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、ユーザー、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。

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ー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 （1 ページ）
- ACL のオブジェクト グループに関する情報 （3 ページ）
- ACL のオブジェクト グループの設定方法 （5 ページ）
- ACL 用オブジェクト グループの設定例 （14 ページ）
- ACL 用オブジェクト グループに関する追加情報 （17 ページ）
- ACL のオブジェクトグループの機能履歴 （17 ページ）

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。Cisco Catalyst 9500X シリーズ スイッチCisco Catalyst 9600 シリーズ スーパーバイザ 2 モジュールでは、オブジェクト グループは拡張 ACL でのみサポートされています。Cisco Catalyst 9500X シリーズ スイッチでは、オブジェクトグループは拡張 ACL でのみサポートされています。

- オブジェクトグループベースの ACL は、IPv4 または IPv6 アドレスのみをサポートします。Cisco Catalyst 9500X シリーズ スイッチでは、オブジェクト グループベースの ACL は IPv4 および IPv6 アドレスの両方をサポートしています。
- 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）、ポート チャネル インターフェイス、およびサブインターフェイスのみをサポートします。

  Cisco Catalyst 9500X シリーズ スイッチのレイヤ 2 インターフェイスはサポートされていません。
- 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。これは、Cisco Catalyst 9500X シリーズ スイッチには適用されません。
- 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。
- Cisco Catalyst 9500X シリーズ スイッチでは、オブジェクト グループベースの ACL は入力ポートでのみサポートされています。出力方向ではサポートされていません。
- ログオプション付きの IPv6 オブジェクトグループベースの ACL は、Cisco Catalyst 9500X シリーズ スイッチ ではサポートされていません。ただし、ログオプション付きの IPv4 オブジェクトグループベースの ACL はサポートされています。
- マルチキャストパケット制御用の IPv4 オブジェクトグループベースの ACL は、Cisco Catalyst 9500X シリーズ スイッチではサポートされていません。
- 制御パケット用の IPv6 オブジェクトグループベースの ACL は、Cisco Catalyst 9500X シリーズ スイッチではサポートされていません。
- Cisco Catalyst 9500X シリーズ スイッチでは、同じ ACL 内で従来の ACE とオブジェクトグループを参照する ACE を設定することはできません。
- Cisco Catalyst 9500X シリーズ スイッチでは、255.255.0.0 255.0.0.0 などの連続したアドレスマスク（ワイルドカード）のみがサポートされています。
- Cisco Catalyst 9500X シリーズ スイッチでは、ACE 単位の統計は拒否 ACE でのみサポートされています。ACE 単位の統計は、許可 ACE ではサポートされていません。同じ ACL が複数のポートに適用される場合、拒否カウンタは ACL が接続されているすべてのポートで累積されます。
- 拡張アクセスリスト コンフィギュレーション モードの **log** および **log-input** コマンドの **deny** および **permit** オプションは CLI を介して設定できますが、これらのオプションはサポートされていません。

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、ユーザーのグループが特定のサーバー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、ユーザー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。 プロンプトが表示されたらパスワードを入力します。
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。
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：	（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。

	コマンドまたはアクション	目的
	`Device(config-network-group)# host 209.165.200.237`	• 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）。

	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。 プロンプトが表示されたらパスワードを入力します。
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。
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*]	（オプション）TCP、UDP、または両方を指定します。

	コマンドまたはアクション	目的
	例： `Device(config-service-group)# tcp-udp range 2000 2005`	
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）。 • 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。	—

	コマンドまたはアクション	目的
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。 プロンプトが表示されたらパスワードを入力します。
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。

	コマンドまたはアクション	目的

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* 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、*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。
		• 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

	コマンドまたはアクション	目的
		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。 （注） **log** および **log-input** オプションは CLI を介して設定できますが、これらのオプションはサポートされていません。
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。 • 必要に応じて、**object-group** *destination-network-object-group-name* キーワードおよび引数を、

	コマンドまたはアクション	目的
		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に一致します。 • 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。 （注） **log** および **log-input** オプションは CLI を介して設定できますが、これらのオプションはサポートされていません。
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。

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。 プロンプトが表示されたらパスワードを入力します。
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。 プロンプトが表示されたらパスワードを入力します。
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。

	コマンドまたはアクション	目的
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：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
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 内のユーザー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。 プロンプトが表示されたらパスワードを入力します。
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：	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

	コマンドまたはアクション	目的
	`Device(config-if)# ip access-group my-ogacl-policy in`	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	• 『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 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 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。
Cisco IOS XE Cupertino 17.7.1	ACL のオブジェクト グループ	この機能は、C9500X-28C8D モデルに導入されました。
Cisco IOS XE Dublin 17.10.1b	ACL のオブジェクト グループ	この機能は、C9500X-60L4D モデルに導入されました。

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 にアクセスするには、https://cfnng.cisco.com/ に進みます。

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。