CHAPTER 11

ポート セキュリティの設定

この章では、ポート セキュリティを設定する手順について次の内容で説明します。

- 「ポート セキュリティの概要」（P.11-1）
- 「注意事項および制約事項」（P.11-6）
- 「その他の関連資料」（P.11-19）
- 「ポート セキュリティの設定」（P.11-6）
- 「ポート セキュリティの設定の確認」（P.11-19）
- 「セキュア MAC アドレスの表示」（P.11-19）
- 「ポート セキュリティの設定例」（P.11-19）
- 「その他の関連資料」（P.11-19）
- 「ポート セキュリティの機能の履歴」（P.11-20）

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、限定的なセキュア MAC アドレスからのインバウンド トラフィックを許可するようにレイヤ 2 インターフェイスを設定することができます。セキュアな MAC アドレスからのトラフィックは、同じ VLAN 内の別のインターフェイス上では許可されません。「セキュア」にできる MAC アドレスの数は、インターフェイス単位で設定します。

ここでは、次の内容について説明します。

- 「セキュア MAC アドレスの学習」（P.11-1）
- 「ダイナミック アドレスのエージング」（P.11-2）
- 「セキュア MAC アドレスの最大数」（P.11-3）
- 「セキュリティ違反と処理」（P.11-4）
- 「ポート セキュリティとポート タイプ」（P.11-5）

セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。学習できるアドレスの数には制限があります（「セキュア MAC アドレスの最大数」（P.11-3）を参照）。ポート セキュリティがイネーブルになっているインターフェイスでのアドレス学習には、次の方式を使用できます。

- 「スタティック方式」（P.11-2）

- 「ダイナミック方式」（P.11-2）（デフォルトの方式）
- 「スティッキ方式」（P.11-2）

スタティック方式

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

スタティック セキュア MAC アドレスのエントリは、明示的に削除するまで、インターフェイスの設定内に維持されます。詳細については、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

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

ダイナミック方式

デフォルトでは、インターフェイスのポート セキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、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。

ダイナミック アドレスはエージングが行われ、エージングの期限に達すると、ドロップされます（「ダイナミック アドレスのエージング」（P.11-2）を参照）。

ダイナミック アドレスは、再起動後は維持されません。

ダイナミック方式で学習された特定のアドレス、または特定のインターフェイスでダイナミックに学習されたすべてのアドレスを削除する場合は、「ダイナミック セキュア MAC アドレスの削除」（P.11-12）を参照してください。

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミック アドレス学習と同じ方法で MAC アドレスをセキュア アドレスにします。これらのアドレスは、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（**copy run start**）することにより、再起動後も維持することができます。

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すると、ダイナミック学習が停止されて、代わりにスティッキ学習が使用されます。スティッキ学習をディセーブルにすると、ダイナミック学習が再開されます。

スティッキ セキュア MAC アドレスはエージングされません。

スティッキ方式で学習された特定のアドレスを削除する場合は、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

ダイナミック アドレスのエージング

ダイナミック方式で学習された MAC アドレスはエージングされ、エージングの期限に達するとドロップされます。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。

アドレス エージングの判断には、2 つの方法があります。

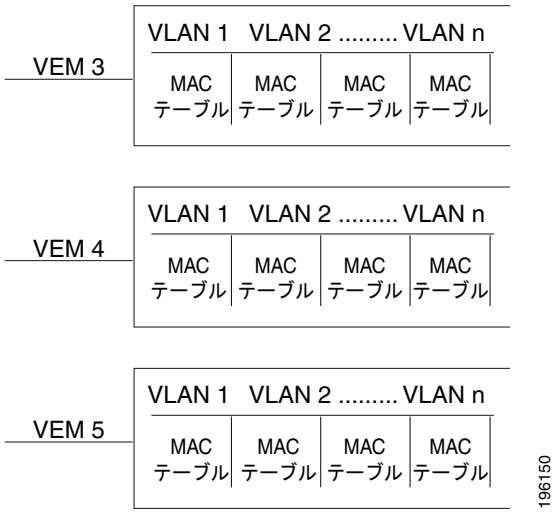
- 非アクティブ：適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。
- 絶対時間：デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。

