Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 3.1

マニュアルの発行日：2012 年 8 月 9 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 リリース 3.1

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』
- ASDM オンライン ヘルプ
- 『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。ダウンロードした後、クライアントは自動的にインストールと設定を行い、ASA への IPsec（IKEv2）または SSL 接続を確立します。

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。

その他のサポート対象モジュール

Cisco AnyConnect Secure Mobility Client バージョン 3.1 は、以下のモジュールを AnyConnect クライアント パッケージに統合します。

- AnyConnect ネットワーク アクセス マネージャ：（以前の Cisco Secure Services Client）このモジュールは、最適なレイヤ 2 アクセス ネットワークを検出して選択し、有線およびワイヤレス ネットワークの両方へのアクセスに対するデバイス認証を実行します。
- AnyConnect ポスチャ アセスメント：AnyConnect Secure Mobility Client に、ASA へのリモート アクセス接続を確立する前に、ホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別する機能を提供します。プリログインの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。ホスト スキャン アプリケーションは、ポスチャ モジュールに同梱される、この情報を収集するアプリケーションです。
- AnyConnect テレメトリ：アンチウイルス ソフトウェアで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 では、このデータを使用して、URL のフィルタリング ルールを改善します。
- AnyConnect Web セキュリティ：HTTP トラフィックを、コンテンツ分析、マルウェアの検出、およびアクセプタブル ユース ポリシーの管理を実行する ScanSafe Web Security スキャン プロキシ サーバにルーティングします。
- AnyConnect 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。
- AnyConnect Start Before Logon（SBL）：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。
- AnyConnect カスタマー エクスペリエンスのフィードバック：ソフトウェアの品質やユーザ エクスペリエンスがさらに改善されるよう、ユーザ エクスペリエンス、クラッシュ インシデントの基本などを探るためのクライアント情報をシスコに提供する機能です。

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

概要

AnyConnect Secure Mobility Client は、VPN セッションおよび Web セキュリティをサポートするためにライセンス アクティベーションを必要とします。必要なライセンスは、使用する AnyConnect VPN Client および Secure Mobility の機能、およびサポートするセッションの数によって異なります。導入には次の AnyConnect ライセンスが 1 つまたは複数必要になる場合があります。

ライセンス	説明	適用先
AnyConnect Essentials	SSL および IPSec VPN 接続用の基本的な AnyConnect 機能をサポートします。このライセンスは、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します。	Cisco ASA 8.0(x) 以降
AnyConnect Premium	AnyConnect Essentials の基本的な機能すべてに加えて、ブラウザ ベースの VPN アクセスなどの Premium AnyConnect クライアント機能、Cisco Secure Desktop、およびホスト スキャン/ポスチャ モジュール機能をサポートします。このライセンスは、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します。このライセンス タイプは共有することもできます。	Cisco ASA 8.0(x) 以降
AnyConnect Mobile	セキュリティ アプライアンスへの AnyConnect モバイル アクセスをサポートします。AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれかの追加として使用できます。追加するには、これらのいずれかが必要です。	Cisco ASA 8.0(x) 以降
AnyConnect Flex	Flex ライセンスは、すべてのライセンスされた機能に対してビジネスの継続性をサポートします。	Cisco ASA 8.0(x) 以降
Advanced Endpoint Assessment	高度なエンドポイント アセスメント機能（自動修復など）を有効にします。アクティブな AnyConnect Premium ライセンスが必要です。	Cisco ASA
Cisco Secure Mobility for AnyConnect	Cisco IronPort Web セキュリティ アプライアンス（WSA）によって提供される Web セキュリティ機能をサポートします。ライセンス名は、ASA 上でアクティブな AnyConnect ライセンス（Essentials または Premium）によって異なります。Cisco IronPort Web セキュリティ アプライアンスのライセンスも必要です。	Cisco WSA 7.0 以降
Cisco Secure Mobility for Cisco Cloud Web Security	AnyConnect Web セキュリティ モジュールのセキュリティ機能をサポートし、ローミング ユーザを Cisco Cloud Web Security（ScanSafe）によって保護します。Cisco Cloud Web Security Web Filtering ライセンスおよび Cisco Cloud Web Security Malware Scanning ライセンスのいずれか一方または両方に加えて、このライセンスが必要です。	

AnyConnect Essentials ライセンスおよび Premium ライセンス

- AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれかを Cisco ASA 8.0(x) 以降でアクティブにできますが、両方のライセンスを同時にアクティブにすることはできません。一部の機能では、機能表に示すように、それ以降の ASA のバージョンが必要です。使用する AnyConnect Secure Mobility 機能に基づきアクティブにするライセンスを選択します。
- AnyConnect 接続に加えて、ASA でアクティブにされた AnyConnect Essentials は、シスコのレガシー VPN クライアントを使用して確立されたセッションをサポートし、企業アプリケーションへフル トンネリング アクセスを行います。クライアントレス VPN アクセスと Cisco Secure Desktop は AnyConnect Essentials ライセンスでは使用できません。
- AnyConnect Premium ライセンスでアクティブにされた ASA は、AnyConnect Essentials ライセンスで許可されたすべてのアクセスと次の AnyConnect Premium 機能をサポートします。
  - クライアントレス VPN アクセス：リモート ユーザはブラウザを使用して VPN セッションを確立でき、特定のアプリケーションはブラウザを使用して、そのセッションにアクセスできます。

- Cisco Secure Desktop：ブラウザベースのセッションと AnyConnect セッションの両方向けです。
- ログイン後の VPN 常時接続：ユーザがコンピュータにログインすると、自動的に VPN セッションを常時接続で確立します。詳細については、VPN 常時接続を参照してください。この機能には、接続失敗ポリシーとキャプティブ 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。

（注）　常時接続は、WSA で Cisco Secure Mobility for AnyConnect ライセンス、ASA で AnyConnect Essentials ライセンスをアクティブにして有効にすることもできます。

- エンドポイント アセスメント：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。

  エンドポイント修復には、以下で説明するように AnyConnect Premium ライセンスの他に Advanced Endpoint Assessment ライセンスが必要です。
- 検疫：Dynamic Access Policies を使用した非準拠 AnyConnect ユーザの検疫。ユーザにカスタム メッセージを通知できます。

- 次には AnyConnect Essentials ライセンスまたは Premium ライセンスのいずれも必要ありません。
  - ネットワーク アクセス マネージャ モジュール。シスコ ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、RADIUS サーバで使用する場合は、無償でライセンスが与えられています。関連するシスコの装置では、現在の SmartNet 契約が必要です。
  - DART モジュールおよびカスタマー フィードバック機能。

AnyConnect Mobile ライセンス

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、AnyConnect 機能には対応していません。AnyConnect Essentials ライセンスまたは AnyConnect Premium 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 3.1 は現在、モバイル デバイスには対応していません。旧バージョンの AnyConnect で動作している Android または Apple iOS デバイスから接続したい場合は、ASA でこのライセンスをアクティブにする必要があります。

AnyConnect Flex ライセンス

AnyConnect Flex ライセンスは、ライセンスを取得した機能に対してのみビジネスの継続性をサポートします。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 日間サポートします。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。

Advanced Endpoint Assessment ライセンス

Advanced Endpoint Assessment ライセンスは、AnyConnect Premium ライセンスとともにアクティブにする必要があります。このライセンスで、エンドポイント修復を開始できます。

エンドポイント修復は、ASA で Dynamic Access Policies（DAPs）による接続ができなくなった場合に開始します。エンドポイント修復は、エンドポイントのアンチウイルス、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、そのソフトウェアのさまざまな側面を修復しようとします。エンドポイント修復が正常に行われると、DAP は以降の接続を許可します。

Cisco Secure Mobility for AnyConnect ライセンス

WSA でアクティブにされた Cisco Secure Mobility for AnyConnect ライセンスは、次のようなブラウザベースの SSL セッションおよび AnyConnect VPN セッションのサービスを提供します。

- マルウェア防御
- アクセプタブル ユース ポリシーの適用
- Web でのデータ漏洩の防止
- すべての HTTP および HTTPS 要求を許可または拒否することによる、安全でないとわかった Web サイトからのエンドポイントの保護
- 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の提供

Cisco Secure Mobility for AnyConnect ライセンスは、次のようにアクティブにする必要があります。

- Cisco Secure Mobility for AnyConnect Premium ライセンスを WSA でアクティブにするには、ASA で 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にする必要があります。
- Cisco Secure Mobility for AnyConnect Essentials ライセンスを WSA でアクティブにするには、ASA で AnyConnect Essentials ライセンスをアクティブにする必要があります。WSA でアクティブにされた Cisco Secure Mobility for AnyConnect Essentials ライセンスは、ASA でアクティブにされた AnyConnect Premium ライセンスとともに使用することはできません。

  （注） Premium 機能であるログイン後の VPN 常時接続は、AnyConnect ライセンスを WSA、または AnyConnect Essentials ライセンスを ASA でアクティブにして有効にできます。

- WSA でアクティブにされた Cisco Secure Mobility for AnyConnect ライセンスは、ASA でアクティブにされた AnyConnect ライセンスでサポートされている VPN セッション数と一致するか、それを超える必要があります。

AnyConnect、Premium または Essentials のこの Cisco Secure Mobility ライセンスは、アクティブにされた Cisco IronPort Web セキュリティ アプライアンスのライセンスとは別に追加されます。

詳細については、『*Cisco IronPort Web Security Appliances Introduction*』を参照してください。

AnyConnect ライセンスの組み合わせ

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	モバイル アクセス	クライアントレス 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	エンドポイント アセスメント	エンドポイント修復
AnyConnect Essentials	(ベース ライセンス)	✓						
+	AnyConnect Mobile	✓	✓					
+	Cisco Secure Mobility for AnyConnect Essentials	✓	✓		✓	✓		
+	AnyConnect Flex[1]	✓	✓		✓	✓		
AnyConnect Premium SSL VPN Edition	(ベース ライセンス)	✓		✓	✓		✓	
+	AnyConnect Mobile	✓	✓	✓	✓		✓	
+	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓	✓	
+	Advanced Endpoint Assessment	✓	✓	✓	✓	✓	✓	✓
+	AnyConnect 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。

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、グループを選択する必要もあります。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 [Address] または [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 [Logon] 画面で入力し、グループを選択して、[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、[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 [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。[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 パッケージを導入する場合、AnyConnect を企業ソフトウェア展開システムに導入する場合でも、AnyConnect のどのバージョンがセッションを確立できるかという点について、ASA がシングル ポイント適用になるようにします。AnyConnect パッケージを ASA にロードする場合、ASA でロードされたバージョンと同じ新しいバージョン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、クライアントがクライアント ダウンローダをバイパスし、ASA でクライアント パッケージ ファイルが必要なくなるようなローカル ポリシー ファイルを導入できます。ただし、Weblaunch や自動アップデートなど他の機能は無効になっています。

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。一部の機能については、プロファイルの一部の設定をユーザが制御できる設定として指定できます。AnyConnect グラフィカル ユーザ インターフェイスは、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。

ユーザが 1 つのプロファイル ファイルを持っている場合、このプロファイルにはユーザで必要なすべてのホスト、また必要に応じてその他の設定が入っています。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 をサポートするための WSA 設定ガイドとして、『Cisco AnyConnect Secure Mobility Solution Guide』の 17 ページにある「Configuring WSA Support of the AnyConnect Secure Mobility Solution」の項に移動します。

ステップ 2　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.3-21）
- 「VPN 常時接続」（P.3-23）
- 「VPN 常時接続用の [Disconnect] ボタン」（P.3-28）
- 「VPN 常時接続に関する接続障害ポリシー」（P.3-29）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-32）
- 「SCEP による認証登録の設定」（P.3-45）

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 で AnyConnect を構築する際に、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。

この API は、クライアントの VPN 機能のみサポートします。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。

AnyConnect アクセシビリティ

AnyConnect には、マウスを使用せずにウィンドウ上のボタンにアクセスできる機能が用意されています。

次のナビゲーション ショートカットは、視力に問題があるか目の見えない担当者がアプリケーションを使用する際に役立ちます。

キーストローク	アクション
Alt	フォーカスをブラウザのメニュー バーに移動します。
Enter	フォーカスされたアイテムを選択します。
Alt+ 矢印キー	ブラウザ メニュー間を移動します。
Alt+ アンダースコア	メニューに移動します。

キーストローク	アクション
Space	チェックボックスのオンとオフなど、コントロールを切り替えます。
Tab	タブ順の次のアイテムまたは次のコントロール グループにフォーカスを移動します。
Shift+Tab	タブ順の前のアイテムまたはグループにフォーカスを移動します。
矢印キー	グループ内のコントロール間を移動します。
Home	複数画面にわたる情報がある場合、ウィンドウの一番上に移動します。 ユーザが入力したテキストの行頭に移動します。
End	ユーザが入力したテキストの行末に移動します。 複数画面にわたる情報がある場合、ウィンドウの一番下に移動します。
Page Up	1 画面分上にスクロールします。
Page Down	1 画面分下にスクロールします。

CHAPTER 2

AnyConnect Secure Mobility Client の展開

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

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

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

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

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

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

AnyConnect クライアント プロファイルの概要

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect プロファイルで有効になっています。これらのプロファイルには、コア クライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、ポスチャ、テレメトリ、Web セキュリティの構成設定が入っています。ASA は AnyConnect のインストールおよびアップデート中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

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

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

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

プロファイルをすべての AnyConnect ユーザにグローバルに展開するか、またはグループ ポリシーに基づいてユーザに展開するように ASA を設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのプロファイル ファイルを持ちます。1 人のユーザに複数の VPN プロファイルを割り当てる必要があることがあります。複数の場所で作業するユーザには、複数の VPN プロファイルが必要になることがあります。Start Before Login など、一部のプロファイル設定は、グローバル レベルで接続を制御します。その他の設定は特定のグループ ポリシーに一意であり、どのグループ ポリシーがクライアントにダウンロードされたかにより異なります。

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

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

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

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。各オペレーティング システムで使用されるファイル名およびパスに関する詳細については、「すべてのオペレーティング システムに対するプロファイルの場所」の表 2-13 を参照してください。クライアント プロファイル作成の詳細については、次の各項を参照してください。

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

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

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

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージには、すべてのオペレーティング システム用のプロファイル エディタが入っています。AnyConnect クライアント イメージを ASA にロードすると、ASDM はプロファイル エディタをアクティブにします。

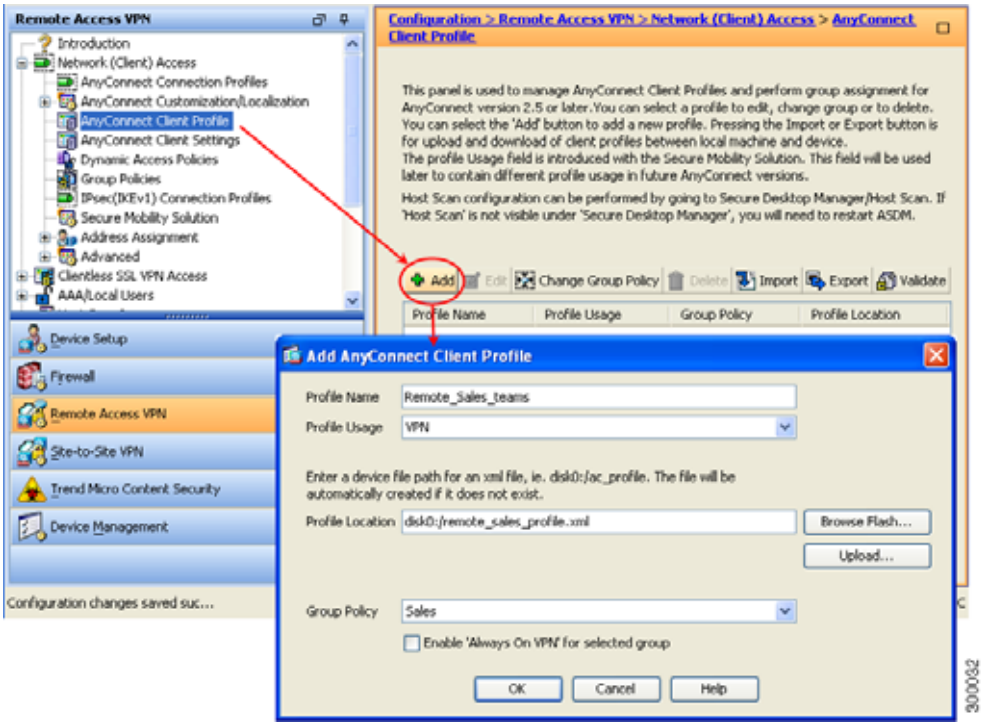
複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからクライアント プロファイル エディタがアクティブにされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

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

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

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

図 2-1　AnyConnect プロファイルの追加



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

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

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

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

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

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

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

ステップ 10　ASDM を終了し、再起動します。

AnyConnect クライアント プロファイルの展開

AnyConnect クライアント プロファイルの ASA からの展開

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

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

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

- 第 3 章「VPN アクセスの設定」

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

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

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

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

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

ステップ 6　[OK] をクリックします。

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

ステップ 8　[Save] をクリックします。

ステップ 9　設定が終了したら、[OK] をクリックします。

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

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

Web 展開 AnyConnect

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

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

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

要件

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

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

Windows

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

OS X

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

Linux

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

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

ステップ 1　Firefox がインストールされている。

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

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

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

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

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

制限事項

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

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

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

ASA 展開用の AnyConnect ファイル パッケージ

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

表 2-1　ASA 展開用の AnyConnect パッケージ ファイル名

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

AnyConnect の正常インストールの確認

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

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

自己署名証明書を受け入れるためのエンドポイントの設定

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

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

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

手順の詳細

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

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

ステップ 3　[Next] をクリックします。

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

ステップ 5　[Browse] をクリックします。

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

ステップ 7　[Next] をクリックします。

ステップ 8　[Finish] をクリックします。

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

ステップ 10　[OK] をクリックして、このウィンドウを閉じます。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

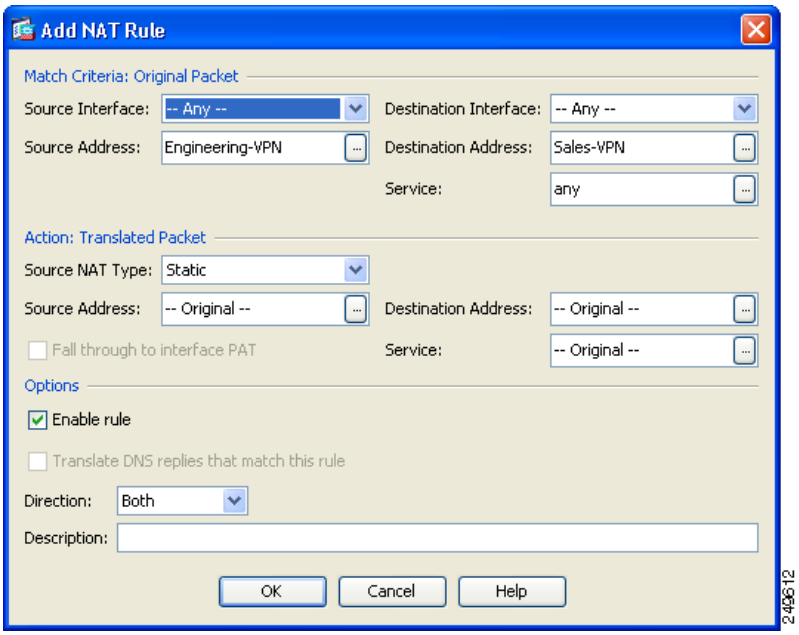
ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

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

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

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

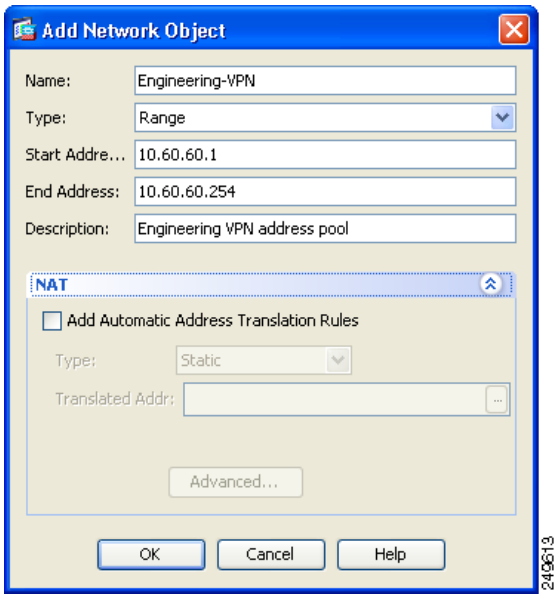
図 2-2　[Add NAT Rule] ダイアログボックス



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

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

図 2-3　VPN アドレス プールのネットワーク オブジェクトの作成



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

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

c. [Options] エリアで、次のフィールドを設定します。

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

d. [OK] をクリックします。

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

CLI の例：

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

f. [Send] をクリックします。

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

CLI の例：

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

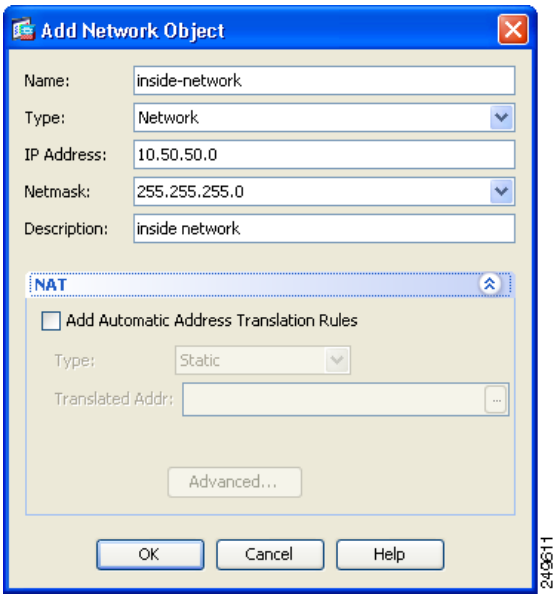
ステップ 4　Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。ステップ 2 で規則を作成したときのようにこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで Engineering VPN アドレス プールを送信元アドレスおよび宛先アドレス両方として指定します。

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

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

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

図 2-4　inside-network オブジェクトの追加



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

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

c. [Options] エリアで、次のフィールドを設定します。

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

d. [OK] をクリックします。

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

CLI の例

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

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

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

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

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

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

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

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

d. [Options] エリアで、次のフィールドを設定します。

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

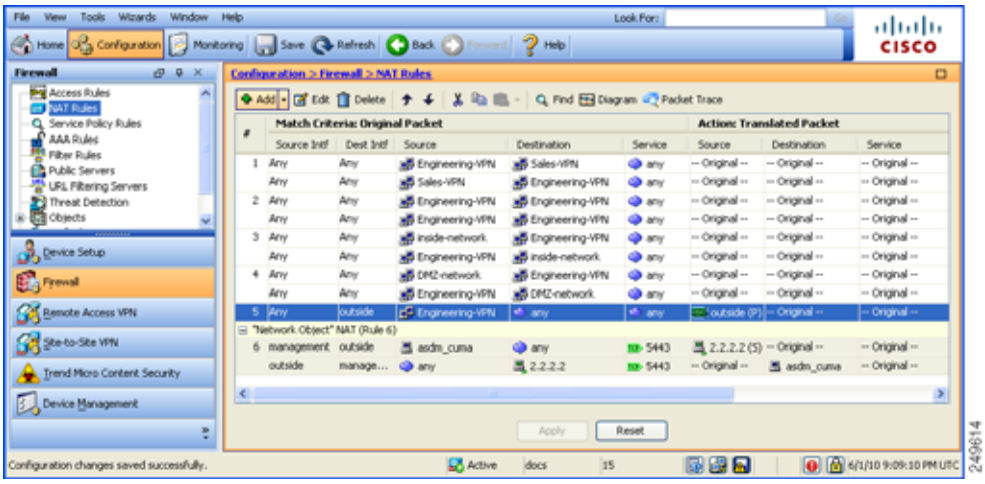
e. [OK] をクリックします。

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

CLI の例：

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

図 2-5　Unified NAT テーブル



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

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

非推奨の DES-only SSL 暗号化用 ASA 設定

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

モバイル ブロードバンド カードとの接続

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

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

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

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

グループ ポリシー設定の無効化

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

Web 展開時のインストーラの動作の変更

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

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

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

Linux のインストーラの変更には対応していません。

AnyConnect をダウンロードするための ASA の設定

前提条件

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

手順の詳細

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

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

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

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

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

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

ステップ 5　[OK] または [Upload] をクリックします。

ステップ 6　[Apply] をクリックします。

アドレスの割り当て方式を設定する

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

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

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

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

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

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

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

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

リモート ユーザへの AnyConnect ダウンロードの要求

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

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

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

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

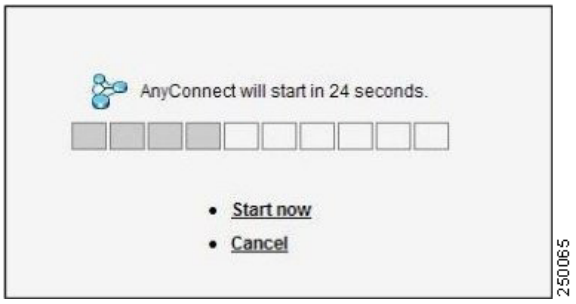
ステップ 2　ナビゲーション ペインで、[Advanced] > [AnyConnect Client] > [Login Settings] を選択します。[Post Login settings] が表示されます。必要に応じて [Inherit] チェックボックスをオフにし、[Post Login setting] を選択します。

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

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

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

図 2-6　リモート ユーザに表示されるログイン後プロンプト



ステップ 4　[Save] をクリックします。

アップグレードに対するユーザ制御

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

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

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

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

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

延期アップデートのカスタム属性

次の属性と値により、延期アップデートを設定します。

表 2-3　延期アップデートのカスタム属性

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

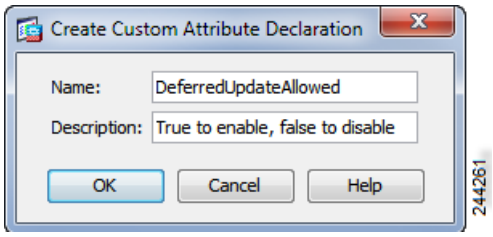
* カスタム属性値は大文字と小文字を区別します。

ASDM での属性の追加

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

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

図 2-7　ASA へのカスタム属性の追加



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

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

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

ステップ 6　[Add] をクリックします。

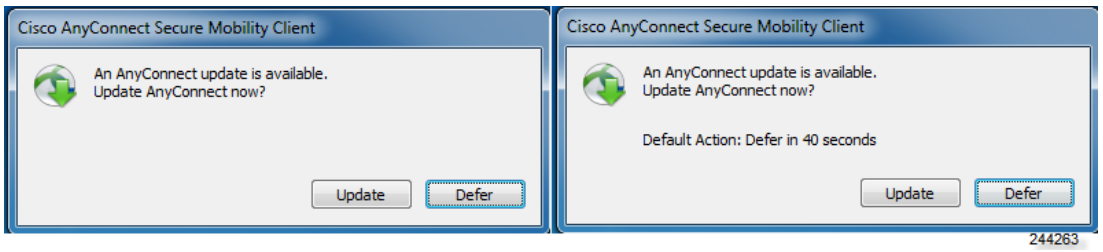
ステップ 7　[Declared Attribute Name] を選択し、設定する属性を選択して設定します。

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

延期アップデートの GUI

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

図 2-8　延期アップデートの UI



追加機能で使用するモジュールの有効化

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

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

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

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

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

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

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

IPsec IKEv2 接続の有効化

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

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

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

図 2-9　AnyConnect VPN Wizard

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

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

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

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

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

IKEv2 対応クライアント プロファイルの事前展開

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

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

ステップ 2　次のフォルダを参照します。

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

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

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

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

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

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

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

表 2-4　クライアントを展開するためのパス

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

事前展開に関するその他のヒント

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

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

クライアントの Weblaunch

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

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

<asa> は ASA の IP アドレスまたは FQDN です。IP アドレスを使用する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイの使用はサポートしていません。

AnyConnect の事前展開

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

- 「事前展開パッケージ ファイル情報」（P.2-23）
- 「Windows コンピュータへの事前展開」（P.2-23）
- 「Linux および Mac OS X コンピュータへの事前展開」（P.2-30）
- 「AnyConnect ファイル情報」（P.2-33）

制限事項

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

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

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

事前展開パッケージ ファイル情報

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

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

Windows コンピュータへの事前展開

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

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

ISO ファイルの使用

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

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

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

ガイドラインと制限事項

システム MTU のリセット

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

ActiveX コントロールをオンにする

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

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

事前展開にインストール ユーティリティを使用する

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

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

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

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

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

SMS を使用して AnyConnect モジュールを事前展開する

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

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

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

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

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

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

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

要件

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

手順の詳細

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

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

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

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

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

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

ステップ 5　AnyConnect モジュールの事前展開用のパッケージをとくていするには、「ISO ファイルの使用」（P.2-24）を参照してください。

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

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

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

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

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

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

前提条件

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

手順の詳細

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

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

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

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

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

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

手順の詳細

ステップ 1　テレメトリ モジュールをアンインストールします。

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

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

ステップ 4　DART をアンインストールします。

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

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

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

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

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

MSI インストールのコマンドライン呼び出し

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

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
Web セキュリティ	msiexec /package anyconnect-websecurity-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-<*version*>-pre-deploy-k9-install-datetimestamp.log
ポスチャ	msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-<*version*>-pre-deploy-k9-install-datetimestamp.log
テレメトリ	msiexec /package anyconnect-telemetry-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-telemetry-<*version*>-pre-deploy-k9-install-datetimestamp.log

Windows のロックダウン オプション

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

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

プログラムの追加と削除リストで AnyConnect を非表示にする

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

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

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

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

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

手順の詳細

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

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

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

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

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

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

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

事前展開中のインストーラ動作の変更

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

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

Linux および Mac OS X コンピュータへの事前展開

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

インストーラ動作の変更

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

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

XML ファイルの形式は次のとおりです。

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

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

Linux のインストーラの変更には対応していません。

カスタマー エクスペリエンス フィードバック モジュールの無効化

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

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

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

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

要件

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

手順の詳細

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

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

ステップ 3　ポスチャ モジュールをインストールします。

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

手順の詳細

ステップ 1　ポスチャ モジュールをアンインストールします。

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

ステップ 3　DART をアンインストールします。

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

システムでのアプリケーションの制限

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

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

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

Firefox によるサーバ証明書の検証

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

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

AnyConnect ファイル情報

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

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

エンドポイント コンピュータ上のモジュールのファイル名

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

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

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

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

表 2-6　ASA または事前展開の DART パッケージ ファイル名

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

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

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

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

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

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

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

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

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

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

表 2-9　ASA または事前展開のポスチャ モジュール ファイル名

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

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

表 2-10　ASA または事前展開のテレメトリ ファイル名

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

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

表 2-11　ASA または事前展開の Web セキュリティ ファイル名

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

AnyConnect プロファイルの展開場所

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

表 2-12　エンドポイント上のプロファイル ファイル

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

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

表 2-13　すべてのオペレーティング システムに対するプロファイルの場所

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

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

ローカル コンピュータにインストールされたユーザ プリファレンス

また一部のプロファイル設定は、ユーザ コンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、クライアント GUI の [Preferences] タブにユーザ制御可能設定をクライアントで表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

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

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

表 2-14　ユーザ プリファレンス ファイルおよびインストール パス

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

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

スタンドアロン AnyConnect プロファイル エディタの使用

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

スタンドアロン プロファイル エディタのシステム要件

サポートされるオペレーティング システム

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

Java 要件

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

ブラウザ要件

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

必要なハード ドライブ容量

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

スタンドアロン AnyConnect プロファイル エディタのインストール

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

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

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

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

ステップ 3　[Welcome] 画面で、[Next] をクリックします。

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

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

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

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

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

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

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

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

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

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

ステップ 3　[Next] をクリックします。

ステップ 4　[Modify] をクリックします。

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

ステップ 6　[Install] をクリックします。

ステップ 7　[Finish] をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 VPN プロファイル エディタのパラメータに関する説明」（P.3-80）

AnyConnect クライアントの IP アドレスの設定

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし、VPN では、実際には 2 セットのアドレスが存在します。最初のセットは、パブリック ネットワーク上でクライアントとサーバを接続します。この接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

ASA のアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

この項は、次の内容で構成されています。

- 「IP アドレスの割り当てポリシー」（P.3-2）
- 「内部 IP アドレス プール」（P.3-3）
- 「IP アドレスの AnyConnect 接続への割り当て」（P.3-5）

IP アドレスの割り当てポリシー

- [Use authentication server]：ユーザ単位で外部認証、認可、アカウンティング サーバからアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することをお勧めします。[Configuration] > [AAA Setup] ペインで AAA サーバを設定できます。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
- [Use DHCP]：DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。DHCP を使用する場合は、[Configuration] > [Remote Access VPN] > [DHCP Server] ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- [Use an internal address pool]：内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] ペインで IP アドレス プールを設定します。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
  - [Allow the reuse of an IP address so many minutes after it is released]：IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、これはチェックされません。つまり、ASA は遅延時間を課しません。遅延時間を設定する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 1 ～ 480 の範囲で指定します。この設定要素は IPv4 の割り当てポリシーに使用できます。

ASDM を使用した IPv4 および IPv6 のアドレス割り当ての設定

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ 2　[IPv4 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server] : IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバを使用できるようにします。
- [Use DHCP] : IP アドレスを提供するために設定したダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

[Use internal address pools] を有効にする場合、IPv4 アドレスが解放された後、そのアドレスの再利用を有効にできます。IP v4 アドレスが再利用できるようになる時間範囲を 0 ～ 480 分から指定できます。

ステップ 3　[IPv6 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server] : IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

ステップ 4　[Apply] をクリックします。

ステップ 5　[OK] をクリックします。

内部 IP アドレス プール

VPN リモート アクセス トンネルを使用するよう IPv4 または IPv6 アドレス プールを設定するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add/Edit IP Pool] を選択します。

アドレス プールを削除するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] を選択します。削除するアドレス プールを選択し、[Delete] をクリックします。

ASA は、接続の接続プロファイルまたはグループ ポリシーに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定する場合、ASA はそれらを ASA に追加した順序で使用します。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

（注）　IPv4 および IPv6 両方の ASA の外部インターフェイス アドレスは、アドレス プールで定義されているようにプライベート側のアドレス空間と重複できません。

ASDM を使用したローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス プールが、名前ごとに、それぞれの IP アドレス範囲（たとえば、10.10.147.100 ～ 10.10.147.177）とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2　IPv4 アドレスを追加するには、[Add] > [IPv4 Address pool] をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3　[Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Pool Name]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [Starting Address]：設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- [Ending Address]：設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。たとえば 10.10.147.177 のように、ドット付き 10 進数表記を使用します。
- [Subnet Mask]：この IP アドレスが常駐するサブネットを指定します。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

ASDM を使用したローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス プールが、名前ごとに、開始 IP アドレス範囲、アドレス プレフィックス、プールに設定できるアドレス数とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2　IPv6 アドレスを追加するには、[Add] > [IPv6 Address pool] をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3　[Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Name]：設定された各アドレス プールの名前を表示します。
- [Starting IP Address]：設定されたプールで使用可能な最初の IP アドレスを入力します。たとえば、2001:DB8::1 となります。
- [Prefix Length]：IP アドレス プレフィックス長をビット単位で入力します。たとえば、32 は CIDR 表記で /32 を表します。プレフィックス長は、IP アドレスが常駐するプールのサブネットを定義します。

- [Number of Addresses]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

IP アドレスの AnyConnect 接続への割り当て

次のいずれかの方法で IP アドレスを VPN 接続に割り当てます。

- 「内部アドレス プールを使用した IP アドレスの割り当て」（P.3-5）：内部プールはグループ ポリシーに関連付けられており、ASA で設定されています。IPv4 アドレスまたは IPv6 アドレスが使用できます。
- 「DHCP を使用した IP アドレスの割り当て」（P.3-6）：DHCP サーバを ASA で設定されているグループ ポリシーに関連付けます。IPv4 アドレスのみ使用できます。
- 「IP アドレスのローカル ユーザへの割り当て」（P.3-6）：IP アドレスを ASA で設定されたユーザに割り当てます。IPv4 アドレスまたは IPv6 アドレスが使用できます。

内部アドレス プールを使用した IP アドレスの割り当て

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセス グループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

同じグループ ポリシーで IPv4 と IPv6 両方のアドレス ポリシーを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

ステップ 1　ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2　新しいグループ ポリシーまたは内部アドレス プールで設定するグループ ポリシーを作成し、[Edit] をクリックします。

[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。

ステップ 3　[Address Pools] フィールドを使用して、このグループ ポリシーの IPv4 アドレス プールを指定します。[Select] をクリックし、IPv4 アドレス プールを追加または編集します。詳細については、「ASDM を使用したローカル IPv4 アドレス プールの設定」（P.3-4）を参照してください。

ステップ 4　[IPv6 Address Pools] フィールドを使用して、このグループ ポリシーに使用する IPv6 アドレス プールを指定します。[Select] をクリックし、IPv6 アドレス プールを追加または編集します。「ASDM を使用したローカル IPv6 アドレス プールの設定」（P.3-4）を参照してください。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックします。

DHCP を使用した IP アドレスの割り当て

DHCP サーバを使用して IPv4 アドレスを割り当てるには、以下の指示に従って DHCP を使用するよう IP アドレス割り当てポリシーを設定します。DHCP サーバを使用して IPv6 アドレスを AnyConnect クライアントに割り当てることはできません。

ステップ 1　ASDM を使用して ASA に接続します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ 3　[Use DHCP] をクリックします。

ステップ 4　[Apply] をクリックします。

ステップ 5　[Configuration] > [Remote Access VPN] > [DHCP Server] を選択して、DHCP サーバを設定します。

IP アドレスのローカル ユーザへの割り当て

ASA 管理者は、ASA の個々のユーザのアカウントを作成できます。これらのアカウントはグループ ポリシーを使用するよう設定したり、特にローカル ユーザ ポリシーで設定されたグループ ポリシーで検出された同じ VPN 属性を多数持ったりすることができます。またこれら個々のユーザのアカウントに、AnyConnect 属性をいくつか設定させることができます。

ここでは、ローカル ユーザのすべての属性を設定する方法について説明します。

前提条件

この手順では、既存のユーザを編集する方法について説明します。ユーザを追加するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、[Add] をクリックします。詳細については、『*Cisco ASA 5500 Configuration Guide Using ASDM*』の第 42 章「Configuring AAA Servers and the Local Database」の「Adding a User Account to the Local Database」を参照してください。

ガイドライン

デフォルトでは、[Edit User Account] 画面の設定ごとに [Inherit] チェックボックスがオンになっています。つまり、ユーザ アカウントは、デフォルト グループ ポリシー DfltGrpPolicy のその設定の値を継承するということです。

各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。次の「手順の詳細」で、[Edit User Account] 画面の各設定について説明しています。

手順の詳細

ステップ 1　ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。

ステップ 2　設定するユーザを選択し、[Edit] をクリックします。

[Edit User Account] 画面が開きます。

ステップ 3　左側のペインで、[VPN Policy] をクリックします。

ステップ 4　ユーザのグループ ポリシーを指定します。ユーザ ポリシーは、このグループ ポリシーの属性を継承します。この画面にデフォルト グループ ポリシーの設定を**継承するよう**設定されている他のフィールドがある場合、このグループ ポリシーで指定された属性がデフォルト グループ ポリシーで設定された属性より優先されます。

ステップ 5　ユーザが使用できるトンネリング プロトコルを指定するか、グループ ポリシーから値を継承するかどうかを指定します。目的の [Tunneling Protocols] チェックボックスをオンにし、使用できる VPN トンネリング プロトコルを選択します。選択されたプロトコルのみが使用可能になります。次の選択肢があります。

- （SSL/TLS を利用する VPN）クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- SSL VPN クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect Secure Mobility Client 対応の IPsec IKEv2。IKEv2 を使用した IPsec による AnyConnect 接続では、SSL VPN 接続が使用できる同じ機能セットを利用できます。
- L2TP over IPSec では、複数の PC やモバイル PC に採用されている一般的なオペレーティング システムに付属の VPN クライアントを使用するリモート ユーザが、パブリック IP ネットワークを介して ASA およびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。

（注）　プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

ステップ 6　使用するフィルタ（IPv4 または IPv6）を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。フィルタは、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] を選択します。

[Manage] をクリックして、ACL と ACE を追加、編集、および削除できる [ACL Manager] ペインを表示します。

ステップ 7　接続プロファイル（トンネル グループ ロック）がある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。同一ではなかった場合、ASA はユーザによる接続を禁止します。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8　[Store Password on Client System] 設定をグループから継承するかどうかを指定します。[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] をクリックすると、ログイン パスワードがクライアント システムに保存されます（セキュリティが低下

するおそれのあるオプションです）。接続ごとにユーザにパスワードの入力を求めるようにするには、[No] をクリックします（デフォルト）。セキュリティを最大限に確保するためにも、パスワードの保存は*許可しない*ことを推奨します。

ステップ 9　このユーザに適用するアクセス時間ポリシーを指定する、そのユーザの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] ダイアログボックスを開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。

ステップ 10　ユーザによる同時ログイン数を指定します。Simultaneous Logins パラメータは、このユーザに指定できる最大同時ログイン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。

（注）　最大値を設定て制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

ステップ 11　ユーザ接続時間の**最大接続時間**を分で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] チェックボックスをオンにします（デフォルト）。

ステップ 12　ユーザのアイドル タイムアウトを分で指定します。この期間、このユーザの接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は、クライアントレス SSL VPN 接続のユーザには適用されません。

ステップ 13　セッション アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、セッション アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 14　アイドル アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、アイドル アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 15　このユーザに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address] 領域（任意）で、IPv4 アドレスおよびサブネット マスクを入力します。

ステップ 16　このユーザに対して専用の IPv6 アドレスを設定する場合は、[Dedicated IPv6 Address] フィールド（任意）で、IPv6 アドレスを IPv6 プレフィックスとともに入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。

ステップ 17　クライアントレス SSL の設定を行う場合は、左側のペインで、[Clientless SSL VPN] をクリックします。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

ステップ 18　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

IPv4 または IPv6 トラフィックを設定して VPN をバイパスする

クライアント バイパス プロトコル機能により、ASA で IPv6 トラフィックのみ予想されている場合に AnyConnect クライアントが IPv4 トラフィックを管理する方法、または ASA で IPv4 トラフィックのみ予想されている場合に AnyConnect が IPv6 トラフィックを管理する方法を設定できます。

AnyConnect クライアントで ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

クライアント バイパス プロトコルが 1 つの IP プロトコルに対して有効で、そのプロトコルにアドレス プールが設定されていない（つまり、そのプロトコルの IP アドレスが ASA からクライアントにプッシュされていなかった）場合、そのプロトコルを使用した IP トラフィックは VPN トンネル経由で送信されず、クリア テキストで AnyConnect クライアントから送信されます。

一方、クライアント バイパス プロトコルが無効で、そのプロトコルにアドレス プールが設定されていない場合、VPN トンネルが確立されると、その IP プロトコルのすべてのトラフィックがドロップされます。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定してください。エンドポイントが IPv6 アドレスに達しようとするときにクライアント バイパス プロトコルが無効な場合、IPv6 トラフィックはドロップされ、クライアント バイパス プロトコルが有効な場合、IPv6 トラフィックはクリア テキストでクライアントから送信されます。

クライアント バイパス プロトコルを ASA でグループ ポリシーに対して設定します。

ステップ 1　ASDM を使用して ASA に接続します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 3　グループ ポリシーを選択して、[Edit] をクリックします。

ステップ 4　[Advanced] > [AnyConnect] を選択します。

ステップ 5　デフォルト グループ ポリシー以外のグループ ポリシーの場合、[Client Bypass Protocol] の隣にある [Inherit] のチェックボックスをオフにします。

ステップ 6　次のオプションのいずれかを選択します。

- ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[Disable] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[Enable] をクリックします。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

AnyConnect プロファイルの設定と編集

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。

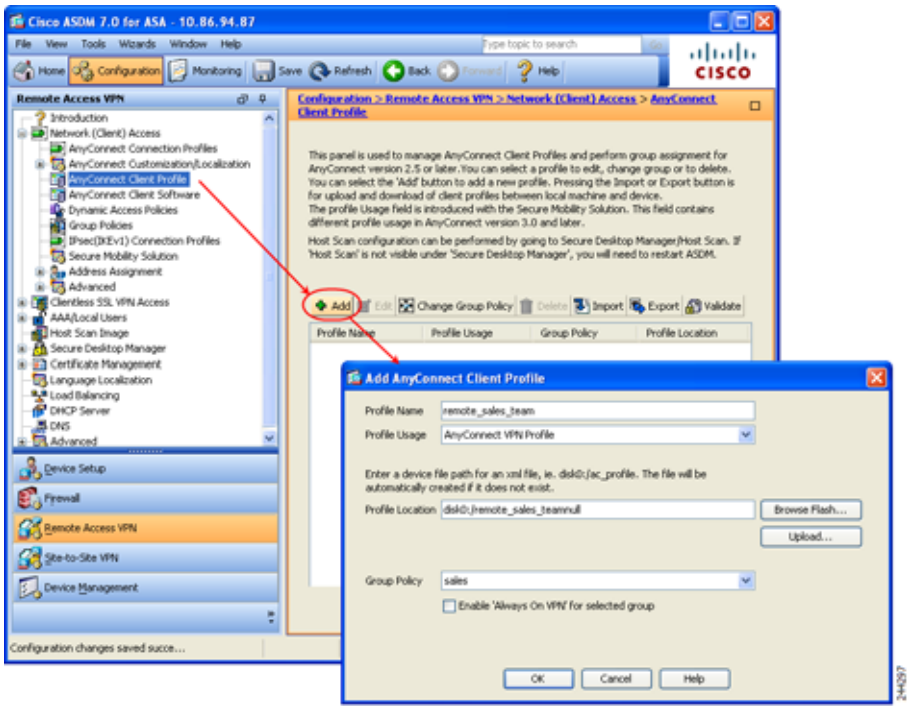
ASDM でプロファイル エディタをアクティブ化する手順は次のとおりです。

ステップ 1　AnyConnect ソフトウェア パッケージを AnyConnect Client イメージとしてロードします。まだロードしていない場合は、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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。[AnyConnect Client Profile] ペインが開きます。

