CHAPTER 9

NGE、FIPS、および追加セキュリティ

NGE（Next Generation Encryption）は、セキュリティおよびパフォーマンスの増大する要件を満たすために、暗号化、認証、デジタル署名、およびキー交換用の新しいアルゴリズムを導入しています。NSA（National Security Agency）は、デバイスが暗号化の強度に関する米国連邦基準を満たすためにサポートしなければならない一連の暗号アルゴリズムを指定しています。Suite B 暗号化スイートは RFC 6379 で定義されています。NSA Suite B として定義されたアルゴリズムの集合的なセットは標準になりつつあるので、AnyConnect IPsec VPN（KEv2 のみ）、PKI、802.1X、および EAP サブシステムがそれらをサポートするようになりました。AnyConnect 3.1 は、Suite B 暗号の CiscoSSL 0.9.8r.1.3 FIPS 認定の実装を使用します（AnyConnect 3.1 は TLS/DTLS、SRTP、および SSH Suite B をサポートしません）。シスコの Suite B 仕様の実装は、FIPS 認定を受けており、AnyConnect および ASDM の設定を通して、NGE 機能が FIPS と見なされます。

AnyConnect VPN コンポーネントは、2 つの VPN ヘッド エンドのうちのいずれかに接続できます。

- ASA
- IOS

この機能を使用するためにクライアント側の設定は必要ありません。

AnyConnect コンポーネントは、適応型セキュリティ アプライアンス（ASA）の設定に基づいて NGE とネゴシエートしてそれを使用します。AnyConnect クライアントの [Statistics] パネル（[Transport Information] ヘッダーの下）には、使用中の暗号名が表示されます。

この章で説明する内容は、次のとおりです。

NGE および AnyConnect に関する情報

AnyConnect 3.1 VPN およびネットワーク アクセス マネージャの NGE（Next Generation Encryption）には次の機能が含まれています。

- 対称暗号化と整合性のための AES-GCM サポート（128、192、256 ビット キー）
  - （ネットワーク アクセス マネージャ）ソフトウェアにおける有線トラフィック暗号化向けの 802.1AE（MACsec）（Windows 7）
  - （VPN）IKEv2 ペイロード暗号化および認証（AES-GCM のみ）

  - （VPN）ESP パケット暗号化および認証
- ハッシュ用の SHA-2（256/384/512 ビットの SHA）サポート
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で SHA-2 を使用して証明書を使用できる機能
  - （VPN）IKEv2 ペイロード認証（Windows Vista 以降および Mac OS X 10.6 以降）
  - （VPN）IKEv2 パケット認証（Windows Vista 以降および Mac OS X 10.6 以降）
- キー交換向けの ECDH サポート
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で ECDHE を使用できる機能（Windows 7 および Windows XP）
  - （VPN）グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS
- デジタル署名、非対称暗号化、および認証用の ECDSA サポート（256、384、521 ビット楕円曲線）
  - （ネットワーク アクセス マネージャ）TLS ベースの EAP 方式で ECDSA と証明書を使用できる機能（クライアント証明書には Windows 7 および Vista のみをサポート。スマート カードには Windows 7 のみをサポート）。
  - （VPN）IKEv2 ユーザ認証およびサーバ証明書の確認

  （注） Linux では、AnyConnect は Firefox 証明書ストアまたは AnyConnect ファイル証明書ストアの両方を使用できます。ECDSA 証明書には、AnyConnect ファイル ストアのみサポートされています。ファイル ストアに証明書を追加するには、「Mac および Linux での PEM 証明書ストアの作成」を参照してください。

- IPsecV3 VPN 用の新しい暗号アルゴリズム。AnyConnect 3.1 は、ヌル暗号化を除く、IPsecV3 で必要とされるアルゴリズムをサポートしています。IPsecV3 は、ESN（Extended Sequence Numbers）がサポートされなければならないことも明記していますが、AnyConnect 3.1 は ESN をサポートしません。
- アルゴリズム間のその他の暗号スイートの依存関係は、AnyConnect 3.1 における次の内容に対するサポートを促進します。
  - IKEv2 用の Diffie-Hellman Groups 14 および 24
  - DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書

要件

- 暗号化および整合性の両方が 1 回の操作で実行される複合モードの暗号化アルゴリズムは、ハードウェア クリプト アクセラレーションを使用する SMP ASA ゲートウェイ（5585 および 5515-X など）でのみサポートされます。AES-GCM は、シスコがサポートする複合モードの暗号化アルゴリズムです。

（注）　IKEv2 ポリシーは、通常モードまたは複合モードの暗号化アルゴリズムのうちの 1 つを含めることができますが、両方は不可能です。複合モードのアルゴリズムが IKEv2 ポリシーで設定されると、通常モードのアルゴリズムすべてがディセーブルになるので、唯一有効な整合性アルゴリズムは NULL です。

IKEv2 IPsec プロポーザルは別のモデルを使用し、同じプロポーザル内で標準モードおよび複合モード両方の暗号化アルゴリズムを指定できます。この使用方法では、両方に整合性アルゴリズムを設定する必要があります。その結果、非 NULL 整合性アルゴリズムが AES-GCM 暗号化で設定されます。

