



ACL のオブジェクト グループ

- [ACL のオブジェクト グループ \(1 ページ\)](#)

ACL のオブジェクト グループ

ACL のオブジェクトグループ機能を使用して、ユーザ、デバイス、またはプロトコルをグループに分類し、これらのグループをアクセスコントロールリスト (ACL) に適用してアクセスコントロールポリシーを作成できます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクトグループを使用できるようになります。この機能は、複数のアクセスコントロールエントリ (ACE) を許可しますが、各 ACE を使用して、ユーザのグループ全体に対してサーバまたはサービスのグループへのアクセスを許可または禁止できます。

大規模なネットワークでは、ACL の行数が大量 (数百行) になり、特に ACL が頻繁に変更される場合は ACL の設定および管理が困難になります。オブジェクトグループベースの ACL は、従来の ACL よりも小さく、読みやすく、設定と管理が容易であるため、Cisco IOS ルータでの大規模なユーザアクセス環境での静的および動的な ACL の導入が簡素化されます。

Cisco IOS ファイアウォールでは、オブジェクトグループはポリシーの作成を簡素化することから (たとえば、グループ A にグループ A サービスへのアクセスを許可するなど) オブジェクトグループによるメリットが得られます。

ACL のオブジェクト グループに関する制約事項

- オブジェクトグループは、拡張名付き ACL および番号付き ACL でのみ使用できます。
- オブジェクトグループベースの ACL は、IPv4/IPv6 アドレスのみをサポートします。
- オブジェクトグループベースの ACL は、レイヤ3 インターフェイス (ルーテッドインターフェイスや VLAN インターフェイスなど) とサブインターフェイスのみをサポートします。
- オブジェクトグループベースの ACL は、IPsec ではサポートされていません。

- オブジェクトグループを使用する ACL ステートメントは、処理のために RP に送信されるパケットでは無視されます。
- ACL でサポートされるオブジェクトグループベースの ACE の数は、TCAM が利用できるかどうかに応じてプラットフォームによって異なります。

ACL のオブジェクト グループに関する情報

従来型 ACE を設定し、ACE が同じ ACL 内のオブジェクトグループを参照するように設定できます。

オブジェクトグループベースの ACL は、Quality of Service (QoS) 一致基準、Cisco IOS ファイアウォール、Dynamic Host Configuration Protocol (DHCP)、およびその他の拡張 ACL を使用する機能で使用できます。さらに、マルチキャストトラフィックでオブジェクトグループベースの ACL を使用することもできます。

多数のインバウンドおよびアウトバウンドパケットがある場合、オブジェクトグループベースの ACL を使用すると、従来型の ACL を使用する場合よりパフォーマンスが向上します。また、大規模な構成では、ACE でオブジェクトグループを使用することで、アドレスとプロトコルのペアごとに個別の ACE を定義する必要がなくなるため、NVRAM に必要なストレージを削減できます。

オブジェクト グループ

オブジェクトグループには、単一のオブジェクト（単一の IP アドレス、ネットワーク、またはサブネットなど）または複数のオブジェクト（複数の IP アドレスの組み合わせ、ネットワーク、またはサブネットなど）を含めることができます。

一般的なアクセス コントロール エントリ (ACE) では、ユーザのグループが特定のサーバグループにのみアクセスできます。オブジェクトグループベースのアクセスコントロールリスト (ACL) では、多数の ACE を作成する（各 ACE に異なる IP アドレスが必要）代わりに、オブジェクトグループ名を使用する単一の ACE を作成できます。同様のオブジェクトグループ（プロトコルポートグループなど）を拡張して、ユーザグループの一連のアプリケーションのみアクセス可能にできます。ACE には、送信元のみ、宛先のみ、なし、または両方のオブジェクトグループを含めることができます。

オブジェクトグループを使用して、ACE のコンポーネントの所有権を分離できます。たとえば、組織内の各部門がそのグループメンバーシップを制御し、管理者が ACE 自体を所有して、どの部門が相互に通信できるかを制御します。

