



トラフィックの前処理のカスタマイズ

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

この章では、次の設定を行う方法について説明します。

- [アクセス コントロールのデフォルト侵入ポリシーの設定\(20-1 ページ\)](#)では、システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセス コントロール ポリシーのデフォルトの侵入ポリシーを変更する方法について説明します。
- [ネットワーク分析ポリシーによる前処理のカスタマイズ\(20-3 ページ\)](#)では、一致するトラフィックを前処理するためのカスタム ネットワーク分析ポリシーを割り当てることで、特定のトラフィック前処理オプションを特定のセキュリティゾーンおよびネットワークに合わせてカスタマイズする方法を説明します。

他の章では、アクセス コントロール ポリシーに対するポリシー全体の前処理とパフォーマンスのオプションを説明します。詳細については、以下を参照してください。

- [トランスポート/ネットワークの詳細設定の構成\(24-2 ページ\)](#)
- [パッシブ展開における前処理の調整\(25-1 ページ\)](#)
- [侵入防御パフォーマンスの調整\(11-7 ページ\)](#)
- [ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整\(11-19 ページ\)](#)

アクセス コントロールのデフォルト侵入ポリシーの設定

ライセンス:任意(Any)

各アクセス コントロール ポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってはシステムがトラフィックを処理するアクセス コントロール ルール(存在する場合)を決定する前に、接続の最初の数パケットを処理し**通過を許可**する必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、アプリケーション制御および URL フィルタリングを実行する場合に特に有用です。たとえば、パケットがアプリケーションまたは URL 条件を持つアクセスコントロールルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたは URL の識別が完了するまで通過することを許可されます。通常は 3 ~ 5 パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。システムが接続を処理する必要があるアクセスコントロールルールまたはデフォルトアクションを識別した後、接続内の残りのパケットが適宜処理され検査されます。

アクセスコントロールポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルトアクションによって異なります。アクセスコントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] (システムによって提供されるポリシー) は、最初に [侵入防御 (Intrusion Prevention)] デフォルトアクションを選択した場合のアクセスコントロールポリシーのデフォルトの侵入ポリシーです。
- [アクティブなルールなし (No Rules Active)] は、最初に [すべてのトラフィックをブロック (Block all traffic)] デフォルトアクションを選択した場合の、アクセスコントロールポリシーのデフォルトの侵入ポリシーです。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。



(注)

侵入インスペクションを実行しない場合は、[アクティブなルールなし (No Rules Active)] ポリシーをデフォルトの侵入ポリシーとしておきます。詳細については、[アクセスコントロールポリシーとルールのトラブルシューティング \(4-15 ページ\)](#) を参照してください。

アクセスコントロールポリシーを作成後にデフォルトアクションを変更する場合は、デフォルトの侵入ポリシーが自動的に変更されないことに注意してください。手動で変更するには、アクセスコントロールポリシーの詳細オプションを使用します。

アクセスコントロールポリシーのデフォルト侵入ポリシーを変更するには、次の手順を実行します。

- 手順 1** デフォルトの侵入ポリシーを変更するアクセスコントロールポリシーで、[詳細設定 (Advanced)] タブを選択し、[ネットワーク分析と侵入ポリシー (Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン(✎)をクリックします。

[ネットワーク分析ポリシー (Network Analysis Policies)] ダイアログボックスが表示されます。

- 手順 2** [アクセスコントロールルールが決定される前に使用される侵入ポリシー (Intrusion Policy used before Access Control rule is determined)] ドロップダウンリストから、デフォルトの侵入ポリシーを選択します。システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン(✎)をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。



注意

Cisco の担当者から指示された場合を除き、Experimental Policy 1 は使用しないでください。Cisco では、試験用にこのポリシーを使用します。

手順 3 [OK] をクリックして変更を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。

ネットワーク分析ポリシーによる前処理のカスタマイズ

ライセンス:任意(Any)

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティ インテリジェンスのブラックリスト登録およびトラフィックの復号化の後で、侵入ポリシーによるパケット インспекションの前に行われます。デフォルトでは、システムによって提供される [バランスの取れたセキュリティと接続(Balanced Security and Connectivity)] ネットワーク分析ポリシーは、アクセス コントロール ポリシーによって処理されるすべてのトラフィックに適用されます。



