CHAPTER 19

認証ポリシーの管理

Cisco Identity Services Engine（Cisco ISE）管理者ポータルのユーザ インターフェイスを使用して、ネットワーク上のリソースにアクセスできるユーザを特定する認証ポリシーを定義できます。この章は次のトピックで構成されています。

C シスコ ISE 認証ポリシー

認証ポリシーは、Cisco ISE がネットワーク デバイスと通信するために使用するプロトコルを定義します。また、認証に使用するソースを特定します。ポリシーは、一連の条件と結果で構成されています。ポリシー条件は、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。複合条件は、1 つ以上の単純条件で構成され、それぞれの条件が AND または OR 演算子で結合されています。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。

認証ポリシーは次の要素で構成されています。

- ネットワーク アクセス サービス：このサービスは次のいずれかとなります。
  - 許可されるプロトコル サービス。初期要求およびプロトコル ネゴシエーションを処理するためのプロトコルを選択します。
  - プロキシ サービス。外部 RADIUS サーバが処理を行うように要求をプロキシします。
- ID ソース：認証に使用する ID ソースまたは ID ソース順序。

インストール後に、認証に使用される Cisco ISE でデフォルトの ID 認証ポリシーが使用できます。認証ポリシーを更新すると、デフォルトの設定が上書きされます。

関連項目

- 「ポリシー状態の評価」（P.19-2）
- 「サポートされる認証プロトコル」（P.19-2）
- 「サポートされる認証タイプおよびデータベース」（P.19-2）
- 「認証失敗 のタイプ」（P.19-3）
- 「認証ポリシーの用語」（P.19-4）

ポリシー状態の評価

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」という条件の場合に 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。

サポートされる認証プロトコル

認証ポリシーの定義時に選択可能なプロトコルを次に示します。

- Password Authentication Protocol（PAP）
- Protected Extensible Authentication Protocol（PEAP）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Extensible Authentication Protocol-Message Digest 5（EAP-MD5）
- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）
- Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）

ここでは、次のトピックについて説明します。

- 「サポートされる認証タイプおよびデータベース」（P.19-2）
- 「認証ポリシーの用語」（P.19-4）
- 「簡易認証ポリシー」（P.19-4）
- 「ルールベースの認証ポリシー」（P.19-6）

サポートされる認証タイプおよびデータベース

認証タイプは、選択されたプロトコルに基づきます。表 14-1（P.14-7）に、各種データベースでサポートされる認証タイプおよびプロトコルを示します。

認証タイプはパスワード ベースです。認証は、要求内に存在するユーザ名とパスワードを使用してデータベースに対して実行されます。認証ポリシーの結果である ID 特定方法は、次のいずれかになります。

- アクセスを拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID データベース：次のいずれかの単一の ID データベース。
  - 内部ユーザ
  - ゲスト ユーザ
  - 内部エンドポイント
  - Active Directory
  - Lightweight Directory Access Protocol（LDAP）データベース
  - RADIUS トークン サーバ（RSA または SafeWord サーバ）
  - 証明書認証プロファイル
- ID ソース順序：認証に使用する ID データベースの順序。

デフォルトでは、Cisco ISE がユーザ情報の検索に使用する ID ソースは、内部のユーザ データベースです。

認証失敗 のタイプ

識別方法としてアクセス拒否を選択した場合、要求への応答として拒否メッセージが送信されます。ID データベースまたは ID データベース順序を選択して、認証が成功した場合、認証ポリシーの処理が続行されます。一部の認証は失敗し、その場合次のように分類されます。

- 認証の失敗：クレデンシャルが正しくない、無効なユーザであることなどが原因で認証が失敗したことを示す明確な応答を受信します。アクションのデフォルト コースは拒否です。
- ユーザが見つからない：どの ID データベースでもこのユーザが見つかりませんでした。アクションのデフォルト コースは拒否です。
- 処理の失敗：ID データベース（複数の場合もある）にアクセスできません。アクションのデフォルト コースはドロップです。

Cisco ISE では、認証失敗に対して次のアクションのコースのいずれかを設定することができます。

- 拒否：拒否応答が送信されます。
- ドロップ：応答は送信されません。
- 続行：認可ポリシーに従って Cisco ISE を継続します。

[続行（Continue）] オプションを選択した場合でも、使用されているプロトコルの制限により Cisco ISE が要求の処理を実行できない場合があります。認証に失敗した場合、PAP/ASCII、EAP-TLS、または MAC 認証バイパス（MAB またはホスト ルックアップ）の認証ポリシーの処理を続行できます。

その他のすべての認証プロトコルの場合、認証に失敗すると、次のいずれかの状態となります。

- 認証の失敗：拒否応答が送信されます。
- ユーザまたはホストが見つからない：拒否応答が送信されます。
- 処理に問題が発生：応答は送信されず、要求はドロップされます。

認証ポリシーの用語

以下は認証ポリシー ページの一般用語の一部です。

- 許可されるプロトコル：許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。
- アイデンティティ ソース：Cisco ISE データベースがユーザ情報に使用する ID ソースを定義します。データベースは内部データベースの場合や、Active Directory または LDAP などの外部 ID ソースの場合もあります。一連のデータベースを ID ソース順序に加えて、この順序をポリシー内で ID ソースとしてリストできます。Cisco ISE は、リストされている順序でデータベース内のクレデンシャルを検索します。
- フェールオーバー オプション：認証に失敗した、ユーザが見つからない、または処理に失敗した場合に Cisco ISE が取るべきアクションのコースを指定できます。

簡易認証ポリシー

簡易認証ポリシーでは、Cisco ISE が通信に使用する、許可されるプロトコルおよび ID ソースまたは ID ソース順序を静的に定義できます。簡易ポリシーでは条件を定義できません。Cisco ISE ではすべての条件が満たされていると想定され、次の定義を使用して結果が決まります。

- 常に使用する必要がある許可されるプロトコルおよび ID ソースを静的に定義でき、条件のチェックが必要ない環境では、簡易ポリシーを作成できます。
- プロキシ サービスベースの簡易ポリシーを作成することもできます。Cisco ISE は、ポリシー サーバに要求をプロキシして、ユーザ認証に使用する ID ソースを決定します。要求が別のポリシー サーバにプロキシされた場合、プロトコル ネゴシエーションは発生しません。ポリシー サーバはどの ID ソースを認証に使用するべきかを評価し、応答を Cisco ISE に返します。

