CHAPTER 23

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）Cisco のサービスであり、ネットワークに接続するすべてのエンドポイントの状態（ポスチャと呼ばれることもあります）がサービス企業のセキュリティ ポリシーに準拠しているかチェックできるようにします。これにより、ネットワークの保護された領域にアクセスするクライアントを制御できます。

ここでは、Cisco ISE のポスチャ サービスについて説明します。次のトピックを扱います。

ポスチャ サービス

クライアントにインストールされているネットワーク アドミッション コントロール（NAC）Agent は、ポスチャ サービスとの対話により、保護されたネットワークに対するアクセスを取得しようとするすべてのエンドポイントに対してセキュリティ ポリシーを適用します。NAC Agent は、ポスチャ ポリシーに対してクライアントを評価し、コンプライアンスを満たすようにクライアントにセキュリティ ポリシーを適用するのに役立ちます。

Cisco ISE の NAC Agent は、ネイティブ サプリカントの使用時に Windows Fast User Switching をサポートしません。これは、古いユーザが明確に接続解除されていないからです。新しいユーザが送信されると、Agent は古いユーザ プロセスとセッション ID でハングするため、新しいポスチャを行うことができません。Microsoft Security ポリシーに従って、Fast User Switching 無効にすることを推奨します。

クライアント プロビジョニングは、クライアントのポスチャ評価および修復を提供する適切なエージェントでクライアントがセットアップされていることを保証するサービスです。

関連項目

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およびポスチャのランタイム サービスが含まれます。

ポスチャ管理サービス

Cisco ISE に拡張ライセンスをインストールしていない場合は、ポスチャ管理サービスのオプションは管理者ポータルで使用できません。

管理サービスは、ポスチャ サービスに設定されている要件および許可ポリシーに関連付けられている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。

ポスチャのランタイム サービス

ポスチャのランタイム サービスは、SWISS プロトコル サービス、およびポスチャ評価とクライアントの修復のために NAC エージェントと Cisco ISE サーバ間で行われるすべての対話をカプセル化します。

SWISS プロトコルは、管理対象クライアントで実行されている NAC Agent が Cisco ISE サーバを検出し、設定および動作情報を取得できるようにするステートレスな要求応答プロトコルです。NAC Agent は、Cisco ISE サーバに接続するため、ポリシー サービス ペルソナを担当する Cisco ISE ノードがクライアントに応答を送信するまで、SWISS ユニキャスト検出パケットを User Datagram Protocol (UDP) ポート 8905 に送信します。SWISS プロトコルでは、すべてのメッセージに対して TCP トランスポートを使用し、定期的な要求に対しては UDP トランスポートを使用します。NAC Agent では HTTPS 経由ですべての SWISS 要求をトンネリングし、Cisco ISE SWISS UDP サーバに対し、その認証およびポスチャ状態の変更を確認する ping を実行します。

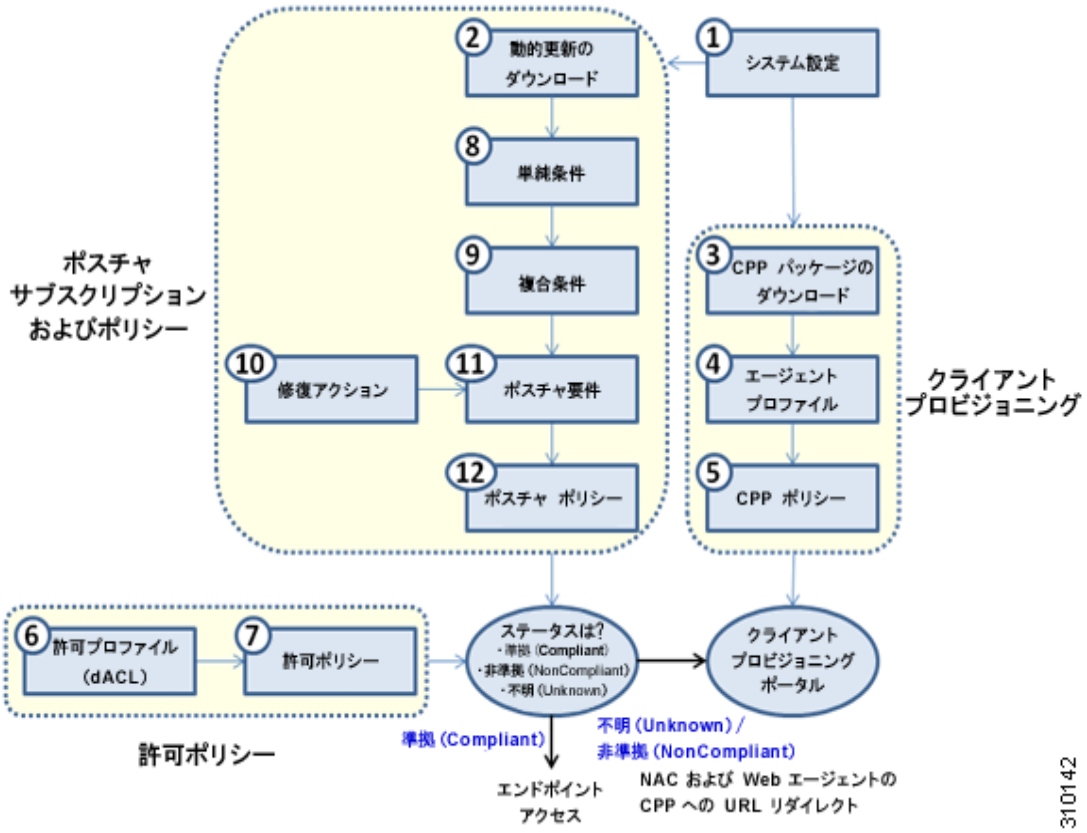
クライアント マシンからの SWISS 要求メッセージには、次の項目のリソース タイプに関する情報が含まれます。

