CHAPTER 6

VPN 3000 Concentrator 上での VPN クライアント ソフトウェアのアップデート

VPN クライアント ソフトウェアをアップデートするには 2 通りの方法があります。新しいリリースまたはアップデートを *アップデート サーバ*と呼ばれる Web サーバに配置し、すべてのクライアント タイプ（Linux、Windows、Mac OS X など）のリモート ユーザに対して、アップデート済みソフトウェアの取得場所およびインストール場所を通知することができます。また Windows 2000 および Windows XP のリモート ユーザに対しては、VPN クライアント ソフトウェアをリリース 4.6 から順に自動でアップデートすることもできます。

ここでは、次の項目について説明します。

詳細については、VPN クライアント アップデート ファイルと同じダウンロード場所（www.cisco.com）にある自動アップデートに関するホワイト ペーパーを参照してください。

クライアント アップデートの有効化（すべてのクライアント タイプ）

VPN クライアント ソフトウェアをアップデートするには、VPN Concentrator でクライアント アップデートを有効にする必要があります。クライアント アップデートを有効にすると、VPN クライアント ユーザには適時、それぞれのリモート システム上で VPN クライアント ソフトウェアをアップデートするよう通知されます。このとき、アップデート パッケージの所在も合わせて通知されます（アップデートは自動的には実行されません）。

（注） Web サーバ上の各アップデート フォルダには、シスコのバージョン パッケージが 1 つだけ格納されている必要があります。複数のバージョンが必要な場合は、VPN Concentrator 上で複数のグループを設定し、Web サーバの別々のフォルダからアップデートできるようにしてください。

VPN 3000 Concentrator でのクライアント通知の設定は、次のクライアント アップデートの手順に従って行います。

ステップ 1　クライアント アップデートを有効にするため、[Configuration | System | Client Update] を選択し、[Enable] をクリックします。

ステップ 2　[Configuration | System | Client Update | Enable] 画面で、[Enabled] をオンにし（デフォルト）、[Apply] をクリックします。

ステップ 3　[Configuration | System | Client Update] 画面で、[Entries] をクリックします。

ステップ 4　[Entries] 画面で、[Add] をクリックします。VPN Concentrator Manager に、[Configuration | System | Client Update | Entries | Add] 画面または [Modify] 画面が表示されます。

ステップ 5　[Client Type] に、通知対象となるオペレーティング システムを入力します。

- Windows（Windows ベースのすべてのプラットフォームが対象）。
- WIN9X（Windows 95、Windows 98、および Windows ME の各プラットフォームが対象）。
- WinNT（Windows NT 4.0、Windows 2000、Windows XP、および Windows Vista の各プラットフォームが対象）。
- Linux
- Solaris
- Mac OS X

（注）　VPN 3000 Concentrator では、クライアント アップデート リスト内の各エントリに対して通知メッセージが個別に送信されます。そのため、クライアント アップデート エントリは重複していないことが必要です。たとえば、Windows という値にはすべての Windows プラットフォームが含まれ、WinNT という値には Windows NT 4.0、Windows 2000、および Windows XP の各プラットフォームが含まれています。このため、Windows と WinNT を同時に指定することはできません。クライアント タイプおよびバージョン情報を確認する場合は、シスコ VPN クライアントのメイン ウィンドウの左上隅にある鍵アイコンをクリックし、[About VPN Client] を選択します。

ステップ 6　[URL] フィールドに、通知を表示する URL を入力します。

[VPN Client Notification] の [Launch] ボタンをアクティブにするためには、プロトコルとして HTTP または HTTPS、およびアップデートが置かれているサイトのサーバ アドレスをメッセージに含める必要があります。メッセージには、http://www.oz.org/upgrades/clientupdate など、アップデートのディレクトリおよびファイル名を含めることもできます。リモート ユーザに対して [Launch] ボタンをアクティブにしない場合は、メッセージにプロトコルを含める必要はありません。

ステップ 7　すでに最新ソフトウェアを使用しているためアップデートが不要なクライアント リビジョンのカンマ区切りリストを [Revisions] フィールドに入力します。たとえば、値 4.0 (Rel), `4.0.3` は対応リリースを表します。その他の VPN クライアントはすべてアップグレードの必要があります。

