Cisco AnyConnect Secure Mobility Client 管理者ガイド

リリース 3.0

最終更新日：2012 年 12 月 3 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco AnyConnect Secure Mobility Client 管理者ガイド

CONTENTS

このマニュアルについて

このマニュアルでは、Cisco AnyConnect Secure Mobility Client イメージを中央サイトの ASA にインストールする方法、リモート ユーザ コンピュータへ導入するための AnyConnect の設定方法、ASDM で AnyConnect の接続プロファイルおよびグループ ポリシーを設定する方法、AnyConnect をモバイル デバイスにインストールする方法、および AnyConnect 接続のモニタリングとトラブルシューティングを行う方法について説明します。

このマニュアル中で「ASA」という用語は、すべてのモデルの Cisco ASA 5500 シリーズ（ASA 5505 以上）を意味します。

対象読者

このマニュアルは、次の作業を行う管理者を対象としています。

- ネットワーク セキュリティの管理
- ASA のインストールおよび設定
- VPN の設定

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス 「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

関連資料

- 『AnyConnect Secure Mobility Client 3.0 Release Notes』
- 『AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5』
- 『Cisco ASA 5500 Series Adaptive Security Appliances Release Notes』
- 『Cisco ASA 5500 Series Adaptive Security Appliances Install and Upgrade Guides』
- 『Cisco ASA 5500 Series Adaptive Security Appliances Configuration Guides』
- 『Cisco ASA 5500 Series Adaptive Security Appliances Command References』
- 『Cisco ASA 5500 Series Adaptive Security Appliances Error and System Messages』
- 『Cisco Adaptive Security Device Manager Release Notes』
- 『Cisco Adaptive Security Device Manager Configuration Guides』
- 『Online help for ASDM』
- 『Cisco Secure Desktop Release Notes』
- 『Cisco Secure Desktop Configuration Guides』
- この製品のオープン ソース ライセンス情報については、次のリンクを参照してください。
  http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

AnyConnect Secure Mobility Client の概要

Cisco AnyConnect Secure Mobility Client は、Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）への、安全な IPsec（IKEv2）または SSL VPN 接続をリモート ユーザに提供する次世代型 VPN クライアントです。AnyConnect は、今日の増殖を続けるマネージドおよびアンマネージド モバイル デバイス全体でのセキュア モビリティにより、インテリジェントでシームレスな常時接続をエンド ユーザに体験させてくれます。

ASA またはエンタープライズ ソフトウェア導入システムから導入可能

AnyConnect は、ASA から、またはエンタープライズ ソフトウェア導入システムを使用してリモート ユーザに導入できます。ASA から導入する場合、リモート ユーザはクライアントレス SSL VPN 接続を許可するよう設定された ASA のブラウザで IP アドレスまたは DNS 名を入力することで、ASA に最初の SSL 接続を行います。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。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

カスタマイズ可能および変換可能

AnyConnect をカスタマイズして、リモート ユーザに、自社企業のイメージを表示できます。デフォルトの GUI コンポーネントを置き換えて AnyConnect のブランドを変更し、より広範囲にブランド変更するために作成したトランスフォームを導入したり、AnyConnect API を使用する自分のクライアント GUI を導入したりできます。AnyConnect またはインストーラ プログラムの表示メッセージは、リモート ユーザが希望する言語に翻訳することもできます。

簡単な設定

ASDM を使用して、AnyConnect 機能を簡単にクライアント プロファイルに設定できます。この XML ファイルは、接続確立に関する基本情報、および Start Before Logon（SBL）などの拡張機能を提供します。一部の機能については、ASA の設定を行うことも必要です。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導入します。

追加されたサポート対象モジュール

Cisco AnyConnect Secure Mobility Client バージョン 3.0 は、以下の新しいモジュールを AnyConnect クライアント パッケージに統合します。

- ネットワーク アクセス マネージャ：（以前は Cisco Secure Services Client と呼ばれていました）レイヤ 2 のデバイス管理、および有線と無線の両方のネットワーク アクセスの認証を提供します。
- ポスチャ評価：このモジュールにより、AnyConnect Secure Mobility Client は、ASA へのリモート アクセス接続を作成するよりも前にホストにインストールされた、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できま

す。このプリログイン評価に基づいて、どのホストに対して、セキュリティ アプライアンスへのリモート アクセス接続の作成を許可す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。

- テレメトリ：アンチウイルス ソフトウェアによって検出された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。WSA は、このデータを使用して、より優れた URL のフィルタリング ルールを提供します。
- Web セキュリティ：HTTP トラフィックおよび HTTPS 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。
- Diagnostic and Reporting Tool（DART）：トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。
- Start Before Logon（SBL）：Windows ダイアログボックスが表示される前に AnyConnect を起動します。Windows ログイン ダイアログボックスが表示される前に AnyConnect を起動することによって、ユーザは Windows にログインする前に VPN 接続を介して企業インフラストラクチャに強制的に接続されます。

この章は、次の項で構成されています。

AnyConnect ライセンス オプション

AnyConnect Secure Mobility Client では、VPN セッションをサポートするために、ライセンスのアクティブ化が必要です。シスコでは、AnyConnect クライアントと Secure Mobility 機能、およびサポートするセッションの数に応じて、以下の 3 段階のライセンス オプションを提供しています。

- AnyConnect Essentials：AnyConnect Secure Mobility Client をサポートします。このライセンスは、Premium としてラベル付けされている機能を除く、すべての AnyConnect クライアント機能をサポートします。また、従来のクライアント（Cisco VPN Client）を使用して確立されたセッションもサポートします。このライセンスは適応型セキュリティ アプライアンスでアクティブ化します。
- Premium：すべての AnyConnect Essentials 機能、ブラウザベースの VPN アクセス、Premium AnyConnect クライアント機能、およびブラウザベースと AnyConnect セッションの両方の Cisco Secure Desktop をサポートします。このライセンスは適応型セキュリティ アプライアンスでアクティブ化します。
- AnyConnect Secure Mobility：Web セキュリティ機能をサポートします。このライセンスは、Cisco Web セキュリティ アプライアンスでアクティブ化します。ライセンス名は、ライセンス適応型セキュリティ アプライアンスに応じて異なります。
- Cisco IronPort Web セキュリティ アプライアンス ライセンス。

ASA 上でアクティブ化され、AnyConnect Premium ライセンスでアクティブ化された適応型セキュリティ アプライアンスは、AnyConnect Essentials ライセンスおよび以下の AnyConnect Secure Mobility Client Premium 機能によってサポートされるのと同じアクセス テクノロジーをサポートします。

- VPN 常時接続および関連オプション機能：接続障害終了ポリシー、キャプティブ ポータルの修復、ローカル印刷、およびテザー デバイスのサポート。
- Cisco Secure Desktop。
- 最適ゲートウェイの選択。
- グループ ポリシーごとのファイアウォール ルール。
- VPN セッションが隔離状態になった場合のユーザ メッセージ。

AnyConnect Essentials および AnyConnect Premium の両方のライセンスには、サポートされる VPN セッションの合計数を指定する段階オプションがあります。

Cisco Secure Mobility for AnyConnect Premium ライセンスまたは Cisco Secure Mobility for AnyConnect Essentials ライセンスでアクティブ化された Cisco IronPort Web セキュリティ アプライアンスによって、適応型セキュリティ アプライアンスを使用するブラウザベースの SSL セッションおよび AnyConnect VPN セッションの以下のサービスが提供されます。

- アクセプタブル ユース ポリシーを強制し、すべての HTTP と HTTPS の要求を許可または拒否することによって、安全でないと見なされる Web サイトからエンドポイントを保護します。
- すべての VPN セッションのインターネット使用状況レポートへの管理者アクセスを提供します。

これらのサービスでは、Cisco IronPort Web セキュリティ アプライアンス ライセンスが必要です。Cisco Secure Mobility for AnyConnect Premium ライセンスをアクティブ化するには、適応型セキュリティ アプライアンスでの AnyConnect Premium ライセンスまたは AnyConnect Essentials ライセンスのいずれかをアクティブ化する必要があります。Cisco Secure Mobility for AnyConnect Essentials ライセンスのアクティブ化でも、適応型セキュリティ アプライアンスでの AnyConnect Essentials ライセンスをアクティブ化する必要があります。適応型セキュリティ アプライアンスでアクティブ化した Premium ライセンスと組み合わせて、Web セキュリティ アプライアンスでアクティブ化した Essentials ライセンスは使用できません。Web セキュリティ アプライアンスでアクティブ化した AnyConnect ライセンスは、適応型セキュリティ アプライアンスでアクティブ化した AnyConnect ライセンスによってサポートされる VPN セッションの数に一致するか、または超えている必要があります。

Standalone オプションと WebLaunch オプション

ユーザは AnyConnect を次のモードで使用できます。

- Standalone モード：ユーザは、Web ブラウザを使用せずに AnyConnect 接続を確立できます。ユーザの PC に AnyConnect を永続的にインストールした場合、Standalone モードで実行できます。Standalone モードでは、ユーザは AnyConnect をその他のアプリケーションと同じように開き、ユーザ名とパスワード クレデンシャルを AnyConnect GUI のフィールドに入力します。システムの設定によっては、グループを選択しなければならない場合もあります。接続が確立すると、ASA は、ユーザの PC 上の AnyConnect のバージョンを調べ、必要に応じて、クライアントは最新バージョンをダウンロードします。
- WebLaunch モード：ユーザは、HTTPS プロトコルを使用して、ブラウザの [アドレス（Address）] または [場所（Location）] フィールドに ASA の URL を入力します。次に、ユーザ名とパスワードの情報を [ログイン（Logon）] 画面で入力し、グループを選択して、[送信（Submit）] をクリックします。バナーが指定されている場合はその情報が表示され、[続行（Continue）] をクリックしてバナーを確認します。

ポータル ウィンドウが表示されます。AnyConnect を開始するには、メイン ペインで [AnyConnect の起動（Start AnyConnect）] をクリックします。一連の文書ウィンドウが表示されます。[接続を確立しました（Connection Established）] ダイアログボックスが表示されると、接続が機能し、ユーザがオンライン アクティビティを処理できるようになります。

ASA を設定して AnyConnect パッケージを展開するときは、企業のソフトウェア展開システムを使用して AnyConnect を展開する場合でも、ASA が、AnyConnect のバージョンがセッションを確立できる、唯一の適用ポイントであることを確認します。ASA に AnyConnect パッケージをロードするとき、ASA にロードされるバージョンと同じバージョンのみが接続できるポリシーを適用します。AnyConnect は ASA に接続すると自動的にアップグレードされます。または、クライアントが ASA のクライアント パッケージ ファイルの要件を排除して、クライアント ダウンローダを無視するかどうかを指定するローカル ポリシー ファイルを展開できます。ただし、WebLaunch や自動アップデートのようなその他の機能が無効になります。

AnyConnect ライセンス オプション

以下のセクションでは、ライセンス オプションを AnyConnect コンポーネントに関連付けます。

ネットワーク アクセス マネージャ

AnyConnect ネットワーク アクセス マネージャは、無償でシスコの無線アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、および RADIUS サーバで使用できるようにライセンスされています。AnyConnect Essentials ライセンスまたは Premium ライセンスは必要ありません。関連するシスコの装置では、現在の SmartNet 契約が必要です。

Web セキュリティ

Web セキュリティには、サポート対象となるエンドポイントの数を指定する Web セキュリティ ライセンスが必要です。

VPN ライセンス

SSL および IKEv2 アクセスの AnyConnect サポートには、同時にサポートされるリモート アクセス セッションの最大数を指定する、以下のいずれかのライセンスが必要です。

- AnyConnect Essentials ライセンス
- AnyConnect Premium SSL VPN Edition ライセンス

いずれのライセンスも AnyConnect 基本機能をサポートしています。

表 1-1 は Essentials ライセンスおよび Premium ライセンスと組み合わせることができるライセンスを示しています。

表 1-1　VPN の高度な AnyConnect ライセンス オプション

セッション ライセンス	ライセンス オプション	基本アクセス	ログイン後の VPN 常時接続	マルウェア防御、アクセプタブル ユース ポリシーの適用、および Web でのデータ漏洩の防止	クライアントレス アクセス	エンドポイント アセスメント	エンドポイント修復	ビジネス継続性
AnyConnect Essentials	(ベース ライセンス)	✓						
	Cisco Secure Mobility for AnyConnect Essentials	✓	✓	✓				
AnyConnect Premium SSL VPN Edition	(ベース ライセンス)	✓	✓		✓	✓		
	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓		
	Advanced Endpoint Assessment	✓	✓		✓	✓	✓	
	Flex[1]	✓	✓	✓	✓	✓	✓	✓

1. Flex ライセンスは、マルウェア防御、アクセプタブル ユース ポリシーの適用、Web でのデータ漏洩の防止、およびエンドポイント修復の各機能がライセンスされている場合に限り、これらの機能に対するビジネス継続性をサポートします。

AnyConnect Essentials、*AnyConnect Premium SSL VPN Edition*、*Advanced Endpoint Assessment*、および *Flex* の各ライセンスは、8.0(x) 以降を実行しているシスコ適応型セキュリティ アプライアンス（ASA）でアクティブ化している必要がありますが、それ以降のバージョンの ASA が必要な機能もあります。

Cisco Secure Mobility ライセンスは、7.0 以降を実行する Cisco IronPort Web Security Appliance（WSA）でアクティブ化する必要があります。

ASA での *AnyConnect Mobile* ライセンスのアクティブ化はモバイル アクセスに対応していますが、この表の機能には対応していません。AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのいずれかで、オプションとして使用できます。

AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのいずれかで使用できる機能のリストについては、基本機能テーブルを参照してください。

表 1-1 に示すオプション ライセンスでイネーブルにされている機能は次のとおりです。

- *ログイン後の VPN 常時接続*は、ユーザがコンピュータにログインすると、自動的に VPN セッションを確立します。詳細については、常時接続 VPN を参照してください。この機能には常時接続 VPN に関する接続障害ポリシーおよびキャプティブ ポータル ホットスポットの検出と修復も含まれています。

- *マルウェア防御、アクセプタブル ユース ポリシーの適用、および Web でのデータ漏洩の防止*は、Cisco IronPort Web Security Appliance（WSA）で提供される機能です。詳細については、『*Cisco IronPort Web Security Appliances Introduction*』を参照してください。
- *クライアントレス アクセス*では、ブラウザを使用して VPN セッションを確立し、特定のアプリケーションでブラウザを使用して、このセッションにアクセスできます。
- *エンドポイント アセスメント*は、選択したアンチウイルス ソフトウェアのバージョン、アンチスパイウェアのバージョン、関連する更新定義、ファイアウォール ソフトウェアのバージョン、および企業財産の検証チェックがポリシーを遵守しているかどうかを確認し、VPN にアクセスできるようにセッションに資格を与えます。
- *エンドポイントの修復*は、エンドポイントの障害を解決し、アンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェアおよび定義ファイルの各要件に関する企業の要件を満たそうとします。
- *ビジネス継続性*は、ライセンスされたリモート アクセス VPN セッション数を増やし、大流行など異常事態時の一時的な使用の急増に備えます。各 Flex ライセンスは、ASA 専用であり、60 日間のサポートを提供します。この日数は、連続した日数および連続していない日数の両方で構成できます。

『*Cisco Secure Remote Access: VPN Licensing Overview*』では、AnyConnect ライセンス オプションおよび SKU の例が簡単に説明されています。

AnyConnect の機能、ライセンス、リリース要件、および各機能に対応しているエンドポイント OS の詳しいリストについては、『*Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.0*』を参照してください。

コンフィギュレーションおよび導入の概要

ユーザはブラウザで ASA に VPN 接続を行う場合、AnyConnect Profile エディタを使用して、プロファイル ファイルの AnyConnect 機能を設定します。次に、ASA を設定して AnyConnect クライアントとともにこのファイルを自動的にダウンロードします。プロファイル ファイルによって、ユーザ インターフェイスの表示が決まり、ホスト コンピュータの名前とアドレスが定義されます。さまざまなプロファイルを作成し、ASA で設定されたグループ ポリシーに割り当てることで、これらの機能へのアクセスを区別できます。該当するグループ ポリシーへの割り当てに続いて、ASA は、接続設定時にユーザに割り当てられたプロファイルを自動的にプッシュします。

プロファイルによって、接続設定に関する基本情報が提供されますが、ユーザはそれを管理または変更できません。プロファイルは、アクセスできるようにするセキュア ゲートウェイ（ASA）ホストを識別できるようにする XML ファイルです。さらに、ユーザについての追加の接続属性および制約がプロファイルで伝搬されます。一部の機能では、プロファイルの特定の設定をユーザ設定可能として指定できます。AnyConnect GUI は、これらの設定のコントロールをエンド ユーザに表示します。

通常、ユーザごとに 1 つのプロファイル ファイルを使用します。このプロファイルには、ユーザが必要とするすべてのホスト、および必要に応じて追加の設定が含まれます。特定のユーザに複数のプロファイルを割り当てたい場合があります。たとえば、複数の場所で作業するユーザは、複数のプロファイルが必要な場合があります。ただし、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。特定のホストに固有の設定など、その他の設定は、選択されたホストにより異なります。

または、後でアクセスできるよう、エンタープライズ ソフトウェア導入システムを使用して、プロファイル ファイルおよびクライアントをアプリケーションとしてコンピュータにインストールできます。

AnyConnect Secure Mobility 機能の設定ガイドライン

AnyConnect Secure Mobility は、VPN エンドポイントのセキュリティを最適化するために設定できる機能セットです。AnyConnect Secure Mobility Client オプションをすべて設定するには、次の項を参照してください。

ステップ 1　「AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定」（P.2-49）に移動します。

ステップ 2　『*Cisco AnyConnect Secure Mobility Solution Guide*』を AnyConnect をサポートするための WSA を設定する注意事項として使用します。

ステップ 3　AnyConnect プロファイル エディタを使用して次の機能を設定します。

- 「Trusted Network Detection」（P.3-17）
- 「常時接続 VPN」（P.3-19）
- 「常時接続 VPN 用の [接続解除（Disconnect）] ボタン」（P.3-26）
- 「常時接続 VPN に関する接続障害ポリシー」（P.3-27）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-30）
- 「SCEP による認証登録の設定」（P.3-34）

API

AnyConnect との VPN 接続を別のアプリケーションから自動的に行う場合は、次のような Application Programming Interface（API）を使用します。

- プリファレンス
- tunnel-group メソッドの設定

API パッケージには、AnyConnect の C++ インターフェイスに対応するマニュアル、ソース ファイル、およびライブラリ ファイルが含まれています。Windows、Linux、および Mac OS X 上で AnyConnect を構築するために、ライブラリおよびプログラム例を使用できます。API パッケージには Windows プラットフォーム用のプロジェクト ファイル（Makefile）が付属しています。その他のプラットフォームに対しては、プラットフォーム固有のスクリプトにサンプル コードのコンパイル方法が示されています。アプリケーション（GUI、CLI、または組み込みアプリケーション）と、これらのファイルやバイナリをリンクできます。

API は、クライアントの VPN 機能のみをサポートします。これは、ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリなど、オプションの AnyConnect モジュールをサポートしません。

ホスト スキャンのインストール

ホストが VPN 接続を確立することによって発生するイントラネット感染の可能性を減らすために、ホスト スキャンを設定して、アンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェア（および VPN セッションを確立する条件として、関連する定義ファイルの更新）をダウンロードおよ

び確認できます。以前は、ホスト スキャンは Cisco Secure Desktop（CSD）のコンポーネントとしてのみ使用できました。AnyConnect Secure Mobility Client の今回のリリースでは、ホスト スキャンは、CSD とは別にインストールおよびアップデートできる別個のモジュールになりました。

（注）　ホスト スキャンおよび一部のサードパーティ ファイアウォールは、グループ ポリシーにより任意に導入されたファイアウォール機能と干渉する可能性があります。

ホスト スキャンのインストールおよび管理の詳細については、第 5 章「ホスト スキャンの設定」を参照してください。

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。

ASA から展開された場合、リモート ユーザは、ASA への最初の SSL 接続を行います。リモート ユーザは、クライアントレス SSL VPN 接続を受け入れるように設定されている ASA の IP アドレスまたは DNS 名をブラウザに入力します。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。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

Cisco AnyConnect Secure Mobility Client バージョン 3.0 では、新規モジュールが AnyConnect クライアント パッケージと統合されています。ASA を使用して AnyConnect を展開する場合、ASA では、すべてのオプション モジュールも展開できます。ASA によって AnyConnect クライアントおよびさまざまなモジュールを展開する方法を「Web 展開」と呼びます。

SMS を使用して AnyConnect ソフトウェアをエンドポイントに配布し、エンドポイントが ASA に接続する前にインストールする方法を「事前展開」と呼びます。この方法を使用すると、VPN サービスを実現するコア クライアントおよびオプション モジュールを展開できますが、インストール順序およびその他の詳細事項に特に注意する必要があります。

バージョン 3.0 には、ASA への SSL と IPsec（IKEv2）によるセキュア VPN 接続を実現するコア AnyConnect VPN クライアントの他に、次のモジュールがあります。

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

ここでは、次の項目について説明します。

- 「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-44）
- 「AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定」（P.2-49）

（注）　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）だけがある場合、ASA 上で複数の AnyConnect クライアント パッケージを保存およびロードすると、問題が発生することがあります。この制限事項は、オプション モジュールを含む AnyConnect 3.0 クライアントの場合、特に該当します。フラッシュ メモリにパッケージ ファイルを保持するために十分な容量がある場合でも、クライアント イメージの unzip とロードのときに 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。

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 プロファイルでイネーブルにします。プロファイルは、コア クライアントと VPN 機能のための設定およびオプション クライアント モジュール（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）のための設定を含む XML ファイルであり、複数ファイルあります。ASA は AnyConnect のインストールおよび更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

プロファイルは、ASDM から起動する、GUI ベースの便利なツールである、AnyConnect プロファイル エディタを使用して設定できます。Windows 用 AnyConnect ソフトウェア パッケージ バージョン 2.5 以降には、エディタが含まれています。このエディタは、AnyConnect パッケージを ASA にロードし、AnyConnect クライアント イメージとして指定するとアクティブ化されます。

ASDM に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロン バージョンも使用できます。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。

これで、クライアント プロファイル XML ファイルを手動で編集し、プロファイルとして ASA にインポートできます。

2 つのバージョンの Cisco AnyConnect プロファイル エディタは、テレメトリ クライアント プロファイルを設定するプロファイル エディタには「スタンドアロン」バージョンがない点が異なり、各エディタは別々に配布、起動されます。その他のすべての点は、2 つのバージョンのプロファイル エディタで同一です。

ASA 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。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は、複数の VPN プロファイルを必要とすることがあります。Start Before Logon 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、特定のホストに固有であり、選択したホストによって異なります。

（注）　プロファイルが複数ある場合、AnyConnect では、プロファイル内のサーバ リストを統合して、GUI のドロップリストにすべてのサーバを表示します。ユーザがサーバを選択すると、そのサーバを含むプロファイルが AnyConnect で使用されます。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、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。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 2-15 を参照してください。クライアント プロファイルの作成の詳細については、次の各項を参照してください。

- 「統合された 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.2-44）

統合された 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 バージョン 2.5 以降（すべてのオペレーティング システム用）にはプロファイル エディタが含まれています。プロファイル エディタは、ASA 上で AnyConnect ソフトウェア パッケージを SSL VPN クライアント イメージとしてロードした時点で ASDM によりアクティブ化されます。

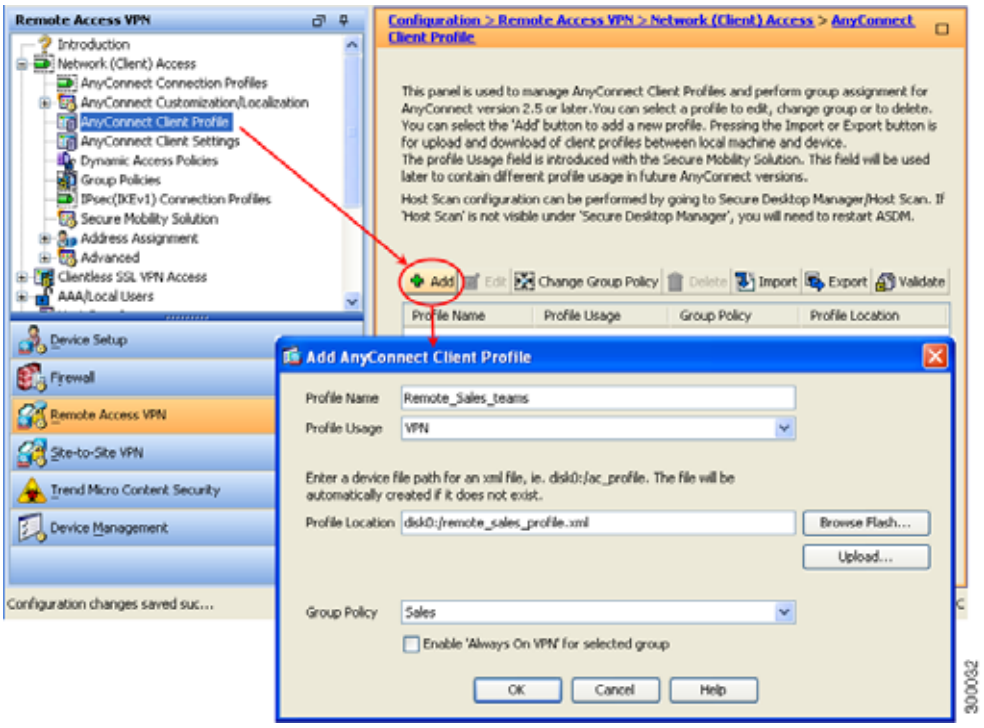
複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからプロファイル エディタがロードされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

ASDM でプロファイル エディタをアクティブ化する手順は次のとおりです。

ステップ 1　AnyConnect ソフトウェア パッケージを SSL VPN イメージとしてロードします。まだ行っていない場合は、第 2 章「AnyConnect をダウンロードするための ASA の設定」を参照してください。

ステップ 2　[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。[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ペインが開きます。[追加（Add）] をクリックします。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウが開きます（図 2-1）。

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　[プロファイルの使用（Profile Usage）] フィールドで、作成するクライアント プロファイルのタイプを、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはテレメトリから指定します。

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。

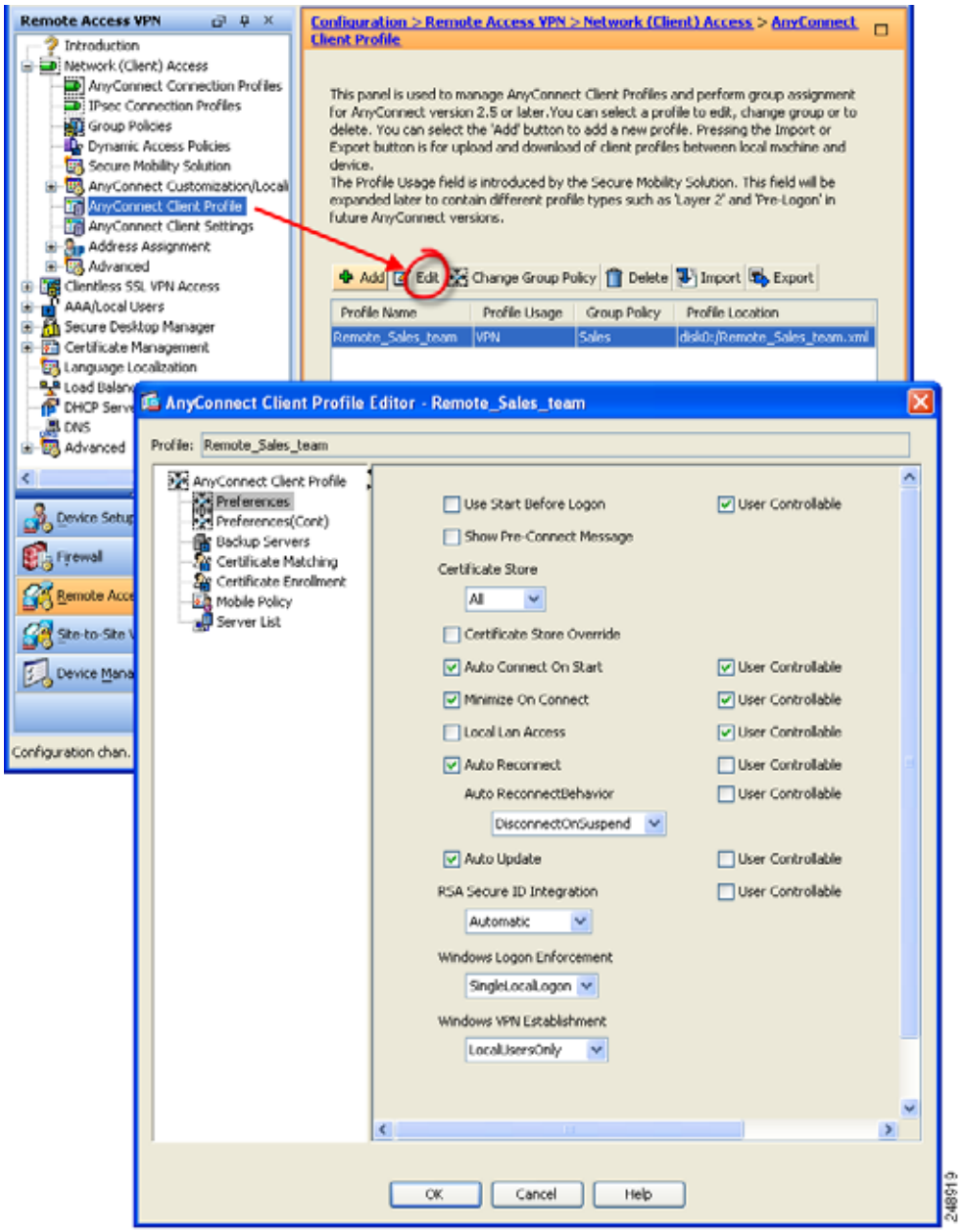
ステップ 6　[OK] をクリックします。ASDM によりプロファイルが作成され、そのプロファイルはプロファイル テーブルに表示されます。

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。[編集（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（図 2-2）。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 8　[適用（Apply）] をクリックします。

ステップ 9　ASDM を終了して再起動します。

図 2-2　VPN クライアント プロファイルの編集例



AnyConnect クライアント プロファイルの展開

AnyConnect クライアント プロファイルは、以下の方法を使用して展開できます。

- 「ASA からの AnyConnect クライアント プロファイルの展開」（P.2-6）
- 「スタンドアロン プロファイル エディタで作成したクライアント プロファイルの展開」（P.2-7）

ASA からの AnyConnect クライアント プロファイルの展開

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　「統合された 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 に統合されているプロファイル 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」

（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.3-54）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」

ステップ 3　クライアント プロファイルをグループ ポリシーと関連付けます。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 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、[グループ ポリシーの変更（Change Group Policy）] をクリックします。

ステップ 5　[プロファイルのグループ ポリシー <ポリシー名> の変更（Change Group Policy for Profile ***policy name***）] ウィンドウで、[使用可能なグループ ポリシー（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 [選択されたグループ ポリシー（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 クライアント プロファイル（AnyConnect Client Profile）] ページで、[適用（Apply）] をクリックします。

ステップ 8　[保存（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 エディタで作成したクライアント 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、「事前展開された AnyConnect モジュールのインストール」（P.2-32）を参照してください。スタンドアロン AnyConnect プロファイル エディタのインストールと使用の手順については、「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-44）を参照してください。

AnyConnect を Web 展開する ASA の設定

この項では、次のトピックについて取り上げます。

ASA 展開用の AnyConnect ファイル パッケージ

表 2-1 に、ASA による AnyConnect 展開用の AnyConnect ファイル パッケージの名前を示します。

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 3.0 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。

証明書に関するユーザ プロンプトを最小限にする

AnyConnect のセットアップ中のユーザへのプロンプトを最小限にするには、次のようにクライアント PC と ASA の証明書データを一致させます。

- ASA 上の証明書に対して Certificate Authority（CA; 認証局）を使用する場合は、クライアント マシンで信頼済み CA として設定された証明書を選択します。
- ASA 上の自己署名証明書を使用するか、自社内の証明書サーバで生成した証明書を使用する会社の場合は、必ず、信頼できるルート証明書として証明書をクライアントにインストールしてください。

  手順はブラウザによって異なります。この項の次の手順を参照してください。
- VPN の確立に先立って、エンドポイントから認証局および内部証明書サーバに到達可能である必要があります。
- ASA 証明書の Common Name（CN; 通常名）と、AnyConnect が接続に使用する名前が一致していることを確認します。デフォルトでは、ASA 証明書の CN フィールドは IP アドレスになっています。AnyConnect が DNS 名を使用する場合は、ASA 証明書の CN フィールドをその名前に変更します。

  証明書に SAN（Subject Alternate Name）が含まれている場合、ブラウザは [件名（Subject）] フィールドの CN 値を無視し、[SAN] フィールドの [DNS 名（DNS Name）] エントリを調べます。

  ユーザがホスト名を使用して ASA に接続する場合は、SAN に ASA のホスト名とドメイン名が含まれている必要があります。たとえば、SAN フィールドには次が含まれます。
  `DNS Name=hostname.domain.com.`

  ユーザが IP アドレスを使用して ASA に接続する場合は、SAN に ASA の IP アドレスが含まれている必要があります。たとえば、SAN フィールドには `DNS Name=209.165.200.254` と入力されます。

AnyConnect 用 Cisco Security Agent ルールの作成

AnyConnect のインストール中に、Cisco Security Agent（CSA）から警告が表示されることがあります。

現在出荷中の CSA バージョンには、AnyConnect と互換性のある組み込みルールがありません。CSA バージョン 5.0 以降を使用すると、次の手順により次のルールを作成できます。

ステップ 1　ルール モジュール「Cisco Secure Tunneling Client Module」で次の FACL を追加します。

```
Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx"
Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web
Browsers"
Attempt: Read file, Write File
```

すべての @SYSTEM\vpnweb.ocx ファイルで、次のことを行います。

ステップ 2　アプリケーション クラス :「Cisco Secure Tunneling Client - Installation Applications」に次のプロセス名を追加します。

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect Secure Mobility Client\vpndownloader.exe
```

Internet Explorer の信頼済みサイト リストに対する ASA の追加（Vista および Windows 7）

Microsoft Internet Explorer（MSIE）ユーザは、信頼済みサイト リストに ASA を追加するか、Java をインストールすることをお勧めします。信頼済みサイト リストに追加すると、ActiveX コントロールで、最小限のユーザ操作によるインストールが可能になります。セキュリティが強化された Windows XP SP2 のユーザにとって、この推奨事項は特に重要です。

Vista ユーザおよび Windows 7 ユーザの場合は、AnyConnect クライアントを展開する ASA が、ユーザ コンピュータ上の信頼済みサイトのリストにある必要があります。そうでない場合は、WebLaunch は起動しません。

ユーザは、次の手順を実行することにより、Microsoft Internet Explorer の信頼済みサイト リストに ASA を追加できます。

（注）　これは、Windows Vista および Windows 7 で WebLaunch を使用するために必要です。

ステップ 1　[ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。[インターネット オプション（Internet Options）] ウィンドウが開きます。

ステップ 2　[セキュリティ（Security）] タブをクリックします。

ステップ 3　[信頼されたサイト（Trusted Sites）] アイコンをクリックします。

ステップ 4　[サイト（Sites）] をクリックします。[信頼されたサイト（Trusted Sites）] ウィンドウが開きます。

ステップ 5　ASA のホスト名または IP アドレスを入力します。複数のサイトをサポートするため、https://*.yourcompany.com のようなワイルドカードを使用して、yourcompany.com ドメイン内のすべての ASA 5500 が使用できるようにします。

ステップ 6　[追加（Add）] をクリックします。

ステップ 7　[OK] をクリックします。[信頼されたサイト（Trusted Sites）] ウィンドウが閉じます。

ステップ 8　[インターネット オプション（Internet Options）] ウィンドウで [OK] をクリックします。

ブラウザの警告ウィンドウに対応するセキュリティ証明書の追加

ここでは、ブラウザの警告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。

Microsoft Internet Explorer の [セキュリティ アラート（Security Alert）] ウィンドウへの対応

ここでは、Microsoft Internet Explorer の [セキュリティ アラート（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。[セキュリティ アラート（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.
```

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　[セキュリティの警告（Security Alert）] ウィンドウの [証明書の表示（View Certificate）] をクリックします。[証明書（Certificate）] ウィンドウが開きます。

ステップ 2　[証明書のインストール（Install Certificate）] をクリックします。[証明書インポート ウィザード ようこそ（Certificate Import Wizard Welcome）] が開きます。

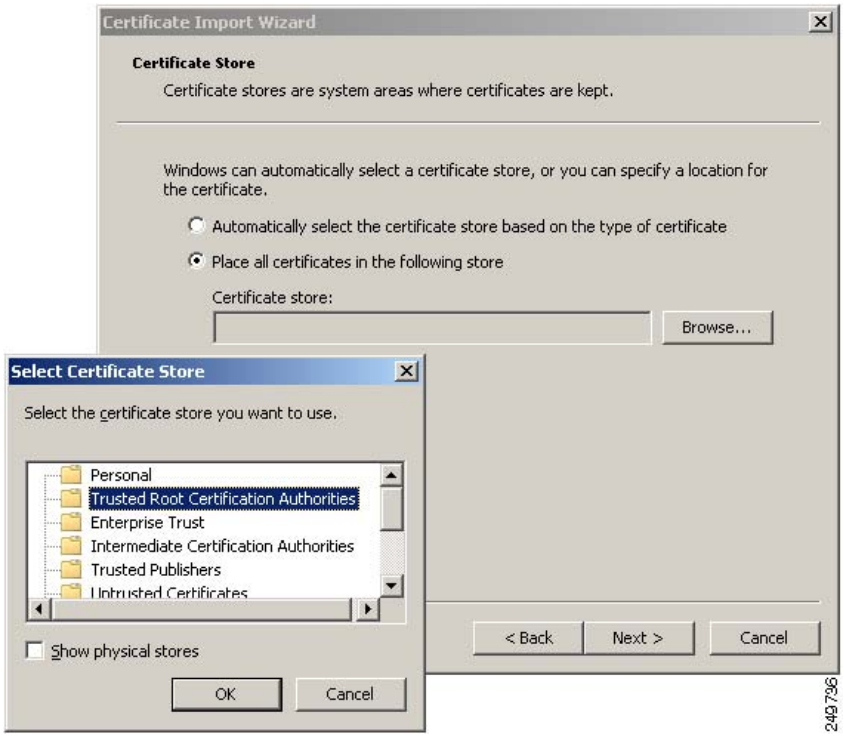
ステップ 3　[次へ（Next）] をクリックします。[証明書インポート ウィザード - 証明書ストア（Certificate Import Wizard - Certificate Store）] ウィンドウが開きます。

ステップ 4　[すべての証明書を次のストアに配置する（Place all certificates in the following store）] を選択します。

ステップ 5　[参照（Browse）] をクリックします。[証明書ストアの選択（Select Certificate Store）] ウィンドウが開きます。

ステップ 6　ドロップダウン リストで、[信頼済みルート認証局（Trusted Root Certification Authorities）] を選択します（図 2-3 を参照）。

図 2-3　　証明書のインポート



ステップ 7　[次へ（Next）] をクリックします。[証明書インポート ウィザード - 完了（Certificate Import Wizard - Completing）] ウィンドウが開きます。

ステップ 8　[完了（Finish）] をクリックします。別の [セキュリティ上の警告（Security Warning）] ウィンドウで「Do you want to install this certificate?」というメッセージが表示されます。

ステップ 9　[はい（Yes）] をクリックします。[証明書インポート ウィザード（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、[証明書（Certificate）] ウィンドウを閉じます。

ステップ 12　[はい（Yes）] をクリックして、[セキュリティ アラート（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 [不明な認証局により認証済み（Certified by an Unknown Authority）] ウィンドウへの対応

ここでは、[不明な認証局により認証された Web サイト（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　[不明な認証局により認証された Web サイト（Web Site Certified by an Unknown Authority）] ウィンドウの [証明書の検証（Examine Certificate）] をクリックします。[証明書ビューア（Certificate Viewer）] ウィンドウが開きます。

ステップ 2　[この証明書を常に承認する（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。

複数の AnyConnect イメージをロードする場合の接続時間の短縮方法

複数の AnyConnect イメージを ASA にロードする場合は、リモート ユーザ数が最大のときに接続時間が最短になる順序で、イメージをロードする必要があります。

セキュリティ アプライアンスは、オペレーティング システムと一致するまで、AnyConnect イメージの一部をリモート コンピュータにダウンロードします。イメージのダウンロードは、リストの上から順に行われます。そのため、リモート コンピュータで最も頻繁に使用されているオペレーティング システムと一致するイメージを、リストの先頭に指定する必要があります。

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

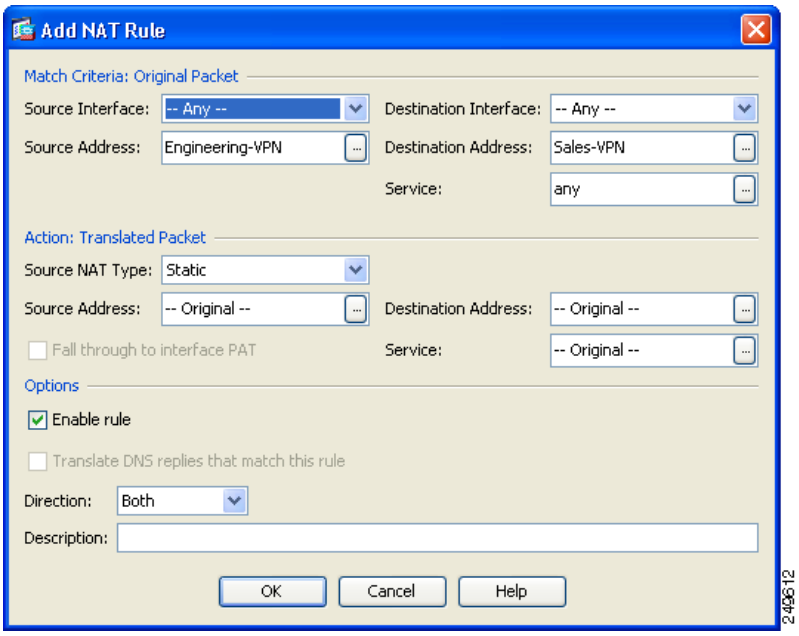
ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

ステップ 1　ASDM にログインし、[設定（Configuration）] > [ファイアウォール（Firewall）] > [NAT ルール（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 ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。[NAT ルールの追加（Add NAT rule）] ダイアログボックスの例については、図 2-4（P.2-12）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。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。

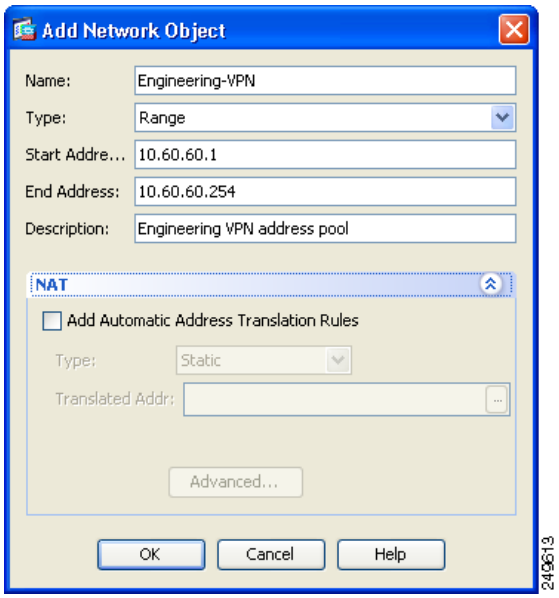
図 2-4　[NAT ルールの追加（Add NAT Rule）] ダイアログ ボックス



a.　[一致基準：元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス：（Source Interface:）] Any
- [宛先インターフェイス：（Destination Interface:）] Any
- [送信元アドレス：（Source Address:）] [送信元アドレス（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 2-5 を参照してください。
- [宛先アドレス：（Destination Address:）] [宛先アドレス（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 2-5　　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. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Static
- [送信元アドレス：（Source Address:）] Original
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

c. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

d. [OK] をクリックします。

e. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された 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. [送信（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、[同一インターフェイスに接続している複数のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）] オプションをイネーブルにする必要があります。これを行うには ASDM で、[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス（Interfaces）] を選択します。[インターフェイス（Interface）] パネルの下の [同一インターフェイスに接続している複数のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）] をオンにし、[適用（Apply）] をクリックします。

CLI の例：

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

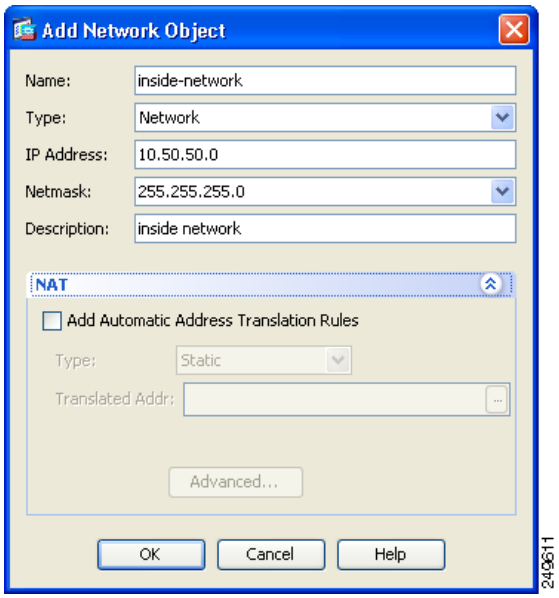
ステップ 4　Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。ステップ 2 で規則を作成したときのようにこの規則を作成します。ただし、[一致基準 : 元のパケット（Match criteria: Original Packet）] エリアで Engineering VPN アドレス プールを送信元アドレスおよび宛先アドレス両方として指定します。

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 ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。

a. [一致基準 : 元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス :（Source Interface:）] Any
- [宛先インターフェイス :（Destination Interface:）] Any
- [送信元アドレス :（Source Address:）] [送信元アドレス（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。
- [宛先アドレス :（Destination Address:）] [宛先アドレス（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 2-6　inside-network オブジェクトの追加



b. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Static
- [送信元アドレス：（Source Address:）] Original
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

c. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

d. [OK] をクリックします。

e. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された 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 ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。

b. [一致基準：元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス：（Source Interface:）] Any
- [宛先インターフェイス：（Destination Interface:）] Any [アクション：変換されたパケット（Action: Translated Packet）] エリアの [送信元アドレス（Source Address）] に [外部（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。
- [送信元アドレス：（Source Address:）] [送信元アドレス（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。
- [宛先アドレス：（Destination Address:）] Any

c. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Dynamic PAT (Hide)
- [送信元アドレス：（Source Address:）] [送信元アドレス（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。
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

d. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

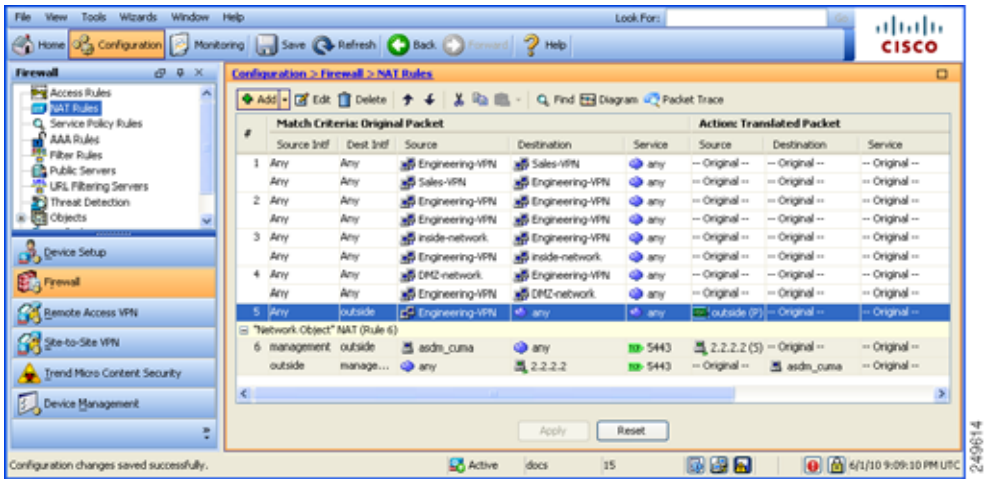
e. [OK] をクリックします。

f. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された 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 2-7　統合された NAT テーブル



ステップ 8　Engineering VPN アドレス プール、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接続するように Engineering VPN アドレス プールを設定した後で、Sales VPN アドレス プールについて、同じ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 [ファイル（File）] メニューで [実行コンフィギュレーションをフラッシュに保存する（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

Windows Vista および Windows 7 は、デフォルトでは、DES SSL 暗号化をサポートしません。ASA に DES-only を設定した場合、AnyConnect 接続は失敗します。これらのオペレーティング システムの DES 対応設定は難しいため、ASA には、DES のみの SSL 暗号化を設定しないことをお勧めします。

3G カードとの接続

一部の 3G 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。

- modem manually connect
- modem auto connect except when roaming
- 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。

AnyConnect をダウンロードするための ASA の設定

AnyConnect の Web 展開用に ASA を準備するには、次の手順を実行します。

ステップ 1　「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。

ステップ 2　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 3　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。[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 クライアント設定（AnyConnect Client Settings）] に移動します。AnyConnect イメージとして指定されたクライアント ファイルをリストした、[AnyConnect クライアント設定（AnyConnect Client Settings）] パネルが表示されます（図 2-8）。表示順序は、ASA によるリモート コンピュータへのダウンロード順序を示しています。

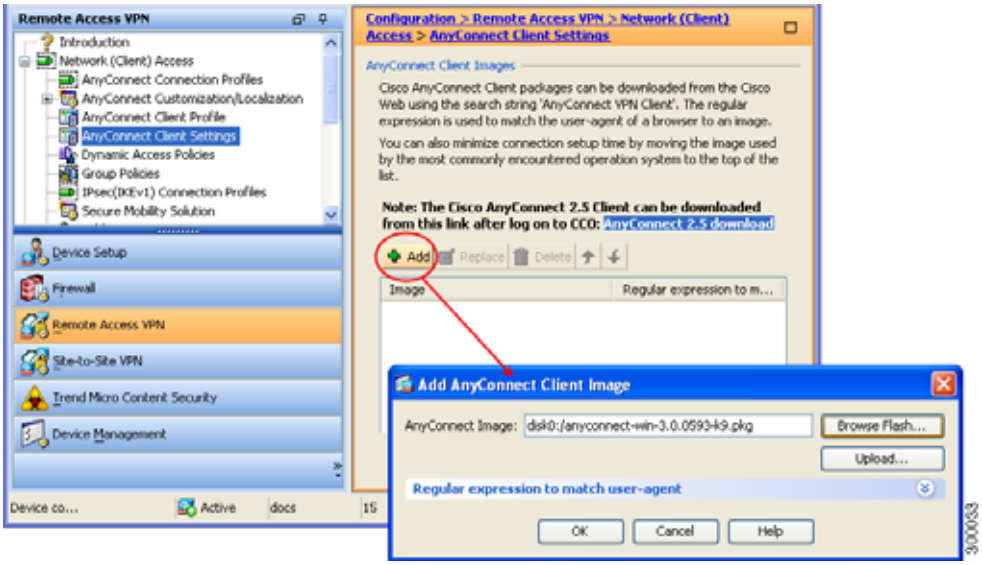
ステップ 4　AnyConnect イメージを追加するには、[AnyConnect クライアント イメージ（AnyConnect Client Images）] エリアで [追加（Add）] をクリックします。

- ASA にアップロードした AnyConnect イメージを選択するには、[フラッシュの参照（Browse Flash）] をクリックします。
- 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、[アップロード（Upload）] をクリックします。

ステップ 5　[OK] または [アップロード（Upload）] をクリックします。

ステップ 6　[適用（Apply）] をクリックします。

図 2-8　AnyConnect イメージの指定

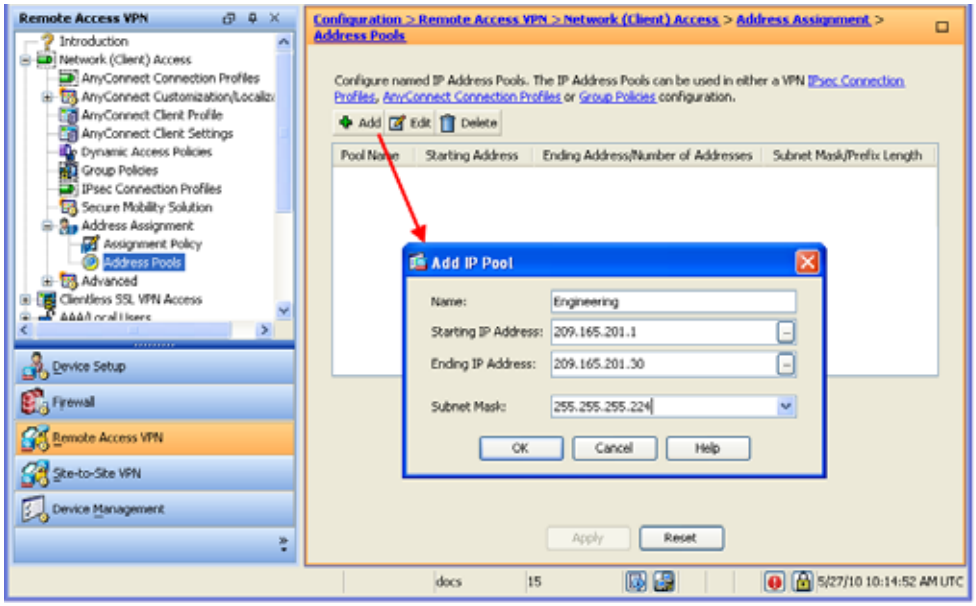


ステップ 7　アドレスの割り当て方式を設定します。

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方法もあります。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。

[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）] > [アドレス割り当て（Address Assignment）] > [アドレス プール（Address Pools）] を選択します（図 2-9）。[IP プールの追加（Add IP Pool）] ウィンドウにアドレス プール情報を入力します。

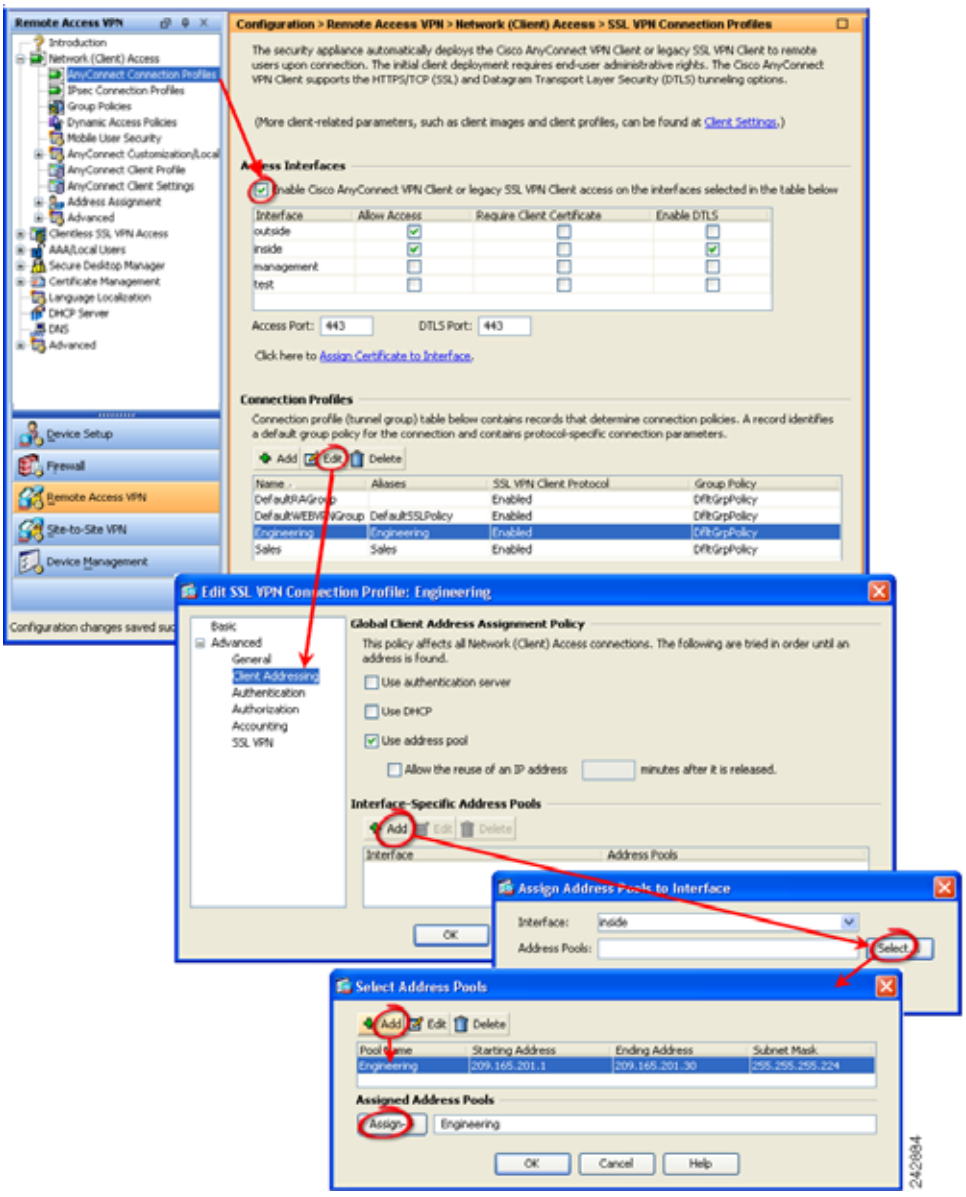
図 2-9　[IP プールの追加（Add IP Pool）] ダイアログ



ステップ 8　AnyConnect のダウンロードをイネーブルにし、接続プロファイルのアドレス プールを割り当てます。

[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 接続プロファイル（AnyConnect Connection Profiles）] を選択します。（図 2-10）の矢印に従って AnyConnect クライアントをイネーブルにしてから、アドレス プールを割り当てます。

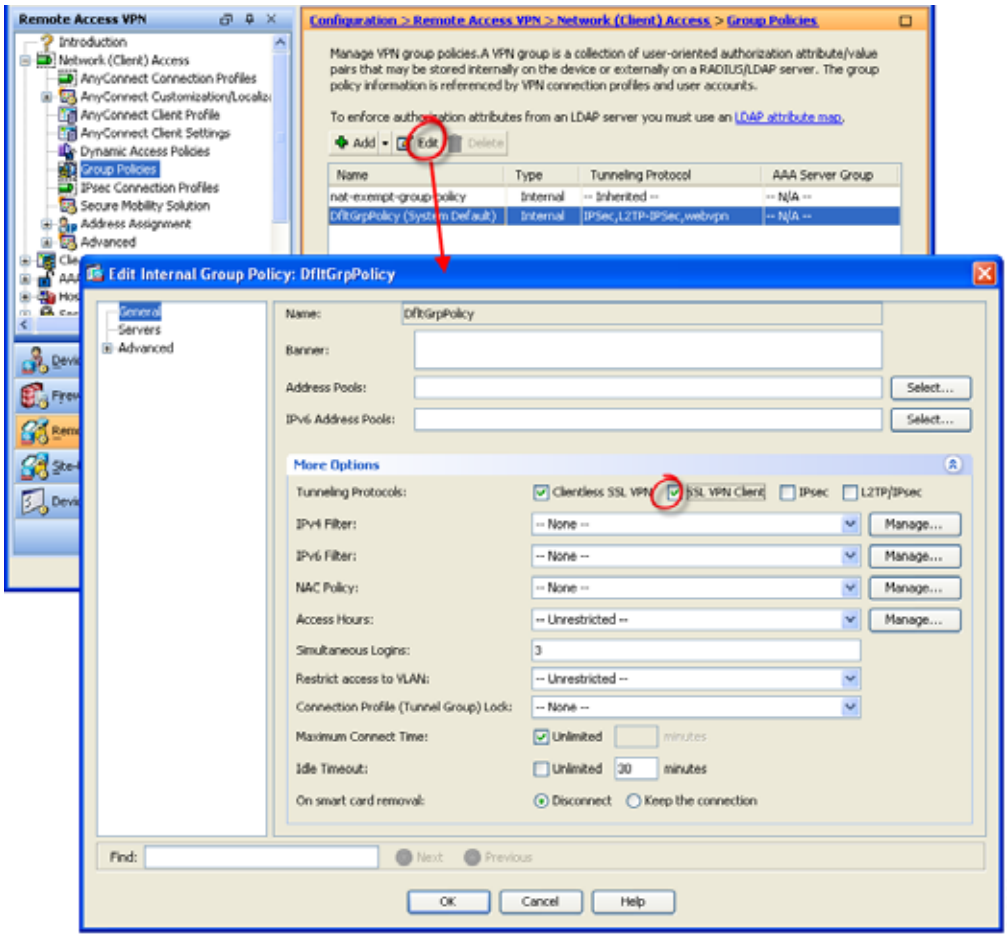
図 2-10　AnyConnect のダウンロードのイネーブル化



ステップ 9　グループ ポリシーで許可された VPN トンネリング プロトコルとして SSL VPN クライアントを指定します。

[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）] > [グループ ポリシー（Group Policies）] を選択します。[グループ ポリシー（Group Policies）] パネルが表示されます。図 2-11 の矢印に従って、グループの SSL VPN クライアントをイネーブルにします。

図 2-11　トンネリング プロトコルとしての SSL VPN の指定



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。

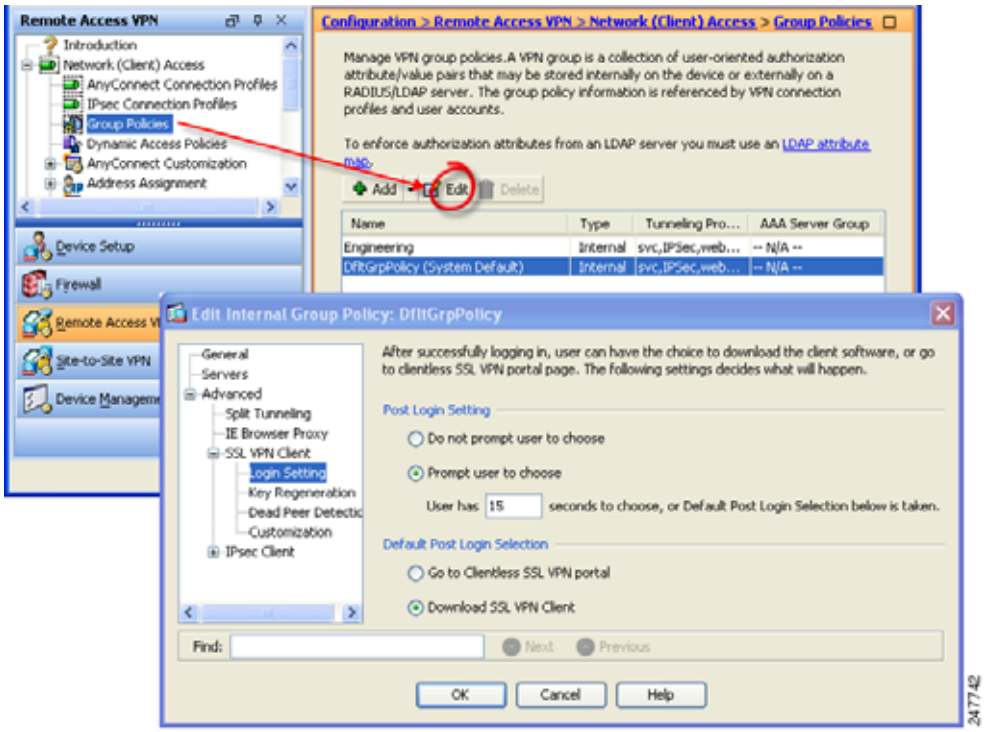
この機能は、グループ ポリシーまたはユーザに対して設定できます。このようなログイン設定を変更するには、次の手順に従ってください。

ステップ 1　[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）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます（図 2-12）。

ステップ 2　ナビゲーション ペインで、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [ログイン設定（Login Settings）] を選択します。[ログイン後の設定（Post Login settings）] が表示されます。必要に応じて [継承（Inherit）] チェックボックスをオフにし、[ログイン後の設定（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。

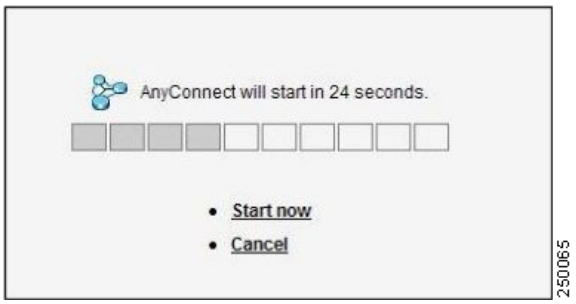
図 2-12　ログイン設定の変更



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 2-13 は、[Prompt user to choose] と [SSL VPN クライアントのダウンロード（Download SSL VPN 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 2-13　リモート ユーザに表示されるログイン後プロンプト



追加機能で使用するモジュールのイネーブル化

AnyConnect で機能をイネーブルにすると、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。

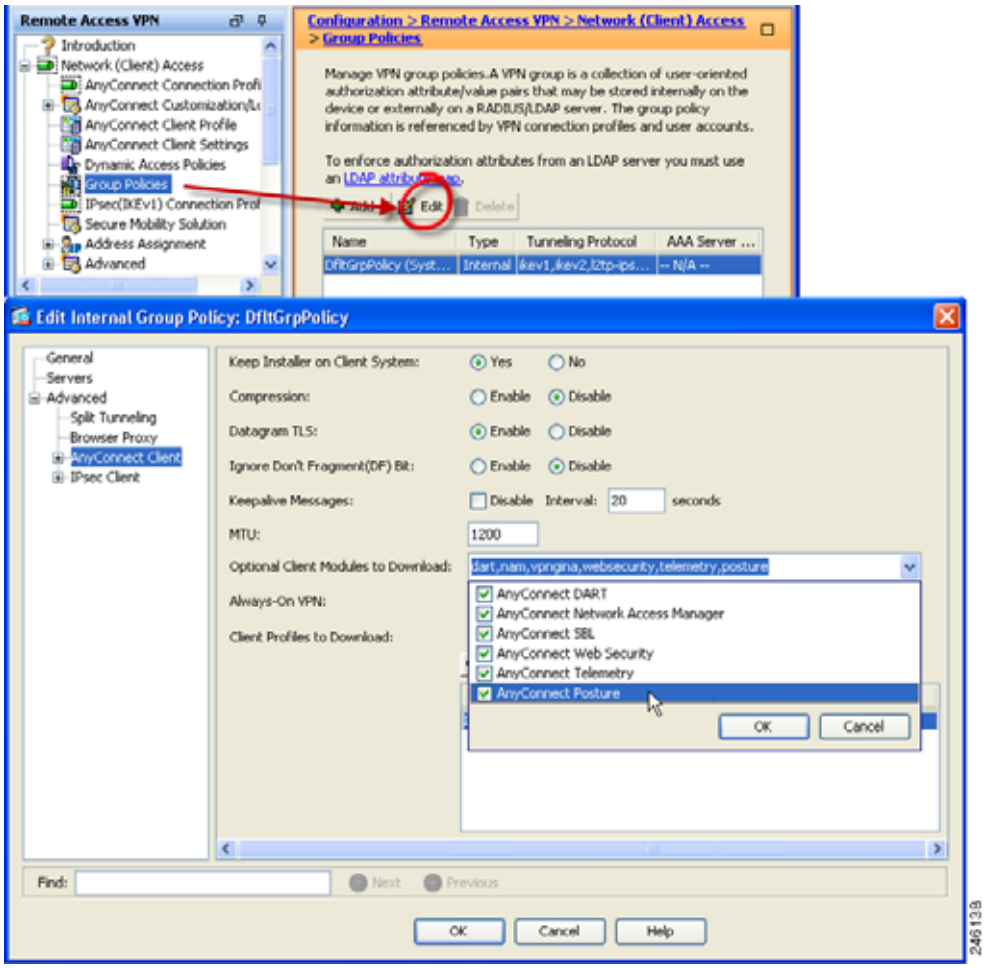
新機能をイネーブルにするには、グループ ポリシーまたはユーザ名の設定の一部として、新しいモジュール名を指定する必要があります。グループ ポリシーのモジュール ダウンロードをイネーブルにするには、次の手順に従います。

ステップ 1　[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）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます（図 2-14）。

ステップ 2　ナビゲーション ペインで、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] を選択します。 [ダウンロードするオプションのクライアント モジュール（Optional Client Module to Download）] ドロップリストをクリックし、モジュールを選択します。

- AnyConnect DART：DART をダウンロードすると、AnyConnect のインストールと収集に関する問題のトラブルシューティングに有用なデータを収集できます。
- AnyConnect ネットワーク アクセス マネージャ：このモジュールにより、最適なレイヤ 2 アクセス ネットワークの検出と選択ができ、有線とワイヤレスの両方のネットワークにアクセスするためのデバイス認証を実行できます。
- 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 をイネーブルにするさまざまな理由については、「Start Before Logon の設定」（P.3-7）を参照してください。
- AnyConnect Web セキュリティ：Web セキュリティは、HTTP トラフィックを ScanSafe スキャニング プロキシにルーティングするエンドポイント コンポーネントです。トラフィックは、プロキシ上で ScanSafe Web スキャニング サービスによって評価されます。
- AnyConnect テレメトリ：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 ポスチャ：ポスチャ モジュールにより、クライアントでは、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、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できます。

図 2-14　ダウンロードするオプションのクライアント モジュールの指定



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。

（注）　[ログイン前の起動（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イネーブル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 接続のイネーブル化

ここでは、ASA 上で IPsec IKEv2 接続をイネーブルにする手順を示します。

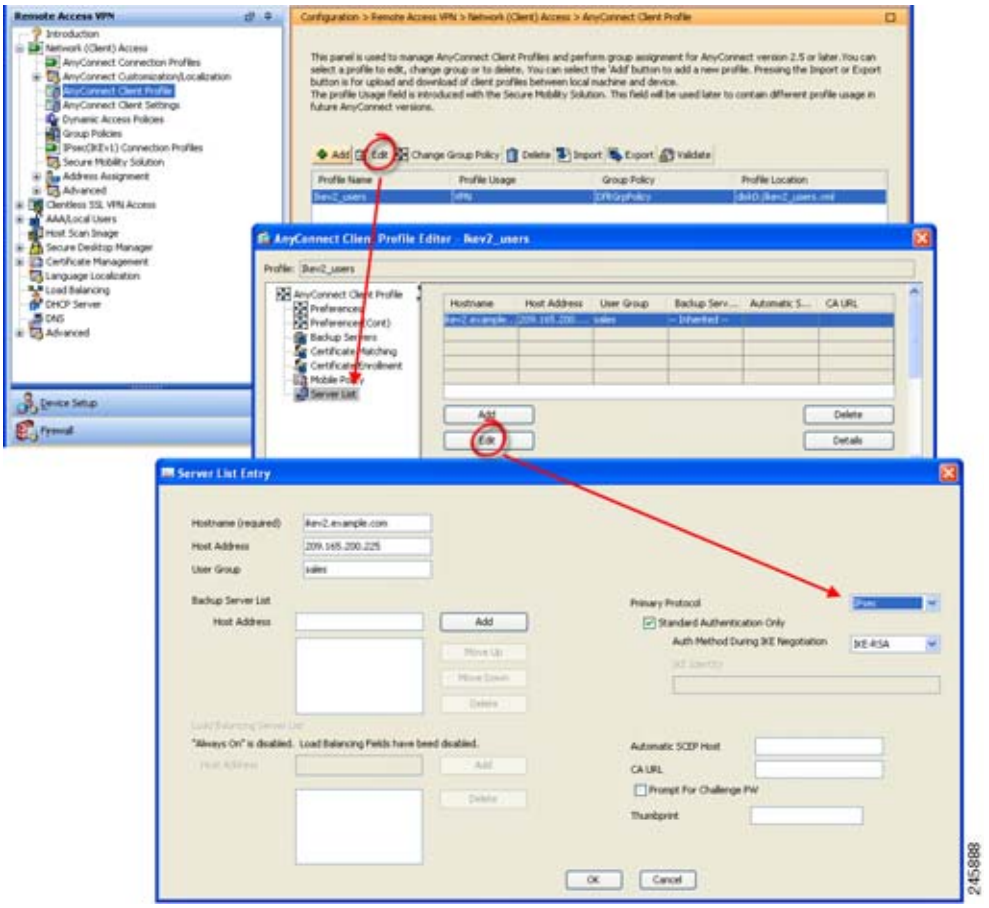
AnyConnect クライアント パッケージを ASA にロードした後で、次の手順を実行して、ASA に IPsec IKEv2 接続を設定します。

ステップ 1　AnyConnect VPN Wizard を実行します。[ツール（Tools）] > [ウィザード（Wizards）] > [AnyConnect VPN Wizard] を選択します（図 2-15）。ウィザードの手順に従って、IPsec IKEv2 接続用の基本 VPN 接続を作成します。

図 2-15　AnyConnect VPN Wizard

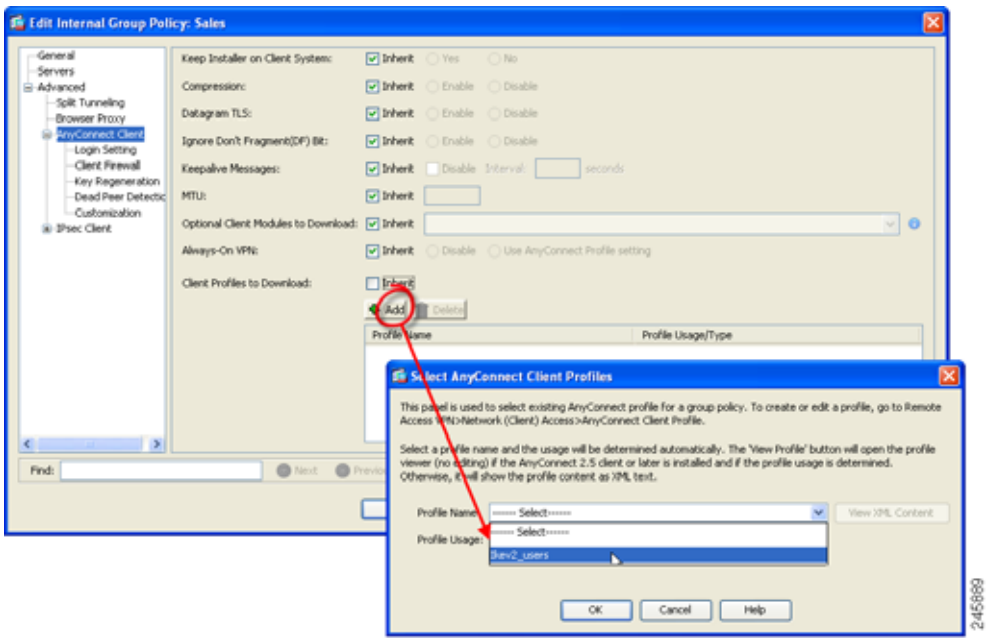
ステップ 2　プロファイル エディタを使用して、VPN プロファイルの [サーバ リスト（Server List）] エントリを編集します。[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します（図 2-16）。

図 2-16　AnyConnect クライアント プロファイルでの IKEv2 の指定



ステップ 3　VPN プロファイルを、使用するグループ ポリシーと関連付けます。[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）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを編集し、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] に移動します（図 2-17）。

図 2-17　　プロファイルとグループ ポリシーの関連付け



IKEv2-enabled 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ときは、IKEv2-enabled 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、7-zip、または同様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て選択します。

anyconnect-win-3.0.0xxx-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、[すべて選択（Select all）] をオフに、[AnyConnect VPN モジュール（AnyConnect VPN Module）] のみをオンにします。

仮想 CD マウント ソフトウェアによるクライアント プロファイルの事前展開

SlySoft、PowerISO などの仮想 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　仮想 CD マウント ソフトウェアを使用して、.ISO をマウントします。

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 2-3 を参照）。

表 2-3　クライアントの展開先パス

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/

（注）　前のリリースの AnyConnect では、AnyConnect コンポーネントはパス /opt/cisco/vpn にインストールされました。現在、AnyConnect コンポーネントは、パス /opt/cisco/anyconnect にインストールされます。

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する場合、MSI では、クライアント プロファイル（Profiles@@pl\vpn フォルダ）に配置されている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。

インストール後にプロファイルを手動で事前展開する場合は、手動か、Altiris などの SMS を使用してプロファイルをコピーすることにより、適切なフォルダにプロファイルを展開してください。

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>

AnyConnect クライアントおよびオプション モジュールの事前展開

ここでは、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クライアントを展開するために必要な情報など、AnyConnect Secure Mobility Client の事前展開プロセスについて説明します。

以下の項では、AnyConnect クライアントを事前展開する方法について説明します。

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 3.0 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。

表 2-4 に、事前展開する AnyConnect パッケージのファイル名を OS ごとに示します。

表 2-4　事前展開する AnyConnect パッケージ ファイルの名前

OS	AnyConnect 3.0 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 3.0 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 ファイルの展開」（P.2-30）
- 「インストール ユーティリティのユーザへの展開」（P.2-30）
- 「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）
- 「事前展開された AnyConnect モジュールのインストール」（P.2-32）
- 「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」（P.2-34）
- 「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.2-35）
- 「レガシー クライアントおよびオプション モジュールのアップグレード」（P.2-36）
- 「インストーラのカスタマイズとローカライズ」（P.2-36）

ISO ファイルの展開

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および MSI インストーラ ファイルを含む ISO パッケージ ファイルにバンドルされています。ISO パッケージ ファイルを展開すると、セットアップ プログラム（setup.exe）によって、インストール ユーティリティ メニューが実行および展開されます。このメニューは、インストールする AnyConnect モジュールをユーザが選択できる、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。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、Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序を参照してください。

表 2-5 に、ISO パッケージ ファイルを含んでいるファイルおよび各ファイルの目的を示します。

表 2-5　事前展開用 ISO ファイルの内容

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。

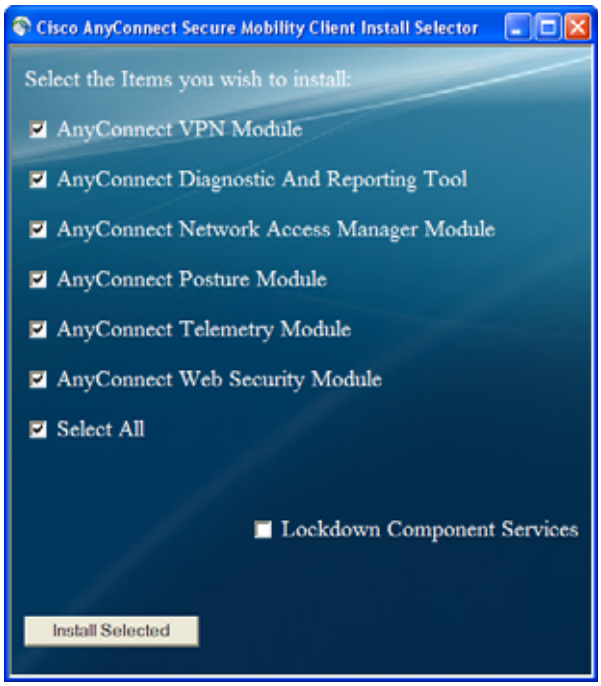
インストール ユーティリティのユーザへの展開

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です。そのままでよい場合、ユーザは [インストール（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。

図 2-18 に、インストール ユーティリティ GUI を示します。

図 2-18　インストール ユーティリティの GUI



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。ユーザは、コンピュータを手動でリブートする必要があります。

Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序

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。さらに、オプション モジュール用のインストーラは、前提条件として、同じバージョンの AnyConnect 3.0 コア クライアントがインストールされていることを必要としています。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。

インストール順序

インストールの順序は重要です。AnyConnect モジュールは次の順番でインストールします。

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。

2. AnyConnect Diagnostic and Reporting Tool（DART）モジュールをインストール。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。
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。
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。

アンインストール順序

アンインストールの順序も重要です。次の順序でモジュールをアンインストールします。

1. テレメトリ モジュールをアンインストールします。
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。
3. AnyConnect コア クライアントをアンインストールします。
4. 最後に 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。

事前展開された AnyConnect モジュールのインストール

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。

（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 [ネットワーク（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

事前展開モジュールは、「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）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。

VPN モジュールとともにオプションの AnyConnect モジュールを事前展開するには、次の手順を実行します。

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」

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は、表 2-5、「事前展開用 ISO ファイルの内容」で確認してください。

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.2-35）で説明されている手順を実行して、「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）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。

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 モジュールのネットワーク アクセス マネージャおよび Web セキュリティは、ユーザ コンピュータ上にスタンドアロン アプリケーションとして展開できます 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***および（または）***AnyConnect Web セキュリティ モジュール*

一方、***Cisco AnyConnect VPN モジュールはオフにするように指示します。***このようにすると、コア クライアントの VPN 機能がディセーブルになり、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。

インストール ユーティリティを展開していない場合は、MSI プロパティ PRE_DEPLOY_DISABLE_VPN=1 を設定するようにソフトウェア管理システム（SMS）を設定することにより、VPN 機能をディセーブルにする必要があります。次に、例を示します。

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx*
```

これを行った場合、MSI では、MSI に埋め込まれた VPNDisable_ServiceProfile.xml ファイルを、VPN 機能のプロファイル用に指定されているディレクトリにコピーします（ファイル パスについては、表 2-15 を参照してください）。

（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。

その後、オプション モジュール用のインストーラを実行できます。このインストーラでは、VPN サービスなしで AnyConnect GUI を使用できます。

ユーザが [Install Selected] ボタンをクリックすると、次の処理が行われます。

ステップ 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。

ステップ 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 3.0 コア インストーラが起動されます。

ステップ 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。

ステップ 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。

ステップ 5　指定に応じて、AnyConnect 3.0 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 サービスなしでイネーブルになります。

（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。

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.2-35）
- 「AnyConnect プロファイルの展開場所」（P.2-42）
- 「スタンドアロン アプリケーションとしてのネットワーク アクセス マネージャまたは Web セキュリティのインストール」（P.2-36）
- 「AnyConnect をプログラムの追加と削除のリストから非表示にする MSI コマンド」（P.2-36）

MSI インストールのコマンドライン呼び出し

表 2-6 に、個々の AnyConnect モジュールをインストールするために使用する、MSI インストールのコマンドライン呼び出しを示します。コマンドによって生成されるログ ファイルも示してあります。

表 2-6　MSI インストールのコマンドライン呼び出しおよび生成されるログ ファイル

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
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

スタンドアロン アプリケーションとしてのネットワーク アクセス マネージャまたは Web セキュリティのインストール

ネットワーク アクセス マネージャまたは Web セキュリティを VPN サービスなしでインストールするには、次のコマンドを実行する必要があります。

```
msiexec /package anyconnect-win-ver-pre-deloy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1
```

コア クライアント用の MSI を実行すると、コア クライアントがインストールまたは更新され、既存のすべてのプロファイルが削除されて、プロファイルの場所に VPNDisable_ServiceProfile.xml がインストールされます。その後、オプション モジュール用のインストーラを実行できます。その後、スタンドアロン コンポーネントでは、VPN サービスなしで AnyConnect GUI を使用できます。

AnyConnect をプログラムの追加と削除のリストから非表示にする MSI コマンド

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。

レガシー クライアントおよびオプション モジュールのアップグレード

前のバージョンをアップグレードする場合、AnyConnect Secure Mobility Client バージョン 3.0 は、以下の処理を行います。

- 前のバージョンの全コア クライアントをアップグレードし、すべての VPN 設定を保持します。
- Cisco SSC 5.x をネットワーク アクセス マネージャ モジュールにアップグレードし、ネットワーク アクセス マネージャで使用するためにすべての SSC 設定を保持し、SSC 5.x を削除します。
- Cisco セキュア デスクトップで使用するホスト スキャン ファイルをアップグレードします。AnyConnect 3.0 クライアントは、セキュア デスクトップと共存できます。
- Cisco IPsec VPN クライアントはアップグレード ***しません***（削除もしません）。ただし、AnyConnect 3.0 クライアントは、コンピュータ上で IPsec VPN クライアントと共存できます。
- ScanSafe Web セキュリティ機能は、アップグレード***せず***、同じコンピュータ上で共存できません。AnyWhere+ をアンインストールする必要があります。

インストーラのカスタマイズとローカライズ

トランスフォームを使用して Windows 用 AnyConnect コア インストーラをカスタマイズでき、コア インストーラの表示するメッセージを、リモート ユーザの優先言語に翻訳できます。AnyConnect のクライアントとインストーラのカスタマイズとローカライズ（翻訳）の詳細については、第 11 章「AnyConnect クライアントとインストーラのカスタマイズとローカライズ」を参照してください。

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。

- 「Linux および MAC OS X 用モジュールの場合の推奨されるインストールまたはアンインストールの順序」（P.2-37）

Linux および MAC OS X 用モジュールの場合の推奨されるインストールまたはアンインストールの順序

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。

ファイルを手動で配布する場合は、次のインストール順序を強くお勧めします。

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。
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。
3. ポスチャ モジュールをインストールします。

AnyConnect モジュールのアンインストール

アンインストールの順序も重要です。次の順序でモジュールをアンインストールします。

1. ポスチャ モジュールをアンインストールします。
2. AnyConnect コア クライアントをアンインストールします。
3. 最後に 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。

Ubuntu 9.x 64 ビットを実行しているコンピュータの場合の AnyConnect 要件

Ubuntu 9.x 64 ビットを実行しているコンピュータ上で Cisco AnyConnect Secure Mobility Client を実行するために、AnyConnect では、以下の要件を必要とします。

- 32 ビット互換ライブラリがコンピュータ上にインストールされている。
- Ubuntu 9.x 32 ビット バージョンの NSS 暗号ライブラリが /usr/local/firefox にインストールされている。
- Firefox 証明書ストアと対話できるようにユーザ ホーム ディレクトリに格納された .mozilla/firefox プロファイル

これらの問題に対処するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、32 ビット互換ライブラリをインストールします。

```
administrator@ubuntu-904-64:/usr/local$ sudo apt-get install ia32-libs lib32nss-mdns
```

ステップ 2　32 ビット版の FireFox を http://www.mozilla.com からダウンロードして、/usr/local/firefox にインストールします。

AnyConnect は、必要な NSS 暗号化ライブラリを先にこのディレクトリで検索します。

ステップ 3　次のコマンドを入力して、ここで示すディレクトリに Firefox インストールを展開します。

```
administrator@ubuntu-904-64:/usr/local$ sudo tar -C /usr/local -xvjf
~/Desktop/firefox-version.tar.bz2
```

ステップ 4　AnyConnect を使用するユーザとしてログインし、少なくとも 1 回、Firefox を実行します。

これによって、AnyConnect が Firefox 証明書ストアと対話するために必要な .mozilla/firefox プロファイルがユーザのホーム ディレクトリに作成されます。

ステップ 5　Standalone モードで AnyConnect をインストールします。

Mac OS X で Java インストーラが失敗した場合の手動インストール オプションの使用

Mac 上で WebLaunch を使用して AnyConnect を起動し、Java インストーラが失敗した場合は、ダイアログボックスに [手動インストール（Manual Install）] リンクが表示されます。この場合、ユーザは、次の手順を実行する必要があります。

ステップ 1　[手動インストール（Manual Install）] をクリックします。ダイアログボックスに、vpnsetup.sh ファイルを保存するオプションが表示されます。

ステップ 2　vpnsetup.sh ファイルを Mac 上に保存します。

ステップ 3　ターミナル ウィンドウを開き、CD コマンドを使用して、保存したファイルがあるディレクトリに移動します。

ステップ 4　次のコマンドを入力します。

```
sudo /bin/sh vpnsetup.sh
```

vpnsetup スクリプトによって AnyConnect インストールが開始されます。

ステップ 5　インストール後、[アプリケーション（Applications）] > [Cisco] > [Cisco AnyConnect Secure Mobility Client] の順に選択して、AnyConnect セッションを開始します。

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
- あらゆる場所

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 は、署名付きのアプリケーションで、この設定または **Anywhere** 設定で通常実行されます。**Mac App Store** 設定を選択した場合、AnyConnect をインストールおよび実行するには、Ctrl キーを押しながらクリックする必要があります。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。

（注）　これは新しいスタンドアロンのインストールにのみ適用され、Web の起動または OS のアップグレード（たとえば、10.7 から 10.8）には適用されません。

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.2-39）
- 「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.2-43）
- 「AnyConnect プロファイルの展開場所」（P.2-42）

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 2-7 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 2-7　ASA 展開または事前展開用の AnyConnect コア ファイル名

AnyConnect 3.0 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 2-8 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 2-8　ASA 展開または事前展開用の DART パッケージ ファイル名

DART	Web-Deploy ファイル名およびパッケージ（ダウンロード）	Pre-Deploy 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 2-9 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 2-9　ASA 展開または事前展開用の 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）	Pre-Deploy インストーラ
Windows	anyconnect-gina-win-(ver)-web-deploy-k9.exe	anyconnect-gina-win-(ver)-pre-deploy-k9.msi

表 2-10 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 2-10　ASA 展開または事前展開用のネットワーク アクセス マネージャ ファイル名

Network Access Manager	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-nam-win-(ver)-k9.msi	anyconnect-nam-win-(ver)-k9.msi

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 2-11　ASA 展開または事前展開用のポスチャ モジュール ファイル名

Posture	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy 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

表 2-12 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 2-12　ASA 展開または事前展開用のテレメトリ ファイル名

Telemetry	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-telemetry-win-(ver)-web-deploy-k9.exe. Dependent upon installation of anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-telemetry-win-(ver)-pre-deploy-k9.msi. Dependent upon installation of anyconnect-posture-win-(ver)-pre-deploy-k9.msi.

表 2-13 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 2-13　ASA 展開または事前展開用の Web セキュリティ ファイル名

Web Security	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 2-14 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 2-14　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 2-15 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 2-15　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	ロケーション
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
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

表 2-15　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	ロケーション
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
Mac OS X	すべてのモジュール	/opt/cisco/anyconnect/profile
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 [プリファレンス（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 2-16 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 2-16　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 Secure Mobility Client\preferences.xml
	グローバル	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ preferences_global.xml
Windows XP	ユーザ	C:\Documents and Settings**username**\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
	グローバル	C:\Documents and Settings\AllUsers\Application Data\Cisco\ Cisco AnyConnect Secure Mobility 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、VPN 用、ネットワーク アクセス マネージャ用、AnyConnect Secure Mobility Client のための Web セキュリティ モジュール用のクライアント 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 用、ネットワーク アクセス マネージャ用、Web セキュリティ モジュール用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

このアプリケーションは、Windows XP 上と Windows 7 上でテストされています。MSI は、Windows 上だけで実行されます。

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。

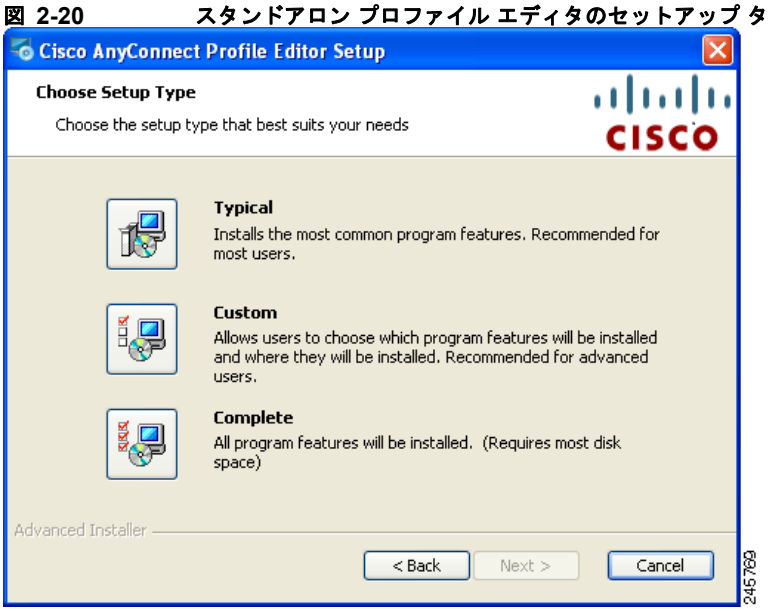
ステップ 3　[ようこそ（Welcome）] 画面で、[次へ（Next）] をクリックします。

図 2-19　スタンドアロン プロファイル エディタの [ようこそ（Welcome）] 画面

ステップ 4　[セットアップ タイプの選択（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、[次へ（Next）] をクリックします。

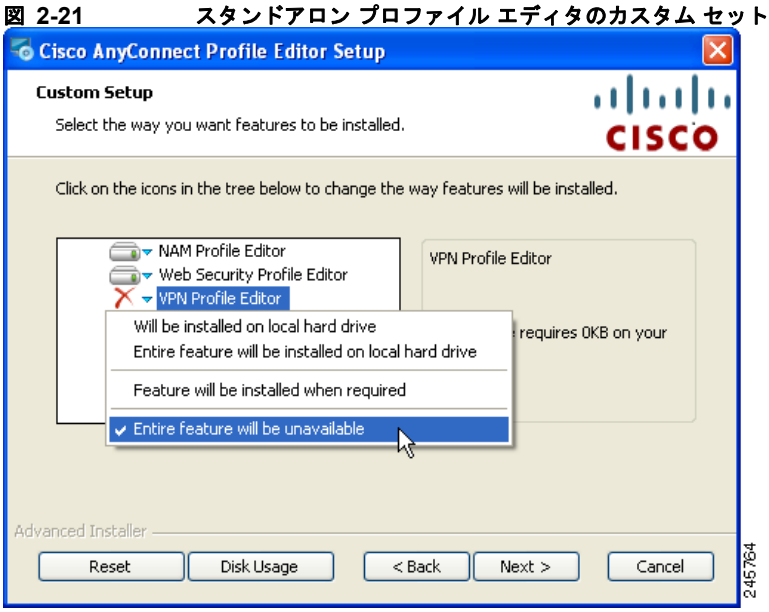
- [標準（Typical）]：ネットワーク アクセス マネージャ プロファイル エディタのみが自動的にインストールされます。
- [カスタム（Custom）]：ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、VPN プロファイル エディタから任意のプロファイル エディタを選択してインストールできます。
- [フル（Complete）]：ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、VPN プロファイル エディタが自動的にインストールされます。

図 2-20　スタンドアロン プロファイル エディタのセットアップ タイプの選択



ステップ 5　前のステップで [標準（Typical）] または [フル（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 [カスタム（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、[ローカルのハード ドライブにインストールする（Will be installed on local hard drive）] を選択するか、[すべての機能を利用しない（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。[次へ（Next）] をクリックします。

図 2-21　スタンドアロン プロファイル エディタのカスタム セットアップ



ステップ 6　[インストール準備完了（Ready to Install）] 画面で [インストール（Install）] をクリックします。[Cisco AnyConnect プロファイル エディタのインストール（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。

図 2-22　スタンドアロン プロファイル エディタのインストール準備完了

ステップ 7　[Cisco AnyConnect プロファイル エディタ セットアップ ウィザードの完了（Completing the Cisco AnyConnect Profile Editor Setup Wizard）] で [完了（Finish）] をクリックします。

図 2-23　スタンドアロン プロファイル エディタのインストールが完了

- 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。
- [スタート（Start）] > [すべてのプログラム（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、または Web セキュリティのプロファイル 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 インストールを修正できます。

ステップ 1　Windows のコントロール パネルを開いて [プログラムの追加または削除（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、[変更（Change）] をクリックします。

ステップ 3　[次へ（Next）] をクリックします。

ステップ 4　[変更（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、[次へ（Next）] をクリックします。

ステップ 6　[インストール（Install）] をクリックします。

ステップ 7　[完了（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 [プログラムの追加または削除（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、[削除（Remove）] をクリックします。

ステップ 3　[はい（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、または Web セキュリティのプロファイル エディタを起動します。これには、デスクトップ上のアイコンをダブルクリックするか、[スタート（Start）] > [すべてのプログラム（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、または Web セキュリティのプロファイル 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」

ステップ 3　[ファイル（File）] > [保存（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　VPN、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、デスクトップ上のアイコンをダブルクリックするか、[スタート（Start）] > [すべてのプログラム（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、または Web セキュリティのプロファイル エディタを選択します。

ステップ 2　[ファイル（File）] > [オープン（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、[ファイル（File）] > [保存（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。

AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定

現在、ユーザとその所有デバイスは、オフィス、自宅、空港、カフェといったさまざまな場所からインターネットに接続するなど、さらにモバイル化が進んでいます。従来、ネットワーク内のユーザはセキュリティの脅威から保護されていましたが、従来のネットワーク外のユーザはアクセプタブル ユース ポリシーが適用されずにマルウェアから最小限しか保護されないため、現在よりもデータ損失のリスクが高まっています。

雇用主は、従業員やパートナーが場所やデバイスを問わずに作業できるフレキシブルな作業環境の創出を望んでいますが、同時に、企業の利益と資産をインターネット ベースの脅威から常時保護したいと考えています。

従来のネットワーク セキュリティ ソリューションやコンテンツ セキュリティ ソリューションは、ユーザと資産をネットワーク ファイアウォールで保護する点では理想的でしたが、ユーザまたはデバイスがネットワークに接続していない場合や、セキュリティ ソリューションを介してデータがルーティングされない場合には効果がありません。

シスコは AnyConnect Secure Mobility を提供してリモート エンドポイントへのネットワーク境界を拡張し、Web セキュリティ アプライアンスで提供される Web フィルタリング サービスをシームレスに統合できます。Cisco AnyConnect Secure Mobility は、コンピュータ対応プラットフォームやスマートフォン対応プラットフォーム上のモバイル ユーザを保護する革新的な新しい方法を実現し、エンドユーザには、よりシームレスな常時保護されたエクスペリエンスが提供され、IT 管理者は包括的にポリシーを適用できるようになります。

AnyConnect Secure Mobility は、次のシスコ製品全体の機能のコレクションです。

- Cisco IronPort Web セキュリティ アプライアンス（WSA）
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- Cisco AnyConnect クライアント

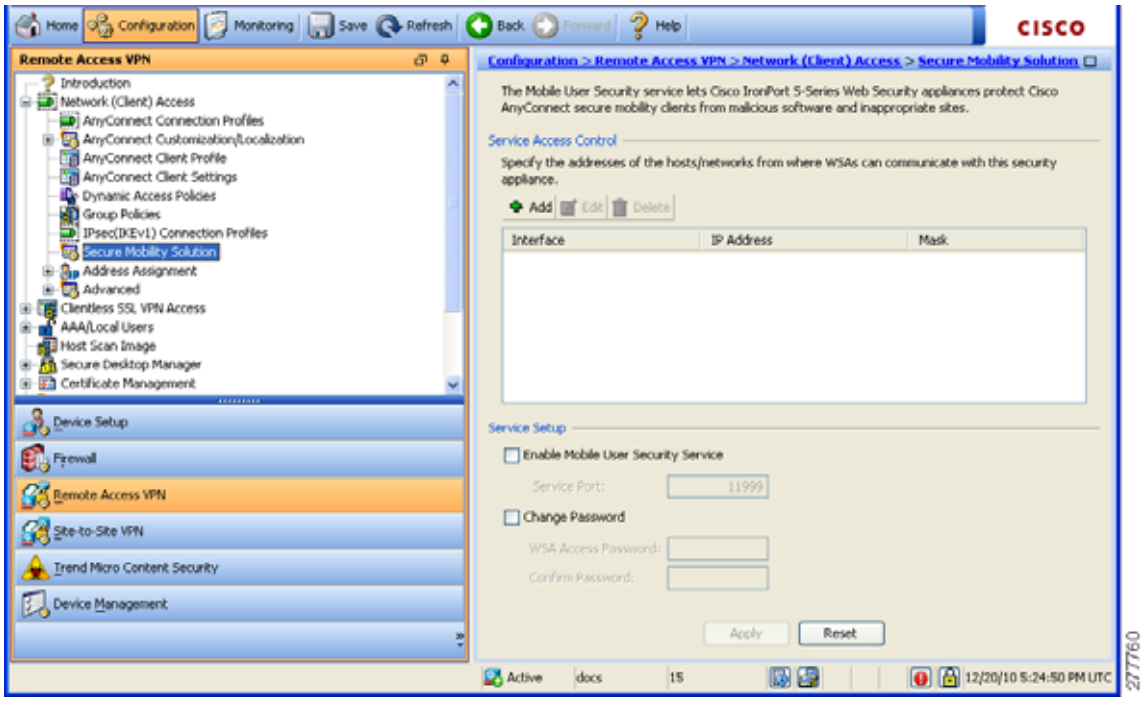
Cisco AnyConnect Secure Mobility は、次の機能を提供してモバイル ワークフォースの課題に対処します。

- **セキュアかつ持続的な接続**：（適応型セキュリティ アプライアンスをヘッドエンドに使用する）Cisco AnyConnect は、AnyConnect Secure Mobility のリモート アクセス接続機能部分を提供します。ネットワークへのアクセスを許可する前に、ユーザとデバイスの両方を認証して検証する必要があるため、セキュアな接続が得られます。通常、Cisco AnyConnect はネットワーク間のローミング時も常時接続に設定されるため、接続は固定されます。Cisco AnyConnect は常時接続でありながら、十分な柔軟性も備えているため、ロケーションに応じてさまざまなポリシーを適用できます。また、インターネットにアクセスする前に契約条項に同意する必要がある「キャプティブ ポータル」で、ユーザのインターネット アクセスを許可します。
- **持続的なセキュリティとポリシーの適用**：Web セキュリティ アプライアンスは、アクセプタブル ユース ポリシーやマルウェアからの保護などのコンテキストに対応したポリシーを、モバイル（リモート）ユーザも含めたあらゆるユーザに適用します。また Web セキュリティ アプライアンスは、AnyConnect クライアントからユーザ認証情報を受け入れ、ユーザが Web コンテンツにアクセスできるよう自動認証手順を提供します。

[セキュア モビリティ ソリューション（Secure Mobility Solution）] ダイアログ ボックスを使用して、この機能の ASA 部分を設定します。AnyConnect Secure Mobility により Cisco IronPort S シリーズ Web セキュリティ アプライアンスは Cisco AnyConnect セキュア モビリティ クライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティ アプライアンス保護がイネーブルになっているか定期的に確認します。

WSA サポートのために ASA を設定するには、ASDM を起動し、[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）] > [セキュア モビリティ ソリューション（Secure Mobility Solution）] パネルを選択します（図 2-24 を参照）。詳細については [ヘルプ（Help）] をクリックします。

図 2-24　AnyConnect Secure Mobility ウィンドウ



（注）

- この機能では、Cisco AnyConnect セキュア モビリティ クライアントの AnyConnect Secure Mobility ライセンスをサポートする Cisco IronPort Web セキュリティ アプライアンスのリリースが必要です。また、AnyConnect Secure Mobility 機能をサポートする AnyConnect リリースが必要です。
- この機能は、SSL プロトコルまたは IPsec IKEv2 プロトコルを使用した AnyConnect 接続で使用可能です。

ステップ 1　次のいずれかの方法を使用して、どのホストまたはネットワーク アドレスから WSA が通信し、リモート ユーザを識別できるかを指定します。

- **IP アドレスによる関連付け**：Web セキュリティ アプライアンス管理者は、リモート デバイスに割り当てられていると見なす IP アドレスの範囲を指定します。通常、適応型セキュリティ アプライアンスは、VPN 機能を使用して接続しているデバイスに、これらの IP アドレスを割り当てます。Web セキュリティ アプライアンスは、設定されているいずれかの IP アドレスからトランザクションを受信すると、そのユーザをリモート ユーザと見なします。この設定では、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと通信しません。
- **Cisco ASA との統合**：Web セキュリティ アプライアンス管理者は、1 つ以上の適応型セキュリティ アプライアンスと通信するよう Web セキュリティ アプリケーションを設定します。適応型セキュリティ アプライアンスは、IP アドレスとユーザのマッピングを保持し、その情報を Web セキュリティ アプライアンスに伝達します。Web プロキシはトランザクションを受信すると、IP アドレスを取得して IP アドレスとユーザのマッピングをチェックし、ユーザ名を特定します。適応型セキュリティ アプライアンスと統合すると、リモート ユーザのシングル サインオンを有効にできます。この設定により、Web セキュリティ アプライアンスは適応型セキュリティ アプライアンスと通信します。

- [追加（Add）]：適応型セキュリティ アプライアンスが通信できる Web セキュリティ アプライアンスを 1 つ以上追加できる [アクセス コントロール設定の追加（Add Access Control Configuration）] ダイアログボックスを開きます。
- [編集（Edit）]：選択した接続の [アクセス コントロール設定の編集（Edit Access Control Configuration）] ダイアログボックスが開きます。
- [削除（Delete）]：選択した接続をテーブルから削除します。確認されず、やり直しもできません。

ステップ 2　モバイル ユーザ セキュリティ サービスをイネーブルにする場合、VPN を介してクライアントと接続を開始します。Web セキュリティ アプライアンスは、適応型セキュリティ アプライアンスと統合するように設定されると、初回起動時に、設定されているすべての適応型セキュリティ アプライアンスと HTTPS 接続を確立しようとします。接続が確立されると Web セキュリティ アプライアンスは、設定されている ASA アクセス パスワードを使用して適応型セキュリティ アプライアンスを認証します。認証が正常に行われると、適応型セキュリティ アプライアンスは Web セキュリティ アプライアンスに IP アドレスとユーザのマッピングを送信します。WSA が存在しない場合、ステータスは disabled になります。

ステップ 3　サービスをイネーブルにする場合、サービスのどのポート番号を使用するかを指定します。ポートの範囲は 1 ～ 65535 で、管理システムにより WSA にプロビジョニングされた対応する値と一致させる必要があります。デフォルトは 11999 です。

ステップ 4　必要な場合、WSA アクセス パスワードを変更します。適応型セキュリティ アプライアンスと Web セキュリティ アプライアンス間の認証に必要な Web セキュリティ アプライアンス アクセス パスワードを変更できます。このパスワードは、Web セキュリティ アプライアンスに設定されている当該パスワードと一致する必要があります。

ステップ 5　[WSA アクセス パスワード（WSA Access Password）] フィールドで、ASA と WSA 間の認証に必要な共有秘密パスワードを指定します。

ステップ 6　指定されたパスワードを再入力します。

ステップ 7　[WSA セッションの表示（Show WSA Sessions）] により ASA に接続された WSA のセッション情報を表示できます。接続されている（または接続された）WSA のホスト IP アドレスおよび接続時間がダイアログボックスに返されます。

エンドポイントから WSA にトラフィックをリダイレクトするプロキシ サーバの設定

エンドポイントからの Web トラフィックを WSA にリダイレクトするように、Web プロキシを設定する必要があります。これを行うには、WCCP ルータを使用してトランスペアレント プロキシを設定するか、次の手順を実行して明示的なプロキシを設定します。

ステップ 1　ASA 上で ASDM を起動し、[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）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　Web vpn 用に設定されているグループ ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3　[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウの左ペインで、[詳細（Advanced）] ノードを展開し、[ブラウザ プロキシ（Browser Proxy）] を選択します。

ステップ 4　[プロキシ サーバ ポリシー（Proxy Server Policy）] エリアの [継承（Inherit）] をオフにします。

ステップ 5　[以下からプロキシ サーバの設定を選択する（Select proxy server settings from the following）] を選択し、[下記のプロキシ サーバの設定を使用する（Use proxy server settings given below）] をオンにします。

ステップ 6　[プロキシ サーバの設定（Proxy Server Settings）] エリアを展開し、[サーバ アドレスおよびポート（Server Address and Port）] の [継承（Inherit）] チェックボックスをオンにします。WSA の IP アドレスおよびポート番号を指定します。

ステップ 7　[ローカル アドレスに対してサーバをバイパスする（Bypass server for local addresses）] の [継承（Inherit）] チェックボックスをオフにし、[はい（Yes）] を選択します。

ステップ 8　プロキシ サーバ経由でアクセスしないアドレスのリストを入力する場合は、[除外リスト（Exception list）] の [継承（Inherit）] チェックボックスをオフにし、IP アドレスを入力します。[除外リスト（Exception list）] エリアで、これらの IP アドレスを例外に指定できます。

ステップ 9　[OK] をクリックします。

ステップ 10　[適用（Apply）] をクリックします。

CHAPTER 3

VPN アクセスの設定

ここでは、Cisco AnyConnect Secure Mobility Client の VPN プロファイルと機能、およびそれらの設定方法について説明します。

AnyConnect プロファイルの設定と編集

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージ バージョン 2.5 以降（すべてのオペレーティング システム用）にはプロファイル エディタが含まれています。プロファイル エディタは、ASA 上で AnyConnect ソフトウェア パッケージを SSL VPN クライアント イメージとしてロードした時点で ASDM によりアクティブ化されます。

複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからプロファイル エディタがロードされます。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。

（注） 手動で VPN プロファイルを配置している場合、ASA にプロファイルをアップロードする必要があります。クライアント システムが接続する場合、クライアントのプロファイルが ASA のプロファイルに一致することを AnyConnect が確認します。

無効化されたプロファイルのアップデートがあり、ASA プロファイルがクライアントと異なる場合、手動で展開したプロファイルは動作しません。

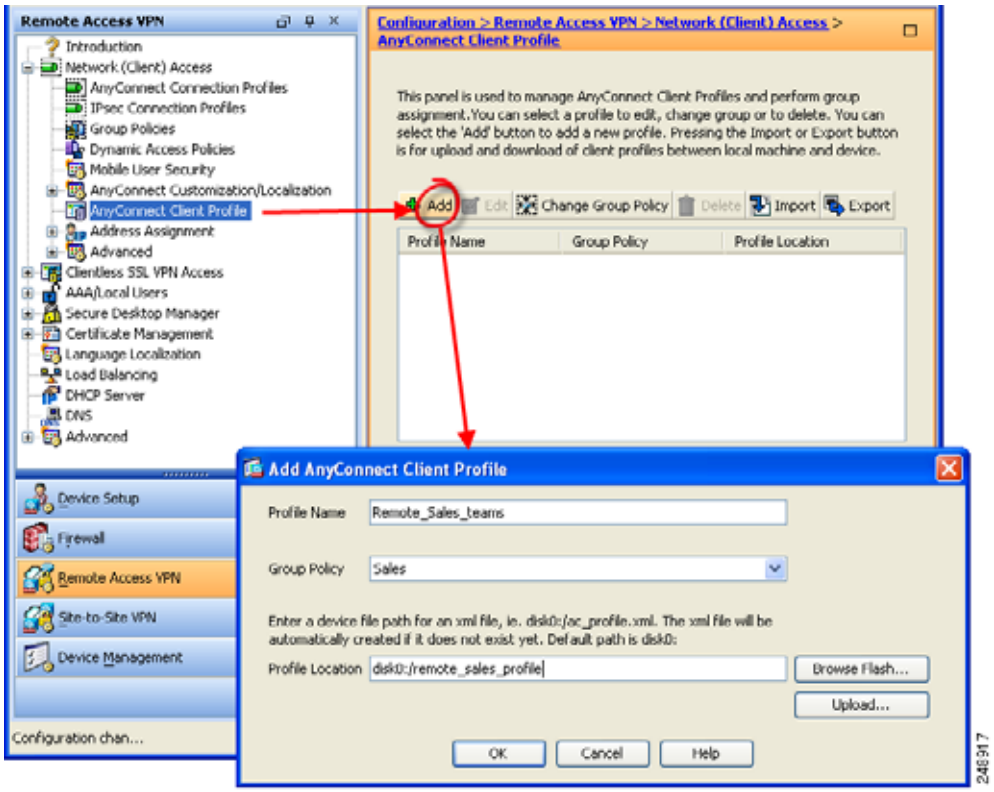
プロファイル エディタをアクティブ化し、ASDM でプロファイルを作成および編集するには、次の手順に従います。

ステップ 1　まだ実行していない場合は、AnyConnect クライアント イメージとして AnyConnect ソフトウェアパッケージをロードします。

ステップ 2　[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。[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ペインが開きます。

ステップ 3　[追加（Add）] をクリックします。

図 3-1　AnyConnect プロファイルの追加



ステップ 4　プロファイル名を指定します [プロファイル ロケーション（Profile Location）] で別の値を指定しない限り、ASDM では XML ファイルが ASA のフラッシュ メモリ上に同じ名前で作成されます。

（注）　名前を指定するときに、.xml 拡張子は含めないでください。プロファイルに example.xml という名前を付けた場合、ASDM により自動的に .xml 拡張子が追加されて、名前が example.xml.xml に変更されます。この場合、ASA の [プロファイル ロケーション（Profile Location）] フィールドで名前を example.xml に変更しても、リモート アクセスで AnyConnect に接続したときに、名前は example.xml.xml に戻ってしまいます。（.xml 拡張子の重複により）AnyConnect がプロファイル名を認識できない場合、IKEv2 接続は失敗する場合があります。

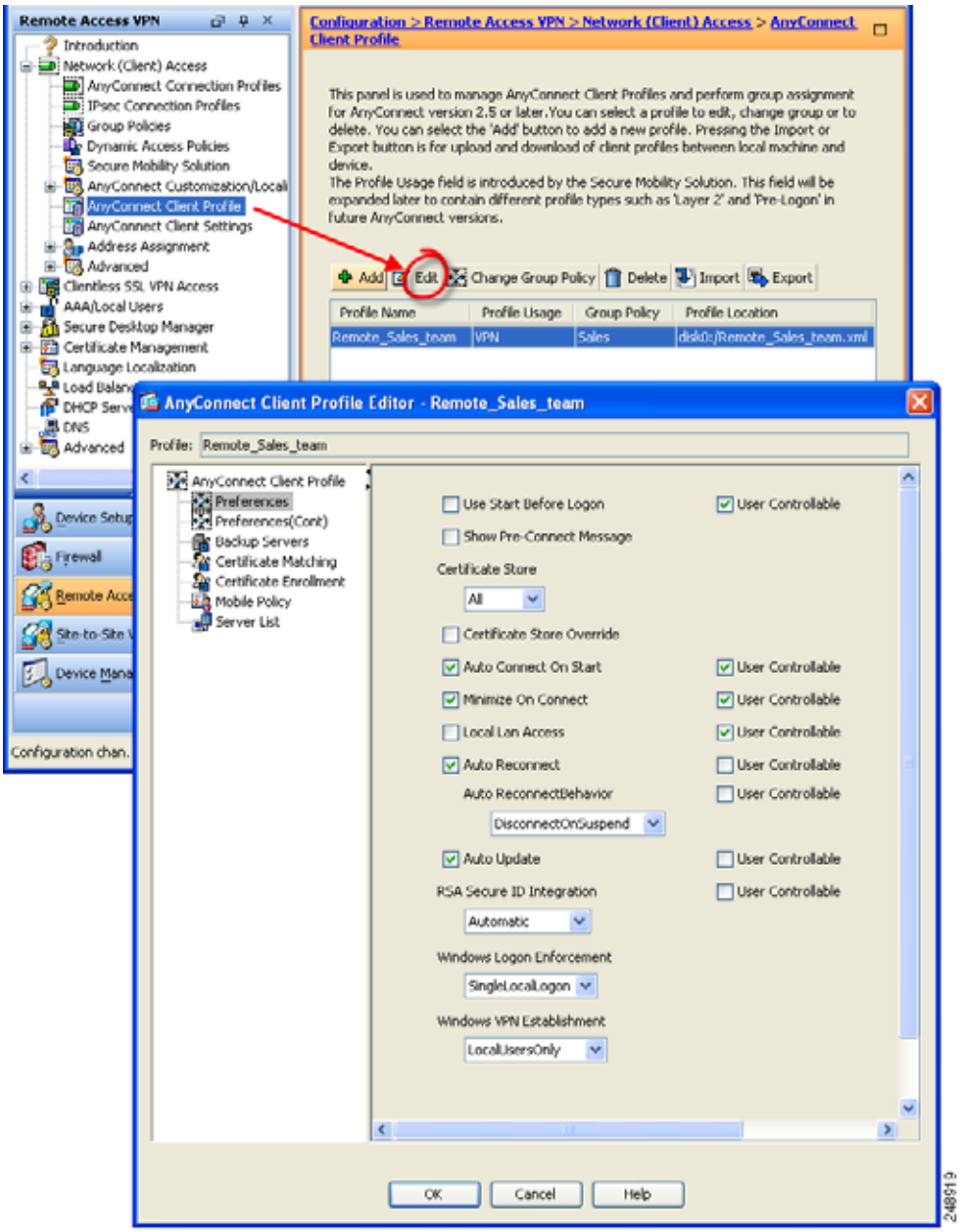
ステップ 5　グループ ポリシーを選択します（任意）。ASA は、このプロファイルをグループ ポリシー内の全 AnyConnect ユーザに適用します。

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。[編集（Edit）] をクリックします。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。

ステップ 8　終了したら、[OK] をクリックします。

図 3-2　プロファイルの編集



AnyConnect プロファイルの展開

プロファイルは、ASDM または ASA コマンドライン インターフェイスでインポートできます。

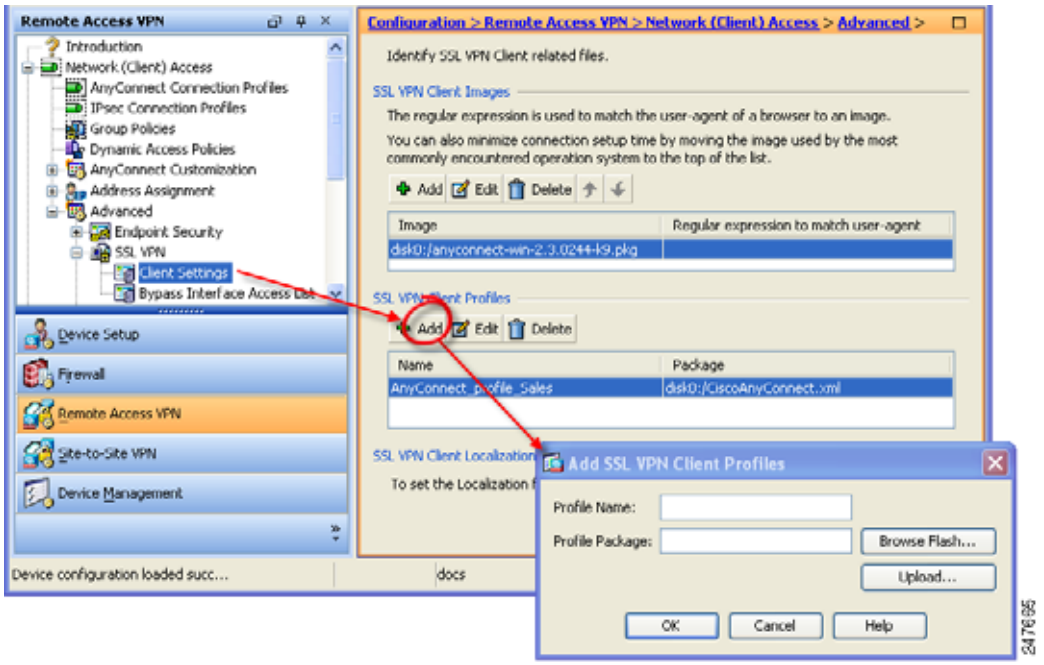
（注）　クライアント GUI に、最初の VPN 接続でユーザが制御可能な設定がすべて表示されるように、プロファイルのホスト リストには ASA を含める必要があります。ASA のアドレスまたは FQDN をホスト エントリとしてプロファイルに追加していない場合、フィルタがセッションに適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルに ASA をホスト エントリとして追加しなかった場合、この証明書照合は無視されます。プロファイルへのホスト エントリの追加に関する詳細については、「サーバ リストの設定」（P.3-54）を参照してください。

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　キャッシュ メモリにロードする AnyConnect プロファイル ファイルを特定します。[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）] > [詳細（Advanced）] > [クライアント設定（Client Settings）] を選択します。

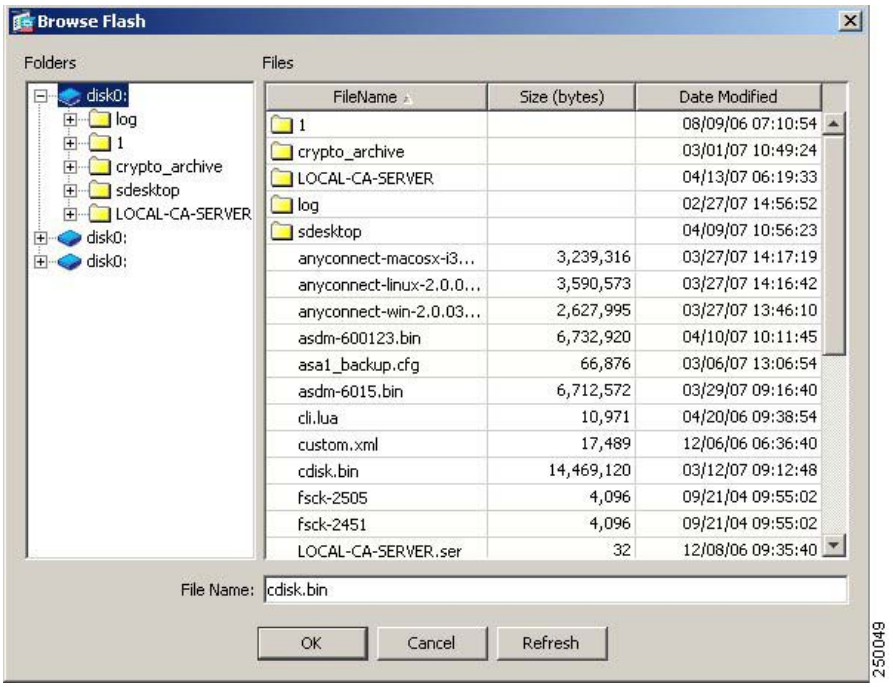
ステップ 2　[SSL VPN クライアント プロファイル（SSL VPN Client Profiles）] エリアで [追加（Add）] をクリックします。

図 3-3　AnyConnect プロファイルの追加



ステップ 3　プロファイル名およびプロファイル パッケージ名を対応するフィールドに入力します。プロファイル パッケージ名を参照するには、[フラッシュの参照（Browse Flash）] をクリックします。

図 3-4　[フラッシュの参照（Browse Flash）] ダイアログボックス



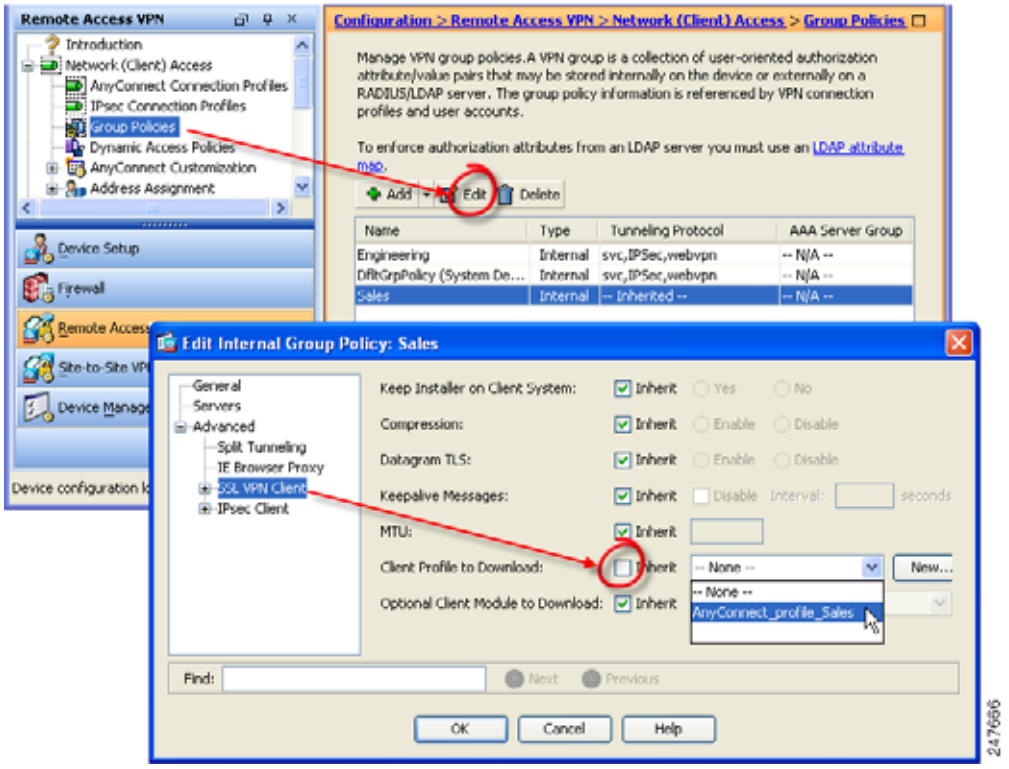
ステップ 4　テーブルからファイルを選択します。ファイル名が、テーブルの下の [ファイル名（File Name）] フィールドに表示されます。

ステップ 5　[OK] をクリックします。選択したファイル名が、[SSL VPN クライアント プロファイルの追加（Add SSL VPN Client Profiles）] ダイアログボックスまたは [SSL VPN クライアント プロファイルの編集（Edit SSL VPN Client Profiles）] ダイアログボックスの [プロファイル パッケージ（Profile Package）] フィールドに表示されます。

ステップ 6　[SSL VPN クライアント プロファイルの追加（Add SSL VPN Client Profiles）] または [SSL VPN クライアント プロファイルの編集（Edit SSL VPN Client Profiles）] ダイアログボックスで、[OK] をクリックします。これによって、AnyConnect ユーザのグループ ポリシーおよびユーザ名の属性にプロファイルを使用できるようになります。

ステップ 7　グループ ポリシーのプロファイルを指定するには、[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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [SSL VPN クライアント（SSL VPN Client）] の順に選択します。

図 3-5　グループ ポリシーに使用するプロファイルの指定



ステップ 8　[継承（Inherit）] をオフにして、ダウンロードする AnyConnect プロファイルをドロップダウン リストから選択します。

ステップ 9　設定が終了したら、[OK] をクリックします。

Start Before Logon の設定

Start Before Logon（SBL）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 VPN 接続を介して企業インフラへ強制的に接続させます。ASA で認証が行われると、Windows ログイン ダイアログが表示され、ユーザは通常どおりにログインします。SBL は Windows でのみ使用可能で、ログイン スクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。

（注）　AnyConnect は、Windows XP x64（64 ビット）Edition 用の SBL をサポートしていません。

SBL をイネーブルにする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループ ポリシーでキャッシュのクレデンシャル使用が許可されない場合）。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- インフラストラクチャとの接続を必要とする場合があるネットワーキング コンポーネント（MS NAP/CS NAC など）が存在する。

SBL 機能をイネーブルにするには、AnyConnect プロファイルを変更して、ASA が SBL 用の AnyConnect モジュールをダウンロードできるようにする必要があります。

SBL に必要な設定は、この機能をイネーブルにすることだけです。ログイン前に実施されるこのプロセスは、ネットワーク管理者がそれぞれの状況の要件に基づいて処理します。ログイン スクリプトは、ドメインまたは個々のユーザに割り当てることができます。通常ドメインの管理者は、バッチ ファイルまたはそれに類するものを Microsoft Active Directory のユーザまたはグループに定義しています。ユーザがログインするとすぐに、ログイン スクリプトが実行されます。

SBL を使用すると、ローカルの社内 LAN 上にあるものと同等のネットワークを構成できます。たとえば、SBL を有効にすると、ユーザはローカルのインフラストラクチャにアクセスできるため、通常はオフィス内のユーザが実行するログイン スクリプトをリモート ユーザからも使用できるようになります。これには、ドメイン ログイン スクリプト、グループ ポリシー オブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。

これ以外の例として、コンピュータへのログインに使用するキャッシュ クレデンシャルを許可しないようにシステムを設定する場合があります。このシナリオでは、コンピュータへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。

SBL は、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、またはその他のワイヤレス認証を設定する必要があります。ネットワーク アクセス マネージャがインストールされている場合、マシン接続を展開して、適切な接続を確実に使用できるようにする必要があります。詳細については、第 4 章「ネットワーク アクセス マネージャの設定」を参照してください。

AnyConnect は、高速ユーザ切り替えと互換性がありません。

ここでは、次の内容について説明します。

- 「Start Before Logon コンポーネントのインストール（Windows のみ）」（P.3-8）
- 「Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定」（P.3-12）

Start Before Logon コンポーネントのインストール（Windows のみ）

Start Before Logon コンポーネントは、コア クライアントのインストール*後*にインストールする必要があります。さらに、2.5 の Start Before Logon コンポーネントの場合は、バージョン 2.5 以降のコア クライアント ソフトウェアのインストールが必要です。MSI ファイルを使用して AnyConnect および Start Before Logon コンポーネントを事前に展開する場合（Altiris、Active Directory、SMS など独自

のソフトウェア展開手段を持つ大企業の場合など）は、正しい順序でインストールする必要があります。インストールの順序は、Web 展開または Web 更新されている AnyConnect を管理者がロードした時点で自動的に処理されます。

（注）　AnyConnect は、サードパーティの Start Before Logon アプリケーションでは起動できません。

Windows のバージョン違いによる Start Before Logon の差異

Windows 7 および Vista システムでは、SBL のイネーブル化の手順が一部異なります。Vista よりも前のシステムでは、VPNGINA（virtual private network graphical identification and authentication の略称）というコンポーネントにより SBL が実装されていました。Windows 7 および Vista システムでは、SBL の実装に PLAP という名前のコンポーネントが使用されます。

AnyConnect では、Windows 7 または Vista の SBL 機能は Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、ネットワーク管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログイン前に実行することができます。Windows 7 および Windows Vista の SBL 機能は、PLAP により実現されます。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、Windows 7 および Vista の x86 バージョンおよび x64 バージョンをサポートします。

（注）　この項で説明する VPNGINA とは Vista 以前のプラットフォームの Start Before Logon 機能を指し、PLAP は Windows 7 および Vista システムの Start Before Logon 機能を指します。

GINA は、ユーザが Ctrl キー、Alt キー、および Del キーを同時に押すと起動します。PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [ネットワーク接続（Network Connect）] ボタンで任意のネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

以下の項では、VPNGINA と PLAP SBL の設定および手順について説明します。Windows 7 プラットフォームまたは Windows Vista プラットフォームにおける SBL 機能（PLAP）の有効化および使用に関する詳細については、「Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定」（P.12）を参照してください。

AnyConnect プロファイルでの SBL のイネーブル化

AnyConnect プロファイルで SBL をイネーブルにする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Preferences）] ペインに移動し、[ログイン前の起動の使用（Use Start Before Logon）] をオンにします。

ステップ 3　（任意）リモート ユーザが SBL の使用を制御できるようにする場合は、[ユーザ制御可（User Controllable）] をオンにします。

（注）　SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

セキュリティ アプライアンスでの SBL の有効化

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コア 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。SBL を有効にするには、ASA のグループ ポリシーで、SBL モジュール名を指定する必要があります。手順は次のとおりです。

ステップ 1　[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）] > [グループ ポリシー（Group Policies）] を選択します。

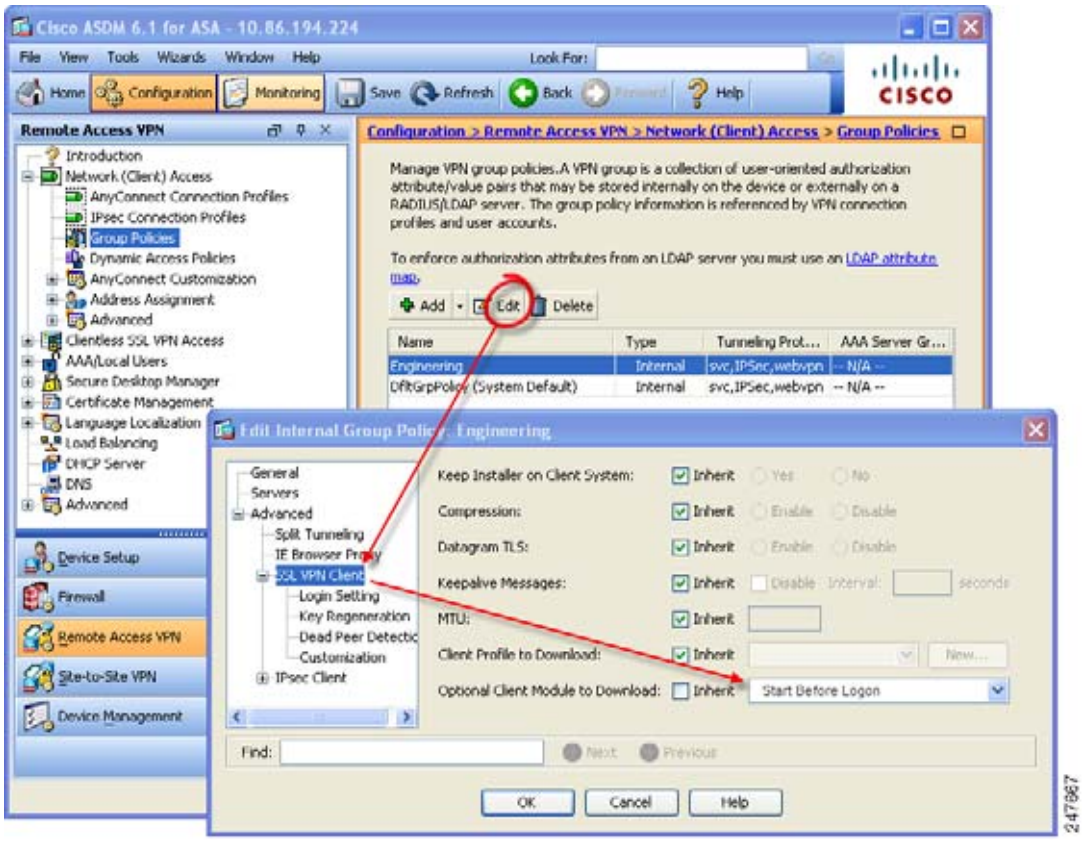
ステップ 2　グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます。

ステップ 3　左側のナビゲーション ペインで [詳細（Advanced）] > [SSL VPN クライアント（SSL VPN Client）] の順に選択します。SSL VPN 設定が表示されます。

ステップ 4　[ダウンロードするオプションのクライアント モジュール（Optional Client Module for Download）] 設定の [継承（Inherit）] をオフにします。

ステップ 5　ドロップダウン リストで、[ログイン前の起動（Start Before Logon）] モジュールを選択します。

図 3-6　ダウンロードする SBL モジュールの指定



SBL に関するトラブルシューティング

SBL で問題が発生した場合は、次の手順に従ってください。

ステップ 1　AnyConnect プロファイルが ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2　以前のプロファイルを削除します（*.xml と指定してハード ドライブ上の格納場所を検索します）。

ステップ 3　Windows の [プログラムの追加/削除（Add/Remove Programs）] を使用して SBL コンポーネントをアンインストールします。コンピュータをリブートして、再テストします。

ステップ 4　イベント ビューアでユーザの AnyConnect ログをクリアし、再テストします。

ステップ 5　Web をブラウズしてセキュリティ アプライアンスに戻り、AnyConnect を再インストールします。

ステップ 6　いったんリブートします。次回リブート時には、[ログイン前の起動（Start Before Logon）] プロンプトが表示されます。

ステップ 7　イベント ログを .evt フォーマットでシスコに送信します

ステップ 8　次のエラーが表示された場合は、ユーザの AnyConnect プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All
Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility
Client\Profile\VABaseProfile.xml. Host data not available.
```

