CHAPTER 8

FIPS と追加セキュリティのイネーブル化

Cisco AnyConnect Secure Mobility Client の VPN 機能およびオプションのネットワーク アクセス マネージャとテレメトリ モジュールでは、暗号モジュールを対象とする詳細セキュリティ要件の米国政府規格である連邦情報処理標準（FIPS）140-2 のレベル 1 に対応しています。FIPS 140-2 標準は、暗号ベースのセキュリティ システムを使用してコンピュータおよび遠隔通信システム内の機密情報を保護するすべての政府機関に適用されます。

FIPS 機能は、ASA に対してモデルごとに使用許諾されます。次の AnyConnect クライアント モジュールには、独自の FIPS 設定と要件があります。

- AnyConnect コア VPN クライアント：FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルにある FIPS モード パラメータによってイネーブルにします。このファイルは、セキュリティ設定を含む XML ファイルであり、ASA によって展開されませんが、手動でインストールするか、エンタープライズ ソフトウェア展開システムを使用して展開する必要があります。クライアントの接続先である ASA 用の FIPS ライセンスを購入する必要があります。
- AnyConnect ネットワーク アクセス マネージャ：Windows XP コンピュータのみでサポートされており、AnyConnect クライアント プロファイルでイネーブルにします。ネットワーク アクセス マネージャ用の FIPS サポートのためには、ネットワーク アクセス マネージャと統合された対応ドライバとともに、3e Technologies International から配布される 3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）を展開する必要があります。部品番号 AIR-SSCFIPS-DRV を使用して、FIPS 3eTI CKL 対応ドライバ インストーラをシスコに注文してください（CD で配布）。ドライバおよびサポートされているチップセットについては、AnyConnect ソフトウェア ダウンロード ページにある『*Release Notes for 3eTI Cryptographic Client Software Model 3e-010F-3-IA*』を参照してください。

ここでは、次の項目について説明します。

AnyConnect コア VPN クライアントのための FIPS のイネーブル化

コア AnyConnect セキュリティ モビリティ クライアントの FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルでイネーブルにします。このファイルは、セキュリティ設定を含む XML ファイルであり、ASA によって展開されません。このファイルは、手動でインストールするか、エンタープライズ ソフトウェア展開システムを使用してユーザ コンピュータに展開する必要があります。クライアントの接続先である ASA 用の FIPS ライセンスを購入する必要があります。

AnyConnect ローカル ポリシーのパラメータは、*AnyConnectLocalPolicy.xml* という名前の XML ファイルにあります。このファイルは ASA では導入されません。エンタープライズ ソフトウェア導入システムを使用してこのファイルを導入するか、ユーザ コンピュータ上でファイルを手動で変更する必要があります。

AnyConnect ローカル ポリシーのその他のパラメータは、リモート アップデートを禁止して中間者攻撃を防いだり、管理者またはルート以外のユーザがクライアント設定を修正できないようにしたりすることによって、セキュリティを高めます。

ASA に設定されている SSL 暗号化タイプのリストで、FIPS 準拠の暗号がリストの先頭に設定されていることも確認する必要があります。それ以外の場合は、DTLS 接続が失敗します。

ここでは、AnyConnect コア VPN クライアント用に FIPS モードおよび追加のセキュリティをイネーブルにする方法を示します。次の項目を取り上げます。

Windows クライアントでの MST ファイルを使用した FIPS のイネーブル化

Windows インストールでは、当社が提供する MST ファイルを標準 MSI インストール ファイルに適用して、AnyConnect ローカル ポリシーで FIPS をイネーブルにできます。MST は FIPS をイネーブルにするだけであり、他のパラメータは変更しません。インストール時に、FIPS がイネーブルにされた AnyConnect ローカル ポリシー ファイルが生成されます。

MST のダウンロード元の詳細については、FIPS クライアント用に受け取ったライセンシング情報を参照してください。

独自の MST ファイルを使用した FIPS およびその他のローカル ポリシー パラメータのイネーブル化

独自の MST ファイルを作成して、任意のローカル ポリシー パラメータを変更できます。次のパラメータを使用して、独自の MST ファイルを作成してください。名前は、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のパラメータに対応しています。これらのパラメータの説明と設定可能な値については、表 8-9 を参照してください。

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

（注）　AnyConnect インストールは、ユーザ コンピュータ上にある既存のローカル ポリシー ファイルを自動的には上書きしません。クライアント インストーラで新しいポリシー ファイルを作成するには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

Enable FIPS Tool を使用した FIPS およびその他パラメータのイネーブル化

すべてのオペレーティング システムで、Enable FIPS ツールを使用して、FIPS をイネーブルにした AnyConnect ローカル ポリシー ファイルを作成できます。Enable FIPS ツールはコマンドライン ツールで、実行するには、Windows では管理者権限が必要です。Linux および Mac では、root ユーザとして実行する必要があります。

Enable FIPS ツールのダウンロード元の詳細については、FIPS クライアント用に受け取ったライセンシング情報を参照してください。

表 8-1 に、指定できるポリシー設定と、使用する引数および構文を示します。引数値の動作は、表 8-9 で AnyConnect ローカル ポリシー ファイルのパラメータに指定されている動作と同じです。

Enable FIPS ツールを実行するには、コンピュータのコマンド ラインから **EnableFIPS** <*arguments*> コマンドを入力します。Enable FIPS ツールを使用するときは、次のことに注意してください。

- 引数を何も指定しなかった場合、ツールによって FIPS がイネーブルにされ、vpnagent サービス（Windows）または vpnagent デーモン（Mac および Linux）が再起動されます。
- 複数の引数はスペースで区切ります。

次に、Windows コンピュータ上で実行する Enable FIPS ツールのコマンド例を示します。

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

次に、Linux または Mac コンピュータ上で実行するコマンド例を示します。

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

表 8-1 に、ポリシー設定と Enable FIPS ツールの引数を示します。

表 8-1　ポリシー設定と Enable FIPS ツールの引数

ポリシー設定	引数および構文
FIPS モード	**fm=[true** | **false]**
ダウンローダのバイパス	**bd=[true** | **false]**
WebLaunch の制限	**rwl=[true** | **false]**
厳格な証明書トラスト	**sct=[true** | **false]**
プリファレンス キャッシングの制限	**rpc=[Credentials** | **Thumbprints** | **CredentialsAndThumbprints** | **All** | **false]**
Firefox NSS 証明書ストアの除外（Linux および Mac）	efn=[true | false]
PEM ファイル証明書ストアの除外（Linux および Mac）	**epf=[true** | **false]**
Mac ネイティブ証明書ストアの除外（Mac のみ）	**emn=[true** | **false]**

ローカル ポリシー内のローカル ポリシー パラメータの手動変更

AnyConnect ローカル ポリシー パラメータを手動で変更するには、次の手順に従ってください。

ステップ 1　クライアント インストールから、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のコピーを取得します。

表 8-2 は、各オペレーティング システムのインストール パスを示しています。

表 8-2　オペレーティング システムと AnyConnect ローカル ポリシー ファイルのインストール パス

オペレーティング システム	インストール パス
Windows 7	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client[1]
Linux	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect

1. AnyConnect 3.0 では、Windows Mobile をサポートしていません。このパスは、AnyConnect 2.5 のローカル ポリシー ファイル用です。

ステップ 2　パラメータ設定を編集します。次の例は、Windows の AnyConnect ローカル ポリシー ファイルの内容を示しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
```

```
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

ステップ 3　ファイルを *AnyConnectLocalPolicy.xml* として保存し、エンタープライズ ソフトウェア展開システムを使用してこのファイルをリモート コンピュータに展開します。

ASA で FIPS 準拠の SSL 暗号化を使用するための設定

デフォルトでは、ASA に対する AnyConnect の SSL 接続は、データグラム トランスポート層セキュリティ（DTLS）を使用します。これにより、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。ASA に設定されている SSL 暗号化のリストに指定されている暗号が、この接続用に指定される暗号です。

デフォルトでは、ASA 上の SSL 暗号化リストは、次の暗号を次の順序で含みます。

- RC4-SHA1
- AES128-SHA1（FIPS 準拠）
- AES256-SHA1（FIPS 準拠）
- 3DES-SHA1（FIPS 準拠）

したがって、ASA は、デフォルトでは、*FIPS 準拠でない* RC4-SHA1 をこの接続用に指定します。FIPS 準拠にするには、FIPS 準拠の暗号が SSL 暗号化リストの先頭に指定されていることを確認する必要があります。それ以外の場合は、DTLS 接続が失敗します。さらに、接続が失敗しないように、FIPS に準拠しないすべての暗号をリストから削除することをお勧めします。

SSL 暗号化タイプを指定するために、ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [詳細（Advanced）] > [SSL 設定（SSL Settings）] に移動します。[暗号化（Encryption）] エリアで、FIPS 準拠の暗号をリストの先頭に移動します。

CLI を使用している場合は、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用して、リストを順序付けしてください。

AnyConnect FIPS のレジストリ変更によるエンドポイントに関する問題の回避

コア AnyConnect クライアント用に FIPS をイネーブルにすると、エンドポイント デバイスのシステム全体に影響します。AnyConnect は、エンドポイント上の Windows レジストリの設定値を変更します。エンドポイント上の他のコンポーネントでは、AnyConnect が FIPS をイネーブルにしたことを検出でき、同じく暗号化の使用を開始できます。たとえば、リモート デスクトップ プロトコル（RDP）では、サーバで FIPS 準拠の暗号化を使用している必要があるため、Microsoft Terminal Services クライアントの RDP は機能しません。

