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。

- システム要件
- ライセンス要件
- 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
- 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 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 Cisco Cloud Web Security 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
- 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」（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、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）

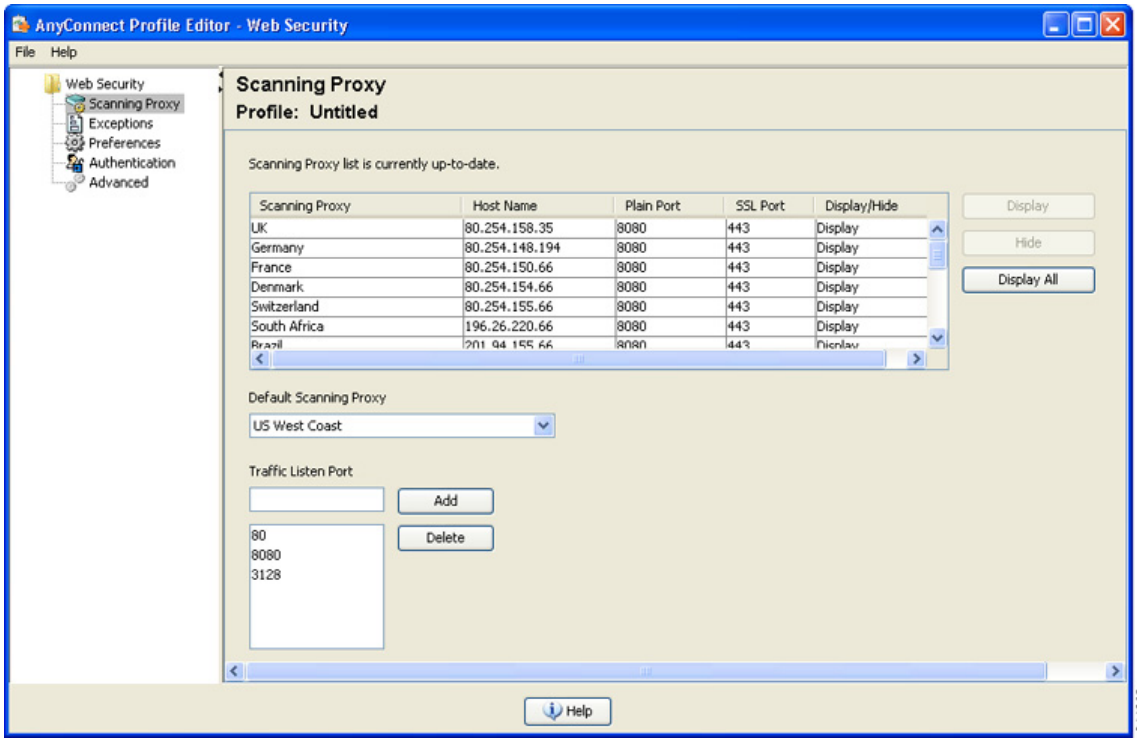
- 「Secure Trusted Network Detection の設定」（P.6-17）
- 「認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信」（P.6-18）