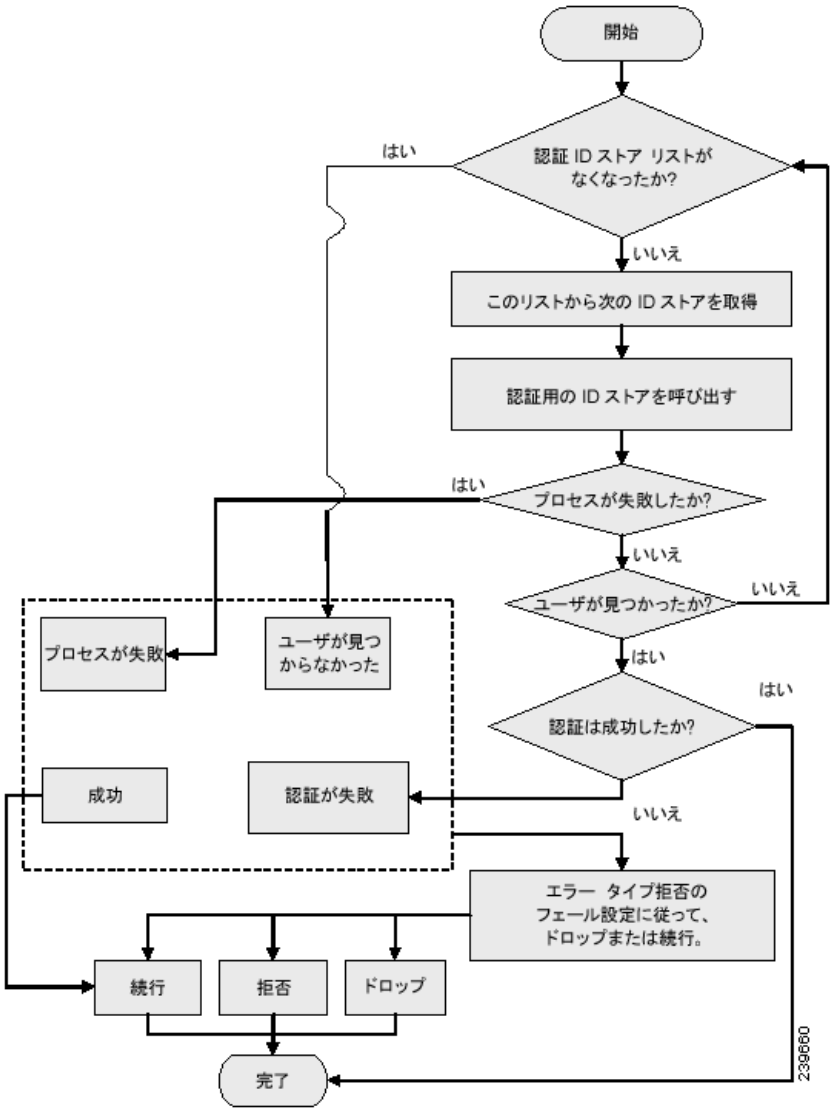
簡易認証ポリシーの設定手順には、許可されるプロトコル サービスの定義および簡易認証ポリシーの設定が含まれます。許可されるプロトコル サービスの作成方法については、「ネットワーク アクセス用の許可されるプロトコルの定義」（P.19-15）を参照してください。

関連項目

- 「簡易認証ポリシーのフロー」（P.19-5）
- 「簡易認証ポリシー設定のガイドライン」（P.19-6）
- 「簡易認証ポリシーの設定」（P.19-23）
- 「ルールベースの認証ポリシー」（P.19-6）

簡易認証ポリシーのフロー

図 19-1　簡易認証ポリシーのフロー



簡易ポリシーの結果は、次のどちらかになります。

- 認証に成功しました
- 認証に失敗しました

認証は次のいずれかの原因で失敗することがあります。

- 正しくないクレデンシャルまたは無効なユーザです。
- ユーザが見つかりません。
- 認証プロセスが失敗しました。

簡易認証ポリシー設定のガイドライン

簡易認証ポリシーの設定中に従うべきガイドラインは、次のとおりです。

- RADIUS サーバ順序を使用する場合は、このアクセス サービスを定義してからポリシーを定義する必要があります。詳細については、「RADIUS プロキシ サーバとして機能する CIsco ISE」（P.19-19）を参照してください。
- ユーザが外部 ID ソースで定義されている場合、ポリシーを定義する前に Cisco ISE でこれらの ID ソースが設定されていることを確認してください。外部 ID ソースの設定方法については、「ユーザおよび外部 ID ソースの管理」（P.14-1）を参照してください。
- ID ソース順序を使用してユーザを認証する場合、ポリシーを定義する前に、ID ソース順序が作成済みであることを確認してください。詳細については、「ID ソース順序の作成」（P.14-40）を参照してください。
- 簡易ポリシーとルールベースのポリシーを切り替える場合、最初に設定したポリシーは失われます。たとえば、簡易認証ポリシーを設定した後でルールベースの認証ポリシーに移動すると、簡易認証ポリシーは失われます。また、ルール ベースの認証ポリシーから簡易認証ポリシーに移動した場合は、ルール ベースの認証ポリシーは失われます。
- ホスト認証は、MAC アドレスのみを使用して実行されます（MAB）。

ルールベースの認証ポリシー

ルールベースの認証ポリシーは、属性ベースの条件で構成されています。この条件により、要求の処理に使用される許可されるプロトコルおよび ID ソースまたは ID ソース順序が決定されます。簡易認証ポリシーでは、許可されるプロトコルおよび ID ソースを静的に定義できます。ルールベースのポリシーでは、条件を定義することによって、Cisco ISE は許可されるプロトコルおよび ID ソースを動的に選択できるようになります。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。ポリシー条件で使用できる、ディクショナリによってサポートされる固定属性をリストした表 19-1 を参照してください。

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。ポリシー作成ページ内で条件を作成することも可能です。条件には 2 種類あります。

- 簡易条件
- 複合条件

関連項目

- 「単純および複合条件」（P.18-1）
- 「単純条件の作成」（P.18-2）
- 「複合条件の作成」（P.18-3）
- 「ルール ベースの認証ポリシーの設定」（P.19-23）

