を実行し、自動更新（Web 展開）を実行するためにヘッドエンドに接続している Linux ユーザーは、次のエラーを受け取る場合があります。「セキュアゲートウェイが接続試行を拒否しました。同じまたは別のセキュアゲートウェイへの新しい接続の試行が必要であり、再認証が必要です。（The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication.）」正常に接続するには、Cisco Secure Client のアップグレード後に別の VPN 接続を手動で開始します。4.9.01xxx 以降に最初にアップグレードした後は、この問題は発生しません。

AnyConnect 4.7MR4 からのアップグレード後のワイヤレスネットワークへの接続に関する潜在的な問題

ネットワーク アクセス マネージャは、メモリ内の一時プロファイルを使用するのではなく、ワイヤレス LAN プロファイルをディスクに書き込むように改訂されました。Microsoft は OS のバグに対処するためにこの変更を要求しましたが、[ワイヤレスLANデータの使用状況（Wireless LAN Data Usage）] ウィンドウがクラッシュし、最終的に断続的なワイヤレス接続の問題が発生しました。これらの問題を防ぐために、ネットワーク アクセス マネージャを、メモリ内の元の一時的な WLAN プロファイルを使用するように戻しました。ネットワーク アクセス マネージャは、バージョン 4.8MR2 以降にアップグレードするときに、ディスク上のほとんどのワイヤレス LAN プロファイルを削除します。一部のハードプロファイルは、指示さ

れたときにOS WLANサービスによって削除できませんが、ネットワーク アクセス マネージャがワイヤレスネットワークに接続する機能を妨げるものがあります。4.7MR4 から 4.8MR2 へのアップグレード後にワイヤレスネットワークへの接続に問題が発生した場合は、次の手順を実行します。

1. Secure Client ネットワーク アクセス マネージャ サービスを停止します。
2. 管理者のコマンドプロンプトから、次のように入力します

```
netsh wlan delete profile name=*(AC)
```

これにより、以前のバージョン（Secure Client 4.7MR4 ー 4.8MR2）から残りのプロファイルが削除されます。または、名前に **AC** が追加されたプロファイルを検索し、ネイティブサプリカントから削除することもできます。

nslookup コマンドを予期したように機能させるには MacOS の修正が必要

macOS 11 では、nslookup コマンドに関連する AnyConnect バージョン 4.8.03036 以降で発生した問題（split-include トンネリング構成で nslookup が VPN トンネルを介して DNS クエリを送信しない問題）が修正されました。この問題は、不具合 CSCvo18938 の修正がそのバージョンに含まれていた場合に AnyConnect 4.8.03036 で発生します。Apple が提案したその不具合の変更により、nslookup の問題動作を引き起こす別の OS の 問題が明らかになりました。

macOS 10.x の回避策として、VPN DNS サーバーをパラメータとして nslookup に渡すことができます（**`nslookup [name] [ip_dnsServer_vpn]`**）。

サーバー証明書の検証エラー

（CSCvu71024）Cisco Secure Firewall ASA ヘッドエンドまたは SAML プロバイダーが AddTrust ルート（またはいずれかの仲介者）によって署名された証明書を使用する場合、2020 年 5 月に期限切れになるため、Cisco Secure Client 認証が失敗する場合があります。期限切れの証明書は、オペレーティングシステムが 2020 年 5 月の有効期限に対応するのに必要な更新を行うまで、Cisco Secure Client の失敗の原因となり、サーバー証明書検証エラーとして表示されます。

Windows DNS クライアントの最適化に関する注意事項

Windows 8 以降の Windows DNS クライアント最適化では、スプリット DNS が有効になっている場合に、特定のドメイン名の解決に失敗する可能性があります。回避策は、次のレジストリキーを更新して、このような最適化を無効にすることです。

