APPENDIX C

ユーザ ガイドラインのやりとり

VPN ユーザと次のガイドラインをやりとりするようにしてください。また、ユーザからガイドラインを求められたときに、この項を参考にしてください。内容は、次のとおりです。

Apple MobileMe と AnyConnect との競合

MobileMe のユーザが「Back to my Mac」を設定している場合、AnyConnect の接続問題が発生します。AnyConnect と MobileME の両方が「utun0」という名前の仮想アダプタを使用します。MobileMe は、コンピュータのブート時に AnyConnect よりも前に起動されるため、常に utun0 インターフェイスが最初に使用され、これが原因で Cisco AnyConnect が失敗します。いずれのアプリケーションも、「utun1」などの別のインターフェイスを使用するように設定できません。

Mac ユーザは、AnyConnect VPN に接続する前に「Back to my Mac」をオフにする必要があります。VPN への接続後に、「Back to my Mac」を再度イネーブルにできます。

Mac OS X 10.5 での TUN/TAP エラー メッセージへの対応

Mac OS X 10.5 以前のバージョンに AnyConnect をインストールするときに、次のエラー メッセージが表示されることがあります。

```
A version of the TUN virtual network driver is already installed on this system that is
incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and
prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your
System Administrator, or reference the AnyConnect Release Notes for assistance in
resolving this issue.
```

Mac OS X 10.6 ではこの問題は解決されています。AnyConnect で必要なバージョンの TUN/TAP 仮想ネットワーク ドライバが提供されているためです。

10.6 よりも前のバージョンの Mac OS X には、TUN/TAP 仮想ネットワーク ドライバは組み込まれていないため、AnyConnect は、これらのオペレーティング システムに独自のドライバをインストールします。ただし、Parallels などの一部のソフトウェア、データ カードを管理するソフトウェア、および一部の VPN アプリケーションは、独自の TUN/TAP ドライバをインストールします。AnyConnect インストール ソフトウェアでは、ドライバがすでに存在するという理由で上記のエラー メッセージが表示されますが、そのドライバのバージョンは AnyConnect とは互換性がありません。

AnyConnect をインストールするには、TUN/TAP 仮想ネットワーク ドライバを削除する必要があります。

（注）　TUN/TAP 仮想ネットワーク ドライバを削除すると、システムで最初にドライバをインストールしたソフトウェアに問題が発生するおそれがあります。

TUN/TAP 仮想ネットワーク ドライバを削除するには、コンソール アプリケーションを開き、次のコマンドを入力します。

sudo rm -rf /Library/Extensions/tap.kext

sudo rm -rf /Library/Extensions/tun.kext

sudo rm -rf /Library/StartupItems/tap

sudo rm -rf /Library/StartupItems/tun

sudo rm -rf /System/Library/Extensions/tun.kext

sudo rm -rf /System/Library/Extensions/tap.kext

sudo rm -rf /System/Library/StartupItems/tap

sudo rm -rf /System/Library/StartupItems/tun

これらのコマンドの入力後に、Mac OS を再起動してから、AnyConnect を再インストールします。

未対応 64 ビット版 Internet Explorer

WebLaunch からの AnyConnect のインストールでは 64 ビット版の Internet Explorer はサポートされていません。Windows on x64（64 ビット版）を使用している場合、32 ビット版の Internet Explorer または Firefox を使用して WebLaunch をインストールしてください。現時点では、Firefox は 32 ビット版でのみ使用できます。

Wireless Hosted Network の回避

Windows 7 Wireless Hosted Network 機能を使用すると AnyConnect が不安定になるおそれがあります。AnyConnect の使用時には、この機能をイネーブルにしたり、この機能をイネーブルにするフロントエンド アプリケーション（Connectify や Virtual Router など）を実行したりすることはお勧めしません。

Start Before Logon および DART のインストール

Start Before Logon コンポーネントでは、最初に AnyConnect をインストールしておく必要があります。

SBL または DART が接続しているエンドポイントから手動でアンインストールされている場合、これらのコンポーネントは再インストールされます。ヘッドエンド設定でこれらのコンポーネントのインストールが指定されていて、（エンドポイントに設定されている）プリファレンスでアップグレードが許可されている場合のみ、この動作が発生します。