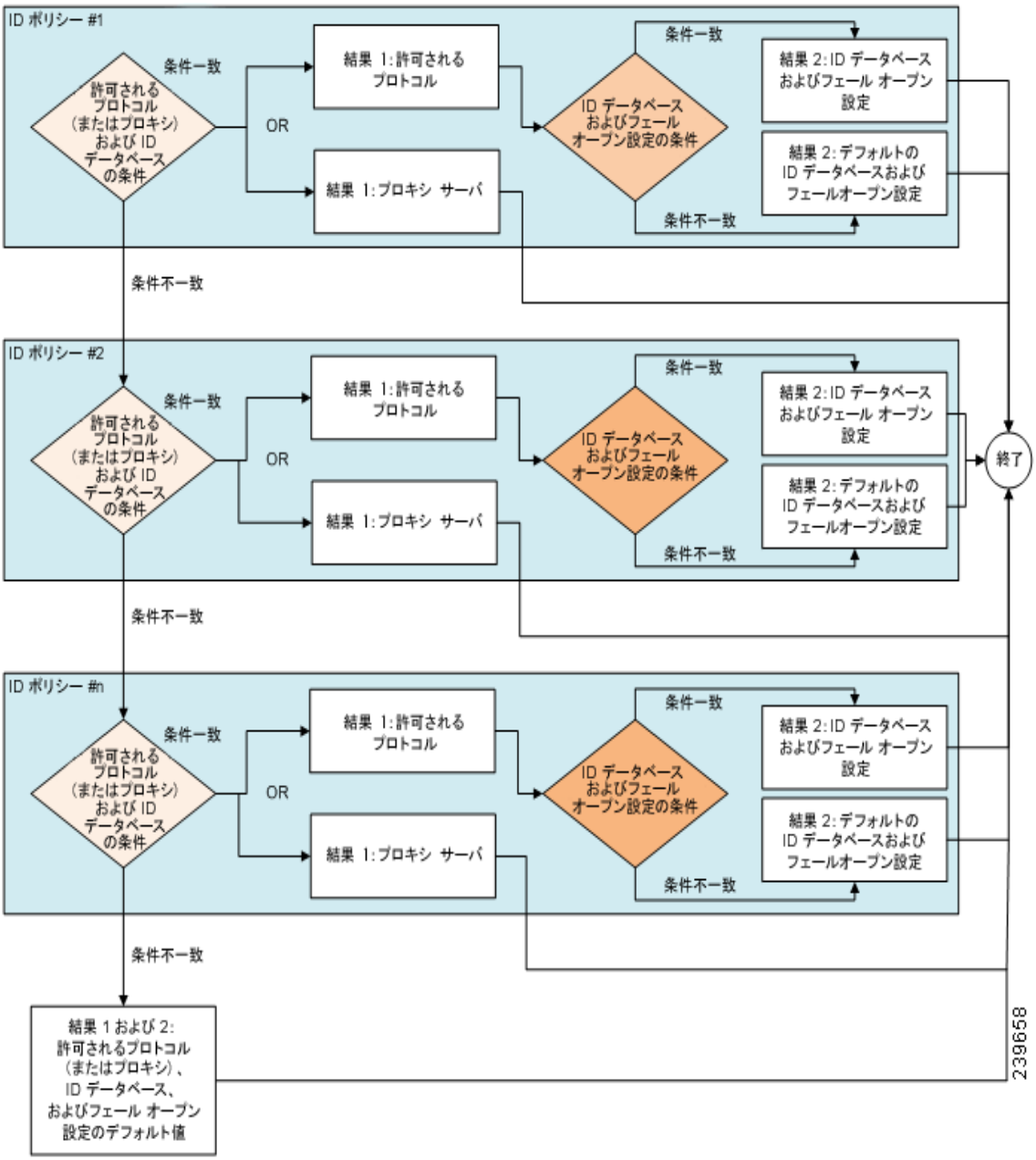
ルールベースの認証ポリシーのフロー

ルールベースのポリシーでは、図 19-2 に示すように複数のルールを定義できます。ID データベースは、基準に一致する最初のルールに基づいて選択されます。

異なるデータベースで構成される ID ソース順序を定義することもできます。Cisco ISE がデータベースを検索する順序を定義できます。Cisco ISE は、認証が成功するまで指定された順序でこれらのデータベースにアクセスします。1 つの外部データベースに同一ユーザの複数のインスタンスが存在する場合、認証は失敗します。1 つの ID ソース内で、ユーザ レコードは重複できません。

ID ソース順序には、3 つのデータベース、または多くとも 4 つのデータベースを使用することを推奨します。

図 19-2　ルールベースの認証ポリシー



ルール ベースの認証ポリシーのサポート ディクショナリ

Cisco ISE は次のディクショナリをサポートします。

- システム定義されたディクショナリ
  - CERTIFICATE
  - DEVICE
  - RADIUS

- RADIUS ベンダー ディクショナリ
  - *Airespace*
  - *Cisco*
  - *Cisco BBSM*
  - *Cisco VPN3000*
  - *Microsoft*
  - *Network Access*

Cisco ISE の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.10-1）を参照してください。

ディクショナリによってサポートされる属性

表 19-1 に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。

作成する条件のタイプによっては、使用できない属性もあります。たとえば、認証ポリシー内でアクセス サービスを選択する条件を作成する場合、使用できるネットワーク アクセス属性は、Device IP Address、ISE Host Name、Network Device Name、Protocol、および Use Case のみです。

表 19-1　ディクショナリによってサポートされる属性のリスト

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Device	Device Type（定義済みのネットワーク デバイス グループ）	Yes	Yes
	Device Location（定義済みのネットワーク デバイス グループ）		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	すべての属性	Yes	Yes

表 19-1　ディクショナリによってサポートされる属性のリスト （続き）

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Network Access	ISE Host Name	Yes	Yes
	AuthenticationMethod	No	Yes
	AuthenticationStatus	No	No
	CTSDeviceID	No	No
	Device IP Address	Yes	Yes
	EapAuthentication（マシンのユーザの認証時に使用される EAP 方式）	No	Yes
	EapTunnel（トンネルの確立に使用される EAP 方式）	No	Yes
	Protocol	Yes	Yes
	UseCase	Yes	Yes
	UserName	No	Yes
	WasMachineAuthenticated	No	No

表 19-1　ディクショナリによってサポートされる属性のリスト （続き）

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Certificate	Common Name	No	Yes
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

認証のプロトコル設定

プロトコルを使用して認証要求を処理するには、初めに Cisco ISE でグローバル プロトコル設定を定義する必要があります。[プロトコル設定（Protocol Settings）] ページを使用して、ネットワーク内の他のデバイスと通信する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）、および Protected Extensible Authentication Protocol（PEAP）の各プロトコルのグローバル オプションを定義できます。ここでは、次のトピックについて説明します。

- 「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）
- 「EAP-FAST 設定の設定」（P.19-12）

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

次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です。

- EAP-FAST 受信クライアント証明書が認証されたプロビジョニングで有効な場合は、EAP-TLS 内部方式を有効にすることを強く推奨します。認証されたプロビジョニングの EAP-FAST 受信クライアント証明書は別の認証方式ではなく、ユーザを認証するのと同じ証明書認証タイプを使用した略式のクライアント証明書認証ですが、内部方式を実行する必要がありません。
- PAC なしの完全なハンドシェイクおよび認定 PAC プロビジョニングとの認証プロビジョニング作業に対するクライアント証明書を受け入れます。PAC なしのセッション再開、匿名 PAC プロビジョニング、PAC ベース認証には動作しません。
- EAP 属性は、認証の順序とは関係なく、ID ごとに監視ツールの認証詳細にまずユーザ順に次にマシン順に表示されます（したがって EAP チェーニングは 2 回表示されます）。
- EAP-FAST 認可 PAC が使用される場合、ライブ ログに表示される EAP 認証方式は完全認証に使用される認証方式と同じ（PEAP でのように）であり、参照としてではありません。
- EAP チェーン モードでは、トンネル PAC が期限切れになると、ISE がプロビジョニングにフォールバックし、AC 要求ユーザおよびマシン認可 PAC（マシン許可 PAC）はプロビジョニングできません。後続の PAC ベースの認証通信で AC が要求したときにプロビジョニングされます。
- Cisco ISE がチェーンに、AC がシングル モードに設定されている場合は、AC は IdentityType TLV で ISE に応答します ただし、2 番目の特定認証は失敗します。この通信から、クライアントのチェーニング実行は適切であるが、現在はシングル モードで構成されていることが分かります。
- Cisco ISE は AD にのみチェーンしている EAP-FAST のマシンとユーザの両方の属性およびグループをサポートします。LDAP および内部 DB ISE に対しては、最新の ID 属性のみを使用します。

EAP-FAST 設定の設定

[グローバル オプション（Global Options）] ページで、EAP-FAST プロトコルのランタイム特性を設定できます。

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システム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] を選択します。

ステップ 2　[EAP-FAST] > [EAP FAST 設定（EAP FAST Settings）] を選択します。

ステップ 3　EAP-FAST プロトコルの定義に必要な詳細を入力します。

ステップ 4　以前に生成されたマスター キーおよび PAC をすべて失効させるには、[失効（Revoke）] をクリックします。

ステップ 5　EAP-FAST 設定を保存するには、[保存（Save）] をクリックします。

関連項目

- 「EAP-FAST 設定」（P.A-23）
- 「EAP-FAST の PAC の生成」（P.19-13）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

EAP-FAST の PAC の生成

Cisco ISE の [PAC の生成（Generate PAC）] オプションを使用して、EAP-FAST プロトコルのトンネル PAC またはマシン PAC を生成できます。

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システム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] の順に選択します。

ステップ 2　左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3　[EAP-FAST] > [PAC の生成（Generate PAC）] を選択します。

ステップ 4　EAP-FAST プロトコルのマシン PAC を生成する場合に必要な詳細を入力します。

ステップ 5　[PAC の生成（Generate PAC）] をクリックします。

関連項目

- 「EAP-FAST の PAC の生成設定」（P.A-24）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

