ポリシーのユーザ インターフェイスのリファレンス

この章は、Cisco Identity Services Engine（ISE）で提供される管理者ポータル要素のリファレンスで、次のポリシー関連の項が含まれます。

- 「認証」（P.B-1）
- 「許可ポリシーの設定」（P.B-4）
- 「エンドポイント プロファイリング ポリシーの設定」（P.B-5）
- 「ディクショナリ」（P.B-8）
- 「条件（Conditions）」（P.B-9）
- 「結果」（P.B-18）

認証

ここでは、次の内容について説明します。

- 「単純な認証ポリシーの設定」（P.B-1）
- 「ルール ベースの認証ポリシーの設定」（P.B-2）

単純な認証ポリシーの設定

次の表に、単純な認証ポリシーを設定できるようにする単純な認証ポリシー ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [認証（Authentication）] > [単純（Simple）] です。

表 B-1　　単純な認証ポリシーの設定

フィールド	使用上のガイドライン
ネットワーク アクセス サービス（Network Access Service）	作成済みの許可されるプロトコルを選択します。

表 B-1　単純な認証ポリシーの設定 （続き）

フィールド	使用上のガイドライン
ID ソース（Identity Source）	認証に使用する ID ソースを選択します。ID ソース順序が設定済みである場合、これを選択することも可能です。ID ソース順序の設定方法については、「ID ソース順序の作成」（P.14-40）を参照してください。
オプション（Options）	認証に失敗した場合、ユーザが見つからない場合、または処理に問題が発生した場合のアクションのコースを詳細に指定できます。次のいずれかのオプションを選択できます。 • [拒否（Reject）] : 拒否応答が送信されます。 • [ドロップ（Drop）] : 応答が送信されません。 • [続行（Continue）] : Cisco ISE は認証ポリシーの処理を続行します。

関連項目

- 「簡易認証ポリシーの設定」（P.19-23）
- ID ソース順序の設定方法については、「ID ソース順序の作成」（P.14-40）を参照してください。

ルール ベースの認証ポリシーの設定

次の表に、ルール ベースの認証ポリシーを設定できる、ルール ベースの認証ポリシー ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [認証（Authentication）] > [ルールベース（Rule-Based）] です。

表 B-2　ルール ベースの認証ポリシーの設定

フィールド	使用上のガイドライン
ステータス（Status）	このポリシーのステータスを選択します。次のいずれかを指定できます。 • [有効（Enabled）] : このポリシー条件はアクティブです。 • [無効（Disabled）] : このポリシー条件は非アクティブであり、評価されません。 • [モニタのみ（Monitor Only）] : このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加したいけれども、条件が正しい結果を生じるかどうかわかりません。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
標準ルール（Standard Rule）	このポリシーの名前を入力し、条件および許可されるプロトコルを選択します。
条件（Conditions）	プラス [+] 記号をクリックして条件の固定オーバーレイを展開し、マイナス [-] 記号をクリックするか、または固定オーバーレイの外側をクリックして閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] : シスコ事前定義の条件をポリシー要素ライブラリから選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] : さまざまなシステム ディクショナリまたはユーザ定義ディクショナリから属性を選択して、式を定義できます。

表 B-2　ルール ベースの認証ポリシーの設定 （続き）

フィールド	使用上のガイドライン
既存の条件をライブラリから選択（Select Existing Condition from Library）	次の操作が可能です。 1. ポリシー要素での認証用に定義しておいた事前定義済み条件を選択し、AND または OR 演算子を使用して複数の条件を追加します。 次のディクショナリまたは属性を含む、特定の事前定義済み条件は選択できません。 • ディクショナリ「Certificate」、およびすべての属性 • ディクショナリ「Network Access」、および次の属性： – Device IP Address – ISE Host Name – NetworkDeviceName – Protocol – UseCase このような条件が使用できる場合、選択ボックスの最初のエントリは「関連する条件のみ選択可能」になります。 2. [操作（Action）] アイコンをクリックし、後のステップで次の操作を行います。 • [属性/値の追加（Add Attribute/Value）]：アドホック属性/値のペアを追加できます。 • [条件をライブラリから追加（Add Condition from Library）]：シスコ事前定義の条件を追加できます。 • [複製（Duplicate）]：選択した条件のコピーを作成します。 • [条件をライブラリに追加（Add Condition to Library）]：作成したアドホック属性/値のペアをポリシー要素ライブラリに保存できます。 • [削除（Remove）]：選択した条件を削除します。
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	次の操作が可能です。 1. アドホック属性/値のペアを式に追加し、AND または OR 演算子を使用して複数の条件を追加できます。 2. [操作（Action）] アイコンをクリックし、後のステップで次の操作を行います。 – [属性/値の追加（Add Attribute/Value）]：アドホック属性/値のペアを追加できます。 – [条件をライブラリから追加（Add Condition from Library）]：シスコ事前定義の条件を追加できます。 – [複製（Duplicate）]：選択した条件のコピーを作成します。 – [条件をライブラリに追加（Add Condition to Library）]：作成したアドホック属性/値のペアをポリシー要素ライブラリに保存できます。 – [削除（Remove）]：選択した条件を削除します。ここでは、AND または OR 演算子を使用できます
ネットワーク アクセスの選択（Network Access）	許可されるプロトコルまたは RADIUS サーバ順序から選択します。
	ID ソース選択条件を定義する場合にクリックします。
ID ソース順序	

表 B-2　ルール ベースの認証ポリシーの設定 （続き）

フィールド	使用上のガイドライン
[操作（Action）] アイコン	デフォルトの ID ソースの行のアクション アイコンをクリックして、[新規行を上に挿入（Insert new row above）] をクリックします。
ストアのルール名 1 の入力（Enter a store rule name 1）	作成した ID ソース ルールの名前を入力します。
	ボタンをクリックして、選択する ID ソースに応じて条件を定義します。
内部ユーザ（Internal Users）	ID ソース順序または ID ソースを選択し、Cisco ISE で実行するアクションを選択します。

関連項目

「ルール ベースの認証ポリシーの設定」（P.19-23）

許可ポリシーの設定

次の表に、認証ポリシーを設定できるようにする認証ポリシー ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [認証（Authentication）] です。

表 B-3　許可ポリシーの設定

フィールド	使用上のガイドライン
ステータス（Status）	ポリシーを適用するには、次のいずれかを選択します。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニタのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加したいけれども、条件が正しい結果を生じるかどうかわかりません。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名（Rule Name）	ルール名に名前を入力します。
条件（Conditions）（ID グループおよびその他の条件）	最初のドロップダウンから ID グループを選択します。 2 番めのドロップダウンから条件を選択します。 既存の条件から選択することも、新しい条件を作成することもできます。
権限（Permissions）	**標準**カテゴリから許可プロファイルを選択します。

関連項目

「許可ポリシーの設定」（P.20-8）

エンドポイント プロファイリング ポリシーの設定

次の表に、[エンドポイント ポリシー（Endpoint Policies）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）] です。

表 B-4　エンドポイント プロファイリング ポリシーの設定

フィールド	使用上のガイドライン
名前（Name）	作成するエンドポイント プロファイリング ポリシーの名前を入力します。
説明（Description）	作成するエンドポイント プロファイリングのポリシーの説明を入力します。
ポリシー有効（Policy Enabled）	エンドポイントをプロファイリングするときに一致するプロファイリング ポリシーを関連付けるために、デフォルトでは、[ポリシー有効（Policy Enabled）] チェックボックスはオンになっています。 オフの場合は、エンドポイントをプロファイリングするときにエンドポイント プロファイリング ポリシーは除外されます。
最小確実度係数（Minimum Certainty Factor）	プロファイリング ポリシーに関連付ける最小値を入力します。デフォルト値は、10 です。
例外アクション（Exception Actions）	プロファイリング ポリシーのルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは NONE です。例外アクションは次の場所で定義されています。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）]。
ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）	必要に応じて、プロファイリング ポリシーのルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは NONE です。例外アクションは次の場所で定義されています。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]。
ポリシーの ID グループを作成（Create an Identity Group for the policy）	エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。 • **はい、一致する ID グループを作成します（Yes, create matching Identity Group）** • **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**
はい、一致する ID グループを作成します（Yes, create matching Identity Group）	既存のプロファイリング ポリシーを使用する場合にこのオプションを選択します。 このオプションは、エンドポイントの一致 ID グループを作成します。その ID グループは、エンドポイント プロファイルが既存のプロファイリング ポリシーに一致する場合にプロファイリングされたエンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

