Cisco AnyConnect Secure Mobility Client リリース 4.9 リリースノート

AnyConnect Secure Mobility Client リリース 4.9 リリースノート

このリリースノートには、Windows、macOS、および Linux プラットフォーム上の AnyConnect セキュア モビリティ クライアントに関する情報が記載されています。AnyConnect クライアントデバイスは、常時利用可能なインテリジェント VPN を通じて、最適なネットワーク アクセスポイントを自動的に選択し、そのトンネリングプロトコルを最も効率的な方法に適応させます。

（注） AnyConnect リリース 4.9.x は 4.x のバグのメンテナンスパスになります。AnyConnect 4.0、4.1、4.2、4.3、4.4、4.5、4.6、4.7、および 4.8 を使用している場合、将来の不具合の修正によるメリットを得るには AnyConnect 4.9.x にアップグレードする必要があります。AnyConnect 4.0.x、4.1.x、4.2.x、4.3.x、4.4.x、4.5.x、4.6.x、4.7.x、および 4.8.x で見つかった不具合は、AnyConnect 4.9.x メンテナンスリリースでのみ修正されます。

macOS 10.15 を使用している Cisco AnyConnect ユーザーは VPN 接続を確立できなかったり、システム ポップアップ メッセージを受信したりする場合があります。ソフトウェアのアップグレードが推奨されます。

Cisco AnyConnect および HostScan には、今後の macOS Catalina リリース（10.15）との互換性のために更新されたリリースが必要です。macOS Catalina リリース（10.15）以降では、オペレーティングシステムが 32 ビット バイナリの実行をサポートしなくなります。さらに、オペレーティングシステムによってインストールされるためには、アプリケーションが暗号的に認証される必要があります。Cisco AnyConnect 4.8.00175 は、macOS Catalina での動作を正式にサポートし、32 ビットコードが含まれない最初のバージョンです。

最新バージョンの AnyConnect のダウンロード

始める前に

最新バージョンの AnyConnect 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 次のリンクで Cisco AnyConnect Secure Mobility Client 製品サポートページにアクセスします。

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 AnyConnect 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 AnyConnect Secure Mobility Client リリース 4.x の管理者ガイドを参照してください。

Web 展開用の AnyConnect パッケージファイル名

OS	AnyConnect Web 展開パッケージ名
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux（64 ビット）	anyconnect-linux64-*version*-webdeploy-k9.pkg

事前展開する AnyConnect パッケージファイルの名前

OS	AnyConnect 事前展開パッケージ名
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux（64 ビット）	anyconnect-linux64-*version*-predeploy-k9.tar.gz

AnyConnect 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。

AnyConnect 4.9.06037 の新機能

この AnyConnect 4.9.06037 のリリースは、次の更新と拡張機能を導入し、AnyConnect 4.9.06037（43 ページ）に記載されている不具合が修正されています。

- （CSCvy53730：Windows のみ）AnyConnect 4.9.06037 以降では、AnyConnect 4.9MR5 以前に付属している ISE の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 以降にはバージョン 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。
- （CSCvw92182）ASA SSL ゲートウェイに最初に接続した数秒後、またはインターフェイスを変更した数秒後に、VPN モジュールが再接続する macOS のみの問題を修正しました。この再接続は、TLS のみのトンネルに影響を与えていました。この修正により、ISE ポスチャモジュールに「ポリシーサーバーが検出されませんでした（No policy server detected）」と表示されなくなりました。
- ASA の新しい未リリースバージョンに接続する際の DTLS セッションの障害に対処するために、CiscoSSL ライブラリが更新されました。
- NVM が、DTLS モードで証明書を検証するように更新されました（Windows のみ）。
- （CSCvw53140）Windows での VPN モジュールに関する AnyConnect 4.9.03049（およびそれ以降）のスマートカードの問題を修正しました。この問題は、キーストレージプロバイダ（KSP）をサポートしていないスマートカード、またはレガシーの暗号化サービスプロバイダ（CSP）をサポートしているスマートカードでの暗号化操作で発生していました。

AnyConnect 4.9.05042 の新機能

このリリースでは、AnyConnect 4.9.05042 （44 ページ）に記載されている不具合を解決します。

AnyConnect 4.9.04053 の新機能

この AnyConnect 4.9.4053 のリリースは、次の拡張機能を導入し、AnyConnect 4.9.04053 （45 ページ）に記載されている不具合が修正されています。

VPN プロファイルの更新およびソフトウェアの更新機能を維持しながら、特定のダウンローダ機能をバイパスできる設定を VPN ローカルポリシーエディタに追加しました。AnyConnect ダウンローダの他の機能に影響を与えることなく、ASA からのスクリプト、ローカリゼーションファイル、ヘルプファイル、または UI カスタマイズの Web 展開を無効にできます。

- [スクリプト Web 展開の更新の制限（Restrict Script Web-deploy Updates）]：管理者がサーバーからの接続時のスクリプトの更新をカスタマイズできないようにします。
- [リソース Web 展開の更新の制限（Restrict Resource Web-deploy Updates）]：管理者がサーバーからのユーザーインターフェイス要素の更新をカスタマイズできないようにします。

- [ヘルプWeb展開の更新の制限（Restrict Help Web-deploy Updates）]：管理者がサーバーからのヘルプファイルの更新をカスタマイズできないようにします。
- [ローカリゼーションWeb展開の更新の制限（Restrict Localization Web-deploy Updates）]：管理者がサーバーからのローカリゼーションの更新をカスタマイズできないようにします。

これら 4 つのカスタマー Web 展開パラメータをバイパス（**true**）に設定するには、1）以下で説明する AnyConnectLocal Policy.xml ファイルのアウトオブバンド更新、2）これらのファイルに対する今後のすべての更新のアウトオブバンド展開が必要です。

- <RestrictStrictWebDeploy> は、次の場所にある OnConnect スクリプトのダウンロードを制御します。
  - Windows：<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\script
  - macOS：/opt/cisco/anyconnect/script
  - Linux：/opt/cisco/anyconnect/script
- <RestrictResourceWebDeploy> は、次のディレクトリへの UI カスタマイズのダウンロードを制御します。
  - Windows：<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\res
  - macOS：/opt/cisco/anyconnect/res
  - Linux：/opt/cisco/anyconnect/res
- <RestrictHelpWebDeploy> は、次のディレクトリへのヘルプファイルのダウンロードを制御します。
  - Windows：<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help
  - macOS：/opt/cisco/anyconnect/help
  - Linux：/opt/cisco/anyconnect/help
- <RestrictLocalizationWebDeploy> は、次の場所への L10N ローカリゼーションファイルのダウンロードを制御します。
  - Windows：<DriveLetter>\ProgramData\Cisco\Cisco AnyConnect Secure MobilityClient\110n
  - macOS：/opt/cisco/anyconnect/110n
  - Linux：/opt/cisco/anyconnect/110n

AnyConnect 4.9.04043 の新機能

この AnyConnect 4.9.04043 リリースでは、macOS 11.x（Big Sur）のサポートと、Apple ハードウェアを実行するデバイスとの互換性が導入されています。また、AnyConnect 4.9.04043 （46 ページ）に記載されている不具合を解決します。

macOS 11 で実行している場合、AnyConnect は以前のバージョンの AnyConnect で使用されていたカーネル拡張とは異なり、システム拡張を使用します。

以前のバージョンの AnyConnect は macOS 11 でも引き続き動作しますが、MDM ベースの AnyConnect カーネル拡張の承認が macOS 11 以降で必要であるため、MDM 管理対象デバイスでのみ動作します。macOS 11（Big Sur）に関連する AnyConnect の変更については、『AnyConnect macOS 11 Big Sur Advisory』を参照してください。

AnyConnect 4.9.03049 の新機能

AnyConnect 4.9.03049 は、AnyConnect 4.9.03049 （48 ページ）で説明されている問題を解決する Windows 専用のリリースです。

AnyConnect 4.9.03047 の新機能

この AnyConnect 4.9.03047 のリリースは、次の拡張機能を導入し、AnyConnect 4.9.03047 （48 ページ）に記載されている不具合が修正されています。

- （CSCvu14970）プロファイルエディタの [設定（パート1）（Preferences (Part 1)）] の [ログオン強制（Logon Enforcementt）] の設定を使用して、VPN 接続全体で 1 人のローカルユーザーのみがログオンできるようにします。
- [常にオン（Always On）] の間に VPN が切断されたときに、設定されたホストにエンドポイントがアクセスできるようにします（プロファイルエディタの [設定（パート2）（Preferences (Part 2)）] の [VPNの切断時に次のホストへのアクセスを許可（Allow Access to the Following Hosts with VPN Disconnected）] の設定を使用）。
- VPN 接続用のサーバー名識別（SNI）のサポートを追加します（HostScan またはその他のモジュールは含まれません）。
- AnyConnect クライアントプロファイルの信頼できるドメインと信頼できるサーバーに基づいて、Umbrella セキュア Web ゲートウェイ（SWG）モジュールで SWG 信頼ネットワーク検出のサポートを追加します。
- SWG プロキシが、標準の 80 および 443 ポート以外の非標準ポートからの HTTP および HTTPS トラフィックを代行受信できるようにします。
- SWG プロキシ URL に送信される複数の要求（たとえば、100 以上）を処理するためのサポートを追加します。
- NVM が DTLS を介してコレクタに安全にデータを送信するかどうかを決定します。

