付録：macOS 11（およびそれ以降のバージョン）に関する AnyConnect の変更点

macOS 11 用の AnyConnect 4.9.04xxx 以降を実行している必要があります。macOS で使用可能なシステム拡張フレームワークを利用します。以前はカーネル拡張フレームワークを使用していましたが、現在は廃止されています。この変更により、管理者は AnyConnect システム拡張を承認する必要があり、これらの更新で正しい動作を確保できます。また、重大なシステム拡張（または関連する OS フレームワーク）の問題が発生した場合は、最終的な回避策として、AnyConnect カーネル拡張にフェールオーバーするための手順に従うことができます。ただし、この拡張はこの目的のためだけにインストールされ、デフォルトでは使用されなくなりました。

AnyConnect のシステム拡張について

AnyConnect は、macOS 11（およびそれ以降のバージョン）で AnyConnect ソケットフィルタという名前のアプリケーションにバンドルされたネットワークシステム拡張を使用しますこのアプリケーションは拡張のアクティブ化と非アクティブ化を制御するものであり、/Applications/Cisco にインストールされます。

AnyConnect 拡張には、macOS の [システム環境設定（System Preferences）] > [ネットワークUI（Network UI）] ウィンドウに表示される次の 3 つのコンポーネントがあります。

- DNS プロキシ
- アプリケーション/トランスペアレントプロキシ
- コンテンツフィルタ

AnyConnect が適切に動作するには、そのシステム拡張とそのすべてのコンポーネントがアクティブである必要があります。これは、前述のコンポーネントがすべて存在し、macOS ネットワークの UI の左側のペインに緑色（実行中）で表示されていることで確認できます。

AnyConnect のシステム機能拡張の許可

macOS 11 以降では、システム拡張を実行する前に、エンドユーザーによる拡張の承認、またはエンドユーザーの承認なしの MDM 承認が必要です。AnyConnect のシステム拡張には 2 つの承認が必要です。

• システム拡張のロード/アクティブ化の承認 （2 ページ）
• MDM を使用したシステム拡張の許可 （3 ページ）

システム拡張のロード/アクティブ化の承認

AnyConnect のシステム拡張とそのコンテンツ フィルタ コンポーネントは、OS プロンプトに従うか、またはより明示的に AnyConnect 通知アプリケーションの指示に従って承認します。

手順

ステップ 1 AnyConnect 通知アプリケーションの [環境設定を開く（Open Preferences）] ボタンをクリックするか、「システム拡張機能がブロックされました（System Extension Blocked）」というアプリケーションメッセージが表示された場合は、[セキュリティの環境設定を開く（Open Security Preferences）] ボタンをクリックします。システム設定アプリケーションに移動して、[セキュリティとプライバシー（Security&Privacy）] ウィンドウに移動することもできます。

ステップ 2 左下のロックをクリックし、要求されたクレデンシャルを入力してロックを解除し、変更を許可します。

ステップ 3 [セキュリティとプライバシー（Security & Privacy）] ウィンドウで [許可（Allow）] をクリックして、AnyConnect ソケットフィルタを受け入れます。

複数のシステム拡張が承認を必要とする場合、ボタンには [詳細...（Details...）] ラベルが付いています。。この場合、[詳細...（Details...）] をクリックし、[AnyConnectソケットフィルタ（Socket Filter）] チェックボックスをオンにして、[OK] をクリックし、許可を必要とする後続のプロンプトを承認します。

次のタスク

拡張のコンテンツ フィルタ コンポーネントが承認されると、通知が届きます。

MDM を使用したシステム拡張の許可

AnyConnectのシステム拡張を、エンドユーザーが操作することなく、次の設定で管理プロファイルの SystemExtensions ペイロードを使用して承認します。

プロパティ	値
チーム識別子	DE8Y96K9QP
バンドル識別子	com.cisco.anyconnect.macos.acsockext
システム拡張タイプ	NetworkExtension

次の WebContentFilter ペイロード設定を使用して、拡張のコンテンツ フィルタ コンポーネントを承認します。

プロパティ	値
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	ファイアウォール
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
PluginBundleID	com.cisco.anyconnect.macos.acsockext
VendorConfig	
UserDefinedName	Cisco AnyConnect コンテンツフィルタ

AnyConnect システム拡張のアクティブ化の確認

AnyConnect システム拡張が承認され、アクティブになっていることを確認するには、**systemextensionsctl list** コマンドを実行します。

```
% systemextensionsctl list
1 extension(s)
```

```
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsockext
(4.9.03038/4.9.03038) Cisco AnyConnect Socket Filter Extension
[activated enabled]
```

また、[システム設定（System Preferences）] ネットワーク UI を確認して、3 つの AnyConnect 拡張コンポーネントがすべてアクティブであることを確認することもできます。

AnyConnect システム拡張機能を無効にする

AnyConnect のアンインストール時に、ユーザーはシステム拡張の非アクティブ化を承認するための管理者クレデンシャルの入力を求められます。macOS 12（およびそれ以降のバージョン）では、RemovableSystemExtensions プロパティを SystemExtensions ペイロードに追加し管理プロファイルを展開した後、AnyConnect システム拡張をサイレントに削除できます。このプロパティには、AnyConnect システム拡張（com.cisco.anyconnect.macos.acsockext）のバンドル識別子が含まれている必要があります。

