CHAPTER 17

許可ポリシーおよびプロファイルの管理

この章では、Cisco Identity Services Engine（ISE）で許可プロファイルを作成するときに使用する許可ポリシーについて説明します。ISE ユーザ インターフェイスのメニュー、タブ、およびオプションを使用して、許可プロファイルの基盤を形成する許可ポリシーを作成できます。

許可ポリシーでは、許可ルールから構成される全体的な許可ポリシーが生成されます。許可ルールには、名前、属性、および権限の 3 つの要素があります。許可プロファイルにマップするのは権限の機能です。

この章では、許可ポリシーについて説明し、次の許可ポリシー関連タスクの手順の例を示します。

許可ポリシーについて

許可ポリシーは、ネットワーク リソースにアクセスする特定のユーザおよびユーザのグループのために許可ポリシーの定義および許可プロファイルの設定を可能にする Cisco ISE ネットワーク許可サービスのコンポーネントです。

ネットワーク許可ポリシーは、特定のユーザおよびグループの ID にルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーによって返され、ネットワーク アクセスがこれに応じて許可されます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1 つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1 つ以上の ID グループを組み合わせます。また、特定の ID グループを使用しない条件付きの要件が存在する場合もあります（デフォルトの「Any」の使用など）。Cisco ISE は属性ベースのポリシー システムであり、ID グループが、その多数の重要な属性の 1 つとなります。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイスベースのプロファイル

プロファイルは、ディクショナリに保存されているリソース セットから選択された属性で構成され、特定の許可ポリシーの複合条件が一致したときに返されます。許可ポリシーには単一のネットワーク サービス ルールにマッピングする複合条件を含めることができるため、許可チェックのリストを含めることもできます。

単純なシナリオでは、すべての許可チェックがルール内で AND ブール演算子を使用して作成されます。高度なシナリオでは、任意のタイプの許可確認式を使用できますが、これらのすべての許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザ定義名を含む 1 つ以上の条件から構成され、他の許可ポリシーで再利用できます。

詳細情報：

- ポリシーの用語の詳細については、「許可ポリシーの用語について」（P.17-2）を参照してください。
- ポリシーおよびプロファイルの詳細については、「Cisco ISE 許可ポリシーおよびプロファイル」（P.17-5）を参照してください。
- ポリシーの設定の詳細については、「許可ポリシーの設定」（P.17-14）を参照してください。
- ポリシー要素の条件の設定の詳細については、「ポリシー要素条件の設定」（P.17-18）を参照してください。
- プロファイルの権限の設定の詳細については、「許可プロファイルの権限の設定」（P.17-28）を参照してください。
- DACLs 用の権限の設定については、「ダウンロード可能 ACL の権限の設定」（P.17-34）を参照してください。

許可ポリシーの用語について

表 17-1 は、Cisco ISE 許可ポリシーおよびプロファイルの基本的な用語を定義して説明しています。

表 17-1　Cisco ISE の許可ポリシーおよびプロファイルの基本的な用語

用語	説明
ネットワーク許可	許可は、いずれのユーザが Cisco ISE ネットワークおよびそのリソースにアクセスできるかを保証するための重要な要件です。ネットワーク許可は、ネットワークおよびそのリソースへのユーザ アクセスならびに各ユーザがシステム上でこれらのリソースに対して実行できることを制御します。Cisco ISE ネットワークは、読み取り、書き込み、および実行の権限を許可する権限セットを定義します。Cisco ISE では、ネットワークのニーズに合わせて、多数のさまざまな許可ポリシーを作成できます。このリリースでは、Cisco ISE ネットワークおよびそのリソースへのリモート認証ダイヤルイン ユーザ サービス（RADIUS）アクセスのみがサポートされます。
ポリシー要素	ポリシー要素は、許可ポリシーを定義するコンポーネントです。ポリシー要素は次のとおりです。 • ルール名 • ID グループ • 条件 • 権限 これらのポリシー要素は、ポリシー ルールを作成したときに参照され、条件および属性の選択によって、特定のタイプの許可プロファイルを作成できます。
許可プロファイル	許可プロファイルは、多数の特定の権限によって一連のネットワーク サービスへのアクセスが許可されるコンテナとして機能します。許可プロファイルには、ネットワーク アクセス要求に付与される権限セットを定義し、次のものを含めることができます。 • プロファイル名 • プロファイルの説明 • 関連 DACL • 関連 VLAN • 関連 SGACL • 任意の数の他のディクショナリベースの属性

表 17-1　Cisco ISE の許可ポリシーおよびプロファイルの基本的な用語 （続き）

用語	説明
許可ポリシー	許可ポリシーは、ユーザ定義の単一のルールまたはルールのセットで構成できます。これらのルールは、特定のポリシーを作成するために機能します。たとえば、標準ポリシーは、ID グループ用に入力した値と特定の条件または属性をリンクする If-Then 表記法を使用するルール名を含め、一意の許可プロファイルを作成する特定の権限セットを生成できます。設定できる許可ポリシー オプションは 2 つあります。 • 最初に一致したルールの適用（First Matched Rules Apply） • 複数の一致したルールの適用（Multiple Matched Rule Applies） これら 2 つのオプションは、ユーザの権限セットと一致したときに、標準ポリシー テーブルにリストされている最初に一致したルール タイプの使用または複数の一致したルール タイプの使用のいずれかを Cisco ISE に指示します。設定できる許可ポリシーには、次の 2 つのタイプがあります。 • 標準 • 例外 標準ポリシーは、長期間有効なままにし、ユーザ、デバイスまたはグループの大規模なグループに適用し、特定またはすべてのネットワーク エンドポイントへのアクセスを許可するために作成されるポリシーです。標準ポリシーは不変であり、共通の権限セットを共有するユーザ、デバイス、およびグループの大規模なグループに適用されます。 標準ポリシーは、元の値を変更して特定の ID グループのニーズに対応するテンプレートとして使用し、特定の条件または権限を使用して別のタイプの標準ポリシーを作成し、新しい部門、ユーザのグループ、デバイス、またはネットワーク内のグループのニーズを満たすことができます。 これとは対照的に、例外ポリシーは、標準ポリシーの例外として機能するタイプのポリシーであるため、適切な名前を付けられます。例外ポリシーは、さまざまな要因（短期間のポリシー期間、特定のタイプのネットワーク デバイス、ネットワーク エンドポイントまたはグループ、特別な条件や権限を満たすニーズ、あるいは即時要件）に基づく制限されたアクセスを許可することを目的としています。 例外ポリシーは、制限された数のユーザ、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザまたはユーザのサブセットに合わせて調整された、ID グループ、条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。これにより、さまざまな、またはカスタマイズされたポリシーを作成し、企業、グループ、またはネットワークのニーズを満たすことができます。
アクセス コントロール リスト	Cisco ISE システムの ACL は、特定のオブジェクトまたはネットワーク リソースに関連付けられた権限のリストです。ACL は、いずれのユーザまたはグループがオブジェクトへのアクセス権を付与されるか、および指定されたオブジェクトまたはネットワーク リソースでどの操作が許可されるかを指定します。一般的な ACL の各エントリは、サブジェクトおよび操作を指定するか、または状態（たとえば、許可または拒否）を提供します。DACL は、ダウンロード可能な ACL を表します。

Cisco ISE 許可ポリシーおよびプロファイル

この項では、Cisco ISE で使用する許可ポリシーおよび許可プロファイルについて説明します。Cisco ISE ユーザ インターフェイス（[許可ポリシー（Authorization Policy）] ページおよび [許可プロファイル（Authorization Profile）] ページ）を使用すると、次のポリシー管理操作を実行することによって、すべての許可ポリシーおよびプロファイルを管理できます。

- 既存のポリシーの表示
- 新しいポリシーの作成
- 既存のポリシーの複製（新しいポリシーを作成するために変更できるテンプレートとして使用するため）
- 既存のポリシーの変更（目的のルールまたは権限を変更してカスタマイズされたポリシーを作成）
- 既存のポリシーの削除

詳細情報：

ポリシーおよびプロファイルの作成に使用する [許可ポリシー（Authorization Policy）] ページおよび [許可プロファイル（Authorization Profile）] ページのコンポーネントと要素の説明は、次のトピックを参照してください。

- 許可ポリシーの作成に使用できるユーザ インターフェイス要素の詳細については、「[許可ポリシー（Authorization Policy）] ページ」（P.17-5）および「許可ポリシーおよびプロファイルのユーザ インターフェイス」（P.17-10）を参照してください。
- 許可プロファイルの作成に使用できるユーザ インターフェイス要素の詳細については、「[許可プロファイル（Authorization Profile）] ページ」（P.17-8）および「許可ポリシーおよびプロファイルのユーザ インターフェイス」（P.17-10）を参照してください。
- 許可ポリシーおよびプロファイルの作成のガイドラインについては、「許可ポリシーおよびプロファイルのガイドライン」（P.17-9）を参照してください。

