CHAPTER 2

AnyConnect Secure Mobility Client の展開

ASA からか、エンタープライズ ソフトウェア管理システム（SMS）を使用して、リモート ユーザに Cisco AnyConnect Secure Mobility Client を展開できます。これら 2 つの事前展開シナリオまたは Web 展開シナリオについて、この章で説明します。

VPN トンネルは、AnyConnect クライアントが VPN API コンポーネントに基づいてダウンローダ プロセスを開始するスタンドアロン起動、または ActiveX/Java コンポーネントが Web ブラウザのクライアントレス ポータルからダウンローダ プロセスを起動する Web 起動のいずれかで開始されます。

この章では、すべての AnyConnect パッケージ ファイル名の説明を記載しています。

- Windows の場合、モジュールごとに標準の Windows インストーラ ファイル（.msi）を提供します。これらのファイルは、msiexec という Windows ユーティリティを使用してインストールされます。特に Web 展開シナリオの場合にインストーラのファイル サイズを減らすため、これらの .msi ファイルが入った自己解凍型 .exe ファイルを提供する場合があります。
- Mac OS X の場合、OS X インストーラ ユーティリティでインストールされる、OS X 標準の .pkg（または .mpkg）インストーラが入ったディスク イメージを提供します。
- Linux の場合、GZIP 圧縮された Tar アーカイブ ファイルである .tgz ファイルを提供します。アーカイブにはインストール ファイルと、ファイルを正しい場所にコピーするインストール スクリプトが入っています。

ASA へセキュアな SSL および IPsec（IKEv2）VPN 接続を行うコア AnyConnect VPN クライアントに加えて、バージョン 3.1 は次のモジュールを備えています。

- ネットワーク アクセス マネージャ
- ポスチャ アセスメント
- テレメトリ
- Web セキュリティ
- AnyConnect Diagnostic and Reporting Tool（DART）
- Start Before Logon（SBL）

AnyConnect クライアント プロファイルの概要

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect 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 モジュールであるネットワーク アクセス マネージャ、ポスチャ、テレメトリ、Web セキュリティの構成設定が入っています。ASA は AnyConnect のインストールおよびアップデート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。

プロファイルは AnyConnect プロファイル エディタを使用して作成されます。プロファイル エディタは ASDM から起動される GUI ベースの設定ツールです。Windows 向けに、ASDM 内蔵のプロファイル エディタの代わりに使用できる、スタンドアロン版のプロファイル エディタもあります。クライアントを事前展開する場合は、ソフトウェア管理システムを使用してコンピュータに展開する、VPN サービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイル エディタを使用して作成できます。

プロファイル エディタの完全インストールでも、ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリ、カスタマー エクスペリエンス フィードバック モジュール、AnyConnect クライアント ローカル ポリシーのスタンドアロン エディタが提供されます。

（注）　セキュリティ上の理由で、クライアント プロファイル XML ファイルを手動で編集するのではなく、プロファイル エディタを使用することをお勧めします。

プロファイルをすべての AnyConnect ユーザにグローバルに展開するか、またはグループ ポリシーに基づいてユーザに展開するように ASA を設定できます。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。1 人のユーザに複数の VPN プロファイルを割り当てる必要があることがあります。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ることがあります。Start Before Login など、一部のプロファイル設定は、グローバル レベルで接続を制御します。その他の設定は特定のグループ ポリシーに一意であり、どのグループ ポリシーがクライアントにダウンロードされたかにより異なります。

（注）　複数のサーバが接続プロファイルに使用できる場合、AnyConnect はプロファイルのサーバ リストを統合し、すべてのサーバをドロップ リストに表示します。ユーザがサーバを選択すると、サーバが表示されるプロファイルが使用されます。一方、接続後は、その ASA 上に設定されているプロファイルが使用されます。

一部のプロファイル設定は、ユーザ 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、クライアント GUI の [Preferences] タブにユーザ制御可能設定を AnyConnect クライアントで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入っています。

Web 展開中、ダウンローダは ASA で設定された AnyConnect プロファイルをエンド ユーザのデバイスの正しい場所にコピーします。事前展開中では、.msi ファイルが入った具体的に名前を指定したディレクトリにプロファイルを配置できます。インストーラは実行時にそれらのファイルを自動的に正しい場所にコピーします。

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。各オペレーティング システムで使用されるファイル名およびパスに関する詳細については、「すべてのオペレーティング システムに対するプロファイルの場所」の表 2-13 を参照してください。クライアント プロファイル作成の詳細については、次の各項を参照してください。

- 「内蔵 AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集」（P.2-3）
- 「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-38）

内蔵 AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集

ここでは、ASDM からプロファイル エディタを起動する方法、およびプロファイルを新規作成する方法について説明します。

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 エディタが入っています。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にします。

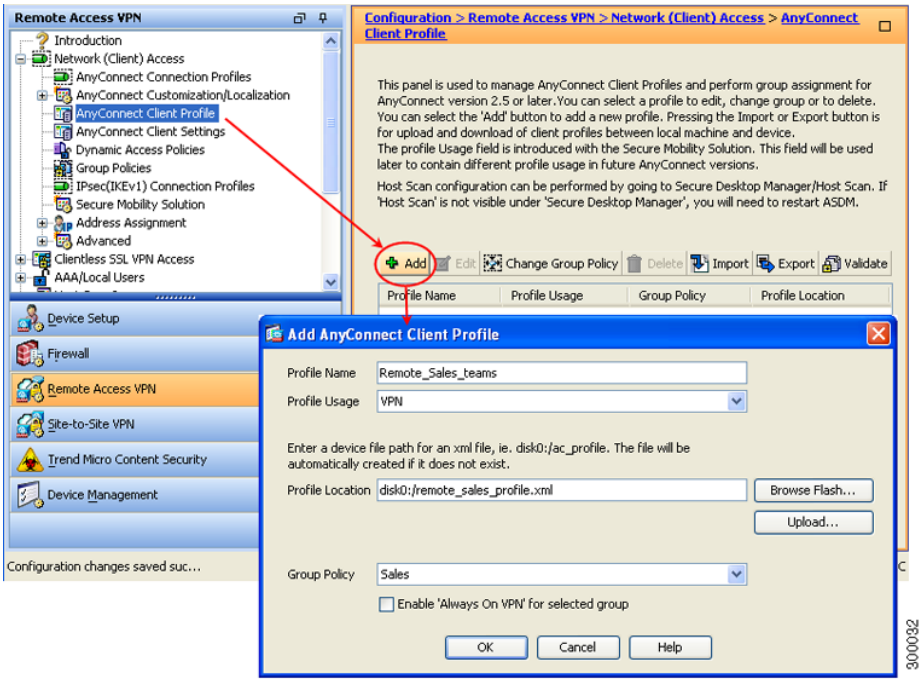
複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからクライアント プロファイル エディタがアクティブにされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

ステップ 1　まだロードしていない場合は、AnyConnect クライアント イメージを ASA にロードします。

「AnyConnect をダウンロードするための ASA の設定」（P.2-15）を参照してください。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。[AnyConnect Client Profile] ペインが開きます。[Add] をクリックします。[Add AnyConnect Client Profile] ウィンドウが開きます。

図 2-1　AnyConnect プロファイルの追加



ステップ 3　プロファイル名を指定します プロファイルの場所として別の値を指定していない場合、ASDM では、ASA フラッシュ メモリ上に同じ名前でクライアント プロファイル ファイルを作成します。

ステップ 4　[Profile Usage] フィールドで、[AnyConnect VPN Profile]、[Network Access Manager Service Profile]、[Web Security Service Profile]、[Telemetry Service Profile]、または [Customer Experience Feedback Profile] のうち、作成しているクライアント プロファイルのタイプを指定します。

ステップ 5　グループ ポリシーを選択します（任意）。ASA は、このプロファイルをグループ ポリシー内の全 AnyConnect ユーザに適用します。

ステップ 6　[OK] をクリックします。ASDM によりプロファイルが作成され、そのプロファイルはプロファイル テーブルに表示されます。

ステップ 7　作成されたばかりのプロファイルをプロファイル テーブルから選択します。[Edit] をクリックします。プロファイル エディタが表示されます。

ステップ 8　プロファイル エディタの各ペインで、AnyConnect 機能を有効にします。終了したら、[OK] をクリックします。

ステップ 9　[Apply] をクリックし、[Save] をクリックします。

ステップ 10　ASDM を終了し、再起動します。

AnyConnect クライアント プロファイルの展開

AnyConnect クライアント プロファイルの ASA からの展開

AnyConnect にプロファイルを展開するには、次の手順に従って ASA を設定します。

ステップ 1　「内蔵 AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集」（P.2-3）に従って、クライアント プロファイルを作成します。

ステップ 2　ASDM に内蔵されたプロファイル エディタを使用して、インストールするモジュールのクライアント プロファイルを作成します。さまざまなクライアント プロファイルの設定手順については、次の章を参照してください。

- 第 3 章「VPN アクセスの設定」

（注）　最初の接続に関するユーザ制御可能なすべての設定をクライアント GUI に表示するには、VPN プロファイル サーバ リストに ASA を含める必要があります。それ以外の場合、フィルタは適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、ASA がそのプロファイルにホスト エントリとして存在しない場合、この証明書照合は無視されます。詳細については、「サーバ リストの設定」（P.3-60）を参照してください。

- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」
- 第 7 章「WSA に対する AnyConnect テレメトリの設定」
- 第 8 章「Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュールの使用」
- 第 9 章「NGE、FIPS、および追加セキュリティ」の AnyConnect ローカル ポリシーのパラメータと値

ステップ 3　クライアント プロファイルとグループ ポリシーを関連付けます。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 4　グループと関連付けるクライアント プロファイルを選択し、[Change Group Policy] をクリックします。

ステップ 5　[Change Group Policy for Profile <*policy name*>] ウィンドウで、[Available Group Policies] フィールドからグループ ポリシーを選択し、右矢印をクリックして [Selected Group Policies] フィールドに移動します。

ステップ 6　[OK] をクリックします。

ステップ 7　[AnyConnect Client Profile] ページで、[Apply] をクリックします。

ステップ 8　[Save] をクリックします。

ステップ 9　設定が終了したら、[OK] をクリックします。

スタンドアロン プロファイル エディタで作成されたクライアント プロファイルの展開

スタンドアロン プロファイル エディタを使用して作成したクライアント プロファイルの展開手順については、「SMS を使用して AnyConnect モジュールを事前展開する」（P.2-25）を参照してください。スタンドアロン AnyConnect プロファイル エディタをインストールして、使用する手順については、「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-38）を参照してください。

Web 展開 AnyConnect

Cisco AnyConnect Secure Mobility Client バージョン 3.1 は、モジュールを AnyConnect クライアント パッケージに統合します。ASA を使用して AnyConnect を展開する場合、ASA はすべてのオプション モジュールも展開できます。Web 展開シナリオでは、インストールとアップグレードは ASA ヘッドエンドで展開されたパッケージの AnyConnect ダウンローダにより自動的に行われます。このシナリオでは、ダウンローダはすでにインストール済みの AnyConnect クライアント（スタンドアロン）または ActiveX/Java コンポーネント（Web 起動）により起動されます。

