Cisco AnyConnect セキュア モビリティ クライアント リリース 4.10 リリースノート

初版：2023 年 5 月 4 日

最終更新：2024 年 2 月 26 日

Cisco AnyConnect セキュア モビリティ クライアント リリース 4.10 リリースノート

このリリースノートには、Windows、macOS、および Linux 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 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。

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 AnyConnect セキュア モビリティ クライアント 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 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 AnyConnect セキュア モビリティ クライアント 管理者ガイド、リリース 4.x を参照してください。

Web 展開用の AnyConnect セキュア モビリティ クライアント 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

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

事前展開用の AnyConnect パッケージファイル名

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）	（スクリプトインストーラーの場合）anyconnect-linux64-version-predeploy-k9.tar.gz （RPM インストーラ*の場合）anyconnect-linux64-*version*-predeploy-rpm-k9.tar.gz （DEB インストーラ*の場合）anyconnect-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

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 4.10.08029 の新機能

これは、次の新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、AnyConnect 4.10.08029 （49 ページ）に記載されている不具合を修正します。

- Windows 10 ARM64 のサポートは終了しました。
- ダイナミックスプリット除外は、CNAME DNS 応答に基づいて macOS AnyConnect でサポートされています

既知の問題：

- CSCwj04530：特定のシナリオにおいて、macOS12 でキャプティブポータルが組み込みブラウザにロードされない
- CSCwi99127：NVM：マルチホーミングがサポートされない

AnyConnect 4.10.08025 の新機能

これは、次の新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、AnyConnect 4.10.08025（50 ページ）に記載されている不具合を修正します。