次の手順：

許可ポリシーおよびプロファイルを設定するには、次のトピックを参照してください。

- 「許可ポリシーの設定」（P.17-14）
- 「ポリシー要素条件の設定」（P.17-18）
- 「許可プロファイルの権限の設定」（P.17-28）
- 「ダウンロード可能 ACL の権限の設定」（P.17-34）

[許可ポリシー（Authorization Policy）] ページ

[許可ポリシー（Authorization Policy）] ページを表示するには、[ポリシー（Policy）] > [許可（Authorization）] を選択します。[許可ポリシー（Authorization Policy）] ページは、次のタイプの Cisco ISE 許可ポリシーを作成する開始点です。

- 例外：例外ポリシーは、この名前が示すように、多数のユーザまたはグループが使用するために、または長期間有効のままにするために設計されている標準ポリシーの例外です。例外ポリシーは、標準ポリシーとは異なり、特別な目的や短期間の適用、または特定の目的で 1 人以上のユーザやグループが使用するために設計されています。
- 標準：標準ポリシーは、長期間、多数のユーザまたはグループが使用するために作成し、標準的なネットワーク ニーズ用に調整された権限およびルールの標準セットを提供するものです。

（注） Cisco ISE ユーザ インターフェイスにはそれぞれの許可ポリシーに対するステータス インジケータが備えられており、[有効（Enabled）]、[無効（Disabled）]、または [モニタのみ（Monitor Only）] の 3 つの状態の 1 つを表示するように設定できます。

許可ポリシーを管理する際は、既存の例外または標準ポリシーを表示し、これらのポリシーを作成、変更、または削除して、ネットワーク内の特定のユーザまたはグループの要件を満たすことができます。新しい例外または標準許可ポリシーを作成するには、次の一連のタスクを実行し、次の 4 つのポリシー要素値を設定する必要があります。

- [ルール名（Rule Name）] : 許可ポリシーに一意の名前を定義します。
- [ID グループ（Identity Groups）] : 選択可能な選択肢のリストから既存の ID グループを選択します。
- [その他の条件（Other Conditions）] : 既存の条件名ディクショナリの選択肢から単純条件（または複合条件）を選択します（または既存の属性ディクショナリの選択肢から属性を選択できます）。
- [権限（Permissions）] : 既存のプロファイル ディクショナリの選択肢からプロファイルを選択します。

[許可ポリシー（Authorization Policy）] ページの Cisco ISE ユーザ インターフェイスのメニューおよびオプションを使用して、これら 4 つのポリシー要素の値を選択して組み合わせることによって、新しい許可ポリシーを作成できます。ポリシーの選択肢を選択したら、[完了（Done）] をクリックします。

作成したポリシーが [許可ポリシー（Authorization Policy）] ページに読み取り専用モードで表示されます。

許可ポリシーの [編集（Edit）] リンクをクリックしてポリシー ルールを編集できます。ポリシーの選択肢を変更したら、[完了（Done）] をクリックします。

新しいポリシーの追加または既存のポリシーの編集を行うと、鉛筆アイコンがルール名の横に表示されます。鉛筆アイコンは、保存されていない許可ポリシーの変更があることを示しています。[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存する必要があります。

許可ポリシー ルールは、リスト内でランクごとにグループ化され、次のオプションを使用して、このランキング リスト内でルールの位置を変更できます。

- 強調表示（選択）されているポリシーの上または下に、新しいポリシーを挿入します。
- 強調表示（選択）されているポリシーの上または下に、選択したポリシーの複製を挿入します。
- 選択したポリシーを削除します。

ルールをドラッグ アンド ドロップしてリスト内のランクを変更することも可能です。

新しい許可ポリシーを作成すると、必要なすべてのポリシー フィールドにデフォルト値が読み込まれます。次の操作を実行することを要求されます。

- 既存の許可ポリシーを変更するには、変更するポリシー要素を選択し、その値を変更し、[保存（Save）] をクリックして、変更したポリシーを Cisco ISE システム データベースに作成します。
- 既存の許可ポリシーを削除するには、表示されたリストから選択し、[削除（Delete）] をクリックして、このポリシーを Cisco ISE システム データベースから削除します。通常、サポートしないことにしたか、または将来のポリシーでテンプレートとして使用しないことにした許可ポリシーのみを削除します。

（注） 既存の許可ポリシーを削除すると、選択したポリシーが Cisco ISE システム データベースから削除される前に、削除の確認を要求されます。ポリシーに対して加えた変更は、[保存（Save）] をクリックしないと、Cisco ISE システム データベースに送信されず、登録されません。

- 既存のポリシーを複製するには、ランキング リストで目的の位置（上または下）を選択します。Cisco ISE は、既存のポリシーからポリシー値すべてをコピーし、異なるポリシー ID を持つこと以外は同じポリシーを作成します（Cisco ISE では各ポリシー ID が一意である必要があります）。既存のポリシーの複製を使用して開始することによって、これをテンプレートとして使用し、選択したフィールドまたは属性を変更し、新しい許可ポリシーを作成できます。

（注）　作成した各例外または標準許可ポリシーを [有効（Enabled）]、[無効（Disabled）]、または [モニタのみ（Monitor Only）] に設定できます。これを行うには、各エントリの [ルール名（Rule Name）] カラムに隣接する緑のチェックボックスをオンにします。

- 許可ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザの認証中にアクセスされた最後の ID ソースを識別します。
  - 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
  - ID ソース順序の認証中、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

  AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ（LDAP13）を使用してユーザが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

（注）　AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

- 以前認証されたエンドポイント ID グループに基づく許可条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。

  このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザ情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

  エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザ関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザ情報が内部ユーザ属性に基づいている場合は、内部ユーザ ディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

詳細情報：

- エンドポイント ID グループの詳細については、「エンドポイント ID グループ（Endpoint Identity Groups）」（P.4-76）を参照してください。

許可ポリシーとサポートされているディクショナリ

単純条件ベースのポリシー シナリオでは、許可チェックはルール内で AND ブール演算子を使用して作成されます。複合条件ベースのポリシーでは、任意のタイプの許可確認式を使用できます。ただし、両方の許可ポリシーのタイプで、確認は返される許可プロファイルに準拠する必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザ定義名を含む 1 つ（または複数の）条件が含まれます。次のディクショナリをサポートしている Cisco ISE ディクショナリの属性を使用して条件を定義します。

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- RADIUS

RADIUS はシステム定義ディクショナリで、Airespace、Cisco、Cisco-BBSM、Cisco-VPN3000、および Microsoft は RADIUS ベンダー ディクショナリです。Cisco ISE ディクショナリの詳細については、「ディクショナリおよびディクショナリ属性」（P.7-1）を参照してください。

[許可プロファイル（Authorization Profile）] ページ

[許可プロファイル（Authorization Profile）] ページを表示するには、[ポリシー（Policy）] タブから開始します（[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）] を選択します）。[許可プロファイル（Authorization Profile）] ページは、Cisco ISE 標準許可プロファイルを管理する開始点です。ここでは、既存のプロファイルを表示したり、新しいプロファイルを作成したり、特定のユーザまたはグループのネットワークのニーズを満たすために、既存の許可プロファイルを変更または削除したりできます。

新しい許可プロファイルを作成するには、プロファイル名およびアクセス タイプを定義する必要があります。他のすべてのプロファイル要素はオプションです。これら他のプロファイル要素の値を設定するには、次の [許可プロファイル（Authorization Profile）] ページのカラムでテキスト フィールド、ドロップダウン リスト、およびチェックボックスを使用します。

- **許可プロファイル（Authorization Profile）**
  - 名前（Name）
  - 説明（Description）
  - アクセス タイプ（Access Type）

（注） 新しい許可プロファイルを作成するために必要なプロファイル要素は、プロファイルの名前とアクセス タイプのみで、これらにはアスタリスク（*）が付いています。他のすべてのプロファイル要素はオプションの要素です。

- **共通タスク（Common Tasks）**

  一般的に使用される属性をサポートする設定を行うことができます。
  - DACL 名（DACL Name）
  - VLAN

- 音声ドメイン権限（Voice Domain Permission）
- ポスチャ検出（Posture Discovery）
- 中央集中 Web 認証（Centralized Web Authentication）
- Auto SmartPort
- フィルタ ID（Filter-ID）
- 再認証（Reauthentication）
- MACSec ポリシー（MACSec Policy）
- NEAT
- Web 認証（ローカル Web 認証）（Web Authentication (Local Web Auth)）
- ワイヤレス LAN コントローラ（WLC）（Wireless LAN Controller (WLC)）
- ASA VPN

（注）　[共通タスク（Common Task）] 設定の詳細については、「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）を参照してください。

