CHAPTER 10

# 相互運用性のガイドラインおよび要件

この章では、次の方法について説明します。



## 検疫を使用した非準拠クライアントの制限

検疫の使用により、VPN 接続を開始しようとしている特定のクライアントを制限することができます。ASA は制限付き ACL をセッションに適用し、[Configuration] > [Remote Access VPN] > [Network (Client) Access or Clientless SSL VPN Access] > [Dynamic Access Policies] で設定されたダイナミック アクセス ポリシーに基づいて制限付きグループを形成します。エンドポイントが管理面で定義されているポリシーに準拠していない場合でも、ユーザは（アンチウイルス アプリケーションのアップデートなど）サービスにアクセスして修復できますが、ユーザに制限がかけられます。修復後、ユーザは再接続できます。この再接続により、新しいポスチャ アセスメントが起動されます。このアセスメントに合格すると、ユーザは制限なしで接続されます。

### 検疫要件

検疫時には、適応型セキュリティ アプライアンスで AnyConnect Premium ライセンスがアクティブになっている必要があります。Advanced Endpoint Assessment は、アンチウイルス、スパイウェア、およびファイアウォールなどのアプリケーションのダイナミック ポリシー要件、また関連付けられている任意のアプリケーション定義ファイル要件に準拠しないエンドポイントを修復します。Advanced Endpoint Assessment は Cisco Secure Desktop のホスト スキャン機能であるため、AnyConnect では、Windows Mobile も含めて、AnyConnect でサポートされるすべての OS での検疫がサポートされます。

ASA リリース 8.3（1）以降では、ユーザに対して最初に検疫が通知されるときに、AnyConnect GUI にユーザ メッセージを表示するダイナミック アクセス ポリシーおよびグループ ポリシーの機能を備えています。その他の検疫メッセージ（「Quarantined - Remediation Required」および「To attempt a normal connection, please reconnect」など）もレポートされますが、これらのメッセージは管理者が定義してユーザに表示することはできません。検疫では ASA をアップグレードする必要はなく、ユーザ メッセージでのみ ASA のアップグレードが必要です。

ASA ソフトウェアをアップグレードする場合、新機能を設定できるようにするため ASDM をリリース 6.3（1）以降にアップグレードすることもお勧めします。

AnyConnect は、Windows Mobile など AnyConnect でサポートされているすべての OS での検疫をサポートします。クライアントは、Windows 7、Vista、XP、および Mac OS と Linux で検疫ユーザ メッセージをサポートしますが、Windows Mobile ではサポートしません。

## 検疫の設定

検疫を設定するには、次の手順を実行します。

**ステップ 1**　（任意）非準拠コンピュータを修復するよう Host Scan を設定するには、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] > [Advanced Endpoint Assessment] を選択します。

**ステップ 2**　[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択して [Add] をクリックし、非準拠コンピュータを識別するエンドポイント属性を使用する DAP を作成します。[Action] タブをクリックし、[Quarantine] をクリックします。

**ステップ 3**　（任意指定）検疫されたセッションのユーザに表示するメッセージを入力します。

ダイナミック アクセス ポリシーの設定の詳細を知りたい場合は、ASDM ヘルプをご覧ください。

# Microsoft Active Directory を使用して、ドメイン ユーザの Internet Explorer の信頼済みサイト リストにセキュリティ アプライアンスを追加する方法

Active Directory のドメイン管理者は、グループ ポリシーをドメイン ユーザにプッシュして、Internet Explorer の信頼済みサイトのリストにセキュリティ アプライアンスを追加できます。これは、ユーザが個別に信頼済みサイトのリストにセキュリティ アプライアンスを追加する手順とは異なります。この手順は、ドメイン管理者が管理している Windows マシンの Internet Explorer にのみ適用されます。

セキュリティ アプライアンスでは、フィルタリング テーブルに格納されているデータを使用して、ドメイン名および IP アドレス パス セグメントなどの URL 要求属性が評価され、ローカルで保持されているデータベース レコードと照合されます。一致が見つかった場合、アクセス ポリシー設定によりアクションが決定されて、トラフィックがブロックまたはモニタリングされます。一致が見つからない場合は、プロセスが続行されます。

**（注）**　Windows Vista または Windows 7 を実行していて、WebLaunch を使用する予定のユーザは、セキュリティ アプライアンスを Internet Explorer の信頼済みサイトのリストに追加する必要があります。

Active Directory を使用して、グループ ポリシーによってセキュリティ アプライアンスを Internet Explorer の信頼済みサイト セキュリティ ゾーンに追加するポリシーを作成するには、次の手順を実行します。

