クライアント ポスチャ ポリシーの設定

ポスチャは、Cisco Identity Services Engine（ISE）のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティ ポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。

ポスチャ サービス

ポスチャは、Cisco Identity Services Engine（Cisco ISE）のサービスです。ポスチャを使用すると、ネットワークに接続する前に、エンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックできます。AnyConnect ISE ポスチャ エージェントなどのポスチャ エージェントは、エンドポイントで実行されます。クライアント プロビジョニングは、エンドポイントが適切なポスチャ エージェントを受信できるようにします。

Cisco ISE の ISE ポスチャ エージェントでは、以前のユーザと完全に切断されていないため、ネイティブ サプリカントを使用する場合は Windows のユーザの簡易切り替え機能がサポートされません。新しいユーザが送信されると、古いユーザのプロセスとセッション ID がエージェントによってハングされるため、新しいポスチャ セッションが開始できません。Microsoft のセキュリティ ポリシーに従い、ユーザの簡易切り替え機能を無効にすることを推奨します。

（注） ISE では、セッション制御は複数のノードで行われます。

MnT ノードでは、セッションは次の場合に削除されます。

- アカウンティングの開始があるのにアカウンティングの停止（古いセッション）がない場合、セッションは 5 日以内に削除されます。
- アカウンティングの停止後にアカウンティングの開始がある場合、セッションは数時間以内に削除されます。
- アカウンティングの開始または停止がない場合、セッションは数時間以内に削除されます。

PSN ノードでは、セッションは次の場合に削除されます。

- アカウンティングの停止を受信した場合。
- セッション キャッシュが消去された場合、特に多くのセッションがある場合、または PSN をリロードした場合。

リダイレクトのないポスチャをマルチノード展開で使用し、セッションを適切に管理しないと、ポスチャ機能に影響する可能性があります。

ISE コミュニティ リソース

Configure ISE 2.1 and AnyConnect 4.3 Posture USB Check

How To Configure Posture with AnyConnect Compliance Module and ISE 2.0

関連トピック

ポスチャ サービスのコンポーネント （3 ページ）
ポスチャおよびクライアント プロビジョニング ポリシー ワークフロー （4 ページ）
ポスチャ サービス ライセンス （4 ページ）

ポスチャ サービスのコンポーネント

Cisco ISE ポスチャ サービスには、主にポスチャ管理サービスとポスチャ ランタイム サービスが含まれます。

ポスチャ管理サービス

Cisco ISE に APeX ライセンスをインストールしていない場合、ポスチャ管理サービス オプションは管理者ポータルから使用できません。

管理サービスは、ポスチャ サービス用に設定された要件および許可ポリシーに関連付けられた、ポスチャ固有のカスタム条件および修復アクションに対するバックエンドサポートを提供します。

ポスチャ ランタイム サービス

ポスチャ ランタイム サービスでは、ポスチャ評価およびクライアントの修復のためにクライアント エージェントと Cisco ISE サーバの間で実行されるすべての相互作用をカプセル化します。

ポスチャ ランタイム サービスは検出フェーズから開始します。エンドポイント セッションは、エンドポイントが 802.1x 認証に成功した後に作成されます。クライアント エージェントは、次の順序で各種の方式によって検出パケットを送信して Cisco ISE ノードへの接続を試行します。

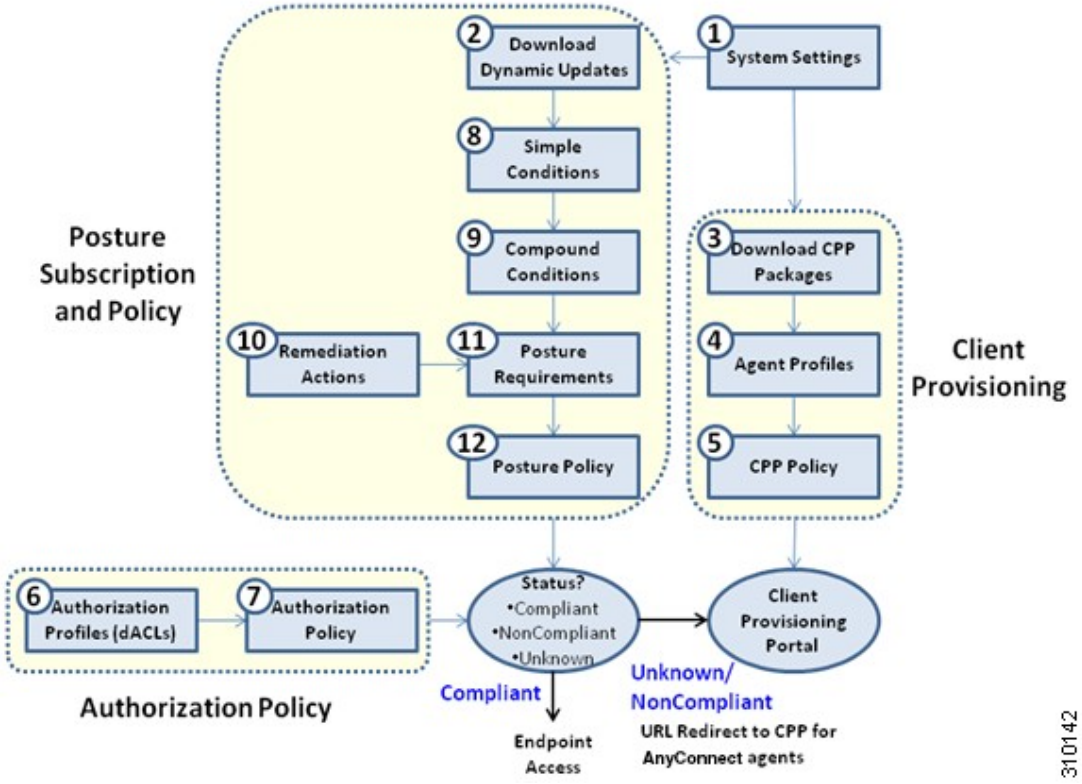
1. HTTP 経由で Cisco ISE サーバのポート 80 へ（設定されている場合）
2. HTTPS 経由で Cisco ISE サーバのポート 8905 へ（設定されている場合）
3. HTTP 経由でデフォルト ゲートウェイのポート 80 へ
4. HTTPS 経由でポート 8905 からそれぞれ前にアクセスしたサーバへ
5. HTTP 経由で enroll.cisco.com のポート 80 へ

ポスチャ フェーズは、利用規定（存在する場合）が受け入れられると開始されます。Cisco ISE ノードはクライアント エージェントにポスチャ ドメインのポスチャ トークンを発行します。ポスチャ トークンにより、エンドポイントではポスチャ プロセスを再度実行せずにネットワークに再接続できます。これには、エージェント GUID、利用規定のステータス、エンドポイントのオペレーティング システム情報などの情報が含まれています。

ポスチャ フェーズで使用されるメッセージは、NEA PB/PA 形式（RFC5792）です。

ポスチャおよびクライアントプロビジョニングポリシーワークフロー

図 *1 : Cisco ISE* のポスチャおよびクライアント プロビジョニング ポリシー ワークフロー



ポスチャ検出のステージ 1 では、すべてのディスカバリプローブが、ポスチャエージェントによって同時に実行されます。タイムアウト値は 5 秒です。ステージ 2 には 2 つのディスカバリプローブが含まれています。これにより、ポスチャモジュールは PSN への接続を確立できます。この PSN への接続は、リダイレクションがサポートされていない環境での認証をサポートしています。ステージ 2 では、すべてのプローブが連続しています。ステージ 2 に障害が発生した場合、ポスチャエージェントは再度ステージ 1 を試行します。このサイクルは 30 秒間継続します。その後、「ポリシーサーバが検出されません」と表示されます。この状態は、ディスカバリプローブがトリガーされるまで続きます。

ポスチャ サービス ライセンス

Cisco ISE は、Base ライセンス、Plus ライセンス、APeX ライセンスの 3 種類のライセンスを提供します。プライマリ PAN で APeX ライセンスをインストールしないと、ポスチャ要求は Cisco ISE で実行されません。Cisco ISE のポスチャ サービスは、1 つのノードまたは複数のノードで実行できます。

ポスチャ サービス展開

Cisco ISE は、スタンドアロン環境（単一ノード）または分散環境（複数ノード）に展開できます。

スタンドアロン Cisco ISE 展開では、単一のノードをすべての管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスに設定できます。

分散 Cisco ISE 展開では、各ノードを、管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスの Cisco ISE ノードとして設定できます。管理サービスを実行しているノードは、Cisco ISE 展開内のプライマリ ノードです。他のサービスを実行している他のノードは、互いのバックアップ サービス用に設定できるセカンダリ ノードです。

Cisco ISE でのポスチャ セッション サービスの有効化

始める前に

- クライアントから受信したすべてのポスチャ要求に対応するには、Cisco ISE でセッション サービスを有効にし、拡張ライセンス パッケージをインストールする必要があります。
- 分散展開に複数のノードを登録している場合は、登録したすべてのノードがプライマリ ノードとは別に [展開ノード（Deployment Nodes）] ページに表示されます。各ノードを Cisco ISE ノード（管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナ）として設定できます。
- ポスチャ サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、分散展開で管理ペルソナとモニタリング ペルソナを担当する Cisco ISE ノードでは実行されません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ウィンドウから Cisco ISE ノードを選択します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] チェックボックスをオンにします。

