



## アクセス制御のオブジェクト

オブジェクトとは、コンフィギュレーションで使用するための再利用可能なコンポーネントです。インライン IP アドレス、サービス、名前などの代わりに、Cisco ASA コンフィギュレーションでオブジェクトを定義し、使用できます。オブジェクトを使用すると、コンフィギュレーションのメンテナンスが容易になります。これは、一箇所でオブジェクトを変更し、このオブジェクトを参照している他のすべての場所に反映できるからです。オブジェクトを使用しなければ、1 回だけ変更するのではなく、必要に応じて各機能のパラメータを変更する必要があります。たとえば、ネットワーク オブジェクトによって IP アドレスおよびサブネットマスクが定義されており、このアドレスを変更する場合、この IP アドレスを参照する各機能ではなく、オブジェクト定義でアドレスを変更することだけが必要です。

- [オブジェクトのガイドライン \(1 ページ\)](#)
- [オブジェクトの設定 \(2 ページ\)](#)
- [オブジェクトのモニタリング \(12 ページ\)](#)
- [オブジェクトの履歴 \(13 ページ\)](#)

## オブジェクトのガイドライン

### IPv6 のガイドライン

IPv6 のサポートには次の制約が伴います。

- 1 つのネットワーク オブジェクト グループの中で IPv4 および IPv6 のエントリを混在させることができますが、NAT に対しては、混合オブジェクト グループは使用できません。

### その他のガイドラインと制限事項

- オブジェクトおよびオブジェクト グループは同じネーム スペースを共有するため、オブジェクトの名前は固有のものでなければなりません。「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場合、少なくとも 1 つのオブジェクトグループ名の最後に識別子（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特定可能にすることができます。

- オブジェクト名は、文字、数字、および `!@#%&()-_{}` を含めて、64 文字までに制限されています。オブジェクト名は、大文字と小文字が区別されます。
- 前方参照 (**forward-reference enable** コマンド) をイネーブルにしない限り、コマンドで使用されているオブジェクトを削除したり、空にすることはできません。

## オブジェクトの設定

次の各項では、主にアクセスコントロールで使用されるオブジェクトを設定する方法について説明します。

### ネットワーク オブジェクトとグループの設定

ネットワーク オブジェクトおよびグループは、IP アドレスまたはホスト名を特定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

#### ネットワーク オブジェクトの設定

1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名 (FQDN) を入れることができます。

また、オブジェクトに対して NAT ルールをイネーブルにすることもできます (FQDN オブジェクトを除く)。オブジェクト NAT の設定の詳細については、[Network Address Translation \(NAT\)](#) を参照してください。

#### 手順

**ステップ 1** オブジェクト名を使用して、ネットワーク オブジェクトを作成または編集します: **object network object\_name**

例:

```
hostname(config)# object network email-server
```

**ステップ 2** 次のいずれかのコマンドを使用して、オブジェクトにアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **host {IPv4\_address|IPv6\_address}**: 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet {IPv4\_address IPv4\_mask|IPv6\_address|IPv6\_prefix}**: ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6

の場合、2001:DB8:0:CD30::/60のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

- **range start\_address end\_address** : アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。
- **fqdn [v4|v6]fully\_qualified\_domain\_name** : 完全修飾ドメイン名。つまり、www.example.com のようなホスト名。アドレスを IPv4 に制限するには **v4**、IPv6 に制限するには **v6** を指定します。アドレス タイプを指定しない場合、IPv4 が使用されます。

例 :

```
hostname(config-network-object)# host 10.2.2.2
```

**ステップ 3** (任意) 説明を追加します。 **description string**

## ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループには、インライン ネットワークやホストと同様に複数のネットワーク オブジェクトを含めることができます。ネットワーク オブジェクトグループは、IPv4 と IPv6 の両方のアドレスの混在を含めることができます。

ただし、IPv4 と IPv6 が混在するオブジェクト グループや、FQDN オブジェクトが含まれているオブジェクト グループを、NAT に使用することはできません。

