Cisco Secure Client プロファイルエディタ

プロファイル エディタについて

Cisco Secure Client ソフトウェアパッケージには、Windows 対応のプロファイルエディタが含まれています。Cisco Secure Client イメージを Cisco Secure Firewall ASA にロードすると、ASDM はプロファイルエディタをアクティブにします。ローカルまたはフラッシュからクライアントプロファイルをアップロードできます。

複数の Cisco Secure Client パッケージをロードした場合は、最新の Cisco Secure Client パッケージからクライアント プロファイル エディタがアクティブにされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の Cisco Secure Client で使用される機能が表示されます。

Windows で動作するスタンドアロン プロファイル エディタもあります。

ASDM からの新しいプロファイルの追加

（注） クライアント プロファイルを作成する前に、まずクライアント イメージをアップロードする必要があります。

プロファイルが Cisco Secure Client の一部としてエンドポイント上の管理者定義のエンドユーザー要件および認証ポリシーに展開され、これにより、エンドユーザーが事前設定済みのネットワークプロファイルを使用できるようになります。プロファイルエディターを使用して、1 つ以上のプロファイルを作成および構成します。Cisco Secure Client には、ASDM の一部として、およびスタンドアロンの Windows プログラムとしてプロファイルエディタが含まれています。

新しいクライアント プロファイルを ASDM から Cisco Secure Firewall ASA に追加するには、次の手順を実行します。

ステップ 1 ASDM で、**[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 [プロファイルの使用（Profile Usage）] ドロップダウン リストから、プロファイルを作成するモジュールを選択します。

ステップ 5 （任意）[プロファイルの場所（Profile Location）] フィールドで [フラッシュの参照（Browse Flash）] をクリックし、Cisco Secure Firewall ASA の XML ファイルのデバイスファイルパスを選択します。

ステップ 6 （任意）スタンドアロン エディタを使用してプロファイルを作成した場合、[アップロード（Upload）] をクリックして、そのプロファイル定義を使用します。

ステップ 7 （任意）ドロップダウンリストから Cisco Secure Client グループポリシーを選択します。

ステップ 8 [OK] をクリックします。

[Cisco Secure ClientVPNプロファイル（VPN Profile）]

Cisco Secure Client機能は、Cisco Secure Client プロファイルで有効になっています。これらのプロファイルには、コアクライアント VPN 機能とオプション クライアント モジュール（Network Access Manager、ISE ポスチャ、Umbrella、Network Visibility Module、Cisco Secure Endpoint、カスタマー エクスペリエンス フィードバックなど）の構成設定が含まれています。Cisco Secure Firewall ASA は Cisco Secure Client のインストールおよび更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

Cisco Secure Firewall ASA または ISE は、すべての Cisco Secure Client ユーザーにグローバルにプロファイルを展開するか、ユーザーのグループポリシーに基づいて展開するように設定できます。通常、ユーザーは、インストールされている Cisco Secure Client モジュールごとに 1 つのプロファイルを持ちます。場合によっては、1 人のユーザーに複数の VPN プロファイルを提供することが必要になります。たとえば、複数の場所で働くユーザーなどの場合です。

一部のプロファイル設定は、ユーザのコンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザーファイルには、クライアント GUI の [設定（Preferences）] タブにユーザー制御可能設定を Cisco Secure Client で表示するうえで必要となる情報、およびユーザー、グループ、ホストなど、直近の接続に関する情報が保存されます。

同じ <HostAddress> を持つ複数の Secure Client プロファイルを使用しないことをお勧めします。これにより、プロファイルの設定がマージされ、接続に対してより安全な接続設定が選択されます。マージすると、エンドポイントで機能が失われたり、接続が拒否されたりする可能性があります。

グローバルファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Login や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

Cisco Secure Client プロファイルエディタ、プリファレンス（Part 1）

- [Start Before Loginを使用（Use Start Before Login）]：（Windows のみ）クライアントで使用するために Start Before Login を有効にします。[Start Before Loginを使用（Use Start Before Login）]が有効になっていると、Windows ログインダイアログボックスが表示される前に Cisco Secure Client が起動します。ユーザは、Windows にログインする前に、VPN 接続を介してエンタープライズインフラストラクチャに接続します。認証後、ログインダイアログボックスが表示され、ユーザは通常どおりログインします。

- [事前接続メッセージの表示（Show Pre-connect Message）]：管理者は、ユーザーが初めて接続を試行する前にワンタイムメッセージを表示させることができます。たとえば、メッセージを表示して、ユーザにスマート カードをリーダに挿入するよう促すことができます。このメッセージは、Cisco Secure Client メッセージカタログに表示され、ローカライズされています。

- [クライアント証明書ストア（Client Certificate Store）]：Cisco Secure Client がどの証明書ストアを使用してクライアント証明書を読み取るかを制御します。セキュア ゲートウェイは、適切に設定し、複数の証明書認証の組み合わせのうちどれが特定の VPN 接続で許容されるかをクライアントに指定する必要があります。

  セキュアゲートウェイに許容される証明書のタイプは、2 ユーザ証明書か、1 マシンおよび 1 ユーザ証明書のどちらかです。

  Cisco Secure Client がアクセスできる証明書ストアをさらに絞り込めるようにするには、Windows 用、macOS 用、または Linux 用のドロップダウンから証明書ストアを設定できます。プロファイル設定では、次の値がサポートされます。

  - **Windows**

（注） VPN 接続が開始されたネットワークから証明書失効チェックを実行できない場合、クライアント証明書の列挙に時間がかかることがあります。

  - [すべて（All）]：（デフォルト）Windows マシンとユーザの両方の証明書ストアのクライアント証明書を使用します。
  - [マシン（Machine）]：Windows 証明書ストアのクライアント証明書のみを使用します。
  - [ユーザ（User）]：Windows 証明書ストアのクライアント証明書のみを使用します。
  - **macOS**

- [すべて（All）]：（デフォルト）利用可能なすべてのキーチェーンおよび PEM ファイルストアのクライアント証明書を使用します。
- [システム（System）]：システムキーチェーンおよびシステム PEM ファイルストアのクライアント証明書のみを使用します。
- [ログイン（Login）]：ユーザログインキーチェーンとダイナミック スマートカードキーチェーン、およびユーザ PEM ファイルストアのクライアント証明書のみを使用します。
- **Linux**
- [すべて（All）]：（デフォルト）システムとユーザの両方の PEM ファイルストア、およびユーザ Firefox NSS ストアのクライアント証明書を使用します。
- [マシン（Machine）]：システム PEM ファイルストアのクライアント証明書のみを使用します。
- [ユーザ（User）]：ユーザ PEM ファイルストア、およびユーザ Firefox NSS ストアのクライアント証明書のみを使用します。

- [Windows証明書ストアの上書き（Windows Certificate Store Override）]：管理者は、Windows マシン（ローカルシステム）証明書ストア内の証明書をクライアント証明書認証に使用するように Cisco Secure Client に指示できます。証明書ストアの上書きは、デフォルトでは UI プロセスによって接続が開始される SSL にのみ適用されます。IPSec/IKEv2 を使用している場合、Cisco Secure Client プロファイルのこの機能は適用されません。

（注） マシン証明書を使用して Windows に接続するには、このオプションが有効にされている事前展開されたプロファイルが必要です。接続する前に Windows デバイスにこのプロファイルが存在しない場合、証明書はマシン ストアにアクセスできず、接続は失敗します。

  - True：Cisco Secure Client は、Windows マシン証明書ストア内の証明書を検索します。[クライアント証明書ストア（Client Certificate Store）]（Windows）は、[すべて（All）] または [マシン（Machine）] に設定する必要があります。
  - False：（デフォルト）ユーザーが管理者権限を持っていない場合、Cisco Secure Client は、Windows マシン証明書ストア内の証明書を検索しません。

- AutomaticCertSelection：セキュア ゲートウェイで複数証明書の認証を設定するときは、この値を true に設定する必要があります。
- [起動時に自動接続（Auto Connect on Start）]：Cisco Secure Client の起動時に、Cisco Secure Client プロファイルで指定されたセキュア ゲートウェイまたはクライアントが最後に接続していたゲートウェイとの VPN 接続が自動的に確立されます。

- [接続時に最小化（Minimize On Connect）]：VPN 接続の確立後、Cisco Secure Client GUI が最小化されます。
- [ローカル LAN アドレス（Local LAN Access）]：Cisco Secure Firewall ASA への VPN セッション中にリモートコンピュータへ接続したローカル LAN に対してユーザーが無制限にアクセスできるようになります。

（注） ローカル LAN アクセスを有効にすると、パブリック ネットワークからユーザ コンピュータを経由して、社内ネットワークにセキュリティの脆弱性が生じる可能性があります。代替手段として、セキュリティアプライアンス（バージョン 8.4(1) 以降）で、デフォルト グループ ポリシーに含まれている Cisco Secure Client ローカル印刷ファイアウォールルールを使用した SSL クライアントファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [プリファレンス（Part 2）（Preferences (Part 2)）] で、[自動 VPN ポリシー（Automatic VPN Policy）]、[常にオン（Always on）]、および [VPN の接続解除を許可（Allow VPN Disconnect）] も有効にする必要があります。