ASA から展開された場合、リモート ユーザは ASA に最初の SSL 接続を行います。ユーザは、ブラウザでクライアントレス SSL VPN 接続を受け入れるよう設定された ASA の IP アドレスと DNS 名を入力します。ブラウザ ウィンドウにログイン画面が表示され、ユーザがログインおよび認証に成功すると、コンピュータのオペレーティング システムに対応したクライアントがダウンロードされます。ダウンロードした後、クライアントは自動的にインストールと設定を行い、ASA への IPsec（IKEv2）または SSL 接続を確立します。

- 「ASA 展開用の AnyConnect ファイル パッケージ」（P.2-7）
- 「AnyConnect の正常インストールの確認」（P.2-7）
- 「AnyConnect をダウンロードするための ASA の設定」（P.2-15）
- 「追加機能で使用するモジュールの有効化」（P.2-19）
- 「Web 展開時のインストーラの動作の変更」（P.2-15）

要件

Web 展開では、確認にコード署名を使用します。AnyConnect のコード署名証明書のルート証明書は VeriSign により発行され、一般名は「VeriSign Class 3 Public Primary Certification Authority - G5」です。

この証明書のアベイラビリティと正しい設定は、クライアントのオペレーティング システムにより異なります。

Windows

信頼できるルート認証局証明書ストアには、インストールされ、ソフトウェア メーカーについて信頼された AnyConnect のコード署名証明書の VeriSign ルート CA 証明書がなければなりません。通常この証明書は、Microsoft のオペレーティング システム アップデートによりインストールされ、ユーザまたは管理者の操作は必要ありません。

OS X

システム キーチェーンには、インストールされ、ソフトウェア メーカーについて信頼された AnyConnect のコード署名証明書の VeriSign ルート CA 証明書がなければなりません。通常この証明書は、Apple のオペレーティング システム アップデートによりインストールされ、ユーザまたは管理者の操作は必要ありません。

Linux

PEM 証明書ファイル ストアには、インストールされ、ソフトウェア メーカーについて信頼された VeriSign ルート CA 証明書がなければなりません。AnyConnect バージョン 3.0.3 から始まる AnyConnect がインストールされている場合、VeriSign ルート CA 証明書は PEM 証明書ファイル ストアに保存されており、/opt/.cisco/certificates/ca にあります。

証明書がストアにない場合、Linux の Web 展開では次が必要になります。

ステップ 1　Firefox がインストールされている。

ステップ 2　VeriSign Class 3 Public Primary Certification Authority - G5 ルート認証局のトラスト設定に、ソフトウェア メーカーを特定するトラストが含まれている。

最新版の Firefox に、この VeriSign ルート CA 証明書が入っている。AnyConnect クライアントをインストール後、それ以上ユーザまたは管理者の操作は必要ありません。Firefox 証明書ストアに関するこの要件は、Linux への 3.1 AnyConnect クライアントの事前展開（手動）インストールには適用されません。

証明書とトラストが正しくない場合、Web 展開はクライアントをインストールできず、AnyConnect Web ポータルに、ユーザがクライアントを手動でダウンロードし、インストールするためのリンクが表示されます。ユーザは、Firefox ブラウザでトラスト設定を編集して再度やり直すか、単にクライアントをダウンロードして自分でインストールできます。インストール中、クライアントは VeriSign ルートで PEM ストアを設定し、コード署名証明書を確認し、VeriSign ルートを設定します。AnyConnect を起動する場合、コード署名の確認に PEM ストアの VeriSign ルートが使用されます。

Linux Web 展開で Firefox にトラスト設定をするには、次の手順に従います。

1. Firefox ツールバーで、[Edit] -> [Preferences] を選択します。
2. [Advance] タブを選択し、[Encryption] サブタブを選択します。
3. [View Certificates] を選択し、[Authorities] タブを選択します。
4. 下にスクロールして、[VeriSign Class 3 Public Primary Certification Authority - G5] を選択します。
5. [Edit Trust] をクリックし、[This certificate can identify software makers] をオンにします。

制限事項

- ASA にデフォルトの内部フラッシュ メモリ サイズまたはデフォルトの DRAM サイズ（キャッシュ メモリ用）だけしかない場合、ASA 上で複数の AnyConnect クライアント パッケージの格納とロードを行うと、問題が発生することがあります。フラッシュ メモリにパッケージ ファイルを保存するのに十分な容量がある場合でも、クライアント イメージを解凍し、ロードする時に ASA

のキャッシュ メモリが不足する場合があります。AnyConnect を使用する場合の ASA のメモリ要件について、および ASA で行えるメモリ アップグレードについて詳しくは、Cisco ASA 5500 シリーズの最新のリリース ノートを参照してください。

- レガシー クライアントまたはオプション モジュールをアップグレードしている場合、次が発生します。
  - 過去のすべてのバージョンのコア クライアントがアップグレードされ、すべての VPN 設定が保持されます。
  - Cisco SSC 5.x がネットワーク アクセス マネージャ モジュールにアップグレードされ、ネットワーク アクセス マネージャで使用するすべての SSC 設定が保持され、SSC 5.x が削除されます。
  - Cisco Secure Desktop で使用されるホスト スキャン ファイルがアップグレードされ、両者は共存できます。
  - Cisco IPsec VPN クライアントはアップグレードも削除もされません。ただし、両者は共存できます。
  - ScanSafe Web Security 機能はアップグレードされず、共存できません。AnyWhere+ をアンインストールする必要があります。

ASA 展開用の AnyConnect ファイル パッケージ

表 2-1 は、ASA を使用して AnyConnect を展開する場合の AnyConnect ファイル パッケージ名を示します。

表 2-1　ASA 展開用の AnyConnect パッケージ ファイル名

OS	ASA にロードされる AnyConnect 3.1 Web 展開パッケージ名
Windows	anyconnect-win-(ver)-k9.pkg
Mac	anyconnect-macosx-i386-(ver)-k9.pkg
Linux	anyconnect-linux-(ver)-k9.pkg

AnyConnect の正常インストールの確認

AnyConnect Secure Mobility Client がユーザ コンピュータに正常にインストールされたことを確認するには、次の項を確認してください。

- 「自己署名証明書を受け入れるためのエンドポイントの設定」（P.2-8）
- 「AnyConnect トラフィックに対するネットワーク アドレス変換（NAT）の免除」（P.2-9）
- 「非推奨の DES-only SSL 暗号化用 ASA 設定」（P.2-14）
- 「モバイル ブロードバンド カードとの接続」（P.2-14）
- 「グループ ポリシー設定の無効化」（P.2-15）

自己署名証明書を受け入れるためのエンドポイントの設定

Microsoft Internet Explorer の [Security Alert] ウィンドウへの対応

ここでは、Microsoft Internet Explorer の [Security Alert] ウィンドウへの対応として、自己署名証明書を信頼済みルート証明書としてクライアントにインストールする方法について説明します。このウィンドウは、Microsoft Internet Explorer で、信頼済みサイトとして認識されない ASA への接続が確立するときに開きます。[Security Alert] ウィンドウの上半分には、次のテキストが表示されます。

```
Information you exchange with this site cannot be viewed or changed by others.However,
there is a problem with the site's security certificate.The security certificate was
issued by a company you have not chosen to trust.View the certificate to determine
whether you want to trust the certifying authority.
```

手順の詳細

ステップ 1　[Security Alert] ウィンドウの [View Certificate] をクリックします。

ステップ 2　[Install Certificate] をクリックします。

ステップ 3　[Next] をクリックします。

ステップ 4　[Place all certificates in the following store] を選択します。

ステップ 5　[Browse] をクリックします。

ステップ 6　ドロップダウン リストで、[Trusted Root Certification Authorities] を選択します。

ステップ 7　[Next] をクリックします。

ステップ 8　[Finish] をクリックします。

ステップ 9　[Security Warning] ウィンドウで、[Yes] をクリックします。[Certificate Import Wizard] ウィンドウに、インポートが成功したというメッセージが表示されます。

ステップ 10　[OK] をクリックして、このウィンドウを閉じます。

ステップ 11　[OK] をクリックして、[Certificate] ウィンドウを閉じます。

ステップ 12　[Yes] をクリックして、[Security Alert] ウィンドウを閉じます。ASA のウィンドウが開き、証明書が信頼されたというメッセージが表示されます。

Netscape、Mozilla、または Firefox の [Certified by an Unknown Authority] ウィンドウへの対応

ここでは、[Web Site Certified by an Unknown Authority] ウィンドウへの対応として、自己署名証明書を信頼済みルート証明書としてクライアントにインストールする方法について説明します。このウィンドウは、Netscape、Mozilla、または Firefox で、信頼済みサイトとして認識されない ASA への接続が確立するときに開きます。このウィンドウには、次のテキストが表示されます。

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

次の手順にしたがって、信頼済みルート証明書として証明書をインストールします。

ステップ 1　[Web Site Certified by an Unknown Authority] ウィンドウの [Examine Certificate] をクリックします。[Certificate Viewer] ウィンドウが開きます。

ステップ 2　[Accept this certificate permanently] オプションをクリックします。

ステップ 3　[OK] をクリックします。ASA のウィンドウが開き、証明書が信頼されたというメッセージが表示されます。

AnyConnect トラフィックに対するネットワーク アドレス変換（NAT）の免除

ネットワーク アドレス変換（NAT）を実行するように ASA を設定してある場合は、AnyConnect クライアントのトラフィックを変換から除外して、AnyConnect クライアント、内部ネットワーク、DMZ 上のエンタープライズ リソースが、相互にネットワーク接続を開始できるようにする必要があります。AnyConnect クライアント トラフィックを変換の対象外にできないと、AnyConnect クライアントおよび他の企業リソースが通信できなくなります。

「アイデンティティ NAT」（「NAT」免除とも呼ばれている）によりアドレスを自らに変換できます。これにより効果的に NAT が回避されます。アイデンティティ NAT は 2 つのアドレス プール、アドレス プールとサブネットワーク、または 2 つのサブネットワーク間で適用できます。

この手順は、例にあるネットワーク トポロジの次の仮定のネットワーク オブジェクト間でアイデンティティ NAT を設定する方法を示しています。それらは、Engineering VPN アドレス プール、Sales VPN アドレス プール、ネットワーク内、DMZ ネットワーク、およびインターネットです。アイデンティティ NAT 設定ではそれぞれ、NAT 規則が 1 つ必要です。

