PureFlow GS1

トラフィックシェーパー
PF7000A
PF7001A
PF7010A
PF7011A
取扱説明書
コンフィギュレーションガイド

第15版

・製品を適切・安全にご使用いただくために，製品をご使用になる前に，本書を必ずお読みください。
・本書に記載以外の各種注意事項は PureFlow GS1 トラフィックシェーパー PF7000A/PF7001A/ PF7010A/ PF7011A 取扱説明書に記載の事項に準じますので，そちらをお読みください。
・本書は製品とともに保管してください。

アンリツネットワークス株式会社

管理番号：PF-WP011AW-15.0

安全情報の表示について

当社では人身事故や財産の損害を避けるために，危険の程度に応じて下記のようなシグナルワードを用いて安全に関する情報を提供しています。記述内容を十分理解して機器を操作するようにしてください。
下記の表示およびシンボルは，そのすべてが本器に使用されているとは限りません。また，外観図などが本書に含まれるとき，製品に貼り付けたラベルなどがその図に記入されていない場合があります。

本書中の表示について

⚠ 危険	回避しなければ，死亡または重傷に至る切迫した危険状況があることを警告しています。
⚠ 警告	回避しなければ，死亡または重傷に至る恐れがある潜在的危険について警告しています。
⚠ 注意	回避しなければ，軽度または中程度の人体の傷害に至る恐れがある潜在的危険，または，物的損害の発生のみが予測されるような危険状況について警告しています。

機器に表示または本書に使用されるシンボルについて

機器の内部や操作箇所の近くに，または本書に，安全上または操作上の注意を喚起するための表示があります。
これらの表示に使用しているシンボルの意味についても十分理解して，注意に従ってください。

禁止行為を示します。丸の中や近くに禁止内容が描かれています。

守るべき義務的行為を示します。丸の中や近くに守るべき内容が描かれています。

警告や注意を喚起することを示します。三角の中や近くにその内容が描かれています。

注意すべきことを示します。四角の中にその内容が書かれています。

このマークを付けた部品がリサイクル可能であることを示しています。

PureFlow GS1
トラフィックシェーパー　PF7000A/PF7001A/PF7010A/PF7011A
取扱説明書　コンフィギュレーションガイド

2005年（平成17年）10月19日（初　版）
2012年（平成24年）11月２日（第15版）

保証

アンリツネットワークス株式会社は，納入後 1 年以内に製造上の原因に基づく故障が発生した場合は，無償で修復することを保証します。
ただし，次のような場合は上記保証の対象外とさせていただきます。

- 取扱説明書に記載されている保証対象外に該当する故障の場合。
- お客様の誤操作，誤使用，無断改造・修理による故障の場合。
- 通常の使用を明らかに超える過酷な使用による故障の場合。
- お客様の不適当または不十分な保守による故障の場合。
- 火災，風水害，地震，そのほか天災地変などの不可抗力による故障の場合。
- 指定外の接続機器，応用機器，応用部品，消耗品による故障の場合。
- 指定外の電源，設置場所による故障の場合。

また，この保証は，原契約者のみ有効で，再販売されたものについては保証しかねます。

なお，本製品の使用，あるいは使用不能によって生じた損害およびお客様の取引上の損失については，責任を負いかねます。

当社へのお問い合わせ

本製品の故障については，本説明書（紙版説明書では巻末，CD-ROM 版説明書では別ファイル）に記載の「本製品についてのお問い合わせ窓口」へすみやかにご連絡ください。

国外持出しに関する注意

1. 本製品は日本国内仕様であり，外国の安全規格などに準拠していない場合もありますので，国外へ持ち出して使用された場合，当社は一切の責任を負いかねます。
2. 本製品および添付マニュアル類は，輸出および国外持ち出しの際には，「外国為替及び外国貿易法」により，日本国政府の輸出許可や役務取引許可を必要とする場合があります。また，米国の「輸出管理規則」により，日本からの再輸出には米国政府の再輸出許可を必要とする場合があります。
   本製品や添付マニュアル類を輸出または国外持ち出しする場合は，事前に必ず弊社の営業担当までご連絡ください。
   輸出規制を受ける製品やマニュアル類を廃棄処分する場合は，軍事用途等に不正使用されないように，破砕または裁断処理していただきますようお願い致します。

商標・登録商標

Microsoft，Microsoft Windows XP，および Microsoft Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。
Java，J2SE，および Java 関連の商標およびロゴは，米国 Sun Microsystems，Inc.の米国およびその他の国における商標または登録商標です。

はじめに

この取扱説明書は，PureFlow GS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A（以下，本装置）で動作するソフトウェアの設定方法と使用方法を説明します。本装置を設置，導入，管理を行うネットワーク管理者を対象としています。インターネットワーキングに対する以下のような基礎知識を持った読者を想定しています。

- ローカルエリアネットワーク（LAN）
- Ethernet
- インターネットプロトコル（IP）

本装置の設置および取り扱い，コマンドの詳細については，下記説明書をご利用ください。

PureFlowGS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A 取扱説明書
この説明書は，本装置の設置および取り扱いについて記述してあります。

PureFlowGS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A 取扱説明書 コマンドリファレンス
この説明書は，本装置で使用するコマンドの詳細について記述してあります。

目次

VI.

第1章　ソフトウェアの概要

ここでは，本装置ソフトウェアの概要について説明します。

主要な機能を以下に列記します。

- トラフィックコントロール機能
- Network ポートバイパス機能
- リンクダウン転送機能
- Simple Network Management Protocol（SNMP）機能
- 統計情報
- Web による監視機能

ここでは，本装置ソフトウェアの基本機能について説明します。

2.1 トラフィックコントロール機能

音声通信や TV 会議などのミッションクリティカルな業務は，回線帯域不足によるパケット消失や通信遅延が発生すると業務効率を低下させ，重大な支障をきたすことにつながります。こうしたミッションクリティカルなトラフィックを回線帯域不足や通信遅延から守るために，回線帯域を拠点やユーザ，またはアプリケーションごとに分割し，必要な帯域を割り当てたり，トラフィックの優先制御を行う必要があります。本装置は，ネットワークの通信経路上に設置され，回線帯域を分割し，割り当てた帯域に対して最低帯域を保証したり，最大帯域制限を行うなどのトラフィックコントロールを行うことができます。

トラフィックコントロール機能についてのさらに詳細な説明は，「第 8 章 トラフィックコントロール機能」を参照してください。

2.2 Network ポートバイパス機能

停電時または装置異常時に，Network ポートの通信路をハード的に完全に装置から切り離すことにより，ネットワーク上に流れるトラフィックの通信を継続することができます。本機能は PureFlow GS1-FB，PureFlow GS1-GB で使用することができます。

Network ポートバイパス機能についてのさらに詳細な説明は，「第 10 章 Network ポートバイパス機能」を参照してください。

2.3 リンクダウン転送機能

一方のリンクのダウンを検出すると他方のリンクをダウンさせ，リンク異常を通知することができます。

リンクダウン転送機能についてのさらに詳細な説明は，「第 11 章 リンクダウン転送機能」を参照してください。

2.4 Simple Network Management Protocol（SNMP）機能

SNMP は，ルータやサーバなどのネットワーク機器に対してネットワークを通してリモートで管理するためのプロトコルです。

SNMP 機能についてのさらに詳細な説明は，「第 13 章 SNMP の設定」を参照してください。

2.5 統計情報

各カウンタ，キューバッファ情報などの統計情報があります。

統計情報についてのさらに詳細な説明は，「第 14 章 統計情報」を参照してください。

2.6　Web による監視機能

Web ブラウザを使用してネットワーク状態や，装置の状態を監視することができます。

Web による監視機能についてのさらに詳細な説明は，「第 16 章 Web による監視機能」を参照してください。

ここでは，設定の基本について説明します。

本装置の設定は Command Line Interface（CLI）を使用します。CLI はコンソールポートからコンソールケーブル経由で接続したターミナル（端末），またはシステムの IP ネットワークインタフェース（システムインタフェース）へのネットワーク経由で Telnet および SSH によるリモートアクセスが利用可能です。システムインタフェースへの通信は，Ethernet ポートまたは Network ポート経由のどちらかで行うことができます。

3.1 Command Line Interface（CLI）

CLI は，装置の動作パラメータの表示や設定を行うことができます。コマンドの詳細については，「PureFlow GS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A 取扱説明書 コマンドリファレンス」を参照してください。

（1）コンソールポート

コンソールポートの接続条件は次のとおりです。

通信速度：　9600 bit/s
キャラクタ長：　8 ビット
パリティ：　なし
ストップビット長：1 ビット
フロー制御：　なし

コンソールを接続するシリアルインタフェースコネクタは本体の前面にあります。添付のコンソールケーブルとコンソールアダプタを使用して接続してください。

（2）Telnet

Telnet を使用するためには，本装置のシステムインタフェースの設定を行う必要があります。SSH セッションと Telnet セッションを合わせ，最大 4 セッションまで同時利用可能です。

Ethernet ポートまたは Network ポートに接続されたネットワークを経由した端末から Telnet を使用してください。

システムインタフェースの設定の説明は「第 7 章 システムインタフェースの設定」を参照してください。

Telnet を使用しない場合は，set telnet コマンドで Telnet を無効にしてください。

（3）SSH

本装置の SSH(Secure SHell)は，SSH Version2 をサポートしています。SSH を使用するためには，SSH Version2 に対応した端末を使用してください。SSH セッションと Telnet セッションを合わせ，最大 4 セッションまで同時利用可能です。

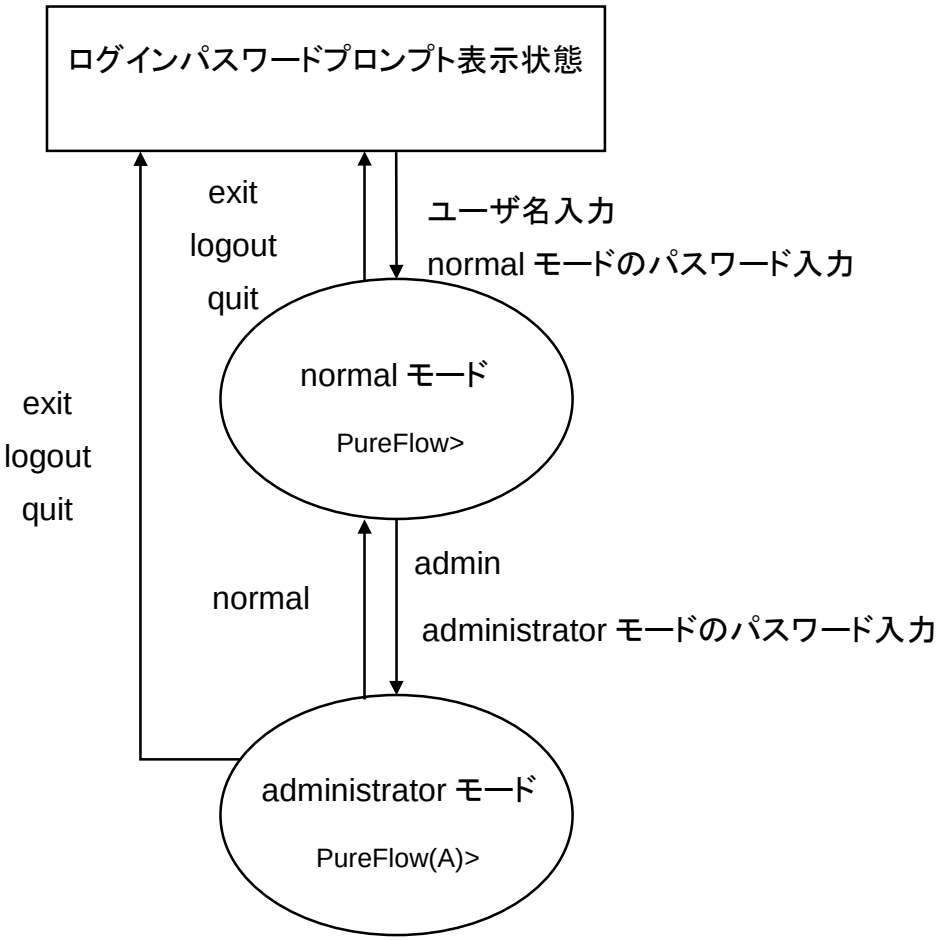
3.2　コマンド構造の説明

本装置の CLI には normal モードと administrator モードの 2 つがあります。normal モードでは，ステータスやカウンタ，および設定値の表示だけができます。administrator モードでは，すべての設定・変更・表示を行うことができます。

本装置のセキュリティを確保するため，normal モードに入るためのパスワードと administrator モードに入るためのパスワードを設定できます。パスワードが設定されている状態では，正しいパスワードを入力しないと，それぞれのモードに移行できません。

また，RADIUS 機能を使用しログイン認証を実施した場合，RADIUS サーバに設定されるユーザごとのサービスタイプに従って，normal モードまたは administrator モードに入ります。詳細は RADIUS 機能を参照してください。

CLI プロンプト表示	CLI モード
PureFlow>	normal モード
PureFlow(A)>	administrator モード



3.3　コマンドシンタックス

本装置 CLI のコマンドシンタックスは以下のような体系です。

アクション　設定項目　値

たとえば

アクション	設定項目	値
↓	↓	↓
設定する	時刻	数値
↓	↓	↓
set	date	20050518101010

また，機能に関する設定項目が多数あるので，「設定項目」は，「設定グループ＋設定項目」のように階層化している場合があります。

設定グループの例

ip
scenario
port

設定グループを伴うコマンドシンタックスの例を以下に示します。

アクション	設定グループ	設定項目	値
↓	↓	↓	↓
設定する	PORT グループ	1/2 の SPEED	100 M 固定
↓	↓	↓	↓
set	port	speed 1/2	100M

3.4　ヘルプ機能

システムプロンプト，またはコマンドの途中で疑問符(?)を入力すると，各コマンド入力モードで使用できるコマンドのリストを表示します。

```
PureFlow(A)> ?
Command                    Description
-------------------------------------------------------------------------------------------
?                          Lists the top-level commands available
add                        Adds some parameters, use 'add ?' for more
                           information
arp                        Shows address resolution table and control
clear                      Clears system statistics, use 'clear ?' for
                           more information
delete                     Deletes some parameters, use 'delete ?' for
                           more information
    .                          .
    .                          .
```

```
PureFlow(A)> add scenario ?
  vchannel                 Adds virtual channel scenario
                           information
  vpipe                    Adds virtual pipe scenario information
```

（注）
<?>キーによるヘルプ機能はコマンドラインの最後尾でのみ動作します。

3.5　コマンドの省略形と補完

各コマンドは判別可能な範囲で省略可能です。たとえば，s で始まるコマンドは save，set，show などがありますが，2 文字目が異なっているので，se と入力されれば“set”コマンドであると判別可能です。以下の二つの入力は，同じコマンドを表します。

```
set port autonegotiation 1/2 disable  ＝  se po au 1/2 d
```

判別可能な文字を入力した段階で，<TAB>キーを入力すると，キーワードを補完して表示します。

```
PureFlow(A)> set po<TAB>
                    ↓
PureFlow(A)> set port
```

（注）
<TAB>キーによる補完機能はコマンドラインの最後尾でのみ動作します。また，コマンドのキーワードによっては，省略および<TAB>キーが動作しないものがあります。その場合は，ヘルプ機能でキーワードを確認し，すべてのキーワードを入力してください。

3.6　ヒストリ機能

コマンド ヒストリの使用方法

CLI は，入力されたコマンドの履歴（記録）機能を持っています。
コマンドヒストリから，次に入力しようとするコマンドに類似した履歴コマンドを呼び出し，あとで説明するコマンド編集機能で編集後，実行することができます。

コマンドヒストリは下記のキー入力で履歴を呼び出すことができます。

Ctrl-Pまたは上矢印キー

最も新しいコマンドからヒストリ バッファのコマンドを呼び出します。このキー操作を繰り返すと，続けて古いコマンドが呼び出されます。

Ctrl-Nまたは下矢印キー

Ctrl-P または上矢印キーでコマンドが呼び出されてから，ヒストリ バッファの新しいコマンドに戻ります。このキー操作を繰り返すと，続けて新しいコマンドが呼び出されます。

また，“show history”コマンドにより，すべてのコマンド履歴を表示することができます。

3.7　コマンド編集機能

コマンドラインを編集するために必要なキーストロークを示します。

Ctrl-Bまたは左矢印キー

カーソルを 1 文字分後退させます。

Ctrl-Fまたは右矢印キー

カーソルを 1 文字分前に進めます。

Ctrl-Aキー

カーソルを行の先頭に戻します。

Ctrl-Eキー

カーソルを行の最後に進めます。

Ctrl-DまたはDeleteキー

カーソルの位置にある文字を削除します。

Ctrl-HキーまたはBSキー

カーソルの位置の前の文字を削除します。

Ctrl-Kキー

カーソル以降の文字列を削除するとともに，バッファにコピーします。

Ctrl-Wキー

カーソルで選択された単語を削除するとともに，バッファにコピーします。

Ctrl-Yキー

カーソル位置にバッファの内容をペーストします。

Ctrl-Uキー

カーソルの行を削除するとともに，バッファにコピーします。

（注）
コマンドライン編集機能はコマンドライン表示が 1 行に収まる場合のみ動作します。

3.8　ページャ機能

ターミナルへの表示を伴うコマンドを実行したとき表示内容が 24 行を超えるものについては，画面単位および行単位のページャ機能による表示を行います。その場合は画面の最終行に“—More—”と表示し，表示内容がその行以降も続いていることを表します。
“—More—”が表示されているときに入力可能なキーは，以下のとおりです。

スペースまたはFキー

次の画面を表示します。

Enterキー

次の行を表示します。

Qキー

表示を終了します。

3.9　起動と設定

本装置の電源を投入すると，装置内部の内蔵フラッシュメモリ（以後，内蔵フラッシュメモリ）のソフトウェアオブジェクトを自動で読み込み起動します。また，CF カードスロットに，ソフトウェアオブジェクト（ファイル名：gs.bin）が入った CF カードを挿入して電源を投入すると CF カード内のソフトウェアオブジェクトを優先して読み込み起動します。CF カードの読み込み中は，CF カードに対しアクセスをしていますので，CF カードを抜いたり電源をオフにすると，CF カードが破損する恐れがあります。

本装置のコンソールポートに接続されている場合は，下記のような起動メッセージが表示されます（起動メッセージでの表示項目については，ソフトウェアバージョンによって，変更されることがあります）。

```
Anritsu PureFlow PX700001A Software Version 1.1.1
Copyright 2005 ANRITSU CORPORATION,    All rights reserved.

Serial Port                 ... [OK]
Backup Memory Checking      ... [OK]
Real Time Clock Checking    ... [OK]
File System Checking        ... [OK]
EEPROM Checking             ... [OK]
Ethernet Controller Checking
Management Port             ... [OK]
        Internal Port       ... [OK]

.
Loading Forwarding Processor module software..... completed
Slot 1 boot up complete
        Medium type GbE/2T with 2 ports

System booting up.....
Loading Configuration from Master.
Restoration in progress
....
Restoration completed
completed
CONSOLE login verification..

login:
```

設定に際しては，まずシステムコンソールとしてコンソールポートに添付のコンソールケーブルを接続します。コンソールが接続され，[Enter]キーを入力すると，コンソール上に次のようなメッセージを表示し，ログイン受付状態となります。

```
login:
```

本装置のユーザ名は“root”です。また，工場出荷時の初期状態において，ログインパスワードは未設定となっています。ログインが認証されると，プロンプトが表示され，コマンド受付状態になります。

```
login:root
Password:([Enter]キーを入力)
FureFlow＞
```

この状態は normal モードで，設定内容を見ることはできますが，内容を変更することはできません。設定を行うためには administrator モードに移行する必要があります。この移行は“admin”コマンドで行います。

```
PureFlow＞admin
Password:([Enter]キーを入力)
FureFlow(A)＞
```

この administrator モードでは，各種パラメータの表示に加えて，動作パラメータの変更，パスワードの設定が可能になります。administrator モードには，同時に複数のユーザが移行でき，同時に設定変更が行えます。administrator モードには，パスワードを設定するなど，administrator 権限のユーザ管理を行ってください。

3.10 設定の保存方法

本装置にて設定した内容は，コマンドによる設定後すみやかに有効となりますが，そのままでは電源断時に失われ，再起動後は無効となります。本装置は内蔵フラッシュメモリに設定内容をコンフィギュレーションファイルとして保存することが可能です。次回電源投入後に設定内容を有効にするためには内蔵フラッシュメモリに save コマンドにて設定内容を保存する必要があります。

保存方法は次のとおりです。

```
PureFlow(A)＞ save config
Do you wish to save the system configuration into the flash memory (y/n)? y
.....
Done
PureFlow(A)＞
```

本装置の電源を投入すると，内蔵フラッシュメモリに保存されたコンフィギュレーションファイルを自動で読み込みます。また，CF カードスロットに，コンフィギュレーションファイル（ファイル名：extgscnf.txt）が入った CF カードを挿入して電源を投入すると，CF カード内のコンフィギュレーションファイルを優先して読み込みます。CF カードの読み込み中は，CF カードに対しアクセスをしていますので，CF カードを抜いたり電源をオフにすると，CF カードが破損する恐れがあります。

（注）
コンフィギュレーション情報量によって，save コマンド実行時間および電源投入時の起動時間が変化します。以下に，参考値を示します。

PureFlow GS1-F／GS1-FB の場合

	コンフィギュレーション情報量		
	デフォルト	フィルタ　100 件 シナリオ　100 件 登録時	フィルタ　8192 件 シナリオ　2048 件 登録時
save コマンド 実行時間	1 秒以下	約 2 秒	約 55 秒
起動時間	約 25 秒	約 28 秒	約 180 秒

PureFlow GS1-G／GS1-GB の場合

	コンフィギュレーション情報量		
	デフォルト	フィルタ　100 件 シナリオ　100 件 登録時	フィルタ　8192 件 シナリオ　4096 件 登録時
save コマンド 実行時間	1 秒以下	約 2 秒	約 61 秒
起動時間	約 25 秒	約 28 秒	約 205 秒

※　フィルタ／シナリオの設定の説明は「第 8 章　トラフィックコントロール機能」を参照してください。
※　save コマンド実行時間と機動時間は，設定コマンドのライン数やパラメータの数によって変化します。

本装置には時刻，CLI パスワードなどの装置全体にかかわる設定や，ハードウェア，ソフトウェアのバージョン表示などの装置全体にかかわる情報があります。これらの情報表示と設定について説明します。

本装置には，下記の装置本体情報と設定項目があります。

日付／時刻	装置内蔵のカレンダ・クロックです。SYSLOG によるイベントの記録に使用されます。
SNTP	Simple Network Time Protocol（SNTP）クライアント機能です。
ユーザ名とパスワード	CLI による装置へのアクセス制御のためのユーザ名とパスワードです。
SYSLOG 設定	装置の状態変化イベントやエラーイベントを内蔵メモリ，バッテリバックアップメモリに保存したり，リモートホストに送信することができます。
モジュール情報	装置内の各モジュール情報（バージョンなど）です。

4.1　日付／時刻

本装置は，カレンダ機能に対応しています。日付，時刻はSYSLOG によるイベントの記録に使用されます。日付，時刻の設定は CLI コマンドで指定する方法と，SNTP クライアント機能により NTP サーバの時刻に自動同期させる方法があります。

CLIコマンドによる設定

CLI で設定する場合は以下のコマンドを使用します。

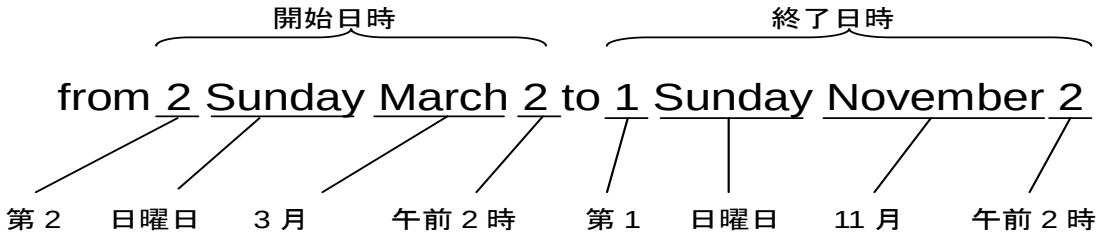
set date <yyyymmddhhmmss>	日付，時刻の設定を行います。
set timezone <hours-offset> [<minuts-offset>]	協定世界時（**UTC**:Coordinated Universal Time）からの**タイムゾーン** オフセットを設定します。 デフォルト値は+9[時間]0[分]です。
set summertime from <week> <day> <month> <hh> to <week> <day> <month> <hh> [offset]	夏時間の設定を行います。 デフォルトでは設定されていません。
unset summertime	夏時間の設定を解除します。
show date	日付，時刻の表示を行います。

コマンドの実行例を示します。

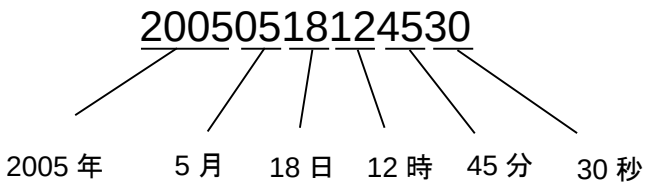
```
PureFlow(A)> set timezone +9
PureFlow(A)> set summertime from 2 Sunday March 2 to 1 Sunday November 2
PureFlow(A)> set date 20050518124530
PureFlow(A)> show date
May 18 2005(Mon) 12:45:32

UTC Offset      : +09:00
Summer Time     : From Second Sunday March 02:00
                  To     First Sunday November 02:00
                  Offset 60 minutes
PureFlow(A)>
```

タイムゾーンの設定は，UTC（協定世界時）からのオフセット時間を符号付きで入力します。必要な場合は，分単位のオフセットを入力します。

夏時間の設定は，夏時間の開始日時と終了日時を指定します。必要な場合は夏時間である間，時刻に加えるオフセットを分単位で入力します。オフセットを省略した場合は 60[分]が適用されます。
開始日時および終了日時は以下のフォーマットで指定します。



日付，時刻の設定は西暦年，月，日，時，分，秒を続けて 14 桁で入力します。



カレンダ・クロックに設定した時刻は，装置内部のバッテリで駆動され，装置電源がオフの状態でも止まらずに進み続けます。

4.2 Simple Network Time Protocol（SNTP）

本装置は，SNTP クライアント機能を実装しています。SNTP クライアントは Ethernet ポートまたは Network ポート経由で NTP サーバと通信し，本装置の日付および時刻を NTP サーバと同期させます。SNTP クライアントを使用するためには，本装置のシステムインタフェースの設定を行う必要があります。システムインタフェースの設定の説明は「第 7 章 システムインタフェースの設定」を参照してください。

SNTP クライアントの設定には以下のコマンドを使用します。

set sntp {enable | disable}	SNTP クライアント機能を有効化／無効化します。
set sntp server <IP_address>	NTP サーバの IPv4 アドレスを設定します。NTP サーバは 1 つのみ指定できます。
set sntp interval <interval>	NTP サーバへ定期的に時刻の問い合わせを行う間隔を秒単位で設定します。設定範囲は 60～86400[秒]です。デフォルトは 3600[秒]です。
show sntp	SNTP クライアントの状態および設定を表示します。

NTP サーバ 192.168.10.10，問い合わせ間隔 86400 秒を設定する場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set sntp server 192.168.10.10
PureFlow(A)> set sntp interval 86400
PureFlow(A)> set sntp enable
PureFlow(A)> show sntp
Status      : enable
Server      : 192.168.10.10
Interval    : 86400
Sync        : kept
PureFlow(A)>
```

show sntp コマンドの Sync の表示が kept になっていれば，NTP サーバとの同期が取れている状態です。時刻の修正は NTP サーバと本装置が 3 秒以上ずれている場合に行われます。

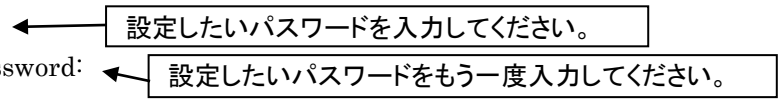
4.3　ユーザ名とパスワード

装置のセキュリティを保つために装置設定をシリアルコンソール，または Telnet で行う前にはユーザ名とパスワードによる認証が行われます。このパスワードはユーザが変更することができます。

set password	ログインパスワードを設定します。ログインパスワードは 16 文字以内です。
set adminpassword	administorator モードに移行するためのログインパスワードを設定します。ログインパスワードは 16 文字以内です。

コマンドの実行例を示します。

```
PureFlow(A)> set password
Changing the Password for the Normal Mode
New password:
Retype the new password:
```



ログインパスワードに設定できる文字は，以下の ASCII 文字です。

```
1234567890
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
!#$%&'()=~-^|¥@`[]{}:*;+_/.,<>
```

ログインパスワードを設定解除する場合は，“New password”の問いに対し，パスワードを入力せず，[Enter]キーを入力してください。

4.4 SYSLOG

装置に起きたエラーイベントやリンクアップ・ダウンなどのイベント(以後，ログデータと呼ぶ)を複数の方法で記録することができます。本装置はログデータを通電状態で内蔵メモリに最大 8000 イベント保持します。内蔵メモリに保持するログデータは電源が遮断されると消失します。ログデータは内蔵バックアップメモリと，ネットワークを介した SYSLOG ホストに記録することができます。内蔵バックアップメモリへは，前回と前々回の装置稼働時におけるログデータを，それぞれ最大 1200 イベント保持します。内蔵バックアップメモリに保持するログデータは，電源を遮断しても消失しません。

show syslog	内蔵メモリに記録されたログデータを表示します。
show backup syslog [last | second_last]	内蔵バックアップメモリに記録されたログデータを表示します。
clear syslog	内蔵メモリに記録されたログデータをクリアします。
set syslog severity <severity_level>	ログデータを記録するレベルを指定します。
show syslog host	システムログ出力に関する設定を表示します。
set syslog host {enable | disable}	SYSLOG ホストへの記録を有効化／無効化します。
add syslog host ip <IP_address> [<udp_port>]	SYSLOG ホストの IPv4 アドレス／UDP ポートを追加します。set syslog host ip コマンドでも追加可能です。
delete syslog host ip <IP_address>	SYSLOG ホストの IPv4 アドレス／UDP ポートを削除します。unset syslog host ip コマンドでも削除可能です。
set syslog host ip <IP_address> [<udp_port>]	SYSLOG ホストの IPv4 アドレス／UDP ポートを設定します。
unset syslog host ip	SYSLOG ホストの IPv4 アドレス／UDP ポートを解除します。
set syslog facility {ccpu | fcpu} <facility_code>	システムログの facility を設定します。 ccpu： Control CPU(制御系 CPU)で検出，記録したログメッセージ fcpu： Forwarding CPU(フォワーディング系 CPU)で検出，記録したログメッセージ

ログデータはテキストデータとして以下のフォーマットで装置内に記録されています。

プライオリティ	日時	メッセージ
134	2005 May 18 16:51:19	Port 1/1 changed Up from Down.

プライオリティ

プライオリティはログメッセージの特徴を示すコードです。プライオリティのコードは RFC3164 で規定されている方式で計算し，格納されます。プライオリティコードはメッセージのカテゴリを表す Facility とメッセージの重大度を示す Severity の 2 つの数値を組み合わせたコードで表現されます。

プライオリティ＝Facility×8＋Severity

本装置の SYSLOG メッセージの Facility は設定が可能です。設定可能な Facility の範囲は 0～23 です。デフォルト値は以下となります。

control CPU：16
forwarding CPU：17

コマンドの実行例を以下に示します。

```
PureFlow(A)> set syslog facility ccpu 18
PureFlow(A)> set syslog facility fcpu 19
```

control cpuのFacilityを18にします。

forwarding cpuのFacilityを19にします。

Severity には 0 から 6 までの数値が格納されます。プライオリティ 0 が最も重大度が高く，数値が大きくなるほど低くなります。各メッセージの重大度は RFC 3164 に規定された以下の基準に従って割り当てられています。

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages

たとえばプライオリティ 129（16×8＋1）のメッセージは Facility が 16，Severity が 1 です。つまり Control CPU で検出された Alert レベル（緊急）メッセージです。

日時

イベントが発生した日時です。

メッセージ

イベントの内容を示すメッセージが格納されます。

メッセージは show syslog コマンドで表示できます。

```
PureFlow> show syslog
-------------------------------------------------------------------------------------------------
Pri     Date            Time       Message
-------------------------------------------------------------------------------------------------
134    2005 May 18 16:51:19 Port 1/1 changed Up from Down.
```

データは装置の通電中，メモリに保持されていますが，オペレータがメッセージをクリアすることができます。

```
PureFlow> clear syslog
PureFlow> show syslog
-------------------------------------------------------------------------------------------------
Pri     Date            Time       Message
-------------------------------------------------------------------------------------------------
PureFlow>
```

4.5　モジュール情報

装置内の各モジュール情報を表示します。バージョン，製造番号などを確認することができます。

show module	各モジュール情報を表示します。

モジュール情報には，以下のものがあります。

MACアドレス

装置の MAC アドレスです。

本体

本体の形名，ハードウェアバージョン，製造番号です。形名は，以下のとおりです。

PF7000A：PureFlow GS1-F
PF7001A：PureFlow GS1-FB
PF7010A：PureFlow GS1-G
PF7011A：PureFlow GS1GB

モジュール

本体に内蔵しているモジュールの形名，ハードウェアバージョン，製造番号です。形名は，以下のとおりです。

PM700101A：PureFlow GS1-F に内蔵しているモジュール
PM700102A：PureFlow GS1-FB に内蔵しているモジュール
PM700111A：PureFlow GS1-G に内蔵しているモジュール
PM700112A：PureFlow GS1-GB に内蔵しているモジュール

ソフトウェア

ソフトウェアの形名，バージョンです。形名は，以下のとおりです。

PX700001A：PureFlow GS1 の基本ソフトウェア

Field Programmable Gate Array（FPGA）

FPGA のバージョンです。

パケット受信バッファサイズ

装置内のパケット受信バッファサイズです。

PF7000A：128 Mbyte
PF7001A：128 Mbyte
PF7010A：256 Mbyte
PF7011A：256 Mbyte

ブートモニタ

ブートモニタのバージョンです。

温度

装置内部の温度です。本装置内部には，2 箇所に温度センサがあり，各温度センサの温度を表示します。

コマンドの実行例を示します。

```
PureFlow(A)> show module
Anritsu PureFlow PX700001A Software Version 1.1.1
Copyright 2005-2006 ANRITSU CORPORATION,  All rights reserved.

MAC Address                              : 00-00-91-12-34-56

Chassis Model Name                       : PF7010A
Chassis Version                          : A00
Chassis Serial Number                    : 2600010003

Module Model Name                        : PM700111A
Module Version                           : 100
Module Serial Number                     : 2600010003

Management Software Model Name           : PX700001A
Management Software Version              : 1.1.1
Forwarding Software Model Name           : PX700001A
Forwarding Software Version              : 1.1.1
FPGA Version                             : 1.1.0

Receive Buffer Size                      : 256 Mbyte

Management Boot Monitor Version          : 1.0.1
Forwarding Boot Monitor Version          : 1.0.1

Uptime                                   : 107 days, 03:10:55
Temperature 1                            : 33C
Temperature 2                            : 33C
PureFlow(A)>
```

4.6 ライセンスキー

ライセンスキーを購入すると以下の機能を使用できるようになります。

- コンテンツ・アウェア・シェーピング機能（第 9 章参照）
- 3 階層帯域制御機能
- シナリオ拡張機能

ライセンスキーを装置購入後に購入する場合は，装置シリアル番号をご指定ください。

ライセンスキーは，キーを記載したカードで提供されます。ライセンスキーを本装置に設定するには，“set option”コマンドを入力してください。ライセンスキー入力を促すメッセージが表示されますのでライセンスキーを入力してください。ライセンスキー入力の際，4 文字ごとにハイフンを入力しても，ハイフンを入力しなくても同じライセンスキーとして認識します。入力されたライセンスキーと装置のシリアル番号を比較し，一致した場合にライセンスが有効になります。

ライセンスキーに関するコマンドには以下ものがあります。

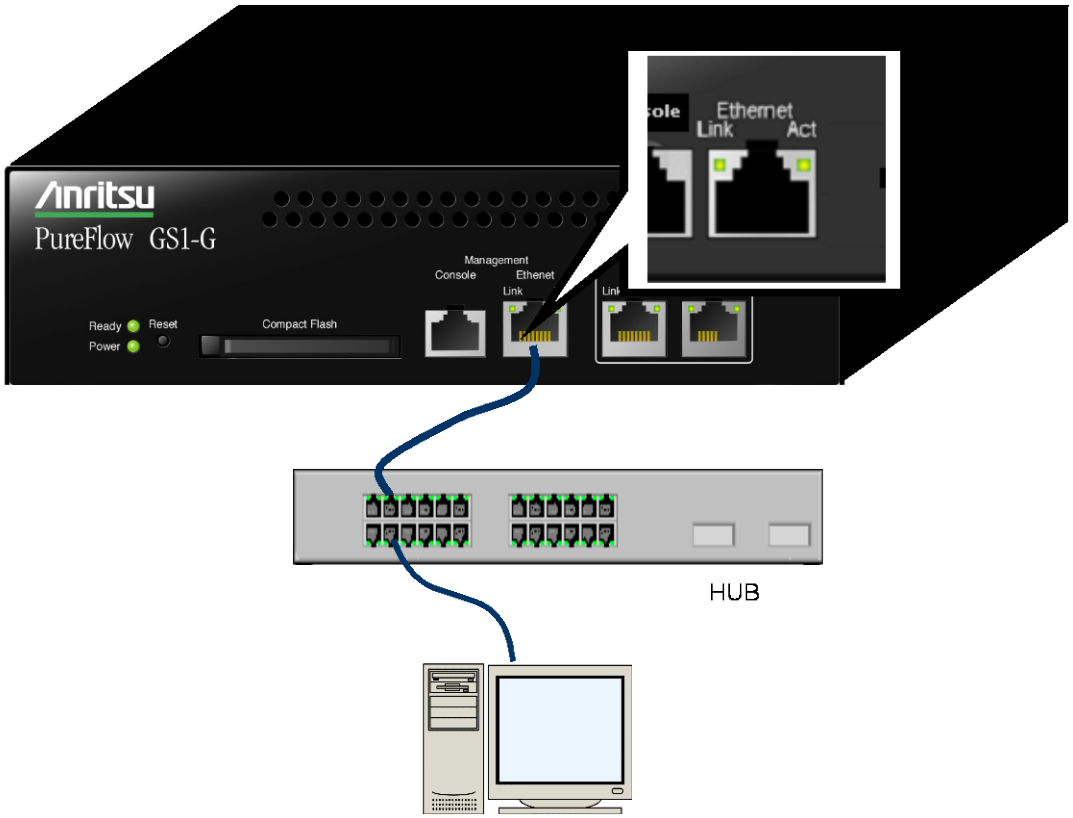
set option	ライセンスキーを本装置に設定します。
show option	有効になっているライセンスを表示します。

コマンドの実行例を示します。

```
PureFlow(A)> set option
Enter the option key : XFS8wbFEFBNkfqLJ

Authentication succeed.

    Making be available : GS1 License Key 1 (Contents Aware Shaping)
Updation done.
PureFlow(A)>
PureFlow(A)> show option
    GS1 License Key 1 available (Contents Aware Shaping )
    GS1 License Key 2 available (Three-Stages Traffic Control )
    GS1 License Key 3 available (Extended Max Scenario Entries )
PureFlow(A)>
```

本装置は，ネットワーク経由のリモートによる設定，制御を行うために，Ethernet ポートを装置前面に持っています。
本ポートはマネジメント用のローカルポートで，Network ポートとは切り離されています。本ポートは Auto-MDIX ポートで 10BASE-T，100BASE-TX をサポートし，AutoNegotiation モードで相手機器と接続します。

（注）
本ポートは，AutoNegotiation モードのみ対応です。通信速度／デュプレックスモードは，設定できません。



Ethernet ポートに接続されたネットワーク経由のリモートによる設定，制御を行うためには，本装置のシステムインタフェースの設定を行う必要があります。システムインタフェースの設定の説明は「第 7 章 システムインタフェースの設定」を参照してください。

ここでは，本装置の Network ポートの設定について説明します。Network ポートとは，ネットワーク上に流れるトラフィックをコントロール（トラフィックコントロール）するためのポートです。また，Network ポートに接続されたネットワーク経由のリモートによる設定，制御を行うこともできます。

本装置では，以下に示す Network ポートをサポートしています。

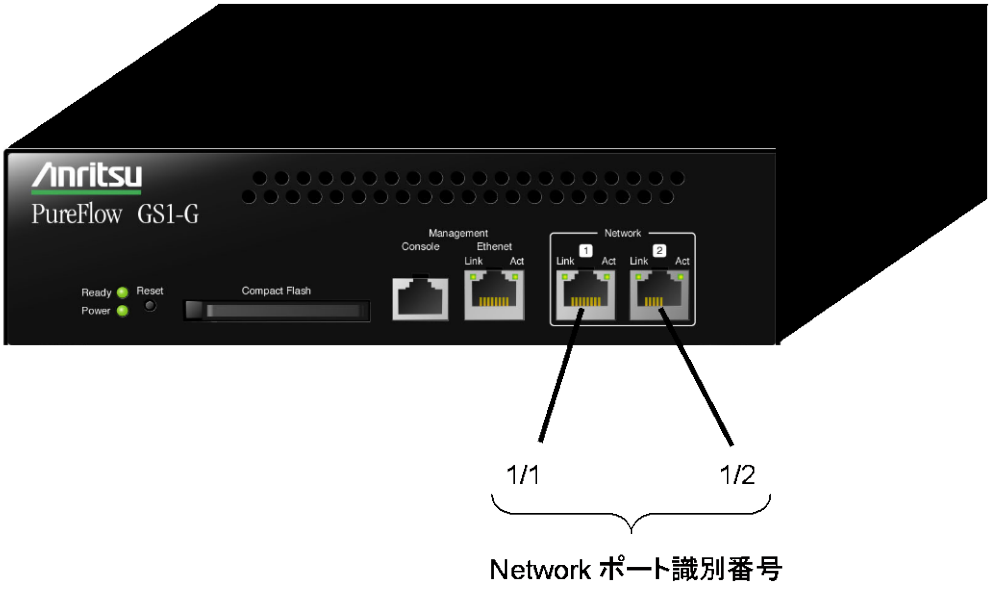
PureFlow GS1-F　：10BASE-T／100BASE-TX（RJ-45／Auto-MDIX）
PureFlow GS1-FB：10BASE-T／100BASE-TX（RJ-45／Auto-MDIX）
PureFlow GS1-G　：10BASE-T／100BASE-TX／1000BASE-T（RJ-45／Auto-MDIX）
PureFlow GS1-GB：10BASE-T／100BASE-TX／1000BASE-T（RJ-45／Auto-MDIX）

Network ポートには以下の設定が可能です。

AutoNegotiation の有効／無効（注 1，注 2，注 3 参照）
フローコントロール（auto，pause フレーム受信／送信）
通信速度（10Mbit/s，100Mbit/s）（注 1，注 2 参照）
デュプレックスモード（full，half）（注 1，注 2 参照）
強制リンクアップの有効／無効（通信速度が 10 Mbit/s の場合）（注 4 参照）

CLI から Network ポートを指定するには＜スロット番号／ポート番号＞の組み合わせで指定します。PureFlow GS1 のスロット番号には 1 を指定します。

スロット内のポート番号は左から順番に 1/1，1/2 と番号付けられており，これにより，Network ポートの識別番号は以下のようになります。



Network ポート識別番号

Network ポートに接続されたネットワーク経由のリモートによる設定，制御を行うためには，本装置のシステムインタフェースの設定を行う必要があります。システムインタフェースの設定の説明は「第 7 章 システムインタフェースの設定」を参照してください。

（注 1）
通信速度／デュプレックスモードは，AutoNegotiation 無効のときのみ有効です。AutoNegotiation 有効のとき，これらの設定内容は無効です。

（注 2）
GS1-G／GS1-GB（1000BASE-T）の 1Gbit/s 通信は，AutoNegotiation 有効で使用してください。また，通信速度が 1Gbit/s のときは，half デュプレックスをサポートしません。

（注 3）
Auto-MDIX は，AutoNegotiation 有効時のみ動作します。AutoNegotiation 無効時は，接続するケーブルの種類（ストレート／クロス）を確認してください。パソコンなどと接続する場合は，クロスケーブルで接続してください。スイッチ／HUB などと接続する場合は，ストレートケーブルで接続してください。

（注 4）
通信速度が 10Mbit/s 設定の場合，ネットワーク上にトラフィックの負荷がある状態でケーブル接続，または装置起動すると，対向装置の種類によっては本装置がリンクアップ状態になるまで時間がかかることがあります。しばらくしてもリンクアップしない場合，トラフィックの負荷を軽減，または停止するとリンクアップします。もし，トラフィックの負荷を軽減，または停止することができない場合，“set port forcelinkup”コマンドで強制的にリンクアップさせることができます。

Network ポート 1/1 の AutoNegotiation 無効，通信速度 10Mbit/s，デュプレックス full で，強制的にリンクアップさせる場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set port autonegotiation 1/1 disable
PureFlow(A)> set port speed 1/1 10M
PureFlow(A)> set port duplex 1/1 full
PureFlow(A)> set port forcelinkup 1/1 enable
```

ただし，強制的にリンクアップさせる場合，以下の制約事項にご注意ください。

（制約事項 1）
“set port forcelinkup”コマンドで強制リンクアップを有効にする場合，Network ポートの属性は以下の条件下で使用してください。本コマンドを実行する場合は，あらかじめ AutoNegotiation 無効，通信速度 10Mbit/s に設定してください。

AutoNegotiation	無効のみ
通信速度	10Mbit/s のみ
デュプレックスモード	制限なし
フローコントロール	制限なし

（制約事項 2）
“set port forcelinkup”コマンドを実行すると，強制的にリンクアップ状態になるため，ケーブルを抜いた状態でもリンクダウン状態に変化しません。また，強制リンクアップ状態では，Link LED が常時点灯します。

6.1　Network ポートの属性の設定

AutoNegotiation 無効のときは，Network ポートの通信速度やデュプレックスといったポートの動作属性を CLI から変更できます。これらの Network ポート属性は，通常 AutoNegotiation により，最も適切な動作モードに自動的に設定されます。接続先のスイッチやノードが AutoNegotiation をサポートしていない場合は，本コマンドにより，マニュアル設定する必要があります。逆に，接続先が AutoNegotiation 設定になっている場合は，本装置も AutoNegotiation 設定にしてください。片方がマニュアル設定で，他方が AutoNegotiation 設定になっていると，正しく接続できません。

set port autonegotiation <slot/port> {enable | disable}	Network ポートの AutoNegotiation の有効／無効を設定します。デフォルトは enable です。
set port speed <slot/port> {10M | 100M}	Network ポートの通信速度を設定します。本設定は，AutoNegotiation 無効のときの通信速度設定です。AutoNegotiation 有効のとき，この設定内容は無効です。デフォルトは 100M です。 注）GS1-G ／ GS1-GB（1000BASE-T）の 1Gbit/s 通信は，AutoNegotiation 有効で使用してください。
set port duplex <slot/port> {full | half}	Network ポートのデュプレックスモードを設定します。本設定は，AutoNegotiation 無効のときのデュプレックスモード設定です。AutoNegotiation 有効のとき，この設定内容は無効です。デフォルトは full です。
set port flow_control <slot/port> auto set port flow_control <slot/port> {recv | send} {on | off}	Network ポートのフローコントロールを設定します。デフォルトは auto です。AutoNegotiation による自動決定を行わない場合のデフォルトは recv と send の両方とも off です。
set port forcelinkup <slot/port> {enable | disable}	Network ポートの強制リンクアップの有効／無効を設定します。デフォルトは disable です。

Network ポート 1/2 の AutoNegotiation 無効，通信速度 100 Mbit/s，デュプレックス full を設定する場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set port autonegotiation 1/2 disable
PureFlow(A)> set port speed 1/2 100M
PureFlow(A)> set port duplex 1/2 full
```

また，Network ポート 1/2 のフローコントロールで pause フレームを送受信しない設定にする場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set port flow_control 1/2 recv off
PureFlow(A)> set port flow_control 1/2 send off
PureFlow(A)>
```

6.2　設定，状態の確認

設定コマンドで設定した内容や，現在の Network ポートの動作状態を確認するには，“show port”コマンドを使用します。

```
PureFlow(A)>  show port
Port    Type            Status    Link   Autonego  Speed   Duplex
----    --------------  ------    ----   --------  -----   ------
1/1     100BASE-TX      Enabled   Up     Enabled   100M    Full
1/2     100BASE-TX      Enabled   Up     Enabled   100M    Full
system  100BASE-TX      Enabled   Up     Enabled   100M    Full
PureFlow(A)>
```

“show port”コマンドにより，実装されているすべての Network ポートの状態が確認できます。さらに詳細な情報を確認するには，Network ポート識別番号をコマンド引数で指定することにより，確認できます。

```
PureFlow> show port 1/1

Slot/Port        :1/1
Port type        :1000BASE-T
Admin status     :Enabled
Oper status      :Up
Auto negotiation :Enabled
Admin speed      :100M
Admin duplex     :Full
Tx Flow control  :Auto
Rx Flow control  :Auto
PureFlow>
```

Network ポートの統計情報を確認するには，“show counter”コマンドを使用します。本コマンドで表示するカウンタ長は，32 ビットです。

```
PureFlow(A)> show counter
Port      Rcv Octets   Rcv Packets   Trs Octets   Trs Packets
-------   ----------   -----------   ----------   -----------
 1/1        57566366      14194297            0             0
 1/2               0             0     59383412      14195494
system         58368           152        85424           152

Port      Rcv Broad    Rcv Multi    Trs Broad    Trs Multi
-------   ----------   ----------   ----------   ----------
 1/1           10000     14208097            0           0
 1/2               0            0        10000    14209615
system             5            0           10           0

Port      Err Packets   Collision    Discard
-------   -----------   ----------   ----------
 1/1                0           0           0
 1/2                0           0           0
system            N/A         N/A         N/A
```

また，Network ポート識別番号をコマンド引数で指定することにより，詳細内容を表示できます。本コマンドで表示する Rcv Packets，Rcv Broad，Rcv Multi，Rcv Octets，Trs Packets，Trs Broad，Trs Multi，Trs Octets，Discard のカウンタ長は，64 ビットです。それ以外のカウンタ長は，32 ビットです。

```
PureFlow(A)> show counter 1/1
Rcv Packets                  14194297
Rcv Broad                       10000
Rcv Multi                    14208097
Rcv Octets                   57566366
Rcv Rate                           16 [kbps]
Trs Packets                         0
Trs Broad                           0
Trs Multi                           0
Trs Octets                          0
Trs Rate                            0 [kbps]
Collision                           0
Drop                                0
Discard                             0
Error Packets                       0
       CRC Align Error                      0
       Undersize Packet                     0
       Oversize Packet                      0
```