- [キャプティブポータル検出を無効にする（Disable Captive Portal Detection）]：Cisco Secure Clientが受信する証明書の共通名が、Cisco Secure Firewall ASA 名と一致しない場合、キャプティブポータルが検出されます。この動作により、ユーザによる認証が促されます。自己署名証明書を使用する一部のユーザは、HTTP キャプティブ ポータルで保護されている企業リソースへの接続を有効にすることを望むことがあるため、[キャプティブポータル検出を無効にする（Disable Captive Portal Detection）] チェックボックスをオンにする必要があります。管理者は、このオプションをユーザが設定できるようにするかどうかを判断し、判断に基づいてチェックボックスをオンにすることもできます。ユーザーが設定できるようにした場合は、Cisco Secure Client UI の [プリファレンス（Preferences）] タブにチェックボックスが表示されます。
- [自動再接続（Auto Reconnect）]：接続が解除された場合、Cisco Secure Client により VPN 接続の再確立が試行されます。[自動再接続（Auto Reconnect）] を無効にすると、接続解除の原因にかかわらず、再接続は試行されません。

（注） 自動再接続は、ユーザがクライアントの動作を制御するシナリオで使用します。この機能は、AlwaysOn ではサポートされません。

- **自動再接続の動作**
  - Disconnect On Suspend：Cisco Secure Client では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。

- ReconnectAfterResume（デフォルト）：接続が解除された場合、Cisco Secure Client により VPN 接続の再確立が試行されます。

- [コネクトスタンバイ中に AnyConnect を一時停止する（Suspend AnyConnect During Connected Standby）]：（Windows のみ）コネクトスタンバイをサポートするデバイスでのみ使用できます。コネクトスタンバイ中、オペレーティングシステムはシステムプロセスをスロットリングするため、パケットの処理方法に影響を与える可能性があります。このオプションを使用すると、システムがコネクトスタンバイモードになったときに VPN トラフィックを無効にすることができます。この機能はデフォルトで無効に設定されています。
- [自動更新（Auto Update）]：オンにすると、クライアントの自動アップデートが有効になります。[ユーザ制御可（User Controllable）] チェックボックスをオンにすると、クライアントのこの設定を無効にできます。
- [RSA セキュア ID 連携（RSA Secure ID Integration）]（Windows のみ）：ユーザが RSA とどのように対話するかを制御します。デフォルトでは、Cisco Secure Client が RSA の適切な対話方法を決定します（自動設定：ソフトウェアトークンとハードウェアトークンの両方を受け入れます）。
- [Windows ログインの強制（Windows Logon Enforcement）]：Remote Desktop Protocol（RDP）セッションから VPN セッションを確立することを許可します。スプリット トンネリングはグループ ポリシーで設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は Cisco Secure Client により解除されます。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。
  - [シングルローカルログイン（Single Local Logon）]（デフォルト）：（ローカル：1、リモート：制限なし）VPN 接続全体で、ログインできるローカルユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザーがログインしている場合でも、ローカル ユーザーが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザー ログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

  - [シングルログイン（Single Logon）]：（ローカル + リモート：1）VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。

VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

（注） 複数同時ログオンはサポートされません。

- [シングルログイン（リモートなし）（Single Logon No Remote）]：（ローカル：1、リモート：0）VPN 接続全体で、ログインできるローカルユーザは 1 人だけです。リモートユーザは許可されません。VPN接続の確立時に、複数のローカルユーザまたはリモートユーザがログインしている場合、接続は許可されません。VPN接続中に第2のローカルユーザまたはリモートユーザがログインすると、VPN接続が終了します。

- [Windows VPN確立（Windows VPN Establishment）]：クライアント PC にリモート ログインしたユーザーが VPN 接続を確立した場合の Cisco Secure Client の動作を決定します。設定可能な値は次のとおりです。
  - [ローカルユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの Cisco Secure Client と同じ機能です。
  - [リモートユーザーを許可（Allow Remote Users）]：リモート ユーザーは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。リモート ユーザが VPN 接続を終了せずにリモート ログイン セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。

（注） この設定は、エンドポイントへの接続に Remote Desktop Protocol（RDP）が使用されている場合に機能します。

- [Linux ログインの適用（Linux Logon Enforcement）]：SSH セッションから VPN セッションを確立できます。グループポリシーにスプリットトンネリングを設定する必要があります。VPN 接続を確立したユーザーがログオフすると、Cisco Secure Client は VPN 確立を接続解除します。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。
  - [シングルローカルログイン（Single Local Logon）]（デフォルト）：（ローカル：1、リモート：制限なし）VPN接続全体で、ログインできるローカルユーザは1人だけです。また、クライアント PC に複数のリモート ユーザーがログインしている場合でも、ローカル ユーザーが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザー ログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN接続のルーティング設定によって異なります。

- [シングルログイン（Single Logon）]：（ローカル＋リモート：1）VPN 接続全体で、ログインできるユーザは1人だけです。VPN接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第2のユーザがログインすると、VPN接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

（注） 複数同時ログオンはサポートされません。

- [シングルログイン（リモートなし）（Single Logon No Remote）]：（ローカル：1、リモート：0）VPN 接続全体で、ログインできるローカルユーザは 1 人だけです。リモートユーザは許可されません。VPN接続の確立時に、複数のローカルユーザまたはリモートユーザがログインしている場合、接続は許可されません。VPN接続中に第2のローカルユーザまたはリモートユーザがログインすると、VPN接続が終了します。

- [Linux VPN 確立（Linux VPN Establishment）]：SSH を使用してクライアント PC にログインしたユーザーが VPN 接続を確立した場合の Cisco Secure Client の動作を決定します。設定可能な値は次のとおりです。
  - [ローカル ユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは VPN 接続を確立できません。
  - [リモート ユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。

- [スマートカード PIN のクリア（Clear SmartCard PIN）]：この機能をサポートするのは特定のスマートカードのみです。これにより、スマートカードのユーザーは、追加の PIN プロンプトなしでスマートカードを使用していた別のユーザによって最近既にロックが解除されている場合でも、VPN 認証中に PIN を再入力する必要があります。
- [サポートされているIPプロトコル（IP Protocol Supported）]：IPv4 アドレスおよび IPv6 アドレスの両方で Cisco Secure Client を使用して Cisco Secure Firewall ASA に接続しようとしているクライアントの場合、Cisco Secure Client は接続の開始に際してどの IP プロトコルを使用するか決定する必要があります。デフォルトで、Cisco Secure Client は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、Cisco Secure Client は IPv6 を使用して接続を開始しようとします。

このフィールドでは、最初の IP プロトコルとフォールバックの順序を設定します。

- [IPv4]：Cisco Secure Firewall ASA に対して IPv4 接続のみ可能です。
- [IPv6]：Cisco Secure Firewall ASA に対して IPv6 接続のみを確立できます。
- [IPv4、IPv6]：最初に Cisco Secure Firewall ASA に IPv4 接続しようとします。クライアントが IPv4 を使用して接続できない場合、IPv6 接続をしようとします。
- [IPv6、IPv4]：最初に Cisco Secure Firewall ASA に IPv6 接続しようとします。クライアントが IPv6 を使用して接続できない場合、IPv4 接続をしようとします。

（注） IP プロトコルのフェールオーバーも VPN セッション中に行うことができます。フェールオーバーは、VPNセッションの前に実行された場合でも VPN セッション中に実行された場合でも、現在使用されているセキュアゲートウェイのIPアドレスに到達できなくなるまで維持されます。クライアントは、現在使用されている IP アドレスに到達できない場合、代替 IP プロトコル（利用可能な場合）に一致する IP アドレスにフェールオーバーします。

Cisco Secure Client プロファイルエディタ、プリファレンス（Part 2）

- [自動証明書選択の無効化（Disable Automatic Certificate Selection）]（Windows のみ）：クライアントによる自動証明書選択を無効にし、ユーザに対して認証証明書を選択するためのプロンプトを表示します。
- [プロキシ設定（Proxy Settings）]：プロキシサーバーへのクライアントアクセスを制御するために Cisco Secure Client プロファイルにポリシーを指定します。これは、プロキシ設定によってユーザが社内ネットワークの外からトンネルを確立できない場合に使用します。
  - [ネイティブ（Native）]：クライアントは、Cisco Secure Client によって以前に設定されたプロキシ設定とブラウザに設定されたプロキシ設定の両方を使用します。グローバル ユーザ プリファレンスに設定されたプロキシ設定は、ブラウザのプロキシ設定に追加されます。
  - [プロキシを無視（IgnoreProxy）]：ユーザのコンピュータのブラウザのプロキシ設定を無視します。
  - [上書き（Override）]：パブリック プロキシサーバーのアドレスを手動で設定します。パブリック プロキシは、Linux でサポートされている唯一のプロキシです。Windows も、パブリック プロキシをサポートしています。[ユーザ制御可（User Controllable）] になるようにパブリック プロキシ アドレスを設定できます。

- [ローカルプロキシ接続を許可（Allow Local Proxy Connections）]：デフォルトでは、Windows ユーザーは Cisco Secure Client でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシサービスを介して VPN セッションを確立するようになっています。ローカルプロキシ接続のサポートを無効にする場合は、このパラメータをオフにします。トランスペアレントプロキシサービスを提供する要素の例として、一部のワイヤレスデータカードによって提供されるアクセラレーション ソフトウェアや、一部のウイルス対策ソフトウェアに備えられたネットワークコンポーネントなどがあります。

- [最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）]（OGS）、（IPv4 クライアントのみ）：Cisco Secure Client では、ラウンドトリップ時間（RTT）に基づいて接続または再接続に最適なセキュアゲートウェイが特定され、それが選択されます。これにより、ユーザーが介入することなくインターネットトラフィックの遅延を最小限に抑えることができます。OGS はセキュリティ機能ではなく、セキュア ゲートウェイ クラスタ間またはクラスタ内部でのロード バランシングは実行されません。OGS のアクティブ化/非アクティブ化を制御し、エンドユーザがこの機能そのものを制御できるようにするかどうかを指定します。クライアント GUI の [接続（Connection）] タブにある [接続先（Connect To）] ドロップダウン リストには [自動選択（Automatic Selection）] が表示されます。