検疫状態への対応

アクセスに関して企業のポリシーに準拠しないエンドポイントのネットワーク ステータスは、AnyConnect の [接続（Connection）] タブで [隔離済み（Quarantined）] と表示されます。

通常、検疫されたセッションに適用されるダイナミック アクセス ポリシーに割り当てられた ACL では、アンチウイルスおよびアンチスパイウェアのアップデートなど修復サービスへのアクセスのみ許可されます。

検疫状態のセッションでは、エンドポイントの修復に十分な時間が必要です。この時間に続き、ユーザは [再接続（Reconnect）] をクリックし、その状態を終了し新しいポスチャ アセスメントを開始する必要があります。

AnyConnect CLI コマンドを使用した接続

Cisco AnyConnect VPN Client には、グラフィカル ユーザ インターフェイスを使用せずにクライアント コマンドを入力することを希望するユーザ向けに、コマンドライン インターフェイス（CLI）があります。ここでは、CLI コマンド プロンプトの起動方法および CLI で使用可能なコマンドについて説明します。

「クライアント CLI プロンプトの起動」（P.C-3）

「クライアント CLI コマンドの使用」（P.C-3）

「ASA によるセッションの終了時に Windows ポップアップ メッセージを防ぐ」（P.C-5）

クライアント CLI プロンプトの起動

CLI コマンド プロンプトを起動するには、次の手順を実行します。

Windows の場合 : Windows フォルダ C:\Program Files\Cisco\Cisco AnyConnect VPN Client でファイル *vpncli.exe* を見つけます。ファイル *vpncli.exe* をダブルクリックします。

Linux および Mac OS X の場合：フォルダ /opt/cisco/anyconnect/bin/ でファイル ***vpn*** を見つけます。ファイル ***vpn*** **を実行します。**

クライアント CLI コマンドの使用

インタラクティブ モードで CLI を実行する場合、独自のプロンプトが表示されます。コマンド ラインを使用することもできます。表 3-1 に、CLI コマンドを示します。

表 3-1　AnyConnect クライアント CLI コマンド

コマンド	アクション
connect *IP address or alias*	特定の ASA への接続を確立します。
disconnect	前に確立した接続を閉じます。
stats	確立した接続に関する統計情報を表示します。
quit	CLI インタラクティブ モードを終了します。
exit	CLI インタラクティブ モードを終了します。

次の例は、ユーザがコマンド ラインから接続を確立し、終了する例です。

Windows

connect 209.165.200.224
アドレスが 209.165.200.224. のセキュリティ アプライアンスへの接続を確立します。要求されたホストに接続した後、AnyConnect クライアントは、ユーザが属するグループを表示し、ユーザのユーザ名とパスワードを要求します。オプションのバナーを表示するよう指定されている場合、ユーザはバナーに応答する必要があります。デフォルトの応答は **n** で、接続試行を終了します。次に、例を示します。

```
VPN> connect 209.165.200.224
    >>contacting host (209.165.200.224) for login information...
    >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
    >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
    >> notice: Authentication succeeded. Checking for updates...
    >> state: Connecting
    >> notice: Establishing connection to 209.165.200.224.
    >> State: Connected
    >> notice: VPN session established.
VPN>
```

stats
現在の接続の統計情報を表示します。次の例を参考にしてください。

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None

[ Data Transfer ]

    Bytes (sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
```

```
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect
前に確立した接続を閉じます。次の例を参考にしてください。

```
VPN> disconnect
    >> state: Disconnecting
    >> state: Disconnected
    >> notice: VPN session ended.
VPN>
```

quit または **exit**

どちらかのコマンドで、CLI のインタラクティブ モードを終了します。次の例を参考にしてください。

```
quit
goodbye
    >>state: Disconnected
```

Linux または Mac OS X

/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
アドレスが *1.2.3.4* の ASA への接続を確立します。

/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
プロファイルを読み込み、エイリアス *some_asa_alias* を検索してアドレスを探し、ASA への接続を確立します。

