CHAPTER 13

ポート セキュリティの設定

この章では、ポート セキュリティ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。

ポート セキュリティの概要

ポート セキュリティを使用すると、限定された MAC アドレス セットからのインバウンド トラフィックだけを許可するようなレイヤ 2 インターフェイスを設定できます。この限定セットの MAC アドレスをセキュア MAC アドレスといいます。さらに、デバイスは、同じ VLAN 内の別のインターフェイスでは、これらの MAC アドレスからのトラフィックを許可しません。セキュア MAC アドレスの数は、インターフェイス単位で設定します。

ここでは、次の内容について説明します。

セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。学習できるアドレスの数には制限があります（「セキュア MAC アドレスの最大数」[p.13-3] を参照）。デバイスは、ポート セキュリティがイネーブルに設定されたインターフェイスごとに、スタティック、ダイナミック、またはスティッキの方式でアドレスを学習します。

スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイス設定にセキュア MAC アドレスを追加したり、設定から削除したりできます。

スタティック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザが明示的に設定からアドレスを削除します。詳細については、「インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除」（p.13-13）を参照してください。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定します。詳細については、「ポート タイプの変更」（p.13-5）を参照してください。

スタティック方式では、ダイナミック方式またはスティッキ方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

ダイナミック方式

デフォルトでは、インターフェイスのポート セキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、そのインターフェイスを通じた入力トラフィックパスとして MAC アドレスをセキュア アドレスにします。このようなアドレスがまだセキュア アドレスではなく、デバイスのアドレス数が適用可能な最大数に達していなければ、デバイスはそのアドレスをセキュア アドレスにして、トラフィックを許可します。

デバイスは、ダイナミック アドレスのエージングを行い、エージングの制限時間に達すると、そのアドレスをドロップします（「ダイナミック アドレスのエージング」[p.13-3] を参照）。

ダイナミック アドレスは、デバイスやインターフェイスの再起動後は維持されません。

ダイナミック方式で学習された特定のアドレス、または特定のインターフェイスでダイナミックに学習されたすべてのアドレスを削除する場合は、「ダイナミック セキュア MAC アドレスの削除」（p.13-14）を参照してください。

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミック アドレス学習と同じ方法で MAC アドレスをセキュア アドレスにしますが、この方法で学習されたアドレスは NVRAM に保存されます。そのため、スティッキ方式で学習されたアドレスは、デバイスの再起動後も維持されます。スティッキ セキュア MAC アドレスは、インターフェイスの実行コンフィギュレーション内にはありません。

ダイナミックとスタティックのアドレス学習を両方同時にイネーブルにすることはできません。あるインターフェイスのスタティック学習をイネーブルにした場合、デバイスはダイナミック学習を停止して、代わりにスタティック学習を実行します。スタティック学習をディセーブルにすると、デバイスはダイナミック学習を再開します。

デバイスは、スティッキ セキュア MAC アドレスのエージングは行いません。

スティッキ方式で学習された特定のアドレスを削除する場合は、「インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除」（p.13-13）を参照してください。

ダイナミック アドレスのエージング

デバイスは、ダイナミック方式で学習された MAC アドレスのエージングを行い、エージングの期限に達すると、アドレスをドロップします。エージングの期限は、インターフェイスごとに設定できます。設定できる範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

MAC アドレスのエージングを判断するためにデバイスが使用する方法も設定できます。アドレス エージングの判断には、次に示す 2 つの方法が使用されます。

- 非アクティブ — 適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間
- 絶対時間 — デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。

セキュア MAC アドレスの最大数

デフォルトでは、各インターフェイスのセキュア MAC アドレスは 1 つだけです。各インターフェイス、またはインターフェイス上の各 VLAN に許容可能な最大 MAC アドレス数を設定できます。最大数は、ダイナミック、スティッキ、スタティックのいずれの方式で学習された MAC アドレスにも適用されます。