  - [一時停止時間しきい値（時間）（Suspension Time Threshold (hours)）]：新しいゲートウェイ選択の計算を呼び出す前に VPN を一時停止しておく必要がある最小時間を（時間単位で）入力します。次の設定可能パラメータ（パフォーマンス向上しきい値（Performance Improvement Threshold））と組み合わせてこの値を最適化することで、最適なゲートウェイの選択と、クレデンシャルの再入力を強制する回数の削減の間の適切なバランスを見つけることができます。

  - [パフォーマンス向上しきい値（%）（Performance Improvement Threshold (%)）]：システムの再開後にクライアントが別のセキュア ゲートウェイに再接続する際の基準となるパフォーマンス向上率。特定のネットワークに対してこれらの値を調整すれば、最適なゲートウェイを選択することと、クレデンシャルを強制的に入力させる回数を減らすこととの間で適切なバランスを取ることができます。デフォルトは 20% です。

  OGS が有効な場合は、この機能の設定をユーザが行えるようにすることも推奨します。

  OGS には次の制約事項があります。

  - Always-On を設定した状態では動作できません
  - 自動プロキシ検出を設定した状態では動作できません。
  - プロキシ自動設定（PAC）ファイルを設定した状態では動作できません。
  - AAA が使用されている場合は、別のセキュア ゲートウェイへの遷移時にユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。この問題は、証明書を使用すると解消されます。

- [自動 VPN ポリシー（Automatic VPN Policy）]（Windows および macOS のみ）：信頼ネットワーク検出を有効にして、Cisco Secure Client が信頼ネットワークポリシーと非信頼ネットワークポリシーに従って VPN 接続をいつ開始または停止するかを自動的に管理できる

ようにします。無効の場合、VPN 接続の開始および停止は手動でのみ行うことができます。[自動 VPN ポリシー（Automatic VPN Policy）] を設定しても、ユーザは VPN 接続を手動で制御できます。

- [信頼されたネットワークポリシー（Trusted Network Policy）]：ユーザーが社内ネットワーク（信頼ネットワーク）に存在する場合に Cisco Secure Client が VPN 接続で自動的に実行するアクション。
  - [接続解除（Disconnect）]（デフォルト）：信頼ネットワークが検出されると VPN 接続が解除されます。
  - [接続（Connect）]：信頼ネットワークが検出されると VPN 接続が開始されます。
  - [何もしない（Do Nothing）]：非信頼ネットワークでは動作はありません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。
  - [一時停止（Pause）]：ユーザーが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、Cisco Secure Client は VPN セッションを接続解除するのではなく、一時停止します。ユーザーが再び信頼ネットワークの外に出ると、そのセッションは Cisco Secure Client により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

- **[信頼されていないネットワークポリシー（Untrusted Network Policy）]**：ユーザーが企業ネットワークの外（非信頼ネットワーク）に存在する場合、Cisco Secure Client により VPN 接続が自動的に開始されます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。
  - [接続（Connect）]（デフォルト）：非信頼ネットワークが検出されると、VPN 接続が開始されます。
  - [何もしない（Do Nothing）]：信頼ネットワークでは動作はありません。このオプションを指定すると、 Always-OnVPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

- [信頼された DNS ドメイン（Trusted DNS Domains）]：クライアントが信頼ネットワーク内に存在する場合にネットワークインターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。

（注） Network Visibility Module を使用している場合、信頼できる DNS ドメインとサーバーはサポートされません。これは、Network Visibility Module が管理者定義の信頼できるサーバーと証明書ハッシュを使用して、ユーザーが信頼できるネットワーク上にあるかどうかを判断するためです。

- [信頼された DNS サーバー（Trusted DNS Servers）]：クライアントが信頼ネットワーク内に存在する場合にネットワークインターフェイスに割り当てることができる DNS サーバーアドレス（カンマ区切りの IP アドレス）。たとえば、192.168.1.2、2001:DB8::1 です。IPv4 または IPv6 DNS サーバーアドレスでは、ワイルドカード（*）がサポートされています。

- **Trusted Servers @ https://<server>[:<port>]**：信頼できる URL として追加するホスト URL。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラーメッセージが表示されます。

  信頼できる証明書を使用してアクセス可能なセキュア Web サーバーが、信頼できるサーバーとして見なされる必要があります。Secure TND は、リスト内の最初に設定されたサーバーへの接続を試行します。サーバーに接続できない場合、または証明書のハッシュが一致しない場合、セキュア TND は設定済みリスト内の次のサーバーへの接続を試行します。サーバーに接続できて、ハッシュが信頼できる場合、「信頼できる」基準が満たされます。

  証明書が更新または変更された場合、証明書ハッシュは ASDM プロファイル設定で自動的に更新されません。ハッシュを更新するには、サーバーを削除してこのフィールドに再度追加する必要があります。証明書ハッシュまたはサムプリント番号がわかっている場合は、ASDM プロファイルのハッシュ値を更新できます。その後、VPN プロファイルでセキュア TND サーバーを手動で再設定します。予期されるサーバーポリシーが適用されるようにするには、新しいプロファイルをエンドポイントにプッシュする必要があります。これは、サーバー証明書の変更が ASDM またはプロファイルエディタによって自動的に追跡されず、VPN プロファイルに書き込まれないためです。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバーを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバーが定義されていない場合、このフィールドは無効になります。

- [信頼されたネットワークで信頼されたサーバー接続のないインターフェイスを無効にする（Disable interfaces without trusted server connectivity while in trusted network）]（macOS および Linux のみ）：デュアルホームエンドポイントが企業ネットワークか

らパブリックネットワークに切り替わって、企業の個人情報が漏洩しないように、信頼できないインターフェイスを無効にします。プロファイルで Secure Trusted Network Detection を有効にする必要があります。これにより、静的 DNS 設定によって信頼できるネットワークが検出されると、追加のチェックとして HTTPS プローブが構成済みの信頼できるサーバーに送信されます。

これは、信頼できるネットワークと信頼できないネットワークの両方に接続されたデュアルホームデバイスに適用されます。1 つのインターフェイスがプロファイルの信頼できるネットワークポリシーの DNS 設定と一致している必要があり、セキュアな信頼ネットワーク検出プローブがそのインターフェイス上で成功し、信頼できるネットワークに接続されていると見なされる必要があります。エンドポイントが異なる信頼レベルのゾーン（信頼できるネットワークまたは信頼できないネットワーク）に属していることが検出されると、この機能がアクティブになり、信頼できないネットワークへのアクセスが無効になります。

- [常時接続（Always On）]：対応している Windows または macOS オペレーティングシステムのいずれかを実行しているコンピュータにユーザーがログインした場合、Cisco Secure Client が VPN へ自動的に接続するかどうかを判断します。コンピュータが信頼ネットワーク内に存在しない場合にはインターネットリソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーを適用できます。グループ ポリシーおよびダイナミック アクセス ポリシーに Always-On VPN パラメータを設定し、ポリシーの割り当てに使用される一致基準に基づいて例外を指定することにより、この設定を上書きすることもできます。 Cisco Secure Client ポリシーでは Always-On が有効になっているが、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では無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。有効にした後に、追加のパラメータを設定できます。

（注） AlwaysOn は、ユーザによる設定なしで接続が確立し冗長性が動作するシナリオで使用します。そのため、この機能を使用しているときは、[プリファレンス,パート 1（Preferences, part 1）] で自動再接続を有効に設定する必要はありません。

  - [VPNの接続解除を許可（Allow VPN Disconnect）]：Cisco Secure Client で Always-On VPN セッション用の [接続解除（Disconnect）] ボタンが表示されるようにするかどうかを指定します。VPN セッションの中断後に現在の VPN セッションまたは再接続で問題が発生し、パフォーマンスが低下したなどの理由により、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

    [接続解除（Disconnect）] ボタンを使用すると、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPN セッションの確立には必要のないインターネットアクセスからコンピュータを保護す

ることができます。上述した理由により、[接続解除（Disconnect）] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

- [VPNの切断時に次のホストへのアクセスを許可（Allow Access to the Following Hosts with VPN Disconnected）]：[常にオン（Always On）] の間に VPN が切断されたときに、設定されたホストにエンドポイントがアクセスできるようにします。値は、IP アドレス、IP アドレス範囲（CIDR 形式）、または FQDN を指定できるホストのカンマ区切りリストです。設定されたドメインのすべてのサブドメインへのアクセスも許可されます。最大 500 のホストを指定できます。ワイルドカードは使用できません。

  警告：指定された FQDN へのアクセスは、信頼できないネットワークで実行される名前解決に依存します。

- [接続エラーポリシー（Connect Failure Policy）]：Cisco Secure Client が VPN セッションを確立できない場合（到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、[Always-On] および [VPN の接続解除を許可（Allow VPN Disconnect）] が有効の場合にだけ適用されます。[Always-On] を選択した場合、フェールオープン ポリシーはネットワーク接続を許可し、フェールクローズポリシーはネットワーク接続を無効にします。

  - [クローズド（Closed）]：VPN が到達不能の場合にネットワーク アクセスを制限します。この設定の目的は、エンドポイントを保護するプライベートネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。
  - [オープン（Open）]：VPN が到達不能の場合でもネットワーク アクセスを許可します。

⚠

注意 Cisco Secure Client が VPN セッションの確立に失敗した場合は、接続障害クローズドポリシーによりネットワークアクセスは制限されます。このポリシーは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する非常にセキュリティの高い組織向きです。このポリシーでは、スプリット トンネリングによって許可され、ACL によって制限されたすべてのプリンタやテザード デバイスなどのローカル リソース以外のネットワーク アクセスを防止します。ユーザーが VPN を越えてインターネットにアクセスする必要がある場合に、セキュアゲートウェイを利用できないときには、このポリシーを適用すると生産性が低下する可能性があります。Cisco Secure Client はほとんどのキャプティブポータルを検出します。キャプティブ ポータルを検出できない場合、接続障害クローズドポリシーによりすべてのネットワーク接続が制限されます。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープンポリシーを使用して Always-On VPN を展開し、ユーザーを通じて Cisco Secure Client がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPNユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

