CHAPTER 24

QoS の設定

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に割り込みされ、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、遅延と呼ばれます。音声やビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。Quality of Service（QoS）機能を使用すると、重要なトラフィックのプライオリティを高くし、帯域幅の過剰な使用を防ぎ、ネットワーク ボトルネックを管理してパケットのドロップを防止できます。

この章では、QoS ポリシーを適用する方法について説明します。次の項目を取り上げます。

- 「QoS の概要」（P.24-1）
- 「QoS のライセンス要件」（P.24-5）
- 「注意事項と制約事項」（P.24-5）
- 「QoS の設定」（P.24-6）
- 「QoS のモニタリング」（P.24-16）
- 「QoS の機能履歴」（P.24-19）

QoS の概要

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

（注） QoS は、シングル コンテキスト モードでのみ使用できます。

この項では、セキュリティ アプライアンス でサポートされる QoS 機能について説明します。次の項目を取り上げます。

- 「サポートされる QoS 機能」（P.24-2）
- 「トークン バケットとは」（P.24-2）
- 「ポリシングに関する情報」（P.24-3）
- 「プライオリティ キューイングに関する情報」（P.24-3）
- 「トラフィック シェーピングに関する情報」（P.24-4）
- 「DSCP および DiffServ の維持」（P.24-5）

サポートされる QoS 機能

セキュリティ アプライアンスは、次の QoS の機能をサポートしています。

- ポリシング：特定のフローがネットワーク帯域幅を大量に使用するのを防ぐため、フローごとの最大使用帯域幅を制限できます。詳細については、「ポリシングに関する情報」（P.24-3）を参照してください。
- プライオリティ キューイング：Voice over IP（VoIP）のような遅延を許されない重要なトラフィックについて、トラフィックを Low Latency Queuing（LLQ; 低遅延キューイング）に指定することで、常に他のトラフィックより先に送信できます。詳細については、「プライオリティ キューイングに関する情報」（P.24-3）を参照してください。
- トラフィック シェーピング：ファスト イーサネットでのセキュリティ アプライアンスなどのように高速でパケットを送信するデバイスがあり、それがケーブル モデムのような低速デバイスに接続されている場合、ケーブル モデムがボトルネックになって頻繁にパケットがドロップされます。異なる速度の回線を含むネットワークを管理するには、低めの固定レートでパケットを送信するようにセキュリティ アプライアンスを設定できます。詳細については、「トラフィック シェーピングに関する情報」（P.24-4）を参照してください。

トークン バケットとは

トークン バケットは、フロー内のデータを規制するデバイスの管理に使用されます。規制機能としては、たとえばトラフィック ポリシング機能やトラフィック シェーパーなどがあります。トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。むしろ、トークン バケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。

トークン バケットは、転送レートの正式な定義です。トークン バケットには、バースト サイズ、平均レート、時間間隔という 3 つのコンポーネントがあります。平均レートは通常 1 秒間のビット数で表されますが、次のような関係によって、任意の 2 つの値を 3 番目の値から求めることができます。

平均レート = バースト サイズ / 時間間隔

これらの用語の定義は次のとおりです。

- 平均レート：Committed Information Rate（CIR; 認定情報レート）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バースト サイズ：Committed Burst（Bc; 認定バースト）サイズとも呼ばれ、スケジューリングに関する問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのビット数またはバイト数で指定します （トラフィック シェーピングの場合はバーストごとのビット数を指定し、ポリシングの場合はバーストごとのバイト数を指定します）。
- 時間間隔：測定間隔とも呼ばれ、バーストごとの時間を秒単位で指定します。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信するのに十分なトークンがバケット内にない場合、パケットはバケットに十分なトークンが溜まるまで待機するか（トラフィック シェーピングの場合）、または廃棄されるかダウンとマークされます（ポリシングの場合）。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

トラフィック シェーピングに使用されるトークン バケット メカニズムは、トークン バケットとデータ バッファまたはキューの両方を持っています。データ バッファを持たない場合は、ポリシング機能になります。トラフィック シェーピングの場合、到着したパケットですぐに送信できないものは、データ バッファで遅延されます。

トラフィック シェーピングでは、トークン バケットはバースト性を許可する一方で、それを抑制します。トラフィック シェーピングは、トークン バケットの容量を時間間隔で割った値に設定されているトークン バケットへのトークンの格納レートを加えた値より速くフローが送信しないように、バースト性を抑制します。次の式を参照してください。