表 2-2　VPN クライアントのアイデンティティ NAT を設定するネットワーク アドレス アドレッシング

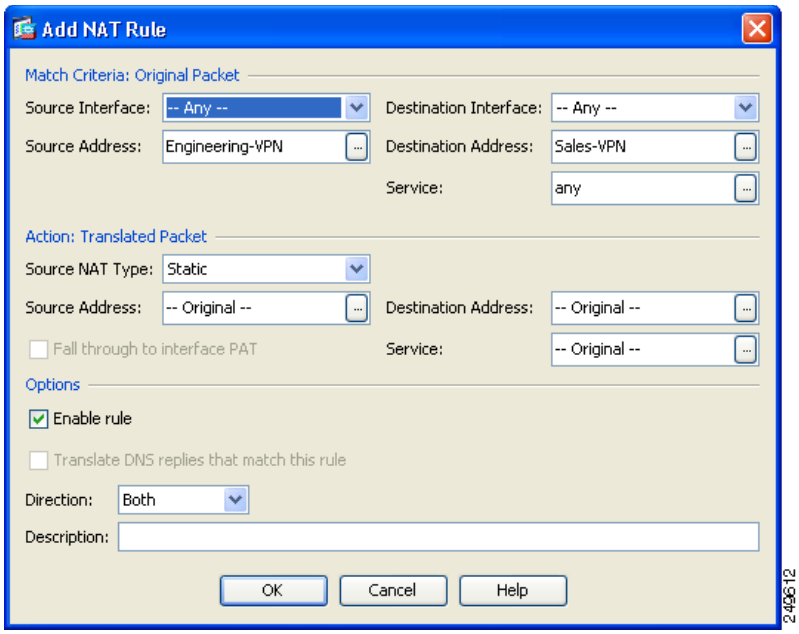
ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

ステップ 1　ASDM にログインし、[Configuration] > [Firewall] > [NAT Rules] を選択します。

ステップ 2　Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則の前にこの規則を評価するよう、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。[Add NAT rule] ダイアログボックスの例については、図 2-2（P.2-10）を参照してください。

（注）　ASA ソフトウェア バージョン 8.3 では、NAT 規則の評価は上から下へ最初に一致したものに適用されます。ASA によりいったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

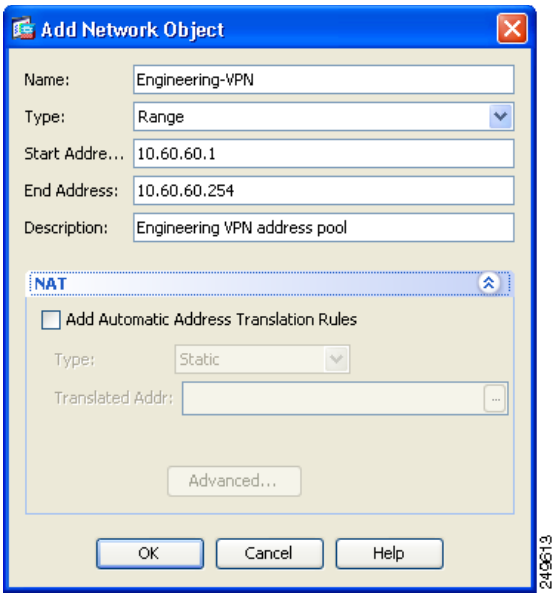
図 2-2　[Add NAT Rule] ダイアログボックス



a. [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。例については、図 2-3 を参照してください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。

図 2-3　VPN アドレス プールのネットワーク オブジェクトの作成



b. [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Static
- [Source Address:] Original
- [Destination Address:] Original
- [Service:] Original

c. [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

d. [OK] をクリックします。

e. [Apply] をクリックします。規則は図 2-5（P.2-14）の「Unified NAT テーブル」の規則 1 のようになるはずです。

CLI の例：

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN
Sales-VPN
```

f. [Send] をクリックします。

ステップ 3　ASA が NAT を実行している場合、同じ VPN プール内の 2 つのホストが互いに接続できるよう、またはそれらのホストが VPN トンネル経由でインターネットに接続できるよう、[Enable traffic between two or more hosts connected to the same interface] オプションを有効にする必要があります。これを行うには ASDM で、[Configuration] > [Device Setup] > [Interfaces] を選択します。[Interface] パネルの下の [Enable traffic between two or more hosts connected to the same interface] をオンにし、[Apply] をクリックします。

CLI の例：

```
same-security-traffic permit inter-interface
```

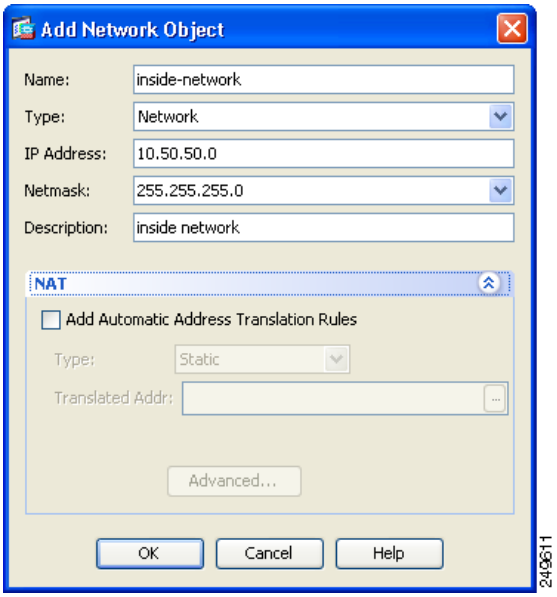
ステップ 4　Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。ステップ 2 で規則を作成したときのようにこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで Engineering VPN アドレス プールを送信元アドレスおよび宛先アドレス両方として指定します。

ステップ 5　Engineering VPN リモート アクセス クライアントが「内部」ネットワークに接続できるよう NAT 規則を作成します。この規則が他の規則の前に処理されるよう [NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

a. [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、内部ネットワークを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**ネットワーク**として定義します。自動アドレス トランスレーション ルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。

図 2-4　inside-network オブジェクトの追加



b. [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Static
- [Source Address:] Original
- [Destination Address:] Original
- [Service:] Original

c. [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

d. [OK] をクリックします。

e. [Apply] をクリックします。規則は図 2-5（P.2-14）の「Unified NAT テーブル」の規則 2 のようになるはずです。

CLI の例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

ステップ 6　ステップ 5 の方法にしたがって新しい規則を作成し、Engineering VPN アドレス プールと DMZ ネットワーク間の接続のアイデンティティ NAT を設定します。DMZ ネットワークを送信元アドレス、Engineering VPN アドレス プールを宛先アドレスとして使用します。

ステップ 7　新しい NAT 規則を作成して、Engineering VPN アドレス プールをトンネル経由にインターネットにアクセスできるようにします。この場合、アイデンティティ NAT は使用しません。送信元アドレスをプライベート アドレスからインターネット ルーティング可能なアドレスに変更するためです。この規則を作成するには、次の手順に従います。

a. この規則が他の規則の前に処理されるよう [NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

b. [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any。[Action: Translated Packet] エリアの [Source Address] に [outside] を選択すると、このフィールドには自動的に「outside」が入力されます。
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。
- [Destination Address:] Any

c. [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Dynamic PAT (Hide)
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、outside インターフェイスを選択します。
- [Destination Address:] Original
- [Service:] Original

d. [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

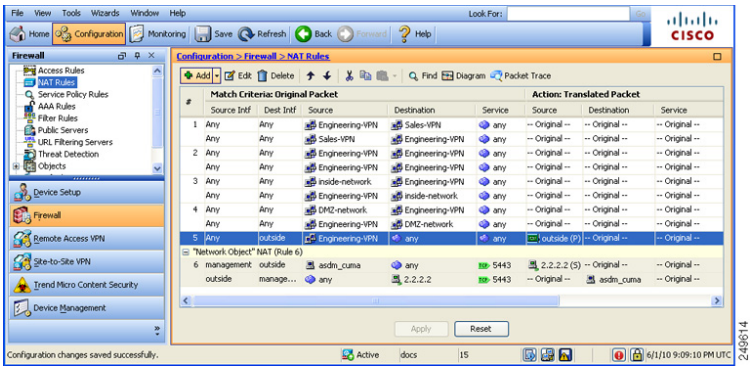
e. [OK] をクリックします。

f. [Apply] をクリックします。規則は図 2-5（P.2-14）の「Unified NAT テーブル」の規則 5 のようになるはずです。

CLI の例：