表 B-4　エンドポイント プロファイリング ポリシーの設定 （続き）

フィールド	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てる場合にこのチェックボックスをオンにします。 このオプションを使用すると、エンドポイント プロファイリング ポリシー階層を利用して、エンドポイントをいずれかの一致する親エンドポイント ID グループ、関連付けられたエンドポイント ID グループ、さらに親 ID グループに割り当てることができます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次に例を示します。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合は、Cisco-IP-Phone エンドポイント ID グループの下にグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合は、Workstation エンドポイント ID グループの下にグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内のプロファイリングされたエンドポイント ID グループに関連付けられます。
親ポリシー（Parent Policy）	新しいエンドポイント プロファイリング ポリシーに関連付ける、システムで定義されている親プロファイリング ポリシーを選択します。 ルールおよび条件を子に継承できる親プロファイリング ポリシーを選択できます。
関連 CoA タイプ（Associated CoA Type）	エンドポイント プロファイリング ポリシーに関連付ける、次の CoA タイプのいずれかを選択します。 • CoA なし • ポート バウンス • 再認証 • [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されるグローバル設定
ルール（Rules）	エンドポイント プロファイリング ポリシーで定義された 1 つ以上のルールがエンドポイントの一致するプロファイリング ポリシーを決定し、それにより、プロファイルに従ってエンドポイントをグループ化できます。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件が、全体的な分類のためにエンドポイント属性とその値を評価するルールで使用されます。

表 B-4　エンドポイント プロファイリング ポリシーの設定 （続き）

フィールド	使用上のガイドライン
条件（Conditions）	プラス [+] 記号をクリックして条件の固定オーバーレイを展開し、マイナス [-] 記号をクリックするか、または固定オーバーレイの外側をクリックして閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：シスコ事前定義の条件をポリシー要素ライブラリから選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム ディクショナリまたはユーザ定義ディクショナリから属性を選択して、式を定義できます。 次のいずれかをプロファイリング条件に関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件に関連付ける、次の事前定義済み設定のいずれかを選択します。 • [確実度係数が増加（Certainty Factor Increases）]：全体の分類に関してすべての一致するルールに対して追加できる各ルールの確実度値を入力します。 • [ネットワーク スキャン アクションの実行（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Actions）] フィールドで設定された例外アクションをトリガーします。 • [ネットワーク スキャン アクションの実行（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）] フィールドで設定されたネットワーク スキャン アクションをトリガーします。

表 B-4　エンドポイント プロファイリング ポリシーの設定 （続き）

フィールド	使用上のガイドライン
既存の条件をライブラリから選択（Select Existing Condition from Library）	次の操作が可能です。 • ポリシー要素ライブラリで使用できるシスコ事前定義の条件を選択し、AND または OR 演算子を使用して複数の条件を追加します。 • [操作（Action）] アイコンをクリックし、後のステップで次の操作を行います。 – [属性/値の追加（Add Attribute/Value）]：アドホック属性/値のペアを追加できます。 – [条件をライブラリから追加（Add Condition from Library）]：シスコ事前定義の条件を追加できます。 – [複製（Duplicate）]：選択した条件のコピーを作成します。 – [条件をライブラリに追加（Add Condition to Library）]：作成したアドホック属性/値のペアをポリシー要素ライブラリに保存できます。 – [削除（Remove）]：選択した条件を削除します。
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	次の操作が可能です。 • アドホック属性/値のペアを式に追加し、AND または OR 演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックし、後のステップで次の操作を行います。 – [属性/値の追加（Add Attribute/Value）]：アドホック属性/値のペアを追加できます。 – [条件をライブラリから追加（Add Condition from Library）]：シスコ事前定義の条件を追加できます。 – [複製（Duplicate）]：選択した条件のコピーを作成します。 – [条件をライブラリに追加（Add Condition to Library）]：作成したアドホック属性/値のペアをポリシー要素ライブラリに保存できます。 – [削除（Remove）]：選択した条件を削除します。ここでは、AND または OR 演算子を使用できます

ディクショナリ

RADIUS ベンダー ディクショナリ属性の設定

次の表に、RADIUS ベンダーのディクショナリ属性を設定できるようにする RADIUS ベンダーのディクショナリ ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [RADIUS ベンダー（RADIUS Vendors）] です。

表 B-5　RADIUS ベンダー ディクショナリ属性の設定

フィールド	使用上のガイドライン
属性名（Attribute Name）	選択した RADIUS ベンダーのベンダー固有属性名を入力します。
説明（Description）	ベンダー固有属性のオプションの説明を入力します。

表 B-5　RADIUS ベンダー ディクショナリ属性の設定 （続き）

フィールド	使用上のガイドライン
内部名（Internal Name）	内部のデータベースで表されるベンダー固有属性の名前を入力します。
データ タイプ（Data Type）	ベンダー固有属性の次のデータ型のいずれかを選択します。 • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4
MAC を有効にするオプション（Enable MAC option）	MAC アドレスとしての RADIUS 属性の比較を有効にするには、このチェックボックスをオンにします。デフォルトで、RADIUS 属性 Calling-Station-ID に対して、このオプションは有効とマークされ、無効にできません。RADIUS ベンダー ディクショナリ内の別のディクショナリ属性（文字列型）の場合は、このオプションを有効または無効にできます。 このオプションを有効にした場合、認証および許可条件の設定中に、テキスト オプションを選択して比較をクリアな文字列にするか、または MAC アドレスオプションを選択して比較を MAC アドレスにするかを定義できます。
方向（Direction）	RADIUS メッセージに適用するいずれかのオプションを選択します。
ID	ベンダー属性 ID を入力します。有効な範囲は 0 ～ 255 です。
タギングの許可（Allow Tagging）	このチェックボックスをオンにします。
プロファイルでこの属性の複数のインスタンスを許可する（Allow multiple instances of this attribute in a profile）	プロファイルでこの RADIUS ベンダー固有属性の複数のインスタンスが必要な場合は、このチェックボックスをオンにします。

条件（Conditions）

この項では、次のフィールド設定表について説明します。

- 「プロファイラ条件の設定」（P.B-9）
- 「ポスチャ条件の設定」（P.B-10）
- 「時刻と日付の条件の設定」（P.B-18）

プロファイラ条件の設定

次の表に、[プロファイラ条件（Profiler Condition）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）] です。

表 B-6　プロファイラ条件の設定

フィールド	使用上のガイドライン
名前（Name）	プロファイラ条件の名前。
説明（Description）	プロファイラ条件の説明。

表 B-6　プロファイラ条件の設定 （続き）

フィールド	使用上のガイドライン
タイプ（Type）	事前定義済みタイプのいずれかを選択します。
属性名（Attribute Name）	プロファイラ条件が基づく属性を選択します。
演算子（Operator）	演算子を選択します。
属性値（Attribute Value）	選択した属性に値を入力します。事前定義された属性値を含む属性名の場合、このオプションでは事前定義された値を含むドロップダウン リストが表示され、値を選択できます。
システム タイプ（System Type）	プロファイリング条件を次のいずれかのタイプになります。 • シスコ提供：展開時に Cisco ISE によって提供されたプロファイリング条件は、シスコ提供として識別されます。システムでそれらを編集または削除できません。 • 管理者作成：Cisco ISE の管理者として作成したプロファイリング条件は、管理者作成として識別されます。

関連項目

「プロファイラ条件」（P.18-4）

ポスチャ条件の設定

この項では、次のフィールド設定表について説明します。

- 「ファイル条件の設定」（P.B-10）
- 「レジストリ条件の設定」（P.B-12）
- 「アプリケーション条件の設定」（P.B-12）
- 「サービス条件の設定」（P.B-13）
- 「ポスチャ複合条件の設定」（P.B-13）
- 「アンチウイルス複合条件の設定」（P.B-14）
- 「アンチスパイウェア複合条件の設定」（P.B-15）
- 「ディクショナリ単純条件の設定」（P.B-16）
- 「ディクショナリ複合条件の設定」（P.B-17）

ファイル条件の設定

次の表に、[ファイル条件（File condition）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[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）] です。

