ポスチャの設定

AnyConnect Secure Mobility Client は ASA ポスチャ モジュールおよび ISE ポスチャ モジュールを提供します。両方のモジュールにより、Cisco AnyConnect Secure Mobility Client で、ホストにインストールされたアンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェアなどについてエンドポイントのコンプライアンスを評価できます。その後、エンドポイントがコンプライアンスに対応するまでネットワーク アクセスを制限したり、修復方法を確立できるようにローカル ユーザの権限を強化したりできます。

ASA ポスチャは、hostscan_version.pkg にバインドされています。これは、どのようなオペレーティング システム、アンチウイルス、アンチスパイウェア、およびソフトウェアがホストにインストールされているかを収集するアプリケーションです。ISE ポスチャは、ISE 制御ネットワークにアクセスするときに、AnyConnect と NAC Agent の両方を展開するのではなく、1 つのクライアントを展開します。ISE ポスチャは、AnyConnect 製品に（Web セキュリティやネットワーク アクセス マネージャなどと同じように）追加のセキュリティ コンポーネントとしてインストールできるモジュールです。リリース 3.x の AnyConnect バンドルの一部であった HostScan は、別個にインストールされるようになりました。

ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。エンドポイントがコンプライアンス対応かどうかを実際には ISE が判断する場合でも、ISE はエンドポイント独自のポリシー評価を利用します。

一方、HostScan はサーバ側評価を実行します。ASA がエンドポイント属性（オペレーティング システム、IP アドレス、レジストリ エントリ、ローカル証明書、ファイル名など）のリストのみを要求し、これらが HostScan によって返されます。ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

（注） 2 つの異なるポスチャ エージェントを実行すると予期しない結果が生じる可能性があるため、HostScan と ISE ポスチャ エージェントの組み合わせは推奨されません。

次のポスチャ チェックは、HostScan ではサポートされますが、ISE ポスチャではサポートされません。

- ホストネーム

- IP アドレス
- MAC アドレス
- ポート番号
- OPSWAT バージョン
- BIOS シリアル番号
- パーソナル ファイアウォール
- チェックサム検証によるファイル チェック
- 証明書フィールド属性

ISE ポスチャ モジュールの提供内容

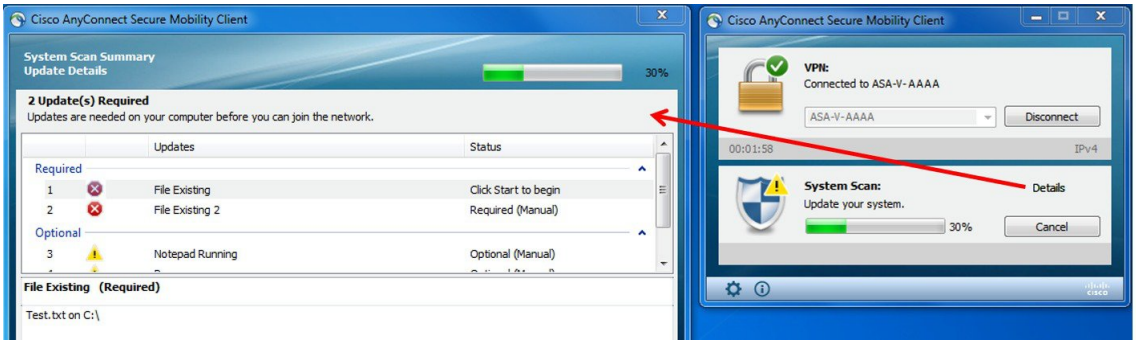
ポスチャ チェック

ISE ポスチャ モジュールはポスチャ チェックの実行に OPSWAT v3 ライブラリを使用します。初回のポスチャ チェックでは、すべての必須要件への一致に失敗したエンドポイントがすべて非準拠と見なされます。その他のエンドポイントの許可ステータスは、ポスチャ不明または準拠（必須要件に合致）です。

ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。

必要な修復

修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。AnyConnect UI の ISE ポスチャ タイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。必須の手動修復が存在する場合、修復ウィンドウが開き、対処が必要な項目が表示されます。この [システム スキャンの概要：アップデートの詳細（System Scan Summary: Update Details）] ウィンドウに、アップデートの進捗状況、割り当てられたアップデート時間の残り時間、すべての要件のステータス、およびシステムの準拠状態が表示されます。