ヒント

システムによって提供される [バランスの取れたセキュリティと接続(Balanced Security and Connectivity)] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続(Balanced Security and Connectivity)] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。[カスタム ネットワーク分析ポリシーの作成 \(21-2 ページ\)](#) を参照してください。使用可能な調整オプションは、プリプロセッサによって異なります。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。すると、さまざまなセキュリティ ゾーンまたはネットワークを使用するトラフィックの前処理をこれらのポリシーを使用して制御するように、システムを設定することができます。

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。



(注)

プリプロセッサが無効に設定されていても、システムでは、有効になっている侵入ルールまたはプリプロセッサ ルールと照合して前処理されたパケットを評価する必要がある場合、システムは、プリプロセッサを自動的に有効にして使用します。ただし、ネットワーク分析ポリシー インターフェイスでは、プリプロセッサは無効のままです。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理および侵入インспекションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。詳細については、[カスタム ポリシーに関する制約事項\(18-13 ページ\)](#) を参照してください。

詳細については、次の項を参照してください。

- [アクセスコントロールのデフォルト ネットワーク分析ポリシーの設定 \(20-4 ページ\)](#)
- [ネットワーク分析ルールを使用して前処理するトラフィックの指定 \(20-5 ページ\)](#)
- [ネットワーク分析ルールの管理 \(20-9 ページ\)](#)

アクセスコントロールのデフォルト ネットワーク分析ポリシーの設定

ライセンス:任意 (Any)

デフォルトでは、システムによって提供される [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] ネットワーク分析ポリシーは、アクセスコントロールポリシーによって処理されるすべてのトラフィックに適用されます。トラフィックの前処理オプションを調整するためにネットワーク分析ルールを追加する場合は、デフォルトのネットワーク分析ポリシーがそのルールで処理されないすべてのトラフィックを前処理します。

アクセスコントロールポリシーの詳細設定によって、このデフォルトポリシーを変更することができます。

アクセスコントロールポリシーのデフォルトのネットワーク分析ポリシーを変更するには、次の手順を実行します。

手順 1 デフォルトのネットワーク分析ポリシーを変更するアクセスコントロールポリシーで、[詳細設定 (Advanced)] タブを選択し、[ネットワーク分析と侵入ポリシー (Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン (✎) をクリックします。

[ネットワーク分析ポリシー (Network Analysis Policies)] ダイアログボックスが表示されます。

手順 2 [デフォルトのネットワーク分析ポリシー (Default Network Analysis Policy)] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン (✎) をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。



注意

Cisco の担当者から指示された場合を除き、Experimental Policy 1 は使用しないでください。Cisco では、試験用にこのポリシーを使用します。

手順 3 [OK] をクリックして変更を保存します。

変更を反映するには、アクセスコントロールポリシーを適用する必要があります。

ネットワーク分析ルールを使用して前処理するトラフィックの指定

ライセンス:任意(Any)

アクセス コントロール ポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワークトラフィックへの前処理設定を調整できます。アクセス コントロール ルールと同様に、ネットワーク分析ルールには 1 から始まる番号が付いています。

システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。次の表に、ルールに追加できる条件を示します。

表 20-1 ネットワーク分析ルール条件のタイプ

条件	トラフィックの照合	詳細 (Details)
ゾーン	特定のセキュリティゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティゾーンは、ご使用の導入ポリシーおよびセキュリティポリシーに準じた 1 つ以上のインターフェイスの論理グループです。ゾーン条件を作成するには、 ゾーンごとのトラフィックの前処理 (20-6 ページ) を参照してください。
ネットワーク	その送信元または宛先 IP アドレスによる	IP アドレスを明示的に指定できます。ネットワーク条件を作成するには、 ネットワークごとのトラフィックの前処理 (20-7 ページ) を参照してください。

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

カスタム ネットワーク分析ルールを追加するには、次の手順を実行します。

- 手順 1** カスタム前処理設定を作成するアクセス コントロール ポリシーで、[詳細設定 (Advanced)] タブを選択して、[ネットワーク分析と侵入ポリシー (Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン(✎)をクリックします。

[ネットワーク分析ポリシー (Network Analysis Policies)] ダイアログボックスが表示されます。モジュール インターフェイスには、カスタムのネットワーク分析ルールを追加していない場合は [カスタムルールなし (No Custom Rules)] と表示され、追加済みの場合は、設定されているルールの数が表示されます。



