CHAPTER 33

コントロール プレーンのセキュリティ設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにコントロール プレーンのセキュリティ機能の設定方法について説明します。いずれのネットワークでも、レイヤ 2 スイッチおよびレイヤ 3 スイッチは、ネットワーク内の他のスイッチと制御パケットを交換します。Cisco ME スイッチは、カスタマー ネットワークとサービスプロバイダー ネットワーク間の変換として機能し、コントロール プレーン セキュリティを使用して 2 つのネットワーク間のトポロジ情報が分離されていることを確認します。このメカニズムにより、起こりうる他のカスタマー ネットワークによる DoS 攻撃から保護します。

コントロール プレーンのセキュリティの概要

Cisco ME スイッチでは、Network Node Interface（NNI; ネットワーク ノード インターフェイス）として設定されたポートがサービス プロバイダー ネットワークに接続されます。このスイッチは、これらのポートを介してネットワークのその他のスイッチと通信し、通常のトラフィックに加えてプロトコル制御パケットを交換します。Cisco ME スイッチ上のその他のポートは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）であり、カスタマー側のポートとして使用されます。ポートはそれぞれ単一のカスタマーに接続され、通常、スイッチとカスタマー間のネットワーク プロトコル制御パケット交換は必要ありません。レイヤ 2 プロトコルのほとんどは、UNI ではサポートされていません。偶発的または意図的な CPU 過負荷から保護するために、Cisco ME スイッチでは UNI の事前定義された一組のレイヤ 2 制御パケットおよび一部のレイヤ 3 制御パケットを廃棄またはレート制限することにより、自動的にコントロール プレーン セキュリティを実現します。

3 番目のポート タイプである、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）も設定できます。ENI は、UNI と同様、カスタマー側のインターフェイスです。ENI 上では、デフォルトで、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）などのレイヤ 2 制御プロトコルがディセーブルになっています。ENI 上では、UNI とは異なり、これらのプロトコルをイネーブルにできます。ポート チャネルで ENI を設定する際に、Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）、および Port Aggregation Protocol（PAgP; ポート集約プロトコル）もイネーブルにできます。プロトコルがインターフェイス上でイネーブルになっているかディセーブルになっているかによって、ENI は、プロトコル パケットを破棄するか、またはレート制限します。ENI 上の他のすべての制御プロトコルに関して、スイッチは、UNI の場合と同じ方法でパケットを破棄するかレート制限します。

CPU 保護（デフォルトでイネーブルになっています）では、ポートごとに 19 のポリサーが使用されます。CPU 保護がイネーブルになっている場合、ポートごとに最大 45 のポリサーを設定できます。ポートごとのポリサーをより多く設定する必要がある場合、**no policer cpu uni all** 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スイッチをリロードすることによって、CPU 保護をディセーブルにできます。CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上に 62）を、class-default に対して 1 つのポリサーを設定できます。

（注）　CPU をオフにするとプロトコル パケットが CPU に到達可能となり、これが、CPU 処理の過負荷や、ソフトウェアによるストーム制御の原因となる可能性があります。

コントロール プレーンのセキュリティは、ポートがルーティング モードまたは非ルーティング モードであるかにかかわらず、ルータの MAC アドレスを含むレイヤ 2 制御パケットおよび非 IP パケットに対して、ポート上でサポートされます （ポートがルーティング モードとなるのは、グローバル IP ルーティングがイネーブルで、ポートが **no switchport** インターフェイス コンフィギュレーション コマンドにより設定されているか、または Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）がアクティブな VLAN に関連付けられている場合です）。これらのパケットは、レイヤ 2 プロトコル設定に応じて、廃棄されるかまたはレート制限されます。レイヤ 3 制御パケットの場合、ルーティング モードのポート上では（レイヤ 3 サービス ポリシーが付加されているかどうかにかかわらず）、コントロール プレーンのセキュリティにより、Internet Group Management Protocol（IGMP）制御パケットのレート制限だけがサポートされます。レイヤ 3 パケットの場合、非ルーティング モードのポート上では（レイヤ 2 サービス ポリシーが付加されているかどうかにかかわらず）、ルータ MAC アドレスが設定された IP パケットだけが廃棄されます。