/opt/cisco/anyconnect/bin/vpn stats
VPN 接続に関する統計情報を表示します。

/opt/cisco/anyconnect/bin/vpn disconnect
VPN セッションがある場合、接続解除します。

ASA によるセッションの終了時に Windows ポップアップ メッセージを防ぐ

ASA から session reset を発行して AnyConnect セッションを終了すると、次の Windows ポップアップ メッセージがエンド ユーザに表示されます。

```
The secure gateway has terminated the vpn connection. The following message was
received for the gateway: Administrator Reset
```

このメッセージが表示されるのは望ましくないことがあります。たとえば、CLI コマンドを使用して VPN トンネルを開始するときです。クライアントへの接続後にクライアント CLI を再起動することで、このメッセージが表示されるのを防止できます。次に、この作業の実行時の CLI 出力例を示します。

```
C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 3.0.1).
Copyright (c) 2004 - 2011 Cisco Systems, Inc.
All Rights Reserved.
  >> state: Connected
```

```
  >> state: Connected
  >> notice: Connected to asa.cisco.com.
  >> notice: Connected to asa.cisco.com.
  >> registered with local VPN subsystem.
  >> state: Connected
  >> notice: Connected to asa.cisco.com.
  >> state: Disconnecting
  >> notice: Disconnect in progress, please wait...
  >> state: Disconnected
  >> notice: On a trusted network.
  >> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

または、次の場所にあるエンドポイント デバイスでは、Windows レジストリに SuppressModalDialogs という名前の 32 ビットの倍精度値を作成できます。クライアントは名前の有無を検査しますが、値は無視します。

- 64 ビット Windows：

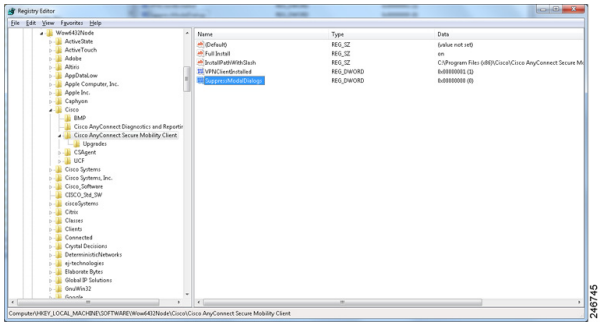
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\
  Cisco AnyConnect Secure Mobility Client

- 32 ビット Windows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

図 C-1 に、64 ビット Windows のレジストリ値を示します。

図 C-1　Windows ポップアップ メッセージを抑制するためのレジストリ値



セキュア接続（Lock）アイコンの設定

Lock アイコンは、セキュアな接続を示しています。Windows XP では、このアイコンは最近使用されていない他のアイコンと同様に自動的に非表示になります。Windows XP でこのアイコンが非表示にされないようにするには、次の手順に従ってください。

ステップ 1　トレイ アイコンが表示されたタスクバーの、かぎカッコ（<）を右クリックします。

ステップ 2　[通知のカスタマイズ ...（Customize Notifications...）] を選択します。

