CHAPTER 7

自動 VPN 実行の構成：Windows のみ

（注） まず初めに、ホワイト ペーパー『Wireless LAN Security』をお読みください。http://www.cisco.com/ja/JP/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_tk809_TSD_Technologies_White_Paper.html から入手できます。このマニュアルは、VPN を使用して無線 LAN のセキュリティを実装する場合のベスト プラクティスを分析しています。サンプル設定については、『Configuring Automatic VPN Initiation on a Cisco VPN Client in a Wireless LAN Environment』の TAC テクニカル ノートを参照してください。セキュア ゲートウェイでのグループまたはユーザ設定、VPN クライアントでの自動実行の構成、Aironet でのワイヤレスの構成を説明した段階的な手順一式が示されています。

自動 VPN 実行（自動実行）は、セキュア ゲートウェイからオンサイト無線 LAN（WLAN）環境でセキュアな接続を実現します。自動実行を VPN クライアントで設定する場合は、VPN クライアントは次を行います。

- ユーザが自分の PC を開始する、または待機または休止状態の PC がアクティブになるとすぐにアクティブになります。
- 自動実行が必要と定義された IP アドレスが PC にあることを検出します。
- ネットワークに定義されたセキュア ゲートウェイへの VPN トンネルを確立し、ユーザに認証を求めて、そのユーザのネットワーク アクセスを許可します。

自動実行は、無線環境向けに設計されていた場合でも、どのネットワーク環境でも使用できます。自動実行は、VPN クライアント PC が特定のネットワークに基づいていても、いなくても接続を自動実行する一般的な方法です。

ほとんどの場合、保存済みの Group and Username パスワードは、この機能のシームレスな性質を最も簡単に表しています。

（注） 自動実行のネットワークを含むおよび除外する自動実行構成を設定できます。

Linux および Mac OS X VPN クライアントは両方とも自動実行をサポートしていますが、ブート時にこの機能を開始するグラフィカル ユーザ インターフェイス コンポーネントまたはサービスは備えていません。これら Windows 以外のクライアントで自動実行を開始する CLI コマンドは **vpnclient autoinit** です。

（注） Windows での自動実行は Start Before Logon 機能の代替機能にはなりません。自動実行はユーザがログインした後にアクティブになります。

図 7-1 は、オンサイト WLAN のセキュリティを確保する VPN を採用した単純なネットワーク構成を示します。この場合のセキュア ゲートウェイである VPN 3000 Concentrator は、ロード バランシングを使用している場合としていない場合があり、非信頼ネットワークと信頼ネットワーク間のゲートウェイとなります。DHCP サーバは VPN 3000 Concentrator の片側に配置できます。無線 NIC カードを搭載したラップトップを持つ VPN クライアント ユーザは、キャンパスや建物のまわりにあるアクセス ポイント（AP）から接続し、非信頼 10.10.10.x ネットワークから信頼 30.30.30.x ネットワークにトンネリングできます。ネットワーク管理者は、多くの場合に VPN クライアント ユーザが意識しなくて済むように、この種類のシナリオを設定できます。