これらの問題を回避するために、パラメータ [暗号化、ハッシュ、および署名の FIPS 準拠アルゴリズムの使用（Use FIPS compliant algorithms for encryption, hashing, and signing）] を [無効（Disabled）] に変更することにより、[Windows ローカル システム暗号化（Windows Local System Cryptography）] 設定で、FIPS 暗号化を一時的にディセーブルにできます。

エンドポイント デバイスをリブートすると、この設定が変更されてイネーブルに戻ることに注意してください。

表 8-3 に、AnyConnect によって実行される、注意を要する Windows レジストリの変更を示します。

表 8-3　AnyConnect で FIPS をイネーブルにしたときに実行される Windows レジストリ キーの変更

Windows のバージョン	レジストリ キー	行われるアクション
Windows XP 以降	HKLM\System\CurrentControlSet\Control\Lsa	FIPSAlgorithmPolicy が 0 から 1 に変更されます。

Windows のバージョン	レジストリ キー	行われるアクション
Windows Vista 以降	HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy	Enabled が 0 から 1 に変更されます。
	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。
	HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。 これにより、1 つのグループ ポリシーに対する TLSv1 が設定されます。

ソフトウェア ロックおよびプロファイル ロックのイネーブル化

ソフトウェア ロックまたはプロファイル ロックを使用すると、許可した ASA からだけソフトウェアまたはクライアント プロファイルの更新を取得するように、クライアントを制限できます デフォルトでは、ロックはディセーブルです。AnyConnect クライアントは、ソフトウェアまたはクライアント プロファイルの更新を任意の ASA から受信できます。

ソフトウェア ロックがイネーブルの場合、クライアントでは、その ASA が許可サーバのリストにあることを確認してから、コア VPN クライアントおよび任意のオプション クライアント モジュール（ネットワーク アクセス マネージャ、テレメトリ、Web セキュリティなど）を更新します。ASA にロードされているクライアントのバージョンがエンドポイント上のクライアントよりも新しい一方で、その ASA がソフトウェア ロックのサーバのリストにない場合、エンドポイント クライアントは接続できません。クライアント バージョンが同一の場合、エンドポイント クライアントはその ASA に接続できます。

プロファイル ロックがイネーブルの場合、クライアントでは、同じリストを確認してから、VPN などのモジュールのクライアント プロファイルを更新します。その ASA がリストにない場合、クライアントはその ASA に接続しますが、プロファイルは更新しません。この場合は、次の機能を使用できません。

- サービスのディセーブル化
- 証明書ストアの上書き
- 事前接続メッセージの表示
- ローカル LAN へのアクセス
- Start Before Logon
- ローカル プロキシ接続
- PPP 除外
- 自動 VPN ポリシー
- 信頼ネットワーク ポリシー
- 非信頼ネットワーク ポリシー
- 信頼できる DNS ドメイン
- 信頼できる DNS サーバ
- 常時接続
- キャプティブ ポータルの修復
- スクリプト化
- ログオフ時の VPN の保持
- 必要なデバイス ロック
- 自動サーバ選択

AnyConnect のアップグレード

ASA に接続したときに新しい AnyConnect クライアント パッケージが提供されている場合、クライアントでは、まず、ローカル ポリシー ファイル内の*許可サーバ リスト*にあるサーバ名またはグローバル プリファレンス ファイルから取得した*デフォルト ドメイン*と、ASA 名を比較することにより、その

ASA が許可サーバであるかどうかを判別します。ASA が許可サーバである場合、クライアントは、すべてのモジュールをダウンロードしてコア VPN クライアントのアップグレードを起動し、プラグイン ディレクトリを削除して再作成します。これにより、現在インストールされているすべてのオプション モジュールがディセーブルになります。

コア VPN クライアントのアップグレードが終わると、その ASA で指定されているオプション モジュールがアップグレードされます。すでにインストールされている一方で、ASA で指定されていないモジュールは、アップグレードされずにディセーブルのままになります。クライアントでは、VPN プロファイルや、エンドポイント コンピュータでサポートされている他のサービス プロファイルを含む、すべてのプロファイルのダウンロードも行います。

その ASA が許可サーバでない場合、クライアントでは、ソフトウェア ロックおよび VPN プロファイル ロックを確認します。許可されていない場合、ダウンロードされるクライアント プロファイルは VPN プロファイルだけになります。オプション モジュールのプロファイルは、ロックの状態を問わず、ダウンロードされません。

（注） その ASA が許可されていない場合、ネットワーク アクセス マネージャ、テレメトリ、Web セキュリティ プロファイルは、プロファイル ロックを問わず、その ASA にダウンロードされません。

許可されていない ASA への接続

ソフトウェア ロックがオンの場合、クライアントでは、いずれのアップグレードも行わないで切断します。ソフトウェア ロックがオフの場合、クライアントでは、ASA にあるオプション モジュールのリストを無視し、現在システム上にインストールされている全モジュールのリストを *VPNmanifest.dat* ファイルから取得して、そのモジュールだけを ASA からアップグレードします。したがって、この許可されていない ASA で指定されている新規モジュールはいずれもインストールされず、ASA にあるモジュールはいずれもイネーブルにされませんが、現在エンドポイント コンピュータにインストールされているモジュールはディセーブルになりません。

ソフトウェア ロックは、ダウンロード、カスタマイズ、ローカライズ、スクリプト、トランスフォームも制御します。ソフトウェア ロックがオンの場合、これらは、許可されていない ASA からダウンロードされません。したがって、企業外資産に対してスクリプトを介したポリシーの適用が行われていないことを確認する必要があります。

（注） 企業資産および企業外資産の両方が特定の 1 つの ASA に接続し、この ASA でポリシーを適用するためのスクリプトを展開する場合、そのスクリプトは、ソフトウェア ロックがオンの企業外資産では実行されません。これに対処するには、該当する企業外資産のユーザを、ASA 上で別のグループ ポリシーに分離します。

VPN プロファイル ロックがオフの場合、クライアントでは、VPN プロファイルのみを取得して保存します。オンの場合、VPN プロファイルはダウンロードされません。クライアントは、プロファイルなしで接続を続行し、その結果、多くの機能が使用不可になります。

異なるモジュールがイネーブルにされている同一バージョン

許可されている ASA に接続し、モジュールが変更されていることを確認したクライアントは、その ASA で指定されているすべての新規モジュールをダウンロードしてインストールします。コア VPN クライアントが更新されていない場合、プラグイン ディレクトリは削除されません。したがって、インストールされており、ASA に指定されていないモジュールは、イネーブルのままになります。

許可されていない ASA の場合、クライアントでは、いずれの新規モジュールもインストールせず、その ASA で指定されているいずれのモジュールもディセーブルにしません。

コア VPN クライアントのアンインストール

コア VPN クライアントを手動でアンインストールする場合は（Windows の [プログラムの追加または削除（Add or Remove Programs）] を使用）、インストールされているコア VPN クライアントのバージョンにかかわらず、オプションのすべてのクライアント モジュールもアンインストールされます。

デフォルトの許可ドメイン

クライアントが ASA に初めて接続するとき、グローバル プリファレンス ファイルには、デフォルト ドメインの値が設定されていません。値がなく、許可サーバ リストが空の場合は、現在の ASA ドメイン名（ASA 名からホスト名を除去した値）が、デフォルト ドメインとしてグローバル プリファレンス ファイルに追加されます。たとえば、ASA が vpn.newyork.example.com の場合は、以下の行がグローバル プリファレンス ファイルに追加されます。

```
<DefaultDomain>example.com</DefaultDomain>
```

デフォルト ドメインは、ローカル ポリシー ファイルの許可サーバのリストにあるかのように、許可された ASA として扱われます。ローカル ポリシーに定義されている設定の方が、デフォルト ドメインよりも優先されることに注意してください。したがって、ソフトウェア管理システム（または他の何らかの方法）を使用して、許可サーバのリストを含む新しいローカル ポリシー ファイルを展開する場合、デフォルト ドメインは無視されます。

プロファイル ロックがオフのときの許可されていない ASA への接続

常時接続機能がイネーブルにされている許可されていない ASA にクライアントが接続し、ローカル ポリシーで VPN プロファイル ロックがオフの場合は、古いプロファイルが削除されてクライアントはその ASA に再接続できません。したがって、企業資産の検出にホスト スキャンを使用するか、適切なグループ パーティションをイネーブルにしてある場合は、企業外資産およびゲストに対して常時接続機能を強制しないように注意してください。

ロギング

ダウンローダは、ダウンロード履歴を記録する個別のテキスト ログ（UpdateHistory.log）を作成します。このログは、更新時刻、クライアントを更新した ASA、更新されたモジュール、インストールされているバージョン（アップグレードの前および後）を含みます。このログ ファイルは、次の場所に保存されます。

%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs ディレクトリ。

ソフトウェア ロックおよびプロファイル ロックのための XML タグ

次のテキストは、ローカル ポリシー ファイルの一例です。ソフトウェア ロックおよびプロファイル ロックのための XML タグは、UpdatePolicy タグの間に配置されます。これらのタグは、次の例では、太字で示してあります。

許可サーバは、<AuthorizedServerList> タグの間にリストします。サーバは、FQDN または IP アドレスのいずれかを 1 つ含むことができます。ワイルド カードを含むこともできます。例：newyork.example.com、*.example.com、または 1.2.3.*

（注） リモート ユーザによる接続にサーバの IP アドレスを使用するには、必ず、許可サーバ リストに IP アドレスをリストしてください。ユーザが IP アドレスを使用して接続しようとしたときに、サーバが FQDN でリストされている場合、この試行は、許可されていないドメインへの接続として扱われます。

たとえば、サーバ名 *seattle.example.com* および *newyork.example.com* は、許可サーバの FQDN です。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
        <AuthorizedServerList>
            <ServerName>seattle.example.com</ServerName>
            <ServerName>newyork.example.com</ServerName>
        </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

