CHAPTER 6

Web セキュリティの設定

AnyConnect Web セキュリティ モジュールは、ScanSafe Web スキャニング サービスが評価する ScanSafe スキャニング プロキシに HTTP トラフィックをルーティングするエンドポイント コンポーネントです。

ScanSafe Web スキャニング サービスは、Web ページの各要素を同時に分析できるように、これらの要素を分解します。たとえば、特定の Web ページが HTTP、Flash、および Java 要素の組み合わせである場合、別個の「scanlets」がこれらの各要素を並行して分析します。ScanSafe Web スキャニング サービスは、ScanCenter 管理ポータルに定義されたセキュリティ ポリシーに基づいて、良性または受け入れ可能なコンテンツを許可し、悪意のあるか受け入れられないコンテンツをドロップします。これは、少数のコンテンツが許容されないために Web ページ全体が制限される「過剰ブロック」、または依然として許容されないか場合によっては有害なコンテンツがページで提供されるのにページ全体が許可される「不十分なブロック」を防止します。ScanSafe Web スキャニング サービスは、ユーザが企業ネットワーク上に存在する場合も存在しない場合もユーザを保護します。

多数の ScanSafe スキャニング プロキシが世界各国に普及することで、AnyConnect Web セキュリティを活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い ScanSafe スキャニング プロキシにトラフィックをルーティングできます。

社内 LAN 上にあるエンドポイントを特定するよう、ビーコン サーバの 1 つ以上のインスタンスを設定できます。これは、「Detect-On-LAN」機能です。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。ビーコン サーバは、企業の一意の公開 / 秘密キー ペアを使用して、正しい公開キーを持つ Cisco ScanSafe Web セキュリティの顧客のみが、ネットワークへの接続中に ScanSafe スキャニング プロキシをバイパスできるようにしています。ネットワークにビーコン サーバの複数のインスタンスを展開する場合、各インスタンスは同一の公開 / 秘密キー ペアを使用する必要があります。

AnyConnect Web セキュリティ機能は、AnyConnect のプロファイル エディタを使用して編集する AnyConnect Web セキュリティ クライアント プラットフォームを使用して設定されます。

ScanCenter は、ScanSafe Web スキャニング サービスの管理ポータルです。ScanCenter を使用して作成または設定されたコンポーネントの一部は、AnyConnect Web セキュリティ クライアント プロファイルにも組み込まれています。

次の項では、AnyConnect Web セキュリティ クライアント プロファイルと機能、およびこれらの設定方法について説明します。

- AnyConnect Web セキュリティ クライアント プロファイルの作成
- クライアント プロファイルでの ScanSafe スキャニング プロキシの設定
- Web スキャニング サービスからのエンドポイント トラフィックの除外
- Web スキャニング サービス プリファレンスの設定
- ビーコン サーバのインストール
- 認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信
- Web セキュリティ クライアント プロファイル ファイル
- スタンドアロン Web セキュリティ クライアント プロファイルのインストール
- Web セキュリティ トラフィックのスプリットトンネリングの設定
- Web セキュリティ クライアント プロファイルの ScanCenter ホステッド コンフィギュレーション サポートの設定
- Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化

最初に AnyConnect Web セキュリティ クライアント プロファイルの作成によって AnyConnect Web セキュリティを設定できます。

システム要件

次に、AnyConnect Web セキュリティ モジュールのシステム要件を示します。

- AnyConnect Web セキュリティ モジュール
- ASA と ASDM に関する要件
- ビーコン サーバの要件

AnyConnect Web セキュリティ モジュール

Web セキュリティでは、次のオペレーティング システムがサポートされます。

- Windows XP SP3 x86（32 ビット）
- Windows Vista x86（32 ビット）または x64（64 ビット）
- Windows 7 x86（32 ビット）または x64（64 ビット）
- OS X v10.5 x86（32 ビット）
- Mac OS X v10.6 x86（32 ビット）または x64（64 ビット）
- Mac OS X v10.7 x86（32 ビット）または x64（64 ビット）

ASA と ASDM に関する要件

AnyConnect Secure Mobility Client を Web セキュリティ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4(1)
- ASDM 6.4(0)104

ビーコン サーバの要件

ビーコン サーバは、次のオペレーティング システムでサポートされます。

- Windows Server 2003 R1 x86（32 ビット）または x64（64 ビット）
- Windows Server 2003 R2 x86（32 ビット）または x64（64 ビット）
- Windows Server 2008 R1 x86（32 ビット）または x64（64 ビット）
- Windows Server 2008 R2 x64（64 ビット）

システムの制限

Web セキュリティを実行するユーザは、Anywhere Plus も実行することはできません。Web セキュリティをインストールする前に、Anywhere Plus を削除する必要があります。

ライセンス要件

次の項では、AnyConnect Web セキュリティ モジュールのさまざまな導入方法のライセンス要件について説明します。

- 「スタンドアロン コンポーネントとして導入された Web セキュリティ」（P.6-3）
- 「AnyConnect のコンポーネントとして導入された Web セキュリティ」（P.6-3）

スタンドアロン コンポーネントとして導入された Web セキュリティ

Web セキュリティ モジュールを導入して、ASA をインストールしたり、AnyConnect Secure Mobility Client の VPN 機能をイネーブルにしたりすることなく、ScanSafe Web スキャニング サービスの利点を得ることができます。

ScanSafe Web スキャニング サービスでローミング ユーザを保護するには、ScanSafe Web Filtering や ScanSafe Malware Scanning のライセンスに加えて、引き続き Secure Mobility for ScanSafe ライセンスが必要です。

（注）　Web セキュリティ モジュールのみとともに AnyConnect Secure Mobility Client を使用する場合、AnyConnect Essentials または AnyConnect Premium のライセンスは不要です。

AnyConnect のコンポーネントとして導入された Web セキュリティ

AnyConnect ライセンス

Web セキュリティに固有の AnyConnect ライセンスはありません。Web セキュリティ モジュールは、AnyConnect Essentials または AnyConnect Premium にいずれかとともに機能します。

ScanCenter ライセンス

ScanSafe Web スキャニング サービスでローミング ユーザを保護するには、ScanSafe Web Filtering や ScanSafe Malware Scanning のライセンスに加えて、Secure Mobility for ScanSafe ライセンスが必要です。

IPv6 Web トラフィックでの Web セキュリティの動作に関するユーザ ガイドライン

IPv6 アドレス、ドメイン名、アドレス範囲、またはワイルド カードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。ここで DNS ルックアップが実行され、ユーザがアクセスしようとしている URL に IPv4 アドレスがあるかどうかが確認されます。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合は、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスするように設定する場合は、すべての IPv6 トラフィック **::/0** にこの静的な例外を追加します。つまり、この場合は IPv6 トラフィックは Web セキュリティで保護されません。

ASA とともに使用するための AnyConnect Web セキュリティ モジュールのインストール

Web セキュリティ モジュールは、AnyConnect とともに導入する場合、またはスタンドアロン モジュールとして導入する場合、クライアント プロファイルを必要とします。

ステップ 1　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。

ステップ 2　Web 導入および事前導入の方法を使用した Web セキュリティ モジュールのインストールに関する手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を読んでください。

ASA なしで使用するための AnyConnect Web セキュリティ モジュールのインストール

Web セキュリティ モジュールをスタンドアロン アプリケーションとして導入して、AnyConnect VPN モジュールをイネーブルにせずに、ASA なしで ScanSafe ScanCenter とともに使用できます。ここでは次の内容について説明します。

- AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストール
- AnyConnect インストーラを使用した Mac OS X への Web セキュリティ モジュールのインストール

（注）　Windows が実行されているコンピュータでは、AnyConnect がユーザ ID を判別できない場合、内部 IP アドレスがユーザ ID として使用されます。たとえば、これは、enterprise_domains プロファイル エントリが指定されていない場合に発生する可能性があります。その場合、ScanCenter でレポートを生成するために、内部 IP アドレスを使用する必要があります。

Mac OS X が実行されているコンピュータでは、Mac がドメインにバインドされている場合、Web セキュリティ モジュールは、コンピュータがログインしているドメインを報告できます。ドメインにバインドされていない場合、Web セキュリティ モジュールは、Mac の IP アドレスまたは現在ログインしているユーザ名を報告できます。

AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストール

この手順では、ScanSafe とともに使用するために Windows OS で Cisco AnyConnect Secure Mobility Client Web セキュリティ モジュールを設定する方法について説明します。大まかには、次のタスクを実行します。

1. Cisco AnyConnect Secure Mobility Client ISO イメージをダウンロードします。
2. ISO ファイルの内容を抽出します。
3. スタンドアロン プロファイル エディタをインストールし、Web セキュリティ プロファイルを作成して、Web セキュリティ プロファイル ファイルを ISO ファイルの抽出済みの内容に追加することによって、Web セキュリティ モジュールをカスタマイズします。
4. カスタマイズ済みの Web セキュリティ モジュールをインストールします。

ScanSafe とともに使用するために Windows OS で Cisco AnyConnect Secure Mobility Client Web セキュリティ モジュールを設定するには、次の手順を実行します。

ステップ 1　ScanCenter サポート エリアまたは Cisco.com から Cisco AnyConnect Secure Mobility Client パッケージをダウンロードします。

ステップ 2　新しいディレクトリを作成します。

ステップ 3　WinZip や 7-Zip などのアプリケーションを使用して、ISO ファイルの内容を、新たに作成したディレクトリに抽出します。

（注）　この時点では Web セキュリティ モジュールをインストール**しないで**ください。

ステップ 4　スタンドアロンの AnyConnect プロファイル エディタをインストールします。詳細については、「スタンドアロン AnyConnect プロファイル エディタのインストール」（P.2-44）を参照してください。

（注）　デフォルトでは、Web セキュリティのプロファイル エディタ コンポーネントはインストールされていません。カスタム インストールの一部として選択するか、完全なインストールを選択する必要があります。

ステップ 5　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ プロファイル エディタを起動してプロファイルを作成します。

ステップ 6　プロファイルに **WebSecurity_ServiceProfile.xml** という名前を付けて安全な場所に保存します。

Web セキュリティ プロファイル エディタにより、**WebSecurity_ServiceProfile.wso** という名前のプロファイルの難読化バージョンが追加作成され、WebSecurity_ServiceProfile.xml ファイルと同じ場所に保存されます。

ステップ 7　WebSecurity_ServiceProfile.wso という難読化バージョンの Web セキュリティ プロファイルを、ステップ 3 で抽出した **Profiles\websecurity** フォルダにコピーします。

ステップ 8　**Setup.exe** を開始して、クライアント ソフトウェアをインストールします。

ステップ 9　[Cisco AnyConnect Secure Mobility Client インストール セレクタ（Cisco AnyConnect Secure Mobility Client Install Selector）] で、次のようにします。

- [AnyConnect Web セキュリティ モジュール（AnyConnect Web Security Module）] チェックボックスがオンになっていることを確認します。
- [Cisco AnyConnect VPN モジュール（Cisco AnyConnect VPN Module）] がオフになっていることを確認します。これでコア クライアントの VPN 機能がオフになり、インストール ユーティリティによって、ネットワーク アクセス マネージャと Web セキュリティが、VPN 機能なしのスタンドアロン アプリケーションとしてインストールされます。
- （任意）[ロック ダウン コンポーネント サービス（Lock Down Component Services）] チェックボックスを選択します。ロックダウン コンポーネント サービスによって、ユーザは、Windows Web セキュリティ サービスをディセーブルまたは停止できなくなります。

ステップ 10　[選択した内容のインストール（Install Selected）] をクリックして、[OK] をクリックします。インストールが正常に完了したら、システム トレイに [Cisco AnyConnect Secure Mobility Client] アイコンが表示されます。

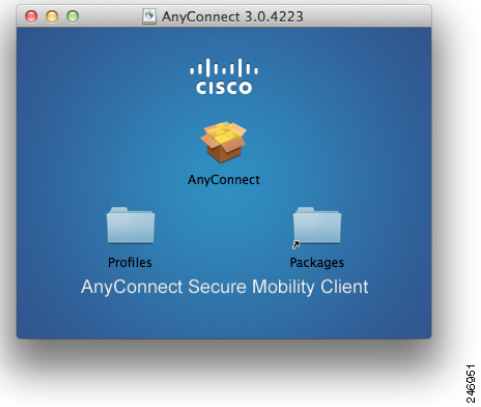
AnyConnect インストーラを使用した Mac OS X への Web セキュリティ モジュールのインストール