EAP-TLS 設定の設定

[グローバル オプション（Global Options）] ページで、EAP-TLS プロトコルのランタイム特性を設定できます。

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システム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] の順に選択します。

ステップ 2　左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3　[EAP-TLS] を選択します。

ステップ 4　EAP-TLS プロトコルの定義に必要な詳細を入力します。

ステップ 5　EAP-TLS 設定を保存するには、[保存（Save）] をクリックします。

関連項目

- 「EAP-TLS 設定」（P.A-24）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

PEAP 設定の設定

[グローバル オプション（Global Options）] ページで、PEAP プロトコルのランタイム特性を設定できます。

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システム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] の順に選択します。

ステップ 2　左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3　[PEAP] を選択します。

ステップ 4　PEAP プロトコルの定義に必要な詳細を入力します。

ステップ 5　PEAP 設定を保存するには、[保存（Save）] をクリックします。

関連項目

- 「PEAP 設定」（P.A-25）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

RADIUS 設定の設定

認証に失敗、または認証成功のレポートの繰り返しの抑制に失敗したクライアントを検出するように RADIUS 設定を設定することができます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] の順に選択します。

ステップ 2　[設定（Settings）] ナビゲーション ペインで [プロトコル（Protocols）] をクリックします。

ステップ 3　[RADIUS] を選択します。

ステップ 4　RADIUS 設定の定義に必要な詳細を入力します。

ステップ 5　[保存（Save）] をクリックして、設定を保存します。

関連項目

- 「RADIUS 設定」（P.A-25）

ネットワーク アクセス サービス

ネットワーク アクセス サービスには、要求に対する認証ポリシー条件が含まれています。たとえば有線 802.1X や有線 MAB など、さまざまな用途向けに個別のネットワーク アクセス サービスを作成することができます。認証ポリシー内で使用できる次の 2 つのネットワーク アクセス サービスがあります。

- 「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）
- 「RADIUS プロキシ サーバとして機能する CIsco ISE」（P.19-19）

関連項目

- 「簡易認証ポリシー」（P.19-4）
- 「ルール ベースの認証ポリシーの設定」（P.19-23）

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

許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。許可されるプロトコル アクセス サービスは、認証ポリシーを設定する前に作成する必要がある独立したエントリです。許可されるプロトコル アクセス サービスは、特定の使用例に対して選択されたプロトコルが含まれているオブジェクトです。

[許可されるプロトコル サービス（Allowed Protocols Services）] ページには、作成した許可されるプロトコル サービスがすべて表示されます。Cisco ISE で事前に定義されたデフォルトのネットワーク アクセス サービスが存在します。

はじめる前に

この手順を開始する前に、認証に使用するプロトコル サービスの基本を理解している必要があります。

C シスコ ISE 認証ポリシーを確認すれば、各種データベースでサポートされる認証タイプおよびプロトコルが分かります。

PAC オプションを確認して、各プロトコル サービスの機能とオプションを理解し、使用しているネットワークに最適な選択ができるようにしてください。

手順を進める前に、グローバル プロトコル設定を必ず定義してください。詳細については、「認証のプロトコル設定」（P.19-11）を参照してください。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシーの要素（Policy Elements）] > [結果（Results）]> [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] を選択します。

Cisco ISE が FIPS モードで動作するように設定されている場合は、一部のプロトコルがデフォルトで無効化され、それらのプロトコルを設定できません。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　必要な情報を入力します。

ステップ 4　ネットワークに適切な認証プロトコルとオプションを選択します。

ステップ 5　PAC の使用を選択した場合、適切な選択を行います。

匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と Extensible Authentication Protocol-Generic Token Card（EAP-GTC）の両方を選択する必要があります。また Cisco ISE では、マシン認証の外部 ID ソースとしては Active Directory だけがサポートされる点に注意してください。

ステップ 6　[送信（Submit）] をクリックして、許可されるプロトコル サービスを保存します。

許可されるプロトコル サービスは、簡易認証ポリシーおよびルールベースの認証ポリシーのページで独立したオブジェクトとして表示されます。このオブジェクトは異なるルールに使用できます。

これで、簡易認証ポリシーおよびルールベースの認証ポリシーを作成できるようになります。

内部方式として EAP-MSCHAP を無効化し、PEAP または EAP-FAST の EAP-GTC と EAP-TLS 内部方式を有効化すると、ISE は内部方式のネゴシエーション中に EAP-GTC 内部方式を開始します。最初の EAP-GTC メッセージがクライアントに送信される前に、ISE は ID 選択のポリシーを実行して、ID ストアから GTC パスワード プロンプトを取得します。このポリシーの実行中、Network Access: EapAuthentication 属性は EAP-GTC と同じです。EAP-GTC 内部方式がクライアントによって拒否され、EAP-TLS がネゴシエートされても、ID ストア ポリシーが再び実行されることはありません。ID ストア ポリシーが Network Access: EapAuthentication 属性に基づいている場合、本当の EAP 認証は EAP-TLS でありながら ID ポリシー評価後に設定されたため、予期しない結果になることがあります。

関連項目

- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」
- 「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）
- 「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）

シスコ以外のデバイスからの MAB の有効化

表 19-2 の説明に従い次の設定を順番に設定して、シスコ以外のデバイスから MAB を設定します。

表 19-2　シスコ以外のデバイスからの MAB 有効化の設定

	タスク	詳細情報
ステップ 1	認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。Profiler サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。	詳細については、「Cisco ISE でのネットワーク デバイス定義の作成」（P.9-3）を参照してください。

表 19-2　シスコ以外のデバイスからの MAB 有効化の設定 （続き）

	タスク	詳細情報
ステップ 2	シスコ以外のデバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて許可されるプロトコル サービスを作成します。 1. [ポリシー（Policy）] > [ポリシーの要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] を選択します。 2. 許可されるプロトコル サービスの名前を入力します。たとえば、シスコ以外のデバイス用の MAB 3. シスコ以外のデバイスによって使用される MAC 認証タイプに基づいてプロトコルを選択します。 – PAP：[PAP/ASCII を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての PAP の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 – CHAP：[CHAP を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての CHAP の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 – EAP-MD5：[EAP-MD5 を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての EAP-MD5 の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 これらのプロトコルごとに、次のチェックボックスを確認することを推奨します。 – [パスワードを確認（Check Password）]：送信側ネットワーク デバイスの認証を行う簡易 MAB パスワードの確認する場合に有効にします。 – [Calling-Station-ID が MAC アドレスと等しいことを確認（Check Calling-Station-Id equals MAC address）]：Calling-Station-Id が送信中に、追加セキュリティ チェックとして有効にします。 4. 許可されるプロトコル サービスを保存します。	詳細については、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および許可されるプロトコル サービスの設定を参照してください。
ステップ 3：	シスコ以外のデバイスから MAB を有効化する認証ポリシー ルールを設定します。 1. [ポリシー（Policy）] > [認証（Authentication）] を選択します。 2. ルール ベースの認証ポリシーを選択します。 3. MAB の新しいルールを挿入します。 4. このルールのステップ 2 で作成した許可されたプロトコル サービス（シスコ以外のデバイス用の MAB）を選択します。 5. このルールのアイデンティティ ソースとしての内部エンドポイント データベースを選択します。 6. 認証ポリシーを保存します。	詳細については、「ルールベースの認証ポリシーの設定」（P.19-23）を参照してください。