手順

**ステップ 1** オブジェクト名を使用して、ネットワーク オブジェクト グループを作成または編集します。  
**object-group network group\_name**

例 :

```
hostname(config)# object-group network admin
```

**ステップ 2** 次のコマンドの 1 つまたは複数を使用して、ネットワーク オブジェクト グループにオブジェクトとアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **network-object host {IPv4\_address|IPv6\_address}** : 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **network-object {IPv4\_address IPv4\_mask|IPv6\_address/IPv6\_prefix}** : ネットワークまたはホストのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **network-object object object\_name** : 既存のネットワーク オブジェクトの名前。

- **group-object** *object\_group\_name* : 既存のネットワークオブジェクトグループの名前。

例 :

```
hostname (config-network-object-group) # network-object 10.1.1.0 255.255.255.0
hostname (config-network-object-group) # network-object 2001:db8:0:cd30::/60
hostname (config-network-object-group) # network-object host 10.1.1.1
hostname (config-network-object-group) # network-object host 2001:DB8::0DB8:800:200C:417A
hostname (config-network-object-group) # network-object object existing-object-1
hostname (config-network-object-group) # group-object existing-network-object-group
```

### ステップ3 (任意) 説明を追加します。 **description string**

例

3人の管理者のIPアドレスを含むネットワークグループを作成するには、次のコマンドを入力します。

```
hostname (config) # object-group network admins
hostname (config-protocol) # description Administrator Addresses
hostname (config-protocol) # network-object host 10.2.2.4
hostname (config-protocol) # network-object host 10.2.2.78
hostname (config-protocol) # network-object host 10.2.2.34
```

次のコマンドを入力して、さまざまな部門に所属する特権ユーザのネットワークオブジェクトグループを作成します。

```
hostname (config) # object-group network eng
hostname (config-network) # network-object host 10.1.1.5
hostname (config-network) # network-object host 10.1.1.9
hostname (config-network) # network-object host 10.1.1.89

hostname (config) # object-group network hr
hostname (config-network) # network-object host 10.1.2.8
hostname (config-network) # network-object host 10.1.2.12

hostname (config) # object-group network finance
hostname (config-network) # network-object host 10.1.4.89
hostname (config-network) # network-object host 10.1.4.100
```

その後、3つすべてのグループを次のようにネストします。

```
hostname (config) # object-group network admin
hostname (config-network) # group-object eng
hostname (config-network) # group-object hr
hostname (config-network) # group-object finance
```

## サービスオブジェクトとサービスグループの設定

サービスオブジェクトとグループでは、プロトコルおよびポートを指定します。これらのオブジェクトをアクセスコントロールリストで使用して、ルールを簡素化できます。

### サービスオブジェクトの設定

サービスオブジェクトには、単一のプロトコル仕様を含めることができます。

#### 手順

**ステップ 1** オブジェクト名を使用して、サービスオブジェクトを作成または編集します。 **object service** *object\_name*

例：

```
hostname(config)# object service web
```

**ステップ 2** 次のいずれかのコマンドを使用して、オブジェクトにサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service protocol** : IP プロトコルの名前または番号 (0 ~ 255) 。 **ip** を指定すると、すべてのプロトコルに適用されます。
- **service {icmp | icmp6} [icmp-type [icmp\_code]]** : ICMP または ICMP バージョン 6 のメッセージ用。ICMP タイプを名前または番号 (0 ~ 255) で指定することで、オブジェクトをそのメッセージタイプに制限できます (オプション) 。タイプを指定する場合、そのタイプ (1 ~ 255) に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。
- **service {tcp | udp | sctp} [source operator port] [destination operator port]** : TCP、UDP、または Sctp 用。送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは、名前または番号で指定できます。operator には次のいずれかを指定できます。
  - **lt** : 小なり。
  - **gt** : 大なり。
  - **eq** : 等しい。
  - **neq** : 非同値。
  - **range** : 値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します (例 : **range 100 200**) 。