[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 ポリシーサービスペルソナでネットワーク アクセス、ポスチャ、ゲスト、およびクライアントプロビジョニングのセッション サービスを実行するには、[セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにします。セッション サービスを停止するには、このチェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

ポスチャ評価レポートの実行

ポスチャの詳細な評価を実行して、ポスチャ評価中に使用されるポスチャ ポリシーに対するクライアントのコンプライアンスの詳細なステータスを生成できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ポスチャの詳細な評価（Posture Detail Assessment）]** を選択します。

ステップ 2 [時間範囲（Time Range）] ドロップダウン リストから特定の期間を選択します。

ステップ 3 [実行（Run）] をクリックして、選択した期間中にアクティブだったすべてのエンド ポイントの概要を表示します。

ポスチャ管理の設定

ポスチャ サービス用の管理者ポータルをグローバルに設定できます。シスコから Web 経由で自動的に Cisco ISE サーバに更新をダウンロードできます。また、オフラインで、後で、Cisco ISE を手動で更新することもできます。さらに、クライアントに AnyConnect、NAC Agent、Web Agent などのエージェントがインストールされていると、クライアントにポスチャ評価および修復サービスが提供されます。クライアント エージェントは、Cisco ISE に対してクライアントのコンプライアンス ステータスを定期的に更新します。ログインおよびポスチャの要件評価が正常に完了した後、ネットワーク使用の利用規約への準拠をエンドユーザに求めるリンクが示されたダイアログがクライアント エージェントに表示されます。このリンクを使用して、エンドユーザがネットワークへのアクセス権を取得する前に同意する、企業ネットワークのネットワーク使用情報を定義できます。

関連トピック

クライアントのタイマー設定 （6 ページ）
非エージェント デバイスへのポスチャ ステータスの設定 （8 ページ）
ポスチャのリース （9 ページ）
ポスチャ評価の利用規定の設定 （12 ページ）

クライアントのタイマー設定

ユーザが修復するためのタイマー、あるステータスから別のステータスに移行するためのタイマー、およびログイン成功画面を制御するためのタイマーをセットアップできます。

エージェントプロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を制御するために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。[NACまたはAnyConnectポスチャプロファイル（NAC or AnyConnect Posture Profile）] ウィンドウ（**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [NACまたはAnyConnectポスチャ**

プロファイル（NAC or AnyConnect Posture Profile）]）で、クライアント プロビジョニング リソースのエージェントに対して、これらすべてのタイマーを設定できます。

しかし、クライアント プロビジョニング ポリシーに一致するように設定されたエージェント プロファイルがない場合、[全般設定（General Settings）] の設定ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**）の設定を使用できます。

関連トピック

指定した時間内で修復するためのクライアントの修復タイマーの設定 （7 ページ）
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 （7 ページ）
ログイン成功ウィンドウを自動的に閉じる設定 （8 ページ）

指定した時間内で修復するためのクライアントの修復タイマーの設定

指定した時間内にクライアントを修復するためのタイマーを設定できます。最初の評価時にクライアントが設定されたポスチャ ポリシーを満たすことに失敗した場合、エージェントは修復タイマーに設定された時間内にクライアントが修復するのを待ちます。クライアントがこの指定時間内の修復に失敗すると、クライアント エージェントはポスチャ ランタイム サービスにレポートを送信します。その後、クライアントは非準拠ステートに移行されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [修復タイマー（Remediation Timer）] フィールドに、分単位で時間の値を入力します。

デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。

ステップ 3 [保存（Save）] をクリックします。

クライアントの遷移のためのネットワーク遷移遅延タイマーの設定

ネットワーク遷移遅延タイマーを使用して、指定した時間内に、クライアントがある状態から別の状態に遷移するためのタイマーを設定できます。これは、許可変更（CoA）が完了するために必要となります。ポスチャの成功時と失敗時にクライアントが新しい VLAN の IP アドレスを取得するための時間がかかる場合は、より長い遅延時間が必要になることがあります。クライアントが正常にポスチャされると、Cisco ISE は、ネットワーク遷移遅延タイマーで指定された時間内に未知から準拠モードへ移行することを許可します。ポスチャに失敗すると、Cisco ISE は、タイマーで指定された時間内にクライアントが未知から非準拠モードへ移行することを許可します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [ネットワーク遷移遅延（Network Transition Delay）] フィールドに時間値を秒単位で入力します。

デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。

ステップ 3 [保存（Save）] をクリックします。

ログイン成功ウィンドウを自動的に閉じる設定

ポスチャ評価が正常に完了した後、クライアント エージェントは一時的なネットワーク アクセス画面を表示します。ユーザはログイン ウィンドウで [OK] ボタンをクリックして、この画面を閉じる必要があります。指定した時間の経過後にこのログイン画面を自動的に閉じるタイマーを設定できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスをオンにします。

ステップ 3 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスの横のフィールドに時間値を秒単位で入力します。

有効な値の範囲は 0 ～ 300 秒です。時間をゼロに設定すると、AnyConnect はログイン成功画面を表示しません。

ステップ 4 [保存（Save）] をクリックします。

非エージェント デバイスへのポスチャ ステータスの設定

Linux または iDevice などの非エージェント デバイスで実行されるエンドポイントのポスチャ ステータスを設定できます。Android デバイスおよび iPod、iPhone、iPad などの Apple の iDevice が Cisco ISE 対応ネットワークに接続する場合、これらのデバイスはデフォルト ポスチャ ステータスの設定を引き継ぎます。

これらの設定は、ポスチャのランタイム中に一致するポリシーが見つからない場合、Windows および Macintosh オペレーティング システムで実行されるエンドポイントにも適用されます。

始める前に

エンドポイントにポリシーを適用するには、対応するクライアント プロビジョニング ポリシー（エージェントのインストール パッケージ）を設定する必要があります。そうしないと、エンドポイントのポスチャ ステータスは自動的にデフォルト設定が反映されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [デフォルトポスチャステータス（Default Posture Status）] ドロップダウン リストから、オプションに [準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

ポスチャのリース

ユーザがネットワークにログインするたびにポスチャ評価を実行したり、指定した間隔でポスチャ評価を実行したりするよう Cisco ISE を設定できます。有効な範囲は 1 ～ 365 日です。

この設定は、ポスチャ評価にAnyConnectエージェントを使用するユーザだけに適用されます。

ポスチャ リースがアクティブな場合、Cisco ISE は最新の既知のポスチャを使用しますが、コンプライアンスの確認のためにエンドポイントに接続しません。ただし、ポスチャ リースが期限切れになると、Cisco ISE はエンドポイントの再認証またはポスチャ再評価を自動的にトリガーしません。同じセッションが使用されているため、エンドポイントは同じコンプライアンス状態のままになります。エンドポイントが再認証されると、ポスチャが実行され、ポスチャ リース時間がリセットされます。

使用例のシナリオ

- ユーザはエンドポイントにログオンし、1 日に設定されているポスチャ リースにポスチャ準拠させます。
- ユーザは4時間後にエンドポイントからログオフします（この時点で、ポスチャ リースは 20 時間残っています）。
- ユーザは 1 時間後に再度ログオンします。この時点で、ポスチャ リースは 19 時間残っています。最新の既知のポスチャ状態は準拠状態でした。したがって、エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- ユーザは 4 時間後にログオフします（この時点で、ポスチャ リースは 15 時間残っています）。
- ユーザは 14 時間後にログオンします。ポスチャ リースは 1 時間残っています。最新の既知のポスチャ状態は準拠状態でした。エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- 1 時間後、ポスチャ リースは期限切れになります。同じユーザ セッションが使用されているため、ユーザは引き続きネットワークに接続されています。
- 1 時間後、ユーザはログオフします（セッションはユーザに関連付けられていますが、マシンには関連付けられていないため、マシンはネットワーク上に留まることができます）。
- 1 時間後、ユーザはログオンします。ポスチャ リースが期限切れになり、新しいユーザ セッションが開始されるため、マシンはポスチャ アセスメントを実行し、その結果がCisco ISE に送信され、ポスチャ リース時間が 1 日にリセットされます（この使用例の場合）。

定期的再評価

定期的再評価（PRA）は、コンプライアンスについてすでに適切にポスチャされているクライアントにのみ実行できます。PRAは、クライアントがネットワーク上で準拠していない場合には実行されません。

PRAは、エンドポイントが準拠ステートになっている場合にのみ有効であり、適用可能です。ポリシーサービスノードは関連するポリシーを調べ、設定で定義されているクライアントロールに応じて要件をコンパイルし、PRA を適用します。PRA 設定の一致が見つかった場合、ポリシーサービスノードは、クライアントのPRA設定で定義されているPRA属性を使用して、クライアント エージェントに応答してから、CoA 要求を発行します。クライアント エージェントは、設定に指定された間隔に基づいて定期的に PRA 要求を送信します。PRA が成功した場合、または、PRA設定に指定されているアクションが続行になっている場合、クライアントは準拠ステートのままになります。クライアントが PRA を満たしていない場合、準拠ステートから非準拠ステートに移行します。