- エージェント プロファイル
- エージェント コンプライアンス モジュール
- エージェント カスタマイズ パッケージ

これらの要求項目の応答に加えて、Cisco ISE サーバからの SWISS 応答には、クライアント マシン上でポスチャ評価および修復を実行するために必要な現在の Agent と URL を更新するプロンプトを含むことができます。

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 23-1　Cisco ISE における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



関連項目

- 「クライアント プロビジョニング リソース ポリシーの設定」（P.22-30）
- 第 22 章「クライアント プロビジョニングの設定」
- *『Cisco Identity Services Engine Network Component Compatibility, Release 1.2』*

ポスチャ サービス ライセンス

Cisco ISE は、基本ライセンスと拡張ライセンスの 2 種類のライセンスを提供します。Cisco ISE の基本サービスには基本ライセンスを、すべてのサービスには拡張ライセンスをインストールする必要があります。展開のタイプとインストールされているライセンスに応じて、Cisco ISE のポスチャ サービスを単一ノードまたは複数ノードで実行できます。また、評価ライセンスがあり、評価ライセンス期間が終了したら適切な基本または拡張ライセンスにアップグレードできます。

プライマリ管理ノードに拡張ライセンスをインストールしていない場合は、実行中に SWISS サーバは初期化されません。SWISS サーバが初期化されない場合、ポスチャ要求は Cisco ISE によって提供されません。ポスチャ実行時サービスは、Cisco ISE 展開で拡張ライセンス ファイルを追加または削除す

ると、適切なアクションを実行します。実行時に、拡張ライセンスを追加した場合は SWISS サーバが初期化され、拡張ライセンスを削除した場合、または拡張ライセンスが期限切れになった場合は、SWISS サーバが停止します。

ポスチャ サービス展開

Cisco ISE サービスは、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、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すべてを 1 つのノードで設定できます。

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、または、必要に応じてインライン ポスチャ ノードとして設定できます。管理サービスを実行するノードが、その Cisco ISE 展開におけるプライマリ ノードです。他のサービスを実行する他のノードはセカンダリ ノードであり、互いのバックアップ サービス用に設定できます。

ポスチャ セッション サービスの展開

SWISS サーバを初期化し、クライアントから受信したすべてのポスチャ要求を処理するには、Cisco ISE のセッション 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。

はじめる前に

- 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 ノードから離れて [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、ポリシー サービス、およびモニタリング ペルソナ）またはインライン ポスチャ ノード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　Cisco ISE ノードを [展開ノード（Deployment Nodes）] ページで選択します。

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）] タブの [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　[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て、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 サービスを実行します。セッション サービスを停止するには、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 レポートの実行

ポスチャ評価で使用されたポスチャ 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するには、Posture Detail Assessment レポートを実行できます。

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）] > [Posture Detail Assessment] を選択します。

ステップ 2　[時間範囲（Time Range）] ドロップダウン矢印をクリックし、ディクショナリ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、選択された期間における、ログオンしたすべてのエンドポイントの概要を表示します。

