ポート セキュリティの設定

この章では、Cisco NX-OS デバイスにポート セキュリティを設定する手順について説明します。

この章は、次の項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、限定された MAC アドレス セットからの入力トラフィックだけを許可するようなレイヤ 2 物理インターフェイスおよびレイヤ 2 ポート チャネル インターフェイスを設定できます。この制限されたセット内の MAC アドレスは、セキュア MAC アドレスと呼ばれます。さらに、デバイスは、これらの MAC アドレスからのトラフィックでも、同じ VLAN 内の別のインターフェイスからの場合は許可しません。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。

Note 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とポートチャネル インターフェイスの両方を意味します。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 セキュリティが有効に設定されたインターフェイスごとに、スタティックまたはダイナミック方式で、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。

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。アドレスがまだ保護されていず、デバイスが該当する最大値に達していない場合、デバイスはそのアドレスを保護し、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。

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。

Note この機能は Cisco Nexus 9200 および 9300-EX シリーズ スイッチでサポートされています。

絶対値（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。

Note 絶対エージング タイムを設定すると、送信元MAC からのトラフィックが流れていても、MACエージングが発生します。ただし、MACエージングおよび再学習中に、一時的なトラフィック ドロップが発生する可能性があります。

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、スタティックまたはダイナミックに学習された MAC アドレスにも適用されます。

Tip 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。

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。

MAC 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えてしまう場合

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。

- デバイスが 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 番目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。

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。

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

レイヤ 2 転送モジュール（L2FM）のロギング レベルが 4 または 5 に増加した場合にのみ、MAC 移動通知が表示されます。

MAC 移動違反が発生すると、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を増分し、設定された違反モードに関係なく、インターフェイスはエラーディセーブルになります。違反モードが[制限（Restrict）]または[保護（Protect）]に設定されている場合、違反はシステム ログに記録されます。

MAC移動違反は、設定された違反モードに関係なく、インターフェイスがエラーディセーブルになるため、**errdisable** コマンドを使用して自動 errdisable リカバリをイネーブルにすることを推奨します。

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次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。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。

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。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

レイヤ 2 イーサネット ポート チャネル インターフェイスのポート セキュリティはアクセス モードまたはトランク モードで設定できます。

Note VXLAN インターフェイスではポート セキュリティを設定できません。

Note ポート セキュリティは、Cisco Nexus 9300-EX/FX/FX2/FX3 シリーズ スイッチ上の非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。Cisco NX-OSリリース 9.3(5) 以降、Cisco Nexus 9300-FX3 シリーズ スイッチがサポートされます。

ポート セキュリティとポート チャネル インターフェイス

ポートセキュリティは、レイヤ2ポートチャネルインターフェイスでサポートされます。ポート チャネル インターフェイス上で動作するポート セキュリティは、ここで説明する内容以外は、物理インターフェイスの場合と同じです。

一般的なガイドライン

ポート チャネル インターフェイスのポート セキュリティは、アクセス モードまたはトランク モードのいずれかで動作します。トランク モードでは、ポート セキュリティで適用される MAC アドレスの制限が、VLAN 単位ですべてのメンバ ポートに適用されます。

ポート チャネル インターフェイスのポート セキュリティを有効にしても、ポート チャネルのロード バランシングには影響しません。

ポート セキュリティは、ポート チャネル インターフェイスを通過するポート チャネル制御トラフィックには適用されません。ポート セキュリティを使用すると、セキュリティ違反にならないようにして、ポート チャネル制御パケットを通過させることができます。ポート チャネル制御トラフィックには、次のプロトコルが含まれます。

- ポート集約プロトコル（PAgP）
- リンク集約制御プロトコル（LACP）
- Inter-Switch Link（ISL）
- IEEE 802.1Q

セキュア メンバ ポートの設定

ポート チャネル インターフェイスのポート セキュリティ設定は、メンバ ポートのポート セキュリティ設定には影響しません。

メンバ ポートの追加

セキュア インターフェイスをポート チャネル インターフェイスのメンバ ポートとして追加した場合、デバイスはメンバ ポートで学習されたダイナミック セキュア アドレスをすべて廃棄しますが、メンバ ポートのその他のポート セキュリティ設定はすべて実行コンフィギュレーションに保持します。セキュア メンバ ポートで学習されたスティッキ方式とスタティック方式のセキュア MAC アドレスも、NVRAM ではなく実行コンフィギュレーションに保存されます。

ポート セキュリティがメンバ ポートでは有効になっていて、ポート チャネル インターフェイスでは有効になっていない場合、メンバ ポートをポート チャネル インターフェイスに追加しようとすると警告されます。セキュア メンバ ポートをセキュア ポート チャネル インターフェイス以外のインターフェイスに強制的に追加するには、**force** キーワードを指定して **channel-group** コマンドを使用します。

ポートがポート チャネル インターフェイスのメンバである間は、メンバ ポートのポート セキュリティを設定できません。これを行うには、まずメンバ ポートをポート チャネル インターフェイスから削除する必要があります。

メンバ ポートの削除

メンバ ポートをポート チャネル インターフェイスから削除すると、メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそのポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。

（注） ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポート セキュリティ設定を詳細に検査することを推奨します。

ポート チャネル インターフェイスの削除

セキュア ポート チャネル インターフェイスを削除すると、次の処理が行われます。

- ポート チャネル インターフェイスの学習されたセキュア MAC アドレスがすべて廃棄されます。これには、ポート チャネル インターフェイスで学習されたスタティック方式のセキュア MAC アドレスが含まれます。
- 各メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそれらのメンバポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。ポートチャネルインターフェイスへの参加前にメンバポートでポートセキュリティが有効になっていなかった場合、そのメンバポートでは、ポートチャネル インターフェイスの削除後もポート セキュリティが有効になりません。