管理者は、ISE ポスチャ プロセスの最後に表示されるネットワーク使用ポリシーを設定できます。ポリシーにアクセスすると、VLAN へのアクセス権が付与される前にユーザが同意する必要のある必須の諸条件がすべて表示されます。

オプションのアップデートのみが残っている場合、[スキップ（Skip）] を選択して次の更新に進むことも、[すべてスキップ（Skip All）] を選択して残りの修復をすべて無視することも可能です。時間を節約するためにオプションの修復をスキップしても、ネットワーク アクセスは維持されます。

修復後（または修復が必要でない場合は要件チェック後）、アクセプタブルユースポリシーの通知を受け取る場合があります。この場合、ネットワーク アクセスのポリシーに同意する必要があり、同意しなかった場合はアクセスが制限されます。修復のこの部分では、AnyConnect UI のポスチャ タイル部分に、「システム スキャン：ネットワークのアクセプタブルユース ポリシー（System Scan: Network Acceptable Use Policy）」と表示されます。

修復が完了すると、必須アップデートとしてリストされたチェック項目がすべて [完了（Done）] ステータスとなり、緑色のチェックボックスが表示されます。修復後、エージェントは ISE にポスチャ結果を送信します。

（注） Symantec 製品のアーキテクチャの変更に伴い、ISE ポスチャでは Symantec AV 12.1.x 以降の修復がサポートされません。

パッチ管理チェックと修復

AnyConnect 4.x および Microsoft System Center Configuration Manager（SCCM）の統合により、重要なパッチのみを対象としたパッチ管理チェックとパッチ管理修復が導入されました。エンドポイントで重要なパッチの更新状況をチェックした後、Windows OS ソフトウェア パッチが欠落している場合にだけ修復が実行されることがわかります。欠落が無ければ、パッチ管理チェックはそのまま終了します。

ISE のポリシー状態の設定方法については http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010010.html#task_A0E2F8D2BF5F4F2EA75B6E6E67CA393Dhttp://を参照してください。またパッチ管理修復の詳細については http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_011110.html#reference_E6D05562981847AFAC2BCE9D1E4A22F8を参照してください。

エンドポイント コンプライアンスの再評価

エンドポイントがコンプライアンス対応と見なされ、ネットワーク アクセスが許可されると、管理者が設定した制御に基づいてエンドポイントを任意で定期的に再評価できます。パッシブ再評価ポスチャ チェックは、初期のポスチャ チェックとは異なります。失敗した場合、ユーザには修復するオプションが与えられます（管理者がそのように設定していた場合）。この構成設定では、1 つ以上の必須要件が満たされていない場合でも、ユーザが信頼ネットワーク アクセスを維持するかどうかを制御します。初期のポスチャ評価では、すべての必須要件が満たされていないと、エンドポイントはコンプライアンス非対応と見なされます。管理者は、結果を [続行（Continue）]、[ログオフ（Logoff）]、または [修復（Remediate）] に設定し、適用や猶予時間など他のオプションを設定できます。

ISE UI のこの機能はデフォルトでは無効であり、ユーザ ロールに対して有効になっている場合、ポスチャは 1 ～ 24 時間ごとに再評価されます。

自動コンプライアンス

ポスチャ リースにより、ISE サーバは、ポスチャを完全にスキップし、簡単にシステムを準拠状態にすることができます。この機能により、ユーザは、自分のシステムが最近ポスチャされている場合に、ネットワーク間の切り替えによる遅延を感じることがありません。ISE ポスチャ エージェントは、単に、ISE サーバが検出されたすぐ後に、システムが準拠しているかどうかを示すステータス メッセージを UI に送信します。ISE の UI（[設定（Settings）] > [ポスチャ（Posture）] > [一般設定（General Settings）]）で、最初のコンプライアンス チェックの後にエンドポイントがポスチャ準拠と見なされる時間を指定できます。ユーザがある通信インターフェイスから別の通信インターフェイスに切り替えた場合でも、コンプライアンス ステータスは維持されることが予期されています。

（注） ポスチャ リースでは、ISE でセッションが有効な場合に、エンドポイントがポスチャ不明状態から準拠状態に移行することが予期されます。

VLAN のモニタリングと遷移

サイトによっては、異なる VLAN またはサブネットを使用して、企業グループおよびアクセス レベル用にネットワークを分割しています。ISE からの認可変更（CoA）では、VLAN の変更を指定します。変更は、セッション終了など管理者のアクションによって発生することもあります。VPN 接続中の VLAN 変更をサポートするには、ISE ポスチャ プロファイルに次の設定を行います。

