macOS 11（Big Sur）に関連する AnyConnect の変更点

目次

図の目次

1. はじめに

AnyConnect 4.9.04xxx は、macOS 11（Big Sur）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。この点で、現在は廃止されているカーネル拡張フレームワークに依存する過去の

AnyConnect バージョンとは異なっています。これが macOS 11 で AnyConnect を実行するために必要な最小バージョンとなります。

このアドバイザリでは、AnyConnect の新しいバージョンで導入された変更点と、AnyConnect が macOS 11 で正常に動作していることを確認するために管理者が実行できる手順について説明します。次の項で詳しく説明するように、AnyConnect のシステム拡張の承認には重要な変更点があります。

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の最終的な回避策として、AnyConnect のカーネル拡張にフェールオーバーする手順についても詳しく説明します。AnyConnect のカーネル拡張は、このためにのみ macOS 11 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。

2. AnyConnect のシステム拡張について

AnyConnect は、macOS 11 で Cisco 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、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

これらのコンポーネントは、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ます。

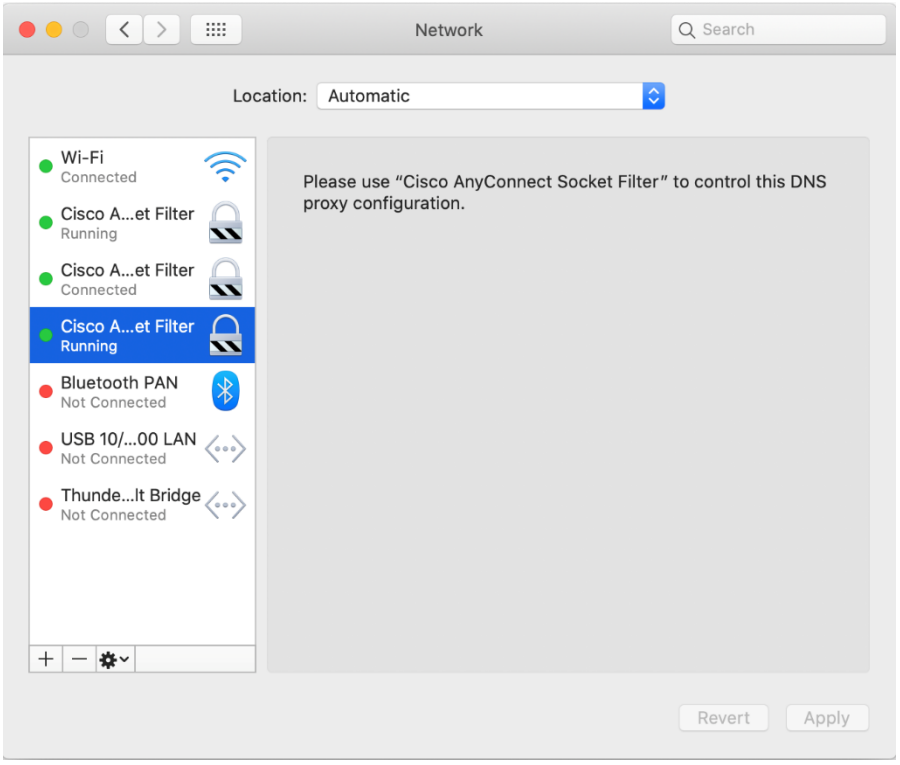

図1：プロキシコンポーネント

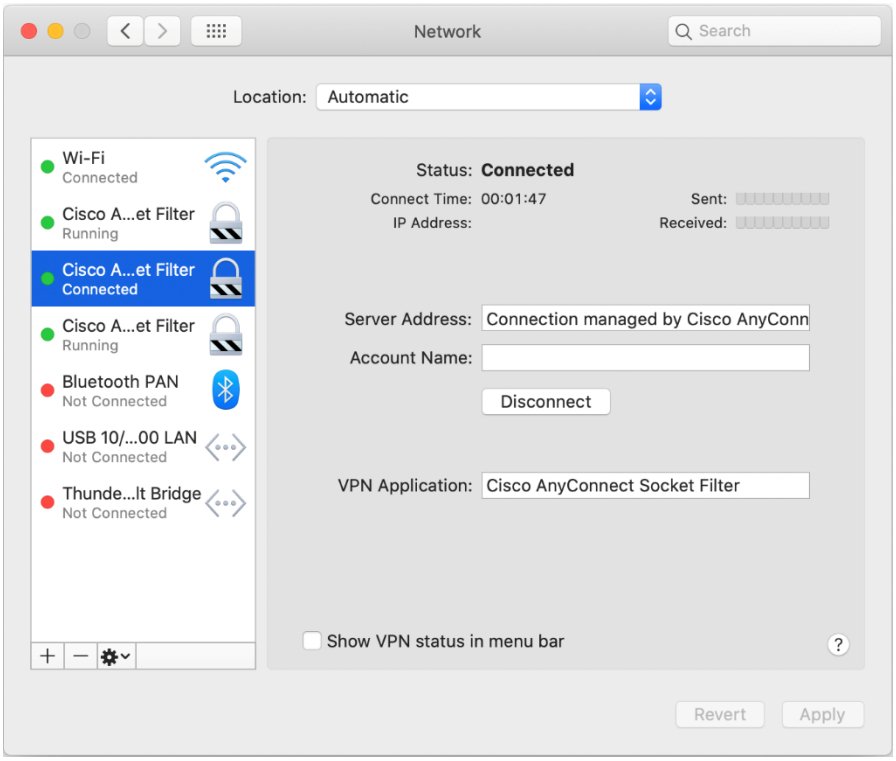

図2：アプリ/トランスペアレント プロキシ コンポーネント

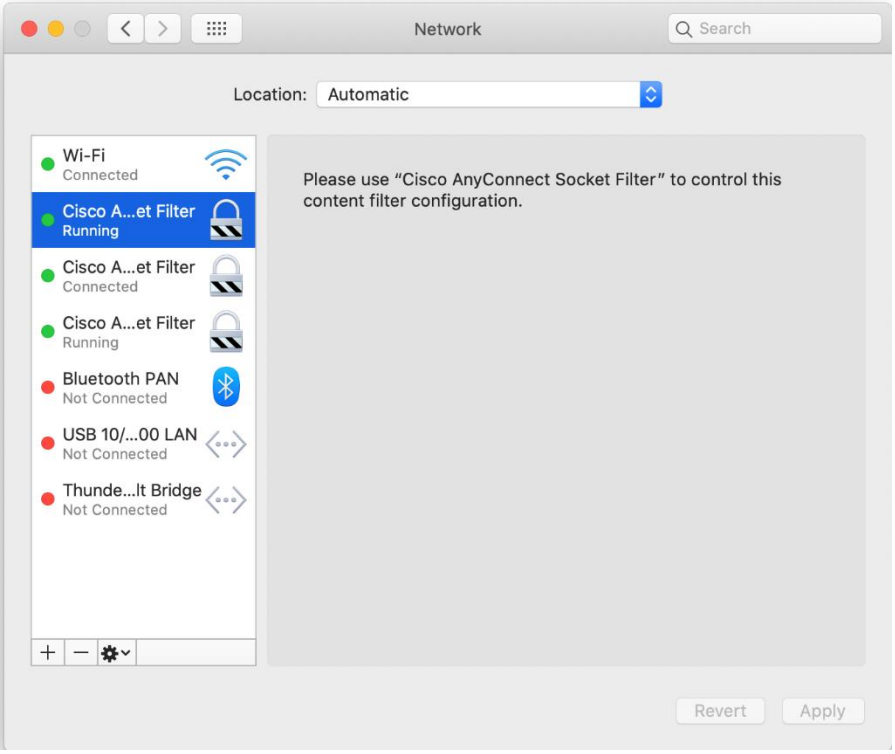

図3：コンテンツ フィルタ コンポーネント

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、上に示したスクリーンショットのように、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。

3. AnyConnect のシステム拡張の承認

macOS 11 では、システム拡張の実行を許可する前に、エンドユーザーまたは MDM の承認が必要です。

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。
- 拡張のコンテンツ フィルタ コンポーネントのアクティブ化の承認。