ステップ 3　[Add] をクリックします。[Add AnyConnect Client Profile] ウィンドウが開きます（図 3-1）。

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 [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。

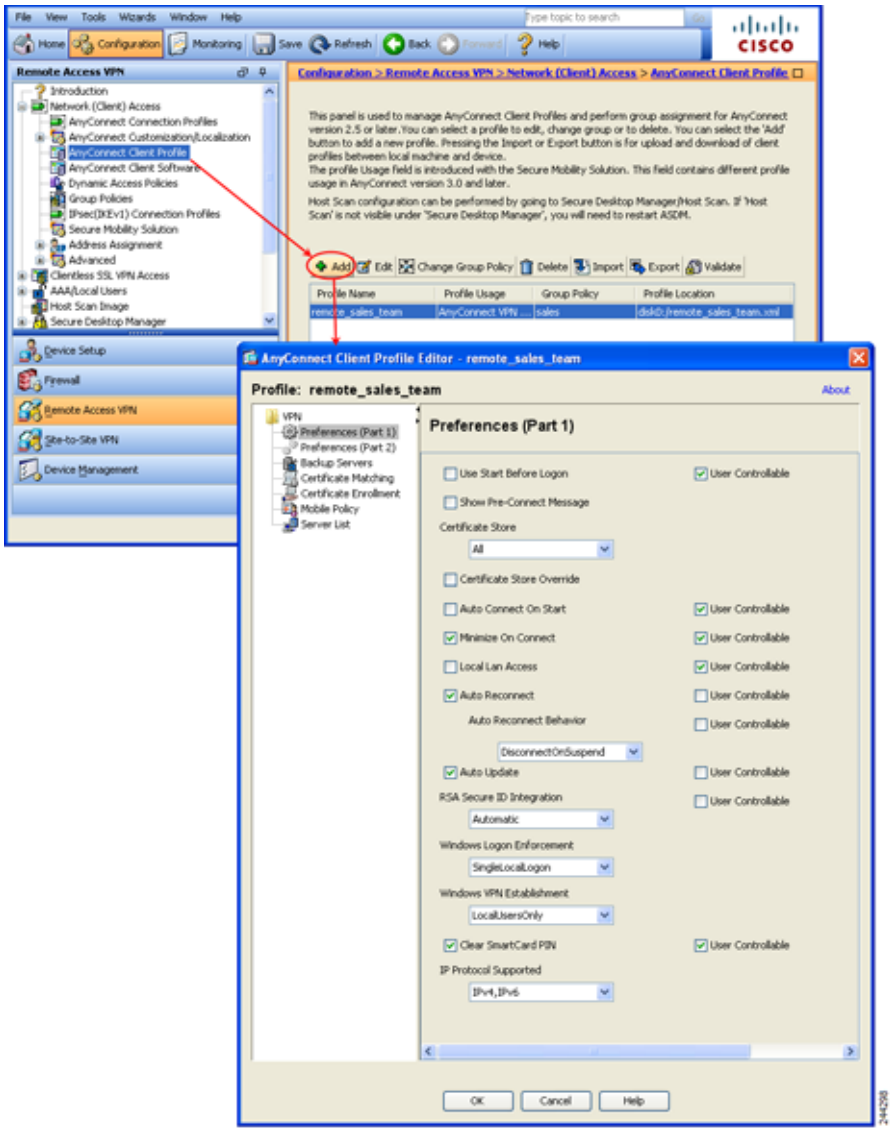
（注）　名前を指定するときに、.xml 拡張子は含めないでください。プロファイルに example.xml という名前を付けた場合、ASDM により自動的に .xml 拡張子が追加されて、名前が example.xml.xml に変更されます。この場合、ASA の [Profile Location] フィールドで名前を example.xml に変更しても、リモート アクセスで AnyConnect に接続したときに、名前は example.xml.xml に戻ってしまいます。（.xml 拡張子の重複により）AnyConnect がプロファイル名を認識できない場合、IKEv2 接続は失敗する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

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。[Edit] をクリックします。プロファイル エディタは図 3-2 のように表示されます。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。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

（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 エントリの追加の詳細については、「サーバ リストの設定」（P.3-60）を参照してください。

ステップ 1　クライアント プロファイルとグループ ポリシーを関連付けます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2　新しいグループ ポリシーを追加するか、グループ ポリシー テーブルからグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Advanced] > [AnyConnect Client] の順に選択します。

ステップ 4　[Inherit] チェックボックスをオフにし、[Select AnyConnect Client Profile] ダイアログボックスを使用して、ダウンロードする AnyConnect プロファイルを選択します。

ステップ 5　設定が完了したら、[OK] をクリックし、[Apply] をクリックします。

VPN ロード バランシングの設定

AnyConnect クライアントのロード バランシングの設定は、『*Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*』の第 67 章「Configuring IKE, Load Balancing, and NAC」の「Configuring Load Balancing」ですべて説明しています。

そこで定義されているガイドラインに加えて、次のガイドラインに注目してください。

- IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv6 アドレス経由または GSS サーバ経由で AnyConnect 接続を行うことができます。同様に、IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv4 アドレス経由または GSS サーバ経由で AnyConnect VPN 接続を行うことができます。どちらのタイプの接続も ASA クラスタ内でロード バランシングできます。

  IPv6 アドレスを使用したクライアントが ASA の公開されている IPv4 アドレスに正常に接続するには、IPv6 から IPv4 へネットワーク アドレス変換が可能なデバイスがネットワークに存在する必要があります。

- AnyConnect でロード バランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントにより、この IP アドレスを通してその名前チェックがすべて実行されます。お客様は、この IP アドレスが証明書の一般名、つまり **subject alt name** に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

- RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。クラスタリング環境では、証明書の設定により異なります。クラスタで使用されている証明書が 1 つの場合、それがクラスタの IP になり、証明書には Subject Alternative Name 拡張子があり、それぞれ ASA の IP と FQDN を持っています。クラスタで使用されている証明書が複数の場合、それが再度 ASA の IP アドレスになるはずです。

Start Before Logon の設定

Start Before Logon（SBL）によりユーザは、Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。

Windows ログインでは、Windows 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 を有効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 機能を有効にするには、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、この機能を有効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。

この項では、次のトピックについて取り上げます。

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。また、Start Before Logon コンポーネントには、コア クライアント コンポーネントをインストールする必要があります。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 の有効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 [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.3-16）を参照してください。

AnyConnect プロファイルでの SBL の有効化

AnyConnect プロファイルで SBL 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.3-9）を参照）。

ステップ 2　[Preferences] ペインに移動し、[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、[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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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、[Edit] をクリックします。

ステップ 3　左側のナビゲーション ペインで [Advanced] > [AnyConnect Client] を選択します。AnyConnect Client 設定が表示されます。

ステップ 4　[Optional Client Module for Download] 設定の [Inherit] をオフにします。

ステップ 5　ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

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 [プログラムの追加と削除] 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　1 回リブートします。次回リブート時には、[Start Before Logon] プロンプトが表示されます。

ステップ 7　DART バンドルを収集し、AnyConnect 管理者に送付します。「DART を使用したトラブルシューティング情報の収集」（P.13-4）を参照してください。

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 VPN 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無効となり、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。「AnyConnect プロファイルでの SBL の有効化」（P.3-15）を参照してください。アクティブ化後に、ユーザは [Switch User] をクリックし、さらに画面下右側の [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 を有効にした状態で、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 3-3）。

図 3-3　[Network Connect] ボタンが表示されたログイン ウィンドウの例

[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 3-4）。

図 3-4　[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　[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。赤丸で囲まれているのは [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 [Switch User] をクリックしても、VPN 接続は解除されません。[Network Connect] をクリックすると、元の VPN 接続が終了します。[Cancel] をクリックすると、VPN 接続が終了します。

図 3-5　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 [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 [Disconnect] ボタンである点です（図 3-5）。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 3-6　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（図 3-6 で囲まれた）[Disconnect] ボタンが表示されます。

[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、[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 [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

Trusted Network Detection（TND）は、この AnyConnect リリースでサポートされた Microsoft Windows および Mac OS X オペレーティング システムを動作しているコンピュータでサポートされています。

常時接続が設定されている、またはされていない Trusted Network Detection は、IPv4 ネットワークおよび IPv6 ネットワークで ASA に接続された IPv6 および IPv4 の VPN 接続でサポートされています。

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.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Automatic VPN Policy] をオンにします。

（注）　[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。

- [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。
- [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。
- [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。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection（TND）は無効となります。
- [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。

- [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。
- [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、VPN 常時接続は無効となります。[Trusted Network Policy] および [Untrusted Network Policy] を共に [*Do Nothing*] に設定すると、Trusted Network Detection は無効となります。

ステップ 6　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））を指定します。*.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。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。

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、203.0.113.1,2001:DB8::1 です。DNS サーバ アドレスでは、ワイルドカード（*）はサポートされていません。

（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
example.com（のみ）	example.com
example.com および anyconnect.cisco.com	*.example.com または example.com, anyconnect.example.com
asa.example.com および example.cisco.com	*.example.com または asa.example.com, anyconnect.example.com

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 を有効にする。
- 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。

VPN 常時接続

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）VPN 常時接続*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 VPN 常時接続では、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 VPN 常時接続が検出されると、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、VPN 常時接続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。

- VPN 常時接続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 VPN 常時接続ポリシーを無視することができます。VPN 常時接続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。

VPN 常時接続の要件

VPN 常時接続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 VPN 常時接続をサポートできます。

VPN 常時接続を使用するには、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。

VPN 常時接続を設定する場合は、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。

VPN 常時接続は、このリリースでサポートされている Microsoft Windows および Mac OS X オペレーティング システムを実行するコンピュータを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 VPN 常時接続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。

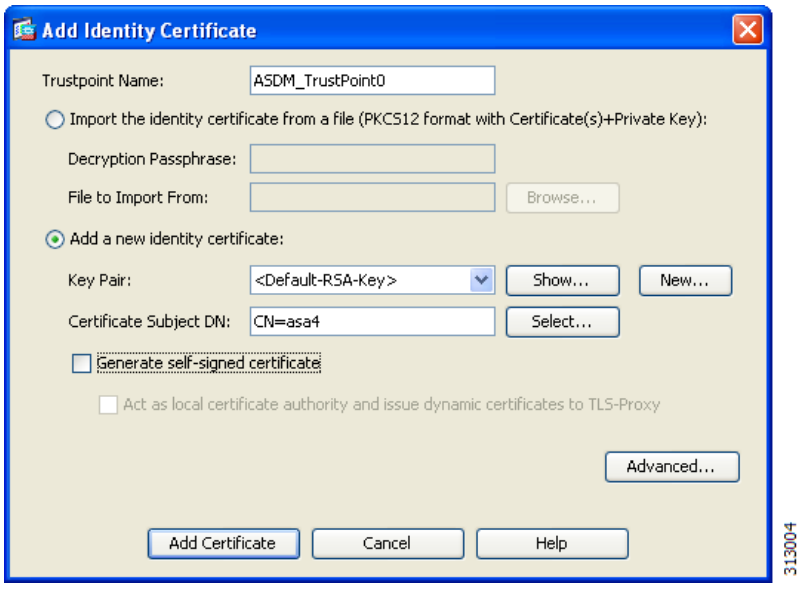
ヒント　認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。

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、[Identity Certificates] パネル（[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates]）に、公開証明書を容易に登録するための [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 [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できます。

図 3-7　[Add Identity Certificate] ダイアログ

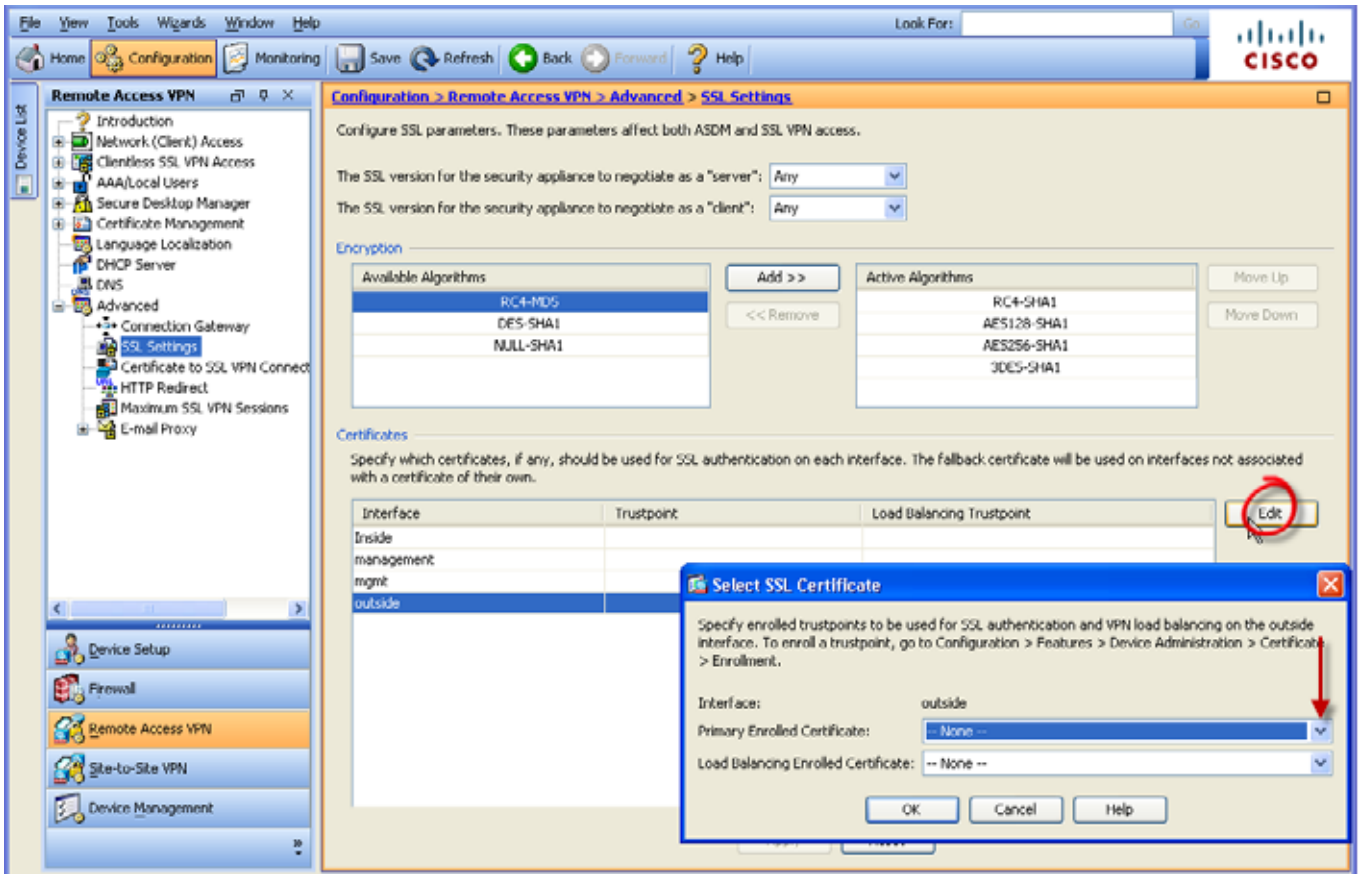


（注）　これらの手順は、証明書の設定に関するガイドラインとして記載されたものです。詳細については、ASDM の [Help] ボタンをクリックするか、設定するセキュア ゲートウェイ用の ASDM または CLI ガイドを参照してください。

自己署名インターフェイスを生成する場合は、[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。

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、[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings] を選択し、[Certificates] エリアで「outside」エントリを編集して、[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 3-8　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

VPN 常時接続は、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。VPN 常時接続を無効にした状態では、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。VPN 常時接続を有効にすると、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.3-9）を参照）。

ステップ 2　[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、[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。

VPN 常時接続の設定

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　TND を設定します（「Trusted Network Detection の設定」（P.3-21）を参照）。

ステップ 2　[Always On] をオンにします。

VPN 常時接続からユーザを除外するポリシーの設定

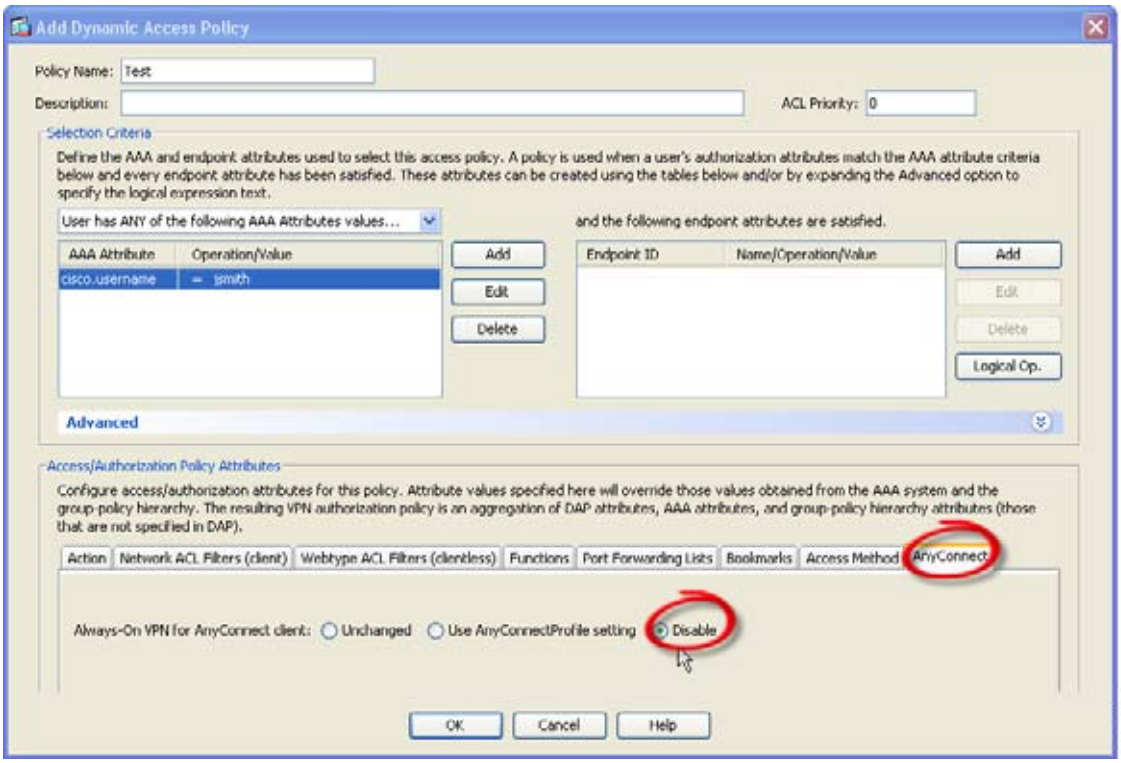
VPN 常時接続は、デフォルトでは無効になっています。常時接続ポリシーに優先して適用される除外規定を設定することができます。たとえば、特定のユーザに対して他社との VPN セッションを確立できるようにしつつ、企業外資産に対しては VPN 常時接続ポリシーを除外するという場合があります。

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 VPN 常時接続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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add] または [Edit] を選択します。

図 3-9　　VPN 常時接続からのユーザの除外



ステップ 2　ユーザを VPN 常時接続から除外する条件を設定します。たとえば、[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　[Add Dynamic Access Policy] ウィンドウまたは [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　[Always-On VPN for AnyConnect client] の横にある [Disable] をクリックします。

Cisco AnyConnect Secure Mobility Client ポリシーでは VPN 常時接続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 常時接続用の [Disconnect] ボタン

AnyConnect は、VPN 常時接続セッション用の [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 [Disconnect] ボタンが表示されます。VPN 常時接続セッションのユーザは、[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。

[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　[Disconnect] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

VPN 常時接続セッション中にユーザが [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　[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、[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。

[Disconnect] ボタンに関する要件

VPN 常時接続用の接続解除オプションに関する要件は、「VPN 常時接続の要件」（P.3-24）と同じです。

[Disconnect] ボタンの有効化 / 無効化

VPN 常時接続を有効すると、プロファイル エディタでは、[Disconnect] ボタンがデフォルトで有効になります。[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.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Allow VPN Disconnect] をオンまたはオフにします。

VPN 常時接続に関する接続障害ポリシー

接続障害ポリシーでは、VPN 常時接続が有効であり、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 ポリシーでは、ネットワーク接続が許可

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。

VPN 常時接続ポリシー	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」（P.3-32）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 VPN 常時接続を展開し、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 10.6、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、VPN 常時接続が設定され、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.3-21）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] パラメータを次のいずれかに設定します。

- [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 フィルタを有効にすることで、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有効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 [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。[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。
- [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。[Disconnect] ボタンが有効で、かつユーザが [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。

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 ポータルの修復に関する要件

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 ポータルの検出と修復は、AnyConnect のこのリリースでサポートされている Microsoft Windows および Mac OS X オペレーティング システムでサポートされています。

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。

VPN 常時接続が有効であり、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 [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 [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 ポータル修復を有効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 ポータルを修復できます。

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 ポータル修復を有効にするには、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.3-31）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。

- 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。
- 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。

  VPN 常時接続が有効な場合に、ユーザが [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、DoS 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。

キャプティブ ポータルの検出の失敗

次のような状況では、誤ってキャプティブ ポータルと見なされる場合があります。

- AnyConnect が、サーバ名が正しくない証明書（CN）を持った ASA に接続しようとしている場合、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。

  これを回避するには、ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアント プロファイルの ASA サーバの名前と一致する必要があります。

- ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる ASA への接続に応答すると、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。これは、ユーザが内部ネットワークに存在し、ファイアウォールを介して ASA に接続している場合に発生する可能性があります。

  企業内から ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。ASA への HTTP/HTTPS アクセスは許可するか、完全にブロック（ブラック ホールとも呼ばれます）し、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

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、Windows Mobile デバイス（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 [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れさます。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 ファイアウォール機能は、このリリースでサポートされている Windows、Mac OS X、および Linux オペレーティング システムでサポートされています。

（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ファイアウォール 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。

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.3-36）
- 「テザー デバイスのサポート」（P.3-37）

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。
- ASA 9.0 から、パブリック ネットワーク ルールおよびプライベート ネットワーク ルールは、ユニファイド アクセス コントロール リストをサポートしています。これらのアクセス コントロール リストは、同じルールで IPv4 および IPv6 トラフィックを定義する場合に使用できます。

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特定の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。

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、AnyConnect 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。

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

表 3-3 は、ローカル印刷に関する ACL ルールの例です。

表 3-3　ローカル印刷に関する ACL ルールの例

説明	権限	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

表 3-3　ローカル印刷に関する ACL ルールの例 （続き）

説明	権限	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
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 [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

ステップ 1　グループ ポリシーで、AnyConnect クライアント ファイアウォールを有効にします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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、[Edit] をクリックします。[Edit Internal Group Policy] ウィンドウが表示されます。

ステップ 3　[Advanced] > [AnyConnect Client] > [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 [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 [Preferences (Cont)] に移動し、[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。

（注）　AnyConnect を実行するコンピュータと同期する必要がある Windows モバイルデバイスについては、ACL で IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

手順は次のとおりです。

ステップ 1　ASDM で、[Group Policy] > [Advanced] > [Split Tunneling] を選択します。

ステップ 2　[Network List] フィールドの隣にある [Inherit] チェックボックスをオフにし、[Manage] をクリックします。[ACL Manager] が表示されます。

ステップ 3　[Extended ACL] タブをクリックします。

ステップ 4　[Add] をクリックし、さらに [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、[Add] をクリックし、さらに [Add ACE] をクリックします。[Edit ACE] ウィンドウが表示されます。

ステップ 6　[Action] で [Permit] オプション ボタンを選択します。

ステップ 7　宛先条件エリアで、IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

ステップ 8　[Service] に対して *IP* を選択します。

ステップ 9　[OK] をクリックします。

ステップ 10　[OK] をクリックして、ACL を保存します。

ステップ 11　内部グループ ポリシーの [Split Tunneling] ペインで、ステップ 7 で指定した IP アドレスに応じて [Inherit for the Policy or IPv6 Policy] チェックボックスをオフにして、[Exclude Network List Below] を選択します。[Network List] で、作成した ACL を選択します。

ステップ 12　[OK] をクリックします。

ステップ 13　[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。リリース 3.0.4 以降では、AnyConnect コンポーネントは **/opt/cisco/anyconnect** パスにインストールされています。

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 トンネリングの設定

スプリット トンネリングにより、VPN トンネル経由（暗号化されている）でエンドポイントから ASA へネットワーク トラフィックをルーティングし、VPN トンネル外（暗号化されていない、つまりクリア テキスト）のエンドポイントからその他のネットワーク トラフィックをルーティングできます。

ユニファイド アクセス コントロール リストを作成し、そのリストを VPN トンネルに組み込むよう要求する、または VPN トンネルから除外するよう要求することで、スプリット トンネリングを実装します。ユニファイド アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。

スプリット トンネリングは、ASA のネットワーク（クライアント）アクセス内部グループ ポリシーで設定されています。

AnyConnect クライアントおよびレガシー Cisco VPN クライアント（IPsec/IKEv1 クライアント）は、ASA によってクライアントに割り当てられた 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 によってクライアントに割り当てられた 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。レガシー Cisco VPN Client は、ASA によって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。

したがって、スプリット トンネル IPv4 または IPv6 ポリシーで定義されたユニファイド アクセス コントロール リストでは、予想されたローカル サブネットを正しく参照する割り当て済み IP アドレスのネットマスクを使用します。

（注）　次の手順では、フィールドの隣に [Inherit] チェックボックスがあるすべてのケースで、[Inherit] チェックボックスがオンのままの場合、設定しているグループ ポリシーは、そのフィールドについて、デフォルト グループ ポリシーと同じ値を使用することを意味します。[Inherit] チェックボックスをオフにすると、グループ ポリシーに固有の新しい値を指定できます。

ステップ 1　ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2　[Add] をクリックして新しいグループ ポリシーを追加するか、既存のグループ ポリシーを選択して [Edit] をクリックします。

ステップ 3　[Advanced] > [Split Tunneling] を選択します。

ステップ 4　[DNS Names] フィールドで、クライアントに送信されるこのグループ ポリシーに固有の DNS サーバの名前を入力します。フィールドには、完全修飾ドメイン名、IPv4 アドレス、または IPv6 アドレスを入力できます。DNS エントリが複数ある場合は、カンマ、スペース、またはセミコロンで区切ります。

ステップ 5　[Send All DNS Lookups Through Tunnel] フィールドは、VPN トンネル（SSL または IPsec/IKEv2）経由のすべての DNS アドレスを解決するように AnyConnect クライアントに指示します。DNS 解決に失敗すると、アドレスは未解決のまま残ります。AnyConnect Client は、パブリック DNS サーバ経由でアドレスを解決しようとはしません。[No]（デフォルト）を選択すると、クライアントは、スプリット トンネル ポリシーに従ってトンネルを介して DNS クエリーを送信します。

ステップ 6　[Policy] フィールドと [IPv6 Policy] フィールドを設定します。[Policy] フィールドでは、IPv4 ネットワーク トラフィックのスプリット トンネリング ポリシーを定義します。[IPv6 Policy] フィールドでは、IPv6 ネットワーク トラフィックのスプリット トンネリング ポリシーを選択します。そうした違い以外は、これらのフィールドの目的は同じです。

[Inherit] チェックボックスをオフにし、スプリット トンネリング ポリシーを選択して、スプリット トンネリングを設定します。[Inherit] チェックボックスをオフにしない場合、グループ ポリシーでは、デフォルト グループ ポリシーである「DfltGrpPolicy」で定義されたスプリット トンネリング設定が使用されます。デフォルト グループ ポリシーのスプリット トンネリング ポリシー設定は [Tunnel All Networks] することです。

[Inherit] チェックボックスをオフにしたら、次のいずれかのポリシー オプションを選択できます。

- [Exclude Network List Below] : このポリシーは、クリア テキストで送信されるトラフィックの宛先ネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。このオプションは、Cisco VPN Client に対してだけ適用されます。
- [Tunnel Network List Below] : このポリシーでは、[Network List] で指定されたネットワーク間のすべてのトラフィックがトンネリングされます。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。それ他すべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。
- [Tunnel All Networks] : このポリシーは、トラフィックを暗号化しないで送信しないこと、または ASA 以外の宛先に送信しないことを指定します。この指定では、実質的にスプリット トンネリングは無効になります。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。これがデフォルトのオプションです。

（注）　[Tunnel All Networks] が設定されている場合、AnyConnect では、ローカル DHCP トラフィックはクリア テキストで流れることができます。このために、VPN クライアントが接続すると、特定のルートがローカル DHCP サーバに追加されます。また、このルートでのデータ漏えいを防ぐため、AnyConnect はホスト マシンの LAN アダプタに暗黙的なフィルタを適用し、DHCP トラフィックを除く、そのルートのすべてのトラフィックをブロックします。

ステップ 7　[Network List] フィールドで、スプリット トンネリング ポリシーを適用するユニファイド アクセス コントロール リストを選択します。[Inherit] チェックボックスをオフにしないと、グループ ポリシーでは、デフォルト グループ ポリシーで指定されたネットワーク リストが使用されます。デフォルト グループ ポリシーのネットワーク リストのデフォルト値は [None] です。

[Manage] コマンド ボタンを使用して [ACL Manager] ダイアログボックスを開きます。このボックスで、アクセス コントロール リストを設定したり、既存のアクセス コントロール リストを選択してネットワーク リストとして使用したりできます。ネットワーク リストを作成または編集する場合の詳細については、『*Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*』の第 24 章「Using the ACL Manager」の「Adding ACLs and ACEs」を参照してください。

（注）　拡張 ACL リストは IPv4 アドレスおよび IPv6 アドレスの両方に使用できます。

ステップ 8　[Intercept DHCP Configuration Message from Microsoft Clients] は DHCP 代行受信に固有の追加パラメータを示します。DHCP 代行受信によって Microsoft XP クライアントは、ASA でスプリット トンネリングを使用できるようになります。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。

- [Intercept] : DHCP 代行受信を許可するかどうかを指定します。Inherit を選択しない場合、デフォルト設定は No です。
- [Subnet Mask] : 使用するサブネット マスクを選択します。

ステップ 9　[OK] をクリックします。

ステップ 10　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

AnyConnect の DNS サーバおよび WINS サーバの設定

DNS サーバおよび WINS サーバは、ネットワーク（クライアント）アクセス グループ ポリシーで設定されています。

内部グループ ポリシーの DNS サーバの設定

内部ネットワーク（クライアント）アクセス グループ ポリシーの DNS サーバを設定するには、次の手順を使用します。

（注）　この設定は、ASDM の [Configuration] > [Remote Access VPN] > [DNS] ウィンドウで設定された DNS 設定より優先されます。

ステップ 1　ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Servers] を選択します。

ステップ 2　DefaultGroupPolicy を編集していない限り、[DNS Servers] の [Inherit] チェックボックスをオフにします。

ステップ 3　[DNS Servers] フィールドで、このグループを使用する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを追加します。

DNS サーバ アドレスは最大 4 つ、IPv4 アドレスと IPv6 アドレスで 2 つずつ指定できます。複数の DNS サーバを指定する場合、リモート アクセス クライアントは、フィールドで指定された順序で DNS サーバを使用しようとします。

ステップ 4　[More Options] バーの二重矢印をクリックして、[More Options] エリアを展開します。

ステップ 5　デフォルト ドメインが [Configuration] > [Remote Access VPN] > [DNS] ウィンドウに指定されていない場合、[Default Domain] フィールドにデフォルト ドメインを指定する必要があります。たとえば、**example.com.** というドメイン名およびトップ レベル ドメインを使用します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックします。

ステップ 8　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

内部グループ ポリシーの WINS サーバの設定

プライマリ WINS サーバとセカンダリ WINS サーバを設定するには、次の手順を使用します。それぞれのデフォルト値は none です。

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Servers] を選択します。

ステップ 2　[WINS Servers] の [Inherit] チェックボックスをオフにします。

ステップ 3　[WINS Servers] フィールドに、プライマリ WINS サーバとセカンダリ WINS サーバの IP アドレスを入力します。最初に指定する IP アドレスがプライマリ WINS サーバの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ WINS サーバの IP アドレスです。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

ステップ 6　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

スプリット DNS の機能拡張

AnyConnect 3.1 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 トンネリングが有効になっており、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。

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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] で [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。

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 トンネリングの有効にする
- トンネリングするドメインを 1 つ以上指定する
- [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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] にあります。

Mac OS X の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

AnyConnect ログによる確認

スプリット DNS が有効化どうか確認するには、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。有効な場合、このエントリに *Split DNS:enabled* と示されます。IPv4 および IPv6 のスプリット DNS には別々のログ エントリがあります。

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　[Configuration] > [Remote AccessVPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] を選択します。

ステップ 2　[Policy] ドロップダウン メニューで [Tunnel List Below] を選択し、[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。

DNS サーバの設定

ステップ 1　[Configuration] > [Remote AccessVPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Servers] を選択します。

ステップ 2　[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。

ネットワーク ローミング

AnyConnect 3.1 は、IPv4 ネットワークと IPv6 ネットワーク間のローミングに対応しています。AnyConnect が 2 種類のネットワーク間を移動している場合、AnyConnect クライアントは ASA の完全修飾ドメイン名（FQDN）を使用して、そのセキュア ゲートウェイへの接続を維持します。

NAT46 対応ネットワークおよび NAT64 対応ネットワーク（通常は DNS46 設定および DNS64 設定も必要）間のローミングを容易に行うには、クライアントは VPN セッション中にネットワーク ローミングが検出されると必ず ASA FQDN の名前解決を行います。これは、VPN セッションの再確立に使用する ASA IP アドレスを判断するためです。

ロード バランシングを使用している ASA 環境では、ASA の FQDN を設定せずに、ローミング中にプロファイル FQDN を解決できない理由を判断できそうもありません。これは、クライアントが最初に到達する ASA の IP アドレスが、クライアント接続先のデバイスの ASA に属していることを保証できないためです。

（注）　上記の ASA FQDN は、本来、トンネル確立に使用するプロファイル FQDN ではなく、トンネル確立中にクライアントにプッシュされた ASA デバイスの FQDN です。

前提条件

IPv4 ネットワークと IPv6 ネットワーク間のネットワーク ローミングの設定は、ASA のグループ ポリシーで行われます。

内部グループ ポリシーの追加方法または編集方法については、『*ASA Series ASDM Configuration Guide*』の第 73 章「General VPN Setup」の「Configuring Network (Client) Access Internal Group Policies」を参照してください。

IPv4 ネットワークと IPv6 ネットワーク間のネットワーク ローミングの設定

ステップ 1　ASDM を起動し、[Remote Access VPN] > [Configuration] > [Network (Client) Access] > [Group Policies] > [Group Policies] を選択します。

ステップ 2　設定しようとしているグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Edit Internal Group Policy] ページで [Advanced] > [AnyConnect] をクリックします。

ステップ 4　[FQDN] 行で、[FQDN] チェックボックスをオフにし、[FQDN] テキスト ボックスに ASA の FQDN を追加します。

上記を設定していない場合、ASA は ASA の [Hostname] フィールドおよび [Domain Name] フィールドで定義された FQDN を [Configuration] > [Device Setup] > [Device Name/Password] でプッシュします。ドメイン名は FQDN になるように記入する必要があります。

ドメイン名が FQDN として送信されていない場合、クライアントは ASA の名前解決のみ実行します。それ以外の場合は、AnyConnect は、トンネルを開始して VPN セッションを再確立したときに決定された IP アドレスを使用します。

ステップ 5　変更をグループ ポリシーまたは [Device Name/Password Device Setup] に保存します。

SCEP による認証登録の設定

SCEP を使用した証明書登録に関する情報

セキュア モビリティ スタンドアロン 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、使用可能な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。

当社の SCEP の実装では、クライアントが証明書要求を開始し、認証局（CA）が自動的に要求を承諾または拒否します。SCEP では、クライアントが証明書を要求してから、承諾または拒否の応答を受信するまで CA にポーリングするという方式も許可されています。ポーリング方式は、このリリースでは実装されていません。

サポートされている登録方式

ASA では、次の 3 つの方式で SCEP を使用した証明書登録がサポートされています。

レガシー SCEP

- クライアントは（VPN トンネルを構築する）ASA に接続し、拡張トンネル経由で CA から証明書を取得します。

- 証明書の期限が切れると、クライアントはこのプロセスを繰り返します。
- これは、AnyConnect 2.4 以降でサポートされています。

SCEP プロキシ

- ASA は SCEP 要求および応答のプロキシとして動作します。クライアントは ASA に接続し、SCEP 要求を送信します。ASA は登録要求を CA に転送し、CA の応答を転送します。クライアントは CA URL に接続する必要はありません。
- VPN プロファイルで証明書失効しきい値が設定されている場合は、ユーザが介入しなくても、クライアントは証明書の期限が切れる前に証明書を更新できます。
- これは、AnyConnect 3.0 以降でサポートされています。

手動 SCEP

- ASA に接続した後、ユーザは SCEP 登録用に設定されたグループを選択します。クライアントには、[Get Certificate] ボタンが表示されたダイアログが表示され、要求は直接 CA に送信されます。この方式では、CA により証明書要求の内容がチェックされないため、他の方式よりも安全性が劣ります。
- 証明書の期限が切れると、クライアントはこのプロセスを繰り返します。

SCEP の登録処理

次に、どのように SCEP 証明書要求が作成され、証明書接続が確立されるかを説明します。

1. クライアントは、証明書ベースの接続プロファイルおよびグループ ポリシー（tunnel-group）を使用して、ASA への接続を試行します。クライアントに有効な証明書が存在しない場合、SCEP がトリガーされます。
2. ASA への接続は、レガシーの場合は AAA、プロキシの場合は AAA と証明書を使用して確立されます。

   手動 SCEP では、フル認証は必要とされません。

   レガシー SCEP および手動 SCEP の場合、この接続では内部 CA へのアクセスが許可されている必要があります。
3. レガシー SCEP の場合、VPN クライアント プロファイルで自動 SCEP ホストが設定されていれば、クライアントは自動的に SCEP 要求を ASA に送信します。

   SCEP プロキシは自動 SCEP ホストを無視し、常に SCEP 要求を送信します。

   手動 SCEP の場合は、ユーザが [Get Certificate] ボタンをクリックしてクレデンシャルを入力すると、SCEP 要求が直接 CA に送信されます。

   証明書要求にマシン ID が使用される場合、クライアントは hostscan をロードしているはずです。
4. SCEP プロキシの場合、ASA は SCEP 要求と CA からの応答をリレーします。

   レガシー SCEP の場合、ASA は CA に要求を転送します。

   手動 SCEP の場合、CA はクライアントに直接応答します。
5. 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、セッションが接続解除されます。クライアントは、証明書および証明書接続プロファイルを使用して、新しいセッションを開始します。

   登録が失敗すると、クライアントに（設定可能な）メッセージが表示され、接続解除されます。

SCEP プロキシの場合、ASA はクライアントから受信した要求をログに記録しますが、接続が失敗した理由は示されません。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。

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。

自動による証明書要求

AnyConnect レガシー SCEP および SCEP プロキシは、既存のクライアント プロファイルが SCEP ホスト用に設定されていない場合でも、自動証明書要求をサポートします。

- クライアントが設定されている場合：クライアント プロファイルで、証明書登録が有効になっています。クライアントは SCEP を有効にした接続プロファイルでグループ ポリシーを選択し、ASA はクライアントとの VPN 接続を確立して、CA への SCEP 証明書要求を開始します。
- クライアントが設定されていない場合：ユーザが SCEP を有効にした接続プロファイルのグループ URL を選択する必要があります。VPN 接続が確立され、クライアント プロファイルがダウンロードされて、ASA は CA への SCEP 証明書要求を開始します。レガシー SCEP の場合、新しいクライアント プロファイルの自動 SCEP ホストおよび CA の URL が設定されている必要があります。

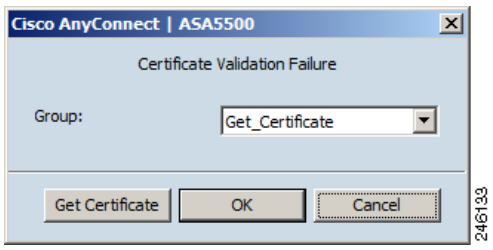
クライアントが自動的に新しい証明書の取得を試行する前に、クライアントの証明書認証は失敗します。

手動証明書要求

ユーザは、クライアント インターフェイスの [Get Certificate] ボタンをクリックすることで、新しい証明書の要求を開始します。手動登録では、ユーザ認証は必要ありません。

手動 SCEP 登録を使用する場合、クライアント プロファイルで CA パスワードを有効にして、証明書登録のセキュリティを強化することをお勧めします。

図 3-10　[Get Certificate] ボタン



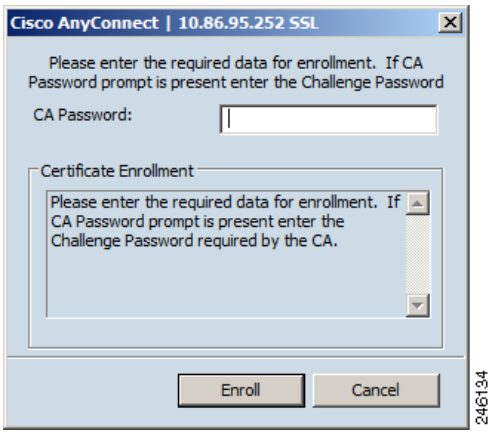
このボタンは、クライアント プロファイルで SCEP 機能が有効になっており、次の条件が満たされている場合にクライアントに表示されます。

- ASA はクライアントから証明書を要求したが、使用可能なホストに受け入れ可能な証明書が存在しない。
- AnyConnect で使用されている現在の証明書が、クライアント プロファイルの [Certificate Expiration Threshold] の設定で定義された日数以内に失効する。AnyConnect で使用されている現在の証明書がすでに失効している。

CA パスワード

クライアント プロファイルで **Prompt For Challenge PW** 属性が有効になっている場合は、ユーザに「CA パスワード」の入力を求めるプロンプトが表示されます。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。次に、[Enroll] ボタンが表示された [CA Password] ウィンドウの図を示します。

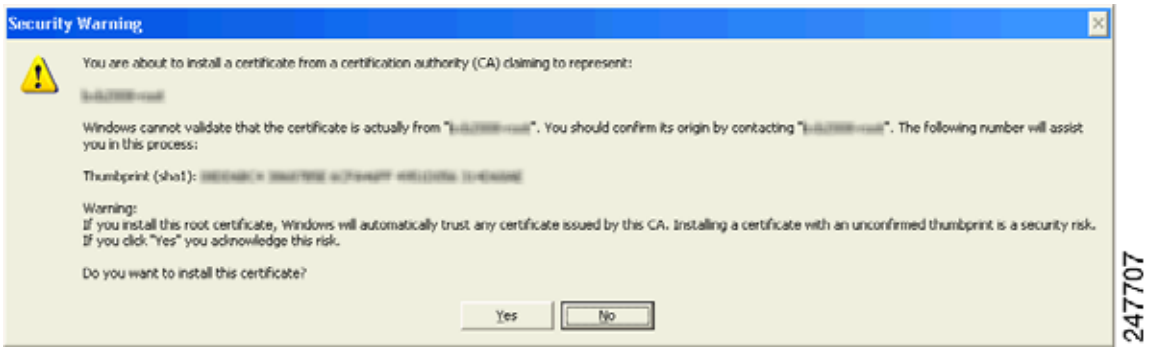
図 3-11　[CA Password] ウィンドウ



Windows 証明書の警告

Windows クライアントが初めて認証局から証明書を取得しようとした場合、それが自動か手動かによらず図 3-12 のような警告が表示されることがあります。プロンプトが表示されたら、[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るようになります。クライアント証明書を使用して接続する機能には影響ありません。

図 3-12　Windows 証明書のセキュリティ警告



SCEP を使用した証明書登録のガイドラインと制限

- SCEP 要求は、クライアント プロファイルにより開始されます。SCEP は、その他の証明書認証よりも優先されます。

- SCEP は、AnyConnect をサポートしているすべてのオペレーティング システムでサポートされています。
- ロードバランシングがサポートされています。
- クライアントレス（ブラウザベース）でのアクセスは 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）ではサポートしています。
- 証明書要求にマシン ID が使用される場合、クライアントは hostscan をロードしている必要があります。

SCEP を使用した証明書登録の前提条件

- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- 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。
- レガシー SCEP および手動 SCEP の場合、プライベート CA は ASA にアクセス可能である必要があります。
- ASA は AnyConnect SSL または IKEv2 VPN セッションを使用する必要があります。
- 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。

SCEP による認証登録の設定

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.3-9）を参照）。

ステップ 2　ASDM では、[Add]（または [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 Client Profile] ツリーで、[Certificate Enrollment] をクリックします。

ステップ 4　[Certificate Enrollment] ペインで、[Certificate Enrollment] をオンにします。

ステップ 5　レガシー SCEP のみ、証明書を取得するためにクライアントをリダイレクトする [Automatic SCEP Host] 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）を入力します。たとえば、ASA の名前として **asa.cisco.com**、接続プロファイルの名前として **scep_eng** を入力します。

ステップ 6　レガシー SCEP のみ、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（**http://ca01.cisco.com** など）。

ステップ 7　（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、[Prompt For Challenge PW] をオンにします。