表 B-7　ファイル条件の設定

フィールド	使用上のガイドライン
名前（Name）	ファイル条件の名前を入力します。
説明（Description）	ファイル条件の説明を入力します。

表 B-7　ファイル条件の設定 （続き）

フィールド	使用上のガイドライン
ファイル パス（File Path）	次の事前定義済み設定のいずれかを選択します。 • **ABSOLUTE_PATH**：ファイルの完全修飾パスでファイルをチェックします。たとえば、C:\<directory>\file name。その他の設定では、ファイル名だけを入力します。 • **SYSTEM_32**：C:\WINDOWS\system32 ディレクトリ内のファイルを調べます。ファイル名を入力します。 • **SYSTEM_DRIVE**：C:\ ドライブ内のファイルを調べます。ファイル名を入力します。 • **SYSTEM_PROGRAMS**：C:\Program Files 内のファイルを調べます。ファイル名を入力します。 • **SYSTEM_ROOT**：Windows システムのルート パスのファイルを調べます。ファイル名を入力します。
ファイルのタイプ（File Type）	次の事前定義済み設定のいずれかを選択します。 • [FileExistence]：システムにファイルが存在するかどうかを調べます。 • [FileDate]：特定のファイル作成日またはファイル変更日を持つファイルがシステムに存在するかどうかを調べます。 • [FileVersion]：特定のバージョンのファイルがシステムに存在するかどうかを調べます。
ファイルのデータ タイプ（File Date Type）	（ファイルのタイプとして **FileDate** を選択した場合のみ使用可能）ファイルのデータ タイプを選択します。
ファイル演算子 / 演算子（File Operator/Operator）	ファイル演算子オプションは、ファイル タイプで選択した設定に応じて異なります。設定を適切に選択します。 **FileExistence** • Exists • DoesNotExist **FileDate** • EarlierThan • LaterThan • EqualTo **FileVersion** • EarlierThan • LaterThan • EqualTo
日付と時刻（Date and Time）	（ファイルのタイプとして **File Date** を選択した場合のみ使用可能）mm/dd/yyyy and hh:mm:ss の形式でクライアント システムの日付と時刻を入力します。
ファイル バージョン（File Version）	（ファイル タイプとして **File Version** を選択した場合のみ使用可能）調べるファイルのバージョンを入力します。
オペレーティング システム（Operating System）	ファイル条件が適用されるオペレーティング システムを選択します。

レジストリ条件の設定

次の表に、[レジストリ条件（Registry Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [レジストリ条件（Registry Conditions）] です。

表 B-8　レジストリ条件の設定

フィールド	使用上のガイドライン
名前（Name）	レジストリ条件の名前を入力します。
説明（Description）	レジストリ条件の説明を入力します。
レジストリのタイプ（Registry Type）	レジストリのタイプとして事前定義された設定のいずれかを選択します。
レジストリ ルート キー（Registry Root Key）	レジストリ ルート キーとして事前定義された設定のいずれかを選択します。
サブ キー（Sub Key）	レジストリ ルート キーで指定されたパスのレジストリ キーを調べるには、バックスラッシュ ("\") を使用せずにサブ キーを入力します。 たとえば、OFTWARE\Symantec\Norton AntiVirus\version は次のパスのキーを調べます。 HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
値の名前（Value Name）	（レジストリのタイプとして **RegistryValue** または **RegistryValueDefault** を選択した場合のみ使用可能）調べるレジストリ キー値の名前を **RegistryValue** に入力します。 これは **RegistryValueDefault** のデフォルト フィールドです。
値のデータ タイプ（Value Data Type）	（レジストリのタイプとして **RegistryValue** または **RegistryValueDefault** を選択した場合のみ使用可能）次のいずれかの設定を選択します。 • **指定なし**：レジストリ キー値があるかどうかを調べます。このオプションは、**RegistryValue** の場合のみ使用できます • **数**：レジストリ キー値の指定した数を調べます • **文字列**：レジストリ キー値の文字列を調べます • **バージョン**：レジストリ キー値のバージョンを調べます
値演算子（Value Operator）	設定を適切に選択します。
値のデータ（Value Data）	（レジストリのタイプとして **RegistryValue** または **RegistryValueDefault** を選択した場合のみ使用可能）[値のデータ タイプ（Value Data Type）] で選択したデータ タイプに従ってレジストリ キーの値を入力します。
オペレーティング システム（Operating System）	レジストリ条件が適用されるオペレーティング システムを選択します。

アプリケーション条件の設定

次の表に、[アプリケーション条件（Application Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [アプリケーション条件（Application Conditions）] です。

表 B-9　アプリケーション条件の設定

フィールド	使用上のガイドライン
名前（Name）	アプリケーション条件の名前を入力します。
説明（Description）	アプリケーション条件の説明を入力します。
プロセス名（Process Name）	調べるアプリケーションの名前を入力します。
アプリケーション演算子（Application Operator）	調べるステータスを選択します。
オペレーティング システム（Operating System）	アプリケーション条件が適用されるオペレーティング システムを選択します。

サービス条件の設定

次の表に、[サービス条件（Service Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [サービス条件（Service Conditions）] です。

表 B-10　サービス条件の設定

フィールド	使用上のガイドライン
名前（Name）	サービス条件の名前を入力します。
説明（Description）	サービス条件の説明を入力します。
Service Name	調べるサービスの名前を入力します。
サービス演算子（Service Operator）	調べるステータスを選択します。
オペレーティング システム（Operating System）	サービス条件が適用されるオペレーティング システムを選択します。

ポスチャ複合条件の設定

次の表に、[複合条件（Compound Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[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）] です。

表 B-11　ポスチャ複合条件の設定

フィールド	使用上のガイドライン
名前（Name）	作成する複合条件の名前を入力します。
説明（Description）	作成する複合条件の説明を入力します。
オペレーティング システム（Operating System）	1 つ以上の Windows オペレーティング システムを選択します。これにより、条件が適用される Windows オペレーティング システムを関連付けることができます。
カッコ（）（Parentheses ( )）	次の単純条件のタイプから 2 つの単純条件を組み合わせるには、カッコをクリックします。ファイル、レジストリ、アプリケーション、およびサービス条件。

表 B-11　ポスチャ複合条件の設定 （続き）

フィールド	使用上のガイドライン
([&])：AND 演算子（AND 演算子として "&" を使用、引用符なし）	複合条件内には AND 演算子オペレータ（アンパサンド（&））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
([|])：OR 演算子（OR 演算子として "|" を使用、引用符なし）	複合条件内には OR 演算子（縦線（|））を使用できます。たとえば、**Condition1	Condition2** と入力します。
([!])：NOT 演算子（NOT 演算子として "!" を使用、引用符なし）	複合条件内には NOT 演算子（感嘆符（!））を使用できます。たとえば、**Condition1 & (!Condition2)** と入力します。
単純条件	次のタイプの単純条件のリストから選択します。ファイル、レジストリ、アプリケーション、サービス条件。 オブジェクト セレクタからもファイル、レジストリ、アプリケーション、およびサービス条件の単純条件を作成できます。 ファイル、レジストリ、アプリケーション、およびサービス条件の単純条件を作成するには、[操作（Action）] ボタンのクイック ピッカー（下矢印）をクリックします。

アンチウイルス複合条件の設定

次の表に、[AV 複合条件（AV Compound Conditions）] のページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [AV 複合条件（AV Compound Conditions）] です。

表 B-12　アンチウイルス複合条件の設定

フィールド	使用上のガイドライン
名前（Name）	作成するアンチウイルス複合条件の名前を入力します。
説明（Description）	作成するアンチウイルス複合条件の説明を入力します。
オペレーティング システム（Operating System）	オペレーティング システムを選択して、クライアント上のアンチウイルス プログラムのインストールを調べるか、または条件が適用される最新のアンチウイルス定義ファイルの更新を調べます。
ベンダー（Vendor）	ドロップダウン リストからベンダー選択します。ベンダーを選択すると、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されるアンチウイルス製品およびバージョンが取得されます。
チェック タイプ（Check Type）	クライアント上でインストールを調べるか、または最新の定義ファイルの更新を調べるかを選択します。
インストール（Installation）	クライアント上のアンチウイルス プログラムのインストールのみ調べることを選択します。
定義（Definition）	クライアント上のアンチウイルス製品の最新の定義ファイルの更新のみ調べることを選択します。
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）（それ以外の場合は、最新の定義ファイルの日付に対してチェックします）。	（定義チェック タイプを選択した場合のみ使用可能）Cisco ISE のポスチャ更新の結果として使用可能な場合、最新のアンチウイルス定義ファイルのバージョンに対して、クライアント上のアンチウイルス定義ファイルのバージョンをチェックすることを選択します。それ以外の場合は、このオプションでは、Cisco ISE の最新の定義ファイルの日付に対して、クライアント上の定義ファイルの日付をチェックできます。

