CHAPTER 19

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（19-1 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（19-3 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のネットワーク分析ポリシーを割り当てて、特定のセキュリティ ゾーンおよびネットワークに対する特定のトラフィックの前処理オプションをカスタマイズする方法について説明します。

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（23-1 ページ）
- パッシブ展開における前処理の調整（24-1 ページ）
- 侵入防御パフォーマンスの調整（11-6 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（11-17 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：すべて

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。

- 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 [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。
- 最初に [Block all traffic]デフォルト アクションを選択した場合、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は No Rules Active になります。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、[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（4-13 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。

ステップ 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、[Advanced]タブを選択し、[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。

[Network and Analysis Policies] ダイアログボックスが表示されます。

ステップ 2　[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　シスコ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。シスコでは、試験用にこのポリシーを使用します。

ステップ 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:すべて

*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復号化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、侵入ポリシーによるパケット インスペク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 Balanced Security and Connectivity ネットワーク分析ポリシーが、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 Balanced Security and Connectivity ネットワーク分析ポリシーおよび 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。しかし、ネットワーク分析ポリシーは前処理オプションの大部分を制御するのに対し、侵入ポリシーは侵入ルールの大部分を制御します。

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（20-2 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。

複雑な環境でのアドバンス 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。次に、システムがこれらのポリシーを使用し、異なるセキュリティ ゾーンまたはネットワークを使用してトラフィックの前処理を制御するように、システムを設定します。

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　プリプロセッサを無効にしているが、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。しかし、ネットワーク分析ポリシー インターフェイスでは無効のままです。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た前処理の調整は、**高度な**タスクです。前処理および侵入インスペク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 ポリシーの制限（17-12 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（19-4 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（19-4 ページ）
- ネットワーク分析ルールの管理（19-8 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:すべて

デフォルトでは、システムによって提供される 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。

ステップ 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、[Advanced]タブを選択し、[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。

[Network and Analysis Policies] ダイアログボックスが表示されます。

ステップ 2　[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　シスコ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。シスコでは、試験用にこのポリシーを使用します。

ステップ 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:すべて

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 19-1　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
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（19-6 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（19-7 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。

ステップ 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、[Advanced]タブを選択して、[Intrusion and Network Analysis 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。

[Network and Analysis Policies] ダイアログボックスが表示されます。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、モジュール インターフェイスには **No Custom Rules**（カスタム ルールがない）が示され、追加済みの場合はそれらのルールの数が表示されます。


ヒント

新しいウィンドウで [Network Analysis Policy] ページを表示するには、[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（20-3 ページ）を参照してください。

ステップ 2　[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）。

ステップ 3　[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。

ステップ 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（19-6 ページ）
- ネットワークごとのトラフィックの前処理（19-7 ページ）

ステップ 5　[Network Analysis]タブをクリックし、[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　シスコ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。シスコでは、試験用にこのポリシーを使用します。

ステップ 6　[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（19-8 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：すべて

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（2-35 ページ）を参照してください。

1 つのゾーン条件で [Source Zones]および [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 [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 [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 つを通っ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（4-13 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。

ステップ 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（19-4 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[Zones]タブを選択します。

[Zones] タブが表示されます。

ステップ 3　[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、[Available Zones]リストの上にある [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 [Select All] を選択します。

ステップ 4　[Add to Source]または [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。

ステップ 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（4-12 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：すべて

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すると、それを使用してネットワーク分析ルールを作成したり、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 アドレスを表すオブジェクトとして使用したりできます。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（2-3 ページ）を参照してください。

1 つのネットワーク条件で [Source Networks]および [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、[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、[Destination Networks]を設定します。

送信元ネットワーク条件と宛先ネットワーク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 IP アドレスの 1 つから発生し、宛先 IP アドレスの 1 つに向かう必要があります。

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（4-13 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。

ステップ 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（19-4 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[Networks]タブを選択します。

[Networks] タブが表示されます。

ステップ 3　[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。

- ネットワーク オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[Available Networks]リストの上にある追加アイコン（⊕）をクリックします。ネットワーク オブジェクトの操作（2-3 ページ） を参照してください。
- 追加するネットワークを検索するには、[Available Networks]リストの上にある [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 [Select All]を選択します。

ステップ 4　[Add to Source]または [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。

ステップ 5　手動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。

[Source Networks]リストまたは [Destination Networks] リストの下にある [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 [Add] をクリックします。

ステップ 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（4-12 ページ）を参照してください）。

ネットワーク分析ルールの管理

ライセンス：すべて

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。

ステップ 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、[Advanced]タブを選択して、[Intrusion and Network Analysis 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。

[Network and Analysis Policies] ダイアログボックスが表示されます。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、Web インターフェイスには **No Custom Rules**（カスタム ルールがない）と示され、追加済みの場合はそれらのルールの数が表示されます。

ステップ 2　[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）。

ステップ 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。

ステップ 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（4-12 ページ）を参照してください）。