- NGE には、NSA Suite B アルゴリズムを使用する IKEv2 リモート アクセス接続用の AnyConnect Premium ライセンスが必要です。ほかの接続または目的（たとえば PKI）向けの Suite B アルゴリズムの使用には制限がありません。ライセンス チェックは、リモートアクセス接続に対して実行されます。AnyConnect Premium ライセンスがない状態で NSA Suite B 暗号化アルゴリズムを使用しようとしているというメッセージを受信した場合、Premium ライセンスをインストールするか、暗号化の設定を適切なレベルに再設定するか選択できます。
- IPSec 接続には、デジタル署名の Key Usage 属性とキー暗号化、さらにはサーバ認証の Enhanced Key Usage 属性または IKE 中間を含むサーバ証明書が必要です。Key Usage を含まない IPSec サーバ証明書は、すべての Key Usage に対して無効と見なされ、同様に、Enhanced Key Usage を含まない IPSec サーバ証明書は、すべての Enhanced Key Usage に対して無効と見なされることに注意してください。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

- Suite B は IKEv2/IPsec でのみ利用できます。
- SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。
- TLS v1.2 ハンドシェイクは AnyConnect 3.1 ではサポートされません。
- TLS v1.2 証明書認証は AnyConnect 3.1 ではサポートされません。
- ECDSA 証明書は、Windows Vista 以降、Mac OS X 10.6 以降、Linux Red Hat 6（32 ビット）、および Linux Ubuntu 9.x、10.x、11.x（32 ビット）でサポートされています。ECDSA スマートカードは、Windows 7 でのみサポートされています。
- ECDSA 証明書には、カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
- Suite B プロファイルは、証明書内に特定のポリシー プロパティを持つ必要がある場合がありますが、これらの要件は ASA 上で強制され、AnyConnect 上では強制されません。
- ASA は SSL VPN の ECDSA 証明書をサポートしていないので、そのような証明書を SSL VPN に使用しないでください。
- ASA が SSL および IPsec 用の異なるサーバ証明書で設定されている場合は、信頼できる証明書を使用してください。異なる IPsec および SSL 証明書を持つ Suite B（ECDSA）の信用されていない証明書を使用する場合、ポスチャ評価、WebLaunch、またはダウンローダの障害が発生する可能性があります。
- AES-GCM は、計算集約型のアルゴリズムであるため、これらのアルゴリズムを使用するときは、全体的なデータ レートが低くなる可能性があります。新しい Intel プロセッサの一部は、特に AES-GCM の性能を向上させるために採用された特別な命令を含むものもあります。AnyConnect

3.1 は、それが実行されるプロセッサ上でそれらの新しい命令がサポートされているかどうかを自動的に検出します。サポートされている場合は、AnyConnect は新しい命令を使用し、特別な命令を持たないプロセッサと比較して VPN データ レートを大幅に向上させます。新しい命令をサポートするプロセッサのリストについては、http://ark.intel.com/search/advanced/?s=t&AESTech=true を参照してください。詳細については、http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/ を参照してください。

- IPSec 接続は、サーバ証明書で名前の検証を実行します。IPSec の名前検証では、次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name のみを使用します。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あるけれども関連する属性を含んでいない場合、名前検証は、証明書の Subject で見つかった　Common Name 属性を使用します。
  - 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。この規則に準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

NGE での AnyConnect モジュールについて

AnyConnect に関する FIPS 認定の機能は、モデルごとに ASA に対して使用許諾されています。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。XML ファイル AnyConnectLocalPolicy にはセキュリティ設定が含まれていますが、それは ASA によって展開されません。これは、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展開する必要があります。クライアントの接続先である各 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：ネットワーク アクセス マネージャにおける FIPS サポートは、ユーザ コンピュータ上の AnyConnectLocalPolicy.xml に含まれる FIPS モード パラメータ、およびネットワーク アクセス マネージャのグループ ポリシーに含まれる FIPS モード パラメータによってイネーブルになります。

  ネットワーク アクセス マネージャ用の FIPS は、Windows 7/Vista および Windows XP でサポートされます。Windows XP には、3e Technologies International が提供する 3eTI FIPS 準拠の Cryptographic Kernel Library（CKL）と、ネットワーク アクセス マネージャに統合されたサポート済みのドライバが必要です。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。

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か、事前に展開された AnyConnect インストーラ内にファイルを含める必要があります。

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。

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、Cisco 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。この MST は FIPS をイネーブルにするだけであり、ほか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。

AnyConnect 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。

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

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。MST パラメータ名は、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、AnyConnect ローカル ポリシーのパラメータと値 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 インストーラが新しいポリシー ファイルを作成できるようにするには、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 ツールを使用した 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、シスコの 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 9-1 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、AnyConnect ローカル ポリシーのパラメータと値 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 9-1 に、ポリシー設定と Enable FIPS ツールの引数を示します。ポリシー設定の説明は、「AnyConnect ローカル ポリシーのパラメータと値」（P.9-15）に記載されています。

表 9-1　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]**

表 9-1　ポリシー設定と Enable FIPS ツールの引数 （続き）

ポリシー設定	引数および構文
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。次の表は、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 9-2　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 以降では、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。AnyConnectLocalPolicy ファイルを手動で編集するか、AnyConnect プロファイル エディタのインストーラとともに配布される VPN ローカル ポリシー エディタを使用できます。パラメータは、「AnyConnect ローカル ポリシーのパラメータと値」（P.9-15）で説明されています。

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。

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ほかのコンポーネントでは、AnyConnect が FIPS をイネーブルにしたこと、および暗号化の使用を開始したことを検出できます。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 [*Use FIPS compliant algorithms for encryption, hashing, and signing*] を [Disabled] に変更することにより、[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 9-3 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 9-3　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 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 からのみ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ほかのサービス 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 [プログラムの追加と削除] 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。

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 9-4、表 9-5、表 9-6、表 9-7 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 9-4　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 9-5　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、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 9-6　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、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 9-7　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 9-8 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 9-8　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