関連項目

- 第 26 章「レポート」

ポスチャ管理の設定

ポスチャ サービス用に管理者ポータルをグローバルに設定できます。更新を、シスコから Web を経由して Cisco ISE サーバに自動的にダウンロードできます。後で Cisco ISE をオフラインで手動で更新できます。さらに、クライアント上にインストールされている NAC Agent と Web Agent は、クライアントにポスチャ評価および修復サービスを提供します。NAC Agent および Web Agent では、Cisco ISE に対する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。ログインし、ポスチャの要件評価に成功すると、Windows 上の NAC Agent および Web Agent によって、ネットワーク利用条件に従うことをエンド ユーザに求めるリンクを示すダイアログが表示されます。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。

関連項目

- 「クライアントのタイマー設定」（P.23-5）
- 「非エージェント デバイスのポスチャ ステータスの設定」（P.23-7）
- 「定期的再評価」（P.23-8）
- 「ポスチャ更新のダウンロード」（P.23-9）
- 「ポスチャ更新の自動ダウンロード」（P.23-10）
- 「ポスチャ評価のアクセプタブル ユース ポリシーの設定」（P.23-11）

クライアントのタイマー設定

ユーザが修復したり、ある状態から別の状態に遷移したり、ログイン成功画面を制御したりするためのタイマーを設定できます。

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を使用してエージェント プロファイルを設定して、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。[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）] > [新しいプロファイル（New Profile）] のクライアント プロビジョニング リソースで、これらすべてのタイマーをエージェントに設定できます。

ただし、クライアント プロビジョニング ポリシーと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、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] 設定ページで設定を使用できます。

関連項目

- 「エージェント プロファイル パラメータおよび適用可能な値」（P.22-15）
- 「ユーザが修復するためのタイマーの設定」（P.23-6）
- 「ユーザが遷移するための時間の設定」（P.23-6）
- 「自動的にログイン ウィンドウを閉じるためのタイマーの設定」（P.23-7）

ユーザが修復するためのタイマーの設定

指定した時間内にクライアントが自ら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すると、NAC Agent はクライアントが修復タイマーに設定された時間内に修復するを待ちます。クライアントがこの指定時間内に修復できない場合、NAC Agent はポスチャ実行時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状態に移動されます。

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、分単位で時間値を入力します。

デフォルト値は 4 分です。有効範囲は 1 ～ 300 分です。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「ポスチャの全般設定」（P.A-20）

ユーザが遷移するための時間の設定

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、許可変更が（CoA）が完了するために必要です。ポスチャの成功および失敗の際に、クライアントが新規 VLAN IP アドレスを取得するための時間を必要とする場合、より長い遅延時間が必要となる場合があります。ポスチャが成功した場合、Cisco ISE では、クライアントに、ネットワーク遷移遅延タイマーで指定された時間内に不明から準拠モードに遷移することを許可します。ポスチャが失敗した場合、Cisco ISE ではクライアントに、タイマーで指定された時間内に不明から非準拠モードに遷移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）] フィールドにネットワーク遅延フィールドの秒単位で時間値を入力します。

デフォルト値は 3 秒です。有効範囲は 2 ～ 30 秒です。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ポスチャの全般設定」（P.A-20）

自動的にログイン ウィンドウを閉じるためのタイマーの設定

ポスチャ評価が成功すると、NAC Agent および Web Agent 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。ユーザがログイン画面を閉じるには、ログイン画面で [OK] ボタンをクリックする必要があります。指定時間後にこのログイン画面を自動的に閉じるための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　[一定時間（秒）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　[一定時間（秒）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隣にあるフィールドに、秒単位で時間値を入力します。

有効な範囲は、0 ～ 300 秒です。時間がゼロに設定された場合、NAC Agent および Web Agent で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。

関連項目

- 「ポスチャの全般設定」（P.A-20）

非エージェント デバイスのポスチャ ステータスの設定

Linux または iDevices などの非エージェント デバイス上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 iDevices が Cisco ISE に対応の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のポスチャ ステータス設定を使用します。

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ない場合に、Windows および Macintosh オペレーティング システム上で実行されるエンドポイントにも適用できます。

はじめる前に

一致するポスチャ ポリシーで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。そうでない場合は、エンドポイントのポスチャ ステータスにデフォルト設定が自動的に反映されます。詳細については、「クライアント プロビジョニング リソース ポリシーの設定」（P.22-30）を参照してください。