PostureStatus属性は、ポスチャ再評価要求の場合でも、PRA要求で現在のポスチャステータスを不明ではなく準拠と示します。PostureStatus はモニタリング レポートでも更新されます。

ポスチャのリースが有効期限内の場合、アクセス コントロール リスト（ACL）に基づいてエンドポイントが準拠し、PRA が開始されます。PRA が失敗すると、エンドポイントが非準拠になり、ポスチャのリースがリセットされます。

定期的再評価の設定

コンプライアンスに対してすでに正常にポスチャされているクライアントだけの定期的な再評価を設定できます。システムで定義されているユーザ ID グループに各 PRA を設定できます。

始める前に

- 各 PRA 設定に、一意のグループ、または設定に割り当てられているユーザ ID グループの一意の組み合わせがあることを確認します。
- 2 つの一意のロールである role_test_1 および role_test_2 を PRA 設定に割り当てることができます。論理演算子とこれら 2 つのロールを組み合わせ、2 つのロールの一意の組み合わせとして PRA 設定に割り当てることができます。たとえば、role_test_1 OR role_test_2 とします。
- 2 つの PRA 設定に共通のユーザ ID グループがないことを確認します。
- PRA設定がユーザIDグループ「Any」にすでに存在する場合、次のことを実行しないと、他の PRA 設定を作成できません。
  - *Any* 以外のユーザ ID グループを反映するように、任意のユーザ ID グループで既存の PRA 設定を更新します。
  - ユーザ ID グループ「*Any*」の既存の PRA 設定を削除します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 新しい PRA を作成するには、[新規再評価の設定（New Reassessment Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックして、PRA 設定を作成します。

関連トピック

定期的再評価 （10 ページ）

Cisco ISE へのポスチャ更新のダウンロード

ポスチャ更新には、Windows および Macintosh オペレーティング システムの両方のアンチウイルスとアンチスパイウェアの一連の事前定義済みのチェック、ルール、サポート表、およびシスコでサポートされるオペレーティング システム情報が含まれます。また、ローカル ファイル システムの更新の最新のアーカイブを含むファイルから Cisco ISE をオフラインで更新することもできます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。通常、このプロセスには約 20 分かかります。初回ダウンロード後に、差分更新が自動的にダウンロードされるように Cisco ISE を設定できます。

Cisco ISE では、初回ポスチャ更新時に 1 回のみ、デフォルトのポスチャ ポリシー、要件、および修復を作成します。それらを削除した場合、Cisco ISE は後続の手動またはスケジュールされた更新中にこれらを再作成しません。

始める前に

ポスチャ リソースを Cisco ISE にダウンロードできる適切なリモート ロケーションにアクセスできるようにするには、5-2 ページの「Cisco ISE でのプロキシ設定の指定」の説明に従ってネットワークにプロキシが正しく設定されていることを確認する必要がある場合があります。

[ポスチャ更新（Posture Update）]ページを使用して、Web から更新を動的にダウンロードできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [Web] オプションを選択して、更新を動的にダウンロードします。

ステップ 3 [デフォルトに設定（Set to Default）] をクリックして、[フィードURLの更新（Update Feed URL）] フィールドにシスコのデフォルト値を設定します。

ネットワークで URL リダイレクション機能（プロキシ サーバ経由など）を制限しているために、上記の URL へのアクセスに問題がある場合は、Cisco ISE で関連トピックの代替 URL を指定してください。

ステップ 4 [ポスチャ更新（Posture Updates）] ページの値を変更します。

ステップ 5 シスコからの更新をダウンロードするには、[今すぐ更新（Update Now）] をクリックします。

ステップ 6 Cisco ISE で他のタスクを続行するには [OK] をクリックします。

更新された後、[ポスチャ更新（Posture Updates）] ページに、[ポスチャ更新（Posture Updates）] ページの [更新情報（Update Information）] セクションの更新の確認として現在のシスコ更新のバージョン情報が表示されます。

関連トピック

ポスチャ更新の自動ダウンロード （12 ページ）

ポスチャ更新の自動ダウンロード

最初の更新後に、更新を確認し、自動的にダウンロードするようにCisco ISEを設定できます。

始める前に

- 最初にポスチャ更新をダウンロードして、更新を確認し、自動的にダウンロードするように Cisco ISE を設定しておく必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [ポスチャ更新（Posture Updates）] ページで [初期遅延から開始される更新の自動確認（Automatically check for updates starting from initial delay）] チェックボックスをオンにします。

ステップ 3 初期遅延時間を hh:mm:ss の形式で入力します。

Cisco ISE は、初期遅延時間の終了後に確認を開始します。

ステップ 4 時間間隔を時間単位で入力します。

Cisco ISE は初期遅延時間から指定した間隔で、展開に更新をダウンロードします。

ステップ 5 [はい（Yes）] をクリックして続行します。

ステップ 6 [保存（Save）] をクリックします。

ポスチャ評価の利用規定の設定

ログインし、クライアントのポスチャ評価が成功すると、クライアントエージェントにより一時的なネットワークアクセス画面が表示されます。この画面には、利用規定（AUP）へのリンクが含まれています。ユーザがリンクをクリックすると、ネットワーク利用条件を表示するページにリダイレクトされます。その条件を読み、同意する必要があります。

各利用規定設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。Cisco ISE は最初に一致したユーザ ID グループの AUP を見つけ、AUP を表示するクライアント エージェントと通信します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [新規利用規定設定（New Acceptable Use Policy Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの 1 つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして pc_ が付けられ、複合条件はプレフィクスとして pr_ が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザ定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

[ポスチャナビゲーション（Posture Navigation）] ペインを使用して、次の単純条件を管理できます。

- ファイル条件：ファイルの存在、ファイルの日付、およびクライアントのファイル バージョンを確認する条件。
- レジストリ条件：レジストリ キーの存在またはクライアントのレジストリ キーの値を確認する条件。
- アプリケーション条件：アプリケーションまたはプロセスがクライアント上で実行されているかまたは実行されていないかを確認する条件。

（注） プロセスがインストールされ実行されている場合、ユーザは準拠します。ただし、アプリケーション条件が逆ロジックで動作している場合は、アプリケーションがインストールされておらず実行されていなくも、エンドユーザは準拠します。アプリケーションがインストールされ実行されている場合、エンドユーザは準拠しません。

- サービス条件：サービスがクライアント上で実行されているかまたは実行されていないかを確認する条件。
- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マス ストレージ デバイスの有無をチェックする条件。

関連トピック

ファイル条件の設定
レジストリ条件の設定
アプリケーション条件の設定
サービス条件の設定
ディクショナリ単純条件の設定
USB 条件の設定

単純ポスチャ条件の作成

ポスチャ ポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 [ファイル（File）]、[レジストリ（Registry）]、[アプリケーション（Application）]、[サービス（Service）]、または [ディクショナリ単純条件（Dictionary Simple Condition）] のいずれかを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

複合ポスチャ条件

複合条件は、1つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1 つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます
- アンチウイルス複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます
- アンチスパイウェア複合条件：1 つ以上の AS 条件、または AS 複合条件が含まれます
- ディクショナリ複合条件：1 つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます
- マルウェア対策条件：1 つ以上の AM 条件が含まれます

Windowsクライアントでの自動アップデートを有効にするための事前定義の条件

pr_AutoUpdateCheck_Ruleはシスコによって事前定義された条件であり、[複合条件（Compound Conditions）]ページにダウンロードされます。この条件を使用すると、Windowsクライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windowsクライアントがこの要件を満たさない場合、ネットワークアクセスコントロール（NAC）エージェントによって、Windowsクライアントの自動アップデート機能が強制的に有効になります（修復）。この修復後、Windowsクライアントはポスチャ準拠になります。自動アップデート機能が Windows クライアント上で有効になっていない場合は、ポスチャ ポリシーで関連付けた Windows Update 修復で Windows 管理者設定を上書きします。

事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISE の [AV 複合条件（AV Compound Condition）] および [AS 複合条件（AS Compound Condition）] ページには、アンチウイルスとアンチスパイウェアの事前設定済みの複合条件がロードされます。これらの条件は、WindowsおよびMacintoshオペレーティング システムのアンチウイルスおよびアンチスパイウェア サポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するかどうかを確認できます。Cisco ISE で新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISE は、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェア サポート表を使用します。ユーザは頻繁にアンチウイルスとアンチスパイウェア サポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェア サポート表が更新されるたびに、NAC Agent は新しいアンチウイルスとアンチスパイウェア ライブラリを受け取ります。これは、NAC Agent がより新しい追加機能をサポートするのに役立ちます。NAC Agent がこのサポート情報を取得すると、定期的に更新される se-checks.xml ファイル（se-templates.tar.gz アーカイブで se-rules.xml ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャ ポリシーに準拠しているかどうかを決定します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスとアンチスパイウェア ライブラリによってサポートされている機能に応じて、適切な要件が NAC Agent に送信され、ポスチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

アンチウイルスとアンチスパイウェア サポート表は、Cisco.com で参照できます。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポスチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