次の制御パケット タイプが、廃棄またはレート制限されます。

- レイヤ 2 プロトコル制御パケット
  - UNI および ENI 上で常に廃棄される制御パケット（Dynamic Trunking Protocol [DTP; ダイナミック トランキング プロトコル] パケットおよび一部の Bridge Protocol Data Unit [BPDU; ブリッジ プロトコル データ ユニット] など）
  - デフォルトでは廃棄されるが、イネーブルまたはトンネリングできる制御パケット（CDP、STP、LLDP、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコル、LACP および PAgP パケットなど）。これらのプロトコル パケットがイネーブルである場合は、スイッチによりレート制限およびトンネリングされます。
  - スイッチで必要とされる制御パケットまたは管理パケット（キープアライブ パケットなど）。これらの制御パケットは CPU により処理されますが、CPU が過負荷にならないよう標準または安全限界にレート制限されます。
- ルータ MAC アドレスが設定された非 IP パケット
- ルータ MAC アドレスが設定された IP パケット
- デフォルトでイネーブルに設定されていて、レート制限される必要がある IGMP 制御パケット。ただし、IGMP スヌーピングおよび IP マルチキャスト ルーティングがディセーブルである場合、これらのパケットはデータ パケットのように処理され、ポリサーは割り当てされません。

スイッチではポリシングを使用して、レイヤ 2 制御プロトコルを廃棄またはレート制限することにより、コントロール プレーンのセキュリティを実行します。レイヤ 2 プロトコルが UNI または ENI ポートでイネーブルであり、スイッチ上でトンネリングされる場合に、これらのプロトコル パケットはレート制限されます。レート制限されない場合は、制御パケットが廃棄されます。

プロトコル トラフィックには、デフォルトで CPU により廃棄されるものと、レート制限されるものがあります。表 33-1 に、この機能がイネーブルである場合またはレイヤ 2 プロトコル トンネリングがプロトコルに対してイネーブルである場合のデフォルト アクションおよびレイヤ 2 プロトコル パケットに対するアクションを示します。これらの機能には、UNI 上でイネーブルにできないものがあり、す

べてのプロトコルをトンネリングできるわけではない（ダッシュで示される）ことに注意してください。レイヤ 2 プロトコル トンネリングが*任意*のサポート対象プロトコル（CDP、STP、VTP、LLDP、LACP、PAgP、または UDLD）に対してイネーブルである場合、スイッチのレイヤ 2 プロトコル トンネリング プロトコルはすべてのポート上でレート制限ポリサーを使用します。UDLD がポート上でイネーブルであるか、UDLD トンネリングがイネーブルである場合、UDLD パケットはレート制限されます。

表 33-1　UNI または ENI で受信されるレイヤ 2 プロトコル パケットのコントロール プレーンのセキュリティ アクション

プロトコル	デフォルト	機能がイネーブルである場合	レイヤ 2 プロトコル トンネリングがイネーブルである場合 [1]
STP	廃棄	レート制限 **（注）** STP をイネーブルにできるのは、ENI 上でだけです。	レート制限
RSCD_STP（予約された IEEE 802.1D アドレス）	廃棄	Ethernet Link Management Interface（ELMI）がイネーブルである場合、グローバルまたはポート単位のいずれか最後に設定された方法で、スロットル ポリサーがポートに割り当てられる。ELMI がディセーブルである場合、（グローバルまたはポート単位のいずれか最後に設定された方法で）廃棄ポリサーがポートに割り当てられる。	
PVST+	廃棄	–	レート制限
LACP	廃棄	レート制限 **（注）** LACP をイネーブルにできるのは、ENI 上でだけです。	レート制限
PAgP	廃棄	レート制限 **（注）** PAgP をイネーブルにできるのは、ENI 上でだけです。	レート制限
IEEE 802.1x	廃棄	レート制限	–
CDP	廃棄	レート制限 **（注）** CDP をイネーブルにできるのは、ENI 上でだけです。	レート制限
LLDP	廃棄	レート制限 **（注）** LLDP をイネーブルにできるのは、ENI 上でだけです。	レート制限
DTP	廃棄	–	–
UDLD	廃棄	レート制限	レート制限
VTP	廃棄	–	レート制限
CISCO_L2（MAC アドレス 01:00:0c:cc:cc:cc が設定されたその他のシスコ レイヤ 2 プロトコル）	廃棄	–	CDP、DTP、UDLD、PAgP、または VTP がレイヤ 2 トンネリングされる場合にレート制限される。