[接続エラー ポリシー（Connect Failure Policy）] が [クローズド（Closed）] である場合、次の設定を行うことができます。

- [キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]：クライアントによりキャプティブポータル（ホットスポット）が検出された場合、クローズ接続障害ポリシーにより適用されるネットワークアクセスの制限が Cisco Secure Client により解除されます。ホテルや空港では、ユーザがブラウザを開いてインターネットアクセスの許可に必要な条件を満たすことができるようにするため、キャプティブポータルを使用するのが一般的です。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。
- [修復タイムアウト（Remediation Timeout）]： Cisco Secure Client によりネットワークアクセスの制限が解除されるまでの時間（分）。このパラメータは、[キャプティブポータルの修復を許可（Allow Captive Portal Remediation）] パラメータがオンになっており、かつクライアントによりキャプティブ ポー

タルが検出された場合に適用されます。キャプティブ ポータルの通常の要求を満たすことができるだけの十分な時間を指定します（5 分など）。

- [最新のVPNローカルリソースルールを適用（Apply Last VPN Local Resource Rules）]：VPN が到達不能の場合、クライアントでは Cisco Secure Firewall ASA から受信した最後のクライアント ファイアウォールが適用されます。この中には、ローカル LAN 上のリソースへのアクセスを許可する ACL が含まれている場合もあります。

- [キャプティブポータルの修復ブラウザのフェールオーバー（Captive Portal Remediation Browser Failover）]：エンドユーザーが（Cisco Secure Client ブラウザを閉じた後）キャプティブポータルの修復に外部ブラウザを使用できるようにします。
- [手動でのホスト入力を許可する（Allow Manual Host Input）]：ユーザーが、Cisco Secure Client UI のドロップダウン ボックスにリストされていない VPN アドレスを入力できるようにします。このチェックボックスをオフにすると、VPN接続の選択項目は、ドロップダウン ボックスに表示されているものに限定され、ユーザによる新しい VPN アドレスの入力が制限されます。
- [PPP 除外（PPP Exclusion）]：PPP 接続上の VPN トンネルの場合、除外ルートを決定するかどうかとその方法を指定します。クライアントでは、セキュア ゲートウェイより先を宛先としてトンネリングされたトラフィックから、このセキュア ゲートウェイを宛先とするトラフィックを除外できます。除外ルートは、セキュアでないルートとして Cisco Secure Client GUI の [ルートの詳細（Route Details）] 画面に表示されます。この機能をユーザ設定可能にした場合、ユーザは PPP 除外設定の読み取りや変更を行うことができます。
  - [自動（Automatic）]：PPP 除外を有効にします。Cisco Secure Client は、PPP サーバーの IP アドレスを自動的に決定します。
  - [オーバーライド（Override）]：[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで指定された定義済みのサーバー IP アドレスを使用して PPP 除外を有効にします。[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドは、このオーバーライド方式にのみ適用され、[自動（Automatic）] オプションで PPP サーバーの IP アドレスを検出できない場合にのみ使用する必要があります。

    [PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで [ユーザ制御可（User Controllable）] をオンにすると、エンドユーザーは preferences.xml ファイルを使用して IP アドレスを手動で更新できます。
  - [無効（Disabled）]：PPP 除外は適用されません。
- [スクリプトの有効化（Enable Scripting）]：OnConnect スクリプトおよび OnDisconnect スクリプトがセキュリティ アプライアンスのフラッシュ メモリに存在する場合はそれらを起動します。
  - [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）]：スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプトプロセ

スを終了します。たとえば、VPN セッションが終了すると、Cisco Secure Client では実行中の OnConnect スクリプトが終了し、クライアントで新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。

- [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）]：SBL で VPN セッションが確立された場合に OnConnect スクリプトが（存在すれば）起動されるようにします（VPN エンドポイントで Microsoft Windows を実行している場合にのみサポート）。

- [ログオフ時にVPNを保持（Retain VPN On Logoff）]：ユーザが Windows または macOS からログオフした場合に、VPN セッションを維持するかどうかを指定します。
  - [ユーザの強制設定（User Enforcement）]：別のユーザがログインした場合に VPN セッションを終了するかどうかを指定します。このパラメータが適用されるのは、[ログオフ時にVPNを保持（Retain VPN On Logoff）] がオンになっており、かつ VPN セッションが確立されている間に元のユーザが Windows または macOS からログオフした場合のみです。

- [認証タイムアウト値（Authentication Timeout Values）]：接続試行のユーザークレデンシャルを正常に送信した後、クライアントがヘッドエンドからの認証応答を待機する秒数。10 ～ 120 の範囲で秒数を入力します。

（注） クライアントがオペレーティングシステムからクライアント証明書を受け取るように設定されている場合、プロファイルの値は考慮されません。

Cisco Secure Client プロファイルエディタのバックアップサーバー

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップサーバのリストを設定できます。ユーザが選択したサーバで障害が発生した場合、クライアントはリストの先頭にある最適なサーバのバックアップに接続しようとします。それが失敗した場合、クライアントは選択結果の順序に従って [最適なゲートウェイの選択（Optimal Gateway Selection）] リストの残りの各サーバを試します。

（注） ここで設定するバックアップ サーバは、「Cisco Secure Client プロファイルエディタのサーバーリストの追加/編集 （25 ページ）」でバックアップ サーバが定義されていないときに**のみ**、試行されます。サーバのリストで設定されるサーバが優先され、ここにリストされているバックアップ サーバは上書きされます。

[ホストアドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

Cisco Secure Client プロファイルエディタの証明書照合

このペインでは、クライアント証明書の自動選択の詳細設定に使用できるさまざまな属性の定義を有効にします。

証明書一致基準を指定しない場合、Cisco Secure Client は、次の証明書照合ルールを適用します。

- キーの使用状況：Digital_Signature
- 拡張キーの使用状況：Client Auth

仕様に一致する任意の条件がプロファイルで作成される場合、プロファイルに明記されない限り、上記一致ルールのいずれも適用されません。

- [キーの使用状況（Key Usage）]：受け入れ可能なクライアント証明書を選択する場合は、次のような証明書キー属性を使用できます。
  - Decipher_Only：データを復号化します。他のビットは設定されません（Key_Agreement は除く）。
  - Encipher_Only：データを暗号化します。他のビットは設定されません（Key_Agreement は除く）。
  - CRL_Sign：CRL の CA 署名を確認します。
  - Key_Cert_Sign：証明書の CA 署名を確認します。
  - Key_Agreement：キー共有。
  - Data_Encipherment：Key_Encipherment 以外のデータを暗号化します。
  - Key_Encipherment：キーを暗号化します。
  - Non_Repudiation：一部のアクションを誤って拒否しないように、Key_Cert_sign および CRL_Sign 以外のデジタル署名を確認します。

- Digital_Signature：Non_Repudiation、Key_Cert_Sign、およびCRL_Sign以外のデジタル署名を確認します。

- [拡張キーの使用状況（Extended Key Usage）]：次の拡張キーの使用状況設定を使用します。OIDは丸カッコ内に記載してあります。
  - ServerAuth（1.3.6.1.5.5.7.3.1）
  - ClientAuth（1.3.6.1.5.5.7.3.2）
  - CodeSign（1.3.6.1.5.5.7.3.3）
  - EmailProtect（1.3.6.1.5.5.7.3.4）
  - IPSecEndSystem（1.3.6.1.5.5.7.3.5）
  - IPSecTunnel（1.3.6.1.5.5.7.3.6）
  - IPSecUser（1.3.6.1.5.5.7.3.7）
  - TimeStamp（1.3.6.1.5.5.7.3.8）
  - OCSPSign（1.3.6.1.5.5.7.3.9）
  - DVCS（1.3.6.1.5.5.7.3.10）
  - IKE Intermediate

- [カスタム拡張照合キー（最大10）（Custom Extended Match Key (Max 10)）]：カスタム拡張照合キー（もしあれば）を指定します（最大10個）。証明書は入力したすべての指定キーに一致する必要があります。OID形式でキーを入力します（1.3.6.1.5.5.7.3.11など）。

（注） カスタム拡張照合キーを30文字を超えるOIDサイズで作成すると、[OK]ボタンのクリック時に拒否されます。OIDの最大文字数は、30文字です。

- [拡張キーの使用状況が設定されている証明書のみを適合（Match only certificates with Extended key usage）]：以前の動作では、証明書識別名（DN）の照合ルールが設定されると、クライアントは特定のEKU OIDが設定されている証明書と、EKUが設定されていないすべての証明書とを適合させていました。一貫性を保ちながら、より明確にするため、EKUが設定されていない証明書との適合を拒否できます。デフォルトでは、お客様が予想している従来の動作が保持されます。新しい動作を有効にし、適合を拒否するには、チェックボックスをオンにする必要があります。

- [識別名（最大10）（Distinguished Name (Max 10)）]：受け入れ可能なクライアント証明書を選択する際に完全一致基準として使用する識別名（DN）を指定します。
  - [名前（Name）]：照合に使用する識別名（DN）。