シスコ デバイスからの MAB の有効化

表 19-3 の説明に従い次の設定を順番に設定して、シスコ デバイスから MAB を設定します。

表 19-3　シスコ デバイスからの MAB 有効化の設定

	タスク	詳細情報
ステップ 1	認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。Profiler サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。	詳細については、「Cisco ISE でのネットワーク デバイス定義の作成」（P.9-3）を参照してください。
ステップ 2	シスコ デバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて許可されるプロトコル サービスを作成します。 **1.** [ポリシー（Policy）] > [ポリシーの要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] を選択します。 **2.** 許可されるプロトコル サービスの名前を入力します。たとえば、シスコ デバイス用の MAB **3.** [ホスト ルックアップを処理（Process Host Lookup）] チェックボックスをオンにします。 **4.** シスコ デバイスによって使用される MAC 認証タイプに基づいてプロトコルを選択します。 – PAP：[PAP/ASCII を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての PAP の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 – CHAP：[CHAP を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての CHAP の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 – EAP-MD5：[EAP-MD5 を許可（Allow PAP/ASCII）] チェックボックスをオンにし、[ホスト ルックアップとしての EAP-MD5 の削除（Detect PAP as Host Lookup）] チェックボックスをオンにします。 これらのプロトコルごとに、次のチェックボックスを確認することを推奨します。 – [パスワードを確認（Check Password）]：送信側ネットワーク デバイスの認証を行う簡易 MAB パスワードの確認する場合に有効にします。 – [Calling-Station-ID が MAC アドレスと等しいことを確認（Check Calling-Station-Id equals MAC address）]：Calling-Station-Id が送信中に、追加セキュリティ チェックとして有効にします。 **5.** 許可されるプロトコル サービスを保存します。	詳細については、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および許可されるプロトコル サービスの設定を参照してください。

表 19-3　シスコ デバイスからの MAB 有効化の設定 （続き）

	タスク	詳細情報
ステップ 3：	シスコ デバイスから MAB を有効化する認証ポリシー ルールを設定します。 1. [ポリシー（Policy）] > [認証（Authentication）] を選択します。 2. ルール ベースの認証ポリシーを選択します。 3. MAB の新しいルールを挿入します。 4. このルールのステップ 2 で作成した許可されたプロトコル サービス（シスコ デバイス用の MAB）を選択します。 5. このルールのアイデンティティ ソースとしての内部エンドポイント データベースを選択します。 6. 認証ポリシーを保存します。	詳細については、「ルールベースの認証ポリシーの設定」（P.19-23）を参照してください。

RADIUS プロキシ サーバとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバおよび RADIUS プロキシ サーバとして機能できます。!プロキシ サーバとして機能する場合、Cisco ISE はネットワーク アクセス サーバ（NAS）から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバに転送します。Cisco ISE は要求の結果を受けとり、NAS に返します。

Cisco ISE は、同時に複数の外部 RADIUS サーバへのプロキシ サーバとして動作できます。RADIUS サーバ順序で設定した外部 RADIUS サーバを使用できます。次に説明する [外部 RADIUS サーバ（External RADIUS Server）] ページには、Cisco ISE で定義した外部 RADIUS サーバがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の RADIUS サーバを検索することができます。簡易認証ポリシーとルールベースの認証ポリシーの両方で、RADIUS サーバ順序を使用して要求を RADIUS サーバにプロキシできます。

RADIUS サーバ順序は、RADIUS-Username 属性からドメイン名を抜き取り（ストリッピング）、RADIUS 認証に使用します。このドメイン ストリッピングは EAP 認証には使用できません。EAP 認証では EAP-Identity 属性が使用されます。RADIUS プロキシ サーバは RADIUS-Username 属性からユーザ名を取得し、RADIUS サーバ順序の設定時に指定した文字列からユーザ名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバはユーザ名を EAP-Identity 属性から取得します。RADIUS サーバ順序を使用する EAP 認証は、EAP-Identity 値と RADIUS-Username 値が同一である場合のみ成功します。

RADIUS サーバ順序を認証に使用するには、次の作業を確実に完了する必要があります。

- 「外部 RADIUS サーバの設定」（P.19-19）
- 「RADIUS サーバ順序の定義」（P.19-20）

外部 RADIUS サーバの設定

Cisco ISE で外部 RADIUS サーバを設定して、要求を外部 RADIUS サーバに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

はじめる前に

- この項で作成した外部 RADIUS サーバは、それだけでは使用できません。RADIUS サーバ順序を作成して、この項で作成した RADIUS サーバを使用するように設定する必要があります。これにより、RADIUS サーバ順序を認証ポリシーで使用できるようになります。

  RADIUS サーバ順序を作成する方法については、「RADIUS サーバの順序」（P.19-20）を参照してください。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 RADIUS サーバ（External RADIUS Servers）] を選択します。

[RADIUS サーバ（RADIUS Servers）] ページが表示され、Cisco ISE で定義された外部 RADIUS サーバのリストが示されます。

ステップ 2　外部 RADIUS サーバを追加するには、[追加（Add）] をクリックします。

ステップ 3　必要に応じて値を入力します。

ステップ 4　[送信（Submit）] をクリックして、外部 RADIUS サーバの設定を保存します。

関連項目

- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

RADIUS サーバの順序

Cisco の RADIUS サーバ順序を使用すると、NAD からの要求を外部 RADIUS サーバにプロキシできます。外部 RADIUS サーバは要求を処理して結果を Cisco に返し、Cisco ISE はその応答を NAD に転送します。

[RADIUS サーバ順序（RADIUS Server Sequences）] ページに、Cisco ISE で定義したすべての RADIUS サーバの順序が表示されます。このページを使用して、RADIUS サーバの作成、編集、または複製が可能です。

関連項目

- 「RADIUS プロキシ サーバとして機能する CIsco ISE」（P.19-19）
- 「RADIUS サーバ順序の定義」（P.19-20）
- 「外部 RADIUS サーバの設定」（P.19-19）

RADIUS サーバ順序の定義

このページから RADIUS サーバの順序を追加できます。

はじめる前に

- この手順を開始する前に、プロキシ サービスの基本を理解している必要があり、また外部 RADIUS サーバの設定を完了している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [RADIUS サーバ順序（RADIUS Server Sequences）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　必要に応じて値を入力します。

ステップ 4　[送信（Submit）] をクリックして、ポリシーに使用する RADIUS サーバ順序を保存します。

次の作業

作成した RADIUS サーバ順序を使用した簡易認証ポリシーの設定方法については、「ルール ベースの認証ポリシーの設定」（P.19-23）を参照してください。

関連項目

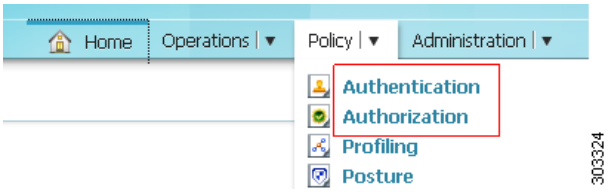
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」
- 「RADIUS サーバの順序」（P.19-20）

ポリシー モード

Cisco ISE には、簡易モードとポリシー セット モードの 2 種類のポリシー モードがあります。2 種類のうちのどちらかのモードを選択して、認証および認可ポリシーを設定します。ポリシー モードを変更すると、Cisco ISE インターフェイスに再度ログインするように促されます。ポリシー セットのモードから簡易モードに切替えた場合、すべてのポリシー セットのデータはデフォルト ポリシーを除いて削除されます。[ポリシー（Policy）] メニュー オプションはポリシー モードの選択に基づいて変化します。