（ビット単位のトークン バケット容量 / 秒単位の時間間隔）+ 設定されている bps 単位のレート = bps 単位の最大フロー速度

このようなバースト性抑制方法は、長期的な送信レートが設定されているバケットへのトークン格納レートを超えないことも保証します。

ポリシングに関する情報

ポリシングは、設定した最大レート（ビット/秒）を超えるトラフィックが発生しないようにして、1 つのトラフィック フローまたはクラスが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、セキュリティ アプライアンスは超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

プライオリティ キューイングに関する情報

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

セキュリティ アプライアンス は、次の 2 つのタイプのプライオリティ キューイングをサポートしています。

- 標準プライオリティ キューイング：標準プライオリティ キューイングはインターフェイスの LLQ プライオリティ キューを使用しますが（「インターフェイス用の標準プライオリティ キューの設定」（P.24-8）を参照）、他のすべてのトラフィックは「ベスト エフォート」キューに入れられます。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。
- 階層型プライオリティ キューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キューがイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。階層型プライオリティ キューイングについては、次のガイドラインを参照してください。
  - プライオリティ パケットは常にシェープ キューの先頭に格納されるので、常に他の非プライオリティ キュー パケットよりも前に送信されます。
  - プライオリティ トラフィックの平均レートがシェープ レートを超えない限り、プライオリティ パケットがシェープ キューからドロップされることはありません。
  - IPsec-encrypted パケットの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。

- プライオリティ トラフィック分類では、IPsec-over-TCP はサポートされません。

トラフィック シェーピングに関する情報

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延の原因になる可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。

- トラフィック シェーピングは、物理インターフェイスのすべての発信トラフィック、または ASA 5505 の場合は VLAN 上のすべての発信トラフィックに適用する必要があります。特定のタイプのトラフィックにはトラフィック シェーピングを設定できません。
- トラフィック シェーピングは、パケットがインターフェイスで送信する準備ができている場合に実装されます。そのため、レートの計算は、IPSec ヘッダーや L2 ヘッダーなどの潜在的なすべてのオーバーヘッドを含む、送信されるパケットの実際のサイズに基づいて実行されます。
- シェーピングされるトラフィックには、through-the-box トラフィックと from-the-box トラフィックの両方が含まれます。
- シェープ レートの計算は、標準トークン バケット アルゴリズムに基づいて行われます。トークン バケットのサイズは、バースト サイズの値の 2 倍です。「トークン バケットとは」（P.24-2）を参照してください。
- バースト性のトラフィックが指定されたシェープ レートを超えると、パケットはキューに入れられて、後で送信されます。次に、シェープ キューに関するいくつかの特性を示します（階層型プライオリティ キューイングについては、「プライオリティ キューイングに関する情報」（P.24-3）を参照してください）。
  - キューのサイズは、シェープ レートに基づいて計算されます。キューは、1500 バイトのパケットとして 200 ミリ秒に相当するシェープ レート トラフィックを保持できます。最小キュー サイズは 64 です。
  - キューの制限に達すると、パケットはキューの末尾からドロップされます。
  - OSPF Hello パケットなどの一部の重要なキープアライブ パケットは、ドロップされません。
  - 時間間隔は、*time_interval* = *burst_size* / *average_rate* によって求められます。時間間隔が長くなるほど、シェープ トラフィックのバースト性は高くなり、リンクのアイドル状態が長くなる可能性があります。この効果は、次のような誇張した例を使うとよく理解できます。

    平均レート = 1000000

    バースト サイズ = 1000000

    この例では、時間間隔は 1 秒であり、これは、100 Mbps の FE リンクでは 1 Mbps のトラフィックを時間間隔 1 秒の最初の 10 ミリ秒内にバースト送信できることを意味し、残りの 990 ミリ秒間はアイドル状態になって、次の時間間隔になるまでパケットを送信できません。したがって、音声トラフィックのように遅延が問題になるトラフィックがある場合は、バースト サイズを平均レートと比較して小さくし、時間間隔を短くする必要があります。

QoS 機能の相互作用のしくみ

セキュリティ アプライアンスで必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能をセキュリティ アプライアンスに設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。たとえば、グローバル ポリシーに標準プライオリティ キューイングを設定して、特定のインターフェイスにトラフィック シェーピングを設定する場合、最後に設定した機能は拒否されます。これは、グローバル ポリシーがインターフェイス ポリシーと重複するためです。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定はセキュリティ アプライアンスでは制限されていません。