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　[デフォルトのポスチャ ステータス（Default Posture Status）] から、オプションを [準拠（Compliant）] または [非準拠（Noncompliant）] として選択します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ポスチャの全般設定」（P.A-20）

定期的再評価

定期的再評価（PRA）の設定は、コンプライアンスのためにすでに正常にポスチャされているクライアントにのみ行うことができます。ネットワーク上でクライアントが準拠していない場合、PRA は実行できません。

NAC Agent では、クライアントが正常にポスチャされ、ネットワーク上で準拠状態にある場合、ポリシー サービス ノードにコンプライアンス レポートを送信します。PRA は、エンドポイントが準拠状態にある場合にのみ、有効かつ適用可能です。ポリシー サービス ノードでは、関連ポリシーを確認し、PRA を適用するための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 ノードでは、CoA 要求を発行する前に、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 NAC Agent に応答します。NAC Agent では、設定で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 設定に設定されたアクションが続行される場合、クライアントは準拠状態のままになります。クライアントが PRA を満たすことができない場合、そのクライアントは準拠状態から非準拠状態に移行します。

PRA 要求では、これがポスチャの再評価要求であるにもかかわらず、PostureStatus 属性に現在のポスチャ ステータスが不明ではなく準拠と表示されます。PostureStatus は、モニタリング レポートでも更新されます。認証の成功後にクライアントがポスチャされていることを前提として、PRA 要求でサーバから取得した新しい要件およびポスチャ ポリシーを再評価する前のクライアントの PostureStatus 属性のときに、ポスチャ ステータスは不明です。

関連項目

- 「定期的再評価の設定」（P.23-8）

定期的再評価の設定

定期的再評価は、コンプライアンスのためにすでに正常にポスチャされているクライアントにのみ設定することができます。システムで定義されているユーザ ID グループに対して各 PRA を設定できます。[任意（Any）] ロールで PRA を設定した場合、このロールを持つ設定だけが存在し、他の設定はシステムに存在しません。

はじめる前に

- 各 PRA 設定には、必ず、一意の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割り当てられるようにします。
- role_test_1 および role_test_2 を割り当てることができます。これらは、PRA 設定への 2 つの一意のロールです。これらの 2 つのロールを論理演算子で結合し、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。
- 2 つの PRA 設定に共通のユーザの ID グループがないことを確認します。
- ユーザ ID グループ [*任意（Any）*] を含む PRA 設定がすでに存在する場合は、次の操作を実行しないと、他の PRA 設定を作成できません。

- 既存の PRA 設定を [任意（Any）] ユーザ ID グループで更新し、[任意（Any）] 以外のユーザの ID グループを反映するようにします。

  または

- ユーザ ID グループ「*任意（Any）*」を含む既存の 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 メッセージを作成するには、[新しい再評価設定（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。

関連項目

- 「ポスチャ再評価の設定」（P.A-21）

ポスチャ更新のダウンロード

ポスチャ更新には、Windows と Macintosh の両方のオペレーティング システム用のアンチウイルスおよび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、およびサポート表、およびシスコがサポートするオペレーティング システム情報が含まれます。ローカル システム上の最新の更新のアーカイブを含むファイルから、オフラインで Cisco ISE を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。このプロセスには通常約 20 分かかります。初期ダウンロード後、差分更新の確認およびダウンロードが自動的に行われるように 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による更新中にこれらを再作成しません。

はじめる前に

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の場所にアクセスできるようにするには、「Cisco ISE でのプロキシ設定の指定」（P.5-3）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。

Web から更新を動的にダウンロードするには、[ポスチャの更新（Posture Update）] ページを使用できます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [アップデート（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すします。

ステップ 3　[更新フィード URL（Update Feed URL）] フィールドにシスコのデフォルト値を設定するには、[デフォルトに設定（Set to Default）] をクリックします。デフォルトの更新のフィード URL は https://www.cisco.com/web/secure/pmbu/posture-update.xml です。

ネットワークが URL リダイレクション機能を制限し（プロキシ サーバ経由など）、上記の URL へのアクセスに問題がある場合は、Cisco ISE も https://www.perfigo.com/ise/posture-update.xml を指すようにします。

ステップ 4　[ポスチャの更新（Posture Update）] ページで値を変更します。

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

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

更新されると、[ポスチャの更新（Posture Update）] ページに、現在の Cisco updates のバージョン情報が、[ポスチャの更新（Posture Update）] ページの [更新情報（Update Information）] セクションの更新の検証として表示されます。