ソフトウェア ロックの使用例

表 8-4、表 8-5、表 8-6、表 8-7 に、同一バージョンおよび異なるバージョンのクライアント パッケージをインストールした、許可されているか許可されていない ASA に接続するクライアントの使用例を示します。

表 8-4　新しい AnyConnect パッケージをインストールした、許可された ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、X、Y がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。	A、B、C が ASA にロードされているバージョンで更新されます。 ASA にロードされているバージョンの D がインストールされます。	A および B が ASA にロードされているバージョンで更新されます。 ASA にロードされているバージョンの X および Y がインストールされます。 C はディセーブルになりますが、インストールされたまま残り、アップグレードされません。	A および B が ASA にロードされているバージョンで更新されます。 C はディセーブルになりますが、インストールされたまま残り、アップグレードされません。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。	A、B、C が更新されます。 C はイネーブルになります。 D がインストールされます。	A および B が更新されます。 X および Y がインストールされます。 C はディセーブルのままとなり、更新されません。	A および B が更新されます。 C はディセーブルのままとなり、更新されません。

表 8-5　新しい AnyConnect パッケージをインストールした、許可されていない ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、X、Y がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオフ。	A、B、および C が ASA にロードされているバージョンで更新されます。 D はダウンロードされません。	A および B が ASA にロードされているバージョンで更新されます。 この ASA で指定されていない場合でも C は更新されます。 X および Y はダウンロードされません。	A および B が ASA にロードされているバージョンで更新されます。 この ASA で指定されていない場合でも C は更新されます。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。 ソフトウェア ロックはオフ。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。	A および B が ASA にロードされているバージョンで更新されます。 C は更新されず、ディセーブルのままになります。
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオン。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。 ソフトウェア ロックはオン。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。	モジュールはダウンロードも更新もされず、クライアントは接続解除されます。

表 8-6　同じバージョンでモジュールの異なる AnyConnect パッケージをインストールした、許可され ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、D がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。	D がダウンロードされインストールされます。 A、B、C、D がインストールされ、イネーブルにされます。	D がダウンロードされインストールされます。 C は、ディセーブルにされません。 A、B、C、D がインストールされ、イネーブルにされます。[1]	モジュールはダウンロードされません。 A、B、および C はイネーブルのままになります。
A、B、C がインストールされている。 C は以前の更新によりディセーブルになっている。	D がダウンロードされインストールされます。 A、B、および D がインストールされイネーブルにされます。 C はディセーブルのままになります。[2]	D がダウンロードされインストールされます。 A、B、および D がインストールされイネーブルにされます。 C はディセーブルのままになります。	モジュールはダウンロードされません。 A、および B はイネーブルのままになります。 C はディセーブルのままになります。

1. C をディセーブルにするには、[Disable Service] をイネーブルにしたクライアント VPN プロファイルを展開する必要があります。
2. C をイネーブルにできるのは、新しい AnyConnect パッケージをロードする場合で、C がイネーブルにされているときだけです。

表 8-7　同じバージョンでモジュールが異なる AnyConnect パッケージをインストールした、許可されていない ASA への接続

最初にインストールされているクライアント モジュール	モジュール A、B、C、D がイネーブルの ASA	モジュール A、B、D がイネーブルの ASA	モジュール A、B がイネーブルの ASA
A、B、C がインストールされ、イネーブルになっている。 ソフトウェア ロックはオフまたはオン。	モジュールはダウンロードされません。 A、B、および C はイネーブルのままになります。	モジュールはダウンロードされず、ディセーブルにもなりません。 A、B、および C はイネーブルのままになります。	モジュールはディセーブルになりません。 A、B、および C はイネーブルのままになります。

ソフトウェアおよびプロファイルのロックの例

次のシナリオ例では、クライアント PC 上および ASA 上の AnyConnect パッケージのバージョンを変えながら、クライアント アップグレード動作について説明します。表 8-8 に、3 台の ASA に対する AnyConnect パッケージのバージョンを示します。

表 8-8　ASA および AnyConnect クライアントの例に関する情報

ASA	ロードされている AnyConnect パッケージ	ダウンロードするモジュール
seattle.example.com	バージョン 3.0.0350	VPN、ネットワーク アクセス マネージャ、Web セキュリティ
newyork.example.com	バージョン 3.0.0351	VPN、ネットワーク アクセス マネージャ
raleigh.example.com	バージョン 3.0.0352	VPN、ポスチャ、テレメトリ

この例を続けます。ローカル ポリシー XML ファイルは、次の内容です。

```
<UpdatePolicy>
    <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
    <AuthorizedServerList>
        <ServerName>seattle.example.com</ServerName>
        <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
</UpdatePolicy>
```

このローカル ポリシーによると、ソフトウェア ロックは*オフ*、VPN プロファイル ロックは*オン*です。

AnyConnect クライアント ユーザは、まず、seattle.example.com に接続します。次に、VPN、ネットワーク アクセス マネージャ、Web セキュリティがインストールされます（バージョン 3.0.0350 によってサポートされているすべてのモジュール）。次に、ユーザは newyork.example.com に接続します。これは、新しいバージョン（バージョン 3.0.0351）を実行している許可された ASA です。ASA はプラグイン ディレクトリを削除し、VPN およびネットワーク アクセス マネージャをバージョン 3.0.0351 にアップグレードします。Web セキュリティはバージョン 3.0.0350 のままとなり、ディセーブルになります。

次に、ユーザは、許可サーバ リストにない raleigh.example.com に接続します。ソフトウェア ロックはオンではないため、VPN およびネットワーク アクセス マネージャは 3.0.0352 にアップグレードされます。ただし、指定されているその他のモジュール（ポスチャおよびテレメトリ）はインストールされません。Web セキュリティはバージョン 3.0.0350 のままとなり、ディセーブルになります。

VPN プロファイル ロックはオンであるため、VPN クライアント プロファイルはダウンロードされません。raleigh-example.com は許可サーバでないため、その他のサービス プロファイルもダウンロードされません。

AnyConnect ローカル ポリシーのパラメータと値

（注）　プロファイル ファイルのポリシー パラメータを省略した場合、機能はデフォルト動作になります。

表 8-9 に、AnyConnect ローカル ポリシー ファイルのパラメータとその値を示します。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値

