CHAPTER 18

ポリシー条件の設定

Cisco ISE は、ポリシー ベースのネットワーク アクセス コントロール ソリューションで、次のサービスを提供します。ネットワーク アクセス、ゲスト、ポスチャ、クライアント プロビジョニング、およびプロファイラ サービス。Cisco ISE の設定中に、認証、許可、ゲスト、ポスチャ、およびプロファイラ ポリシーを作成します。ポリシー条件は、ポリシーの基本的な構築ブロックです。単純と複合の 2 つのタイプのポリシー条件があります。

この章では、ポリシー条件、および Cisco ISE が提供するさまざまなサービスのポリシー条件を作成する方法について説明します。

この章の内容は、次のとおりです。

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「単純条件の作成」（P.18-2）
- 「複合条件の作成」（P.18-3）
- 「プロファイラ条件」（P.18-4）
- 「ポスチャ条件」（P.18-5）
- 「時刻と日付の条件の作成」（P.18-8）

単純および複合条件

Cisco ISE は、ネットワーク アクセス、プロファイラ、ポスチャ、ゲスト サービスを提供するために、ルール ベースのポリシーを使用します。これらのルール ベースのポリシーは、条件で構成されたルールから構成されます。Cisco ISE では、個別の再利用可能なポリシー要素として条件を作成でき、これらの条件は別のルールベースのポリシーから参照することが可能です。条件には次の 2 種類があります。

- 単純条件：単純条件は、オペランド（属性）、演算子（equal to、not equal to、greater than など）、および値で構成されています。単純条件を保存し、他のルール ベースのポリシーで使用できます。

  単純条件は、A オペランド B の形式をとります。ここで、A は Cisco ISE ディクショナリ内の任意の属性とすることができ、B は属性 A がとり得るいずれかの値とすることができます。デバイス タイプは、属性の値としてすべてのデバイス タイプを含めることができるすべてのネットワーク デバイスの属性として使用され、次の形式での A Equals B を意味します。

  [DEVICE]:[デバイス タイプ（Device Type）] [等しい（Equals）] [すべてのデバイス タイプ（All Device Types）]

- 複合条件：AND あるいは OR 演算子で結合された 1 つ以上の単純条件で構成されています。複合条件は、単純条件に基づいて構成されます。複合条件を保存し、他のルール ベースのポリシーで再使用できます。

  複合条件は次のいずれかの形式をとります。

  - （X オペランド Y）AND（A オペランド B）AND（X オペランド Z）AND（以下同様）
  - （X オペランド Y）OR（A オペランド B）OR（X オペランド Z）OR（以下同様）

    ここで、X および A は、ユーザ名およびデバイス タイプなどの Cisco ISE ディクショナリの属性です。

  次は、複合条件の例です。

  [DEVICE]:[モデル名（Model Name）] [一致（Matches）] [Catalyst6K] [AND] [ネットワークへのアクセス（Network Access）]:[使用例（Use Case）] [等しい（Equals）] [ホスト ルックアップ（Host Lookup）]。

  ポリシーで使用されているか、または複合条件の一部である条件を削除できません

関連項目

- 「単純条件の作成」（P.18-2）
- 「複合条件の作成」（P.18-3）

ポリシー評価

通常、ポリシーはルールで構成され、各ルールは条件で構成され、条件が満たされた場合に、ネットワーク リソースへのアクセスなどのアクションの実行が許可されます。ルールベースの条件は、ポリシーの基盤、つまり要求を評価するときに使用するルールのセットを形成します。

実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

ポリシー条件の評価時に、Cisco ISE は属性と値を比較します。ポリシー条件で指定された属性に、要求内で割り当てられた値が含まれていない場合があります。このとき、比較に使用されている演算子が「not equal to」である場合、この条件は true と評価されます。その他の場合、この条件は false と評価されます。