ここでの例を続けると、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

次のパラメータは、VPN ローカル ポリシー エディタおよび AnyConnectLocalPolicy.xml ファイル内の要素です。XML 要素は、山括弧 <> で囲んで表示されています。

（注） ファイルを手動で編集し、ポリシー パラメータを省略した場合、この機能はデフォルトの動作を用います。

<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。

Fips モード

<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。

ダウンローダのバイパス

<BypassDownloader>

オンにすると、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。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。

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。

Web Launch の制限

<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。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。

厳格な証明書トラスト

<StrictCertificateTrust>

選択すると、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.
```

選択しないと、クライアントはユーザに証明書を受け入れるように要求します。これはデフォルトの動作で、AnyConnect の以前のバージョンと一致します。

（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。

プリファレンス キャッシングの制限
<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）。

トンネル プロトコルの制限
サポートされていません。

PEM ファイル証明書ストアを除外（Linux および Mac）
<ExcludePemFileCertStore>

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できないようにします。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。

Windows のネイティブ証明書ストアの除外（Windows のみ）
このオプションは、現在、サポートされていません。

Mac のネイティブ証明書ストアの除外（Mac のみ）

<ExcludeMacNativeCertStore>

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できないようにします。

FireFox の NSS 証明書ストアの除外（Linux および Mac）

<ExcludeFirefoxNSSCertStore>