ステップ 9　.tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定

その他の Windows プラットフォームと同じように、Start Before Logon（SBL）機能によって、ユーザが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。Microsoft の Windows 7 および Windows Vista には Windows XP とは異なるメカニズムが使用されているため、Windows 7 および Windows Vista の SBL 機能に使用されているメカニズムも異なります。

SBL AnyConnect 機能は、Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、プログラマチック ネットワーク管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログイン前に実行することができます。Windows 7 および Windows Vista の SBL 機能は、PLAP により実現されます。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

（注）　この項では、VPNGINA は Windows XP の Start Before Logon 機能を指し、PLAP は Windows 7 および Windows Vista の Start Before Logon 機能を指します。

PLAP のインストール

vpnplap.dll および vpnplap64.dll の両コンポーネントは、既存の GINA インストール パッケージの一部になっているため、単一のアドオン SBL パッケージをセキュリティ アプライアンスにロードできます。ロードされると、該当するコンポーネントがターゲット プラットフォームにインストールされます。PLAP はオプションの機能です。インストーラ ソフトウェアは、基盤のオペレーティング システムを検出して該当する DLL をシステム ディレクトリに配置します。Windows 7 および Windows Vista よりも前のシステムでは、インストーラにより 32 ビット版のオペレーティング システムに vpngina.dll コンポーネントがインストールされます。Windows 7 または Vista、または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネントをインストールします。

（注）　VPNGINA または PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、VPNGINA または PLAP のコンポーネントはディセーブルとなり、リモート ユーザの画面に表示されなくなります。

PLAP は、インストールされた後でも、SBL がアクティブ化されるようにユーザ プロファイル <profile.xml> ファイルが変更されるまでアクティブ化されません。「Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定」（P.3-12）を参照してください。ア

クティブ化後に、ユーザは [ユーザのスイッチ（Switch User）] をクリックし、さらに画面下右側の [ネットワーク接続（Network Connect）] アイコンをクリックして Network Connect コンポーネントを呼び出します。

（注）　誤ってユーザ インターフェイスの画面表示を最小化した場合は、**Alt+Tab** キーの組み合わせで元に戻ります。

PLAP を使用した Windows 7 または Windows Vista PC へのログイン

ユーザは、次の手順に従って PLAP をイネーブルにした状態で、Windows 7 または Windows Vista にログインできます。この手順は、Microsoft の要件です。画面の例は、Windows Vista のものです

ステップ 1　Windows のスタート画面で、**Ctrl+Alt+Delete** キーの組み合わせを押します。

図 3-7　[ネットワーク接続（Network Connect）] ボタンが表示されたログイン ウィンドウの例

[ユーザのスイッチ（Switch User）] ボタンが表示された Vista のログイン ウィンドウが表示されます。

図 3-8　[ユーザのスイッチ（Switch User）] ボタンが表示されたログイン ウィンドウの例

ステップ 2　[ユーザのスイッチ（Switch User）]（図内の赤丸で囲まれているボタン）をクリックします。Vista のネットワーク接続ウィンドウが表示されます。図 3-8 の中で赤丸で囲まれているのは [ネットワーク ログイン（Network Login）] アイコンです。

（注）　AnyConnect 接続によってすでに接続済みのユーザが [ユーザのスイッチ（Switch User）] をクリックしても、VPN 接続は解除されません。[ネットワーク接続（Network Connect）] をクリックすると、元の VPN 接続が終了します。[キャンセル（Cancel）] をクリックすると、VPN 接続が終了します。

図 3-9　ネットワーク接続ウィンドウの例

ステップ 3　ウィンドウの右下にある [ネットワーク接続（Network Connect）] ボタンをクリックして、AnyConnect を起動します。AnyConnect のログイン ウィンドウが表示されます。

ステップ 4　この GUI を使用して通常どおりログインします。

（注）　この例は、AnyConnect がただ 1 つのインストール済み接続プロバイダーであることを前提としたものです。複数のプロバイダーをインストールしている場合は、このウィンドウに表示される項目の中から、ユーザが使用するものをいずれか 1 つ選択する必要があります。

ステップ 5　接続されると、Vista のネットワーク接続ウィンドウとほぼ同じ画面が表示されます。異なるのは、右下隅に表示されるのが Microsoft の [接続解除（Disconnect）] ボタンである点です。このボタンは、正常に接続されたことを通知するためだけのものです。

図 3-10　接続解除ウィンドウの例

各ユーザのログイン用アイコンをクリックします。この例では、[VistaAdmin] をクリックするとコンピュータへのログインが完了します。

注意　接続が確立されると、ログイン時間が無制限になります。接続の確立後にユーザがログインを忘れた場合、VPN セッションは無期限に継続されます。

PLAP を使用した AnyConnect からの接続解除

VPN セッションが正常に確立されると、PLAP コンポーネントは元のウィンドウに戻ります。このときウィンドウの右下隅には [接続解除（Disconnect）] ボタン（図 3-10 の丸印で囲まれたボタン）が表示されます。

[接続解除（Disconnect）] をクリックすると、VPN トンネルが接続解除されます。

トンネルは、[接続解除（Disconnect）] ボタンの操作によって明示的に接続解除される以外に、次のような状況でも接続解除されます。

- ユーザが PLAP を使用して PC にログインした後で [キャンセル（Cancel）] を押した。
- ユーザがシステムへログインする前に PC がシャットダウンした。

この動作は、Windows Vista PLAP アーキテクチャの機能であり、AnyConnect の機能ではありません。

Trusted Network Detection

Trusted Network Detection（TND）を使用すると、ユーザが企業ネットワークの中（*信頼*ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、企業ネットワークの外（*非信頼*ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。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。

さらに AnyConnect で Start Before Logon（SBL）が実行されている場合は、ユーザが信頼ネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。

TND を使用している場合でも、ユーザが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザが信頼ネットワークに移動した場合だけです。たとえば、ユーザが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

TND 機能では AnyConnect の GUI を制御することで接続が自動的に開始されるため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。

TND は AnyConnect VPN Client プロファイルに設定します。ASA の設定を変更する必要はありません。

Trusted Network Detection の要件

TND は、Microsoft Windows 7、Vista、XP、および Mac OS X 10.5、10.6、10.7 が実行されているコンピュータのみサポートしています。

Trusted Network Detection の設定

クライアント プロファイルで TND の設定を行う手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Part 2）（Preferences (Part 2)）] ペインに移動します。

ステップ 3　[自動 VPN ポリシー（Automatic VPN Policy）] をオンにします。

（注）　[自動 VPN ポリシー（Automatic VPN Policy）] の設定にかかわらず、ユーザは VPN 接続を手動で制御できます。

ステップ 4　ユーザが企業ネットワークの中（信頼ネットワーク）にいる場合のクライアントの動作を規定する信頼ネットワーク ポリシーを選択します。次のオプションがあります。

- [接続解除（Disconnect）] : 信頼ネットワークではクライアントにより VPN 接続が終了します。
- [接続（Connect）] : 信頼ネットワークではクライアントにより 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クライアントの動作はありません。[信頼されたネットワークポリシー（Trusted Network Policy）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を共に [何もしない（Do Nothing）] に設定すると、Trusted Network Detection（TND）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。

ステップ 5　ユーザが企業ネットワークの外にいる場合のクライアントの動作を規定する非信頼ネットワーク ポリシーを選択します。次のオプションがあります。

- [接続（Connect）] : 非信頼ネットワークが検出されるとクライアントにより 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が検出されるとクライアントにより VPN 接続が開始されます。このオプションを選択すると、常時接続 VPN は無効となります。[信頼されたネットワークポリシー（Trusted Network Policy）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を共に [*何もしない（Do Nothing）*] に設定すると、Trusted Network Detection は無効となります。

ステップ 6　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）を指定します。スプリット DNS リストに追加しても、複数の DNS サフィックスを割り当てることができます。DNS サフィックスの照合の例については、表 3-1 を参照してください。

AnyConnect クライアントは、次の順序で DNS サフィックスのリストを構築します。

- ヘッド エンドから渡されたドメイン
- ヘッド エンドから渡されたスプリット DNS リスト
- 設定されている場合、パブリック インターフェイスの DNS サフィックス。設定されていない場合は、プライマリ DNS サフィックスの親サフィックスをともなうプライマリおよび接続固有のサフィックス（対応するボックスが拡張 TCP/IP 設定でオンの場合）

ステップ 7　信頼 DNS サーバを指定します。ここでは、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すべての DNS サーバ アドレス（カンマ区切りの文字列）を指定します。たとえば 161.44.124.* や 64.102.6.247 などです。DNS サーバ アドレスでは、ワイルドカード（*）がサポートされます。

（注）　TND を機能させるためには、すべての DNS サーバを指定する必要があります。TrustedDNSDomains と TrustedDNSServers の両方を設定した場合は、セッションが両方の設定に一致していないと、信頼ネットワークの中にあると見なされません。

表 3-1　DNS サフィックスの一致の例

照合する DNS サフィックス	TrustedDNSDomains に使用する値
cisco.com（単独）	*cisco.com
cisco.com および anyconnect.cisco.com	*.cisco.com または cisco.com、anyconnect.cisco.com
asa.cisco.com および anyconnect.cisco.com	*.cisco.com または asa.cisco.com、anyconnect.cisco.com

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。

TND と複数のプロファイルで複数のセキュリティ アプライアンスに接続するユーザ

ユーザのコンピュータ上に複数のプロファイルがあると、ユーザが TND の有効なセキュリティ アプライアンスから TND が有効でないセキュリティ アプライアンスへ接続を変更する際に問題が発生することがあります。ユーザが TND の有効なセキュリティ アプライアンスに接続していた場合、そのユーザは TND が有効なプロファイルを受け取っています。そのユーザが、信頼ネットワークの外でコンピュータをリブートすると、TND が有効であるクライアントの GUI が表示され、最後に接続していたセキュリティ アプライアンスへの接続が試行されますが、このセキュリティ アプライアンスでは、TND が有効でない可能性があります。

クライアントが TND の有効なセキュリティ アプライアンスに接続している場合、ユーザが TND の有効でない ASA に接続するためには、手動で接続解除してから、TND の有効でないセキュリティ アプライアンスに接続する必要があります。ユーザが TND の有効なセキュリティ アプライアンスと TND が有効でないセキュリティ アプライアンスのどちらにも接続する可能性がある場合は、TND を有効にする前にこの問題を考慮してください。

この問題を回避する手段としては、次のような対策が考えられます。

- 企業ネットワーク上にある*すべての ASA* にロードされるクライアント プロファイルで、TND をイネーブルにする。
- すべての ASA がリストされた *1 つのプロファイル*をホスト エントリ セクションに作成し、このプロファイルを*すべての* ASA にロードする。
- 複数の異なるプロファイルが必要ない場合は、*すべての* ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 ASA により上書きされます。

常時接続 VPN

ユーザがコンピュータにログインすると VPN セッションが自動的に確立されるように AnyConnect の設定を行うことができます。VPN セッションは、ユーザがコンピュータからログアウトするか、セッション タイマーまたはアイドル セッション タイマーが期限に達するまでは開いた状態が維持されます。これらのタイマーの値は、セッションに割り当てられたグループ ポリシーに指定されます。AnyConnect と ASA の接続が解除されても、このいずれかのタイマーが期限に達しない限り、ASA お

よびクライアントではセッションに割り当てられたリソースが保持されます。AnyConnect では、セッションが開いている場合は、それを再アクティブ化するために接続の再確立が継続して試行され、セッションが開いていない場合は、新しい VPN セッションの確立が継続的に試行されます。

（注） 常時接続がオンであっても、ユーザがログインしていない場合は、AnyConnect は VPN 接続を確立しません。AnyConnect が VPN 接続を確立するのは、ログイン後に限られます。

（ログイン後の）常時接続 VPN では、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が適用されます。

注意 現在、常時接続 VPN では、プロキシを介した接続はサポートされていません。

AnyConnect では、プロファイルで常時接続 VPN が検出されると、エンドポイントを保護するためにその他の AnyConnect プロファイルがすべて削除され、ASA に接続するよう設定されたパブリック プロキシはいずれも無視されます。

脅威に対する保護を強化するためにも、常時接続 VPN の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- 常時接続 VPN が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより、常時接続 VPN ポリシーを無視することができます。常時接続 VPN の安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。
- Windows コンピュータ上で次のフォルダまたはシスコ サブフォルダへのアクセスを制限します。
  - Windows XP ユーザの場合：C:\Document and Settings\All Users
  - Windows Vista ユーザおよび Windows 7 ユーザの場合：C:\ProgramData

  限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、AnyConnect プロファイル ファイルを削除できるため、常時接続機能を無効にすることができます。
- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。Mac OS ユーザに対してもこれに相当するものを事前に展開します。

常時接続 VPN の要件

常時接続 VPN をサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、常時接続 VPN をサポートできます。
- 常時接続 VPN を使用するには、ASA 上に有効なサーバ証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。

常時接続 VPN を設定する場合は、ご使用のサーバ証明書がストリクト モードに合格できることを確認してください。

常時接続 VPN は、Microsoft Windows 7、Vista、XP、および Mac OS X 10.5、10.6、10.7 が実行されているコンピュータのみサポートしています。

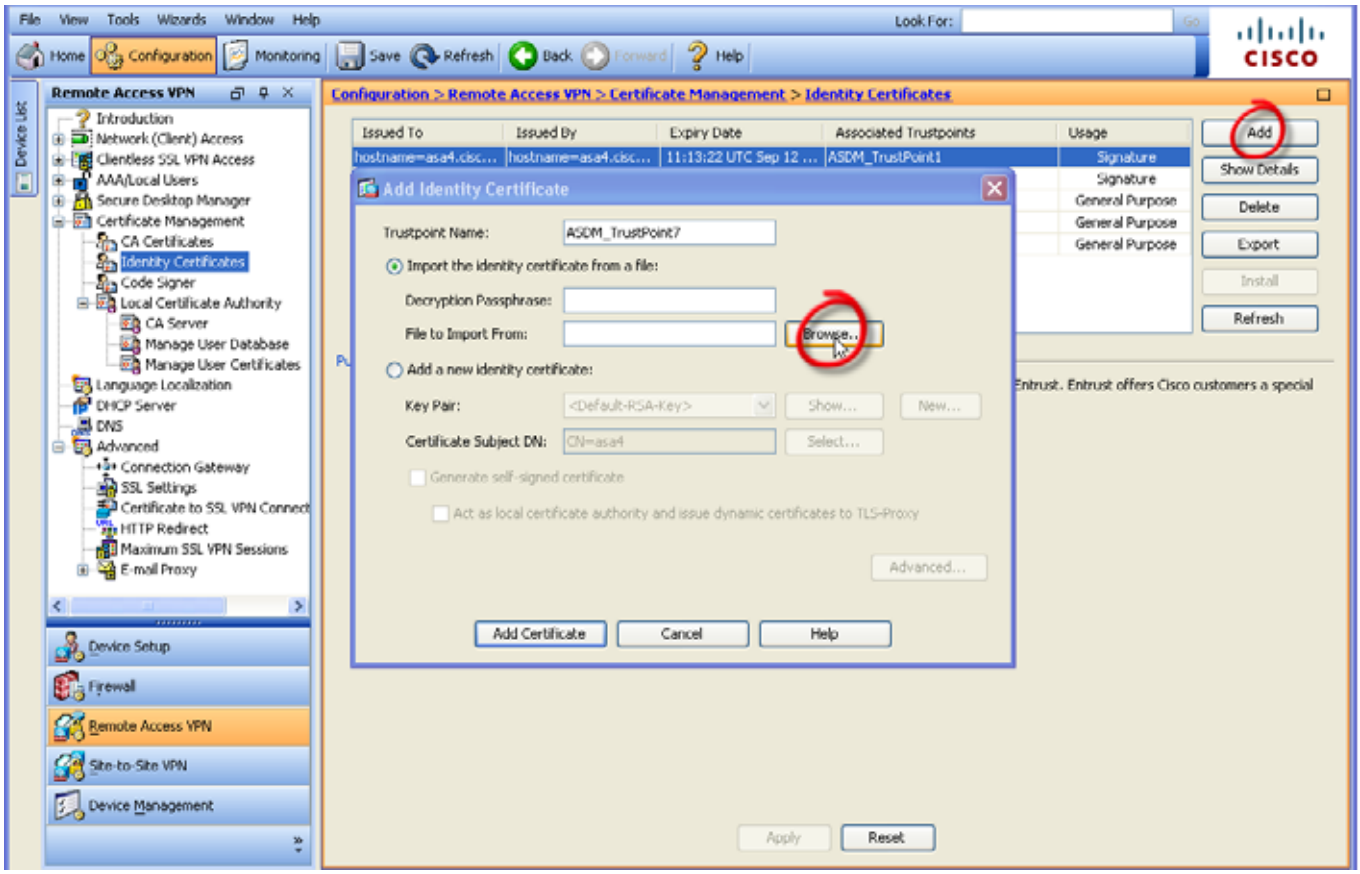
不正なサーバへの VPN 接続をロックする常時接続 VPN プロファイルをダウンロードできないようにするため、AnyConnect クライアントでは、セキュア ゲートウェイに接続する際、有効で信頼できるサーバ証明書が必要となります。認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。

自己署名証明書を生成すると、接続するユーザには証明書の警告が表示されます。この場合は、その証明書を信頼するようにブラウザを設定すると、それ以降は警告が表示されないようにすることができます。

（注）　自己署名証明書の使用はお勧めしません。理由は、ユーザが誤って不正なサーバ上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

ASDM では、ASA 上でのこの問題を解決できるよう、[アイデンティティ証明書（Identity Certificates）] パネル（[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] > [アイデンティティ証明書（Identity Certificates）]）に、公開証明書を容易に登録するための [ASA SSL VPN を Entrust で登録（Enroll ASA SSL VPN with Entrust）] ボタンが用意されています。このパネルにある [追加（Add）] ボタンを使用すると、ファイルから公開証明書をインポートするか、または自己署名証明書を生成することができます。

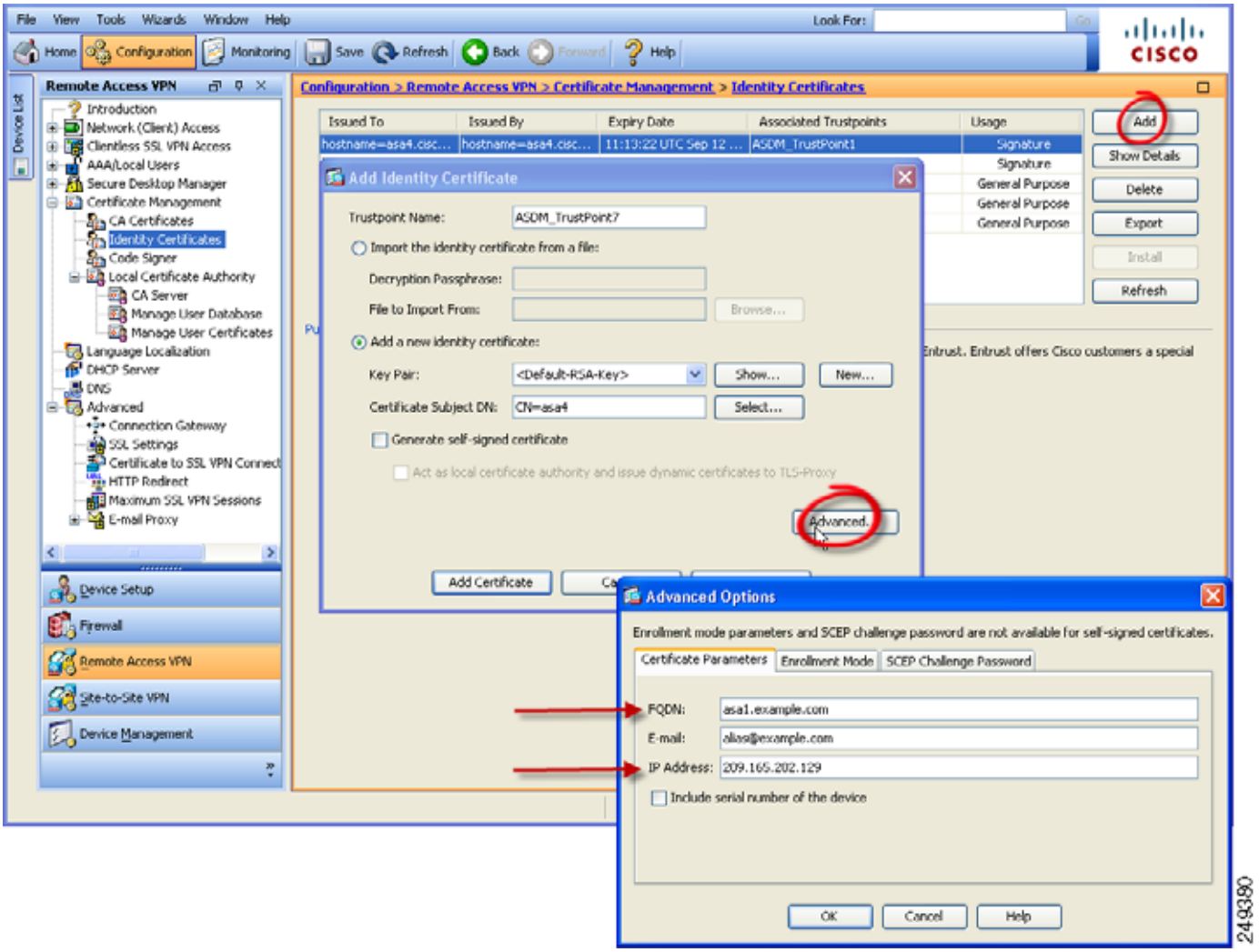
図 3-11　公開証明書の登録（画面は ASDM 6.3）



（注）　これらの手順は、証明書の設定に関するガイドラインとして記載されたものです。詳細については、ASDM の [ヘルプ（Help）] ボタンをクリックするか、設定するセキュア ゲートウェイ用の ASDM または CLI ガイドを参照してください。

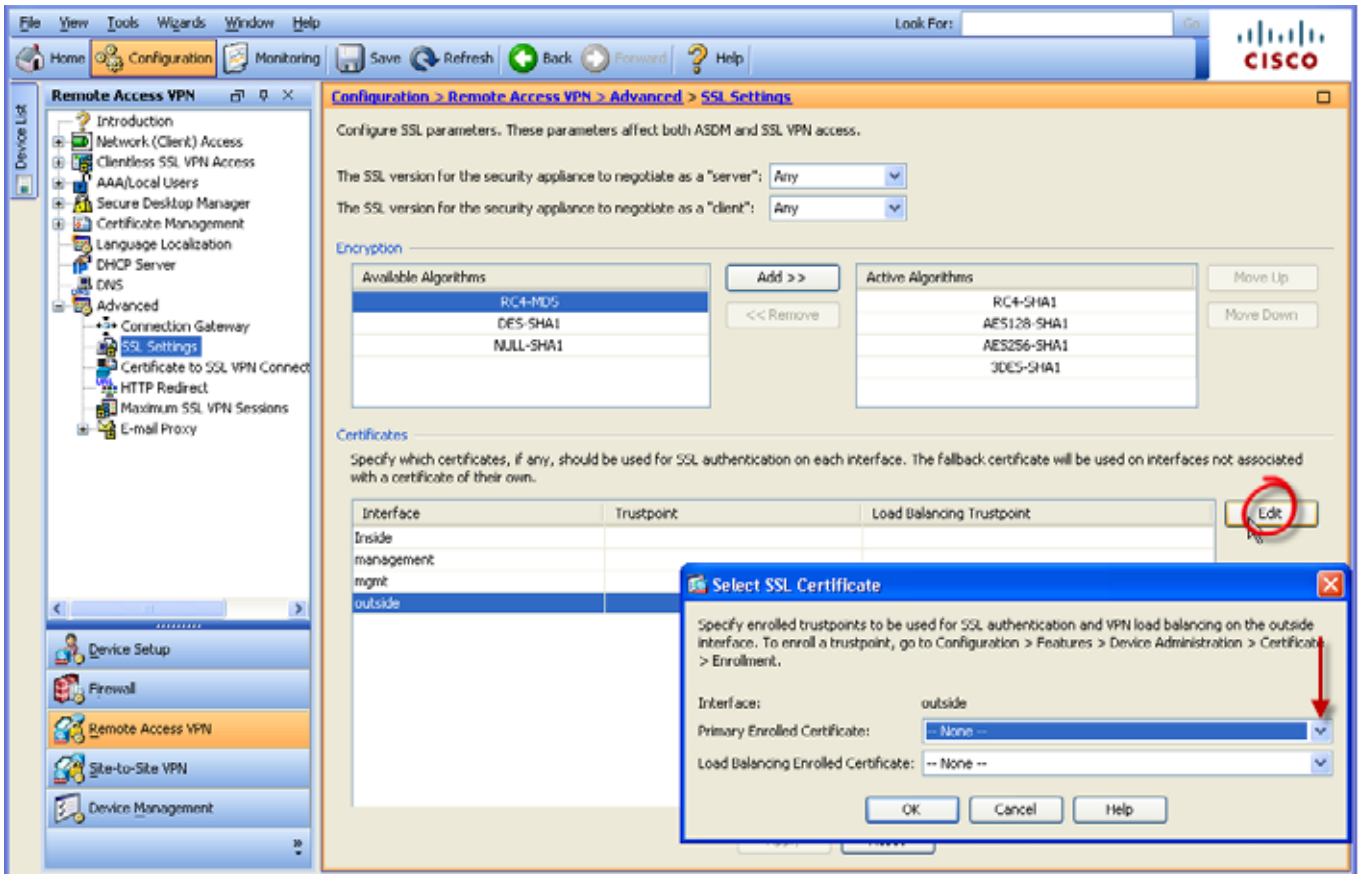
自己署名インターフェイスを生成する場合は、[詳細（Advanced）] ボタンを使用して、outside インターフェイスのドメイン名および IP アドレスを指定します。

図 3-12　自己署名証明書の生成（画面は ASDM 6.3）



証明書を登録したら、それを outside インターフェイスに割り当てます。その手順として、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [詳細（Advanced）] > [SSL 設定（SSL Settings）] を選択し、[証明書（Certificates）] エリアで「outside」エントリを編集して、[登録済みプライマリ証明書（Primary Enrolled Certificate）] ドロップダウン リストから証明書を選択します。

図 3-13　outside インターフェイスへの証明書の割り当て（画面は ASDM 6.3）



すべてのセキュア ゲートウェイに証明書を追加し、それを outside インターフェイスの IP アドレスに関連付けます。

サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加

常時接続 VPN は、AnyConnect VPN セッションのロード バランシングに影響を与えます。常時接続 VPN をディセーブルにした状態では、クライアントからロードバランシング クラスタ内のマスター デバイスに接続すると、クライアントはマスター デバイスから任意のバックアップ クラスタ メンバーにリダイレクトされます。常時接続 VPN を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがマスター デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロードバランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[サーバ リスト（Server List）] ペインに移動します。

ステップ 3　ロードバランシング クラスタのマスター デバイスであるサーバを選択して、[編集（Edit）] をクリックします。

ステップ 4　いずれかのロードバランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

常時接続 VPN の設定

コンピュータが非信頼ネットワーク内に存在することが検知された場合に限って VPN セッションが自動的に確立されるよう AnyConnect を設定する手順は次のとおりです。

ステップ 1　「Trusted Network Detection の設定」（P.3-17）に従って、Trusted Network Detection を設定します。

ステップ 2　[Always On] をオンにします。

常時接続 VPN からユーザを除外するポリシーの設定

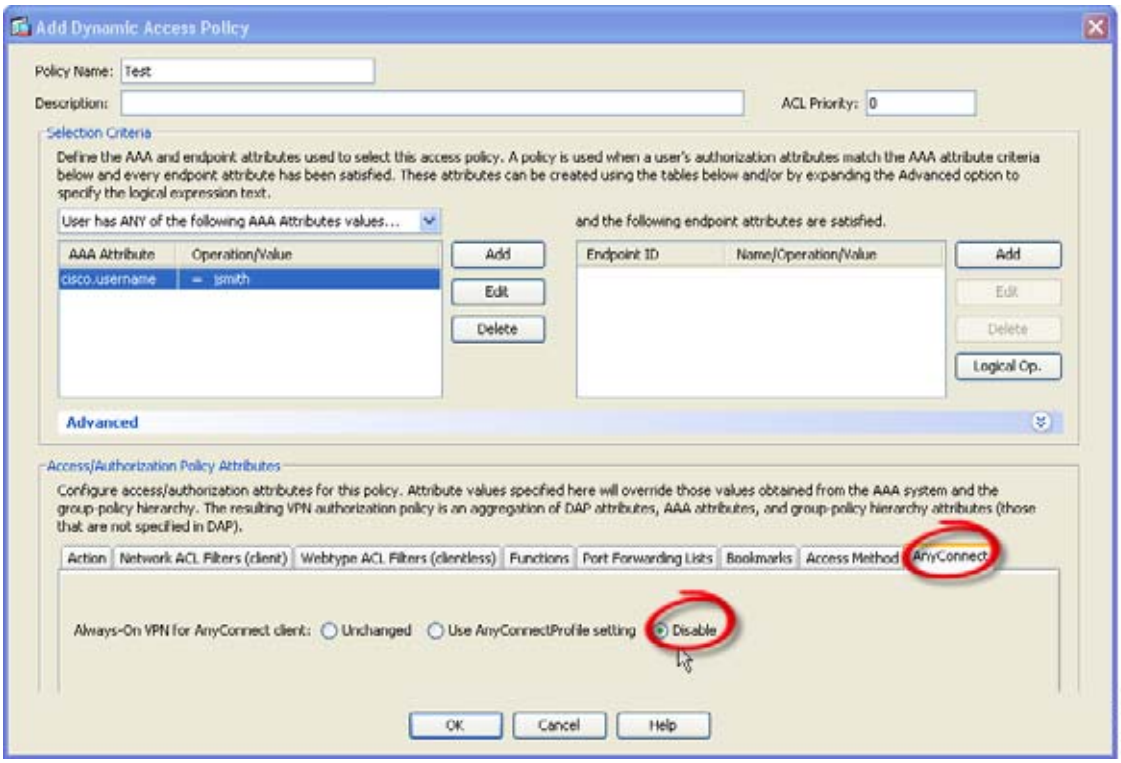
常時接続 VPN は、デフォルトでは無効になっています。常時接続ポリシーに優先して適用される除外規定を設定することができます。たとえば、特定のユーザに対して他社との VPN セッションを確立できるようにしつつ、企業外資産に対しては常時接続 VPN ポリシーを除外するという場合があります。

グループ ポリシーおよびダイナミック アクセス ポリシーで VPN 常時接続パラメータを設定すると、常時接続ポリシーを上書きすることができます。これにより、ポリシーの割り当てに使用される一致基準に従って例外を指定できます。AnyConnect ポリシーでは常時接続 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。

次に、AAA またはエンドポイント条件を使用して企業外資産へのセッションを照合するダイナミック アクセス ポリシーを設定する手順を示します。

ステップ 1　[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）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

図 3-14　常時接続 VPN からのユーザの除外



ステップ 2　ユーザを常時接続 VPN から除外する条件を設定します。たとえば、[選択基準（Selection Criteria）] エリアを使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3　[ダイナミック アクセス ポリシーの追加（Add Dynamic Access Policy）] ウィンドウまたは [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] ウィンドウの下半分にある [AnyConnect] タブをクリックします。

ステップ 4　[AnyConnect クライアントの常時接続 VPN（Always-On VPN for AnyConnect client）] の横にある [無効（Disable）] をクリックします。

Cisco AnyConnect Secure Mobility Client ポリシーでは常時接続 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。

常時接続 VPN 用の [接続解除（Disconnect）] ボタン

AnyConnect は、常時接続 VPN セッション用の [接続解除（Disconnect）] ボタンをサポートしています。これを有効にすると、AnyConnect では VPN セッションが確立された時点で [接続解除（Disconnect）] ボタンが表示されます。常時接続 VPN セッションのユーザは、[接続解除（Disconnect）] をクリックすることが必要になる場合があるため、次のような問題に対処できるよう代替セキュア ゲートウェイを選択することができます。

- 現在の VPN セッションに関するパフォーマンスの問題。
- VPN セッションが中断した後に生じる再接続の問題。

[接続解除（Disconnect）] ボタンをクリックすると、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、データの漏洩を防ぐことができるほか、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。

注意　[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。

常時接続 VPN セッション中にユーザが [接続解除（Disconnect）] ボタンをクリックすると、AnyConnect では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、データの漏洩を防ぐことができるほか、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。AnyConnect では、接続障害ポリシーの内容にかかわらず、すべてのインターフェイスがロックされます。

注意　[接続解除（Disconnect）] ボタンをクリックすると、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、データの漏洩を防ぐことができるほか、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。

[接続解除（Disconnect）] ボタンに関する要件

常時接続 VPN 用の接続解除オプションに関する要件は、「常時接続 VPN の要件」（P.3-20）と同じです。

[接続解除（Disconnect）] ボタンの有効化 / 無効化

常時接続 VPN を有効すると、プロファイル エディタでは、[接続解除（Disconnect）] ボタンがデフォルトで有効になります。[接続解除（Disconnect）] ボタンの設定を表示および変更する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Part 2）（Preferences (Part 2)）] ペインに移動します。

ステップ 3　[VPN の接続解除を許可（Allow VPN Disconnect）] をオンまたはオフにします。

常時接続 VPN に関する接続障害ポリシー

接続障害ポリシーでは、常時接続 VPN が有効であり、かつ AnyConnect で VPN セッションが確立できない場合（セキュア ゲートウェイが到達不能の場合など）に、コンピュータから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。フェールクローズド ポリシーでは、VPN アクセスを除くネットワーク接続が無効になります。フェールオープンでは、インターネットまたはその他の

ローカル ネットワーク リソースへの接続が許可されます。AnyConnect では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。次の表は、フェール オープン ポリシーおよびフェール クローズド ポリシーに関する説明をまとめたものです。

常時接続 VPN ポリシー	シナリオ	メリット	トレードオフ
フェール オープン	AnyConnect が VPN セッションの確立または再確立に失敗しました。この障害は、セキュア ゲートウェイが使用できない場合、または AnyConnect で（空港、喫茶店、ホテルなどで使用されることの多い）キャプティブ ポータルの存在を検出できない場合に発生することがあります。	最大限のネットワーク アクセス権を付与することで、インターネット リソースを始めとするローカル ネットワーク リソースへのアクセスが必要なタスクをユーザが継続的に実行できるようにします。	VPN セッションが確立されるまで、セキュリティや保護の対策は実行できません。そのため、エンドポイント デバイスが Web ベースのマルウェアに感染する可能性があるほか、機密データが漏洩する可能性もあります。
フェール クローズ	このオプションは主に、ネットワーク アクセスが常時利用できることよりもセキュリティの永続性の方が重視される、安全意識のきわめて高い組織に適しています。この点を除けば上記と同じです。	スプリット トンネリングにより許可されるプリンタやテザー デバイスといったローカル リソースへのアクセスを除くすべてのネットワーク アクセスが制限されます。テザー デバイスへのアクセスを除くすべてのネットワーク アクセスが制限されるため、エンドポイントは Web ベースのマルウェアから保護され、機密データの漏洩も常時防ぐことができます。	このオプションを選択した場合、VPN セッションが確立されるまでは、プリンタやテザー デバイスといったローカル リソースへのアクセスを除くすべてのネットワーク アクセスが制限されます。そのため、ユーザが VPN 外部のインターネット アクセスを要求したにもかかわらずセキュア ゲートウェイにアクセスできない場合には、生産性が著しく低下します。

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。AnyConnect では、「キャプティブ ポータル ホットスポットの検出と修復の要件」（P.3-30）で説明されているキャプティブ ポータルの大半が検出されます。ただし、キャプティブ ポータルを検出できない場合は、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。接続障害クローズド ポリシーは、細心の注意を払って実装してください。

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常時接続 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。

接続障害ポリシーに関する要件

接続障害ポリシー機能をサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、接続障害ポリシーをサポートできます。

接続障害ポリシーは、Microsoft Windows 7、Vista、XP、および Mac OS X 10.5、10.6、10.7 が実行されているコンピュータのみサポートしています。

接続障害ポリシーの設定

接続障害ポリシーのデフォルト設定では、常時接続 VPN が設定され、かつ VPN が到達不能の場合、インターネット アクセスが制限されます。接続障害ポリシーの設定を行う手順は次のとおりです。

ステップ 1　TND を設定します（「Trusted Network Detection の設定」（P.3-17）を参照）。

ステップ 2　[Always On] をオンにします。

ステップ 3　[Connect Failure Policy（接続エラーポリシー）] パラメータを次のいずれかに設定します。

- [クローズド（Closed）] :（デフォルト）セキュア ゲートウェイが到達不能の場合は、インターネット アクセスが制限されます。AnyConnect では、コンピュータが接続を許可されているセキュア ゲートウェイにバインドされていない、エンドポイントからのトラフィックをすべてブロックするパケット フィルタをイネーブルにすることで、この制限が実現されています。

  キャプティブ ポータル修復（次の項で説明）は、ポリシーの一部として特にイネーブルにされていない限り、フェールクローズド ポリシーでは制限されます。クライアント プロファイルで [最後の VPN ローカル リソースの適用（Apply Last VPN Local Resources）] が有効になっている場合、制限された状態では、直近の VPN セッションにより適用されたローカル リソース ルールを適用することができます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。常時接続が有効な場合は、AnyConnect ソフトウェアのアップグレード中、ネットワークはブロックされずオープンの状態になります。[クローズド（Closed）] 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）] : この設定では、クライアントが ASA に接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。[接続解除（Disconnect）] ボタンがイネーブルで、かつユーザが [接続解除（Disconnect）] をクリックした場合は、オープン接続障害ポリシーは適用されません。

（注）　ASA は、スプリット トンリングに対して IPv6 アドレスをサポートしていないため、ローカル印刷機能は IPv6 プリンタをサポートしていません。

キャプティブ ポータル ホットスポットの検出と修復

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、*キャプティブ ポータル*と呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。

ここでは、キャプティブ ポータル ホットスポットの検出機能および修復機能について説明します。

キャプティブ ポータル ホットスポットの検出と修復の要件

キャプティブ ポータルの検出と修復をどちらもサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、キャプティブ ポータルの検出および修復をサポートできます。

キャプティブ ポータル検出および修復は、Microsoft Windows 7、Windows Vista、Windows XP、および Mac OS X 10.5、10.6、10.7 が実行されているコンピュータのみサポートしています。

キャプティブ ポータル ホットスポットの検出

AnyConnect では、接続ができない場合、その原因を問わず GUI に「Unable to contact *VPN server*」というメッセージが表示されます。*VPN server* は、セキュア ゲートウェイを表します。常時接続が有効であり、かつキャプティブ ポータルが存在しない場合、クライアントでは VPN への接続が継続的に試行され、それによってステータス メッセージが更新されます。

常時接続 VPN が有効であり、接続障害ポリシーがクローズで、かつキャプティブ ポータルの修復が無効の場合に、AnyConnect でキャプティブ ポータルの存在が検出されると、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

AnyConnect によりキャプティブ ポータルの存在が検出され、かつ AnyConnect の設定が上述した内容と異なる場合、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

キャプティブ ポータルの検出はデフォルトで有効になっており、設定を行うことはできません。

キャプティブ ポータル検出中は、AnyConnect によりブラウザの設定が変更されることはありません。

キャプティブ ポータル ホットスポット修復

*キャプティブ ポータルの修復*は、ネットワーク アクセス権を取得できるように、キャプティブ ポータルのホット スポット要件を満たすためのプロセスです。

キャプティブ ポータルの修復は、AnyConnect により実行されるものではなく、エンド ユーザによる修復の実行に依存しています。

エンド ユーザは、ホットスポット プロバイダーの要件を満たすことで、キャプティブ ポータル修復を実行します。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

AnyConnect の常時接続が有効になっており、接続障害ポリシーが [クローズド（Closed）] に設定されている場合は、AnyConnect VPN Client プロファイルで、キャプティブ ポータル修復を明示的に許可する必要があります。常時接続が有効になっており、接続障害ポリシーが [オープン（Open）] に設定されている場合は、ユーザはネットワークへのアクセスを制限されることはないため、AnyConnect VPN Client プロファイルでキャプティブ ポータル修復を明示的に許可する必要はありません。

キャプティブ ポータル ホットスポット修復をサポートするための設定

常時接続機能が有効になっており、接続障害ポリシーがクローズドに設定されている場合は、AnyConnect VPN クライアント ポリシーでキャプティブ ポータル修復をイネーブルにする必要があります。接続障害ポリシーがオープンに設定されている場合は、ユーザがネットワーク アクセスを制限されることがないため、AnyConnect VPN クライアント ポリシーでその他の設定を行わなくても、キャプティブ ポータルは修復されます。

デフォルトの場合、キャプティブ ポータルの修復は無効です。キャプティブ ポータル修復をイネーブルにするには、次の作業を実行します。

ステップ 1　接続障害ポリシーの設定を行います（「接続障害ポリシーの設定」（P.3-29）を参照）。

ステップ 2　接続障害ポリシーをクローズドに設定した場合は、次のパラメータを設定します。

- [キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]：オンにすると、クローズ接続障害ポリシーにより適用されたネットワーク アクセスの制限が Cisco AnyConnect Secure Mobility Client により解除されます。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 アクセス制限が解除される時間を分単位で入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

  常時接続 VPN が有効な場合に、ユーザが [接続（Connect）] をクリックするか、または再接続が実行されると、キャプティブ ポータルが存在することを示すメッセージ ウィンドウが表示されます。この時点でユーザは、Web ブラウザ ウィンドウを開いてキャプティブ ポータルを修復することができます。

ユーザがキャプティブ ポータル ページにアクセスできない場合

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、修復できるようになるまで次の手順を試行するようユーザに指示してください。

ステップ 1　ネットワーク インターフェイスを無効にした後、再度有効にします。この操作により、キャプティブ ポータルの検出が再試行されます。

ステップ 2　修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP Phone クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、「Denial of Service」攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

ステップ 3　ステップ 1 を再試行します。

ステップ 4　コンピュータをリスタートします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォール

ユーザが ASA に接続すると、すべてのトラフィックがその接続を介してトンネリングされるため、ユーザはローカル ネットワーク上のリソースにアクセスできなくなります。こうしたリソースには、ローカル コンピュータと同期するプリンタ、カメラ、テザー デバイスなどが含まれます。この問題は、クライアント プロファイルで [ローカル LAN アドレス（Local LAN Access）] を有効にすることで解消されます。ただし、ローカル ネットワークへのアクセスが無制限になるため、一部の企業ではセキュリティやポリシーについて懸念が生じる可能性があります。ASA を使用してエンドポイントの OS のファイアウォール機能を導入することにより、プリンタやテザー デバイスなど特定タイプのローカル リソースに対するアクセスを制限することができます。

そのための操作として、印刷用の特定ポートに対するクライアント ファイアウォール ルールを有効にします。クライアントでは、着信ルールと発信ルールが区別されます。印刷機能の場合、クライアントでは発信接続に必要なポートは開放されますが、着信トラフィックはすべてブロックされます。クライアント ファイアウォールは、常時接続機能とは独立したものです。

クライアント ファイアウォール機能は、Windows 7、Vista、および XP、Mac OS X 10.5-10.8、Red Hat Enterprise Linux 5 および 6（デスクトップ）、Ubuntu 9.x、10.x でサポートされます。

（注）　管理者としてログインしたユーザは、ASA によりクライアントへ展開されたファイアウォール ルールを修正できることに注意が必要です。限定的な権限を持つユーザは、ルールを修正できません。どちらのユーザの場合も、接続が終了した時点でクライアントによりルールが再適用されます。

クライアント ファイアウォールを設定している場合、ユーザが Active Directory（AD）サーバで認証されると、クライアントでは引き続き ASA のファイアウォール ポリシーが適用されます。ただし、AD グループ ポリシーで定義されたルールは、クライアント ファイアウォールのルールよりも優先されます。

ファイアウォールの動作に関する注意事項

ここに記載したのは、AnyConnect クライアントではファイアウォールがどのように使用されるかについての注意事項です。

- ファイアウォール ルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォール ルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。プライベート ルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect のファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォール ルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアントへプッシュされても、ユーザがカスタムの拒否ルールを作成していれば、AnyConnect ルールは適用されません。
- Windows Vista の場合、ファイアウォール ルールが作成されると、Windows Vista ではポート番号の範囲がカンマ区切りの文字列として認識されます。ポート範囲は、最大で 300 ポートです（1 ～ 300、5000 ～ 5300 など）。指定した範囲が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォール ルールが適用されます。
- ファイアウォール サービスが AnyConnect クライアントにより開始される必要がある（システムにより自動的に開始されない）Windows ユーザは、VPN 接続の確立にかなりの時間を要する場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用されたのと同じ順序でルールが適用されます。グローバル ルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティ ファイアウォールの双方で許可されたタイプのトラフィックのみ通過できます。AnyConnect クライアントで許可されているタイプのトラフィックであっても、サードパーティ ファイアウォールによってブロックされれば、そのトラフィックはクライアントでもブロックされます。

以下の項では、次の処理を行うための手順について説明します。

- 「ローカル プリンタをサポートするためのクライアント ファイアウォールの導入」（P.3-33）
- 「テザー デバイスのサポート」（P.3-35）

ローカル プリンタをサポートするためのクライアント ファイアウォールの導入

ASA は、ASA バージョン 8.3(1) 以降、および ASDM バージョン 6.3(1) 以降で、SSL VPN クライアント ファイアウォール機能をサポートしています。この項では、ローカル プリンタへのアクセスが許可されるようにクライアント ファイアウォールを設定する方法、および VPN 接続の失敗時にファイアウォールを使用するようクライアント プロファイルを設定する方法について説明します。

クライアント ファイアウォールの制限事項

クライアント ファイアウォールを使用してローカル LAN アクセスを制限する場合には次の制限事項が適用されます。

- OS の制限事項により、Windows XP が実行されているコンピュータのクライアント ファイアウォール ポリシーは、着信トラフィックに対してのみ適用されます。発信ルールおよび双方向ルールは無視されます。これには、「permit ip any any」などのファイアウォール ルールが含まれます。
- ホスト スキャンや一部のサードパーティ ファイアウォールは、ファイアウォールを妨害する可能性があります。
- ASA はスプリット トンネリングに対して IPv6 アドレスをサポートしていないため、クライアント ファイアウォールもローカル ネットワーク上の IPv6 デバイスをサポートしていません。

表 3-2 は、送信元ポートおよび宛先ポートの設定により影響を受けるトラフィックの方向をまとめたものです。

表 3-2　送信元ポート/宛先ポートと影響を受けるトラフィックの方向

送信元ポート	宛先ポート	影響を受けるトラフィックの方向
特定のポート番号	特定のポート番号	着信および発信
範囲または「すべて」（値は 0）	範囲または「すべて」（値は 0）	着信および発信
特定のポート番号	範囲または「すべて」（値は 0）	着信のみ
範囲または「すべて」（値は 0）	特定のポート番号	発信のみ

ローカル印刷に関する ACL ルールの例

ACL AnyConnect_Client_Local_Print は、クライアント ファイアウォールを設定しやすくするために、ASDM を備えています。グループ ポリシーの [クライアント ファイアウォール（Client Firewall）] ペインのパブリック ネットワーク ルールのために ACL を選択する際は、一覧に次の ACE を含めます。

表 3-3　AnyConnect_Client_Local_Print の ACL ルール

説明	許可	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
すべて拒否	拒否	パブリック	任意	デフォルト[1]	任意	デフォルト
LPD	許可	パブリック	TCP	デフォルト	任意	515
IPP	許可	パブリック	TCP	デフォルト	任意	631
プリンタ	許可	パブリック	TCP	デフォルト	任意	9100
mDNS	許可	パブリック	UDP	デフォルト	224.0.0.251	5353
LLMNR	許可	パブリック	UDP	デフォルト	224.0.0.252	5355
NetBios	許可	パブリック	TCP	デフォルト	任意	137
NetBios	許可	パブリック	UDP	デフォルト	任意	137

1. ポート範囲は 1 ～ 65535 です。

（注）　ローカル印刷を有効にするには、定義済み ACL ルール「*allow Any Any*」に対し、クライアント プロファイルの [ローカル LAN アドレス（Local LAN Access）] 機能を有効にする必要があります。

ローカル印刷サポートの設定

ローカル印刷サポートを有効にする手順は次のとおりです。

ステップ 1　グループ ポリシーで、SSL VPN クライアント ファイアウォールを有効にします。[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）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます。

ステップ 3　[詳細（Advanced）] > [SSL VPN クライアント（SSL VPN Client）] > [クライアント ファイアウォール（Client Firewall）] を選択します。プライベート ネットワーク ルールに対応する [管理（Manage）] をクリックします。

ステップ 4　表 3-3 にあるルールを使用して、ACL を作成し ACE を指定します。この ACL をパブリック ネットワーク ルールとして追加します。

ステップ 5　常時接続の自動 VPN ポリシーを有効にし、かつクローズド ポリシーを指定している場合、VPN 障害が発生するとユーザはローカル リソースにアクセスできません。このシナリオでは、プロファイル エディタで [プリファレンス（Part 2）（Preferences (Part 2)）] に移動し、[最後のローカル VPN リソース ルールの適用（Apply last local VPN resource rules）] をオンにするとファイアウォール ルールを適用することができます。

テザー デバイスのサポート

テザー デバイスをサポートして企業ネットワークを保護する場合は、グループ ポリシーで標準的な ACL を作成し、テザー デバイスで使用する宛先アドレスの範囲を指定します。さらに、トンネリング VPN トラフィックから除外するネットワーク リストとしてスプリット トンネリング用の ACL を指定します。また、VPN 障害時には最後の VPN ローカル リソース ルールが使用されるようにクライアント プロファイルを設定することも必要です。

ステップ 1　ASDM で、[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] を選択します。

ステップ 2　[ネットワーク リスト（Network List）] フィールドの横にある [管理（Manage）] をクリックします。ACL Manager が表示されます。

ステップ 3　[標準 ACL（Standard ACL）] タブをクリックします。

ステップ 4　[追加（Add）] をクリックし、さらに [ACL の追加（Add ACL）] をクリックします。新しい ACL の名前を指定します。

ステップ 5　テーブルで新しい ACL を選択して、[追加（Add）] をクリックし、さらに [ACE の追加（Add ACE）] をクリックします。[ACE の編集（Edit ACE）] ウィンドウが表示されます。

ステップ 6　[アクション（Action）] で [許可（Permit）] オプション ボタンを選択します。[宛先（Destination）] に *169.254.0.0* と指定します。[サービス：（Service:）] に対して *IP* を選択します。[OK] をクリックします。

ステップ 7　[スプリット トンネリング（Split Tunneling）] ペインで、[ポリシー（Policy）] に対し [以下のネットワーク リストを除外する（Exclude Network List Below）] を選択します。[ネットワーク リスト（Network List）] で、作成した ACL を選択します。[OK] をクリックし、さらに [適用（Apply）] をクリックします。

Mac OS X の新規インストール ディレクトリ構造

AnyConnect の以前のリリースでは、AnyConnect コンポーネントは **opt/cisco/vpn** のパスにインストールされました。現在、AnyConnect コンポーネントは、パス /opt/cisco/anyconnect にインストールされます。

Web セキュリティ クライアント プロファイルの ScanCenter ホステッド コンフィギュレーション サポート

Web セキュリティ ホステッド クライアント プロファイルの ScanCenter ホステッド コンフィギュレーションを使用すると、管理者は Web セキュリティ クライアントに新しい Web セキュリティ クライアント プロファイルを提供できます。Web セキュリティを備えたデバイスは、クラウドから新しいクライアント プロファイルをダウンロードできます（ホステッド コンフィギュレーション ファイルは ScanCenter サーバに格納されています）。この機能の唯一の前提条件は、有効なクライアント プロファイルでデバイスに Web セキュリティがインストールされていることです。

管理者は、Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを ScanCenter サーバにアップロードします。この XML ファイルには、ScanSafe からの有効なライセンス キーが含まれている必要があります。ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Web セキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。いったん新しいクライアント プロファイルがダウンロードされたら、管理者が新しいクライアント プロファイル ファイルを使用可能にするまで、Web セキュリティにより同じファイルが再度ダウンロードされることはありません。

（注）　ホステッド コンフィギュレーション機能を使用するためには、ScanSafe ライセンス キーが含まれた有効なクライアント プロファイル ファイルを使用して、Web セキュリティ クライアント デバイスをあらかじめインストールしておく必要があります。

スプリット DNS の機能拡張

AnyConnect は、レガシー IPsec クライアントと同様に、Windows プラットフォームと Mac OS X プラットフォーム向けのトゥルー スプリット DNS 機能をサポートしています。セキュリティ アプライアンスのグループ ポリシーにより Split-Include トンネリングがイネーブルになっており、トンネリング対象の DNS 名が指定されている場合、AnyConnect は、この名前に一致するすべての DNS クエリーをプライベート DNS サーバにトンネリングします。トゥルー スプリット DNS を使用すると、ASA に

よってプッシュダウンされたドメインに一致する DNS 要求へのトンネル アクセスのみが許可されます。これらの要求は、クリア テキストでは送信されません。一方、DNS 要求が ASA によってプッシュダウンされたドメインに一致しない場合は、AnyConnect は、クライアントのオペレーティング システムにある DNS リゾルバから、DNS 解決に使用されるホスト名を暗号化せずに送信させます。

（注）
- スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。
- スプリット DNS は、「Exclude Network List Below」スプリット トンネリング ポリシーをサポートしません。「Tunnel Network List Below」スプリット トンネリング ポリシーを使用して、スプリット DNS を設定します。

グループ ポリシーによりトンネリングされるドメインが指定されていない場合、または [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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] で [すべてのネットワークをトンネリング（Tunnel All Networks）] が選択されている場合は、AnyConnect はすべての DNS クエリーをトンネリングします。ドメイン名解決には、オペレーティング システムの DNS リゾルバに依存するあらゆるツールまたはアプリケーションを使用できます。たとえば、ping または Web ブラウザを使用してスプリット DNS ソリューションをテストできます。nslookup または dig などのその他のツールは、OS DNS リゾルバを回避します。

Mac OS X には、IPv6 アドレス プールを設定しない場合に限り、AnyConnect は、実際のスプリット DNS を使用できます。IPv6 アドレス プールが設定されている場合、AnyConnect は、スプリット トンネリング用の DNS フォールバックを有効にできます。

この機能には、次のことが必要です。

- 少なくとも 1 台の DNS サーバを設定する
- Split-Include トンネリングのイネーブルにする
- トンネリングするドメインを 1 つ以上指定する
- [すべての DNS ルックアップをトンネルを通じて送信する（Send All DNS lookups through tunnel）] チェックボックスをオフにする。このチェックボックスは、[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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] にあります。

AnyConnect ログによる確認

スプリット DNS がイネーブルであることを確認するには、AnyConnect のログで、「Received VPN Session Configuration Settings」が含まれたエントリを検索します。イネーブルである場合、このエントリに *Split DNS:enabled* と示されます。

スプリット DNS を使用しているドメインの確認

クライアントを使用して、どのドメインがスプリット DNS に使用されているかを確認する手順は次のとおりです。

ステップ 1　**ipconfig/all** を実行して、DNS サフィックス検索リストの横にリストされたドメインを記録します。

ステップ 2　VPN 接続を確立し、DNS サフィックス検索リストの横にリストされたドメインを再度確認します。

トンネルを確立した後に追加されたドメインは、スプリット DNS で使用されるドメインです。

（注）　このプロセスは、ASA からプッシュされたドメインと、クライアント ホストで設定済みのドメインがオーバーラップしていないことを前提としています。

スプリット DNS の設定

この機能を設定するには、セキュリティ アプライアンスへの ASDM 接続を確立して、次の手順を両方とも実行します。

Split-Include トンネリングの設定

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote AccessVPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] を選択します。

ステップ 2　[ポリシー（Policy）] ドロップダウン メニューで [以下のトンネル リスト（Tunnel List Below）] を選択し、[ネットワーク リスト（Network List）] ドロップダウン メニューから該当するネットワーク リストを選択します。

AnyConnect 3.0.7 リリース以降では、Split-Include ネットワークがローカル サブネットの完全一致（192.168.1.0/24 など）の場合、対応するトラフィックはトンネリングされています。Split-Include ネットワークがローカル サブネットのスーパーセット（192.168.0.0/16 など）の場合、対応するトラフィックは、ローカル サブネットを除き、トンネリングされています。ローカル サブネット トラフィックをトンネリングするには、一致する Split-Include ネットワーク（192.168.1.0/24 および 192.168.0.0/16 の両方を Split-Include ネットワークとして指定）を追加する必要があります。

DNS サーバの設定

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote AccessVPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [サーバ（Servers）] を選択します。

ステップ 2　[DNS サーバ（DNS Servers）] フィールドに、プライベート DNS サーバを 1 つ以上入力します。

AnyConnect 3.0.4 以降の場合、[DNS サーバ（DNS Servers）] フィールドで最大 25 台の DNS サーバ エントリをサポートし、それ以前のリリースでは、最大 10 台の DNS サーバ エントリをサポートします。

SCEP による認証登録の設定

SCEP を使用した証明書登録について

AnyConnect セキュア モビリティ クライアントでは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一環として証明書のプロビジョニングおよび更新を行うことができます。SCEP の目的は、既存のテクノロジーを使用して、スケーラブルな方法で、ネットワーク デバイスに証明書を安全に発行できるようにすることです。

SCEP を使用した証明書の登録は、ASA への AnyConnect IPsec および SSL VPN 接続で次のようにサポートされます。

- SCEP プロキシ : ASA はクライアントと CA 間の SCEP 要求と応答のプロキシとして機能します。
  - クライアントが CA に直接アクセスしないため、CA は、AnyConnect クライアントではなく ASA にアクセスできる必要があります。
  - 登録は、クライアントにより常に自動的に開始されます。ユーザの介入は必要ありません。
  - SCEP プロキシでは、AnyConnect 3.0 以降でサポートされます。
- レガシー SCEP : AnyConnect クライアントは CA と直接通信をして、証明書を登録し取得します。
  - CA は、確立された VPN トンネルを介して、またはクライアントが存在する同じネットワークで直接、ASA ではなく AnyConnect クライアントにアクセス可能である必要があります。
  - 登録はクライアントによって自動的に開始されますが、設定されている場合は、ユーザによって手動で開始される場合があります。
  - レガシー SCEP は、AnyConnect 2.4 以降でサポートされます。

SCEP プロキシの登録

次の手順は、AnyConnect および ASA が SCEP プロキシ用に設定されている場合、証明書が取得された証明書ベースの接続が行われたプロセスについて説明します。

1. ユーザは、証明書と AAA 認証の両方用に設定された接続プロファイルを使用して、ASA ヘッドエンドに接続します。ASA は、クライアントからの認証用に証明書と AAA クレデンシャルを要求します。
2. ユーザが AAA クレデンシャルを入力しますが、有効な証明書は使用可能ではありません。この状況は、入力された AAA クレデンシャルを使用してトンネルが確立された後で、クライアントが自動 SCEP 登録要求を送信するトリガーになります。
3. ASA が CA に対して登録要求を転送し、CA の応答をクライアントに返します。
4. SCEP 登録が成功すると、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは、証明書認証を使用して、ASA トンネル グループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは管理者に連絡する必要があります。

SCEP プロキシのメモ

- クライアントは、[**証明書失効しきい値（Certificate Expiration Threshold**）] フィールドが VPN プロファイルで設定されている場合、ユーザの介入なしで、期限が切れる前に自動で証明書を更新します。

- SCEP プロキシ登録は、SSL および IPSec トンネルの証明書認証用に SSL を使用する必要があります。

レガシー SCEP の登録

次の手順は、AnyConnect がレガシー SCEP 用に設定されている場合、証明書が取得された証明書ベースの接続が行われたプロセスについて説明します。

1. ユーザは、証明書認証用に設定されたトンネル グループを使用して ASA ヘッドエンドへの接続を開始します。ASA はクライアントからの認証用に証明書を要求します。
2. 有効な証明書はクライアントで使用可能ではなく、接続を確立することができません。この証明書の失敗は、SCEP 登録を行う必要があることを示します。
3. ユーザは、AAA 認証用に設定されたトンネル グループを使用して、アドレスがクライアント プロファイルで設定された**自動 SECP ホスト**に一致する ASA ヘッドエンドへの接続を開始する必要があります。ASA は、クライアントからの AAA クレデンシャルを要求します。
4. クライアントは、AAA クレデンシャルを入力するためのユーザ用ダイアログ ボックスを提示します。

   クライアントが手動登録用に設定され、クライアントが SCEP 登録開始の必要性を認識した場合（ステップ 2 を参照）、[証明書を取得（Get Certificate）] ボタンがクレデンシャル ダイアログ ボックスに表示されます。クライアントがネットワークの CA にダイレクト アクセスがある場合、ユーザは手動でこのボタンをクリックすることで、証明書を取得することができます。

   （注） CA へのアクセスが確立された VPN トンネルに依存する場合、現在確立された VPN トンネルがないため（AAA クレデンシャルが入力されていないため）、この時点での手動登録はできません。

5. ユーザは、AAA クレデンシャルを入力し、VPN 接続を確立します。
6. クライアントは、SCEP 登録開始の必要性を認識した場合（ステップ 2 を参照）、確立された VPN トンネルを介して CA に登録要求を開始し、応答は CA から受信します。
7. SCEP 登録が成功すると、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは、証明書認証を使用して、ASA トンネル グループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは管理者に連絡する必要があります。
8. クライアントが手動登録用に設定されており、**[証明書失効しきい値（Certificate Expiration Threshold）]** の値が一致した場合、[証明書を取得（Get Certificate)] ボタンが提示されたトンネル グループの選択ダイアログ ボックスに表示されます。ユーザはこのボタンをクリックすることで、手動で証明書を更新できます。

レガシー SCEP のメモ

- 手動でレガシー SCEP 登録を使用する場合は、クライアント プロファイルのイネーブル CA パスワードを推奨します。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。
- 証明書の有効期限が切れ、クライアントに有効な証明書が存在しない場合、クライアントはレガシー SCEP 登録プロセスを実行します。

SCEP のガイドラインと制限事項

- ASA ロード バランシングは、SCEP 登録でサポートされます。
- ASA へのクライアントレス（ブラウザ ベース）VPN アクセスは、SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）がサポートされます。
- ASA は、クライアントから受信した要求を記録しますが、登録が失敗した理由は表示しません。接続の問題は、CA またはクライアントでデバッグされる必要があります。
- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- 一部の CA は、登録パスワードを電子メールでユーザに送信するように設定できます。これにより、セキュリティがより一層強化されます。このパスワードも、AnyConnect クライアント プロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

Windows 証明書の警告

Windows クライアントが最初に認証局から証明書を取得しようとした際に、警告がなされる可能性があります。プロンプトが表示されたら、[はい（Yes）] をクリックしてください。これにより、ルート証明書をインポートできます。クライアント証明書との接続に影響しません。

ポリシーを適用するため登録接続を特定

ASA で、登録接続を捕捉し、選択された DAP レコードの適切なポリシーを適用するために、aaa.cisco.sceprequired 属性が使用されます。

証明書のみの認証および ASA での証明書マッピング

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルと共に、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が ASA に提供された時点でこのトンネル グループにユーザが配置されるようにすることができます。

SCEP プロキシ証明書登録の設定

SCEP プロキシ登録用 VPN クライアント プロファイルの設定

ステップ 1　ASDM からプロファイル エディタを起動するか、またはスタンドアロンの VPN プロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ASDM では、[**追加（Add）**]（または [**編集（Edit）**] をクリックして、AnyConnect プロファイルを作成（または編集）します。スタンドアロン エディタでは、既存のプロファイルを開くか、新しいプロファイルの作成を続行します。

ステップ 3　左側の [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ツリーで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 4　[証明書の登録（Certificate Enrollment）] ペインで、[証明書の登録（Certificate Enrollment）] をオンにします。

ステップ 5　登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの [証明書の登録（Certificate Enrollment）]」（P.3-83）を参照してください。

（注）
- %machineid% を使用した場合は、デスクトップ クライアントに Hostscan/Posture がロードされます。
- モバイル クライアントの場合、証明書フィールドのうち少なくとも 1 つを指定する必要があります。

SCEP プロキシ登録をサポートするための ASA の設定

SCEP プロキシのため、1 つの ASA 接続プロファイルは、証明書登録および認証された VPN 接続をサポートします。

前提条件

SCEP プロキシ用のクライアント プロファイル（例：ac_vpn_scep_proxy）を設定します。「SCEP プロキシ登録用 VPN クライアント プロファイルの設定」（P.3-41）を参照してください。

ステップ 1　グループ ポリシー（例：cert_group）を作成します。次のフィールドを設定します。

- [一般（General）] で、[SCEP フォワーディング URL（SCEP Forwarding URL）] に CA への URL を入力します。
- [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアント プロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、SCEP プロキシ用に設定されたクライアント プロファイルを指定します。　たとえば、ac_vpn_scep_proxy クライアント プロファイルを指定します。

ステップ 2　証明書の登録および接続を認証した証明書（例：cert_tunnel）用の接続プロファイルを作成します。

- [認証（Authentication）] : Both（AAA および Certificate）
- デフォルトのグループ ポリシー：cert_group
- [詳細（Advanced）] > [一般（General）] で、[この接続プロファイルへの SCEP 登録を有効にする（Enable SCEP Enrollment for this Connction Profile）] をオンにします。
- [詳細（Advanced）] > [グループエイリアス / グループ URL（GroupAlias/Group URL）] で、この接続プロファイルのグループ（cert_group）が含まれるグループ URL を作成します。

レガシー SCEP 証明書登録の設定

レガシー SCEP 登録用 VPN クライアント プロファイルの設定

ステップ 1　ASDM からプロファイル エディタを起動するか、またはスタンドアロンの VPN プロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ASDM では、[**追加（Add）**]（または [**編集（Edit）**] をクリックして、AnyConnect プロファイルを作成（または編集）します。スタンドアロン エディタでは、既存のプロファイルを開くか、新しいプロファイルの作成を続行します。

ステップ 3　左側の [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ツリーで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 4　[証明書の登録（Certificate Enrollment）] ペインで、[証明書の登録（Certificate Enrollment）] をオンにします。

ステップ 5　クライアントに証明書を検索するよう指示するため、**自動 SCEP ホスト**を指定します。

FQDN または IP アドレス、および SCEP 証明書取得用に設定された接続プロファイル（トンネル グループ）のエイリアスを入力します。たとえば、**asa.cisco.com** が ASA のホスト名で、**scep_eng** が接続プロファイルのエイリアスの場合、**asa.cisco.com/scep-eng** と入力します。

ユーザが接続を開始すると、レガシー SCEP 登録を正常に実行するために、選択または指定されたアドレスがこの値に正確に一致する必要があります。たとえば、このフィールドが FQDN に設定される場合、ユーザは IP アドレス（SCEP 登録が失敗する）を指定します。

ステップ 6　認証局の属性の設定：

（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、発行された証明書の「fingerprint」または「thumbprint」属性フィールドからではなく、サーバから直接取得します。

a.　SCEP CA サーバを識別するための CA URL を指定します。FQDN または IP アドレスを入力します 例：**http://ca01.cisco.com/certsrv/mscep/mscep.dll**。

b.　（任意）ユーザに対して、そのユーザ名および 1 回限定利用のパスワードに関するプロンプトを表示する場合は、[チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにします。

c.　（任意）CA 証明書のサムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します （8475B661202E3414D4BB223A464E6AAB8CA123AB など）。

ステップ 7　登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの [証明書の登録（Certificate Enrollment）]」（P.3-83）を参照してください。

（注）　%machineid% を使用した場合は、クライアントに Hostscan/Posture がロードされます。

ステップ 8　（任意）[証明書取得ボタンを表示（Display Get Certificate Button）] をオンして、認証証明書のプロビジョニングや更新をユーザが手動で行えるようにします。このボタンは、証明書認証が失敗した場合に表示されます。

ステップ 9　（任意）サーバ リストで特定のホストに対して SCEP を有効にします。これにより、前述の証明書登録のペインの SCEP の設定を上書きします。

a. 左にある AnyConnect クライアント プロファイル ツリーの [**サーバ リスト（Server List）**] をクリックして、[サーバ リスト（Server List）] ペインに移動します。

b. **サーバ リスト エントリを追加**または**編集**します。

c. ステップ 5 と 6 の説明に従って、自動 SCEP のホストと認証局の属性を指定します。

レガシー SCEP 登録をサポートするための ASA の設定

ASA のレガシー SCEP 用に、接続プロファイルとグループ ポリシーを証明書登録向けに作成し、2 番目の接続プロファイルとグループ ポリシーを認証された VPN 接続用に作成する必要があります。

前提条件

レガシー SCEP 用のクライアント プロファイル（例：ac_vpn__legacy_scep）を設定します 「レガシー SCEP 登録用 VPN クライアント プロファイルの設定」（P.3-43）を参照してください。

ステップ 1　登録用のグループ ポリシー（例：cert_enroll_group）を作成します。次のフィールドを設定します。

- [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアント プロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、レガシー SCEP 用に設定されたクライアント プロファイルを指定します。　たとえば、ac_vpn_legacy_scep クライアント プロファイルを指定します。

ステップ 2　認証用の 2 つ目のグループ ポリシー（例：cert_auth_group）を作成します。

ステップ 3　登録用の接続プロファイル（例：cert_enroll_tunnel）を作成します。次のフィールドを設定します。

- [基本（Basic）] ペインで、AAA の認証方式を設定します。
- [基本（Basic）] ペインで、cert_enroll_group にデフォルトのグループ ポリシーを設定します。
- [詳細（Advanced）] > [グループエイリアス / グループ URL（GroupAlias/Group URL）] で、この接続プロファイルの登録グループ（cert_enroll_group）が含まれるグループ URL を作成します。
- ASA ではこの接続プロファイルをイネーブルにしないでください。ユーザにグループを公開しなくても、ユーザはグループにアクセスできます。

ステップ 4　認証用の接続プロファイル（例：cert_auth_tunnel）を作成します。次のフィールドを設定します。

- [基本（Basic）] ペインで、証明書の認証方式を設定します。
- [基本（Basic）] ペインで、cert_auth_group にデフォルトのグループ ポリシーを設定します。
- ASA ではこの接続プロファイルをイネーブルにしないでください。ユーザにグループを公開しなくても、ユーザはグループにアクセスできます。

ステップ 5　（任意）各グループ ポリシーの [一般（General）] ペインで、対応する SCEP 接続プロファイルに [接続プロファイル（トンネル グループ）ロック（Connection Profile (Tunnel Group) Lock）] を設定します。これにより、SCEP が設定された接続プロファイルへのトラフィックが制限されます。

証明書の失効通知の設定

これらの認証証明書の期限が発生したユーザに警告するため、AnyConnect を設定します。[証明書失効しきい値（Certificate Expiration Threshold）] の設定では、AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを指定します。AnyConnect は、証明書が実際に期限切れか、新しい証明書が取得されるまで、ユーザが接続するたびに警告します。

（注）　RADIUS 登録では、[証明書失効しきい値（Certificate Expiration Threshold）] 機能は使用できません。

ステップ 1　ASDM からプロファイル エディタを起動するか、またはスタンドアロンの VPN プロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ASDM では、[追加（Add）]（または [編集（Edit）] をクリックして、AnyConnect プロファイルを作成（または編集）します。スタンドアロン エディタでは、既存のプロファイルを開くか、新しいプロファイルの作成を続行します。

ステップ 3　左側の [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ツリーで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 4　[証明書の登録（Certificate Enrollment）] ペインで、[証明書の登録（Certificate Enrollment）] をオンにします。

ステップ 5　証明書**失効しきい値**を指定します。

AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかの数字です。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 6　[OK] をクリックします。

証明書ストアの設定

AnyConnect がローカル ホスト上で証明書を格納し、処理する方法を設定できます。プラットフォームによっては、特定ストアへのアクセスが制限される場合や、ブラウザ ベースのストアの代わりにファイルを使用できる場合があります。この目的は、クライアント証明書の使用だけでなく、サーバ証明書の確認のための適切な場所に AnyConnect を振り向けることです。

Windows では、クライアントがどの証明書ストアで証明書を検索するかを制御できます。証明書の検索をユーザ ストアのみ、またはマシン ストアのみに制限するようにクライアントを設定できます。Mac および Linux では、PEM 形式の証明書ファイル用の証明書ストアを作成できます。

これらの証明書ストアの検索設定は、AnyConnect クライアント プロファイルに格納されます。

（注）　また、AnyConnect ローカル ポリシーに、さらに証明書ストアの制約を設定できます。AnyConnect ローカル ポリシーは、企業のソフトウェア展開システムを使用して展開する XML ファイルであり、AnyConnect クライアント ファイルからは独立しています。ファイル内の設定により、Firefox NSS (Linux と Mac)、PEM ファイル、Mac ネイティブ（キーチェーン）、および Windows Internet Explorer ネイティブ証明書ストアの使用が制限されます。詳細については、第 8 章「FIPS と追加セキュリティのイネーブル化」を参照してください。

ここでは、証明書ストアを設定し、その使用を制御する手順について説明します。

- 「Windows での証明書ストアの制御」（P.3-46）
- 「Mac および Linux での PEM 証明書ストアの作成」（P.3-48）

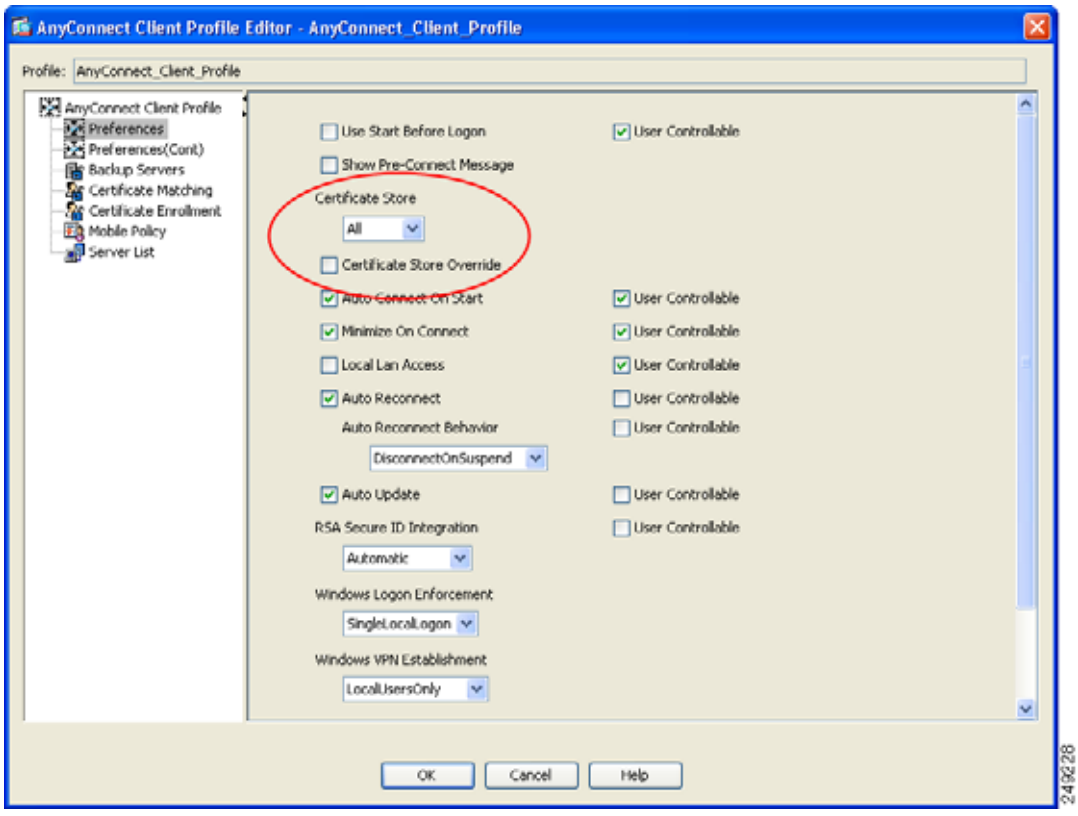
Windows での証明書ストアの制御

Windows では、ローカル マシン用の証明書ストアと現在のユーザ用の証明書ストアが別々に用意されます。プロファイル エディタを使用すると、AnyConnect クライアントがどの証明書ストアで証明書を検索するかを指定できます。

コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。

AnyConnect がどの証明書ストアで証明書を検索するかは、プロファイル エディタの [プリファレンス（Preferences）] ペインにある [証明書ストア（Certificate Store）] リスト ボックスを使用して設定します。[証明書ストアの上書き（Certificate Store Override）] チェックボックスを使用すると、AnyConnect では非管理者権限を持つユーザでもマシン証明書ストアを検索できるようになります。

図 3-15　[証明書ストア（Certificate Store）] リスト ボックスと [証明書ストアの上書き（Certificate Store Override）] チェックボックス



[証明書ストア（Certificate Store）] は次の 3 つの設定が可能です。

- [すべて（All）]：（デフォルト）すべての証明書ストアを検索します。
- [マシン（Machine）]：マシン証明書ストア（コンピュータで識別された証明書）を検索します。

- [ユーザ（User）]：ユーザ証明書ストアを検索します。

[証明書ストアの上書き（Certificate Store Override）] は次の 2 つの設定が可能です。

- オン：ユーザが管理者権限を持っていない場合でも、AnyConnect は、コンピュータのマシン証明書ストアを検索できます。
- オフ：（デフォルト）AnyConnect は、管理者権限のないユーザのマシン証明書ストアを検索できません。

図 3-15 は、[証明書ストア（Certificate Store）] および [証明書ストアの上書き（Certificate Store Override）] の設定例を示したものです。

表 3-4　証明書ストアと証明書ストア上書き設定の例

[証明書ストア（Certificate Store）] の設定	[証明書ストアの上書き（Certificate Store Override）] の設定	AnyConnect の処理
すべて（All）	オフ	AnyConnect は、すべての証明書ストアを検索します。ユーザが非管理者権限を持っている場合、AnyConnect は、マシン ストアにアクセスできません。 これがデフォルトの設定です。ほとんどの場合、この設定が適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
すべて（All）	オン	AnyConnect は、すべての証明書ストアを検索します。ユーザが管理者以外の権限を持っている場合、AnyConnect は、マシン ストアにアクセスできます。
マシン（Machine）	オン	AnyConnect は、マシン証明書ストアを検索します。AnyConnect は、非管理者アカウントのマシン ストアを検索することができます。
マシン（Machine）	オフ	AnyConnect は、マシン証明書ストアを検索します。ユーザが管理者以外の権限を持っている場合、AnyConnect は、マシン ストアを検索できません。 **（注）** 証明書を使用する認証が限定されたユーザのグループにのみ許可されている場合、この設定が使用される場合があります。
ユーザ（User）	適用されない	AnyConnect は、ユーザ証明書ストア内のみ検索します。非管理者アカウントがこの証明書ストアにアクセス権を持つため、証明書ストアの上書きは適用されません。

AnyConnect クライアントがどの証明書ストアで証明書を検索するかを指定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Preferences）] ペインをクリックし、ドロップダウン リストから証明書ストアのタイプを選択します。

- [すべて（All）]：（デフォルト）すべての証明書ストアを検索します。

- [マシン（Machine）]：マシン証明書ストア（コンピュータで識別された証明書）を検索します。
- [ユーザ（User）]：ユーザ証明書ストアを検索します。

ステップ 3　ユーザが非管理者アカウントを持つ場合は、AnyConnect クライアントがマシン証明書ストアにアクセスできるようにするため、[証明書ストアの上書き（Certificate Store Override）] チェックボックスをオンまたはオフにします。

ステップ 4　[OK] をクリックします。

Mac および Linux での PEM 証明書ストアの作成

AnyConnect は、Privacy Enhanced Mail（PEM）形式のファイル ストアを使用した証明書認証をサポートしています。ブラウザに依存して証明書の確認および署名を行う代わりに、クライアントがリモート コンピュータのファイル システムから PEM 形式の証明書ファイルを読み取り、確認と署名を行います。

PEM ファイルのファイル名に関する制約事項

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子 **.pem** で終わっていること。
- すべての秘密キー ファイルは、拡張子 **.key** で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること（client.pem と client.key など）。

（注）　PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

ユーザ証明書の保存

PEM ファイル証明書ストアを作成する場合は、表 3-5 に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

表 3-5　PEM ファイル証明書ストアのフォルダと保存される証明書のタイプ

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca[1]	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

1. ~ は、ホーム ディレクトリを表します。

（注）　マシン証明書の要件は、PEM ファイル証明書の要件と同じですが、ルート ディレクトリが異なります。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外は、表 3-5 に示すパス、フォルダ、および証明書のタイプが適用されます。

証明書照合の設定

AnyConnect は、次の証明書照合タイプをサポートしています。これらの一部またはすべてを使用して、クライアント証明書を照合できます。証明書照合は、AnyConnect プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- キーの用途
- キーの拡張用途
- 識別名

証明書キーの用途による照合

証明書キーの用途は、ある特定の証明書で実行可能な幅広い操作に対する制約のセットとして与えられます。サポートされるセットは次のとおりです。

- DIGITAL_SIGNATURE
- NON_REPUDIATION
- KEY_ENCIPHERMENT
- DATA_ENCIPHERMENT
- KEY_AGREEMENT
- KEY_CERT_SIGN
- CRL_SIGN
- ENCIPHER_ONLY
- DECIPHER_ONLY

プロファイルには、0 個以上の一致基準を含めることができます。1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

「証明書照合の例」（P.3-52）の例には、これらの属性を設定する方法が記載されています。

証明書キーの拡張用途による照合

この照合では、*Extended Key Usage* フィールドに基づいて、クライアントが使用できる証明書を管理者が制限できます。表 3-6 は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

表 3-6　証明書キーの拡張用途

制約	OID
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

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。プロファイルには、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。

証明書の識別名による照合

証明書識別名マッピング機能によって、管理者は、クライアントが使用できる証明書を特定の基準および基準照合条件に一致する証明書に制限できます。表 3-7 は、サポートされる基準をリストにまとめたものです。

表 3-7　証明書の識別名による照合の基準

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState

表 3-7　証明書の識別名による照合の基準 （続き）

ID	説明
CN	SubjectCommonName
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

プロファイルには、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。*識別名*による照合によって、追加の照合基準が提供されます。たとえば、管理者が、指定した文字列が証明書に含まれている必要があるか、含まれていてはいけないかを指定できます。また、文字列のワイルドカードも使用できます。

デフォルトの証明書照合

クライアント証明書は、AnyConnect で使用するために一致する有効な、非期限切れの証明書である必要があります。

証明書の一致基準が [証明書照合（Certificate Matching）] ペインで指定されていない場合、AnyConnect は暗黙的に次の証明書照合ルールを適用します。

- キーの用途：DIGITAL_SIGNATURE
- キーの拡張用途：Client Auth (1.3.6.1.5.5.7.3.2)

他のキーの用途またはキーの拡張用途基準がクライアント認証で指定される場合、これらの仕様も照合するためにクライアント証明書で指定する必要があります。

証明書照合の例

（注）　これ以降の例で使用する KeyUsage、ExtendedKeyUsage、および DistinguishedName のプロファイル値はあくまでも例です。証明書一致基準は、使用する証明書に適用するもののみ設定してください。

クライアント プロファイルで証明書照合を設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[証明書照合（Certificate Matching）] ペインに移動します。

ステップ 3　[キーの用途（Key Usage）] および [キーの拡張用途（Extended Key Usage）] の設定をオンにし、受け入れ可能なクライアント証明書を選択します。指定されたキーの少なくとも 1 つが一致する証明書が選択されます。これらの用途設定に関する詳細については、「AnyConnect プロファイル エディタの [証明書照合（Certificate Matching）]」（P.3-81）を参照してください。

ステップ 4　カスタム拡張照合キーを指定します。これらは、1.3.6.1.5.5.7.3.11 など既知の MIB OID 値であることが必要です。0 個以上のカスタム拡張照合キーを指定することができます。指定されたすべてのキーが一致する証明書が選択されます。キーは、OID 形式であることが必要です （1.3.6.1.5.5.7.3.11 など）。

ステップ 5　[識別名（Distinguished Names）] テーブルの横にある [追加（Add）] をクリックして、[識別名エントリ（Distinguished Name Entry）] ウィンドウを起動します。

- [名前（Name）] : 識別名。
- [パターン（Pattern）] : 照合に使用する文字列。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）] : 照合を実行する際に使用する演算子。
  - [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）] : ワイルドカード パターン照合を使用します。この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する（Match Case）] : 有効にすると、大文字と小文字を区別したパターン照合を実行できます。

認証証明書選択のプロンプト

ユーザに対して有効な証明書のリストを表示し、セッションに認証に使用する証明書をユーザが選択できるように AnyConnect の設定を行うことができます。この設定は、Windows 7、Windows Vista、および Windows XP でのみ行うことができます。デフォルトの場合、ユーザの証明書選択は無効です。証明書の選択をイネーブルにするには、AnyConnect プロファイルで次の作業を実行します。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

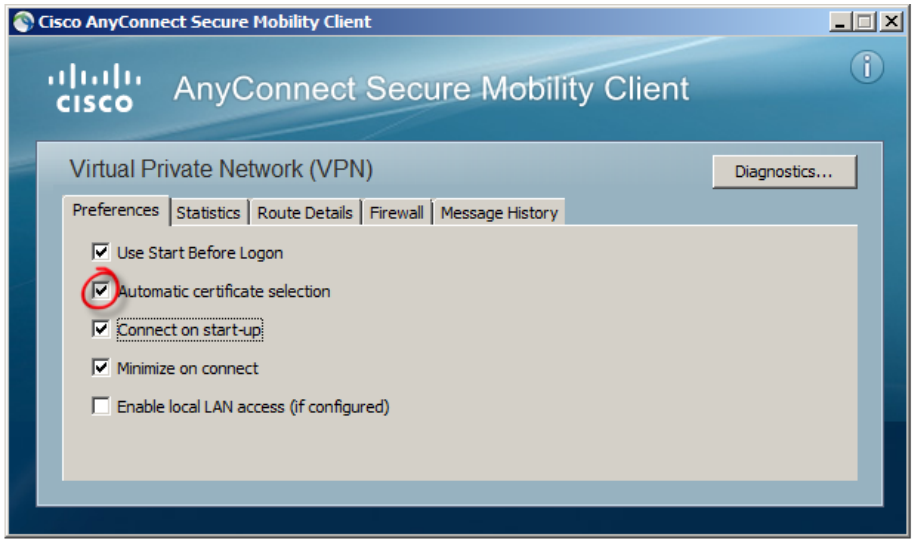
ステップ 2　[プリファレンス（Part 2）（Preferences (Part 2)）] ペインに移動し、[証明書選択を無効にする（Disable Certificate Selection）] をオフにします。これによりクライアントでは、ユーザに対して認証証明書を選択するためのプロンプトが表示されます。

ユーザによる AnyConnect プリファレンスでの自動証明書選択の設定

ユーザの証明書選択を有効にすると、AnyConnect の [プリファレンス（Preferences）] ダイアログ ボックスに、[証明書の自動選択（Automatic certificate selection）] チェックボックスが表示されます。ユーザは、[証明書の自動選択（Automatic certificate selection）] チェックボックスをオンまたはオフにすることで、自動証明書選択をオンまたはオフにできます。

図 3-16 は、[証明書の自動選択（Automatic Certificate Selection）] チェックボックスが表示された [プリファレンス（Preferences）] ウィンドウです。

図 3-16　[証明書の自動選択（Automatic Certificate Selection）] チェックボックス



サーバ リストの設定

プロファイルの主要な使用目的の 1 つは、ユーザが接続サーバをリストできるようにすることです。このサーバ リストは、ホスト名とホスト アドレスのペアで構成されています。ホスト名は、ホストを参照するために使用するエイリアスのほか、FQDN、または IP アドレスにできます。サーバ リストには、AnyConnect GUI の [接続先（Connect to）] ドロップダウン リストにあるサーバのホスト名が表示されます。ユーザはこのリストからサーバを選択できます。

図 3-17　[接続先（Connect to）] ドロップダウン リストにホストが表示されたユーザ GUI

最初は、リストの先頭にある設定したホストがデフォルト サーバとなり、GUI ドロップダウン リスト

に表示されます。ユーザがリストから別のサーバを選択すると、クライアントではその選択内容がリモート コンピュータ上のユーザ プリファレンス ファイルに記録され、選択されたサーバが新たなデフォルト サーバとなります。

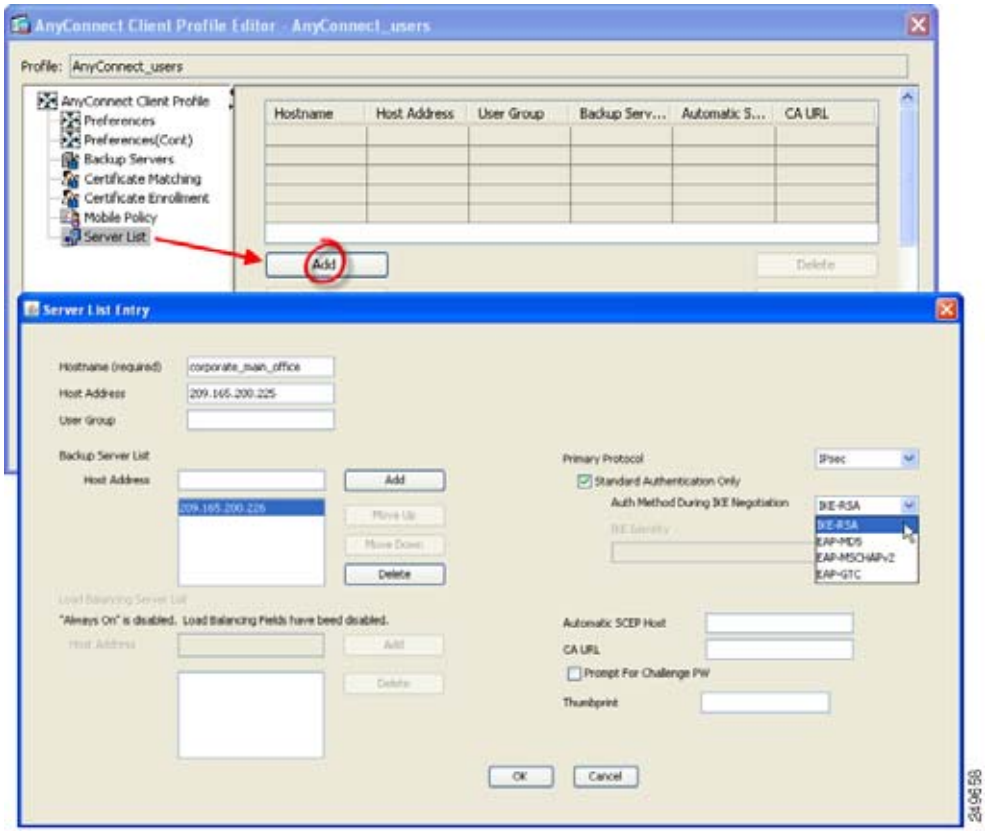
サーバ リストを設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[サーバ リスト（Server List）] をクリックします。[サーバ リスト（Server List）] ペインが開きます。

ステップ 3　[追加（Add）] をクリックします。[サーバ リスト エントリ（Server List Entry）] ウィンドウが開きます（図 3-21）。

図 3-18　サーバ リストの追加



ステップ 4　ホスト名を入力します。ホスト名は、ホストを参照するために使用するエイリアスのほか、FQDN、または IP アドレスにできます。FQDN または IP アドレスを入力した場合、ホスト アドレスを入力する必要はありません。

ステップ 5　必要に応じてホスト アドレスを入力します。

ステップ 6　ユーザ グループを指定します（任意）。クライアントでは、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。

（注）　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。

ステップ 7　（AnyConnect リリース 3.0.1047 以降の場合）。モバイルデバイス用のサーバ リストを設定するには、[追加のモバイル専用設定（Additional mobile-only settings）] チェックボックスをオンにして、[編集（Edit）] をクリックします。詳細については、「サーバ リストの設定」のモバイル デバイス用の設定についての説明を参照してください。

ステップ 8　バックアップ サーバを追加します（任意）。サーバ リスト内のサーバが使用できない場合、クライアントではグローバル バックアップ サーバ リストを使用する前に、そのサーバのバックアップ リストにあるサーバへの接続が試行されます。

ステップ 9　ロード バランシング バックアップ サーバを追加します（任意）。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、かつ常時接続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常時接続機能によりブロックされます。

ステップ 10　この ASA に対して使用するクライアントのプライマリ プロトコル（SSL または IKEv2 を使用した IPsec）を指定します（任意）。デフォルトは SSL です。デフォルトの認証方式（独自の AnyConnect EAP 方式）をディセーブルにするには、[標準認証のみ（Standard Authentication Only）] をオンにし、ドロップダウン リストから方式を選択します。

（注）　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。

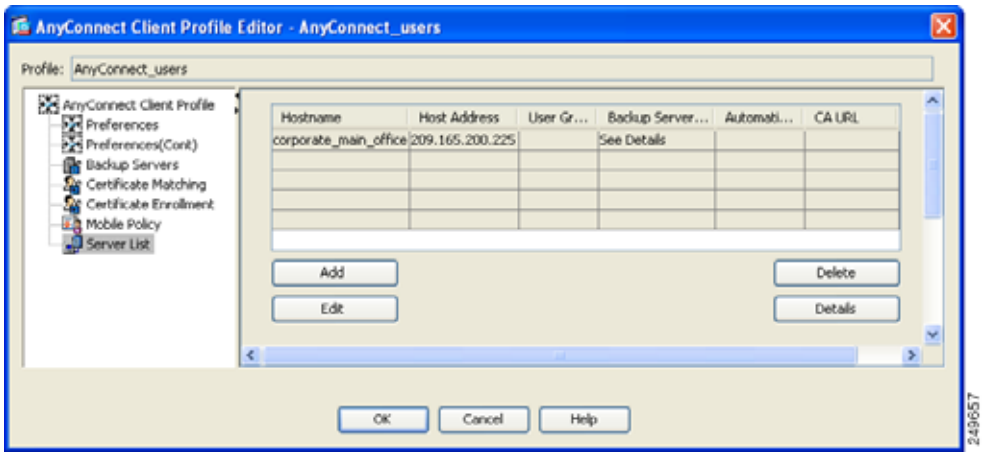
ステップ 11　SCEP CA サーバの URL を指定します（任意）。FQDN または IP アドレスを入力します（http://ca01.cisco.com など）。

ステップ 12　[チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにして（任意）、ユーザが証明書を手動で要求できるようにします。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。

ステップ 13　CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します 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、発行した証明書の「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。

ステップ 14　[OK] をクリックします。設定した新規のサーバ リスト エントリが、サーバ リスト テーブルに表示されます。

図 3-19　新規のサーバ リスト エントリ



モバイル デバイス用接続設定

前提条件

- 「サーバ リストの設定」（P.3-54）のステップ 1 ～ 6 を実行します。
- バージョン 3.0.1047 以降のプロファイル エディタを使用する必要があります。
- Apple iOS バージョン 4.1 以降を実行する Apple モバイルデバイスでサポートされます。

ガイドライン

ASA からモバイルデバイスに配信された AnyConnect VPN クライアント プロファイルは、再設定したり、モバイルデバイスから削除したりすることはできません。ユーザが、新しい VPN 接続用にデバイス上で独自のクライアント プロファイルを作成した場合は、そのプロファイルを設定、編集、削除できます。

手順の詳細

ステップ 1　[サーバ リスト エントリ（Server List Entry）] ダイアログボックスで、[追加のモバイル専用設定（Additional mobile-only settings）] をオンにして [編集（Edit）] をクリックします。

ステップ 2　[Apple iOS / Android の設定（Apple iOS / Android Settings）] エリアでは、Apple iOS または Android オペレーティング システムを実行するデバイスに、次の属性を設定できます。

a. 証明書認証タイプを選択します。

– [自動（Automatic）] : AnyConnect では、認証で使用されるクライアント証明書が自動的に選択されます。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、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、自動認証と同様に認証で使用される証明書を検索します。ただし、手動証明書認証タイプでは、VPN クライアント プロファイルで定義された一致条件に一致する証明書がいったん検出されると、AnyConnect はその証明書を接続用に割り当てます。この場合、ユーザが新しい VPN 接続の確立を試行しても、新しい証明書の検索は行われません。
- [無効（Disabled）] : 認証にクライアント証明書は使用されません。

b. [プロファイルがインポートされた場合、このサーバ リスト エントリをアクティブにする（Make this Server List Entry active when profile is imported）] チェックボックスをオンにした場合、VPN プロファイルがデバイスにダウンロードされたときに、このサーバ リスト エントリをデフォルトの接続として定義したことになります。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。デフォルトではオフになっています。

ステップ 3　[Apple iOS のみの設定（Apple iOS Only Settings）] エリアでは、Apple iOS を実行するデバイスのみに、次の属性を設定できます。

a. [3G/Wifi ネットワーク間でローミングされた場合は再接続（Reconnect when roaming between 3G/Wifi networks）] チェックボックスを設定します。デフォルトではこのボックスはオンになっており、3G ネットワークと Wifi ネットワークの切り替え時に、AnyConnect は VPN 接続を維持するように試行します。このボックスをオフにすると、3G ネットワークと Wifi ネットワークの切り替え時に、AnyConnect は VPN 接続を維持するように試行しません。

b. [オンデマンド接続（Connect on Demand）] チェックボックスを設定します。

このエリアを使用して、Apple iOS から提供される 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、その都度チェックされるルールのリストを作成できます。

[オンデマンド接続（Connect on Demand）] は、[証明書の認証（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のみオンにできます。[証明書の認証（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。

c. [ドメインまたはホストと一致（Match Domain or Host）] フィールドに、Connect on Demand ルールを作成する対象のホスト名（host.example.com）、ドメイン名（.example.com）、または部分ドメイン（.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。

d. [オンデマンド アクション（On Demand Action）] フィールドで、ユーザが前のステップで定義したドメインまたはホストへの接続を試行したときに実行されるアクションを、次のいずれかに指定します。

- [常に接続（Always connect）] : このリストのルールに一致したときに、iOS は必ず VPN 接続の開始を試行します。
- [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 接続の開始を試行します。
- [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 接続の開始を試行しません。[常に接続（Always connect）] または [必要に応じて接続（Connect if needed）] のルールよりも、このリストのルールが優先されます。

  Connect On Demand がイネーブルの場合、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。この動作を望まない場合は、このルールを削除できます。

e. [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）] フィールドを使用してルールを作成したら、[追加（Add）] をクリックします。

このルールが、下部のルール リストに表示されます。

ステップ 4　[OK] をクリックします。

ステップ 5　「サーバ リストの設定」（P.3-54）のステップ 8 に戻ります。

バックアップ サーバ リストの設定

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。これらのサーバは、AnyConnect プロファイルの [バックアップ サーバ（Backup Servers）] ペインで指定します。場合によっては、このリストでホスト固有の設定を指定することがあります。手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[バックアップ サーバ（Backup Servers）] ペインに移動し、バックアップ サーバのホスト アドレスを入力します。

Connect On Start-up の設定

Connect on Start-up は、VPN クライアント プロファイルで指定されたセキュア ゲートウェイを使用して、自動的に VPN 接続を確立します。接続時、クライアントでは、セキュア ゲートウェイから提供されたプロファイルとローカル プロファイルが同じでない場合、セキュア ゲートウェイから提供されたプロファイルでローカル プロファイルが置き換えられ、このプロファイルの設定が適用されます。

デフォルトでは、Connect on Start-up は**ディセーブル**です。ユーザが AnyConnect クライアントを起動すると、GUI にはユーザ制御可能設定としてデフォルトの設定が表示されます。ユーザは、GUI の [接続先（Connect to）] ドロップダウン リストでセキュア ゲートウェイの名前を選択し、[接続（Connect）] をクリックする必要があります。接続時、クライアントでは、セキュリティ アプライアンスから提供されたクライアント プロファイルの設定が適用されます。

AnyConnect は、AnyConnect の起動時に自動的に VPN 接続を確立する機能から、ログイン後の常時接続機能により、その VPN 接続を「常時接続」にする機能に進化しました。Connect on Start-up 要素のデフォルトがディセーブルになっているのは、この進化を反映しているためです。企業の展開で Connect on Start-up 機能を使用している場合は、この代わりに Trusted Network Detection を使用することを検討してください。

Trusted Network Detection（TND）を使用すると、ユーザが企業ネットワークの中（信頼ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、企業ネットワークの外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。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。Trusted Network Detection の設定の詳細については、「Trusted Network Detection」（P.3-17）を参照してください。

デフォルトでは、Connect on Start-up はディセーブルです。有効にするには、次の手順に従います。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ナビゲーション ペインで [プリファレンス（Preferences）] を選択します。

ステップ 3　[起動時に接続（Connect On Start-up）] をオンにします。

自動再接続の設定

IPsec VPN クライアントとは異なり、AnyConnect は、初期接続に使用したメディアによらず、VPN セッションの中断から復旧することおよびセッションを再確立することができます。たとえば、有線、ワイヤレス、または 3G のセッションを再確立できます。

自動再接続機能を設定すると、接続が解除された場合に VPN 接続の再確立が試行されます（デフォルトの動作）。また、*システムの一時停止*または*システムのレジューム*が発生して以降に接続の動作を定義することもできます。システムの一時停止とは、低電力スタンバイ、Windows の「休止状態」、Mac OS または Linux の「スリープ」のことです。システムのレジュームとは、システムの一時停止からの回復です。

（注）　AnyConnect 2.3 よりも前までは、システムの一時停止に対するデフォルトの動作として、VPN セッションに割り当てられたリソースを保持し、システムのレジューム後に VPN 接続を再確立していました。この動作を維持する場合は、自動再接続の動作として [*再開後に再接続（Reconnect After Resume）*] を有効にします。

クライアント プロファイルで [自動再接続（Auto Reconnect）] の設定を行う手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ナビゲーション ペインで [プリファレンス（Preferences）] を選択します。

ステップ 3　[自動再接続（Auto Reconnect）] をオンにします。

（注）　[*自動再接続（Auto Reconnect）*] をオフにすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。

ステップ 4　自動再接続の動作を選択します（Linux ではサポートされていません）。

- [中断時に接続解除（Disconnect On Suspend）]：AnyConnect では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
- [再開後に再接続（Reconnect After Resume）]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムのレジューム後は再接続が試行されます。

ローカル プロキシ接続

デフォルトでは、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を介して VPN セッションを確立するようになっています。

次に示すのは、透過的なプロキシ サービスを実現する要素の一例です。

- 一部のワイヤレス データ カードから入手できるアクセラレーション ソフトウェア
- Kaspersky など一部のアンチウイルス ソフトウェア上のネットワーク コンポーネント

ローカル プロキシ接続に関する要件

AnyConnect は、次の Microsoft OS 上でこの機能をサポートしています。

- Windows 7（32 ビットおよび 64 ビット）
- Windows Vista（32 ビットおよび 64 ビット）SP2 または KB952876 を適用した Vista Service Pack 1
- Windows XP SP2 および SP3

この機能をサポートするためには、AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのどちらかが必要です。