- CN：サブジェクトの一般名
- C：サブジェクトの国
- DC：ドメイン コンポーネント
- DNQ：サブジェクトの DN 修飾子
- EA：サブジェクトの電子メール アドレス
- GENQ：サブジェクトの GEN 修飾子
- GN：サブジェクトの名
- I：サブジェクトのイニシャル
- L：サブジェクトの都市
- N：サブジェクトの非構造体名
- O：サブジェクトの会社
- OU：サブジェクトの部署
- SN：サブジェクトの姓
- SP：サブジェクトの州
- ST：サブジェクトの州
- T：サブジェクトの敬称
- ISSUER-CN：発行元の一般名
- ISSUER-DC：発行元のコンポーネント
- ISSUER-SN：発行元の姓
- ISSUER-GN：発行元の名
- ISSUER-N：発行元の非構造体名
- ISSUER-I：発行元のイニシャル
- ISSUER-GENQ：発行元の GEN 修飾子
- ISSUER-DNQ：発行元の DN 修飾子
- ISSUER-C：発行元の国
- ISSUER-L：発行元の都市
- ISSUER-SP：発行元の州
- ISSUER-ST：発行元の州
- ISSUER-O：発行元の会社

- ISSUER-OU：発行元の部署
- ISSUER-T：発行元の敬称
- ISSUER-EA：発行元の電子メール アドレス

- [パターン（Pattern）]：照合する文字列を指定します。 照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

  abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。

- [演算子（Operator）]：この DN で照合する場合に使用する演算子です。
  - [等しい（Equal）]：== と同等
  - [等しくない（Not Equal）]：!= と同等

- [ワイルドカード（Wildcard）]：[有効（Enabled）] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。
- [大文字と小文字を区別（Match Case）]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

関連トピック

証明書照合の設定

Cisco Secure Client プロファイルエディタの [証明書の登録（Certificate Enrollment）]

[証明書の登録（Certificate Enrollment）]によって、Cisco Secure Client がクライアント認証に使用する証明書のプロビジョニングおよび更新を行う場合に、Simple Certificate Enrollment Protocol（SCEP）を使用できるようにします。

- [証明書失効しきい値（Certificate Expiration Threshold）]：Cisco Secure Client が、証明書の有効期限の何日前にユーザーに対して証明書の失効が近づいていることを警告する日数（RADIUS パスワード管理ではサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。

- [クライアント証明書インポートストア（Client Certificate Import Store）]：どの証明書ストアに登録証明書を保存するかを選択します。
  - **Windows**
  - [すべて（All）]：（デフォルト）Windows マシンとユーザの両方の証明書ストアに登録証明書をインポートします。

- [マシン（Machine）]：Windows マシン証明書ストアのみに登録証明書をインポートします。
- [ユーザ（User）]：Windows ユーザ証明書ストアのみに登録証明書をインポートします。
- **Linux**
- [すべて（All）]：（デフォルト）ユーザ PEM ファイルとユーザ Firefox NSS の両方の証明書ストアに登録証明書をインポートします。
- [UserFirefoxNSS]：ユーザ Firefox NSS 証明書ストアのみに登録証明書をインポートします。
- [UserPEMFile]：ユーザ PEM ファイル証明書ストアのみに登録証明書をインポートします。

- **macOS**
- ユーザログインキーチェーンのみに登録証明書をインポートできます。
- **モバイルプラットフォーム**
- アプリケーション サンドボックスのみに登録証明書をインポートできます。

- [証明書の内容（Certificate Contents）]：SCEP 登録要求に含める証明書の内容を指定します。
  - Name (CN)：証明書での一般名。
  - Department (OU)：証明書に指定されている部署名。
  - Company (O)：証明書に指定されている会社名。
  - State (ST)：証明書に指定されている州 ID。
  - State (SP)：別の州 ID。
  - Country (C)：証明書に指定されている国 ID。
  - Email (EA)：電子メール アドレス。次の例では、Email (EA) は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
  - Domain (DC)：ドメイン コンポーネント。次の例では、Domain (DC) は cisco.com に設定されています。
  - SurName (SN)：姓または名。
  - GivenName (GN)：通常は名。
  - UnstructName (N)：定義されていない名前。
  - Initials (I)：ユーザのイニシャル。
  - Qualifier (GEN)：ユーザの世代修飾子。たとえば、「Jr.」や「III」です。

- Qualifier (DN)：完全 DN の修飾子。
- City (L)：都市 ID。
- Title (T)：個人の敬称。たとえば、Ms.、Mrs.、Mr. など。
- CA Domain：SCEP 登録に使用されます。通常は CA ドメイン。
- Key size：登録する証明書用に生成された RSA キーのサイズ。

- [証明書取得ボタンを表示（Display Get Certificate Button）]：次の条件下で Cisco Secure Client GUI が [証明書を取得（Get Certificate）] ボタンを表示できるようにします。
  - 証明書は [証明書失効しきい値（Certificate Expiration Threshold）] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
  - 証明書の期限が切れています。
  - 証明書が存在しません。
  - 証明書を照合できません。

関連トピック

証明書登録の設定

Cisco Secure Client プロファイルエディタの証明書ピン

前提条件

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定には、VPN プロファイルエディタを使用します。[グローバルピン（Global Pins）] セクション内のプリファレンスが有効になっている場合は、サーバーリスト内のホストごとの証明書のみピン留めできます。プリファレンスを有効にすると、クライアントが証明書ピン検証に使用するグローバルピンのリストを設定できます。[サーバーリスト（Server List）] セクションでのホストごとのピンの追加は、グローバルピンの追加と同様です。証明書チェーン内の任意の証明書をピン留めでき、証明書は、ピン留めのために必要な情報を計算するため、プロファイルエディタにインポートされます。

[ピンを追加（Add Pin）]：証明書のプロファイルエディタへのインポートおよびピン留めを手引きする証明書ピン留めウィザードが開始します。

ウィンドウの [証明書の詳細（Certificate Details）] 部分では、[件名（Subject）] 列および [発行元（Issuer）] 列を視覚的に確認することができます。

証明書ピン留めウィザード

ピン留めに必要な情報を指定するため、サーバ証明書チェーンからの任意の証明書をプロファイル エディタにインポートすることができます。プロファイル エディタは、次の 3 つの証明書インポート オプションをサポートしています。

- ローカルのファイルを参照：お使いのコンピュータにローカルに存在している証明書を選択します。
- URL からファイルをダウンロード：任意のファイル ホスティング サーバから証明書をダウンロードします。
- PEM 形式の情報をペースト：証明書の開始および終了ヘッダーを含む PEM 形式の情報を挿入します。

（注） インポートできるのは、データ形式が DER、PEM、および PKCS7 の証明書のみです。

Cisco Secure Client プロファイルエディタのサーバーリスト

クライアント GUI に表示されるサーバ リストの設定を行うことができます。ユーザは、VPN 接続を確立する際、このリストでサーバを選択することができます。

[サーバ リスト（Server List）] テーブルの列は次のとおりです。

- [ホスト名（Hostname）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアス。
- [ホスト アドレス（Host Address）]：サーバの IP アドレスまたは FQDN。
- [ユーザ グループ（User Group）]：[ホスト アドレス（Host Address）] と組み合わせて使用することによりグループ ベースの URL が構成されます。
- [自動 SCEP ホスト（Automatic SCEP Host）]：クライアント認証に使用する証明書のプロビジョニング用および更新用として指定された Simple Certificate Enrollment Protocol。
- [CA URL]：このサーバが認証局（CA）へ接続する際に使用する URL。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「Cisco Secure Client プロファイルエディタの証明書ピン （23 ページ）」を参照してください。

（注） クライアントは、ピン検証の際に、グローバル ピンおよび対応するホストごとのピンを使用します。ホストごとのピンの設定は、証明書ピン留めウィザードの使用によるグローバル ピンの設定と同様に行います。

[追加/編集（Add/Edit）]：上記のサーバのパラメータを指定できる [サーバ リスト エントリ（Server List Entry）] ダイアログを起動します。

[削除（Delete）]：サーバ リストからサーバを削除します。

[詳細（Details）]：サーバのバックアップ サーバまたは CA URL に関する詳細情報を表示します。

関連トピック

VPN 接続サーバーの設定

Cisco Secure Client プロファイルエディタのサーバーリストの追加/編集

- [ホスト表示名（Host Display Name）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアスを入力します。
- [FQDN または IP アドレス（FQDN or IP Address）]：サーバの IP アドレスまたは FQDN を指定します。
  - [ホストアドレス（Host Address）] フィールドに IP アドレスまたは FQDN を指定すると、[ホスト名（Host Name）] フィールドのエントリが Cisco Secure Client トレイフライアウト内の接続ドロップダウンリストに表示されるサーバーのラベルになります。
  - [ホスト名（Hostname）] フィールドで FQDN のみを指定し、[ホスト アドレス（Host Address）] フィールドでは IP アドレスを指定しない場合、[ホスト名（Hostname）] フィールドの FQDN が DNS サーバによって解決されます。
  - IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。
- [ユーザ グループ（User Group）]：ユーザ グループを指定します。

  このユーザ グループとホストアドレスを組み合わせてグループ ベースの URL が構成されます。プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url。

（注） IKEv2/IPsec 接続では、プライマリサーバに到達できない場合、プライマリサーバに入力された**ユーザグループ**情報がバックアップサーバに転送されます。SSL で同じ動作をさせるには、FQDN だけでなく、ユーザグループ情報を URL（https://example.com/usergroup など）としてバックアップサーバに提供する必要もあります。

- [モバイル専用追加設定（Additional mobile-only settings）]：Apple iOS および Android モバイル デバイスを設定する場合に選択します。
- **バックアップ サーバ リスト**

  ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定することをお勧めします。サーバで障害が発生した場合、クライア

ントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストの下方向に移動します。

（注） 逆の面から述べれば、「Cisco Secure Client プロファイルエディタのバックアップサーバー（17ページ）」で設定されるバックアップサーバは、すべての接続エントリのグローバル項目です。プロファイルエディタのバックアップサーバに入力したエントリは、ここで、個々のサーバリストエントリとしてバックアップサーバリストに入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