ステップ 8　[Add] をクリックします。

リモート ユーザが VPN デバイスに初めて接続した場合、またはユーザが [Connection Status] ダイアログボックスの [Notification] ボタンをクリックした場合は [Notification] ダイアログボックスが表示されます。通知がポップアップ表示されたら、VPN クライアントの [Notification] ダイアログボックスにある [Launch] をクリックしてデフォルトのブラウザを開き、アップデートが置かれている URL にアクセスします。

Windows 2000 システムおよび Windows XP システムにおける VPN クライアント ソフトウェアの自動アップデート

Windows 2000 および Windows XP 用の VPN クライアント ソフトウェアでは、アップデートおよび新規バージョンを、VPN 3000 Concentrator や通知を発行できるその他の VPN サーバから自動的にトンネルを経由して安全にダウンロードすることができます。

*自動アップデート*と呼ばれるこの機能を使用すると、ユーザは旧バージョンのソフトウェアをアンインストールしてリブートし、新規バージョンをインストールした後再度リブートするという操作が必要なくなります。管理者がアップデートやプロファイルを Web サーバから入手できるようにすることにより、リモート ユーザが VPN クライアントを起動した時点で、ダウンロード対象が入手可能であることをソフトウェアが検出しそれを自動的に取得します。

（メジャー アップグレードの際）新規バージョンに対してリブートが必要なときでも、リモート ユーザがリブートする必要があるのは、プログラムにより旧バージョンがインストールされる場合とダウンロードが完了した場合の 2 回だけです。マイナー アップグレードなど新規バーションに対してリブートが不要な場合は、リブートが不要であるという通知が自動アップグレードによってユーザへ送信されます。また、ユーザが VPN クライアントとの接続解除によりダウンロードを中断した場合、後で再接続すれば、ダウンロードは中断された箇所から再開されます。

自動アップデートの管理

ここでは、VPN クライアント ソフトウェアの自動アップデートに必要なマネージャのタスクについて説明します。通常、管理者が実行するのは次のようなタスクです。

- *アップデート サーバ*と呼ばれる、ダウンロード パッケージを配置するための Web サーバを設定する。パッケージには、シスコが提供する update-x.x.xx.xxxx-minor/major-K9 ファイルが含まれます。この手順の概要は、Web サーバの設定方法をすでに知っているユーザを想定しているため、その手順は含まれていません。
- VPN Concentrator による自動アップデート実行を有効にする。
- シスコから最新バージョン パッケージを取得する。
- 新規プロファイルまたは更新済みプロファイル（.pcf ファイル）が格納されたパッケージであるプロファイル バンドルを作成する（任意）。
- バージョン情報ファイル（new_update_config.ini）の内容を変更する（任意）。
- OEM zip パッケージを作成し、これらのパッケージの名前を new_update_config.ini ファイルに入力する（任意）。

（注） VPN クライアントの自動アップデートは、Windows Vista をサポートしていません。

前提条件

リモート ユーザが自動アップデート機能を使用するためには、それぞれの PC 上に Windows 用の VPN クライアント 4.6 以降がインストールされている必要があります。

自動アップデートに対するクライアント アップデートの有効化

VPN クライアント ソフトウェアの自動アップデートに対し VPN Concentrator 上でクライアント アップデートを設定する手順は、通知機能について説明したクライアント アップデートの有効化（すべてのクライアント タイプ）の中に記載されています。クライアント アップデートの設定方法に関する詳細については、『*Cisco VPN 3000 Series Concentrator Reference, Vol.I: Configuration*』にあるクライアント アップデートについての項を参照してください。

ASDM を使用して Cisco ASA シリーズ 5500 適応型セキュリティ アプライアンス上でクライアント アップデートを設定する方法の詳細については、「ASDM を使用したクライアント ソフトウェア アップデートの設定」（P.2-14）を参照してください。コマンドライン インターフェイスを使用して実行する場合は、「ASDM を使用したクライアント ソフトウェア アップデートの設定」（P.3-10）を参照してください。