- CSCur83728：EAP-FAST ネットワークがあり、証明書によって認証されている場合、[スマートカードの削除ポリシー（Smart Card Removal Policy）] で [ネットワークからの切断（Disconnect from Network）] を選択すると、ネットワークが切断されたときにスマートカードが削除されます。
- Windows の修正プログラムが利用可能になるまで PMF IGTK の設定を無効にするために、ネットワーク アクセス マネージャの追加機能を実装しました。Microsoft は、Windows 10 22H2 および Windows 11 21H2（およびそれ以降）の修正プログラムが 2024 年の前半に利用可能になると見積もっています。これにより、ネットワーク アクセス マネージャから IGTK を設定できるようになります。それまでは、PMF IGTK の設定を無効にしておけば、管理フレーム保護（PMF）を提供するように設定されたネットワークへ接続できます。Windows の修正プログラムがまだ利用できず、PMF が有効になっているネットワークへの接続を回避できない場合は、次のレジストリキーを DWORD として追加し、説明に従って設定することで Windows レジストリエディタを変更し、ネットワーク アクセス マネージャによる IGTK の使用を無効にする必要があります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableIGTK
 set to 1
```

（注） ワイヤレス管理フレームを保護するため、必要な場合以外は PMF IGTK を無効にしないことを強くお勧めします。

- **既知の問題**：
  - CSCwh23924：SBL/Network Access Manager のインストール後、再起動を求めるポップアップが表示されない
  - CSCwi53240：4.10 MR8 ビルドで、最新のカーネルを使用する Ubuntu で Network Visibility Module のインストールが失敗する

AnyConnect 4.10.07073 の新機能

これは、次の Cisco Umbrella ローミング セキュリティ モジュールに対する更新を含むメンテナンスリリースであり、「AnyConnect 4.10.07073 （54 ページ）」に記載されている不具合を修正します。

- 一部のデュアルスタック IPv6 ネットワークでの DNS 保護の信頼性向上
- DNS セキュリティモジュールの保護または接続が定期的に失われる問題の修正

AnyConnect 4.10.07062 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 AnyConnect メンテナンスリリースです。解決済みの不具合の詳細については、AnyConnect 4.10.07062 （54 ページ）を参照してください。

AnyConnect 4.10.07061 の新機能

これは、次の新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、「AnyConnect 4.10.07061 （55 ページ）」に記載されている不具合を修正します。

- 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。
- 802.1x-SHA256 のサポートが、ネットワーク アクセス マネージャのワイヤレス認証キー管理スイートに追加されました（CSCwe38560）。
- [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。
- [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：

（CSCwf21453）：[ログオフ時にVPNを保持（Retain VPN on Logoff）]のクライアントプロファイル設定が [有効（Enabled）] で、[ユーザーの強制（User Enforcement）] が [すべてのユーザー（Any User）] に設定されている場合でも、ユーザーがサインアウトし、別のユーザーがログインしたときに、確立された VPN 接続が保持されません。「VPNクライアントエージェント

がプライベート側プロキシ設定を構成しているため、ユーザーログオン中にパブリックプロキシ設定を復元できません。（The VPN client agent has configured private-side proxy settings and is unable to restore public proxy settings during user logon.）」というエラーで VPN 接続が終了します。

AnyConnect 4.10.06090 の新機能

これは、「AnyConnect 4.10.06090 （60 ページ）」に記載されている不具合を修正するメンテナンスリリースです。

AnyConnect 4.10.06079 の新機能

これは、次の新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、AnyConnect 4.10.06079 （60 ページ）に記載されている不具合を修正します。

- Network Access Manager でのキャプティブポータルの検出のサポート。
- プロファイルエディタ設定の認証タイムアウト値の処理を調整しました（CSCvx35970）。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.10』の「*AnyConnect Profile Editor, Preferences (Part 2)*」を参照してください。
- AnyConnect は、外部ブラウザ SAML 認証による DNS ロードバランシングをサポートしていません。

AnyConnect 4.10.05111 の新機能

これは、「AnyConnect 4.10.05111 （64 ページ）」に記載されている不具合を修正するメンテナンスリリースです。

AnyConnect 4.10.05095 の新機能

これはメンテナンス リリースで、次の拡張機能を含み、AnyConnect 4.10.05095 （64 ページ）に記載されている不具合が修正されています。

- Windows では、WebView2 ランタイムがインストールされていると、AnyConnect 組み込みブラウザはデフォルトで WebView2 になります。従来の組み込みブラウザのコントロールに戻す必要がある場合は、1 に設定された **DWORD** レジストリ値 UseLegacyEmbeddedBrowser を次のレジストリキーのいずれかに追加します。
  - （64 ビットマシン）Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco AnyConnect Secure Mobility Client
  - （32 ビットマシン）Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

- （32 ビットまたは 64 ビットマシン）
  Computer\HKEY_CURRENT_USER\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

- macOS 11 以降のバージョンでドメインネームシステム全体の障害を引き起こし、解決のために AnyConnect の再起動か削除が必要になる可能性がある Umbrella の問題が修正されました。
- ポスチャ条件スクリプトを作成およびアップロードして、エンドポイントでポスチャチェックを実行できる機能
  - Windows：PowerShell script (.ps1)
  - macOS：Shell script (.sh)
  - Linux：Shell script (.sh)

AnyConnect 4.10.05085 の新機能

これは、次のサポートの更新を含むメンテナンスリリースであり、「AnyConnect 4.10.05085 （65 ページ）」に記載されている不具合を修正します。

- Big Sur（macOS 11.x）以降のバージョンの Apple AirDrop に関して、AnyConnect VPN の相互運用性が追加されました。このような相互運用性を確保するには、VPN ポリシーで IPv6 ローカル LAN スプリット除外トンネリングを有効にする必要があります。（CSCwa59261）
- Linux プラットフォームの Network Visibility Module で発生していた UDID 衝突の問題は修正されており、AnyConnect 4.10.05081 へのアップグレード後に是正されます。

AnyConnect 4.10.04071 の新機能

これは、「AnyConnect 4.10.04071 （67 ページ）」に記載されている不具合を修正するメンテナンスリリースです。

AnyConnect 4.10.04065 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、「AnyConnect 4.10.04065 （68 ページ）」に記載されている不具合を修正します。

- AnyConnect VPN SAML 外部ブラウザのサポート：オプションのアドオンとして、AnyConnect VPN SAML 外部ブラウザで使用する外部ブラウザパッケージ（external-sso-4.10.04065-webdeploy-k9.pkg）を選択できます。AnyConnect 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、Web 認証の実行時に AnyConnect クライアントが AnyConnect 組み込みブラウザではなくローカルブラウザを使用することを選択できます。この機能により、AnyConnect は WebAuthN およびその他の

SAMLベースのWeb認証オプション（シングルサインオン（SSO）、生体認証、または組み込みブラウザでは利用できないその他の拡張方法など）をサポートします。SAML外部ブラウザを使用するには、ASA リリース 9.17.1（CLI）、ASDM 7.17.1、または FDM 7.1 以降を使用して設定を実行する必要があります。

この機能を設定するには、次の関連ドキュメントを参照してください。

ASA コマンドリファレンス

anyconnect external-browser-pkg

external-browser

show webvpn anyconnect external-browser-pkg

Cisco ASA Series VPN ASDM Configuration Guide, 7.17.1

AnyConnect Connection Profile, Basic Attributes

AnyConnect VPN External Browser SAML Package

Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Release 7.1

Configure AAA for a Connection Profile

Cisco Firepower Management Center Device Configuration Guide, 7.1

Configure AAA Settings for Remote Access VPN

- （CSCvv92919）外部 SAML ID プロバイダーによる常時接続 VPN のサポート：相互運用性を許可するには、「Use Always-On VPN with External SAML Identity Provider」の説明に従って常時接続を設定する必要があります。
- （CSCvt99770）Windows での SAML 認証を使用した DNS ロードバランシングのサポート。
- Network Visibility Module コレクションの更新：フローの方向と追加のログインユーザーリスト
- （CSCvz99382）より低いバージョンが存在することを ADVERTISE が示したときに、Windows で SCCM を使用してネットワーク アクセス マネージャ モジュールを正常にアップグレードするための修正。
- （CSCvz77002）RPM/DEB インストーラの Linux サポート。「RPM/DEB インストーラ使用時の制限事項 （28 ページ）」を参照してください。

既知の問題

CSCwa22837：（ASA または Umbrella クラウドを介して）AnyConnect をアップグレードした後に断続的な acumbrellaagent クラッシュが見られる

CSCvz74755—Windows 11：Umbrella ダッシュボードに Windows 11 クライアントの OS バージョンが誤って「Windows 10」と表示される

CSCvz17505—Windows：acumbrella プラグインライブラリの .NET/CLR 例外が原因で Umbrella エージェントがクラッシュする

AnyConnect 4.10.03104 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、「AnyConnect 4.10.03104（70 ページ）」に記載されている不具合を修正します。

- OCSP チェック（Linux のみ）：この機能により、クライアントは Online Certificate Status Protocol（OCSP）レスポンダにリクエストを送信して OSCP 応答を解析し、リアルタイムで各証明書のステータスをクエリできます。この機能は、PEM ファイル証明書ストアでのみ機能します。ルート CA と Firefox NSS ストアの競合（Linux のみ）（29 ページ）を参照してください。
- 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。

既知の問題

CSCvy92621—posture-asa：AC Windows バージョンで HS 10.02067 を使用する Windows 11 ではなく Windows 10 が誤って表示される

CSCvy92676—Posture-ISE：Windows 11 OS が Windows 11 ではなく Windows 10 Professional として表示される

CSCvz74755—Windows 11：Umbrella ダッシュボードに Windows 11 クライアントの OS バージョンが誤って「Windows 10」と表示される

CSCvz74132—macOS 12：OS を beta7 にアップデートした後に acumbrellaagent のクラッシュが見られる

CSCvz17505—Windows：acumbrella プラグインライブラリの .NET/CLR 例外が原因で Umbrella エージェントがクラッシュする

AnyConnect 4.10.02086 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、「AnyConnect 4.10.02086（72 ページ）」に記載されている不具合を修正します。

- クライアント証明書ストア（AnyConnect プロファイルエディタ、設定：パート 1 と AnyConnect プロファイルエディタ、証明書登録）、関連する AnyConnect ローカル ポリシー プロファイルの追加、および複数の証明書認証か基本的な証明書認証による VPN アクセスを設定するためのオプションを含む、Linux の拡張機能。
- Web セキュリティモジュールの削除：https://www.cisco.com/c/en/us/products/security/cloud-web-security/eos-eol-notice-listing.html

- AnyConnect VPN と macOS Big Sur の VMware V5 との相互運用性（CSCvy10495）：macOS Big Sur ホストで実行されている AnyConnect VPN トンネルとの VMware V5 仮想マシンの接続は、少なくとも制限のあるローカル LAN スプリット除外トンネリングが VPN ヘッドエンドで有効になっている場合に可能です。詳細については、『Cisco AnyConnect セキュア モビリティ クライアント リリース 4.10 管理者ガイド』の「トラブルシューティング」の章に記載されている「VM ベースサブシステムの接続の問題」を参照してください。AnyConnect のインストール（またはバージョン 4.10.01075 以前からのアップグレード）中に V5 VM がアクティブになった場合、V5 VM のネットワーク接続を復元するには、AnyConnect のインストール後にリブートか V5 の再起動が必要です。その後の AnyConnect のアップグレードでは、リブートや再起動は必要ありません。

- Windows 7 の限定的な拡張サポートは、Microsoft とアクティブな Windows 7 の拡張サポート契約を結んでいるお客様に提供されます。シスコは Windows 7 で実質的な品質保証テストを実施しなくなりましたが、可能な限り問題は解決します。セキュリティ強化機能を利用するには、AnyConnect および Windows の最新バージョンにアップグレードすることを強く推奨します。

- ネイティブ macOS arm64 サポート：単一の macOS インストーラは、x86_64 と Apple Silicon（M1 チップ）の両方をネイティブで（Rosetta なしで）サポートします。これにより、OPSWAT コンプライアンスモジュールを含む、今後のすべてのバイナリはユニバーサルバイナリになります。そのため、4.3.1858.0 より前にリリースされた macOS 用の OPSWAT コンプライアンスモジュールでは、Apple シリコン（M1 チップ）はサポートされません。一方、OPSWAT コンプライアンスモジュール 4.3.1858.0 以降では、Intel（x86_64）デバイスと Apple シリコン（M1 チップ）デバイスの両方がサポートされます。Apple シリコン（M1 チップ）のサポートにおけるこのような動的な導入に伴い、AnyConnect 4.10.02086 以降（と ISE ポスチャか HostScan のいずれか）を使用する macOS エンドポイントでも、ポスチャ コンプライアンス モジュールを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 ISE ポスチャ コンプライアンス ライブラリの最小バージョン	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	macOS：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バージョンが常に推奨されます。	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	macOS：4.3.1935.4353 以降が必要です。	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。

（注） 上記の arm64 サポートは、ISE 3.1 リリースとは無関係です。

- ISE ポスチャモジュールの Linux サポート。
- AnyConnect ローカルポリシー設定内の ISE に対する信頼検証の拡張。スクリプト修復の場合、ISE の信頼を確立するために、ISE 証明書チェーン内の証明書の SHA256 フィンガープリントを設定することが必須となっています。管理ガイドの「Local Policy Preferences」を参照してください。
- ISE ポスチャの詳細と Cisco Secure Client の詳細に、スクリプト修復メッセージが追加されました。

既知の問題

CSCvz17505—Windows：acumbrella プラグインライブラリの .NET/CLR 例外が原因で Umbrella エージェントがクラッシュする

AnyConnect 4.10.01075 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、「AnyConnect 4.10.01075 （76 ページ）」に記載されている不具合を修正します。

- スプリット除外トンネリングのスプリット DNS を追加（CSCuq893）：スプリット除外トンネリングのスプリット DNS が設定されている場合、特定の DNS クエリは VPN トンネルの外部でパブリック DNS サーバーに送信されます。他のすべての DNS クエリは、VPN DNS サーバにトンネルされます。
- VM ベースサブシステムとの相互運用性のサポートを追加（CSCvw81982）：Windows Subsystem for Linux 2（WSL2）には、Windows 10 ホストでアクティブになっている AnyConnect VPN との接続の問題がありました。シスコでは、ローカル LAN ワイルドカードスプリット除外トンネリングのサポートを強化する（特に仮想アダプタのサブネットにローカル LAN スプリット除外を制限できるようにする）ことにより、この問題を解決しました。詳細については、『Cisco AnyConnect セキュア モビリティ クライアント リリース 4.10 管理者ガイド』の「トラブルシューティング」の章に記載されている「VM ベースサブシステムの接続の問題」を参照してください。

AnyConnect 4.10.00093 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 4.10.00093 （79 ページ）に記載されている不具合を解決します。

- macOS における強化されたキャプティブポータル修復のサポート。
- ローカルプラットフォームのセキュリティ問題に対処するためのダウンローダーのアーキテクチャの改善。
- ローカルポリシーでスクリプト、ヘルプ、リソース、またはローカリゼーションのアップデートを個別に許可または禁止する機能（以前は、[ソフトウェアアップデートの許可（Allow Software Updates）] の一部）。

- Cisco SSL の変更：TLS のみの EMS の有効化、および DTLS の EMS の無効化。
- 古いバージョンを削除するための、オペレーティングシステムのサポートの変更。「AnyConnect でサポートされているオペレーティングシステム （20 ページ）」を参照してください。
- Linux 要件の改訂（Linux ビルドツールチェーンまたは GTK の移行による改訂）。「AnyConnect における Linux のサポート （24 ページ）」を参照してください。
- CSCvx78941：（Windows のみ）製品コード署名証明書が、VeriSign ではなく、DigiCert によって発行された新しい証明書で更新されました。コード署名が OS によって検証および信頼されるようにするには、オペレーティングシステムの信頼できるルート証明書のリストにルート証明書がインストールされている必要があります。Windows の信頼できるルート証明書の更新が無効になっている場合、AnyConnect のインストールまたはアップグレードが失敗する可能性があります。必要に応じて、CN = DigiCert Assured ID Root CA ルート証明書を、DigiCert からダウンロードして Windows の信頼できるルートストアにインストールします（https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt.pem).）。

AnyConnect HostScan Engine Update 4.10.08029 の新機能

AnyConnect HostScan 4.10.08029 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ており、これによって「HostScan 4.10.08029 （81 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.08025 の新機能

AnyConnect HostScan 4.10.08025 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ており、これによって「HostScan 4.10.08025 （82 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.07073 の新機能

AnyConnect HostScan 4.10.07073 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ています。

AnyConnect HostScan Engine Update 4.10.07061 の新機能

HostScan 4.10.07061 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ており、これによって「HostScan 4.10.07061 （83 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.06090 の新機能

HostScan 4.10.06090 には、Windows、macOS、Linux 用のOPSWAT エンジンバージョンへの更新が含まれています。

AnyConnect HostScan Engine Update 4.10.06083 の新機能

AnyConnect HostScan 4.10.06083 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ており、これによって「HostScan 4.10.06083 （85 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.06081 の新機能

AnyConnect HostScan 4.10.06081 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ており、これによって「HostScan 4.10.06081 （85 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.05111 の新機能

AnyConnect HostScan 4.10.05111 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を提供し、「HostScan 4.10.05111 （86 ページ）」に記載されている不具合を修正します。

AnyConnect HostScan Engine Update 4.10.05095 の新機能

AnyConnect HostScan 4.10.05095 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を提供します。

AnyConnect HostScan Engine Update 4.10.05085 の新機能

AnyConnect HostScan 4.10.05085 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ており、これによって「HostScan 4.10.05085 （87 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.04071 の新機能

AnyConnect HostScan 4.10.04071 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ており、これによって「HostScan 4.10.04071 （87 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.04065 の新機能

AnyConnect HostScan 4.10.04065 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ており、これによって「HostScan 4.10.04065 （88 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.03104 の新機能

AnyConnect HostScan 4.10.03104 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ており、これによって「HostScan 4.10.03104 （88 ページ）」に記載されている不具合が修正されます。

AnyConnect HostScan Engine Update 4.10.02089 の新機能

AnyConnect HostScan 4.10.02089 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ており、これによって「HostScan 4.10.02089 （89 ページ）」に記載されている不具合が修正されます。このリリースは、HostScanモジュール専用です。

AnyConnect HostScan Engine Update 4.10.02086 の新機能

AnyConnect HostScan 4.10.02086 は、「HostScan 4.10.02086 （89 ページ）」に記載されている不具合を修正します。

AnyConnect HostScan Engine Update 4.10.01094 の新機能