ヒント　アドレスの最大数を 1 に設定し、接続された装置の MAC アドレスを設定すると、その装置にはポートの全帯域幅が保証されます。

各インターフェイスに許容されるセキュア MAC アドレスの数は、次の 3 つの制限によって決定されます。

- デバイスの最大数 — デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。
- インターフェイスの最大数 — ポート セキュリティで保護されるインターフェイスごとに、セキュア MAC アドレスの最大数を設定できます。デフォルトでは、インターフェイスの最大数は 1 です。インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。
- VLAN の最大数 — ポート セキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。VLAN の最大数を、インターフェイスの最大数より大きくすることはできません。VLAN 最大数の設定が適しているのは、トランク ポートの場合だけです。VLAN の最大数には、デフォルト値はありません。

  VLAN とインターフェイスの最大値の関係については、「セキュリティ違反と処理」（p.13-4）に例が示されています。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュア アドレス数より少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。ダイナミックに学習されたアドレスの削除方法については、「ダイナミック セキュア MAC アドレスの削除」（p.13-14）を参照してください。スティッキまたはスタティック方式で学習されたアドレスの削除方法については、「インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除」（p.13-13）を参照してください。

セキュリティ違反と処理

次の 2 つのイベントのいずれかが発生すると、ポート セキュリティ機能によってセキュリティ違反がトリガーされます。

- セキュア MAC アドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超えてしまう場合

  VLAN とインターフェイスの両方の最大数が設定されていて、どちらかの最大数を超える場合。たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

  - VLAN 1 の最大アドレス数は 5 です。
  - このインターフェイスの最大アドレス数は 10 です。

  デバイスは、次のいずれかが発生すると違反を検出します。

  - VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合
  - このインターフェイス上のアドレスをすでに 10 個学習していて、11 番めのアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合
- あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

（注）　あるセキュア　ポートでセキュア　MAC　アドレスが設定または学習されたあと、同じ VLAN 内の別のポート上でこのセキュア MAC アドレスが検出された場合に発生する一連のイベントを、MAC の移行違反と呼びます。

セキュリティ違反が発生すると、デバイスは、該当するインターフェイスのポート セキュリティ設定に指定されている処理を実行します。デバイスが実行できる処理は次のとおりです。

- シャットダウン — 違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。このインターフェイスはエラー ディセーブル状態になります。これがデフォルトの処理です。インターフェイスの再起動後も、セキュア MAC アドレスを含めて、ポート セキュリティの設定は維持されます。

  シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再起動することもできます。
- 制限 — セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。デバイスは、ドロップされたパケット数のカウントを維持します。
- 保護 — 違反の発生を防止します。インターフェイスの最大 MAC アドレス数に到達するまでアドレス学習を継続し、到達後はそのインターフェイスでの学習をディセーブルにして、セキュア MAC アドレスイが以外のアドレスからの入力トラフィックをすべてドロップします。

セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合、デバイスはトラフィックを受信したインターフェイスに対して処理を実行します。

ポート セキュリティとポート タイプ

ポート セキュリティを設定できるのは、レイヤ 2 インターフェイスだけです。各種のインターフェイスまたはポートとポート セキュリティについて以下に詳しく説明します。

- アクセス ポート — レイヤ 2 アクセス ポートとして設定したインターフェイスにポート セキュリティを設定できます。アクセス ポートでポート セキュリティが適用されるのは、アクセス VLAN だけです。
- トランク ポート — レイヤ 2 トランク ポートとして設定したインターフェイスにポート セキュリティを設定できます。アクセス ポートには、VLAN 最大数を設定しても効果はありません。デバイスが VLAN 最大数を適用するのは、トランク ポートに関連付けられた VLAN だけです。
- SPAN ポート — SPAN 送信元ポートにはポート セキュリティを設定できますが、SPAN 宛先ポートには設定できません。
- イーサネット ポート チャネル — イーサネット ポート チャネルでは、ポート セキュリティはサポートされていません。