- ISE ポスチャでのエンドツーエンドのエージェントレス ポスチャ フローのサポートを追加します。

AnyConnect 4.9.03047 は、macOS 11（Big Sur）ベータ 9（またはパブリックベータ 5）以降で機能します。macOS 11（Big Sur）で実行している場合、AnyConnect は以前のバージョンの AnyConnect で使用されていたカーネル拡張とは異なり、システム拡張を使用します。

以前のバージョンの AnyConnect は macOS 11 でも引き続き動作しますが、MDM ベースの AnyConnect カーネル拡張の承認が macOS 11 以降で必要であるため、MDM 管理対象デバイスでのみ動作します。

お客様は今すぐテストできます。常に最新の Big Sur ベータビルドでテストしてください。

Big Sur の互換性に関する問題は、**ask-anyconnect@cisco.com** に送信してください。macOS 11（Big Sur）に関連する AnyConnect の変更については、『AnyConnect macOS 11 Big Sur Advisory』を参照してください。Big Sur OS リリース以前は、互換性の問題で TAC ケースをオープンできません。

AnyConnect 4.9.02028 の新機能

この AnyConnect 4.9.02028 のリリースは、次の拡張機能を導入し、AnyConnect 4.9.02028 （50 ページ）に記載されている不具合が修正されています。

AnyConnect 4.9.02028 は macOS 専用リリースで、macOS 11（Big Sur）ベータ 5（またはパブリックベータ 2）以降でも機能します。macOS 11（Big Sur）で実行している場合、AnyConnect は以前のバージョンの AnyConnect で使用されていたカーネル拡張とは異なり、システム拡張を使用します。

以前のバージョンの AnyConnect は macOS 11 でも引き続き動作しますが、MDM ベースの AnyConnect カーネル拡張の承認が macOS 11 以降で必要であるため、MDM 管理対象デバイスでのみ動作します。

AnyConnect 4.9.01095 の新機能

この AnyConnect 4.9.01095 のリリースは、次の拡張機能と制限を導入し、AnyConnect 4.9.01095（51 ページ）に記載されている不具合が修正されています。

- Linux ユーザーが VM インスタンス/Docker コンテナでネットワークトラフィックをルーティングする機能。
- AnyConnect 4.9.01095 へのアップグレード後に自動再接続が失敗する（Linux のみ）。詳細については、「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）」セクションを参照してください。

AnyConnect 4.9.00086 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、AnyConnect 4.9.00086 （54 ページ）に記載されている不具合を解決します。

- Splunk アプリケーション 3.x と連携する新しい NVM コレクタとフロー情報のタイムスタンプを含む、フローおよびエンドポイントのデータを強化するために NVM を拡張しました。
- SSL VPN の場合、AnyConnect は TLS と DTLS の両方からの暗号スイート、DHE-RSA-AES256-SHA と DES-CBC3-SHA をサポートしなくなりました。
- IKEv2/IPsec については、AnyConnect は次のアルゴリズムをサポートしなくなりました。
  - 暗号化アルゴリズム：DES と 3DES
  - 疑似ランダム関数（PRF）アルゴリズム：MD5
  - 整合性アルゴリズム：MD5
  - Diffie-Hellman（DH）グループ：2、5、14、24

    サポートされている暗号化アルゴリズムと暗号スイートのリストについては、『AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.9』機能ガイドを参照してください。
- OpenSSL（Cisco SSL）ライブラリの更新

AnyConnect HostScan Engine Update 4.9.06046 の新機能

この AnyConnect HostScan のみのリリースには、Windows、macOS、および Linux 用の OPSWAT エンジンのバージョンに対する更新が含まれ、HostScan 4.9.06046 （58 ページ）に記載されている不具合が修正されています。

AnyConnect HostScan Engine Update 4.9.06037 の新機能

AnyConnect HostScan 4.9.06037 は、HostScan 4.9.06037 （59 ページ）に記載されている不具合を解決します。

AnyConnect HostScan Engine Update 4.9.05042 の新機能

AnyConnect HostScan 4.9.05042 は、ARM64 デバイスを検出するためのサポートを追加します。これには HostScan モジュールの更新が含まれており、HostScan 4.9.05042 （59 ページ）に記載されている不具合を解決します。

AnyConnect HostScan Engine Update 4.9.04045 の新機能

この AnyConnect HostScan 4.9.04045 リリースは、macOS 11.x（Big Sur）の正式なサポートを提供します。これには、Windows、macOS、Linux 用の OPSWAT エンジンのバージョンの更新が含まれています。

macOS Big Sur ベータ版または公式の macOS Big Sur（バージョン 11.x）リリースを HostScan で使用している場合は、エンドポイント上の AnyConnect HostScan ポスチャモジュール（以前にインストールされている場合）と ASA 上の HostScan PKG を 4.9.04045 以降にアップグレードする必要があります。

AnyConnect HostScan Engine Update 4.9.03047 の新機能

AnyConnect HostScan 4.9.03047 は、macOS 11（Big Sur）ベータ 9（またはパブリックベータ 5）以降のバージョンをサポートし、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新を含みます。

HostScan で macOS 11 ベータ版を使用している場合、HostScan の以前のバージョンは正しく機能しません。そのため、エンドポイント上の AnyConnect HostScan ポスチャモジュール（以前にインストールされていた場合）と ASA 上の HostScan PKG は 4.9.02028 以降にアップグレードする必要があります。

AnyConnect HostScan Engine Update 4.9.02028 の新機能

AnyConnect HostScan 4.9.02028 は、macOS 11（Big Sur）ベータ 5（またはパブリックベータ 2）以降のバージョンをサポートし、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新を含みます。

このリリースには新しい macOS 11 のサポートが含まれ、HostScan 4.9.02028 （60 ページ）に記載されている不具合が解決されています。

HostScan で macOS 11 ベータ版を使用している場合、HostScan の以前のバージョンは正しく機能しません。そのため、エンドポイント上の AnyConnect HostScan ポスチャモジュール（以前にインストールされていた場合）と ASA 上の HostScan PKG は 4.9.02028 にアップグレードする必要があります。

AnyConnect HostScan Engine Update 4.9.01095 の新機能

AnyConnect HostScan 4.9.01095 は HostScan モジュールのこの更新が含まれており、HostScan 4.9.01095 （61 ページ）に記載されている不具合を解決します。

Windows 10 エンドポイントの Microsoft Defender Advanced Threat Protection（ATP）のサポート。

AnyConnect HostScan Engine Update 4.9.00086 の新機能

AnyConnect HostScan 4.9.00086 は HostScan モジュールの更新が含まれており、HostScan 4.9.00086（61 ページ）に記載されている不具合を解決します。

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 サポートおよびライセンス要件については、『AnyConnect Secure Mobility Client の機能、ライセンス、および OS』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。

AnyConnect プロファイルエディタの変更点

プロファイルエディタをインストールする前に、Java（バージョン 6 以降）をインストールする必要があります。

AnyConnect 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以前の TLS 1.2 をサポートする ISE の EAP-FAST を使用して、NAM 4.7 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 AnyConnect 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。
- AnyConnect 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、AnyConnect ソフトウェアをエンドポイントに展開し、AnyConnect 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することができる最小リリースです。
- ISE 2.0 は AnyConnect リリース 4.0 以降だけを展開できます。AnyConnect 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。

ISE ライセンス要件

ISE ヘッドエンドから AnyConnect 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 Apex 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 管理ガイド』の「*Cisco ISE* ライセンス」の章を参照してください。

AnyConnect の ASA 要件

特定の機能に関する最小 ASA/ASDM リリース要件

- DTLSv1.2 を使用するには、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 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。
- NVM 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。
- TLS 1.2 を使用するには、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、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
  - AnyConnect 4.x 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、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）
- AnyConnect クライアントの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、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、Web セキュリティ、テレメトリなど）の編集。
  - Cisco IronPort Web セキュリティアプライアンスでサポートされているサービスの使用。これらのサービスにより、アクセプタブル ユース ポリシーを適用し、すべての HTTP および HTTPS 要求を許可または拒否することによって、安全でないと見なされる Web サイトからエンドポイントを保護できます。
  - 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。
  - AnyConnect セッションが隔離されているときに AnyConnect 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 HostScan 移行を実行するには、ASDM 7.9.2 以降が必要です。

ASA のメモリ要件

注意 AnyConnect 4.0 以降を使用するすべての ASA 5500 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。