表 33-1　UNI または ENI で受信されるレイヤ 2 プロトコル パケットのコントロール プレーンのセキュリティ アクション（続き）

プロトコル	デフォルト	機能がイネーブルである場合	レイヤ 2 プロトコル トンネリングがイネーブルである場合 [1]
KEEPALIVE（MAC アドレス、SNAP カプセル化、LLC、Org ID、または HDLC パケット）	レート制限	–	–
イーサネット Connectivity Fault Management（CFM）	ポリサーは割り当てられない	CFM がグローバルにイネーブルである場合、スロットル ポリサーがすべてのポートに割り当てられる。CFM がグローバルにディセーブルである場合、ヌル ポリサーがすべてのポートに割り当てられる。	–

1. レイヤ 2 プロトコル トンネリングが任意のポートの任意のプロトコルに対してイネーブルである場合に、レイヤ 2 プロトコル トラフィックがレート制限されます。

スイッチは、CPU 保護のため、自動的に 27 のコントロール プレーンのセキュリティ ポリサーを割り当てます。システムの起動時に、0 ～ 26 に番号付けされたポートごとに 1 つのポリサーを割り当てます。ポートに割り当てられたポリサーは、ポートに着信したプロトコル パケットがレート制限されるか廃棄されるかを決定します。ME 3400E-24TS スイッチ上では、ポリサー 26 は、廃棄ポリサーを意味するグローバル ポリサーです。いずれのポートでも、26 として示されるすべてのトラフィック タイプは廃棄されます。ポリサー 0 ～ 25 はレート制限ポリサーで、プロトコルのポートに割り当てられます。ポリサー 0 ～ 23 はファスト イーサネット ポート 1 ～ 24 の論理 ID で、ポリサー 24 および 25 はそれぞれ、ギガビット イーサネット ポート 1 および 2 を意味します。ポリサー 255 は、ポリサーがプロトコルに割り当てられないことを意味します。

ME 3400EG-12CS および ME 34000EG-2CS スイッチの場合、ポリサー 4 は、廃棄ポリサーを意味します。ポート上で 4 として示されるトラフィック タイプは破棄されます。ポリサー 0 ～ 3 はレート制限ポリサーで、プロトコルのポートに割り当てられます。

インターフェイス上のプロトコルに割り当てられるポリサー アクションを確認するには、**show platform policer cpu interface** *interface-id* 特権 EXEC コマンドを入力します。

（注）　特に指示の無い場合、例は ME 3400E-24TS スイッチのものです。

次に、UNI でのデフォルト ポリサー設定を示します。ポートがファスト イーサネット 1 であるため、レート制限されるプロトコルの ID は 0 で、ファスト イーサネット ポート 5 には、ID 4 が表示されます。*Policer Index* は、特定のプロトコルを意味します。ASIC 番号は、ポリサーが異なる ASIC 上にある場合を表します。

UNI では、STP、CDP、LLDP、LACP、および PAgP がサポートされていないので、これらのパケットは破棄されます（物理ポリサー 26）。ENI でもこれらのプロトコルはデフォルトでディセーブルになっていますが、イネーブルにすることが可能です。ENI 上でイネーブルにすると、制御パケットがレート制限され、レート制限ポリサーが、これらのプロトコルに割り当てられます（物理ポリサー 22）。