3.1 エンドユーザーによる拡張の承認

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、エンドユーザーが承認できます。

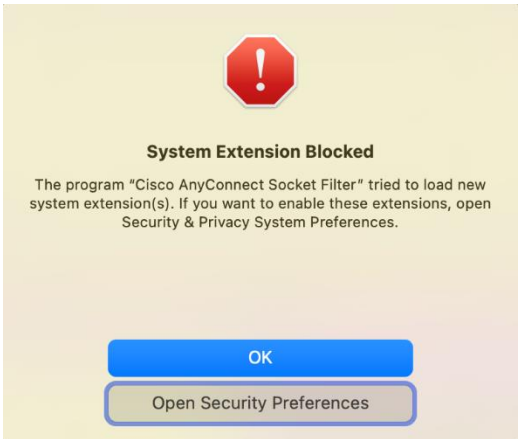

図4：ブロックされた拡張 - OS プロンプト

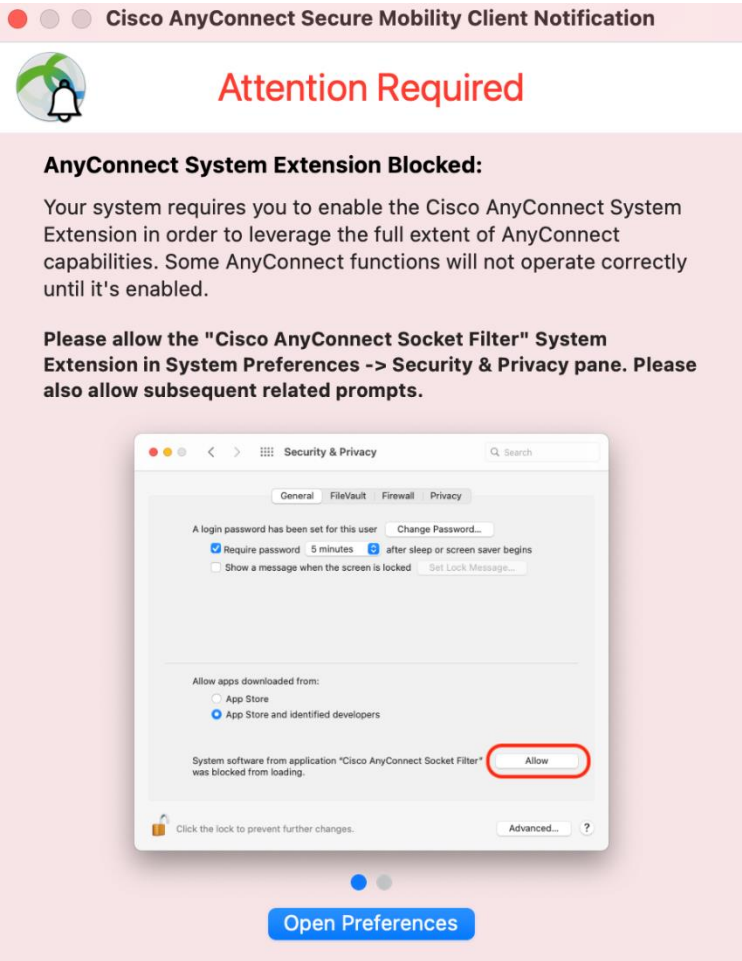

図5：ブロックされた拡張 - AnyConnect プロンプト

[セキュリティおよびプライバシーの設定（Security & Privacy Preferences）] ウィンドウを開いたら、左下の錠をクリックし、プロンプトに従って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。

ウィンドウの外観は、AnyConnect 拡張が承認を必要とする唯一の拡張であるかどうかによって異なります。唯一の拡張である場合は、[許可（Allow）] ボタンをクリックします。