```
nat (any,outside) source dynamic Engineering-VPN interface
```

図 2-5　Unified NAT テーブル



ステップ 8　Engineering VPN アドレス プールがそのプール自体、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに到達するように設定した後に、Sales VPN アドレス プールについてこのプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プール トラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワーク アドレス変換の対象外となるようにします。

ステップ 9　ASA の [File] メニューで [Save Running Configuration to Flash] を選択し、アイデンティティ NAT 規則を実装します。

非推奨の DES-only SSL 暗号化用 ASA 設定

デフォルトで、Windows Vista および Windows 7 は DES SSL 暗号化に対応していません。ASA に DES-only を設定した場合、AnyConnect 接続は失敗します。DES にこれらのオペレーティング システムを設定するのは難しいため、DES SSL 暗号化のためだけに ASA を設定することはお勧めしません。

モバイル ブロードバンド カードとの接続

一部の 3G または 4g カードには、AnyConnect に接続する前に必要な設定手順があります。たとえば、Verizon Access Manager には、次の 3 つの設定があります。

- モデムの手動接続
- ローミング時以外のモデムの自動接続
- lan adapter auto connect

[lan adapter auto connect] を選択した場合は、プリファレンスを NDIS モードに設定できます。NDIS は、VZAccess Manager が終了されても接続を続行できる、常時接続です。VZAccess Manager では、AnyConnect インストールの準備ができると、自動接続 LAN アダプタをデバイス接続のプリファレンスとして表示します。AnyConnect インターフェイスが検出されると、3G マネージャはインターフェイスをドロップし、AnyConnect 接続を許可します。

優先度の高い接続に移動する場合、有線ネットワークの優先度が最も高くなり、次に wi-fi、モバイル ブロードバンドの順になります。AnyConnect は古い接続を遮断する前に新しい接続を確立します。

グループ ポリシー設定の無効化

AnyConnect を Windows 7 または Windows Vista にインストールする場合、AlwaysInstallElevated または Windows User Account Control（UAC）グループ ポリシー設定のいずれかを無効にする必要があります。

Web 展開時のインストーラの動作の変更

Windows では、トランスフォームを使用して、インストーラ ユーティリティ msiexec によるプロパティ テーブルの解釈方法を変更できます。ASA で、トランスフォーム ファイル（.mst）をアップロードすると、インストール時にダウンローダがそれらのファイルを .msi に適用します（msiexec /package vpn.msi TRANSFORMS=hello.mst など）。

Mac OS X では、.pkg 動作をカスタマイズする一般的な方法はありません。必要なカスタマイズを実装できるようにするため、ACTtransforms.xml を作成し、インストーラとともに配置し、インストーラ実行時に読み取ります。XML ファイルの形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

Linux のインストーラの変更には対応していません。

AnyConnect をダウンロードするための ASA の設定

前提条件

- 「AnyConnect の正常インストールの確認」（P.2-7）の手順を確認して、自社に該当する手順を実行します。
- AnyConnect で機能を有効にすると、新機能を使用するため VPN エンドポイントのモジュールを更新する必要があります。ダウンロード時間を最小限に抑えるため、AnyConnect は、サポートされる各機能に必要なモジュールだけ（ASA から）ダウンロードするよう要求します。展開する AnyConnect パッケージを決定します。

手順の詳細

ステップ 1　Cisco AnyConnect Software Download の Web ページから最新の Cisco AnyConnect Secure Mobility Client パッケージをダウンロードします。AnyConnect ファイル パッケージのリストについては、「ASA 展開用の AnyConnect ファイル パッケージ」（P.2-7）を参照してください。

ステップ 2　Cisco AnyConnect Secure Mobility Client パッケージ ファイルをクライアント イメージとして指定します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Software] を選択します。[AnyConnect Client Software] パネルに AnyConnect イメージとして特定されるクライアント ファイルを一覧表示しています。

ステップ 3　（任意）カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。このフィードバック モジュールにより、お客様が使用し、有効にした機能とモジュールを確認できます。このクライアント情報を収集することでユーザ エクスペリエンスを探り、シスコは AnyConnect の品質、信頼性、パフォーマンス、ユーザ エクスペリエンスを継続して改善できます。この機能を無効にする場合は、ASDM で [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Customized Installer Transforms] を参照しま

す。[Import] を選択すると、サンプル トランスフォームをダウンロードしたり、DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK インストーラ プロパティを設定する自分のトランスフォームを作成したりできます。

ステップ 4　AnyConnect イメージを追加するには、[Add] をクリックします。

- [Browse Flash] をクリックして、ASA にすでにアップロードした AnyConnect イメージを選択します。
- コンピュータ上にローカルに保存した AnyConnect イメージを参照して選択するには、[Upload] をクリックします。

ステップ 5　[OK] または [Upload] をクリックします。

ステップ 6　[Apply] をクリックします。

アドレスの割り当て方式を設定する

DHCP や、ユーザが割り当てたアドレス指定を使用できます。ローカル IP アドレス プールを作成し、そのプールを接続プロファイルに割り当てることもできます。このガイドでは、一般的なアドレス プール方式を例として使用します。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。[Add] ウィンドウにアドレス プール情報を入力します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、[Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below] チェックボックスをオンにします。

ステップ 3　[Connection Profiles] で、[Edit] をクリックし、接続プロファイルで AnyConnect にアドレス プールを割り当てます。

ステップ 4　[Edit AnyConnect Connection Profile] ウィンドウで、クライアント アドレス プールまたはクライアント IPv6 アドレス プールを選択します。

ステップ 5　[Select Address Pools] ウィンドウで [Add] をクリックし、アドレス プールをインターフェイスに割り当てます。

ステップ 6　グループ ポリシーの VPN トンネリング プロトコルとして許可されているクライアントを指定する必要があります。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。[Group Policies] パネルが表示されます。

ステップ 7　[Edit] をクリックし、トンネリング プロトコルとして SSL VPN を選択します。

リモート ユーザへの AnyConnect ダウンロードの要求

リモート ユーザが最初にブラウザで接続している場合、デフォルトでは ASA は AnyConnect をダウンロードしません。ユーザの認証後、デフォルトのクライアントレス ポータル ページに [Start AnyConnect Client] ドロワーが表示され、ユーザが AnyConnect のダウンロードを選択できるようになっています。または、クライアントレス ポータル ページを表示することなく、すぐに AnyConnect をダウンロードするよう ASA を設定できます。

リモート ユーザにプロンプトを表示し、設定された時間内に AnyConnect をダウンロードするか、クライアントレス ポータル ページを表示するよう ASA を設定することもできます。

この機能は、グループ ポリシーまたはユーザに対して設定できます。このようなログイン設定を変更するには、次の手順に従ってください。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。グループ ポリシーを選択して、[Edit] をクリックします。[Edit Internal Group Policy] ウィンドウが表示されます。

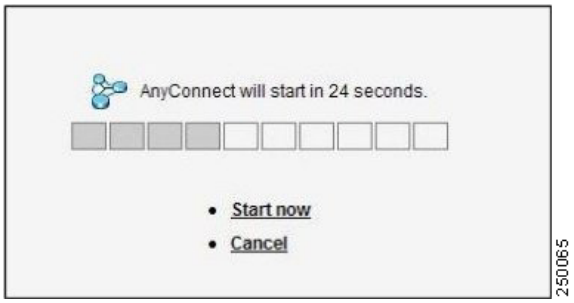
ステップ 2　ナビゲーション ペインで、[Advanced] > [AnyConnect Client] > [Login Settings] を選択します。[Post Login settings] が表示されます。必要に応じて [Inherit] チェックボックスをオフにし、[Post Login setting] を選択します。

ユーザにプロンプトを表示する場合は、タイムアウト時間を指定し、その時間経過後のデフォルト動作を [Default Post Login Selection] エリアで選択します。

ステップ 3　[OK] をクリックし、変更をグループ ポリシーに適用します。

図 2-6 は、[Prompt user to choose] と [Download AnyConnect Client] を選択した場合に、リモート ユーザに表示されるプロンプトを示しています。

図 2-6　リモート ユーザに表示されるログイン後プロンプト



ステップ 4　[Save] をクリックします。

アップグレードに対するユーザ制御

ユーザに強制的にクライアント アップデート行わせたり、後までアップデートを延期させたりできます。

- 自動アップデート：VPN プロファイルで有効にされると、ユーザに強制的にアップデートを行わせます。ユーザが自動アップデートを無効にできるよう AutoUpdate を設定することもできますが、これによりクライアントは、一切アップデートを取得できなくなる可能性があります。

  自動アップデートについては、第 3 章「AnyConnect VPN プロファイル エディタのパラメータに関する説明」で説明します。

- 延期アップデート：クライアント アップデートが可能な場合、AnyConnect は、アップデートを実施するか、延期するかユーザに尋ねるダイアログを開きます。

  延期アップデートは、ASA へカスタム属性を追加し、それらの属性を参照し、グループ ポリシーに設定することで有効になります。すべての Windows、Linux、OS X でサポートされています。

延期アップデートのカスタム属性

次の属性と値により、延期アップデートを設定します。