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/1
STP                                  1            26             0
LACP                                 2            26             0
```

```
8021X                                3            26            0
RSVD_STP                             4            26            0
PVST_PLUS                            5            26            0
CDP                                  6            26            0
LLDP                                 7            26            0
DTP                                  8            26            0
UDLD                                 9            26            0
PAGP                                10            26            0
VTP                                 11            26            0
CISCO_L2                            12            26            0
KEEPALIVE                           13             0            0
CFM                                 14           255            0
SWITCH_MAC                          15            26            0
SWITCH_ROUTER_MAC                   16            26            0
SWITCH_IGMP                         17             0            0
SWITCH_L2PT                         18            26            0
```

次に、制御プロトコルがインターフェイス上でイネーブルになったときに ENI に割り当てられるポリサーの例を示します。値 22 は、プロトコル パケットが、そのプロトコルに関してレート制限されていることを示しています。プロトコルがイネーブルになっていない場合、デフォルトは UNI の場合と同じです。

```
Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=========================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=========================================================================
Fa0/23
STP                                 1             26            0
LACP                                2             22            0
8021X                               3             26            0
RSVD_STP                            4             26            0
PVST_PLUS                           5             26            0
CDP                                 6             22            0
LLDP                                7             26            0
DTP                                 8             26            0
UDLD                                9             26            0
PAGP                               10             26            0
VTP                                11             26            0
CISCO_L2                           12             22            0
KEEPALIVE                          13             22            0
CFM                                14            255            0
SWITCH_MAC                         15             26            0
SWITCH_ROUTER_MAC                  16             26            0
SWITCH_IGMP                        17             22            0
SWITCH_L2PT                        18             22            0
```

次に、ME 3400EG-12CS または ME 34000EG-2CS スイッチ上でのレート制限の例を示します。値 1 は、プロトコル パケットが、そのプロトコルに関してレート制限されていることを示しています。

```
Switch #show platform policer cpu interface gigabitethernet 0/2
Policers assigned for CPU protection
=========================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=========================================================================
Gi0/2
STP                                 1              4            0
LACP                                2              4            0
8021X                               3              4            0
RSVD_STP                            4              1            0
PVST_PLUS                           5              4            0
```

```
CDP                                6            4            0
LLDP                               7            4            0
DTP                                8            4            0
UDLD                               9            4            0
PAGP                              10            4            0
VTP                               11            4            0
CISCO_L2                          12            4            0
KEEPALIVE                         13            1            0
CFM                               14          255            0
SWITCH_MAC                        15            4            0
SWITCH_ROUTER_MAC                 16            4            0
SWITCH_IGMP                       17            1            0
SWITCH_L2PT                       18            4            0
```

次に、NNI に割り当てられるデフォルト ポリサーを示します。ほとんどのプロトコルでは、NNI にポリサーが割り当てられません。値 255 は、プロトコルのポートにポリサーが割り当てられないことを意味します。

