APPENDIX A

VPN XML リファレンス

AnyConnect 3.1、3.0、または 2.5 および ASDM 6.3(1) 以降を使用している場合、このリファレンスは必要ありません。ASDM から起動されたプロファイル エディタまたは Cisco.com からダウンロードできるスタンドアロン プロファイル エディタを使用して、クライアント プロファイルを作成して編集します。詳細については、「AnyConnect クライアント プロファイルの概要」（P.2-1）を参照してください。

この付録は、ASDM を 6.3（1）以降にアップグレードしていない場合にのみ使用してください。AnyConnect 2.5 は、AnyConnect 機能を設定するためにアクセス可能なプロファイル エディタをサポートします。ただし、ASDM 6.3(1) 以降を使用する場合のみ、このプロファイル エディタにアクセスできます。それ以前の AnyConnect のバージョンには、Windows にインストール可能な独立型のプロファイル エディタが提供されていましたが、このプロファイル エディタは独立型のエディタとしてマニュアル化されておらず、サポート対象でなかったため、現在は提供されていません。プロファイルの作成、編集、および管理を直接行う場合、従来のエディタよりも AnyConnect プロファイル エディタで行う方がはるかに容易なことから、ASDM にアップグレードすることを強くお勧めします。新しいプロファイル エディタはマニュアル化され、サポート対象であり、独自のオンライン ヘルプを利用できます。AnyConnect 2.5 を使用する場合、ASDM 6.3（1）でサポートされる最小 ASA ソフトウェア リリースは ASA 8.0（2）です。ただし、新しいクライアント機能のメリットを最大限に利点できるように、ASA 8.3（1）以降にアップグレードすることをお勧めします。

AnyConnect プロファイルおよび機能の詳細については、第 3 章「AnyConnect クライアント機能の設定」を参照してください。この付録では、同章とは別の方法について説明します。

次の項では、各クライアント機能について簡単に説明し、XML タグ名、オプション、説明、およびコード例を記載します。プロファイルで値が指定されていない場合、AnyConnect はデフォルト値を使用します。それぞれの値内のすべてのプロファイル タグおよび特定のオプションを入力する場合について考慮します。この章で示される値は、エラー条件を避けるため、大文字または小文字を一致させる必要があります。

（注） 本書の例をカット アンド ペーストしないでください。カット アンド ペーストすると、改行が入り、XML が機能しなくなることがあります。代わりに、プロファイル テンプレート ファイルをテキスト エディタ（メモ帳やワードパッドなど）で開いてください。

- 「ローカル プロキシ接続」（P.A-2）
- 「Optimal Gateway Selection（OGS）」（P.A-2）
- 「Trusted Network Detection」（P.A-3）
- 「常時接続の VPN および下位機能」（P.A-4）
- 「ロード バランシングを備えた常時接続の VPN」（P.A-6）
- 「Windows の証明書ストア」（P.A-7）

- 「証明書ストアの使用の制限」（P.A-8）
- 「証明書のプロビジョニングと更新を行う SCEP プロトコル」（P.A-8）
- 「自動証明書選択」（P.A-14）
- 「バックアップ サーバ リスト パラメータ」（P.A-14）
- 「Windows Mobile ポリシー」（P.A-15）
- 「サーバ リスト」（P.A-17）
- 「スクリプト化」（P.A-19）
- 「認証タイムアウト コントロール」（P.A-20）
- 「Windows ユーザのための、RDP セッションからの AnyConnect セッションの許可」（P.A-20）
- 「L2TP または PPTP を介した AnyConnect」（P.A-21）
- 「その他の AnyConnect プロファイル設定」（P.A-22）

ローカル プロキシ接続

表 A-1 に、ローカル プロキシ接続のサポートを設定するための、タグ名、オプション、および説明を示します。

表 A-1　ローカル プロキシ接続の設定

XML タグ名	オプション	説明
AllowLocalProxyConnections	true（デフォルト）	ローカル プロキシ接続を有効にします。
	false	ローカル プロキシ接続を無効にします。

例：ローカル プロキシ接続の無効

ローカル プロキシ接続の AnyConnect サポートを無効にするには、次の例を参照してください。

```
<ClientInitialization>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
</ClientInitialization>
```

Optimal Gateway Selection（OGS）

表 A-2 に、OGS を設定するためのタグ名、オプション、および説明を示します。

表 A-2　OGS 設定

XML タグ名	オプション	説明
EnableAutomaticServerSelection	true	デフォルトで OGS が有効になります。
	false	デフォルトで OGS が無効になります。
EnableAutomaticServerSelection UserControllable	true	ユーザがクライアント設定で OGS を有効または無効に切り替えることを許可します。*
	false	デフォルトに戻します。デフォルトでは、ユーザは自動サーバ選択を制御できません。

表 A-2　OGS 設定 （続き）

XML タグ名	オプション	説明
AutoServerSelectionImprovement	整数。デフォルトは 20 % です。	クライアントが別のセキュア ゲートウェイに接続する際の基準となるパフォーマンス向上率。
AutoServerSelectionSuspendTime	整数。デフォルトは 4 時間です。	現在のセキュア ゲートウェイを接続解除してから、別のセキュア ゲートウェイに再接続するまでの経過時間（単位は時間）を指定します。

