



ポート セキュリティ

- [ポートセキュリティの前提条件](#) (1 ページ)
- [ポートセキュリティの制約事項](#) (1 ページ)
- [ポートセキュリティの概要](#) (1 ページ)
- [ポートセキュリティの設定方法](#) (7 ページ)
- [ポートセキュリティの設定例](#) (15 ページ)
- [その他の参考資料](#) (17 ページ)
- [ポートセキュリティの機能情報](#) (17 ページ)

ポート セキュリティの前提条件

最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとする、コマンドが拒否されます。

ポート セキュリティの制約事項

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、使用可能な MAC アドレス（その他のレイヤ2機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用する MAC アドレスを含む）の総数を表します。

ポート セキュリティの概要

ポート セキュリティ

ポートセキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュアポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレスグループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を1つに制限し、単一

のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュアポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュアポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュアポートにアクセスしようとしたときにも、違反のフラグが立てられます。

セキュア MAC アドレスのタイプ

デバイスは、次のセキュア MAC アドレスのタイプをサポートします。

- **スタティックセキュア MAC アドレス** : `switchport port-security mac-address mac-address` インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレステーブルに保存された後、スイッチの実行コンフィギュレーションに追加されます。
- **ダイナミックセキュア MAC アドレス** : 動的に設定されてアドレステーブルにのみ保存され、スイッチの再起動時に削除されます。
- **スティッキーセキュア MAC アドレス** : 動的に学習することも、手動で設定することもできます。アドレステーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーションファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキーセキュア MAC アドレス

スティッキーラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキーセキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキーラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミックセキュア MAC アドレスをスティッキーセキュア MAC アドレスに変換します。すべてのスティッキーセキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキーセキュア MAC アドレスは、コンフィギュレーションファイル（スイッチが再起動されるたびに使用されるスタートアップコンフィギュレーション）に、自動的に反映されません。スティッキーセキュア MAC アドレスをコンフィギュレーションファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキーセキュアアドレスを保存しない場合、アドレスは失われます。

スティッキーラーニングがディセーブルの場合、スティッキーセキュア MAC アドレスはダイナミックセキュアアドレスに変換され、実行コンフィギュレーションから削除されます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレステーブルに追加されている状態で、アドレステーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。
- ポートセキュリティが有効な状態で診断テストを実行しています。

違反が発生した場合の対処に基づいて、次の3種類の違反モードのいずれかにインターフェイスを設定できます。

- **Protect (保護)** : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。



(注) トランク ポートに **protect** 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングが無効になります。

- **Restrict (制限)** : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- **Shutdown (シャットダウン)** : ポートセキュリティ違反により、インターフェイスが **error-disabled** になり、ただちにシャットダウンされます。その後、ポートの LED が消灯します。セキュアポートが **error-disabled** ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解消するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再度イネーブルにできます。これは、デフォルトのモードです。
- **Shutdown VLAN (VLAN シャットダウン)** : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が **errdisable** になります。

次の表に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 1: セキュリティ違反モードの処置

| 違反モード | トラフィックの転送 1 | SNMP トラップの送信 | Syslog メッセージの送信 | エラー メッセージの表示 2 | 違反カウンタの増加 | ポートの シャットダウン |
|--|--------------------------------|-----------------|--------------------|--------------------------------------|-----------|------------------------|
| protect (保護) | x | x | x | x | x | x |
| restrict (制限) | x | あり | あり | x | あり | x |
| shutdown (シャット ダウン) | x | x | x | x | あり | あり |
| shutdown vlan (VLAN シャット ダウン) | x | x | あり | x | あり | x 3 |

¹ 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。

² セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラーメッセージを返します。

³ 違反が発生した VLAN のみシャットダウンします。

ポートセキュリティ エージング

ポート上のすべてのセキュアアドレスにエージングタイムを設定するには、ポートセキュリティエージングを使用します。ポートごとに2つのタイプのエージングがサポートされています。

- **absolute** : 指定されたエージングタイムの経過後に、ポート上のセキュアアドレスが削除されます。
- **inactivity** : 指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュアアドレスが削除されます。

デフォルトのポートセキュリティ設定

表 2: デフォルトのポートセキュリティ設定

| \ | |
|--------------------------|--|
| 機能 | デフォルト設定 |
| ポートセキュリティ | ポート上でディセーブル |
| スティッキーアドレスラーニング | ディセーブル |
| ポートあたりのセキュア MAC アドレスの最大数 | 1 |
| 違反モード | シャットダウン。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。 |
| ポートセキュリティ エージング | ディセーブルエージング タイムは 0 スタティック エージングはディセーブル タイプは absolute |

ポートセキュリティの設定時の注意事項

- ポートセキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ (SPAN) の宛先ポートにすることはできません。
- 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。
- 音声 VLAN が設定された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場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合は、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュアアドレスを設定する必要があります。
- トランクポートがポートセキュリティで設定され、データトラフィック用のアクセス VLAN と音声トラフィック用の音声 VLAN に割り当てられている場合、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。

- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。
- デバイスはスティッキーセキュア MAC アドレスのポートセキュリティ エージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポートセキュリティについてまとめます。

表 3: 他の機能とポートセキュリティとの互換性

| ポート タイプまたはポートの機能 | ポートセキュリティとの互換性 |
|-----------------------------------|----------------|
| DTP ⁴ ポート ⁵ | なし |
| トランク ポート | あり |
| ダイナミックアクセスポート ⁶ | なし |
| ルーテッド ポート | なし |
| SPAN 送信元ポート | あり |
| SPAN 宛先ポート | なし |
| EtherChannel | あり |
| トンネリング ポート | あり |
| 保護ポート | あり |
| IEEE 802.1x ポート | あり |
| 音声 VLAN ポート ⁷ | あり |
| IP ソース ガード | あり |
| ダイナミックアドレス解決プロトコル (ARP) インスペクション | あり |
| Flex Link | あり |

⁴ DTP = Dynamic Trunking Protocol

⁵ **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。

⁶ **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定される VLAN Query Protocol (VQP) ポート。

- ⁷ ポートに最大限可能なセキュアなアドレスを設定します（アクセスVLANで可能なセキュアなアドレスの最大数に2を加えた数）。

ポートセキュリティの設定方法

ポートセキュリティのイネーブル化および設定

始める前に

このタスクは、ポートにアクセスできるステーションのMACアドレスを制限および識別して、インターフェイスへの入力を制約します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | 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 3 | port-security mac-address forbidden mac address 例： Device(config)# port-security mac-address forbidden 2.2.2 | すべてのインターフェイスのポートセキュリティで禁止する MAC アドレスを指定します。 |
| ステップ 4 | interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1 | 設定するインターフェイスを指定し、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 5 | switchport mode {access trunk} 例： | インターフェイススイッチポートモードを access または trunk に設定します。デフォルトモード（dynamic auto）の |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | Device(config-if)# switchport mode access | インターフェイスは、セキュアポートとして設定できません。 |
| ステップ 6 | switchport voice vlan <i>vlan-id</i> 例 : Device(config-if)# switchport voice vlan 22 | ポート上で音声 VLAN をイネーブルにします。 <ul style="list-style-type: none"> • <i>vlan-id</i> : 音声トラフィックに使用する VLAN を指定します。 |
| ステップ 7 | switchport port-security 例 : Device(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。 |
| ステップ 8 | switchport port-security [maximum <i>value</i> [vlan {<i>vlan-list</i> {access voice}}]] 例 : Device(config-if)# switchport port-security maximum 20 | (任意) インターフェイスの最大セキュア MAC アドレス数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。 (任意) vlan : VLAN あたりの最大値を設定します vlan キーワードを入力後、次のいずれかのオプションを入力します。 <ul style="list-style-type: none"> • <i>vlan-list</i> : トランクポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • access : アクセスポートで、VLAN をアクセス VLAN として指定します。 |

| | コマンドまたはアクション | 目的 |
|---------------|---|--|
| | | <ul style="list-style-type: none"> • voice : アクセスポートで、VLANを音声 VLAN として指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p> |
| <p>ステップ 9</p> | <p>switchport port-security violation {protect restrict shutdown shutdown vlan}</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security violation restrict</pre> | <p>(任意) 違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> • protect : ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 <p>(注) トランクポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングが無効になります。</p> <ul style="list-style-type: none"> • restrict : セキュア MAC アドレス数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| | | <p>SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。</p> <ul style="list-style-type: none"> • shutdown : 違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。SNMP トラップが送信されず。Syslog メッセージがロギングされ、違反カウンタが増加します。 • shutdown vlan : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 <p>(注) セキュア ポートが error-disabled ステートの場合は、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、shutdown および no shutdown 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か、clear errdisable interface vlan 特権 EXEC コマンドを入力します。</p> |
| ステップ 10 | <p>switchport port-security [mac-address mac-address [vlan {vlan-id} {access voice}]]</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security mac-address</pre> | <p>(任意) インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。</p> |

