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

macOS 11 以降では、Cisco Secure Client は macOS システム拡張フレームワークを利用しています。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。以下のセクションで説明するように、管理者は Cisco Secure Client システム拡張を承認する必要があります。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は、最終的な回避策として、Cisco Secure Client 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。

Cisco Secure Client のシステム拡張について

Cisco Secure Client は、macOS 11（およびそれ以降）で Cisco Secure Client - 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。

Cisco Secure Client 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

Cisco Secure Client 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。

Cisco Secure Client のシステム機能拡張の許可

Cisco Secure Client のシステム拡張機能のアクティブ化には、管理者権限を持つエンドユーザーによる承認または MDM 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

Cisco Secure Client 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 Cisco Secure Client - 通知アプリケーションの指示に従って承認します。

ステップ 1 Cisco Secure Client - 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、macOS からの「システム拡張機能がブロックされました（System Extension Blocked）」という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、Cisco Secure Client - ソケットフィルタの拡張を受け入れます。

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、[Cisco Secure Client - ソケットフィルタ（Cisco Secure Client - 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 コンポーネントを承認するプロンプトを受け入れると、その時点で通知が届きます。

MDM を使用したシステム拡張の許可

Cisco Secure Client 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

Cisco Secure Client システム拡張のアクティブ化の確認

Cisco Secure Client 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
(5.0.00xxx/5.0..00xxx) Cisco Secure Client - 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 Cisco Secure Client 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。

Cisco Secure Client システム拡張機能を無効にする

Cisco Secure Client 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、Cisco Secure Client 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、Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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

Cisco Secure Client は引き続き macOS 11 以降のバージョンにカーネル拡張をインストールします。ただし、カーネル拡張は macOS 10.15 で Apple によって廃止されているため、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フォールバックとしてのみ、および Cisco Technical Assistance Center（TAC）による指示があった場合に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。

ステップ 1 Cisco Secure Client 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
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、Cisco Secure Client 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。

- macOS 13 以降の場合

  % osascript -e 'quit app "Cisco Secure Client - AnyConnect VPN Service.app"' && open -W -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app" --args uninstall && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kf && open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"

- macOS 12 以前の場合

  % sudolaunchctl unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kf && sudolaunchctl load /Library/LaunchDaemons/com.cisco.secureclient.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**

Cisco Secure Client 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 Cisco Secure Client にシステム拡張に切り替えるように指示します。実行しているCisco Secure Clientバージョンによってコマンドは異なります。

Cisco TAC がシステム拡張の問題の修正を確認した場合は、推奨される Cisco Secure Client または修正を適用した macOS バージョンをインストールします。

提案された修正を適用した（それにより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）後、次のコマンドを実行し、Cisco Secure Client にシステム拡張に切り替えるように指示します。実行している macOS バージョンによってコマンドが変わります。

macOS 13 以降の場合

```
% osascript -e 'quit app "Cisco Secure Client - AnyConnect VPN Service.app"' && open -W
-a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app" --args
uninstall && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kfr && open -a
"/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

macOS 12 以前の場合

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist
&& sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kfr && sudo launchctl load
/Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist
```

Cisco Secure Client 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 Cisco Secure Client 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>Cisco Secure Client 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>Cisco Secure Client 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 Secure Client 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 Cisco Secure Client 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。