表 B-12　アンチウイルス複合条件の設定 （続き）

フィールド	使用上のガイドライン
ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)）	（定義チェック タイプを選択した場合のみ使用可能）アンチウイルス定義ファイルのバージョンおよびクライアント上の最新のアンチウイルス定義ファイルの日付をチェックすることを選択します。最新の定義ファイルの日付は、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数より古くなることはできません。 オフの場合、Cisco ISE では、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してアンチウイルス定義ファイルのバージョンのみをチェックすることができます。
より古い日数（days older than）	クライアント上の最新のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付より、古くなることができる日数を定義します。デフォルト値は 0 です。
最新のファイルの日付（latest file date）	[より古い日数（days older than）] フィールドで定義した日数だけ古い可能性がある、クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。 日数をデフォルト値（0）に設定する場合は、クライアント上のアンチウイルス定義ファイルの日付は、製品の最新のアンチウイルス定義ファイルの日付より古くなってはいけません。
現在のシステム日付（current system date）	[より古い日数（days older than）] フィールドで定義した日数だけ古い可能性がある、クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。 日数をデフォルト値（0）に設定する場合は、クライアント上のアンチウイルス定義ファイルの日付は、現在のシステム日付より古くなってはいけません。
選択したベンダーの製品（Products for Selected Vendor）	テーブルからアンチウイルス製品を選択します。[新しいアンチウイルス複合条件（New Anti-virus Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチウイルス製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチウイルス プログラムのインストールを確認したり、最新のアンチウイルス定義ファイルの日付および最新バージョンを確認したりできます。

アンチスパイウェア複合条件の設定

次の表に、[AS 複合条件（AS Compound Conditions）] のページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [AS 複合条件（AS Compound Conditions）] です。

表 B-13　アンチスパイウェア複合条件の設定

フィールド	使用上のガイドライン
名前（Name）	作成するアンチスパイウェア複合条件の名前を入力します。
説明（Description）	作成するアンチスパイウェア複合条件の説明を入力します。

表 B-13　アンチスパイウェア複合条件の設定 （続き）

フィールド	使用上のガイドライン
オペレーティング システム（Operating System）	オペレーティング システムを選択すると、クライアント上のアンチスパイウェア プログラムのインストールを調べるか、または条件が適用される最新のアンチスパイウェア定義ファイルの更新を調べることができます。
ベンダー（Vendor）	ドロップダウン リストからベンダー選択します。ベンダーを選択すると、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されるアンチスパイウェア製品およびバージョンが取得されます。
チェック タイプ（Check Type）	クライアント上でインストールを調べるか、または最新の定義ファイルの更新を調べるか、というタイプを選択するかどうかを選択します。
インストール（Installation）	クライアント上のアンチスパイウェア プログラムのインストールのみ調べるかどうかを選択します。
定義（Definition）	クライアント上のアンチスパイウェア製品の最新の定義ファイルの更新のみ調べるかどうかを選択します。
ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)）	このチェックボックスは、アンチスパイウェア定義チェック タイプを作成するときはオンにし、アンチスパイウェア インストール チェック タイプを作成するときはオフにします。 オンにすると、その選択により、クライアント上のアンチスパイウェア定義ファイルのバージョンおよび最新のアンチスパイウェア定義ファイルの日付をチェックできます。最新の定義ファイルの日付は、現在のシステム日付から、[より古い日数（days older than）] フィールドで定義した日数より古くなることはできません。 オフの場合、その選択により、[ウイルス定義ファイルをにすることを許可する（Allow virus definition file to be）] チェックボックスがオフのときに、アンチスパイウェア定義ファイルのバージョンのみをチェックすることができます。
より古い日数（days older than）	クライアント上の最新のアンチスパイウェア定義ファイルの日付が、現在のシステム日付より、古くなることができる日数を定義します。デフォルト値は 0 です。
現在のシステム日付（current system date）	[より古い日数（days older than）] フィールドで定義した日数だけ古い可能性がある、クライアント上のアンチスパイウェア定義ファイルの日付をチェックすることを選択します。 日数をデフォルト値（0）に設定する場合は、クライアント上のアンチスパイウェア定義ファイルの日付は、現在のシステム日付より古くなってはいけません。
選択したベンダーの製品（Products for Selected Vendor）	テーブルからアンチスパイウェア製品を選択します。[新しいアンチスパイウェア複合条件（New Anti-spyware Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチスパイウェア製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチスパイウェア プログラムのインストールを確認したり、最新のアンチスパイウェア定義ファイルの日付および最新バージョンを確認したりできます。

ディクショナリ単純条件の設定

次の表に、[ディクショナリ単純条件（Dictionary Simple Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ単純条件（Dictionary Simple Conditions）] です。

表 B-14　ディクショナリ単純条件の設定

フィールド	使用上のガイドライン
名前（Name）	作成するディクショナリ単純条件の名前を入力します。
説明（Description）	作成するディクショナリ単純条件の説明を入力します。
属性（Attribute）	ディクショナリから属性を選択します。
演算子（Operator）	選択した属性に値を関連付ける演算子を選択します。
値（Value）	ディクショナリ属性に関連づける値を入力するか、またはドロップダウン リストから事前定義済みの値を選択します。

ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] のページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ複合条件（Dictionary Compound Conditions）] です。

表 B-15　ディクショナリ複合条件の設定

フィールド	使用上のガイドライン
名前（Name）	作成するディクショナリ複合条件の名前を入力します。
説明（Description）	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（Select Existing Condition from Library）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（Condition Name）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（Expression）	[条件名（Condition Name）] ドロップダウン リストでの選択に基づいて式が更新されます。
AND または OR 演算子（AND or OR operator）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）] アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • 条件をライブラリから追加（Add Condition from Library） • 削除（Delete）
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	さまざまなシステム ディクショナリまたはユーザ定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（Condition Name）	すでに作成したディクショナリ単純条件を選択します。
式（Expression）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子（Operator）	属性に値を関連付ける演算子を選択します。
値（Value）	ディクショナリ属性に関連づける値を入力するか、またはドロップダウン リストから値を選択します。

関連項目

「エンドポイント プロファイリング ポリシーの作成」（P.21-23）

時刻と日付の条件の設定

次の表に、[時刻と日付の条件（Time and Date Conditions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [共通（Common）] > [時刻と日付（Time and Date）] です。

表 B-16　時刻と日付の条件の設定

フィールド	使用上のガイドライン
条件名（Condition Name）	時刻と日付の条件の名前を入力します。
説明（Description）	時刻と日付の条件の説明を入力します。
標準設定（Standard Settings）	
終日（All Day）	（デフォルト）日全体に対して設定します。
特定の時間（Specific Hours）	時、分、および AM/PM を設定して時間範囲を設定します。
毎日（Every Day）	（デフォルト）毎日に対して設定します。
特定の曜日（Specific Days）	1 つ以上の特定の曜日を設定します。
開始日と終了日なし（No Start and End Dates）	（デフォルト）開始または終了日なしで設定します。
特定の日付範囲（Specific Date Range）	月、日、および年を設定して日付範囲を設定します。
特定の日付（Specific Date）	特定の月、日、年を設定します。
例外（Exceptions）	
時間範囲（Time Range）	時、分、および AM/PM を設定して時間範囲を設定します。
曜日（Week Days）	1 つ以上の特定の曜日を設定します。
日付の範囲（Date Range）	次の 2 つのオプションについて選択します。 • [特定の日付範囲（Specific Date Range）]：月、日、および年で特定の日付範囲を設定するために使用できるドロップダウン リストが提供されます。 • [特定の日付（Specific Date）]：特定の月、日、および年を設定するために使用できるドロップダウン リストが提供されます。

関連項目

「時刻と日付の条件の作成」（P.18-8）

結果

ここでは、次の内容について説明します。

- 「許可されるプロトコル サービスの設定」（P.B-19）
- 「PAC オプション」（P.B-23）

- 「許可プロファイルの設定」（P.B-25）
- 「プロファイリング例外アクションの設定」（P.B-27）
- 「ファイル修復」（P.B-28）
- 「リンク修復」（P.B-28）
- 「アンチウイルス修復」（P.B-29）
- 「アンチスパイウェア修復」（P.B-30）
- 「プログラム起動修復」（P.B-30）
- 「Windows Update 修復」（P.B-31）
- 「Windows Server Update Service 修復」（P.B-32）
- 「クライアントのポスチャ要件」（P.B-33）

許可されるプロトコル サービスの設定

次の表に、認証中に使用するプロトコルを設定できるようにする [許可されるプロトコル サービス（Allowed Protocols Services）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されたプロトコル（Allowed Protocols）] です。