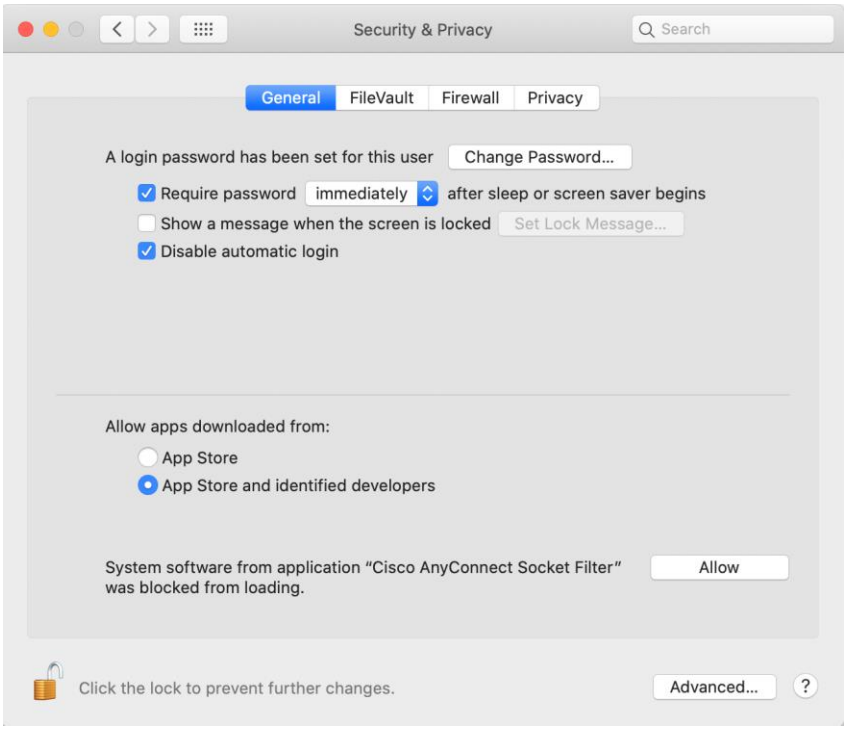

図6：AnyConnect 拡張の承認

それ以外の場合は [詳細…（Details…）] ボタンをクリックし、[Cisco AnyConnect ソケットフィルタ（Cisco AnyConnect Socket Filter）] チェックボックスをオンにして [OK] をクリックします。