次の手順では、スタンドアロン プロファイル エディタをインストールして、Web セキュリティ プロファイルを作成し、その Web セキュリティ プロファイルを DMG パッケージに追加することによって、Web セキュリティ モジュールをカスタマイズする方法について説明します。

ステップ 1　ScanCenter サポート エリアまたは Cisco.com のダウンロード エリアから Cisco AnyConnect Secure Mobility Client DMG パッケージをダウンロードします。

ステップ 2　ファイルを開いて、インストーラにアクセスします（図 6-1）。ダウンロードしたイメージは読み取り専用ファイルです。

図 6-1　AnyConnect インストーラ イメージ



ステップ 3　**ディスク ユーティリティ**を実行するか、次のように**端末** アプリケーションを使用して、インストーラ イメージを書き込み可能にします。

```
Hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

ステップ 4　Windows オペレーティング システムが実行されているコンピュータにスタンドアロンの AnyConnect プロファイル エディタをインストールします。詳細については、「スタンドアロン AnyConnect プロファイル エディタのインストール」（P.2-44）を参照してください。

（注）　デフォルトでは、Web セキュリティのプロファイル エディタ コンポーネントはインストールされていません。カスタム インストールの一部として選択するか、完全なインストールを選択する必要があります。

ステップ 5　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ プロファイル エディタを起動してプロファイルを作成します。

ステップ 6　プロファイルに **WebSecurity_ServiceProfile.xml** という名前を付けて安全な場所に保存します。

Web セキュリティ プロファイル エディタにより、**WebSecurity_ServiceProfile.wso** という名前のプロファイルの難読化バージョンが追加作成され、WebSecurity_ServiceProfile.xml ファイルと同じ場所に保存されます。

ステップ 7　WebSecurity_ServiceProfile.wso ファイルを Windows マシンから **AnyConnect 3.0.5074/Profiles/websecurity** Mac OS X インストーラ パッケージにコピーします。

または、次のように**端末**アプリケーションを使用することもできます。

```
Copy WebSecurity_ServiceProfile.wso
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

ステップ 8　Mac OS X インストーラで、**AnyConnect 3.0.5074/Profiles** ディレクトリに移動し、TextEdit で **ACTransforms.xml** ファイルを開いてファイルを編集します。VPN 機能がインストールされないように、<DisableVPN> 要素を **True** に設定します。

```
<ACTransforms>
    <DisableVPN>True</DisableVPN>
</ACTransforms>
```

ステップ 9　Cisco.com の AnyConnect Secure Mobility Client **3.0.4235** のダウンロード エリアで、**VPNDisable_ServiceProfile.xml** ファイルを見つけて、AnyConnect Web セキュリティをインストールするコンピュータにダウンロードします。

ステップ 10　**VPNDisable_ServiceProfile.xml** ファイルを AnyConnect インストーラの **AnyConnect 3.0.5074/profiles/vpn** ディレクトリに保存します。

（注）　AnyConnect 3.0.4235 用の Web セキュリティ モジュールのみを Mac OS X にインストールする場合、AnyConnect ユーザ インターフェイスは、ブートアップ時に自動的に起動するよう設定する必要があります。これによって、AnyConnect は、Web セキュリティ モジュールに必要なユーザおよびグループ情報を指定できるようになります。手順 9 および 10 では、ブート時に AnyConnect ユーザ インターフェイスを自動的に起動できるようにする正しい設定を指定します。

ステップ 11　これで、AnyConnect DMG パッケージをユーザに配布する準備ができました。

コマンドライン インストールを使用した Windows OS への Web セキュリティ モジュールのインストール

コマンド プロンプトから Web セキュリティ モジュールをインストールするには、次の手順を実行します。

ステップ 1　AnyConnect インストーラを使用した Windows OS への Web セキュリティ モジュールのインストールのステップ 1 ～ステップ 6 に従います。

ステップ 2　VPN 機能をオフにして AnyConnect Secure Mobility Client VPN モジュールをインストールします。

```
msiexec /package anyconnect-win-<version>-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* c:\test.log
```

ステップ 3　Web セキュリティ モジュールをインストールします。

```
msiexec /package anyconnect-websecurity-win-<version>-pre-deploy-k9.msi /norestart
/passive /lvx* c:\test.log
```

ステップ 4　（任意）DART をインストールします。

```
misexec /package annyconnect-dart-win-<version>-k9.msi /norestart /passive /lvx*
c:\test.log
```

ステップ 5　難解化 Web セキュリティ クライアント プロファイルのコピーを、表 2-15（P.2-42）で定義した正しい Windows フォルダに保存します。

ステップ 6　「Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化」（P.6-42）の手順に従って、Cisco AnyConnect Web セキュリティ エージェント Windows サービスを再起動します。

（注）　これらのコマンドは、Systems Management Server（SMS）の導入にも使用できます。

AnyConnect Web セキュリティ クライアント プロファイルの作成

AnyConnect Web セキュリティ クライアント プロファイルを作成するには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Accessess）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。
- Windows OS のスタンドアロン モードで、[スタート（Start）] > [プログラム（Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択します。

ステップ 2　[追加（Add）] をクリックしてクライアント プロファイルを作成します。

ステップ 3　クライアント プロファイルの**名前**を指定します。

ステップ 4　[プロファイルの使用（Profile Usage）] フィールドをクリックして、[Web セキュリティ（Web Security）] を選択します。

ステップ 5　デフォルトのプロファイルの場所を使用するか、[参照（Browse）] をクリックして代わりのファイルの場所を指定します。

ステップ 6　（任意）[グループ ポリシー（Group Policy）] を選択してクライアント プロファイルを添付するか、クライアント プロファイルを <Unassigned> のままにします。

ステップ 7　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

AnyConnect Web セキュリティ クライアント プロファイルを作成してある場合は、プロファイルの次の側面を設定する必要があります。

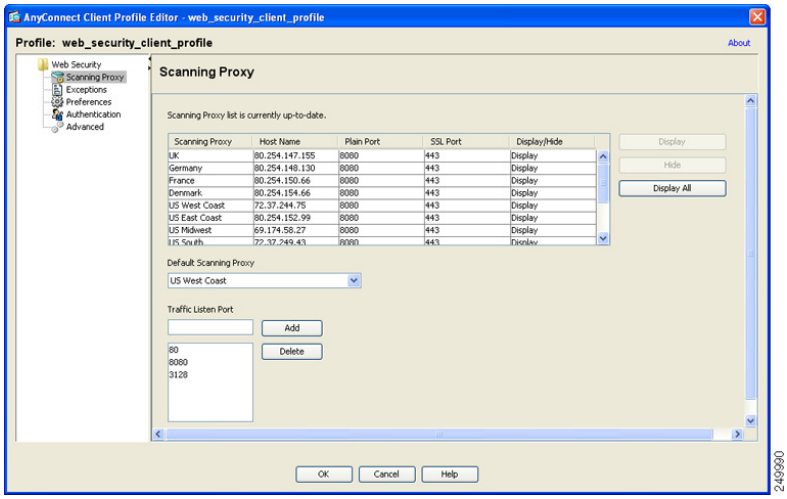
- 「クライアント プロファイルでの ScanSafe スキャニング プロキシの設定」（P.6-9）
- 「Web スキャニング サービスからのエンドポイント トラフィックの除外」（P.6-13）
- 「ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算」（P.6-16）
- 「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）
- 「認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信」（P.6-31）

AnyConnect Web セキュリティ クライアント プロファイルを作成して保存した後で、ASDM は、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルで、もう 1 つはプレーン テキスト形式です。これらのファイルの詳細については、「Web セキュリティ クライアント プロファイル ファイル」（P.6-36）を参照してください。

クライアント プロファイルでの ScanSafe スキャニング プロキシの設定

ScanSafe Web スキャニング サービスは Web コンテンツを分析します。これは、セキュリティ ポリシーに基づいてブラウザへの良性のコンテンツの配信を許可し、悪意のあるコンテンツをブロックします。スキャニング プロキシは、ScanSafe Web スキャニング サービスが Web コンテンツを分析する ScanSafe プロキシ サーバです。AnyConnect Web セキュリティ プロファイル エディタ内の [スキャン プロキシ（Scanning Proxy）] パネルは、AnyConnect Web セキュリティ モジュールによる Web ネットワーク トラフィックの送信先 ScanSafe スキャニング プロキシを定義します。

図 6-2　Web セキュリティ クライアント プロファイルの [スキャン プロキシ（Scanning Proxy）] パネル



AnyConnect Web セキュリティ クライアント プロファイルで ScanSafe スキャニング プロキシを定義するには、次の手順を使用します。

- 「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）
- 「スキャニング プロキシのユーザへの表示または非表示」（P.6-11）
- 「デフォルトのスキャニング プロキシの選択」（P.6-12）
- 「HTTP（S）トラフィック リスニング ポートの指定」（P.6-13）

スキャニング プロキシ リストの更新

Web セキュリティ プロファイル エディタのスキャニング プロキシ リストは編集不可能です。ScanCenter スキャニング プロキシを Web セキュリティ プロファイル エディタ内のテーブルで追加したり削除したりすることはできません。

Web セキュリティ プロファイル エディタを起動した後で、スキャニング プロキシの最新のリストが保持されている ScanCenter Web サイトにアクセスすることで、スキャニング プロキシ リストが自動的に更新されます。

AnyConnect Web セキュリティ クライアント プロファイルの追加または編集時に、プロファイル エディタは、ScanSafe スキャニング プロキシの既存のリストを、ScanSafe Web サイトからダウンロードしたスキャニング プロキシ リストと比較します。リストが古い場合は、「スキャン プロキシ リストは期限切れです（Scanning Proxy list is out of date）」というメッセージと、[リストの更新（Update List）] というラベルが付いたコマンド ボタンが表示されます。スキャニング プロキシ リストを、ScanSafe スキャニング プロキシの最新のリストで更新するには、[リストの更新（Update List）] ボタンをクリックします。

[リストの更新（Update List）] をクリックすると、プロファイル エディタによって、既存の設定が可能な限り保持されます。プロファイル エディタは、デフォルトのスキャニング プロキシ設定、および既存の ScanSafe スキャニング プロキシの表示または非表示設定を保存します。

Web セキュリティ クライアント プロファイルでのデフォルトのスキャニング プロキシ設定

デフォルトでは、作成するプロファイルには、次の ScanSafe スキャニング プロキシ属性があります。

- スキャニング プロキシ リストには、ユーザがアクセスできるすべての ScanSafe スキャニング プロキシが読み込まれ、すべて「Display」とマークされます。詳細については、「スキャニング プロキシのユーザへの表示または非表示」（P.6-11）を参照してください。
- デフォルトの ScanSafe スキャニング プロキシは事前選択されています。デフォルトの ScanSafe スキャニング プロキシを設定するには、「デフォルトのスキャニング プロキシの選択」（P.6-12）を参照してください。
- AnyConnect Web Security モジュールが HTTP トラフィックを受信するポートのリストは、いくつかのポートにプロビジョニングされます。詳細については、「HTTP（S）トラフィック リスニング ポートの指定」（P.6-13）を参照してください。

スキャニング プロキシのユーザへの表示または非表示

ユーザが ASA への VPN 接続を確立した後で、ASA は、クライアント プロファイルをエンドポイントにダウンロードします。AnyConnect Web セキュリティ クライアント プロファイルは、ユーザに表示される ScanSafe スキャニング プロキシを判別します。

ユーザは、次の方法で、AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ リストで「Display」とマークされたスキャニング プロキシと対話します。

- ScanSafe スキャニング プロキシは、Cisco AnyConnect Secure Mobility Client インターフェイスの [Web セキュリティ（Web Security）] パネルの [詳細（Advanced）] 設定のユーザに表示されます。
- AnyConnect Web セキュリティ モジュールは、応答時間でスキャニング プロキシを順序付ける際に、「Display」とマークされた ScanSafe スキャニング プロキシをテストします。
- ユーザは、自分のプロファイルでユーザ制御が許可される場合に接続する ScanSafe スキャニング プロキシを選択できます。
- AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ テーブルで「Hide」とマークされている ScanSafe スキャニング プロキシは、ユーザに表示されず、応答時間でスキャニング プロキシを順序付ける際に評価されません。ユーザは、「Hide」とマークされたスキャニング プロキシには接続できません。

（注） ローミング ユーザが最大の利点を得るには、すべての ScanSafe スキャニング プロキシをすべてのユーザに「表示」することをお勧めします。

ScanSafe スキャニング プロキシをユーザに非表示または表示するには、次の手順を実行します。

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

ステップ 2　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　ScanSafe スキャニング プロキシを非表示または表示するには、次の手順を実行します。