ステップ 8　（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）。

（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。

ステップ 9　登録証明書で、要求する [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 [Certificate Enrollment]」（P.3-89）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 10　[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、サーバでの証明書照合が失敗した場合に表示されます。

ステップ 11　（任意）[General] ペインで、SCEP 接続プロファイルに [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。

ステップ 12　（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、ステップ 4 の SCEP ホスト設定は上書きされます。[Server List] ペインに移動し、既存のホスト エントリを編集するか、または SCEP ホストを使用して新規のホスト エントリを作成します。サーバ リストの設定の詳細については、<<add link>> を参照してください。

SCEP プロキシをサポートするための ASA の設定

次に、ASA で SCEP プロキシをサポートするように ASA を設定する高度な手順について説明します。SCEP プロキシでは、1 つの接続プロファイルで、証明書接続および証明書登録をサポートします。

ステップ 1　「SCEP 登録用 VPN クライアント プロファイルの設定」（P.3-49）のプロファイルの作成手順に従って、クライアント プロファイル（例：ac_scep）を作成します。

ステップ 2　グループ ポリシー（例：certgroup）を作成します。

- [General] で、[SCEP Forwarding URL] に CA への URL を入力します。
- [Advanced] > [AnyConnect Client] で、[Inherit for Client Profiles to Download] をオフにし、SCEP のクライアント（ac_scep）を追加します。

ステップ 3　登録用の接続プロファイル（例：certtunnel）を作成します。

- [Authentication]：Both（AAA および Certificate）
- [Default Group Policy]：certgroup
- [Advanced] > [General] で、[Enable SCEP Enrollment for this tunnel] をオンにします。
- [Advanced] > [SSL VPN Client] の [Client Profile to Download] で、ac_scep クライアント プロファイルを選択します。
- [Advanced] > [GroupAlias/Group URL] で、この接続プロファイルのグループ（centgroup）が含まれるグループ URL を作成します。

SCEP レガシーをサポートするための ASA の設定

ステップ 1　「SCEP 登録用 VPN クライアント プロファイルの設定」（P.3-49）のプロファイルの作成手順に従って、クライアント プロファイル（例：ac_scep）を作成します。このプロファイルに CA URL が設定されていることを確認します。

ステップ 2　登録用のグループ ポリシー（例：certenroll）を作成します。

ステップ 3　認証用の 2 つ目のグループ ポリシー（例：certauth）を作成します。

ステップ 4　登録用の接続プロファイル（例：scep_cp）を作成します。

- [Authentication]：AAA
- [Default Group Policy]：certenroll
- [Advanced] > [SSL VPN Client] の [Client Profile to Download] で、ac_sep クライアント プロファイルを選択します。
- [Advanced] > [GroupAlias/Group URL] で、この接続プロファイルの登録グループ（centroll）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有効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　認証用の接続プロファイル（例：centauth）を作成します。

- [Authorization]：Certificate

  ASA ではこの接続プロファイルを有効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。

ASA における証明書のみの認証の設定

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 の DAP レコード

aaa.cisco.sceprequired：この属性を使用して登録接続を確立し、適切な制限ポリシーを選択したレコードに適用できます。

証明書の失効通知の設定

ユーザに対して証明書の失効が近いことを警告できるように、クライアント プロファイルを設定することができます。[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。

（注）　RADIUS 登録では、[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 エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Add]（または [Edit]）をクリックして AnyConnect プロファイルを作成（または編集）し、左側の [AnyConnect Client Profile] ツリーで [Certificate Enrollment] をクリックします。

ステップ 3　[Certificate Enrollment] ペインで、[Certificate Enrollment] をオンにします。

ステップ 4　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表す証明書失効しきい値を指定します。

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 5　[OK] をクリックします。

証明書ストアの設定

AnyConnect がクライアントのシステムの証明書ストアを見つけ、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有効化」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.3-52）
- 「Mac および Linux での PEM 証明書ストアの作成」（P.3-54）

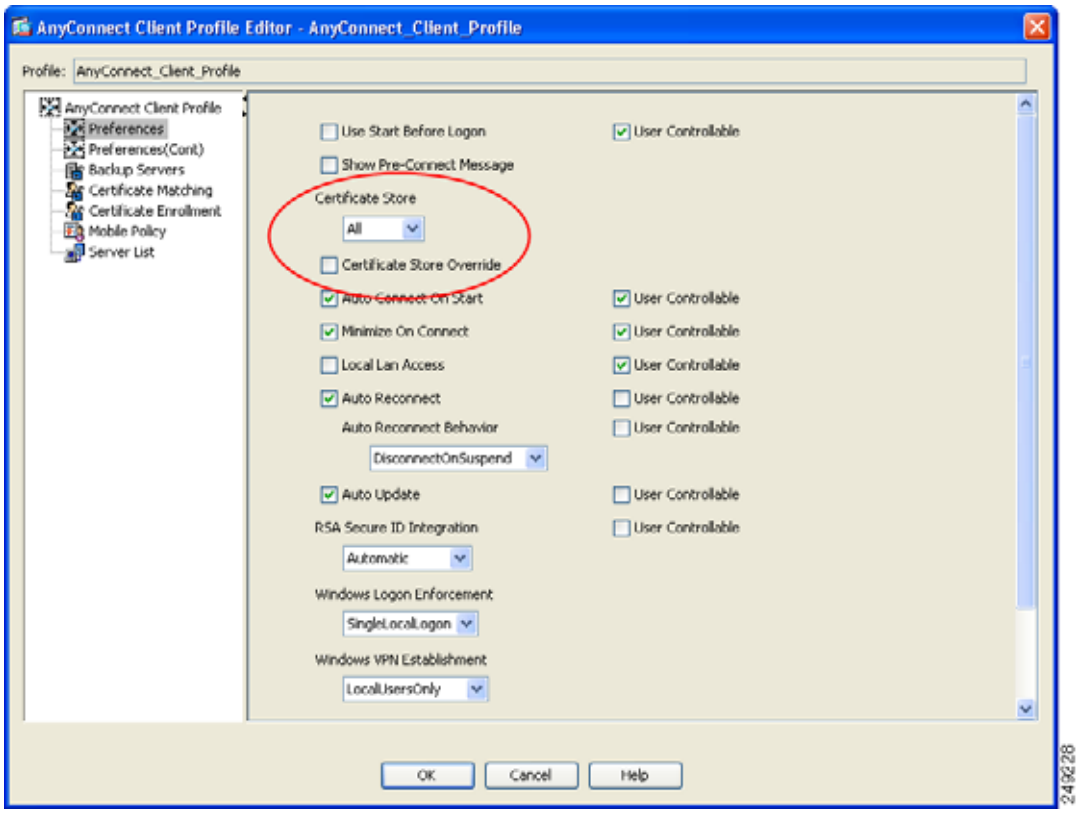
Windows での証明書ストアの制御

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。クライアント プロファイルは、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します。

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。通常、Windows XP ユーザには、管理者権限がありますが、Windows 7 ユーザにはありません。

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 [Preferences (Part 1)] ペインにある [Certificate Store] リスト ボックスを使用して設定します。[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 3-13　[Certificate Store] リスト ボックスと [Certificate Store Override] チェックボックス



[Certificate Store] は次の 3 つの設定が可能です。

- [All]：（デフォルト）すべての証明書ストアを検索します。
- [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。
- [User]：ユーザ証明書ストアを検索します。

[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。

表 3-4 は、[Certificate Store] および [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

[Certificate Store] の設定	[Certificate Store Override] の設定	AnyConnect の処理
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。 これは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。
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。
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。
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。
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。

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 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 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 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、[Certificate Matching] ペインの AnyConnect VPN クライアント 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

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。

証明書キーの用途による照合

証明書照合キーの用途は、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。サポート対象のセットは、VPN クライアント プロファイルの *Key Usage* リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN

- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

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.3-58）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

この照合により管理者は、VPN クライアント プロファイルの [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
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キー

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。

証明書の識別名による照合

クライアント プロファイルの [Certificate Matching] ペインの [Distinguished Name] テーブルには、クライアントで使用できる証明書を指定された基準および基準照合条件に一致する証明書に制限する証明書 ID が入っています。[Add] ボタンをクリックすると、いずれかの基準をリストに追加し、値またはワイルドカードを設定してその基準の内容と照合させることができます。表 3-7 にサポート対象の基準を一覧表示します。

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
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。

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.3-9）を参照）。

ステップ 2　[Certificate Matching] ペインに移動します。

ステップ 3　[Key Usage] および [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 [Certificate Matching]」（P.3-87）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　[Distinguished Names] テーブルの横にある [Add] をクリックして、[Distinguished Name Entry] ウィンドウを起動します。

- [Name]：識別名。
- [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。
- [Operator]：照合を実行する際に使用する演算子。
  - [Equal]：== と同等
  - [Not Equal]：!= と同等
- [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。
- [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。

証明書の選択を有効にするには、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.3-9）を参照）。

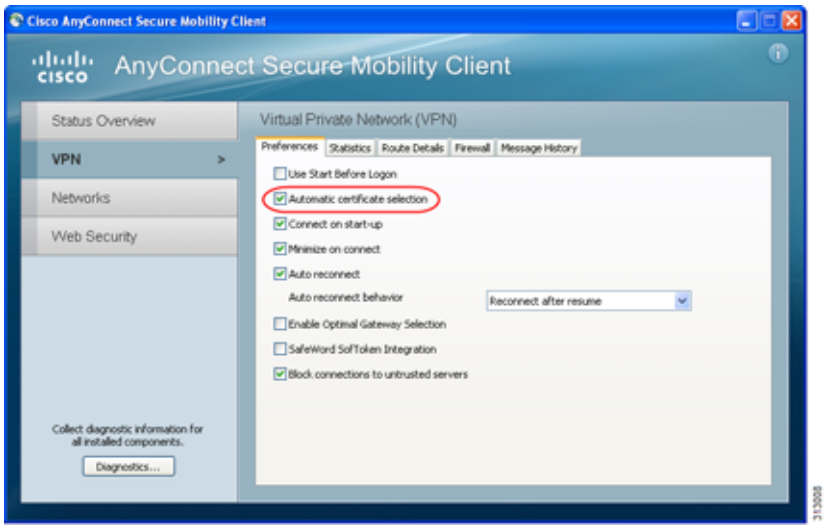
ステップ 2　[Preferences (Part 2)] ペインに移動し、[Disable Certificate Selection] をオフにします。これによりクライアントでは、ユーザに対して認証証明書を選択するためのプロンプトが表示されます。

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 [Preferences] ダイアログボックスに、[Automatic Certificate Selection] チェックボックスが表示されます。ユーザは、[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 3-19 は、[Preferences] ウィンドウに表示された [Automatic Certificate Selection] チェックボックスを示します。

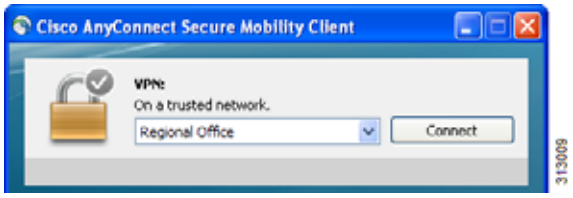
図 3-14　[Automatic Certificate Selection] チェックボックス



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 [*Connect to*] ドロップダウン リスト（図 3-20）にあるサーバのホスト名が一覧表示されます。ユーザはこのリストからサーバを選択できます。

図 3-15　[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。

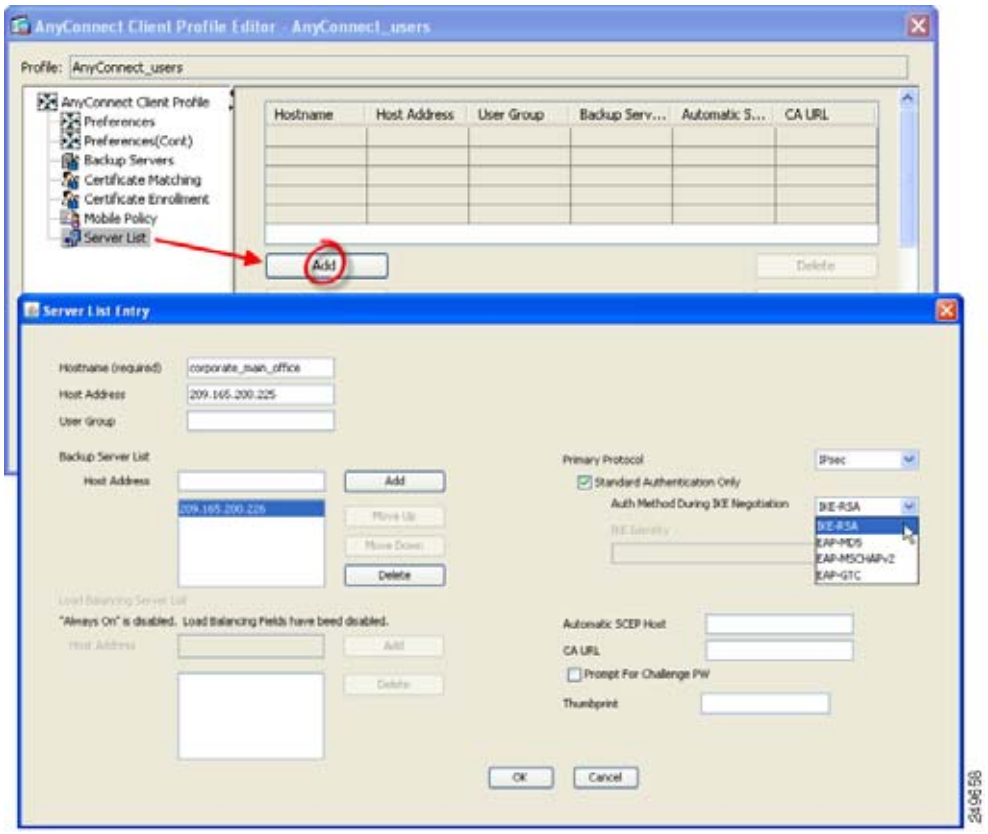
サーバ リストを設定する手順は次のとおりです。

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.3-9）を参照）。

ステップ 2　[Server List] をクリックします。[Server List] ペインが開きます。

ステップ 3　[Add] をクリックします。[Server List Entry] ウィンドウが開きます（図 3-21）。

図 3-16　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。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイの使用はサポートしていません。

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、[Additional mobile-only settings] チェックボックスをオンにして、[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）を無効にするには、[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。

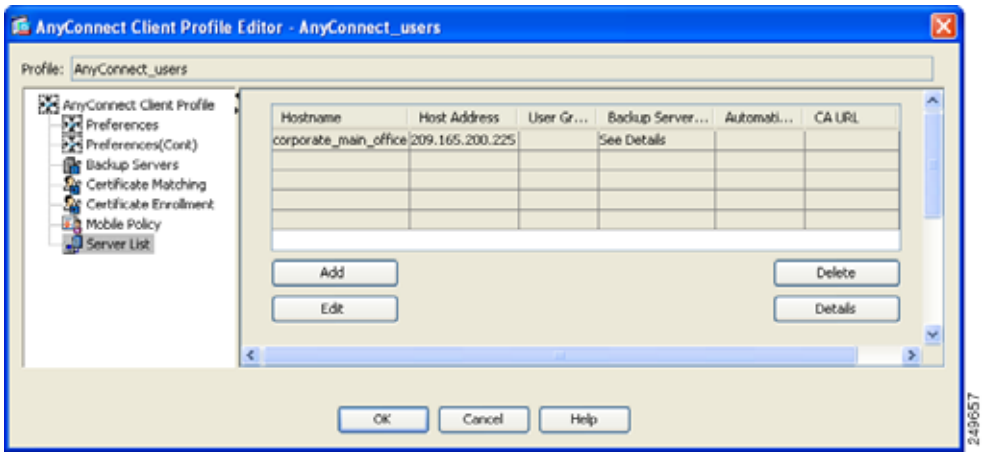
ステップ 11　SCEP CA サーバの URL を指定します（任意）。FQDN または IP アドレスを入力します（http://ca01.cisco.com など）。

ステップ 12　[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 [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 3-22）。

図 3-17　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.3-60）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　[Server List Entry] ダイアログボックスで、[Additional mobile-only settings] をオンにして [Edit] をクリックします。

ステップ 2　[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。

– [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。

- [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。
- [Disabled]：認証にクライアント証明書は使用されません。

b. [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 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. [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. [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。

[Connect on Demand] は、[Certificate Authentication] フィールドが [Manual] または [Automatic] に設定されている場合のみオンにできます。[Certificate Authentication] フィールドが [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。[Match Domain or Host] フィールドおよび [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. [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. [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。

- [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。
- [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。
- [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。[Always connect] または [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 が有効の場合、アプリケーションは自動的にこのリストにサーバ アドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作を望まない場合は、このルールを削除できます。

e. [Match Domain or Host] フィールドおよび [On Demand Action] フィールドを使用してルールを作成したら、[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.3-60）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 [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.3-9）を参照）。

ステップ 2　[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**無効**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 [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、[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 VPN 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無効になっているのは、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 の設定」（P.3-21）を参照してください。

デフォルトでは、Connect on Start-up は無効です。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.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences] を選択します。

ステップ 3　[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。

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.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences (Part 1)] を選択します。

ステップ 3　[Auto Reconnect] をオンにします。

（注）　[*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）。

- [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。
- [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 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.3-9）を参照）。

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

ステップ 3　パネル上部付近にある [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 を有効にして 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 [Backup Servers]」（P.3-86）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、このリリースに適合した Windows および Mac OS X オペレーティング システムを実行する VPN エンドポイントで、最適ゲートウェイ選択をサポートします。

この機能は IPv4 クライアントでのみ使用できます。

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.3-9）を参照）。

ステップ 2　[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　[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、[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（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、[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 が有効になっている場合は、[VPN: Ready to connect] パネルの [Connect] ボタンの横に [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、[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、[Disconnect] をクリックします。

ステップ 2　[Advanced] をクリックします。

ステップ 3　[Preferences] タブを開き、[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（[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]）の AutoReconnect（ReconnectAfterResume）設定を有効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 [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。

この項では、次のトピックについて取り上げます。

- 「スクリプトの要件と制限」（P.3-70）
- 「スクリプトの作成、テスト、および展開」（P.3-72）
- 「スクリプトに関する AnyConnect プロファイルの設定」（P.3-73）
- 「スクリプトのトラブルシューティング」（P.3-74）

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。

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 Mobile 用スクリプト

AnyConnect がサポートするすべての Microsoft Windows プラットフォーム、Mac OS X プラットフォーム、および Linux プラットフォームで、スクリプトの起動がサポートされます。Microsoft Windows Mobile では、スクリプト言語のネイティブ サポートはありませんが、スクリプト ファイル名プレフィックスとディレクトリ要件を使用してコンパイルすれば、OnConnect アプリケーションと OnDisconnect アプリケーションを作成して自動的に実行できます。

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。

スクリプトの有効化

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。[Network (Client) Access] > [AnyConnect Customization/Localization] > [Script] を選択します。

  （注） Microsoft Windows Mobile では、このオプションはサポートされません。このオペレーティング システム用のスクリプトを展開するには、企業のソフトウェア展開システムを使用してください。

  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
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.3-9）を参照）。

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

ステップ 3　[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　[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　[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　[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.3-9）を参照）。

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

ステップ 3　[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.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Proxy Settings] ドロップダウン リストで、[Ignore Proxy] を選択します。[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 [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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [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 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。

プロキシを使用しないパラメータが有効の場合、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 [Connections] タブのロック

ある条件下では、AnyConnect によって Internet Explorer の [Tools] > [Internet Options] > [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、[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 [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したり、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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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、[Edit] をクリックします。[Edit Internal Group Policy] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Advanced] > [Browser Proxy] に移動します。[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有効にして、AnyConnect のセッション中は [Internet Explorer Connections] タブを非表示にするには、[Inherit] をオフにして [Yes] を選択します。または、プロキシのロックダウンを無効にして、AnyConnect のセッション中は [Internet Explorer Connections] タブを表示するには、[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　[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 Logon Enforcement] に対しては次の設定を使用できます。

- [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 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。

- [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。

- [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 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 Establishment] の設定が [*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.3-9）を参照）。

ステップ 2　[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。

- [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。
- [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。

- [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。
- [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 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 [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
- ユーザによる PPP 除外の上書き

L2TP または PPTP を介した AnyConnect の設定

デフォルトでは、[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.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[PPP Exclusion] でその方式を選択します。このフィールドで [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。

- [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。
- [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。
- [Disabled] : PPP 除外は適用されません。

ステップ 4　[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 [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 VPN Client\preferences.xml。次に例を示します。
  - Windows Vista : C:\Users*username*\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
  - Windows XP : C:\Documents and Settings**username**\Local Settings\Application Data\Cisco\Cisco AnyConnect VPN 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 VPN プロファイル エディタのパラメータに関する説明

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）

[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。

[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.12-15）を参照してください。

[Certificate Store]：AnyConnect がどの証明書ストアで証明書を保存し、読み取るかを制御します。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。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。

- [All]：（デフォルト）証明書は両方のストアに保存されています。
- [Machine]：マシン ストアを使用します。
- [User]：ユーザ証明書ストアを使用します。

[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、証明書がマシン 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。

[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。

[Minimize On Connect]：VPN 接続の確立後、AnyConnect GUI が最小化されます。

[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）　[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、デフォルト グループ ポリシーに含まれている AnyConnect クライアント ローカル印刷ファイアウォール ルールを使用した SSL クライアント ファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [Preferences (Part 2)] で [Automatic VPN Policy]、[Always On]、および [Allow VPN Disconnect] も有効にする必要があります。

[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）。[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。

[Auto Update]：オンにすると、クライアントの自動アップデートが有効になります。[User Controllable] チェックボックスをオンにすると、クライアントのこの設定を無効にできます。

[RSA 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）。

- [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。
- [Software Token]：ソフトウェア トークンのみ許可されます。
- [Hardware Token]：ハードウェア トークンのみ許可されます。

[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 トンネリングはグループ ポリシーで設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は AnyConnect により解除されます。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。

- [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。
- [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 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。

- [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。
- [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 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 Establishment] の設定が [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。

- [IP Protocol Supported]：IPv4 アドレスおよび IPv6 アドレスの両方で AnyConnect を使用して ASA に接続しようとしているクライアントの場合、AnyConnect は接続の開始に際してどの IP プロトコルを使用するか決定する必要があります。デフォルトで、AnyConnect は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、IPv6 を使用して接続を開始しようとします。

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

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

（注）　IPv4 から IPv6、IPv6 から IPv4 プロトコルへのフェールオーバーも VPN セッション中に行うことができます。プライマリ IP プロトコルが失われると、可能な場合に、セカンダリ IP プロトコルを介して VPN セッションが再確立されます。

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。

- 「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.3-16）
- 「証明書の失効通知の設定」（P.3-51）
- 「自動再接続の設定」（P.3-66）
- 「Windows RDP セッションによる VPN セッションの起動」（P.3-77）

AnyConnect プロファイル エディタ、プリファレンス（パート 2）

[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。

[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。

[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。

- [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。
- [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。
- [Override]（サポートされていません）

[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 [Connection] タブにある [Connect To] ドロップダウン リストには [Automatic Selection] が表示されます。

- [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。
- [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。

[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） [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。

- [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。
  - [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。
  - [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。
  - [Do Nothing]：信頼ネットワークでは動作はありません。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。

  - [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。

- [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。
  - [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。
  - [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、VPN 常時接続は無効となります。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。
- [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。
- [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、192.168.1.2, 2001:DB8::1 です。
- [Always On]：対応している Windows または Mac OS X オペレーティング システムのいずれかを実行しているコンピュータにユーザがログインした場合、AnyConnect が VPN へ自動的に接続するかどうかを判断します。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 VPN 常時接続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 VPN 常時接続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。

  [Always On] チェックボックスをオンにした後、[Allow VPN Disconnect] チェックボックスをオンにできます。
- [Allow VPN Disconnect]：AnyConnect で VPN 常時接続セッション用の [Disconnect] ボタンが表示されるようにするかどうかを指定します。VPN 常時接続セッションのユーザは、[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　[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、[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、「VPN 常時接続用の [Disconnect] ボタン」（P.3-28）を参照してください。

[AllowVPN Disconnect] を有効にした後、[Connect Failure Policy]、[Allow Captive Portal Remediation]、および [Apply Last VPN Local Resource Rules] を設定できます。

- [Connect Failure Policy] : AnyConnect が VPN セッションを確立できない場合（ASA が到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、VPN 常時接続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「VPN 常時接続に関する接続障害ポリシー」（P.3-29）を一読してください。

  - [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。
  - [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。

    [Connect Failure Policy] : 接続障害ポリシーを Closed にすると、次の設定を行うことができます。
  - [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。
  - [Remediation Timeout] : AnyConnect によりネットワーク アクセスの制限が解除されるまでの時間（分）。このパラメータは、[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）。
  - [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 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 [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。

- [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。
- [Disabled] : PPP 除外は適用されません。
- [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.3-79）の説明に従うよう指示してください。

[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。

[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。

- [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。
- [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）。

[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。

- [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、[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。

[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」（P.3-66）
- 「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」（P.3-75）
- 「最適ゲートウェイ選択」（P.3-67）
- 「Trusted Network Detection の設定」（P.3-21）
- 「VPN 常時接続」（P.3-23）
- 「VPN 常時接続に関する接続障害ポリシー」（P.3-29）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-32）
- 「L2TP または PPTP を介した AnyConnect」（P.3-78）
- 「認証タイムアウト コントロール」（P.3-74）

AnyConnect プロファイル エディタの [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。

[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。

[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。

[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。

[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。

[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.3-65）を参照してください。

AnyConnect プロファイル エディタの [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。

[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。

[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）

[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）。

[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。

[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

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

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

[Wildcard]：[Enabled] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。

[Operator]：この DN で照合する場合に使用する演算子です。

- [Equal]：== と同等
- [Not Equal]：!= と同等

[Match Case]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

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.3-55）を参照してください。

AnyConnect プロファイル エディタの [Certificate Enrollment]

[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。

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

[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]：レガシー SCEP の場合、SCEP CA サーバを特定します。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）。

- [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 [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。
- [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、発行したサーバ証明書の「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。

[Certificate Contents]：SCEP 登録要求に含める証明書の内容を指定します。

- Name (CN)：証明書での一般名。
- Department (OU)：証明書に指定されている部署名。
- Company (O)：証明書に指定されている会社名。
- State (ST)：証明書に指定されている州 ID。
- State (SP)：別の州 ID。
- Country (C)：証明書に指定されている国 ID。

- Email (EA)：電子メール アドレス。次の例では、[Email (EA)] は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
- Domain (DC)：ドメイン コンポーネント。次の例では、[Domain (DC)] は cisco.com に設定されています。
- SurName (SN)：姓または名。
- GivenName (GN)：通常は名。
- UnstructName (N)：定義されていない名前。
- Initials (I)：ユーザのイニシャル。
- Qualifier (GEN)：ユーザの世代修飾子 （「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。

[Display Get Certificate Button]：次の条件下で AnyConnect GUI が [Get Certificate] ボタンを表示できるようにします。

- 証明書は [Certificate Expiration Threshold] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
- 証明書の期限が切れている。
- 証明書がない。
- 証明書を照合できない。

[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.3-45）を参照してください。

AnyConnect プロファイル エディタの [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。

- [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。
- [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。
- [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。
- [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。
  - [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。
  - [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 [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。

[Server List] テーブルの列は次のとおりです。

- [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。
- [Host Address]：サーバの IP アドレスまたは FQDN。
- [User Group]：[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。
- [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。

[Add/Edit]：サーバのパラメータを指定できる [Server List Entry] ダイアログを起動します。

[Delete]：サーバ リストからサーバを削除します。

[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 [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。

[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。

[Host Address]：サーバの IP アドレスまたは FQDN を指定します。

（注）
- [Host Address] フィールドに IP アドレスまたは FQDN を指定すると、[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。
- [Hostname] フィールドで FQDN のみを指定し、[Host Address] フィールドでは IP アドレスを指定しない場合、[Hostname] フィールドの FQDN が DNS で解決されます。
- IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイの使用はサポートしていません。

[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。

[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。

- [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。
- [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。
- [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。
- [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。
- [Delete]：サーバ リストからバックアップ サーバを削除します。

[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。

- [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。
- [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。
- [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。

[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。

[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、一部の機能が無効になります。

（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 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）。

- [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 [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。
- [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.3-60）を参照してください。

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。

- Windows 7 における有線（IEEE 802.3）、ワイヤレス（IEEE 802.11）、一部のモバイル ブロードバンド（3G）ネットワーク アダプタ。サポート対象アダプタのリスト一式については、『*Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1*』を参照してください。
- Windows マシン クレデンシャルを使用した事前ログイン認証
- 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 メソッド群：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみ EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）
- 内部 EAP メソッド群：
  - 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 メソッド（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 対応の唯一のアダプタは、Cisco CB21AG on Windows XP です。

- スマートカード提供クレデンシャル。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（CNG）
  - Windows ログオンは ECDSA 証明書に対応していないため、ネットワーク アクセス マネージャのシングル サインオン（SSO）は ECDSA クライアント証明書に対応していません。

（注）　ネットワーク アクセス マネージャは MAC または Linux には対応していません。

Suite B および FIPS

次の機能は FIPS 認定で、例外を列挙しています。

- ACS および ISE は SuiteB には対応していませんが、FreeRADIUS 2.x + OpenSSL 1.x は対応しています。Microsoft NPS 2008 は Suite-B に一部対応しています（NPS の証明書は RSA でなければなりません）。
- 802.1X/EAP は（RFC5430 で定義されているように）暫定 Suite B プロファイルにのみ対応しています。TLS 1.2 には対応していません。
- MACsec は Windows 7 でのみ FIPS 対応です。
- Windows 7 および XP の Elliptic Curve Diffie-Hellman（ECDH）キー交換
- ECDSA クライアント証明書は Windows 7 および Vista のみに対応しています
- OS ストアの ECDSA CA 証明書は Windows 7 および Vista のみに対応しています。
- PEM エンコードされた）ネットワーク プロファイルの ECDSA CA 証明書は Windows XP/7/Vista に対応しています。
- サーバの ECDSA 証明書チェーン検証は Windows XP/7/Vista に対応しています。

シングル サインオン「シングル ユーザ」の適用

Microsoft Windows XP、Windows 7 および Vista では、複数のユーザが同時にログインできますが、AnyConnect ネットワーク アクセス マネージャはネットワーク認証を 1 人のユーザに制限しています。AnyConnect ネットワーク アクセス マネージャは、ログインしているユーザの数に関係なく、デスクトップまたはサーバ当たり 1 人のユーザにのみアクティブにできます。シングル ユーザ ログインの適用は、いつでもシステムにログインできるユーザは 1 人のみで、管理者は現在ログインしているユーザを強制的にログオフできないことを示しています。

ネットワーク アクセス マネージャ クライアント モジュールが Windows デスクトップにインストールされている場合、デフォルト動作はシングル ユーザ ログインを適用することです。サーバにインストールされている場合、デフォルト動作はシングル ユーザ ログインの適用を緩和することです。 いずれの場合も、レジストリ キーを変更または追加して、デフォルト動作を変更できます。

シングル サインオンのシングル ユーザの適用には、次の機能と制限事項があります。

- Windows 管理者は、現在ログインしているユーザの強制的なログオフが制限されます。
- 接続されたワークステーションへの RDP は同一ユーザにサポートされています。
- 同一ユーザと見なされるためには、クレデンシャルを同じフォーマットにする必要があります。たとえば、me/mydomain は me@mydomain.com と同じではありません。
- また、スマートカード ユーザが同じ PIN を持っている場合、同一ユーザと見なされます。

シングル サインオンのシングル ユーザの適用の設定

Window のワークステーションまたはサーバによる複数ユーザの処理方法を変更したい場合は、レジストリの EnforceSingleLogon の値を変更します。ネットワーク アクセス マネージャはそのキーを Windows XP に追加しませんが、Windows ログイン アクセスを変更する場合は追加できます。レジストリ キーは EnforceSingleLogon で、OverlayIcon レジストリ キーと同じ場所にあります。値 1 は、シングル ユーザ ログインが適用されていることを示し、値 0 は複数ユーザがログインしている可能性があることを示します。

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 6.8

（注） スタンドアロン ネットワーク アクセス マネージャ エディタが、ネットワーク アクセス マネージャ プロファイルを設定する代替方法としてサポートされています。セキュリティ上の理由で、AnyConnect は、AnyConnect プロファイル エディタ外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 マネージャに対応しています。
  - 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）、IPv6 および Suite-B はサポート対象外
  - Windows Server 2008 R2

ライセンスとアップグレード要件

シスコ ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、RADIUS サーバで使用する場合は、AnyConnect ネットワーク アクセス マネージャは無償でライセンスが与えられています。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 マネージャの展開

ネットワーク アクセス マネージャは AnyConnect の一部として展開されます。AnyConnect のインストール方法、またネットワーク アクセス マネージャと他のモジュールについては、「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 プロファイルの作成

ネットワーク アクセス マネージャ プロファイルは AnyConnnect の一部としてエンドポイントで展開されているため、ネットワーク アクセス マネージャは管理上定義されたエンド ユーザ要件および認証ポリシーを適用でき、エンド ユーザは事前設定されたネットワーク プロファイルを利用できます。

ネットワーク アクセス マネージャ プロファイル エディタを使用して、1 つ以上のネットワーク アクセス マネージャ プロファイルを作成し、設定します。AnyConnect には ASDM の一部であるプロファイル エディタが、スタンドアロン Windows 版として組み込まれています。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。

（注）　クライアント イメージをアップロードするまで、クライアント プロファイルを作成できません。

ASDM からの新しいプロファイルの追加

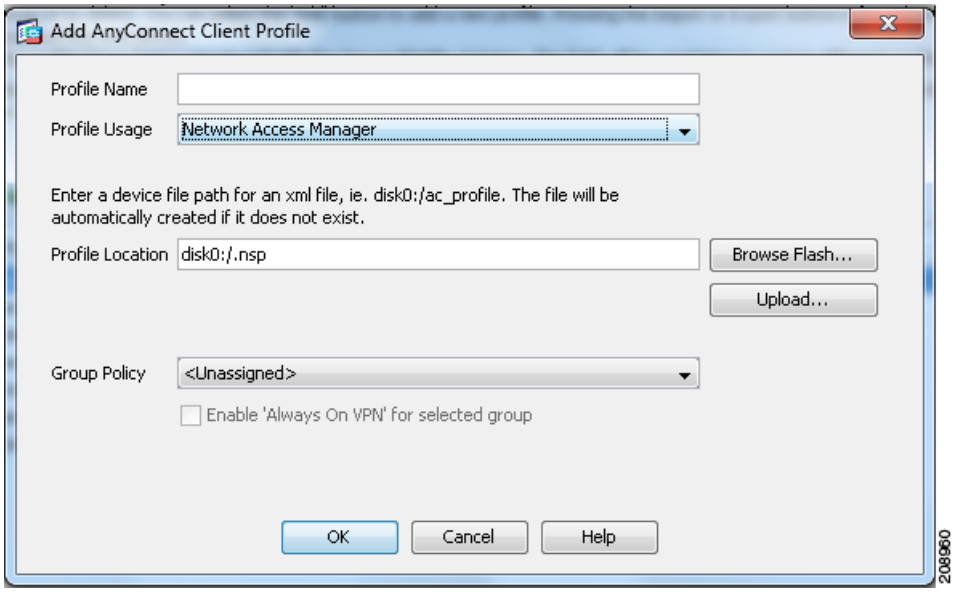
次の手順を実行して、新しいネットワーク アクセス マネージャ クライアント プロファイルを ASDM から ASA に追加します。

ステップ 1　ASDM を開いて [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 2　[Add] をクリックします。

ステップ 3　[Add AnyConnect Client Profile] ウィンドウが開きます（図 4-1 を参照）。

図 4-1　[Add AnyConnect Client Profile] ウィンドウ



ステップ 4　プロファイル名を入力します。

ステップ 5　[Profile Usage] ドロップダウン リストから、[Network Access Manager] を選択します。

ステップ 6　（任意）[Profile Location] フィールドで [Browse Flash] をクリックし、ASA の XML ファイルのデバイス ファイル パスを選択します。

ステップ 7　（任意）スタンドアロン エディタを使用してネットワーク アクセス マネージャ プロファイルを作成した場合、[Upload] をクリックして、そのプロファイル定義を使用します。

ステップ 8　（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 9　[OK] をクリックします。

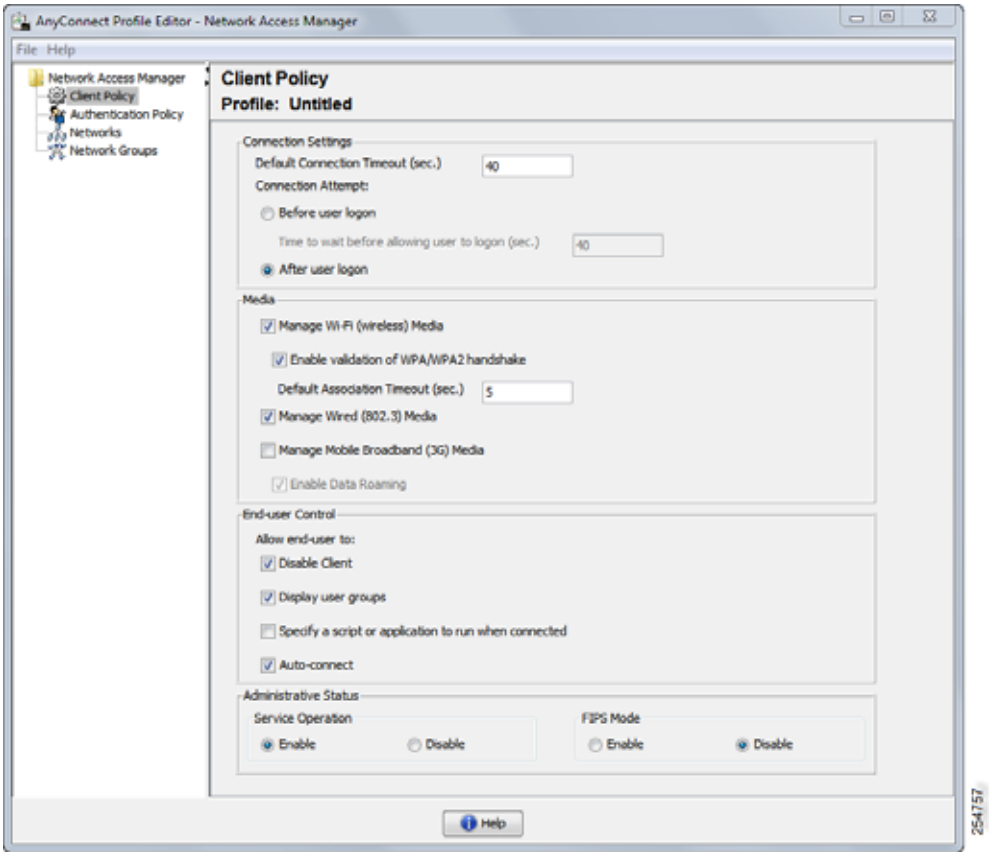
ネットワーク アクセス マネージャ プロファイルの設定

ネットワーク アクセス マネージャ プロファイルは、ネットワーク アクセス マネージャ プロファイル エディタで設定されます。このエディタは ASDM でスタンドアロン Windows アプリケーションとして使用できます。

[Client Policy] ウィンドウ

[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　[Client Policy] ウィンドウ



次の 4 つのセクションで構成されます。

- [Connection Settings]：ユーザ ログインの前または後にネットワーク接続しようとするかどうかを定義できます。
  - [Default Connection Timeout]：ユーザ作成ネットワークの接続タイムアウトとして使用する秒数。デフォルト値は 40 秒です。
  - [Before User Logon]：ユーザがログインする前にネットワークに接続します。サポートされているユーザ ログインの種類として、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、GPO ベースのログイン スクリプト実行があります。

    [Before User Logon] を選択した場合、[Time to Wait Before Allowing a User to Logon] も設定することになります。

    [Time to Wait Before Allowing User to Logon]：ネットワーク アクセス マネージャが完全にネットワーク接続するのに待機する最大（最悪のケース）秒数を指定します。この時間内にネットワーク接続が確立できない場合、Windows ログイン プロセスはユーザ ログインにより継続されます。デフォルトは 5 秒です。

（注）　ワイヤレス接続を管理するようネットワーク アクセス マネージャが設定されている場合、[Time to wait before allowing user to logon] を 30 秒以上に設定します。ワイヤレス接続の確立にさらに時間が必要になる可能性があるためです。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。

  - [After User Logon]：ユーザが Windows にログインした後に、ネットワーク アクセス マネージャがネットワーク接続を確立しようとすることを指定します。

- [Media]：ネットワーク アクセス マネージャ クライアントにより制御されるメディアの種類を指定します。
  - [Manage Wi-Fi (wireless) Media] : WiFi メディアの管理、また任意で WPA/WPA2 ハンドシェイクの検証ができるようになります。

    IEEE 802.11i ワイヤレス ネットワーキング規格は、サプリカント（ここではネットワーク アクセス マネージャ）が、キー導出中に IEEE 801.X プロトコル パケットの EAPOL Key データで送信されたアクセス ポイントの RSN IE（Robust Secure Network Information Exchange）がビーコン/プローブ応答フレームで検出されたアクセス ポイントの RSN IE と一致することを検証する必要があることを指定します。WPA/WPA2 ハンドシェイクの検証を有効にする場合、デフォルトのアソシエーション 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有効化をオフにすると、この検証手順は省略されます。

    （注）　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。

  - [Manage Wired (IEEE 802.3) Media]：有線接続の管理を有効にします。
  - [Manage Mobile Broadband (3G) Media]：Windows 7 モバイル ブロードバンド アダプタの管理を有効にし、データ ローミングを許可するか指定します。この機能はベータ版に入っています。

    （注）　Cisco TAC は、ベータ版には対応していません。

- [End-user Control]：ユーザの次の制御を設定できます。
  - [Disable Client]：ユーザは、AnyConnect UI を使用して、ネットワーク アクセス マネージャによる有線メディアおよびワイヤレス メディアの管理を無効および有効にできます。
  - [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。
  - [Specify a Script or Application To Run When Connected]：ユーザは、ネットワーク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指定できます。

（注）　スクリプト設定は 1 つのユーザ設定ネットワークに固有であり、ユーザはローカル ファイル（.exe、.bat、または .cmd）を指定して、そのネットワークが接続状態になった時に実行できます。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、ユーザが実行中のスクリプトを設定できないようにする場合、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。

  - [Auto-connect]：選択されている場合、ユーザが選択しなくても、ネットワーク アクセス マネージャは自動的にネットワークに接続します。デフォルトは自動接続です。

- Administrative Status
  - [Service Operation]：このサービスを無効にすると、このプロファイルを使用しているクライアントはレイヤ 2 接続を確立するために接続できません。
  - [FIPS Mode]：連邦情報処理標準（FIPS 140-2 Level 1）は米国 政府の規格で、暗号化モジュールのセキュリティ要件を指定します。FIPS モードを有効にすると、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操作を行います。追加情報については、第 9 章「NGE、FIPS、および追加セキュリティ」を参照してください。

    FIPS は、次の表に示すようにソフトウェアとハードウェアの種類に応じて、MACsec または Wifi 向けのネットワーク アクセス マネージャによりサポートされています。

表 4-1　ネットワーク アクセス マネージャによる FIPS サポート

メディア/オペレーティング システム	Windows XP/2003	Windows 7/Vista
MACsec で有線	FIPS に準拠していません。	Intel HW MACsec 対応 NIC の場合、またはハードウェア以外の MACsec を使用している場合に FIPS に準拠しています。
Wifi	3eti ドライバがインストールされている場合に FIPS に準拠しています。	FIPS に準拠していません。

[Authentication Policy] ウィンドウ

[Authentication Policy] ウィンドウでは、すべてのネットワーク接続に適用される、アソシエーションおよび認証ネットワーク フィルタを作成できます。アソシエーション モードまたは認証モードのいずれもオンにしない場合、認証 wi-fi ネットワークに接続できません。モードのサブセットを選択すると、それらのタイプのネットワークにのみ接続できます。目的のアソシエーション モードまたは認証モードをそれぞれ選択するか、[Select All] を選択します。

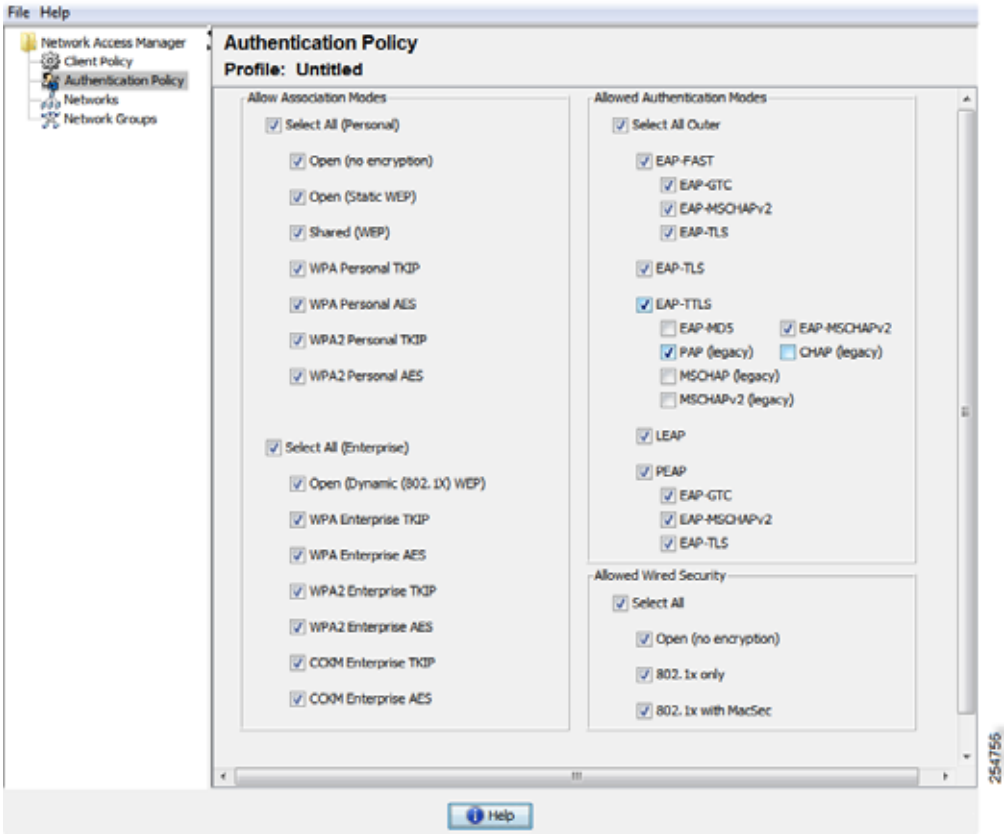
内部方式も特定の認証プロトコルのみに制限される可能性がある点に注意してください。内部方式は、[Allowed Authentication Modes] ペインの外部方式（トンネリング）下にインデントされて表示されます。