| | コマンドまたはアクション | 目的 |
|----------------|--|--|
| | <p>00:A0:C7:12:C9:25 vlan 3 voice</p> | <p>(注) このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュアアドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。</p> <p>(任意) vlan : VLAN あたりの最大値を設定します。</p> <p>vlan キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • vlan-id : トランクポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセスポートで、VLAN をアクセス VLAN として指定します。 • voice : アクセスポートで、VLAN を音声 VLAN として指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p> |
| <p>ステップ 11</p> | <p>switchport port-security mac-address sticky</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security mac-address sticky</pre> | <p>(任意) インターフェイス上でスティッキーラーニングをイネーブルにします。</p> |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| ステップ 12 | <p>switchport port-security mac-address sticky [<i>mac-address</i> vlan {<i>vlan-id</i> {access voice}}]</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice</pre> | <p>(任意) スティックキーセキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキーセキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p>(注) このコマンドの入力前にスティッキーラーニングをイネーブルにしないと、エラーメッセージが表示されてスティッキーセキュア MAC アドレスを入力できません。</p> <p>(任意) vlan : VLAN あたりの最大値を設定します。</p> <p>vlan キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • vlan-id : トランクポートで、VLAN ID および MAC アドレスを指定できます。VLANID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセスポートで、VLAN をアクセス VLAN として指定します。 • voice : アクセスポートで、VLAN を音声 VLAN として指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。</p> |
| ステップ 13 | <p>switchport port-security mac-address forbidden <i>mac address</i></p> <p>例 :</p> | <p>特定のインターフェイスのポートセキュリティで禁止する MAC アドレスを指定します。</p> |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| | Device(config-if)# switchport port-security mac-address forbidden 2.2.2 | |
| ステップ 14 | end 例： Device(config-f)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 15 | show port-security 例： Device# show port-security | ポートセキュリティ設定に関する情報を表示します。 |

ポートセキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | 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 3 | interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1 | 設定するインターフェイスを指定し、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。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 4 | <p>switchport port-security aging {static time <i>time</i> type {absolute inactivity}}</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security aging time 120</pre> | <p>セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。</p> <p>(注) デバイスはスタティックセキュアアドレスのポートセキュリティ エージングをサポートしていません。</p> <ul style="list-style-type: none"> このポートに、スタティックに設定されたセキュアアドレスのエージングをイネーブルにする場合は、static キーワードを入力します。 time 引数は、このポートのエージング タイムを指定します。有効値の範囲は 0 ~ 1440 分です。 type キーワードには、次のキーワードのいずれかを選択します。 <ul style="list-style-type: none"> absolute : エージングタイプを絶対エージングとして設定します。このポートのセキュアアドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュアアドレスリストから削除されます。 inactivity : エージングタイプを非アクティブエージングとして設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュアアドレスが期限切れになります。 |
| ステップ 5 | <p>end</p> <p>例 :</p> <pre>Device(config-f)# end</pre> | <p>インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p> |

| | コマンドまたはアクション | 目的 |
|--------|---|--------------------------|
| ステップ 6 | show port-security 例 : Device# show port-security | ポートセキュリティ設定に関する情報を表示します。 |

ポートセキュリティの監視

次の表に、ポートセキュリティ情報を表示します。

表 4: ポートセキュリティのステータスおよび設定を表示するコマンド

| コマンド | 目的 |
|---|--|
| show port-security [interface interface-id] | スイッチまたは指定されたインターフェイスのポートセキュリティ設定を、各インターフェイスで許容されるセキュアMACアドレスの最大数、インターフェイスのセキュアMACアドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。 |
| show port-security [interface interface-id] address | すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュアMACアドレス、および各アドレスのエージング情報を表示します。 |
| show port-security interface interface-id vlan | 指定されたインターフェイスに VLAN 単位で設定されているセキュアMACアドレスの数を表示します。 |

ポートセキュリティの設定例

例：ポートセキュリティのイネーブル化および設定

次に、ポート上でポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティックセキュアMACアドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
```

例：ポートセキュリティ エージングのイネーブル化および設定

```
Device(config-if)# switchport port-security maximum 50
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# end
```

次に、ポートの VLAN 3 上にスタティックセキュア MAC アドレスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
Device(config-if)# end
```

次に、ポートのスティッキー ポートセキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュアアドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
Device> enable
Device# configure terminal
Device(config)# interface tengigabitethernet 1/0/1
Device(config-if)# switchport access vlan 21
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 22
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 20
Device(config-if)# switchport port-security violation restrict
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Device(config-if)# switchport port-security mac-address 0000.0000.0003
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Device(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Device(config-if)# switchport port-security maximum 10 vlan access
Device(config-if)# switchport port-security maximum 10 vlan voice
Device(config-if)# end
```

例：ポートセキュリティ エージングのイネーブル化および設定

次の例では、ポートセキュリティエージングのイネーブル化方法と設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# switchport port-security aging time 120
Device(config-if)# end
```


その他の参考資料

関連資料

| 関連項目 | マニュアル タイトル |
|-------------------------------|---|
| この章で使用するコマンドの完全な構文および使用方法の詳細。 | Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches) |

シスコのテクニカル サポート

| 説明 | リンク |
|--|---|
| <p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p> | http://www.cisco.com/support |

ポートセキュリティの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 5: ポートセキュリティの機能情報

| 機能名 | リリース | 機能情報 |
|-----------|--------------------------|--|
| ポートセキュリティ | Cisco IOS リリース 15.2(7)E1 | この機能を使用して、ポートへのアクセスを許可するステーションのMACアドレスを制限および識別して、インターフェイスへの入力を制限します。 |