VPN 3000 シリーズ Concentrator 上でクライアント アップデートを有効にする場合は、クライアント アップデートの有効化（すべてのクライアント タイプ）の項に記載されている手順を参照してください。

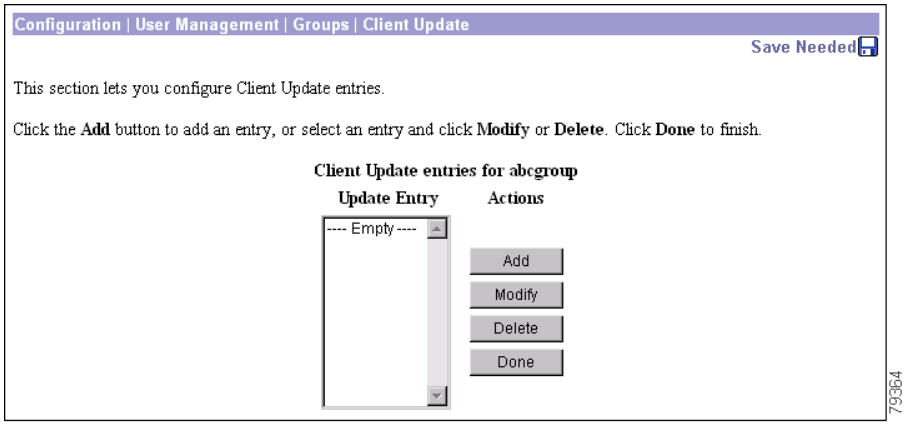
場合によっては、自動アップデートに特化したグループを作成する必要があります。手順は次のとおりです。

ステップ 1　クライアント アップデートを VPN グループ レベルで有効にするため、[Configuration | User Management | Groups] を選択します。

ステップ 2　自動アップデートに特化したグループを新たに追加するため、[Add] をクリックし、グループの名前を入力します。次に、[Apply] をクリックします。[Current] リストに新しいグループが表示されます。この時点で、クライアント アップデート用のグループを選択し、それを修正することができます。

ステップ 3　次に、[Current] リストでクライアント アップデート用のグループを修正するため、そのグループを選択し [Client Update] をクリックします。マネージャに [Client Update] 画面が表示されます。

図 6-1　VPN Concentrator の [Client Update] 画面



ステップ 4　[Client Update | Entries | Add] 画面または [Modify] 画面を表示したら、次のようにして各フィールドに情報を入力します。

a. クライアント タイプ情報を入力します。自動アップデートは Windows 2000 および Windows XP でのみ実行されるため、その他のクライアント タイプではいずれも手動でアップデートが行われます。たとえば WinNT と入力したとします。この場合、Windows 2000 ユーザおよび Windows XP ユーザに対しては自動アップデートが実行されますが、Windows NT ユーザは通知を受け取り、アップデート サーバから手動でアップデートを取得します。

b. アップデート ダウンロード パッケージおよび通知が格納されているアップデート サーバの URL を [URL] フィールドに入力します。URL には、**http://** も含める必要があります（http://update_server_engineering など）。

c. この自動アップデートに対するリビジョンを入力します（update-4.6 など）。

ステップ 5　[Add] または [Apply] をクリックします。

VPN クライアント ソフトウェアでは通知を受け取ると、自動アップデート プログラムが起動し、アップデート済みバージョンおよびプロファイル（存在する場合）のダウンロード元がそのプログラムに渡されます。

シスコのアップデート済みソフトウェアの取得

VPN クライアント ソフトウェアによりアップデート サーバからダウンロードされるインストール パッケージは、完全に新規のリリース（フル インストール）の場合もあれば、アップデートの場合もあります。新規（メジャー）リリースの名前は、update-x.x.xx.xxxx-major-K9.zip という形式であり、マイナー リリースの名前は update-x.x.xx.xxxx.-minor-K9.zip という形式です。最新の VPN クライアント ソフトウェアは次の場所からダウンロードできます。

