



ポート セキュリティの設定

この章の内容は、次のとおりです。

- [ポートセキュリティについて, 1 ページ](#)
- [ポートセキュリティのライセンス要件, 7 ページ](#)
- [ポートセキュリティの前提条件, 8 ページ](#)
- [ポートセキュリティの注意事項と制約事項, 8 ページ](#)
- [vPC 上のポートセキュリティの注意事項と制約事項, 9 ページ](#)
- [ポートセキュリティの設定, 10 ページ](#)
- [ポートセキュリティの設定の確認, 21 ページ](#)
- [セキュア MAC アドレスの表示, 21 ページ](#)
- [ポートセキュリティの設定例, 22 ページ](#)
- [vPC ドメインでのポートセキュリティの設定例, 22 ページ](#)
- [ポートセキュリティのデフォルト設定, 22 ページ](#)
- [ポートセキュリティに関する追加情報, 23 ページ](#)

ポート セキュリティについて

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着信トラフィックだけを許可するようにレイヤ 2 物理インターフェイス、レイヤ 2 ポート チャンネル インターフェイス、および仮想ポート チャンネル (vPC) 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。



(注) 特に指定がなければ、インターフェイスは物理インターフェイス、ポートチャンネルインターフェイス、および vPC を意味します。同様に、レイヤ 2 インターフェイスはレイヤ 2 物理インターフェイスとレイヤ 2 ポート チャンネルインターフェイスの両方を意味します。

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) 学習したすべての MAC アドレスは 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、vPC ピアの両方でエージングの期限に達した場合に限り、ダイナミック MAC アドレスがドロップされます。

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。

Inactivity

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。

Absolute

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、スティック、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 上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。

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1025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 スイッチにセキュア MAC アドレスの最大数を設定します。セカンダリ スイッチにセキュア MAC アドレスの最大数が設定されていても、プライマリ vPC スイッチは数の検証を行います。

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。

最大数違反

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過してしまう場合ブロックされたエントリは、Cisco Nexus スイッチの転送モジュール (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過すると、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は、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せん。

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。

MAC アドレスは非セキュアポートに移行せず、非セキュアポート上のフレームはドロップされます。

制限

非セキュア MAC アドレスからの入力トラフィックをすべてドロップし、ブロックされた MAC エントリとして MAC アドレスを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、ブロックされた MAC アドレスのうち、制限モードで違反が発生してポートセキュリティ テーブルに追加されたアドレスは、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数を保持しますが、これをセキュリティ違反回数と呼びます。インターフェイスで発生するセキュリティ違反が最大数に到達するまでアドレス学習を継続します。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。

違反の最大数 (10) に達すると違反がトリガーされ、デバイスは新しい MAC アドレスの学習を停止します。

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) vPC では、プライマリ vPC スイッチに設定された違反処理が有効になります。したがって、セキュリティ違反がトリガーされると、プライマリ vPC スイッチに定義されたセキュリティ処理が常に実行されます。

最大数違反に設定された最大値（10）に到達すると、インターフェイスはシャットダウンされ、**errdisabled** 状態に移行します。

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。VLANが存在する場合、スティッキMACアドレスは同じVLANに維持されます。存在しない場合、そのMACアドレスは、トランクポートのネイティブVLANに移動します。

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 ライセンス方式の詳細については、『 <i>License and Copyright Information for Cisco NX-OS Software</i> 』（次の URL で入手できます。 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 ピア上の両方の 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にイネーブルにする必要があります。**configsync** コマンドを使用して、両方の vPC ピアで設定が一致していることを確認することを推奨します。

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、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 ポートでサポートされています。
- ポートセキュリティは、スイッチドポートアナライザ (SPAN) 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 リンクではサポートされていません。
- 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 インターフェイスではサポートされていません。

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。
- 学習したすべての MAC アドレスは 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ク 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。セカンダリスイッチにセキュア MAC アドレスの最大数が設定されていても、プライマリ vPC スイッチは数の検証を行います。
- 違反時の処理は、プライマリ vPC 上で設定します。したがって、セキュリティ違反がトリガーされると、プライマリ vPC スイッチに定義されたセキュリティ処理が常に実行されます。
- 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ブिस 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ディセーブルにすると、インターフェイスのすべてのポートセキュリティ設定が無効になります。ポートセキュリティをグローバルにディセーブル化すると、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ン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ポートチャン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、先にポートチャン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、そのポートチャン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ンネルインターフェイスのインターフェイス

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> interface port-channel <i>channel-number</i> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	コンフィギュレーション モードを開始します。 (注) これが 10G ブレークアウト ポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	switchport 例 : <pre>switch(config-if)# switchport</pre>	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 : <pre>switch(config-if)# switchport port-security</pre>	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 : <pre>switch(config-if)# show running-config port-security</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	(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： <pre>switch# configure terminal switch(config)#</pre>	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。 <ul style="list-style-type: none"> • interface ethernet slot/port • interface port-channel channel-number 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 (注) これが 10G ブレークアウト ポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	switchport 例： <pre>switch(config-if)# switchport</pre>	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： <pre>switch(config-if)# switchport port-security mac-address sticky</pre>	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： <pre>switch(config-if)# show running-config port-security</pre>	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： <pre>switch(config-if)# copy running-config startup-config</pre>	(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 : <pre>switch# configure terminal switch(config)#</pre>	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。 <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 (注) これが 10G ブレークアウトポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	[no] switchport port-security mac-address address [vlan vlan-ID] 例 : <pre>switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE</pre>	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。 <ul style="list-style-type: none"> • 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。 (注) これが 10G ブレークアウト ポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
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。 (注) これが 10G ブレークアウト ポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。

	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。 <ul style="list-style-type: none"> • interface ethernet slot/port • interface port-channel channel-number 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 <i>slot</i> 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。 (注) これが 10G ブレークアウト ポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	[no] switchport port-security maximum number [vlan vlan-ID] 例： <pre>switch(config-if)# switchport port-security maximum 425</pre>	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。 <i>number</i> 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： <pre>switch(config-if)# show running-config port-security</pre>	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： <pre>switch(config-if)# copy running-config startup-config</pre>	(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： <pre>switch# configure terminal switch(config)#</pre>	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。 <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 (注) これが 10G ブレークアウトポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	[no] switchport port-security aging type {absolute inactivity} 例： <pre>switch(config-if)# switchport port-security aging type inactivity</pre>	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： <pre>switch(config-if)# switchport port-security aging time 120</pre>	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。 <i>minutes</i> 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： <pre>switch(config-if)# show running-config port-security</pre>	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： <pre>switch(config-if)# copy running-config startup-config</pre>	(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： <pre>switch# configure terminal switch(config)#</pre>	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。 <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 (注) これが 10G ブレークアウトポートの場合、 <i>slot/port</i> 構文は <i>slot/QSFP-module/port</i> になります。
ステップ 3	[no] switchport port-security violation {protect restrict shutdown} 例： <pre>switch(config-if)# switchport port-security violation restrict</pre>	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： <pre>switch(config-if)# show running-config port-security</pre>	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： <pre>switch(config-if)# copy running-config startup-config</pre>	(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についての詳細は、ご使用のプラットフォームの『[Security Command Reference](#)』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、ご使用のプラットフォームの『[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
```

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	マニュアルタイトル
レイヤ 2 スイッチング	『Cisco Nexus 6000 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 6000 Series NX-OS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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
<ul style="list-style-type: none"> • CISCO-PORT-SECURITY-MIB <p>(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。</p>	<p>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。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/ctmk/mibs.shtml</p>