例：

```
hostname(config-service-object)# service tcp destination eq http
```

### ステップ3 (任意) 説明を追加します。 **description string**

## サービスグループの設定

1つのサービスオブジェクトグループには、さまざまなプロトコルが混在しています。必要に応じて、それらを使用するプロトコルの送信元および宛先ポート、およびICMPのタイプおよびコードを入れることができます。

### 始める前に

ここで説明する一般的なサービス オブジェクト グループを使用して、すべてのサービスをモデル化できます。ただし、ASA 8.3(1)よりも前に使用可能であったサービスグループオブジェクトのタイプを設定することもできます。こうした従来のオブジェクトには、TCP/UDP/TCP-UDPポートグループ、プロトコルグループ、およびICMPグループが含まれます。これらのグループのコンテンツは、ICMP6またはICMPコードをサポートしないICMPグループを除く、一般的なサービス オブジェクト グループの関連する設定に相当します。これらの従来のオブジェクトを使用したい場合は、`object-service` コマンドに関する説明を [Cisco.com](http://Cisco.com) のコマンドリファレンスで確認してください。

### 手順

**ステップ1** オブジェクト名を使用して、サービス オブジェクト グループを作成または編集します。  
**object-group service *object\_name***

例：

```
hostname(config)# object-group service general-services
```

**ステップ2** 次のコマンドの1つまたは複数を使用して、サービス オブジェクト グループにオブジェクトとサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service-object *protocol*** : IPプロトコルの名前または番号 (0～255)。**ip** を指定すると、すべてのプロトコルに適用されます。
- **service-object {*icmp* | *icmp6*} [*icmp-type* [*icmp\_code*]]** : ICMP または ICMP バージョン 6 のメッセージ用。ICMPタイプを名前または番号 (0～255) で指定することで、オブジェクトをそのメッセージタイプに制限できます (オプション)。タイプを指定する場合、そのタイプ (1～255) に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。
- **service-object {*tcp* | *udp* | *tcp-udp* | *sctp*} [*source operator port*] [*destination operator port*]** : TCP、UDP、その両方、または SCTP 用。送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは、名前または番号で指定できます。**operator** には次のいずれかを指定できます。
  - **lt** : 小なり。

- **gt** : 大なり。
  - **eq** : 等しい。
  - **neq** : 非同値。
  - **range** : 値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します (例 : **range 100 200**) 。
- 
- **service-object object *object\_name*** : 既存のサービス オブジェクトの名前。
  - **group-object object *group\_name*** : 既存のサービス オブジェクト グループの名前。

例 :

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

### ステップ3 (任意) 説明を追加します。 **description string**

例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

## ローカル ユーザ グループの設定

作成したローカル ユーザ グループは、アイデンティティ ファイアウォールをサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールでも使用できるようになります。

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリを送信します。ASA は、そのグループをアイデンティティ ベースのルール用にインポートします。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。

ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ACL でユーザ名とユーザ グループ名を直接使用できるため、次の場合にだけローカル ユーザ グループを設定する必要があります。

- ローカル データベースで定義されているユーザのグループを作成する。
- AD サーバで定義されている単一のユーザ グループでキャプチャされなかったユーザまたはユーザ グループのグループを作成する。

### 手順

**ステップ 1** オブジェクト名を使用して、ユーザ オブジェクト グループを作成または編集します。

**object-group user group\_name**

例 :

```
hostname (config)# object-group user admins
```

**ステップ 2** 次のコマンドの 1 つまたは複数を使用して、ユーザ オブジェクト グループにユーザとグループを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **user [domain\_NETBIOS\_name]username** : ユーザ名。ドメイン名またはユーザ名にスペースが含まれている場合は、ドメイン名とユーザ名を引用符で囲む必要があります。ドメイン名には、LOCAL (ローカル データベースで定義されているユーザ向け)、または **user-identity domain domain\_NetBIOS\_name aaa-server aaa\_server\_group\_tag** コマンドで指定されている Active Directory (AD) のドメイン名を指定できます。AD ドメインに定義されているユーザを追加する場合、**user\_name** には、一意ではない可能性がある Common Name (CN) ではなく、一意の Active Directory sAMAccountName を指定する必要があります。ドメイン名を指定しない場合、デフォルト値が使用されます。デフォルト値は、LOCAL または **user-identity default-domain** コマンドで定義されている値のいずれかです。