ローカル プロキシ接続の設定

AnyConnect は、VPN セッションを確立するためのローカル プロキシ サービスをデフォルトでサポートしています。AnyConnect によるローカル プロキシ サービスのサポートを無効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ナビゲーション ペインで [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 3　パネル上部付近にある [ローカルプロキシ接続を許可（Allow Local Proxy Connections）] をオフにします。

最適ゲートウェイ選択

最適ゲートウェイ選択（OGS）機能を使用すると、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 を使用すると、AnyConnect では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。OGS は、初回接続時または、直前の接続解除から 4 時間以上経過した後の再接続時に開始されます。

最良のパフォーマンスを実現するために、遠隔地に移動するユーザは、移動先の場所に一番近いセキュア ゲートウェイに接続します。自宅と会社では同じゲートウェイからほぼ同じ結果が得られるため、このような事例では通常セキュア ゲートウェイの切り替えは行われません。別のセキュア ゲートウェイへの接続が行われることはほとんどなく、行われるとしてもパフォーマンスの向上率が 20 % 以上の場合に限られます。

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。オプションで、エンド ユーザがこの機能の有効化/無効化を切り替えられるようにすることができます。

最小ラウンド トリップ時間（RTT）ソリューションでは、クライアントと他のすべてのゲートウェイとの間で RTT が最短となるセキュア ゲートウェイが選択されます。クライアントでは、経過時間が 4 時間以内の場合は常に、最後のセキュア ゲートウェイに対して再接続が行われます。ネットワーク接続の負荷やその状態の一時的変動といった要素は、インターネット トラフィックの遅延だけでなく、選択プロセスにも影響を与える場合があります。

OGS は、RTT の結果のキャッシュを維持して、その後実行する必要のある測定の数を最小限に抑えます。OGS をイネーブルにして AnyConnect を起動すると、OGS はネットワーク情報（DNS サフィックス、DNS サーバ IP など）を取得してユーザの位置を特定します。RTT の結果は、特定した場所と一緒に OGS キャッシュに保存されます。その後 14 日間は、AC が再起動されるたびに同じ方法で場所が特定され、すでに RTT の結果が存在するかどうかが解読されます。ヘッドエンドはキャッシュに基づいて選択されるため、ヘッドエンドの再 RRT は必要ありません。この 14 日間の終了時、この場所はキャッシュから削除され、AC を再起動すると新しい RTT のセットが発生します。

選択プロセスでは、最適なサーバを特定する際プライマリ サーバにのみ問い合わせが行われます。特定後の接続アルゴリズムは次のとおりです。

1. 最適なサーバへの接続を試行する。
2. 失敗した場合は、最適なサーバのバックアップ サーバ リストに対して試行する。
3. 失敗した場合は、選択結果に応じて OGS 選択リストに残っている各サーバに対して試行する。

バックアップ サーバの詳細については、「AnyConnect プロファイル エディタの [バックアップ サーバ（Backup Servers）]」（P.3-81）を参照してください。

最適ゲートウェイ選択に関する要件

AnyConnect は、次の OS が実行されている VPN エンドポイントをサポートしています。

- Windows 7、Vista、および XP
- Mac OS X 10.5 および Mac OS X 10.6

最適ゲートウェイ選択の設定

OGS のアクティブ化/非アクティブ化の制御や、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の指定は、AnyConnect プロファイルで行います。プロファイル エディタを使用して OGS を設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）] チェックボックスをオンにして、OGS をアクティブ化します。

ステップ 3　[ユーザ制御可（User Controllable）] チェックボックスをオンにして、クライアント GUI にアクセスするリモート ユーザが OGS の設定を行えるようにします。

（注） 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 により選択されたゲートウェイへの接続が AnyConnect クライアントによって確立できないときには、ユーザがプロファイルから別のゲートウェイを選択できることが必要となる場合があります。

ステップ 4　VPN が一時停止してから、ゲートウェイを選択するための新たな計算が開始されるまでに要する最小の時間（単位は時間）を、[中断時間しきい値（Suspension Time Threshold）] パラメータに入力します。デフォルトは 4 時間です。

（注） このしきい値は、プロファイル エディタを使用して設定できます。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。

ステップ 5　システムのレジューム後にクライアントから別のセキュア ゲートウェイへの再接続が行われるために必要なパフォーマンスの向上率を、[パフォーマンス向上しきい値（Performance Improvement Threshold）] パラメータに入力します。デフォルトは 20 % です。

（注） 移行の発生回数が多く、ユーザがクレデンシャルを頻繁に再入力しなければならないような場合は、これらのしきい値の一方または両方を大きくしてください。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。

クライアント GUI の起動時に OGS がイネーブルになっている場合は、[VPN：接続する準備ができました（VPN: Ready to connect）] パネルの [接続（Connect）] ボタンの横に [自動選択（Automatic Selection）] が表示されます。この選択は変更できません。OGS を使用すると、最適なセキュア ゲートウェイが自動的に選択され、ステータス バーにその選択されたゲートウェイが表示されます。接続プロセスを開始するためには、[選択（Select）] をクリックすることが必要となる場合もあります。

この機能の設定をユーザが行えるようにした場合、選択されたセキュア ゲートウェイをユーザが手動で上書きすることができます。手順は次のとおりです。

ステップ 1　現在接続中の場合は、[接続解除（Disconnect）] をクリックします。

ステップ 2　[詳細（Advanced）] をクリックします。

ステップ 3　[プリファレンス（Preferences）] タブを開き、[最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）] をオフにします。

ステップ 4　目的のセキュア ゲートウェイを選択します。

（注） AAA が使用されている場合は、別のセキュア ゲートウェイへの移行時にエンド 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。証明書を使用していれば、その必要はありません。

OGS とスリープ モード

エンドポイントがスリープ モードまたはハイバネーション モードに移行するときは、AnyConnect では接続が確立されているはずです。ASDM のプロファイル エディタ（[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）]）の AutoReconnect（ReconnectAfterResume）設定をイネーブルにする必要があります。これをユーザ制御可能にした場合、デバイスをスリープにする前に AnyConnect Secure Mobility Client の [プリファレンス（Preferences）] タブで設定できます。両方を設定すると、デバイスがスリープから復帰したときに、AC は再接続試行用に選択したヘッドエンドを使用して、自動的に OGS を実行します。

OGS とプロキシ検出

自動プロキシ検出が設定されている場合は、OGS は実行できません。また、プロキシ自動設定（PAC）ファイルを設定した状態でも、動作しません。

スクリプトの作成および展開

AnyConnect では、次のイベントが発生したときに、スクリプトをダウンロードして実行できます。

- セキュリティ アプライアンスで新しいクライアント VPN セッションが確立された。このイベントによって起動するスクリプトを *OnConnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。
- セキュリティ アプライアンスでクライアント VPN セッションが切断された。このイベントによって起動するスクリプトを *OnDisconnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。

これにより、Trusted Network Detection によって開始された新しいクライアント VPN セッションが確立すると、OnConnect スクリプトが起動します（このスクリプトを実行する要件が満たされている場合）。ネットワーク切断後に永続的な VPN セッションが再接続されても、OnConnect スクリプトは起動しません。

この機能には次のような使用例があります。

- VPN 接続時にグループ ポリシーを更新する。
- VPN 接続時にネットワーク ドライブをマッピングし、接続解除後にマッピングを解除する。
- VPN 接続時にサービスにログインし、接続解除後にログオフする。

AnyConnect は、WebLaunch の起動中およびスタンドアロン起動中でのスクリプトの起動をサポートしています。

ここでの説明は、スクリプトの作成方法と、ターゲット エンドポイントのコマンドラインからスクリプトを実行し、テストする方法についての知識があることを前提としています。

（注） AnyConnect のソフトウェア ダウンロード サイトでは、サンプル スクリプトがいくつか提供されています。これらを確認する場合は、単なるサンプルであることに留意してください。これらのサンプル スクリプトは、スクリプトを実行するために必要なローカル コンピュータの要件を満たしていない場合があります。また、ご使用のネットワークおよびユーザのニーズに応じてカスタマイズしてからでないと使用できません。シスコでは、サンプル スクリプトまたはユーザ作成スクリプトはサポートしていません。

ここでは、次の内容について説明します。

スクリプトの要件と制限

次のスクリプトの要件と制限事項に留意してください。

サポートされるスクリプトの数

AnyConnect は、1 つの OnConnect スクリプトおよび 1 つの OnDisconnect スクリプトのみを実行します。ただし、これらのスクリプトが別のスクリプトを起動する場合があります。

ファイル形式

AnyConnect は、ファイル名で OnConnect および onDisconnect スクリプトを識別します。また、ファイルの拡張子に関係なく、OnConnect または OnDisconnect で始まるファイルを検索します。照合プレフィックスに関連する最初のスクリプトが実行されます。解釈されたスクリプト（VBS、Perl、Bash など）または実行可能ファイルを認識します。

スクリプト言語

クライアントでは、スクリプトを特定の言語で作成する必要はありません。ただし、スクリプトを実行可能なアプリケーションが、クライアント コンピュータにインストールされている必要があります。クライアントでスクリプトを起動するためには、このスクリプトがコマンドラインから実行可能であることが必要です。

Windows セキュリティ環境によるスクリプトの制限

Microsoft Windows 上の AnyConnect では、ユーザが Windows にログインして VPN セッションを確立した後でないと、スクリプトを起動できません。そのため、ユーザのセキュリティ環境に伴う制限が、これらのスクリプトに適用されます。スクリプトが実行できる機能は、ユーザが起動権限を持つ機能に限られます。AnyConnect は、Windows でスクリプトを実行中は CMD ウィンドウを非表示にします。したがって、テストの目的で、.bat ファイル内のメッセージを表示するスクリプトを実行しても機能しません。

スクリプトのイネーブル化

デフォルトでは、クライアントによってスクリプトが起動することはありません。AnyConnect プロファイルの EnableScripting パラメータを使用して、スクリプトを有効にしてください。これにより、クライアントではスクリプトが存在する必要がなくなります。

クライアント GUI の終了

クライアント GUI を終了しても、必ずしも VPN セッションは終了しません。OnDisconnect スクリプトは、セッションが終了した後で実行されます。

64 ビット Windows でのスクリプトの実行

AnyConnect クライアントは、32 ビット アプリケーションです。Windows 7 x64 および Windows Vista SP2 x64 などの 64 ビット Windows バージョンで動作させる場合は、バッチ スクリプトを実行するときに、32 ビット バージョンの cmd.exe を使用します。

32 ビットの cmd.exe では、64 ビットの cmd.exe でサポートされているコマンドの一部が欠けているため、一部のスクリプトについては、サポートされていないコマンドの実行を試行したときにスクリプトの実行が停止したり、一部実行されてから停止したりする場合があります。たとえば、64 ビットの cmd.exe でサポートされている **msg** コマンドは、32 ビット バージョンの Windows 7（%WINDIR%\SysWOW64 に含まれる）では理解されない場合があります。

そのため、スクリプトを作成する場合は、32 ビットの cmd.exe でサポートされているコマンドを使用してください。

スクリプトの作成、テスト、および展開

AnyConnect スクリプトを展開する手順は次のとおりです。

ステップ 1　AnyConnect が起動したスクリプトが実行されるオペレーティング システムのタイプに基づいて、スクリプトの作成とテストを行います。

（注）　Microsoft Windows コンピュータで作成されたスクリプトの行末コードは、Mac OS および Linux で作成されたスクリプトの行末コードとは異なります。そのため、ターゲットのオペレーティング システムでスクリプトを作成し、テストする必要があります。ネイティブ オペレーティング システムのコマンドラインからスクリプトを正しく実行できない場合は、AnyConnect でも正しく実行できません。

ステップ 2　次のいずれかを実行して、スクリプトを展開します。

- ASDM を使用して、スクリプトをバイナリ ファイルとして ASA にインポートします。[ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [スクリプト（Script）] を選択します。

  ASDM バージョン 6.3 以降を使用している場合、ASA では、ファイルをスクリプトとして識別できるように、プレフィックス *scripts_* とプレフィックス *OnConnect* または *OnDisconnect* がユーザのファイル名に追加されます。クライアントが接続すると、セキュリティ アプライアンスは、リモート コンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードし、*scripts_* プレフィックスを削除し、*OnConnect* プレフィックスまたは *OnDisconnect* プレフィックスをそのまま残します。たとえば、*myscript.bat* スクリプトをインポートする場合、スクリプトは、セキュリティ アプライアンス上では *scripts_OnConnect_myscript.bat* となります。リモート コンピュータ上では、スクリプトは *OnConnect_myscript.bat* となります。

  6.3 よりも前の ASDM バージョンを使用している場合には、次のプレフィックスでスクリプトをインポートする必要があります。

  - scripts_OnConnect
  - scripts_OnDisconnect

  スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- 企業のソフトウェア展開システムを使用して、スクリプトを実行する VPN エンドポイントにスクリプトを手動で展開します。

  この方式を使用する場合は、次のファイル名プレフィックスを使用します。

  - OnConnect

– OnDisconnect

表 3-8 に示すディレクトリにスクリプトをインストールします。

表 3-8　スクリプトの所定の場所

OS	ディレクトリ
Microsoft Windows 7 および Microsoft Vista	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Microsoft Windows XP	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Script
Linux （Linux では、User、Group、Other にファイルの実行権限を割り当てます）	/opt/cisco/anyconnect/script
Mac OS X	/opt/cisco/anyconnect/script

スクリプトに関する AnyConnect プロファイルの設定

クライアント プロファイルでスクリプトを有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ナビゲーション ペインで [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 3　[スクリプトの有効化（Enable Scripting）] をオンにします。クライアントでは、VPN 接続の接続時または接続解除時にスクリプトが起動します。

ステップ 4　[ユーザ制御可（User Controllable）] をオンにして、On Connect スクリプトおよび OnDisconnect スクリプトの実行をユーザが有効または無効にすることができるようにします。

ステップ 5　[次のイベント時にスクリプトを終了する（Terminate Script On Next Event）] をオンにして、スクリプト処理可能な別のイベントへの移行が発生した場合に、実行中のスクリプト プロセスをクライアントが終了できるようにします。たとえば、VPN セッションが終了すると、クライアントでは実行中の On Connect スクリプトが終了し、AnyConnect 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。Mac OS 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。

ステップ 6　[Post SBL OnConnect スクリプト有効にする（Enable Post SBL On Connect Script）] をオンにして（デフォルトでオン）、SBL で VPN セッションが確立された場合にクライアントにより OnConnect スクリプトが（存在すれば）起動するようにします。

（注）　必ずクライアント プロファイルを ASA のグループ ポリシーに追加し、それを VPN エンドポイントにダウンロードしてください。

スクリプトのトラブルシューティング

スクリプトの実行に失敗した場合は、次のようにして問題を解決してください。

ステップ 1　スクリプトに、OnConnect または OnDisconnect のプレフィックス名が付いていることを確認します。表 3-8 には、各オペレーティング システムの所定のスクリプト ディレクトリが記載されています。

ステップ 2　スクリプトをコマンドラインから実行してみます。コマンドラインから実行できないスクリプトは、クライアントでも実行できません。コマンドラインでスクリプトの実行に失敗する場合は、スクリプトを実行するアプリケーションがインストールされていることを確認し、そのオペレーティング システムでスクリプトを作成し直してください。

ステップ 3　VPN エンドポイントのスクリプト ディレクトリ内に OnConnect スクリプトと OnDisconnect スクリプトがそれぞれ 1 つだけ存在することを確認します。最初の ASA で OnConnect スクリプトがダウンロードされ、その後の接続で次の ASA により別のファイル名拡張子を持つ OnConnect スクリプトがダウンロードされる、クライアントでは不要なスクリプトが実行される可能性があります。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつスクリプトの展開に ASA を使用している場合は、スクリプト ディレクトリ内のファイルを削除し、VPN セッションを再確立します。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつ手動展開を使用している場合は、不要なスクリプトを削除し、AnyConnect VPN セッションを再確立します。

ステップ 4　オペレーティング システムが Linux の場合は、スクリプト ファイルに実行権限が設定されていることを確認します。

ステップ 5　クライアント プロファイルでスクリプトが有効になっていることを確認します。

認証タイムアウト コントロール

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。次の項の説明に従って、このタイマーの値を変更します。

認証タイムアウト コントロールに関する要件

AnyConnect は、AnyConnect がサポートしているすべての OS 上でこの機能をサポートしています。

この機能をサポートするためには、AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのどちらかが必要です。

認証タイムアウトの設定

AnyConnect が接続の試行を終了しないでセキュア ゲートウェイでの認証を待機している秒数を変更する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　ナビゲーション ペインで [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 3　[認証タイムアウト値（Authentication Timeout Values）] テキスト ボックスに 10 ～ 120 の範囲で秒数を入力します。

プロキシ サポート

ここでは、プロキシ サポート拡張機能の使用方法について説明します。

ブラウザのプロキシ設定を無視するためのクライアントの設定

AnyConnect プロファイルでは、ユーザの PC 上で Microsoft Internet Explorer のプロキシ設定が無視されるようにポリシーを指定できます。これは、プロキシ設定によってユーザが企業ネットワークの外部からトンネルを確立できない場合に役立ちます。

（注）　常時接続機能が有効な場合、プロキシ経由の接続はサポートされません。そのため、常時接続を有効にした場合は、プロキシ設定を無視するようにクライアントを設定する必要はありません。

AnyConnect で Internet Explorer のプロキシ設定が無視されるようにする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Part 2）（Preferences (Part 2)）] ペインに移動します。

ステップ 3　[プロキシ設定（Proxy Settings）] ドロップダウン リストで、[プロキシを無視（Ignore Proxy）] を選択します。[プロキシを無視（Ignore Proxy）] を選択すると、クライアントはすべてのプロキシ設定を無視します。ASA に到達するプロキシには、何のアクションも実行されません。

（注）　AnyConnect では、プロキシの設定として [上書き（Override）] はサポートしていません。

プライベート プロキシ

トンネルを確立した後、グループ ポリシー内に設定されたプライベート プロキシ設定をブラウザにダウンロードするように、グループ ポリシーを設定できます。VPN セッションが終了すると、設定は元の状態に復元されます。

プライベート プロキシの要件

AnyConnect Essentials ライセンスは、この機能の最小 ASA ライセンス アクティブ化要件です。

AnyConnect は、以下が動作するコンピュータ上でこの機能をサポートします。

- Windows 上の Internet Explorer
- Mac OS 上の Safari

グループ ポリシーを設定してプライベート プロキシをダウンロード

プロキシ設定を設定するには、セキュリティ アプライアンスで ASDM セッションを確立し、[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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [ブラウザ プロキシ（Browser Proxy）] の順に選択します。6.3(1) より前の ASDM バージョンでは、このオプションは [IE ブラウザ プロキシ（IE Browser Proxy）] として表示されます。しかし、現在 AnyConnect は、使用する ASDM バージョンに関係なく、プライベート プロキシの設定を Internet Explorer に限定していません。

（注） Mac 環境では、（VPN 接続時に）ASA からプッシュダウンされたプロキシ情報は、ターミナルが開いて「scutil --proxy」を発行するまで、ブラウザで表示されません。

プロキシを使用しないパラメータがイネーブルの場合、セッションの間、ブラウザからプロキシ設定が削除されます。

Internet Explorer の [接続（Connections）] タブのロック

ある条件下では、AnyConnect によって Internet Explorer の [ツール（Tools）] > [インターネット オプション（Internet Options）] > [接続（Connections）] タブが非表示にされます。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックは接続解除すると反転され、このタブに関する管理者定義のポリシーの方が優先されます。このロックは、次のいずれかの条件で行われます。

- ASA の設定で、[接続（Connections）] タブのロックが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。
- Windows のグループ ポリシーにより、以前に [接続（Connections）] タブがロックされている（**no lockdown** ASA グループ ポリシー設定の上書き）。

グループ ポリシーで、ASA がプロキシのロックダウンを許可する、または許可しないように設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

ステップ 1　[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）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[詳細（Advanced）] > [ブラウザ プロキシ（Browser Proxy）] に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4　[Proxy Lockdown] をクリックして、その他のプロキシ設定を表示します。

ステップ 5　プロキシのロックダウンをイネーブルにして、AnyConnect のセッション中は Internet Explorer の [接続（Connections）] タブを非表示にするには、[継承（Inherit）] をオフにして [はい（Yes）] を選択します。または、プロキシのロックダウンをディセーブルにして、AnyConnect のセッション中は Internet Explorer の [接続（Connections）] タブを表示するには、[いいえ（No）] を選択します。

ステップ 6　[OK] をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7　[適用（Apply）] をクリックして、グループ ポリシーの変更を保存します。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

一部のバージョンの ASA では、AnyConnect セッションが確立された後も、プロキシ サーバを経由するクライアントレス ポータル アクセスを許可するために追加の AnyConnect 設定が必要です。AnyConnect では、この設定が行われるように、プロキシ自動設定（PAC）ファイルを使用してクライアント側プロキシ設定が修正されます。AnyConnect でこのファイルが生成されるのは、ASA でプライベート側プロキシ設定が指定されていない場合のみです。

Windows RDP セッションによる VPN セッションの起動

Windows リモート デスクトップ プロトコル（RDP）を使用して、ユーザが Cisco AnyConnect Secure Mobility Client を実行するコンピュータにログインして、RDP セッションからセキュア ゲートウェイへの VPN 接続を作成するように許可できます。この機能が正しく動作するには、スプリット トンネリング VPN 設定が必要です。

デフォルトでは、他のローカル ユーザがログインしていない場合に限り、ローカルにログインしたユーザが VPN 接続を確立できます。ユーザがログアウトすると VPN 接続は終了し、VPN 接続中に別のローカル ログインが行われると接続は切断されます。VPN 接続中のリモート ログインおよびログアウトは制限されません。

（注）　この機能を使用すると、AnyConnect では、VPN 接続を確立したユーザがログオフした時点でその VPN 接続が解除されます。接続がリモート ユーザによって確立された場合は、そのリモート ユーザがログオフした時点で VPN 接続は終了します。

[Windows ログインの強制（Windows Logon Enforcement）] に対しては次の設定を使用できます。

- [シングル ローカル ログイン（Single Local Logon）] : 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。この設定では、ローカル ユーザは 1 人以上のリモート ユーザがクライアント PC にログインしている場合でも VPN 接続を確立できますが、VPN 接続が排他的トンネリング用に設定されている場合は、VPN 接続のクライアント PC 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 ログオ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決まります。SingleLocalLogin 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。
- [SingleLogon] : VPN 接続の全体で、ログインできるユーザは 1 人だけです。1 人以上のユーザがログインして、ローカルまたはリモートで VPN 接続を確率した場合、接続は許可されません。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、その VPN 接続は終了します。

（注）　SingleLogon 設定を選択した場合、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。

クライアント プロファイルの [Windows VPN 確立（Windows VPN Establishment）] の設定では、AnyConnect が実行されているコンピュータにリモート ログインしたユーザが VPN 接続を確立する場合のクライアントの動作が指定されます。次の値が可能です。

- [ローカルユーザのみ（Local Users Only）]：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。AnyConnect クライアント バージョン 2.3 以前の動作はこの方式でした。
- [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 コンピュータ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 セッションを終了せずに RDP セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。

（注）　現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN 確立（Windows VPN Establishment）] 設定が適用されることはありません。AnyConnect では、VPN 接続を確立したのがログイン前のリモート ユーザかどうかの判定は行われません。そのため、[Windows VPN 確立（Windows VPN Establishment）] の設定が [*ローカルユーザのみ（Local Users Only）*] でも、リモート ユーザが SBL を介して VPN 接続を確立することは可能です。

Windows RDP セッションから AnyConnect セッションを有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Preferences）] ペインに移動します。

ステップ 3　Windows ログイン実行方式を選択します。

- [シングル ローカル ログイン（Single Local Logon）]：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。
- [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。

ステップ 4　リモート ログインしたユーザが VPN 接続を確立する場合のクライアントの動作を指定する Windows ログイン実行方式を選択します。

- [ローカルユーザのみ（Local Users Only）]：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。

（注）　現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN 確立（Windows VPN Establishment）] 設定が適用されることはありません。

L2TP または PPTP を介した AnyConnect

一部の国の ISP では、L2TP トンネリング プロトコルおよび PPTP トンネリング プロトコルのサポートが必要です。

セキュア ゲートウェイを宛先としたトラフィックを PPP 接続上で送信する場合、AnyConnect では外部トンネルが生成したポイントツーポイント アダプタが使用されます。PPP 接続上で VPN トンネルを確立する場合、クライアントでは ASA 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 ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、

除外ルートを特定する方法を指定する場合は、AnyConnect プロファイルの [PPP Exclusion] 設定を使用します。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。

ここでは、PPP 除外の設定方法について説明します。

- 「L2TP または PPTP を介した AnyConnect の設定」（P.3-73）
- 「ユーザによる PPP 除外の上書き」（P.3-73）

L2TP または PPTP を介した AnyConnect の設定

デフォルトでは、[PPP 除外（PPP Exclusion）] は無効です。プロファイルで PPP 除外を有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-2）を参照）。

ステップ 2　[プリファレンス（Part 2）（Preferences (Part 2)）] ペインに移動します。

ステップ 3　[PPP 除外（PPP Exclusion）] でその方式を選択します。このフィールドで [ユーザ制御可（User Controllable）] をオンにすると、ユーザには次の設定が表示され、ユーザはそれらを変更することができます。

- [自動（Automatic）] : PPP 除外を有効にします。AnyConnect では自動的に、PPP サーバの IP アドレスが使用されます。この値は、自動検出による IP アドレスの取得に失敗す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。
- [上書き（Override）] : 同様に PPP 除外を有効にします。自動検出で PPP サーバの IP アドレスを取得できず、PPPExclusion の UserControllable 値が true である場合は、次項の説明に従ってこの設定を使用するよう、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。

ステップ 4　[PPP 除外サーバ IP（PPP Exclusion Server IP）] フィールドに、PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレスを入力します。このフィールドで [ユーザ制御可（User Controllable）] をオンにすると、ユーザにこの IP アドレスが表示され、ユーザをそれを変更することができます。

ユーザによる PPP 除外の上書き

自動検出が機能しない場合に、PPP 除外をユーザ設定可能に設定すると、ユーザはローカル コンピュータ上で AnyConnect プリファレンス ファイルを編集することにより、これらの設定を上書きすることができます。次の手順では、その方法について説明します。

ステップ 1　メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows : %LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。次に例を示します。
  - Windows Vista : C:\Users*username*\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml

  - Windows XP：C:\Documents and Settings**username**\Local Settings\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
- Mac OS X：/Users/username/.anyconnect
- Linux：/home/username/.anyconnect

ステップ 2　PPPExclusion の詳細を <ControllablePreferences> の下に挿入して、Override 値と PPP サーバの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に、例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3　ファイルを保存します。

ステップ 4　AnyConnect を終了し、リスタートします。

AnyConnect プロファイル エディタの VPN パラメータに関する詳細

ここでは、プロファイル エディタのさまざまなペインに表示されるすべての設定について説明します。

AnyConnect プロファイル エディタ、プリファレンス（パート 1）

[ログイン前の起動の使用（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。SBL では、ログイン スクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。

[接続前のメッセージを表示する（Show Pre-connect Message）]：初めて接続を試行するユーザに対してメッセージを表示します。たとえば、スマートカードをリーダーに必ず挿入するようユーザに知らせることもできます。事前接続メッセージの設定または変更の詳細については、「デフォルトの AnyConnect の英語メッセージの変更」（P.11-20）を参照してください。

[証明書ストア（Certificate Store）]：AnyConnect がどの証明書ストアで証明書を検索するかを制御します。Windows では、ローカル マシン用の証明書ストアと現在のユーザ用の証明書ストアが別々に用意されます。コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。ほとんどの場合、デフォルト設定（All）が適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。

- [すべて（All）]：（デフォルト）すべての証明書を受け入れ可能です。
- [マシン（Machine）]：マシン証明書（コンピュータで識別された証明書）を使用します。
- [ユーザ（User）]：ユーザ生成の証明書を使用します。

[証明書ストアの上書き（Certificate Store Override）] : Windows のマシン証明書ストアで証明書を検索するよう AnyConnect を設定することができます。これは、証明書がこのストアにあり、ユーザにマシンの管理者権限がない場合に役立ちます。

[起動時に自動接続（Auto Connect on Start）] : AnyConnect の起動時に、AnyConnect 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 アドレス（Local LAN Access）] 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、企業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 8.3(1) 以降）で、新しい 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（クライアント プロファイルの [常時接続 VPN（Always-on VPN）] セクションで [Apply last local VPN resource rules] を有効にします）。

[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（デフォルトで有効）。[自動再接続（Auto Reconnect）] を有効にすると、接続解除の原因にかかわらず、再接続は試行されません。

自動再接続の動作は次のとおりです。

- [DisconnectOnSuspend]（デフォルト）: 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、システムのレジューム後も再接続は試行されません。
- [ReconnectAfterResume] : 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。

（注） AnyConnect 2.3 よりも前までは、システムの一時停止に対するデフォルトの動作として、VPN セッションに割り当てられたリソースを保持し、システムのレジューム後に VPN 接続を再確立していました。この動作を維持する場合は、自動再接続の動作として **ReconnectAfterResume** を選択します。

[自動更新（Auto Update）] : クライアントの自動更新を無効にします。

[RSA セキュア ID 連携（RSA Secure ID Integration）]（Windows のみ）: ユーザが RSA とどのようにインタラクトするかを制御します。デフォルトでは、AnyConnect により RSA インタラクションの適切な方式が指定されます（自動設定）。

- [自動（Automatic）] : ソフトウェア トークンおよびハードウェア トークンが許可されます。
- [ソフトウェア トークン（Software Token）] : ソフトウェア トークンのみ許可されます。
- [ハードウェア トークン（Hardware Token）] : ハードウェア トークンのみ許可されます。

[Windows ログインの強制（Windows Logon Enforcement）] : リモート デスクトップ プロトコル（RDP）からの VPN セッションの確立を許可します。（スプリット トンネリング VPN 設定が必要です）。VPN 接続を確立したユーザがログオフすると、AnyConnect は VPN 確立を接続解除します。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。

- [シングル ローカル ログイン（Single Local Logon）]：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。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。
- [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。

[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。次の値が可能です。

- [ローカルユーザのみ（Local Users Only）]：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。

（注） 現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN 確立（Windows VPN Establishment）] 設定が適用されることはありません。AnyConnect では、VPN 接続を確立したのがログイン前のリモート ユーザかどうかの判定は行われません。そのため、[Windows VPN 確立（Windows VPN Establishment）] の設定が [ローカルユーザのみ（Local Users Only）] でも、リモート ユーザが SBL を介して VPN 接続を確立することは可能です。

このペインに表示されるクライアント機能に関するより詳細な設定情報については、次の各項を参照してください。

Start Before Logon：「Start Before Logon の設定」（P.3-7）

証明書ストアおよび証明書の上書き：「証明書ストアの設定」（P.3-45）

自動再接続：「自動再接続の設定」（P.3-60）

Windows ログインの強制：**Windows RDP セッションによる VPN セッションの起動**

AnyConnect プロファイル エディタ、プリファレンス（パート 2）

[証明書選択を無効にする（Disable Certificate Selection）]：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。

[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を介して VPN セッションを確立するようになっています。次に示すのは、透過的なプロキシ サービスを実現する要素の一例です。

- 一部のワイヤレス データ カードから入手できるアクセラレーション ソフトウェア
- 一部のアンチウイルス ソフトウェア上のネットワーク コンポーネント

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。

[プロキシ設定（Proxy Settings）]：リモート コンピュータ上の Microsoft Internet Explorer または Mac Safari のプロキシ設定を無視するように、AnyConnect プロファイルでポリシーを指定できます。これは、プロキシ設定によってユーザが企業ネットワークの外部からトンネルを確立できない場合に役立ちます。ASA 上のプロキシ設定と併用します。

- [ネイティブ（Native）]：クライアントは、クライアントで設定されたプロキシ設定および Internet Explorer で設定されたプロキシ設定の両方を使用します。ネイティブ OS プロキシ設定（Windows の MSIE に設定されたものなど）が使用され、グローバル ユーザ プリファレンスで設定されたプロキシ設定はこれらのネイティブ設定の先頭に追加されます。
- [プロキシを無視（Ignore Proxy）]：ユーザ コンピュータ上の Microsoft Internet Explorer または Mac Safari のプロキシ設定が無視されます。ASA に到達するプロキシには、何のアクションも実行されません。
- [上書き（Override）]（サポートされていません）

[最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）]：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。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。

- [中断時間しきい値（Suspension Time Threshold）]（単位は時間）：現在のセキュア ゲートウェイへの接続が解除されてから、別のセキュア ゲートウェイに再接続するまでの経過時間。ユーザが対応するゲートウェイ間の移行が極端に多い場合は、この時間を長くします。
- [パフォーマンス向上しきい値（Performance Improvement Threshold）]（単位は %）：クライアントが別のセキュア ゲートウェイに接続する際の基準となるパフォーマンス向上率。デフォルトは 20 % です。

（注） AAA が使用されている場合は、別のセキュア ゲートウェイへの移行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 Mac のみ）：信頼ネットワーク ポリシーおよび非信頼ネットワーク ポリシーに従って VPN 接続を開始または停止することが必要な状況を自動で管理します。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。

（注） [自動 VPN ポリシー（Automatic VPN Policy）] の設定にかかわらず、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）]：ユーザが企業ネットワークの中（信頼ネットワーク）に存在する場合、AnyConnect により VPN 接続が自動的に解除されます。
  - [接続解除（Disconnect）]：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）]：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）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を共に [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）]：ユーザが企業ネットワークの外（非信頼ネットワーク）に存在する場合、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）]：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）]：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。このオプションを選択すると、常時接続 VPN は無効となります。[信頼されたネットワークポリシー（Trusted Network Policy）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を共に [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（カンマ区切りの文字列）。たとえば 161.44.124.* や 64.102.6.247 などです。DNS サーバ アドレスでは、ワイルドカード（*）がサポートされます。
- [Always On]：Windows 7、Windows Vista、Windows XP、Mac OS X 10.5、または Mac OS X 10.6 が実行されているコンピュータにユーザがログインした場合、VPN への接続を AnyConnect で自動的に行うかどうかを指定します。この機能を使用すると、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が適用されます。グループ ポリシーおよびダイナミック アクセス ポリシーで常時接続 VPN パラメータを設定すると、この設定を上書きすることができます。これにより、ポリシーの割り当てに使用される一致基準に従って例外を指定できます。AnyConnect ポリシーでは常時接続 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。
- [VPN の接続解除を許可（Allow VPN Disconnect）]：AnyConnect で常時接続 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。常時接続 VPN セッションのユーザは、[接続解除（Disconnect）] をクリックすることが必要になる場合があるため、次のような問題に対処できるよう代替セキュア ゲートウェイを選択することができます。
  - 現在の VPN セッションに関するパフォーマンスの問題。
  - VPN セッションが中断した後に生じる再接続の問題。

注意　[接続解除（Disconnect）] ボタンをクリックすると、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、データの漏洩を防ぐことができるほか、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。

この機能の詳細については、「常時接続 VPN 用の [接続解除（Disconnect）] ボタン」（P.3-26）を参照してください。

- [Connect Failure Policy（接続エラーポリシー）]：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、常時接続 VPN が有効な場合にのみ適用されます。

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。AnyConnect では、キャプティブ ポータルの大半が検出されます。ただし、キャプティブ ポータルを検出できない場合は、接続障害クローズド ポリシーによりネットワーク接続は制限されます。接続障害ポリシーの設定を行う場合は必ず、事前に「接続障害ポリシーに関する要件」（P.3-29）を一読してください。

  - [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。
  - [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、ユーザが必ず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）]：Number of minutes 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 ポータルの要件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）。
  - [最後の VPN ローカル リソース ルールの適用（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。

[PPP 除外（PPP Exclusion）]：PPP 接続上で VPN トンネルについて、除外ルートを特定するかどうかや、除外ルートを特定する方法を指定します。これにより、クライアントでは、セキュリティ ゲートウェイよりも先を宛先としてトンネリングされたトラフィックから、このセキュリティ ゲートウェイを宛先とするトラフィックを除外することができます。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 では自動的に、PPP サーバの IP アドレスが使用されます。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。自動検出で PPP サーバの IP アドレスを取得できず、かつ PPP 除外をユーザ設定可能に設定している場合は、ユーザに対して「ユーザによる PPP 除外の上書き」（P.3-73）の説明に従うよう指示してください。

[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移行が発生した場合に、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。Mac OS 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 7、Windows XP、または Windows Vista が実行され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 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 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。

このペインに表示されるクライアント機能に関するより詳細な設定情報については、次の各項を参照してください。

ローカル プロキシ接続の許可	「ローカル プロキシ接続に関する要件」（P.3-61）
プロキシの設定	「ローカル プロキシ接続の設定」（P.3-61）
最適ゲートウェイ選択	「最適ゲートウェイ選択に関する要件」（P.3-62）
自動 VPN ポリシーおよび Trusted Network Detection	「Trusted Network Detection の設定」（P.3-17）
VPN 常時接続	「常時接続 VPN の設定」（P.3-25）
接続障害ポリシー	「接続障害ポリシーの設定」（P.3-29）
キャプティブ ポータル修復の許可	「キャプティブ ポータル ホットスポット修復」（P.3-31）
PPP 除外	「L2TP または PPTP を介した AnyConnect」（P.3-72）
認証タイムアウト値	「認証タイムアウトの設定」（P.3-68）

AnyConnect プロファイル エディタの [バックアップ サーバ（Backup Servers）]

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を下方向へ移動します。

[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を下方向へ移動します。

[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。

バックアップ サーバの設定に関する詳細については、「バックアップ サーバ リストの設定」（P.3-59）を参照してください。

AnyConnect プロファイル エディタの [証明書照合（Certificate Matching）]

このペインでは、クライアントによる自動証明書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。

[キーの用途（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：一部の処理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。

[キーの拡張用途（Extended Key Usage）]：次のキーの拡張用途設定を使用します。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）

[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）。

[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）]：照合に使用する文字列。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。

[ワイルドカード（Wildcard）]：有効にすると、ワイルドカード パターン照合を使用することができます。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。

[演算子（Operator）]：照合を実行する際に使用する演算子。

- [等しい（Equal）]：== と同等
- [等しくない（Not Equal）]：!= と同等

[大文字と小文字を区別する（Match Case）]：有効にすると、パターンに適用するパターン照合で大文字と小文字が区別されます。

- オン：大文字と小文字を区別したパターン照合を実行します。
- オフ：大文字と小文字を区別しないパターン照合を実行します。

証明書の照合に関するより詳細な設定情報については、「証明書照合の設定」（P.3-49）を参照してください。

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

このペインでは、証明書登録の設定を行います。

[証明書の登録（Certificate Enrollment）]：AnyConnect で、クライアント認証に使用する証明書のプロビジョニングおよび更新を行う場合に、Simple Certificate Enrollment Protocol（SCEP）を使用できるようにします。クライアントから証明書要求が送信されると、その要求は認証局（CA）により自動的に承諾または拒否されます。

（注） SCEP プロトコルを使用すると、クライアントが証明書を要求した後、その応答を受信するまで CA にポーリングすることもできます。ただしこのポーリング方式は、このリリースではサポートされていません。

[証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するか（SCEP が有効な場合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。

[自動 SCEP ホスト（Automatic SCEP Host）] : SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル（トンネル グループ）を指定します。ASA の完全修飾ドメイン名（FQDN）または接続プロファイル名を入力してください （ホスト名 *asa.cisco.com*、接続プロファイル名 *scep_eng* など）。

[CA URL] : SCEP CA サーバを指定します。CA サーバの FQDN または IP アドレスを入力してください （*http://ca01.cisco.com* など）。

- [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。
- [サムプリント（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、発行した証明書の「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。

[証明書の内容（Certificate Contents）] : 証明書の内容をクライアントが要求する方法を定義します。

- 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 （「Jr.」、「III.」など）。
- Qualifier (DN) : 完全 DN の修飾子。
- City (L) : 都市 ID。
- Title (T) : 個人の敬称 （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する（Display Get Cert Button）] : 有効にすると、AnyConnect GUI に [証明書を取得（Get Certificate] ボタンが表示されます。デフォルトでは、ユーザに対して [登録（Enroll）] ボタンが表示されるほか、AnyConnect が認証局へ証明書登録を要求していることを知らせるメッセージが表示されます。[証明書を取得（Get Certificate）] を表示することで、ユーザは AnyConnect インターフェイスを操作する際に、その操作内容をより明確に理解することができます。

証明書失効しきい値により定義された期間内に証明書が失効するよう設定されている場合に、証明書が失効するか、または証明書が存在しないと、ユーザに対してこのボタンが表示されます。

（注）　認証証明書のプロビジョニングまたは更新をユーザが手動で要求できるようにする場合は、[証明書取得ボタンを表示する（Display Get Cert Button）] を有効にします。通常これらのユーザは、あらかじめ VPN トンネルを作成することなく認証局にアクセスできます。そうでない場合は、この機能を有効にしないでください。

[証明書の登録（Certificate Enrollment）] に関するより詳細な設定情報については、「SCEP による認証登録の設定」（P.3-39）を参照してください。

AnyConnect プロファイル エディタの [モバイル ポリシー（Mobile Policy）]

このペインでは、Windows Mobile 上で実行中の AnyConnect で使用するパラメータを設定します。

（注）　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 管理者ガイド リリース 2.5*』を参照してください。

- [デバイスロックが必要（Device Lock Required）] : VPN 接続を確立する前に Windows Mobile デバイスに対してパスワードまたは PIN を設定する必要があります。これが適用されるのは、Microsoft Local Authentication Plug-ins（LAPs）を使用する Windows Mobile デバイスのみです。
- [最大タイムアウト時間（分単位）（Maximum Timeout Minutes）] : デバイス ロックが有効になるまでの最長時間（単位は分）。設定は必須です。
- [最小パスワード長（Minimum Password Length）] : デバイス ロック用のパスワードまたは PIN に必要な最低文字数を指定します。
- [パスワードの複雑さ（Password Complexity）] : 必要なデバイス ロックのパスワードに対して複雑度を指定します。
  - [アルファ（alpha）] : 英数字のパスワードであることが必要。
  - [PIN] : 数字の PIN であることが必要。
  - [強力（strong）] : 7 文字以上で構成され、うち最低 3 文字は大文字、小文字、数字、句読記号のいずれかである強度の高い英数字のパスワードであることが必要。

AnyConnect プロファイル エディタの [サーバ リスト（Server List）]

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。

[追加 / 編集（Add/Edit）] : 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。

AnyConnect プロファイル エディタの [サーバ リストの追加 / 編集（Add/Edit Server List）]

このペインでは、サーバとそのバックアップ サーバ、およびロード バランシング バックアップ デバイスを追加します。

[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を入力します。

[ホスト アドレス（Host Address）] : サーバの IP アドレスまたは FQDN を指定します。

（注）
- [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 で解決されます。

[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。

（注）　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。

[バックアップ サーバ リスト（Backup Server List）] : 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。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を下方向へ移動します。

- [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 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を下方向へ移動します。
- [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（Load Balancing Server List）]：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、かつ常時接続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常時接続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サーバの 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 ASA 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（Standard Authentication Only）]：デフォルトでは、AnyConnect クライアントは独自の AnyConnect EAP 認証方式を使用します。クライアントで標準ベースの方式を使用する場合は、これをオンにして設定します。ただし、そうした場合はクライアントのダイナミック ダウンロード機能が制限され、一部の機能がディセーブルになります。

（注） 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 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（*http://ca01.cisco.com* など）。

- [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。
- [サムプリント（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、発行した証明書の「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。

サーバ リストの作成に関するより詳細な設定情報については、「サーバ リストの設定」（P.3-54）を参照してください。

AnyConnect クライアント接続タイムアウトの設定

アイドルの AnyConnect VPN 接続を終了または保持するには、次の手順に従います。

アクティビティが発生していない場合でも、ASA がユーザに対して AnyConnect VPN 接続を維持する長さを制限できます。VPN セッションがアイドルになった場合、接続を終了するか、または接続を再ネゴシエートできます。

AnyConnect 接続の終了

AnyConnect 接続を終了するには、ユーザはセキュア ゲートウェイに対してエンドポイントを再認証し、新しい VPN 接続を作成する必要があります。

次の設定パラメータは、単純なタイムアウトに基づいて、VPN セッションを終了します。

- Default Idle Timeout：指定した期間、セッションが非アクティブの状態が続いた場合に、ユーザのセッションを終了します。デフォルト値は 30 分です。

  default-idle-timeout は、webvpn コンフィギュレーション モードで CLI を使用した場合のみ変更できます。デフォルト値は 1800 秒です。default-idle-timeout の設定方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Configuring Session Timeouts」を参照してください。

- VPN Idle Timeout：指定した期間、セッションが非アクティブの状態が続いた場合に、ユーザのセッションを終了します。SSL-VPN の場合のみ、vpn-idle-timeout が設定されていないと、default-idle-timeout が使用されます。

  ASDM を使用して VPN アイドル タイムアウトを設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using ASDM*』の「Adding or Editing a Remote Access Internal Group Policy, General Attributes」を参照してください。

  CLI を使用して VPN アイドル タイムアウトを設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Configuring VPN-Specific Attributes」のステップ 4 を参照してください。

AnyConnect 接続の再ネゴシエートと維持

次の設定パラメータは、トンネルを終了または再ネゴシエートします。ただし、セッションは終了しません。

- キープアライブ：ASA は定期的にキープアライブ メッセージを送信します。これらのメッセージは、ASA によって無視されますが、クライアントと ASA 間のデバイスとの接続の維持に役立ちます。

  ASDM を使用してキープアライブを設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using ASDM*』の「Configuring AnyConnect VPN Client Connections」を参照してください。

  CLI を使用してキープアライブを設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Group-Policy Attributes for AnyConnect Secure Mobility Client Connections」のステップ 5 を参照してください。

- Dead Peer Detection：ASA および/または AnyConnect クライアントは、「R-U-There」メッセージを送信します。これらのメッセージは、IPsec のキープアライブ メッセージよりも少ない頻度で送信されます。

  - クライアントが ASA の DPD メッセージに応答しない場合は、ASA はもう 3 回試行してから、セッションを「再開待機」モードに移行します。このモードでは、ユーザはネットワークをローミングしたり、スリープ モードに移行してから後で接続を復帰したりできます。デフォルトのアイドル タイムアウトが発生する前に、ユーザが再接続しなかった場合は、ASA はトンネルを終了します。推奨されるゲートウェイ DPD 間隔は 300 秒です。

– ASA がクライアントの DPD メッセージに応答しない場合、クライアントはもう 3 回試行してから、トンネルを終了します。推奨されるクライアント DPD 間隔は 30 秒です。

ASA（ゲートウェイ）およびクライアントの両方を、DPD メッセージを送信するようにイネーブルにして、タイムアウト間隔を設定できます。

ASDM を使用して DPD を設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using ASDM*』の「Dead Peer Detection」を参照してください。

CLI を使用して DPD を設定する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Configuring Group-Policy Attributes for AnyConnect Secure Mobility Client Connections」のステップ 4 を参照してください。

ベスト プラクティス

- クライアント DPD を 30 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。
- サーバ DPD を 300 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。
- SSL および IPsec の両方のキー再生成を 1 時間に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [キー再作成（Key Regeneration）]）。

CHAPTER 4

ネットワーク アクセス マネージャの設定

この章では、ネットワーク アクセス マネージャ設定の概要について、ならびにユーザ ポリシーおよびネットワーク プロファイルの追加と設定の手順について説明します。この章で説明する内容は、次のとおりです。

概要

ネットワーク アクセス マネージャは、企業ネットワーク管理者によって定められたポリシーに従って、セキュアなレイヤ 2 ネットワークを提供するクライアント ソフトウェアです。ネットワーク アクセス マネージャは、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。ネットワーク アクセス マネージャは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。管理者定義のポリシーに違反する接続をエンド ユーザが確立しないように、インテリジェントに動作します。

AnyConnect Secure Mobility Client のネットワーク アクセス マネージャ コンポーネントは、次の主な機能をサポートします。

- 有線（IEEE 802.3）およびワイヤレス（IEEE 802.11）ネットワーク アダプタ
- Windows マシン クレデンシャルを使用する Pre-login 認証

- Windows ログイン クレデンシャルを使用するシングル サインオン ユーザ認証
- 簡略で使いやすい IEEE 802.1X 設定
- IEEE MACsec 有線暗号化および企業ポリシー制御
- EAP 方式：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみの EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）
- 内部 EAP 方式：
  - PEAP：EAP-GTC、EAP-MSCHAPv2、および EAP-TLS
  - EAP-TTLS：EAP-MD5 および EAP-MSCHAPv2 およびレガシー方式（PAP、CHAP、MSCHAP、および MSCHAPv2）
  - EAP-FAST：GTC、EAP-MSCHAPv2、および EAP-TLS
- 暗号化モード：
  - スタティック WEP（オープンまたは共有）、ダイナミック WEP、TKIP、および AES
- キー確立プロトコル：
  - WPA、WPA2/802.11i、および CCKM（IEEE 802.11 NIC カードに応じて選択）

（注） CCKM でサポートされるアダプタは、Windows XP 上の Cisco CB21AG のみです

- スマート カードが提供するクレデンシャル。AnyConnect は、次の環境のスマート カードをサポートします。
  - Windows XP、7、および Vista 上の Microsoft CAPI 1.0 および CAPI 2.0
  - Mac OS X（10.4 以降）でトークンされたキーチェーン

（注） AnyConnect は、Linux または PKCS #11 デバイス上のスマート カードをサポートしません。

ネットワーク アクセス マネージャのシステム要件

ネットワーク アクセス マネージャ モジュールには、次が必要です。

- ASDM バージョン 6.4(0)104 以降

（注） スタンドアロン ネットワーク アクセス マネージャ エディタは、ネットワーク アクセス マネージャ プロファイル設定の代替としてサポートされています。セキュリティ上の理由から、AnyConnect は、標準エディタで編集されたネットワーク アクセス マネージャ プロファイルは受け入れません。

- 次のオペレーティング システムがネットワーク アクセス マネージャをサポートしています。
  - Windows 7（x86（32 ビット）および x64（64 ビット））
  - Windows Vista SP2（x86（32 ビット）および x64（64 ビット））
  - Windows XP SP3（x86（32 ビット））

– Windows Server 2003 SP2（x86（32 ビット））

ライセンスとアップグレード要件

AnyConnect ネットワーク アクセス マネージャは、無償でシスコの無線アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、および RADIUS サーバで使用できるようにライセンスされています。AnyConnect Essentials ライセンスまたは Premium ライセンスは必要ありません。関連するシスコの装置では、現在の SmartNet 契約が必要です。

ネットワーク アクセス マネージャの事前展開

ネットワーク アクセス マネージャを事前展開する場合、AnyConnect クライアントが ASA への初期接続を確立する前に、ネットワーク アクセス マネージャをエンドポイントにインストールします。ネットワーク アクセス マネージャ モジュールをインストールする前に、AnyConnect Secure Mobility Client をエンドポイントにインストールする必要があります。AnyConnect Secure Mobility Client のインストール手順については、「AnyConnect Secure Mobility Client の展開」（P.2-1）を参照してください。

ネットワーク アクセス マネージャの停止と起動

ローカル管理者特権を持つユーザが、ネットワーク アクセス マネージャを起動および停止できます。ローカル管理者特権を持たないユーザは、プロファイル エディタの [認証（Authentication）] パネルで定義されるサービス パスワードを使用しないと、ネットワーク アクセス マネージャを起動および停止できません。

プロファイル エディタ

ネットワーク アクセス マネージャ プロファイル エディタは、設定プロファイルの作成と事前設定クライアント プロファイルの作成のために設計されました。この設定がエンドポイントで展開されると、ネットワーク アクセス マネージャが管理面で定義されているエンド ユーザおよび認証ポリシーを適用できるようになり、事前設定ネットワーク プロファイルをエンド ユーザが使用できるようになります。プロファイル エディタを使用するには、プロファイルの設定を作成して保存し、設定をクライアントに配置します。AnyConnect には、ASDM 内にプロファイル エディタが含まれていますが、スタンドアロン バージョンも使用できます。プロファイル エディタの要件と展開手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。

新しいプロファイルの追加

ネットワーク アクセス マネージャに新しいプロファイルを追加するには、次の手順を実行します。

ステップ 1　ASDM ツールバーの [設定（Configuration）] をクリックします。

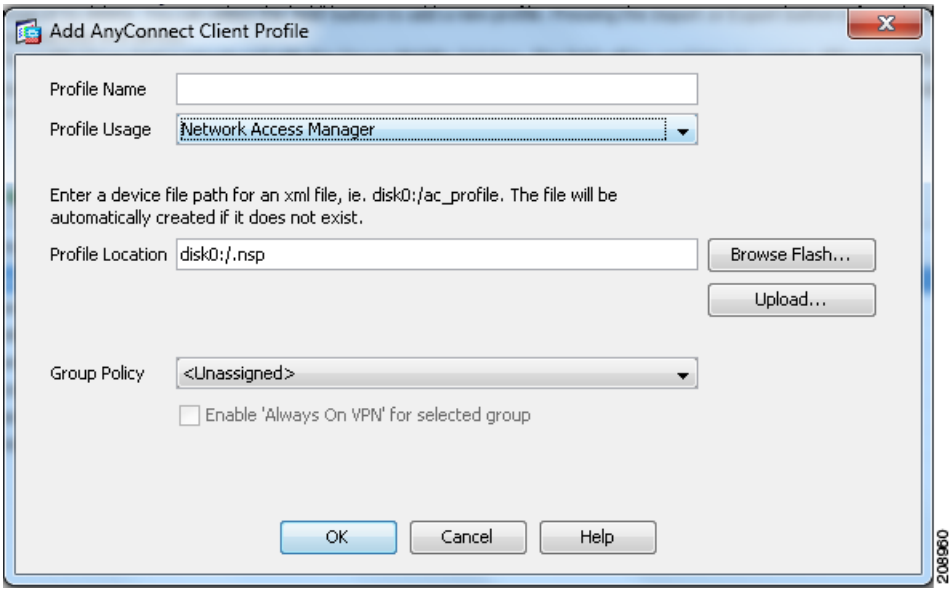
ステップ 2　ナビゲーション領域の左端にある [リモート アクセス VPN（Remote Access VPN）] をクリックします。

ステップ 3　[ネットワーク クライアント アクセス（Network Client Access）] をクリックします。

ステップ 4　[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] をクリックします。[プロファイル（profile）] ウィンドウが表示されます。

ステップ 5　[追加（Add）] をクリックします。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウが表示されます（図 4-1 を参照）。

図 4-1　[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウ



ステップ 6　プロファイル名を入力します。

（注）　ネットワーク アクセス マネージャ プロファイルの作成にスタンドアロン プロファイル エディタを使用している場合は、[プロファイル名（Profile Name）] フィールドのエントリとして **configuration.xml** を使用する必要があります。プロファイル エディタは、このファイルを newConfigFiles ディレクトリにコピーします。このプロセスを開始するには、ユーザがネットワーク アクセス マネージャを修復する必要があります。ネットワーク アクセス マネージャが再起動されると、新しい設定ファイルが検証されてネットワーク アクセス マネージャ /system ディレクトリに移動されます。

ステップ 7　[プロファイルの使用（Profile Usage）] ドロップダウン リストから [ネットワーク アクセス マネージャ（Network Access Manager）] を選択して、[OK] をクリックします。

ステップ 8　（任意）[プロファイル ロケーション（Profile Location）] パラメータに、XML ファイルのデバイス ファイル パスを確立します。

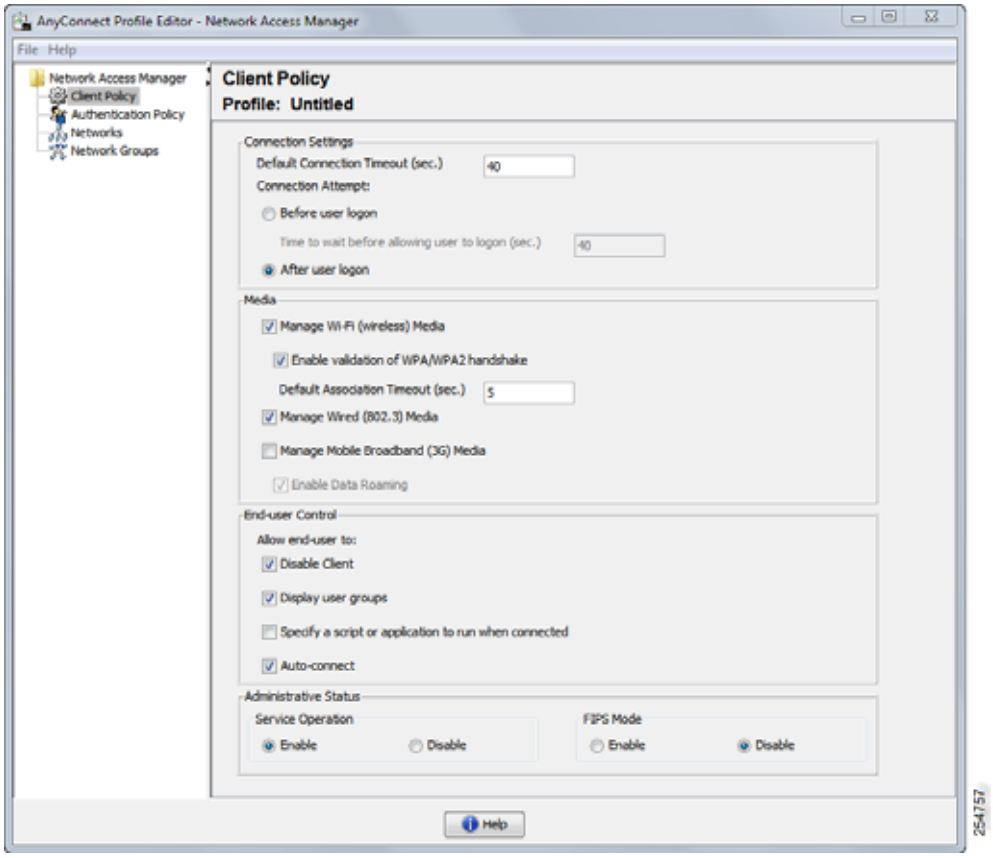
ステップ 9　（任意）ドロップダウン リストから AnyConnect グループ ポリシーを選択します。

ステップ 10　[OK] をクリックします。

クライアント ポリシーの設定

[クライアント ポリシー（Client Policy）] ウィンドウでは、クライアント ポリシー オプションを設定できます（図 4-2 を参照）。

図 4-2　　[クライアント ポリシー（Client Policy）] ウィンドウ



次の 4 つのセクションで構成されます。

- 管理ステータス（Administrative Status）
  - [サービス オペレーション（Service Operation）] パラメータを使用すると、ネットワーク アクセス マネージャ機能をオンまたはオフに切り替えられます。サービスをディセーブルにすることを選択した場合、ネットワーク アクセス マネージャは、クライアント上のネットワーク接続を管理できません。
  - FIPS モードをオンまたはオフに切り替えられます。連邦情報処理標準（FIPS 104-2）は、米国 政府の標準で、暗号化モジュールのセキュリティ要件について定めています。FIPS モードをイネーブルにすると、ネットワーク アクセス マネージャは、政府の要件を満たす方法で暗号化の処理を実行します。処理の通常の FIPS モードはディセーブルです。詳細については、「FIPS と追加セキュリティのイネーブル化」（P.8-1）を参照してください。
- [接続の設定（Connection Settings）] : ユーザ ログインの前または後にユーザ接続コンポーネントを使用したネットワークの試行をするかどうかを定義できます。

- [デフォルトの接続タイムアウト（Default Connection Timeout）]：ユーザが作成したネットワークの接続タイムアウト パラメータとして使用する秒数を指定します。デフォルト値は、40 秒です。
- [ユーザ ログインの前（Before User Logon）]：Windows ユーザ ログイン手順が実行される前に、ネットワーク アクセス マネージャがユーザ接続をすぐに試行するように指定します。Windows ログイン手順には、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、および GPO ベースのログイン スクリプトの実行が含まれます。
- [ユーザ ログインまでの待機時間（Time to Wait Before Allowing User to Logon）]：ネットワーク アクセス マネージャが完全なネットワーク接続を確立するまでに待機する最大秒数（最悪のケース）を指定します。ネットワーク接続がこの時間内に確立できない場合、Windows ログイン プロセスでユーザ ログインが続行されます。デフォルトは 5 秒です。

  （注）　ネットワーク アクセス マネージャがワイヤレス接続を管理するように設定されている場合、ワイヤレス接続の確立には時間が余計に必要なため、30 秒以上を使用することを推奨します。DHCP 経由で IP アドレスを取得するために必要な時間も考慮する必要があります。2 つ以上のネットワーク プロファイルが設定されている場合、2 つ以上の接続試行に対応するように値を大きくできます。

- [ユーザ ログイン後（After User Logon）]：Windows ユーザ ログイン手順後に、ネットワーク アクセス マネージャがユーザ接続を試行することを指定します。

- [メディア（Media）]：ネットワーク アクセス マネージャ クライアントによって制御されるメディア タイプが選択できます。
  - [Wi-Fi（ワイヤレス）メディアの管理（Manage Wi-Fi (wireless) Media）]：WiFi メディアの管理をイネーブルにします。任意で WPA/WPA2 ハンドシェイク検証もイネーブルにできます。

    IEEE 802.11i ワイヤレス ネットワーキング標準には、キー導出中に EAPOL キー データの送信されたアクセス ポイントの RSN IE がビーコン/プローブ応答フレームにあるアクセス ポイントの RSN IE と一致することをサプリカントが検証する必要があることが定められています。WPA/WPA2 ハンドシェイクの検証をイネーブルにする場合は、デフォルト アソシエーション タイムアウトを指定する必要があります。WPA/WPA2 ハンドシェイク設定の検証のイネーブル化をオフにすると、この検証手順は省略されます。

    （注）　ただし、一部のアダプタでは、アクセス ポイントの RSN IE を常に提供するわけではないため、認証試行に失敗し、クライアントが接続されません。

  - [有線（IEEE 802.3）メディアの管理（Manage Wired (IEEE 802.3) Media）]：ネットワーク アクセス マネージャの有線メディアの管理をイネーブルにします。

- [エンドユーザの制御（End-user Control）]：ユーザの次の制御を決定できます。
  - [クライアントの無効化（Disable Client）]：AnyConnect UI を使用した有線およびワイヤレス メディアのネットワーク アクセス マネージャによる管理をユーザがディセーブルまたはイネーブルにできます。
  - [ユーザ グループの表示（Display User Groups）]：管理者定義のグループに対応しない場合でも、ユーザが作成したグループ（CSSC 5.x から作成）を表示して、接続できるようにします。
  - [接続時に実行するスクリプトまたはアプリケーションの指定（Specify a Script or Application To Run When Connected）]：ネットワークの接続時に実行するスクリプトまたはアプリケーションをユーザが指定できます。

（注）　スクリプトの設定は、1 つのユーザ設定ネットワークに固有であり、そのネットワークが接続状態になったときに実行するローカル ファイル（.exe、.bat、または .cmd）をユーザが指定できます。競合を避けるために、スクリプト機能では、ユーザはユーザ定義のネットワークのスクリプトまたはアプリケーションの設定のみを実行でき、管理者定義のネットワークは実行できません。スクリプト機能では、スクリプトの実行に関して管理者ネットワークをユーザが変更できません。このため、ユーザは管理者ネットワークのインターフェイスを使用できません。また、ユーザにスクリプトの実行設定を許可しない場合、この機能はネットワーク アクセス マネージャ GUI に表示されません。

- [自動接続（Auto-connect）] : 選択すると、ネットワーク アクセス マネージャは、ユーザが選択する必要なく、自動的にネットワークに接続されます。デフォルトは自動接続です。

認証ポリシーの設定

このウィンドウでは、グローバル アソシエーションおよび認証ネットワーク ポリシーを定義できます。これらのポリシーは、ユーザが作成できるすべてのネットワークに適用されます。ポリシーを使用すると、ユーザが GUI で作成できるネットワークのタイプが制限できます。いずれかのアソシエーションまたは認証モードをオンにしない場合、ユーザはネットワークを作成できません。モードのサブセットを選択すると、ユーザはこれらのタイプのネットワークを作成できますが、オフのタイプは作成できません。目的のアソシエーションまたは認証モードをそれぞれ選択するか、[すべて選択（Select All）] を選択します。

[ネットワーク アクセス マネージャ（Network Access Manager）] メニューから [認証ポリシー（Authentication Policy）] を選択すると、図 4-3 に示されているウィンドウが表示されます。

お客様の要件に応じて、セキュア モビリティ環境で異なる認証メカニズムが使用されますが、すべてのメカニズムが IEEE 802.1X、EAP、および RADIUS をサポートするプロトコルとして使用します。これらのプロトコルでは、ワイヤレス LAN クライアントの認証成功に基づいたアクセス制御ができ、またユーザがワイヤレス LAN ネットワークを認証することもできます。

このシステムでは、AAA のその他の要素（許可およびアカウンティング）も RADIUS および RADIUS アカウンティングを通じて通信するポリシーを通じて提供されています。

認証プロトコル選択のメカニズムは、現在のクライアント認証データベースと統合されています。セキュアなワイヤレス LAN 展開では、ユーザが新しい認証システムを作成する必要はありません。

EAP

EAP とは、認証プロトコルがそれを伝送するトランスポート プロトコルからデカップリングされていることの要件に対処する IEFT RFC のことです。このデカップリングによって、トランスポート プロトコル（IEEE 802.1X、UDP、または RADIUS など）は、認証プロトコルを変更せずに、EAP プロトコルを伝送できます。

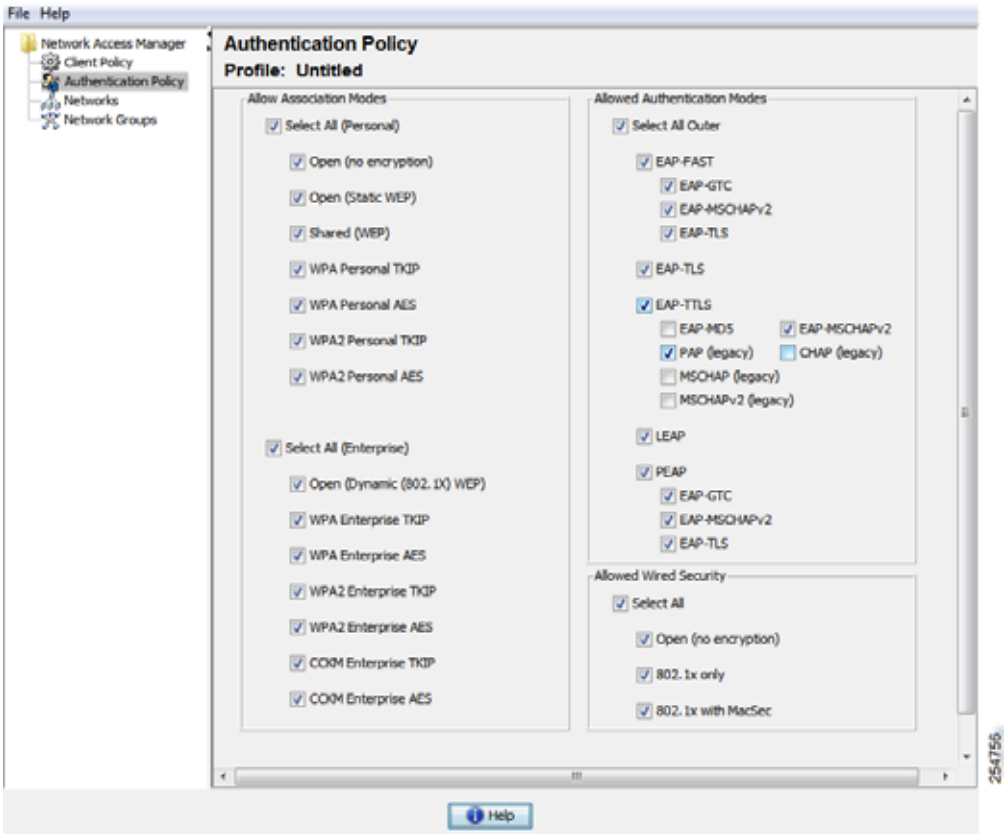
基本的な EAP プロトコルは、比較的単純で次の 4 つのパケット タイプから構成されます。

- EAP 要求 : オーセンティケータは、要求パケットをサプリカントに送信します。各要求には type フィールドがあり、要求されている内容を示します。これには、使用するサプリカント アイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。

- EAP 応答：サプリカントは、オーセンティケータに応答パケットを送信して、EAP 要求開始に一致するシーケンス番号を使用します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が NAK の場合は除きます。
- EAP success：オーセンティケータは、認証に成功すると、成功パケットをサプリカントに送信します。
- EAP failure：オーセンティケータは、認証に失敗すると、失敗パケットをサプリカントに送信します。

EAP を IEEE 802.11X システムで使用している場合、アクセス ポイントは EAP パススルー モードで動作します。このモードでは、アクセス ポイントはコード、識別子、および長さのフィールドを確認して、サプリカントから受信した EAP パケットを AAA サーバに転送します。オーセンティケータで AAA サーバから受信したパケットは、サプリカントに転送されます。

図 4-3　　[認証ポリシー（Authentication Policy）] ウィンドウ



このページの各オプションの説明については、次を参照してください。

- 個人または企業アソシエーション モードについて：ネットワーク セキュリティ レベルの定義
- 許可された認証モードについて：ネットワーク マシンまたはユーザ認証の定義
- 許可された有線セキュリティについて：ネットワーク接続タイプの定義

ネットワークの設定

[ネットワーク（Networks）] ウィンドウでは、企業ユーザ向けに事前定義のネットワークを設定できます。すべてのグループで使用できるネットワークを設定する、または特定のネットワークで使用するグループを作成できます。

グループとは、基本的に、設定された接続（ネットワーク）の集合です。各設定された接続は、グループに属するか、すべてのグループのメンバである必要があります。

（注） 下位互換性を確保するため、Cisco Secure Services Client で展開された管理者作成のネットワークは、SSID をブロードキャストしない非表示ネットワークとして扱われます。ユーザ ネットワークは、自身の SSID をブロードキャストするネットワークとして扱われます。

新しいグループを作成できるのは管理者だけです。設定にグループが定義されていない場合、プロファイル エディタによって自動生成グループが作成されます。自動生成グループには、管理者定義のグループに割り当てられていないネットワークが含まれます。クライアントは、アクティブ グループに定義されている接続を使用してネットワーク接続の確立を試みます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create networks）] オプションの設定に応じて、エンド ユーザは、ユーザ ネットワークをアクティブ グループに追加するか、アクティブ グループからユーザ ネットワークを削除できます。

定義されているネットワークは、リストの先頭にあるすべてのグループで使用できます。globalNetworks 内にあるネットワークを制御できるため、エンド ユーザが接続できる企業ネットワークを指定できます。これは、ユーザ定義のネットワーク内にある場合も同様です。管理者設定のネットワークは、エンド ユーザは削除できません。

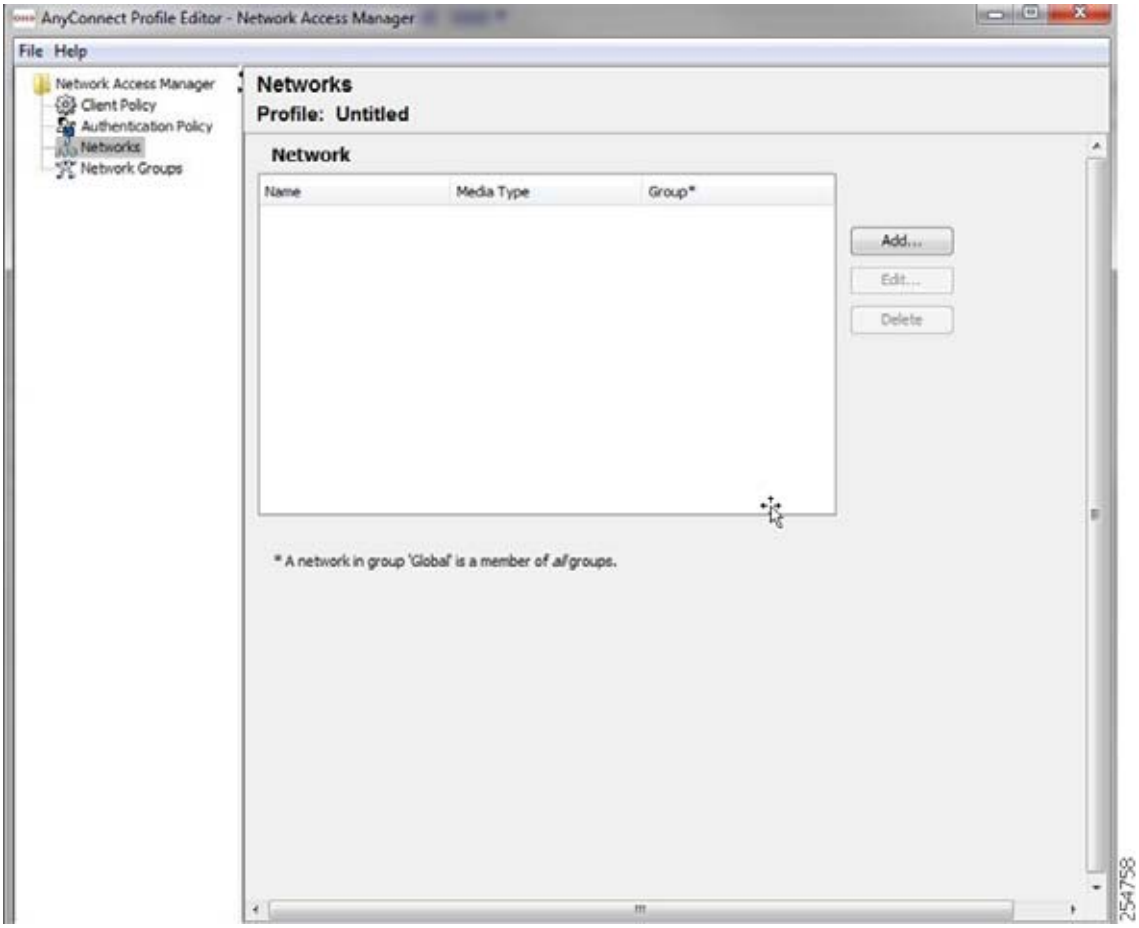
（注） エンド ユーザは、ネットワークをグループに追加できますが、globalNetworks セクションにあるネットワークは除きます。これは、globalNetworks セクションにあるネットワークはすべてのグループに存在するためで、これらはプロファイル エディタを使用してのみ作成できます。

企業ネットワークの一般的なエンド ユーザは、このクライアントを使用するためにグループの知識を必要としないことに注意してください。アクティブ グループは、設定の最初のグループです。ただし、1 つのグループのみが使用できる場合は、クライアントはアクティブ グループを認識せず、アクティブ グループを表示しません。一方で、複数のグループが存在する場合、UI にはアクティブ グループが選択されたことを示すコンボ ボックスが表示されます。これにより、ユーザはアクティブ グループからの選択ができ、設定は再起動後も持続します。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create networks）] オプションの設定に応じて、エンド ユーザはグループを使用せずに自身のネットワークを追加または削除できます。

（注） グループ選択は再起動後も持続して、ネットワークは修復されます（トレイ アイコンを右クリックしながら [ネットワーク修復（Network Repair）] を選択して実行することにより）。ネットワーク アクセス マネージャが修復されたか再起動された場合、ネットワーク アクセス マネージャは以前のアクティブ グループを使用して起動します。

[ネットワーク アクセス マネージャ（Network Access Manager）] メニューから [ネットワーク（Networks）] を選択すると、図 4-4 に示されているウィンドウが表示されます。

図 4-4　[ネットワーク（Networks）] ウィンドウ



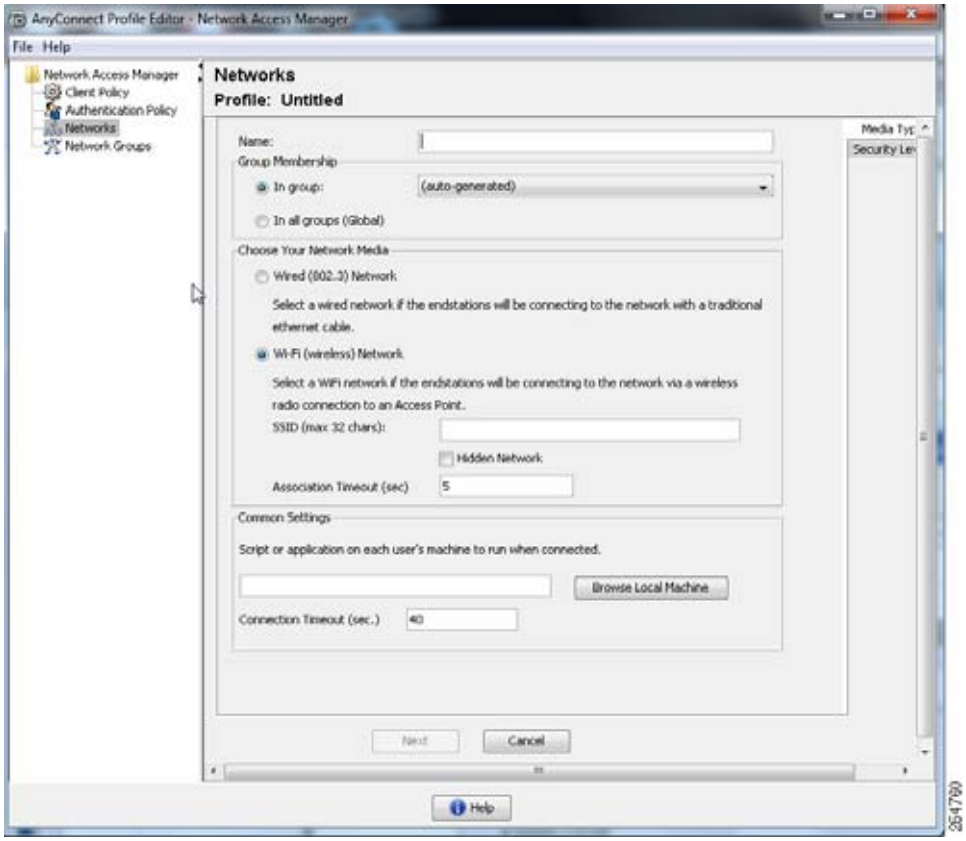
次のいずれかのアクションを選択します。

- [追加（Add）] をクリックし、新しいネットワークを作成します。新しいネットワークの作成を選択する場合は、後のネットワーク メディア タイプの定義の項の手順に従います。
- 変更するネットワークを選択して、[編集（Edit）] をクリックします。
- 削除するネットワークを選択して、[削除（Delete）] をクリックします。

ネットワーク メディア タイプの定義

このウィンドウ パネルでは、有線またはワイヤレス ネットワークを作成または編集できます。設定は、有線またはワイヤレスのいずれを選択するかにより異なります。図 4-5 に、Wi-Fi ネットワークを選択すると表示されるウィンドウを示します。この項では、有線と Wi-Fi オプションの両方について説明します。

図 4-5　[メディア タイプ（Media Type）] パネル



ステップ 1　[名前（Name）] フィールドに、このネットワークに対して表示する名前を入力します。

ステップ 2　（Wi-Fi のみ）[SSID] パラメータに、ワイヤレス ネットワークの SSID を入力します。

ステップ 3　（Wi-Fi のみ）ネットワークが自身の SSID をブロードキャストしていない場合は、[非表示のネットワーク（Hidden Network）] を選択します。

（注）　ネットワーク アクセス マネージャの選択アルゴリズムは、ネットワーク スキャン リストを活用するように最適化されます。自身の SSID をブロードキャストするネットワークの場合、ネットワーク アクセス マネージャは、これらのネットワークがネットワーク スキャン リストに表示されたときに、これらのネットワークとの接続のみを試行します。

ステップ 4　（Wi-Fi のみ）[アソシエーション タイムアウト（Association Timeout）] パラメータに、ネットワーク アクセス マネージャが使用可能なネットワークを再評価する前に特定のワイヤレス ネットワークとのアソシエーションを待機する期間を入力します。デフォルトのアソシエーション タイムアウトは 5 秒です。

ステップ 5　[共通設定（Common Settings）] セクションでは、実行するファイルのパスおよびファイル名を入力するか、場所を参照して実行するファイルを選択します。

スクリプトおよびアプリケーションには、次が適用されます。

- .exe、.bat、または .cmd 拡張子のファイルが受け入れられます。

- ユーザは、管理者作成のネットワーク内で定義されているスクリプトまたはアプリケーションを変更できません。
- プロファイル エディタを使用してパスおよびスクリプトまたはアプリケーションのファイル名の指定のみができます。スクリプトまたはアプリケーションがユーザのマシンに存在しない場合は、エラー メッセージが表示されます。スクリプトまたはアプリケーションがユーザのマシンに存在しないこと、およびシステム管理者に問い合わせが必要なことがユーザに通知されます。
- アプリケーションがユーザのパスに存在する場合を除いて、実行するアプリケーションのフル パスを指定する必要があります。アプリケーションがユーザのパスに存在する場合は、アプリケーション名またはスクリプト名だけを指定できます。

ステップ 6　[接続タイムアウト（Connection Timeout）] パラメータに、ネットワーク アクセス マネージャが別のネットワークへの接続を試行する（接続モードが自動の場合）または別のアダプタを使用する前に、ネットワーク接続の確立を待機する秒数を入力します。

（注）　スマート カード認証システムによっては、認証を完了するまでに 60 秒近くが必要です。スマート カードを使用するときは、[接続タイムアウト（Connection Timeout）] 値を大きくする必要がある場合があります。

ステップ 7　[次へ（Next）] をクリックします。

ネットワーク セキュリティ レベルの定義

有線またはワイヤレス ネットワークのセキュリティ レベル タイプを定義できます。[セキュリティ レベル（Security Level）] 領域で、目的のネットワーク タイプを選択します。

- 認証有線ネットワークの使用：セキュアな企業有線ネットワークで推奨。
- オープン ネットワークの使用：推奨されていないが、有線ネットワーク上のゲスト アクセスで使用可能。
- 共有キーの使用：小規模オフィスやホーム オフィスなどのワイヤレス ネットワークで推奨。
- 認証 WiFi ネットワークの使用：セキュアな企業ワイヤレス ネットワークで推奨。

認証有線ネットワークの使用

セキュリティ レベルに IEEE 802.1X 認証を使用する場合は、次の手順を実行します。

ステップ 1　[ネットワークの認証中（Authenticating Network）] を選択します。

（注）　[ネットワーク メディア タイプ（Network Media Type）] パネルで [有線（802.3）ネットワーク（Wired (802.3) Network）] を必ず選択します（図 4-5 を参照）。

ステップ 2　ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

- [認証期間（秒）（authPeriod(sec.)）]：認証が開始された場合、認証メッセージの間隔がこの時間を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。

- [保持期間（秒）（heldPeriod(sec.)）]：認証が失敗した場合、サプリカントはここで定義された時間だけ待機し、この時間を超えると別の認証が試行されます。
- [開始期間（秒）（startPeriod(sec.)）]：EAPoL-Start を送信してオーセンティケータを使用して認証の試行を開始した後、サプリカントはこのタイマーで定義された時間だけオーセンティケータからの応答を待機します。この時間を超えると認証が再度開始されます（次の EAPoL-Start を送信するなど）。
- [最大開始（maxStart）]：EAPoL-Start を送信してオーセンティケータを使用してサプリカントが認証を開始する回数です。この回数を超えるとサプリカントはオーセンティケータが存在しないと見なします。これが発生した場合は、サプリカントはデータ トラフィックを許可します。

ヒント　単一の認証有線接続がオープンおよび認証ネットワークの両方と動作するように設定できます。これは、[開始期間（startPeriod）] および [最大開始（maxStart）] を注意深く設定して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも小さくなるようにします（[開始期間（startPeriod）] x [最大開始（maxStart）] < ネットワーク接続タイマー）。

（注）このシナリオでは、ネットワーク接続タイマーを（[開始期間（startPeriod）] x [最大開始（maxStart）]）秒だけ大きくして、DHCP アドレスを取得してネットワーク接続を完了するために十分な時間をクライアントに与えます。

逆に、認証が成功した場合のみデータ トラフィックを許可する管理者の場合は、[開始期間（startPeriod）] および [最大開始（maxStart）] を確認して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも大きくなるようにします（[開始期間（startPeriod）] x [最大開始（maxStart）] > ネットワーク接続タイマー）。

ステップ 3　次のセキュリティ レベルから選択します。

- [キーの管理（Key Management）]：有線ネットワークで使用するキー管理プロトコルを、ドロップダウン リストを使用して決定します。
  - [なし（None）]：キー管理プロトコルを使用しません。また、有線暗号化を実行しません。
  - [MKA]：サプリカントは、MACsec Key Agreement および暗号キーのネゴシエートを試行します。MACsec とは、MAC Layer Security のことで、有線ネットワークを介した MAC レイヤ暗号化を提供します。MACsec プロトコルは、暗号化を使用して MAC レベル フレームを保護する手段であり、MACsec Key Agreement（MKA）エンティティに依存して暗号キーをネゴシエートおよび配布します。

    （注）　MACsec Key Agreement の定義の詳細については、IEEE-802.1X-Rev を参照してください。また、MACsec 暗号化プロトコルの定義の詳細については、IEEE 802.1AE-2006 を参照してください。
    さらに、利点と制限事項、機能の概要、設計上の考慮事項、展開、およびトラブルシューティングなどを含む MACsec の詳細については、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html を参照してください。

- 暗号化
  - [なし（None）]：データ トラフィックの整合性チェックは行われますが、暗号化はされません。
  - [MACsec: AES-GCM-128]：データ トラフィックは、AES-GCM-128 を使用して暗号化されます。

ステップ 4　[ポート認証の例外ポリシー（Port Authentication Exception Policy）] を選択します。[ポート認証の例外ポリシー（Port Authentication Exception Policy）] をイネーブルにすることで、IEEE 802.1X サプリカントの認証プロセス中の動作を調整できます。ポートの例外がイネーブルではない場合、サプリカントは、既存の動作を続けて完全な設定が正常に完了すると（またはこの項で前に説明したように、オーセンティケータからの応答を受信せずに [最大開始（maxStart）] の回数だけ認証が開始された後で）ポートを開くことだけを行います。次のいずれかのオプションを選択します。

- [認証前にデータ トラフィックを許可（Allow data traffic before authentication）]：選択すると、この例外により認証試行の前にデータ トラフィックが許可されます。
- [次の場合でも認証後にデータ トラフィックを許可（Allow data traffic after authentication even if）]
  - [EAP で失敗（EAP Fails）]：選択すると、サプリカントは認証を試行します。しかし、認証に失敗した場合、サプリカントは認証に失敗したにもかかわらず、データ トラフィックを許可します。
  - [EAP では成功したがキー管理で失敗（EAP succeeds but key management fails）]：選択すると、サプリカントはキー サーバとのキーのネゴシエートを試行しますが、何らかの理由によりキー ネゴシエーションに失敗した場合でもデータ トラフィックを許可します。この設定は、キー管理が設定されている場合のみ有効です。キー管理がなしに設定されている場合、このチェックボックスはグレー表示されます。

（注）　MACsec は、ACS バージョン 5.1 以降および MACsec 対応スイッチを必要とします。ACS またはスイッチ設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

オープン ネットワークの使用

オープン ネットワークは、認証や暗号化を使用しません。オープン（非セキュア）ネットワークを作成するには、次の手順を実行します。

ステップ 1　[セキュリティ レベル（Security Level）] パネルから [ネットワークを開く（Open Network）] を選択します。この選択肢では、最もセキュリティ レベルの低いネットワークが提供されます。これは、ゲスト アクセス ワイヤレス ネットワークに推奨されています。

ステップ 2　[次へ（Next）] をクリックします。

ステップ 3　接続タイプを決定します。「ネットワーク接続タイプの定義」（P.4-17）を参照してください。

共有キーの使用

Wi-Fi ネットワークは、エンド ステーションとネットワーク アクセス ポイント間のデータを暗号化するときに使用するための、暗号キーを導出するために共有キーを使用することがあります。共有キーが WPA または WPA2 Personal とともに使用される場合、この設定では、小規模オフィスやホーム オフィスに適した中 レベルのセキュリティ クラスを提供します。

（注）　この設定は、企業ワイヤレス ネットワークでは推奨されません。

セキュリティレベルに共有キー ネットワークを指定する場合は、次の手順を実行します。

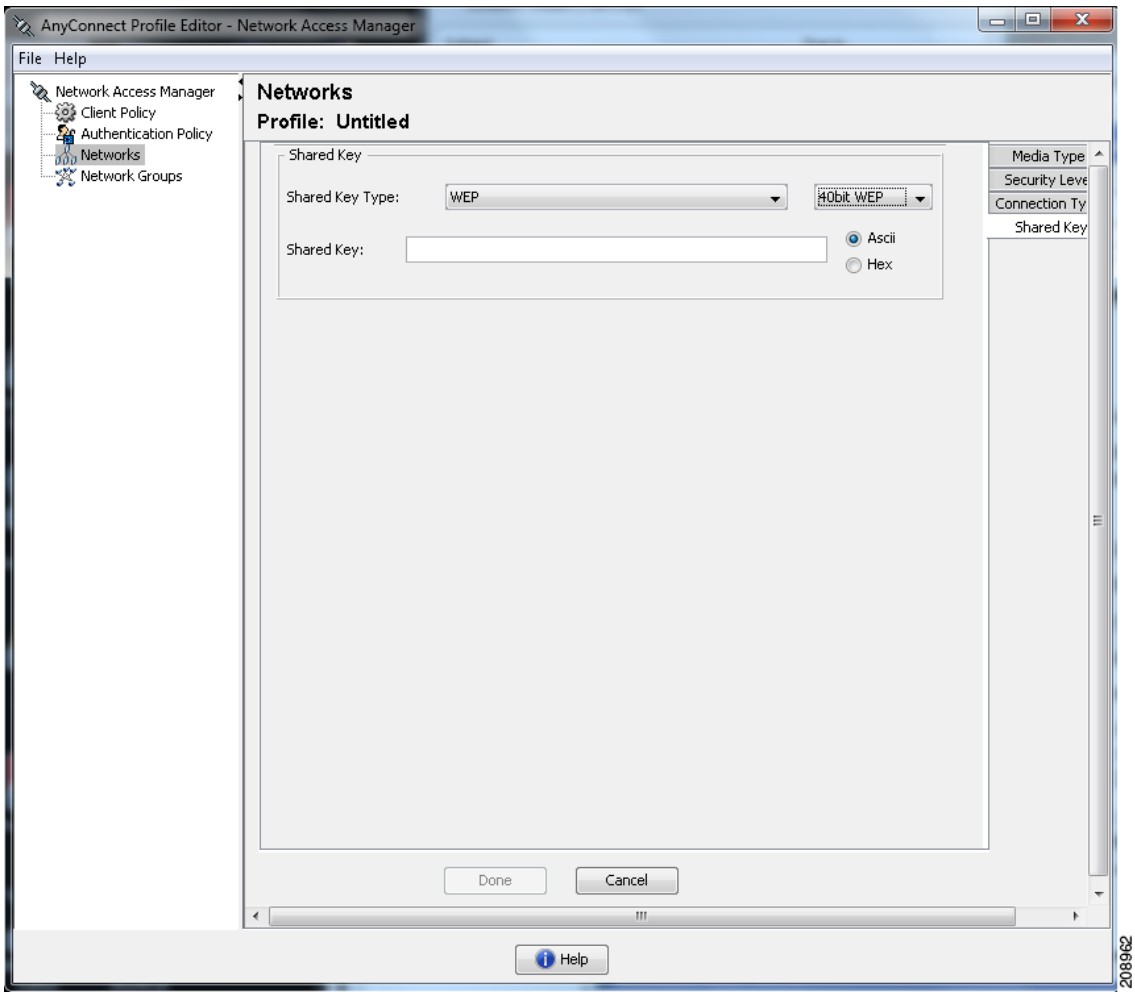
ステップ 1　[共有キー ネットワーク（Shared Key Network）] を選択します。

ステップ 2　[セキュリティ レベル（Security Level）] ウィンドウで [次へ（Next）] をクリックします。

ステップ 3　[ユーザ接続（User Connection）] または [マシン接続（Machine Connection）] を指定します。詳細については、「ネットワーク接続タイプの定義」（P.4-17）を参照してください。

ステップ 4　[次へ（Next）] をクリックします。[共有キー（Shared Key）] パネルが表示されます（図 4-6 を参照）。

図 4-6　[共有キー（Shared Key）] パネル



ステップ 5　[共有キー タイプ（Shared Key Type）] : 共有キー タイプを定める共有キー アソシエーション モードを指定します。次の選択肢があります。

- [WEP] : スタティック WEP 暗号化を使用するレガシー IEEE 802.11 オープンシステム アソシエーション。
- [共有（Shared]）] : レガシー IEEE 802.11 共有キー アソシエーション。
- [WPA/WPA2- パーソナル（WPA/WPA2-Personal）] : Wi-Fi セキュリティ プロトコル。パスフレーズ事前共有キー（PSK）から暗号キーを導出します。

ステップ 6　レガシー IEEE 802.11 WEP または共有キーを選択する場合は、40 ビット、64 ビット、104 ビット、または 128 ビットを選択します。40 または 64 ビットの WEP キーは、5 個の ASCII 文字または 10 桁の 16 進数である必要があります。104 または 128 ビットの WEP キーは、13 個の ASCII 文字または 26 桁の 16 進数である必要があります。

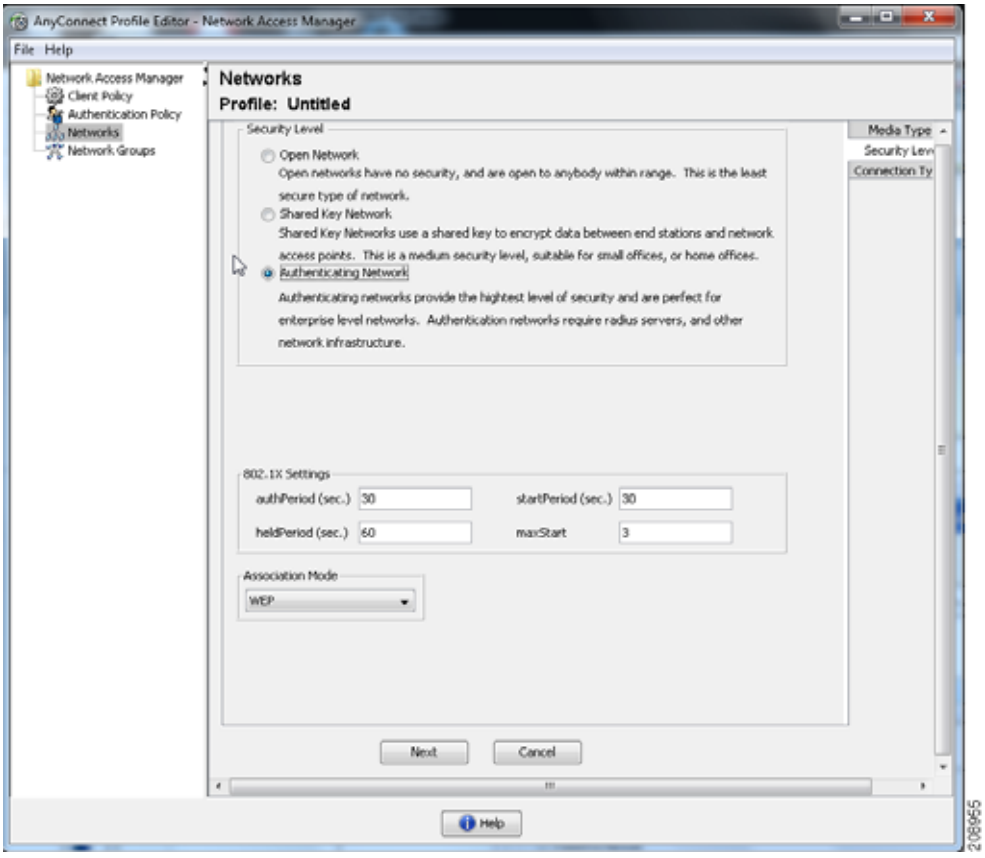
ステップ 7　WPA または WPA2 Personal を選択する場合は、使用する暗号化タイプ（TKIP/AES）を選択してから共有キーを入力します。入力するキーは、8 ～ 63 個の ASCII 文字またはちょうど 64 桁の 16 進数である必要があります。共有キーが ASCII 文字で構成されている場合は、[ASCII] を選択します。共有キーに 64 桁の 16 進数が含まれている場合は、[16 進数（Hexadecimal）] を選択します。

認証 WiFi ネットワークの使用

[ネットワークの認証中（Authenticating Network）] を選択すると、IEEE 802.1X および EAP に基づいたセキュアなワイヤレス ネットワークを作成できます。

セキュリティ レベルに認証ネットワークを指定する場合は、次の手順を実行します（図 4-7 を参照）。

図 4-7　　認証ネットワーク セキュリティ レベル



ステップ 1　[ネットワークの認証中（Authenticating Network）] を選択します。

ステップ 2　大半のネットワークでデフォルト値が機能するはずですが、必要に応じて環境に合わせて IEEE 802.1X 設定を実行することもできます。

- [認証期間（秒）（authPeriod(sec.)）]：認証が開始された場合、認証メッセージの間隔がこの時間を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。デフォルトは 30 秒です。
- [保持期間（秒）（heldPeriod(sec.)）]：認証が失敗した場合、サプリカントはここで定義された時間だけ待機し、この時間を超えると別の認証が試行されます。デフォルトは 60 秒です。
- [開始期間（秒）（startPeriod(sec.)）]：EAPoL-Start を送信してオーセンティケータを使用して認証の試行を開始した後、サプリカントはこのタイマーで定義された時間だけオーセンティケータからの応答を待機します。この時間を超えると認証が再度開始されます（次の EAPoL-Start を送信するなど）。デフォルトは 30 秒です。
- [最大開始（maxStart）]：EAPoL-Start を送信してオーセンティケータを使用してサプリカントが認証を開始する連続回数です（オーセンティケータからの応答を受信せずに）。この回数を超えるとサプリカントはオーセンティケータが存在しないと見なします。これが発生した場合は、サプリカントはデータ トラフィックを許可します。デフォルトは 3 回です。

（注）　このセクションでは、オーセンティケータがクライアント サプリカントに EAP アイデンティティ要求を送信すると認証が開始します。

ステップ 3　[アソシエーション モード（Association Mode）] には、使用するワイヤレス セキュリティ タイプを指定します。

ネットワーク接続タイプの定義

[接続タイプ（Connection Type）] パネルでは、ネットワーク接続タイプの選択およびこのネットワークを使用した接続試行を許可するときの指定（図 4-8 を参照）ができます。[マシン接続（Machine Connection）] オプションでは、接続にマシン接続タイプを定義します。マシン接続はいつでも使用できますが、通常は接続にユーザ クレデンシャルが不要な場合に常に使用します。[ユーザ接続（User Connection）] オプションでは、接続にユーザ接続タイプを定義します。ユーザは、PC へのログイン試行開始した後にだけ接続を確立できます。必須ではありませんが、ユーザ接続では通常ログイン済みのユーザのクレデンシャルを接続の確立に使用します。

マシンおよびユーザ ネットワークは、マシン部分およびユーザ部分から構成されていますが、マシン部分はユーザが PC にログインしていないときにだけ有効です。設定は 2 つの部分に対して同じですが、マシン接続の認証タイプおよびクレデンシャルは、ユーザ接続の認証タイプおよびクレデンシャルと異なる場合があります。

- [マシン接続（Machine Connection）]：ユーザがログオフしていてユーザ クレデンシャルが使用できないときでも、エンド ステーションがネットワークにログインする必要がある場合は、このオプションを選択します。このオプションは、ユーザがアクセスできるようになる前に、ドメインに接続するため、また GPO および他のアップデートをネットワークから取得するために通常は使用されます。

（注）　VPN Start Before Login（SBL）を期待どおりに機能させるには、ユーザが VPN の開始を試行するときにネットワーク接続が存在する必要があることを考慮する必要があります。ネットワーク アクセス マネージャがインストールされている場合、マシン接続を展開して、適切な接続を確実に使用できるようにする必要があります。

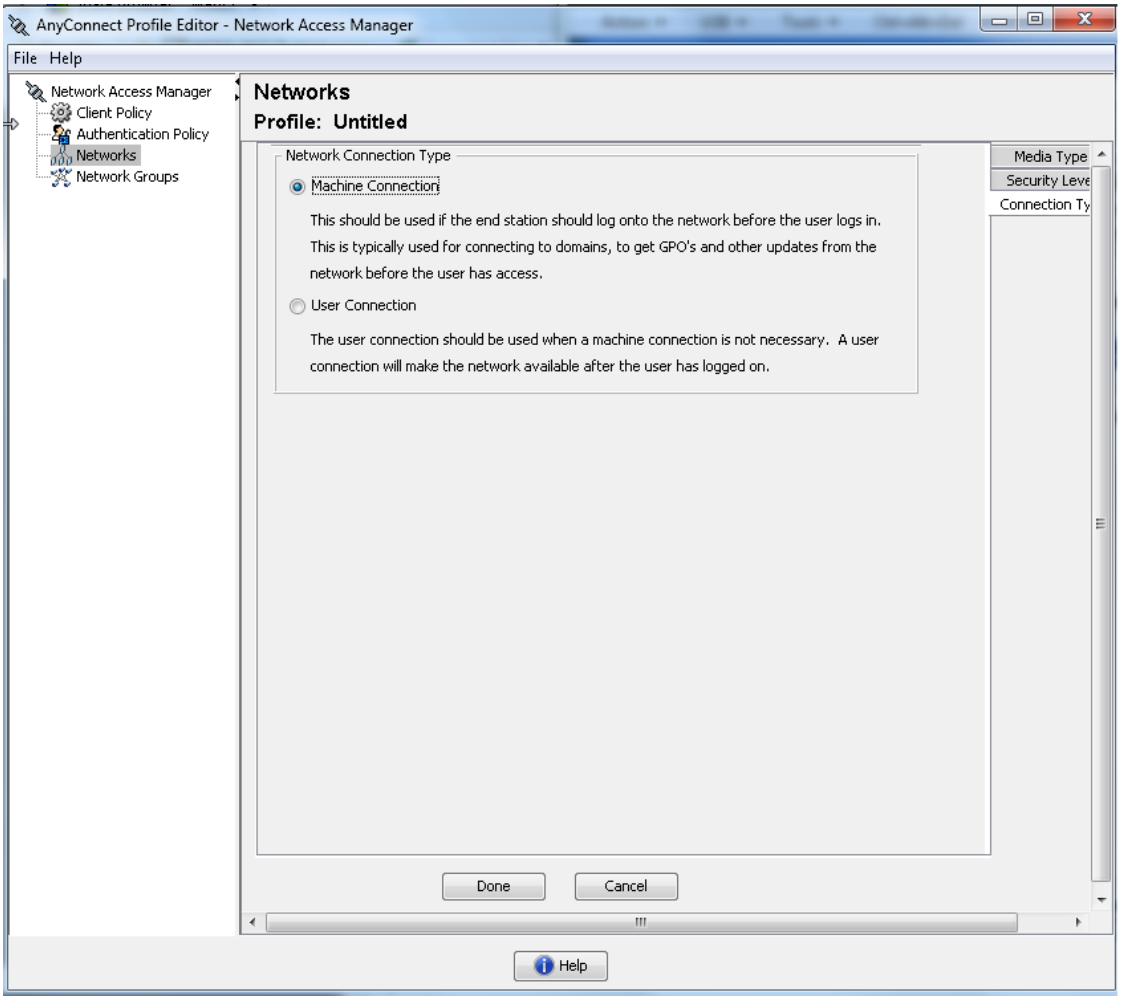
- [ユーザ接続（User Connection）]：マシン接続が不要な場合は、このオプションを選択します。ユーザ接続では、ユーザが PC へのログイン試行を開始した後でネットワークが使用できるようになります。ユーザがその後ログオフすると、ネットワーク接続は終了します。ただし、ユーザ ログオフ後も接続を拡張するように接続が設定されている場合は除きます。

（注）　[クライアント ポリシー接続（Client Policy Connection）] 設定では、ネットワーク アクセス マネージャによってユーザがログインしていると見なすかどうかを決定します（「クライアント ポリシーの設定」（P.4-5）を参照）。[接続の設定（Connection Settings）] が [ユーザ ログインの前に接続を試行（Attempt connection before use logon）] に設定されている場合、ネットワーク アクセス マネージャは、ユーザが入力したクレデンシャルを使用して実際のログイン前にネットワーク接続の確立を試みます。[接続の設定（Connection Settings）] が [ユーザ ログインの後に接続を試行（Attempt connection after use logon）] に設定されている場合、ネットワーク アクセス マネージャは、ユーザが実際にログインするまで待機してからネットワーク接続を確立します。

- [マシンおよびユーザ接続（Machine and User Connection）]：[マシン接続（Machine Connection）] を使用していてユーザがログインしていないとき、および [ユーザ接続（User Connection）] を使用していてユーザがログインしているときにネットワークに PC を常時接続するには、このオプションを選択します。

（注）　オープンおよび共有キー ネットワークの場合は、[マシンおよびユーザ接続（Machine and User Connection）] オプションは使用できません。

図 4-8　[ネットワーク接続タイプ（Network Connection Type）] パネル

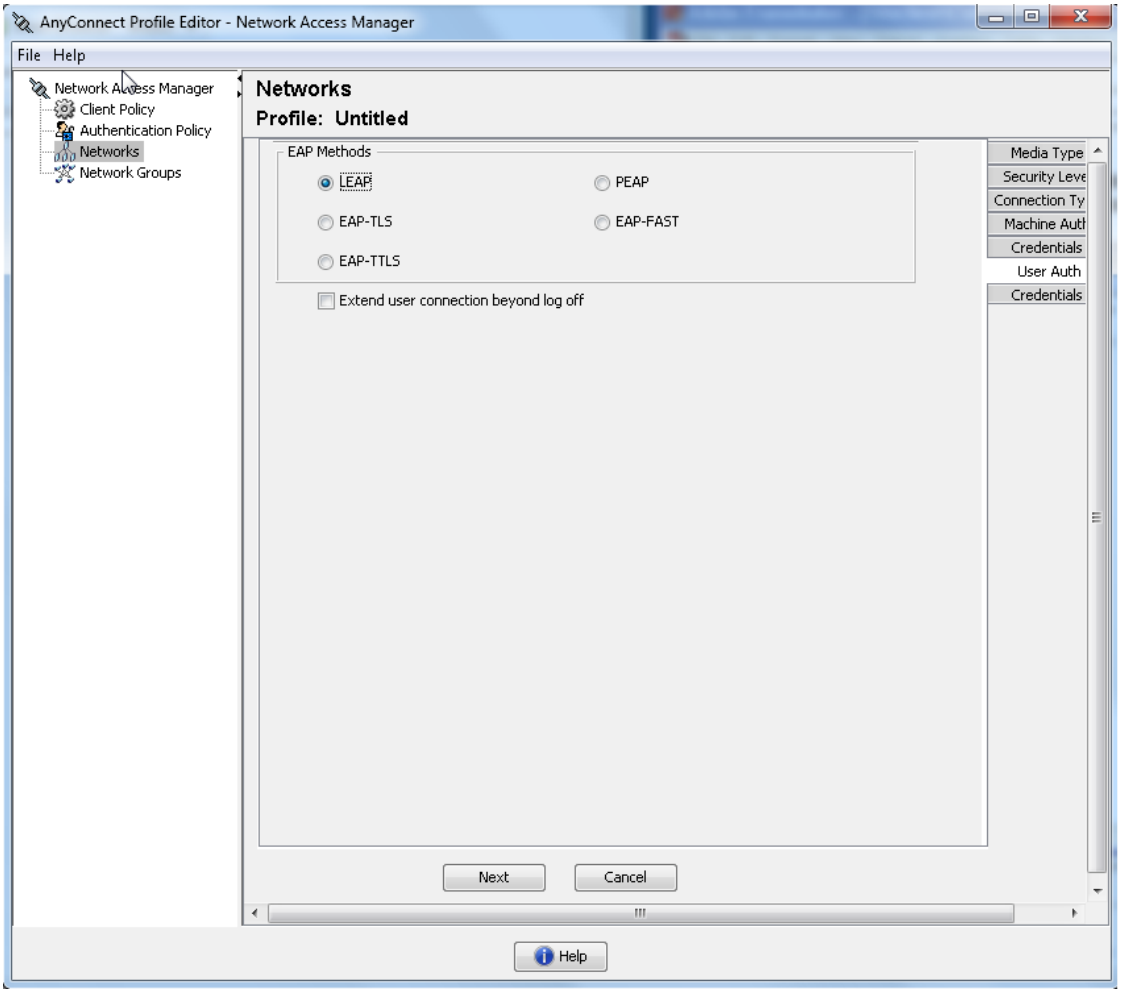


ネットワーク マシンまたはユーザ認証の定義

[マシン認証（Machine Authentication）] または [ユーザ認証（User Authentication）] パネルを使用すると、マシンまたはユーザ（図 4-9 を参照）の認証方式を選択できます。認証方式を指定すると、ウィンドウの中心が選択した方式に適応して、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP、または EAP-GTC に関する詳細を指定するように要求されます。

接続がネットワーク コンピュータのネットワーク アクセス マネージャによって管理されている最中に、ネットワーク コンピュータにリモート アクセスする方法の詳細については、「Windows Remote Desktop の使用」（P.C-7）を参照してください。ここでは、マシン、ユーザ、またはマシンおよびユーザ認証を使用したネットワーク プロファイルについて説明しています。

図 4-9　[マシン認証（Machine Authentication）] または [ユーザ認証（User Authentication）] パネル



（注）　MACsec をイネーブルにした場合は、PEAP、EAP-TLS、または EAP-FAST などの MSK キー導出をサポートする EAP 方式を必ず選択します。

EAP のオプションを選択した場合は、追加設定が必要です。

- EAP-GTC：「EAP-GTC の設定」（P.4-21）を参照してください
- EAP-TLS：「EAP-TLS の設定」（P.4-21）を参照してください。
- EAP-TTLS：「EAP-TTLS の設定」（P.4-22）を参照してください。
- PEAP：「PEAP オプションの設定」（P.4-23）を参照してください。
- EAP-FAST：「EAP-FAST の設定」（P.4-24）を参照してください。

EAP-GTC の設定

EAP-GTC は、単純なユーザ名とパスワード認証に基づく EAP 認証方式です。チャレンジ/レスポンス方式を使用せずに、ユーザ名とパスワードの両方がクリア テキストで渡されます。EAP 方式は、トンネリング EAP 方式の内部で使用（次のトンネリング EAP 方式を参照）、または OTP（トークン）を使用する場合に推奨されます。

EAP-GTC は、相互認証を提供しません。クライアント認証だけを行うため、不正なサーバがユーザのクレデンシャルを取得する可能性があります。相互認証が必要な場合、EAP-GTC は、サーバ認証を提供するトンネリング EAP 方式の内部で使用されます。

キー関連情報は EAP-GTC によって提供されないため、MACsec ではこの方式を使用できません。さらなるトラフィック暗号化のためにキー関連情報が必要な場合、EAP-GTC は、キー関連情報（および必要に応じて内部および外部の EAP 方式の暗号化バインド）を提供するトンネリング EAP 方式の内部で使用されます。

パスワード ソース オプションには、次の 2 つがあります。

- [パスワードを使用した認証（Authenticate using a Password）]：正しく保護されている有線環境にのみ適しています
- [トークンを使用した認証（Authenticate using a Token）]：トークン コードのライフタイムが短い（通常約 10 秒）ため、または OTP であるため、より高いセキュリティを備えています

（注） ネットワーク アクセス マネージャ、オーセンティケータ、または EAP-GTC プロトコルのいずれもパスワードとトークン コード間を区別できません。これらのオプションは、ネットワーク アクセス マネージャ内のクレデンシャルのライフタイムにのみ影響を与えます。パスワードは、ログアウトまでかそれ以降も記憶できますが、トークン コードは記憶できません（認証ごとにユーザがトークン コードの入力を求められるため）。

パスワードが認証に使用される場合、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。これは、パスワードがオーセンティケータにクリア テキストで渡されるためです。この方式は、データベースがリークしている可能性がある場合に推奨されます。

EAP-TLS の設定

EAP-Transport Layer Security（EAP-TLS）は、TLS プロトコル（RFC 2246）に基づく IEEE 802.1X EAP 認証アルゴリズムです。TLS は、X.509 デジタル証明書に基づく相互認証を使用します。EAP-TLS メッセージ交換は、相互認証、暗号スイート ネゴシエーション、キー交換、クライアントと認証サーバ間の検証、およびトラフィック暗号化に使用できるキー関連情報を提供します。

次のリストに、EAP-TLS クライアント証明書が有線およびワイヤレス接続に強固な認証を提供できる主な理由を示します。

- 通常、ユーザが介入することなく認証が自動で実行される。
- ユーザ パスワードに依存しない。
- デジタル証明書が強固な認証保護を提供する。
- メッセージ交換が公開キー暗号化により保護される。
- ディクショナリ攻撃の被害を受けにくい。
- 認証プロセスにより、データ暗号化および署名のための相互決定されたキーが生成される。

EAP-TLS には、次の 2 つのオプションが含まれています。

- [サーバ証明書の検証（Validate Server Certificate）] : サーバ証明書の検証をイネーブルにします。
- [高速な再接続の有効化（Enable Fast Reconnect）] : TLS セッション再開をイネーブルにします。これにより、TLS セッション データがクライアントとサーバの両方で保持されている限り、短縮化した TLS ハンドシェイクを使用することによってはるかに高速な再認証ができます。

（注）　[スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシン認証では使用できません。

（注）　Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

EAP-TTLS の設定

EAP-Tunneled Transport Layer Security（EAP-TTLS）は、EAP-TLS 機能を拡張する 2 フェーズのプロトコルです。フェーズ 1 では、完全な TLS セッションを実行して、フェーズ 2 で使用するセッション キーを導出して、サーバとクライアント間で属性を安全にトンネリングします。フェーズ 2 中には、多数のさまざまなメカニズムを使用する追加認証の実行にトンネリングされた属性を使用できます。

ネットワーク アクセス マネージャは、EAP-TTLS 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

フェーズ 2 で使用できる認証メカニズムには、次のプロトコルが含まれます。

- PAP（パスワード認証プロトコル）：ピアが双方向ハンドシェイクを使用してそのアイデンティティを証明する単純な方式を提供します。ID/ パスワード ペアは、認証が認められるか失敗するまで、ピアからオーセンティケータに繰り返し送信されます。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。

  パスワードがオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

  （注）　EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用できます。

- CHAP（チャレンジ ハンドシェイク認証プロトコル）：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証してください。このチャレンジ/ レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
- MS-CHAP（Microsoft CHAP）：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証してください。パスワードの NT-hash に基づいてこのチャレンジ/ レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。
- MS-CHAPv2：応答パケット内にピア チャレンジおよび成功パケット内にオーセンティケータ応答を含めることによって、ピア間の相互認証を提供します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃を防ぐために）サーバをクライアントの前に認証する必要がある場

合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

- EAP：次の EAP 方式が使用できます。
  - EAP-MD5（EAP-Message Digest 5）：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します（CHAP と類似）。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
  - EAP-MSCHAPv2：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。
- EAP-TTLS 設定
  - [サーバ ID の検証（Validate Server Identity）]：サーバ証明書の検証をイネーブルにします。
  - [高速な再接続の有効化（Enable Fast Reconnect）]：内部認証が省略されたかどうか、またはオーセンティケータによって制御されているかどうかに関係なく、外部 TLS セッション再開のみをイネーブルにします。

（注）　[スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシン認証では使用できません。Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

- [内部方式（Inner Methods）]：TLS トンネルが作成された後で内部方式の使用を指定します。

PEAP オプションの設定

Protected EAP（PEAP）は、トンネリング TLS ベースの EAP 方式です。PEAP は、内部認証方式の暗号化に対するクライアント認証の前に、サーバ認証に TLS を使用します。内部認証は、信頼される暗号保護されたトンネル内部で実行され、証明書、トークン、およびパスワードを含む、さまざまな内部認証方式をサポートします。ネットワーク アクセス マネージャは、PEAP 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケットに対する TLS トンネル作成
- メッセージ認証
- メッセージの暗号化
- クライアントに対するサーバの認証

次の認証方法を使用できます。

- パスワード
  - EAP-MSCHAPv2：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、PEAP を設定してサーバの証明

書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

  - EAP-GTC（EAP Generic Token Card）：ユーザ名とパスワードを伝送するために EAP エンベロープを定義します。相互認証が必要な場合は、PEAP を設定してサーバの証明書を検証する必要があります。パスワードがクリア テキストでオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

- トークン
  - EAP-GTC：トークン コードまたは OTP を伝送するために EAP エンベロープを定義します。
- 証明書
  - EAP-TLS：ユーザ証明書を伝送するために EAP エンベロープを定義します。中間者攻撃（有効なユーザの接続のハイジャック）を避けるため、同じオーセンティケータに対する認証用に PEAP（EAP-TLS）および EAP-TLS プロファイルを混在させないことを推奨します。その設定に応じて、オーセンティケータを設定する必要があります（プレーンおよびトンネリングされた EAP-TLS の両方をイネーブルにしない）。
- PEAP 設定
  - [サーバ ID の検証（Validate Server Identity）] : サーバ証明書の検証をイネーブルにします。
  - [高速な再接続の有効化（Enable Fast Reconnect）] : 外部 TLS セッション再開のみをイネーブルにします。オーセンティケータは、内部オーセンティケータを省略するかどうかを制御します。
- [スマート カード使用時には無効化（Disable when using a Smart Card）] および [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）] オプションは、マシン認証では使用できません。
- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）] : パスワードまたは証明書を使用する認証が選択できます。
  - [パスワードを使用した認証（Authenticate using a Password）] : [EAP-MSCHAPv2] または [EAP-GTC]
  - [EAP-TLS、証明書を使用（EAP-TLS, using Certificate）]
  - [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）]

（注） Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

EAP-FAST の設定

EAP-FAST は、IEEE 802.1X 認証タイプで、柔軟性があり、展開や管理も容易です。EAP-FAST は、さまざまなユーザおよびパスワード データベース タイプ、サーバ主導のパスワードの失効と変更、およびデジタル証明書（任意）をサポートします。

EAP-FAST は、証明書を使用せず、ディクショナリ攻撃からの保護を提供する IEEE 802.1X EAP タイプを展開するお客様向けに開発されました。

EAP-FAST は、TLS メッセージを EAP 内にカプセル化します。また、次の 3 つのプロトコル フェーズから構成されます。

1. Authenticated Diffie-Hellman Protocol（ADHP）を使用して Protected Access Credential（PAC）と呼ばれる共有秘密クレデンシャルを持つクライアントをプロビジョニングするプロビジョニング フェーズ。
2. トンネルの確立に PAC を使用するトンネル確立フェーズ。
3. 認証サーバでユーザのクレデンシャル（トークン、ユーザ名 / パスワード、またはデジタル証明書）を認証する認証フェーズ。

他の 2 つのトンネリング EAP 方式とは異なり、EAP-FAST は内部および外部方式間に暗号化バインドを提供して、攻撃者が有効なユーザの接続をハイジャックする特殊な中間者攻撃を防止します。