- **高度な属性設定（Advanced Attributes Settings）**

  ドロップダウン リストからアクセスできるディクショナリに含まれている属性を使用して、高度な属性設定を行うことができます。

- **属性詳細（Attributes Details）**

  [共通設定（Common Settings）] グループ ボックスおよび [高度な属性（Advanced Attribute）] グループ ボックスで設定する属性が表示されます。

許可プロファイルの選択肢を選択または入力した後、[送信（Submit）] をクリックして、新しい許可プロファイルを作成します。

既存の許可プロファイルを変更するには、変更するプロファイルに対応するチェックボックスをオンにし、目的に応じてプロファイル設定を変更し、[保存（Save）] をクリックして新しい変更した許可プロファイルを作成します。プロファイルに対して加えた変更は、[保存（Save）] をクリックしないと、Cisco ISE システム データベースに送信されず、登録されません。

既存の許可プロファイルを削除するには、削除するプロファイルに対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。許可プロファイルを作成、変更、または削除する方法を説明する手順については、「許可プロファイルの権限の設定」（P.17-28）を参照してください。

許可ポリシーおよびプロファイルのガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字セットのみを使用する必要があります。
  - 記号：プラス（+）、ハイフン（-）、アンダースコア（_）、ピリオド（.）、およびスペース（ ）。
  - 英文字：A ～ Z と a ～ z。
  - 数字：0 ～ 9。
- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザに適用できます）。

- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。次に、条件を作成する 2 つの方法を示します。
  - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
  - 推奨値を選択またはテキスト ボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字セットのみを使用する必要があります。
  - 記号：ハイフン（-）、アンダースコア（_）、およびピリオド（.）。
  - 英文字：A ～ Z と a ～ z。
  - 数字：0 ～ 9。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザが特定の ID グループ（デバイス管理者など）に属しており、そのユーザが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。

（注）　必ず [保存（Save）] をクリックして、新規または変更したポリシーやプロファイルを Cisco ISE データベースに保存します。

許可ポリシーおよびプロファイルのユーザ インターフェイス

許可ポリシーおよび許可プロファイルを管理するには、対応する各ユーザ インターフェイス ページ内の制御を使用します。次のタスクを実行するために必要な次の Cisco ISE ユーザ インターフェイス制御および要素を使用します。

- 許可ポリシーを設定するには：[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）]（または [例外（Exception）]）を選択します
- 許可プロファイルを設定するには：[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）] を選択します

許可ポリシー、ルール、およびプロファイルの設定のデフォルト

Cisco ISE ソフトウェアには、共通設定を提供する多数のデフォルトの条件、ルール、およびプロファイルが事前インストールされているため、Cisco ISE 許可ポリシーおよびプロファイルで必要なルールおよびポリシーを容易に作成できます。これらの組み込み設定のデフォルトには、表 17-2 で説明されている指定された値が含まれています。

表 17-2　許可ポリシー、プロファイル、およびルールの設定のデフォルト

名前	UI のパス	説明	追加情報
許可ポリシー設定のデフォルト			
許可ポリシーのデフォルトの複合条件	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）]	これらは、許可ポリシーで使用される条件、ルール、およびプロファイルの事前インストールされた設定のデフォルトです。	許可ポリシーを作成するために、次の関連属性を使用できます。 • 有線 802.1x • 有線 MAB • 無線 802.1x • Catalyst スイッチ ローカル Web 認証 • WLC Web 認証

表 17-2　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	UI のパス	説明	追加情報
許可ポリシー設定のデフォルト			
有線 802.1X 複合条件（Wired 802.1X Compound Condition）	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	この複合条件では、次の属性と値をチェックします。 • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Ethernet	この複合条件は、有線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、有線 802.1X 許可ポリシーに基づいて評価されます。
有線 MAB 複合条件（Wired MAB Compound Condition）	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	この複合条件では、次の属性と値をチェックします。 • RADIUS:Service-Type = Call-Check • RADIUS:NAS-Port-Type = Ethernet	この複合条件は、有線 MAB 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、有線 MAB 許可ポリシーに基づいて評価されます。
無線 802.1X 複合条件（Wireless 802.1X Compound Condition）	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	この複合条件では、次の属性と値をチェックします。 • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	この複合条件は、無線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、無線 802.1X 許可ポリシーに基づいて評価されます。
Catalyst スイッチ ローカル Web 認証複合条件（Catalyst Switch Local Web Authentication Compound Condition）	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	この複合条件では、次の属性と値をチェックします。 • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Ethernet	この複合条件を使用するには、この条件をチェックする許可ポリシーを作成する必要があります。
ワイヤレス LAN コントローラ（WLC）ローカル Web 認証複合条件（Wireless Lan Controller (WLC) Local Web Authentication Compound Condition）	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	この複合条件では、次の属性と値をチェックします。 • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	この複合条件を使用するには、この条件をチェックする許可ポリシーを作成する必要があります。

表 17-2　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	UI のパス	説明	追加情報
許可ルール設定のデフォルト			
無線ブラックリストのデフォルトの許可ルール	[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]	この許可ポリシーでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）] : [無線ブラックリストのデフォルト（Wireless Black List Default）] • [エンドポイント ID グループ（Endpoint Identity Group）] : [ブラックリスト（Blacklist）] • [条件（Conditions）] : [Wireless_802.1X] • [権限/許可プロファイル（Permissions/Authorization Profile）] : [Blackhole_Wireless_Access]	このデフォルト ルールは、「失われた」ユーザ デバイスがシステムから削除されるか、または「元に戻される」まで、このようなデバイスを適切にプロビジョニングするように設計されています。
プロファイリングされた Cisco IP Phone 許可ルール	[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]	この許可ポリシーでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）] : [プロファイリングされた Cisco IP Phone（Profiled Cisco IP Phones）] • [エンドポイント ID グループ（Endpoint Identity Group）] : [Cisco-IP-Phones] • [条件（Conditions）] : [任意（Any）] • [権限/許可プロファイル（Permissions/Authorization Profile）] : [Cisco_IP_Phones]	このデフォルト ルールは、デフォルトのエンドポイント ID グループとして Cisco IP Phone を使用し、このテーブルにリストされている値を使用します。

表 17-2　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	UI のパス	説明	追加情報
デフォルトの許可ルール	[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]	この許可ポリシーでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）] : [デフォルト（Default）] • [エンドポイント ID グループ（Endpoint Identity Group）] : [任意（Any）] • [条件（Conditions）] : [任意（Any）] • [許可プロファイル（Authorization Profile）] : [PermitAccess]	このデフォルト ルールは、デフォルトのエンドポイント ID グループとして [任意（Any）] を使用し、このテーブルにリストされている値を使用します。
許可プロファイル設定のデフォルト			
Blackhole_Wireless_Access	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [Blackhole_Wireless_Access]	この許可プロファイルは、ブラックリストに登録されているデバイスへのアクセスを拒否します。ブラックリストに登録されているデバイスはすべて、次の URL にリダイレクトされます。 url-redirect=https://ip:port/mydevices/blackhole.jsp	このデフォルトの許可プロファイルは、デバイス ポータルで「失われた」として宣言されているすべてのエンドポイントに適用されます。
Cisco_IP_Phones	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [Cisco_IP_Phones]	この許可プロファイルでは、次の値の設定デフォルト プロファイルを使用します。 • [名前（Name）] : [Cisco IP Phone] • [DACL] : [PERMIT_ALL_TRAFFIC] • [VSA] : [cisco:av-pair:device-traffic-class=voice] このプロファイルは、このプロファイルで指定された基準に一致する要求を評価します。	このデフォルトの許可プロファイルは、DACL およびベンダー固有属性（VSA）を使用して、すべての「音声」トラフィックを許可します（PERMIT_ALL_TRAFFIC）。

許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページでは、許可ポリシーを表示、作成、複製/変更、または削除できます。次のトピックでは、次の作業を実行するための手順について説明します。

- 「既存の許可ポリシーの表示および一致するルール ポリシーの設定」（P.17-15）
- 「新しい許可ポリシーの作成」（P.17-15）

- 「既存の許可ポリシーの複製および変更」（P.17-17）
- 「既存の許可ポリシーの削除」（P.17-18）

（注）　次の許可ポリシー プロファイルの各項には、標準許可ポリシーで指示されるアクションの例が示されています。同じプロセスに従って例外許可ポリシーを管理できます。

既存の許可ポリシーの表示および一致するルール ポリシーの設定

この手順を使用して、既存のすべての例外または標準許可ポリシーの表示一致するルール ポリシーの選択、または選択可能なポリシーベースの選択肢の表示を実行できます。

既存の許可ポリシーを表示して、一致するルール ポリシーを設定するには、次の手順を実行します。

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

[許可ポリシー（Authorization Policy）] ページが表示され、既存のすべての設定済み許可ポリシーがリストされます。ここには、このページに初めてアクセスしたときに表示される、[デフォルト（Default）]、[プロファイリングされた Cisco IP Phone（Profiled Cisco IP Phones）]、および [ブラックリストのデフォルト（Black List Default）] という名前の 3 つのデフォルトのポリシーが含まれます。