- [VLAN 検出間隔（VLAN Detection Interval）]：エージェントが VLAN の遷移を検出する頻度およびモニタリングを無効にするかどうかを決定します。VLAN モニタリングは、この間隔が 0 以外の値に設定されている場合に有効になります。Mac OS X の場合、この値は 5 以上に設定します。

  VLAN モニタリングは Windows と Mac OS X の両方に実装されていますが、Mac では予期しない VLAN 変更を検出するためにのみ必要です。VPN が接続される場合、または acise（メインの AnyConnect ISE プロセス）が実行されていない場合は、自動的に無効になります。有効な値の範囲は 0 ～ 900 秒です。

- [エージェント IP 更新の有効化（Enable Agent IP Refresh）]：オフにすると、ISE はエージェントに [ネットワーク遷移遅延（Network Transition Delay）] 値を送信します。オンにすると、ISE はエージェントに DHCP リリースおよび更新の値を送信し、エージェントは IP 更新を行って最新の IP アドレスを取得します。

- [DHCP リリース遅延（DHCP release delay）] と [DHCP 更新遅延（DHCP renew delay）]：IP 更新および [エージェント IP 更新の有効化（Enable Agent IP Refresh）] 設定との相関で使用されます。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスをオンにし、この値が 0 でない場合、エージェントはリリース遅延秒数を待機し、IP アドレスを更新し、更新遅延秒数を待機します。VPN が接続されている場合、IP 更新は自動的に無効になります。

- [ネットワーク遷移遅延（Network Transition Delay）]：（[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスで）VLAN モニタリングがエージェントによって無効または有効にされた場合に使用されます。この遅延により、VLAN が使用されていない場合にはバッファが追加され、サーバからの正確なステータスを待機する十分な時間がエージェントに与えられます。ISE はエージェントにこの値を送信します。また、ISE UI のグローバル設定に [ネットワーク遷移遅延（Network Transition Delay）] 値を設定した場合、ISE ポスチャ プロファイル エディタの値でその値が上書きされます。

（注） ASA は VLAN 変更をサポートしないため、クライアントが ASA を介して ISE に接続されているときには、これらの設定は適用されません。

トラブルシューティング

ポスチャの完了後にエンドポイント デバイスがネットワークにアクセスできない場合は、次の点を確認してください。

- VLAN 変更は ISE UI で設定されていますか。
  - 設定されている場合、DHCP リリース遅延および更新遅延がプロファイルに設定されていますか。
  - どちらの設定も 0 の場合、[ネットワーク遷移遅延（Network Transition Delay）] がプロファイルに設定されていますか。

AnyConnect ISE フローを中断する操作

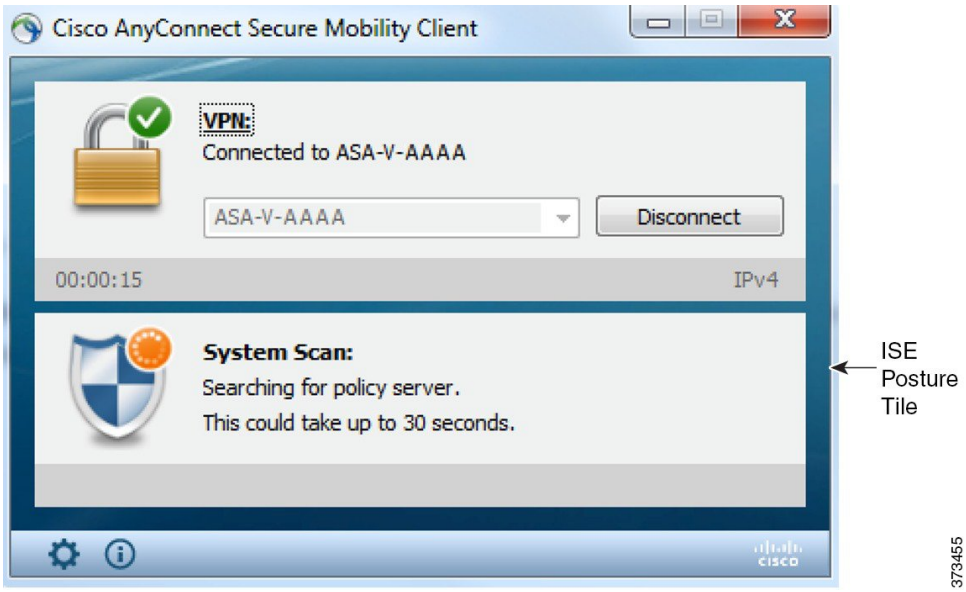
さまざまな理由から、AnyConnect ISE ポスチャ フローは最初のポスチャ再アセスメントまたはパッシブ再アセスメント中に中断されることがあります。