ポート タイプの変更

レイヤ 2 インターフェイスにポート セキュリティを設定し、そのインターフェイスのポート タイプを変更した場合、デバイスは次のように動作します。

- アクセス ポートからトランク ポートへ — レイヤ 2 インターフェイスをアクセス ポートからトランク ポートに変更すると、デバイスはダイナミック方式で学習したすべてのセキュア アドレスをドロップします。ネイティブ トランク VLAN に接続されているデバイスは、スタティック方式またはスティッキ方式で学習したアドレスを移行します。
- トランク ポートからアクセス ポートへ — レイヤ 2 インターフェイスをアクセス ポートからトランク ポートに変更すると、デバイスはダイナミック方式で学習したすべてのセキュア アドレスをドロップします。ネイティブ トランク VLAN でスティッキ方式で学習されたアドレスはすべて、アクセス VLAN に移行されます。ネイティブ トランク VLAN でない場合、スティッキ方式で学習されたセキュア アドレスはドロップされます。
- スイッチド ポートからルーテッド ポートへ — インターフェイスをレイヤ 2 インターフェイスからレイヤ 3 インターフェイスに変更すると、デバイスはそのインターフェイスのポート セキュリティをディセーブルにし、そのインターフェイスのすべてのポート セキュリティ設定を廃棄します。デバイスは、学習方式に関係なく、そのインターフェイスのセキュア MAC アドレスもすべて廃棄します。

- ルーテッド ポートからスイッチド ポートへ — インターフェイスをレイヤ 3 インターフェイスからレイヤ 2 インターフェイスに変更すると、デバイス上のそのインターフェイスのポート セキュリティ設定はなくなります。

802.1X とポート セキュリティ

ポート セキュリティと 802.1X は同じインターフェイス上に設定できます。ポート セキュリティによって、802.1X 認証の MAC アドレスを保護できます。802.1X はポート セキュリティよりも前にパケットを処理するので、1 つのインターフェイスで両方をイネーブルにすると、802.1X が、そのインターフェイスで、未知の MAC アドレスからのインバウンド トラフィックを妨げます。

同じインターフェイス上で 802.1X とポート セキュリティをイネーブルにしても、ポート セキュリティは設定どおりにスティッキ方式またはダイナミック方式で MAC アドレスの学習を続行します。また、単一ホスト モードと複数ホスト モードのどちらで 802.1X をイネーブルにするかによって、次のいずれかが発生します。

- 単一ホスト モード — ポート セキュリティは認証済みのホストの MAC アドレスを学習します。
- 複数ホスト モード — ポート セキュリティは、このインターフェイスでダイナミックに学習された MAC アドレスをドロップし、802.1X で認証された最初のホストの MAC アドレスを学習します。

802.1X がポート セキュリティに渡した MAC アドレスによってセキュア MAC アドレスの適用可能な最大数を違反することになる場合、デバイスはホストに認証エラー メッセージを送信します。

802.1X によって認証された MAC アドレスは、たとえそのアドレスがポート セキュリティによってスティッキ方式またはスタティック方式で学習されていたとしても、ダイナミック方式で学習されたアドレスと同様に扱われます。802.1X で認証されたセキュア MAC アドレスを削除しようとしても、そのアドレスはセキュア アドレスのまま保持されます。

認証済みのホストの MAC アドレスがスティッキ方式またはスタティック方式でセキュア アドレスになった場合、デバイスはそのアドレスをダイナミック方式で学習されたものとして扱うので、その MAC アドレスを手動で削除することはできません。

認証済みのホストのセキュア MAC アドレスがポート セキュリティのエージング期限に達すると、ポート セキュリティは 802.1X と連動して、そのホストを再認証します。デバイスは、エージングのタイプに応じて、次のように異なる動作をします。

- 絶対 — ポート セキュリティは 802.1X に通知し、デバイスはホストの再認証を試行します。そのアドレスが引き続きセキュア アドレスになるかどうかは、再認証の結果によって決まります。最認証が成功すれば、デバイスはそのセキュア アドレスのエージング タイマーを再起動します。最認証に失敗した場合、デバイスはそのインターフェイスのセキュア アドレス リストからそのアドレスをドロップします。
- 非アクティブ — ポート セキュリティは、そのインターフェイスのセキュア アドレス リストからそのセキュア アドレスをドロップし、802.1X に通知します。デバイスはホストの再認証を試行します。最認証が成功すれば、ポート セキュリティは再度そのアドレスをセキュア アドレスにします。

バーチャライゼーション サポート

ポート セキュリティは次のように VDC をサポートします。

- ポート セキュリティは各 VDC に設定されます。ポート セキュリティは VDC 単位でイネーブルにし設定できます。
- セキュア MAC アドレスは VDC ごとに個別に維持されます。
- ある VDC のセキュア MAC アドレスが別の VDC の保護インターフェイス上にあっても、セキュリティ違反にはなりません。