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。

内部トンネリングに使用できる EAP 方式は、内部方式のクレデンシャル タイプと外部トンネリング方式に基づいています。次のリストで、外部トンネル方式はそれぞれ、各クレデンシャル タイプに対応した内部方式の種類を一覧表示しています。

- PEAP
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-FAST
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-TTLS
  - パスワード クレデンシャル：EAP-MSCHAPv2、EAP-MD5、PAP（L）、CHAP（L）、MSCHAP（L）、MSCHAP-v2（レガシー）
  - トークン クレデンシャル：PAP（レガシー）チャレンジ/レスポンス方式はトークン ベースの認証には適していないため、NAM でサポートされるデフォルト トークン オプションは PAP です。
  - 証明書クレデンシャル：該当なし

図 4-3　[Authentication Policy] ウィンドウ



[Networks] ウィンドウ

[Networks] ウィンドウでは、企業ユーザの事前定義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。[Networks] ウィンドウでは、ウィザードが起動して既存のウィンドウにペインが追加される場合があり、[Next] をクリックして詳細な設定オプションに進みます。

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。[Network Groups] ウィンドウの [*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。グローバル ネットワーク 内にあるネットワークを制御できるため、ユーザ定義のネットワーク内にある場合でも、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。エンド ユーザは管理者が設定したネットワークを変更したり、削除したりできません。

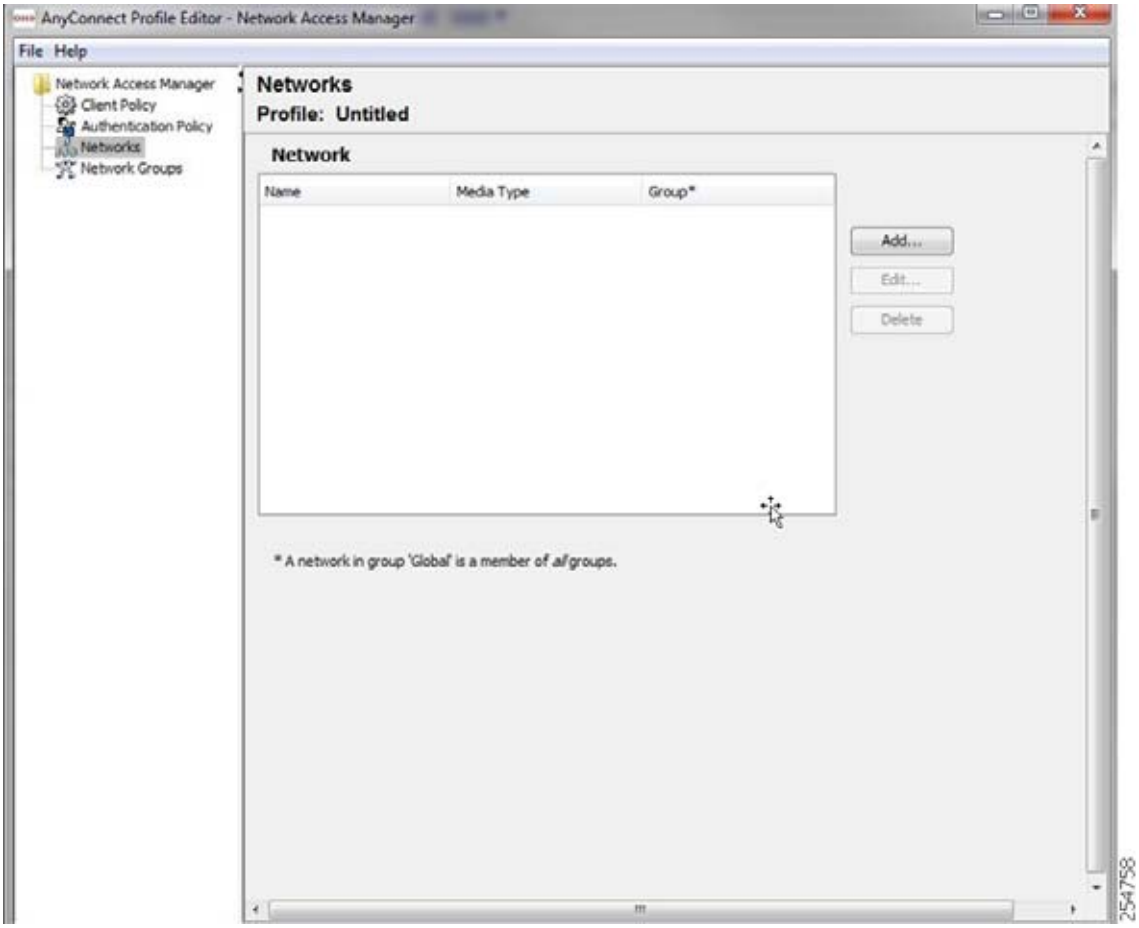
（注） エンド ユーザは、globalNetworks セクションのネットワークを除き、グループにネットワークを追加できます。これらのネットワークはすべてのグループ内に存在し、プロファイル エディタを使用してしか作成できないためです。

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 グループは設定内の最初のグループですが、グループが 1 つしか使用できない場合、アクティブ グループは認識されず、表示されません。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。ユーザはアクティブ グループから選択でき、設定は再起動後も保持されます。[Network Groups] ウィンドウの [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分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 [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。

[Network Access Manager] メニューから [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　[Networks] ウィンドウ



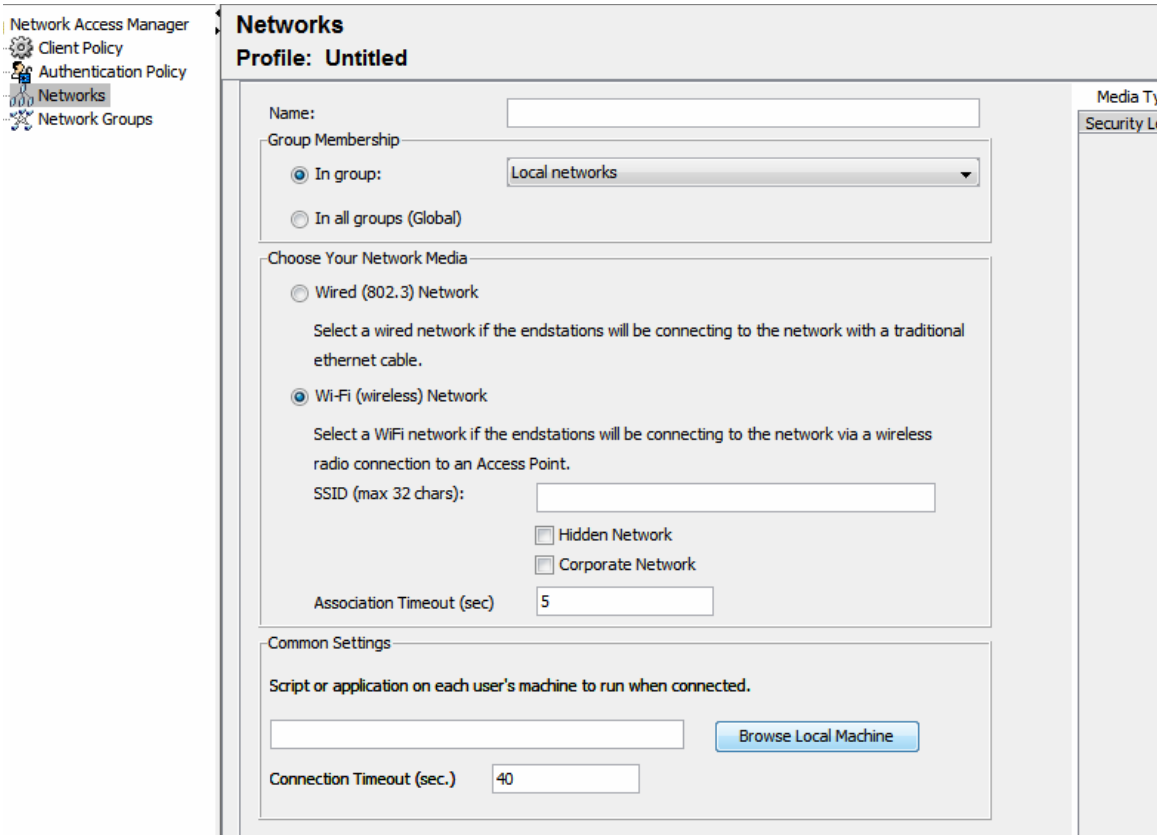
次のいずれかのアクションを選択します。

- 新しいネットワークを作成するには、[Add] をクリックします。新しいネットワークを作成する場合、次の項の情報を使用して、クライアント プロファイルを設定します。まず、次の項 [Networks] - [Media Type] ページから始めます。
- 変更するネットワークを選択して、[Edit] をクリックします。
- 削除するネットワークを選択して、[Delete] をクリックします。

[Networks] - [Media Type] ページ

[Networks] ウィンドウの [Media Type] ページにより、有線ネットワークまたはワイヤレス ネットワークを作成または編集できます。設定は、有線を選択するか、ワイヤレスを選択するかによって異なります。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　[Media Type] ページ



最初のダイアログでは、セクションは 4 つあります。

- [Group Membership]：このプロファイルが使用できるはずであるネットワーク グループ（複数の場合もあり）を選択します。
- [Name]：このネットワークに表示される名前を入力します。
- [Network Media]：[Wired] または [Wi-Fi (wireless)] を選択します。[Wi-Fi] を選択すると、次のパラメータも設定できます。
  - SSID パラメータで、ワイヤレス ネットワークの SSID（Service Set Identifier）を入力します。
  - ネットワークの SSID をブロードキャストしていなくても、ネットワークに接続させる場合は [Hidden Network] を選択します。
  - 企業ネットワークが近くにある場合、最初に Corporate として設定されたネットワークへ強制的に接続する場合は [Corporate Network] を選択します。企業ネットワークが非ブロードキャスト（非表示）SSID を使用し、非表示として設定されている場合、NAM は非表示 SSID をアクティブにプローブし、企業の SSID が圏内にある場合、接続を確立します。
  - [Association Timeout]：ネットワーク アクセス マネージャが、使用できるネットワークを再評価するまで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時間を入力します。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。

- [Common Settings] :
  - [Script or application] : ローカル システムで実行するファイルのパスとファイル名を入力するか、フォルダを参照してファイルを選択します。次のルールは、スクリプトおよびアプリケーションに適用されます。

    .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、管理者が作成したネットワークで定義されたスクリプトまたはアプリケーションは変更できません。

    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、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。
  - [Connection Timeout] : ネットワーク アクセス マネージャが、（接続モードが自動の場合）別のネットワークに接続しようとする、または別のアダプタを使用するまで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） 認証を完了するまでに 60 秒近くかかるスマートカード認証システムもあります。スマートカードを使用している場合、特に、スマートカードが接続に成功するまでにいくつかネットワークに接続しなければならない場合に、[Connection Timeout] 値を増やさなければならない場合があります。

ネットワーク接続に関する注意事項

ネットワーク アクセス マネージャは、エンド ユーザのネットワーク スキャン リストで見つかった設定済みネットワークにのみ接続しようとします。

Windows 7 では、ネットワーク アクセス マネージャは非表示 SSID をプローブします。最初の非表示 SSID が見つかると、検索を中止します。複数の非表示ネットワークが設定されている場合、ネットワーク アクセス マネージャは次のように SSID を選択します。

- 管理者が定義した最初の非表示企業ネットワーク
- 管理者が定義した非表示ネットワーク
- ユーザが定義した最初の非表示ネットワーク

ネットワーク アクセス マネージャは一度に 1 つの非ブロードキャスト SSID しかプローブしないため、サイトの非表示企業ネットワークは 1 つのみにすることをお勧めします。

ネットワークの設定が完了したら、[Next] をクリックして、[Networks] ウィザードの [Security Level] ペインを表示します。

[Networks] - [Security Level] ページ

[Networks] ウィザードの [Security Level] ページで、[Open Network]、[Authentication Network]、または（ワイヤレス ネットワーク メディアにのみ表示された）[Shared Key Network] を選択します。これらのネットワーク タイプの設定フローはそれぞれ異なっており、次の項で説明します。

- [Authenticating Network] の設定：**セキュアな企業**にお勧めします。
- オープン ネットワークの設定：お勧めしませんが、キャプティブ ポータル環境からゲスト アクセスをする場合に使用できます。
- 共有キー ネットワークの設定：**小規模オフィス**または自宅のオフィスなど、ワイヤレス ネットワークにお勧めします。

[Authenticating Network] の設定

[Security Level] セクションで [Authenticating Network] を選択した場合、以下に説明するペインが追加で表示されます。このペインの設定を完了したら、[Next] ボタンをクリックするか、[Connection Type] タブを選択して [Network Connection Type] ダイアログを開きます。

[802.1X Settings] ペイン

ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

- [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。
- [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。
- [startPeriod(sec)]：EAPOL-Start メッセージに対する応答をオーセンティケータから受信しない場合に、EAPOL-Start メッセージを再送信する間隔（秒）です。
- [maxStart]：サプリカントが、オーセンティケータがいないと見なす前に、IEEE 801.X プロトコル パケット、EAPOL Key データ、EAPoL-Start を送信することで、サプリカントがオーセンティケータの認証を開始する回数です。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、[startPeriod] および [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（[startPeriod] x [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（[startPeriod] x [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 トラフィックを行いたい管理者は、認証の開始に費やした総時間がネットワーク接続タイマーより長くなるような startPeriod および maxStart になるようにします（[start Period x maxStart] > [Network Connection Timer]）。

[Security] ペイン

有線ネットワークの場合のみ表示されます。

[Security] ペインで、次のパラメータの値を選択します。

- [Key Management]：ドロップダウン リストを使用して、MACsec 対応有線ネットワークで使用するキー管理プロトコルを決定します。
  - [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 キー管理プロトコル ポリシーと暗号キーをネゴシエートしようとします。MACsec は MAC レイヤ セキュリティで、有線ネットワークで MAC レイヤ暗号化を行います。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。

- Encryption
  - [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]：このオプションは、キー管理に MKA を選択した場合のみ使用できます。ES-GCM-128 を使用して、データ トラフィックが暗号化されます。

[Port Authentication Exception Policy] ペイン

有線ネットワークの場合のみ表示されます。

[Port Authentication Exception Policy] では、認証プロセス中の IEEE 802.1x サプリカントの動作を変更できます。ポート例外が有効でない場合、サプリカントはその既存の動作を続け、設定が完全に成功した場合のみ（または、この項で前述したように、オーセンティケータからの応答がない状態で maxStarts 数の認証が開始された後に）ポートを開きます。次のいずれかのオプションを選択します。

- [Allow data traffic before authentication]：このオプションにより、認証試行の前にデータ トラフィックが許可されます。
- [Allow data traffic after authentication even if]：次の場合でもデータ トラフィックが許可されます。
  - [EAP Fails]：選択すると、EAP が失敗した場合でも、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 succeeds but key management fails]：選択すると、EAP は成功してキー管理が失敗した場合、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 またはスイッチの設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

アソシエーション モード

ワイヤレス ネットワークの場合のみ表示されます。

アソシエーション モードを選択します。オプションは次のとおりです。

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- [CCKM (TKIP)]：（Cisco CB21AG ワイヤレス NIC が必要）
- [CCKM (AES)]：（Cisco CB21AG ワイヤレス NIC が必要）

オープン ネットワークの設定

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　[Security Level] ページで [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　[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。[Networks] - [Network Connection Type] ペインを参照してください。

[Next] をクリックするか [Connection Type] タブを選択すると、[Network Connection Type] ダイアログが開きます。

共有キー ネットワークの設定

Wi-Fi ネットワークは、エンド ポイントとネットワーク 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、暗号キーを導出する場合に共有キーを使用することがあります。WPA または WPA2 Personal を備えた共有キーを使用すると、小規模オフィスや自宅オフィスに適した Medium レベルのセキュリティ クラスが実現します。

（注）　共有キーによるセキュリティは、企業ワイヤレス ネットワークにはお勧めしません。

セキュリティ レベルを [Shared Key Network] にする場合は、次の手順を実行します。

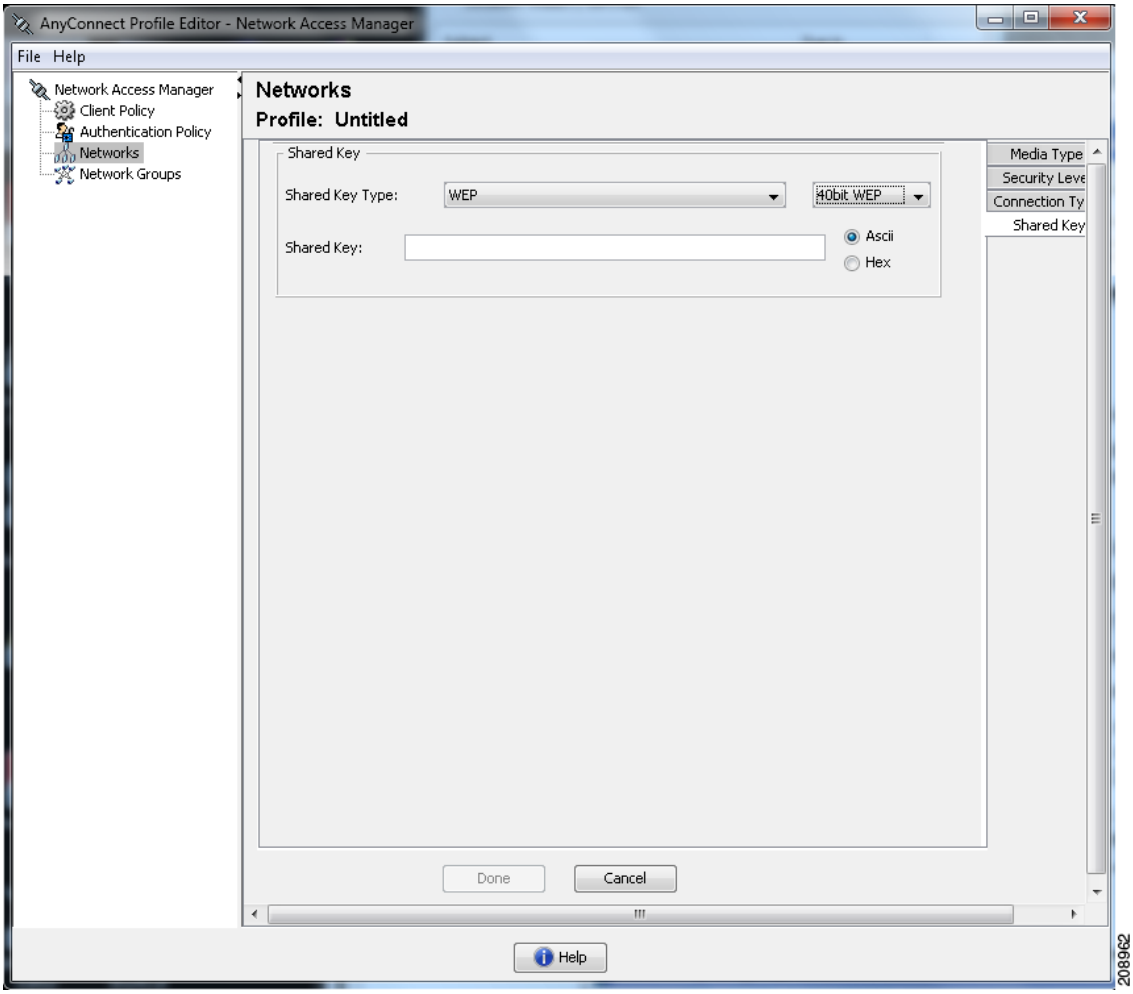
ステップ 1　[Shared Key Network] を選択します。

ステップ 2　[Security Level] ウィンドウで [Next] をクリックします。

ステップ 3　[User Connection] または [Machine Connection] を指定します。詳細については、「[Networks] - [Network Connection Type] ペイン」（P.4-19）を参照してください。

ステップ 4　[Next] をクリックします。[Shared Key] ペインが表示されます（図 4-6 を参照）。

図 4-6　[Shared Key] ペイン



ステップ 5　[Shared Key Type]：共有キーのタイプを決定する共有キー 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 暗号化とのレガシー IEEE 802.11 オープン システム アソシエーション
- [Shared]：スタティック WEP 暗号化とのレガシー IEEE 802.11 共有キー アソシエーション
- [WPA/WPA2-Personal]：パスフレーズ事前共有キー（PSK）から暗号キーを導出する Wi-Fi セキュリティ プロトコル

ステップ 6　レガシー IEEE 802.11 WEP または共有キーを選択した場合は、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 を選択した場合は、（TKIP/AES）を使用する暗号化のタイプを選択し、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、[Hexadecimal] を選択します。

ステップ 8　[Done] をクリックします。[OK] をクリックします。

[Networks] - [Network Connection Type] ペイン

ここでは、ネットワーク アクセス マネージャ プロファイル エディタのセキュリティ レベルに続いて、[Networks] ウィンドウの [Network Connection Type] ペインについて説明します。オープン ネットワークのペインを図 4-7 に示します。次のいずれかの接続タイプを選択します。

- [Machine Connection] : マシンの Windows Active Directory ID を認証に使用します。マシン接続は通常、接続時にユーザ クレデンシャルが必要ない場合に使用します。ユーザがログオフし、ユーザ クレデンシャルが使用できない場合でも、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にこのオプションを選択します。このオプションは通常、ユーザがアクセスする前に、ドメインに接続し、ネットワークから GPO および他のアップデートを取得する場合に使用します。

  （注）　既知のネットワークが使用できない場合、VPN start before login（SBL）は失敗します。しかし、ネットワーク アクセス マネージャを [*Before user logon*] に、またマシン接続認証を設定している場合、ネットワーク アクセス マネージャはユーザにネットワーク情報を要求し、VPN SBL は正常に行われます。

- [User Connection] : ユーザ クレデンシャルを認証に使用します。

  [Client Policy] ペインで [*Before user logon*] が選択された場合、Windows スタート画面でユーザがログオン クレデンシャルを入力した後、ネットワーク アクセス マネージャはユーザのクレデンシャルを収集します。Windows がユーザの Windows セッションを開始している間に、ネットワーク接続が確立されます。

  [Client Policy] ペインで [*After user logon*] が選択された場合、ユーザが Windows にログインしてから、接続が開始されます。

  ユーザがログオフすると、現在のユーザのネットワーク接続は終了します。マシン ネットワーク プロファイルが使用できる場合、NAM はマシン ネットワークに再接続します。

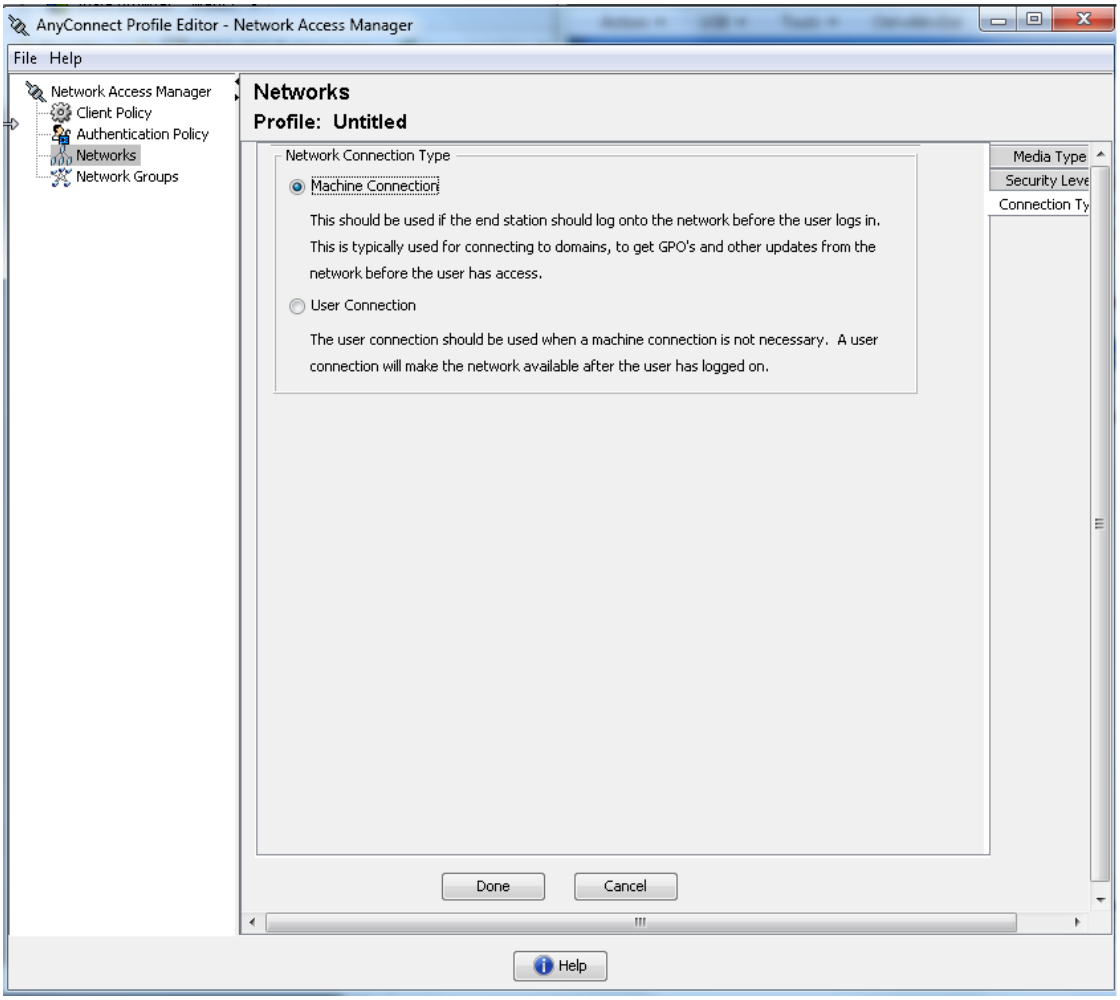
- [Machine and User Connection] : [Security Level] ペインで選択したように、[*Authenticating Network*] を設定している場合のみ指定できます。マシン ID とユーザ クレデンシャルの両方を使用しますが、マシン部分はユーザが PC にログインしていない場合のみ有効です。2 つの部分の設定は同じですが、マシン接続の認証タイプとクレデンシャルは、ユーザ接続の認証タイプとクレデンシャルと異なる場合があります。

  [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 [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。

  EAP-FAST が（次のペインで）EAP 方式として設定されている場合、EAP チェーンがサポートされています。つまりネットワーク アクセス マネージャは、マシンとユーザが既知のエンティティで、企業により管理されていることを検証するということです。これは、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）に便利です。

  [Network Connection Type] を選択すると、[Networks] ダイアログにその他のタブが表示されます。これらのタブでは、選択された [Network Connection Type] の EAP 方式とクレデンシャルを設定できます。

図 4-7　オープン ネットワークの [Network Connection Type] ペイン



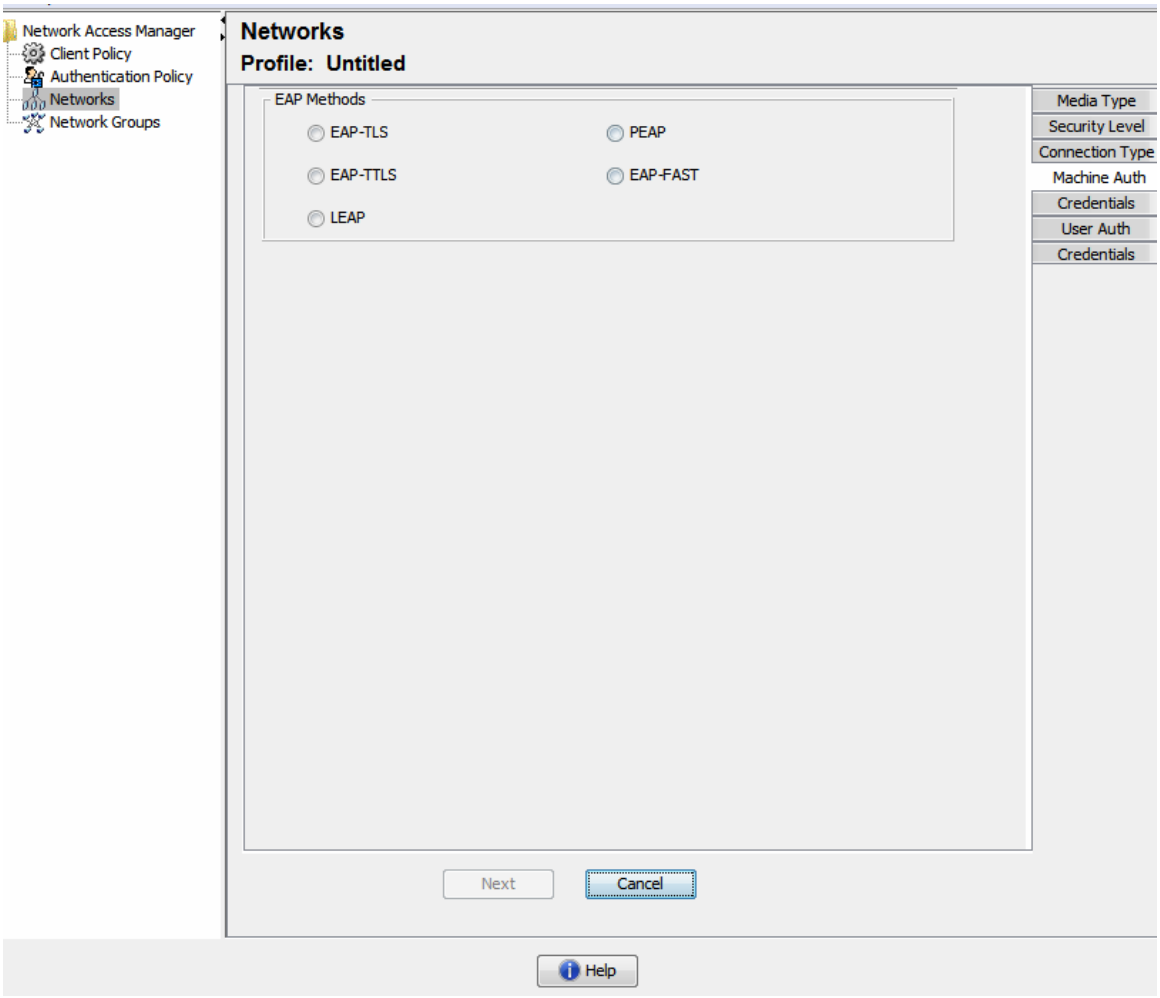
[Networks] - [User Authentication] または [Machine Authentication] ページ

[Network Connection Type] を選択した後、それらの接続タイプの認証方式を選択しました。認証方式を選択したら、ウィンドウの中央に選択した方式が適用され、さらに情報を指定する必要があります。

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、「Using a Windows Remote Desktop」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 4-8 の [EAP Methods] ペインは、ワイヤレス ネットワークのユーザ認証を示しています。

図 4-8　ワイヤレスの [User Authentication] ペイン



（注）　MACsec を有効にした場合は、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。

選択した EAP 方式によって、このペインで設定を追加できます。

- EAP-GTC：「EAP-GTC の設定」（P.4-22）を参照してください。
- EAP-TLS：「EAP-TLS の設定」（P.4-23）を参照してください。
- EAP-TTLS：「EAP-TTLS の設定」（P.4-23）を参照してください。
- PEAP：「PEAP オプションの設定」（P.4-25）を参照してください。
- EAP-FAST：「EAP-FAST の設定」（P.4-26）を参照してください。
- LEAP：「LEAP の設定」（P.4-28）を参照してください。

EAP の概要

EAP は、認証プロトコルを伝送するトランスポート プロトコルから認証プロトコルをデカップリングするための要件に対応する IETF RFC 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：サプリカントは応答パケットをオーセンティケータに送信し、シーケンス番号を使用して開始 EAP 要求と照合します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が負（NAK）の場合は除きます。
- EAP 成功：オーセンティケータは、サプリカントの認証が成功した場合、成功パケットを送信します。
- EAP 失敗：オーセンティケータは、認証が失敗した場合、サプリカントに失敗パケットを送信します。

EAP が IEEE 802.11X システムで使用中の場合、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。

EAP-GTC の設定

EAP-GTC は、単純なユーザ名とパスワードに基づく 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。この方式は、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。クライアントのみ認証するため、不正なサーバがユーザのクレデンシャルを取得するおそれがあります。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。

EAP-GTC によりキー関連情報は提供されないため、MACsec ではこの方式は使用できません。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。

- [Authenticate using a Password]：十分に保護された有線環境にのみ適しています。
- [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。

- [Validate Server Certificate]：サーバ証明書の検証を有効にします。
- [Enable Fast Reconnect]：TLS セッション再開を有効にします。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）　[Disable when using a Smart Card] オプションは、マシン接続認証では使用できません。

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-TTLS の設定（SNMP Configuration）

- 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
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。
  - [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有効にします。

    （注）　[Disable when using a Smart Card] は、マシン接続認証では使用できません。

- [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。Wi-Fi メディアタイプにのみ使用できます。

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。

- パスワードを使った認証
  - 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。
- 証明書を使った EAP-TLS
  - 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 の両方を有効にしない）。

PEAP の設定

- PEAP-EAP の設定
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。
  - [Enable Fast Reconnect]：外部 TLS セッション再開のみを有効にします。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。
  - [Disable when using a Smart Card]：スマート カードを使用して認証する場合に高速再接続を使用しません。スマート カードは、ユーザ接続にのみ適用されます。

  - [Authenticate using a Token and EAP GTC]：マシン認証には使用できません。
- クレデンシャル ソースに基づく内部方式
  - [Authenticate using a password]：EAP-MSCHAPv2 または EAP-GTC に対応
  - [Authenticate using a Certificate]：EAP-TLS に対応
  - [Authenticate using a Token and EAP-GTC]：マシン認証には使用できません。

（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-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。

AnyConnect 3.1 の時点では、マシン接続とユーザ接続の両方が設定されている場合、EAP チェーンがサポートされています。つまりネットワーク アクセス マネージャは、マシンとユーザが既知のエンティティで、企業により管理されていることを検証するということです。これは、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）に便利です。EAP チェーンの詳細については、RFC 3748 を参照してください。

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 の設定

- EAP-FAST の設定
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。これを有効にすると、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 [Certificate] ペインがさらに追加されます。
  - [Enable Fast Reconnect]：セッション再開を有効にします。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 [Enable Fast Reconnect] パラメータは、両方のメカニズムを有効または無効にします。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 パラメータの有効 / 無効によって処理されます。

（注）　[Disable when using a Smart Card] オプションは、ユーザ接続認証にのみ使用できます。

- [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。
  - [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。パスワードは 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、ハッシュ化された（または不可逆的に暗号化された）データベースに対する認証でこのプロトコルを使用できます。

    パスワード ベースの内部方式を使用している場合、認証されていない PAC プロビジョニングを許可する追加オプションが使用できます。
  - [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。
  - Authenticate Using a Token and EAP-GTC
- [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無効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 Files] ペインを選択して、[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、[Remove] をクリックします。

  [Password protected] : PAC がパスワード保護でエクスポートされた場合は、[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。

LEAP の設定

LEAP（Lightweight EAP）はワイヤレス ネットワークに対応しています。拡張認証プロトコル（EAP）フレームワークに基づき、WEP よりセキュアなプロトコルを作成するためシスコにより開発されました。

（注）　強力なパスワードおよび定期的に失効するパスワードを使用しない限り、LEAP はディクショナリ攻撃を受ける場合があります。認証方式がディクショナリ攻撃の被害を受けにくい EAP-FAST、PEAP または EAP-TLS を使用することをお勧めします。LEAP セキュリティの詳細については、http://www.cisco.com/en/US/tech/tk722/tk809/technologies_security_notice09186a00801aa80f.html を参照してください。

LEAP 設定はユーザ認証にのみ使用できます。

- [Extend user connection beyond log off]：ユーザ認証のみについて、ユーザがログオフした場合に接続を維持します。同じユーザが再度ネットワークにログインしても、接続はアクティブのままになります。

ネットワーク クレデンシャルの定義

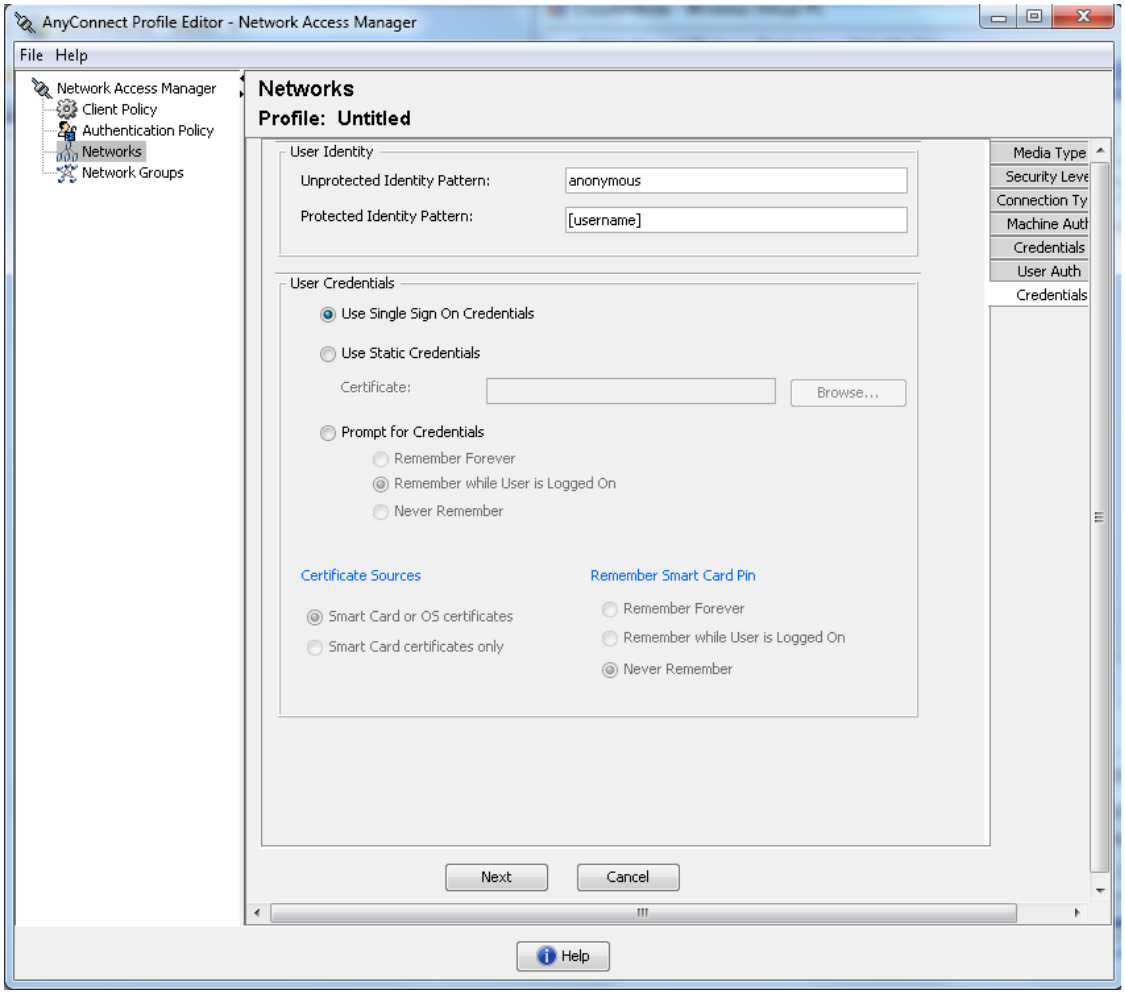
[Networks] > [Credentials] ペインで、ユーザ クレデンシャルまたはマシン クレデンシャルのいずれを使用するか指定し、信頼サーバ検証ルールを設定します。

- 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

[Credentials] ペインでは、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 4-9 を参照）の認証で使用するために指定できます。

図 4-9　EAP-TLS の [User Credentials] ペイン



ステップ 1　[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。

- [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。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザの PC のドメインを指定します。

ユーザ接続で、プレースホルダ [username] および [domain] を使用する場合、次の条件が当てはまります。

- 認証にクライアント証明書を使用する場合は、[username] と [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/DC=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@[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。
- [username]@[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有効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。

- [username]@[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。

- [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。

- [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。
- [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。
  - [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。
  - [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。
  - [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。

- [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。
- [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　[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。

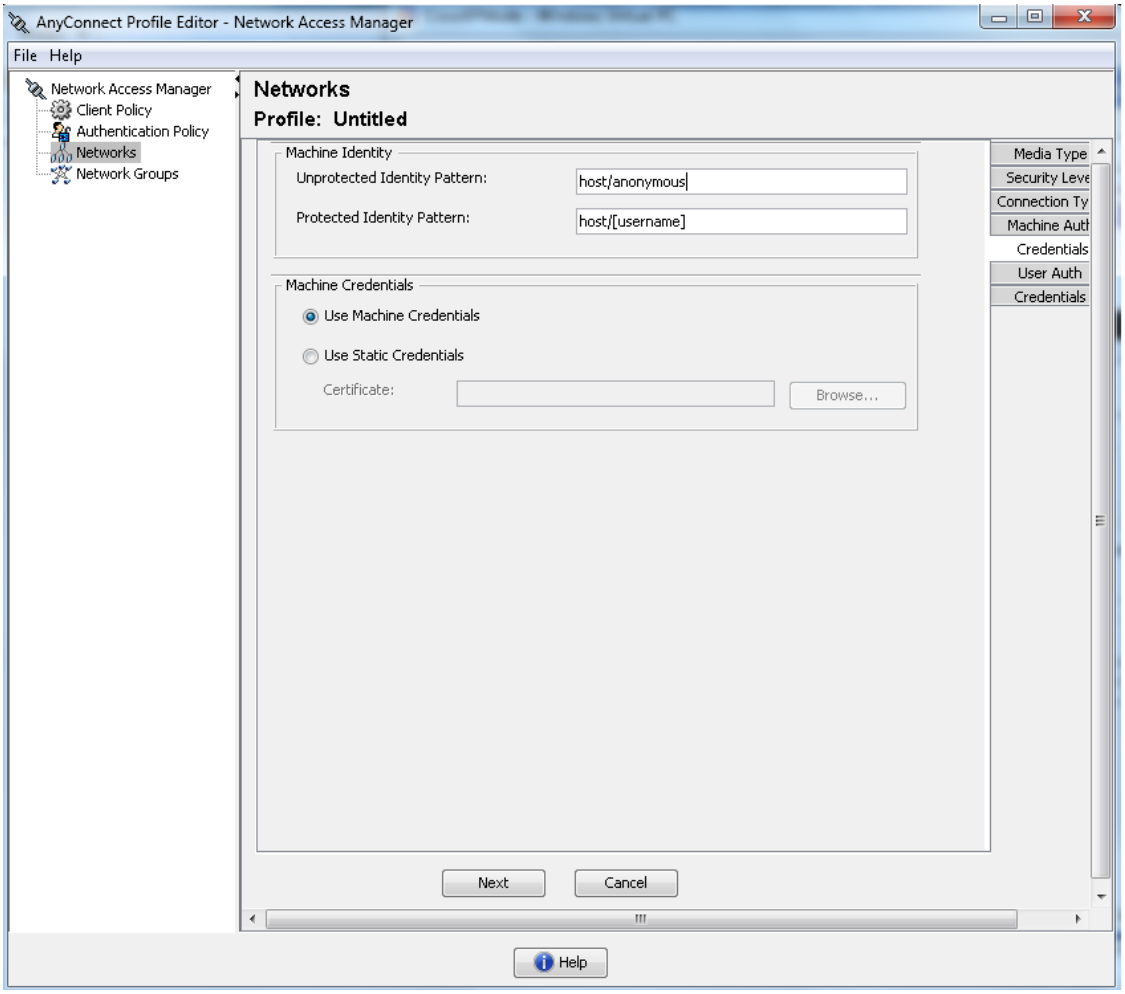
（注）　PIN は、証明書自体よりも長く保存されることは決してありません。

別名 Cryptographic Service Provider（CSP）および Key Storage Provider（KSP）というスマート カードのチップとドライバによっては、他より接続に時間がかかるスマート カードもあります。ネットワークで、スマート カードを使用して認証するのに十分な時間を与えるため、接続タイムアウトを増やさなければならない場合があります。

マシン クレデンシャルの設定

[Credentials] パネルでは、目的のマシン クレデンシャル（図 4-10 を参照）を指定できます。

図 4-10　マシン クレデンシャル



ステップ 1　[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。

- [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。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザの PC のドメインを指定します。

マシン接続の場合に、[username] および [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、[username] と [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、[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@[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有効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/[username]@[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。

- [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。
- [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

[Validate Server Identity] オプションが [EAP] 方式に設定されている場合、[Certificate] パネルが有効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 [Certificate Field] および [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　[Value] フィールドに、値を入力します。