AnyConnect HostScan 4.10.01094 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ており、これによって「HostScan 4.10.01094 （90 ページ）」に記載されている不具合が修正されます。このリリースは、HostScanモジュール専用です。

AnyConnect HostScan Engine Update 4.10.01075 の新機能

AnyConnect HostScan 4.10.01075 は HostScan モジュールの更新が含まれており、HostScan 4.10.01075 （90 ページ）に記載されている不具合を解決します。

AnyConnect HostScan Engine Update 4.10.00093 の新機能

AnyConnect HostScan 4.10.00093 は HostScan モジュールの更新が含まれており、HostScan 4.10.00093 （91 ページ）に記載されている不具合を解決します。

VPN のインストールまたはアップグレードに影響を与える可能性がある、コード署名証明書に対する重要な変更については、「AnyConnect 4.10.00093 の新機能 （10 ページ）」を参照してください。

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、『AnyConnect 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。

AnyConnect 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。AnyConnect 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。

SAML の要件

SAML を使用する場合は、以下のガイドラインに従ってください。

- AnyConnect VPN SAML 組み込みブラウザの場合

  Safari アップデート 14.1.2（以降）が必要：さまざまな動作を解決する、最新の Webkit バージョンが含まれています。

- AnyConnect VPN SAML 外部ブラウザ

  AnyConnect リリース 4.10.04065（以降）

  ASA 9.17.1/ASDM 7/7/1（以降）

  FDM 7.1（以降）

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 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。
- AnyConnect 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 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 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。

AnyConnect 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

- 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。
- 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
  - AnyConnect 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）
  - AnyConnect 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。
- 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。

Cisco Secure Firewall ASA のメモリ要件

⚠

注意 AnyConnect 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、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。

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 AnyConnect 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。

HostScan

AnyConnect 4.10.x クライアントは、Secure Firewall Posture 5.0（またはそれ以降）または HostScan 4.10.x を使用する必要があります。

（注） AnyConnect 4.10.x 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。したがって、4.10.x より前のバージョンの HostScan を使用している場合は、Secure Firewall Posture 5.0.x（またはそれ以降）または HostScan 4.10.x にアップグレードする必要があります。CCO でダウンロード可能な最新バージョンへのアップグレードを常にお勧めします。

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、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 モジュールにより、AnyConnect 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 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 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 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 HostScan モジュール（以前にインストールされている場合）と Cisco Secure Firewall 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ような動的な導入に伴い、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 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。

Start Before Login（SBL）と Secure Firewall Posture 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 Posture の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。

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。

HostScan 4.3.x 終了日の通知

HostScan 4.3.x のサポート終了（EOS）が 2018 年 12 月 31 日に発表されました。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。

ISE ポスチャ準拠モジュール

（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。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 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。

AnyConnect 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 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」[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。

AnyConnect でサポートされてい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
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	×	対応
	対応	×	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 11	対応	×	対応	×	対応	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
macOS 14 Sonoma、macOS 13 Ventura、macOS 12 Monterey、および macOS 11 Big Sur（すべて 64 ビット）	対応	×	対応	対応	対応	対応	対応	対応	対応

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

AnyConnect 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、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 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 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、AnyConnect 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。

- 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 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 AnyConnect 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。

AnyConnect 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。
- Snap バージョンの Firefox は、Linux 上の AnyConnect ではサポートされません。
- 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
- 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（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）
- libnm（libnm.so または libnm-glib.so）：Network Visibility Module を使用する場合にのみ必要

AnyConnect における macOS のサポート

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 AnyConnect 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。
- macOS 10.15 でのアクセス制御の導入により、Cisco Secure Firewall Posture（旧 HostScan）または ISE ポスチャがエンドポイントでスキャンを実行しているときに、追加のポップアップが表示される場合があります。アクセスしてスキャンできるファイルとフォルダを承認する必要があります。

AnyConnect 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, AnyConnect セキュア モビリティ クライアント』[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 AnyConnect セキュア モビリティ クライアント』[英語] 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 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 AnyConnect を展開して VPN と HostScan 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。『AnyConnect 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、『AnyConnect セキュア モビリティ クライアント Features, Licenses, and OSs』[英語] 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 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。AnyConnect 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：AnyConnect 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、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 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、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。
- 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。

- AnyConnect 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 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、Cisco Secure Firewall 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 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、AnyConnect 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。

AnyConnect サポートポリシー

シスコでは、最新の バージョン 4.10 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 バージョン 4.10 のリリースバージョンを実行するアクティブな AnyConnect バージョン 4.10 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 バージョン 4.10 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

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。

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。

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 AnyConnect セキュア モビリティ クライアント 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 12.x での DNS（名前解決）が失敗することがある

macOS 12.x で AnyConnect 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 AnyConnect 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。

暗号化された DNS の影響とその影響の軽減

暗号化されたドメインネームシステム（DNS）の解決は、AnyConnect セキュア モビリティ クライアント の機能に影響します。具体的に言うと、暗号化された DNS を介して解決される FQDN をターゲットとするネットワークフローは、AnyConnect セキュア モビリティ クライアント の次の機能により、回避されるか、適切に処理されません：Cisco Umbrella DNS の保護、Cisco Umbrella Web の保護（名前ベースのリダイレクトルールが使用されている場合）、VPN（ダイナミック スプリット トンネリングと名前ベースの例外のある常時接続）、Network Visibility（ピア FQDN のレポート）。このような影響を軽減するには、AnyConnect セキュア モビリティ クライアント ユーザーに関連するブラウザ設定で暗号化された DNS を無効にする必要があります。

追加の軽減策として、AnyConnect セキュア モビリティ クライアント は、ローカルポリシー設定を介した Windows DNS クライアントの DNS over HTTPS（DoH）名前解決（**DNS over HTTP（DoH）名前解決の設定**（[コンピュータの設定（Computer Configuration）] > [管理テンプレート（Administrative Templates）] > [ネットワーク（Network）] > [DNSクライアント（DNS Client）]））を禁止します。この変更は、Windows 11 以降のバージョンに該当するものであり、VPN、Cisco Umbrella ローミングセキュリティ、または Network Visibility のいずれかのモジュールがアクティブなときに適用されます。（ドメイン GPO 設定などの）優先順位の高い競合設定が検出された場合、AnyConnect セキュア モビリティ クライアント はこのポリシー設定を変更しません。

RPM/DEB インストーラ使用時の制限事項

RPM/DEB インストーラを使用して、スクリプトによってインストールされたバージョンからアップグレードする場合、次の制限があります。

- ヘッドエンドからの自動クライアント更新はサポートされていません。システムパッケージ マネージャを使用して、アウトオブバンドで更新を行う必要があります。

- RPM および DEB インストーラでサポートされる AnyConnect モジュールは、VPN と DART のみです。
- RPM または DEB インストーラの使用に切り替える前に、（すべてのモジュールを含む）現在の既存の AnyConnect をアンインストールする必要があります。既知の問題の回避策については、CSCwa16755 を参照してください。
- スクリプトインストーラを使用して、既存の RPM または DEB のインストールを更新することはできません。

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、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 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、AnyConnect 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. AnyConnect 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（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 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、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のに必要な更新を行うまで、AnyConnect 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 HostScan と システムスキャン 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。

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 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。

HostScan 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 HostScan 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 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 [英語] を参照してください。

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 AnyConnect 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 HostScan 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. AnyConnect セキュア モビリティ クライアント 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

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（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/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 AnyConnect 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、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

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 AnyConnect を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 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 AnyConnect 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 AnyConnect のアクセスを制限するように AnyConnect 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。
- 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、[AnyConnect Umbrellaローミ

ングセキュリティモジュール（AnyConnect Umbrella Roaming Security Module）] セクションの [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

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。

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 AnyConnect 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）。

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、期待どおりの結果を得るために AnyConnect 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

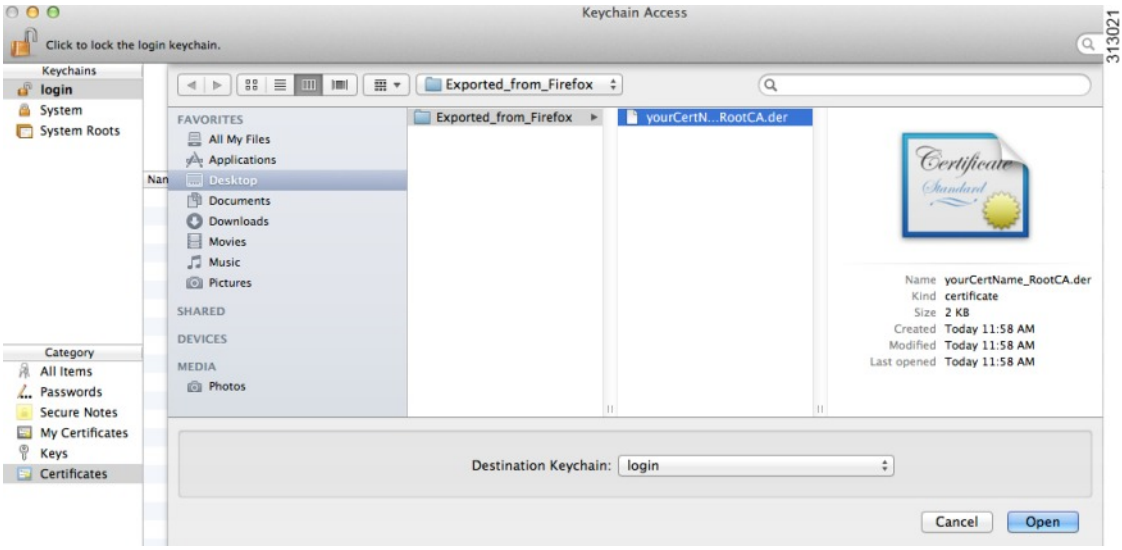
macOS 上の Firefox 証明書ストアは、任意のユーザーによるストアの内容の変更を許可するアクセス権を使用して保存されます。これにより、未認可のユーザーまたはプロセスが不正な CA を信頼されたルートストアに追加することが可能になります。AnyConnect は、サーバー検証またはクライアント証明書に Firefox ストアを使用しなくなりました。

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。一例として、AnyConnect 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. 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。

多くの場合、AnyConnect 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。

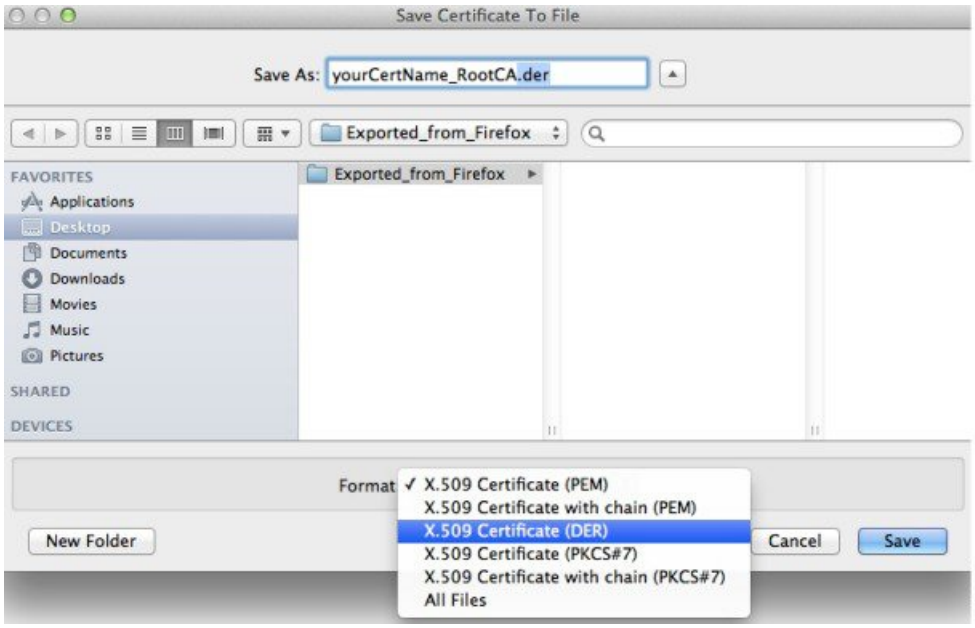


（注） 複数の AnyConnect 証明書または秘密キー（あるいはその両方）が使用される場合や必要な場合は、証明書ごとに上記のプロセスを繰り返してください。

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限り、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

Java 7 では、AnyConnect と HostScan 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 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

AnyConnect 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、AnyConnect 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、

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。

テザーデバイス上の AnyConnect

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 AnyConnect で検証する必要があります。

AnyConnect スマートカードのサポート

AnyConnect 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） 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 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、AnyConnect 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 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

Cisco Secure Firewall 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、Cisco Secure Firewall ASA に同じバージョンか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、Cisco Secure Firewall ASA で同じバージョンか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。

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、AnyConnect セキュア モビリティ クライアント 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 のモジュールかパッケージをインストールしたら、AnyConnect のインストールフォルダを許可するか、AnyConnect 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

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 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

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、AnyConnect 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）。

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。

AnyConnect ホストが（AnyConnect 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、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 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 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。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
```