ポート セキュリティのライセンス要件

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	ポート セキュリティ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 デバイス 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。

ポート セキュリティの前提条件

ポート セキュリティの前提条件は次のとおりです。

- ポート セキュリティで保護するデバイスのポート セキュリティをグローバルにイネーブル化する必要があります。

注意事項および制約事項

ポート セキュリティを設定する場合は、次の注意事項に従ってください。

- ポート セキュリティは、イーサネット ポート チャネル インターフェイスや、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートをサポートしていません。
- ポート セキュリティは他の機能に依存していません。
- ポート セキュリティは 802.1X との連動が可能です（「802.1X とポート セキュリティ」[p.13-6] を参照）。

ポート セキュリティの設定

ここでは、次の内容について説明します。

ポート セキュリティのグローバルなイネーブル化またはディセーブル化

デバイスに対してポート セキュリティ機能のグローバルなイネーブル化またはディセーブル化が可能です。

ポート セキュリティをグローバルにディセーブルにすると、スタティック方式で設定されたセキュア MAC アドレス、ダイナミックまたはスティッキ方式のセキュア MAC アドレスを含めて、すべてのポート セキュリティ設定が削除されます。

作業を開始する前に

デフォルトでは、ポート セキュリティはディセーブルです。

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）。

手順の概要

1. **config t**
2. **[no] feature port-security**
3. **show port-security**
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] feature port-security`
	
	例：
	`switch(config)# feature port-security`
		ポート セキュリティをグローバルにイネーブル化します。**no** オプションを使用すると ポート セキュリティはグローバルにディセーブル化されます。

	コマンド	目的
ステップ 3	**show port-security** **例：** switch(config)# show port-security	ポート セキュリティのステータスを表示します。
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。

レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対してポート セキュリティ機能のイネーブル化またはディセーブル化が可能です。MAC アドレスのダイナミック学習についての詳細は、「セキュア MAC アドレスの学習」（p.13-2）を参照してください。

（注）　ルーテッド インターフェイスでは、ポート セキュリティをイネーブルにできません。

作業を開始する前に

デフォルトでは、ポート セキュリティはすべてのインターフェイスでディセーブルです。

インターフェイスのポート セキュリティをイネーブルにすると、MAC アドレスのダイナミック学習もイネーブルになります。スティッキ方式の MAC アドレス学習をイネーブルにするには、「スティッキ MAC アドレス学習のイネーブル化またはディセーブル化」（p.13-10）の手順も完了する必要があります。

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）。

ポート セキュリティがイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをイネーブルにする手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **switchport**
4. **[no] switchport port-security**
5. **show running-config port-security**
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	**interface** *type slot/port* **例：** switch(config)# interface ethernet 2/1 switch(config-if)#	ポート セキュリティを設定する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	**switchport** **例：** switch(config-if)# switchport	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	[**no**] **switchport port-security** **例：** switch(config-if)# switchport port-security	そのインターフェイスのポート セキュリティをイネーブルにします。**no** オプションを使用すると、そのインターフェイスのポート セキュリティがディセーブルになります。
ステップ 5	**show running-config port-security** **例：** switch(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 6	**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。

スティッキ MAC アドレス学習のイネーブル化またはディセーブル化

インターフェイスのスティッキ MAC アドレス学習をディセーブルまたはイネーブルに設定できます。スティッキ学習をディセーブルにすると、そのインターフェイスはダイナミック MAC アドレス学習（デフォルトの学習方式）に戻ります。

作業を開始する前に

デフォルトでは、スティッキ MAC アドレス学習はディセーブルです。

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）。

ポート セキュリティが、グローバルにイネーブル化され、さらに目的のインターフェイスでもイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをグローバルにイネーブルにする手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（p.13-9）を参照してください。

手順の概要

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

3. **switchport**
4. **[no] switchport port-security mac-address sticky**
5. **show running-config port-security**
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	**interface** *type slot/port* **例：** switch(config)# interface ethernet 2/1 switch(config-if)#	スティッキ MAC アドレス学習を設定する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	**switchport** **例：** switch(config-if)# switchport	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	**[no] switchport port-security mac-address sticky** **例：** switch(config-if)# switchport port-security mac-address sticky	そのインターフェイスのスティッキ MAC アドレス学習をイネーブルにします。**no** オプションを使用すると スティッキ MAC アドレス学習がディセーブルになります。
ステップ 5	**show running-config port-security** **例：** switch(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 6	**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。

インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加できます。

作業を開始する前に

デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。

インターフェイスのセキュア MAC アドレス最大数に達しているかどうかを判断します（**show port-security** コマンドを使用）。必要な場合は、セキュア MAC アドレスを削除できます（「インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除」[p.13-13] または 「ダイナミック セキュア MAC アドレスの削除」[p.13-14] を参照）。あるいは、インターフェイスのセキュア アドレスの最大数を変更することもできます（「MAC アドレスの最大数の設定」[p.13-14] を参照）。

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）。

ポート セキュリティが、グローバルにイネーブル化され、さらに、そのインターフェイスでもイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをグローバルにイネーブル化する手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（p.13-9）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. [**no**] **switchport port-security mac-address** *address* [***vlan*** *vlan-ID*]
4. **show running-config port-security**
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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		指定した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	[**no**] **switchport port-security mac-address** *address* [***vlan*** *vlan-ID*] **例：** `switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、***vlan*** キーワードを使用します。
ステップ 4	**show running-config port-security** **例：** `switch(config-if)# show running-config port-security`	ポート セキュリティ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。

インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除

レイヤ 2 インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスを削除できます。

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）。

ポート セキュリティがイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをグローバルにイネーブル化する手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（p.13-9）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **no switchport port-security mac-address** *address* [***vlan*** *vlan-ID*]
4. **show running-config port-security**
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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スタティック方式またはスティッキ方式のセキュア MAC アドレスを削除する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	**no switchport port-security mac-address** *address* **例：** `switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティから MAC アドレスを削除します。
ステップ 4	**show running-config port-security** **例：** `switch(config-if)# show running-config port-security`	ポート セキュリティ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。

ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除できます。

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、**switchto vdc** コマンドを使用します）。

手順の概要

1. **config t**
2. **clear port-security dynamic** {**interface ethernet** *slot/port* | **address** *address*} [**vlan** *vlan-ID*]
3. **show port-security address**

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	**clear port-security dynamic** {**interface ethernet** *slot/port* | **address** *address*} [**vlan** *vlan-ID*] **例：** switch(config)# clear port-security dynamic interface ethernet 2/1	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 ***interface*** キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 ***address*** キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、***vlan*** キーワードを使用します。
ステップ 3	**show port-security address** **例：** switch(config)# show port-security address	セキュア MAC アドレスを表示します。

MAC アドレスの最大数の設定

レイヤ 2 インターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定できます。レイヤ 2 インターフェイス上の VLAN 単位でも MAC アドレスの最大数を設定できます。設定できる最大アドレス数は 4096 です。

（注）　インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、デバイスはこのコマンドを拒否します。スティッキ方式またはスタティック方式で学習されたアドレスの数を減らす場合は、「インターフェイスのスタティック方式またはスティッキ方式のセキュア MAC アドレスの削除」（p.13-13）を参照してください。ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

作業を開始する前に

デフォルトでは、各インターフェイスのセキュア MAC アドレスの最大数は 1 です。VLAN には、セキュア MAC アドレス数のデフォルトの最大値はありません。

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）。

ポート セキュリティがイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをイネーブルにする手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot*
3. [**no**] **switchport port-security maximum** *number* [***vlan*** *vlan-ID*]
4. **show running-config port-security**
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** *type slot*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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。*slot* は、MAC アドレスの最大数を設定するインターフェイスです。

ステップ 3	[**no**] **switchport port-security maximum** *number* [***vlan*** *vlan-ID*] **例：** `switch(config-if)# switchport port-security maximum 425`	現在のインターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定します。*number* の最大値は 4096 です。**no** オプションを使用すると、MAC アドレスの最大数がデフォルト値（1）にリセットされます。 最大数を VLAN に適用したい場合は、***vlan*** キーワードを使用します。
ステップ 4	**show running-config port-security** **例：** `switch(config-if)# show running-config port-security`	ポート セキュリティ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。

アドレス エージングのタイプと期間

MAC アドレス エージングのタイプと期間を設定できます。デバイスは、ダイナミック方式で学習された MAC アドレスがエージング期限に到達する時期を判断するためにこれらの設定を使用します。