たとえば、「Radius.Calling_Station_ID Not Equal to 1.1.1.1」という条件において RADIUS 要求に Calling Station ID が存在しない場合、この条件は true と評価されます。この評価は RADIUS ディクショナリに特有なものではなく、「Not Equal to」演算子の使用に起因して発生します。

単純条件の作成

単純条件を作成し、認証、許可、またはゲスト ポリシーを定義するときに再利用できます。

はじめる前に

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）] を選択します。

ステップ 2　[認証（Authentication）] または [許可（Authorization）] または [ゲスト（Guest）] の隣にある矢印をクリックし、[単純条件（Simple Conditions）] をクリックします。

ステップ 3　[追加（Add）] をクリックします。

ステップ 4　[名前（Name）]、[属性（Attribute）]、[演算子（Operator）] および [値（Value）] フィールドに適切な値を入力します。

（注）　単純条件で ID グループを指定した場合、これらを次のように FQDN 形式で表記していることを確認してください。

```
(InternalUser:IdentityGroup) : Equal : (UserIdentityGroups: Identity Group Name)
```

Cisco ISE では、次の形式の ID グループ エントリを正確に解決できません。

```
(InternalUser:IdentityGroup) : Equal :  (Identity Group Name)。
```

ステップ 5　[送信（Submit）] をクリックして、条件を保存します。

次の作業

- 単純条件を使用したルールベースの認証ポリシーの定義方法については、16-27 ページの「Creating a Rule-Based Authentication Policy」の項を参照してください。
- 単純条件を使用した許可ポリシーの定義方法については、17-8 ページの「Configuring Authorization Policies」の項を参照してください。
- 単純条件を使用してスポンサー グループ ポリシーを定義する方法については、「スポンサー グループ ポリシーの作成」（P.16-7）を参照してください。

複合条件の作成

複合条件を作成し、認証ポリシーを定義するときに再利用できます。

はじめる前に

- Cisco ISE には、最も一般的な使用例の一部として事前定義された複合条件があります。これらの事前定義された条件を要件に合わせて編集できます。
- 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）] を選択します。

ステップ 2　[認証（Authentication）] または [許可（Authorization）] または [ゲスト（Guest）] の隣にある矢印をクリックし、[複合条件（Compound Conditions）] をクリックします。

ステップ 3　[追加（Add）] をクリックします。

ステップ 4　複合条件の名前を入力します。任意で説明を入力できます。

ステップ 5　[既存の条件をライブラリから選択（Select Existing Condition from Library）] をクリックして既存の単純条件を選択するか、[新しい条件の作成（Create New Condition）] をクリックして、式ビルダーから属性、演算子、および値を選択します。

ステップ 6　さらに条件を追加するには、この行の終わりでアクション アイコンをクリックします。

ステップ 7　[属性 / 値の追加（Add Attribute/Value）] をクリックして新しい条件を作成するか、[条件をライブラリから追加（Add Condition from Library）] をクリックして既存の単純条件を追加します。

ステップ 8　ドロップダウン リストから、オペランドを選択します。[AND] または [OR] を選択できます。この複合条件のすべての条件間で同じオペランドが使用されます。

ステップ 9　[送信（Submit）] をクリックして複合条件を作成します。

次の作業

- 複合条件を使用したルールベースの認証ポリシーの定義方法については、16-27 ページの「Creating a Rule-Based Authentication Policy」の項を参照してください。
- 複合条件を使用した許可ポリシーの定義方法については、17-8 ページの「Configuring Authorization Policies」の項を参照してください。
- 複合条件を使用してスポンサー グループ ポリシーを定義する方法については、「スポンサー グループ ポリシーの作成」（P.16-7）を参照してください。

プロファイラ条件

プロファイリング条件は、ポリシー要素であり、他の条件と似ています。ただし、認証、許可、およびゲスト条件とは異なり、プロファイラ条件は属性の数に基づくことがあります。[プロファイラ条件（Profiler Condition）] ページに、Cisco ISE で使用できる属性とその説明が一覧表示されます。