- ユーザが AnyConnect ISE をキャンセルする：ポスチャのチェックと修復の期間に、ユーザは AnyConnect ISE をキャンセルできます。UI にはキャンセルが進行中であることがただちに通知されますが、これはエンドポイントを問題のある状態にすることを回避するときにだけ発生します。サードパーティ ソフトウェアを使用している場合、キャンセル操作によってはリブートが必要な場合があります。キャンセル後、AnyConnect UI のポスチャ タイル部分には、準拠状態が示されます。
- 修復タイマーが期限切れになる：ポスチャ要件を満たすための管理者制御時間が終了しました。アセスメント レポートがヘッドエンドに送信されます。パッシブ再アセスメント時には、ユーザはネットワーク アクセスを保持し、ポスチャ アセスメントでは、必須要件すべてが満たされた場合にネットワーク アクセスが許可されます。
- ポスチャ チェック中のエラー：ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- 修復中のエラー：修復フェーズでエラーが発生し、AnyConnect ISE ポスチャが続行可能な場合は、ユーザに通知されます。失敗した修復ステップが必須のポスチャ要件と関連付けられている場合、AnyConnect ISE ポスチャは修復プロセスを停止します。失敗した修正ステップがオプションのポスチャの要件に関連付けられている場合は、次のステップに進んで ISE ポスチャ操作を終了しようとします。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- デフォルト ゲートウェイの変更：デフォルト ゲートウェイに対する変更により、ユーザが信頼ネットワークへのアクセスを失う場合があります。これにより、ISE ポスチャは ISE の再検出を試みます。AnyConnect UI の ISE ポスチャ タイル部分では、再検出モードに入ると ISE ポスチャのステータスが表示されます。
- AnyConnect と ISE 間の接続の喪失：エンドポイントが準拠状態と見なされてネットワーク アクセスが許可された後に、さまざまなネットワーク シナリオが発生する可能性があります。エンドポイントがネットワーク接続を完全に失う場合があります。ISE がダウンする場

合があります。ISE ポスチャが失敗する場合があります（セッション タイムアウト、手動リスタートなどによる）。ASA の背後の ISE が VPN トンネルを喪失する場合があります。

ISE ポスチャのステータス

AnyConnect ISE ポスチャが機能し、想定どおりにネットワーク アクセスをブロックしている場合に、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：ポリシー サーバを検索しています（System Scan: Searching for policy server）] と表示されます。Windows タスク マネージャまたは Mac OS X システム ログには、プロセスが実行中であると示される場合があります。サービスが実行されていない場合は、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：サービスは使用できません（System Scan: Service is unavailable）] と表示されます。



ネットワークを変更すると、検出フェーズが開始されます。AnyConnect ISE ポスチャの場合、プライマリ インターフェイスのデフォルト ルートが変更された場合、エージェントが検出プロセスに戻ります。たとえば、WiFi およびプライマリ LAN が接続された場合、エージェントは検出をリスタートします。同様に、WiFi およびプライマリ LAN が接続されたものの、その後、WiFi の接続が解除された場合、エージェントは検出をリスタートしません。

また、「システム スキャン」後、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに次のステータス メッセージが表示される場合があります。

- [限定的または接続なし（Limited or no connectivity）]：接続がないため検出は発生していません。AnyConnect ISE ポスチャ エージェントは、ネットワーク上の不正なエンドポイントで検出を実行している可能性があります。
- [システム スキャンは現在の WiFi では不要（System scan not required on current WiFi）]：セキュアでない WiFi が検出されたため検出は発生していません。AnyConnect ISE ポスチャ エー

ジェントは、LAN、ワイヤレス（802.1X 認証が使用されている場合）、および VPN でのみ検出を開始します。WiFi がセキュアでないか、またはエージェント プロファイルで OperateOnNonDot1XWireless を 1 に設定してこの機能を無効にしています。