（注） ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポート セキュリティ設定を詳細に検査することを推奨します。

ポート セキュリティの無効化

いずれかのメンバ ポートでポート セキュリティが有効になっている場合、ポート チャネル インターフェイスのポート セキュリティを無効にできません。これを行うには、まずすべてのセキュア メンバ ポートをポート チャネル インターフェイスから削除します。メンバ ポートのポート セキュリティを無効にしたあと、必要に応じて、ポート チャネル インターフェイスに再度追加できます。

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。

ポートからトランク ポートへのアクセス

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。

スイッチ ポートからルート 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。

ルート ポートからスイッチ 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。

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。

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	Dynamic
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、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、VXLAN対応VLANのトラフィックを伝送するスイッチポートインターフェイスではサポートされません。
- ポート セキュリティは、Cisco Nexus 9300-EX シリーズ スイッチの非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。
- Cisco Nexus 9000 シリーズ スイッチの USB ポートを無効にする方法はサポートされていません。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上に限り存続します。

Note 一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

プライマリ VLAN とセカンダリ VLAN 間の関連付けを設定した後、次の手順を実行します。

- セカンダリ VLAN のスタティック MAC アドレスは作成できません。
- セカンダリ VLAN を学習したダイナミック MAC アドレスは期限切れになります。

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および制限事項とは別に、vPC のポート セキュリティに関する次の注意事項および制限事項を満たしていることを確認します。

- ポート セキュリティは、vPC 展開の FEX インターフェイスではサポートされません。
- 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有効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 セキュリティを有効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。スタティック 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 アドレスも設定できます。第二スタティック 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。
- プライマリ vPC ポートとセカンダリ vPC ポートの両方で、最大 MAC カウント値が同じであることを確認する必要があります。

- セカンダリ vPC ポートでは、スタティック MAC の制限チェックは行われません。シスコは、最大 MAC カウントで定義されているように、セカンダリ vPC ポートで同じ数のスタティック MAC を設定することを推奨します。
- 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タティック MAC アドレスの学習方式で設定できます。シスコは、同じ方法を使用して両方の vPC ピアを設定することを推奨します。これは、vPC ロールの変更など、特定の場合にポートのシャットダウン（errDisabled 状態）を防ぐのに役立ちます。
- 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。プライマリ vPC スイッチは数の検証を行い、セカンダリ スイッチで最大数設定を無視します。
- 違反時の処理は、プライマリ vPC 上で設定します。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。
- 両方の vPC ピアで設定が正しいことを確認するには、**show vpc consistency-parameters id** 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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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** **Example:** `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無効化されます。
ステップ 3	(Optional) **show port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。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。

Before you begin

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。

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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** **Example:** `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** **Example:** `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	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`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** **Example:** `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** **Example:** `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 ラーニングが無効になります。
ステップ 5	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`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*] **Example:** `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	(Optional) **show running-config port-security** **Example:** `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。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`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* **Example:** `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。
ステップ 4	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

スティッキ セキュア MAC アドレスの削除

スティッキ セキュア MAC アドレスを削除できます。この際、削除するアドレスが設定されているインターフェイスで、スティッキ方式のアドレス学習を一時的にディセーブルにする必要があります。

始める前に

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 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 sticky** 例： `switch(config-if)# no switchport port-security mac-address sticky`	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にします。これにより、インターフェイスのスティッキ セキュア MAC アドレスが、ダイナミック セキュア MAC アドレスに変換されます。
ステップ 4	**clear port-security dynamic address** *address* 例： `switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD`	指定したダイナミック セキュア MAC アドレスを削除します。
ステップ 5	（任意） **show port-security address interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} 例： `switch(config)# show port-security address interface ethernet 2/1`	セキュア MAC アドレスを表示します。削除したアドレスは表示されません。

	コマンドまたはアクション	目的
ステップ 6	（任意） **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 ラーニングを再度イネーブルにします。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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*] **Example:** `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	(Optional) **show port-security address** **Example:** `switch(config)# show port-security address`	セキュアMACアドレスを表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`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。

	Command or Action	Purpose
ステップ 3	[**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*] **Example:** `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。有効な *number* の最高値は 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	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

アドレス エージング タイプおよび時間を設定する

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（エージングは無効）です。

Before you begin

ポート セキュリティがグローバルに有効にされている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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。

	Command or Action	Purpose

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*
	Example:
	`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**} **Example:** `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* **Example:** `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（エージングは無効）にリセットされます。 **Note** Cisco Nexus 9200 および 9300-EX シリーズ スイッチの場合、設定されたエージング タイムに最大 2 分が追加されることがあります。たとえば、エージング タイムを 10 分に設定すると、エージ アウトはトラフィックが停止してから 10 ー 12 分後に発生します。
ステップ 5	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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*
	Example:
	`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**} **Example:** `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	(Optional) **show running-config port-security** **Example:** `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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

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 vpc consistency-parameters vpc id	両方の vPC ピアの設定を確認します。

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。

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。スイッチでポート セキュリティを設定する前に、vPC ドメインを作成し、vPC ピア リンク隣接関係が確立されていることを確認します。

例：孤立ポートでのポート セキュリティの設定

```
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)# feature port-security
secondary_switch(config)# int e3/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondaryy_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# copy running-config startup-config
```

例：vPC レッグ上のポート セキュリティの設定

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int po10
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)# vpc 10
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int po10
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondaryy_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# vpc 10
secondary_switch(config-if)# copy running-config startup-config
```

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 9000 Series NX-OS Layer 2 Switching Configuration Guide*』

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 **Note** 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 [英語]