- **user-group** `[domain_NETBIOS_name\\]username` : ユーザグループ。ドメイン名またはグループ名にスペースが含まれている場合は、ドメイン名とグループ名を引用符で囲む必要があります。ドメイン名とグループ名を区切る二重の \\ に注意してください。
- **group-object** `object_group_name` : 既存のユーザ オブジェクト グループの名前。

例 :

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\managers
hostname(config-user-object-group)# group-object local-admins
```

ステップ3 (任意) 説明を追加します。 **description string**

## セキュリティ グループオブジェクト グループの設定

作成したセキュリティ グループオブジェクトグループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセスルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバリソースへのマッピングを行います。セキュリティ グループ ACL のプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ローカライズされたセキュリティ ポリシーを持つローカルセキュリティ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカルセキュリティグループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカルセキュリティグループを作成するには、ローカルセキュリティオブジェクトグループを作成します。1つのローカルセキュリティオブジェクトグループに、1つ以上のネストされたセキュリティオブジェクトグループまたはセキュリティ ID またはセキュリティグループ名を入れることができます。ユーザは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティグループ名を作成することもできます。

ASA 上で作成したセキュリティオブジェクトグループは、ネットワークリソースへのアクセスの制御に使用できます。セキュリティオブジェクトグループを、アクセスグループやサービスポリシーの一部として使用できます。



**ヒント** ASAにとって不明なタグや名前を使用してグループを作成する場合、そのタグや名前が ISEで解決されるまで、そのグループを使用するすべてのルールが非アクティブになります。

## 手順

**ステップ 1** オブジェクト名を使用して、セキュリティ グループ オブジェクト グループを作成または編集します。 **object-group security group\_name**

例：