- [不正なポリシー サーバ（Unauthorized policy server）]：ネットワーク アクセスが制限されているか存在しないため、ホストが ISE ネットワークのサーバ名ルールに一致していません。
- [AnyConnect ダウンローダが更新を実行しています…（The AnyConnect Downloader is performing update...）]：ダウンローダが呼び出され、パッケージバージョンを比較し、AnyConnect 設定をダウンロードし、必要なアップグレードを行います。
- [システムをスキャンしています...（Scanning System...）]：アンチウイルス/アンチスパイウェアのセキュリティ製品のスキャンが開始されました。このプロセス中にネットワークが変更された場合、エージェントはログ ファイルの生成プロセスをリサイクルし、ステータスは [検出されたポリシー サーバなし（No policy server detected）] に戻ります。
- [AnyConnect スキャンのバイパス（Bypassing AnyConnect scan）]：ネットワークは、Cisco NAC Agent を使用するように設定されています。
- [ユーザによってキャンセルされた信頼できないポリシー サーバ（Untrusted Policy Server Cancelled by the user）]：AnyConnect UI の [システム スキャン プリファレンス（System Scan Preferences）] タブで信頼できないサーバへの接続のブロックを解除すると、ポップアップ ウィンドウに AnyConnect ダウンローダのセキュリティ警告が表示されます。この警告ページで [接続のキャンセル（Cancel Connection）] をクリックすると、[ISE ポスチャ（ISE Posture）] タイルがこのステータスに変わります。
- [ネットワークの利用規定（Network Acceptable Use Policy）]：ネットワークへのアクセスには、アクセプタブル ユース ポリシーを確認し、受け入れる必要があります。ポリシーを拒否すると、ネットワーク アクセスが制限される可能性があります。
- [ネットワーク設定の更新（Updating Network Settings）]：ISE UI の [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] では、ネットワーク遷移間で発生させる遅延の秒数を指定できます。
- [コンプライアンス非対応。更新時間の期限が切れました。（Not Compliant. Update time expired.）]：修復のために設定された時間の期限が切れました。
- [コンプライアンス対応。ネットワーク アクセスが許可されています。（Compliant. Network access allowed.）]：修復が完了しました。[システム スキャン（System Scan）] > [スキャン概要（Scan Summary）] にも、ステータスが完了と示されます。
- [検出されたポリシー サーバなし（No policy server detected）]：ISE ネットワークが見つかりません。30 秒後、エージェントによるプローブは低下します。デフォルトのネットワーク アクセスが有効になります。

エンドポイントの同時ユーザ

AnyConnect ISE は、複数のユーザが同時にエンドポイントにログインしてネットワーク接続を共有した場合、個別のポスチャ評価をサポートしません。最初に AnyConnect ISE を実行したユーザ

が正常にポスチャされ、エンドポイントに信頼ネットワーク アクセスが許可されると、エンドポイントの他のすべてのユーザがネットワーク アクセスを継承します。これを防ぐため、管理者はエンドポイントに同時ユーザを許可する機能を無効にできます。

ポスチャ モジュールのロギング

ISEポスチャの場合、イベントはネイティブ オペレーティング システムのイベント ログ（Windows イベント ログ ビューアまたは Mac OS X システム ログ）に記録されます。

ASA ポスチャの場合、エラーおよび警告は syslog（Windows 以外の場合）とイベント ビューア（Windows の場合）に送信されます。使用可能なすべてのメッセージがログ ファイルに記録されます。

ASA ポスチャ モジュール コンポーネントは、オペレーティング システム、特権レベル、および起動メカニズム（Web 起動または AnyConnect）に基づいて、次の 3 つのログに出力します。

- cstub.log：AnyConnect Web 起動が使用された場合にログを取り込みます。
- libcsd.log：ASA ポスチャ API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成される、ASA ポスチャのメインのログです。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。

ポスチャ モジュールのログ ファイルと場所

ISE ポスチャの場合、イベントはインストールされた AnyConnect バージョンの独自のサブフォルダに含まれているため、AnyConnect イベントの他の部分から容易に分離できます。各ビューアでは、キーワードの検索およびフィルタリングが可能です。Web Agent イベントは、標準のアプリケーション ログに書き込まれます。

トラブルシューティングのために、ISE ポスチャ要件ポリシーとアセスメント レポートがイベントログではなく、エンドポイントの別の難解化されたファイルに記録されます。一部のログ ファイル サイズ（aciseposture など）は、管理者がプロファイルに設定できますが、UI ログ サイズは事前に定義されています。