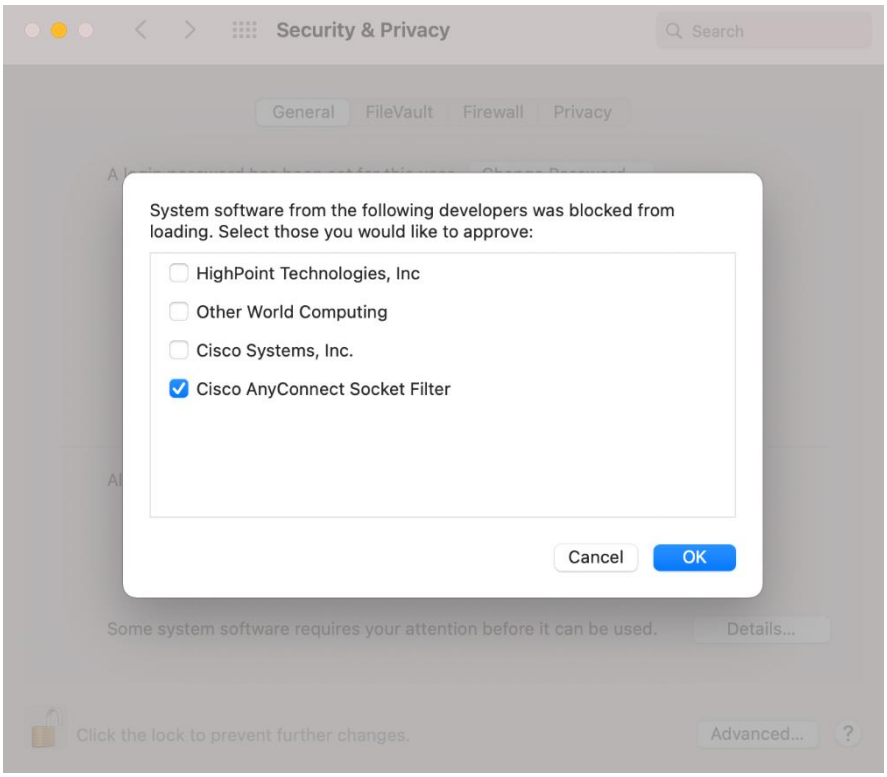

図7：AnyConnect 拡張の承認（複数の未承認の拡張）

AnyConnect 拡張を承認した直後に、拡張のコンテンツ フィルタ コンポーネントを承認するための別のポップアップがユーザーに表示されます。

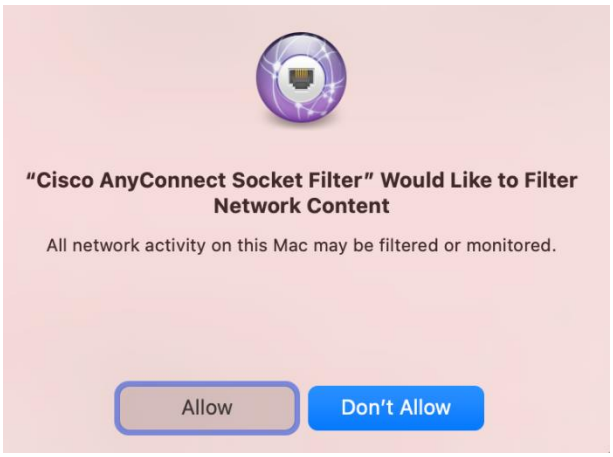

図8：AnyConnect 拡張のコンテンツフィルタの承認

拡張のコンテンツフィルタの承認が完了すると、AnyConnect 通知アプリケーションで確認されたとおりに、拡張とそのコンポーネントがアクティブになります。

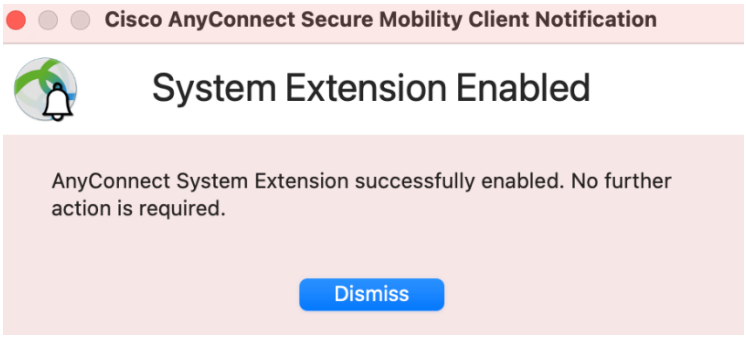

図9：AnyConnect 拡張承認の確認

3.2 MDM を使用した拡張の承認

AnyConnect のシステム拡張は、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することもできます。

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

拡張のコンテンツ フィルタ コンポーネントを承認するには、次の設定で WebContentFilter ペイロードを使用できます。

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

3.3 AnyConnect 拡張の承認の確認

systemextensionsctl list コマンドを実行して、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（Network UI）] を調べ、「AnyConnect システム拡張について」の項に従って 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します。

3.4 AnyConnect 拡張の非アクティブ化

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。

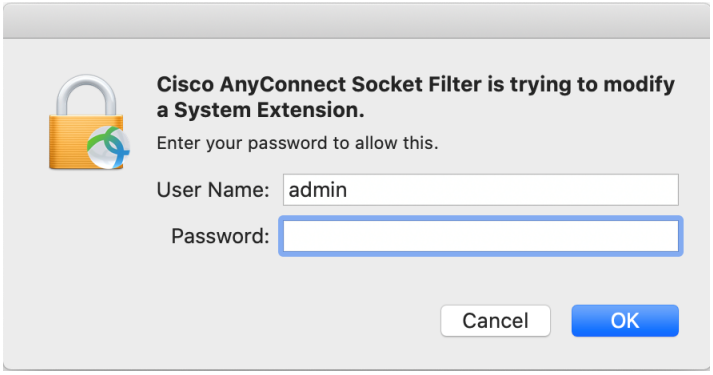

図 10：拡張機能の非アクティブ化のプロンプト

4. 最終的な回避策：カーネル拡張へのフェールオーバー

AnyConnect は、以前の OS バージョンと同様に、macOS 11 にも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）の場合にのみ、フォールバックとしてインストールされます。

最終的な一時の回避策として、Cisco TAC はシステム拡張からレガシーカーネル拡張に切り替えることを推奨します。これにより、同等の機能が提供されます。

4.1 MDM を使用したカーネル拡張の承認

カーネル拡張は、macOS 11 にロードするために MDM を介した承認が必要です。エンドユーザーの承認はオプションではありません。

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できます。

プロパティ	値
チーム識別子	DE8Y96K9QP
バンドル識別子	com.cisco.kext.acsock

4.2 カーネル拡張へのフェールオーバー

前の項で詳しく説明した MDM 設定プロファイルをインストールしたら、次のコマンドを実行して AnyConnect にシステム拡張を非アクティブ化し、代わりにカーネル拡張を使用するように指示します。

（ユーザーは、「AnyConnect 拡張の非アクティブ化」の項に従ってシステム拡張の非アクティブ化プロンプトに対応する必要があります。）

```
% 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
```

上記のコマンドの実行時に AnyConnect がカーネル拡張のロードに失敗した場合は再起動を実行する必要があります。これは、次のコマンドを実行することで確認できます（カーネル拡張のロードに成功すると、1 つのエントリが返されます）。

```
% kextstat | grep com.cisco.kext.acsock
```

カーネル拡張へのフェールオーバーの原因となっているシステム拡張の問題が Cisco TAC によって解決されたことが確認されたら、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
```

次に、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。

5. 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>
```

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。