ベンダーは頻繁に製品バージョンや定義ファイルの日付を更新するので、頻繁にアップデートのコンプライアンス モジュールをポーリングすることで、各ベンダーの製品の最新バージョンおよび定義ファイルの日付を調べる必要があります。新しいベンダー、製品、およびリリースのサポートを反映してコンプライアンス モジュールが更新されるたびに、AnyConnect のエージェントは新しいライブラリを受信します。これは、AnyConnect のエージェントがより新しい追加機能をサポートするのに役立ちます。AnyConnect のエージェントがこのサポート情報を取得すると、定期的に更新される se-checks.xml ファイル（se-templates.tar.gz アーカイブで se-rules.xml ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャ ポリシーに準拠しているかどうかを決定します。特定のアンチウイルス、アンチスパイウェア、マルウェア対策、ディスク暗号化またはパッチ管理製品のライブラリによってサポートされている機能に応じて、適切な要件が AnyConnect エージェントに送信され、ポスチャ検証中にクライアント上でそれらの存在、およびクライアントでの特定の製品のステータスが検証されます。

コンプライアンス モジュールは、Cisco.com で入手可能です。

次の表に、ISE ポスチャ ポリシーをサポートするまたはしない OPSWAT API バージョンを示します。バージョン 3 および 4 をサポートするエージェントごとに異なるポリシー ルールがあります。

表 *1 : OPSWAT API* バージョン

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降
USB	4.x 以降
非 OPSWAT	
ファイル（File）	すべてのバージョン
Application	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン

（注）

- 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。
- OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。
- バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [複合条件（Compound Conditions）] > [追加（Add）]** を選択します。

ステップ 2 フィールドに適切な値を入力します。

ステップ 3 条件を検証するために [式の確認（Validate Expression）] をクリックします。

ステップ 4 [送信（Submit）] をクリックします。

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager（SCCM）、クライアント バージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。

（注） Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。

- Cisco ISE バージョン 1.4 以降
- AnyConnect バージョン 4.1 以降

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [パッチ管理条件（Patch Management Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] フィールドに条件名を入力し、[説明（Description）] フィールドにその説明を入力します。

ステップ 4 [オペレーティングシステム（Operating System）] ドロップダウン フィールドから、適切なオペレーティング システムを選択します。

ステップ 5 ドロップダウン リストから [コンプライアンスモジュール（Compliance Module）] を選択します。

ステップ 6 ドロップダウン リストから [ベンダー名（Vendor Name）] を選択します。

ステップ 7 [チェックタイプ（Check Type）] を選択します。

ステップ 8 [インストール済みパッチの確認（Check Patches Installed）] ドロップダウン リストから適切なパッチを選択します。

ステップ 9 [送信（Submit）] をクリックします。

関連トピック

パッチ管理条件の設定

パッチ管理修復の追加 （30 ページ）

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンド ポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンド ポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。AnyConnect ISE ポスチャ エージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ディスク暗号化条件（Disk Encryption Condition）] ページで、フィールドに適切な値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ ポリシーの設定

ポスチャ ポリシーは 1 つ以上の ID グループおよびオペレーティング システムに関連付けられたポスチャ要件の集合です。ディクショナリ属性は、デバイスの異なるポリシーを定義する、ID グループおよびオペレーティング システムと組み合わされたオプションの条件です。

Cisco ISE には、適合しないデバイスの猶予時間を設定するオプションが用意されています。デバイスが適合していないことが判明した場合、Cisco ISE はポスチャ評価結果キャッシュ内で以前の正常な状態を検索し、デバイスに猶予時間を与えます。デバイスには、猶予期間中にネットワークへのアクセス権が付与されます。分、時、または日単位（最大 30 日）で猶予期間を設定できます。

詳細については、Cisco ISE 構成ガイドの「ポスチャ サービス」を参照してください。

（注）

- 猶予期間が延長または短縮されると、デバイスがポスチャ フローを再び通過した場合（たとえば、[遅延通知（Delayed Notification）] オプションが有効で、[再スキャン（Re-Scan）] オプションが選択されている場合、デバイスとネットワークの切断や再接続が行われます）、新しい猶予期間および遅延通知が適用されます。
- 猶予期間は Temporal Agent には適用されません。
- （それぞれ異なる猶予期間を設定した）複数のポスチャ ポリシーにデバイスが一致する場合、それらの異なるポリシーで設定された最大の猶予期間がデバイスに与えられます。
- デバイスが猶予期間になると、アクセプタブル ユース ポリシー（AUP）は表示されません。

始める前に

- AUP について理解している必要があります。
- 定期的再評価（PRA）について理解している必要があります。
- AnyConnect エージェント 4.7 以降を使用して、コンプライアンス関連の通知を表示する必要があります。AnyConnect エージェントの設定に関する詳細については、AnyConnect 設定の作成を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポスチャ（Posture）]** または **[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ ポリシー（Posture Policy）]** を選択します。

ステップ 2 ドロップダウンの矢印を使用して新しいポリシーを追加します。

ステップ 3 [ルールステータス（Rule Status）] ドロップダウン リストで [有効（Enabled）] または [無効（Disabled）] を選択します。

ステップ 4 [ポリシーオプション（Policy Options）] でドロップダウンを選択し、[猶予期間の設定（Grace Period Settings）] を分単位、時間単位、日単位で指定します。

有効な値は次のとおりです。

- 1 ～ 30 日
- 1 ～ 720 時間
- 1 ～ 43200 分

デフォルトでは、この設定は無効です。

（注） ポスチャ評価の結果が適合しない場合でも、デバイスが以前に準拠しており、キャッシュの期限がまだ切れていなければ、[猶予期間の設定（Grace Period Settings）] で指定された時間にわたり、デバイスにアクセス権が付与されます。

ステップ 5 （オプション）[遅延通知（Delayed Notification）] という名前のスライダをドラッグし、猶予期間の特定の割合が過ぎるまで、猶予期間プロンプトがユーザに遅れて表示されるようにします。たとえば、通知遅延期間が 50 % に設定され、設定されている猶予期間が 10 分の場合、Cisco ISE は 5 分後にポスチャステータスをチェックし、エンドポイントが準拠していないと判断した場合は猶予期間通知を表示します。エンドポイントのステータスが準拠している場合、猶予期間通知は表示されません。通知遅延期間が 0 % に設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。ただし、エンドポイントは、猶予期間の有効期限が切れるまで、アクセス権が付与されます。このフィールドのデフォルト値は 0% です。有効な範囲は 0 ～ 95% です。

ステップ 6 [ルール名（Rule Name）] フィールドに、ポリシーの名前を入力します。

（注） 予期しない結果を回避するためのベストプラクティスは、各要件でポスチャ ポリシーを個別のルールとして設定することです。

ステップ 7 [IDグループ（Identity Groups）] 列から任意の ID グループを選択します。

ユーザまたはエンドポイントの ID グループに基づいて、ポスチャ ポリシーを作成することができます。

ステップ 8 [オペレーティングシステム（Operating Systems）] 列からオペレーティング システムを選択します。

ステップ 9 [準拠モジュール（Compliance Module）] 列から必要な準拠モジュールを選択します。

- 4.x 以降（4.x or Later）：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。
- 3.x 以前（3.x or Earlier）：ウイルス対策、スパイウェア対策、ディスク暗号化、および Patch Management の各種条件をサポートします
- すべてのバージョン（Any Version）：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。

ステップ 10 [ポスチャタイプ（Posture Type）] 列から、[ポスチャタイプ（Posture Type）] を選択します。

- [AnyConnect]：AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポリシーを監視し、適用します。
- [AnyConnect ステルス（AnyConnect Stealth）]：AnyConnect エージェントを展開し、クライアントとやりとりしない Cisco ISE ポスチャ ポリシーを監視し、適用します。
- [Temporal Agent]：準拠のステータスを確認するためにクライアント上で実行される一時実行可能ファイル。

ステップ 11 [その他の条件（Other Conditions）] では、1 つ以上のディクショナリ属性を追加し、単純条件または複合条件としてディクショナリに保存できます。

（注） [ポスチャポリシー（Posture Policy）] ウィンドウで作成したディクショナリ単純条件とディクショナリ複合条件は、許可ポリシーを設定するときには表示されません。

ステップ 12 [要件（Requirements）] フィールドに要件を指定します。

ステップ 13 [保存（Save）] をクリックします。

関連トピック

クライアントのポスチャ要件の作成 （35 ページ）
定期的再評価の設定 （10 ページ）

証明書ベースの条件のための前提条件

クライアント プロビジョニングおよびポスチャ ポリシーのルールに、証明書の属性に基づく条件を含めることができます。クライアント プロビジョニングまたはポスチャ ポリシーにおける証明書ベースの条件では、同じ証明書属性に基づいて一致する許可ポリシー ルールが存在することが前提条件になります。

たとえば、図に示されているように同じ属性を使用する必要があります。[発行者 - 共通名（Issuer – Common Name）] 属性が、クライアント プロビジョニングまたはポスチャと許可ポリシーの両方で使用されています。