表 B-17　許可されるプロトコル サービスの設定

フィールド	使用上のガイドライン
許可されたプロトコル（Allowed Protocols）	
ホスト ルックアップの処理（Process Host Lookup）	たとえば RADIUS Service-Type が 10 の場合に [ホスト ルックアップ（Host Lookup）] フィールドを処理し、RADIUS Calling-Station-ID 属性の System UserName 属性を使用するように ISE を設定するには、このチェックボックスをにオンにします。ISE でホスト ルックアップ要求を無視し、認証に system UserName 属性の元の値を使用するには、このチェックボックスをオフにします。オフにすると、メッセージ処理はプロトコル（たとえば PAP）に従って行われます。
認証プロトコル（Authentication Protocols）	
PAP/ASCII を許可（Allow PAP/ASCII）	[PAP をホスト ルックアップとして検出する（Detect PAP as Host Lookup）] をオンにして、このタイプの要求を PAP ではなくホスト ルックアップ要求として検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。 このオプションによって、PAP/ASCII が有効になります。PAP は、平文パスワード（つまり暗号化されていないパスワード）を使用する最もセキュリティ レベルの低い認証プロトコルです。
CHAP を許可（Allow CHAP）	[CHAP をホスト ルックアップとして検出する（Detect PAP as Host Lookup）] をオンにして、このタイプの要求をホスト ルックアップ要求として検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。このオプションを有効にすると、ISE により非シスコのデバイスで MAB が許可されます。 このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ / レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
MS-CHAPv1 を許可（Allow MS-CHAPv1）	MS-CHAPv1 を有効にするには、このチェック ボックスをオンにします。
MS-CHAPv2 を許可（Allow MS-CHAPv2）	MS-CHAPv2 を有効にするには、このチェック ボックスをオンにします。

表 B-17　許可されるプロトコル サービスの設定 （続き）

フィールド	使用上のガイドライン
EAP-MD5 を許可（Allow EAP-MD5）	EAP ベースの MD5 ハッシュ認証を有効にするには、このチェック ボックスをオンにします。 [EAP-MD5 を許可（Allow EAP-MD5）] チェックボックスをオンにすると、[EAP-MD5 をホスト ルックアップとして検出する（Detect EAP-MD5 as Host Lookup）] チェックボックスをオンにして、このタイプの要求を EAP-MD5 ではなくホスト ルックアップ要求として検出するように Cisco ISE を設定できます。
EAP-TLS を許可（Allow EAP-TLS）	EAP-TLS 認証プロトコルを有効にする場合、および EAP-TLS 設定値を設定する場合は、このチェック ボックスをオンにします。エンドユーザ クライアントからの EAP Identity 応答で提示されたユーザ ID を Cisco ISE が確認する方法を指定できます。ユーザ ID は、エンドユーザ クライアントによって提示された証明書の情報に照らして確認されます。この比較は、Cisco ISE とエンドユーザ クライアントとの間に EAP-TLS トンネルが確立されたあとに行われます。 **（注）** EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS 認証が行われるのは、証明書の設定に必要な手順を完了した場合にかぎられます。証明書の詳細については、第 8 章「証明書の管理」を参照してください。
LEAP を許可（Allow LEAP）	Lightweight Extensible Authentication Protocol（LEAP）認証を有効にするには、このチェック ボックスをオンにします。

表 B-17　許可されるプロトコル サービスの設定 （続き）

フィールド	使用上のガイドライン
PEAP を許可（Allow PEAP）	PEAP 認証プロトコルおよび PEAP 設定値を有効にする場合は、このチェックボックスをオンにします。デフォルトの内部方式は、MS-CHAPv2 です。 [PEAP を許可（Allow PEAP）] チェックボックスをオンにすると、次の PEAP 内部方式を設定できます。 • [EAP-MS-CHAPv2 を許可（Allow EAP-MS-CHAPv2）] : 内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。 – [パスワード変更の許可（Allow Password Change）] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 – [再試行（Retry Attempts）] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効値は 1 ～ 3 です。 • [EAP-GTC を許可（Allow EAP-GTC）] : 内部方式として EAP-GTC を使用する場合は、このチェックボックスをオンにします。 – [パスワード変更の許可（Allow Password Change）] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 – [再試行（Retry Attempts）] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効値は 1 ～ 3 です。 • [EAP-TLS を許可（Allow EAP-TLS）] : 内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。 • [レガシー クライアントにのみ PEAPv0 を許可（Allow PEAPv0 only for legacy clients）] : PEAP サプリカントが PEAPv0 を使用してネゴシエーションできるようにするには、このチェックボックスをオンにします。一部のレガシー クライアントは PEAPv1 プロトコル規格に準拠しません。そのような EAP カンバセーションがドロップされないようにするには、このチェックボックスをオンにします。

表 B-17　許可されるプロトコル サービスの設定 （続き）

フィールド	使用上のガイドライン
EAP-FAST を許可（Allow EAP-FAST）	EAP-FAST 認証プロトコルおよび EAP-FAST 設定値を有効にする場合は、このチェックボックスをオンにします。EAP-FAST プロトコルは、同じサーバ上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MS-CHAPv2 です。 EAP-FAST での Protected Access Credentials の使用については、「PAC オプション」（P.B-23）を参照してください。EAP チェーンの詳細は、「認証プロトコルとして EAP-FAST を使用するためのガイドライン」（P.19-12）を参照してください。 [EAP-FAST を許可（Allow EAP-FAST）] チェックボックスをオンにすると、EAP-FAST を内部方式として設定できます。 • EAP-MS-CHAPv2 を許可（Allow EAP-MS-CHAPv2） – [パスワード変更の許可（Allow Password Change）] : Cisco ISE で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合は、このチェックボックスをオンにします。 – [再試行（Retry Attempts）] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • EAP-GTC を許可（Allow EAP-GTC） – [パスワード変更の許可（Allow Password Change）] : Cisco ISE で EAP-FAST のフェーズ 0 とフェーズ 2 でのパスワード変更をサポートする場合は、このチェックボックスをオンにします。 – [再試行（Retry Attempts）] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 1 ～ 3 です。 • [PAC の使用（Use PACs）] : EAP-FAST クライアントに認可 PAC[1] をプロビジョニングするように Cisco ISE を設定する場合にこのオプションを選択します。追加の PAC オプションが表示されます。 • [PAC を使用しない（Don’t use PACs）] : トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように Cisco ISE を設定する場合にこのオプションを選択します。PAC のすべての要求は無視され、Cisco ISE は PAC を含まない Success-TLV で応答します。 このオプションを選択すると、マシン認証を実行するように Cisco ISE を設定できます。

1. PAC = Protected Access Credential。

関連項目

「ネットワーク アクセス用の許可されるプロトコルの定義」（P.19-15）

PAC オプション

次の表に、[許可されるプロトコル サービス リスト（Allowed Protocols Services List）] ページで [PAC の使用（Use PACs）] を選択した後のフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されたプロトコル（Allowed Protocols）] です。

表 B-18　PAC オプション（PAC Options）

フィールド	使用上のガイドライン
PAC を使用（Use PAC）	• [トンネル PAC の存続可能時間（Tunnel PAC Time To Live）] : 存続可能時間（TTL）の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは、90 日です。値の範囲は 1 ～ 1825 日です。 • [プロアクティブ PAC 更新の条件 : <n%> の PAC TTL が残っている場合（Proactive PAC Update When: <n%> of PAC TTL is Left）] : Update 値により、クライアントに有効な PAC が保持されます。Cisco ISE は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。update 値は、TTL の残り時間のパーセンテージです デフォルト値は 90 % です。 • [匿名インバンド PAC プロビジョニングを許可（Allow Anonymous In-band PAC Provisioning）] : Cisco ISE でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントに PAC をプロビジョニングする場合にこのチェックボックスをオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。匿名 PAC プロビジョニングをイネーブルにするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。 • [認証付きインバンド PAC プロビジョニング（Allow Authenticated In-band PAC Provisioning）] : Cisco ISE は SSL サーバ側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバ証明書および信頼できるルート CA が Cisco ISE にインストールされている必要があります。 このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すように Cisco ISE を設定できます。 – [認証されたプロビジョニングの後にサーバから Access-Accept を返す（Server Returns Access Accept After Authenticated Provisioning）] : 認証された PAC プロビジョニングの後に Cisco ISE から access-accept パッケージを返す場合にこのチェックボックスをオンにします。 • [マシン認証を許可（Allow Machine Authentication）] : Cisco ISE でエンドユーザ クライアントにマシン PAC をプロビジョニングし、（マシン クレデンシャルを持たないエンドユーザ クライアントに対して）マシン認証を実行する場合にこのチェックボックスをオンにします。マシン PAC は、要求（インバンド）によって、または管理者（アウトオブバンド）によって、クライアントにプロビジョニングできます。Cisco ISE がエンドユーザ クライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、Cisco ISE 外部 ID ソースで確認されます。マシン認証の外部 ID ソースとして Cisco ISE によってサポートされるのは、Active Directory だけです。その詳細が正しいことが確認されると、その後の認証は実行されません。 このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。Cisco ISE は、期限切れのマシン PAC を受け取ると、（エンドユーザ クライアントからの新規マシン PAC 要求を待たずに）エンドユーザ クライアントに新規マシン PAC を自動的に再プロビジョニングします。 • [ステートレス セッション再開の有効化（Enable Stateless Session Resume）] : Cisco ISE で EAP-FAST クライアントに認可 PAC をプロビジョニングし、常に EAP-FAST のフェーズ 2 を実行する場合に、このチェックボックスをオンにします（デフォルトはオン）。 次のような場合にこのチェックボックスをオフにします。 – Cisco ISE が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 – EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザ認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。Cisco ISE は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。 • [優先 EAP プロトコル（Preferred EAP Protocol）] : 優先 EAP プロトコルを EAP-FAST、PEAP、LEAP、EAP-TLS、および EAP-MD5 から選択する場合はこのチェックボックスをオンにします。デフォルトでは、LEAP は、このフィールドを有効にしない場合に使用する優先プロトコルです。