ここでは，本装置のシステムインタフェースの設定について説明します。

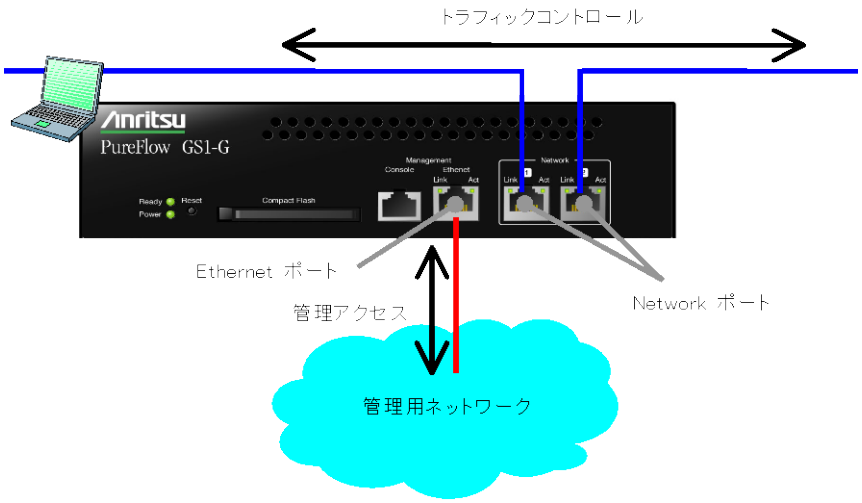
7.1　概要

システムインタフェースとは，管理者が本装置をネットワーク経由でリモートアクセスするための IP ネットワークインタフェースです。本装置へのリモートからの制御には Telnet，SNMP などの手段を用い，本装置の設定，および状態監視を行うことができます。

以下に示すように，システムインタフェースは，Ethernetポート経由でアクセスするか，Networkポート経由でアクセスするかのいずれかを選択することができます。

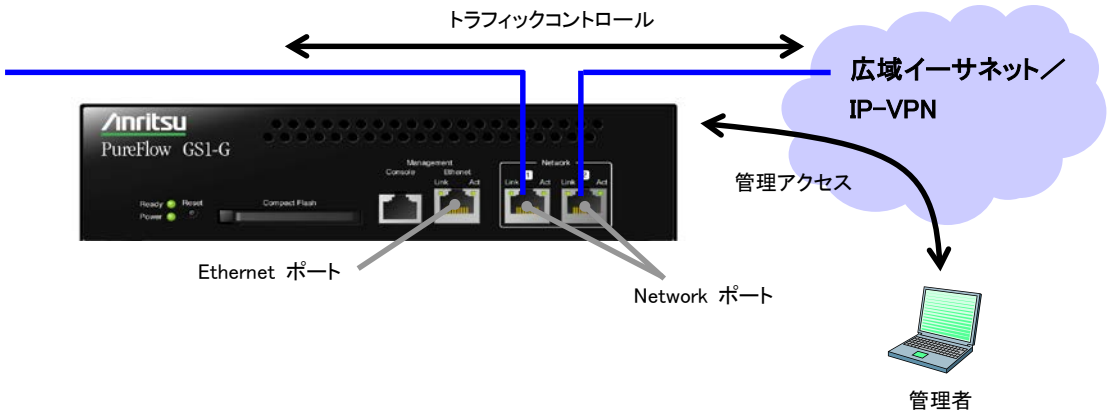
（1）Ethernet ポート経由によるリモート管理

トラフィックコントロールを行うネットワーク（Network ポートからの入出力）とは別の管理用ネットワークに管理者端末を配置し，Ethernet ポートを経由して制御することができます。セキュリティ上，トラフィックコントロールを行うネットワーク内からアクセスをさせたくない場合などに有効です。



（2）Network ポート経由によるリモート管理

トラフィックコントロールを行うネットワーク内に管理者端末を配置し，Network ポートを経由して制御することができます。管理専用のネットワークを用意する必要がないため，ネットワーク構成をシンプルにすることができます。



7.2　システムインタフェース通信

システムインタフェースへの通信は，Ethernet ポートまたは Network ポート経由のどちらかで行うことができます。Ethernet ポート経由で行う場合は，VLAN Tag なしパケットの通信を行うことができます。また，Network ポート経由で行う場合は，通信を行う Network ポートを指定（1/1 のみ，1/2 のみ，すべて）でき，VLAN Tag なしパケットまたは VLAN Tag ありパケットの通信を行うことができます。

また，Network ポート経由で行う場合，不特定多数の端末からシステムインタフェースへの通信を制限するためにフィルタ機能を使用することもできます。

システムインタフェース通信で利用できる機能を以下に示します。

- Telnet（CLI）
- SSH（CLI）
- RADIUS
- TFTP（ダウンロード／アップロード）
- SYSLOG
- PING
- SNTP
- SNMP
- WEB

ファイアーウォール等のセキュリティ設定を行っている場合は，以下のサービスが通信できるように設定を変更してください。

ポート番号	TCP/UDP	サービス名	備考
23	TCP	telnet	telnet 接続，コンフィグマネージャとの接続
22	TCP	ssh	SSH 接続
1812	UDP	radius	RADIUS 認証
69	UDP	tftp	TFTP 接続
514	UDP	syslog	SYSLOG 設定
123	UDP	ntp	SNTP クライアント機能
161	UDP	snmp	SNMP 監視
162	UDP	snmptrap	SNMP TRAP 送信
80	TCP	http	WEB による監視機能
51967	TCP	－	モニタリングマネージャとの接続

（注 1）
Ethernet ポートと Network ポートのどちらか一方でのみ通信を行うことができます。

（注 2）
Ethernet ポート経由の場合，VLAN Tag なしパケットのみ通信を行うことができます。

（注 3）
Network ポート経由の場合，システムインタフェースへの通信中は Network ポートの帯域を使用します。ネットワーク上を流れるトラフィックをコントロールするための帯域を割り当てるときは，システムインタフェース通信の帯域も考慮して設定してください。トラフィックコントロールの設定の説明は「第 8 章 トラフィックコントロール機能」を参照してください。

（注 4）
システムインタフェースへの通信は，IPv4 のみサポートします。

（注 5）
IP フラグメントされていないパケットのみ通信を行うことができます。

システムインタフェースの設定には以下のコマンドを使用します。

set ip system	システムインタフェースの IPv4 アドレスとサブネットマスクを設定します。 IPv4 アドレスのデフォルト値は 192.168.1.1 です。サブネットマスクのデフォルト値は 255.255.255.0 です。
set ip system port	システムインタフェースの通信ポート（Ethernet ポート／Network ポート）を設定します。 また，システムインタフェースへの通信ポートとして Network ポートを指定した場合は，以下の内容も設定します。 - Network ポート識別番号（1/1，1/2，all） - VLAN ID（0～4094／none） Network ポート識別番号のデフォルト値は“all”（すべての Network ポート）です。VLAN ID のデフォルト値は“none”（VLAN Tag なしパケット通信）です。 通信ポートのデフォルト値は Ethernet ポートです。
set ip system gateway	システムインタフェースのデフォルトゲートウェイアドレスを設定します。
unset ip system gateway	システムインタフェースのデフォルトゲートウェイアドレスを解除します。
show ip system	システムインタフェース情報を表示します。

システムインタフェースに IPv4 アドレス（192.168.10.3），サブネットマスク（255.255.255.0），通信ポート（Ethernet ポート），デフォルトゲートウェイ（192.168.10.1）を設定する場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set ip system 192.168.10.3 netmask 255.255.255.0 up
PureFlow(A)> set ip system port ethernet
PureFlow(A)> set ip system gateway 192.168.10.1
```

システムインタフェースに IPv4 アドレス（192.168.10.3），サブネットマスク（255.255.255.0），通信ポート（Network ポート（1/1 のみ）），VLAN ID（10），デフォルトゲートウェイ（192.168.10.1）を設定する場合，以下に示すコマンドを実行します。

```
PureFlow(A)> set ip system 192.168.10.3 netmask 255.255.255.0 up
PureFlow(A)> set ip system port network in 1/1 vid 10
PureFlow(A)> set ip system gateway 192.168.10.1
```

また，システムインタフェースでは以下のコマンドを使用して，ネットワークの疎通確認をすることができます。

ping	ICMP ECHO_REQUEST パケットを指定 IPv4 アドレスに送信します。
arp	ARP エントリの内容を表示（-a），または削除（-d）します。ARP エントリは，最大 50 件まで学習します。

IPv4 アドレス 192.168.10.100 との疎通確認を行う場合，以下に示すコマンドを実行します。

```
PureFlow(A)> ping 192.168.10.100
192.168.10.100 is alive
PureFlow(A)> arp –a
IP address          MAC address                type
-------------------------------------------------------------------------------
192.168.10.3        00-00-91-01-11-23          permanent publish
192.168.10.100      00-00-91-01-23-45
PureFlow(A)>
```

疎通確認失敗時は，以下のように表示します。システムインタフェースの設定，およびネットワーク接続を確認してください。

```
PureFlow(A)> ping 192.168.10.101
no answer from 192.168.10.101
PureFlow(A)>
```

IPv4 アドレス 192.168.10.101 の ARP エントリを削除する場合，以下に示すコマンドを実行します。

```
PureFlow(A)> arp –d 192.168.10.100
PureFlow(A)> arp –a
IP address          MAC address                type
-------------------------------------------------------------------------------
192.168.10.3        00-00-91-01-11-23          permanent publish
PureFlow(A)>
```

7.3　システムインタフェースフィルタ

システムインタフェースへの通信を，ホストごとなどの単位で有効にしたり，無効にしたりすることができます。Ethernet ポートまたは Network ポート経由のどちらでも行うことができます。

システムインタフェースへの通信を識別するルールは，システムフィルタにより定義します。IP パケットの以下のフィールド，およびその組み合わせで定義します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- TOS
- プロトコル番号
- 送信元ポート番号（Sport）
- 宛先ポート番号（Dport）

システムインタフェースフィルタの設定には以下のコマンドを使用します。

add ip system filter	システムインタフェースのフィルタを設定します。
delete ip system filter	システムインタフェースのフィルタを削除します。
show ip system	システムインタフェース情報を表示します。

システムインタフェースに IPv4 アドレス（192.168.10.3），サブネットマスク（255.255.255.0）を設定し，IPv4 アドレス（192.168.10.100）のパソコンからのみ装置にアクセスできるようにする場合は，以下に示すコマンドを実行します。

```
PureFlow(A)> set ip system 192.168.10.3 netmask 255.255.255.0 up
PureFlow(A)> set ip system gateway 192.168.10.1
PureFlow(A)> add ip system filter 20 sip 192.168.10.100 permit
PureFlow(A)> add ip system filter 30 deny
```

システムインタフェースフィルタをすべて解除する場合は，以下に示すコマンドを実行します。

```
PureFlow(A)> delete ip system filter all
```

システムインタフェースフィルタの 30 を解除する場合は，以下に示すコマンドを実行します。

```
PureFlow(A)> delete ip system filter 30
```

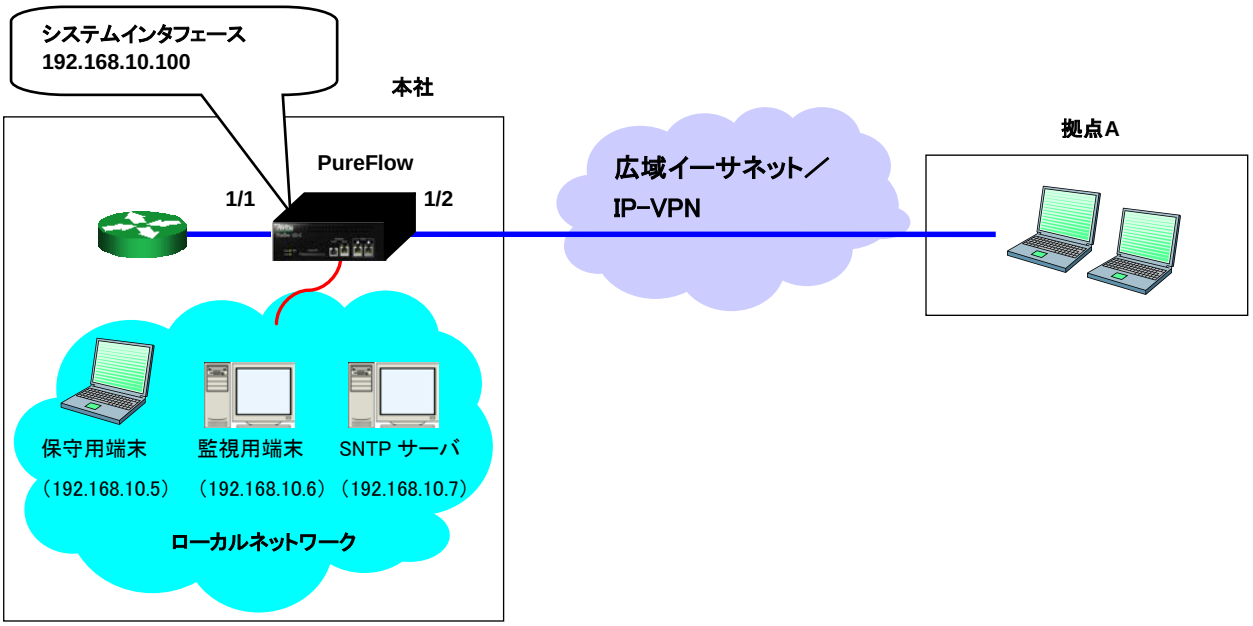
（注意）
システムインタフェースフィルタの設定は十分気をつけてください。
機能を有効にする場合は permit を初めに設定し，そのあとに deny の設定を行ってください。機能を削除する場合は，deny を初めに削除し，そのあと permit の削除を行ってください。または，delete ip system filter all コマンドですべてを削除してください。

7.4　コンフィギュレーション例

以下のネットワーク環境において，遠隔による保守／監視を行う場合のコンフィギュレーション例を示します。

[Case 1]ローカルネットワークから Ethernet ポートを経由して保守／監視を行う

- 本社内のローカルネットワークは 192.168.10.0/24 です。
- システムインタフェースの IPv4 アドレス 192.168.10.100，サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.10.1 です。
- 保守用端末（CLI，ダウンロード／アップロード）の IPv4 アドレス 192.168.10.5 です。
- 監視用端末（SNMP，Syslog）の IPv4 アドレス 192.168.10.6 です。
- SNTP サーバの IPv4 アドレス 192.168.10.7 です。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.10.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port ethernet
PureFlow(A)> set ip system gateway 192.168.10.1
```

＜SNMP ホスト設定＞

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community honsya_system_management view All
PureFlow(A)> add snmp host 192.168.10.6 version v2c
                community honsya_system_management trap
```

＜Syslog ホスト設定＞

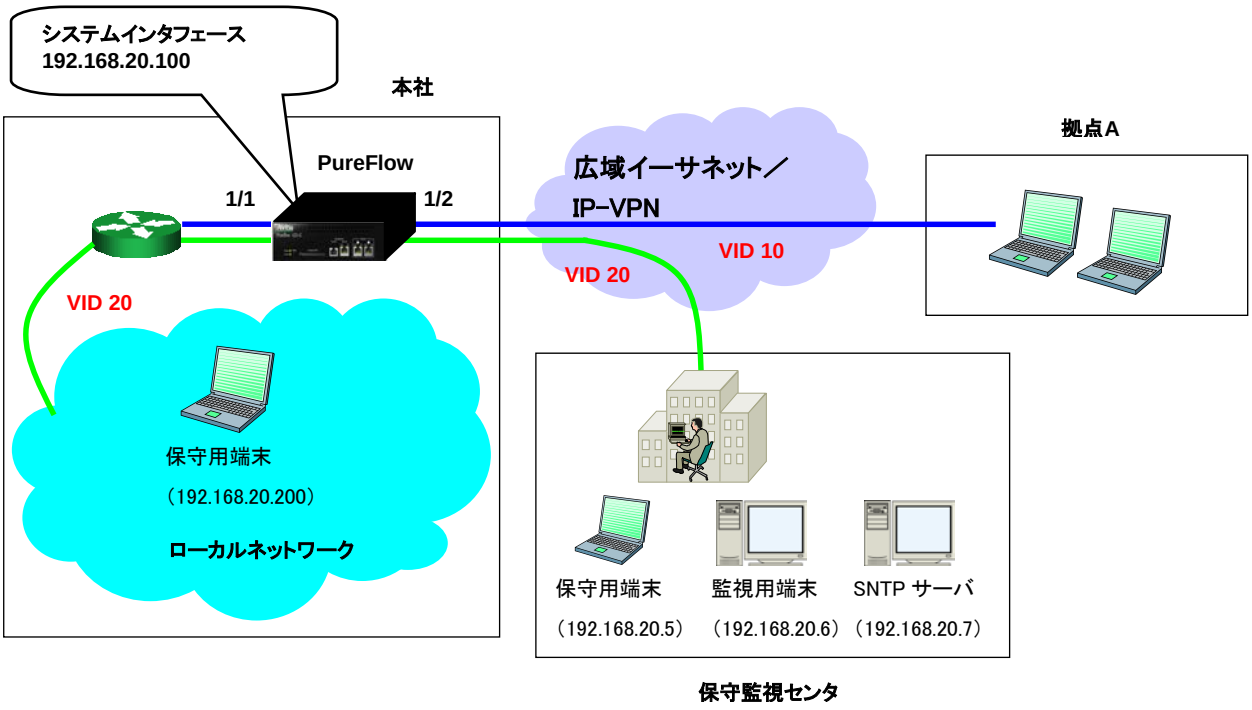
```
PureFlow(A)> set syslog host ip 192.168.10.6
PureFlow(A)> set syslog host enable
```

＜SNTP サーバ設定＞

```
PureFlow(A)> set sntp server 192.168.10.7
PureFlow(A)> set sntp enable
```

[Case 2]広域イーサネット／IP-VPN のネットワークとローカルネットワークから Network ポートを経由して保守／監視を行う（VLAN Tag ありパケット通信）

- 拠点 A へのネットワークは VLAN ID 10 です。
- 保守監視センタへのネットワークは VLAN ID 20 です。
- システムインタフェースの IPv4 アドレス 192.168.20.100，サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.20.1 です。
- すべての Network ポートからシステムインタフェースへの通信を行います。
- 保守用端末（CLI，ダウンロード／アップロード）の IPv4 アドレス 192.168.20.5，192.168.20.200 です。
- 監視用端末（SNMP，Syslog）の IPv4 アドレス 192.168.20.6 です。
- SNTP サーバの IPv4 アドレス 192.168.20.7 です。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.20.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port network in all vid 20
PureFlow(A)> set ip system gateway 192.168.20.1
```

＜SNMP ホスト設定＞

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community honsya_system_management view All
PureFlow(A)> add snmp host 192.168.20.6 version v2c
                community honsya_system_management trap
```

＜Syslog ホスト設定＞

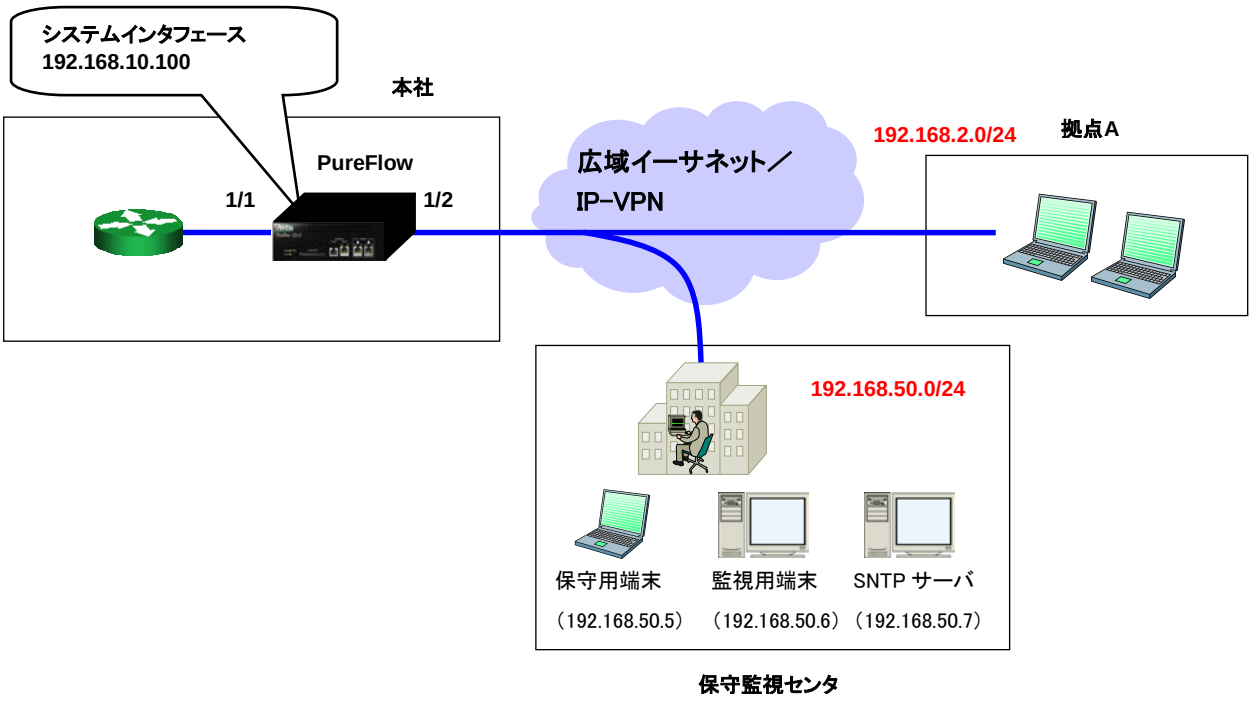
```
PureFlow(A)> set syslog host ip 192.168.20.6
PureFlow(A)> set syslog host enable
```

＜SNTP サーバ設定＞

```
PureFlow(A)> set sntp server 192.168.20.7
PureFlow(A)> set sntp enable
```

[Case 3]広域イーサネット／IP-VPN のネットワークから Network ポートを経由して保守／監視を行う（VLAN Tag なしパケット通信）

- 拠点 A へのネットワークは 192.168.2.0/24 です。
- 保守監視センタへのネットワークは 192.168.50.0/24 です。
- システムインタフェースの IPv4 アドレス 192.168.10.100，サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.10.1 です。
- Network ポート 1/2 からのみシステムインタフェースへの通信を行います。
- 保守用端末（CLI，ダウンロード／アップロード）の IPv4 アドレス 192.168.50.5 です。
- 監視用端末（SNMP，Syslog）の IPv4 アドレス 192.168.50.6 です。
- SNTP サーバの IPv4 アドレス 192.168.50.7 です。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.10.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port network in 1/2 vid none
PureFlow(A)> set ip system gateway 192.168.10.1
```

＜SNMP ホスト設定＞

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community honsya_system_management view All
PureFlow(A)> add snmp host 192.168.50.6 version v2c
                community honsya_system_management trap
```

＜Syslog ホスト設定＞

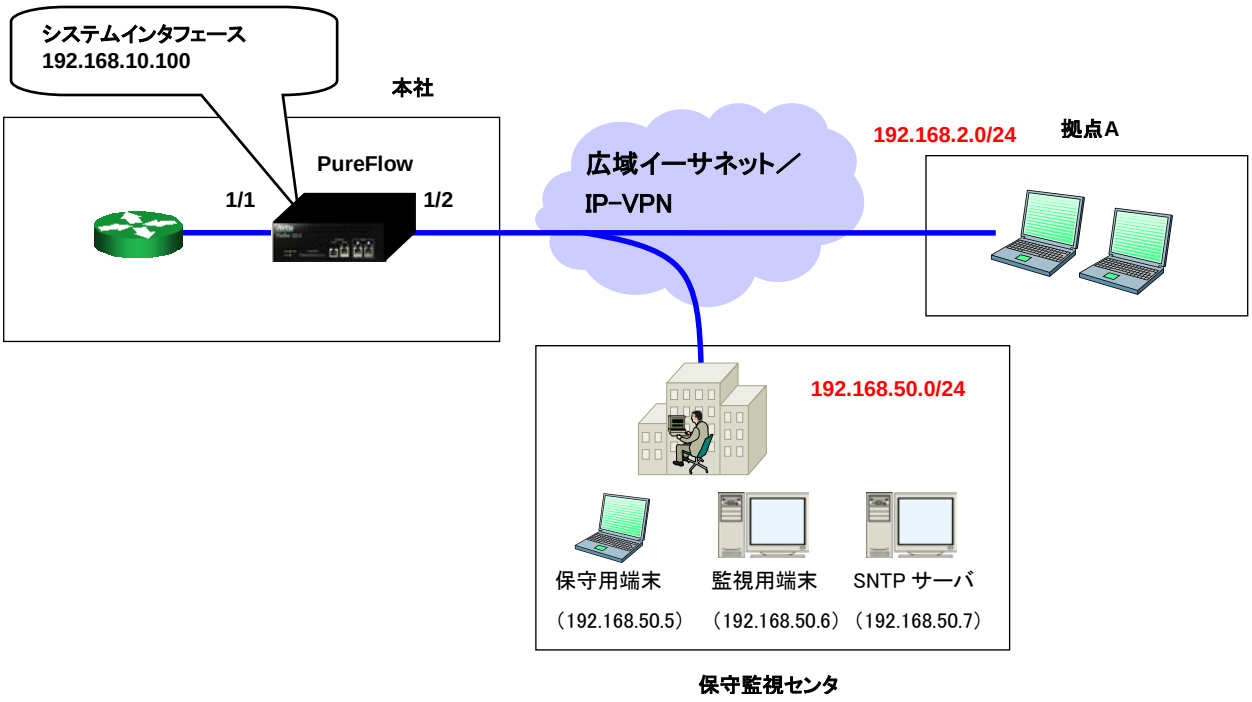
```
PureFlow(A)> set syslog host ip 192.168.50.6
PureFlow(A)> set syslog host enable
```

＜SNTP サーバ設定＞

```
PureFlow(A)> set sntp server 192.168.50.7
PureFlow(A)> set sntp enable
```

[Case 4]広域イーサネット／IP-VPN のネットワークから Network ポートを経由して保守／監視を行う（特定ネットワークからのアクセスのみ許可）

- 拠点 A へのネットワークは 192.168.2.0/24 です。
- 保守監視センタへのネットワークは 192.168.50.0/24 です。
- システムインタフェースの IPv4 アドレス 192.168.10.100，サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.10.1 です。
- Network ポート 1/2 からのみシステムインタフェースへの通信を行います。
- 保守用端末（CLI，ダウンロード／アップロード）の IPv4 アドレス 192.168.50.5 です。
- 監視用端末（SNMP，Syslog）の IPv4 アドレス 192.168.50.6 です。
- SNTP サーバの IPv4 アドレス 192.168.50.7 です。
- システムインタフェースへの通信は，保守監視センタからのみ許可します。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.10.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port network in 1/2 vid none
PureFlow(A)> set ip system gateway 192.168.10.1
```

＜フィルタ設定＞

```
PureFlow(A)> add filter 10000 ipv4 in 1/2 sip 192.168.50.0/255.255.255.0 dip 192.168.10.100
PureFlow(A)> set filter 10000 action forward
PureFlow(A)> add filter 10001 ipv4 in 1/2 dip 192.168.10.100
PureFlow(A)> set filter 10001 action discard
```

＜SNMP ホスト設定＞

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community honsya_system_management view All
PureFlow(A)> add snmp host 192.168.50.6 version v2c
                community honsya_system_management trap
```

＜Syslog ホスト設定＞

PureFlow(A)> set syslog host ip 192.168.50.6

PureFlow(A)> set syslog host enable

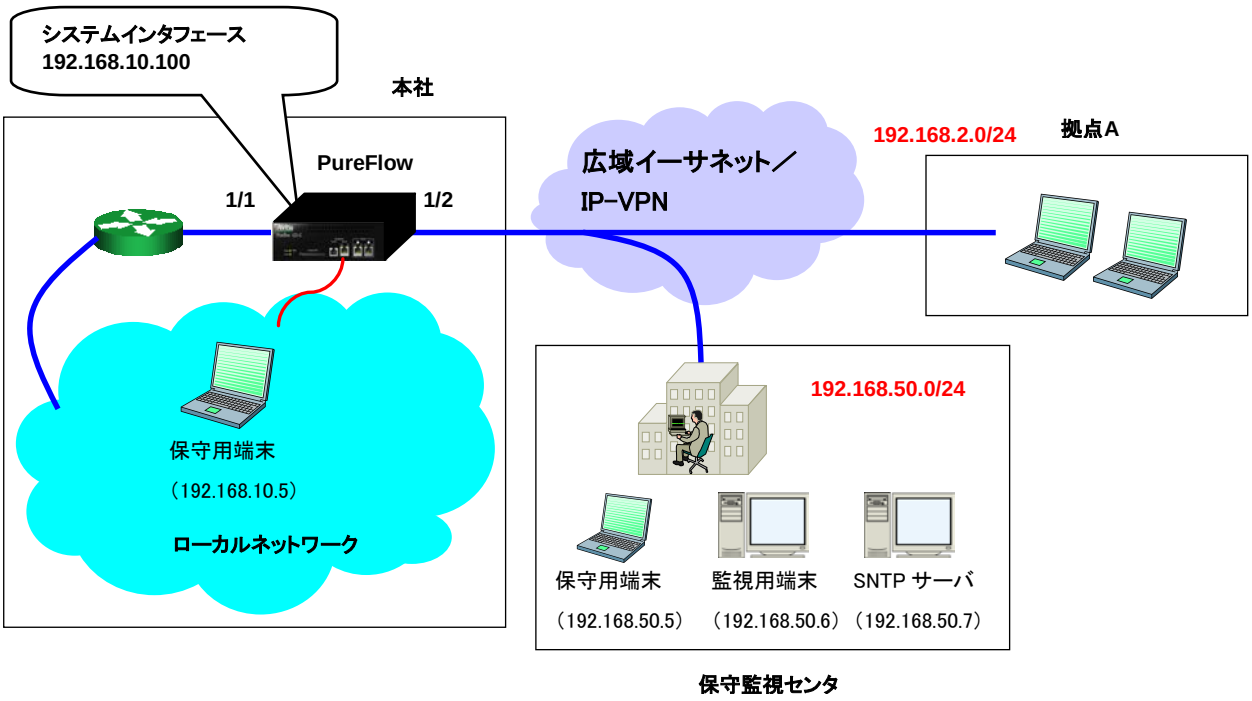
＜SNTP サーバ設定＞

PureFlow(A)> set sntp server 192.168.50.7

PureFlow(A)> set sntp enable

[Case 5]広域イーサネット／IP-VPN のネットワークとローカルネットワークから Ethernet ポートを経由して保守／監視を行う

- 本社内のローカルネットワークは 192.168.10.0/24 です。
- 拠点 A へのネットワークは 192.168.2.0/24 です。
- 保守監視センタへのネットワークは 192.168.50.0/24 です。
- システムインタフェースの IPv4 アドレス 192.168.10.100，サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.10.1 です。
- 保守用端末（CLI，ダウンロード／アップロード）の IPv4 アドレス 192.168.50.5，192.168.10.5 です。
- 監視用端末（SNMP，Syslog）の IPv4 アドレス 192.168.50.6 です。
- SNTP サーバの IPv4 アドレス 192.168.50.7 です。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.10.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port ethernet
PureFlow(A)> set ip system gateway 192.168.10.1
```

＜SNMP ホスト設定＞

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community honsya_system_management view All
PureFlow(A)> add snmp host 192.168.50.6 version v2c
                community honsya_system_management trap
```

＜Syslog ホスト設定＞

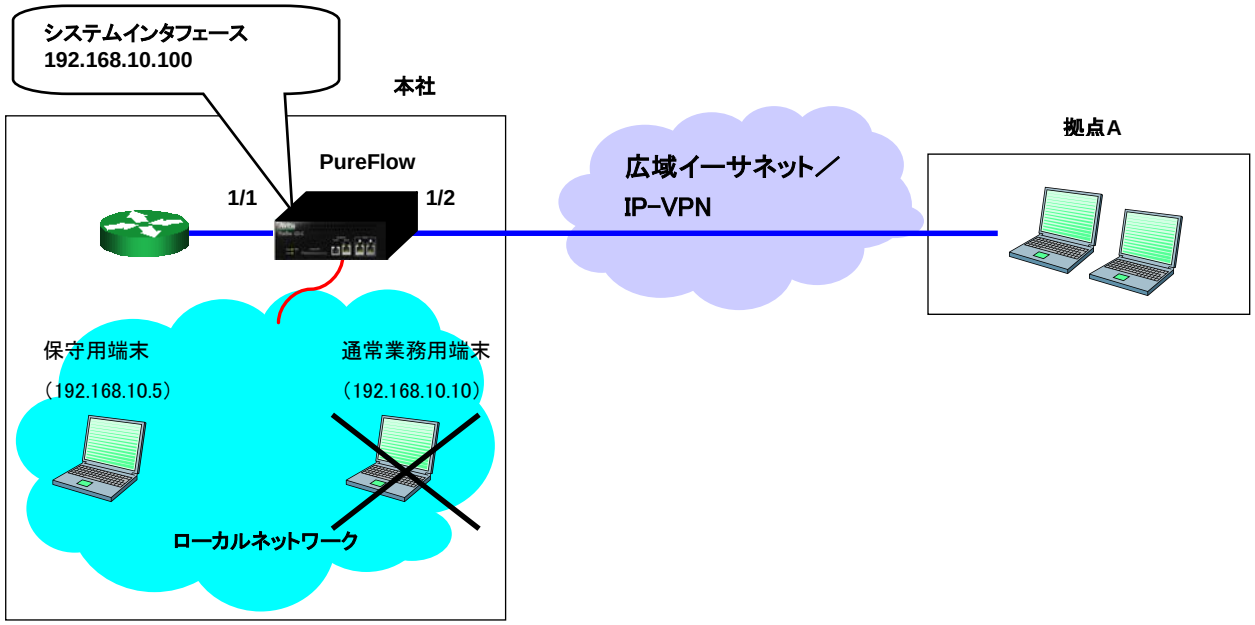
```
PureFlow(A)> set syslog host ip 192.168.50.6
PureFlow(A)> set syslog host enable
```

＜SNTP サーバ設定＞

```
PureFlow(A)> set sntp server 192.168.50.7
PureFlow(A)> set sntp enable
```

[Case 6]特定の端末から Ethernet ポートを経由して保守／監視を行う
不特定の端末からは監視を行わない

- 本社内のローカルネットワークは 192.168.10.0/24 です。
- システムインタフェースの IPv4 アドレス 192.168.10.100, サブネットマスク 255.255.255.0 です。
- システムインタフェースのデフォルトゲートウェイアドレス 192.168.10.1 です。
- 保守用端末(CLI, ダウンロード／アップロード)の IPv4 アドレス 192.168.10.5 です。
- 通常業務用端末の IPv4 アドレス 192.168.10.10 です。



以下のコマンドを実行します。

＜システムインタフェース設定＞

```
PureFlow(A)> set ip system 192.168.10.100 netmask 255.255.255.0 up
PureFlow(A)> set ip system port ethernet
PureFlow(A)> set ip system gateway 192.168.10.1
```

＜システムインタフェースフィルタ設定＞

```
PureFlow(A)> “add ip system filter 10 sip 192.168.10.5 permit”
PureFlow(A)> add ip system filter 20 deny
```

7.5　設定，状態の確認

システムインタフェースの設定コマンドで設定した内容を確認するには，“show ip system”コマンドを使用します。

```
PureFlow(A)> show ip system
Status          : Up
IP Address      : 192.168.10.3
Netmask         : 255.255.255.0
Broadcast       : 192.168.10.255
Default Gateway : 192.168.10.1
Port            : Network (1/2)
VID             : 20

Number of system filter entries: 0
PureFlow(A)>
```

システムインタフェースの統計情報を確認するには，“show counter”コマンドを使用します。本コマンドで表示するカウンタ長は，32 ビットです。

```
PureFlow(A)> show counter
Port      Rcv Octets   Rcv Packets   Trs Octets   Trs Packets
-------   ----------   -----------   ----------   -----------
 1/1        57566366      14194297            0             0
 1/2               0             0     59383412      14195494
system         58368           152        85424           152

Port      Rcv Broad    Rcv Multi    Trs Broad    Trs Multi
-------   ----------   ----------   ----------   ----------
 1/1           10000     14208097            0           0
 1/2               0            0        10000    14209615
system             5            0           10           0

Port      Err Packets   Collision    Discard
-------   -----------   ----------   ----------
 1/1                0            0           0
 1/2                0            0           0
system            N/A          N/A         N/A
```

また，システムインタフェースをコマンド引数に指定することにより，詳細内容を表示できます。本コマンドで表示する Rcv Packets, Rcv Broad, Rcv Multi, Rcv Octets, Trs Packets, Trs Broad, Trs Multi, Trs Octets のカウンタ長は，64 ビットです。