ステップ 2　一致するルール ポリシーを許可ポリシーに設定するには、[許可プロファイル（Authorization Profiles）] の下でドロップダウン矢印をクリックし、[最初に一致したルールの適用（First Matched Rule Applies）] または [複数の一致したルールの適用（Multiple Matched Rule Applies）] を選択します。

新しい許可ポリシーの作成

この手順を使用して、新しい許可ポリシーを作成します。

新しい許可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　[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）] を選択します。

ステップ 2　[操作（action）] アイコン（右端にある下矢印）をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のいずれかを選択します。

[許可ポリシー（Authorization Policy）] ページの [標準（Standard）] パネルで指定した位置に新しいポリシー エントリが表示されます。

ステップ 3　次の許可ポリシーのフィールドに値を入力します。

- [ルール名（Rule Name）] : 新しいポリシーにルール名を定義する必要があります。
- [条件（Conditions）]（ID グループおよびその他の条件）: ポリシーに関連付けられた ID グループの条件または属性のタイプを選択します。[条件（Conditions）] の横の [+] をクリックし、次の設定できる条件および属性の選択肢のリストを表示します。
  - 文字 [任意（Any）] の横の [+]（「プラス」記号）をクリックし、グループの選択肢のドロップダウン リストを表示するか、またはこの ID グループのポリシーに [任意（Any）] を選択し、すべてのユーザを含めます。

- 必要に応じて、ドロップダウン リストから [条件名（Condition Name）] オプションを選択します（[単純条件（Simple Conditions）]、[複合条件（Compound Conditions）]、または [時刻と日付の条件（Time and Date Conditions）]）。
- 必要に応じていずれかの [属性（Attribute）] オプションを選択します。これにより、ディクショナリ タイプに関連する特定の属性を含むディクショナリのリストが表示されます。

  属性を選択すると、演算子オプションのドロップダウン リストを使用して、[等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] を指定し、ドロップダウン ディレクティブ オプションを使用して [AND] または [OR] ディレクティブを選択できます。

（注）　選択したすべての属性に [等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] の演算子オプションが含まれているとは限りません。

（注）　[一致（Matches）] 演算子では、ワイルドカードではなく正規表現（REGEX）がサポートされ、使用されます。

例 1a : [等しい（Equals）] : RADIUS ディクショナリを選択し、[式（Expression）] フィールドに RADIUS:Error-Cause を表示する Error-Cause 値を選択します。2 番目のフィールド（ドロップダウン リスト）で [等しい（Equals）] 演算子を選択します。3 番目のフィールド（ドロップダウン リスト）で、RADIUS:Error-Cause と等しくする値を選択する（たとえば、Unsupported Service）、またはこのフィールドの右側にあるドロップダウン矢印を使用して既存のライブラリから別の属性タイプを選択します。この条件は、次のように設定されます。RADIUS:Error-Cause EQUALS Unsupported Service。

例 1b : [等しい（Equals）] : CERTIFICATE ディクショナリを選択し、[式（Expression）] フィールドに CERTIFICATE:Subject を表示する Subject 値を選択します。2 番目のフィールド（ドロップダウン リスト）で [等しい（Equals）] 演算子を選択します。3 番目のフィールド（テキスト フィールド）で、CERTIFICATE:Subject と等しくする値を正しく設定する（たとえば、User123 などのユーザ名）、またはこのフィールドの右側にあるドロップダウン矢印を使用して既存のライブラリから別の属性タイプを選択する必要があります。一致を実現するには、この条件はプレフィックス「cn=」を使用して次のように設定する必要があります。CERTIFICATE:Subject EQUALS cn=User123。

例 1c : [等しい（Equals）] : CERTIFICATE ディクショナリを選択し、[式（Expression）] フィールドに CERTIFICATE:Subject Alternative Name を表示する Subject Alternative Name 値を選択します。2 番目のフィールド（ドロップダウン リスト）で [等しい（Equals）] 演算子を選択します。3 番目のフィールド（テキスト フィールド）で、CERTIFICATE:Subject Alternative Name と等しくする値を正しく設定する（たとえば、User123@acme.com などのユーザ名）、またはこのフィールドの右側にあるドロップダウン矢印を使用して既存のライブラリから別の属性タイプを選択する必要があります。一致を実現するには、この条件を次のように設定する必要があります。CERTIFICATE:Subject Alternative Name EQUALS User123@acme.com。

例 2 : [等しくない（Not Equals）] : RADIUS ディクショナリを選択し、[式（Expression）] フィールドに RADIUS:User-Name を表示する User-Name 値を選択します。2 番目のフィールド（ドロップダウン リスト）で [等しくない（Not Equals）] 演算子を選択します。3 番目のフィールド（テキスト ボックス）で、RADIUS:User-Name と等しくないようにする値を入力する（たとえば、guest113）、またはこのフィールドの右側にあるドロップダウン矢印を使用して既存のライブラリから別の属性タイプを選択します。この条件は、次のように設定されます。RADIUS:User-Name NOT_EQUALS guest113。

例 3 : [一致（Matches）] : CERTIFICATE ディクショナリを選択し、[式（Expression）] フィールドに CERTIFICATE:Organization を表示する Organization 値を選択します。2 番目のフィールド（ドロップダウン リスト）で [一致（Matches）] 演算子を選択します。3 番目のフィールド（テキスト ボックス）で、Organization 値と一致する REGEX 値を入力するか、またはこのフィールドの右側にあるドロップダウン矢印を使用して既存のライブラリから別の属性タイプを選択します。次に、[一致（Matches）] の一般的なオプションの一部を示します。

- [次で始まる（Starts with）] : たとえば、REGEX 値 ^(Acme).* を使用する場合、この条件は、CERTIFICATE:Organization MATCHES 'Acme' として設定されます（「Acme」で始まる条件との一致）。
- [次で終わる（Ends with）] : たとえば、REGEX 値 .*(mktg)$ を使用する場合、この条件は、CERTIFICATE:Organization MATCHES 'mktg' として設定されます（「mktg」で終わる条件との一致）。
- [次を含む（Contains）] : たとえば、REGEX 値 .*(1234).* を使用する場合、この条件は、CERTIFICATE:Organization MATCHES '1234' として設定されます（Eng1234、1234Dev、Corp1234Mktg など「1234」を含む条件との一致）。
- [で始まらない（Does not start with）] : たとえば、REGEX 値 ^(?!LDAP).* を使用する場合、この条件は、CERTIFICATE:Organization MATCHES 'LDAP' として設定されます（usLDAP、CorpLDAPmktg など「LDAP」で始まらない条件との一致）。

- [権限（Permissions）] : 許可プロファイルを選択してこの許可ポリシーと関連付けます。
  - [権限（Permissions）] の横の [+] をクリックして、プロファイルの選択肢のドロップダウン リストを表示します。プロファイル オプションを選択します（たとえば、[標準（Standard）] プロファイルは 2 つのデフォルトの選択肢 [DenyAccess] または [PermitAccess] を提供します）。

d. [完了（Done）] をクリックします。

ステップ 4　[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

既存の許可ポリシーの複製および変更

この手順を使用して、既存の許可ポリシーを複製し、これを変更してこの既存の値の初期セットに基づく新しいポリシーを作成します。

既存の許可ポリシーを複製して変更するには、次の手順を実行します。

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

ステップ 2　複製して変更する許可ポリシーを選択するには、[操作（action）] アイコンをクリックし、[上に複製（Duplicate above）] または [下に複製（Duplicate below）] をクリックします。

複製ポリシー エントリが [許可ポリシー（Authorization Policy）] ページの [標準（Standard）] パネルに表示されます（選択した既存のポリシーの上または下のいずれか）。

ステップ 3　このポリシーの新しい名前を [ルール名（Rule Name）] フィールドに入力します。

ステップ 4　対応するフィールドで目的のオプションの選択肢セットを選択することによって、目的の値を変更して新しい許可ポリシーを作成します。

ステップ 5　[保存（Save）] をクリックして、変更を Cisco ISE データベースに保存し、この新しい許可ポリシーを作成します。

既存の許可ポリシーの削除

この手順を使用して、既存の許可ポリシーを削除し、これを Cisco ISE データベースから削除します。

既存の許可ポリシーを削除するには、次の手順を実行します。

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

ステップ 2　削除する許可ポリシーを選択するには、そのポリシーの [操作（action）]（アイコン）をクリックし、[削除（Delete）] を選択します。

[許可ポリシー（Authorization Policy）] ページの [標準（Standard）] パネルに確認用のダイアログが表示されます。

ステップ 3　[削除（Delete）] をクリックして、この許可ポリシーを削除することを確認します。

ステップ 4　[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この許可ポリシーを削除します。

（注）　[保存（Save）] をクリックしないと、許可ポリシーはローカルで削除されるだけになります。

ポリシー要素条件の設定

Cisco ISE には、独立した再利用可能なポリシー要素として条件を作成する機能があります。このような条件は、他のルールベース ポリシーから参照することができます。条件は、ポリシーのページから作成できます。独立したポリシー要素として作成すると、Cisco ISE の他のタイプのポリシー（たとえばスポンサー グループやクライアント プロビジョニングのポリシー）から再利用できます。ポリシーの評価が行われるときは、そのポリシーを構成する条件が最初に評価されます。