ASA 5505 のフラッシュ サイズの制限（最大 128 MB）により、AnyConnect 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。AnyConnect 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、HostScan をなくす、など）。

AnyConnect 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。

ASA にデフォルトの内部フラッシュメモリサイズまたはデフォルトの 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 AnyConnect クライアント 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 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 5500 シリーズの最新のリリースノートを参照してください。

VPN ポスチャと HostScan の相互運用性

VPN ポスチャ（HostScan）モジュールにより、Cisco AnyConnect Secure Mobility Client は、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、マルウェア対策ソフトウェア、およびファイアウォール ソフトウェアを識別できます。

VPN ポスチャ（HostScan）モジュールでは、この情報を収集するために HostScan が必要です。HostScan（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、マルウェア対策ソフトウェア、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。通常、最新バージョンの HostScan（AnyConnect と同じバージョン）を実行することが推奨されます。

Start Before Logon（SBL）および HostScan を使用する場合、SBL は事前ログインであるため、完全な HostScan 機能を実現するには、AnyConnect/HostScan ポスチャ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。

HostScan 4.4 以降では、ウイルス対策、スパイウェア対策、およびファイアウォールのエンドポイントデータ（エンドポイント属性）が変更されました。スパイウェア対策（*endpoint.as*）とウイルス対策（*endpoint.av*）はどちらもマルウェア対策（*endpoint.am*）として分類されます。ファイアウォール（*endpoint.pw*）はファイアウォール（*endpoint.pfw*）として分類されます。この設定の詳細については、『AnyConnect HostScan 4.3.x から 4.6.x への移行』を参照してください。

HostScan 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。

（注） AnyConnect は、互換性のない HostScan バージョンと使用すると VPN 接続を確立しません。また、HostScan 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。

HostScan では、macOS Big Sur（バージョン 11.x）が正式にサポートされています。したがって、macOS Big Sur ベータ版または公式の macOS Big Sur（バージョン 11.x）リリースを HostScan で使用している場合は、エンドポイント上の AnyConnect HostScan ポスチャモジュール（以前にインストールされている場合）と ASA 上の HostScan パッケージを 4.9.04045 以降にアップグレードする必要があります。

Apple シリコン（M1 チップ）のサポートにおけるこの動的な導入に伴い、AnyConnect 4.10.02086 以降を使用する macOS エンドポイントでも、HostScan パッケージのバージョンを 4.10.02086 以降にアップグレードする必要があります。次の表に、最小要件の概要を示します。

AnyConnect のバージョン	サポート対象/必須の HostScan Engine（.pkg）の最小バージョン
4.10.01075 以前	CCO で公開されているすべてのバージョンがサポートされます。公開されている最新の HostScan.pkg が常に推奨されます。
4.10.02086 以降	4.10.02086 以降が必要です。公開されている最新の HostScan.pkg が常に推奨されます。

AnyConnect 4.3 の HostScan 更新の終了に関する事前通知

AnyConnect 4.3 以前の HostScan の更新は、2018 年 12 月 31 日に終了しました。HostScan の更新は、AnyConnect 4.4.x 以降および ASDM 7.9.2 以降と互換性のある HostScan 4.6 以降のモジュールを対象に提供されます。HostScan の移行の詳細については、こちらの移行ガイドを参照してください。

ISE ポスチャ準拠モジュール

（CSCvy53730：Windows のみ）AnyConnect 4.9.06037 以降では、AnyConnect 4.9MR5 以前に付属している ISE の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 以降にはバージョン 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。HostScan 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 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 準拠モジュールに関するドキュメントを参照してください。

AnyConnect の IOS 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 AnyConnect 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
- AnyConnect 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」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 を参照してください。

AnyConnect でサポートされているオペレーティングシステム

AnyConnect Secure Mobility Client は、次のオペレーティングシステムをサポートします。

サポートされているオペレーティングシステム	VPN クライアント	ネットワーク アクセス マネージャ	クラウド Web セキュリティ	VPN 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
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	対応	非対応	×	×	非対応	対応	対応	非対応	×	×
Windows 7、8、8.1 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	対応	対応	対応

サポートされているオペレーティングシステム	VPN クライアント	ネットワーク アクセス マネージャ	クラウド Web セキュリティ	VPN 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
macOS 11.x、10.15、10.14 および 10.13（10.15 以降では 64 ビットのみがサポートされています）	対応	非対応	対応	対応	対応	対応	対応	対応	対応	対応
Linux Red Hat 8.2、7、6 および Ubuntu 20.04（LTS）、18.04（LTS）および 16.04（LTS）	対応	非対応	非対応	対応	対応	対応	対応	対応	×	×

* Windows 11 のサポートには次の既知の問題があり、すべて、代わりに Windows 10 が不適切に表示されることに関連します：CSCvy92621、CSCvy92676、CSCvz74755

AnyConnect の Microsoft Windows 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、AnyConnect 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で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 AnyConnect 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。AnyConnect 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）AnyConnect を再インストールしてください。
- WebLaunch で AnyConnect 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。
- AnyConnect 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、AnyConnect 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、AnyConnect 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、AnyConnect が VPN 接続を確立することを妨げます。

    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。
- AnyConnect 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、AnyConnect は Windows 8 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 AnyConnect と連動しません。
- Windows 2008 はサポートされていません。ただし、この OS に AnyConnect のインストールすることは可能です。また、Windows Server 2008 R2 にはオプションの SysWow64 コンポーネントが必要です。
- 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。NAM はオペレーティングシステムと Active Directory サーバーの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、企業クレデンシャルが使用されると、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、適切なネットワーク アクセス制限がユーザーのネットワーク接続に適用されます。
- 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 と相互作用する 3G データカードと互換性があります。

AnyConnect の Linux 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。
- Snap バージョンの Firefox は、Linux 上の AnyConnect ではサポートされません。
- x86 命令セット
- 64 ビットプロセッサ
- 32 MB の RAM
- 20 MB のハードディスク容量
- インストールにはスーパーユーザー権限が必要です。
- network-manager
- libnm（libnm.so または libnm-glib.so）
- libstdc++ ユーザーは libstdc++.so.6（GLIBCXX_3.4）以上（ただし、バージョン 4 未満）を使用する必要があります。
- Java 5（1.5）以降 Web インストールで機能する唯一のバージョンは Sun Java です。Sun Java をインストールし、それをデフォルトパッケージの代わりに使用するようにブラウザを設定する必要があります。
- zlib（SSL deflate 圧縮をサポートするため）
- xterm：ASA クライアントレスポータルから Weblaunch 経由で AnyConnect の初期展開を行う場合にのみ必要
- gtk 2.24
- webkitgtk+ 2.10 以降（AnyConnect 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）
- iptables 1.2.7a 以降
- カーネル 2.4.21 または 2.6 で提供される TUN モジュール

AnyConnect の macOS サポート

macOS の要件

- AnyConnect 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、AnyConnect の最小ディスプレイの解像度を 1024 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 AnyConnect 4.8 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。

AnyConnect のライセンス

最新のエンドユーザーライセンス契約については、『Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 4.x』を参照してください。

オープンソースライセンス通知については、『Open Source Software Used in AnyConnect Secure Mobility Client』を参照してください。

ISE ヘッドエンドから AnyConnect 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 Apex ライセンスが必要です。ISE ライセンスの詳細については、『CiscoIdentity Services Engine 』の「*Cisco ISE* ライセンス」の章を参照してください。

ASA ヘッドエンドから AnyConnect を展開し、VPN および VPN ポスチャ（HostScan）モジュールを使用するには、AnyConnect 4.X Plus または Apex ライセンスが必要です。トライアルライセンスを使用できます。『Cisco AnyConnect Ordering Guide』を参照してください。

AnyConnect 4.X Plus および Apex ライセンスの概要とその機能が使用するライセンスの説明については、『AnyConnect Secure Mobility Client の機能、ライセンス、および OS』を参照してください。

AnyConnect のインストールの概要

AnyConnect の展開は、AnyConnect クライアント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 AnyConnect Secure Mobility Client は、次の方法によってリモートユーザーに展開できます。

- 事前展開：新規インストールとアップグレードは、エンドユーザーによって、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：AnyConnect パッケージは、ヘッドエンド（ASA または ISE サーバー）にロードされます。ユーザーが ASA または ISE に接続すると、AnyConnect 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 AnyConnect クライアント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、AnyConnect がすでにインストールされているシステムで AnyConnect を実行することにより、またはユーザーを 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。
- クラウド更新：Umbrella ローミング セキュリティ モジュールの展開後に、上記およびクラウド更新のいずれかの方法を使用して AnyConnect モジュールを更新できます。クラウ

ド更新では、ソフトウェアアップグレードは Umbrella クラウド インフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。デフォルトでは、クラウド更新からの自動更新は無効です。

AnyConnect を展開する場合に、追加機能を含めるオプションのモジュール、および VPN やその他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。