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、AnyConnect 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 AnyConnect が不安定になる可能性があります。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 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。

AnyConnect 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。

AnyConnect 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。

HostScan 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。HostScan 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。

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。

AnyConnect セキュア モビリティ クライアント 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 セキュア モビリティ クライアントには、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、AnyConnect 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 4.10.08029

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
CSCwh73937	core	ENH：CNAME DNS 応答に基づいてダイナミックスプリット除外をサポートする macOS AnyConnect
CSCwi69374	core	macOS：PAC ファイルプロキシ設定を使用した AnyConnect ブラウザを介してキャプティブポータルの修復ができない
CSCwi69388	core	macOS：AnyConnect ブラウザがキャプティブポータルの修復に断続的にのみ使用される
CSCwd21905	posture-ise	値が設定されていない場合に、AutoDART がバンドルを生成する

AnyConnect 4.10.08025

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
CSCwc58452	core	Windows 用の Cisco AnyConnect セキュア モビリティ クライアントの情報漏洩の脆弱性
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

識別子	コンポーネント	タイトル
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
CSCwf67833	core	（Windows のみ）エラー：VPN クライアントがプライベート側のプロキシ設定を行えない
CSCwh57935	core	AnyConnect がコア更新の外部でクライアント ダウンローダー ポップアップを起動する
CSCwi07144	core	zlib の脆弱性：複数のバージョン
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
CSCur83728	nam	CAC カードが取り外されたときに AnyConnect NAM が EAPol ログオフを送信しない
CSCvq05530	nam	ENH：NAM：管理フレーム保護（PMF）のサポートを追加
CSCwb94282	nam	NAM が WPA2+WPA3/エンタープライズ SSID に接続できない
CSCwd26172	nam	AnyConnect NAM で Unicode 文字の SSID の表示/接続ができない
CSCwf08769	nam	NAM：Windows 10 および Windows 11 21H2 での Windows RnR の無効化
CSCwh45972	nam	PE：SSID に単語間のスペースがある場合、NAM プロファイルを保存できない