```
hostname(config)# object-group security mktg-sg
```

**ステップ 2** 次のコマンドの 1 つまたは複数を使用して、サービス グループ オブジェクト グループにオブジェクトを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **security-group {tag sgt\_number | name sg\_name}** : セキュリティ グループ タグ (SGT) または名前。タグは、1 から 65533 までの数字であり、IEEE 802.1X 認証、Web 認証、または ISE による MAC 認証バイパス (MAB) を通じてデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。有効なタグと名前については、ISE の設定を参照してください。
- **group-object object\_group\_name** : 既存のセキュリティ グループ オブジェクト グループの名前。

例：

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

**ステップ 3** (任意) 説明を追加します。 **description string**

## 時間範囲の設定

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能または資産に時間ベースでアクセスするために ACL ルールで使用されます。たとえば、勤務時間中のみ特定のサーバへのアクセスを許可するアクセスルールを作成できます。



(注) 時間範囲オブジェクトには複数の定期的エントリを含めることができます。1 つの時間範囲に **absolute** 値と **periodic** 値の両方が指定されている場合は、**periodic** 値は **absolute** の開始時刻に到達した後にのみ評価され、**absolute** の終了時刻に到達した後は評価されません。

時間範囲を作成してもデバイスへのアクセスは制限されません。この手順では、時間範囲だけを定義します。その後、アクセスコントロールルールでオブジェクトを使用する必要があります。

## 手順

**ステップ 1** 時間範囲を作成します。 **time-range name**

**ステップ 2** (任意) 時間範囲に開始時刻または終了時刻 (または両方) を追加します。

**absolute** [*start time date*] [*end time date*]

開始時刻を指定しない場合、現在の時刻がデフォルトの開始時刻になります。

*time* は 24 時間形式 (*hh:mm*) で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

*date* は *day month year* の形式で指定します (たとえば、**1 January 2014**) 。

**ステップ 3** (任意) 繰り返しの期間を追加します。

**periodic** *days-of-the-week time to* [*days-of-the-week*] *time*

*days-of-the-week* には次の値を指定できます。最初の引数に曜日を 1 つ指定した場合にのみ、2 番目の曜日を指定できることに注意してください。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、または **Sunday**。最初の *days-of-the-week* 引数には、複数の曜日をスペースで区切って指定できます。
- **daily**
- **weekdays**
- **weekend**

*time* は 24 時間形式 (*hh:mm*) で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

このコマンドを繰り返して、複数の繰り返し期間を設定できます。

## 例

次に、2006 年 1 月 1 日の午前 8 時に始まる絶対的な時間範囲の例を示します。終了時刻も終了日も指定されていないため、時間範囲は事実上無期限になります。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の午前 8 時～午後 6 時に毎週繰り返される定期的な時間範囲の例を示します。

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

次の例では、時間範囲の終了日を設定し、平日の期間を午前8時～午後5時に設定し、火曜日、木曜日と比較して月曜日、水曜日、金曜日に対して午後5時の後に異なる時間数を加算します。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

## オブジェクトのモニタリング

オブジェクトおよびグループをモニタするには、次のコマンドを入力します。

- **show access-list**

アクセスリストのエントリを表示します。オブジェクトを含むエントリは、オブジェクトのコンテンツに基づいて個々のエントリへも拡大しています。

- **show running-config object [id object\_id]**

現在のすべてのオブジェクトを表示します。**id** キーワードを使用すると、単一のオブジェクトを名前別に表示できます。

- **show running-config object object\_type**

現在のオブジェクトをタイプ、ネットワーク、またはサービス別に表示します。

- **show running-config object-group [id group\_id]**

現在のすべてのオブジェクトグループを表示します。**id** キーワードを使用すると、単一のオブジェクトグループを名前別に表示できます。

- **show running-config object-group grp\_type**

現在のオブジェクトグループをグループタイプごとに表示します。

## オブジェクトの履歴

機能名	プラットフォーム リリース	説明
オブジェクト グループ	7.0(1)	オブジェクト グループによって、ACL の作成とメンテナンスが簡素化されます。  <b>object-group protocol</b> 、 <b>object-group network</b> 、 <b>object-group service</b> 、 <b>object-group icmp_type</b> の各コマンドが導入または変更されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。 <b>class-map type regex</b> コマンド、 <b>regex</b> コマンド、および <b>match regex</b> コマンドが導入されました。
オブジェクト	8.3(1)	オブジェクトのサポートが導入されました。  次のコマンドが導入または変更されました。 <b>object-network</b> 、 <b>object-service</b> 、 <b>object-group</b> ネットワーク、 <b>object-group</b> サービス、 <b>network object</b> 、 <b>access-list extended</b> 、 <b>access-list webtype</b> 、 <b>access-list remark</b> 。
アイデンティティ ファイアウォールでのユーザ オブジェクト グループの使用	8.4(2)	アイデンティティ ファイアウォールのためのユーザ オブジェクト グループが導入されました。  <b>object-network user</b> 、 <b>user</b> のコマンドが導入されました。
Cisco TrustSec のためのセキュリティ グループ オブジェクト グループ	8.4(2)	Cisco TrustSec のためのセキュリティ グループ オブジェクト グループが導入されました。  <b>object-network security</b> および <b>security</b> コマンドが導入されました。
IPv4 および IPv6 の混合ネットワーク オブジェクト グループ	9.0(1)	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在では、ネットワーク オブジェクト グループが、IPv4 と IPv6 の両方のアドレスの混合をサポートするようになりました。  (注) 混合オブジェクト グループを NAT に使用することはできません。  <b>object-group network</b> コマンドが変更されました。

機能名	プラットフォーム リリース	説明
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 <b>access-list extended</b> 、 <b>service-object</b> 、 <b>service</b> の各コマンドが導入または変更されました。
Stream Control Transmission Protocol (SCTP) のサービスオブジェクトのサポート	9.5(2)	特定の SCTP ポートに対するサービス オブジェクトおよびグループを作成できるようになりました。 次のコマンドが変更されました。 <b>service-object</b> 、 <b>service</b>