Cisco Policy Language (CPL) クラスマップを使用する機能でオブジェクトグループを使用できます。

この機能は、ACL パラメータをグループ化するために、ネットワーク オブジェクト グループとサービス オブジェクト グループの 2 種類のオブジェクトグループをサポートします。これらのオブジェクトグループを使用して、IP アドレス、プロトコル、プロトコルサービス（ポート）、および Internet Control Message Protocol (ICMP) タイプをグループ化します。

ネットワーク オブジェクト グループで許可されるオブジェクト

ネットワーク オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- 0.0.0.0 から 255.255.255.255 までの範囲の任意の IP アドレス (**any** コマンドを使用して指定します)。
- ホスト IP アドレス
- ホスト名
- その他のネットワーク オブジェクト グループ
- サブネット

- ホスト IP アドレス
- グループ メンバーのネットワーク アドレス
- ネストされたオブジェクト グループ

サービス オブジェクト グループで許可されるオブジェクト

サービス オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- 送信元および宛先プロトコルポート (Telnet や Simple Network Management Protocol (SNMP) など)
- Internet Control Message Protocol (ICMP) タイプ (エコー、エコー応答、ホスト到達不能など)
- トップレベルプロトコル (Encapsulating Security Payload (ESP)、TCP、UDP など)
- その他のサービス オブジェクト グループ

オブジェクト グループに基づく ACL

従来のアクセス コントロール リスト (ACL) を使用または参照する機能はすべて、オブジェクトグループベースの ACL と互換性があり、従来の ACL の機能インタラクションはオブジェクトグループベース ACL と同じです。この機能により、オブジェクトグループベースの ACL をサポートできるように従来の ACL が拡張され、新しいキーワードと、送信元アドレス、宛先アドレス、送信元ポート、および宛先ポートが追加されます。

オブジェクト グループ メンバーシップ リストでは、(オブジェクト グループを削除および再定義せずに) オブジェクトを動的に追加、削除、または変更できます。また、オブジェクトグループ メンバーシップ リストでは、オブジェクト グループを使用する ACL アクセス コントロール エントリ (ACE) を再定義せずに、オブジェクトを追加、削除、または変更できます。グループにオブジェクトを追加してから、グループからオブジェクトを削除することで、ACL をインターフェイスに再適用せずに、オブジェクトグループベースの ACL 内で変更が正しく機能することを確認できます。

ソース グループのみ、宛先グループのみ、またはソース グループと宛先グループの両方を使用して、オブジェクトグループベースの ACL を複数回設定できます。

ACL 内またはクラス ベース ポリシー言語 (CPL) ポリシー内で使用されているオブジェクト グループは削除できません。

ACL のオブジェクト グループの設定方法

ACL のオブジェクト グループを設定するには、最初に 1 つ以上のオブジェクト グループを作成します。作成するオブジェクトグループは、ネットワーク オブジェクト グループ (ホスト アドレスやネットワークアドレスなどのオブジェクトが含まれるグループ) またはサービス オブジェクト グループ (ポート番号に **lt**、**eq**、**gt**、**neq**、**range** などの演算子を使用するグループ) を任意に組み合わせることができます。オブジェクトグループを作成した後、それらのグループにポリシー (**permit** または **deny** など) を適用するアクセス コントロール エントリ (ACE) を作成します。

ネットワーク オブジェクト グループの作成

単一のオブジェクト (単一の IP アドレス、ホスト名、別のネットワーク オブジェクト グループ、またはサブネットなど) または複数のオブジェクトを含むネットワーク オブジェクト グループには、オブジェクトのアクセス制御ポリシーを作成するための、ネットワーク オブジェクト グループ ベース ACL が関連付けられています。

ネットワーク オブジェクト グループを作成するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	object-group network <i>object-group-name</i> 例 : Device(config)# object-group network my-network-object-group	オブジェクトグループ名を定義し、ネットワーク オブジェクト グループ コンフィギュレーション モードを開始します。
ステップ 4	description <i>description-text</i> 例 : Device(config-network-group)# description test engineers	(オプション) オブジェクト グループの説明を指定します。 • 最大 200 文字を使用できます。