[EAP-FAST 設定（EAP-FAST Settings）] パネルでは、EAP-FAST 設定ができます。

- EAP-FAST 設定（EAP-FAST Settings）
  - [サーバ ID の検証（Validate Server Identity）] : サーバ証明書の検証をイネーブルにします。これをイネーブルにすると、管理ユーティリティに 2 つの追加のダイアログが導入されて、ネットワーク アクセス マネージャ プロファイル エディタのタスク リストに [証明書（Certificate）] パネルがさらに追加されます。
  - [高速な再接続の有効化（Enable Fast Reconnect）] : セッション再開をイネーブルにします。EAP-FAST で認証セッションをレジュームする 2 つのメカニズムには、内部認証を再開するユーザ認可 PAC、また短縮化した外部 TLS ハンドシェイクができる TLS セッション再開が含まれます。この [高速な再接続の有効化（Enable Fast Reconnect）] パラメータは、両方のメカニズムをイネーブルまたはディセーブルにします。オーセンティケータがいずれを使用するかを決定します。

    （注）　マシン PAC は、短縮化した TLS ハンドシェイクを提供し、内部認証を省きます。この制御は、PAC パラメータのイネーブル / ディセーブルによって処理されます。

    （注）　Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

    （注）　[スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシンでは使用できません。

- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）] : パスワードまたは証明書を使用する認証ができます。
  - [パスワードを使用した認証（Authenticate using a Password）] : [EAP-MSCHAPv2] または [EAP-GTC] EAP-MSCHAPv2 は、相互認証を提供しますが、サーバを認証する前にクライアントを認証します。サーバを最初に認証する相互認証を使用する場合は、EAP-FAST を認証付きプロビジョニングのみに設定して、サーバの証明書を検証します。パスワードの NT-hash に基づいてこのチャレンジ / レスポンス方式を使用して、EAP-MSCHAPv2 を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。パスワードが EAP-GTC 内でクリア テキストでオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

パスワード ベースの内部方式を使用している場合、Protected Access Credential（PAC）を使用する追加オプションが適用されます。認証されていない PAC プロビジョニングを許可するか許可しないかを選択します。

- [証明書を使用した認証（Authenticate using a certificate）] : 証明書を使用する認証に対しての基準を、要求された場合にクライアント証明書を暗号化しないで送信、トンネル内でのみクライアント証明書を送信、またはトンネル内で EAP-TLS を使用してクライアント証明書を送信から決定します。
- [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）]

- [PAC の使用（Use PACs）] : EAP-FAST 認証での PAC の使用を指定できます。PAC は、ネットワーク認証を最適化するためにクライアントに配布されるクレデンシャルです。

（注） EAP-FAST では大半の認証サーバが PAC を使用するため、通常は PAC オプションを使用します。このオプションを削除する前に、認証サーバが EAP-FAST で PAC を使用しないことを確認します。使用する場合は、クライアントの認証試行が失敗します。認証サーバが認証された PAC プロビジョニングをサポートする場合は、認証されていないプロビジョニングをディセーブルにすることを推奨します。認証されていないプロビジョニングはサーバの証明書を検証しないため、不正なオーセンティケータがディクショナリ攻撃を開始できます。

1 つ以上の特定の PAC ファイルを配布と認証のために手動で指定するには、[PAC ファイル（PAC Files）] パネルを選択して、[追加（Add）] をクリックします。リストから PAC ファイルを削除するには、PAC ファイルを強調表示して、[削除（Remove）] をクリックします。

[パスワード保護（Password protected）] : PAC がパスワード保護でエクスポートされた場合は、[パスワード保護（Password protected）] チェックボックスをオンにして、PAC が暗号化したファイルのパスワードと一致するパスワードを入力します。

ネットワーク クレデンシャルの定義

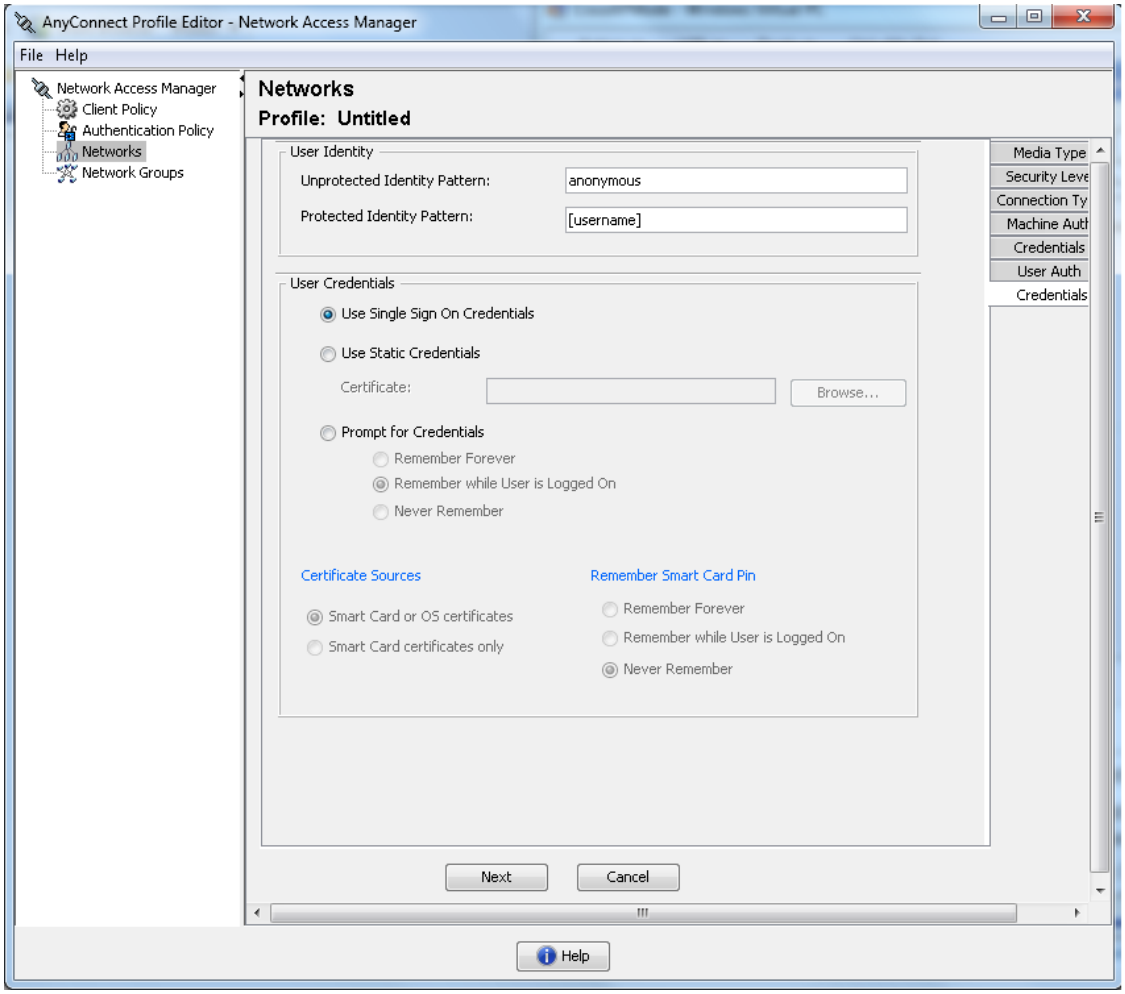
[ネットワーク クレデンシャル（Network Credentials）] では、ユーザまたはマシン クレデンシャルを確立して、信頼サーバの検証規則が確立できます。

- ユーザ クレデンシャルの設定
- マシン クレデンシャルの設定
- 信頼サーバの検証規則の設定

ユーザ クレデンシャルの設定

[クレデンシャル（Credentials）] パネルでは、目的のクレデンシャルを関連付けられたネットワーク（図 4-10 を参照）の認証で使用するために指定できます。

図 4-10　[ユーザ クレデンシャル（User Credentials）] パネル



ステップ 1　[保護されたアイデンティティ パターン（Protected Identity Pattern）] でユーザ アイデンティティを特定する必要があります。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [ユーザ名（username）]：ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [未加工（raw）]：ユーザの入力のとおりにユーザ名を指定します。
- [ドメイン（domain）]：ユーザの PC のドメインを指定します。

ユーザ接続の場合に、[ユーザ名（username）] および [ドメイン（domain）] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合は、[ユーザ名（username）] と [パスワード（password）] のプレースホルダ値はさまざまな X509 証明書プロパティから取得されます。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザ名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザ名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析さ

れます。

ユーザ証明書に基づいた認証：

- SubjectAlternativeName: UPN = userA@cisco.com
- Subject = .../CN=userA@cisco.com/...
- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco.com/...
- Subject = userA (no domain)

マシン証明書に基づいた認証：

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- クレデンシャル ソースがエンド ユーザの場合、プレースホルダの値はユーザが入力する情報から取得されます。
- クレデンシャルがオペレーティング システムから取得された場合、プレースホルダの値はログイン情報から取得されます。
- クレデンシャルがスタティックの場合は、プレースホルダを使用しないでください。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。典型的な保護されていないアイデンティティのパターンは次のとおりです。

- anonymous@[ドメイン（domain）]：値がクリア テキストで送信されるときに、ユーザ アイデンティティを隠すために、トンネリングされた方式内でよく使用されます。実際のユーザ アイデンティティは、保護されたアイデンティティとして、内部方式で提供されます。
- [ユーザ名（username）]@[ドメイン（domain）]：トンネリングされていない方式の場合

（注） 保護されていないアイデンティティはクリア テキストで送信されます。最初のクリア テキスト アイデンティティ要求または応答が改ざんされた場合は、TLS セッションが確立されるとサーバがアイデンティティを検証できないことを検出することがあります。たとえば、ユーザ ID が無効であるか、または EAP サーバが処理する領域内にない場合があります。

保護されたアイデンティティは、異なる方法でクリア テキスト アイデンティティを表します。userID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングをイネーブルにするために必要な情報のみを指定する場合があります。典型的な保護されているアイデンティティのパターンは次のとおりです。

- [ユーザ名（username）]@[ドメイン（domain）]
- ユーザのアイデンティティとして使用する実際の文字列（プレースホルダなし）

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ステップ 2　次のユーザ クレデンシャル情報をさらに提供します。

- [シングル サイン オン クレデンシャルの使用（Use Single Sign On Credentials）]：クレデンシャルをオペレーティング システムのログイン情報から取得します。ログイン クレデンシャルが失敗すると、ネットワーク アクセス マネージャは一時的に（次のログインまで）切り替わり、ユーザに GUI でクレデンシャルの入力を求めます。
- [スタティック クレデンシャルの使用（Use Static Credentials）]：ユーザ クレデンシャルをこのプロファイル エディタが提供するネットワーク プロファイルから取得します。スタティック クレデンシャルが失敗すると、ネットワーク アクセス マネージャは、新しい設定がロードされるまでクレデンシャルを再度使用しません。
- [クレデンシャルのプロンプト（Prompt for Credentials）]：クレデンシャルを次に指定されたとおりに AnyConnect GUI を使用してエンド ユーザから取得します。
  - [永久に記憶（Remember Forever）]：クレデンシャルは永久に記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。クレデンシャルはファイルに保存され、ローカル マシン パスワードを使用して暗号化されます。
  - [ユーザのログイン中は記憶（Remember while User is Logged On）]：クレデンシャルはユーザがログオフするまで記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。
  - [記憶しない（Never Remember）]：クレデンシャルは一切記憶されません。ネットワーク アクセス マネージャは、認証のためにクレデンシャル情報が必要なたびに、ユーザに入力を求めます。

ステップ 3　証明書が要求されたときに、認証のためにいずれの証明書ソースを使用するかを決定します。

- [スマート カードまたは OS の証明書（Smart Card or OS certificates）]：ネットワーク アクセス マネージャは、OS の証明書ストアまたはスマート カードで検出される証明書を使用します。
- [スマート カードの証明書のみ（Smart Card certificates only）]：ネットワーク アクセス マネージャは、スマート カードで検出される証明書のみを使用します。

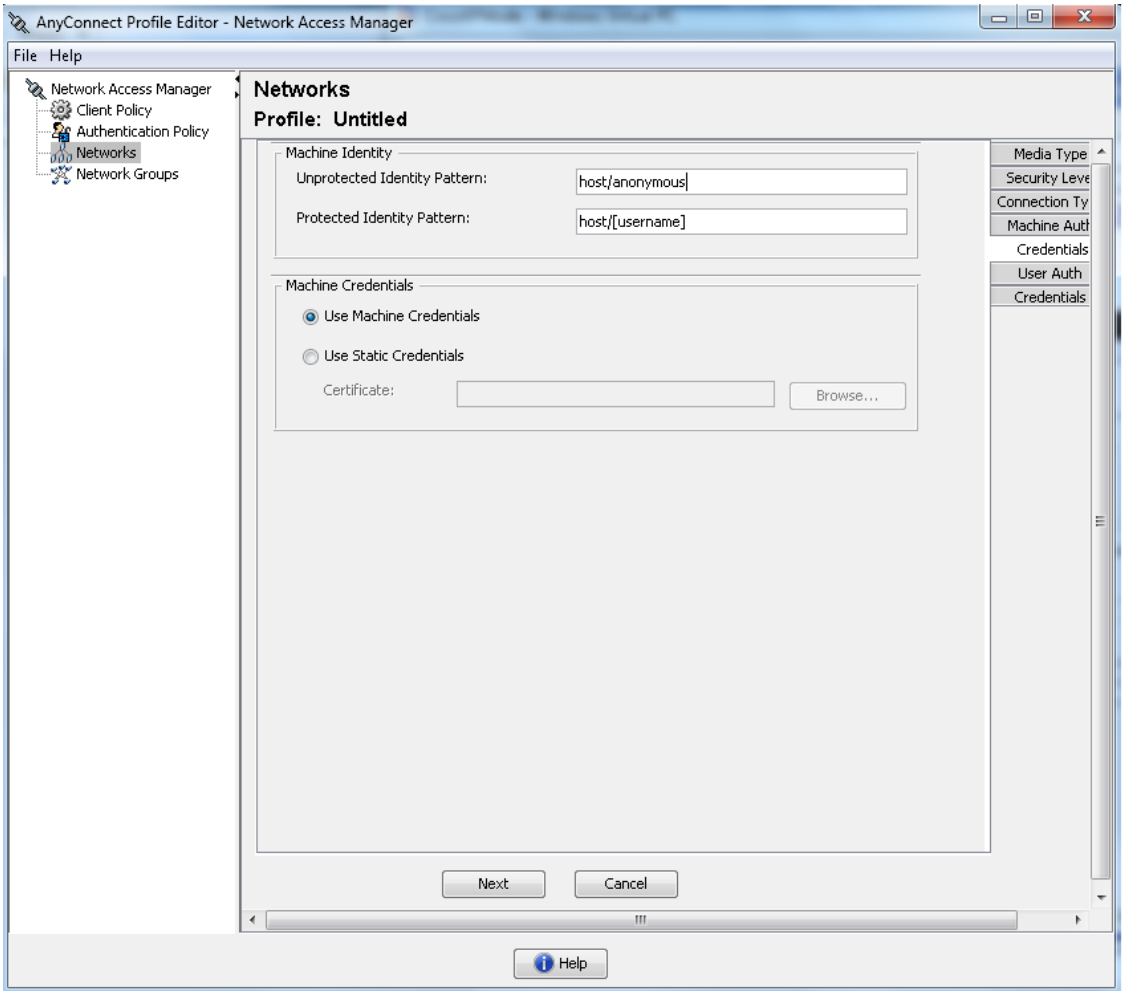
ステップ 4　[スマート カードの PIN の記憶（Remember Smart Card Pin）] パラメータでは、ネットワーク アクセス マネージャがスマート カードから証明書を取得するために使用した PIN を記憶する期間を決定します。使用できるオプションについては、ステップ 2 を参照してください。

（注）　PIN は、証明書自体よりも長く保存されることは決してありません。

マシン クレデンシャルの設定

[クレデンシャル（Credentials）] パネルでは、目的のマシン クレデンシャル（図 4-11 を参照）を指定できます。

図 4-11　　マシン クレデンシャル



ステップ 1　[保護されたアイデンティティ パターン（Protected Identity Pattern）] でマシン アイデンティティを特定する必要があります。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [ユーザ名（username）]：ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [未加工（raw）]：ユーザの入力のとおりにユーザ名を指定します。

マシン接続の場合に、[ユーザ名（username）] および [ドメイン（domain）] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合は、[ユーザ名（username）] と [パスワード（password）] のプレースホルダ値はさまざまな X509 証明書プロパティから取得されます。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザ名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザ名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析されます。

  ユーザ証明書に基づいた認証：

  - SubjectAlternativeName: UPN = userA@cisco.com
  - Subject = .../CN=userA@cisco.com/...
  - Subject = userA@cisco.com
  - Subject = .../CN=userA/DC=cisco.com/...
  - Subject = userA (no domain)

  マシン証明書に基づいた認証：

  - SubjectAlternativeName: DNS = hostA.cisco.com
  - Subject = .../DC=hostA.cisco.com/...
  - Subject = .../CN=hostA.cisco.com/...
  - Subject = hostA.cisco.com

- クライアント証明書が認証に使用されない場合、クレデンシャルはオペレーティング システムから取得されて、[ユーザ名（username）] プレースホルダは割り当てられたマシン名を表します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。典型的な保護されていないマシン アイデンティティのパターンは次のとおりです。

- host/anonymous@[ドメイン（domain）]
- マシンのアイデンティティとして送信する実際の文字列（プレースホルダなし）

保護されたアイデンティティは、異なる方法でクリア テキスト アイデンティティを表します。userID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングをイネーブルにするために必要な情報のみを指定する場合があります。典型的な保護されているマシン アイデンティティのパターンは次のとおりです。

- host/[ユーザ名（username）]@[ドメイン（domain）]
- マシンのアイデンティティとして使用する実際の文字列（プレースホルダなし）

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ステップ 2　次のマシン クレデンシャル情報をさらに提供します。

- [マシン クレデンシャルの使用（Use Machine Credentials）]：クレデンシャルをオペレーティング システムから取得します。

- [スタティック クレデンシャルの使用（Use Static Credentials）]：スタティック クレデンシャルの使用を選択する場合、展開ファイルで送信する実際のスタティック パスワードを指定できます。スタティック クレデンシャルは、証明書ベースの認証には適用されません。

信頼サーバの検証規則の設定

[サーバ ID の検証（Validate Server Identity）] オプションが [EAP] 方式に設定されている場合、[証明書（Certificate）] パネルがイネーブルになって証明書サーバまたは認証局に対する検証規則を設定できます。検証の結果によって、証明書サーバまたは認証局が信頼されるかどうかが決定されます。

証明書サーバの検証規則を定義するには、次の手順を実行します。

ステップ 1　オプション設定が [証明書フィールド（Certificate Field）] および [一致（Match）] カラムに表示されたときに、ドロップダウン矢印をクリックし、目的の設定を強調表示します。

ステップ 2　[値（Value）] フィールドに、値を入力します。

ステップ 3　規則の下で [追加（Add）] をクリックします。

ステップ 4　[信頼された機関の認証（Certificate Trusted Authority）] の部分で、次のいずれかのオプションを選択します。

- [OS にインストールされた任意のルート証明機関を信頼（Trust any Root Certificate Authority (CA) Installed on the OS）]：選択すると、ローカル マシンまたは証明書ストアのみがサーバの証明書チェーン検証の対象になります。
- [ルート証明機関（CA）を含める（Include Root Certificate Authority (CA) Certificates）]

（注）　[ルート証明機関（CA）を含める（Include Root Certificate Authority (CA) Certificates）] を選択した場合は、[追加（Add）] をクリックして CA 証明書を設定にインポートする必要があります。

ネットワーク グループの定義

[ネットワーク グループ（Network Groups）] パネルでは、ネットワーク接続を特定のグループに割り当てられます（図 4-12 を参照）。接続をグループに分類することにより、次の複数の利点がもたらされます。

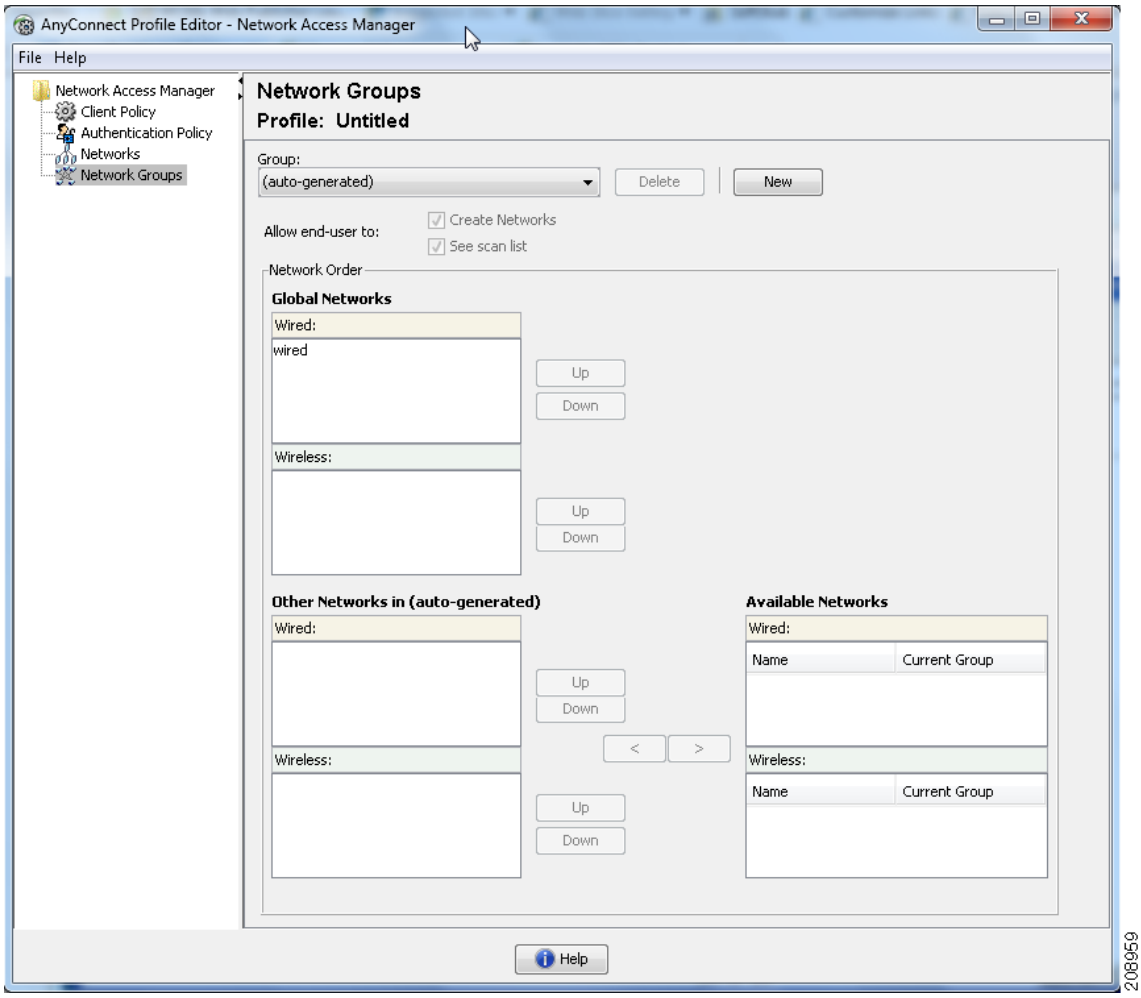
- 接続の確立試行時のユーザ エクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。この利点により、企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザ ネットワークから分離できます。

配布パッケージの一部として定義されたネットワークはロックされています。これは、ユーザが設定を編集することや、ネットワーク プロファイルを削除することを防止するためです。

ネットワークをグローバルに定義できます。グローバルに定義すると、ネットワークは [グローバル ネットワーク（Global Networks）] セクションに表示されます。このセクションは、有線とワイヤレス ネットワーク タイプの間で分割されます。このタイプのネットワークに対してのみソート順序編集を実行できます。

すべての非グローバル ネットワークは、グループ内に存在する必要があります。ネットワークが追加されていない場合、事前に定義されているデフォルト グループに追加されます。

図 4-12　　[ネットワーク グループ（Network Groups）] ウィンドウ



ステップ 1　ドロップダウン リストから選択して、[グループ（Group）] を選択します。

ステップ 2　[ネットワークの作成（Create networks）] を選択して、エンド ユーザがこのグループ内にネットワークを作成できるようにします。これをオフにした場合、展開されたときにネットワーク アクセス マネージャはこのグループからユーザ作成ネットワークをすべて削除します。これにより、ユーザがネットワーク設定を別のグループに再入力する必要が生じることがあります。

ステップ 3　[スキャン リストの表示（See scan list）] を選択して、AnyConnect GUI を使用してグループがアクティブ グループとして選択されたときに、エンド ユーザがスキャン リストを表示できるようにします。または、このチェックボックスをオフにして、ユーザによるスキャン リストの表示を制限します。たとえば、ユーザが近くのデバイスに誤って接続することを防ぐ必要がある場合に、スキャン リストへのアクセスを制限します。

（注）　これらの設定は、グループごとに適用されます。

ステップ 4　右矢印 [>] および左矢印 [<] を使用して、[グループ（Group）] ドロップダウン リストから選択したグループに対してネットワークを挿入または削除します。ネットワークが現在のグループから移動された場合は、デフォルト グループに配置されます。デフォルト グループを編集する場合、デフォルト グループからネットワークを移動できません（[>] ボタンを使用）。

（注）　指定のネットワーク内で、各ネットワークの表示名は一意である必要があります。このため、1 つのグループには同じ表示名を持つ 2 つ以上のネットワークを含められません。

ステップ 5　[上（Up）] および [下（Down）] 矢印を使用してグループ内のネットワークの優先順位を変更します。

CHAPTER 5

ホスト スキャンの設定

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility クライアントは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 モジュールのコンポーネントに含まれる、こうした情報を収集するアプリケーションです。

適応型セキュリティ アプライアンス（ASA）では、オペレーティング システム、IP アドレス、レジストリ エントリ、ローカル証明書、ファイル名など、エンドポイント属性を評価するプリログイン ポリシーを作成できます。プリログイン ポリシーの評価結果に基づいて、セキュリティ アプライアンスへのリモート アクセス接続の作成を許可するホストを制御できます。

AnyConnect 3.0 より、ホスト スキャン パッケージは AnyConnect Secure Mobility クライアントおよび Cisco Secure Desktop（CSD）の共有コンポーネントになっています。それ以前は、ホスト スキャン パッケージは CSD をインストールすることによってのみ利用可能になるコンポーネントの 1 つでした。

ホスト スキャン パッケージを CSD から分離したのは、CSD の一部として提供されていたときよりも、ユーザが頻繁にホスト スキャン サポート表を更新できるようにするためです。ホスト スキャン サポート表には、ダイナミック アクセス ポリシー（DAP）を割り当てるために使用されるアンチウイルス、スパイウェア、およびファイアウォールのアプリケーションの製品名とバージョン情報が記載されます。シスコでは、ホスト スキャン パッケージにホスト スキャン アプリケーション、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

スタンドアロン ホスト スキャン パッケージおよびポスチャ モジュールに同梱されるホスト スキャン パッケージでは、同じ機能が提供されます。シスコでは、ホスト スキャン サポート表を簡単に更新できるように、別個のホスト スキャン パッケージを提供しています。

ホスト スキャン パッケージは、現在、AnyConnect ポスチャ モジュールとともに、CSD とともに、またはスタンドアロン パッケージとして、これら 3 つの方法のいずれかで提供されます。AnyConnect ポスチャ モジュールには 2 つのタイプがあります。1 つ目のバージョンは、AnyConnect のインストールと一緒に ASA によってプッシュされます。もう 1 つのバージョンは、事前展開モジュールとして設定されます。事前展開モジュールは、ASA への初期接続を確立する前に、エンドポイントにインストールできます。

エンドポイントにインストールされたオペレーティング 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ことに加え、ホスト スキャン パッケージによって、プリログイン評価の実行、キーストローク ロガーの識別、およびエンドポイントで実行されるホスト エミュレーションと仮想マシンの検出を行うコンポーネントが提供されます。キーストローク ロガーの検出およびホスト エミュレーションと仮想マシンの検出は、CSD の機能でもありましたが、今ではホスト スキャン パッケージに組み込まれています。

しかし、ホスト スキャン パッケージは、CSD に代わるものではありません。Secure Vault が必要なお客様は、ホスト スキャン パッケージの他に CSD をインストールして、有効にする必要があります。Secure Vault 機能の詳細については、CSD 設定ガイド http://www.cisco.com/en/US/products/ps6742/products_installation_and_configuration_guides_list.html を参照してください。

AnyConnect クライアントは、Secure Desktop 内から起動することはできません。最初に ASA へのクライアントレス SSL VPN 接続を確立し、ポータル ページから AnyConnect を起動することで、ユーザは AnyConnect に接続できます。

ASA の Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイスを使用して、ホスト スキャンのインストール、アンインストール、イネーブル、およびディセーブルを行えます。ASDM の Secure Desktop Manager ツールを使用して、プリログイン ポリシーを設定できます。

ポスチャ評価および AnyConnect テレメトリ モジュールを使用するには、ホスト スキャンがホストにインストールされている必要があります。

この章は、次の内容で構成されています。

ホスト スキャン ワークフロー

以下のワークフローで説明するように、ホスト スキャンは ASA と連携して、企業ネットワークを保護します。

1. リモート デバイスでは、クライアントレス SSL VPN またはセキュリティ アプライアンスとの AnyConnect Client セッション確立が試行されます。
2. ASA はホスト スキャンをクライアントにダウンロードして、ASA とクライアントが同じバージョンのホスト スキャンを使用するようにします。
3. プリログイン評価は、リモート コンピュータについて以下のチェックを行います。
   - オペレーティング システム
   - CSD 管理者が指定するファイルの有無。
   - CSD 管理者が指定するレジストリ キーの有無。このチェックは、コンピュータが Microsoft Windows を実行している場合だけに適用されます。
   - CSD 管理者が指定するデジタル証明書の有無。このチェックについても、コンピュータが Microsoft Windows を実行している場合だけに適用されます。

- CSD 管理者が指定する IP アドレスの範囲。

4. クライアントでプリログイン評価が実行されているときに並行して、ホスト スキャンはエンドポイント アセスメントを実行し、アンチウイルス、ファイアウォール、およびアンチスパイウェアのバージョン情報を収集します。また、ダイナミック アクセス ポリシーで指定したレジストリ キー、ファイル、およびプロセスのスキャンも行います。
5. プリログイン評価の結果に応じて、次のイベントのいずれかが発生します。
   - プリログイン評価が実行され、[ログインが拒否されました（Login Denied）] エンドノードで終了するシーケンスを経由する場合は、リモート コンピュータに「ログインが拒否されました（Login Denied）」メッセージが表示されます。この場合、ASA とリモート デバイス間の対話は停止します。
   - プリログイン評価は、プリログイン ポリシー名をデバイスに割り当て、そのプリログイン ポリシー名を ASA に報告します。
6. ホスト スキャンは、プリログイン評価後にリモート コンピュータが割り当てられたプリログイン ポリシーの設定に基づいて、リモート コンピュータのキーストローク ロガーおよびホスト エミュレーションをチェックします。
7. 保証対象であり、Advanced Endpoint Assessment のライセンスがある場合、アンチウイルス、ファイアウォール、またはアンチスパイウェアの修復が実行されます。
8. ユーザがログインします。
9. ASA は、通常、3. で収集された認証データとともに、4. で収集されたエンドポイント属性の設定基準（これには、プリログイン ポリシーやホスト スキャンの結果と同様の値が含まれる場合があります）を使用して、ダイナミック アクセス ポリシーをセッションに適用します。
10. ユーザ セッションが終了した後、ホスト スキャンが終了し、キャッシュ クリーナがクリーンアップ機能を実行します。

AnyConnect ポスチャ モジュールで使用可能な機能

プリログイン評価

プリログイン評価は、ユーザが ASA に接続した後、かつログインする前に、実行されます。この評価では、ファイル、デジタル証明書、OS、IP アドレス、および Microsoft Windows レジストリ キーについてリモート デバイスをチェックできます。

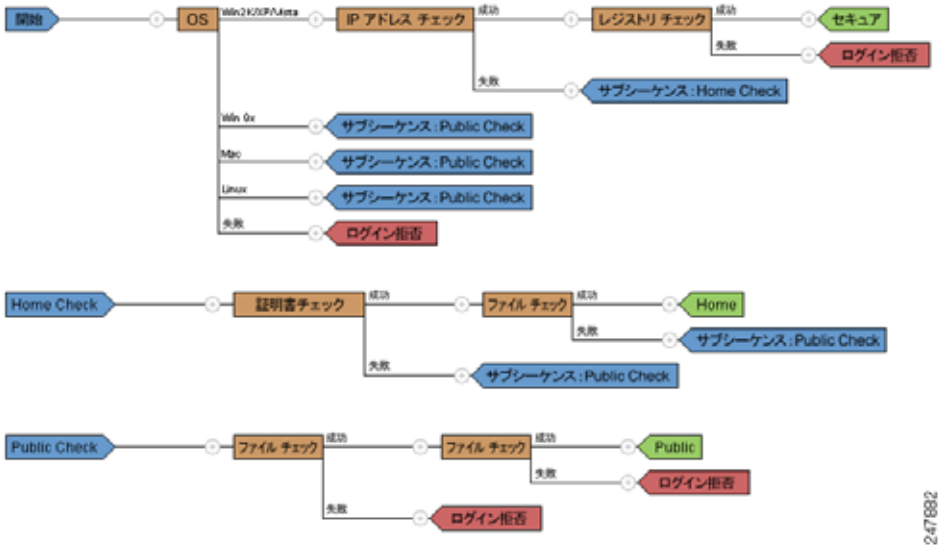
管理者とホスト スキャンのインターフェイスとなる Secure Desktop Manager では、プリログイン評価モジュールを簡単に設定できるグラフィカル シーケンス エディタが提供されます。

プリログイン評価モジュールを設定するときに、ホスト スキャン管理者は「シーケンス」と呼ばれるノードのブランチを作成します。各シーケンスは [スタート（Start）] ノードで始まり、続いてエンドポイント チェックが実行されます。チェックの結果により、別のエンドポイント チェックを実行するかどうか、またはエンドノードでシーケンスを終了するかどうかを判定します。

エンドノードでは、「ログインが拒否されました（Login Denied）」メッセージを表示するかどうか、プリログイン ポリシーをデバイスに割り当てるかどうか、または「サブシーケンス」と呼ばれるセカンダリ チェックのセットを実行するかどうかを判定します。「*サブシーケンス*」は、シーケンスの連続で、通常、詳細なエンドポイント チェックとエンドノードで構成されます。この機能は、以下の処理を行う場合に便利です。

- 特定のケースで、チェックのシーケンスを再利用する。
- サブシーケンス名を使用して文書化するといった全体的な目的を持つ条件セットを作成する。
- グラフィカル シーケンス エディタが占める水平方向の領域を制限する。

図 5-1　　完全なプリログイン評価の例

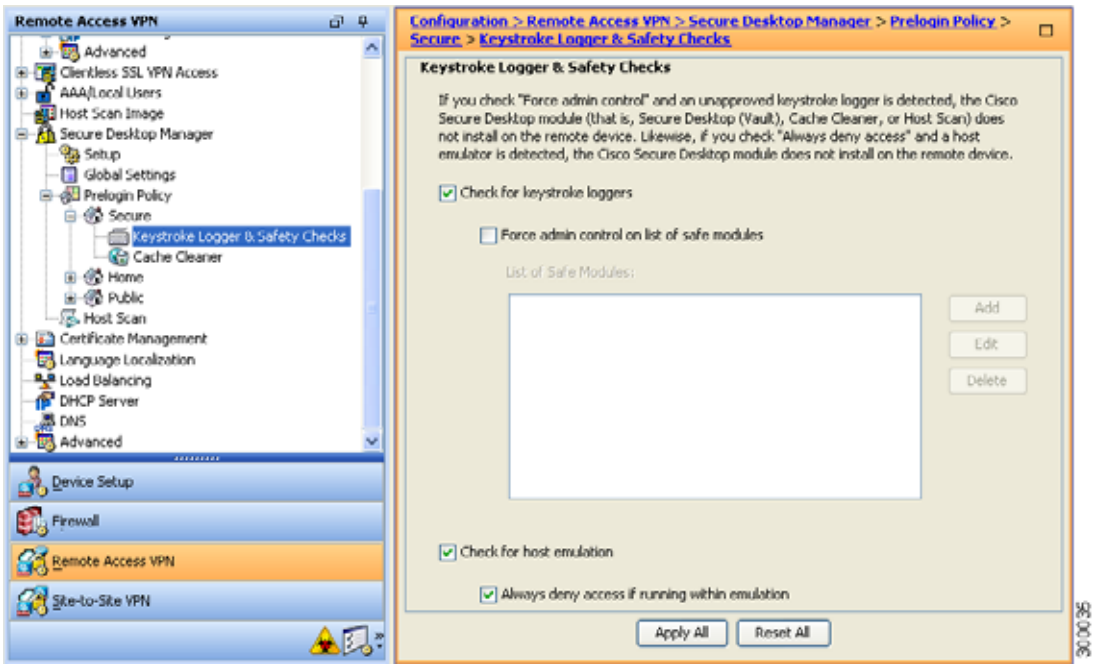


プリログイン ポリシー

グラフィカル シーケンス エディタで設定されたプリログイン評価（図 5-1）のチェックの結果によって、プリログイン評価が特定のプリログイン ポリシーに割り当てられるか、または拒否されるリモート アクセス接続となるかが判明します。

ポリシーを作成するたびに、Secure Desktop Manager によりポリシーにちなんだ名前が追加されます。ポリシーのメニューごとに、ポリシーに対して一意な設定を割り当てることができます。これらの設定によって、キーストローク ロガー検出、ホスト エミュレーション検出、またはキャッシュ クリーナが、ポリシーに割り当てられたプリログイン条件に一致するリモート デバイスにインストールされるかどうかが決定します。管理者は通常、これらのモジュールを企業以外のコンピュータに割り当て、セッション終了後の企業データやファイルへのアクセスを防止します。

図 5-2　プリログイン ポリシー



キーストローク ロガー検出

ユーザが入力したキー入力を記録するプロセスまたはモジュールのスキャンを選択したプリログイン ポリシーを設定して、疑わしいキー入力ロギング アプリケーションが存在する場合は、VPN アクセスを拒否できます。

デフォルトでは、キーストローク ロガー検出はすべてのプリログイン ポリシーでディセーブルになっています。Secure Desktop Manager を使用して、キーストローク ロガー検出をイネーブルまたはディセーブルにできます。安全なキーストローク ロガーを指定するか、またはリモート コンピュータ上のキャッシュ クリーナまたはホスト スキャンを実行するための条件としてスキャンで識別されたキーストローク ロガーをリモート ユーザに対話的に承認させることができます。

イネーブルにすると、キーストローク ロガー検出はキャッシュ クリーナまたはホスト スキャンとともにリモート コンピュータにダウンロードされます。ダウンロードが完了したキーストローク ロガー検出は、OS が Windows で、かつユーザが管理者権限を持っている場合に限り実行されます。

関連モジュールは、スキャンに問題がない場合、または、管理者がユーザに管理作業を割り当て、スキャンで識別されたアプリケーションをユーザが承認する場合に限り実行されます。

（注）　キーストローク ロガー検出は、エンドユーザが管理者権限でログインしている限り、ユーザ モードとカーネル モードの両方のロガーに適用されます。

キーストローク ロガー検出は、32 ビット版 Microsoft Windows OS 環境に限り実行できます。「キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出では、潜在的に悪意のあるキーストローク ロガーのすべてを検出できない場合があります。ハードウェアのキー入力ロギング デバイスは検出されません。

ホスト エミュレーション検出

プリログイン ポリシーのもう 1 つの機能であるホスト エミュレーション検出では、リモートの Microsoft Windows オペレーティング システムがバーチャライゼーション ソフトウェア上で実行されているかどうかを判断します。Secure Desktop Manager を使用して、この機能をイネーブルまたはディセーブルにできます。また、ホスト エミュレータが存在する場合にアクセスを拒否したり、ユーザに検出を報告し、続行するか終了するかの判断をユーザに委ねることができます。

デフォルトでは、ホスト エミュレーション検出はすべてのプリログイン ポリシーでディセーブルになっています。この機能をイネーブルにすると、Secure Desktop、Cache Cleaner、またはホスト スキャンと共にリモート コンピュータにダウンロードされます。ダウンロードが完了すると、まずホスト エミュレーション検出が実行され、キーストローク ロガー検出の実行が設定されている場合は同時に実行されます。続いて、次のいずれかの条件に当てはまる場合は、関連モジュールが実行されます。

- ホストがエミュレータ（または、バーチャライゼーション ソフトウェア）上で実行されていない。
- アクセスを常に拒否するように設定しておらず、ユーザが検出されたホスト エミュレータを承認する。

「キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム

キーストローク ロガー検出およびホスト エミュレーション検出は、以下のオペレーティング システムで実行します。

- x86（32 ビット）の Windows Vista SP1 および SP2

  SP1 および SP2 を使用しない Windows Vista を実行するコンピュータの場合、KB935855 をインストールする必要があります。

- x86（32 ビット）の Windows XP SP2 および SP3

（注）　Secure Desktop、キーストローク ロガー検出、およびホスト エミュレーション検出は Windows 7 ではサポートされません。

Cache Cleaner

Secure Desktop の代替機能となる Cache Cleaner は機能面で制限がありますが、多くのオペレーティング システムをサポートする柔軟性を備えています。Cache Cleaner では、クライアントレス SSL VPN または AnyConnect Client セッション終了時に、ブラウザ キャッシュから情報を削除しようとします。この情報には、入力されたパスワード、オートコンプリート テキスト、ブラウザでキャッシュされたファイル、セッション時に行われたブラウザ設定の変更、およびクッキーが含まれます。

Cache Cleaner は、Microsoft Windows、Apple Mac OS、Linux 上で実行されます。システム要件の詳細については、『Cisco Secure Desktop Release Notes』を参照してください。

これは、通常、キャッシュ クリーナが展開され、エンドポイントがクライアントレス SSL VPN 接続を作成しようとするとき、または Web 起動を使用する AnyConnect を起動しようとするときのイベントのシーケンスになります。

ステップ 1　ユーザがブラウザに URL を入力すると、エンドポイントは ASA に接続します。

ステップ 2　ホスト スキャンはプリログイン評価を実行します。

ステップ 3　エンドポイントがプリログイン評価を通過することが前提ですが、AnyConnect の認証が開始されます。ユーザはパスワードを入力するか、認証用の証明書を使用できます。

ステップ 4　[現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）（Clean the whole cache in addition to the current session cache (IE only)）] をイネーブルにしないで Internet Explorer を実行しているユーザ、または Safari や Firefoxfor を実行しているユーザの場合、ユーザ認証の後、約 1 分間、キャッシュ クリーナによってブラウザのキャッシュのスナップショットが取られます。

ステップ 5　ユーザが操作すると、ブラウザは情報をキャッシュします。

ステップ 6　ユーザが VPN セッションをログアウトすると、以下が実行されます。

- [現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）（Clean the whole cache in addition to the current session cache (IE only)）] をイネーブルにして Internet Explorer を実行しているユーザの場合、キャッシュ クリーナはブラウザのすべてのキャッシュを削除しようとします。
- [現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）（Clean the whole cache in addition to the current session cache (IE only)）] をイネーブルにしないで Internet Explorer を実行しているユーザ、または Safari や Firefoxfor を実行しているユーザの場合、キャッシュ クリーナはブラウザのすべてのキャッシュの削除を試行してから、そのキャッシュに対して取ったスナップショットを復元します。

  機密情報をコンピュータに復元しないようにするため、セッションが終了した後、ブラウザを閉じてから、ブラウザのキャッシュを手動で消去することを推奨します。

（注）　[現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）（Clean the whole cache in addition to the current session cache (IE only)）] オプションをイネーブルにしてキャッシュ クリーナを設定することを推奨します。

ホスト スキャン

ホスト スキャンは、ユーザが ASA に接続した後、かつログインする前に、リモート デバイス上にインストールされるパッケージです。ホスト スキャンは、CSD 管理者が設定する基本ホスト スキャン モジュール、エンドポイント アセスメントモジュール、Advanced Endpoint Assessment モジュールの任意の組み合わせで構成されます。ホスト スキャンは、Microsoft Windows、Apple Mac OS X、および Linux 上で実行されます。詳細な要件については、「システム要件」（P.5-11）を参照してください。

ホスト スキャン パッケージは、CSD とバンドルされて、スタンドアロン モジュールとして、また AnyConnect 3.0 クライアントのポスチャ モジュールの一部として提供されます。

基本ホスト スキャン機能

ホスト スキャンは、CSD またはホスト スキャン/CSD が ASA でイネーブルにされている場合に、Cisco クライアントレス SSL VPN または AnyConnect クライアント セッションを確立するリモート デバイスのオペレーティング システムおよびサービス パックを自動的に識別します。

Secure Desktop Manager を使用して、特定のプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスについて、エンドポイントを検査するようにホスト スキャンを設定することもできます。Secure Desktop Manager は、ASA 上で Adaptive Security Device Manager（ASDM）と統合されます。

ホスト スキャンは、ユーザがコンピュータにログオンする前に、これらすべての検査を実行します。

ホスト スキャンは、オペレーティング システムとサービス パックの情報とともに、収集するように設定されたプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスをエンドポイントから収集した後、その情報を ASA に送信します。ASA では、その情報は、企業所有のコンピュータ、個人用コンピュータ、パブリック コンピュータを区別するために使用されます。また、この情報はプリログイン評価にも使用されます。詳細については、「プリログイン評価」（P.5-3）を参照してください。

また、ホスト スキャンは、設定した DAP エンドポイント条件と照合して評価するために、以下の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、Linux のビルド
- Microsoft Windows が実行されている接続ホスト上でアクティブなリスニング ポート
- 接続ホスト上にインストールされている CSD コンポーネント
- Microsoft サポート技術情報（KB）番号

DAP および Lua 表現の詳細については、「Dynamic Access Policies との統合」（P.5-10）および『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

エンドポイント アセスメント

エンドポイント アセスメントは、ホスト スキャンの拡張機能であり、アンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールの大規模な収集について、リモート コンピュータを検査します。ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して要件を満たすようにエンドポイント条件を組み合わせることができます。DAP の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

Advanced Endpoint Assessment：アンチウイルス、アンチスパイウェア、およびファイアウォールの修復

ASA にインストールされた **Advanced Endpoint Assessment** ライセンスを購入すると、以下のホスト スキャンの高度な機能を使用できます。

修復

Windows、Mac OS X、および Linux のデスクトップでは、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

アンチウイルス：Advanced Endpoint Assessment は、アンチウイルス ソフトウェアの以下のコンポーネントを修復しようとします。

- ファイル システム保護の強制：アンチウイルス ソフトウェアがディセーブルの場合に、Advanced Endpoint Assessment はこのコンポーネントをイネーブルにできます。
- ウイルス定義更新の強制：Advanced Endpoint Assessment の設定で定義された日数の間、アンチウイルス定義が更新されなかった場合に、Advanced Endpoint Assessment は、ウイルス定義の更新を開始しようとします。

アンチスパイウェア：Advanced Endpoint Assessment の設定で定義された日数の間、アンチスパイウェア定義が更新されなかった場合に、Advanced Endpoint Assessment は、アンチスパイウェア定義の更新を開始しようとします。

パーソナル ファイアウォール：ファイアウォール設定およびルールが Advanced Endpoint Assessment の設定で定義された要件を満たしていない場合、Advanced Endpoint Assessment モジュールは、それらを再設定しようとします。

- ファイアウォールは、イネーブルまたはディセーブルにできます。
- アプリケーションを実行しないように、または実行するようにできます。
- ポートをブロックする、または開くこともできます。

（注） この機能は、すべてのパーソナル ファイアウォールでサポートされているわけではありません。

エンドユーザがアンチウイルスまたはパーソナル ファイアウォールをディセーブルにした場合、正常に VPN 接続を確立した後、Advanced Endpoint Assessment の機能は約 60 秒以内にそのアプリケーションを再びイネーブルにしようとします。

ホスト スキャン サポート表

ホスト スキャン サポート表に、プリログイン ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォールのアプリケーションの製品名およびバージョン情報が記載されます。ホスト スキャンおよびホスト スキャン サポート表は、ホスト スキャン パッケージに同梱されます。

AnyConnect Secure Mobility Client のこのリリースでは、ホスト スキャン パッケージは、Cisco Secure Desktop（CSD）とは別にアップロードできます。これは、CSD をインストールしなくてもホスト スキャンの機能を展開できること、また、最新のホスト スキャン パッケージに更新することで、ホスト スキャン サポート表を更新できることを意味します。

ホスト スキャン サポート表は、cisco.com（http://www.cisco.com/en/US/products/ps10884/products_device_support_tables_list.html）からダウンロードできます。

これらのサポート表は、Microsoft Excel、Microsoft Excel Viewer、または OpenOffice を使用して表示できます。Firefox、Chrome、Safari などのブラウザでは、ダウンロードの最適な操作性が提供されます。

ホスト スキャン用のアンチウイルス アプリケーションの設定

アンチウイルス アプリケーションが、ポスチャ モジュールやホスト スキャン パッケージを含む一部のアプリケーションの動作を誤って悪意のあるものと判断する場合があります。ポスチャ モジュールまたはホスト スキャン パッケージをインストールする前に、以下のホスト スキャン アプリケーションをアンチウイルス ソフトウェアの「ホワイトリスト」に設定するか、セキュリティ例外を設けます。

- cscan.exe
- ciscod.exe
- cstub.exe

Dynamic Access Policies との統合

ASA では、ホスト スキャンの機能が Dynamic Access Policies（DAP）に統合されます。設定に応じて、ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされるホスト スキャンの機能には、OS 検出、プリログイン ポリシー、基本ホスト スキャン結果、およびエンドポイント アセスメントがあります。

（注）　ホスト スキャンの機能をイネーブルにするには、AnyConnect Premium ライセンスを ASA にインストールする必要があります。

管理者は、セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

ポスチャ モジュールとスタンドアロン ホスト スキャン パッケージの相違点

AnyConnect ポスチャ モジュールは、ASA を使用してエンドポイントに展開できます。または、エンドポイントが ASA への初期接続を行う前に、事前展開キットを使用してエンドポイントにインストールできます。

ポスチャ モジュールには、ホスト スキャン パッケージ、プリログイン評価、キーストローク ロガー検出、ホスト エミュレーション検出、キャッシュ クリーナ、およびホスト スキャン アプリケーションが必要とするいくつかのその他のモジュールが含まれます。ポスチャ モジュールを展開することにより、エンドポイントのユーザが管理者ではなくても、ホスト スキャンは特権動作を実行できます。また、その他の AnyConnect モジュールをホスト スキャンを使用して開始することもできます。

スタンドアロン ホスト スキャン パッケージは、ホスト スキャン エンジン、プリログイン評価モジュール、キーストローク ロガー検出、およびホスト エミュレーション検出を提供します。

AnyConnect ポスチャ モジュールの依存関係およびシステム要件

AnyConnect ポスチャ モジュールには、ホスト スキャン パッケージやその他のコンポーネントが含まれています。

依存関係

AnyConnect Secure Mobility Client をポスチャ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

これらの AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- ホスト スキャン
- SCEP 認証
- AnyConnect テレメトリ モジュール

ホスト スキャン、CSD、および AnyConnect Secure Mobility Client の相互運用性

注意　ホスト スキャンを AnyConnect Secure Mobility Client バージョン 3.0.x で展開する場合、AnyConnect Secure Mobility Client は、同じバージョン番号、または自分よりも新しいバージョン番号のホスト スキャンが必要です。

Cisco Secure Desktop（CSD）バージョン 3.5 以前を ASA でイネーブルにしていて、展開している AnyConnect Secure Mobility Client 3.0.x のバージョンに一致するまたはそれ以降のホスト スキャン パッケージにアップグレードしない場合、プリログイン評価は失敗し、ユーザは VPN セッションを確立できません。ASA は、ASA でイネーブルにされているホスト スキャン パッケージに一致するように、エンドポイントのホスト スキャン パッケージを自動的にダウングレードするため、AnyConnect 3.0.x ポスチャ モジュールがエンドポイントに事前展開されていても、この問題は発生します。

AnyConnect 2.5.3005 以前の場合は、Host Scan と互換性がありません。

システム要件

ポスチャ モジュールは、以下のプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）

（注）　ホスト スキャンは、32 ビット アプリケーションで、コア 32 ビット ライブラリを 64 ビット版 Linux オペレーティング システムにインストールする必要があります。ホスト スキャンは、インストールされた時点で、これらの 32 ビット ライブラリを提供しません。まだプロビジョニングしていない場合、お客様は自分で 32 ビット ライブラリをエンドポイントにインストールする必要があります。

ライセンシング

ポスチャ モジュールには、以下の AnyConnect のライセンシング要件があります。

- AnyConnect Premium ライセンスは、基本ホスト スキャン、エンドポイント アセスメント、および Advanced Endpoint Assessment を含むホスト スキャンによって提供されるすべての機能に対して必要です。
- Advanced Endpoint Assessment ライセンスは、以下の機能が必要とする追加のライセンスです。

- 修復
- モバイル デバイス管理

Advanced Endpoint Assessment をサポートするためのアクティベーション キーの入力

Advanced Endpoint Assessment には、エンドポイント アセスメントのすべての機能が含まれており、バージョン要件を満たすために非準拠のコンピュータのアップデートを試行するように設定できます。次の手順に従い、Advanced Endpoint Assessment をサポートするために、シスコからキーを取得したら、ASDM を使用してキーのアクティベーションを行います。

ステップ 1　[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [アクティベーション キー（Activation Key）] を選択します。

ステップ 2　[新規アクティベーション キー（New Activation Key）] フィールドにキーを入力します。

ステップ 3　[アクティベーション キーの更新（Update Activation Key）] をクリックします。

ステップ 4　[ファイル（File）] > [実行コンフィギュレーションをフラッシュに保存する（Save Running Configuration to Flash）] を選択します。

Advanced Endpoint Assessment のエントリが表示され、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [ホスト スキャン（Host Scan）] ペインの [ホスト スキャン拡張（Host Scan Extensions）] の領域内の [設定（Configure）] ボタンが有効になります。[ホスト スキャン（Host Scan）] ペインは、CSD がイネーブルになっている場合に限りアクセスできます。

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*-k9.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-win-*version*-k9.pkg** は、AnyeConnct Secure Mobility パッケージをアップロードすることにより、アップロードできます。
- **csd_version-k9.pkg** は、Cisco Secure Desktop パッケージをアップロードすることによってアップロードできます。

表 5-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
hostscan-*version*-k9.pkg	このファイルには、ホスト スキャン イメージ、ホスト スキャン サポート表、プリログイン評価モジュール、キャッシュ クリーナ、キーストローク ロガー検出、およびホスト エミュレーション検出が含まれます。
anyconnect-win-*version*-k9.pkg	このパッケージには、hostscan-*version*-k9.pkg ファイルに含まれるすべての Cisco AnyConnect Secure Mobility Client の機能が含まれます。

表 5-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン サポート表、Secure Desktop（Vault）、キャッシュ クリーナ、キーストローク ロガー検出、ホスト エミュレーション検出など、すべての Cisco Secure Desktop 機能が含まれます。

ASA 上に複数ロードされた場合にイネーブルになるホスト スキャン イメージ

ホスト スキャン イメージは、ホスト スキャン パッケージに同梱されます。このイメージは、スタンドアロン ホスト スキャン パッケージ、完全な AnyConnect Secure Mobility Client パッケージ、および Cisco Secure Desktop からエンドポイントに展開できます。ASA にインストールしたライセンスの内容によっては、ASA にこれらのすべてのパッケージをロードできます。この場合、ASA は、ホスト スキャン イメージとして最初に指定したイメージをイネーブルにします。1 つも指定しなかった場合、ASA は Cisco Secure Desktop からホスト スキャンの機能をイネーブルにします。「ホスト スキャンのインストールまたはアップグレード」（P.5-16）を参照してください。

ホスト スキャン パッケージをアンインストールすると、ASA はそのホスト スキャン イメージをイネーブルにできなくなります。

以下のシナリオは、複数ロードされた場合に、ASA が配布するホスト スキャン パッケージについて説明します。

- ASA にスタンドアロン ホスト スキャン パッケージをインストールし、それをホスト スキャン イメージとして指定して、CSD/hostscan をイネーブルにしている場合、ASA はスタンドアロン ホスト スキャン パッケージを配布します。
- ASA にスタンドアロン ホスト スキャン パッケージをインストールして、それをホスト スキャン イメージとして指定し、また ASA に CSD イメージをインストールして、CSD/hostscan をイネーブルにしている場合、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- ASA にホスト スキャン イメージをインストールしたが、それをイネーブルにはせず、また ASA に CSD イメージをインストールして、CSD/hostscan をイネーブルにしている場合、ホスト スキャン イメージがアンインストールされていないため、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- ASA に AnyConnect Secure Mobility Client パッケージをインストールし､それをホスト スキャン イメージとして指定した場合、ASA はそのパッケージからホスト スキャン イメージを配布します。
- ASA に AnyConnect Secure Mobility Client パッケージ ファイルをインストールしたが､それをホスト スキャン イメージとして指定しない場合、ASA はその AnyConnect パッケージに関連付けられたホスト スキャン パッケージを配布しません。ASA は、インストールされたホスト スキャン パッケージまたは CSD パッケージを配布し、提供される CSD はイネーブルにされます。

AnyConnect ポスチャ モジュールおよびホスト スキャンの展開

ポスチャ モジュールおよびホスト スキャンには、2 つの異なる展開シナリオがあります。

Pre-Deployment. 事前展開方式を使用する場合、エンドポイントが ASA への接続を確立しようとする前に、AnyConnect クライアントおよびポスチャ モジュールをインストールします。事前展開のポスチャ モジュール パッケージには、ポスチャ属性や「AnyConnect ポスチャ モジュールで使用可能な機能」（P.5-3）で説明されている機能を提供するアプリケーションを収集するために使用するすべてのコンポーネント、ライブラリ、およびサポート表が含まれています。ASA にインストールされている AnyConnect クライアントおよびポスチャ モジュールの同じバージョンをエンドポイントに事前展開する場合、エンドポイントが ASA に接続するときに、追加のポスチャ モジュールが ASA からプッシュされることはありません。

Web-Deployment. Web 展開方式を使用する場合、エンドポイントが ASA に接続するときに、ASA は AnyConnect クライアントおよびポスチャ モジュールをエンドポイントにプッシュします。可能な限り短時間かつ効率的にダウンロードを実行するために、ASA は必須のポスチャ モジュール ファイルのみをダウンロードします。

エンドポイントが再び接続するときに、必須のポスチャ モジュール ファイルが、エンドポイント アセスメントを実行するために必要な他のライブラリまたはファイルを判別し、それらのファイルを ASA から取得します。たとえば、ポスチャ モジュールは、Norton アンチウイルスのあるバージョンがエンドポイントで実行されているために、すべての Norton アンチウイルス ソフトウェアのホスト スキャン サポート表を取得する場合があります。ポスチャ モジュールは必要とする追加ファイルを取得した後、エンドポイント アセスメントを実行し、ASA に属性を転送します。エンドポイントの属性がダイナミック アクセス ポリシー（DAP）ルールを満たしていると、ASA はエンドポイントに接続を許可します。DAP を満たした結果に従って、ポスチャ モジュールの残りの部分をエンドポイントにプッシュするかどうかについて、ASA を設定できます。

ポスチャ モジュール全体をエンドポイントに Web 展開しない場合、1 つのポスチャ ファイルのみをエンドポイントにダウンロードする、またエンドポイント アセスメントを実行するために必要なホスト スキャン ライブラリのみを要求する制限付き Web 展開を実行できます。このシナリオでは、非常に短い時間で ASA からエンドポイントにダウンロードできますが、Advanced Endpoint Assessment を実行する機能やアンチウイルス、アンチスパイウェア、またはファイアウォールの修復タスクを実行する機能は使用できなくなります。

AnyConnect ポスチャ モジュールの事前展開

ポスチャ モジュールを事前展開する場合、AnyConnect クライアントが ASA への初期接続を行う前に、そのポスチャ モジュールをエンドポイントにインストールします。

ポスチャ モジュールをインストールする前に、AnyConnect Secure Mobility Client をエンドポイントにインストールする必要があります。Web 展開方式および事前展開方式を使用して、AnyConnect Secure Mobility Client およびポスチャ モジュールをインストールする手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。

表 5-2 では、ポスチャ モジュールの事前展開キットがリストされています。

表 5-2　ポスチャ モジュールの Pre-Deployment キット

ファイル	説明
Windows	anyconnect-posture-win-*version*-pre-deploy-k9.msi
Linux	anyconnect-linux-*version*-posture-k9.tar.gz
Mac OS X	anyconnect-macosx-posture-i386-*version*-i386-k9.dmg

ASA でのホスト スキャンのインストールおよびイネーブル化

以下のタスクでは、ASA 上でのホスト スキャンのインストールとイネーブル化について説明します。

- 最新のホスト スキャン エンジン更新のダウンロード
- ホスト スキャンのインストールまたはアップグレード
- ASA でのホスト スキャンのイネーブル化またはディセーブル化
- ホスト スキャンのアンインストール
- AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

最新のホスト スキャン エンジン更新のダウンロード

最新の Cisco ホスト スキャン エンジンの更新をダウンロードするには、Cisco.com に登録されたユーザである必要があります。

ステップ 1　次のリンクをクリックして、Cisco VPN Client ツールのソフトウェア ダウンロード エリアに移動します。

http://www.cisco.com/cisco/software/release.html?mdfid=282414594&flowid=4470&softwareid=282364364&release=Engine%20Updates&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　製品ディレクトリ ツリーの [最新リリース（Latest Releases）] を展開します。

ステップ 3　[エンジンの更新（Engine Updates）] をクリックします。

ステップ 4　右側の列で、**hostscan_3.0.xxxx-k9.pkg** の最新バージョンを探し、[今すぐダウンロード（Download Now）] をクリックします。

ステップ 5　cisco.com クレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 6　[ダウンロードに進む（Proceed with Download）] をクリックします。

ステップ 7　エンド ユーザ ライセンス契約書を読み、[同意（Agree）] をクリックします。

ステップ 8　ダウンロード マネージャ オプションを選択し、[ダウンロード（download）] リンクをクリックして、ダウンロードを続行します。

ホスト スキャンのインストールまたはアップグレード

以下の手順を使用して、ASA での新規ホスト スキャン イメージのアップロードまたはアップグレード、およびイネーブル化を実行します。このイメージを使用して、AnyConnect のホスト スキャンの機能をイネーブルにするか、または Cisco Secure Desktop（CSD）の既存の展開のホスト スキャン サポート表をアップグレードします。

スタンドアロン ホスト スキャン パッケージまたは AnyConnect Secure Mobility Client バージョン 3.0 以降のパッケージをフィールドに指定できます。

以前に、CSD イメージを ASA にアップロードしたことがある場合、指定するホストスキャン イメージは、その CSD パッケージに同梱されていた既存のホスト スキャン ファイルをアップグレードまたはダウングレードします。

ホスト スキャンをインストールまたはアップグレードした後に、セキュリティ アプライアンスを再起動する必要はありませんが、Adaptive Security Device Manager（ASDM）の Secure Desktop Manager ツールにアクセスするには、ASDM を終了して再起動する必要があります。

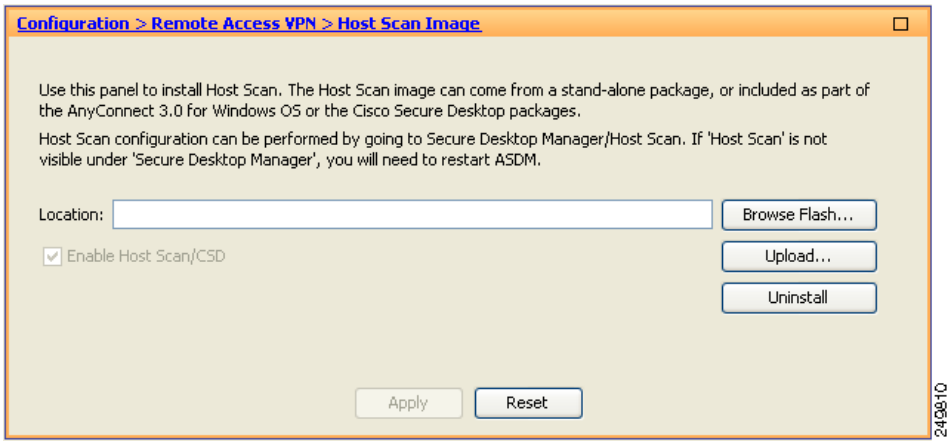
（注）　ホスト スキャンには、AnyConnect Secure Mobility Client Premium ライセンスが必要です。

ステップ 1　「最新のホスト スキャン エンジン更新のダウンロード」（P.5-15）を使用して、最新バージョンのホスト スキャン パッケージをダウンロードします。

（注）　ソフトウェアをダウンロードするには、Cisco.com のアカウントを使用してログインする必要があります。

ステップ 2　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。ASDM は [ホスト スキャン イメージ（Host Scan Image）] パネル（図 5-3）を開きます。

図 5-3　ホスト スキャン イメージ パネル



ステップ 3　[アップロード（Upload）] をクリックして、ホスト スキャン パッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。

ステップ 4　[イメージのアップロード（Upload Image）] ダイアログボックスで [ローカル ファイルの参照（Browse Local Files）] をクリックし、ローカル コンピュータのホスト スキャン パッケージを検索します。

ステップ 5　手順 1 でダウンロードした **hostscan_*version*.pkg** ファイルまたは **anyconnect-win-*version*-k9.pkg** ファイルを選択し、[選択（Select）] をクリックします。選択したファイルへのパスは、[ローカル ファイルのパス（Local File Path）] フィールドに表示され、[フラッシュ ファイルのシステム パス（Flash File System Path）] フィールドには、ホスト スキャン パッケージの宛先パスが反映されます。ASA に複数のフラッシュ ドライブがある場合、[フラッシュ ファイルのシステム パス（Flash File System Path）] を編集して別のフラッシュ ドライブを指定できます。

ステップ 6　[ファイルのアップロード（Upload File）] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。[情報（Information）] ダイアログボックスには、次のメッセージが表示されます。

```
File has been uploaded to flash successfully.
```

ステップ 7　[OK] をクリックします。

ステップ 8　[アップロードしたイメージの使用（Use Uploaded Image）] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードしたホスト スキャン パッケージ ファイルを使用します。

ステップ 9　[ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] がまだオフになっている場合、オンにします。

ステップ 10　[適用（Apply）] をクリックします。

（注）　ASA 上で AnyConnect Essentials がイネーブルになっている場合、ホスト スキャンおよび CSD は AnyConnect Essentials では機能しないというメッセージが表示されます。AnyConnect Essentials を**ディセーブル**にするか、**保持**するかを選択します。

ステップ 11　[保存（Save）] をクリックします。

ASA でのホスト スキャンのイネーブル化またはディセーブル化

ASDM を使用してホスト スキャン イメージを最初にアップロードまたはアップグレードするときに、その手順の一環としてイメージをイネーブルにします。「ASA でのホスト スキャンのインストールおよびイネーブル化」（P.5-15）を参照してください。

それ以外の場合、ASDM を使用してホストスキャン イメージをイネーブルまたはディセーブルにするには、以下の手順に従います。

ステップ 1　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。ASDM は [ホスト スキャン イメージ（Host Scan Image）] パネル（図 5-3）を開きます。

ステップ 2　[ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] をオンにして、ホスト スキャンをイネーブルにする、または [ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] をオフにしてホスト スキャンをディセーブルにします。

ステップ 3　[適用（Apply）] をクリックします。

ステップ 4　[保存（Save）] をクリックします。

ASA 上での CSD の有効化または無効化

Cisco Secure Desktop（CSD）をイネーブルにすると、CSD 設定ファイルおよび data.xml がフラッシュ デバイスから実行コンフィギュレーションにロードされます。CSD をディセーブルにしても、CSD 設定は変更されません。

次の手順に従い、ASDM を使用して CSD をイネーブルまたはディセーブルにします。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [設定（Setup）] を選択します。

ASDM によって、[設定（Setup）] ペインが開きます（図 5-3）。

（注）　[Secure Desktop イメージ（Secure Desktop Image）] フィールドに現在インストールされているイメージ（およびバージョン）が表示されます。[Secure Desktop の有効化（Enable Secure Desktop）] チェックボックスは、CSD がイネーブルになっているかどうかを示します。

ステップ 2　[Secure Desktop の有効化（Enable Secure Desktop）] をオンにして CSD をイネーブルにするか、[Secure Desktop の有効化（Enable Secure Desktop）] をオフにして CSD をディセーブルにします。

ステップ 3　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 4　[保存（Save）] をクリックします。ASDM は設定を保存して閉じます。

ホスト スキャンおよび CSD のアップグレードとダウングレード

ASA は、イネーブルにされたホスト スキャン パッケージがスタンドアロン ホスト スキャン パッケージ、AnyConnect Secure Mobility Client に含まれるパッケージ、または Cisco Secure Desktop に含まれるパッケージであるかにかかわらず、そのパッケージをエンドポイントに自動的に配布します。エンドポイントに古いバージョンのホスト スキャン パッケージがインストールされている場合、エンドポイントのそのパッケージはアップグレードされます。エンドポイントに新しいバージョンのホスト スキャン パッケージがある場合、エンドポイントのそのパッケージはダウングレードされます。

ASA でイネーブルにされたホスト スキャン イメージの判別

ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。

[ホスト スキャン イメージ（Host Scan Image）] ロケーション フィールドにホスト スキャン イメージが指定されていて、[ホスト スキャン/CSD の有効化（Enable HostScan/CSD）] ボックスがオンの場合、そのイメージのバージョンが ASA によって使用されるホスト スキャンのバージョンになります。

[ホスト スキャン イメージ（Host Scan Image）] フィールドが空で、[ホスト スキャン/CSD の有効化（Enable HostScan/CSD）] ボックスがオンの場合、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] を選択します。[Secure Desktop イメージのロケーション（Secure Desktop Image Location）] フィールドの CSD のバージョンが、ASA によって使用されるホスト スキャンのバージョンになります。

ホスト スキャンのアンインストール

ホスト スキャン パッケージのアンインストール

ホスト スキャン パッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、ホスト スキャンまたは CSD がイネーブルの場合でも ASA によってホスト スキャン パッケージは展開されません。ホスト スキャンをアンインストールしても、ホスト スキャン パッケージはフラッシュ ドライブから削除されません。

以下の手順を使用して、セキュリティ アプライアンスでホスト スキャンをアンインストールします。

ステップ 1　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。

ステップ 2　[ホスト スキャン イメージ（Host Scan Image）] ペインで、[アンインストール（Uninstall）] をクリックします。ASDM はテキストを [ロケーション（Location）] テキスト ボックスから削除します。

ステップ 3　[保存（Save）] をクリックします。

ASA からの CSD のアンインストール

Cisco Secure Desktop（CSD）をアンインストールすると、**フラッシュ カード上のデスクトップ ディレクトリから CSD 設定ファイルおよび data.xml が削除されます**。このファイルを保存する場合は、CSD をアンインストールする前に、別の名前を使用してファイルをコピーするか、ワークステーションにダウンロードします。

以下の手順を使用して、セキュリティ アプライアンスで CSD をアンインストールします。

ステップ 1　ASDM を開き、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [設定（Setup）] を選択します。

ASDM によって、[設定（Setup）] ペインが開きます（図 5-3）。

ステップ 2　[アンインストール（Uninstall）] をクリックします。

次のメッセージが確認ウィンドウに表示されます。

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

ステップ 3　[はい（Yes）] をクリックします。

ASDM によって、[ロケーション（Location）] テキスト ボックスからテキストが削除され、[設定（Setup）] の下にある [Secure Desktop Manager] メニュー オプションが削除されます。

ステップ 4　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 5　[保存（Save）] をクリックします。ASDM は設定を保存して閉じます。

AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

ステップ 1　ASDM を開き、[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）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　[グループ ポリシー（Group Policies）] パネルで、[追加（Add）] をクリックし、新規グループ ポリシーを作成するか、ホスト スキャン パッケージを割り当てるグループ ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3　[内部グループ ポリシーの編集（Edit Internal Group Policy）] パネルで、パネルの左側にある [詳細（Advanced）] ナビゲーション ツリーを拡張し、[AnyConnect クライアント（AnyConnect Client）] を選択します。

ステップ 4　[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] の [継承（Inherit）] チェックボックスをオフにします。

ステップ 5　[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] ドロップダウン メニューで、[AnyConnect Posture モジュール（AnyConnect Posture Module）] をオンにし、[OK] をクリックします。

ステップ 6　[OK] をクリックします。

ホスト スキャン ロギング

ホスト スキャンは、Windows プラットフォームの場合イベント ビューアに、また Windows プラットフォーム以外の場合 syslog にログを記録します。イベント ビューアでは、すべてのログは、独自の「Cisco AnyConnect Secure Mobility Client Posture」フォルダに保存されます。

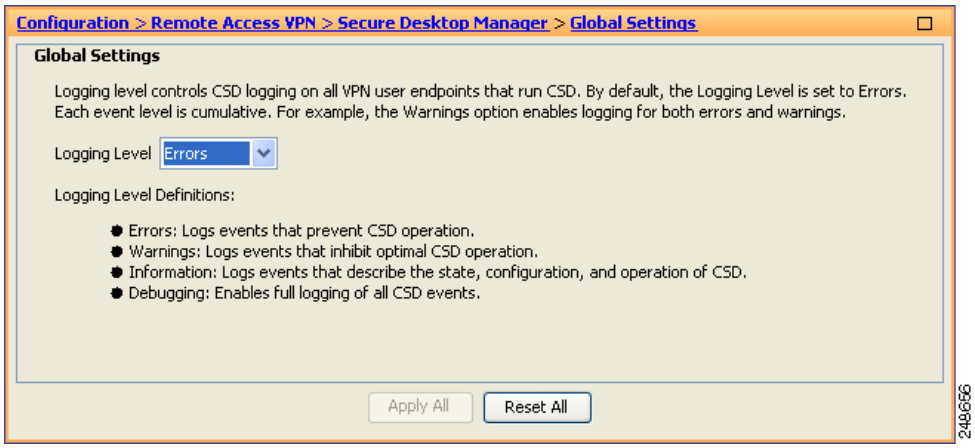
すべてのポスチャ モジュール コンポーネントのロギング レベルの設定

デフォルトでは、ポスチャ モジュールのコンポーネントは、「Error」重大度レベルのイベントをログに記録します。以下の手順を使用して、ポスチャ モジュールのすべてのコンポーネントのロギング重大度レベルを変更します。

ポスチャ モジュールは、ユーザのホーム フォルダに cscan.log ファイルをインストールします。cscan.log ファイルには、最後の VPN セッションからのエントリだけが表示されます。ユーザが ASA に接続するたびに、ホスト スキャンでは新しいロギング データでこのファイルのエントリを上書きします。

ポスチャのロギング レベルを表示または変更するには、次の手順に従います。

ステップ 1　ASDM インターフェイスから、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [グローバル設定（Global Settings）] を選択します。[グローバル設定（Global Settings）] パネルが開きます。



ステップ 2　パネル内の [ロギング レベルの定義（Logging Level Definitions）] を参考に、[ロギング レベル（Logging Level）] を設定します。

ステップ 3　実行コンフィギュレーションに加えられた変更を保存するには、[すべて適用（Apply All）] をクリックします。

（注）　特定の接続プロファイルに対してホスト スキャンがディセーブルになっている場合、その接続プロファイルを使用しているユーザにはホスト スキャンのロギングは実行されません。

ポスチャ モジュールのログ ファイルと場所

ポスチャ モジュール コンポーネントは、ご使用のオペレーティング システム、特権レベル、および起動メカニズム（Web 起動または AnyConnect）に基づいて、以下の 3 つのログに出力します。

- cstub.log：AnyConnect Web 起動が使用されると、ロギングをキャプチャします。
- libcsd.log：ホスト スキャン API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成され、ポスチャおよびホスト スキャンのメイン ログになります。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。

ポスチャ モジュールは、これらのログ ファイルをユーザのホーム フォルダに配置します。場所は、オペレーティング システムおよび VPN 方式によって異なります。

Cisco Technical Assistant Center（TAC）では、必要が生じた場合に、これらのログ ファイルを使用して問題のデバッグを行います。お客様がこれらのファイルを確認する必要はありません。Cisco TAC では、これらのログ ファイルを必要とする場合に、DART バンドルを使用してそれらのファイルを提供するようにお客様に依頼することがあります。DART ユーティリティは、すべての AnyConnect 設定およびログ ファイルを収集し、TAC に送信することになる圧縮ファイルにそれらのログ ファイルを保存します。DART の詳細については、「DART を使用したトラブルシューティング情報の収集」（P.12-4）を参照してください。

Lua 表現での BIOS シリアル番号の使用

ホスト スキャンは、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用し、その BIOS シリアル番号に基づいて ASA への VPN 接続を許可または拒否できます。

Lua 表現での BIOS の表現

これは、ASDM の [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] 画面の [詳細（Advanced）] フィールドで使用できる Lua 論理式です。

endpoint.device.id=***BIOSSerialNumber***

ここで、***BIOSSerialNumber*** は、ASA への接続を試行するハードウェア デバイスの BIOS シリアル番号を表します。この文字列は可変長文字列で、通常、OS 固有の文字列です。

DAP エンドポイント属性としての BIOS の指定

ステップ 1　ASDM にログオンします。

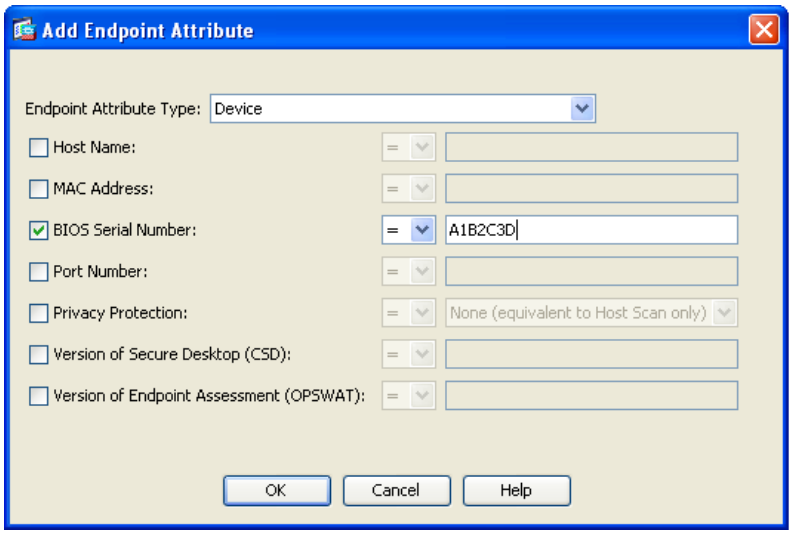
ステップ 2　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] を選択するか、[クライアントレス SSL VPN アクセス（Clientless SSL VPN Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] を選択します。

ステップ 3　[ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（Edit）] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4　エンドポイント ID 表の右にある [追加（Add）] をクリックします。

ステップ 5　[エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6　[BIOS シリアル番号（BIOS Serial Number）] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS シリアル番号（BIOS Serial Number）] フィールドに BIOS 番号を入力します。



ステップ 7　[OK] をクリックし、[エンドポイント属性（Endpoint Attribute）] ダイアログボックスでの変更を保存します。

ステップ 8　[OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 9　[適用（Apply）] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 10　[保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

以下のリソースは、さまざまなエンドポイントで BIOS シリアル番号を取得する方法を説明しています。

- Windows：http://support.microsoft.com/kb/558124
- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：次のコマンドを使用します。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

その他の重要な資料

ホスト スキャンがエンドポイント コンピュータからポスチャ クレデンシャルを収集した後は、情報を活用するために、ユーザはプリログイン ポリシーの設定、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらの内容については、次のマニュアルで詳しく説明します。

- 『Cisco Secure Desktop Configuration Guides』
- 『Cisco Adaptive Security Device Manager Configuration Guides』

- ホスト スキャンによってサポートされるアンチウイルス、アンチスパイウェア、およびファイアウォールのアプリケーションのリスト

CHAPTER 6

Web セキュリティの設定

AnyConnect Web セキュリティ モジュールは、ScanSafe Web スキャニング サービスが評価する ScanSafe スキャニング プロキシに HTTP トラフィックをルーティングするエンドポイント コンポーネントです。

ScanSafe Web スキャニング サービスは、Web ページの各要素を同時に分析できるように、これらの要素を分解します。たとえば、特定の Web ページが HTTP、Flash、および Java 要素の組み合わせである場合、別個の「scanlets」がこれらの各要素を並行して分析します。ScanSafe Web スキャニング サービスは、ScanCenter 管理ポータルに定義されたセキュリティ ポリシーに基づいて、良性または受け入れ可能なコンテンツを許可し、悪意のあるか受け入れられないコンテンツをドロップします。これは、少数のコンテンツが許容されないために Web ページ全体が制限される「過剰ブロック」、または依然として許容されないか場合によっては有害なコンテンツがページで提供されるのにページ全体が許可される「不十分なブロック」を防止します。ScanSafe Web スキャニング サービスは、ユーザが企業ネットワーク上に存在する場合も存在しない場合もユーザを保護します。

多数の ScanSafe スキャニング プロキシが世界各国に普及することで、AnyConnect Web セキュリティを活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い ScanSafe スキャニング プロキシにトラフィックをルーティングできます。

社内 LAN 上にあるエンドポイントを特定するよう、ビーコン サーバの 1 つ以上のインスタンスを設定できます。これは、「Detect-On-LAN」機能です。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。ビーコン サーバは、企業の一意の公開/秘密キー ペアを使用して、正しい公開キーを持つ Cisco ScanSafe Web セキュリティの顧客のみが、ネットワークへの接続中に ScanSafe スキャニング プロキシをバイパスできるようにしています。ネットワークにビーコン サーバの複数のインスタンスを展開する場合、各インスタンスは同一の公開/秘密キー ペアを使用する必要があります。

AnyConnect Web セキュリティ機能は、AnyConnect のプロファイル エディタを使用して編集する AnyConnect Web セキュリティ クライアント プラットフォームを使用して設定されます。

ScanCenter は、ScanSafe Web スキャニング サービスの管理ポータルです。ScanCenter を使用して作成または設定されたコンポーネントの一部は、AnyConnect Web セキュリティ クライアント プロファイルにも組み込まれています。

次の項では、AnyConnect Web セキュリティ クライアント プロファイルと機能、およびこれらの設定方法について説明します。

- AnyConnect Web セキュリティ クライアント プロファイルの作成
- クライアント プロファイルでの ScanSafe スキャニング プロキシの設定
- Web スキャニング サービスからのエンドポイント トラフィックの除外
- Web スキャニング サービス プリファレンスの設定
- ビーコン サーバのインストール
- 認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信
- Web セキュリティ クライアント プロファイル ファイル
- スタンドアロン Web セキュリティ クライアント プロファイルのインストール
- Web セキュリティ トラフィックのスプリットトンネリングの設定
- Web セキュリティ クライアント プロファイルの ScanCenter ホステッド コンフィギュレーション サポートの設定
- Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化

最初に AnyConnect Web セキュリティ クライアント プロファイルの作成によって AnyConnect Web セキュリティを設定できます。

システム要件

次に、AnyConnect Web セキュリティ モジュールのシステム要件を示します。

- AnyConnect Web セキュリティ モジュール
- ASA と ASDM に関する要件
- ビーコン サーバの要件

AnyConnect Web セキュリティ モジュール

Web セキュリティでは、次のオペレーティング システムがサポートされます。

- Windows XP SP3 x86（32 ビット）
- Windows Vista x86（32 ビット）または x64（64 ビット）
- Windows 7 x86（32 ビット）または x64（64 ビット）
- OS X v10.5 x86（32 ビット）
- Mac OS X v10.6 x86（32 ビット）または x64（64 ビット）
- Mac OS X v10.7 x86（32 ビット）または x64（64 ビット）

ASA と ASDM に関する要件

AnyConnect Secure Mobility Client を Web セキュリティ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4(1)
- ASDM 6.4(0)104

ビーコン サーバの要件

ビーコン サーバは、次のオペレーティング システムでサポートされます。

- Windows Server 2003 R1 x86（32 ビット）または x64（64 ビット）
- Windows Server 2003 R2 x86（32 ビット）または x64（64 ビット）
- Windows Server 2008 R1 x86（32 ビット）または x64（64 ビット）
- Windows Server 2008 R2 x64（64 ビット）

システムの制限

Web セキュリティを実行するユーザは、Anywhere Plus も実行することはできません。Web セキュリティをインストールする前に、Anywhere Plus を削除する必要があります。

ライセンス要件

次の項では、AnyConnect Web セキュリティ モジュールのさまざまな導入方法のライセンス要件について説明します。

- 「スタンドアロン コンポーネントとして導入された Web セキュリティ」（P.6-3）
- 「AnyConnect のコンポーネントとして導入された Web セキュリティ」（P.6-3）

スタンドアロン コンポーネントとして導入された Web セキュリティ

Web セキュリティ モジュールを導入して、ASA をインストールしたり、AnyConnect Secure Mobility Client の VPN 機能をイネーブルにしたりすることなく、ScanSafe Web スキャニング サービスの利点を得ることができます。

ScanSafe Web スキャニング サービスでローミング ユーザを保護するには、ScanSafe Web Filtering や ScanSafe Malware Scanning のライセンスに加えて、引き続き Secure Mobility for ScanSafe ライセンスが必要です。

（注）　Web セキュリティ モジュールのみとともに AnyConnect Secure Mobility Client を使用する場合、AnyConnect Essentials または AnyConnect Premium のライセンスは不要です。

AnyConnect のコンポーネントとして導入された Web セキュリティ

AnyConnect ライセンス

Web セキュリティに固有の AnyConnect ライセンスはありません。Web セキュリティ モジュールは、AnyConnect Essentials または AnyConnect Premium にいずれかとともに機能します。

ScanCenter ライセンス

ScanSafe Web スキャニング サービスでローミング ユーザを保護するには、ScanSafe Web Filtering や ScanSafe Malware Scanning のライセンスに加えて、Secure Mobility for ScanSafe ライセンスが必要です。

IPv6 Web トラフィックでの Web セキュリティの動作に関するユーザ ガイドライン

IPv6 アドレス、ドメイン名、アドレス範囲、またはワイルド カードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。ここで DNS ルックアップが実行され、ユーザがアクセスしようとしている URL に IPv4 アドレスがあるかどうかが確認されます。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合は、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスするように設定する場合は、すべての IPv6 トラフィック **::/0** にこの静的な例外を追加します。つまり、この場合は IPv6 トラフィックは Web セキュリティで保護されません。

ASA とともに使用するための AnyConnect Web セキュリティ モジュールのインストール

Web セキュリティ モジュールは、AnyConnect とともに導入する場合、またはスタンドアロン モジュールとして導入する場合、クライアント プロファイルを必要とします。

ステップ 1　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。

ステップ 2　Web 導入および事前導入の方法を使用した Web セキュリティ モジュールのインストールに関する手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を読んでください。

ASA なしで使用するための AnyConnect Web セキュリティ モジュールのインストール

Web セキュリティ モジュールをスタンドアロン アプリケーションとして導入して、AnyConnect VPN モジュールをイネーブルにせずに、ASA なしで ScanSafe ScanCenter とともに使用できます。ここでは次の内容について説明します。

- AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストール
- AnyConnect インストーラを使用した Mac OS X への Web セキュリティ モジュールのインストール

（注）　Windows が実行されているコンピュータでは、AnyConnect がユーザ ID を判別できない場合、内部 IP アドレスがユーザ ID として使用されます。たとえば、これは、enterprise_domains プロファイル エントリが指定されていない場合に発生する可能性があります。その場合、ScanCenter でレポートを生成するために、内部 IP アドレスを使用する必要があります。

Mac OS X が実行されているコンピュータでは、Mac がドメインにバインドされている場合、Web セキュリティ モジュールは、コンピュータがログインしているドメインを報告できます。ドメインにバインドされていない場合、Web セキュリティ モジュールは、Mac の IP アドレスまたは現在ログインしているユーザ名を報告できます。

AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストール

この手順では、ScanSafe とともに使用するために Windows OS で Cisco AnyConnect Secure Mobility Client Web セキュリティ モジュールを設定する方法について説明します。大まかには、次のタスクを実行します。

1. Cisco AnyConnect Secure Mobility Client ISO イメージをダウンロードします。
2. ISO ファイルの内容を抽出します。
3. スタンドアロン プロファイル エディタをインストールし、Web セキュリティ プロファイルを作成して、Web セキュリティ プロファイル ファイルを ISO ファイルの抽出済みの内容に追加することによって、Web セキュリティ モジュールをカスタマイズします。
4. カスタマイズ済みの Web セキュリティ モジュールをインストールします。

ScanSafe とともに使用するために Windows OS で Cisco AnyConnect Secure Mobility Client Web セキュリティ モジュールを設定するには、次の手順を実行します。

ステップ 1　ScanCenter サポート エリアまたは Cisco.com から Cisco AnyConnect Secure Mobility Client パッケージをダウンロードします。

ステップ 2　新しいディレクトリを作成します。

ステップ 3　WinZip や 7-Zip などのアプリケーションを使用して、ISO ファイルの内容を、新たに作成したディレクトリに抽出します。

（注）　この時点では Web セキュリティ モジュールをインストール**しないで**ください。

ステップ 4　スタンドアロンの AnyConnect プロファイル エディタをインストールします。詳細については、「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」（P.2-44）を参照してください。

（注）　デフォルトでは、Web セキュリティのプロファイル エディタ コンポーネントはインストールされていません。カスタム インストールの一部として選択するか、完全なインストールを選択する必要があります。

ステップ 5　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ プロファイル エディタを起動してプロファイルを作成します。

ステップ 6　プロファイルに **WebSecurity_ServiceProfile.xml** という名前を付けて安全な場所に保存します。

Web セキュリティ プロファイル エディタにより、**WebSecurity_ServiceProfile.wso** という名前のプロファイルの難読化バージョンが追加作成され、WebSecurity_ServiceProfile.xml ファイルと同じ場所に保存されます。

ステップ 7　WebSecurity_ServiceProfile.wso という難読化バージョンの Web セキュリティ プロファイルを、ステップ 3 で抽出した **Profiles\websecurity** フォルダにコピーします。

ステップ 8　**Setup.exe** を開始して、クライアント ソフトウェアをインストールします。

ステップ 9　[Cisco AnyConnect Secure Mobility Client インストール セレクタ（Cisco AnyConnect Secure Mobility Client Install Selector）] で、次のようにします。

- [AnyConnect Web セキュリティ モジュール（AnyConnect Web Security Module）] チェックボックスがオンになっていることを確認します。
- [Cisco AnyConnect VPN モジュール（Cisco AnyConnect VPN Module）] がオフになっていることを確認します。これでコア クライアントの VPN 機能がオフになり、インストール ユーティリティによって、ネットワーク アクセス マネージャと Web セキュリティが、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。
- （任意）[ロック ダウン コンポーネント サービス（Lock Down Component Services）] チェックボックスを選択します。ロックダウン コンポーネント サービスによって、ユーザは、Windows Web セキュリティ サービスをディセーブルまたは停止できなくなります。

ステップ 10　[選択した内容のインストール（Install Selected）] をクリックして、[OK] をクリックします。インストールが正常に完了したら、システム トレイに [Cisco AnyConnect Secure Mobility Client] アイコンが表示されます。

AnyConnect インストーラを使用した Mac OS X への Web セキュリティ モジュールのインストール

次の手順では、スタンドアロン プロファイル エディタをインストールして、Web セキュリティ プロファイルを作成し、その Web セキュリティ プロファイルを DMG パッケージに追加することによって、Web セキュリティ モジュールをカスタマイズする方法について説明します。

ステップ 1　ScanCenter サポート エリアまたは Cisco.com のダウンロード エリアから Cisco AnyConnect Secure Mobility Client DMG パッケージをダウンロードします。

ステップ 2　ファイルを開いて、インストーラにアクセスします（図 6-1）。ダウンロードしたイメージは読み取り専用ファイルです。

図 6-1　AnyConnect インストーラ イメージ

ステップ 3　**ディスク ユーティリティ**を実行するか、次のように**端末** アプリケーションを使用して、インストーラ イメージを書き込み可能にします。

```
Hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

ステップ 4　Windows オペレーティング システムが実行されているコンピュータにスタンドアロンの AnyConnect プロファイル エディタをインストールします。詳細については、「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」（P.2-44）を参照してください。

（注）　デフォルトでは、Web セキュリティのプロファイル エディタ コンポーネントはインストールされていません。カスタム インストールの一部として選択するか、完全なインストールを選択する必要があります。

ステップ 5　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ プロファイル エディタを起動してプロファイルを作成します。

ステップ 6　プロファイルに **WebSecurity_ServiceProfile.xml** という名前を付けて安全な場所に保存します。

Web セキュリティ プロファイル エディタにより、**WebSecurity_ServiceProfile.wso** という名前のプロファイルの難読化バージョンが追加作成され、WebSecurity_ServiceProfile.xml ファイルと同じ場所に保存されます。

ステップ 7　WebSecurity_ServiceProfile.wso ファイルを Windows マシンから **AnyConnect 3.0.5074/Profiles/websecurity** Mac OS X インストーラ パッケージにコピーします。

または、次のように**端末**アプリケーションを使用することもできます。

```
Copy WebSecurity_ServiceProfile.wso
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

ステップ 8　Mac OS X インストーラで、**AnyConnect 3.0.5074/Profiles** ディレクトリに移動し、TextEdit で **ACTransforms.xml** ファイルを開いてファイルを編集します。VPN 機能がインストールされないように、<DisableVPN> 要素を **True** に設定します。

```
<ACTransforms>
    <DisableVPN>True</DisableVPN>
</ACTransforms>
```

ステップ 9　Cisco.com の AnyConnect Secure Mobility Client **3.0.4235** のダウンロード エリアで、**VPNDisable_ServiceProfile.xml** ファイルを見つけて、AnyConnect Web セキュリティをインストールするコンピュータにダウンロードします。

ステップ 10　**VPNDisable_ServiceProfile.xml** ファイルを AnyConnect インストーラの **AnyConnect 3.0.5074/profiles/vpn** ディレクトリに保存します。

（注）　AnyConnect 3.0.4235 用の Web セキュリティ モジュールのみを Mac OS X にインストールする場合、AnyConnect ユーザ インターフェイスは、ブートアップ時に自動的に起動するよう設定する必要があります。これによって、AnyConnect は、Web セキュリティ モジュールに必要なユーザおよびグループ情報を指定できるようになります。手順 9 および 10 では、ブート時に AnyConnect ユーザ インターフェイスを自動的に起動できるようにする正しい設定を指定します。

ステップ 11　これで、AnyConnect DMG パッケージをユーザに配布する準備ができました。

コマンドライン インストールを使用した Windows OS への Web セキュリティ モジュールのインストール

コマンド プロンプトから Web セキュリティ モジュール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　AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストールのステップ 1 ～ステップ 6 に従います。

ステップ 2　VPN 機能をオフにして AnyConnect Secure Mobility Client VPN モジュールをインストールします。

```
msiexec /package anyconnect-win-<version>-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* c:\test.log
```

ステップ 3　Web セキュリティ モジュールをインストールします。

```
msiexec /package anyconnect-websecurity-win-<version>-pre-deploy-k9.msi /norestart
/passive /lvx* c:\test.log
```

ステップ 4　（任意）DART をインストールします。

```
misexec /package annyconnect-dart-win-<version>-k9.msi /norestart /passive /lvx*
c:\test.log
```

ステップ 5　難解化 Web セキュリティ クライアント プロファイルのコピーを、表 2-15（P.2-42）で定義した正しい Windows フォルダに保存します。

ステップ 6　「Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化」（P.6-42）の手順に従って、Cisco AnyConnect Web セキュリティ エージェント Windows サービスを再起動します。

（注）　これらのコマンドは、Systems Management Server（SMS）の導入にも使用できます。

AnyConnect Web セキュリティ クライアント プロファイルの作成

AnyConnect Web セキュリティ クライアント プロファイルを作成するには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、ASDM を開いて [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) Accessess）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。
- Windows OS のスタンドアロン モードで、[スタート（Start）] > [プログラム（Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択します。

ステップ 2　[追加（Add）] をクリックしてクライアント プロファイルを作成します。

ステップ 3　クライアント プロファイルの**名前**を指定します。

ステップ 4　[プロファイルの使用（Profile Usage）] フィールドをクリックして、[Web セキュリティ（Web Security）] を選択します。

ステップ 5　デフォルトのプロファイルの場所を使用するか、[参照（Browse）] をクリックして代わりのファイルの場所を指定します。

ステップ 6　（任意）[グループ ポリシー（Group Policy）] を選択してクライアント プロファイルを添付するか、クライアント プロファイルを <Unassigned> のままにします。

ステップ 7　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

AnyConnect Web セキュリティ クライアント プロファイルを作成してある場合は、プロファイルの次の側面を設定する必要があります。

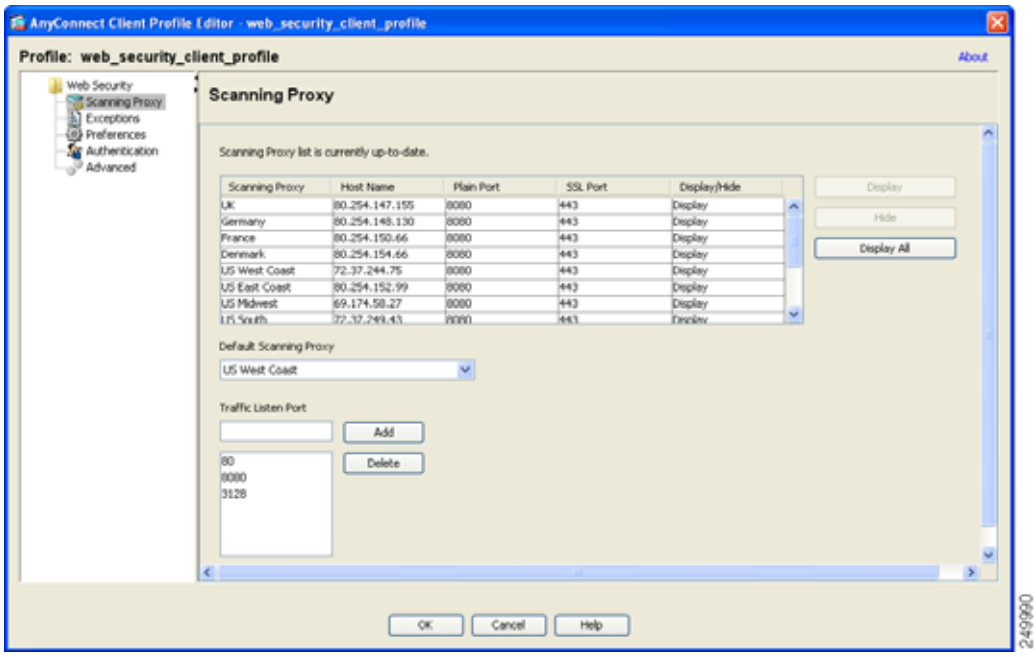
- 「クライアント プロファイルでの ScanSafe スキャニング プロキシの設定」（P.6-9）
- 「Web スキャニング サービスからのエンドポイント トラフィックの除外」（P.6-13）
- 「ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算」（P.6-16）
- 「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）
- 「認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信」（P.6-31）

AnyConnect Web セキュリティ クライアント プロファイルを作成して保存した後で、ASDM は、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルで、もう 1 つはプレーン テキスト形式です。これらのファイルの詳細については、「Web セキュリティ クライアント プロファイル ファイル」（P.6-36）を参照してください。

クライアント プロファイルでの ScanSafe スキャニング プロキシの設定

ScanSafe Web スキャニング サービスは Web コンテンツを分析します。これは、セキュリティ ポリシーに基づいてブラウザへの良性のコンテンツの配信を許可し、悪意のあるコンテンツをブロックします。スキャニング プロキシは、ScanSafe Web スキャニング サービスが Web コンテンツを分析する ScanSafe プロキシ サーバです。AnyConnect Web セキュリティ プロファイル エディタ内の [スキャン プロキシ（Scanning Proxy）] パネルは、AnyConnect Web セキュリティ モジュールによる Web ネットワーク トラフィックの送信先 ScanSafe スキャニング プロキシを定義します。

図 6-2　Web セキュリティ クライアント プロファイルの [スキャン プロキシ（Scanning Proxy）] パネル



AnyConnect Web セキュリティ クライアント プロファイルで ScanSafe スキャニング プロキシを定義するには、次の手順を使用します。

- 「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）
- 「スキャニング プロキシのユーザへの表示または非表示」（P.6-11）
- 「デフォルトのスキャニング プロキシの選択」（P.6-12）
- 「HTTP（S）トラフィック リスニング ポートの指定」（P.6-13）

スキャニング プロキシ リストの更新

Web セキュリティ プロファイル エディタのスキャニング プロキシ リストは編集不可能です。ScanCenter スキャニング プロキシを Web セキュリティ プロファイル エディタ内のテーブルで追加したり削除したりすることはできません。

Web セキュリティ プロファイル エディタを起動した後で、スキャニング プロキシの最新のリストが保持されている ScanCenter Web サイトにアクセスすることで、スキャニング プロキシ リストが自動的に更新されます。

AnyConnect Web セキュリティ クライアント プロファイルの追加または編集時に、プロファイル エディタは、ScanSafe スキャニング プロキシの既存のリストを、ScanSafe Web サイトからダウンロードしたスキャニング プロキシ リストと比較します。リストが古い場合は、「スキャン プロキシ リストは期限切れです（Scanning Proxy list is out of date）」というメッセージと、[リストの更新（Update List）] というラベルが付いたコマンド ボタンが表示されます。スキャニング プロキシ リストを、ScanSafe スキャニング プロキシの最新のリストで更新するには、[リストの更新（Update List）] ボタンをクリックします。

[リストの更新（Update List）] をクリックすると、プロファイル エディタによって、既存の設定が可能な限り保持されます。プロファイル エディタは、デフォルトのスキャニング プロキシ設定、および既存の ScanSafe スキャニング プロキシの表示または非表示設定を保存します。

Web セキュリティ クライアント プロファイルでのデフォルトのスキャニング プロキシ設定

デフォルトでは、作成するプロファイルには、次の ScanSafe スキャニング プロキシ属性があります。

- スキャニング プロキシ リストには、ユーザがアクセスできるすべての ScanSafe スキャニング プロキシが読み込まれ、すべて「Display」とマークされます。詳細については、「スキャニング プロキシのユーザへの表示または非表示」（P.6-11）を参照してください。
- デフォルトの ScanSafe スキャニング プロキシは事前選択されています。デフォルトの ScanSafe スキャニング プロキシを設定するには、「デフォルトのスキャニング プロキシの選択」（P.6-12）を参照してください。
- AnyConnect Web Security モジュールが HTTP トラフィックを受信するポートのリストは、いくつかのポートにプロビジョニングされます。詳細については、「HTTP（S）トラフィック リスニング ポートの指定」（P.6-13）を参照してください。

スキャニング プロキシのユーザへの表示または非表示

ユーザが ASA への VPN 接続を確立した後で、ASA は、クライアント プロファイルをエンドポイントにダウンロードします。AnyConnect Web セキュリティ クライアント プロファイルは、ユーザに表示される ScanSafe スキャニング プロキシを判別します。

ユーザは、次の方法で、AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ リストで「Display」とマークされたスキャニング プロキシと対話します。

- ScanSafe スキャニング プロキシは、Cisco AnyConnect Secure Mobility Client インターフェイスの [Web セキュリティ（Web Security）] パネルの [詳細（Advanced）] 設定のユーザに表示されます。
- AnyConnect Web セキュリティ モジュールは、応答時間でスキャニング プロキシを順序付ける際に、「Display」とマークされた ScanSafe スキャニング プロキシをテストします。
- ユーザは、自分のプロファイルでユーザ制御が許可される場合に接続する ScanSafe スキャニング プロキシを選択できます。
- AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ テーブルで「Hide」とマークされている ScanSafe スキャニング プロキシは、ユーザに表示されず、応答時間でスキャニング プロキシを順序付ける際に評価されません。ユーザは、「Hide」とマークされたスキャニング プロキシには接続できません。

（注） ローミング ユーザが最大の利点を得るには、すべての ScanSafe スキャニング プロキシをすべてのユーザに「表示」することをお勧めします。

ScanSafe スキャニング プロキシをユーザに非表示または表示するには、次の手順を実行します。

ステップ 1　ASDM を開いて [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) Accessess）] > [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　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　ScanSafe スキャニング プロキシを非表示または表示するには、次の手順を実行します。

- **スキャニング プロキシを非表示にするには**、非表示にするスキャニング プロキシを選択して、[非表示（Hide）] をクリックします。

- **スキャニング プロキシを表示するには**、表示するスキャニング プロキシの名前を選択して、[表示（Display）] をクリックします。すべての ScanSafe スキャニング プロキシを表示する設定を推奨します。

ステップ 4　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

デフォルトのスキャニング プロキシの選択

デフォルトの ScanSafe スキャニング プロキシを定義するには、次の手順を実行します。

ステップ 1　ASDM を開いて [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) Accessess）] > [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　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　[デフォルトのスキャン プロキシ（Default Scanning Proxy）] フィールドからデフォルトのスキャニング プロキシを選択します。

ステップ 4　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

ユーザがスキャニング プロキシに接続する方法

1. ユーザが初めてネットワークに接続すると、デフォルトのスキャニング プロキシにルーティングされます。
2. その後、プロファイルの設定方法に応じて、ユーザはスキャニング プロキシを選択するか、AnyConnect Web セキュリティ モジュールが、応答時間が最も早いスキャニング プロキシにユーザを接続します。
   - ユーザのクライアント プロファイルでユーザ制御が許可される場合、ユーザは、Cisco AnyConnect Secure Mobility Client Web セキュリティ トレイの [設定（Settings）] タブからスキャニング プロキシを選択します。
   - クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] プリファレンスがイネーブルになっている場合、AnyConnect Web セキュリティは、スキャニング プロキシを速い順にして、応答時間が最も早いスキャニング プロキシにユーザを接続します。
   - クライアント プロファイルでユーザ制御が許可されなくても、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] がイネーブルになっているときは、AnyConnect Web セキュリティは、ユーザをデフォルトのスキャニング プロキシから、応答時間が最も早いスキャニング プロキシに切り替えます（応答時間が、最初に接続したデフォルトのスキャニング プロキシよりも大幅に早い場合）。
   - ユーザが、現在のスキャニング プロキシからローミングし始めたときに、クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が設定されていれば、AnyConnect Web セキュリティは、ユーザを新しいスキャニング プロキシに切り替えることがあります（応答時間が現在のスキャニング プロキシよりも大幅に早い場合）。

AnyConnect Web セキュリティでは、Windows の拡張された AnyConnect トレイ アイコン、AnyConnect GUI の [詳細設定（Advanced Settings）] タブ、および [統計情報詳細（Advanced Statistics）] タブにイネーブルになっているスキャニング プロキシ名が表示されるため、ユーザは接続先のスキャニング プロキシを確認できます。

HTTP（S）トラフィック リスニング ポートの指定

Scan Safe Web スキャニング サービスは、デフォルトで HTTP Web トラフィックを分析し、HTTPS Web トラフィックをフィルタリングするよう設定可能です。Web セキュリティ クライアント プロファイルで、Web セキュリティにこれらのタイプのネットワーク トラフィックを「受信」させるポートを指定できます。

ステップ 1　ASDM を開いて [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　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [Edit] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　[トラフィック リスン ポート（Traffic Listen Port）] フィールドに、Web セキュリティ モジュールに HTTP または HTTPS トラフィックまたはその両方を「受信」させる論理ポート番号を入力します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

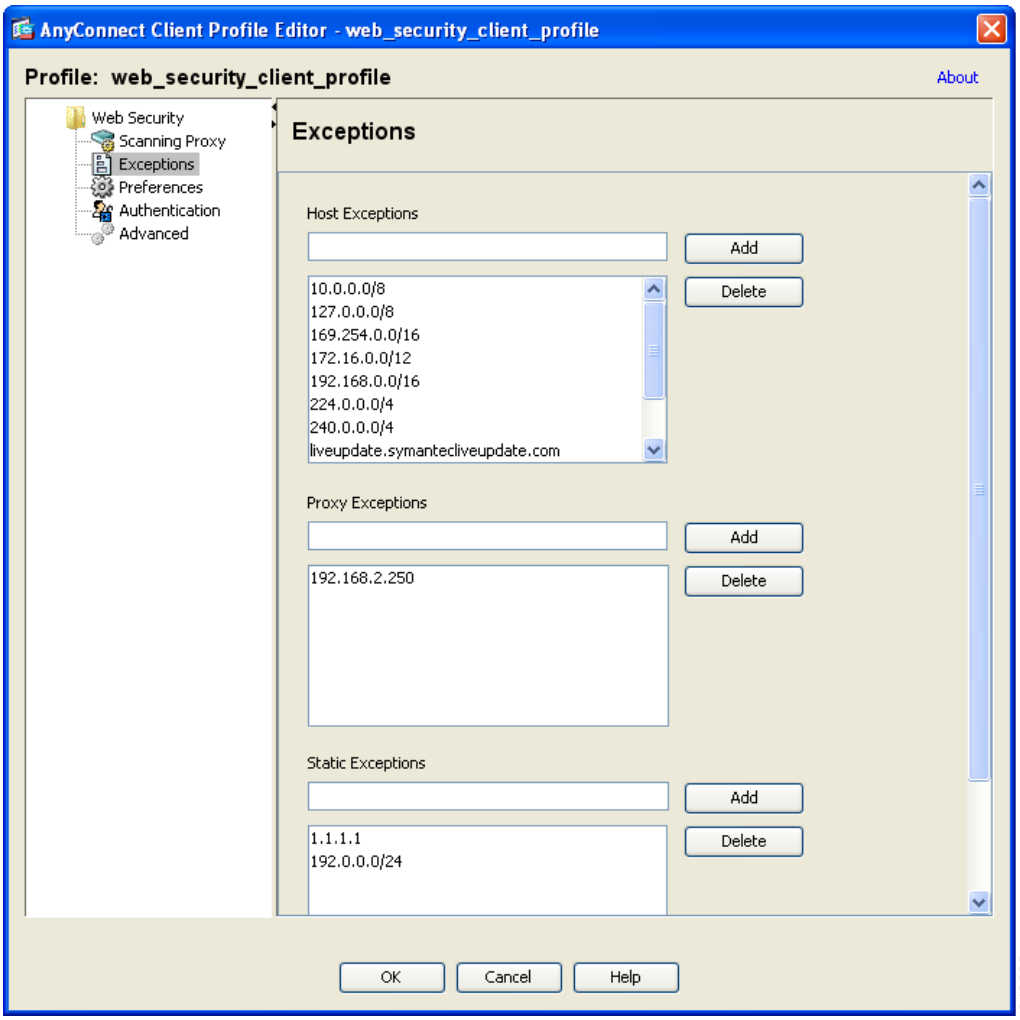
Web スキャニング サービスからのエンドポイント トラフィックの除外

特定の IP アドレスから発信されるネットワーク トラフィックを ScanSafe Web スキャニング サービスで評価しない場合、次のいずれかのカテゴリでそのアドレスの例外を設定できます。

- ホスト例外
- プロキシ例外
- 静的な例外

これらの除外は、Web セキュリティ プロファイル エディタの [除外（Exceptions）] パネルで設定します。図 6-3 を参照してください。

図 6-3　Web セキュリティ プロファイル エディタの [除外（Exceptions）] パネル



ホスト例外

[ホスト除外（Host Exceptions）] リストで、ScanSafe Web スキャニング サービスをバイパスする内部サブネットとパブリック Web サイトを追加します。[除外（Exceptions）] パネルの図については、図 6-3 を参照してください。

たとえば、デフォルトにまだ追加されていない、使用する内部サブネットを追加する必要があります。

```
192.0.2.0/8
```

直接アクセスをイネーブルにする内部または外部 Web サイトも追加する必要があります。次に、例を示します。

```
update.microsoft.com
*.salesforce.com
*.mycompanydomain.com
```

また、イントラネット サービスに使用するパブリック IP アドレスを追加する必要があります。追加しないと、Web セキュリティからこれらのイントラネット サーバにアクセスできません。

RFC 1918 で説明されているすべてのプライベート IP アドレスが、デフォルトでホスト例外リストに含められています。

次の構文を使用して、サブネットと IP アドレスを入力できます。

構文	例
個々の IPv4 および IPv6 アドレス	80.254.145.118 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing（CIDR）表記	10.0.0.0/8 2001:DB8::/48
完全修飾ドメイン名	windowsupdate.microsoft.com ipv6.google.com **（注）** 部分的なドメインはサポートされません。たとえば、example.com はサポートされません。
完全修飾ドメイン名または IP アドレスのワイルドカード	127.0.0.* *.cisco.com

注意 トップレベル ドメインの両側にワイルドカードを使用しないでください（たとえば *.cisco.*）。これには、フィッシング サイトが含まれることがあるためです。

注意 デフォルトのホスト例外エントリを削除または変更しないでください。

プロキシ例外

[プロキシ除外（Proxy Exceptions）] エリアで、認定された内部プロキシの IP アドレスを入力します。`192.168.2.250` などです。[除外（Exceptions）] パネルの図については、図 6-3 を参照してください。

このフィールドに IPv4 および IPv6 アドレスを指定できますが、ポート番号を一緒に指定することはできません。CIDR 表記を使用して IP アドレスを指定できます。

IP アドレスを指定すると、ScanSafe Web スキャニング サービスが、これらのサーバ宛の Web データを代行受信し、SSL を使用してデータをトンネリングしないようにします。これによって、プロキシ サーバは中断なしで動作できます。ここでプロキシ サーバを追加しなかった場合、プロキシ サーバは ScanSafe Web スキャニング サービス トラフィックを SSL トンネルと見なします。

このリストにないプロキシについては、Web セキュリティは、SSL を使用してトンネリングしようとするため、ユーザが、インターネット アクセスのためにプロキシがネットワークから出る必要がある別の企業サイトにいる場合、ScanSafe Web スキャニング サービスは、開いているインターネット接続を使用しているときと同じレベルのサポートを提供します。

静的な例外

トラフィックが ScanSafe Web スキャニング サービスをバイパスする必要がある個々の IP アドレスまたは IP アドレスの範囲のリストを Classless Inter-Domain Routing（CIDR）表記で追加します。リストには、VPN ゲートウェイの入力 IP アドレスを含めます。図 6-3 を参照してください。

CIDR 表記を使用して、IPv4 および IPv6 アドレスまたはアドレスの範囲を指定できます。完全修飾ドメイン名を指定したり、IP アドレスにワイルドカードを使用したりすることはできません。次に、正しい構文の例を示します。

```
10.10.10.5
192.0.2.0/24
```

（注）　必ず SSL VPN コンセントレータの IP アドレスを静的な除外リストに追加してください。

IPv6 Web トラフィックに関するユーザ ガイドライン

IPv6 アドレス、ドメイン名、アドレス範囲、またはワイルド カードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。ここで DNS ルックアップが実行され、ユーザがアクセスしようとしている URL に IPv4 アドレスがあるかどうかが確認されます。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合は、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスするように設定する場合は、すべての IPv6 トラフィック **::/0** にこの静的な例外を追加します。これを行うことで、すべての IPv6 トラフィックがすべてのスキャニング プロキシをバイパスします。つまり、この場合は IPv6 トラフィックは Web セキュリティで保護されません。

Web スキャニング サービス プリファレンスの設定

次のプリファレンスを設定するには、このパネルを使用します。

- 「ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算」（P.6-16）
- 「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）

ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算

ユーザが、接続先の ScanSafe スキャニング プロキシを選択できるようにするには、次の手順を実行します。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[プリファレンス（Preferences）] をクリックします。この手順で設定したフィールドの図については、図 6-4 を参照してください。

ステップ 4　[ユーザ制御可（User Controllable）] をオンにします。（これはデフォルト設定です）。[ユーザ制御可（User Controllable）] は、ユーザが AnyConnect インターフェイスで [タワーの自動選択（Automatic Tower Selection）] および [スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] 設定を変更できるかどうかを決定します。

ステップ 5　Web セキュリティにスキャニング プロキシを自動的に選択させるには、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] をオンにします。これを行うと、[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] は自動的にオンになります。

- [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] を選択すると、Web セキュリティは、応答時間が最も早いスキャニング プロキシを判別して、ユーザをそのスキャニング プロキシに自動的に接続します。

- [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しなくても、まだ [スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] が選択されている場合、ユーザには、接続できるスキャニング プロキシのリストが、応答時間が早い順に表示されます。

（注）　[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] をイネーブルにすると、一時的な通信の中断と障害が原因で、アクティブなスキャニング プロキシの選択が自動的に変更される可能性があります。スキャニング プロキシの変更は望ましくないことがあります。これは、別の言語を使用する別の国のスキャニング プロキシから検索結果が戻されるなど、予期しない動作の原因となる可能性があるためです。

ステップ 6　[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] をオンにした場合は、応答時間が最も早いスキャニング プロキシを計算するための設定を行います。

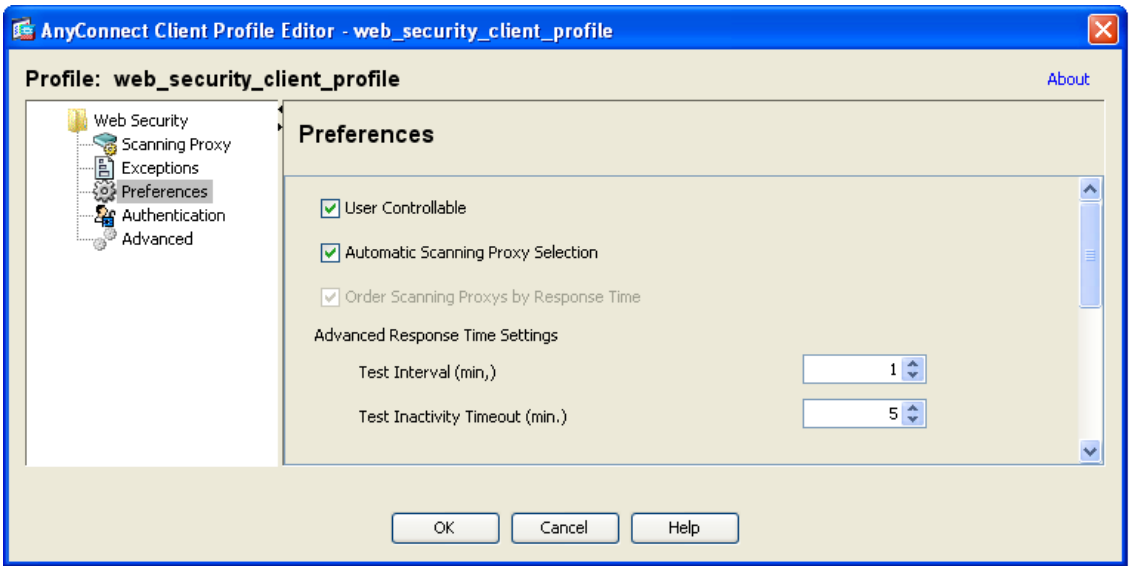
- [テスト間隔（Test Interval）] : 各パフォーマンス テストの実行間の時間（分単位）。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。
- [テスト非アクティブ タイムアウト（Test Inactivity Timeout）] : Web セキュリティが、ユーザ非アクティブのために応答時間テストを一時停止するまでの時間。Web セキュリティは、スキャニング プロキシで接続試行が行われるとすぐにテストを再開します。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