表 2-3　延期アップデートのカスタム属性

カスタム属性 *	Valid 値	デフォルト値	注意事項
DeferredUpdateAllowed	true false	false	[true] を指定すると、延期アップデートが有効になります。延期アップデートが無効（false）の場合、下記の設定は無視されます。
DeferredUpdateMinimumVersion	x.y.z	0.0.0	アップデートを延期できるようにするため、インストールする必要がある最小バージョンの AnyConnect。 最小バージョンのチェックは、ヘッドエンドで有効になっているすべてのモジュールに適用されます。VPN を含む有効な任意のモジュールがインストールされていない、または最小要件を満たしていない場合、接続して延期アップデートすることはできません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、延期プロンプトが表示されるか（自動的に却下されます）。
DeferredUpdateDismissTimeout	0 ～ 300（秒）	なし（無効）	延期アップグレード プロンプトが表示され、自動的に却下されるまでの秒数。この属性は、延期アップデートプロンプトを表示する場合のみ適用されます（最小バージョンの属性が最初に評価されます）。 この属性が見つからない場合、自動却下機能が無効になり、ユーザが応答するまで（必要に応じて）ダイアログが表示されます。 この属性をゼロに設定すると、次に基づいて強制的に自動延期またはアップグレードが実施されます。 • インストール済みバージョンと DeferredUpdateMinimumVersion の値 • DeferredUpdateDismissResponse の値
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout 発生時に実施するアクション。

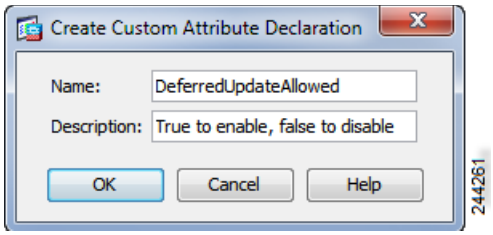
* カスタム属性値は大文字と小文字を区別します。

ASDM での属性の追加

ステップ 1　ASDM に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced > AnyConnect Custom Attributes] を選択します。

ステップ 2　[Add] をクリックし、たとえば次のような Deferred Update のカスタム属性を作成します。

図 2-7　ASA へのカスタム属性の追加



ステップ 3　[Apply] をクリックし、[Save] をクリックします。この手順を繰り返して、カスタム属性のテストを定義できます。

ステップ 4　[Configuration] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 5　Deferred Update に設定するグループ ポリシーを編集するには、[Advanced] > [AnyConnect Client] > [Custom Attributes] を選択します。

ステップ 6　[Add] をクリックします。

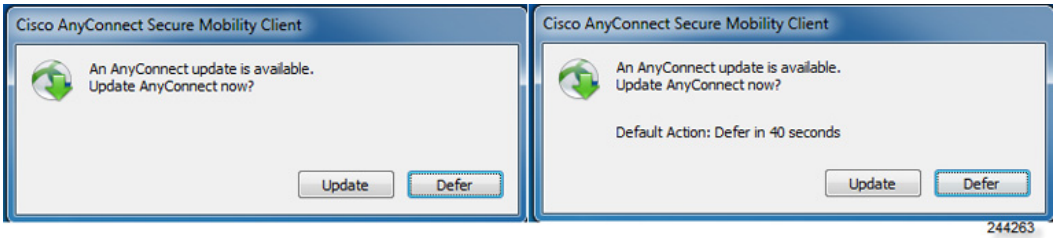
ステップ 7　[Declared Attribute Name] を選択し、設定する属性を選択して設定します。

ステップ 8　残りの Deferred Upgrade カスタム属性をポリシーに追加し、表 2-3（P.2-18）の情報を使用してそれらを設定します。

延期アップデートの GUI

次の図は、アップデートが可能で、Deferred Update が設定されている場合に表示される UI を示します。図の右側は [DeferredUpdateDismissTimeout] が設定されている場合の UI を示しています。

図 2-8　延期アップデートの UI



追加機能で使用するモジュールの有効化

AnyConnect で機能を有効にすると、新機能を使用するため VPN エンドポイントのモジュールを更新する必要があります。ダウンロード時間を最小限に抑えるため、AnyConnect は、サポートされる各機能に必要なモジュールだけ（ASA から）ダウンロードするよう要求します。

新機能を有効にするには、グループ ポリシーまたはユーザ名の設定の一部として、新しいモジュール名を指定する必要があります。グループ ポリシーのモジュール ダウンロードを有効にするには、次の手順に従います。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。グループ ポリシーを選択して、[Edit] をクリックします。[Edit Internal Group Policy] ウィンドウが表示されます。

ステップ 2　ナビゲーション ペインで、[Advanced] > [AnyConnect VPN Client] を選択します。[Client Profiles to Download] で、[Add] をクリックし、関連するプロファイルの使用状況を表示する目的のプロファイル名を選択します。プロファイルの使用状況が次のいずれかとして表示されます。

- [AnyConnect DART] : DART をダウンロードすると、AnyConnect のインストールおよび収集に関する問題のトラブルシューティングに役立つデータを収集できます。
- [AnyConnect Network Access Manager] : このモジュールは、最適なレイヤ 2 アクセス ネットワークを検出して選択し、有線およびワイヤレス ネットワークの両方へのアクセスに対するデバイス認証を実行します。
- [AnyConnect SBL] : Start Before Logon（SBL）モジュールは、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 へのログイン前に企業インフラへ強制的に接続させます。SBL を有効にする理由については、「Start Before Logon の設定」（P.3-13）を参照してください。
- [AnyConnect Web Security] : HTTP トラフィックを、コンテンツ分析、マルウェアの検出、およびアクセプタブル ユース ポリシーの管理を実行する ScanSafe Web Security スキャン プロキシ サーバにルーティングします。
- [AnyConnect Telemetry] : テレメトリ モジュールは、悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス（WSA）の Web フィルタリング インフラストラクチャに送信します。
- [AnyConnect Posture] : AnyConnect Secure Mobility Client に、ASA へのリモート アクセス接続を確立する前に、ホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別する機能を提供します。プリログインの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。ホスト スキャン アプリケーションは、ポスチャ モジュールに同梱される、この情報を収集するアプリケーションです。
- [AnyConnect Customer Experience Feedback] : ソフトウェアの品質やユーザ エクスペリエンスがさらに改善されるよう、ユーザ エクスペリエンス統計情報、クラッシュ インシデントの基本などを探るためのクライアント情報をシスコに提供する機能です。

ステップ 3　[Apply] をクリックし、変更をグループ ポリシーに保存します。

（注）　[Start Before Logon] を選択した場合は、AnyConnect クライアント プロファイルでもこの機能を有効にする必要があります。詳細については、第 3 章「VPN アクセスの設定」を参照してください。

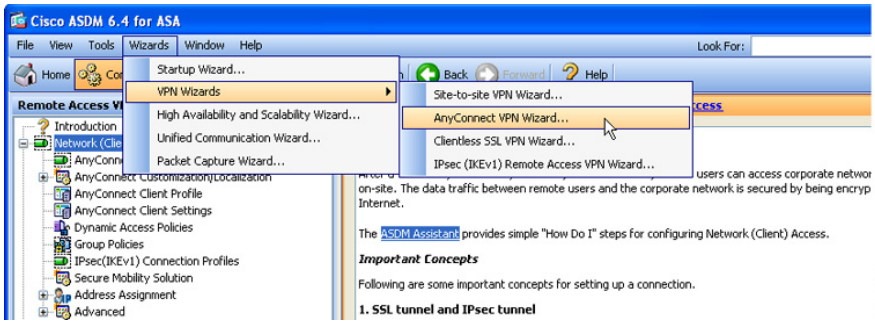
IPsec IKEv2 接続の有効化

ここでは、ASA 上で IPsec IKEv2 接続を有効にする手順を示します。

AnyConnect クライアント パッケージを ASA にロードした後で、次の手順を実行して、ASA に IPsec IKEv2 接続を設定します。

ステップ 1　AnyConnect VPN Wizard を実行します。[Wizards] > [VPN Wizards] > [AnyConnect VPN Wizard] を選択します（図 2-9）。ウィザードに従って IPsec IKEv2 接続の基本 VPN 接続を確立します。

図 2-9　AnyConnect VPN Wizard



ステップ 2　プロファイル エディタを使用して VPN プロファイルのサーバ リスト エントリを編集します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 3　[AnyConnect Client Profile Editor] ウィンドウで [Edit] をクリックし、[Server List] を選択します。

ステップ 4　編集するサーバを強調表示し、[Edit] をクリックし、プライマリ プロトコルを選択します。

ステップ 5　VPN プロファイルと使用するグループ ポリシーを関連付けます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。グループ ポリシーを編集し、[Advanced] > [AnyConnect Client] を選択します。

ステップ 6　[Client Profiles to Download] で、[Add] をクリックし、プロファイル使用状況を選択します。

IKEv2 対応クライアント プロファイルの事前展開

ソフトウェア管理システムを使用してクライアントを事前展開する場合、IKEv2 対応クライアント プロファイルも事前展開する必要があります。手順は次のとおりです。

ステップ 1　Winzip または 7-zip などのユーティリティを使用して .ISO を解凍します。

ステップ 2　次のフォルダを参照します。

anyconnect-win-3.1.0xxx-pre-deploy-k9\Profiles\vpn

ステップ 3　プロファイル エディタ（ASDM バージョンまたはスタンドアロン バージョン）を使用して作成した IKEv2/IPSec VPN プロファイルを、次のフォルダにコピーします。

ステップ 4　Setup.exe を実行して、インストーラを実行し、[Select all] をオフに、[AnyConnect VPN Module] のみをオンにします。

仮想 CD マウント ソフトウェアを使用したクライアント プロファイルの事前展開

SlySoft または PowerISO など仮想 CD マウント ソフトウェアを使用してクライアント プロファイルを事前展開することもできます。手順は次のとおりです。

ステップ 1　.ISO を仮想 CD マウント ソフトウェアにマウントします。

ステップ 2　ソフトウェアのインストール後、プロファイルを適切なフォルダに展開します（表 2-4 を参照）。

表 2-4　クライアントを展開するためのパス

OS	ディレクトリ パス
Windows 7 および Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\
Windows XP	C:\Document and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
Mac OS X および Linux	/opt/cisco/anyconnect/profile/

事前展開に関するその他のヒント

MSI インストーラを使用している場合、MSI はクライアント プロファイル（Profiles\vpn フォルダ）に配置された任意のプロファイルを選択し、インストール中に適切なフォルダに配置します。

インストール後に手動でプロファイルを事前展開する場合は、プロファイルを手動でコピーし、Altiris などの SMS を使用してプロファイルを適切なフォルダに展開します。

クライアントの Weblaunch

AnyConnect クライアントを Weblaunch するには、ASA の URL を次の形式でブラウザに入力して、ログインと AnyConnect クライアントのダウンロードを行うよう、ユーザに指示してください。