- [ホストアドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたはFQDNを指定します。クライアントでは、ホストに接続できない場合には、バックアップ サーバへの接続が試行されます。
- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

- **ロード バランシング サーバ リスト**

  このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつAlways-On機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスはAlways-On機能によりブロックされます。

  - [ホスト アドレス（Host Address）]：ロードバランシング クラスタにあるバックアップ デバイスの IP アドレスまたは FQDN を指定します。
  - [追加（Add）]：ロード バランシング バックアップ サーバ リストにアドレスを追加します。
  - [削除（Delete）]：ロード バランシング バックアップ サーバをリストから削除します。

- [プライマリ プロトコル（Primary Protocol）]：このサーバも接続するプロトコル（SSL または IKEv2 を使用した IPsec）を指定します。デフォルトは SSL です。

- [標準認証のみ（IOS ゲートウェイ）（Standard Authentication Only (IOS Gateways)）]：プロトコルとして IPsec を選択した場合、このオプションを選択して、IOS サーバへの接続の認証方式を制限できます。

（注） このサーバーが Cisco Secure Firewall ASA である場合、認証方式を独自の Cisco Secure Client EAP から標準ベースの方式に変更すると、Cisco Secure Firewall ASA でセッションタイムアウト、アイドルタイムアウト、接続解除タイムアウト、スプリットトンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

- [IKE ネゴシエーション中の認証方式（Auth Method During IKE Negotiation）]：標準ベースの認証方式の 1 つを選択します。
  - [IKE ID（IKE Identity）]：標準ベースの EAP 認証方式を選択した場合、このフィールドにグループまたはドメインをクライアントアイデンティティとして入力できます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。デフォルトでは、文字列は *$AnyConnectClient$* です。

- [CA URL]：SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「Cisco Secure Client プロファイルエディタの証明書ピン （23 ページ）」を参照してください。
- [チャレンジ PW のプロンプト（Prompt For Challenge PW）]：有効にすると、証明書をユーザが手動で要求できるようになります。 ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [CA サムプリント（CA Thumbprint）]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注） CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行元の証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

関連トピック

VPN 接続サーバーの設定

Cisco Secure Client プロファイルエディタのモバイル設定

Apple iOS/Android の設定

- [証明書認証（Certificate Authentication）]：接続エントリに関連付けられた証明書認証ポリシー属性は、証明書がこの接続にどのように処理されるかを指定します。有効な値は次のとおりです。
  - [自動（Automatic）]：Cisco Secure Client は、接続がいつなされるかを認証するクライアント証明書を自動で選択します。この場合、Cisco Secure Clientでインストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアントプロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、デバイス ユーザが VPN 接続の確立を試行するたびに実行されます。
  - [手動（Manual）]：Cisco Secure Client は、プロファイルがダウンロードされ、次のいずれかを行うときに、Android デバイスの Cisco Secure Client 証明書ストアで証明書を検索します。
    - Cisco Secure Client は、VPN クライアントプロファイルで定められる基準に一致している証明書に基づく証明書を見つけた場合、証明書を接続エントリに割り当て、接続が確立されたときにその証明書を使用します。
    - 一致する証明書が見つからない場合、証明書認証ポリシーが [自動（Automatic）] に設定されます。
    - 割り当てられた証明書が、何らかの理由で Cisco Secure Client 証明書ストアから削除された場合、Cisco Secure Client は [自動（Automatic）] に証明書認証ポリシーをリセットします。
  - [無効（Disabled）]：クライアント証明書は認証に使用されません。
- [プロファイルがインポートされたときにサーバ リスト エントリをアクティブ化（Make this Server List Entry active when profile is imported）]：VPN 接続がデバイスにダウンロードされたら、サーバ リスト エントリをデフォルトとして定義します。この宛先を設定できるのは、1 つのサーバリストエントリのみです。デフォルトでは、無効に設定されています。

Apple iOS のみの設定

- [Connect on Demand（証明書の認証が必要）（Connect on Demand (requires certificate authorization)）]：このフィールドでは、Apple iOS で提供される Connect on Demand 機能を設定できます。その他のアプリケーションが、ドメイン ネーム システム（DNS）を使用して解決されるネットワーク接続を開始したときに、毎回チェックされるルールのリストを作成できます。

  [Connect on Demand] は、[証明書認証（Certificate Authentication）] フィールドが [手動（Manual）] または [自動（Automatic）] に設定されている場合にのみ使用できるオプショ

ンです。[証明書認証（Certificate Authentication）] フィールドが [無効（Disabled）] に設定されている場合は、このチェックボックスはグレー表示されます。[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび[オンデマンドアクション（On Demand Action）] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

- [ドメインまたはホストと一致（Match Domain or Host）]：ユーザが Connect on Demand ルールを作成するホスト名（host.example.com）、ドメイン名（.example.com）、またはドメインの一部（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。
- [オンデマンドアクション（On Demand Action）]：デバイスユーザーが前の手順で定義されたドメインまたはホストに接続しようとしたときに実行するアクションを次の中から 1 つ指定します。
  - [接続しない（Never Connect）]：このリストのルールに一致しても、iOS は絶対に VPN 接続を開始しません。このリストのルールは他のどのリストよりも優先されます

（注） Connect On Demand が有効の場合、アプリケーションは自動的にこのリストにサーバアドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレスポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。

  - [必要に応じて接続（Connect if Needed）]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続を開始します。
  - [常に接続（Always Connect）]：常時接続動作は、リリースに依存します。
    - Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
    - iOS 7.x では、[常に接続する（Always Connect）] はサポートされていません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
    - 以降のリリースでは、[常に接続する（Always Connect）] は使用されません。設定済みのルールは [必要に応じて接続（Connect if needed）] リストに移動され、それに応じて動作します。
- [追加または削除（Add or Delete）]：[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドに指定されたルールをルール テーブルに追加するか、または選択したルールをルール テーブルから削除します。

Network Visibility Module のプロファイルエディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、またはデュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。収集データを Cisco Secure Cloud Analytics 7.3.1 以前のリリース（または Splunk や同様の SIEM ツール以外のもの）に送信する場合、キャッシュデータは信頼ネットワークに送信はされますが、処理されません。Cisco Secure Cloud Analytics アプリケーションについては、『Cisco Secure Cloud Analytics Enterprise Endpoint License and NVM Configuration Guide』[英語] を参照してください。

TND が Network Visibility Module プロファイルに設定されている場合、信頼ネットワーク検出は Network Visibility Module によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステムログに信頼ネットワーク検出の使用状況が表示されます。

Network Visibility Module プロファイルで TND を直接設定する場合、管理者が定義した信頼できるサーバーと証明書ハッシュによって、ユーザーが信頼できるネットワーク上にいるか、信頼できないネットワーク上にいるかが判別されます。コア VPN プロファイルの信頼ネットワーク検出を設定する管理者は、代わりに、コア VPN プロファイルで信頼された DNS ドメインと信頼された DNS サーバーを設定します。Cisco Secure Client プロファイルエディタ、プリファレンス（Part 2） （9 ページ）

- [デスクトップ（Desktop）] または [モバイル（Mobile）]：Network Visibility Module をデスクトップとモバイルデバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）]：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [ポート（Port）]：コレクタがリッスンするポート番号を指定します。

- [セキュア（Secure）]：Network Visibility Module が DTLS 経由でコレクタにデータを安全に送信するかどうかを決定します。このチェックボックスをオンにすると、Network Visibility Module はトランスポートに DTLS を使用します。DTLS 接続では、DTLS サーバ（コレクタ）証明書がエンドポイントによって信頼されている必要があります。信頼できない証明書はサイレントに拒否されます。

  DTLS サポートには CESA Splunk App v3.1.0 の一部としてのコレクタが必要であり、DTLS 1.2 が最小サポートバージョンです。

- **キャッシュの設定**
  - [最大サイズ（Max Size）]：データベースが到達できる最大サイズを指定します。以前はキャッシュサイズに事前設定の制限がありましたが、プロファイル内で設定できるようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

    サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

  - [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

    日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- **[定期テンプレート（Periodic Template）]**：テンプレートがエンドポイントから送信される間隔を指定します。デフォルト値は 1440 分です。

- [定期的なフローレポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フローレポートが定期送信されます。デフォルトで、Network Visibility Module は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、*n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- **[集約間隔（Aggregation interval）]**：データフローをエンドポイントからエクスポートする間隔を指定します。デフォルト値の 5 秒を使用すると、単一のパケットで複数のデータフローがキャプチャされます。間隔の値が 0 秒の場合は、パケットごとに単一のデータフローが含まれます。有効な範囲は 0 ~ 600 秒です。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンドユーザーへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイムデータとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

キャッシュデータはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または[すべてのネットワーク（all networks）] を選択します。
- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。
  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにかかる時間が削減されるよう、ブロードキャストパケットおよびマルチキャストパケットの収集はオフになっています。ブロードキャストパケットとマルチキャストパケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。
  - [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。
- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時にアクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

  [追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。
  - ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
  - それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
  - より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
  - 選択したコレクションモードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。

- 以前の Cisco Secure Client リリースのプロファイルがそれより後の Cisco Secure Client リリースのプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。

- [名前（Name）]：作成するポリシーの名前を指定します。

- [ネットワーク タイプ（Network Type）]：収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。

- [フロー フィルタ ルール（Flow Filter Rule）]：一連の条件と、すべての条件が満たされたときに実行するアクションを、フローの収集または無視として定義します。最大 25 のルールを設定でき、各ルールに最大 25 の条件を定義できます。[フロー フィルタ ルール（Flow Filter Rule）] リストの右側にある上下ボタンを使用してルールの優先順位を調整し、後続のルールよりも優先的に考慮されるように設定します。[追加（Add）] をクリックし、フロー フィルタ ルールのコンポーネントを設定します。