プロファイラ条件は、次のいずれかになります。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件があり、それらは [プロファイラ条件（Profiler Condition）] ページでシスコ提供として識別されます。シスコ提供のプロファイリング条件は削除できません。

  シスコ提供の条件は、次の場所にあるシステム プロファイラ ディクショナリにもあります。[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）]。

  たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。
- 管理者作成：Cisco ISE の管理者として作成したプロファイラ条件、または複製された事前定義済み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。[プロファイラ条件（Profiler Condition）] ページのプロファイラ ディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

はじめる前に

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）] > [プロファイリング（Profiling）] > [追加（Add）] を選択します。

ステップ 2　「プロファイラ条件の設定」（P.B-9）に説明されているようにフィールドに値を入力します。

ステップ 3　[送信（Submit）] をクリックして、プロファイラ条件を保存します。

ステップ 4　さらに多くの条件を作成するには、この手順を繰り返します。

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「プロファイラ条件の設定」（P.B-9）

ポスチャ条件

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。

ネットワーク上に初めて Cisco ISE 導入するときは、最初に 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ックスとして pr_ が付けられ、複合条件はプレフィックスとして pc_ 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 を介して定期的に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できません。

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および複合条件の両方が含まれます。

関連項目

- 「ポスチャ更新のダウンロード」（P.23-9）
- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「ポスチャ条件の設定」（P.B-10）

単純ポスチャ条件

[ポスチャ（Posture）] ナビゲーション 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上のファイルのバージョンを確認する条件。
- レジストリ条件：クライアント上のレジストリ キーの存在またたレジストリ 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（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。
- 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および値を確認する条件。

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「ポスチャ条件の設定」（P.B-10）

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の単純条件を作成できます。

はじめる前に

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　次のいずれかを選択してください。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の単純条件。

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。

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「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）
- 「ディクショナリ単純条件の設定」（P.B-16）

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から構成されます。ポスチャ ポリシーを定義しているときに、次の複合条件を使用できます。

- 複合条件：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タイプの 1 つ以上の単純な条件または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

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「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）
- 「ディクショナリ複合条件の設定」（P.B-17）
- 「アンチウイルスとアンチスパイウェア サポート表」（P.18-7）

Windows クライアントで自動アップデートを有効にするシスコ事前定義の条件

pr_AutoUpdateCheck_Rule はシスコ事前定義の条件であり、[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していない場合は、ネットワーク アクセス コントロール（NAC）エージェントは自動アップデート機能を有効に（修復）するように Windows クライアントに強制します。修復が完了されたら、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。

シスコ時前設定のアンチウイルス条件とアンチスパイウェア条件

Cisco ISE は [AV と AS の複合条件（AV and AS Compound Condition）] ページで、事前設定されているアンチウイルスとアンチスパイウェアの複合条件をロードします。それらは、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とアンチスパイウェア サポート表で定義されています。これらの複合条件は、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して、更新されていないか確認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ので、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、次の URL の Cisco.com で参照できます。

http://www.cisco.com/en/US/docs/security/ise/1.1/release_notes/win-avas-3-4-27-1.pdf

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。

はじめる前に

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。

関連項目

- 「単純および複合条件」（P.18-1）
- 「ポリシー評価」（P.18-2）
- 「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）
- 「ディクショナリ複合条件の設定」（P.B-17）

時刻と日付の条件の作成

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を制限または拡張ことができます。

はじめる前に

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）] > [時刻と日付（Time and Date）] > [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。

- [標準設定（Standard Settings）] 領域で、アクセスを提供する時刻と日付を指定します。
- [例外（Exceptions）] 領域で、アクセスを制限する時刻と日付の範囲を指定します。

ステップ 3　[送信（Submit）] をクリックします。

関連項目

- 「単純および複合条件」（P.18-1）

- 「ポリシー評価」（P.18-2）