作業を開始する前に

デフォルトのエージング タイムは 0 分（エージングはディセーブル）です。

デフォルトのエージング タイプは絶対エージングです。

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）。

ポート セキュリティがイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをイネーブルにする手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot*
3. [**no**] **switchport port-security aging type** {***absolute*** | ***inactivity***}
4. [**no**] **switchport port-security aging time** *minutes*
5. **show running-config port-security**
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	**interface** *type slot* **例：** switch(config)# interface ethernet 2/1 switch(config-if)#	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。*slot* は、MAC エージングのタイプと期間を設定するインターフェイスです。
ステップ 3	[**no**] **switchport port-security aging type** {***absolute*** | ***inactivity***} **例：** switch(config-if)# switchport port-security aging type inactivity	ダイナミックに学習された MAC アドレスにデバイスが適用するエージング タイプを設定します。**no** オプションを使用すると、エージング タイプがデフォルト値（絶対エージング）にリセットされます。
ステップ 4	[**no**] **switchport port-security aging time** *minutes* **例：** switch(config-if)# switchport port-security aging time 120	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で設定します。*minutes* の最大値は 1440 です。**no** オプションを使用すると、エージング タイムがデフォルト値である 0（エージングはディセーブル）にリセットされます。

	コマンド	目的
ステップ 5	**show running-config port-security** **例：** `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 6	**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。

セキュリティ違反時の処理の設定

セキュリティ違反が発生した場合にデバイスが実行する処理を設定できます。違反時の処理は、ポート セキュリティをイネーブルにしたインターフェイスごとに設定できます。

作業を開始する前に

デフォルトのセキュリティ処理では、セキュリティ 違反が発生したポートがシャットダウンされます。

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）。

ポート セキュリティがイネーブルになっていることを確認します。設定を確認する手順については、「ポート セキュリティの設定の確認」（p.13-18）を参照してください。ポート セキュリティをイネーブルにする手順については、「ポート セキュリティのグローバルなイネーブル化またはディセーブル化」（p.13-8）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **[no] switchport port-security violation {protect | restrict | shutdown}**
4. **show running-config port-security**
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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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。*slot* は、セキュリティ違反時の処理を設定するインターフェイスです。

	コマンド	目的
ステップ 3	[no] **switchport port-security** ***violation*** {***protect*** | ***restrict*** | ***shutdown***} **例**： `switch(config-if)# switchport port-security violation restrict`	現在のインターフェイスのポート セキュリティにセキュリティ違反時の処理を設定します。**no** オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。
ステップ 4	**show running-config port-security** **例**： `switch(config-if)# show running-config port-security`	ポート セキュリティ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。

ポート セキュリティの設定の確認

ポート セキュリティ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 running-config port-security	ポート セキュリティの設定を表示します。
show port-security	ポート セキュリティのステータスを表示します。

こ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。

セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。こ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。

ポート セキュリティ の設定例

次に示す例は、VLAN とインターフェイスのセキュア アドレス最大数が指定されているイーサネット 2/1 インターフェイスのポート セキュリティ設定です。この例のインターフェイスはトランクポートです。違反時の処理は Restrict（制限）に設定されています。

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

デフォルト設定

表 13-1 に ポート セキュリティ パラメータのデフォルトの設定値を示します。

表 13-1　ポート セキュリティ パラメータのデフォルト値

パラメータ	デフォルト
ポート セキュリティがグローバルにイネーブルかどうか	ディセーブル
インターフェイス単位でポート セキュリティがイネーブルかどうか	ディセーブル
MAC アドレス学習方式	ダイナミック
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

その他の参考資料

ポート セキュリティ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.13-19）
- 規格（p.13-19）
- MIB（p.13-19）

関連資料

関連事項	タイトル
レイヤ 2 スイッチング	『*Cisco NX-OS Layer 2 Switching Configuration Guide*』
ポート セキュリティ 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。	—

MIB

NX-OS はポート セキュリティに関して読み取り専用の SNMP をサポートしています。

MIB	MIB リンク
• CISCO-PORT-SECURITY-MIB	MIB のロケーションとダウンロードについては、次の URL を参照してください。 http://www.cisco.com/nx-os/mibs