* OGS が有効のときは、この機能をユーザ制御可能にすることをお勧めします。

例：OGS

OGS を設定するには、次の例を参照してください。

```
<ClientInitialization>
    <EnableAutomaticServerSelection UserControllable="true">
     true
         <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
         <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
     </EnableAutomaticServerSelection>
</ClientInitialization>
```

Trusted Network Detection

表 A-3 に、Trusted Network Detection を設定するためのタグ名、オプション、および説明を示します。

表 A-3　Trusted Network Detection の設定

XML タグ名	オプション	説明
AutomaticVPNPolicy	true	TND を有効にします。*TrustedNetworkPolicy* パラメータおよび *UntrustedNetworkPolicy* パラメータに従って、VPN 接続を開始または停止する必要があるときに自動的に管理します。
	false	TND を無効にします。VPN 接続は、手動でないと開始および停止できません。
TrustedNetworkPolicy	Disconnect	信頼ネットワークで VPN 接続を接続解除します。
	Connect	信頼ネットワークで VPN 接続を開始します（VPN 接続がない場合）。
	DoNothing	信頼ネットワークでは何もしません。
	Pause	信頼ネットワークの外で VPN セッションが確立された後に、ユーザが信頼できると設定されたネットワークに入る場合、VPN セッションを接続解除する代わりにそのセッションを一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。
UntrustedNetworkPolicy	Connect	非信頼ネットワークを検知すると、VPN 接続を開始します。
	DoNothing	非信頼ネットワークを検知すると、VPN 接続を開始します。このオプションは、常時接続の VPN と互換性がありません。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。

表 A-3　Trusted Network Detection の設定 （続き）

XML タグ名	オプション	説明
TrustedDNSDomains	文字列	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性のある DNS サフィックスのリスト（カンマ区切りの文字列）。次に、TrustedDNSDomain 文字列の例を示します。 *.cisco.com DNS サフィックスでは、ワイルドカード（*）がサポートされます。
TrustedDNSServers	文字列	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性のある DNS サーバ アドレスのリスト（カンマ区切りの文字列）。次に、TrustedDNSServers 文字列の例を示します。 161.44.124.*,64.102.6.247 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされます。

例：Trusted Network Detection

Trusted Network Detection を設定するには、次の例を参照してください。この例では、信頼ネットワークの中に存在するときは自動的に VPN 接続を接続解除し、非信頼ネットワークに存在するときは VPN 接続を開始するようにクライアントが設定されます。

```
<AutomaticVPNPolicy>true
    <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
    <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
    <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
    <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

常時接続の VPN および下位機能

常時接続の VPN を選択する場合、フェールオープン ポリシーはネットワーク接続を許可し、フェールクローズ ポリシーはネットワーク接続を無効にします。

表 A-4 に、常時接続の VPN を設定するためのタグ名、オプション、および説明を示します。

表 A-4　常時接続の VPN 設定

XML タグ名	オプション	説明
AutomaticVPNPolicy	true	自動 VPN ポリシーを有効にします。
	false	自動 VPN ポリシーを無効にします。
TrustedDNSDomains	string	クライアントが信頼ネットワーク内に存在するときに、ネットワーク インターフェイスが持つ可能性がある DNS サフィックスを指定します。
TrustedDNSServers	string	クライアントが信頼ネットワーク内にいるときに、ネットワーク インターフェイスが持つ可能性がある DNS サーバ アドレスを指定します。
TrustedNetworkPolicy	disconnect	信頼ネットワークが検知されると、VPN から接続解除します。
	connect	信頼ネットワークが検知されると、VPN に接続します。
	donothing	信頼ネットワークが検知されると VPN に接続しないか、VPN から接続解除します。

表 A-4　常時接続の VPN 設定 （続き）

XML タグ名	オプション	説明
UntrustedNetworkPolicy	connect	非信頼ネットワークが検知されると、VPN から接続解除します。
	disconnect	非信頼ネットワークが検知されると、VPN に接続します。
	donothing	非信頼ネットワークが検知されると VPN に接続しないか、VPN から接続解除します。
AlwaysOn	true	常時接続の VPN を有効にします。
	false	常時接続の VPN を無効にします。
ConnectFailurePolicy	open	AnyConnect が VPN セッションを確立できないとき（たとえば、適応型セキュリティ アプライアンスが到達不能である場合）に、ネットワーク アクセスを制限しません。
	closed	VPN が到達不能の場合でもネットワーク アクセスを制限します。この制限された状態では、コンピュータが接続を許可されているセキュア ゲートウェイに対してのみアクセスが許可されます。
AllowCaptivePortalRemediation	true	ユーザがキャプティブ ポータルを修復できるように、接続障害終了ポリシーによるネットワーク制限が CaptivePortalRemediationTimeout タグで指定した時間（分単位）の間だけ緩和されます。
	false	AnyConnect がキャプティブ ポータルを検出した場合でも、接続障害終了ポリシーによるネットワーク制限を適用します。
CaptivePortalRemediationTimeout	整数型	AnyConnect がネットワーク アクセス制限を解除する時間（分単位）。
ApplyLastVPNLocalResourceRules	true	セキュリティ アプライアンスから受信した最新のクライアント ファイアウォールを適用します。セキュリティ アプライアンスには、ローカル LAN 上のリソースへのアクセスを許可する ACL を含めることができます。
	false	セキュリティ アプライアンスから受信した最新のクライアント ファイアウォールを適用しません。
AllowVPNDisconnect	true	[Disconnect] ボタンを表示して、常時接続の VPN セッションを接続解除するためのオプションをユーザに表示します。ユーザは、再接続する前に代替セキュア ゲートウェイを選択するために、このオプションを使用できます。
	false	[Disconnect] ボタンを表示しません。このオプションは、AnyConnect GUI を使用して VPN を接続解除できないようにします。

注意　AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。このポリシーは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する非常にセキュリティの高い組織向きです。このポリシーでは、スプリット トンネリングによって許可され、ACL によって制限されたすべてのプリンターやテザード デバイスなどのローカル リソース以外のネットワーク アクセスを防止します。ユーザが VPN を越えてインターネットにアクセスする必要がある場合に、セキュア ゲートウェイを利用できないときには、このポリシーを適用すると生産性が低下する可能性があります。AnyConnect はほとんどのキャプティブ ポータルを検出します（「キャプティブ ポータル ホットスポットの検出」（P.3-32）で説明）。キャプティブ ポータルを検出できない場合、接続障害クローズド ポリシーによりすべてのネットワーク接続は制限されます。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障

害オープン ポリシーを使用して常時接続の VPN を展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズド ポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズド ポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

常時接続の VPN：XML の例

リリース 6.3（1）以前の ASDM を使用している場合は、次の例を使用して、AnyConnect XML プロファイルを手動で編集してください。この常時接続の VPN 例では、次の操作を実行します。

- [Disconnect] ボタンを有効にし（AllowVPNDisconnect）、ユーザが VPN セッションを別のセキュア ゲートウェイで確立できるようにします。
- 接続障害ポリシーを closed に指定します。
- キャプティブ ポータルを修復するために、接続障害終了ポリシーによるネットワーク制限が 5 分間緩和されます。
- 最後の VPN セッション中に割り当てられた ACL ルールを適用します。