- **スキャニング プロキシを非表示にするには**、非表示にするスキャニング プロキシを選択して、[非表示（Hide）] をクリックします。

- **スキャニング プロキシを表示するには**、表示するスキャニング プロキシの名前を選択して、[表示（Display）] をクリックします。すべての ScanSafe スキャニング プロキシを表示する設定を推奨します。

ステップ 4　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

デフォルトのスキャニング プロキシの選択

デフォルトの ScanSafe スキャニング プロキシを定義するには、次の手順を実行します。

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

ステップ 2　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　[デフォルトのスキャン プロキシ（Default Scanning Proxy）] フィールドからデフォルトのスキャニング プロキシを選択します。

ステップ 4　AnyConnect Web セキュリティ クライアント プロファイルを保存します。

ユーザがスキャニング プロキシに接続する方法

1. ユーザが初めてネットワークに接続すると、デフォルトのスキャニング プロキシにルーティングされます。
2. その後、プロファイルの設定方法に応じて、ユーザはスキャニング プロキシを選択するか、AnyConnect Web セキュリティ モジュールが、応答時間が最も早いスキャニング プロキシにユーザを接続します。
   - ユーザのクライアント プロファイルでユーザ制御が許可される場合、ユーザは、Cisco AnyConnect Secure Mobility Client Web セキュリティ トレイの [設定（Settings）] タブからスキャニング プロキシを選択します。
   - クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] プリファレンスがイネーブルになっている場合、AnyConnect Web セキュリティは、スキャニング プロキシを速い順にして、応答時間が最も早いスキャニング プロキシにユーザを接続します。
   - クライアント プロファイルでユーザ制御が許可されなくても、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] がイネーブルになっているときは、AnyConnect Web セキュリティは、ユーザをデフォルトのスキャニング プロキシから、応答時間が最も早いスキャニング プロキシに切り替えます（応答時間が、最初に接続したデフォルトのスキャニング プロキシよりも大幅に早い場合）。
   - ユーザが、現在のスキャニング プロキシからローミングし始めたときに、クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が設定されていれば、AnyConnect Web セキュリティは、ユーザを新しいスキャニング プロキシに切り替えることがあります（応答時間が現在のスキャニング プロキシよりも大幅に早い場合）。

AnyConnect Web セキュリティでは、Windows の拡張された AnyConnect トレイ アイコン、AnyConnect GUI の [詳細設定（Advanced Settings）] タブ、および [統計情報詳細（Advanced Statistics）] タブにイネーブルになっているスキャニング プロキシ名が表示されるため、ユーザは接続先のスキャニング プロキシを確認できます。

HTTP（S）トラフィック リスニング ポートの指定

Scan Safe Web スキャニング サービスは、デフォルトで HTTP Web トラフィックを分析し、HTTPS Web トラフィックをフィルタリングするよう設定可能です。Web セキュリティ クライアント プロファイルで、Web セキュリティにこれらのタイプのネットワーク トラフィックを「受信」させるポートを指定できます。

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

ステップ 2　編集する AnyConnect Web セキュリティ クライアント プロファイルを選択して [Edit] をクリックします。Web セキュリティ プロファイル エディタが開き、[スキャン プロキシ（Scanning Proxy）] パネルが表示されます（図 6-2 を参照）。

ステップ 3　[トラフィック リスン ポート（Traffic Listen Port）] フィールドに、Web セキュリティ モジュールに HTTP または HTTPS トラフィックまたはその両方を「受信」させる論理ポート番号を入力します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

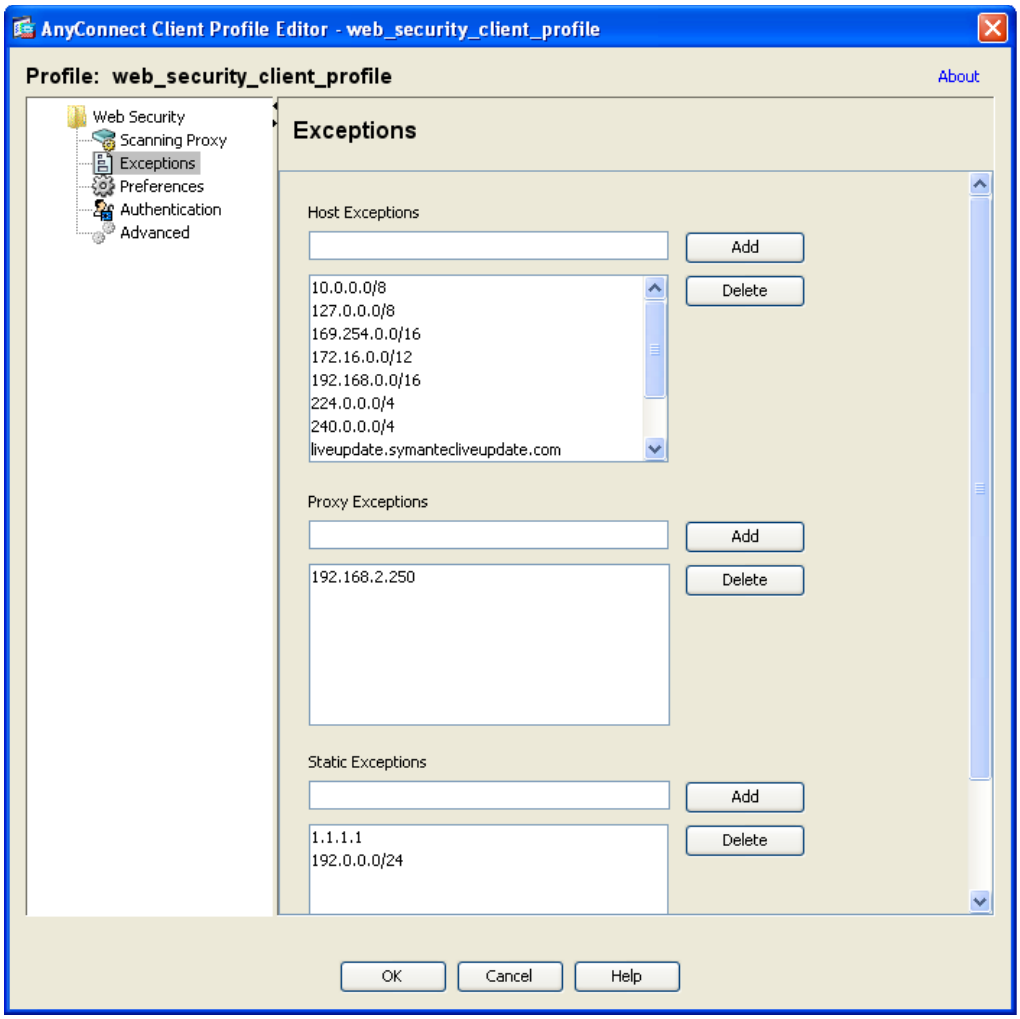
Web スキャニング サービスからのエンドポイント トラフィックの除外

特定の IP アドレスから発信されるネットワーク トラフィックを ScanSafe Web スキャニング サービスで評価しない場合、次のいずれかのカテゴリでそのアドレスの例外を設定できます。

- ホスト例外
- プロキシ例外
- 静的な例外

これらの除外は、Web セキュリティ プロファイル エディタの [除外（Exceptions）] パネルで設定します。図 6-3 を参照してください。

図 6-3　Web セキュリティ プロファイル エディタの [除外（Exceptions）] パネル



ホスト例外

[ホスト除外（Host Exceptions）] リストで、ScanSafe Web スキャニング サービスをバイパスする内部サブネットとパブリック Web サイトを追加します。[除外（Exceptions）] パネルの図については、図 6-3 を参照してください。

たとえば、デフォルトにまだ追加されていない、使用する内部サブネットを追加する必要があります。

```
192.0.2.0/8
```

直接アクセスをイネーブルにする内部または外部 Web サイトも追加する必要があります。次に、例を示します。

```
update.microsoft.com
*.salesforce.com
*.mycompanydomain.com
```

また、イントラネット サービスに使用するパブリック IP アドレスを追加する必要があります。追加しないと、Web セキュリティからこれらのイントラネット サーバにアクセスできません。

RFC 1918 で説明されているすべてのプライベート IP アドレスが、デフォルトでホスト例外リストに含められています。

次の構文を使用して、サブネットと IP アドレスを入力できます。

構文	例
個々の IPv4 および IPv6 アドレス	80.254.145.118 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing（CIDR）表記	10.0.0.0/8 2001:DB8::/48
完全修飾ドメイン名	windowsupdate.microsoft.com ipv6.google.com **（注）** 部分的なドメインはサポートされません。たとえば、example.com はサポートされません。
完全修飾ドメイン名または IP アドレスのワイルドカード	127.0.0.* *.cisco.com

注意 トップレベル ドメインの両側にワイルドカードを使用しないでください（たとえば *.cisco.*）。これには、フィッシング サイトが含まれることがあるためです。

注意 デフォルトのホスト例外エントリを削除または変更しないでください。

プロキシ例外

[プロキシ除外（Proxy Exceptions）] エリアで、認定された内部プロキシの IP アドレスを入力します。`192.168.2.250` などです。[除外（Exceptions）] パネルの図については、図 6-3 を参照してください。

このフィールドに IPv4 および IPv6 アドレスを指定できますが、ポート番号を一緒に指定することはできません。CIDR 表記を使用して IP アドレスを指定できます。

IP アドレスを指定すると、ScanSafe Web スキャニング サービスが、これらのサーバ宛の Web データを代行受信し、SSL を使用してデータをトンネリングしないようにします。これによって、プロキシ サーバは中断なしで動作できます。ここでプロキシ サーバを追加しなかった場合、プロキシ サーバは ScanSafe Web スキャニング サービス トラフィックを SSL トンネルと見なします。

このリストにないプロキシについては、Web セキュリティは、SSL を使用してトンネリングしようとするため、ユーザが、インターネット アクセスのためにプロキシがネットワークから出る必要がある別の企業サイトにいる場合、ScanSafe Web スキャニング サービスは、開いているインターネット接続を使用しているときと同じレベルのサポートを提供します。

静的な例外

トラフィックが ScanSafe Web スキャニング サービスをバイパスする必要がある個々の IP アドレスまたは IP アドレスの範囲のリストを Classless Inter-Domain Routing（CIDR）表記で追加します。リストには、VPN ゲートウェイの入力 IP アドレスを含めます。図 6-3 を参照してください。

CIDR 表記を使用して、IPv4 および IPv6 アドレスまたはアドレスの範囲を指定できます。完全修飾ドメイン名を指定したり、IP アドレスにワイルドカードを使用したりすることはできません。次に、正しい構文の例を示します。

```
10.10.10.5
192.0.2.0/24
```

（注）　必ず SSL VPN コンセントレータの IP アドレスを静的な除外リストに追加してください。

IPv6 Web トラフィックに関するユーザ ガイドライン

IPv6 アドレス、ドメイン名、アドレス範囲、またはワイルド カードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。ここで DNS ルックアップが実行され、ユーザがアクセスしようとしている URL に IPv4 アドレスがあるかどうかが確認されます。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合は、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスするように設定する場合は、すべての IPv6 トラフィック **::/0** にこの静的な例外を追加します。これを行うことで、すべての IPv6 トラフィックがすべてのスキャニング プロキシをバイパスします。つまり、この場合は IPv6 トラフィックは Web セキュリティで保護されません。

Web スキャニング サービス プリファレンスの設定

次のプリファレンスを設定するには、このパネルを使用します。

- 「ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算」（P.6-16）
- 「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）

ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算

ユーザが、接続先の ScanSafe スキャニング プロキシを選択できるようにするには、次の手順を実行します。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[プリファレンス（Preferences）] をクリックします。この手順で設定したフィールドの図については、図 6-4 を参照してください。

ステップ 4　[ユーザ制御可（User Controllable）] をオンにします。（これはデフォルト設定です）。[ユーザ制御可（User Controllable）] は、ユーザが AnyConnect インターフェイスで [タワーの自動選択（Automatic Tower Selection）] および [スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] 設定を変更できるかどうかを決定します。

ステップ 5　Web セキュリティにスキャニング プロキシを自動的に選択させるには、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] をオンにします。これを行うと、[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] は自動的にオンになります。

- [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] を選択すると、Web セキュリティは、応答時間が最も早いスキャニング プロキシを判別して、ユーザをそのスキャニング プロキシに自動的に接続します。

