CHAPTER 4

FIPS およびその他のセキュリティのローカル ポリシーでのイネーブル化

AnyConnect ローカル ポリシーは、Cisco AnyConnect Secure Mobility Client のその他のセキュリティ パラメータを指定します。これには、Federal Information Processing Standard（FIPS; 連邦情報処理標準）レベル 1、暗号化モジュール固有のセキュリティ要件に関する合衆国政府の標準である 140-2 準拠モードでの動作が含まれます。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。

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。

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。

Windows に対しては、標準 MST インストール ファイルに適用して FIPS をイネーブル可能な Microsoft Transform（MST）ファイルを用意してあります。この MST では、その他の AnyConnect ローカル ポリシー パラメータは変更されません。コマンドライン ツールの Enable FIPS ツールを使用することもできます。このツールを実行するには、Windows 上では管理者権限が必要です。Linux または Mac 上では、root ユーザとして実行する必要があります。FIPS ライセンスを購入する場合、MST または Enable FIPS ツールの情報を受信し、その情報を利用してこれらのツールをダウンロードできます。

または、AnyConnect ローカル ポリシー ファイルのコピーをクライアント インストールから取得し、手動でパラメータを編集して、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ユーザのコンピュータに導入してください。

ここでは、次の内容について説明します。

MST ファイルを使用した Windows クライアント用 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。この MST は FIPS をイネーブルにするだけで、その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 4-3 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 ツールを使用した FIPS およびその他の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 4-1 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 4-3 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 4-1 に、ポリシー設定と Enable FIPS ツールの引数を示します。

表 4-1　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 4-2 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 4-2　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 VPN Client
Windows Vista	C:¥ProgramData¥Cisco¥Cisco AnyConnect VPN Client
Windows XP	C:¥Documents and Settings¥All Users¥Application Data¥Cisco¥Cisco AnyConnect VPN Client
Windows Mobile	%PROGRAMFILES%¥Cisco AnyConnect VPN Client

表 4-2　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 （続き）

オペレーティング システム	インストール パス
Linux	/opt/cisco/vpn
Mac OS X	/opt/cisco/vpn

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 IT ソフトウェア導入システムを使用してこのファイルをリモート コンピュータに導入します。

AnyConnect ローカル ポリシー ファイルのパラメータと値

（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 4-3 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 4-3　AnyConnect 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、イベント ログ警告が発行されます。	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">

表 4-3　AnyConnect 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
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）。
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、ASA 上に、翻訳、カスタマイゼーション、オプションのモジュール、コア ソフトウェアのアップデートなど、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せん。ただし、クライントの VPN クライアント プロファイルを ASA でそのグループ ポリシーと関連付けられたプロファイルと比較しようとします。 *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 VPN 接続は行われますが、その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が含まれていることがあるため、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を除いて、BypassDownloader を *true* に設定しないでください。

表 4-3　AnyConnect 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
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）。
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。これらの証明書を受け入れるようにプロンプトを表示することはありません。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 設計上、AnyConnect は、機密情報をディスクにキャッシュしません。このパラメータをイネーブルにすると、AnyConnect プリファレンスに格納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ど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）。
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。セキュリティ 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）。

表 4-3　AnyConnect 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
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）。

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>
```