```
<ClientInitialization>
    <AutomaticVPNPolicy>true
        <TrustedDNSDomains>example.com</TrustedDNSDomains>
        <TrustedDNSServers>1.1.1.1</TrustedDNSServers>
        <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
        <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
        <AlwaysOn>true
            <AllowVPNDisconnect>true</AllowVPNDisconnect>
            <ConnectFailurePolicy>Closed
                <AllowCaptivePortalRemediation>true
                    <CaptivePortalRemediationTimeout>5</CaptivePortalRemediationTimeout>
                </AllowCaptivePortalRemediation>
                <ApplyLastVPNLocalResourceRules>true</ApplyLastVPNLocalResourceRules>
            </ConnectFailurePolicy>
        </AlwaysOn>
    </AutomaticVPNPolicy>
</ClientInitialization>
```

ロード バランシングを備えた常時接続の VPN

表 A-5 に、ロード バランシングと常時接続の VPN を設定するためのタグ名、オプション、および説明を示します。

表 A-5　ロード バランシング設定とともに常時接続の VPN を使用する

XML タグ名	オプション	説明
LoadBalancingServerList	FQDN または IP アドレス	クラスタのバックアップ デバイスを指定します。このオプションを指定しないと、常時接続の VPN が有効ではない場合に、AnyConnect はロード バランシング クラスタのバックアップ デバイスへのアクセスをブロックします。

例：ロード バランシングを備えた常時接続の VPN

```
<ServerList>
```

```
        <!--
            This is the data needed to attempt a connection to a specific
            host.
          -->
 <HostEntry>
   <HostName>ASA</HostName>
   <HostAddress>10.86.95.249</HostAddress>
  <LoadBalancingServerList>
     <!--
    Can be a FQDN or IP address.
        -->
      <HostAddress>loadbalancing1.domain.com</HostAddress>
      <HostAddress>loadbalancing2.domain.com</HostAddress>
      <HostAddress>11.24.116.172</HostAddress>
</LoadBalancingServerList>
  </HostEntry>
</ServerList>
```

Start Before Logon

表 A-6 に、Start Before Logon を設定するためのタグ名、オプション、および説明を示します。

表 A-6　Start Before Logon の設定

XML タグ名	オプション	説明
UseStartBeforeLogon	true	Start Before Logon を有効にします。
	false	Start Before Logon を無効にします。
UseStartBeforeLogon UserControllable	true	SBL をユーザが制御できるようにします。
	false	デフォルト設定に戻します。デフォルト設定では、ユーザが SBL を制御できません。

例：Start Before Logon

SBL を設定するには、次の例を参照してください。

```
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

Windows の証明書ストア

表 A-7 に、証明書ストアを設定するためのタグ名、オプション、および説明を示します。

表 A-7　証明書ストアの設定

XML タグ名	オプション	説明
CertificateStore	All	（デフォルト）すべての証明書ストアを使用して証明書を検索するよう AnyConnect クライアントに指示します。
	Machine	Windows ローカル マシン証明証ストアへの証明書ルックアップを制限するように AnyConnect クライアントに指示します。
	User	ローカル ユーザ証明証ストアへの証明書ルックアップを制限するように AnyConnect クライアントに指示します。

例：証明書のストア
証明書ストアを設定するには、次の例を参照してください。

```
<CertificateStore>Machine</CertificateStore>
```