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。

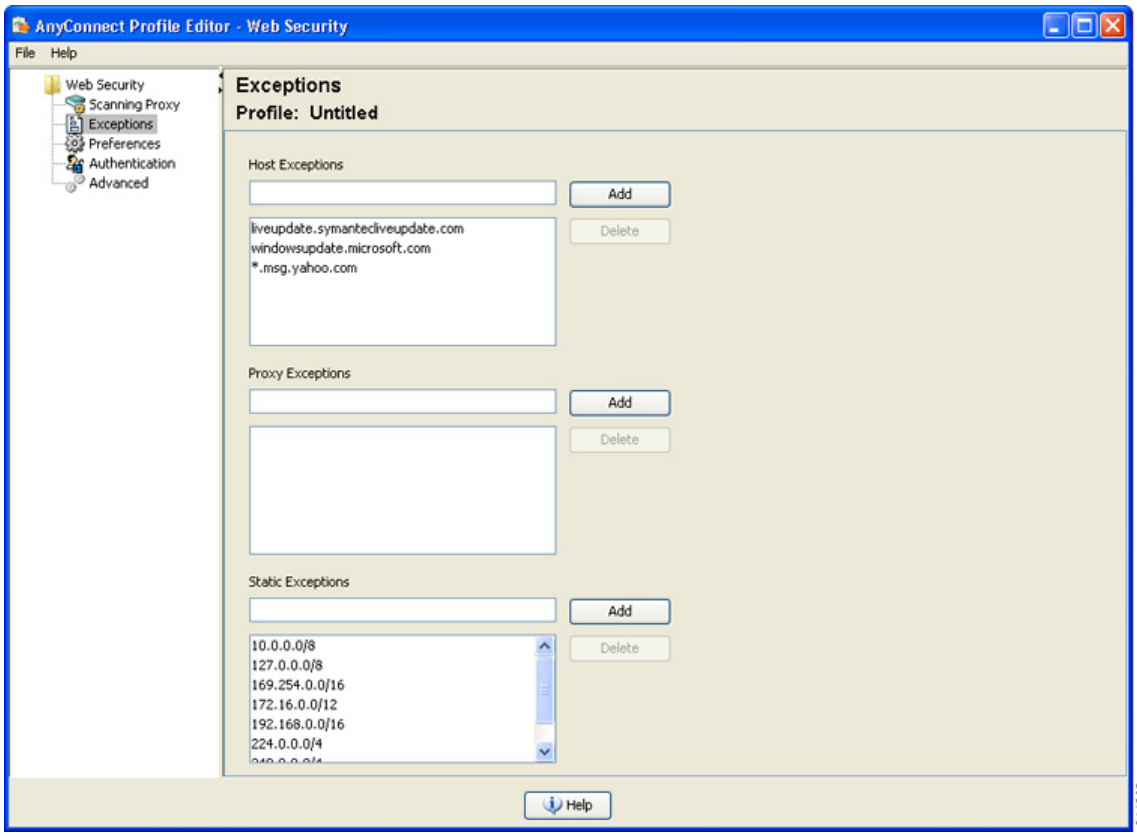
Web スキャニング サービスからのエンドポイント トラフィックの除外

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。

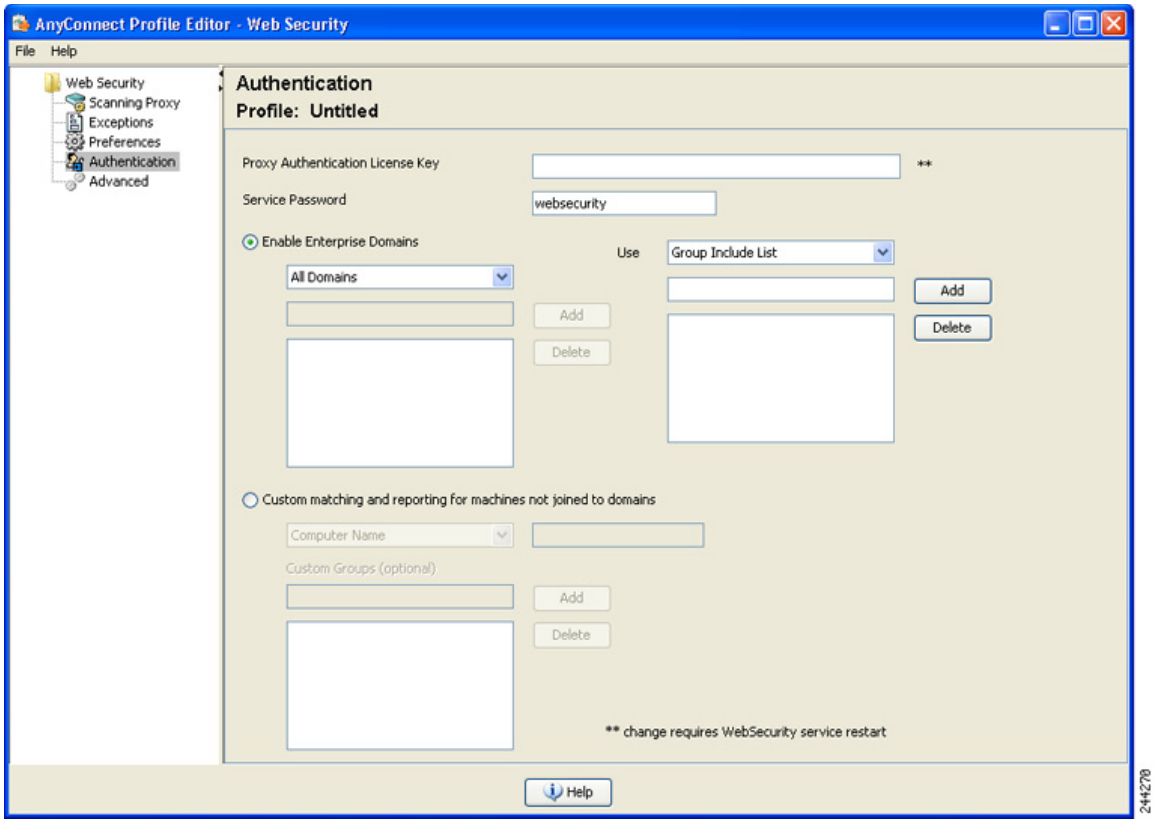
- コンピュータの名前を使用するには、リストの中で [Computer Name] をクリックします。または、ローカル ユーザ名を使用するには、[Local User] をクリックします。または、[Custom Name] をクリックしてカスタム ユーザ名を入力します。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する Cisco ScanCenter レポートで使用されます。
- [Authentication 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。