	コマンドまたはアクション	目的
ステップ 5	host { <i>host-address</i> <i>host-name</i> } 例 : <pre>Device(config-network-group)# host 209.165.200.237</pre>	(オプション) ホストの IP アドレスまたは名前を指定します。 <ul style="list-style-type: none"> ホストアドレスを指定する場合、IPv4 アドレスを使用する必要があります。
ステップ 6	network-address { <i>/nn</i> <i>network-mask</i> } 例 : <pre>Device(config-network-group)# 209.165.200.225 255.255.255.224</pre>	(オプション) サブネットオブジェクトを指定します。 <ul style="list-style-type: none"> ネットワークアドレスには IPv4 アドレスを指定する必要があります。デフォルトのネットワークマスクは 255.255.255.255 です。
ステップ 7	group-object <i>nested-object-group-name</i> 例 : <pre>Device(config-network-group)# group-object my-nested-object-group</pre>	(オプション) 現在の (親) オブジェクトグループに含めるネストされた (子) オブジェクトグループを指定します。 <ul style="list-style-type: none"> 子オブジェクトグループのタイプは親のタイプと一致している必要があります (たとえば、ネットワークオブジェクトグループを作成する場合、子として別のネットワークオブジェクトグループを指定する必要があります)。 グループオブジェクト内で重複するオブジェクトの使用は、オブジェクトグループのネストによるのみ可能です。たとえば、オブジェクト 1 がグループ A とグループ B の両方に含まれる場合、A と B の両方を含むグループ C を定義できません。ただし、グループ階層の循環を引き起こすグループオブジェクトを含めることはできません (たとえば、グループ A をグループ B に含め、次にグループ B をグループ A に含めることはできません)。 ネストされたオブジェクトグループのレベルの数は無制限に使用できます (ただし、最大 2 つのレベルを推奨します)。

	コマンドまたはアクション	目的
ステップ 8	オブジェクトグループのベースとなるオブジェクトを指定するまで、手順を繰り返します。	—
ステップ 9	end 例： Device(config-network-group)# end	ネットワークオブジェクトグループコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

サービスオブジェクトグループの作成

TCP または UDP ポートまたはポート範囲を指定するにはサービスオブジェクトグループを使用します。サービスオブジェクトグループがアクセスコントロールリスト (ACL) に関連付けられると、このサービスオブジェクトグループベースの ACL はポートへのアクセスを制御できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	object-group service <i>object-group-name</i> 例： Device(config)# object-group service my-service-object-group	オブジェクトグループ名を定義し、サービスオブジェクトグループコンフィギュレーションモードを開始します。
ステップ 4	description <i>description-text</i> 例： Device(config-service-group)# description test engineers	(オプション) オブジェクトグループの説明を指定します。 • 最大 200 文字を使用できます。
ステップ 5	protocol 例： Device(config-service-group)# ahp	(オプション) IP プロトコルの番号または名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	<p>{tcp udp tcp-udp} [source {[eq] lt gt} port1 range port1 port2}] [[eq] lt gt} port1 range port1 port2]</p> <p>例 :</p> <pre>Device(config-service-group)# tcp-udp range 2000 2005</pre>	<p>(オプション) TCP、UDP、または両方を指定します。</p>
ステップ 7	<p>icmp icmp-type</p> <p>例 :</p> <pre>Device(config-service-group)# icmp conversion-error</pre>	<p>(オプション) Internet Control Message Protocol (ICMP) タイプの 10 進数または名前を指定します。</p>
ステップ 8	<p>group-object nested-object-group-name</p> <p>例 :</p> <pre>Device(config-service-group)# group-object my-nested-object-group</pre>	<p>(オプション) 現在の (親) オブジェクトグループに含めるネストされた (子) オブジェクトグループを指定します。</p> <ul style="list-style-type: none"> 子オブジェクトグループのタイプは親のタイプと一致している必要があります (たとえば、ネットワークオブジェクトグループを作成する場合、子として別のネットワークオブジェクトグループを指定する必要があります)。 グループオブジェクト内で重複するオブジェクトの使用は、オブジェクトグループのネストによってのみ可能です。たとえば、オブジェクト 1 がグループ A とグループ B の両方に含まれる場合、A と B の両方を含むグループ C を定義できます。ただし、グループ階層の循環を引き起こすグループオブジェクトを含めることはできません (たとえば、グループ A をグループ B に含め、次にグループ B をグループ A に含めることはできません)。 ネストされたオブジェクトグループのレベルの数は無制限に使用できます (ただし、最大 2 つのレベルを推奨します)。