証明書ストアの使用の制限

表 A-8 に、証明書ストアの使用を制限するためのタグ名、オプション、および説明を示します。

表 A-8　証明書ストアの制限の設定

XML タグ名	オプション	説明
ExcludeFirefoxNSSCertStore（Linux および Mac）	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）	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）	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）	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）。

証明書のプロビジョニングと更新を行う SCEP プロトコル

表 A-9 に、証明書をプロビジョニングおよび更新するためのタグ名、オプション、SCEP プロトコルの設定に関する説明を示します。

表 A-9　SCEP プロトコル設定

XML タグ名	オプション	説明
CertificateEnrollment		証明書登録の開始タグ。
CertificateExpirationThreshold	number of days	AnyConnect がユーザに証明書の失効が近づいていることを警告するタイミングを指定します。

表 A-9　SCEP プロトコル設定 （続き）

AutomaticSCEPHost	ASA\ 接続プロファイルの完全修飾ドメイン名	この属性で ASA ホスト名が指定され、SCEP 証明書取得用の接続プロファイル（トンネル グループ）が設定されている場合、ホストは自動証明書取得を試行します。
	ASA\ 接続プロファイル名の IP アドレス	
CAURL	完全修飾ドメイン名	
	CA サーバの IP アドレス	
CertificateSCEP		証明書の内容の要求方法を定義します。
CADomain		認証局のドメイン。
Name_CN		証明書の共通名。
Department_OU		証明書で指定されている部門名。
Company_O		証明書で指定されている企業名。
State_ST		証明書で指定されている州 ID。
Country_C		証明書で指定されている国 ID。
Email_EA		電子メール アドレス。
Domain_DC		ドメイン コンポーネント。
DisplayGetCertButton	true	認証の証明書のプロビジョニングまたは更新をユーザが手動で要求できるようにします。通常、ユーザはあらかじめ VPN トンネルを作成する必要なく、認証局にアクセスできます。
	false	認証の証明書のプロビジョニングまたは更新をユーザが手動で要求できないようにします。
ServerList		サーバ リストの開始タグ。サーバ リストは、AnyConnect が最初に起動されたときに表示されます。ユーザは、ログインする ASA を選択できます。
HostEntry		ASA の設定の開始タグ。
HostName		ASA のホスト名。
HostAddress		ASA の完全修飾ドメイン名。

例：SCEP プロトコル

ユーザ プロファイルの SCEP 要素を設定するには、以下の例を参照してください。

```
<AnyConnectProfile>
    <ClientInitialization>
        <CertificateEnrollment>
            <CertificateExpirationThreshold>14</CertificateExpirationThreshold>
            <AutomaticSCEPHost>asa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="true"
Thumbprint="8475B661202E3414D4BB223A464E6AAB8CA123AB">http://ca01.cisco.com</CAURL>
            <CertificateSCEP>
                <CADomain>cisco.com</CADomain>
                <Name_CN>%USER%</Name_CN>
                <Department_OU>Engineering</Department_OU>
                <Company_O>Cisco Systems</Company_O>
                <State_ST>Colorado</State_ST>
                <Country_C>US</Country_C>
                <Email_EA>%USER%@cisco.com</Email_EA>
                <Domain_DC>cisco.com</Domain_DC>
                <DisplayGetCertButton>false</DisplayGetCertButton>
```

```
            </CertificateSCEP>
        </CertificateEnrollment>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>ABC-ASA</HostName>
            <HostAddress>ABC-asa-cluster.cisco.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>Certificate Enroll</HostName>
            <HostAddress>ourasa.cisco.com</HostAddress>
            <AutomaticSCEPHost>ourasa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="false"
Thumbprint="8475B655202E3414D4BB223A464E6AAB8CA123AB">http://ca02.cisco.com</CAURL>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

証明書照合

表 A-10 に、証明書照合を設定するためのタグ名、オプション、および説明を示します。

表 A-10　証明書照合

XML タグ名	オプション	説明
CertificateExpirationThreshold		証明書の有効期限までの日数を指定します。ユーザは証明書の失効が近づいていることについて警告されます。
CertificateMatch	n/a	クライアント証明書選択を調整するプリファレンスを定義します。証明書が認証の一部として使用される場合にのみ含めます。ユーザ証明書を一意に識別するために必要な CertificateMatch サブセクション（KeyUsage、ExtendedKeyUsage、および DistinguishedName）だけをプロファイルに含める必要があります。
KeyUsage	n/a	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を指定します。
MatchKey	Decipher_Only Encipher_Only CRL_Sign Key_Cert_Sign Key_Agreement Data_Encipherment Key_Encipherment Non_Repudiation Digital_Signature	KeyUsage グループの MatchKey 属性で、受け入れ可能なクライアント証明書の選択に使用できる属性を指定します。1 つ以上の照合キーを指定します。指定されたキーの少なくとも 1 つが一致する証明書が選択されます。
ExtendedKeyUsage	n/a	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を選択します。

表 A-10　証明書照合 （続き）

XML タグ名	オプション	説明
ExtendedMatchKey	ClientAuth ServerAuth codeSign EmailProtect IPSecEndSystem IPSecUsers Timestamp OCSPSigns DVCS	ExtendedKeyUsage グループの ExtendedMatchKey で、受け入れ可能なクライアント証明書の選択に使用できる属性を指定します。0 個以上の拡張照合キーを指定します。指定されたすべてのキーが一致する証明書が選択されます。
CustomExtendedMatchKey	既知の MIB OID 値、1.3.6.1.5.5.7.3.11 など。	ExtendedKeyUsage グループで、0 個以上のカスタム拡張照合キーを指定できます。指定されたすべてのキーが一致する証明書が選択されます。キーは、OID 形式で指定する必要があります（1.3.6.1.5.5.7.3.11 など）。
DistinguishedName	n/a	グループ ID。DistinguishedName グループでは、証明書の識別名による照合によって受け入れ可能なクライアント証明書を選択するための、一致基準を指定できます。
DistinguishedNameDefinition	太字はデフォルト値を示します。 • Wildcard: **"Enabled"** "Disabled" • Operator: **"Equal" (==)** "NotEqual" (!==) • MatchCase: **"Enabled"** "Disabled"	DistinguishedNameDefinition で、照合で使用する単一の識別名属性を定義する演算子のセットを指定します。Operator は、照合を実行するときに使用する動作を指定します。MatchCase は、パターン マッチングで大文字と小文字を区別するかどうかを指定します。

表 A-10　証明書照合 （続き）

XML タグ名	オプション	説明
Name	CN DC SN GN N I GENQ DNQ C L SP ST O OU T EA ISSUER-CN ISSUER-DC ISSUER-SN ISSUER-GN ISSUER-N ISSUER-I ISSUER-GENQ ISSUER-DNQ ISSUER-C ISSUER-L ISSUER-SP ISSUER-ST ISSUER-O ISSUER-OU ISSUER-T ISSUER-EA	照合で使用する DistinguishedName 属性。最大で 10 個の属性を指定できます。

表 A-10　証明書照合 （続き）

XML タグ名	オプション	説明
Pattern	二重引用符で囲まれたストリング（1 ～ 30 文字）。ワイルドカードを有効にすると、パターンを文字列内の任意の場所に指定できます。	照合で使用する文字列（パターン）を指定します。この定義では、ワイルドカード パターン マッチはデフォルトで無効になっています。

例：証明書照合

クライアント証明書選択を調整するために使用できる属性を有効にするには、次の例を参照してください。

（注） この例の KeyUsage、ExtendedKeyUsage、および DistinguishedName のプロファイル オプションは単なる例です。CertificateMatch 基準は、使用する証明書に適用するもののみ設定する必要があります。

