AnyConnect 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 AnyConnect Secure Mobility Client ソフトウェア パッケージには、すべてのオペレーティング システム用のプロファイル エディタが含まれています。AnyConnect クライアント イメージを 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化します。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 AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージのクライアント プロファイル エディタがアクティブ化されます。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 AnyConnect 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 AnyConnect 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 ユーザが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。1 つ以上のプロファイルを作成および設定するには、プロファイル エディタを使用します。AnyConnect には ASDM の一部であるプロファイル エディタが、スタンドアロン Windows プログラムとして組み込まれています。

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

手順

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、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 AnyConnect 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。

AnyConnect VPN プロファイル

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect プロファイルで有効になります。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 モジュールであるネットワーク アクセス マネージャ、ISE ポスチャ、カスタマー エクスペリエンス フィードバック、Web セキュリティの構成設定が含まれています。ASA は、AnyConnect のインストールと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。

ASA または ISE は、すべての AnyConnect ユーザにグローバルにプロファイルを展開するか、ユーザのグループ ポリシーに基づいて展開するように設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのプロファイル ファイルを持ちます。場合により、1 人のユーザに複数の VPN プロファイルを割り当てることがあります。複数の場所で作業するユーザには、複数の VPN プロファイルが必要になります。

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 ファイルには、AnyConnect クライアントが、クライアント GUI の [プリファレンス（Preferences）] タブにユーザ制御可能設定を表示するうえで必要となる情報、およびユーザ、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。

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 Logon 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。

AnyConnect プロファイル エディタ、プリファレンス（Part 1）

- [Start Before Logon の使用（Use Start Before Logon）]（Windows のみ）：Windows のログイン ダイアログボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。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、AnyConnect 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。

- [証明書ストア（Certificate Store）]：AnyConnect がどの証明書ストアで証明書を保存し、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。

  VPN プロファイルの CertificateStore 設定の値は、セキュア ゲートウェイに許容される証明書のタイプによって異なります。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。

  macOS 上で AnyConnect がアクセスできる証明書ストアをさらに絞りこめるようにするには、Windows 用または macOS 用のドロップダウンから証明書ストアを設定できます。macOS のための新しいプロファイル プリファレンスは CertificateStoreMac といい、次の追加された値をサポートします。

  - [すべて（All）]（Windows 用）：1 マシンおよび 1 ユーザ証明書が ASA 設定によって許容されます。
  - [ユーザ（User）]（Windows 用）：2 ユーザ証明書が ASA 設定によって許容されます。
  - [すべて（All）]（macOS 用）：利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。
  - [システム（System）]（macOS 用）：macOS システム キーチェーンおよびシステム ファイル/PEM ストアからの証明書のみを使用します。
  - [ログイン（Log in）]（macOS 用）：ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

- [証明書ストアの上書き（Certificate Store Override）]：ユーザに自分のデバイスに対する管理者権限がない場合、管理者は Windows マシン証明書ストアで証明書を検索するように AnyConnect 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、AnyConnect 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：AnyConnect は、Windows マシン証明書ストア内の証明書を検索します。CertificateStore を [すべて（all）] に設定する場合、CertificateStoreOverride は true に設定する必要があります。
- False：AnyConnect 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）]：AnyConnect の起動時に、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、AnyConnect GUI が最小化されます。
- [ローカル LAN アドレス（Local LAN Access）]：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 AnyConnect クライアント 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）]：AnyConnect クライアントが受信する証明書の共通名が、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。ユーザが設定できるようにした場合は、AnyConnect Secure Mobility 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、AnyConnect 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**
    - DisconnectOnSuspend：AnyConnect では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムの再開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、AnyConnect により VPN 接続の再確立が試行されます。

- [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、AnyConnect 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 AnyConnect 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）：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 ユーザがログインしている場合でも、ローカル ユーザが 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 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）]：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。

- [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が VPN 接続を確立した場合の AnyConnect 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 AnyConnect と同じ機能です。
  - [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。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。
- [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がログオフすると、その VPN 接続は AnyConnect 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）：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 ユーザがログインしている場合でも、ローカル ユーザが 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 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）]：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） 複数の同時ログインは、単一のログイン セッションとして処理されます。ユーザにローカルとリモートの両方のログイン セッションがある場合、ユーザはローカル ユーザとして扱われます。