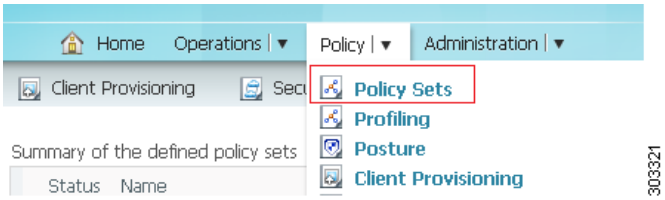
- 簡易モード：[簡易（Simple）] モードを選択した場合は、[ポリシー（Policy）] メニューで認証および認可ポリシーを別々に定義できます。

図 19-3　　簡易モードポリシーメニュー



- ポリシー セット モード：[ポリシー セット（Policy Set）] モードを選択した場合は、ポリシー セットを作成して、認証と認可を論理的に同一グループにグループ化できます。必要に応じて複数のグループを作成できます。

図 19-4　　ポリシー セット モード メニュー



関連項目

- 「ポリシー モード変更のガイドライン」（P.19-22）
- 「ポリシー モードの変更」（P.19-22）
- 「簡易認証ポリシー」（P.19-4）
- 「ルール ベースの認証ポリシーの設定」（P.19-23）
- 「ポリシー セット」（P.19-25）
- 「許可ポリシーおよびプロファイルの管理」

ポリシー モード変更のガイドライン

ポリシー モード変更のためのガイドラインは、次のとおりです。

- Cisco ISE、リリース 1.1 から新たにインストールまたは更新すると、簡易モード ポリシー モデルがデフォルトで選択されます。
- 簡易モードからポリシー セット モードに切替えると、認証および認可ポリシーはデフォルト ポリシー セットに移行されます。
- ポリシー セット モードからの簡易モードに切替えると、デフォルト ポリシー セットの認証および認可が認証および認可ポリシーに移行されます。その他のポリシー セット ポリシーは削除されます。

ポリシー モードの変更

このページを使用して、ポリシー モードを変更します。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポリシー セット（Policy Sets）] を選択します。

ステップ 2　ポリシー セット モードを有効化または無効化します。

ステップ 3　[保存（Save）] をクリックします。

新しいポリシー モードを有効にするために、もう一度ログインするよう促されます。

関連項目

- 「簡易認証ポリシー」（P.19-4）
- 「ルールベースの認証ポリシー」（P.19-6）
- 「ポリシー セット」（P.19-25）
- 「許可ポリシーおよびプロファイルの管理」

簡易認証ポリシーの設定

簡易認証ポリシーの設定手順には、許可されるプロトコル サービスの定義および簡易認証ポリシーの設定が含まれます。許可されるプロトコル サービスの作成方法については、「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）を参照してください。

はじめる前に

- この手順を始める前に、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の作業を正常に完了している必要があります。
- RADIUS サーバ順序を使用した簡易認証ポリシーを設定するには、プロキシ サービスの基礎を理解しておく必要があります。また、RADIUS サーバの順序を正常に完了している必要があります。
- RADIUS サーバを使用して簡易認証ポリシーを設定するには、さまざまなデータベースがサポートする認証タイプとプロトコルの理解のために、C シスコ ISE 認証ポリシーの基本的な理解が必要です。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

このプロセスにより、RADIUS サーバ順序を使用した簡易ポリシーの設定も可能です。

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

ステップ 2　メッセージが表示されたら、[OK] をクリックします。

ステップ 3　必要に応じて値を入力します。

ステップ 4　[保存（Save）] をクリックして、設定した簡易認証ポリシーを保存します。

関連項目

- 「単純な認証ポリシーの設定」（P.B-1）
- 「C シスコ ISE 認証ポリシー」（P.19-1）
- 「RADIUS プロキシ サーバとして機能する CIsco ISE」（P.19-19）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

ルール ベースの認証ポリシーの設定

ルールベースのポリシーでは、条件を定義することによって、Cisco ISE は許可されるプロトコルおよび ID ソースを動的に選択できるようになります。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。「表 19-1 に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。」（P.19-9）を参照してください。

ワンポイントアドバイス　ルールベースの認証ポリシーを作成する前に、許可されるプロトコル アクセス サービス、条件、および ID ソース順序を作成することを推奨します。RADIUS サーバ順序を使用する場合、ポリシーを作成する前に RADIUS サーバ順序を定義できます。詳細については、「RADIUS プロキシ サーバとして機能する CIsco ISE」（P.19-19）を参照してください。

はじめる前に

- 作業を開始する前に、「ルールベースの認証ポリシー」（P.19-6）の基本的な内容を理解しておく必要があり、また「ルール ベースの認証ポリシーの設定」（P.19-23）を読んでおく必要があり、さらに次の作業を正常に完了している必要があります。
  - 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
  - ID ソース順序の作成（ID ソース順序を使用する場合）
  - RADIUS サーバの順序（許可されるプロトコル アクセス サービスの代わりに RADIUS サーバ順序を使用する場合）
- Cisco ISE では、有線 802.1X、無線 802.1X、および有線 MAB を使用する場合の標準的なルールベースの認証ポリシーが事前に用意されています。これらの事前定義されたポリシーの詳細については、「認証ポリシーの組み込み設定」（P.19-28）を参照してください。これらの事前定義されたポリシー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システム管理者である必要があります。
- ユーザが外部の ID ソースで定義されている場合、Cisco ISE でこれらの ID ソースが設定されていることを確認してください。外部 ID ソースの設定方法については、第 14 章「ユーザおよび外部 ID ソースの管理」を参照してください。

（注）　簡易ポリシーとルールベースのポリシーを切り替える場合、最初に設定したポリシーは失われます。たとえば、簡易認証ポリシーを設定した後でルールベースの認証ポリシーに移動すると、簡易認証ポリシーは失われます。また、ルール ベースの認証ポリシーから簡易認証ポリシーに移動した場合は、ルール ベースの認証ポリシーは失われます。

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

ステップ 2　[ルールベース（Rule-Based）] オプション ボタンをクリックします。

ステップ 3　メッセージが表示されたら、[OK] をクリックします。

ステップ 4　アクション アイコンをクリックして、新しいポリシーを表示するリスト上の位置に応じて [新しい行を上に挿入（Insert new row above）] または [新しい行を下に挿入（Insert new row above）] をクリックします。ポリシーは、順序に従って評価されます。

このルールベースのポリシーのページ内の各行は、簡易認証ポリシーと同等です。各行には、許可されるプロトコルおよび ID ソースを決定する一連の条件が含まれています。

ステップ 5　必要に応じて新しい認証ポリシーを作成するための値を入力します。

ステップ 6　[保存（Save）] をクリックして、作成したルールベースの認証ポリシーを保存します。

デフォルトの ID ソースを編集して、このルールで定義されたいずれの ID ソースにも一致しない場合に Cisco ISE が使用する ID ソースを指定できます。

このポリシー ページの最後の行は、いずれのルールにも要求が一致しない場合に適用されるデフォルトのポリシーです。このデフォルトのポリシーの許可されるプロトコルおよび ID ソースを編集できます。

EAP-FAST クライアント認証が外部 TLS ネゴシエーションで送信されたときに認証ポリシーを設定する場合は、「Username」属性は指定できません。シスコは、「CN」および「SAN」などの証明書フィールドを使用することを推奨します。

他のいかなる作成済みポリシーにも要求が一致しない場合のデフォルトのポリシーで、ID ソースとして [アクセスを拒否（Deny Access）] を選択することを推奨します。

関連項目

- 「ルール ベースの認証ポリシーの設定」（P.B-2）
- 「C シスコ ISE 認証ポリシー」（P.19-1）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