プロセスが異常終了したときは、他の AnyConnect モジュールと同じように、常にミニダンプ ファイルが生成されます。

ASA ポスチャの場合、ファイルはユーザのホーム フォルダの次のディレクトリにあります。

- （Windows 以外）：.cisco/hostscan/log
- （Windows）：Win7/Win8

  C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

OPSWAT サポート表

OPSWAT サポート表には、使用するアンチウイルス/アンチスパイウェア/ファイアウォール アプリケーションの製品名とバージョン情報が含まれています。HostScan は v2 OPSWAT API をサポートし、ISE ポスチャ コンプライアンス モジュールは v3 OPSWAT API をサポートします。これら 2 つのバージョンの編成における最大の違いは、v2 ではベンダーによってライブラリ ファイルが編成されるのに対して、v3 では製品タイプでライブラリ ファイルが編成されることです。

ライブラリ（zip ファイル）内の個別の XML ファイルは、OPSWAT, Inc. によってデジタル署名され、ライブラリ自体はシスコの証明書によって署名されたコードである単一の自己解凍実行可能ファイルとしてパッケージ化されています。これらの表は、Microsoft Excel、Microsoft Excel ビューア、または OpenOffice を使用して表示できます。

ヘッドエンド（ISE または ASA）とエンドポイント間のバージョン番号に不一致がある場合は、OPSWAT コンプライアンス モジュールが更新またはダウングレードされます。これらのアップグレード/ダウングレードは必須であり、ヘッドエンドへの接続が確立されるとすぐにエンドユーザの介入なしで自動的に実行されます。

Host Scan では、OPSWAT バイナリはパッケージの一部に含まれており、標準インストーラの一部としてインストールされます。HostScan サポート表は、cisco.com のアンチウイルス/アンチスパイウェア/ファイアウォール アプリケーションのリスト [英語] からダウンロードできます。

AnyConnect ISE ポスチャでは、OPSWAT バイナリは別個のインストーラにパッケージ化されています。

OPSWAT v3 ライブラリのみを ISE にアップロードでき、ローカル ファイル システムから、または直接 ISE の [フィード URL の更新（Update Feed URL）] によって、ISE に手動でロードできます。

ASA ポスチャ モジュールの提供内容

HostScan

HostScan は、ユーザが ASA に接続した後、かつログインする前に、リモート デバイス上にインストールされるパッケージです。HostScan は、基本モジュール、Endpoint Assessment モジュール、および Advanced Endpoint Assessment モジュールで構成されています。

（注） AnyConnect リリース 3.x では、このパッケージは hostscan_version.pkg ファイルにバンドルされ、HostScan が機能するためには ASA の HostScan イメージ下で更新されて有効化される必要がありました。現在は、独立したインストールです。

基本的機能

HostScan は自動的に Cisco クライアントレス SSL VPN または AnyConnect VPN クライアント セッションを確立しているリモート デバイスのオペレーティング システムとサービス パックを識別します。

特定のプロセス、ファイル、およびレジストリ キーについて、エンドポイントを検査するように HostScan を設定することもできます。HostScan は、トンネルが完全に確立される前にこれらのすべての検査を実行し、この情報を ASA に送信して、会社所有、個人用、および公共のコンピュータを識別します。この情報は、評価にも使用できます。

（注） ログイン前の評価および証明書情報の返送は実行できません。HostScan は認証方式ではありません。HotScan は、接続しようとしているデバイスの内容を検証するチェックを実行するだけです。

また、HostScan は、設定した DAP エンドポイント条件と照合して評価するために、次の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、および Linux オペレーティング システム
- Microsoft サポート技術情報（KB）番号
- デバイス エンドポイント属性タイプ（ホスト名、MAC アドレス、BIOS シリアル番号、ポート番号（レガシー属性）、TCP/UDP ポート番号、プライバシー保護、およびエンドポイント アセスメント（OPSWAT）のバージョンなど）。

（注） HostScan は Windows クライアント システム上の Microsoft のソフトウェア アップデートに関するサービス リリース（GDR）の情報を収集します。サービス リリースには複数のホットフィックスが含まれます。サービス リリース エンドポイント属性は、ホット フィックスではなく、DAP ルールに使用されます。

エンドポイント アセスメント

エンドポイント アセスメントは、HostScan の拡張機能であり、多くの種類のアンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールについて、リモート コンピュータを検査します。ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して要件を満たすようにエンドポイント条件を組み合わせることができます。