図 7-1　　自動実行のシナリオ

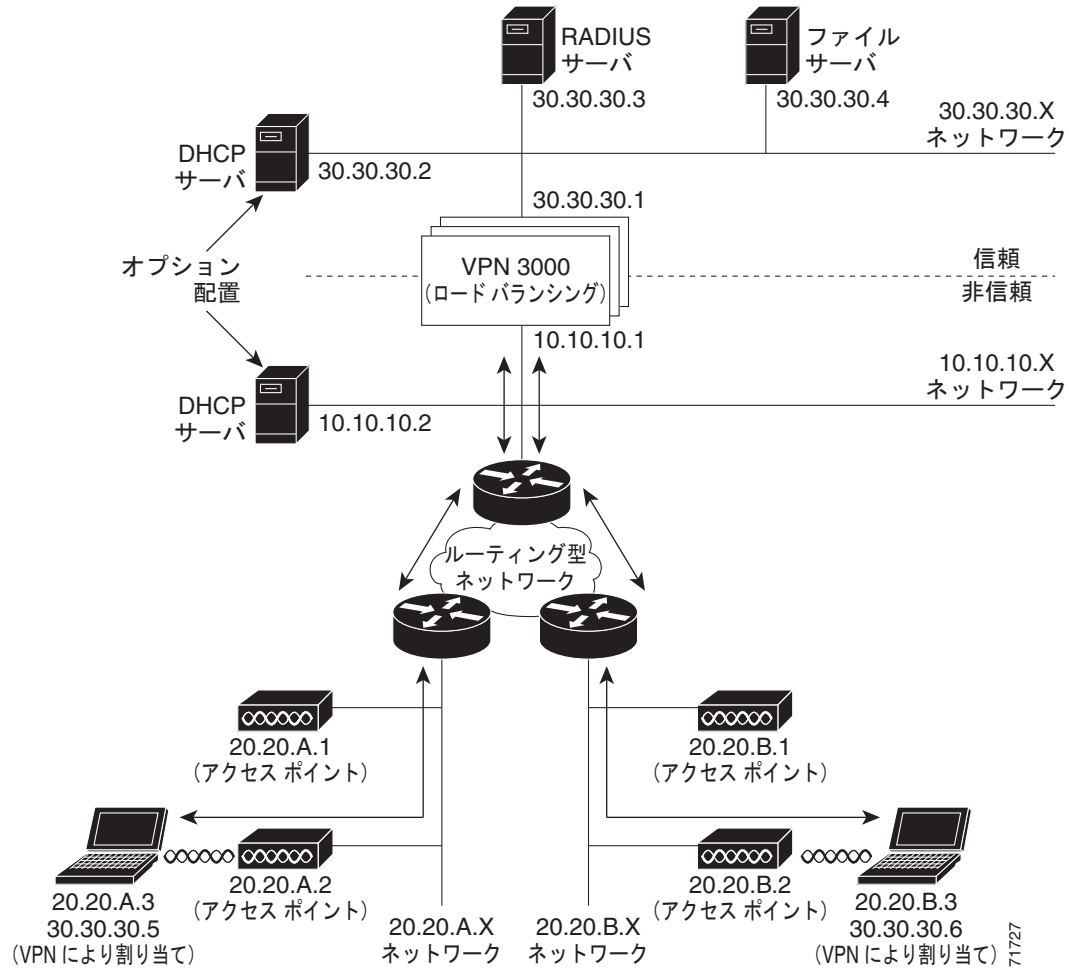

図 7-1 で、ネットワーク番号 30.30.30 という信頼（有線）ネットワークが図の上部にあり、VPN Concentrator により信頼されていないとされる他のネットワークと分けられています。非信頼ネットワークには、20.20.A.x および 20.20.B.x などの無線サブネットが入っています。非信頼ネットワークのすべてのデバイスは、VPN トンネルを使用して信頼ネットワークのリソースにアクセスする必要があります。非信頼ネットワークのデバイスが VPN Concentrator に最初に IP 接続できるよう、DHCP サーバにアクセスできるようにする必要があります。図では、DHCP サーバは VPN Concentrator で DHCP リレーをイネーブルにした状態で信頼ネットワークまたは非信頼ネットワークに配置できるため、任意に配置されています。

ネットワークのユーザに自動実行を構成するには、パラメータを VPN クライアントのグローバル プロファイル（vpnclient.ini）に追加します。グローバル プロファイルの作成方法または使用方法については、「グローバル プロファイルの作成」（P.5-2）を参照してください。

VPN Client GUI を使用して、ユーザは自動実行のイネーブルまたはディセーブル、およびリトライ間隔の変更のみできます。自動実行がグローバル プロファイルで構成された場合、これらの機能は [Options] メニューに表示されます。自動実行が構成されていない場合は、これらのオプションは [Options] メニューには表示されません。自動実行が Windows システムで VPN クライアント ユーザに表示される様子の詳細については、『*Cisco VPN Client User Guide for Windows*』の「Using Automatic VPN Initiation」を参照してください。

自動実行機能は、他のベンダーの NIC カードおよびアクセス ポイントを備えた WLAN 環境で使用できます。

vpnclient.ini ファイルでの自動 VPN 実行の作成

この項では、vpnclient.ini ファイルを作成または編集して、VPN クライアントで自動実行をアクティブにする方法を示しています。

準備

まず初めに、自動実行の構成に必要な次のような情報を収集します。

- クライアント ネットワークのネットワーク IP アドレス
- クライアント ネットワークのサブネット マスク
- ユーザが接続に使用しているすべての接続エントリの名前

実行する手順

自動実行を構成するには、次のキーワードおよび値を vpnclient.ini グローバル プロファイル ファイルの [Main] セクションに追加する必要があります。

- AutoInitiationEnable：自動実行をイネーブルまたはディセーブルにします。自動実行をイネーブルにするには、1 を入力します。ディセーブルにするには、0 を入力します。
- AutoInitiationRetryInterval：自動実行接続をリトライするまでに待つ分数を指定します。値の範囲は 1 ～ 10 分または 5 ～ 600 秒です。このパラメータをファイルに指定しない場合は、リトライ間隔のデフォルト値は 1 分になります。
- AutoInitiationRetryIntervalType：retry AutoInitiationRetryInterval パラメータが分で表示されるか、秒で表示されるかを指定します。デフォルト値は 0（分）です。秒数で示すにはこのパラメータを 1 に設定します。
- AutoInitiationList：一連のセクション名を提供します。各セクション名には、ネットワーク アドレス、サブネット マスク、接続エントリ名、任意で接続フラグが含まれています。セクション（ネットワーク）エントリは最大で 64 個まで含めることができます。
  - セクション名は自動実行リスト中のエントリの（角カッコで囲んだ）名前です。
  - ネットワークおよびサブネット マスクはサブネットを示します。
  - 接続エントリは、自動実行用に設定された接続プロファイル（.pcf ファイル）を指定します。