ステップ 3　規則の下で [Add] をクリックします。

ステップ 4　[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。

- [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。
- Include Root Certificate Authority (CA) Certificates

（注）　[Include Root Certificate Authority (CA) Certificates] を選択した場合は、[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。

[Network Groups] ウィンドウ

[Network Groups] ウィンドウで、ネットワーク接続を特定のグループに割り当てます（図 4-11 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。

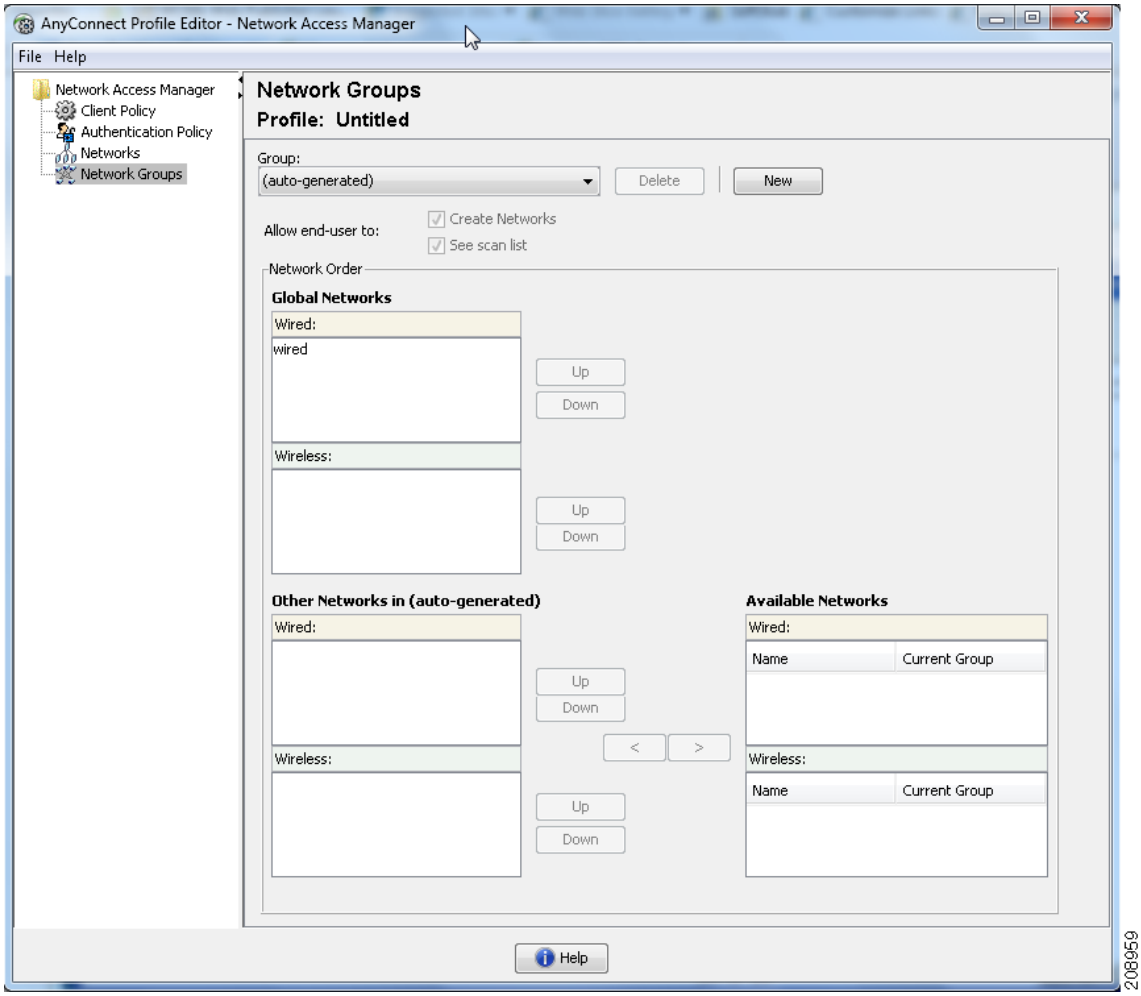
- 接続の確立試行時のユーザ エクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。この利点により、企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザ ネットワークから分離できます。

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 [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。あるグループがデフォルトで作成されている場合、すべてのネットワークがグローバルの場合にそのグループを削除できます。

図 4-11　[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、[Group] を選択します。

ステップ 2　[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　[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、[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　[Up] および [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、ファイル名などのエンドポイント属性を評価するポリシーを作成できます。ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

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 スキャンは、Dynamic Access Policies（DAPs）の割り当てに使用するアンチウイルス、アンチスパイウェア、ファイアウォールの各アプリケーションの製品名とバージョン情報を含む表をサポートします。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。

ポスチャ モジュールに同梱されたスタンドアロン ホスト スキャン パッケージとホスト スキャン パッケージが提供する機能は同じです。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、AnyConnect ポスチャ モジュール、CSD、スタンドアロン パッケージの 3 種類の方法で提供できるようになりました。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、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。

それでも、ホスト スキャンは CSD の代わりにはなりません。キャッシュ クリーンナップや 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。

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 スキャンをインストール、アンインストール、有効および無効にできます。Secure Desktop Manager ツールを ASDM で使用して、ポリシーを設定できます。

ポスチャ アセスメントおよび AnyConnect テレメトリ モジュールは、ホストにホスト スキャンがインストールされている必要があります。

この章の内容は、次のとおりです。

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、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. 評価は、リモート コンピュータについて次のチェックを行います。
   - オペレーティング システム
   - 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. クライアントが評価を行っていると同時に、ホスト スキャンはそのエンドポイントの評価を行っており、アンチウイルス、ファイアウォール、アンチスパイウェアのバージョン情報を収集しています。同時に、Dynamic Access Policies で指定したレジストリ キー、ファイル、プロセスをスキャンしています。
5. 評価結果に応じて、次のいずれかのイベントが発生します。

  - 評価が実行され、[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「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。
  - 評価により、ポリシー名がデバイスに割り当てられ、ポリシー名が ASA に報告されます。

6. ホスト スキャンは、評価後にリモート コンピュータが割り当てた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確認します。
7. 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は、保証があり、Advanced Endpoint Assessment ライセンスを保有している場合に修復されます。
8. ユーザがログインします。
9. 通常 ASA は、3. で収集した認証データ、さらに 4. で収集した設定済みのエンドポイント属性条件を使用します。この条件には、ポリシーおよびホスト スキャン結果などの値が入っており、ダイナミック アクセス ポリシーをセッションに適用できます。
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 モジュールで有効になる機能

評価

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、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。

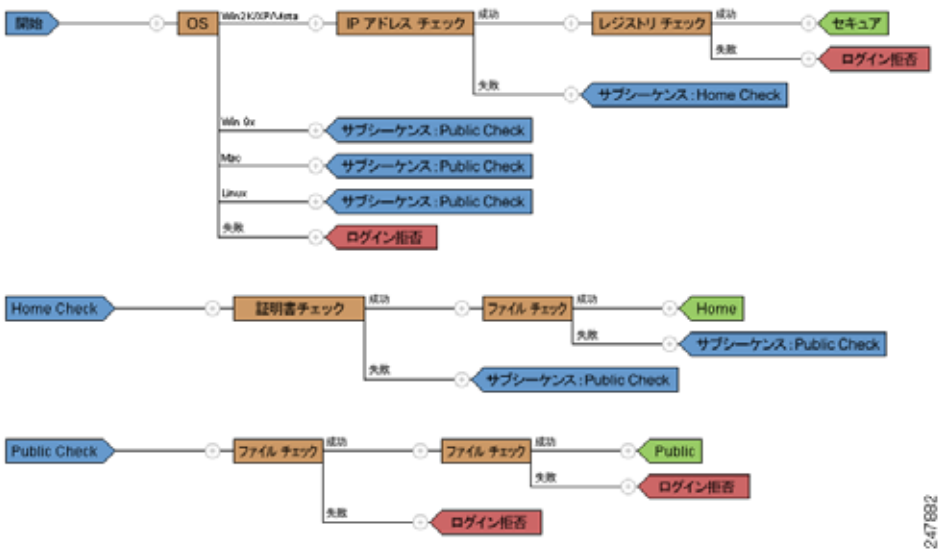
評価モジュールを設定するときに、ホスト スキャン管理者は「*シーケンス*」と呼ばれるノードのブランチを作成します。各シーケンスは [Start] ノードで始まり、続いてエンドポイント チェックが実行されます。チェックの結果により、別のエンドポイント チェックを実行するかどうか、またはエンド ノードでシーケンスを終了するかどうかを判定します。

エンドノードでは、「Login Denied」メッセージを表示するかどうか、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　　完全な評価の例



ポリシー

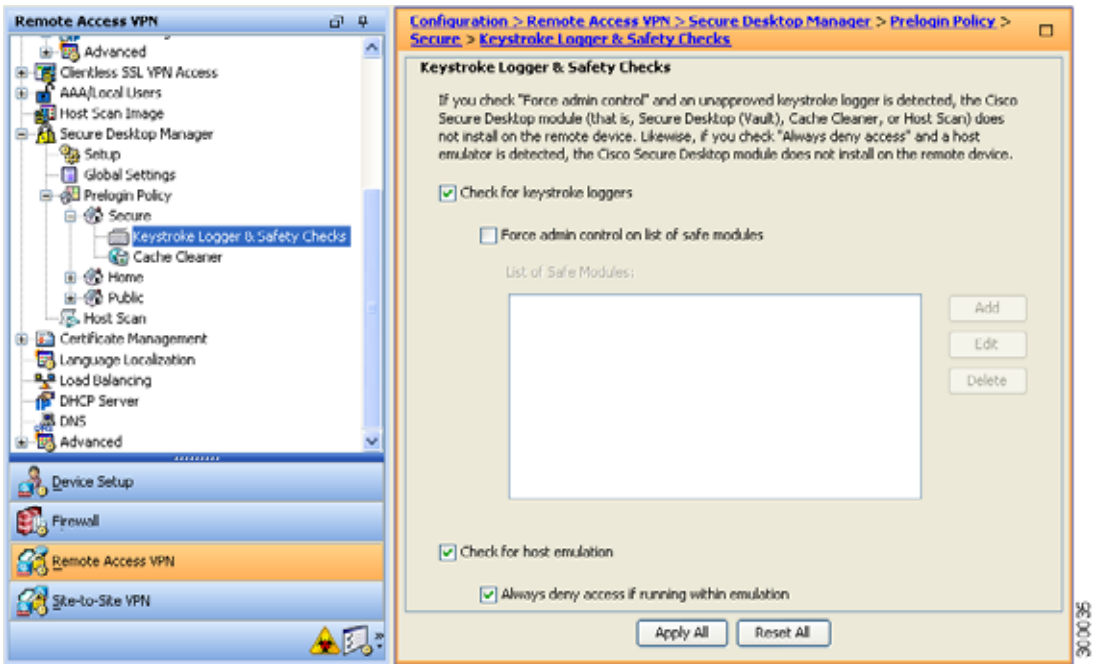
グラフィカル シーケンス エディタで設定された評価（図 5-1）のチェックの結果によって、評価が特定のポリシーに割り当てられるか、または拒否されるリモート アクセス接続となるかが判明します。

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。これらの設定により、ポリシーに割り当てられた条件に一致するリモート デバイス上にキーストローク 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 クリーナがインストールされるかが決まります。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。

ホスト スキャンおよびポリシーの設定の詳細については、『*Cisco Secure Desktop Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Release 3.6*』の次の章を参照してください。

- Confirming Host Scan
- Tutorial: Assigning Criteria to Policies
- Details: Assigning Criteria to Policies

図 5-2　　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をスキャンするよう、選択した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ポリシーで無効になっています。Secure Desktop Manager を使用して、キーストローク ロガー検出を有効または無効にできます。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。

有効にすると、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

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、この機能を有効または無効にできます。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ポリシーで無効になっています。この機能を有効にすると、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、次のオペレーティング システムで動作します。

- x86（32 ビット）の Windows Vista SP1 および SP2

  SP1 または SP2 が適用されていない Windows Vista を実行しているコンピュータには 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 には対応していません。

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、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、キャッシュ クリーナが導入され、エンドポイントがクライアントレス SSL VPN 接続を確立しようとする、または Web 起動を使用して AnyConnect を起動しようとする場合の一連のイベントです。

ステップ 1　ユーザがエンドポイントの URL をブラウザに入力すると、エンドポイントは ASA に接続されます。

ステップ 2　ホスト スキャンにより評価を行います。

ステップ 3　エンドポイントが評価を通過することが前提で、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、証明書を使用して認証します。

ステップ 4　[Clean the whole cache in addition to the current session cache (IE only)] を有効にしないで Internet Explorer を実行しているユーザ、または Safari や Firefox 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 セッションからログアウトした場合：

- [Clean the whole cache in addition to the current session cache (IE only)] を有効にして Internet Explorer を実行しているユーザについては、キャッシュ クリーナによってブラウザのキャッシュ全体が削除されます。
- [Clean the whole cache in addition to the current session cache (IE only)] を有効にしないで Internet Explorer を実行しているユーザ、または Safari や Firefox 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。

  機密情報がコンピュータ上に復元されないようにするため、セッション終了後に手動でブラウザのキャッシュを消去し、ブラウザを閉じることをお勧めします。

（注）　キャッシュ クリーナを、[Clean the whole cache in addition to the current session cache (IE only)] オプションを有効にして設定することをお勧めします。

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 で有効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。情報は、評価にも使用できます。詳細については、「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

ホスト スキャン拡張機能であるエンドポイント アセスメントでは、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コレクションについて、リモート コンピュータを検査します。この機能を使用して、ASA によって特定の DAP がセッションに割り当てられる前に、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 機能は、アンチウイルス ソフトウェアの次のコンポーネントを修復できます。

- [Force File System Protection]：アンチウイルス ソフトウェアが無効の場合に、Advanced Endpoint Assessment はこのコンポーネントを有効にできます。
- [Force Virus Definitions Update]：アンチウイルス定義が Advanced Endpoint Assessment 設定で定義された日数内に更新されていない場合、Advanced Endpoint Assessment はウイルス定義のアップデートを開始できます。

アンチスパイウェア：アンチスパイウェア定義が Advanced Endpoint Assessment 設定で定義された日数内に更新されていない場合、Advanced Endpoint Assessment はアンチスパイウェア定義のアップデートを開始できます。

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、有効または無効にできます。
- アプリケーションを実行、または実行できないようにできます。

- ポートをブロックまたは開くことができます。

（注）　すべてのパーソナル ファイアウォールがこの機能をサポートし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無効にする場合、VPN 接続が正常に確立された後、Advanced Endpoint Assessment 機能は約 60 秒以内にそのアプリケーションを再度有効にしようとします。

Windows モバイル デバイスの Lua 表現

Windows モバイル デバイスについて、管理者は Dynamic Access Policies（DAPs）で Lua 表現を作成し、モバイル デバイス固有の属性についてポスチャ チェックを実施きるようになります。これらの Lua 表現の例については、『*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。

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、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 パッケージで提供されます。

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、および Safari などのブラウザは、最高のダウンロード エクスペリエンスを実現します。

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、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 スキャンの機能を有効にするには、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。

（注）　ASDM を使用して ASA で DAP を設定する方法の詳細については、ご使用の ASDM バージョンの『Adaptive Security Device Manager (ASDM) Configuration Guide』で、「Configuring Dynamic Access Policies」の章をご覧ください。

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、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 アプリケーションで必要なその他のモジュールがいくつか含まれます。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、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

次の 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　AnyConnect Secure Mobility Client、バージョン 3.0.x でホスト スキャンを展開する場合、AnyConnect Secure Mobility Client では、ホスト スキャンのバージョン番号は同じか、それ以降にする必要があります。

Cisco Secure Desktop（CSD）バージョン 3.5 以前を ASA で有効にしていて、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、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 で有効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 3.0.x は旧バージョンのホスト スキャンまたは CSD と互換性はありませんが、旧バージョンの AnyConnect は新しいバージョンのホスト スキャン パッケージと互換性があります。たとえば、CSD 3.6 以前および AnyConnect 2.5.6 以前を使用していてホスト スキャン イメージを 3.0.8 以降にアップグレードする場合、評価は成功します。

システム要件

ポスチャ モジュールは、次のいずれか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、10.7 および 10.8（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。

- Windows Mobile

ライセンシング

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本ホスト スキャン、エンドポイント アセスメント、Advanced Endpoint Assessment などのホスト スキャンに同梱されたすべての機能に AnyConnect Premium ライセンスが必要です。
- 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、Endpoint Assessment 機能のすべてが含まれており、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　[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択します。

ステップ 2　[New Activation Key] フィールドにキーを入力します。

ステップ 3　[Update Activation Key] をクリックします。

ステップ 4　[File] > [Save Running Configuration to Flash] を選択します。

[Advanced Endpoint Assessment] エントリが表示され、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] ペインの [Host Scan Extensions] 領域内の [Configure] ボタンがアクティブになります。[Host Scan] ペインは、CSD が有効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、AnyConnect Secure Mobility 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。

- **csd_version-k9.pkg** は、Cisco Secure Desktop 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、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、ホスト エミュレーション検出が含まれています。
anyconnect-win-*version*-k9.pkg	このパッケージには、hostscan-*version*-k9.pkg ファイルなど、すべての AnyConnect Secure Mobility Client 機能が含まれています。
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、またホスト 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、およびホスト エミュレーション検出などのすべての Cisco Secure Desktop 機能が含まれています。

複数のホスト スキャン イメージが ASA にロードされている場合に有効になるホスト 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。その場合、ASA は最初にホスト スキャン イメージとして指定したイメージを有効にし、イメージを指定していない場合は、Cisco Secure Desktop からホスト スキャン機能を有効にします。「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.5-15）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 イメージを有効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 を有効にしている場合、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 を有効にしている場合、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、それを有効にはせず、また ASA に CSD イメージをインストールして、CSD/hostscan を有効にしている場合、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。
- AnyConnect Secure Mobility Client パッケージを ASA にインストールし、それをホスト スキャン イメージと指定した場合、ホスト スキャン イメージはそのパッケージから配布されます。

- 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、CSD が有効であることを前提に、インストール済みのホスト 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 種類の展開シナリオがあります。

事前展開：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。事前展開ポスチャ モジュール パッケージには、ポスチャ属性の収集に使用できるあらゆるコンポーネント、ライブラリ、サポート表、また「AnyConnect ポスチャ モジュールで有効になる機能」（P.5-3）に記載の機能を提供するアプリケーションが入っています。ASA にインストールされた同じバージョンの AnyConnect クライアントとポスチャ モジュール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 ファイルは ASA からプッシュダウンされません。

Web 展開：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 クライアントとポスチャ モジュールをエンドポイントにプッシュダウンします。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接続すると、必須のポスチャ モジュール ファイルにより、エンドポイント アセスメントの実施に必要なその他のライブラリまたはファイルが判断され、それらのファイルが ASA から取得されます。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。エンドポイント属性がダイナミック アクセス ポリシー（DAP）のルールを十分に満たすことを前提に、ASA はエンドポイントを接続させることができます。DAP を満たしたら、ASA は残りのポスチャ モジュールをエンドポイントにプッシュするかどうか設定できます。

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、制限付き Web 展開を実施できます。この場合、エンドポイントにはポスチャ ファイルが 1 つだけダウンロードされ、エンドポイント アセスメントの実施に必要なホスト スキャン ライブラリのみ要求されます。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 クライアントが初めて ASA に接続する前に、エンドポイントにモジュールを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 に、ポスチャ モジュール事前展開キットを一覧表示します。

表 5-2　ポスチャ モジュール事前展開キット

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 上でのホスト スキャンのインストールと有効化

次のタスクでは、ASA 上でのホスト スキャンのインストールと有効化について説明します。

- ホスト スキャン エンジン最新版アップデートのダウンロード
- 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 でホスト スキャンを有効または無効にする
- 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

ホスト スキャン エンジン最新版アップデートのダウンロード

Cisco Host Scan Engine の最新版アップデートをダウンロードするには、Cisco.com にユーザ登録する必要があります。

ステップ 1　Cisco VPN クライアント ツールのソフトウェア ダウンロード エリアに移動するには、このリンクをクリックします。

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 [Latest Releases] を展開します。

ステップ 3　[Engine Updates] をクリックします。

ステップ 4　右のカラムで、最新版の **hostscan_3.0.xxxx-k9.pkg** を見つけ、[Download Now] をクリックします。

ステップ 5　cisco.com のクレデンシャルを入力し、[Login] をクリックします。

ステップ 6　[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、[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、[download] リンクをクリックしてダウンロードを行います。

ホスト スキャンのインストールまたはアップグレード

次の手順を使用して、ASA 上で新しいホスト スキャン イメージをアップロードまたはアップグレードし、有効にすることができます。イメージを使用して AnyConnect のホスト スキャン機能を有効にするか、Cisco Secure Desktop（CSD）の既存の展開についてホスト スキャン サポート表をアップグレードします。

フィールドに、スタンドアロンのホスト スキャン パッケージ、または AnyConnect セキュア モビリティ クライアント パッケージのバージョン 3.0 以降を指定することができます。

以前に CSD イメージを ASA にアップロードしていた場合は、指定するホスト スキャン イメージによって、CSD パッケージに同梱されていた既存のホスト スキャン ファイルがアップグレードまたはダウングレードされます。

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、ASDM の Secure Desktop Manager ツールにアクセスするには、Adaptive Security Device Manager（ASDM）を終了して再起動する必要があります。

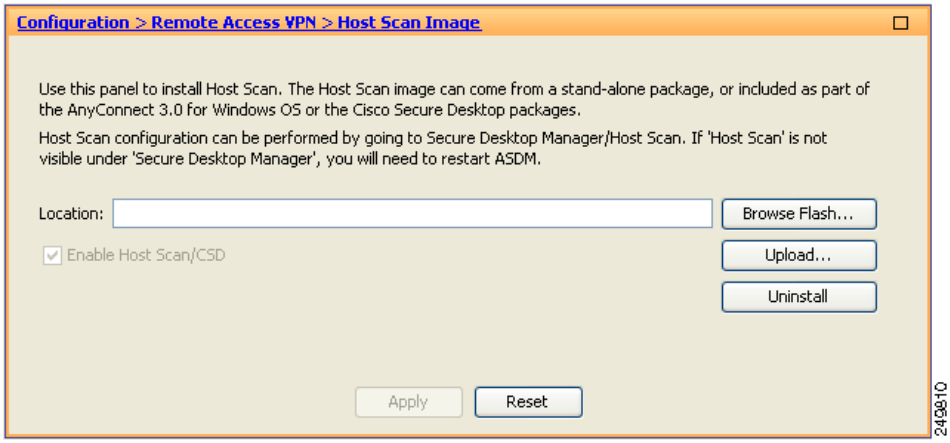
（注） ホスト スキャンには、AnyConnect Secure Mobility Client Premium ライセンスが必要です。

ステップ 1　「ホスト スキャン エンジン最新版アップデートのダウンロード」（P.5-15）を使用して、最新版のホスト 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 のアカウントでログインする必要があります。

ステップ 2　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネル（図 5-3）が開きます。

図 5-3　[Host Scan Image] パネル



ステップ 3　[Upload] をクリックして、ご使用のコンピュータから ASA 上のドライブにホスト スキャン パッケージのコピーを転送する準備をします。

ステップ 4　[Upload Image] ダイアログボックスで、[Browse Local Files] をクリックしてローカル 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　ステップ 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、[Select] をクリックします。[Local File Path] フィールドおよび [Flash File System Path] フィールドで選択したファイルのパスには、ホスト スキャン パッケージのアップロード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は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。

ステップ 6　[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。[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　[Use Uploaded Image] ダイアログで [OK] をクリックして、現行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　[Enable Host Scan/CSD] がオンになっていない場合はオンにします。

ステップ 10　[Apply] をクリックします。

（注）　ASA 上で AnyConnect Essentials が有効になっている場合、ホスト スキャンと CSD は AnyConnect Essentials と組み合わせて動作しないというメッセージが表示されます。AnyConnect Essentials を**無効**にするか、**保持**するかを選択します。

ステップ 11　[Save] をクリックします。

ASA でホスト スキャンを有効または無効にする

ASDM を使用して初めてホスト スキャン イメージをインストールまたはアップグレードする場合は、手順の一部としてそのイメージを有効にします。「ASA 上でのホスト スキャンのインストールと有効化」（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 イメージを有効または無効にするには、次の手順を実行します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネル（図 5-3）が開きます。

ステップ 2　[Enable Host Scan/CSD] をオンにしてホスト スキャンを有効にするか、または [Enable Host Scan/CSD] をオフにしてホスト スキャンを無効にします。

ステップ 3　[Apply] をクリックします。

ステップ 4　[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）を有効にすると、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 を無効にしても、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 を有効または無効にします。

ステップ 1　[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 5-3）。

（注）　[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。[Enable Secure Desktop] チェックボックスは、CSD が有効になっているかどうかを示します。

ステップ 2　[Enable Secure Desktop] をオンにして CSD を有効にするか、[Enable Secure Desktop] をオフにして CSD を無効にします。

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　[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

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 に同梱されたパッケージ、または Cisco Secure Desktop に同梱されたパッケージのいずれであっても、ASA は、有効なホスト スキャン パッケージを自動的にエンドポイントに配布します。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 で有効にされたホスト スキャン イメージの判別

ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。

[Host Scan Image Location] フィールドにホスト スキャン イメージが指定されており、[Enable HostScan/CSD] ボックスがオンになっている場合は、そのイメージのバージョンが ASA で使用されるホスト スキャン バージョンとなります。

[Host Scan Image] フィールドが空で、[Enable HostScan/CSD] ボックスがオンになっている場合は、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] を選択します。[Secure Desktop Image Location] フィールドの CSD のバージョンが、ASA で使用されるホスト スキャン バージョンとなります。

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 が有効の場合でも ASA によるホスト スキャン パッケージの展開が回避されます。ホスト スキャンをアンインストールしても、フラッシュ ドライブのホスト スキャン パッケージは削除されません。

セキュリティ アプライアンスのホスト スキャンをアンインストールするには、次の手順を使用します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。

ステップ 2　[Host Scan Image] ペインで [Uninstall] をクリックします。ASDM では、[Location] テキスト ボックスのテキストが削除されます。

ステップ 3　[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 設定ファイルである 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。

セキュリティ アプライアンスの CSD をアンインストールするには、次の手順を使用します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 5-3）。

ステップ 2　[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　[Yes] をクリックします。

ASDM によって、[Location] テキスト ボックスからテキストが削除され、[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　[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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] の順に選択します。

ステップ 2　[Group Policies] パネルで [Add] をクリックして新規グループ ポリシーを作成するか、またはホスト 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、[Edit] をクリックします。

ステップ 3　[Edit Internal Group Policy] パネルで、左側の [Advanced] ナビゲーション ツリーを展開し、[AnyConnect Client] を選択します。

ステップ 4　[Optional Client Modules to Download Inherit] チェックボックスをオフにします。

ステップ 5　[Optional Client Modules to Download] ドロップダウン メニューで [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。

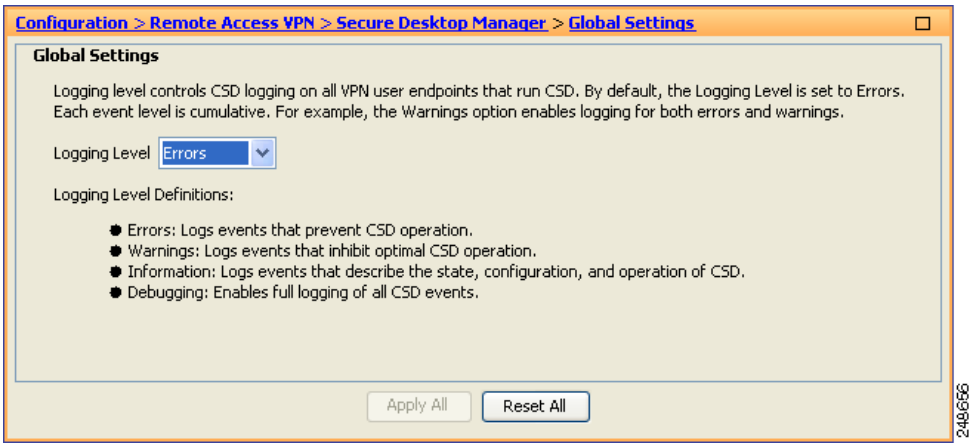
すべてのポスチャ モジュール コンポーネントのロギング レベルの設定

デフォルトでは、ポスチャ モジュール コンポーネントは、「エラー」の重大度レベル イベントを記録します。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、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Global Settings] を選択します。[Global Settings] パネルが開きます。



ステップ 2　ペイン内の [Logging Level Definitions] を参考に、[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、[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 スキャンが無効になっている場合、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、オペレーティング システム、特権レベル、権限レベル、起動メカニズム（Web 起動または AnyConnect）に基づいて、次に示す最大 3 つのログを出力します。

- 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：スキャン実行ファイル（cscan.exe）により作成される、ポスチャおよびホスト スキャンのメイン ログです。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）は、必要な場合に、これらのログ ファイルを使用して問題をデバッグします。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、必要なすべての AnyConnect 設定とログ ファイルを収集し、圧縮ファイルに保存して TAC に送信します。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.13-4）を参照してください。

BIOS シリアル番号の DAP での使用

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）を使用して、その BIOS シリアル番号に基づいて ASA への VPN 接続を可能または回避できます。

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。

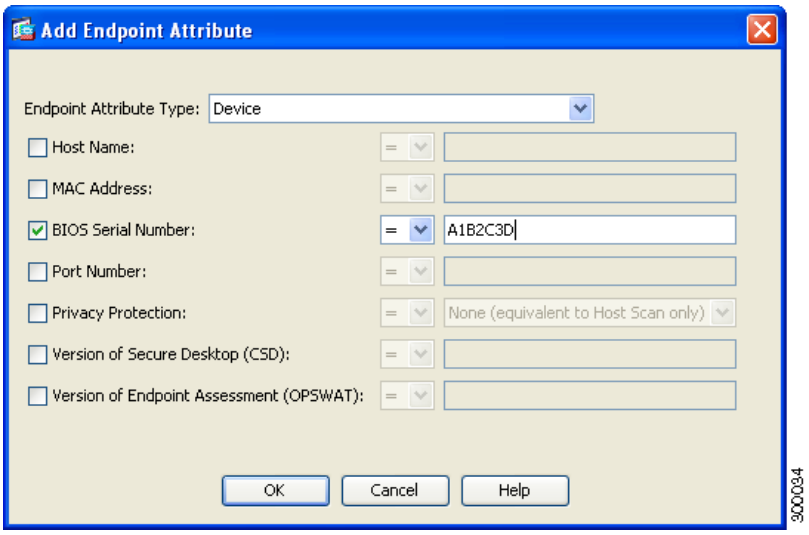
ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] を選択するか、[Clientless SSL VPN Access] > [Dynamic Access Policies] を選択します。

ステップ 3　[Configure Dynamic Access Policies] パネルで、[Add] または [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 [Add] をクリックします。

ステップ 5　[Endpoint Attribute Type] フィールドで [Device] を選択します。

ステップ 6　[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 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、[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、[Edit Dynamic Access Policy] への変更を保存します。