ポスチャ更新の自動ダウンロード

初期更新後、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。

はじめる前に

- 最初にポスチャ更新をダウンロードして、Cisco ISE を設定して、更新を確認し、自動的にダウンロードするようにしているはずです。「ポスチャ更新のダウンロード」（P.23-9）を参照してください。

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

ステップ 2　[ポスチャの更新（Posture Update）] ページで、[初期遅延から開始する更新を自動的に確認する（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。

初期遅延時間の経過後に、Cisco ISE による更新のチェックが開始されます。

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更新を展開に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。

（注）　更新を自動的に確認するように Cisco ISE を設定すると、最新の AV/AS サポート表がそれに従って読み込まれます。いずれにしても、最新のコンプライアンス モジュールをダウンロードし、クライアントのプロビジョニング ポリシーに手動で追加する必要があります。最新のサポート表が既存のコンプライアンス モジュールと同期していない場合は、最新のコンプライアンス モジュールをダウンロードして、クライアントのプロビジョニング ポリシーに追加していることを確認します。

関連項目

- Cisco ISE のオフライン ポスチャ パッケージの更新の実行の詳細については、『*Release Notes for the Cisco Identity Services Engine, Release 1.2*』の「Cisco ISE Offline Updates」の項を参照してください。
- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソース ポリシーの設定」（P.22-30）
- 「ポスチャのカスタム条件」（P.23-14）

ポスチャ評価のアクセプタブル ユース ポリシーの設定

ログインし、クライアントのポスチャ評価が成功すると、NAC Agent および Web Agent 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、アクセプタブル ユース ポリシー（AUP）へのリンクが含まれます。ユーザがリンクをクリックすると、読んで承諾する必要がある、network-usage terms and conditions を表示するページにリダイレクトされます。

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 NAC Agent および Web Agent 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。

関連項目

- 「ポスチャ アクセプタブル ユース ポリシーの設定」（P.A-22）

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ているポスチャ要件の集合です。ディクショナリ属性は、ID グループ、およびクライアントの異なるポリシーを定義できるようにするオペレーティング システムと併せて、オプションの条件です。

はじめる前に

- 利用規定（AUP）について理解しておく必要があります。次を参照してください。「ポスチャ評価のアクセプタブル ユース ポリシーの設定」（P.23-11）
- 定期的再評価（PRA））について理解しておく必要があります。「定期的再評価の設定」（P.23-8）を参照してください。

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　[ステータス（Status）] タイプを選択します。

ステップ 3　[ルール名（Rule Name）] テキスト ボックスに、ポリシー名を入力します。

ステップ 4　[ID グループ（identity Groups）] から、ロールを選択します。

ステップ 5　[オペレーティング システム（Operating Systems）] から、オペレーティング システムを選択します。

ステップ 6　[その他の条件（Other Conditions）] で、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）] ページ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している間は表示されません。

ステップ 7　[要件（Requirements）] から、要件を選択します。新しい要件も作成できます。

ステップ 8　[完了（Done）] をクリックします。

ステップ 9　[保存（Save）] をクリックします。

関連項目

- 「ポスチャ評価のオプション」（P.23-12）
- 「クライアント ポスチャ要件の作成」（P.23-20）
- 「単純ポスチャ条件の作成」（P.18-6）
- 「複合ポスチャ条件の作成」（P.18-8）
- 「時刻と日付の条件」（P.20-10）
- 「エージェントがポスチャ評価の開始に失敗する」（P.G-32）

ポスチャ評価のオプション

次の表に、Windows および Macintosh の NAC 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）のリストを示します。

表 23-1　ポスチャ評価のオプション

Windows 用 NAC Agent	Windows 用 Web Agent	Macintosh OS X 用 NAC Agent
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（Operating System/Service Packs/Hotfixes）	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（Operating System/Service Packs/Hotfixes）	—
プロセス チェック（Process Check）	プロセス チェック（Process Check）	—
レジストリ チェック（Registry Check）	レジストリ チェック（Registry Check）	—
ファイル チェック（File Check）	ファイル チェック（File Check）	—
アプリケーション チェック（Application Check）	アプリケーション チェック（Application Check）	—
アンチウイルスのインストール（Antivirus Installation）	アンチウイルスのインストール（Antivirus Installation）	アンチウイルスのインストール（Antivirus Installation）
アンチウイルスのバージョン/アンチウイルス定義日付（Antivirus Version/ Antivirus Definition Date）	アンチウイルスのバージョン/アンチウイルス定義日付（Antivirus Version/ Antivirus Definition Date）	アンチウイルスのバージョン/アンチウイルス定義日付（Antivirus Version/ Antivirus Definition Date）