図 *2 : Cisco* のプロビジョニング ポリシー

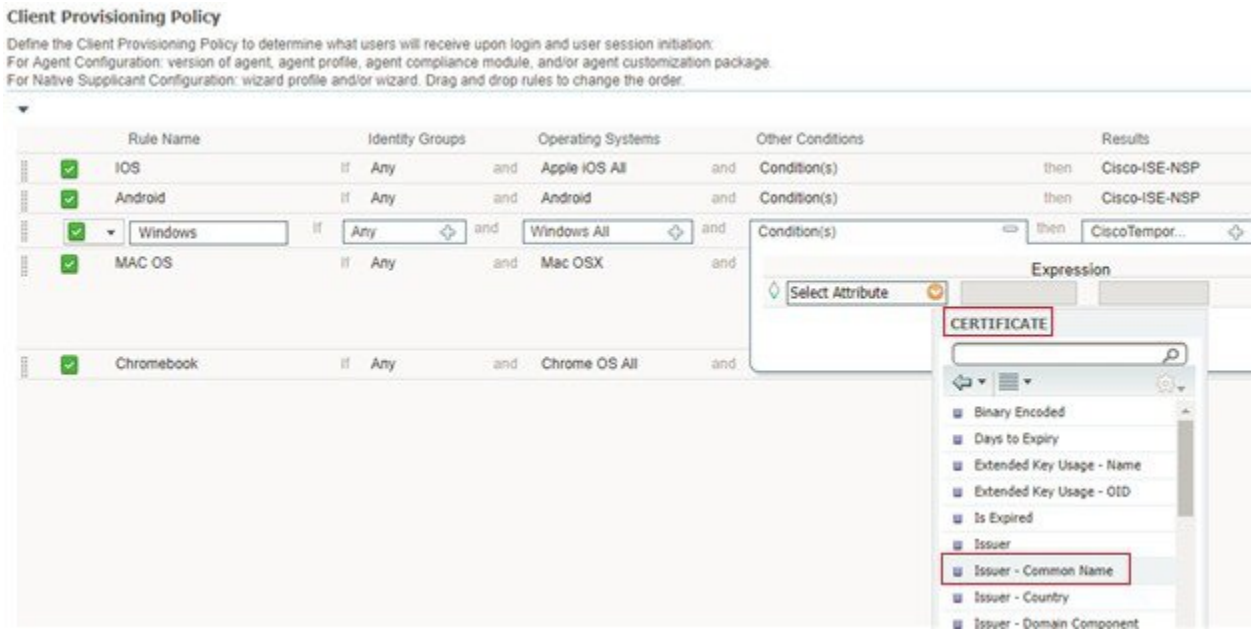
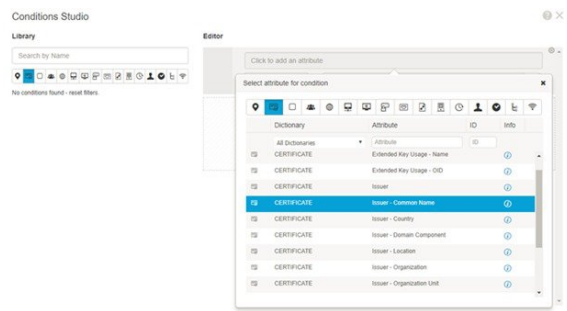


図 *3 : [*条件スタジオ（*Conditions Studio*）*]*



（注） ISE サーバ証明書は、AnyConnect 4.6 MR2 以降のシステム証明書ストアで信頼できる必要があります。昇格権限を必要とするポスチャ チェックおよび修復は、サーバが信頼されていない場合は機能しません。

- Windows OS：サーバ証明書をシステム証明書ストアに追加する必要があります。
- MACOS：サーバ証明書をシステム キーチェーンに追加する必要があります。コマンドライン ユーティリティを使用して証明書を信頼することをお勧めします。キーチェーン アクセス アプリケーションを使用してシステム キーチェーンに証明書を追加しても、ログイン キーチェーンにすでに存在する場合は機能しないことがあります。

デフォルトのポスチャ ポリシー

Cisco ISE ソフトウェアには、ポスチャ ポリシーおよびプロファイルの作成を容易にする、事前設定されたポスチャ ポリシー（[ポリシー（Policy）]>[ポスチャ（Posture）]）が多数用意されています。これらのポリシーは、デフォルトで無効になっています。要件に基づいて、これらのポリシーを有効にできます。以下は、デフォルトのポスチャ ポリシーの一部です。

ルール名（**Rule Name**）	説明	要件
Default_Antimalware_Policy_Mac	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation
Default_Antimalware_Policy_Win	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Mac

ルール名（**Rule Name**）	説明	要件
Default_AppVis_Policy_Win	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	エンドポイント デバイスに USB ストレージ デバイスが接続されていないことを確認します。	USB_Block

ポスチャ評価オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされるポスチャ評価（ポスチャ条件）オプションのリストを示します。

表 *2:* ポスチャ評価オプション

Windows 用 ISE ポスチャ エージェント	**Windows 用 Cisco Temporal エージェント**	**Macintosh OS X 用 ISE ポスチャ エージェント**	**Macintosh OS X 用 Cisco Temporal エージェント**
オペレーティング システム/サービス パック/ホットフィックス	—	—	—
サービス チェック	サービス チェック（Temporal エージェント 4.5 および ISE 2.3）	サービス チェック（AC 4.1 および ISE 1.4）	デーモンチェックはサポートされていません

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャエージェント	Macintosh OS X 用 Cisco Temporal エージェント
レジストリ チェック	レジストリ チェック（Temporal エージェント 4.5 および ISE 2.3）	—	—
ファイル チェック	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）	ファイル チェック（AC 4.1 および ISE 1.4）	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）
アプリケーション チェック	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）	アプリケーション チェック（AC 4.1 および ISE 1.4）	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）
アンチウイルスのインストール	マルウェア対策のインストール	アンチウイルスのインストール	マルウェア対策のインストール
アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
パッチ管理チェック（AC 4.1 および ISE 1.4）	パッチ管理のインストールのみチェック	パッチ管理チェック（AC 4.1 および ISE 1.4）	—

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャ エージェント	Macintosh OS X 用 Cisco Temporal エージェント
実行中の Windows Update	—	—	—
Windows Update の設定	—	—	—
WSUS のコンプライアンス設定	—	—	—

ポスチャ修復オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされる修復オプション（ポスチャ条件）のリストを示します。

表 *3:* ポスチャ修復オプション

ISE ポスチャ エージェント Windows	ISE ポスチャ エージェント Macintosh OS X
メッセージ テキスト（ローカル チェック）	メッセージ テキスト（ローカル チェック）
URL リンク（リンク分散）	URL リンク（リンク分散）
ファイル配布	—
プログラム起動	—
アンチウイルス定義更新	アンチウイルス ライブ更新
アンチスパイウェア定義更新	アンチスパイウェア ライブ更新
パッチ管理修復（AC 4.1 および ISE 1.4）	—
Windows Update	—
WSUS	—

ISE Community Resource

Cisco ISE and SCCM integration Reference Guide

ポスチャのカスタム条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

最初のポスチャ更新の後に、Cisco ISE もシスコ定義の単純条件と複合条件を作成します。シスコ定義の単純条件では pc_ as が使用され、複合条件では pr_ as が使用されます。

ユーザ定義の条件またはシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

ポスチャ サービスは、アンチウイルスおよびアンチスパイウェア（AV/AS）複合条件に基づいた内部チェックを使用します。このため、ポスチャ レポートは、作成した正確な AV/AS 複合条件名を反映しません。レポートには、AV/AS 複合条件の内部チェックの名前だけが表示されます。

たとえば、任意のベンダーおよび製品をチェックする「MyCondition_AV_Check」という名前の AV 複合条件を作成した場合、ポスチャ レポートには、条件名として、「MyCondition_AV_Check」ではなく、内部チェック「av_def_ANY」が表示されます。

ポスチャ エンドポイントのカスタム属性

ポスチャ エンドポイントのカスタム属性を使用して、クライアント プロビジョニングおよびポスチャ ポリシーを作成できます。最大100個のエンドポイントのカスタム属性を作成できます。以下のタイプのエンドポイントカスタム属性がサポートされています：Int、String、Long、Boolean、Float、IP、および Date。

エンドポイントカスタム属性は、特定の属性に基づいてデバイスをホワイトリスト登録またはブラックリスト登録するために使用することも、ポスチャまたはクライアントプロビジョニング ポリシーに基づいて特定の権限を割り当てるために使用することもできます。