関連項目

「ネットワーク アクセス用の許可されるプロトコルの定義」（P.19-15）

許可プロファイルの設定

次の表に、[標準許可プロファイル（Standard Authorization Profiles）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] です。

表 B-19　許可プロファイルの設定

フィールド	使用上のガイドライン
名前（Name）	新しい許可プロファイルを識別する名前を入力します。
説明（Description）	許可プロファイルの説明を入力します。
アクセス タイプ（Access Type）	アクセス タイプ オプション（[ACCESS_ACCEPT] または [ACCESS_REJECT]）を選択します。
サービス テンプレート（Service Template）	Cisco ISE で SAnet 対応デバイスから接続しているセッションをサポートできるようにする場合にこのチェックボックスをオンにします。ISE は、サービス テンプレートを、「サービス テンプレート」互換としてマークする特別なフラグを含む許可プロファイルとして実行します。このようにすると、認可プロファイルでもあるサービス テンプレートを 1 つのポリシーで使用して、SAnet および非 SAnet デバイスとの接続をサポートできます。
共通タスク（Common Tasks）	
DACL 名（DACL Name）	チェックボックスをオンにし、使用可能な既存のダウンロード可能 ACL オプションを選択します（たとえば、Cisco ISE には、ドロップダウン リストに **PERMIT_ALL_TRAFFIC** または **DENY_ALL_TRAFFIC** の 2 つのデフォルト値が用意されています）。リストには、ローカル データベースの、現在のすべての DACL が含まれています。
VLAN	チェックボックスをオンにし、作成している新しい許可プロファイルに関連付ける仮想 LAN（VLAN）ID を識別する属性値を入力します（VLAN ID には整数値と文字列値の両方がサポートされます）。このエントリの形式は、*Tunnel-Private-Group-ID:VLANnumber* です。 **（注）** VLAN ID を選択しないと、Cisco ISE は、デフォルト値である VLAN ID = 1 を使用します。たとえば、VLAN 番号として 123 とのみ入力した場合、[属性詳細（Attributes Details）] ペインは次の値を反映します。Tunnel-Private-Group-ID = 1:123。
音声ドメイン権限（Voice Domain Permission）	チェックボックスをオンにして「cisco-av-pair」のベンダー固有属性（VSA）を有効にし、「device-traffic-class=voice」の値と関連付けます。複数ドメインの許可モードでは、ネットワーク スイッチがこの VSA を受信した場合、エンドポイントは、許可後に音声ドメインに配置されます。
ポスチャ検出（Posture Discovery）	チェックボックスをオンにして Cisco ISE のポスチャ検出に使用されるリダイレクト プロセスを有効にし、この許可プロファイルに関連付けるデバイスの ACL を入力します。たとえば、入力した値が acl119 の場合、これは [属性詳細（Attributes Details）] ペインで cisco-av-pair = url-redirect-acl = acl119 として反映されます。[属性詳細（Attributes Details）] ペインには、cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cpp も表示されます。

表 B-19　許可プロファイルの設定 （続き）

フィールド	使用上のガイドライン
中央集中 Web 認証（Centralized Web Authentication）	チェックボックスをオンにして、ポスチャ検出と似ているがゲスト ユーザのアクセス要求を Cisco ISE のゲスト サーバにリダイレクトするリダイレクト プロセスを有効にします。この許可プロファイルに関連付けるデバイスの ACL を入力し、redirect オプションとして [デフォルト（Default）] または [手動（Manual）] を選択します。たとえば、入力した値が acl-999 の場合、これは [属性詳細（Attributes Details）] ペインで cisco-av-pair = url-redirect-acl = acl-99 として反映されます。[属性詳細（Attributes Details）] ペインには、cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cwa も表示されます。 ユーザをリダイレクトする正確な IP アドレスまたはホスト名を指定するには、[スタティック IP/ホスト名（Static IP/Host Name）] チェックボックスをオンにします。このチェックボックスがオフの場合、ユーザはこの要求を受信したポリシー サービス ノードの FQDN にリダイレクトされます。
Web リダイレクト（Web Redirection）（CWA、RWA、MDM、NSP、CPP）	
Auto SmartPort	チェックボックスをオンにして Auto SmartPort 機能を有効にし、対応するイベント名の値をテキスト ボックスに入力します。これにより、VSA cisco-av-pair が有効になり、このオプションの値が「auto-smart-port=event_name」になります。選択は [属性詳細（Attributes Details）] ペインに反映されます。
フィルタ ID（Filter-ID）	チェックボックスをオンにして、テキスト ボックスで定義した ACL 名（これには自動的に「.in」が付加されます）を送信する RADIUS フィルタ属性を有効にします。選択は [属性詳細（Attributes Details）] ペインに反映されます。
再認証（Reauthentication）	チェックボックスをオンにし、再認証中に接続を維持するために値を秒単位で入力します。[タイマー（Timer）] ドロップダウン リストから属性値を選択することもできます。デフォルト（値 0）または [RADIUS 要求（RADIUS-Request）]（値 1）を使用すること選択して、再認証中に接続を維持することを選択します。これを [RADIUS 要求（RADIUS-Request）] 値に設定すると、再認証プロセス中に接続が維持されます。
MACSec ポリシー（MACSec Policy）	チェックボックスをオンにして、MACSec 対応クライアントが Cisco ISE に接続したときに必ず MACSec 暗号化ポリシーを有効にし、次の 3 つのオプションのいずれかを選択します。[must-secure]、[should-secure]、または [must-not-secure]。たとえば、選択肢は [属性詳細（Attributes Details）] ペインに cisco-av-pair = linksec-policy=must-secure として反映されます。
NEAT	チェックボックスをオンにして、ネットワーク間の ID 認識を拡張する機能であるネットワーク エッジ アクセス トポロジ（NEAT）を有効にします。このチェックボックスをオンにすると、[属性詳細（Attributes Details）] ペインに、cisco-av-pair = device-traffic-class=switch という値が表示されます。
Web 認証（ローカル Web 認証）（Web Authentication (Local Web Auth)）	チェックボックスをオンにしてこの許可プロファイルのローカル Web 認証を有効にします。この値では、Cisco ISE が DACL とともに VSA を送信することによって Web 認証の許可をスイッチが認識できます。VSA は cisco-av-pair = priv-lvl=15 で、これは [属性詳細（Attributes Details）] ペインで反映されます。
ワイヤレス LAN コントローラ（WLC）（Wireless LAN Controller (WLC)）	チェックボックスをオンにし、テキスト フィールドに ACL 名を入力します。この値は、必須の [Airespace VSA] で使用され、ローカルで定義された ACL の WLC 上の接続への追加を許可します。たとえば、rsa-1188 と入力した場合、これは [属性詳細（Attributes Details）] ペインに Airespace-ACL-Name = rsa-1188 として反映されます。
ASA VPN	チェックボックスをオンにして、適応型セキュリティ アプライアンス（ASA）VPN グループ ポリシーを有効にします。[属性（Attribute）] リストから値を選択してこの設定を行います。