識別子	コンポーネント	タイトル
CSCwi27062	nam	NAM が Eero メッシュ AP に接続できない
CSCwi27137	nam	NAM がデフォルトの PMF IGTK 暗号を認識しない
CSCwb30765	opswat-ise	ENH：Trend Micro の Cyber Eye Security Agent をポスチャ条件に追加
CSCwb91318	opswat-ise	Sophos Endpoint Agent および Sophos Cloud Agent 2.20.13 が CM 4.3.2815 の定義チェックに失敗する
CSCwc10117	opswat-ise	AnyConnect が Check Point Endpoint Security 86.25 の定義を検出しない
CSCwc22358	opswat-ise	ENH：Windows：パッチ管理の最新条件の失敗に関するエラーコードの追加
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
CSCwe11874	opswat-ise	ENH：ISE ポスチャが Kaspersky Endpoint Security 12.x をサポートしない
CSCwe33823	opswat-ise	ISE コンプライアンスモジュールが McAfee endpoint Disk Encryption バージョン 7.4.x を検出できない
CSCwh70413	posture-ise	ENH：ISE ポスチャ：バージョン 2171 および 2172 の Apple XProtect のサポート
CSCwi03257	posture-ise	Symantec WSS が接続されると macOS 上の ISE ポスチャ IPC が破損し、ポスチャ障害が発生す

識別子	コンポーネント	タイトル
CSCwd81612	profile-editor	SSID が PE の UNICODE 文字である場合、NAMプロファイルを保存できない
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
CSCwf37767	swg	カスタムフラグファイルの存在に基づく SWG最大デバッグログの有効化
CSCwd68113	vpn	正しいパスワードを入力しても AAA 認証が失敗する
CSCwe45817	vpn	HTTP リダイレクトのエンコードされていない埋め込み URL により、キャプティブポータルの検出が妨げられる
CSCwe49687	vpn	macOS 12 および 13：CP 修復前の遅延が起こる可能性、AnyConnect ブラウザが使用されない
CSCwe83519	vpn	DTLS MTU DPD の設定が早すぎるため、ヘッドエンドによってドロップされることがある
CSCwf21381	vpn	Cisco Secure Client のサービス妨害（DoS）の脆弱性
CSCwf33688	vpn	新しく有効になったネットワーク インターフェイスで、常にオンのフィルタリングの適用がわずかに遅延する
CSCwf92553	vpn	Cisco Secure Client のサービス妨害（DoS）の脆弱性
CSCwh51369	vpn	SBL が再接続中にプロキシ設定を復元できない

識別子	コンポーネント	タイトル
CSCwh75976	vpn	v117.x へのアップグレード後、キャプティブポータルが WebView2 ベースの組み込みブラウザにロードされない
CSCwf94247	web	SAML について、外部ブラウザで QR コードが正しく表示されないことがある

AnyConnect 4.10.07073

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
CSCwh02451	core	スマートカードからのクライアント証明書認証が失敗する
CSCwh06886	nam	NAM が、カーリーアポストロフィが含まれている SSID に接続できない
CSCwd21905	posture-ise	値が設定されていない場合に、AutoDART がバンドルを生成する

AnyConnect 4.10.07062

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

AnyConnect 4.10.07061

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
CSCwc92975	cli	VPN CLI が切断状態でスタックする
CSCvu77796	core	CIAM：libxml 2.9.10
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
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
CSCwd74058	core	libxml2 2.9.10 での脆弱性
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

識別子	コンポーネント	タイトル
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
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
CSCwc64861	gui	SAML 認証が成功した後の AnyConnect GUI メッセージの更新
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
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
CSCwd90898	nam	WPA3 OWE および SAE ネットワークのサポートを追加
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 のネットワーク GUID をすべて大文字にする必要がある
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

識別子	コンポーネント	タイトル
CSCvw43299	opswat-ise	ISE ポスチャモジュールが macOS の SEP 14.3 ビルド 82 のインストールチェックを検出しない
CSCvx19454	opswat-ise	[ENH] Sophos Home 10.x のサポートを追加
CSCvz20268	opswat-ise	ENH：ISE ポスチャが Google Chrome バージョン 89 をサポートしていない
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
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
CSCwb20579	opswat-ise	アンインストール修復について、ISE ポスチャが Docker Desktop アプリケーションをサポート
CSCwc76493	opswat-ise	Windows 11：パッチ管理チェックの失敗
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
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
CSCwe11588	opswat-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
CSCwe70047	posture-ise	MacOS：ISE ポスチャが FileValue の「状態」（オン/オフ）を正確に検出しない

識別子	コンポーネント	タイトル
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
CSCwe22036	swg	noNetwork、Trusted Network、VPNの場合のみSWG保護をバックオフする
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
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
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
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
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
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
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
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
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
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
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）
CSCwd17651	vpn	管理トンネルが 4 ～ 7 日後にダウンしてから、切断される
CSCwd40263	vpn	プロキシ設定がどこにも適用されない
CSCwd82040	vpn	Linux/Mac/iOS：証明書認証を使用した TLS1.3 ヘッドエンドに接続している TLS1.2 クライアントがネゴシエーションに失敗することがある

AnyConnect 4.10.06090

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
CSCwd34655	opswat-ise	Windows：Cortex XDR での定義チェックの失敗
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
CSCwe05151	posture-ise	EDR 製品の定義情報と RTP 状態の取得中のインターネットチェックのスキップ
CSCwd83114	umbrella	dcp2 crash fix
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
CSCwd82040	vpn	Linux/macOS：証明書認証を使用した TLS 1.3 ヘッドエンドに接続している TLS 1.2 クライアントがネゴシエーションに失敗することがある

AnyConnect 4.10.06079

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
CSCwb41421	core	CiscoSSL CVE-2022-0778
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
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
CSCwa94606	core	AnyConnect は ACIDEX でヌルの MAC アドレスを処理する必要がある
CSCwb48021	core	AnyConnect：Linux/KVM：IPtables でドロップされた VM 宛てのトラフィック
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
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
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
CSCvz70357	fireamp	コネクタのバイナリコードを検証するための AMP イネーブラ

識別子	コンポーネント	タイトル
CSCwc13889	fireamp	アンインストールがエラーコード ValidateCodeSign failed with 4 で失敗する
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
CSCvo07690	nam	ENH：キャプティブポータルが検出されると Web ブラウザを自動起動するための NAM サポートを追加
CSCvx54528	nam	AnyConnect NAM は、バージョン 4.9 へのアップグレード時に「ログオン前に接続を許可」を自動的に有効にする
CSCwb14670	posture-ise	ISE は中国語版の Windows OS をサポートしていない
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
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
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
CSCwc61270	swg	信頼済みネットワークで Web 保護の状態が適切に更新されない

識別子	コンポーネント	タイトル
CSCwa91811	umbrella	UAC クライアントは非常に長いドメイン名を解決できない
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
CSCvx62066	vpn	デバイスタイプに（&）文字が含まれている場合、AnyConnect が ACIDEX 属性を取得しない
CSCwb25527	vpn	macOS：一致の分割除外にもかかわらず、VPN 時に VPN 前の TCP 接続のトラフィックがブロックされる
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
CSCwd14401	vpn	Windows Always on：VPN の切断後に VPN が接続できず（DNS エラー）、接続に失敗すると予期される

識別子	コンポーネント	タイトル
CSCwa44949	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エラー
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

AnyConnect 4.10.05111

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
CSCwc03545	core	macOS 12.4：iPhone のホットスポットに切り替えた後、または DNS サーバーに IPv6 リンクローカルがある場合に DNS が停止する
CSCwb89172	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
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
CSCwb91574	vpn	WebView 2 の AllowSingleSignOnUsingOSPrimaryAccount のデフォルト設定を変更

AnyConnect 4.10.05095

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
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かった
CSCvy78997	web	AnyConnect のログからロギングエントリ「新しいウィンドウはまだサポートされていません（New window not yet supported）」を削除する必要がある

AnyConnect 4.10.05085

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
CSCwa59261	core	Big Sur（macOS 11）の AirDrop は、Split Exclude Tunnel タイプでは機能しない
CSCwa77222	core	スプリットトンネリングと Zentera セキュリティソフトウェアの相互運用性
CSCvz50397	nam	ネットワーク アクセス マネージャ：NAM プロファイルで FIPS モードを有効にした後に認証に失敗した
CSCvz69614	nam	ユーザー定義ネットワークのスクリプトを編集できない
CSCwa85342	nvm	TLS 1.3 で TND 解決が行われると、Network Visibility Module のクラッシュが見られる