- すべての AnyConnect モジュールおよびプロファイルを事前展開できます。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 Hostscan 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、ASA から Web 展開できません。

（注） 新しい AnyConnect 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 7 および 8 上の Internet Explorer バージョン 10 および 11 に適用されます。

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、AnyConnect の Web 展開時に Active X に問題が発生します。

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。

AnyConnect のサポートポリシー

シスコでは、最新の 4.x リリースに基づいてのみ修正と拡張機能を提供しています。TAC サポートは、AnyConnect 4.x のリリースバージョンを実行するアクティブな AnyConnect 4.x 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 AnyConnect 4.x 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

Ubuntu 20 で NVM のインストールが失敗する

Ubuntu 20.04（カーネルバージョン 5.4 を使用）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 NVM 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、AnyConnect 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 AnyConnect 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、AnyConnect 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 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。」正常に接続するには、AnyConnect のアップグレード後に別の VPN 接続を手動で開始できます。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. Cisco AnyConnect Network Access Manager 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（AnyConnect 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 の修正は、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、つまり、split-include 設定で nslookup が VPN トンネルを介して DNS クエリを送信しない問題を修正するために保留中となっています。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 CSCvo18938 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。

Apple では、基本的な OS の問題を直接エスカレーションするようお客様に求めています。Apple にエスカレーションする場合は、MacOS の不具合 FB7670484 を参照してください。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）ASA ヘッドエンドまたは SAML プロバイダが 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、AnyConnect 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ように必要な更新を行うまで、AnyConnect が失敗し、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。最適なユーザーエクスペリエンスのために、macOS 10.15 での動作を正式にサポートし、32 ビットコードが含まれない最初のバージョンである AnyConnect 4.8 にアップグレードすることを推奨します。

そうしない場合は、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 AnyConnect HostScan バージョンは、macOS 10.15 では機能しません。「HostScan は、アップグレードなしの macOS 10.15 では機能しない（CSCvq11813） （23 ページ）」を参照してください。
- macOS 10.15 で AnyConnect HostScan および SystemScan を使用する場合、初期起動時に権限ポップアップが表示されます。「AnyConnect HostScan またはシステムスキャンの初回起動時の権限ポップアップ（CSCvq64942） （24 ページ）」を参照してください。

HostScan 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 AnyConnect 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 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が受信されます。

HostScan ユーザーに対して VPN 接続が正常に行われるようにするには、すべての DAP ポリシーおよび HostScan ポリシーが HostScan 4.8.00175（またはそれ以降）と互換性があることが必要です。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 4.3.x から 4.6.x への移行』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、ASA ヘッドエンドに HostScan パッケージを使用するシステムの管理者が HostScan を無効にする方法があります。無効にすると、すべての HostScan 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 を参照してください。

AnyConnect HostScan またはシステムスキャン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、HostScan の初回起動時に、システムスキャン（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 HostScan 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 ポスチャおよび HostScan はエンドポイントのポスチャ評価に OPSWAT を使用し、設定された製品および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 AnyConnect Secure Mobility Client フォルダ内のフォルダアクセスに関連した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

AnyConnect 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。

AnyConnect 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 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することによって、ACL を再設定する必要があります。4.8 からの 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）]** 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/anyconnect/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。

ISE ポスチャでのデフォルトのパッチ管理が検出されない（CSCvq64901）

macOS 10.15 の使用時に、ISE ポスチャがデフォルトのパッチ管理を検出できませんでした。この状況を解決するには、OPSWAT フィックスが必要です。

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 セキュリティ上の制約のために、DART でログを収集するには、macOS、Ubuntu 18.04、および Red Hat 7 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 を使用している場合、IPsec 接続で問題が発生していました。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 AnyConnect は、リリース 9.6 より古い 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 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、AnyConnect 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 AnyConnect 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。

AnyConnect の macOS 10.13（High Sierra）互換性

macOS 10.13（High Sierra）に関する AnyConnect の推奨バージョンは、AnyConnect 4.5.02XXX 以降です。

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 AnyConnect ソフトウェア拡張機能を有効にすることにより、AnyConnect の全機能を活用するために必要な手順をガイドする追加機能および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 AnyConnect を 4.5.02XXX 以降にアップグレードすると、AnyConnect 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の AnyConnect 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 AnyConnect ソフトウェア拡張機能を有効にする必要があります。AnyConnect 4.4.04030 および 4.5.01044 は macOS 10.13 以降で動作することがテストされていますが、それらのユーザーには AnyConnect 4.5.02XXX で提供される追加機能および警告ガイダンスがありません。4.5.02xxx より前のバージョンの AnyConnectの拡張機能を有効にした後は、手動で再起動する必要がある場合があります。

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/ja-jp/HT208019 を参照）。これは現在サポートされているバージョンの AnyConnect 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、AnyConnect ダウンローダ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

この「timestamp signature and/or certificate could not be verified or is malformed」というエラーは、Windows でのみ、ASA または ISE からの AnyConnect 4.4MR2 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 NAM、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 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

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

コマンドを実行することにより、問題が AnyConnect の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、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 AnyConnect アクセスを厳密に制限するように AnyConnect VPN プロファイルを設定します（ASDM プロファイルエディタで、[プリファレンス（Part 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。
- AnyConnect 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の秘密キーのアクセス制御設定を設定します。

Umbrella ローミング セキュリティ プラグインの変更

`OrgInfo.json` ファイルを取得するためのダッシュボードは、現在、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）] に移動し、左上にある [+]（追加アイコン）をクリックして、[AnyConnect Umbrella ローミングセキュリティモジュール（AnyConnect Umbrella Roaming Security Module）] セクションから [モジュールプロファイル（Module Profile）] をクリックします。

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と Microsoft が誤って Windows 10 の更新をブロックする

Microsoft は、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ときに以前のバージョンの Windows への更新をブロックすることを意図していましたが、Windows 10 および Creators Edition（RS2）も誤ってブロックされていました。このエラー（Microsoft Sysdev 11911272）のために、Creators Editor（RS2）にアップグレードには、まずネットワーク 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。アップグレード後にモ

ジュールを再インストールできます。このエラーに関する Microsoft の修正は、2017 年 6 月に予定されています。

Windows 10 Defender の誤検出：Cisco AnyConnect アダプタに関する問題

Windows 10 Creator Update (April 2017) にアップグレードすると、AnyConnect アダプタに問題があることを示す Windows Defender メッセージが表示される場合があります。Windows Defender により、[デバイスのパフォーマンスと正常性（Device Performance and Health）] セクションでアダプタを有効にするように指示されます。実際には、使用していないときはアダプタを無効にしてください（手動で操作しないでください）。この誤検知エラーは、Sysdev 番号 11295710 で Microsoft にレポートされています。

AnyConnect 4.4MR1 以降および 4.3MR5 は、Windows 10 Creators Edition（RS2）と互換性があります。

AnyConnect の Microsoft Windows 10 との互換性

AnyConnect 4.1MR4（4.1.04011）以降は、Windows 10 の公式リリースと互換性があります。Technical Assistance Center（TAC）のサポートは 2015 年 7 月 29 日から開始されています。

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 AnyConnect のクリーンインストールをお勧めします。AnyConnect 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 AnyConnect 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、AnyConnect 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。

AnyConnect リリース 4.2 MR 1 で導入されたこの動作については、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。

- AnyConnectプロファイル（プロファイルエディタの[プリファレンス（Part 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）。

Microsoft の SHA-1 サポートの廃止

SHA-1 証明書または SHA-1 中間証明書付き証明書を持つセキュアゲートウェイは、2017 年 2 月 14 日以降、Windows Internet Explorer 11/Edge ブラウザまたは Windows AnyConnect エンドポイントによって有効と見なされなくなる可能性があります。2017 年 2 月 14 日以降、Windows エンドポイントは、SHA-1 証明書または中間証明書を持つセキュアゲートウェイを信頼できると見なさなくなる可能性があります。セキュアゲートウェイに SHA-1 アイデンティティ証明書を持たせないことと、中間証明書を SHA-1 ではないものにすることを強くお勧めします。

Microsoft は、当初のレコードの計画とタイミングを変更しました。Microsoft は環境が 2017 年 2 月の変更によって影響を受けるかどうかをテストする方法の詳細を公開しました。シスコでは、SHA-1 セキュアゲートウェイまたは中間証明書を使用しているか古いバージョンの AnyConnect を実行している場合に AnyConnect の正常な動作を保証できません。

利用可能な修正をすべて確実に適用するために、AnyConnect の現在のメンテナンスリリースで常に最新の状態に保つことをお勧めします。AnyConnect 4.x 以降の最新バージョンは、アクティブな AnyConnect Plus、Apex、および VPN Only の契約期間がある場合に Cisco.com Software Center で入手できます。AnyConnect バージョン 3.x はすでに積極的なメンテナンスが行われなくなっているため、どの展開にも使用しないでください。