表 B-19　許可プロファイルの設定 （続き）

フィールド	使用上のガイドライン
高度な属性設定（Advanced Attributes Settings）	
ディクショナリ（Dictionaries）	下矢印アイコンをクリックし、[ディクショナリ（Dictionaries）] ウィンドウに選択可能なオプションを表示します。目的のディクショナリおよび属性をクリックして選択し、最初のフィールドで設定します。
属性値（Attribute Values）	下矢印アイコンをクリックし、[属性値（Attribute Values）] ウィンドウに選択可能なオプションを表示します。2 番めのフィールドに目的の属性グループおよび属性値をクリックして選択します。この値は、最初のフィールドで選択した値と一致します。設定する [高度な属性（Advanced Attributes）] 設定が [属性詳細（Attribute Details）] パネルに表示されます。 **（注）** [属性詳細（Attributes Details）] ペインに表示された読み取り専用値を変更または削除するには、対応する [共通タスク（Common Tasks）] フィールドまたは [高度な属性設定（Advanced Attributes Settings）] ペインの [属性値（Attribute Values）] テキストボックスで選択した属性でこれらの値を変更または削除する必要があります。
属性詳細（Attributes Details）	このペインは、[共通タスク（Common Tasks）] および [高度な属性（Advanced Attributes）] に設定した設定済みの属性値を表示します。 **（注）** [属性詳細（Attributes Details）] ペインに表示される値は読み取り専用で、このペインでは編集または削除できません。

関連項目

「新しい標準許可プロファイル の権限の設定」（P.20-11）

プロファイリング例外アクションの設定

次の表に、[新規プロファイラ例外条件（New Profiler Exception Action）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）] です。

表 B-20　例外アクションの作成

フィールド	使用上のガイドライン
名前（Name）	作成する例外のアクションの名前を入力します。
説明（Description）	作成する例外のアクションの説明を入力します。
CoA を適用するための CoA アクション（CoA Action to enforce CoA）	CoA を適用するには、[CoA アクション（CoA Action）] チェックボックスをオンにします。 エンドポイント プロファイリング ポリシーで例外アクションを関連付けて CoA を適用する場合は、Cisco ISE で CoA をグローバルに設定する必要があります。これは、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で実行できます。 詳細については、「COA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定」（P.21-15）を参照してください。

表 B-20　例外アクションの作成 （続き）

フィールド	使用上のガイドライン
ポリシー割り当て（Policy Assignment）	Cisco ISE で設定されているエンドポイント プロファイリング ポリシーを表示する [ポリシー割り当て（Policy Assignment）] ドロップダウン リストをクリックして、例外アクションがトリガーされたときに一致する値に関係なくエンドポイントをプロファイリングするためのプロファイリング ポリシーを選択します。
システム タイプ（System Type）	例外アクションは次のいずれかのタイプになります。 • シスコ提供：AuthorizationChange、EndpointDelete および FirstTimeProfile が含まれます • 管理者作成：あります。Cisco ISE の管理者として作成するものが含まれます

関連項目

「例外アクションの作成」（P.21-31）

ファイル修復

次の表に、[ファイル修復（File Remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [ファイル修復（File Remediations）] です。

表 B-21　ファイル修復

フィールド	使用上のガイドライン
ファイル修復名（File Remediation Name）	ファイル修復の名前を入力します。作成して保存した後は、ファイル修復の名前は編集できません。
ファイル修復の説明（File Remediation Description）	ファイル修復の説明を入力します。
バージョン（Version）	ファイル バージョンを入力します。
アップロードするファイル（File to upload）	[参照（Browse）] をクリックして、Cisco ISE サーバにアップロードするファイル名を検索します。これは、ファイル修復アクションがトリガーされたときにクライアントにダウンロードされるファイルです。

リンク修復

次の表に、[リンク修復（Link Remediation）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [リンク修復（Link Remediation）] です。

表 B-22　リンク修復

フィールド	使用上のガイドライン
リンク修復名（Link Remediation Name）	リンク修復の名前を入力します。
リンク修復の説明（Link Remediation Description）	リンク修復の説明を入力します。
修復タイプ（Remediation Type）	次のいずれかを選択します。 • **自動**：選択した場合、間隔および再試行回数の値を入力する必要があります。 • **手動**：選択されている場合、[再試行回数（Retry Count）] および [間隔（Interval）] フィールドは編集できません。
再試行回数（Retry Count）	クライアントがリンクからの修復を試行できる試行回数を入力します。
間隔（秒単位）（Interval (in seconds)）	クライアントが以前の試行後にリンクからの修復を試行できる時間間隔を秒単位で入力します。
URL	修復のページまたはリソースに案内する有効な URL を入力します。

アンチウイルス修復

次の表に、[AV 修復（AV Remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [AV 修復（AV Remediations）] です。

表 B-23　アンチウイルス修復

フィールド	使用上のガイドライン
名前（Name）	アンチウイルス修復の名前を入力します。
説明（Description）	アンチウイルス修復の説明を入力します。
修復タイプ（Remediation Type）	次のいずれかを選択します。 • **自動**：選択した場合、間隔および再試行回数の値を入力する必要があります。 • **手動**：選択されている場合、[再試行回数（Retry Count）] および [間隔（Interval）] フィールドは編集できません。
間隔（秒単位）（Interval (in seconds)）	クライアントが以前の試行後に修復を試行できる時間間隔を秒単位で入力します。
再試行回数（Retry Count）	クライアントがアンチウイルス定義の更新を試行できる試行回数を入力します。
オペレーティング システム（Operating System）	次のいずれかを選択します。 • **Windows** • **Macintosh**：修復タイプを選択した場合、[再試行回数（Retry Count）] および [間隔（Interval）] フィールドは編集できません。
AV のベンダー名（AV Vendor Name）	アンチウイルス ベンダーを選択します。

アンチスパイウェア修復

次の表に、[AS 修復（AS Remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [AS 修復（AS Remediations）] です。

表 B-24　アンチスパイウェア修復

フィールド	使用上のガイドライン
名前（Name）	アンチスパイウェア修復の名前を入力します。
説明（Description）	アンチスパイウェア修復の説明を入力します。
修復タイプ（Remediation Type）	次のいずれかを選択します。 • **自動**：選択した場合、間隔および再試行回数の値を入力する必要があります。 • **手動**：選択されている場合、[再試行回数（Retry Count）] および [間隔（Interval）] フィールドは編集できません。
間隔（秒単位）（Interval (in seconds)）	クライアントが以前の試行後に修復を試行できる時間間隔を秒単位で入力します。
再試行回数（Retry Count）	クライアントがアンチスパイウェア定義の更新を試行できる試行回数を入力します。
オペレーティング システム（Operating System）	次のいずれかを選択します。 • **Windows** • **Macintosh**：修復タイプを選択した場合、[再試行回数（Retry Count）] および [間隔（Interval）] フィールドは編集できません。
AS のベンダー名（AV Vendor Name）	アンチスパイウェア ベンダーを選択します。

プログラム起動修復

次の表に、[プログラム起動修復（Launch Program Remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [プログラム起動修復（Launch Program Remediations）] です。

表 B-25　プログラム起動修復

フィールド	使用上のガイドライン
名前（Name）	プログラム起動修復の名前を入力します。
説明（Description）	作成するプログラム起動修復の説明を入力します。
修復タイプ（Remediation Type）	次のいずれかを選択します。 • **自動**：選択した場合、[再試行回数（Retry Count）] および [間隔（Interval）] オプションに入力する必要があります。 • **手動**：選択されている場合、[間隔（Interval）] および [再試行回数（Retry Count）] フィールドは編集できません。
間隔（秒単位）（Interval (in seconds)）	クライアントが以前の試行後に修復を試行できる時間間隔を秒単位で入力します。

表 B-25　プログラム起動修復 （続き）

フィールド	使用上のガイドライン
再試行回数（Retry Count）	クライアントが必要なプログラムの起動を試行できる試行回数を入力します。
プログラムのインストール パス（Program Installation Path）	ドロップダウン リストから、修正プログラムをインストールする必要があるパスを選択します。 • **ABSOLUTE_PATH**：修復プログラムがファイルの完全修飾パスにインストールされます。たとえば、C:\<directory>\ • **SYSTEM_32**：修復プログラムは C:\WINDOWS\system32 ディレクトリにインストールされます。 • **SYSTEM_DRIVE**：修復プログラムは C:\ ドライブにインストールされます。 • **SYSTEM_PROGRAMS**：修復プログラムは C:\Program Files にインストールされます。 • **SYSTEM_ROOT**：修復プログラムは、Windows システムのルート パスにインストールされます。
プログラム実行ファイル（Program Executable）	修復プログラム実行ファイルまたはインストール ファイルの名前を入力します。
プログラム パラメータ（Program Parameters）	修復プログラムに必要なパラメータを入力します。
既存のプログラム（Existing Programs）	既存のプログラム テーブルには、修復プログラムのインストール パス、名前、およびパラメータ（ある場合）が表示されます。 • [追加（Add）] をクリックして、[既存のプログラム（Existing Programs）] リストに修復プログラムを追加します。 • 削除アイコンをクリックして、リストから修復プログラムを削除します。

