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。この機能では、複数のアクセス コントロール エントリ（ACE）を使用できます。それぞれの ACE を使用してユーザのグループ全体にサーバやサービスのグループに対するアクセスを許可したり、アクセスを拒否したりできるため、ACL のサイズが削減されて管理が容易になります。

このモジュールでは、ゾーンベース ポリシー ファイアウォールでのオブジェクト グループ ACL の概要と、ゾーンベース ファイアウォールを設定する方法を説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ACL のオブジェクト グループに関する制約事項

以下の制限が、ゾーンベース ファイアウォール上の ACL 用オブジェクト グループ機能に適用されます。

- IPv6 はサポートされていません。
- 動的およびユーザ単位のアクセス コントロール リスト（ACL）はサポートされません。
- ACL 内で使用されている場合は、オブジェクト グループを削除したり、オブジェクト グループを空にしたりすることができません。
- 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。
- オブジェクト グループは IP 拡張 ACL でのみサポートされます。

ACL のオブジェクト グループに関する情報

ACL のオブジェクト グループの概要

大規模なネットワークでは、アクセス コントロール リスト（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 は小規模で読みやすく、簡単に設定および管理できます。オブジェクト グループベースの ACL により、Cisco IOS ルータの大規模なユーザ アクセス環境でのスタティック ACL の導入が容易になります。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）、ゾーンベース ファイアウォールにはオブジェクト グループによるメリットが得られます。

従来型のアクセス コントロール エントリ（ACE）を設定し、複数の 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、ゾーンベース ポリシー 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、この機能により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。

ゾーンベース ファイアウォールとオブジェクト グループの統合

ゾーンベース ファイアウォールでは特定のトラフィックにポリシーを適用するために、オブジェクト グループ アクセス コントロール リスト（ACL）を使用します。オブジェクト グルー

プ ACL を定義し、その ACL をゾーンベース ファイアウォール ポリシーに関連付けて、ゾーン ペアにポリシーを適用してトラフィックを検査します。

Cisco IOS XE リリース 3.12S の場合、ファイアウォールでサポートされるのは拡張オブジェクト グループ ACL のみです。

ファイアウォールで設定されたオブジェクト グループには、次の機能が有効です。

- スタティックおよびダイナミック ネットワーク アドレス変換（NAT）
- サービス NAT（**ip nat service** コマンドで設定された標準外の FTP ポート番号をサポートする NAT）
- FTP アプリケーション層ゲートウェイ（ALG）
- Session Initiation Protocol（SIP）ALG

クラスマップには、**match access-group** コマンドを使用して最大 64 のマッチングステートメントを設定できます。

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。

- IPv6 アドレス
- ホスト IPv6 アドレス
- 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

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、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。

オブジェクト グループ ACL のガイドライン

- オブジェクト グループには、固有の名前が必要となります。例として、「Engineering」という名前のネットワーク オブジェクト グループと「Engineering」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とします。この場合、少なくとも 1 つのオブジェクト グループ名に識別子（またはタグ）を追加して、その名前を固有のものにする必要があります。たとえば、「Engineering-admins」と「Engineering-hosts」という名前を使用すると、オブジェクト グループの名前を固有のものにして識別しやすくすることができます。
- 既存のオブジェクト グループに、さらにオブジェクトを追加することができます。オブジェクト グループを追加した後、同じグループ名で必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。オブジェクトグループを削除するまで以前の設定がそのまま保持されます。
- さまざまなオブジェクトをグループ化することができます。たとえば、ホスト、プロトコル、サービスなどのオブジェクトがグループ化され、同じグループ名で設定できます。ネットワーク オブジェクトは、ネットワーク オブジェクト グループでのみ定義し、サービス オブジェクトはサービス グループでのみ定義できます。
- **object-group** コマンドでグループを定義した後に任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはそのグループの各項目に適用されます。この機能を使用すると、コンフィギュレーションのサイズを大幅に削減できます。
- ZBF 検査のクラスマップに関連付けられている ACL にオブジェクトグループが含まれている場合、ACL にエントリを追加したり、ACL からエントリを削除したりすると、アクセスリスト コンフィギュレーション プロンプトを終了した後にのみ変更が有効になります。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group network** *object-group-name*
4. **description** *description-text*
5. **host** {*host-address* | *host-name*}
6. *network-address* {*/nn* | *network-mask*}
7. **group-object** *nested-object-group-name*
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。
9. **end**

手順の詳細

	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** *object-group-name* 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。

