IP ベースのアクセス コントロール ポリシーの設定

IP ベースのアクセス コントロール ポリシー

IP ベースのアクセス コントロール ポリシーは、アクセス コントロール リスト（ACL）と同じ方法でシスコ デバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセス コントロール ポリシーにはプロトコル タイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィック フローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセス コントロール ポリシーを使用して、セキュリティ、モニターリング、ルート選択、ネットワーク アドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセス コントロール ポリシーには、次の 2 つの主要コンポーネントがあります。

- [IP Network Groups]：IP ネットワーク グループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワーク グループに含めることができる IP サブネットは 1 つだけです。
- [Access Contract]：アクセス コントラクトは、IP ベースのアクセス コントロール ポリシーとグループベースのアクセス コントロール ポリシーの両方で使用される共通の構成要素

です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセス コントロール ポリシー設定のワークフロー

始める前に

- 新しい IP ベースのアクセス コントロール ポリシーを作成中に、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** ウィンドウでグループを追加する場合は、Cisco ISE は必須ではありません。
- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
  - ネットワークサーバー（AAA、DHCP、DNS サーバーなど）：グローバル ネットワーク サーバーの設定 を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのログイン情報：グローバル デバイス クレデンシャルの概要を参照。
  - IP アドレスプール：IP アドレス プールを設定するを参照。
  - SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなどのワイヤレス設定：グローバル ワイヤレス設定の構成を参照。
  - デバイスのプロビジョニング。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「IP ネットワーク グループの作成 （3 ページ）」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IP ベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション（許可または拒否）を指定します。詳細については、「IP ベースのアクセス コントロール契約の作成 （4 ページ）」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、IP ベースのアクセス コントロール ポリシーの作成 （5 ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP Server]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS Server]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

IP ネットワーク グループの作成

ステップ 1 メニューアイコン（☰）をクリックして、 **[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[グループの追加（Add Group）]** をクリックします。

ステップ 3 **[名前（Name）]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 **[説明（Description）]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 **[IP アドレスまたは IP/CIDR（IP Address or IP/CIDR）]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[IP ネットワーク グループ（IP Network Groups）]** テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- グループを変更するには、**[編集（Edit）]**をクリックします。フィールドの定義については、IP ネットワーク グループの作成 （3 ページ） を参照してください。必要な変更を行って、[Save] をクリックします。
- グループを削除するには、**[削除（Delete）]** をクリックし、次に **[はい（Yes）]** をクリックして確定します。

IP ベースのアクセス コントロール契約の作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 [コントラクトの追加（Add Contract）] をクリックします。

ステップ 3 契約の名前と説明を入力します。

ステップ 4 **[暗黙的アクション（Implicit Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 5 テーブルの **[アクション（Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 6 **[ポート/プロトコル（Port/Protocol）]** ドロップダウン リストから、ポートまたはプロトコルを選択します。

a) Cisco DNA Centerに必要なポートまたはプロトコルがない場合は、**[ポート/プロトコルの追加（Add Port/Protocol）]** をクリックして、自分で作成します。
b) **[名前（Name）]** フィールドで、ポートまたはプロトコルの名前を入力します。
c) [Protocol] ドロップダウンリストから、[UDP]、[TDP]、または [TCP/UDP] を選択します。
d) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。
e) Cisco DNA Centerで定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、**[競合を無視する（Ignore Conflict）]** チェックボックスをオンにします。

f) **[保存（Save）]** をクリックします。

ステップ 7 （任意） 契約にさらにルールを含めるには、**[追加（Add）]** をクリックして、手順 5 および 6 を繰り返します。

ステップ 8 [Save] をクリックします。

IP ベースのアクセス コントロール ポリシー契約の編集または削除

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセス コントロール ポリシー（IP Based Access Control Policies）]** ウィンドウのポリシーの状態が **[変更（MODIFIED）]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[編集（Edit）]をクリックして変更を行い、[保存（Save）] をクリックします。フィールドの定義については、IP ベースのアクセス コントロール契約の作成 （4 ページ）を参照してください。

  （注） ポリシーで使用されている契約を変更した場合は、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]**の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[Deploy] をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、[削除（Delete）] をクリックします。

IP ベースのアクセス コントロール ポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセス コントロール ポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、シスコ ワイヤレス コントローラ が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。

- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す [変更済み（Modified）] というステータスでフラグが付けられます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 [ポリシーの追加（Add Policy）] をクリックします。

ステップ 3 次のフィールドに入力します。

フィールド	説明
Policy Name	ポリシーの名前。
Description	ポリシーを表す単語またはフレーズ。
SSID	SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセス ポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。 （注） SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。 ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。
Site Scope	サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲を参照してください。
Source	契約の影響を受けるトラフィックの送信元。[Source] ドロップダウンリストから、IP ネットワークグループを選択します。使用したい IP ネットワークがない場合は、[+ グループの追加（+Group）] をクリックして作成します。
Contract	ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加（Add Contract）] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可（permit）]（すべてのトラフィックを許可）または [拒否（deny）]（すべてのトラフィックを拒否）を選択することもできます。

フィールド	説明
Destination	契約の影響を受けるトラフィックの宛先。[宛先（Destination）] ドロップダウン リストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+ IP ネットワーク グループの作成（+Create IP Network Group）] をクリックして作成します。
Direction	送信元と宛先間のトラフィック フローの関係を設定します。送信元から宛先へのトラフィック フローの契約を有効にするには、[一方向（One-Way）] を選択します。両方向（送信元から宛先へ、および宛先から送信元へ）でのトラフィック フローの契約を有効にするには、[双方向（Bi-directional）] を選択します。

ステップ 4 （任意） IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成（Create IP Network Group）] をクリックします。

ステップ 5 （任意） 別のルールを追加するには、プラス記号をクリックします。

（注） ルールを削除するには、[x] をクリックします。

ステップ 6 （任意） ルールの順序を変更するには、変更したい順序でルールをドラッグ アンド ドロップします。

ステップ 7 [Deploy] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの [ステータス（Status）] は、[展開済み（DEPLOYED）] として表示されます。[ポリシー名（Policy Name）] の横にあるワイヤレス アイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセス コントロール ポリシーの編集または削除

必要な場合は、IP ベースのアクセス コントロール ポリシーを変更または削除できます。

（注） ポリシーを編集すると、[IPベースのアクセスコントロールポリシー（IP-Based Access Control Policies）] ウィンドウのポリシーの状態が [変更（MODIFIED）] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 編集または削除するポリシーの横にあるチェック ボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集（Edit）]をクリックします。完了したら、[Save]をクリックします。フィールドの定義については、IP ベースのアクセス コントロール ポリシーの作成 （5 ページ）を参照してください。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

ステップ 3 ポリシーを変更した場合は、ポリシー名の横にあるチェック ボックスをオンにして [展開（Deploy）] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセス コントロール ポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 展開するポリシーを探します。

ステップ 3 ポリシーの横にあるチェック ボックスをオンにします。

ステップ 4 [Deploy] をクリックします。
ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ 5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、**[今すぐ実行（Run Now）]** ラジオ ボタンをクリックし、**[適用（Apply）]** をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。