ポリシー セット

ポリシー セットでは、論理的に同じセット内の認証および認可ポリシーをグループ化することができます。位置、アクセス タイプ、類似パラメータに基づくポリシー セットなどの領域に基づいて、複数のポリシー セットを作成できます。

ポリシー セットは最初に一致したポリシーです。各ポリシーには簡易または複合条件のどちらかがあり、次のサポート ディクショナリがあります。

- Airspace
- Cisco
- Cisco BBSM
- Cisco VPN3000
- Device、Microsoft
- NetworkAccess
- RADIUS

ポリシー セットが一致し選択されたら、認証および認可ポリシーが評価されます。さらに、ポリシー セット モデルの一部として、グローバル認証例外ポリシーが利用できます。

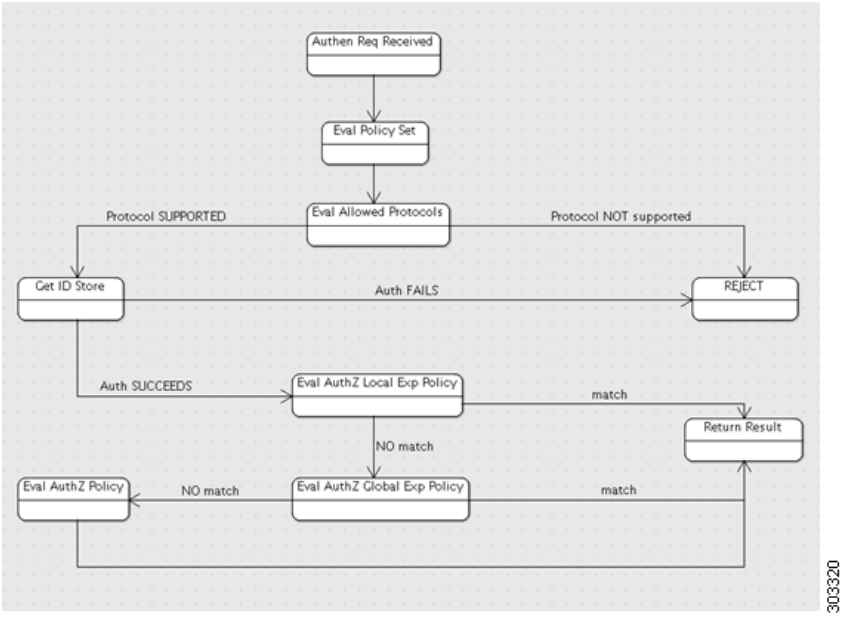
常時 1 つのポリシー セットが定義されています。それがデフォルト ポリシー セットです。

関連項目

- 「ポリシー セットの評価フロー」（P.19-26）
- 「ポリシー セットを作成のガイドライン」（P.19-26）
- 「グローバル認可例外ポリシー」（P.19-27）
- 「ポリシー セットの設定」（P.19-27）

ポリシー セットの評価フロー

図 19-5　ポリシー セットの認証および認可評価のフロー



ポリシー セットの順序および認証/許可評価フローは、次のとおりです。

1. ポリシー セットを評価します（ポリシー セットの状態を評価する）。その結果、ポリシー セットが 1 つ選択されます。
2. 選択したポリシー セットの許可されたプロトコル ルールを評価します。
3. 選択したポリシー セットの ID ストア ルールを評価します。
4. 次のパラダイムに基づいて,選択したポリシー セットの許可ルールを評価します。
   a. 定義されている場合は、ローカル例外ポリシーを評価
   b. 上記手順 1 で一致がない場合、定義されていればグローバル例外ポリシーを評価
   c. 上記手順 2 で一致がない場合、許可ルールを評価

どのポリシー セットにも一致しない場合は、デフォルトのポリシー セットが選択されます。

ポリシー セットを作成のガイドライン

ポリシー セット作成のためのガイドラインは、次のとおりです。

- ルールは、名前、条件、結果で指定する必要があります。すべての認証および認可のルールが定義されていない限り、ポリシー セットを保存できません。
- 同じルール タイプ（認証または許可）と同じポリシー セットからのみであれば、ルールを複製できます。
- 異なるポリシー セットはルールを共有できません。各ポリシー セットには独自のルールがあります。ただし、条件ライブラリを使用している場合は、条件を共有することができます。

グローバル認可例外ポリシー

グローバル許可例外ポリシーにより、すべてのポリシー セットに適用するルールを定義できます。グローバル許可例外ポリシーは、すべてのポリシー セットのすべての認可ポリシーに追加されます。グローバル許可例外ポリシーは、ポリシー セットのリストからグローバル例外オプションを選択することによって更新できます。

各許可ポリシーには、ローカル例外規則、グローバル例外規則、通常ルールがあります。ローカル許可例外ルールを設定すると、（ある許可ポリシー用の）グローバル例外許可ルールが、ローカル許可例外ルールと並んで読み取り専用モードで表示されます。ローカル許可例外ルールは、グローバル例外ルールに優先します。許可ルールは、許可ポリシーのローカル例外規則、グローバル例外規則、通常ルールの順番で処理されます。

ポリシー セットの設定

このページを使用して、ポリシー セットを使用できます。

はじめる前に

ポリシー セットが設定できるように、ポリシー モードをポリシー セットとして選択しておくする必要があります。これを行うには、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポリシー セット（Policy Sets）] に移動します。

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

ステップ 2　[デフォルト（Default）] ポリシーをクリックします。デフォルト ポリシーが右側に表示されます。

ステップ 3　上部のプラス（+）記号をクリックして、[上を作成（Create Above）] を選択します。

ステップ 4　このグループ ポリシーの名前、説明、条件を入力します。

ステップ 5　認証ポリシーを定義します。

ステップ 6　許可ポリシーを定義します。

ステップ 7　[送信（Submit）] をクリックします。ポリシー セットの設定後、Cisco ISE からログアウトされます。管理者ポータルにアクセスするために再度ログインする必要があります。

関連項目

- 「ポリシー モードの変更」（P.19-22）
- 「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」（P.20-8）
- 「ポリシー セットの評価フロー」（P.19-26）
- 「ポリシー セットを作成のガイドライン」（P.19-26）
- 「グローバル認可例外ポリシー」（P.19-27）

認証ポリシーの組み込み設定

Cisco ISE ソフトウェアには、いくつかの組み込み設定が用意されおり、一部の一般的な用途に対応しています。これらの組み込み設定はデフォルトと呼ばれます。表 19-4 では、認証ポリシーに関連するデフォルトについて説明します。

表 19-4　認証ポリシー設定のデフォルト

名前	ユーザ インターフェイスのパス	説明	その他の情報
ネットワーク アクセスのデフォルトの許可されるプロトコル アクセス サービス	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [設定（Configuration）] > [許可されるプロトコル（Allowed Protocols）]	このデフォルトは、認証ポリシーに使用されるネットワーク アクセスの組み込みの許可されるプロトコル サービスです。	このアクセス サービスは、有線および無線の 802.1X、および有線 MAB の認証ポリシーに使用できます。
有線 802.1X 複合条件	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認証（Authentication）] > [ゲスト（Guest）] > [複合条件（Compound Conditions）] を選択します。	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Ethernet	この複合条件は、有線 802.1X 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、有線 802.1X 認証ポリシーに基づいて評価されます。
無線 802.1X 複合条件	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認証（Authentication）] > [ゲスト（Guest）] > [複合条件（Compound Conditions）] を選択します。	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	この複合条件は、無線 802.1X 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、無線 802.1X 認証ポリシーに基づいて評価されます。
有線 MAB 複合条件	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認証（Authentication）] > [ゲスト（Guest）] > [複合条件（Compound Conditions）] を選択します。	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type は Call-Check • RADIUS:NAS-Port-Type equals Ethernet	この複合条件は、有線 MAB 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、有線 MAB 認証ポリシーに基づいて評価されます。
Catalyst スイッチのローカル Web 認証複合条件	[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認証（Authentication）] > [ゲスト（Guest）] > [複合条件（Compound Conditions）] を選択します。	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Ethernet	この複合条件を使用するには、この条件を確認する認証ポリシーを作成する必要があります。詳細については、ルールベースの認証ポリシーの設定を参照してください。また、要件に基づいてアクセス サービスを定義するか、このポリシーのデフォルト ネットワーク アクセス許可プロトコル サービスを利用できます。詳細については、ネットワーク アクセス サービスを参照してください。