（注）　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] で、初期の [条件（Conditions）] ページに、[認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[ゲスト（Guest）]、および [共通（Common）] というポリシー要素条件オプションが表示されます。

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、アクション（ネットワーク リソースへのアクセスなど）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。

単純条件は、1 つの属性、1 つの演算子、および 1 つの値で構成されます。単純条件はポリシーのページから作成できます。他のポリシーで再利用できる、独立したポリシー要素として作成することもできます。ISE では、単純許可条件を作成、編集、および削除できます。許可されると、Cisco ISE は権限を返します。

複合条件は、通常、2 つ以上の単純条件で構成されます。複合条件は、再利用可能なオブジェクトとしてポリシー作成ページから、または [条件（Conditions）] ページから作成できます。このページには、ISE で定義したすべての複合条件がリストされます。

単純条件

前提条件：

- いずれの手順を始める前にも、ルールベース許可ポリシー、ID グループ、条件や権限の基本的な構築ブロック、およびこれらを Cisco ISE ユーザ インターフェイスで使用する方法に関する基礎を理解しておく必要があります。詳細については、「許可ポリシーの用語について」（P.17-2）、「[許可ポリシー（Authorization Policy）] ページ」（P.17-5）、および「ポリシー要素条件の設定」（P.17-18）を参照してください。
- 各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはポリシー管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、表 4-11 を参照してください。

単純条件の形式

このタイプは、*属性オペランド値*の形式を使用します。ルールベース条件は、本質的に値（値を持つ属性）の比較であり、保存して他のルールベース ポリシーで再利用できます。

単純条件は A オペランド B の形式となり、ここで、A は Cisco ISE ディクショナリの任意の属性、B は属性 A に使用できる値の 1 つにできます。たとえば、単純条件は次の形式にできます。

- Network Access:Protocol Equals RADIUS。

複合条件

前提条件：

- いずれの手順を始める前にも、ルールベース許可ポリシー、ID グループ、条件や権限の基本的な構築ブロック、およびこれらを Cisco ISE ユーザ インターフェイスで表現する方法に関する基礎を理解しておく必要があります。詳細については、「許可ポリシーの用語について」（P.17-2）、「[許可ポリシー（Authorization Policy）] ページ」（P.17-5）、および「ポリシー要素条件の設定」（P.17-18）を参照してください。
- Cisco ISE には、最も一般的な用途のために事前定義された複合条件が用意されています。これらの事前定義された条件の詳細については、「許可ポリシー、ルール、およびプロファイルの設定のデフォルト」（P.17-10）を参照してください。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。
- 各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはポリシー管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、表 4-11 を参照してください。

複合条件の形式

この条件タイプは、AND または OR の関係を使用した 1 つ以上の単純条件から構成されます。これらは、単純条件に基づいて構築され、保存して他のルールベース ポリシーで再利用できます。複合条件は、次の形式のいずれかを取ることができます。

- (X オペランド Y) AND (A オペランド B) AND (X オペランド Z) AND ...（続く）
- (X オペランド Y) OR (A オペランド B) OR (X オペランド Z) OR ...（続く）

  ここで、X および A は Cisco ISE ディクショナリの属性で、ユーザ名およびデバイス タイプを含むことができます。たとえば、複合条件は次の形式を取ることができます。

– [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）]。

許可ポリシー条件の設定

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、許可ポリシー要素条件を表示、作成、変更、削除、複製、および検索します。次のトピックでは、次の作業を実行するための手順について説明します。

- 「既存の許可ポリシー要素条件の表示」（P.17-20）
- 「新しい許可ポリシー要素条件の作成」（P.17-20）
- 「既存の許可ポリシー要素条件の変更」（P.17-21）
- 「既存の許可ポリシー要素条件の複製」（P.17-22）
- 「既存の許可ポリシー要素条件の削除」（P.17-23）
- 「既存の許可ポリシー要素条件の検索」（P.17-23）

（注）　単純条件および複合条件の詳細については、「ポリシー要素条件の設定」（P.17-18）を参照してください。

既存の許可ポリシー要素条件の表示

この手順を使用して、既存のすべての許可ポリシー要素条件（単純または複合）を表示します。

既存の許可ポリシー要素条件を表示するには、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の、設定済みのすべての許可ポリシー（選択した条件タイプ（単純または複合）に対応します）がリストされます。

新しい許可ポリシー要素条件の作成

この手順を使用して、新しい許可ポリシー要素条件（単純または複合）を作成します。

新しい許可ポリシー要素条件を作成するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の設定済み許可ポリシー要素条件がすべて示されます。

ステップ 2　新しい単純条件を作成するには、[作成（Create）] をクリックします。

[単純条件（Simple Conditions）] ページが表示されます。

ステップ 3　次のフィールドに値を入力して新しい単純条件を定義します。

- [名前（Name）]：単純条件の名前を入力します。
- [説明（Description）]：単純条件の説明を入力します。

- [属性（Attribute）] : ディクショナリ オプションのドロップダウン リストからディクショナリを選択し、対応する属性の選択肢から属性を選択する場合にクリックします。
- [演算子（Operator）] : [等しい（Equals）] または [等しくない（Not Equals）] を選択します。
- [値（Value）] : 選択した属性に一致する値を入力します。

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE データベースに保存し、この許可条件を作成します。

（注） 単純条件の [名前（Name）]、[属性（Attribute）]、[演算子（Operator）]、および [値（Value）] フィールドは必須であり、アスタリスク（*）が付いています。

（注） 複合条件は、さまざまな [等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] の演算子および「AND」と「OR」のディレクティブを含む 1 つ以上の単純条件で構成され、既存の単純条件上に構築されます。新しい複合条件を作成する手順は、単純条件を作成する手順とプロセスに従います。複合条件の詳細については、「複合条件」（P.17-19）を参照してください。

（注） [一致（Matches）] 演算子では、ワイルドカードではなく正規表現（REGEX）がサポートされ、使用されます。

既存の許可ポリシー要素条件の変更

この手順を使用して、既存の許可ポリシー要素条件（単純または複合）を変更します。

既存の許可ポリシー要素条件を変更するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の設定済み許可ポリシー要素条件がすべて示されます。

ステップ 2　既存の条件を編集するには、変更する条件に対応するチェックボックスをオンにして、[編集（Edit）] をクリックします。

[単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）ページが表示されます。必要に応じて次のフィールドの値を変更します。

- [名前（Name）] : 単純条件の名前を入力します。
- [説明（Description）] : 単純条件の説明を入力します。
- [属性（Attribute）] : ディクショナリ オプションのドロップダウン リストからディクショナリを選択し、対応する属性の選択肢から属性を選択する場合にクリックします。
- [演算子（Operator）] : [等しい（Equals）] または [等しくない（Not Equals）] を選択します。
- [値（Value）] : 選択した属性に一致する値を入力します。

ステップ 3　[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この変更した許可条件を作成します。

（注） 単純条件の [名前（Name）]、[属性（Attribute）]、[演算子（Operator）] および [値（Value）] フィールドは必須であり、アスタリスク（*）が付いています。

（注） 複合条件は、さまざまな [等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] の演算子および「AND」と「OR」のディレクティブを含む 1 つ以上の単純条件で構成され、既存の単純条件上に構築されます。新しい複合条件を作成する手順は、単純条件を作成するために使用した手順と同じ順序に従います。複合条件の詳細については、「複合条件」（P.17-19）を参照してください。

（注） [一致（Matches）] 演算子では、ワイルドカードではなく正規表現（REGEX）がサポートされ、使用されます。

既存の許可ポリシー要素条件の複製

この手順を使用して、既存の許可ポリシー要素条件（単純または複合）を複製します。このオプションでは、次のことを実行できるテンプレートとして既存の許可ポリシーを使用する方法が提供されます。

- 同じポリシー要素条件の複製ポリシーを名前を変えて作成します。
- 名前を変え、目的のポリシー要素を 1 つ以上変更します。

（注） 既存のポリシー要素条件を複製した場合は、いずれの場合も [送信（Submit）] をクリックして変更を Cisco ISE データベースに保存する必要があります。

既存の許可ポリシー要素条件を複製するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の設定済み許可ポリシー要素条件がすべて示されます。

ステップ 2　既存の単純条件許可ポリシーを複製するには、複製する条件に対応するチェックボックスをオンにして、[複製（Duplicate）] をクリックします。

[単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）ページが表示されます。このポリシーの名前を変更できます。