（注） シスコでは、Microsoft が SHA-1 の廃止を進めても、AnyConnect 4.3 および 4.4 以降のリリースは正常に動作しつづけることを確認しました。Microsoft ではあらゆる状況において Windows 全体で SHA-1 の信用を廃止する長期的な計画を持っていますが、Microsoft の現在のアドバイザリでは、これに関する詳細やタイミングは提供されていません。その廃止の正確な日付によっては、いつでも AnyConnect の古いバージョンの多くが動作しなくなる可能性があります。詳細については、Microsoft のアドバイザリを参照してください。

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

OpenSSL 暗号スイートの変更

OpenSSL 規格開発チームがいくつかの暗号スイートをセキュリティ侵害を受けたものとしてマークしたため、それらは AnyConnect 3.1.05187 以降ではサポートされなくなりました。サポートされない暗号スイートにはDES-CBC-SHA、RC4-SHA、およびRC4-MD5が含まれます。

同様に、シスコの暗号ツールキットではRC4暗号がサポートされなくなりました。そのため、それらのシスコのサポートは、リリース 3.1.13011 および 4.2.01035 以降では中止されています。

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、予期どおりの結果を得るために AnyConnect 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

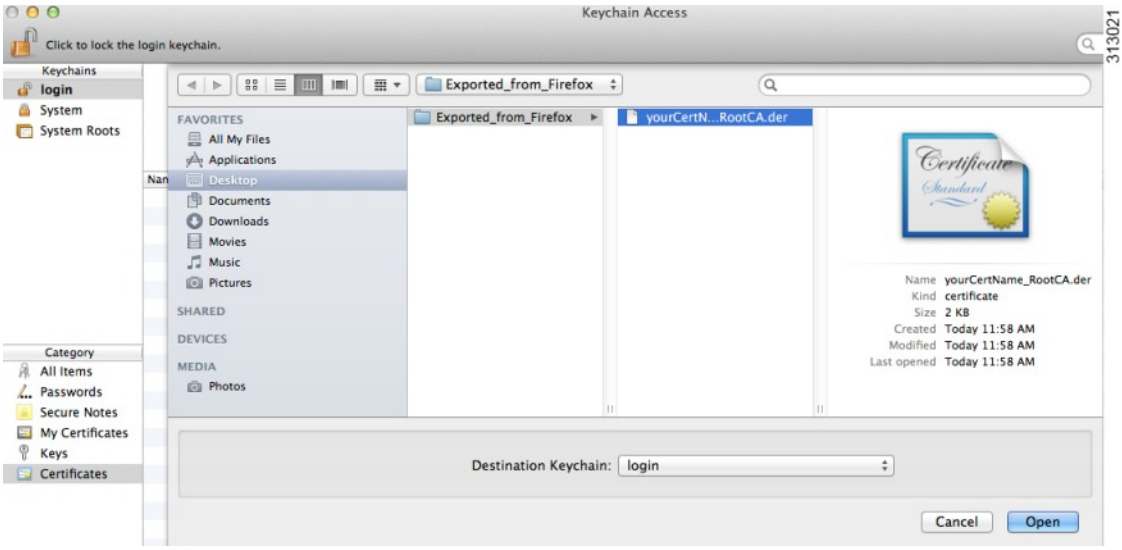
macOS 上の Firefox 証明書ストアは、任意のユーザーがストアの内容を変更することを許可するアクセス権を使用して保存されます。これにより、未認可のユーザーまたはプロセスが不正なCAを信頼されたルートストアに追加することが可能になります。AnyConnectは、サーバー検証またはクライアント証明書に Firefox ストアを使用しなくなりました。

必要に応じて、AnyConnect 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。次の手順は、AnyConnect ユーザーへの指示の一例です。

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. AnyConnect 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。

   AnyConnect 証明書は、多くの場合、[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。

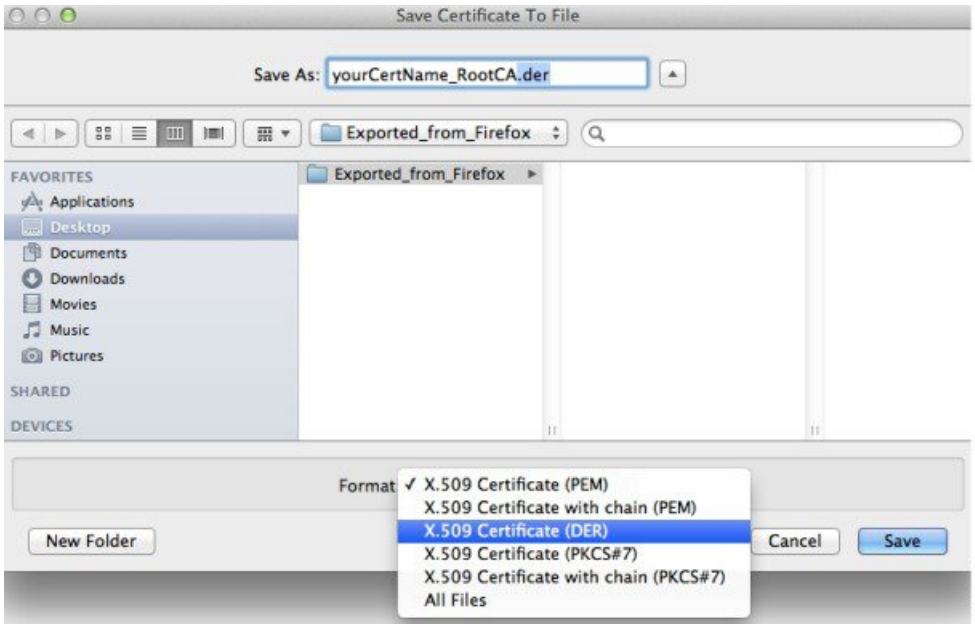


注 複数の AnyConnect 証明書または秘密キー（あるいはその両方）が使用される場合や必要な場合は、証明書ごとに上記のプロセスを繰り返してください。

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. AnyConnect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。

SSLv3 が HostScan の機能を妨げる

（CSCue04930）ASDM で SSLv3 オプションの [SSLv3のみ（SSLv3 only）] または [SSL V3をネゴシエート（Negotiate SSL V3）] が選択されている（[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [詳細設定（Advanced）] > [SSL設定（SSL Settings）] > [セキュリティアプライアンスがサーバーとしてネゴシエートするためのSSLバージョン（The SSL version for the security appliance to negotiate as a server）]）場合、HostScan は機能しません。管理者に警告するために、ASDM に警告メッセージが表示されます。

Safari を使用する場合の WebLaunch の問題

Safari を使用すると WebLaunch で問題が発生します。OS X 10.9（Mavericks）に付属しているバージョンの Safari のデフォルトセキュリティ設定では、AnyConnect Weblaunch は機能しません。WebLaunch が機能するように Safari を設定するには、次のように ASA の URL を「安全でないモード」に編集します。

Safari 9 以前

1. Safari の [環境設定（Preferences）] を開きます。
2. [セキュリティ（Security）] 設定を選択します。
3. [Webサイト設定を管理...（Manage Website Settings...）] ボタンをクリックします。
4. 左側のオプションリストから [Java] を選択します。

5. 接続を試みる Web サイト「Hostname_or_IP_address」のオプションを [開かない（Block）] から [常に許可（Allow Always）] に変更します。
6. [完了（Done）] をクリックします。

Safari 10 以降

1. Safari の [環境設定（Preferences）] を開きます。
2. [セキュリティ（Security）] 設定を選択します。
3. [インターネットプラグイン:（Internet plug-ins:）] オプションの [プラグインを許可（allow plug-ins）] をオンにします。
4. [プラグイン設定（Plug-ins Settings）] ボタンを選択します。
5. 左側のオプションリストから [Java] を選択します。
6. 接続を試みる「Hostname_or_IP_address」を強調表示します。
7. **Alt** キー（または **Option** キー）を押したままドロップダウンメニューをクリックします。[オン（On）] がオンになっていることと [安全なモードで実行（Run in Safe Mode）] がオフになっていることを確認します。
8. [完了（Done）] をクリックします。

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かぎり、WebLaunch による AnyConnect 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、AnyConnect 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

AnyConnect Secure Mobility Client、Hostscan、CSD、およびクライアントレス SSL VPN（WebVPN）は、Java 7 によって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『Java 7 Issues with AnyConnect, CSD/Hostscan, and WebVPN - Troubleshooting Guide』（[セキュリティ（Security）] > [Cisco Hostscan] 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

トンネルオールネットワークが設定されている場合に暗号化されていないローカル DHCP トラフィックフローを可能にするために、AnyConnect は、AnyConnect クライアントが接続したと

きに ローカル DHCP サーバーへの特定のルートを追加します。また、このルートでのデータ漏えいを防ぐため、AnyConnect 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。

テザーデバイスを介した AnyConnect VPN

シスコでは、Bluetooth または USB テザリングの Apple iPhoneを介した AnyConnect VPN クライアントのみを認定しています。他のテザーデバイスによって提供されるネットワーク接続は、展開前に AnyConnect VPN クライアントで確認する必要があります。