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
Value:DisableParallelAandAAAA
Data: 1
Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient
Value: DisableSmartNameResolution
Data: 1
```

macOS 10.15 ユーザーの準備

macOS 10.15 オペレーティングシステムでは、32 ビットのバイナリがサポートされません。さらに、10.15 にインストールされているすべてのソフトウェアは、デジタル署名によって暗号的に認証されていることが Apple に確認されます。AnyConnect 4.8 以降、macOS 10.15 での操作は 32 ビットコードなしでサポートされます。

次の制限事項に注意してください。

- 4.7.03052 よりも前の AnyConnect バージョンでは、アップグレードにアクティブなインターネット接続が必要な場合があります。
- 4.8.x より前の HostScan バージョンは、macOS 10.15 では機能しません。
- macOS 10.15 で Secure Firewall ポスチャ と ISE ポスチャ を使用する場合、初回起動時に権限ポップアップが表示されます。

Secure Firewall ポスチャ はアップグレードなしの macOS 10.15 では機能しない（CSCvq11813）

4.8.x より前の HostScan パッケージは、macOS Catalina（10.15）では機能しません。4.8.x より前の HostScan パッケージを実行しているエンドユーザーが macOS Catalina から Cisco Secure Firewall ASA ヘッドエンドに接続しようとすると、VPN 接続を正常に完了できず、ポスチャ評価失敗メッセージを受信します。

macOS Big Sur (11.x) 上の AnyConnect 4.10.x クライアントでは、HostScan 4.9.04045 以降を使用する必要があります。

Secure Firewall ポスチャ ユーザが VPN 接続を正常に行えるようにするには、すべての DAP ポリシーと Secure Firewall ポスチャ ポリシーが HostScan 4.8.00175 （以降）に準拠していなければなりません。HostScan 4.3.x から 4.8.x へのポリシー移行に関するその他の情報については、『AnyConnect HostScan Migration 4.3.x to 4.6.x and Later』[英語] を参照してください。

VPN 接続を復元するための回避策として、Cisco Secure Firewall ASA ヘッドエンドに Secure Firewall ポスチャ パッケージを使用するシステムの管理者が Secure Firewall ポスチャ を無効にする方法があります。無効にすると、すべての Secure Firewall ポスチャ のポスチャ機能、およびエンドポイント情報に依存する DAP ポリシーは使用できなくなります。

関連する Field Notice については、https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70445.html [英語] を参照してください。

Secure Firewall ポスチャ またはISE ポスチャの初回起動時の権限ポップアップ（CSCvq64942）

macOS 10.15（およびそれ以降）では、デスクトップ、ドキュメント、ダウンロード、およびネットワークボリュームの各フォルダにアクセスするためのユーザー権限をアプリケーションが取得する必要があります。このアクセス権を付与するにあたり、Secure Firewall ポスチャ の初回起動時にISE ポスチャ（ネットワークで ISE ポスチャが有効になっている場合）、または DART（ISE ポスチャまたは Cisco Secure Client がインストールされている場合）のポップアッ

プが表示されることがあります。ISE ポスチャと Secure Firewall ポスチャ はエンドポイントのポスチャアセスメントに OPSWAT を使用し、設定された製品とポリシーに基づいてポスチャがこれらのフォルダのアクセス権を確認します。

このようなポップアップでは、[OK] をクリックしてこれらのフォルダへのアクセスを許可し、ポスチャ フローを続行する必要があります。[許可しない（Don't Allow）] をクリックした場合、エンドポイントが準拠しなくなり、これらのフォルダにアクセスせずにポスチャ評価および修復が失敗することがあります。

[許可しない（Don't Allow）] の選択を修復するには

これらのポップアップを再表示してフォルダにアクセス権を付与するには、キャッシュされた設定を編集します。

1. [システム設定（System Preferences）] を開きます。
2. **[セキュリティおよびプライバシー（Security & privacy）]** > **[プライバシー（Privacy）]** > **[ファイルおよびフォルダ（Files and Folders）]** に移動します。
3. Cisco Secure Client フォルダ内のフォルダアクセスに関連するキャッシュの詳細を削除します。

権限ポップアップの再表示に続いてポスチャが開始され、ユーザーが [OK] をクリックするとアクセス権を付与できます。

macOS での GUI カスタマイズはサポートされていない

MacOS での GUI リソースのカスタマイズは現在サポートされていません。

SentinelOne との非互換性

Cisco Secure Client Umbrella モジュールは、SentinelOne エンドポイント セキュリティ ソフトウェアと互換性がありません。

4.8 へのアップグレード後に macOS 管理トンネルが切断される

次のいずれかのシナリオが発生した場合は、Apple 認証に準拠するためのセキュリティ改善に関連しています。

- AnyConnect 4.7 では管理トンネル接続ができていた同じ環境で、AnyConnect 4.8 バージョンが失敗する。
- VPN統計情報ウィンドウに、管理トンネルの状態として「接続解除（接続失敗）（Disconnect (Connect Failed)）」と表示される。
- コンソール ログには、「証明書の検証エラー（Certificate Validation Failure）」が示される。これは、管理トンネルの接続解除を意味します。

Cisco Secure Client アプリケーションまたは実行可能ファイルへのアクセスを（プロンプトなしで）許可するように設定されている場合、AnyConnect 4.8（以降）にアップグレードした後に、

アプリケーションまたは実行可能ファイルを再度追加してACLを再設定する必要があります。vpnagentd プロセスを含めるには、キーチェーンアクセスのシステムストアの秘密キーアクセスを変更する必要があります。

1. **[システムキーチェーン（System Keychain）] > [システム（System）] > [証明書（My Certificates）] > [秘密キー（Private key）]**の順に移動します。
2. [アクセス制御（access control）] タブから vpnagentd プロセスを削除します。
3. 現在の vpnagentd を /opt/cisco/secureclient/bin フォルダに追加します。
4. プロンプトが表示されたら、パスワードを入力します。
5. キーチェーンアクセスを終了し、VPN サービスを停止します。
6. 再起動します。

PMK ベースのローミングはネットワーク アクセス マネージャでサポートされていない

Windows では、ネットワーク アクセス マネージャで PMK ベースのローミングを使用できません。

DART には Admin 権限が必要

システムセキュリティの制約により、DART でログを収集するには、macOS、Ubuntu、および Red Hat の管理者権限が必要になりました。

FIPS モードで復元される IPsec 接続（CSCvm87884）

AnyConnect リリース 4.6.2 および 4.6.3 には、IPsec 接続の問題がありました。AnyConnect リリース 4.7 以降で IPsec 接続（CSCvm87884）を復元する場合、FIPS モードの Diffie-Hellman グループ 2 および 5 がサポートされなくなります。そのため、FIPS モードの Cisco Secure Client は、リリース 9.6 より古い Cisco Secure Firewall ASA および DH グループ 2 または 5 を指定するように設定された Cisco Secure Firewall ASA に接続できなくなっています。

Firefox 58 上の証明書ストアデータベース（NSS ライブラリ更新）にともなう変更点

（*58* より前のバージョンの *Firefox* を使用しているユーザーにのみ影響）Firefox 58 以降、NSS 証明書ストア DB 形式が変更されたため、Cisco Secure Client も新しい証明書 DB を使用するように変更されました。58 より前のバージョンの Firefox を使用している場合は、Firefox と Cisco Secure Client が同じ DB ファイルにアクセスできるように、NSS_DEFAULT_DB_TYPE="sql" 環境変数を 58 に設定してください。

ネットワーク アクセス マネージャおよびグループポリシーとの競合

有線またはワイヤレスネットワーク設定や特定の SSID が Windows グループポリシーからプッシュされた場合、それらはネットワーク アクセス マネージャの適切な動作と競合する可能性

があります。ネットワーク アクセス マネージャがインストールされている場合、ワイヤレス設定のグループポリシーはサポートされません。

Windows 10 バージョン 1703 でネットワーク アクセス マネージャに非表示ネットワークスキャンリストがない（CSCvg04014）

Windows 10 バージョン 1703 では、WLAN の動作が変更されたため、ネットワーク アクセス マネージャがワイヤレスネットワーク SSID をスキャンするときに中断が発生していました。Microsoft が調査中の Windows コードのバグのために、ネットワーク アクセス マネージャの非表示ネットワークへのアクセスの試みが影響を受けます。最適なユーザーエクスペリエンスを提供するために、ネットワーク アクセスマネージャのインストール時に2つのレジストリキーを設定し、アンインストール時にそれらを削除することによって、Microsoft の新機能を無効化しています。

Cisco Secure Client の macOS 10.13（High Sierra）互換性

AnyConnect 4.5.02XXX 以降では、macOS の [システム環境設定（Preferences）]>[セキュリティとプライバシー（Security & Privacy）] ペインで Secure Client（旧 AnyConnect） ソフトウェア拡張機能を有効にすることにより、全機能を活用するのに必要な手順をガイドする追加機能と警告が提供されます。ソフトウェア拡張機能を手動で有効にする必要があることが、macOS 10.13（High Sierra）の新しいオペレーティングシステム要件です。さらに、ユーザーのシステムを macOS 10.13 以降にアップグレードする前に Secure Client をアップグレードすると、Secure Client ソフトウェア拡張機能は自動的に有効になります。

ユーザーのシステムが macOS 10.13（以降）である場合、4.5.02XXX より前のバージョンを使用しているときは、macOS の [システム環境設定（Preferences）]>[セキュリティとプライバシー（Security & Privacy）] ペインで Secure Client（旧 AnyConnect）ソフトウェア拡張機能を有効にする必要があります。拡張機能を有効にした後は、手動での再起動が必要になる場合があります。

macOS システム管理者は User Approved Kernel Extension Loading を無効にする追加機能を利用できる場合があります（https://support.apple.com/en-gb/HT208019 [英語] を参照）。これは現在サポートされているバージョンの Secure Client で有効です。

電源イベントまたはネットワークの中断が発生したときのポスチャへの影響

ネットワークの変更または電源イベントが発生した場合、中断されたポスチャプロセスは正常に完了しません。ネットワークまたは電力の変更により、Cisco Secure Client ダウンローダーエラーが発生します。ユーザーがこれを確認しないと、プロセスを続行できません。

ネットワーク アクセス マネージャが WWAN/3G/4G/5G に自動的にフォールバックしない

WWAN/3G/4G/5G へのすべての接続は、ユーザーによって手動でトリガーされる必要があります。有線またはワイヤレス接続を利用できない場合、ネットワーク アクセス マネージャは、これらのネットワークに自動的に接続しません。

NAM、DART、ISE ポスチャ、またはポスチャの Web 展開が署名/ファイル整合性検証エラーで失敗する

「タイムスタンプの署名及び/または証明書を検証できないか、または形式が違います（timestamp signature and/or certificate could not be verified or is malformed）」というエラーは、Windows でのみ、Cisco Secure Firewall ASA または ISE からの AnyConnect 4.4MR2（またはそれ以降）の Web 展開時に発生します。MSI ファイルとして展開されるネットワーク アクセス マネージャ、DART、ISE ポスチャ、およびポスチャモジュールだけが影響を受けます。SHA-2 タイムスタンプ証明書サービスを使用することから、タイムスタンプ証明書チェーンを正しく検証するために、最新の信頼できるルート証明書が必要です。事前展開や、ルート証明書を自動的に更新するように設定された標準の Windows システムでは、この問題は発生しません。ただし、自動ルート証明書更新設定が無効になっている（デフォルトではない）場合は、https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx [英語] を参照するか、シスコが使用するタイムスタンプルート証明書を手動でインストールしてください。署名ツールを使用して、Microsoft 提供の Windows SDK からコマンドを実行することにより、問題が Cisco Secure Client の