```
PureFlow(A)> show counter system
Rcv Packets                          152
Rcv Broad                              5
Rcv Multi                              0
Rcv Octets                         58368
Rcv Rate                             N/A
Trs Packets                          152
Trs Broad                             10
Trs Multi                              0
Trs Octets                         85424
Trs Rate                             N/A
Collision                            N/A
Drop                                 N/A
Discard                              N/A
Error Packets                        N/A
       CRC Align Error                          N/A
       Undersize Packet                         N/A
       Oversize Packet                          N/A
```

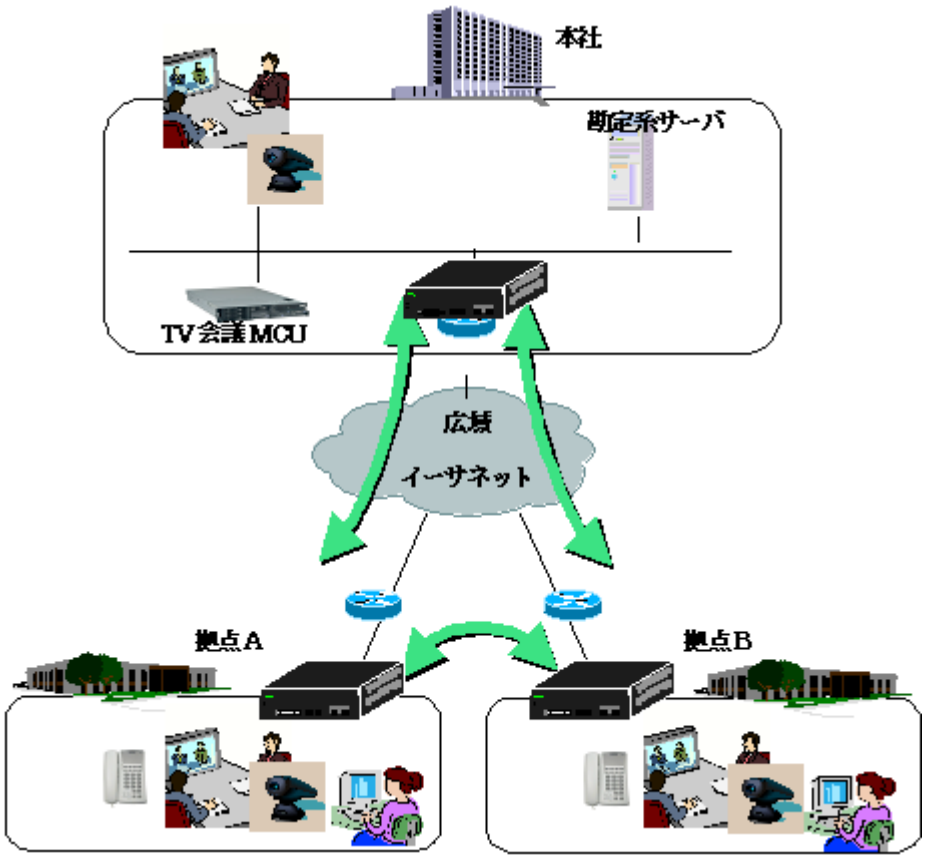
ここでは，トラフィックコントロール機能と設定について説明します。

8.1　概要

従来の専用線やATM回線に変わり，より高速で低コストのIP-VPNや広域イーサネットサービスにより拠点間を接続する形態が普及してきました。専用線やATM回線と異なり，IP-VPNや広域イーサネットはQoSが保証されないパケット交換網を使用します。IP-VPNや広域イーサネットの回線は，通信事業者から提供され，回線速度や最大帯域が規定されていますが，特定のユーザやアプリケーションが回線の帯域を多く占有してしまうと，その他のユーザやアプリケーションが利用できる回線帯域が不足したり，通信遅延が発生するなどの障害が起こります。

このような通信品質の劣化は，音声通信やTV会議などのミッションクリティカルな業務効率を低下させ，重大な支障をきたすことにつながります。こうしたミッションクリティカルなトラフィックを回線帯域不足や通信遅延から守るために，回線帯域を拠点やユーザ，またはアプリケーションごとに分割し，必要な帯域を割り当てたり，トラフィックの優先制御を行う必要があります。回線帯域を分割し，割り当てた帯域に対して最低帯域を保証したり，最大帯域制限を行うことをトラフィックコントロールと呼びます。

大規模な企業ネットワークでは，トラフィックコントロールを拠点やユーザ，またはアプリケーションごとに複雑に組み合わせる必要があります。たとえば，特定ユーザ（拠点A）に2 Mbit/sの帯域を割り当て，さらにその帯域内でVoIPに70 kbit/sの帯域を保証するといった階層的なトラフィックコントロールが必要とされます。本装置では，回線帯域を分割し，必要な帯域を割り当て，さらにその帯域内で帯域を再分割することを階層化シェーピングと呼びます。また，音声通信やTV会議などのアプリケーショントラフィックを認識し，各アプリケーションのメディアセッション（制御セッション／音声セッション／映像セッション／データセッション）ごとに必要な帯域を割り当て，最適なトラフィックコントロール（コンテンツ・アウェア・シェーピング）を行うこともできます。



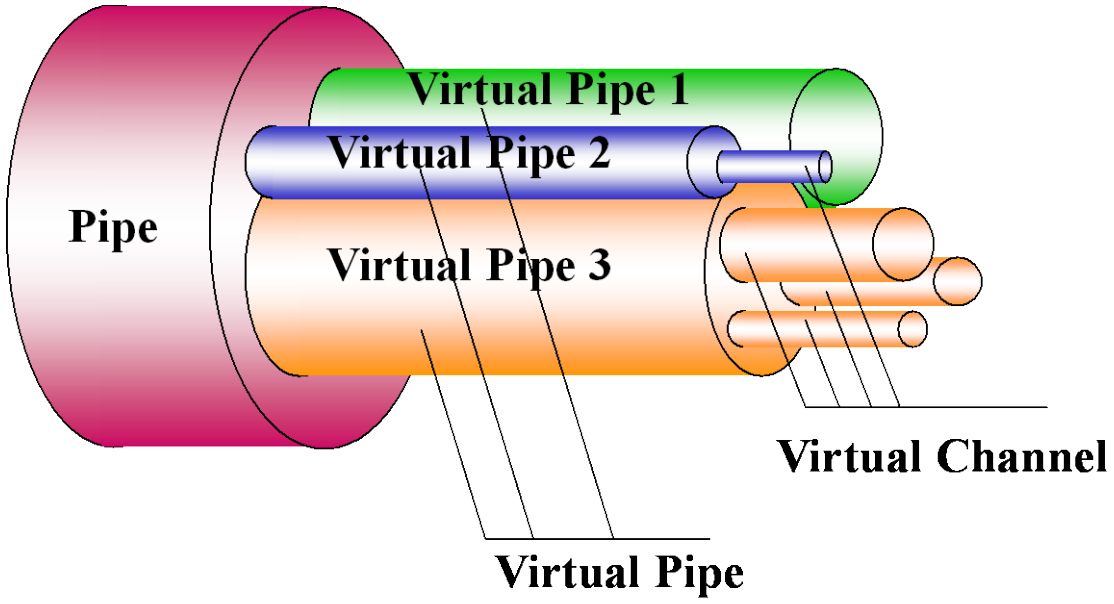
8.2　階層化シェーピング

階層化シェーピングは，拠点やユーザ向けに回線帯域を分割し，必要な帯域を割り当て，さらにその帯域内でアプリケーションごとに帯域を割り当てるといった階層的なトラフィックコントロールです。

本装置は，回線上のパケットを分類し，拠点やユーザなどのトラフィックを抽出します。抽出したトラフィックを Virtual Pipe（仮想パイプ）という仮想回線に流します。Virtual Pipe ごとに回線帯域を分割し，それぞれに個別の帯域を割り当てることができます。

Virtual Pipe に割り当てた帯域は，さらにその帯域内で再分割することができます。Virtual Pipe を流れるトラフィックをさらに細かく分類し，特定のアプリケーションのトラフィックを抽出します。抽出したトラフィックを Virtual Channel（仮想チャネル）という論理的な通信経路に流します。Virtual Channel は Virtual Pipe に割り当てた帯域を再分割し，帯域を割り当てることができます。

以下に，階層化シェーピングの概念を示します。



Pipe（パイプ）：
　入力 Network ポートと出力 Network ポートの組み合わせで，回線帯域となります。
　パイプを通過する総帯域を，トラフィックコントロール（帯域制御）します。
　（パイプの総帯域を制御するには「GS1 ライセンスキー2」が必要です。）

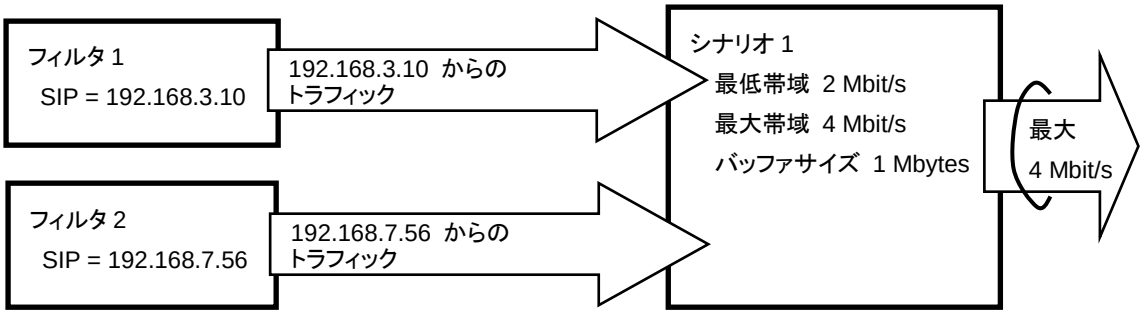
Virtual Pipe（仮想パイプ）：
　パイプ内の帯域を分割し，トラフィックコントロール（帯域保証）します。
　仮想パイプは 1 つ，または複数の仮想チャネルを集約でき，
　仮想チャネルの論理的なグループとなります。

Virtual Channel（仮想チャネル）：
　仮想パイプ内の帯域を再分割し，
　トラフィックコントロール（最低帯域保証／最大帯域制限）します。
　特定のアプリケーションやホストからのトラフィックを制御する単位で，
　論理的な通信経路となります。

8.3　フィルタとシナリオ

本装置は，パイプ上に流れるパケットをフィルタルールにより分類し，トラフィックを抽出します。フィルタルールにより分類されたトラフィックは，シナリオと呼ばれるトラフィックアトリビュート（最低帯域，最大帯域，バッファサイズ）に従ってトラフィックコントロールします。

複数のフィルタを同じシナリオに結び付けることが可能で，複数ユーザやアプリケーションで共有する帯域を割り当てることもできます。



SIP：送信元 IP アドレス

8.3.1　フィルタ

パケットを分類するルールは，フィルタにより定義します。Ethernet フレーム，もしくは IP パケットの以下のフィールド，およびその組み合わせで定義し，トラフィックを抽出します。

・Ethernet フレーム

VLAN ID，CoS

・IPv4／IPv6 パケット

IPv4　IP アドレス，プロトコル番号，ポート番号，ToS
IPv6　IP アドレス，プロトコル番号，ポート番号，トラフィッククラス

フィルタには，VLAN Tag フィールドのみ分類する VLAN フィルタと VLAN Tag フィールド，IP ヘッダ，TCP／UDP ヘッダのすべてを分類する IP フィルタの 2 種類があります。

1. VLAN フィルタとは，Ethernet フレーム（ARP パケット，IP パケットなど）を対象にしたフィルタです。IEEE802.1p 準拠の VLAN Tag フィールドにより Ethernet フレームを分類したい場合に使用します。たとえば，VLAN ID＝1と，VLAN ID＝2のネットワークがある場合に，各 VLAN ID ごとにフローを作成し，帯域を制御することが可能です。
   以下の Ethernet フレームフィールドをフィルタ識別します。

   - VLAN ID（VLAN Tag あり／なしも識別）
   - CoS

   VLAN Tag が複数付いているパケットを受信した場合，パケット先頭の VLAN Tagged フィールドから VLAN ID と CoS を抽出し，フィルタ識別します。

2. IP フィルタとは，IP パケット（ARP パケットなどは含まれません）を対象にしたフィルタです。IP パケットフィールドにより IP パケットを分類したい場合に使用します。
以下の IP パケットフィールドをフィルタ識別します。

- VLAN ID （VLAN Tag あり／なしも識別）
- CoS
- 送信元 IP アドレス（SIP）
- 宛先 IP アドレス（DIP）
- ToS またはトラフィッククラス
- プロトコル番号
- 送信元ポート番号（Sport）
- 宛先ポート番号（Dport）
- アプリケーション名

本装置では，アプリケーション名を指定した IP フィルタをアプリケーションフィルタと呼び，アプリケーションフィルタに一致したトラフィックをアプリケーション認識します。アプリケーションフィルタを使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。（アプリケーションフィルタの詳細は，「第 9 章 コンテンツ・アウェア・シェーピング機能」を参照してください）

VLAN Tag が複数付いているパケットを受信した場合，このパケットを IP 以外のパケットとしてフィルタ識別され，IP フィルタではパケット分類されません。

8.3.2　フィルタの親子関係

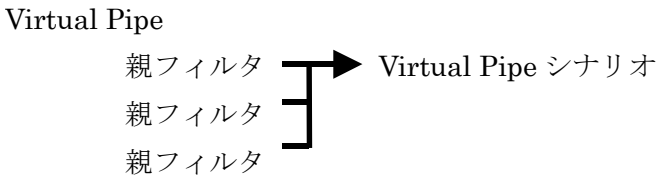
階層化シェーピングを行うために，フィルタ／シナリオに親子関係を持たせて組み合わせる必要があります。Virtual Pipe 内に流すトラフィックを抽出するためのフィルタを親フィルタ，Virtual Channel 内に流すトラフィックを抽出するためのフィルタを子フィルタと呼び，親フィルタと子フィルタに親子関係を作成することで，Virtual Pipe と Virtual Channel の組み合わせができます。

Virtual Pipe 内に流すトラフィックは，親フィルタにより分類します。親フィルタにより抽出されたトラフィックは，Virtual Pipe シナリオというトラフィックアトリビュートによって，トラフィックコントロールを行います。

1. 親フィルタとは，Virtual Pipe 内に流すパケットを分類するためのフィルタです。

2. Virtual Pipe シナリオとは，Virtual Pipe のトラフィックコントロールを行うためのパラメータです。

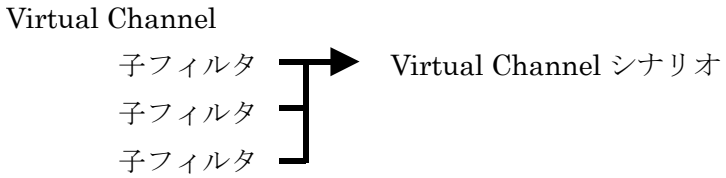
親フィルタと Virtual Pipe シナリオを結び付けることで Virtual Pipe を作成することができます。また，同じ Network ポートのフィルタ条件ならば複数の親フィルタを同じ Virtual Pipe シナリオに結び付けることも可能です。



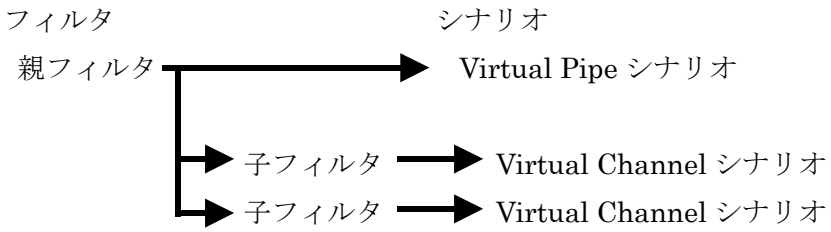
Virtual Channel 内に流すトラフィックは，子フィルタにより分類します。子フィルタにより抽出されたトラフィックは，Virtual Channel シナリオというトラフィックアトリビュートによって，トラフィックコントロールを行います。

1. 子フィルタとは，Virtual Channel 内に流すパケットを分類するためのフィルタです。
2. Virtual Channel シナリオとは，Virtual Channel のトラフィックコントロールを行うためのパラメータです。

子フィルタとVirtual Channelシナリオを結び付けることでVirtual Channelを作成することができます。また，同じNetworkポートのフィルタ条件ならば複数の子フィルタを同じVirtual Channelシナリオに結び付けることも可能です。ただし，Virtual Channelシナリオを複数のVirtual Pipeシナリオと組み合わせることはできません。



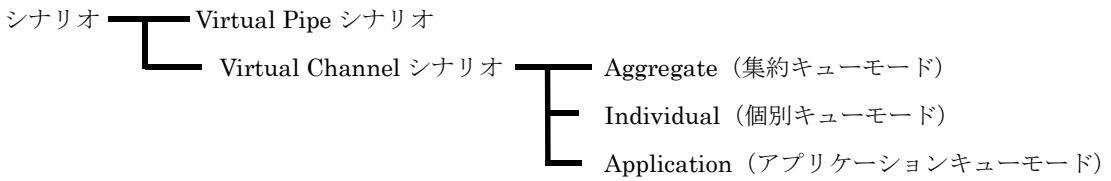
この親フィルタと子フィルタに親子関係を作成することで，Virtual PipeとVirtual Channelの組み合わせができ，階層化シェーピングを行うことができます。



8.3.3　シナリオ

シナリオは，フィルタにより抽出されたトラフィックに対して，トラフィックコントロールを行うための設定（トラフィックアトリビュート）です。シナリオには，Virtual Pipe 用のシナリオと Virtual Channel 用のシナリオの 2 種類があります。

さらに，Virtual Channel 用のシナリオには，トラフィックをひとつの固まりとしてコントロールする Aggregate（集約キューモード）と，トラフィック内をさらに個々のフロー（装置内で識別できるトラフィックの最小単位）ごとに識別し，各フローごとにトラフィックコントロールする Individual（個別キューモード）と，アプリケーションフィルタにより認識したアプリケーションのメディアセッションごとにトラフィックコントロールする Application（アプリケーションキューモード）があります。アプリケーションキューモード機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。（アプリケーションキューモードの詳細は，「第 9 章 コンテンツ・アウェア・シェーピング機能」を参照してください）。トラフィックは，複数のフローからなるグループと考えることができます（フローの詳細は 8.6.1 章を参照してください）。



1. Virtual Pipe シナリオとは，Virtual Pipe 内に入力されたトラフィックをコントロールするためのパラメータです。指定できるものは保証帯域，デフォルトバッファサイズです。

   - 保証帯域 ： Virtual Pipe に割り当てる保証帯域です。ほかの Virtual Pipe 内にトラフィックが流れている状態でも，この帯域を保証します。

   - デフォルトバッファサイズ ： Virtual Pipe に割り当てるキューで許容できる入力バースト長（バイト）です。入力バースト長を超えると，パケットは廃棄されます（デフォルト値が設定されるので，通常は設定する必要ありません）。

   Virtual Pipe には，以下のキューが割り当てられます。

   - VP デフォルトキュー ： Virtual Pipe に割り当てるキューを VP デフォルトキューと呼びます。VP デフォルトキューは，Virtual Pipe 内で Virtual Channel に該当しないトラフィックを転送するためのキューです（キューの詳細は 8.6.2 章を参照してください）。

2. Virtual Channelシナリオとは，Virtual Channel内に入力されたトラフィックをコントロールするためのパラメータです。指定できるものはクラス，最低帯域，最大帯域，バッファサイズです。

   - クラス　：　キューの優先順位です。クラス1が最優先とし以下クラス2，3，4，5，6，7，8 の順となります（デフォルト値が設定されるので，通常は設定する必要ありません）。

   - 最低帯域　：　Virtual Channelに割り当てる最低帯域です。優先度が高いクラスに割り当てられたトラフィックは，ほかのトラフィックが流れている状態でも，この最低帯域を保証します。指定しない場合は，最低帯域を保証しません。

   - 最大帯域　：　Virtual Channelに割り当てる最大帯域です。指定しない場合は，Virtual Pipeの保証帯域でトラフィックコントロールします。

   - バッファサイズ　：　Virtual Channelに割り当てるキューで許容できる入力バースト長です。入力バースト長を超えると，パケットは廃棄されます（デフォルト値が設定されるので，通常は設定する必要ありません）。

   Application（アプリケーションキューモード）では，アプリケーションフィルタにより認識したアプリケーションのメディアセッションごとに必要な帯域とバッファサイズを割り当てることができます（コンテンツ・アウェア・シェーピングの詳細は，「第 9 章 コンテンツ・アウェア・シェーピング機能」を参照してください）。

   Virtual Channelには，以下のキューが割り当てられます。

   - VCキュー　：　Virtual Channelに割り当てるキューをVCキューと呼びます。VCキューは，Virtual Channelに該当するトラフィックを転送するためのキューです（キューの詳細は8.6.2章を参照してください）。

   また，VCキューには，以下3種類のキュー割り当てモードがあります。

   - Aggregate（集約キューモード）：トラフィックをひとつの固まりとしてコントロールします（複数のフローを1つのVCキューに割り当てます）。

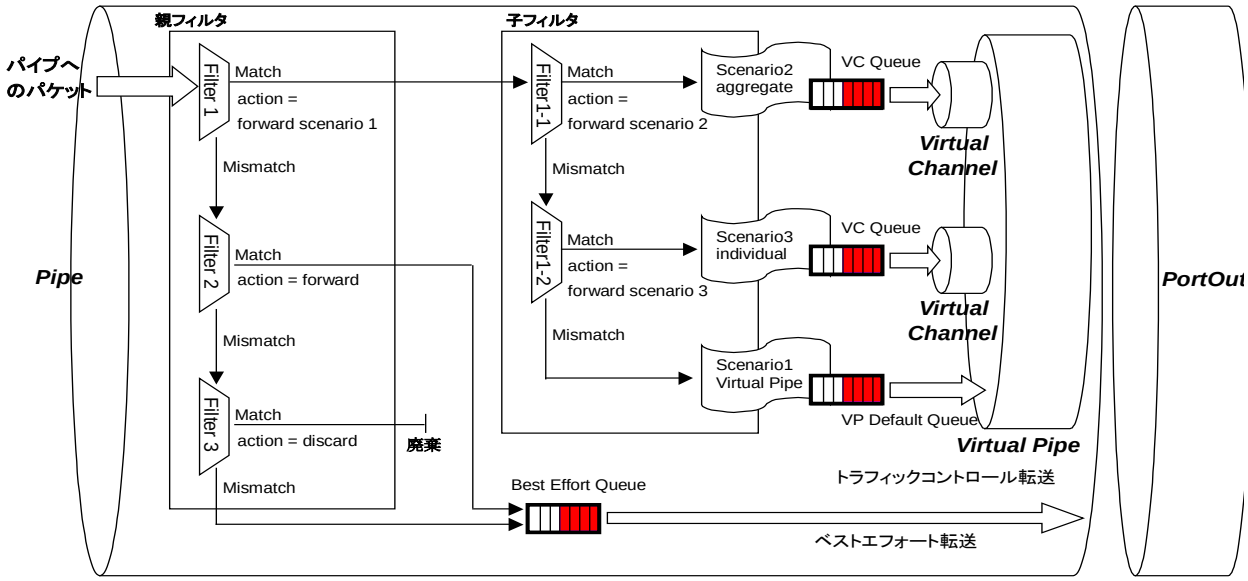
   - Individual（個別キューモード）：トラフィック内をさらに個々のフローごとに識別し，各フローごとにトラフィックコントロールします（複数のフローを個別のVCキューに割り当てます）。

   - Application（アプリケーションキューモード）：アプリケーションフィルタにより認識したアプリケーションのメディアセッションごとにトラフィックコントロールします。アプリケーションキューモード機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。（アプリケーションキューモードの詳細は，「第 9 章 コンテンツ・アウェア・シェーピング機能」を参照してください）。

また，Virtual Pipe／Virtual Channelシナリオには，シナリオ名を設定することが可能です。シナリオ名に拠点やユーザの名前を設定しておくと，各 Virtual Pipe／Virtual Channelシナリオの管理が容易になります。

8.3.4　フィルタとシナリオの関係

本装置は，Pipe 内に流れるパケットをフィルタで分類し，トラフィックを抽出します。抽出したトラフィックを帯域，バッファサイズなどのトラフィックアトリビュートに従ってトラフィックコントロール転送します。



上図は，フィルタとシナリオの設定と，実際のトラフィックコントロール動作の関係を示した概念図です。Pipe，Virtual Pipe，Virtual Channel での帯域制御，および，フィルタ設定による廃棄，転送が制御可能です。（Pipe の最大帯域，および，Virtual Pipe の最低帯域を設定するにはライセンスキー2 が必要です。）

フィルタの動作は，“forward scenario”，“forward”，“discard”の指定が可能です。フィルタのルールに一致したパケットは，フィルタに設定した動作に従います。

装置はパケットが Pipe に入ってくると，親フィルタを通過し，親フィルタインデックスの若い順から親フィルタルールと一致するかどうか調べます。

ある親フィルタルールと一致した場合，親フィルタの動作が“forward scenario”の場合は，その親フィルタと親子関係のある子フィルタを通過し，子フィルタインデックスの若い順から子フィルタルールと一致するかどうか調べます。“forward”の場合は，トラフィックコントロールを行わずに，パケットをベストエフォート転送します。“discard”の場合は，パケットを廃棄します。

親フィルタを“forward”，または“discard”にした場合，その親フィルタと親子関係にある子フィルタは無効となります。子フィルタ条件に一致するトラフィックであっても，親フィルタに設定した動作に従います。

ある子フィルタルールと一致した場合，子フィルタの動作が“forward scenario”の場合は，Virtual Channel シナリオで指定されたトラフィックアトリビュートに従って，Virtual Channel 内でパケットを転送します。“forward”の場合は，Virtual Pipe シナリオで指定されたトラフィックアトリビュートに従って，Virtual Pipe 内でパケットを転送します。“discard”の場合は，パケットを廃棄します。また，子フィルタルールと一致しない場合も，Virtual Pipe 内で転送します。

フィルタには，VLAN フィルタか IP フィルタの指定が可能です。VLAN フィルタは，親フィルタインデックス，子フィルタインデックスとも 1 から 4096 まで使用できます。IP フィルタは，親フィルタインデックス，子フィルタインデックスとも 10000 から 14095 まで使用できます。優先順位は，インデックスの若いほうが優先となります。

8.3.5　ルールリスト

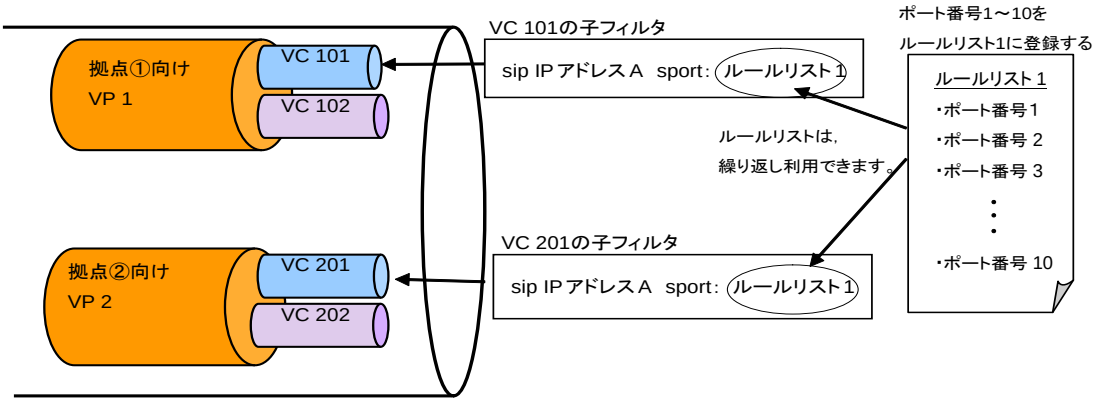
ルールリストは，複数のトラフィック分類条件（IP アドレスやポート番号）をグループ化する機能です。これにより，複数のトラフィック分類条件を単一のルールリスト名で指定することができます。

ルールリスト名をフィルタ追加コマンドの引数に指定することで，トラフィック分類条件として設定することとができます。

ルールリストに指定可能なトラフィック分類条件は，以下の通りです。

① IPv4 アドレス　　：IP アドレスとビットマスク
② IPv6 アドレス　　：IP アドレスとビットマスク
③ L4 ポート番号　　：ポート番号範囲

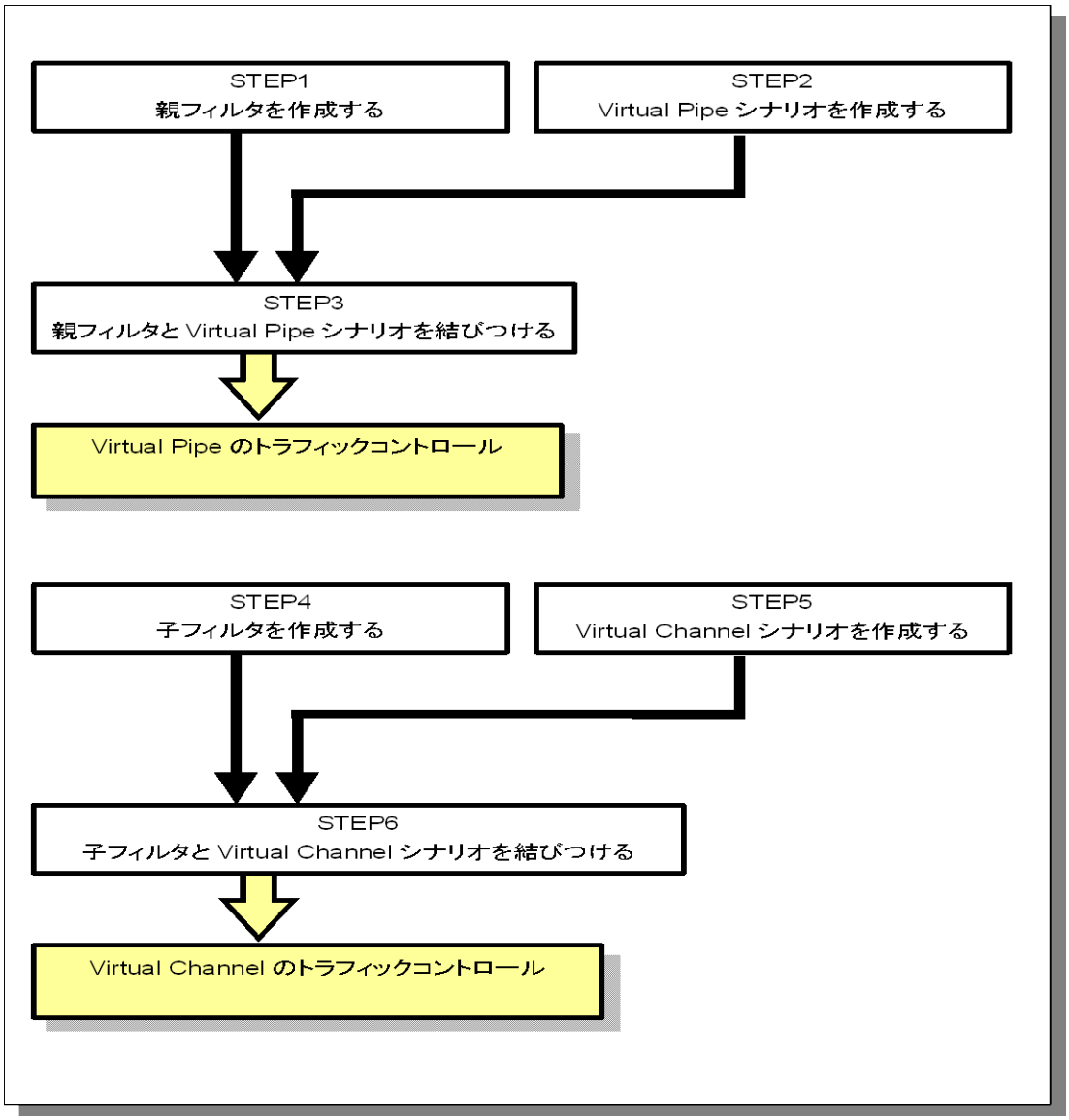
ルールリストは複数のフィルタで繰り返し指定できます。ルールリストを使用することでフィルタ数や設定行数を削減できます。



上図は，ルールリストの設定と，実際のトラフィックコントロール動作の関係を示した概念図です。この概念図では，ルールリスト1に，複数の TCP/UDP ポート番号を登録しておき，VC101 と VC201 のフィルタ追加コマンドにおいて，sport（送信元ポート番号）のパラメータとして利用しています。

8.4　設定方法

設定方法の流れをまとめると下図のようになります。



次に，流れに沿って設定方法を説明します。

STEP 1： 親フィルタの設定

本装置は，Ethernet フレーム，IPv4 パケット，IPv6 パケットのトラフィックを親フィルタによりフィルタ識別します。

親フィルタに設定できるパラメータを，以下に示します。

パラメータ		設定範囲	省略可能／不可
親フィルタインデックス		1 – 4096（VLAN）， 10000 – 14095（IPv4/IPv6）	不可
フィルタタイプ		vlan, ipv4, ipv6	不可
入力 Network ポート		1/1 – 1/2	不可
VLAN ID		0 – 4094（範囲指定可能）， none（VLAN Tag なし）	可能
CoS		0 – 7（VLAN フィルタのみ範囲指定可能）	可能
送信元 IP アドレス／マスク	IPv4	0.0.0.0 – 255.255.255.255 ルールリスト名	可能 IP フィルタのみ有効
	IPv6	0::0 – FFFF:...:FFFF （小文字入力可能） ルールリスト名	可能 IP フィルタのみ有効
宛先 IP アドレス／マスク	IPv4	0.0.0.0 – 255.255.255.255 ルールリスト名	可能 IP フィルタのみ有効
	IPv6	0::0 – FFFF:...:FFFF （小文字入力可能） ルールリスト名	可能 IP フィルタのみ有効
ToS，または Traffic Class	IPv4	0 – 255（範囲指定可能）	可能 IP フィルタのみ有効
	IPv6	0－255（範囲指定可能）	可能 IP フィルタのみ有効
プロトコル番号		0 – 255（範囲指定可能） （tcp，udp，icmp は文字入力可能）	可能 IP フィルタのみ有効
送信元ポート番号		0 – 65535（範囲指定可能） ルールリスト名	可能 IP フィルタのみ有効
宛先ポート番号		0 – 65535（範囲指定可能） ルールリスト名	可能 IP フィルタのみ有効
アプリケーション名		h323（H.323） h323.control（H.323 制御セッション） h323.voice（H.323 音声セッション） h323.video（H.323 映像セッション） h323.data（H.323 データセッション） sip（Session Initiation Protocol） sip.control（SIP 制御セッション） sip.voice（SIP 音声セッション） sip.video（SIP 映像セッション） sip.data（SIP データセッション） ftp（File Transfer Protocol ftp.control（FTP 制御セッション） ftp.data（FTP データセッション）	可能 IP フィルタのみ有効 本機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。

親フィルタの設定に関する CLI は以下のコマンドです。

add filter <filter_idx> vlan in <slot/port> [vid {<VID> | none}] [cos <user_priority>]	親 VLAN フィルタを追加します。 Ethernet フレームをフィルタの対象にします。
add filter <filter_idx> ipv4 in <slot/port> [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv4 フィルタを追加します。 IPv4 パケットのみをフィルタの対象にします。
add filter <filter_idx> ipv6 in <slot/port> [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv6 フィルタを追加します。 IPv6 パケットのみをフィルタの対象にします。
add filter subrule <filter_idx> <subrule_idx> vlan [vid {<VID> | none}] [cos <user_priority>]	親 VLAN フィルタにサブルールを追加します。
add filter subrule <filter_idx> <subrule_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv4 フィルタにサブルールを追加します。
add filter subrule <filter_idx> <subrule_idx> ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv6 フィルタにサブルールを追加します。
delete filter subrule <filter_idx> { <subrule_idx>| all}	サブルールを削除します。
delete filter {<filter_idx> | all}	親フィルタを削除します。
show filter [<filter_idx>] [summary]	親フィルタを表示します。

親フィルタは，以下のルールに従って設定してください。

(1) 親フィルタの識別に用います。装置内で重複しないユニークな値を設定してください。

(2) パケットが入力された場合，親フィルタに一致するかを検査しますが，この親フィルタインデックスは，パケットを検査する順序を示します。パケットが複数のフィルタルールに一致する場合，親フィルタインデックスの小さいフィルタに一致したとみなされ，親フィルタインデックスの大きいほうの親フィルタは検査されません。

(3) “add filter”コマンドで，省略可能なパラメータを省略した場合は，そのパラメータは検査されません(すべて一致と見なされます)。

(4) 親フィルタのフィルタルールにOR条件を追加する場合は，サブルールを設定してください。親フィルタのフィルタルールに一致するトラフィックと，サブルールに一致するトラフィックの両方を，親フィルタに一致したトラフィックとして制御します。

(5) ルールリストエントリが登録されていないルールリストをフィルタのパラメータに設定した場合，フィルタには一致しません。

親フィルタの設定を変更する CLI は以下のコマンドです。

renew filter <filter_idx> vlan [vid {<VID>|none}] [cos <user_priority>]	親 VLAN フィルタの分類条件を新しく設定します。
renew filter <filter_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv4 フィルタの分類条件を新しく設定します。
renew filter <filter_idx> ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	親 IPv6 フィルタの分類条件を新しく設定します。
renew filter subrule <filter_idx> {<subrule_idx>} vlan [vid {<VID>|none}] [cos <user_priority>]	サブルールの分類条件を新しく設定します。
renew filter subrule <filter_idx> <subrule_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	サブルールの分類条件を新しく設定します。
renew filter subrule <filter_idx> {<subrule_idx>} ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	サブルールの分類条件を新しく設定します。

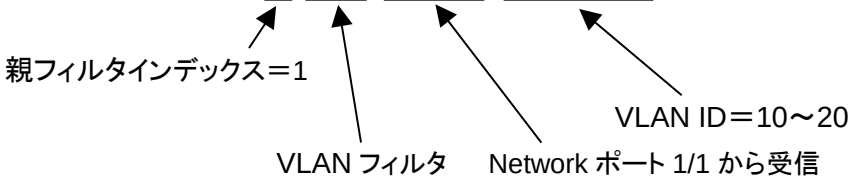
注 1）renew filter コマンドは，新たに指定されたフィルタルールのみを再登録します。
add filter コマンドで指定したフィルタルールは，消去されます。

注 2）renew filter コマンドは，set filter コマンドで指定された action を保持します。
すでに，set filter コマンドで action が設定されている filter に対して，再度，set filter コマンドを入力する必要はありません。

以下に，親フィルタのサンプルを設定するコマンドを示します。

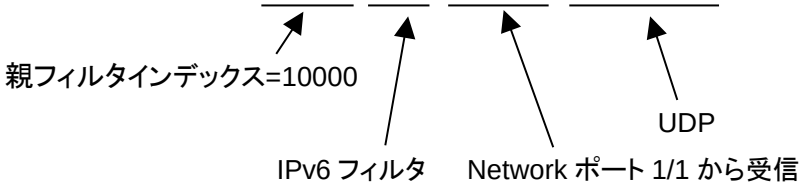
Sample 1）　Network ポート 1/1 から受信する Ethernet フレームで VLAN ID が 10～20 のフレームに対するフィルタ

```
PureFlow(A)> add filter 1 vlan in 1/1 vid 10-20
```



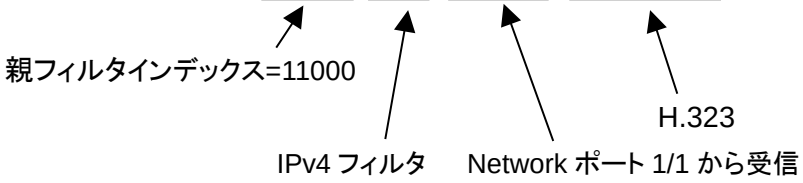
Sample 2）　Network ポート 1/1 から受信する IPv6 パケットで UDP のパケットに対するフィルタ

```
PureFlow(A)> add filter 10000 ipv6 in 1/1 proto udp
```



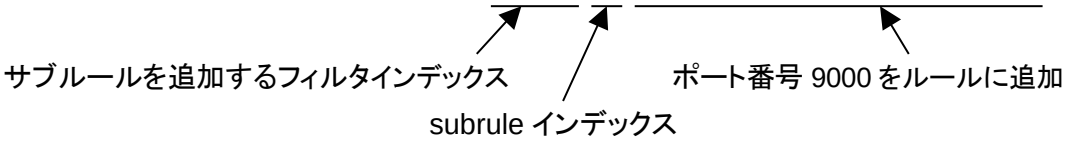
Sample 3）　Network ポート 1/1 から受信する IPv4 パケットで H.323 に対するフィルタ

```
PureFlow(A)> add filter 11000 ipv4 in 1/1 appli h323
```



Sample 4）　ソースポート番号 8000 と 9000 のパケットに対するフィルタ
親フィルタのフィルタルールに，サブルール（OR 条件）を追加します。

```
PureFlow(A)> add filter 12000 ipv4 in 1/1 proto udp sport 8000
PureFlow(A)> add filter subrule 12000 1 ipv4 proto udp sport 9000
```

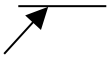


“add filter”コマンドにおいて，指定していないパラメータは，Don’t care として扱います。

（注）
アプリケーションフィルタによるアプリケーション認識を行う場合は，フロー識別モードの設定も行う必要があります（フロー識別モードの詳細は 8.6.1 章を参照してください）。

Sample 5）　親フィルタのフィルタルールを変更する。

```
PureFlow(A)> add filter 12000 ipv4 in 1/1 dip 10.16.1.0/255.255.255.0
PureFlow(A)> renew filter 12000 ipv4 sip 172.16.1.0/255.255.255.0
PureFlow(A)> renew filter 12000 ipv4 proto tcp
```



フィルタルールを変更するフィルタインデックス

“renew filter”コマンドにおいて，指定していないパラメータは，Don’t care として扱います。

上記の親フィルタ 12000 は，最後の“renew filter”コマンドで指定したフィルタルールのみが有効になります。

STEP 2 : Virtual Pipe シナリオの設定

本装置は，Virtual Pipe シナリオの設定により，Virtual Pipe のトラフィックアトリビュートを割り当てます。

Virtual Pipe シナリオに設定できるパラメータを，以下に示します。

パラメータ	設定範囲	省略可能／不可	説明
保証帯域 （vpipe_bandwidth）	10 k [bit/s]－100 M [bit/s] （GS1-F／GS1-FB） 10 k [bit/s]－1000 M [bit/s] （GS1-G／GS1-GB）	不可 または 可能	ライセンスキー2 が無効な場合，省略できません。ライセンスキー2 が有効なとき，パラメータは peak_bandwidth（最大帯域）として設定されます。 有効な設定単位は 1 k [bit/s] です。 k は 1000 を，M は 1000000 を表します。
最低帯域 （min_bandwidth）	0 k [bit/s]－100 M [bit/s] （GS1-F／GS1-FB） 0 k [bit/s]－1000 M [bit/s] （GS1-G／GS1-GB）	可能	ライセンスキー2 が有効なとき，設定可能です。 有効な設定単位は 1 k [bit/s] です。 k は 1000 を，M は 1000000 を表します。
最大帯域 （peak_bandwidth）	10 k [bit/s]－100 M [bit/s] （GS1-F／GS1-FB） 10 k [bit/s]－1000 M [bit/s] （GS1-G／GS1-GB）	可能	ライセンスキー2 が有効なとき，設定可能です。 有効な設定単位は 1 k [bit/s] です。 k は 1000 を，M は 1000000 を表します。
デフォルトバッファサイズ （default_bufsize）	2k [バイト]－10M [バイト]	可能	省略時：1M [バイト] 有効な設定単位は 1k [バイト] です。 k は 1024 を，M は 1048576 を表します。
シナリオ名 （scenario_name）	1 文字－128 文字	可能	省略時：シナリオ名なし 数字だけのシナリオ名は指定できません。また，装置内で重複したシナリオ名は使用しないでください。

Virtual Pipe シナリオの設定に関する CLI は以下のコマンドがあります。

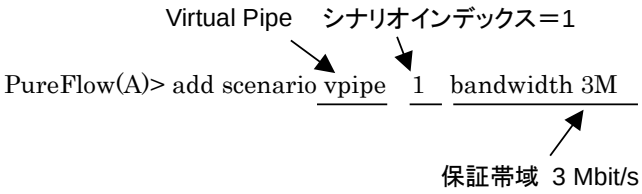
add scenario vpipe <scenario_id> [bandwidth <vpipe_bandwidth>] [min_bandwidth <min_bandwidth>] [peak_bandwidth <peak_bandwidth>] [default_bufsize <default_bufsize>] [name <scenario_name>]	Virtual Pipe シナリオを追加します。 GS1 ライセンスキー2 が有効のとき，min_bandwidthとpeak_bandwidthが指定可能です。 vpipe_bandwidth を指定した場合，指定された帯域は，peak_bandwidth として保存されます。 min_bandwidth と peak_bandwidth は vpipe_bandwidth と同時に指定できません。 GS1 ライセンスキー2 が無効のとき，vpipe_bandwidth は省略できず，また，min_bandwidth と peak_bandwidth は設定できません。
update scenario vpipe <scenario_id> [bandwidth <vpipe_bandwidth>] [min_bandwidth <min_bandwidth>] [peak_bandwidth <peak_bandwidth>] [default_bufsize <default_bufsize>] [name <scenario_name>]	すでに存在するVirtual Pipeシナリオに対してパラメータを変更します。親フィルタと Virtual Pipe シナリオを結合した後でも変更可能です。 GS1 ライセンスキー2 が有効のとき，min_bandwidthとpeak_bandwidthが指定可能です。 vpipe_bandwidth を指定した場合，指定された帯域は，peak_bandwidth として保存されます。 min_bandwidth と peak_bandwidth は vpipe_bandwidth と同時に指定できません。
delete scenario <scenario_id>	指定した Virtual Pipe シナリオを削除します。
show scenario [<scenario_id>]	Virtual Pipe シナリオの情報を表示します。

Virtual Pipe シナリオを設定するには，シナリオインデックスを付与する必要があります。シナリオインデックスは以下のルールに従って付与してください。

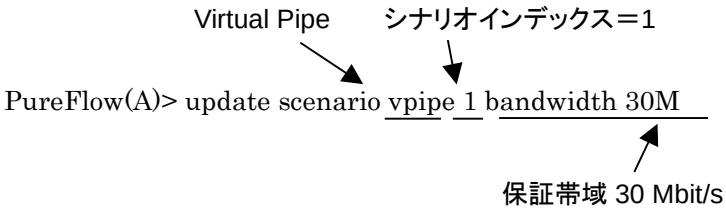
（1）シナリオの識別に用います。装置内で重複しないユニークな値を設定してください。

以下に，Virtual Pipe シナリオのサンプルを設定するコマンドを示します。

Sample 1）　Virtual Pipe で保証帯域 3 Mbit/s に設定する場合



Sample 2）　すでに存在する Virtual Pipe シナリオのインデックス 1 に対して，保証帯域 30 Mbit/s に変更する場合



STEP 3： 親フィルタとVirtual Pipeシナリオの結合

STEP1，STEP2 で設定した親フィルタと Virtual Pipe シナリオを結合することにより，親フィルタに一致したフローが，結合された Virtual Pipe シナリオに従ってトラフィックコントロールされて転送されます。

親フィルタと Virtual Pipe シナリオの結合に関する CLI は以下のコマンドがあります。

set filter <index>　action forward scenario <scenario_id>	親フィルタと Virtual Pipe シナリオを結合します。
unset filter <index>	親フィルタと Virtual Pipe シナリオの結合を解除します。

コマンドの実行例を示します。

PureFlow(A)> set filter 10000 action forward scenario 1
PureFlow(A)> unset filter 10000
PureFlow(A)>

STEP 4： 子フィルタの設定

本装置は，Ethernet フレーム，IPv4 パケット，IPv6 パケットのトラフィックを子フィルタによりフィルタ識別します。

子フィルタに設定できるパラメータを，以下に示します。

パラメータ		設定範囲	省略可能／不可
親フィルタインデックス		1 – 4096（VLAN）， 10000 – 14095（IPv4/IPv6）	不可
子フィルタインデックス		1 – 4096（VLAN）， 10000 – 14095（IPv4/IPv6）	不可
フィルタタイプ		vlan, ipv4, ipv6	不可
入力 Network ポート		1/1 – 1/2	不可
VLAN ID		0 – 4094（範囲指定可能）， none（VLAN Tag なし）	可能
CoS		0 – 7（範囲指定可能）	可能
送信元 IP アドレス／マスク	IPv4	0.0.0.0 – 255.255.255.255	可能 IP フィルタのみ有効
	IPv6	0::0 – FFFF:...:FFFF （小文字入力可能）	可能 IP フィルタのみ有効
宛先 IP アドレス／マスク	IPv4	0.0.0.0 – 255.255.255.255	可能 IP フィルタのみ有効
	IPv6	0::0 – FFFF:...:FFFF （小文字入力可能）	可能 IP フィルタのみ有効
ToS または Traffic Class	IPv4	0 – 255（範囲指定可能）	可能 IP フィルタのみ有効
	IPv6	0－255（範囲指定可能）	可能 IP フィルタのみ有効
プロトコル番号		0 – 255（範囲指定可能） （tcp，udp，icmp は文字入力可能）	可能 IP フィルタのみ有効
送信元ポート番号		0 – 65535（範囲指定可能）	可能 IP フィルタのみ有効
宛先ポート番号		0 – 65535（範囲指定可能）	可能 IP フィルタのみ有効

パラメータ	設定範囲	省略可能／不可
アプリケーション名	h323（H.323） 　h323.control（H.323 制御セッション） 　h323.voice（H.323 音声セッション） 　h323.video（H.323 映像セッション） 　h323.data（H.323 データセッション） sip（Session Initiation Protocol） 　sip.control（SIP 制御セッション） 　sip.voice（SIP 音声セッション） 　sip.video（SIP 映像セッション） 　sip.data（SIP データセッション） ftp（File Transfer Protocol） 　ftp.control（FTP 制御セッション） 　ftp.data（FTP データセッション）	可能 IP フィルタのみ有効 本機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。

子フィルタを設定するには，親フィルタインデックスも指定し，親フィルタと子フィルタの親子関係を作成してください。

子フィルタの設定に関する CLI は以下のコマンドです。

add filter <filter_idx>-<sub_idx> vlan in <slot/port> [vid {<VID> | none}] [cos <user_priority>]	子 VLAN フィルタを追加します。 Ethernet フレームをフィルタの対象にします。
add filter <filter_idx>-<sub_idx> ipv4 in <slot/port> [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv4 フィルタを追加します。 IPv4 パケットのみをフィルタの対象にします。
add filter <filter_idx>-<sub_idx> ipv6 in <slot/port> [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv6 フィルタを追加します。 IPv6 パケットのみをフィルタの対象にします。
add filter subrule <filter_idx>-<sub_idx> <subrule_idx> vlan [vid {<VID> | none}] [cos <user_priority>]	子 VLAN フィルタにサブルールを追加します。
add filter subrule <filter_idx>-<sub_idx> <subrule_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv4 フィルタにサブルールを追加します。
add filter subrule <filter_idx>-<sub_idx> <subrule_idx> ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv6 フィルタにサブルールを追加します。
delete filter subrule <filter_idx>-<sub_idx> {<subrule_idx>| all}	サブルールを削除します。
delete filter {<filter_idx>-<sub_idx> | all}	子フィルタを削除します。
show filter [<filter_idx>-<sub_idx>] [summary]	子フィルタを表示します。

子フィルタは，以下のルールに従って設定してください。

(1) 子フィルタの識別に用います。装置内で重複しないユニークな値を設定してください。

(2) パケットが入力された場合，親フィルタに一致する場合は，その親フィルタと親子関係にある子フィルタに一致するかを検査しますが，この子フィルタインデックスは，パケットを検査する順序を示します。パケットが複数のフィルタルールに一致する場合，子フィルタインデックスの小さいフィルタに一致したとみなされ，子フィルタインデックスの大きいほうの子フィルタは検査されません。

（3）“add filter”コマンドで，省略可能なパラメータを省略した場合は，そのパラメータは検査されません（すべて一致と見なされます）。

（4）子フィルタのフィルタルールにOR条件を追加する場合は，サブルールを設定してください。子フィルタのフィルタルールに一致するトラフィックと，サブルールに一致するトラフィックの両方を，子フィルタに一致したトラフィックとして制御します。

子フィルタの設定を変更する CLI は以下のコマンドです。

renew filter <filter_idx>-<sub_idx> vlan [vid {<VID>|none}] [cos <user_priority>]	子 VLAN フィルタの分類条件を新しく設定します。
renew filter <filter_idx>-<sub_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv4 フィルタの分類条件を新しく設定します。
renew filter <filter_idx>-<sub_idx> ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	子 IPv6 フィルタの分類条件を新しく設定します。
renew filter subrule <filter_idx>-<sub_idx> <subrule_idx> vlan [vid {<VID>|none}] [cos <user_priority>]	サブルールの分類条件を新しく設定します。
renew filter subrule <filter_idx>-<sub_idx> <subrule_idx> ipv4 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	サブルールの分類条件を新しく設定します。
renew filter subrule <filter_idx>-<sub_idx> <subrule_idx> ipv6 [vid {<VID> | none}] [cos <user_priority>] [sip [list] {<src_IP_address>|<list_name>}] [dip [list] {<dst_IP_address>|<list_name>}] [tos <type_of_service>] [proto <protocol>] [sport [list] {<sport>|<list_name>}] [dport [list] {<dport>|<list_name>}] [appli <application>]	サブルールの分類条件を新しく設定します。

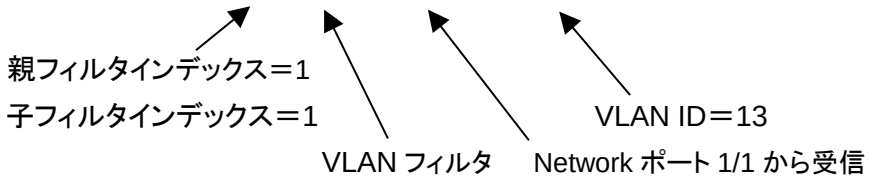
注 1）renew filter コマンドは，新たに指定されたフィルタルールのみを再登録します。
add filter コマンドで指定したフィルタルールは，消去されます。

注 2）renew filter コマンドは，set filter コマンドで指定された action を保持します。
すでに，set filter コマンドで action が設定されている filter に対して，再度，set filter コマンドを入力する必要はありません。

以下に，子フィルタのサンプルを設定するコマンドを示します。

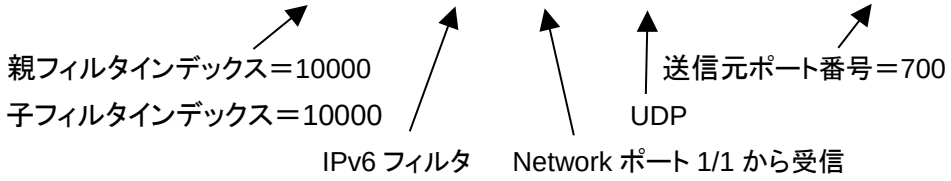
Sample 1）　Network ポート 1/1 から受信する Ethernet フレームで VLAN ID が 13 のフレームに対するフィルタ

```
PureFlow(A)> add filter 1-1 vlan in 1/1 vid 13
```



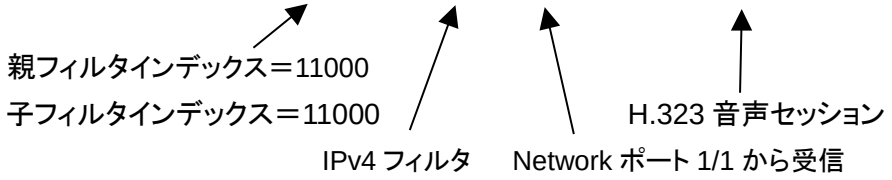
Sample 2）　Network ポート 1/1 から受信する IPv6 パケットで UDP のソースポート番号が 700 のパケットに対するフィルタ

```
PureFlow(A)> add filter 10000-10000 ipv6 in 1/1 proto udp sport 700
```



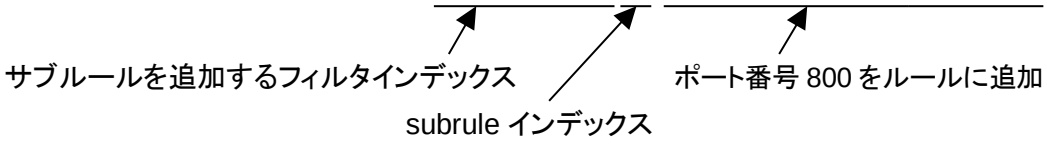
Sample 3）　Network ポート 1/1 から受信する IPv4 パケットで H.323 の音声セッションに対するフィルタ

```
PureFlow(A)> add filter 11000-11000 ipv6 in 1/1 appli h323.voice
```



Sample 4）　ソースポート番号 700 と 800 のパケットに対するフィルタ
子フィルタのフィルタルールに，サブルール（OR 条件）を追加します。

```
PureFlow(A)> add filter 10000-10000 ipv4 in 1/1  proto udp sport 700
PureFlow(A)> add filter subrule 10000-10000 1 ipv4 proto udp sport 800
```



“add filter”コマンドにおいて，指定していないパラメータは，Don’t care として扱います。

（注）
アプリケーションフィルタによるアプリケーション認識を行う場合は，フロー識別モードの設定も行う必要があります（フロー識別モードの詳細は 8.6.1 章を参照してください）。

STEP 5 : Virtual Channel シナリオの設定

本装置は，Virtual Channel シナリオの設定により，Virtual Channel のトラフィックアトリビュートを割り当てます。

Individual（個別キューモード）では，子フィルタに一致したフローごとにトラフィックアトリビュートを割り当てますが，最大帯域の合計が実際の物理速度を超えても設定が可能となっております。
個別キューモードで，VC キューの最大数を超えてフローを作成する場合は，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。（キューの詳細は 8.6.2 章を参照してください）

Aggregate／Individual の Virtual Channel シナリオに設定できるパラメータを，以下に示します。

パラメータ	設定範囲	省略可能／不可	説明
VC キューモード	aggregate（集約キューモード）／individual（個別キューモード）	不可	
クラス	クラス 1／クラス 2／クラス 3／クラス 4／クラス 5／クラス 6／クラス 7／クラス 8	可能	省略時：クラス 2
最低帯域 （min_bandwidth）	0 [bit/s]－100 M [bit/s] （GS1-F／GS1-FB） 0 [bit/s]－1000 M [bit/s] （GS1-G／GS1-GB）	可能	省略時：最低帯域保証なし 有効な設定単位は 1 k [bit/s]です。 k は 1000 を，M は 1000000 を表します。
最大帯域 （peak_bandwidth）	10 k [bit/s]－100 M [bit/s] （GS1-F／GS1-FB） 10 k [bit/s]－1000 M [bit/s] （GS1-G／GS1-GB）	可能	省略時：最大帯域制限なし 有効な設定単位は 1 k [bit/s]です。 k は 1000 を，M は 1000000 を表します。
バッファサイズ （bufsize）	2 k [バイト]－10 M [バイト]	可能	省略時：1 M [バイト] 有効な設定単位は 1 k [バイト]です。 k は 1024 を，M は 1048576 を表します。
VC キュー最大数 （maxqnum）	Virtual Channel シナリオで割り当てる VC キューの最大数 1－512 キュー （GS1-F／GS1-FB） 1－1024 キュー （GS1-G／GS1-GB） 1－4096 キュー （ライセンスキー3 有効時）	可能	省略時： GS1-F／GS1-FB： 512 キュー GS1-G／GS1-GB： 1024 キュー ライセンスキー3 有効時： 4096 キュー 個別キューモードのみ有効

注）ライセンスキー3（シナリオ拡張オプション）は，GS1-G/GS1-GB にのみ，適用可能です。

パラメータ	設定範囲	省略可能／不可	説明
フェイルアクション（failaction）	forward：下記条件の場合に，VP デフォルトキューで転送する。 discard：下記条件の場合に，廃棄する。 ・VCキューを最大数まで使用している	可能	省略時：forward 個別キューモードのみ有効
シナリオ名（scenario_name）	1 文字－128 文字	可能	省略時：シナリオ名なし 数字だけのシナリオ名は指定できません。また，装置内で重複したシナリオ名は使用しないでください。

Application（アプリケーションキューモード）では，子アプリケーションフィルタに一致したアプリケーションのメディアセッションごとにトラフィックアトリビュートを割り当てますが，各メディアセッションごとに割り当てた最低帯域の合計が total_min_bandwidth（ひとつのシナリオで割り当てる合計最低帯域）を超えた場合は，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。
なお，本機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。

Application の Virtual Channel シナリオに設定できるパラメータを，以下に示します。

パラメータ		設定範囲	省略可能／不可	説明
VC キューモード		application（アプリケーションキューモード）	不可	
クラス		クラス 1／クラス 2／クラス 3／クラス 4／クラス 5／クラス 6／クラス 7／クラス 8	可能	省略時：クラス 2
合計最低帯域（total_min_bandwidth）		10 k [bit/s]－100 M [bit/s]（GS1-F／GS1-FB） 10 k [bit/s] － 1000 M [bit/s]（GS1-G／GS1-GB）	不可	有効な設定単位は 1 k [bit/s] です。 k は 1000 を，M は 1000000 を表します。
制御セッション（control）	最低帯域（min_bw）	0 [%]（最低帯域保証なし）－100 [%]	可能	省略時：5 [%] total_min_bandwidth に対する割合です。
	最大帯域（peak_bw）	0（最大帯域制限なし）， または 100 [%]－200 [%]	可能	省略時：最大帯域制限なし 制御セッションに割り当てた最低帯域に対する割合です。
	バッファサイズ（buffer）	バイト指定： 2 k [バイト]－10 M [バイト] 時間指定： 1 ms－10000 ms	可能	省略時：1 M [バイト] バイト指定，または時間指定が可能です。時間指定の場合は，“msec”の文字列を明示的に入力してください。 k は 1024 を，M は 1048576 を表します。m は 0.001 を表します。

パラメータ		設定範囲	省略可能／不可	説明
音声セッション（voice）	最大帯域（peak_bw）	0（最大帯域制限なし）， または 100 [%]－200 [%]	可能	省略時：最大帯域制限なし 音声セッションに割り当てた最低帯域に対する割合です。 最低帯域は，音声セッションの要求帯域，または音声コーデックにより自動で割り当てます。
	バッファサイズ（buffer）	バイト指定： 2 k [バイト]－10 M [バイト] 時間指定： 1 ms－10000 ms	可能	省略時：400 ms バイト指定，または時間指定が可能です。時間指定の場合は，“msec”の文字列を明示的に入力してください。 k は 1024 を，M は 1048576 を表します。m は 0.001 を表します。
映像セッション（video）	最大帯域（peak_bw）	0（最大帯域制限なし）， または 100 [%]－200 [%]	可能	省略時：140 [%] 映像セッションに割り当てた最低帯域に対する割合です。 最低帯域は，映像セッションの要求帯域，または映像コーデックにより自動で割り当てます。
	バッファサイズ（buffer）	バイト指定： 2 k [バイト]－10 M [バイト] 時間指定： 1 ms－10000 ms	可能	省略時：400 ms バイト指定，または時間指定が可能です。時間指定の場合は，“msec”の文字列を明示的に入力してください。 k は 1024 を，M は 1048576 を表します。m は 0.001 を表します。

パラメータ		設定範囲	省略可能／不可	説明
データセッション（data）	最低帯域（min_bw）	0 [%]（最低帯域保証なし）－100 [%]	可能	省略時：最低帯域保証なし total_min_bandwidth に対する割合です。
	最大帯域（peak_bw）	0（最大帯域制限なし）， または 100 [%]－200 [%]	可能	省略時：最大帯域制限なし データセッションに割り当てた最低帯域に対する割合です。
	バッファサイズ（buffer）	バイト指定： 2 k [バイト]－10 M [バイト] 時間指定： 1 ms－10000 ms	可能	省略時：1 M [バイト] バイト指定，または時間指定が可能です。時間指定の場合は，“msec”の文字列を明示的に入力してください。 k は 1024 を，M は 1048576 を表します。m は 0.001 を表します。
VC キュー最大数（maxqnum）		Virtual Channel シナリオで割り当てる VC キューの最大数 1－512 キュー （GS1-F／GS1-FB） 1－1024 キュー （GS1-G／GS1-GB） 1－4096 キュー （ライセンスキー3 有効時）	可能	省略時： GS1-F／GS1-FB： 512 キュー GS1-G／GS1-GB： 1024 キュー ライセンスキー3 有効時： 4096 キュー
フェイルアクション（failaction）		forward：下記条件の場合に，VP デフォルトキューで転送する。 discard：下記条件の場合に，廃棄する。 ・VC キューを最大数まで使用している ・メディアセッションに割り当てた最低帯域の合計が合計最低帯域を超えた ・メディアセッション帯域を認識できなかった	可能	省略時：forward
シナリオ名（scenario_name）		1 文字－128 文字	可能	省略時：シナリオ名なし 数字だけのシナリオ名は指定できません。また，装置内で重複したシナリオ名は使用しないでください。

Virtual Channel シナリオの設定に関する CLI は以下のコマンドがあります。

add scenario vchannel aggregate <scenario_id> [class <class>] [min_bandwidth <min_bandwidth>] [peak_bandwidth <peak_bandwidth>] [bufsize <bufsize>] [name <scenario_name>]	Aggregate の Virtual Channel シナリオを追加します。
add scenario vchannel individual <scenario_id> [class <class>] [min_bandwidth <min_bandwidth>] [peak_bandwidth <peak_bandwidth>] [bufsize <bufsize>] [maxqnum <max_queue_num>] [failaction {forward | discard}] [name <scenario_name>]	Individual の Virtual Channel シナリオを追加します。
add scenario vchannel application <scenario_id> [class <class>] total_min_bandwidth <total_min_bandwidth> [control [min_bw <min_bw>] [peak_bw <peak_bw>] [buffer <buffer>]] [voice [peak_bw <peak_bw>] [buffer <buffer>]] [video [peak_bw <peak_bw>] [buffer <buffer>]] [data [min_bw <min_bw>] [peak_bw <peak_bw>] [buffer <buffer>]] [maxqnum <max_queue_num>] [failaction {forward | discard}] [name <scenario_name>]	Application の Virtual Channel シナリオを追加します。

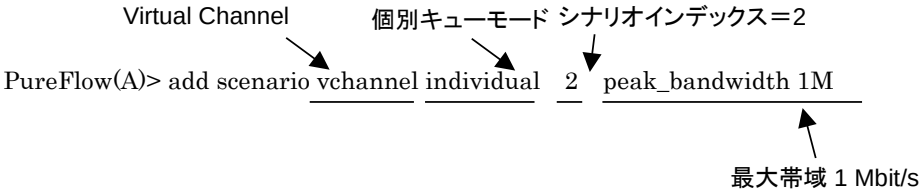
update scenario vchannel aggregate <scenario_id> [min_bandwidth < min_bandwidth >] [peak_bandwidth < peak_bandwidth >] [bufsize <bufsize>] [name <scenario_name>]	すでに存在する Aggregate の Virtual Channel シナリオに対してパラメータを変更します。子フィルタと Virtual Channel シナリオを結合した後でも変更可能です。
update scenario vchannel individual <scenario_id> [min_bandwidth < min_bandwidth >] [peak_bandwidth < peak_bandwidth >] [bufsize <bufsize>] [maxqnum <max_queue_num>] [failaction {forward | discard}] [name <scenario_name>]	すでに存在する Individual の Virtual Channel シナリオに対してパラメータを変更します。子フィルタと Virtual Channel シナリオを結合した後でも変更可能です。
update scenario vchannel application <scenario_id> [class <class>] [total_min_bandwidth <total_min_bandwidth>] [control [min_bw <min_bw>] [peak_bw <peak_bw>] [buffer <buffer>]] [voice [peak_bw <peak_bw>] [buffer <buffer>]] [video [peak_bw <peak_bw>] [buffer <buffer>]] [data [min_bw <min_bw>] [peak_bw <peak_bw>] [buffer <buffer>]] [maxqnum <max_queue_num>] [failaction {forward | discard}] [name <scenario_name>]	すでに存在する Application の Virtual Channel シナリオに対してパラメータを変更します。子アプリケーションフィルタと Virtual Channel シナリオを結合した後でも変更可能です。
delete scenario <scenario_id>	指定した Virtual Channel シナリオを削除します。
show scenario [<scenario_id>]	Virtual Channel シナリオの情報を表示します。

Virtual Channel シナリオを設定するには，シナリオインデックスを付与する必要があります。シナリオインデックスは以下のルールに従って付与してください。

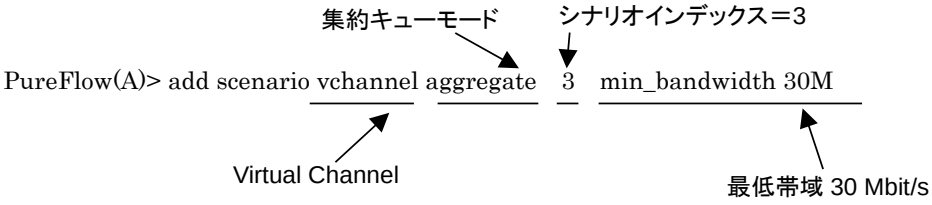
（1）シナリオの識別に用います。装置内で重複しないユニークな値を設定してください。

以下に，Virtual Channel シナリオのサンプルを設定するコマンドを示します。

Sample 1）　個別キューモードで最大帯域 1 Mbit/s に設定する場合



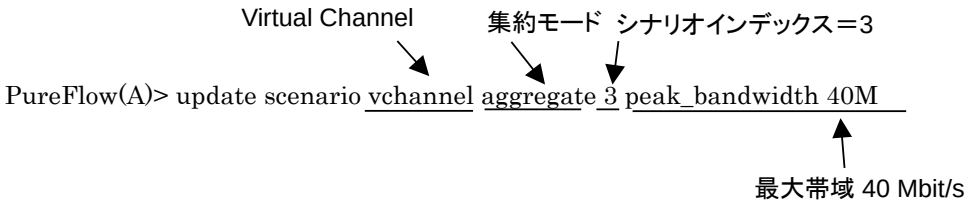
Sample 2）　集約キューモードで最低帯域 30 Mbit/s に設定する場合



“add scenario”コマンドにおいて，指定していないパラメータはデフォルト値（Sample2 では peak_bandwidth は最大帯域制限なし）として扱います。

Sample 3）　アプリケーションキューモードで割り当てる合計最低帯域 100 Mbit/s に設定する場合

Sample 4）　すでに存在する Virtual Channel シナリオのインデックス 3 に対して，最大帯域 40 Mbit/s に上書き設定する場合



STEP 6： 子フィルタと Virtual Channel シナリオの結合

STEP4, STEP5 で設定した子フィルタと Virtual Channel シナリオを結合することにより，子フィルタに一致したフローが，結合された Virtual Channel シナリオに従ってトラフィックコントロールされて転送されます。

子フィルタと Virtual Channel シナリオの結合に関する CLI は以下のコマンドがあります。

set filter <index>-<sub_index> action forward scenario <scenario_id>	子フィルタと Virtual Channel シナリオを結合します。
unset filter <index>-<sub_index>	子フィルタと Virtual Channel シナリオの結合を解除します。

コマンドの実行例を示します。

