ACL の IPv6 オブジェクトグループ

ACL の IPv6 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）に適用してグループのアクセス 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 IPv6 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）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、VLAN ACL（VACL）やポート ACL（PACL）などのレイヤ 2 機能をサポートしません。
- 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。
- ACL でサポートされるオブジェクトグループベースの ACE の最大数は 2048 です。

- 空のオブジェクトグループは自動的に削除されます。
- オブジェクトグループは、アクセスリストで参照する前に作成する必要があります。オブジェクトグループは、アクセスリストなどの他の機能によって参照されている場合は削除できません。
- パケットフローに対して ACL 照合が実行される場合、ACL エントリを含むオブジェクトグループはスキップされます。

ACL の IPv6 オブジェクトグループに関する情報

従来型のアクセス制御エントリ（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、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。

大規模な設定では、ACE でオブジェクトグループを使用する場合、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。

IPv6 アドレスおよびサービス（プロトコル）はオブジェクトとして扱われ、その後、必要に応じてさまざまなオブジェクトグループにグループ化されます。オブジェクトグループには、v6-network オブジェクトグループ（アドレス用）と v6-service オブジェクトグループ（プロトコル用）の 2 種類があります。必要に応じて、オブジェクトグループをネストできます。

オブジェクトグループは、IPv6 ACE の設定時に、プロトコルや送信元アドレスまたは宛先アドレスの代わりに参照できます。オブジェクトグループを含む ACE は、個別の ACE（各オブジェクトの）に展開され、ハードウェアにプログラムされます。

IPv6 ネットワークおよびサービス オブジェクト グループには、オブジェクトが追加される独自のコンフィギュレーション サブモードがあります。

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。

- 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。

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。

IPv6 オブジェクトグループの設定

オブジェクト グループ

次のオブジェクトグループが追加されています。

```
Device# enable
Device# configure terminal
Device(config)# object-group ?
network     network group
security    security group
service     service group
v6-network  IPv6 network group
v6-service  IPv6 service group
```

IPv6 ACL でのオブジェクトグループの使用

オブジェクトグループは、プロトコル、送信元 IPv6 アドレス、および宛先 IPv6 アドレスの 3 つの位置にあるアクセスリストで使用できます。

次のオブジェクト グループ オプションが既存のプロトコル/アドレスオプションに追加されています。

```
Device(config-v6network-group)#?

Device(config-ipv6-acl)# [no] { permit | deny } [ <protocol options> | object-group
<v6service og name> ] { <source address options> | object-group <v6network OG
name> } { <destination address options> | object-group <v6network OG name> }
```

IPv6 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。

IPv6 ネットワーク オブジェクト グループを作成するには、次の手順を実行します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-network name
Device(config-v6network-group)# [no] { description <desc> | <x.x.x.x::x/prefix_len> |
host <x.x.x.x::x> | group-object <nested OG name> }


Device(config)#object-group v6-net ognet1
Device(config-v6network-group)#?


V6-Network object group configuration commands:
X:X:X:X::X/<0-128>  - IPv6 network address/prefix length
description         - Network object group description
exit                - Exit from object group configuration mode
group-object        - Nested object group
host                - Host address of group member
no                  - Negate or set default values of a command
```

IPv6 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。

IPv6 サービス オブジェクト グループを作成するには、次の手順を実行します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-service <name>
Device(config-v6service-group)# [no] {description <desc> | <0-255> | ahp | esp | hbh
|icmp [<message type>]
| ipv6 | pcp | { <sctp | tcp | udp | tcp-udp> [source <src port options>]}
[<dest port options>] | group-object <nested OG name> }
Device(config-service-group)# end
```

```
Device# (config-v6service-group)#?
IPv6 Service object group configuration commands:
<0-255>         -  An IP protocol number
ahp             - Authentication Header Protocol
description     - Service object group description
esp             - Encapsulation Security Payload
exit            - Exit from object-group configuration mode
group-object    - Nested object group
hbh             - Hop by Hop options header
icmp            - Internet Control Message Protocol
ipv6            - Any Internet Protocol (v6)
no              - Negate or set default values of a command
pcp             - Payload Compression Protocol
sctp            - Streams Control Transmission Protocol
```

```
tcp             - Transmission Control Protocol
tcp-udp         - TCP or UDP protocol
udp             - User Datagram Protocol
```

ACL の IPv6 オブジェクトグループの確認

ACL の IPv6 オブジェクトグループを確認するには、次の手順を実行します。

```
Device# enable
Device# show running int <name>-------to check if ACL is applied on the interface
Device# show object-group object-group-name --------to check if configured object groups
 are referenced
Device# show ipv6 access-list --------to check the configured ACL
```

上記の show コマンドは、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：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』
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。