```
<CertificateMatch>
     <!--
         Specifies Certificate Key attributes that can be used for choosing
         acceptable client certificates.
       -->
    <KeyUsage>
        <MatchKey>Non_Repudiation</MatchKey>
        <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
     <!--
         Specifies Certificate Extended Key attributes that can be used for
         choosing acceptable client certificates.
       -->
    <ExtendedKeyUsage>
        <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
        <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
        <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
    </ExtendedKeyUsage>
     <!--
         Certificate Distinguished Name matching allows for exact
         match criteria in the choosing of acceptable client
         certificates.
       -->
    <DistinguishedName>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled">
            <Name>CN</Name>
            <Pattern>ASASecurity</Pattern>
        </DistinguishedNameDefinition>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
            <Name>L</Name>
            <Pattern>Boulder</Pattern>
        </DistinguishedNameDefinition>
    </DistinguishedName>
</CertificateMatch>
```

自動証明書選択

表 A-11 に、自動証明書選択を設定するためのタグ名、オプション、および説明を示します。

表 A-11　自動証明書選択の設定

XML タグ名	オプション	説明
AutomaticCertSelection	true	AnyConnect は自動的に認証証明書を選択できます。
	false	ユーザに認証証明書を選択するよう求めるプロンプトを表示します。

例：AutomaticCertSelection

AutomaticCertSelection を使用してクライアント プロファイルを設定するには、次の例を参照してください。

```
<AnyConnectProfile>
    <ClientInitialization>
        <AutomaticCertSelection>false</AutomaticCertSelection>
    </ClientInitialization>
</AnyConnectProfile>
```

バックアップ サーバ リスト パラメータ

表 A-12 に、バックアップ サーバ リストを設定するためのタグ名、オプション、および説明を示します。

表 A-12　バックアップ サーバ リストの設定

XML タグ名	オプション	説明
BackupServerList	n/a	グループ ID を判別します。
HostAddress	IP アドレスまたは完全修飾ドメイン名（FQDN）	バックアップ サーバ リストに含めるホスト アドレスを指定します。

例：バックアップ サーバ リスト

バックアップ サーバ リスト パラメータを設定するには、次の例を参照してください。