セキュア MAC アドレスの最大数

セキュア ポート上のセキュア MAC アドレスは、他の標準的な MAC と同じ MAC アドレス テーブルに挿入されます。MAC テーブルの上限に達すると、その VLAN に対する新しいセキュア MAC の学習は行われなくなります。

図 11-1 に示すように、VEM 内の VLAN ごとに 1 つの転送テーブルがあり、各転送テーブルにセキュア MAC アドレスを最大数まで格納できます。現在の MAC アドレスの最大数については、「セキュリティ設定の制限値」（P.17-1）を参照してください。

図 11-1　VEM あたりのセキュア MAC アドレス



インターフェイスのセキュア MAC アドレス

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

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

インターフェイス 1 つあたりの許容されるセキュア MAC アドレスの数は、次の制限値によって決定されます。

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

  VLAN とインターフェイスの最大数の関係については、「セキュリティ違反と処理」（P.11-4）に例が示されています。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュア アドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。ダイナミックに学習されたアドレスの削除方法については、「ダイナミック セキュア MAC アドレスの削除」（P.11-12）を参照してください。スティッキまたはスタティック方式で学習されたアドレスの削除方法については、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

セキュリティ違反と処理

次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。

- 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。

  次のいずれかが発生すると、違反が検出されます。

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

（注） 特定のセキュア ポートでセキュア MAC アドレスが設定または学習された後、同一 VLAN 上の別のポートでポート セキュリティがセキュア MAC アドレスを検出したときに発生する一連のイベントは、MAC 移動の違反と呼ばれます。

インターフェイス上でセキュリティ違反が発生したときは、そのインターフェイスのポート セキュリティ設定で指定されている処理が適用されます。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。

  Example:
  ```
  n1000v(config)# errdisable recovery cause psecure-violation
  n1000v(config)# copy running-config startup-config (Optional)
  ```

- 保護：違反の発生を防止します。インターフェイスの最大 MAC アドレス数に到達するまでアドレス学習を継続し、到達後はそのインターフェイスでの学習をディセーブルにして、セキュア MAC アドレス以外のアドレスからの入力トラフィックをすべてドロップします。

セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合は、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が適用されます。MAC の移行違反は、別のインターフェイスですでにセキュアになっている MAC を認識するポートでトリガーされます。

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

アクセス ポートからトランク ポートへの変更による影響

ポート セキュリティが設定されているレイヤ 2 インターフェイスでアクセス ポートをトランク ポートに変更すると、ダイナミック方式で学習されたすべてのセキュア アドレスがドロップされます。ネイティブ トランク VLAN に接続されているデバイスは、スタティック方式またはスティッキ方式で学習したアドレスを移行します。

トランク ポートからアクセス ポートへの変更による影響

ポート セキュリティが設定されているレイヤ 2 インターフェイスでトランク ポートをアクセス ポートに変更すると、ダイナミック方式で学習されたすべてのセキュア アドレスがドロップされます。設定済みの MAC アドレスおよびスティッキ MAC アドレスは、ネイティブ トランク VLAN に存在しない場合、かつ移行先のアクセス ポートに対して設定されたアクセス VLAN とも一致しない場合は、すべてドロップされます。

注意事項および制約事項

ポート セキュリティを設定する場合、次の注意事項に従ってください。

- ポート セキュリティは、次でサポートされていません。
  - イーサネット インターフェイス
  - イーサネット ポートチャネル インターフェイス
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポート
- 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 802.1X をサポートしていません。
- ポート セキュリティは、スタティック MAC がすでに存在するインターフェイスには設定できません。
- VLAN にスタティック MAC がすでに存在する場合、それが別のインターフェイスでプログラムされている場合でも、その VLAN のインターフェイスでポート セキュリティをイネーブルにすることはできません。