	コマンドまたはアクション	目的
ステップ 4	**description** *description-text* 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。
ステップ 5	**host** {*host-address* | *host-name*} 例： `Device(config-network-group)# host 209.165.200.237`	（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。 • 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* {*/nn* | *network-mask*} 例： `Device(config-network-group)# 209.165.200.225 255.255.255.224`	（オプション）サブネット オブジェクトを指定します。 • 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** *nested-object-group-name* 例： `Device(config-network-group)# group-object my-nested-object-group`	（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。 • 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）。
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。	—

	コマンドまたはアクション	目的
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。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group service** *object-group-name*
4. **description** *description-text*
5. *protocol*
6. {**tcp** | **udp** | **tcp-udp**} [**source** {{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*}] [{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*]
7. **icmp** *icmp-type*
8. **group-object** *nested-object-group-name*
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。
10. **end**

手順の詳細

	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** *object-group-name* 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。

	コマンドまたはアクション	目的
ステップ 4	**description** *description-text* 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。
ステップ 6	{**tcp** | **udp** | **tcp-udp**} [**source** {{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*}] [{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*] 例： `Device(config-service-group)# tcp-udp range 2000 2005`	（オプション）TCP、UDP、または両方を指定します。
ステップ 7	**icmp** *icmp-type* 例： `Device(config-service-group)# icmp conversion-error`	（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。
ステップ 8	**group-object** *nested-object-group-name* 例： `Device(config-service-group)# group-object my-nested-object-group`	（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。 • 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）。

	コマンドまたはアクション	目的
		• 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）。
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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. **remark** *remark*
5. **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**]
6. **remark** *remark*
7. **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
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。
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• 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** *access-list-name* 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** *remark* 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。 • 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	**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**]
	例：
	`Device(config-ext-nacl)# deny ip 209.165.200.244 255.255.255.224 host 209.165.200.245 log`
	`Example based on object-group:`
	`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`
		（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。
		• 必要に応じて、**object-group** *service-object-group-name* キーワードおよび引数を、*protocol* の代わりに使用します。argument
		• 必要に応じて、**object-group** *source-network-object-group-name* キーワードおよび引数を、*source source-wildcard* 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、*destination destination-wildcard* 引数の代わりに使用します。
		• *source-wildcard* または *destination-wildcard* 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。

	コマンドまたはアクション	目的
		• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* 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 *source* 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先と *destination* 0.0.0.0 の宛先ワイルドカードを示します。 • 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	**remark** *remark* 例： `Device(config-ext-nacl)# remark allow TCP from any source to any destination`	（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。
ステップ 7	**permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any any`	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。 • 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** *service-object-group-name* キーワードおよび引数を、*protocol* 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、*source source-wildcard* の代わりに使用します。

	コマンドまたはアクション	目的
		• 必要に応じて、**object-group** *destination-network-object-group-name* キーワードおよび引数を、*destination destination-wildcard* の代わりに使用します。 • *source-wildcard* または *destination-wildcard* 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、*source source-wildcard* または *destination destination-wildcard* 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： `Device(config-ext-nacl)# end`	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。

オブジェクト グループのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-all** *class-map-name*
4. **match access-group name** *access-list-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **pass**
9. **exit**

10. **class class-default**
11. **drop**
12. **end**

手順の詳細

	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	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ogacl-cmap`	レイヤ 3 およびレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ 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	**match access-group name** *access-list-name* 例： `Device(config-cmap)# match access-group name my-ogacl-policy`	指定された ACL に基づいて、クラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ogacl-pmap`	検査タイプ ポリシーマップを作成して、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ogacl-cmap`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**pass** 例： `Device(config-pmap-c)# pass`	検査なしでパケットをデバイスに送信できるようにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップコンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更するデフォルト クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**drop** 例： `Device(config-pmap-c)# drop`	デバイスに送信されるパケットをドロップします。
ステップ 12	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス 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。

オブジェクト グループのゾーンの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **interface** *type number*
8. **zone-member security** *zone-name*
9. **end**

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security outside`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security inside`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、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 8	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 9	**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、グローバル コンフィギュレーション モードに戻ります。

オブジェクト グループのゾーン ペアへのポリシー マップの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone-pair security** *zone-pair-name* **source** {*zone-name* | **default** | **self**} **destination** {*zone-name* | **default** | **self**}
4. **service-policy type inspect** *policy-map-name*
5. **end**