```
PureFlow(A)> set filter 10000-10000 action forward scenario 2
PureFlow(A)> unset filter 10000-10000
PureFlow(A)>
```

8.5　ルールリストの設定方法

本章ではルールリストの設定方法について説明します。

ルールリストを利用するには以下の手順で設定します。
手順 1 ルールリストを設定する。
手順 2 ルールリストに対してルールリストエントリを追加する。
手順 3 フィルタ追加コマンドにルールリストを指定する。

ルールリストおよびルールリストエントリのパラメータを，以下に示します。

ルールリストのパラメータ

パラメータ	設定範囲
ルールリスト名	1 文字-32 文字
ルールリストタイプ	Ipv4, ipv6, l4port

ルールリストエントリのパラメータ

パラメータ		設定範囲
ルールリスト名		登録済みのルールリスト名を指定する
ルールリストタイプ		ipv4, ipv6, l4port
トラフィック分類条件	IPv4 アドレス／マスク	0.0.0.0 -255.255.255.255
	IPv6 アドレス／マスク	0::0 – FFFF:…:FFFF （小文字入力可能）
	TCP／UDP ポート番号	0 – 65535（範囲指定可能）

ルールリストの設定に関する CLI は以下のコマンドです。

add rulelist group <list_name> {ipv4 | ipv6 | l4port}	ルールリストを追加します。 ipv4，ipv6，l4port のいずれかを対象にします。
add rulelist entry <list_name> ipv4 <IP_address>	IPv4 アドレスをルールリストに追加します。
add rulelist entry <list_name> ipv6 <IP_address>	Ipv6 アドレスをルールリストに追加します。
add rulelist entry <list_name> l4port <port>	l4port ポート番号をルールリストに追加します。
delete rulelist group {<list_name> | all}	ルールリストを削除します。
delete rulelist entry <list_name> ipv4 <IP_address>	IPv4 アドレスをルールリストから削除します。
delete rulelist entry <list_name> ipv6 <IP_address>	IPv6 アドレスをルールリストから削除します。
delete rulelist entry <list_name> l4port <port>	L4port ポート番号をルールリストから削除します。
show rulelist [<list_name>]	ルールリストを表示します。

ルールリストは，以下のルールに従って設定してください。

(1) 装置内で重複しないユニークなルールリスト名を設定してください。

(2) “delete rulelist group”コマンドは，フィルタに登録されていないルールリストに対してのみ行うことができます。

(3) ルールリスト名には，”all”は指定できません。

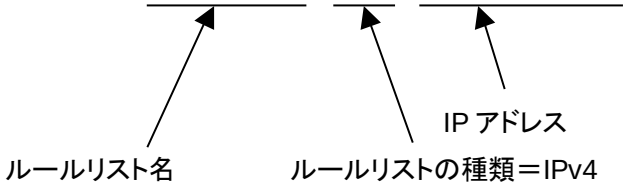
以下に，ルールリストのサンプルを設定するコマンド手順を示します。

手順 1）　ルールリスト“TVCservers”を登録する。

```
PureFlow(A)> add rulelist group “TVCservers” ipv4
```

手順 2）　ルールリスト“TVCservers”に，ルールリストエントリを追加する。

```
PureFlow(A)> add rulelist entry “TVCservers” ipv4 172.16.111.11
```



手順 3）　フィルタ追加コマンドの sip にルールリスト名”TVCservers”を指定する。

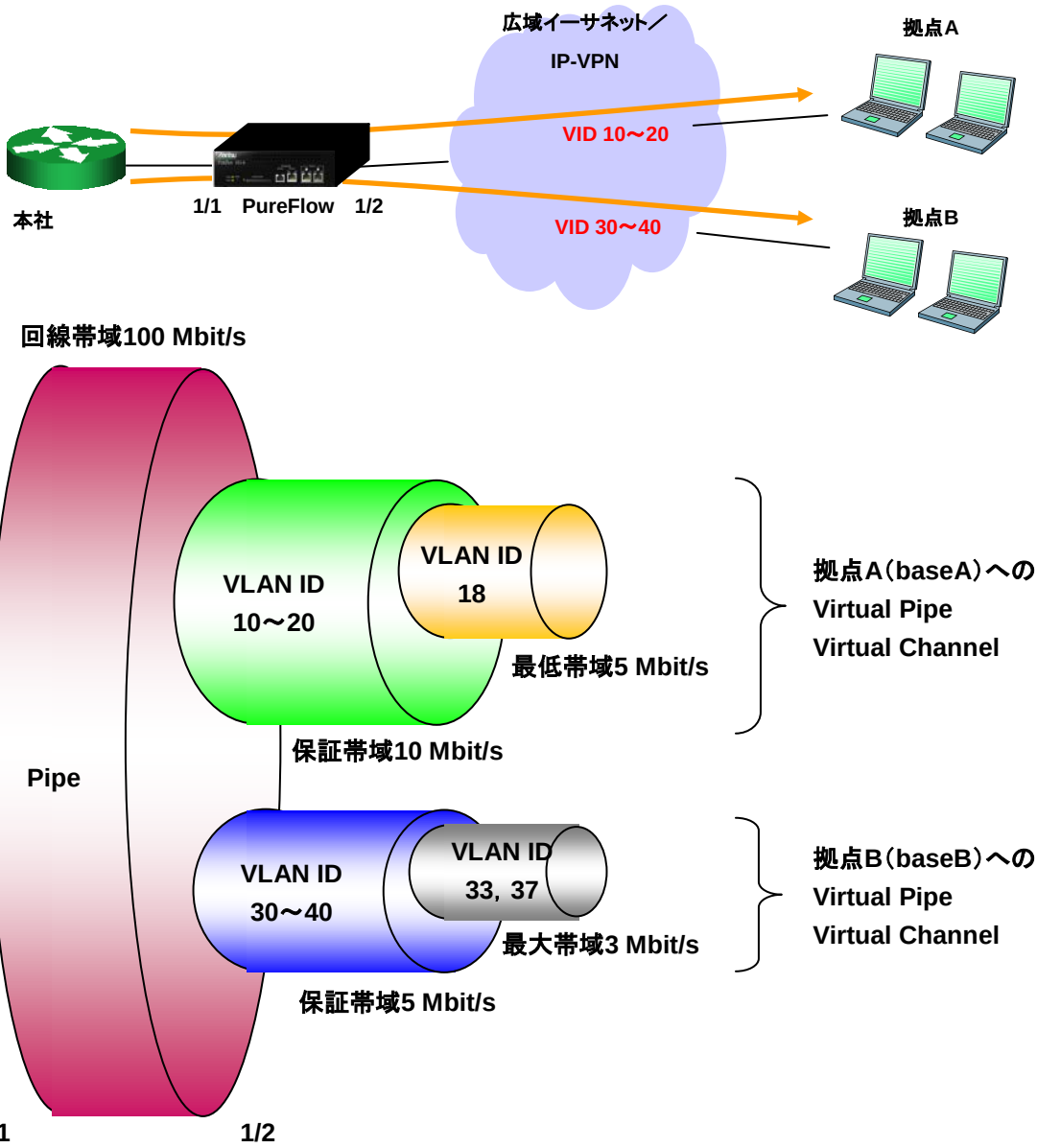
```
PureFlow(A)> add filter 10000 ipv4 in 1/1 sip list “TVCservers”
```

8.6　コンフィギュレーション例

以下のネットワーク環境の設定を行う場合のコンフィギュレーション例を示します(コンテンツ・アウェア・シェーピングのコンフィギュレーション例は,「第9章 コンテンツ・アウェア・シェーピング機能」を参照してください)。

[Case 1]VLANごとのトラフィックコントロールを行う

- 拠点 A のネットワークは VLAN ID 10～20 です。
- 拠点 B のネットワークは VLAN ID 30～40 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で, 拠点 A への VLAN ID 18 のトラフィックは最低帯域 5 Mbit/s にします(Virtual Channel)。
- 本社から拠点 B への通信グループ(baseB)を保証帯域 5 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で, 拠点 B への VLAN ID 33 と 37 のトラフィックは最大帯域 3 Mbit/s にします(Virtual Channel)。



以下のコマンドを実行します。

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 1 vlan in 1/1 vid 10-20
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 1 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 1-1 vlan in 1/1 vid 18
PureFlow(A)> add scenario vchannel aggregate 2 min_bandwidth 5M name baseA_VC
PureFlow(A)> set filter 1-1 action forward scenario 2
```

＜拠点 B への Virtual Pipe＞

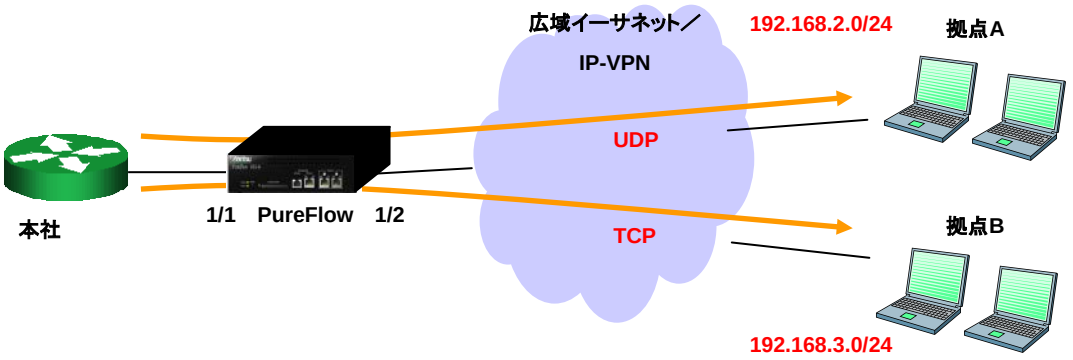
```
PureFlow(A)> add filter 10 vlan in 1/1 vid 30-40
PureFlow(A)> add scenario vpipe 10 bandwidth 5M name baseB
PureFlow(A)> set filter 10 action forward scenario 10
```

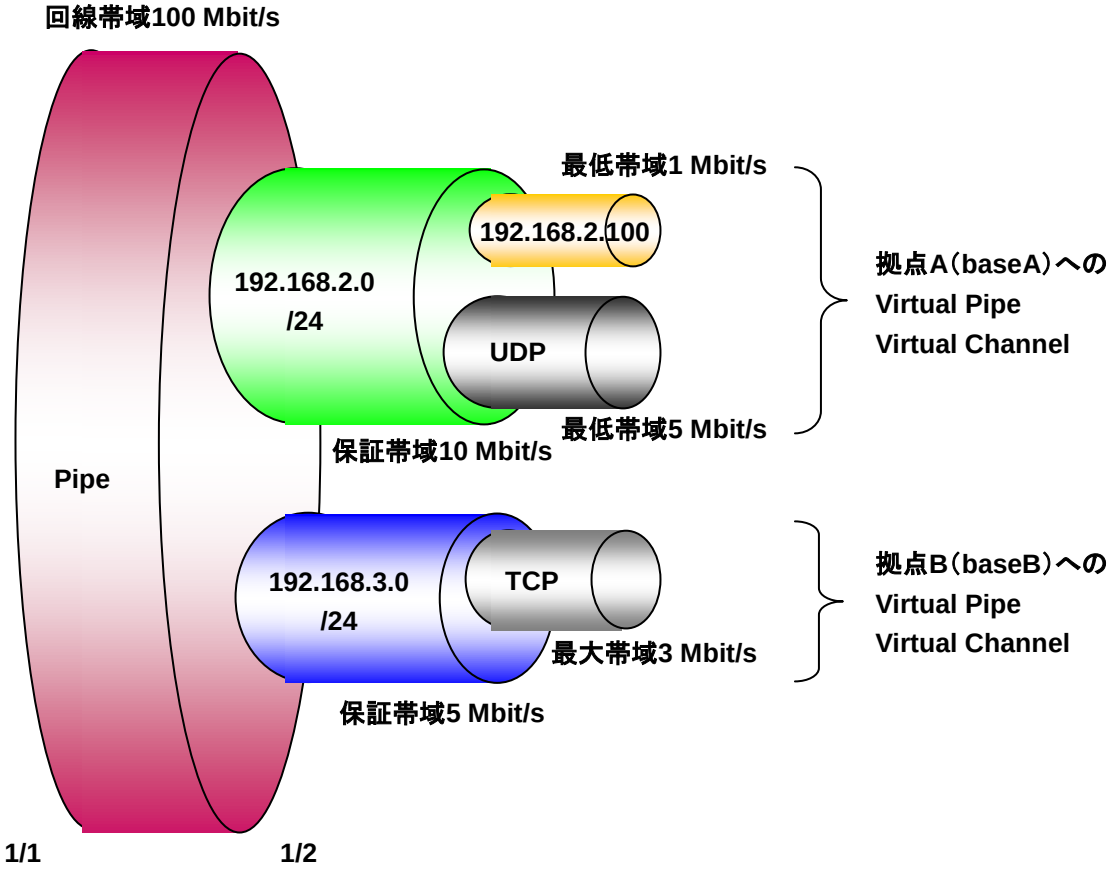
＜拠点 B への Virtual Channel＞

```
PureFlow(A)> add filter 10-10 vlan in 1/1 vid 33
PureFlow(A)> add filter 10-11 vlan in 1/1 vid 37
PureFlow(A)> add scenario vchannel aggregate 11 peak_bandwidth 3M name baseB_VC
PureFlow(A)> set filter 10-10 action forward scenario 11
PureFlow(A)> set filter 10-11 action forward scenario 11
```

[Case 2]IPサブネットとプロトコルを組み合わせてトラフィックコントロールを行う

- 拠点 A のネットワークは 192.168.2.0/24 です。
- 拠点 B のネットワークは 192.168.3.0/24 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で，特定ホスト 192.168.2.100 への通信は最低帯域 1 Mbit/s にします。
  また，拠点 A への UDP 通信は最低帯域 5 Mbit/s にします(Virtual Channel)。
- 本社から拠点 B への通信グループ(baseB)を保証帯域 5 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で，拠点 B への TCP 通信は最大帯域 3 Mbit/s にします(Virtual Channel)。





以下のコマンドを実行します。

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 10000 ipv4 in 1/1 dip 192.168.2.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 10000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 10000-10000 ipv4 in 1/1 dip 192.168.2.100
PureFlow(A)> add filter 10000-10001 ipv4 in 1/1 proto udp
PureFlow(A)> add scenario vchannel aggregate 2 min_bandwidth 1M name baseA_VC1
PureFlow(A)> add scenario vchannel aggregate 3 min_bandwidth 5M name baseA_VC2
PureFlow(A)> set filter 10000-10000 action forward scenario 2
PureFlow(A)> set filter 10000-10001 action forward scenario 3
```

＜拠点 B への Virtual Pipe＞

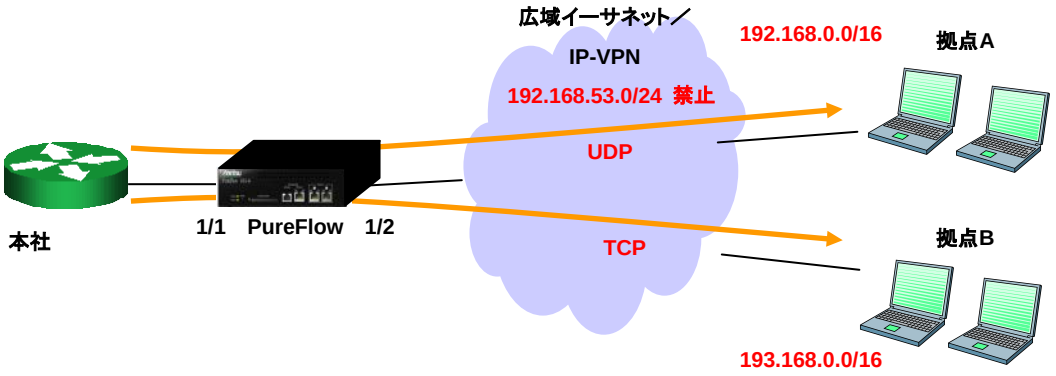
```
PureFlow(A)> add filter 10010 ipv4 in 1/1 dip 192.168.3.0/255.255.255.0
PureFlow(A)> add scenario vpipe 10 bandwidth 5M name baseB
PureFlow(A)> set filter 10010 action forward scenario 10
```

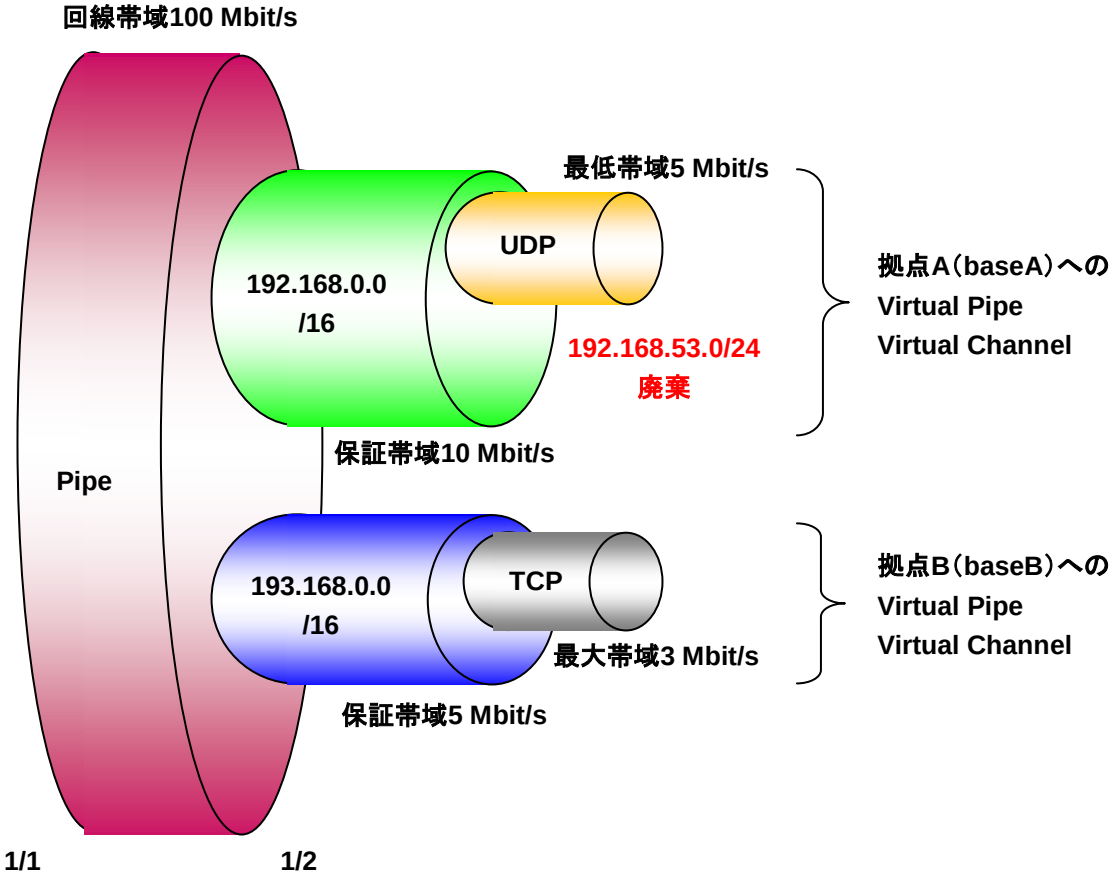
＜拠点 B への Virtual Channel＞

```
PureFlow(A)> add filter 10010-10010 ipv4 in 1/1 proto tcp
PureFlow(A)> add scenario vchannel aggregate 11 peak_bandwidth 3M name baseB_VC
PureFlow(A)> set filter 10010-10010 action forward scenario 11
```

[Case 3]トラフィックコントロールとファイアウォールを同時に行う

- 拠点 A のネットワークは 192.168.0.0/16 です。
- 拠点 B のネットワークは 193.168.0.0/16 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で, 拠点 A への UDP 通信は最低帯域 5 Mbit/s にします(Virtual Channel)。
  ただし, 拠点 A 内のネットワーク 192.168.53.0/24 への通信は禁止とします。
- 本社から拠点 B への通信グループ(baseB)を保証帯域 5 Mbit/s にします(Virtual Pipe)。
  その保証帯域内で, 拠点 B への TCP 通信は最大帯域 3 Mbit/s にします(Virtual Channel)。





以下のコマンドを実行します。

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 10000 ipv4 in 1/1 dip 192.168.0.0/255.255.0.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 10000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 10000-10000 ipv4 in 1/1 proto udp
PureFlow(A)> add filter 10000-10001 ipv4 in 1/1 dip 192.168.53.0/255.255.255.0
PureFlow(A)> add scenario vchannel aggregate 2 min_bandwidth 5M name baseA_VC
PureFlow(A)> set filter 10000-10000 action forward scenario 2
PureFlow(A)> set filter 10000-10001 action discard
```

＜拠点 B への Virtual Pipe＞

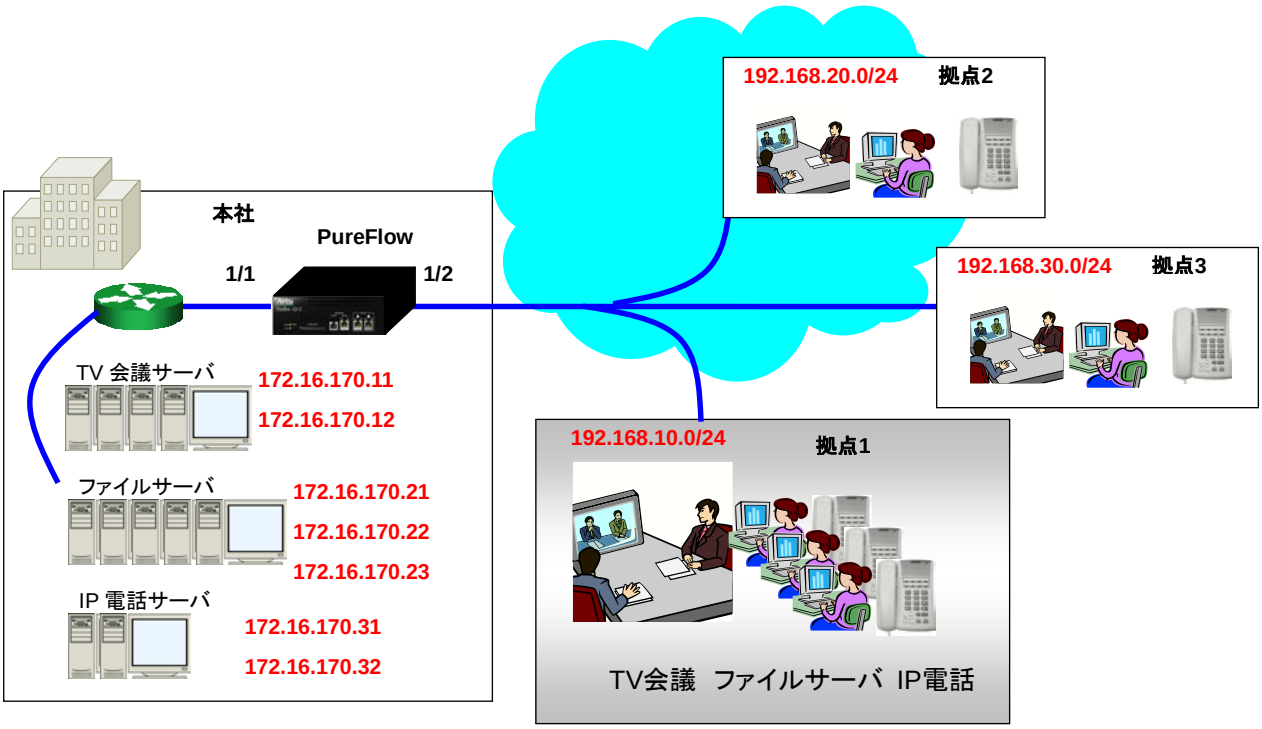
```
PureFlow(A)> add filter 10010 ipv4 in 1/1 dip 193.168.0.0/255.255.0.0
PureFlow(A)> add scenario vpipe 10 bandwidth 5M name baseB
PureFlow(A)> set filter 10010 action forward scenario 10
```

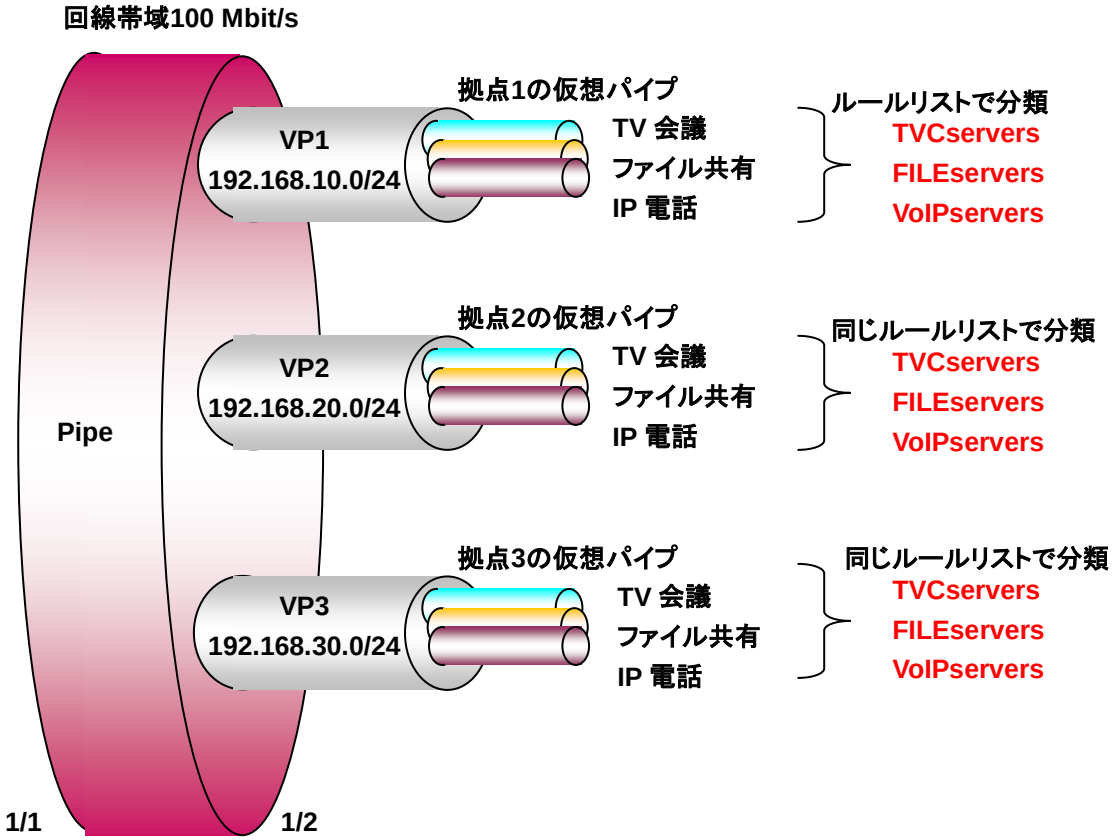
＜拠点 B への Virtual Channel＞

```
PureFlow(A)> add filter 10010-10010 ipv4 in 1/1 proto tcp
PureFlow(A)> add scenario vchannel aggregate 11 peak_bandwidth 3M name baseB_VC
PureFlow(A)> set filter 10010-10010 action forward scenario 11
```

［Case 4］ルールリストを使って，フィルタ設定を簡素化する。

- 各拠点は，本社に設置されたサーバを利用している。（TV 会議，ファイルサーバ，VoIP）
- PureFlowGS1 は，各拠点に，通信帯域を割り当て，さらに，サービスごとに，通信帯域を割り当てる。





＜サービスごとにルールリストに登録する。＞

・ TV 会議サーバの IP アドレスをルールリストに登録する。

```
PureFlow(A)> add rulelist group “TVCservers” ipv4
PureFlow(A)> add rulelist entry “TVCservers” ipv4 172.16.170.11
PureFlow(A)> add rulelist entry “TVCservers” ipv4 172.16.170.12
```

・ ファイルサーバの IP アドレスをルールリストに登録する。

```
PureFlow(A)> add rulelist group “FILEservers” ipv4
PureFlow(A)> add rulelist entry “FILEservers” ipv4 172.16.170.21
PureFlow(A)> add rulelist entry “FILEservers” ipv4 172.16.170.22
PureFlow(A)> add rulelist entry “FILEservers” ipv4 172.16.170.23
```

・ IP 電話サーバの IP アドレスをルールリストに登録する。

```
PureFlow(A)> add rulelist group “VoIPservers” ipv4
PureFlow(A)> add rulelist entry “VoIPservers” ipv4 172.16.170.31
PureFlow(A)> add rulelist entry “VoIPservers” ipv4 172.16.170.32
```

＜拠点 1 への Virtual Pipe を登録する＞

・ 拠点1へのトラフィック総量を設定する。

```
PureFlow(A)> add filter 10010 ipv4 in 1/1 dip 192.168.10.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 10010 action forward scenario 1
```

・ TV 会議サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10010-10011 ipv4 in 1/1 sip list “TVCservers”
PureFlow(A)> add scenario vchannel aggregate 11 min_bandwidth 5M name baseA_TVC
PureFlow(A)> set filter 10010-10011 action forward scenario 11
```

・ ファイルサーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10010-10012 ipv4 in 1/1 sip list “FILEservers”
PureFlow(A)> add scenario vchannel aggregate 12 min_bandwidth 4M name baseA_FILE
PureFlow(A)> set filter 10010-10012 action forward scenario 12
```

・ IP 電話サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10010-10013 ipv4 in 1/1 sip list “VoIPservers”
PureFlow(A)> add scenario vchannel aggregate 13 min_bandwidth 1M name baseA_VoIP
PureFlow(A)> set filter 10010-10013 action forward scenario 13
```

同じルールリストを使って，拠点 2 と拠点 3 のトラフィックを登録します。

＜拠点 2 への Virtual Pipe を登録する＞

・ トラフィック総量を登録する。

```
PureFlow(A)> add filter 10020 ipv4 in 1/1 dip 192.168.20.0/255.255.255.0
PureFlow(A)> add scenario vpipe 2 bandwidth 10M name baseB
PureFlow(A)> set filter 10020 action forward scenario 2
```

・ TV 会議サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10020-10021 ipv4 in 1/1 sip list “TVCservers”
PureFlow(A)> add scenario vchannel aggregate 21 min_bandwidth 5M name baseB_TVC
PureFlow(A)> set filter 10020-10021 action forward scenario 21
```

・ ファイルサーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10020-10022 ipv4 in 1/1 sip list “FILEservers”
PureFlow(A)> add scenario vchannel aggregate 22 min_bandwidth 4M name baseB_FILE
PureFlow(A)> set filter 10020-10022 action forward scenario 22
```

・ IP 電話サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10020-10023 ipv4 in 1/1 sip list “VoIPservers”
PureFlow(A)> add scenario vchannel aggregate 23 min_bandwidth 1M name baseB_VoIP
PureFlow(A)> set filter 10020-10023 action forward scenario 23
```

＜拠点 3 への Virtual Pipe を登録する＞

・ トラフィック総量を登録する。

```
PureFlow(A)> add filter 10030 ipv4 in 1/1 dip 192.168.30.0/255.255.255.0
PureFlow(A)> add scenario vpipe 3 bandwidth 10M name baseC
PureFlow(A)> set filter 10030 action forward scenario 3
```

・ TV 会議サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10030-10031 ipv4 in 1/1 sip list “TVCservers”
PureFlow(A)> add scenario vchannel aggregate 31 min_bandwidth 5M name baseC_TVC
PureFlow(A)> set filter 10030-10031 action forward scenario 31
```

・ ファイルサーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10030-10032 ipv4 in 1/1 sip list “FILEservers”
PureFlow(A)> add scenario vchannel aggregate 32 min_bandwidth 4M name baseC_FILE
PureFlow(A)> set filter 10030-10032 action forward scenario 32
```

・ IP 電話サーバのルールリストを使ってトラフィックを登録する。

```
PureFlow(A)> add filter 10030-10033 ipv4 in 1/1 sip list “VoIPservers”
PureFlow(A)> add scenario vchannel aggregate 33 min_bandwidth 1M name baseC_VoIP
PureFlow(A)> set filter 10030-10033 action forward scenario 33
```

8.7　さらに高度な設定

本装置には，さらに高度な設定として，以下の設定があります。

- フロー識別モード
- キュー
- 通信ギャップモード

8.7.1　フロー識別モード

フローとは，装置内で識別できるトラフィックの最小単位です。トラフィックは，複数のフローからなるグループと考えることができます。

本装置は，パケットを受信すると，そのパケットを転送するためのフローを登録します。登録したフローは，フィルタに設定した動作に従ってキューにパケットを格納し，トラフィックコントロールします。

フローには，Ethernet フレームを転送するための VLAN フローと IP パケットを転送するための IP フローの 2 種類があります。

1. VLAN フローは，Ethernet フレーム（ARP パケット，IP パケットなど）を転送するためのフローです。
   以下の Ethernet フレームフィールドをフロー識別します。

   - VLAN ID（VLAN Tag あり／なしも識別）
   - CoS

2. IP フローは，IP パケット（ARP パケットなどは含まれません）を転送するためのフローです。
   以下の IP パケットフィールドをフロー識別します。

   - VLAN ID（VLAN Tag あり／なしも識別）
   - CoS
   - 送信元 IP アドレス（SIP）
   - 宛先 IP アドレス（DIP）
   - ToS またはトラフィッククラス
   - プロトコル番号
   - 送信元ポート番号（Sport）
   - 宛先ポート番号（Dport）

本装置では，フィルタの組み合わせにより，使用するフローが異なります。

		子フィルタ	
		VLAN フィルタ	IP フィルタ
親フィルタ	VLAN フィルタ	VLAN フロー（注 1）	VLAN フロー／IP フロー（注 2）
	IP フィルタ	IP フロー	IP フロー

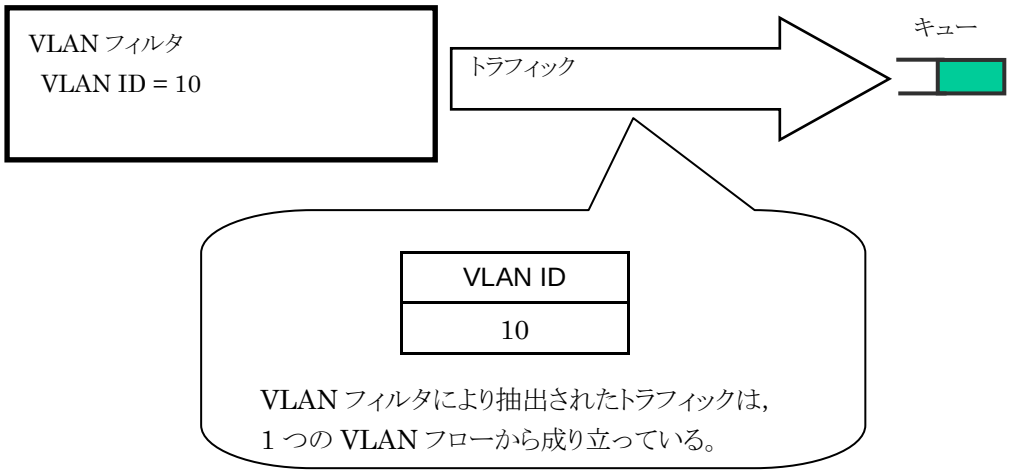
（注 1）
すべての Ethernet フレーム（IP パケット含む）を VLAN フローで転送します。

（注 2）
IP パケットは IP フローで，親フィルタに一致する IP パケット以外の Ethernet フレームは VLAN フローで転送します。

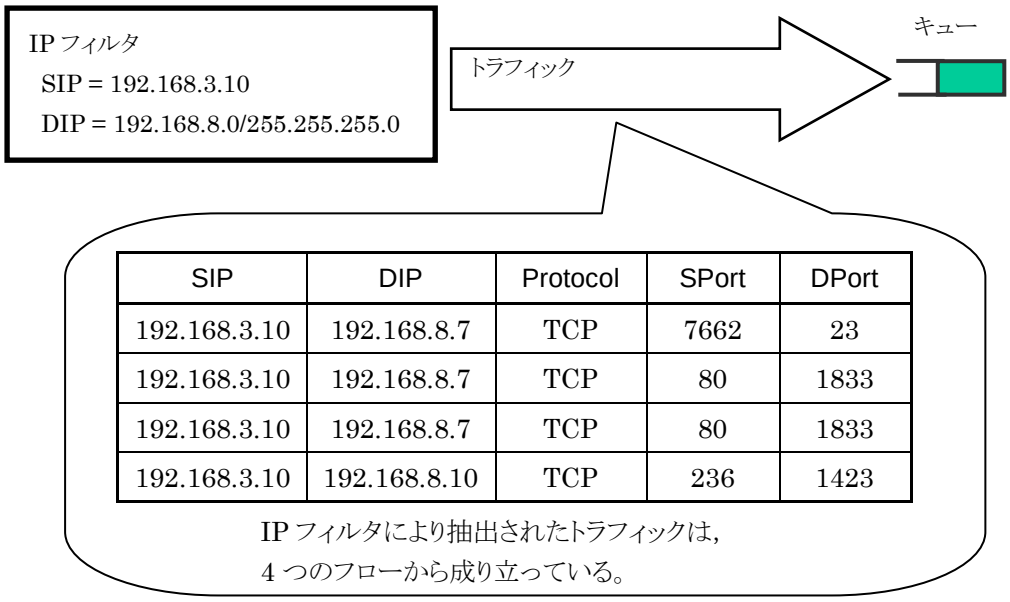
VLAN フローは，VLAN フィルタとシナリオを結び付けると，Ethernet フレームを受信しなくても静的に作成します。VLAN フローは，VLAN フィルタとシナリオの結び付けを解除するまで削除しません。

IP フローは，IP パケットを受信すると動的に作成します。パケットを受信しなくなった IP フローは，エージングタイム経過後に削除します。

通常，VLAN フローは，VLAN ID が一致するトラフィックです。



通常，IP フローは，送信元 IP アドレス（SIP），宛先 IP アドレス（DIP），プロトコル番号（Protocol），送信元ポート番号（SPort），宛先ポート番号（DPort）がすべて一致するトラフィックです。



本装置は，このフローを識別するフィールドの組み合わせ（フロー識別モード）を変更することが可能です。各フィールドが異なるパケットを異なるフローとして転送させたり，同じフローとして転送させることができます。

VLAN フロー／IP フローのいずれも，フロー識別に必ず VLAN ID を用います。VLAN ID をフロー識別の対象から除外することはできません。

また，アプリケーションフィルタによるアプリケーション認識を行う場合も，フロー識別モードの設定を行う必要があります。

フロー識別モードに設定できるパラメータを，以下に示します。

パラメータ	設定範囲	省略可能／不可
入力 Network ポート	1/1 – 1/2	不可
フィールド名	default ：フローの識別フィールドをデフォルトにします。 送信元 IP アドレス，宛先 IP アドレス，プロトコル番号，送信元ポート番号，宛先ポート番号をフロー識別します。 cos ：CoS をフロー識別します。 sip ：送信元 IP アドレスをフロー識別します。 dip ：宛先 IP アドレスをフロー識別します。 tos ：ToS，または Traffic Class をフロー識別します。 proto ：プロトコル番号，送信元ポート番号，宛先ポート番号をフロー識別します。 appli ：アプリケーション認識します。 appli を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。	不可

本パラメータは，カンマ(,)で区切って複数指定することができます。

(注 3)
アプリケーションフィルタによるアプリケーション認識を行う場合は，すべての Network ポートに対するフロー識別モードで appli 指定をしてください(その他のフィールドと組み合わせても可)。すべての Network ポートで appli 指定しないと，正常にアプリケーション認識できません。

(注 4)
アプリケーションキューモードを指定したシナリオを使用する場合は，フロー識別モードに“appli”のみを指定してください。“tos,appli”など，フロー識別モードに“appli”以外のフィールドを同時に指定した場合，アプリケーションキューモードの自動帯域割当において，一時的に必要帯域の 2 倍の帯域を確保する場合があります。

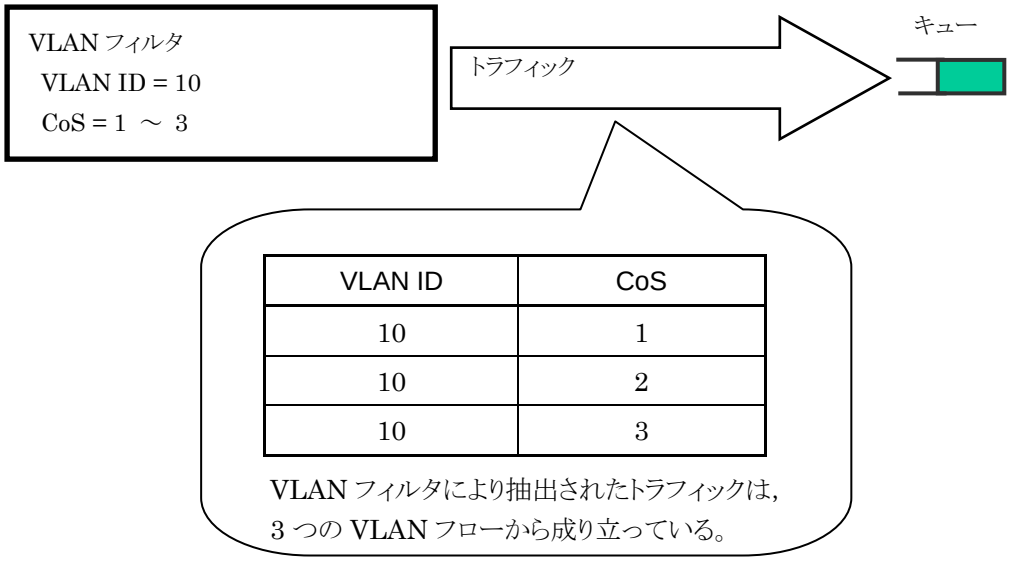
フロー識別モードに関する CLI は以下のコマンドがあります。

set filter mode in <slot/port> <field>	フローの識別フィールドを選択します。<field> のデフォルト値は“default”です。

コマンドの実行例を示します。

```
PureFlow(A)> set filter mode in 1/1 cos
PureFlow(A)> set filter mode in 1/2 sip,dip
PureFlow(A)>
```

たとえば，VLAN ID に加え CoS が異なる Ethernet フレームを別のフローとして識別し，各フローごとにトラフィックコントロールを行いたい場合，cos を有効にします。このフロー識別モードの場合，“add filter”で登録した VLAN フィルタの条件は，VLAN ID と CoS がフィルタ対象となります。フロー識別モードで指定したフィールド以外のフィールドが設定されている VLAN フィルタは，無効と見なします。



※ 各フローごとにトラフィックコントロールしたい場合は，
Virtual Channel の個別キューモードを使用してください。

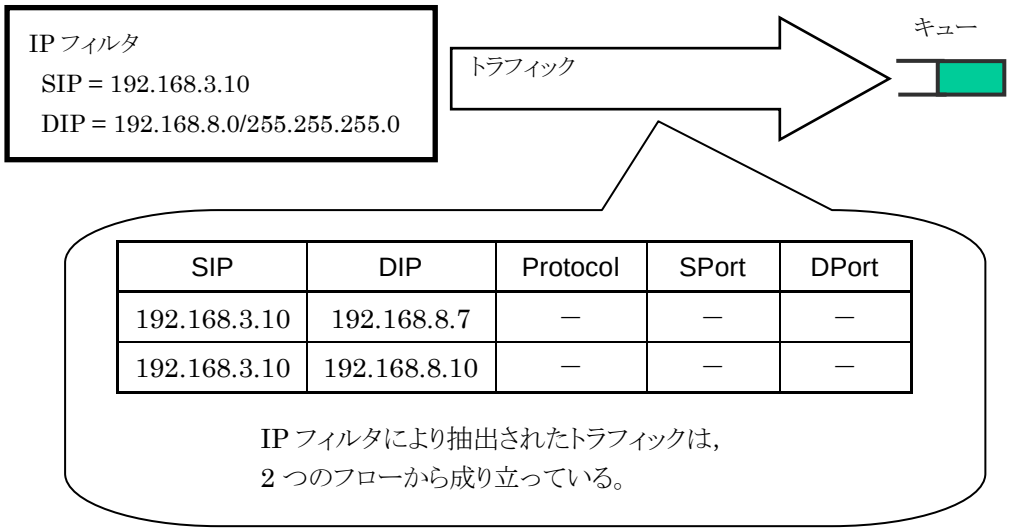
VLAN フィルタ使用時に，指定フィールド名と VLAN フローで識別するフィールドの関係を，以下に示します。