DSCP および DiffServ の維持

- DSCP のマーキングは、セキュリティ アプライアンスを通過するすべてのトラフィックで維持されます。
- セキュリティ アプライアンスは分類済みのトラフィックをローカルにマーク付けまたは再マーク付けすることはなく、すべてのパケットの緊急転送（EF）DSCP ビットを使用して、「優先的な」処理が必要かどうかを判断し、必要なパケットは LLQ に誘導します。
- 搬送中に QoS を適用できるように（QoS トンネル事前分類）、パケットの DiffServ マーキングはサービス プロバイダーのバックボーンを通過するときに維持されます。

QoS 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。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドラインと制限事項

- トラフィック シェーピングの場合は、**class-default** クラス マップだけを使用できます。このクラス マップはセキュリティ アプライアンスによって自動的に作成され、すべてのトラフィックを照合します。
- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- 階層型プライオリティ キューイングの場合、暗号化された VPN トラフィックについては、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。トンネル グループを照合することはできません。
- 階層型プライオリティ キューイングの場合、IPsec-over-TCP トラフィックはサポートされません。
- 同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。
- 標準プライオリティ キューイングの場合、キューは物理インターフェイス用または ASA 5505 の VLAN 用に設定する必要があります。
- 10 ギガビット イーサネット インターフェイスには、標準プライオリティ キューを作成できません。高帯域幅のインターフェイスには、プライオリティ キューイングは必要ありません。

QoS の設定

この項では、次のトピックについて取り上げます。

- 「標準プライオリティ キューのプライオリティ キューおよび TX リング制限の決定」（P.24-7）
- 「インターフェイス用の標準プライオリティ キューの設定」（P.24-8）
- 「標準プライオリティ キューイングとポリシング用のサービス ルールの設定」（P.24-10）
- 「トラフィック シェーピングと階層型プライオリティ キューイング用のサービス ルールの設定」（P.24-13）

標準プライオリティ キューのプライオリティ キューおよび TX リング制限の決定

プライオリティ キューおよび TX リング制限を決定するには、次のワークシートを使用します。

表 24-1 は、プライオリティ キューのサイズを計算する方法を示しています。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるには、「インターフェイス用の標準プライオリティ キューの設定」（P.24-8）に従ってキューのバッファ サイズを調節します。

表 24-1　キュー制限のワークシート

ステップ 1	_____ *アウトバウンド帯域幅（Mbps または Kbps）*[1]	Mbps	x	**125**	=	_____ *バイト数/ミリ秒*		
		Kbps	x	**.125**	=	_____ *バイト数/ミリ秒*		
ステップ 2	_____ *ステップ 1 からのバイト数/ミリ秒*	÷	_____ *平均パケット サイズ（バイト）*[2]	x	_____ *遅延（ミリ秒）*[3]	=	_____ *キュー制限（パケット数）*	

1. たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
2. この値はコーデックまたはサンプリング サイズから決定します。たとえば、VoIP over VPN の場合は、160 バイトなどを使用します。使用するサイズがわからない場合は、256 バイトにすることをお勧めします。
3. 遅延はアプリケーションによって決まります。たとえば、VoIP の場合の推奨される最大遅延は 200 ミリ秒です。使用する遅延がわからない場合は、500 ミリ秒にすることをお勧めします。

表 24-2 は、TX リング制限を計算する方法を示しています。この制限により、イーサネット送信ドライバが受け入れるパケットの最大数が決まります。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

表 24-2　TX リング制限のワークシート

ステップ 1	_____ *アウトバウンド帯域幅（Mbps または Kbps）[1]*	Mbps	x	**125**	=	_____ *バイト数/ミリ秒*		
		Kbps	x	**0.125**	=	_____ *バイト数/ミリ秒*		
ステップ 2	_____ *ステップ 1 からのバイト数/ミリ秒*		÷	_____ *最大パケット サイズ（バイト）[2]*	x	_____ *遅延（ミリ秒）[3]*	=	_____ *TX リング制限（パケット数）*

1. たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
2. 通常、タグ付けされたイーサネットの最大サイズは 1538 バイトまたは 1542 バイトです。ジャンボ フレームを許可する場合（プラットフォームでサポートされている場合）、パケット サイズはさらに大きくなる場合があります。
3. 遅延はアプリケーションによって決まります。たとえば、VoIP のジッタを制御するには、20 ミリ秒を使用します。

インターフェイス用の標準プライオリティ キューの設定

物理インターフェイスでトラフィックに対する標準プライオリティ キューイングをイネーブルにする場合は、各インターフェイスでプライオリティ キューを作成する必要もあります。各物理インターフェイスは、プライオリティ トラフィック用と、他のすべてのトラフィック用に、2 つのキューを使用します。他のトラフィックについては、必要に応じてポリシングを設定できます。

（注） トラフィック シェーピングでの階層型プライオリティ キューイングには、標準プライオリティ キューは必要ありません。詳細については、「プライオリティ キューイングに関する情報」（P.24-3）を参照してください。

制約事項

10 ギガビット イーサネット インターフェイスには、プライオリティ キューを作成できません。高帯域幅のインターフェイスには、プライオリティ キューイングは必要ありません。

手順の詳細

	コマンド	目的
ステップ 1	**priority-queue** *interface_name* **例：** `hostname(config)# priority-queue inside`	プライオリティ キューを作成します。*interface_name* 引数には、プライオリティ キューをイネーブルにする物理インターフェイスの名前、または ASA 5505 の場合は VLAN インターフェイス名を指定します。
ステップ 2	**queue-limit** *number_of_packets* **例：** `hostname(config-priority-queue)# queue-limit 260`	プライオリティ キューのサイズを変更します。デフォルトのキューの制限は 1024 パケットです。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。 **queue-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **queue-limit ?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。 指定した **queue-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。
ステップ 3	**tx-ring-limit** *number_of_packets* **例：** `hostname(config-priority-queue)# tx-ring-limit 3`	プライオリティ キューの深さを指定します。デフォルトの tx-ring-limit は 128 パケットです。このコマンドは、イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。 **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **tx-ring-limit ?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。 指定した **tx-ring-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