詳細については、Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides の適切なバージョンのの「*Dynamic Access Policies*」の章を参照してください。

Advanced Endpoint Assessment：アンチウイルス、アンチスパイウェア、およびファイアウォールの修復

Windows、Mac OS X、およびLinuxのデスクトップでは、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

アンチウイルス：アンチウイルス ソフトウェアの次の部分を修復します。

- ファイル システム保護の強制：無効になっているアンチウイルス ソフトウェアを有効にします。
- ウイルス定義更新の強制：ウイルス定義がAdvanced Endpoint Assessmentの設定で定義された日数内に更新されていない場合、ウイルス定義の更新を開始します。

アンチスパイウェア：アンチスパイウェア定義がAdvanced Endpoint Assessmentの設定で定義された日数内に更新されていない場合、アンチスパイウェア定義の更新を開始します。

パーソナル ファイアウォール：Advanced Endpoint Assessment設定で定義されている要件を満たさないファイアウォール設定およびルールを再設定します。次の例を参考にしてください。

- ファイアウォールを有効または無効にします。
- アプリケーションの実行を防止または許可します。
- ポートをブロックまたは開きます。

（注） この機能は、すべてのパーソナル ファイアウォールでサポートされているわけではありません。

正常にVPN接続を確立した後にエンドユーザがアンチウイルスまたはパーソナルファイアウォールを無効にした場合、Advanced Endpoint Assessmentの機能は約60秒以内にそのアプリケーションを再び有効にしようとします。

HostScan 用のアンチウイルス アプリケーションの設定

ASA ポスチャ モジュールまたはHostScanをインストールする前に、アンチウイルス ソフトウェアを「ホワイトリスト」に設定するか、または、次の各アプリケーションについてセキュリティ例外を作成します。アンチウイルス アプリケーションは、これらのアプリケーションの動作を悪意があるものと誤って認識する場合があります。

- cscan.exe
- ciscod.exe
- cstub.exe

ダイナミック アクセス ポリシーとの統合

ASA では、HostScan の機能がダイナミック アクセス ポリシー（DAP）に統合されます。設定に応じて、ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされる HostScan の機能には、OS 検出、ポリシー、基本結果、およびエンドポイント アセスメントがあります。

セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

『*Cisco ASA Series VPN ASDM Configuration Guide*』の「*Configuring Dynamic Access Policies*」を参照してください。

DAP の BIOS シリアル番号

ASA ポスチャは、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用し、その BIOS シリアル番号に基づいて ASA への VPN 接続を許可または拒否できます。

DAP エンドポイント属性としての BIOS の指定

手順

ステップ 1 ASDM にログインします。

ステップ 2 [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク(クライアント)アクセス（Network (Client) Access）] または [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] を選択します。

ステップ 3 [ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（Edit）] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4 エンドポイント ID 表の右にある [追加（Add）] をクリックします。

ステップ 5 [エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6 [BIOS シリアル番号（BIOS Serial Number）] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS シリアル番号（BIOS Serial Number）] フィールドに BIOS

番号を入力します。[OK] をクリックし、[エンドポイント属性（Endpoint Attribute）] ダイアログボックスでの変更を保存します。

ステップ 7 [OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 8 [適用（Apply）] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 9 [保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

- Windows：http://support.microsoft.com/kb/558124
- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：このコマンドを使用してください。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

ASA で有効にされたホスト スキャン イメージの判別

ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（HostScan Image）] を選択します。

ISE ポスチャ プロファイル エディタ

管理者は、ポスチャ プロファイルを作成し、ISE にアップロードするために、このスタンドアロンエディタを使用することを選択できます。それ以外の場合、組み込みのポスチャ プロファイル エディタが ISE UI の [ポリシー要素（Policy Elements）] に設定されます。AnyConnect コンフィギュレーション エディタが ISE で起動すると、AnyConnect ソフトウェアおよび関連するモジュール、プロファイル、OPSWAT、およびカスタマイズを備えた AnyConnect 設定が作成されます。ASA の ISE ポスチャ用のスタンドアロン プロファイル エディタには、次のパラメータが含まれています。

- **エージェントの動作**
  - [署名チェックの有効化（Enable signature check）]：オンにすると、エージェントによって実行される前に実行可能ファイルの署名チェックが有効になります。
  - [ログ ファイル サイズ（Log file size）]：エージェント ログ ファイルの最大サイズ。有効な値は 5 ～ 200 MB です。
  - [修復タイマー（Remediation Timer）]：コンプライアンス非対応とタグ付けされるまでにユーザが修復に割くことができる時間。有効な値は 1 ～ 300 分です。