- [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しなくても、まだ [スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] が選択されている場合、ユーザには、接続できるスキャニング プロキシのリストが、応答時間が早い順に表示されます。

（注）　[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] をイネーブルにすると、一時的な通信の中断と障害が原因で、アクティブなスキャニング プロキシの選択が自動的に変更される可能性があります。スキャニング プロキシの変更は望ましくないことがあります。これは、別の言語を使用する別の国のスキャニング プロキシから検索結果が戻されるなど、予期しない動作の原因となる可能性があるためです。

ステップ 6　[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] をオンにした場合は、応答時間が最も早いスキャニング プロキシを計算するための設定を行います。

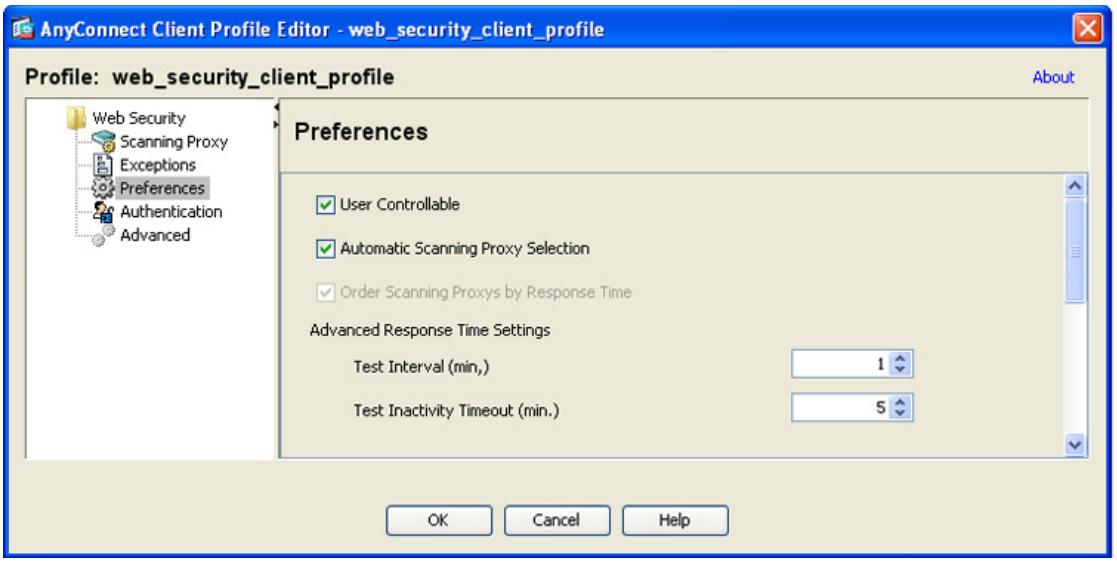
- [テスト間隔（Test Interval）] : 各パフォーマンス テストの実行間の時間（分単位）。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。
- [テスト非アクティブ タイムアウト（Test Inactivity Timeout）] : Web セキュリティが、ユーザ非アクティブのために応答時間テストを一時停止するまでの時間。Web セキュリティは、スキャニング プロキシで接続試行が行われるとすぐにテストを再開します。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

（注）　[スキャン プロキシを応答時間順に並べ替え（Order Scanning Proxies by Response Time）] テストは、次の例外を除き、テスト間隔に基づいて実行し続けます。

- 「Detect-On-LAN」がイネーブルで、マシンが社内 LAN 上にあることをビーコン サーバが検出した。
- Web セキュリティのライセンス キーがないか、無効である。
- ユーザが、設定済みの時間非アクティブで、その結果 [テスト非アクティブ タイムアウト（Test Inactivity Timeout）] しきい値に達した。

ステップ 7　Web セキュリティ クライアント プロファイルを保存します。

図 6-4　ユーザ制御および応答時間制御によるスキャニング プロキシの順序付け



Detect-On-LAN 用のビーコン サーバ接続の設定

Detect-On-LAN 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。詳細については、「Detect-On-LAN」（P.6-40）を参照してください。

ビーコン サーバは、企業の一意の公開 / 秘密キー ペアを使用して、正しい公開キーを持つ Cisco ScanSafe Web セキュリティの顧客のみが、ネットワークへの接続中に ScanSafe スキャニング プロキシをバイパスできるようにしています。ネットワークにビーコン サーバの複数のインスタンスを展開する場合、各インスタンスは同一の公開 / 秘密キー ペアを使用する必要があります。

（注）　ネットワークにプロキシが存在する（ScanSafe Connector など）状態で、ビーコン サーバを使用しない場合は、プロファイル エディタの [除外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。「プロキシ例外」（P.6-15）を参照してください。

Web セキュリティのビーコン サーバとの対話を設定するには、次の手順を実行します。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[プリファレンス（Preferences）] をクリックします。[プリファレンス（Preferences）] パネルの図については、図 6-5 を参照してください。

ステップ 4　ビーコン サーバをネットワーク上にインストールし、Web セキュリティ ユーザからのトラフィックを受信するようにこのビーコン サーバを設定した場合は、[ビーコン確認（Beacon Check）] をオンにします。

ステップ 5　[パブリック キー ファイル（Public Key File）] フィールドで [参照（Browse）] をクリックして、企業の公開キー証明書を選択します。ビーコン サーバは、認証に RSA 公開 / 秘密キー ペアを使用します。秘密キーの長さは 512 ビット以上である必要があります。ただし、シスコでは 1,024 ビットのキーを推奨します。

ステップ 6　[ビーコンの新しいアドレス（New Beacon Address）] フィールドで、ビーコン サーバがインストールされているコンピュータを指定します。有効な IP アドレスまたはドメイン名のいずれかを使用します。正しい構文の例を示します。

構文	例
個々の IPv4 アドレス	`10.10.10.123`
完全修飾ドメイン名	`beaconserver.cisco.com`

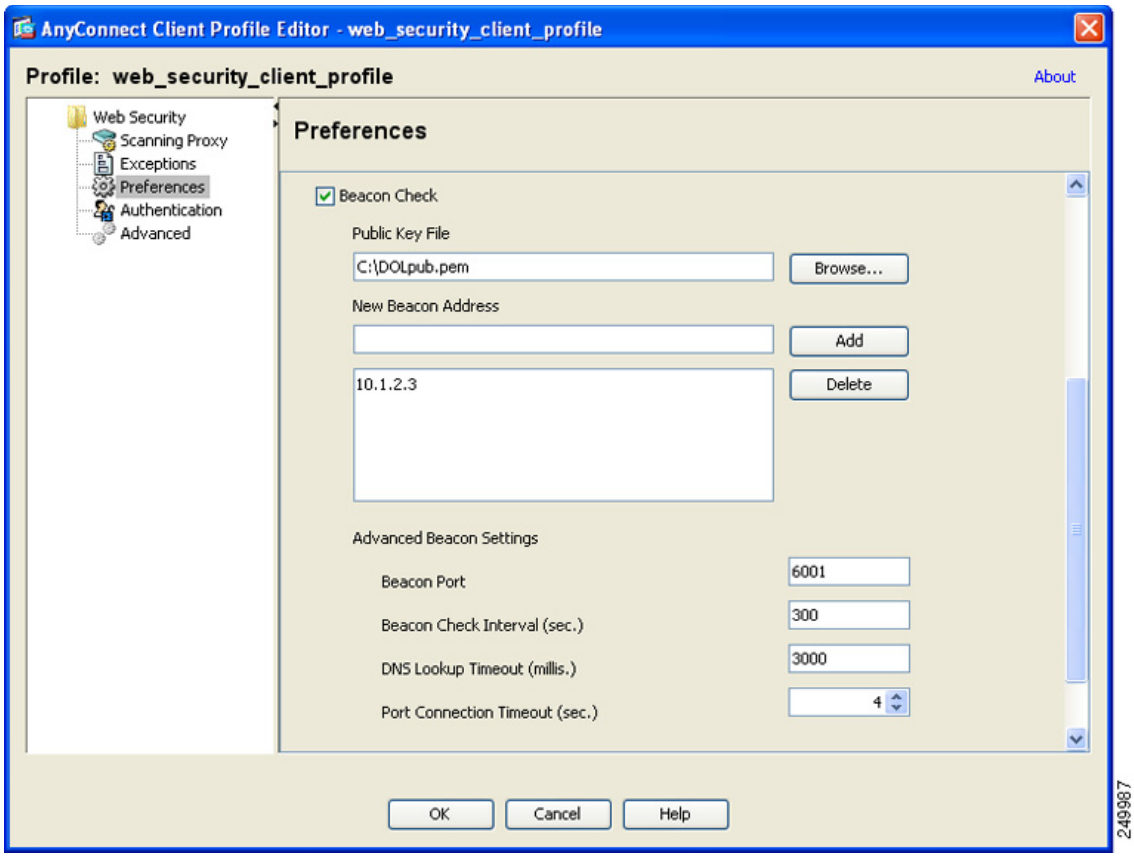
（注）　部分的なドメインはサポートされません。たとえば、cisco.com はサポートされません。

ステップ 7　次の高度なビーコン設定を行います。

- [ビーコンのポート（Beacon Port）] : この要素は、サービスによって使用される TCP/IP ポートを指定します。ポート 6001 でサービスがすでに実行中の場合、この要素を変更できます。ビーコン サーバがインストールされているコンピュータの websecurity.config ファイルで対応する要素を変更する必要もあります。
- [ビーコン確認間隔（Beacon Check Interval）] : Web セキュリティは、ビーコン サーバへの接続の試行の間、秒単位で指定されたこの時間待機し、このビーコン サーバが LAN 上にあるかどうかを判別します。
- [DNS ルックアップ タイムアウト（DNS Lookup Timeout）] : <Beacons> 設定で指定されたホスト名（指定された場合）での DNS ルックアップのタイムアウト（ミリ秒）。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。
- [ポート接続タイムアウト（Port Connection Timeout）] : この要素は、ビーコン サーバにデータを送信していない接続が閉じられるまでの時間を秒単位で指定します。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

ステップ 8　Web セキュリティ クライアント プロファイルを保存します。

図 6-5　ビーコン サーバ チェックの設定

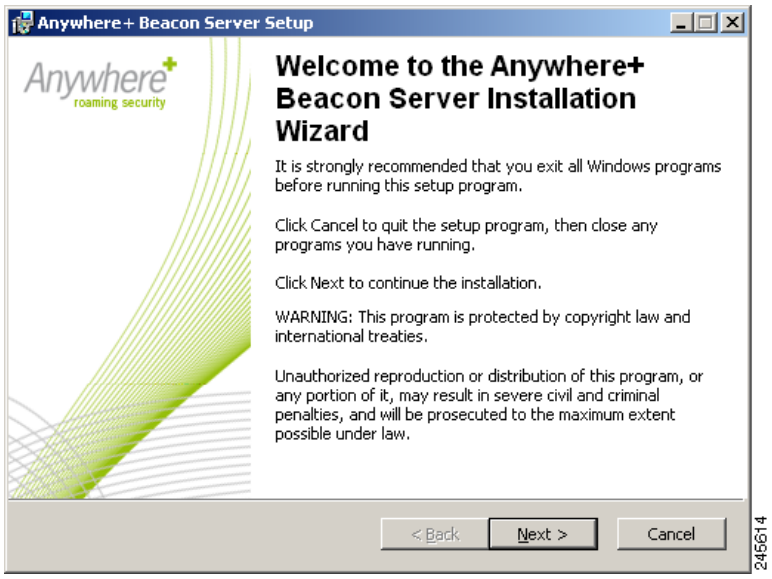


ビーコン サーバのインストール

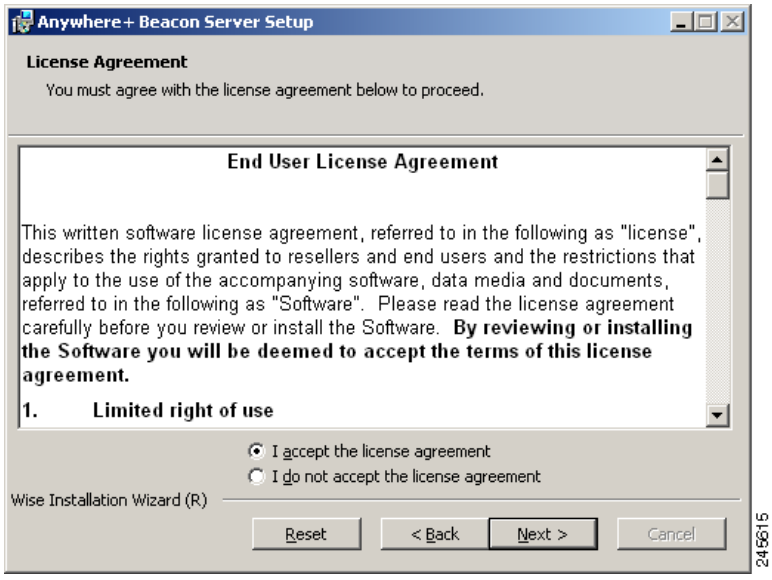
ビーコン サーバをインストールする前に、DOLprv.pem ファイルを BeaconServer.msi プログラム ファイルが含まれているインストール フォルダにコピーする必要があります。「秘密キーおよび公開キーの生成」（P.6-41）を参照してください。BeaconServer.config ファイルを同じフォルダにコピーした場合、これは、デフォルトの設定ファイルの代わりにインストールされます。設定ファイルはインストール後に編集できるため、これは、ビーコン サーバの複数のコピーをインストールする場合を除き不要です。「ビーコン サーバの設定」（P.6-27）を参照してください。標準のインストール方法に加えて、サイレント インストールの実行を選択できます。「サイレント インストール」（P.6-23）を参照してください。

