CHAPTER 11

MAC ACL の設定

この章では、Media Access ControlMAC; メディア アクセス制御）アクセス リスト（ACL）の設定方法について説明します。

この章の内容は次のとおりです。

MAC ACL の概要

MAC ACL は、各パケットのレイヤ 2 ヘッダー内の情報を使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。これらの共通機能については、「ACL の概要」（p.10-2）を参照してください。

MAC ACL のライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
NX-OS	MAC ACL にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は、Cisco NX-OS システム イメージにバンドルされており、追加料金なしで利用できます。NX-OS のライセンス スキームに関する詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

MAC ACL の前提条件

MAC ACL の前提条件は次のとおりです。

- MAC ACL を設定するためには、MAC アドレッシングおよびプロトコルに関する知識が必要です。
- 「ACL の概要」（p.10-2）に記載されている内容を理解している必要があります。

注意事項および制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- MAC ACL は入力トラフィックのみに適用されます。

MAC ACL の設定

ここでは、次の内容について説明します。

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **mac access-list** *name*
3. {**permit** | **deny**} *source destination protocol*
4. **statistics**
5. **show mac access-lists** *name*
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 2	**mac access-list** *name*
	
	例：
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		MAC ACL を作成し、ACL 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	{**permit** | **deny**} *source destination protocol* **例：** `switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	MAC ACL のルールを作成します。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco NX-OS Security Command Reference*』を参照してください。
ステップ 4	**statistics** **例：** `switch(config-mac-acl)# statistics`	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。

	コマンド	目的
ステップ 5	**show mac access-lists** *name* **例：** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意）MAC ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config-mac-acl)# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の変更

既存の MAC ACL に対して、ルールの追加と削除を行うことができます。既存のルールを変更することはできません。ルールを変更したい場合は、そのルールを削除し、目的の変更を加えたルールを再作成します。

既存のルールの間に、現在のシーケンス番号では許容できない数のルールを追加する必要がある場合は、**resequence** コマンドを使用することにより、シーケンス番号を再割り当てできます。詳細については、「MAC ACL のシーケンス番号の変更」（p.11-6）を参照してください。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **mac access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} *source destination protocol*
4. **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}
5. [**no**] **statistics**
6. **show mac access-lists** *name*
7. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 2	**mac access-list** *name*
	
	例：
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		名前を指定する ACL の ACL コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	[*sequence-number*] {**permit** | **deny**} *source destination protocol* **例**： `switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	（任意）MAC ACL のルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、最後のルールの後ろに追加されます。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco NX-OS Security Command Reference*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} **例**： `switch(config-mac-acl)# no 80`	（任意）指定したルールを MAC ACL から削除します。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics** **例**： `switch(config-mac-acl)# statistics`	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	**show mac access-lists** *name* **例**： `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意）MAC ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** **例**： `switch(config-mac-acl)# copy running-config startup-config`	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の削除

MAC ACL をデバイスから削除できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

その ACL がインターフェイスに適用されているかどうかを確認します。削除できるのは、現在 適用されている ACL です。ACL を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。デバイスは削除された ACL を空であるとみなします。

手順の概要

1. **config t**
2. **no mac access-list** *name*
3. **show mac access-lists**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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 2	**no mac access-list** *name* **例：** switch(config)# no mac access-list acl-mac-01 switch(config)#	名前を指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	**show mac access-lists** **例：** switch(config)# show mac access-lists	（任意）MAC ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL のシーケンス番号の変更

MAC ACL のルールに割り当てられているすべてのシーケンス番号を変更できます。シーケンス番号の変更は、ACL にルールを挿入する必要があり、使用できるシーケンス番号が十分にない場合に役立ちます。詳細については、「ルールについて」（p.10-5）を参照してください。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. **show mac access-lists** *name*
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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 2	**resequence mac access-list** *name starting-sequence-number increment* **例：** switch(config)# resequence mac access-list acl-mac-01 100 10	ACL 内のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。その後ろの各ルールには、前のルールよりも 一定数だけ大きい番号が割り当てられます。番号の差異は、指定した増分によって決まります。
ステップ 3	**show mac access-lists** *name* **例：** switch(config)# show mac access-lists acl-mac-01	（任意）MAC ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として次のインターフェイス タイプに適用できます。

- レイヤ 2 インターフェイス
- レイヤ 3 インターフェイス
- ポートチャネル インターフェイス

作業を開始する前に

適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。MAC ACL の設定については、「MAC ACL の設定」（p.11-3）を参照してください。

手順の概要

1. **config t**
2. **interface *ethernet*** *slot/port*

   interface *port-channel* *channel-number*
3. **mac port access-group** *access-list*
4. **show running-config aclmgr**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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 2	**interface *ethernet*** *slot/port* **例：** switch(config)# interface ethernet 2/1 switch(config-if)#	レイヤ 2 またはレイヤ 3 のインターフェイス コンフィギュレーション モードを開始します。
	interface *port-channel* *channel-number* **例：** switch(config)# interface port-channel 5 switch(config-if)#	ポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mac port access-group** *access-list* **例：** switch(config-if)# mac port access-group acl-01	MAC ACL をインターフェイスに適用します。
ステップ 4	**show running-config aclmgr** **例：** switch(config-if)# show running-config aclmgr	（任意）ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** switch(config-if)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL としての MAC ACL の適用

MAC ACL は VACL として適用できます。MAC ACL を使用した VACL の作成方法については、「VACL の作成または変更」（p.12-5）を参照してください。

MAC ACL の設定の確認

MAC ACL の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr	MAC ACL およびこの ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show running-config interface	ACL を適用したインターフェイスの設定を表示します。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

MAC ACL の統計情報の表示とクリア

各ルールと一致したパケット数を含めて、MAC ACL についての統計情報を表示するには、**show ip access-lists** コマンドを使用します。

MAC ACL の統計情報の表示またはクリアを行うには、次のいずれかの作業を行います。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に **statistics** コマンドが含まれている場合は、**show mac access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear mac access-list counters	すべての MAC ACL または特定の MAC ACL の統計情報をクリアします。

これらのコマンドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

MAC ACL の設定例

acl-mac-01 という名前の MAC ACL を作成し、これをイーサネット インターフェイス 2/1 レイヤ 2 インターフェイス）に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac access-group acl-mac-01
```

デフォルト設定

表 11-1 に MAC ACL パラメータのデフォルトの設定値を示します。

表 11-1　MAC ACL パラメータのデフォルト値

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙ルールが適用されます（「暗黙ルール」[p.10-6] を参照）。

その他の参考資料

MAC ACL の実装に関する詳細情報については、次を参照してください。

- 関連資料（p.11-10）
- 規格（p.11-10）

関連資料

関連事項	タイトル
ACL の概念	ACL の概要（p.10-2）
MAC ACL コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』

規格

規格	タイトル
この機能のサポート対象の規格には、新規規格も変更された規格もありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—