```
https://<asa>
```

<asa> は ASA の IP アドレスまたは FQDN です。IP アドレスを使用する場合、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 ゲートウェイの使用はサポートしていません。

AnyConnect の事前展開

エンドポイントが ASA に接続される前に SMS を使用して、AnyConnect ソフトウェアをエンドポイントに配信してインストールする場合、これを「事前展開」と呼びます。事前展開を使用する場合、インストールの順序とその他の詳細について特に注意してください。

- 「事前展開パッケージ ファイル情報」（P.2-23）
- 「Windows コンピュータへの事前展開」（P.2-23）
- 「Linux および Mac OS X コンピュータへの事前展開」（P.2-30）
- 「AnyConnect ファイル情報」（P.2-32）

制限事項

レガシー クライアントまたはオプション モジュールをアップグレードしている場合、次が発生します。

- 過去のすべてのバージョンのコア クライアントがアップグレードされ、すべての VPN 設定が保持されます。
- Cisco SSC 5.x がネットワーク アクセス マネージャ モジュールにアップグレードされ、ネットワーク アクセス マネージャで使用するすべての SSC 設定が保持され、SSC 5.x が削除されます。

- Cisco Secure Desktop で使用されるホスト スキャン ファイルがアップグレードされ、両者は共存できます。
- Cisco IPsec VPN クライアントはアップグレードも削除もされません。ただし、両者は共存できます。
- ScanSafe Web Security 機能はアップグレードされず、共存できません。AnyWhere+ をアンインストールする必要があります。

事前展開パッケージ ファイル情報

AnyConnect VPN クライアントのコア モジュールおよびオプション モジュール（SBL、AnyConnect AnyConnect Diagnostic Reporting Tool など）は、独自のインストール ファイルまたはプログラムによってインストール、更新されます。AnyConnect バージョン 3.1 の場合、Windows デスクトップ インストール ファイルは、ISO イメージ（*.iso）に含まれています。その他のすべてのプラットフォームの場合は、AnyConnect バージョン 2.5 以前の場合と同じ方法で個々の任意のインストール ファイルを、任意の方法で個別に配布できます。

OS	AnyConnect 3.1 事前展開パッケージ名
Windows	anyconnect-win-<*version*>-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux	anyconnect-linux-<*version*>-k9.tar.gz

Windows コンピュータへの事前展開

Windows コンピュータ（モバイルではなくデスクトップ）用の AnyConnect 3.1 事前展開インストールは、ISO イメージで配布されます。この ISO パッケージ ファイルは、*インストール ユーティリティ*（個々のコンポーネント インストーラを起動するセレクタ メニュー プログラム）AnyConnect のコア モジュールとオプション モジュール用の MSI を含みます。

以下の項では、Windows コンピュータに事前展開する方法について説明します。

- 「ISO ファイルの使用」（P.2-23）
- 「ガイドラインと制限事項」（P.2-24）
- 「事前展開にインストール ユーティリティを使用する」（P.2-25）
- 「SMS を使用して AnyConnect モジュールを事前展開する」（P.2-25）
- 「事前展開中のインストーラ動作の変更」（P.2-30）

ISO ファイルの使用

事前展開パッケージは、ユーザ コンピュータに展開するプログラムと exec インストーラ ファイルが入った ISO パッケージ ファイルに同梱されています。ISO パッケージ ファイルを展開する場合、セットアップ プログラム（setup.exe）が [Install Utility] メニューを実行し、展開します。このメニューは、ユーザがインストールする AnyConnect モジュールを選択できる便利な GUI です。

必要に応じて、ISO イメージから個々のインストーラを取り出して、手動で配布することもできます。事前展開パッケージ内の各インストーラは、個別に実行できます。AnyConnect コア クライアントの .msi インストーラを開始する場合、管理者はエンド ユーザ ライセンス契約書（EULA）を承諾する必要があります。ファイルを展開する順序は、非常に重要です。詳細については、SMS を使用して

AnyConnect モジュールを事前展開するを参照してください。

ファイル	目的
GUI.ico	AnyConnect アイコン画像。
Setup.exe	インストール ユーティリティ（setup.hta）を起動します。
anyconnect-dart-win-<*version*>-k9.msi	DART オプション モジュール用 MSI インストーラ ファイル。
anyconnect-gina-win-<*version*>-pre-deploy-k9.msi	SBL オプション モジュール用 MSI インストーラ ファイル。
anyconnect-nam-win-<*version*>.msi	ネットワーク アクセス マネージャ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-posture-win-<*version*>-pre-deploy-k9.msi	ポスチャ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-telemetry-win-<*version*>-pre-deploy-k9.msi	テレメトリ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-websecurity-win-<*version*>-pre-deploy-k9.msi	Web セキュリティ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-win-<*version*>-pre-deploy-k9.msi	AnyConnect コア クライアント用 MSI インストーラ ファイル。
autorun.inf	setup.exe 用セットアップ情報ファイル。
cues_bg.jpg	インストール ユーティリティ GUI の背景画像。
setup.hta	インストール ユーティリティの HTML アプリケーション（HTA）。このプログラムはカスタマイズできます。
update.txt	AnyConnect バージョン番号をリストしたテキスト ファイル。

ガイドラインと制限事項

システム MTU のリセット

Windows インストーラ オプションで、すべてのアダプタの MTU をリセットできます。各 MSI インストーラでは、共通のプロパティ（RESET_ADAPTER_MTU）がサポートされます。これは、1 に設定されている場合に、すべての Windows ネットワーク アダプタの MTU 設定値がデフォルト値にリセットされます。変更を有効にするには再起動する必要があります。VPN インストーラのみこのオプションを備えています。コマンド ライン パラメータを次のように設定します。
msiexec/package anyconnect-win-ver-pre-deploy-k9.msi/passive RESET_ADAPTER_MTU=1

ActiveX コントロールをオンにする

AnyConnect 事前展開 VPN パッケージでは、すでに VPN WebLaunch ActiveX コントロールがデフォルトでインストールされています。AnyConnect 3.1 を開始すると、VPN ActiveX コントロールのインストールはデフォルトでオフになります。この変更は、最もセキュアな設定をデフォルト動作にするために行われました。

AnyConnect クライアントとオプション モジュールを事前展開する場合、VPN ActiveX コントロールを AnyConnect でインストールする必要がある場合、msiexec またはトランスフォームとともに NOINSTALLACTIVEX=0 オプションを使用する必要があります。

事前展開にインストール ユーティリティを使用する

ユーザは、インストール ユーティリティを使用して、インストールする項目を選択します。デフォルトでは、すべてのコンポーネントのチェックボックスがオンになっています。そのままでよい場合、ユーザは [Install] ボタンをクリックして、[Selections To Install] ダイアログボックスにリストされたコンポーネントに同意できます。選択に基づいて、インストールするコンポーネントが判別されます。

インストール ユーティリティは、ISO パッケージ ファイルとしてパッケージ化されている、*setup.hta* という HTML アプリケーション（HTA）です。このプログラムに対しては、任意の変更を、任意に加えることができます。このユーティリティは、必要に応じてカスタマイズしてください。

各インストーラは、サイレント実行されます。コンピュータのリブートを必要とするインストーラの場合は、インストーラの最終実行後にユーザに通知されます。インストール ユーティリティは、リブートを開始しません。

1 つ以上のオプション モジュールに加えてコア クライアントを導入する場合、lockdown プロパティを各インストーラに適用する必要があります。この操作は片方向のみであり、製品を再インストールしない限り削除できません。

このオプションは、VPN インストーラ、ネットワーク アクセス マネージャ インストーラ、および Web セキュリティ インストーラに使用できます。

SMS を使用して AnyConnect モジュールを事前展開する

AnyConnect モジュールを事前展開する場合、管理者は、事前展開モジュールおよび対応するクライアント プロファイル（モジュールで必要な場合）をエンドポイントにコピーする必要があります。このタイプの事前展開では、VPN クライアントをインストールする必要はなく、一部のモジュールはスタンドアロン モードで動作できます。

（注） ネットワーク アクセス マネージャを使用する場合は、[Hide icon and notifications] オプションを選択して、Windows の事前展開の際に Microsoft の [Network] アイコンが表示されないようにする必要があります。デフォルトでは、このアイコンは*通知のみを表示*モードです。このモードでは、変更と更新のアラートが出されます。

以下のモジュールには、AnyConnect クライアント プロファイルが必要です。

- AnyConnect VPN モジュール
- AnyConnect テレメトリ モジュール
- AnyConnect ネットワーク アクセス マネージャ モジュール
- AnyConnect Web セキュリティ モジュール

以下の機能には、AnyConnect クライアント プロファイルは必要ありません。

- AnyConnect VPN Start Before Login
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect ポスチャ モジュール
- AnyConnect カスタマー エクスペリエンス フィードバック モジュール

事前展開モジュールは、「SMS を使用して AnyConnect モジュールを事前展開する」（P.2-25）で説明されている順序でインストールする必要があります。

要件

AnyConnect を Windows 7 または Windows Vista にインストールする場合、AlwaysInstallElevated または Windows User Account Control（UAC）グループ ポリシー設定のいずれかを無効にする必要があります。

手順の詳細

ステップ 1　**anyconnect-win-<*version*>-pre-deploy-k9.iso** を cisco.com からダウンロードします。

ステップ 2　Winzip、7-zip、または同様のユーティリティを使用して、.iso ファイルの内容を解凍します。

ステップ 3　クライアント プロファイルを必要とするモジュールの場合は、ASDM と統合されているプロファイル エディタかスタンドアロン プロファイル エディタを使用して、インストールするモジュール用のクライアント プロファイルを作成します。さまざまなクライアント プロファイルの設定手順については、次の章を参照してください。

- 第 3 章「VPN アクセスの設定」
- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」
- 第 7 章「WSA に対する AnyConnect テレメトリの設定」
- 第 8 章「Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュールの使用」
- 第 9 章「NGE、FIPS、および追加セキュリティ」

ステップ 4　作成したクライアント プロファイルは、.iso ファイルから解凍した適切なディレクトリにコピーしてください。

- Profiles\vpn
- Profiles\nam
- Profiles\websecurity
- Profiles\telemetry

ステップ 5　AnyConnect モジュールの事前展開用のパッケージをとくていするには、「ISO ファイルの使用」（P.2-23）を参照してください。

（注）　AnyConnect を Windows 7 または Windows Vista にインストールする場合、AlwaysInstallElevated または Windows User Account Control（UAC）グループ ポリシー設定のいずれかを無効にする必要があります。

ステップ 6　ソフトウェア管理システムを使用して、事前展開ソフトウェア パッケージと、クライアント プロファイルを含んでいる **Profiles** ディレクトリをエンドポイントに展開します

ステップ 7　「エンタープライズ ソフトウェア展開システム用 MSI ファイルのパッケージ化」（P.2-28）で説明されている手順を実行して、「SMS を使用して AnyConnect モジュールを事前展開する」（P.2-25）に定義されている順序で、AnyConnect モジュールをインストールします。

Windows 用 AnyConnect モジュールのインストール（推奨する順序）

必要に応じて、ISO イメージから個々のインストーラを取り出して、手動で配布することもできます。事前展開パッケージ内の各インストーラは、個別に実行できます。.iso ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

ファイルを手動で配布する場合は、選択したコンポーネント間の依存関係に対処する必要があります。コア クライアント MSI は、オプション モジュールで使用する必要のある、すべての VPN 機能コンポーネントおよび共通コンポーネントを含みます。これらのインストーラでは、同じバージョンのコア クライアントが存在していることを確認してから、インストールを始めます。

前提条件

オプション モジュールのインストーラには、同じバージョンの AnyConnect 3.1 コア クライアントがインストールされている必要があります。一致していない場合、オプション モジュールはインストールされず、一致していないことがインストーラからユーザに通知されます。インストール ユーティリティを使用する場合は、パッケージ内のモジュールが、まとめてビルドおよびパッケージ化されるため、バージョンは常に一致します。

手順の詳細

ステップ 1　AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

ステップ 2　AnyConnect Diagnostic and Reporting Tool（DART）モジュールをインストールします。このモジュールは、AnyConnect コア クライアント インストールに関する、有用な診断情報を提供します。

ステップ 3　SBL、ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ モジュールを、任意の順序でインストールします。

ステップ 4　テレメトリ モジュールをインストールします。このモジュールには、ポスチャ モジュールが必要です。

（注）　オプション モジュール用の個々のインストーラでは、インストールされているコア VPN クライアントのバージョンを確認してから、インストールを行います。 コア モジュールとオプション モジュールのバージョンは一致している必要があります。一致していない場合、オプション モジュールはインストールされず、一致していないことがインストーラからユーザに通知されます。インストール ユーティリティを使用する場合は、パッケージ内のモジュールが、まとめてビルドおよびパッケージ化されるため、バージョンは常に一致します。

Windows 用 AnyConnect モジュールのアンインストール（推奨する順序）

手順の詳細

ステップ 1　テレメトリ モジュールをアンインストールします。

ステップ 2　ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ、SBL を任意の順序でアンインストールします。

ステップ 3　AnyConnect コア クライアントをアンインストールします。

ステップ 4　DART をアンインストールします。

DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。

（注）　設計上、一部の XML ファイルは AnyConnect のアンインストール後もそのままの状態です。

エンタープライズ ソフトウェア展開システム用 MSI ファイルのパッケージ化

ここでは、MSI インストール コマンドライン呼び出しなどのエンタープライズ ソフトウェア展開システムを使用して AnyConnect クライアントおよびオプション モジュールを展開するために必要な情報と、プロファイルの展開先の場所について説明します。