```
signtool.exe verify /v /all/debug/pa<file to verify>
```

外部にあるかどうかを確認することもできます。

認証時の macOS キーチェーンプロンプト

macOS では、VPN 接続の開始後にキーチェーン認証プロンプトが表示される場合があります。このプロンプトは、セキュアゲートウェイからのクライアント証明書要求後に、クライアント証明書の秘密キーへのアクセスが必要な場合にのみ表示されます。トンネルグループに証明書認証が設定されていなくても、Cisco Secure Firewall ASA で証明書マッピングが 設定されている可能性があります。その場合、クライアント証明書の秘密キーのアクセス制御設定が [アクセスを許可する前に確認する（Confirm Before Allowing Access）] に設定されているとキーチェーンプロンプトが表示されます。

ログインキーチェーンからクライアント証明書への Secure Client のアクセスを制限するように Cisco Secure Client プロファイルを設定します（ASDM プロファイルエディタで、[設定（パート1）（Preferences (Part 1)）] > [証明書ストア（Certificate Store）] > [macOS] の [ログイン（Login）] を選択）。キーチェーン認証プロンプトを停止するには、次のいずれかの操作を行います。

- 既知のシステムキーチェーン証明書を除外するようにクライアントプロファイルの証明書一致基準を設定します。
- Cisco Secure Client へのアクセスを許可するようにシステムキーチェーン内のクライアント証明書秘密キーのアクセス制御設定を指定します。

Umbrella ローミング セキュリティ モジュールの変更

`OrgInfo.json` ファイルを取得するためのダッシュボードは、https://dashboard.umbrella.com です。そこから [アイデンティティ（Identity）]>[ローミングコンピュータ（Roaming Computers）] の順に移動し、左上にある [+]（追加アイコン）をクリックして、[Cisco Secure Client Umbrella

ローミングセキュリティモジュール（AnyConnect Umbrella Roaming Security Module）]セクションの [モジュールプロファイル（Module Profile）] をクリックします。

Cisco Secure Client の Microsoft Windows 10 との互換性

最良の結果を得るために、Windows 7/8/8.1 からのアップグレードではなく Windows 10 システムへの Cisco Secure Client のクリーンインストールをお勧めします。Cisco Secure Client がプレインストールされた Windows 7/8/8.1 からアップグレードする場合は、オペレーティングシステムをアップグレードする前に、必ず、まず Cisco Secure Client をアップグレードしてください。Windows 10 にアップグレードする前に、ネットワーク アクセス マネージャ モジュールをアンインストールする**必要があります**。システムのアップグレードが完了したら、ネットワーク アクセス マネージャをシステムに再インストールできます。また、Windows 10 へのアップグレード後に、Cisco Secure Client を完全にアンインストールし、サポートされているいずれかのバージョンを再インストールすることもできます。

新しいスプリット包含トンネルの動作（CSCum90946）

以前は、スプリット包含ネットワークがローカル サブネットのスーパーネットである場合、ローカルサブネットと完全に一致するスプリット包含ネットワークが設定されていないかぎり、ローカル サブネット トラフィックはトンネリングされませんでした。CSCum90946 の解決により、スプリット包含ネットワークがローカルサブネットのスーパーネットである場合、アクセスリスト（ACE/ACL）でスプリット除外（deny 0.0.0.0/32 or ::/128）も設定されていないかぎり、ローカル サブネット トラフィックはトンネリングされます。

スーパーネットがスプリット包含 で設定されており、かつ、 目的の動作が LocalLan アクセスの許可である場合、次の設定が必要です。

- アクセスリスト（ACE/ACL）には、スーパーネットに関する許可アクションと、0.0.0.0/32 または ::/128 に関する拒否アクションの両方を含める必要があります。
- プロファイルエディタの Cisco Secure Client プロファイル（[設定（パート1）（Preferences (Part 1)）] メニュー）で [ローカルLANアクセス（Local LAN Access）] を有効にします（ユーザー制御可能にするオプションもあります）。

認証に SHA512 証明書を使用した場合に認証に失敗する

（バージョン 4.9.03047 以前の AnyConnect を実行している Windows 7、8、および 8.1 ユーザーの場合）クライアントが認証に SHA512 証明書を使用すると、証明書が使用されていることがクライアントログに記録されていても認証は失敗します。ASA ログには、AnyConnect によって証明書が送信されていないことが正しく示されます。これらのバージョンの Windows では、TLS 1.2 で SHA512 証明書のサポートを有効にする必要があります。これはデフォルトではサポートされていません。これらの SHA512 証明書のサポートの有効化については https://support.microsoft.com/en-us/kb/2973337 を参照してください。4.9.03049

ISE ポスチャでのログ トレースの使用

新規インストールが完了すると、予期どおりの動作として、ISE ポスチャ ログ トレース メッセージが表示されます。ただし、ISE ポスチャ プロファイル エディタを開いて [エージェント ログトレースファイルの有効化（Enable Agent Log Trace file）] を 0（無効）に変更する場合は、期待どおりの結果を得るために Cisco Secure Client のサービスを再起動する必要があります。

macOS での ISE ポスチャとの相互運用性

macOS 10.9 以降を使用しており、ISE ポスチャを使用する場合は、問題を回避するために次の作業を行う必要があります。

- ポスチャアセスメント時に「ポリシーサーバーへの接続の失敗」というエラーが発生することを回避するには、証明書の検証を無効にします。
- キャプティブ ポータル アプリケーションを無効にします。無効にしない場合は、検出プローブがブロックされ、アプリケーションはポスチャ前の ACL 状態のままになります。

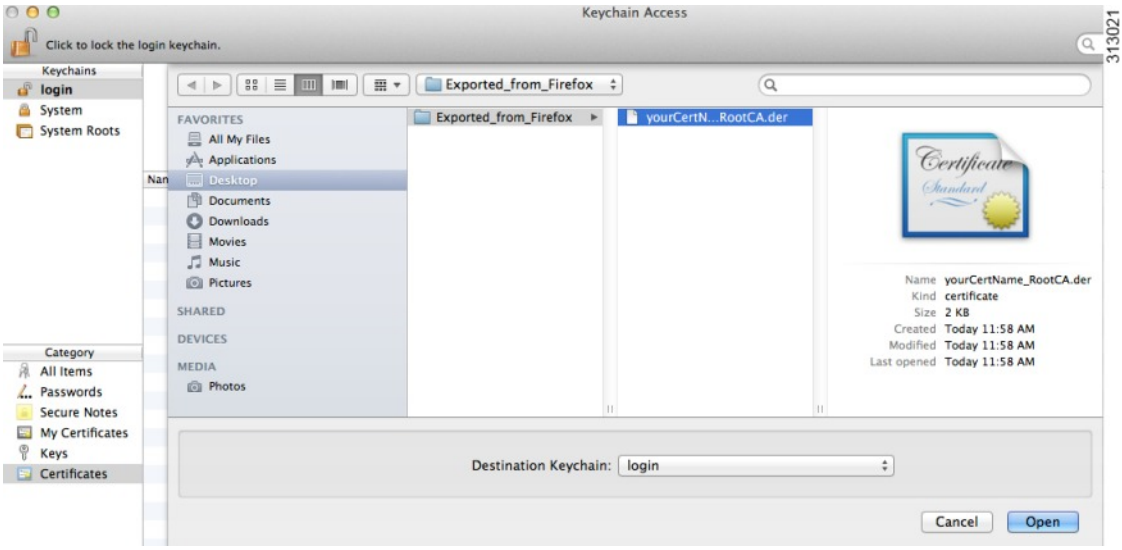
macOS 上の Firefox 証明書ストアはサポートされない

macOS 上の Firefox 証明書ストアは、任意のユーザーによるストアの内容の変更を許可するアクセス権を使用して保存されます。これにより、未認可のユーザーまたはプロセスが不正な CA を信頼されたルートストアに追加することが可能になります。Cisco Secure Client は、サーバー検証またはクライアント証明書に Firefox ストアを使用しなくなりました。

必要に応じて、Cisco Secure Client 証明書を Firefox の証明書ストアからエクスポートする方法とそれらを macOS キーチェーンにインポートする方法をユーザーに指示してください。一例として、Cisco Secure Client ユーザーに次のような手順を伝えます。

1. Firefox の [オプション（Preferences）]>[プライバシーとセキュリティ（Privacy & Security）]>[詳細設定（Advanced）] の [証明書（Certificates）] タブに移動し、[証明書を表示（View Certificates）] をクリックします。
2. Cisco Secure Client に使用する証明書を選択し、[エクスポート（Export）] をクリックします。