```
<BackupServerList>
   <HostAddress>bos</HostAddress>
   <HostAddress>bos.example.com</HostAddress>
</BackupServerList>
```

Windows Mobile ポリシー

表 A-13 に、Windows Mobile ポリシーを設定するためのタグ名、オプション、および説明を示します。

（注）　この設定では、すでに存在するポリシーが確認されるだけで、変更されません。

表 A-13　Windows Mobile ポリシー

XML タグ名	オプション	説明
MobilePolicy	n/a	グループ ID を判別します。
DeviceLockRequired	n/a	グループ ID。MobilePolicy グループの DeviceLockRequired は、VPN 接続を確立する前に、パスワードまたは PIN を使用して Windows Mobile デバイスを設定する必要があることを示します。この設定が有効なのは、Microsoft のデフォルト ローカル認証プロバイダー（LAP）を使用する Windows Mobile デバイスだけです。 （注）　AnyConnect クライアントは、Windows Mobile 5.0、WM5AKU2+、および Windows Mobile 6.0 でモバイル デバイス ロックをサポートしますが、Windows Mobile 6.1 ではサポートしません。
MaximumTimeoutMinutes	任意の負ではない整数	DeviceLockRequired グループのこのパラメータに負ではない数値が設定された場合、設定が必要な、デバイス ロックが有効になるまでの最大時間を分単位で指定します。
MinimumPasswordLength	任意の負ではない整数	DeviceLockRequired グループのこのパラメータに負ではない数値が設定された場合、デバイス ロックに使用する PIN またはパスワードの文字数が、指定された数値以上必要であることを示します。 この設定は、強制する前に、Exchange サーバと同期してモバイル デバイスにプッシュする必要があります。（WM5AKU2+）
PasswordComplexity	"alpha"：英数字のパスワードが必要です。 "pin"：数値の PIN が必要です。 "strong"：Microsoft の定義による、強い英数字のパスワードが必要です。7 文字以上で、大文字、小文字、数字、区切り文字のうち少なくとも 3 種類が含まれている必要があります。	指定された場合、左のカラムで示すパスワード サブタイプのチェックが行われます。 この設定は、強制する前に、Exchange サーバと同期してモバイル デバイスにプッシュする必要があります。（WM5AKU2+）

例：Windows Mobile ポリシー
XML を使用して Windows Mobile ポリシーを設定するには、次の例を参照してください。

```
<MobilePolicy>
<DeviceLockRequired>
```

```
    MaximumTimeoutMinutes=”60”
    MinimumPasswordLength=”4”
    PasswordComplexity=”pin”
</DeviceLockRequired>
</MobilePolicy>
```

起動時自動接続

表 A-14 に、起動時自動接続を設定するためのタグ名、オプション、および説明を示します。

表 A-14　起動時自動接続の設定

XML タグ名	オプション	説明
AutoConnectOnStart	true	自動接続設定を開始します。
	false	デフォルトの自動接続設定に戻します。
AutoConnectOnStart UserControllable	true	ユーザ制御属性を挿入します。
	false	ユーザ制御属性を削除します。

例：起動時自動接続
起動時自動接続を設定するには、次の例を参照してください。

```
<AutoConnectOnStart>
true
</AutoConnectOnStart>
```

自動再接続

表 A-15 に、自動再接続を設定するためのタグ名、オプション、および説明を示します。

表 A-15　自動再接続の設定

XML タグ名	オプション	説明
AutoReconnect	true	VPN セッションが中断された場合、クライアントはセッションに割り当てられたリソースを保持し、再接続を試行します。
	false	VPN セッションが中断された場合、クライアントはセッションに割り当てられたリソースを解放し、再接続を試行しません。
AutoReconnectBehavior	DisconnectOnSuspend	AnyConnect はシステムが一時停止したときに VPN セッションに割り当てられたリソースを解放し、システムがレジュームした後で再接続を試行しません。
	ReconnectAfterResume	クライアントは、システムの一時停止中に、VPN セッションに割り当てられたリソースを保持します。システムのレジューム後に、再接続を試行します。

例：自動再接続

クライアントの初期化セクションでの AnyConnect VPN の再接続動作を設定するには、以下の例を参照してください。

```
<AutoReconnect>
    true
</AutoReconnect>

<AutoReconnect UserControllable=”true”>true
<AutoReconnectBehavior
UserControllable=”true”>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

サーバ リスト

表 A-16 に、サーバ リストを設定するためのタグ名、オプション、および説明を示します。

表 A-16　サーバ リストの設定

XML タグ名	オプション	説明
ServerList	n/a	グループ ID を指定します。
HostEntry	n/a	グループ ID。ServerList の子属性。特定のホストへの接続を試行するために必要なデータです。
HostName	ホストを参照するために使用されるエイリアス、FQDN、または IP アドレス。これが FQDN または IP アドレスの場合、HostAddress は必要ありません。	HostEntry グループの HostName パラメータは、サーバ リスト内でホスト名を指定します。
HostAddress	ホストを参照するために使用される IP アドレスまたは完全修飾ドメイン名（FQDN）。HostName が FQDN または IP アドレスの場合、HostAddress は必要ありません。	グループ ID。CertificateMatch の子属性。これらの属性を使用して、受け入れ可能なクライアント証明書を選択します。
PrimaryProtocol	SSL または IPsec	VPN トンネルの暗号化プロトコルは、SSL（デフォルト）または IPsec（IKEv2）のいずれか。 IPsec の場合、クライアントはデフォルトで独自の AnyConnect EAP 認証方式を使用します。
StandardAuthenticationOnly	n/a	StandardAuthenticationOnly パラメータを使用して、認証方式をデフォルトのプロパティ AnyConnect EAP の認証方式から標準ベースの方式に変更します。 この方式に変更すると、クライアントのダイナミック ダウンロード機能が制限され、一部の機能が無効になります。また、セッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定などを設定する ASA の機能が無効になることに注意してください。