http://www.cisco.com/cgi-bin/tablebuild.pl/updates

Windows 用の VPN クライアント ソフトウェアのフル リリースにはそれぞれ、次のオブジェクトが必要です。

- vpnclient-win-msi-x.x.int_x-k9.exe：Microsoft インストール ファイル（vpnclient-win-msi-5.0.04.0300-k9.exe または vpnclient-win-msi-5.0.4rel-k9.exe：2000/XP/Vista 用 VPN クライアント ソフトウェア - Microsoft インストーラ、vpnclient-win-msi-5.0.04.0300-k9-jp_wohelp.exe：オンライン ヘルプなし日本版 2000/XP/Vista 用 VPN クライアント ソフトウェア - Microsoft インストーラなど）。
- update-5.0.04.0300-major-K9.zip：Windows 自動アップデート コンポーネントの Zip ファイル。
- 5.0.04.0300 用 ReadMe ファイル。
- sig.dat：binary.zip および MSI インストール ファイルのシグニチャを含むシグニチャ ファイル。このファイルは、2 つのファイルが不正に改ざんされていないことを確認する検証プロセスで使用されます。自動アップデートでは、アップデートのダウンロードが完了した時点でこのファイルは削除されます。
- binary_config.ini：アップデート サーバで入手可能なバージョンが列記されたコンフィギュレーション ファイル。自動アップデートでは、このファイルに基づいて、アップデートを入手する必要があるかどうかが判断されます。このファイル内の最後のメジャー バージョン番号（5.0.4.0300 など）が現在のバージョンよりも大きい場合、自動アップデートではフル インストールがダウンロードされます。それ以外の場合、自動アップデートではバージョン フィールドが参照されます。バージョン番号が PC の現在のバージョン（4.6.1.1 など）よりも大きい場合、自動アップデートではアップデートがダウンロードされます。いずれの場合も、自動アップデートによるアップデート パッケージのダウンロードが完了した時点で、このファイルは削除されます。

- new_update_config.ini：自動アップデート プログラムでは、このオプションのコンフィギュレーション ファイルに基づいてダウンロードするカスタム設定が判断されます。プロファイルおよび OEM パッケージをアップデートに追加する場合、管理者は新規またはアップデート済みのプロファイルおよび OEM パッケージが含まれるファイルの名前を、このファイルに入力する必要があります。自動アップデートによりアップデートが完了すると、このファイルはユーザのシステム上で update_config.ini になります。

これらのオブジェクトのうち、新規またはアップデート済みのプロファイルを配布する際に管理者がアップデートを行うのは new_update_config.ini ファイルのみです。パッケージ内のその他のファイルを修正する必要はありません。これらのファイルはシスコが提供するもので、sig.dat ファイル内のシグニチャにより機密性が確保されています。

アップデート コンフィギュレーション ファイルの新規作成

新規または修正済みのプロファイルを配布する場合、管理者は new_update_config.ini ファイルに情報を入力する必要があります。このファイルの構成は、標準コンフィギュレーション ファイルと同じです（「すべてのプロファイル ファイルに適用されるファイル書式」（P.5-2）を参照）。次に示すのは new_update_config.ini ファイルのサンプルです。

```
[Update]
Version=1
FileName=profiles.zip
MaxSize=7000

[Oem]
FileName=oem.zip
MaxSize=10000

[Transform]
Filename=transform.zip
MaxSize=12000

[Autoupdate]
Required=1
```

new_update_config.ini ファイルのキーワードと値

表 6-1 は、new_update_config.ini ファイルの各構成要素について説明したものです。

表 6-1　new_update_config.ini ファイルのパラメータ

キーワード	説明	値
[Update]	アップデート情報を表すための必須のキーワードです。	ここに示したとおりの表記を使用します。
Version=	アップデート パッケージのバージョン番号です。このファイルの新規バージョンが存在するたびにこの値を 1 ずつ増加させることで、管理者はこのパラメータを使用してアップデートを追跡することができます。	0 以上の値を入力します。