- [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が VPN 接続を確立した場合の AnyConnect 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。
- **スマートカードのピンのクリア（Clear SmartCard PIN）**
- [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 AnyConnect を使用して ASA に接続しようとしているクライアントの場合、AnyConnect 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、AnyConnect 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、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]：ASA に対して IPv4 接続のみ可能です。
  - [IPv6]：ASA に対して IPv6 接続のみ可能です。
  - [IPv4, IPv6]：最初に 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 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） IPv4 から IPv6、IPv6 から IPv4 プロトコルへ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。プライマリ IP プロトコルが失われると、可能な場合に、セカンダリ IP プロトコルを介して VPN セッションが再確立されます。

AnyConnect 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。

  関連項目：証明書選択の設定

- [プロキシ設定（Proxy Settings）]：プロキシ サーバへのクライアント アクセスを制御するために AnyConnect 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、AnyConnect 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 ユーザは AnyConnect 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、一部のアンチウイルス 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）：AnyConnect 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）：Trusted Network Detection を有効にして、AnyConnect 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 AnyConnect 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、AnyConnect 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 AnyConnect 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）]：ユーザが社内ネットワークの外（非信頼ネットワーク）に存在する場合、AnyConnect 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。
- [信頼された DNS サーバ（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 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 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。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 サーバが、信頼できるサーバとして見なされる必要があります。[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。

（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。

- [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がログインした場合、AnyConnect 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。AnyConnect ポリシーではAlways-On VPN 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。

関連項目：常時接続を使用した VPN 接続の要求

  - [VPN の接続解除を許可（Allow VPN Disconnect）]：AnyConnect 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。

  - [接続エラー ポリシー（Connect Failure Policy）]：AnyConnect が VPN セッションを確立できない場合（ASA が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 AnyConnect 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。AnyConnect 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、ユーザを通じて AnyConnect 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。

関連項目：キャプティブ ポータルについて

[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 AnyConnect 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）]：AnyConnect 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 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。

関連項目：接続障害ポリシーの設定

- [手動でのホスト入力を許可する（Allow Manual Host Input）]：ユーザが、AnyConnect 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 AnyConnect 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。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
  - [無効（Disabled）]：PPP 除外は適用されません。
  - [上書き（Override）]：同様に PPP 除外を有効にします。自動検出による PPP サーバの IP アドレスの取得に失敗し、PPP 除外をユーザ制御可能として設定した場合に選択します。

[PPP 除外（PPP Exclusion）] を有効にした場合は、次も設定します。

- [PPP 除外サーバ IP（PPP Exclusion Server IP）]：PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレス。

- [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、AnyConnect 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 Mac OS 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 Mac OS X 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）]：デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。10 ～ 120 の範囲で秒数を入力します。

AnyConnect プロファイル エディタのバックアップ サーバ

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、「AnyConnect プロファイル エディタのサーバ リストの追加/編集 （22 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。

AnyConnect 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、AnyConnect 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

AnyConnect プロファイル エディタの証明書の登録

証明書登録により、AnyConnect は Simple Certificate Enrollment Protocol（SCEP）を使用してクライアント認証のために証明書をプロビジョニングし、更新できます。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect が、証明書の有効期限の何日前にユーザ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。
- [証明書インポート ストア（Certificate Import Store）]：どの Windows 証明書ストアに登録証明書を保存するかを選択します。

- [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 AnyConnect 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

AnyConnect プロファイル エディタの証明書ピン

前提条件

証明書のピン留めを開始する前のベストプラクティスについては、「証明書のピン留めについて」を参照してください。

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 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 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。

AnyConnect プロファイル エディタのモバイル ポリシー

AnyConnect のバージョン 3.0 以降では、Windows Mobile デバイスをサポートしません。Windows Mobile デバイスに関する情報は、『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5』を参照してください。

AnyConnect プロファイル エディタのサーバ 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。「AnyConnect プロファイル エディタの証明書ピン （20 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 接続サーバの設定

AnyConnect プロファイル エディタのサーバ 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 AnyConnect 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 または group-alias です。
- [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、「AnyConnect プロファイル エディタのバックアップ サーバ （14 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。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして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） このサーバが ASA である場合、認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、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。「AnyConnect プロファイル エディタの証明書ピン （20 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 接続サーバの設定

AnyConnect 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）]：AnyConnect 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、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）]：AnyConnect 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 AnyConnect 証明書ストアで証明書を検索します。

- AnyConnect 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 AnyConnect 証明書ストアから削除された場合、AnyConnect 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

• [3G/WiFi ネットワーク間のローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]：有効（デフォルト）の場合、AnyConnect は、接続が解除された後やデバイスが起動した後、もしくは接続種別（EDGE（2G）、1xRTT（2G）、3G または Wi-Fi など）が変更になった後で、再接続にかかる時間を制限しません。この機能は、ネットワーク全体とのセキュアな接続を維持することで、シームレスなモビリティを提供します。企業への接続が必要で、かつバッテリ寿命の消費が多いアプリケーションには有用です。