パラメータおよび説明	値および値の形式
acversion このファイルのすべてのパラメータを解釈できる AnyConnect クライアントの最小バージョンを指定します。指定されているバージョンよりも古いクライアントがファイルを読み取った場合、クライアントはイベント ログ警告を発行します。	形式は acversion="<version number>" です。
xmlns XML 名前空間指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xmlns=http://schemas.xmlsoap.org/encoding/
xsi:schemaLocation スキーマ ロケーションの XML 指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">
xmlns:xsi XML スキーマ インスタンス指定子です。ほとんどの場合、管理者はこのパラメータを変更しません。	形式は URL です。例： xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
FipsMode クライアントの FIPS モードをイネーブルにします。クライアントは、FIPS 標準で承認されているアルゴリズムおよびプロトコルだけを使用します。	*true*：FIPS モードをイネーブルにします。 *false*：FIPS モードをディセーブルにします（デフォルト）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
BypassDownloader ダイナミック コンテンツのローカル バージョンの存在を検出し、アップデートする VPNDownloader.exe モジュールの起動をディセーブルにします。	*true*：クライアントは、翻訳、カスタマイズ、オプション モジュール、コア ソフトウェアの更新などのダイナミック コンテンツが ASA 上にあるかどうかをチェックしません。ただし、クライアントでは、クライアントの VPN クライアント プロファイルと、ASA 上のグループ ポリシーと関連付けられているプロファイルの比較を試みます。 *false*：クライアントは、ASA 上にダイナミック コンテンツがあるかどうかをチェックします（デフォルト）。 クライアントが ASA に接続しようとする場合、クライアントと ASA には同じ VPN クライアント プロファイルをインストールしておく必要があります。VPN クライアント プロファイルが同じでない場合、クライアントは選択された ASA AnyConnect 接続プロファイルに割り当てられた VPN クライアント プロファイルをダウンロードしようとします。**BypassDownloader** が **true** に設定されている場合、VPN クライアント プロファイルはダウンロードされません。 VPN クライアント プロファイルがダウンロードされないと、次のいずれかが発生します。 • ASA の VPN クライアント プロファイルがクライアント上のプロファイルと異なっている場合、クライアントは接続を中止します。ASA の VPN クライアント プロファイルにより定義されたポリシーが実施されないためです。 • ASA に VPN クライアント プロファイルが存在しない場合でもクライアントは VPN 接続を行いますが、クライアントにハードコードされた VPN クライアント プロファイル設定を使用します。 **（注）** ASA でクライアント プロファイルを設定する場合は、BypassDownloader を *true* に設定した ASA に接続する前に、クライアント プロファイルをクライアントにインストールしておく必要があります。プロファイルには管理者が定義したポリシーを含めることができるため、BypassDownloader 設定 *true* は、ASA を使用してクライアント プロファイルを集中管理しない場合に限りお勧めします。
RestrictWebLaunch WebLaunch の使用を禁止し、強制的に AnyConnect FIPS 準拠のスタンドアロン接続モードでユーザを接続することで、ユーザが FIPS 準拠でないブラウザを使用して AnyConnect トンネルの開始に使用するセキュリティ クッキーを取得しないようにします。	*true*：WebLaunch の試行は失敗し、クライアントからユーザに情報メッセージが表示されます。 *false*：WebLaunch を許可します（デフォルト。AnyConnect 2.3 以前と同じ動作）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
StrictCertificateTrust リモート セキュリティ ゲートウェイを認証するときに、AnyConnect は確認できない証明書を許可しません。クライアントでは、これらの証明書を受け入れるようユーザにプロンプトを表示するのではなく、自己署名証明書を使用したセキュリティ ゲートウェイへの接続を失敗します。 **（注）** 以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストをイネーブルにすることを、強くお勧めします。 – 明確な悪意を持った攻撃が増えているため、ローカル ポリシーで厳格な証明書トラストをイネーブルにすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザが接続している場合に「中間者」攻撃を防ぐために役立ちます。 – 完全に検証可能で信頼できる証明書を使用する場合でも、AnyConnect クライアントは、デフォルトでは、未検証の証明書の受け入れをエンド ユーザに許可します。エンド ユーザが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエンド ユーザにプロンプトが表示されます。エンド ユーザによるこの判断を回避するには、厳格な証明書トラストをイネーブルにします。	*true*：クライアントから自己署名証明書を使用するセキュリティ ゲートウェイへの接続が失敗し、次のメッセージが表示されます。 `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.` *false*：クライアントは、証明書を受け入れるようにプロンプトを表示します（デフォルト。AnyConnect 2.3 以前と同じ動作）。
RestrictPreferenceCaching AnyConnect は機密情報をディスクにキャッシュしないように設計されています。このパラメータをイネーブルにすると、AnyConnect プリファレンスに保存されているすべての種類のユーザ情報に、このポリシーが拡張されます。	*Credentials*：ユーザ名および第 2 ユーザ名はキャッシュされません。 *Thumbprints*：クライアントおよびサーバ証明書のサムプリントはキャッシュされません。 *CredentialsAndThumbprints*：証明書のサムプリントおよびユーザ名はキャッシュされません。 *All*：自動プリファレンスはいずれもキャッシュされません。 *false*：すべてのプリファレンスがディスクに書き込まれます（デフォルト。AnyConnect 2.3 以前と同じ動作）。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
RestrictTunnelProtocols（現在はサポート対象外） 特定のトンネル プロトコル ファミリを使用して ASA への接続を確立することを禁止します。	*TLS*：クライアントは IKEv2 および ESP のみを使用してトンネルを確立します。セキュア ゲートウェイへの情報伝達に、TLS/DTLS は使用しません。 *IPSec*：クライアントは、認証およびトンネリングに TLS/DTLS だけを使用します。 *false*：接続の確立で、任意の暗号化プロトコルを使用できます（デフォルト）。 （注）　TLS またはその他のプロトコルの使用を禁止した場合、Secure Desktop の自動アップグレードなど、一部の拡張機能が使用できなくなる場合があります。
ExcludeFirefoxNSSCertStore（Linux および Mac） クライアントが Firefox NSS 証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。ストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。	true：*Firefox NSS 証明書ストアを除外します。* *false*：Firefox NSS 証明書ストアを許可します（デフォルト）。
ExcludePemFileCertStore（Linux および Mac） クライアントが PEM ファイル証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。FIPS 対応の OpenSSL を使用するストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。PEM ファイル証明書ストアを許可することで、リモート ユーザは FIPS 準拠の証明書ストアを使用することになります。	*true*：PEM ファイル証明書ストアを除外します。 *false*：PEM ファイル証明書ストアを許可します（デフォルト）。
ExcludeMacNativeCertStore（Mac 専用） クライアントが Mac ネイティブ（キーチェーン）証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。	*true*：Mac ネイティブ証明書ストアを除外します。 *false*：Mac ネイティブ証明書ストアを許可します（デフォルト）。
ExcludeWinNativeCertStore （Windows 専用。現在はサポート対象外） クライアントが Windows Internet Explorer ネイティブ証明書ストアを使用してサーバ証明書を確認することを、許可または除外します。	*true*：Windows Internet Explorer 証明書ストアを除外します。 *false*：Windows Internet Explorer 証明書ストアを許可します（デフォルト）。
AllowSoftwareUpdateFromAnyServer 任意の ASA からのソフトウェア更新を許可するか、クライアントに制限を加えて、許可した ASA からのみソフトウェアを取得するようにします。	*true*：任意の ASA からの AnyConnect クライアント用ソフトウェア更新を許可します（デフォルト）。 *false*：AuthorizedServerList セクションに指定された ASA からの AnyConnect クライアント用ソフトウェア更新だけを許可します。
AllowVPNPolicyUpdateFromAnyServer 任意の ASA からの VPN ローカル ポリシー ファイルへの更新を許可するか、クライアントに制限を加えて、許可した ASA からのみ更新を取得するようにします。	*true*：任意の ASA からの AnyConnect クライアント用 VPN ローカル ポリシー ファイルの更新を許可します（デフォルト）。 *false*：AuthorizedServerList セクションに指定された ASA からの AnyConnect クライアント用 VPN ローカル ポリシー ファイル更新だけを許可します。

表 8-9　AnyConnect のローカル ポリシー ファイルとその値 （続き）

パラメータおよび説明	値および値の形式
AuthorizedServerList AnyConnect クライアント ソフトウェアまたは VPN ローカル ポリシー ファイルの更新を許可されたサーバのリスト。	サーバ名は、ServerName を使用してリストします。
ServerName ローカル ポリシー ロックのソフトウェアに対するサーバ名。	AnyConnect クライアントで、ソフトウェアまたは VPN ローカル ポリシー ファイルの更新を受信できるサーバの名前です。ServerName には、FQDN、IP アドレス、ドメイン名、またはワイルドカードを含むドメイン名を使用できます。

ローカル ポリシー ファイルの例

次に、AnyConnect ローカル ポリシー ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

ネットワーク アクセス マネージャに対する FIPS のイネーブル化

ネットワーク アクセス マネージャに対する FIPS 準拠は、Windows XP のみでサポートされており、AnyConnect クライアント ネットワーク アクセス マネージャ プロファイルで FIPS モードをイネーブルにする必要と、FIPS ネットワークに接続しているユーザ コンピュータに 3eTI FIPS Certified Crypto Kernel Library（CKL）を展開する必要があります。

ネットワーク アクセス マネージャを FIPS 準拠に設定してあっても、ユーザは FIPS 準拠でないネットワークに接続できます。ただし、ユーザが FIPS 準拠のネットワークに接続する場合、ネットワーク アクセス マネージャは 3eTI FIPS CKL を使用し、AnyConnect GUI の [ネットワーク アクセス マネージャ（Network Access Manager）] ペインに FIPS 準拠のステータスを表示します（レジストリ キー *FIPSAlgorithmPolicy* が非ゼロの場合）。

この章では、ネットワーク アクセス マネージャの FIPS 準拠をイネーブルにする方法を説明します。次の項目を取り上げます。

- 「ネットワーク アクセス マネージャでの FIPS モードの適用」（P.8-19）
- 「AnyConnect GUI を使用した FIPS ステータス レポートのイネーブル化」（P.8-19）
- 「3eTI ドライバのインストール」（P.8-20）
- 「3eTI ドライバ インストーラ ソフトウェアの入手」（P.8-33）

（注）　ネットワーク アクセス マネージャの FIPS 準拠は、Windows XP を実行しているユーザ コンピュータ上でのみサポートされています。

ネットワーク アクセス マネージャでの FIPS モードの適用

AnyConnect プロファイルのネットワーク アクセス マネージャの設定セクションで、許可する関連付け、暗号化モード、認証方式を制限することにより、企業の従業員に対して FIPS 準拠のネットワークのみへの接続を許可できます。

ネットワーク アクセス マネージャの FIPS 準拠では、WPA2 パーソナル（WPA2-PSK）、WPA2 エンタープライズ（802.1X）などの FIPS 認定の AES 暗号化方式をサポートしています。

ネットワーク アクセス マネージャの FIPS サポートには、EAP メソッド EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-FAST が含まれています。

ネットワーク アクセス マネージャを使用すると、FIPS 準拠の WLAN プロファイルと、クライアント VPN セキュリティをイネーブルにした Wi-Fi ホットスポットへのアクセスなど、オプションの非準拠のコンフィギュレーションの両方をサポートできます。管理者は、ネットワークで FIPS がイネーブルにされているかどうかがわかるように、プロファイルに適切な名前を付ける必要があります。

ソリューションを FIPS に完全に準拠させるには、3 つのコンポーネントが必要です。

- ネットワーク アクセス マネージャ
- サポートされている NIC アダプタ ドライバを含む 3eTI FIPS 認定の Crypto Kernel Library（CKL）
- FIPS 準拠のネットワーク プロファイル設定

ネットワーク アクセス マネージャ プロファイル エディタで、FIPS モードをイネーブルにできます。詳細については、「クライアント ポリシーの設定」（P.4-5）を参照してください。

AnyConnect GUI を使用した FIPS ステータス レポートのイネーブル化

AnyConnect GUI の [ネットワーク アクセス マネージャ（Network Access Manager）] ペインには、FIPS ステータス インジケータがあります。FIPS ステータス インジケータをイネーブルにするには、エンドポイント コンピュータ上の次のレジストリ キーに非ゼロの値を設定する必要があります。

HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy

FIPS 統合

確実に FIPS 準拠のソリューションにするには、FIPS 準拠の EAP タイプまたは WPA2 パーソナル（事前共有キー）による AES 暗号化との WPA2 ハンドシェイクのみを許可する、ネットワーク プロファイルをセットアップする必要があります。

ネットワーク アクセス マネージャの Log Packager ユーティリティは、3eTI パケットのログを収集します。

3eTI CKL ドライバ インストーラ

3eTI FIPS 認定の CKL およびサポートされているドライバをインストールする手順については、「3eTI ドライバのインストール」（P.8-20）を参照してください。