ステップ 3　[Cisco Systems AnyConnect VPN Client] を選択し、[常に表示（Always Show）] に設定します。

Internet Explorer の [接続（Connections）] タブを非表示にする AnyConnect

ある条件では、Internet Explorer の [ツール（Tools）]、[インターネット オプション（Internet Options）] にある [接続（Connections）] タブが非表示になります。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックは接続解除すると反転され、このタブに関する管理者定義のポリシーの方が優先されます。このロックは、次のいずれかの条件で行われます。

- ASA の設定で、[接続（Connections）] タブのロックが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。
- Windows のグループ ポリシーにより、以前に [接続（Connections）] タブがロックされている（**no lockdown** ASA グループ ポリシー設定の上書き）。

Windows Remote Desktop の使用

次の 3 つの方法のうちいずれかを使用して、ネットワーク コンピュータでネットワーク アクセス マネージャによって接続を管理しているときに、そのネットワーク コンピュータにリモートでアクセスできます。

- マシンのみの認証を使用したネットワーク プロファイル
- マシンおよびユーザ認証を使用したネットワーク プロファイル
- ユーザのみの認証を使用したネットワーク プロファイル

マシンのみの認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをマシン認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。ユーザがリモートでログインすると、ネットワーク アクセス マネージャは、マシンのクレデンシャルで認証されたままになります。ユーザのクレデンシャルでの認証またはマシンのクレデンシャルでの再認証は試行されません。

マシンおよびユーザ認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをマシン認証とユーザ認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。ログインしているユーザがいない場合、ネットワーク アクセス マネージャは、マシンのクレデンシャルで認証します。

Vista または Windows 7 の場合、ローカルまたはリモートでユーザがログインすると、ネットワーク アクセス マネージャ認証では最初のユーザ セッションのみが認証され、最初のセッションが持続している間は後続のログイン セッションが無視されます。最初のログイン セッションが終了したら、ネットワーク アクセス マネージャはユーザ接続を停止し、マシン接続に戻します。ネットワーク アクセス マネージャは、最初のセッションが終了したときにセカンダリ セッションが存在したかどうかにかかわらず、元のセッションがユーザ セッションとして終了した後、最初に成功したログイン試行を追跡します。ネットワーク アクセス マネージャは、最初のセッションが動作している間は後続のログイン セッションを無視するため、元のセッションが破棄されたとき、または後続のログインが試行されたときに、最初のセッションの後に作成されたすべてのセカンダリ セッションの接続が一時的に失われます。最初のユーザがローカルでログインした場合、リモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

（注） 最初のログイン ユーザ セッションのみが AnyConnect GUI にアクセスできます。

Windows XP の場合、ローカルでもリモートでもユーザ セッションの数は 1 に制限されています。そのため、新しいユーザがログインすると必ず前のユーザがログオフします。ユーザがローカルでログインした場合、同一ユーザのリモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