表 23-1　ポスチャ評価のオプション （続き）

Windows 用 NAC Agent	Windows 用 Web Agent	Macintosh OS X 用 NAC Agent
アンチスパイウェアのインストール（Antispyware Installation）	アンチスパイウェアのインストール（Antispyware Installation）	アンチスパイウェアのインストール（Antispyware Installation）
アンチスパイウェアのバージョン/アンチスパイウェア定義日付（Antispyware Version/ Antispyware Definition Date）	アンチスパイウェアのバージョン/アンチスパイウェア定義日付（Antispyware Version/ Antispyware Definition Date）	アンチスパイウェアのバージョン/アンチスパイウェア定義日付（Antispyware Version/ Antispyware Definition Date）
Windows Update 実行中（Windows Update Running）	Windows Update 実行中（Windows Update Running）	—
Windows Update 設定（Windows Update Configuration）	Windows Update 設定（Windows Update Configuration）	—
WSUS コンプライアンス設定（WSUS Compliance Settings）	WSUS コンプライアンス設定（WSUS Compliance Settings）	—

ポスチャ修復オプション

次の表に、Windows および Macintosh の NAC Agent、および Windows の Web Agent でサポートされるポスチャ修復のリストを示します。

表 23-2　ポスチャ修復オプション

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
メッセージ テキスト（ローカル チェック）（Message Text (Local Check)）	メッセージ テキスト（ローカル チェック）（Message Text (Local Check)）	メッセージ テキスト（ローカル チェック）（Message Text (Local Check)）
URL リンク（リンク配布）（URL Link (Link Distribution)）	URL リンク（リンク配布）（URL Link (Link Distribution)）	URL リンク（リンク配布）（URL Link (Link Distribution)）
ファイル配布（File Distribution）	ファイル配布（File Distribution）	—
プログラム起動（Launch Program）	—	—
アンチウイルス定義更新（Antivirus Definition Update）	—	アンチウイルス ライブ更新（Antivirus Live Update）

表 23-2　ポスチャ修復オプション （続き）

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
アンチスパイウェア定義更新（Antispyware Definition Update）	—	アンチスパイウェア ライブ更新（Antispyware Live Update）
Windows Update	—	—
WSUS	—	—

ポスチャのカスタム条件

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のいずれの単純条件もポスチャ条件として使用できます。これらの単純条件の 1 つ以上の条件が複合条件を形成し、それをポスチャ要件に関連付けることができます。

初期ポスチャ更新後に、Cisco ISE でもシスコ定義の単純条件および複合条件を作成します。シスコ定義の単純条件は pc_ as を使用し、複合条件は pr_ as を使用します。

ユーザ定義条件またはシスコ定義の条件には単純と複合の両方の条件が含まれます。

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）の複合条件に基づいて内部チェックを使用します。したがって、ポスチャ レポートは、作成した正確な AV/AS の複合条件名を反映しません。レポートには、AV/AS の複合条件の内部チェック名だけが表示されます。

たとえば、ベンダーおよび製品をチェックするために "MyCondition_AV_Check" という名前の AV 複合条件を作成した場合は、条件名として "MyCondition_AV_Check" ではなく、内部チェック、つまり "av_def_ANY" が表示されます。

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポスチャ条件」（P.18-5）
- 「単純ポスチャ条件」（P.18-5）
- 「単純ポスチャ条件の作成」（P.18-6）
- 「複合ポスチャ条件」（P.18-6）
- 「複合ポスチャ条件の作成」（P.18-8）

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 アップデート、Windows Server Update Service（WSUS）の修復タイプです。

表 23-3 に、Windows と Macintosh クライアント用の NAC Web Agent および NAC Agent によってサポートされる修復のタイプを示します。

表 23-3　各エージェントでサポートされる修復タイプ

修復タイプ	Windows 用の NAC Agent	Windows 用の Web Agent	Macintosh 用の NAC Agent
ファイル修復	サポート対象	サポート対象	—
リンク修復（手動）	サポート対象	サポート対象	サポート対象
リンク修復（自動）	サポート対象	非サポート	非サポート
アンチウイルス修復（手動）	サポート対象	未サポート	サポート対象
アンチウイルス修復（自動）	サポート対象	未サポート	非サポート
アンチスパイウェア修復（手動）	サポート対象	未サポート	非サポート
アンチスパイウェア修復（自動）	サポート対象	未サポート	非サポート
プログラム起動修復（手動）	サポート対象	未サポート	—
プログラム起動修復（自動）	サポート対象	未サポート	—
Windows Update 修復（手動）	サポート対象	未サポート	—
Windows Update 修復（自動）	サポート対象	未サポート	—
Windows Server Update Service 修復（手動）	サポート対象	未サポート	—
Windows Server Update Service 修復（自動）	サポート対象	未サポート	—