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できないようにします。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。

ポリシーの更新

<UpdatePolicy>

このセクションでは、クライアントがどの ASAS からソフトウェアまたはプロファイルの更新を取得できるかを制御することができます。これらのタイプの更新のいずれかまたは両方をディセーブルにする場合は、クライアントがソフトウェアおよびローカル ポリシー プロファイルの更新を入手できるサーバを追加する必要があります。

ソフトウェアおよびプロファイル更新の設定がクライアントの更新にどのように影響するかに関する詳細については、「ソフトウェア ロックの使用例」（P.9-12）を参照してください。

- 任意のサーバからソフトウェア更新を許可

  <AllowSoftwareUpdatesFromAnyServer>

  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、サーバのリストに追加した ASA からのみソフトウェアを取得するようにします。

- 任意のサーバから VPN ポリシー更新を許可

  <AllowVPNProfileUpdatesFromAnyServer>

  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、サーバのリストに追加した ASA からのみ更新を取得できるようにします。

- サーバ名

  <ServerName>

  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各サーバを追加します。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

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="3.0.0592">
    <FipsMode>true</FipsMode>
    <BypassDownloader>true</BypassDownloader>
    <RestrictWebLaunch>true</RestrictWebLaunch>
    <StrictCertificateTrust>true</StrictCertificateTrust>
    RestrictTunnelProtocols IPSec RestrictTunnelProtocols
    <RestrictPreferenceCaching>Credentials</RestrictPreferenceCaching>
    <ExcludePemFileCertStore>true</ExcludePemFileCertStore>
    <ExcludeWinNativeCertStore>true</ExcludeWinNativeCertStore>
    <ExcludeMacNativeCertStore>true</ExcludeMacNativeCertStore>
    <ExcludeFirefoxNSSCertStore>true</ExcludeFirefoxNSSCertStore>
```