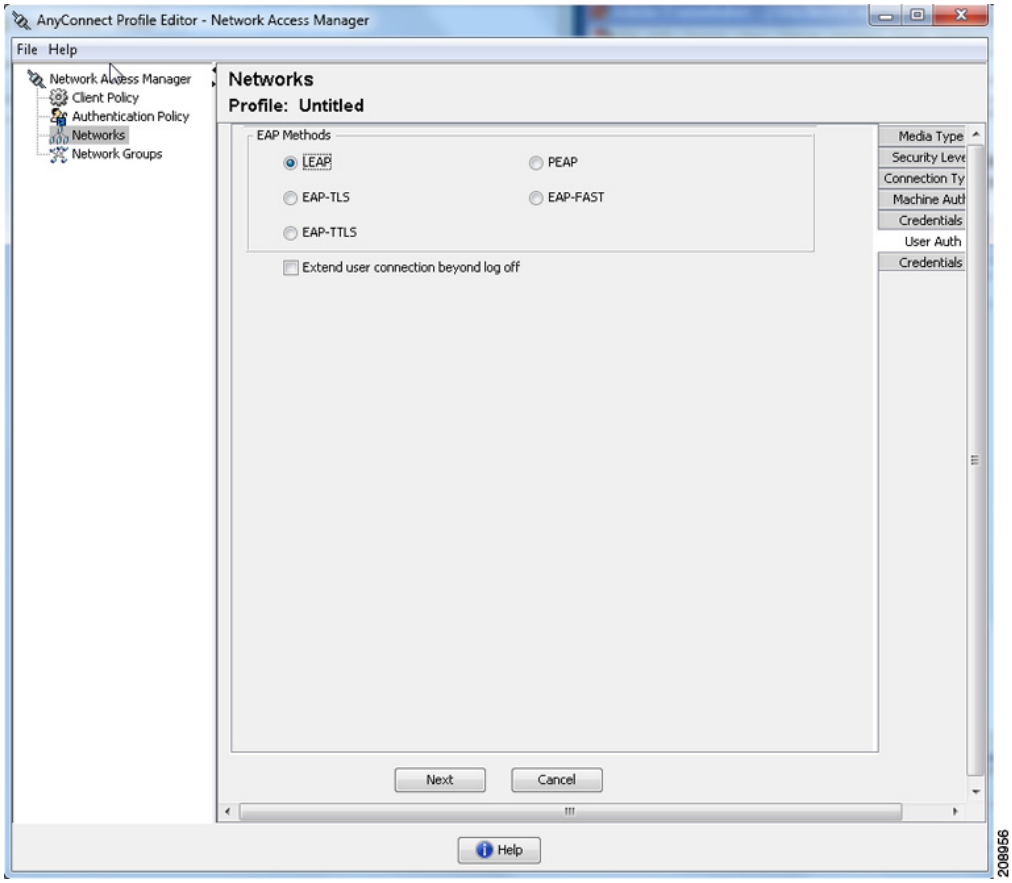
（注） マシン認証とユーザ認証を使用する場合、複雑になる可能性があります。たとえば、設定によっては、マシン プロファイルとユーザ プロファイルは、コンピュータに異なるネットワークを割り当てます（通常は VLAN。ここでは*ユーザ VLAN* と *マシン VLAN* と呼ばれます）。そのため、コンピュータがマシン VLAN 上のマシンとして接続されており（ユーザはログオフ済み）、後からリモートでアクセスされる場合、そのコンピュータはユーザ VLAN として接続します。この理由から、異なる VLAN（ユーザ VLAN）の異なる IP アドレスを使用して、リモート デスクトップ セッションを再確立する必要がある場合があります。

ユーザのみの認証を使用したネットワーク プロファイル

この方法を使用するには、ネットワーク アクセス マネージャをユーザのみの認証用に設定する必要があります。設定の詳細については、「ネットワーク マシンまたはユーザ認証の定義」（P.4-19）を参照してください。通常、この設定を使用し、ログインしているユーザがいない場合、ネットワーク アクセス マネージャはネットワーク接続を確立できません。そのため、リモート デスクトップ接続は不可能です。ユーザがログインしたときに、リモート デスクトップ接続を確立できるようになりました。このリモート セッションによってユーザの再認証は行われません。

extendUserConnectionBeyondLogoff パラメータ（図 C-2 を参照）を使用すると、ローカル ユーザがログオフした後でもアクティブ（接続済み）のままになるようにユーザ認証を設定できます。そのため、リモート デスクトップ機能をサポートするためだけの場合、マシン認証は必要ありません。

図 C-2　[ログオフ後もユーザの接続をアクティブなままにする（Extend User Connection Beyond Logoff）] パラメータの GUI の場所



ユーザのログアウト時にクレデンシャルを必要とする再認証が行われて、ネットワーク アクセス マネージャが必要なクレデンシャル（ユーザ証明書など）にアクセスできなくなっている場合、ネットワーク アクセス マネージャは、接続を再認証できません。その結果、認証の試行はタイムアウトになり、オーセンティケータは最終的にクライアントから切断されます。これが発生すると、ネットワーク アクセス マネージャは、使用可能な接続を再評価して、使用可能なマシン接続からネットワーク接続を作成しようとします。

Vista または Windows 7 の場合、ローカルまたはリモートでユーザがログインすると、ネットワーク アクセス マネージャ認証では最初のユーザ セッションのみが認証され、最初のセッションが持続している間は後続のログイン セッションが無視されます。最初のログイン セッションが終了したら、ネットワーク アクセス マネージャはユーザ接続を停止し、マシン接続に戻します。ネットワーク アクセス マネージャは、最初のセッションが終了したときにセカンダリ セッションが存在したかどうかにかかわらず、元のセッションがユーザ セッションとして終了した後、最初に成功したログイン試行を追跡します。ネットワーク アクセス マネージャは、最初のセッションが動作している間は後続のログイン セッションを無視するため、元のセッションが破棄されたとき、または後続のログインが試行されたときに、最初のセッションの後に作成されたすべてのセカンダリ セッションの接続が一時的に失われます。最初のユーザがローカルでログインした場合、リモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

（注）　最初のログイン ユーザ セッションのみが AnyConnect GUI にアクセスできます。