関連項目

- 「ファイル修復の追加」（P.23-15）
- 「リンク修復の追加」（P.23-16）
- 「アンチウイルス修復の追加」（P.23-16）
- 「アンチスパイウェア修復の追加」（P.23-17）
- 「プログラム起動修復の追加」（P.23-17）
- 「Windows Update 修復の追加」（P.23-18）
- 「Windows Server Update Service 修復の追加」（P.23-19）
- 「エージェントがポスチャ評価の開始に失敗する」（P.G-32）

ファイル修復の追加

ファイル修復を行うと、クライアントはコンプライアンスのために必要なファイル バージョンをダウンロードできます。NAC Agent と Web Agent は、コンプライアンスのためにクライアントが必要なファイルで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、または削除できますが、ファイル修復を編集できません。[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　[新しいファイル修復（New File 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。

関連項目

- 「ファイル修復」（P.B-28）

リンク修復の追加

リンク修復を使用すると、クライアントは URL をクリックして修復ページまたはリソースにアクセスできます。NAC Agent と Web Agent はリンクによってブラウザを開き、クライアントがコンプライアンスのために自ら修復できるようになります。

[リンク修復（Link Remediations）] 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　[新しいリンク修復（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。

関連項目

- 「リンク修復」（P.B-28）

アンチウイルス修復の追加

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する、アンチウイルス修復を作成できます。

[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　[新しい 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。

関連項目

- 「アンチウイルス修復」（P.B-29）

アンチスパイウェア修復の追加

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する、アンチスパイウェア修復を作成できます。

[AS 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　[AS 修復（AS 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　[新しい 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。

関連項目

- 「アンチスパイウェア修復」（P.B-30）

プログラム起動修復の追加

NAC Agent と Web Agent がコンプライアンスのために 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起動修復を作成できます。

[プログラム起動修復（Launch Program Remediations）] ページには、すべてのプログラム起動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　[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　[新しいプログラム起動修復（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。

関連項目

- 「プログラム起動修復」（P.B-30）

Windows Update 修復

Windows Update 修復は、Windows クライアントで自動更新の設定がセキュリティ ポリシーごとにオンになっていることを確認します。Windows 管理者には、Windows クライアント上での自動更新をオンまたはオフにするオプションがあります。Microsoft Windows では、この機能を使用して更新を定期的に確認します。自動更新機能が有効になっている場合、Windows は他の更新の前に、ウィンドウ推奨のアップデートを自動的に更新します。

Windows 自動更新設定は、Windows オペレーティング システムの種類によって異なります。

たとえば、Windows XP では、自動更新設定に次の設定があります。

- 自動（推奨）：Windows は、クライアントが推奨された Windows アップデートを自動的にダウンロードしてインストールできるようにします
- 更新をダウンロードするが、インストールする時間はクライアントが選択する：Windows はクライアントの更新をダウンロードし、更新をインストールする時間はクライアントが選択できます
- クライアントに通知するが、自動的にダウンロードおよびインストールしない：Windows は、更新をクライアントに通知するだけで、自動的にダウンロードまたはインストールしません
- 自動更新をオフにする：Windows は、クライアントが自動更新機能をオフにできるようにします。ここでは、クライアントが更新を定期的にインストールしない限り、クライアントは脆弱です。更新は Windows Update Web サイト リンクから実行できます。

Windows Update サービス（wuaserv）が任意の Windows クライアントで開始または停止されているかどうかを、**pr_AutoUpdateCheck_Rule** を使用して確認できます。これは、ポスチャ要件を作成するために使用できる事前定義されたシスコのルールです。ポスチャ要件が失敗した場合、要件に関連付けた Windows Update 修復は、Windows クライアントに自動更新のオプションの 1 つを使用して修復するように強制します。

関連項目

- Windows Update 修復の追加

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　[新しい 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。

