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。

- 送信元と宛先のセキュリティ ゾーン
- 送信元と宛先の 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 コードオプションを含む、送信元と宛先のポート

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 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、および一部の復号化と前処理は、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化することができます。

表 *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	任意

- セキュリティ ゾーンによるトラフィックの制御 （2 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

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できます。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、追加で同様に設定されたデバイスを配置して、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も、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 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、[Destination Zone] が [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 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。

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 [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を離れ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**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 [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。

ステップ 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を参照してください。

ステップ 2 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（設定変更の導入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、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再利用可能なネットワーク オブジェクトおよび地理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 オブジェクトや位置情報オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、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。詳細については、再使用可能オブジェクトの管理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、確実に最新の地理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ために、ASA FirePOWER モジュールで地理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お勧めします。地理情報データベースについてを参照してください。

表 *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	任意

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、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、[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、[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を参照してください。

ネットワーク条件により、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

元のネットワーク クライアント：none または any

アクション：ブロック

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：許可

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。

[Source Networks]：any

元のクライアント ネットワーク：209.165.201.1

アクション：ブロック

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。

ステップ 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を参照してください。

ステップ 2 ルール エディタで、[Networks] タブを選択します。

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。

- 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 [Networks] タブをクリックします。地理位置情報オブジェクトを表示するには [Geolocation] タブをクリックします。
- ネットワーク オブジェクト（後で条件に追加可能）をその場で追加するには、[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を参照してください。
- 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、[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 [Select All] を選択します。

ステップ 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。

- [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。
- [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、元のクライアントの IP アドレスは、ルールに一致するネットワークの 1 つと一致する必要があります。

ステップ 5 [Add to Source]、[Add to Original Client]、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 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。

[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 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（設定変更の導入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

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、名前を 1 つ以上のポートに関連付ける再利用可能なポート 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ポートを表すオブジェクトとして使用したりできます。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 ルールの設定時にその場で作成できます。詳細については、このセクションの後半の手順を参照してください。

1 つのネットワーク条件で [Selected Source Ports] および [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、[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、[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。詳細については、ポート オブジェクトの操作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。

ステップ 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 ルールを使用したトラフィック フローの調整を参照してください。

ステップ 2 ルール エディタで、[Ports] タブを選択します。

[Ports] タブが表示されます。

ステップ 3 [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。

- ポート オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Ports] リストの上にある追加アイコンをクリックします。ポート オブジェクトの操作を参照してください。
- 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、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクト内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 モジュールにシスコ提供の 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 [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、[Selected Source Ports] リストの下の [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、[Selected Destination Ports] リストの下の [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 [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。詳細については、IANA サイト ICMP types and codes または ICMP v6 types and codes 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。

[Add] をクリックします。ASA FirePOWER モジュールでは、無効な設定となるルール条件にはポートが追加されません。

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（設定変更の導入を参照してください）。