指定フィールド名	フロー識別フィールド							
	VLAN ID	CoS	SIP	DIP	ToS	プロトコル番号	Sport 番号	Dport 番号
default	○	×	×	×	×	×	×	×
cos	○	○	×	×	×	×	×	×
sip	○	×	×	×	×	×	×	×
dip	○	×	×	×	×	×	×	×
tos	○	×	×	×	×	×	×	×
proto	○	×	×	×	×	×	×	×
appli	○	×	×	×	×	×	×	×

○:フロー識別する
×:フロー識別しない

上表のように，VLAN フィルタ使用時は，VLAN フローを使用し，IP アドレスやプロトコル番号などをフロー識別には用いません。VLAN フローは，フロー識別モードにより IP アドレスやプロトコル番号などが指定された場合でも，IP アドレスやプロトコル番号などを無視します。

また，送信元 IP アドレスと宛先 IP アドレスのみでフローを識別し，その他のフィールドが異なる IP パケットは同じ IP フローとしてトラフィックコントロールしたい場合，sip と dip を有効にします。このフロー識別モードの場合，“add filter”で登録した IP フィルタの条件は，送信元 IP アドレス，宛先 IP アドレスがフィルタ対象となります。フロー識別モードで指定したフィールド以外のフィールドが設定されている IP フィルタは，無効と見なします。



SIP	DIP	Protocol	SPort	DPort
192.168.3.10	192.168.8.7	—	—	—
192.168.3.10	192.168.8.10	—	—	—

※ 各フローごとにトラフィックコントロールしたい場合は，
Virtual Channel の個別キューモードを使用してください。

IP フィルタ使用時に，指定フィールド名と IP フローで識別するフィールドの関係を，以下に示します。

指定フィールド名	フロー識別フィールド							
	VLAN ID	CoS	SIP	DIP	ToS	プロトコル番号	Sport 番号	Dport 番号
default	○	×	○	○	×	○	○	○
cos	○	○	×	×	×	×	×	×
sip	○	×	○	×	×	×	×	×
dip	○	×	×	○	×	×	×	×
tos	○	×	×	×	○	×	×	×
proto	○	×	×	×	×	○	○	○
appli	○	×	○	○	×	○	○	○

○:フロー識別する
×:フロー識別しない

上表のように，appli を有効にすると，VLAN ID に加え，自動的に SIP，DIP，プロトコル番号，Sport 番号，Dport 番号をフロー識別するようになります。

8.7.2　キュー

本装置は，各フローに対してキューを割り当て，受信したパケットを割り当てたキューに格納します。キューは，Virtual Pipe に割り当てる VP デフォルトキューと Virtual Channel に割り当てる VC キューの 2 種類があります。キューに格納したパケットはスケジューリングされ，トラフィックコントロール転送されます。

（1）VP デフォルトキュー

Virtual Pipe 内で Virtual Channel に該当しないフローを転送するためのキューです。VP デフォルトキューは，ベストエフォートクラス（クラス 9）となります。

親フィルタに一致し，子フィルタに一致しないすべてのフローを同じ VP デフォルトキューに割り当て，トラフィックコントロールを行います。

たとえば，Virtual Pipe シナリオで保証帯域 100 Mbit/s に設定した場合は，以下のようになります。

本装置に，以下のフィルタを登録したと仮定します。

- 親フィルタ 1
  送信元 IP アドレス ： 192.168.0.0/16
  宛先 IP アドレス ： 192.168.0.0/16
- 子フィルタ 1-1
  送信元 IP アドレス ： 192.168.10.0/24
  宛先 IP アドレス ： 192.168.10.0/24

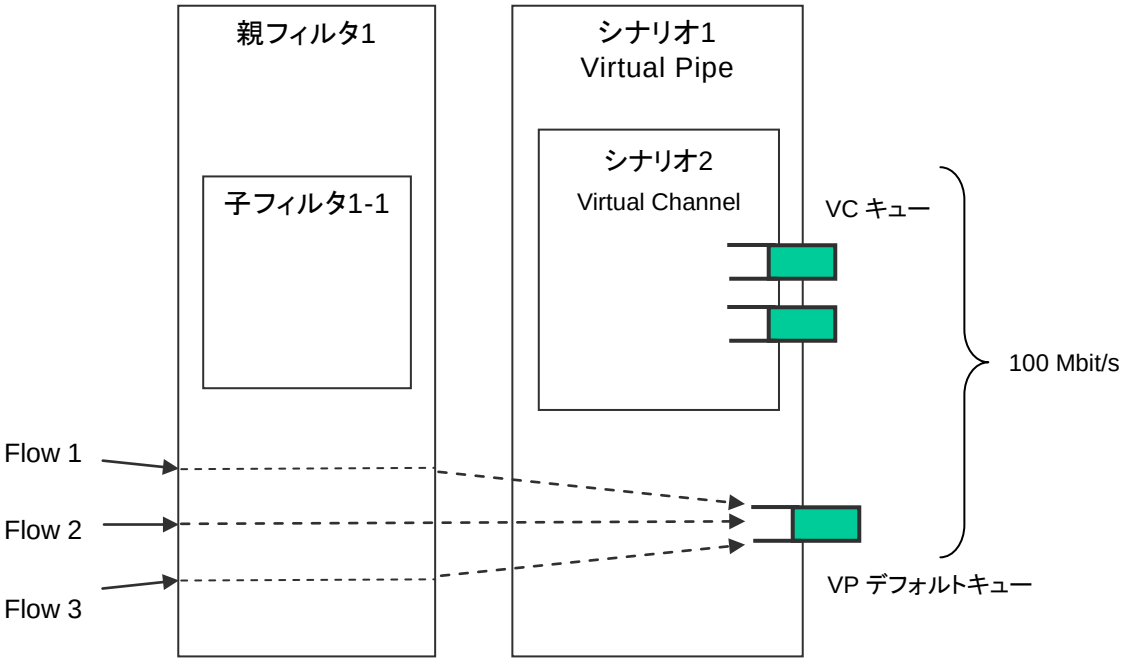
また，以下の 3 つのトラフィックが入力されたと仮定します。

- 192.168.1.1 から 192.168.1.100 へのトラフィック（Flow 1）
- 192.168.1.1 から 192.168.1.150 へのトラフィック（Flow 2）
- 192.168.1.1 から 192.168.1.200 へのトラフィック（Flow 3）

これらのフローは，親フィルタに一致し，子フィルタに一致しないため，VP デフォルトキューにパケットを格納します。

- Flow 1～3 の合計が 100 Mbit/s

Virtual Pipe として，合計 100 Mbit/s の帯域を保証します。



ただし，Virtual Channel で優先度が高いクラスの VC キューに割り当てられたフローが流れている場合，VP デフォルトキューに割り当てられたフローの合計は 100 Mbit/s の帯域を保証することができません。Virtual Channel のフローで使用している帯域と合わせて，100 Mbit/s を保証します。

(2) 集約キュー(VC キュー)

Aggregate(集約キューモード)の Virtual Channel シナリオとは，子フィルタに一致した複数のフローを 1 つの VC キューに集約して割り当てる方式です。

親フィルタに一致し，子フィルタにも一致したすべてのフローを同じ VC キューに割り当て，トラフィックコントロールを行います。

たとえば，送信元 IP アドレスが 192.168.10.1 で，宛先 IP アドレスが 192.168.10.100，192.168.10.150，192.168.10.200 の場合に，Virtual Channel シナリオの集約キューで最大帯域 10 Mbit/s に設定した場合は，以下のようになります。

本装置に，以下のフィルタを登録したと仮定します。

- 親フィルタ 1
  送信元 IP アドレス ： 192.168.0.0/16
  宛先 IP アドレス ： 192.168.0.0/16
- 子フィルタ 1-1
  送信元 IP アドレス ： 192.168.10.0/24
  宛先 IP アドレス ： 192.168.10.0/24

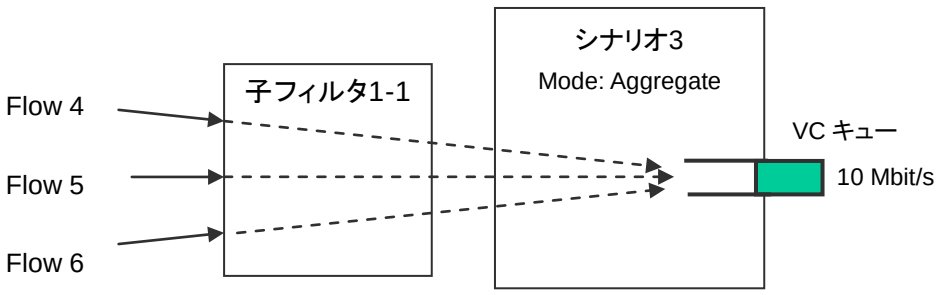
また，以下の 3 つのトラフィックが入力されたと仮定します。

- 192.168.10.1 から 192.168.10.100 へのトラフィック(Flow 4)
- 192.168.10.1 から 192.168.10.150 へのトラフィック(Flow 5)
- 192.168.10.1 から 192.168.10.200 へのトラフィック(Flow 6)

これらのフローは，親フィルタに一致し，子フィルタにも一致するため，VC キュー(集約キュー)にパケットを格納します。

- Flow 4～6 の合計が 10 Mbit/s

Virtual Channel として，合計 10 Mbit/s の帯域を使用します。



（3）個別キュー（VC キュー）

Individual（個別キューモード）の Virtual Channel シナリオとは，子フィルタに一致した複数のフローに対して，個別の VC キューを割り当てる方式です。

親フィルタに一致し，子フィルタにも一致したフローごとに VC キューを割り当て，トラフィックコントロールを行います。

たとえば，送信元 IP アドレスが 192.168.20.1 で，宛先 IP アドレスが 192.168.20.100，192.168.20.150，192.168.20.200 の場合に，Virtual Channel シナリオの個別キューで最大帯域 10 Mbit/s に設定した場合は，以下のようになります。

本装置に，以下のフィルタを登録したと仮定します。

- 親フィルタ 1
  送信元 IP アドレス ： 192.168.0.0/16
  宛先 IP アドレス ： 192.168.0.0/16
- 子フィルタ 1-2
  送信元 IP アドレス ： 192.168.20.0/24
  宛先 IP アドレス ： 192.168.20.0/24

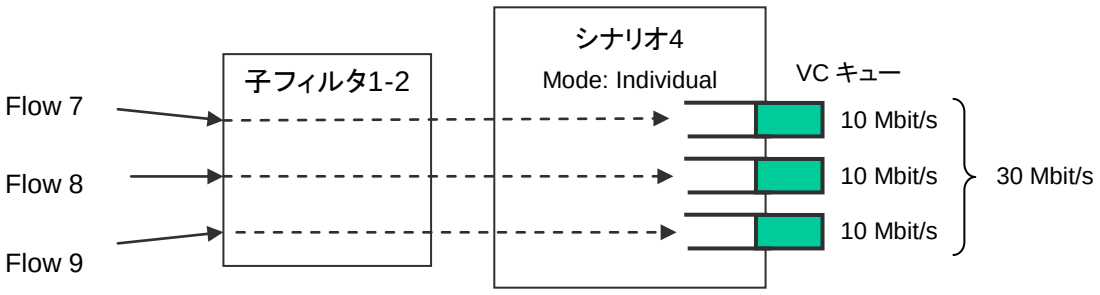
また，以下の 3 つのトラフィックが入力されたと仮定します。

- 192.168.20.1 から 192.168.20.100 へのトラフィック（Flow 7）
- 192.168.20.1 から 192.168.20.150 へのトラフィック（Flow 8）
- 192.168.20.1 から 192.168.20.200 へのトラフィック（Flow 9）

これらのフローは，親フィルタに一致し，子フィルタにも一致するため，VC キュー（個別キュー）にパケットを格納します。

- Flow 7 は 10 Mbit/s
- Flow 8 は 10 Mbit/s
- Flow 9 は 10 Mbit/s

Virtual Channel として，合計 30 Mbit/s の帯域を使用します。



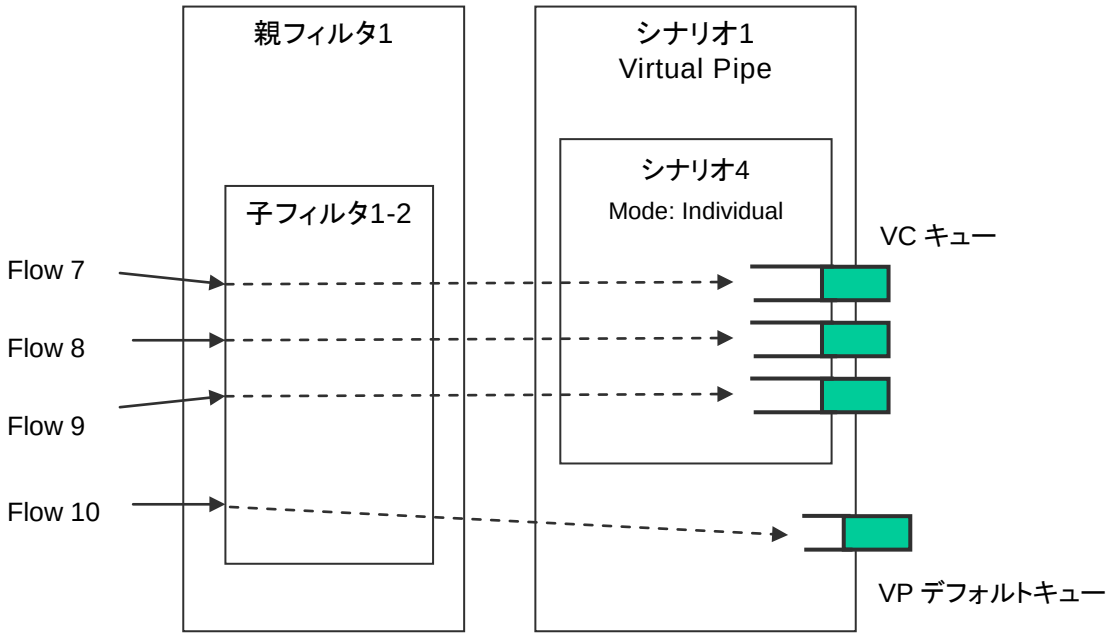
個別キューモードの場合，Virtual Channel シナリオで割り当てる VC キューの最大数を設定することが可能です。VC キューの最大数を超えてフローを作成する場合は，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。

たとえば，上記の例で，シナリオ 4 の VC キュー最大数 3，フェイルアクション forward とします。

本装置に，Flow 7～Flow 9 に加えて，以下のトラフィックが入力されたと仮定します。

- 192.168.20.1 から 192.168.20.250 へのトラフィック（Flow 10）

このフローは，親フィルタに一致し，子フィルタにも一致しますが，すでに VC キューを 3 個割り当てているため，フェイルアクション（Virtual Pipe 内でのベストエフォート転送）に従います。



また，フェイルアクション discard の場合は，Flow 10 のトラフィックを廃棄します。

VLAN フロー／キューは，VLAN フィルタにシナリオを結び付けると，Ethernet パケットを受信しなくても静的に作成します。たとえば，Virtual Channel シナリオ（個別キューモード）に結び付けた VLAN フィルタのフィルタ条件が VLAN ID=10～13 の場合，各 VLAN ID ごとに 4 個の VLAN フローを作成（フロー識別モードで CoS を識別しないとき）します。ただし，VC キュー最大数が 3 のため，VLAN ID=10～12 の 3 個の VLAN フローは VC キューに割り当てられますが，VLAN ID=13 の VLAN フローはフェイルアクションに従います。

（注）
VLAN フロー／キューの個別キューモードの場合，各 VLAN フローごとに VC キューを割り当てるため，VLAN フロー数分の VC キューを割り当てます。VLAN フィルタ条件をすべて省略した場合，すべての VLAN ID ごと（VLAN ID=0～4094，および VLAN Tag なし）の VLAN フローを作成しますので，装置内の VC キューが枯渇してしまいますのでご注意ください。これを回避するためには，VLAN フィルタ条件で範囲を制限するか，シナリオの VC キュー最大数を設定してください。

（4）アプリケーションキュー（VC キュー）

Application（アプリケーションキューモード）の Virtual Channel シナリオとは，アプリケーションの動作に応じて，各アプリケーションのメディアセッションごとに VC キューを動的に割り当てる方式です。アプリケーションキューを使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。

H.323 や SIP（Session Initiation Protocol）などの通話系アプリケーションの場合，以下のように VC キューを割り当て，トラフィックコントロールを行います。

- 制御セッション
  すべてのフローを同じ VC キュー（制御セッション用：制御セッションキュー）に割り当てます。（集約キュー）
- 音声セッション
  フローごとに VC キュー（音声セッション用：音声セッションキュー）を動的に割り当てます。
  音声セッションキューに割り当てる帯域やバッファサイズは，アプリケーションフィルタで認識したメディアセッション帯域を割り当てます。（個別キュー）
- 映像セッション
  フローごとに VC キュー（映像セッション用：映像セッションキュー）を動的に割り当てます。
  映像セッションキューに割り当てる帯域やバッファサイズは，アプリケーションフィルタで認識したメディアセッション帯域を割り当てます。（個別キュー）
- データセッション
  すべてのフローを同じ VC キュー（データセッション用：データセッションキュー）に割り当てます。（集約キュー）

FTP などのファイル転送系アプリケーションの場合，以下のように VC キューを割り当て，トラフィックコントロールを行います。

- 制御セッション
  すべてのフローを同じ VC キュー（制御セッション用：制御セッションキュー）に割り当てます。（集約キュー）
- データセッション
  すべてのフローを同じ VC キュー（データセッション用：データセッションキュー）に割り当てます。（集約キュー）

たとえば，H.323 の通話系アプリケーションの場合に，Virtual Channel シナリオのアプリケーションキューで割り当てる合計最低帯域 10 Mbit/s，制御セッションの最低帯域 500 kbit/s（5%），データセッションの最低帯域 1 Mbit/s（10%）に設定した場合は，以下のようになります。

本装置に，以下のフィルタを登録したと仮定します。

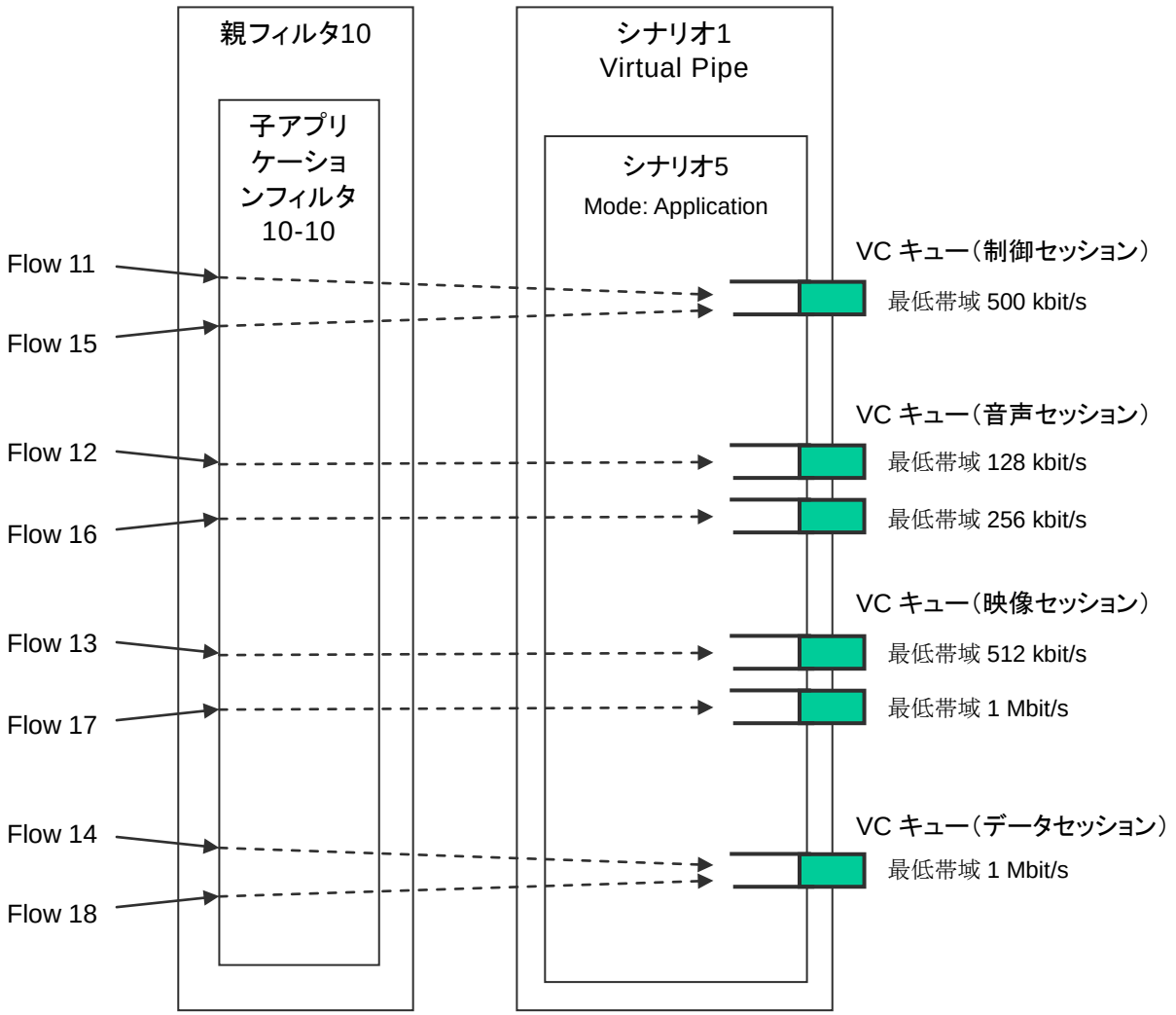
- 親フィルタ 10
  送信元 IP アドレス ： 192.168.30.0/24
- 子アプリケーションフィルタ 10-10
  アプリケーション名 ： h323

また，以下の 8 つの H.323 アプリケーショントラフィックが入力されたと仮定します。

- 192.168.30.1 からの H.323 制御トラフィック 1（Flow 11）
- 192.168.30.1 からの H.323 音声トラフィック 1（Flow 12）
- 192.168.30.1 からの H.323 映像トラフィック 1（Flow 13）
- 192.168.30.1 からの H.323 データトラフィック 1（Flow 14）
- 192.168.30.2 からの H.323 制御トラフィック 2（Flow 15）
- 192.168.30.2 からの H.323 音声トラフィック 2（Flow 16）
- 192.168.30.2 からの H.323 映像トラフィック 2（Flow 17）
- 192.168.30.2 からの H.323 データトラフィック 2（Flow 18）

これらのフローは，親フィルタに一致し，子アプリケーションフィルタにも一致するため，VC キュー（アプリケーションキュー）にパケットを格納します。

- Flow 11 と Flow15 の最低帯域 500 kbit/s（制御セッションキュー）
- Flow 12 のメディアセッション帯域 128 kbit/s（音声セッションキュー）
- Flow 13 のメディアセッション帯域 512 kbit/s（映像セッションキュー）
- Flow 16 のメディアセッション帯域 256 kbit/s（音声セッションキュー）
- Flow 17 のメディアセッション帯域 1 Mbit/s（映像セッションキュー）
- Flow 14 と Flow 18 の最低帯域 1 Mbit/s（データセッションキュー）

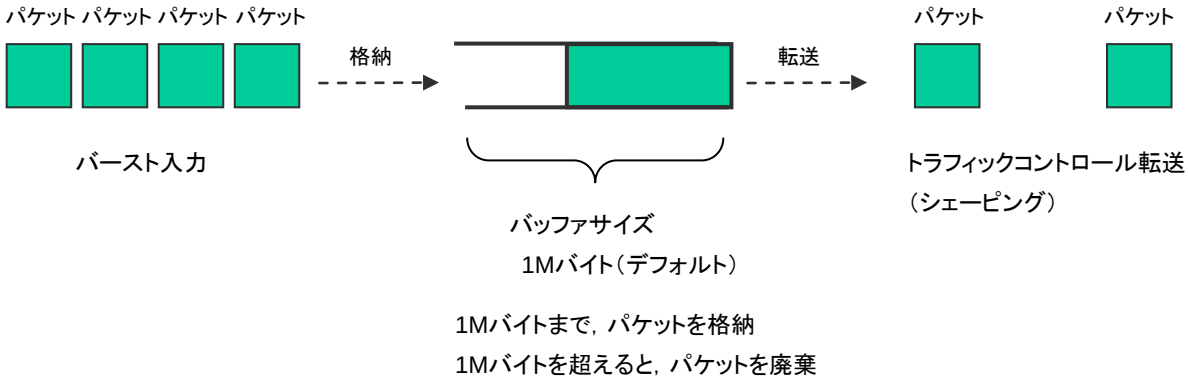


制御セッションキューとデータセッションキューは，アプリケーショントラフィックを受信しなくても静的に作成します。音声セッションキューと映像セッションキューは，アプリケーショントラフィックを受信したとき動的に作成します。

（5）バッファサイズ

VP デフォルトキュー／VC キューは，バッファサイズを設定することが可能です。

バッファサイズは，キューで許容できる入力バースト長です。バーストでパケット受信したときに，キューに格納できるバイト数です。

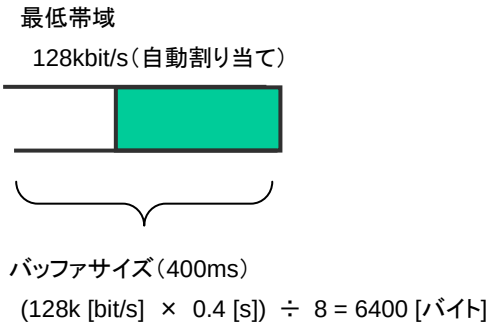


入力バースト長が，バッファサイズを超えてしまうと，パケットを廃棄します。バッファサイズ不足により，パケットが廃棄されてしまう場合，Virtual Pipe／Virtual Channel シナリオ（トラフィックアトリビュート）でバッファサイズを設定してください。

パケットが廃棄されているかどうかは，キュー統計情報で確認することができます。（詳細は第 10 章を参照してください）

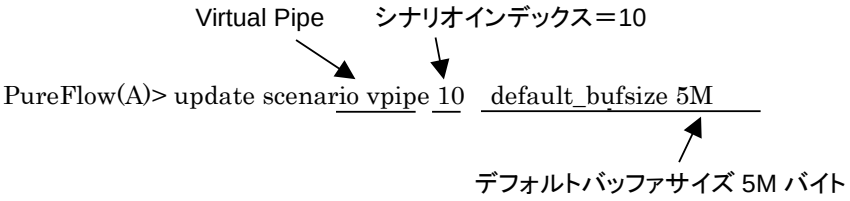
VP デフォルトキュー，および Aggregate／Individual の Virtual Channel シナリオで割り当てる VC キューのバッファサイズは，バイト指定で設定します。

Application の Virtual Channel シナリオで割り当てる VC キューのバッファサイズは，バイト指定，または時間指定で設定します。時間指定では，各メディアセッションの VC キューに自動で割り当てた最低帯域に対する時間となります。例えば，400ms と設定，VC キューの最低帯域として 128kbit/s が自動で割り当てられた場合は，6400 バイトとなります。

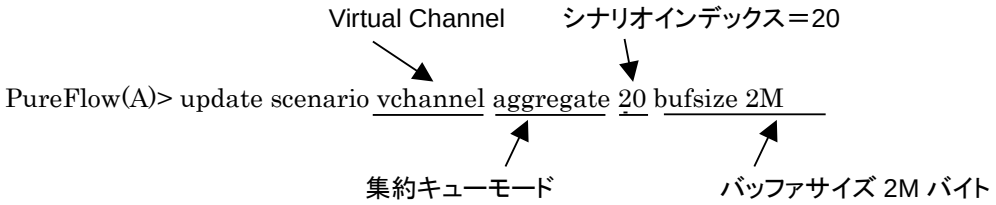


以下に，Virtual Pipe／Virtual Channel シナリオのバッファサイズを変更するコマンドを示します。

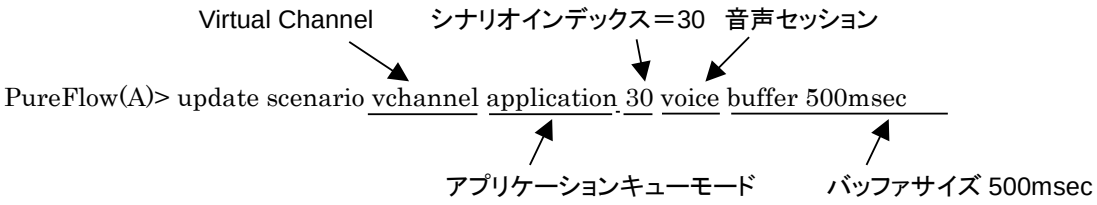
Sample 1）　すでに存在する Virtual Pipe シナリオのインデックス 10 に対して，デフォルトバッファサイズ 5M バイトに変更する場合



Sample 2）　すでに存在する Virtual Channel シナリオ（集約キューモード）のインデックス 20 に対して，バッファサイズ 2M バイトに変更する場合



Sample 3）　すでに存在する Virtual Channel シナリオ（アプリケーションキューモード）のインデックス 30 に対して，音声セッションのバッファサイズ 500ms に変更する場合



(6) クラス

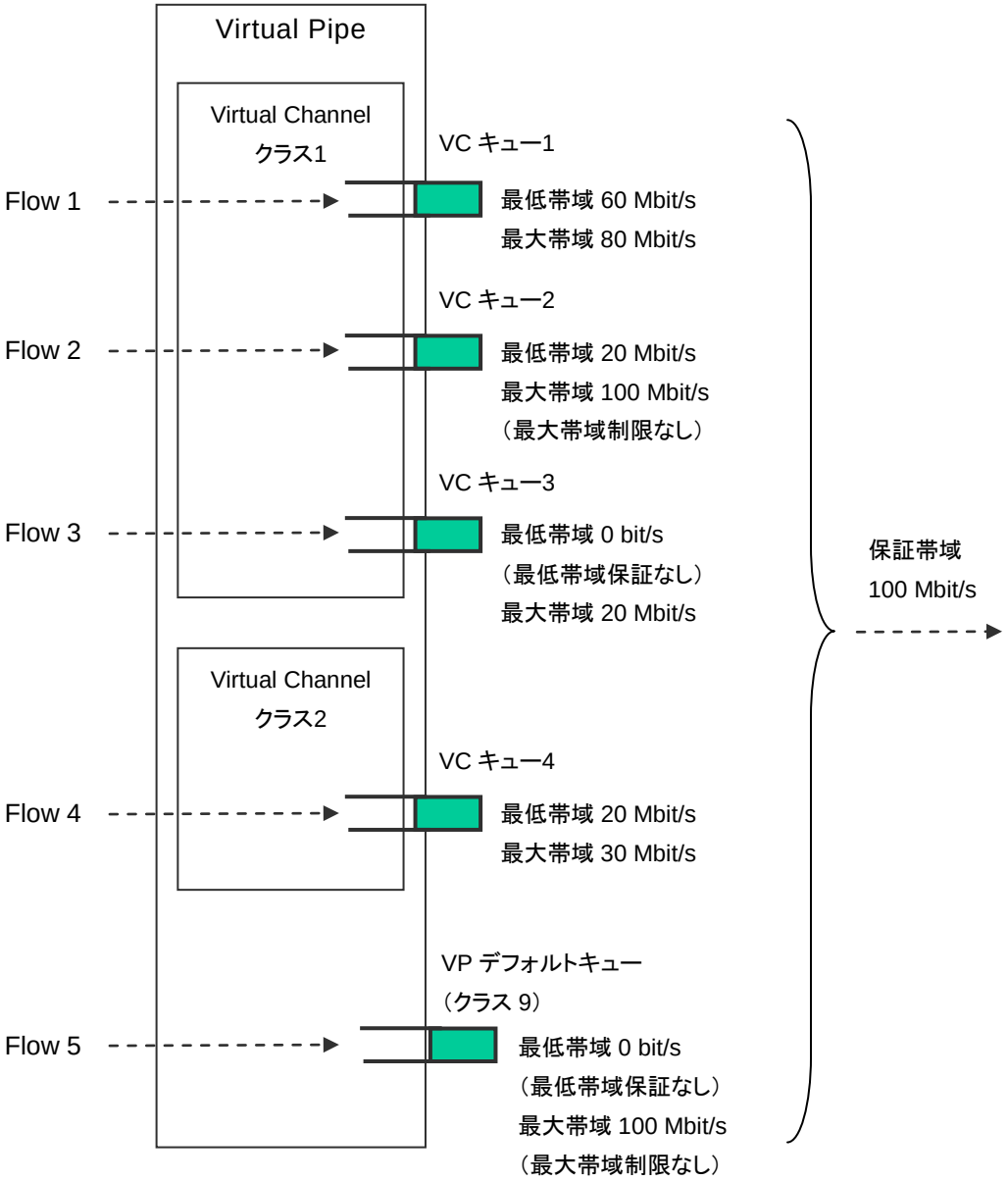
VC キューには，クラス(キューの優先順位)を設定することが可能です。

本装置のトラフィックコントロール方式は，9 クラス(クラス 1～8，およびクラス 9)の優先度に基づくキュー間を，優先度の高いものから出力していく方式(Strict Priority)です。

以下に，Strict Priority 動作を示します。

本装置に，以下の Virtual Pipe／Virtual Channel のキューを割り当てたものと仮定します。

- VP デフォルトキュー(クラス 9，保証帯域 100 Mbit/s)
- VC キュー1(クラス 1，最低帯域 60 Mbit/s／最大帯域 80 Mbit/s)
- VC キュー2(クラス 1，最低帯域 10 Mbit/s／最大帯域制限なし)
- VC キュー3(クラス 1，最低帯域保証なし／最大帯域 10 Mbit/s)
- VC キュー4(クラス 2，最低帯域 20 Mbit/s／最大帯域 30 Mbit/s)



a）　Virtual Pipe は，帯域を保証します。

たとえば，Virtual Pipe 外で 990 Mbit/s のフローが流れている場合でも，Virtual Pipe 内のフローは 100 Mbit/s を保証します。

ただし，各 Virtual Pipe に割り当てた保証帯域の合計が，Pipe の帯域を超えている場合，Virtual Pipe の帯域を保証できません。

b）　最低帯域保証ありの VC キューに割り当てられたフローは，最低帯域を保証します。

たとえば，Flow3（100 Mbit/s）のフローが流れている場合でも，Flow1（60 Mbit/s）のフローは 60 Mbit/s，Flow2（20 Mbit/s）のフローは 20 Mbit/s でトラフィックコントロールします。

ただし，各 Virtual Channel に割り当てた最低帯域の合計が，Virtual Pipe の保証帯域を超えている場合，Virtual Channel の最低帯域を保証できません。

c）　同じ Virtual Pipe 内に，複数のクラスの VC キューを割り当てた場合，優先度が低いクラスの VC キューのフローは，最低帯域を保証できません。優先度が低いクラスの VC キューは，優先度が高いクラスの余剰帯域でトラフィックコントロールします。

たとえば，Flow1（60 Mbit/s），Flow2（20 Mbit/s），Flow3（15 Mbit/s）のフロー（クラス 1）と，Flow4（20 Mbit/s）のフロー（クラス 2）が流れている場合，Flow4 は 5 Mbit/s でトラフィックコントロールします。

d）　最大帯域制限ありの VC キューに割り当てられたフローは，その最大帯域で制限します。

たとえば，Flow3（30 Mbit/s）が流れている場合は，Flow3 は 20 Mbit/s でトラフィックコントロールします。

また，VC キューの最大帯域が，Virtual Pipe の保証帯域を超えている場合，Virtual Pipe の保証帯域でトラフィックコントロールします。

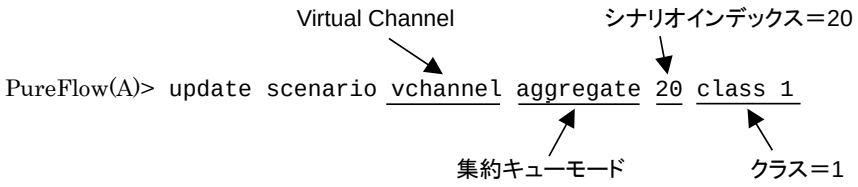
e）　最大帯域制限なしの VC キューに割り当てられたフローは，Virtual Pipe の保証帯域でトラフィックコントロールします。

たとえば，Flow2（120 Mbit/s）が流れている場合，Flow2 は 100 Mbit/s でトラフィックコントロールします。

VC キューに優先度をつけると，優先度の高いクラスのキューに格納されたパケットを優先して転送しますので，優先度が低いクラスに比べて，揺らぎが小さくなります。VC キューに優先度をつけたい場合，Virtual Channel シナリオ（トラフィックアトリビュート）でクラスを設定してください。

以下に，Virtual Channel シナリオのクラスを変更するコマンドを示します。

Sample）　すでに存在する Virtual Channel シナリオ（集約キューモード）のインデックス 20 に対して，クラス 1 に変更する場合



8.7.3　通信ギャップモード

Ethernetは，フレームを連続して送信する場合，フレームとフレームの間にギャップとプリアンブルが挿入されます。トラフィックアトリビュート（シナリオ，Network ポート）の帯域を設定するときに，これらを含めてトラフィックコントロール（ネットワーク帯域全体）を行うか，または含めないでトラフィックコントロール（フレームのみを対象）を行うかを選択することができます。本設定は，装置全体に適用します。

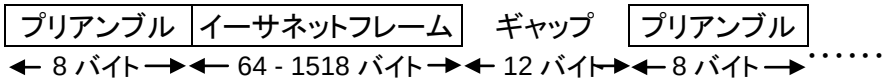


図　イーサネットフレームのギャップとプリアンブルについて

通信ギャップモードに関するCLIは以下のコマンドがあります。

set bandwidth mode {gap | no_gap}	通信帯域設定で，フレーム間ギャップとプリアンブルの有効／無効を選択します。デフォルト値は“no_gap”（無効）です。

コマンドの実行例を示します。

```
PureFlow(A)> set bandwidth mode gap
PureFlow(A)>
```

通信ギャップモードを有効としたときは，トラフィックアトリビュート（シナリオ，Network ポート）の帯域設定値による制御がフレーム間ギャップとプリアンブルを含めた制御となります。この設定は，帯域設定値が物理回線と同じ数値の意味を示しますので，出力 WAN 回線の帯域に対する輻輳回避や，トラフィックの優先制御を実施する場合に有効です。

通信ギャップモードを無効としたときは，トラフィックアトリビュート（シナリオ，Network ポート）の帯域設定値による制御がフレーム間ギャップとプリアンブルを含めないイーサネットフレームのみのデータレートとして制御します。この設定は，一般的にフレーム間ギャップやプリアンブルを含まないデータレートで示されているコンテンツ，映像，音声などのバースト回避のための平滑化，サーバに対して受信レートを制御するなどのコンテンツレート制御に有効です。

通信ギャップモードを無効で使用する場合は，トラフィックアトリビュート（シナリオ，Network ポート）の帯域設定値が回線帯域と異なる出力レートとなるので，通信ギャップを考慮した帯域設定値にする必要があります。たとえば回線帯域が100 Mbit/sの場合，すべてのフレーム長（64バイト～1522バイト）においてフレーム落ちなく転送できる設定値は約 76 Mbit/s になります。この場合，いかなるフレーム長においても 76 Mbit/s に制限するので，フレーム長が長いほど転送量に無駄が生じることになります。回線帯域を無駄なく使用する場合は，通信ギャップモードを有効に設定し，フレーム間ギャップを含めた帯域を設定してください。

8.7.4　Bridge-Ctrlパケット優先設定

本装置は，Bridge-Ctrl パケットと ARP パケットの優先制御機能を持ちます。
それらのパケットを優先することで，安定した通信を確保した上で，帯域制御を行うことができます。

本装置に対して VP の帯域の合計値が物理回線帯域と同じか超えてしまうような設定を行うと，VP のトラフィックが帯域を占有して Bridge-Ctrl パケットや ARP パケットの疎通ができなくなる場合があります。

本機能を利用することにより，Brdige-Ctrl パケットや ARP パケットを VP 内のトラフィックよりもさらに優先させ，通信の安定化をはかることが可能となります。

Bridge-Ctrl パケットとは，スパニングツリープロトコルで使用する BPDU パケットなどのような Destination MAC Address が 01-80-c2-00-00-00 から 01-80-c2-00-00-ff のパケットを言います。

Bridge-Ctrl パケット優先設定に関する CLI は以下のコマンドがあります。

set bridge-ctrl priority {high | low}	Bridge-Ctrl パケット優先設定で，Bridge-Ctrl パケットの通信優先度を設定します。デフォルト値は“low”です。

コマンドの実行例を示します。

```
PureFlow(A)> set bridge-ctrl priority high
PureFlow(A)>
```

8.7.5　シナリオ拡張オプション機能

この機能は PF7010A および PF7011A において，ライセンスキー3 が有効な場合のみ使用することができます。ライセンスキー3 が有効な場合，設定可能なシナリオ数の上限が拡張され，さらに，個別キューモードで使用可能なキュー数も拡張されます。

8.7.6　使用上の注意

(1) add filter subrule コマンドで，フィルタサブルールを設定した場合，PureFlow コンフィグマネージャによる管理は動作保証外になります。

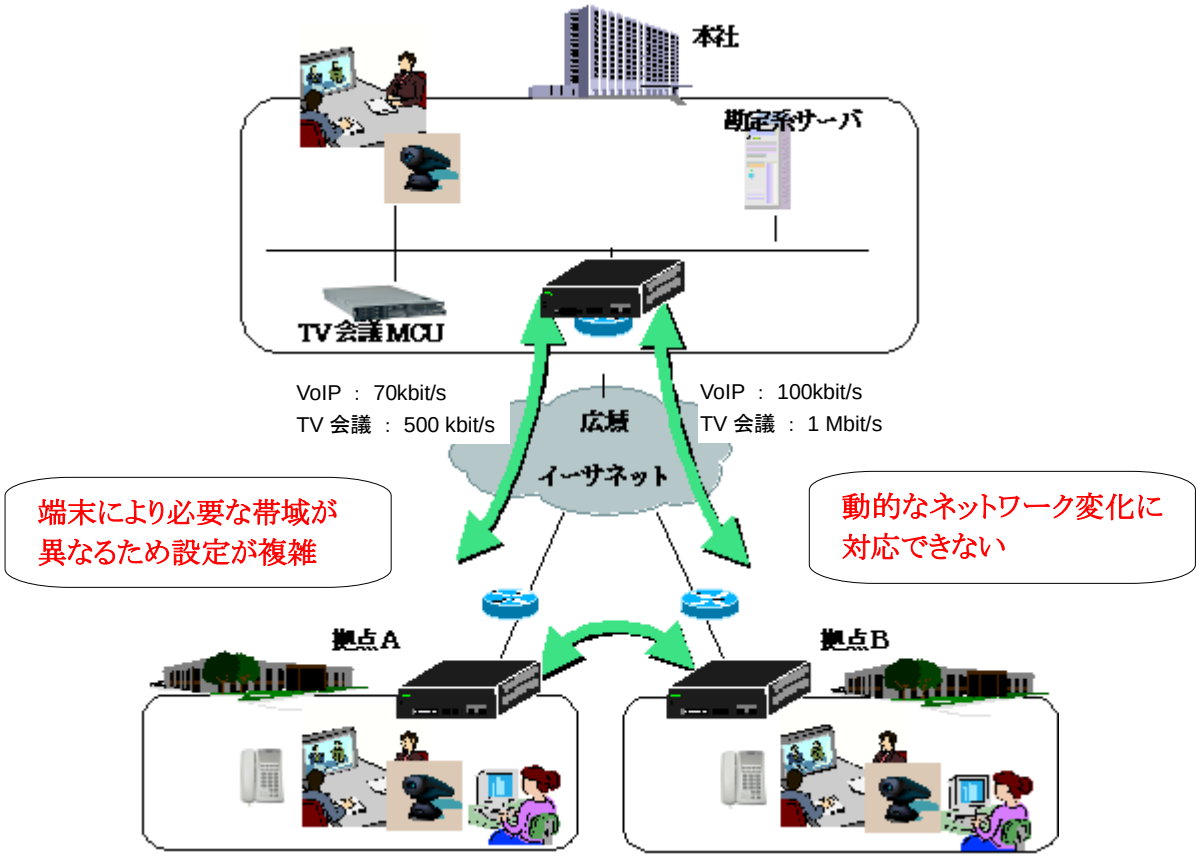
(2) ライセンスキー3(シナリオ拡張オプション)を有効にし，シナリオを 1024 個以上設定した場合，Web 監視機能，PureFlow モニタリングマネージャ，PureFlow コンフィグマネージャによる管理，監視は動作保証外になります。

前章の「トラフィックコントロール機能」では，基本的な階層化シェーピング機能と設定について説明しました。ここでは，その階層化シェーピング機能を拡張したコンテンツ・アウェア・シェーピング機能と設定について説明します。
なお，本機能を使用するにはオプションの「GS1 ライセンスキー1」を購入していただく必要があります。

9.1　概要

従来，ネットワーク管理者は，音声通信や TV 会議等のミッションクリティカルなトラフィックを回線帯域不足や通信遅延などの障害から守るために，各アプリケーションのメディアセッション（制御セッション／音声セッション／映像セッション／データセッションなど）ごとに必要な帯域を静的に割り当てる必要がありました。

ただし，これらのメディアセッションは，通話端末や使用するアプリケーションによって必要な帯域も異なるため，今までのような帯域を静的に割り当てる方法では，最適なトラフィックコントロールを行うことができません。また，アプリケーションごとに動的な任意のポート番号が使用されるので特定のメディアセッションを識別することが困難で，複雑な設定になってしまいます。さらに，IP 電話端末の追加／削除や IP アドレスの変更（DHCP による IP アドレス付与も含む）があった場合は，ルータや帯域制御装置の設定変更を行わなければなりません。

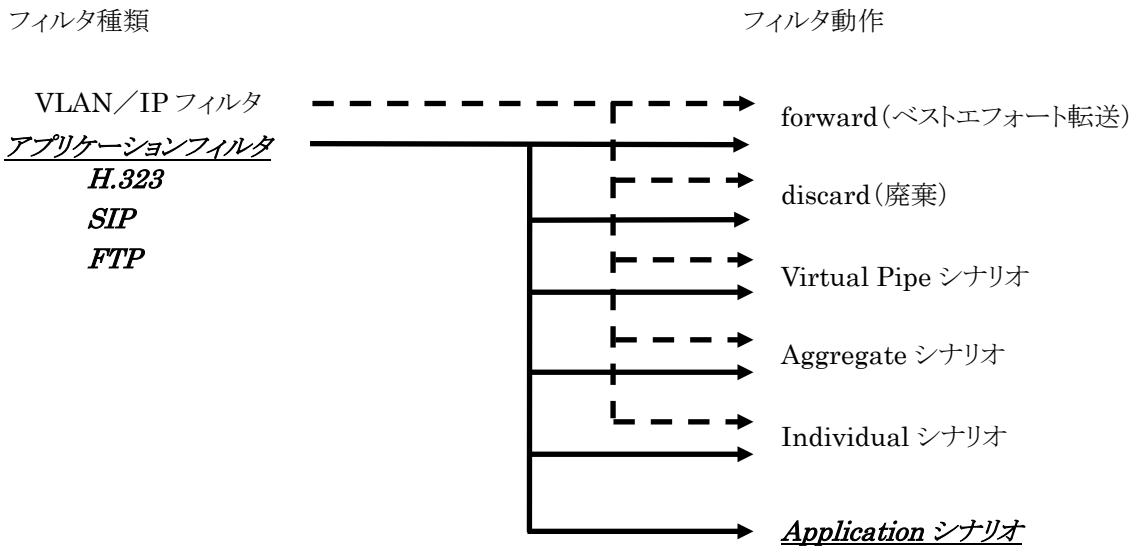


本装置は，このような問題を解決するために，音声通信や TV 会議等のアプリケーショントラフィックを認識し，各アプリケーションのメディアセッションごとに必要な帯域を自動で割り当てることで，最適なトラフィックコントロール（コンテンツ・アウェア・シェーピング）を実現します。

9.2　アプリケーションフィルタとアプリケーションシナリオ

従来のフィルタとシナリオでは，IP アドレスやポート番号などを明示的に指定することでトラフィックを分類し，分類したトラフィックに対して帯域を静的に割り当てることしかできません。そのため，自律的に変化するネットワークトラフィックに対して動的，かつ最適なトラフィックコントロールを行うことができませんでした。

本装置は，コンテンツ・アウェア・シェーピングを行うために，アプリケーションフィルタとアプリケーションシナリオを使用します。従来の VLAN／IP フィルタは，下図の点線で示すフィルタ動作を行うことができます。またアプリケーションフィルタは，下図の実線で示すフィルタ動作を行うことができます。



（注）
VLAN／IP フィルタを Application シナリオに結び付けることも可能ですが，各メディアトラフィックごとのトラフィックコントロールを行うことができません。この場合，すべてのフローはデータセッションキューに割り当てられます（キューの詳細は 8.6.2 章を参照してください）。

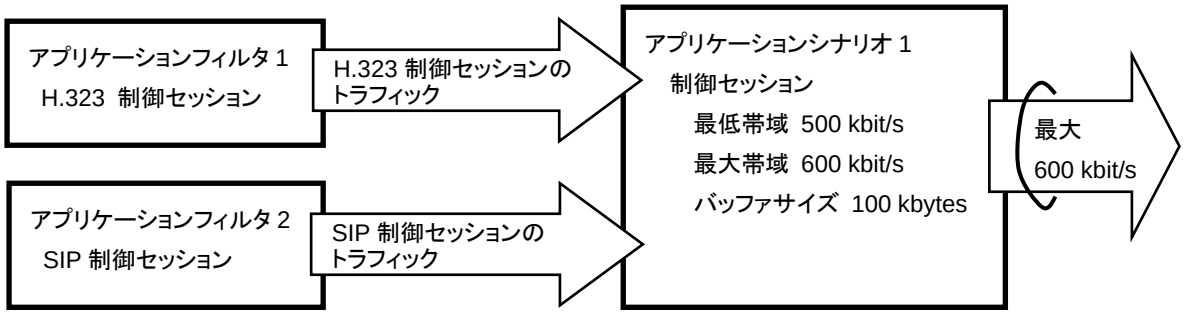
アプリケーションフィルタにより，各アプリケーションで使用する IP アドレスやポート番号などを分析し，各メディアセッションを認識します。

