IP ベースおよび URL 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 Catalyst 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。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー詳細については、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 クレデンシャル。詳細については、グローバル デバイス クレデンシャルの概要を参照してください。
  - IP アドレス プール詳細については、「IP アドレス プールを設定する」を参照してください。
  - SSID、ワイヤレス インターフェイス、および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です。詳細については、「グローバル ワイヤレス設定の構成」を参照してください。

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 （4 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 ベースおよび URL ベースのアクセス コントロール ポリシーを作成する （6 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Network Settings]** > **[Servers]** の順に選択します。

ステップ 2 [DHCP]エリアを展開して、クライアントデバイスのネットワーキング設定を管理するための1つまたは複数の専用 Dynamic Host Configuration Protocol（DHCP）サーバーを指定します。

ステップ 3 [Add DHCP servers] チェックボックスをオンにして、フィールドを表示します。

ステップ 4 [IP Address] フィールドに DHCP サーバーの IP アドレスを入力します。アイコンをクリックして、IP アドレスを追加します。

（注） + 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 アドレスを削除するには、アイコンをクリックします。

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 5 [DNS] 領域を展開してネットワークのドメイン名を設定し、ホスト名解決用のドメインネームシステム（DNS）サーバーを指定します。

ステップ 6 [Set a domain name] チェックボックスをオンにして、DNS サーバーのドメイン名を入力します。

ステップ 7 [Add DNS servers] チェックボックスをオンにして、IP アドレスを入力します。

（注） + 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 アドレスを削除するには、アイコンをクリックします。

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 8 [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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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。フィールド定義の詳細については、IP ネットワーク グループの作成 （4 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

IP ベースのアクセス契約を作成するには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[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 [Add Contract] slide-in paneの [Name] フィールドに、アクセス契約の名前を入力します。

ステップ 4 （任意） [Description] フィールドに、アクセス契約の説明を入力します。

ステップ 5 **[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 6 [Add] をクリックして、ポートまたはプロトコルを追加します。

ステップ 7 [Add Port/Protocol] ダイアログボックスで、次の手順を実行します。

a) [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

b) **[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。

c) [Save] をクリックします。

ステップ 8 Catalyst Center に必要なポートまたはプロトコルがない場合は、[Create Port/Protocol] をクリックしてポートとプロトコルを作成し、[Create Port/Protocol] ダイアログボックスで次の手順を実行します。

a) **[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。

b) ドロップダウンリストから、プロトコル（[Any]、[AHP]、[ESP]、[IGMP]、[IP]、[NOS]、[PCP]、[TDP]、[UDP]、または [TCP/UDP]）を選択します。

c) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。

d) Catalyst 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、[Ignore Conflict] チェックボックスをオンにします。

e) [Save] をクリックします。

ステップ 9 （任意） アクセス契約にさらにルールを含めるには、[Add] をクリックして、ステップ 7 （5 ページ）を繰り返します。

ステップ 10 [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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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、[Edit] をクリックして変更を行い、[Save] をクリックします。フィールド定義の詳細については、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。

（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 ベースおよび URL ベースのアクセス コントロール ポリシーを作成する

ネットワークの認証後アクセスコントロールリスト（ACL）を作成できます。ACL は、IP、URL、またはその両方に基づくことができます。

始める前に

IP ベースのアクセス コントロール契約の作成 （4 ページ）。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[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。

または、最初の 2 つの手順の代わりに、メニューアイコンをクリックして、**[Workflows]** > **[Create IP & URL-Based Access Control Policy]** を選択できます。 [Overview] ウィンドウが開いたら、[Let's Do it] をクリックしてワークフローを開始します。

ステップ 3 [Policy Name and Details] ウィンドウで、次の手順を実行します。

a) ポリシーの名前と説明を入力します。

b) [Select ACL Type] で、[IP] チェックボックス、[URL] チェックボックスをオンにするか、または [IP] チェックボックスと [URL] チェックボックスの両方をオンにします。

ステップ 4 [Select Site and SSID] ウィンドウで、ポリシーを適用するサイトを選択します。

サイトが非ファブリック SSID ですでにプロビジョニングされていることを確認してください。

ステップ 5 [Policy Name and Details] ウィンドウで [IP] チェックボックスをオンにした場合は、[IP Access Control List] ウィンドウで次の手順を実行します。

a) [Add New Row] をクリックし、[Source]、[Destination]、[Contracts]、または [Direction] を選択します。

b) [Add]をクリックします。

ステップ 6 [Policy Name and Details] ウィンドウで [URL] チェックボックスをオンにした場合は、[URL Access Control List] ウィンドウで次の手順を実行します。

1. URL を入力します。

2. [Action] ドロップダウンリストをクリックして [Permit] または [Deny] を選択します。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 8 [Schedule Provision] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ワイヤレスデバイス構成の可視性と制御を参照してください。

ステップ 9 [Next] をクリックします。

[Now] または [Later] を選択した場合、[Submit] をクリックすると、デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認できます。

ステップ 10 [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、[Preview Configuration] ウィンドウで、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、ワイヤレスデバイス構成の可視性と制御を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

IP ベースおよび URL 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 ベースおよび URL 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。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 ポリシーを編集するには、編集するポリシーの名前をクリックし、必要な変更を加えて、[Save & Schedule] をクリックします。詳細については、IP ベースおよび URL ベースのアクセス コントロール ポリシーを作成する （6 ページ）を参照してください。

ステップ 3 ポリシーを削除するには、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 [Delete] をクリックします。

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。