- 「MSI インストールのコマンドライン呼び出し」（P.2-28）
- 「Windows のロックダウン オプション」（P.2-29）
- 「AnyConnect プロファイルの展開場所」（P.2-35）
- 「プログラムの追加と削除リストで AnyConnect を非表示にする」（P.2-29）

MSI インストールのコマンドライン呼び出し

インストールされるモジュール	コマンドおよびログ ファイル
VPN なしの AnyConnect コア クライアント機能。 スタンドアロン ネットワーク アクセス マネージャまたは Web セキュリティ モジュールをインストールするときに使用します。	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
VPN ありの AnyConnect コア クライアント機能。	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
カスタマー エクスペリエンスのフィードバック	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool（DART）	msiexec /package anyconnect-dart-win-ver-k9.msi /norestart /passive /lvx* anyconnect-dart-<*version*>-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-ver-k9.msi /norestart /passive /lvx* anyconnect-gina-<*version*>-pre-deploy-k9-install-datetimestamp.log
ネットワーク アクセス マネージャ	msiexec /package anyconnect-nam-win-ver-k9.msi /norestart /passive /lvx* anyconnect-nam-<*version*>-pre-deploy-k9-install-datetimestamp.log
Web セキュリティ	msiexec /package anyconnect-websecurity-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-<*version*>-pre-deploy-k9-install-datetimestamp.log
ポスチャ	msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-<*version*>-pre-deploy-k9-install-datetimestamp.log
テレメトリ	msiexec /package anyconnect-telemetry-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-telemetry-<*version*>-pre-deploy-k9-install-datetimestamp.log

Windows のロックダウン オプション

シスコでは、AnyConnect Secure Mobility クライアントをホストするデバイスで制限された権限をエンド ユーザに付与することをお勧めします。エンド ユーザに追加の権限を認可する場合、インストーラは、ユーザとローカル管理者がエンドポイントでロックダウン済みとして設定された Windows サービスをオフに切り替えたり停止したりできないようにするロックダウン機能を提供できます。引き続き、サービス パスワードを使用して、コマンド プロンプトからサービスを停止できます。

各 MSI インストーラでは、共通のプロパティ（LOCKDOWN）がサポートされます。これは、ゼロ以外の値に設定されている場合に、そのインストーラに関連付けられた Windows サービスがエンドポイント デバイスでユーザまたはローカル管理者によって制御されないようにします。このプロパティを設定して、ロックダウンする各 MSI インストーラにトランスフォームを適用するには、インストール時に提供されるサンプルのトランスフォームを使用することをお勧めします。ロックダウン オプションも ISO インストール ユーティリティ内のチェックボックスです。

プログラムの追加と削除リストで AnyConnect を非表示にする

Windows のプログラムの追加と削除リストを表示するユーザに対して、インストールされている AnyConnect モジュールを非表示にできます。ARPSYSTEMCOMPONENT=1 を使用して任意のインストーラを起動した場合、そのモジュールは、Windows のプログラムの追加と削除リストに表示されません。

本書に記載されているトランスフォームの例を使用して、非表示にするモジュールごとの各 MSI インストーラにトランスフォームを適用しながら、このプロパティを設定することをお勧めします。

ネットワーク アクセス マネージャおよび Web セキュリティをスタンドアロン アプリケーションとしてインストールするためのユーザ指示

AnyConnect モジュールであるネットワーク アクセス マネージャと Web セキュリティを、上記の MSI インストール コマンド ライン コール表のコマンドを使用して、ユーザ コンピュータにスタンドアロン アプリケーションとして展開できます。

（注） クライアントは、すべての VPN クライアント プロファイルを読み取ります。任意のプロファイルで <ServiceDisable> が true に設定されている場合、VPN は無効になっています。

手順の詳細

ステップ 1　インストール ユーティリティをユーザに展開してある場合は、以下の項目をオンにするようユーザに指示します。

*AnyConnect ネットワーク アクセス マネージャ*または *AnyConnect Web セキュリティ モジュール*

ステップ 2　Cisco AnyConnect VPN モジュールのチェックボックスをオフにするようユーザに指示してください。

このようにすると、コア クライアントの VPN 機能が無効になり、ネットワーク アクセス マネージャおよび Web セキュリティが、インストール ユーティリティによって、VPN 機能なしのスタンドアロン アプリケーションとしてインストールされます。

ステップ 3　オプション モジュールのインストーラを実行します。このインストーラでは、VPN サービスのない AnyConnect GUI を使用できます。

1. スタンドアロン ネットワーク アクセス マネージャおよびスタンドアロン Web セキュリティ モジュールの選択を確認するポップアップ ダイアログボックスが表示されます。

2. ユーザが [OK] をクリックすると、設定値 PRE_DEPLOY_DISABLE_VPN=1 を使用して、インストール ユーティリティにより、AnyConnect 3.1 コア インストーラが起動されます。
3. インストール ユーティリティは、既存のすべての VPN プロファイルを削除してから VPNDisable_ServiceProfile.xml をインストールします。
4. インストール ユーティリティは、指定に応じて、ネットワーク アクセス マネージャ インストーラおよび Web セキュリティ インストーラを起動します。
5. 指定に応じて、AnyConnect 3.1 ネットワーク アクセス マネージャおよび Web セキュリティ モジュールが、コンピュータ上で VPN サービスなしで有効になります。

（注）　コンピュータ上にネットワーク アクセス マネージャが事前にインストールされていなかった場合、ユーザは、ネットワーク アクセス マネージャのインストールを完了するためにコンピュータをリブートする必要があります。一部のシステム ファイルのアップグレードを必要とする、アップグレード インストールの場合も、ユーザはリブートを必要とします。

事前展開中のインストーラ動作の変更

コマンド ラインを使用して、インストーラのプロパティを指定し、通常のインストール動作を制御できます。msiexec /package vpn.msi SOME_PROPERTY=1 などのコマンドにより、インストーラ パラメータが msiexec に渡されます。同じコマンド ラインで複数のプロパティを渡すことができます。

Windows では、トランスフォームを使用して、インストーラ ユーティリティ msiexec によるプロパティ テーブルの解釈方法を変更することもできます。ASA で、トランスフォーム ファイル（.mst）をアップロードすると、インストール時にダウンローダがそれらのファイルを .msi に適用します（msiexec /package vpn.msi TRANSFORMS=hello.mst など）。

Linux および Mac OS X コンピュータへの事前展開

以下の項では、Linux および Mac OS X コンピュータへの事前展開に特化した情報を示します。内容は次のとおりです。

インストーラ動作の変更

Mac OS X では、.pkg 動作をカスタマイズする一般的な方法はありません。必要なカスタマイズを実装できるようにするため、ACTtransforms.xml を作成し、インストーラとともに配置し、インストーラ実行時に読み取ります。ファイルをインストーラからの特定の相対パスに配置する必要があります。インストーラは、次の場所で変更が見つかるかどうかこの順序で検索します。

1. .pkg インストーラ ファイルと同じディレクトリにある「Profile」ディレクトリ中
2. マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ中

3. .dmg ファイルと同じディレクトリにある「Profile」ディレクトリ中

XML ファイルの形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

たとえば、OS X ACTtransforms.xml プロパティは、ネットワーク アクセス マネージャまたは Web セキュリティの「スタンドアロン」展開を作成する場合 *DisableVPN* です。

Linux のインストーラの変更には対応していません。

カスタマー エクスペリエンス フィードバック モジュールの無効化

カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。このフィードバック モジュールにより、お客様が使用し、有効にした機能とモジュールを確認できます。このクライアント情報を収集することでユーザ エクスペリエンスを探り、シスコは AnyConnect の品質、信頼性、パフォーマンス、ユーザ エクスペリエンスを継続して改善できます。Mac OS X では、プログラム バイナリをインストールするのではなくこの機能を無効にする場合は、OS X ACTransforms.xml プロパティは DisableCustomerExperienceFeedback です。

（注） ディスク ユーティリティまたは **hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o anyconnect-macosx-i386-ver-k9-rw.dmg** を使用して、dmg を読み取り専用から読み取り / 書き込みに変換する必要があります。

Linux および Mac OS X のモジュールのインストール（推奨する順序）

Linux および Mac 用の個々のインストーラを取り出して、手動で配布できます。事前展開パッケージ内の各インストーラは、個別に実行できます。tar.gz ファイルまたは .dmg ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

要件

Mac OS X で正しく動作させるには、AnyConnect の最小ディスプレイの解像度を 1024 x 640 ピクセルに設定する必要があります。

手順の詳細

ステップ 1　AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

ステップ 2　DART モジュールをインストールします。このモジュールは、AnyConnect コア クライアント インストールに関する、有用な診断情報を提供します。

ステップ 3　ポスチャ モジュールをインストールします。

Linux および Mac OS X のモジュールのアンインストール（推奨する順序）

手順の詳細

ステップ 1　ポスチャ モジュールをアンインストールします。

ステップ 2　AnyConnect コア クライアントをアンインストールします。

ステップ 3　DART をアンインストールします。

DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。

システムでのアプリケーションの制限

Mac OS X 10.8 では、システムで動作できるアプリケーションを制限するゲートキーパーという新機能が導入されています。次からダウンロードされたアプリケーションを許可するか選択できます。

- Mac App Store
- Mac App Store and identified developers
- Anywhere

デフォルト設定は [Mac App Store and identified developers]（署名付きアプリケーション）です。AnyConnect リリース 3.1 は署名付きアプリケーションですが、Apple 証明書では署名されていません。つまり、Anywhere 設定を選択するか、コントロール クリックを使用して選択された設定をバイパスし、AnyConnect を事前展開インストールからインストールして、実行する必要があります。Web 展開する、またはすでに AnyConnect をインストールしたユーザには影響ありません。詳細については、http://www.apple.com/macosx/mountain-lion/security.html を参照してください。

Firefox によるサーバ証明書の検証

AnyConnect を Linux デバイスにインストールした後、AnyConnect 接続を初めて試行する前に、Firefox ブラウザを開始します。AnyConnect では、Firefox を使用してサーバ証明書を検証します。Firefox を開くとプロファイルが作成されます。このプロファイルなしでは、サーバ証明書を信頼済みであると検証できません。

Firefox を使用しない場合は、Firefox 証明書ストアを除外するようにローカル ポリシーを設定する必要があります。これには、PEM ストアの設定も必要です。

AnyConnect ファイル情報

ここでは、次の項で、ユーザ コンピュータ上の AnyConnect ファイルの場所について説明します。

- 「エンドポイント コンピュータ上のモジュールのファイル名」（P.2-33）
- 「ローカル コンピュータにインストールされたユーザ プリファレンス」（P.2-37）
- 「AnyConnect プロファイルの展開場所」（P.2-35）

エンドポイント コンピュータ上のモジュールのファイル名

表 2-5 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の AnyConnect ファイル名を、オペレーティング システム タイプごとに示します。

表 2-5　ASA 展開または事前展開用の AnyConnect コア ファイル名

AnyConnect 3.1 コア	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-win-(ver)-web-deploy-k9.exe	anyconnect-win-(ver)-pre-deploy-k9.msi
Mac	anyconnectsetup.dmg	anyconnect-macosx-i386-(ver)-k9.dmg
Linux	anyconnectsetup.sh	anyconnect-linux-(ver)-k9.tar.gz

表 2-6 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の DART ファイル名を、オペレーティング システム タイプごとに示します。3.0.3050 よりも前のリリースでは、DART コンポーネントは Web 展開用に個別のダウンロード（dmg、.sh、または .msi ファイル）になっていました。リリース 3.0.3050 以降では、DART コンポーネントは .pkg ファイルに含まれています。

表 2-6　ASA または事前展開の DART パッケージ ファイル名

DART	Web 展開 ファイル名およびパッケージ（ダウンロード）	事前展開 インストーラ
Windows	*リリース 3.0.3050 以降：* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	3.0.3050 よりも前のリリース： anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac	*リリース 3.0.3050 以降：* anyconnect-macosx-i386-(ver)-k9.pkg	anyconnect-macosx-i386-(ver)-k9.dmg
	3.0.3.050 よりも前のリリース： anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	*リリース 3.0.3050 以降：* anyconnect-linux-(ver)-k9.pkg	anyconnect-predeploy-linux-(ver)-k9.tar.gz
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz

* Web 展開パッケージおよび事前展開パッケージは、ISO イメージ（*.iso）に含まれています。ISO イメージ ファイルには、ユーザのコンピュータへの展開に必要なプログラムと MSI インストーラ ファイルが含まれています。

表 2-7 に、クライアントを Windows コンピュータに事前展開または ASA 展開するときの、エンドポイント コンピュータ上の SBL ファイル名を示します。

表 2-7　ASA または事前展開の Start Before Logon パッケージ ファイル名

SBL（Gina）	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-gina-win-(ver)-web-deploy-k9.exe	anyconnect-gina-win-(ver)-pre-deploy-k9.msi