  - [名前（Name）]：フロー フィルタ ルールの一意の名前。

  - [タイプ（Type）]：各フィルタ ルールには [収集（Collect）] または [無視（Ignore）] が指定されます。フィルタ ルールが満たされた場合に適用するアクション（[収集（Collect）] または [無視（Ignore）]）を決定します。[収集（Collect）] する場合、条件が満たされるとフローが許可されます。[無視（Ignore）] する場合、フローはドロップされます。

  - [条件（Conditions）]：照合する各フィールドのエントリと、合致と見なすのはそのフィールド値が等しいときか等しくないときか、判断する操作を追加します。各操作にはフィールド識別子とそのフィールドに対応する値が含まれます。フィールドの一致では、フィルタ エンジン ルールの設定でルール セットに大文字と小文字を区別しない操作（EqualsIgnoreCase）を適用しない限り、大文字と小文字が区別されます。有効にした後、ルール下で設定された値フィールドへの入力は、大文字と小文字が区別されません。

- **[包含（Include）]/[除外（Exclude）]**

  - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドはすべて収集されます。どのフィールドもオンになっていない場合は、フィールドはすべて収集されます。

  - [フィールド（Fields）]：エンドポイントから受信する情報と、ポリシー要件を満たすためにデータ収集に含めるフィールドを決定します。ネットワークタイプ、およびどのフィールドを含めるか、または除外するかに基づいて、Network Visibility Module はエンドポイント上で適切なデータを収集します。

（注） 次のシナリオのいずれかが存在する場合、アップグレード中に、ProcessPath、ParentProcessPath、ProcessArgs、および ParentProcessArgs はデフォルトで、フロー情報でレポートされないように除外されます。

- 古いバージョンの Network Visibility Module のプロファイルにデータ収集ポリシーがない場合、またはデータ収集ポリシーが含まれていない場合。
- 古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあり、新しいバージョンのプロファイルエディタでプロファイルが開かれて保存された場合。古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあったが、新しい 4.9 以降のバージョンのプロファイルエディタでプロファイルが開かれて保存されていない場合は、次の 4 つのフィールドが含まれます。

Network Visibility Module が親プロセス ID を計算できない場合、値はデフォルトで 4294967295 になります。

FlowStartMsec と FlowStopMsec は、フローのエポックタイムスタンプをミリ秒単位で決定します。

インターフェイスの状態と SSID を選択して、インターフェイスのネットワーク状態が信頼できるかどうかを指定できます。

- [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードを、プライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。次に、実際の値ではなく、値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

  包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- [Knoxのデータ収集ポリシー（モバイルのみ）（Data Collection Policy for Knox (Mobile Specific)]：モバイルプロファイルを選択した場合にデータ収集ポリシーを指定するオプションです。Knox コンテナのデータ収集ポリシーを作成するには、[範囲（Scope）] の下の [Knox のみ（Knox-Only）] チェックボックスをオンにします。[デバイスの範囲（Device Scope）] で適用されるデータ収集ポリシーは、別の Knox コンテナデータ収集ポリシーが指定されていない限り、Knox コンテナトラフィックの場合も適用されます。データ収集ポリシーを追加または削除するには、前述の [データ収集ポリシー（Data Collection Policy）] の説明を参照してください。モバイルプロファイルでは最大 6 つの異なるデータ収集ポリシー（デバイス用に 3 つ、Knox 用に 3 つ）を設定できます。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、Network Visibility Module が設定されると、ユーザーに対して表示されるようになります。リモートユーザーは、Network Visibility Module アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して Network Visibility Module を制御します。

- [モバイルネットワークでのエクスポート（Export on Mobile Network）]（オプションおよびモバイルのみ）：デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローのエクスポートを許可するかどうかを指定します。有効な場合（デフォルト値）、エンドユーザーは、[利用許可ポリシー（Acceptable User Policy）] ウィンドウが表示されているとき、または後で Cisco Secure Client Android アプリケーションで **[設定（Settings）] > [NVM 設定（NVM-Settings）] > > [NVM にモバイルデータを使用する（Use mobile data for NVM）]** チェックボックスをオンにして、管理者を上書きできます。[モバイルネットワークでのエクスポート（Export on Mobile Network）] チェックボックスをオフにすると、デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローがエクスポートされず、エンドユーザーはそれを変更できません。

- [信頼ネットワーク検出（Trusted Network Detection）]：この機能は、エンドポイントが物理的に社内ネットワーク上にあるかどうかを検出します。ネットワークの状態は、いつデータをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために Network Visibility Module によって使用されます。[設定（Configure）] をクリックして、信頼ネットワーク検出の設定を行います。SSL プローブが設定済みの信頼できるヘッドエンドに送信され、到達可能であれば、証明書で応答します。次に、サムプリント（SHA-256 ハッシュ）が抽出され、プロファイル エディタのハッシュ セットと照合されます。一致が見つかった場合はエンドポイントが信頼ネットワーク内にあることを意味します。ただし、ヘッドエンドが到達不能である場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼されていないネットワーク内にあると見なされます。

（注） 内部ネットワーク外から操作している場合、信頼ネットワーク検出は DNS 要求を行い、設定されたサーバーへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

1. **https://**：信頼されている各サーバの URL（IP アドレス、FQDN、またはポート アドレス）を入力し、[追加（Add）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

2. [証明書ハッシュ（SHA-256）（Certificate Hash (SHA-256)）]：信頼されているサーバへのSSL接続が成功した場合、このフィールドは自動的に入力されます。それ以外の場合は、サーバ証明書の SHA-256 ハッシュを入力して [設定（Set）] をクリックすることにより手動で設定できます。
3. [信頼されているサーバのリスト（List of Trusted Servers）]：このプロセスで複数の信頼されているサーバを定義できます（最大値は 10 です）。サーバは、設定されている順序で信頼ネットワーク検出に対して試行されるため、[上に移動（Move Up）] ボタンと [下に移動（Move |Down）] ボタンを使用して順序を調整できます。エンドポイントが最初のサーバに接続できなかった場合は、2 番目のサーバという順序で試行されます。リスト内のすべてのサーバをした後、エンドポイントは 10 秒待機してからもう一度途最終試行を行います。サーバが認証されると、エンドポイントは信頼ネットワーク内で考慮されます。

プロファイルを `NVM_ServiceProfile.xml` として保存します。この名前でプロファイルを保存する必要があります。そうしないと、Network Visibility Module はデータの収集と送信に失敗します。

Cisco Secure Client ローカルポリシー

AnyConnectLocalPolicy.xml は、AnyConnect VPN インストーラを使用してクライアントに自動的にインストールされるファイルで、いくつかのデフォルトのセキュリティ値が含まれています。このファイルは、Cisco Secure Firewall ASA によって展開されません。Cisco Secure Client がその UI からインストールされるときに、SecureX から、この AnyConnectLocalPolicy.xml ファイルを展開できます。ユーザーのシステムに既存のローカルポリシーファイルに変更を加えた場合は、変更を有効にするために再起動する必要があります。

ローカルポリシー設定

VPN ローカルポリシーエディタで、`AnyConnectLocalPolicy.xml` ファイルに含める次の設定を指定できます。

- **FIPS モード（FIPS Mode）**

  クライアントの FIPS モードを有効にします。この設定は、FIPS 標準で承認されているアルゴリズムおよびプロトコルだけを使用するようにクライアントに強制します。

- **ダウンローダのバイパス**

  オンにすると、ダイナミック コンテンツのローカル バージョンの存在を検出し、アップデートする VPNDownloader.exe モジュールの起動を無効にします。クライアントは、変換、カスタマイズ、オプションモジュール、コアソフトウェア更新など、Cisco Secure Firewall ASA のダイナミックコンテンツをチェックしません。

  [ダウンローダーのバイパス（Bypass Downloader）] をオンにすると、Cisco Secure Firewall ASA へのクライアント接続時に、次の 2 つのことのいずれかが行われます。

- Cisco Secure Firewall ASA 上の VPN クライアントプロファイルがクライアント上のものと異なる場合、クライアントは接続の試行を中断します。
- Cisco Secure Firewall ASA に VPN クライアントプロファイルが存在しない場合でもクライアントは VPN 接続を行いますが、クライアントにハードコードされた VPN クライアントプロファイル設定を使用します。

（注） Cisco Secure Firewall ASA で VPN クライアントプロファイルを設定する場合は、BypassDownloader を true に設定した Cisco Secure Firewall ASA に接続する前に、クライアントプロファイルをクライアントにインストールしておく必要があります。プロファイルには管理者が定義したポリシーを含めることができるため、BypassDownloader 設定 true は、Cisco Secure Firewall ASA を使用してクライアントプロファイルを集中管理しない場合に限りお勧めします。

- **CRL チェックの有効化（Enable CRL Check）**

  この機能は *Windows* デスクトップでのみ実装されます。SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。この設定を有効にすると、Cisco Secure Client はチェーン内のすべての証明書を対象とした最新の CRL を取得します。Cisco Secure Client は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認します。認証局（CA）によって失効された証明書であることが判明すると、AnyConnect は接続しません。

  CRL チェックは、デフォルトでは無効です。Cisco Secure Client が CRL チェックを実行するのは、[CLRチェックの有効化（Enable CRL Check）] がオンである場合（有効な場合）だけであるため、エンドユーザーに対し次のような状況が発生することがあります。