エンドポイント カスタム属性を使用したポスチャ ポリシーの作成

エンドポイント カスタム属性を使用してポスチャ 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 エンドポイント カスタム属性を作成します。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域に、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）を入力します。

c) [保存（Save）] をクリックします。

ステップ 2 カスタム属性に値を割り当てます。

a) [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の順に選択します。

b) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要なMACアドレスをクリックし、[エンドポイント（Endpoints）]ページで[編集（Edit）] をクリックします。

c) 作成したカスタム属性が、[エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attributes）] 領域に表示されていることを確認します。

d) [編集（Edit）] をクリックし、必要な属性値を入力します（たとえば、deviceType = Apple-iPhone）。

e) [保存（Save）] をクリックします。

ステップ 3 カスタム属性と値を使用してポスチャ ポリシーを作成します。

a) [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ ポリシー（Posture Policy）] を選択します。

b) 必要なポリシーを作成します。[その他の条件（Other Conditions）] をクリックしてカスタム属性を選択し、必要なディクショナリを選択します（たとえば、ステップ 1 で作成したカスタム属性である [エンドポイント（Endpoints）] > [deviceType] を選択します）。詳細については、Cisco Temporal Agent のワークフロー （44 ページ） を参照してください。

c) [保存（Save）] をクリックします。

エンドポイント カスタム属性を使用してクライアント プロビジョニング ポリシーを作成するには、次の手順を実行します。

1. [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [クライアント プロビジョニング（Client Provisioning）] > [クライアント プロビジョニング ポリシー（Client Provisioning Policy）] を選択します。
2. 必要なポリシーを作成します。
   - 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - [その他の条件（Other Conditions）] をクリックして必要なディクショナリを選択して、カスタム属性を選択します。

カスタム ポスチャ修復アクション

カスタム ポスチャ修復アクションは、ファイル、リンク、アンチウイルスまたはアンチスパイウェア定義の更新、プログラムの起動、Windows Update、Windows Server Update Services（WSUS）の修復タイプです。

関連トピック

ファイル修復の追加 （29 ページ）
リンク修復の追加 （30 ページ）
アンチウイルス修復の追加 （31 ページ）
アンチスパイウェア修復の追加 （31 ページ）
プログラム修復起動の追加 （31 ページ）
Windows Update 修復の追加 （32 ページ）
Windows Server Update Services 修復の追加 （33 ページ）
パッチ管理修復の追加 （30 ページ）

ファイル修復の追加

ファイル修復により、クライアントはコンプライアンスに必要なファイルのバージョンをダウンロードできます。クライアントエージェントは、コンプライアンスのためにクライアントが必要とするファイルを使用してエンドポイントを修復します。

[ファイル修復（File Remediations）]ページでファイル修復をフィルタリング、表示、追加、または削除することはできますが、ファイル修復を編集することはできません。[ファイル修復（File Remediations）]ページには、すべてのファイル修復がそれらの名前と説明、および修復に必要なファイルとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [ファイル修復（File Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [名前（Name）] フィールドに名前を入力し、[説明（Description）] フィールドにファイル修復の説明を入力します。

ステップ 6 [新規ファイル修復（New File Remediation）] ページで値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

リンク修復の追加

リンク修復により、クライアントは修復ページまたはリソースにアクセスするための URL をクリックできます。クライアントエージェントはリンクを使用してブラウザを開き、クライアントはコンプライアンスのために自身を修復できます。

[リンク修復（Link Remediation）]ページには、すべてのリンク修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [リンク修復（Link Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規リンク修復（New Link Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

パッチ管理修復の追加

パッチ管理修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[パッチ管理修復（Patch Management Remediation）]ページには、修復タイプ、パッチ管理ベンダーの名前、およびさまざまな修復オプションが表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [パッチ管理修復（Patch Management Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [パッチ管理修復（Patch Management Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックして、[パッチ管理修復（Patch Management Remediation）] ページに修復アクションを追加します。

関連トピック

パッチ管理修復

アンチウイルス修復の追加

アンチウイルス修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AV 修復（AV Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AV 修復（AV Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AV 修復（New AV Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

アンチスパイウェア修復の追加

アンチスパイウェア修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AS 修復（AS Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AS 修復（AS Remediations）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AS 修復（New AS Remediations）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

関連トピック

アンチスパイウェア修復

プログラム修復起動の追加

コンプライアンスのために、クライアントエージェントが 1 つ以上のアプリケーションを起動してクライアントを修復するプログラム修復起動を作成できます。

[プログラム修復起動（Launch Program Remediations）] ページには、すべてのプログラム修復起動がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [プログラム起動修復（Launch Program Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規プログラム修復起動（New Launch Program Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

プログラム修復起動のトラブルシューティング

問題

プログラム修復起動を使用して、アプリケーションを修復として起動すると、アプリケーションは正常に開始されます（Windows Task Manager で観察されます）が、アプリケーション UI は表示されません。

ソリューション

プログラム起動 UI アプリケーションはシステム権限で実行され、[インタラクティブサービス検出（ISD）（Interactive Service Detection (ISD)）] ウィンドウに表示されます。プログラム起動 UI アプリケーションを表示するには、次の OS で ISD をイネーブルにする必要があります。

- Windows Vista：ISD はデフォルトで停止状態になっています。services.msc で ISD サービスを起動して、ISD をイネーブルにします。
- Windows 7：ISD サービスはデフォルトでイネーブルになっています。
- Windows 8/8.1：レジストリ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows で「NoInteractiveServices」を 1 から 0 に変更することで ISD をイネーブルにします。

Windows Update 修復の追加

[Windows Update 修復（Windows update remediations）] ページには、すべての Windows Update 修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > > **[ポスチャ（Posture）]** を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [Windows Update 修復（Windows Update Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 Windows Update 修復（New Windows Update Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

Windows Server Update Services 修復の追加

コンプライアンスのためにローカルに管理されているか、または Microsoft で管理されている WSUS サーバから最新の WSUS 更新を受信するように Windows クライアントを設定できます。Windows Server Update Services（WSUS）修復は、ローカルに管理されている WSUS サーバまたは Microsoft で管理されている WSUS サーバから最新の Windows サービス パック、ホットフィックス、およびパッチをインストールします。

クライアント エージェントをローカルの WSUS Agent と統合して、エンドポイントの WSUS 更新が最新かどうかをチェックする WSUS 修復を作成できます。

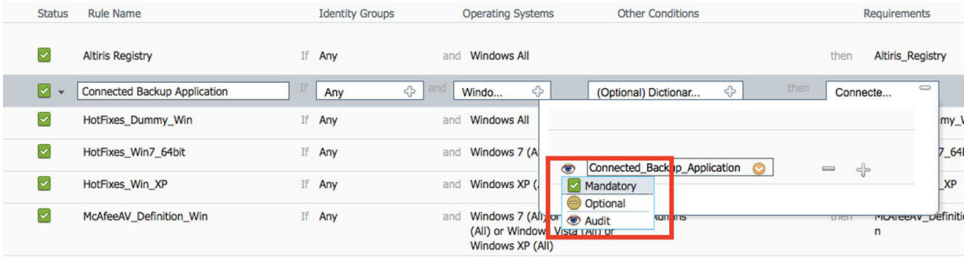
ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。
ステップ 3 [Windows Server Update Service 修復（Windows Server Update Services Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 Windows Server Update Service 修復（New Windows Server Update Services Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

ポスチャ評価要件

ポスチャ要件は、ロールおよびオペレーティング システムとリンクできる修復アクションを伴う一連の複合条件です。ネットワークに接続しているすべてのクライアントは、ネットワークで適合ホストになるためにはポスチャ評価中に必須要件を満たす必要があります。

ポスチャ ポリシー要件は、ポスチャ ポリシーの必須、オプション、または監査タイプに設定できます。要件がオプションで、クライアントがこれらの要件を満たさない場合、クライアントにはエンドポイントのポスチャ評価中に続行するオプションがあります。

図 *4:* ポスチャ ポリシーの要件タイプ



必須要件

ポリシーの評価時に、エージェントはポスチャ ポリシーに定義されている必須要件を満たすことができないクライアントに修復オプションを提供します。エンドユーザは、修復タイマー設定で指定された時間内に要件を満たすように修復する必要があります。

たとえば、絶対パス内に C:\temp\text.file があるかをチェックするために、ユーザ定義の条件を含む必須要件を指定したとします。ファイルがない場合、必須要件は失敗し、ユーザは [非準拠（Non-Compliant）] 状態になります。

オプション要件

ポリシーの評価時に、クライアントがポスチャ ポリシーに指定されたオプション要件を満たすことができない場合に、エージェントは続行するためのオプションをクライアントに提供します。エンドユーザは、指定されたオプション要件をスキップすることができます。

たとえば、Calc.exe などのクライアント マシンで実行するアプリケーションをチェックするために、ユーザ定義の条件を含むオプション要件を指定したとします。クライアントが条件を満たすことができない場合、オプション要件がスキップされ、エンドユーザが [準拠（Compliant）] 状態になるように、さらに続行するためのオプションがエージェントによって促されます。

監査要件

監査要件は内部用に指定され、エージェントはポリシー評価時の合格または失敗のステータスに関係なく、メッセージやエンドユーザからの入力を促しません。

たとえば、エンドユーザにアンチウイルス プログラムの最新バージョンがあるかどうかを確認するために、必須のポリシー条件を作成中だとします。ポリシー条件として実際に適用する前に非準拠のエンドユーザを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシー評価の間に、エージェントが可視性要件のコンプライアンス データを 5 ～ 10 分ごとにレポートします。

非準拠ステートでスタックしたクライアント システム

クライアント マシンが必須要件を修復できない場合、ポスチャ ステータスは「非準拠」に変更され、エージェント セッションは隔離されます。クライアント マシンを「非準拠」状態から移行するには、エージェントがクライアントマシン上でポスチャ評価を再び開始するようにポスチャ セッションを再起動する必要があります。次のようにポスチャ セッションを再起動できます。