AnyConnect のスマートカードサポート

AnyConnect は、次の環境でスマートカードにより提供されるクレデンシャルに対応します。

- 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 AnyConnect 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。

AnyConnect の仮想テスト環境

シスコは、次の仮想マシン環境を使用して AnyConnect 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 AnyConnect の実行はサポートしませんが、シスコがテストする VMWare 環境では AnyConnect は適切に機能すると予測されます。

仮想環境で AnyConnect 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。

AnyConnect パスワードの UTF-8 文字サポート

ASA 8.4(1) 以降で使用される AnyConnect 3.0 以降で、RADIUS/MSCHAP および LDAP プロトコルを使用して送信されるパスワードの UTF-8 文字がサポートされます。

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

AnyConnect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、ASAに同じバージョンまたはそれ以前のバージョンの AnyConnect 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、ASA で同じバージョンまたはそれ以前のバージョンの AnyConnect 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、AnyConnect 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。

SHA 2 証明書検証エラーの回避（CSCtn59317）

AnyConnect クライアントは、IPsec/IKEv2 VPN 接続の IKEv2 認証フェーズ中に必要とされるデータのハッシングおよび署名を Windows Cryptographic Service Provider（CSP）に依存しています。CSP が SHA 2 アルゴリズムをサポートしていておらず、ASA が疑似乱数関数（PRF）SHA256、SHA384、SHA512 用に設定されていて、接続プロファイル（tunnel-group）が証明書用、または証明書と AAA 認証用に設定されている場合、証明書認証は失敗します。ユーザーは「Certificate Validation Failure」というメッセージを受け取ります。

このエラーは、SHA 2 タイプのアルゴリズムをサポートしていない CSP に属する証明書を、Windows で使用した場合のみ発生します。その他のサポート対象 OS では、この問題は発生しません。

この問題を回避するには、ASA の IKEv2 ポリシーで、PRF を md5 または sha（SHA 1）に設定します。あるいは、証明書の CSP 値を、機能するネイティブ CSP（Microsoft Enhanced RSA や AES Cryptographic Provider など）に変更することもできます。SmartCards 証明書には、この回避策を使用しないでください。CSP 名を変更できません。代わりに、SmartCard のプロバイダに問い合わせて、SHA 2 アルゴリズムをサポートする、更新された CSP を入手してください。

注意 次の回避策は、手順を誤って実行した場合、ユーザー証明書を破損するおそれがあります。証明書で変更を指定するときは、十分に注意してください。

Microsoft Certutil.exe ユーティリティを使用して、証明書 CSP 値を変更できます。Certutil は、Windows CA を管理するためのコマンドライン ユーティリティで、Microsoft Windows Server 2003 Administration Tools Pack に同梱されています。Tools Pack は、次の URL からダウンロードできます。

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Certutil.exe を実行して証明書 CSP 値を変更するには、次の作業を実行します。

1. エンドポイントコンピュータでコマンドウィンドウを開きます。
2. **certutil -store -user My** コマンドを使用して、ユーザーストアに格納されている証明書と、その証明書の現在の CSP 値を表示します。

   次に、このコマンドで表示される証明書の内容の例を示します。

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

3. この証明書の <CN> 属性を特定します。この例では、CN は Carol Smith です。この情報は次のステップに必要です。
4. 次のコマンドを使用して、証明書CSP を変更します。次に、サブジェクト <CN> 値を使用して、変更する証明書を選択する例を示します。その他の属性も使用できます。

   Windows 7 以降の場合は、**certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore -user My <CN> carol smith** コマンドを使用します。
5. ステップ 2 を繰り返して、表示される証明書の新しい CSP 値を確認します。

AnyConnect 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 AnyConnect 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。AnyConnectのモジュールまたはパッケージをインストールしたら、Cisco AnyConnect のインストールフォルダを許可するか、Cisco AnyConnect アプリケーションに関するセキュリティ例外を指定するようにウィ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

HostScan 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 HostScan パッケージを含む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 HostScan パッケージをインストールする前に、以下の HostScan アプリケーションに対してセキュリティの例外を許可するか指定するようにマルウェア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

AnyConnect 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、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）] > [SSL VPNクライアント（SSL VPN 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 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）に戻す必要があります。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、ASA での MTU 設定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、AnyConnect は完全認証のたびにクレデンシャル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）。

IPv6 Web トラフィックでの Cisco クラウド Web セキュリティの動作に関するユーザーガイドライン

IPv6アドレス、ドメイン名、アドレス範囲、またはワイルドカードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニングプロキシに送信されます。ここで DNS ルックアップが実行され、ユーザーがアクセスしようとしている URL に IPv4 アドレスがあるかどうかが確認されます。IPv4アドレスが見つかると、スキャニングプロキシはそのアドレスを使用して接続します。IPv4 アドレスが見つからない場合は、接続はドロップされます。

すべての IPv6 トラフィックがスキャニングプロキシをバイパスするように設定する場合は、すべてのIPv6トラフィック ::/0にこの静的な例外を追加します。これを行うことで、すべての

IPv6 トラフィックがすべてのスキャニングプロキシをバイパスします。つまり、この場合は IPv6 トラフィックは Cisco クラウド Web セキュリティで保護されません。

LAN 内の他のデバイスでのホスト名の表示を防止する

AnyConnect 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 内の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。

AnyConnect ホストがサブネット間でのホスト名（AnyConnect エンドポイントホストの名前を含む）の漏洩を確実に防ぐために、そのエンドポイントがプライマリブラウザ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、AnyConnect 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 AnyConnect 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 AnyConnect のパフォーマンス

macOS 用の AnyConnect クライアントが、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 AnyConnect クライアントが特定タイプのルータ（Cisco Virtual Office（CVO）ルータなど）の背後から 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、残りのトラフィックがドロップされる可能性があります。AnyConnect 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、AnyConnect アダプタの MTU の値を手動で減らします。

`sudo ifconfig utun0 mtu 1200`（macOS v10.7 以降の場合）

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。これにより、AnyConnect プロファイルファイルを削除できるため、常時接続機能を無効にすることができます。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 AnyConnect が不安定になるおそれがあります。AnyConnect 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。

AnyConnect では 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る

AnyConnect では、ASA が TLSv1 トラフィックまたは 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。

このため、AnyConnect クライアントは、「ssl server-version」について次の 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。

HostScan のレポートの内容

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のどれもが、最終スキャン時間情報をレポートしません。HostScan では次の内容がレポートされます。

- 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。リリース 3.1.03103 では、マルチホームシステムを使用している場合にも、再接続に時間がかかることがあります。

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

Windows 7 以降では、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 AnyConnect クライアント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。Windows 7 では、高速ローミングは使用できません。

AnyConnect Secure Mobility 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

AnyConnect Secure Mobility 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 AnyConnect VPN クライアントの 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。

AnyConnect 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。

AnyConnect 4.9.06037

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://tools.cisco.com/RPF/register/register.do 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
CSCvw53140	certificate	Windows での VPN モジュールに関するスマートカードの問題

識別子	コンポーネント	タイトル
CSCvw54056	core	Big Sur で AC 4.8 を 4.904043 にアップグレードした後、永続的な「シスコシステム拡張がブロックされました（Cisco System Extensions Blocked）」というプロンプトが表示される
CSCvw26076	nam	NAM PE：[ログオン前の接続の許可（Allow Connection Before Logon）] ユーザー設定のデフォルトに対する管理制御を追加
CSCvx25251	nvm	Ubuntu 20 の最新カーネルバージョンで NVM のインストールが失敗する
CSCvv73666	opswat-ise	ボリューム名に非標準文字が含まれているため、ISE ポスチャのディスク暗号化条件が失敗する
CSCvt62025	posture-ise	アダプタの状態が変化すると、ポスチャモジュールがトリガーされる
CSCvw72250	vpn	macOS：FQDN がデフォルトドメイン以外の DNS 名と一致する場合、短縮名による DNS クエリが失敗する
CSCvw92182	vpn	ASA TLS のみに接続された macOS 上の AnyConnect が、接続から約 20 秒後に再接続する

AnyConnect 4.9.05042

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://tools.cisco.com/RPF/register/register.do 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
CSCvw19751	core	macOS デュアル NIC：いずれかの NIC を切断して再接続した後、トンネルを再確立できない
CSCvw21846	nam	ルート CA 証明書のみを含めるように設定すると、NAM サービスがクラッシュする
CSCvw55271	nam	ユーザーネットワークで、ユーザー制御ポリシーが許可しない場合に[ログオン前の接続の許可（Allow Connect Before Logon）] を設定できる
CSCvw23375	posture-ise	ISE ポスチャが Crowdstrike バージョン 6.x を検出しない
CSCvw30269	vpn	macOS：以前はサードパーティ フィルタリングで許可されていた事前 VPN 接続が、AnyConnect でブロックされない