例

次の例は、デフォルトの queue-limit と tx-ring-limit を使用して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
```

次の例は、queue-limit を 260 パケット、tx-ring-limit を 3 に設定して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

標準プライオリティ キューイングとポリシング用のサービス ルールの設定

同じポリシー マップ内の異なるクラス マップに対し、標準プライオリティ キューイングとポリシングを設定できます。有効な QoS 設定については、「QoS 機能の相互作用のしくみ」（P.24-4）を参照してください。

ポリシー マップを作成するには、次の手順を実行します。

制約事項

- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- 同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。

ガイドライン

- プライオリティ トラフィックの場合は、遅延が問題になるトラフィックだけを指定します。
- ポリシング トラフィックの場合は、他のすべてのトラフィックをポリシングすることも、トラフィックを特定のタイプに制限することもできます。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *priority_map_name* **例：** `hostname(config)# class-map priority_traffic`	プライオリティ トラフィックの場合、プライオリティ キューイングを実行するトラフィックを識別するためのクラス マップを作成します。
ステップ 2	**match** *parameter* **例：** `hostname(config-cmap)# match access-list priority`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの識別（レイヤ 3/4 クラス マップ）」（P.21-4）を参照してください。
ステップ 3	**class-map** *policing_map_name* **例：** `hostname(config)# class-map policing_traffic`	ポリシング トラフィックの場合、ポリシングを実行するトラフィックを識別するためのクラス マップを作成します。
ステップ 4	**match** *parameter* **例：** `hostname(config-cmap)# match access-list policing`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの識別（レイヤ 3/4 クラス マップ）」（P.21-4）を参照してください。
ステップ 5	**policy-map** *name* **例：** `hostname(config)# policy-map QoS_policy`	ポリシー マップを追加または編集します。

	コマンド	目的
ステップ 6	**class** *priority_map_name* **例：** hostname(config-pmap)# class priority_class	ステップ 1 で優先トラフィック用に作成したクラス マップを識別します。
ステップ 7	**priority** **例：** hostname(config-pmap-c)# priority	クラスのプライオリティ キューイングを設定します。
ステップ 8	**class** *policing_map_name* **例：** hostname(config-pmap)# class policing_class	ステップ 3 でポリシング設定トラフィック用に作成したクラス マップを識別します。
ステップ 9	**police** {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]] **例：** hostname(config-pmap-c)# police output 56000 10500	クラスのポリシングを設定します。次のオプションを参照してください。 • *conform-burst argument*：適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。 • **conform-action**：レートが *conform_burst* 値を下回ったときに実行するアクションを設定します。 • *conform-rate*：このトラフィック フローのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。 • **drop**：パケットをドロップします。 • **exceed-action**：レートが *conform-rate* 値～ *conform-burst* 値の範囲にあるときに実行するアクションを設定します。 • **input**：入力方向のトラフィック フローのポリシングをイネーブルにします。 • **output**：出力方向のトラフィック フローのポリシングをイネーブルにします。 • **transmit**：パケットを送信します。
ステップ 10	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy QoS_policy interface inside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

例

例 24-1　VPN トラフィックのクラス マップの例

次の例で、**class-map** コマンドは tcp_traffic というアクセス リストを使用して、すべての非トンネル TCP トラフィックを分類します。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

次の例では、より限定的な一致基準を使用して、特定のセキュリティ関連のトンネル グループにトラフィックを分類します。これらの特定の一致基準では、トラフィックが特定のトンネルに分類されるために、最初の一致特性としてトンネルグループ（この例では、すでに定義されている Tunnel-Group-1）に一致する必要があります。次に、別の照合行でトラフィックを分類できます（IP DiffServ コード ポイント、緊急転送）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

次の例では、**class-map** コマンドはトンネル トラフィックと非トンネル トラフィックの両方をトラフィック タイプに従って分類します。

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

次の例は、クラス トラフィックがトンネルとして指定されておらず、トンネルを*通過する*場合に、トンネル内のフローをポリシングする方法を示します。この例では、192.168.10.10 がリモート トンネルのプライベート側のホスト マシンのアドレスで、アクセス リストの名前は「host-over-l2l」です。クラスマップ（名前は「host-specific」）を作成すると、LAN-to-LAN 接続によるトンネルのポリシングの前に、「host-specific」クラスをポリシングできます。この例では、トンネルの前で「host-specific」トラフィックのレートが制限され、次にトンネルのレートが制限されます。

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

次の例は、前の項で作成したコンフィギュレーションで構築されています。前の例と同様に、tcp_traffic と TG1-voice という 2 つのクラスマップがあります。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

第 3 のクラス マップを追加することで、次のように、トンネルおよび非トンネル QoS ポリシーを定義する基本が提供されます。トンネルおよび非トンネル トラフィックに対する単純な QoS ポリシーが作成され、クラス TG1-voice のパケットが低遅延キューに割り当てられ、tcp_traffic および TG1-best-effort フローにレート制限が設定されます。

例 24-2　　プライオリティとポリシングの例