ビーコン サーバをインストールするには、次の手順を実行します。

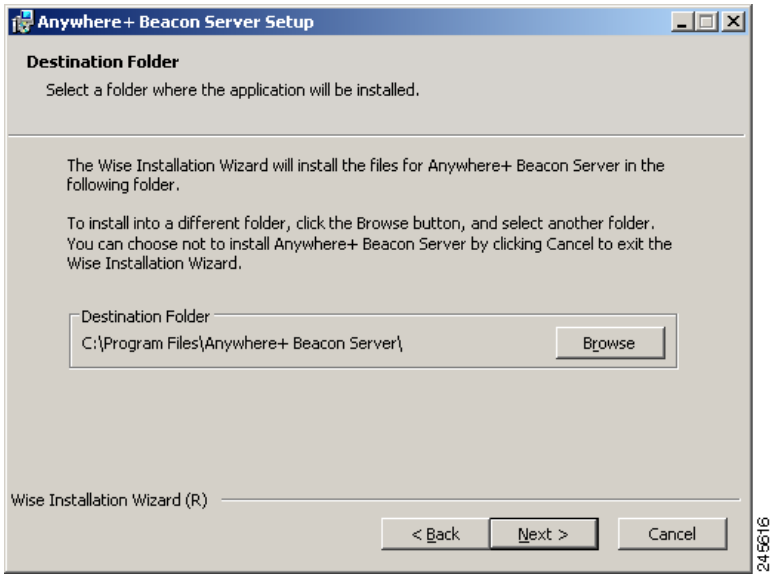
ステップ 1　BeaconServer.msi プログラム ファイルをダブルクリックして、インストール ウィザードを実行します。



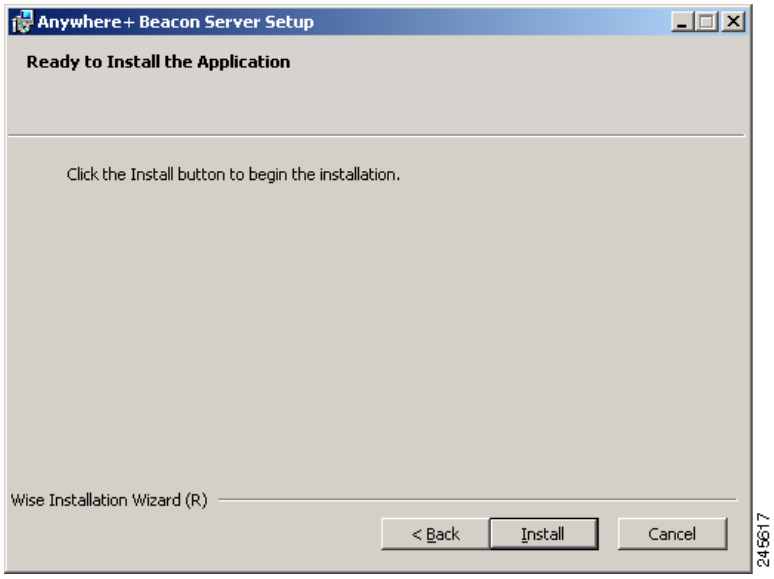
ステップ 2　[次へ（Next）] をクリックすると、[ライセンス契約書（License Agreement）] ダイアログが表示されます。



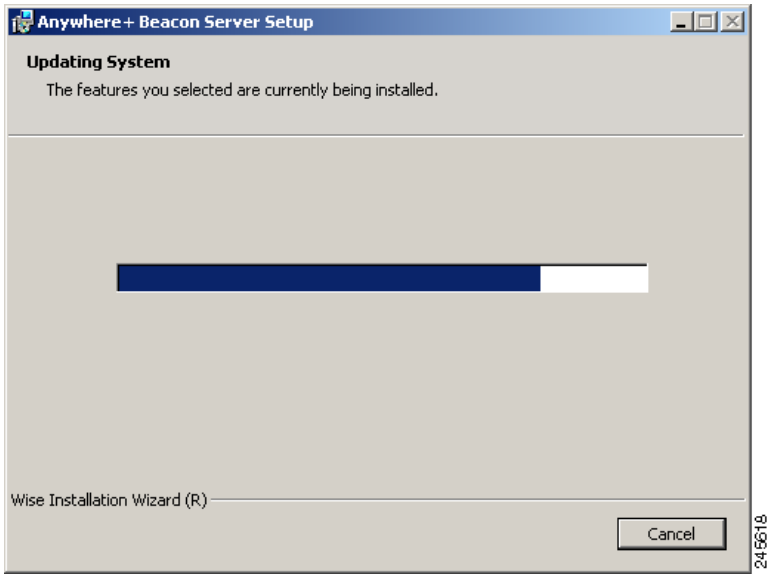
ステップ 3　エンド ユーザ ライセンス契約書を読みます。条件に同意する場合は [ライセンス契約書に同意します（I accept the license agreement）] をクリックし、次に [次へ（Next）] をクリックして [インストール先フォルダ（Destination Folder）] ダイアログを表示します。条件に同意しない場合は、[キャンセル（Cancel）] をクリックしてインストールを中止します。



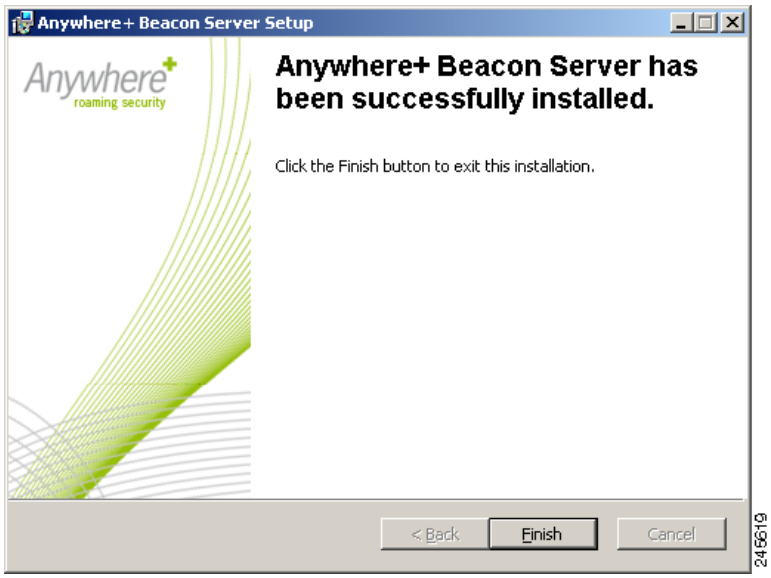
ステップ 4　[次へ（Next）] をクリックしてデフォルトのインストール フォルダを確定します。または、[参照（Browse）] をクリックして必要なフォルダに移動し、[次へ（Next）] をクリックして [アプリケーションをインストールします（Ready to Install the Application）] を表示します。



ステップ 5　[インストール（Install）] をクリックすると、インストールが開始されます。



ステップ 6　インストールが正常に完了すると、次のダイアログが表示されます。



（注）　インストールに問題が発生した場合、コマンド プロンプトからインストーラを起動します。msiexec /i <path>/BeaconServer.msi /l*vx install.log と入力します。install.log というログ ファイルが作成されます。

サイレント インストール

ビーコン サーバでは、次のコマンドを使用すると MSI インストーラのサイレント モードを利用できます。

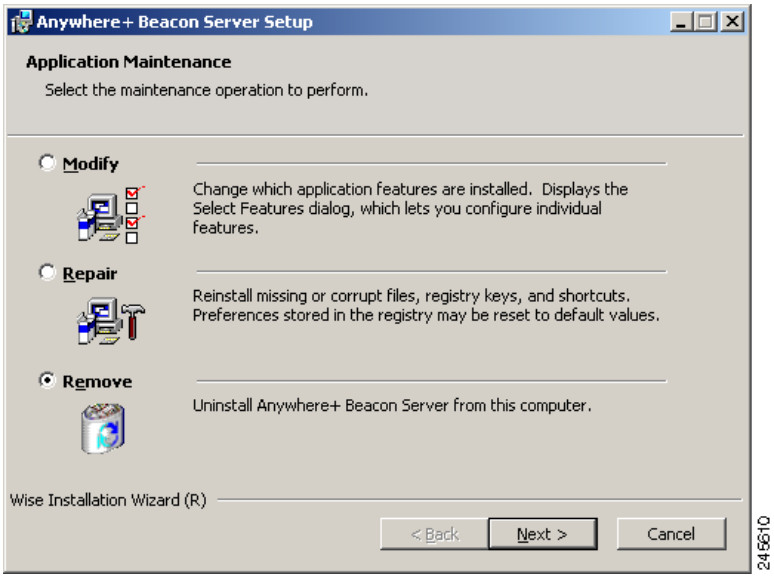
```
msiexec /i <path>/BeaconServer.msi /l*vx install.log /qn
```

パスは、ローカル フォルダ（C:\temp など）またはネットワーク共有（\\server\share など）のどちらでもかまいません。

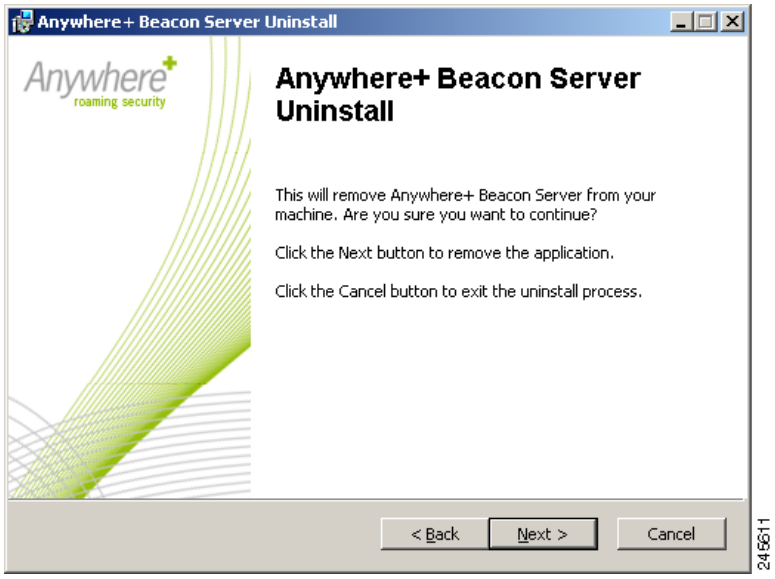
ビーコン サーバの削除

ビーコン サーバを削除する前に、ビーコン サーバ サービスが停止されていることを確認します。ビーコン サーバを削除するには、コントロール パネルのプログラムの追加と削除を使用するか、コマンド プロンプトで **msiexec /x <path>BeaconServer.msi /l*vx uninstall.log /qn** と入力します。または、ウィザードを使用してサーバからビーコン サーバを削除するには、次の手順を実行します。