手順の詳細

	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	**zone-pair security** *zone-pair-name* **source** {*zone-name* | **default** | **self**} **destination** {*zone-name* | **default** | **self**} 例： `Device(config)# zone-pair security out-to-in source outside destination inside`	ゾーン ペアを作成し、セキュリティ ゾーンペア 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	**service-policy type inspect** *policy-map-name* 例： `Device(conf-sec-zone-pair)# service-policy type inspect ogacl-pmap`	ファイアウォール ポリシー マップをセキュリティ ゾーン ペアにアタッチします。
ステップ 5	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ACL のオブジェクト グループの確認

手順の概要

1. **enable**
2. **show object-group** [*object-group-name*]
3. **show ip access-list** [*access-list-name*]

手順の詳細

	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）。

	コマンドまたはアクション	目的
ステップ 2	**show object-group** [*object-group-name*] 例： `Device# show object-group my-object-group`	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** [*access-list-name*] 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：IPv6 ネットワーク オブジェクト グループの作成

次に、v6-network ognet1 という名前の IPv6 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 v6-network ognet1
Device(config-v6-network-group)# 1:1:2::0/32
Device(config-v6-network-group)# host AB:233::23D5
Device(config-v6-network-group)# exit
```

次に、1つのホスト、1つのサブネット、および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、v6-network ognet2 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 v6-network ognet2
Device(config-v6network-group)# 1:2:3::4/36
Device(config-v6network-group)# host AABB::CCDD
Device(config-v6network-group)# group-object ognet1
Device(config-v6network-group)# exit
```

例：IPv6 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 プロトコルをオブジェクトとして含む、v6-service ogserv1 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
Device# configure terminal
```

```
Device(config)# object-group service v6-service ogserv1
Device(config-v6service-group)# icmp unreachable
Device(config-v6service-group)# tcp smtp
Device(config-v6service-group)# tcp telnet
Device(config-v6service-group)# tcp source range 3000 4000 telnet
Device(config-v6service-group)# pcp
Device(config-v6service-group)# udp domain
Device(config-v6service-group)# hph
Device(config-v6service-group)# exit
```

例：IPv6 オブジェクトグループベースの ACL の作成

次に、パケットを許可する IPv6 オブジェクトグループベース ACL を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list ogacl1
Device(config-ipv6-acl)# permit object-group ogserv1 5:6:7::5/56 object-group ognet1
Device(config-ipv6-acl)# deny ip object-group ognet2 object-group ognet3
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
```

例：オブジェクト グループのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-all ogacl-cmap
Device(config-cmap)# match access-group name my-ogacl-policy
Device(config-cmap)# exit
Device(config)# policy-map type inspect ogacl-pmap
Device(config-pmap)# class type inspect ogacl-cmap
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：オブジェクト グループのゾーンの設定

```
Device# configure terminal
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone-pair security out-to-in source outside destination inside
Device(conf-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# zone-member security outside
```

```
Device(config-if)# end
```

例：オブジェクト グループのゾーン ペアへのポリシー マップの適用

```
Device# configure terminal
Device(config)# zone-pair security out-to-in source outside destination inside
Device(config-sec-zone-pair)# service-policy type inspect ogacl-pmap
Device(config-sec-zone-pair)# end
```

例：ACL 用 IPv6 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

V6-Network object group ognet1
1:1:2::/32
host AB:233::23D5
V6-Network object group ognet2
1:2:3::4/36
host AABB::CCDD
group-object ognet1
V6-Network object group ognet3
host 1::1
host 1::2
host 1::3
V6-Service object group ogserv1
icmp unreachable
tcp source range 3000 4000 eq telnet
pcp
hbh
```

次に、IPv6 オブジェクトグループベース ACL に関する情報を表示する例を示します。

```
Device# show ipv6 access-list
IPv6 access list ogacl1
      permit object-group ogserv1 5:6:7::/56 object-group ognet1 sequence 10
      deny ipv6 object-group ognet2 object-group ognet3 sequence 20
      permit ipv6 any any sequence 30
```

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
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 用 IPv6 オブジェクトグループに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : ACL* 用オブジェクト グループに関する機能情報

機能名	リリース	機能情報
ACL の IPv6 オブジェクトグループ	Cisco IOS XE リリース 16.11.1	ACL 用 IPv6 オブジェクトグループ機能を使用すれば、ユーザー、デバイス、またはプロトコルをグループに分類して、それらをアクセス制御リスト（ACL）に適用し、そのグループ用のアクセス制御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、ユーザーのグループ全体に対してサーバー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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。