**ステップ 1**　Domain Admins グループのメンバーとしてログインします。

**ステップ 2**　[Active Directory Users and Computers MMC] スナップインを開きます。

**ステップ 3**　グループ ポリシー オブジェクトを作成するドメインまたは組織ユニットを右クリックして、[Properties] をクリックします。

**ステップ 4**　[Group Policy] タブを選択して、[New] をクリックします。

**ステップ 5**　新しいグループ ポリシー オブジェクトの名前を入力して、Enter を押します。

**ステップ 6**　一部のユーザまたはグループにこの新しいポリシーが適用されないようにするには、[Properties] をクリックします。[Security] タブを選択します。このポリシーを適用 *しない* ユーザまたはグループを追加し、[Allow] カラムの [Read] チェックボックスと [Apply Group Policy] チェックボックスをオフにします。[OK] をクリックします。

**ステップ 7**　[Edit] をクリックして、[User Configuration] > [Windows Settings] > [Internet Explorer Maintenance] > [Security] を選択します。

**ステップ 8**　右側のペインで [Security Zones and Content Ratings] を右クリックし、[Properties] をクリックします。

**ステップ 9**　[Import the current security zones and privacy settings] を選択します。プロンプトが表示されたら、[Continue] をクリックします。

**ステップ 10**　[Modify Settings] をクリックし、[Trusted Sites] を選択して、[Sites] をクリックします。

**ステップ 11**　信頼済みサイトのリストに追加するセキュリティ アプライアンスの URL を入力し、[Add] をクリックします。フォーマットは、ホスト名（https://vpn.mycompany.com）または IP アドレス（https://192.168.1.100）です。完全一致（https://vpn.mycompany.com）を使用することも、ワイルドカード（https://*.mycompany.com）を使用することもできます。

**ステップ 12**　[Close] をクリックし、すべてのダイアログボックスが閉じるまで [OK] をクリックします。

**ステップ 13**　ドメインまたはフォレスト全体にポリシーが伝搬されるまで待ちます。

**ステップ 14**　[Internet Options] ウィンドウで [OK] をクリックします。

# AnyConnect および Cisco Secure Desktop を CSA と相互運用するための設定方法

リモート ユーザに Cisco Security Agent（CSA）がインストールされている場合は、AnyConnect および Cisco Secure Desktop を ASA と相互運用できるように、CSA ポリシーをリモート ユーザにインポートする必要があります。

これを実行するには、次のステップを実行します。

**ステップ 1**　AnyConnect および Cisco Secure Desktop の CSA ポリシーを取得します。次の場所からファイルを取得できます。

- ASA に同梱の CD
- ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェア ダウンロード ページ（http://www.cisco.com/cgi-bin/tablebuild.pl/asa）

ファイル名は、AnyConnect-CSA.zip および CSD-for-CSA-updates.zip です。

**ステップ 2**　.zip パッケージ ファイルから、.export ファイルを展開します。

**ステップ 3**　インポートする正しいバージョンの .export ファイルを選択します。CSA バージョン 5.2 以降の場合は、バージョン 5.2 のエクスポート ファイルです。CSA バージョン 5.0 および 5.1 の場合は、5.x のエクスポート ファイルです。

**ステップ 4**　CSA Management Center の [Maintenance] > [Export/Import] タブを使用して、ファイルをインポートします。

**ステップ 5**　VPN ポリシーに新しいルール モジュールを追加して、ルールを生成します。

詳細については、CSA のマニュアル『*Using Management Center for Cisco Security Agents 5.2*』を参照してください。ポリシーのエクスポートに関する情報は、「*Exporting and Importing Configurations*」の項にあります。

# AnyConnect およびレガシー VPN クライアントのポート情報

表 10-1 および表 10-2 に、レガシー Cisco VPN クライアントから Cisco AnyConnect Secure Mobility Client にユーザを移行する際に役立つポート情報を示します。

**表 10-1　AnyConnect Client により使用されるポート**

| プロトコル | Cisco AnyConnect Client ポート |
|---|---|
| TLS（SSL） | TCP 443 |
| SSL リダイレクション | TCP 80（任意） |
| DTLS | UDP 443（任意、ただし*強く*推奨） |
| IPsec/IKEv2 | UDP 500、UDP 4500 |

**表 10-2　Cisco VPN（IPsec）Client により使用されるポート**

| プロトコル | Cisco VPN Client（IPsec）ポート |
|---|---|
| IPsec/NATT | UDP 500、UDP 4500 |
| IPsec/NATT | UDP 500、UDP 4500 |
| IPsec/TCP | TCP（設定可能） |
| IPsec/UDP | UDP 500、UDP X（設定可能） |

# サブネット内でのトラフィックのクライアント スプリット トンネリング動作の違い

AnyConnect クライアントおよびレガシー Cisco VPN（IPsec/IKEv1 クライアント）は、ASA によって割り当てられた IP アドレスと同じサブネット内のサイトにトラフィックを渡す場合、動作が異なります。AnyConnect では、クライアントは、設定済みのスプリット トンネリング ポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内に含まれるすべてのサイトにトラフィックを渡します。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。

これとは対照的に、レガシー Cisco VPN Client は、クライアントに割り当てられたサブネットに関係なく、スプリット トンネリング ポリシーで指定されたアドレスだけにトラフィックを渡します。

そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。