ステップ 9　[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　[Save] をクリックします。

BIOS シリアル番号の取得方法

次のリソースでは、さまざまなエンドポイントの BIOS シリアル番号の取得方法について説明しています。

- 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
```

CHAPTER 6

Web セキュリティの設定

AnyConnect Web セキュリティ モジュールとは、Cisco Cloud Web Security が HTTP トラフィックを評価する Cisco Cloud Web Security スキャニング プロキシに、そのトラフィックをルーティングするエンドポイント コンポーネントのことです。

同時に各要素を分析できるように、Cisco Cloud Web Security は Web ページ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。Cisco Cloud Web Security は、Cisco 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、悪意が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。Cisco Cloud Web Security は、社内ネットワークに接続しているか否かにかかわらずユーザを保護します。

多数の Cisco Cloud Web Security 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 Cisco Cloud Web Security 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識別するように Secure Trusted Network Detection 機能を設定できます。この機能が有効になっている場合、社内 LAN からのネットワーク トラフィックはすべて、送信元の Cisco Cloud Web Security 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、Cisco Cloud Web Security 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。

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。

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。Cisco 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。

- Web スキャニング サービス プリファレンスの設定
- 認証の設定および Cisco Cloud Web Security 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 エディタを使用した Web セキュリティ クライアント プロファイルの作成
- Web セキュリティのスプリット除外ポリシーの設定
- Web セキュリティ クライアント プロファイルの Cisco 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

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）
- 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）
- Mac OS X v10.8 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

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

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、Cisco Cloud Web Security の利点を得ることができます。

ただし、AnyConnect を展開しているローミング ユーザ用に Cisco Cloud Web Security ライセンスおよび Cisco Cloud Web Security Secure Mobility 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。

Cisco Cloud Web Security ライセンス

ローミング ユーザを Cisco Cloud Web Security で保護するには、Cisco Cloud Web Security Web Filtering または Cisco Cloud Web Security Malware Scanning のライセンス（あるいはその両方）に加え、Secure Mobility for Cisco Cloud Web Security 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

AnyConnect VPN モジュールを有効にせず、ASA のない状態でであっても 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展開し、Cisco Cloud Web Security と連動させることができます。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 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、Cisco 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 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、Cisco Cloud Web Security と連動させるために Windows 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。

（注）　Windows のロックダウンの有効化を含む一般的なインストール手順については、第 2 章を参照してください。

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て Web セキュリティ プロファイルを作成し、ISO ファイルの抽出されたコンテンツに Web セキュリティ プロファイルのファイルを追加することで、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。

Cisco Cloud Web Security と連動させるために Windows 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、次の手順に従います。

ステップ 1　Cisco 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 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.2-38）を参照してください。

（注）　Web セキュリティ プロファイル エディタ コンポーネントは、デフォルトではインストールされません。カスタム インストールでそれを選択して含めるか、完全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　安全な場所に、**WebSecurity_ServiceProfile.xml** という名前でプロファイルを保存します。

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 Install Selector で次の操作を行います。

- [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 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、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。

- （任意）[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　[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.2-38）を参照してください。

（注）　Web セキュリティ プロファイル エディタ コンポーネントは、デフォルトではインストールされません。カスタム インストールでそれを選択して含めるか、完全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　安全な場所に、**WebSecurity_ServiceProfile.xml** という名前でプロファイルを保存します。

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.x.xxxxx/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.x.xxxxx/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.x.xxxxx** 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.x.xxxxx/profiles/vpn** ディレクトリに保存します。

（注）　AnyConnect 3.x.xxxxx 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。ステップ 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 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 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 2-13（P.2-36）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.6-28）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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択し、[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。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [Web Security Profile Editor] を選択します。

ステップ 2　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、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 3　[Profile Usage] フィールドをクリックして、[Web Security] を選択します。

ステップ 4　デフォルトのプロファイルの場所を使用するか、[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 5　（任意）[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 6　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 Cisco Cloud Web Security 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）

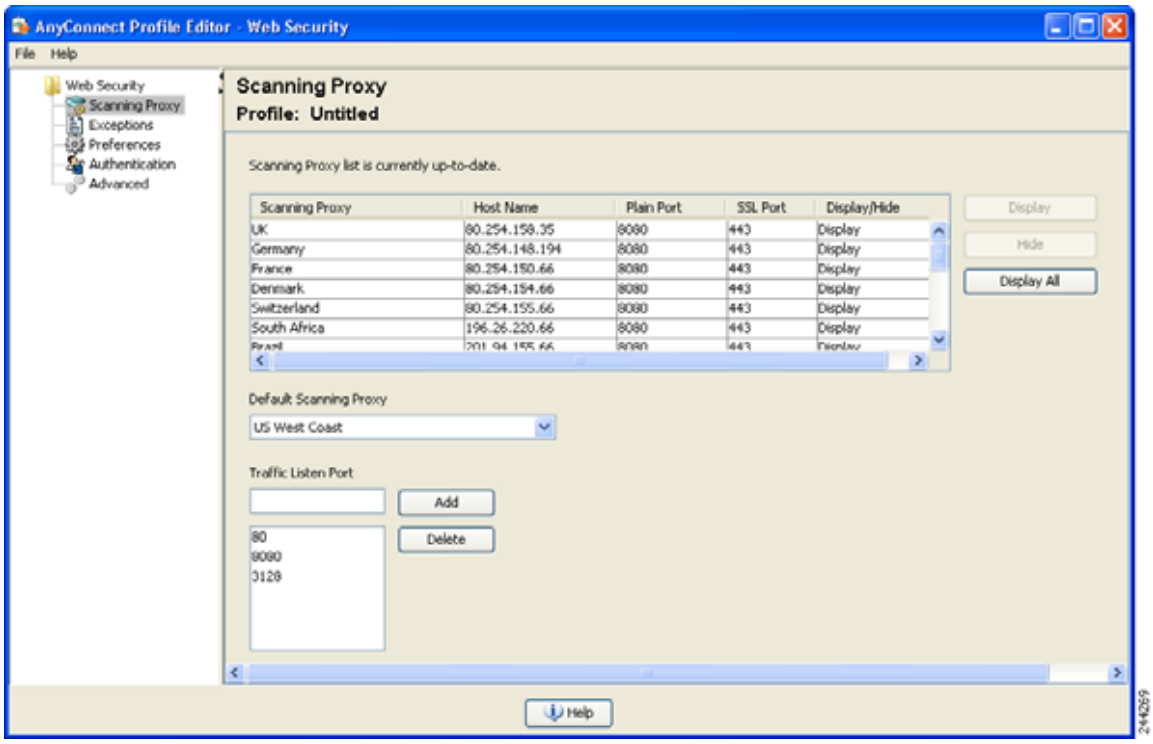
- 「Secure Trusted Network Detection の設定」（P.6-17）
- 「認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信」（P.6-18）

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.6-23）を参照してください。

クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシの設定

Cisco Cloud Web Security 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、Cisco Cloud Web Security が Web コンテンツを分析する Cisco Cloud Web セキュリティ 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 [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 Cisco Cloud Web Security スキャニング プロキシ定義します。

図 6-2　Web セキュリティ クライアント プロファイルの [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 Cisco Cloud Web Security 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.6-10）
- 「デフォルトのスキャニング プロキシの選択」（P.6-11）

- 「HTTP（S）トラフィック リスニング ポートの指定」（P.6-12）

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。Cisco Cloud Web Security 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 Cisco Cloud Web Security 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、Cisco Cloud Web Security スキャニング プロキシの既存のリストを、http://www.scansafe.cisco.com/ の 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、「Scanning Proxy list is out of date」というメッセージと、[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、Cisco Cloud Web Security スキャニング プロキシの最新のリストで更新するには、[Update List] ボタンをクリックします。

[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 Cisco Cloud Web Security 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 Cisco Cloud Web Security 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 Cisco Cloud Web Security 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.6-10）を参照してください。
- デフォルトの Cisco Cloud Web Security 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 Cisco Cloud Web Security 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.6-11）を参照してください。
- AnyConnect Web セキュリティ 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.6-12）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 Cisco Cloud Web Security 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。

- Cisco Cloud Web Security 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 Security] パネルの [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 Cisco Cloud Web Security 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 Cisco Cloud Web Security 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 Cisco Cloud Web Security 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、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 Cisco Cloud Web Security 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。

Cisco Cloud Web Security 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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　Cisco Cloud Web Security 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、[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、[Display] をクリックします。すべての Cisco Cloud Web Security 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 Cisco Cloud Web Security 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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[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 [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 [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、[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 [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 [Advanced Settings] タブ、および [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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[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。

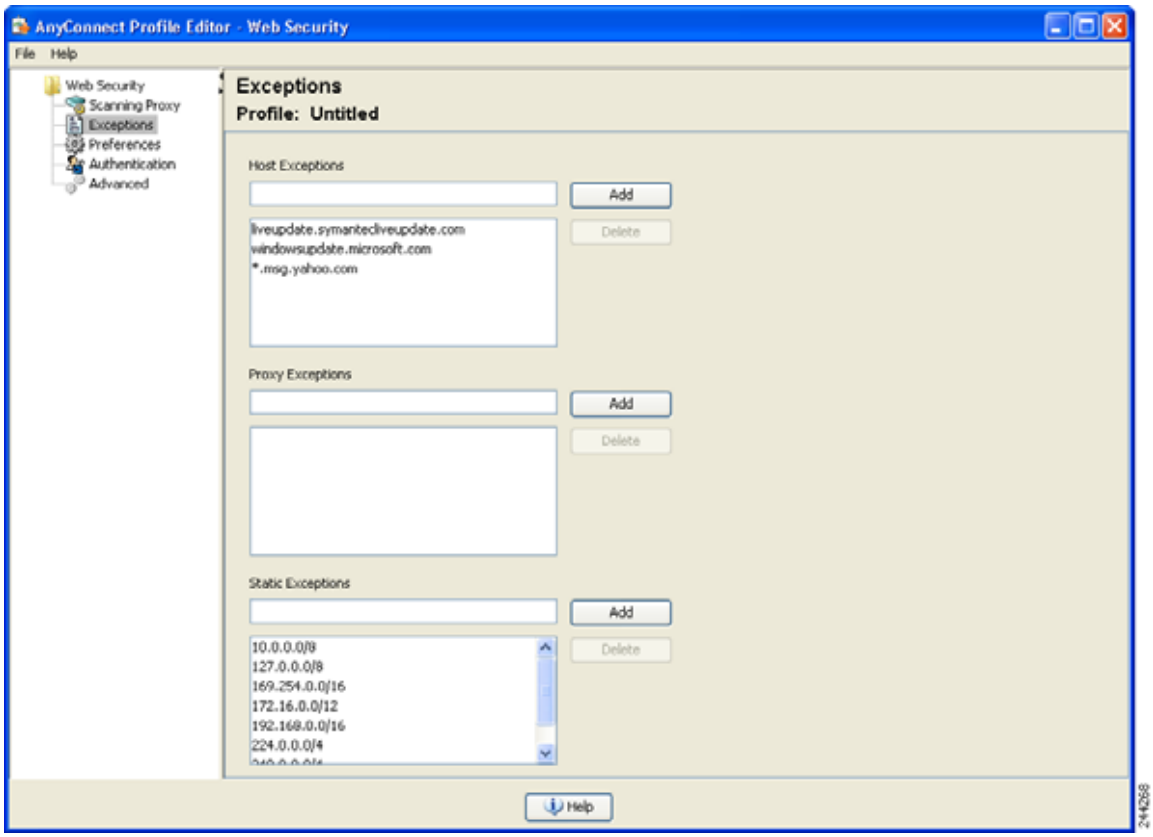
Web スキャニング サービスからのエンドポイント トラフィックの除外

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 Cisco Cloud Web Security 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 [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 [Exceptions] パネル



ホスト例外

[Host Exceptions] リストで、Cisco Cloud Web Security 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。

（注）　HTTPS のホスト例外は IP 形式である必要があります。HTTPS 通信ではホスト名が暗号化されているので、ホスト名は機能しません。

[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。

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

[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。[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せん。

IP アドレスを指定すると、Cisco Cloud Web Security が、これらのサーバ宛の Web データを代行受信して SSL を使用してデータをトンネリングすることがないようにします。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。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 Cisco Cloud Web Security 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、Cisco Cloud Web Security 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 Cisco Cloud Web Security 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。

RFC 1918 に記載されたプライベート IP アドレスは、デフォルトで静的な例外リストに含まれています。

（注）　静的な例外リストに記載されたいずれかの範囲に含まれる IP アドレスを持つプロキシ サーバがある場合は、ホストの例外リストにその例外を移動する必要があります。たとえば、静的な例外リストに 10.0.0.0/8 が記載されているとします。10.1.2.3 に設定されているプロキシがある場合、ホストの例外リストに 10.0.0.0/8 を移動する必要があります。そうしないと、このプロキシに送信されたトラフィックは Cloud Web Security をバイパスします。

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）
- 「Secure Trusted Network Detection の設定」（P.6-17）

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 Cisco Cloud Web Security 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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[Preferences] をクリックします。

ステップ 4　[User Controllable] をオンにします。（これはデフォルト設定です）。[User Controllable] は、ユーザが AnyConnect インターフェイスで [Automatic Tower Selection] および [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　[Enable Cloud-Hosted Configuration] を選択し、Cisco ScanCenter 経由でのプロファイルの更新をイネーブルにします。詳細については、『*ScanCenter Administrator Guide, Release 5.2*』を参照してください。

ステップ 6　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、[Automatic Scanning Proxy Selection] をオンにします。これを行うと、[Order Scanning Proxies by Response Time] は自動的にオンになります。

- [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。
- [Automatic Scanning Proxy Selection] を選択しなくても、まだ [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。
- [Automatic Scanning Proxy Selection] を選択しない場合、ユーザは AnyConnect ユーザ インターフェイスからこの機能を自由にイネーブルできますが、いったんイネーブルにすると、再度オフにすることはできません。

（注）　[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 7　[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。

- [Test Interval]：各パフォーマンス テストの実行間の時間（分単位）。デフォルトは 2 分間です。[Enable Test Interval] チェックボックスをオフにすることで、テスト間隔をオフにして、テストが実行されないようにできます。
- [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）　[Ordering 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。

- 「Secure Trusted Network Detection」がイネーブルで、マシンが社内 LAN 上にあることが検出された。
- 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 [Test Inactivity Timeout] しきい値に達した。

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。

Secure Trusted Network Detection の設定

Secure Trusted Network Detection 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。Secure Trusted Network Detection 機能がイネーブルになっている場合、社内 LAN からのネットワーク トラフィックはすべて、送信元の Cisco Cloud Web Security 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、Cisco Cloud Web Security 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。

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [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.6-14）を参照してください。

（注）　社内ネットワークの外部から操作する場合は、Secure Trusted Network Detection が DNS 要求を行い、プロビジョニングした HTTPS サーバに接続を試みます。シスコでは、社内ネットワークの外部で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになってしまわないように、エイリアス設定の使用をお勧めします。

Web セキュリティの Secure Trusted Network Detection 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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[Web Security] ツリー ペインで、[Preferences] をクリックします。

ステップ 4　[Enable Trusted Network Detection] を選択します。

ステップ 5　[https] ボックスの中で、追加する信頼サーバごとに RL を追加し、[Add] をクリックします。URL にはポート アドレスを含めることができます。プロファイル エディタは、信頼サーバへの接続を試みます。何らかの理由で接続できないけれども、サーバの証明書の SHA-256 ハッシュをご存じの場合は、[Certificate hash] ボックスに入力し、[Set] をクリックできます。

（注）　プロキシの背後にある信頼サーバはサポートされません。

ステップ 6　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。

認証の設定および Cisco Cloud Web Security 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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[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 6-4 を参照してください。

ステップ 4　[Proxy Authentication License Key] フィールドに、Cisco 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。Cisco 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。次のような特殊文字は、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ります。

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

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 [Authentication] パネルで設定します。」（P.6-28）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 Cisco Cloud Web Security 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。

- [Enable Enterprise Domains] をクリックします。リストの中で、[All Domains] をクリックします。[All Domains] オプションが選択され、マシンがドメイン上にある場合、ユーザがどのドメインに属していても、ドメインが一致し、ユーザ名およびグループ メンバーシップ情報が Cisco Cloud Web Security 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。
- または、[Specify Individual Domains] をクリックします。

  NetBIOS 形式で各ドメイン名を入力し、[Add] をクリックします。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

  [Enterprise Domain name] フィールドにドメイン名を指定すると、Cisco Cloud Web Security 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。
- [Use] リストで、[Group Include List] または [Group Exclude List] をクリックし、Cisco Cloud Web Security 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します。値には、照合する文字列の任意の部分文字列を指定できます。

  [Group Include List]。[Group Include List] の選択後に、HTTP 要求で Cisco Cloud Web Security スキャニング プロキシ サーバに送信する Cisco Cloud Web Security または Active Directory グループ名を [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。

  [Group Exclude List]。[Group Exclude List] の選択後に、HTTP 要求で Cisco Cloud Web Security スキャニング プロキシ サーバに送信しない Cisco Cloud Web Security または Active Directory グループ名を [Group Exclude List] に追加します。ユーザが、[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 Cisco Cloud Web Security 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。

  ここで、ステップ 8 に進みます。

ステップ 7　スキャニング プロキシ サーバのカスタム名を送信するには、[Custom matching and reporting for machines not joined to domains] をクリックします。

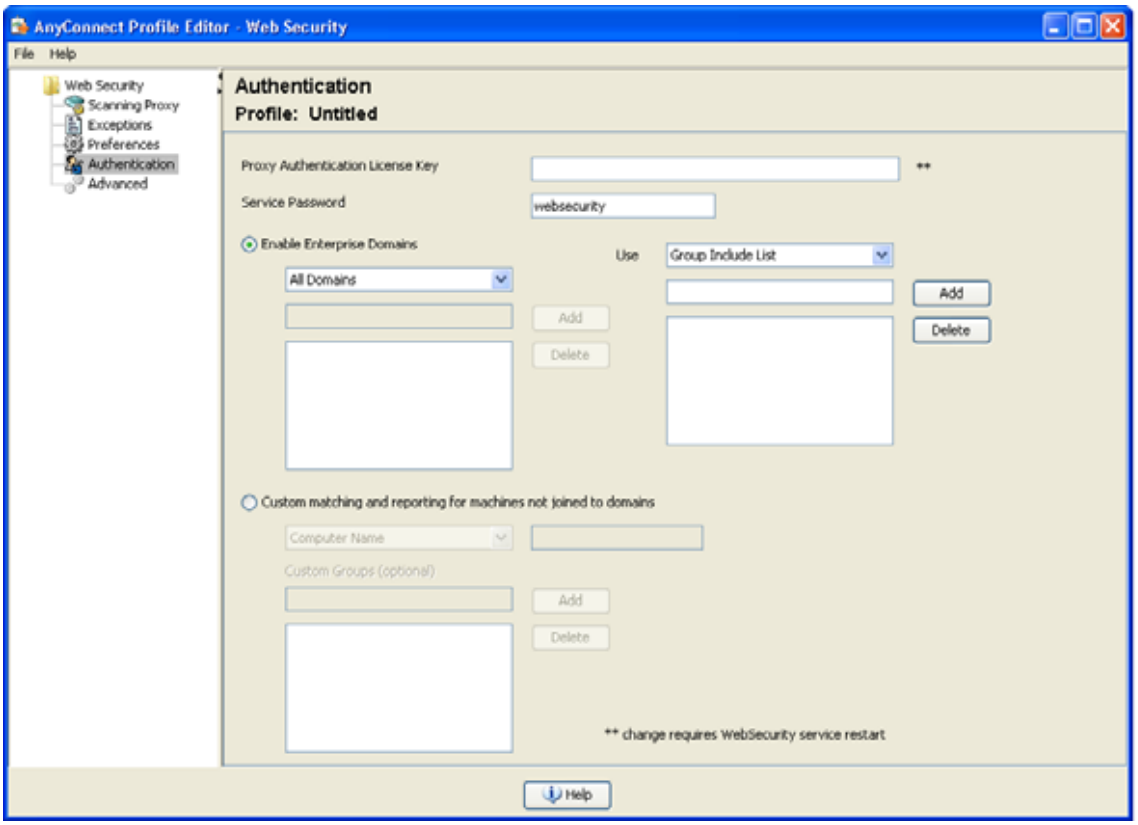
- コンピュータの名前を使用するには、リストの中で [Computer Name] をクリックします。または、ローカル ユーザ名を使用するには、[Local User] をクリックします。または、[Custom Name] をクリックしてカスタム ユーザ名を入力します。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する Cisco ScanCenter レポートで使用されます。
- [Authentication 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、[Add] をクリックします。

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。

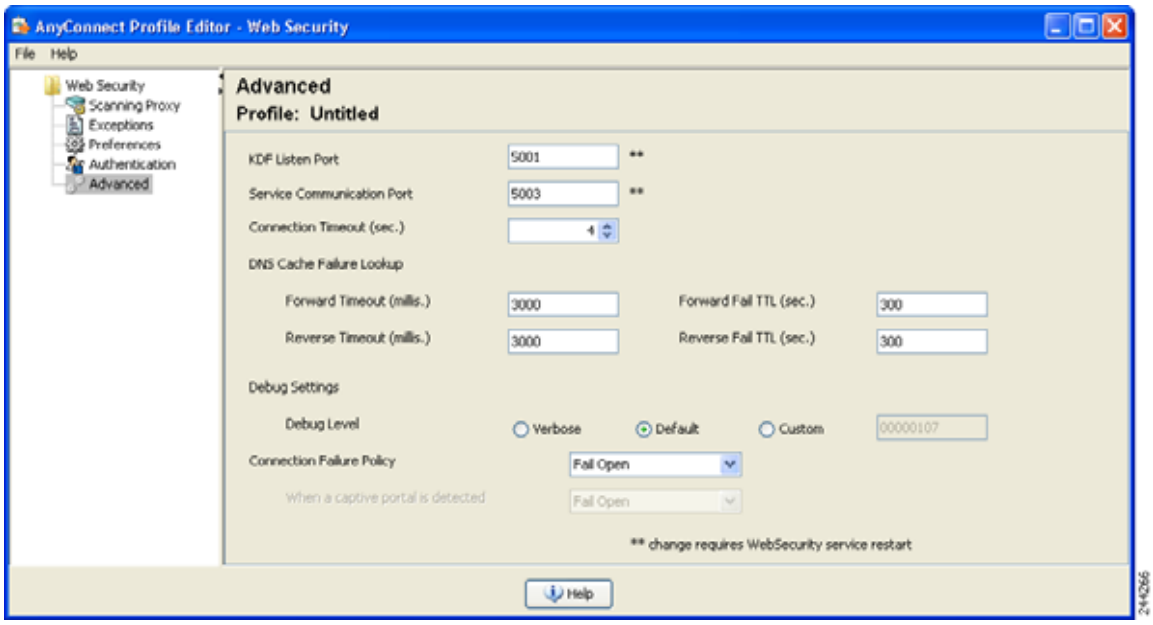
図 6-4　Cisco Cloud Web Security スキャニング プロキシ認証の設定



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 [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 6-5　Web セキュリティ クライアント プロファイルの [Advanced] パネル



プロファイル エディタの [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.6-21）
- 「サービス通信ポートの設定」（P.6-22）
- 「接続タイムアウトの設定」（P.6-22）
- 「DNS キャッシュ障害ルックアップの設定」（P.6-23）
- 「デバッグの設定」（P.6-23）
- 「フェール動作の設定」（P.6-23）

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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[Web Security] ツリー ペインで、[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 [Advanced] 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　[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 5　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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 [Edit] をクリックします。[Web Security] ツリー ペインで、[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 [Advanced] 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 3　[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。

[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　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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。
- Windows のスタンドアロン モードで、[Start] > [Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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 プロファイルを開きます。

ステップ 3　[Web Security] ツリー ペインで、[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 [Advanced] 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　[Connection Timeout] フィールドを変更します。

ステップ 5　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 [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

[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。

フェール動作の設定

Cisco Cloud Web Security プロキシ サーバへの接続が確立できない場合、トラフィックをブロックするように [Connection Failure Policy] リストで [Fail Close] を選択します。または、[Fail Open] を選択し、トラフィックを許可します。

Cisco Cloud Web Security プロキシ サーバへの接続が確立できないけれども、Wi-Fi ホット スポットなどのキャプティブ ポータルが検出された場合は、[When a captive portal is detected] リストで [Fail Open] を選択します。または、[Fail Open] を選択し、トラフィックをブロックします。

Web セキュリティ ロギング

Windows

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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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 [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。[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　[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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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 [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 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　[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、[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、[Tools] > [File Management] を選択します。

ステップ 2　[File Management] 画面で、[File Transfer] > [Between Local PC and Flash] をクリックして、[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 エディタを使用した Web セキュリティ クライアント プロファイルの作成

ステップ 1　[Start] > [All Programs] > [Cisco] > [Cisco AnyConnect Profile Editor] > [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　[File] > [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.6-28）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 セキュリティのスプリット除外ポリシーの設定

スプリット除外ポリシーの情報

ユーザが VPN セッションを確立すると、すべてのネットワーク トラフィックが VPN トンネルを介して送信されます。ただし、AnyConnect ユーザが Web セキュリティを使用している場合は、エンドポイントから送信される HTTP トラフィックをトンネルから除外し、Cloud Web Security スキャニング プロキシに直接送信する必要があります。

Cisco Cloud Web Security スキャニング プロキシのためのトラフィックのスプリット トンネル除外を設定するには、グループ ポリシーの [Set up split exclusion for Web Security] ボタンを使用します。

前提条件

- AnyConnect クライアントで使用するために Web セキュリティを設定する必要があります。
- グループ ポリシーを作成し、Web セキュリティを使用して設定された AnyConnect クライアント用の接続プロファイルにそれを割り当てている必要があります。

手順の詳細

ステップ 1　設定するヘッド エンド向けの ASDM セッションを開始し、[Remote Access VPN] > [Configuration] > [Group Policies] を選択します。

ステップ 2　設定するグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Advanced] > [Split Tunneling] を選択します。

ステップ 4　[Set up split exclusion for Web Security] を選択します。

ステップ 5　Web Security のスプリット除外に使用されるアクセス リストを新規に入力するか、既存のものを選択します。ASDM は、ネットワーク リストで使用するためのアクセス リストを設定します。

ステップ 6　新しいリストには [Create Access List for a new list] をクリックし、既存のリストには [Update Access List for an existing list] をクリックします。

ステップ 7　[OK] をクリックします。

ヒント　Secure Trusted Network Detection 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、HTTPS 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。

次の実施手順

スキャン プロキシが追加されたら、この手順で作成された統合アクセス リストを新しい情報で更新します。

Web セキュリティ クライアント プロファイルの Cisco 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 Cisco 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 Cisco 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 Cisco ScanCenter サーバにアップロードします。この XML ファイルには、Cisco Cloud Web Security 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（Cisco 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、Cisco Cloud Web Security 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。このクライアントは、Cisco Cloud Web Security ライセンス キーを含んでいる必要があります。ライセンス キーの詳細については、『*Cisco ScanCenter Administration Guide, Release 5.2*』を参照してください。

ステップ 2　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 Cisco 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。Cisco Cloud Web Security 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、『*Cisco ScanCenter Administration Guide, Release 5.2*』を参照してください。

ステップ 3　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、企業向けの Cisco ScanCenter 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、Cisco ScanCenter のホステッド コンフィギュレーション エリア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。

（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。

Secure Trusted Network Detection

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。Secure Trusted Network Detection 機能がイネーブルになっている場合、社内 LAN からのネットワーク トラフィックはすべて、送信元の Cisco Cloud Web Security 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、Cisco Cloud Web Security 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。

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [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.6-14）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、Secure Trusted Network Detection 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。

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化およびイネーブルにできます。

Windows を使用したフィルタのスイッチ オフおよびオン

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 [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　フィルタのスイッチ オンまたはオフ：

- 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

- フィルタリングをオフにするには **acwebsecagent.exe -disablesvc -*servicepassword*** と入力します。

Mac OS X を使用したフィルタのスイッチ オフおよびオン

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 [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　フィルタリングのスイッチ オフまたはオン

- フィルタリングをオンにするには、**./acwebsecagent -enablesvc** と入力します。
- フィルタリングをオフにするには、**./acwebsecagent -disablesvc -*servicepassword*** と入力します。

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。

（注） カスタマー エクスペリエンス フィードバック モジュールがインストールされイネーブルになっている場合、フィードバック モジュールがカスタマー フィードバック データとともにテレメトリ レポートを弊社のカスタマー フィードバック センターに送信します。フィードバック モジュールがイネーブルになっていない場合、テレメトリ モジュールは、Cisco IronPort Web セキュリティ アプライアンス（WSA）にそのレポートを送信します。

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））
- Windows Vista SP2（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、『Cisco AnyConnect Secure Mobility Solution Guide』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. [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、[Enable] をクリックしてから [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、anyconnect-win-<version>-k9.pkg の命名規則に従っています。

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、[Configuration] > [Remote Access VPN] > [Network(Client) Access] > [AnyConnect Client Settings] を選択します。

b. [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。[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、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。

b. [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. [Enable Host Scan/CSD] をオンにします。

d. [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、[Configuration] > [Remote Access VPN] > [Network(Client) Access] > [Group Policies] を選択し、編集するグループ ポリシーを選択して [Edit] をクリックします。

b. [Advanced] > [AnyConnect Client] の順に選択します。

c. [Optional Client Modules to Download 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 Telemetry] および [AnyConnect Posture] を選択します。

d. [OK] をクリックします。[Apply] をクリックします。[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、[Configuration] > [Remote Access VPN] > [Network(Client) Access] > [AnyConnect Connection Profiles] 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。[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. [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。[Apply] をクリックします。[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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profiles] を選択します。

b. [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、[Profile Usage] フィールドで [Telemetry] を選択します。

c. [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. [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. [Telemetry Policy] パネルの [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。[Apply] をクリックします。[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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Secure Mobility Solution] を選択します。

b. [Service Setup] エリアで、[Enable Mobile User Security Service] をオンにします。

c. [Apply] をクリックします。[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、次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、テレメトリ モジュールは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。

（注）　カスタマー エクスペリエンス フィードバック モジュールがインストールされイネーブルになっている場合、フィードバック モジュールがカスタマー フィードバック データとともにテレメトリ レポートを弊社のカスタマー フィードバック センターに送信します。フィードバック モジュールがイネーブルになっていない場合、テレメトリ モジュールは、Cisco IronPort Web セキュリティ アプライアンス（WSA）にそのレポートを送信します。

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。
   - エンドポイントにカスタマー エクスペリエンス フィードバック モジュールがインストールされ、それがイネーブルの場合、テレメトリ レポートはそのモジュールによって送信されます。

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、[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。

- [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。
- [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、[Configuration] > [Remote Access VPN] > [Configuration] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 2　[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　[Profile Usage] フィールドをクリックし、[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、[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）[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 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、[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、[Enable Service] チェックボックスをオンにします。

ステップ 9　[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　[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　[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　[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　[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。

- [Administration 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、[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**。

- [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、[Administration Defined Exceptions] リスト ボックスにリストされます。

ステップ 14　[Custom Certificate Select from file] フィールドで、[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　[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	場所	説明および優先順位
actsettings.xml	Installed on the endpoint here: %ALLUSERSPROFILE%\Application Data 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。 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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	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

Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュールの使用

（注） この機能は、デフォルトでイネーブルになっています。

シスコは、カスタマー エクスペリエンス フィードバック コンポーネントを作成しています。これは、お客様がどの機能およびモジュールを使用し、イネーブルにしているかに関する情報を提供してくれます。このクライアント情報を収集することでユーザ エクスペリエンスを探り、シスコは AnyConnect の品質、信頼性、パフォーマンス、ユーザ エクスペリエンスを継続して改善できます。

すべてのデータは匿名で収集され、個人を特定できるデータは含まれません。また、データは安全に送信されます。詳細については、[About Menu] からエンド ユーザ ライセンス契約書やプライバシー ポリシーを参照できます。[Cisco Online Privacy Statement Highlights] ページから [AnyConnect Secure Mobility Client Supplement] にアクセスできます。そこでは、情報の収集および使用について詳細が説明されています。

カスタマー エクスペリエンス フィードバックで収集されるデータには次の 3 種類のものがあります。

- ユーザビリティ データ：詳細については、プライバシー ポリシーをご参照ください。このデータは、毎月一度収集され送信されます。
- Web 脅威のデータ：テレメトリ モジュールがインストールされ、イネーブルになっている場合、カスタマー エクスペリエンス フィードバック モジュールを使用してテレメトリの収集データを転送できます。このデータは、脅威が報告されるたびに送信されます。テレメトリ モジュールの詳細については、第 7 章「WSA に対する AnyConnect テレメトリの設定」を参照してください。
- クラッシュ レポート：AnyConnect が生成したクラッシュ ダンプ ファイルが 24 時間おきにチェックされ、収集され、カスタマー エクスペリエンス フィードバック サーバに送信されます。

カスタマー エクスペリエンス フィードバック モジュールの主なコンポーネントは次のとおりです。

- フィードバック モジュール：AnyConnect のソフトウェア コンポーネントで、情報を収集し定期的にサーバに送信します。
- Cisco フィードバック サーバ：カスタマー エクスペリエンス フィードバック データを収集し、未処理形式で一時的なストレージに保存する、シスコが所有するクラウド インフラストラクチャです。

カスタマー エクスペリエンス フィードバック モジュールの設定

Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュールは、デフォルトでイネーブルになります。管理者は、推奨される設定を使用してプロファイルを設定することで、フィードバックを停止するように選択できます。エンドユーザは、管理者が決めた設定に従う必要があります。

要件

カスタマー エクスペリエンス フィードバック モジュールは、Windows および Mac OS X でサポートされています。

手順の詳細

ステップ 1　ASDM からプロファイル エディタを起動し、新しいプロファイルを作成するには、「内蔵 AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集」（P.2-3）で説明する手順に従います。ASDM と統合されたプロファイル エディタを使用して、カスタマー フィードバックモ ジュールのクライアント プロファイルを作成したら、手順 2 に進みます。

ステップ 2　ASDM を開いて [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 3　選択した AnyConnect カスタマー エクスペリエンス フィードバックのクライアント プロファイルを選択し、[Edit] をクリックします。カスタマー エクスペリエンス フィードバックのプロファイル エディタが開きます。

ステップ 4　デフォルトでは、カスタマー エクスペリエンス フィードバック モジュールをイネーブルになります。フィードバックの提供に参加したくない場合は、この項目を無効にする必要があります。このディセーブルは、インストール後いつでも行うことができ、カスタマー エクスペリエンス フィードバックを停止するのには推奨される方法です。

（注）　カスタマー エクスペリエンス フィードバックがイネーブルの場合、カスタマー エクスペリエンス フィードバック モジュールを使用してデバイスがテレメトリの役割を引き継ぐため、Cisco Web セキュリティ アプライアンス（WSA）は使用されません。カスタマー エクスペリエンス フィードバックがディセーブルの場合、テレメトリのデータが WSA に送信されます。

ステップ 5　デフォルトでは、クラッシュ レポートが含まれます。管理者は、AnyConnect が生成したクラッシュ レポートを収集しない場合はチェックボックスをオフにする必要があります。

ステップ 6　シスコでは、管理者が選択したカスタマー キーまたは ID を入力することをお勧めします。このキーは、シスコが特にお客様の組織から収集した情報を特定できるようにしたい場合、データを客様の組織と結び付けます。このキーがないと、シスコは組織別にレポートをグループ化できません。

インストール時のディセーブル化

カスタマー エクスペリエンス フィードバック モジュールをインストール時に削除することもできます。

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

- Windows 事前展開の場合
  - 「SMS を使用して AnyConnect モジュールを事前展開する」（P.2-25）を参照してください。
- Linux または Mac の事前展開の場合
  - 「Linux および Mac OS X コンピュータへの事前展開」（P.2-30）を参照してください。

（注）　このプロセスは、カスタマー エクスペリエンス フィードバック モジュールをディセーブルにするのに推奨されるオプションではありません。推奨される方法については、上記のステップ 4 を参照してください。

CHAPTER 9

NGE、FIPS、および追加セキュリティ

NGE（Next Generation Encryption）は、セキュリティおよびパフォーマンスの増大する要件を満たすために、暗号化、認証、デジタル署名、およびキー交換用の新しいアルゴリズムを導入しています。NSA（National Security Agency）は、デバイスが暗号化の強度に関する米国連邦基準を満たすためにサポートしなければならない一連の暗号アルゴリズムを指定しています。Suite B 暗号化スイートは RFC 6379 で定義されています。NSA Suite B として定義されたアルゴリズムの集合的なセットは標準になりつつあるので、AnyConnect IPsec VPN（KEv2 のみ）、PKI、802.1X、および EAP サブシステムがそれらをサポートするようになりました。AnyConnect 3.1 は、Suite B 暗号の CiscoSSL 0.9.8r.1.3 FIPS 認定の実装を使用します（AnyConnect 3.1 は TLS/DTLS、SRTP、および SSH Suite B をサポートしません）。シスコの Suite B 仕様の実装は、FIPS 認定を受けており、AnyConnect および ASDM の設定を通して、NGE 機能が FIPS と見なされます。

AnyConnect VPN コンポーネントは、2 つの VPN ヘッド エンドのうちのいずれかに接続できます。

- ASA
- IOS

この機能を使用するためにクライアント側の設定は必要ありません。

AnyConnect コンポーネントは、適応型セキュリティ アプライアンス（ASA）の設定に基づいて NGE とネゴシエートしてそれを使用します。AnyConnect クライアントの [Statistics] パネル（[Transport Information] ヘッダーの下）には、使用中の暗号名が表示されます。

この章で説明する内容は、次のとおりです。

NGE および AnyConnect に関する情報

AnyConnect 3.1 VPN およびネットワーク アクセス マネージャの NGE（Next Generation Encryption）には次の機能が含まれています。

- 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）
  - （ネットワーク アクセス マネージャ）ソフトウェアにおける有線トラフィック暗号化向けの 802.1AE（MACsec）（Windows 7）
  - （VPN）IKEv2 ペイロード暗号化および認証（AES-GCM のみ）

  - （VPN）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
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で SHA-2 を使用して証明書を使用できる機能
  - （VPN）IKEv2 ペイロード認証（Windows Vista 以降および Mac OS X 10.6 以降）
  - （VPN）IKEv2 パケット認証（Windows Vista 以降および Mac OS X 10.6 以降）
- キー交換向けの ECDH サポート
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で ECDHE を使用できる機能（Windows 7 および Windows XP）
  - （VPN）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、521 ビット楕円曲線）
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で ECDSA と証明書を使用できる機能（クライアント証明書には Windows 7 および Vista のみをサポート。スマート カードには Windows 7 のみをサポート）。
  - （VPN）IKEv2 ユーザ認証およびサーバ証明書の確認

（注） Linux では、AnyConnect は Firefox 証明書ストアまたは AnyConnect ファイル証明書ストアの両方を使用できます。ECDSA 証明書には、AnyConnect ファイル ストアのみサポートされています。ファイル ストアに証明書を追加するには、「Mac および Linux での PEM 証明書ストアの作成」を参照してください。

- IPsecV3 VPN 用の新しい暗号アルゴリズム。AnyConnect 3.1 は、ヌル暗号化を除く、IPsecV3 で必要とされるアルゴリズムをサポートしています。IPsecV3 は、ESN（Extended Sequence Numbers）がサポートされなければならないことも明記していますが、AnyConnect 3.1 は ESN をサポートしません。
- アルゴリズム間のその他の暗号スイートの依存関係は、AnyConnect 3.1 における次の内容に対する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

- 暗号化および整合性の両方が 1 回の操作で実行される複合モードの暗号化アルゴリズムは、ハードウェア クリプト アクセラレーションを使用する SMP ASA ゲートウェイ（5585 および 5515-X など）でのみサポートされます。AES-GCM は、シスコがサポートする複合モードの暗号化アルゴリズムです。

（注）　IKEv2 ポリシーは、通常モードまたは複合モードの暗号化アルゴリズムのうちの 1 つを含めることができますが、両方は不可能です。複合モードのアルゴリズムが IKEv2 ポリシーで設定されると、通常モードのアルゴリズムすべてがディセーブルになるので、唯一有効な整合性アルゴリズムは NULL です。

IKEv2 IPsec プロポーザルは別のモデルを使用し、同じプロポーザル内で標準モードおよび複合モード両方の暗号化アルゴリズムを指定できます。この使用方法では、両方に整合性アルゴリズムを設定する必要があります。その結果、非 NULL 整合性アルゴリズムが AES-GCM 暗号化で設定されます。

- NGE には、NSA Suite B アルゴリズムを使用する IKEv2 リモート アクセス接続用の AnyConnect Premium ライセンスが必要です。ほかの接続または目的（たとえば PKI）向けの Suite B アルゴリズムの使用には制限がありません。ライセンス チェックは、リモートアクセス接続に対して実行されます。AnyConnect Premium ライセンスがない状態で NSA Suite B 暗号化アルゴリズムを使用しようとしているというメッセージを受信した場合、Premium ライセンスをインストールするか、暗号化の設定を適切なレベルに再設定するか選択できます。
- IPSec 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 IKE 中間を含むサーバ証明書が必要です。Key Usage を含まない IPSec 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 IPSec 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。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

- Suite B は IKEv2/IPsec でのみ利用できます。
- 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。
- TLS v1.2 ハンドシェイクは AnyConnect 3.1 ではサポートされません。
- TLS v1.2 証明書認証は AnyConnect 3.1 ではサポートされません。
- ECDSA 証明書は、Windows Vista 以降、Mac OS X 10.6 以降、Linux Red Hat 6（32 ビット）、および Linux Ubuntu 9.x、10.x、11.x（32 ビット）でサポートされています。ECDSA スマートカードは、Windows 7 でのみサポートされています。
- 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。
- Suite B プロファイルは、証明書内に特定のポリシー プロパティを持つ必要がある場合がありますが、これらの要件は ASA 上で強制され、AnyConnect 上では強制されません。
- ASA は SSL VPN の ECDSA 証明書をサポートしていないので、そのような証明書を SSL VPN に使用しないでください。
- ASA が SSL および IPsec 用の異なるサーバ証明書で設定されている場合は、信頼できる証明書を使用してください。異なる IPsec および SSL 証明書を持つ Suite B（ECDSA）の信用されていない証明書を使用する場合、ポスチャ評価、WebLaunch、またはダウンローダの障害が発生する可能性があります。
- AES-GCM は、計算集約型のアルゴリズムであるため、これらのアルゴリズムを使用するときは、全体的なデータ レートが低くなる可能性があります。新しい Intel プロセッサの一部は、特に AES-GCM の性能を向上させるために採用された特別な命令を含むものもあります。AnyConnect

3.1 は、それが実行されるプロセッサ上でそれらの新しい命令がサポートされているかどうかを自動的に検出します。サポートされている場合は、AnyConnect は新しい命令を使用し、特別な命令を持たないプロセッサと比較して VPN データ レートを大幅に向上させます。新しい命令をサポートするプロセッサのリストについては、http://ark.intel.com/search/advanced/?s=t&AESTech=true を参照してください。詳細については、http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/ を参照してください。

- IPSec 接続は、サーバ証明書で名前の検証を実行します。IPSec の名前検証では、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、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。

NGE での AnyConnect モジュールについて

AnyConnect に関する FIPS 認定の機能は、モデルごとに ASA に対して使用許諾されています。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。XML ファイル AnyConnectLocalPolicy にはセキュリティ設定が含まれていますが、それは ASA によって展開されません。これは、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展開する必要があります。クライアントの接続先である各 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:ネットワーク アクセス マネージャにおける FIPS サポートは、ユーザ コンピュータ上の AnyConnectLocalPolicy.xml に含まれる FIPS モード パラメータ、およびネットワーク アクセス マネージャのグループ ポリシーに含まれる FIPS モード パラメータによってイネーブルになります。

  ネットワーク アクセス マネージャ用の FIPS は、Windows 7/Vista および Windows XP でサポートされます。Windows XP には、3e Technologies International が提供する 3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）と、ネットワーク アクセス マネージャに統合されたサポート済みのドライバが必要です。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。

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か、事前に展開された AnyConnect インストーラ内にファイルを含める必要があります。

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。

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、Cisco 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。この MST は FIPS をイネーブルにするだけであり、ほか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。

AnyConnect 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。

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

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。MST パラメータ名は、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、AnyConnect ローカル ポリシーのパラメータと値 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 インストーラが新しいポリシー ファイルを作成できるようにするには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

Enable FIPS ツールを使用した 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、シスコの 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 9-1 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、AnyConnect ローカル ポリシーのパラメータと値 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 9-1 に、ポリシー設定と Enable FIPS ツールの引数を示します。ポリシー設定の説明は、「AnyConnect ローカル ポリシーのパラメータと値」（P.9-15）に記載されています。

表 9-1　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]**

表 9-1　ポリシー設定と Enable FIPS ツールの引数 （続き）

ポリシー設定	引数および構文
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。次の表は、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 9-2　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 以降では、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。AnyConnectLocalPolicy ファイルを手動で編集するか、AnyConnect プロファイル エディタのインストーラとともに配布される VPN ローカル ポリシー エディタを使用できます。パラメータは、「AnyConnect ローカル ポリシーのパラメータと値」（P.9-15）で説明されています。

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。

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ほかのコンポーネントでは、AnyConnect が FIPS をイネーブルにしたこと、および暗号化の使用を開始したことを検出できます。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 [*Use FIPS compliant algorithms for encryption, hashing, and signing*] を [Disabled] に変更することにより、[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 9-3 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 9-3　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 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 からのみ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ほかのサービス 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 [プログラムの追加と削除] 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。

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 9-4、表 9-5、表 9-6、表 9-7 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 9-4　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 9-5　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、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 9-6　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、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 9-7　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 9-8 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 9-8　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

ここでの例を続けると、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

次のパラメータは、VPN ローカル ポリシー エディタおよび AnyConnectLocalPolicy.xml ファイル内の要素です。XML 要素は、山括弧 <> で囲んで表示されています。

（注） ファイルを手動で編集し、ポリシー パラメータを省略した場合、この機能はデフォルトの動作を用います。

<acversion>

このファイルのすべてのパラメータを解釈できる AnyConnect クライアントの最小バージョンを指定します。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。

Fips モード

<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。

ダウンローダのバイパス

<BypassDownloader>

オンにすると、ダイナミック コンテンツのローカル バージョンの存在を検出し、アップデートする VPNDownloader.exe モジュールの起動をディセーブルにします。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。

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。

Web Launch の制限

<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。クライアントからユーザに情報メッセージが表示されます。

厳格な証明書トラスト

<StrictCertificateTrust>

選択すると、リモート セキュリティ ゲートウェイを認証するときに、AnyConnect は確認できない証明書を許可しません。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.
```

選択しないと、クライアントはユーザに証明書を受け入れるように要求します。これはデフォルトの動作で、AnyConnect の以前のバージョンと一致します。

（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。

プリファレンス キャッシングの制限
<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）。

トンネル プロトコルの制限
サポートされていません。

PEM ファイル証明書ストアを除外（Linux および Mac）
<ExcludePemFileCertStore>

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

Windows のネイティブ証明書ストアの除外（Windows のみ）
このオプションは、現在、サポートされていません。

Mac のネイティブ証明書ストアの除外（Mac のみ）

<ExcludeMacNativeCertStore>

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できないようにします。

FireFox の NSS 証明書ストアの除外（Linux および Mac）

<ExcludeFirefoxNSSCertStore>

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

ポリシーの更新

<UpdatePolicy>

このセクションでは、クライアントがどの ASAS からソフトウェアまたはプロファイルの更新を取得できるかを制御することができます。これらのタイプの更新のいずれかまたは両方をディセーブルにする場合は、クライアントがソフトウェアおよびローカル ポリシー プロファイルの更新を入手できるサーバを追加する必要があります。

ソフトウェアおよびプロファイル更新の設定がクライアントの更新にどのように影響するかに関する詳細については、「ソフトウェア ロックの使用例」（P.9-12）を参照してください。

- 任意のサーバからソフトウェア更新を許可

  <AllowSoftwareUpdatesFromAnyServer>

  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、サーバのリストに追加した ASA からのみソフトウェアを取得するようにします。

- 任意のサーバから VPN ポリシー更新を許可

  <AllowVPNProfileUpdatesFromAnyServer>

  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、サーバのリストに追加した ASA からのみ更新を取得できるようにします。

- サーバ名

  <ServerName>

  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各サーバを追加します。ServerName には、FQDN、IP アドレス、ドメイン名、またはワイルドカードを含むドメイン名を使用できます。

ローカル ポリシー ファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="3.0.0592">
    <FipsMode>true</FipsMode>
    <BypassDownloader>true</BypassDownloader>
    <RestrictWebLaunch>true</RestrictWebLaunch>
    <StrictCertificateTrust>true</StrictCertificateTrust>
    RestrictTunnelProtocols IPSec RestrictTunnelProtocols
    <RestrictPreferenceCaching>Credentials</RestrictPreferenceCaching>
    <ExcludePemFileCertStore>true</ExcludePemFileCertStore>
    <ExcludeWinNativeCertStore>true</ExcludeWinNativeCertStore>
    <ExcludeMacNativeCertStore>true</ExcludeMacNativeCertStore>
    <ExcludeFirefoxNSSCertStore>true</ExcludeFirefoxNSSCertStore>
```

```
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
            <AuthorizedServerList>
                <ServerName>asa.one</ServerName>
                <ServerName>asa.two</ServerName>
            </AuthorizedServerList>
    </UpdatePolicy>
</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、AnyConnect ネットワーク アクセス マネージャ クライアント プロファイルで FIPS モードをイネーブル化し、ローカル ポリシー内で FIPS モードをイネーブル化することでサポートされます。Windows XP では、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）を展開する必要もあります。

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 [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 モードの強制」（P.9-19）
- 「3eTI ドライバのインストール」（P.9-20）
- 「3eTI ドライバ インストーラ ソフトウェアの入手」（P.9-32）

ネットワーク アクセス マネージャでの FIPS モードの強制

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強制できます。

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、PEAP、EAP-FAST、および LEAP 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 モジュール
- FIPS 準拠のローカル ポリシー ファイル
- 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）（Windows XP のみ）

ネットワーク アクセス マネージャ プロファイル エディタを使用して、ローカル ポリシー ファイルの中で FIPS モードをイネーブルにします。詳細については、「[Client Policy] ウィンドウ」（P.4-5）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、完全な 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対象のドライバを使用して 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。

Windows XP システムの場合、ネットワーク アクセス マネージャの Log Packager ユーティリティが 3eTI パケットのログを収集します。

特記事項

1. 3eTI CKL ドライバ インストーラは、常に 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。

  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。

例：

- *–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、ほか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* 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。
  - 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 Explorer 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。

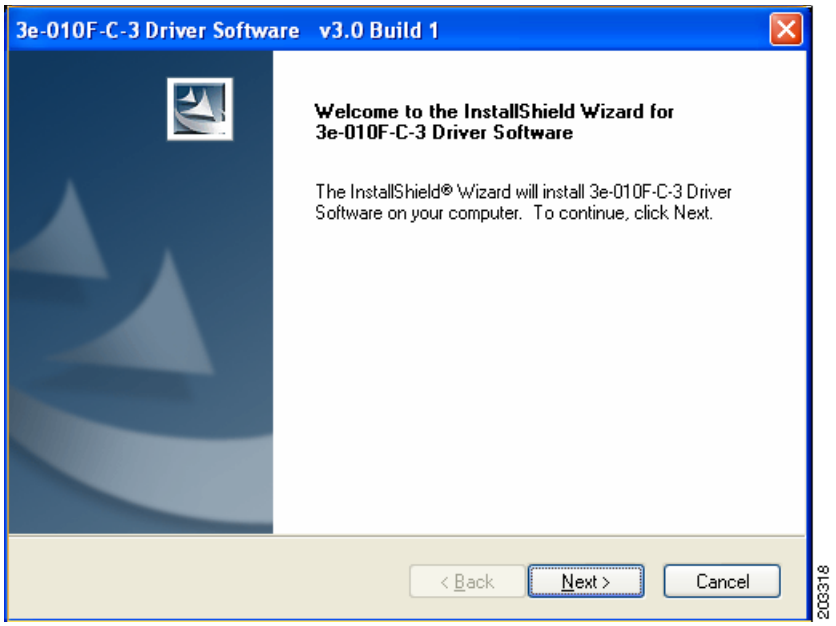
b. [Start] > [Run] をクリックし、次のインストーラ実行コマンドを入力します。

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。

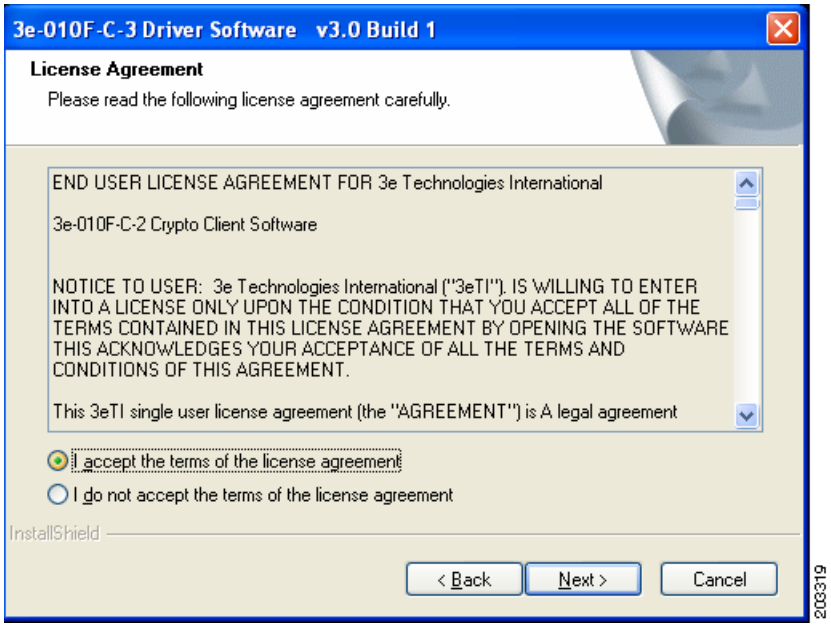
[Driver Welcome] ウィンドウが表示されます（図 9-1）。

図 9-1　[Driver Welcome] ウィンドウ



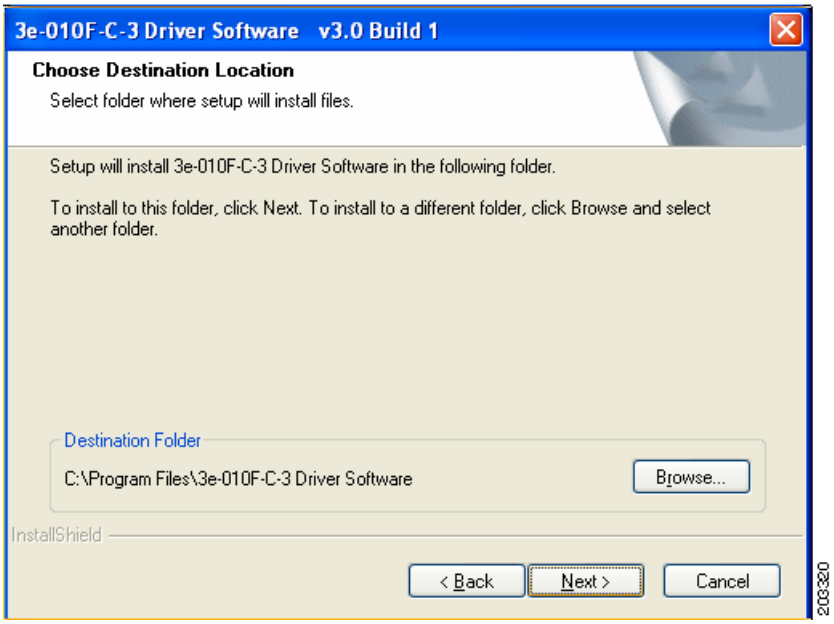
ステップ 2　[Next] をクリックすると、ライセンス契約書が表示されます（図 9-2 を参照）。

図 9-2　ライセンス契約書



ステップ 3　使用許諾契約を読み、同意して、[Next] をクリックします。[Destination Location Window] が開きます（図 9-3）。

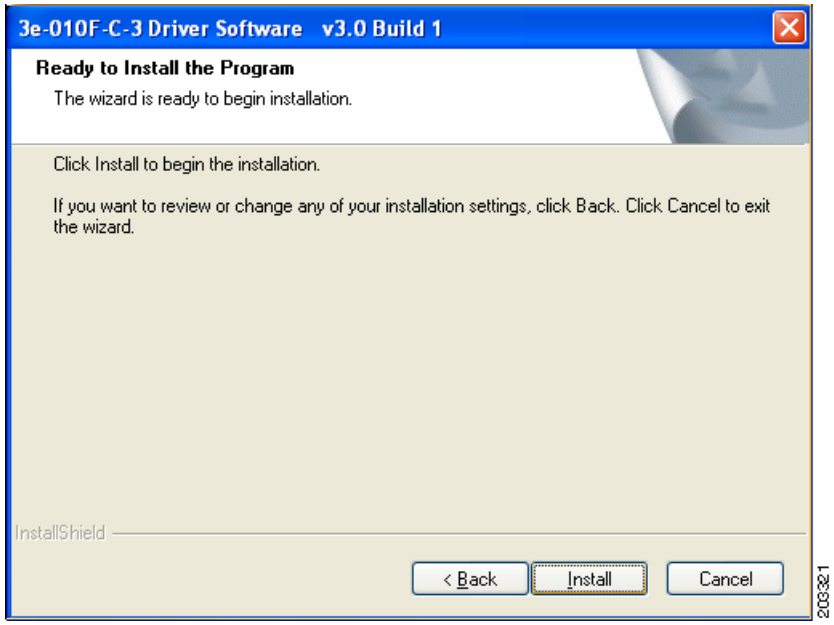
図 9-3　[Destination Location] ウィンドウ



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、[Browse] をクリックして目的のフォルダを探します。

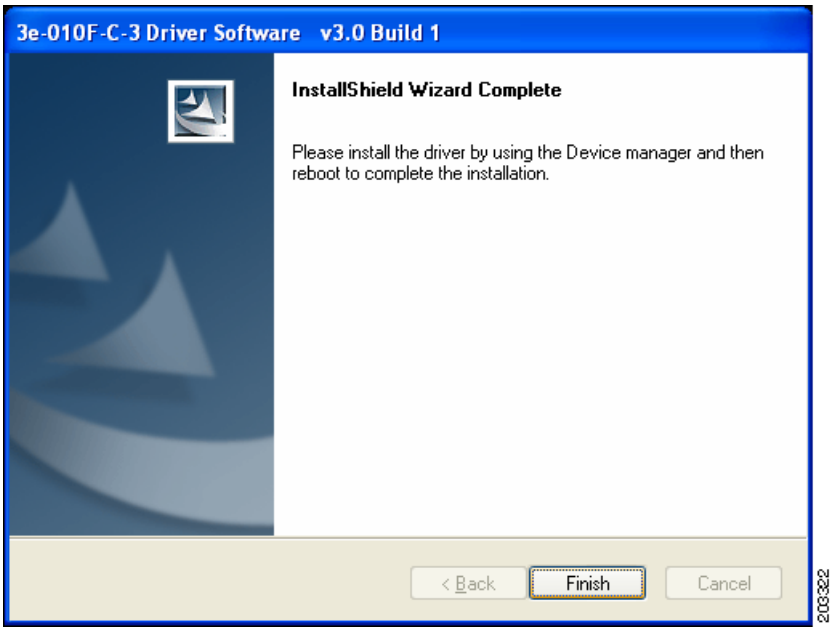
ステップ 5　[Next] をクリックします。[Ready to Install] ウィンドウが開きます（図 9-4）。

図 9-4　[Ready to Install] ウィンドウ



ステップ 6　[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、[Wizard Complete] ウィンドウが開きます（図 9-5）。

図 9-5　[Wizard Complete] ウィンドウ



ステップ 7　[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

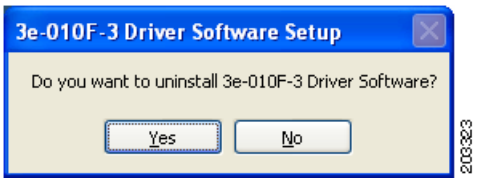
以前の 3eTI ドライバ ソフトウェアをアンインストールするには、次の手順を実行します。

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、[Start] > [Settings] > [Control Panel] > [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、[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 9-6 を参照）。