3eTI ドライバのインストール

ここでは、完結した FIPS ソリューションを実現するために、ネットワーク アクセス マネージャと統合されたサポートされているドライバとともに、3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）をインストールする手順を説明します。

特記事項

1. 3eTI CKL ドライバ インストーラは、任意の時点で 1 つのシステムに 1 つの 3eTI ワイヤレス ドライバのみをインストールできるように設計されています。異なるタイプのドライバをインストールするには、事前に、それまでのドライバをアンインストールする必要があります。同じタイプのドライバの場合は、今回のインストールで既存のドライバを更新するのみであるため、それまでのドライバをアンインストールする必要はありません。
2. ハードウェアが存在しており、システムに取り付けられている場合、インストーラでは、3eTI CKL をサポートする、3eTI で加工済みのドライバで、対応する OEM ワイヤレス NIC アダプタ ドライバを更新します。

3eTI CKL ドライバ インストーラの概要

3eTI CKL ドライバ インストーラは、次のいずれかの方法で開始できます。

- .exe ファイルのダブルクリック：インストーラを実行する前に NIC アダプタが PC に取り付けられている、通常のドライバ インストールの場合のみ使用可能です。
- コマンドライン オプションを付けないインストーラ コマンドを使用：通常のドライバ インストールの場合のみ使用可能です。
- コマンドライン オプションを付けたインストーラ コマンドを使用：通常のドライバ インストールおよび事前インストール ドライバ インストールで使用可能です。

.exe ファイルをダブルクリックするか、コマンドライン オプションを付けないコマンドの実行を使用してドライバ インストーラを開始した場合、インストーラでは、以下の操作を実行します。

- FIPS 操作のために、サポートされている NIC アダプタ ドライバとともに、3eTI CKL を検出してインストールします。
- 3eTI CKL をサポートしている NIC アダプタが複数検出された場合、インストーラでは、アダプタ選択のプロンプトをユーザに出します。
- 互換性のある NIC アダプタが PC 上に見つからない場合、インストーラはインストールを中止し、次のエラー メッセージを表示します。

  FIPS サポートを実現する NIC チップセットを自動検出できません。プリインストールを強制的に実行するには、コマンド ラインを使ってインストーラを実行する必要があります。操作方法または詳細については、ネットワーク管理者にお問い合わせください。（The installer cannot auto-detect a NIC chipset to provide FIPS support. To enforce a pre-installation, you are required to run the installer using the command line.For instructions or further assistance, please contact your network administrator.）

（注） 事前インストール シナリオは、具体的なインストール オプションを指定できるコマンドライン オプションを使用する場合に最適です。事前インストール方式は、通常は初心者ユーザではなく、ネットワーク管理者が実施します。

インストーラ コマンドおよびコマンドライン オプション

インストーラでは、次のコマンドおよびコマンドライン オプションをサポートしています。

3eTI-drv-installer.exe -s -auto Type= XXXX

-s	ユーザにプロンプトを出さないサイレント インストールを実行する場合に使用します。
-auto	インテリジェント インストールを実行する場合に使用します。インテリジェント インストールでは、インストーラが PC 内のサポートされている NIC アダプタを判別し、適切なドライバをインストールします。これにより、インストーラは、コマンドライン オプションを付けないでコマンドを入力した場合と同じ操作を実行します。
Type=*XXXX*	事前インストールまたは通常インストール用の NIC アダプタ チップセットを指定するために使用します。 *事前インストール*は、指定した NIC アダプタを PC に取り付ける前に、ドライバをインストールすることを意味します。 *通常インストール*は、ドライバをインストールする前に NIC アダプタを取り付けることを意味します。

XXXX の値	**説明**
Intel3945	Intel3945 チップセット用のドライバを指定します。
Centrino	Intel 2100、l2200、2915 チップセット用のドライバを指定します。
Broadcom	インストーラによってサポートされている Broadcom チップセット用のドライバを指定します。
Atheros	Atheros 5001、5004、5005、AR5211、AR5212 チップセット用のドライバを指定します。
Cisco	Atheros チップセットを搭載した Cisco AIR-CB21 カード用のドライバを指定します。

（注） -s を使用してサイレント インストールを実行する場合は、-auto または Type=XXXX か、-auto と Type=XXXX の両方も指定する必要があります。

次に、例を示します。

- *-auto* と *-s* の併用：
  - 取り付けられている NIC アダプタを自動検出して、インテリジェント インストールを実行します
  - ユーザにプロンプトを出さないサイレント インストールを実行します。
  - 複数の NIC アダプタが検出された場合は、サポートされている任意のチップセットを選択します。
- *-auto* と *Type=XXXX* の併用：
  - Type=XXXX で指定された NIC アダプタ チップセット用のドライバのインストールを試行します。
  - 検出された NIC アダプタが指定されたチップセットをサポートしていない場合は、サポートされているチップセットを搭載した任意の NIC アダプタ用のドライバをインストールします。

- *3eTI-drv-installer.exe Type=Intel3945 -auto -s* の使用：
  - ユーザにプロンプトを表示せずに、Intel3945 チップセット用ドライバのインストールを試行します。
  - Intel3945 チップセットを搭載した NIC アダプタが検出されない場合は、サポートされているチップセットを搭載した、他の任意の検出された NIC アダプタ用のドライバをサイレント インストールします。
  - サポートされているチップセットを搭載した NIC アダプタが検出されない場合は、いずれのドライバも事前インストールしません。
- *3eTI-drv-installer.exe Type=Intel3945 -s* を使用：
  - ユーザにプロンプトを表示せずに、Intel3945 チップセット用ドライバのインストールを試行します。
  - サポートされている NIC アダプタ チップセットが検出されない場合は、指定されたチップセット ドライバをインストールすることにより、事前インストールを実行します。

コマンドライン オプションを使用しないインストーラの実行

NIC アダプタを PC に取り付けて通常インストールを実行するには、次の手順を実行します。

ステップ 1　次のいずれかの手順を実行して、インストーラを開始します。

a. Windows エクスプローラを使用して、PC 上の **3eTI-drv-installer.exe** ファイルを見つけ、ファイル名をダブルクリックします。

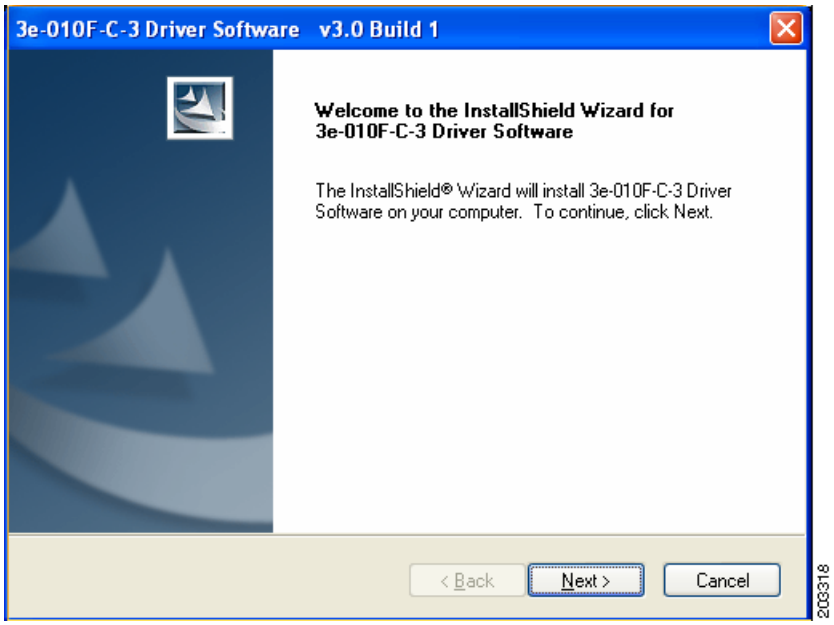
b. [スタート（Start）] > [ファイル名を指定して実行（Run）] をクリックし、次のインストーラ実行コマンドを入力します。

path **/ 3eTI-drv-installer.exe**

ここでの *path* は、インストーラ ファイルのディレクトリ パスです。

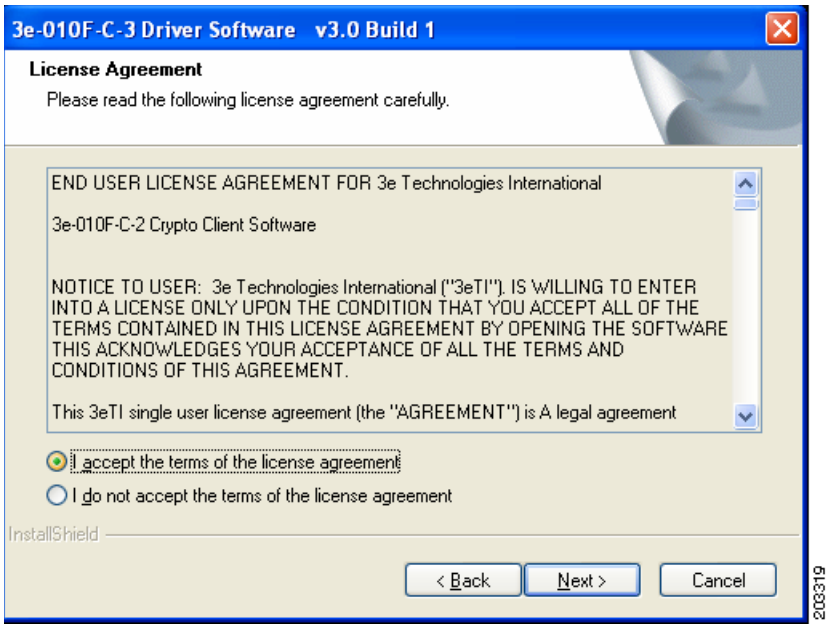
[ドライバへようこそ（Driver Welcome）] ウィンドウが表示されます（図 8-1）。