この例では、tcp_traffic クラスのトラフィックの最大レートは 56,000 ビット/秒で、最大バースト サイズは 10,500 バイト/秒です。TC1-BestEffort クラスの最大レートは 200,000 ビット/秒で、最大バーストは 37,500 バイト/秒です。TC1-voice クラスのトラフィックは、プライオリティ クラスに属しているため、最大速度またはバースト レートでポリシングされません。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

トラフィック シェーピングと階層型プライオリティ キューイング用のサービス ルールの設定

インターフェイスのすべてのトラフィックにトラフィック シェーピングを設定でき、必要に応じて遅延が問題になるトラフィックのサブセットに階層型プライオリティ キューイングを設定できます。

この項では、次のトピックについて取り上げます。

- 「(任意）階層型プライオリティ キューイング ポリシーの設定」（P.24-13）
- 「サービス ルールの設定」（P.24-14）

（任意）階層型プライオリティ キューイング ポリシーの設定

必要に応じて、遅延が問題になるトラフィックのサブセットにプライオリティ キューイングを設定できます。

ガイドライン

- プライオリティ キューイングには、パケットの並べ替えという副作用があります。IPsec パケットでは、アンチ リプレイ ウィンドウ内にない不連続パケットにより、警告 syslog メッセージが生成されます。このような警告は、プライオリティ キューイングの場合は不正アラームです。不正アラームが発生しないように、IPsec のリプレイ攻撃防止ウィンドウのサイズを設定できます。

『*Cisco Security Appliance Command Reference*』の **crypto ipsec security-association replay** コマンドに関する説明を参照してください。階層型プライオリティ キューイングについては、インターフェイスにプライオリティ キューを作成する必要はありません。

制約事項

- 階層型プライオリティ キューイングの場合、暗号化された VPN トラフィックについては、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。トンネル グループを照合することはできません。
- 階層型プライオリティ キューイングの場合、IPsec-over-TCP トラフィックはサポートされません。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *priority_map_name* **例：** `hostname(config)# class-map priority_traffic`	階層型プライオリティ キューイングの場合、プライオリティ キューイングを実行するトラフィックを識別するためのクラス マップを作成します。
ステップ 2	**match** *parameter* **例：** `hostname(config-cmap)# match access-list priority`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの識別（レイヤ 3/4 クラス マップ）」（P.21-4）を参照してください。暗号化された VPN トラフィックの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。トンネル グループを照合することはできません。
ステップ 3	**policy-map** *priority_map_name* **例：** `hostname(config)# policy-map priority-sub-policy`	ポリシー マップを作成します。
ステップ 4	**class** *priority_map_name* **例：** `hostname(config-pmap)# class priority-sub-map`	ステップ 1 で作成したクラス マップを指定します。
ステップ 5	**priority** **例：** `hostname(config-pmap-c)# priority`	プライオリティ キューイング アクションをクラス マップに適用します。 **（注）** このポリシーは、まだアクティブになっていません。シェーピング ポリシーの一部として、このポリシーをアクティブにする必要があります。「サービス ルールの設定」（P.24-14）を参照してください。

サービス ルールの設定

トラフィック シェーピングおよびオプションの階層型プライオリティ キューイングを設定するには、次の手順を実行します。

制約事項

- トラフィック シェーピングの場合は、**class-default** クラス マップだけを使用できます。このクラス マップはセキュリティ アプライアンスによって自動的に作成され、すべてのトラフィックを照合します。
- 同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。有効な QoS 設定については、「QoS 機能の相互作用のしくみ」（P.24-4）を参照してください。
- グローバル ポリシーではトラフィック シェーピングを設定できません。

手順の詳細

	コマンド	目的
ステップ 1	**policy-map** *name* **例：** `hostname(config)# policy-map shape_policy`	ポリシー マップを追加または編集します。このポリシー マップは、階層型プライオリティ キューイング マップとは異なるものであることが必要です。
ステップ 2	**class class-default** **例：** `hostname(config-pmap)# class class-default`	トラフィック シェーピングのすべてのトラフィックを識別します。指定できるのは **class-default** クラス マップだけです。セキュリティ アプライアンス ではトラフィック シェーピングの場合はすべてのトラフィックを照合する必要があるので、このクラス マップは **match any** と定義されています。
ステップ 3	**shape average** *rate* [*burst_size*] **例：** `hostname(config-pmap-c)# shape average 70000 4000`	トラフィック シェーピングをイネーブルにします。**average** *rate* 引数は、特定の固定時間間隔に対するトラフィックの平均レートを 1 秒間のビット数で設定します。値の範囲は 64000 ～ 154400000 です。8000 の倍数の値を指定します。時間間隔を計算する方法の詳細については、「トラフィック シェーピングに関する情報」（P.24-4）を参照してください。 *burst_size* 引数は、特定の固定時間間隔に送信できる平均バースト サイズをビット単位で指定します。値の範囲は 2048 ～ 154400000 です。128 の倍数の値を指定します。*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット / 秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。
ステップ 4	（任意） **service-policy** *priority_policy_map_name* **例：** `hostname(config-pmap-c)# service-policy priority-sub-policy`	階層型プライオリティ キューイングを設定します。*priority_policy_map_name* は、「（任意）階層型プライオリティ キューイング ポリシーの設定」（P.24-13）で優先トラフィックに対して作成したポリシー マップです。
ステップ 5	**service-policy** *policymap_name* **interface** *interface_name* **例：** `hostname(config)# service-policy shape-policy interface inside`	インターフェイスでシェーピング ポリシー マップをアクティブにします。

例

次の例では、外部インターフェイスでトラフィック シェーピングをイネーブルにし、トラフィックを 2 Mbps に制限しています。プライオリティ キューイングは、DSCP EF および AF13 でタグ付けされている VoIP トラフィックと、IKE トラフィックに対してイネーブルになっています。