	コマンドまたはアクション	目的
ステップ 9	手順を繰り返して、オブジェクト グループのベースとなるオブジェクトを指定します。	—
ステップ 10	end 例： Device(config-service-group)# end	サービス オブジェクト グループ コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

オブジェクト グループ ベース ACL の作成

オブジェクト グループ ベースのアクセス コントロール リスト (ACL) を作成する場合、1 つ以上のオブジェクトグループを参照する ACL を設定します。従来の ACE と同様に、同じアクセス ポリシーを 1 つまたは複数のインターフェイスと関連付けることができます。

同じオブジェクトグループベース ACL 内のオブジェクトグループを参照する、複数のアクセス コントロール エントリ (ACE) を定義できます。また、複数の ACE で特定のオブジェクトグループを再利用できます。

オブジェクト グループ ベース ACL を作成するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ip access-list extended <i>access-list-name</i> 例： Device(config)# ip access-list extended nomarketing	名前を使用して拡張 IP アクセス リストを定義し、拡張アクセス リスト コンフィギュレーションモードを開始します。
ステップ 4	remark <i>remark</i> 例： Device(config-ext-nacl)# remark protect server by denying access from the Marketing network	(任意) 設定されたアクセス リスト エントリに関するコメントを追加します。 • 注釈はアクセス リスト エントリの前または後に指定できます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> この例では、注釈によって、後続のエントリがインターフェイスに対する Marketing ネットワークアクセスを拒否することをネットワーク管理者に示します。
ステップ 5	<p>deny protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log log-input] [time-range time-range-name] [fragments]</p> <p>例 :</p> <pre>Device(config-ext-nacl)# deny ip 209.165.200.244 255.255.255.224 host 209.165.200.245 log</pre> <p>Example based on object-group:</p> <pre>Router(config)#object-group network my_network_object_group Router(config-network-group)#209.165.200.224 255.255.255.224 Router(config-network-group)#exit Router(config)#object-group network my_other_network_object_group Router(config-network-group)#host 209.165.200.245 Router(config-network-group)#exit Router(config)#ip access-list extended nomarketing Router(config-ext-nacl)#deny ip object-group my_network_object_group object-group my_other_network_object_group log</pre>	<p>(任意) ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。</p> <ul style="list-style-type: none"> 必要に応じて、object-group service-object-group-name キーワードおよび引数を、<i>protocol</i> 引数の代わりに使用します。 必要に応じて、object-group source-network-object-group-name キーワードおよび引数を、<i>source source-wildcard</i> 引数の代わりに使用します。 必要に応じて、object-group destination-network-object-group-name キーワードおよび引数を、<i>destination destination-wildcard</i> 引数の代わりに使用します。 <i>source-wildcard</i> または <i>destination-wildcard</i> を省略すると、0.0.0.0 のワイルドカードマスクが想定され、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 必要に応じて、<i>source source-wildcard</i> または <i>destination destination-wildcard</i> の代わりに、キーワード any を使用して、アドレスと 0.0.0.0 255.255.255.255 のワイルドカードを指定します。 必要に応じて、host source キーワードおよび引数を使用して送信元と <i>source</i> 0.0.0.0 の送信元ワイルドカードを示すか、host destination キーワードおよび引数を使用して宛