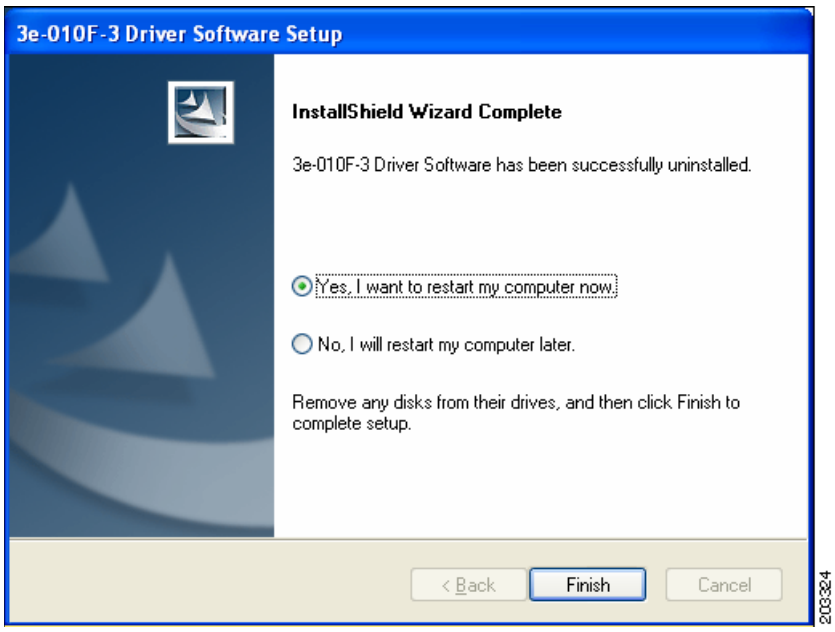
図 9-6　[Uninstall Driver Software] ポップアップ



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。

[Restart Computer Now] ウィンドウが開きます（図 9-7）。

図 9-7　[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、[Yes] をオンにします。

ステップ 5　[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*

各記号の意味は次のとおりです。

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.9-21）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　[Start] > [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*

各記号の意味は次のとおりです。

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.9-21）を参照）。

図 9-1 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.9-22) 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。

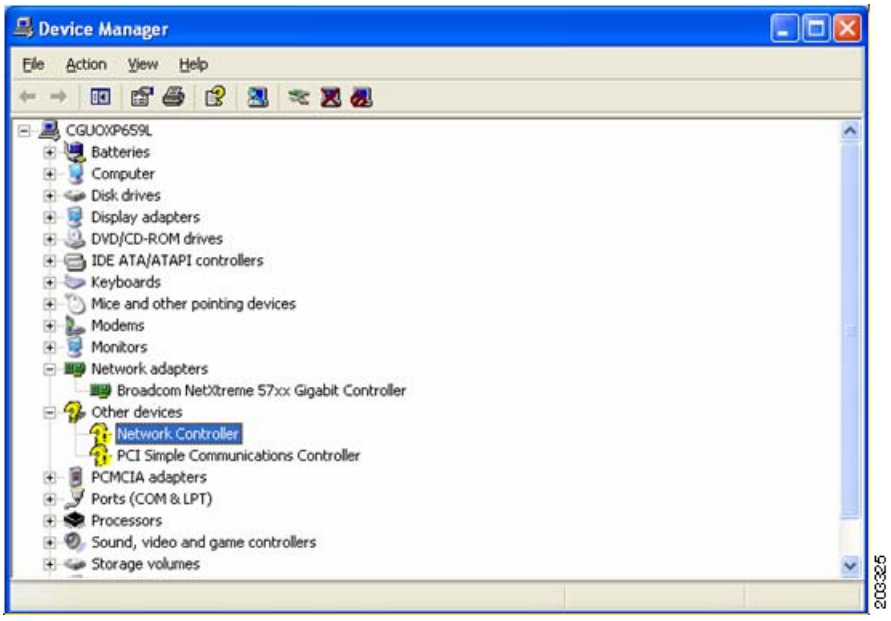
Windows のデバイス マネージャを使用して 3eTI ドライバ ソフトウェアを手動でアップグレードするには、次の手順を実行します。

ステップ 1　デスクトップ上の [My Computer] アイコンを右クリックし、[Properties] を選択します。

ステップ 2　[System Properties] ウィンドウで [Hardware] をクリックし、[Device Manager] をクリックします。

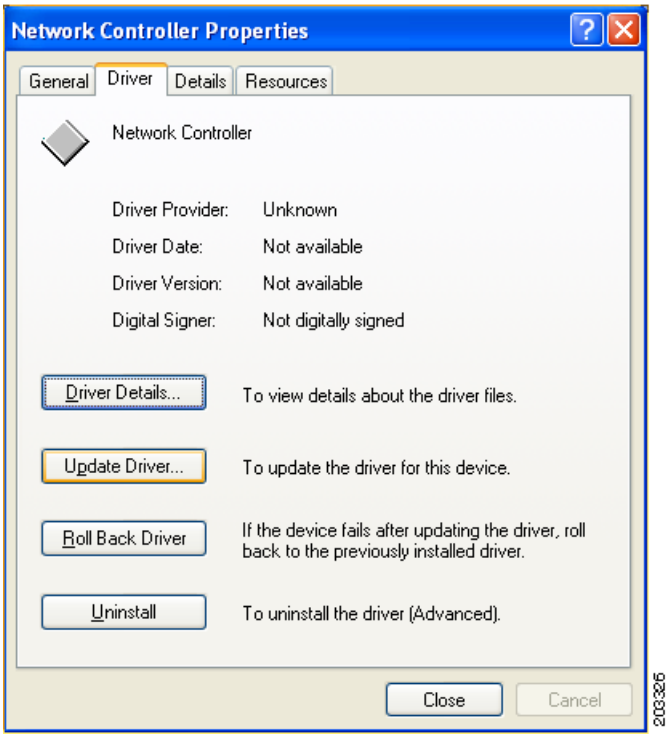
[Windows Device Manager] ウィンドウが開きます（図 9-8）。

図 9-8　[Windows 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、[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、[Properties] を選択します。[Network Controller Properties] ウィンドウが開きます（図 9-9）。

図 9-9　[Network Controller Properties] ウィンドウ



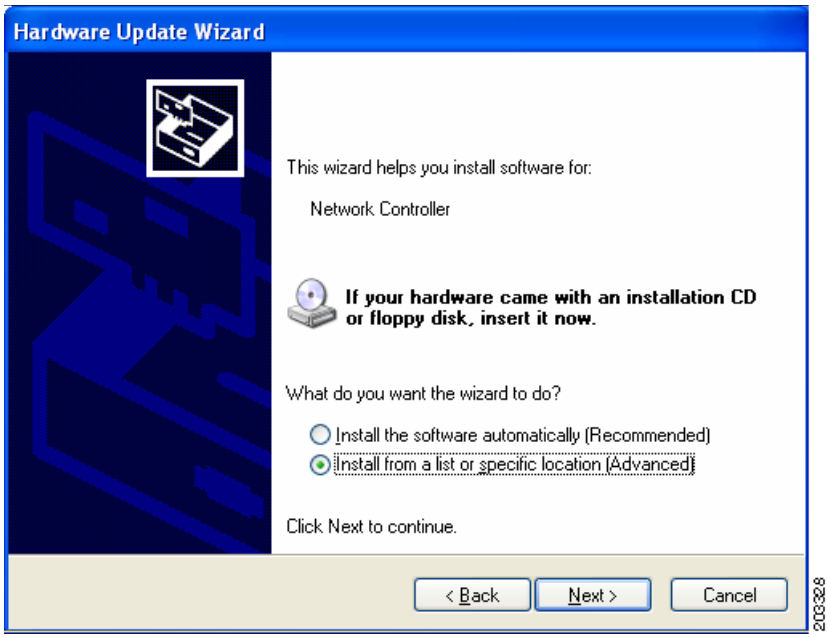
ステップ 4　[Driver] > [Update Driver] をクリックします。

[Windows Hardware Update Wizard] ウィンドウが開きます（図 9-10）。

図 9-10　[Windows Hardware Update Wizard] ウィンドウ

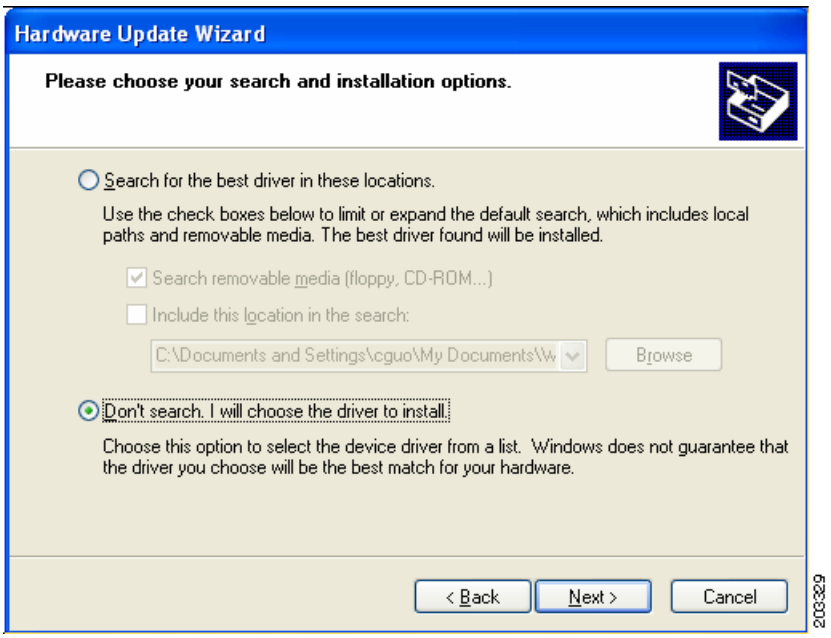
ステップ 5　Windows にドライバ ソフトウェアを検索させないために [No] をオンにし、[Next] をクリックします。[Hardware Update wizard] ウィンドウが続行します（図 9-11）。

図 9-11　[Installation CD or Floppy Disk Option] ウィンドウ



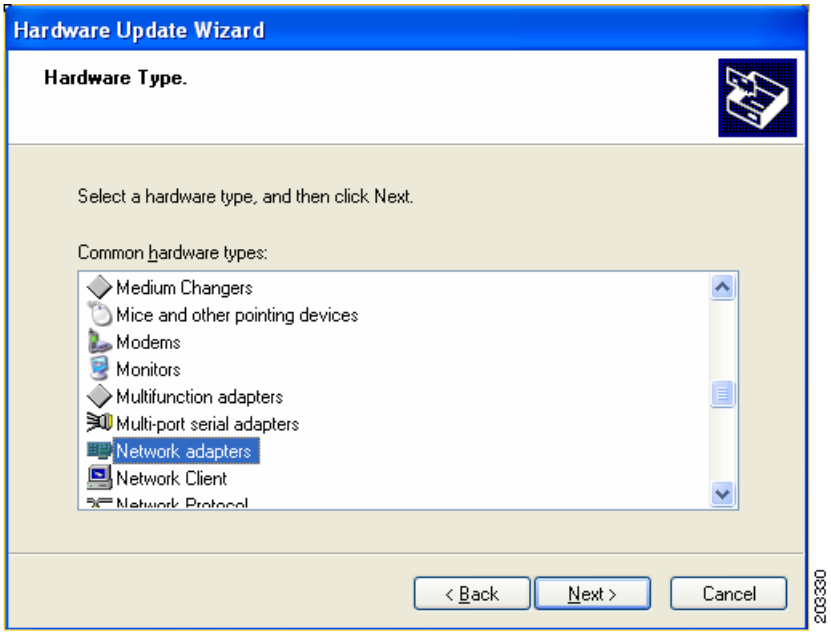
ステップ 6　[Install from a list or specific location (Advanced)] をオンにし、[Next] をクリックします。[Search and Installation Options] ウィンドウが開きます（図 9-12）。

図 9-12　[Search and Installation Options] ウィンドウ



ステップ 7　[Don't search. I will choose the driver to install] をオンにし、[Next] をクリックします。[Windows Hardware Type] ウィンドウが開きます（図 9-13）。

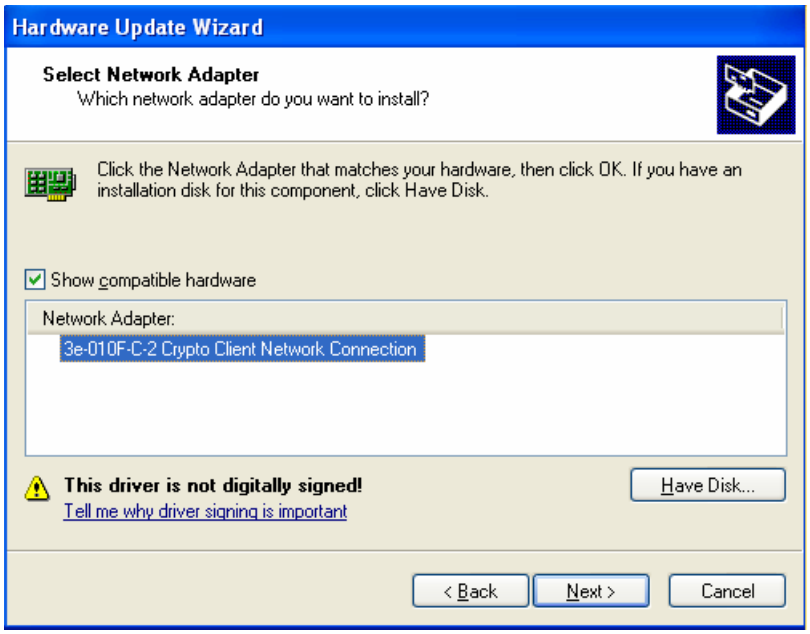
図 9-13　[Windows Hardware Type] ウィンドウ



ステップ 8　[Network adapter] を選択し、[Next] をクリックします。

ステップ 9　[Select Network Adapter] ウィンドウが開きます（図 9-14）。

図 9-14　[Select Network Adapter] ウィンドウ

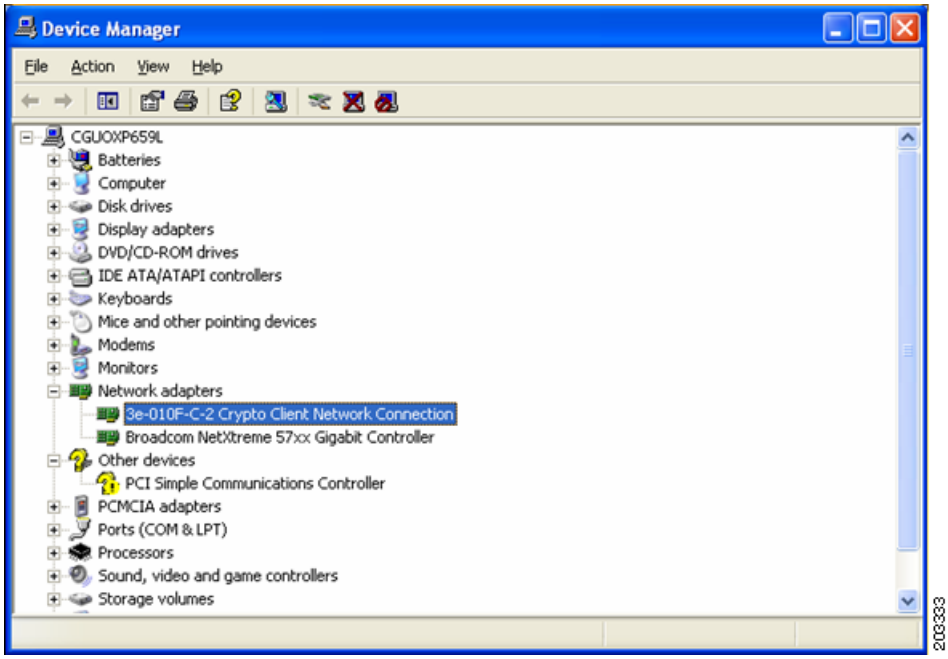


ステップ 10　3eTI ネットワーク接続を選択し、[Next] をクリックします。
[Installation Complete] ウィンドウが開きます（図 9-15）。

図 9-15　[Installation Complete] ウィンドウ

ステップ 11　ハードウェア ドライバのインストールが完了しました。[Finish] をクリックします。
[Device Manager] ウィンドウが再表示されます（図 9-16 を参照）。

図 9-16　更新された、Windows の [Device Manager] ウィンドウ



ステップ 12　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、[Properties] を選択します。アダプタのプロパティ ウィンドウの [Device status] で、「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 10

相互運用性のガイドラインおよび要件

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、[Configuration] > [Remote Access VPN] > [Network (Client) Access or Clientless SSL VPN Access] > [Dynamic Access Policies] で設定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

検疫時には、適応型セキュリティ アプライアンスで AnyConnect Premium ライセンスがアクティブになっている必要があります。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、Windows Mobile も含めて、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 は、Windows Mobile など AnyConnect でサポートされているすべての OS での検疫をサポートします。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が、Windows Mobile ではサポートしません。

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　（任意）非準拠コンピュータを修復するよう Host Scan を設定するには、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] > [Advanced Endpoint Assessment] を選択します。

ステップ 2　[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択して [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。[Action] タブをクリックし、[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 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、[Properties] をクリックします。

ステップ 4　[Group Policy] タブを選択して、[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、[Properties] をクリックします。[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、[Allow] カラムの [Read] チェックボックスと [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　[Edit] をクリックして、[User Configuration] > [Windows Settings] > [Internet Explorer Maintenance] > [Security] を選択します。

ステップ 8　右側のペインで [Security Zones and Content Ratings] を右クリックし、[Properties] をクリックします。

ステップ 9　[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、[Continue] をクリックします。

ステップ 10　[Modify Settings] をクリックし、[Trusted Sites] を選択して、[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、[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　[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　[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 [Maintenance] > [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 10-1 および表 10-2 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 10-1　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 10-2　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 Client 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 11

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。

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。

（注） 証明書のみの認証には、トンネル プロトコル（IKEV2 または SSL）の有無にかかわらず、デジタル証明書内で [Extended Key Usage]（EKU）属性を正しく設定する必要があります。ASA ID 証明書では、EKU 属性を `server-authentication` に設定する必要があります。クライアント ID 証明書では、EKU 属性を `client-authentication` に設定する必要があります。

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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。接続プロファイルを選択し、[Edit] をクリックします。[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 [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 [Authentication] エリアで、[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、[Configuration] > [Remote Access VPN] > [AnyConnect Connection Profiles] を選択します。右ペインの [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、[Device Certificate] をクリックします。

ステップ 5　[Specify Device Certificate] ダイアログで、[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、[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、「証明書の失効通知の設定」（P.3-51）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。

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）のトークンを使用したキーチェーン

（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。

- 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:] 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 [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.11-12) 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。

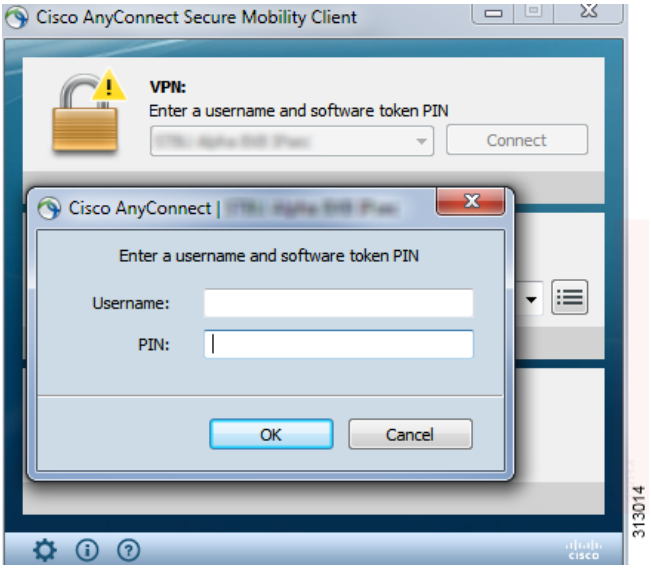
AnyConnect との互換性が保持される ASA 設定の詳細については、「RADIUS/SDI プロキシと AnyConnect との互換性の保持」（P.11-10）を参照してください。

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 11-1 のようなダイアログボックスが表示されます。

図 11-1　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 11-2、図 11-3、および図 11-4 を参照してください。

図 11-2　　パスコードまたは PIN ダイアログボックス

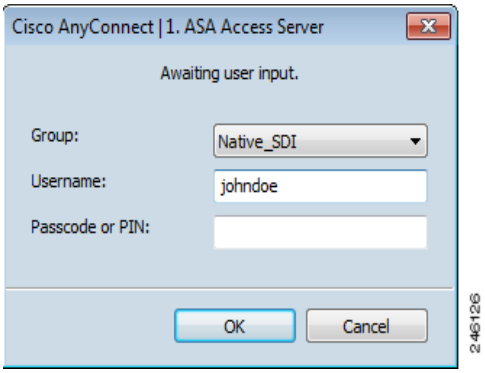


図 11-3　　PIN ダイアログボックス

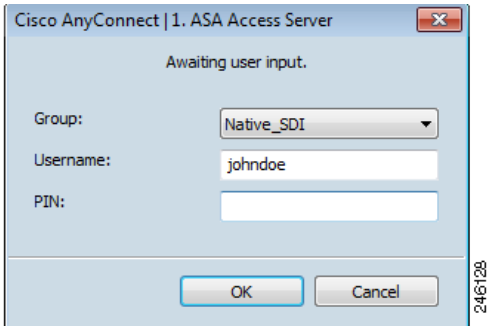
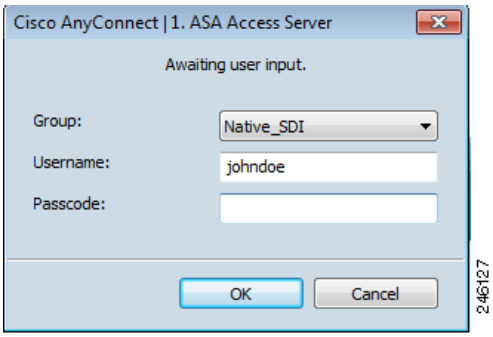


図 11-4　　パスコード ダイアログボックス



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、[Network (Client) Access AnyConnect Connection Profiles] ページで [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 [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 [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 [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 [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.11-10）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 [Continue]（図 11-5）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 11-6）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 11-5　ユーザが PIN の作成を選択

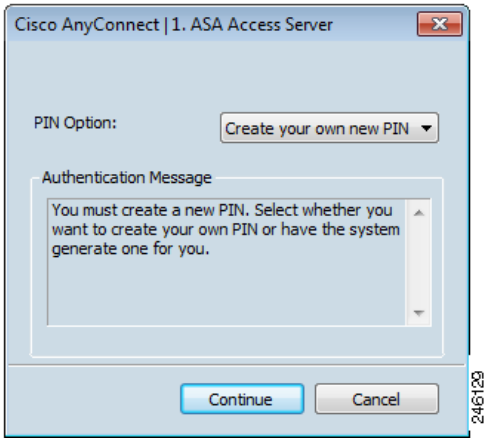
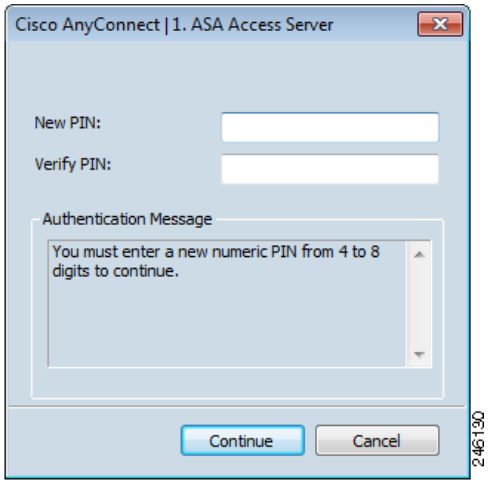


図 11-6　新規 PIN の作成



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、[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 [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。この項では、次のトピックを扱います。

- 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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [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、[Edit] をクリックします。

ステップ 3　[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 [Advanced] ノードを展開して、[Group Alias / Group URL] を選択します。

ステップ 4　[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　[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] を選択します。

ステップ 7　[Add] をクリックして、AAA サーバ グループを追加します。

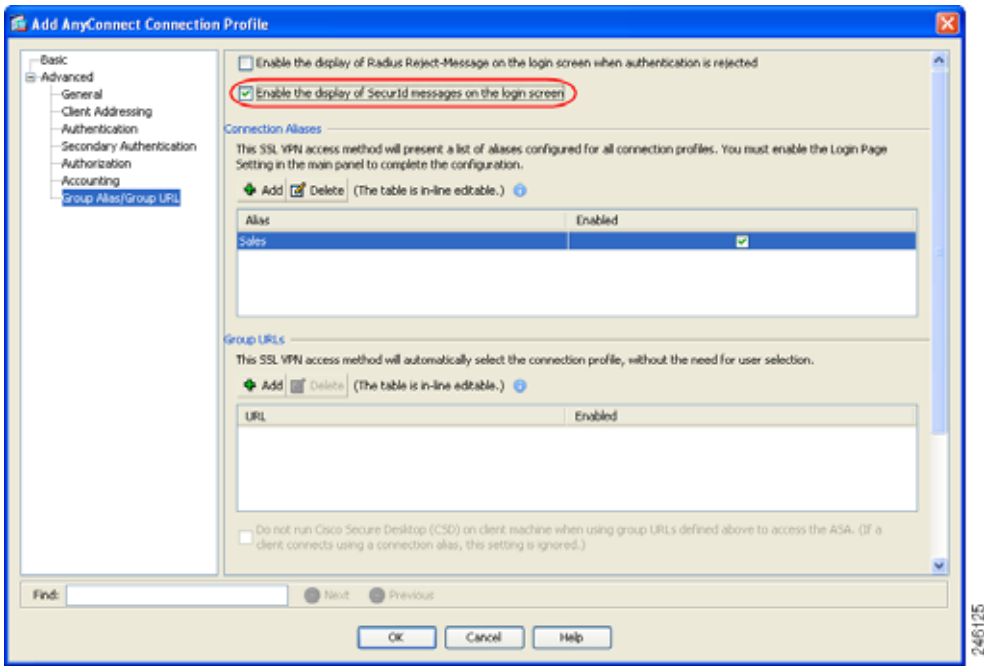
ステップ 8　[Edit AAA Server Group] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9　[AAA Server Groups] 領域で作成した AAA サーバ グループを選択し、[Servers in the Selected Group] 領域で [Add] をクリックします。

ステップ 10　[SDI Messages] 領域で [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。[Apply] をクリックします。[Save] をクリックします。

図 11-7　[Add/Edit AnyConnect Connection Profile] 画面



ASA 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。Cisco 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 11-1 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 11-1　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 12

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 GUI 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、インストーラでリモート 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。「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」（P.12-2）を参照してください。
- 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インポートする（Windows のみ。「トランスフォームを使用した GUI のカスタマイズ」（P.12-3）を参照）。インストーラを使用して ASA から展開されます。
- 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）。「クライアント API を使用する実行ファイルの展開」（P.12-5）を参照してください。

（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。

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

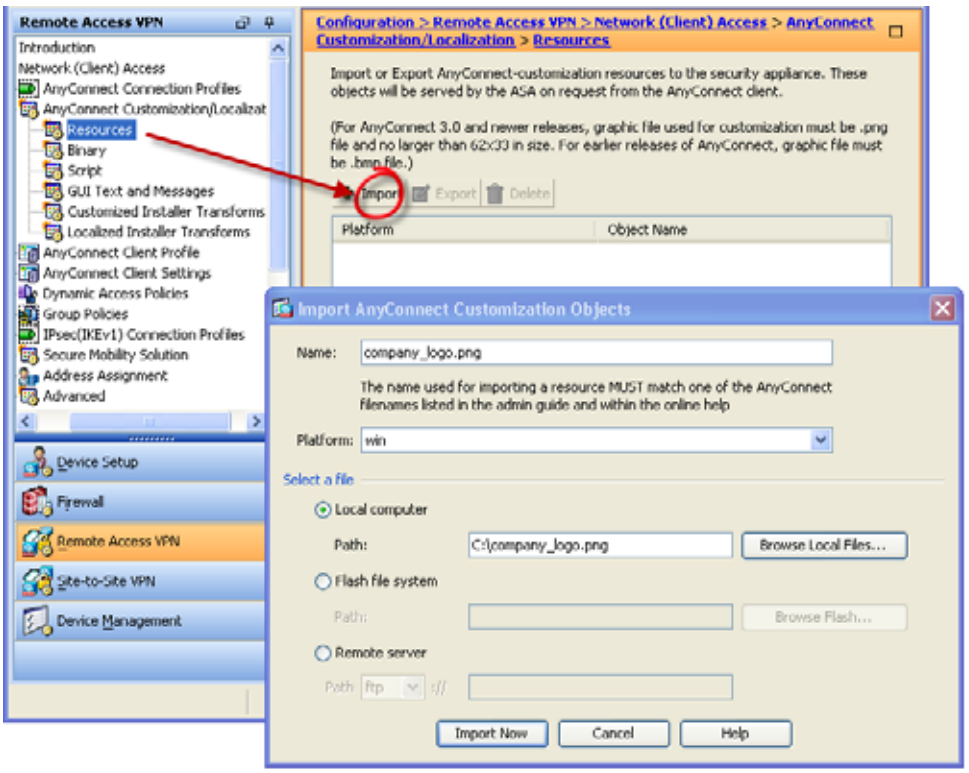
独自のカスタム ファイルをセキュリティ アプライアンスにインポートし、その新しいファイルをクライアントに展開することによって、AnyConnect をカスタマイズすることができます。表 12-2、表 12-3、および表 12-4 に、オリジナルの GUI アイコンのサンプル イメージとそのサイズを示します。

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、次の手順を実行します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Resources] の順に選択します。

[Import] をクリックします。[Import AnyConnect Customization Object] ウィンドウが表示されます（図 12-1）。

図 12-1　カスタマイゼーション オブジェクトのインポート

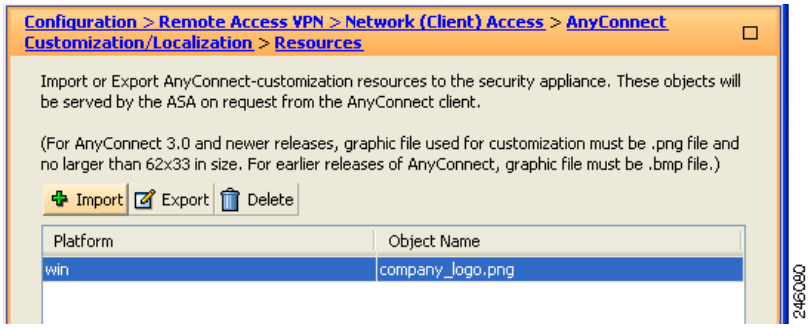


ステップ 2　インポートするファイルの名前を入力します。置き換え可能なすべての GUI コンポーネントのファイル名については、表 12-2、表 12-3、および表 12-4 を参照してください。

（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。[Import Now] をクリックします。ファイルがテーブル（図 12-2）に表示されます。

図 12-2　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。

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 ソフトウェア開発キット（SDK）の一部であり、これは 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。

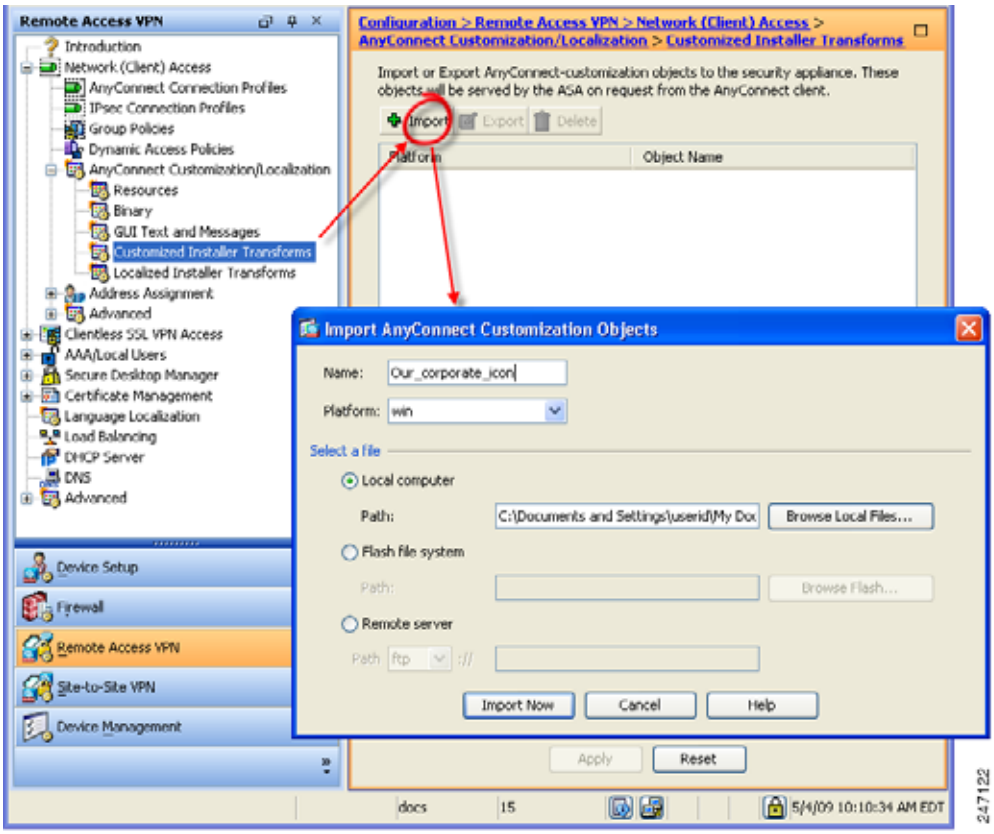
C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

Orca ソフトウェアをインストールしてから、[Start] > [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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Customized Installer Transforms] の順に選択します。[Import] をクリックします。[Import AnyConnect Customization Objects] ウィンドウが表示されます（図 12-3）。

図 12-3　カスタマイズ用トランスフォームのインポート

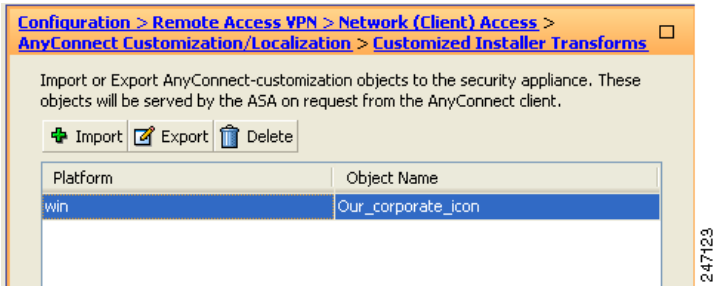


ステップ 2　インポートするファイルの名前を入力します。他のカスタマイズ用オブジェクトの名前とは異なり、この名前は ASA にとって重要ではないため、自由に指定できます。