- [名前（Name）] : この単純条件の新しい名前を入力するか、または必要に応じて次のフィールドの 1 つ以上の値を変更して新しい単純条件ポリシーを定義できます。
- [説明（Description）] : 単純条件の説明を入力します。
- [属性（Attribute）] : ディクショナリ オプションのドロップダウン リストからディクショナリを選択し、対応する属性の選択肢から属性を選択する場合にクリックします。
- [演算子（Operator）] : [等しい（Equals）] または [等しくない（Not Equals）] を選択します。
- [値（Value）] : 選択した属性に一致する値を入力します。

ステップ 3　[送信（Submit）] をクリックして変更を Cisco ISE データベースに保存し、この許可条件を作成します。

（注）　単純条件の [名前（Name）]、[属性（Attribute）]、[演算子（Operator）]、および [値（Value）] フィールドは必須であり、アスタリスク（*）が付いています。

（注）　複合条件は、さまざまな [等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] の演算子および「AND」と「OR」のディレクティブを含む 1 つ以上の単純条件で構成され、既存の単純条件上に構築されます。新しい複合条件を作成する手順は、単純条件を作成する手順とプロセスに従います。複合条件の詳細については、「複合条件」（P.17-19）を参照してください。

（注）　[一致（Matches）] 演算子では、ワイルドカードではなく正規表現（REGEX）がサポートされ、使用されます。

既存の許可ポリシー要素条件の削除

この手順を使用して、既存の許可ポリシー要素条件を削除します。

既存の許可ポリシー要素条件を削除するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の設定済み許可ポリシー要素条件がすべて示されます。

ステップ 2　既存の条件を削除するには、削除する条件に対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。

- 確認用のダイアログが表示され、選択した項目を削除するかどうかを確認するメッセージが表示されます。
- [削除（Delete）] をクリックして、この許可条件を削除することを確認します（または [キャンセル（Cancel）] をクリックして操作を終了します）。

既存の許可ポリシー要素条件の検索

この手順を使用して、目的の検索基準と一致する既存の許可ポリシー要素条件を検索します。

既存の許可ポリシー要素条件を検索するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]（または [複合条件（Compound Conditions）]）を選択します。

[条件（Conditions）] ページが表示され、既存の設定済み許可ポリシー要素条件がすべて示されます。

ステップ 2　既存の許可ポリシー条件における、特定の値を検索するには、[フィルタ（Filter）] をクリックし、[クイック フィルタ（Quick Filter）] または [拡張フィルタ（Advanced Filter）] のいずれかを選択します。

- [クイック フィルタ（Quick Filter）] を選択した場合、指定した条件名または説明属性値と一致する許可ポリシー条件を検索できます。
  - [名前（Name）] または [説明（Description）] フィールドのいずれかに検索する値を入力します。
  - 指定した条件名または説明と一致する属性が [条件（Conditions）] テーブルに表示されます。
- [拡張フィルタ（Advanced Filter）] を選択した場合、次の検索ルールで設定する属性、演算子、および値のフィールドと一致するさまざまな許可ポリシー条件を使用して検索できます。
  - [フィルタ（Filter）] ドロップダウン リストから、[名前（Name）] または [説明（Description）] を選択します。
  - 演算子ドロップダウン リストから、次のいずれかのオプションを選択します。[次を含む（Contains）]、[次を含まない（Does not contain）]、[等しくない（Does not equal）]、[次で終わる（Ends with）]、[空白（Is empty）]、[次に等しい（Is exactly (or equals)）]、[空白ではない（Is not empty）]、または [次で始まる（Starts with）]。
  - フィルタリングする検索値と一致する属性を入力します。追加ルールを追加できます。
- [実行（Go）] をクリックして [条件（Conditions）] テーブルに一致する条件を表示します。

時刻と日付の条件の設定

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

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、作成した属性設定で目的とした特定の時刻と日付に設定または制限できます。次のトピックでは、時刻と日付の属性に関連するタスクを実行する手順について説明します。

- 「既存の時刻と日付の条件の表示」（P.17-24）
- 「新しい時刻と日付の条件の作成」（P.17-25）
- 「既存の時刻と日付の条件の変更」（P.17-26）
- 「既存の時刻と日付の条件の削除」（P.17-26）
- 「既存の時刻と日付の条件の複製」（P.17-27）
- 「既存の時刻と日付の条件の検索」（P.17-27）

既存の時刻と日付の条件の表示

この手順を使用して、既存のすべての時刻と日付のポリシー要素条件を表示します。

既存のすべての時刻と日付の条件を表示するには、[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

新しい時刻と日付の条件の作成

この手順を使用して、新しい時刻と日付のポリシー要素条件を作成します。

新しい時刻と日付の条件を作成するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

ステップ 2　新しい時刻と日付の条件を作成するには、[追加（Add）] をクリックします。

[時刻と日付の条件（Time and Date Condition）] ページが表示されます。

ステップ 3　次のフィールドに値を入力して新しい時刻と日付の条件を定義します。

- [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。

（注）　[標準設定（Standard Settings）] ペインまたは [例外（Exceptions）] ペインのオプションを使用して時刻と日付の条件を作成することを選択できます。

- [標準設定（Standard Settings）] ペインのオプションの使用を選択した場合：設定する時刻と日付の条件に対応するオプションを選択します。
  - [終日（All Day）]（デフォルトのオプション）または [特定の時間（Specific Hours）]（このオプションでは、時、分、および AM/PM を設定して時間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）。
  - [毎日（Every Day）]（デフォルトのオプション）または [特定の曜日（Specific Days）]（このオプションでは、1 つ以上の曜日を設定するために使用できるチェックボックスが提供されます）。
  - [開始日と終了日なし（No Start and End Dates）]（デフォルトのオプション）、または [特定の日付範囲（Specific Date Range）]（このオプションでは、月、日、および年を設定して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）。または、[特定の日付（Specific Date）]（このオプションでは、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）。
- [例外（Exceptions）] ペインのオプションの使用を選択した場合：設定する時刻と日付の条件に対応するオプションを選択します。
  - [時間範囲（Time Range）]（このオプションでは、時、分、および AM/PM を設定して時間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）。
  - [曜日（Week Days）]（このオプションでは、1 つ以上の曜日を設定するために使用できるチェックボックスが提供されます）。
  - [日付範囲（Date Range）]（2 つのオプションが提供されます）。

    [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。

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE データベースに保存し、この時刻と日付の条件を作成します。

（注）　時刻と日付の条件の [条件名（Condition Name）] フィールドは必須であり、アスタリスク（*）が付いています。

既存の時刻と日付の条件の変更

この手順を使用して、既存の時刻と日付のポリシー要素条件を変更します。

既存の時刻と日付の条件を変更するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

ステップ 2　既存の時刻と日付の条件を編集するには、変更する条件に対応するチェックボックスをオンにして、[編集（Edit）] をクリックします。

[時刻と日付の条件（Time and Date Condition）] ページが表示されます。必要に応じて次のフィールドのオプションおよび設定を変更します（「新しい時刻と日付の条件の作成」（P.17-25）のフィールドとオプションの説明を参照）。

- 条件名（Condition Name）
- 説明（Description）
- 標準設定（Standard Settings）または例外（Exceptions）（選択したパネルのオプション セットを使用）

ステップ 3　[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この変更した時刻と日付の条件を作成します。

（注）　時刻と日付の条件の [条件名（Condition Name）] フィールドは必須であり、アスタリスク（*）が付いています。

既存の時刻と日付の条件の削除

この手順を使用して、既存の時刻と日付のポリシー要素条件を削除します。

既存の時刻と日付の条件を削除するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

ステップ 2　既存の条件を削除するには、削除する時刻と日付の条件に対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。

- 確認用のダイアログが表示されます。

- [OK] をクリックして、選択した時刻と日付の条件を削除することを確認します（または [キャンセル（Cancel）] をクリックして操作を終了します）。
- 条件が正常に削除されたことを示すダイアログが表示されます。

既存の時刻と日付の条件の複製

この手順を使用して、既存の時刻と日付のポリシー要素条件を複製し、これから新しい時刻と日付の条件を作成できます。

既存の時刻と日付の条件を複製するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

ステップ 2　既存の時刻と日付の条件を複製するには、複製する条件に対応するチェックボックスをオンにして、[複製（Duplicate）] をクリックします。

[時刻と日付の条件（Time and Date Conditions）] ページが表示されます。必要に応じて、上部パネルで次の条件を変更できます。

- [名前（Name）] : この条件の新しい名前を入力するか、または必要に応じて次のフィールドの 1 つ以上の値を変更して新しい時刻と日付の条件を定義できます。
- [説明（Description）] : 時刻と日付の条件の説明を入力します。