表 2-8 に、クライアントを Windows コンピュータに事前展開または ASA 展開するときの、エンドポイント コンピュータ上のネットワーク アクセス マネージャ ファイル名を示します。

表 2-8　ASA または事前展開のネットワーク アクセス マネージャ ファイル名

ネットワーク アクセス マネージャ	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-nam-win-(ver)-k9.msi	anyconnect-nam-win-(ver)-k9.msi

表 2-9 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上のポスチャ モジュール ファイル名を、オペレーティング システム タイプごとに示します。

表 2-9　ASA または事前展開のポスチャ モジュール ファイル名

ポスチャ	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-posture-win-(ver)-pre-deploy-k9.msi
Mac	anyconnect-posturesetup.dmg	anyconnect-posture-macosx-i386-(ver)-k9.dmg
Linux	anyconnect-posturesetup.sh	anyconnect-posture-linux-(ver)-k9.tar.gz
Linux-64	anyconnect-posturesetup.sh	anyconnect-posture-linux-(ver)-k9.tar.gz

表 2-10 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の Windows 用テレメトリ モジュールのファイル名を示します。

表 2-10　ASA または事前展開のテレメトリ ファイル名

テレメトリ	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-telemetry-win-(ver)-web-deploy-k9.exe。anyconnect-posture-win-(ver)-web-deploy-k9.msi のインストールに依存。	anyconnect-telemetry-win-(ver)-pre-deploy-k9.msi。anyconnect-posture-win-(ver)-pre-deploy-k9.msi のインストールに依存。

表 2-11 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の Windows 用 Web セキュリティ モジュールのファイル名を示します。

表 2-11　ASA または事前展開の Web セキュリティ ファイル名

Web セキュリティ	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-websecurity-win-(ver)-web-deploy-k9.exe	anyconnect-websecurity-win-(ver)-pre-deploy-k9.msi

AnyConnect プロファイルの展開場所

表 2-12 に、AnyConnect によってローカル コンピュータにダウンロードされるプロファイル関連のファイルおよびファイルの目的を示します。

表 2-12　エンドポイント上のプロファイル ファイル

ファイル	説明
anyfilename.xml	AnyConnect プロファイル。このファイルは、特定のユーザ タイプに対して設定される機能および属性値を指定します。
AnyConnectProfile.tmpl	AnyConnect ソフトウェアに付属するクライアント プロファイルの例。
AnyConnectProfile.xsd	XML スキーマ フォーマットを定義します。AnyConnect はこのファイルを使用して、プロファイルを確認します。

表 2-13 に、すべてのオペレーティング システムについて、AnyConnect プロファイルの場所を示します。

表 2-13　すべてのオペレーティング システムに対するプロファイルの場所

オペレーティング システム	モジュール	場所
Windows XP	VPN を使用するコア クライアント	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	カスタマー エクスペリエンスのフィードバック	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Windows Vista	VPN を使用するコア クライアント	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	カスタマー エクスペリエンスのフィードバック	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Windows 7	VPN を使用するコア クライアント	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security

オペレーティング システム	モジュール	場所
	カスタマー エクスペリエンスのフィードバック	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Mac OS X	その他のすべてのモジュール	/opt/cisco/anyconnect/profile
	カスタマー エクスペリエンスのフィードバック	/opt/cisco/anyconnect/CustomerExperienceFeedback
Linux	すべてのモジュール	/opt/cisco/anyconnect/profile

ローカル コンピュータにインストールされたユーザ プリファレンス

また一部のプロファイル設定は、ユーザ 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、クライアント GUI の [Preferences] タブにユーザ制御可能設定をクライアントで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することができます。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。

表 2-14 に、クライアント コンピュータ上のプリファレンス ファイルのファイル名およびインストール先パスを示します。

表 2-14　ユーザ プリファレンス ファイルおよびインストール パス

オペレーティング システム	タイプ	ファイルおよびパス
Windows Vista Windows 7	ユーザ	C:\Users*username*\AppData\Local\Cisco\ Cisco AnyConnect VPN Client\preferences.xml
	グローバル	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\ preferences_global.xml
Windows XP	ユーザ	C:\Documents and Settings**username**\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect VPN Client\preferences.xml
	グローバル	C:\Documents and Settings\AllUsers\Application Data\Cisco\ Cisco AnyConnect VPN Client\preferences_global.xml
Mac OS X	ユーザ	/Users/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

オペレーティング システム	タイプ	ファイルおよびパス
Linux	ユーザ	/home/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

スタンドアロン AnyConnect プロファイル エディタの使用

スタンドアロン AnyConnect プロファイル エディタを使用すると、管理者は、AnyConnect Secure Mobility Client の VPN、ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリおよびカスタマー エクスペリエンス フィードバック モジュールのクライアント プロファイルを設定できます。これらのプロファイルは、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、カスタマー エクスペリエンス フィードバック モジュールの事前展開キットを使用して配布できます。

スタンドアロン プロファイル エディタのシステム要件

サポートされるオペレーティング システム

スタンドアロン プロファイル エディタは Windows のみ対応しています。

Java 要件

このアプリケーションは、JRE 1.6 を必要とします。インストールされていない場合は、MSI インストーラによって自動的にインストールされます。

ブラウザ要件

このアプリケーションに含まれているヘルプ ファイルは、Firefox および Internet Explorer でサポートされています。その他のブラウザではテストされていません。

必要なハード ドライブ容量

Cisco AnyConnect プロファイル エディタ アプリケーションは、最大 5 MB のハード ドライブ容量を必要とします。JRE 1.6 は、最大 100 MB のハード ドライブ容量を必要とします。

スタンドアロン AnyConnect プロファイル エディタのインストール

スタンドアロン AnyConnect プロファイル エディタは、AnyConnect の ISO ファイルおよび .pkg ファイルとは別に Windows 実行ファイル（.exe）として配布され、ファイルの命名規則は **anyconnect-profileeditor-win-**<*version*>**-k9.exe** となっています。

スタンドアロン プロファイル エディタをインストールするには、次の手順を実行します。

ステップ 1　Cisco.com から **anyconnect-profileeditor-win-**<*version*>**-k9.exe** をダウンロードします。

ステップ 2　**anyconnect-profileeditor-win-**<*version*>**-k9.exe** をダブルクリックして、インストール ウィザードを起動します。

ステップ 3　[Welcome] 画面で、[Next] をクリックします。

ステップ 4　[Choose Setup Type] ウィンドウで、次のいずれかのボタンをクリックし、[Next] をクリックします。

- [Typical] : ネットワーク アクセス マネージャ プロファイル エディタのみが自動的にインストールされます。
- [Custom] : ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、カスタマー エクスペリエンス フィードバック プロファイル エディタ、および VPN プロファイル エディタから任意のプロファイル エディタを選択してインストールできます。
- [Complete] : ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、カスタマー エクスペリエンス フィードバック プロファイル エディタ、テレメトリ、VPN ローカル ポリシー エディタ、および VPN プロファイル エディタを自動的にインストールします。

ステップ 5　前のステップで [Typical] または [Complete] をクリックした場合は、ステップ 6 までスキップしてください。前のステップで [Custom] をクリックした場合は、インストールするスタンドアロン プロファイル エディタのアイコンをクリックし、[Will be installed on local hard drive] を選択するか、[Entire Feature will be unavailable] をクリックして、そのスタンドアロン プロファイル エディタがインストールされないようにします。[Next] をクリックします。

ステップ 6　[Ready to Install] 画面で [Install] をクリックします。[Installing Cisco AnyConnect Profile Editor] 画面にインストールの進行状況が表示されます。

ステップ 7　[Completing the Cisco AnyConnect Profile Editor Setup Wizard] で [Finish] をクリックします。

- スタンドアロン AnyConnect プロファイル エディタは、**C:\Program Files\Cisco\Cisco AnyConnect Profile Editor** ディレクトリにインストールされます。
- [Start] > [All Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] を選択してから、サブメニューで目的のスタンドアロン プロファイル エディタをクリックするか、デスクトップ上にインストールされる該当するプロファイル エディタ ショートカット アイコンをクリックすることにより、VPN、ネットワーク アクセス マネージャ、Web セキュリティのプロファイル エディタを起動できます。

スタンドアロン AnyConnect プロファイル エディタ インストールの修正

次の手順を実行することにより、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリ、またはカスタマー エクスペリエンス フィードバックのプロファイル エディタをインストールまたは削除するように、スタンドアロン Cisco AnyConnect プロファイル エディタ インストールを変更できます。

ステップ 1　Windows のコントロール パネルを開いて [Add or Remove Programs] をクリックします。

ステップ 2　[Cisco AnyConnect Profile Editor] を選択し、[Change] をクリックします。

ステップ 3　[Next] をクリックします。

ステップ 4　[Modify] をクリックします。

ステップ 5　インストールまたは削除するプロファイル エディタのリストを編集し、[Next] をクリックします。

ステップ 6　[Install] をクリックします。

ステップ 7　[Finish] をクリックします。

スタンドアロン AnyConnect プロファイル エディタのアンインストール

ステップ 1　Windows のコントロール パネルを開いて [Add or Remove Programs] をクリックします。

ステップ 2　Cisco AnyConnect プロファイル エディタを選択し、[Remove] をクリックします。

ステップ 3　[Yes] をクリックして、Cisco AnyConnect プロファイル エディタをアンインストールすることを確認します。

（注）　スタンドアロン プロファイル エディタをアンインストールするときに、JRE 1.6 は自動的にアンインストールされません。別途アンインストールする必要があります。

スタンドアロン プロファイル エディタを使用したクライアント プロファイルの作成

ステップ 1　VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはカスタマー エクスペリエンス フィードバックのプロファイル エディタを起動します。これには、デスクトップ上のショートカット アイコンをダブルクリックするか、[Start] > [All Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] の順に選択して、サブメニューから VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはカスタマー エクスペリエンス フィードバックのプロファイル エディタを選択します。

ステップ 2　『AnyConnect Administrator Guide』の以下の章にある、クライアント プロファイルの作成手順を実行します。

- 第 3 章「VPN アクセスの設定」
- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」
- 第 7 章「WSA に対する AnyConnect テレメトリの設定」
- 第 8 章「Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュールの使用」
- 第 9 章「NGE、FIPS、および追加セキュリティ」の AnyConnect ローカル ポリシーのパラメータと値

ステップ 3　[File] > [Save] を選択して、クライアント プロファイルを保存します。プロファイル エディタの各パネルには、クライアント プロファイルのパスおよびファイル名が表示されます。

スタンドアロン プロファイル エディタを使用したクライアント プロファイルの編集

ステップ 1　デスクトップ上のショートカット アイコンをダブルクリックするか、[Start] > [All Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] の順に選択し、サブメニューから目的のプロファイル エディタを選択して、起動します。

ステップ 2　[File] > [Open] を選択し、編集するクライアント プロファイル XML ファイルまで移動します。

（注）　たとえば、Web セキュリティ機能のクライアント プロファイルを、誤って、VPN など別の機能のプロファイル エディタを使用して開こうとすると、「Schema Validation failed」というメッセージが表示され、プロファイルを編集できません。

ステップ 3　プロファイルに変更を加え、[File] > [Save] を選択して変更を保存します。

（注）　誤って、同じ種類のプロファイル エディタのインスタンスを 2 つ使用して、同じクライアント プロファイルを編集しようとした場合は、そのクライアント プロファイルに加えた最後の変更が保存されます。