H.323 や SIP（Session Initiation Protocol）などの通話系アプリケーションの場合，メディアセッションとして制御セッション，音声セッション，映像セッション，データセッションを認識します。また，音声セッションと映像セッションについては，そのメディアセッションで要求された帯域（メディアセッション帯域）も自動で認識します。その後，アプリケーションシナリオというトラフィックアトリビュートにより，アプリケーションフィルタで認識したメディアセッション帯域やバッファサイズを動的に割り当て，トラフィックコントロールを行います。

FTP などのファイル転送系アプリケーションの場合，メディアセッションとして制御セッション，データセッションを認識します。

通常，各メディアセッションに必要な帯域は，端末設定や通話ごとに変動します。このため，自律的に変化するネットワークトラフィックを分析し，動的なトラフィックコントロールを行うことが必要となります。本装置のアプリケーションフィルタによりメディアセッションを認識することで，メディアセッションごとの柔軟なトラフィックコントロールを行うことができます。さらに H.323 や SIP などの通話系アプリケーションの場合，アプリケーションシナリオと組み合わせることで，メディアセッション帯域やバッファサイズを動的に割り当てること，最適なトラフィックコントロールを行うことができます。また，ノードアドレスの指定も不要なので，ノードの追加／削除が容易となり，DHCP 環境でも簡単に使用することができます。

また，複数のアプリケーションフィルタを同じシナリオに結び付けることが可能で，複数アプリケーションのメディアセッションで共有する帯域を割り当てることもできます。



9.2.1　アプリケーションフィルタ

アプリケーション認識するルールは，アプリケーションフィルタにより定義します。本装置では，アプリケーション名を指定した IP フィルタをアプリケーションフィルタと呼びます。

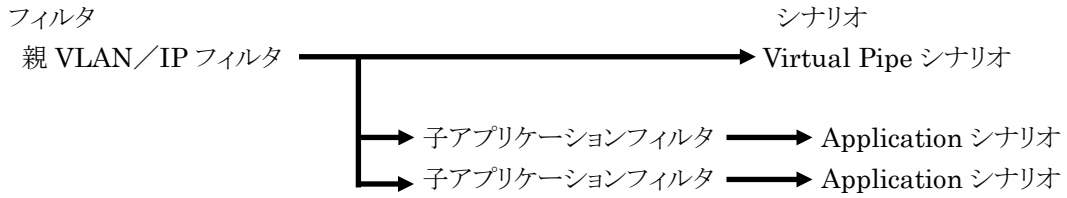
アプリケーションフィルタでは，以下のアプリケーションを認識します。

- H.323
- H.323 Control（H.323 制御セッション）
- H.323 Voice（H.323 音声セッション）
- H.323 Video（H.323 映像セッション）
- H.323 Data（H.323 データセッション）
- SIP（Session Initiation Protocol）
- SIP Control（SIP 制御セッション）
- SIP Voice（SIP 音声セッション）
- SIP Video（SIP 映像セッション）
- SIP Data（SIP データセッション）
- FTP（File Transfer Protocol）
- FTP Control（FTP 制御セッション）
- FTP Data（FTP データセッション）

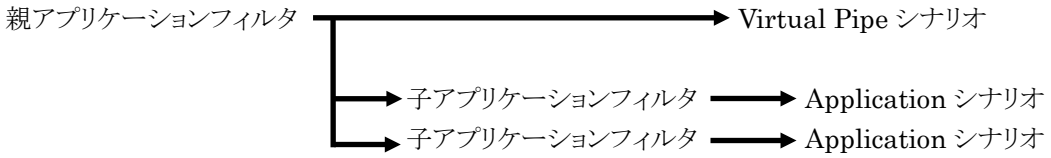
9.2.2　アプリケーションフィルタの親子関係

コンテンツ・アウェア・シェーピングを行うために，フィルタ／シナリオに親子関係を持たせて組み合わせる必要があります。

親 VLAN／IP フィルタで Virtual Pipe 内に流すトラフィックを抽出し，子アプリケーションフィルタで Virtual Channel 内に流すアプリケーションのメディアトラフィックを抽出します。アプリケーションシナリオには，子アプリケーションフィルタを結び付けてください。子アプリケーションフィルタで認識したメディアセッション帯域やバッファサイズを動的に割り当て，最適なトラフィックコントロールを行います。



また，子アプリケーションフィルタは，親アプリケーションフィルタと親子関係を作成することもできます。親アプリケーションフィルタで Virtual Pipe 内に流すアプリケーショントラフィックを抽出し，さらに子アプリケーションフィルタで Virtual Channel 内に流すアプリケーションのメディアトラフィックを抽出します。



9.2.3　アプリケーションシナリオ

アプリケーションシナリオは，アプリケーションフィルタにより認識したアプリケーションに応じて，各アプリケーションのメディアセッションに対して，動的なトラフィックコントロールを行うための設定（トラフィックアトリビュート）です。

アプリケーションシナリオには，以下のパラメータが指定できます。

- クラス　：　キューの優先順位です。クラス1が最優先とし以下クラス2，3，4，5，6，7，8　の順となります（デフォルト値が設定されるので，通常は設定する必要ありません）。

- 合計最低帯域　：　各メディアセッションごとに割り当てる最低帯域の合計です。この合計最低帯域内で，各メディアセッションの最低帯域を割り当てます。各メディアセッションに割り当てた最低帯域の合計が超えると，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。

- 制御セッション

  最低帯域　：　制御セッションに割り当てる最低帯域をパーセント指定します。本パラメータは，合計最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。

  最大帯域　：　制御セッションに割り当てる最大帯域をパーセント指定します。本パラメータは，制御セッションに割り当てた最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。

  バッファサイズ　：　制御セッションの許容できる入力バースト長です。本パラメータは，バイト指定，または時間指定ができます。時間指定では，制御セッションに割り当てた最低帯域に対する時間を設定します。入力バースト長を超えると，パケットは廃棄されます。

- 音声セッション

  最大帯域　：　音声セッションに割り当てる最大帯域をパーセント指定します。本パラメータは，音声セッションに割り当てた最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。音声セッションの最低帯域は，アプリケーションフィルタで認識したメディアセッション帯域を自動で割り当てます。

  バッファサイズ　：　音声セッションの許容できる入力バースト長です。本パラメータは，バイト指定，または時間指定ができます。時間指定では，音声セッションに割り当てた最低帯域に対する時間を設定します。入力バースト長を超えると，パケットは廃棄されます。（デフォルト値が設定されるので，通常は設定する必要ありません）。

- 映像セッション

  最大帯域　：　映像セッションに割り当てる最大帯域をパーセント指定します。本パラメータは，映像セッションに割り当てた最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。映像セッションの最低帯域は，アプリケーションフィルタで認識したメディアセッション帯域を自動で割り当てます。

  バッファサイズ　：　映像セッションの許容できる入力バースト長です。本パラメータは，バイト指定，または時間指定ができます。時間指定では，映像セッションに割り当てた最低帯域に対する時間を設定します。入力バースト長を超えると，パケットは廃棄されます。（デフォルト値が設定されるので，通常は設定する必要ありません）。

- データセッション

  最低帯域　：　データセッションに割り当てる最低帯域をパーセント指定します。本パラメータは，合計最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。

  最大帯域　：　データセッションに割り当てる最大帯域をパーセント指定します。本パラメータは，データセッションに割り当てた最低帯域に対する割合です（デフォルト値が設定されるので，通常は設定する必要ありません）。

  バッファサイズ　：　データセッションの許容できる入力バースト長です。本パラメータは，バイト指定，または時間指定ができます。時間指定では，データセッションに割り当てた最低帯域に対する時間を設定します。入力バースト長を超えると，パケットは廃棄されます。

- VC キュー最大数（maxqnum）　：　アプリケーションシナリオで割り当てる VC キューの最大数です。メディアセッションに割り当てた VC キューが最大数を超えると，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。

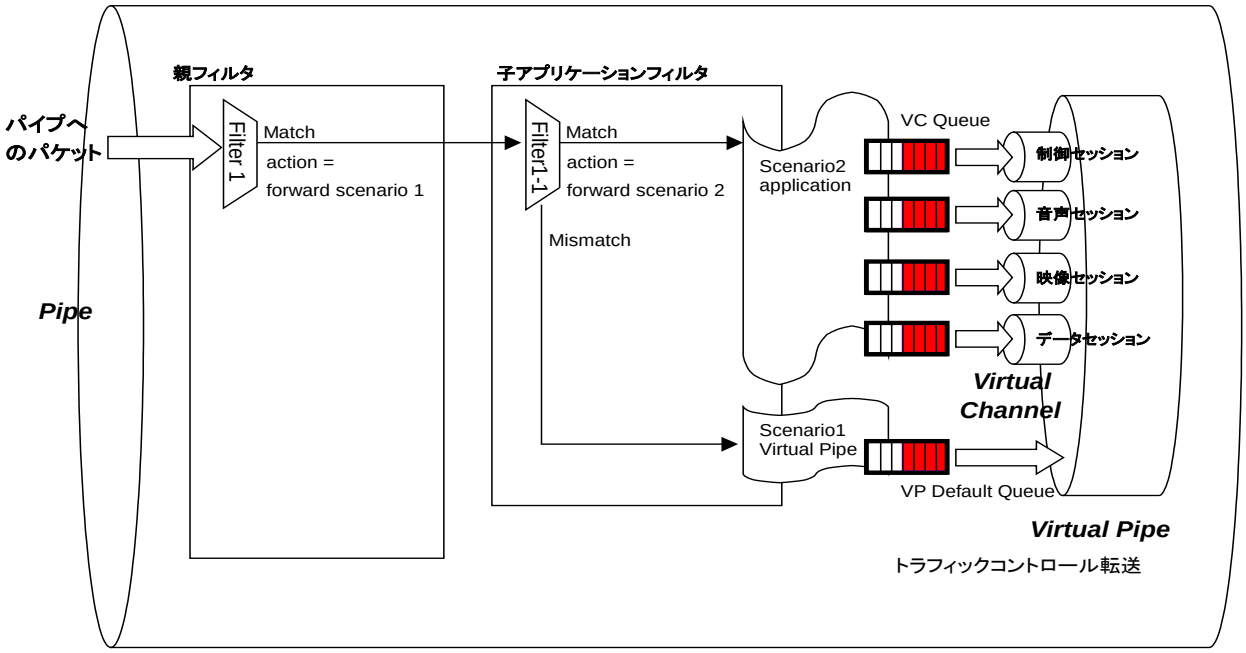
- フェイルアクション（failaction）　：　下記条件の場合に，VP デフォルトキューで転送，または廃棄します。
  ・VC キューを最大数まで使用している
  ・メディアセッションに割り当てた最低帯域の合計が合計最低帯域を超えた
  ・メディアセッション帯域を認識できなかった

アプリケーションシナリオは，Virtual Channel 用のシナリオです。

また，Virtual Pipe／Virtual Channel シナリオには，シナリオ名を設定することが可能です。シナリオ名に拠点やユーザの名前を設定しておくと，各 Virtual Pipe／Virtual Channel シナリオの管理が容易になります。

9.2.4　アプリケーションフィルタとアプリケーションシナリオの関係

本装置は，Pipe 内に流れるパケットをフィルタで分類し，アプリケーショントラフィックを抽出します。抽出したアプリケーショントラフィックを帯域，バッファサイズなどのトラフィックアトリビュートに従ってトラフィックコントロール転送します。



上図は，アプリケーションフィルタとアプリケーションシナリオの設定と，実際のトラフィックコントロール動作の関係を示した概念図です。

装置はパケットが Pipe に入ってくると，親フィルタを通過し，親フィルタインデックスの若い順から親フィルタルールと一致するかどうか調べます。

ある親フィルタルールと一致した場合，親フィルタの動作が“forward scenario”の場合は，その親フィルタと親子関係のある子フィルタを通過し，子フィルタインデックスの若い順から子フィルタルールと一致するかどうか調べます。

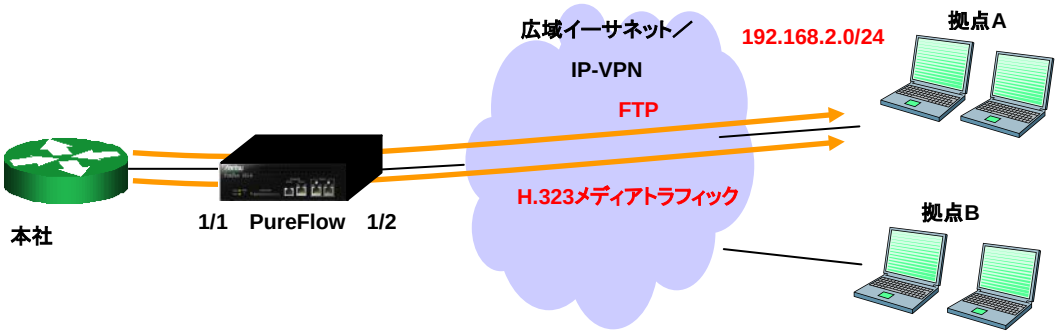
ある子アプリケーションフィルタルールと一致した場合，子アプリケーションフィルタの動作が“forward scenario”で Application の Virtual Channel シナリオと結び付けられている場合は，子アプリケーションフィルタにより認識したアプリケーションの動作に応じて，各アプリケーションのメディアセッションごとに Virtual Channel 内でパケットを転送します。また，子アプリケーションフィルタルールと一致しない場合は，Virtual Pipe 内で転送します。

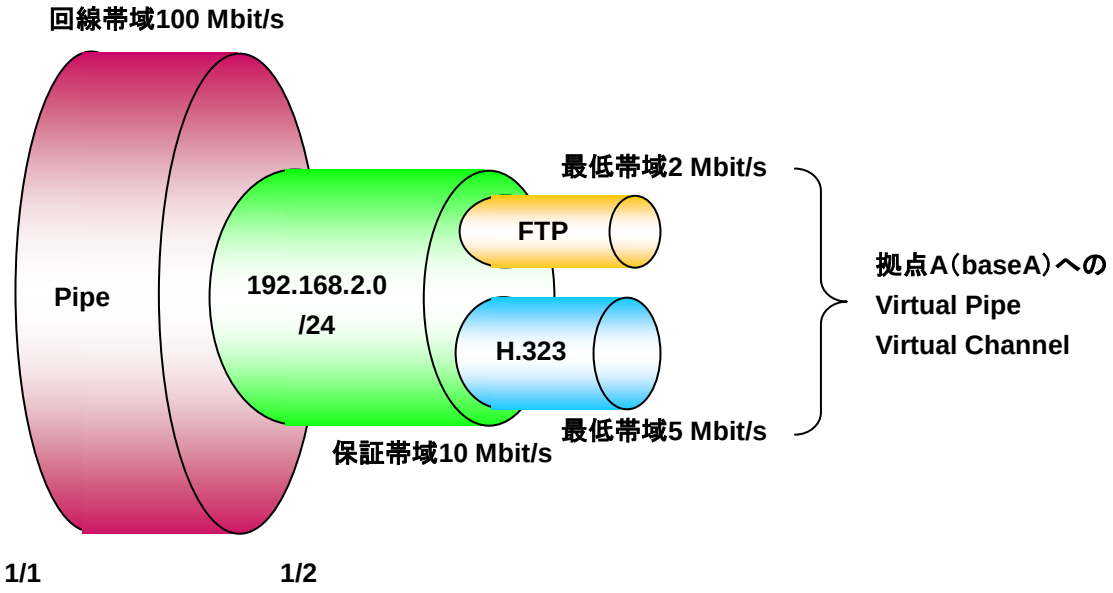
9.3　コンフィギュレーション例

以下のネットワーク環境の設定を行う場合のコンフィギュレーション例を示します。

[Case 1]アプリケーショントラフィックごとにトラフィックコントロールを行う

- 拠点 A のネットワークは 192.168.2.0/24 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
- 本社から拠点 A への保証帯域内で FTP トラフィックは最低帯域 2 Mbit/s にします(Virtual Channel)。
- 本社から拠点 A への保証帯域内で TV 会議(H.323)トラフィックは最低帯域 5 Mbit/s にします(Virtual Channel)。





以下のコマンドを実行します。

＜フロー識別モード＞

```
PureFlow(A)> set filter mode in 1/1 appli
PureFlow(A)> set filter mode in 1/2 appli
```

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 11000 ipv4 in 1/1 dip 192.168.2.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 11000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 11000-11000 ipv4 in 1/1 appli ftp
PureFlow(A)> add filter 11000-11001 ipv4 in 1/1 appli h323
PureFlow(A)> add scenario vchannel aggregate 2 min_bandwidth 2M name baseA_FTP
PureFlow(A)> add scenario vchannel aggregate 3 min_bandwidth 5M name baseA_H323
PureFlow(A)> set filter 11000-11000 action forward scenario 2
PureFlow(A)> set filter 11000-11001 action forward scenario 3
```

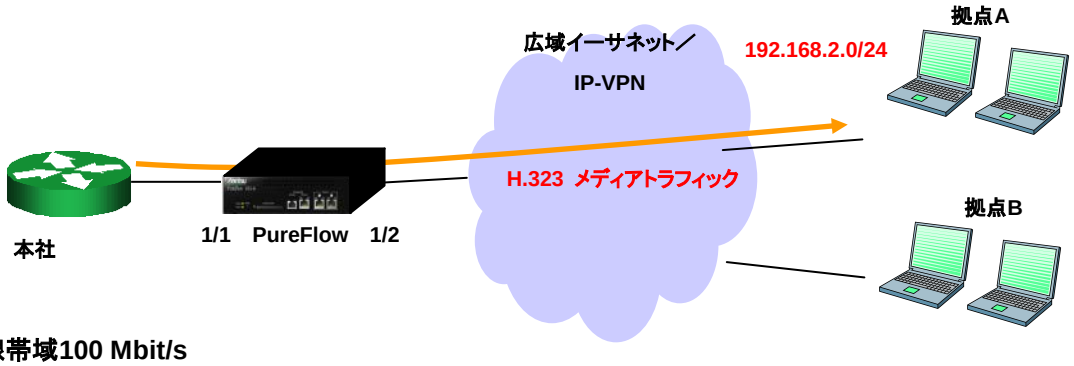
また，現在のアプリケーション認識しているセッションを確認するには，以下のコマンドを使用します。

```
PureFlow(A)> show application session
Session Information
-----------------------------------------------------------------
Session ID
  InPort               VID
  SIP
  DIP
  Protocol           SPort               DPort
  Session       ElapsedTime[sec]       RequestBW[bps]
-----------------------------------------------------------------
Session 1
  1/1                 none
  192.168.1.100
  192.168.2.100
  TCP                2042                  21
  ftp.control         86                  ----
-----------------------------------------------------------------
Session 2
  1/1                 none
  192.168.1.100
  192.168.2.100
  TCP                2049                  20
  ftp.data            63                  ----
-----------------------------------------------------------------
Session 3
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                5047                 5047
  h323.control        31                  ----
-----------------------------------------------------------------
Session 4
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                5046                 5046
  h323.voice          31                  128k
-----------------------------------------------------------------
Session 5
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                5049                 5049
  h323.control        63                  ----
-----------------------------------------------------------------
Session 6
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                5048                 5048
  h323.video          63                  512k
PureFlow(A)>
```

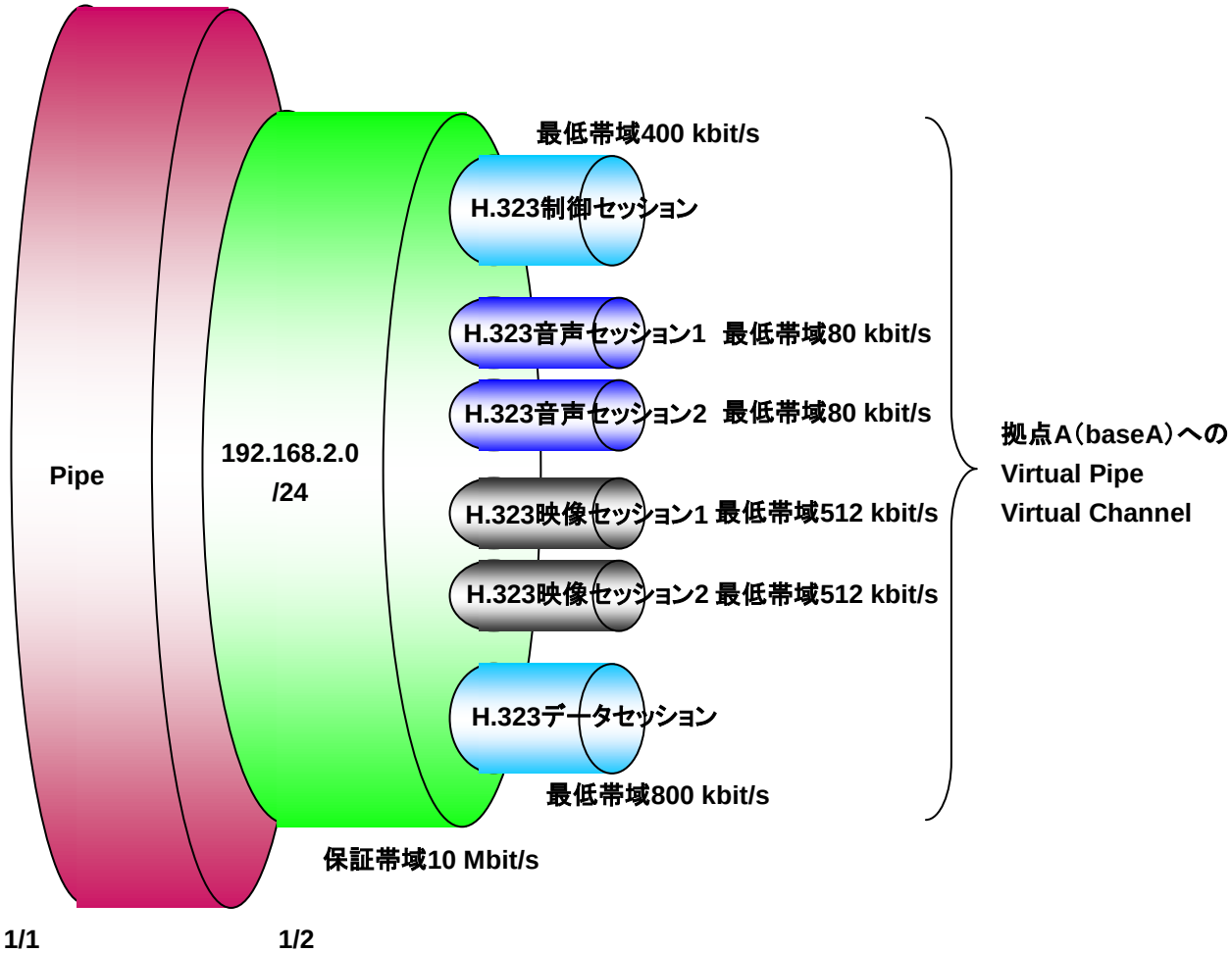
FTP制御セッション（Session 1），FTPデータセッション（Session 2），H.323制御セッション（Session 3, 5），H.323音声セッション（Session 4），H.323映像セッション（Session 6）を認識していることが分かります。
[Case 1] の場合，H.323音声セッションとH.323映像セッションに対して，Aggregate（集約キューモード）のVirtual Channelシナリオを結び付けているので，アプリケーションフィルタにより認識したメディアセッション帯域（RequestBW）を割り当てません。

[Case 2]アプリケーショントラフィックのメディアセッションごとにトラフィックコントロールを行う

- 拠点 A のネットワークは 192.168.2.0/24 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
- 本社から拠点 A への保証帯域内で，H.323 制御セッションは最低帯域 400 kbit/s にします(Virtual Channel)。
- 本社から拠点 A への保証帯域内で，H.323 音声セッションはそれぞれ最低帯域 80 kbit/s(Virtual Channel)。
- 本社から拠点 A への保証帯域内で，H.323 映像セッションはそれぞれ最低帯域 512 kbit/s(Virtual Channel)。
- 本社から拠点 A への保証帯域内で，H.323 データセッションは最低帯域 800 kbit/s にします(Virtual Channel)。



回線帯域100 Mbit/s



以下のコマンドを実行します。

＜フロー識別モード＞

```
PureFlow(A)> set filter mode in 1/1 appli
PureFlow(A)> set filter mode in 1/2 appli
```

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 11000 ipv4 in 1/1 dip 192.168.2.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 11000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 11000-11000 ipv4 in 1/1 appli h323.control
PureFlow(A)> add filter 11000-11001 ipv4 in 1/1 appli h323.voice
PureFlow(A)> add filter 11000-11002 ipv4 in 1/1 appli h323.video
PureFlow(A)> add filter 11000-11003 ipv4 in 1/1 appli h323.data
PureFlow(A)> add scenario vchannel aggregate 2 min_bandwidth 400k
                name baseA_H323_CONTROL
PureFlow(A)> add scenario vchannel individual 3 min_bandwidth 80k
                name baseA_H323_VOICE
PureFlow(A)> add scenario vchannel individual 4 min_bandwidth 512k
                name baseA_H323_VIDEO
PureFlow(A)> add scenario vchannel aggregate 5 min_bandwidth 800k
                name baseA_H323_DATA
PureFlow(A)> set filter 11000-11000 action forward scenario 2
PureFlow(A)> set filter 11000-11001 action forward scenario 3
PureFlow(A)> set filter 11000-11002 action forward scenario 4
PureFlow(A)> set filter 11000-11003 action forward scenario 5
```

また，現在のアプリケーション認識しているセッションを確認するには，以下のコマンドを使用します。

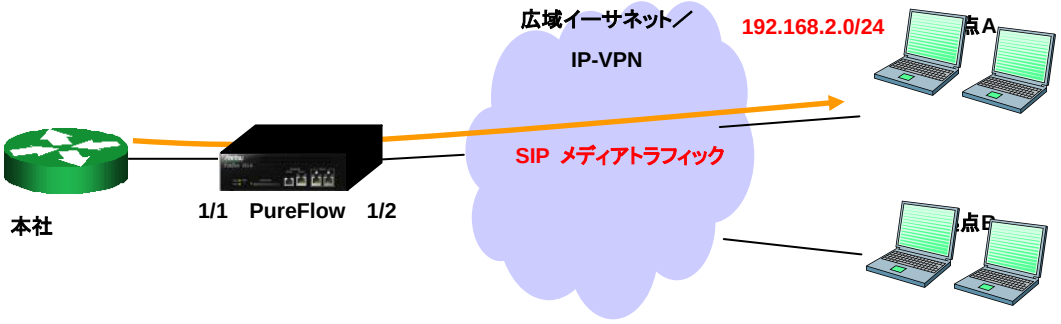
```
PureFlow(A)> show application session
Session Information
-----------------------------------------------------------------
Session ID
  InPort                VID
  SIP
  DIP
  Protocol            SPort                DPort
  Session       ElapsedTime[sec]       RequestBW[bps]
-----------------------------------------------------------------
Session 1
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5045                 5045
  h323.control          27                 ----
-----------------------------------------------------------------
Session 2
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5044                 5044
  h323.voice            28                 128k
-----------------------------------------------------------------
Session 3
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5047                 5047
  h323.control          31                 ----
-----------------------------------------------------------------
Session 4
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5046                 5046
  h323.video            31                 512k
-----------------------------------------------------------------
Session 5
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6045                 6045
  h323.control          27                 ----
-----------------------------------------------------------------
Session 6
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6044                 6044
  h323.voice            28                 256k
-----------------------------------------------------------------
Session 7
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6047                 6047
  h323.control          31                 ----
-----------------------------------------------------------------
Session 8
```

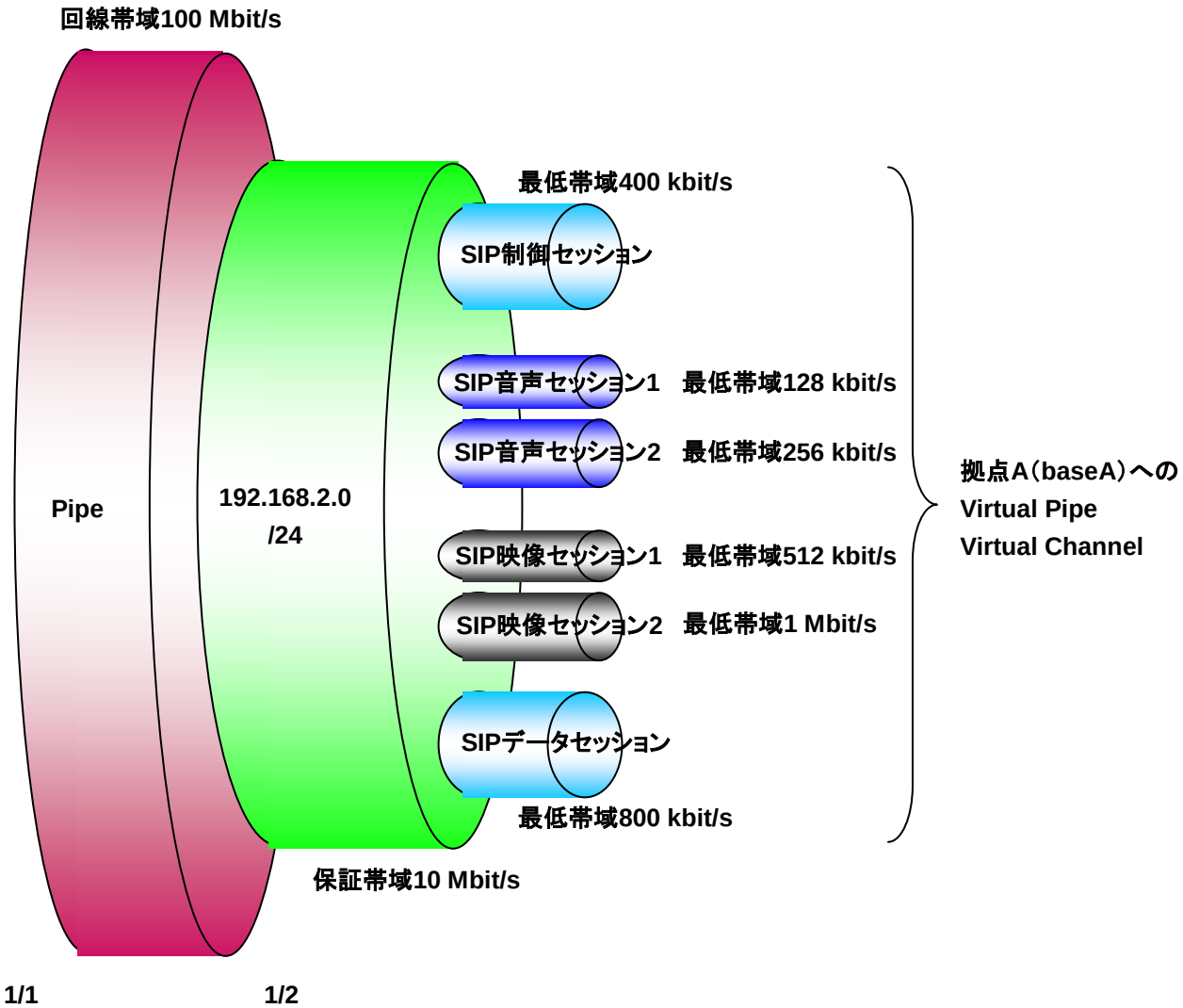
```
  1/1                  none
  192.168.1.201
  192.168.2.201
  UDP                  6046                 6046
  h323.video             31                 1M
PureFlow(A)>
```

H.323制御セッション（Session 1, 3, 5, 7），H.323音声セッション（Session 2, 6），H.323映像セッション（Session 4, 8）を認識していることが分かります。
[Case 2] の場合，H.323音声セッションとH.323映像セッションに対して，Individual（個別キューモード）のVirtual Channelシナリオを結び付けているので，アプリケーションフィルタにより認識したメディアセッション帯域（RequestBW）を割り当てません。

[Case 3]アプリケーショントラフィックの自動帯域割り当てによりトラフィックコントロールを行う

- 拠点 A のネットワークは 192.168.2.0/24 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
- 本社から拠点 A への保証帯域内で，SIP アプリケーションに割り当てる最低帯域の合計を 8 Mbit/s(合計最低帯域)とし，SIP 制御セッションは最低帯域 400 kbit/s(合計最低帯域の 5%)，データセッションの最低帯域 800 kbit/s(合計最低帯域の 10%)，SIP 音声セッションと SIP 映像セッションはメディアセッション帯域を自動認識し，メディアセッションごとに必要な帯域を割り当てます(Virtual Channel)。





以下のコマンドを実行します。

＜フロー識別モード＞

```
PureFlow(A)> set filter mode in 1/1 appli
PureFlow(A)> set filter mode in 1/2 appli
```

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 11000 ipv4 in 1/1 dip 192.168.2.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 11000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 11000-11000 ipv4 in 1/1 appli sip
PureFlow(A)> add scenario vchannel application 2 total_min_bandwidth 8M
                 control min_bw 5 data min_bw 10 name baseA_SIP_APPLICATION
PureFlow(A)> set filter 11000-11000 action forward scenario 2
```

また，現在のアプリケーション認識しているセッションを確認するには，以下のコマンドを使用します。

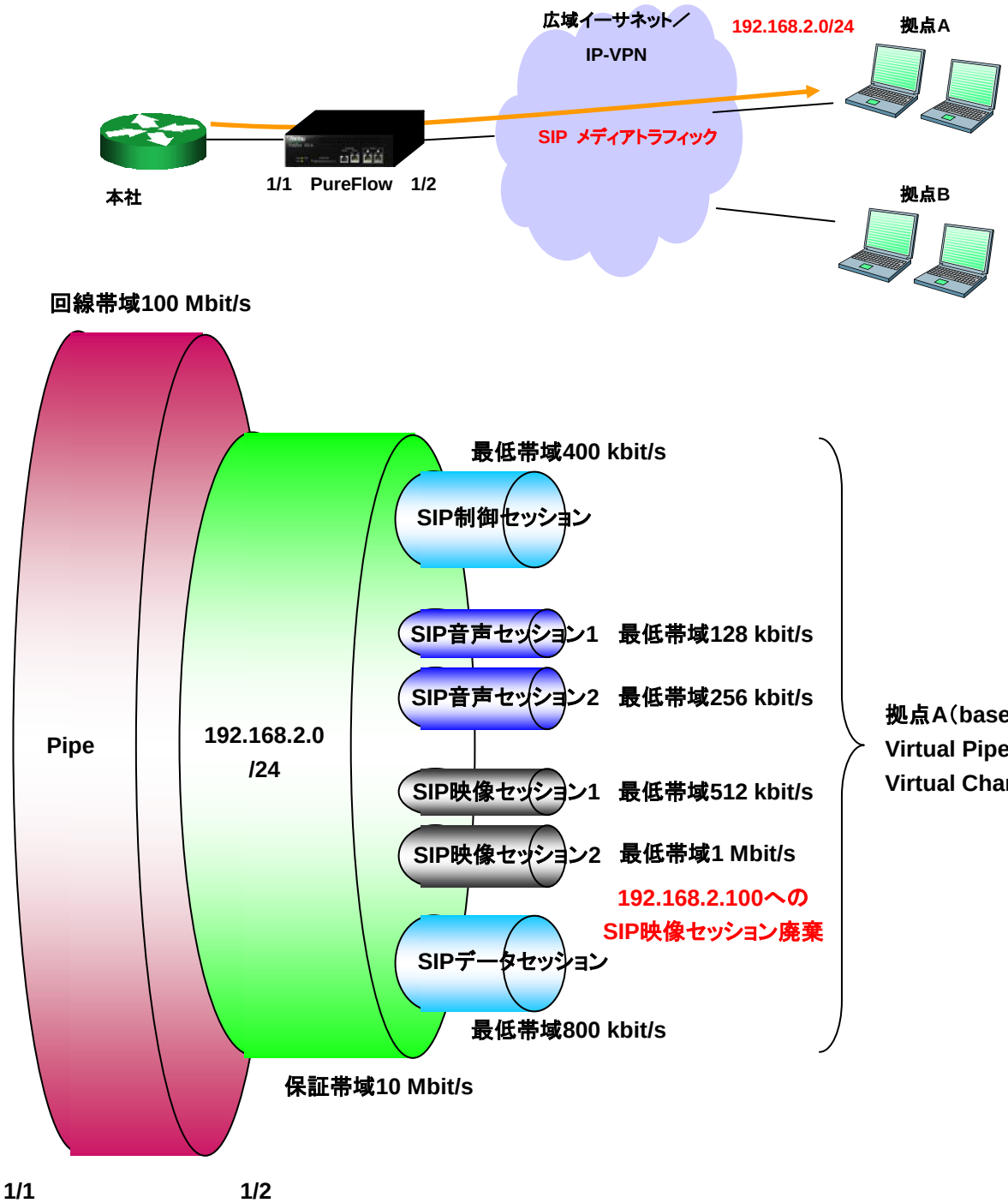
```
PureFlow(A)> show application session
Session Information
-----------------------------------------------------------------
Session ID
  InPort               VID
  SIP
  DIP
  Protocol           SPort               DPort
  Session       ElapsedTime[sec]       RequestBW[bps]
-----------------------------------------------------------------
Session 1
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5045                5045
  sip.control           27                ----
-----------------------------------------------------------------
Session 2
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5044                5044
  sip.voice             28                128k
-----------------------------------------------------------------
Session 3
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5047                5047
  sip.control           31                ----
-----------------------------------------------------------------
Session 4
  1/1                 none
  192.168.1.200
  192.168.2.200
  UDP                 5046                5046
  sip.video             31                512k
-----------------------------------------------------------------
Session 5
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6045                6045
  sip.control           27                ----
-----------------------------------------------------------------
Session 6
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6044                6044
  sip.voice             28                256k
-----------------------------------------------------------------
Session 7
  1/1                 none
  192.168.1.201
  192.168.2.201
  UDP                 6047                6047
  sip.control           31                ----
-----------------------------------------------------------------
Session 8
```

```
  1/1                  none
  192.168.1.201
  192.168.2.201
  UDP                  6046                 6046
  sip.video              31                   1M
PureFlow(A)>
```

SIP制御セッション（Session 1, 3, 5, 7），SIP音声セッション（Session 2, 6），SIP映像セッション（Session 4, 8）を認識していることが分かります。
[Case 3] の場合，SIP音声セッションとSIP映像セッションに対して，Application（アプリケーションキューモード）のVirtual Channelシナリオを結び付けているので，アプリケーションフィルタにより認識したメディアセッション帯域（RequestBW）を割り当てます。

[Case 4]アプリケーショントラフィックの自動帯域割り当てによるトラフィックコントロールとファイアウォールを同時に行う

- 拠点 A のネットワークは 192.168.2.0/24 です。
- 本社から拠点Aへの通信グループ(baseA)を保証帯域 10 Mbit/s にします(Virtual Pipe)。
- 本社から拠点 A への保証帯域内で，SIP アプリケーションに割り当てる最低帯域の合計を 8 Mbit/s(合計最低帯域)とし，SIP 制御セッションは最低帯域 400 kbit/s(合計最低帯域の 5%)，データセッションの最低帯域 800 kbit/s(合計最低帯域の 10%)，SIP 音声セッションと SIP 映像セッションはメディアセッション帯域を自動認識し，メディアセッションごとに必要な帯域を割り当てます(Virtual Channel)。
- 拠点 A 内の端末 192.168.2.100 への SIP 映像セッション通信は禁止とします。



以下のコマンドを実行します。

＜フロー識別モード＞

```
PureFlow(A)> set filter mode in 1/1 appli
PureFlow(A)> set filter mode in 1/2 appli
```

＜拠点 A への Virtual Pipe＞

```
PureFlow(A)> add filter 11000 ipv4 in 1/1 dip 192.168.2.0/255.255.255.0
PureFlow(A)> add scenario vpipe 1 bandwidth 10M name baseA
PureFlow(A)> set filter 11000 action forward scenario 1
```

＜拠点 A への Virtual Channel＞

```
PureFlow(A)> add filter 11000-11000 ipv4 in 1/1 dip 192.168.2.100 appli sip.video
PureFlow(A)> add filter 11000-11001 ipv4 in 1/1 appli sip
PureFlow(A)> add scenario vchannel application 2 total_min_bandwidth 8M
                control min_bw 5 data min_bw 10 name baseA_SIP_APPLICATION
PureFlow(A)> set filter 11000-11000 action discard
PureFlow(A)> set filter 11000-11001 action forward scenario 2
```

9.4　注意事項

コンテンツ・アウェア・シェーピングを使用するときの注意事項を，以下に示します。

（注 1）
ITU-T（International Telecommunication Union Telecommunication Standardization sector），RFC（Request For Comment）に準拠した動作をサポートします（サポートプロトコルは 9.5 章を参照してください）。一部の端末ベンダ固有の仕様については，サポートしません。

（注 2）
セッション制御プロトコルがメディアセッション帯域を通知しない場合，コーデックの種別から必要な帯域を決定します（認識可能なコーデックは 9.5 章を参照してください）。本装置で認識できないコーデックの場合は，最低帯域を割り当てることができないため，フェイルアクション（Virtual Pipe 内でのベストエフォート転送，または廃棄）に従います。最低帯域を割り当てることができなかったコーデック情報は Syslog に出力されます。

（注 3）
本装置のアプリケーション処理能力を超えて，セッション制御パケットがバースト的に発生した場合，正常にアプリケーション認識できない場合があります。その場合，セッション制御パケットはアプリケーションフィルタに一致しないため，トラフィックコントロールしないで転送します。

（注 4）
各アプリケーションで認識可能な最大同時接続数を下表に示します。これは，各アプリケーションを単独で使用した場合の最大同時接続数となります。これらのアプリケーションを組み合わせて使用した場合は，これ以下となります。

	最大同時接続数［接続］
H.323 音声	400
H.323 映像	222
SIP 音声	666
SIP 映像	285
FTP	1000

9.5　補足

9.5.1　サポートプロトコル

以下のプロトコルに準拠した動作をサポートします。

セッション制御プロトコル	H.323	ITU-T Recommendation H.323 – Annex R (2001), Robustness Methods for H.323 Entities ITU-T Recommendation H.225.0 (2000), Call signaling protocols and media stream packetization For packet based multimedia communications Systems ITU-T Recommendation H.245 (2003), Control protocol for multimedia communication ITU-T Recommendation Q.931 (1998), ISDN user-network interface layer 3 specification for basic call control
	SIP	RFC3261（SIP: Session Initiation Protocol） RFC2327（SDP: Session Description Protocol）
	RTCP	RFC1890（RTP Profile for Audio and Video Conferences with Minimal Control） RFC3551（RTP Profile for Audio and Video Conferences with Minimal Control）
メディア転送プロトコル	RTP	RFC1889（RTP: A Transport Protocol for Real-Time Applications） RFC3550（RTP: A Transport Protocol for Real-Time Applications）
ファイル転送プロトコル	FTP	RFC959（FILE TRANSFER PROTOCOL (FTP)） RFC2428（FTP Extensions for IPv6 and NATs）

9.5.2　コーデック

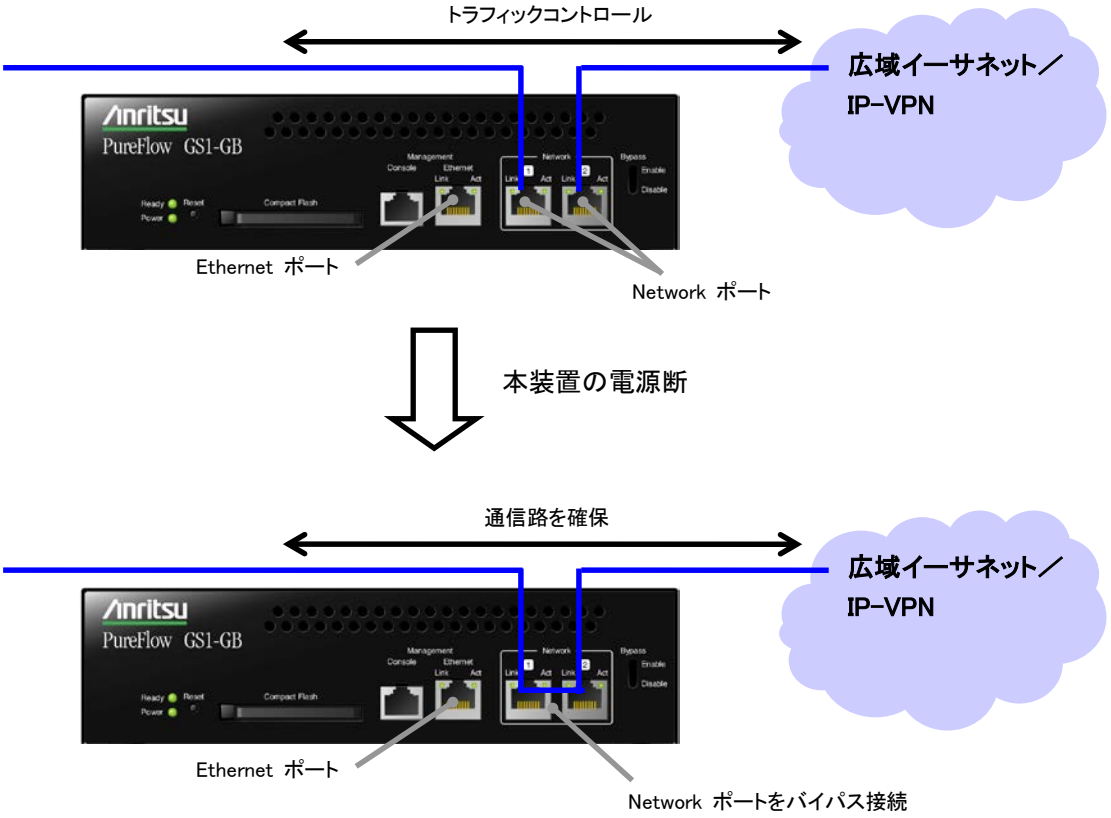
本装置で認識可能なコーデックを，以下に示します。

音声コーデック	G.711, G722.1, G722.2, G726, G.728, G729, G.723.1
映像コーデック	H.261, H263, H.263+, H.264

ここでは，Network ポートバイパス機能と設定について説明します。本機能は PureFlow GS1-FB，PureFlow GS1-GB で使用することができます。

10.1 概要

Network ポートバイパス機能とは，本装置の電源断時や障害発生時に Network ポートをバイパス接続して通信路を確保する機能です。



Network ポートをバイパス接続すると，本装置は Network ポートに接続されたネットワークから切り離された状態となります。その時，ポートがいったんリンクダウン状態となりますが，スイッチ／ルータ間で再度リンクが確立され通信が再開されます。ただし，Network ポートをバイパス接続した状態では本装置のトラフィックコントロールは働かず，スイッチ／ルータ間を直結した場合と同じになります。

Network ポートバイパス機能は 2 つの機能から成ります。

- 電源断時のバイパス機能
- 装置動作中のバイパス操作機能

以下ではそれぞれの機能について詳細を説明します。

10.2 電源断時のバイパス機能

本装置の電源が遮断されたとき Network ポートをバイパス接続します。本機能は装置前面のスイッチにより有効／無効の設定が可能です。

（注）
本機能によるバイパス接続は syslog への記録を行いません。

10.3 装置動作中のバイパス操作機能

本装置の動作中に自動または任意のバイパス操作を行うことができます。

任意のバイパス操作は以下のコマンドで行います。

set bypass {auto | connect | disconnect}	バイパスの操作方法を設定します。 auto 指定の場合，バイパス操作は自動で行われます。 connect 指定の場合，Network ポートを強制的にバイパス接続し，その状態を保ちます。 disconnect 指定の場合，Network ポートのバイパス接続を強制的に解除し，その状態を保ちます。 デフォルトは auto です。
bypass time <time> {connect | disconnect}	一時的なバイパス操作を実行します。 本コマンドを実行すると指定のバイパス操作を実行し，time 秒経過後にコマンド実行前のバイパス状態に戻します。 注）本コマンドは save config コマンドによる保存はできません。
show bypass	バイパスの状態および設定を表示します。

Network ポートを強制的にバイパス接続する場合，以下に示すコマンドを実行します。

システムインタフェースの通信ポートを Ethernet ポートに設定している場合
```
PureFlow(A)> set bypass connect
PureFlow(A)>
```

システムインタフェースの通信ポートを Network ポートに設定している場合
```
PureFlow(A)> set bypass connect
System interface might be disconnected from the network, ok (y/n)?y
Done
PureFlow(A)>
```

Network ポートを一時的に 300 秒間バイパス接続する場合，以下に示すコマンドを実行します。

システムインタフェースの通信ポートを Ethernet ポートに設定している場合
PureFlow(A)> bypass time 300 connect
Current time　: Nov 18　17:38:47
Expire time　: Nov 18　17:43:47
PureFlow(A)>

システムインタフェースの通信ポートを Network ポートに設定している場合
PureFlow(A)> bypass time 300 connect
System interface might be disconnected from the network, ok (y/n)?y
Current time　: Nov 18　17:38:47
Expire time　: Nov 18　17:43:47
Done
PureFlow(A)>

設定コマンドで設定した内容や，現在の Network ポートのバイパス状態を確認するには，“show bypass”コマンドを使用します。