```
hostname(config)# access-list ike permit udp any any eq 500
hostname(config)# class-map ike
hostname(config-cmap)# match access-list ike

hostname(config-cmap)# class-map voice_traffic
hostname(config-cmap)# match dscp EF AF13

hostname(config-cmap)# policy-map qos_class_policy
hostname(config-pmap)# class voice_traffic
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class ike
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map qos_outside_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape average 2000000 16000
hostname(config-pmap-c)# service-policy qos_class_policy

hostname(config-pmap-c)# service-policy qos_outside_policy interface outside
```

QoS のモニタリング

この項では、次のトピックについて取り上げます。

- 「QoS ポリシング統計情報の表示」（P.24-16）
- 「QoS 標準プライオリティ統計情報の表示」（P.24-17）
- 「QoS シェーピング統計情報の表示」（P.24-17）
- 「QoS 標準プライオリティ キュー統計情報の表示」（P.24-18）

QoS ポリシング統計情報の表示

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy** コマンドと **police** キーワードを使用します。

```
hostname# show service-policy police
```

次に、**show service-policy police** コマンドの出力例を示します。

```
hostname# show service-policy police

Global policy:
    Service-policy: global_fw_policy

Interface outside:
    Service-policy: qos
        Class-map: browse
            police Interface outside:
                cir 56000 bps, bc 10500 bytes
                conformed 10065 packets, 12621510 bytes; actions: transmit
                exceeded 499 packets, 625146 bytes; actions: drop
```

```
            conformed 5600 bps, exceed 5016 bps
        Class-map: cmap2
            police Interface outside:
                cir 200000 bps, bc 37500 bytes
                conformed 17179 packets, 20614800 bytes; actions: transmit
                exceeded 617 packets, 770718 bytes; actions: drop
                conformed 198785 bps, exceed 2303 bps
```

QoS 標準プライオリティ統計情報の表示

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy** コマンドと **priority** キーワードを使用します。

```
hostname# show service-policy priority
```

次に、**show service-policy priority** コマンドの出力例を示します。

```
hostname# show service-policy priority
Global policy:
    Service-policy: global_fw_policy
Interface outside:
    Service-policy: qos
        Class-map: TG1-voice
            Priority:
                Interface outside: aggregate drop 0, aggregate transmit 9383
```

（注） 「aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

QoS シェーピング統計情報の表示

shape コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy** コマンドと **shape** キーワードを使用します。

```
hostname# show service-policy shape
```

次に、**show service-policy shape** コマンドの出力例を示します。

```
hostname# show service-policy shape
Interface outside
  Service-policy: shape
    Class-map: class-default

      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

      shape (average) cir 2000000, bc 8000, be 8000
```

次に、**show service policy shape** コマンドの出力例を示します。この例には、階層型プライオリティ ポリシーと関連する統計情報を呼び出す **shape** コマンドおよび **service-policy** コマンドを含むサービス ポリシーが含まれます。

```
hostname# show service-policy shape

Interface outside:
```

```
Service-policy: shape
    Class-map: class-default

      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

      shape (average) cir 2000000, bc 16000, be 16000

      Service-policy: voip
        Class-map: voip

          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: class-default

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

QoS 標準プライオリティ キュー統計情報の表示

インターフェイスのプライオリティ キュー統計情報を表示するには、特権 EXEC モードで **show priority-queue statistics** コマンドを実行します。ベストエフォート（BE）キューと低遅延キュー（LLQ）の両方の統計情報が表示されます。次の例に、test という名前のインターフェイスに対する **show priority-queue statistics** コマンドの使用方法とコマンド出力を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
hostname#
```

この統計情報レポートの項目の意味は、次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューに入れられたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。

QoS の機能履歴

表 24-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 24-3　QoS の機能履歴

機能名	プラットフォーム リリース	機能情報
プライオリティ キューイングとポリシング	7.0(1)	QoS プライオリティ キューイングとポリシングが導入されました。 **priority-queue**、**queue-limit**、**tx-ring-limit**、**priority**、**police**、**show priority-queue statistics**、**show service-policy police**、**show service-policy priority**、**show running-config priority-queue**、**clear configure priority-queue** の各コマンドが導入されました。
シェーピングおよび階層型プライオリティ キューイング	7.2(4)/8.0(4)	QoS シェーピングおよび階層型プライオリティ キューイングが導入されました。 **shape**、**show service-policy shape** の各コマンドが導入されました。