   多くの場合、Cisco Secure Client 証明書は [認証局証明書（Authorities）] カテゴリにあります。目的の証明書は別のカテゴリ（[あなたの証明書（Your Certificates）] または [サーバー証明書（Servers）]）に含まれている可能性があるため、証明書管理者に確認してください。
3. 証明書を保存する場所（デスクトップ上のフォルダなど）を選択します。
4. [ファイルの種類（Format）] プルダウンメニューで、[X.509 証明書（DER）（X.509 Certificate (DER)）] を選択します。必要に応じて、証明書名に .der 拡張子を追加します。

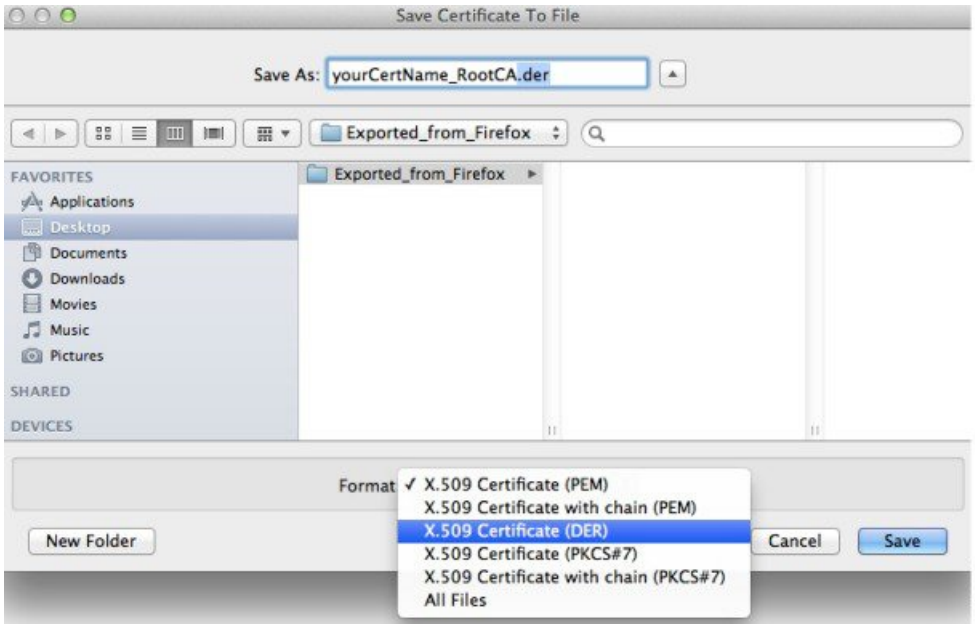


（注） 複数の Cisco Secure Client 証明書または秘密キー（あるいはその両方）が使用される場合や必要な場合は、証明書ごとに上記のプロセスを繰り返してください。

5. KeyChain を起動します。[ファイル（File）]>[アイテムのインポート...（Import Items…）] に移動し、Firefox からエクスポートした証明書を選択します。

   [宛先キーチェーン:（Destination Keychain:）] で目的のキーチェーンを選択します。この例で使用されているログインキーチェーンは、ユーザーの会社で使用されているものと異なる場合があります。証明書をインポートする必要があるキーチェーンについては、証明書管理者に問い合わせてください。

6. [宛先キーチェーン:（Destination Keychain:）] で目的のキーチェーンを選択します。この例で使用されているログインキーチェーンは、ユーザーの会社で使用されているものと異なる場合があります。証明書をインポートする必要があるキーチェーンについては、証明書管理者に問い合わせてください。



7. Cisco Secure Client に使用される（または必要な）追加の証明書について、上記の手順を繰り返します。

Active X のアップグレードで WebLaunch が無効になることがある

ActiveX コントロールに必要な変更を加えない限り、WebLaunch による Cisco Secure Client ソフトウェアの自動アップグレードは、限定的なユーザーアカウントで機能します。

場合によっては、このコントロールが、セキュリティの修正または新しい機能の追加によって変更されます。

限定的なユーザーアカウントからコントロールを起動するときにコントロールのアップグレードが必要な場合、管理者は、Cisco Secure Client プレインストーラ、SMS、GPO、またはその他の管理展開方法を使用してコントロールを展開する必要があります。

Java 7 の問題

Java 7 では、Cisco Secure Client と Secure Firewall ポスチャ で問題が発生する可能性があります。この問題と回避策については、トラブルシューティングテクニカルノートの『ava 7 Issues with AnyConnect, CSD/HostScan, and WebVPN - Troubleshooting Guide』[英語]（[セキュリティ（Security）] > [Cisco Secure Firewall ポスチャ] にあるシスコのドキュメント）を参照してください。

トンネルオールネットワークが設定されていると暗黙の DHCP フィルタが適用される

Cisco Secure Client は、すべてのネットワークのトンネルが設定されているときにローカル DHCP トラフィックを暗号化せずに流せるようにするために、Cisco Secure Client の接続時にローカル DHCP サーバーに特殊なルートを追加します。また、このルートでのデータ漏洩を防

ぐため、Cisco Secure Client はホストマシンの LAN アダプタに暗黙的なフィルタを適用し、DHCP トラフィックを除く、そのルートのすべてのトラフィックをブロックします。

テザーデバイス上の Cisco Secure Client

Bluetooth か USB でテザリングされた携帯電話またはモバイルデータデバイスが提供するネットワーク接続は、シスコによって特に認定されていないため、展開前に Cisco Secure Client で検証する必要があります。

Cisco Secure Client スマートカードのサポート

Cisco Secure Client は、次の環境でスマートカードによって提供されるログイン情報に対応します。

- Windows 7、Windows 8、Windows 10 上の Microsoft CAPI 1.0 および CAPI 2.0。
- macOS 上のキーチェーンと macOS 10.12 以降上の CryptoTokenKit。

（注） Cisco Secure Client は、Linux または PKCS #11 デバイスではスマートカードをサポートしていません。

Cisco Secure Client 仮想テスト環境

シスコは、次の仮想マシン環境を使用して Cisco Secure Client クライアントテストの一部を実行します。

- VM Fusion 7.5.x、10.x、11.5.x
- ESXi ハイパーバイザ 6.0.0、6.5.0、および 6.7.x
- VMware Workstation 15.x

仮想環境での Cisco Secure Client の実行はサポートしませんが、Cisco Secure Client はシスコがテストする VMware 環境で適切に機能すると予測されます。

仮想環境で Cisco Secure Client の問題が発生した場合は、報告してください。シスコが解決に向けて最善を尽くします。

自動更新を無効にするとバージョンの競合によって接続が妨げられる場合がある

Cisco Secure Client を実行するクライアントの自動更新が無効になっている場合、Cisco Secure Firewall ASA に同じバージョンかそれ以前のバージョンの Cisco Secure Client がインストールされていないと、クライアントは VPN に接続できません。

この問題を回避するには、Cisco Secure Firewall ASA で同じバージョンかそれ以前のバージョンの Cisco Secure Client パッケージを設定するか、自動更新を有効にしてクライアントを新しいバージョンにアップグレードします。

ネットワーク アクセス マネージャと他の接続マネージャの間の相互運用性

ネットワーク アクセス マネージャが動作している場合、ネットワーク アダプタが排他的に制御され、他のソフトウェア接続マネージャ（Windows のネイティブ接続マネージャを含む）による接続確立の試みがブロックされます。そのため、Cisco Secure Client ユーザーにエンドポイントコンピュータ上の他の接続マネージャ（iPassConnect Mobility Manager など）を使用させる場合は、ネットワーク アクセス マネージャ GUI のクライアント無効化オプションを使用するか、ネットワーク アクセス マネージャ サービスを停止することによって、ネットワーク アクセス マネージャを無効にする必要があります。

ネットワーク アクセス マネージャと互換性のないネットワーク インターフェイス カード ドライバ

Intel ワイヤレス ネットワーク インターフェイス カード ドライバ バージョン 12.4.4.5 は、ネットワーク アクセス マネージャと互換性がありません。このドライバがネットワーク アクセス マネージャと同じエンドポイントにインストールされている場合、一貫性のないネットワーク接続や Windows オペレーティングシステムの突然のシャットダウンが発生する可能性があります。

Cisco Secure Client 用のウイルス対策アプリケーションの設定

ウイルス対策、マルウェア対策、侵入防御システム（IPS）などのアプリケーションが、Cisco Secure Client アプリケーションの動作を誤って悪意のあるものと判断する場合があります。そのような誤解釈を避けるために例外を設定できます。Cisco Secure Client のモジュールかパッケージをインストールしたら、Secure Client のインストールフォルダを許可するか、Secure Client アプリケーションのセキュリティ例外を指定するようにウイルス対策ソフトウェアを設定します。