識別子	コンポーネント	タイトル
CSCvy88561	opswat-ise	FireEye セキュリティ エージェント バージョン 33.x が最新の ISE ポスチャの更新に含まれていない
CSCvz75848	opswat-ise	AVG AntiVirus 20.x の macOS バージョンに対する ISE コンプライアンスモジュール v4.3.1981.4353 のサポート
CSCvz75853	opswat-ise	Avast Mac Security 15.x の macOS バージョンに対する ISE コンプライアンスモジュール 4.3.1981.4353 のサポート
CSCvz97883	opswat-ise	Windows：Cisco AMP インストールチェックの失敗
CSCwa06784	opswat-ise	Windows：パッチ管理チェックの失敗
CSCwa07578	opswat-ise	macOS：コンプライアンスモジュール 4.3.2009.4353：Symantec Endpoint Protection：間違ったバージョン
CSCwa23013	opswat-ise	Checkpoint Endpoint Security 85.x が AV/AM の条件にリストされていない
CSCwa64826	opswat-ise	Check Point Endpoint Security 85.x および 86.x は未サポート
CSCvz74132	umbrella	macOS：OS を 12 beta7 にアップデートした後に acumbrellaagent.crash が表示される
CSCvy79511	vpn	プロファイルで AutoUpdate が「false」に設定されていても、AnyConnect 4.10 が引き続き更新される
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

識別子	コンポーネント	タイトル
CSCvz71309	vpn	ダイナミック スプリット トンネリングが有効になっている VPN セッション中の BSOD（DPC_WATCHDOG_VIOLATION）
CSCwa62414	vpn	Windows 10：スプリットトンネリングと tunnel-all-DNS が有効になっていると、Active Directory のブラウジングが非常に遅くなる
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
CSCwb06945	vpn	Secure TND プローブが Poly1305 暗号をネゴシエートすると、VPN エージェントがクラッシュする

AnyConnect 4.10.04071

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
CSCvz90541	nam	AnyConnect NAM 4.9.x/4.10.x は ISE 3.1 では認証に失敗するが、以前の ISE バージョンでは成功する
CSCvz17505	umbrella	Windows：acumbrella プラグインライブラリの .NET/CLR 例外が原因で Umbrella エージェントがクラッシュする

AnyConnect 4.10.04065

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
CSCvt36114	core	ENH：SAML の外部ブラウザ サポートの復活 [シングルサインオン]
CSCvt99770	core	ENH：Windows での SAML 認証を使用した AnyConnect による DNS ロードバランシング/ラウンドロビンのサポートの脆弱性
CSCvw60190	core	ENH：SBL を使用すると AnyConnect UI に管理トンネルの HostName エントリが表示される
CSCvy23801	core	macOS 11：VPN エージェントが予期せずクラッシュする
CSCvz25236	core	Split-DNS または tunnel-all-DNS が有効になっていると、デュアルスタック Windows DNS 解決が失敗する
CSCvz67203	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
CSCvz67532	download_install	SG 名を解決できず、プロキシ経由で接続する必要がある場合、AnyConnect 4.10 ダウンローダーが失敗する
CSCvz99382	download_install	SCCM を使用して展開すると、NAM インストーラの ADVERTISE 修正が機能しない

識別子	コンポーネント	タイトル
CSCvz55627	opswat-ise	Cybereason AM 条件で ANY を選択すると、ISEにリストされていない場合にバージョン 21.x が検出される
CSCvy92443	posture-ise	セキュリティ製品の下に AM 定義のバージョンと日付の情報が表示されない
CSCvz79420	posture-ise	接続済みスタンバイイベントを終了するマシンでポスチャが検出されない
CSCvz37687	swg	AnyConnect SWG モジュールが有効になっているキャプティブポータル経由でホットスポットに接続できない
CSCvz74132	umbrella	macOS：OS を 12 beta7 にアップデートした後に acumbrellaagent.crash が表示される
CSCvm51303	vpn	ENH：AnyConnect クライアントの設定ウィンドウのスクロールバー
CSCvp09954	vpn	常時接続では、先頭の IP アドレスへのアクセスを重要なプロセスのみに制限する必要がある
CSCvv92919	vpn	ENH：常時接続のフェールクローズが有効になっている SAML 認証（外部 IdP）
CSCvz75859	vpn	ゲートウェイの FQDN が常時接続ホストの例外として追加されている場合に VPN 接続が失敗する

AnyConnect 4.10.03104

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
CSCvy99682	api	ENH：MCA は SBL 中にマシンと PIV ストアから順番に証明書を送信する必要がある
CSCvw43009	certificate	クライアントのアップグレード後に AnyConnect 4.9 の IKEv2 セッションでサーバー証明書の検証が失敗する
CSCvz22856	certificate	ENH：暗号化プロバイダーからサポート対象の sig が提供されていない場合は、AnyConnect で cURL に SHA-256 と SHA-1 を設定する必要がある
CSCvw51951	core	macOSAnyConnect クラッシュ - 例外タイプ：EXC_CRASH（SIGABRT）
CSCvw52376	core	macOS：IPsec トンネルの終了中に vpnagentd が CPU を 100% 使用し、過剰なエラーログが記録される
CSCvx36273	core	ENH：拡張 DSI/DSE の両方に対する例外ドメイン検証を導入
CSCvw79615	download_install	ENH：Windows でサポートされていない MSI ADVERTISE オプションの AnyConnect でのアンインストールを改善
CSCvz27629	download_install	AnyConnect ダウンローダー IPC の問題

識別子	コンポーネント	タイトル
CSCvz67532	download_install	SG名を解決できず、プロキシ経由で接続する必要がある場合、4.10 ダウンローダーが失敗する
CSCvw50627	nam	NAM が AnyConnect 仮想アダプタにバインドしている
CSCvx65595	nvm	NVM は DNS 接続テストとして www.gstatic.com を利用すべきではない
CSCvz08505	opswat-ise	ENH：Bitdefender 9.X Antivirus for macOS
CSCvz11091	umbrella	macOS 12：IPv4 ネットワークで acumbrellaagent のクラッシュが断続的に見られる
CSCvy69858	vpn	スプリット除外トンネルを使用している場合、名前解決がパブリックインターフェイス DNS サーバーにフェールバックしない
CSCvz01007	vpn	macOS：ユーザーがダウンローダーログのキャンセルを選択すると、ASA のアップグレード中に vpndownloader がクラッシュする
CSCvz16781	vpn	Linux：AnyConnect が「Internet」ではなく「Other」フォルダに配置される
CSCvz37517	vpn	クライアントに顧客属性がプッシュされていない場合、VPN トンネルの最適化が誤って無効化される
CSCvz46724	vpn	Secure TND：信頼できるネットワーク間での移行時に信頼できないネットワークが誤って検出される

識別子	コンポーネント	タイトル
CSCvz55373	vpn	「SSLエンジンでエラーが発生しました（SSL engine encountered an error）」と表示され、VPN 接続の試行がランダムに失敗する

AnyConnect 4.10.02086

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
CSCvy60749	api	ENH：マシンストアとスマートカードからの証明書を使用した SBL 中の MCA に対する AnyConnect のサポート
CSCvu42428	core	sqlite3 3.28.0 の複数の脆弱性
CSCvx65653	core	AnyConnect プロファイルエディタ - 証明書の登録 - 修飾子 GEN および DN - スキーマの検証に失敗
CSCvx89290	core	CIAM：sqlite 3.29.0
CSCvy23333	core	macOS 11：リンクローカル リゾルバ アドレスによって CPU が占有され、DNS が失敗する
CSCvy99119	core	macOS 12：IPv4 接続なしで VPN 接続が失敗する
CSCvy99325	core	macOS 12：ホストファイルエントリにかかわらず、VPN エージェントが「DNS 接続なし」と誤って報告する
CSCvn07053	nam	Windows でランダム MAC アドレスが有効になっていると NAM が SSID に接続できない

識別子	コンポーネント	タイトル
CSCvy59155	nam	NAM DART ファイルに acnamim ドライバのエラーが表示される
CSCvy10479	nvm	nvzFlowLoggedInUser でシステムプロセスが「none」になっている
CSCvu06648	opswat-ise	OPSWAT モジュールが実際のデータベースのリリース日 KES 11.3 を読み取れない
CSCvv34965	opswat-ise	Kaspersky Security Center 12 のサポート
CSCvv96231	opswat-ise	Trend Micro Apex One Security Agent 16.x（Windows プラットフォーム）のサポート
CSCvw81617	opswat-ise	ENH：ISE ポスチャに ESET Endpoint Antivirus バージョン 8 のサポートを含める
CSCvw99789	opswat-ise	MalwareBytes 定義チェックで 0 を返す source_time と last_update
CSCvx48049	opswat-ise	コンプライアンス モジュール バージョン 4.3.1466.4353 を使用しているユーザーの JAMF インストール状態が失敗になっている
CSCvx76435	opswat-ise	ISE ポスチャの Bitlocker 状態がバージョンを検出していない
CSCvx75464	opswat-ise	Trend Micro Apex One（macOS）3.x の定義チェックが失敗する
CSCvy14274	opswat-ise	FireEye エンドポイントエージェントの GetDefinitionState がスタックする：Windows の CM 4.3.1614.6145