```
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
            <AuthorizedServerList>
                <ServerName>asa.one</ServerName>
                <ServerName>asa.two</ServerName>
            </AuthorizedServerList>
    </UpdatePolicy>
</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、AnyConnect ネットワーク アクセス マネージャ クライアント プロファイルで FIPS モードをイネーブル化し、ローカル ポリシー内で FIPS モードをイネーブル化することでサポートされます。Windows XP では、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）を展開する必要もあります。

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 [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 モードの強制」（P.9-19）
- 「3eTI ドライバのインストール」（P.9-20）
- 「3eTI ドライバ インストーラ ソフトウェアの入手」（P.9-32）

ネットワーク アクセス マネージャでの FIPS モードの強制

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強制できます。

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、PEAP、EAP-FAST、および LEAP 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 モジュール
- FIPS 準拠のローカル ポリシー ファイル
- 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）（Windows XP のみ）

ネットワーク アクセス マネージャ プロファイル エディタを使用して、ローカル ポリシー ファイルの中で FIPS モードをイネーブルにします。詳細については、「[Client Policy] ウィンドウ」（P.4-5）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、完全な 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対象のドライバを使用して 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。

Windows XP システムの場合、ネットワーク アクセス マネージャの Log Packager ユーティリティが 3eTI パケットのログを収集します。

特記事項

1. 3eTI CKL ドライバ インストーラは、常に 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。