表 A-16　サーバ リストの設定 （続き）

XML タグ名	オプション	説明
AuthMethodDuringIKENegotiation	IKE-RSA、EAP-MD5、EAP-MSCHAPv2、EAP-GTC	標準ベース認証の認証方式を指定します。
IKEIdentity	英数字文字列。	標準ベースの EAP 認証方式を選択する場合、このフィールドにクライアント ID としてグループまたはドメインを入力できます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。 デフォルトでは、文字列は *$AnyConnectClient$* です。 文字列に、ターミネータ（たとえば、null または CR）を含めることはできません。
UserGroup	指定されたホストに接続するときに使用する接続プロファイル（トンネル グループ）。 このパラメータはオプションです。	このオプションが存在する場合は、HostAddress とともに使用してグループベースの URL を形成します。 プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。 **（注）** グループ ベースの URL をサポートするには、ASA バージョン 8.0.3 以降が必要です。

例：サーバ リスト
サーバ リストを設定するには、次の例を参照してください。

```
<ServerList>
    <HostEntry>
        <HostName>ASA-01</HostName>
        <HostAddress>cvc-asa01.cisco.com
         </HostAddress>
    </HostEntry>
    <HostEntry>
        <HostName>ASA-02</HostName>
         <HostAddress>cvc-asa02.cisco.com
         </HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa03.cisco.com
            </HostAddress>
         </BackupServerList>
    </HostEntry>
</ServerList>
```

スクリプト化

表 A-17 に、スクリプトを設定するためのタグ名、オプション、および説明を示します。

表 A-17　スクリプトの設定

XML タグ名	オプション	説明
EnableScripting	true	OnConnect スクリプトおよび OnDisconnect スクリプトがあれば、起動します。
	false	（デフォルト）スクリプトを起動しません。
UserControllable	true	ユーザが OnConnect スクリプトおよび OnDisconnect スクリプトの実行を、有効または無効にできます。
	false	（デフォルト）ユーザがスクリプト機能を制御できません。
TerminateScriptOnNextEvent	true	別のスクリプト処理可能なイベントへの移行が発生した場合に、実行中のスクリプト プロセスを終了します。たとえば、VPN セッションが終了すると、AnyConnect は実行中の OnConnect スクリプトを終了します。AnyConnect が新しい VPN セッションを開始すると、実行中の OnDisconnect スクリプトを終了します。Microsoft Windows では、AnyConnect は OnConnect スクリプトまたは OnDisconnect スクリプトが起動した任意のスクリプトと、そのすべての従属スクリプトも終了します。Mac OS および Linux では、AnyConnect は OnConnect スクリプトまたは OnDisconnect スクリプトだけを終了し、子スクリプトは終了しません。
	false	（デフォルト）別のスクリプト処理可能なイベントへの移行が発生しても、スクリプト プロセスを終了しません。
EnablePostSBLOnConnectScript	true	SBL が VPN セッションを確立したときに、OnConnect スクリプトを起動しません。
	false	（デフォルト）SBL が VPN セッションを確立したときに OnConnect スクリプトが存在する場合、OnConnect スクリプトを起動する。

例：スクリプト化

スクリプトを設定するには、次の例を参照してください。

```
<ClientInitialization>

<EnableScripting>true</EnableScripting>

</ClientInitialization>
```

この例では、スクリプトを有効にし、その他のスクリプト パラメータのデフォルト オプションを上書きします。

```
<ClientInitialization>

<EnableScripting UserControllable="true">true
    <TerminateScriptOnNextEvent>true</TerminateScriptOnNextEvent>
    <EnablePostSBLOnConnectScript>false</EnablePostSBLOnConnectScript>
</EnableScripting>

</ClientInitialization>
```

認証タイムアウト コントロール

デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。

表 A-18 に、認証タイマーを変更するためのタグ名、オプション、および説明を示します。

表 A-18　認証タイムアウト コントロール

XML タグ名	オプション	説明
AuthenticationTimeout	10 ～ 120 までの整数	このタイマを変更するには、時間を秒数で入力してください。

例：認証タイムアウト コントロール
次の例では、認証タイムアウトを 20 秒に変更しています。

```
<ClientInitialization>
    <AuthenticationTimeout>20</AuthenticationTimeout>
</ClientInitialization>
```

プロキシの無視

表 A-19 に、プロキシの無視を設定するためのタグ名、オプション、および説明を示します。

表 A-19　プロキシの無視の設定

XML タグ名	オプション	説明
ProxySettings	IgnoreProxy	プロキシの無視を有効にします。
	native	サポートされていません。
	override	サポートされていません。

例：プロキシの無視
クライアントの初期化セクションでプロキシの無視を設定するには、次の例を参照してください。

```
<ProxySettings>IgnoreProxy</ProxySettings>
```

Windows ユーザのための、RDP セッションからの AnyConnect セッションの許可

表 A-20 に、RDP セッションを設定するためのタグ名、オプション、および説明を示します。

表 A-20　RDP セッションからの AnyConnect セッションの許可

XML タグ名	オプション	説明
WindowsLogonEnforcement	SingleLocalLogon	VPN 接続の全体で、ログインできるローカル ユーザは 1 人だけです。この設定では、1 人以上のリモート ユーザがクライアント PC にログオンしているときに、ローカル ユーザが VPN 接続を確立できます。VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログオンは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログオンが接続解除されるかどうかは、VPN 接続のルーティング設定によって決まります。SingleLocalLogin 設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。
	SingleLogon	VPN 接続の全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、その VPN 接続は終了します。
WindowsVPNEstablishment	LocalUsersOnly	リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect クライアントの機能と同じ機能です。
	AllowRemoteUsers	リモート ユーザが VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。