識別子	コンポーネント	タイトル
CSCvy18948	opswat-ise	Windows：CrowdStrike Falcon の定義チェックの遅延
CSCvy30728	opswat-ise	KES 21.3.10.394 の Opswat サポート
CSCvy37094	opswat-ise	HostScan での ESET AM アクティブスキャン保護の問題
CSCvy37121	opswat-ise	Cybereason ActiveProbe の定義日として現在の日付/時刻を返す HostScan 4.9.06046
CSCvy51930	opswat-ise	Windows を管理する Manage Engine Manager Plus をサポートするために CM のポスチャを更新
CSCvw60979	posture-ise	ENH：メッセージ変更要求「お使いのネットワークは Cisco NAC エージェントを使用するように設定されています（Your network is configured to use Cisco NAC Agent）」
CSCvy42987	posture-ise	macOS エンドポイント用の CMバージョンのダンロードが必要
CSCvy44614	posture-ise	機密性の高いログを aciseagent の暗号化されたログに移動
CSCvy38455	profile-editor-wer	AnyConnect ローカルポリシーエディタ 4.10 で「Restrict Server Cert Store」パラメータが表示されない
CSCvz11091	umbrella	macOS 12：IPv6 カスタムリゾルバを使用すると、IPv4 ネットワークで acumbrellaagent のクラッシュが断続的に見られる

識別子	コンポーネント	タイトル
CSCvv74971	vpn	AnyConnect モビリティクライアントを使用して Windows ホストファイルにエントリを追加することが可能
CSCvx92746	vpn	昇格されたプライマリ SG アドレスに到達できない場合、セカンダリ SG アドレスが到達可能になってもフェールオーバーは行われない
CSCvy10495	vpn	macOS 11：VMware ゲストがホストで実行されている VPN とのネットワーク接続を失う
CSCvy24725	vpn	AnyConnect クライアントが [接続を最適化しています...（Optimizing connection...）] または [接続解除中（Disconnecting）] 状態のままになる
CSCvy32808	vpn	AnyConnect の通知ポップアップが 6K モニターの間違った場所に表示される
CSCvy34972	vpn	LocalLAN スプリット除外にかかわらず、AnyConnect のルート修正によって新しい仮想 if. サブネットルートが削除される
CSCvy60649	vpn	WinINet プロキシオプションはユーザースペースから設定する必要がある
CSCvy86968	vpn	macOS 12 ベータ版：IPv4 LocalLAN スプリット除外で VPN 接続が失敗する
CSCvt10982	web	ENH：（Windows プラットフォーム）複数の Windows「ポップアップ」に対する AnyConnect 組み込みブラウザのサポート

AnyConnect 4.10.01075

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
CSCvw81982	core	ENH：Windows 10 VPN トンネルで WSL（Linux 2 用 Windows サブシステム）のトラフィックをキャプチャする必要がある
CSCvx31341	core	macOS 11：アップグレード後に DST 対応ヘッドエンドへの VPN 接続が「DNS コンポーネント」エラーで失敗する
CSCvx58220	core	AnyConnect 管理 VPN トンネルが使用されている場合の Windows Update の問題
CSCvx89289	core	AnyConnect openssl 1.1.1k アップデート
CSCvy07747	core	macOS：間違ったルータを復元すると、パブリックインターフェイスで 2 つのデフォルトルートの VPN 接続が失敗する
CSCvw22016	down_install-wer	Cisco AnyConnect セキュア モビリティ クライアントを介してエクスプロイト可能な macOS 特権昇格
CSCvy04232	download_install	AnyConnect VPN インストーラが x64 エミュレーションによる Windows 10 ARM64 インサイダへのインストールを妨げる
CSCvw94933	nam	NAM プロンプトに関連する文字列の追加の翻訳を導入

識別子	コンポーネント	タイトル
CSCvw30775	nvm	NVM サービスの再起動直後に VPN に接続すると、NVM で TND チェックが実行される
CSCvx57786	nvm	NVM の信頼できるサーバーの再試行間隔
CSCvx77722	nvm	Linux：カーネル更新後に動作しない
CSCvu06648	opswat-ise	OPSWAT モジュールがデータベースのリリース日 KES 11.3 を読み取れない
CSCvw81049	opswat-ise	OPSWAT が KES 11.5.0.590 の実際のバージョンを検出できず、代わりに誤ったバージョン 21.2.x を検出する
CSCvo36890	posture-ise	[IPv6] 特定の IPv6 ネットワークが原因で ISE ポスチャ検出が無限ループに入る [MS Teredo]
CSCvx56591	posture-ise	Cisco AnyConnect ポスチャバイパスの脆弱性
CSCvx57152	posture-ise	AM 定義条件が設定されている場合にのみ AM 定義情報を取得
CSCvx58922	posture-ise	ENH：ISE ポスチャ モジュール バージョン アップグレード後の iseposture フォルダファイルの保持
CSCvx70102	posture-ise	1 つの dll の署名検証が行われない
CSCuq89328	vpn	ENH：ドメイン名を含めるのではなく除外できるようにスプリット DNS を強化
CSCvt21946	vpn	ENH：AnyConnect MTU 検出プロセスの時間を短縮

識別子	コンポーネント	タイトル
CSCvt21979	vpn	ENH：MTU検出プロセスが完了するまで、AnyConnectで「接続済み（Connected）」を表示しない
CSCvv93458	vpn	ENH：一時的なIPv6アドレスが作成または変更されるとAnyConnectがVPNトンネルを再起動する
CSCvv95822	vpn	XMLプロファイルからバックアップサーバーに接続しているときに、AnyConnectがtunnel-group属性を送信しない
CSCvw96507	vpn	macOS ENH：ネットワークインターフェイスの変更後もVPNトンネルのDNS設定が有効であることを確認
CSCvx32879	vpn	ENH：BitLockerの回復キーのエントロピと一致するようにciscoacvpnuserのパスワードのエントロピを増やす
CSCvx42883	vpn	Internet Explorer（IE）のプロキシ設定がリモートログイン用に復元されない
CSCvx81669	vpn	ENH：Microsoftの推奨に従ってVPNアダプタのアドレス割り当てを検出
CSCvx85975	vpn	macOS：awd10アドレスのリフレッシュ数が50を超える（DST除外率が高くなる）とDSTドメインの解決がタイムアウトする
CSCvx87886	vpn	4.10 FCSでのダウンローダーのクラッシュにより、トンネルが自動的に切断される
CSCvx92871	vpn	macOS 11：AnyConnectの拡張機能が予期しない無効化によってクラッシュする

AnyConnect 4.10.00093

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
CSCvx63335	certificate	Windows：AnyConnect がランダムに「証明書の期限が切れています（Certificate has expired）」エラーをスローする
CSCvx78941	certificate	Symantec ルート CA を信用できないため、AnyConnect のコード署名証明書を更新する必要がある
CSCvs75542	core	ENH：macOS における強化されたキャプティブポータル修復のサポート
CSCvu14938	core	Windows プロファイル用 Cisco AnyConnect セキュア モビリティ クライアントにおけるフォルダ変更の脆弱性
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
CSCvv30103	core	Cisco AnyConnect セキュア モビリティ クライアントにおける任意のコード実行の脆弱性
CSCvw16391	core	keepidle タイマーがサードパーティのファイアウォールによってブロックされた後、UI がエージェントとの IPC または TCP チャネルを失う

識別子	コンポーネント	タイトル
CSCvw16601	core	IPSec または IKEv2 を使用すると、AnyConnect が IPv6 にフォールバックしない
CSCvw29572	core	Cisco AnyConnect セキュア モビリティ クライアントのサービス妨害（DoS）の脆弱性
CSCvx04208	core	macOS：ダイナミックトンネルの包含率が高い、または数が多いために、Webex アプリのコールが中断する
CSCvx55399	core	HostScan enable + tunnel-group-list disable の場合、デフォルトのトンネルグループが選択される
CSCvw21825	down_install-wer	Cisco AnyConnect セキュアモビリティファイルの上書きの脆弱性
CSCvx23656	download_install	プロキシ環境変数が原因でダウンローダーの起動が失敗する
CSCvr54037	nam	ネットワーク アクセス マネージャ PE で、Cert Matching Rule-Machine EAP-TLS のユーザー定義 EKU が保存されない
CSCvw63452	nam	DIFxAPI を使用したバージョンからのネットワーク アクセス マネージャのアップグレード中に NAM バインド制御 DLL が削除される
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
CSCvw08005	opswat-ise	ISE ポスチャモジュールで SEP バージョン 14.3.1148.0100 が検出されない