- 802.1X 環境での有線およびワイヤレス許可変更（CoA）：
  - [新しい許可プロファイル（New Authorization Profiles）] ページで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。詳細については、20-11 ページの「ダウンロード可能 ACL の権限の設定」の項を参照してください。
  - 有線ユーザは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザは、ワイヤレス LAN コントローラ（WLC）から切断し、ユーザのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。
- VPN 環境：VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件（Requirements）] ページでは、ユーザ定義の条件とシスコ定義の条件、および修復アクションを関連付けて要件を作成できます。[要件（Requirements）] ページで作成および保存されたユーザ定義の条件および修復アクションは、それぞれのリスト ページに表示されます。

始める前に

- ポスチャの利用規定（AUP）について理解している必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択します。

ステップ 2 [要件（Requirements）] ページに値を入力します。

ステップ 3 読み取り専用モードでポスチャ要件を保存するには、[完了（Done）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

非準拠ステートでスタックしたクライアント システム （35 ページ）
ポスチャ評価要件 （33 ページ）

ポスチャのカスタム権限

カスタム権限は、Cisco ISE で定義する標準許可プロファイルです。標準許可プロファイルは、エンドポイントの一致するコンプライアンス ステータスに基づいてアクセス権を設定します。ポスチャ サービスでは、ポスチャは大きく不明プロファイル、準拠プロファイル、および非準拠プロファイルに分類されます。ポスチャ ポリシーおよびポスチャ要件によって、エンドポイントのコンプライアンス ステータスが決まります。

VLAN、DACL および他の属性値ペアの異なるセットを持つことができるエンドポイントの不明、準拠、および非準拠のポスチャ ステータスに対して 3 つの異なる許可プロファイルを作成する必要があります。これらのプロファイルは、3 つの異なる許可ポリシーに関連付けることができます。これらの許可ポリシーを区別するために、Session:PostureStatus 属性を他の条件とともに使用できます。

不明プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されていない場合、そのエンドポイントのポスチャ コンプライアンス ステータスは不明に設定されることがあります。不明のポスチャ コンプライアンス ステータスは、一致するポスチャ ポリシーが有効であるが、エンドポイントに対してポスチャ評価がまだ行われておらず、従ってクライアント エージェントによってコンプライアンス レポートが提供されていないエンドポイントにも適用できます。

準拠プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されている場合、そのエンドポイントのポスチャ コンプライアンス ステータスは準拠に設定されます。ポスチャ評価が行われると、エンドポイントは、一致するポスチャ ポリシー内に定義されているすべての必須要件を満たします。準拠とポスチャされているエンドポイントには、ネットワークに対する特権ネットワーク アクセスを付与できます。

非準拠プロファイル

エンドポイントのポスチャ コンプライアンス ステータスが非準拠に設定されるのは、そのエンドポイントに対して一致するポスチャ ポリシーが定義されているが、ポスチャ評価の実行中にすべての必須要件を満たすことができない場合です。非準拠としてポスチャされたエンドポイントは、修復アクションを含むポスチャ要件に一致し、自らを修復するために修復リソースへ制限付きのネットワーク アクセスが付与される必要があります。

標準許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページでは、標準許可ポリシーと例外許可ポリシーの 2 種類の許可ポリシーを定義できます。ポスチャに固有の標準許可ポリシーは、エンドポイントのコンプライアンス ステータスに基づいて、ポリシー決定を行うために使用されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [ビュー（View）] 列で、対応するデフォルトポリシーに隣接する矢印アイコンをクリックします。

ステップ 3 [アクション（Actions）] 列で、歯車アイコンをクリックし、ドロップダウン リストから新しい認証ポリシーを選択します
[ポリシーセット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 着信サービス名を入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックして、読み取り専用モードで新しい標準許可ポリシーを作成します。

ステップ 8 [保存（Save）] をクリックします。

ポスチャとネットワーク ドライブ マッピングのベスト プラクティス

Windows エンドポイントのポスチャ アセスメント実行中に、エンドポイント ユーザがデスクトップへのアクセスするときに遅延が生じることがあります。これは、Windows でユーザがデスクトップにアクセスできるようにする前に、ファイル サーバのドライブ文字のマッピングを復元しようとすることが原因で発生する場合があります。ポスチャ実行中の遅延を防ぐためのベスト プラクティスを次に示します。

- ファイル サーバ ドライブ文字をマッピングするときには AD にアクセスする必要があるため、エンドポイントは Active Directory サーバにアクセスできる必要があります。（AnyConnect ISE ポスチャ エージェントを使用した）ポスチャがトリガーされると、AD へのアクセスがブロックされ、これが原因でログインが遅延します。ポスチャが完了する前に、ポスチャ修復 ACL を使用して AD サーバへのアクセスを提供します。
- ポスチャ完了までのログイン スクリプトの遅延を設定し、その後 Persistence 属性を NO に設定する必要があります。Windows はログイン中にすべてのネットワーク ドライブへの再接続を試行しますが、AnyConnect ISE ポスチャ エージェントが完全なネットワーク アクセスを得るまでは、この操作を完了できません。

AnyConnect ステルス モード ワークフロー

ステルス モードでの AnyConnect の設定プロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 AnyConnect エージェント プロファイルを作成します。「AnyConnect エージェント プロファイルの作成」を参照してください。

ステップ 2 AnyConnect パッケージの AnyConnect 設定を作成します。「AnyConnect パッケージの AnyConnect 設定の作成」を参照してください。

ステップ 3 Cisco ISE でオープン DNS プロファイルをアップロードします。「Cisco ISE へのオープン DNS プロファイルのアップロード」を参照してください。

ステップ 4 クライアント プロビジョニング ポリシーを作成します。「クライアント プロビジョニング ポリシーの作成」を参照してください。

ステップ 5 ポスチャ条件を作成します。「ポスチャ条件の作成」を参照してください。

ステップ 6 ポスチャ修復を作成します。「ポスチャ修復の作成」を参照してください。

ステップ 7 クライアントレス モードでポスチャ要件を作成します。「ステルス モードでのポスチャ要件の作成」を参照してください。

ステップ 8 ポスチャ ポリシーを作成します。「ポスチャ ポリシーの作成」を参照してください。

AnyConnect エージェント プロファイルの作成

始める前に

Mac および Windows OS 用の AnyConnect Cisco パッケージおよび AnyConnect 準拠モジュールをアップロードする必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページを選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[NAC エージェントまたは AnyConnect ポスチャ プロファイル（NAC Agent or AnyConnect Posture Profile）] を選択します。

ステップ 3 [ポスチャ エージェント プロファイルの設定（Posture Agent Profile Settings）] ドロップダウンリストから [AnyConnect] を選択します。

ステップ 4 [名前（Name）] フィールドに、目的の名前（たとえば、AC_Agent_Profile）を入力します。

ステップ 5 [エージェントの動作（Agent Behavior）] セクションでは、[ステルス モード（Stealth Mode）] パラメータで[クライアントレス（Clientless）][有効（Enabled）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

AnyConnect パッケージの AnyConnect 設定を作成する必要があります。

AnyConnect パッケージの AnyConnect 設定の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[AnyConnect 設定（AnyConnect Configuration）] を選択します。

ステップ 3 [AnyConnect パッケージの選択（Select AnyConnect Package）] ドロップダウン リストから、必要な AnyConnect パッケージを選択します（AnyConnectDesktopWindows 4.4.117.0 など）。

ステップ 4 [設定名（Configuration Name）] テキスト ボックスに、必要な名前を入力します（AC_Win_44117 など）。

ステップ 5 [コンプライアンス モジュール（Compliance Module）] ドロップダウン リストで、必要なコンプライアンス モジュールを選択します（AnyConnectComplianceModuleWindows 4.2.437.0 など）。

ステップ 6 [AnyConnect モジュール選択（AnyConnect Module Selection）] セクションで、[ISE ポスチャ（ISE Posture）] と [ネットワーク アクセス マネージャ（Network Access Manager）] のチェック ボックスにマークを付けます。

ステップ 7 [プロファイル選択（Profile Selection）] セクションの [ISE ポスチャ（ISE Posture）] ドロップダウン リストで、AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

ステップ 8 [ネットワーク アクセス マネージャ（Network Access Manager）] ドロップダウン リストから、必要な AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

次のタスク

クライアントにプッシュされるオープン DNS プロファイルをアップロードする必要があります。

Cisco ISE へのオープン DNS プロファイルのアップロード

オープン DNS プロファイルがクライアントにプッシュされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[ローカル ディスクのエージェント リソース（Agent Resources From Local Disk）] を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウン リストから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから、[AnyConnect プロファイル（AnyConnect Profile）] を選択します。

ステップ 5 [名前（Name）] テキスト ボックスに、目的の名前（たとえば、OpenDNS）を入力します。

ステップ 6 [参照（Browse）] をクリックして、ローカル ディスクから JSON ファイルを見つけます。
ステップ 7 [送信（Submit）] をクリックします。

次のタスク

クライアント プロビジョニング ポリシーを作成する必要があります。

クライアント プロビジョニング ポリシーの作成

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** ページに移動します。
ステップ 2 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

次のタスク

ポスチャ条件を作成する必要があります。

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Condition）]** の順に移動します。
ステップ 2 必要な名前を入力します（filechk など）。
ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。
ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。
ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。
ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