Windows XP の場合、ローカルでもリモートでもユーザ セッションの数は 1 に制限されています。そのため、新しいユーザがログインすると必ず前のユーザがログオフします。ユーザがローカルでログインした場合、同一ユーザのリモート デスクトップ セッションでこのユーザの再認証が行われることはありません。

マシン認証とユーザ認証を使用する場合、複雑になる可能性があります。たとえば、設定によっては、マシン プロファイルとユーザ プロファイルは、コンピュータに異なるネットワークを割り当てます（通常は VLAN。ここではユーザ VLAN とマシン VLAN と呼ばれます）。そのため、コンピュータがマシン VLAN 上のマシンとして接続されており（ユーザはログオフ済み）、後からリモートでアクセスされる場合、そのコンピュータはユーザ VLAN として接続します。この理由から、異なる VLAN（ユーザ VLAN）の異なる IP アドレスを使用して、リモート デスクトップ セッションを再確立する必要がある場合があります。

Microsoft Vista および Win 7 のクレデンシャル プロバイダー

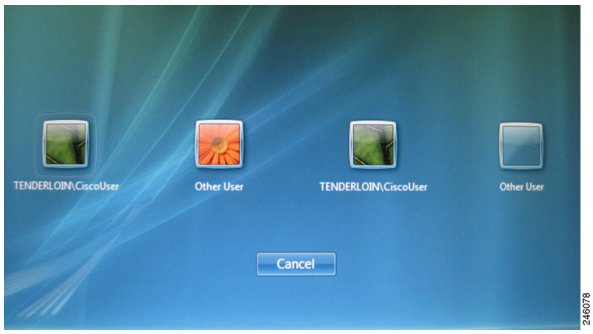
Microsoft Vista および Windows 7 で Windows ログイン クレデンシャルを使用してシングル サインオン（SSO）ユーザ認証を提供するために、ネットワーク アクセス マネージャ モジュールは、パスワード（ログイン）クレデンシャル プロバイダーを実装します。クレデンシャル プロバイダー（CP）は、ログイン プロセス中に Windows クレデンシャルを取り込んで、ネットワーク アクセス マネージャ サービスがマシン認証とユーザ認証を切り替えることができるように、ユーザがシステムにログインしたりシステムからログアウトしたりしたときに通知します。

AnyConnect 3.0 では、ネットワーク アクセス マネージャ CP は、複数のログイン タイル セットが表示されないようにネットワーク アクセス マネージャ CP によってフィルタリングで除外される、Microsoft パスワード クレデンシャル プロバイダーの周囲にラッパーとして実装されます。このフィルタリングが行われない場合、CP ごとにログイン タイルが表示されます。

サードパーティの CP がシステムにインストールされている場合、ネットワーク アクセス マネージャはこれを検出せず、ユーザには複数のログイン タイル セットが表示されることがあります。ユーザがログインのためにサードパーティの CP を選択すると、ネットワーク アクセス マネージャは、Windows クレデンシャルを取得できないため、シングル サインオンのユーザ認証操作を行うことができません。

図 C-3 に、ネットワーク アクセス マネージャ CP とサードパーティ CP の両方をインストールしたシステムからのログイン画面を示します。

図 C-3　オーバーレイなしの AnyConnect アイコン



この問題には、次の 2 つのオプションがあります。

1. ユーザがタイルを区別できるように、ネットワーク アクセス マネージャ CP が、ログイン タイル上に AnyConnect アイコンをオーバーレイするオプションを提供します。小さい AnyConnect アイコンは、ログイン タイル ビットマップの右下隅に配置されます。ユーザにログイン タイル イメージが表示され、AnyConnect がアクティブであることが引き続きわかります。この Anyconnect アイコンがないと、ユーザは、ログイン タイルが AnyConnect によって管理されているかどうかわかりません。

   デフォルトでは、CP は上述のとおり動作します。ユーザは、レジストリで値を変更してディセーブルにでき、CP はログイン タイル上に AnyConnect アイコンをオーバーレイしなくなります。アイコンは、AnyConnect がインストールされていない場合とまったく同じように表示されます。

   このオプションをディセーブルにするには、次のレジストリ値を使用します。

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayIcon]
   ```