除外する一般的なディレクトリを次に示しますが、リストは完全ではない場合があります。

- C:\Users\<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files x86)\Cisco

Secure Firewall ポスチャ 用のウイルス対策アプリケーションの設定

ウイルス対策アプリケーションが、ポスチャモジュールや Secure Firewall ポスチャ パッケージに含まれる一部のアプリケーションの動作を誤って悪意のあるものと判断する場合があります。ポスチャモジュールまたは Secure Firewall ポスチャ パッケージをインストールする前に、以下の Secure Firewall ポスチャ アプリケーションに対してセキュリティ例外を許可するか指定するようにウイルス対策ソフトウェアを設定します。

- cscan.exe
- ciscod.exe
- cstub.exe

IKEv2 でサポートされないパブリックプロキシ

IKEv2 はパブリック側プロキシをサポートしていません。この機能のサポートが必要な場合は、SSL を使用してください。プライベート側プロキシは、セキュアゲートウェイから送信される設定の指示に従って、IKEv2 と SSL の両方でサポートされます。IKEv2 はゲートウェイから送信されるプロキシ設定を適用し、それ以降の HTTP トラフィックはそのプロキシ設定の影響を受けます。

IKEv2 に関してグループポリシーの MTU 調整が必要な場合がある

Cisco Secure Client は、一部のルータによるパケットフラグメントを受信およびドロップする場合があり、その結果として、一部の Web トラフィックが通過できなくなります。

この問題を回避するには MTU の値を小さくします。推奨値は 1200 です。次に、CLI を使用してこれを実行する例を示します。

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

ASDM を使用して MTU を設定するには、[設定（Configuration）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] の順に選択します。

DTLS 使用時に MTU が自動的に調整される

DTLS に関してデッドピア検出（DPD）が有効になっている場合、クライアントは自動的にパス MTU を決定します。以前に Cisco Secure Firewall ASA を使用して MTU を減らした場合は、設定をデフォルト値（1406）に復元する必要があります。トンネルの確立時に、クライアントは、特別な DPD パケットを使用して MTU を自動調整します。それでも問題が解決しない場合は、Cisco Secure Firewall ASA での MTU 構成を使用して以前と同様に MTU を制限します。

ネットワーク アクセス マネージャとグループポリシー

Windows Active Directory ワイヤレスグループポリシーにより、特定の Active Directory ドメイン内の PC に展開されるワイヤレス設定とワイヤレスネットワークが管理されます。ネットワーク アクセス マネージャをインストールする場合、管理者は、特定のワイヤレス グループ ポリシー オブジェクト（GPO）がネットワーク アクセス マネージャの動作に影響を与える可能性があることに注意する必要があります。完全な GPO 展開を実行する前に、必ず、ネットワーク アクセス マネージャを使用して GPO ポリシー設定をテストしてください。ワイヤレスネットワークに関連する GPO はサポートされていません。

ネットワーク アクセス マネージャを使用する場合の FreeRADIUS 設定

ネットワーク アクセスマネージャを使用するには、FreeRADIUS設定を調整する必要があります。脆弱性を防ぐために、ECDH 関連の暗号はデフォルトで無効になっています。/etc/raddb/eap.conf で cipher_list の値を変更してください。

アクセスポイント間のローミングには完全認証が必要

Windows 7 以降を実行しているモバイルエンドポイントは、クライアントが同じネットワーク上のアクセスポイント間をローミングするときに、より迅速な PMKID 再アソシエーションを利用する代わりに、完全なEAP認証を実行する必要があります。その結果、場合によっては、Cisco Secure Client は完全認証のたびにログイン情報を入力するようにユーザーに要求します（アクティブプロファイルによって要求される場合）。

LAN 内の他のデバイスでのホスト名の表示を防止する

Cisco Secure Client を使用してリモート LAN 上の Windows 7 以降と VPN セッションを確立すると、ユーザーの LAN 内にある他のデバイス上のネットワークブラウザに保護されたリモートネットワーク上のホストの名前が表示されます。ただし、他のデバイスはこれらのホストにアクセスできません。

Cisco Secure Client ホストが（Cisco Secure Client エンドポイントホストの名前を含む）サブネット間でのホスト名の漏洩を確実に防ぐようにするために、そのエンドポイントがプライマリまたはバックアップブラウザにならないように設定してください。

1. [プログラムとファイルの検索（Search Programs and Files）]テキストボックスに「**regedit**」と入力します。
2. **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters** に移動します。
3. [MaintainServerList] をダブルクリックします。

[文字列の編集（Edit String）] ウィンドウが開きます。

1. 「**No**」と入力します。
2. [OK] をクリックします。
3. [レジストリエディター（Registry Editor）] ウィンドウを閉じます。

失効メッセージ

配信ポイントが内部的にしかアクセスできない場合に、Secure Client が LDAP 証明書失効リスト（CRL）の配信ポイントを指定するサーバー証明書を確認しようとすると、認証後に Cisco Secure Client 証明書失効警告ポップアップウィンドウが表示されます。

このポップアップウィンドウが表示されないようにするには、次のいずれかを実行します。

- プライベート CRL 要件を持たない証明書を取得します。

- Internet Explorer でサーバー証明書失効確認を無効にします。

注意 Internet Explorer でサーバー証明書失効確認を無効にすると、他の OS の使用に関してセキュリティ上の重大な悪影響が生じる可能性があります。

ローカリゼーションファイル内のメッセージが複数行になる場合がある

ローカリゼーションファイル内のメッセージの検索を試みると、次の例のように、それらが複数行になる場合があります。

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

特定のルータの背後にある場合の macOS 用 Cisco Secure Client のパフォーマンス

macOS 用の Cisco Secure Client が、iOS を実行するゲートウェイへの SSL 接続の確立を試みる場合、または Cisco Secure Client が特定タイプのルータ（Cisco Virtual Office（CVO）ルータなど）の背後から Cisco Secure Firewall ASA への IPsec 接続の確立を試みる場合、一部の Web トラフィックが接続を通過し、その他のトラフィックがドロップされる可能性があります。Cisco Secure Client は MTU を誤って計算する場合があります。

この問題を回避するには、macOS コマンドラインから次のコマンドを使用して、Cisco Secure Client アダプタの MTU の値を手動で減らします。