Windows Update 修復

次の表に、[Windows Update 修復（Windows update remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [Windows Update 修復（Windows update remediations）] です。

表 B-26　Windows Update 修復

フィールド	使用上のガイドライン
名前（Name）	Windows Update 修復の名前を入力します。
説明（Description）	Windows Update 修復の説明を入力します。
修復タイプ（Remediation Type）	次のいずれかを選択します。 • **自動**：選択した場合、[再試行回数（Retry Count）] および [間隔（Interval）] オプションに入力する必要があります。 • **手動**：選択されている場合、[間隔（Interval）] および [再試行回数（Retry Count）] フィールドは編集できません。
間隔（秒単位）（Interval (in seconds)）	クライアントが以前の試行後に修復を試行できる時間間隔を秒単位で入力します。
再試行回数（Retry Count）	Windows クライアントが Windows Update の試行ができる試行回数を入力します。

表 B-26　Windows Update 修復 （続き）

フィールド	使用上のガイドライン
Windows Update 設定（Windows Update Setting）	次の中から選択します。 • [設定を変更しない（Do not change setting）] : Windows 自動更新のクライアント設定は、Windows Update 修復中または実行後に変更されません。 • [ダウンロードおよびインストールを通知（Notify to download and install）] : Windows ではクライアントへの通知のみが行われ、ダウンロードやインストールは自動的には行われません。 • [自動的にダウンロードし、インストールを通知（Automatically download and notify to install）] : Windows ではクライアントに更新がダウンロードされ、クライアントに Windows Updates をインストールするように通知が行われます。 • [自動的にダウンロードしてインストール（Automatically download and install）] : Windows では自動的に Windows Update がダウンロードされてインストールされます。これは、Windows クライアントに対して強く推奨される設定です。
Windows Update 設定を管理者の設定でオーバーライド（OverrideUser's Windows Update setting with administrator's）	Windows Update 修復の実行中および実行後に、管理者が Windows 自動更新に対して指定した設定をすべてのクライアント マシンに適用するには、このチェックボックスをチェックします。 このチェックボックスをオフにすると、次の設定が適用されます。 • 管理者が指定した設定（Windows クライアントで自動更新が無効になっている場合のみ）。 • Windows クライアントが指定した設定（Windows 自動更新がクライアントで有効になっている場合のみ）。

Windows Server Update Service 修復

次の表に、[Windows Update 修復（Windows update remediations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation action）] > [Windows Update 修復（Windows update remediations）] です。

表 B-27　WSUS 修復

フィールド	使用上のガイドライン
名前（Name）	WSUS 修復の名前を入力します。
説明（Description）	WSUS 修復の説明を入力します。
修復タイプ（Remediation Type）	次の中から選択します。 • [自動（Automatic）] : NAC Agent は、Windows クライアントを最新の WSUS 更新で更新します。 • [手動（Manual）] : 選択すると、[間隔（Interval）] フィールドと [再試行回数（Retry Count）] フィールドを編集できなくなります。ユーザは、コンプライアンスのために、Microsoft で管理されている WSUS サーバから、またはローカルに管理されている WSUS サーバからの最新の WSUS 更新を使用して、Windows クライアントを手動で更新します。
間隔（秒単位）（Interval (in seconds)）	NAC Agent と Web Agent が前回の試行後から再試行までに WSUS 更新を遅延する間隔を秒数で入力します（デフォルトの間隔は 0 です）。

表 B-27　WSUS 修復 （続き）

フィールド	使用上のガイドライン
再試行回数（Retry Count）	NAC Agent と Web Agent が WSUS 更新を使用して Windows クライアントの更新を再試行する回数を入力します。
Windows Update の検証方法（Validate Windows updates using）	次の中から選択します。 • **シスコ ルール（Cisco Rules）**：このオプションを選択した場合、ポスチャ要件で条件としてカスタム ルールまたは事前設定済みルールを選択できます • **重大度レベル（Severity Level）**：このオプションを選択した場合、ポスチャ要件で条件としてカスタム ルールまたは事前設定済みルールを選択できますが、これらは使用されません。このため、WSUS 修復を指定するポスチャ要件内にはプレースホルダ条件（ダミー条件）として pr_WSUSRule を使用できます。
Windows Update 重大度レベル（Windows Updates Severity Level）	重大度レベルを選択します。 • [緊急（Critical）]：緊急の Windows Update のみをインストールします • [高速（Express）]：重要な Windows Update と緊急の Windows Update をインストールします • [中（Medium）]：緊急の Windows Update、重要な Windows Update、および警告の Windows Update をすべてインストールします • [すべて（All）]：緊急の Windows Update、重要な Windows Update、警告の Windows Update、および注意の Windows Update をすべてインストールします **（注）** 重要度レベル オプションを使用して Windows Updates を検証するために WSUS 修復アクションをポスチャ要件に関連付ける場合、ポスチャ要件で pr_WSUSRule（ダミーの複合条件）の複合条件を選択する必要があります。ポスチャ要件が失敗すると、NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて修復アクション（Windows Updates）を適用します。
最新の OS サービス パックに更新（Update to latest OS Service Pack）	このチェックボックスをオンにすると、WSUS 修復によって、クライアントのオペレーティング システムに使用可能な最新のサービス パックが自動的にインストールされます。 **（注）** オペレーティング システムのサービス パックは、WSUS 修復で選択されている [中（Medium）] および [すべて（All）] の重大度レベル オプションに関係なく、自動的に更新されます。
Windows Update インストール ソース（Windows Updates Installation Source）	Windows クライアントにインストールする WSUS 更新のソースを指定します。 • [Microsoft サーバ（Microsoft server）]：Microsoft で管理されている WSUS サーバ • [管理対象サーバ（Managed server）]：ローカルに管理されている WSUS サーバ
インストール ウィザード インターフェイス設定（Installation Wizard Interface Setting）	WSUS 更新中にクライアントにインストール ウィザードを表示できるようにします。 • [UI を表示（Show UI）]：Windows クライアントで Windows Update インストール ウィザードを表示します。WSUS 更新中にインストール ウィザードを表示するには、ユーザはクライアント マシン上に管理者権限を持っている必要があります。 • [UI なし（No UI）]：Windows クライアントで Windows Update インストール ウィザードを非表示にします。

クライアントのポスチャ要件

次の表に、[ポスチャ要件（Posture Requirements）] ページのフィールドについて説明します。このページへのナビゲーション パスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）] です。

表 B-28　ポスチャ要件

フィールド	使用上のガイドライン
名前（Name）	要件の名前を入力します。
オペレーティング システム（Operating Systems）	オペレーティング システムを選択します。 プラス記号 [+] をクリックして、複数のオペレーティング システムをポリシーに関連付けます。 マイナス記号 [-] をクリックして、ポリシーからオペレーティング システムを削除します。
条件（Conditions）	リストから条件を選択します。 [操作（Action）] アイコンをクリックして、ユーザ定義の条件を作成して、要件に関連付けることもできます。ユーザ定義の条件を作成中に関連する親オペレーティング システムは編集できません。 pr_WSUSRule は、関連 Windows Server Update Service（WSUS）修復を指定したポスチャ要件で使用されるダミーの複合条件です。関連 WSUS 修復アクションは、重大度レベル オプションを使用して Windows Updates を検証するように設定する必要があります。この要件が失敗すると、Windows クライアントにインストールされている NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて WSUS 修復アクションを適用します。 pr_WSUSRule は、複合条件のリスト ページには表示できません。条件ウィジェットからのみ pr_WSUSRule を選択できます。
修復アクション（Remediation Actions）	リストから修復を選択します。 修復アクションを作成して、要件に関連付けることもできます。 Agent ユーザとの通信に使用できるすべての修復タイプのテキスト ボックスがあります。修復アクションに加えて、クライアントの非準拠に関してメッセージで Agent ユーザと通信することができます。 [メッセージ テキストのみ（Message Text Only）] オプションで Agent ユーザに非準拠について通知します。また、詳細情報を得るためにヘルプ デスクに連絡したり、クライアントを手動で修復したりするオプションの手順がユーザに提供されています。このシナリオでは、NAC Agent は修復アクションをトリガーしません。