識別子	コンポーネント	タイトル
CSCvt26597	posture-ise	ENH：Linux OS での ISE ポスチャモジュールのサポート
CSCvu23579	vpn	ENH：ダイナミック スプリット トンネル リストで20,000 文字を許可
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
CSCvw92182	vpn	ASA TLS のみに接続された macOS 上の AnyConnect が、接続から 20 秒後に再接続する
CSCvw96331	vpn	Linux：ポリシー、ソフトウェア、およびプロファイルのロック機能の更新が機能しない
CSCvx04190	vpn	OGS を使用しているときに、Linux で vpncli を使用して接続すると、anyconnect_global ファイルが破損する
CSCvx20136	vpn	AnyConnect 4.9 を使用して macOS Big Sur でスリープから復帰すると、一部の FQDN に対する DNS クエリが失敗する
CSCvx27372	vpn	macOS：DST 対応ヘッドエンド（低 TTL DST ドメイン）にしばらく接続していると、接続が失われる
CSCvx65570	vpn	Linux でプロファイルが使用されていない場合、AnyConnect UI に空白の [接続先：（Connect To:）] が表示される

HostScan 4.10.08029

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
CSCwh68527	opwat-asa	これは、AnyConnect および CSC での Sophos Endpoint Agent 2023.1.3.5 のサポートを追加するための ENH です

HostScan 4.10.08025

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
CSCwb54510	opswat-asa	CSCvy37094 の修正にもかかわらず、Windows 10 へのアップグレード後に HostScan が ESET AM アクティブスキャンを検出できない
CSCwd39477	opswat-asa	Sophos Endpoint Agent 2022.2.1.9 が Secure FW Posture（HostScan）5.0.00529 で定義チェックに失敗する

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
CSCwf52023	opswat-asa	HostScan 4.10.x ファイアウォールの状態とアクティブスキャンチェックにより、Crowdstrike Falcon で予期しない遅延が発生する
CSCwf70012	opswat-asa	HostScan が TrendMicro Apex One の定義チェックでスタックする
CSCwh25309	opswat-asa	ENH：HostScan に AnyConnect 4.10 での Sophos Endpoint Agent 2023.1.2.3 のサポートを追加
CSCwc62461	posture-asa	ASDM にログインすると、イメージに重要なセキュリティ修正が含まれていないという、HostScan のポップアップが表示される
CSCwf35884	posture-asa	EDR 製品のインターネットチェックをスキップする ASDM UI
CSCwh71692	posture-asa	HostScan：60 秒ごとのアセスメントでヘッダーを追加する定期的なポーリング

HostScan 4.10.07073

HostScan 4.10.07073 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 4.10.07061

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
CSCwc37015	opswat-asa	ENH：macOS での Cybereason ActiveProbe Antimalware 21.2.270+ の HostScan サポート
CSCwd05214	opwat-asa	ENH：firewalld 1.1.x および 1.2.x のサポートを追加
CSCwd94368	opswat-asa	ENH：Cisco Secure Endpoint 7.5.5.21061 の HostScan サポート
CSCwe21646	opswat-asa	AnyConnect：インターネットアクセステストのために URL をポーリングする cscan が原因で、Microsoft がアクセスをブロックする
CSCwe34677	opswat-asa	最新の HostScan バージョンが、macOS の Gatekeeper バージョン 13.2 をサポートしていない
CSCwe51207	opswat-asa	ENH：HostScan 4.10 が最新バージョンの Linux 用 CrowdStrike をサポート
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
CSCwe25243	posture-asa	VPN ユーザーのログイン後に OPSWAT インターネット接続チェックをスキップする

HostScan 4.10.06090

HostScan 4.10.06090 には、Windows、macOS、Linux 用のOPSWAT エンジンバージョンへの更新が含まれています。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 4.10.06083

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
CSCwd44206	opswat-asa	HostScan：HostScan バージョン 4.10.05111 へのアップグレード後にファイアウォールがシステム資格情報を要求する

HostScan 4.10.06081

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
CSCvy87936	opswat-asa	OPSWAT ISE および HS の Mac 12 サポート
CSCvz70815	opswat-asa	Windows および macOS の HostScan で Cisco Secure Endpoint（マルウェア対策）のサポートを追加する必要がある
CSCwa32346	opswat-asa	ENH：macOS エンドポイントの Microsoft Defender Threat Protection（ATP）の HostScan サポート

識別子	コンポーネント	タイトル
CSCwc37015	opswat-asa	ENH：macOS での Cybereason ActiveProbe Antimalware 21.2.270+ の HostScan サポート
CSCwc62378	opwat-asa	Libwalocal.dll のクラッシュにより HostScan がハングし、トークンの検証が失敗する
CSCvy30093	posture-asa	HostScan ガ Linux エンドポイントからの証明書情報を取得できない
CSCwb38379	posture-asa	macOS クライアントで、VPN がタイムアウトになり、コンソール ログに CScan のクラッシュが表示される
CSCwc68714	posture-asa	ENH：Sophos Endpoint Agent バージョン 2022.2.1.9 をサポートする HostScan イメージ

HostScan 4.10.05111

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
CSCwb45946	opswat-asa	Windows：コマンドプロンプトへのアクセスを妨げる場合の HostScan 認証のタイムアウト

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 4.10.05095

HostScan 4.10.05095 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 4.10.05085

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
CSCvz73177	opswat-asa	Windows：コンプライアンス モジュール ライブラリの初期化の問題

HostScan 4.10.04071

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
CSCvz69382	opswat-asa	ENH：HostScan を介した Bitdefender Endpoint Security バージョン 7.2.2.90 の検出のサポート

HostScan 4.10.04065

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
CSCvy53770	opswat-asa	macOS の CrowdStrike Falcon の最終更新「2」を返す HostScan 4.10.x バージョン
CSCvz63025	posture-asa	Linux で HostScan を実行するとゲームのパックマンが起動する（インストールされている場合）

HostScan 4.10.03104

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
CSCvx38469	opswat-asa	AnyConnect では、iptables のチェック中に「-n」を使用する必要がある
CSCvx75497	posture-asa	macOS で実行中の名前が長いプロセスを HostScan のプロセスチェックで検出できない
CSCvy52914	posture-asa	レジストリの複数文字列値タイプをサポートするための拡張機能

識別子	コンポーネント	タイトル
CSCvz38526	posture-asa	複数回のダウンロードの再試行
CSCvz38540	posture-asa	オンデマンドでの curl 操作のロギング

HostScan 4.10.02089

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
CSCvx38469	opswat-asa	AnyConnect では、iptables のチェック中に「n」を使用する必要がある
CSCvy52914	posture-asa	レジストリの複数文字列値タイプをサポートするための拡張機能

HostScan 4.10.02086

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
CSCvx65190	posture-asa	「HostScan は次のスキャンを待機しています（HostScan is waiting for the next scan）」というメッセージは誤解を招く

識別子	コンポーネント	タイトル
CSCvy54697	posture-asa	レジストリチェックにおけるワイルドカードのサポート
CSCvy54733	posture-asa	Windows でファイルチェックを行うための環境変数展開

HostScan 4.10.01094

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
CSCvx41020	opswat-asa	Cybereason ActiveProbe を使用する OPSWAT での Windows の遅延
CSCvy21260	opswat-asa	Windows：Windows Defender のバージョンチェックにおける 30 秒の遅延
CSCvy37121	opswat-asa	Cybereason ActiveProbe の定義日として現在の日付/時刻を返す HostScan 4.9.06046

HostScan 4.10.01075

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
CSCvu75511	opswat-asa	ENH：Linux エンドポイントの Microsoft Defender Advanced Threat Protection（ATP）の HostScan サポート
CSCvx38993	posture-asa	MR1 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
CSCvx82055	posture-asa	Oracle Linux 7.9 で AnyConnect 4.9.06037 と HostScan 4.9.06046 が「HostScan state idle」でスタックする

HostScan 4.10.00093

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
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
CSCvx82055	posture-asa	Oracle Linux 7.9 で AnyConnect 4.9.06037 と HostScan 4.9.06046 が「HostScan state idle」でスタックする

関連資料

AnyConnect の他のマニュアル

- 『Cisco AnyConnect Secure Mobility Client Administrator Guide』

- 『Cisco AnyConnect Secure Mobility Client Features, Licenses, and OSs』
- 『Open Source Software Used in AnyConnect Secure Mobility Client』
- 『Cisco General Terms, AnyConnect Secure Mobility Client, Release 4.x』

ASA 関連資料

- Cisco ASA シリーズのリリースノート
- Cisco ASA シリーズ ドキュメント一覧
- Cisco ASA 5500-X Series Next-Generation Firewall 構成ガイド
- サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ
- ホストスキャンサポート表

ISE 関連資料

- 『Release Notes for Cisco Identity Service Engine』

【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。

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。