

macOS11（およびそれ以降のバージョン）に関する Cisco Secure Client の変更点

- Cisco Secure Client のシステム拡張について （1 ページ）
- Cisco Secure Client のシステム機能拡張の許可 （2 ページ）
- Cisco Secure Client システム拡張機能を無効にする （4 ページ）
- Cisco Secure Client システム拡張の承認のためのサンプル MDM 設定プロファイル （4 ページ）
- 管理対象ログイン項目 （4 ページ）
- Cisco Secure Client が管理するログイン項目の MDM 設定プロファイルのサンプル （5 ページ）

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。

サードパーティ製品が DNS プロキシ機能を備えたシステム拡張を使用している場合、Cisco Secure Client またはサードパーティ製品（またはその両方）が適切に機能しない可能性があります。macOS は、一度に 1 つのアクティブな DNS プロキシ拡張のみをサポートします。

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 （2 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。

手順

ステップ 1 macOS から「System Extension Blocked」メッセージを受信した場合は、次の操作を実行します。

- macOS 15（以降）の場合、Cisco Secure Client - 通知アプリケーションの [システム設定を開く（Open System Settings）] ボタンをクリックし、[システム設定（System Settings）] > [一般（General）] > [ログイン項目と拡張機能（Login Items and Extensions）] セクションで [ネットワーク拡張機能（Network Extensions）] を選択します。
- macOS 13 および 14 の場合は、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、または [セキュリティ設定を開く（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ます。

ステップ 3 macOS 15 の場合は、クリックして Cisco Secure Client ソケットフィルタを許可します。macOS 13 または 14 の場合は、[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。

「System Extension Enabled」というメッセージが表示されます。

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.acsock
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。

Cisco Secure Client システム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>

       </plist>
```

管理対象ログイン項目

macOS 13（以降）および Secure Client 5.1 の場合、VPN および ZTA モジュールは、機能させる前にユーザーの承認が必要です。ユーザーの介入なしに承認を実行するか、Secure Client が

所有するログイン項目をユーザーが無効にできないようにするには、管理対象ログイン項目の次の属性を使用して MDM プロファイルをプッシュする必要があります。

- バンドル識別子プレフィックス：com.cisco.secureclient
- チーム識別子：DE8Y96K9QP

詳細については、「Web Deploy Upgrade on macOS 13 (or Later) Requires Admin Privileges」または Apple Platform Deployment ドキュメントを参照してください。

Cisco Secure Client が管理するログイン項目の MDM 設定プロファイルのサンプル

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。