```
PureFlow> show bypass
Control mode     : connect
Bypass state     : connect
Remaining time   : 0 [s]
PureFlow>
```

コマンドによるバイパス操作の他に通信の停止を回避するための自動バイパス操作機能があります。“set bypass”コマンドで auto を指定している場合，以下のタイミングでバイパス操作が行われます。

- 装置起動完了時
  Forwarding CPU の起動異常時にバイパス接続を行います。正常に起動した場合はバイパス接続の解除を行います。

- 装置異常検出時
  Forwarding CPU の異常検出時および Control CPU での重度のエラー発生時にバイパス接続を行います。

- “reboot system“コマンド実行時
  再起動前にバイパス接続を行います。

Control CPU での重度のエラー発生時のバイパス操作については syslog への記録は行われませんが，他のバイパス操作はいずれも syslog へ記録されます。記録される syslog メッセージは次の通りです。

- バイパス接続
  Bypass connected

- バイパス接続解除
  Bypass disconnected

10.4 Network ポートバイパス機能の注意事項

Network ポートをバイパス接続すると本装置がネットワークから切り離されるため，下記事項に注意してください。

バイパス接続状態では本装置はクロスケーブルであるかのように振舞います。本装置と対向装置を接続するケーブルの種類（クロス／ストレート）は，バイパス接続状態／未接続状態のいずれでもリンク確立できるように「PureFlow GS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A 取扱説明書」を参照し正しく選択してください。

バイパス接続状態では対向装置間が直結状態となるため，対向装置間の合計ケーブル長が 60m を超えないように接続してください。

バイパス操作時は対向装置のポートはいったんリンクダウンし，数秒後リンクが再確立します。
再確立するまでの時間は接続装置の特性により異なります。実運用前に確認することを推奨します。

バイパス接続状態の本装置の Network ポートはリンクダウン状態となり，リンク LED は消灯します。このため，Ethernet ポート経由で装置管理を行っている場合，バイパス操作時に SNMP のリンク変化トラップやリンク変化 syslog が送出されます。ただし，装置異常検出時のバイパス操作ではリンク変化が検出されない場合があります。

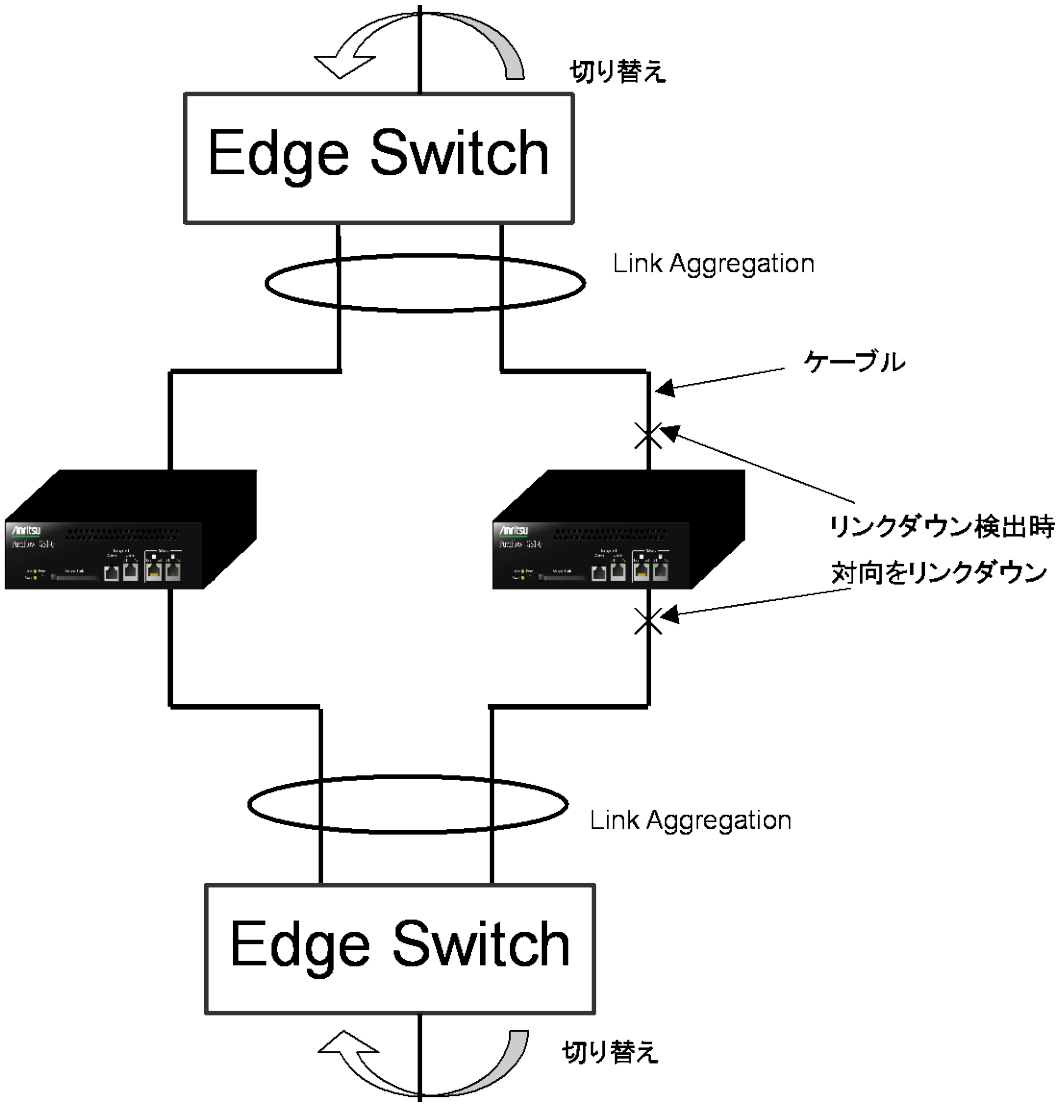
Network ポート経由で装置管理を行っている場合，バイパス接続状態では本装置のリモート管理ができなくなります。バイパス接続状態においてもリモート管理を行いたい場合，Ethernet ポート経由で管理してください。

ここでは，リンクダウン転送機能について説明します。

11.1 リンクダウン転送機能

本装置のリンクダウン転送機能を使用すると，「IEEE802.3ad Link Aggregation」などの回線冗長機能を使用している装置の間に本装置を挿入しても外部装置間の回線冗長機能を妨げることなく協調動作を行います。

本装置では，リンクダウンを検出すると対向のリンクをダウンさせることにより対向装置に対して，警報の転送を行います。対向の装置は，そのリンクダウンを検出することにより回線を切り替えることが可能となります。



リンクダウン転送機能の設定を以下に示します。

set lpt {enable | disable}	ポート（1/1）のリンクがダウンした場合に対向のポート（1/2）をリンクダウンさせて警報転送を行う機能と，ポート（1/2）のリンクがダウンした場合に対向のポート（1/1）をリンクダウンさせて警報転送を行う機能の有効／無効を設定します。
show lpt	リンクダウン転送機能の有効／無効状態を表示します。

コマンドの実行例を示します。

PureFlow(A)> set lpt enable
PureFlow(A)>

（注意）リンクダウン転送機能を有効にしている状態で，ケーブルを本装置に接続すると，数秒間，LinkLED が点灯していないのに ActiveLED が点滅する場合があります。この状態は動作上問題はありません。また，この状態では，show counter にはカウントされませんので注意してください。

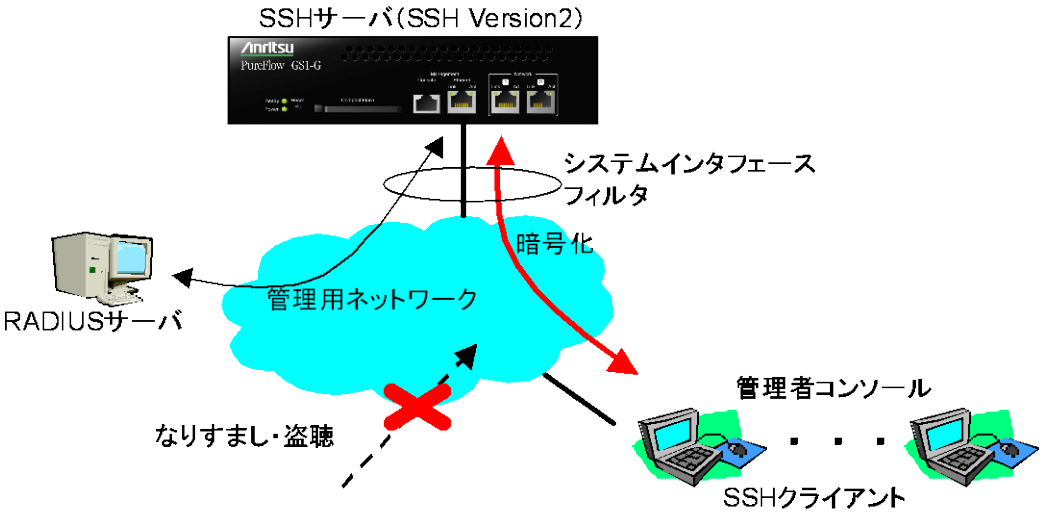
第 6 章“Network の設定”の（注 4）の説明にある set port forcelink コマンドにより，強制リンクアップを行っている状態では，リンクダウン転送機能はご使用できませんのでご注意ください。

ここでは，SSH（Secure SHell）機能について説明します。

12.1 概要

本装置は，SSH バージョン 2 に準拠した SSH サーバ機能を提供します。SSH サーバ機能により，本装置と SSH クライアント間の通信が暗号化され，安全性が保証されていないネットワークを経由する場合でも，セキュアな遠隔操作が可能になります。また，強力なサーバ認証機能を有し，第 3 者による「盗聴」や「なりすまし」を防止することができます。

SSH サーバによる接続を利用する場合も，不特定多数の端末から本装置への通信を制限するためのシステムインタフェースフィルタを設定することができます。詳細は，「第 7 章 システムインタフェースの設定」を参照してください。また，Telnet と同様に，ローカルに設定された root ユーザのパスワード認証だけでなく，RADIUS サーバ経由でのパスワード認証が利用できます。RADIUS 機能の詳細は，「第 17 章 RADIUS 機能」を参照してください。



12.2 仕様一覧

本装置の SSH サーバ機能の仕様一覧を記載します。

項目	内容
SSH バージョン	SSH Ver.2（SSHv2）準拠
ユーザ認証方式	パスワード認証
鍵交換アルゴリズム	Diffie-Hellman group exchange
公開鍵アルゴリズム	RSA, DSA
暗号化アルゴリズム	AES128-CBC, 3DES-CBC
MAC アルゴリズム	HMAC-MD5, HMAC-SHA1
接続ポート番号	22
クライアント最大接続数	4（telnet 接続数と合わせて）

12.3 SSH の利用方法

12.3.1 本体の設定

本装置の SSH サーバ機能を使用するには，以下の設定が必要です。

（1）システムインタフェースの設定

本装置の IP アドレスや Gateway を設定します。接続する端末を制限する場合は，システムインタフェースフィルタを設定します。詳細は，「第 7 章 システムインタフェースの設定」を参照してください。

（2）ホスト鍵の生成

SSH サーバは，SSH クライアントとの接続を確立するために，ホスト鍵（RSA 認証鍵または DSA 認証鍵）を必要とします。このホスト鍵は，工場出荷時に無作為に生成された鍵が設定されており，装置外部からは参照できない状態で装置内部に保存しています。特に，新しく生成する必要はありませんが，必要に応じてシリアルコンソールから変更することができます。

12.3.2 SSHクライアントの準備

SSH バージョン 2 に準拠した SSH クライアントを用意してください。本装置の SSH サーバは，SSH バージョン 1 はサポートしていません。

12.3.3 注意事項

（1）初めて SSH 接続を行うときの注意事項

SSH クライアントからリモートホストに初めて接続するとき，そのホストを信用していいかどうかを確認するサーバ認証を行います。このとき，SSH クライアントは，リモートホストが通知してきた認証鍵の fingerprint を表示し，このホストに接続していいかの確認を求めます。この場合は，SSH クライアントが表示したリモートホストの fingerprint と本装置の fingerprint が一致しているかどうかを確認することを推奨します。

本装置の RSA 認証鍵および DSA 認証鍵の fingerprint は，「show ssh コマンド」で表示可能です。

（2）ホスト鍵の再生成

本装置の SSH サーバが使用するホスト鍵（RSA 認証鍵または DSA 認証鍵）は，工場出荷時に生成され本装置内部に保存されています。このホスト鍵は，set ssh server key コマンドで変更することが可能ですが，このコマンドは，シリアルコンソールからログインしたときだけ実行可能です。

（3）ホスト鍵を再生成したあとの SSH 接続

SSH クライアントは，過去に接続したリモートホストの fingerprint を記憶しており，過去に通知してきた fingerprint が異なる場合，SSH クライアントは，ワーニングを表示し，リモートホストへの SSH 接続を切断します。これは，リモートホストの「なりすまし」を防止するための動作であり，多くの SSH クライアントが同様な動作をします。

本装置のホスト鍵を再生成した場合は，本装置に SSH で接続したことがある SSH クライアントから，本装置の fingerprint を削除または更新する必要があります。詳細は，SSH クライアントのマニュアルを参照してください。

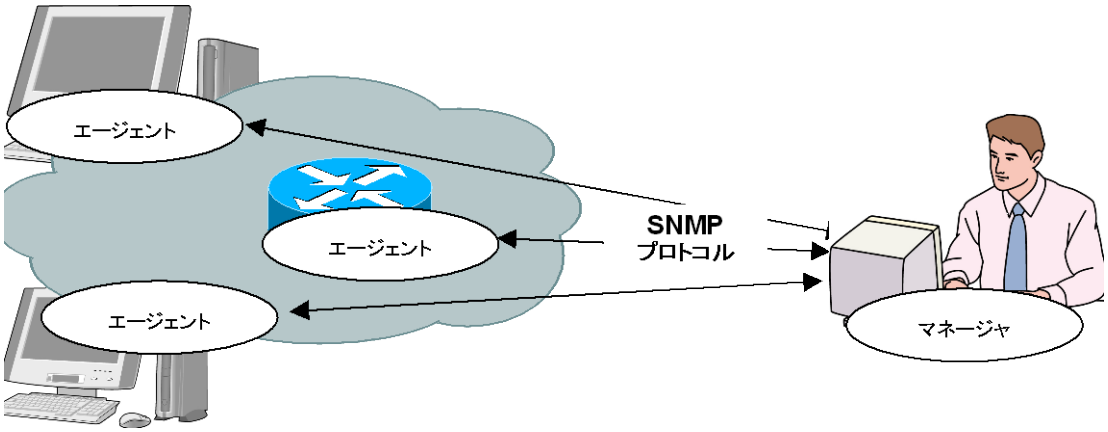
（4）RADIUS 機能を有効にした場合の SSH 接続

本装置の RADIUS 機能を有効にした場合，本装置は，ログイン認証時に RADIUS サーバに問い合わせます。SSH クライアントから本装置に新しい SSH セッションの接続を試みた場合，SSH クライアントと本装置の通信は SSH 機能により暗号化されますが，RADIUS サーバと本装置の通信は，暗号化されません。RADIUS サーバとの通信を傍受された場合，パスワードは RADIUS プロトコルにより秘匿されますが，ログイン名が第三者によって解読される可能性があります。

ここでは，SNMP の機能と設定について説明します。

13.1 SNMP の概要

SNMP は，ルータやサーバなどのネットワーク機器に対してネットワークを通してリモートで管理するためのプロトコルです。SNMP では，ルータやサーバなどの管理される側をエージェントノード（またはエージェント），管理用のアプリケーションソフトウェアをインストールしたPCやEWSをマネジメントノード（またはマネージャ）と呼んでいます。ネットワーク管理者はマネジメントノードのコンソールを使って，ネットワーク機器（エージェントノード）の障害を発見したり，設定を変更することで，日々のネットワーク管理業務を遂行します。



SNMP には SNMPv1，SNMPv2c，SNMPv3 の 3 つのバージョンが存在します。
本装置は SNMPv1，SNMPv2c，SNMPv3 の 3 つのバージョンをすべてサポートしています。それぞれのバージョンによる違いは以下のとおりです。

・ SNMPv1：最もシンプルで簡単なプロトコルで，管理情報の取得，設定，トラップ（警報）の 3 つのオペレーションから成り立っています。セキュリティはコミュニティ名と呼ばれる文字列（パスワードのようなもの）で実現されています。コミュニティ名は SNMPv1 データ要求とともにパケットに含まれてしまうため，ネットワークを測定器などでモニタされると盗み見されてしまいます。コミュニティ名は暗号化されないため，安全とみなすことはできません。外部の人間がネットワークに接続しないイントラネットなどでしか用いることができません。

・ SNMPv2c：管理情報の取得に，バルク転送と呼ばれるデータの一括取得処理をサポートすることで，プロトコルのオーバヘッドを軽減しました。アクセス・セキュリティは SNMPv1 と同様にコミュニティ文字列で行うため，セキュリティ強度は SNMPv1 と同等です。

・ SNMPv3：最新のプロトコルで，ユーザ名とそれに対応した暗号化パスワードでアクセスを認証します。エージェントへのアクセスはユーザ名が必要です。ユーザ名はグループという単位でまとめられ，グループごとに管理情報の取得，設定の権限の範囲を変えておくことで，コーポレートごとの管理者グループ，部門管理者グループ，一般ユーザグループという具合いに，権限を階層構造にもたせることができます。大規模イントラネットからインターネットまで，一般的な用途で利用可能です。SNMPv3 のセキュリティは暗号化機能も持ちますが，本装置では暗号化機能をサポートしていません。

一般的なマネジメントソフトウェアは，エージェントがサポートできるバージョンを自動検知し，最も高いバージョンを優先使用します。

13.2 SNMPv1/SNMPv2c の設定

SNMPv1 および SNMPv2c はどちらもコミュニティ名と呼ばれる文字列（パスワードのようなもの）を設定することでマネジメントノードからのアクセスが可能となります。

add snmp community <community_string> [version {v1 | v2c}] [view <view_name>] [permission {ro | rw}]	SNMPv1/v2c のコミュニティを追加します。
delete snmp community <community_string>	コミュニティを削除します。
add snmp view <view_name> <oid> {included | excluded}	SNMP の View（管理範囲の制限）を設定します。 注）snmpv2 グループは，本コマンドで指定可能ですが SNMP によるアクセスはできません。
delete snmp view <view_name> [<oid>]	SNMP の View（管理範囲の制限）を削除します。
show snmp community [<community_string>]	設定されているコミュニティを表示します。
show snmp view [<view_name>]	設定されている View を表示します。

最初に SNMPv1 コミュニティに“netman1”，SNMPv2c コミュニティに“netman2”というコミュニティ名を設定します。

```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp community netman1 version v1 permission rw
PureFlow(A)> add snmp community netman2 version v2c permission rw
```

View はそのコミュニティ名でアクセスするマネジメントノードが本装置のどの MIB Tree に対してアクセス可能かを許可／制限する機構です。add snmp community で view を省略時は“All”の View 名に対してアクセスが可能となります。また，v2c のトラップ送信を使用する場合，<oid>パラメータに，“private”を指定する際は “system”と“snmpmodules”の“included”設定も追加してください。

SNMPv1 コミュニティ netman1 を interfaces グループだけにアクセス制限をかけるには，以下のコマンドを実行します。

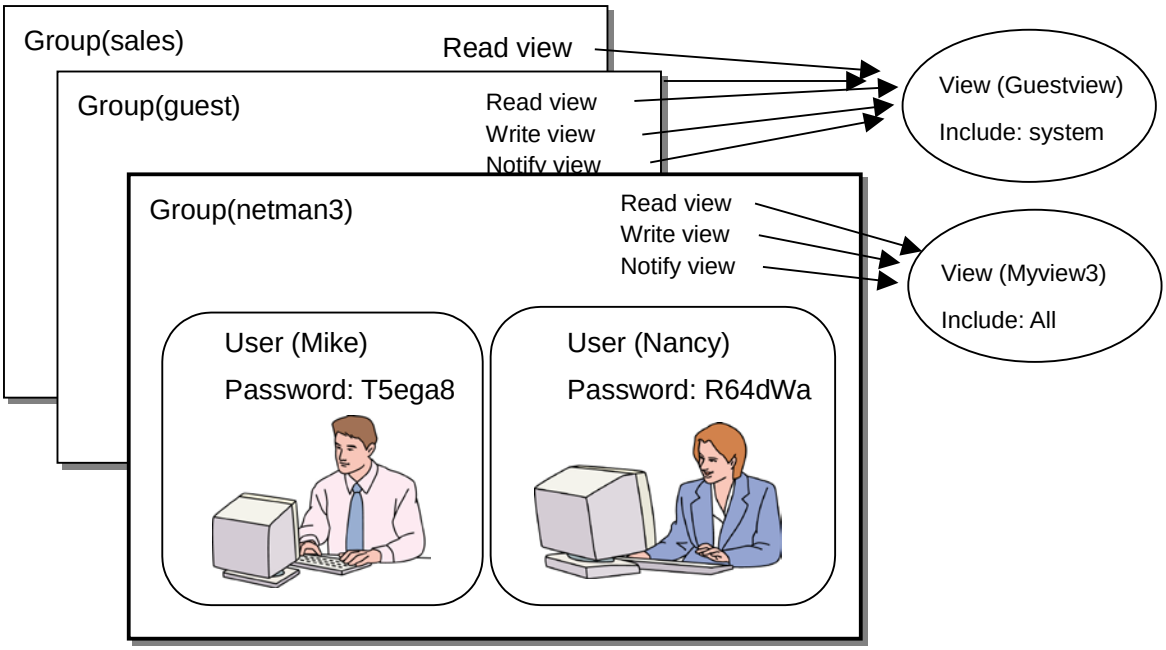
```
PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp view myview1 interface included
PureFlow(A)> add snmp community netman1 version v1 view myview1 permission rw
```

設定コマンドで設定した community 名や view の内容を確認するには，show snmp community コマンドと show snmp view コマンドを使用します。

```
PureFlow> show snmp community
-----------------------------------------------------------------
Community Name                  :netman1
Version                         :v1
Read View                       :myview1
Write View                      :myview1
-----------------------------------------------------------------
Community Name                  :netman2
Version                         :v2c
Read View                       :All
Write View                      :All
-----------------------------------------------------------------
PureFlow>
PureFlow> show snmp view
-------------------------------------------------------------------------------
View name                       :All
Subtree                         :iso
Access State                    :included
-------------------------------------------------------------------------------
View name                       :myview1
Subtree                         :interface
Access State                    :Included
PureFlow>
```

13.3 SNMPv3 の設定

SNMPv3 の管理フレームワークは，ユーザごとにセキュリティを設定するユーザベースセキュリティです。各ユーザはグループに属し，グループの属性として View を設定します。



SNMPv3 を使用するためには，グループ，ユーザ，View の設定が必要です。以下のコマンドを使用します。

add snmp group <group_name> [auth_type {auth | noauth}] [read <readview>] [write <writeview>] [notify <notifyview>]	SNMPv3 のグループを追加します。
delete snmp group <group_name>	グループを削除します。
add snmp user <user_name> <group_name> [auth_type {auth | noauth}] [password <auth_password>]	SNMPv3 のユーザを追加します。パスワードを指定する場合，8 文字以上 24 文字以下で指定してください。
delete snmp user <user_name>	ユーザを削除します。
add snmp view <view_name> <oid> {included | excluded}	SNMP の View（管理範囲の制限）を設定します。 注）snmpv2 グループは，本コマンドで指定可能ですが SNMP によるアクセスはできません。
delete snmp view <view_name> [<oid>]	SNMP の View（管理範囲の制限）を削除します。
show snmp group [<group_name>]	設定されているグループを表示します。
show snmp user [<user_name>]	設定されているユーザを表示します。
show snmp view [<view_name>]	設定されている View を表示します。

View はそのグループ，ユーザ名でアクセスするマネジメントノードが本装置のどの MIB Tree に対してアクセス可能かを許可／制限する機構です。add snmp group で view を省略時は“All”の View 名に対してアクセスが可能となります。また，v3 のトラップ送信を使用する場合，<oid>パラメータに，“private”を指定する際は “system”と“snmpmodules”の“included”設定も追加してください。

以下のコマンド例は SNMPv3 ユーザ Mike と Nancy をグループ netman3 の一員として設定します。

```
PureFlow(A)> add snmp view myview3 iso included
PureFlow(A)> add snmp group netman3 auth_type auth read  myview3 write  myview3
notify myview3
PureFlow(A)> add snmp user Mike netman3 auth_type auth password T5ega8GH
PureFlow(A)> add snmp user Nancy netman3 auth_type auth password R64dWa99
```

13.4 TRAP の設定

SNMP ではエージェントノードの状態変化を検出して，マネジメントノードへ通知する機能があります。通知用の View とマネジメントノード（ホスト）のアドレスを設定することでマネジメントノードへの TRAP（ノーティフィケーション）の送信が可能となります。

add snmp view <view_name> <oid> {included | excluded}	SNMP の View（管理範囲の制限）を設定します。
add snmp host <host_address> version {v1 | v2c | v3 [auth_type { auth | noauth}] } {user | community} <community_string / username> } {trap | inform} [udp_port <port_number>] [<notification_type>]	SNMP TRAP（ノーティフィケーション）の送信先を示すホストを追加します。
delete snmp host <host_address>	TRAP の送信先を示すホストを削除します。
set snmp traps {authentication | linkup | linkdown | warmstart | coldstart | modulefailurealarm | modulefailurerecovery | systemheatalarm | systemheatrecovery} {enable | disable}	SNMP の TRAP 送信を有効／無効に設定します。トラップ種別ごとに設定することができます。 <trapname>には， “authentication”， “linkup”， “linkdown”， “warmstart”， “coldstart”， “modulefailurealarm”， “modulefailurerecovery”， “systemheatalarm”， “systemheatrecovery” を指定することができます。
show snmp host [<host_address>]	TRAP の送信先を示すホストの一覧を表示します。

最初に SNMP TRAP 送信用に View を設定します。SNMP 基本 TRAP は snmpv2 オブジェクト，Enterprise TRAP は private オブジェクトに含まれています。snmpv2 オブジェクト，private オブジェクトへのアクセスを有効にすることで TRAP をマネジメントノードの送信することが可能となります。

PureFlow(A)> add snmp view All iso included
PureFlow(A)> add snmp host 192.168.1.10 version v1 community public trap udp_port 162

authenticationFailure TRAP の送信を無効にするには下記を設定します。

PureFlow(A)> set snmp traps authentication disable

設定コマンドで設定したホストの内容を確認するには，show snmp host コマンドを使用します。

```
PureFlow(A)> show snmp host
-----------------------------------------------------
Host Address                :192.168.1.10
Version                     :v1
Security                    :No Authentication
Security Name               :public
UDP port                    :162
Notification Type           :all
-----------------------------------------------------
Host Address                :192.168.1.11
Version                     :v2c
Security                    :No Authentication
Security Name               :public
UDP port                    :162
Notification Type           :all
PureFlow(A)>
```

設定コマンドで設定した TRAP の有効／無効の内容を確認するには，show snmp system コマンドを使用します。

```
PureFlow(A)> show snmp system
-------------------------------------------------------------------------------
System Location                 :Not Yet Set
System Contact                  :Not Yet Set
System Name                     :Not Yet Set
Engine ID                       :00:00:04:7f:00:00:00:a1:c0:a8:01:01

Traps
  authentication                :disable
  linkup                        :enable
  linkdown                      :enable
  warmstart                     :enable
  coldstart                     :enable
  modulefailurealarm            :enable
  modulefailurerecovery         :enable
  systemheatalarm               :enable
  systemheatrecovery            :enable
-------------------------------------------------------------------------------
PureFlow(A)>
```

ここでは，統計情報について説明します。
本装置には，ポート統計情報，キュー統計情報，シナリオ統計情報があります。

14.1 ポート統計情報

ポート統計情報には，Network ポートカウンタおよびシステムインタフェースカウンタがあります。
この情報は，Network ポートごと，およびシステムインタフェースの統計情報です。

14.1.1 ポートカウンタ

Network ポートごと，およびシステムインタフェースのカウンタです。
ポートカウンタでは，以下の内容を表示します。

- 受信バイト数
- 受信パケット数
- 受信ブロードキャストパケット数
- 受信マルチキャストパケット数
- 送信バイト数
- 送信パケット数
- 送信ブロードキャストパケット数
- 受信マルチキャストパケット数
- 受信エラーパケット数
- Collision（パケットの衝突）発生回数
- 廃棄パケット数
- 受信したパケットの平均レート（単位 kbit/s）
- 送信したパケットの平均レート（単位 kbit/s）

システムインタフェースカウンタでは，以下の内容を表示します。

- 受信バイト数
- 受信パケット数
- 受信ブロードキャストパケット数
- 受信マルチキャストパケット数
- 送信バイト数
- 送信パケット数
- 送信ブロードキャストパケット数
- 受信マルチキャストパケット数

ポートカウンタに関する CLI は以下のコマンドがあります。

show counter [brief]	すべての Network ポートおよびシステムインタフェースのカウンタを表示します。brief を指定した場合は，概要を表示します。
show counter {<slot/port> | system}	指定 Network ポートまたはシステムインタフェースのカウンタを表示します。
clear counter [<slot/port> | system]	Network ポートシステムインタフェースのカウンタをクリアします。

14.2 キュー統計情報

キュー統計情報には，キューカウンタ，キューバッファ情報，レート測定があります。
この情報は，キューごとの統計情報です。

14.2.1 キューカウンタ

キューごとのカウンタです。
キューカウンタでは，以下の内容を表示します。

- 受信バイト数，受信パケット数
- 送信バイト数，送信パケット数
- 廃棄バイト数，廃棄パケット数

キューカウンタに関する CLI は以下のコマンドがあります。

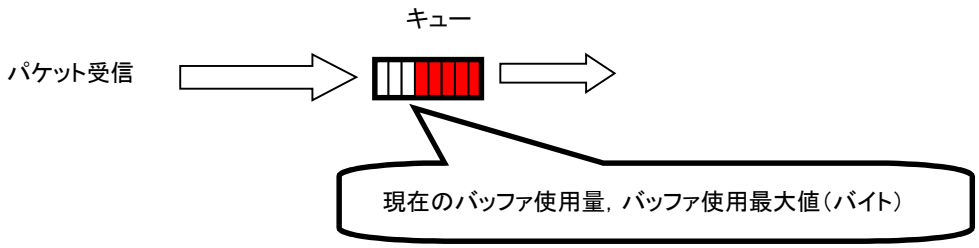
show queue counter <filter_id> [<QID>]	キューのカウンタを表示します。
show queue counter summary	キューのカウンタを一覧で表示します。
clear queue counter [<filter_id> [<QID>]]	キューのカウンタをクリアします。

<filter_id>は，“add filter”コマンドで指定した親フィルタインデックス，または子フィルタインデックスを指定します。

14.2.2 キューバッファ情報

キューごとのバッファ情報です。
キューバッファ情報では，以下の内容を表示します。

- バッファ使用量とバッファ使用率
- バッファピークホールド（バッファ使用最大値）



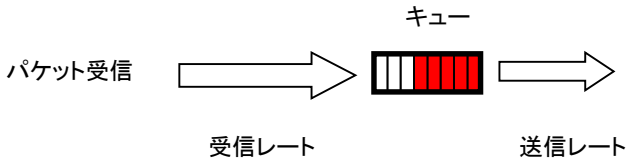
キューバッファ情報に関する CLI は以下のコマンドがあります。

show queue info <filter_id> [<QID>]	キューのバッファ情報を表示します。
show queue info summary	キューのバッファ情報を一覧で表示します。
clear queue peakhold buffer [<filter_id> [<QID>]]	キューのバッファ使用最大値をクリアします。

<filter_id>は，“add filter”コマンドで指定した親フィルタインデックス，または子フィルタインデックスを指定します。

14.2.3 レート測定

キューの受信／送信レートを測定します。受信／送信レートは，1 秒ごとに測定を行い，指定回数分表示します。
表示単位は kbit/s で，小数点以下 3 桁まで表示します。また，受信／送信レートの測定は，パケットのみを対象とし，フレーム間ギャップとプリアンブルを含みません。



レート測定に関する CLI は以下のコマンドがあります。

monitor rate <QID> [<num>]	キューの受信／送信レートを測定します。

コマンドの実行例を示します。

```
PureFlow(A)> monitor rate 10 3
QID : 10

  Times[s]          Rcv Rate[kbps]          Trs Rate[kbps]
  --------------------------------------------------------------------------
         1               3587.562               1254.531
         2               3482.826               1198.426
         3               3624.692               1217.879
  --------------------------------------------------------------------------
  Average                3565.026               1223.612
PureFlow(A)>
```

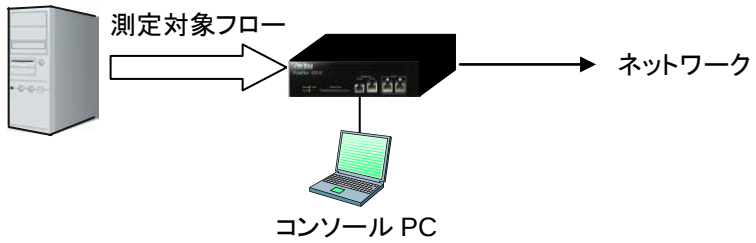
注）CLI 中の“bps”は bit/s を表します。

14.2.4 シナリオパラメータ決定方法

キュー統計情報を用いることで，キューの平均レート，バーストサイズを測定し，パラメータ決定の参考にすることができます。以下に，決定方法を説明します。

STEP1　レート測定機能を用いた平均レートの測定方法

レート測定するためには，キューを割り当てる必要があります。測定対象フローに対し，フィルタを設定します。シナリオを設定し，フィルタに結び付けます。



まず，仮想パイプのトラフィックアトリビュートの保証帯域は設定可能最大値 1000 Mbit/s（GS1-F／GS1-FB の場合 100 Mbit/s）に設定します。仮想チャネルのトラフィックアトリビュートの最大帯域は設定可能最大値 1000 Mbit/s（GS1-F／GS1-FB の場合 100 Mbit/s），許容できる入力バースト長は設定可能最大値 10 Mbyte に設定します。

設定例：

```
PureFlow(A)> add filter 10000 ipv4 in 1/1
PureFlow(A)> add filter 10000-10000 ipv4 in 1/1 sip 192.168.10.9
PureFlow(A)> add scenario vpipe 10 bandwidth 1000M
PureFlow(A)> add scenario vchannel aggregate 11 peak_bandwidth 1000M bufsize 10M
PureFlow(A)> set filter 10000 action forward scenario 10
PureFlow(A)> set filter 10000-10000 action forward scenario 11
```

まず，仮想チャネルのバッファキューの番号（QID）を確認します。

```
PureFlow(A)> show queue info 10000-10000
Scenario                : 11(-----)
VC Queue:
      Create Mode       : Aggregate
      Class             : 2
      Min Bandwidth     : -----
      Peak Bandwidth    : 1000M[bps]
      Buf Size          : 10M[Bytes]

QID     Buffer Information [Bytes(%)]
        Current         Peak
-------------------------------------------------------------
  1          0(   0%)            0(   0%)
PureFlow(A)>
```

測定対象フローの QID が 1 であることが分かります。

注）CLI 中の“bps”は bit/s を表します。

実際にフローを流し，判明した QID 1 に対してレート測定を実行します。

```
PureFlow(A)> monitor rate 1 3
QID：1

  Times[s]          Rcv Rate[kbps]          Trs Rate[kbps]
-------------------------------------------------------------------------------
         1               3587.562               3587.562
         2               3482.826               3482.826
         3               3624.692               3624.692
-------------------------------------------------------------------------------
   Average               3565.026               3565.026
PureFlow(A)>
```

注） CLI 中の“bps”は bit/s を表します。

レート測定の結果，平均レートが約 3.6 Mbit/s であることが分かります。

STEP2 バッファピークホールドを用いたバッファ使用最大値の測定方法

次にバッファサイズを決定するためにバーストサイズの測定を行います。STEP1 の測定により得られた平均レートに 10%程度のマージンを加えたレートをトラフィックアトリビュートに再設定します。

下記の例では，4 Mbit/s のレートをトラフィックアトリビュートに再設定しています。

```
PureFlow(A)> update scenario vchannel aggregate 11 peak_bandwidth 4M
```

次にフローを流している状態で，バッファ使用最大値をクリアします。

```
PureFlow(A)> clear queue peakhold buffer 10000-10000
```

この状態で，バッファ使用最大値の再記録が行われます。通常の映像トラフィックであれば 1 分程度で映像のバーストサイズがバッファ使用最大値として記録されます。

記録されたバッファ使用最大値を以下のように表示させます。

```
PureFlow(A)> show queue info 10000-10000
Scenario                    : 11(-----)
VC Queue:
    Create Mode             : Aggregate
    Class                   : 2
    Min Bandwidth           : -----
    Peak Bandwidth          : 4M[bps]
    Buf Size                : 10M[Bytes]

QID     Buffer Information [Bytes(%)]
        Current             Peak
-------------------------------------------------------
   1        105384(   0%)        149504(   1%)
PureFlow(A)>
```

バッファ使用最大値が 149504 バイトであることが分かります。測定により得られたバッファ使用最大値に安全率 2 を与え，bufsize を 300000 バイトとします。

```
PureFlow(A)> update scenario vchannel aggregate 11 bufsize 300000
```

以上で，対象フローへのトラフィックアトリビュートは下記の値となります。

PeakBandwidth： 4 Mbit/s
BufSize　：　　300000 bytes

（注）

安全率は，ネットワーク環境やトラフィックにより適性値を与えてください。

14.3 シナリオ統計情報

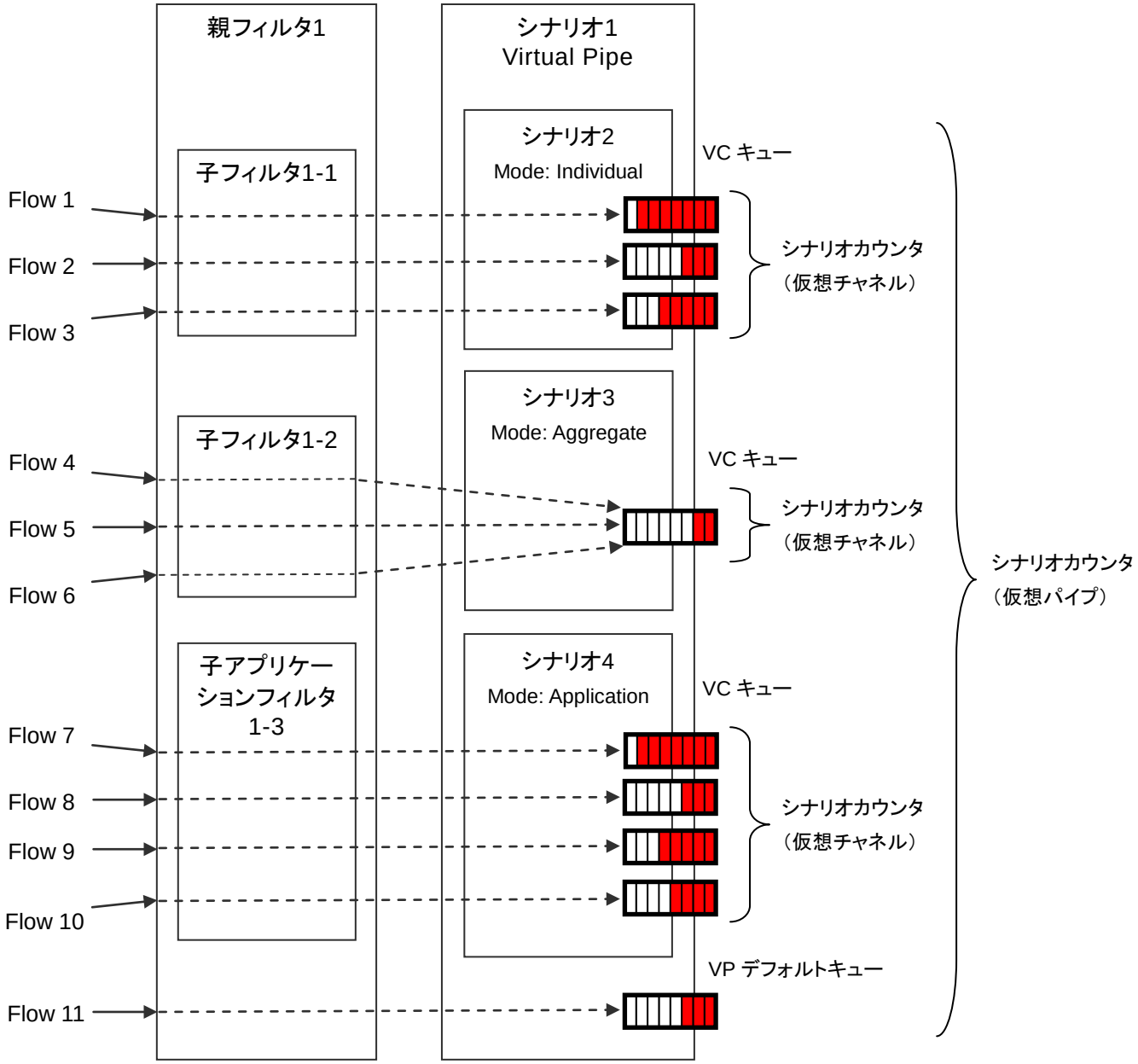
シナリオ統計情報には，シナリオカウンタ，シナリオバッファ情報があります。
この情報は，シナリオ（仮想パイプ／仮想チャネル）ごとの統計情報です。

14.3.1 シナリオカウンタ

シナリオ（仮想パイプ／仮想チャネル）ごとのカウンタです。
シナリオカウンタでは，以下の内容を表示します。

- 受信バイト数，受信パケット数
- 送信バイト数，送信パケット数
- 廃棄バイト数，廃棄パケット数

仮想パイプのシナリオカウンタは，関連する仮想チャネルのシナリオカウンタを含めた合計値となります。



シナリオカウンタに関する CLI は以下のコマンドがあります。

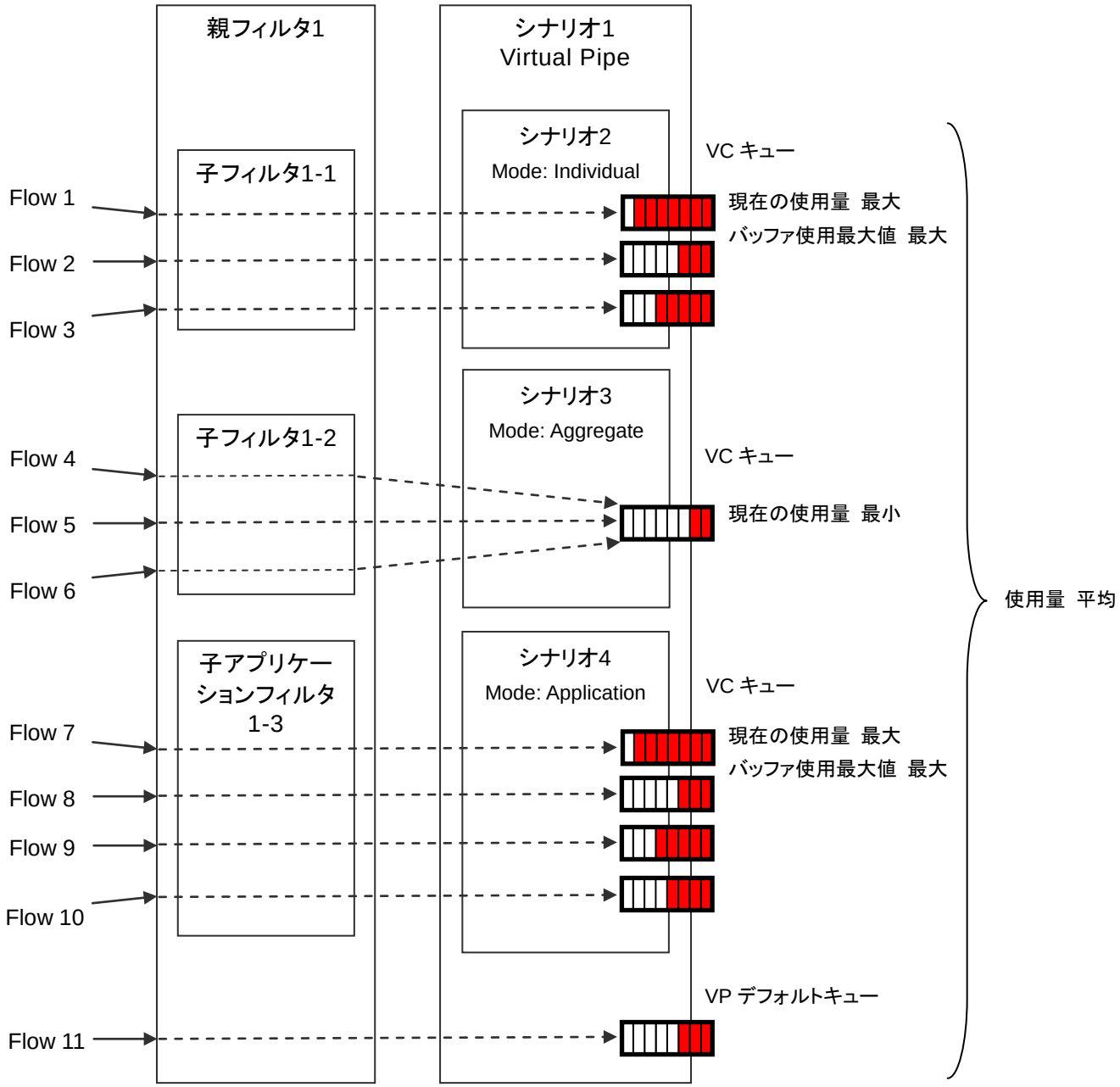
show scenario counter <scenario_id>	シナリオのカウンタを表示します。
show scenario counter summary	シナリオのカウンタを一覧で表示します。
clear scenario counter [<scenario_id>]	シナリオのカウンタをクリアします。

シナリオカウンタをクリアすると，そのシナリオで割り当てたキューのカウンタもクリアします。

14.3.2 シナリオバッファ情報

シナリオ（仮想パイプ／仮想チャネル）ごとに割り当てたキューのバッファ情報です。
シナリオバッファ情報では，以下の内容を表示します。

＜仮想パイプ＞
仮想パイプに関連するキューの中から，以下のバッファ情報を表示します。
・バッファ使用量が最大のキューのバッファ使用量とバッファ使用率
・バッファ使用量が最小のキューのバッファ使用量とバッファ使用率
・バッファ使用量とバッファ使用率の平均値
・バッファピークホールド（バッファ使用最大値）が最大のキューのバッファ使用最大値



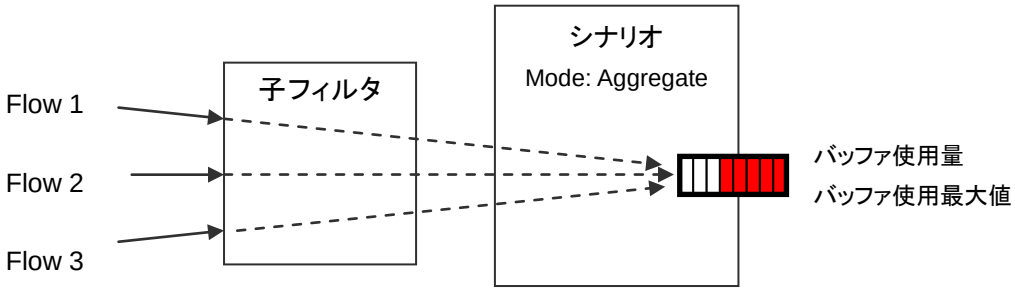
バッファ使用最大値は，今までに割り当てたキューの中で，最大のバッファ使用最大値を表示します。

＜仮想チャネル（集約キューモード）＞

仮想チャネルの集約キューモードで割り当てたキューのバッファ情報を表示します。

・バッファ使用量とバッファ使用率

・バッファピークホールド（バッファ使用最大値）



＜仮想チャネル（個別キューモード）＞

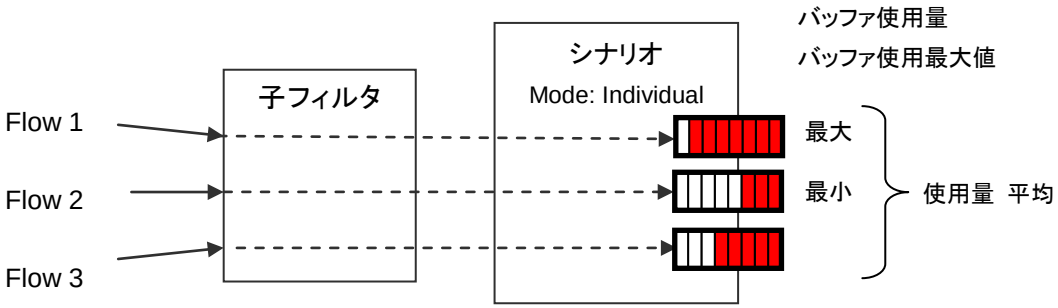
仮想チャネルの個別キューモードで割り当てたキューのバッファ情報を表示します。

・バッファ使用量が最大のキューのバッファ使用量とバッファ使用率

・バッファ使用量が最小のキューのバッファ使用量とバッファ使用率

・バッファ使用量とバッファ使用率の平均

・バッファピークホールド（バッファ使用最大値）が最大のキューのバッファ使用最大値

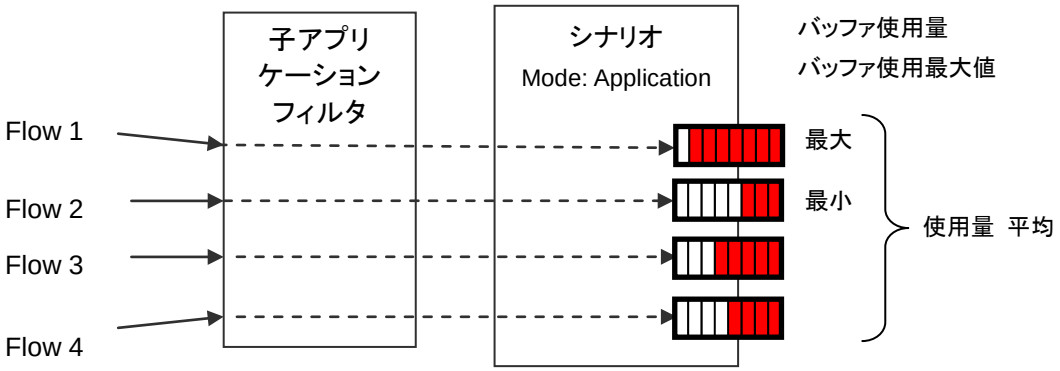


バッファ使用最大値は，今までに割り当てたキューの中で，最大のバッファ使用最大値を表示します。

＜仮想チャネル（アプリケーションキューモード）＞

仮想チャネルのアプリケーションキューモードで割り当てたキューのバッファ情報を表示します。

・バッファ使用量が最大のキューのバッファ使用量とバッファ使用率
・バッファ使用量が最小のキューのバッファ使用量とバッファ使用率
・バッファ使用量とバッファ使用率の平均
・バッファピークホールド（バッファ使用最大値）が最大のキューのバッファ使用最大値



バッファ使用最大値は，今までに割り当てたキューの中で，最大のバッファ使用最大値を表示します。

シナリオバッファ情報に関する CLI は以下のコマンドがあります。

show scenario info <scenario_id>	シナリオのバッファ情報を表示します。
show scenario info summary	シナリオのバッファ情報を一覧で表示します。
clear scenario peakhold buffer [<scenario_id>]	シナリオのバッファ使用最大値をクリアします。

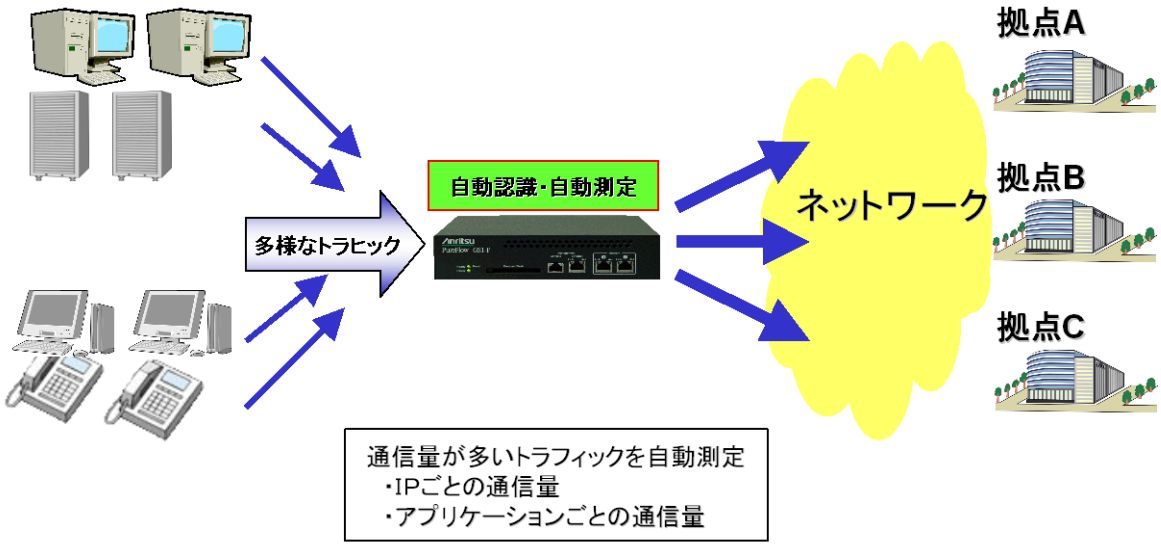
シナリオのバッファ使用最大値をクリアすると，そのシナリオで割り当てたキューのバッファ使用最大値もクリアします。

ここでは，トップカウンタ機能について説明します。

15.1 概要

トップカウンタ機能は，トラフィックの利用状況を把握するための機能です。この機能は，IP アドレスごとまたはアプリケーションポート番号ごとにトラフィック量を自動認識，流量測定し，トラフィック量が多い順に上位 100 位までのトラフィック量を表示します。

また，PureFlow モニタリングマネージャを使用することにより，利用状況をリアルタイムにグラフ表示し，過去のデータを含めたレポートを作成することができます。詳細は PureFlow モニタリングマネージャの取扱説明書を参照してください。



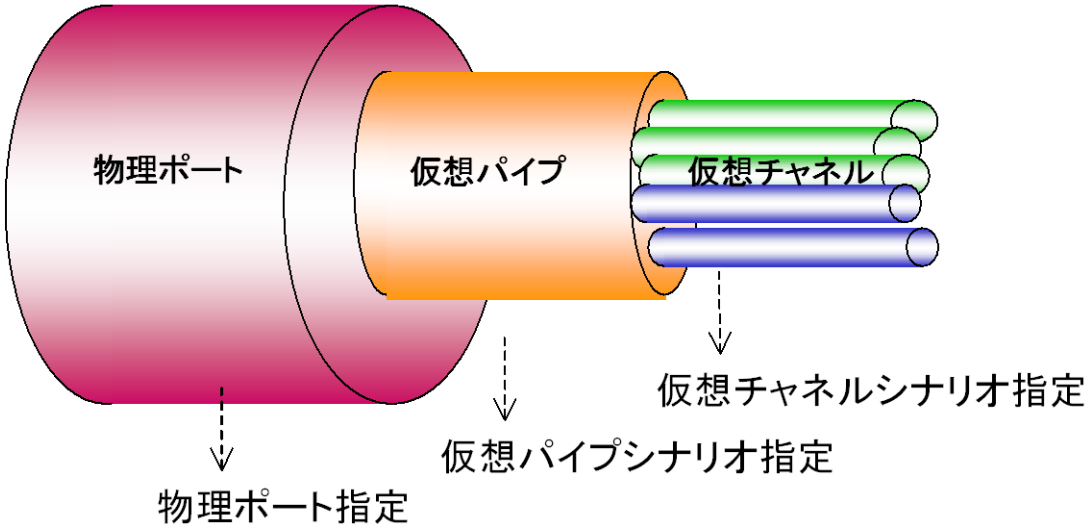
15.2 トップカウンタの表示単位について

トップカウンタ機能は，以下の 4 種の表示単位でトラフィックを計測し，それぞれの表示単位ごとに，上位 100 位までのトラフィック量を表示します。

- 送信元 IP アドレス（SIP）
- 宛先 IP アドレス（DIP）
- 送信元 IP アドレスと宛先 IP アドレスの組（SIP_DIP）
- アプリケーションポート番号（APPLI）

15.3 トップカウンタの測定範囲について

トップカウンタ機能は，本装置を通過する全トラフィックの中から，トップカウンタを測定する範囲を指定することができます。測定範囲として，任意の「物理ポート」，「仮想パイプ」，「仮想チャネル」を指定でき，最大で 32 個まで登録できます。

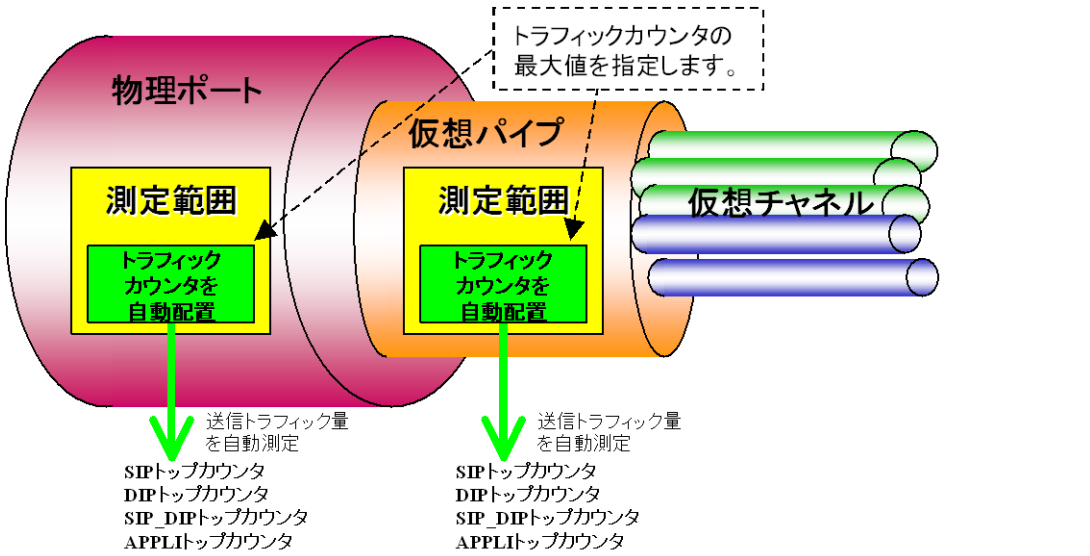


たとえば，ある仮想パイプを通過するトラフィックにおいて，通信帯域をより多く消費しているトラフィックを観測する場合は，測定範囲に該当する仮想パイプシナリオを指定します。これにより，仮想パイプに入力されたトラフィックの中から，送出量が最も多いトラフィックを把握することができます。

15.4 トラフィックカウンタについて

トラフィックカウンタは，トラフィックの IP アドレスやアプリケーションポート番号ごとなど，自動認識したトラフィックごとに自動配置され，それぞれの送信トラフィック量を測定するカウンタです。

トップカウンタ機能を使用する場合，あらかじめ，利用可能なトラフィックカウンタの最大値を，それぞれの測定範囲ごとに指定する必要があります。トラフィックカウンタの総数は，GS1-F の場合 100,000 個まで，GS1-G の場合 400,000 個までです。



15.5 アプリケーションポート番号の測定について

トップカウンタ機能は，特定のアプリケーションポート番号だけにトラフィックカウンタを割り当て，トラフィック量を測定します。デフォルト状態で測定を実施するアプリケーションポート番号は，show topcounter config all コマンドで確認してください。

また，任意のアプリケーションポート番号も測定することができます。測定したいアプリケーションポート番号を，add topcounter config appli port コマンドで追加してください。

15.6 操作コマンド一覧

トップカウンタ機能の操作は，以下のコマンドで行います。

set topcounter	トップカウンタの有効／無効を設定します。
set topcounter config interval time	トップカウンタの収集周期を設定します。
add topcounter target	トップカウンタの測定範囲を追加します。
update topcounter target	トップカウンタの測定範囲に指定されているパラメータを変更します。
delete topcounter target	トップカウンタの測定範囲を削除します。
show topcounter config	トップカウンタの設定を表示します。
show topcounter target	トップカウンタを表示します。
add topcounter config appli port	トップカウンタを測定するアプリケーションポート番号を追加します。
delete topcounter config appli port	トップカウンタを測定するアプリケーションポート番号を削除します。

15.7 操作手順

トップカウンタ機能を操作する手順は以下のとおりです。

(1) トップカウンタの測定範囲を設定する。
add topcounter target コマンドを使用し，トップカウンタを測定するトラフィックを指定してください。測定範囲として，任意の物理ポート，仮想パイプシナリオ，仮想チャネルシナリオのトラフィックを指定することができます。

(2) 必要に応じて，トップカウンタの収集周期を設定する。
set topcounter config interval time コマンドを使用し，トップカウンタの収集周期を変更することができます。ただし，PureFlow モニタリングマネージャを接続している場合，収集周期が変更される場合があります。動作中の収集周期は，show topcounter config コマンドで確認することができます。

(3) 必要に応じて，トップカウンタで測定するアプリケーションポート番号を追加する。
デフォルト設定以外のアプリケーションポート番号を測定する場合は，add topcounter config appli port コマンドを使用し，任意のポート番号を追加することができます。デフォルト設定のポート番号は，show topcounter config all コマンドで確認することができます。

(4) トップカウンタの収集を有効にする。
set topcounter enable コマンドを使用し，トップカウンタ機能を有効にしてください。トップカウンタ機能が有効になってから，収集周期が経過した後，トップカウンタを表示します。

(5) トップカウンタを表示する。
show topcounter target コマンドを使用し，トップカウンタを表示します。送信元 IP アドレスごと，宛先 IP アドレスごと，送信元 IP アドレスと宛先 IP アドレスの組み合わせごと，アプリケーションポート番号ごとなど，それぞれのトップカウンタを表示することができます。

15.8 操作例

以下の表に示す設定で，トップカウンタ機能を使用する時のコマンド設定例を記載します。

ユーザ設定項目	設定値	備考
測定範囲	物理ポート 1/1	トラフィックカウンタ数を任意に設定
	仮想パイプシナリオ　1000	トラフィックカウンタ数をデフォルト設定
	仮想チャネルシナリオ 1040	トラフィックカウンタ数をデフォルト設定
収集周期	10 分	ただし，モニタリングマネージャを接続した場合，収集周期が変更される場合があります。
アプリケーションポート番号	測定するアプリケーションポート番号を追加 10000 20000～2003	デフォルト設定のアプリケーションポート番号に加えて，10000，20000，20001，20002，20003のアプリケーションポート番号を測定する。

設定コマンドは，以下のとおりです。