  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。

例：

- *–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、ほか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* 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。
  - 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 Explorer 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。

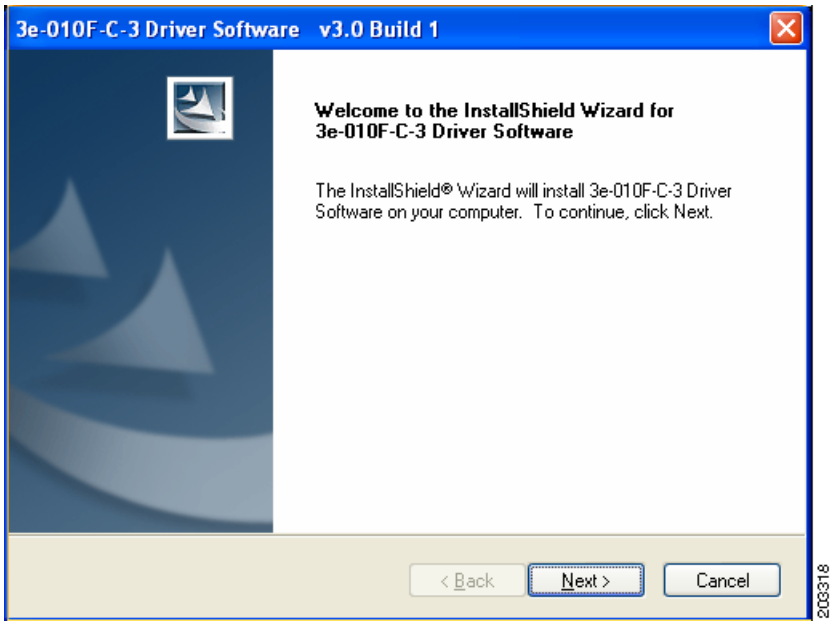
b. [Start] > [Run] をクリックし、次のインストーラ実行コマンドを入力します。

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。

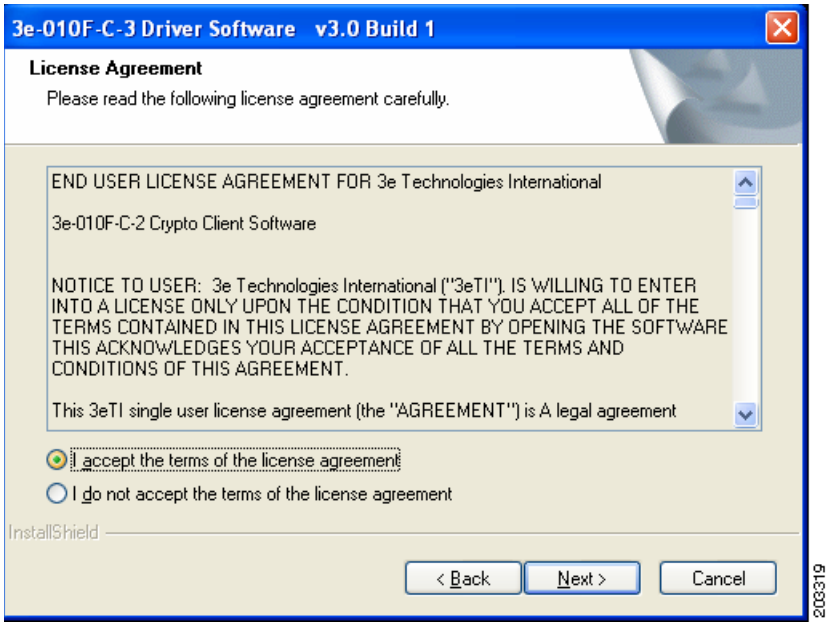
[Driver Welcome] ウィンドウが表示されます（図 9-1）。

図 9-1　[Driver Welcome] ウィンドウ



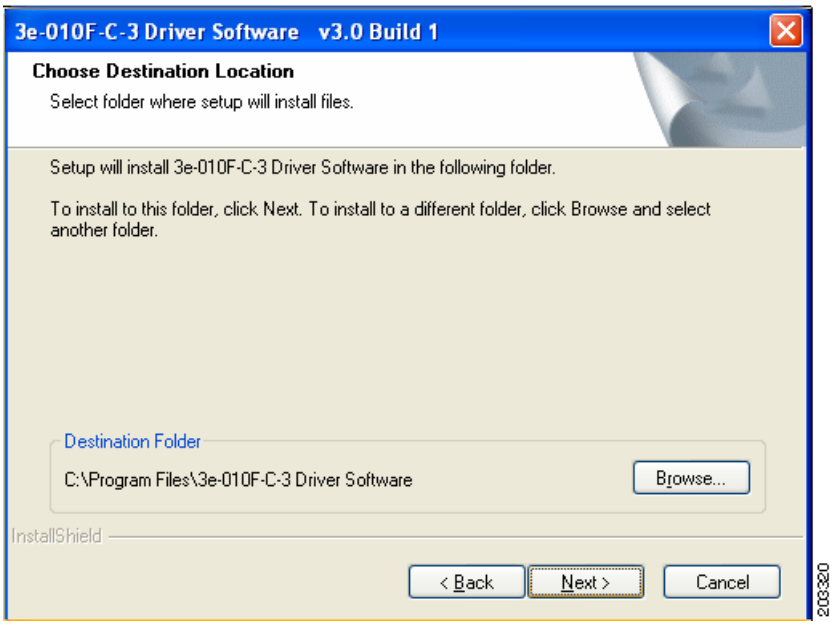
ステップ 2　[Next] をクリックすると、ライセンス契約書が表示されます（図 9-2 を参照）。

図 9-2　ライセンス契約書



ステップ 3　使用許諾契約を読み、同意して、[Next] をクリックします。[Destination Location Window] が開きます（図 9-3）。

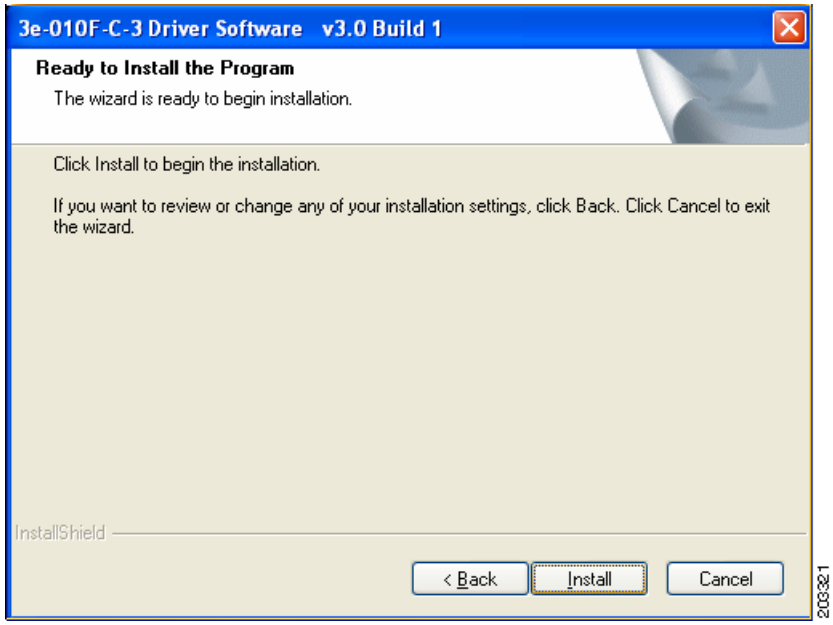
図 9-3　[Destination Location] ウィンドウ



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、[Browse] をクリックして目的のフォルダを探します。

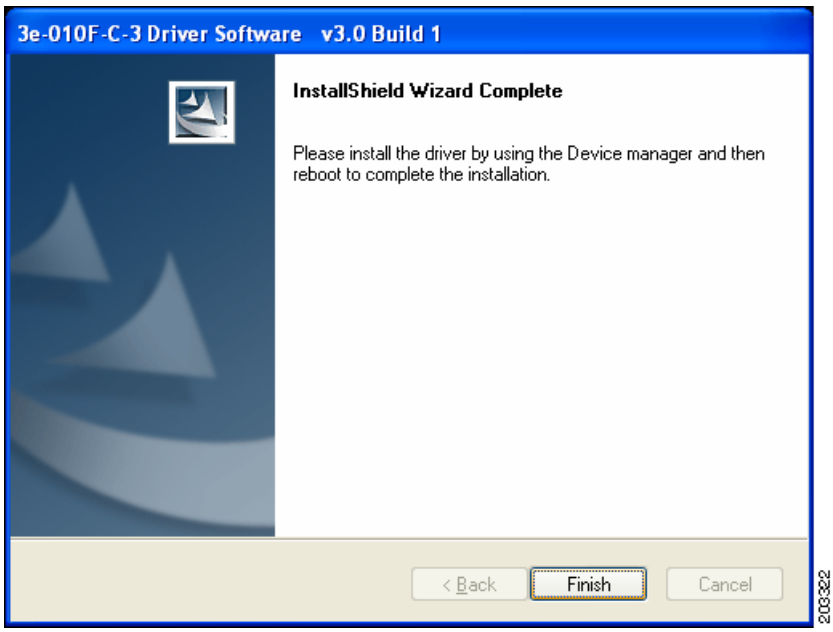
ステップ 5　[Next] をクリックします。[Ready to Install] ウィンドウが開きます（図 9-4）。

図 9-4　[Ready to Install] ウィンドウ



ステップ 6　[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、[Wizard Complete] ウィンドウが開きます（図 9-5）。

図 9-5　[Wizard Complete] ウィンドウ



ステップ 7　[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

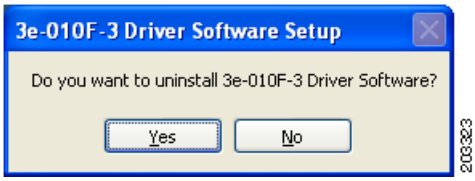
以前の 3eTI ドライバ ソフトウェアをアンインストールするには、次の手順を実行します。