次のタスク

ポスチャ修復を作成する必要があります。

ポスチャ修復の作成

ファイル条件により、test.txt ファイルがエンドポイントに存在するかどうかが確認されます。存在しない場合の修復は、USB ポートをブロックし、USB デバイスを使用したファイルのインストールを防止することです。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [修復アクション（Remediation Actions）] > [USB 修復（USB Remediations）]** ページに移動します。

ステップ 2 必要な名前を入力します（clientless_mode_block など）。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

ポスチャ要件を作成する必要があります。

ステルス モードでのポスチャ要件の作成

[要件（Requirements）] ページから修復アクションを作成する際は、ステルス モードに適した次の修復だけが表示されます：[マルウェア対策（Anti-Malware）]、[プログラム起動（Launch Program）]、[パッチ管理（Patch Management）]、[USB]、[Windows Server Update Services]、および [Windows Update]。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 ポスチャの必須要件を作成します（たとえば、Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

次のタスク

ポスチャ ポリシーを作成する必要があります。

ポスチャ ポリシーの作成

始める前に

ポスチャ ポリシーの要件およびポリシーがクライアントレス モードで作成されていることを確認してください。

ステップ 1 **[ポリシー（Policy）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します。たとえば、Identity Groups=Any and Operating Systems=Windows 7(All) および Compliance Module=4.x or late および Posture Type=AnyConnect Stealth の場合、Requirements=win7Req となります。

（注） URL リダイレクションのないクライアント プロビジョニングの場合、ネットワーク アクセスまたはRADIUS に固有の属性を使用して条件を設定しても条件は機能せず、Cisco ISE サーバで特定ユーザのセッション情報が使用可能ではないことが原因で、クライアントプロビジョニング ポリシーの照合が失敗することがあります。ただし、Cisco ISE では外部で追加された ID グループに対して条件を設定できます。

AnyConnect ステルス モード通知の有効化

Cisco ISE では AnyConnect ステルス モード展開に対し、いくつかの新しい障害の発生通知を提供します。ステルス モードでの障害の発生通知を有効にすると、有線、ワイヤレスまたはVPN 接続で問題を特定できます。ステルス モードでの通知を有効にするには、次のようにします。

（注） AnyConnect バージョン 4.5.0.3040 は、ステルス モードでの通知をサポートします。

始める前に

ステルス モードで AnyConnect を設定します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [NAC AgentまたはAnyConnect ISEポスチャプロファイル（NAC Agent or AnyConnect ISE Posture Profile）]** を選択します。

ステップ 3 [カテゴリの選択（Select a Category）] ドロップダウン リストから [AnyConnect] を選択します。

ステップ 4 [エージェントの動作（Agent Behavior）] セクションで、[ステルスモードで通知を有効にする（Enable notifications in stealth mode）] オプションに [有効（Enabled）] を選択します。

ポスチャ タイプ

Cisco ISE ポスチャ ポリシーを監視および適用するために使用できる 3 つのポスチャ タイプがあります。

- AnyConnect：AnyConnectエージェントを展開し、クライアントとのやりとりが必要なCisco ISE ポスチャ ポリシーを監視し、適用します。
- AnyConnect Stealth：ユーザの操作なしで、サービスとしてポスチャを実行します。
- Temporal Agent：クライアント上で実行するようにCisco ISE GUI で設定できる一時実行可能ファイル。クライアントが信頼ネットワークにアクセスしようとすると、Cisco ISEは、

ユーザがクライアント上で実行する必要のある実行可能ファイルをプッシュします。Termporal Agent は、コンプライアンス ステータスを再び検査し、そのステータスを Cisco ISE に送信します。Cisco ISE は結果に基づいて必要なアクションを実行します。コンプライアンス処理が完了すると、クライアントから一時エージェントが削除されます。一時エージェントは、カスタム修復をサポートしていません。デフォルトの修復では、メッセージ テキストのみがサポートされます。

（注）

- [ポスチャ タイプ（Posture Types）] を [Temporal Agent]、[コンプライアンス モジュール（Compliance Module）] を [4.x 以降（4.x or later）] として、ポスチャ ポリシーを設定できます。このようなポリシーの修復と要件を作成する際は、コンプライアンス モジュールを「3.x 以前」または「任意のバージョン」に変更しないように注意してください。
- Termporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。
- Cisco ISE は、Mac OSX 向け Temporal Agent を使用した VLAN 制御ポスチャ環境をサポートしていません。これは、ネットワーク アクセスを既存の VLAN から新しい VLAN に変更するときに、VLAN の変更前にユーザの IP アドレスを解放し、ユーザが新しい VLAN に接続するときに新しい IP アドレスを DHCP 経由で要求する必要があるためです。これにはルート権限が必要ですが、Temporal Agent はユーザ プロセスとして実行します。

  Cisco ISE は、エンドポイント IP アドレスの更新を必要としない ACL 制御のポスチャ環境をサポートしています。

Temporal Agent によってサポートされない条件：

- サービス条件 MAC：システム デーモン チェック
- サービス条件 MAC：デーモンまたはユーザ エージェント チェック
- PM：最新チェック
- PM：有効化チェック
- DE：暗号化チェック

[クライアント プロビジョニング（Client Provisioning）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]）と [ポスチャ要件（Posture Requirements）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]）に、ポスチャ タイプが含まれており、推奨されるベス

トプラクティスは、[クライアントプロビジョニング（Client Provisioning）]ページでポスチャプロファイルをプロビジョニングすることです。

ポスチャ要件で AnyConnect ステルス ポスチャ タイプを選択すると、一部の条件、修復、または条件内の属性が無効になります（灰色表示）。たとえば、手動修復ではクライアント側のやりとりが必要となるため、AnyConnect ステルス要件を有効にすると、[手動修復タイプ（Manual Remediation Type）] が無効になります（灰色表示）。

AnyConnect ステルス モードの展開で、ポスチャ プロファイルを AnyConnect 設定にマッピングし、Anyconnect設定を[クライアントプロビジョニング（Client Provisioning）]ページにマッピングする場合、次の処理がサポートされます。

- AnyConnect によるポスチャ プロファイルの読み取りと必要なモードの設定
- 初回ポスチャ要求における AnyConnect による選択したモードに関する情報の Cisco ISE への送信
- Cisco ISE によるモードおよびその他の要因（ID グループ、OS、コンプライアンス モジュールなど）に基づく正しいポリシーの照合。

（注） AnyConnect バージョン 4.4 以降では、ステルス モードでの Cisco ISE ポスチャがサポートされています。

関連トピック

AnyConnect ステルス モード ワークフロー （38 ページ）
Cisco Temporal Agent のワークフロー （44 ページ）

Cisco Temporal Agent のワークフロー

Cisco temporal agent を設定するプロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 ポスチャ条件の作成
ステップ 2 ポスチャ要件の作成
ステップ 3 ポスチャ ポリシーの作成
ステップ 4 クライアント プロビジョニング ポリシーの設定
ステップ 5 Cisco Temporal Agent のダウンロードと起動

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Condition）]** の順に移動します。

ステップ 2 必要な名前を入力します（filecondwin など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

ポスチャ要件の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択します。

ステップ 2 [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。

ステップ 3 [名前（Name）]、[オペレーティング システム（Operating Systems）]、および [コンプライアンス モジュール（Compliance Module）] を入力します（たとえば、Name filereqwin、Operating Systems Windows All、Compliance Module 4.x or later）。

ステップ 4 [ポスチャ タイプ（Posture Type）] ドロップダウンで、[Temporal Agent] を選択します。

ステップ 5 必要な条件（たとえば、filecondwin）を選択します。

（注） Cisco Temporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。

ステップ 6 [メッセージ テキストのみ（Message Text Only）] 修復アクションを選択します。

（注） 一時エージェントは、AnyConnect 4.x 以降でサポートされています。

ポスチャ ポリシーの作成

ステップ 1 **[ポリシー（Policy）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Name=filepolicywin、Identity Groups=Any、Operating Systems=Windows All、Compliance Module=4.x or later、Posture Type=Temporal Agent、および Requirements=filereqwin）。

クライアント プロビジョニング ポリシーの設定

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

Cisco Temporal Agent のダウンロードと起動

ステップ 1 SSID に接続します。

ステップ 2 ブラウザを起動すると、クライアント プロビジョニング ポータルにリダイレクトされます。

ステップ 3 [開始（Start）] をクリックします。これにより、Cisco Temporal Agent がインストールされ、動作しているかどうかがチェックされます。

ステップ 4 [ここに初めて来ました（This Is My First Time Here）] をクリックします。

ステップ 5 [Cisco Temporal Agent をダウンロードして起動するにはここをクリック（Click Here to Download and Launch Cisco Temporal Agent）] を選択します。

ステップ 6 Windows または Mac OSX 用の Cisco Temporal Agent .exe または .dmg ファイルをそれぞれ保存します。
Windows の場合は .exe ファイルを実行し、Mac OSX の場合は .dmg ファイルをダブルクリックして、acisetempagent アプリケーションを実行します。
Cisco Temporal Agent はクライアントをスキャンし、結果（非準拠を示す赤い十字マークなど）を表示します。