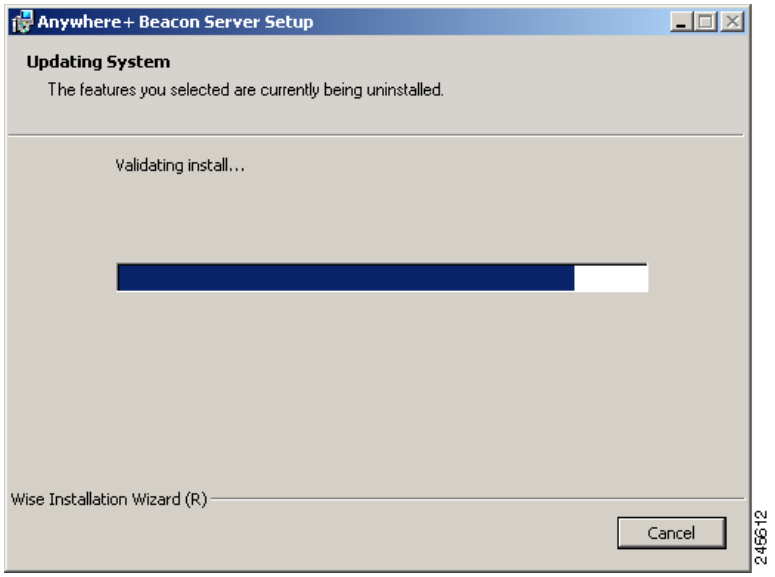
ステップ 1　BeaconServer.msi プログラム ファイルをダブルクリックして、ウィザードを実行します。



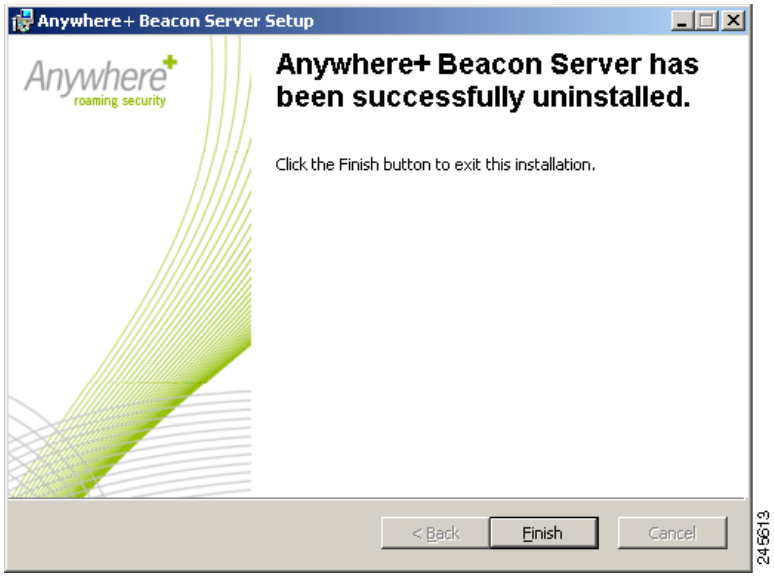
ステップ 2　[削除（Remove）] をクリックし、次に [次へ（Next）] をクリックして [ビーコン サーバのアンインストール（Beacon Server Uninstall）] ダイアログを表示します。



ステップ 3　[次へ（Next）] をクリックしてビーコン サーバを削除します。または、[キャンセル（Cancel）] をクリックして削除プロセスを中止します。



ステップ 4　削除が正常に完了すると、次のダイアログが表示されます。



ステップ 5　[完了（Finish）] をクリックしてウィザードを終了します。

ビーコン サーバの設定

ビーコン サーバを設定するには、BeaconServer.config XML ファイルを編集します。このファイルは、ビーコン サーバがインストールされているフォルダ（通常、C:\Program Files\Anywhere+ Beacon Server\）にあります。デフォルト設定は次のとおりです。

```
<DetectOnLANServer>
    <ConfigurationParameters>
        <!-- Beacon Port, default 6001 -->
        <BeaconPort>6001</BeaconPort>
        <!-- Connection Timeout in secs, default 10 -->
        <ConnectionTimeout>10</ConnectionTimeout>
        <!-- Disallowed Source IP addresses ';' separated -->
        <DisallowedSourceIP></DisallowedSourceIP>
        <Logging>
            <debug_level>00000107</debug_level>
            <!-- Log file size in kilobytes (KB) -->
            <LogFileSize>1000</LogFileSize>
            <!-- Number of log files to retain -->
            <NumLogFilesToRetain>10</NumLogFilesToRetain>
            <!-- This setting specifies the time for which a log file can be retained
before being deleted -->
            <LogFileRetentionTime>
                <Days>7</Days>
                <Hours>0</Hours>
                <Minutes>0</Minutes>
            </LogFileRetentionTime>
        </Logging>
    </ConfigurationParameters>
</DetectOnLANServer>
```

サポートから指示があった場合を除いて、次の要素だけを変更します。

BeaconPort	この要素は、サービスによって使用される TCP/IP ポートを指定します。ポート 6001 でサービスがすでに実行中の場合、この要素を変更できます。各クライアント コンピュータの Admin.cfg ファイル内の対応する要素も変更する必要があります。
ConnectionTimeout	この要素は、ビーコン サーバにデータを送信していない接続が閉じられるまでの時間を秒単位で指定します。
DisallowedSourceIP	この要素には、ビーコン サーバを経由する AnyConnect サービスをバイパスしない IP アドレスが含まれます。複数の要素を使用するのではなく、各 IP アドレスをセミコロン（;）で区切って 1 つの要素だけを使用します。
Logging	ロギングを参照してください。

ロギング

ログ ファイルの循環を管理する一連のサブタグが含まれます。

debug_level	カスタマー サポート担当者から指示がない限り、これは変更しません。
LogFileSize	許容される最大ログ ファイル サイズ（100 ～ 10,000 キロバイト）。現在のログ ファイルが許容される最大サイズに達すると、バックアップされて新しいログ ファイルが作成されます。デフォルトのサイズは 100 KB です。
NumLogFilesToRetain	保持する古いログ ファイルの数。デフォルトは 10 です。許容数に達すると、古いログ ファイルは削除されます。
LogFileRetentionTime	ログ ファイルの最大数に達したかどうかに関係なく、ログ ファイルが削除されるまでの時間。次のサブタグで指定します。 • Days • Hours • Minutes

システム トレイ アイコン

システム トレイ アイコンは、サービスのステータスを示します。


サービスが実行中です。


サービスに問題が発生しています。

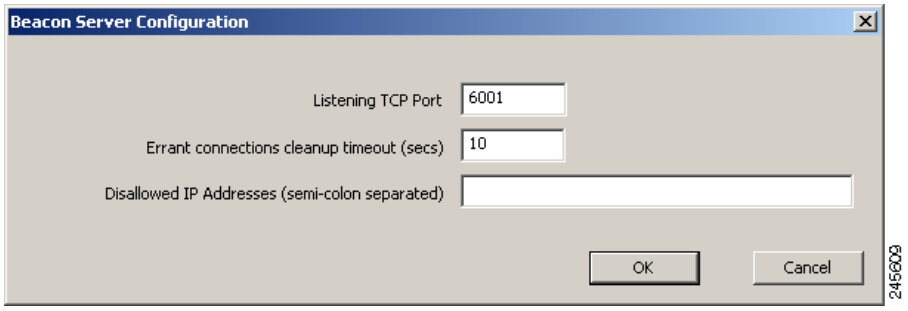

サービスが停止しているか、秘密キー ファイルがないか、秘密キー ファイルが破損しています。

サービスを開始するには、アイコンを右クリックして [ビーコン サーバの起動（Start Beacon Server）] をクリックします。

サービスを停止するには、アイコンを右クリックして [ビーコン サーバの停止（Stop Beacon Server）] をクリックします。

ビーコン サーバを設定するには、次の手順を実行します。

ステップ 1　アイコンを右クリックして [プリファレンス（Preferences）] をクリックし、[ビーコンの設定（Beacon Configuration）] ダイアログを表示します。



ステップ 2　[TCP ポートのリスニング（Listening TCP port）] ボックスに、サービスが使用する TCP/IP ポートを入力します。

ステップ 3　[不正接続クリーンアップ タイムアウト（秒）（Errant connections cleanup timeout (secs)）] ボックスに、接続を開いたままにする時間を秒単位で入力します。

ステップ 4　[不可 IP アドレス（セミコロン区切り）（Disallowed IP Addresses (semi-colon separated)）] ボックスに、AnyConnect サービスをバイパスする IP アドレスまたはホスト名をセミコロン（;）で区切って入力します。

ステップ 5　[OK] をクリックして、BeaconServer.config ファイルに変更を保存します。または、[キャンセル（Cancel）] をクリックして変更を破棄します。

システム トレイ アプリケーションを終了するには、アイコンを右クリックして [GUI の終了（Terminate GUI）] をクリックします。サービスが実行中の場合、これによってサービスは停止されません。システム トレイ アイコンを再起動するには、コマンド プロンプトに次のように入力します。

```
<BeaconServerInstallFolder>\BeaconServer -BD
```

Detect-On-LAN の設定

Detect-On-LAN 機能を設定するには、次の手順を実行します。

ステップ 1　ビーコン サーバの 1 つ以上のコピーをネットワークにインストールします。「ビーコン サーバのインストール」（P.6-20）を参照してください。

（注）　ビーコン サーバは、物理的に社内 LAN にするすべての Web セキュリティ インストールおよびフル トンネル VPN 経由で接続されている Web セキュリティ インストールからアクセス可能でなければなりません。

ステップ 2　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。クライアント プロファイルが、AnyConnect ユーザに導入するグループ ポリシーを指定していることを確認してください。

ステップ 3　「Detect-On-LAN 用のビーコン サーバ接続の設定」（P.6-18）を使用して、Web セキュリティ クライアント プロファイルの [プリファレンス（Preferences）] パネルで次の設定を行います。

- [ビーコン確認（Beacon Check）] をオンにしてイネーブルにします。
- [パブリック キー ファイル（Public Key File）] フィールドで、公開 / 秘密キー ペアの一部として作成した公開キー ファイル（DOLpub.pem）を指定します。

- ビーコン サーバの各インスタンスの IP アドレスを [ビーコンの新しいアドレス（New Beacon Address）] フィールドに追加します。

ステップ 4　Web セキュリティ クライアント プロファイルの残りを設定して、保存します。

ステップ 5　Detect-On-LAN 機能が設定されたこの Web セキュリティ クライアント プロファイルを受信するには、ユーザは、ASA への VPN 接続の確立を試行する際に、AnyConnect Secure Mobility Client の [VPN] コンボ ボックスでこのクライアント プロファイルの名前を選択する必要があります。

認証の設定および ScanSafe スキャニング プロキシへのグループ メンバーシップの送信

ステップ 1　次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。
- Windows OS のスタンドアロン モードで、[スタート（Start）] > [プログラム（Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択します。

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 3　[認証（Authentication）] をクリックします。この手順で設定したフィールドの図については、図 6-6 を参照してください。

ステップ 4　[Proxy Authentication License Key] フィールドに、ScanCenter で作成した企業キー、グループ キー、またはユーザ キーに対応するライセンス キーを入力します。企業ドメインに基づいてユーザを認証する場合は、作成した企業キーを入力します。ScanCenter または Active Directory グループに基づいてユーザを認証する場合は、作成したグループ キーを入力します。デフォルトでは、このタグは空です。空のままにした場合、Web セキュリティはパススルー モードで動作します。

ステップ 5　[Service Password] に入力します。Web セキュリティのデフォルト パスワードは **websecurity** です。このパスワードは、プロファイルのカスタマイズ時に変更できます。パスワードには英数字（a ～ z、A ～ Z、0 ～ 9）のみを使用する必要があります。その他の文字は、Windows コマンド シェルによって制御文字と間違われる可能性があるか、XML で特殊な意味を持つことがあるためです。

このパスワードを使用して、管理者以外の権限を持っているユーザは、Web セキュリティ サービスの開始および停止を行うことができます。管理者権限を持つユーザは、このパスワードなしで Web セキュリティ サービスを開始および停止できます。詳細については、「この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。」（P.6-42）を参照してください。

ステップ 6　すべての HTTP 要求とともに企業ドメイン情報および ScanSafe または Active Directory グループ情報をスキャニング プロキシ サーバに送信できます。スキャニング プロキシは、ユーザのドメインおよびグループ メンバーシップについて認識している内容に基づいてトラフィック フィルタリング ルールを適用します。

（注）　ユーザのカスタム ユーザ名とカスタム グループ情報をスキャニング サーバ プロキシに送信する場合、または企業が Active Directory を使用しない場合は、この手順をスキップして、ステップ 7 に進みます。

