ポート セキュリティの設定

この章は、次の内容で構成されています。

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、レイヤ 2 物理インターフェイス、レイヤ 2 ポート チャネル インターフェイス、および仮想ポートチャネル（vPC）を、MACアドレスの限定された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に設定できます。 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。

（注） 特に指定されていない限り、インターフェイスという用語は物理インターフェイス、ポート チャネル インターフェイス、および vPC を示します。同様に、レイヤ *2* インターフェイスという用語は、レイヤ 2 物理インターフェイスとレイヤ 2 ポート チャネル インターフェイスの両方を示します。

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。MACアドレスは、1つのインターフェイスだけでセキュアMACアドレスになることができます。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、限られた数のMACアドレスを学習できます。デバイスがセキュアMACアドレスを格納する方法は、デバイスがセキュアMACアドレスを学習した方法によって異なります。

（注） 学習された MAC アドレスはすべて、vPC ピア間で同期されます。

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の実行コンフィギュレーションにセキュアMACアドレスを追加したり、設定から削除したりできます。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すると、デバイスを再起動してもスタティック セキュア MAC アドレスには影響がありません。

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た場合。
- 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た場合。

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、入力トラフィックがインターフェイスを通過するときに 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 セキュア MAC アドレスをメモリに保存します。 ダイナミック 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。

- デバイスが再起動した場合。
- インターフェイスが再起動した場合。
- アドレスが、ユーザによって設定されたインターフェイスのエージング期限に達した場合。
- ユーザがアドレスを明示的に削除した場合。
- 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た場合。

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。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。 あるインターフェイスのスティッキ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、代わりにスティッキ学習を実行します。 スティッキ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。

スティッキ 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。

- ユーザがアドレスを明示的に削除した場合。
- 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た場合。

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。 有効な範囲は 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。

vPC ドメインでは、ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。

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

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。

（注） vPC ドメインでは、プライマリ vPC の設定が有効になります。

ヒント アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイス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。

最大デバイス数

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。

最大インターフェイス数

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、1025 のセキュア 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アドレス数は 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。

vPC ドメインでは、プライマリ vPC スイッチのセキュア MAC アドレスの最大数を設定します。 最大数のセキュア MAC アドレスがセカンダリ スイッチに設定されている場合でも、プライマリ vPC スイッチではカウントを確認します。

最大 VLAN 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 の最大数は、インターフェイスに設定されている最大数より大きくできません。 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。

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 アドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。

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。

MAX カウント違反

あるインターフェイスにセキュア 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。 ブロックされたエントリは、Cisco Nexus 5000 シリーズ スイッチ上の Forwarding Module（FWM）に追加されます。

あるインターフェイスに VLAN とインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。 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。

MAC 移動違反

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。 ブロックされたエントリが、ドロップ エントリとしてポート セキュリティ テーブルに追加されます。

セキュリティ違反が発生すると、デバイスは、インターフェイスのセキュリティ違反カウンタの値を増加させ、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。 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。

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。

Cisco Nexus 5010 および 5020 スイッチでは、MAC アドレスはセキュアでないポートに移動せず、セキュアでないポートのフレームは転送されます。 Cisco Nexus 5500 スイッチでは、MAC アドレスはセキュアでないポートに移動せず、セキュアでないポートのフレームはドロップされます。

制限

セキュアでない MAC アドレスからの入力トラフィックをドロップします。そして、この MAC アドレスを、ブロックされた MAC エントリとしてポート セキュリティ テーブルに追加します。

（注） vPC ドメインでは、制限モードで違反が発生したためにポート セキュリティ テーブルに追加されたブロックされた MAC アドレスは、vPC ピア間で同期されません。

デバイスはドロップされたパケットの数を保持します。これはセキュリティ違反カウントと呼ばれます。 アドレス ラーニングはインターフェイス上で最大回数のセキュリティ違反が発生するまで続行されます。 最初のセキュリティ違反のあとに学習されたアドレスからのトラフィックはドロップされます。

MAX カウント違反の最大数（10）に到達した後、インターフェイスはシャット ダウンされ、Cisco Nexus 5010 スイッチおよび 5020 スイッチで **errdisabled** 状態に置かれ、Cisco Nexus 5500 スイッチの保護モードに移動されます。

保護

これ以上の違反の発生を防止します。 セキュリティ違反をトリガーしたアドレスは学習されますが、そのアドレスからのトラフィックはドロップされます。 それ以降、アドレス学習は実行されなくなります。