（注）　[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] テストは、次の例外を除き、テスト間隔に基づいて実行し続けます。

- 「Detect-On-LAN」がイネーブルで、マシンが社内 LAN 上にあることをビーコン サーバが検出した。
- Web セキュリティのライセンス キーがないか、無効である。
- ユーザが、設定済みの時間非アクティブで、その結果 [テスト非アクティブ タイムアウト（Test Inactivity Timeout）] しきい値に達した。

ステップ 7　Web セキュリティ クライアント プロファイルを保存します。

図 6-4　ユーザ制御および応答時間制御によるスキャニング プロキシの順序付け



Detect-On-LAN 用のビーコン サーバ接続の設定

Detect-On-LAN 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。詳細については、「Detect-On-LAN」（P.6-40）を参照してください。

ビーコン サーバは、企業の一意の公開 / 秘密キー ペアを使用して、正しい公開キーを持つ Cisco ScanSafe Web セキュリティの顧客のみが、ネットワークへの接続中に ScanSafe スキャニング プロキシをバイパスできるようにしています。ネットワークにビーコン サーバの複数のインスタンスを展開する場合、各インスタンスは同一の公開 / 秘密キー ペアを使用する必要があります。

（注）　ネットワークにプロキシが存在する（ScanSafe Connector など）状態で、ビーコン サーバを使用しない場合は、プロファイル エディタの [除外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。「プロキシ例外」（P.6-15）を参照してください。

Web セキュリティのビーコン サーバとの対話を設定するには、次の手順を実行します。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[プリファレンス（Preferences）] をクリックします。[プリファレンス（Preferences）] パネルの図については、図 6-5 を参照してください。

ステップ 4　ビーコン サーバをネットワーク上にインストールし、Web セキュリティ ユーザからのトラフィックを受信するようにこのビーコン サーバを設定した場合は、[ビーコン確認（Beacon Check）] をオンにします。

ステップ 5　[パブリック キー ファイル（Public Key File）] フィールドで [参照（Browse）] をクリックして、企業の公開キー証明書を選択します。ビーコン サーバは、認証に RSA 公開 / 秘密キー ペアを使用します。秘密キーの長さは 512 ビット以上である必要があります。ただし、シスコでは 1,024 ビットのキーを推奨します。

ステップ 6　[ビーコンの新しいアドレス（New Beacon Address）] フィールドで、ビーコン サーバがインストールされているコンピュータを指定します。有効な IP アドレスまたはドメイン名のいずれかを使用します。正しい構文の例を示します。

構文	例
個々の IPv4 アドレス	`10.10.10.123`
完全修飾ドメイン名	`beaconserver.cisco.com`

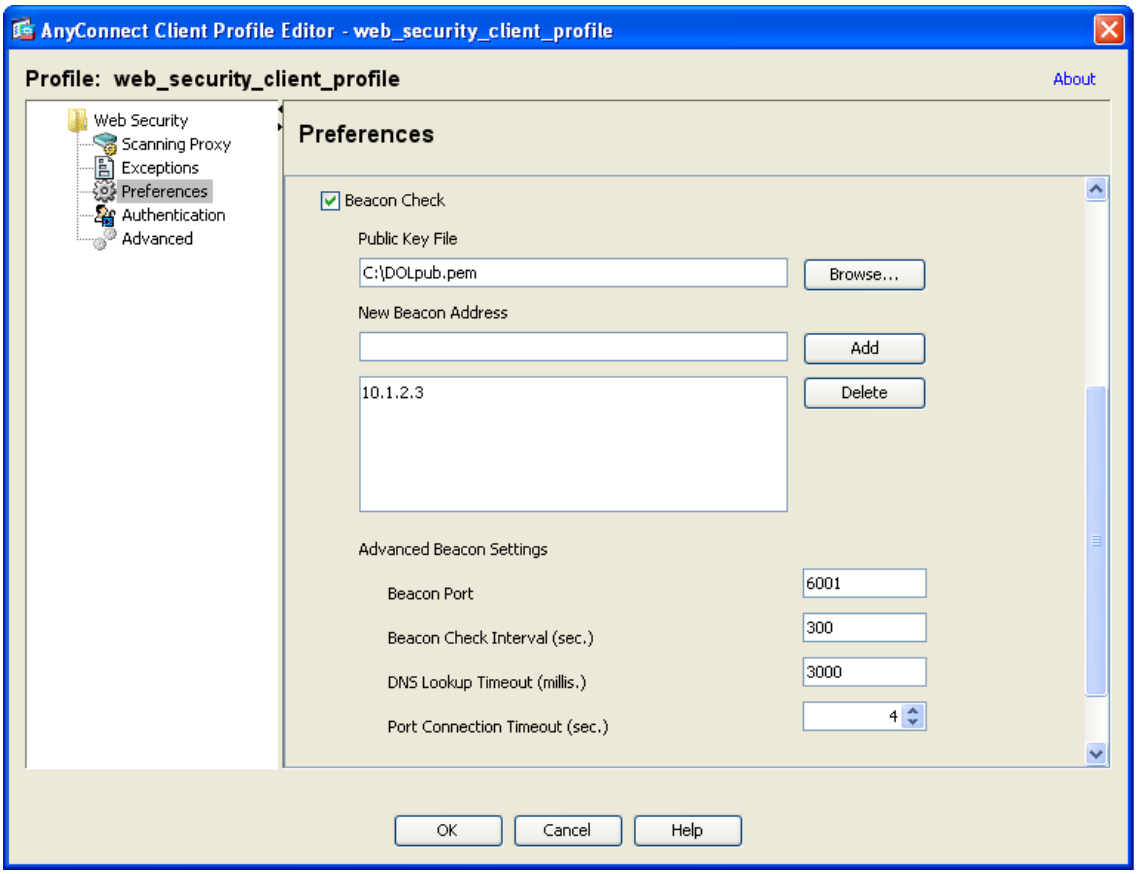
（注）　部分的なドメインはサポートされません。たとえば、cisco.com はサポートされません。

ステップ 7　次の高度なビーコン設定を行います。

- [ビーコンのポート（Beacon Port）] : この要素は、サービスによって使用される TCP/IP ポートを指定します。ポート 6001 でサービスがすでに実行中の場合、この要素を変更できます。ビーコン サーバがインストールされているコンピュータの websecurity.config ファイルで対応する要素を変更する必要もあります。
- [ビーコン確認間隔（Beacon Check Interval）] : Web セキュリティは、ビーコン サーバへの接続の試行の間、秒単位で指定されたこの時間待機し、このビーコン サーバが LAN 上にあるかどうかを判別します。
- [DNS ルックアップ タイムアウト（DNS Lookup Timeout）] : <Beacons> 設定で指定されたホスト名（指定された場合）での DNS ルックアップのタイムアウト（ミリ秒）。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。
- [ポート接続タイムアウト（Port Connection Timeout）] : この要素は、ビーコン サーバにデータを送信していない接続が閉じられるまでの時間を秒単位で指定します。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

ステップ 8　Web セキュリティ クライアント プロファイルを保存します。

図 6-5　ビーコン サーバ チェックの設定

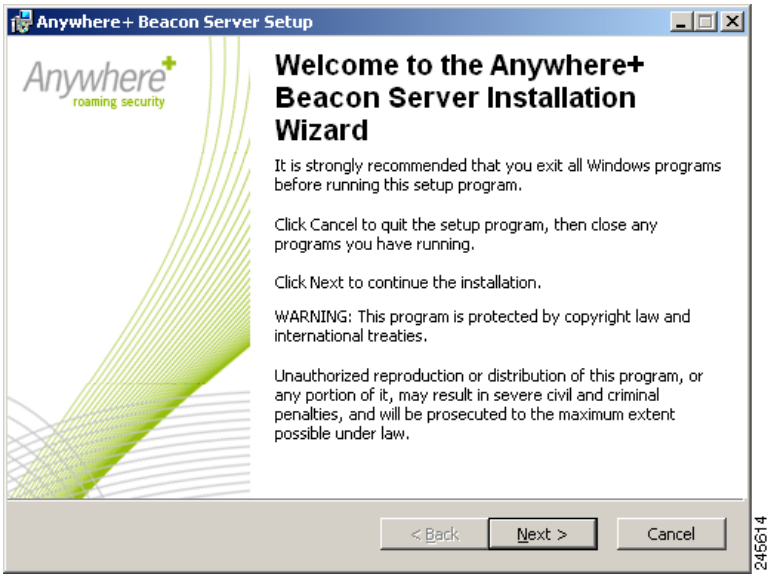


ビーコン サーバのインストール

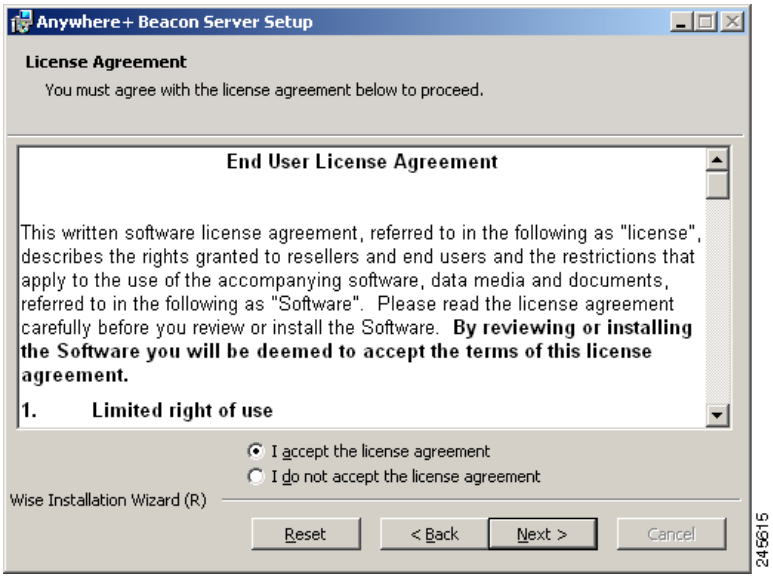
ビーコン サーバをインストールする前に、DOLprv.pem ファイルを BeaconServer.msi プログラム ファイルが含まれているインストール フォルダにコピーする必要があります。「秘密キーおよび公開キーの生成」（P.6-41）を参照してください。BeaconServer.config ファイルを同じフォルダにコピーした場合、これは、デフォルトの設定ファイルの代わりにインストールされます。設定ファイルはインストール後に編集できるため、これは、ビーコン サーバの複数のコピーをインストールする場合を除き不要です。「ビーコン サーバの設定」（P.6-27）を参照してください。標準のインストール方法に加えて、サイレント インストールの実行を選択できます。「サイレント インストール」（P.6-23）を参照してください。

ビーコン サーバをインストールするには、次の手順を実行します。

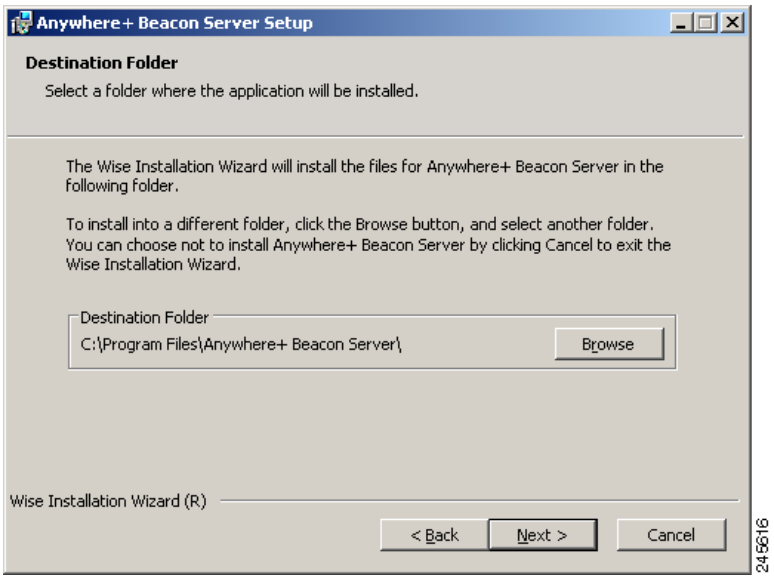
ステップ 1　BeaconServer.msi プログラム ファイルをダブルクリックして、インストール ウィザードを実行します。



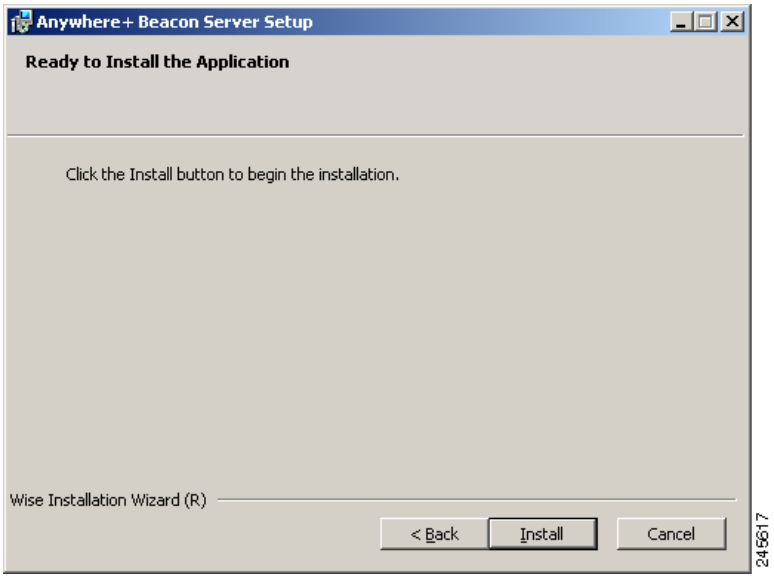
ステップ 2　[次へ（Next）] をクリックすると、[ライセンス契約書（License Agreement）] ダイアログが表示されます。



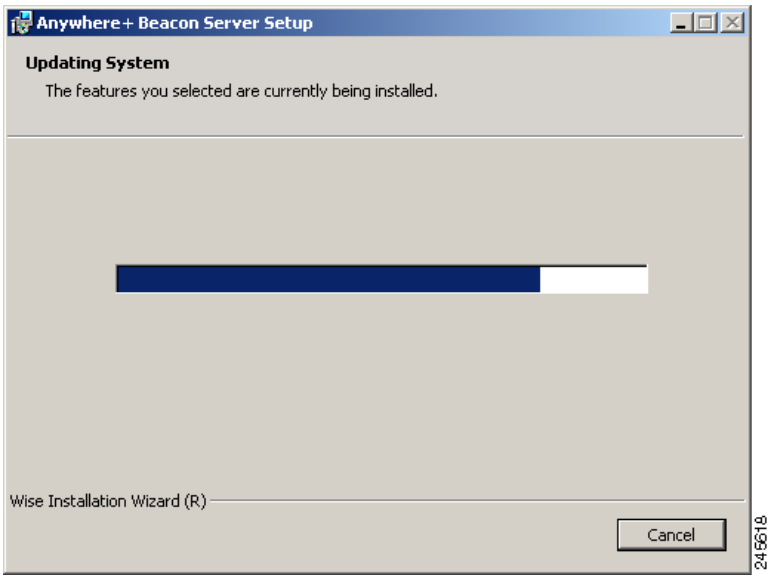
ステップ 3　エンド ユーザ ライセンス契約書を読みます。条件に同意する場合は [ライセンス契約書に同意します（I accept the license agreement）] をクリックし、次に [次へ（Next）] をクリックして [インストール先フォルダ（Destination Folder）] ダイアログを表示します。条件に同意しない場合は、[キャンセル（Cancel）] をクリックしてインストールを中止します。



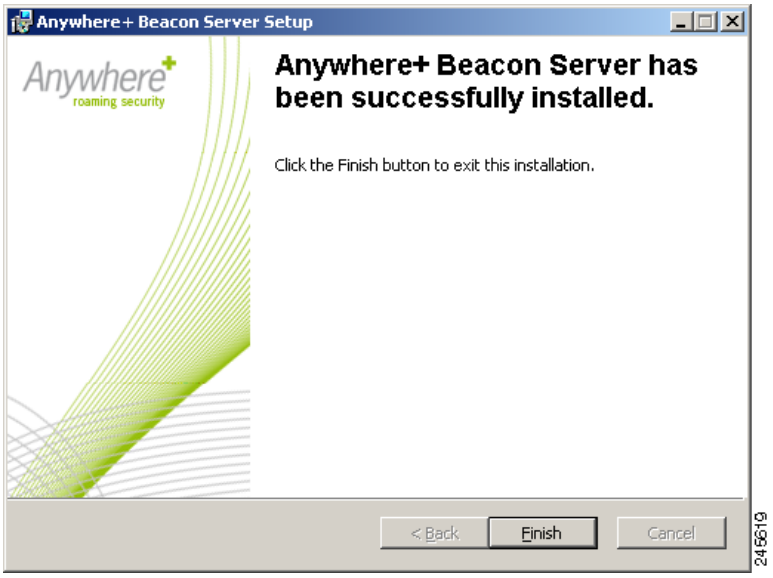
ステップ 4　[次へ（Next）] をクリックしてデフォルトのインストール フォルダを確定します。または、[参照（Browse）] をクリックして必要なフォルダに移動し、[次へ（Next）] をクリックして [アプリケーションをインストールします（Ready to Install the Application）] を表示します。



ステップ 5　[インストール（Install）] をクリックすると、インストールが開始されます。



ステップ 6　インストールが正常に完了すると、次のダイアログが表示されます。



（注）　インストールに問題が発生した場合、コマンド プロンプトからインストーラを起動します。msiexec /i <path>/BeaconServer.msi /l*vx install.log と入力します。install.log というログ ファイルが作成されます。

サイレント インストール

ビーコン サーバでは、次のコマンドを使用すると MSI インストーラのサイレント モードを利用できます。

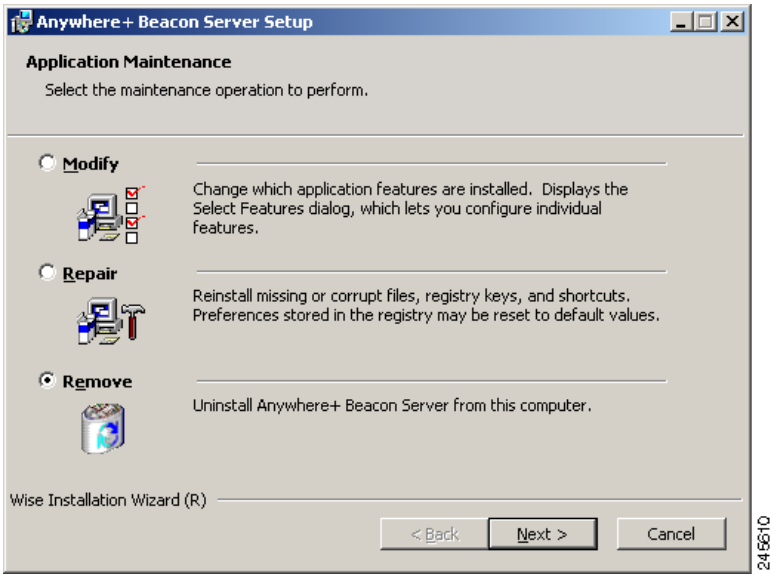
```
msiexec /i <path>/BeaconServer.msi /l*vx install.log /qn
```

パスは、ローカル フォルダ（C:\temp など）またはネットワーク共有（\\server\share など）のどちらでもかまいません。

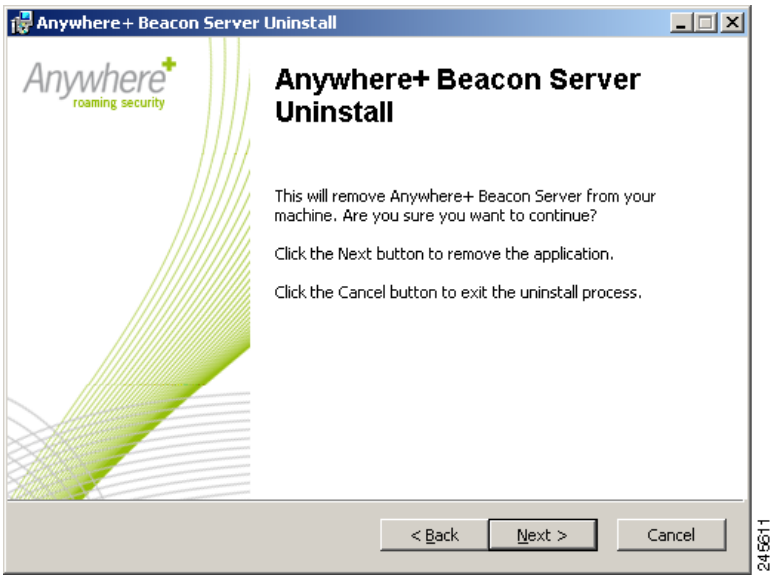
ビーコン サーバの削除

ビーコン サーバを削除する前に、ビーコン サーバ サービスが停止されていることを確認します。ビーコン サーバを削除するには、コントロール パネルのプログラムの追加と削除を使用するか、コマンド プロンプトで **msiexec /x <path>BeaconServer.msi /l*vx uninstall.log /qn** と入力します。または、ウィザードを使用してサーバからビーコン サーバを削除するには、次の手順を実行します。

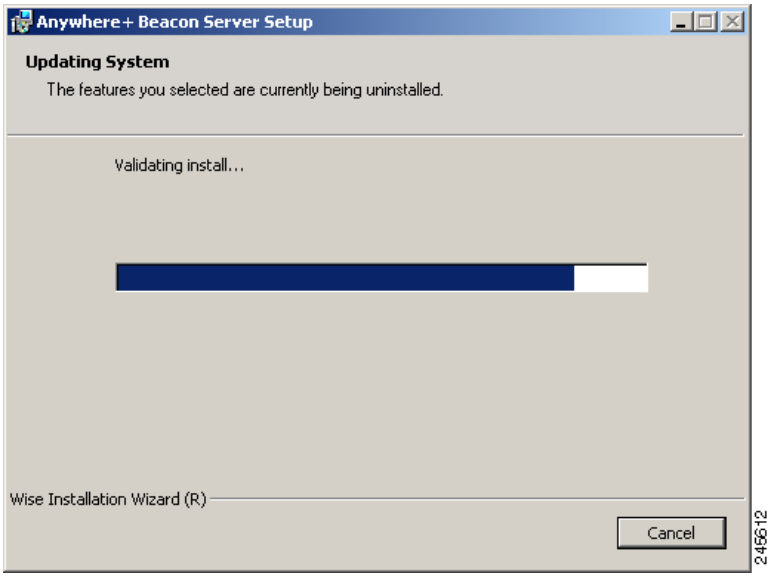
ステップ 1　BeaconServer.msi プログラム ファイルをダブルクリックして、ウィザードを実行します。



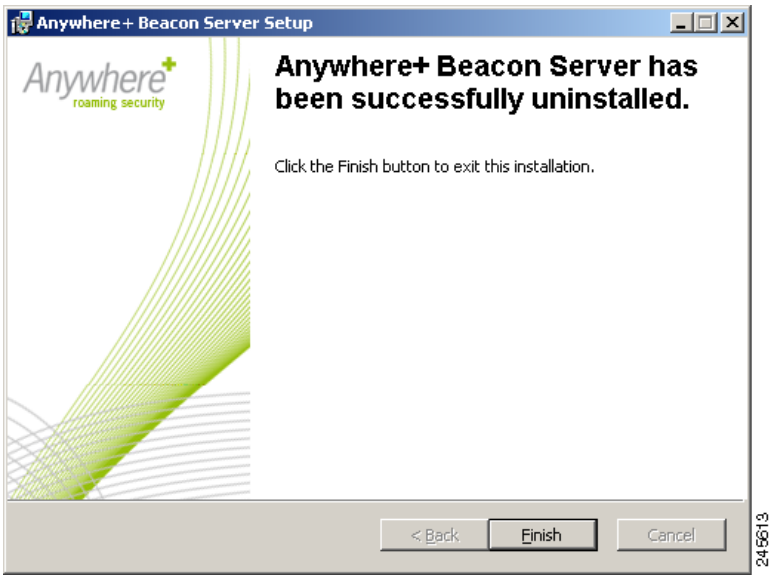
ステップ 2　[削除（Remove）] をクリックし、次に [次へ（Next）] をクリックして [ビーコン サーバのアンインストール（Beacon Server Uninstall）] ダイアログを表示します。



ステップ 3　[次へ（Next）] をクリックしてビーコン サーバを削除します。または、[キャンセル（Cancel）] をクリックして削除プロセスを中止します。



ステップ 4　削除が正常に完了すると、次のダイアログが表示されます。



ステップ 5　[完了（Finish）] をクリックしてウィザードを終了します。

ビーコン サーバの設定

ビーコン サーバを設定するには、BeaconServer.config XML ファイルを編集します。このファイルは、ビーコン サーバがインストールされているフォルダ（通常、C:\Program Files\Anywhere+ Beacon Server\）にあります。デフォルト設定は次のとおりです。

```
<DetectOnLANServer>
    <ConfigurationParameters>
        <!-- Beacon Port, default 6001 -->
        <BeaconPort>6001</BeaconPort>
        <!-- Connection Timeout in secs, default 10 -->
        <ConnectionTimeout>10</ConnectionTimeout>
        <!-- Disallowed Source IP addresses ';' separated -->
        <DisallowedSourceIP></DisallowedSourceIP>
        <Logging>
            <debug_level>00000107</debug_level>
            <!-- Log file size in kilobytes (KB) -->
            <LogFileSize>1000</LogFileSize>
            <!-- Number of log files to retain -->
            <NumLogFilesToRetain>10</NumLogFilesToRetain>
            <!-- This setting specifies the time for which a log file can be retained
before being deleted -->
            <LogFileRetentionTime>
                <Days>7</Days>
                <Hours>0</Hours>
                <Minutes>0</Minutes>
            </LogFileRetentionTime>
        </Logging>
    </ConfigurationParameters>
</DetectOnLANServer>
```

サポートから指示があった場合を除いて、次の要素だけを変更します。

BeaconPort	この要素は、サービスによって使用される TCP/IP ポートを指定します。ポート 6001 でサービスがすでに実行中の場合、この要素を変更できます。各クライアント コンピュータの Admin.cfg ファイル内の対応する要素も変更する必要があります。
ConnectionTimeout	この要素は、ビーコン サーバにデータを送信していない接続が閉じられるまでの時間を秒単位で指定します。
DisallowedSourceIP	この要素には、ビーコン サーバを経由する AnyConnect サービスをバイパスしない IP アドレスが含まれます。複数の要素を使用するのではなく、各 IP アドレスをセミコロン（;）で区切って 1 つの要素だけを使用します。
Logging	ロギングを参照してください。

ロギング

ログ ファイルの循環を管理する一連のサブタグが含まれます。

debug_level	カスタマー サポート担当者から指示がない限り、これは変更しません。
LogFileSize	許容される最大ログ ファイル サイズ（100 ～ 10,000 キロバイト）。現在のログ ファイルが許容される最大サイズに達すると、バックアップされて新しいログ ファイルが作成されます。デフォルトのサイズは 100 KB です。
NumLogFilesToRetain	保持する古いログ ファイルの数。デフォルトは 10 です。許容数に達すると、古いログ ファイルは削除されます。
LogFileRetentionTime	ログ ファイルの最大数に達したかどうかに関係なく、ログ ファイルが削除されるまでの時間。次のサブタグで指定します。 • Days • Hours • Minutes

システム トレイ アイコン

システム トレイ アイコンは、サービスのステータスを示します。


サービスが実行中です。


サービスに問題が発生しています。

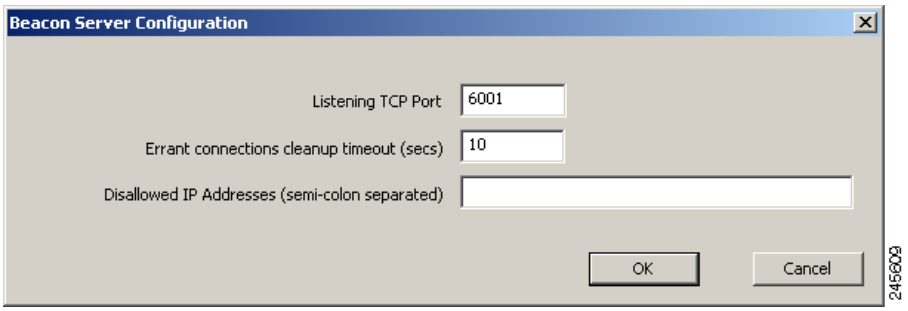

サービスが停止しているか、秘密キー ファイルがないか、秘密キー ファイルが破損しています。

サービスを開始するには、アイコンを右クリックして [ビーコン サーバの起動（Start Beacon Server）] をクリックします。

サービスを停止するには、アイコンを右クリックして [ビーコン サーバの停止（Stop Beacon Server）] をクリックします。

ビーコン サーバを設定するには、次の手順を実行します。

ステップ 1　アイコンを右クリックして [プリファレンス（Preferences）] をクリックし、[ビーコンの設定（Beacon Configuration）] ダイアログを表示します。



ステップ 2　[TCP ポートのリスニング（Listening TCP port）] ボックスに、サービスが使用する TCP/IP ポートを入力します。

ステップ 3　[不正接続クリーンアップ タイムアウト（秒）（Errant connections cleanup timeout (secs)）] ボックスに、接続を開いたままにする時間を秒単位で入力します。

ステップ 4　[不可 IP アドレス（セミコロン区切り）（Disallowed IP Addresses (semi-colon separated)）] ボックスに、AnyConnect サービスをバイパスする IP アドレスまたはホスト名をセミコロン（;）で区切って入力します。

ステップ 5　[OK] をクリックして、BeaconServer.config ファイルに変更を保存します。または、[キャンセル（Cancel）] をクリックして変更を破棄します。

システム トレイ アプリケーションを終了するには、アイコンを右クリックして [GUI の終了（Terminate GUI）] をクリックします。サービスが実行中の場合、これによってサービスは停止されません。システム トレイ アイコンを再起動するには、コマンド プロンプトに次のように入力します。

```
<BeaconServerInstallFolder>\BeaconServer -BD
```

Detect-On-LAN の設定

Detect-On-LAN 機能を設定するには、次の手順を実行します。

ステップ 1　ビーコン サーバの 1 つ以上のコピーをネットワークにインストールします。「ビーコン サーバのインストール」（P.6-20）を参照してください。

（注）　ビーコン サーバは、物理的に社内 LAN にするすべての Web セキュリティ インストールおよびフル トンネル VPN 経由で接続されている Web セキュリティ インストールからアクセス可能でなければなりません。

ステップ 2　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。クライアント プロファイルが、AnyConnect ユーザに導入するグループ ポリシーを指定していることを確認してください。

ステップ 3　「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）を使用して、Web セキュリティ クライアント プロファイルの [プリファレンス（Preferences）] パネルで次の設定を行います。

- [ビーコン確認（Beacon Check）] をオンにしてイネーブルにします。
- [パブリック キー ファイル（Public Key File）] フィールドで、公開 / 秘密キー ペアの一部として作成した公開キー ファイル（DOLpub.pem）を指定します。

- ビーコン サーバの各インスタンスの IP アドレスを [ビーコンの新しいアドレス（New Beacon Address）] フィールドに追加します。

ステップ 4　Web セキュリティ クライアント プロファイルの残りを設定して、保存します。

ステップ 5　Detect-On-LAN 機能が設定されたこの Web セキュリティ クライアント プロファイルを受信するには、ユーザは、ASA への VPN 接続の確立を試行する際に、AnyConnect Secure Mobility Client の [VPN] コンボ ボックスでこのクライアント プロファイルの名前を選択する必要があります。

認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信

ステップ 1　次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、ASDM を開いて [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。
- Windows OS のスタンドアロン モードで、[スタート（Start）] > [プログラム（Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択します。

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[認証（Authentication）] をクリックします。この手順で設定したフィールドの図については、図 6-6 を参照してください。

ステップ 4　[Proxy Authentication License Key] フィールドに、ScanCenter で作成した企業キー、グループ キー、またはユーザ キーに対応するライセンス キーを入力します。企業ドメインに基づいてユーザを認証する場合は、作成した企業キーを入力します。ScanCenter または Active Directory グループに基づいてユーザを認証する場合は、作成したグループ キーを入力します。デフォルトでは、このタグは空です。空のままにした場合、Web セキュリティはパススルー モードで動作します。

ステップ 5　[Service Password] に入力します。Web セキュリティのデフォルト パスワードは **websecurity** です。このパスワードは、プロファイルのカスタマイズ時に変更できます。パスワードには英数字（a ～ z、A ～ Z、0 ～ 9）のみを使用する必要があります。その他の文字は、Windows コマンド シェルによって制御文字と間違われる可能性があるか、XML で特殊な意味を持つことがあるためです。

このパスワードを使用して、管理者以外の権限を持っているユーザは、Web セキュリティ サービスの開始および停止を行うことができます。管理者権限を持つユーザは、このパスワードなしで Web セキュリティ サービスを開始および停止できます。詳細については、「この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。」（P.6-42）を参照してください。

ステップ 6　すべての HTTP 要求とともに企業ドメイン情報および ScanSafe または Active Directory グループ情報をスキャニング プロキシ サーバに送信できます。スキャニング プロキシは、ユーザのドメインおよびグループ メンバーシップについて認識している内容に基づいてトラフィック フィルタリング ルールを適用します。

（注）　ユーザのカスタム ユーザ名とカスタム グループ情報をスキャニング サーバ プロキシに送信する場合、または企業が Active Directory を使用しない場合は、この手順をスキップして、ステップ 7 に進みます。

- [エンタープライズ ドメインの使用（Use Enterprise Domains）] オプション ボタンをクリックします。

  ドメイン名を NetBIOS 形式で入力します。たとえば、**example.cisco.com** の NetBIOS 形式は **cisco** です。DNS 形式を使用したドメイン名（**abc.def.com**）を入力しないでください

  [エンタープライズ ドメイン名（Enterprise Domain name）] フィールドにドメイン名を指定すると、ScanCenter は、現在ログインしている Active Directory ユーザを識別して、そのユーザの Active Directory グループを列挙します。その情報は、すべての要求とともにスキャニング プロキシに送信されます。

  次のいずれかを示すには、企業ドメインとしてアスタリスク（*）を入力できます。

  - （*）は、任意のドメインを示すワイルドカードとして使用されます。Windows と Mac OS X の両方のコンピュータでは、企業ドメインの入力が（*）で、マシンがドメインにある場合、ユーザが属するすべてのドメインが一致し、ユーザ名とグループ メンバーシップ情報が ScanSafe スキャニング プロキシに送信されます。これは、複数のドメインが存在する企業にとって役に立ちます。
  - Mac OS X クライアントは、Active Directory ドメイン ユーザ名を持たないユーザには、IP アドレスの代わりにユーザ名を使用する必要があります。

- ScanSafe スキャニング プロキシに対する HTTP 要求でグループ情報を含めるか除外するには、[グループ包含リスト（Group Include List）] と [グループ除外リストの使用（Use Group Exclude List）] エリアを使用します。

  [グループ包含リスト（Group Include List）]。[グループ包含リスト（Group Include List）] の選択後に、HTTP 要求とともに ScanSafe スキャニング プロキシ サーバに送信する ScanSafe または Active Directory グループ名を [グループ包含リスト（Group Include List）] に追加します。要求が、指定された企業ドメイン内のユーザから出された場合、HTTP 要求は、ユーザのグループ メンバーシップに従ってフィルタリングされます。ユーザにグループ メンバーシップがない場合、HTTP 要求は、デフォルトのフィルタリング ルール セットを使用してフィルタリングされます。

  [グループ除外リスト（Group Exclude List）]。[グループ除外リスト（Group Exclude List）] の選択後に、HTTP 要求とともに ScanSafe スキャニング プロキシ サーバに送信しない ScanSafe または Active Directory グループ名を [グループ除外リスト（Group Exclude List）] に追加します。ユーザが、[グループ除外リスト（Group Exclude List）] のいずれかのグループに属している場合、そのグループ名はスキャニング プロキシ サーバに送信されず、ユーザの HTTP 要求は、その他のグループ メンバーシップ、または最低でも Active Directory または ScanSafe グループ所属を持たないユーザに対して定義されたデフォルトのフィルタリング ルール セットのいずれかによってフィルタリングされます。

ステップ 7　カスタム ユーザ名とグループ名をスキャニング プロキシ サーバに送信するには、[認証済みユーザ / グループの使用（Use Authenticated User/Group）] オプション ボタンをクリックします。

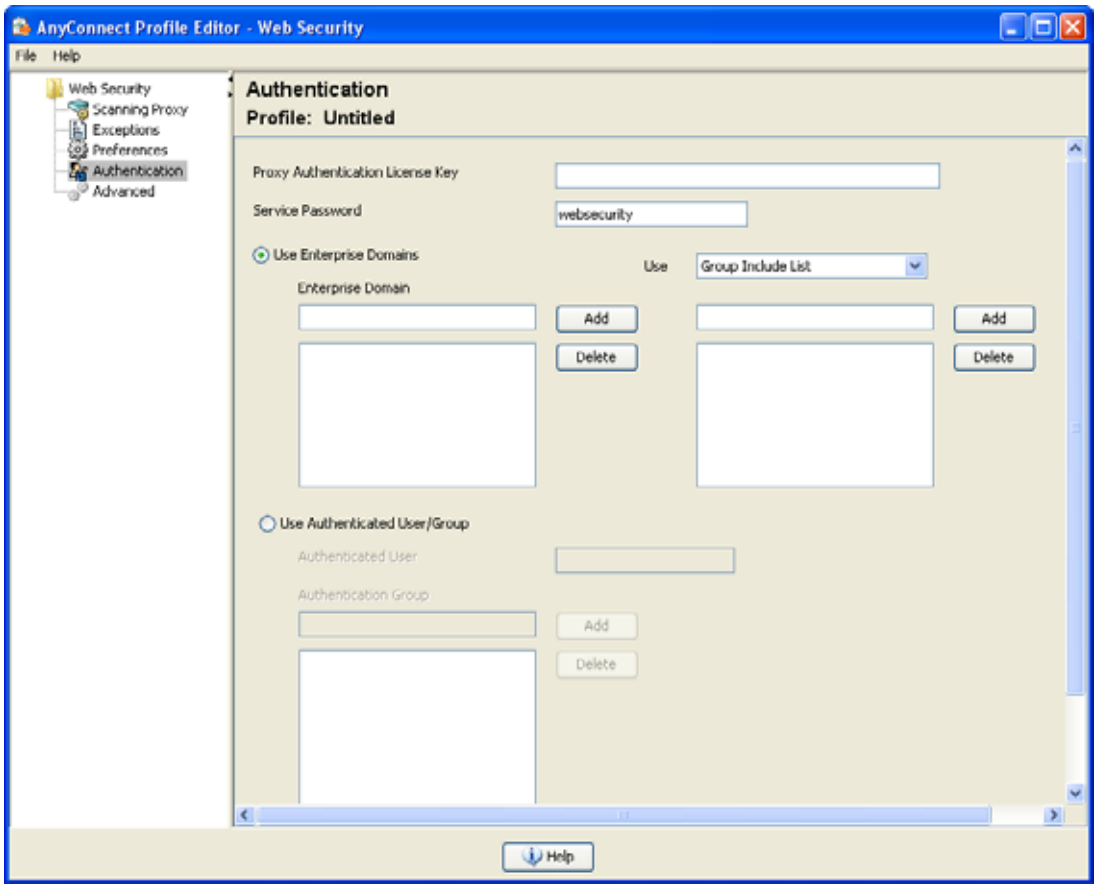
- [認証済みユーザ（Authenticated User）] フィールドに、カスタム ユーザ名を入力します。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する ScanCenter レポートで使用されます。
- [認証グループ（Authentication Group）] フィールドに、最大 256 文字の英数字のカスタム グループ名を入力します。

HTTP 要求がスキャニング プロキシ サーバに送信されると、カスタム グループ名が送信された場合に、スキャニング プロキシ サーバに対応するグループ名があれば、HTTP トラフィックは、カスタム グループ名に関連付けられたルールによってフィルタリングされます。スキャニング プロキシ サーバで定義された対応するカスタム グループがない場合、HTTP 要求はデフォルト ルールによってフィルタリングされます。

カスタム ユーザ名のみを設定し、カスタム グループを設定していない場合、HTTP 要求は、スキャニング プロキシ サーバのデフォルト ルールによってフィルタリングされます。

ステップ 8　Web セキュリティ クライアント プロファイルを保存します。

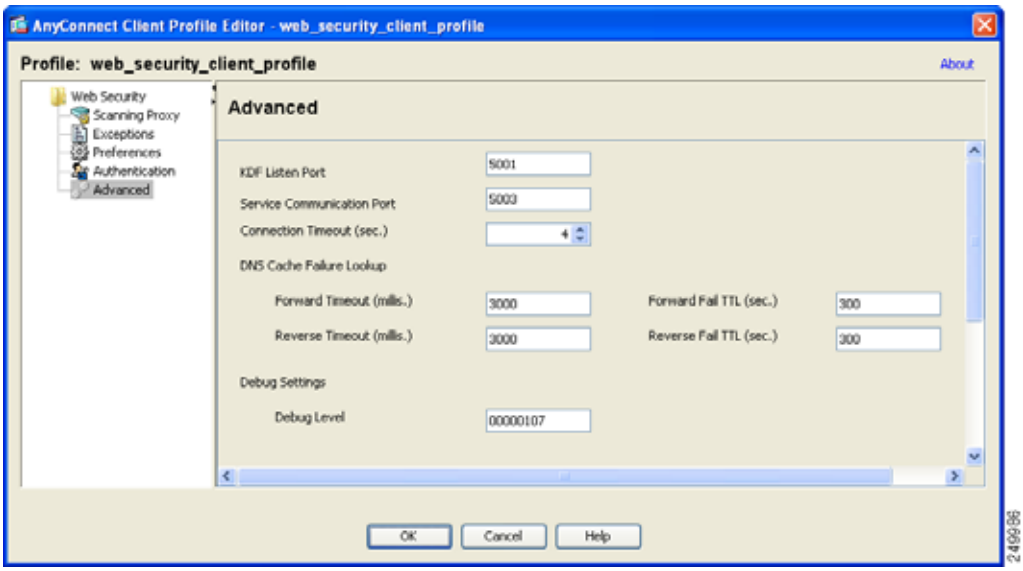
図 6-6　ScanSafe スキャニング プロキシ認証の設定



Web セキュリティの詳細設定

Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネルには、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ついくつかの設定が表示されます。このパネルの設定は、カスタマー サポートから指示された場合以外は変更しないでください。

図 6-7　Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネル



プロファイル エディタの [詳細（Advanced）] パネルで、次のタスクを実行できます。

- 「KDF リスニング ポートの設定」（P.6-34）
- 「サービス通信ポートの設定」（P.6-35）
- 「接続タイムアウトの設定」（P.6-35）
- 「DNS キャッシュ障害ルックアップの設定」（P.6-35）
- 「デバッグの設定」（P.6-36）

KDF リスニング ポートの設定

Kernel Driver Framework（KDF）は、トラフィック リスニング ポートの 1 つを宛先ポートとして使用する接続をすべて代行受信して、トラフィックを KDF リスニング ポートに転送します。Web スキャニング サービスは、KDF リスニング ポートに転送されるトラフィックをすべて分析します。

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[KDF リスン ポート（KDF Listen Port）] フィールドに KDF リッスン ポートを指定します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

サービス通信ポートの設定

サービス通信ポートは、Web スキャニング サービスが、AnyConnect GUI コンポーネントおよびその他のユーティリティ コンポーネントからの着信接続を受信するポートです。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[サービス通信ポート（Service Communication Port）] フィールドを編集します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

接続タイムアウトの設定

接続タイムアウト設定によって、Web セキュリティがスキャニング プロキシを使用せずに直接インターネットにアクセスしようとするまでのタイムアウトを設定できます。空白のままにすると、デフォルト値の 4 秒が使用されます。これにより、再試行する前にタイムアウトになるのをそれほど長く待機する必要がなく、ユーザは有料ネットワーク サービスにより速くアクセスできます。

[接続のタイムアウト（Connection Timeout）] フィールドを設定するには、次の手順に従います。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[接続のタイムアウト（Connection Timeout）] フィールドを変更します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

DNS キャッシュ障害ルックアップの設定

プロファイル エディタの [詳細（Advanced）] パネルに、ドメイン ネーム サーバ ルックアップを管理するためのフィールドがいくつか表示されます。これらは、DNS ルックアップに最適な値を使用して設定されています。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

デバッグの設定

[デバッグ レベル（Debug Level）] は設定可能なフィールドです。ただし、この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

Web セキュリティ ロギング

Windows OS

すべての Web セキュリティ メッセージは、Windows イベント ビューアの **Event Viewer (Local)\Cisco AnyConect Web Security Module** フォルダに記録されます。Web セキュリティがイベント ビューアに記録するイベントは、Cisco Technical Assistance Center のエンジニアによる分析用です。

Mac OS X

Web セキュリティ メッセージは、syslog またはコンソールから表示できます。

Web セキュリティ クライアント プロファイル ファイル

AnyConnect にバンドルされたプロファイル エディタを使用して Web セキュリティ クライアント プロファイルを作成して保存した後で、プロファイル エディタは、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.wsp を使用します。

スタンドアロン プロファイル エディタを使用して Web セキュリティ クライアント プロファイルを作成して保存した後で、プレーン テキスト バージョンのクライアント プロファイルのファイル命名規則は *filename*.xml になり、難解化ファイルの命名規則は *filename*.wso になります。

これらの 2 つの形式を使用することで、管理者は、必要に応じて次の特殊な処理を実行できます。

- 管理者は、難解化 Web セキュリティ クライアント プロファイルを ASA からエクスポートして、エンドポイント デバイスに配布できます。
- 管理者は、プレーン テキストの Web セキュリティ クライアント プロファイルを編集して、AnyConnect Web セキュリティ プロファイル エディタでサポートされない編集を実行できます。プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルは、カスタマー サポートから指示された場合以外は変更しないでください。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3　ファイルを保存するローカル フォルダを参照します。[ローカル パス（Local Path）] フィールドのファイル名を編集すると、その新しいファイル名で Web セキュリティ クライアント プロファイルが保存されます。

ステップ 4　[エクスポート（Export）] をクリックします。ASDM は、Web セキュリティ クライアント プロファイルのプレーン テキスト バージョンである *filename*.wsp をエクスポートします。

DART バンドルのプレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

Diagnostic AnyConnect Reporting Tool（DART）バンドルをシスコのカスタマー サービスに送信する必要がある場合、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイル ファイル *filename*.wsp または *filename*.xml を DART バンドルとともに送信する必要があります。シスコのカスタマー サービスは、難解化バージョンを読み取ることができません。

ASDM でプロファイル エディタによって作成されたプレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを収集するには、プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポートの手順を使用します。

スタンドアロン バージョンのプロファイル エディタは、2 つのバージョンの Web セキュリティ プロファイル ファイルを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.xml を使用します。プレーン テキスト バージョンのファイル *filename*.xml を収集します。

DART バンドルをシスコのカスタマー サービスに送信する前に、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを DART バンドルに追加します。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルの編集および ASDM からのインポート

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルをエクスポートしたら、任意のプレーン テキストまたは XML エディタを使用してローカル コンピュータで編集できます。インポートには、この手順を使用します。

注意　ファイルをインポートすると、選択した Web セキュリティ クライアント プロファイルの内容は**上書きされます**。

ステップ 1　ASDM を開いて [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　編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3　*filename*.wsp ファイルを変更した後で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページに戻って、編集したファイルのプロファイル名を選択します。

ステップ 4　[インポート（Import）] をクリックします。

ステップ 5　編集したバージョンの Web セキュリティ クライアント プロファイルを参照して、[インポート（Import）] をクリックします。

難解化 Web セキュリティ クライアント プロファイル ファイルのエクスポート

ステップ 1　ASDM を開き、[ツール（Tools）] > [ファイル管理（File Management）] を選択します。

ステップ 2　[ファイル管理（File Management）] 画面で、[ファイル転送（File Transfer）] > [ローカル PC とフラッシュ間（Between Local PC and Flash）] をクリックして、[ファイル転送（File Transfer）] ダイアログを使用して難解化 *filename*.wso クライアント プロファイル ファイルをローカル コンピュータに転送します。

スタンドアロン Web セキュリティ クライアント プロファイルのインストール

ASA がない場合に Web セキュリティ クライアント プロファイルを作成するには、スタンドアロン プロファイル エディタを使用します。

ステップ 1　[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択して、Web セキュリティ スタンドアロン プロファイル エディタを開きます。

ステップ 2　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。

ステップ 3　[ファイル（File）] > [保存（Save）] を選択して、Web セキュリティ クライアント プロファイルを保存します。スタンドアロン プロファイル エディタは、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.xml（ASDM ツールによって生成される wsp ファイルと同等）を使用します。

ステップ 4　名前 **WebSecurity_ServiceProfile.wso** の難解化 *filename*.wso クライアント プロファイル ファイルを名前変更するか、次のいずれかのディレクトリに保存します。

- Windows XP ユーザの場合、ファイルをフォルダ **%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** に入れます
- Windows Vista および Windows 7 ユーザの場合、ファイルをフォルダ **%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** に入れます
- Mac ユーザの場合、ファイルを次のフォルダに入れます。**/opt/cisco/anyconnect/websecurity**

ステップ 5　「Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化」（P.6-42）の手順に従って、Cisco AnyConnect Web セキュリティ エージェント Windows サービスを再起動します。

Web セキュリティ トラフィックのスプリットトンネリングの設定

Web セキュリティおよび VPN は同時に使用できます。この設定で最適なパフォーマンスを確保するには、ScanSafe スキャニング プロキシの IP アドレスをトンネルから除外することをお勧めします。

ScanSafe スキャニング プロキシに送信されるトラフィックに関する決定はすべて Web セキュリティ設定によって行われるため、他のスプリット除外を設定する必要はありません。

ScanSafe スキャニング プロキシ IP アドレスのリストを取得するには、アドレスのリストが記載されている次のライブ マニュアルを参照してください。

http://80.254.145.118/websecurity-config-v2ip.xml

Detect-On-LAN 機能を使用する場合に、Web セキュリティと VPN が同時にアクティブになるようにするには、ビーコン サーバが VPN トンネル経由で到達可能にならないようにネットワークを設定します。この方法では、ユーザが社内 LAN 上にいるときに限り、Web セキュリティ機能はバイパス モードになります。

Web セキュリティ クライアント プロファイルの ScanCenter ホステッド コンフィギュレーション サポートの設定

AnyConnect リリース 3.0.4 から、Web セキュリティ ホステッド クライアント プロファイルの ScanCenter ホステッド コンフィギュレーションにより、管理者は、Web セキュリティ クライアントに新しい設定を提供できます。これを行うには、Web セキュリティを使用するデバイスでクラウド（ホステッド コンフィギュレーション ファイルは ScanCenter サーバにあります）から新しい Web セキュリティ ホステッド クライアント プロファイルをダウンロードできるようにします。この機能の唯一の前提条件は、有効なクライアント プロファイルでデバイスに Web セキュリティがインストールされていることです。管理者は、Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを ScanCenter サーバにアップロードします。この XML ファイルには、ScanSafe からの有効なライセンス キーが含まれている必要があります。クライアントは、ホステッド コンフィギュレーション サーバへの適用後に、最大で 8 時間新しい設定ファイルを取得します。

ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Web セキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。新しいクライアント プロファイルをダウンロードした場合、Web セキュリティは、管理者が新しいクライアント プロファイル ファイルを使用可能にするまで同じファイルを再度ダウンロードしません。

クライアント プロファイル ファイルを作成して、Web セキュリティ デバイスでダウンロード可能にするプロセスは次のとおりです。

（注）　ホステッド コンフィギュレーション機能を使用するためには、ScanSafe ライセンス キーが含まれた有効なクライアント プロファイル ファイルを使用して、Web セキュリティ クライアント デバイスをあらかじめインストールしておく必要があります。

ステップ 1　Web セキュリティ プロファイル エディタを使用して、Web セキュリティ デバイス用の新しいクライアント プロファイルを作成します。このクライアント プロファイルには ScanSafe ライセンス キーが含まれている必要があります。ライセンス キーの詳細については、『ScanCenter Administration Guide, Release 5.1』を参照してください。

クライアント プロファイル ファイルをクリア テキストの XML ファイルとして保存します。このファイルを ScanCenter サーバにアップロードします。このファイルをアップロードすると、新しいクライアント プロファイルを Web セキュリティ クライアントで使用可能にできます。ScanSafe でのホステッド コンフィギュレーションの詳細については、『ScanCenter Administration Guide, Release 5.1』を参照してください。

企業でホステッド コンフィギュレーション機能がイネーブルになっている場合、新しいクライアント プロファイルは、企業の ScanCenter ポータルからアップロードおよび適用できます。ホステッド クライアント プロファイルはライセンスに関連付けられています。これは、使用中の別のライセンス（たとえば、別のグループ ライセンス キー）がある場合、各ライセンスには、独自のクライアント プロファイルが関連付けられていることを意味します。これによって、管理者は、使用するよう設定されているライセンスに応じて、異なるクライアント プロファイルを別のユーザにプッシュダウンできます。管理者は、ライセンスごとにさまざまな設定を格納して、ダウンロードするクライアントのデフォルト クライアント プロファイルを設定できます。その後、そのクライアント プロファイルをデフォルトとして選択することで、ホステッド コンフィギュレーション ポータルに格納されている他のリビジョンの設定の 1 つに切り替えることができます。1 つのライセンスに関連付けることができるクライアント プロファイルは 1 つのみです。これは、複数のリビジョンがライセンスに関連付けられている場合に、1 つのクライアント プロファイルのみをデフォルトにできることを意味します。

ステップ 2　クライアントがホステッド クライアント プロファイルをダウンロードした後で、新しいクライアント プロファイルが自動的に使用されますが、ユーザは次のいずれかを行う必要があります。

- デバイスをスリープ モードにしてから、再開する。再開時に、クライアントは新しい設定を使用します。
- デバイスを再起動する。
- デバイスで Web セキュリティ エージェント サービスを再開する。

（注）　Web セキュリティ エージェント サービスの再開オプションは、サービスを再開するために必要な権限を持つユーザのみが使用可能です。

Detect-On-LAN

Detect-On-LAN 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。

正しい公開キーを持つ Web セキュリティ クライアントのみが、ネットワークへの接続中にスキャニング プロキシをバイパスできるように、ビーコン サーバは、組織に固有の公開 / 秘密キー ペアを使用します。同じ秘密 / 公開キー ペアを使用する場合、必要に応じて、ビーコン サーバの複数のコピーを導入することもできます。秘密 / 公開キー ペアは、ScanCenter ポータルで生成します。

ネットワークにプロキシが存在する（ScanSafe Connector など）状態で、ビーコン サーバを使用しない場合は、プロファイル エディタの [除外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。詳細については、「プロキシ例外」（P.6-15）を参照してください。

データ損失防止（DLP）アプライアンスなど、一部のサードパーティ ソリューションでは、Detect-On-LAN の設定も必要です。トラフィックが Web セキュリティの影響を受けないようにする必要があります。

秘密キーおよび公開キーの生成

ビーコン サーバは、認証に RSA 公開 / 秘密キー ペアを使用します。秘密キーの長さは 512 ビット以上である必要があります。ただし、シスコでは 1,024 ビットのキーを推奨します。

秘密キー ファイル名は DOLprv.pem、公開キー ファイル名は DOLpub.pem にする必要があります。公開キーは、設定ファイルに組み込まれます。

RSA キー ペアを生成するには、Microsoft Certificate Services（Windows Server オペレーティング システムのコンポーネント）や OpenSSL（http://www.openssl.org/）などのツールが必要です。Microsoft Certificate Services の使用については、ベンダーのマニュアルを参照してください。

OpenSSL を使用した秘密キーの生成

openssl.exe プログラム ファイルが含まれているフォルダに移動して、次のように入力します。

```
openssl genrsa -out DOLprv.pem 1024
```

DOLprv.pem ファイルを、BeaconServer.msi ファイルが含まれているフォルダにコピーします。または、ビーコン サーバがすでにインストールされている場合は、DOLprv.pem ファイルを、ビーコン サーバをインストールしたフォルダにコピーします。

OpenSSL を使用した公開キーの生成

公開キーを生成する前に、DOLprv.pem という秘密キーを openssl.exe プログラムと同じフォルダ内に作成する必要があります。公開キーを作成するには、次を入力します。

```
openssl rsa -in DOLprv.pem -out DOLpub.pem -outform PEM -pubout
```

DOLpub.pem ファイルを、AnyConnect Web セキュリティ モジュールをインストールしたフォルダにコピーします。

注意　AnyConnect Web セキュリティ モジュールのインストール時に公開キーを導入していない場合、AnyConnect がインストールされているすべてのコンピュータに手動でインストールする必要があります。

Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化

管理者は、次の手順を実行することで、Web トラフィックを代行受信する Cisco AnyConnect Web セキュリティ エージェントの機能をディセーブルおよびイネーブルにできます。

Windows を使用したフィルタのディセーブル化およびイネーブル化

この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

ステップ 1　コマンド プロンプト ウィンドウを開きます。

ステップ 2　**%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** フォルダに変更します。

ステップ 3　フィルタリングをディセーブルまたはイネーブルにします。

- フィルタリングをイネーブルにするには、**acwebsecagent.exe -enablesvc** と入力します
- フィルタリングをディセーブルにするには、**acwebsecagent.exe -disablesvc -*servicepassword*** と入力します

Mac OS X を使用したフィルタリングのディセーブル化およびイネーブル化

この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

ステップ 1　端末アプリケーションを起動します。

ステップ 2　**/opt/cisco/anyconnect/bin** フォルダに変更します。

ステップ 3　フィルタリングをディセーブルまたはイネーブルにします。

- フィルタリングをイネーブルにするには、**acwebsecagent -enablesvc** と入力します
- フィルタリングをディセーブルにするには、**acwebsecagent -disablesvc -*servicepassword*** と入力します

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。

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。

（注）　この機能は Mac OS X クライアントでは使用不可です。

CHAPTER 7

WSA に対する AnyConnect テレメトリの設定

AnyConnect Secure Mobility Client 用の AnyConnect テレメトリ モジュールでは、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。この Web フィルタリング インフラストラクチャでは、Web セキュリティ スキャニング アルゴリズムの強化、URL カテゴリと Web レピュテーション データベースの精度の向上、最終的な URL フィルタリング ルールの改良のために、このデータを使用します。

AnyConnect テレメトリ モジュールは、次の機能を実行します。

- エンドポイントでコンテンツの到着を監視します。
- 可能であれば、エンドポイントで受信する任意のコンテンツの発信元を識別および記録します。
- 悪意のあるコンテンツの検出およびその発信元を、シスコの Threat Operations Center にレポートします。
- 24 時間ごとに ASA を調べて、更新されたホスト スキャン イメージを確認します。更新されたホスト スキャン イメージが提供されている場合は、イメージをエンドポイントにダウンロードします。

ここでは、次の項目について説明します。

システム要件

AnyConnect テレメトリ モジュール（以降、「テレメトリ モジュール」）は、以下のプラットフォームで実行されている、このリリースの AnyConnect Secure Mobility Client で使用可能です。

- Windows 7（x86（32 ビット）および x64（64 ビット））
- SP2 を適用した Windows Vista（x86（32 ビット）および x64（64 ビット））
- Windows XP SP3（x86（32 ビット）および x64（64 ビット））

テレメトリ モジュールでは、Internet Explorer 7、Internet Explorer 8 など、**wininit.dll** を使用するブラウザについてのみ、URL 発信元のトレースを実行できます。Firefox、Chrome など **wininit.dll** を使用しないブラウザを使用してファイルをダウンロードした場合、ファイルのダウンロードに使用されたブラウザは識別できますが、ファイルのダウンロード元の URL は識別できません。

テレメトリ モジュールを使用するには、AnyConnect ポスチャ モジュールでサポートしているアンチウイルス アプリケーションをエンドポイントにインストールする必要があります。

（注）　AnyConnect ポスチャ モジュールは、CSD に付属しているイメージと同じホスト スキャン イメージを含みます。ホスト スキャンでサポートされるアンチウイルス、アンチスパイウェア、ファイアウォール アプリケーションのリストは、AnyConnect と CSD で同一です。

ASA と ASDM に関する要件

AnyConnect Secure Mobility Client をテレメトリ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM が 6.3.1

AnyConnect Secure Mobility Client モジュールに関する要件

テレメトリ モジュールは AnyConnect Secure Mobility Client のアドオンであり、以下のモジュールを以下の順序でエンドポイントにインストールする必要があります。

1. AnyConnect VPN モジュール
2. AnyConnect ポスチャ モジュール
3. AnyConnect テレメトリ モジュール

Cisco IronPort Web セキュリティ アプライアンスの相互運用性に関する要件

テレメトリ機能は、Cisco IronPort Web セキュリティ アプライアンス（WSA）と組み合わせて AnyConnect セキュア モビリティ ソリューションを使用している場合のみイネーブルにできます。WSA を使用するには、WSA セキュア モビリティ ソリューション ライセンスが必要です。必要な WSA の最小バージョンは 7.1 です。

AnyConnect テレメトリ機能を使用するには、セキュア モビリティ ソリューションを適切に設定しておく必要があります。まだ設定していない場合は、「AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定」（P.2-49）を参照し、説明に従って、WSA と適切に連携するように ASA を設定してください。

Cisco IronPort Web セキュリティ アプライアンス上での SenderBase のイネーブル化

テレメトリ モジュールでは、Threat Operations Center に転送したり、他の脅威情報と集約したりできるように、ウイルス攻撃のインシデント情報およびアクティビティ情報を WSA に送信します。これを行うには、WSA で、標準モードの SenderBase ネットワーク参加がイネーブルになっている必要があります。

以下は、SenderBase セキュリティ サービスをイネーブルにする手順の概略です。SenderBase セキュリティ サービスの詳細な説明については、WSA のマニュアルを参照してください。

1. Web ブラウザを使用して、WSA 管理者 GUI にログインします。
2. [セキュリティ サービス（Security Services）] > [SenderBase] を選択します。
3. SenderBase ネットワーク参加がディセーブルの場合は、[有効（Enable）] をクリックしてから [グローバル設定の編集（Edit Global Settings）] をクリックして、参加レベルを設定します。標準（フル）参加をお勧めします。

（注）　制限付き参加レベルと標準参加レベルの違いの詳細については、『*IronPort AsyncOS for Web User Guide*』を参照してください。

4. 変更を送信し、保存します。

AnyConnect テレメトリ モジュールのインストール

テレメトリ モジュールをインストールする前に、エンドポイントに AnyConnect Secure Mobility Client および AnyConnect ポスチャ モジュールをインストールする必要があります。Web 展開方式および事前展開方式を使用してテレメトリ モジュールをインストールする手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。テレメトリ モジュールを展開する基本手順のみを知りたい場合は、AnyConnect テレメトリ モジュールの高速展開を参照してください。

テレメトリ モジュールをインストールすると、開始されるすべての新規プロセスについて、アクションの記録が即座に開始されます。ただし、テレメトリ モジュールでは、モジュールをインストールする前からコンピュータ上で実行されていたプロセスのアクションは記録できません。

テレメトリ モジュールのインストール後、ユーザがログアウトしてログインし直すまでは、ファイルのコピーや名前変更など、Windows エクスプローラ（explorer.exe）のプロセスはテレメトリ モジュールによって追跡されません。さらに、テレメトリ モジュールでは、ユーザがコンピュータをリブートしないうちは、ユーザ ログインの前に開始された他のプロセスのアクションを記録できません。

（注）　要件ではありませんが、テレメトリ モジュールのインストール後にエンドポイントをリブートすることを、強くお勧めします。

AnyConnect テレメトリ モジュールの高速展開

AnyConnect とともにテレメトリ モジュールを展開する場合に実行する必要のある手順の概略を以下に示します。この手順は、グループ ポリシーおよび AnyConnect VPN ユーザ用の接続プロファイルをすでに設定してあることを前提としています。AnyConnect テレメトリ モジュールを展開するには、次の手順を実行します。

ステップ 1　Cisco.com から AnyConnect Windows パッケージをダウンロードします。このファイルは、次の命名規則に従っています。anyconnect-win-*<version>*-k9.pkg

ステップ 2　AnyConnect Windows パッケージを ASA にアップロードします。

a. ASDM を起動し、[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。

b. [追加（Add）] をクリックします。

c. AnyConnect Windows パッケージを ASDM にアップロードします。プロンプトが表示されたら、AnyConnect パッケージを現在の新しいイメージとして使用するために、[OK] をクリックします。

d. [OK] をクリックします。[適用（Apply）] をクリックします。

e. **ASDM** を再起動します。

ステップ 3　AnyConnect パッケージをホスト スキャン パッケージに指定し、ホスト スキャンをイネーブルにします。

a. ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。

b. [フラッシュの参照（Browse Flash）] をクリックし、前のステップでホスト スキャン イメージとしてアップロードした anyconnect-win-<*version*>-k9.pkg を選択します。

c. [ホスト スキャン /CSD の有効化（Enable Host Scan/CSD）] をオンにします。

d. [適用（Apply）] をクリックします。

e. **ASDM** を再起動します。

（注）　このステップを実行すると、クライアントレス SSL VPN アクセスのホスト スキャンもイネーブルになります。

ステップ 4　テレメトリをオプション モジュールとして展開するように、グループ ポリシーを設定します。

a. 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）] > [グループ ポリシー（Group Policies）] を選択し、編集するグループ ポリシーを選択して [編集（Edit）] をクリックします。

b. [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] の順に選択します。

c. [ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] オプションの [継承（Inherit）] チェックボックスをオフにします。ドロップダウン ボックスから、[AnyConnect テレメトリ（AnyConnect Telemetry）] および [AnyConnect ポスチャ（AnyConnect Posture）] を選択します。

d. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 5　ここで設定したグループ ポリシーを指定する接続プロファイルを設定します。

a. 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、テレメトリ用に設定する接続プロファイルを選択します。[編集（Edit）] をクリックします。[Basic] 設定パネルが自動的に開きます。

b. [デフォルト グループ ポリシー（Default Group Policy）] エリアで、前のステップでテレメトリの展開用に設定したグループ ポリシーを選択します。

c. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 6　テレメトリ クライアント プロファイルを作成し、テレメトリをイネーブルにします。

a. 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。

b. [追加（Add）] をクリックしてテレメトリ プロファイルを作成します。プロファイルに名前を付け、[プロファイルの使用（Profile Usage）] フィールドで [テレメトリ（Telemetry）] を選択します。

c. [グループ ポリシー（Group Policy）] フィールドで、テレメトリの展開用に作成したグループ ポリシーをオプション モジュールとして選択します。[OK] をクリックします。

d. [プロファイル名（Profile Names）] リストから、ここで作成したテレメトリ クライアント プロファイルを選択し、[Edit] をクリックします。

e. [テレメトリ サービス（Telemetry Policy）] パネルの [サービスの有効化（Enable Service）] をクリックし、テレメトリ クライアント プロファイルに対するすべてのデフォルト値を受け入れます。

f. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 7　セキュア モビリティ ソリューションをイネーブルにします。

a. 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）] > [セキュア モビリティ ソリューション（Secure Mobility Solution）] を選択します。

b. [サービスの設定（Service Setup）] エリアで、[モバイル ユーザ セキュリティ サービスの有効化（Enable Mobile User Security Service）] をオンにします。

c. [適用（Apply）] をクリックします。[保存（Save）] をクリックします。

AnyConnect テレメトリ モジュールの相互運用性

この項では、テレメトリ モジュールと他の AnyConnect Secure Mobility Client コンポーネントの対話について説明します。

- AnyConnect VPN モジュール
- AnyConnect ポスチャ モジュール
- サードパーティ製アンチウイルス ソフトウェア

AnyConnect VPN モジュール

AnyConnect VPN モジュールでは、以下の方法でテレメトリ モジュールと対話します。

- AnyConnect の VPN サービス プロセスは、サービスの開始時に、他のすべてのプラグイン モジュールとともに、テレメトリ モジュールのロードと初期化を行います。
- AnyConnect VPN モジュールでは、状態が変化したときに、セッション状態情報および AnyConnect Secure Mobility（ACSM）状態情報を提供します。
- AnyConnect VPN モジュールでは、WSA からテレメトリ設定を取得するための、WSA からのセキュア モビリティ サービス ステータス応答の XML を用意します。

これ以外に、テレメトリ モジュールと VPN モジュールとの対話はほとんどなく、VPN モジュールがテレメトリ モジュールをシャットダウンするか、VPN プロセスが終了するまで、独立してを実行されます。

AnyConnect ポスチャ モジュール

AnyConect ポスチャ モジュール（以降「ポスチャ モジュール」）は、ホスト スキャン イメージを含みます。ホスト スキャン イメージは、ホスト スキャン互換のアンチウイルス ソフトウェアからのウイルス検出情報をテレメトリ モジュールに渡します。ホスト スキャンでは、テレメトリ レポートで必要な場合、システム ポスチャ情報を AnyConnect テレメトリ モジュールに渡すこともできます。

テレメトリ モジュールでは、24 時間ごとに ASA を調べて更新されたホスト スキャン イメージを確認します。更新されたホスト スキャン イメージが ASA にインストールされている場合、テレメトリ モジュールはイメージを取得して、更新をエンドポイントに自動的にインストールします。

サードパーティ製アンチウイルス ソフトウェア

AnyConnect テレメトリ モジュールを使用するには、ウイルスおよびマルウェアを検出する、ホスト スキャン準拠のアンチウイルス アプリケーションが必要です。ホスト スキャンでは、アンチウイルス アプリケーションの脅威ログを定期的に確認し、ウイルス検出インシデントをテレメトリ モジュールに転送します。

アンチウイルス アプリケーションの脅威ログは、常にイネーブルにされている必要があります。そうでない場合、ホスト スキャンでは、テレメトリ レポートをトリガーできません。

テレメトリ アクティビティ履歴リポジトリ

テレメトリ アクティビティ履歴リポジトリは、テレメトリ モジュールでアクティビティ ファイルを保存する、エンドポイント上のディレクトリです。アクティビティ履歴リポジトリは次の場所にあります。

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\data\

テレメトリ モジュールでは、システム操作、ユーザ操作、API 関数呼び出しを代行受信します。テレメトリ モジュールでは、これらの情報を使用して、エンドポイントに着信するコンテンツの発信元を識別できます。テレメトリ モジュールでは、Internet Explorer（iexplorer.exe）による URL からのファイルのダウンロード、Windows エクスプローラ（explorer.exe）によるリムーバブル デバイスからのファイルのコピーなど、アプリケーション アクティビティに、この情報を集約します。

テレメトリ モジュールは、このアクティビティを収集し、activity.dat ファイルに記録します。activity.dat ファイルが、アクティビティ履歴ファイルです。

activity.dat ファイルのサイズがほぼ 1 MB になると、テレメトリ モジュールは、保存時点のタイムスタンプを名前とする新しいファイル、たとえば、20110114111312430.dat として、現在の activity.dat ファイルを保存します。テレメトリ モジュールは、次に、引き続き最新のアクティビティ履歴を保存する、新しい activity.dat ファイルを作成します。

アクティビティ履歴リポジトリが一定のサイズに達すると、テレメトリ モジュールは、一番古いアクティビティ履歴ファイルを削除します。アクティビティ履歴リポジトリのサイズは、テレメトリ プロファイルに設定されている [Maximum History Log] 変数によって管理されます。一定期間が経過したアクティビティ履歴ファイルは、テレメトリ モジュールによって、アクティビティ履歴リポジトリから削除されます。アクティビティ履歴ファイルの存続期間は、テレメトリ プロファイルに設定されている [Maximum History (Days)] 変数によって定義されます。これらの変数の設定手順については、「テレメトリ クライアント プロファイルの設定」（P.7-10）を参照してください。

（注）　テレメトリ モジュールでは、winnit.dll、Kerel32.dll などの Windows 関数からアクティビティ情報を受信します。これらの関数を使用していないブラウザまたは電子メール アプリケーションの場合、テレメトリ モジュールでは、いずれのアクティビティ データも受信しません。したがって、テレメトリ モジュールでは、Firefox、Chrome などのブラウザからアクティビティ履歴を受信しません。

（注）　アクティビティ履歴リポジトリに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。詳細については、「URL の暗号化」（P.7-9）を参照してください。

テレメトリのレポート

テレメトリ レポートは、ローカル アンチウイルス ソフトウェアによって識別されたウイルスに関する情報およびエンドポイントをウイルスから保護するためにアンチウイルス ソフトウェアが実行したアクションに関する情報を含みます。テレメトリ モジュールは、レポートを暗号化して WSA に送信します。WSA は、このレポートを Cisco Threat Operations Center（TOC）に転送します。TOC では、このレポートを他のレポートと組み合わせて、新しい URL フィルタとマルウェア フィルタ エンジンの更新を生成し、すべての WSA に配布します。

各テレメトリ レポートは、インシデント セクション 1 つと、それに続く 1 つ以上のアクティビティ セクションを持ちます。インシデント セクションは、マルウェア、ローカル アンチウイルス アプリケーション、マルウェアから防御するために実行されたアクション、エンドポイントのシステム情報に関する情報を含みます。アクティビティ セクションは、インシデントにつながったアクティビティおよびウイルスの発信元の候補に関する情報を含みます。

エンドポイントがバーチャル プライベート ネットワークを介して ASA に接続されている場合、テレメトリ モジュールでは、ASA を介して、WSA に即座にレポートを送信します。WSA へのレポートの送信を終えたテレメトリ モジュールは、ローカル コピーを削除します。

エンドポイントが VPN を介して ASA に接続されていない場合、テレメトリ モジュールでは、エンドポイント上の次の場所にレポートを保存します。

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\reports\

テレメトリ レポート ファイル名には、レポートの作成時刻の年月日、時間、分、秒を反映する、**YYYYMMDDHHSSmmm.trt** という命名規則が使用されます。

（注）　テレメトリ レポートに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。詳細については、「URL の暗号化」（P.7-9）を参照してください。

テレメトリ モジュールによる個人情報の移動の可能性

テレメトリ インシデント レポートは、マルウェアの名前に加え、ローカル システム上でマルウェアが検出された場所も含みます。この場所であるディレクトリ パスは、多くの場合、マルウェアをダウンロードしたユーザのユーザ ID を含みます。たとえば、Jonathan Doe が「malware.txt」をダウンロードした場合、テレメトリ レポートに含まれるディレクトリ名は、「C:\Documents and Settings**jdoe**\Local Settings\Temp\Cookies**jdoe**@malware[1].txt」のようになります。

（注）　シスコのエンド ユーザ ライセンス契約書に同意してテレメトリ モジュールをインストールすると、シスコによる個人情報および非個人情報の収集、使用、処理、保管に同意することになります。この個人情報と非個人情報は、ユーザによるシスコ製品との対話方法をシスコが知るためや、ネットワーク処理の技術サポートの提供とシスコの製品とサービスの改良を目的として、シスコに転送されます。これには、米国や欧州経済領域外のその他の国に対するこれらの情報の転送を含みます。シスコは、選ばれた第三者と、匿名化して集約された形式で、この情報を共有することがあります。この個人情報および非個人情報を使用して、個人の特定や問い合わせを行うことはありません。これらの個人情報および非個人情報の使用には、シスコのプライバシー ポリシー（http://www.cisco.com/web/siteassets/legal/privacy.html）が適用されます。個人情報および非個人情報の収集、使用、処理、保管に関するこの同意は、テレメトリ モジュールをオフにするか、テレメトリ モジュールをアンインストールすることにより、随時撤回できます。

テレメトリのワークフロー

以下の手順は、テレメトリ モジュールによる情報の収集方法と WSA へのレポート方法の一例を示します。

1. ユーザが Web サイト **http://www.unabashedevil.com** を開き、圧縮ファイル **myriad_evils.zip** をダウンロードします。テレメトリ モジュールは、両方のアクティビティを記録し、activity.dat に保存します。
2. 少し経ってから、ユーザが圧縮ファイルから内容の **evil_virus.exe** を解凍します。テレメトリ モジュールは、このアクティビティを記録し、activity.dat に保存します。
3. ホスト スキャン準拠のアンチウイルス アプリケーションが **evil_virus.exe** に含まれているウイルスを識別し、ファイルを削除します。アンチウイルス アプリケーションのアクティビティを契機として、テレメトリ モジュールは、このインシデントに関するレポートを作成します。
4. テレメトリ モジュールは、この時点で activity.dat ファイル内の情報をさかのぼりながら処理して、ウイルスの発信元を判別します。テレメトリ モジュールでは、アンチウイルス アプリケーション インシデントから、**evil_virus.exe** がウイルスであったこと、およびアンチウイルス アプリケーションによって削除されたことを確認します。テレメトリ モジュールは、activity.dat ファイルから、**evil_virus.exe** が **myriad_evils.zip** から解凍されたことおよびこの圧縮ファイルは **http://www.unabashedevil.com** からダウンロードされたことを確認します。

   このすべての情報が、1 つのレポートに結合されます。
5. テレメトリ モジュールは、テレメトリ レポートを WSA に転送します。
   - エンドポイントがバーチャル プライベート ネットワークを介して ASA に接続されている場合、テレメトリ モジュールでは、レポートを即座に WSA に送信し、レポートのローカル コピーを削除します。
   - エンドポイントが VPN を介して ASA に接続されていない場合、テレメトリ モジュールは、レポート リポジトリにレポートを保存し、次回チャンスのあるときに WSA に送信します。
6. SenderBase ネットワークへの参加がイネーブルの場合、WSA では、Threat Operations Center にレポートを転送します。そこで、他の情報源からのデータと合わせて、この情報が分析されます。WSA は、テレメトリ データなど複数情報源からの情報を組み込んだ、URL カテゴリおよび Web レピュテーション データベースに対するシグニチャ更新を受信します。この新規シグニチャ更新および WSA に設定されているさまざまなポリシーに応じて、ユーザによる **http://www.unabashedevil.com** へのアクセスがブロックされ、**myriad_evils.zip** のダウンロードが禁止されます。

URL の暗号化

アクティビティ履歴リポジトリおよびテレメトリ レポート リポジトリに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。

テレメトリ モジュールでは、URL を「内部」または「外部」のいずれかとして扱います。内部 URL の例としては、会社のイントラネット ホーム ページがあります。外部 URL の例としては、インターネット上でアクセスできる任意の URL があります。

SenderBase ネットワークへの参加から除外するように WSA 上に設定されているすべてのドメインおよび IP アドレスは、テレメトリ モジュールでは、内部 URL として定義されます。いずれのドメインおよび IP アドレスも Senderbase ネットワークへの参加から除外しない場合、テレメトリ モジュールでは、すべての URL を外部として扱います。

内部と外部の両方の URL が暗号化された形式でテレメトリ レポートに組み込まれ、WSA に送信されます。

テレメトリ レポートおよびアクティビティ履歴リポジトリに指定されるすべての内部 URL は、内部 URL 用の対称 AES キーを使用して暗号化されます。テレメトリ レポートおよびアクティビティ履歴リポジトリに指定されるすべての外部 URL は、外部 URL 用の対称 AES キーを使用して暗号化されます。これらの対称 AES キーは、各 VPN セッションの開始時またはテレメトリ サービスの開始時に、ランダムに生成されます。

内部 URL の暗号化に使用された AES キーは、自社の公開キーで暗号化されて、AES 暗号化された内部 URL とともに、テレメトリ レポートに含めて送信されます。テレメトリ プロファイル内の公開キーは、[カスタム証明書（Custom Certificates）] エリアで指定できます。自社で用意した、PEM 形式の任意の X.509 公開キー証明書を公開キーとして使用できます。

外部 URL の暗号化に使用された AES キーは、シスコの公開キーおよび自社の公開キーによって暗号化されます。両方の暗号化バージョンの AES キーが、AES 暗号化された外部 URL とともに、テレメトリ レポートに含めて送信されます。シスコの公開キーは、シスコの公開証明書の 1 つであり、テレメトリ モジュールと一緒に配布されます。ASDM または ASA を使用してシスコの公開キーを変更することはできません。

したがって、内部 URL は、会社の秘密キーを使用して復号化できます。外部 URL は、シスコの秘密キーまたは自社の秘密キーを使用して復号化できます。これにより、シスコの秘密キーを持ち、他の会社の秘密キーを持たない Cisco Threat Operations Center では、外部 URL を調査できる一方で、内部 URL は復号化できません。

最後に、WSA の SenderBase 参加レベルによって、暗号化およびレポートされる URL の量が決まります。

- [標準（Standard）]。URL 全体がシスコの公開キーで暗号化されてレポートされます。
- [制限付き（Limited）]。URL の URI 部分が各社の秘密キーで暗号化されて、結果の URL 全体がシスコの公開キーで暗号化されます。

  たとえば、URL https://www.internetdocs.example.com/Doc?docid=a1b2c3d4e5f6g7h8=en に関するテレメトリ レポートの場合は、**Doc?docid=a1b2c3d4e5f6g7h8=en** の部分が各社の秘密キーで暗号化されます。使用する秘密キーに応じて、結果の URL は、次のような文字列になります。

  https://www.internetdocs.example.com/93a68d78c787d8f6sa7d09s1455623

この文字列がシスコの公開キーで暗号化されてレポートされます。この結果、シスコの Threat Operations Center では、URL に含まれているドメイン名のみを復号化できます。

テレメトリ レポートの暗号化

新規テレメトリ レポートを WSA に送信する準備のできたテレメトリ モジュールでは、エンドポイント、ASA、WSA 間に設定されている共有秘密に基づいてレポートを暗号化します。テレメトリ モジュールでは、次に、HTTP POST 要求を WSA に送信することにより、暗号化されたレポートを送信します。WSA では、データを集約し、SenderBase ネットワークへの参加を使用して Threat Operations Center に送信します。この POST 要求が正常に完了した場合、テレメトリ モジュールでは、ローカル レポート リポジトリからレポートを削除します。

テレメトリ クライアント プロファイルの設定

ステップ 1　ASDM を開き、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [設定（Configuration）] > [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）] をクリックしてクライアント プロファイルを作成します。

ステップ 3　クライアント プロファイルの**名前**を指定します。

ステップ 4　[プロファイルの使用（Profile Usage）] フィールドをクリックし、[テレメトリ（Telemetry）] を選択します。

ステップ 5　デフォルトのプロファイルの場所を使用するか、[参照（Browse）] をクリックして代わりのファイルの場所を指定します。

ステップ 6　（任意）[グループ ポリシー（Group Policy）] を選択してクライアント プロファイルを添付するか、クライアント プロファイルを <Unassigned> のままにします。

ステップ 7　[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページで、作成したばかりのテレメトリ プロファイルを選択し、[編集（Edit）] をクリックします。これで、テレメトリ プロファイル エディタ画面で、テレメトリ プロファイルを編集できるようになりました。

ステップ 8　テレメトリをイネーブルにするために、[サービスの有効化（Enable Service）] チェックボックスをオンにします。

ステップ 9　[最大履歴ログ（MB）（Maximum History Log (MB)）] フィールドで、アクティビティ履歴リポジトリの最大サイズを指定します。

- 値の範囲：2 ～ 1,000 MB。
- デフォルト値：100 MB。

ステップ 10　[最大履歴（日数）（Maximum History (Days)）] フィールドで、アクティビティ履歴を保持する最大日数を指定します。

- 値の範囲：1 ～ 1,000（日間）。
- デフォルト値：180 日間。

ステップ 11　[アンチウイルス確認間隔（秒）（Antivirus Check Interval (secs)）] フィールドで、テレメトリ モジュールが新しいアンチウイルス脅威ログ情報を確認するようにポスチャ モジュールに促す間隔を指定します。

- 値の範囲：5 ～ 300 秒。
- デフォルト値：60 秒

ステップ 12　[再送信試行回数（Retry Send Attempts）] フィールドで、最初の試行が失敗した場合に、テレメトリ モジュールで WSA へのテレメトリ レポートの送信を試行する回数を指定します。

- 値の範囲：0 ～ 10

- デフォルト値：2

ステップ 13　[管理者定義除外（Administrator Defined Exceptions）] フィールドで、そのアプリケーションの動作についての情報をテレメトリ レポートから除外する、アプリケーションの実行ファイルを指定します。実行ファイルは、2 通りの方法で追加できます。

- [管理者定義除外（Administrator Defined Exceptions）] テキスト ボックスに、テレメトリ レポートから除外するファイルの名前またはファイルのフル パスを入力し、[追加（Add）] をクリックします。次に、例を示します。

  trusted.exe

  C:\Program Files\trusted.exe

  ファイル名だけを指定した場合は、ファイルのあるディレクトリにかかわらず、そのファイルの動作は追跡され**ません**。フル ディレクトリ パスおよびファイル名を追加した場合は、指定したディレクトリにある場合に、そのファイルの動作は追跡され**ません**。

- [参照（Browse）] ボタンをクリックし、テレメトリ レポートから除外するローカル ファイルを選択します。追加するファイルを参照して選択すると、テレメトリ プロファイル エディタにより、ファイルのフル パスが入力されます。テレメトリ モジュールでは、このテレメトリ プロファイルを使用するすべてのエンドポイント上で、このパスの終端にある、このファイルを探します。このパスおよびファイル名は、管理者だけでなくこのテレメトリ プロファイルのすべてのユーザにとって正しい必要があります。

  いずれの場合も、ファイルは、[管理者定義除外（Administrator Defined Exceptions）] リスト ボックスにリストされます。

ステップ 14　[ファイルからのカスタム証明書の選択（Custom Certificate Select from file）] フィールドで、[参照（Browse）] をクリックして、XML 形式で証明書を含むプロファイルを生成するために、プライバシー エンハンスト メール（**.pem**）タイプの証明書を見つけます。

ステップ 15　[OK] をクリックします。

ステップ 16　[適用（Apply）] をクリックします。

設定プロファイルの階層

テレメトリ動作を制御するクライアント プロファイル リソースは 3 種類あります。これらのファイルは、優先順序に従って作用します。

表 7-1　テレメトリ クライアント プロファイル ファイル

ファイル名	ロケーション	説明および優先順位
actsettings.xml	エンドポイントの %ALLUSERSPROFILE%\Application Data にインストールされます。\Cisco\Cisco AnyConnect Secure Mobility Client \Telemetry	テレメトリ用の基本設定を含むファイル。
telemetry_profile.tsp このファイル名前は、ASA 管理者によって指定されます。	ASA 上に保存されます。このファイルの場所は、次の画面で指定します。 [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）]	テレメトリ クライアント プロファイル ファイル。作成されて、ASA 上に保存されます。 このメッセージに定義されている要素は、いずれも、actsettings.xml ファイル内の要素を上書きします。
WSA によって送信されるテレメトリ プロファイル メッセージ	該当なし これは、ファイルではありません。	WSA 上に XML ファイルはありませんが、ステータス クエリー要求に応答するとき、WSA では、XML 形式のメッセージを送信します。 このメッセージに定義されている要素は、いずれも、*telemetry_profile*.tsp ファイル内の要素を上書きします。

CHAPTER 8

FIPS と追加セキュリティのイネーブル化

Cisco AnyConnect Secure Mobility Client の VPN 機能およびオプションのネットワーク アクセス マネージャとテレメトリ モジュールでは、暗号モジュールを対象とする詳細セキュリティ要件の米国政府規格である連邦情報処理標準（FIPS）140-2 のレベル 1 に対応しています。FIPS 140-2 標準は、暗号ベースのセキュリティ システムを使用してコンピュータおよび遠隔通信システム内の機密情報を保護するすべての政府機関に適用されます。

FIPS 機能は、ASA に対してモデルごとに使用許諾されます。次の AnyConnect クライアント モジュールには、独自の FIPS 設定と要件があります。

- AnyConnect コア VPN クライアント：FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルにある FIPS モード パラメータによってイネーブルにします。このファイルは、セキュリティ設定を含む XML ファイルであり、ASA によって展開されませんが、手動でインストールするか、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展開する必要があります。クライアントの接続先である ASA 用の FIPS ライセンスを購入する必要があります。
- AnyConnect ネットワーク アクセス マネージャ：Windows XP コンピュータのみでサポートされており、AnyConnect クライアント プロファイルでイネーブルにします。ネットワーク アクセス マネージャ用の FIPS サポートのためには、ネットワーク アクセス マネージャと統合された対応ドライバとともに、3e Technologies International から配布される 3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）を展開する必要があります。部品番号 AIR-SSCFIPS-DRV を使用して、FIPS 3eTI CKL 対応ドライバ インストーラをシスコに注文してください（CD で配布）。ドライバおよびサポートされているチップセットについては、AnyConnect ソフトウェア ダウンロード ページにある『*Release Notes for 3eTI Cryptographic Client Software Model 3e-010F-3-IA*』を参照してください。

ここでは、次の項目について説明します。

AnyConnect コア VPN クライアントのための FIPS のイネーブル化

コア AnyConnect セキュリティ モビリティ クライアントの FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルでイネーブルにします。このファイルは、セキュリティ設定を含む XML ファイルであり、ASA によって展開されません。このファイルは、手動でインストールするか、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ユーザ コンピュータに展開する必要があります。クライアントの接続先である ASA 用の FIPS ライセンスを購入する必要があります。

AnyConnect ローカル ポリシーのパラメータは、*AnyConnectLocalPolicy.xml* という名前の XML ファイルにあります。このファイルは ASA では導入されません。エンタープライズ ソフトウェア導入システムを使用してこのファイルを導入するか、ユーザ コンピュータ上でファイルを手動で変更する必要があります。

AnyConnect ローカル ポリシーのその他のパラメータは、リモート アップデートを禁止して中間者攻撃を防いだり、管理者またはルート以外のユーザがクライアント設定を修正できないようにしたりすることによって、セキュリティを高めます。

ASA に設定されている SSL 暗号化タイプのリストで、FIPS 準拠の暗号がリストの先頭に設定されていることも確認する必要があります。それ以外の場合は、DTLS 接続が失敗します。

ここでは、AnyConnect コア VPN クライアント用に FIPS モードおよび追加のセキュリティをイネーブルにする方法を示します。次の項目を取り上げます。

Windows クライアントでの MST ファイルを使用した FIPS のイネーブル化

Windows インストールでは、当社が提供する MST ファイルを標準 MSI インストール ファイルに適用して、AnyConnect ローカル ポリシーで FIPS をイネーブルにできます。MST は FIPS をイネーブルにするだけであり、他のパラメータは変更しません。インストール時に、FIPS がイネーブルにされた AnyConnect ローカル ポリシー ファイルが生成されます。

MST 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。

独自の MST ファイルを使用した FIPS およびその他のローカル ポリシー パラメータのイネーブル化

独自の MST ファイルを作成して、任意のローカル ポリシー パラメータを変更できます。次のパラメータを使用して、独自の MST ファイルを作成してください。名前は、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のパラメータに対応しています。これらのパラメータの説明と設定可能な値については、表 8-9 を参照してください。

- 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 インストーラで新しいポリシー ファイルを作成するには、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。

Enable FIPS Tool を使用した FIPS およびその他パラメータのイネーブル化

すべてのオペレーティング システムで、Enable FIPS ツールを使用して、FIPS をイネーブルにした 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 Mac 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。

表 8-1 に、指定できるポリシー設定と、使用する引数および構文を示します。引数値の動作は、表 8-9 で AnyConnect ローカル ポリシー ファイルのパラメータに指定されている動作と同じです。

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 がイネーブルにされ、vpnagent サービス（Windows）または vpnagent デーモン（Mac および Linux）が再起動されます。
- 複数の引数はスペースで区切ります。

次に、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示します。

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

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

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

表 8-1 に、ポリシー設定と Enable FIPS ツールの引数を示します。

表 8-1　ポリシー設定と Enable FIPS ツールの引数

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 NSS 証明書ストアの除外（Linux および Mac）	efn=[true | false]
PEM ファイル証明書ストアの除外（Linux および Mac）	**epf=[true | false]**
Mac ネイティブ証明書ストアの除外（Mac のみ）	**emn=[true | false]**

ローカル ポリシー内のローカル ポリシー パラメータの手動変更

AnyConnect ローカル ポリシー パラメータを手動で変更するには、次の手順に従ってください。

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 8-2 は、各オペレーティング システムのインストール パスを示しています。

表 8-2　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 7	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client[1]
Linux	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect

1. AnyConnect 3.0 では、Windows Mobile をサポートしていません。このパスは、AnyConnect 2.5 のローカル ポリシー ファイル用です。

ステップ 2　パラメータ設定を編集します。次の例は、Windows の AnyConnect ローカル ポリシー ファイルの内容を示しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
```

```
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

ステップ 3　ファイルを *AnyConnectLocalPolicy.xml* として保存し、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このファイルをリモート コンピュータに展開します。

ASA で FIPS 準拠の SSL 暗号化を使用するための設定

デフォルトでは、ASA に対する AnyConnect の SSL 接続は、データグラム トランスポート層セキュリティ（DTLS）を使用します。これにより、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。ASA に設定されている SSL 暗号化のリストに指定されている暗号が、この接続用に指定される暗号です。

デフォルトでは、ASA 上の SSL 暗号化リストは、次の暗号を次の順序で含みます。

- RC4-SHA1
- AES128-SHA1（FIPS 準拠）
- AES256-SHA1（FIPS 準拠）
- 3DES-SHA1（FIPS 準拠）

したがって、ASA は、デフォルトでは、*FIPS 準拠でない* RC4-SHA1 をこの接続用に指定します。FIPS 準拠にするには、FIPS 準拠の暗号が SSL 暗号化リストの先頭に指定されていることを確認する必要があります。それ以外の場合は、DTLS 接続が失敗します。さらに、接続が失敗しないように、FIPS に準拠しないすべての暗号をリストから削除することをお勧めします。

SSL 暗号化タイプを指定するために、ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [詳細（Advanced）] > [SSL 設定（SSL Settings）] に移動します。[暗号化（Encryption）] エリアで、FIPS 準拠の暗号をリストの先頭に移動します。

CLI を使用している場合は、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用して、リストを順序付けしてください。

AnyConnect FIPS のレジストリ変更によるエンドポイントに関する問題の回避

コア AnyConnect クライアント用に FIPS をイネーブルにすると、エンドポイント デバイスのシステム全体に影響します。AnyConnect は、エンドポイント上の Windows レジストリの設定値を変更します。エンドポイント上の他のコンポーネントでは、AnyConnect が FIPS をイネーブルにしたことを検出でき、同じく暗号化の使用を開始できます。たとえば、リモート デスクトップ プロトコル（RDP）では、サーバで FIPS 準拠の暗号化を使用している必要があるため、Microsoft Terminal Services クライアントの RDP は機能しません。

これらの問題を回避するために、パラメータ [暗号化、ハッシュ、および署名の FIPS 準拠アルゴリズムの使用（Use FIPS compliant algorithms for encryption, hashing, and signing）] を [無効（Disabled）] に変更することにより、[Windows ローカル システム暗号化（Windows Local System Cryptography）] 設定で、FIPS 暗号化を一時的にディセーブルにできます。

エンドポイント デバイスをリブートすると、この設定が変更されてイネーブルに戻ることに注意してください。

表 8-3 に、AnyConnect によって実行される、注意を要する Windows レジストリの変更を示します。

表 8-3　AnyConnect で FIPS をイネーブルにしたときに実行される Windows レジストリ キーの変更

Windows のバージョン	レジストリ キー	行われるアクション
Windows XP 以降	HKLM\System\CurrentControlSet\Control\Lsa	FIPSAlgorithmPolicy が 0 から 1 に変更されます。

Windows のバージョン	レジストリ キー	行われるアクション
Windows Vista 以降	HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy	Enabled が 0 から 1 に変更されます。
	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。
	HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。 これにより、1 つのグループ ポリシーに対する TLSv1 が設定されます。

ソフトウェア ロックおよびプロファイル ロックのイネーブル化

ソフトウェア ロックまたはプロファイル ロックを使用すると、許可した ASA からだけソフトウェアまたはクライアント プロファイルの更新を取得するように、クライアントを制限できます デフォルトでは、ロックはディセーブルです。AnyConnect クライアントは、ソフトウェアまたはクライアント プロファイルの更新を任意の ASA から受信できます。

ソフトウェア ロックがイネーブルの場合、クライアントでは、その ASA が許可サーバのリストにあることを確認してから、コア VPN クライアントおよび任意のオプション クライアント モジュール（ネットワーク アクセス マネージャ、テレメトリ、Web セキュリティなど）を更新します。ASA にロードされているクライアントのバージョンがエンドポイント上のクライアントよりも新しい一方で、その ASA がソフトウェア ロックのサーバのリストにない場合、エンドポイント クライアントは接続できません。クライアント バージョンが同一の場合、エンドポイント クライアントはその ASA に接続できます。

プロファイル ロックがイネーブルの場合、クライアントでは、同じリストを確認してから、VPN などのモジュールのクライアント プロファイルを更新します。その ASA がリストにない場合、クライアントはその ASA に接続しますが、プロファイルは更新しません。この場合は、次の機能を使用できません。

- サービスのディセーブル化
- 証明書ストアの上書き
- 事前接続メッセージの表示
- ローカル LAN へのアクセス
- Start Before Logon
- ローカル プロキシ接続
- PPP 除外
- 自動 VPN ポリシー
- 信頼ネットワーク ポリシー
- 非信頼ネットワーク ポリシー
- 信頼できる DNS ドメイン
- 信頼できる DNS サーバ
- 常時接続
- キャプティブ ポータルの修復
- スクリプト化
- ログオフ時の VPN の保持
- 必要なデバイス ロック
- 自動サーバ選択

AnyConnect のアップグレード

ASA に接続したときに新しい AnyConnect クライアント パッケージが提供されている場合、クライアントでは、まず、ローカル ポリシー ファイル内の*許可サーバ リスト*にあるサーバ名またはグローバル プリファレンス ファイルから取得した*デフォルト ドメイン*と、ASA 名を比較することにより、その

ASA が許可サーバであるかどうかを判別します。ASA が許可サーバである場合、クライアントは、すべてのモジュールをダウンロードしてコア VPN クライアントのアップグレードを起動し、プラグイン ディレクトリを削除して再作成します。これにより、現在インストールされているすべてのオプション モジュールがディセーブルになります。

コア VPN クライアントのアップグレードが終わると、その ASA で指定されているオプション モジュールがアップグレードされます。すでにインストールされている一方で、ASA で指定されていないモジュールは、アップグレードされずにディセーブルのままになります。クライアントでは、VPN プロファイルや、エンドポイント コンピュータでサポートされている他のサービス プロファイルを含む、すべてのプロファイルのダウンロードも行います。

その ASA が許可サーバでない場合、クライアントでは、ソフトウェア ロックおよび VPN プロファイル ロックを確認します。許可されていない場合、ダウンロードされるクライアント プロファイルは VPN プロファイルだけになります。オプション モジュールのプロファイルは、ロックの状態を問わず、ダウンロードされません。

（注） その ASA が許可されていない場合、ネットワーク アクセス マネージャ、テレメトリ、Web セキュリティ プロファイルは、プロファイル ロックを問わず、その ASA にダウンロードされません。

許可されていない ASA への接続

ソフトウェア ロックがオンの場合、クライアントでは、いずれのアップグレードも行わないで切断します。ソフトウェア ロックがオフの場合、クライアントでは、ASA にあるオプション モジュールのリストを無視し、現在システム上にインストールされている全モジュールのリストを *VPNmanifest.dat* ファイルから取得して、そのモジュールだけを ASA からアップグレードします。したがって、この許可されていない ASA で指定されている新規モジュールはいずれもインストールされず、ASA にあるモジュールはいずれもイネーブルにされませんが、現在エンドポイント コンピュータにインストールされているモジュールはディセーブルになりません。

ソフトウェア ロックは、ダウンロード、カスタマイズ、ローカライズ、スクリプト、トランスフォームも制御します。ソフトウェア ロックがオンの場合、これらは、許可されていない ASA からダウンロードされません。したがって、企業外資産に対してスクリプトを介したポリシーの適用が行われていないことを確認する必要があります。

（注） 企業資産および企業外資産の両方が特定の 1 つの ASA に接続し、この ASA でポリシーを適用するためのスクリプトを展開する場合、そのスクリプトは、ソフトウェア ロックがオンの企業外資産では実行されません。これに対処するには、該当する企業外資産のユーザを、ASA 上で別のグループ ポリシーに分離します。

VPN プロファイル ロックがオフの場合、クライアントでは、VPN プロファイルのみを取得して保存します。オンの場合、VPN プロファイルはダウンロードされません。クライアントは、プロファイルなしで接続を続行し、その結果、多くの機能が使用不可になります。

異なるモジュールがイネーブルにされている同一バージョン

許可されている ASA に接続し、モジュールが変更されていることを確認したクライアントは、その ASA で指定されているすべての新規モジュールをダウンロードしてインストールします。コア VPN クライアントが更新されていない場合、プラグイン ディレクトリは削除されません。したがって、インストールされており、ASA に指定されていないモジュールは、イネーブルのままになります。

許可されていない ASA の場合、クライアントでは、いずれの新規モジュールもインストールせず、その ASA で指定されているいずれのモジュールもディセーブルにしません。

コア VPN クライアントのアンインストール

コア VPN クライアントを手動でアンインストールする場合は（Windows の [プログラムの追加または削除（Add or Remove Programs）] を使用）、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にかかわらず、オプションのすべてのクライアント モジュールもアンインストールされます。

デフォルトの許可ドメイン

クライアントが ASA に初めて接続するとき、グローバル プリファレンス ファイルには、デフォルト ドメインの値が設定されていません。値がなく、許可サーバ リストが空の場合は、現在の ASA ドメイン名（ASA 名からホスト名を除去した値）が、デフォルト ドメインとしてグローバル プリファレンス ファイルに追加されます。たとえば、ASA が vpn.newyork.example.com の場合は、以下の行がグローバル プリファレンス ファイルに追加されます。

```
<DefaultDomain>example.com</DefaultDomain>
```

デフォルト ドメインは、ローカル ポリシー ファイルの許可サーバのリストにあるかのように、許可された ASA として扱われます。ローカル ポリシーに定義されている設定の方が、デフォルト ドメインよりも優先されることに注意してください。したがって、ソフトウェア管理システム（または他の何らかの方法）を使用して、許可サーバのリストを含む新しいローカル ポリシー ファイルを展開する場合、デフォルト ドメインは無視されます。

プロファイル ロックがオフのときの許可されていない ASA への接続

常時接続機能がイネーブルにされている許可されていない ASA にクライアントが接続し、ローカル ポリシーで VPN プロファイル ロックがオフの場合は、古いプロファイルが削除されてクライアントはその ASA に再接続できません。したがって、企業資産の検出にホスト スキャンを使用するか、適切なグループ パーティションをイネーブルにしてある場合は、企業外資産およびゲストに対して常時接続機能を強制しないように注意してください。

ロギング

ダウンローダは、ダウンロード履歴を記録する個別のテキスト ログ（UpdateHistory.log）を作成します。このログは、更新時刻、クライアントを更新した ASA、更新されたモジュール、インストールされているバージョン（アップグレードの前および後）を含みます。このログ ファイルは、次の場所に保存されます。

%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs ディレクトリ。

ソフトウェア ロックおよびプロファイル ロックのための XML タグ

次のテキストは、ローカル ポリシー ファイルの一例です。ソフトウェア ロックおよびプロファイル ロックのための XML タグは、UpdatePolicy タグの間に配置されます。これらのタグは、次の例では、太字で示してあります。

許可サーバは、<AuthorizedServerList> タグの間にリストします。サーバは、FQDN または IP アドレスのいずれかを 1 つ含むことができます。ワイルド カードを含むこともできます。例：newyork.example.com、*.example.com、または 1.2.3.*

（注） リモート ユーザによる接続にサーバの IP アドレスを使用するには、必ず、許可サーバ リストに IP アドレスをリストしてください。ユーザが IP アドレスを使用して接続しようとしたときに、サーバが FQDN でリストされている場合、この試行は、許可されていないドメインへの接続として扱われます。

たとえば、サーバ名 *seattle.example.com* および *newyork.example.com* は、許可サーバの FQDN です。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
        <AuthorizedServerList>
            <ServerName>seattle.example.com</ServerName>
            <ServerName>newyork.example.com</ServerName>
        </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

ソフトウェア ロックの使用例

表 8-4、表 8-5、表 8-6、表 8-7 に、同一バージョンおよび異なるバージョンのクライアント パッケージをインストールした、許可されているか許可されていない ASA に接続するクライアントの使用例を示します。

表 8-4　新しい AnyConnect パッケージをインストールした、許可された ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、X、Y がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。	A、B、C が ASA にロードされているバージョンで更新されます。 ASA にロードされているバージョンの D がインストールされます。	A および B が ASA にロードされているバージョンで更新されます。 ASA にロードされているバージョンの X および Y がインストールされます。 C はディセーブルになりますが、インストールされたまま残り、アップグレードされません。	A および B が ASA にロードされているバージョンで更新されます。 C はディセーブルになりますが、インストールされたまま残り、アップグレードされません。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。	A、B、C が更新されます。 C はイネーブルになります。 D がインストールされます。	A および B が更新されます。 X および Y がインストールされます。 C はディセーブルのままとなり、更新されません。	A および B が更新されます。 C はディセーブルのままとなり、更新されません。

表 8-5　新しい AnyConnect パッケージをインストールした、許可されていない ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、X、Y がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオフ。	A、B、および C が ASA にロードされているバージョンで更新されます。 D はダウンロードされません。	A および B が ASA にロードされているバージョンで更新されます。 この ASA で指定されていない場合でも C は更新されます。 X および Y はダウンロードされません。	A および B が ASA にロードされているバージョンで更新されます。 この ASA で指定されていない場合でも C は更新されます。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。 ソフトウェア ロックはオフ。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオン。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。 ソフトウェア ロックはオン。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。

表 8-6　同じバージョンでモジュールの異なる AnyConnect パッケージをインストールした、許可され ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、D がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。	D がダウンロードされインストールされます。 A、B、C、D がインストールされ、イネーブルにされます。	D がダウンロードされインストールされます。 C は、ディセーブルにされません。 A、B、C、D がインストールされ、イネーブルにされます。[1]	モジュールはダウンロードされません。 A、B、および C はイネーブルのままになります。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。	D がダウンロードされインストールされます。 A、B、および D がインストールされイネーブルにされます。 C はディセーブルのままになります。[2]	D がダウンロードされインストールされます。 A、B、および D がインストールされイネーブルにされます。 C はディセーブルのままになります。	モジュールはダウンロードされません。 A、および B はイネーブルのままになります。 C はディセーブルのままになります。

1. C をディセーブルにするには、[Disable Service] をイネーブルにしたクライアント VPN プロファイルを展開する必要があります。
2. C をイネーブルにできるのは、新しい AnyConnect パッケージをロードする場合で、C がイネーブルにされているときだけです。

表 8-7　同じバージョンでモジュールが異なる AnyConnect パッケージをインストールした、許可されていない ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、D がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオフまたはオン。	モジュールはダウンロードされません。 A、B、および C はイネーブルのままになります。	モジュールはダウンロードされず、ディセーブルにもなりません。 A、B、および C はイネーブルのままになります。	モジュールはディセーブルになりません。 A、B、および C はイネーブルのままになります。

ソフトウェアおよびプロファイルのロックの例

次のシナリオ例では、クライアント PC 上および ASA 上の AnyConnect パッケージのバージョンを変えながら、クライアント アップグレード動作について説明します。表 8-8 に、3 台の ASA に対する AnyConnect パッケージのバージョンを示します。

表 8-8　ASA および AnyConnect クライアントの例に関する情報

ASA	ロードされている AnyConnect パッケージ	ダウンロードするモジュール
seattle.example.com	バージョン 3.0.0350	VPN、ネットワーク アクセス マネージャ、Web セキュリティ
newyork.example.com	バージョン 3.0.0351	VPN、ネットワーク アクセス マネージャ
raleigh.example.com	バージョン 3.0.0352	VPN、ポスチャ、テレメトリ

この例を続けます。ローカル ポリシー XML ファイルは、次の内容です。

```
<UpdatePolicy>
    <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
    <AuthorizedServerList>
        <ServerName>seattle.example.com</ServerName>
        <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
</UpdatePolicy>
```

このローカル ポリシーによると、ソフトウェア ロックは*オフ*、VPN プロファイル ロックは*オン*です。

AnyConnect クライアント ユーザは、まず、seattle.example.com に接続します。次に、VPN、ネットワーク アクセス マネージャ、Web セキュリティがインストールされます（バージョン 3.0.0350 によってサポートされているすべてのモジュール）。次に、ユーザは newyork.example.com に接続します。これは、新しいバージョン（バージョン 3.0.0351）を実行している許可された ASA です。ASA はプラグイン ディレクトリを削除し、VPN およびネットワーク アクセス マネージャをバージョン 3.0.0351 にアップグレードします。Web セキュリティはバージョン 3.0.0350 のままとなり、ディセーブルになります。

次に、ユーザは、許可サーバ リストにない raleigh.example.com に接続します。ソフトウェア ロックはオンではないため、VPN およびネットワーク アクセス マネージャは 3.0.0352 にアップグレードされます。ただし、指定されているその他のモジュール（ポスチャおよびテレメトリ）はインストールされません。Web セキュリティはバージョン 3.0.0350 のままとなり、ディセーブルになります。

VPN プロファイル ロックはオンであるため、VPN クライアント プロファイルはダウンロードされません。raleigh-example.com は許可サーバでないため、その他のサービス プロファイルもダウンロードされません。

AnyConnect ローカル ポリシーのパラメータと値

（注）　プロファイル ファイルのポリシー パラメータを省略した場合、機能はデフォルト動作になります。

表 8-9 に、AnyConnect ローカル ポリシー ファイルのパラメータとその値を示します。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値

パラメータおよび説明	値および値の形式
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。指定されているバージョンよりも古いクライアントがファイルを読み取った場合、クライアントはイベント ログ警告を発行します。	形式は acversion="<version number>" です。
xmlns XML 名前空間指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xmlns=http://schemas.xmlsoap.org/encoding/
xsi:schemaLocation スキーマ ロケーションの XML 指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">
xmlns:xsi XML スキーマ インスタンス指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
FipsMode クライアントの FIPS モードをイネーブルにします。クライアントは、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します。	*true*：FIPS モードをイネーブルにします。 *false*：FIPS モードをディセーブルにします（デフォルト）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
BypassDownloader 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ディセーブルにします。	*true*：クライアントは、翻訳、カスタマイズ、オプション モジュール、コア ソフトウェアの更新などのダイナミック コンテンツが ASA 上にあるかどうかをチェックしません。ただし、クライアントでは、クライアントの VPN クライアント プロファイルと、ASA 上のグループ ポリシーと関連付けられているプロファイルの比較を試みます。 *false*：クライアントは、ASA 上にダイナミック コンテンツがあるかどうかをチェックします（デフォルト）。 クライアントが ASA に接続しようとする場合、クライアントと ASA には同じ VPN クライアント プロファイルをインストールしておく必要があります。VPN クライアント プロファイルが同じでない場合、クライアントは選択された ASA AnyConnect 接続プロファイルに割り当てられた VPN クライアント プロファイルをダウンロードしようとします。**BypassDownloader** が **true** に設定されている場合、VPN クライアント プロファイルはダウンロードされません。 VPN クライアント プロファイルがダウンロードされないと、次のいずれかが発生します。 • ASA の VPN クライアント プロファイルがクライアント上のプロファイルと異なっている場合、クライアントは接続を中止します。ASA の VPN クライアント プロファイルにより定義されたポリシーが実施されないためです。 • 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。
RestrictWebLaunch WebLaunch の使用を禁止し、強制的に AnyConnect FIPS 準拠のスタンドアロン接続モードでユーザを接続することで、ユーザが FIPS 準拠でないブラウザを使用して AnyConnect トンネルの開始に使用するセキュリティ クッキーを取得しないようにします。	*true*：WebLaunch の試行は失敗し、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。 *false*：WebLaunch を許可します（デフォルト。AnyConnect 2.3 以前と同じ動作）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
StrictCertificateTrust 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。クライアントでは、これらの証明書を受け入れるようユーザにプロンプトを表示するのではなく、自己署名証明書を使用したセキュリティ ゲートウェイへの接続を失敗します。 **（注）** 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イネーブルにすることを、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イネーブルにすると、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 ユーザにプロンプトが表示されます。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イネーブルにします。	*true*：クライアントから自己署名証明書を使用するセキュリティ ゲートウェイへの接続が失敗し、次のメッセージが表示されます。 `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.` *false*：クライアントは、証明書を受け入れるようにプロンプトを表示します（デフォルト。AnyConnect 2.3 以前と同じ動作）。
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。このパラメータをイネーブルにすると、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。	*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。 *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。 *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。 *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。AnyConnect 2.3 以前と同じ動作）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
RestrictTunnelProtocols（現在はサポート対象外） 特定のトンネル プロトコル ファミリを使用して ASA への接続を確立することを禁止します。	*TLS*：クライアントは IKEv2 および ESP のみを使用してトンネルを確立します。セキュア ゲートウェイへの情報伝達に、TLS/DTLS は使用しません。 *IPSec*：クライアントは、認証およびトンネリングに TLS/DTLS だけを使用します。 *false*：接続の確立で、任意の暗号化プロトコルを使用できます（デフォルト）。 （注）　TLS またはその他のプロトコルの使用を禁止した場合、Secure Desktop の自動アップグレードなど、一部の拡張機能が使用できなくなる場合があります。
ExcludeFirefoxNSSCertStore（Linux および Mac） クライアントが Firefox NSS 証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。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。	true：*Firefox NSS 証明書ストアを除外します。* *false*：Firefox NSS 証明書ストアを許可します（デフォルト）。
ExcludePemFileCertStore（Linux および Mac） クライアントが PEM ファイル証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。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。	*true*：PEM ファイル証明書ストアを除外します。 *false*：PEM ファイル証明書ストアを許可します（デフォルト）。
ExcludeMacNativeCertStore（Mac 専用） 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してサーバ証明書を確認することを、許可または除外します。	*true*：Mac ネイティブ証明書ストアを除外します。 *false*：Mac ネイティブ証明書ストアを許可します（デフォルト）。
ExcludeWinNativeCertStore （Windows 専用。現在はサポート対象外） クライアントが Windows Internet Explorer ネイティブ証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。	*true*：Windows Internet Explorer 証明書ストアを除外します。 *false*：Windows Internet Explorer 証明書ストアを許可します（デフォルト）。
AllowSoftwareUpdateFromAnyServer 任意の ASA からのソフトウェア更新を許可するか、クライアントに制限を加えて、許可した ASA からのみソフトウェアを取得するようにします。	*true*：任意の ASA からの AnyConnect クライアント用ソフトウェア更新を許可します（デフォルト）。 *false*：AuthorizedServerList セクションに指定された ASA からの AnyConnect クライアント用ソフトウェア更新だけを許可します。
AllowVPNPolicyUpdateFromAnyServer 任意の ASA からの VPN ローカル ポリシー ファイルへの更新を許可するか、クライアントに制限を加えて、許可した ASA からのみ更新を取得するようにします。	*true*：任意の ASA からの AnyConnect クライアント用 VPN ローカル ポリシー ファイルの更新を許可します（デフォルト）。 *false*：AuthorizedServerList セクションに指定された ASA からの AnyConnect クライアント用 VPN ローカル ポリシー ファイル更新だけを許可します。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
AuthorizedServerList AnyConnect クライアント ソフトウェアまたは VPN ローカル ポリシー ファイルの更新を許可されたサーバのリスト。	サーバ名は、ServerName を使用してリストします。
ServerName ローカル ポリシー ロックのソフトウェアに対するサーバ名。	AnyConnect クライアントで、ソフトウェアまたは VPN ローカル ポリシー ファイルの更新を受信できるサーバの名前です。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 ファイルの例

次に、AnyConnect ローカル ポリシー ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

ネットワーク アクセス マネージャに対する FIPS のイネーブル化

ネットワーク アクセス マネージャに対する FIPS 準拠は、Windows XP のみでサポートされており、AnyConnect クライアント ネットワーク アクセス マネージャ プロファイルで FIPS モードをイネーブルにする必要と、FIPS ネットワークに接続しているユーザ コンピュータに 3eTI FIPS Certified Crypto Kernel Library（CKL）を展開する必要があります。

ネットワーク アクセス マネージャを FIPS 準拠に設定してあっても、ユーザは FIPS 準拠でないネットワークに接続できます。ただし、ユーザが FIPS 準拠のネットワークに接続する場合、ネットワーク アクセス マネージャは 3eTI FIPS CKL を使用し、AnyConnect GUI の [ネットワーク アクセス マネージャ（Network Access Manager）] ペインに FIPS 準拠のステータスを表示します（レジストリ キー *FIPSAlgorithmPolicy* が非ゼロの場合）。

この章では、ネットワーク アクセス マネージャの FIPS 準拠をイネーブルにする方法を説明します。次の項目を取り上げます。

- 「ネットワーク アクセス マネージャでの FIPS モードの適用」（P.8-19）
- 「AnyConnect GUI を使用した FIPS ステータス レポートのイネーブル化」（P.8-19）
- 「3eTI ドライバのインストール」（P.8-20）
- 「3eTI ドライバ インストーラ ソフトウェアの入手」（P.8-33）

（注）　ネットワーク アクセス マネージャの FIPS 準拠は、Windows XP を実行しているユーザ コンピュータ上でのみサポートされています。

ネットワーク アクセス マネージャでの FIPS モードの適用

AnyConnect プロファイルのネットワーク アクセス マネージャの設定セクションで、許可する関連付け、暗号化モード、認証方式を制限することにより、企業の従業員に対して FIPS 準拠のネットワークのみへの接続を許可できます。

ネットワーク アクセス マネージャの FIPS 準拠では、WPA2 パーソナル（WPA2-PSK）、WPA2 エンタープライズ（802.1X）などの FIPS 認定の AES 暗号化方式をサポートしています。

ネットワーク アクセス マネージャの FIPS サポートには、EAP メソッド EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-FAST が含まれています。

ネットワーク アクセス マネージャを使用すると、FIPS 準拠の WLAN プロファイルと、クライアント VPN セキュリティをイネーブルにした Wi-Fi ホットスポットへのアクセスなど、オプションの非準拠のコンフィギュレーションの両方をサポートできます。管理者は、ネットワークで FIPS がイネーブルにされているかどうかがわかるように、プロファイルに適切な名前を付ける必要があります。

ソリューションを FIPS に完全に準拠させるには、3 つのコンポーネントが必要です。

- ネットワーク アクセス マネージャ
- サポートされている NIC アダプタ ドライバを含む 3eTI FIPS 認定の Crypto Kernel Library（CKL）
- FIPS 準拠のネットワーク プロファイル設定

ネットワーク アクセス マネージャ プロファイル エディタで、FIPS モードをイネーブルにできます。詳細については、「クライアント ポリシーの設定」（P.4-5）を参照してください。

AnyConnect GUI を使用した FIPS ステータス レポートのイネーブル化

AnyConnect GUI の [ネットワーク アクセス マネージャ（Network Access Manager）] ペインには、FIPS ステータス インジケータがあります。FIPS ステータス インジケータをイネーブルにするには、エンドポイント コンピュータ上の次のレジストリ キーに非ゼロの値を設定する必要があります。

HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy

FIPS 統合

確実に FIPS 準拠のソリューションにするには、FIPS 準拠の EAP タイプまたは WPA2 パーソナル（事前共有キー）による AES 暗号化との WPA2 ハンドシェイクのみを許可する、ネットワーク プロファイルをセットアップする必要があります。

ネットワーク アクセス マネージャの Log Packager ユーティリティは、3eTI パケットのログを収集します。

3eTI CKL ドライバ インストーラ

3eTI FIPS 認定の CKL およびサポートされているドライバをインストールする手順については、「3eTI ドライバのインストール」（P.8-20）を参照してください。

3eTI ドライバのインストール

ここでは、完結した FIPS ソリューションを実現するために、ネットワーク アクセス マネージャと統合されたサポートされているドライバとともに、3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）をインストールする手順を説明します。

特記事項

1. 3eTI CKL ドライバ インストーラは、任意の時点で 1 つのシステムに 1 つの 3eTI ワイヤレス ドライバのみをインストールできるように設計されています。異なるタイプのドライバをインストールするには、事前に、それまでのドライバをアンインストールする必要があります。同じタイプのドライバの場合は、今回のインストールで既存のドライバを更新するのみであるため、それまでのドライバをアンインストールする必要はありません。
2. ハードウェアが存在しており、システムに取り付けられている場合、インストーラでは、3eTI CKL をサポートする、3eTI で加工済みのドライバで、対応する OEM ワイヤレス NIC アダプタ ドライバを更新します。

3eTI CKL ドライバ インストーラの概要

3eTI CKL ドライバ インストーラは、次のいずれかの方法で開始できます。

- .exe ファイルのダブルクリック：インストーラを実行する前に NIC アダプタが PC に取り付けられている、通常のドライバ インストールの場合のみ使用可能です。
- コマンドライン オプションを付けないインストーラ コマンドを使用：通常のドライバ インストールの場合のみ使用可能です。
- コマンドライン オプションを付けたインストーラ コマンドを使用：通常のドライバ インストールおよび事前インストール ドライバ インストールで使用可能です。

.exe ファイルをダブルクリックするか、コマンドライン オプションを付けないコマンドの実行を使用してドライバ インストーラを開始した場合、インストーラでは、以下の操作を実行します。

- FIPS 操作のために、サポートされている NIC アダプタ ドライバとともに、3eTI CKL を検出してインストールします。
- 3eTI CKL をサポートしている NIC アダプタが複数検出された場合、インストーラでは、アダプタ選択のプロンプトをユーザに出します。
- 互換性のある NIC アダプタが PC 上に見つからない場合、インストーラはインストールを中止し、次のエラー メッセージを表示します。

  FIPS サポートを実現する NIC チップセットを自動検出できません。プリインストールを強制的に実行するには、コマンド ラインを使ってインストーラを実行する必要があります。操作方法または詳細については、ネットワーク管理者にお問い合わせください。(The installer cannot auto-detect a NIC chipset to provide FIPS support. To enforce a pre-installation, you are required to run the installer using the command line.For instructions or further assistance, please contact your network administrator.)

