ネットワークベースのルールによるトラフィックの制御

*アクセス コントロール ポリシー*内の *アクセス コントロール ルール*は、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。ネットワークベースの条件によって、次の条件の 1 つ以上を使用してネットワークを通過するトラフィックを管理できます。

- 送信元と宛先セキュリティ ゾーン
- 送信元と宛先 IP アドレスまたは地理的位置
- トランスポート層プロトコルおよび ICMP コード オプションも含む、送信元と宛先ポート

ネットワークベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純または複雑にすることができ、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（6-1 ページ）を参照してください。

(注) セキュリティ インテリジェンス ベースのトラフィック フィルタリングと、一部の復号化および前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号することができます。

表 7-1　ネットワークベースのアクセス コントロール ルールのライセンス要件

要件	位置情報制御	他のすべてのネットワークベースの制御
ライセンス	任意（Any）	任意（Any）

ネットワークベースのアクセス コントロール ルールの作成については、以下を参照してください。

- セキュリティ ゾーンによるトラフィックの制御（7-2 ページ）
- ネットワークまたは地理的位置によるトラフィックの制御（7-3 ページ）
- ポートおよび ICMP コードによるトラフィックの制御（7-6 ページ）

セキュリティ ゾーンによるトラフィックの制御

ライセンス:任意（Any）

アクセス コントロール 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制御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。

単純な例として、内部と外部の 2 つのゾーンを作成し、デバイスの最初のインターフェイスのペアをそれらのゾーンに割り当てることが可能です。内部側のネットワークに接続されたホストは、保護されている資産を表します。

このシナリオを拡張するには、同様に設定されたデバイスを追加で展開して、複数の異なるロケーションで同様のリソースを保護することができます。これらの各デバイスは、内部セキュリティ ゾーンのアセットを保護します。

ヒント　内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。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。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、それでもやはり、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したい場合があります。

アクセス コントロールを使用してこれを実現するには、[宛先ゾーン（Destination Zones）] が [内部（Internal）] に設定されているゾーン条件を持つアクセス コントロール ルールを設定します。この単純なアクセス コントロール ルールは、内部ゾーンの任意のインターフェイスからデバイスを離れるトラフィックを照合します。

一致するトラフィックが侵入やマルウェアについて確実に検査されるようにするには、ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。詳細については、ルール アクションを使用したトラフィックの処理とインスペクションの決定（6-8 ページ）および侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（11-1 ページ）を参照してください。

より複雑なルールを作成する場合は、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を*離れる*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ため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン（Destination Zones）] 条件で使用することはできません。
- ゾーン内のインターフェイスからデバイスに*入る*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 つを通って出力する必要があります。

ゾーン条件を作成する際、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。

ゾーン別にトラフィックを制御するには、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制御するアクセス コントロール ポリシーで、新しいアクセス コントロール 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、アクセス コントロール ルールの作成および編集（6-3 ページ）を参照してください。

手順 2　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 [名前で検索（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。

ネットワークまたは地理的位置によるトラフィックの制御

ライセンス：機能に応じて異なる

アクセス コントロール 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制御することができます。次のいずれかの操作を実行できます。

- 制御するトラフィックの送信元および宛先 IP アドレスを明示的に指定します。または、
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御します。

ネットワークベースのアクセス コントロール ルールの条件を作成するには、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報*オブジェクト*を使用してネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトまたは位置情報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。詳細については、再使用可能オブジェクトの管理（2-1 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する必要があります。このため、CiscoではASA FirePOWER モジュールの位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。位置情報データベースの更新（46-22 ページ）を参照してください。

表 7-2　ネットワーク条件のライセンス要件

要件	位置情報制御	IP アドレス制御
ライセンス	任意（Any）	任意（Any）

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、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- IP アドレスまたは地理的位置*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 アドレスまたは地理的位置*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。

ネットワーク条件を使用すると、送信元のクライアントに基づいてプロキシ トラフィックを処理することもできます。送信元ネットワーク条件を使用してプロキシ サーバを指定し、次に、元のクライアント制約を追加して、送信元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアント アドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の 3 つのルールを作成します。

ルール 1：特定の IP アドレス（209.165.201.1）からの非プロキシ トラフィックをブロックします。

送信元ネットワーク：209.165.201.1

元のクライアント ネットワーク：none または any

アクション: Block

ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシ サーバが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238