[ネットワーク ローミング（Network Roaming）] が無効で、AnyConnect の接続が切断された場合、必要に応じて最大 20 秒まで再接続を試みます。接続できない場合は、デバイス ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

（注） ネットワーク ローミングは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響しません。

• [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、常時接続はサポートされません。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、常時接続は使用されません。設定されたルールは [必要に応じて接続（Connect if Needed）] リストに移動され、それに合わせて動作します。
- [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。

NVM 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。

（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。

TND が NVM 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 NVM 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。ただし、TND が NVM プロファイルに明示的に設定されていない場合、NVM は VPN の TND 機能を使用してエンドポイントが信頼ネットワーク内にあるかどうかを判断します。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 TND の使用状況が表示されます。TND パラメータの設定については、「AnyConnect プロファイル エディタ、プリファレンス（Part 2）（8 ページ）」を参照してください。

- [デスクトップ（Desktop）] または [モバイル（Mobile）]：NVM 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。 モバイルは、将来的にサポートされます。
- **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。
- **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、NVM 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。

- [スロットル レート（Throttle Rate）] : スロットリングは、エンド ユーザ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 AnyConnect リリースのプロファイルがそれより後の AnyConnect 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。このフィールドに入力する文字列はすべて、大文字と小文字が区別されます。

[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がすべて収集され、すべてのフィールドがオフにされます。
  - [フィールド（Fields）]：データ収集ポリシーの一部とするフィールドを決定します。 ネットワーク タイプと包含または除外するフィールドに基づいて、NVM はエンドポイント上で該当するデータを収集します。

    AnyConnect リリース 4.4（およびそれ以降）では、インターフェイスの状態と SSID を選択できるようになりました。これによりインターフェイスのネットワーク状態を信頼する/信頼しないを指定します。
  - [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。これにより、フィールド情報は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）：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」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、NVM が設定されると、ユーザに対して表示されるようになります。リモート ユーザは、NVM 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 NVM を制御します。

- [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NVM 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 NVM 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、TND は DNS 要求を行い、設定されたサーバへの 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。

  TND が NVM プロファイルに設定されておらず、VPN モジュールがインストールされている場合、NVM は VPN の TND 機能を使用して、エンドポイントが信頼ネットワーク内にあるかどうかを判断します。NVM プロファイル エディタの TND 設定には次が含まれます。

  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、NVM はデータの収集と送信に失敗します。

AnyConnect ローカル ポリシー

AnyConnectLocalPolicy.xml は、セキュリティ設定を含む、クライアント上の XML ファイルです。このファイルは、ASA によって展開されません。手動でインストールするか、社内のソフトウェア展開システムを使用してユーザ コンピュータに展開する必要があります。ユーザのシステムで既存のローカル ポリシー ファイルに変更を加えた場合は、そのシステムをリブートする必要があります。

ローカル ポリシー パラメータと値

次のパラメータは、VPN ローカル ポリシー エディタおよび `AnyConnectLocalPolicy.xml` ファイル内の要素です。XML 要素は、山カッコで囲んで表示しています。

（注） ファイルを手動で編集し、ポリシーパラメータを省略した場合、この機能にはデフォルトの動作が適用されます。

- <acversion>

  このファイルのすべてのパラメータを解釈できる AnyConnect クライアントの最小バージョンを指定します。このバージョンよりも古いバージョンの AnyConnect を実行しているクライアントがファイルを読み込むと、イベント ログに警告が記録されます。

  形式は acversion="<version number>" です。

- [FIPS モード（FIPS Mode）] <FipsMode>

  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（Bypass Downloader）] <BypassDownloader>

  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、ASA のダイナミック コンテンツをチェックしません。

  [ダウンローダのバイパス（Bypass Downloader）] をオンにすると、ASA へのクライアント接続時に、次の 2 つの事態のいずれかが発生します。

  - 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。
  - 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） 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 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、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。

- [CLRチェックの有効化（Enable CRL Check）] <EnableCRLCheck>

  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、AnyConnect 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。AnyConnect 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。AnyConnect 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） AnyConnect 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、AnyConnect でサービスの中断が発生することがあります。

- [Web起動の制限（Restrict Web Launch）] <RestrictWebLaunch>

  ユーザは、FIPS 準拠のブラウザを使用して、WebLaunch を開始できません。これを行うためには、AnyConnect トンネルを開始するために使用されるセキュリティ Cookie をクライアントが取得できないようにします。クライアントからユーザに情報メッセージが表示されます。