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。[Import Now] をクリックします。ファイルがテーブル（図 12-4）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 12-4　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
```

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（PPC または Intel ベース）コンピュータの場合、AnyConnect API を使用する独自のクライアントを展開できます。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。

（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。

表 12-1 に、クライアント実行ファイルのファイル名を、オペレーティング システム別に示します。

表 12-1　クライアント実行ファイルのファイル名

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	サポート対象外[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 12-1 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。

ASA にインポートするカスタム Windows クライアント バイナリ（GUI または CLI バージョン）には、署名することを推奨します。署名付きバイナリには、使用可能な多くの機能があります。バイナリが署名されていないと、次の機能に影響が生じます。

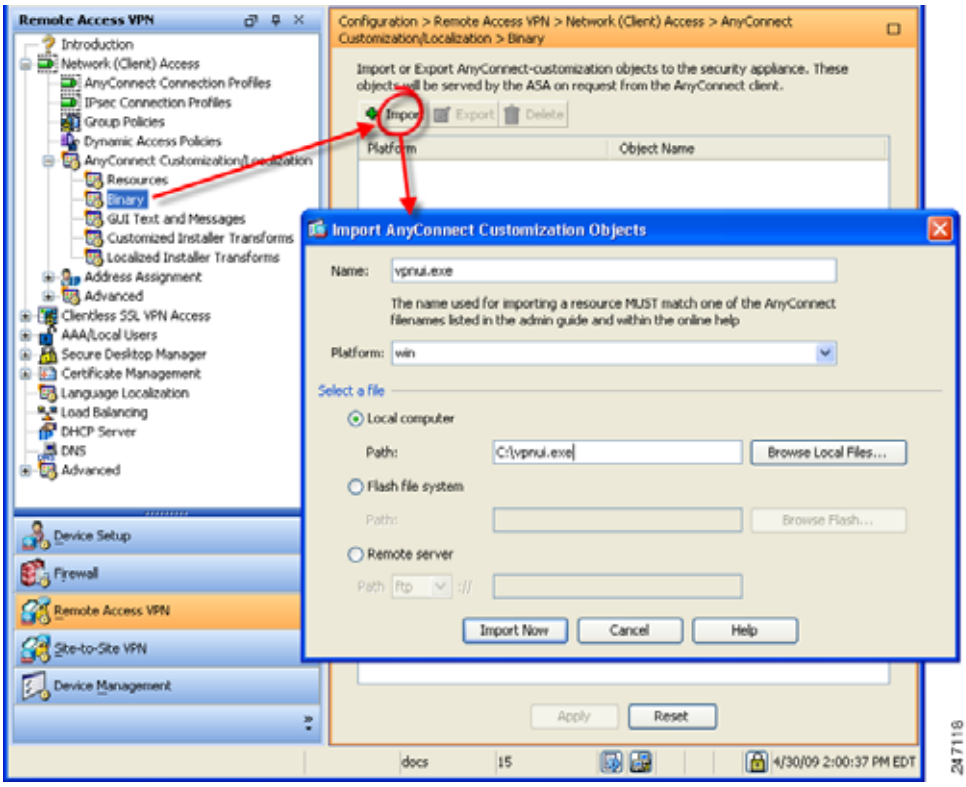
- Web ラウンチ：クライアントレス ポータルは使用可能でユーザ認証も可能です。ただし、トンネル確立周辺の動作が予期したとおりに行われません。クライアントに署名のない GUI が存在すると、クライアントはクライアントレス接続試行の一部として開始されません。また、この状態が検出された場合、クライアントでの接続試行が中断されます。
- SBL：Start Before Logon 機能では、ユーザのクレデンシャルを要求するために使用するクライアント GUI には署名が必要です。署名がないと、GUI は開始されません。SBL は CLI プログラムでサポートされないため、影響を受けるのは GUI バイナリ ファイルだけです。
- 自動アップグレード：クライアントの新バージョンへのアップグレード中は古い GUI が存在しますが、新しい GUI がインストールされると新規 GUI が開始されます。新しい GUI は署名がないと開始されません。Web ラウンチ と同様、この GUI に署名がないと VPN 接続は終了します。ただし、アップグレード後のクライアントはインストールされたままになります。

クライアント GUI をカスタマイズする実行ファイルをインポートする手順は、次のとおりです。

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Binary] の順に選択します。

[Import] をクリックします。[Import AnyConnect Customization Objects] ウィンドウが表示されます（図 12-5）。

図 12-5　実行ファイルのインポート

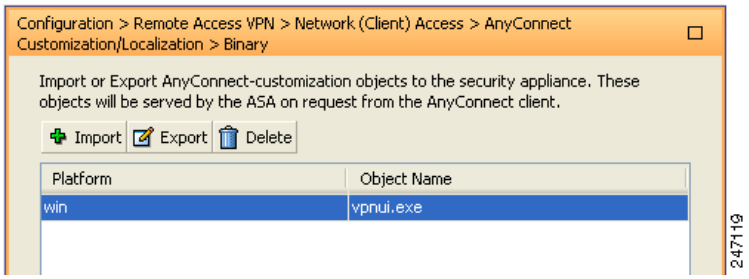


ステップ 2　インポートするファイルの名前を入力します。

実行ファイルのファイル名は、AnyConnect GUI に使用されるファイル名と一致している必要があります。たとえば、Windows クライアント用のクライアント GUI を置き換えるには、独自の実行ファイルを *vpnui.exe* 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実行ファイルを変更しません。

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。[Import Now] をクリックします。ファイルがテーブル（図 12-6）に表示されます。

図 12-6　テーブルに表示されたインポート済みの実行ファイル



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。表に含まれるイメージは、AnyConnect VPN クライアント、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 モジュールにより使用されます。

AnyConnect バージョン 3.1 では、さらに 2 つの UI ダイアログが追加されます。1 つは、ネットワーク接続ステータスの提示用で、もう 1 つは、ユーザがネットワーク接続用のパスワードを更新できるようにするためのものです。

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、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、[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。

Windows の場合

表 12-2 の 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 12-2 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 12-2　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 [Advanced] ダイアログの右上にある [About] ボタン。 サイズは調整できません。 	24 x 24 PNG
about_hover.png [Advanced] ダイアログの右上にある [About] ボタン。 サイズは調整できません。 	24 x 24 PNG
app_logo.png 最大サイズは 128 x 128 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 128 x 128 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。 	128 X 128 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

表 12-2　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
company_logo.png トレイ フライアウトおよび [Advanced] ダイアログの左上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
company_logo_alt.png [About] ダイアログ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 PNG
cues_bg.jpg トレイ フライアウト、[Advanced] ウィンドウ、および [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
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 12-2　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
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
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

表 12-2　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_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
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

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 12-3 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 12-3　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 [About] タブに表示されるアイコン。 	16 x 16 PNG
cvc-connect.png [Connect] ボタンの隣、および [Connection] タブに表示されるアイコン。 	16 x 16 PNG
cvc-disconnect.png [Disconnect] ボタンの隣に表示されるアイコン。 	16 x 16 PNG
cvc-info.png [Statistics] タブに表示されるアイコン。 	16 x 16 PNG

表 12-3　Linux 用 AnyConnect：アイコン ファイル （続き）

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

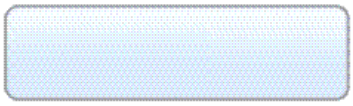
OS X 用のファイルはすべて次の場所に格納されています。

/Applications/Cisco AnyConnect Secure Mobility Client/Contents/Resources

（注）　[Resources] フォルダは、[Applications] > [Cisco] に移動して [Cisco AnyConnect Secure Mobility Client] をクリックし、[Show Package Contents] を選択すると見つかります。

表 12-4 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 12-4　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
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
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
Mac OS X ステータス アイコン。 	16 x 16 PNG

AnyConnect クライアントのヘルプ ファイルの作成およびアップロード

AnyConnect のユーザにヘルプを提供するために、サイトに関する手順を含む HTML ファイルを作成し、ASA にロードします。ユーザが AnyConnect に接続すると、AnyConnect がヘルプ ファイルをダウンロードし、AnyConnect ユーザ インターフェイス上にヘルプ アイコンを表示します。ユーザがヘルプ アイコンをクリックすると、ブラウザにヘルプ ファイルが開きます。

ステップ 1　**help_AnyConnect.html** という名前の HTML ファイルを作成します。

ステップ 2　ASDM を使用して ASA にログインし、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Binary] の順に選択します。

ステップ 3　**help_AnyConnect.xxx** ファイルをインポートします。サポートされる形式は、PDF、HTML、HTM、および MHT 形式です。

ステップ 4　PC 上で AnyConnect を起動し、ASA に接続します。ヘルプ ファイルがクライアント PC にダウンロードされます。

ステップ 5　ヘルプ アイコンが自動的に UI に追加されたことが分かるはずです。

ステップ 6　ヘルプ アイコンをクリックすると、ヘルプ ファイルがブラウザに表示されます。

ヘルプ アイコンが表示されない場合は、ヘルプのディレクトリを確認し、AnyConnect のダウンローダがヘルプ ファイルを取得できたかどうかを確認します。

ファイル名の「help_」の部分はダウンローダにより削除されるので、ご使用のオペレーティング システムに応じて、次のいずれかのディレクトリの中に AnyConnect.html が保存されているはずです。

- Windows 7 および Vista：C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help
- Windows XP：C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Help
- Mac OS：/opt/cisco/anyconnect/help

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開き（追加または編集し）、1 つ以上のメッセージ ID のメッセージ 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。メッセージ ファイルを開いたら、次の操作でそれを編集できます。

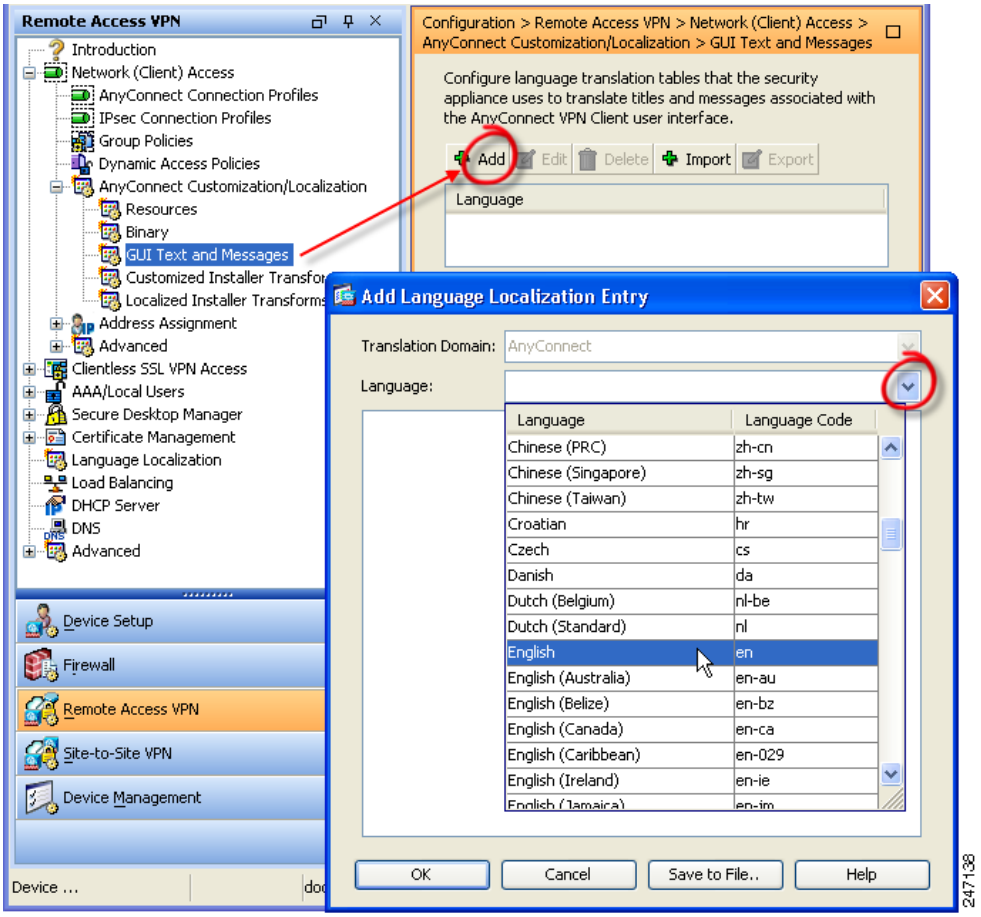
- 開いたダイアログのテキストに変更内容を入力します。
- 開いたダイアログのテキストを、テキスト エディタにコピーし、変更を行い、そのテキストを元のダイアログに渡します。
- [Save to File] をクリックしてメッセージ ファイルをエクスポートし、そのファイルを編集し、ファイルを ASDM にインポートします。

英語変換テーブルは、[Localization] メニュー（[Configuration] > [Remote Access VPN] > [Language Localization]）からも利用できます。ローカリゼーションについては、「AnyConnect クライアントの GUI とインストーラのローカライズ」（P.12-18）で説明します。

次の手順では、ダイアログを編集して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　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [GUI Text and Messages] の順に選択します。[Add] をクリックします。[Add Language Localization Entry] ウィンドウが表示されます（図 12-7）。

図 12-7　英語変換テーブルの追加

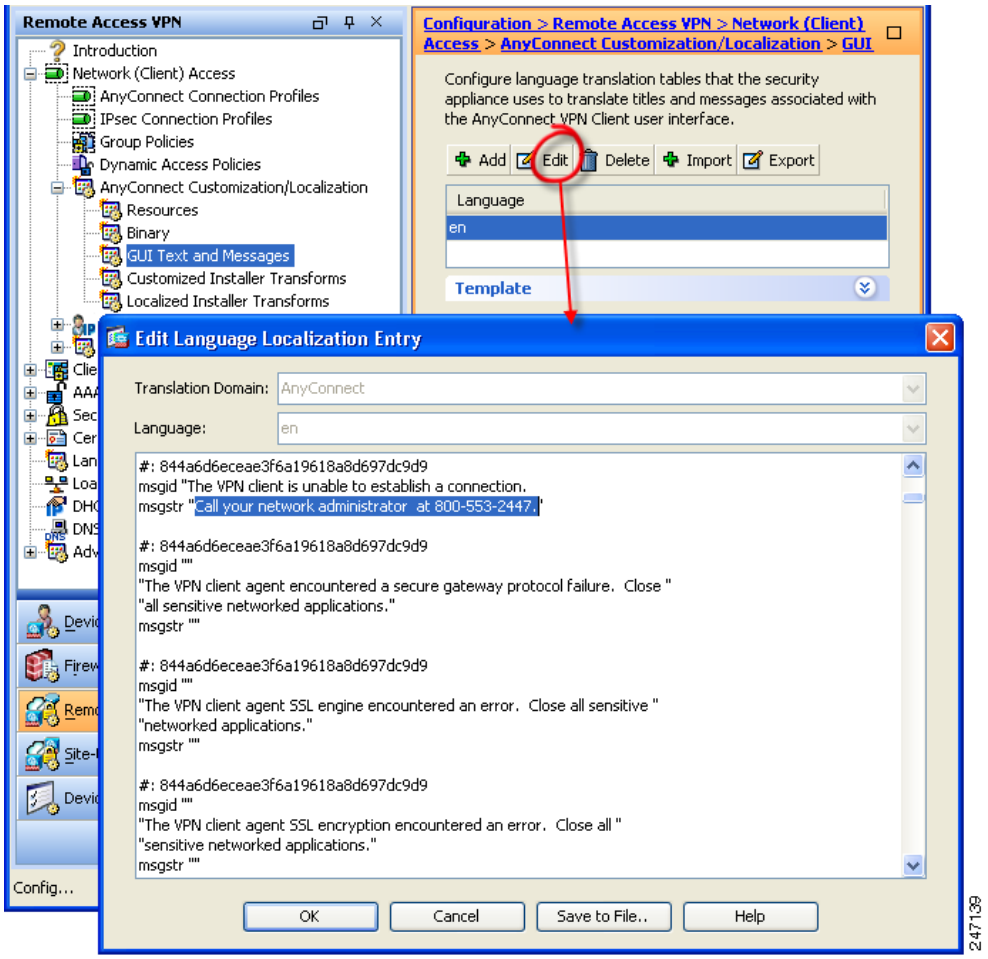


ステップ 2　[Language] ドロップ リストをクリックし、言語として [*English* (en)] を指定します。英語の変換テーブルが、ペインの言語リストに表示されます。

ステップ 3　[Edit] をクリックして、メッセージの編集を開始します。[Edit Language Localization Entry] ウィンドウが表示されます（図 12-8）。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。このテキストは変更*しないでください*。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 12-8　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 Text and Messages] ペインで [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。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

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。変換テーブルとは、翻訳されたメッセージ テキストの文字列を含むテキスト 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、AnyConnect ソフトウェア内の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。または、www.cisco.com から利用可能な次の変換テーブルのいずれかをインポートすることができます。利用可能な変換テーブルの ASA へのインポートを参照してください。

- 日本語
- フランス語（カナダ）
- ドイツ語
- 中国語
- 韓国語
- スペイン語（ラテンアメリカ）
- チェコ語
- ポーランド語

次の項では、目的の言語が利用できない場合や、インポートした変換テーブルをさらにカスタマイズしたい場合などに、GUI テキストおよびメッセージを翻訳するための手順を説明します。

- 「ASDM 変換テーブル エディタを使用した翻訳」（P.12-21）。この方法を使用すると、ファイルを開き（追加または編集し）、1 つ以上のメッセージ ID のメッセージ テキストを変更することで、メッセージ ファイルに変更を加えることができます。メッセージ ファイルを開いたら、次の操作でそれを編集できます。
  - 開いたダイアログのテキストに変更内容を入力します。
  - 開いたダイアログのテキストを、テキスト エディタにコピーし、変更を行い、そのテキストを元のダイアログに渡します。
- 「変換テーブルのエクスポートと編集による翻訳」（P.12-26）。この方法を使用すると、[Save to File] をクリックしてファイルをエクスポートし、そのファイルを編集し、ファイルを元の ASDM にインポートできます。

ASA の変換テーブルを更新したら、クライアントを再起動し、別の接続に成功するまで、更新したメッセージは適用されません。

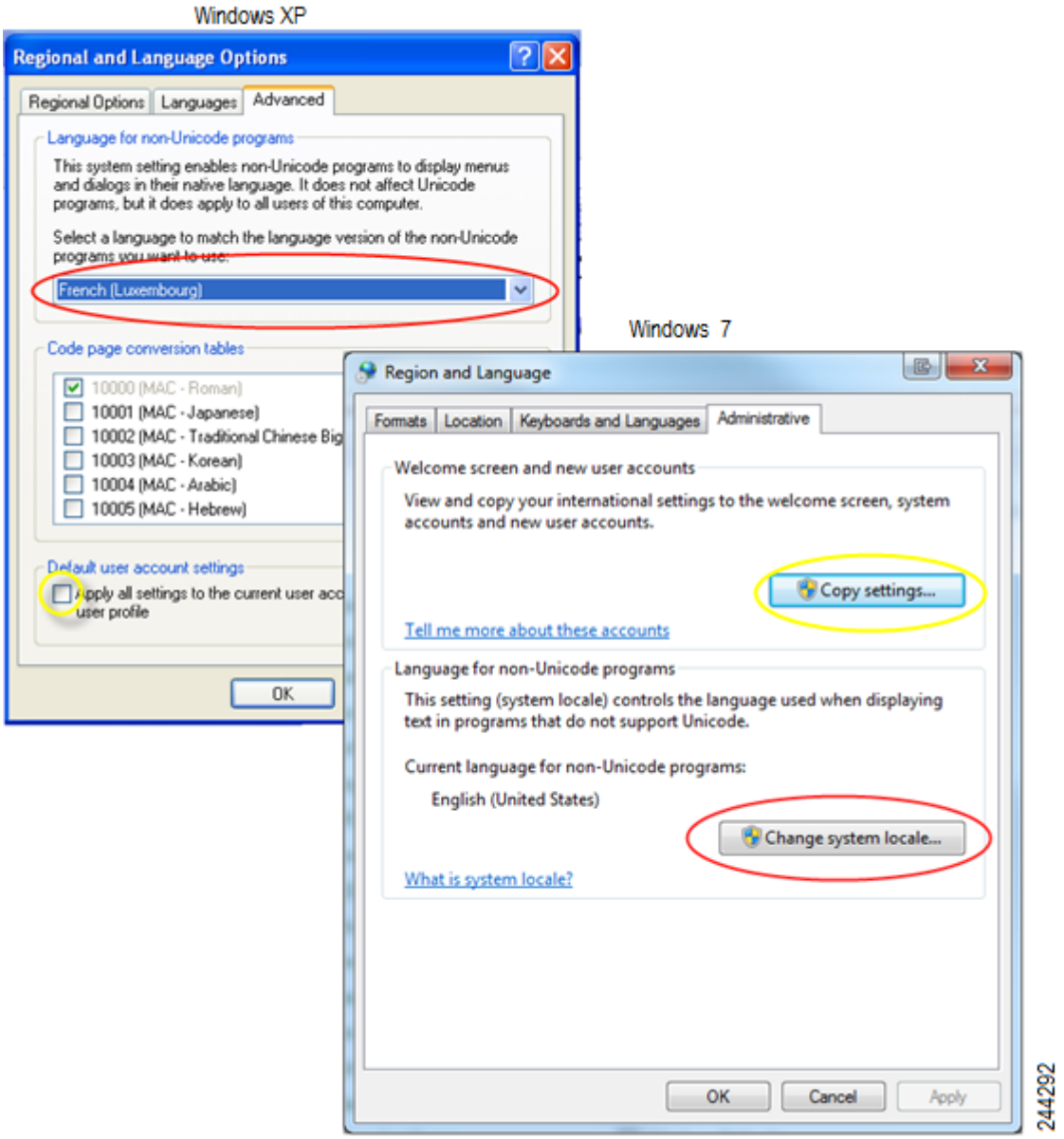
（注）　クライアントを ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのカタログ ユーティリティを使用して、手動で AnyConnect 変換テーブル（anyconnect.po）を .mo ファイルに変換し、その .mo ファイルをクライアント コンピュータの適切なフォルダにインストールします。詳細については、「ツールを使用した社内展開用メッセージ カタログの作成」（P.12-31）を参照してください。

AnyConnect クライアント プラットフォームのシステム ロケールの指定

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、AnyConnect がコンピュータの優先言語を検出し、指定されたシステム ロケールを検出して適切な変換テーブルを適用します。

Windows のクライアント プラットフォーム上で、指定したシステム ロケー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　[Control Panel] > [Region and Languages] ダイアログ ボックスに移動します。コントロール パネルをカテゴリ別に表示している場合は、[Clock]、[Language]、[Region] > [Change display language] の順に選択します。Windows XP および 7 のダイアログの例を次に示します。



ステップ 2　ご使用の Windows のバージョン向けに赤色の丸で囲まれたオプションを使用して、言語 / ロケールの設定を指定します。

ステップ 3　ご使用の Windows のバージョン向けに黄色の丸で囲まれたオプションを使用して、すべてのユーザ アカウントのデフォルトとしてこれらの設定を使用するように指定します。

ステップ 4　Web Security を使用して展開している場合、Web Security エージェントを再起動し、新しい翻訳内容を取得します。

（注）　場所が指定されていない場合、AnyConnect はデフォルトで言語のみに設定されます。たとえば、「fr-ca」ディレクトリが見つからないと、AnyConnect は「fr」ディレクトリを調べます。翻訳内容を表示するのに、表示言語、場所、またはキーボードを変更する必要はありません。

利用可能な変換テーブルの ASA へのインポート

ステップ 1　www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2　ASA で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [GUI Text and Messages]　の順に移動します。

ステップ 3　[Import] をクリックします。[Import Language Localization Entry] ウィンドウが表示されます。

ステップ 4　ドロップダウン リストから適切な**言語**を選択します。

ステップ 5　変換テーブルのインポート元を指定します。

ステップ 6　[Import Now] をクリックします。この変換テーブルが、この優先言語で AnyConnect クライアントに展開されます。ローカリゼーションは、AnyConnect が再起動し、再接続した後に適用されます。

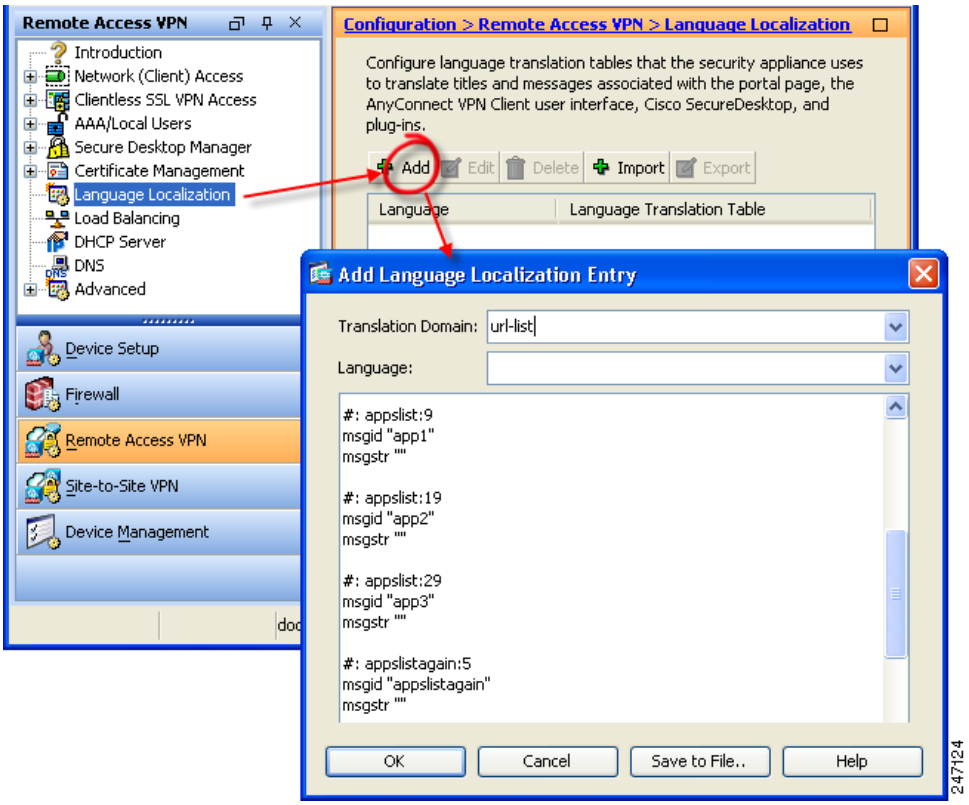
（注）　Cisco Secure Desktop を使用しない場合でも、ホスト スキャン メッセージをローカライズするには、Cisco Secure Desktop の変換テーブルも ASA にインポートする必要があります。

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。

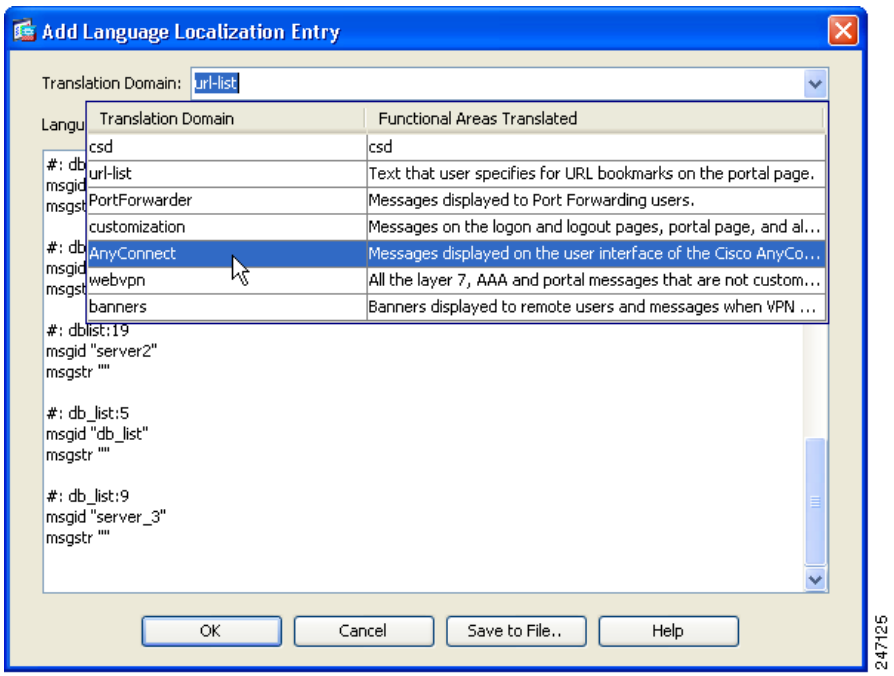
ステップ 1　[Configuration] > [Remote Access VPN] > [Language Localization] の順に選択します。[Add] をクリックします。[Add Language Localization Entry] ウィンドウが表示されます（図 12-9）。

図 12-9　[Language Localization] ペイン



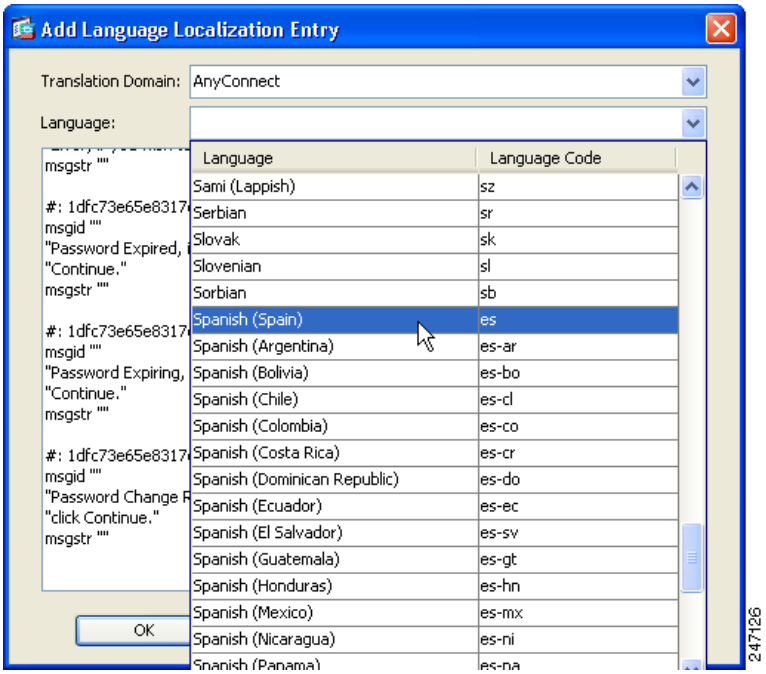
ステップ 2　[Translation Domain] ドロップ リストをクリックし、[AnyConnect] を選択します（図 12-10）。これによって、AnyConnect GUI 関連のメッセージだけが編集用に表示されます。

図 12-10　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 12-11）。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 12-11　言語の選択

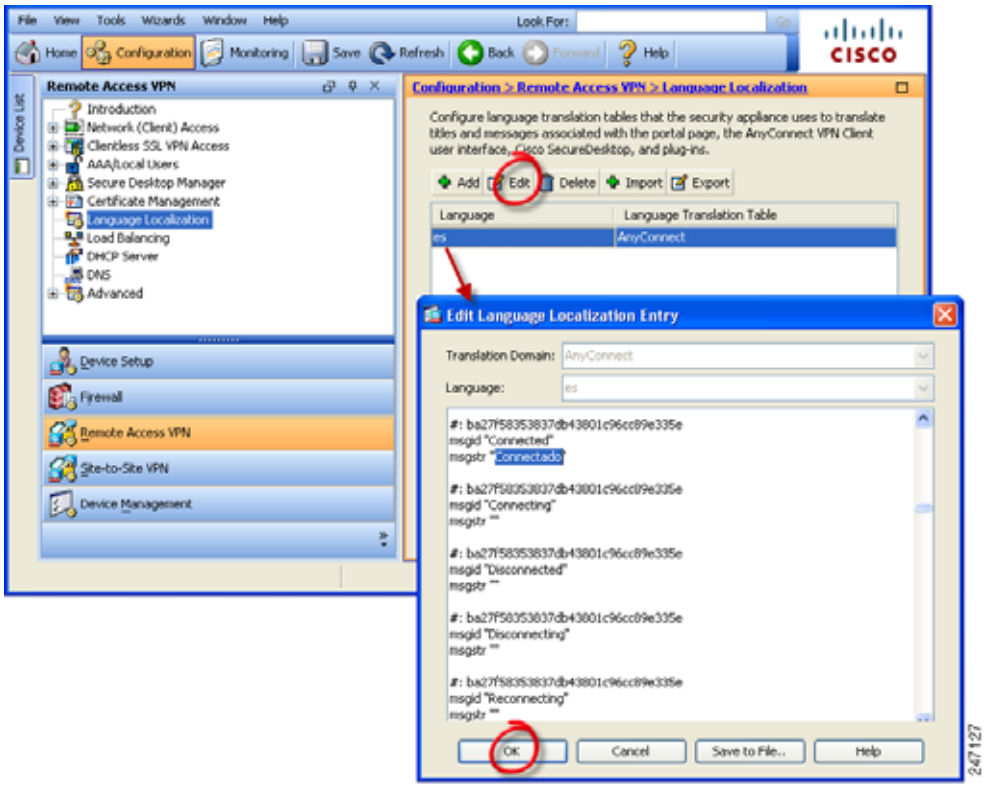


ステップ 4　変換テーブルが、ペインの言語リストに表示されます（この例では *es*）。ただし、翻訳されたメッセージはありません。翻訳されたテキストの追加を開始するには、[Edit] をクリックします。[Edit Language Localization Entry] ウィンドウが表示されます（図 12-12）。

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、[Language Localization] ペインで [Apply] をクリックして変更を保存します。

図 12-12　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

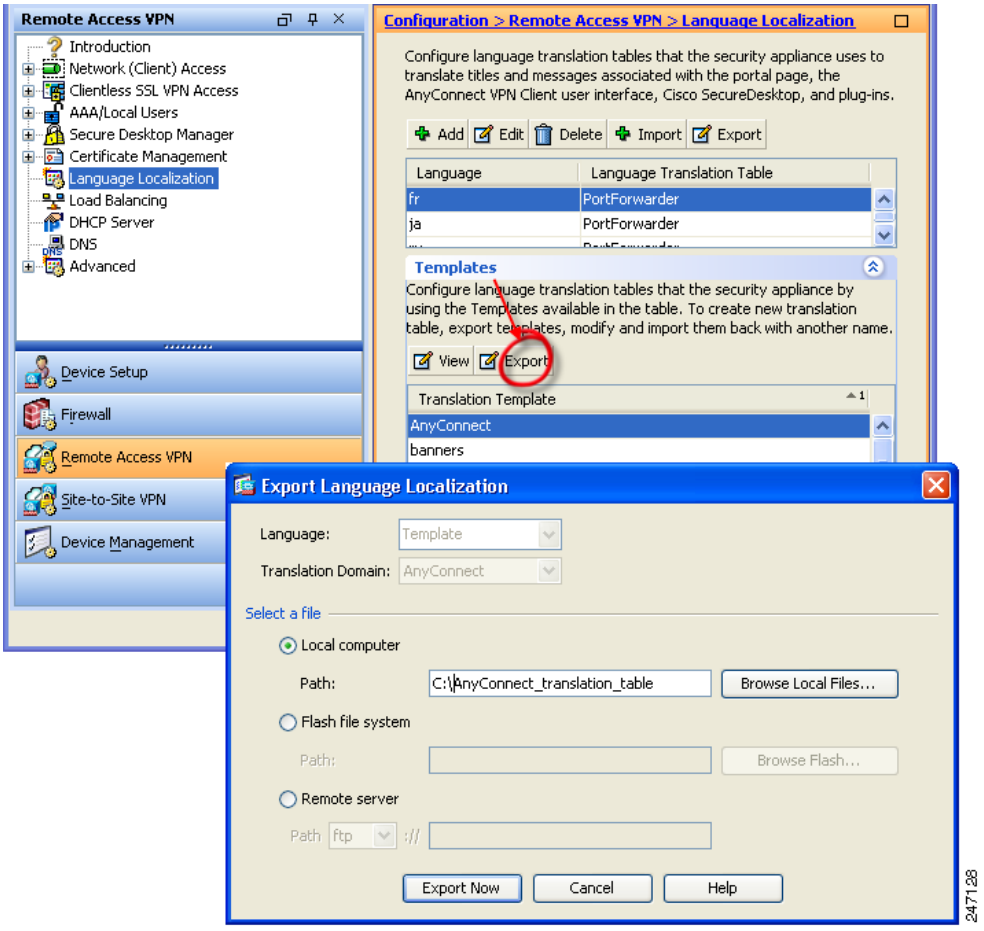
ここでは、AnyConnect 翻訳テンプレートをリモート コンピュータにエクスポートしてから、テキスト エディタや、Gettext または Poedit などのサードパーティ製ツールを使用して変換テーブルを編集する手順について説明します。

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。

[Configuration] > [Remote Access VPN] > [Language Localization] の順に選択します。[Language Localization] ペインが表示されます（図 12-13）。[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、[Export] をクリックします。[Export Language Localization] ウィンドウが表示されます。

図 12-13　翻訳テンプレートのエクスポート



ステップ 2　エクスポートの宛先を選択し、ファイル名を指定します。図 12-13 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。

[Configuration] > [Remote Access VPN] > [Language Localization] の順に選択します。[Language Localization] ペインが表示されます（図 12-14）。[Import] をクリックします。[Import Language Localization] ウィンドウが表示されます。

ステップ 5　[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　[Translation Domain] として *AnyConnect* を指定し、インポート先を選択して、ファイル名を指定します。[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。

[Apply] をクリックし、変更を必ず保存してください。

図 12-13 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 12-15 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 12-14　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

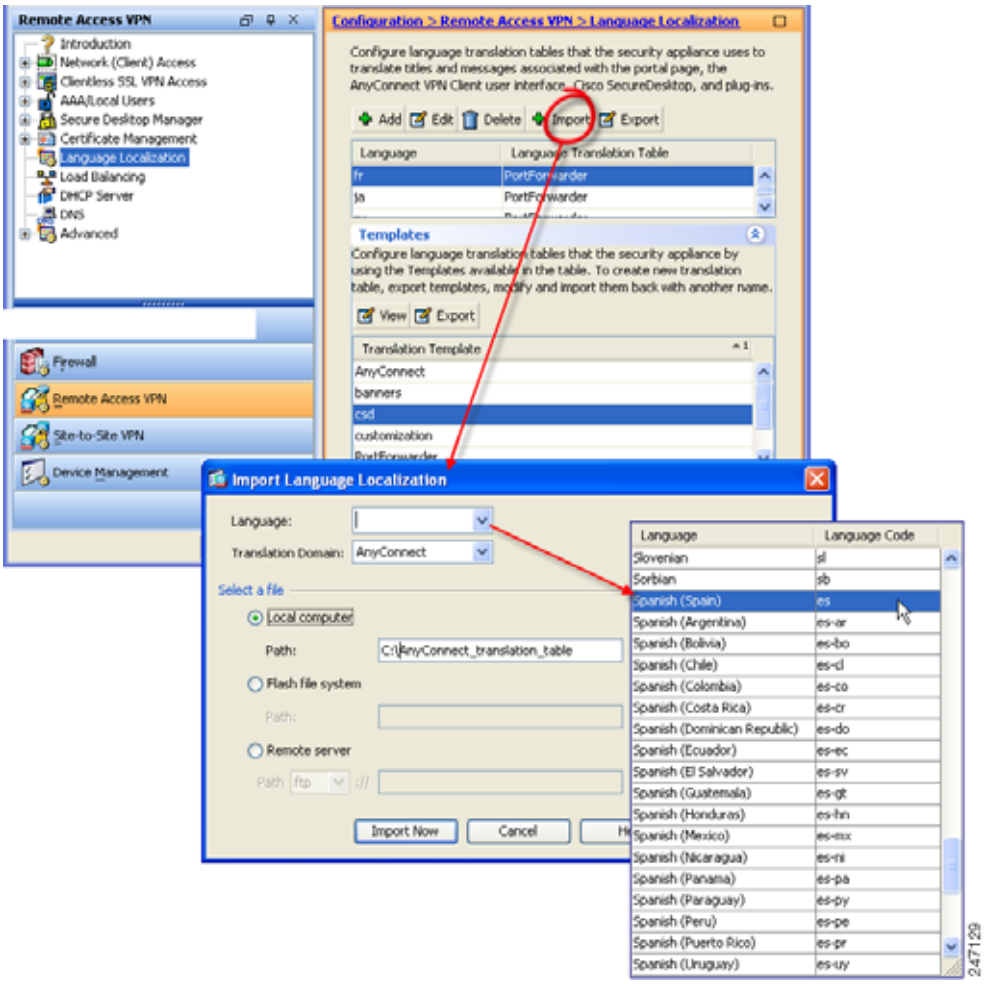
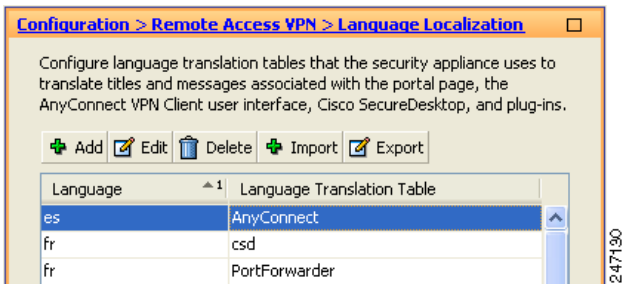


図 12-15　言語テーブルに表示された新しい言語



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（3.1.xxxxx 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 ソフトウェア開発キット（SDK）の一部であり、これは 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.

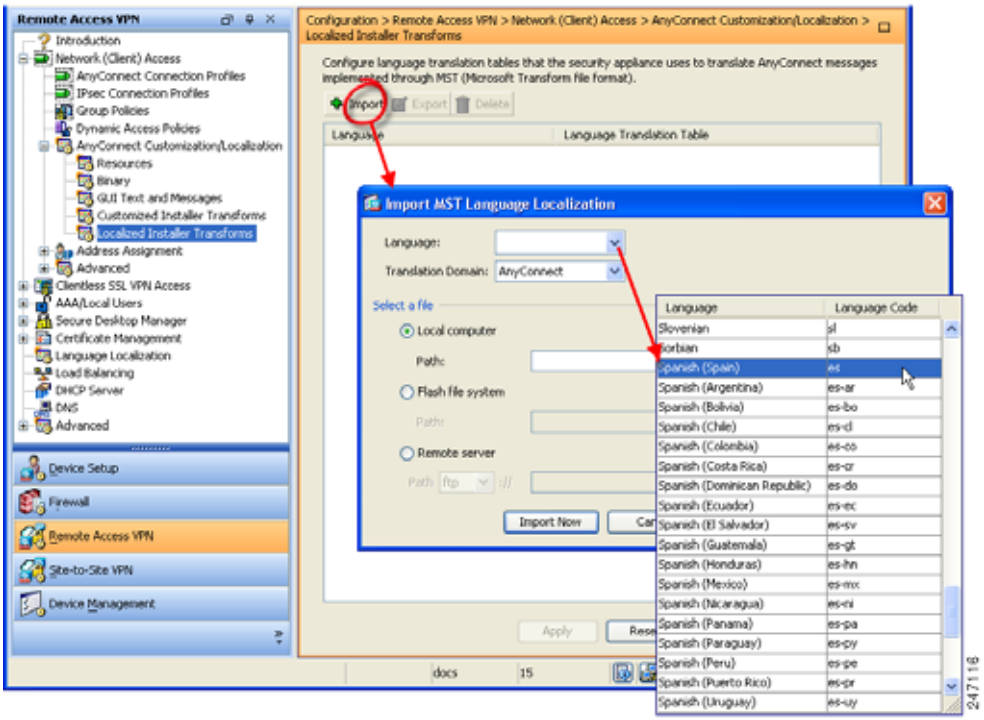
SDK をインストールすると、Orca MSI は、次の場所に格納されます。

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。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Customization/Localization] > [Localized Installer Transforms] の順に選択します。[Import] をクリックします。[Import MST Language Localization] ウィンドウが表示されます（図 12-16）。

図 12-16　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



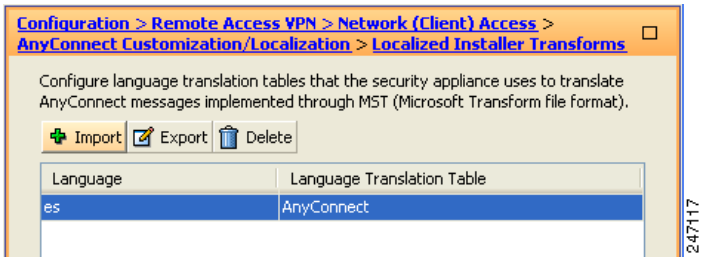
ステップ 2　[Language] ドロップダウン リストをクリックして、このトランスフォーム用の言語（および業界で認められている略称）を選択します。手動で略称を入力する場合は、ブラウザおよびオペレーティング システムが認識できる略称を使用してください。

ステップ 3　[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。

[Apply] をクリックし、変更を必ず保存してください。

図 12-16 では、言語に *Spanish* (es) を指定しています。図 12-17 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 12-17　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　[Remote Access VPN] > [Language Localization] > [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、[File] > [Open] > <AnyConnect.po> の順に選択します。
次に、[Catalog] > [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、[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　統合した変換テーブルを [Remote Access VPN] > [Language Localization] にインポートします。[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 13

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

Cisco AnyConnect Secure Mobility Client 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 **vpn-sessiondb logoff anyconnect** コマンドを使用します。

vpn-sessiondb logoff anyconnect

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 anyconnect
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 イメージの順に付与）は、どちらも **show vpn-sessiondb anyconnect** コマンドの出力に表示されます。

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

管理者またはユーザは、現在の AnyConnect セッションの統計情報を表示できます。Windows で、[Advanced Window] > [VPN drawer] > [Statistics] に移動します。または、Linux では、ユーザ GUI 上の [Details] ボタンをクリックします。

[Statistics Details] ダイアログが表示されます。このウィンドウの [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 コンピュータ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 [(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。

- [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。
- [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。
- [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.13-4）を参照してください。

Windows Mobile デバイスでの統計情報の表示

Windows Mobile デバイスの AnyConnect ユーザも、画面右下の [Menu] をクリックし、表示されたメニューから希望する機能を選択すると、統計情報の詳細のエクスポート機能とロギング機能を使用できます。

[Logging] をクリックすると、ロギング設定ダイアログボックスが開きます。

このダイアログボックスのスライダを動かして、ログ ファイルの総数と各ログ ファイルのサイズを制御したり、タスクの実行タイミングをイネーブルにしたりします。

[Browse Logs] をクリックすると、別のブラウザ ウィンドウにログ メッセージの HTML リストが表示されます。

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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] の順に選択します。

[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　[Advanced] > [SSL VPN Client] の順に選択します。

ステップ 3　[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。

圧縮の排除による VPN パフォーマンスの向上と Windows Mobile 接続の許可

低帯域幅の接続では、圧縮によって転送されるパケットのサイズが削減され、ASA とクライアントとの間の通信パフォーマンスが向上します。デフォルトでは、ASA では、グローバル レベルと特定のグループまたはユーザの両方において、すべての SSL VPN 接続に対する圧縮がイネーブルになっています。ブロードバンド接続では、圧縮によってパフォーマンスが低下することがあります。

（注）　Windows Mobile 用の Cisco AnyConnect Secure Mobility Client は、圧縮をサポートしていません。

グローバル コンフィギュレーション モードから CLI コマンドの **compression anyconnect** コマンドを使用することによって、グローバルに圧縮を設定できます。

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 OS X v10.6、v10.7、v10.8、および Red Hat Enterprise Linux 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 コンピュータにプッシュできます。インストールされると、[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。

（注）　DART バンドルは、Mac OS X v10.6 のアーカイブ ユーティリティでは解凍されません。

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 13-1 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 13-1　ASA または事前展開用の DART ファイルまたはパッケージ ファイル名

DART	Web 展開ファイル名およびパッケージ（ダウンロード）	事前展開インストーラ
Windows	*リリース 3.0.3050 以降：* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	3.0.3050 よりも前のリリース： anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac OS X	*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.2-23）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 で動作するコンピュータ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（**anyconnect 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. [Configuration] をクリックしてから、[Remote Access VPN] > [Network (Client) Access] > [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、[Advanced] を展開し、[SSL VPN Client] をクリックします。

c. [SSL VPN Client] ダイアログボックスで、[Optional Client Modules to Download] オプションの [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、[Apply] をクリックします。

CLI を使用する場合は、**anyconnect modules value dart** コマンドを使用します。

（注）　あとで **anyconnect modules none** に変更したり、[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、[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.13-8）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 の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 Setup] ウィザードを起動します。

ステップ 3　初期画面で [Next] をクリックします。

ステップ 4　[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、[Next] をクリックします。

ステップ 5　[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　[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.13-8）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 の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 OS X デバイスへの DART の手動インストール

Mac OS X 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 の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　[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　[Continue] をクリックしてから、[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、[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、[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、**[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　[Statistics] タブをクリックしてから、ダイアログボックス下部の [Details] ボタンをクリックします。[Statistics Details] ダイアログボックスが表示されます。

ステップ 3　[Statistics Details] ウィンドウ下部の [Troubleshoot] をクリックします。

ステップ 4　初期画面で [Next] をクリックします。[Bundle Creation Option] ダイアログボックスが表示されます。

ステップ 5　[Bundle Creation Option] エリアで、[Default] または [Custom] を選択します。

- [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。

  [Default] を選択してから、ダイアログボックス下部の [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。

- [Custom] を選択した場合は、[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　[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、[Encryption Option] エリアで [Enable Bundle Encryption] にチェックを入れてから、[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 [Mask Password] を選択すると、[Encryption Password] フィールドおよび [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　[Next] をクリックします。[Default] を選択した場合、DART はバンドルの作成を開始します。[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　[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、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 9　[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、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 10　[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。

- [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。
- [Target Bundle Location] フィールドで、バンドルの保存場所を参照します。

[Next] をクリックします。

ステップ 11　[Summary] ダイアログボックスでカスタマイズの内容を確認し、[Next] をクリックしてバンドルを作成するか、[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、[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、[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 OS X 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、[Applications] > [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、[Applications] > [Cisco] > [Cisco DART] から DART を起動します。

ステップ 2　[Statistics] タブをクリックしてから、ダイアログボックス下部の [Details] ボタンをクリックします。[Statistics Details] ダイアログボックスが表示されます。

ステップ 3　[Bundle Creation Option] エリアで、[Default] または [Custom] を選択します。

- [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。

  [Default] を選択してから、ダイアログボックス下部の [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 OS X 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。

- [Custom] を選択した場合は、[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　[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　[Next] をクリックします。[Default] を選択した場合、DART はバンドルの作成を開始します。[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　[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、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 6　[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、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 7　[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。

- [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。
- [Target Bundle Location] フィールドで、バンドルの保存場所を参照します。

[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、[Encryption Option] エリアで [Enable Bundle Encryption] にチェックを入れてから、[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 [Mask Password] を選択すると、[Encryption Password] フィールドおよび [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 OS X 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　[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、[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

anyconnect image xyz コマンドを使用して AnyConnect イメージを設定する場合、**anyconnect 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 anyconnect** 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 7 および Windows Vista
- \Windows\Inf\setupapi.dev.log：Windows 7 および Windows Vista

（注）　Windows 7 および Windows Vista では、非表示のファイルを表示に切り替える必要があります。

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　[Start] > [Run] の順にクリックします。

ステップ 2　[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　[Edit DWORD Value] ウィンドウの [Base] ペインで [Hexadecimal] を選択します。

ステップ 5　[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-3.X.xxxxx-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-3.X.xxxxx-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-3X.xxxx-pre-deploy-k9.msi/lvx* c:\AnyConnect.log

ここで、*anyconnect-win-3.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（Windows 7 および Windows 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.xxxxx-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.xxxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxxx-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.xxxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

（注）　*x.x.xxxxx* 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、anyconnect、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 anyconnect 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 コンピュータの 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. [Start] > [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、[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 コンピュータ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（Linux および Mac OS X）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。

32 ビットの Windows：DWORD レジストリは次のようにならなければなりません。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```

64 ビットの Windows：DWORD レジストリは次のようにならなければなりません。

```
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```

Linux または Mac OS X では、**sudo touch** コマンドを使用して次のパスの中にファイルを作成します。

```
/opt/cisco/anyconnect/debugroutes
```

（注） トンネル接続が開始されると、キーまたはファイルは削除されます。デバッグをイネーブルにするには、ファイルまたはキーが存在するだけで十分なので、キーの値またはファイルの内容は重要ではありません。

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 anyconnect 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 Client] > [Statistics] > [Details] > [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 anyconnect 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　[Start] > [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 コンピュータで [Start] > [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）[Applications and Services Logs] で **Cisco AnyConnect VPN Client** を見つけ、[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 [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、競合メッセージに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、[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。

コンピュータのシステム情報の取得

コンピュータ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.13-4）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　一部のコンピュータに 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. [Tools] > [Settings] > [Acceleration] > [Startup] から AT&T Communications Manager を起動します。
3. **manual** と入力します。
4. [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. [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、[Advanced Tasks] > [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、コンピュータはイーサネット 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。

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　[Protocol Filtering] > [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 access protection] > [HTTP, HTTPS] の順に選択し、[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、[Protocol filtering] > [SSL] に戻り、[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 [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コンピュータのネットワーク 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 コンピュータで 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。

APPENDIX A

VPN XML リファレンス

AnyConnect 3.1、3.0、または 2.5 および ASDM 6.3(1) 以降を使用している場合、このリファレンスは必要ありません。ASDM から起動されたプロファイル エディタまたは Cisco.com からダウンロードできるスタンドアロン 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編集します。詳細については、「AnyConnect クライアント プロファイルの概要」（P.2-1）を参照してください。

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。

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 プロキシ接続を有効にします。
	false	ローカル プロキシ接続を無効にします。

例：ローカル プロキシ接続の無効

ローカル プロキシ接続の AnyConnect サポートを無効にするには、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 が有効になります。
	false	デフォルトで OGS が無効になります。
EnableAutomaticServerSelection UserControllable	true	ユーザがクライアント設定で OGS を有効または無効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 （続き）

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 が有効のときは、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 を有効にします。*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 を無効にします。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。
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、常時接続の VPN と互換性がありません。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。

表 A-3　Trusted Network Detection の設定 （続き）

XML タグ名	オプション	説明
TrustedDNSDomains	文字列	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	文字列	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>
```

常時接続の VPN および下位機能

常時接続の 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無効にします。

表 A-4 に、常時接続の 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　常時接続の VPN 設定

XML タグ名	オプション	説明
AutomaticVPNPolicy	true	自動 VPN ポリシーを有効にします。
	false	自動 VPN ポリシーを無効にします。
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。
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。

表 A-4　常時接続の VPN 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	常時接続の VPN を有効にします。
	false	常時接続の VPN を無効にします。
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	整数型	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	[Disconnect] ボタンを表示して、常時接続の 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	[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.3-32）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の 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。

常時接続の 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。この常時接続の VPN 例では、次の操作を実行します。

- [Disconnect] ボタンを有効にし（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の VPN

表 A-5 に、ロード バランシングと常時接続の 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の 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、常時接続の VPN が有効ではない場合に、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の 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 を有効にします。
	false	Start Before Logon を無効にします。
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>
```

Windows の証明書ストア

表 A-7 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-7　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-8 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-8　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）。
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-9 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-9　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。

表 A-9　SCEP プロトコル設定 （続き）

AutomaticSCEPHost	ASA\ 接続プロファイル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\ 接続プロファイル名の 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。
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

表 A-10 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-10　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-10　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-10　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-10　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）。ワイルドカードを有効にすると、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無効になっています。

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有効にするには、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-11 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-11　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-12 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-12　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-13 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。

表 A-13　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	"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。 "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-14 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-14　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-15 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-15　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>
    true
</AutoReconnect>

<AutoReconnect UserControllable=”true”>true
<AutoReconnectBehavior
UserControllable=”true”>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

サーバ リスト

表 A-16 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-16　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 の子属性。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、一部の機能が無効になります。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 の機能が無効になることに注意してください。

表 A-16　サーバ リストの設定 （続き）

XML タグ名	オプション	説明
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。
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-17 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-17　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、有効または無効にできます。
	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、スクリプトを有効にし、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-18 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-18　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-19 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-19　プロキシの無視の設定

XML タグ名	オプション	説明
ProxySettings	IgnoreProxy	プロキシの無視を有効にします。
	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-20 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-20　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-21 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-21　L2TP または PPTP を介した AnyConnect

XML タグ名	オプション	説明
PPPExclusion	automatic	PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
	override	これも、PPP 除外を有効にします。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.3-79）の手順に従ってください。
	disabled	PPP 除外を適用しません。

表 A-21　L2TP または PPTP を介した AnyConnect （続き）

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：L2TP または PPTP を介した AnyConnect

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-22 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-22　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、このオプションが有効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-22　その他の AnyConnect プロファイル設定 （続き）

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有効のとき、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
Telemetry	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 サービスを有効または無効にします	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有効になります	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 機能の有効	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>
```

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/