- 接続フラグがある場合は、一致があった場合に実行するアクションを示します。Connect パラメータが 1 に設定されている場合は、VPN クライアントは自動実行します。0 の場合、VPN クライアントは自動実行しません。デフォルトの設定は 1 秒です。このパラメータはオプションです。このパラメータを使用して、あるネットワーク範囲を自動実行から除外できます。たとえば、モバイル IP と VPN ソフトウェア クライアントがクライアント PC 上で共存しており、企業のサブネットにない場合に VPN クライアントを自動実行するような状況に対処することがあります。

一般的に、Connect パラメータに例外を設定する場合は、除外するネットワーク範囲を自動実行するネットワーク範囲の前に配置します。何よりも、ソフトウェアは vpnclient.ini ファイルで指定された順序でリストを処理します。リスト中のエントリと一致すると、検索は停止し、そのエントリの Connect 設定により自動実行するか何もしないかを判断します。したがって、Connect = 1 エントリを最初に指定すると、ソフトウェアは Connect=0 エントリに到達することはありません。

リスト中のエントリをネットワークとサブネット マスクの一意性で並べることも重要です。より一意のエントリを最初にリストします。たとえば、10.10.200.* で一致を指定するネットワークまたはマスクを持つエントリは、10.10.*.* で一致を指定するネットワークまたはマスクより前に配置します。そうしないと、ソフトエアは 10.10.*.* と一致し、10.10.200.* に到達することはありません。

ネットワークを自動実行から除外する自動実行リストのエントリの例を次に示します。

```
[Franklin]
Network=10.10.200.0
Subnet=255.255.255.0
ConnectionEntry=robron
Connect=0
```

例 7-1　自動実行の vpnclient.ini ファイルのセクション

営業部長が 3 箇所（シカゴ、デンバー、ララミー）に出張して、営業会議に出席し、これらの場所で無線接続を安全かつ簡単に開始したいと考えているとします。vpnclient.ini には、この例で示すエントリが入っています。各ネットワーク セクションで名前が付けられた接続エントリは、そのオンサイト無線 LAN ネットワークの個々のプロファイル（.pcf）をポイントしています。

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=ChicagoWLAN,DenverWLAN,LaramieWLAN
[ChicagoWLAN]
Network=110.110.110.0
Mask=255.255.255.0
ConnectionEntry=Chicago (points to a connection profile named chicago.pcf)
[DenverWLAN]
Network=220.220.220.0
Mask=255.255.255.0
ConnectionEntry=Denver (points to a connection profile named denver.pcf)
[LaramieWLAN]
Network=221.221.221.0
Mask=255.255.255.0
ConnectionEntry=Laramie (points to a connection profile named laramie.pcf)
```

例 7-2　自動実行を除外および含める自動実行の vpnclient ファイルのセクション

この例では、例外は（より具体的には）ネットワーク アドレスは vpnclient.ini ファイルに最初に表示され、次に自動実行の接続エントリが続きます。自動実行の接続エントリでは、Connect パラメータを指定する必要はありません。

```
[Main]
AutoInitiationEnable=1
```

```
AutoInitiationRetryInterval=3
AutoInitiationList=NetworkAExceptions,NetworkA,NetworkBexceptions,NetworkB
[NetworkAExceptions]
Network=192.168.0.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileA1
Connect=0
[NetworkA]
Network=192.0.0.0
Mask=255.0.0.0
ConnectionEntry=VPNprofileA2
[NetworkBExceptions]
Network=161.200.100.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileB1
Connect=0
[NetworkB]
Network=161.200.0.0
Mask=255.255.0.0
ConnectionEntry=VPNprofileB2
```

例 7-3　　常に自動実行を使用する自動実行の vpnclient ファイルのセクション

次の例では、VPN クライアントは、検出されたネットワーク アドレスとは無関係に、常に接続を確立するよう設定されています。

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=NetworkAll
[NetworkAll]
Network=0.0.0.0
Mask=0.0.0.0
ConnectionEntry=VPNprofileName
Connect=1
```

自動 VPN 実行構成の確認

自動実行を正しく構成したかどうか確認するには、VPN Client GUI アプリケーションを開き、次の手順を実行します。

ステップ 1　[Options] メニューを表示し、[Automatic VPN Initiation] を選択します。

ステップ 2　[Automatic VPN Initiation] ダイアログで、[Enable automatic VPN initiation] が選択されていることを確認します。選択されていない場合は、クリックして選択します。

ステップ 3　[Apply] をクリックしてウィンドウを閉じます。

または、コマンド ラインから次のコマンドを実行して、自動実行の構成を確認できます。

vpnclient verify autoinitconfig

各設定の構成情報およびネットワーク エントリのリストが表示されます。

```
C:\Program Files\Cisco Systems>cd VPN Client

C:\Program Files\Cisco Systems\VPN Client>vpnclient verify autoinitconfig
Cisco Systems VPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Auto-initiation Configuration Information.
Enable:          1
Retry Interval: 2 minutes
List Entry  0:  Network:          10.10.32.32
                Mask:             0.0.0.0
                Connect Flag:     1
                Connection Entry: "Engineering"
```

87684