- [厳格な証明書トラスト（Strict Certificate Trust）] <StrictCertificateTrust>

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、AnyConnect は確認できない証明書を許可しません。ユーザ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. 接続を確立できません。.オフにすると、クライアントはユーザ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、AnyConnect クライアント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、AnyConnect クライアントは、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に許可します。エンドユーザ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 ユーザに求めます。エンド ユーザ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。

- [プリファレンス キャッシングの制限（Restrict Preference Caching）] <RestrictPreferenceCaching>

  AnyConnect 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、AnyConnect 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）]：ユーザ名および第2ユーザ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）。

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

  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、リモートユーザは FIPS 準拠の証明書ストアを使用することになります。

- [Mac のネイティブ証明書ストアの除外（Exclude Mac Native Cert Store）]（macOS のみ）<ExcludeMacNativeCertStore>

  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 Mac ネイティブ（キーチェーン）証明書ストアを使用できないようにします。

- [Firefox の NSS 証明書ストアの除外（Exclude Firefox NSS Cert Store）]（Linux および macOS）<ExcludeFirefoxNSSCertStore>

  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。

- [更新ポリシー（Update Policy）] <UpdatePolicy>

  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。

  - [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）] <AllowSoftwareUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN コア モジュールおよびその他のオプション モジュールのソフトウェア更新を許可または禁止します。

  - [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 AnyServer）]<AllowVPNProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN プロファイル更新を許可または禁止します。

  - [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）]<AllowManagementVPNProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの管理 VPN プロファイル更新を許可または禁止します。

  - [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 AnyServer）] <AllowServiceProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのその他のサービス モジュール プロファイル更新を許可または禁止します。

  - [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）] <AllowISEProfileUpdatesFromAnyServer>

    不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの ISE ポスチャ プロファイル更新を許可または禁止します。

  - [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）] <AllowComplianceModuleUpdatesFromAnyServer>

不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのコンプライアンス モジュール更新を許可または禁止します。

- [サーバ名（Server Name）] <ServerName>

  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AnyConnect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。

ローカル ポリシー パラメータの手動変更

手順

ステップ 1 クライアント インストールから、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のコピーを取得します。

表 *1*：オペレーティング システムと *AnyConnect* ローカル ポリシー ファイルのインストール パス

オペレーティング システム	インストール パス
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

ステップ 2 パラメータ設定を編集します。AnyConnectLocalPolicyファイルを手動で編集するか、AnyConnectプロファイルエディタのインストーラとともに配布されるVPNローカルポリシーエディタを使用できます。

ステップ 3 ファイルを `AnyConnectLocalPolicy.xml` として保存し、社内のソフトウェア展開システムを使用してこのファイルをリモート コンピュータに展開します。

ステップ 4 ローカル ポリシー ファイルへの変更が反映されるように、リモート コンピュータをリブートします。

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 パラメータと値」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） AnyConnect 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。

Enable FIPS ツールによるローカル ポリシー パラメータの有効化

すべてのオペレーティング システムで、シスコの Enable FIPS ツールを使用して、FIPS が有効な AnyConnect ローカル ポリシー ファイルを作成できます。Enable FIPS ツールはコマンド ライン ツールで、実行するには、Windows では管理者権限が必要です。Linux および macOS では、root ユーザとして実行する必要があります。

Enable FIPS ツールのダウンロード元の詳細については、FIPS クライアント用に受け取ったライセンシング情報を参照してください。

Enable FIPS ツールを実行するには、コンピュータのコマンド ラインから EnableFIPS <arguments> コマンドを入力します。Enable FIPS ツールを使用するときは、次のことに注意してください。

- 引数を何も指定しなかった場合、ツールによって FIPS が有効にされ、vpnagent サービス（Windows）または vpnagent デーモン（macOS および Linux）がリスタートされます。
- 複数の引数はスペースで区切ります。

Windows コンピュータ上で実行する Enable FIPS ツールのコマンド例を次に示します。

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

Linux または macOS コンピュータ上で実行するコマンド例を次に示します。

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

次の表に、Enable FIPS ツールで設定できるポリシー設定の例を示します。引数は、AnyConnect ローカル ポリシー ファイルのパラメータに対応します。

ポリシー設定	引数および構文
FIPS モード	fm=[true | false]
ダウンローダのバイパス	bd=[true | false]
WebLaunch の制限	rwl=[true | false]
厳格な証明書トラスト	sct=[true | false]
プリファレンス キャッシングの制限	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
FireFox の NSS 証明書ストアの除外（Linux および macOS）	efn=[true | false]
PEM ファイル証明書ストアの除外 （Linux および macOS）	epf=[true | false]
Mac のネイティブ証明書ストアの除外 （macOS のみ）	emn=[true | false]