元のクライアント ネットワーク：209.165.201.1

アクション: Allow

ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバを使用する場合はブロックします。

送信元ネットワーク：any

元のクライアント ネットワーク：209.165.201.1

アクション: Block

ネットワークまたは地理的位置別にトラフィックを制御するには、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制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（6-3 ページ）を参照してください。

手順 2　ルール エディタで、[ネットワーク（Networks）] タブを選択します。

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。

- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- 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 オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[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て、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　プロキシ トラフィックをフィルタリングするには、以下の手順に従います。

- [送信元（Source）] サブタブをクリックして、送信元ネットワーク制約を指定します。
- [元のクライアント（Original Client）] サブタブをクリックして、元のクライアント ネットワーク制約を指定します。プロキシ接続では、ルールに一致するには、元のクライアントの IP アドレスがこれらのネットワークのいずれか 1 つと一致する必要があります。

手順 5　[送信元に追加（Add to Source）]、[元のクライアントに追加（Add to Original Client）]、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 6　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。

[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 7　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。

ポートおよび ICMP コードによるトラフィックの制御

ライセンス:任意（Any）

アクセス コントロール 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ポート別にトラフィックを制御することができます。このコンテンツでは、「ポート」は次のいずれかを示します。

- TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。システムは、カッコ内に記載されたプロトコル番号 + オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。例：ICMP(1):3:3
- ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

ポート ベースのアクセス コントロール ルールの条件を作成するときは、手動でポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート *オブジェクト*を使用してポート条件を設定できます。

ヒント　ポート オブジェクトを作成しておくと、それを使用してアクセス コントロール 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ポートを表示することもできます。ポート 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するか、またはアクセス コントロール ルールの設定時にオンザフライで作成できます。詳細については、ポート オブジェクトの操作（2-10 ページ）を参照してください。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- ポートからのトラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。

  送信元ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

- ポートへのトラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。

  宛先ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。

- 特定の**選択した送信元ポート**から発生し、特定の**選択した宛先ポート**に向かうトラフィックを照合するには、両方設定します。

  送信元ポートと宛先ポートの両方を条件に追加する場合は、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

ポート条件を作成する際は、次の点に注意します。

- タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートを追加すると、アクセス コントロール ルールは要求されていないエコー応答だけを照合します。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

- 宛先ポート条件として GRE（47）プロトコルを使用する場合、アクセス コントロール ルールに追加できるのは、他のネットワーク ベースの条件（つまりゾーンおよびネットワーク条件）のみです。レピュテーションまたはユーザ ベースの条件を追加する場合は、ルールを保存できません。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクト マネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。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。

ポート別にトラフィックを制御するには、次の手順を実行します。

手順 1　ポート別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール 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、アクセス コントロール ルールの作成および編集（6-3 ページ）を参照してください。

手順 2　ルール エディタで、[ポート（Ports）] タブを選択します。

[ポート（Ports）] タブが表示されます。

手順 3　[使用可能なポート（Available Ports）] から、次のように追加するポートを見つけて選択します。

- ここでポート オブジェクトを作成してリストに追加するには、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（  ）をクリックし、ポート オブジェクトの操作（2-10 ページ）の手順に従います。
- 追加するポート オブジェクトおよびグループを検索するには、[使用可能なポート（Available Ports）] 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、オブジェクトの名前またはオブジェクトのポートの値を入力します。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。たとえば、「80」と入力すると、ASA FirePOWER モジュールには、Cisco 提供の HTTP ポート 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　手動で指定する送信元ポートまたは宛先ポートを追加します。

- 送信元ポートの場合は、[選択した送信元ポート（Selected Source Ports）] リストの下の [プロトコル（Protocol）] ドロップダウンリストから [TCP] または [UDP] を選択します。次に、**ポート**を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。
- 宛先ポートの場合は、[選択した宛先ポート（Selected Destination Ports）] リストの下の [プロトコル（Protocol）] ドロップダウンリストからプロトコル（すべてのプロトコルの場合は [すべて（All）]）を選択します。リストに表示されない割り当てられていないプロトコルの数字を入力することもできます。

  [ICMP] または [IPv6-ICMP] を選択すると、ポップアップ ウィンドウが表示され、タイプと関連するコードを選択できます。ICMP のタイプとコードの詳細については、http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml [英語] および http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml [英語] を参照してください。

  プロトコルを指定しない場合、またはオプションで TCP または UDP を指定した場合は、**ポート**を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

[追加（Add）] をクリックします。ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

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。