ヒント


新しいウィンドウで [ネットワーク分析ポリシー (Network Analysis Policies)] ページを表示するには、[ネットワーク分析ポリシー リスト (Network Analysis Policy List)] をクリックします。このページは、カスタム ネットワーク分析ポリシーを表示および編集するために使用します。[ネットワーク分析ポリシーの管理 \(21-3 ページ\)](#) を参照してください。

- 手順 2** [ネットワーク分析ルール (Network Analysis Rules)] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ダイアログボックスが展開され、カスタム ルールが表示されます(ある場合)。

- 手順 3** [ルールの追加 (Add Rule)] をクリックします。

ネットワーク分析ルール エディタが表示されます。

- 手順 4 ルールの条件を作成します。次の基準を使用して、NAP の前処理を制限できます。
- ・ [ゾーンごとのトラフィックの前処理\(20-6 ページ\)](#)
 - ・ [ネットワークごとのトラフィックの前処理\(20-7 ページ\)](#)
- 手順 5 [ネットワーク分析(Network Analysis)] タブをクリックし、[ネットワーク分析ポリシー(Network Analysis Policy)] ドロップダウンリストからポリシーを選択することによって、ネットワーク分析ポリシーをルールに関連付けます。
- システムは、ユーザが選択したネットワーク分析ポリシーを使用して、すべてのルールの条件を満たすトラフィックを前処理します。ユーザが作成したポリシーを選択した場合は、編集アイコン(✎)をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。
-
-  **注意** Cisco の担当者から指示された場合を除き、Experimental Policy 1 は使用しないでください。Cisco では、試験用にこのポリシーを使用します。
-
- 手順 6 [追加(Add)] をクリックします。
- このルールは他のルールの後に追加されます。ルールの評価順序を変更する場合は、[ネットワーク分析ルールの管理\(20-9 ページ\)](#)を参照してください。
-

ゾーンごとのトラフィックの前処理

ライセンス:任意(Any)

ネットワーク分析ルール内のゾーン条件によって、その送信元および宛先セキュリティゾーン別にトラフィックを前処理することができます。セキュリティゾーンは、1つ以上のインターフェイスのグループです。ゾーン作成の詳細については、[セキュリティゾーンの操作\(2-37 ページ\)](#)を参照してください。

1つのゾーン条件で [送信元ゾーン(Source Zones)] および [宛先ゾーン(Destination Zones)] それぞれに対し、最大 50 のゾーンを追加できます。

- ・ ゾーン内のインターフェイスからデバイスから発信するトラフィックを照合するには、そのゾーンを [宛先ゾーン(Destination Zones)] に追加します。パッシブに展開されたデバイスはトラフィックを送信しないので、宛先ゾーン条件でパッシブインターフェイスから構成されるゾーンは使用できないことに注意してください。
- ・ ゾーン内のインターフェイスからデバイスに着信するトラフィックを照合するには、そのゾーンを [送信元ゾーン(Source Zones)] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの1つから発生し、宛先ゾーンの1つを通して出力する必要があります。

警告アイコン(⚠)は、インターフェイスが含まれていないゾーンなどの無効な設定を示します。詳細は、[アクセスコントロールポリシーとルールのトラブルシューティング\(4-15 ページ\)](#)を参照してください。

ゾーン別にトラフィックを前処理するには、次の手順を実行します。

-
- 手順 1** ゾーン別にトラフィックを前処理するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか、または既存のルールを編集します。
- 詳細な手順については、[ネットワーク分析ルールを使用して前処理するトラフィックの指定 \(20-5 ページ\)](#)を参照してください。
- 手順 2** ネットワーク分析ルール エディタで、[ゾーン (Zones)] タブを選択します。
- [ゾーン (Zones)] タブが表示されます。
- 手順 3** [利用可能なゾーン (Available Zones)] から追加するゾーンを見つけて選択します。
- 追加するゾーンを検索するには、[利用可能なゾーン (Available Zones)] リストの上にある [名前を検索 (Search by name)] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。
- クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択 (Select All)] を選択します。
- 手順 4** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックして、選択したゾーンを適切なリストに追加します。
- 選択したゾーンをドラッグアンドドロップすることもできます。
- 手順 5** ルールを保存するか、編集を続けます。
- 変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。[設定変更の展開 \(4-14 ページ\)](#)を参照してください。
-