デフォルト設定値

表 11-1 に、ポート セキュリティ パラメータのデフォルトの設定値を示します。

表 11-1　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
インターフェイス	ディセーブル
MAC アドレス ラーニング方式	ダイナミック
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

ポート セキュリティの設定

ここでは、次の内容について説明します。

- 「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）
- 「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」（P.11-8）

- 「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」（P.11-9）
- 「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）
- 「ダイナミック セキュア MAC アドレスの削除」（P.11-12）
- 「MAC アドレスの最大数の設定」（P.11-13）
- 「アドレス エージングのタイプと期間の設定」（P.11-15）
- 「セキュリティ違反時の処理の設定」（P.11-16）
- 「ポート セキュリティ違反がディセーブルなポートの回復」（P.11-17）

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 セキュリティをイネーブルまたはディセーブルにするには、次の手順を実行します。MAC アドレスのダイナミック学習についての詳細は、「セキュア MAC アドレスの学習」（P.11-1）を参照してください。

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

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、ポート セキュリティはすべてのインターフェイスでディセーブルです。
- インターフェイスのポート セキュリティをイネーブルにすると、MAC アドレスのダイナミック学習もイネーブルになります。スティッキ方式の MAC アドレス ラーニングをイネーブルにするには、「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」（P.11-8）の手順も完了する必要があります。

手順の概要

1. **config t**
2. **interface** *type number*
3. **[no] switchport port-security**
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(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** **Example:** n1000v(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 4	**show running-config port-security** **Example:** n1000v(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** **Example:** n1000v(config-if)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

スティッキ MAC アドレス 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するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- ダイナミック MAC アドレス ラーニングがインターフェイスのデフォルトです。
- 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。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. [**no**] **switchport port-security mac-address sticky**
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(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 sticky** **Example:** n1000v(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 4	**show running-config port-security** **Example:** n1000v(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** **Example:** n1000v(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 アドレスを追加するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。
- インターフェイスのセキュア MAC アドレス最大数に達しているかどうかを判断します（**show port-security** コマンドを使用）。

- 必要な場合は、セキュア MAC アドレスを削除できます。次のいずれかを参照してください。
  - 「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）
  - 「ダイナミック セキュア MAC アドレスの削除」（P.11-12））
  - 「MAC アドレスの最大数の設定」（P.11-13））。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. [**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(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:** `n1000v(config-if)# switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** **Example:** `n1000v(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** **Example:** `n1000v(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。

インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除

レイヤ 2 インターフェイスからスタティック方式またはスティッキ方式のセキュア MAC アドレスを削除するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. **no switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	目的
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(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* **Example:** n1000v(config-if)# no switchport port-security mac-address 0019.D2D0.00AE	現在のインターフェイスのポート セキュリティから MAC アドレスを削除します。
ステップ 4	**show running-config port-security** **Example:** n1000v(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** **Example:** n1000v(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 アドレスを削除するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 vethernet** *number* | **address** *address*} [**vlan** *vlan-ID*] **Example:** n1000v(config)# clear port-security dynamic interface vethernet 36	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 **interface** キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 **address** キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、**vlan** キーワードを使用します。
ステップ 3	**show port-security address** **Example:** n1000v(config)# show port-security address	セキュア MAC アドレスを表示します。

MAC アドレスの最大数の設定

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

（注）　インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、コマンドは拒否されます。

スティッキ方式またはスタティック方式で学習されたアドレスの数を減らす場合は、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- セキュア MAC は L2 Forwarding Table（L2FT; L2 転送テーブル）を共有します。各 VLAN の転送テーブルには最大 1024 エントリを保持できます。
- 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。

- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** ***type*** *number*
3. [**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(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 maximum** *number* [**vlan** *vlan-ID*] **Example:** `n1000v(config-if)# switchport port-security maximum 425`	現在のインターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定します。*number* の最大値は 4096 です。**no** オプションを使用すると、MAC アドレスの最大数がデフォルト値（1）にリセットされます。 最大数を適用する 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** **Example:** `n1000v(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** **Example:** `n1000v(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

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した時期を判断するために使用される MAC アドレス エージングのタイプと期間を設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトのエージング タイムは 0 分（エージングはディセーブル）です。
- デフォルトのエージング タイプは絶対エージングです。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. [**no**] **switchport port-security aging type** {**absolute** | **inactivity**}
4. [**no**] **switchport port-security aging time** *minutes*
5. **show running-config port-security**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(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 aging type** {**absolute** | **inactivity**} **Example:** n1000v(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。

	コマンド	目的
ステップ 4	**[no] switchport port-security aging time** *minutes* **Example:** n1000v(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** **Example:** n1000v(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** **Example:** n1000v(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

セキュリティ違反に対するインターフェイスの対応方法を設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。
- セキュリティ違反に対する次のインターフェイスの応答を設定できます。
  - protect：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
  - restrict：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、SecurityViolation カウンタを増分させます。
  - shutdown：（デフォルト）即時にインターフェイスを errdisable ステートにして、SNMP トラップ通知を送信します。

  詳細については、「セキュリティ違反と処理」（P.11-4）を参照してください。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*

3. [no] switchport port-security violation {protect | restrict | shutdown}
4. show running-config port-security
5. copy running-config startup-config

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(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 violation** {**protect** | **restrict** | **shutdown**} **Example:** n1000v(config-if)# switchport port-security violation protect	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。 • **protect**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。 • **restrict**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、SecurityViolation カウンタを増分させます。 • **shutdown**：（デフォルト）即時にインターフェイスを errdisable ステートにして、SNMP トラップ通知を送信します。
ステップ 4	**show running-config port-security** **Example:** n1000v(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** **Example:** n1000v(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 セキュリティ違反がディセーブルなポートの回復

ポート セキュリティ違反がディセーブルなインターフェイスを自動的に回復するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- インターフェイスを errdisable ステートから手動で回復するには、**shutdown** コマンドを入力してから、**no shutdown** コマンドを入力する必要があります。
- 詳細については、「セキュリティ違反と処理」（P.11-4）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. **errdisable recovery cause psecure-violation**
4. **errdisable recovery interval** *seconds*
5. **show interface** *type* ***number***

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(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	**errdisable recovery cause psecure-violation** **Example:** `n1000v(config-if)# errdisable recovery cause psecure-violation`	セキュリティ違反がディセーブルな特定のポートの期間指定された自動リカバリをイネーブルにします。
ステップ 4	**errdisable recovery interval** *seconds* **Example:** `n1000v(config-if)# errdisable recovery interval 30`	秒単位のタイマー リカバリ間隔を 30 ～ 65535 秒に設定します。
ステップ 5	**show interface** *type number* **Example:** `n1000v(config-if)# show running-config port-security`	確認のために theinterface ステートを表示します。

ポート セキュリティの設定の確認

ポート セキュリティの設定情報を表示するには、次のコマンドを使用します。

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

このコマンドの出力結果として表示される各フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。このコマンドの出力結果として表示される各フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

ポート セキュリティの設定例

次に、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 vEthernet 36 インターフェイスのポート セキュリティ設定の例を示します。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 Protect（保護）に設定されています。

```
interface vethernet 36
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 protect
```

その他の関連資料

ポート セキュリティの実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.11-20）
- 「標準」（P.11-20）

関連資料

関連項目	参照先
レイヤ 2 スイッチング	*『Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)』*
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 1000V Command Reference, Release 4.2(1)SV1(4a)』*

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。	—

ポート セキュリティの機能の履歴

ここでは、ポート セキュリティ機能のリリース履歴を示します。

機能名	リリース	機能情報
ポート セキュリティ	4.0(4)SV1(1)	この機能が導入されました。