  - CRL によって証明書が失効した場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が無効になっている場合でも、セキュア ゲートウェイへの接続は無条件で失敗します。
  - 到達できない CRL 配布ポイントなどが原因で CRL を取得できない場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が有効になっていると、セキュア ゲートウェイへの接続は無条件で失敗します。[厳格な証明書トラスト（Strict Certificate Trust）] が無効な場合は、ユーザーに対しエラーを無視するように求められることがあります。

（注） Cisco Secure Client は、[常時接続（Always On）] が有効な場合は CRL チェックを実行できません。CRL 配布ポイントがパブリックに到達不能な場合、Cisco Secure Client でサービスの中断が発生することがあります。

- **OCSP チェックの有効化（Enable OCSP Check）**

  この機能は *Linux* にのみ実装されています。この機能により、クライアントはリアルタイムで個々の証明書のステータスを照会できます。その際、OSCP レスポンダにリクエストを送信してOCSP応答を解析し、証明書のステータスを取得します。OCSPは証明書チェーン全体を検証するために使用され、PEM ファイル証明書ストアと一緒の場合にのみ機能します（[FireFoxのNSS証明書ストアの除外（Exclude Firefox NSS Cert Store）] を *True* に設定します）。OCSP レスポンダにアクセスする際、証明書ごとに 5 秒のタイムアウト間隔があります。

  OCSP チェックは、デフォルトで無効になっています。有効にすると、エンドユーザ—は次のことを確認できます。

  - OCSPによって証明書失効が確認されると、AnyConnectローカルポリシーファイルで[厳格な証明書トラスト（Strict Certificate Trust）] が無効になっている場合でも、ゲートウェイへの接続は無条件で切断されます。
  - OCSP レスポンダに到達できない場合、AnyConnect ローカルポリシーファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が有効になっていると、セキュアゲートウェイへの接続は無条件で切断されます。[厳格な証明書トラスト（Strict Certificate Trust）] が無効な場合は、ユーザーに対しエラーを無視するように求められることがあります。

（注） [常時接続（Always On）] が有効になっている場合、Cisco Secure ClientはOCSPチェックを実行しません。また、OCSP レスポンダがパブリックに到達不能な場合、Cisco Secure Client でサービスの中断が発生することがあります。

- **厳格な証明書トラスト（Strict Certificate Trust）**

  選択すると、リモート セキュリティ ゲートウェイを認証するときに、Cisco Secure Client は確認できない証明書を許可しません。ユーザーにこれらの証明書を受け入れるように求める代わりに、クライアントは自己署名証明書を使用したセキュリティゲートウェイの接続に失敗し、「`Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.`」を表示します。 オフにすると、クライアントはユーザーに証明書を受け入れるように求めます。これはデフォルトの動作です。

  以下の理由があるため、Cisco Secure Clientに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

  - 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザーが接続している場合に「中間者」攻撃を防ぐために役立ちます。
  - 完全に検証可能で信頼できる証明書を使用する場合でも、Cisco Secure Client は、デフォルトでは、未検証の証明書の受け入れをエンドユーザーに許可します。エンドユーザーが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエ

ンドユーザーに求めます。エンドユーザーによるこの判断を回避するには、厳格な証明書トラストを有効にします。

- **サーバ証明書ストアの制限（Restrict Server Cert Store）**（Windows、macOS、および Linux）

  クライアントがユーザーベースの証明書ストアを使用してサーバ証明書を検証できないようにします。システムベースの証明書ストアのみが使用されます。これを有効にすると、<StrictCertificateTrust> も有効になり、true に設定されます。

- **プリファレンス キャッシングの制限（Restrict Preference Caching）**

  Cisco Secure Client は機密情報をディスクにキャッシュしないように設計されています。このパラメータを有効にすると、Cisco Secure Client プリファレンスに保存されているすべての種類のユーザー情報に、このポリシーが拡張されます。

  - [クレデンシャル（Credentials）]：ユーザー名および第2ユーザー名はキャッシュされません。
  - [サムプリント（Thumbprints）]：クライアントおよびサーバ証明書のサムプリントはキャッシュされません。
  - [クレデンシャルとサムプリント（CredentialsAndThumbprints）]：証明書のサムプリントおよびユーザー名はキャッシュされません。
  - [すべて（All）]：自動プリファレンスはいずれもキャッシュされません。
  - [false]：すべてのプリファレンスがディスクに書き込まれます（デフォルト）。

- **Web 展開の更新を制限する** — 更新の制限のレベルを定義できます。以下の 「ポリシーの更新」パラメータと連携して、信頼できる Cisco Secure Firewall ASA のリストを作成し、それらの信頼できる ASA からポリシー、ヘルプファイル、変換、スクリプトをダウンロードするように選択して、ダウンローダーの配布を信頼できる Cisco Secure Firewall ASA ソースのみに制限することもできます。次の設定により、VPN プロファイルの更新およびソフトウェアの更新機能を維持しながら、特定のダウンローダー機能をバイパスできます。または、Cisco Secure Client ダウンローダーの他の機能に影響を与えることなく、Cisco Secure Firewall ASA からのスクリプト、ローカリゼーションファイル、ヘルプファイル、または UI カスタマイズの Web 展開を無効にできます。バイパスに設定されている場合、必要な更新はアウトオブバンド ソフトウェア更新メカニズムで行う必要があります。

  - [スクリプトWeb展開の更新の制限（Restrict Script Web-deploy Updates）]：管理者がサーバからの接続時のスクリプトの更新をカスタマイズできないようにします。
  - [リソースWeb展開の更新の制限（Restrict Resource Web-deploy Updates）]：管理者がサーバからのユーザーインターフェイス要素の更新をカスタマイズできないようにします。
  - [ヘルプWeb展開の更新の制限（Restrict Help Web-deploy Updates）]：管理者がサーバからのヘルプファイルの更新をカスタマイズできないようにします。

- [ローカリゼーションWeb展開の更新の制限（Restrict Localization Web-deploy Updates）]：管理者がサーバからのローカリゼーションの更新をカスタマイズできないようにします。

- **PEM ファイル証明書ストアの除外（Exclude Pem File Cert Store）**（Linux および macOS）

  サーバ証明書の検証とクライアント証明書の検索にクライアントが PEM ファイル証明書ストアを使用できないようにします。

  FIPS 対応の OpenSSL を使用するストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。PEM ファイル証明書ストアを許可することで、リモートユーザーは FIPS 準拠の証明書ストアを使用することになります。

- **FireFox の NSS 証明書ストアの除外（Exclude Firefox NSS Cert Store）**（Linux）

  サーバ証明書の検証とクライアント証明書の検索にクライアントが Firefox NSS 証明書ストアを使用できないようにします。

  ストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。

- **ポリシーの更新**

  クライアントがどのヘッドエンドからソフトウェア更新またはプロファイル更新を取得できるかを制御します。デフォルトでは、任意のサーバからの更新の許可は *TRUE* に設定されています。ダウンローダーの配布を信頼できる Cisco Secure Firewall ASA ソースのみに制限するには、[サーバー名（Server Name）]フィールドにサーバー名を追加し、許可しないサーバーの更新を無効にします。以前は、スクリプト、ヘルプファイル、リソース、およびローカリゼーションを含むソフトウェアの更新を許可していましたが、4 つの個別の設定に変更しました。

  - **任意のサーバからのソフトウェア更新を許可（Allow Software Updates From Any Server）**
  - **任意のサーバからのコンプライアンスモジュール更新を許可（Allow Compliance Module Updates From Any Server）**
  - **任意のサーバからの VPN プロファイル更新を許可（Allow VPN Profile Updates From Any Server）**
  - **任意のサーバからの管理 VPN プロファイル更新を許可（Allow Management VPN Profile Updates From Any Server）**
  - **任意のサーバからの ISE ポスチャプロファイル更新を許可（Allow ISE Posture Profile Updates From Any Server）**
  - **任意のサーバからのサービスプロファイル更新を許可（Allow Service Profile Updates From Any Server）**
  - **任意のサーバからのスクリプト更新を許可（Allow Script Updates From Any Server）**
  - **任意のサーバからのヘルプ更新を許可（Allow Help Updates From Any Server）**
  - **任意のサーバからのリソース更新を許可（Allow Resource Updates From Any Server）**

- **任意のサーバからのローカリゼーション更新を許可（Allow Localization Updates From Any Server）**
- **サーバ名（Server Name）**

  このリストに認証されたサーバを指定します。これらのヘッドエンドには、VPN接続時にすべての Cisco Secure Client ソフトウェアとプロファイルの完全な更新が許可されます。ServerNameには、FQDN、IPアドレス、ドメイン名、またはワイルドカードを含むドメイン名を使用できます。

- **信頼できる ISE 証明書のフィンガープリント（SHA256）（Trusted ISE Certificate Fingerprints (SHA-256)）**：ポスチャポリシーを取得する前にISEの信頼を確立できます。ISE 証明書、中間 CA 証明書、または ISE 証明書チェーンのルート CA 証明書の SHA256 フィンガープリントを指定できます。SHA256 フィンガープリントは大文字と小文字を区別せず、コロンを使用するか、コロンなしで追加できます。この設定はスクリプト修復に必須です。

MST ファイルでのローカル ポリシー パラメータの有効化

設定できる説明および値については、「ローカルポリシー設定」を参照してください。

ローカル ポリシー パラメータを変更するには、MST ファイルを作成します。MST パラメータ名は、AnyConnect ローカルポリシーファイル（AnyConnectLocalPolicy.xml）の次のパラメータに対応しています。

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

（注） Cisco Secure Client インストールは、ユーザ コンピュータ上にある既存のローカル ポリシー ファイルを自動的には上書きしません。クライアント インストーラが新しいポリシー ファイルを作成できるようにするには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

（注） ローカル ポリシー ファイルへのすべての変更には、システムのリブートが必要になります。

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。