（注） 事前インストール シナリオは、具体的なインストール オプションを指定できるコマンドライン オプションを使用する場合に最適です。事前インストール方式は、通常は初心者ユーザではなく、ネットワーク管理者が実施します。

インストーラ コマンドおよびコマンドライン オプション

インストーラでは、次のコマンドおよびコマンドライン オプションをサポートしています。

3eTI-drv-installer.exe -s -auto Type= XXXX

-s	ユーザにプロンプトを出さないサイレント インストールを実行する場合に使用します。
-auto	インテリジェント インストールを実行する場合に使用します。インテリジェント インストールでは、インストーラが PC 内のサポートされている NIC アダプタを判別し、適切なドライバをインストールします。これにより、インストーラは、コマンドライン オプションを付けないでコマンドを入力した場合と同じ操作を実行します。
Type=*XXXX*	事前インストールまたは通常インストール用の NIC アダプタ チップセットを指定するために使用します。 *事前インストール*は、指定した NIC アダプタを PC に取り付ける前に、ドライバをインストールすることを意味します。 *通常インストール*は、ドライバをインストールする前に NIC アダプタを取り付けることを意味します。

XXXX の値	**説明**
Intel3945	Intel3945 チップセット用のドライバを指定します。
Centrino	Intel 2100、l2200、2915 チップセット用のドライバを指定します。
Broadcom	インストーラによってサポートされている Broadcom チップセット用のドライバを指定します。
Atheros	Atheros 5001、5004、5005、AR5211、AR5212 チップセット用のドライバを指定します。
Cisco	Atheros チップセットを搭載した Cisco AIR-CB21 カード用のドライバを指定します。

（注） -s を使用してサイレント インストールを実行する場合は、-auto または Type=XXXX か、-auto と Type=XXXX の両方も指定する必要があります。

次に、例を示します。

- *-auto* と *-s* の併用：
  - 取り付けられている NIC アダプタを自動検出して、インテリジェント インストールを実行します
  - ユーザにプロンプトを出さないサイレント インストールを実行します。
  - 複数の NIC アダプタが検出された場合は、サポートされている任意のチップセットを選択します。
- *-auto* と *Type=XXXX* の併用：
  - Type=XXXX で指定された NIC アダプタ チップセット用のドライバのインストールを試行します。
  - 検出された NIC アダプタが指定されたチップセットをサポートしていない場合は、サポートされているチップセットを搭載した任意の NIC アダプタ用のドライバをインストールします。

- *3eTI-drv-installer.exe Type=Intel3945 -auto -s* の使用：
  - ユーザにプロンプトを表示せずに、Intel3945 チップセット用ドライバのインストールを試行します。
  - Intel3945 チップセットを搭載した NIC アダプタが検出されない場合は、サポートされているチップセットを搭載した、他の任意の検出された NIC アダプタ用のドライバをサイレント インストールします。
  - サポートされているチップセットを搭載した NIC アダプタが検出されない場合は、いずれのドライバも事前インストールしません。
- *3eTI-drv-installer.exe Type=Intel3945 -s* を使用：
  - ユーザにプロンプトを表示せずに、Intel3945 チップセット用ドライバのインストールを試行します。
  - サポートされている NIC アダプタ チップセットが検出されない場合は、指定されたチップセット ドライバをインストールすることにより、事前インストールを実行します。

コマンドライン オプションを使用しないインストーラの実行

NIC アダプタを PC に取り付けて通常インストールを実行するには、次の手順を実行します。

ステップ 1　次のいずれかの手順を実行して、インストーラを開始します。

a. Windows エクスプローラを使用して、PC 上の **3eTI-drv-installer.exe** ファイルを見つけ、ファイル名をダブルクリックします。

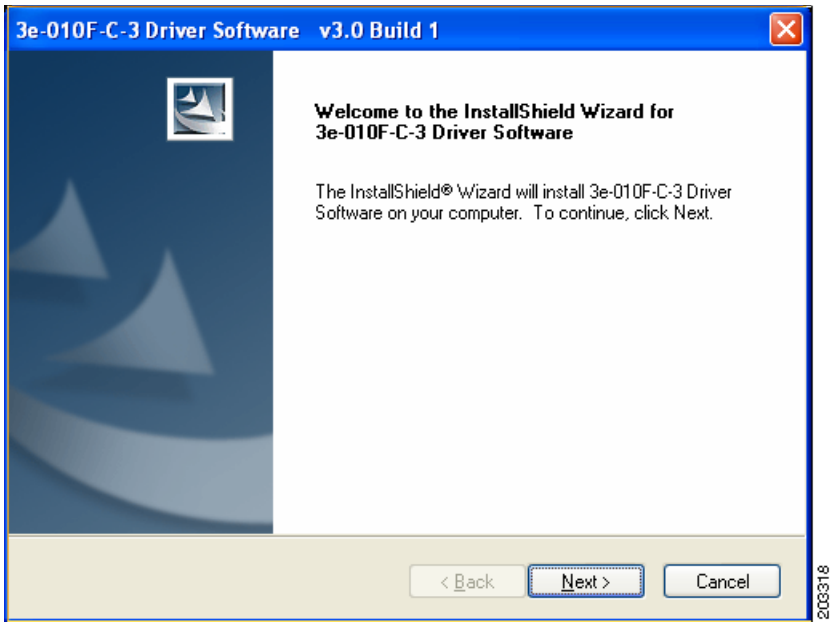
b. [スタート（Start）] > [ファイル名を指定して実行（Run）] をクリックし、次のインストーラ実行コマンドを入力します。

path **/ 3eTI-drv-installer.exe**

ここでの *path* は、インストーラ ファイルのディレクトリ パスです。

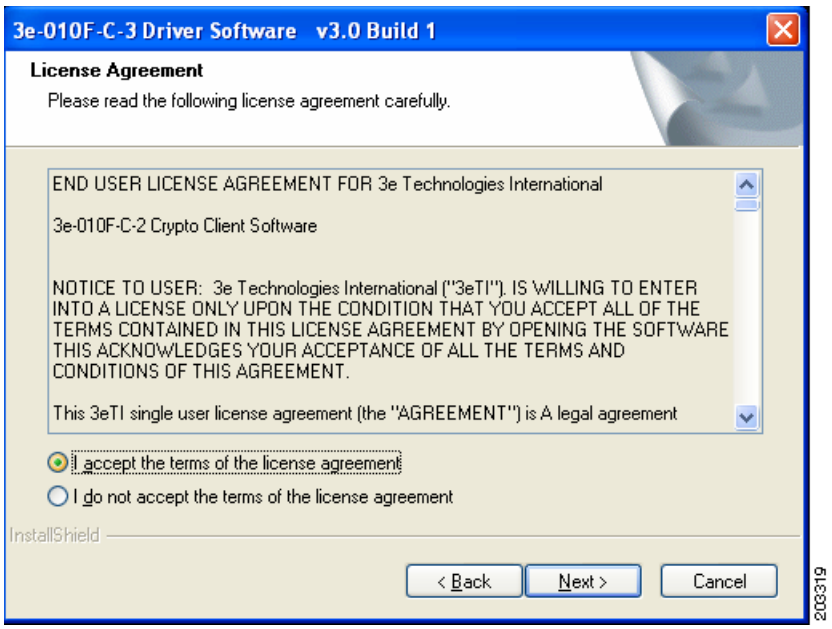
[ドライバへようこそ（Driver Welcome）] ウィンドウが表示されます（図 8-1）。

図 8-1　[ドライバへようこそ（Driver Welcome）] ウィンドウ



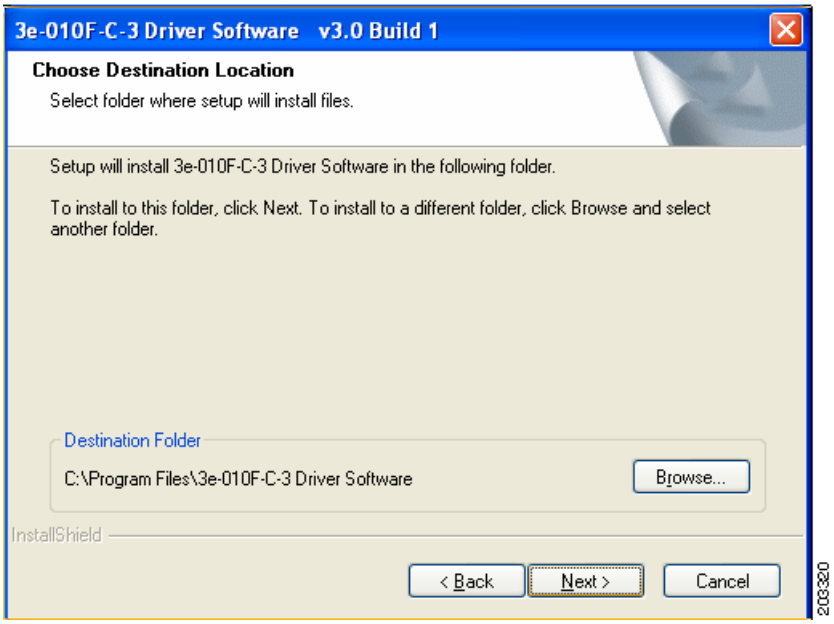
ステップ 2　[次へ（Next）] をクリックすると、ライセンス契約書が表示されます（図 8-2 を参照）。

図 8-2　ライセンス契約書（License Agreement）



ステップ 3　使用許諾契約を読み、同意して、[次へ（Next）] をクリックします。図 8-3 が表示されます。

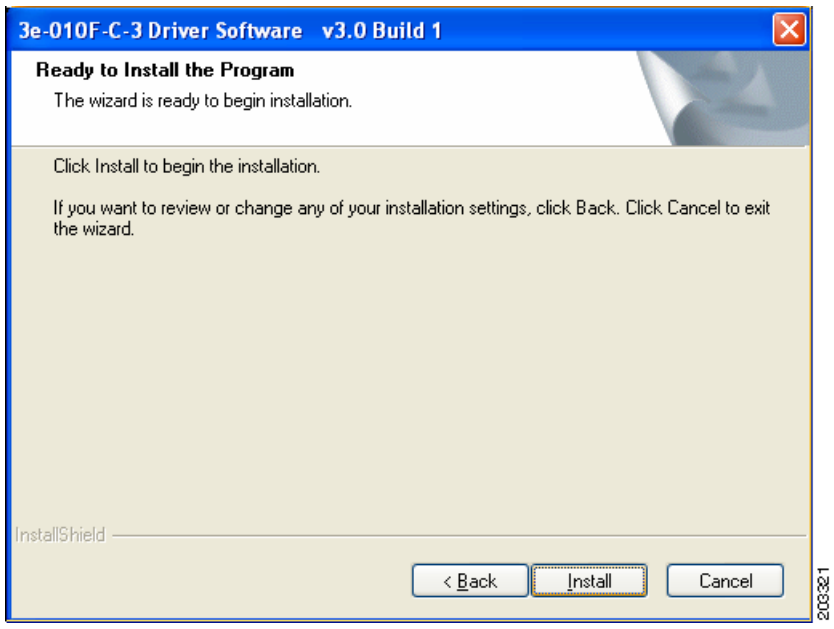
図 8-3　[インストール先の場所（Destination Location）] ウィンドウ



ステップ 4　ドライバ ソフトウェアのデフォルトの宛先フォルダを受け入れるか、[参照（Browse）] をクリックして目的のフォルダを探します。

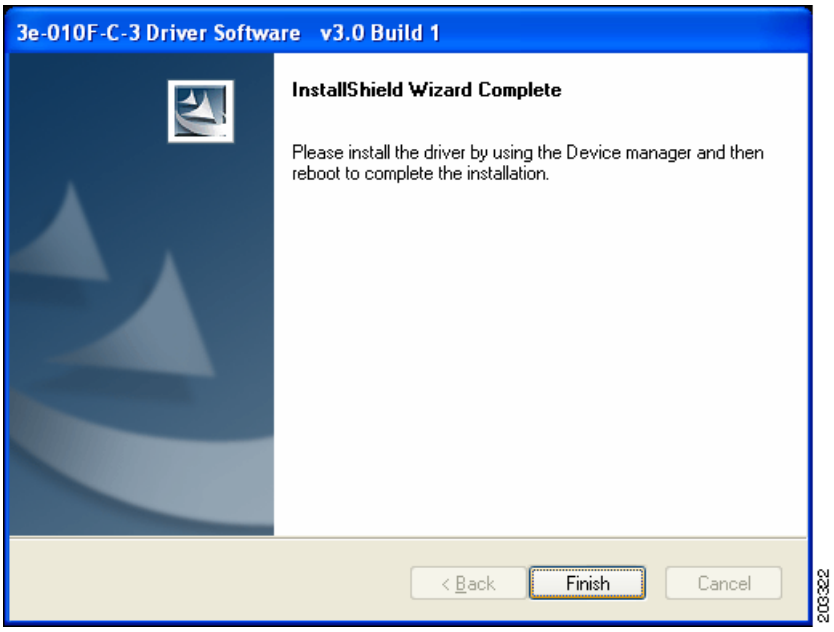
ステップ 5　[次へ（Next）] をクリックすると、図 8-4 が表示されます。

図 8-4　[インストールの準備完了（Ready to Install）] ウィンドウ



ステップ 6　[インストール（Install）] をクリックして、インストール プロセスを開始します。インストールが完了すると、図 8-5 が表示されます。

図 8-5　[ウィザードの完了（Wizard Complete）] ウィンドウ



ステップ 7　[完了（Finish）] をクリックします。

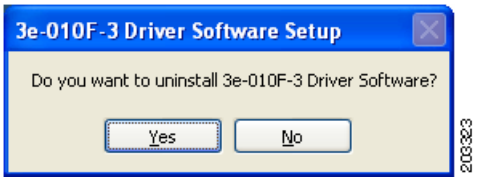
以前の 3eTI ドライバ ソフトウェアのアンインストール

以前の 3eTI ドライバ ソフトウェアをアン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　以前の 3eTI ドライバ ソフトウェアをアンインストールするには、[スタート（Start）] > [設定（Settings）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] をクリックします。

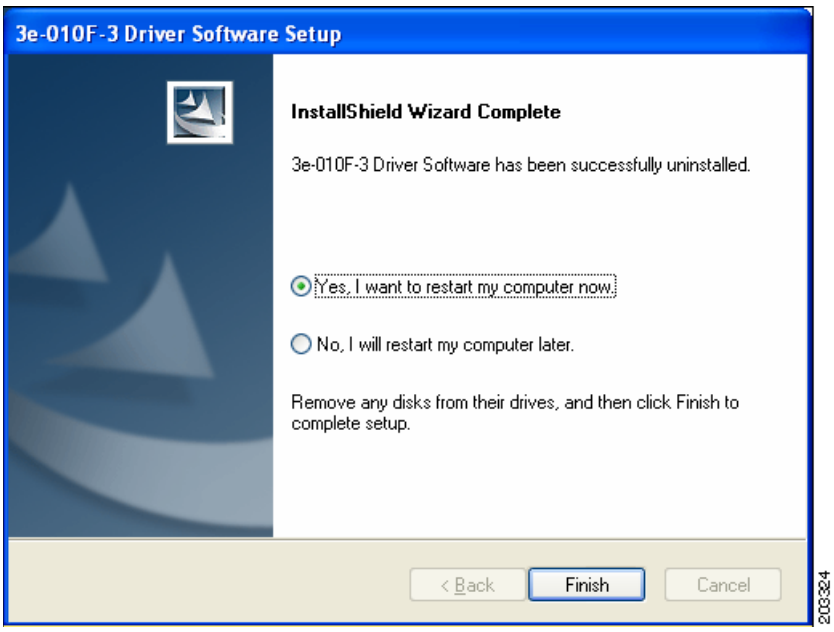
ステップ 2　3e-010F-3 などの 3eTI ドライバ ソフトウェアを選択し、[削除（Remove）] をクリックします。ポップアップ ウィンドウが表示されます（図 8-6 を参照）。

図 8-6　[ドライバー ソフトウェアのアンインストール（Uninstall Driver Software）] ポップアップ



ステップ 3　[Yes] をクリックして、ドライバ ソフトウェアをアンインストールします。図 8-7 が表示されます。

図 8-7　[今すぐコンピューターを再起動する（Restart Computer Now）] ウィンドウ



ステップ 4　コンピュータを再起動するには、[はい（Yes）] をオンにします。

ステップ 5　[完了（Finish）] をクリックします。ドライバ ソフトウェアを完全に削除するために、PC がリブートします。

企業における展開でのドライバのサイレント インストール

サイレント モードを使用してインストーラを実行するには、次の手順を実行します。

ステップ 1　次のコマンドを入力してインストーラを実行します。

path **/ 3eTI-drv-installer.exe -s Type=***XXXX*

説明：

path はインストーラ ファイルへのディレクトリ パスです。

-s は、サイレント インストールを示します。

Type= *XXXX* は、Centrino、Intel3945、Cisco などのチップセットを指定します（「インストーラ コマンドおよびコマンドライン オプション」（P.8-21）を参照）。

ドライバ インストールの進行中を示すポップアップ ステータス ウィンドウが表示され、インストールが完了すると非表示になります。

事前に取り付けたネットワーク アダプタのないドライバのインストール

NIC アダプタを取り付けていない PC に対して 3eTI ドライバ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　[スタート（Start）] > [ファイル名を指定して実行（Run）] をクリックし、次のインストーラ実行コマンドを入力して、インストーラを開始します。

path **/ 3eTI-drv-installer.exe Type =** *XXXX*

説明：

path はインストーラ ファイルへのディレクトリ パスです。

Type= *XXXX* は、Centrino、Intel3945、Cisco などのチップセットを指定します（「インストーラ コマンドおよびコマンドライン オプション」（P.8-21）を参照）。

図 8-1 が表示されます。

ステップ 2　「コマンドライン オプションを使用しないインストーラの実行」(P.8-22) のステップ 2 からステップ 7 を実行します。

ステップ 3　ドライバのインストールが完了したら、NIC アダプタを PC に挿入するか取り付けます。

3eTI ドライバ ソフトウェアの手動アップグレード

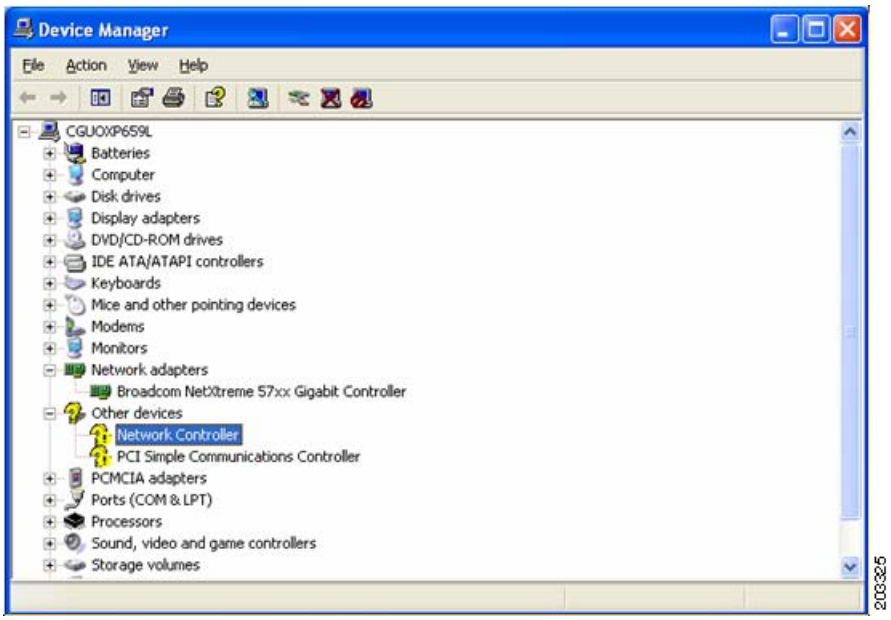
手動アップグレード手順により、ドライバのインストールに関する問題をトラブルシューティングしやすくなります。全社的な展開を構成する手順に組み込むことは想定されていません。

Windows のデバイス マネージャを使用して 3eTI ドライバ ソフトウェアを手動でアップグレードするには、次の手順を実行します。

ステップ 1　デスクトップ上の [マイ コンピューター（My Computer）] アイコンを右クリックし、[プロパティ（Properties）] を選択します。

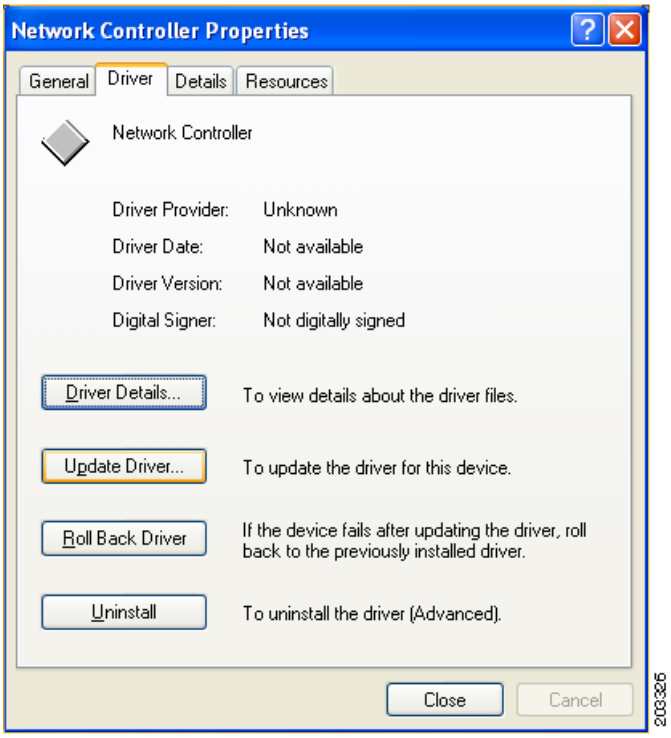
ステップ 2　[システム プロパティ（System Properties）] ウィンドウで [ハードウェア（Hardware）] をクリックし、[デバイス マネージャー（Device Manager）] をクリックします。図 8-8 が表示されます。

図 8-8　Windows の [デバイス マネージャー（Device Manager）] ウィンドウ



ステップ 3　ネットワーク アダプタが取り付けられているか、挿入されており、ドライバ ソフトウェアがインストールされていない場合、デバイスは、[その他のデバイス（Other devices）] の下に黄色の疑問符付きでリストされます。ネットワーク アダプタを右クリックし、[ネットワーク コントローラのプロパティ（Network Controller Properties）] を選択します。[ネットワーク コントローラのプロパティ（Network Controller Properties）] ウィンドウが表示されます（図 8-9 を参照）。

図 8-9　[ネットワーク コントローラのプロパティ（Network Controller Properties）] ウィンドウ

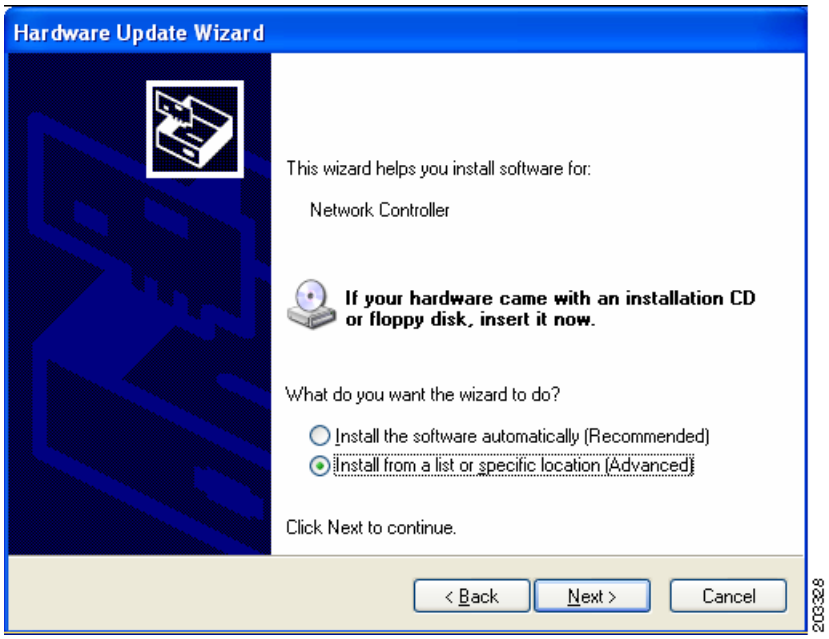


ステップ 4　[ドライバー（Driver）] > [ドライバーの更新（Update Driver）] をクリックします。図 8-10 が表示されます。

図 8-10　Windows の [ハードウェアの更新ウィザード（Hardware Update Wizard）] ウィンドウ

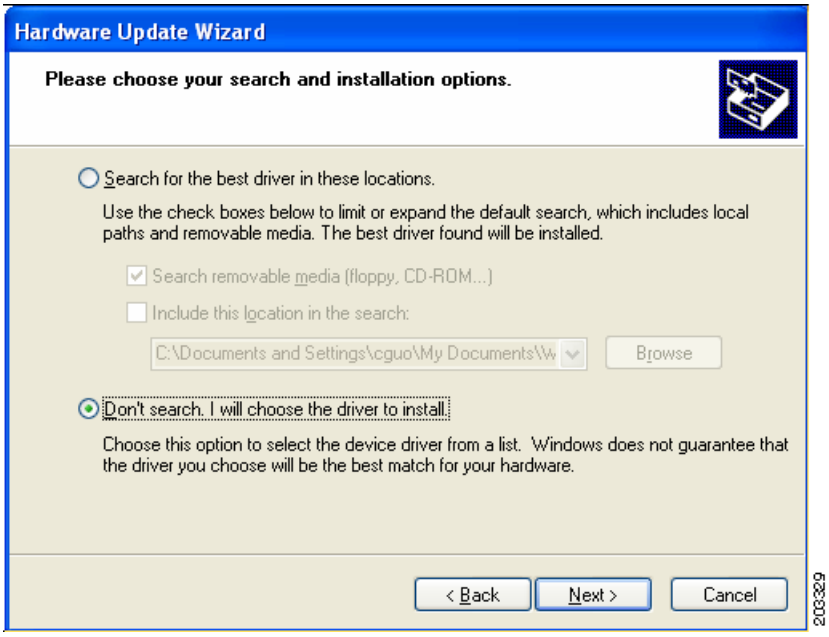
ステップ 5　Windows にドライバ ソフトウェアを検索させないために [いいえ（No）] をオンにし、[次へ（Next）] をクリックします。図 8-11 が表示されます。

図 8-11　[インストール CD またはフロッピー ディスク オプション（Installation CD or Floppy Disk Option）] ウィンドウ



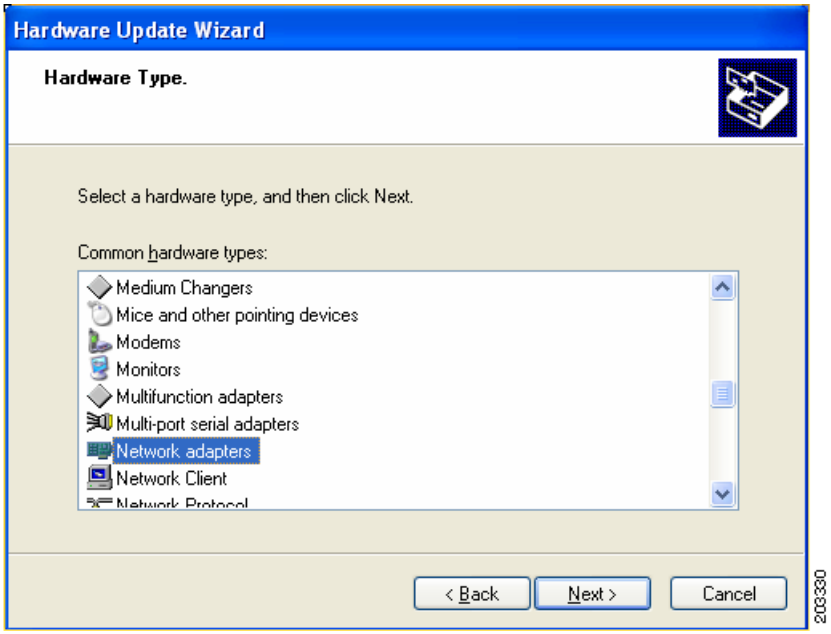
ステップ 6　[一覧または特定の場所からインストールする（詳細）（Install from a list or specific location）] をオンにし、[次へ（Next）] をクリックします。図 8-12 が表示されます。

図 8-12　[検索とインストールのオプション（Search and Installation Options）] ウィンドウ



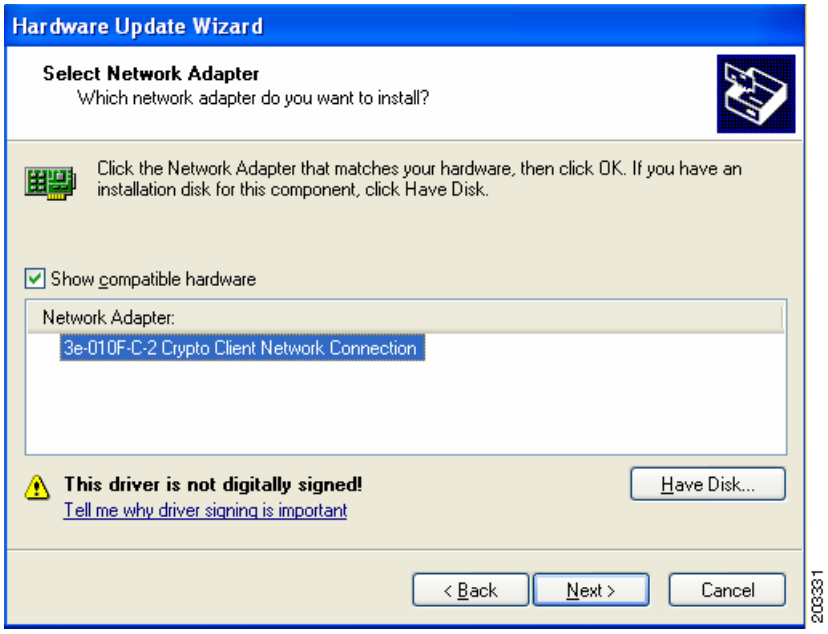
ステップ 7　[検索しないで、インストールするドライバを選択する（Don't search. I will choose the driver to instal）] をオンにし、[次へ（Next）] をクリックします。図 8-13 が表示されます。

図 8-13　Windows の [ハードウェアの種類（Hardware Type）] ウィンドウ



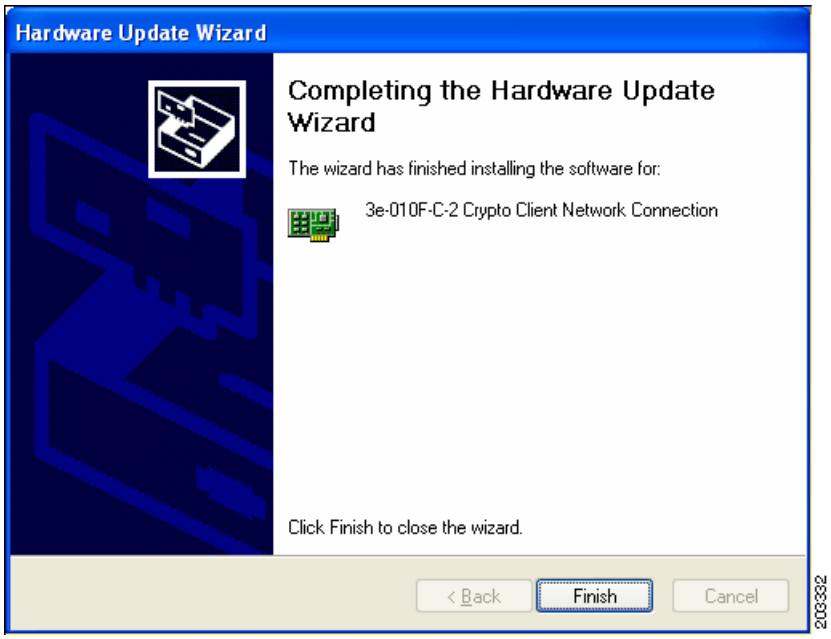
ステップ 8　[ネットワーク アダプター（Network adapter）] を選択し、[次へ（Next）] をクリックします。図 8-14 が表示されます。

図 8-14　[ネットワーク アダプターの選択（Select Network Adapter）] ウィンドウ



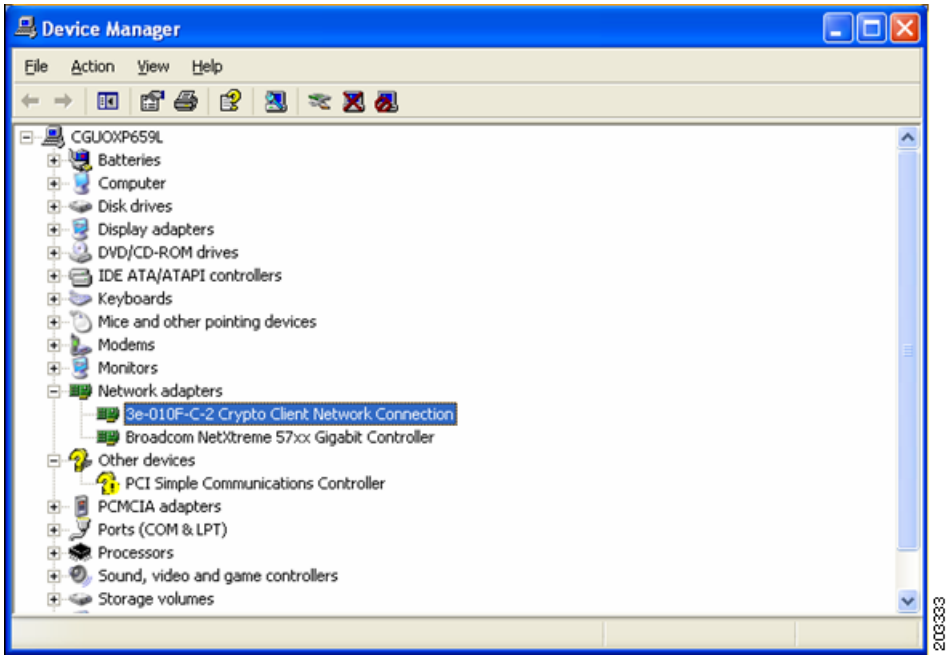
ステップ 9　3eTI ネットワーク接続を選択し、[次へ（Next）] をクリックします。図 8-15 が表示されます。

図 8-15　[インストールの完了（Installation Complete）] ウィンドウ



ステップ 10　ハードウェア ドライバのインストールが完了しました。[完了（Finish）] をクリックします。[デバイス マネージャー（Device Manager）] ウィンドウが再表示されます（図 8-16 を参照）。

図 8-16　更新された、Windows の [デバイス マネージャー（Device Manager）] ウィンドウ



ステップ 11　ドライバが適切にインストールされたことを確認するために、3eTI ネットワーク接続を右クリックし、[プロパティ（Properties）] を選択します。アダプタのプロパティ ウィンドウの [デバイスの状態（Device status）] で、「デバイスは正しく動作しています（This device is working properly）」と示されていることを確認します。

3eTI ドライバ インストーラ ソフトウェアの入手

FIPS 3eTI CKL 対応ドライバ インストーラは、Cisco Software Center からはダウンロードできません。シスコに注文する必要があります。ドライバ インストーラの無期限ライセンスは、製品番号 AIR-SSCFIPS-DRV を使用して、シスコに注文できます。

注文した 3eTI CKL 対応ドライバ インストーラ ソフトウェアは、製品 CD に収録して配布されます。

CHAPTER 9

その他の AnyConnect の管理要件の実現

この章では、次の方法について説明します。

検疫を使用した非準拠クライアントの制限

検疫の使用により、VPN 接続を開始しようとしている特定のクライアントを制限することができます。ASA は制限付き ACL をセッションに適用し、選択されたダイナミック アクセス ポリシーに基づいて制限付きグループを形成します。エンドポイントが管理面で定義されているポリシーに準拠していない場合でも、ユーザは（アンチウイルス アプリケーションのアップデートなど）サービスにアクセスして修復できますが、ユーザに制限がかけられます。修復後、ユーザは再接続できます。この再接続により、新しいポスチャ アセスメントが起動されます。このアセスメントに合格すると、ユーザは制限なしで接続されます。

検疫要件

検疫を行うには、Advanced Endpoint Assessment ライセンスと AnyConnect Premium ライセンスを適応型セキュリティ アプライアンスでアクティブにする必要があります。Advanced Endpoint Assessment は、アンチウイルス、スパイウェア、およびファイアウォールなどのアプリケーションのダイナミック ポリシー要件、また関連付けられている任意のアプリケーション定義ファイル要件に準拠しないエンドポイントを修復します。Advanced Endpoint Assessment は Cisco Secure Desktop のホスト スキャン機能であるため、AnyConnect では、AnyConnect でサポートされるすべての OS での検疫がサポートされます。

ASA リリース 8.3（1）以降では、ユーザに対して最初に検疫が通知されるときに、AnyConnect GUI にユーザ メッセージを表示するダイナミック アクセス ポリシーおよびグループ ポリシーの機能を備えています。その他の検疫メッセージ（「Quarantined - Remediation Required」および「To attempt a normal connection, please reconnect」など）もレポートされますが、これらのメッセージは管理者が定義してユーザに表示することはできません。検疫では ASA をアップグレードする必要はなく、ユーザ メッセージでのみ ASA のアップグレードが必要です。

ASA ソフトウェアをアップグレードする場合、新機能を設定できるようにするため ASDM をリリース 6.3（1）以降にアップグレードすることもお勧めします。

AnyConnect では、AnyConnect でサポートされるすべての OS での検疫がサポートされます。クライアントは、Windows 7、Vista、XP、および Mac OS と Linux で検疫ユーザ メッセージをサポートします。

検疫の設定

検疫を設定するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [ホスト スキャン（Host Scan）] > [Advanced Endpoint Assessment] を選択し、非準拠コンピュータを修復するよう Host Scan を設定します。

ステップ 2　[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）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] を選択して [追加（Add）] をクリックし、非準拠コンピュータを識別するエンドポイント属性を使用する DAP を作成します。[アクション（Action）] タブをクリックし、[検疫（Quarantine）] をクリックします。

ステップ 3　（任意指定）検疫されたセッションのユーザに表示するメッセージを入力します。

ダイナミック アクセス ポリシーの設定の詳細を知りたい場合は、ASDM ヘルプをご覧ください。

Microsoft Active Directory を使用して、ドメイン ユーザの Internet Explorer の信頼済みサイト リストにセキュリティ アプライアンスを追加する方法

Active Directory のドメイン管理者は、グループ ポリシーをドメイン ユーザにプッシュして、Internet Explorer の信頼済みサイトのリストにセキュリティ アプライアンスを追加できます。これは、ユーザが個別に信頼済みサイトのリストにセキュリティ アプライアンスを追加する手順とは異なります。この手順は、ドメイン管理者が管理している Windows マシンの Internet Explorer にのみ適用されます。

セキュリティ アプライアンスでは、フィルタリング テーブルに格納されているデータを使用して、ドメイン名および IP アドレス パス セグメントなどの URL 要求属性が評価され、ローカルで保持されているデータベース レコードと照合されます。一致が見つかった場合、アクセス ポリシー設定によりアクションが決定されて、トラフィックがブロックまたはモニタリングされます。一致が見つからない場合は、プロセスが続行されます。

（注）　Windows Vista または Windows 7 を実行していて、WebLaunch を使用する予定のユーザは、セキュリティ アプライアンスを Internet Explorer の信頼済みサイトのリストに追加する必要があります。

Active Directory を使用して、グループ ポリシーによってセキュリティ アプライアンスを Internet Explorer の信頼済みサイト セキュリティ ゾーンに追加するポリシーを作成するには、次の手順を実行します。

ステップ 1　Domain Admins グループのメンバーとしてログインします。

ステップ 2　[Active Directory ユーザとコンピュータ（Active Directory Users and Computers）] MMC スナップインを開きます。

ステップ 3　グループ ポリシー オブジェクトを作成するドメインまたは組織ユニットを右クリックして、[プロパティ（Properties）] をクリックします。

ステップ 4　[グループ ポリシー（Group Policy）] タブを選択して、[新規（New）] をクリックします。

ステップ 5　新しいグループ ポリシー オブジェクトの名前を入力して、**Enter** を押します。

ステップ 6　一部のユーザまたはグループにこの新しいポリシーが適用されないようにするには、[プロパティ（Properties）] をクリックします。[セキュリティ（Security）] タブを選択します。このポリシーを適用*しない*ユーザまたはグループを追加し、[許可（Allow）] カラムの [読み込み（Read）] チェックボックスと [グループ ポリシーの適用（Apply Group Policy）] チェックボックスをオフにします。[OK] をクリックします。

ステップ 7　[編集（Edit）] をクリックして、[ユーザの構成（User Configuration）] > [Windows の設定（Windows Settings）] > [Internet Explorer メンテナンス（Internet Explorer Maintenance）] > [セキュリティ（Security）] を選択します。

ステップ 8　右側のペインで [セキュリティ ゾーンおよびコンテンツ レーティング（Security Zones and Content Ratings）] を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 9　[現在のセキュリティ ゾーンおよびプライバシー設定をインポートする（Import the current security zones and privacy settings）] を選択します。プロンプトが表示されたら、[続行（Continue）] をクリックします。

ステップ 10　[設定の変更（Modify Settings）] をクリックし、[信頼されたサイト（Trusted Sites）] を選択して、[サイト（Sites）] をクリックします。

ステップ 11　信頼済みサイトのリストに追加するセキュリティ アプライアンスの URL を入力し、[追加（Add）] をクリックします。
フォーマットは、ホスト名（https://vpn.mycompany.com）または IP アドレス（https://192.168.1.100）です。
完全一致（https://vpn.mycompany.com）を使用することも、ワイルドカード（https://*.mycompany.com）を使用することもできます。

ステップ 12　[閉じる（Close）] をクリックし、すべてのダイアログボックスが閉じるまで [OK] をクリックします。

ステップ 13　ドメインまたはフォレスト全体にポリシーが伝搬されるまで待ちます。

ステップ 14　[インターネット オプション（Internet Options）] ウィンドウで [OK] をクリックします。

AnyConnect および Cisco Secure Desktop を CSA と相互運用するための設定方法

リモート ユーザに Cisco Security Agent（CSA）がインストールされている場合は、AnyConnect および Cisco Secure Desktop を ASA と相互運用できるように、CSA ポリシーをリモート ユーザにインポートする必要があります。

これを実行するには、次のステップを実行します。

ステップ 1　AnyConnect および Cisco Secure Desktop の CSA ポリシーを取得します。次の場所からファイルを取得できます。

- ASA に同梱の CD
- ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェア ダウンロード ページ（http://www.cisco.com/cgi-bin/tablebuild.pl/asa）

ファイル名は、AnyConnect-CSA.zip および CSD-for-CSA-updates.zip です。

ステップ 2　.zip パッケージ ファイルから、.export ファイルを展開します。

ステップ 3　インポートする正しいバージョンの .export ファイルを選択します。CSA バージョン 5.2 以降の場合は、バージョン 5.2 のエクスポート ファイルです。CSA バージョン 5.0 および 5.1 の場合は、5.x のエクスポート ファイルです。

ステップ 4　CSA Management Center の [メンテナンス（Maintenance）] > [エクスポート / インポート（Export/Import）] タブを使用して、ファイルをインポートします。

ステップ 5　VPN ポリシーに新しいルール モジュールを追加して、ルールを生成します。

詳細については、CSA のマニュアル『*Using Management Center for Cisco Security Agents 5.2* 』を参照してください。ポリシーのエクスポートに関する情報は、「*Exporting and Importing Configurations*」の項にあります。

AnyConnect およびレガシー VPN クライアントのポート情報

表 9-1 および表 9-2 に、レガシー Cisco VPN クライアントから Cisco AnyConnect Secure Mobility Client にユーザを移行する際に役立つポート情報を示します。

表 9-1　AnyConnect Client により使用されるポート

プロトコル	Cisco AnyConnect Client ポート
TLS（SSL）	TCP 443
SSL リダイレクション	TCP 80（任意）
DTLS	UDP 443（任意、ただし*強く*推奨）
IPsec/IKEv2	UDP 500、UDP 4500

表 9-2　Cisco VPN（IPsec）Client により使用されるポート

プロトコル	Cisco VPN Client（IPsec）ポート
IPsec/NATT	UDP 500、UDP 4500
IPsec/NATT	UDP 500、UDP 4500
IPsec/TCP	TCP（設定可能）
IPsec/UDP	UDP 500、UDP X（設定可能）

サブネット内でのトラフィックのクライアント スプリット トンネリング動作の違い

AnyConnect クライアントおよびレガシー Cisco VPN（IPsec/IKEv1 クライアント）は、ASA によって割り当てられた IP アドレスと同じサブネット内のサイトにトラフィックを渡す場合、動作が異なります。AnyConnect では、クライアントは、設定済みのスプリット トンネリング ポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内に含まれるすべてのサイトにトラフィックを渡します。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。

これとは対照的に、レガシー Cisco VPN クライアントは、クライアントに割り当てられたサブネットに関係なく、スプリット トンネリング ポリシーで指定されたアドレスだけにトラフィックを渡します。

そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

CHAPTER 10

VPN 認証の管理

この章では、Cisco AnyConnect Secure Mobility Client を使用してユーザの VPN 認証を管理する方法について説明します。またこの章では、次のテーマおよびタスクについても説明します。

サーバ証明書の確認（Server Certificate Verification）

次の検証は、受信したサーバ証明書に適用されます。

- FQDN を使用して初期検証に失敗すると、セキュア ゲートウェイの FQDN を使用して実行された AnyConnect クライアントからセキュア ゲートウェイへの SSL および IPSec 接続は、名前検証のために FQDN の解決された IP アドレスでセカンダリ サーバ証明書の確認を行いません。
- AnyConnect クライアントからセキュア ゲートウェイへの SSL および IPSec 接続は、サーバ証明書がデジタル署名とキー暗号化の Key Usage 属性を含める必要があります。
- AnyConnect クライアントからセキュア ゲートウェイへの SSL 接続により、サーバ証明書はサーバ認証の Enhanced Key Usage 属性を含める必要があります。
- AnyConnect クライアントからセキュア ゲートウェイへの IPsec 接続により、サーバ証明書はサーバ認証または IKE 中間の Enhanced Key Usage 属性を含める必要があります。

（注） Key Usage を含まないサーバ証明書は、すべての Key Usage に対して無効と見なされ、同様に、Enhanced Key Usage を含まないサーバ証明書は、すべての Enhanced Key Usage に対して無効と見なされることに注意してください。

- AnyConnect のこのリリースでは、AnyConnect クライアントからセキュア ゲートウェイへの IPsec 接続がサーバ証明書の名前検証を実行します。次の規則は、IPSec および SSL の両方の名前検証を目的として適用されます。

- Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name に対してのみ実行されます。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
- Subject Alternative Name 拡張子がない場合、または、あるけれども関連する属性を含んでいない場合、名前検証は、証明書の Subject で見つかった Common Name 属性に対して実行されます。
- 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。この規則に準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

証明書のみの認証の設定

ユーザ名とパスワードを使用して AAA でユーザを認証するか、デジタル証明書で認証するか（または、その両方を使用するか）を指定する必要があります。証明書のみの認証を設定すると、ユーザはデジタル証明書で接続でき、ユーザ ID とパスワードを入力する必要がなくなります。

証明書のみの認証は、接続プロファイルの中で設定できます。この設定をイネーブルにするには、次の手順に従います。

ステップ 1　[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 接続プロファイル（AnyConnect Connection Profiles）] を選択します。接続プロファイルを選択し、[編集（Edit）] をクリックします。[AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウが開きます。

ステップ 2　選択されていない場合は、ウィンドウの左ペインにあるナビゲーション ツリーの [基本（Basic）] ノードをクリックします。ウィンドウの右ペインにある [認証（Authentication）] エリアで、[証明書（Certificate）] 方式をイネーブルにします。

ステップ 3　[OK] をクリックします。

ステップ 4　（省略可能）各インターフェイスで SSL 認証に使用する証明書があれば、その証明書を指定できます。特定のインターフェイスに対して証明書を指定しない場合、フォールバック証明書が使用されます。

これを実行するには、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。右ペインの [アクセス インターフェイス（Access Interfaces）] エリアで、証明書を指定する対象のインターフェイスを選択して、[デバイス証明書（Device Certificate）] をクリックします。

ステップ 5　[デバイス証明書の指定（Specify Device Certificate）] ダイアログで、[デバイス証明書（Device Certificate）] フィールドをクリックして、選択したインターフェイスへの認証接続に使用する証明書を選択するか、[管理（Manage）] をクリックして、その証明書を追加します。

ステップ 6　[OK] をクリックし、変更を適用します。

（注）

- AnyConnect クライアントが認証証明書を検索する証明書ストアを設定するには、「証明書ストアの設定」（P.3-45）を参照してください。Linux および Mac OS X オペレーティング システムに対する証明書制限の設定についても参照できます。

- セキュア ゲートウェイに対してクライアントを認証するために使用される証明書は有効であり、（CA によって署名された）信頼できるものである必要があります。自己署名されたクライアント証明書は受け入れられません。

AnyConnect のスマート カード サポート

AnyConnect は、次の環境でスマート カードをサポートします。

- Windows XP、7、および Vista 上の Microsoft CAPI 1.0 および CAPI 2.0
- Mac OS X（10.4 以降）でトークンされたキーチェーン

（注）　AnyConnect は、Linux または PKCS #11 デバイスではスマート カードをサポートしていません。

SHA 2 証明書検証エラーの回避

AnyConnect クライアントは、IPsec/IKEv2 VPN 接続の IKEv2 認証フェーズ中に必要とされるデータのハッシングおよび署名を Windows Cryptographic Service Provider（CSP）に依存しています。CSP が SHA 2 アルゴリズムをサポートしていておらず、ASA が疑似乱数関数（PRF）SHA256、SHA384、SHA512 用に設定されていて、接続プロファイル（tunnel-group）が証明書用、または証明書と AAA 認証用に設定されている場合、証明書認証は失敗します。ユーザは「*Certificate Validation Failure*」というメッセージを受け取ります。

このエラーは、SHA 2 タイプのアルゴリズムをサポートしていない CSP に属する証明書を、Windows で使用した場合のみ発生します。その他のサポート対象 OS では、この問題は発生しません。

この問題を回避するには、ASA の IKEv2 ポリシーで、PRF を **md5** または **sha**（SHA 1）に設定します。

または、次の機能がわかっているネイティブ CSP の証明書 CSP 値を変更します。

- Windows XP の場合：Microsoft Enhanced RSA および AES Cryptographic Provider（Prototype）
- Windows 7 および Vista の場合：Microsoft Enhanced RSA および AES Cryptographic Provider

注意　SmartCards 証明書には、この回避策を使用しないでください。CSP 名は絶対に変更してはいけません。代わりに、SmartCard のプロバイダーに問い合わせて、SHA 2 アルゴリズムをサポートする、更新された CSP を入手してください。

注意　次の回避策は、手順を誤って実行した場合、ユーザ証明書を破損するおそれがあります。証明書で変更を指定するときは、十分に注意してください。

Microsoft Certutil.exe ユーティリティを使用して、証明書 CSP 値を変更できます。Certutil は、Windows CA を管理するためのコマンドライン ユーティリティで、Microsoft Windows Server 2003 Administration Tools Pack に同梱されています。Tools Pack は、次の URL からダウンロードできます。

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Certutil.exe を実行して証明書 CSP 値を変更するには、次の作業を実行します。

ステップ 1　エンドポイント コンピュータでコマンド ウィンドウを開きます。

ステップ 2　次のコマンドを使用して、ユーザ ストアに格納されている証明書と、その証明書の現在の CSP 値を表示します。

```
certutil -store -user My
```

次に、このコマンドで表示される証明書の内容の例を示します。

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

ステップ 3　この証明書の <CN> 属性を特定します。この例では、CN は *Carol Smith* です。この情報は次のステップに必要です。

ステップ 4　次のコマンドを使用して、証明書 CSP を変更します。次に、サブジェクト <CN> 値を使用して、変更する証明書を選択する例を示します。その他の属性も使用できます。

Windows Vista および Windows 7 の場合は、次のコマンドを使用します。

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore
-user My <CN> carol smith
```

Windows XP の場合は、次のコマンドを使用します。

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" -f
-repairstore -user My <CN> carol smith
```

ステップ 5　ステップ 2 を繰り返して、表示される証明書の新しい CSP 値を確認します。

SDI トークン（SoftID）の統合

AnyConnect は、Windows 7 x86（32 ビット版）と x64（64 ビット版）、Vista x86 と x64、および XP x86 で動作する RSA SecurID クライアント ソフトウェア バージョン 1.1 以降のサポートを統合します。

RSA SecurID ソフトウェア オーセンティケータは、企業の資産へのセキュアなアクセスのために必要となる管理項目数を減らします。リモート デバイスに常駐する RSA SecurID Software Token は、1 回限定で使用可能なパスコードを 60 秒ごとにランダムに生成します。SDI は Security Dynamics 社製テクノロジーの略称で、ハードウェアとソフトウェアの両方のトークンを使用する、この 1 回限定利用のパスワード生成テクノロジーを意味します。

RSASecureIDIntegration プロファイル設定は、次の 3 つの値のいずれかになります。

- [自動（Automatic）] : クライアントはまずメソッドを 1 つ試行し、それが失敗したら別のメソッドを試行します。デフォルトでは、ユーザ入力がトークン パスコード（HardwareToken）として処理され、これが失敗したら、ユーザ入力がソフトウェア トークン PIN（SoftwareToken）として処理されます。認証が成功すると、成功したメソッドが新しい SDI トークン タイプとして設定され、ユーザ プリファレンス ファイルにキャッシュされます。SDI トークン タイプは、次回の認証試行でいずれのメソッドが最初に試行されるかを定義します。通常、現行の認証試行には、最後に成功した認証試行で使用されたトークンと同じものが使用されます。ただし、ユーザ名またはグループの選択を変更した場合は、入力フィールド ラベルに示されている、デフォルトのメソッドが最初に試行される状態に戻ります。

（注）　SDI トークン タイプは、設定が自動の場合のみ、意味を持ちます。認証モードが自動以外の場合は、SKI トークン タイプのログを無視できます。HardwareToken がデフォルトの場合、次のトークン モードはトリガーされません。

- SoftwareToken : クライアントは、ユーザ入力を常にソフトウェア トークン PIN として解釈し、入力フィールド ラベルは [PIN :（PIN:）] になります。
- HardwareToken : クライアントは、ユーザ入力を常にトークン パスコードとして解釈し、入力フィールド ラベルは [パスコード :（Passcode:）] になります。

（注）　AnyConnect では、RSA Software Token クライアント ソフトウェアにインポートした複数のトークンからの、トークンの選択はサポートされていません。その代わりに、クライアントは RSA SecurID Software Token GUI を介してデフォルト選択のトークンを使用します。

ネイティブ SDI と RADIUS SDI の比較

ネットワーク管理者は、SDI 認証を可能にするセキュア ゲートウェイを次のいずれかのモードで設定することができます。

- *ネイティブ SDI* : SDI サーバと直接通信して SDI 認証を処理できるセキュア ゲートウェイのネイティブ機能です。
- *RADIUS SDI* : RADIUS SDI プロキシを使用して SDI サーバと通信することで SDI 認証を行うセキュア ゲートウェイのプロセスです。

リリース 2.1 以降では、後述の場合を除いて、リモート ユーザからネイティブ SDI と RADIUS SDI を区別できません。SDI メッセージは SDI サーバ上で設定が可能なため、これには、ASA 上のメッセージ テキスト（(P.10-13) を参照）は、SDI サーバ上のメッセージ テキストに一致する必要があります。一致しないと、リモート クライアント ユーザに表示されるプロンプトが、認証中に必要なアクションとして適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS SDI チャレンジは、少数の例外はありますが、基本的にはミラー ネイティブの SDI 交換です。両者とも最終的には SDI サーバと通信するため、クライアントから必要な情報と要求される情報の順序は同じです。明記した場合を除き、ここでは今後、ネイティブ SDI について説明します。

RADIUS SDI 認証を行うリモート ユーザが AnyConnect で ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信し、次にこのサーバは認証について SDI サーバと通信します。

AnyConnect との互換性が保持される ASA 設定の詳細については、「RADIUS/SDI プロキシと AnyConnect との互換性の保持」（P.10-10）を参照してください。

SDI 認証の使用

ログイン（チャレンジ）ダイアログボックスは、ユーザが属するトンネル グループに設定されている認証タイプと一致しています。ログイン ダイアログボックスの入力フィールドには、どのような種類の入力が認証に必要か明確に示されます。

通常、ユーザはツール トレイの [AnyConnect] アイコンをクリックし、接続する接続プロファイルを選択してから、認証ダイアログボックスに適切なクレデンシャルを入力することで AnyConnect に接続します。ユーザ名 / パスワードによる認証を行うユーザには、図 10-1 のようなダイアログボックスが表示されます。

図 10-1　ユーザ名 / パスワードを入力する認証用ログイン ダイアログボックス

SDI 認証では、リモート ユーザは AnyConnect ソフトウェア インターフェイスに個人識別番号（PIN）を入力して RSA SecurID パスコードを受け取ります。セキュアなアプリケーションにパスコードを入力すると、RSA Authentication Manager がこのパスコードを確認してユーザにアクセスを許可します。

RSA SecurID ハードウェアまたはソフトウェアのトークンを使用するユーザには、パスコードまたは PIN、PIN、パスコードのいずれかを入力する入力フィールドが表示されます。ダイアログボックス下部のステータス行には、さらにこの点に関連する情報が表示されます。ユーザは、ソフトウェア トークンの PIN またはパスコードを AnyConnect ユーザ インターフェイスに直接入力します。図 10-2、図 10-3、および図 10-4 を参照してください。

図 10-2　パスコードまたは PIN ダイアログボックス

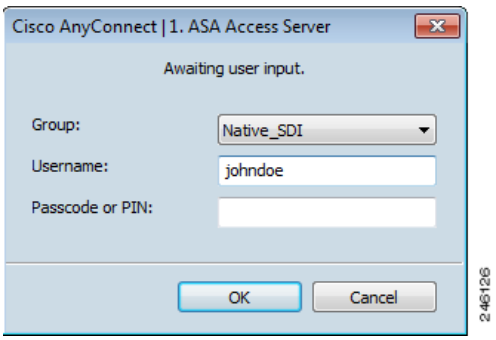


図 10-3　PIN ダイアログボックス

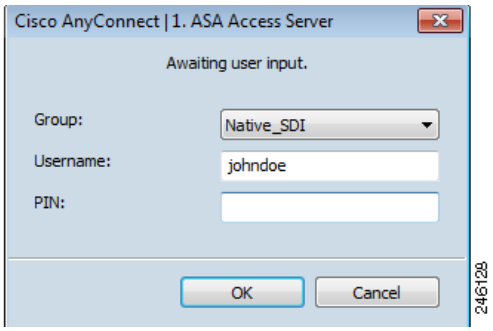
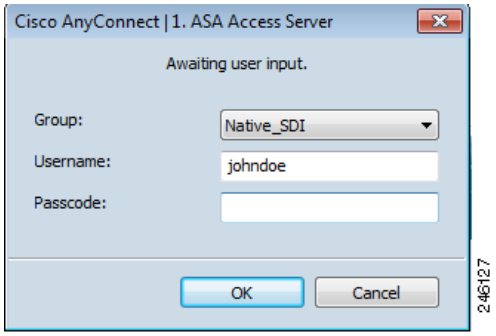


図 10-4　パスコード ダイアログボックス



最初に表示されるログイン ダイアログボックスの外観は、セキュア ゲートウェイの設定によって異なります。セキュア ゲートウェイには、メインのログイン ページ、メインのインデックス URL、トンネル グループのログイン ページ、またはトンネル グループの URL（URL/ トンネル グループ）からアクセスできます。メインのログイン ページからセキュア ゲートウェイにアクセスするには、[ネットワーク（クライアント）アクセス（Network (Client) Access）] の [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] ページで [ユーザに接続の選択を許可する（Allow user to select connection）] チェックボックスをオンにする必要があります。いずれの方法でも、ゲートウェイはクライアントにログイン ページを送信します。メインのログイン ページにはドロップダウン リストがあり、ここからトンネル グループを選択します。トンネルグループ ログイン ページにはこの表示はありません。トンネルグループは URL で指定されるためです。

（接続プロファイルまたはトンネル グループのドロップダウン リストが表示される）メインのログイン ページの場合、デフォルト トンネル グループの認証タイプによって、パスワードの入力フィールド ラベルの初期設定が決まります。たとえば、デフォルト トンネル グループが SDI 認証を使用する場合、フィールド ラベルは [パスコード（Passcode）] になりますが、デフォルト トンネル グループが NTLM 認証を使用する場合は、フィールド ラベルは [パスワード（Password）] になります。リリース 2.1 以降では、異なるトンネル グループをユーザが選択しても、フィールド ラベルが動的に更新されることはありません。トンネルグループのログイン ページでは、フィールド ラベルはトンネル グループの要件に一致します。

クライアントは、パスワード入力フィールドへの RSA SecurID Software Token の PIN の入力をサポートします。RSA SecurID Software Token ソフトウェアがインストールされており、トンネルグループ認証タイプが SDI の場合、フィールド ラベルは [パスコード（Passcode）] となり、ステータス バーに

は、「Enter a username and passcode or software token PIN」と表示されます。PIN を使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [PIN] のフィールドが表示されます。クライアントは、入力された PIN を使用して RSA SecurID Software Token DLL からパスコードを取得します。認証が成功するたびにクライアントはトンネル グループ、ユーザ名、認証タイプを保存し、保存されたトンネル グループが新たにデフォルトのトンネル グループとなります。

AnyConnect では、すべての SDI 認証でパスコードを使用できます。パスワード入力ラベルが [PIN] の場合でも、ユーザはステータス バーの指示どおりにパスコードを入力することができます。クライアントは、セキュア ゲートウェイにパスコードをそのまま送信します。パスコードを使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [パスコード（Passcode）] のフィールドが表示されます。

SDI 認証交換のカテゴリ

すべての SDI 認証交換は次のいずれかのカテゴリに分類されます。

- 通常の SDI 認証ログイン
- 通常ログイン チャレンジ
- 新規ユーザ モード
- 新規 PIN モード
- PIN クリア モード
- 次のトークン コード モード

通常の SDI 認証ログイン

通常ログイン チャレンジは、常に最初のチャレンジです。SDI 認証ユーザは、ユーザ名およびトークン パスコード（ソフトウェア トークンの場合は PIN）を、ユーザ名とパスコードまたは PIN フィールドにそれぞれ指定する必要があります。クライアントはユーザの入力に応じてセキュア ゲートウェイ（中央サイトのデバイス）に情報を返し、セキュア ゲートウェイはこの認証を認証サーバ（SDI または RADIUS プロキシ経由の SDI）で確認します。

認証サーバが認証要求を受け入れた場合、セキュア ゲートウェイは認証が成功したページをクライアントに送信します。これで認証交換が完了します。

パスコードが拒否された場合は認証は失敗し、セキュア ゲートウェイは、エラー メッセージとともに新しいログイン チャレンジ ページを送信します。SDI サーバでパスコード失敗しきい値に達した場合、SDI サーバはトークンを次のトークン コード モードに配置します。「「Next Passcode」および「Next Token Code」チャレンジ」（P.10-10）を参照してください。

新規ユーザ モード、PIN クリア モード、および新規 PIN モード

PIN のクリアは、ネットワーク管理者だけの権限で、SDI サーバでのみ実行できます。

新規ユーザ モード、PIN クリア モード、新規 PIN モードでは、AnyConnect は、後の「next passcode」ログイン チャレンジで使用するために、ユーザ作成 PIN またはシステムが割り当てた PIN をキャッシュに入れます。

PIN クリア モードと新規ユーザ モードは、リモート ユーザから見ると違いがなく、また、セキュア ゲートウェイでの処理も同じです。いずれの場合も、リモート ユーザは新しい PIN を入力するか、SDI サーバから割り当てられる新しい PIN を受け入れる必要があります。唯一の相違点は、最初のチャレンジでのユーザの応答です。

新規 PIN モードでは、通常のチャレンジと同様に、既存の PIN を使用してパスコードが生成されます。PIN クリア モードでは、ユーザがトークン コードだけを入力するハードウェア トークンとして PIN が使用されることはありません。RSA ソフトウェア トークンのパスコードを生成するためにゼロが 8 つ並ぶ PIN（00000000）が使用されます。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新規ユーザを SDI サーバに追加すると、既存ユーザの PIN をクリアする場合と同じ結果になります。いずれの場合も、ユーザは新しい PIN を指定するか、SDI サーバから割り当てられる新しい PIN を受け入れる必要があります。これらのモードでは、ユーザはハードウェア トークンとして、RSA デバイスのトークン コードのみ入力します。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新しい PIN の入手

現行の PIN がない場合、システム設定に応じて、SDI サーバは次の条件のいずれかを満たす必要があります。

- ユーザは、PIN を作成するか、システムの割り当てを受け入れるかを選択できる。
- ユーザは新規 PIN を作成する必要がある。
- システムがユーザに新規 PIN を割り当てる必要がある。

デフォルトでは、PIN はシステムによって割り当てられます。

PIN をリモート ユーザ自身で作成する方法とシステムで割り当てる方法を選択できるように SDI サーバを設定している場合、ログイン画面にはオプションを示すドロップダウン リストが表示されます。ステータス行にプロンプト メッセージが表示されます。いずれの場合も、ユーザは今後のログイン認証のためにこの新規 PIN を忘れないようにする必要があります。

新規 PIN の作成

ユーザが新しく PIN を作成するように選択して [続行（Continue）]（図 10-5）をクリックすると、AnyConnect にこの PIN を入力するためのダイアログボックス（図 10-6）が表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。

図 10-5　ユーザが PIN の作成を選択

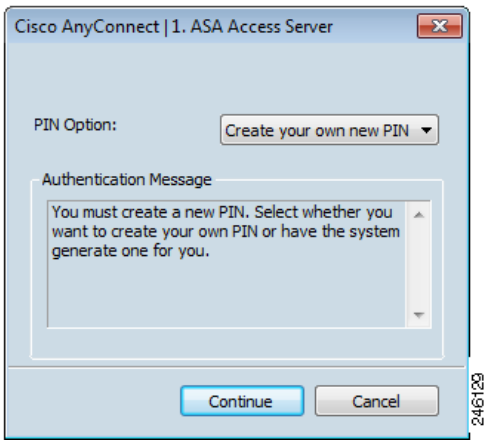
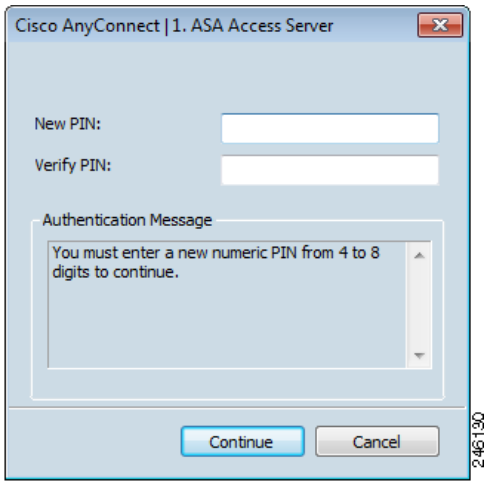


図 10-6　新規 PIN の作成



ユーザが PIN を作成する場合、新規 PIN を入力および確認したら、[続行（Continue）] をクリックします。PIN は一種のパスワードであるため、ユーザがこの入力フィールドに入力する内容はアスタリスクで表示されます。RADIUS プロキシを使用する場合、PIN の確認は、最初のダイアログボックスの次に表示される、別のチャレンジで行われます。クライアントは新しい PIN をセキュア ゲートウェイに送信し、セキュア ゲートウェイは「next passcode」チャレンジに進みます。

システムが割り当てる PIN の場合、ユーザがログイン ページで入力したパスコードを SDI サーバが受け入れると、セキュア ゲートウェイはシステムが割り当てた PIN をクライアントに送信します。ユーザは [続行（Continue）] をクリックする必要があります。クライアントは、ユーザが新規 PIN を確認したことを示す応答をセキュア ゲートウェイに返し、システムは「next passcode」チャレンジに進みます。

いずれの場合も、ユーザは次回のログイン認証のために PIN を忘れないようにする必要があります。

「Next Passcode」および「Next Token Code」チャレンジ

「next passcode」チャレンジでは、クライアントが新規 PIN の作成または割り当て時にキャッシュに入れられた PIN 値を使用して RSA SecurID Software Token DLL から次のパスコードを取得し、ユーザにプロンプト表示せずにこれをセキュア ゲートウェイに返します。同様に、ソフトウェア トークン用の「next Token Code」チャレンジでは、クライアントは RSA SecurID Software Token DLL から次のトークン コードを取得します。

RADIUS/SDI プロキシと AnyConnect との互換性の保持

ここでは、AnyConnect が、RSA SecureID ソフトウェア トークンを使用して、1 台以上の SDI サーバのプロキシ サーバである RADIUS サーバ経由でクライアントに配布されたユーザ プロンプトに適切に応答する手順について説明します。ここでは、次の項目について説明します。

- AnyConnect と RADIUS/SDI サーバのインタラクション
- RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

AnyConnect と RADIUS/SDI サーバのインタラクション

リモート ユーザが AnyConnect で ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバと通信を行い、次に、このサーバが認証について SDI サーバと通信を行います。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージ テキストは、ASA が SDI サーバと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、AnyConnect にネイティブ SDI サーバとして認識させるために、ASA は RADIUS サーバからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージ テキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトは、認証中に必要とされるアクションに対して適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

次の項では、SDI 固有の RADIUS 応答メッセージを解釈し、AnyConnect ユーザに適切なアクションを求めるプロンプトを表示するように ASA を設定する手順について説明します。

RADIUS 応答メッセージを転送するための接続プロファイル（トンネル グループ）を、SDI サーバとの直接通信をシミュレートする方法で設定します。SDI サーバに認証されるユーザは、この接続プロファイルを介して接続する必要があります。

ステップ 1　[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 接続プロファイル（AnyConnect Connection Profiles）] を選択します。

ステップ 2　SDI 固有の RADIUS 応答メッセージを解釈するために設定する接続プロファイルを選択して、[編集（Edit）] をクリックします。

ステップ 3　[EAnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウで、左側のナビゲーション ペインにある [詳細（Advanced）] ノードを展開して、[グループ エイリアス / グループ URL（Group Alias/Group URL）] を選択します。

ステップ 4　[ログイン画面への SecurID メッセージの表示を有効にする（Enable the display of SecurID messages on the login screen）] にチェックマークを付けます。

ステップ 5　[OK] をクリックします。

ステップ 6　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [AAA/ ローカル ユーザ（AAA/Local Users）] > [AAA サーバ グループ（AAA Server Groups）] を選択します。

ステップ 7　[追加（Add）] をクリックして、AAA サーバ グループを追加します。

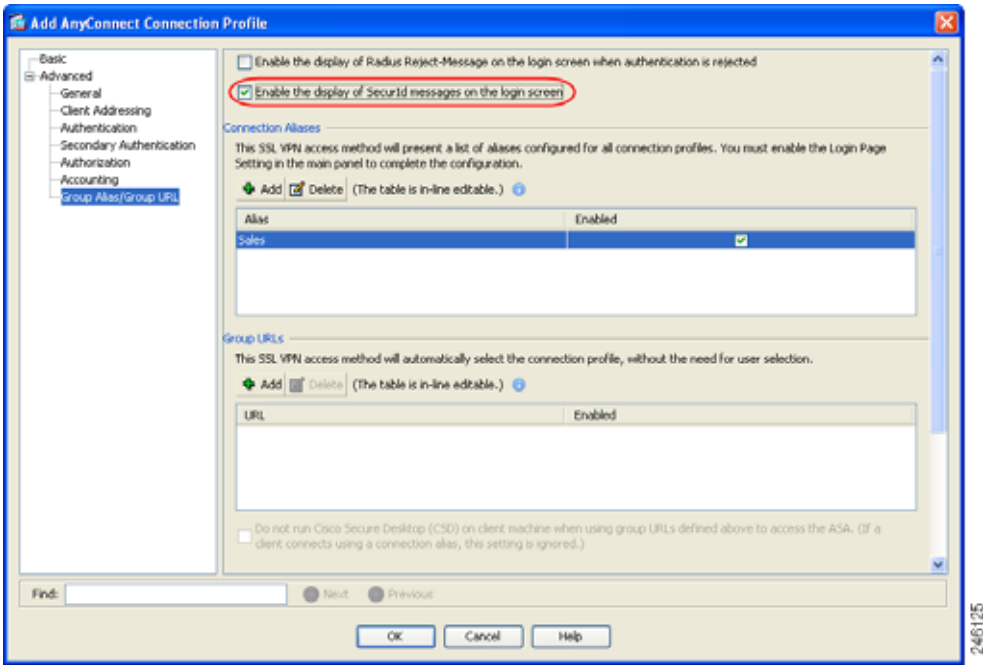
ステップ 8　[AAA サーバ グループの編集（Edit AAA Server Group）] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9　[AAA サーバ グループ（AAA Server Groups）] 領域で作成した AAA サーバ グループを選択し、[選択したグループ内のサーバ（Servers in the Selected Group）] 領域で [追加（Add）] をクリックします。

ステップ 10　[SDI メッセージ（SDI Messages）] 領域で [メッセージ テーブル（Message Table）] 領域を展開します。メッセージ テキスト フィールドをダブルクリックするとメッセージを編集できます。RADIUS サーバから送信されたメッセージとテキストの一部または全体が一致するように、RADIUS 応答メッセージ テキストを ASA で設定します。

ステップ 11　[OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

図 10-7　[AnyConnect 接続プロファイルの追加/編集（Add/Edit AnyConnect Connection Profile）] 画面



が使用するデフォルトのメッセージ テキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージ テキストです。ASACisco Secure ACS を使用していて、デフォルトのメッセージ テキストを使用している場合、ASA でメッセージ テキストを設定する必要はありません。これ以外の場合は、メッセージ テキストが一致するようにメッセージを設定します。

表 10-1 は、メッセージ コード、デフォルトの RADIUS 応答メッセージ テキスト、および各メッセージの機能を示しています。セキュリティ アプライアンスは、表での出現順に文字列を検索するため、メッセージ テキスト用に使用する文字列が別の文字列のサブセットでないことを確認する必要があります。

たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージ テキストのサブセットだとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを一致させます。

表 10-1　SDI 操作コード、デフォルト メッセージ テキスト、およびメッセージ機能

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。

CHAPTER 11

AnyConnect クライアントとインストーラのカスタマイズとローカライズ

Cisco AnyConnect Secure Mobility Client をカスタマイズして、Windows、Linux、および Mac OS X コンピュータ上で稼働するクライアントを含むリモート ユーザに、自社企業のイメージを表示することができます。

クライアントおよびすべてのオプション モジュールは、別の言語にローカライズ（翻訳）できます。また、コア VPN クライアントのインストーラ プログラムもローカライズできます。

この章の次の各項では、カスタマイズおよびローカライズの手順について説明します。

AnyConnect クライアントのカスタマイズ

AnyConnect をカスタマイズして、Windows、Linux、および Mac OS X コンピュータ上で稼働するクライアントを含むリモート ユーザに、自社企業のイメージを表示することができます。

クライアントをカスタマイズするには、次の 3 つ方法のいずれかを使用します。

- 企業ロゴおよびアイコンなど個別のクライアント GUI コンポーネントを ASA にインポートし、インストーラからリモート コンピュータに展開することによって、クライアントのブランドを変更する。
- 独自の GUI または CLI を提供し、AnyConnect API を使用する、独自のプログラムをインポートする（Windows および Linux のみ）。

（注） ネットワーク アクセス マネージャおよび Web セキュリティでは、AnyConnect API はサポートされていません。Web セキュリティまたはネットワーク アクセス マネージャを展開する場合は、コア AnyConnect クライアントを展開する必要があります。

- 多数のブランド変更のために作成したトランスフォームをインポートする（Windows のみ）。インストーラを使用して ASA から展開されます。

これらの方法の手順について、次の項で説明します。

AnyConnect 3.0 以降の推奨イメージ形式

次の理由から、AnyConnect 3.0 以降には、最大サイズが 62 x 33 ピクセルのポータブル ネットワーク グラフィック（PNG）イメージの使用を推奨します。

- PNG イメージは、その他のイメージ形式よりもファイル サイズが小さいため、使用するディスク領域が少なくて済みます。
- PNG では、デフォルトでトランスペアレントがサポートされています。
- AnyConnect 3.0 以降の GUI では、[詳細（Advanced）] ウィンドウおよびトレイ フライアウトにタイトルがロゴ イメージに隣接して表示されます。そのため、これよりも前のクライアントでイメージを使用して指定したタイトルは、ユーザを混乱させる可能性があります。

個別の GUI コンポーネントとカスタム コンポーネントの置き換え

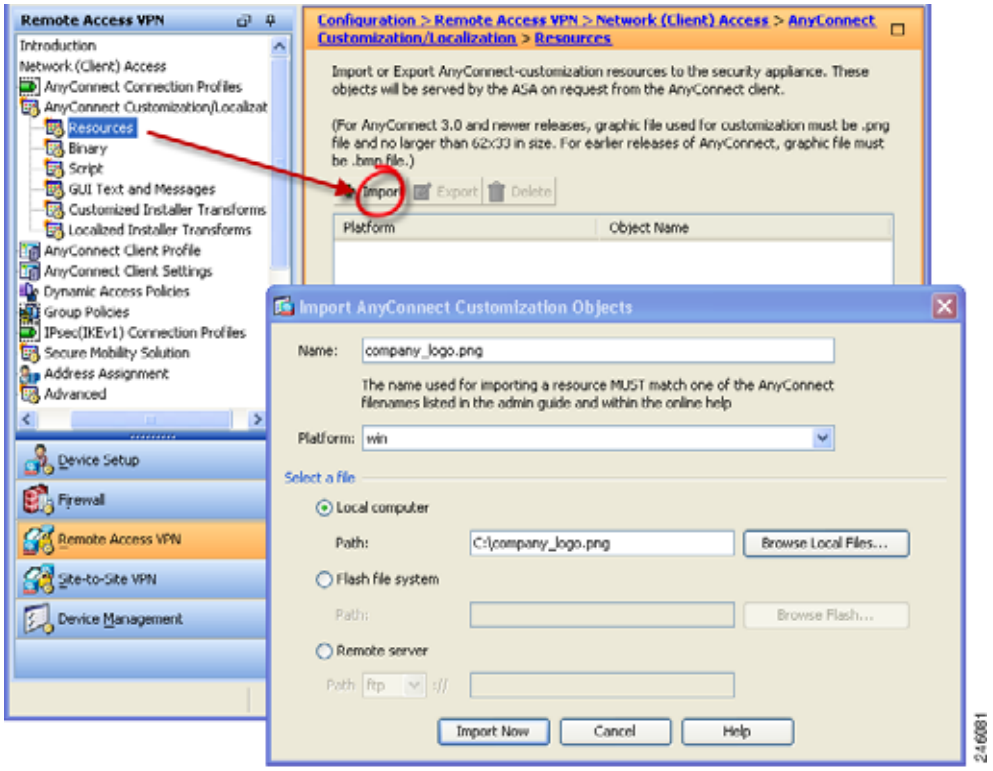
独自のカスタム ファイルをセキュリティ アプライアンスにインポートし、その新しいファイルをクライアントに展開することによって、AnyConnect をカスタマイズすることができます。表 11-2、表 11-3、および表 11-4 に、オリジナルの GUI アイコンのサンプル イメージとそのサイズを示します。

カスタム ファイルをインポートし、クライアントに展開するには、次の手順に従います。

ステップ 1　[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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [リソース（Resources）] の順に選択します。

[インポート（Import）] をクリックします。[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Object）] ウィンドウが表示されます（図 11-1）。

図 11-1　　カスタマイゼーション オブジェクトのインポート

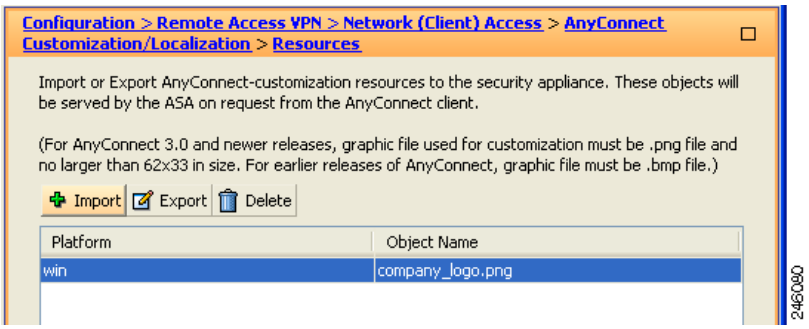


ステップ 2　インポートするファイルの名前を入力します。置き換え可能なすべての GUI コンポーネントのファイル名については、表 11-2、表 11-3、および表 11-4 を参照してください。

（注）　カスタム コンポーネントのファイル名は、AnyConnect GUI で使用されるファイル名と一致している必要があります。これはオペレーティング システムによって異なり、Mac および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを *company_logo.png* としてインポートする必要があります。別のファイル名でインポートすると、AnyConnect インストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソース ファイルを呼び出すことができます。

ステップ 3　プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。ファイルがテーブル（図 11-2）に表示されます。

図 11-2　テーブルに表示されたインポート済みのファイル



（注）　イメージをソース ファイルとして（たとえば、company_logo.bmp）インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、AnyConnect をカスタマイズします。たとえば、company_logo.bmp をカスタム イメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ（または元のシスコ ロゴ イメージ）をインポートするまで、クライアントはこのイメージの表示を継続します。

クライアント API を使用する実行ファイルの展開

Windows、Linux、または Mac コンピュータの場合、AnyConnect API を使用して、自分のユーザ インターフェイス（UI）を展開できます。クライアントのバイナリ ファイルを置き換えることによって、AnyConnect GUI または AnyConnect CLI を置き換えます。

カスタム UI を配信して、AnyConnect ソフトウェア アップデートを管理する必要があります。

次の AnyConnect 機能は、カスタム AnyConnect UI と互換性がありません。

- ASA からの AnyConnect ソフトウェアの展開。ASA で AnyConnect パッケージのバージョンを更新すると、カスタム UI を置き換えるエンド ユーザ クライアントが更新されることがあります。AnyConnect ソフトウェアの配布およびカスタム クライアントを管理する必要があります。AnyConnect クライアントを交換するには、ASDM の [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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [バイナリ（Binary）] ダイアログでバイナリをアップロードできますが、その機能はサポートされません。
- ネットワークアクセスマネージャと Web セキュリティ。[Web セキュリティ（Web Security）] または [ネットワークアクセスマネージャ（Network Access Manager）] を展開する場合は、Cisco AnyConnect Secure Mobility Client GUI を使用する必要があります。
- [ログイン前の起動（Start Before Logon）] はサポートされていません。

次の表に、異なるオペレーティング システムのクライアント実行ファイルのファイル名が表示されます。

表 11-1　クライアント実行ファイルのファイル名前

クライアント OS	クライアント GUI ファイル	クライアント CLI ファイル
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
Mac	非サポート[1]	vpn

1. ASA からの展開はサポートされません。ただし、Altiris Agent などの他の手段によって、クライアント GUI を置き換える Mac 用の実行ファイルを展開できます。

実行ファイルは、ASA にインポートしたあらゆるリソース ファイル（ロゴ イメージなど）を呼び出すことができます（図 11-1 を参照）。事前定義された GUI コンポーネントを置き換える場合とは異なり、独自の実行ファイルを展開する場合は、リソース ファイルに任意のファイル名を使用できます。

トランスフォームを使用した GUI のカスタマイズ

作成した独自のトランスフォームを、クライアント インストーラ プログラムを使用して展開することによって、AnyConnect GUI を大幅にカスタマイズすることができます（Windows のみ）。トランスフォームを ASA にインポートすると、インストーラ プログラムを使用して展開されます。

MSI トランスフォームを作成するには、Microsoft から Orca という名前の無料データベース エディタをダウンロードし、インストールします。このツールを使用して、既存のインストレーションを修正し、場合によっては新しいファイルを追加します。Orca ツールは、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。次のリンクから Orca プログラムを含むバンドルを入手できます。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp

SDK をインストールすると、Orca MSI は、次の場所に格納されます。

C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi

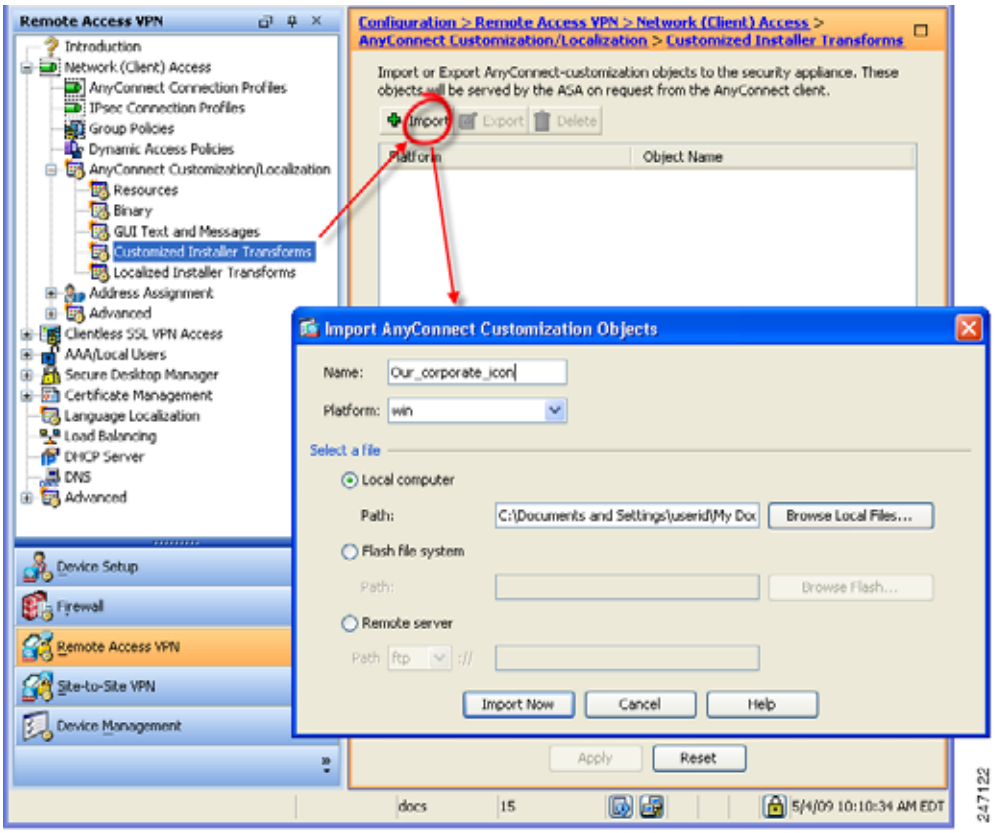
Orca ソフトウェアをインストールしてから、[スタート（Start）] > [すべてのプログラム（All Programs）] メニューを選択して Orca プログラムにアクセスします。

トランスフォームをインポートする手順は、次のとおりです。

ステップ 1　[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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [カスタマイズされたインストーラ トラン

スフォーム（Customized Installer Transforms）] の順に選択します。[インポート（Import）] をクリックします。[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Objects）] ウィンドウが表示されます（図 11-3）。

図 11-3　　カスタマイズ用トランスフォームのインポート

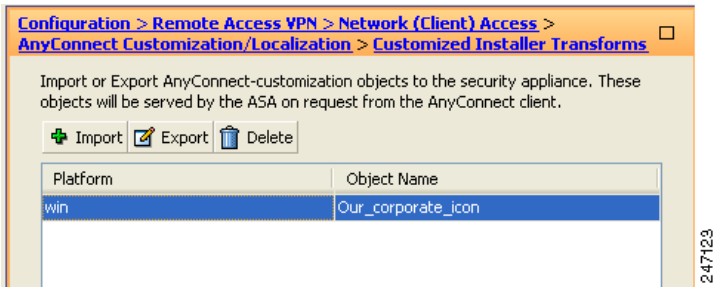


ステップ 2　インポートするファイルの名前を入力します。他のカスタマイズ用オブジェクトの名前とは異なり、この名前は ASA にとって重要ではないため、自由に指定できます。

ステップ 3　プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。ファイルがテーブル（図 11-4）に表示されます。

（注）　トランスフォームの適用先として選択できるのは Windows だけです。

図 11-4　　テーブルに表示されたカスタマイズ用のトランスフォーム



トランスフォームの例

このマニュアルでは、トランスフォームの作成についてのチュートリアルを提供できませんが、トランスフォームの代表的なエントリをいくつか次に示します。これらのエントリでは、*company_logo.bmp* がローカル コピーと置き換えられ、カスタム プロファイル *MyProfile.xml* がインストールされます。

```
DATA CHANGE - Component Component ComponentId
+ MyProfile.xml {39057042-16A2-4034-87C0-8330104D8180}

Directory_ Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml

DATA CHANGE - FeatureComponents Feature_ Component_
  + MainFeature MyProfile.xml

DATA CHANGE - File File Component_ FileName FileSize Version Language Attributes Sequence
  + MyProfile.xml MyProfile.xml MyProf~1.xml|MyProfile.xml 601 8192 35
 <> company_logo.bmp 37302{39430} 8192{0}

DATA CHANGE - Media DiskId LastSequence DiskPrompt Cabinet VolumeLabel Source
  + 2 35
```

カスタム アイコンおよびロゴの作成について

次の表で、AnyConnect がサポートするオペレーティング システムごとに、置き換えることができるファイルを示します。

（注） 独自のカスタム イメージを作成してクライアント アイコンを置き換えるには、使用するイメージのサイズを、オリジナルの Cisco イメージと同じサイズにする必要があります。

Windows の場合

Windows 用のファイルはすべて次の場所に格納されています。

%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\

（注） %PROGRAMFILES% は、同じ名前の環境変数を指します。ほとんどの Windows インストレーションでは、C:\Program Files です。

表 11-2 に、置き換えることができるファイルと、その影響を受けるクライアント GUI エリアを示します。

表 11-2　AnyConnect for Windows：アイコン ファイル

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
about.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
about_hover.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
ArrowDown.png このボタンを使用すると、ユーザはネットワーク アクセス マネージャの [詳細（Advanced）] ウィンドウにある [設定（Configuration）] タブで、[ネットワーク（Networks）] リスト内のネットワークを下に移動できます。 サイズは調整できません。 	16 x 22 PNG
ArrowDownDisabled.png このディセーブルになったボタンを使用すると、ユーザはネットワーク アクセス マネージャの [詳細（Advanced）] ウィンドウにある [設定（Configuration）] タブで、[ネットワーク（Networks）] リスト内のネットワークを下に移動できます。 サイズは調整できません。 	16 x 22 PNG
ArrowUp.png このボタンを使用すると、ユーザはネットワーク アクセス マネージャの [詳細（Advanced）] ウィンドウにある [設定（Configuration）] タブで、[ネットワーク（Networks）] リスト内のネットワークを上に移動できます。 サイズは調整できません。 	16 x 22 PNG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
ArrowUpDisabled.png このディセーブルになったボタンを使用すると、ユーザはネットワーク アクセス マネージャの [詳細（Advanced）] ウィンドウにある [設定（Configuration）] タブで、[ネットワーク（Networks）] リスト内のネットワークを上に移動できます。 サイズは調整できません。 	16 x 22 PNG
company_logo.png トレイ フライアウトおよび [詳細（Advanced）] ダイアログの左上、および [バージョン情報（About）] ダイアログの右下に表示される企業ロゴ。 最大サイズは 97 x 58 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 97 x 58 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	97 x 58（最大） PNG
attention.ico 注意または操作が必要な状態をユーザに通知するシステム トレイ アイコン。たとえば、ユーザ クレデンシャルについてのダイアログです。 サイズは調整できません。 	16 x 16 ICO
error.ico 1 つ以上のコンポーネントで致命的な問題が発生していることをユーザに通知するシステム トレイ アイコン。 サイズは調整できません。 	16 x 16 ICO

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
neutral.ico クライアントのコンポーネントが正常に動作していることを示すシステム トレイ アイコン。 サイズは調整できません。 	16 x 16 ICO
vpn_connected.ico VPN が接続中であることを示すシステム トレイアイコン。 サイズは調整できません。 	16 x 16 ICO
cues_bg.jpg トレイ フライアウト、[詳細（Advanced）] ウィンドウ、および [バージョン情報（About）] ダイアログの背景イメージ。 イメージが引き伸ばされることはないため、過度に小さい置換イメージを使用すると、領域が黒くなります。 	1260 x 1024 JPEG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
gradient.png [詳細（Advanced）] ウィンドウ内のコンポーネント タイトル背景のグラデーション。 	1 x 38 PNG
GUI.tif アプリケーションおよびシステム トレイ アイコン。 	
mftogglebtn.png [詳細（Advanced）] ウィンドウ内の非アクティブ メニューの背景。 AnyConnect のインストールに複数のコンポーネント（ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリなど）が含まれている場合は、GUI の [詳細（Advanced）] ウィンドウには各コンポーネントのメニュー オプションが表示されます。このイメージは、非アクティブのメニュー オプションの背景に使用されます。 	300 x 40 PNG
mftogglebtn-down.png [詳細（Advanced）] ウィンドウ内の [ステータス概要（Status Overview）] メニュー オプションの背景（アクティブのとき）。 AnyConnect のインストールに複数のコンポーネント（ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリなど）が含まれている場合は、GUI の [詳細（Advanced）] ウィンドウには各コンポーネントのメニュー オプションが表示されます。このイメージは、[詳細（Advanced）] ウィンドウが最初に表示されたとき、およびユーザが [ステータス概要（Status Overview）] メニュー オプションをクリックしたときに、このメニュー オプションの背景として使用されます。 	300 x 40 PNG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
mftogglebtn-down-solid.png [ステータス概要（Status Overview）] メニュー オプション以外の [詳細（Advanced）] ウィンドウのメニュー オプションの背景。そのメニュー オプションがにアクティブのときに使用されます。 AnyConnect のインストールに複数のコンポーネント（ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリなど）が含まれている場合は、GUI の [詳細（Advanced）] ウィンドウには各コンポーネントのメニュー オプションが表示されます。このイメージは、[ステータス概要（Status Overview）] メニュー オプション以外のすべてのメニュー オプションについて、ユーザがそのメニュー オプションをクリックしてアクティブにしたときに背景として使用されます。 	300 x 40 PNG
minimize.png トレイ フライアウトの最小化ボタン。 サイズは調整できません。 	16 x 16 PNG
minimize-hover.png トレイ フライアウトの最小化ボタン（マウス オーバーしたときに表示されます）。 サイズは調整できません。 	16 x 16 PNG
pinned.png ネットワーク アクセス マネージャのトレイ フライアウト タイトルに表示されるこのボタンを使用すると、ネットワークが自動的に選択されるようになります。 サイズは調整できません。 	38 x 30 PNG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

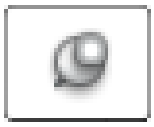
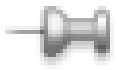
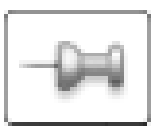
Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
pinned_button.png ネットワーク アクセス マネージャのトレイ フライアウト タイトルに表示されるこのボタン（マウス オーバーしたときに表示されます）を使用すると、ネットワークが自動的に選択されるようになります。 サイズは調整できません。 	38 x 30 PNG
status_ico_attention.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [注意（Attention）] ステータス アイコンで、ユーザの注意が必要なことを示します。 サイズは調整できません。 	16 x 16 PNG
status_ico_error.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [エラー（Error）] ステータス アイコンで、サービス到達不能などの深刻なエラーを示します。 サイズは調整できません。 	16 x 16 PNG
status_ico_good.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [標準（Good）] ステータス アイコンで、そのコンポーネントが正常に動作していることを示します。 サイズは調整できません。 	16 x 16 PNG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
status_ico_neutral.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [中（Neutral）] ステータス アイコンで、そのコンポーネントは正常に動作しているものの、必ずしもそのコンポーネントがアクティブとは限らないことを示します。 サイズは調整できません。 	16 x 16 PNG
status_ico_transition.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [移行中（Transition）] ステータス アイコンで、接続から接続解除への移行など、状態遷移中であることを示します。 サイズは調整できません。 	16 x 16 PNG
status_ico_trusted.png トレイ フライアウトおよび [詳細（Advanced）] ウィンドウの [ステータス概要（Status Overview）] ペインにある各コンポーネントにより使用される [信頼されている（Trusted）] ステータス アイコンで、そのコンポーネントは正常に動作しているものの、Trusted Network Detection（TND）機能などによって設定されたポリシーによってディセーブルになっていることを示します。 サイズは調整できません。 	16 x 16 PNG
transition_1.ico transition_2.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 PNG

表 11-2　AnyConnect for Windows：アイコン ファイル （続き）

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
transition_2.ico transition_1.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 PNG
transition_3.ico transition_1.ico および transition_2.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 PNG
unpinned.png ネットワーク アクセス マネージャのトレイ フライアウト タイトルに表示されるこのボタンを使用すると、ユーザは現在のネットワークに排他的に接続できます。 サイズは調整できません。 	38 x 30 PNG
unpinned_button.png ネットワーク アクセス マネージャのトレイ フライアウト タイトルに表示されるこのボタン（マウス オーバーしたときに表示されます）を使用すると、ユーザは現在のネットワークに排他的に接続できます。 サイズは調整できません。 	38 x 30 PNG

Linux の場合

Linux 用のファイルはすべて次の場所に格納されています。

/opt/cisco/anyconnect/pixmaps/

表 11-3 に、置き換えることができるファイルと、その影響を受けるクライアント GUI エリアを示します。

表 11-3　Linux 用 AnyConnect : アイコン ファイル

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
company-logo.png ユーザ インターフェイスの各タブに表示される企業ロゴ。 AnyConnect 3.0 以降の場合は、62 x 33 ピクセル以下の PNG イメージを使用してください。 	142 x 92 PNG
cvc-about.png [バージョン情報（About）] タブに表示されるアイコン。 	16 x 16 PNG
cvc-connect.png [接続（Connect）] ボタンの隣、および [接続（Connection）] タブに表示されるアイコン。 	16 x 16 PNG
cvc-disconnect.png [接続解除（Disconnect）] ボタンの隣に表示されるアイコン。 	16 x 16 PNG
cvc-info.png [統計情報（Statistics）] タブに表示されるアイコン。 	16 x 16 PNG

表 11-3　Linux 用 AnyConnect：アイコン ファイル

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ x 高さ）およびタイプ
systray_connected.png クライアントが接続中のときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_notconnected.png クライアントが接続中でないときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_disconnecting.png クライアントが接続解除の処理中のときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_quarantined.png クライアントが隔離中のときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_reconnecting.png クライアントが再接続中のときに表示されるトレイ アイコン。 	16 x 16 PNG
vpnui48.png メイン プログラム アイコン。 	48 x 48 PNG

Mac OS X の場合

OS X 用のファイルはすべて次の場所に格納されています。

/Applications/Cisco AnyConnect Secure Mobility Client/Contents/Resources

（注）　Resources フォルダは、[アプリケーション（Applications）] > [Cisco] に移動して [Cisco AnyConnect Secure Mobility Client] をクリックし、[パッケージ コンテンツの表示（Show Package Contents）] を選択すると見つかります。

表 11-4 に、置き換えることができるファイルと、その影響を受けるクライアント GUI エリアを示します。

表 11-4　Mac OS X 用 AnyConnect：アイコン ファイル

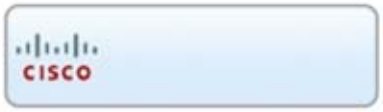
Mac OS X インストレーションでのファイル名	イメージ サイズ（ピクセル数、幅 × 高さ）
bubble.png クライアントが接続または接続解除したときに表示される通知バブル。 	142 x 92 PNG
connected.png クライアントが接続中のときに、接続解除ボタンの下に表示されるアイコン。 	32 x 32 PNG
logo.png メイン画面の右上に表示されるロゴ アイコン。 	50 x 33 PNG
menu_connected.png 接続状態のメニューバー アイコン。 	16 x 16 PNG
menu_error.png エラー状態のメニューバー アイコン。 	16 x 16 PNG

表 11-4　Mac OS X 用 AnyConnect : アイコン ファイル

Mac OS X インストレーションでのファイル名	イメージ サイズ（ピクセル数、幅 × 高さ）
menu_idle.png 接続解除されているアイドル メニューバー アイコン。 	16 x 16 PNG
menu_quarantined.png 隔離状態のメニューバー アイコン。 	16 x 16 PNG
menu_reconnecting.png 再接続処理中のメニューバー アイコン。 	16 x 16 PNG
warning.png さまざまな認証/証明書警告のログイン フィールドの代わりに表示されるアイコン。 	40 x 40 PNG
vpngui.icns すべてのアイコン サービス（Dock、Sheets、Finder など）で使用される Mac OS X アイコン ファイル フォーマット。 	128 x 128 PNG

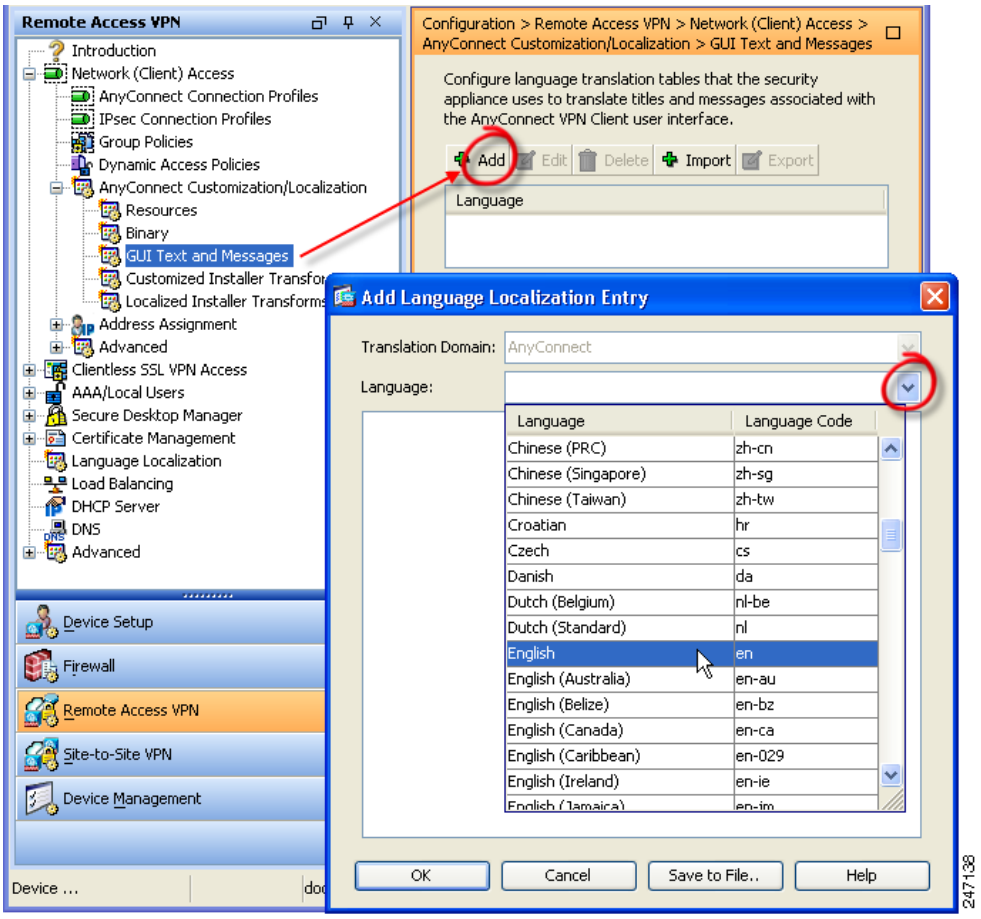
デフォルトの AnyConnect の英語メッセージの変更

英語変換テーブルを追加し、ASDM の編集ウィンドウでメッセージ テキストを変更することによって、AnyConnect GUI に表示される英語のメッセージを変更できます。

ここでは、デフォルトの英語メッセージを変更する方法について説明します。

ステップ 1　[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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）] の順に選択します。[追加（Add）] をクリックします。[言語ローカリゼーション エントリの追加（Add Language Localization Entry）] ウィンドウが表示されます（図 11-5）。

図 11-5　英語変換テーブルの追加

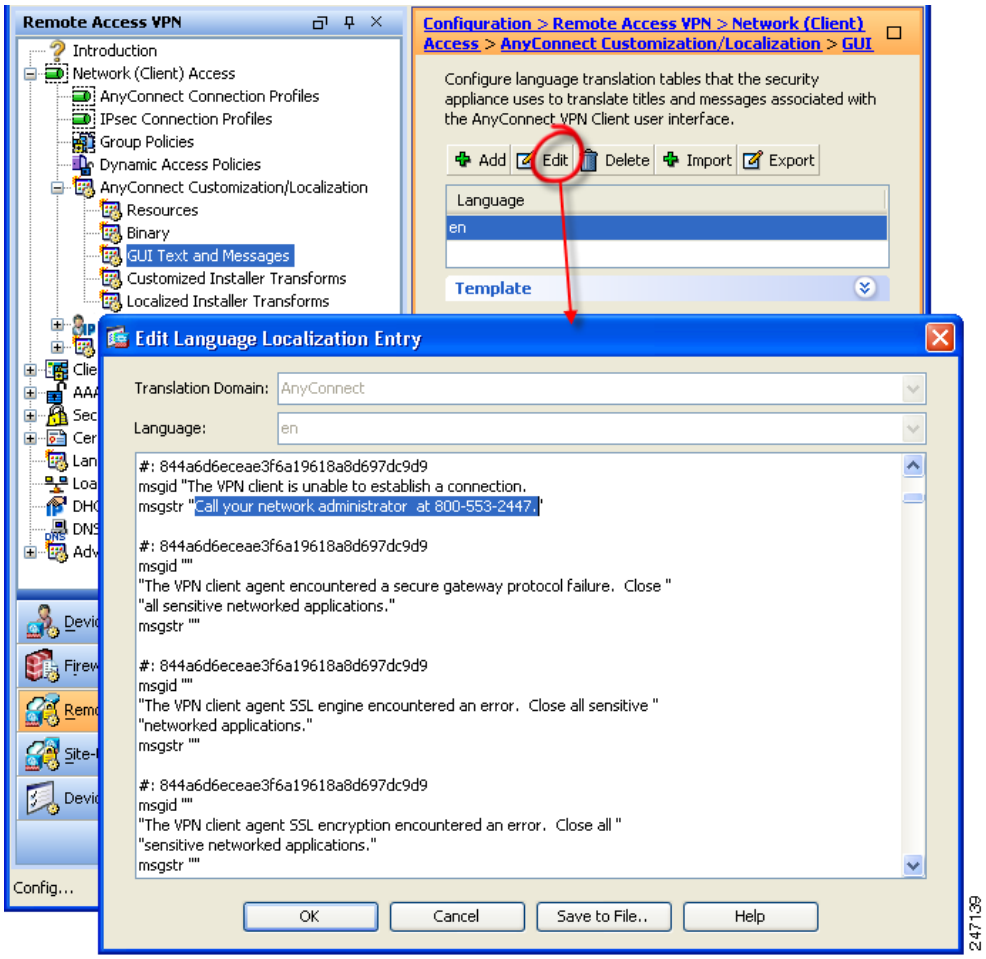


ステップ 2　[言語（Language）] ドロップ リストをクリックし、言語として [英語（en）（*English* (en)）] を指定します。英語の変換テーブルが、ペインの言語リストに表示されます。

ステップ 3　[編集（Edit）] をクリックして、メッセージの編集を開始します。[言語のローカライズ エントリの編集（Edit Language Localization Entry）] ウィンドウが表示されます（図 11-6）。msgid の引用符で囲まれたテキストは、クライアントに表示されるデフォルトの英語テキストです。変更*してはいけません*。msgstr の文字列には、msgid のデフォルト テキストを置き換えるために、クライアントで使用されるテキストが含まれます。msgstr の引用符の間に、使用するテキストを挿入します。

次の例では、「Call your network administrator at 800-553-2447」が挿入されています。

図 11-6　メッセージ テキストの編集



ステップ 4　[OK] をクリックしてから、[GUI テキストおよびメッセージ（GUI Text and Messages）] ペインで [適用（Apply）] をクリックして、変更を保存します。

AnyConnect クライアントの GUI とインストーラのローカライズ

クライアントおよびすべてのオプション モジュールは、別の言語にローカライズ（翻訳）できます。また、VPN サービスを提供するコア VPN クライアントのインストーラ プログラムもローカライズできます。

（注）　Altiris Agent などの社内の IT 展開ソフトウェアを使用して AnyConnect を展開する場合、翻訳できるのはインストーラだけです。クライアントは翻訳できません。ASA からクライアントを展開する場合のみ、クライアントを翻訳できます。

ここでは、この機能の設定について説明し、手順を示します。

- 「AnyConnect GUI のローカライズ」（P.11-22）
- 「AnyConnect インストーラ画面のローカライズ」（P.11-30）
- 「ツールを使用した社内展開用メッセージ カタログの作成」（P.11-32）
- 「新しい翻訳テンプレートと変換テーブルの統合」（P.11-33）

AnyConnect GUI のローカライズ

セキュリティ アプライアンスは、変換テーブルを使用して AnyConnect に表示されるユーザ メッセージを翻訳します。この変換テーブルは、翻訳されたメッセージ テキストを挿入する文字列が記述されたテキスト ファイルです。Windows 用 AnyConnect パッケージ ファイルには、AnyConnect メッセージとして使用する、英語の言語テンプレートが含まれています。クライアント イメージをロードすると、ASA によって自動的にこのファイルがインポートされます。このファイルには、メッセージ文字列の最新の変更が含まれています。これを使用すると、別の言語用の変換テーブルを新しく作成できます。

リモート ユーザが ASA に接続してクライアントをダウンロードすると、クライアントはそのコンピュータの設定言語を検出して、該当する変換テーブルを適用します。クライアントは、オペレーティング システムのインストール時に指定されたロケールを検出します。ASA の変換テーブルを更新する場合、クライアントを再起動し、別の接続に成功するまで、変換されたメッセージは更新されません。

Windows の言語オプションの詳細については、次の URL を参照してください。

http://www.microsoft.com/windowsxp/using/setup/winxp/yourlanguage.mspx
http://www.microsoft.com/globaldev/reference/win2k/setup/changeUI.mspx

（注）　クライアントを ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのカタログ ユーティリティを使用して、手動で AnyConnect 変換テーブル（anyconnect.po）を .mo ファイルに変換し、その .mo ファイルをクライアント コンピュータの適切なフォルダにインストールします。詳細については、「ツールを使用した社内展開用メッセージ カタログの作成」（P.11-32）を参照してください。

次の項では、GUI テキストを翻訳する 2 つの異なる方法について、詳しい手順を説明します。

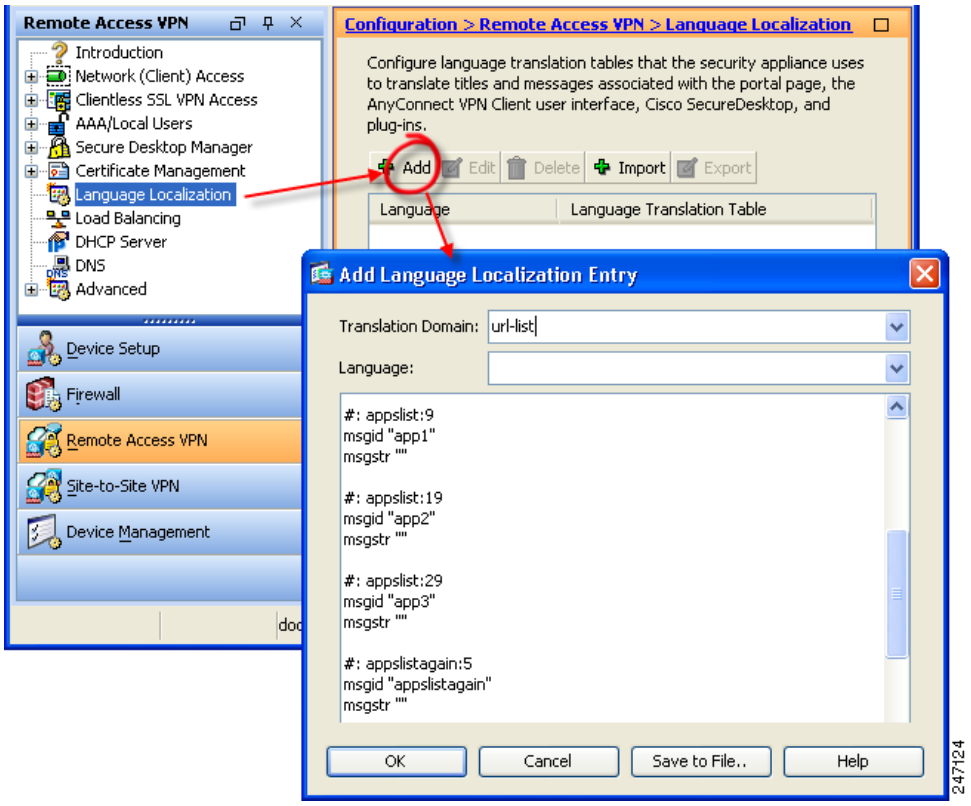
- 「ASDM 変換テーブル エディタを使用した翻訳」（P.11-23）
- 「変換テーブルのエクスポートと編集による翻訳」（P.11-27）

ASDM 変換テーブル エディタを使用した翻訳

ここでは、ASDM を使用して AnyConnect GUI をローカライズする方法について説明します。

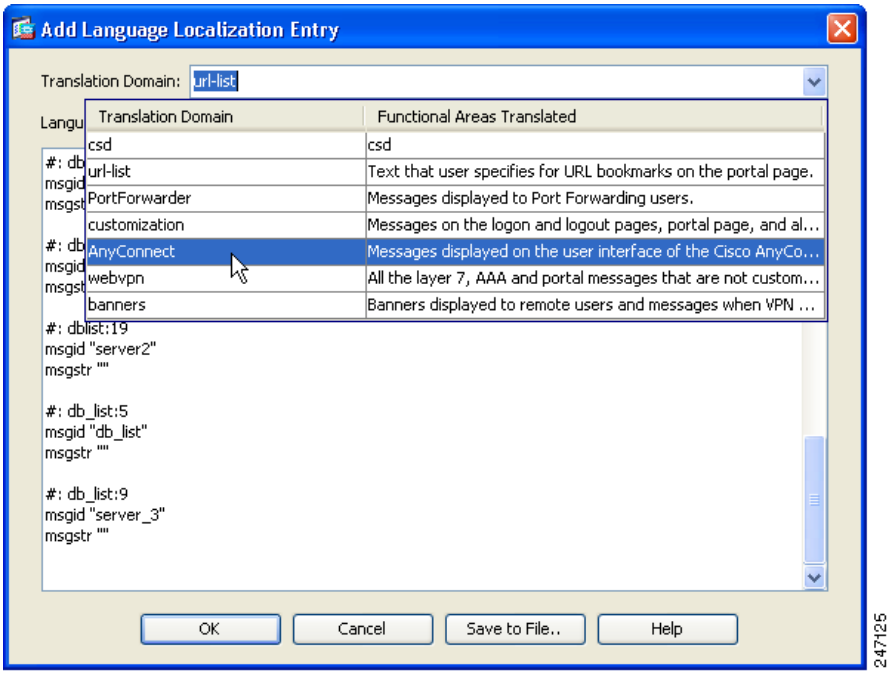
ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] の順に選択します。[追加（Add）] をクリックします。[言語ローカリゼーション エントリの追加（Add Language Localization Entry）] ウィンドウが表示されます（図 11-7）。