ステップ 3　[標準設定（Standard Settings）] パネルで、必要に応じて次の値を変更します。

- 終日（All Day）
- 特定の時間（Specific Hours）（プルダウン オプションを使用して HH:MM:AM/PM で特定の時間範囲を設定）
- 毎日（Every Day）
- 特定の曜日（Specific Days）（目的の日と一致するチェックボックスをオンにする）
- 開始日と終了日なし（No Start and End Date）
- 特定の日付範囲（Specific Date Range）（プルダウン オプションを使用して特定の月：日：年の範囲を設定）
- 特定の日付（Specific Date）（プルダウン オプションを使用して特定の月：日：年の日付を設定）

ステップ 4　[保存（Save）] をクリックして、変更を Cisco ISE データベースに保存し、この許可条件を作成します。

（注）　時刻と日付の条件の [条件名（Condition Name）] フィールドは必須であり、アスタリスク（*）が付いています。

既存の時刻と日付の条件の検索

この手順を使用して、目的の検索基準と一致する既存の日付と時刻のポリシー要素条件を検索します。

既存の時刻と日付の条件を検索するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[時刻と日付の条件（Time and Date Conditions）] ページが表示され、既存の設定済みの時刻と日付の条件がすべて示されます。

ステップ 2　既存の日付と時刻の条件における、特定の値を検索するには、[フィルタ（Filter）] をクリックし、[クイック フィルタ（Quick Filter）] または [拡張フィルタ（Advanced Filter）] のいずれかを選択します。

- [クイック フィルタ（Quick Filter）] を選択した場合、指定した条件名または説明属性値と一致する時刻と日付の条件を検索できます。
  - [条件名（Condition Name）] フィールドまたは [説明（Description）] フィールドに目的の検索属性値を入力します。
  - 指定した条件名または説明と一致する属性が [時刻と日付の条件（Time and Date Conditions）] テーブルに表示されます。
- [拡張フィルタ（Advanced Filter）] を選択した場合、指定した属性値と一致するさまざまな時刻と日付の条件を検索できます。
  - 適切なフィールドに目的の検索属性値を入力します。
  - 指定した検索値と一致する属性が [時刻と日付の条件（Time and Date Conditions）] テーブルに表示されます。

許可プロファイルの権限の設定

許可プロファイルの権限の設定を始める前に、許可ポリシーとプロファイルの関係を理解していること、[許可プロファイル（Authorization Profile）] ページの知識があること、ポリシーおよびプロファイルを設定する場合に従う基本的なガイドラインを知っていること、許可プロファイルの権限が何によって構成されるかを理解していること、および次のトピックで説明する設定デフォルト値について認識していることを確認します。

- 「Cisco ISE 許可ポリシーおよびプロファイル」（P.17-5）
- 「[許可プロファイル（Authorization Profile）] ページ」（P.17-8）
- 「許可ポリシーおよびプロファイルのガイドライン」（P.17-9）
- 「許可ポリシー、ルール、およびプロファイルの設定のデフォルト」（P.17-10）

ネットワークでさまざまなタイプの許可プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として [結果（Results）] ナビゲーション ペインを使用します。次のトピックでは、次の作業を実行するための手順について説明します。

- 「既存の許可プロファイルおよび権限の表示」（P.17-29）
- 「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）
- 「既存の許可プロファイルの変更」（P.17-32）
- 「既存の許可プロファイルの削除」（P.17-32）
- 「既存の許可プロファイルの複製」（P.17-33）
- 「既存の許可プロファイルの検索」（P.17-34）

（注）　[結果（Results）] ペインには、最初 [認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[クライアント プロビジョニング（Client Provisioning）]、および [セキュリティ グループ アクセス（Security Group Access）] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク（Common Tasks）] 設定を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク（Common Tasks）] 属性の値を入力する必要があります。

既存の許可プロファイルおよび権限の表示

この手順を使用して、既存の許可プロファイルの権限を表示します。

（注）　[結果（Results）] ナビゲーション ペインには、[許可（Authorization）] の下に [許可プロファイル（Authorization Profiles）]、[ダウンロード可能 ACL（Downloadable ACL）]、および [インライン ポスチャ ノード（Inline Posture node）] のオプションが表示されます。

許可プロファイルの既存の権限を表示するには、[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

新しい標準許可プロファイルの権限の作成および設定

この手順を使用して、新しい標準許可プロファイルを作成し、その権限を設定します。

新しい標準許可プロファイルおよび権限を作成するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

ステップ 2　新しいプロファイルを作成するには、次の 2 つの方法のいずれかを選択します。

- [許可（Authorization）] ペインで、[操作（action）]（アイコン）をクリックし、[標準許可プロファイルを作成（Create Standard Authorization Profile）] をクリックします

  または

- [標準許可プロファイル（Standard Authorization Profiles）] ページで、[追加（Add）] をクリックします

[許可プロファイル（Authorization Profiles）] > [新しい許可プロファイル（New Authorization profile）] ページが表示されます。

ステップ 3　必要に応じて、次のカラムおよびフィールドに値を入力し、新しい許可プロファイルを作成します。

- **許可プロファイル（Authorization Profile）**
  - [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）] : 2 つのドロップダウン リストのアクセス タイプ オプション（[ACCESS_ACCEPT] または [ACCESS_REJECT]）から選択します。

（注）　[名前（Name）] および [アクセス タイプ（Access Type）] フィールドは必須であり、アスタリスク（*）が付いています。

- **共通タスク（Common Tasks）**
  - [DACL 名（DACL Name）] : 選択するには、チェックボックスをオンにし、ドロップダウン リストから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）。ドロップダウン 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] : 選択するには、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）] : 選択するには、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）] : 選択するには、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。
  - [中央集中 Web 認証（Centralized Web Authentication）] : 選択するには、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、[リダイレクト（Redirect）] ドロップダウン リストから [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。
  - [Auto SmartPort] : 選択するには、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。選択が [属性詳細（Attributes Details）] ペインに反映されます。

- [フィルタ ID（Filter-ID）] : 選択するには、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。選択が [属性詳細（Attributes Details）] ペインに反映されます。
- [再認証（Reauthentication）] : 選択するには、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）またはドロップダウン リストから [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）] : 選択するには、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、対応するドロップダウン リストから次の 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] : 選択するには、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（Web Authentication）]（[ローカル Web 認証（Local Web Auth）]）: 選択するには、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)）] : 選択するには、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] : 選択するには、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。ドロップダウン [属性（Attribute）] リストから値を選択してこの設定を行います。たとえば、[Cisco-BBSM] を選択し、続いて [CBBSM-Bandwidth] を選択した場合、これは、[属性詳細（Attributes Details）] ペインに Class = Cisco-BBSM:CBBSM-Bandwidth として反映されます。

（注）　[名前（Name）] および [アクセス タイプ（Access Type）] フィールドは必須であり、アスタリスク（*）が付いています。

- **高度な属性設定（Advanced Attributes Settings）**
  - 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。
  - 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 番目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。

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

既存の許可プロファイルの変更

この手順を使用して、既存の許可プロファイルの権限を変更します。

既存の許可プロファイルの権限を変更するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

ステップ 2　既存の許可プロファイルの権限を編集するには、変更する既存の許可プロファイルに対応するチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3　[許可プロファイル（Authorization Profile）]、[共通タスク（Common Tasks）]、[高度な属性設定（Advanced Attributes Settings）]、および [属性詳細（Attributes Details）] カラムの値を必要に応じて変更します。

ステップ 4　[保存（Save）] をクリックして、変更を Cisco ISE データベースに保存し、この許可プロファイルを作成します。

詳細情報：

- [許可プロファイル（Authorization Profile）]、[共通タスク（Common Tasks）]、[高度な属性設定（Advanced Attributes Settings）]、および [属性詳細（Attributes Details）] カラムの値の詳細については、「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）の説明を参照してください。

既存の許可プロファイルの削除

この手順を使用して、既存の許可プロファイルを削除します。対応するポリシー要素の権限も削除されます。

既存の許可プロファイルを削除するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

ステップ 2　既存の許可プロファイルを削除するには、削除する既存の許可プロファイルに対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。

削除確認用のダイアログが表示され、許可プロファイルが削除されることを警告します。

ステップ 3　[OK] をクリックして、この許可プロファイルを Cisco ISE システム データベースから削除することを確認します。

既存の許可プロファイルの複製

この手順を使用して、既存の許可プロファイルを複製し、これから新しい許可プロファイルを作成できます。

既存の許可プロファイルを複製するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

ステップ 2　既存の許可を複製するには、複製する許可プロファイルに対応するチェックボックスをオンにして、[複製（Duplicate）] をクリックします。

[許可プロファイル（Authorization Profiles）] ページが表示されます。

ステップ 3　[許可プロファイル（Authorization Profile）]、[共通タスク（Common Tasks）]、[高度な属性設定（Advanced Attributes Settings）]、および [属性詳細（Attributes Details）] カラムの値を必要に応じて変更します。