	コマンドまたはアクション	目的
		<p>先と <i>destination</i> 0.0.0.0 の宛先ワイルドカードを示します。</p> <ul style="list-style-type: none"> この例では、すべての送信元のパケットは、宛先ネットワーク 209.165.200.244 へのアクセスが拒否されます。アクセスリストによって許可または拒否されるパケットに関するロギングメッセージは、logging facility コマンドに設定された設備に送信されます（たとえば、コンソール、端末、syslog）。つまり、パケットがアクセスリストに一致する場合は常に、パケットに関する情報を提供するロギングメッセージが設定された設備に送信されます。コンソールにロギングするメッセージのレベルは、logging console コマンドで制御します。
ステップ 6	<p>remark <i>remark</i></p> <p>例 :</p> <pre>Device(config-ext-nacl)# remark allow TCP from any source to any destination</pre>	<p>(任意) 設定されたアクセスリストエントリに関するコメントを追加します。</p> <ul style="list-style-type: none"> 注釈はアクセスリストエントリの前または後に指定できます。
ステップ 7	<p>permit <i>protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log log-input] [time-range time-range-name] [fragments]</i></p> <p>例 :</p> <pre>Device(config-ext-nacl)# permit tcp any any</pre>	<p>ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。</p> <ul style="list-style-type: none"> 各アクセスリストには、少なくとも 1 つの permit ステートメントが必要です。 必要に応じて、object-group <i>service-object-group-name</i> キーワードおよび引数を、<i>protocol</i> の代わりに使用します。 必要に応じて、object-group <i>source-network-object-group-name</i> キーワードおよび引数を、<i>source source-wildcard</i> の代わりに使用します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 必要に応じて、object-group destination-network-object-group-name キーワードおよび引数を、<i>destination destination-wildcard</i> の代わりに使用します。 • <i>source-wildcard</i> または <i>destination-wildcard</i> を省略すると、0.0.0.0 のワイルドカードマスクが想定され、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、<i>source source-wildcard</i> または <i>destination destination-wildcard</i> の代わりに、キーワード any を使用して、アドレスと 0.0.0.0 255.255.255.255 のワイルドカードを指定します。 • この例では、任意の送信元から任意の宛先への TCP パケットが許可されています。 • log-input キーワードを使用して、ロギング出力に入力インターフェイス、送信元 MAC アドレス、または仮想回線を含めます。
ステップ 8	手順を繰り返して、アクセスリストのベースとなるフィールドと値を指定します。	明示的に許可されていないすべての送信元は、アクセスリストの末尾にある暗黙的な deny ステートメントで拒否されます。
ステップ 9	end 例： <pre>Device(config-ext-nacl)# end</pre>	拡張アクセスリスト コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

インターフェイスへのオブジェクトグループベースの ACL の適用

オブジェクトグループベースの ACL をインターフェイスに適用するには、**ip access-group** コマンドを使用します。オブジェクトグループベースのアクセスコントロールリスト (ACL) を使用して、適用先のインターフェイスのトラフィックを制御できます。

オブジェクトグループベースの ACL をインターフェイスに適用するには、以下のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface type number 例： Device(config)# interface vlan 100	インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	ip access-group {access-list-name access-list-number} {in out} 例： Device(config-if)# ip access-group my-ogacl-policy in	ACL をインターフェイスに適用し、インバウンドパケットまたはアウトバウンドパケットをフィルタリングするかどうかを指定します。
ステップ 5	end 例： Device(config-if)# end	インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ACL のオブジェクトグループの確認

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	show object-group [object-group-name] 例：	名前付きまたは番号付きオブジェクトグループ（名前が入力されていない場合

	コマンドまたはアクション	目的
	Device# show object-group my-object-group	はすべてのオブジェクトグループ) の設定を表示します。
ステップ 3	show ip access-list [<i>access-list-name</i>] 例 : Device# show ip access-list my-ogacl-policy	名前付きまたは番号付きアクセスリストまたはオブジェクトグループベース ACL (名前が入力されていない場合はすべてのアクセスリストおよびオブジェクトグループベース ACL) の内容を表示します。

ACL 用オブジェクトグループの設定例

例：ネットワークオブジェクトグループの作成

次に、2つのホストと1つのサブネットをオブジェクトとして含む、my-network-object-group という名前のネットワークオブジェクトグループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group network my-network-object-group
Device(config-network-group)# description test engineers
Device(config-network-group)# host 209.165.200.237
Device(config-network-group)# host 209.165.200.238

Device(config-network-group)# 209.165.200.241 255.255.255.224
Device(config-network-group)# end
```

次に、2つのホスト、1つのサブネット、および my-nested-object-group という名前の既存のオブジェクトグループ (子) をオブジェクトとして含む、my-company-network という名前のネットワークオブジェクトグループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group network my-company-network
Device(config-network-group)# host host1
Device(config-network-group)# host 209.165.200.242
Device(config-network-group)# 209.165.200.225 255.255.255.224
Device(config-network-group)# group-object my-nested-object-group
Device(config-network-group)# end
```