ネットワークごとのトラフィックの前処理

ライセンス:任意 (Any)

ネットワーク分析ルール内のネットワーク条件によって、その送信元および宛先 IP アドレス別にトラフィックを前処理することができます。前処理するトラフィックに対し送信元と宛先 IP アドレスを手動で指定でき、または、再利用可能で名前を 1 つ以上の IP アドレスおよびアドレスブロックに関連付けるネットワーク オブジェクトでネットワーク条件を設定できます。



ヒント

ネットワーク オブジェクトを作成しておくと、それを使用してネットワーク分析ルールを作成できるだけでなく、システムのモジュール インターフェイスのさまざまな場所で IP アドレスを表示することもできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、ネットワーク分析ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、[ネットワーク オブジェクトの操作 \(2-4 ページ\)](#)を参照してください。

1 つのネットワーク条件で [送信元ネットワーク (Source Networks)] および [宛先ネットワーク (Destination Networks)] それぞれに対し、最大 50 の項目を追加できます。

- IP アドレスからのトラフィックを照合するには、[送信元ネットワーク (Source Networks)] を設定します。
- IP アドレスへのトラフィックを照合するには、[宛先ネットワーク (Destination Networks)] を設定します。

送信元 (Source) ネットワーク条件と宛先 (Destination) ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコン(▲)は無効な設定を示します。詳細は、[アクセスコントロール ポリシーとルールのトラブルシューティング\(4-15 ページ\)](#)を参照してください。

ネットワーク別にトラフィックを前処理するには、次の手順を実行します。




-
- 手順 1** ネットワーク別にトラフィックを前処理するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか、または既存のルールを編集します。
- 詳細な手順については、[ネットワーク分析ルールを使用して前処理するトラフィックの指定\(20-5 ページ\)](#)を参照してください。
- 手順 2** ネットワーク分析ルール エディタで、[ネットワーク (Networks)] タブを選択します。
- [ネットワーク (Networks)] タブが表示されます。
- 手順 3** [利用可能なネットワーク (Available Networks)] から、次のように追加するネットワークを見つけて選択します。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[利用可能なネットワーク (Available Networks)] リストの上にある追加アイコン(+)をクリックし、[ネットワーク オブジェクトの操作\(2-4 ページ\)](#)の手順に従います。
 - 追加するネットワークを検索するには、[利用可能なネットワーク (Available Networks)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。
- オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択 (Select All)] を選択します。
- 手順 4** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックして、選択したオブジェクトを適切なリストに追加します。
- 選択したオブジェクトをドラッグ アンド ドロップすることもできます。
- 手順 5** 手で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。
- [送信元ネットワーク (Source Networks)] リストまたは [宛先ネットワーク (Destination Networks)] リストの下にある [IP アドレスの入力 (Enter an IP address)] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加 (Add)] をクリックします。
- 手順 6** ルールを保存するか、編集を続けます。
- 変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。[設定変更の展開\(4-14 ページ\)](#)を参照してください。
-

ネットワーク分析ルール管理

ライセンス:任意(Any)

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細 オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

カスタム ネットワーク分析ルールを編集するには、次の手順を実行します。

-
- 手順 1** カスタム前処理設定を変更するアクセス コントロール ポリシーで、[詳細設定(Advanced)] タブを選択して、[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン()をクリックします。
- [ネットワーク分析ポリシー(Network Analysis Policies)] ダイアログボックスが表示されます。モジュール インターフェイスには、カスタムのネットワーク分析ルールを追加していない場合は [カスタムルールなし(No Custom Rules)] と表示され、追加済みの場合は、設定されているルールの数が表示されます。
- 手順 2** [ネットワーク分析ルール(Network Analysis Rules)] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。
- ダイアログボックスが展開され、カスタム ルールが表示されます(ある場合)。
- 手順 3** カスタム ルールを編集します。次の選択肢があります。
- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある編集アイコン()をクリックします。
 - ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
 - ルールを削除するには、ルールの横にある削除アイコン()をクリックします。
- 手順 4** [OK] をクリックして変更を保存します。
- 変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。[設定変更の展開\(4-14 ページ\)](#)を参照してください。
-