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE データベースに保存し、新しい許可プロファイルを作成します。

（注）　[名前（Name）] および [アクセス タイプ（Access Type）] フィールドの値は必須であり、アスタリスク（*）が付いています。

詳細情報：

- [許可プロファイル（Authorization Profile）]、[共通タスク（Common Tasks）]、[高度な属性設定（Advanced Attributes Settings）]、および [属性詳細（Attributes Details）] カラムの値の詳細については、「新しい標準許可プロファイルの権限の作成および設定」（P.17-29）の説明を参照してください。

既存の許可プロファイルの検索

この手順を使用して、目的の検索基準と一致する既存の許可プロファイル条件を検索します。

既存の許可プロファイルを検索するには、次の手順を実行します。

ステップ 1　[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）] を選択します。

[許可プロファイル（Authorization Profiles）] ページが表示され、既存の設定済み許可プロファイルがすべて示されます。

ステップ 2　既存の許可ポリシー条件における、特定の値を検索するには、[フィルタ（Filter）] をクリックし、[クイック フィルタ（Quick Filter）] または [拡張フィルタ（Advanced Filter）] のいずれかのオプションを選択します。

[クイック フィルタ（Quick Filter）] を選択した場合、指定した名前または説明値と一致する許可プロファイルを検索できます。

- [名前（Name）] または [説明（Description）] フィールドに検索する値を入力します。

指定した許可プロファイル名または説明と一致する属性が [条件（Conditions）] テーブルに表示されます。

- [拡張フィルタ（Advanced Filter）] を選択した場合、次の検索ルールで設定する属性、演算子、および値のフィールドと一致する許可プロファイルを検索できます。
  - [フィルタ（Filter）] ドロップダウン リストから、[名前（Name）] または [説明（Description）] を選択します。
  - 演算子ドロップダウン リストから次のオプションを選択します。[次を含む（Contains）]、[次を含まない（Does not contain）]、[等しくない（Does not equal）]、[次で終わる（Ends with）]、[空白（Is empty）]、[次に等しい（Is exactly (or equals)）]、[大なり（Is greater than）]、[以上（Is greater than or equal to）]、[小なり（Is less than）]、[以下（Is less than or equal to）]、[空白ではない（Is not empty）]、または [次で始まる（Starts with）]。
  - フィルタリングする検索値と一致する属性を入力します。追加ルールを追加できます。
- [実行（Go）] をクリックして [条件（Conditions）] テーブルに一致する条件を表示します。

ダウンロード可能 ACL の権限の設定

ダウンロード可能 ACL（DACL）のポリシー要素権限を表示、作成、変更、または削除できるプロセスを開始するには、Cisco ISE ユーザ インターフェイスでそのナビゲーション ペインを探す必要があります。これを行うには、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] を選択して、[許可（Authorization）] ナビゲーション ペインを表示します。

[許可（Authorization）] ナビゲーション ペインには最初、次の要素が表示されています。

- 許可プロファイル（Authorization Profiles）
- ダウンロード可能 ACL（Downloadable ACLs）
- インライン ポスチャ ノード プロファイル（Inline Posture Node Profiles）

詳細情報：

- DACL 用の権限の設定および DACL の管理の詳細については、「DACL の設定」（P.17-35）を参照してください。

DACL の設定

次のトピックでは、DACL の権限を設定する手順について説明します。

DACL の既存の権限の表示

この手順を使用して、既存の DACL の権限を表示します。

既存の DACL 権限を表示するには、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

新しい DACL の権限の作成および設定

この手順を使用して、新しい DACL を作成し、その権限を設定します。

新しい DACL の権限を設定するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

ステップ 2　新しい DACL を作成するには、[操作（action）]（アイコン）をクリックし、[DACL の作成（Create DACL）] を選択するか、または [DACL 管理（DACL Management）] ページで [追加（Add）]（+）をクリックします。

ステップ 3　次のフィールドで DACL の値を入力します。

- [名前（Name）] : DACL を識別する名前を入力します。
- [説明（Description）] : DACL の説明を入力します。
- [DACL コンテンツ（DACL Content）] : ACL に目的のコンテンツのタイプを入力します（IPPermit または IPDeny のいずれか）。

（注）　[名前（Name）] および [DACL コンテンツ（DACL Content）] フィールドには値を入力する必要があり、アスタリスク（*）が付いています。

ステップ 4　[送信（Submit）] をクリックして設定した値を Cisco ISE データベースに保存し、この DACL を作成します。

既存の DACL の権限の変更

この手順を使用して、既存の DACL の権限を変更します。

既存の DACL の権限を変更するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

ステップ 2　既存の DACL を編集するには、変更する DACL に対応するチェックボックスをオンにして、[編集（Edit）] をクリックします。

[DACL 管理（DACL Management）] ページが表示されます。

ステップ 3　必要に応じて次のフィールドで DACL の値を変更します。

- [名前（Name）] : DACL を識別する名前を入力します。
- [説明（Description）] : DACL の説明を入力します。
- [DACL コンテンツ（DACL Content）] : ACL で目的のコンテンツのタイプを選択します（IPPermit または IPDeny のいずれか）。

（注）　[名前（Name）] および [DACL コンテンツ（DACL Content）] フィールドには値を入力する必要があり、アスタリスク（*）が付いています。

ステップ 4　[送信（Submit）] をクリックして設定した値を Cisco ISE データベースに保存し、この変更した DACL を作成します。

既存の DACL の削除

この手順を実行して、既存の DACL を削除します。

既存の ACL を削除するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

ステップ 2　既存の DACL を削除するには、削除する DACL に対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。

削除確認用のダイアログが表示されます。

ステップ 3　[OK] をクリックして、DACL を削除することを確認するか、または [キャンセル（Cancel）] をクリックして操作を終了します。

既存の DACL の複製

この手順を使用して、既存の DACL を複製し、これから新しい DACL を作成できます。

既存の DACL を複製するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

ステップ 2　既存の DACL を複製するには、複製する DACL に対応するチェックボックスをオンにして、[複製（Duplicate）] をクリックします。

[ダウンロード可能 ACL（Downloadable ACL）] ページが表示されます。

ステップ 3　必要に応じて、[名前（Name）]、[説明（Description）]、[DACL コンテンツ（DACL Content）] のフィールドの値を変更します。

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE データベースに保存し、新しい許可プロファイルを作成します。

（注）　[名前（Name）] および [DACL コンテンツ（DACL Content）] フィールドには値を入力する必要があり、アスタリスク（*）が付いています。

既存の DACL の検索

この手順を使用して、設定と一致する既存の DACL 値を検索する基準を使用して、既存の DACL を検索します。

既存の DACL を検索するには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

[DACL 管理（DACL Management）] ページが表示され、既存の設定済みの DACL がすべて示されます。

ステップ 2　既存の DACL における、特定の値を検索するには、[フィルタ（Filter）] をクリックし、[クイック フィルタ（Quick Filter）] または [拡張フィルタ（Advanced Filter）] のいずれかのオプションを選択します。

[クイック フィルタ（Quick Filter）] を選択した場合、指定した名前または説明値と一致する DACL 値を検索できます。

- [名前（Name）] または [説明（Description）] フィールドに検索する値を入力します。

指定した DACL 名または説明と一致する属性が [条件（Conditions）] テーブルに表示されます。

- [拡張フィルタ（Advanced Filter）] を選択した場合、次の検索ルールで設定する属性、演算子、および値のフィールドと一致する DACL を検索できます。
  - [フィルタ（Filter）] ドロップダウン リストで、[名前（Name）] または [説明（Description）] のいずれかを選択します。
  - 演算子ドロップダウン リストで、次のオプションから選択します。[次を含む（Contains）]、[次を含まない（Does not contain）]、[等しくない（Does not equal）]、[次で終わる（Ends with）]、[空白（Is empty）]、[次に等しい（Is exactly (or equals)）]、[空白ではない（Is not empty）]、または [次で始まる（Starts with）]。
  - フィルタリングする検索値と一致する属性を入力します。追加ルールを追加できます。
- [実行（Go）] をクリックして [条件（Conditions）] テーブルに一致する条件を表示します。

SGACL 用ポリシーの設定

セキュリティ グループ アクセス コントロール リスト（SGACL）用ポリシーを設定する方法については、「Cisco Security Group Access のポリシー」（P.23-1）を参照してください。

マシン アクセス制限および Active Directory ユーザ

Cisco ISE には、Microsoft Active Directory 認証ユーザの許可を制御する追加の方法を提供する、マシン アクセス制限（MAR）コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性（属性 31）で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定（Active Directory Settings）] ページの [存続可能時間（Time to Live）] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザをエンドユーザ クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザ認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザ認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てる必要があります。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザ認証の許可プロファイルを割り当てる必要があります。

詳細情報

- 詳細については、「マシン認証」（P.5-5）を参照してください。