図 11-7　[言語のローカライズ（Language Localization）] ペイン



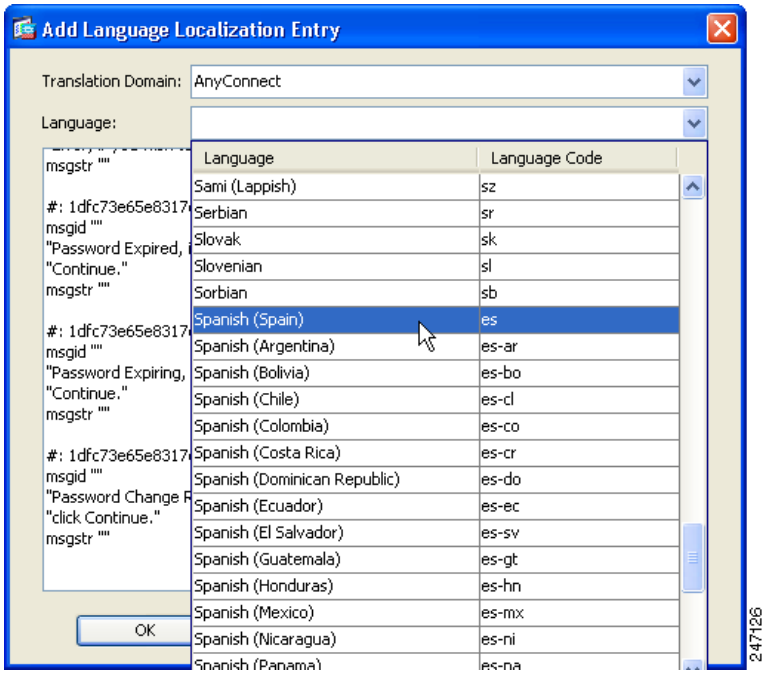
ステップ 2　[変換ドメイン（Translation Domain）] ドロップ リストをクリックし、[AnyConnect] を選択します（図 11-8）。これによって、AnyConnect GUI 関連のメッセージだけが編集用に表示されます。

図 11-8　変換ドメイン



ステップ 3　この変換テーブルの言語を指定します（図 11-9）。ASDM では、Windows およびブラウザで認識される標準的な言語略称が、このテーブルで使用されます（スペイン語は *es* など）。

図 11-9　言語の選択

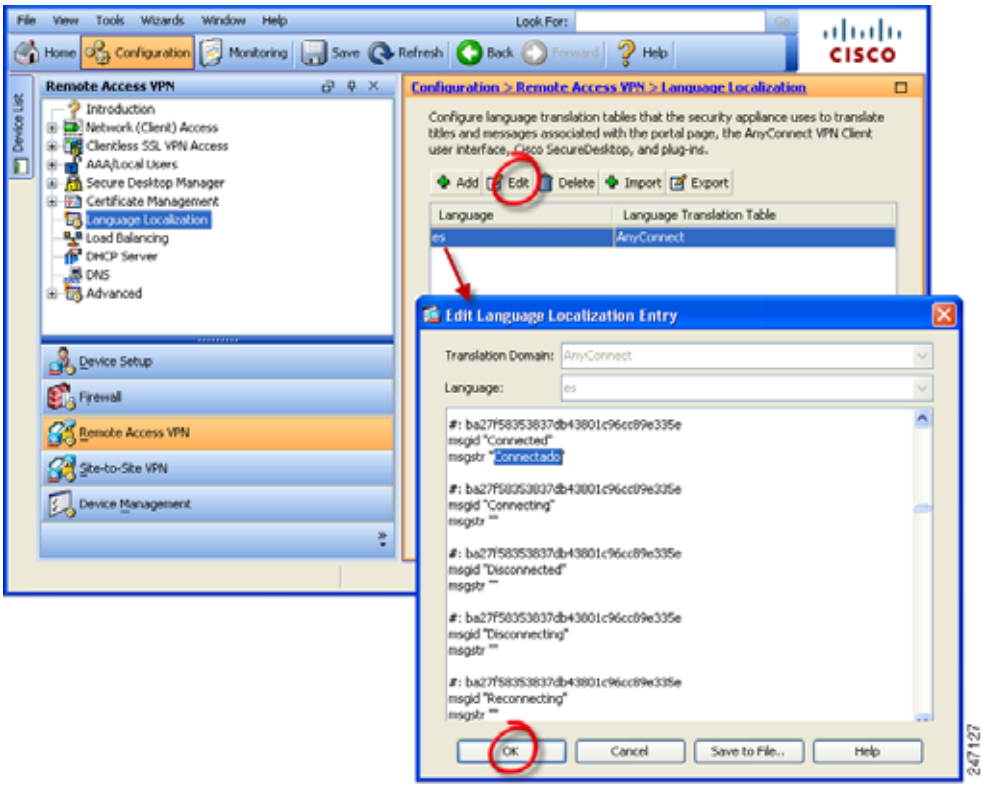


ステップ 4　変換テーブルが、ペインの言語リストに表示されます（この例では *es*）。ただし、翻訳されたメッセージはありません。翻訳されたテキストの追加を開始するには、[編集（Edit）] をクリックします。[言語のローカライズ エントリの編集（Edit Language Localization Entry）] ウィンドウが表示されます（図 11-10）。

メッセージ文字列（msgstr）の引用符の間に、翻訳したテキストを追加します。次の例では、メッセージ文字列の引用符の間に「*Connectado*」（「*Connected*」のスペイン語）を挿入しています。

[OK] をクリックしてから、[言語のローカライズ（Language Localization）] ペインで [適用（Apply）] をクリックして変更を保存します。

図 11-10　変換テーブルの編集



変換テーブルのエクスポートと編集による翻訳

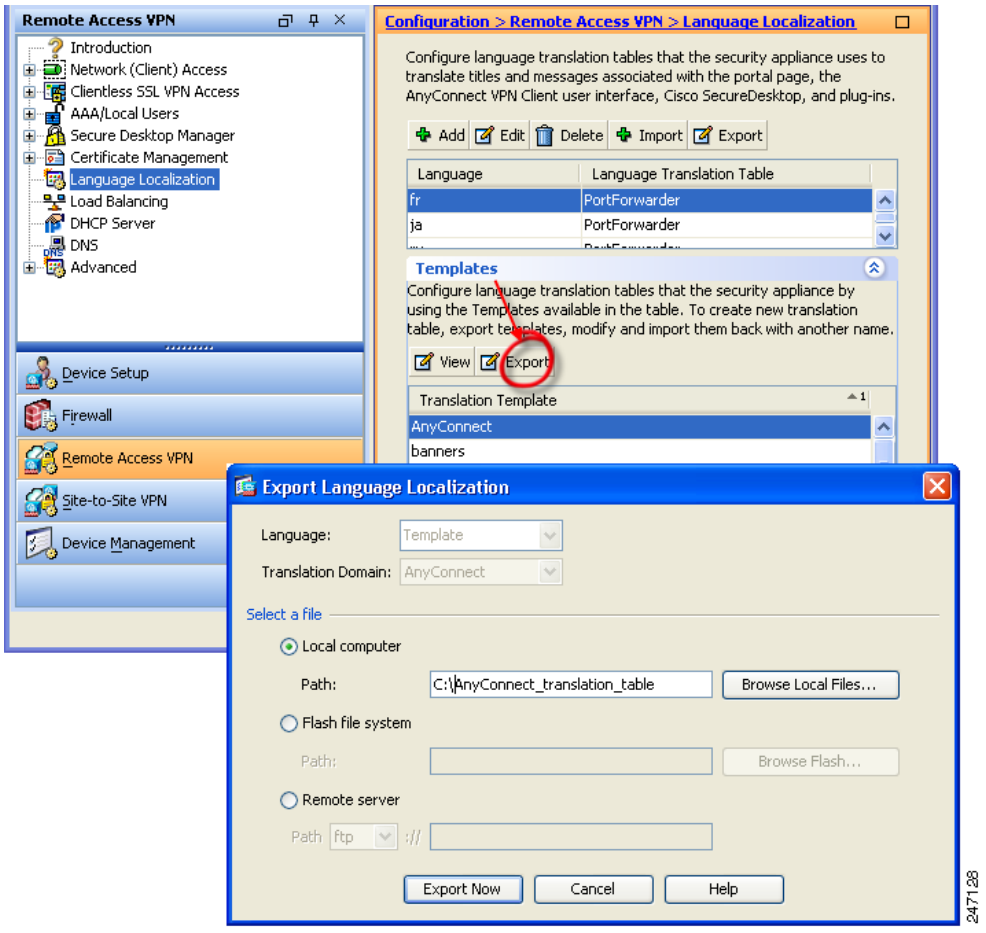
ここでは、AnyConnect 翻訳テンプレートをリモート コンピュータにエクスポートしてから、エディタや、Gettext または Poedit などのサードパーティ製ツールを使用して変換テーブルを編集する手順について説明します。

GNU プロジェクトの Gettext ユーティリティには Windows 版があり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。

ステップ 1　AnyConnect 翻訳テンプレートをエクスポートします。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] の順に選択します。[言語のローカライズ（Language Localization）] ペインが表示されます（図 11-11）。[テンプレート（Templates）] リンクをクリックすると、利用可能なテンプレートのテーブルが表示されます。[AnyConnect] テンプレートを選択し、[エクスポート（Export）] をクリックします。[言語のローカライズのエクスポート（Export Language Localization）] ウィンドウが表示されます。

図 11-11　翻訳テンプレートのエクスポート



ステップ 2　エクスポートの方法を選択し、ファイル名を指定します。図 11-11 では、ファイル名 *AnyConnect_translation_table* で、ローカル コンピュータにエクスポートしています。

ステップ 3　変換テーブルを編集します。

次の例は、AnyConnect テンプレートの一部を示しています。この出力の最後には、メッセージ *Connected* のメッセージ ID フィールド（msgid）とメッセージ文字列フィールド（msgstr）があります。このメッセージは、クライアントが VPN 接続を確立したときに、AnyConnect GUI に表示されます（テンプレート全体には、メッセージ フィールドのペアが多数含まれています）。

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

msgid "Connected"
msgstr ""
```

msgid には、デフォルト変換が含まれています。msgid に続く msgstr が変換を提供します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、メッセージ "Connected" をスペイン語で変換するには、引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

ファイルは必ず保存してください。

ステップ 4　この翻訳テンプレートを、指定した言語用の新しい変換テーブルとしてインポートします。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] の順に選択します。[言語のローカライズ（Language Localization）] ペインが表示されます（図 11-12）。[インポート（Import）] をクリックします。[言語のローカライズのインポート（Import Language Localization）] ウィンドウが表示されます。

ステップ 5　[言語（Language）] ドロップダウン リストをクリックして、この変換テーブルの言語（および業界で認められている略称）を選択します。手動で略称を入力する場合は、ブラウザおよびオペレーティング システムが認識できる略称を使用してください。

ステップ 6　[変換ドメイン（Translation Domain）] として *AnyConnect* を指定し、インポート方法を選択して、ファイル名を指定します。[今すぐインポート（Import Now）] をクリックします。テーブルが正常にインポートされたことを示すメッセージが表示されます。

[適用（Apply）] をクリックし、変更を必ず保存してください。

図 11-11 では、言語として *Spanish*(es) を指定し、ステップ 1 でエクスポートしたファイル（AnyConnect_translation_table）をインポートしています。図 11-13 では、AnyConnect の言語リストに、スペイン語用の新しい変換テーブルが表示されています。

図 11-12　新しい変換テーブルとしての翻訳テンプレートのインポート

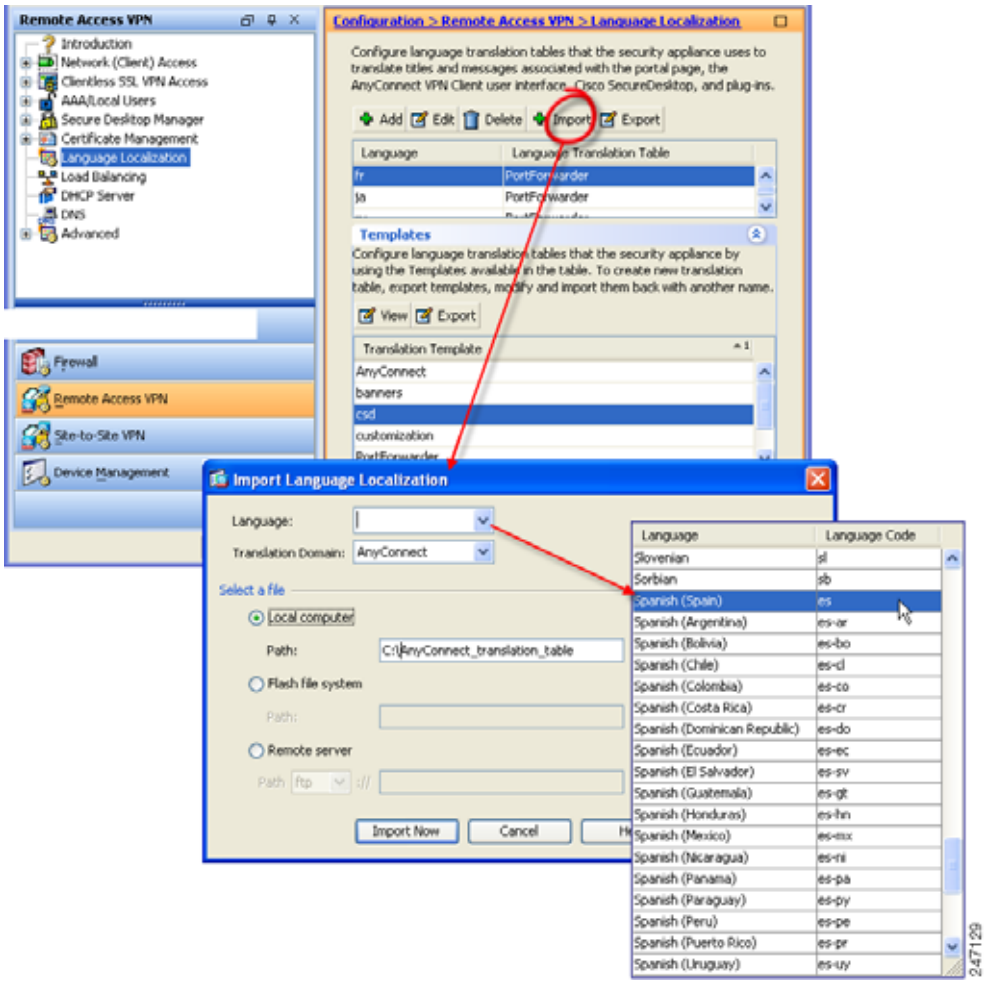
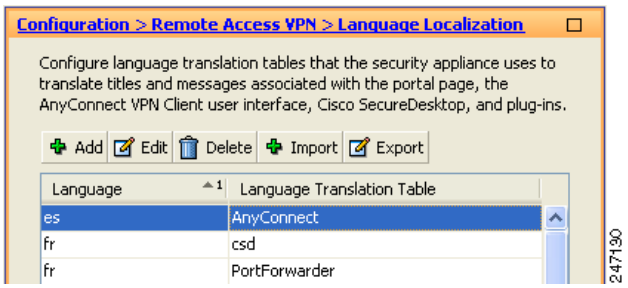


図 11-13　言語テーブルに表示された新しい言語



AnyConnect インストーラ画面のローカライズ

AnyConnect GUI と同様に、VPN サービスをインストールするクライアント インストーラ プログラムで表示されるメッセージを翻訳できます。ASA はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

（注）　AnyConnect のすべてのリリースには、ローカライズされたトランスフォームが含まれています。このトランスフォームは、管理者が新しいソフトウェアを含む AnyConnect パッケージをアップロードすると、必ず ASA にアップロードできます。ローカリゼーション トランスフォームを使用している場合は、新しい AnyConnect パッケージをアップロードする際に、必ず CCO の最新リリースでローカリゼーション トランスフォームをアップデートしてください。

言語にはそれぞれ独自のトランスフォームがあります。トランスフォームは Orca などのトランスフォーム エディタで編集して、メッセージの文字列を変更できます。その後、トランスフォームを ASA にインポートします。ユーザがクライアントをダウンロードすると、クライアントはコンピュータの目的の言語（オペレーティング システムのインストール時に指定されたロケール）を検出し、該当するトランスフォームを適用します。

現時点では、30 の言語に対応するトランスフォームが用意されています。これらのトランスフォームは、cisco.com の AnyConnect ソフトウェア ダウンロード ページから、次の .zip ファイルで入手できます。

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

このファイルの <VERSION> は、AnyConnect のリリース バージョン（2.2.103 など）を表します。

パッケージには使用可能な翻訳用のトランスフォーム（.mst ファイル）が含まれています。用意されている 30 以外の言語をリモート ユーザに表示する必要がある場合は、独自のトランスフォームを作成し、それを新しい言語として ASA にインポートすることができます。Microsoft のデータベース エディタ Orca を使用して、既存のインストレーションおよび新規ファイルを修正できます。Orca は、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。次のリンクから Orca プログラムを含むバンドルを入手できます。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp

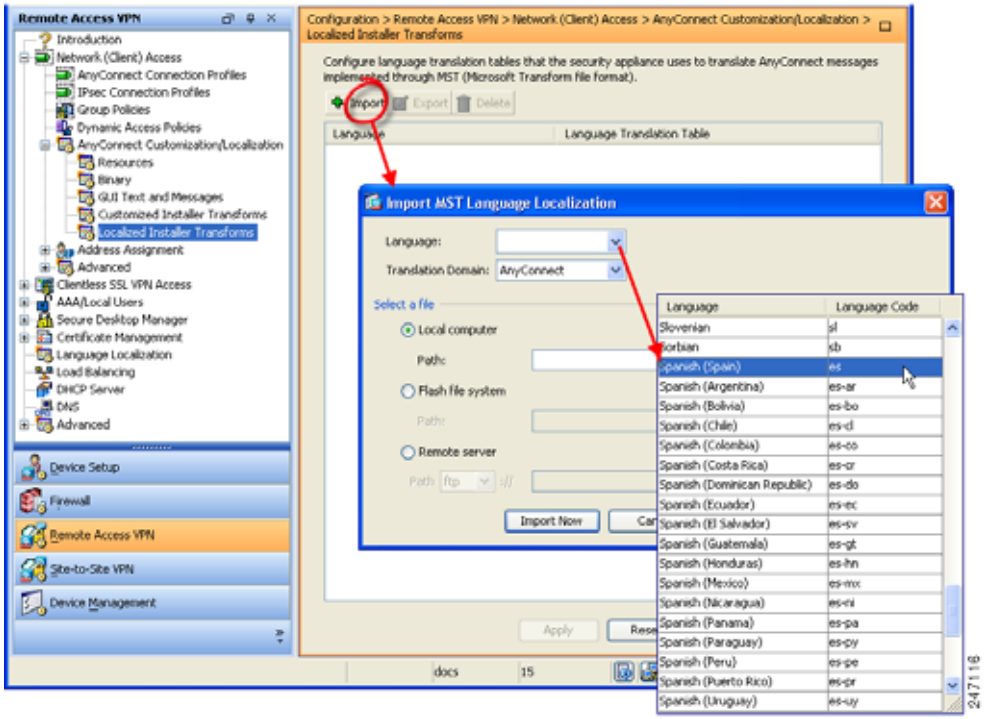
SDK をインストールすると、Orca MSI は、次の場所に格納されます。

C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi

ここでは、ASDM を使用してトランスフォームを ASA にインポートする方法について説明します。

ステップ 1　トランスフォームをインポートします。[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 カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [ローカライズされたインストーラ トランスフォーム（Localized Installer Transforms）] の順に選択します。[インポート（Import）] をクリックします。[MST 言語ローカライズのインポート（Import MST Language Localization）] ウィンドウが表示されます（図 11-14）。

図 11-14　インストーラ プログラムを翻訳するトランスフォームのインポート



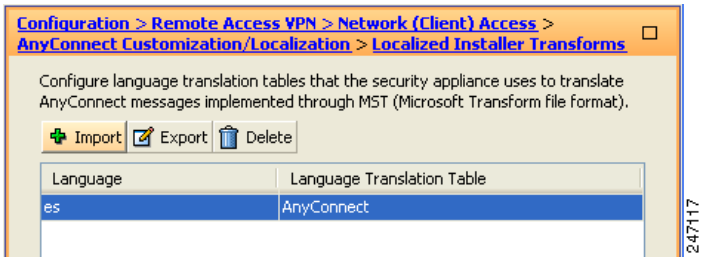
ステップ 2　[言語（Language）] ドロップダウン リストをクリックして、このトランスフォーム用の言語（および業界で認められている略称）を選択します。手動で略称を入力する場合は、ブラウザおよびオペレーティング システムが認識できる略称を使用してください。

ステップ 3　[今すぐインポート（Import Now）] をクリックします。テーブルが正常にインポートされたことを示すメッセージが表示されます。

[適用（Apply）] をクリックし、変更を必ず保存してください。

図 11-14 では、言語に *Spanish* (es) を指定しています。図 11-15 では、AnyConnect の言語リストに、スペイン語用の新しいトランスフォームが表示されています。

図 11-15　テーブルに表示されたインポート済みのトランスフォーム



ツールを使用した社内展開用メッセージ カタログの作成

クライアントを ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのユーティリティを使用して、手動で AnyConnect 変換テーブルをメッセージ カタログに変換できます。テーブルを .po ファイルから .mo ファイルに変換後、そのファイルをクライアント コンピュータ上の該当するフォルダに配置します。

Gettext は GNU プロジェクトのユーティリティであり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。

AnyConnect メッセージ テンプレートのディレクトリ

AnyConnect メッセージ テンプレートは、次に示すフォルダに格納されています。

（注）　**\l10n** ディレクトリは、次に示す各ディレクトリ パスの一部です。このディレクトリ名のスペルは、小文字の l（「エル」）、1、0、小文字の n です。

Windows 7 および Windows Vista

```
<DriveLetter>:\Program Data\Cisco\Cisco AnyConnect Secure Mobility
Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES
```

例：

```
<DriveLetter>:\Program Data\Cisco\Cisco AnyConnect Secure Mobility
Client\l10n\en-us\LC_MESSAGES
```

Windows XP：

```
%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure
Mobility Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES
```

Mac OS X および Linux：

```
/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES
```

メッセージ カタログの作成

Gettext を使用してメッセージ カタログを作成する手順は、次のとおりです。

ステップ 1　Gettext ユーティリティを http://www.gnu.org/software/gettext/ からダウンロードし、管理用のコンピュータ（リモートのユーザ コンピュータ以外）にインストールします。

ステップ 2　AnyConnect がインストールされたコンピュータにある、AnyConnect メッセージ テンプレート *AnyConnect.po* のコピーを取得します。

ステップ 3　この AnyConnect.po ファイルを編集し（notepad.exe または任意のプレーン テキスト エディタを使用）、必要に応じて文字列を変更します。

ステップ 4　Gettext のメッセージ ファイル コンパイラを実行して、次のように .po ファイルから .mo ファイルを作成します。

```
msgfmt -o AnyConnect.mo AnyConnect.po
```

ステップ 5　ユーザのコンピュータ上の正しいメッセージ テンプレート ディレクトリに .mo ファイルのコピーを格納します。詳細については、AnyConnect メッセージ テンプレートのディレクトリを参照してください。

新しい翻訳テンプレートと変換テーブルの統合

当社では、クライアント接続に関する有用な情報を提供するため、AnyConnect ユーザに表示する新しいメッセージを追加することがあります。そのような新しいメッセージの翻訳を可能にするため、当社で新しいメッセージ文字列を作成し、それを最新のクライアント イメージにパッケージされた翻訳テンプレートに含めてあります。そのため、最新のクライアントにアップグレードすると、新しいメッセージが含まれたテンプレートも入手できます。ただし、前のクライアントに含まれていたテンプレートを基礎に変換テーブルを作成してある場合は、リモート ユーザに新しいメッセージが自動的に表示されるわけでは*ありません*。最新のテンプレートを変換テーブルに統合し、変換テーブルに新しいメッセージを含める必要があります。

統合には、便利なサードパーティ製のツールを利用できます。GNU プロジェクトの Gettext ユーティリティには Windows 版があり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。両方の手順を次に示します。

ステップ 1　[リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] > [テンプレート（Templates）] を選択し、最新の AnyConnect 翻訳テンプレートをエクスポートします。*AnyConnect.pot* というファイル名で、テンプレートをエクスポートします。このファイル名にすると、msgmerge.exe プログラムからこのファイルがメッセージ カタログ テンプレートとして認識されます。

（注）　この手順は、すでに最新の AnyConnect イメージ パッケージを ASA にロードしてあることが前提になっています。まだロードしていない場合は、テンプレートをエクスポートできません。

ステップ 2　AnyConnect テンプレートおよび変換テーブルを統合します。

Windows 版の Gettext ユーティリティを使用している場合は、コマンド プロンプト ウィンドウを開き、次のコマンドを実行します。このコマンドでは、次のように、AnyConnect 変換テーブル（.po）とテンプレート（.pot）が統合され、*AnyConnect_merged.po* ファイルが新しく作成されます。

msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot

このコマンドの実行結果の例を次に示します。

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po
AnyConnect.pot
..................................... done.
```

Poedit を使用している場合は、初めに AnyConnect.po ファイルを開きます。それには、[ファイル（File）] > [オープン（Open）] > <AnyConnect.po> の順に選択します。
次に、[カタログ（Catalog）] > [POT ファイル <AnyConnect.pot> から更新する（Update from POT file <*AnyConnect.pot*>）] の順に選択して、テンプレートと統合します。
新しい文字列と使用されなくなった文字列の両方を示す、[サマリーの更新（Update Summary）] ウィンドウが表示されます。ファイルを保存します。このファイルを次の手順でインポートします。

ステップ 3　[リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] から、統合した変換テーブルをインポートします。[インポート（Import）] をクリックし、言語を指定して、翻訳ドメインとして **AnyConnect** を選択します。インポートするファイルとして *AnyConnect_merged.po* を指定します。

CHAPTER 12

AnyConnect セッションの管理、モニタリング、およびトラブルシューティング

この章では、次のテーマおよびタスクについて説明します。

すべての VPN セッションの接続解除

セッションを含め、すべての SSL VPN セッションをログオフするには、グローバル コンフィギュレーション モードで　Cisco AnyConnect Secure Mobility Client **vpn-sessiondb logoff svc** コマンドを使用します。

vpn-sessiondb logoff svc

これに応答して、システムは VPN セッションをログオフするかどうかを確認するように要求します。確認するために、**Enter** キーを押すか、または **y** を入力します。ログオフをキャンセルするには、その他のキーを入力します。

次に、すべての SSL VPN セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions logged off : 6
hostname#
```

個々の VPN セッションの接続解除

name オプションまたは **index** オプションのいずれかを使用して、個々のセッションをログオフできます。

vpn-sessiondb logoff name *name*

vpn-sessiondb logoff index *index*

たとえば、ユーザ tester をログオフさせるには、次のコマンドを入力します。

```
hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
hostname#
```

ユーザ名とインデックス番号（クライアント イメージの順序で設定される）は、両方とも **show vpn-sessiondb svc** コマンドの出力で確認できます。

次の例では、**vpn-sessiondb logoff** コマンドの **name** オプションを使用して、セッションを終了します。

```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

詳細な統計情報の表示

現在の AnyConnect セッションに関する統計情報を表示するには、ユーザの GUI の [詳細（Details）] ボタンをクリックします。

[統計情報詳細（Statistics Details）] ダイアログが表示されます。このウィンドウの [統計情報（Statistics）] タブでは、統計情報のリセットとエクスポート、およびトラブルシューティング用のファイル収集を行えます。

このウィンドウで使用できるオプションは、クライアント PC にロードされているパッケージによって異なります。オプションを使用できない場合は、そのオプションのボタンはアクティブにならず、ダイアログボックスのオプション名の横に [（未インストール）((Not Installed)）] というインジケータが表示されます。オプションは次のとおりです。

- [リセット（Reset）] をクリックすると、接続情報がゼロにリセットされます。AnyConnect による新しいデータの収集がすぐに開始されます。
- [エクスポート ...（Export Stats...）] をクリックすると、接続の統計情報がテキスト ファイルに保存され、あとから分析とデバッグを行えます。
- [トラブルシュート ...（Troubleshoot...）] をクリックすると、AnyConnect Diagnostics and Reporting Tool（DART）ウィザードが起動されます。このウィザードでは、指定したログ ファイルとクライアント接続の分析とデバッグに使用できる診断情報を結び付けます。DART パッケージについては、「DART を使用したトラブルシューティング情報の収集」（P.12-4）を参照してください。

VPN 接続の問題の解決

VPN 接続の問題を解決するために、以下の項を参照してください。

MTU サイズの調整

多くの家庭用エンド ユーザ終端装置（たとえば、ホーム ルータ）は、IP フラグメント（特に UDP）の作成またはアセンブリを適切に処理しません。DTLS は UDP ベースのプロトコルであるため、場合によっては MTU を小さくして、フラグメンテーションを防止する必要があります。MTU パラメータでは、クライアントと ASA にトンネルで転送するパケットの最大サイズが設定されます。VPN ユーザで大量のパケット損失が発生している場合、または Microsoft Outlook などのアプリケーションがトンネル経由で機能しない場合は、フラグメンテーションの問題が発生している可能性があります。ユーザまたはユーザのグループの MTU を減らすことで、問題が解決されることがあります。

AnyConnect が確立する SSL VPN 接続の最大転送ユニット サイズ（256 ～ 1406 バイト）を調整するには、次の手順に従ってください。

ステップ 1　ASDM インターフェイスで、[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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] の順に選択します。

[内部グループ ポリシーの編集（Edit Internal Group Policy）] ダイアログボックスが表示されます。

ステップ 2　[詳細（Advanced）] > [SSL VPN クライアント（SSL VPN Client）] の順に選択します。

ステップ 3　[継承（Inherit）] チェックボックスをオフにして、MTU フィールドで適切な値を指定します。

デフォルトのグループ ポリシーでは、このコマンドのデフォルトのサイズは 1406 です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

この設定が影響を与えるのは、SSL で確立された AnyConnect 接続と、DTLS を使用する SSL で確立された AnyConnect 接続のみです。

最適 MTU（OMTU）

最適 MTU（OMTU）機能を使用して、クライアントが DTLS パケットを正常に渡すことができる最大エンドポイント MTU を検出します。最大 MTU に埋め込まれた DPD パケットを送信することによって、OMTU を実装します。ヘッドエンドから戻されるペイロードの正しいエコーを受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

（注）　OMTU を使用しても、既存のトンネル DPD 機能を妨げることはありません。

この機能を使用するには、ASA で DPD を有効にする必要があります。DPD は、埋め込みが許可されない標準実装に基づくため、この機能は、IPsec とは併用できません。

DART を使用したトラブルシューティング情報の収集

DART は AnyConnect Diagnostics and Reporting Tool の略で、AnyConnect のインストールと接続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の収集に使用できます。DART は、Windows 7、Windows Vista、Windows XP、Mac バージョン 10.5 と 10.6、および Linux Redhat をサポートします。

DART ウィザードは、AnyConnect が稼働するコンピュータ上で実行されます。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。DART の実行に管理者権限は不要です。

DART は、AnyConnect ソフトウェアのコンポーネントに依存せずに機能しますが、AnyConnect から起動可能で、AnyConnect ログ ファイル（存在する場合）の収集を行います。

現在のところ、DART はスタンドアロン インストールを実行できます。または、管理者は AnyConnect ダイナミック ダウンロード インフラストラクチャの一部として、このアプリケーションをクライアント PC にプッシュできます。インストールされると、[スタート（Start）] ボタンにある Cisco フォルダから、DART ウィザードを起動できます。

DART ソフトウェアの入手

Web 展開方式または AnyConnect の事前展開方式のいずれかを使用して、DART をクライアントにインストールできます。

どのバージョンの DART も、すべてのバージョンの AnyConnect に使用できます。それぞれのバージョン番号は同期化されていません。

表 12-1 に、事前展開インストーラおよび Web 展開（ダウンロード）インストーラの DART を含む AnyConnect のダウンロード（ファイルとパッケージの両方）を示します。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 12-1　ASA または Pre-Deployment 用の DART ファイルまたはパッケージ ファイル名

DART	Web-Deploy ファイル名およびパッケージ（ダウンロード）	Pre-Deploy 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
	3.0.3050 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
Linux-64	*リリース 3.0.3050 以降：* anyconnect-linux-64-(ver)-k9.pkg	anyconnect-predeploy-linux-64-(ver)-k9.tar.gz
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.sh	anyconnect-dart-linux-64-(ver)-k9.tar.gz

Web 展開および事前展開のパッケージには、ISO イメージ（.iso）が含まれています。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。.iso イメージとその内容の詳細については、「事前展開パッケージ ファイル情報」（P.2-29）を参照してください。

DART のインストール

管理者は、DART を AnyConnect インストールの一部に含めることができます。

AnyConnect を AnyConnect で動作する PC にダウンロードしたときに、新しいバージョンの DART がある場合は、その DART とともにダウンロードされます。新しいバージョンの AnyConnect が自動アップグレードの一部としてダウンロードされるとき、新しいバージョンの DART がある場合は、それもダウンロードに含まれます。

（注）　グループ ポリシー設定（**svc modules** コマンドまたは対応する ASDM ダイアログで設定）に **dart** キーワードがない場合は、DART がパッケージに含まれていても、AnyConnect は DART をインストールしません。

AnyConnect を使用した DART のインストール

この手順では、次回リモート ユーザが接続するときに、そのユーザのマシンに DART がダウンロードされます。

ステップ 1　他のシスコのソフトウェア パッケージと同様に、DART を含む AnyConnect パッケージを ASA にロードします。

ステップ 2　DART を含む AnyConnect の .pkg ファイルをセキュリティ アプライアンスにインストール後、AnyConnect と一緒に DART をインストールするには、グループ ポリシーで DART を指定する必要があります。これは、次のように ASDM または CLI を使用して実行できます。

ASDM を使用する場合：

a.　[設定（Configuration）] をクリックしてから、[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）] > [グループ ポリシー（Group Policy）] の順にクリックします。

b.　新しいグループ ポリシーを追加するか、既存のグループ ポリシーを編集します。グループ ポリシーのダイアログボックスで、[詳細（Advanced）] を展開し、[SSL VPN クライアント（SSL VPN Client）] をクリックします。

c.　[SSL VPN クライアント（SSL VPN Client）] ダイアログボックスで、[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] オプションの [継承（Inherit）] をオフにします。このオプションのドロップダウン リストから **dart** モジュールを選択します。

d.　使用するバージョンの ASDM に、DART オプションのチェックボックスがない場合は、フィールドにキーワード **dart** を入力します。DART と Start Before Logon の両方をイネーブルにするには、**dart** と **vpngina** の両方を任意の順序でカンマで区切ってそのフィールドに入力します。

[OK] をクリックしてから、[適用（Apply）] をクリックします。

CLI を使用する場合は、**svc modules value dart** コマンドを使用します。

（注）　あとで **svc modules none** に変更したり、[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] フィールドの DART の選択を解除しても、DART はインストールされたままになります。セキュリティ アプライアンスによって、DART がアンインストールされることはありません。DART を削除するには、Windows のコントロール パネルの、[プログラムの追加/削除（Add/Remove Programs）] を使用してください。この方法で DART を削除しても、ユーザが AnyConnect を使用して再接続すると、自動的に再インストールされます。上位バージョンの DART を含んだ AnyConnect パッケージが ASA にアップロードされ、設定されている場合は、ユーザが接続すると DART が自動的にアップグレードされます。

DART の実行方法については、「Windows での DART の実行」（P.12-7）を参照してください。

Windows デバイスへの DART の手動インストール

Windows デバイスに DART 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　anyconnect-dart-win-(ver)-k9.msi をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-win-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　**anyconnect-dart-win-(ver)-k9.msi** ファイルをダブルクリックして、**DART セットアップ ウィザード** を起動します。

ステップ 3　初期画面で [次へ（Next）] をクリックします。

ステップ 4　[ライセンス契約条件に同意します（I accept the terms in the License Agreement）] を選択して、エンド ユーザのライセンス契約に同意し、[次へ（Next）] をクリックします。

ステップ 5　[インストール（Install）] をクリックして、DART をインストールします。インストール ウィザードによって、**DartOffline.exe** が <System Drive>:\Program Files\Cisco\Cisco DART ディレクトリにインストールされます。

ステップ 6　[完了（Finish）] をクリックして、インストールを完了します。

DART の実行方法については、「Windows での DART の実行」（P.12-7）を参照してください。

Linux デバイスへの DART の手動インストール

Linux デバイスに DART 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　anyconnect-dart-linux-(ver)-k9.tar.gz をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-linux-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　端末から、**tar -zxvf** <*path to tar.gz file including the file name*> コマンドを使用して tar.gz ファイルを抽出します。

ステップ 3　端末から、抽出したフォルダに移動し、**sudo ./dart_install.sh** コマンドを使用して dart_install.sh を実行します。

ステップ 4　ライセンス契約書に同意し、インストールが完了するまで待機します。

（注）　DART のアンインストールには、**/opt/cisco/anyconnect/dart/dart_uninstall.sh** しか使用できません。

Mac デバイスへの DART の手動インストール

Mac デバイスに DART 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　anyconnect-dart-macosx-i386-(ver)-k0.dmg をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-macosx-i386-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　ダウンロードが終了したら、.dmg ファイルは自動的にデスクトップにマウントされ、DART インストール ウィザードが自動的に開始します。インストール ウィザードを手動で開始するには、ダウンロード フォルダに移動し、ダウンロードされた .dmg ファイルをダブルクリックしてデスクトップにマウントします。その後、マウントされたデバイスで dart.pkg をダブルクリックします。

インストール ウィザードに、「This package will run a program to determine if the software can be installed」というメッセージが表示されます。

ステップ 3　[続行（Continue）] をクリックします。ウィザードにライセンス契約書が表示されます。

ステップ 4　[続行（Continue）] をクリックしてから、[承認（Accept）] をクリックし、ライセンス契約書に同意します。

ステップ 5　インストール場所を変更するように求められます。必要に応じて変更し、[続行（Continue）] をクリックします。

ステップ 6　開始するには、インストールの管理者クレデンシャルを入力する必要があります。クレデンシャルを入力したら、[続行（Continue）] をクリックします。インストールが開始されます。

ステップ 7　インストールが完了するまで待機し、[キャンセル（Cancel）] をクリックしてプログラムを終了します。

（注）　DART のアンインストールには、**/opt/cisco/anyconnect/bin/dart_uninstall.sh** しか使用できません。

Windows での DART の実行

Windows 用の DART ウィザードを実行して DART バンドルを作成するには、次の手順を実行します。

ステップ 1　Windows デバイスで実行している場合、AnyConnect GUI を起動します。

ステップ 2　[統計情報（Statistics）] タブをクリックしてから、ダイアログボックス下部の [詳細（Details）] ボタンをクリックします。[統計情報詳細（Statistics Details）] ダイアログボックスが表示されます。

ステップ 3　[統計情報詳細（Statistics Details）] ウィンドウ下部の [トラブルシュート（Troubleshoot）] をクリックします。

ステップ 4　初期画面で [次へ（Next）] をクリックします。[バンドルの作成オプション（Bundle Creation Option）] ダイアログボックスが表示されます。

ステップ 5　[バンドルの作成オプション（Bundle Creation Option）] エリアで、[デフォルト（Default）] または [カスタム（Custom）] を選択します。

- [デフォルト（Default）] オプションでは、代表的なログ ファイルと診断情報が含まれます。たとえば、AnyConnect ログ ファイルや Cisco Secure Desktop ログ ファイル、コンピュータの一般情報、DART が実行した内容と実行しなかった内容についての要約などが含まれます。

  [デフォルト（Default）] を選択してから、ダイアログボックス下部の [次へ（Next）] をクリックすると、DART のバンドル作成が開始されます。バンドルのデフォルト名は DARTBundle.zip で、ローカル デスクトップに保存されます。

- [カスタム（Custom）] を選択した場合は、[次へ（Next）] をクリックすると、DART ウィザードによってさらにダイアログボックスが表示され、バンドルに含めるファイルや、バンドルの保存場所を指定します。

ヒント　[カスタム（Custom）] を選択すると、バンドルに含めるファイルはデフォルトのままにして、ファイルの保存場所だけは別の場所を指定するということもできます。

ステップ 6　DART バンドルを暗号化するには、[暗号化オプション（Encryption Option）] エリアで [バンドル暗号化の有効化（Enable Bundle Encryption）] にチェックを入れてから、[暗号化パスワード（Encryption Password）] フィールドにパスワードを入力します。オプションで [パスワードのマスク（Mask Password）] を選択すると、[暗号化パスワード（Encryption Password）] フィールドおよび [パスワードの再入力（Reenter Password）] フィールドに入力したパスワードが、アスタリスク（*）でマスクされるようになります。

ステップ 7　[次へ（Next）] をクリックします。[デフォルト（Default）] を選択した場合、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合は、ウィザードが次のステップに進みます。

ステップ 8　[ログファイルの選択（Log File Selection）] ダイアログボックスで、バンドルに含めるログ ファイルと設定ファイルを選択します。ネットワーク アクセス マネージャ、テレメトリ、ポスチャ、および Web セキュリティの各ログを含めるオプションがあります。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 9　[診断情報の選択（Diagnostic Information Selection）] ダイアログボックスで、バンドルに含める診断情報を選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 10　[コメントとターゲットバンドルの場所（Comments and Target Bundle Location）] ダイアログボックスで、次のフィールドを設定します。

- [コメント（Comments）] エリアに、バンドルに含めるコメントを入力します。DART は、入力したコメントをバンドルに含める comments.txt ファイルに保存します。
- [ターゲットバンドルの場所（Target Bundle Location）] フィールドで、バンドルの保存場所を参照します。

[次へ（Next）] をクリックします。

ステップ 11　[サマリー（Summary）] ダイアログボックスでカスタマイズの内容を確認し、[次へ（Next）] をクリックしてバンドルを作成するか、[戻る（Back）] をクリックしてカスタマイズの内容に変更を加えます。

ステップ 12　DART のバンドル作成が終了したら、[完了（Finish）] をクリックします。

ヒント　状況によっては、DART の実行に数分以上かかったという報告を受けました。デフォルト リストのファイル収集に長い時間を要している思われる場合は、[キャンセル（Cancel）] をクリックしてからウィザードを再実行し、**カスタム** DART バンドルを作成して必要なファイルだけを選択してください。

Linux または Mac での DART の実行

Linux または Mac 用の DART ウィザードを実行して DART バンドルを作成するには、次の手順を実行します。

ステップ 1　Linux デバイスの場合、[アプリケーション（Applications）] > [インターネット（Internet）] > [Cisco DART] または /opt/cisco/anyconnect/dart/dartui から DART を起動します。

Mac デバイスの場合、[アプリケーション（Applications）] > [Cisco] > [Cisco DART] から DART を起動します。

ステップ 2　[統計情報（Statistics）] タブをクリックしてから、ダイアログボックス下部の [詳細（Details）] ボタンをクリックします。[統計情報詳細（Statistics Details）] ダイアログボックスが表示されます。

ステップ 3　[バンドルの作成オプション（Bundle Creation Option）] エリアで、[デフォルト（Default）] または [カスタム（Custom）] を選択します。

- [デフォルト（Default）] オプションでは、代表的なログ ファイルと診断情報が含まれます。たとえば、AnyConnect ログ ファイルや Cisco Secure Desktop ログ ファイル、コンピュータの一般情報、DART が実行した内容と実行しなかった内容についての要約などが含まれます。

  [デフォルト（Default）] を選択してから、ダイアログボックス下部の [次へ（Next）] をクリックすると、DART のバンドル作成が開始されます。バンドルのデフォルト名は DARTBundle.zip で、ローカル デスクトップに保存されます。

  （注）　MAC のオプションは、デフォルトのみです。バンドルに含めるファイルは、カスタマイズできません。

- [カスタム（Custom）] を選択した場合は、[次へ（Next）] をクリックすると、DART ウィザードによってさらにダイアログボックスが表示され、バンドルに含めるファイルや、バンドルの保存場所を指定します。

ヒント　[カスタム（Custom）] を選択すると、バンドルに含めるファイルはデフォルトのままにして、ファイルの保存場所だけは別の場所を指定するということもできます。

ステップ 4　[次へ（Next）] をクリックします。[デフォルト（Default）] を選択した場合、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合は、ウィザードが次のステップに進みます。

ステップ 5　[ログファイルの選択（Log File Selection）] ダイアログボックスで、バンドルに含めるログ ファイルと設定ファイルを選択します。ネットワーク アクセス マネージャ、テレメトリ、ポスチャ、および Web セキュリティの各ログを含めるオプションがあります。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 6　[診断情報の選択（Diagnostic Information Selection）] ダイアログボックスで、バンドルに含める診断情報を選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 7　[コメントとターゲットバンドルの場所（Comments and Target Bundle Location）] ダイアログボックスで、次のフィールドを設定します。

- [コメント（Comments）] エリアに、バンドルに含めるコメントを入力します。DART は、入力したコメントをバンドルに含める comments.txt ファイルに保存します。
- [ターゲットバンドルの場所（Target Bundle Location）] フィールドで、バンドルの保存場所を参照します。

[次へ（Next）] をクリックします。

ステップ 8　DART バンドルを暗号化するには、[暗号化オプション（Encryption Option）] エリアで [バンドル暗号化の有効化（Enable Bundle Encryption）] にチェックを入れてから、[暗号化パスワード（Encryption Password）] フィールドにパスワードを入力します。オプションで [パスワードのマスク（Mask Password）] を選択すると、[暗号化パスワード（Encryption Password）] フィールドおよび [パスワードの再入力（Reenter Password）] フィールドに入力したパスワードが、アスタリスク（*）でマスクされるようになります。

（注）　パスワードをマスクするオプションは、MAC オペレーティング システムでは使用できません。

ステップ 9　[完了（Finish）] をクリックしてウィザードを終了します。

ヒント　状況によっては、DART の実行に数分以上かかったという報告を受けました。デフォルト リストのファイル収集に長い時間を要している思われる場合は、[キャンセル（Cancel）] をクリックしてからウィザードを再実行し、**カスタム** DART バンドルを作成して必要なファイルだけを選択してください。

AnyConnect クライアントのインストール

svc image xyz コマンドを使用して AnyConnect イメージを設定する場合、**svc enable** コマンドを発行する必要があります。このコマンドを発行しないと、AnyConnect は想定したとおりに機能せず、**show webvpn svc** は、インストールされた AnyConnect パッケージをリストする代わりに、「SSL VPN client is not enabled」というメッセージを表示します。

ログ ファイルのインストール

ログ ファイルは、次のファイル内に保持されます。

- \Windows\setupapi.log：Windows XP および Windows 2000
- \Windows\Inf\setupapi.app.log：Windows Vista
- \Windows\Inf\setupapi.dev.log：Windows Vista

（注）　Vista では、隠しファイルを表示する必要があります。

レジストリ情報が setupapi.log ファイルから欠落している場合は、Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにしてください。Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにするには、次の手順に従ってください。

（注）　レジストリが誤って変更されると、重大な問題が発生する可能性があります。念のため、レジストリを変更する前に、レジストリをバックアップしてください。

ステップ 1　[スタート（Start）] > [実行（Run）] の順にクリックします。

ステップ 2　[オープン（Open）] フィールドに **regedit** と入力し、[OK] をクリックします。

ステップ 3　HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup レジストリ サブキーにある **LogLevel** を見つけてダブルクリックします。

ステップ 4　[DWORD 値の編集（Edit DWORD Value）] ウィンドウの [ベース（Base）] ペインで [16 進数（Hexadecimal）] を選択します。

ステップ 5　[値（Value）] データ ボックスに **0x2000FFFF** と入力します。

ステップ 6　[OK] をクリックします。

（注）　冗長ロギングをイネーブルにすると、Setupapi.log ファイルのサイズは約 4MB に増加します。レジストリ値をリセットするには、上記のステップを繰り返しますが、ステップ 5 で DWORD 値を 0 に設定してください。

ログ ファイルの Web インストール

これが新規の Web 展開インストールの場合、このログは次のユーザ別の temp ディレクトリに格納されます。

%TEMP%\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log

アップグレードが最適ゲートウェイからプッシュされた場合、ログ ファイルは次の場所にあります。

%WINDIR%\TEMP\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log

インストールするクライアントのバージョンの最新ファイルを取得します。*xxx* はバージョンによって異なり、**yyyyyyyyyyyyy** はインストールの日時を示します。

ログ ファイルのスタンドアロン インストール

MSI ロギングをオンにし、インストールのログをキャプチャするには、次のコマンドを実行します。

MSIExec.exe/i anyconnect-win-2.X.xxxx-pre-deploy-k9.msi/lvx* c:\AnyConnect.log

ここで、*anyconnect-win-2.X.xxxx-pre-deplay-k9.msi* は、インストールする実際の msi ファイルの完全な名前です。

ログは次の場所に表示されます。

- \Documents and Settings\<username>\Local Settings\Temp（Windows XP および Windows 2000）
- \Users\<username>\AppData\Local\Temp（Vista）
- \Windows\Temp（自動アップグレードの場合）

スタンドアロンのみを使用する（または、システムにインストールされている ActiveX コントロールを使用しない）場合、次のいずれかを実行します。

（注）　以下のアクションを実行しないと、Windows インストーラ パッケージに関する問題を示す Cisco AnyConnect VPN Error 1722 を受け取ることがあります。

- MSI トランスフォームを作成し、ActiveX プロパティをディセーブル（NOINSTALLACTIVEX=1）に設定する。

```
MISExec /i anyconnect-win-x.x.xxxx-pre-deploy-k9.msi NOINSTALLACTIVEX=1
```

- リブートせずに、次のコマンドを実行して Quiet Install を実行する。

```
msiexec /quiet /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi
```

- リブートせずに、次のコマンドを実行して Quiet Uninstall を実行する。

```
msiexec /quiet /x "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

（注）　*x.x.xxx* の値は、インストールされているバージョンによって異なります。

AnyConnect の接続解除または初期接続の確立に関する問題

AnyConnect クライアントの接続解除または初期接続の確立で問題が発生する場合は、以下の推奨事項に従ってください。

1. ASA からコンフィギュレーション ファイルを取得し、次のようにして接続失敗の兆候を探します。
   - ASA コンソールから **write net x.x.x.x:ASA-Config.txt** と入力します。この *x.x.x.x* はネットワーク上の TFTP サーバの IP アドレスです。
   - ASA コンソールから、**show running-config** と入力します。設定を切り取ってテキスト エディタに貼り付け、これを保存します。
2. ASA イベント ログを表示します。
   a. ASA コンソールで、以下の行を追加し、ssl、webvpn、svc、および auth のイベントを調べます。

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

   b. AnyConnect クライアントの接続を試行し、接続エラーが発生した場合は、そのコンソールのログ情報を切り取ってテキスト エディタに貼り付け、保存します。
   c. **no logging enable** と入力し、ロギングをディセーブルにします。
3. クライアント PC の Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。
   a. [スタート（Start）] > [実行（Run）] の順に選択し、**eventvwr.msc /s** と入力します。

b. アプリケーションおよびサービス ログ（Windows Vista および Windows 7 の）で、**Cisco AnyConnect VPN Client** を見つけ、[ログ ファイルの名前を付けて保存...（Save Log File As..）] を選択します。

c. AnyConnectClientLog.evt などのファイル名を割り当てます。.evt ファイル形式を使用する必要があります。

4. AnyConnect GUI を接続解除または終了する際に問題が発生する場合は、vpnagent.exe プロセスを Windows 診断デバッグ ユーティリティにアタッチします。詳細については、WinDbg のマニュアルを参照してください。

5. IPv6/IPv4 IP アドレスの割り当てに競合が確認された場合は、スニファ トレースを取得し、使用中のクライアント PC のレジストリにルーティング デバッグを追加します。このような競合は、AnyConnect イベント ログで次のように表示されます。

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

VPN 接続を確立する前に特定のレジストリ エントリ（Windows）またはファイル（Mac または Linux）を追加すると、ルート デバッグを 1 つの接続に対して 1 回だけイネーブルできます。

トンネル接続が開始され、このキーまたはファイルが検出されると、2 つのルート デバッグ テキスト ファイルがシステムの一時ディレクトリ（通常 Windows では C:\Windows\Temp、Mac または Linux では /tmp）に作成されます。2 つのファイル（debug_routechangesv4.txt4 と debug_routechangesv6.txt）がすでに存在する場合、これらのファイルは上書きされます。

トラフィックを渡す際の問題

いったん接続されたプライベート ネットワークに AnyConnect クライアントがデータを送信できない場合は、次の推奨事項に従ってください。

1. show vpn-sessiondb detail svc filter name <username> コマンドの出力を取得します。出力にフィルタ名 XXXXX が指定されている場合は、show access-list XXXXX コマンドの出力も取得してください。ACL によってトラフィック フローがブロックされていないか確認してください。

2. [AnyConnect VPN クライアント（AnyConnect VPN Client）] > [統計情報（Statistics）] > [詳細（Details）] > [エクスポート（Export）] の順に選択し、DART のファイルまたは出力（AnyConnect-ExportedStats.txt）を取得します。統計情報、インターフェイス、およびルーティング テーブルを調べます。

3. ASA コンフィギュレーション ファイルの NAT 文を確認します。NAT が有効になっている場合は、クライアントに返されるデータをネットワーク アドレス変換から除外する必要があります。たとえば、AnyConnect プールから IP アドレスを NAT 除外するには、次のコードが使用されます。

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. トンネリングされたデフォルト ゲートウェイがその設定に対して有効になっているかどうかを確認してください。従来型のデフォルト ゲートウェイは、次のように非暗号化トラフィックのラスト リゾート ゲートウェイです。

```
route outside 0.0.83.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

VPN クライアントが、VPN ゲートウェイのルーティング テーブルに存在しないリソースにアクセスする必要がある場合、パケットは標準デフォルト ゲートウェイによってルーティングされます。VPN ゲートウェイは、完全な内部ルーティング テーブルを必要としません。トンネリングされたキーワードを使用する場合、IPsec または SSL の VPN 接続から受信した復号化トラフィックはルーティングによって処理されます。VPN ルートから受信したトラフィックは 10.0.4.2 にルーティングされて復号化されますが、標準トラフィックは最終的に 83.145.50.1 にルーティングされます。

5. AnyConnect でトンネルを確立する前後の、ipconfig /all のテキスト ダンプおよび route print の出力を収集します。
6. クライアントでネットワーク パケットキャプチャを実行するか、ASA のキャプチャをイネーブルにします。

（注） 一部のアプリケーション（Microsoft Outlook など）がトンネルで動作しない場合、受け入れられるサイズを確認するために、一定の基準に従って大きくした ping（たとえば、ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000）を使用して、ネットワーク内の既知のデバイスに ping します。ping の結果から、ネットワークにフラグメンテーションの問題が発生しているかがわかります。その後、フラグメンテーションが発生していると思われるユーザの特別なグループを設定して、このグループの svc mtu を 1200 に設定できます。また、古い IPsec クライアントから Set MTU.exe ユーティリティをコピーして、物理アダプタの MTU を強制的に 1300 に設定できます。リブート時に、違いがあるかどうか確認してください。

AnyConnect のクラッシュに関する問題

UI のクラッシュが発生した場合、結果は %temp% ディレクトリ（C:\DOCUME~1\jsmith\LOCALS~1\Temp など）に書き込まれます。リブート後に「The System has recovered from a serious error」というメッセージが表示される場合は、C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson または同様のアプリケーションから生成された .log ファイルおよび .dmp ファイルを収集します。これらのファイルをコピーするか、以下の手順に従ってファイルをバックアップしてください。

ステップ 1　[スタート（Start）] > [実行（Run）] メニューから ワトソン博士（Drwtsn32.exe）という Microsoft ユーティリティを実行します。

ステップ 2　次のように設定し、[OK] をクリックします。

```
Number of Instructions : 25
Number of Errors to Save : 25
Crash Dump Type : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

ステップ 3　クライアント PC で [スタート（Start）] > [実行（Run）] メニューの順に選択し、**eventvwr.msc /s** と入力して、Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。

ステップ 4　（Windows Vista および Windows 7 の）[アプリケーションとサービス ログ（Applications and Services Logs）] で **Cisco AnyConnect VPN Client** を見つけ、[ログ ファイルの名前を付けて保存 ...（Save Log File As..）] を選択します。AnyConnectClientLog.evt などのファイル名を .evt ファイル形式で割り当ててください。

ステップ 5　ドライバ クラッシュが VPNVA.sys で発生する場合は、Cisco VPNVA 仮想アダプタにバインドされた中間ドライバを確認し、それらをオフにします。

ステップ 6　ドライバ クラッシュが vpnagent.exe で発生する場合は、vpnagent.exe プロセスを Windows のデバッグ ツールにアタッチします。ツールがインストールされた後、次の手順を実行します。

a. c:\vpnagent という名前のディレクトリを作成します。

b. タスク マネージャの [プロセス（Process）] タブを調べ、vpnagent.exe のプロセスの PID を判別します。

c. コマンド プロンプトを開き、デバッグ ツールをインストールしたディレクトリに移動します。デフォルトでは、Windows のデバッグ ツールは C:\Program Files\Debugging Tools にあります。

d. **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst** と入力します。この *PID* は、ステップ b で判別した番号です。

オープン ウィンドウを最小化した状態で実行します。モニタリングしている間は、システムをログオフできません。

e. クラッシュが発生すると、c:\vpnagent の中身を zip ファイルに収集します。

f. **!analyze -v** を使用して、crashdmp ファイルをさらに診断します。

VPN サービスへの接続に関する問題

「Unable to Proceed, Cannot Connect to the VPN Service」というメッセージが表示される場合、AnyConnect の VPN サービスは実行されていません。VPN エージェントが予期せず終了した可能性があります。別のアプリケーションがサービスと競合したかどうかにかかわらず、トラブルシューティングするには、次の手順を実行します。

ステップ 1　Windows 管理ツールでサービスを確認して、Cisco AnyConnect VPN エージェントが動作**していない**か確認します。このエージェントが動作している場合、またはエラー メッセージが引き続き表示される場合は、ワークステーション上の別の VPN アプリケーションをディセーブルにする必要があります。また、このアプリケーションのアンインストール、リブート、または再テストが必要になる場合があります。

ステップ 2　Cisco AnyConnect VPN エージェントを起動してみます。こうすることで、起動時にサーバの初期化または別の実行中のサービス（サービスの起動に失敗したため）と競合しているかどうかを判断します。

ステップ 3　イベント ビューアの AnyConnect ログに、サービスを起動できなかったこと示すメッセージがないか確認します。手順 2 での手動による再起動のタイム スタンプおよびワークステーションが起動した時間に注目します。

ステップ 4　イベント ビューアのシステム ログおよびアプリケーション ログに、競合メッセージの同一の一般的なタイム スタンプがないかを確認します。

ステップ 5　サービスの起動に失敗したことをログが示している場合、同一のタイム スタンプの前後にある、次のいずれかを示すその他の情報メッセージを探します。

- 欠落したファイル：欠落したファイルを除外するには、AnyConnect クライアントをスタンドアロン MSI インストールから再インストールします。
- 別の依存するサービスでの遅延：起動アクティビティをディセーブルにして、ワークステーションのブート時間を短縮します。

- 別のアプリケーションまたはサービスとの競合：別のサービスが、vpnagent が使用するポートと同じポート上で受信していないか、または一部の HIDS ソフトウェアによって、シスコのソフトウェアがポート上で受信できなくなっているかどうかを判別します。

ログに原因が直接示されていない場合は、試行錯誤的な方法で競合を識別してください。最も可能性の高い候補を識別したら、[サービス（Services）] パネルから該当するサービス（VPN 製品、HIDS ソフトウェア、spybot クリーナ、スニファ、アンチウイルス ソフトウェアなど）をディセーブルにします。リブート後も VPN エージェント サービスが起動に失敗する場合は、オペレーティング システムのデフォルト インストールでインストールされなかったサービスをオフにします。

PC のシステム情報の取得

PC のシステム情報を取得するには、次のコマンドを入力し、約 2 分間待機します。

- **winmsd /nfo c:\msinfo.nfo**：Windows XP または Windows 2000
- **msinfo32 /nfo c:\msinfo.nfo**：Windows Vista

Systeminfo ファイル ダンプの取得

Windows XP または Vista の場合、コマンド プロンプトに次を入力し、Systeminfo ファイル ダンプを取得します。

systeminfo >> c:\sysinfo.txt

レジストリ ファイルの確認

次の SetupAPI ログ ファイル内のエントリは、ファイルが見つからないことを示しています。

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce レジストリ キーが存在することを確認してください。このレジストリ キーが存在しない場合、すべての inf インストール パッケージが禁止されます。

サードパーティ製アプリケーションとの競合

一部のサードパーティ製アプリケーションでは、AnyConnect 仮想アダプタ ドライバのインストールが禁止されます。この場合、画面がブルー スクリーンになり、ルーティング テーブルを更新できなくなることがあります。DART ツール（「DART を使用したトラブルシューティング情報の収集」（P.12-4）を参照）を使用して、お客様のオペレーティング システム環境に関する情報を収集できます。この診断に基づいて、シスコは次のサードパーティ製アプリケーションとの競合を識別し、解決策を推奨することができます。

Adobe および Apple：Bonjour Printing Service

- Adobe Creative Suite 3
- BonJour Print Service

- iTunes

症状　IP 転送テーブルを正常に検証できない。

考えられる原因　AnyConnect イベント ログは、IP 転送テーブルの識別に失敗したことを示し、ルーティング テーブル内の次のエントリを示しています。

```
Destination 169.254.0.0
Netmask 255.255.0.0
Gateway 10.64.128.162
Interface 10.64.128.162
Metric 29
```

推奨処置　コマンド プロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service をディセーブルにします。mDNSResponder の新しいバージョン（1.0.5.11）が Apple から提供されています。この問題を解決するために、Bonjour の新しいバージョンが iTunes にバンドルされ、個別のダウンロードとして Apple の Web サイトで配布されています。

AT&T Communications Manager バージョン 6.2 および 6.7

症状　一部の PC に AT&T Sierra Wireless 875 カードを装着すると、接続に失敗したり、トラフィックが通過できなくなったりする。バージョン 6.2 ～ 6.7 が AnyConnect と競合していると思われる。

考えられる原因　CSTP 転送障害は、AnyConnect 仮想アダプタによってトランスポート層に障害が発生していることを示します。

推奨処置　この問題を解決するには、次の手順を実行します。

1. Aircard でアクセラレーションをディセーブルにします。
2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
3. **manual** と入力します。
4. [停止（Stop）] をクリックします。

AT&T Global Dialer

症状　クライアントのオペレーティング システムでブルー スクリーンが発生し、ミニ ダンプ ファイルが生成されることがある。

考えられる原因　AT&T Dialer の中間ドライバが保留パケットを適切に処理できず、これがオペレーティング システムのクラッシュの原因となっています。他の NIC カード ドライバ（Broadcom など）では、この問題は発生していません。

推奨処置　AT&T Global Network Client を最新の 7.6.2 にアップグレードしてください。

Citrix Advanced Gateway Client バージョン 2.2.1

症状　AnyConnect セッションを接続解除するときに、次のようなエラーが発生する。

```
VPN Agent Service has encountered a problem and needs to close. We are sorry for
the inconvenience.
```

考えられる原因　メモリを解放するときに、Winsock を使用して Citrix CtxLsp.dll がすべてのプロセスにロードされるため、クラッシュが発生します。

推奨処置　CtxLsp.dll に関するこの問題が解決されるまで、Citrix Advanced Gateway Client を削除してください。

ファイアウォールとの競合

サードパーティ製のファイアウォールが、ASA グループ ポリシーで設定されたファイアウォール機能と干渉する可能性があります。

Juniper Odyssey Client

症状　ワイヤレス サプレッションが有効のときに有線接続を導入すると、無線接続がドロップする。ワイヤレス サプレッションがディセーブルのとき、ワイヤレス機能は期待どおりに動作する。

考えられる原因　Odyssey Client がネットワーク アダプタを管理していません。

推奨処置　次の手順に従って、Odyssey Client を設定します。

1. [ネットワーク接続（Network Connections）] で、アダプタの名前を接続プロパティの表示どおりにコピーします。レジストリを編集する場合、誤って変更すると重大な問題が発生する可能性があるため、バックアップを実行してから、細心の注意を払って変更してください。
2. レジストリを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual に移動します。
3. virtual の下に新しい文字列値を作成します。アダプタの名前をネットワーク プロパティからレジストリ部分にコピーします。追加のレジストリ設定を保存すると、MSI が作成されて他のクライアントにプッシュされたときに、この設定が移植されます。

Kaspersky AV Workstation 6.x

症状　Kaspersky 6.0.3 がインストールされると（ディセーブルであっても）、CSTP state = CONNECTED の直後に ASA への AnyConnect 接続が失敗する。次のメッセージが表示されます。

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure
gateway (proxy authentication, handshake, bad cert, etc.).
```

考えられる原因　Kaspersky AV Workstation 6.x と AnyConnect の間に既知の非互換性が存在します。

推奨処置　Kaspersky をアンインストールし、Kaspersky のフォーラムを参照して追加のアップデートがないか確認してください。

McAfee Firewall 5

症状　UDP DTLS 接続を確立できない。

考えられる原因　McAfee Firewall は、デフォルトで受信 IP フラグメントをブロックするため、フラグメント化されている場合、DTLS はブロックされます。

推奨処置　McAfee Firewall のセンター コンソールで、[高度なタスク（Advanced Tasks）] > [高度なオプションとロギング（Advanced options and Logging）] を選択し、McAfee Firewall の [Block incoming fragments automatically] チェックボックスをオフにします。

Microsoft Internet Explorer 8

症状　Internet Explorer 8 を Windows XP SP3 で使用する場合、AnyConnect を WebVPN ポータルからインストールできない。

考えられる原因　ブラウザがインストールでクラッシュします。

推奨処置　Microsoft の推奨策に従って、MSJVM を削除してください。Microsoft のサポート技術情報 KB826878 を参照してください。

Microsoft Routing and Remote Access Server

症状　AnyConnect がホスト デバイスへの接続の確立を試行するときに、次の終了エラーがイベントログに返されます。

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco
AnyConnect VPN Client.
```

考えられる原因　ルーティング テーブル上で RRAS と AnyConnect が競合しています。RRAS では、PC はイーサネット ルータとして機能するので、AnyConnect と同様にルーティング テーブルが変更されます。AnyConnect はトラフィックを適切に転送するためにルーティング テーブルに依存するので、この 2 つを一緒に実行できません。

推奨処置　RRAS サービスをディセーブルにします。

Microsoft Windows の更新プログラム

症状　VPN 接続の確立を試行すると、次のメッセージが表示される。

```
The VPN client driver has encountered an error.
```

考えられる原因　最近、certclass.inf ファイルに Microsoft 更新プログラムが適用されました。次のエラーが C:\WINDOWS\setupapi.log に表示されます。

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or
invalid. Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject
to driver signing policy.
```

推奨処置　コマンド プロンプトで **C:\>systeminfo** と入力するか、C:\WINDOWS\WindowsUpdate.log を確認して、最近インストールされた更新プログラムを確認してください。修復を試行するには、次の手順を実行します。

1. コマンド プロンプトを管理者として開きます。
2. **net stop CryptSvc** と入力します。
3. **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** と入力してデータベースを分析し、そのデータベースの妥当性を検証するか、%/WINDIR%\system32\catroot2 ディレクトリの名前を catroot2_old に変更します。
4. プロンプトが表示されたら、[OK] を選択して修復を試行します。コマンド プロンプトを終了し、リブートします。

上記の手順を実行すると、カタログが破損していないことが示される場合がありますが、キー ファイルが無署名のもので上書きされた可能性があります。障害が解消されない場合は、ドライバ署名のデータベースの破損原因を特定するために Microsoft に依頼してケースをオープンしてください。

Windows XP（Service Pack 3）

症状　AnyConnect クライアントをインストールできない。次のエラー メッセージが表示されます。

```
This application has failed to start because dot3api.dll was not found.
Re-installing the application may fix this problem.
```

考えられる原因　dot3api.dll ファイルが欠落することは、既知の問題です。

推奨処置　regsvr32 dot3api.dll を再インストールし、オペレーティング システムをリブートします。

OpenVPN クライアント

症状　このバージョンの TUN がこのシステムにすでにインストールされていて、AnyConnect クライアントと互換性がないことを示すエラーが表示される。

考えられる原因　MAC OS X Shimo VPN Client は、この問題を引き起こす可能性があります。

推奨処置　Viscosity OpenVPN Client をアンインストールします。

ロード バランサ

症状　クレデンシャルがないために、接続が失敗する。

考えられる原因　ブラウザが DNS 結果をキャッシュしていても、ポート転送やスマート トンネルなどの追加アプリケーションが DNS 結果をキャッシュしないことがあります。ユーザが X.4 にログインした後、DNS リゾルバが x.15 を使用するように設定されている場合、PF アプレットまたはスマート トンネル アプリケーションは DNS を解決して X.15 に接続します。セッションが確立されていないので、クレデンシャルがないことが原因で接続が失敗します。

推奨処置　サードパーティ製ロード バランサでは、ASA デバイスにかかる負荷を把握できません。ASA のロード バランシング機能は非常にインテリジェントで、VPN の負荷をデバイス全体で均等に分散できるため、ASA 内蔵のロード バランシングを使用することをお勧めします。

Ubuntu 8.04 i386

症状　Ubuntu バージョン 8.04 を使用すると、AnyConnect クライアントが ASA への接続確立に失敗する。VPN クライアント エージェント SSL エンジンでエラーが発生したことがエラー メッセージに示される。

考えられる原因　バージョン 7.04 と 8.04 とで、NSS ライブラリ エクステンションが変更されているため、AnyConnect クライアントは Network Security Service ライブラリを検出できません。

推奨処置　次のスクリプトを使用して NSS ライブラリのリンクを修正してください。

```
#!/bin/sh
if [ `id | sed -e `s/(.*//' ` != "uid=0" ]; then
    echo "Sorry, you need super user privileges to run this script.
    exit 1
fi
echo Creating Firefox NSS compatible symlinks...
ln -s /usr/lib/libnspr4.so.0d /usr/lib/libnspr4.so || exit 1
ln -s /usr/lib/libnss3.so.1d /usr/lib/libnss3.so || exit 1
ln -s /usr/lib/libplc4.so.0d /usr/lib/libplc4.so || exit 1
ln -s /usr/lib/libsmime3/so/1d /usr/lib/libsmime3.so || exit 1
echo "Success!"
```

また、AnyConnect で Ubuntu 64 ビットを使用可能にするための解説が Ubuntu フォーラムにないか確認することもできます。

Wave EMBASSY Trust Suite

症状　AnyConnect クライアントがダウンロードに失敗し、次のエラー メッセージが表示される。

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to
close."
```

考えられる原因　mdmp ファイルを収集している場合は、クラッシュ mdmp ファイルをデコードすると、サードパーティ製 dll が存在することが示されます。

推奨処置　dll の問題をすべて解決するために、パッチ アップデートをバージョン 1.2.1.38 に更新してください。

Layered Service Provider（LSP）モジュールおよび NOD32 AV

症状　AnyConnect が接続の確立を試行するときに、認証および SSL セッションの構築は正常に行われるが、AnyConnect クライアントが vpndownloader でクラッシュする。

考えられる原因　LSP コンポーネントの imon.dll に非互換性問題があります。

推奨処置　ESET NOD32 AV のバージョン 2.7 で Internet Monitor コンポーネントを削除し、バージョン 3.0 にアップグレードしてください。

LSP の症状 2：競合

症状　クライアント上に LSP モジュールが存在する場合、Winsock カタログが競合することがあります。

考えられる原因　impbw.dll などの Intel モバイル帯域幅の LSP モジュールによって、Intel コードで障害が発生した可能性があります。

推奨処置　LSP モジュールをアンインストールしてください。

LSP のデータ スループット低下症状 3：競合

症状　NOD32 V4.0 を使用すると、データ スループットが低下することがあります。

考えられる原因　この競合は、Windows 7 で Cisco AnyConnect と NOD32 アンチウイルス 4.0.468 x64 を使用したときに発生します。

推奨処置　[プロトコル フィルタリング（Protocol Filtering）] > [詳細設定（Advanced Setup）] の [SSL] を選択し、SSL プロトコル スキャンをイネーブルにします。次に、[Web アクセス保護（Web access protectio）] > [HTTP, HTTPS] の順に選択し、[HTTPS プロトコル チェックを使用しない（Do not use HTTPS protocol checking）] をオンにします。設定がイネーブルになったら、[プロトコル フィルタリング（Protocol filtering）] > [SSL] に戻り、[SSL プロトコル スキャン（SSL protocol scanning）] スキャンをディセーブルにします。

EVDO ワイヤレ スカードおよび Venturi ドライバ

症状　クライアントが接続解除され、イベント ログに次のようなメッセージが生成される。

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing
connection: DPD failure.
```

考えられる原因　アプリケーション、システム、および AnyConnect の各イベント ログに関係する接続解除イベントがないか確認すると同時に、NIC カードのリセットが適用されたかどうか判別してください。

推奨処置　Venturi ドライバが最新のものであるか確認してください。AT&T Communications Manager バージョン 6.7 の [ルール エンジンの使用（Use Rules Engine）] をディセーブルにします。

DSL ルータがネゴシエーションに失敗する

症状　DTLS トラフィックが正常にネゴシエーションされたが、DTLS トラフィックに障害が発生した。

考えられる原因　DSL ルータがリターン DTLS トラフィックをブロックしていました。エアー リンク上の設定により、安定した DTLS 接続が許可されません。

推奨処置　工場出荷時の設定で Linksys ルータに接続すると、安定した DTLS セッションが許可され、ping が中断されません。DTLS リターン トラフィックを許可するルールを追加してください。

チェックポイント（および Kaspersky などの他のサードパーティ製ソフトウェア）

症状　AnyConnect ログに、セキュア ゲートウェイへの接続を完全に確立できなかったことが示される。

考えられる原因　クライアント ログに、NETINTERFACE_ERROR_INTERFACE_NOT_AVAILABLE が複数発生したことが示されています。これらのエラーは、セキュア ゲートウェイへの SSL 接続の確立に使用する PC のネットワーク インターフェイス上でクライアントがオペレーティング システム情報を取得しようとしているときに発生します。

推奨処置　整合性エージェントをアンインストールしてから AnyConnect をインストールする場合は、TCP/IP をイネーブルにしてください。整合性エージェントのインストール時に SmartDefense をディセーブルにすると、TCP/IP がチェックされます。サードパーティ製のソフトウェアがネットワーク インターフェイス情報の取得中に、オペレーティング システムの API コールを代行受信またはブロックしている場合は、疑わしい AV、FW、AS などがないか確認してください。デバイス マネージャに AnyConnect アダプタのインスタンスが 1 つだけ表示されていることを確認してください。インスタンスが 1 つだけの場合は、AnyConnect で認証し、5 秒後にデバイス マネージャからアダプタを手動でイネーブルにしてください。疑わしいドライバが AnyConnect アダプタ内でイネーブルにされている場合は、これらのドライバを [Cisco AnyConnect VPN Client Connection] ウィンドウでオフにしてディセーブルにしてください。

Virtual Machine Network Service ドライバでのパフォーマンス問題

症状　一部のクライアント PC で AnyConnect を使用すると、パフォーマンスの問題が発生した。

考えられる原因　仮想マシン ネットワーク ドライバは物理的なネットワーク カードまたは接続を仮想化します。Cisco AnyConnect VPN クライアント接続ネットワーク アダプタに他の仮想マシン ネットワーク サービスをバインドしたときに、パフォーマンス問題が発生しています。クライアント デバイスが何らかのマルウェアに感染し、SSL_write () の周囲で遅延が発生しました。

推奨処置　AnyConnect 仮想アダプタ内のすべての IM デバイスに対するバインドをオフにしてください。アプリケーション dsagent.exe は、C:\Windows\System\dgagent にあります。これはプロセス リストに表示されませんが、TCPview（sysinternals）でソケットを開くと表示できます。このプロセスを終了すると、AnyConnect が正常に動作します。

Kaspersky AntiVirus およびテレメトリ モジュール

症状　テレメトリ モジュールがインストールされている場合、AnyConnect は Kaspersky AntiVirus 8 スイート（avp.exe）のメイン実行可能ファイルを削除する場合があります。

考えられる原因　AnyConnect 3.0.5080 以降を備える 64 ビットでドイツ語の Windows 7 と Kaspersky AV 8 を使用すると、競合の原因となります。

推奨処置　テレメトリ モジュールを取り外します。

CHAPTER 13

モバイル デバイス向け AnyConnect の管理

この章では、デバイス情報、設定情報、サポート情報、Apple iOS および Android デバイス向けの AnyConnect 3.0 に固有の他の管理タスクを提供します。

Apple iOS デバイスの AnyConnect

サポートされる Apple iOS デバイス

デバイス	必要な Apple iOS リリース
iPad 2	6.0 以降
iPad（第 3 世代）	6.0 以降
iPad（第 4 世代）	6.0 以降
iPad mini	6.0 以降
iPhone 3GS	6.0 以降
iPhone 4	6.0 以降
iPhone 4S	6.0 以降
iPhone 5	6.0 以降
iPhone 5C	7.0 以降
iPhone 5S	7.0 以降

デバイス	必要な Apple iOS リリース
iPod Touch（第 4 世代）	6.0 以降
iPod Touch（第 5 世代）	6.0 以降

（注）　AnyConnect は、iPhone 上の場合と同じように iPod Touch 上に表示され、動作します。このデバイスには、『*iPhone User Guide for Cisco AnyConnect Secure Mobility Client*』を使用してください。

Apple iOS デバイスでサポートされている AnyConnect 機能

次の AnyConnect 機能では、Apple iOS 向け AnyConnect 3.0.x でサポートされます。

- トンネル プロトコル
  - Cisco SSL Tunneling Protocol（CSTP）
  - Cisco DTLS Tunneling Protocol（CDTP）
  - IPsec IKEv2
- SSL 暗号スイート
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS の暗号スイート
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - DES-CBC-SHA
- Suite B（IPSec のみ）
- FIPS 140-2 レベル 1
- 認証
- クライアント証明書認証
- 自動再接続（自動再接続プロファイルの指定にかかわらず、ユーザが携帯電話と WiFi ネットワークの間を移動するときに、AnyConnect Mobile は VPN を常に維持する）
- ルーティングポリシー
  - Tunnel All
  - Split Include
  - Split Exclude
- キー再生成

- ネットワーク ローミング
- TLS 圧縮
- Cisco プロファイルのサポート
- プロファイルの更新
- IPv6 over IPv4
- ログイン後バナー
- デッド ピア検出
- トンネル キープアライブ
- バックアップ サーバ リスト
- デフォルト ドメイン
- クラスタのサポート
- DNS サーバ設定
- プライベート側プロキシ サポート
- ネットワーク変更のモニタリング
- 統計情報（Statistics）
- グラフィカル ユーザ インターフェイス
- ログイン前バナー
- Certificate Enrollment Protocol（SCEP）を保護します。
- SCEP プロキシ
- Certificate Management
  - クライアント インターフェイスまたは URI のコマンドを使用して証明書をインポートします。
  - デバイスの証明書をすべて削除します。
- オンデマンド接続（オンデマンドで Apple iOS Connect と互換性がある）
- モバイル ポスチャ
- ローカリゼーション

Apple iOS デバイスの AnyConnect のインストールおよびアップグレード

エンド ユーザは、Apple App Store にアクセスし、アプリケーションをダウンロードすることによって他の iPad、iPhone または iPod touch のアプリケーションなどの Apple iOS デバイス向け AnyConnect セキュア モビリティ クライアントをインストールまたはアップグレードします。AnyConnect クライアント アプリケーションは無料です。詳細なインストール手順については、iPhone または iPad の AnyConnect ユーザ ガイドを参照してください。

Apple iOS デバイスの AnyConnect UI

AnyConnect アプリケーション、ユーザ インターフェイスおよびアプリケーションで実行されたすべてのアクティビティの説明は、iPhone または iPad の AnyConnect ユーザ ガイドを参照してください。

Apple iOS 固有の注意事項

Apple iOS デバイスの AnyConnect をサポートする際には、次の事項に考慮します。

- このマニュアルの SCEP の参照は、Apple iOS SCEP ではなく、AnyConnect SCEP にのみ適用されます。
- Apple iOS に制約があるため、プッシュ電子メール通知は VPN では動作しません。ただし、AnyConnect は、トンネル ポリシーがこれらをセッションから除外する際に、外部にアクセスできる ActiveSync 接続と平行して作動します。

Connect On Demand 機能の使用

Apple iOS Connect On Demand 機能は、ユーザが該当するドメイン リストで指定されたホスト名で任意の宛先にアクセスしようとする場合に VPN 接続を開始します。たとえば、ユーザが internal.example.com に移動し *.example.com が Always Connect リストに存在する場合、デバイスが現在どのネットワーク接続されていても、クライアントは VPN 接続を開始します。

Apple は、iOS 6 の Connect On Demand 機能に Trusted Network Detection（TND）の拡張機能を導入しました。この機能拡張は次のとおりです。

- ユーザが信頼ネットワーク内にいるかどうかを判断して、Connect on Demand 機能を拡張します。
- Wi-Fi 接続だけに適用されます。他のタイプのネットワーク接続に動作している場合、Connect on Demand は、VPN が接続するかどうかを判断するために TND を使用しません。
- 個々の機能はなく、Connect On Demand 機能の外で設定または使用できません。

iOS 6 の Connect on Demand Trusted Network Detection に関する情報は、Apple にお問い合わせください。

（注）　iOS 6 以前のリリースは、信頼ネットワークと非信頼ネットワーク間の識別をサポートしていません。

Connect on Demand の設定に関する注意事項

- 設定された Connect on Demand があるモバイル デバイス用に、証明書ベースの認証トンネル グループに短時間（60 秒）のアイドル タイムアウト（vpn-idle-timeout）が必要です。VPN セッションがアプリケーションにとって重大な問題がなく、常時接続が必要ではない場合は、アイドル タイムアウトを短く設定します。デバイスがスリープ モードに移行するなど必要でなくなった場合、Apple デバイスは VPN 接続を閉じます。トンネル グループのデフォルト アイドル タイムアウトは 60 分です。
- 規則を設定する場合は、[必要に応じて接続（Connect if Needed）] オプションを指定することをお勧めします。Connect if Needed 規則は、内部ホストへの DNS ルックアップに失敗した場合に VPN 接続を開始します。企業内のホスト名が内部 DNS サーバを使用してのみ解決されるよう、正しく DNS を構成する必要があります。
- Apple iOS 7 は、[*常に接続（Always Connect）*] ドメインをサポートしません。Apple iOS 7 デバイスの AnyConnect を実行すると、[*常に接続（Always Connect）*] としてリストアップされているデバイスは、[*必要に応じて接続（Connect if Needed）*] ドメインとして取り扱われます。

詳細な設定手順および機能情報については、「Apple iOS Connect On Demand」を参照してください。

スプリット トンネルによるスプリット DNS 解決の動作

ASA スプリット トンネリング機能では、VPN トンネルにアクセスするトラフィックや、クリア テキストで送信されるトラフィックを指定することができます。スプリット DNS と呼ばれる関連機能は、VPN トンネル上の DNS 解決のために適切な DNS トラフィックや、エンドポイント DNS リゾルバが処理する DNS トラフィックを指定することができます。

Apple iOS 向け AnyConnect は、任意の **split-dns** コマンドをサポートし、解決のために DNS クエリーを指定します。しかし、スプリット トンネル VPN も設定する場合、コマンドは他のデバイスでの働きとは異なる働きをします。

グループ ポリシー コンフィギュレーション モードで入力する **split-dns** コマンドは、VPN セッションを介して解決されるドメインを次のようにリストにまとめます。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2 ...
domain-nameN] | none}
```

split-dns コマンドがない場合、グループ ポリシーはデフォルトのグループ ポリシー内に存在するスプリット トンネル ドメイン リストを継承します。スプリット トンネリング ドメインのリストの継承を防ぐためには、**split-dns none** コマンドを使用します。

Apple iOS 向け AnyConnect は、このコマンドには次のように応答します:

- **split-dns** リストのドメインに対して、DNS クエリーだけを暗号化します AnyConnect は、コマンドで指定されたドメインの DNS クエリーだけをトンネルし、ローカル DNS リゾルバに他の DNS クエリーすべてをクリア テキストで送信します。たとえば、AnyConnect は次のコマンドに対して example1.com および example2.com の DNS クエリーのみトンネルします。

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```

- **default-domain** コマンドのドメインに対して、DNS クエリーだけを暗号化します。**split-dns none** コマンドが存在し、**default-domain** コマンドがドメインを指定する場合、AnyConnect はこのドメインに DNS クエリーだけをトンネルし、他の DNS クエリーすべてをローカル DNS リゾルバにクリア テキストで送信します。たとえば、AnyConnect は次のコマンドに対して example1.com の DNS クエリーのみトンネルします。

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```

- すべての DNS クエリーはクリア テキストで送信されます。グループ ポリシーに **split-dns none** と **default-domain none** コマンドが存在する場合、またはこれらコマンドがグループ ポリシーにはないが、デフォルトのグループ ポリシーに存在する場合、AnyConnect は他の DNS クエリーすべてをローカル DNS リゾルバにクリア テキストで送信します。

Apple iPhone Configuration Utility

Apple for Windows または Mac OS X から入手できる iPhone Configuration Utility（IPCU）を使用して、Apple iOS デバイスの設定を作成および展開できます。これは、セキュア ゲートウェイの AnyConnect XML クライアント プロファイル設定の代わりになります。

Apple で制御される既存の IPCU GUI は、AnyConnect IPsec 機能を認識しません。[サーバ（Server）] フィールドで RFC 2996 で定義されている次の URI 構文を使用することで、IPCU の既存 AnyConnect GUI で IPsec VPN 接続を設定します。

```
[ipsec://][<AUTHENTICATION>[":"<IKE-IDENTITY>"@"]] <HOST>[":"<PORT>]["/"<GROUP-URL>]
```

（注）　このサーバ フィールドの構文は SSL VPN 接続設定のドキュメント化された使用と下位互換性があります。

パラメータは、ここで説明されたとおりに指定されます。

- **ipsec**：IPSec 接続であることを示します。省略すると、SSL が使用されます。
- **AUTHENTICATION**：IPSec 接続の認証方式を指定します。省略すると、EAP-AnyConnect が使用されます。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **IKE-IDENTITY**：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 にセットされているとき、IKE ID を指定します。このパラメータは、他の認証設定に使用されたときに無効になります。
- **HOST**：サーバ アドレスを指定します。使用するホスト名または IP アドレス。
- **PORT**：現在は無視されています。HTTP URI スキームの一貫性のために含まれています。
- **GROUP-URL**：サーバ名に付加されるトンネル グループ名。

例

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

規格に準拠した Cisco IOS ルータにのみ接続するには、次を使用します。

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

Android デバイスの AnyConnect

サポートされる Android デバイス

シスコは次のメーカーのモバイル デバイスをサポートするため、AnyConnect ブランド固有のアプリケーションを提供します。

- Samsung デバイス
- HTC デバイス
- Kindle デバイス

シスコは、Android デバイスをサポートするために次の AnyConnect アプリケーションを提供します。

- Android 4.0 以降のデバイス（ICS+）用の AnyConnect
- root 化されたデバイス向け AnyConnect

（注）　シスコは、Lenovo および Motorola デバイスのブランド仕様 AnyConnect アプリケーションを提供せず、またサポートもしません。Android バージョン 4.0（Ice Cream Sandwich）以降を実行する Lenovo および Motorola のデバイスは AnyConnect ICS+ アプリケーションを使用できます。AnyConnect 3.0 へアップグレードする前に、古いブランド仕様の AnyConnect パッケージをアンインストールします。

Samsung デバイス

Samsung AnyConnect Release 3.0.x および Samsung AnyConnect レガシー リリース 3.0.x は、次に示す Samsung 製品ラインをサポートします。デバイスは、Samsung から最新のソフトウェア アップデートを実行する必要があります。お使いのデバイスに適用するパッケージを判断するには『*Android 向け AnyConnect ユーザ ガイド*』にあるインストール手順を参照してください。

製品	モデル番号
ACE+	GT-S7500、GT-S7500、GT-S7500W
ACE II	GT-I8160
Conquer 4G	SPH-D600
Galaxy Appeal	SGH-I827
Galaxy Beam	GT-I8530
Galaxy Exhilarate	SGH-I577
Galaxy Mini	GT-S5570、GT-S5570B、GT-S5570BD1、GT-S5570L、GT-S5578、SCH-I559、SGH-T499、SGH-T499V、SGH-T499Y、
Galaxy Note	GT-I9220、GT-N7000、GT-N7000B、SHV-E160K、SHV-E160S、SHV-E160L、SCH-I889、SCH-I717M、SCH-I717R、SCH-I717D、SGH-NO54、SCH-I717
Galaxy Note 10.1	GT-N8000、GT-N8005、SHW-M480S、SHW-M480K、GT-N8010、GT-N8013、SHW-M480W
Galaxy Rush	SPH-M830

製品	モデル番号
Galaxy S	GT-I9000、GT-I9000B、GT-I9000L、GT-I9000LD1、GT-I9000M、GT-I9000T、GT-I9001、GT-I9003、GT-I9003B、GT-I9003L、GT-I9008、GT-I9008L、GT-I9018、GT-I9070、GT-I9070P、GT-I9088、SC-02B、SCH-I400、SCH-I405、SCH-I500、SCH-I809、SCH-I909、SGH-I896、SGH-I897、SGH-I927、SGH-I997R、SGH-N013、SGH-T699、SGH-T759、SGH-T769、SGH-T959、SGH-T959D、SGH-T959P、SGH-T959V、SGH-T959W、SHW-M100S、SHW-M110S、SHW-M130L、SHW-M190S、SHW-M220L、SHW-M340K、SHW-M340L、SHW-M340S、SPH-D720
Galaxy S II	GT-I9100、GT-I9100G、GT-I9100M、GT-I9100T、GT-I9100P、GT-I9103、GT-I9108、GT-I9210、GT-I9210T、SC-O2C、SC-O3D、SCH-I510、SCH-I919、SCH-I919U、SCH-I929、SCH-J001、SCH-W999、SGH-I727、SGH-I727R、SGH-I757M、SGH-N033、SGH-N034、SGH-T989、SCH-T989D、SHV-E110S、SHV-E120K、SHV-E120L、SHV-E120S、SHW-M250K、SHW-M250L、SHW-M250S、SPH-D170
Galaxy S III	GT-I9300、SCH-I535、SGH-I747、SGH-T999、SHV-E210K、SHV-E210L、SHV-E210S、SPH-L710
Galaxy S 4	GT-I9500、GT-I9505、SCH-I545、SGH-I337
Galaxy Stellar	SCH-I200
Galaxy Tab 7（WiFi 専用）[1]	GT-P1000、GT-P1000L、GT-P1000M、GT-P1000N、GT-P1000R、GT-P1000T、GT-P1010、SC-01C、SCH-I800、SGH-I849、SGH-I987、SHW-M180L、SHW-M180S
Galaxy Tab 7.0 Plus & 7.7	GT-P6200、GT-P6201、GT-P6210、GT-P6211、GT-P6800、GT-P6801、GT-P6810、GT-P6811、SCH-I815、SGH-N024、SGH-T869、SHV-E150S、SHW-M430W
Galaxy Tab 8.9	GT-P7300、GT-P7300B、GT-P7310、GT-P7320、GT-P7320T、SCH-P739、SGH-I957、SGH-I957M、SGH-I957R、SHV-E140K、SHV-E140L、SHV-E140S、SHW-M300S、SHW-M300W、SHW-M305W
Galaxy Tab 10.1	GT-P7500、GT-P7500D、GT-P7500M、GT-P7500R、GT-P7500V、GT-P7501、GT-P7503、GT-P7510、GT-P7511、SC-01D、SCH-I905、SGH-T859、SHW-M380K、SHW-M380S、SHW-M380W
Galaxy Tab 2 7.0	GT-P3100、GT-P3110、GT-P3113、SCH-I705
Galaxy Tab 2 10.1	GT-P5100、GT-P5110、GT-P5113
Galaxy W	GT-I8150、SGH-T679
Galaxy Xcover	GT-S5690
Galaxy Y Pro	GT-B5510B、GT-B5510L
Illusion	SCH-I110
Infuse	SCH-I997
Rugby	SGH-I847
Stratosphere	SCH-I405
Stratosphere II	SCH-I415
Transform Ultra	SPH-M930

1. Samsung Galaxy Tab 7 モバイル デバイスの Sprint 配布はサポートされません。

（注）　Samsung 社は、各モバイル サービス プロバイダーでこれらの製品ラインのデバイスをブランド変更します。

HTC デバイス

HTC AnyConnect Release 3.0.x は、http://www.htcpro.com/enterprise/VPN に示された HTC 製品ラインが 3.0 を介して Android リリース 2.1（Honeycomb を介した Eclair）を実行している場合、これらをサポートしています。これらのデバイスは、表に示すような必要とされる最小限のソフトウェアを実行しなくてはなりません [設定（Settings）] > [電話について（About phone）] > [ソフトウェア情報（Software information）] > [ソフトウェア番号（Software number）] に進み、デバイスで実行中のソフトウェア番号を確認します。

AnyConnect ICS+ Release 3.0.x は、Android 4.0（Ice Cream Sandwich）以降で実行されている、または Android 4.0（Ice Cream Sandwich）以降にアップグレードされている場合、次の HTC デバイスで使用される必要があります。HTC AnyConnect をインストールする間に、HTC デバイスをアップグレードする場合は、HTC AnyConnect アプリケーションをアンインストールしてから、新しい AnyConnect ICS+ アプリケーションをダウンロードする前に、デバイスを再起動します。

- HTC Rhyme S510b
- HTC ADR6330VW
- HTC Vivid
- HTC EVO Design 4G
- HTC ThunderBolt ADR6400L
- HTC Sensation XE
- HTC Sensation
- HTC Amaze 4G
- Beats Audio 対応 HTC Sensation XL
- HTC EVO 3D
- HTC EVO 3D X515m
- HTC X515d
- HTC ADR6425LVW

HTC Holiday としても知られる HTC Raider は、Cisco AnyConnect では作動しません。シスコと HTC は、実行中の Android のリリースに関係なく、HTC AnyConnect アプリケーションがすべての HTC デバイスで実行できるよう、この問題を対処するために作業しています。

Kindle デバイス

Kindle Fire HD デバイスと新しい Kindle Fire 向けの Cisco AnyConnect（Kindle Tablet Edition）Release 3.0.x を Amazon から入手できます。Anyconnect for Kindle は Android VPN Framework によってサポートされており、AnyConnect ICS+ パッケージと同じ機能を備えています。

Android 4.0 以降のデバイス（ICS+）用の AnyConnect

AnyConnect ICS+ Release 3.0.x は、Android 4.0（Ice Cream Sandwich）以降の Android VPN フレームワーク（AVF）でサポートされる VPN 接続を提供します。このパッケージは、ICS 以降を実行しているすべての Android デバイスで使用できます。

AVF は、基本的な VPN 接続のみ提供します。このような基本的 VPN 機能に依存する AnyConnect AVF クライアントでは、ブランド固有のパッケージが持つフルセットの VPN 機能が提供されません。

（注）　Android 4.0 以降を実行する未サポートのデバイスには、AnyConnect AVF クライアントを推奨します。サポートされているデバイスは、Android オペレーティング システムのバージョンに関係なく、ブランドに固有の AnyConnect クライアントを使用する必要があります。

root 化されたデバイス向け AnyConnect

シスコは、プレビューおよびテストの目的でのみ、Android 2.1 以降を実行する root 化された Android モバイル デバイス向けに Rooted AnyConnect リリース 3.0.x を提供しています。

シスコは、このクライアントをサポートしていませんが、このクライアントは 2.1 以降を実行する大部分の root 化されたデバイス上で動作します。問題が発生した場合は、その問題を android-mobile-feedback@cisco.com に報告してください。解決のために、最大限の努力を払います。

tun.ko モジュールおよび iptables の両方が必要です。不足しているものがある場合は、VPN 接続を確立しようとしたときに、それを通知するエラー メッセージが AnyConnect から表示されます。tun.ko モジュールがない場合、対応するデバイスのカーネルを入手またはビルドして、`/data/local/kernel_modules/` ディレクトリに配置します。

注意　お使いのデバイスを root 化すると、デバイスの保証が無効になります。シスコでは、root 化されたデバイスをサポートしていません。お使いのデバイスを root 化する手順も提供していません。お使いのデバイスのルート化を選択する場合は、ユーザ自身の自己責任において行ってください。

Android デバイスでサポートされる AnyConnect 機能

Android ブランド固有の AnyConnect

Samsung 用に、HTC と Motorola はデバイスをサポートおよび認定し、シスコは Android オペレーティング システム間でフル機能の VPN エクスペリエンスを提供するブランド固有の AnyConnect パッケージを提供しています。これらのブランド固有の AnyConnect パッケージは、デバイス ベンダーとのパートナーシップに従って提供されるものであり、これらデバイスに適した AnyConnect クライアントです。

Android AnyConnect Plus

Motorola がサポートおよび認定したデバイス（2012 年 5 月以降にリリース）に関して、シスコはブランド固有のパッケージと機能面において同等であるフル機能 VPN エクスペリエンスをもたらす特定のベンダーに特化しないパッケージを提供しています。

Android VPN フレームワークの AnyConnect

ブランド仕様の AnyConnect パッケージまたは AnyConnect Plus の使用ができないその他の Android デバイスのため、シスコはを使用することなくです。他の Android デバイスにシスコは、Android 4.0（Ice Cream Sandwich）導入された Android VPN Framework（AVF）にサポートされる VPN 接続をもたらす AnyConnect クライアントを提供しています。AVF は、基本的な VPN 接続のみ提供します。このような基本的 VPN 機能に依存する AnyConnect AVF クライアントでは、デバイス固有のパッケージが持つフルセットの VPN 機能が提供されません。これらの矛盾が表に示されます。Kinde デバイスもこのパッケージを使用しています。

Android をルーツとする AnyConnect

シスコは、ブランド固有パッケージの機能と同等であるルーツ化された Android デバイスに AnyConnect パッケージを提供しています。このパッケージは、Android 2.1 以降を実行するほとんどの root 化されたデバイスで動作します。ブランド仕様の AnyConnect パッケージは、ルーツ化されたデバイスで動作しません。したがって、root 化されたデバイスで AnyConnect の root 化されたバージョンを使用する必要があります。

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネリング	TLS/DTLS	Yes	Yes
	IPsec IKEv2	Yes	Yes
	IKEv2 - NAT-T	Yes	Yes
	IKEv2 - raw ESP	Yes	Yes
	Suite B のサポート	Yes（IPsec のみ）	Yes（IPsec のみ）
	TLS 圧縮	Yes	Yes
	デッド ピア検出	Yes	Yes
	トンネル キープアライブ	Yes	Yes
トンネルの確立	最適ゲートウェイ選択	No	No
	VPN ロード バランシング	Yes	Yes
	バックアップ サーバ リスト	Yes	Yes
	プロファイル インポートの接続をアクティブ化	Yes	Yes
	URI 接続クレデンシャルの事前入力	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネル ポリシー	すべての、または完全なトンネル	Yes	Yes
	スプリット トンネル（スプリットを含む）	Yes	Yes
	ローカル LAN（スプリット を含まない）	Yes	No
	Split-DNS	Yes	スプリットを含んで作動
	常時接続の適用	No	No
	自動再接続	Yes。自動再接続プロファイルの指定にかかわらず、ユーザが 3G と WiFi ネットワークの間を移動するときに、AnyConnect Mobile は VPN を常に維持します。	
	オンデマンド VPN（宛先により起動）	No	No
	オンデマンド VPN（アプリケーションによって起動）	No	No
	Trusted Network Detection（TND）	Yes	No
	キー再生成	Yes	Yes
	ASA グループ プロファイル サポート	Yes、制限されている	Yes、制限されている
	IPv4 パブリック トランスポート	Yes	Yes
	IPv6 パブリック トランスポート	No	No
	IPv4 over IPv4 トンネル	Yes	Yes
	IPv6 over IPv4 トンネル	Yes	Yes
	デフォルト ドメイン	Yes	Yes
	DNS サーバの設定	Yes	Yes
	プライベート側プロキシ サポート	No	No、VPN を確立した場合、WiFi プロキシは無効です。
	ログイン前バナー	Yes	Yes
	ログイン後バナー	Yes	Yes
	スクリプティング	No	No
	VPN の再設定	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネル セキュリティ	ネットワーク変更のモニタリング	Yes	Yes
	シムのインターセプト/フィルタリング	No	No
	組み込みファイアウォール ルール	No	No
	フィルタのサポート（iptables）	Yes	No
認証	手動による証明書のインポート（証明書を取得）	Yes	Yes
	SCEP 登録	Yes	Yes
	SCEP プロキシ	Yes	Yes
	自動証明書選択	Yes	Yes
	手動による証明書の選択	Yes	Yes
	エクスポート不可の証明書	該当なし	該当なし
	スマート カードのサポート	No	No
	ユーザ名およびパスワード	Yes	Yes
	トークン/課題	Yes	Yes
	二重認証	Yes	Yes
	グループ選択	Yes	Yes
	クレデンシャルの事前入力	Yes	Yes
	パスワードの保存	No	No

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
ユーザ インターフェイス	スタンドアロン GUI	Yes	Yes
	ネイティブ OS GUI	No	No
	CLI	No	No
	API	Yes。Java（C++ ではない）	Yes。Java（C++ ではない）
	UI のカスタマイゼーション	Yes（テーマ）	Yes（テーマ）
	UI のローカリゼーション	Yes	Yes
	ユーザ設定	Yes	Yes
	証明書確認の理由	Yes	Yes
	ワンクリック VPN アクセス用のホーム画面のウィジェット	Yes	Yes
	TND で接続が停止した場合の一時停止アイコン	Yes	Yes
	アイドル時の AnyConnect アイコンの非表示	Yes	Yes
	モバイル デバイスの起動	Yes	Yes
	AnyConnect の終了	Yes	Yes
	ユーザ証明書の管理	Yes	Yes
	ユーザ プロファイルの管理	Yes	Yes
	ユーザ ローカリゼーションの管理	Yes	Yes
配備	WebLaunch（ブラウザから開始）	No	No
	アプリケーション ストアへのウェブ リダイレクト	No	No
	スタンドアロン インストーラ	No	No
	OEM によるプレインストール	No	No
	ASA からのインストールまたはアップグレード	No	No
	Android Market からのインストールまたはアップグレード	Yes	Yes
	一部の言語用にパッケージ化されたローカリゼーション	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
設定	接続中の XML クライアント プロファイルのインポート	Yes	Yes
	XML クライアント プロファイルをインポートするための URI ハンドラ サポート	Yes	Yes
	ユーザ設定の接続エントリ	Yes	Yes
ポスチャ評価	デバイス チェック（ピンのロックや暗号化など）	No	No
	実行中またはインストールされたアプリケーション	No	No
	シリアル番号または固有 ID のチェック	No	No
	モバイル ポスチャ	Yes	Yes
URI の処理	接続エントリの追加	Yes	Yes
	VPN への接続	Yes	Yes
	接続時のクレデンシャルの事前入力	Yes	Yes
	VPN の解除	Yes	Yes
	証明書のインポート	Yes	Yes
	ローカリゼーション データのインポート	Yes	Yes
	XML クライアント プロファイルのインポート	Yes	Yes
	URI コマンドの外部（ユーザ）制御	Yes	Yes
トラブルシューティング	統計情報（Statistics）	Yes	Yes
	ログ	Yes	Yes
	電子メールの統計情報、ログ メッセージおよびシステム情報	Yes	Yes
	シスコへの直接的なフィードバック	Yes	Yes
	DART	No	No
サーティフィケーション	FIPS 140-2 レベル 1	Yes	Yes
	共通の基準	No	No

AnyConnect の Android デバイスへのインストールおよびアップグレード

Android デバイス向け AnyConnect は、Android Market からのみ使用できます。AnyConnect は、ASA からダウンロードできません。Android デバイスの適切な AnyConnect パッケージをダウンロードする手順については、『*Cisco AnyConnect セキュア モビリティ クライアント用 Android ユーザ ガイド*』を参照してください

Android デバイスの AnyConnect UI

AnyConnect アプリケーション、ユーザ インターフェイスとすべてのアクティビティついての説明は、『*Cisco AnyConnect セキュア モビリティ クライアント用 Android ユーザ ガイド*』を参照してください。

Android 固有の考慮事項

Android モバイル ポスチャ デバイスの ID 生成

（注） Android でモバイル ポスチャ デバイス ID を生成するアルゴリズムは、AnyConnect 3.0 で変更されました。AnyConnect の旧バージョンから生成されたデバイス ID を使用する DAP 規則を定義している場合、新しく生成されたデバイス ID にバインドするように更新しなければなりません。

AnyConnect 3.0 はインストール時に一義的な 40 バイトのデバイス ID を生成します。生成されたデバイス ID は、インストール時に使用可能な場合、Android ID と次のいずれかの値、もしくは両方の値に基づいています。

- MEID/IMEI（Mobile Equipment Identifier/International Mobile Equipment Identity）
- MAC-ADDRESS（デバイスの MAC アドレス）

デバイス ID はこれらの値の可用性によって生成されます。

使用可能な値	生成アルゴリズム
両方の値がインストール時に検索可能な場合：	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI + MAC-ADDRESS))`
MEID/IMEI のみインストール時に検索可能な場合：	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI))`
MAC-ADDRESS のみインストール時に検索可能な場合	`device-ID = bytesToHexString(SHA1(Android-ID + MAC-ADDRESS))`

ここで、

- Android ID は次のとおり設定されます。

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

- および `bytesToHexString` 機能：

```
String bytesToHexString(byte[] sha1rawbytes)
{
     String hashHex = null;
```

```
        if (sha1rawbytes != null)
        {
            StringBuffer sb = new StringBuffer(sha1rawbytes.length * 2);
            for (int i = 0; i < sha1rawbytes.length; i++)
            {
                String s = Integer.toHexString(0xFF & sha1rawbytes[i]).toUpperCase();
                if (s.length() < 2)
                {
                    sb.append("0");
                }
                sb.append(s);
            }
            hashHex = sb.toString();
        }
        return hashHex;
    }
```

（注）　MEID/IMEI もしくは MAC-ADDRESS 値のいずれかがインストール時に取得可能でない場合、デバイス ID を生成する際に、`Android-ID` と乱数が使用されます。

生成されたデバイス ID は、AnyConnect の **[診断（Diagnostics）] > [ログインとシステム情報（Logging and System Information）] > [システム（System）] > [デバイス識別子（Device Identifiers）]** 画面から、または device_identifiers.txt ファイルの AnyConnect ログから AnyConnect アプリケーションを起動して参照できます。

AnyConnect 2.5 では、MEID/IMEI がデバイス ID として使用されます。MEID/IMEI が使用可能でない場合、AnyConnect は MAC-ADDRESS を使用しようとします。この値も使用可能でない場合、AnyConnect インストールは失敗します。

AnyConnect の動作およびオプション

VPN 接続

VPN 接続を開始するには、ユーザがセキュア ゲートウェイのサーバ アドレスを識別するモバイル デバイスの接続エントリ、または他の接続属性を選択します。サーバ アドレスは、必要に応じてトンネル グループ URL を含めるセキュア ゲートウェイの完全修飾ドメイン名または IP アドレスです。AnyConnect は、モバイル デバイス アドレスの異なるセキュア ゲートウェイまたは VPN トンネル グループの複数の接続エントリをサポートします。複数の接続エントリが設定されている場合は、VPN 接続を開始するためにユーザがどれを使用するかを理解することが重要です。接続エントリは次の方法のいずれかで設定されます。

- ユーザが手動で設定します。

  モバイル デバイスの接続エントリを設定する手順については、適切なユーザ ガイドを参照してください。

- Anyconnect VPN クライアント プロファイルで定義されます。

  AnyConnect VPN クライアント プロファイルは XML ファイルで、クライアントの動作を指定し、VPN 接続エントリを識別します。各接続エントリは、このエンドポイント デバイスにアクセス可能なセキュア ゲートウェイ、およびその他の接続属性、ポリシー、および制約を指定します。詳細については、「AnyConnect プロファイル設定でモバイル デバイス接続の設定」セクションおよび「AnyConnect プロファイルの展開」セクションを参照してください。

- ユーザが管理者により提供されたリンクをクリックした後で追加し、接続エントリを設定します。

  ユーザに対するこの種の接続エントリの設定の提供は、「URI ハンドラを使用した VPN 接続エントリの生成」を参照してください。

VPN 接続を完了するには、ユーザはユーザ名とパスワード、もしくはデジタル証明書、またはその両方の形式でクレデンシャルを提供して認証する必要があります。管理者は、トンネル グループの認証方式を定義します。

モバイル デバイスの最高のユーザ エクスペリエンスのために、認証設定による複数の AnyConnect 接続プロファイルを使用することを推奨します。ユーザ エクスペリエンスとセキュリティのバランスを最適に保つ方法を決める必要があります。

- モバイル デバイスの AAA 対応認証トンネル グループについては、クライアントを再接続状態にし、ユーザが再認証しなくても済むよう、トンネル グループは 24 時間など非常に長時間のアイドル タイムアウトが必要になります。
- 最もトランスペアレントなユーザ エクスペリエンスを達成するには、証明書のみの認証を使用します。デジタル証明書を使用すると、VPN 接続は、ユーザとの対話なしで確立されます。

クライアント証明書

証明書を使用してセキュア ゲートウェイにモバイル デバイスを認証するため、エンド ユーザは、デバイスに証明書をインポートする必要があります。この証明書は自動証明書選択のために使用可能であり、また特定の接続エントリに手動で関連づけることができます。証明書は、次の方法を使用してインポートされます。

- ユーザが管理者により提供されたリンクをクリックした後で追加し、証明書をインポートします。ユーザにこの種の証明書を提供するため証明書をインポートするために、URI ハンドラを使用を参照します。
- SCEP の使用 管理者用の設定は、『*Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 3.0*』の「VPN アクセスの設定」の章の「SCEP を使用して証明書登録を設定する」を参照してください。
- ユーザが手動でインポートします。モバイル デバイスに証明書をインポートするために適切なユーザ ガイドを参照してください。

サーバ証明書

セキュア ゲートウェイで設定される有効で信頼できるサーバの証明書は、ユーザに簡単で安全な VPN 接続を提供します。

モバイル デバイスの AnyConnect は、セキュア ゲートウェイによって提示された証明書が無効または信頼できない、もしくはその両方の場合、VPN 接続をブロックすることでセキュア ゲートウェイにアクセスする際に、改善されたセキュリティ保護を提供します。

新しい [信頼できないサーバのブロッキング（Block Untrusted Servers）] アプリケーション設定は、セキュア ゲートウェイを識別できない場合、AnyConnect が接続をどのようにブロックするか決定します。この保護はデフォルトでは ON です。ユーザが OFF にできますが、OFF にする操作は推奨されません。

AnyConnect はサーバから受信したデジタル証明書を使用してそのアイデンティティを確認します。証明書が無効な場合（期限切れか無効な日付、不正なキーの用途、名前の不一致により証明書エラーがある）、または信頼できない場合（認証局が確認できない）場合、接続はブロックされます。ブロッキング メッセージが表示されるため、ユーザは処理を選択する必要があります。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] が ON の場合、ブロッキング**信頼できない VPN サーバ**の通知は、ユーザにセキュリティ上の脅威を警告します。ユーザは以下を選択できます。

- [安全にしておく（Keep Me Safe）] を選択して、この接続を終らせ、安全にしておきます。
- [信頼できないサーバのブロッキング（Block Untrusted Servers）] アプリケーションを OFF に**設定変更**します。ただし、これは推奨されません。ユーザがこのセキュリティ保護を無効にすると、VPN 接続を再起動しなくてはなりません。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] が OFF の場合、ブロックされていない**信頼できない VPN サーバ**の通知は、ユーザにセキュリティ上の脅威を警告します。ユーザは以下を選択できます。

- **接続をキャンセルし**、安全にしておきます。
- **接続を続行**します。ただし、これは推奨されません。
- **証明書の詳細を表示します。**

  ユーザが確認している証明書が有効であるが信頼できない場合、ユーザは次のことを実行できます。

  - 再使用できるようにサーバ証明書を AnyConnect 証明書ストアにインポートし、[インポートおよび継続（Import and Continue）] を選択して接続を継続します。AnyConnect ストアにこの証明書がインポートされると、このデジタル証明書を使用しているそのサーバに対する後続の接続は自動的に受け入れられます。
  - 前の画面に戻り [キャンセル（Cancel）] または [続行（Continue）] を選択します。

  証明書が無効な場合、または何らかの理由で、ユーザが前の画面にだけ戻ることができる場合 [キャンセル（Cancel）] または [続行（Continue）] を選択します。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] の設定を ON のままにし、自身のセキュア ゲートウェイで設定された有効で信頼できるサーバ証明書を持ち、モバイル ユーザを常に [安全にしておく（Keep Me Safe）] を選択させておくことが、ネットワークの VPN 接続の最も安全な設定です。

AnyConnect プロファイルの展開

モバイル デバイスの接続エントリがある VPN クライアント プロファイルを作成した後、管理者は次のいずれかの方法でクライアント プロファイルを配布する方法を選択する必要があります。

- VPN 接続のモバイル デバイス設定にクライアント プロファイルをアップロードして ASA を設定します。

  クライアント プロファイルを ASA にインポートし、グループ ポリシーと関連付ける方法については、『*Cisco AnyConnect Secure Mobility Client 管理者ガイド*』の「VPN アクセスの設定」の章の「AnyConnect プロファイルの展開」を参照してください。
- クライアント プロファイルをインポートするために、ユーザに AnyConnect URI リンクを提供します。

  詳細については、「VPN クライアント プロファイルをインポートするために URI ハンドラを使用」セクションを参照してください。
- モバイル デバイスのプロファイル管理を使用して AnyConnect プロファイルをインポートします。

  デバイス固有の手順については、該当するモバイル デバイスのユーザ ガイドを参照してください。

管理者がこれらのプロファイルを作成して配布した場合、エンド ユーザは、定義された接続エントリを変更できません。エンド ユーザは、手動で作成する接続エントリだけを変更できます。

AnyConnect は、モバイル デバイス上で一度に 1 つの VPN クライアント プロファイルのみ維持します。次に、現在のプロファイルが存在する場合、それを置換または削除する主要なシナリオをいくつか示します。

- ユーザは手動でプロファイルをインポートします。インポートされたプロファイルは、現在のプロファイルに置き換えられます。
- 自動または手動の VPN 接続を開始すると、現在のプロファイルが新しい接続のプロファイルによって置き換えられます。
- ユーザは手動で現在のプロファイルを削除します。現在のプロファイルが削除されると、削除されたプロファイルに定義されているすべての接続エントリが削除されます。

AnyConnect プロファイル設定でモバイル デバイス接続の設定

ステップ 1　次の点を考慮するデスクトップおよびモバイル エンドポイントに共通の設定手順については、VPN アクセスの設定 を参照してください:

プロファイル属性	例外
自動再接続	自動再接続仕様にかかわらず、AnyConnect Mobile は常に ReconnectAfterResume を試行します。

ステップ 2　この章で説明されているモバイル仕様の属性を設定します。

AnyConnect プロファイル エディタのダウンロード

モバイル デバイスのホスト接続エントリを含む VPN クライアント プロファイルを作成するには、AnyConnect プロファイル エディタ リリース 3.0.1047 以降を使用します。プロファイル エディタはスタンドアロン ツールです。次の方法でプロファイル エディタをダウンロードします。

ステップ 1　www.cisco.com の [AnyConnect セキュア モビリティ クライアント（AnyConnect Secure Mobility Client）] ページにアクセスし、[ソフトウェアをダウンロード（Download Software）] をクリックします。

ステップ 2　[リリースすべてと 3.0（All Releases and 3.0）] ディレクトリを展開し、AnyConnect の **3.0.1047** 以降を選択します。

ステップ 3　右のカラムで、命名規則の **anyconnect-profileeditor-win-<*version*>-k9.exe** でファイルを検索します。AnyConnect 3.0.1047 でリリースされた AnyConnect プロファイル エディタをダウンロードしていた場合、**anyconnect-profileeditor-win-3.0.1047-k9.exe** が見つかります。

ステップ 4　[今すぐダウンロード（Download now）] をクリックし、サイトの手順に従ってダウンロード プロセスを完了します。

Mobile-Specific の属性

証明書認証

接続エントリと関連する**証明書の認証**ポリシー属性が、この接続に証明書をどのように処理するかを指定します。有効な値は、自動、手動、または無効化です。

- **自動**：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、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**：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 は自動に証明書認証ポリシーをリセットします。
- **無効**：クライアント証明書は認証に使用されません。

インポートでのアクティブ化

インポートでのアクティブ化、または**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は、VPN 接続がデバイスにダウンロードされると、**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 ネットワーク ローミング

この属性は、Apple iOS デバイスの接続にだけ適用されます。

[ネットワーク ローミング（Network Roaming）]、または[3G/Wifi ネットワーク間でのローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]は、デフォルトで有効です。無効の場合、AnyConnect は、接続が切断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。

この機能により、ネットワークにおいて揺ぎない安全な接続で、シームレスなモビリティを提供します。エンタープライズとの接続を必要としますが、より良いバッテリ寿命により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、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*。

Apple iOS Connect On Demand

この属性は、Apple iOS デバイスの接続にだけ適用されます。

Apple iOS Connect On Demand 機能を使用すると、Safari などのアプリケーションで VPN 接続を開始できます。Apple iOS は、アプリケーションが要求したドメインを、*アクティブ*な接続エントリ（横にチェック マークが付いているエントリ）のドメイン リスト内の文字列に対して評価します。

iOS の Connect on Demand 経由で VPN 接続が開始されると、iOS は、トンネルが一定の期間非アクティブである（トンネルを通過するトラフィックがない）場合、そのトンネルを切断します。詳細については、Apple の『VPN On Demand』のマニュアルを参照してください。

Apple iOS を評価するドメイン リストを定義します。

- [接続しない（Never Connect）]：Apple iOS は最初に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS はドメイン要求を無視します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は `www.example.com` などのように指定します。

（注） Connect On Demand を有効化すると、AnyConnect によって VPN 設定内のサーバ アドレスが Never Connect リストに追加され、ブラウザを使用してセキュア ゲートウェイに接続したときに VPN 接続が開始されなくなります。この規則をそのままにしておいても、Connect on Demand に悪影響はありません。

- [常に接続（Always Connect）]：Apple iOS は次に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。このリストの最も一般的な用途は、内部リソースへの短時間のアクセス権を取得することです。値は `email.example.com` などのように指定します。

（注） Apple iOS 7 は、[*常に接続（Always Connect）*] ドメインをサポートしません。Apple iOS 7 デバイスの AnyConnect を実行すると、[*常に接続（Always Connect）*] としてリストアップされているデバイスは、[*必要に応じて接続（Connect if Needed）*] ドメインとして取り扱われます。

- [必要に応じて接続（Connect if Needed）]：Apple iOS は、DNS エラーが発生した場合に、ドメイン要求をこのリストに対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

Apple iOS は、次のすべての条件が満たされた場合にのみ、アプリケーションに代わって VPN 接続を確立します。

- VPN 接続がまだ確立されていない。
- Apple iOS Connect on Demand フレームワークに対応するアプリケーションがドメインを要求している。
- 接続エントリが有効な証明書を使用するように設定されている。
- 接続エントリで Connect on Demand が有効化されている。
- Apple iOS が、[接続しない（Never Connect）] リスト内の文字列とドメイン要求の照合に失敗する。
- 次のどちらかの条件を満たしている。

- Apple iOS で、[常に接続（Always Connect）] リスト内にドメイン要求と一致する文字列を見つけている。
- DNS ルックアップが失敗し、Apple iOS で、Connect if Needed リスト内にドメイン要求と一致する文字列を見つけている。

Connect On Demand のルールは、ドメイン名だけをサポートし、IP アドレスをサポートしません。しかし、ルール内で指定されたドメイン名は部分的または全体のドメイン文字列である場合があります。

（注） 統合された Apple iOS IPsec クライアントと AnyConnect は、Demand フレームワークで同じ Apple iOS VPN を使用します。

詳細については、iPad または iPhone ユーザ ガイドの「Connect-On-Demand ルールの設定」または、このマニュアルで後ほど説明する「URI ハンドラを使用した VPN 接続エントリの生成」を参照ください。

モバイル固有属性の設定

ステップ 1　VPN クライアント プロファイルで、[サーバ リスト（Server List）] を選択します。

ステップ 2　リストに新しいサーバ エントリを追加するには、[追加（Add）] を選択するか、リストからサーバ エントリを選択し、サーバ リストの [エントリ（Entry）] ダイアログボックスを開くには、[編集（Edit）] をクリックします。

ステップ 3　[サーバ リスト エントリ（Server List Entry）] ダイアログボックスで、[追加のモバイル専用設定（Additional mobile-only settings）] をオンにして [編集（Edit）] をクリックします。

ステップ 4　[Apple iOS / Android の設定（Apple iOS / Android Settings）] エリアでは、Apple iOS または Android オペレーティング システムを実行するデバイスに、次の属性を設定します。

a.　**証明書認証**タイプの選択：**自動**、**手動**または**無効化**。

b.　必要に応じて、[プロファイルがインポートされた場合、このサーバ リスト エントリをアクティブにする（Make this Server List Entry active when profile is imported）] チェックボックスをオンまたはオフにします。

ステップ 5　[Apple iOS のみの設定（Apple iOS Only Settings）] エリアでは、Apple iOS オペレーティング システムのみを実行するデバイスに、次の属性を設定します。

a.　必要に応じて、[3G/Wifi ネットワーク間でローミングされた場合は再接続（Reconnect when roaming between 3G/Wifi networks）] チェックボックスをオンまたはオフにします。

b.　必要に応じて、[要求に応じて接続（Connect on Demand）] チェックボックスをオンまたはオフにします。

[要求に応じて接続（Connect on Demand）] は、[証明書認証（Certificate Authentication）] フィールドが**手動**または**自動**に設定されている場合に有効です。[証明書の認証（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。

Connect On Demand がイネーブルの場合、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。

c. [ドメインまたはホストと一致（Match Domain or Host）] フィールドに、Connect on Demand ルールを作成する対象のホスト名（host.example.com）、ドメイン名（.example.com）、または部分ドメイン（.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。

d. [オンデマンド アクション（On Demand Action）] フィールドで、ユーザが前述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試みる場合、次のアクションから 1 つ指定します：[常に接続（Always connect）]、[必要に応じて接続（Connect if needed）]、または [接続しない（Never connect）]。

e. [追加（Add）] をクリックします。

このルールが、下部のルール リストに表示されます。

ステップ 6　[**OK**] をクリックします。

推奨する ASA 設定

ステップ 1　次の例外を考慮するデスクトップおよびモバイル エンドポイントに共通する設定手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「General VPN Setup」を参照してください。

属性	ASDM ロケーション	例外
ホーム ページ URL	[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）] > [グループ ポリシー（Group Policies）] > [追加または編集（Add or Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタマイゼーション（Customization）]。	AnyConnect Mobile は、ホーム ページ URL 設定を無視します。認証の成功後に、モバイル クライアントをリダイレクトすることはできません。
AnyConnect 接続プロファイル名およびエイリアス	[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 接続プロファイル（AnyConnect Connection Profiles）] > [追加（Add）]	AnyConnect モバイル クライアント接続に使用するトンネル グループ（接続プロファイル）の [名前（Name）] または [エイリアス（Aliases）] フィールドに特殊文字を使用しないでください。特殊文字の使用により、ゲートウェイからの応答処理ができないことにより、「接続に失敗しました（Connect attempt）」というエラー メッセージがログイン後に表示される原因になります。

ステップ 2　この章で説明したとおり、次の属性を設定します。

デッド ピア検出の設定

サーバ側のデッド ピア検出機能デバイスは、スリープ状態になることを防ぐため、オフになります。ただし、ネットワーク接続性の欠如によりトンネルが終了するときに、または、VPN 接続でトラフィックを送信し続けるには送信品質が非常に低下しているか、不可能かをクライアントが判断するため、クライアント側のデッド ピア検出は、オンになっている必要があります。

キープアライブ メッセージの無効化

クライアント側のデッド ピア検出がすでにイネーブルになっている場合、モバイル デバイスのバッテリ寿命を延ばすため、キープアライブ メッセージをディセーブルにすることをお勧めします。Keepalive Messages パラメータにアクセスするには、ASDM を使用して [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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] に移動します。

モバイル ポスチャの設定

Release 8.2（5+）および 8.4（2）を実行する ASA は、モバイル デバイスを検出する AnyConnect モバイル ポスチャを特徴としています。モバイル ポスチャにより、モバイル接続の受け入れ、拒否、または制限をできます。AnyConnect Premium と AnyConnect モバイル ライセンスが必要です。

モバイル デバイスの次の属性に基づいて、ダイナミック アクセス ポリシー（DAP）を設定します。

- クライアントのバージョン：AnyConnect クライアントのバージョン。
- プラットフォーム：Android および Apple iOS を含むオペレーティング システム。
- Platform Version：オペレーティング システム バージョン番号
- Device Type：iPad または Samsung GT-I9000 などのモバイル デバイス タイプ。
- Device Unique ID：モバイル デバイスの一意の ID Android プラットフォームのデバイス ID に関する重要な情報については、「Android モバイル ポスチャ デバイスの ID 生成」を参照してください。

詳細な手順については、「Cisco 5500 Series Configuration Guide using ASDM, 6.4」の「Adding Mobile Posture Attributes to a DAP」セクション、もしくは「Cisco Security Appliance Configuration Guide using ASDM, 6.2」の「Add/Edit Endpoint Attributes」セクションを参照ください。

VPN 接続の確立からモバイル デバイスの制限

AnyConnect Mobile ライセンスが ASA で動作しない場合は、自動的にモバイル デバイスからの接続要求を拒否します。

AnyConnect Mobile ライセンスでアクティブ化される ASA は、モバイル デバイス VPN 接続をサポートします。デフォルトでは、認証したユーザは AnyConnect が作動するモバイル デバイスからログインできます。

これらの接続を防ぐため、ASA を設定します。設定は ASA リリースによって異なります。

- Release 8.2（5+）および 8.4（2）を実行する ASA は、モバイル デバイスを検出する AnyConnect モバイル ポスチャを特徴としています。
- 以前のリリース、ASA リリース 8.0（4）から 8.2（4）、そして 8.4（1）では、異なる DAP の仕様、Cisco Secure Desktop、AnyConnect Premium ライセンスが必要です。

VPN モバイル デバイス接続を防ぐために ASA を設定するため、次のようにダイナミック アクセス ポリシーを追加します。

モバイル ポスチャを使用するための手順

ステップ 1　ASA で ASDM セッションを確立します。

ステップ 2　[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）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

ステップ 3　エンドポイント属性テーブルの右側にある [追加（Add）] を選択します。

ステップ 4　エンドポイント属性タイプを **AnyConnect** に変更します。

ステップ 5　プラットフォームを **Android** または **Apple iOS** に変更します。

ステップ 6　[デバイス種別（Device Type）] フィールドにモデル名を入力します。

ASDM がデバイス種別の横にあるドロップダウン リストに表示されます。しかし、ドロップダウン オプションはサポートされていません。

ステップ 7　各デバイス用にエンドポイント属性 1 つを DAP 追加し、ポリシーをこれに割り当てます。

ステップ 8　[追加（Add）]、[編集（Edit）]、[ダイナミック アクセス ポリシー（Dynamic Access Policies）] ウィンドウのアクセス / 認証ポリシー属性セクションのタブを使用して、Android 接続の制限の継続、終了、再接続をします。

以前の ASA リリースの手順

ステップ 1　ASA で ASDM セッションを確立します。

ステップ 2　[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）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] を選択します。

ステップ 3　ポリシーに名前をつけます（例：`Apple iOS の拒否` や `Android の拒否`など）。

ステップ 4　[詳細（Advanced）] をクリックします。

ステップ 5　[論理式（Expressions）] テキスト ボックスに次のいずれかを入力します。