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、[Start] > [Settings] > [Control Panel] > [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、[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 9-6 を参照）。

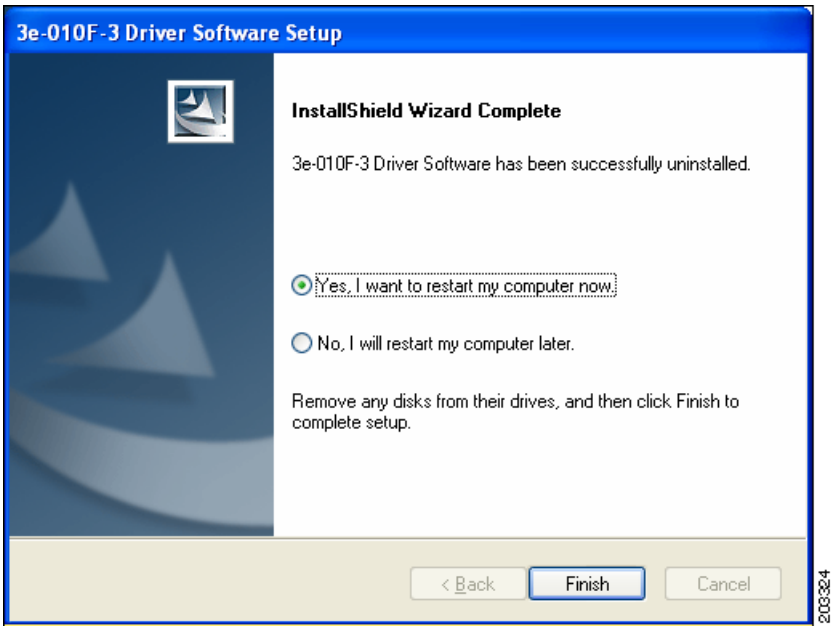
図 9-6　[Uninstall Driver Software] ポップアップ



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。

[Restart Computer Now] ウィンドウが開きます（図 9-7）。

図 9-7　[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、[Yes] をオンにします。

ステップ 5　[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*

各記号の意味は次のとおりです。

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.9-21）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　[Start] > [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*

各記号の意味は次のとおりです。

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.9-21）を参照）。

図 9-1 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.9-22) 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。

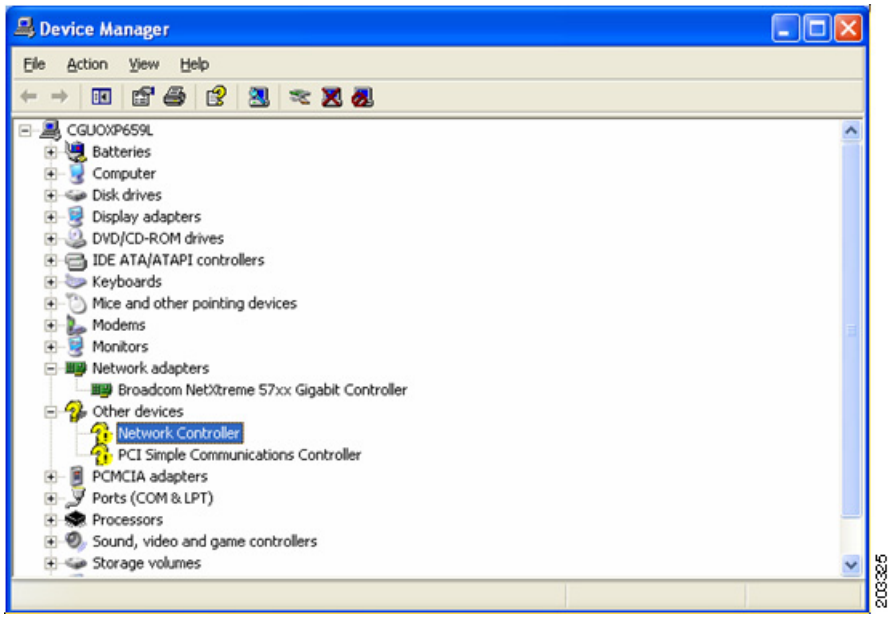
Windows のデバイス マネージャを使用して 3eTI ドライバ ソフトウェアを手動でアップグレードするには、次の手順を実行します。

ステップ 1　デスクトップ上の [My Computer] アイコンを右クリックし、[Properties] を選択します。

ステップ 2　[System Properties] ウィンドウで [Hardware] をクリックし、[Device Manager] をクリックします。

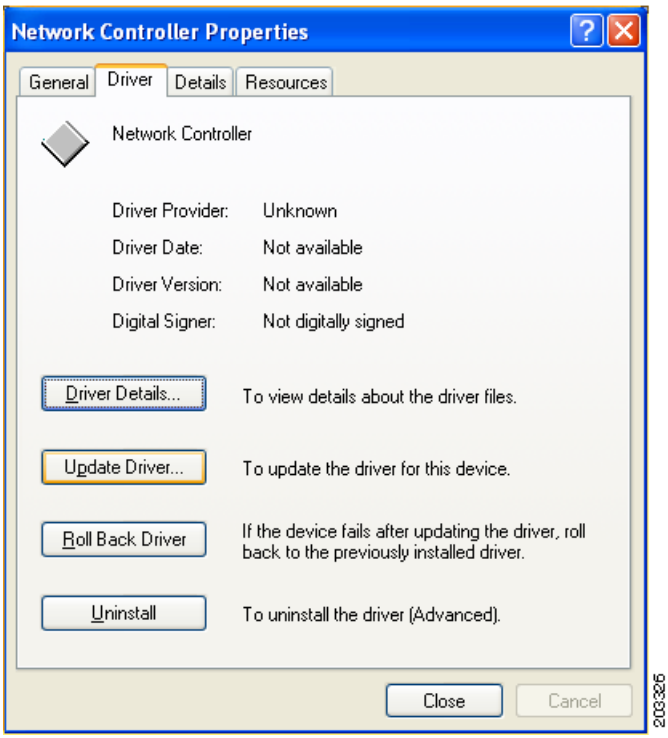
[Windows Device Manager] ウィンドウが開きます（図 9-8）。

図 9-8　[Windows 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、[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、[Properties] を選択します。[Network Controller Properties] ウィンドウが開きます（図 9-9）。

図 9-9　[Network Controller Properties] ウィンドウ



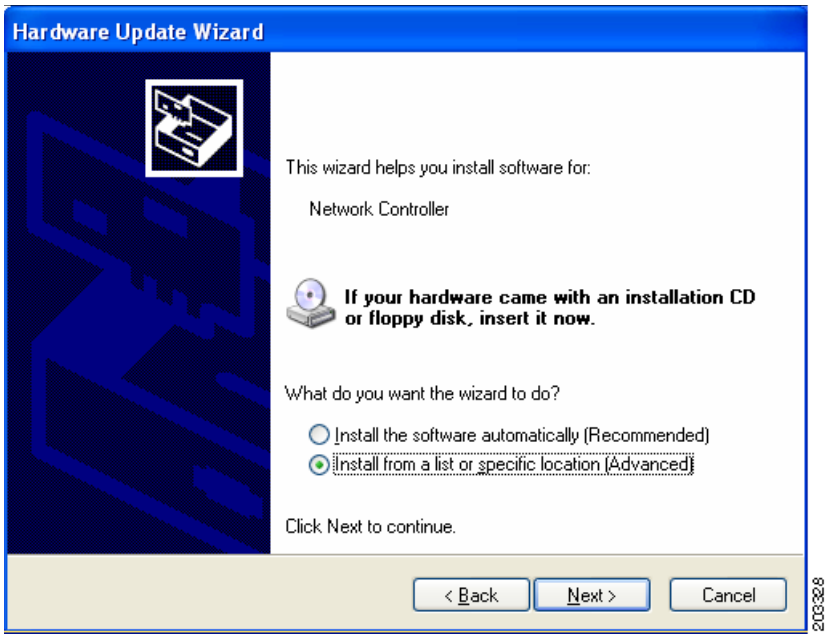