関連項目

- 「Windows Update 修復」（P.B-31）

Windows Server Update Service 修復の追加

コンプライアンスのために、ローカルで管理されているか、または Microsoft の管理する 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 Service（WSUS）修復は、ローカルで管理された WSUS サーバまたは Microsoft の管理する 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。

NAC Agent 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 Services 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　[新しい 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。

関連項目

- 「Windows Server Update Service 修復」（P.B-32）

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 システムにリンクできる関連する修復アクションを含む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、ネットワーク上で準拠するためにポスチャ評価中にすべての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あり、クライアントが要件に失敗した場合、クライアントには、エンドポイントのポスチャ評価中にさらに続行するオプションがあります。

必須要件

クライアントがポスチャ ポリシーで定義されている必須要件を満たすことができなかった場合、ポリシー評価中に修復オプションが与えられます。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修復して要件を満たす必要があります。

クライアント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。クライアントを非準拠状態から移行するには、「非準拠状態のクライアント システム スタック」（P.23-20）を参照してください。

オプション要件

クライアントがポリシー評価中にオプション要件を満たすことができなかった場合、エージェントはエンド ユーザに、オプション要件をスキップできるようにさらに続行するオプションをプロンプトで表示します。

監査要件

監査要件は、エンド ユーザがポリシー評価中に成功または失敗しても表示されません。

関連項目

- 「非準拠状態のクライアント システム スタック」（P.23-20）
- 「カスタム ポスチャ修復アクション」（P.23-14）
- 「エージェントがポスチャ評価の開始に失敗する」（P.G-32）

非準拠状態のクライアント システム スタック

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「不準拠」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、特定の認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、「ダウンロード可能 ACL の権限の設定」（P.20-12）を参照してください。この方法は、インライン ポスチャ展開ではサポートされません。
  - 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。

関連項目

- 「ポスチャ ポリシーの設定」（P.23-11）
- 「カスタム ポスチャ修復アクション」（P.23-14）
- 「クライアント ポスチャ要件の作成」（P.23-20）

クライアント ポスチャ要件の作成

ユーザ定義の条件、シスコ定義の条件、および修復アクションを関連付けることができる [要件（Requirements）] ページで要件を作成できます。[要件（Requirements）] ページで作成および保存すると、ユーザ定義の条件および修復アクションをそれぞれのリスト ページで表示することができます。

はじめる前に

- ポスチャの利用規定（AUPs）について理解しておく必要があります。「ポスチャ評価のアクセプタブル ユース ポリシーの設定」（P.23-11）を参照してください。

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）] ページで値を入力します。

ステップ 3　[完了（Done）] をクリックして、ポスチャ要件を読み取り専用モードで保存します。

ステップ 4　[保存（Save）] をクリックします。

関連項目

- 「標準許可ポリシーの設定」（P.23-22）
- 「クライアントのポスチャ要件」（P.B-33）

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には、[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 NAC Agent 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。

関連項目

- 「標準許可ポリシーの設定」（P.23-22）

標準許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページで、標準認可ポリシーと例外認可ポリシーの 2 種類の認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を決定するために使用されます。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] を選択します。

ステップ 2　[許可ポリシー（Authorization Policy）] ページの上部に表示されるドロップダウン リストから適用する一致ルール タイプの 1 つを選択します。

- [最初に一致したルールの適用（First Matched Rule Applies）] : このオプションは、評価中に標準許可ポリシーのリストで最初に一致する 1 つの許可ポリシーで、アクセス権限を設定します。一致する最初の許可ポリシーが見つかった場合、残りの標準許可ポリシーは評価されません。
- [複数の一致したルールの適用（Multiple Matched Rule Applies）] : このオプションは、評価中に標準許可ポリシーのすべてのリストで一致する複数の許可ポリシーで、アクセス権限を設定します。

ステップ 3　デフォルトの標準許可ポリシー行の [編集（Edit）] の隣にある下矢印をクリックします。

ステップ 4　[新規ルールを上に挿入（Insert New Rule Above）] をクリックします。

ステップ 5　ルール名を入力し、ID グループおよびその他の条件を選択し、デフォルトの標準許可ポリシー行の上に表示される新しい許可ポリシー行に許可プロファイルを関連付けます。

ステップ 6　[完了（Done）] をクリックして、新しい標準許可ポリシーを読み取り専用モードで作成します。

ステップ 7　[保存（Save）] をクリックします。

関連項目

- 「ポスチャのカスタム権限」（P.23-21）
- 「許可ポリシーの設定」（P.B-4）
- 第 20 章「許可ポリシーおよびプロファイルの管理」