表 19-4　認証ポリシー設定のデフォルト （続き）

名前	ユーザ インターフェイスのパス	説明	その他の情報
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）] > [認証（Authentication）] > [ゲスト（Guest）] > [複合条件（Compound Conditions）] を選択します。	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	この複合条件を使用するには、この条件を確認する認証ポリシーを作成する必要があります。詳細については、ルールベースの認証ポリシーの設定を参照してください。また、要件に基づいてアクセス サービスを定義するか、このポリシーのデフォルト ネットワーク アクセス許可プロトコル サービスを利用できます。詳細については、ネットワーク アクセス サービスを参照してください。
有線 802.1X 認証ポリシー	[ポリシー（Policy）] > [認証（Authentication）] > [ルールベース（Rule-Based）]	このポリシーは、有線 802.1X 複合条件およびデフォルトのネットワーク アクセスの許可されるプロトコル サービスを使用します。このポリシーは、有線 802.1X 複合条件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 ポリシーはアイデンティティ ソースとして内部エンドポイント データベースを使用します。このポリシーを編集して、あらゆるアイデンティティ ソースのシーケンスまたはアイデンティティ ソースを必要に応じて設定できます。
無線 802.1X 認証ポリシー	[ポリシー（Policy）] > [認証（Authentication）] > [ルールベース（Rule-Based）]	このポリシーは、無線 802.1X 複合条件およびデフォルトのネットワーク アクセスの許可されるプロトコル サービスを使用します。このポリシーは、無線 802.1X 複合条件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 ポリシーはアイデンティティ ソースとして内部エンドポイント データベースを使用します。このポリシーを編集して、あらゆるアイデンティティ ソースのシーケンスまたはアイデンティティ ソースを必要に応じて設定できます。
有線 MAB 認証ポリシー	[ポリシー（Policy）] > [認証（Authentication）] > [ルールベース（Rule-Based）]	このポリシーは、有線 MAB 複合条件およびデフォルトのネットワーク アクセスの許可されるプロトコル サービスを使用します。このポリシーは、有線 MAB 複合条件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 ポリシーはアイデンティティ ソースとして内部エンドポイント データベースを使用します。

認証結果の表示

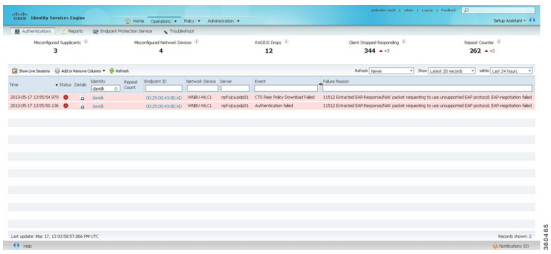
Cisco ISE にはリアルタイムで認証の概要を表示するさまざまな方法があります。

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システム管理者である必要があります。

ステップ 1　[操作（Operations）] > [認証（Authentications）] を選択して、リアルタイムで認証の概要を表示します。図 19-6 に示すようなページが表示されます。

図 19-6　[ライブ認証（Live Authentications）] ページ



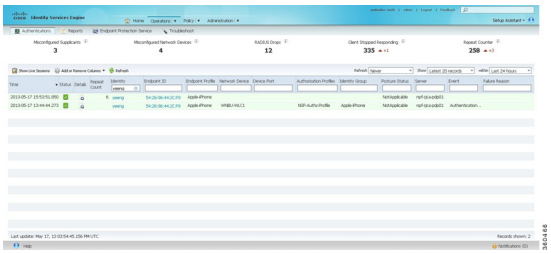
ステップ 2　認証の概要を表示するには、次のような方法があります。

- [ステータス（Status）] アイコンの上にマウス カーソルを移動すると、認証の結果と概要を表示できます。図 19-6 に示すようなポップアップが表示されます。
- 結果をフィルタリングするには、リストの最上部に表示される 1 つ以上の任意のテキスト ボックスに検索条件を入力して Enter を押します。
- 詳細レポートを表示するには、[詳細（Details）] カラムにある虫眼鏡アイコンをクリックします。

（注）　認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

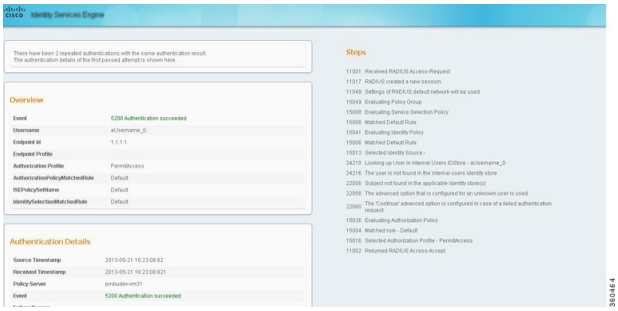
ステップ 3　[ライブセッションの表示（Show Live Sessions）] をクリックして、リアルタイムのセッション概要を表示します。図 19-7 に示すようなページが表示されます。

図 19-7　ライブ セッション ページ



ステップ 4　[ライブ セッション（Live Session）] ページの目的のエントリに対応する [詳細（Details）] アイコンをクリックして、ライブ認証のドリル ダウン レポートを表示します。図 19-8 に示すようなページが表示されます。

図 19-8　ライブ認証はドリル ダウン レポートを詳しく説明します



関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

認証 ダッシュレット

Cisco ISE のダッシュボードには、ネットワークで行われたすべての認証の概要が表示されます。これには、認証ダッシュレットにある認証および許可の失敗についての概要情報が表示されます。

認証ダッシュレットには、Cisco ISE が処理した RADIUS 認証に関する次の統計情報が表示されます。

- 認証成功、認証失敗、同一ユーザによる同時ログインなど、Cisco ISE が処理した RADIUS 認証要求の総数。
- Cisco ISE が処理した RADIUS 認証失敗の総数。

ダッシュボードとダッシュレット上の情報と、より多くの情報にアクセスする方法については、「Cisco ISE ダッシュボード」（P.25-2）と「データベースのモニタリング」（P.25-30）を参照してください。

認証レポートおよびトラブルシューティング ツール

認証の詳細の他に、Cisco ISE では、ネットワークの効率的な管理に使用できるさまざまなレポートおよびトラブルシューティング ツールが提供されます。

ネットワーク内の認証の傾向およびトラフィックを把握するために実行できるさまざまのレポートがあります。現在のデータに加えて履歴のレポートを生成できます。認証レポートのリストは次のとおりです。

- AAA 診断
- RADIUS アカウンティング（RADIUS Accounting）
- RADIUS 認証
- 認証の概要

レポートを生成および使用方法の詳細については、第 26 章「レポート」を参照してください。