```
sudo ifconfig utun0 mtu 1200
```

Windows ユーザーによる常時接続の無効化を防止する

Windows コンピュータでは、限定的な権限または標準的な権限を持つユーザーは、それぞれのプログラムデータフォルダに対して書き込みアクセスを実行できる場合があります。これらの権限により、Cisco Secure Client プロファイルを削除することが可能なため、常時接続機能を無効にできます。これを防止するには、`C:\ProgramData` フォルダ（または少なくとも Cisco サブフォルダ）へのアクセスを制限するようにコンピュータを設定します。

Wireless Hosted Network を無効にする

Windows 7 以降の Wireless Hosted Network 機能を使用すると Cisco Secure Client が不安定になる可能性があります。Cisco Secure Client を使用する場合、この機能を有効にしたり、（Connectify または Virtual Router など）この機能を有効にするフロントエンド アプリケーションを実行したりすることはお勧めしません。

Cisco Secure Client では Cisco Secure Firewall ASA が SSLv3 トラフィックを要求しないように設定する必要があります。

Cisco Secure Client では、Cisco Secure Firewall ASA が TLSv1 または TLSv1.2 トラフィックを受け入れ、SSLv3 トラフィックを受け入れないようにする必要があります。SSLv3 キー生成アルゴリズムは、キー生成機能を低下させる可能性がある方法で MD5 と SHA-1 を使用します。SSLv3 の後継規格である TLSv1 を使用すると、SSLv3 に存在するこの問題とその他のセキュリティ上の問題が解決されます。

Cisco Secure Client は、「ssl server-version」の次の Cisco Secure Firewall ASA 設定では接続を確立できません。

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro がインストールを妨げる

デバイスに Trend Micro がインストールされている場合、ドライバが競合するために、ネットワーク アクセス マネージャをインストールできません。Trend Micro をアンインストールするか [Trend Micro共通ファイアウォールドライバ（trend micro common firewall driver）] をオフにすると、この問題を回避できます。

Secure Firewall ポスチャ がレポートする情報

サポートされているマルウェア対策製品およびファイアウォール製品はいずれも、最終スキャン時間情報をレポートしません。Secure Firewall ポスチャ がレポートする情報は、次のとおりです。

- マルウェア対策について
  - 製品の説明
  - 製品のバージョン
  - ファイルシステム保護ステータス（アクティブスキャン）
  - データファイル時間（最終更新日時とタイムスタンプ）
- ファイアウォールについて
  - 製品の説明
  - 製品のバージョン
  - ファイアウォールの有効/無効

再接続に時間がかかる（CSCtx35606）

IPv6 が有効になっており、プロキシ設定の自動検出が Internet Explorer で有効になっているか現在のネットワーク環境でサポートされていない場合、Windows で再接続に時間がかかることがあります。回避策として、プロキシの自動検出が現在のネットワーク環境でサポートされていない場合は、VPN 接続に使用されない物理ネットワークアダプタを切断するか、IE でプロキシの自動検出を無効にすることができます。

限定的な権限を持つユーザーは ActiveX をアップグレードできない

ActiveX コントロールをサポートする Windows クライアントでは、限定的な権限を持つユーザーアカウントは ActiveX コントロールをアップグレードできないため、Web 展開方式で Cisco Secure Client をアップグレードできません。最も安全な選択肢として、ユーザーが、ヘッドエンドに接続してアップグレードすることにより、アプリケーション内からクライアントをアップグレードすることをお勧めします。

（注） 以前に管理者アカウントを使用して ActiveX コントロールがクライアントにインストールされている場合、ユーザーは ActiveX コントロールをアップグレードできます。

プロアクティブ キー キャッシング（PKC）または CCKM のサポートがない

ネットワーク アクセス マネージャは PKC または CCKM キャッシングをサポートしていません。高速移行と高速ローミングは、すべての Windows プラットフォームで利用できるわけではありません。

Cisco Secure Client のアプリケーション プログラミング インターフェイス

Cisco Secure Client には、独自のクライアントプログラムを構築するユーザー向けのアプリケーション プログラミング インターフェイス（API）が含まれています。

API パッケージには、Cisco Secure Client の C++インターフェイスに対応するマニュアル、ソースファイル、およびライブラリファイルが含まれています。Windows、Linux、および Mac プラットフォームで構築する際に、ライブラリおよびプログラム例を使用できます。Windows プラットフォーム用の Makefile（またはプロジェクトファイル）も含まれています。他のプラットフォーム用には、サンプルコードのコンパイル方法を示すプラットフォーム固有スクリプトが含まれています。ネットワーク管理者は、アプリケーション（GUI、CLI、または組み込みアプリケーション）とこれらのファイルやライブラリをリンクできます。

API は Cisco.com からダウンロードできます。

Cisco Secure Client API に関するサポートの問題については、anyconnect-api-support@cisco.com に電子メールでお問い合わせください。

Cisco Secure Client 5.0.04032

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwe67896	core	openssl CVE-2023-0215 などの脆弱性
CSCwe92223	core	Windows arm64：SplitDNSv6 テストで、トンネル外の pcap に遊離 DNS クエリが表示される
CSCwf32105	core	AnyConnect をバージョン 4.10.06079 から 4.10.06090 にアップグレードした後、AC エージェントがクラッシュする
CSCwf58968	download_install	macOS 14：VPN 通知アプリケーションの起動に失敗する。アンインストール中に KDF の非アクティブ化がスキップされる
CSCwf08769	nam	Windows 10 および Windows 11 21H2 での Windows RnR の無効化
CSCvz20270	opswat-ise	ENH：ISE ポスチャが Mozilla Firefox バージョン 87 をサポートしていない
CSCwd56524	posture-ise	[ドキュメント] Windows ARM64 ビットプラットフォームでの ISE ポスチャの制限付きサポート
CSCwe83519	vpn	DTLS MTU DPD の送信が早すぎるため、ヘッドエンドによってドロップされることがある

Cisco Secure Client 5.0.03076

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwf24327	nam	NAM ポリシーで WPA3 が許可されていない場合、Network Access Manager が WPA2/WPA3 混合パーソナルネットワークへの接続に失敗する

Cisco Secure Client 5.0.03072

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwe67896	core	openssl CVE-2023-0215 などの脆弱性
CSCwf32105	core	AnyConnect をバージョン 4.10.06079 から 4.10.06090 にアップグレードした後、AC エージェントがクラッシュする
CSCwe17889	download_install	Windows：デスクトップ ショートカット トランスフォームが、VPN コア インストーラ プロパティの変更に失敗する
CSCwc09405	gui	AnyConnect / Secure Client は、国際的なアクセシビリティ標準規格を完全にはサポートしていない

識別子	コンポーネント	タイトル
CSCur83728	nam	CAC カードが取り外されたときに AnyConnect ネットワークアクセス マネージャが EAPol ログオフを送信しない。
CSCwb45685	nam	スマートカード証明書にアクセスするときの空の PIN のサポートを追加
CSCwe06686	nam	帯域外パスワードの変更と再認証後に NAM 認証が失敗する
CSCwe33650	nam	NAM acnamcontrol ユーティリティでは、restartAdapter の GUID をすべて大文字にする必要があります
CSCwe38560	nam	NAM が AKM 802.1X EAP SHA256 を使用してネットワークに接続できない
CSCwe40749	nam	acnamihv.dll のファイルと製品のバージョンの不一致
CSCvz20270	opswat-ise	ENH：ISE ポスチャが Mozilla Firefox バージョン 87 をサポートしていない
CSCwa34429	opswat-ise	KB5007186 にアップグレードした後、edgehtml.dll のファイルの日付が間違っている
CSCwc76493	opswat-ise	Windows 11：パッチ管理チェックの失敗
CSCwd73072	opswat-ise	macOS 186.0.0.0 のサポートチャートで Carbon Black Cloud がサポートされなくなった
CSCwe23584	opswat-ise	ENH：Trellix からポスチャ条件に Trellix Drive Encryption 7.4.0.11 が含まれる

識別子	コンポーネント	タイトル
CSCwe51629	opswat-ise	XProtectPlistConfigData の代わりに XProtectPayloads を使用して、Xprotect AM の定義データを収集する