- [エンタープライズ ドメインの使用（Use Enterprise Domains）] オプション ボタンをクリックします。

  ドメイン名を NetBIOS 形式で入力します。たとえば、**example.cisco.com** の NetBIOS 形式は **cisco** です。DNS 形式を使用したドメイン名（**abc.def.com**）を入力しないでください

  [エンタープライズ ドメイン名（Enterprise Domain name）] フィールドにドメイン名を指定すると、ScanCenter は、現在ログインしている Active Directory ユーザを識別して、そのユーザの Active Directory グループを列挙します。その情報は、すべての要求とともにスキャニング プロキシに送信されます。

  次のいずれかを示すには、企業ドメインとしてアスタリスク（*）を入力できます。

  - （*）は、任意のドメインを示すワイルドカードとして使用されます。Windows と Mac OS X の両方のコンピュータでは、企業ドメインの入力が（*）で、マシンがドメインにある場合、ユーザが属するすべてのドメインが一致し、ユーザ名とグループ メンバーシップ情報が ScanSafe スキャニング プロキシに送信されます。これは、複数のドメインが存在する企業にとって役に立ちます。
  - Mac OS X クライアントは、Active Directory ドメイン ユーザ名を持たないユーザには、IP アドレスの代わりにユーザ名を使用する必要があります。

- ScanSafe スキャニング プロキシに対する HTTP 要求でグループ情報を含めるか除外するには、[グループ包含リスト（Group Include List）] と [グループ除外リストの使用（Use Group Exclude List）] エリアを使用します。

  [グループ包含リスト（Group Include List）]。[グループ包含リスト（Group Include List）] の選択後に、HTTP 要求とともに ScanSafe スキャニング プロキシ サーバに送信する ScanSafe または Active Directory グループ名を [グループ包含リスト（Group Include List）] に追加します。要求が、指定された企業ドメイン内のユーザから出された場合、HTTP 要求は、ユーザのグループ メンバーシップに従ってフィルタリングされます。ユーザにグループ メンバーシップがない場合、HTTP 要求は、デフォルトのフィルタリング ルール セットを使用してフィルタリングされます。

  [グループ除外リスト（Group Exclude List）]。[グループ除外リスト（Group Exclude List）] の選択後に、HTTP 要求とともに ScanSafe スキャニング プロキシ サーバに送信しない ScanSafe または Active Directory グループ名を [グループ除外リスト（Group Exclude List）] に追加します。ユーザが、[グループ除外リスト（Group Exclude List）] のいずれかのグループに属している場合、そのグループ名はスキャニング プロキシ サーバに送信されず、ユーザの HTTP 要求は、その他のグループ メンバーシップ、または最低でも Active Directory または ScanSafe グループ所属を持たないユーザに対して定義されたデフォルトのフィルタリング ルール セットのいずれかによってフィルタリングされます。

ステップ 7　カスタム ユーザ名とグループ名をスキャニング プロキシ サーバに送信するには、[認証済みユーザ / グループの使用（Use Authenticated User/Group）] オプション ボタンをクリックします。

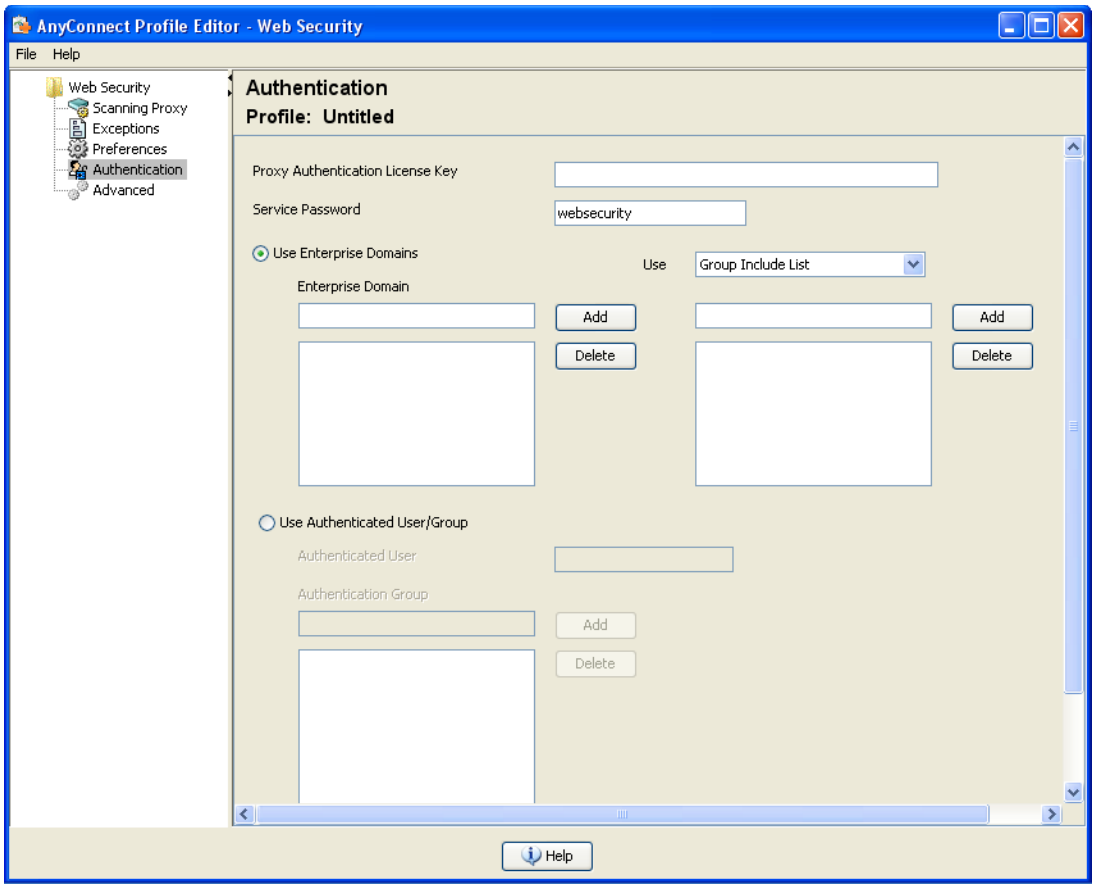
- [認証済みユーザ（Authenticated User）] フィールドに、カスタム ユーザ名を入力します。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する ScanCenter レポートで使用されます。
- [認証グループ（Authentication Group）] フィールドに、最大 256 文字の英数字のカスタム グループ名を入力します。

HTTP 要求がスキャニング プロキシ サーバに送信されると、カスタム グループ名が送信された場合に、スキャニング プロキシ サーバに対応するグループ名があれば、HTTP トラフィックは、カスタム グループ名に関連付けられたルールによってフィルタリングされます。スキャニング プロキシ サーバで定義された対応するカスタム グループがない場合、HTTP 要求はデフォルト ルールによってフィルタリングされます。

カスタム ユーザ名のみを設定し、カスタム グループを設定していない場合、HTTP 要求は、スキャニング プロキシ サーバのデフォルト ルールによってフィルタリングされます。

ステップ 8　Web セキュリティ クライアント プロファイルを保存します。

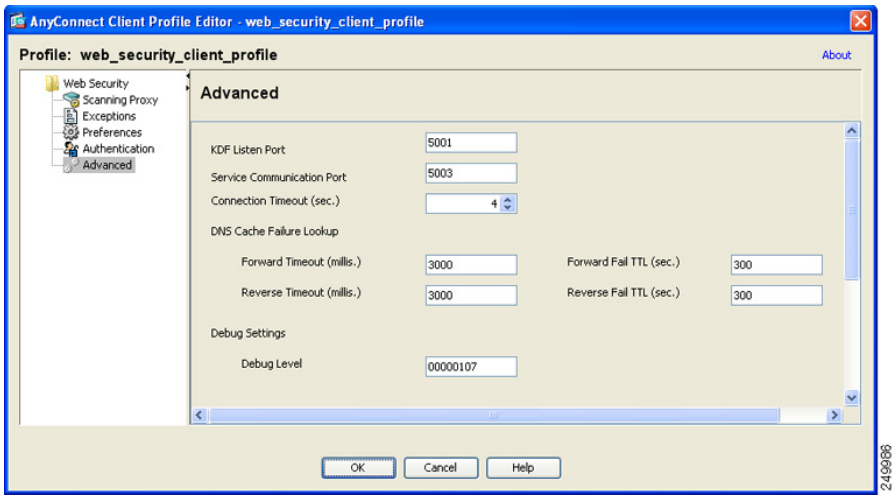
図 6-6　ScanSafe スキャニング プロキシ認証の設定



Web セキュリティの詳細設定

Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネルには、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ついくつかの設定が表示されます。このパネルの設定は、カスタマー サポートから指示された場合以外は変更しないでください。

図 6-7　Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネル



プロファイル エディタの [詳細（Advanced）] パネルで、次のタスクを実行できます。

- 「KDF リスニング ポートの設定」（P.6-34）
- 「サービス通信ポートの設定」（P.6-35）
- 「接続タイムアウトの設定」（P.6-35）
- 「DNS キャッシュ障害ルックアップの設定」（P.6-35）
- 「デバッグの設定」（P.6-36）

KDF リスニング ポートの設定

Kernel Driver Framework（KDF）は、トラフィック リスニング ポートの 1 つを宛先ポートとして使用する接続をすべて代行受信して、トラフィックを KDF リスニング ポートに転送します。Web スキャニング サービスは、KDF リスニング ポートに転送されるトラフィックをすべて分析します。

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[KDF リスン ポート（KDF Listen Port）] フィールドに KDF リッスン ポートを指定します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

サービス通信ポートの設定

サービス通信ポートは、Web スキャニング サービスが、AnyConnect GUI コンポーネントおよびその他のユーティリティ コンポーネントからの着信接続を受信するポートです。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[サービス通信ポート（Service Communication Port）] フィールドを編集します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

接続タイムアウトの設定

接続タイムアウト設定によって、Web セキュリティがスキャニング プロキシを使用せずに直接インターネットにアクセスしようとするまでのタイムアウトを設定できます。空白のままにすると、デフォルト値の 4 秒が使用されます。これにより、再試行する前にタイムアウトになるのをそれほど長く待機する必要がなく、ユーザは有料ネットワーク サービスにより速くアクセスできます。

[接続のタイムアウト（Connection Timeout）] フィールドを設定するには、次の手順に従います。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。Web セキュリティ プロファイル エディタの [詳細（Advanced）] パネルの図については、図 6-7 を参照してください。

ステップ 3　[接続のタイムアウト（Connection Timeout）] フィールドを変更します。

ステップ 4　Web セキュリティ クライアント プロファイルを保存します。

DNS キャッシュ障害ルックアップの設定

プロファイル エディタの [詳細（Advanced）] パネルに、ドメイン ネーム サーバ ルックアップを管理するためのフィールドがいくつか表示されます。これらは、DNS ルックアップに最適な値を使用して設定されています。この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

デバッグの設定

[デバッグ レベル（Debug Level）] は設定可能なフィールドです。ただし、この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

Web セキュリティ ロギング

Windows OS

すべての Web セキュリティ メッセージは、Windows イベント ビューアの **Event Viewer (Local)\Cisco AnyConect Web Security Module** フォルダに記録されます。Web セキュリティがイベント ビューアに記録するイベントは、Cisco Technical Assistance Center のエンジニアによる分析用です。

Mac OS X

Web セキュリティ メッセージは、syslog またはコンソールから表示できます。

Web セキュリティ クライアント プロファイル ファイル

AnyConnect にバンドルされたプロファイル エディタを使用して Web セキュリティ クライアント プロファイルを作成して保存した後で、プロファイル エディタは、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.wsp を使用します。

スタンドアロン プロファイル エディタを使用して Web セキュリティ クライアント プロファイルを作成して保存した後で、プレーン テキスト バージョンのクライアント プロファイルのファイル命名規則は *filename*.xml になり、難解化ファイルの命名規則は *filename*.wso になります。

これらの 2 つの形式を使用することで、管理者は、必要に応じて次の特殊な処理を実行できます。

- 管理者は、難解化 Web セキュリティ クライアント プロファイルを ASA からエクスポートして、エンドポイント デバイスに配布できます。
- 管理者は、プレーン テキストの Web セキュリティ クライアント プロファイルを編集して、AnyConnect Web セキュリティ プロファイル エディタでサポートされない編集を実行できます。プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルは、カスタマー サポートから指示された場合以外は変更しないでください。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3　ファイルを保存するローカル フォルダを参照します。[ローカル パス（Local Path）] フィールドのファイル名を編集すると、その新しいファイル名で Web セキュリティ クライアント プロファイルが保存されます。