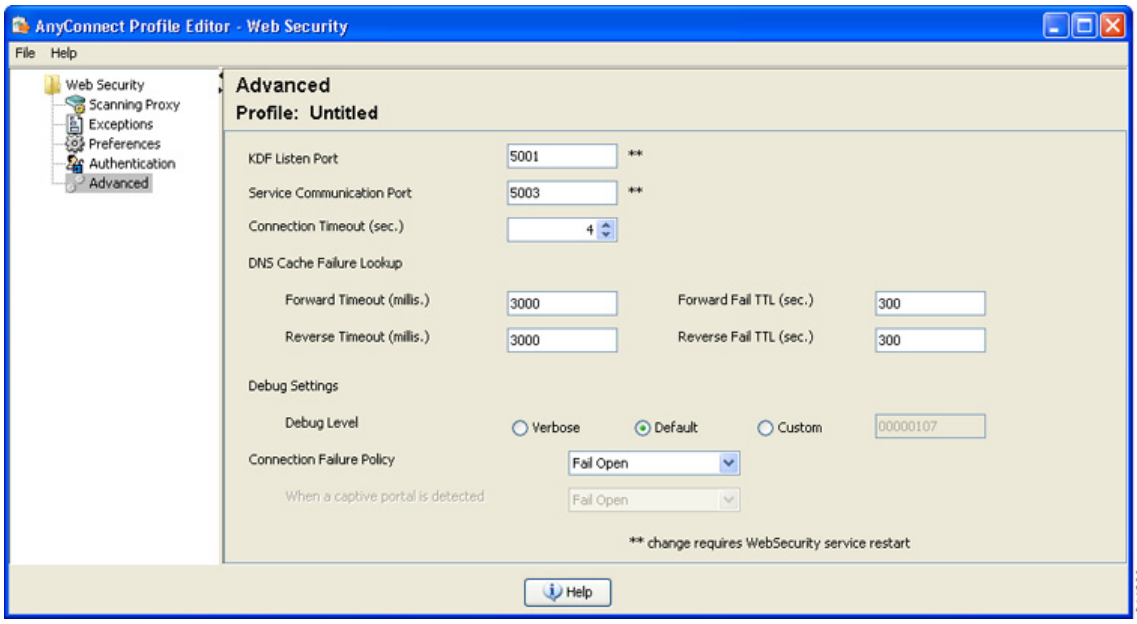
図 6-4　Cisco Cloud Web Security スキャニング プロキシ認証の設定



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。