```
Switch #show platform policer cpu interface gigabitethernet 0/1
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Gi0/1
STP                                1           255            0
LACP                               2           255            0
8021X                              3           255            0
RSVD_STP                           4           255            0
PVST_PLUS                          5           255            0
CDP                                6           255            0
LLDP                               7           255            0
DTP                                8           255            0
UDLD                               9           255            0
PAGP                              10           255            0
VTP                               11           255            0
CISCO_L2                          12           255            0
KEEPALIVE                         13           255            0
CFM                               14           255            0
SWITCH_MAC                        15           255            0
SWITCH_ROUTER_MAC                 16           255            0
SWITCH_IGMP                       17           255            0
SWITCH_L2PT                       18           255            0
```

コントロール プレーンのセキュリティ設定

CPU 保護は、デフォルトでイネーブルになっており、CPU ポリサーは事前に割り当てられています。CPU 保護をディセーブルにするには、**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、再度イネーブルにするには、**policer cpu uni all** グローバル コンフィギュレーション コマンドを入力します。CPU 保護をディセーブルまたはイネーブルにする場合、設定が反映される前に **reload** 特権 EXEC コマンドを入力することによって、スイッチをリロードする必要があります。

CPU 保護がイネーブルになっている場合、ポートごとに設定できるポリサーは 45 だけです。CPU 保護をディセーブルにすると、ポートごとに最大 64 のポリサーを設定できます。CPU 保護をディセーブルにする際はこれらの制限事項について注意してください。

- CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上に 62）を、class-default に対して 1 つのポリサーを設定できます。

- Cisco ME 3400EG-12CS スイッチ上では、ハードウェア制限のため、64 のポート単位 VLAN 単位ポリサーを割り当てられるポート数は最大 6 です。6 を超えるポート単位 VLAN 64 ポリサー ポリシー マップを付加しようとすると、*VLAN labels exceeded* エラー メッセージが出力されて、その付加は失敗します。
- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

設定できるのは、レート制限しきい値だけです。設定されたしきい値は、すべての UNI および ENI 上のすべてのサポート対象制御プロトコルに適用されます。また、プロトコルが ENI 上でイネーブルになっている場合、STP、CDP、LLDP、LACP、および PAgP にも適用されます。

（注） 通常のレイヤ 2 動作時には、UNI または ENI からスイッチに対して ping を実行できません。この制限事項は、NNI には適用されません。テスト状況で ping をイネーブルにする方法については、「ping の使用」（P.46-10）を参照してください。

CPU 保護用にしきい値レートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**policer cpu uni** *rate*	CPU 保護のポリシングしきい値レートを設定します。指定できる範囲は 8000 ～ 409500 b/s です。設定されない場合は、デフォルトの 160000 b/s となります。 **（注）** 設定されたレートは、すべての UNI および ENI 上のすべてのサポート対象およびイネーブルにされた制御プロトコルに適用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show policer cpu uni-eni rate**	設定された CPU ポリサー レートを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのしきい値レートに戻るには、**no policer cpu uni** 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。CPU 保護をディセーブルにするには、**no policer cpu uni all** 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、スイッチをリロードします。

次に、CPU 保護しきい値を 10000 b/s に設定し、その設定を確認する例を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
Switch# show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 10000 bps
```

次に、CPU 保護がディセーブルになっているときの show コマンドの出力例を示します。

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

コントロール プレーンのセキュリティのモニタリング

スイッチまたはインターフェイス上のコントロール プレーンのセキュリティ設定および統計情報は、モニタリングできます。また、これらの統計情報は、表 33-2 に示す特権 EXEC コマンドを使用することによって、いつでも消去できます。このコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

表 33-2　コントロール プレーンのセキュリティをモニタリングするためのコマンド

コマンド	目的
clear policer cpu uni-eni counters {**classification** | **drop**}	機能ごとにコントロール プレーンのすべての統計情報を消去するか（**classification**）、またはコントロール プレーン ポリサーで維持されるすべての統計情報を消去します（**drop**）。
debug platform policer cpu uni-eni	コントロール プレーン ポリサーのデバッグをイネーブルにします。このコマンドにより、CPU 保護に対して何らかの変更があった場合に、情報メッセージが表示されます。
show platform policer cpu {**classification** | **interface** *interface-id*}	コントロール プレーンのポリサー情報を表示します。 • **classification**：分類の統計情報を示します。 • **interface** *interface-id*：指定されたインターフェイスのポリサー インデックスを示します。

show policer cpu uni-eni {**drop** [**interface** *interface-id*] | **rate**}	スイッチの CPU ポリサー情報を表示します。
	• **drop** [**interface** *interface-id*] ：すべてのインターフェイスまたは指定したインターフェイスの廃棄フレーム数を示します。
	• **rate**：CPU ポリサーに設定されたしきい値レートを示します。
	CPU 保護がディセーブルになっている場合、次のメッセージが出力内に表示されます。
	`Switch# show policer cpu uni drop`
	`CPU Protection feature is not enabled`