ステップ 4　[Driver] > [Update Driver] をクリックします。

[Windows Hardware Update Wizard] ウィンドウが開きます（図 9-10）。

図 9-10　[Windows Hardware Update Wizard] ウィンドウ

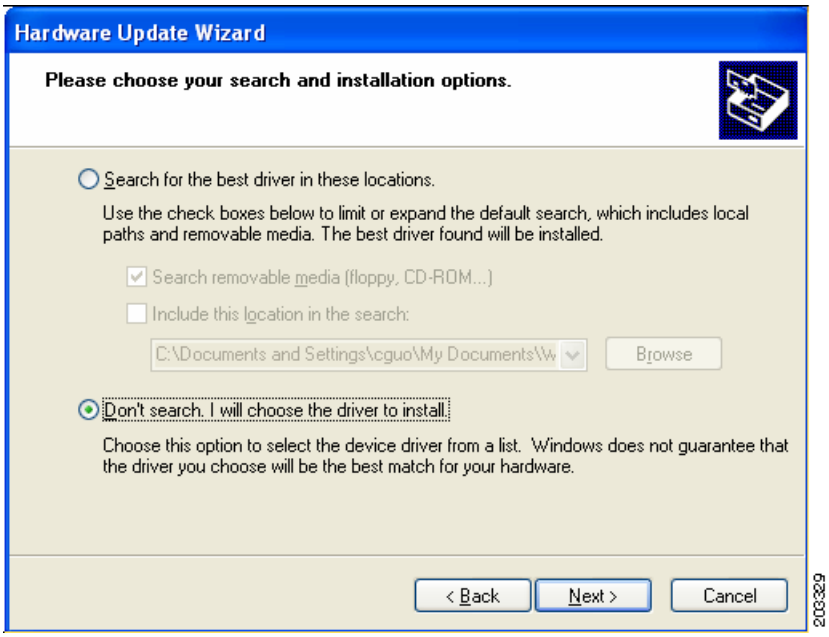
ステップ 5　Windows にドライバ ソフトウェアを検索させないために [No] をオンにし、[Next] をクリックします。[Hardware Update wizard] ウィンドウが続行します（図 9-11）。

図 9-11　[Installation CD or Floppy Disk Option] ウィンドウ



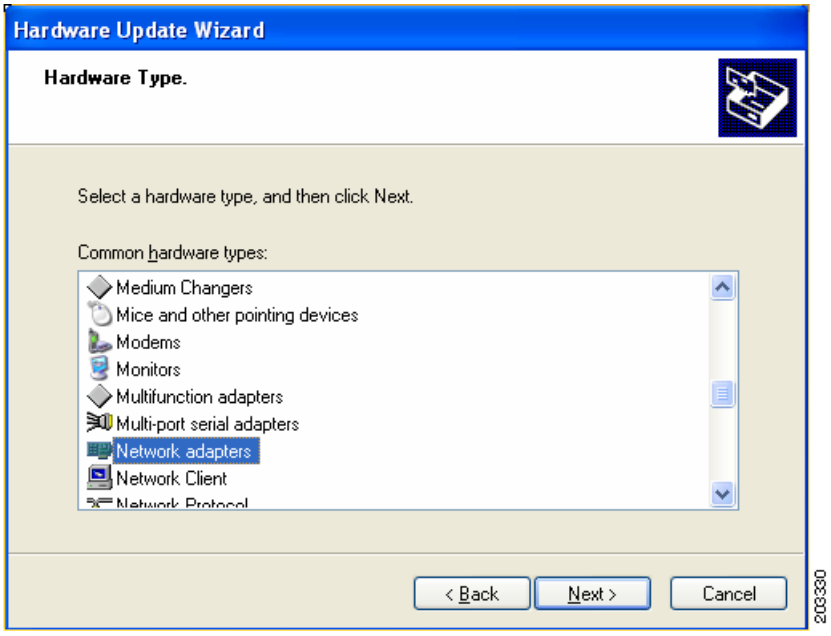
ステップ 6　[Install from a list or specific location (Advanced)] をオンにし、[Next] をクリックします。[Search and Installation Options] ウィンドウが開きます（図 9-12）。

図 9-12　[Search and Installation Options] ウィンドウ



ステップ 7　[Don't search. I will choose the driver to install] をオンにし、[Next] をクリックします。[Windows Hardware Type] ウィンドウが開きます（図 9-13）。

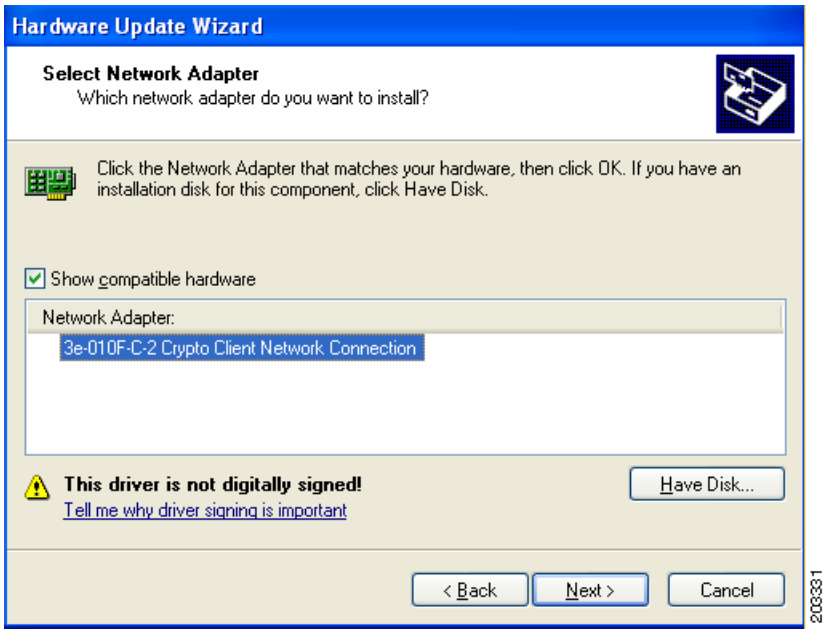
図 9-13　[Windows Hardware Type] ウィンドウ



ステップ 8　[Network adapter] を選択し、[Next] をクリックします。

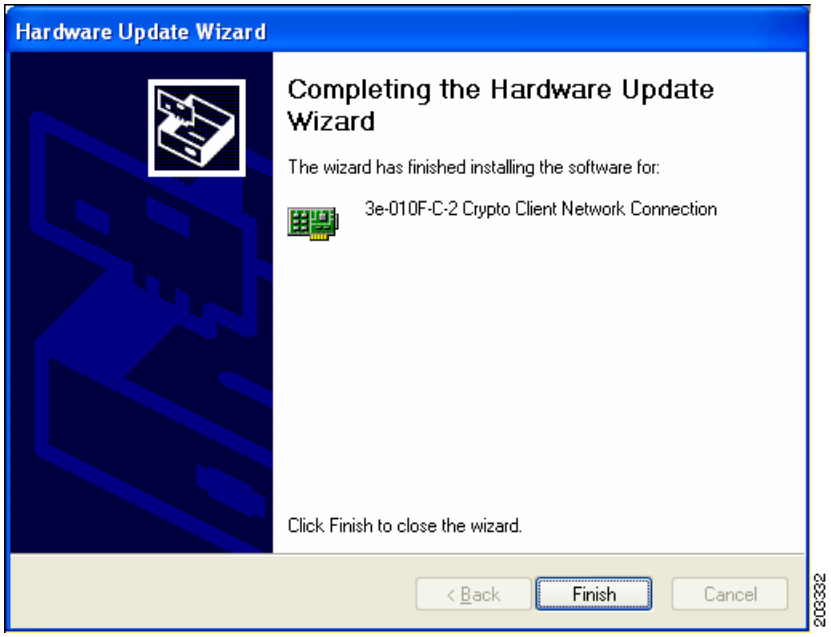
ステップ 9　[Select Network Adapter] ウィンドウが開きます（図 9-14）。

図 9-14　[Select Network Adapter] ウィンドウ



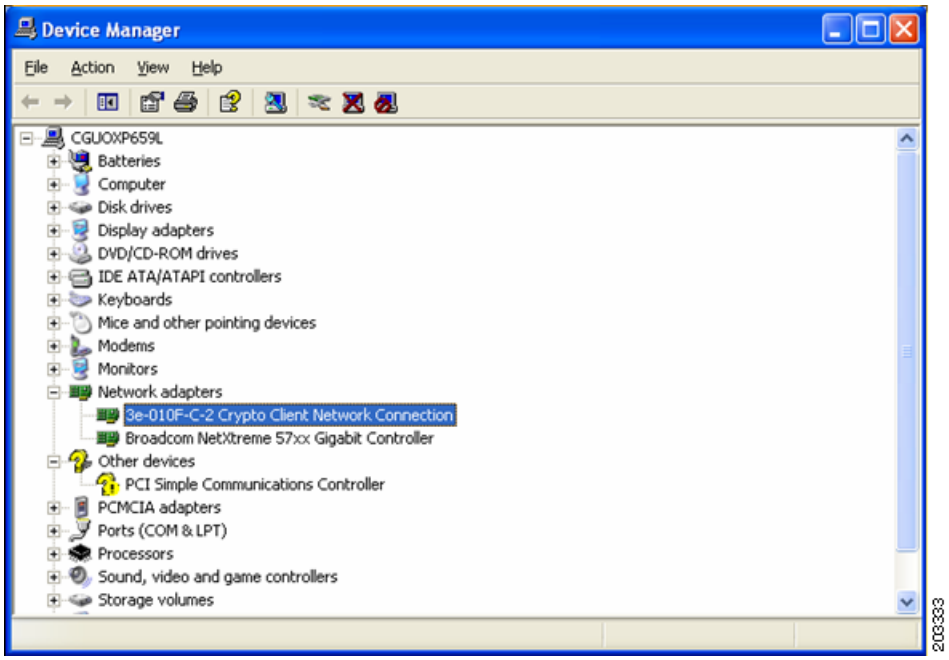
ステップ 10　3eTI ネットワーク接続を選択し、[Next] をクリックします。
[Installation Complete] ウィンドウが開きます（図 9-15）。

図 9-15　[Installation Complete] ウィンドウ



ステップ 11　ハードウェア ドライバのインストールが完了しました。[Finish] をクリックします。
[Device Manager] ウィンドウが再表示されます（図 9-16 を参照）。

図 9-16　更新された、Windows の [Device Manager] ウィンドウ



ステップ 12　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、[Properties] を選択します。アダプタのプロパティ ウィンドウの [Device status] で、「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。