例：サービスオブジェクトグループの作成

次に、複数の ICMP、TCP、UDP、および TCP-UDP プロトコルと my-nested-object-group という名前の既存のオブジェクトグループをオブジェクトとして含む、my-service-object-group という名前のサービスオブジェクトグループを作成する例を示します。

```
Device> enable
```

例：オブジェクトグループベースの ACL の作成

```

Device# configure terminal
Device(config)# object-group service my-service-object-group
Device(config-service-group)# icmp echo
Device(config-service-group)# tcp smtp
Device(config-service-group)# tcp telnet
Device(config-service-group)# tcp source range 1 65535 telnet
Device(config-service-group)# tcp source 2000 ftp
Device(config-service-group)# udp domain
Device(config-service-group)# tcp-udp range 2000 2005
Device(config-service-group)# group-object my-nested-object-group
Device(config-service-group)# end

```

例：オブジェクトグループベースの ACL の作成

次に、プロトコルポートが my-service-object-group で指定されたポートと一致する場合に、my-network-object-group 内のユーザからのパケットを許可する object-group-based ACL を作成する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ip access-list extended my-ogacl-policy
Device(config-ext-nacl)# permit object-group my-service-object-group object-group
my-network-object-group any
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# end

```

インターフェイスへのオブジェクトグループベースの ACL の適用

オブジェクトグループベースの ACL をインターフェイスに適用するには、**ip access-group** コマンドを使用します。オブジェクトグループベースのアクセスコントロールリスト (ACL) を使用して、適用先のインターフェイスのトラフィックを制御できます。

オブジェクトグループベースの ACL をインターフェイスに適用するには、以下のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface <i>type number</i> 例： Device(config)# interface vlan 100	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip access-group { <i>access-list-name</i> <i>access-list-number</i> } { in out } 例： Device(config-if)# ip access-group my-ogacl-policy in	ACL をインターフェイスに適用し、インバウンドパケットまたはアウトバウンドパケットをフィルタリングするかどうかを指定します。
ステップ 5	end 例： Device(config-if)# end	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：ACL 用オブジェクトグループの確認

次に、すべてのオブジェクトグループを表示する例を示します。

```
Device# show object-group

Network object group auth-proxy-acl-deny-dest
 host 209.165.200.235
Service object group auth-proxy-acl-deny-services
 tcp eq www
 tcp eq 443
Network object group auth-proxy-acl-permit-dest
 209.165.200.226 255.255.255.224
 209.165.200.227 255.255.255.224
 209.165.200.228 255.255.255.224
 209.165.200.229 255.255.255.224
 209.165.200.246 255.255.255.224
 209.165.200.230 255.255.255.224
 209.165.200.231 255.255.255.224
 209.165.200.232 255.255.255.224
 209.165.200.233 255.255.255.224
 209.165.200.234 255.255.255.224
Service object group auth-proxy-acl-permit-services
 tcp eq www
 tcp eq 443
```

次に、特定の object-group-based ACL に関する情報を表示する例を示します。

```
Device# show ip access-list my-ogacl-policy

Extended IP access list my-ogacl-policy
10 permit object-group eng_service any any
```

ACL 用オブジェクトグループに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference: Commands A to C』 『Cisco IOS Security Command Reference: Commands D to L』 『Cisco IOS Security Command Reference: Commands M to R』 『Cisco IOS Security Command Reference: Commands S to Z』
ACL 設定ガイド	『セキュリティコンフィギュレーションガイド』の「アクセスコントロールリスト」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL のオブジェクトグループの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.12.1	ACL のオブジェクトグループ	ACL 用オブジェクトグループ機能を使用すれば、ユーザ、デバイス、またはプロトコルをグループに分類して、それらをアクセスコントロールリスト (ACL) に適用し、そのグループ用のアクセスコントロールポリシーを作成することができます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクトグループを使用できるようになります。この機能は、複数のアクセスコントロールエントリ (ACE) を許可しますが、各 ACE を使用して、ユーザのグループ全体に対してサーバまたはサービスのグループへのアクセスを許可または禁止できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