図 8-1　[ドライバへようこそ（Driver Welcome）] ウィンドウ



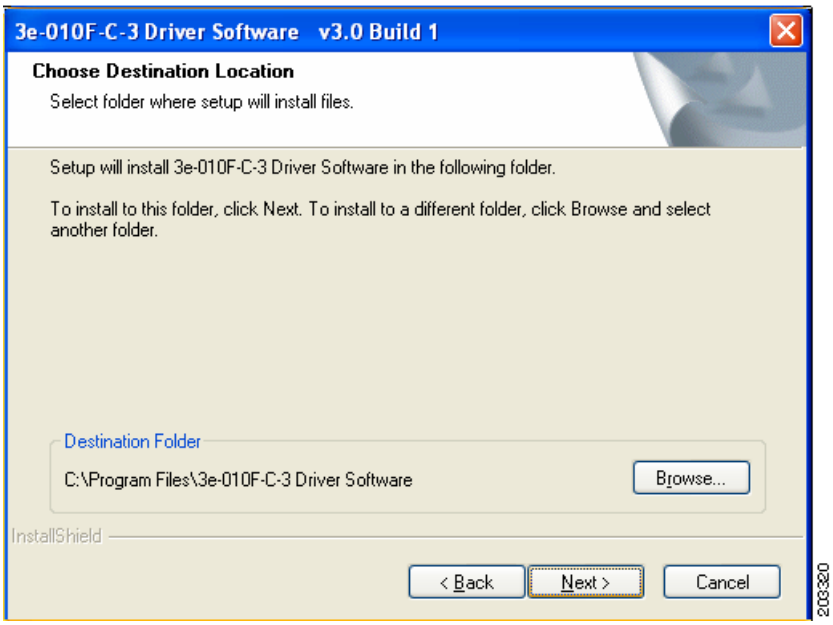
ステップ 2　[次へ（Next）] をクリックすると、ライセンス契約書が表示されます（図 8-2 を参照）。

図 8-2　ライセンス契約書（License Agreement）



ステップ 3　使用許諾契約を読み、同意して、[次へ（Next）] をクリックします。図 8-3 が表示されます。

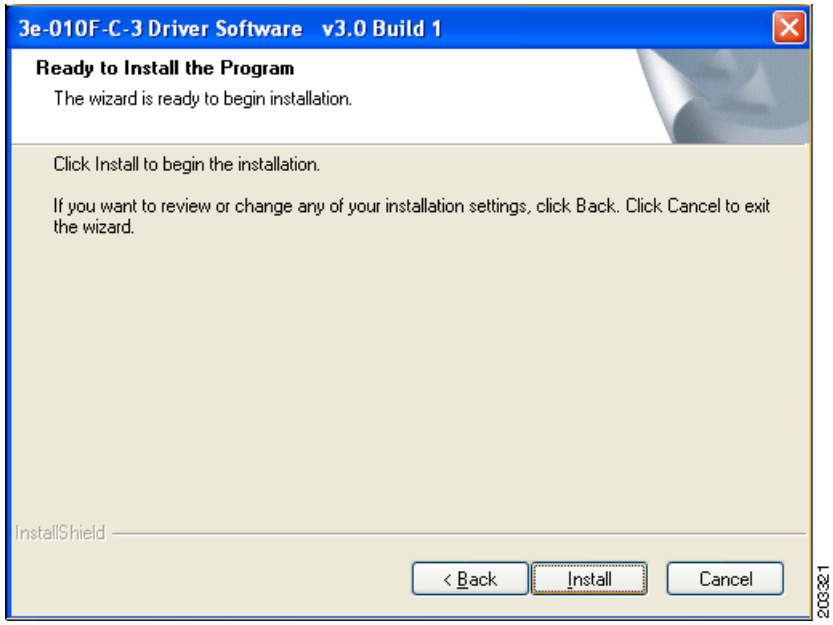
図 8-3　[インストール先の場所（Destination Location）] ウィンドウ



ステップ 4　ドライバ ソフトウェアのデフォルトの宛先フォルダを受け入れるか、[参照（Browse）] をクリックして目的のフォルダを探します。

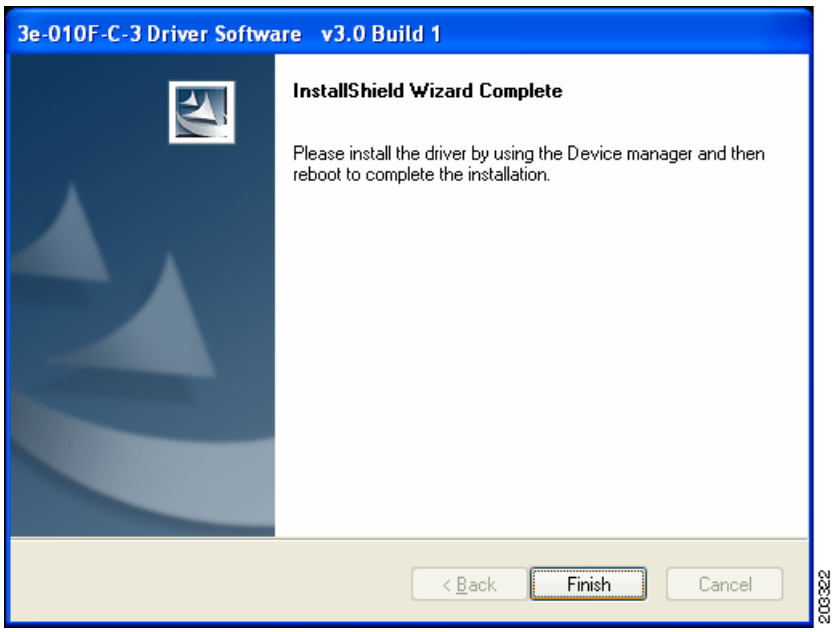
ステップ 5　[次へ（Next）] をクリックすると、図 8-4 が表示されます。

図 8-4　[インストールの準備完了（Ready to Install）] ウィンドウ



ステップ 6　[インストール（Install）] をクリックして、インストール プロセスを開始します。インストールが完了すると、図 8-5 が表示されます。

図 8-5　[ウィザードの完了（Wizard Complete）] ウィンドウ



ステップ 7　[完了（Finish）] をクリックします。

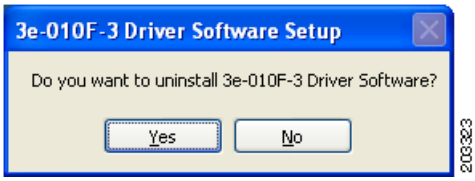
以前の 3eTI ドライバ ソフトウェアのアンインストール

以前の 3eTI ドライバ ソフトウェアをアン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　以前の 3eTI ドライバ ソフトウェアをアンインストールするには、[スタート（Start）] > [設定（Settings）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] をクリックします。

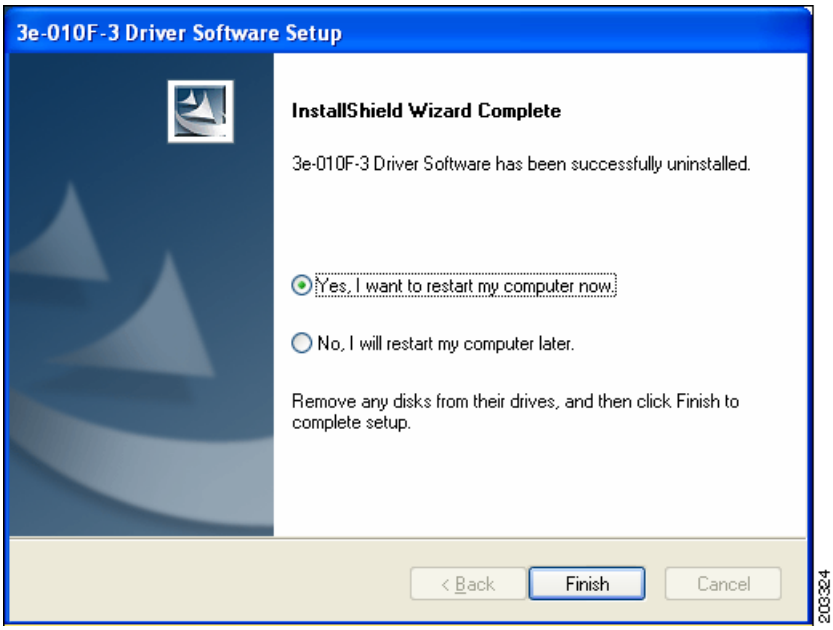
ステップ 2　3e-010F-3 などの 3eTI ドライバ ソフトウェアを選択し、[削除（Remove）] をクリックします。ポップアップ ウィンドウが表示されます（図 8-6 を参照）。

図 8-6　[ドライバー ソフトウェアのアンインストール（Uninstall Driver Software）] ポップアップ



ステップ 3　[Yes] をクリックして、ドライバ ソフトウェアをアンインストールします。図 8-7 が表示されます。

図 8-7　[今すぐコンピューターを再起動する（Restart Computer Now）] ウィンドウ



ステップ 4　コンピュータを再起動するには、[はい（Yes）] をオンにします。

ステップ 5　[完了（Finish）] をクリックします。ドライバ ソフトウェアを完全に削除するために、PC がリブートします。

企業における展開でのドライバのサイレント インストール

サイレント モードを使用してインストーラを実行するには、次の手順を実行します。

ステップ 1　次のコマンドを入力してインストーラを実行します。

path **/ 3eTI-drv-installer.exe -s Type=***XXXX*

説明：

path はインストーラ ファイルへのディレクトリ パスです。

-s は、サイレント インストールを示します。

Type= *XXXX* は、Centrino、Intel3945、Cisco などのチップセットを指定します（「インストーラ コマンドおよびコマンドライン オプション」（P.8-21）を参照）。