（注） 保護のアクションは、Cisco Nexus 5500 スイッチでのみサポートされています。

（注） vPC では、プライマリ vPC スイッチに設定された違反アクションが有効になります。 そのため、セキュリティ違反がトリガーされた場合は常に、プライマリ vPC スイッチ上で定義されているセキュリティの処理が実行されます。

MAX移動違反の最大数（10）に到達した後、インターフェイスはシャットダウンされ、**errdisable** 状態に置かれます。

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

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されたすべてのセキュア アドレスをドロップします。 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ネイティブ トランク VLAN に移行します。

トランク ポートからアクセス ポート

レイヤ 2 インターフェイスをトランク ポートからアクセス 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され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

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

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。

ポート セキュリティのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco 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。 Cisco NX-OS ライセンス方式についての詳細は、『*License and Copyright Information for Cisco NX-OS Software*』次の URL で入手可能です。 http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html 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こと。
- vPC ドメインでは、両方の vPC ピアと、vPC ピアの両方の vPC インターフェイスで、ポート セキュリティをグローバルでイネーブルにする必要があります。 **config sync** コマンドを使用して、両方の vPC ピア間で設定に矛盾がないことを確認してください。

ポート セキュリティの注意事項と制約事項

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、PVLAN ポート上でサポートされます。
- ポート セキュリティは、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ません。
- ポート セキュリティは他の機能に依存しません。

- ポート セキュリティは、vPC ピア リンク上ではサポートされません。
- ポート セキュリティは、ネットワーク インターフェイス（NIF）ポート、Flex Link ポート、または vEthernet インターフェイス上ではサポートされません。

vPC 上のポート セキュリティの注意事項と制約事項

ポート セキュリティに関する注意事項と制約事項に加えて、vPC 上のポート セキュリティに関する追加の注意事項と制約事項があります。 vPC 上のポート 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。

- vPC ドメイン内の両方の vPC ピアで、ポート セキュリティをグローバルにイネーブルにする必要があります。
- 両方の vPC ピアの vPC インターフェイス上でポート セキュリティをイネーブルにする必要があります。
- プライマリ vPC ピアでスタティック セキュア MAC アドレスを設定する必要があります。 この MAC アドレスは、セカンダリ vPC ピアと同期されます。 セカンダリ ピアでスタティック セキュア MAC アドレスを設定しないでください。 この MAC アドレスはセカンダリ vPC 設定に表示されますが、有効にはなりません。
- 学習された MAC アドレスはすべて、vPC ピア間で同期されます。
- 両方の vPC ピアは、ダイナミックまたはスティッキ MAC アドレスの学習方式で設定できます。 ただし、両方の vPC ピアが同じ方式に設定されていることを推奨します。
- ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。
- セキュア MAC アドレスの最大数は、プライマリ vPC スイッチ上で設定します。 最大数のセキュア MAC アドレスがセカンダリ スイッチに設定されている場合でも、プライマリ vPC スイッチではカウントを確認します。
- 違反時の処理は、プライマリ vPC 上で設定します。 そのため、セキュリティ違反がトリガーされた場合は常に、プライマリ vPC スイッチ上で定義されているセキュリティの処理が実行されます。
- ポート セキュリティ機能が両方の vPC ピアでイネーブルになっており、かつポート セキュリティが vPC ピアの両方の vPC インターフェイス上でイネーブルになっている場合に、ポート セキュリティは vPC インターフェイス上でイネーブルになります。 設定が正しいことを確認するには、**config sync** コマンドを使用できます。
- スイッチでインサービス ソフトウェア アップグレード（ISSU）が実行されている間、ポート セキュリティの動作はそのピア スイッチ上で停止されます。 ピア スイッチはどの新しい MAC アドレスも学習せず、この動作中に発生した MAC の移動は無視されます。 ISSU が完了すると、ピア スイッチに通知され、通常のポート セキュリティ機能が再開します。
- 上位バージョンへの ISSU がサポートされていますが、下位バージョンへの ISSU はサポートされていません。

ポート セキュリティの設定

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。 デフォルトで、ポート セキュリティはグローバルにディセーブルになっています。

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、すべてのセキュア MAC アドレスを含むすべてのポート セキュリティ設定が失われます。

（注） vPC ドメインのポートセキュリティをイネーブル、またはディセーブルにするには、vPC ピアの両方でポート セキュリティをグローバルにイネーブル化またはディセーブルにする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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。
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。
ステップ 5	vPC ドメインのポート セキュリティが設定されている場合、ポートセキュリティをグローバルでイネーブルにするには、	—