キーワード	説明	値
Filename=	アップデートまたはインストールするプロファイルが含まれる zip ファイルの名前です。	ファイル名（string.zip）を入力します。 例：newprofile.zip
MaxSize=	プロファイル ファイルのサイズ（バイト）に 5000 バイトを加えた値です。これにより、ファイルのサイズの上限が設定されます。	ファイルのサイズに 5000 バイトを加えた値を入力します。 例：10000
MaxSize=	OEM ファイルのサイズ（バイト）に 5000 バイトを加えた値です。これにより、ファイルのサイズの上限が設定されます。	ファイルのサイズに 5000 バイトを加えた値を入力します。 例：12000
[Transform]	MSI インストールに関する OEM 情報を表すためのオプションのキーワードです。	ここに示したとおりの表記を使用します。
FileName=	アップデートするまたはアップデートをインストールするための MSI インストール プログラムに対するトランスフォーム情報が含まれた zip ファイルの名前です。	ファイル名（string.zip）を入力します。 例：newtransform.zip
MaxSize	トランスフォーム ファイルのサイズ（バイト）に 5000 バイトを加えた値です。これにより、ファイルのサイズの上限が設定されます。	ファイルのサイズに 5000 バイトを加えた値を入力します。 例：14000
[Autoupdate]	自動アップデート セクションを表すためのキーワードです。	ここに示したとおりの表記を使用します。
Required=	アップデートまたはプロファイル アップデートを必須にするかどうかを指定します。	0 または 1 のどちらかを入力します。 0：必須でない 1：必須

（注）　MSI インストールを修正するための zip ファイル内のトランスフォームには、oem.mst という名前を付ける必要があります。

プロファイル配布パッケージの作成

新規またはアップデート済みのプロファイルが自動的に配布されるようにするための手順は次のとおりです。

ステップ 1　新規のプロファイル ファイルを作成するか、または現在のプロファイル ファイルを修正します。個別プロファイル（.pcf ファイル）の作成方法および修正方法の詳細については、「接続プロファイルの作成」（P.5-24）を参照してください。

ステップ 2　アップデート済みプロファイルが含まれる zip ファイルを作成し、profiles.zip などの名前を付けます。

ステップ 3　この .zip ファイルの名前を new_update_config.ini ファイルに入力し、このファイルの [Update] セクション内でバージョン番号を 1 だけ大きくします。

（注） プロファイルをアップデートするために VPN クライアントをアップデートする必要はありませんが、VPN クライアントにより新規のプロファイルが受け入れられるためには、シスコから配布されたすべての必須アップデート ファイルがアップデート サーバに格納されていることが必要です。

ステップ 4　new_update_config.ini、および新規プロファイルが含まれている zip ファイルをアップデート サーバにコピーします。

自動アップデートのしくみ

この項で説明する内容は、管理者がこの機能のしくみをより詳しく理解するためのものです。ここでは自動アップデート機能全体について概説します。

自動アップデート機能（*自動アップデート*）は次の 3 つのプロセスで構成されます。

- autoupdate.exe：アップデート サーバ上にアップデート パッケージが存在することを検出すると、アクセスしてそれを取得します。
- autoinstall.exe：アップデート パッケージをインストールします。
- autoupdategui.exe：リモート ユーザへの通知と、通知に対するユーザからの応答を処理します。

具体的に実行される処理は次のとおりです。

- リモート ユーザが VPN クライアントを起動し、トンネルを確立します。
- VPN クライアント ソフトウェアにより、アップデート パッケージが置かれているサイトの URL が取得されます。
- VPN クライアント ソフトウェアにより autoupdate.exe プログラムが開始され、それにアップデート パッケージの URL が渡されます。
- 自動アップデートで、VPN クライアントの PC 上に存在するアップデートとバージョン情報を比較することにより、アップデートが必要かどうかの判断が行われます。
- そのアップデート パッケージが PC 上のアップデート パッケージより新しい場合は、自動アップデートによりアップデート パッケージがダウンロードされます。
- 自動アップデートにより、アップデート パッケージが入手可能であることがリモート ユーザに通知されます。
- リモート ユーザは、アップデート パッケージを受け入れるかまたは拒否します。
- リモート ユーザがアップデート パッケージを受け入れた場合、自動アップデートではそのアップデートの整合性の検証が行われます。
- 自動アップデートにより、アップデート パッケージが解凍され、そのインストールが行われます。
- エラーがある場合は、自動アップデートまたは自動インストールにより、[VPN Client] フォルダの [Updates] フォルダにある autoupdate.log ファイルおよび autoinstall.log ファイルにエラーが記録されます。