- [エージェント ログ トレースの有効化（Enable agent log trace）]：エージェントでのデバッグ ログを有効にします。
- [非 802.1X ワイヤレス ネットワークでの動作（Operate on non-802.1X wireless networks）]：オンにすると、エージェントは非 802.1X ワイヤレス ネットワークで動作できます。

• IP アドレスの変更

最適なユーザ エクスペリエンスのため、次の値を推奨値に設定してください。

- [VLAN 検出間隔（VLAN detection interval）]：クライアント IP アドレスを更新する前にエージェントが VLAN 変更の検出を試みる間隔。有効な範囲は 0 ～ 900 秒で、推奨値は 5 秒です。
- [ping または ARP（Ping or ARP）]：IP アドレスの変更を検出する方法。推奨設定は ARP です。
- [ping の最大タイムアウト（Maximum timeout for ping）]：1 ～ 10 秒の ping タイムアウト。
- [エージェント IP 更新の有効化（Enable agent IP refresh）]：VLAN 変更の検出を有効にする場合にオンにします。
- [DHCP 更新遅延（DHCP renew delay）]：IP 更新後にエージェントが待機する秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [DHCP リリース遅延（DHCP release delay）]：エージェントによる IP 更新を遅延させる秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [ネットワーク遷移遅延（Network transition delay）]：計画された IP 変更を待機できるようにエージェントがネットワーク モニタリングを一時停止する期間（秒単位）。推奨値は 5 秒です。

• ポスチャ プロトコル

- [ホストの検索（Discovery host）]：エージェントが接続できるサーバ。スタンドアロン プロファイル エディタでは、1 つのホストのみを入力します。
- [サーバ名ルール（Server name rules）]：エージェントが接続できるサーバを定義する、ワイルドカード対応のカンマで区切られた名前のリスト（.cisco.com など）。
- [PRA 再送信時間（PRA retransmission time）]：パッシブ再評価の通信障害が発生した場合に、このエージェントが再試行する間隔を指定します。有効な値の範囲は 60 ～ 3600 秒です。

[詳細（Advanced）] パネル

AnyConnect Secure Mobility Client UI の [詳細（Advanced）] パネルは、コンポーネントの統計情報、ユーザ プリファレンス、およびコンポーネント固有のその他の情報を表示するための各コンポーネントの領域です。AnyConnect システム トレイで、[すべてのコンポーネントの詳細ウィンドウ（Advanced Window for all components）] アイコンをクリックすると、新しい [システム スキャン（System Scan）] セクションに次のタブが含まれます。

（注） Mac OS X では、これらの統計情報、ユーザ プリファレンス、メッセージ履歴などは、[統計情報（Statistics）] ウィンドウの下に表示されます。プリファレンスは [プリファレンス（Preferences）] ウィンドウに表示され、Windows のようなタブ表示はされません。

- [プリファレンス（Preferences）]：信頼できないサーバへの接続をブロックできます。ダウンローダのプロセス中に、証明書が信頼できず検証されていない ISE サーバに対して、「信頼できないサーバをブロックしました（Untrusted Server Blocked）」というメッセージを受信します。ブロッキングを無効にすると、AnyConnect は悪意がある可能性があるネットワーク デバイスへの接続をブロックしなくなります。
- [統計情報（Statistics）]：現在の ISE ポスチャ ステータス（準拠または未準拠）、OPSWAT のバージョン情報、アクセプタブル ユース ポリシーのステータス、ポスチャの最新の実行タイム スタンプ、不足要件、およびトラブルシューティングの目的で表示するのに十分重要であると考えられるその他の統計情報を提供します。
- [セキュリティ製品（Security Products）]：システムにインストールされているアンチウイルスおよびアンチスパイウェア製品のリストにアクセスします。
- [スキャンの概要（Scan Summary）]：管理者がユーザに対して表示するように設定したポスチャ項目をユーザが確認できるようにします。たとえば、設定されている場合、ユーザはシステム上にポスチャされたすべての項目を表示したり、ポスチャ チェックに失敗して修復が必要な項目のみを表示したりすることができます。
- [メッセージ履歴（Message History）]：コンポーネントについて、システム トレイに送信されたすべてのステータス メッセージの履歴を表示します。この履歴は、トラブルシューティングに役立ちます。