AnyConnect 4.9.04053

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://tools.cisco.com/RPF/register/register.do 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
CSCvw48062	download_install	ローカルポリシーによるカスタムスクリプト、ヘルプファイル、UI、およびローカリゼーションのオプションファイル Web 展開の制限

AnyConnect 4.9.04043

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://tools.cisco.com/RPF/register/register.do 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
CSCvu27862	core	jquery 3.2.1 の複数の脆弱性
CSCvv68334	core	ログオン前のステータスで vpncli を呼び出すと、ログオン後のトンネルに接続されてから終了する
CSCvv91510	core	常にオン/TND：DHCP 対応の直接接続されたコンピュータ
CSCvv91836	nam	TLS RSA 暗号がキー交換に選択されていると、802.11 4 ウェイハンドシェイクが完了しない
CSCvv35857	opswat-ise	Check Point Endpoint Security 83.x をサポートするための AnyConnect ISE ポスチャ コンプライアンス モジュールの更新

識別子	コンポーネント	タイトル
CSCvv69211	posture-ise	Windows でモダンスタンバイを有効にすると、AnyConnect で複数の内部エラーポップアップが表示されることがある
CSCvv30401	vpn	200以上のダイナミックトンネル除外を適用した後の macOS ネットワーク接続の問題
CSCvv43515	vpn	ダイナミックスプリット除外トンネリングを使用して設定すると Zoom アプリが遅くなる
CSCvv45271	vpn	AutoConnectOnStart が true で、ASA アップグレード後に VPN トンネルが切断される
CSCvv61677	vpn	Bluetooth NIC を使用している場合、AnyConnect から device-mac/device-public-mac ACIDEX 属性が送信されない
CSCvv68971	vpn	macOS：Windows との一貫性を保つためにプライベートプロキシ設定がプッシュされた場合、SOCKS プロトコルが削除される
CSCvv89360	vpn	サーバーリストの URL にデフォルト以外のポート番号がある場合、AnyConnect はクライアントプロファイル設定を無視する
CSCvv94399	vpn	tunnel-group-list が有効になっていないと AC はローカル CA に登録できない
CSCvw23502	vpn	AnyConnect は、SSL 接続の Windows での認証にユーザー証明書を試行しない

AnyConnect 4.9.03049

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://tools.cisco.com/RPF/register/register.do 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
CSCvw14118	vpn	VPN：Windows：ユーザー名/パスワードにキリル文字/Unicode 文字が含まれていると認証に失敗する

AnyConnect 4.9.03047

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://tools.cisco.com/RPF/register/register.do 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
CSCvs28224	core	デフォルトの ike-id を EAP 認証で使用すると、ルータの FlexVPN が機能しない
CSCvu14970	core	Cisco AnyConnect AllowRemoteUsers バイパス
CSCvu77777	core	CIAM：sqlite 3.28.0
CSCvu78363	core	ネイティブ VPN クライアントが設定されていると、AnyConnect Start Before Logon（SBL）に誤った名前が表示される

識別子	コンポーネント	タイトル
CSCvu83063	core	ダイナミックスプリット除外トンネリングが有効な場合、マルチホームマシンにより AnyConnect が再接続される
CSCvv02329	core	AnyConnect 4.8.03052 がバックアップサーバーへの接続時に IPv4 をスキップする
CSCvv39691	core	AnyConnect 4.9 を使用すると、Windows 起動の PC への事前ログイン時に AnyConnect 管理トンネルが失敗する
CSCvt28992	nam	AnyConnect は、実際に正常に接続しているときにワイヤレスに接続すると -256 の無効な RSSI を表示する
CSCvu26049	nam	NAM が予期しない EAP-FAST PAC プロビジョニングの成功でクラッシュする
CSCvu65082	nam	NAM ログが誤ったタイムゾーンを示す
CSCvv11582	nam	ISE で Dot1x NAM EAP チェーンエラー「失敗の理由 12963 形式が誤った EAP ペイロード TLV を受信しました（Failure reason 12963 received malformed EAP payload TLV）」が発生する
CSCvv32331	nam	NAM が複数の EAP 開始要求をタイムアウト前に送信する
CSCvv45245	nam	CSCvs59943 の回帰。アダプタが関連付けで停止するため、NAM がワイヤレス接続を開けない
CSCvv31801	nvm	NVMS から AC+NVM へのアップグレードで、TND の状態が信頼状態から非信頼状態に変更された

識別子	コンポーネント	タイトル
CSCvq97293	opswat-ise	ENH：macOS 用 Bitdefender 8.0.0.3 のコンプライアンスモジュールのサポート
CSCvs82258	opswat-ise	LANDesk 11.x Security and Patch Manager のサポート
CSCvt07676	opswat-ise	CM 4.3.1053.6145 が Sophos クラウドエンドポイントの定義日として現在の日時を返す
CSCvu65632	opswat-ise	ISE ポスチャモジュールが Windows ファイアウォールステータスを正しく検出しない
CSCvt36028	posture-ise	ISE での Avast Free 20.1 xxxx のサポート
CSCvu99746	posture-ise	macOS で断続的に「aciseposture」プロセスの起動に失敗する
CSCvr70933	vpn	macOS 上の AnyConnect VPN トンネルが Sidecar 機能に干渉する
CSCvv09906	vpn	タイプ 5 の IPsec to ISE VPN 属性を受信したが、最小要件 1 を満たしていない
CSCvv10339	vpn	VPNLB：AnyConnect がプロキシ認証を介して VIP に接続できない
CSCvv65303	vpn	macOS 11：VPN が接続された状態でスリープから復帰した後、システム全体で DNS 解決が失敗する

AnyConnect 4.9.02028

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://tools.cisco.com/RPF/register/register.do 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
CSCvu57985	core	ENH：AnyConnect での NetworkExtension のサポート

AnyConnect 4.9.01095

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://tools.cisco.com/RPF/register/register.do 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
CSCvp53403	core	SBL 経由で接続した後、予期しない（誤った）<HostName> が GUI に表示される
CSCvt08780	core	Linux 上の VM インスタンス/Docker コンテナがネットワークトラフィックをルーティングできない
CSCvu03376	core	「プロキシの自動検出」（グループプロキシに設定されたプライベートプロキシ）を使用すると、断続的なブラウジングエラーが発生する
CSCvu19710	core	WiFi 通話（FaceTime 通話）を使用している場合、IP 転送テーブルを変更できないエラーが発生する
CSCvu82615	core	VPN クライアントエージェントの DNS コンポーネントで予期しないエラー（ダイナミック スプリット トンネリング）が発生する
CSCvv15092	core	macOS 上の AnyConnect 4.9.00086 で高メモリ使用率が報告される

識別子	コンポーネント	タイトル
CSCvu65566	dart	Linux DART が複製された OS でなくても同じ UDID を生成する
CSCvu22557	download_install	4.8.3052 から 4.9.64 にアップグレードした後、AnyConnect が IPsec を介した VPN 接続を確立できない
CSCvu03997	gui	MacOS 組み込み SAML ブラウザが dmg ファイルをダウンロードしない
CSCvs78379	nam	SBL GUI を使用して作成された WiFi ネットワークへのログオン時に接続が維持されない
CSCvs86736	nam	NAM で 1024 バイトを超える PAC ファイルを使用できる
CSCvt06237	nam	VPN 管理トンネルをサポートするために、マシン動作中に接続するユーザー作成ネットワークのオプションを追加
CSCvt74330	nam	管理者が設定した非表示ネットワークが使用できない場合、NAM クライアントがユーザー定義ネットワークへの切り替えに失敗する
CSCvu24358	nam	NAM を使用して PC で RDP セッションを閉じた後、ローカルでログインできない
CSCvu26262	nam	NAM クレデンシャルプロバイダが Imprivata OneSign エージェント クレデンシャル プロバイダ DLL をロードしない
CSCvq97328	opswat-ise	ENH：macOS 用 Kaspersky Internet Security 20.x のコンプライアンスモジュールのサポート

識別子	コンポーネント	タイトル
CSCvu83305	opswat-ise	Cortex 7.x の AnyConnect AM 条件
CSCvc89249	posture-ise	ポスチャ用の TrendMicro WorryFree 6.x のサポート
CSCvm56656	posture-ise	ESET Endpoint Security 7.x の AC コンプライアンスモジュール 4.3.x のサポート
CSCvo46838	posture-ise	Kaspersky Endpoint Security 11.x がポスチャ修復時のディスク暗号化に存在しない
CSCvp27316	posture-ise	ENH：Trend Micro Apex One 14.x のコンプライアンスモジュールのサポート
CSCvq20688	posture-ise	macOS に対するポスチャ KES11 のサポート
CSCvu06725	swg	SWG クライアントのクラッシュ/フリーズ
CSCvu63661	umbrella	大きい応答で複数の TCP DNS 要求を送信した後、DNS 解決がグローバルにハングする
CSCvu68957	umbrella	macOS での Umbrella の同期と状態変更の遅延
CSCvu73467	umbrella	NIC（IPv6 DNS サーバー）でダイナミック IPv6 設定を有効にした後、Umbrella DNS 保護が無効になる
CSCvf65224	vpn	ENH：AnyConnect が Linux マシンの /etc/ssl/certs ディレクトリで CA 証明書を検索できるようにする
CSCvt35162	vpn	Windows 機能の自動再起動サインオン（ARSO）が原因で、AnyConnect SBL アイコンが表示されない