```
EVAL(endpoint.os.version, "EQ", "Apple Plugin", "string")
```

または

```
EVAL(endpoint.os.version, "EQ", "Android", "string")
```

ステップ 6　[追加（Add）]、[編集（Edit）]、[ダイナミック アクセス ポリシー（Dynamic Access Policies）] ウィンドウのアクセス / 認証ポリシー属性セクションのタブを使用して、Android 接続の制限の継続、終了、再接続をします。

ステップ 7　[OK] および [適用（Apply）] をクリックします。

FIPS および Suite B の暗号化

モバイル デバイス向け AnyConnect 3.0 は、Cisco Common Cryptographic Module（C3M）が組み込まれています。これは、新世代の暗号化（NGE）アルゴリズムの一部として FIPS 140-2 に準拠した暗号化モジュールや NSA Suite B 暗号化が含まる Cisco SSL の実装です。

モバイル デバイス向け AnyConnect 3.0 では、Suite B の暗号化は、IPSec VPN でだけ使用可能です。FIPS 準拠の暗号化は、IPSec および SSL VPN で利用可能です。

暗号化アルゴリズムを使用すると、接続の間、ヘッドエンド ルータとネゴシエートされます。ネゴシエーションは、VPN 接続の両端の機能によって異なります。したがって、セキュア ゲートウェイは、FIPS に準拠する暗号化および Suite B の暗号化をサポートする必要があります。

ユーザは、AnyConnect 設定の **FIPS モード**を無効にすることで、ネゴシエーションにおいて NGE アルゴリズムだけを受け入れるように AnyConnect を設定します。FIPS モードが無効の場合、AnyConnect は VPN 接続の非 FIPS 暗号アルゴリズムも受け入れます。

モバイル デバイス向け AnyConnect 3.0 には、次の Suite B のアルゴリズムが含まれます。

- 対称暗号化と整合性のための AES-GCM サポート（128、192、256 ビット キー）
  - IKEv2 ペイロード暗号化および認証（AES-GCM のみ）
  - ESP パケット暗号化および認証
- ハッシュ用の SHA-2（256/384/512 ビットの SHA）サポート
  - IKEv2 認証ペイロード
  - ESP パケット認証
- キー交換向けの ECDH サポート
  - グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS
- デジタル署名、非対称暗号化、および認証用の ECDSA サポート（256、384、512 ビット楕円曲線）
  - IKEv2 ユーザ認証およびサーバ証明書の確認
- アルゴリズム間の他の暗号スイートの依存関係は、次のサポートを促進します。
  - IKEv2 用の Diffie-Hellman Groups 14 および 24
  - DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書

要件

- FIPS または Suite B のサポートは、セキュア ゲートウェイで必要です。シスコは、ASA バージョン 9.0 以降での Suite B 機能、および ASA バージョン 8.4.1 以降の FIPS 機能を提供します。
- ASA への FIPS または Suite B リモート アクセス接続には、AnyConnect Premium のライセンスが必要です。

（注）

- モバイル向け AnyConnect 3.0 のリリース時に、Apple iOS は ECDSA の証明書をサポートしていません。この問題は、Apple によって対処されます。固定されると、次の要件が適用されます。

  Apple iOS 5.0 以降は Suite B の暗号化に必要です。これは Suite B で使用される ECDSA の証明書をサポートする Apple iOS の最も低いバージョンです。

- Android 4.0（Ice Cream Sandwich）以降は、Suite B の暗号化に必要です。これは、SuiteB で使用される ECDSA の証明書をサポートする Android の最も低いバージョンです。
- VPN 接続には、デジタル署名の Key Usage 属性とキー暗号化、さらにはサーバ認証の Enhanced Key Usage 属性または IPsec の IKE 中間を含むサーバ証明書が必要です。キーの用途を含まないサーバ証明書では、すべてのキーの用途が無効と見なされます。同様に、キーの拡張用途を含まないサーバ証明書は、すべてのキーの拡張用途が無効と見なされます。

注意事項と制約事項

- Suite B は IKEv2/IPsec でのみ利用できます。
- FIPS モードで動作しているデバイスは、デジタル証明書、プロキシ方式または従来の方法をモバイル ユーザに提供するために、SCEP 使用との互換性はありません。したがって適切に計画を立てましょう。
- SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。
- ECDSA 証明書には、カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
- VPN 接続は、サーバ証明書で名前の検証を実行します。名前検証では、次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name のみを使用します。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あるけれども関連する属性を含んでいない場合、名前検証は、証明書の Subject で見つかった　Common Name 属性を使用します。
  - 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、サブドメインの最後（右端）の文字でなければなりません。この規則に準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

AnyConnect インターフェイスおよびメッセージのローカライズ

リリース 2.5 から、Android および Apple iOS 用 AnyConnect セキュア モビリティ クライアントは、ローカリゼーションをサポートし、AnyConnect ユーザ インターフェイスやメッセージをユーザのロケールに適用しています。

パッケージ化されたローカリゼーション

AnyConnect パッケージには、次の言語変換が含まれます。

- チェコ語（cs-cz）
- ドイツ語（de-de）
- 中南米スペイン語（es-co）
- カナダ フランス語（fr-ca）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- ポーランド語（pl-pl）
- 簡体字中国語（zh-cn）

AnyConnect のインストール時には、これらの言語のローカリゼーション データがモバイル デバイスにインストールされます。モバイル デバイスで指定されたロケールにより、表示される言語が決定します。AnyConnect は最適なものを判断するため、言語仕様を使用してから、リージョン仕様を使用します。たとえば、インストール後にロケール設定をスイス フランス語（fr-ch）にすると、カナダ フランス語（fr-ca）表示になります。AnyConnect の UI とメッセージは、AnyConnect を起動するとすぐに変換されます。

ダウンロードされたローカリゼーション

AnyConnect パッケージではない言語に関して、管理者は、AnyConnect VPN 接続のデバイスにダウンロードされる ASA にローカライズ データを追加します。ASA のローカリゼーション設定については、Localizing the AnyConnect GUI を参照ください。ASA がデバイスのロケールにローカリゼーション データを含めない場合、AnyConnect アプリケーション パッケージにプリインストールされたローカリゼーション データを引き続き使用します。

シスコでは、ローカライズ可能な AnyConnect 文字列をすべて含む anyconnect.po ファイルを Cisco.com の製品ダウンロード センターで提供しています。AnyConnect 管理者は、anyconnect.po ファイルをダウンロードし、使用可能な文字列を翻訳してから、ASA にファイルをアップロードします。AnyConnect 管理者は、anyconnect.po ファイルを ASA にインストールしたあと、この更新バージョンをダウンロードしてください。

最初に AnyConnect ユーザ インターフェイスおよびメッセージがインストールした言語でユーザに表示されます。エンド ユーザが ASA への初めての接続を確立すると、AnyConnect では、デバイスの優先言語が比較され、ASA でのローカリゼーション言語が使用可能になります。一致するローカリゼーション ファイルが検索されると、ローカライズされたファイルがダウンロードされます。ダウンロードが完了すると、AnyConnect は anyconnect.po ファイルに追加された変換文字列を使用してユーザ インターフェイスおよびユーザ メッセージを表示します。文字列が翻訳されていない場合、AnyConnect ではデフォルトの英語文字列が表示されます。

ASA がデバイスのロケールにローカリゼーション データを含めない場合、使用している AnyConnect アプリケーション パッケージからインストール済みのローカリゼーション データを含めます。

手順

ステップ 1　[製品を選択（Select a Product）] ページから開始します。

ステップ 2　[製品（Products）] > [セキュリティ（Security）] > [仮想プライベート ネットワーク（VPN）（Virtual Private Networks (VPN)）] > [シスコ VPN クライアント（Cisco VPN Clients）] > [シスコ AnyConnect セキュア モビリティ クライアント（Cisco AnyConnect Secure Mobility Client）] を選択します。

ステップ 3　リリースのフォルダ ツリーの**すべてのリリース** フォルダを展開し、**3.0** を展開します。そして、最新の AnyConnect 3.0 リリースを開きます。

ステップ 4　ダウンロード可能なファイルのリストから、**anyconnect.po** を探し、[今すぐダウンロード（Download Now）] をクリックします。

ステップ 5　ファイルをダウンロードするプロンプトに従います。

追加のローカリゼーション

管理者にとって、ユーザのデバイスにローカリゼーション データを取得する追加の方法は、ローカリゼーション データをインポートするために、AnyConnect URI をユーザに提供することです。次に例を示します。

```
anyconnect://import?type=localization&host=asa.example.com&lang=ja-jp
```

詳細については、URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズを参照してください。

ユーザ ローカリゼーションの管理

モバイル デバイスのユーザは、自身のデバイスでローカリゼーションのデータを管理します。次のローカリゼーション アクティビティを実行する手順については、適切なユーザ ガイドを参照してください。

- 指定したサーバからローカリゼーション データをインポートします。ユーザは、ローカリゼーション データのインポートを選択し、セキュア ゲートウェイのアドレスとロケールを指定します。ロケールは ISO 639-1 で指定されており、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。このローカリゼーション データは、インストールされたローカリゼーション データの代わりに使用されます。
- デフォルトのローカリゼーション データのリストア。AnyConnect パッケージから事前ロードされたローカリゼーション データの使用を復元し、インポートされたローカリゼーション データをすべて削除します。

URI ハンドラを使用した AnyConnect アクションの自動化

AnyConnect の URI ハンドラは、他のアプリケーションに Universal Resource Identifiers（URI）形式で AnyConnect に対してアクション要求を割り当てさせます。AnyConnect ユーザ設定プロセスを簡素化するため、URI を Web ページまたは電子メール メッセージにリンクとして埋め込み、これらにアクセスする方法をユーザに提供します。URI では、次を実行できます

- VPN 接続エントリを生成します。
- VPN への接続を確立し、VPN の接続を解除します。
- ローカリゼーション ファイル、証明書および AnyConnect プロファイルをインポートします。

AnyConnect アプリケーションで処理する URI はデフォルトで無効です。モバイル デバイスのユーザは、AnyConnect Application Preference External Control を有効もしくはプロンプトに設定することで、この機能を使用できます。外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。

ユーザは、URI のアクティビティの通知がされ、[プロンプト（Prompt）] を選択することによって、要求時に許可または不許可されます。これらを使用する場合、URI の処理に関連付けられたプロンプトに応答する方法をユーザに通知する必要があります。

URI ハンドラ パラメータ値を入力する場合、URL エンコードを使用する必要があります。アクション要求を符号化するために、リンクでこのようなツールを使用します。

（注）　Android ユーザは、Web ブラウザのアドレス バーにこれらの URI を入力できません。リモート Web サーバからこれらの URI にアクセスする必要がある場合、もしくは電子メールのクライアントにより、電子メールのリンクをクリックできる場合があります。

URI ハンドラを使用した VPN 接続エントリの生成

AnyConnect URI ハンドラの **create** アクションを使用して、ユーザの AnyConnect 接続エントリの生成を簡略化します。

デバイスに追加する各接続エントリの個別のリンクを挿入します。単一のリンクで複数の作成接続エントリ アクションを指定することはサポートされていません。

エンドポイント設定に AnyConnect 接続エントリを追加するため、次の URI 構文を使用します。

anyconnect:[**//**]**create**[**/**]**?name=***Description*&**host=***ServerAddress*[&*Parameter1*=*Value*&*Parameter2*=*Value ...*]

例：

anyconnect://create/?name=SimpleExample**&host=**vpn.example.com

anyconnect:create?name=SimpleExample**&host=**vpn.example.com

スペースに一致させるには、**%20** と入力します。たとえば、`Example Connection 1` という接続エントリに一致させるには、**Example%20Connection%201** と入力します。

作成処理には、`host` パラメータが必要となり、他のすべてのパラメータはオプションとなります。アクションがデバイスで実行すると、AnyConnect は、その `name` と `host` に関連付けられた接続エントリに入力するすべてのパラメータ値を保存します。

パラメータ オプションを作成します。

- **name**：AnyConnect のホーム ウィンドウの接続リストおよび AnyConnect 接続エントリの [説明（Description）] フィールドに表示される接続エントリの一意の名前。AnyConnect は名前が一意の場合のみ応答します。接続リストに収まるように、半角 24 文字以内にすることを推奨します。テキストをフィールドに入力する場合、デバイスに表示されたキーボード上の任意の文字、数字、または記号を使用します。文字の大文字と小文字が区別されます。
- **host**：接続に使用する ASA のドメイン名、IP アドレス、またはグループ URL を入力します。AnyConnect はこのパラメータの値を AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドに挿入します。
- **protocol**（任意、指定されていない場合は、SSL にデフォルト）：この接続に使用される VPN プロトコル。有効な値は次のとおりです。
  - SSL
  - IPsec

  anyconnect:create?name=ExampleIPsec&**host**=vpn.company.com&**protocol**=IPsec
- **authentication**（任意、**プロトコル**が `IPsec` のみを指定している場合に適用、デフォルトは EAP-AnyConnect）：IPsec VPN 接続で使用される認証手法方法。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **ike-identity**（**authentication** が EAP-GTC、EAP-MD5、EAP-MSCAPv2 に設定されている場合に必要）：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 にセットされているときの IKE ID。このパラメータは、他の認証設定に使用されたときに無効になります。

  anyconnect:create?**name**=Description&**host**=vpn.company.com&**protocol**=IPsec&**authentication**=eap-md5&**ike-identity**=012A4F8B29A9BCD
- **netroam**（任意、Apple iOS にのみ適用）：デバイス起動後、または接続タイプ（EDGE、3G、Wi-Fi など）の変更後、再接続にかかる時間を制限するかどうかを決定します。

  anyconnect:create?name=Example%201**&host=**vpn.example.com**&netroam=**true

  （注） このパラメータは、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*。

  有効な値は次のとおりです。
  - **true :**（デフォルト）このオプションでは、VPN アクセスが最適化されます。AnyConnect は値 ON を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドに挿入します。AnyConnect が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定では、アプリケーションは VPN への持続的な接続に依存します。AnyConnect は、再接続にかかる時間を制限しません。
  - **false**：このオプションでは、バッテリ寿命が最適化されます。AnyConnect はこの値を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドの OFF 値と関連付けます。AnyConnect が接続を失った場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。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。

- **usecert**（任意）：ホストへの VPN 接続を確立するときに、デバイスにインストールされているデジタル証明書を使用するかどうかを決定します。

  anyconnect:create?name=Example%201**&host=**vpn.example.com**&usecert=**true

  有効な値は次のとおりです。

  - **true**（デフォルト設定）：ホストとの VPN 接続を確立するときに自動証明書選択を無効化します [証明書（Certificate）] フィールドを自動にする **certcommonname** 値を指定することなしで **usecert** を true に返し、接続時に AnyConnect 証明書ストアから証明書を選択します。
  - **false**：自動証明書の選択を無効化します。

- **certcommonname**（任意、ただし usecert パラメータは必要）：デバイスにあらかじめインストールされた有効な証明書の Common Name（CN; 通常名）を一致させます。AnyConnect はその値を AnyConnect 接続エントリの [証明（Certificate）] フィールドに挿入します。

  デバイスにインストールされているこの証明書を表示するには、[診断（Diagnostics）] > [証明書（Certificates）] をタップします。

  host で必要な証明書を表示するため、スクロールしなければならない場合があります。その他の値と同様に、証明書から読み取った共通名パラメータを表示するために、詳細表示ボタンをタップします。

- **useondemand**（任意、Apple iOS だけに適用、usecert および certcommonname パラメータが必要）：Safari などのアプリケーションが、VPN 接続を開始できるかどうか決定します。
  - **true**：アプリケーションは Apple iOS を使用して VPN 接続を開始できます useondemand パラメータを true に設定すると、AnyConnect は値 ON を AnyConnect 接続エントリの [オンデマンド接続（Connect on Demand）] フィールドに挿入します。
  - **false**（デフォルト）：アプリケーションは VPN 接続を開始できません。このオプションは、DNS 要求を行うアプリケーションが VPN 接続をトリガーしないようにする唯一の手段です。AnyConnect は、AnyConnect 接続エントリの Connect on Demand フィールドで OFF 値でこのオプションを関連付けます。

  anyconnect:create?name=Example%20with%20certificate**&host=**vpn.example.com**&netroam=**true**&usecert=**true**&certcommonname=**example-ID**&useondemand=**true**&domainlistalways=**email.example.com,pay.examplecloud.com**&domainlistnever=**www.example.com**&domainlistifneeded=**intranet.example.com

- **domainlistnever**（オプション、useondemand=true が必要）：Connect on Demand 機能の使用を不適格とするために、一致を評価するドメインをリストにまとめます。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が最初に使用するリストです。ドメイン要求が一致すると、ドメイン要求は無視されます。AnyConnect はこのリストを AnyConnect 接続エントリの [接続しない（Never Connect）] フィールドに挿入します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は www.example.com などのように指定します。

- **domainlistalways**（useondemand=true）の場合、domainlistalways または domainlistifneeded パラメータが必要）：Connect on Demand 機能について一致を評価するドメインをリストします。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が 2 番目に使用するリストです。アプリケーションがこのパラメータで指定されたいずれかのドメインへのアクセスを要求し、VPN 接続がまだ行われていない場合、Apple iOS は VPN 接続を確立しようとします。AnyConnect はこのリストを AnyConnect 接続エントリの [常に接続（Always Connect）] フィールドに挿入します。値リストの例は email.example.com,pay.examplecloud.com です。

- **domainlistifneeded**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：DNS エラーが発生した場合、AnyConnect はこのリストに対してドメイン要求が一致しているかどうか評価します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。AnyConnect はこのリストを AnyConnect 接続エントリの [

必要に応じて接続（Connect if Needed）] フィールドに挿入します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

カンマで区切ったリストを使用して、複数のドメインを指定します。Connect-on-Demand の規則は IP アドレスではなく、ドメイン名のみサポートしています。ただし AnyConnect は、各リスト エントリのドメイン名形式について次のような柔軟性があります。

一致	指示	エントリの例	一致する例	一致しない例
プレフィックスおよびドメイン名が正確に一致。	プレフィックス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
ドメイン名は正確に一致し、プレフィックスは任意。先頭にドットを付けると、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

URI ハンドラを使用した VPN 接続の確立

接続情報を URI に組み込み、ユーザが簡単に VPN 接続を確立できるよう、これら URI を提供します。次の作業を行う URI 文字列を作成します。

- URI での接続名およびホスト名の指定
- URI での接続情報の指定およびユーザ名とパスワードの自動入力
- 二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力
- 接続情報の指定、ユーザ名およびパスワードの自動入力、および接続プロファイル エイリアスの指定

Connect パラメータおよび構文の説明も参照してください。

（注） URI を使用して、VPN 接続を確立するためにワンタイム パスワード（OTP）インフラストラクチャとの組み合わせのみ使用する必要がある場合、パスワードを指定します。

URI での接続名およびホスト名の指定

connect アクションに **name** および **host** パラメータを挿入するには、次のいずれかの構文式を使用します。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]
anyconnect:[//]connect[/]?name=Description&host=ServerAddress
```

完成した URI の例

anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example**&host=**hr.example.com

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

成功または失敗に対するアクションの指定

connect アクションの結果に基づいて特定の URL ベースを開始するために、**onsuccess** または **onerror** パラメータを使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]
[**&onsuccess**=URL**&onerror**=URL]

anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress*[**&onsuccess**=URL**&onerror**=URL]

例

anyconnect://connect?host=vpn.company.com**&onsuccess**=http%3A%2F%2Fwww.cisco.com
anyconnect://connect?host=vpn.company.com**&onerror**=http%3A%2F%2Fwww.cisco.com%2Ffailure.html**&onsuccess**=http%3A%2F%2Fwww.cisco.com

加えて、onsuccess もしくは onerror パラメータで **anyconnect://close** コマンドを使用して、AnyConnect GUI を閉じます。

anyconnect://connect?host=vpn.company.com**&onsuccess**=anyconnect%3A%2F%2Fclose

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

URI での接続情報の指定およびユーザ名とパスワードの自動入力

connect アクションの名前およびホスト パラメータに加えて、事前入力されたユーザ名とパスワード パラメータを指定するには、いずれかの構文を使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=**Description|**host=**ServerAddress]**&prefill_username**=username**&prefill_password**=password

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username**=username**&prefill_password**=password

完成した URI の例

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1

anyconnect:connect?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password**=password1

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力

事前入力されたプライマリおよびセカンダリ ユーザ名および事前入力されたパスワードを connect アクションでの name と host パラメータに加えて指定するには、次のどちらかの構文を使用します。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]&prefill_username=username&prefill_password=password&prefill_secondary_username=username2&prefill_secondary_password=password2
```

```
anyconnect:[//]connect[/]?name=Description&host=ServerAddress&prefill_username=username&prefill_password=password&prefill_secondary_username=username2&prefill_secondary_password=password2
```

完成した URI の例

```
anyconnect://connect/?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_secondary_username=user2&prefill_secondary_password=password2
```

```
anyconnect:connect?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_secondary_username=user2&prefill_secondary_password=password2
```

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

接続情報の指定、ユーザ名およびパスワードの自動入力、および接続プロファイル エイリアスの指定

この例では、接続プロファイル エイリアスを connect アクションで name および host パラメータに加えて、自動入力のユーザ名と自動入力のパスワードを指定する URI に追加しています。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]&prefill_username=username&prefill_password=password&prefill_group_list=10.%20Single%20Authentication
```

```
anyconnect:[//]connect[/]?name=Description&host=ServerAddress&prefill_username=username&prefill_password=password&prefill_group_list=10.%20Single%20Authentication
```

完成した URI の例

```
anyconnect://connect/?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_group_list=10.%20Single%20Authentication
```

```
anyconnect:connect?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_group_list=10.%20Single%20Authentication
```

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

Connect パラメータおよび構文の説明

connect アクションでは name パラメータもしくは host パラメータのいずれかが必要ですが、両方指定できます。ステートメントのすべてのパラメータ値がデバイスの AnyConnect 接続エントリに一致する場合、AnyConnect は接続を確立するために残りのパラメータを使用します。ステートメントのすべてのパラメータが接続エントリのパラメータと一致せず、name パラメータが一意の場合、新しい接続エントリが生成され、VPN 接続が試行されます。

connect パラメータ オプションの説明を次に示します。

- **name**：AnyConnect ホーム ウィンドウの接続リストに表示される、接続エントリの名前。AnyConnect はこの値を AnyConnect 接続エントリの [説明（Description）] フィールドに対して評価し、前回の手順を使用して Apple iOS デバイスに接続エントリを作成した場合、`name` とも呼ばれます。値は大文字と小文字を区別します。ステートメントの文字と接続エントリの文字の大文字または小文字が一致しない場合は、AnyConnect はこのフィールドを一致させません。
- **host**：AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドと一致させるには、ASA のドメイン名、IP アドレス、またはグループ URL を入力します。前回の手順を使用してデバイスに接続エントリを生成した場合 host とも呼ばれます。
- **onsuccess**：接続が接続状態に変わるとき、または **anyconnect:close** コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
- **onerror**：接続が接続解除状態に変わるとき、または **anyconnect:close** コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
- **prefill_username**：connect URI にユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_password**：connect URI にパスワードを指定し、接続プロンプトに自動入力します。

（注） prefill_password のフィールドでは、ワンタイム パスワードに設定されている接続プロファイルでのみ使用する必要があります。

- **prefill_secondary_username**：必要な二重認証に設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_secondary_password**：必要な二重認証に設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名のパスワードを指定し、接続プロンプトに自動入力します。
- **prefill_group_list**：これは、[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 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループ エイリアス / グループ URL（Group Alias/Group URL）] > [接続エイリアス（Connection Aliases）] を選択して、ASDM で定義されている接続エイリアスです。

URI ハンドラを使用した VPN からの切断

disconnect アクションを挿入するには、次の構文を使用します。

anyconnect:[**//**]**disconnect**[**/**]

例：

anyconnect:disconnect

スラッシュは省略可能です。disconnect アクションにはパラメータは必要ありません。

URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズ

（注）　AnyConnect UI やメッセージのローカライズのために URI ハンドラを使用するため、Apple iOS デバイスにインストールされた Apple iOS 5 以降を持っている必要があります。

URI で **import** コマンドを使用するには、次の構文を使用してください。

anyconnect:[**//**]**import**[**/**]**?type=localization&lang=***LanguageCode***&host=***ServerAddress***

例：

anyconnect:import?type=localization&lang=fr**&host=**asa.example.com

スラッシュは省略可能です。インポート アクションは、すべてのパラメータが必要です。**type**、**lang**、および **host** の各パラメータを下に定義します。

- **type**：インポートのタイプ（この場合**はローカリゼーション**）。
- **lang**：anyconnect.po ファイルで指定されて言語を表す 2 文字または 4 文字の言語タグ。たとえば、言語タグは単純に「French」なら fr、「Canadian French」なら fr-ca となります。
- **host**：AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドと一致させるには、ASA のドメイン名または IP アドレスを入力します。

証明書をインポートするために、URI ハンドラを使用

AnyConnect クライアントは、エンドポイントにインストールされた PKCS12 符号化証明書を使用して自ら ASA に認証します。URI ハンドラ **import** コマンドを使用して、PKCS12 符号化証明書バンドルをエンドポイントにインポートします。

PKCS12 証明書を URL からインポートするには、次の構文を使用します。

anyconnect://import/?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

URI の先頭のスラッシュは省略可能です。

スペースに一致させるには、**%20** と入力します。たとえば、`Example Connection 1` という文字列に一致させるには、Example**%20**Connection**%20**1 と入力します。

URI のコロンと一致させるには、**%3A** を使用します。URI のスラッシュと一致させるには、**%2F** を使用します。たとえば、http://example.cisco.com/CertName.p12 と一致させるには、`http`**%3A%2F%2F**`example.cisco.com`**%2F**`CertName.p12` と入力します。

次は、インポート パラメータ オプションの説明です。

- **type**：PKCS12 証明書タイプのみをサポートします。
- **ur**：URL は、証明書がある ID を符号化します。「http」、「https」および「ftp」をサポートします。URI では **%3A** はコロン（:）、**%2F** はスラッシュ（/）、**%40** はアンパサンド（@）を表します。

HTML ハイパーリンクの例

URI を HTML ページに追加するには、URI をハイパーリンクに組み込む必要があります。[HTML] ハイパーリンクで URI を使用する方法を示す例です。例中で太字の部分が URI です。

HTTP の例

```
<p>
<a href="anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12>
click here to import certificate using http</a>
</p>
```

FTP の例

```
<p><ahref="anyconnect://import?type=pkcs12
&uri=ftp%3A%2F%2FAdministrator%3Apassword%40192.168.10.20%2Fcerts%2FCertName.pfx">ここをクリックして、ftp を使用して証明書をインポートします</a>
</p>
```

Secure Digital（SD）カードの例

```
<p><a href="anyconnect://import?type=pkcs12
&uri=file%3A%2F%2F%2Fsdcard%2CertName.pfx">ここをクリックして、モバイル デバイスの SD カードから証明書をインポートします</a>

</p>
```

VPN クライアント プロファイルをインポートするために URI ハンドラを使用

AnyConnect クライアントにクライアント プロファイルを配信するため、この URI ハンドラのメソッドを使用します。

URI で **import** コマンドを使用するには、次の構文を使用してください。

anyconnect:[**//**]**import**[**/**]**?type=profile&uri=***Filename.xml*

例：

anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml

スラッシュは省略可能です。インポート アクションは、uri パラメータが必要です。

トラブルシューティング

モバイル デバイスでログインを有効にし、適切なユーザ ガイドのトラブルシューティングの指示に従ってください。

- *iPhone 用 Cisco AnyConnect セキュア モビリティ クライアント ユーザ ガイド（リリース 3.0.x）*
- *iPad 用 Cisco AnyConnect セキュア モビリティ クライアント ユーザ ガイド（リリース 3.0.x）*
- *Android 用 Cisco AnyConnect セキュア モビリティ クライアント ユーザ ガイド（リリース 3.0.x）*

次の手順で問題が解決しない場合、次の提案を試してください。

- 同じ問題がデスクトップ クライアントで発生しているかどうか判断します。
- AnyConnect Mobile ライセンスが ASA にインストールされていることを確認します。
- 証明書認証が失敗する場合、正しい証明書が選択されていることを確認します。デバイスのクライアント証明書に Extended Key Usage として Client Authentication があることを確認します。AnyConnect プロファイルの証明書一致規則がユーザの選択した証明書を除外していないことを確認します。ユーザが証明書を選択しても、プロファイルのフィルタリング ルールに一致しなければ認証には使用されません。認証メカニズムで ASA に関連するアカウンティング ポリシーが使用されている場合、ユーザが正常に認証できることを確認します。それでも問題が解決されない場合は、クライアントのロギングをイネーブルにし、ASA のデバッグ ロギングをイネーブルにします。
- 証明書のみの認証を使用しようとしている場合に認証画面が表示されたら、グループ URL を使用するよう接続を設定し、トンネル グループのセカンダリ認証が設定されていないことを確認します。詳細については、適切な『ASA 管理者ガイド』を参照してください。

Apple iOS 固有のトラブルシューティング

- デバイスが起動したあとで VPN 接続がリストアされていない場合は、[ネットワーク ローミング（Network Roaming）] が無効になっていることを確認します。
- 証明書認証および Apple iOS Connect On Demand 機能が接続するよう設定されている場合に AnyConnect アプリケーションを使用して Apple iOS が接続開始するよう要求している場合、グループ URL を使用するよう接続を設定します。グループ URL および証明書のみの認証の両方とも Connect on Demand の要件です。

APPENDIX A

VPN XML リファレンス

この付録は、ASDM を 6.3（1）以降にアップグレードしていない場合にのみ使用してください。AnyConnect 2.5 は、AnyConnect 機能を設定するためにアクセス可能なプロファイル エディタをサポートします。ただし、ASDM 6.3(1) 以降を使用する場合のみ、このプロファイル エディタにアクセスできます。それ以前の AnyConnect のバージョンには、Windows にインストール可能な独立型のプロファイル エディタが提供されていましたが、このプロファイル エディタは独立型のエディタとしてマニュアル化されておらず、サポート対象でなかったため、現在は提供されていません。プロファイルの作成、編集、および管理を直接行う場合、従来のエディタよりも AnyConnect プロファイル エディタで行う方がはるかに容易なことから、ASDM にアップグレードすることを強くお勧めします。新しいプロファイル エディタはマニュアル化され、サポート対象であり、独自のオンライン ヘルプを利用できます。AnyConnect 2.5 を使用する場合、ASDM 6.3（1）でサポートされる最小 ASA ソフトウェア リリースは ASA 8.0（2）です。ただし、新しいクライアント機能のメリットを最大限に利点できるように、ASA 8.3（1）以降にアップグレードすることをお勧めします。

AnyConnect プロファイルおよび機能の詳細については、第 3 章「*AnyConnect クライアント機能の設定*」を参照してください。この付録では、同章とは別の方法について説明します。

次の項では、各クライアント機能について簡単に説明し、XML タグ名、オプション、説明、およびコード例を記載します。プロファイルで値が指定されていない場合、AnyConnect はデフォルト値を使用します。それぞれの値内のすべてのプロファイル タグおよび特定のオプションを入力する場合について考慮します。この章で示される値は、エラー条件を避けるため、大文字または小文字を一致させる必要があります。

（注） 本書の例をカット アンド ペーストしないでください。カット アンド ペーストすると、改行が入り、XML が機能しなくなることがあります。代わりに、プロファイル テンプレート ファイルをテキスト エディタ（メモ帳やワードパッドなど）で開いてください。

XML のタグおよび値では、大文字と小文字が区別されます。大文字または小文字を誤って使用する（たとえば、「IPsec」の代わりに「IPSec」を使用する）と設定が失敗する原因になります。

ローカル プロキシ接続

表 A-1 に、ローカル プロキシ接続のサポートを設定するための、タグ名、オプション、および説明を示します。

表 A-1　ローカル プロキシ接続の設定

XML タグ名	オプション	説明
AllowLocalProxyConnections	true（デフォルト）	ローカル プロキシ接続をイネーブルにします。
	false	ローカル プロキシ接続をディセーブルにします。

例：ローカル プロキシ接続のディセーブル

ローカル プロキシ接続の AnyConnect サポートをディセーブルにするには、次の例を参照してください。

```
<ClientInitialization>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
</ClientInitialization>
```

Optimal Gateway Selection（OGS）

表 A-2 に、OGS を設定するためのタグ名、オプション、および説明を示します。

表 A-2　OGS 設定

XML タグ名	オプション	説明
EnableAutomaticServerSelection	true	デフォルトで OGS がイネーブルになります。
	false	デフォルトで OGS がディセーブルになります。
EnableAutomaticServerSelection UserControllable	true	ユーザがクライアント設定で OGS をイネーブルまたはディセーブルに切り替えることを許可します。*
	false	デフォルトに戻します。デフォルトでは、ユーザは自動サーバ選択を制御できません。

表 A-2　OGS 設定

XML タグ名	オプション	説明
AutoServerSelectionImprovement	整数。デフォルトは 20 % です。	クライアントが別のセキュア ゲートウェイに接続する際の基準となるパフォーマンス向上率。
AutoServerSelectionSuspendTime	整数。デフォルトは 4 時間です。	現在のセキュア ゲートウェイを接続解除してから、別のセキュア ゲートウェイに再接続するまでの経過時間（単位は時間）を指定します。

* OGS がイネーブルのときは、この機能をユーザ制御可能にすることをお勧めします。

例：OGS

OGS を設定するには、次の例を参照してください。

```
<ClientInitialization>
    <EnableAutomaticServerSelection UserControllable="true">
     true
         <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
         <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
     </EnableAutomaticServerSelection>
</ClientInitialization>
```

Trusted Network Detection

表 A-3 に、Trusted Network Detection を設定するためのタグ名、オプション、および説明を示します。

表 A-3　Trusted Network Detection の設定

XML タグ名	オプション	説明
AutomaticVPNPolicy	true	TND をイネーブルにします。*TrustedNetworkPolicy* パラメータおよび *UntrustedNetworkPolicy* パラメータに従って、VPN 接続を開始または停止する必要があるときに自動的に管理します。
	false	TND をディセーブルにします。VPN 接続は、手動でないと開始および停止できません。
TrustedNetworkPolicy	Disconnect	信頼ネットワークで VPN 接続を接続解除します。
	Connect	信頼ネットワークで VPN 接続を開始します（VPN 接続がない場合）。
	DoNothing	信頼ネットワークでは何もしません。
	Pause	信頼ネットワークの外で VPN セッションが確立された後に、ユーザが信頼できると設定されたネットワークに入る場合、VPN セッションを接続解除する代わりにそのセッションを一時停止します。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。

表 A-3　Trusted Network Detection の設定 （続き）

XML タグ名	オプション	説明
UntrustedNetworkPolicy	Connect	非信頼ネットワークを検知すると、VPN 接続を開始します。
	DoNothing	非信頼ネットワークを検知すると、VPN 接続を開始します。このオプションは、常時接続 VPN と互換性がありません。[信頼されたネットワークポリシー（Trusted Network Policy）] および [信頼されていないネットワークポリシー（Untrusted Network Policy）] を共に [何もしない（Do Nothing）] に設定すると、Trusted Network Detection はディセーブルになります。
TrustedDNSDomains	String	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性のある DNS サフィックスのリスト（カンマ区切りの文字列）。次に、TrustedDNSDomain 文字列の例を示します。 *.cisco.com 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。
TrustedDNSServers	String	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性のある DNS サーバ アドレスのリスト（カンマ区切りの文字列）。次に、TrustedDNSServers 文字列の例を示します。 161.44.124.*,64.102.6.247 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされます。

例：Trusted Network Detection

Trusted Network Detection を設定するには、次の例を参照してください。この例では、信頼ネットワークの中に存在するときは自動的に VPN 接続を接続解除し、非信頼ネットワークに存在するときは VPN 接続を開始するようにクライアントが設定されます。

```
<AutomaticVPNPolicy>true
    <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
    <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
    <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
    <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

常時接続 VPN および下位機能

常時接続 VPN を選択する場合、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ディセーブルにします。

表 A-4 に、常時接続 VPN を設定するためのタグ名、オプション、および説明を示します。

表 A-4　常時接続 VPN 設定

XML タグ名	オプション	説明
AutomaticVPNPolicy	true	自動 VPN ポリシーをイネーブルにします。
	false	自動 VPN ポリシーをディセーブルにします。
TrustedDNSDomains	string	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性がある DNS サフィックスを指定します。

表 A-4　常時接続 VPN 設定 （続き）

XML タグ名	オプション	説明
TrustedDNSServers	string	クライアントが信頼ネットワーク内にいるときに、ネットワーク インターフェイスが持つ可能性がある DNS サーバ アドレスを指定します。
TrustedNetworkPolicy	disconnect	信頼ネットワークが検知されると、VPN から接続解除します。
	connect	信頼ネットワークが検知されると、VPN に接続します。
	donothing	信頼ネットワークが検知されると VPN に接続しないか、VPN から接続解除します。
UntrustedNetworkPolicy	connect	非信頼ネットワークが検知されると、VPN から接続解除します。
	disconnect	非信頼ネットワークが検知されると、VPN に接続します。
	donothing	非信頼ネットワークが検知されると VPN に接続しないか、VPN から接続解除します。
AlwaysOn	true	常時接続 VPN をイネーブルにします。
	false	常時接続 VPN をディセーブルにします。
ConnectFailurePolicy	open	AnyConnect が VPN セッションを確立できないとき（たとえば、適応型セキュリティ アプライアンスが到達不能である場合）に、ネットワーク アクセスを制限しません。
	closed	VPN が到達不能の場合でもネットワーク アクセスを制限します。この制限された状態では、コンピュータが接続を許可されているセキュア ゲートウェイに対してのみアクセスが許可されます。
AllowCaptivePortalRemediation	true	ユーザがキャプティブ ポータルを修復できるように、接続障害終了ポリシーによるネットワーク制限が CaptivePortalRemediationTimeout タグで指定した時間（分単位）の間だけ緩和されます。
	false	AnyConnect がキャプティブ ポータルを検出した場合でも、接続障害終了ポリシーによるネットワーク制限を適用します。
CaptivePortalRemediationTimeout	Integer	AnyConnect がネットワーク アクセス制限を解除する時間（分単位）。
ApplyLastVPNLocalResourceRules	true	セキュリティ アプライアンスから受信した最新のクライアント ファイアウォールを適用します。セキュリティ アプライアンスには、ローカル LAN 上のリソースへのアクセスを許可する ACL を含めることができます。
	false	セキュリティ アプライアンスから受信した最新のクライアント ファイアウォールを適用しません。
AllowVPNDisconnect	true	[接続解除（Disconnect）] ボタンを表示して、常時接続 VPN セッションを接続解除するためのオプションをユーザに表示します。ユーザは、再接続する前に代替セキュア ゲートウェイを選択するために、このオプションを使用できます。
	false	[接続解除（Disconnect）] ボタンを表示しません。このオプションは、AnyConnect GUI を使用して VPN を接続解除できないようにします。

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ーやテザード 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 ホットスポットの検出」（P.3-30）で説明）。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は制限されます。

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常時接続 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。

常時接続 VPN：XML の例

リリース 6.3（1）以前の ASDM を使用している場合は、次の例を使用して、AnyConnect XML プロファイルを手動で編集してください。この常時接続 VPN 例では、次の操作を実行します。

- [接続解除（Disconnect）] ボタンをイネーブルにし（AllowVPNDisconnect）、ユーザが VPN セッションを別のセキュア ゲートウェイで確立できるようにします。
- 接続障害ポリシーを closed に指定します。
- キャプティブ ポータルを修復するために、接続障害終了ポリシーによるネットワーク制限が 5 分間緩和されます。
- 最後の VPN セッション中に割り当てられた ACL ルールを適用します。

```
<ClientInitialization>
    <AutomaticVPNPolicy>true
        <TrustedDNSDomains>example.com</TrustedDNSDomains>
        <TrustedDNSServers>1.1.1.1</TrustedDNSServers>
        <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
        <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
        <AlwaysOn>true
            <AllowVPNDisconnect>true</AllowVPNDisconnect>
            <ConnectFailurePolicy>Closed
                <AllowCaptivePortalRemediation>true
                    <CaptivePortalRemediationTimeout>5</CaptivePortalRemediationTimeout>
                </AllowCaptivePortalRemediation>
                <ApplyLastVPNLocalResourceRules>true</ApplyLastVPNLocalResourceRules>
            </ConnectFailurePolicy>
        </AlwaysOn>
    </AutomaticVPNPolicy>
</ClientInitialization>
```

ロード バランシングを備えた常時接続 VPN

表 A-5 に、ロード バランシングと常時接続 VPN を設定するためのタグ名、オプション、および説明を示します。

表 A-5　ロード バランシング設定とともに常時接続 VPN を使用する

XML タグ名	オプション	説明
LoadBalancingServerList	FQDN または IP アドレス	クラスタのバックアップ デバイスを指定します。このオプションを指定しないと、常時接続 VPN がイネーブルではない場合に、AnyConnect はロード バランシング クラスタのバックアップ デバイスへのアクセスをブロックします。

例：ロード バランシングを備えた常時接続 VPN

```
<ServerList>
        <!--
            This is the data needed to attempt a connection to a specific
            host.
          -->
 <HostEntry>
   <HostName>ASA</HostName>
   <HostAddress>10.86.95.249</HostAddress>
  <LoadBalancingServerList>
     <!--
    Can be a FQDN or IP address.
        -->
      <HostAddress>loadbalancing1.domain.com</HostAddress>
      <HostAddress>loadbalancing2.domain.com</HostAddress>
      <HostAddress>11.24.116.172</HostAddress>
</LoadBalancingServerList>
  </HostEntry>
</ServerList>
```

Start Before Logon

表 A-6 に、Start Before Logon を設定するためのタグ名、オプション、および説明を示します。

表 A-6　Start Before Logon の設定

XML タグ名	オプション	説明
UseStartBeforeLogon	true	Start Before Logon をイネーブルにします。
	false	Start Before Logon をディセーブルにします。
UseStartBeforeLogon UserControllable	true	SBL をユーザが制御できるようにします。
	false	デフォルト設定に戻します。デフォルト設定では、ユーザが SBL を制御できません。

例：Start Before Logon

SBL を設定するには、次の例を参照してください。

```
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

AnyConnect ローカル ポリシー ファイルのパラメータと値

表 A-7 に、ローカル ポリシーを設定するためのタグ名、オプション、および説明を示します。

表 A-7　AnyConnect ローカル ポリシー設定

XML タグ名	オプション	説明
acversion="<version number>"		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。指定されているバージョンよりも古いクライアントがファイルを読み取った場合、クライアントはイベント ログ警告を発行します。
xmlns=http://schemas.xmlsoap.org/encoding/	ほとんどの場合、管理者はこのパラメータを変更しません。	XML 名前空間指定子です。
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">	ほとんどの場合、管理者はこのパラメータを変更しません。	スキーマ ロケーションの XML 指定子です。
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance	ほとんどの場合、管理者はこのパラメータを変更しません。	XML スキーマ インスタンス指定子です。
FipsMode	true	クライアントの FIPS モードをイネーブルにします。クライアントは、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します。
	false	クライアントの FIPS モードをディセーブルにします。
BypassDownloader	true	クライアントは、ASA 上にプロファイルのアップデート、翻訳、カスタマイゼーション、オプションのモジュール、コア ソフトウェアのアップデートなど、ダイナミック コンテンツがあるかどうかをチェックしません。
	false	クライアントは、ASA 上にダイナミック コンテンツがあるかどうかをチェックします（デフォルト）。
RestrictWebLaunch	true	WebLaunch の試行は失敗し、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。
	false	WebLaunch を許可します（デフォルト。AnyConnect 2.3 以前と同じ動作）。

表 A-7　AnyConnect ローカル ポリシー設定 （続き）

XML タグ名	オプション	説明
StrictCertificateTrust	true	クライアントは、無効な、一致しない、または信頼されていない証明書を使用する、ユーザの操作が必要となるセキュリティ ゲートウェイへの接続に失敗します。
	false	クライアントは、証明書を受け入れるようにプロンプトを表示します（デフォルト。AnyConnect 2.3 以前と同じ動作）。
RestrictPreferenceCaching	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。
	Thumbprints	クライアントおよびサーバの証明書のサムプリントはキャッシュされません。
	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。
	All	自動プリファレンスはど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。AnyConnect 2.3 以前と同じ動作）。
RestrictTunnelProtocols（現在はサポート対象外）	TLS	クライアントは IKEv2 および ESP のみを使用してトンネルを確立します。セキュリティ ゲートウェイへの情報伝達に、TLS/DTLS は使用しません。
	IPSec	クライアントは、認証およびトンネリングに TLS/DTLS だけを使用します。
	false	接続確立で、任意の暗号化プロトコルを使用できます（デフォルト）。
ExcludeFirefoxNSSCertStore（Linux および Mac）	true	Firefox NSS 証明書ストアを除外します。
	false	Firefox NSS 証明書ストアを許可します（デフォルト）。
ExcludePemFileCertStore（Linux および Mac）	true	PEM ファイル証明書ストアを除外します。
	false	PEM ファイル証明書ストアを許可します（デフォルト）。
ExcludeMacNativeCertStore（Mac 専用）	true	Mac ネイティブ証明書ストアを除外します。
	false	Mac ネイティブ証明書ストアを許可します（デフォルト）。
ExcludeWinNativeCertStore（Windows 専用。現在はサポート対象外）	true	Windows Internet Explorer 証明書ストアを除外します。
	false	Windows Internet Explorer 証明書ストアを許可します（デフォルト）。

（注）　プロファイル ファイルのポリシー パラメータを省略した場合、機能はデフォルト動作になります。

例：AnyConnect ローカル ポリシー
AnyConnect ローカル ポリシー ファイルを設定するには、以下の例を参照してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

Windows の証明書ストア

表 A-8 に、証明書ストアを設定するためのタグ名、オプション、および説明を示します。

表 A-8　証明書ストアの設定

XML タグ名	オプション	説明
CertificateStore	All	（デフォルト）すべての証明書ストアを使用して証明書を検索するよう AnyConnect クライアントに指示します。
	Machine	Windows ローカル マシン証明証ストアへの証明書ルックアップを制限するように AnyConnect クライアントに指示します。
	User	ローカル ユーザ証明証ストアへの証明書ルックアップを制限するように AnyConnect クライアントに指示します。

例：証明書のストア
証明書ストアを設定するには、次の例を参照してください。

```
<CertificateStore>Machine</CertificateStore>
```

証明書ストアの使用の制限

表 A-9 に、証明書ストアの使用を制限するためのタグ名、オプション、および説明を示します。

表 A-9　証明書ストアの制限の設定

XML タグ名	オプション	説明
ExcludeFirefoxNSSCertStore（Linux および Mac）	true	Firefox NSS 証明書ストアを除外します。
	false	Firefox NSS 証明書ストアを許可します（デフォルト）。

表 A-9　証明書ストアの制限の設定

XML タグ名	オプション	説明
ExcludePemFileCertStore（Linux および Mac）	true	PEM ファイル証明書ストアを除外します。
	false	PEM ファイル証明書ストアを許可します（デフォルト）。
ExcludeMacNativeCertStore（Mac 専用）	true	Mac ネイティブ証明書ストアを除外します。
	false	Mac ネイティブ証明書ストアを許可します（デフォルト）。
ExcludeWinNativeCertStore（Windows 専用。現在はサポート対象外）	true	Windows Internet Explorer 証明書ストアを除外します。
	false	Windows Internet Explorer 証明書ストアを許可します（デフォルト）。

証明書のプロビジョニングと更新を行う SCEP プロトコル

表 A-10 に、証明書をプロビジョニングおよび更新するためのタグ名、オプション、SCEP プロトコルの設定に関する説明を示します。

表 A-10　SCEP プロトコル設定

XML タグ名	オプション	説明
CertificateEnrollment		証明書登録の開始タグ。
CertificateExpirationThreshold	number of days	AnyConnect がユーザに証明書の失効が近づいていることを警告するタイミングを指定します。
AutomaticSCEPHost	ASA/group-alias の完全修飾ドメイン名	この属性で ASA ホスト名が指定され、SCEP 証明書取得用の接続プロファイル（トンネル グループ）が設定されている場合、ホストは自動証明書取得を試行します。
	ASA/group-alias の IP アドレス	
CAURL	完全修飾ドメイン名	
	CA サーバの IP アドレス	
CertificateSCEP		証明書の内容の要求方法を定義します。
CADomain		認証局のドメイン。
Name_CN		証明書の共通名。
Department_OU		証明書で指定されている部門名。
Company_O		証明書で指定されている企業名。
State_ST		証明書で指定されている州 ID。
Country_C		証明書で指定されている国 ID。
Email_EA		電子メール アドレス。
Domain_DC		ドメイン コンポーネント。
Surname（SN）		姓。
GivenName（GN）		通常は、名。
UnstructName（N）		未定義の名前。
Initials（I）		ユーザのイニシャル。
Qualifier（GEN）		ユーザの世代修飾子。（「Jr.」、「III.」など）。

表 A-10　SCEP プロトコル設定 （続き）

Qualifier（DN）		全体の DN の修飾子。
City（L）		都市 ID。
Title（T）		個人の役職。（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。
キー サイズ		登録する証明書に対して生成された RSA キーのサイズ。
DisplayGetCertButton	true	認証の証明書のプロビジョニングまたは更新をユーザが手動で要求できるようにします。通常、ユーザはあらかじめ VPN トンネルを作成する必要なく、認証局にアクセスできます。
	false	認証の証明書のプロビジョニングまたは更新をユーザが手動で要求できないようにします。
ServerList		サーバ リストの開始タグ。サーバ リストは、AnyConnect が最初に起動されたときに表示されます。ユーザは、ログインする ASA を選択できます。
HostEntry		ASA の設定の開始タグ。
HostName		ASA のホスト名。
HostAddress		ASA の完全修飾ドメイン名。

例：SCEP プロトコル

ユーザ プロファイルの SCEP 要素を設定するには、以下の例を参照してください。

```
<AnyConnectProfile>
    <ClientInitialization>
        <CertificateEnrollment>
            <CertificateExpirationThreshold>14</CertificateExpirationThreshold>
            <AutomaticSCEPHost>asa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="true"
Thumbprint="8475B661202E3414D4BB223A464E6AAB8CA123AB">http://ca01.cisco.com</CAURL>
            <CertificateSCEP>
                <CADomain>cisco.com</CADomain>
                <Name_CN>%USER%</Name_CN>
                <Department_OU>Engineering</Department_OU>
                <Company_O>Cisco Systems</Company_O>
                <State_ST>Colorado</State_ST>
                <Country_C>US</Country_C>
                <Email_EA>%USER%@cisco.com</Email_EA>
                <Domain_DC>cisco.com</Domain_DC>
                <DisplayGetCertButton>false</DisplayGetCertButton>
            </CertificateSCEP>
        </CertificateEnrollment>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>ABC-ASA</HostName>
            <HostAddress>ABC-asa-cluster.cisco.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>Certificate Enroll</HostName>
            <HostAddress>ourasa.cisco.com</HostAddress>
            <AutomaticSCEPHost>ourasa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="false"
Thumbprint="8475B655202E3414D4BB223A464E6AAB8CA123AB">http://ca02.cisco.com</CAURL>
```

```
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

証明書照合

（注）　証明書一致基準を指定しない場合、AnyConnect は、次の証明書一致ルールを適用：

- キーの用途：Digital_Signature
- キーの拡張用途：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。

表 A-11 に、証明書照合を設定するためのタグ名、オプション、および説明を示します。

表 A-11　証明書照合

XML タグ名	オプション	説明
CertificateExpirationThreshold		証明書の有効期限までの日数を指定します。ユーザは証明書の失効が近づいていることについて警告されます。
CertificateMatch	n/a	クライアント証明書選択を調整するプリファレンスを定義します。証明書が認証の一部として使用される場合にのみ含めます。ユーザ証明書を一意に識別するために必要な CertificateMatch サブセクション（KeyUsage、ExtendedKeyUsage、および DistinguishedName）だけをプロファイルに含める必要があります。
KeyUsage	n/a	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を指定します。
MatchKey	Decipher_Only Encipher_Only CRL_Sign Key_Cert_Sign Key_Agreement Data_Encipherment Key_Encipherment Non_Repudiation Digital_Signature	KeyUsage グループの MatchKey 属性で、受け入れ可能なクライアント証明書の選択に使用できる属性を指定します。1 つ以上の照合キーを指定します。指定されたキーの少なくとも 1 つが一致する証明書が選択されます。
ExtendedKeyUsage	n/a	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を選択します。

表 A-11　証明書照合 （続き）

XML タグ名	オプション	説明
ExtendedMatchKey	ClientAuth ServerAuth CodeSign EmailProtect IPSecEndSystem IPSecUsers Timestamp OCSPSigns DVCS	ExtendedKeyUsage グループの ExtendedMatchKey で、受け入れ可能なクライアント証明書の選択に使用できる属性を指定します。0 個以上の拡張照合キーを指定します。指定されたすべてのキーが一致する証明書が選択されます。
CustomExtendedMatchKey	既知の MIB OID 値、1.3.6.1.5.5.7.3.11 など。	ExtendedKeyUsage グループで、0 個以上のカスタム拡張照合キーを指定できます。指定されたすべてのキーが一致する証明書が選択されます。キーは、OID 形式で指定する必要があります（1.3.6.1.5.5.7.3.11 など）。
DistinguishedName	n/a	グループ ID。DistinguishedName グループでは、証明書の識別名による照合によって受け入れ可能なクライアント証明書を選択するための、一致基準を指定できます。
DistinguishedNameDefinition	太字はデフォルト値を示します。 • Wildcard: **"Enabled"** "Disabled" • Operator: **"Equal" (==)** "NotEqual" (!==) • MatchCase: **"Enabled"** "Disabled"	DistinguishedNameDefinition で、照合で使用する単一の識別名属性を定義する演算子のセットを指定します。Operator は、照合を実行するときに使用する動作を指定します。MatchCase は、パターン マッチングで大文字と小文字を区別するかどうかを指定します。

表 A-11　証明書照合 （続き）

XML タグ名	オプション	説明
Name	CN DC SN GN N I GENQ DNQ C L SP ST O OU T EA ISSUER-CN ISSUER-DC ISSUER-SN ISSUER-GN ISSUER-N ISSUER-I ISSUER-GENQ ISSUER-DNQ ISSUER-C ISSUER-L ISSUER-SP ISSUER-ST ISSUER-O ISSUER-OU ISSUER-T ISSUER-EA	照合で使用する DistinguishedName 属性。最大で 10 個の属性を指定できます。

表 A-11　証明書照合 （続き）

XML タグ名	オプション	説明
Pattern	二重引用符で囲まれたストリング（1 ～ 30 文字）。ワイルドカードをイネーブルにすると、パターンを文字列内の任意の場所に指定できます。	照合で使用する文字列（パターン）を指定します。この定義では、ワイルドカード パターン マッチはデフォルトでディセーブルになっています。

例：証明書照合

クライアント証明書選択を調整するために使用できる属性をイネーブルにするには、次の例を参照してください。

（注） この例の KeyUsage、ExtendedKeyUsage、および DistinguishedName のプロファイル オプションは単なる例です。CertificateMatch 基準は、使用する証明書に適用するもののみ設定する必要があります。

```
<CertificateMatch>
     <!--
         Specifies Certificate Key attributes that can be used for choosing
         acceptable client certificates.
       -->
    <KeyUsage>
        <MatchKey>Non_Repudiation</MatchKey>
        <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
     <!--
         Specifies Certificate Extended Key attributes that can be used for
         choosing acceptable client certificates.
       -->
    <ExtendedKeyUsage>
        <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
        <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
        <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
    </ExtendedKeyUsage>
     <!--
         Certificate Distinguished Name matching allows for exact
         match criteria in the choosing of acceptable client
         certificates.
       -->
    <DistinguishedName>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled">
            <Name>CN</Name>
            <Pattern>ASASecurity</Pattern>
        </DistinguishedNameDefinition>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
            <Name>L</Name>
            <Pattern>Boulder</Pattern>
        </DistinguishedNameDefinition>
    </DistinguishedName>
</CertificateMatch>
```

自動証明書選択

表 A-12 に、自動証明書選択を設定するためのタグ名、オプション、および説明を示します。

表 A-12　自動証明書選択の設定

XML タグ名	オプション	説明
AutomaticCertSelection	true	AnyConnect は自動的に認証証明書を選択できます。
	false	ユーザに認証証明書を選択するよう求めるプロンプトを表示します。

例：AutomaticCertSelection
AutomaticCertSelection を使用してクライアント プロファイルを設定するには、次の例を参照してください。

```
<AnyConnectProfile>
    <ClientInitialization>
        <AutomaticCertSelection>false</AutomaticCertSelection>
    </ClientInitialization>
</AnyConnectProfile>
```

バックアップ サーバ リスト パラメータ

表 A-13 に、バックアップ サーバ リストを設定するためのタグ名、オプション、および説明を示します。

表 A-13　バックアップ サーバ リストの設定

XML タグ名	オプション	説明
BackupServerList	n/a	グループ ID を判別します。
HostAddress	IP アドレスまたは完全修飾ドメイン名（FQDN）	バックアップ サーバ リストに含めるホスト アドレスを指定します。

例：バックアップ サーバ リスト
バックアップ サーバ リスト パラメータを設定するには、次の例を参照してください。

```
<BackupServerList>
   <HostAddress>bos</HostAddress>
   <HostAddress>bos.example.com</HostAddress>
</BackupServerList>
```

Windows Mobile ポリシー

表 A-14 に、Windows Mobile ポリシーを設定するためのタグ名、オプション、および説明を示します。

（注）
- この設定では、すでに存在するポリシーが確認されるだけで、変更されません。

- 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 管理者ガイド リリース 2.5*』を参照してください。

表 A-14　Windows Mobile ポリシー

XML タグ名	オプション	説明
MobilePolicy	n/a	グループ ID を判別します。
DeviceLockRequired	n/a	グループ ID。MobilePolicy グループの DeviceLockRequired は、VPN 接続を確立する前に、パスワードまたは PIN を使用して Windows Mobile デバイスを設定する必要があることを示します。この設定が有効なのは、Microsoft のデフォルト ローカル認証プロバイダー（LAP）を使用する Windows Mobile デバイスだけです。 **（注）** AnyConnect クライアントは、Windows Mobile 5.0、WM5AKU2+、および Windows Mobile 6.0 でモバイル デバイス ロックをサポートしますが、Windows Mobile 6.1 ではサポートしません。
MaximumTimeoutMinutes	任意の負ではない整数	DeviceLockRequired グループのこのパラメータに負ではない数値が設定された場合、設定が必要な、デバイス ロックが有効になるまでの最大時間を分単位で指定します。
MinimumPasswordLength	任意の負ではない整数	DeviceLockRequired グループのこのパラメータに負ではない数値が設定された場合、デバイス ロックに使用する PIN またはパスワードの文字数が、指定された数値以上必要であることを示します。 この設定は、強制する前に、Exchange サーバと同期してモバイル デバイスにプッシュする必要があります。（WM5AKU2+）
PasswordComplexity	[アルファ（alpha）]：英数字のパスワードが必要です。 [PIN]：数値の PIN が必要です。 [強力（strong）]：Microsoft の定義による、強い英数字のパスワードが必要です。7 文字以上で、大文字、小文字、数字、区切り文字のうち少なくとも 3 種類が含まれている必要があります。	指定された場合、左のカラムで示すパスワード サブタイプのチェックが行われます。 この設定は、強制する前に、Exchange サーバと同期してモバイル デバイスにプッシュする必要があります。（WM5AKU2+）

例：Windows Mobile ポリシー

XML を使用して Windows Mobile ポリシーを設定するには、次の例を参照してください。

```
<MobilePolicy>
<DeviceLockRequired>
    MaximumTimeoutMinutes=”60”
    MinimumPasswordLength=”4”
    PasswordComplexity=”pin”
```

```
</DeviceLockRequired>
</MobilePolicy>
```

起動時自動接続

表 A-15 に、起動時自動接続を設定するためのタグ名、オプション、および説明を示します。

表 A-15　起動時自動接続の設定

XML タグ名	オプション	説明
AutoConnectOnStart	true	自動接続設定を開始します。
	false	デフォルトの自動接続設定に戻します。
AutoConnectOnStart UserControllable	true	ユーザ制御属性を挿入します。
	false	ユーザ制御属性を削除します。

例：起動時自動接続
起動時自動接続を設定するには、次の例を参照してください。

```
<AutoConnectOnStart>
true
</AutoConnectOnStart>
```

自動再接続

表 A-16 に、自動再接続を設定するためのタグ名、オプション、および説明を示します。

表 A-16　自動再接続の設定

XML タグ名	オプション	説明
AutoReconnect	true	VPN セッションが中断された場合、クライアントはセッションに割り当てられたリソースを保持し、再接続を試行します。
	false	VPN セッションが中断された場合、クライアントはセッションに割り当てられたリソースを解放し、再接続を試行しません。
AutoReconnectBehavior	DisconnectOnSuspend	AnyConnect はシステムが一時停止したときに VPN セッションに割り当てられたリソースを解放し、システムがレジュームした後で再接続を試行しません。
	ReconnectAfterResume	クライアントは、システムの一時停止中に、VPN セッションに割り当てられたリソースを保持します。システムのレジューム後に、再接続を試行します。

例：自動再接続
クライアントの初期化セクションでの AnyConnect VPN の再接続動作を設定するには、以下の例を参照してください。

```
<AutoReconnect UserControllable="true">true
<AutoReconnectBehavior
UserControllable="true">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

サーバ リスト

表 A-17 に、サーバ リストを設定するためのタグ名、オプション、および説明を示します。

表 A-17　サーバ リストの設定

XML タグ名	オプション	説明
ServerList	n/a	グループ ID を指定します。
HostEntry	n/a	グループ ID。ServerList の子パラメータ。特定のホストへの接続を試行するために必要なデータです。
HostName	ホストを参照するために使用されるエイリアス、FQDN、または IP アドレス。これが FQDN または IP アドレスの場合、HostAddress は必要ありません。	HostEntry グループの HostName パラメータは、サーバ リスト内でホスト名を指定します。
HostAddress	ホストを参照するために使用される IP アドレスまたは完全修飾ドメイン名（FQDN）。HostName が FQDN または IP アドレスの場合、HostAddress は必要ありません。	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を選択します。
PrimaryProtocol	SSL または IPsec	VPN トンネルの暗号化プロトコルは、SSL（デフォルト）または IPsec（IKEv2）のいずれか。 IPsec の場合、クライアントはデフォルトで独自の AnyConnect EAP 認証方式を使用します。
StandardAuthenticationOnly	n/a	StandardAuthenticationOnly パラメータを使用して、認証方式をデフォルトのプロパティ AnyConnect EAP の認証方式から標準ベースの方式に変更します。 この方式に変更すると、クライアントのダイナミック ダウンロード機能が制限され、一部の機能がディセーブルになります。また、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 プロキシ設定などを設定する ASA の機能がディセーブルになることに注意してください。
AuthMethodDuringIKENegotiation	IKE-RSA、EAP-MD5、EAP-MSCHAPv2、EAP-GTC	標準ベース認証の認証方式を指定します。

表 A-17　サーバ リストの設定

XML タグ名	オプション	説明
IKEIdentity	英数字文字列。	標準ベースの EAP 認証方式を選択する場合、このフィールドにクライアント ID としてグループまたはドメインを入力できます。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。 文字列に、ターミネータ（たとえば、null または CR）を含めることはできません。
UserGroup	指定されたホストに接続するときに使用する接続プロファイル（トンネル グループ）。 このパラメータはオプションです。	このオプションが存在する場合は、HostAddress とともに使用してグループベースの URL を形成します。 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。 **（注）** グループ ベースの URL をサポートするには、ASA バージョン 8.0.3 以降が必要です。

例：サーバ リスト
サーバ リストを設定するには、次の例を参照してください。

```
<ServerList>
    <HostEntry>
        <HostName>ASA-01</HostName>
        <HostAddress>cvc-asa01.cisco.com
         </HostAddress>
    </HostEntry>
    <HostEntry>
        <HostName>ASA-02</HostName>
         <HostAddress>cvc-asa02.cisco.com
         </HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa03.cisco.com
            </HostAddress>
         </BackupServerList>
    </HostEntry>
</ServerList>
```

スクリプト化

表 A-18 に、スクリプトを設定するためのタグ名、オプション、および説明を示します。

表 A-18　スクリプトの設定

XML タグ名	オプション	説明
EnableScripting	true	OnConnect スクリプトおよび OnDisconnect スクリプトがあれば、起動します。
	false	（デフォルト）スクリプトを起動しません。
UserControllable	true	ユーザが OnConnect スクリプトおよび OnDisconnect スクリプトの実行を、イネーブルまたはディセーブルにできます。
	false	（デフォルト）ユーザがスクリプト機能を制御できません。
TerminateScriptOnNextEvent	true	別のスクリプト処理可能なイベントへの移行が発生した場合に、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 は実行中の OnConnect スクリプトを終了します。AnyConnect が新しい VPN セッションを開始すると、実行中の OnDisconnect スクリプトを終了します。Microsoft Windows では、AnyConnect は OnConnect スクリプトまたは OnDisconnect スクリプトが起動した任意のスクリプトと、そのすべての従属スクリプトも終了します。Mac OS および Linux では、AnyConnect は OnConnect スクリプトまたは OnDisconnect スクリプトだけを終了し、子スクリプトは終了しません。
	false	（デフォルト）別のスクリプト処理可能なイベントへの移行が発生しても、スクリプト プロセスを終了しません。
EnablePostSBLOnConnectScript	true	SBL が VPN セッションを確立したときに、OnConnect スクリプトを起動しません。
	false	（デフォルト）SBL が VPN セッションを確立したときに OnConnect スクリプトが存在する場合、OnConnect スクリプトを起動する。

例：スクリプト化

スクリプトを設定するには、次の例を参照してください。

```
<ClientInitialization>

<EnableScripting>true</EnableScripting>

</ClientInitialization>
```

この例では、スクリプトをイネーブルにし、その他のスクリプト パラメータのデフォルト オプションを上書きします。

```
<ClientInitialization>

<EnableScripting UserControllable="true">true
    <TerminateScriptOnNextEvent>true</TerminateScriptOnNextEvent>
    <EnablePostSBLOnConnectScript>false</EnablePostSBLOnConnectScript>
</EnableScripting>

</ClientInitialization>
```

認証タイムアウト コントロール

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。

表 A-19 に、認証タイマーを変更するためのタグ名、オプション、および説明を示します。

表 A-19　認証タイムアウト コントロール

XML タグ名	オプション	説明
AuthenticationTimeout	10 ～ 120 までの整数	このタイマを変更するには、時間を秒数で入力してください。

例：認証タイムアウト コントロール
次の例では、認証タイムアウトを 20 秒に変更しています。

```
<ClientInitialization>
    <AuthenticationTimeout>20</AuthenticationTimeout>
</ClientInitialization>
```

プロキシの無視

表 A-20 に、プロキシの無視を設定するためのタグ名、オプション、および説明を示します。

表 A-20　プロキシの無視の設定

XML タグ名	オプション	説明
ProxySettings	IgnoreProxy	プロキシの無視をイネーブルにします。
	native	サポートされていません。
	override	サポートされていません。

例：プロキシの無視
クライアントの初期化セクションでプロキシの無視を設定するには、次の例を参照してください。

```
<ProxySettings>IgnoreProxy</ProxySettings>
```

Windows ユーザのための、RDP セッションからの AnyConnect セッションの許可

表 A-21 に、RDP セッションを設定するためのタグ名、オプション、および説明を示します。

表 A-21　RDP セッションからの AnyConnect セッションの許可

XML タグ名	オプション	説明
WindowsLogonEnforcement	SingleLocalLogon	VPN 接続の全体で、ログインできるローカル ユーザは 1 人だけです。この設定では、1 人以上のリモート ユーザがクライアント PC にログオンしているときに、ローカル ユーザが VPN 接続を確立できます。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 ログオ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 ログオ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決まります。SingleLocalLogin 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。
	SingleLogon	VPN 接続の全体で、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、その VPN 接続は終了します。
WindowsVPNEstablishment	LocalUsersOnly	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 クライアントの機能と同じ機能です。
	AllowRemoteUsers	リモート ユーザが 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、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。

例：Windows ユーザのための、RDP セッションからの AnyConnect セッションの許可
RDP セッションから AnyConnect セッションを設定するには、次の例を参照してください。

```
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>

<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
```

L2TP または PPTP を介した AnyConnect

表 A-22 に、L2TP または PPTP を介した AnyConnect を設定するためのタグ名、オプション、および説明を示します。

表 A-22　L2TP または PPTP を介した AnyConnect

XML タグ名	オプション	説明
PPPExclusion	automatic	PPP 除外をイネーブルにします。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。
	override	これも、PPP 除外をイネーブルにします。自動検知による PPP サーバの IP アドレスの取得に失敗し、PPPExclusion UserControllable 値が true の場合は、「ユーザによる PPP 除外の上書き」（P.3-73）の手順に従ってください。
	disabled	PPP 除外を適用しません。

表 A-22　L2TP または PPTP を介した AnyConnect

XML タグ名	オプション	説明
PPPExclusionServerIP	true	PPP サーバの IP アドレスを使用します。
	false	PPP サーバの IP アドレスを使用しません。
PPPExclusion UserControllable=	true	ユーザが PPP 除外設定の読み取りおよび変更を実行できます。
	false	ユーザは PPP 除外設定を表示および変更できません。

例：AnyConnect over L2TP または PPTP
AnyConnect over L2TP または PPTP を設定するには、次の例を参照してください。

```
<ClientInitialization>
    <PPPExclusion UserControllable="true">Automatic
        <PPPExclusionServerIP UserControllable="true">127.0.0.1</PPPExclusionServerIP>
    </PPPExclusion>
    </ClientInitialization>
        <ServerList>
        <HostEntry>
            <HostName>DomainNameofASA</HostName>
            <HostAddress>IPaddressOfASA</HostAddress>
        </HostEntry>
         </ServerList>
</AnyConnectProfile>
```

その他の AnyConnect プロファイル設定

表 A-23 に、ClientInitialization セクションに挿入できるその他のパラメータを示します。

表 A-23　その他の AnyConnect プロファイル設定

XML タグ名	オプション	説明
CertificateStoreOverride	true	管理者は、Windows コンピュータの証明書ストアの証明書を検索するよう AnyConnect に指示できます。このタグは、証明書がこのストアに格納されていて、ユーザがデバイスに対して管理者特権を持っていないときに有効になります。マシン証明書を使用して Windows 7 または VISTA に接続するには、このオプションがイネーブルにされている事前に展開されたプロファイルが必要です。接続する前に Windows 7 または VISTA の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。
	false	（デフォルト）AnyConnect は Windows コンピュータの証明書ストア内の証明書を検索しません。
ShowPreConnectMessage	true	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。
	false	（デフォルト）ユーザが初めて接続を試行する前にメッセージが表示されません。

表 A-23　その他の AnyConnect プロファイル設定

XML タグ名	オプション	説明
MinimizeOnConnect	true	（デフォルト）VPN トンネルが確立されているときの AnyConnect GUI の動作を制御します。デフォルトでは、VPN トンネルが確立されているときには、GUI は最小化されます。
	false	AnyConnect GUI の動作は制御されません。
LocalLanAccess	true	ローカル LAN アクセスがセキュア ゲートウェイ上のリモート クライアントに対してイネーブルのとき、ユーザはローカル LAN アクセスを受け入れるか、あるいは拒否することができます。
	false	（デフォルト）ローカル LAN アクセスを拒否します。
AutoUpdate	true	（デフォルト）新規パッケージを自動的にインストールします。
	false	新規パッケージをインストールしません。
RSASecurIDIntegration	automatic	（デフォルト）管理者は、ユーザと RSA との相互作用方法を制御できます。デフォルトでは、AnyConnect が RSA の適切な相互作用方法を決定します。管理者は RSA をロックするか、ユーザが制御できるようにすることができます。
	software token	
	hardware token	
RetainVPNOnLogoff	true	ユーザが Windows オペレーティング システムをログオフしたときに、VPN セッションを保持します。
	false	（デフォルト）ユーザが Windows オペレーティング システムをログオフすると、VPN セッションを停止します。
UserEnforcement	AnyUser	別のユーザがログオンしても、VPN セッションを続行します。RetainVPNPnLogoff が true で、VPN セッションがアップ状態のときにの元のユーザが Windows をログオフした場合にのみ、この値が適用されます。
	SameUserOnly	別のユーザがログオンすると、VPN セッションを終了します。

APPENDIX B

テレメトリ XML リファレンス

この付録では、テレメトリ クライアント プロファイルで使用される XML 要素について説明します。テレメトリ クライアント プロファイルのトラブルシューティングを行う場合、または ASDM 6.4(1) にアップグレードしておらず、AnyConnect プロファイル エディタ ツールの使用経験がない場合に、この付録を参照してください。

ASDM 6.4(1) にアップグレードしている場合、プレーン テキストや XML エディタを使用してプロファイル ファイルを編集するよりも、AnyConnect プロファイル エディタを使用して、AnyConnect クライアント プロファイルを作成および保守することを強く推奨します。AnyConnect プロファイル エディタでは、独自のオンライン ヘルプを利用できます。

AnyConnect テレメトリ モジュール、クライアント プロファイル、および機能の詳細については「WSA に対する AnyConnect テレメトリの設定」（P.7-1）を参照してください。表 B-1 では、AnyConnect テレメトリ クライアント プロファイルの設定に使用される XML タグ名、オプション、説明、およびコード例が示されています。プロファイルで値が指定されていない場合、AnyConnect はデフォルト値を使用します。

actsettings.xml ファイルに、デフォルトのテレメトリ クライアント プロファイル設定が指定されています。*telemetry_profile*.tsp ファイルのパラメータは、actsettings.xml ファイルで指定されるパラメータに優先されます。*telemetry_profile*.tsp ファイルの詳細については、「テレメトリ クライアント プロファイルの設定」（P.7-10）を参照してください。

サービス ステータス要求への応答として WSA によって送信されるテレメトリ クライアント プロファイル パラメータは、*telemetry_profile*.tsp ファイルで指定されたパラメータに優先します。テレメトリ モジュールには、エンドポイントのレジストリにおける WSA 設定が保存されます。テレメトリ モジュールは、WAS から新しい設定を受信すると、レジストリを更新します。これにより、テレメトリ モジュールは、アクティブな VPN セッションがないときにも、同じ設定を使用できます。

（注） サービス ステータス要求への応答として WSA によって送信されるパラメータは、WSA リリース 7.1 以降で設定されます。

注意 本書の例をカット アンド ペーストしないでください。カット アンド ペーストすると、改行が入り、XML が機能しなくなることがあります。代わりに、プロファイル テンプレート ファイルをテキスト エディタ（メモ帳やワードパッドなど）で開いてください。

表 B-1　XML 設定ファイルで定義されるテレメトリ パラメータ

要素名	説明	範囲	デフォルト値	プロファイル エディタまたは ASDM で指定	WSA で指定
テレメトリ	すべてのテレメトリ モジュール要素の親要素				
ServiceDisable	テレメトリ サービスをイネーブルまたはディセーブルにします	false true	false テレメトリ プロファイルを編集および保存した後は、テレメトリはデフォルトでイネーブルになります	Yes	No
MaxHistLog	アクティビティ履歴リポジトリの最大サイズ	2 ～ 1000 （MB）	100	Yes	No
MaxHistDays	アクティビティ履歴を保持する最大日数	1 ～ 1000 （日）	180	Yes	No
AvCheckInterval	新規アンチウイルス通知を確認する間隔	5 ～ 300 （秒）	60	Yes	No
PostRetries	レポート ポスティングまたはサービス チェックが失敗した場合の再転送の試行回数	0 ～ 10 （時間）	2	Yes	No
NewKeyInterval	内部および外部 AES キーを変更する間隔 （0 はサービス開始時にのみ変更することを意味します）	0 ～ 24 （時間）	0	Yes	No
ExemptFromHooking	テレメトリ レポートから除外されるアプリケーション ファイル名またはアプリケーション ファイル名へのパスを含む <AppName> 要素のリストを示します	なし～無制限	なし	Yes	No
AppName	テレメトリ レポートから除外されるアプリケーション ファイル名またはアプリケーション ファイル名へのパスを示します <ExemptFromHooking> の子要素	なし～ 256 （バイト）	なし	No	
CiscoCert	外部 AES キーを暗号化するための公開キーを使用するシスコの証明書	なし～ 4 （KB）	なし	No	No

要素名	説明	範囲	デフォルト値	プロファイル エディタまたは ASDM で指定	WSA で指定
CustCert	内部 AES キーを暗号化するため、および外部 AES キーを暗号化するための公開キーを使用したユーザの証明書 これは、PEM 証明書タイプである必要があります	なし～ 4（KB）	なし	Yes	No
MaxPayLoad	レポート ポスティング要求の最大ペイロード長	1024 ～ 65535（KB）	10240 KB	No	Yes
ServiceHost	AnyConnect Secure Mobility サービス ポータルの名前	なし～ 1（KB）	mus.cisco.com	No	No
ServiceProxy	ポスティング レポートの「proxy:port」という形式のプロキシ サーバ名とポート	なし～ 1（KB）	なし	No	No
OptIn	AnyConnect Secure Mobility または Telemetry 機能のイネーブル	Yes または No	No	No	Yes
ServiceName	AnyConnect Secure Mobility サービス名を指定	なし～ 1（KB）	TelemetryReport	No	No
RelativeURL	レポート ポスティングの AnyConnect Secure Mobility サービスの相対 URL	なし～ 1（KB）	TelemetryReport	No	Yes
DetailLevel	URL をレポートする詳細レベル（**Standard** は完全な URL を示します。**Limited** はすべてのパス コンポーネントのストア ホスト名およびドメイン名を示します）	Standard または Limited	Limited	No	Yes
ExcludedDoamin	内部 URL のドメイン名を指定する <Domain> 要素のリストを示します	なし～無制限	なし	No	Yes
Domain	テレメトリ レポートから除外される内部 URL を示します。例：**cisco.com** <ExcludedDomain> の子要素	なし～ 1（KB）	なし	No	Yes

要素名	説明	範囲	デフォルト値	プロファイル エディタまたは ASDM で指定	WSA で指定
DebugLevel	ログ メッセージの詳細レベル 0：エラーのみ 1：警告 2：状態 3：情報 4：デバッグ 5：すべて	0 ～ 5	1	No	No
ACTuserDebugLevel	フッキング DLL のデバッグ レベル（actuser.dll） 0：ログなし 1：デバッグ ログ	0 ～ 1	0	No	no

例：AnyConnect テレメトリ クライアント プロファイル

```
Refer to the following example to configure AnyConnect Telemetry:
<?xml version="1.0" encoding="UTF-8"?>
<Telemetry>
        <ServiceDisable>false</ServiceDisable>
        <MaxHistLog>100</MaxHistLog>
        <MaxHistDays>180</MaxHistDays>
        <AvCheckInterval>60</AvCheckInterval>
        <PostRetries>2</PostRetries>
        <ExemptFromHooking>
                <AppName>C:\Program Files\Cisco\CSAgent\bin\okclient.exe</AppName>
        </ExemptFromHooking>
        <CustCert>
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBIQDO5BLlnIfNvuctLkunNIIlNNqB8AYW2X1CQ2UBd0IfJVjquf22
p1UoOUmPx1KqA2zWdqfUzVUqUQUCdZuVw+kWkXOMLVz7lNLpEjmU1PAOoqLeqoUe
NY3IzKInvLIzUQA6oOb8kvCPlN7n7mvjqC6wwvqjJaQCUYbL2/c/4qbIKQIDAQAB
AoIAqIQTjqc7Mlqv2222dOEpQoYtax8ywIqV/q3XQ4U2pOm7wULqLxIU+yIIj/dx
qT6ZIE80jLInUl2W7n1/7vCtylEIqzxKIwJAIOZf+q58KotInzPyIYITAAYU27Tf
qnoICOolwZYiDeXUCA7CWJXLm27oDqF5OlI+ImaUIeqyOUc8cZoUUUXtIQJBAM2J
WlDVI2mxxiIfq2ZtbUdpJzbqtwmEmPEnBEn8PqkqZndY1xdWW3JIuaIl7qQwwO2I
cDbUyM/mtVNvdMDKCjmCQQDTaJUkvB0LED51JIO3KmU8LIQq+4Mamej+qFIZVYiy
cFKfI+U0wqfIo4LILzP78OW4E2OmeaWqmza7VLC4aUUF
-----END RSA PRIVATE KEY-----
        </CustCert>
</Telemetry>
```

APPENDIX C

ユーザ ガイドラインのやりとり

VPN ユーザと次のガイドラインをやりとりするようにしてください。また、ユーザからガイドラインを求められたときに、この項を参考にしてください。内容は、次のとおりです。

Apple MobileMe と AnyConnect との競合

MobileMe のユーザが「Back to my Mac」を設定している場合、AnyConnect の接続問題が発生します。AnyConnect と MobileME の両方が「utun0」という名前の仮想アダプタを使用します。MobileMe は、コンピュータのブート時に AnyConnect よりも前に起動されるため、常に utun0 インターフェイスが最初に使用され、これが原因で Cisco AnyConnect が失敗します。いずれのアプリケーションも、「utun1」などの別のインターフェイスを使用するように設定できません。

Mac ユーザは、AnyConnect VPN に接続する前に「Back to my Mac」をオフにする必要があります。VPN への接続後に、「Back to my Mac」を再度イネーブルにできます。

Mac OS X 10.5 での TUN/TAP エラー メッセージへの対応

Mac OS X 10.5 以前のバージョンに AnyConnect をインストールするときに、次のエラー メッセージが表示されることがあります。

```
A version of the TUN virtual network driver is already installed on this system that is
incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and
prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your
System Administrator, or reference the AnyConnect Release Notes for assistance in
resolving this issue.
```

Mac OS X 10.6 ではこの問題は解決されています。AnyConnect で必要なバージョンの TUN/TAP 仮想ネットワーク ドライバが提供されているためです。

10.6 よりも前のバージョンの Mac OS X には、TUN/TAP 仮想ネットワーク ドライバは組み込まれていないため、AnyConnect は、これらのオペレーティング システムに独自のドライバをインストールします。ただし、Parallels などの一部のソフトウェア、データ カードを管理するソフトウェア、および一部の VPN アプリケーションは、独自の TUN/TAP ドライバをインストールします。AnyConnect インストール ソフトウェアでは、ドライバがすでに存在するという理由で上記のエラー メッセージが表示されますが、そのドライバのバージョンは AnyConnect とは互換性がありません。

AnyConnect をインストールするには、TUN/TAP 仮想ネットワーク ドライバを削除する必要があります。

（注）　TUN/TAP 仮想ネットワーク ドライバを削除すると、システムで最初にドライバをインストールしたソフトウェアに問題が発生するおそれがあります。

TUN/TAP 仮想ネットワーク ドライバを削除するには、コンソール アプリケーションを開き、次のコマンドを入力します。

sudo rm -rf /Library/Extensions/tap.kext

sudo rm -rf /Library/Extensions/tun.kext

sudo rm -rf /Library/StartupItems/tap

sudo rm -rf /Library/StartupItems/tun

sudo rm -rf /System/Library/Extensions/tun.kext

sudo rm -rf /System/Library/Extensions/tap.kext

sudo rm -rf /System/Library/StartupItems/tap

sudo rm -rf /System/Library/StartupItems/tun

これらのコマンドの入力後に、Mac OS を再起動してから、AnyConnect を再インストールします。

未対応 64 ビット版 Internet Explorer

WebLaunch からの AnyConnect のインストールでは 64 ビット版の Internet Explorer はサポートされていません。Windows on x64（64 ビット版）を使用している場合、32 ビット版の Internet Explorer または Firefox を使用して WebLaunch をインストールしてください。現時点では、Firefox は 32 ビット版でのみ使用できます。

Wireless Hosted Network の回避

Windows 7 Wireless Hosted Network 機能を使用すると AnyConnect が不安定になるおそれがあります。AnyConnect の使用時には、この機能をイネーブルにしたり、この機能をイネーブルにするフロントエンド アプリケーション（Connectify や Virtual Router など）を実行したりすることはお勧めしません。

Start Before Logon および DART のインストール

Start Before Logon コンポーネントでは、最初に AnyConnect をインストールしておく必要があります。

SBL または DART が接続しているエンドポイントから手動でアンインストールされている場合、これらのコンポーネントは再インストールされます。ヘッドエンド設定でこれらのコンポーネントのインストールが指定されていて、（エンドポイントに設定されている）プリファレンスでアップグレードが許可されている場合のみ、この動作が発生します。

検疫状態への対応

アクセスに関して企業のポリシーに準拠しないエンドポイントのネットワーク ステータスは、AnyConnect の [接続（Connection）] タブで [隔離済み（Quarantined）] と表示されます。

通常、検疫されたセッションに適用されるダイナミック アクセス ポリシーに割り当てられた ACL では、アンチウイルスおよびアンチスパイウェアのアップデートなど修復サービスへのアクセスのみ許可されます。

検疫状態のセッションでは、エンドポイントの修復に十分な時間が必要です。この時間に続き、ユーザは [再接続（Reconnect）] をクリックし、その状態を終了し新しいポスチャ アセスメントを開始する必要があります。

AnyConnect CLI コマンドを使用した接続

Cisco AnyConnect VPN Client には、グラフィカル ユーザ インターフェイスを使用せずにクライアント コマンドを入力することを希望するユーザ向けに、コマンドライン インターフェイス（CLI）があります。ここでは、CLI コマンド プロンプトの起動方法および CLI で使用可能なコマンドについて説明します。

「クライアント CLI プロンプトの起動」（P.C-3）

「クライアント CLI コマンドの使用」（P.C-3）

「ASA によるセッションの終了時に Windows ポップアップ メッセージを防ぐ」（P.C-5）

クライアント CLI プロンプトの起動

CLI コマンド プロンプトを起動するには、次の手順を実行します。

Windows の場合 : Windows フォルダ C:\Program Files\Cisco\Cisco AnyConnect VPN Client でファイル *vpncli.exe* を見つけます。ファイル *vpncli.exe* をダブルクリックします。

Linux および Mac OS X の場合：フォルダ /opt/cisco/anyconnect/bin/ でファイル ***vpn*** を見つけます。ファイル ***vpn*** **を実行します。**

クライアント CLI コマンドの使用

インタラクティブ モードで CLI を実行する場合、独自のプロンプトが表示されます。コマンド ラインを使用することもできます。表 3-1 に、CLI コマンドを示します。

表 3-1　AnyConnect クライアント CLI コマンド

コマンド	アクション
connect *IP address or alias*	特定の ASA への接続を確立します。
disconnect	前に確立した接続を閉じます。
stats	確立した接続に関する統計情報を表示します。
quit	CLI インタラクティブ モードを終了します。
exit	CLI インタラクティブ モードを終了します。

次の例は、ユーザがコマンド ラインから接続を確立し、終了する例です。

Windows

connect 209.165.200.224
アドレスが 209.165.200.224. のセキュリティ アプライアンスへの接続を確立します。要求されたホストに接続した後、AnyConnect クライアントは、ユーザが属するグループを表示し、ユーザのユーザ名とパスワードを要求します。オプションのバナーを表示するよう指定されている場合、ユーザはバナーに応答する必要があります。デフォルトの応答は **n** で、接続試行を終了します。次に、例を示します。

```
VPN> connect 209.165.200.224
    >>contacting host (209.165.200.224) for login information...
    >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
    >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
    >> notice: Authentication succeeded. Checking for updates...
    >> state: Connecting
    >> notice: Establishing connection to 209.165.200.224.
    >> State: Connected
    >> notice: VPN session established.
VPN>
```

stats
現在の接続の統計情報を表示します。次の例を参考にしてください。

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None

[ Data Transfer ]

    Bytes (sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
```

```
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect
前に確立した接続を閉じます。次の例を参考にしてください。

```
VPN> disconnect
    >> state: Disconnecting
    >> state: Disconnected
    >> notice: VPN session ended.
VPN>
```

quit または **exit**

どちらかのコマンドで、CLI のインタラクティブ モードを終了します。次の例を参考にしてください。

```
quit
goodbye
    >>state: Disconnected
```

Linux または Mac OS X

/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
アドレスが *1.2.3.4* の ASA への接続を確立します。

/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
プロファイルを読み込み、エイリアス *some_asa_alias* を検索してアドレスを探し、ASA への接続を確立します。

/opt/cisco/anyconnect/bin/vpn stats
VPN 接続に関する統計情報を表示します。

/opt/cisco/anyconnect/bin/vpn disconnect
VPN セッションがある場合、接続解除します。

ASA によるセッションの終了時に Windows ポップアップ メッセージを防ぐ

ASA から session reset を発行して AnyConnect セッションを終了すると、次の Windows ポップアップ メッセージがエンド ユーザに表示されます。

```
The secure gateway has terminated the vpn connection. The following message was
received for the gateway: Administrator Reset
```

このメッセージが表示されるのは望ましくないことがあります。たとえば、CLI コマンドを使用して VPN トンネルを開始するときです。クライアントへの接続後にクライアント CLI を再起動することで、このメッセージが表示されるのを防止できます。次に、この作業の実行時の CLI 出力例を示します。

```
C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 3.0.1).
Copyright (c) 2004 - 2011 Cisco Systems, Inc.
All Rights Reserved.
  >> state: Connected
```

```
  >> state: Connected
  >> notice: Connected to asa.cisco.com.
  >> notice: Connected to asa.cisco.com.
  >> registered with local VPN subsystem.
  >> state: Connected
  >> notice: Connected to asa.cisco.com.
  >> state: Disconnecting
  >> notice: Disconnect in progress, please wait...
  >> state: Disconnected
  >> notice: On a trusted network.
  >> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

または、次の場所にあるエンドポイント デバイスでは、Windows レジストリに SuppressModalDialogs という名前の 32 ビットの倍精度値を作成できます。クライアントは名前の有無を検査しますが、値は無視します。

- 64 ビット Windows :

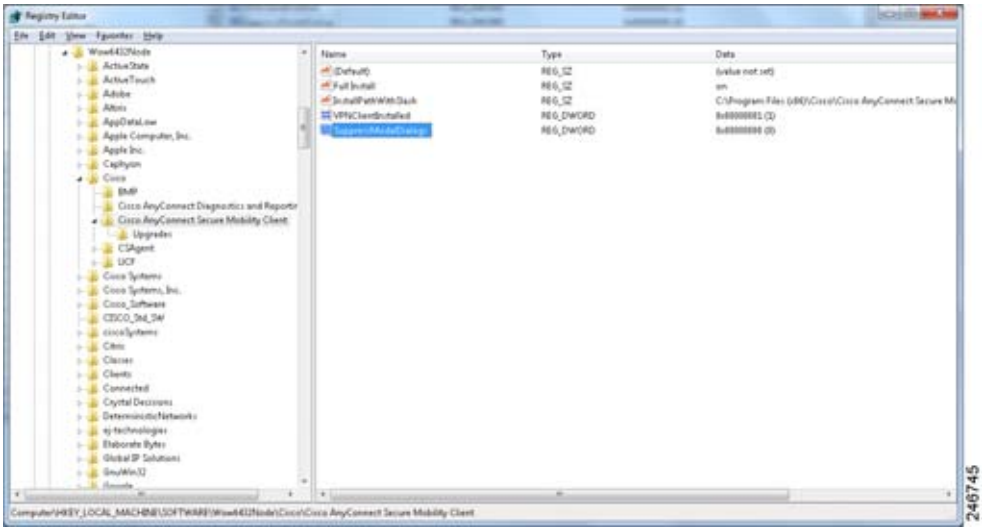
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\
  Cisco AnyConnect Secure Mobility Client

- 32 ビット Windows :

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

図 C-1 に、64 ビット Windows のレジストリ値を示します。

図 C-1　Windows ポップアップ メッセージを抑制するためのレジストリ値



セキュア接続（Lock）アイコンの設定

Lock アイコンは、セキュアな接続を示しています。Windows XP では、このアイコンは最近使用されていない他のアイコンと同様に自動的に非表示になります。Windows XP でこのアイコンが非表示にされないようにするには、次の手順に従ってください。

ステップ 1　トレイ アイコンが表示されたタスクバーの、かぎカッコ（<）を右クリックします。

ステップ 2　[通知のカスタマイズ...（Customize Notifications...）] を選択します。

ステップ 3　[Cisco Systems AnyConnect VPN Client] を選択し、[常に表示（Always Show）] に設定します。

Internet Explorer の [接続（Connections）] タブを非表示にする AnyConnect

ある条件では、Internet Explorer の [ツール（Tools）]、[インターネット オプション（Internet Options）] にある [接続（Connections）] タブが非表示になります。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックは接続解除すると反転され、このタブに関する管理者定義のポリシーの方が優先されます。このロックは、次のいずれかの条件で行われます。

- ASA の設定で、[接続（Connections）] タブのロックが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。
- Windows のグループ ポリシーにより、以前に [接続（Connections）] タブがロックされている（**no lockdown** ASA グループ ポリシー設定の上書き）。

Windows Remote Desktop の使用

次の 3 つの方法のうちいずれかを使用して、ネットワーク コンピュータでネットワーク アクセス マネージャによって接続を管理しているときに、そのネットワーク コンピュータにリモートでアクセスできます。

- マシンのみの認証を使用したネットワーク プロファイル
- マシンおよびユーザ認証を使用したネットワーク プロファイル
- ユーザのみの認証を使用したネットワーク プロファイル

マシンのみの認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをマシン認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。ユーザがリモートでログインすると、ネットワーク アクセス マネージャは、マシンのクレデンシャルで認証されたままになります。ユーザのクレデンシャルでの認証またはマシンのクレデンシャルでの再認証は試行されません。

マシンおよびユーザ認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをマシン認証とユーザ認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。ログインしているユーザがいない場合、ネットワーク アクセス マネージャは、マシンのクレデンシャルで認証します。

Vista または Windows 7 の場合、ローカルまたはリモートでユーザがログインすると、ネットワーク アクセス マネージャ認証では最初のユーザ セッションのみが認証され、最初のセッションが持続している間は後続のログイン セッションが無視されます。最初のログイン セッションが終了したら、ネットワーク アクセス マネージャはユーザ接続を停止し、マシン接続に戻します。ネットワーク アクセス マネージャは、最初のセッションが終了したときにセカンダリ セッションが存在したかどうかにかかわらず、元のセッションがユーザ セッションとして終了した後、最初に成功したログイン試行を追跡します。ネットワーク アクセス マネージャは、最初のセッションが動作している間は後続のログイン セッションを無視するため、元のセッションが破棄されたとき、または後続のログインが試行されたときに、最初のセッションの後に作成されたすべてのセカンダリ セッションの接続が一時的に失われます。最初のユーザがローカルでログインした場合、リモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

（注） 最初のログイン ユーザ セッションのみが AnyConnect GUI にアクセスできます。

Windows XP の場合、ローカルでもリモートでもユーザ セッションの数は 1 に制限されています。そのため、新しいユーザがログインすると必ず前のユーザがログオフします。ユーザがローカルでログインした場合、同一ユーザのリモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

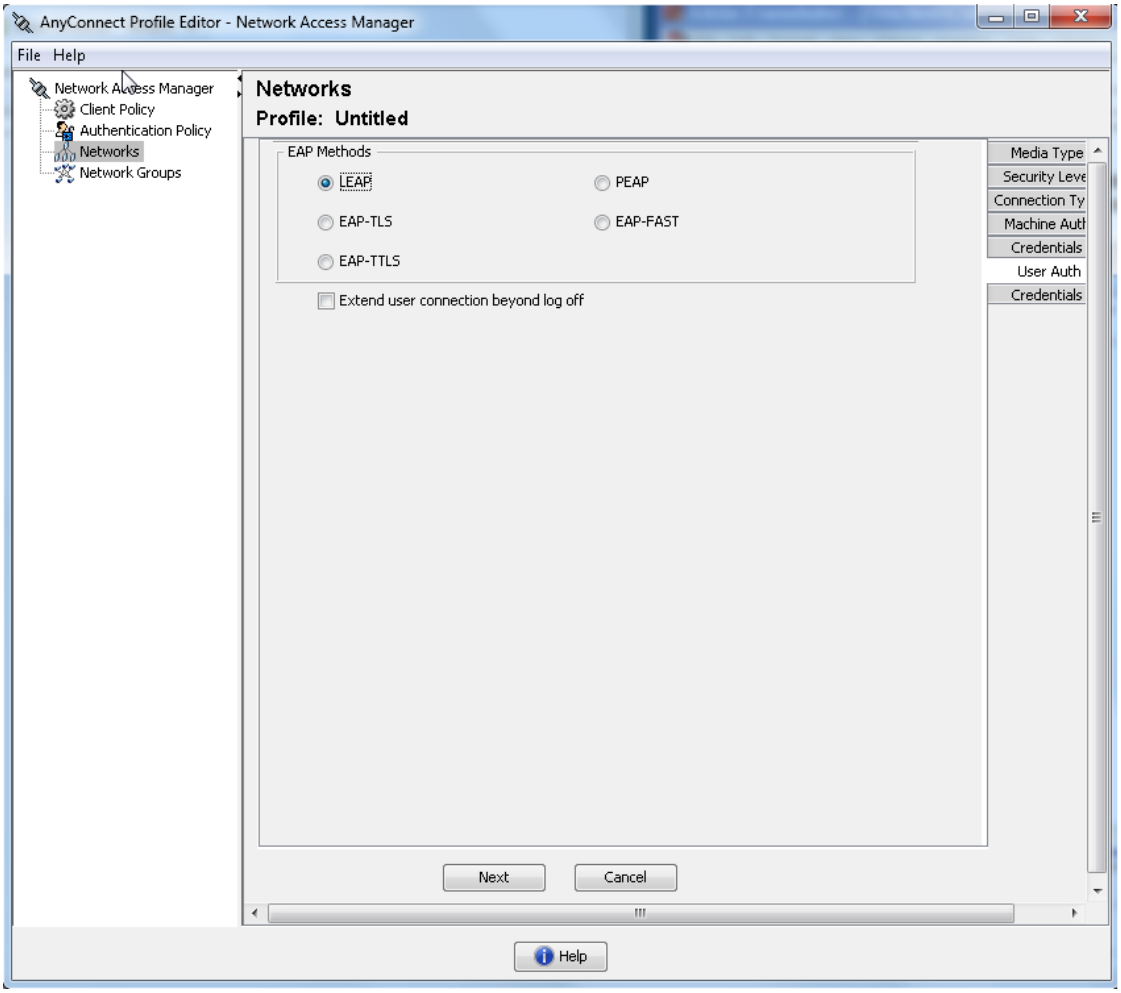
（注） マシン認証とユーザ認証を使用する場合、複雑になる可能性があります。たとえば、設定によっては、マシン プロファイルとユーザ プロファイルは、コンピュータに異なるネットワークを割り当てます（通常は VLAN。ここでは*ユーザ VLAN* と *マシン VLAN* と呼ばれます）。そのため、コンピュータがマシン VLAN 上のマシンとして接続されており（ユーザはログオフ済み）、後からリモートでアクセスされる場合、そのコンピュータはユーザ VLAN として接続します。この理由から、異なる VLAN（ユーザ VLAN）の異なる IP アドレスを使用して、リモート デスクトップ セッションを再確立する必要がある場合があります。

ユーザのみの認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをユーザのみの認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。通常、この設定を使用し、ログインしているユーザがいない場合、ネットワーク アクセス マネージャはネットワーク接続を確立できません。そのため、リモート デスクトップ接続は不可能です。ユーザがログインしたときに、リモート デスクトップ接続を確立できるようになりました。このリモート セッションによってユーザの再認証は行われません。

extendUserConnectionBeyondLogoff パラメータ（図 C-2 を参照）を使用すると、ローカル ユーザがログオフした後でもアクティブ（接続済み）のままになるようにユーザ認証を設定できます。そのため、リモート デスクトップ機能をサポートするためだけの場合、マシン認証は必要ありません。

図 C-2　[ログオフ後もユーザの接続をアクティブなままにする（Extend User Connection Beyond Logoff）] パラメータの GUI の場所



ユーザのログアウト時にクレデンシャルを必要とする再認証が行われて、ネットワーク アクセス マネージャが必要なクレデンシャル（ユーザ証明書など）にアクセスできなくなっている場合、ネットワーク アクセス マネージャは、接続を再認証できません。その結果、認証の試行はタイムアウトになり、オーセンティケータは最終的にクライアントから切断されます。これが発生すると、ネットワーク アクセス マネージャは、使用可能な接続を再評価して、使用可能なマシン接続からネットワーク接続を作成しようとします。

Vista または Windows 7 の場合、ローカルまたはリモートでユーザがログインすると、ネットワーク アクセス マネージャ認証では最初のユーザ セッションのみが認証され、最初のセッションが持続している間は後続のログイン セッションが無視されます。最初のログイン セッションが終了したら、ネットワーク アクセス マネージャはユーザ接続を停止し、マシン接続に戻します。ネットワーク アクセス マネージャは、最初のセッションが終了したときにセカンダリ セッションが存在したかどうかにかかわらず、元のセッションがユーザ セッションとして終了した後、最初に成功したログイン試行を追跡します。ネットワーク アクセス マネージャは、最初のセッションが動作している間は後続のログイン セッションを無視するため、元のセッションが破棄されたとき、または後続のログインが試行されたときに、最初のセッションの後に作成されたすべてのセカンダリ セッションの接続が一時的に失われます。最初のユーザがローカルでログインした場合、リモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

（注）　最初のログイン ユーザ セッションのみが AnyConnect GUI にアクセスできます。

Windows XP の場合、ローカルでもリモートでもユーザ セッションの数は 1 に制限されています。そのため、新しいユーザがログインすると必ず前のユーザがログオフします。ユーザがローカルでログインした場合、同一ユーザのリモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

マシン認証とユーザ認証を使用する場合、複雑になる可能性があります。たとえば、設定によっては、マシン プロファイルとユーザ プロファイルは、コンピュータに異なるネットワークを割り当てます（通常は VLAN。ここではユーザ VLAN とマシン VLAN と呼ばれます）。そのため、コンピュータがマシン VLAN 上のマシンとして接続されており（ユーザはログオフ済み）、後からリモートでアクセスされる場合、そのコンピュータはユーザ VLAN として接続します。この理由から、異なる VLAN（ユーザ VLAN）の異なる IP アドレスを使用して、リモート デスクトップ セッションを再確立する必要がある場合があります。

Microsoft Vista および Win 7 のクレデンシャル プロバイダー

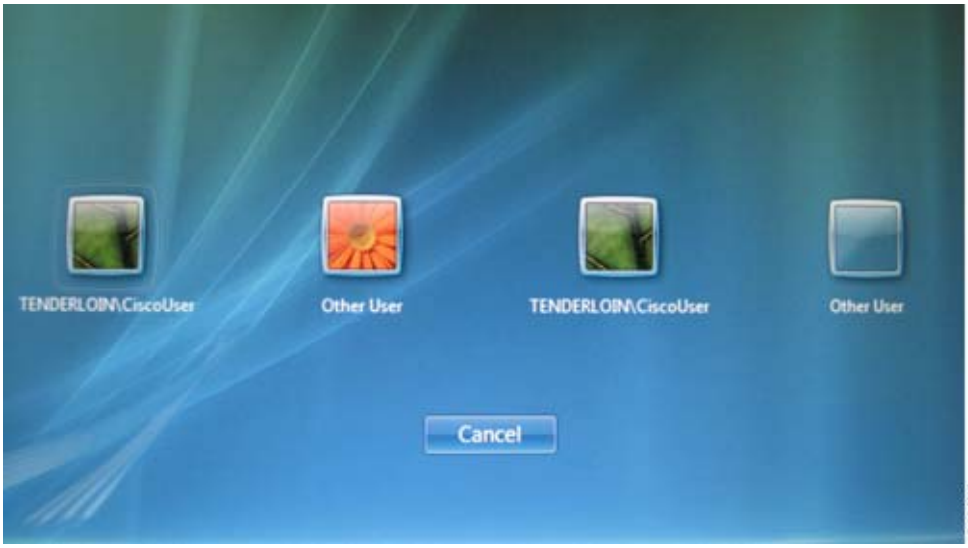
Microsoft Vista および Windows 7 で Windows ログイン クレデンシャルを使用してシングル サインオン（SSO）ユーザ認証を提供するために、ネットワーク アクセス マネージャ モジュールは、パスワード（ログイン）クレデンシャル プロバイダーを実装します。クレデンシャル プロバイダー（CP）は、ログイン プロセス中に Windows クレデンシャルを取り込んで、ネットワーク アクセス マネージャ サービスがマシン認証とユーザ認証を切り替えることができるように、ユーザがシステムにログインしたりシステムからログアウトしたりしたときに通知します。

AnyConnect 3.0 では、ネットワーク アクセス マネージャ CP は、複数のログイン タイル セットが表示されないようにネットワーク アクセス マネージャ CP によってフィルタリングで除外される、Microsoft パスワード クレデンシャル プロバイダーの周囲にラッパーとして実装されます。このフィルタリングが行われない場合、CP ごとにログイン タイルが表示されます。

サードパーティの CP がシステムにインストールされている場合、ネットワーク アクセス マネージャはこれを検出せず、ユーザには複数のログイン タイル セットが表示されることがあります。ユーザがログインのためにサードパーティの CP を選択すると、ネットワーク アクセス マネージャは、Windows クレデンシャルを取得できないため、シングル サインオンのユーザ認証操作を行うことができません。

図 C-3 に、ネットワーク アクセス マネージャ CP とサードパーティ CP の両方をインストールしたシステムからのログイン画面を示します。

図 C-3　オーバーレイなしの AnyConnect アイコン



この問題には、次の 2 つのオプションがあります。

1. ユーザがタイルを区別できるように、ネットワーク アクセス マネージャ CP が、ログイン タイル上に AnyConnect アイコンをオーバーレイするオプションを提供します。小さい AnyConnect アイコンは、ログイン タイル ビットマップの右下隅に配置されます。ユーザにログイン タイル イメージが表示され、AnyConnect がアクティブであることが引き続きわかります。この Anyconnect アイコンがないと、ユーザは、ログイン タイルが AnyConnect によって管理されているかどうかわかりません。

   デフォルトでは、CP は上述のとおり動作します。ユーザは、レジストリで値を変更してディセーブルにでき、CP はログイン タイル上に AnyConnect アイコンをオーバーレイしなくなります。アイコンは、AnyConnect がインストールされていない場合とまったく同じように表示されます。

   このオプションをディセーブルにするには、次のレジストリ値を使用します。

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayIcon]
   ```

   OverLayIcon は REG_DWORD であり、値 0 はオーバーレイ アイコンをディセーブルにし、値 1 はオーバーレイ アイコンをイネーブルにします。このデフォルト値は 1 で、AnyConnect インストーラによって設定されます。レジストリ キーがないか、正しくない場合、CP は値 1 を想定します。

   Windows には、[other users] というラベルのタイルが表示されることがあり、場合によっては関連付けられたタイルには図が表示されません。タイル フレーム内には、タイルが配置されているウィンドウの背景に表示される図が表示されます。そのため、タイルは空であるかトランスペアレントになることがあります。技術的な理由から、CP は、空のタイル上にアイコンをオーバーレイできないため、これが発生した場合 CP は独自のビットマップを提供する必要があります。

   デフォルトでは、CP は、CP 実行可能ファイルに組み込まれたストックのイメージを使用します。ユーザは、図を .bmp ファイルで保存して、ファイルの場所を示すレジストリ文字列値を追加することで、空のストックのタイルの代わりに使用する図を指定できます。

   ビットマップ ファイルの場所を設定するには、次のレジストリ値を追加する必要があります。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
on\Credential Providers\
{B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayEmptyTile]
```

OverlayEmptyTile は、ビットマップ ファイルへのフル パスを含む REG_SZ 値です。
例：「C:\users\jsmith\Pictures\MyEmptyTile.bmp」

（注） ファイルは Windows .bmp ファイルでなければなりません。

（overlayicon レジストリ設定を使用して）オーバーレイがディセーブルになっている場合、OverlayEmptyTile オプションは無視され、ユーザは、アイコン オーバーレイがディセーブルであれば空のタイル ビットマップを指定できません。OverlayEmptyTile 値は AnyConnect インストーラによって指定されません。

図 C-4 に、ネットワーク アクセス マネージャ CP とサードパーティ CP の両方をインストールしたシステムからのログイン画面を示します。この例では、AnyConnect アイコンはログオン タイル上に表示され、ネットワーク アクセス マネージャ CP を示しています。

図 C-4　　オーバーレイを使用した Anyconnect アイコン

2. サードパーティのクレデンシャル プロバイダーのログイン タイルが表示されないようにするには、ネットワーク アクセス マネージャ CP はこれらのタイルをフィルタリングで除外できます。

   このオプションを設定するには、次のレジストリ値を追加する必要があります。

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
   on\Credential Providers\ {B12744B8-5BB7-463a-B85E-BB7627E73002}\Filters]
   ```

   フィルタリングで除外する必要があるすべてのクレデンシャル プロバイダーが、Filters キーに特定の GUID を持つキーとして追加されます。

（注） *Filters* 値は Anyconnect インストーラによって指定されません。

GPO が SSO に対して設定されている場合

GPO ワイヤードまたはワイヤレス プロファイルが SSO に対して設定されている場合、winlogon はクレデンシャル プロバイダーの照会プロセスを省略し、ネットワーク アクセス マネージャ CP に加えてネイティブ L2NA クレデンシャル プロバイダーを直接ロードします。これによって、ユーザに 2 つのタイル セットが表示されます。GPO プロファイルが SSO に対して設定されていない場合、ログイン プロセスは予期したとおりに機能し、Microsoft CP はネットワーク アクセス マネージャ CP によってフィルタリングで除外され、ユーザには単一のタイル セットが表示されます。

SmartCard CP

Microsoft Smartcard Credential Provider はネットワーク アクセス マネージャ CP によってラップされないため、プリログイン スマートカード ベースの証明書認証は、AnyConnect 3.0 用の XP 後のプラットフォームではサポートされません。

ネットワーク アクセス マネージャ CP のプリログイン ステータスの表示

クライアント ポリシーの一部として接続設定値 [Before User Logon] が指定されている場合、ネットワーク アクセス マネージャ CP には、接続ステータスをユーザに通知するためのステータス ダイアログボックスが表示されます。このダイアログボックスは、CP がユーザ クレデンシャルを受け取った後で表示され、接続が正常に行われるか、[Time to Wait Before Allowing User to Logon] で選択された値の期限が切れるまで表示されます。このダイアログボックスはいつでもキャンセルできます。

Windows XP で Internet Explorer を実行する暗号の要件

Windows XP では、Internet Explorer ブラウザは AES を使用できず、RC4 または 3DES のいずれかを必要とします。リモート ユーザが SSL 設定ページで RC4 および 3DES をディセーブルにすると、AnyConnect 接続は失敗します。Internet Explorer を使用して AnyConnect 接続を正常に行うには、リモート ユーザは、IE の SSL 設定で唯一の暗号として AES を指定しないでください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/