ドライバ インストールの進行中を示すポップアップ ステータス ウィンドウが表示され、インストールが完了すると非表示になります。

事前に取り付けたネットワーク アダプタのないドライバのインストール

NIC アダプタを取り付けていない PC に対して 3eTI ドライ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　[スタート（Start）] > [ファイル名を指定して実行（Run）] をクリックし、次のインストーラ実行コマンドを入力して、インストーラを開始します。

path **/ 3eTI-drv-installer.exe Type =** *XXXX*

説明：

path はインストーラ ファイルへのディレクトリ パスです。

Type= *XXXX* は、Centrino、Intel3945、Cisco などのチップセットを指定します（「インストーラ コマンドおよびコマンドライン オプション」（P.8-21）を参照）。

図 8-1 が表示されます。

ステップ 2　「コマンドライン オプションを使用しないインストーラの実行」(P.8-22) のステップ 2 からステップ 7 を実行します。

ステップ 3　ドライバのインストールが完了したら、NIC アダプタを PC に挿入するか取り付けます。

3eTI ドライバ ソフトウェアの手動アップグレード

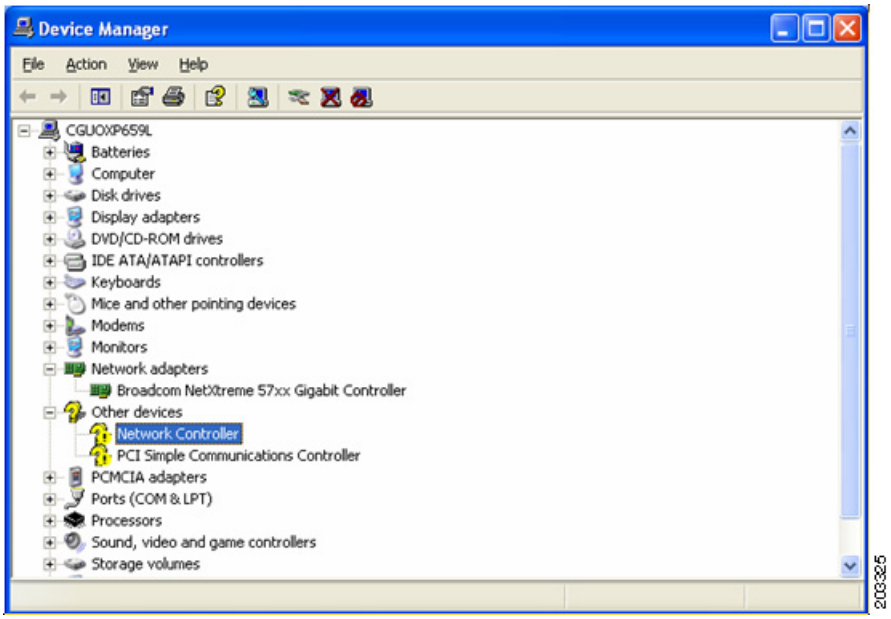
手動アップグレード手順により、ドライバのインストールに関する問題をトラブルシューティングしやすくなります。全社的な展開を構成する手順に組み込むことは想定されていません。

Windows のデバイス マネージャを使用して 3eTI ドライバ ソフトウェアを手動でアップグレードするには、次の手順を実行します。

ステップ 1　デスクトップ上の [マイ コンピューター（My Computer）] アイコンを右クリックし、[プロパティ（Properties）] を選択します。

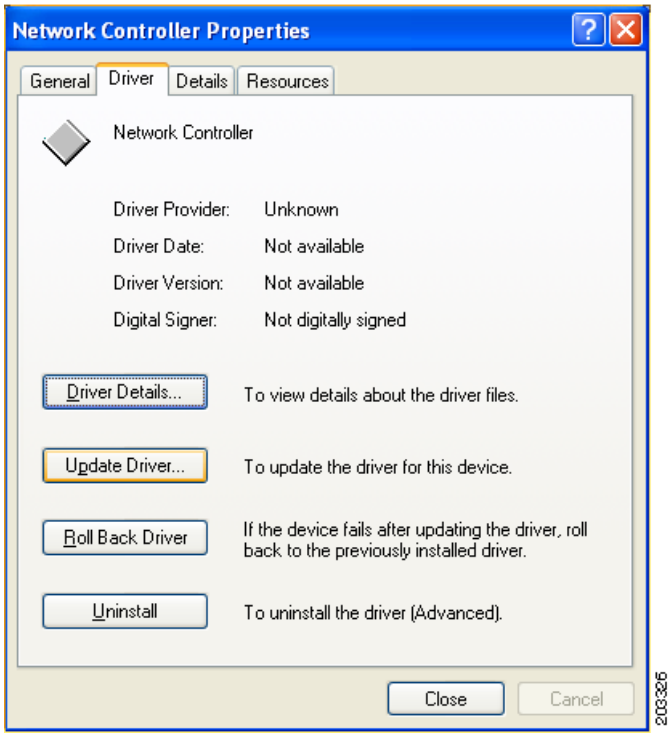
ステップ 2　[システム プロパティ（System Properties）] ウィンドウで [ハードウェア（Hardware）] をクリックし、[デバイス マネージャー（Device Manager）] をクリックします。図 8-8 が表示されます。

図 8-8　Windows の [デバイス マネージャー（Device Manager）] ウィンドウ



ステップ 3　ネットワーク アダプタが取り付けられているか、挿入されており、ドライバ ソフトウェアがインストールされていない場合、デバイスは、[その他のデバイス（Other devices）] の下に黄色の疑問符付きでリストされます。ネットワーク アダプタを右クリックし、[ネットワーク コントローラのプロパティ（Network Controller Properties）] を選択します。[ネットワーク コントローラのプロパティ（Network Controller Properties）] ウィンドウが表示されます（図 8-9 を参照）。

図 8-9　[ネットワーク コントローラのプロパティ（Network Controller Properties）] ウィンドウ

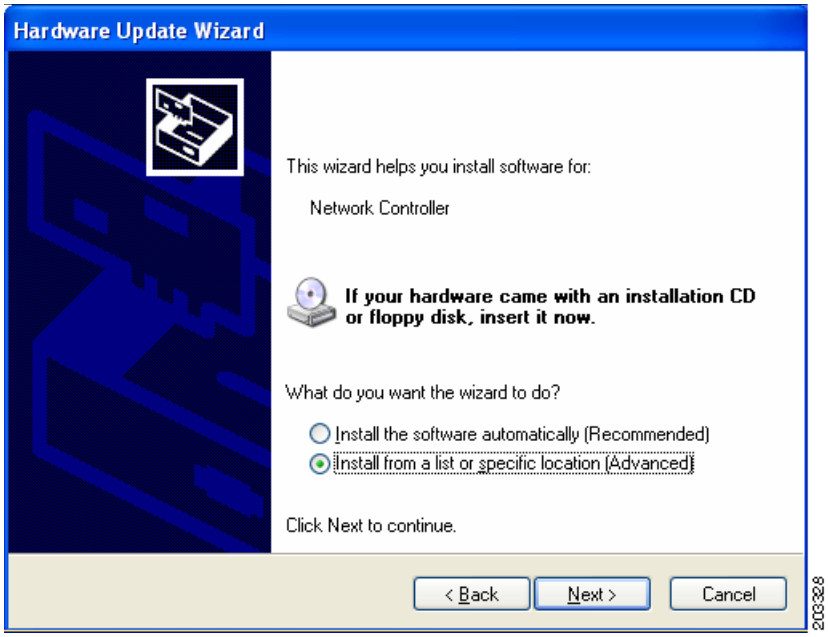


ステップ 4　[ドライバー（Driver）] > [ドライバーの更新（Update Driver）] をクリックします。図 8-10 が表示されます。

図 8-10　Windows の [ハードウェアの更新ウィザード（Hardware Update Wizard）] ウィンドウ

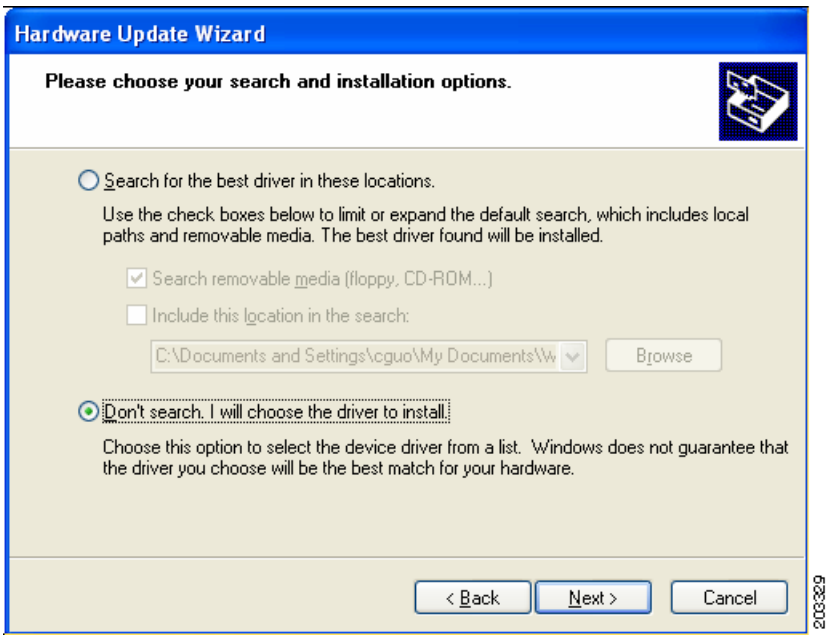
ステップ 5　Windows にドライバ ソフトウェアを検索させないために [いいえ（No）] をオンにし、[次へ（Next）] をクリックします。図 8-11 が表示されます。