（注） 注：この管理プロファイル構成は、管理者が AnyConnect のアンインストールを自動化する場合にのみ使用する必要があります。これにより、root 権限を持つすべてのユーザーまたはプロセスに、ユーザーにパスワードの入力を求めずに AnyConnect システム拡張を削除する機能が付与されます。

カーネル拡張へのフェールオーバー

AnyConnect は引き続き macOS 11 にカーネル拡張をインストールします。ただし、重大なシステム拡張（または関連する OS フレームワーク）の問題が発生した場合、または Cisco Technical Assistance Center（TAC）による指示があった場合のフォールバックとしてのみ使用してください。カーネル拡張は、macOS 11 以降にロードする前に MDM による承認が必要です。エンドユーザの承認はオプションではなくなりました。

始める前に

これらの手順は、最終的な回避策としてのみ使用してください。

手順

ステップ 1 AnyConnect カーネル拡張は、次の設定で管理プロファイルの *SystemPolicyKernelExtensions* ペイロードを使用して承認します。

プロパティ	値
チーム識別子	DE8Y96K9QP

プロパティ	値
バンドル識別子	com.cisco.kext.acsock

MDM 設定プロファイルがインストールされます。

ステップ 2 次のコマンドを実行すると、AnyConnect によってシステム拡張が非アクティブ化され、代わりにカーネル拡張の使用が開始されます。管理者クレデンシャルの入力を求められます。**% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && /Applications/Cisco/Cisco\ AnyConnect\ Socket\ Filter.app/Contents/macOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist**

ステップ 3 次のコマンドを実行して、カーネル拡張がロードされたことを確認します：**% kextstat | grep com.cisco.kext.acsock**

AnyConnect がカーネル拡張のロードに失敗した場合は、リブートを実行します。

システム拡張に戻る

Cisco TAC がシステム拡張の問題の修正を確認した場合（およびカーネル拡張へのフェールオーバーの必要性がなくなった場合）、次のコマンドを実行して AnyConnect にシステム拡張に切り替えるように指示します。

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist &&
sudo kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/anyconnect/acsock.cfg &&
 sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

修正を適用した AnyConnect または macOS バージョンをインストールします。

AnyConnect システムとカーネル拡張の承認のためのサンプル MDM 設定プロファイル

次の MDM 設定プロファイルを使用して、システム拡張のコンテンツ フィルタ コンポーネントを含む AnyConnect システム拡張とカーネル拡張の両方をロードできます。

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

      <dict>

      <key>PayloadContent</key>

      <array>

            <dict>
```

```
            <key>AllowUserOverrides</key>
            <true/>
            <key>AllowedKernelExtensions</key>
            <dict>
                  <key>DE8Y96K9QP</key>
                  <array>
                  <string>com.cisco.kext.acsock</string>
                  </array>
            </dict>
            <key>PayloadDescription</key>
            <string></string>
            <key>PayloadDisplayName</key>
            <string>AnyConnect Kernel Extension</string>
            <key>PayloadEnabled</key>
            <true/>
            <key>PayloadIdentifier</key>
            <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
            <key>PayloadOrganization</key>
            <string>Cisco Systems, Inc.</string>
            <key>PayloadType</key>
            <string>com.apple.syspolicy.kernel-extension-policy</string>
            <key>PayloadUUID</key>
            <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
      </dict>
      <dict>
            <key>AllowUserOverrides</key>
            <true/>
            <key>AllowedSystemExtensions</key>
            <dict>
                  <key>DE8Y96K9QP</key>
```

```
                <array>
                <string>com.cisco.anyconnect.macos.acsockext</string>
                </array>
        </dict>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>AnyConnect System Extension</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadType</key>
        <string>com.apple.system-extension-policy</string>
        <key>PayloadUUID</key>
        <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
<dict>
        <key>Enabled</key>
        <true/>
        <key>AutoFilterEnabled</key>
        <false/>
        <key>FilterBrowsers</key>
        <false/>
        <key>FilterSockets</key>
        <true/>
        <key>FilterPackets</key>
        <false/>
```

```
                        <key>FilterType</key>
                        <string>Plugin</string>
                        <key>FilterGrade</key>
                        <string>firewall</string>
                        <key>PayloadDescription</key>
                        <string></string>
                        <key>PayloadDisplayName</key>
                        <string>Cisco AnyConnect Content Filter</string>
                        <key>PayloadIdentifier</key>

<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
                        <key>PayloadType</key>
                        <string>com.apple.webcontent-filter</string>
                        <key>PayloadUUID</key>
                        <string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
                        <key>PayloadVersion</key>
                        <integer>1</integer>
                        <key>FilterDataProviderBundleIdentifier</key>
                        <string>com.cisco.anyconnect.macos.acsockext</string>
                        <key>FilterDataProviderDesignatedRequirement</key>
                        <string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate
leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string>
                        <key>PluginBundleID</key>
                        <string>com.cisco.anyconnect.macos.acsock</string>
                        <key>UserDefinedName</key>
                        <string>Cisco AnyConnect Content Filter</string>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
```

```
        <string>Approved AnyConnect System and Kernel Extensions</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <true/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
</plist>
```