識別子	コンポーネント	タイトル
CSCvt49314	vpn	アクティブな DTLS セッションが TLS に戻った後、AnyConnect が複数回再接続する
CSCvt63861	vpn	Weblaunch を使用した Linux プラットフォームでの AnyConnect のインストール手順に誤った OS イメージが表示される
CSCvt64638	vpn	Windows のみ：AnyConnect はインターフェイス名に Unicode 文字をサポートしない
CSCvt85695	vpn	AnyConnect が最初の IKE_SA_INIT で Diffie-Hellman グループ 1 または 2 を提供する
CSCvu95344	vpn	AnyConnect がスマートカードの取り外し時に VPN の切断に失敗する
CSCvv19684	vpn	4.9 FCS から 4.9 MR1 へのクラウドアップグレードが開始されない

AnyConnect 4.9.00086

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://tools.cisco.com/RPF/register/register.do 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
CSCvs60391	core	OpenSSL 1.0.2q での複数の脆弱性
CSCvs60397	core	libxml2 2.9.8 での複数の脆弱性

識別子	コンポーネント	タイトル
CSCvt31657	core	Umbrella/SWG クライアントが O365 バイパスを受け入れない
CSCvt74385	core	ダイナミックスプリット除外を追加する際の MacOS/pfctl の遅延
CSCvt92079	core	MacOS：断続的な OS メモリ割り当ての失敗により、IPv6 ルートテーブルが不整合状態のままになる
CSCvu46279	core	MacOS：vpnagent のブロックによるネットワークトラフィックの通過遅延
CSCvu22557	download_install	4.8.3052 から 4.9.64 にアップグレードした後、AnyConnect が IPsec を介した VPN 接続を確立できない
CSCvt82526	gui	AnyConnect for Windows VPN SAML ブラウザが重複した JavaScript キーイベントを生成することがある
CSCvu03997	gui	MacOS 組み込み SAML ブラウザが dmg ファイルをダウンロードしない
CSCvm85974	nam	PSK を使用して SSID に誤ったパスワードを入力した場合に、AnyConnect NAM がパスワードの再入力を要求しない
CSCvt99342	nam	非認証 PAC プロビジョニングのサポートの終了：4.9 以降
CSCvu13185	nam	NAM PE：ユーザーが作成したネットワークがマシンタイム中に接続できるようにする設定ポリシーオプションを追加
CSCvu06461	nvm	パスと引数が大きい場合にドロップされる CFlow

識別子	コンポーネント	タイトル
CSCvt12850	nvm	Android-NVM：NVM TND が信頼できないとして設定されている場合、キャッシュされたフローはすぐに送信されない
CSCvu01704	nvm	NVM コレクタが nvzFlowV4 テンプレートをプリロードしない
CSCvu21676	nvm	Linux：プロセス引数の取得中に NVMAgent がクラッシュする
CSCvr21787	opswat-ise	ENH：Trend Micro OfficeScan クライアントバージョン 14.x のサポート
CSCvc89249	posture-ise	ポスチャ用の TrendMicro WorryFree 6.x のサポート
CSCvm56656	posture-ise	ESET エンドポイント セキュリティの AnyConnect コンプライアンスモジュール 7 のサポート
CSCvo46838	posture-ise	Kaspersky Endpoint Security 11.x がポスチャ修復時のディスク暗号化に存在しない
CSCvp27316	posture-ise	ENH：Trend Micro Apex One 14.x のコンプライアンスモジュールのサポート
CSCvq20688	posture-ise	macOS に対するポスチャ KES11 のサポート
CSCvt72492	umbrella	Umbrella クラウド 更新パラメータの変更が Windows に適用されないことがある
CSCvf32537	vpn	ENH：AnyConnect の VPN 高帯域幅/スループットパフォーマンスの向上

識別子	コンポーネント	タイトル
CSCvq74726	vpn	ENH：AnyConnect ダイナミック スプリット トンネリングは、TTL が低いシナリオをサポートする必要がある
CSCvs78426	vpn	DHCPトラフィックが VPN トンネル経由で誤って送信される
CSCvt49314	vpn	アクティブな DTLS セッションが TLS に戻った後、AnyConnect が複数回再接続する
CSCvt75904	vpn	MacOS：Umbrella が MacOS で予約済みの状態のままになる
CSCvt81585	vpn	AnyConenct VPN がエラー「HTTP/1.1 401 未承認の X による：その他のエラー（HTTP/1.1 401 Unauthorized X-Reason: Other error）」 で接続に失敗する
CSCvt85695	vpn	AnyConnect は最初の IKE_SA_INIT で Diffie-Hellman グループ 1 または 2 を提供してはならない
CSCvt88461	vpn	AnyConenct VPN がアップグレード後にエラー「HTTP/1.1 401 未承認の X による：その他のエラー（HTTP/1.1 401 Unauthorized X-Reason: Other error）」で接続に失敗する
CSCvt90659	vpn	AC 4.8.3036 MacOS：短縮名による DNS クエリが機能しない：MacOS リゾルバがデフォルトドメインを追加しない
CSCvt95013	vpn	AnyConnect VPN ロードバランシング IKEv2 が AC 4.8 で失敗する

識別子	コンポーネント	タイトル
CSCvu03917	vpn	自動証明書選択が有効な状態で AnyConnect が接続に失敗する
CSCvu10868	vpn	静的スプリット除外が動的除外のスーパーネットの場合は、動的スプリット除外によって接続が切断される
CSCvt65103	vpn-wer	ENH：非 RDP リモートデスクトップタイプに関する AnyConnect のサポート

未解決

このリリースに含まれる未解決の不具合に関する最新情報については、Cisco Bug Search Tool を参照してください。

識別子	コンポーネント	タイトル
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
CSCvu51439	nvm	NVM プロファイルが ASDM で編集されるたびに、TND 設定が複製され、エンドポイントにプッシュされる

HostScan 4.9.06046

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://tools.cisco.com/RPF/register/register.do 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
CSCvx11008	posture-asa	macOS 上の Cybereason ActiveProbe が HostScan 4.9.04045 または 4.9.05042 で検出されない
CSCvx38993	posture-asa	Apple M1 チップが挿入された macOS Big Sur のシリアル番号を HostScan が取得できない

HostScan 4.9.06037

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://tools.cisco.com/RPF/register/register.do 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
CSCvw93595	opswat-asa	サーバー名識別（SNI）のサポートの追加

HostScan 4.9.05042

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://tools.cisco.com/RPF/register/register.do 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
CSCvv79007	opswat-asa	HostScan による MS Defender ATP（マルウェア対策クライアントバージョン 101.01.54 および 101.06.63）の検出のサポート
CSCvw72925	opswat-asa	HostScan 4.9.04045 で CrowdStrike 6.x バージョンを検出できない

HostScan 4.9.04045

HostScan 4.9.04045 には、Windows、macOS、Linux 用の更新された OPSWAT エンジンのバージョンが含まれています。詳細については、「Release and Compatibility」の下にある「HostScan Support Charts」を参照してください。

HostScan 4.9.03057

HostScan 4.9.03057 には、Windows、macOS、Linux 用の更新された OPSWAT エンジンのバージョンが含まれています。詳細については、「Release and Compatibility」の下にある「HostScan Support Charts」を参照してください。

HostScan 4.9.02028

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://tools.cisco.com/RPF/register/register.do 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
CSCvu16574	opswat-asa	ENH：Endgame（Elastic）Anti-Malware 3.52.14 の AnyConnect HostScan サポート

HostScan 4.9.01095

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://tools.cisco.com/RPF/register/register.do 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
CSCvr90986	opswat-asa	ENH：Windows 10 エンドポイントの Microsoft Defender Advanced Threat Protection（ATP）の HostScan サポート
CSCvu14696	opswat-asa	HostScan Ciscod デーモンが複数の codesign/pkgutil プロセスを作成する
CSCvu20458	opswat-asa	HostScan が誤って 4.18.1902.5 よりも高いバージョンの Windows Defender を報告する
CSCvt12241	posture-asa	AnyConnect 4.9.x HostScan が Linux で開始されているポスチャアセスメントでスタックする

HostScan 4.9.00086

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://tools.cisco.com/RPF/register/register.do 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
CSCvt12241	posture-asa	AC 98.136.00022（4.9）HostScan が Linux で開始されているポスチャアセスメントでスタックする

【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。