CSCwf08773	opswat-ise	Avast Business 23 が利用できない
CSCwf48234	opswat-ise	ENH：McAfee Total Protection バージョン 16.0 R51 のサポート
CSCvx49570	posture-ise	ISE ポスチャモジュールは Windows 10 ARM64 ベースの PC と互換性がない
CSCwe70047	posture-ise	MacOS：ISE ポスチャが FileVault の「状態」（オン/オフ）を正確に検出しない
CSCwe86806	posture-ise	ENH：バージョン 2166.x の Xprotect のサポート
CSCwd84695	swg	SWG がアクティブになったときに OS DNS キャッシュをクリアする
CSCwe70156	swg	AnyConnect SWG：DNS ルックアップスレッドの枯渇により接続確立の遅延が増える
CSCwe86049	swg	失敗した HTTP コードを接続の失敗として処理し、低速CP ネットワークでの CP 検出ロジックを強化する
CSCwf17017	swg	MSFT URL のプローブ中にタイムアウトが発生した
CSCwf22189	swg	SWG が保護状態にならないことがある
CSCvv75596	umbrella	DNS 応答圧縮の一貫したサポートを追加する

識別子	コンポーネント	タイトル
CSCvy09941	vpn	信頼されていないネットワークポリシーと証明書ベースの認証では、vpn-session-timeout が機能しない
CSCwd09989	vpn	AnyConnect：マシンがコネクトスタンバイから再開した後、プロキシ設定が正しく復元されない
CSCwd68113	vpn	正しいパスワードを入力しても AAA 認証が失敗する

Cisco Secure Client 5.0.02075

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwc55221	core	AnyConnect が SmartCard PIN をクリアしない
CSCwd73497	core	SBL 中にネットワーク接続がない場合、AC は信頼されたネットワークを検出し、UI が終了する
CSCwe00252	core	Windows の特権昇格に対応する Cisco AnyConnect セキュアモビリティ クライアントとセキュアクライアント
CSCwe43455	core	macOS 13：DDR 対応のリゾルバーで DNS 関連の機能が正しく動作しない

識別子	コンポーネント	タイトル
CSCwe17889	download_install	Windows：デスクトップ ショートカット トランスフォームが、VPN コア インストーラ プロパティの変更に失敗する
CSCvp42218	nam	ENH：管理者が証明書の選択に使用する証明書の基準を指定できるようにする
CSCwc78325	nam	証明書照合ルールフィールドの証明書テンプレートのサポート情報
CSCwd79171	nam	libxml2 コードが、無効なメモリアクセスを引き起こす可能性のあるダングリングポインタを指すことがある
CSCwd87145	nam	NAM プロファイルエディタ：以前に保存したネットワークを編集すると、表示が破損することがある
CSCwd90898	nam	WPA3 OWE および SAE ネットワークのサポートを追加
CSCwe40749	nam	acnamihv.dll のファイルと製品のバージョンの不一致
CSCwa34429	opswat-ise	KB5007186 にアップグレードした後、edgehtml.dll のファイルの日付が間違っている
CSCwa64750	opswat-ise	FireEye エージェントバージョン 34.x が、ISE ポスチャ条件で使用できる必要がある
CSCwa81027	opswat-ise	ISE ポスチャパッチ管理条件：BMC クライアント管理エージェント 20.x を追加
CSCwc76493	opswat-ise	Windows 11：パッチ管理チェックの失敗

識別子	コンポーネント	タイトル
CSCwc77619	opswat-ise	AC 4.10 で CM 4.3.3030.6145 をロードできない
CSCwd11788	opswat-ise	CM バージョン 4.3.2998.6145 にアップグレードした後、OPSWAT が FireEye を検出できない
CSCwd37792	opswat-ise	コンプライアンスモジュールのアンインストール中に USB UpperFilter レジストリキーが削除される
CSCwd43799	opswat-ise	macOS 12.6：Xprotect AM インストールバージョンの値が正しく検出されない
CSCwd56796	opswat-ise	Windows 11 22H2 で間違った Windows Update Agent のバージョンが返される
CSCwd62517	opswat-ise	AnyConnect ポスチャ ISE での新しい「CrowdStrike Windows Sensor」アプリケーションの追加
CSCwe11874	opswat-ise	ENH：ISE ポスチャが Kaspersky Endpoint Security 12.x をサポートしない
CSCwb64132	posture-ise	（ENH）AnyConnect で、セッション変更のクライアントに「再評価に失敗しました」という表面的なエラーメッセージが表示される
CSCwd49714	posture-ise	Win、Lin NSA pkg で翻訳が行われない
CSCwd52815	posture-ise	MAC NSA pkg で翻訳が行われない
CSCwe30612	posture-ise	ENH：ISE ポスチャモジュールのポスチャ CLI（MacOS）

識別子	コンポーネント	タイトル
CSCwe22036	swg	noNetwork、Trusted Network、VPN の場合のみ SWG 保護をバックオフする
CSCvv75596	umbrella	DNS 応答圧縮の一貫したサポートを追加する
CSCwe07816	umbrella	Umbrella プラグインで頻繁に報告されるソケットエラーによる Umbrella エージェントのクラッシュ
CSCvf70372	vpn	Umbrella モジュールを使用した AnyConnect および「AutoConnectOnStart」機能で、「AutoConnectOnStart」が失敗する
CSCvx93522	vpn	AnyConnect SAML が tunnel-group-list（group-alias）を無視する
CSCvz63011	vpn	ENH（デスクトップ）：期限切れの認証試行をキャンセルするアイドル認証タイムアウトのサポートを追加
CSCwd15773	vpn	VPN 接続がアクティブな MacOS 13 でサイドカーとコンティニュイティカメラのビデオフィードが機能しない
CSCwd17651	vpn	管理トンネルが 4 ～ 7 日後にダウンし、切断されたままになる
CSCwd40263	vpn	プロキシ設定がどこにも適用されない
CSCwd76149	vpn	SBL/ARM64：再起動後に SBL アイコンが表示されない（シャットダウン + 再起動は正常に機能する）

識別子	コンポーネント	タイトル
CSCwa31551	web	AnyConnect：4.10.03104 へのアップグレード後の SAML 認証の組み込みブラウザが表示されない

Cisco Secure Client 5.0.01242

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCvz84164	api	グループポリシーに XMLprofile がない場合でも、RestrictPreferenceCaching のログイン情報にユーザー名が表示される
CSCwc63454	api	ローカルポリシーファイルでダウンローダーがバイパスされると、VPN 接続が失敗する
CSCwc92975	cli	VPN CLI が切断状態でスタックする
CSCvu77796	core	CIAM：libxml 2.9.10
CSCvx35970	core	AC 4.9MR5 が認証タイムアウト VPN プロファイル設定を無視する
CSCvw31155	core	Always On を使用すると、複数の証明書検証エラーがポップアップ表示される
CSCwb77035	core	Windows セキュリティの「必要なクレデンシャル」ポップアップがフォーカスされていない
CSCwc55221	core	AnyConnect が SmartCard PIN をクリアしない

識別子	コンポーネント	タイトル
CSCvz68411	dart	DART に Umbrella のホワイトリストファイルがない
CSCwb78515	dart	DART が VPN 管理トンネル ミニダンプ クラッシュ ファイルを収集しない
CSCwd06986	dart	Windows 11 の AnyConnect DART バンドルの概要に、「Windows 11」ではなく「Windows 10」と表示される
CSCwb74542	download_install	PC で日付形式を変更すると AnyConnect のインストールに失敗する
CSCuw17364	gui	Pre-Connect ポップアップを閉じずに VPN を確立できる
CSCvz53637	gui	AnyConnect：UserControllable が False に設定されているが、ユーザーが設定を変更できる
CSCwc59031	gui	Secure Client：AnyConnect 4.xx を使用して 8.0.1.x にアップグレードすると、スタートメニューのショートカット リンクが破損する [Windows]
CSCwc64861	gui	SAML 認証が成功した後の AnyConnect GUI メッセージの更新
CSCvo32995	nam	ENH：個別に設定されたワイヤレスネットワークの「自動接続」機能のサポートを追加
CSCvs29773	nam	ENH：NAM により、ユーザーは拡張ロギングを行うために pcap、IHV、fd、資格情報プロバイダーなどをオン/オフにできる。

識別子	コンポーネント	タイトル
CSCwa91572	posture-ise	CSC 用にダウンロードする最小 CM バージョンを義務付ける（Windows、MacOS、Linux）
CSCwd62225	posture-ise	Windows：コンプライアンスモジュールを読み込めない
CSCwc73870	profile-editor	AMP イネーブラ プロファイル エディタが OpenJDK を検出またはロードしない
CSCwb39828	swg	SWG がフェールオープンとフェールクローズの両方で有効になっているとキャプティブポータルページが開かない