例：Windows ユーザのための、RDP セッションからの AnyConnect セッションの許可
RDP セッションから AnyConnect セッションを設定するには、次の例を参照してください。

```
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>

<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
```

L2TP または PPTP を介した AnyConnect

表 A-21 に、L2TP または PPTP を介した AnyConnect を設定するためのタグ名、オプション、および説明を示します。

表 A-21　L2TP または PPTP を介した AnyConnect

XML タグ名	オプション	説明
PPPExclusion	automatic	PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
	override	これも、PPP 除外を有効にします。自動検知による PPP サーバの IP アドレスの取得に失敗し、PPPExclusion UserControllable 値が true の場合は、「ユーザによる PPP 除外の上書き」（P.3-79）の手順に従ってください。
	disabled	PPP 除外を適用しません。

表 A-21　L2TP または PPTP を介した AnyConnect （続き）

XML タグ名	オプション	説明
PPPExclusionServerIP	true	PPP サーバの IP アドレスを使用します。
	false	PPP サーバの IP アドレスを使用しません。
PPPExclusion UserControllable=	true	ユーザが PPP 除外設定の読み取りおよび変更を実行できます。
	false	ユーザは PPP 除外設定を表示および変更できません。

例：L2TP または PPTP を介した AnyConnect

AnyConnect over L2TP または PPTP を設定するには、次の例を参照してください。

```
<ClientInitialization>
    <PPPExclusion UserControllable="true">Automatic
        <PPPExclusionServerIP UserControllable="true">127.0.0.1</PPPExclusionServerIP>
    </PPPExclusion>
    </ClientInitialization>
        <ServerList>
        <HostEntry>
            <HostName>DomainNameofASA</HostName>
            <HostAddress>IPaddressOfASA</HostAddress>
        </HostEntry>
         </ServerList>
</AnyConnectProfile>
```

その他の AnyConnect プロファイル設定

表 A-22 に、ClientInitialization セクションに挿入できるその他のパラメータを示します。

表 A-22　その他の AnyConnect プロファイル設定

XML タグ名	オプション	説明
CertificateStoreOverride	true	管理者は、Windows コンピュータの証明書ストアの証明書を検索するよう AnyConnect に指示できます。このタグは、証明書がこのストアに格納されていて、ユーザがデバイスに対して管理者特権を持っていないときに有効になります。マシン証明書を使用して Windows 7 または VISTA に接続するには、このオプションが有効にされている事前に展開されたプロファイルが必要です。接続する前に Windows 7 または VISTA のデバイスにこのプロファイルが存在しない場合、証明書はマシン ストアにアクセスできず、接続は失敗します。
	false	（デフォルト）AnyConnect は Windows コンピュータの証明書ストア内の証明書を検索しません。
ShowPreConnectMessage	true	管理者は、ユーザが初めて接続を試行する前にワンタイム メッセージを表示させることができます。たとえば、メッセージを表示して、ユーザにスマート カードをリーダに挿入するよう促すことができます。このメッセージは、AnyConnect メッセージ カタログに表示され、ローカライズされています。
	false	（デフォルト）ユーザが初めて接続を試行する前にメッセージが表示されません。

表 A-22　その他の AnyConnect プロファイル設定 （続き）

XML タグ名	オプション	説明
MinimizeOnConnect	true	（デフォルト）VPN トンネルが確立されているときの AnyConnect GUI の動作を制御します。デフォルトでは、VPN トンネルが確立されているときには、GUI は最小化されます。
	false	AnyConnect GUI の動作は制御されません。
LocalLanAccess	true	ローカル LAN アクセスがセキュア ゲートウェイ上のリモート クライアントに対して有効のとき、ユーザはローカル LAN アクセスを受け入れるか、あるいは拒否することができます。
	false	（デフォルト）ローカル LAN アクセスを拒否します。
AutoUpdate	true	（デフォルト）新規パッケージを自動的にインストールします。
	false	新規パッケージをインストールしません。
RSASecurIDIntegration	automatic	（デフォルト）管理者は、ユーザと RSA との相互作用方法を制御できます。デフォルトでは、AnyConnect が RSA の適切な相互作用方法を決定します。管理者は RSA をロックするか、ユーザが制御できるようにすることができます。
	software token	
	hardware token	
RetainVPNOnLogoff	true	ユーザが Windows オペレーティング システムをログオフしたときに、VPN セッションを保持します。
	false	（デフォルト）ユーザが Windows オペレーティング システムをログオフすると、VPN セッションを停止します。
UserEnforcement	AnyUser	別のユーザがログオンしても、VPN セッションを続行します。RetainVPNPnLogoff が true で、VPN セッションがアップ状態のときにの元のユーザが Windows をログオフした場合にのみ、この値が適用されます。
	SameUserOnly	別のユーザがログオンすると、VPN セッションを終了します。