ステップ 4　[エクスポート（Export）] をクリックします。ASDM は、Web セキュリティ クライアント プロファイルのプレーン テキスト バージョンである *filename*.wsp をエクスポートします。

DART バンドルのプレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

Diagnostic AnyConnect Reporting Tool（DART）バンドルをシスコのカスタマー サービスに送信する必要がある場合、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイル ファイル *filename*.wsp または *filename*.xml を DART バンドルとともに送信する必要があります。シスコのカスタマー サービスは、難解化バージョンを読み取ることができません。

ASDM でプロファイル エディタによって作成されたプレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを収集するには、プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポートの手順を使用します。

スタンドアロン バージョンのプロファイル エディタは、2 つのバージョンの Web セキュリティ プロファイル ファイルを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.xml を使用します。プレーン テキスト バージョンのファイル *filename*.xml を収集します。

DART バンドルをシスコのカスタマー サービスに送信する前に、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを DART バンドルに追加します。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルの編集および ASDM からのインポート

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルをエクスポートしたら、任意のプレーン テキストまたは XML エディタを使用してローカル コンピュータで編集できます。インポートには、この手順を使用します。

注意　ファイルをインポートすると、選択した Web セキュリティ クライアント プロファイルの内容は**上書きされます**。

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

ステップ 2　編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3　*filename*.wsp ファイルを変更した後で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページに戻って、編集したファイルのプロファイル名を選択します。

ステップ 4　[インポート（Import）] をクリックします。

ステップ 5　編集したバージョンの Web セキュリティ クライアント プロファイルを参照して、[インポート（Import）] をクリックします。

難解化 Web セキュリティ クライアント プロファイル ファイルのエクスポート

ステップ 1　ASDM を開き、[ツール（Tools）] > [ファイル管理（File Management）] を選択します。

ステップ 2　[ファイル管理（File Management）] 画面で、[ファイル転送（File Transfer）] > [ローカル PC とフラッシュ間（Between Local PC and Flash）] をクリックして、[ファイル転送（File Transfer）] ダイアログを使用して難解化 *filename*.wso クライアント プロファイル ファイルをローカル コンピュータに転送します。

スタンドアロン Web セキュリティ クライアント プロファイルのインストール

ASA がない場合に Web セキュリティ クライアント プロファイルを作成するには、スタンドアロン プロファイル エディタを使用します。

ステップ 1　[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）] を選択して、Web セキュリティ スタンドアロン プロファイル エディタを開きます。

ステップ 2　「AnyConnect Web セキュリティ クライアント プロファイルの作成」（P.6-8）の手順に従って、Web セキュリティ クライアント プロファイルを作成します。

ステップ 3　[ファイル（File）] > [保存（Save）] を選択して、Web セキュリティ クライアント プロファイルを保存します。スタンドアロン プロファイル エディタは、XML ファイルの 2 つのコピーを作成します。1 つは難解化ファイルでファイル命名規則 *filename*.wso を使用し、もう 1 つはプレーン テキスト形式でファイル命名規則 *filename*.xml（ASDM ツールによって生成される wsp ファイルと同等）を使用します。

ステップ 4　名前 **WebSecurity_ServiceProfile.wso** の難解化 *filename*.wso クライアント プロファイル ファイルを名前変更するか、次のいずれかのディレクトリに保存します。

- Windows XP ユーザの場合、ファイルをフォルダ **%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** に入れます
- Windows Vista および Windows 7 ユーザの場合、ファイルをフォルダ **%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** に入れます
- Mac ユーザの場合、ファイルを次のフォルダに入れます。**/opt/cisco/anyconnect/websecurity**

ステップ 5　「Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化」（P.6-42）の手順に従って、Cisco AnyConnect Web セキュリティ エージェント Windows サービスを再起動します。

Web セキュリティ トラフィックのスプリットトンネリングの設定

Web セキュリティおよび VPN は同時に使用できます。この設定で最適なパフォーマンスを確保するには、ScanSafe スキャニング プロキシの IP アドレスをトンネルから除外することをお勧めします。

ScanSafe スキャニング プロキシに送信されるトラフィックに関する決定はすべて Web セキュリティ設定によって行われるため、他のスプリット除外を設定する必要はありません。

ScanSafe スキャニング プロキシ IP アドレスのリストを取得するには、アドレスのリストが記載されている次のライブ マニュアルを参照してください。

http://80.254.145.118/websecurity-config-v2ip.xml

Detect-On-LAN 機能を使用する場合に、Web セキュリティと VPN が同時にアクティブになるようにするには、ビーコン サーバが VPN トンネル経由で到達可能にならないようにネットワークを設定します。この方法では、ユーザが社内 LAN 上にいるときに限り、Web セキュリティ機能はバイパス モードになります。

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

AnyConnect リリース 3.0.4 から、Web セキュリティ ホステッド クライアント プロファイルの ScanCenter ホステッド コンフィギュレーションにより、管理者は、Web セキュリティ クライアントに新しい設定を提供できます。これを行うには、Web セキュリティを使用するデバイスでクラウド（ホステッド コンフィギュレーション ファイルは ScanCenter サーバにあります）から新しい Web セキュリティ ホステッド クライアント プロファイルをダウンロードできるようにします。この機能の唯一の前提条件は、有効なクライアント プロファイルでデバイスに Web セキュリティがインストールされていることです。管理者は、Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを ScanCenter サーバにアップロードします。この XML ファイルには、ScanSafe からの有効なライセンス キーが含まれている必要があります。クライアントは、ホステッド コンフィギュレーション サーバへの適用後に、最大で 8 時間新しい設定ファイルを取得します。

ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Web セキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。新しいクライアント プロファイルをダウンロードした場合、Web セキュリティは、管理者が新しいクライアント プロファイル ファイルを使用可能にするまで同じファイルを再度ダウンロードしません。

クライアント プロファイル ファイルを作成して、Web セキュリティ デバイスでダウンロード可能にするプロセスは次のとおりです。

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

ステップ 1　Web セキュリティ プロファイル エディタを使用して、Web セキュリティ デバイス用の新しいクライアント プロファイルを作成します。このクライアント プロファイルには ScanSafe ライセンス キーが含まれている必要があります。ライセンス キーの詳細については、『ScanCenter Administration Guide, Release 5.1』を参照してください。

クライアント プロファイル ファイルをクリア テキストの XML ファイルとして保存します。このファイルを ScanCenter サーバにアップロードします。このファイルをアップロードすると、新しいクライアント プロファイルを Web セキュリティ クライアントで使用可能にできます。ScanSafe でのホステッド コンフィギュレーションの詳細については、『ScanCenter Administration Guide, Release 5.1』を参照してください。

企業でホステッド コンフィギュレーション機能がイネーブルになっている場合、新しいクライアント プロファイルは、企業の ScanCenter ポータルからアップロードおよび適用できます。ホステッド クライアント プロファイルはライセンスに関連付けられています。これは、使用中の別のライセンス（たとえば、別のグループ ライセンス キー）がある場合、各ライセンスには、独自のクライアント プロファイルが関連付けられていることを意味します。これによって、管理者は、使用するよう設定されているライセンスに応じて、異なるクライアント プロファイルを別のユーザにプッシュダウンできます。管理者は、ライセンスごとにさまざまな設定を格納して、ダウンロードするクライアントのデフォルト クライアント プロファイルを設定できます。その後、そのクライアント プロファイルをデフォルトとして選択することで、ホステッド コンフィギュレーション ポータルに格納されている他のリビジョンの設定の 1 つに切り替えることができます。1 つのライセンスに関連付けることができるクライアント プロファイルは 1 つのみです。これは、複数のリビジョンがライセンスに関連付けられている場合に、1 つのクライアント プロファイルのみをデフォルトにできることを意味します。

ステップ 2　クライアントがホステッド クライアント プロファイルをダウンロードした後で、新しいクライアント プロファイルが自動的に使用されますが、ユーザは次のいずれかを行う必要があります。

- デバイスをスリープ モードにしてから、再開する。再開時に、クライアントは新しい設定を使用します。
- デバイスを再起動する。
- デバイスで Web セキュリティ エージェント サービスを再開する。

（注）　Web セキュリティ エージェント サービスの再開オプションは、サービスを再開するために必要な権限を持つユーザのみが使用可能です。

Detect-On-LAN

Detect-On-LAN 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Detect-On-LAN 機能をイネーブルにすると、社内 LAN から発信されるネットワーク トラフィックはすべて、ScanSafe スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、ScanSafe Web スキャニング サービスではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。

正しい公開キーを持つ Web セキュリティ クライアントのみが、ネットワークへの接続中にスキャニング プロキシをバイパスできるように、ビーコン サーバは、組織に固有の公開 / 秘密キー ペアを使用します。同じ秘密 / 公開キー ペアを使用する場合、必要に応じて、ビーコン サーバの複数のコピーを導入することもできます。秘密 / 公開キー ペアは、ScanCenter ポータルで生成します。

ネットワークにプロキシが存在する（ScanSafe Connector など）状態で、ビーコン サーバを使用しない場合は、プロファイル エディタの [除外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。詳細については、「プロキシ例外」（P.6-15）を参照してください。

データ損失防止（DLP）アプライアンスなど、一部のサードパーティ ソリューションでは、Detect-On-LAN の設定も必要です。トラフィックが Web セキュリティの影響を受けないようにする必要があります。

秘密キーおよび公開キーの生成

ビーコン サーバは、認証に RSA 公開 / 秘密キー ペアを使用します。秘密キーの長さは 512 ビット以上である必要があります。ただし、シスコでは 1,024 ビットのキーを推奨します。

秘密キー ファイル名は DOLprv.pem、公開キー ファイル名は DOLpub.pem にする必要があります。公開キーは、設定ファイルに組み込まれます。

RSA キー ペアを生成するには、Microsoft Certificate Services（Windows Server オペレーティング システムのコンポーネント）や OpenSSL（http://www.openssl.org/）などのツールが必要です。Microsoft Certificate Services の使用については、ベンダーのマニュアルを参照してください。

OpenSSL を使用した秘密キーの生成

openssl.exe プログラム ファイルが含まれているフォルダに移動して、次のように入力します。

```
openssl genrsa -out DOLprv.pem 1024
```

DOLprv.pem ファイルを、BeaconServer.msi ファイルが含まれているフォルダにコピーします。または、ビーコン サーバがすでにインストールされている場合は、DOLprv.pem ファイルを、ビーコン サーバをインストールしたフォルダにコピーします。

OpenSSL を使用した公開キーの生成

公開キーを生成する前に、DOLprv.pem という秘密キーを openssl.exe プログラムと同じフォルダ内に作成する必要があります。公開キーを作成するには、次を入力します。

```
openssl rsa -in DOLprv.pem -out DOLpub.pem -outform PEM -pubout
```

DOLpub.pem ファイルを、AnyConnect Web セキュリティ モジュールをインストールしたフォルダにコピーします。

注意　AnyConnect Web セキュリティ モジュールのインストール時に公開キーを導入していない場合、AnyConnect がインストールされているすべてのコンピュータに手動でインストールする必要があります。

Cisco AnyConnect Web セキュリティ エージェントのディセーブル化およびイネーブル化

管理者は、次の手順を実行することで、Web トラフィックを代行受信する Cisco AnyConnect Web セキュリティ エージェントの機能をディセーブルおよびイネーブルにできます。

Windows を使用したフィルタのディセーブル化およびイネーブル化

この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

ステップ 1　コマンド プロンプト ウィンドウを開きます。

ステップ 2　**%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** フォルダに変更します。

ステップ 3　フィルタリングをディセーブルまたはイネーブルにします。

- フィルタリングをイネーブルにするには、**acwebsecagent.exe -enablesvc** と入力します
- フィルタリングをディセーブルにするには、**acwebsecagent.exe -disablesvc -*servicepassword*** と入力します

Mac OS X を使用したフィルタリングのディセーブル化およびイネーブル化

この手順で使用するサービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

ステップ 1　端末アプリケーションを起動します。

ステップ 2　**/opt/cisco/anyconnect/bin** フォルダに変更します。

ステップ 3　フィルタリングをディセーブルまたはイネーブルにします。

- フィルタリングをイネーブルにするには、**acwebsecagent -enablesvc** と入力します
- フィルタリングをディセーブルにするには、**acwebsecagent -disablesvc -*servicepassword*** と入力します

Windows のロックダウン オプション

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

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

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

（注）　この機能は Mac OS X クライアントでは使用不可です。