図 8-11　[インストール CD またはフロッピー ディスク オプション（Installation CD or Floppy Disk Option）] ウィンドウ



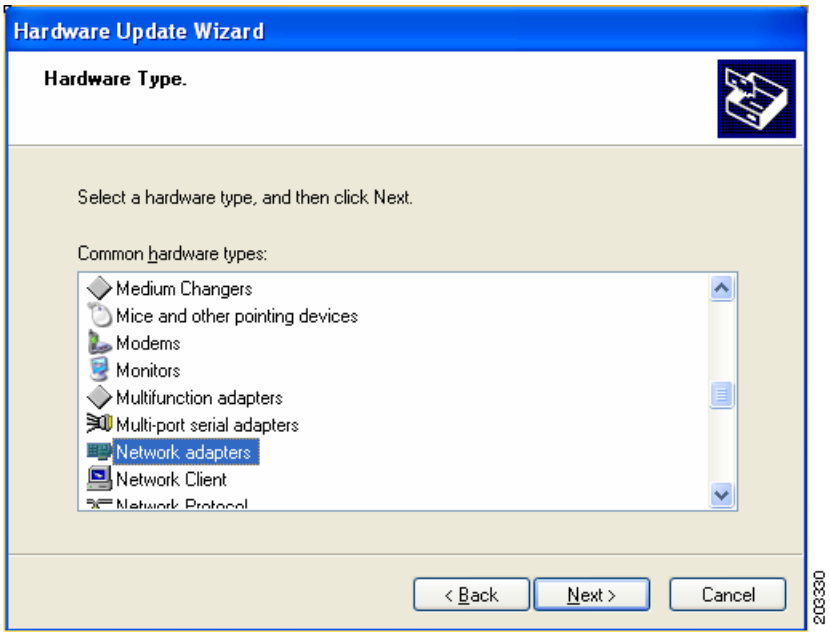
ステップ 6　[一覧または特定の場所からインストールする（詳細）（Install from a list or specific location）] をオンにし、[次へ（Next）] をクリックします。図 8-12 が表示されます。

図 8-12　[検索とインストールのオプション（Search and Installation Options）] ウィンドウ



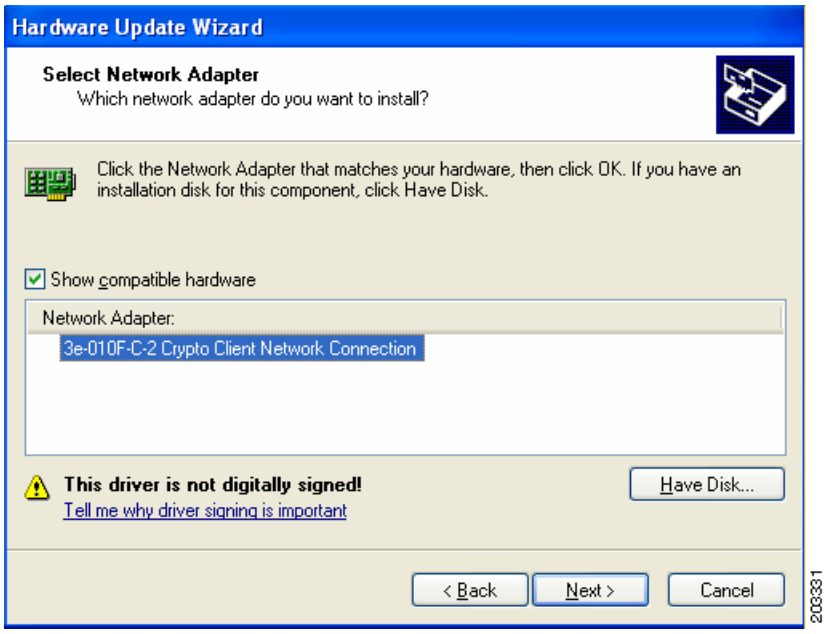
ステップ 7　[検索しないで、インストールするドライバを選択する（Don't search. I will choose the driver to instal）] をオンにし、[次へ（Next）] をクリックします。図 8-13 が表示されます。

図 8-13　Windows の [ハードウェアの種類（Hardware Type）] ウィンドウ



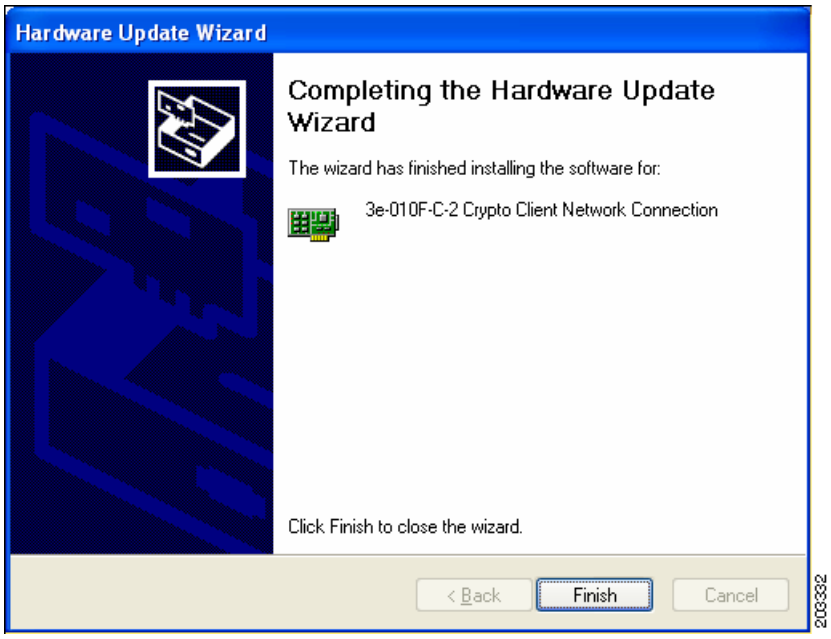
ステップ 8　[ネットワーク アダプター（Network adapter）] を選択し、[次へ（Next）] をクリックします。図 8-14 が表示されます。

図 8-14　[ネットワーク アダプターの選択（Select Network Adapter）] ウィンドウ



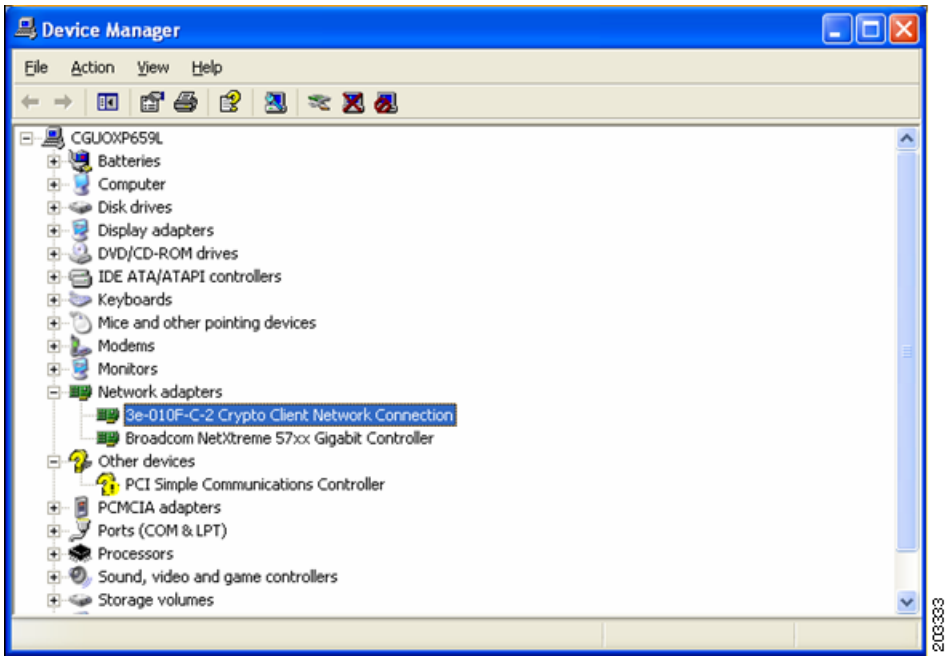
ステップ 9　3eTI ネットワーク接続を選択し、[次へ（Next）] をクリックします。図 8-15 が表示されます。

図 8-15　[インストールの完了（Installation Complete）] ウィンドウ



ステップ 10　ハードウェア ドライバのインストールが完了しました。[完了（Finish）] をクリックします。[デバイス マネージャー（Device Manager）] ウィンドウが再表示されます（図 8-16 を参照）。

図 8-16　更新された、Windows の [デバイス マネージャー（Device Manager）] ウィンドウ



ステップ 11　ドライバが適切にインストールされたことを確認するために、3eTI ネットワーク接続を右クリックし、[プロパティ（Properties）] を選択します。アダプタのプロパティ ウィンドウの [デバイスの状態（Device status）] で、「デバイスは正しく動作しています（This device is working properly）」と示されていることを確認します。

3eTI ドライバ インストーラ ソフトウェアの入手

FIPS 3eTI CKL 対応ドライバ インストーラは、Cisco Software Center からはダウンロードできません。シスコに注文する必要があります。ドライバ インストーラの無期限ライセンスは、製品番号 AIR-SSCFIPS-DRV を使用して、シスコに注文できます。

注文した 3eTI CKL 対応ドライバ インストーラ ソフトウェアは、製品 CD に収録して配布されます。