CSCwc41729	swg	SWG による KDF での逆 DNS ルックアップも、IPv4 でマップされた IPv6 アドレスをターゲットとするフローに対応する
CSCwc53340	swg	macOS：末尾にドットがある FQDN をターゲットとする Web フローで、SWG ドメインバイパスが断続的に失敗する
CSCwd02073	swg	5.x で、CSC Umbrella ではなく AnyConnect Umbrella パスに記録されるログがほとんどない
CSCwd83114	umbrella	dcp2 crash fix
CSCvj04741	vpn	最初のサーバーハッシュが一致しない場合、AC TND は次の TrustedHttpsServer をチェックせずに untrusted に移動する
CSCvy99392	vpn	ローカルプロキシ経由の VPN 接続が機能せず、「このゲートウェイに接続できません（Cannot connect to this gateway）」で失敗する

識別子	コンポーネント	タイトル
CSCvz51167	vpn	macOS での外部ブラウザ認証後に Chrome ブラウザがクラッシュする
CSCvz63011	vpn	ENH（デスクトップ）：期限切れの認証試行をキャンセルするアイドル認証タイムアウトのサポートを追加
CSCwa92301	vpn	SBL 経由で接続すると、アップグレード延期のプロンプトが表示されない
CSCwb67733	vpn	AnyConnect の cURL 証明書署名操作のタイムアウトを 120 秒に延長した
CSCwb85473	vpn	Windows：仮想サブネットのみがトンネルから除外されている場合、RSAT が遅くなる（WSL2 相互運用性のため）
CSCwc15262	vpn	AC 4.10 MR4 または 4.9 MR4 はスマートカード証明書の認証を使用して VPN に接続できない
CSCwc46323	vpn	SAML フローでの Windows 統合認証の失敗
CSCwc50423	vpn	マシンの電源がオフになっている場合、AnyConnect クライアントはプロキシ設定を復元できない
CSCwc64425	vpn	Zenmu 仮想デスクトップと AnyConnect SAML 外部ブラウザの互換性
CSCwc79898	vpn	AnyConnect Ubuntu 22.04：SAML 外部ブラウザが起動しない
CSCwc81098	vpn	AnyConnect LaunchDaemon plist ヘッダーシンタックスの更新

識別子	コンポーネント	タイトル
CSCwc85871	vpn	ENH：IOS-XE のパブリック NAT を使用した IKEv2 IPv4/IPv6 デュアルスタックサポートの元のアドレスペイロードを追加
CSCwd14401	vpn	Windows Always On：VPN の切断後に VPN に接続できず（DNS エラー）、接続に失敗することが予想される
CSCwd16706	vpn	プロキシ設定がすべての場所で正しく復元されない（断続的に）
CSCwd23719	vpn	cURL でのセッション ID キャッシュによる VPN 接続の失敗
CSCwb22799	web	組み込みブラウザのウィンドウサイズが正しくない

Cisco Secure Client 5.0.00556

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCvx10794	opwat-ise	パッチ管理 GUI 修復の有効化が ISE で設定されている場合、Windows Update GUI が開かない
CSCwb99183	opswat-ise	Asia Info Office Scan Agent 16.x（16.0.0283）は ISE サポート条件を追加する必要がある
CSCwc53490	opswat-ise	コンプライアンスモジュールを読み込めない

識別子	コンポーネント	タイトル
CSCwc59876	opswat-ise	Cisco AMP 8.x および Cisco ISE ポスチャ コンプライアンス モジュールのサポート
CSCwc20207	posture-ise	Apex One（MAC）セキュリティエージェント [Trend Micro] AM の最新の定義日/バージョンが反映されない
CSCwc56173	vpn	VPN 接続の試行は、前の認証後の接続の失敗の後、最大 3 分間ハングする

Cisco Secure Client 5.0.00529

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwb41421	core	CiscoSSL CVE-2022-0778
CSCwb78515	dart	DART が VPN 管理トンネル ミニダンプ クラッシュ ファイルを収集しない
CSCvz87690	download_install	プロキシ環境変数が原因で AnyConnect CSD ポスチャ評価が失敗した
CSCvz53637	gui	UserControllable が False に設定されているが、ユーザーが設定を変更できる
CSCvr88852	nam	証明書選択ポリシー
CSCwa48531	opswat-ise	OPSWAT 4.3.2443 が Trendmicro APEXOne エージェントバージョン 14.0.9601 を検出できない

識別子	コンポーネント	タイトル
CSCwb30655	opswat-ise	FireEye セキュリティ エージェント バージョン 34.x が最新の ISE ポスチャの更新に含まれていない
CSCwc53490	opswat-ise	コンプライアンスモジュールを読み込めない
CSCwa69058	profile-editor	Windows 用のスタンドアロン VPN プロファイルエディタは、Oracle Java でのみ動作する

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.04032

これらの警告では、シスコソフトウェアのリリースにおける予想しない動作または不具合について説明します。

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwf09464	opswat-asa	ENH：McAfee LiveSafe - Internet Security バージョン 16.0 R51 のサポート
CSCwf44746	opswat-asa	Cisco Secure Firewall ポスチャ 5.0.03068 を使用する Linux マシンでタイムアウトの問題が発生する

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.03072

これらの警告では、シスコソフトウェアのリリースにおける予想しない動作または不具合について説明します。

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCvz19204	opswat-asa	ENH：HostScan で MacOS 用の「Sophos Endpoint」マルウェア対策 10.1.x のサポートを追加する必要がある
CSCwf44746	opswat-asa	Cisco Secure Firewall ポスチャ 5.0.03068 を使用する Linux マシンでタイムアウトの問題が発生する
CSCwf98852	opswat-asa	Trellix Security Agent が旧製品の McAfee Security Agent として誤って識別される

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.02075

これらの警告では、シスコソフトウェアのリリースにおける予想しない動作または不具合について説明します。

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwd94368	opswat-asa	ENH：Cisco Secure Endpoint 7.5.5.21061 の HostScan サポート
CSCwd81115	posture-asa	ASA/ASDM の DE 機能の csdm.sez が利用できないため、Data.xml ファイルの設定が変更される

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.01242

これらの警告では、シスコソフトウェアのリリースにおける予想しない動作または不具合について説明します。

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警告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] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCvw36365	opswat-asa	ESET Smart Security 14.x 以降を検出するための HostScan のサポート
CSCvz01221	opswat-asa	定義チェックによる HostScan の遅延が原因で AnyConnect SAML 認証が失敗する
CSCwc37138	opswat-asa	Sophos マルウェア対策の修正により、RHEL/Ubuntu クライアントで VPN タイムアウトが発生する
CSCwd39477	opswat-asa	Sophos Endpoint Agent 2022.2.1.9 が Secure Firewall Posture（HostScan）5.0.00529 で定義チェックに失敗する

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00556

Cisco Secure Firewall ポスチャ 5.0.00556 には、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。詳細については、「Release and Compatibility」の「Secure Firewall Posture Support Charts」[英語] を参照してください。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.0.00529

Cisco Secure Firewall ポスチャ 5.0.00529 には、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。詳細については、「Release and Compatibility」の「Secure Firewall Posture Support Charts」[英語] を参照してください。

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。