

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 （1 ページ）
- 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 （2 ページ）
- グローバル ネットワーク サーバーの設定 （3 ページ）
- IP ネットワーク グループの作成 （4 ページ）
- IP ネットワーク グループの編集または削除 （5 ページ）
- IP ベースのアクセスコントロール契約の作成 （5 ページ）
- IP ベースのアクセス コントロール コントラクトの編集または削除 （6 ページ）
- IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 （7 ページ）
- 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 （9 ページ）

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行われるアクション（許可または拒否）や他のルールが一致しないときに行わ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。
- ブラウザまたはネットワークでプロキシ設定が構成されている場合は、IP アクセス コントロール ポリシーにプロキシサブネットを含めます。
- 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 クレデンシャルの設定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。

手順

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 （5 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 ポリシーの作成 （7 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オーバーライドできます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。

ステップ 2 [Servers] タブをクリックします。

ステップ 3 [DHCP]エリアを展開します。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 4 [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 5 [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 6 [DNS]エリア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Domain Name System（DNS）サーバーを指定します。

ステップ 7 [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 8 [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 9 ネットワークのシステムクロックの同期を容易にするために、1 つ以上の Network Time Protocol（NTP）サーバーを指定するには、[NTP] エリアを展開します。

ステップ 10 [Add NTP 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 11 [IP Address] フィールドに、NTP 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。

ステップ 12 [Save] をクリックします。

IP ネットワーク グループの作成

手順

ステップ 1 メインメニューから次を選択します。 **[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

手順

ステップ 1 メインメニューから次を選択します。 **[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。

- グループを編集するには、[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。変更を加えたら、[保存（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。

手順

ステップ 1 メインメニューから次を選択します。**[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] スライドインペインの [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 [ポート/プロトコルの追加（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、[ポート/プロトコルの作成（Create Port/Protocol）] をクリックしてポートとプロトコルを作成し、[ポート/プロトコルの作成（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) プロトコル ドロップダウン リストから、プロトコルを選択します。
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 コントラクトの編集または削除

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。

手順

ステップ 1 メインメニューから次を選択します。**[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コントラクト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 （5 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 ポリシーの作成

ネットワークの認証後アクセス制御リスト（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 ポリシー設定のワークフロー （2 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[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、必要なチェックボックスをオンにします。

- [IPv4] **または [IPv6]**：IP ベースのアクセス コントロール ポリシーを設定します。
- [URL]：URL ベースのアクセス コントロール ポリシーを設定します。
- [IPv4] と [URL]：IPv4 ベースおよび URL ベースのアクセス コントロール ポリシーを設定します。
- [IPv6] と [URL]：IPv6 ベースおよび URLベースのアクセス コントロール ポリシーを設定します。

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

サイトが SSID で既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。

Flex またはファブリック SSID の場合は、AP がサイトでプロビジョニングされていることを確認します。

URL ACL を選択した場合、Flex またはファブリック SSID と併せてローカル SSID を選択することはできません。

ステップ 5 IP ACL を選択した場合、**[IPアクセス制御リスト（IP Access Control List）]** ウィンドウで IP ACL のカスタムルールを設定します。

実行する操作	結果
ルールの追加	**1.** [Add New Rule] をクリックします。 **2.** [新規ルールの追加（Add New Rule）] ダイアログボックスで、対応するドロップダウンリストから送信元、宛先、契約、および方向を選択します。 （注） 双方向ルールの場合は、送信元と宛先が異なることを確認してください。送信元と宛先が [任意（Any）] に設定されている場合は、カスタム契約のみを使用します。 **3.** [Add] をクリックします。
ルールの編集	**1.** 編集するルールの鉛筆アイコンをクリックします。 **2.** 必要な設定を編集します。 **3.** [Save] をクリックします。 （注） デフォルトルールは編集できません。
ルールの削除	削除したいルールの [削除（delete）] アイコンをクリックします。 （注） デフォルトルールは削除できません。
ルールのシーケンスの更新	ルールの アイコンをクリックし、必要な位置にルールをドラッグアンドドロップします。 （注） デフォルトルールのシーケンスは更新できません。

ステップ 6 URL ACL を選択した場合は、**[URLアクセス制御リスト（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。

（注） 最大 20 個の URL を含めることができます。

2. [アクション（Action）] ドロップダウンリストから、[許可（Permit）] または [拒否（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 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開するを参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

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。

手順

ステップ 1 メインメニューから次を選択します。**[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 ポリシーの作成 （7 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。

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。

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。

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。

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。

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。

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。

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。