	コマンドまたはアクション	目的
	vPC ピアでステップ 1 ～ 4 を繰り返します。 例：	

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。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 セキュリティをディセーブルにすると、そのインターフェイスのすべてのスイッチポートのポート セキュリティ設定が失われます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

vPC ドメインにポート セキュリティを設定する場合、両方の vPC ピアでポート セキュリティをグローバルにイネーブル化しておく必要があります。

レイヤ 2 イーサネット インターフェイスがポート チャネル インターフェイスのメンバである場合、レイヤ 2 イーサネット インターフェイスに対するポート セキュリティはイネーブルまたはディセーブルにできません。

セキュア レイヤ 2 ポート チャネル インターフェイスのメンバのいずれかのポート セキュリティがイネーブルになっている場合、先にポートチャネルインターフェイスからセキュア メンバ ポートをすべて削除しない限り、そのポートチャネル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できません。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。 • **interface ethernet** *slot*/*port*	ポート セキュリティを設定するイーサネット インターフェイスまたはポート チャネル インターフェイスのインター

	コマンドまたはアクション	目的

	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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`	インターフェイス上でポート 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。
ステップ 7	vPC ドメインのポートセキュリティを設定している場合、vPC 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には vPC ピアへの手順 1 ～ 6 を繰り返します。	—

スティッキ MAC アドレス ラーニング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 ラーニング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 ラーニング（デフォルトの学習方式）に戻ります。

デフォルトでは、スティッキ MAC アドレス ラーニングはディセーブルです。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スティッキ MAC アドレス ラーニング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 ラーニング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 ラーニング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。

（注） MAC アドレスが任意のインターフェイスでセキュア MAC アドレスである場合、その MAC アドレスがすでにセキュア MAC アドレスとなっているインターフェイスからその MAC アドレスを削除するまで、その MAC アドレスをスタティック セキュア MAC アドレスとして別のインターフェイスに追加することはできません。

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。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

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ないことを確認します。 必要に応じて、セキュア MAC アドレスを削除するか、インターフェイスの最大アドレス数を変更できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	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。

	コマンドまたはアクション	目的
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 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 セキュア MAC アドレスを削除できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スタティック 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 セキュリティからスタティック セキュア MAC アドレスを削除します。

	コマンドまたはアクション	目的
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。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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。

	コマンドまたはアクション	目的
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。
ステップ 4	**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。

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。 インターフェイスに設定できる最大アドレス数は 1025 です。 システムの最大アドレス数は 8192 です。

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。

（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。 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。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal 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。

	コマンドまたはアクション	目的

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	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 1025 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。 最大数を適用する 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。

アドレス エージングのタイプと期間の設定

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。

デフォルトのエージング タイプは絶対エージングです。

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。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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 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。
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。

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。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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 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。

	コマンドまたはアクション	目的
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、次のいずれかの作業を行います。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 NX-OS* コマンド リファレンス』を参照してください。

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	デバイスのポートセキュリティのステータスを表示します。
show port-security interface	特定のインターフェイスのポートセキュリティのステータスを表示します。
show port-security address	セキュア MAC アドレスを表示します。
show running-config interface	実行コンフィギュレーションにあるインターフェイスを表示します。
show mac address-table	MAC アドレス テーブルの内容を表示します。
show system internal port-security info global	デバイスのポートセキュリティの設定を表示します。

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の詳細については、『*Cisco Nexus 5000 Series NX-OS 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
```

vPC ドメインでのポート セキュリティの設定例

次に、vPC ドメインで vPC ピア上のポート セキュリティをイネーブルにして設定する例を示します。 最初のスイッチがプライマリ vPC ピアであり、2 番目のスイッチがセカンダリ vPC ピアです。 ドメイン 103 がすでに作成されていることを前提にしています。

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# int e103/1/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# copy running-config startup-config
```

ポート セキュリティのデフォルト設定

次の表に、ポート セキュリティ パラメータのデフォルト設定を示します。

表 *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 ラーニング方式	ダイナミック

パラメータ	デフォルト
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

ポート セキュリティに関する追加情報

関連資料

関連項目	参照先
レイヤ 2 スイッチング	『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』
vPC	『*Cisco Nexus 5000 Series 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 Nexus 5000 Series NX-OS Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

Cisco 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 のリンク
• CISCO-PORT-SECURITY-MIB （注） トラップは、セキュア MAC アドレスの違反の通知についてサポートされています。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ポート セキュリティの機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2*：ポート セキュリティの機能の履歴

機能名	リリース	機能情報
ポート セキュリティ	5.1(3)N1(1)	このリリースで導入された機能。