   OverLayIcon は REG_DWORD であり、値 0 はオーバーレイ アイコンをディセーブルにし、値 1 はオーバーレイ アイコンをイネーブルにします。このデフォルト値は 1 で、AnyConnect インストーラによって設定されます。レジストリ キーがないか、正しくない場合、CP は値 1 を想定します。

   Windows には、[other users] というラベルのタイルが表示されることがあり、場合によっては関連付けられたタイルには図が表示されません。タイル フレーム内には、タイルが配置されているウィンドウの背景に表示される図が表示されます。そのため、タイルは空であるかトランスペアレントになることがあります。技術的な理由から、CP は、空のタイル上にアイコンをオーバーレイできないため、これが発生した場合 CP は独自のビットマップを提供する必要があります。

   デフォルトでは、CP は、CP 実行可能ファイルに組み込まれたストックのイメージを使用します。ユーザは、図を .bmp ファイルで保存して、ファイルの場所を示すレジストリ文字列値を追加することで、空のストックのタイルの代わりに使用する図を指定できます。

   ビットマップ ファイルの場所を設定するには、次のレジストリ値を追加する必要があります。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
on\Credential Providers\
{B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayEmptyTile]
```

OverlayEmptyTile は、ビットマップ ファイルへのフル パスを含む REG_SZ 値です。
例：「C:\users\jsmith\Pictures\MyEmptyTile.bmp」

（注） ファイルは Windows .bmp ファイルでなければなりません。

（overlayicon レジストリ設定を使用して）オーバーレイがディセーブルになっている場合、OverlayEmptyTile オプションは無視され、ユーザは、アイコン オーバーレイがディセーブルであれば空のタイル ビットマップを指定できません。OverlayEmptyTile 値は AnyConnect インストーラによって指定されません。

図 C-4 に、ネットワーク アクセス マネージャ CP とサードパーティ CP の両方をインストールしたシステムからのログイン画面を示します。この例では、AnyConnect アイコンはログオン タイル上に表示され、ネットワーク アクセス マネージャ CP を示しています。

図 C-4　オーバーレイを使用した Anyconnect アイコン

2. サードパーティのクレデンシャル プロバイダーのログイン タイルが表示されないようにするには、ネットワーク アクセス マネージャ CP はこれらのタイルをフィルタリングで除外できます。

   このオプションを設定するには、次のレジストリ値を追加する必要があります。

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
   on\Credential Providers\ {B12744B8-5BB7-463a-B85E-BB7627E73002}\Filters]
   ```

   フィルタリングで除外する必要があるすべてのクレデンシャル プロバイダーが、Filters キーに特定の GUID を持つキーとして追加されます。

（注） *Filters* 値は Anyconnect インストーラによって指定されません。

GPO が SSO に対して設定されている場合

GPO ワイヤードまたはワイヤレス プロファイルが SSO に対して設定されている場合、winlogon はクレデンシャル プロバイダーの照会プロセスを省略し、ネットワーク アクセス マネージャ CP に加えてネイティブ L2NA クレデンシャル プロバイダーを直接ロードします。これによって、ユーザに 2 つのタイル セットが表示されます。GPO プロファイルが SSO に対して設定されていない場合、ログイン プロセスは予期したとおりに機能し、Microsoft CP はネットワーク アクセス マネージャ CP によってフィルタリングで除外され、ユーザには単一のタイル セットが表示されます。

SmartCard CP

Microsoft Smartcard Credential Provider はネットワーク アクセス マネージャ CP によってラップされないため、プリログイン スマートカード ベースの証明書認証は、AnyConnect 3.0 用の XP 後のプラットフォームではサポートされません。

ネットワーク アクセス マネージャ CP のプリログイン ステータスの表示

クライアント ポリシーの一部として接続設定値 [Before User Logon] が指定されている場合、ネットワーク アクセス マネージャ CP には、接続ステータスをユーザに通知するためのステータス ダイアログボックスが表示されます。このダイアログボックスは、CP がユーザ クレデンシャルを受け取った後で表示され、接続が正常に行われるか、[Time to Wait Before Allowing User to Logon] で選択された値の期限が切れるまで表示されます。このダイアログボックスはいつでもキャンセルできます。

Windows XP で Internet Explorer を実行する暗号の要件

Windows XP では、Internet Explorer ブラウザは AES を使用できず、RC4 または 3DES のいずれかを必要とします。リモート ユーザが SSL 設定ページで RC4 および 3DES をディセーブルにすると、AnyConnect 接続は失敗します。Internet Explorer を使用して AnyConnect 接続を正常に行うには、リモート ユーザは、IE の SSL 設定で唯一の暗号として AES を指定しないでください。