```
PureFlow(A)> add topcounter target port in 1/1 sip 10000 dip 10000 sip_dip 10000 appli 250
PureFlow(A)> add topcounter target scenario 1000
PureFlow(A)> add topcounter target scenario 1040
PureFlow(A)> set topcounter config interval time 10
PureFlow(A)> add topcounter config appli port 10000
PureFlow(A)> add topcounter config appli port 20000-20003
PureFlow(A)> set topcounter enable
PureFlow(A)>
```

トップカウンタは，以下のように表示されます。

```
PureFlow(A)> show topcounter target port in 1/1 group sip
From          : 2008 Jan 02 19:47:55   To            : 2008 Jan 02 19:57:55
Total Octet: 1475806000                Total Packet: 1475806

Order   IP Address                                Tx Octet          Tx Packet
-----   ----------------------------------------  ----------------  ----------------
    1   192.168.101.121                                 8214               111
    2   192.168.101.122                                 5846                79
    3   fe80:0000:0000:0000:0290:ccff:fe22:8b4c         5772                78
    4   fe80:0000:0000:0000:0290:ccff:fe22:8b4d         5698                77
    5   fe80:0000:0000:0000:0290:ccff:fe22:8b4e         3848                52
PureFlow(A)>
```

15.9 注意事項

(1) トラフィックカウンタが不足した場合，正確なトップカウンタを表示しない場合があります。
割り当てたトラフィックカウンタの数よりも，実際に通信している通信ノードが多い場合，トラフィックカウンタが不足する場合があります。トラフィックカウンタが割り当てられていない通信ノードは，個別の流量を測定することができないため，トップカウンタとして表示されません。

(2) PureFlow モニタリングマネージャを使用している場合，CLI で設定した収集周期とは異なる周期でトップカウンタを集計する場合があります。
本装置に PureFlow モニタリングマネージャが接続された場合，トップカウンタの収集周期がモニタリングマネージャによって変更される場合があります。CLI で設定された収集周期と，PureFlow モニタリングマネージャの GUI で設定された収集周期を比較し，より長いほうの周期でトップカウンタを収集します。動作中の収集周期は，show topcounter config コマンドで確認してください。

(3) 受信した TCP/IP パケットにおいて，送信元ポート番号と宛先ポート番号の両方が，トップカウンタを測定するアプリケーションポート番号として登録されている場合，そのパケットは，宛先ポート番号のトラフィックカウンタに計上されます。送信元ポート番号のトラフィックカウンタには計上されません。

(4) トップカウンタを測定するアプリケーションポート番号を必要に応じて追加できますが，デフォルトで設定されているアプリケーションポート番号は削除できません。

(5) CLI または PureFlow モニタリングマネージャからトップカウンタの収集周期を変更した場合，一度だけ，設定されている収集周期よりも短い期間で集計されたトップカウンタを表示する場合があります。これは，前回の収集周期に達した時刻から，収集周期を変更した時刻までのトップカウンタの集計結果です。

(6) トップカウンタは，トップカウンタの収集周期に到達してから約 1 分ほど経過したときに更新されます。

ここでは，WEB による監視機能について説明します。

16.1 概要

本装置は，ネットワークに接続した端末から，WEB ブラウザを利用して以下の情報を表示することができます。

(1) トラフィックモニタ

パイプ，仮想パイプおよび関連する仮想チャネル（シナリオツリー）のトラフィック情報を表示します。表示方法はグラフとカウンタの2種類あり，指定したサンプリング周期でトラフィック情報が更新されます。グラフは，仮想チャネルの積み上げグラフで表示されます。

トラフィック量の計測は，シナリオカウンタを使用しています。シナリオカウンタの詳細は「第 14 章 統計情報」を参照してください。

(2) システムログ

装置内蔵メモリに記録されたログデータの取得および保存ができます。

システムログの詳細は「第 4 章 装置本体の情報表示と設定」を参照してください。

16.2 動作環境

WEB による監視機能を使用する端末の動作環境は，以下のとおりです。

(1) OS

Microsoft 社製 Windows XP を使用してください。

(2) ブラウザ

Microsoft 社製 Internet Explorer 6.0 以降を使用してください。

(3) CPU

300 MHz 以上の CPU を搭載した端末を使用してください。
Pentium/Celeron 系列，AMD K6/Athlon/Duron ファミリ，またはこれらと互換のプロセッサを推奨。

(4) メモリ

128 Mbyte 以上のメモリを搭載した端末を使用してください。

(5) 電源オプション

スタンバイ状態，休止状態ではグラフの更新は行われません。
コントロールパネルの電源オプションで設定を“なし”に変更してください。

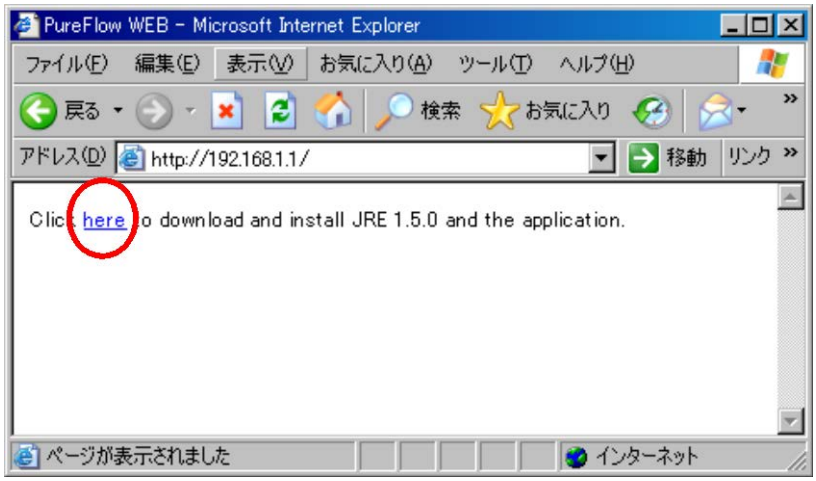
16.3 初期設定

WEB による監視機能を使用するためには，本装置のシステムインタフェースの設定を行う必要があります。システムインタフェースの設定の詳細は「第 7 章　システムインタフェースの設定」を参照してください。

システムインタフェースの設定完了後，Internet Explorer を起動して，装置の IP アドレスを指定します。装置の IP アドレスが 192.168.1.1 の場合，以下のように指定します。

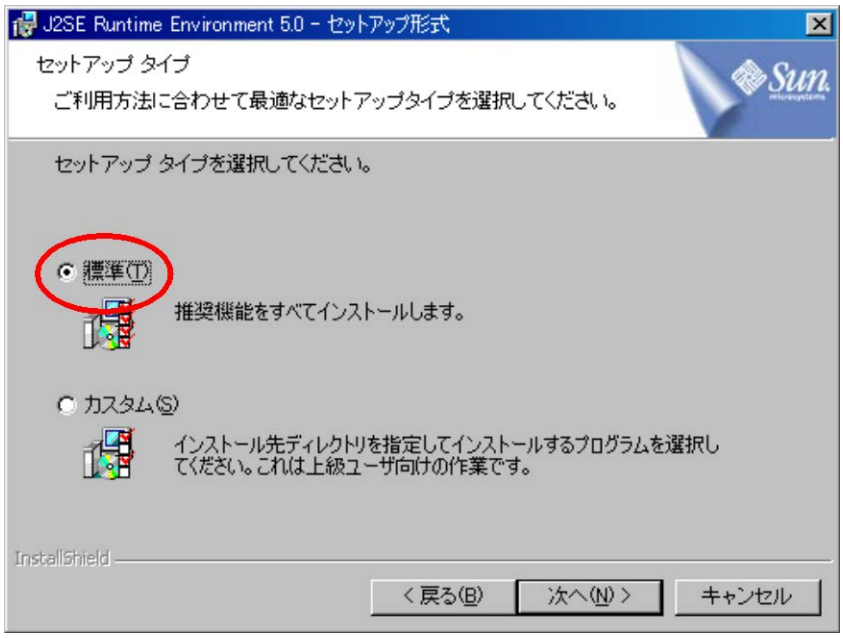
http://192.168.1.1/

本装置の WEB による監視機能は，Sun Microsystems 社製 Java 2 Platform Standard Edition Runtime Environment 5.0（以下 J2SE）を必要としており，端末にインストールされていない場合，ブラウザ上に以下のように表示がされます。



「here」を左クリックすると Oracle 社の Web サイトが表示されますので，Java SE Downloads の Previous Releases から Java SE Runtime Environment 5.0u22 をダウンロードし，インストールを開始します。

「使用許諾契約の条項に同意します」を選択し，「次へ」を左クリックしてください。



「標準」を選択し，「次へ」を左クリックしてください。左クリック後 J2SE のインストール画面が表示されますので，完了するまでお待ちください。インストール完了後，以下のように表示されますので，「完了」をクリックしてください。これで J2SE のインストールは完了です。インストール後，自動でログイン画面に進みます。

（注 1）
J2SE をインストールするためには，インターネットに接続できる環境が必要となります。また，イントラネットから接続するためには，ブラウザのプロキシ設定が必要となる場合があります。

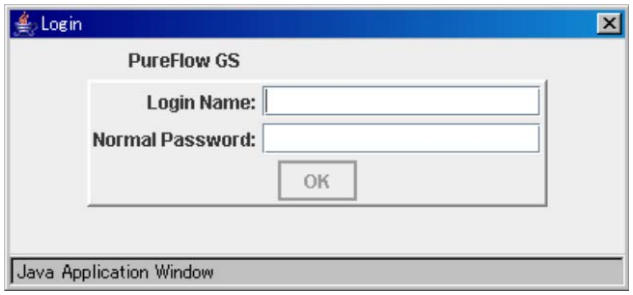
（注 2）
J2SE をインストールするために必要なディスクサイズは約 92 Mbyte です。また標準セットアップを指定した場合，インストール先ディレクトリをインストーラが自動で決定します。インストール先を変更する場合は，標準セットアップではなくカスタムセットアップを選択してください。

16.4 操作方法

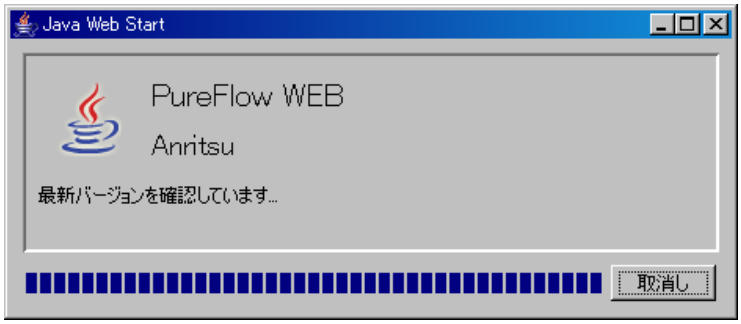
16.4.1 ログイン画面の表示

J2SE インストールの完了後，再度アクセスすると，以下のような画面が出ます。ここで，「Launch the PureFlow WEB」を左クリックしてください。ログイン画面まで進みます。

以下がログイン画面になります。本装置に設定されたログイン名およびログインパスワードを入力してください。ログイン名とログインパスワードの設定は，「第 4 章　装置本体の情報表示と設定」を参照してください。



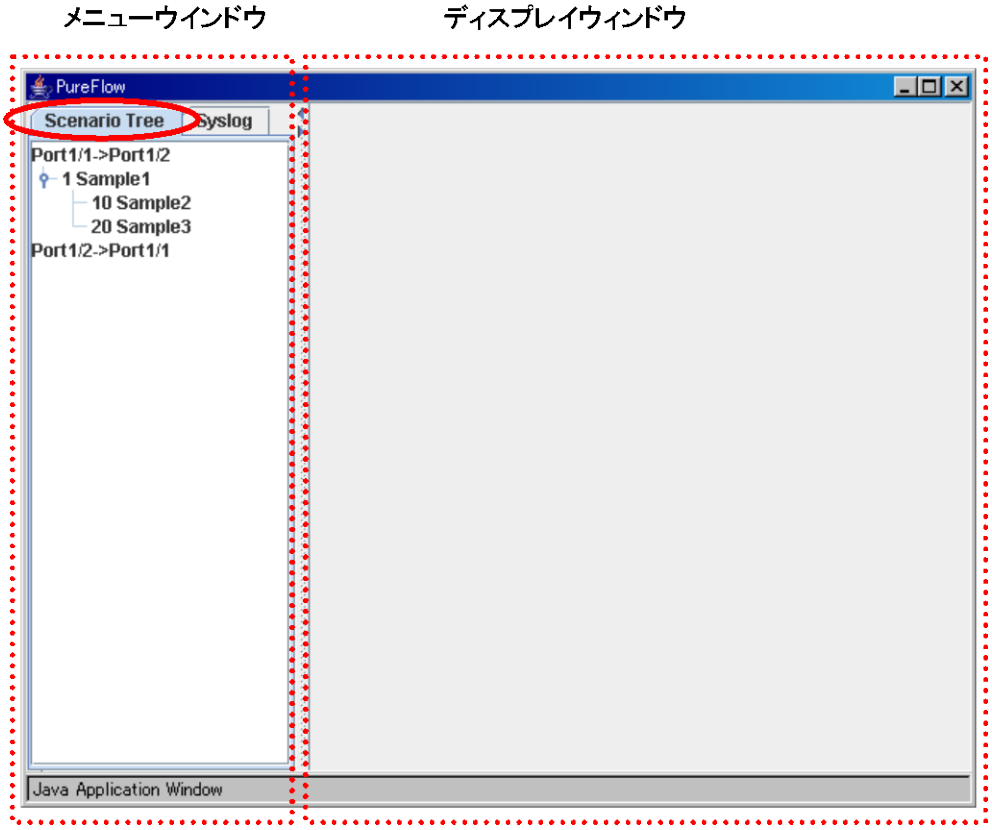
（注 1）
ログイン画面が表示される前に，以下のような表示が出ることがあります。これは，はじめて装置にアクセスしたときや，ソフトウェアをバージョンアップしたあとにアクセスするときに表示されます。「取消し」ボタンを押した場合，アプリケーションは終了します。押してしまった場合は，再度アクセスしてください。



（注 2）
1 装置につき Web による監視機能は telnet による装置への接続数とあわせて，4 接続までです。

16.4.2 トラフィックモニタ

トラフィックモニタについて説明します。ログイン後，以下の画面が表示されます。画面左側をメニューウィンドウ，右側をディスプレイウィンドウと呼びます。最初にメニューウィンドウの「Scenario Tree」タブを左クリックしてください。

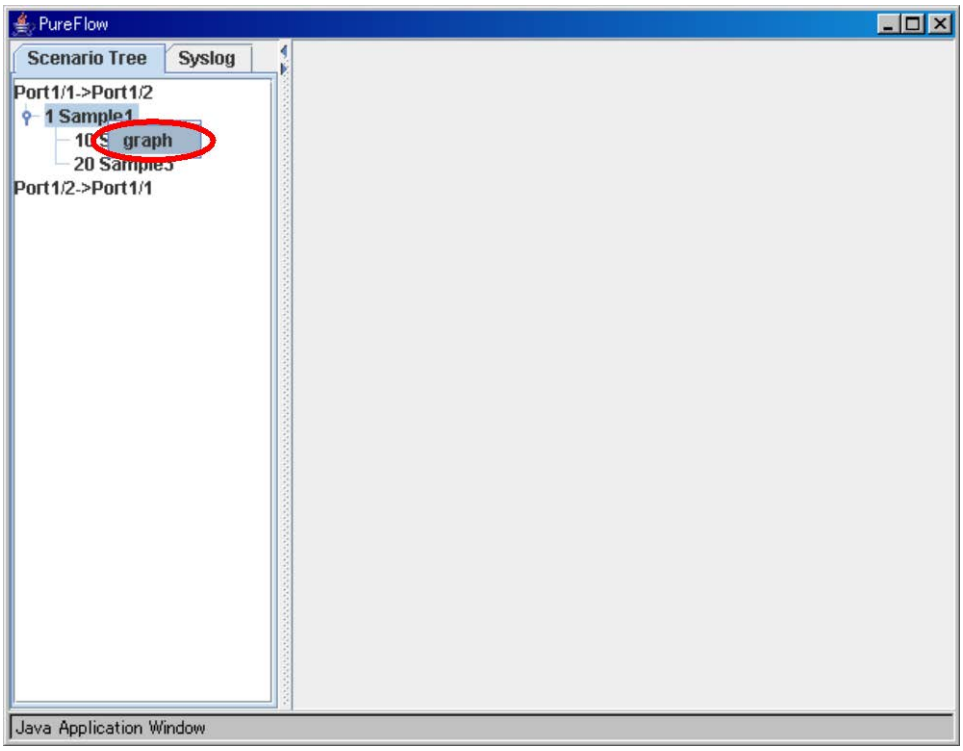


上記は，入力 Network ポートを 1/1 とする仮想パイプを 1 つ，関連する仮想チャネルを 2 つ設定した例です。仮想パイプはシナリオインデックス 1 でシナリオ名を Sample1 と設定しています。仮想チャネルはそれぞれ，シナリオインデックス 10 でシナリオ名を Sample2，シナリオインデックス 20 でシナリオ名を Sample3 としています。

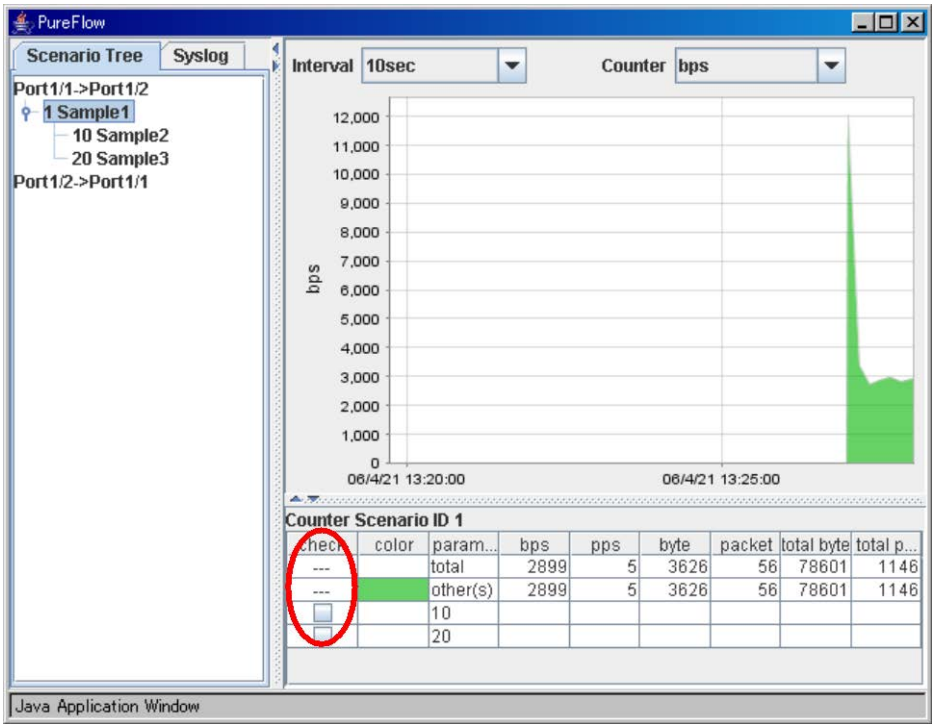
仮想パイプ，仮想チャネルの設定については，「第 8 章 トラフィックコントロール機能」を参照してください。

（1）仮想パイプのトラフィックモニタ

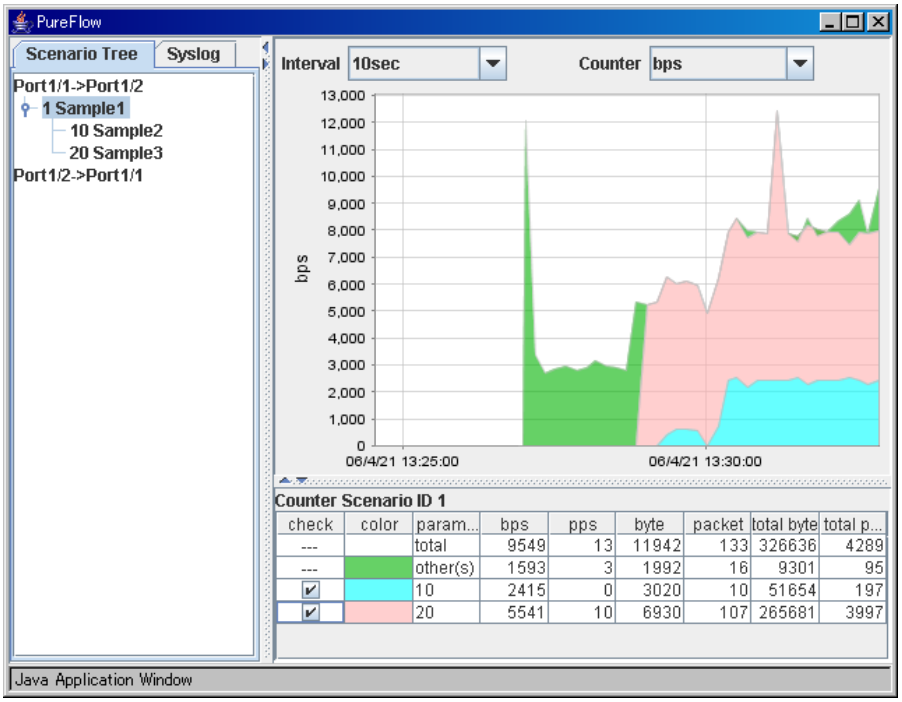
仮想パイプのシナリオへマウスを動かし，右クリックをするとサブウィンドウが表示されますので，「graph」を選択します。選択後，トラフィック量のグラフおよびカウンタが表示されます。



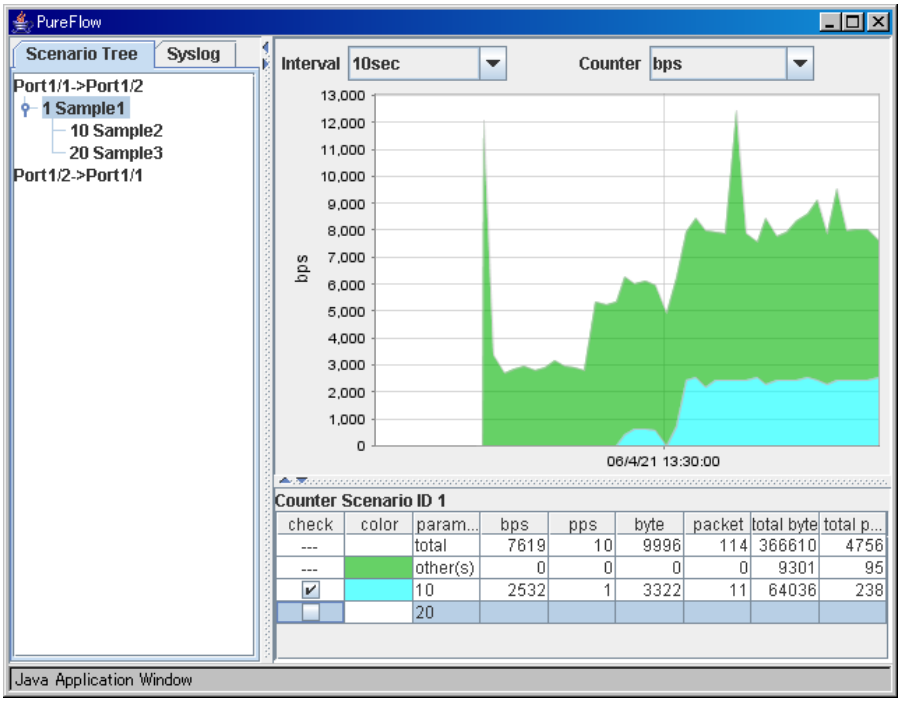
仮想パイプのトラフィック情報は以下のように表示されます。初期設定では，仮想チャネルを含めた仮想パイプ全体のトラフィック量を表示します。仮想チャネルのトラフィック量を個別にグラフ表示したい場合は，ディスプレイウィンドウにあるチェックボックスを左クリックして有効にします。



2 つの仮想チャネルを有効にした場合のグラフ表示は以下のようになります。グラフ表示を有効にした時点からの仮想チャネルのトラフィック量がグラフ上に表示されます。仮想パイプを有効にしたのこりの緑色部分は，その他のトラフィック量（仮想パイプ内の選択していない仮想チャネル内を流れているトラフィック量）となります。

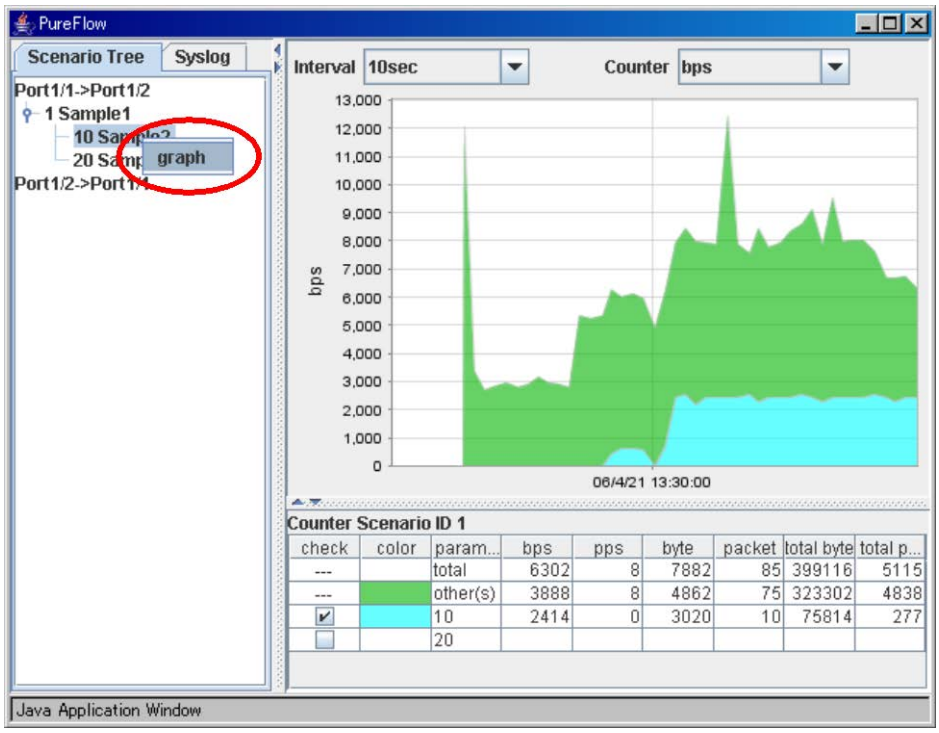


表示する必要のない仮想チャネルを無効にする場合は，チェックボックスを左クリックします。チェックをはずした仮想チャネルのグラフ表示がなくなり，そのほかのトラフィック量として表示されます。Sample3 を無効にした場合の表示は，以下のようになります。

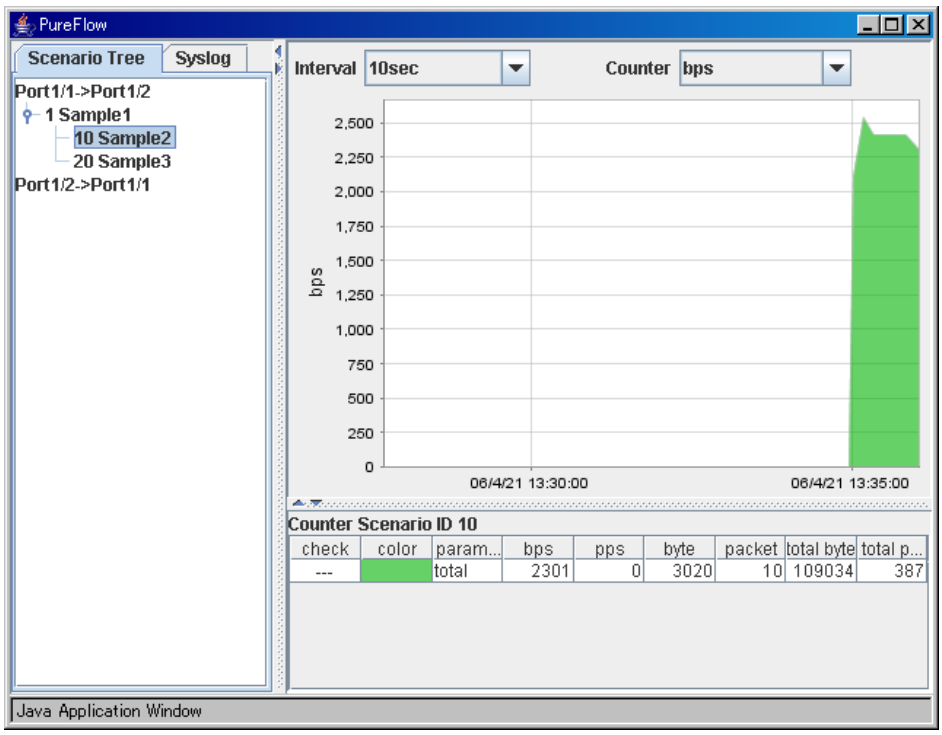


（2）仮想チャネルのトラフィックモニタ

メニューウインドウ上にある仮想チャネルのシナリオにマウスを動かし，右クリック後「graph」を選択すると，トラフィック量が表示されます。



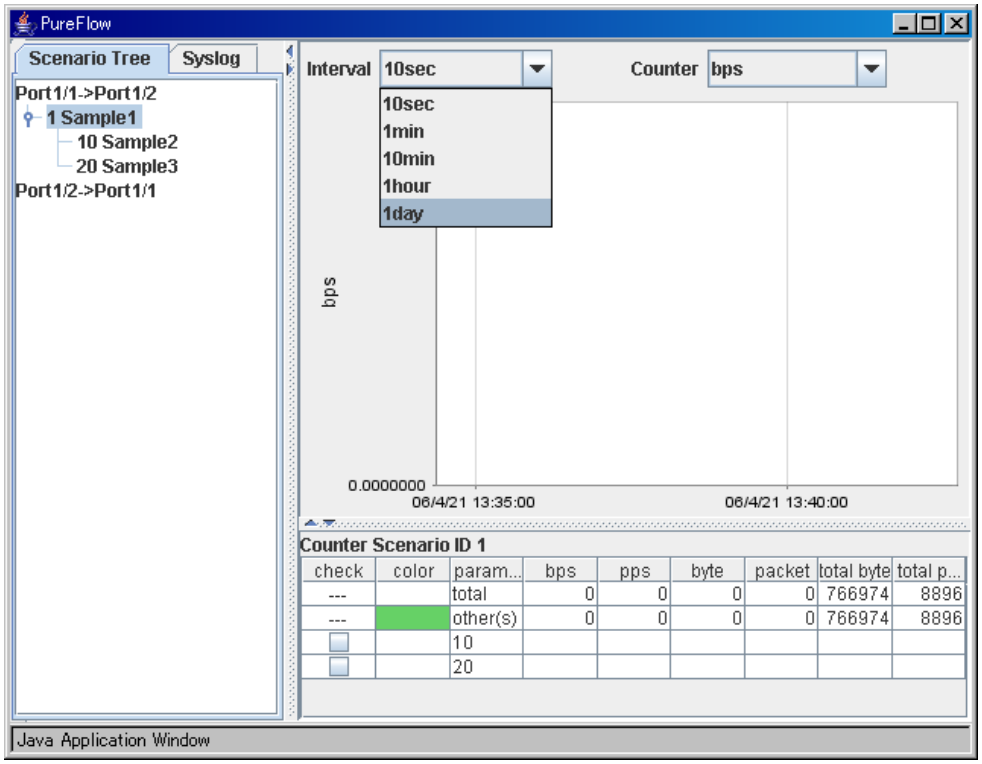
以下が仮想チャネルのトラフィック量の画面になります。



(3) グラフ表示のサンプリング周期／トラフィック種別

グラフ表示を行う際，サンプリング周期およびトラフィック種別を変更できます。

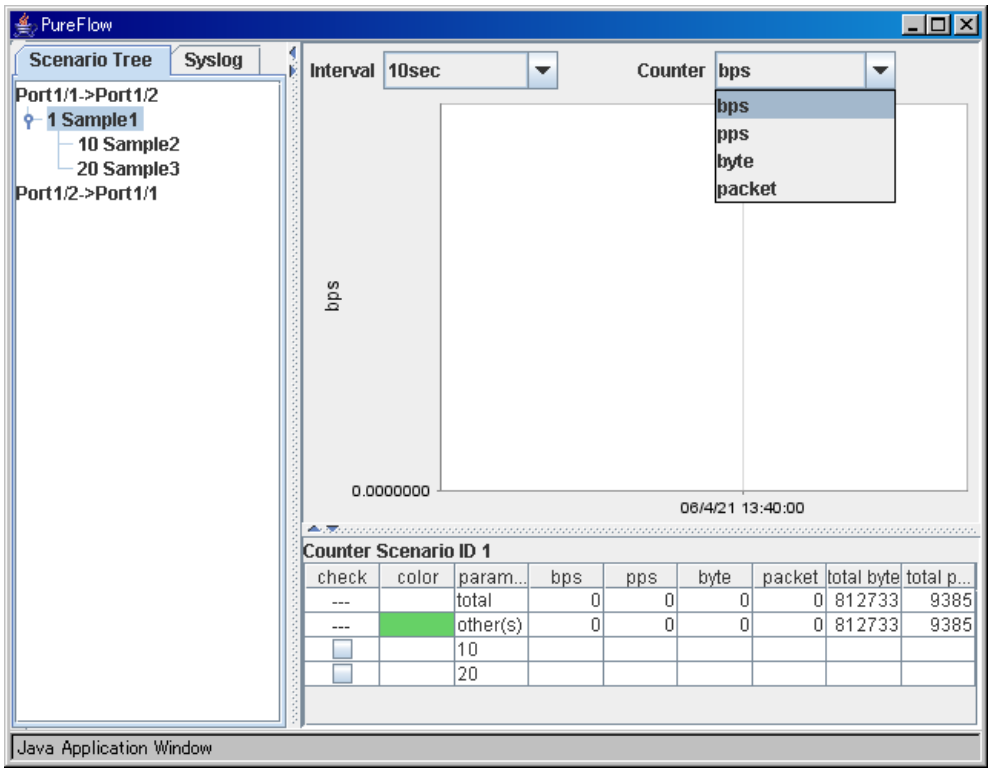
サンプリング周期は 10 秒，1 分，10 分，1 時間，1 日が指定できます。サンプリング周期のデフォルト値は 10 秒です。サンプリング周期を変更するには，ディスプレイウィンドウの「Interval」を左クリックし，サンプリング周期を選択します。グラフの横幅は，サンプリング周期の 50 倍です。



トラフィック種別は，以下の指定ができます。

- bps（bit per second）
  サンプリング周期の間に流れた合計パケット長から計算した平均トラフィックです。
- pps（packet per second）
  サンプリング周期の間に流れた合計パケット数から計算した平均トラフィックです。
- byte
  サンプリング周期の間に流れた合計パケット長です。
- packet
  サンプリング周期の間に流れた合計パケット数です。

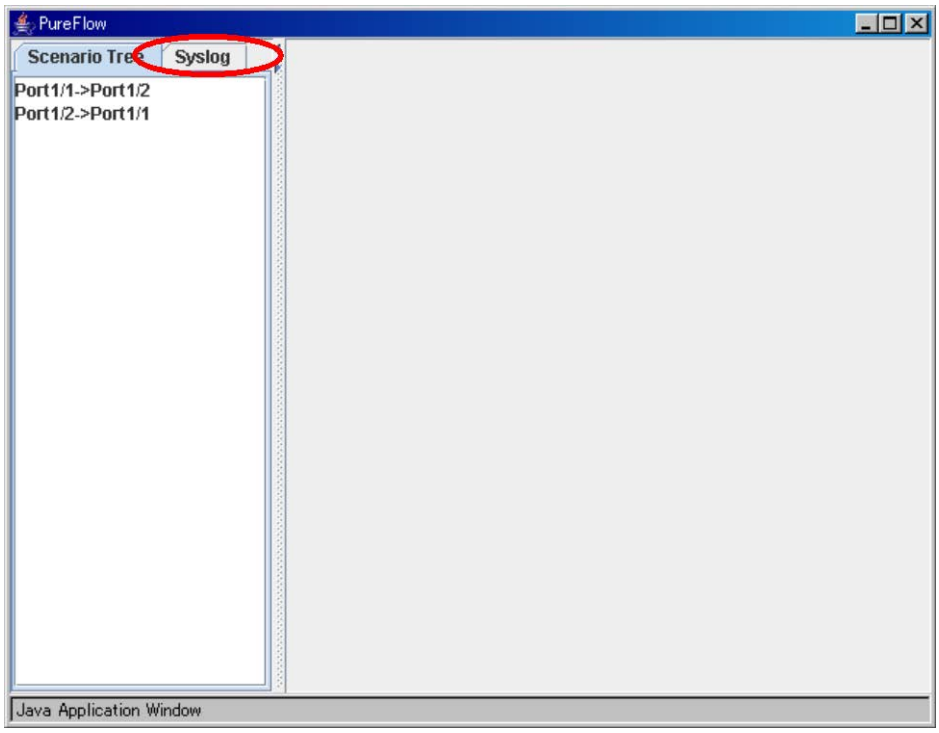
トラフィック種別のデフォルト値は bit/s です。グラフ表示するトラフィック種別を変更するには，ディスプレイウィンドウの“Counter”を左クリックし，トラフィック種別を選択します。



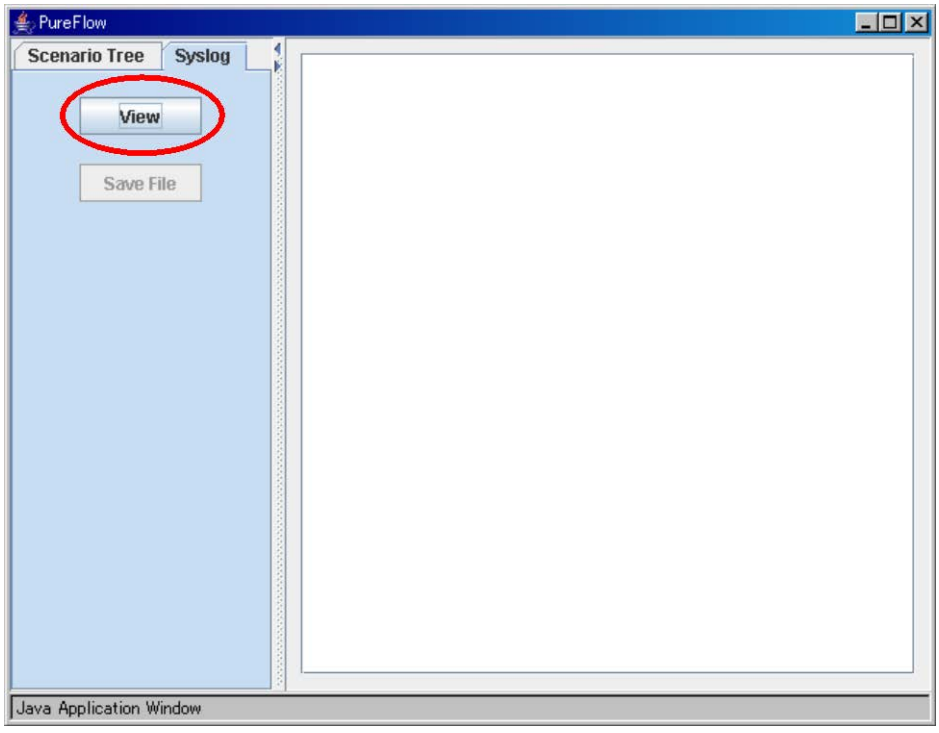
（注 1）
グラフ表示中に，フィルタやシナリオの設定を変えた場合，一度 WEB ブラウザをクローズしてから，再度起動してください。
（注 2）
サンプリング周期やトラフィック種別を変更した場合，それまで表示されていたグラフはクリアされます。
（注 3）
WEB ブラウザをクローズすると，それまで表示されていたグラフはクリアされます。

16.4.3 システムログの表示方法

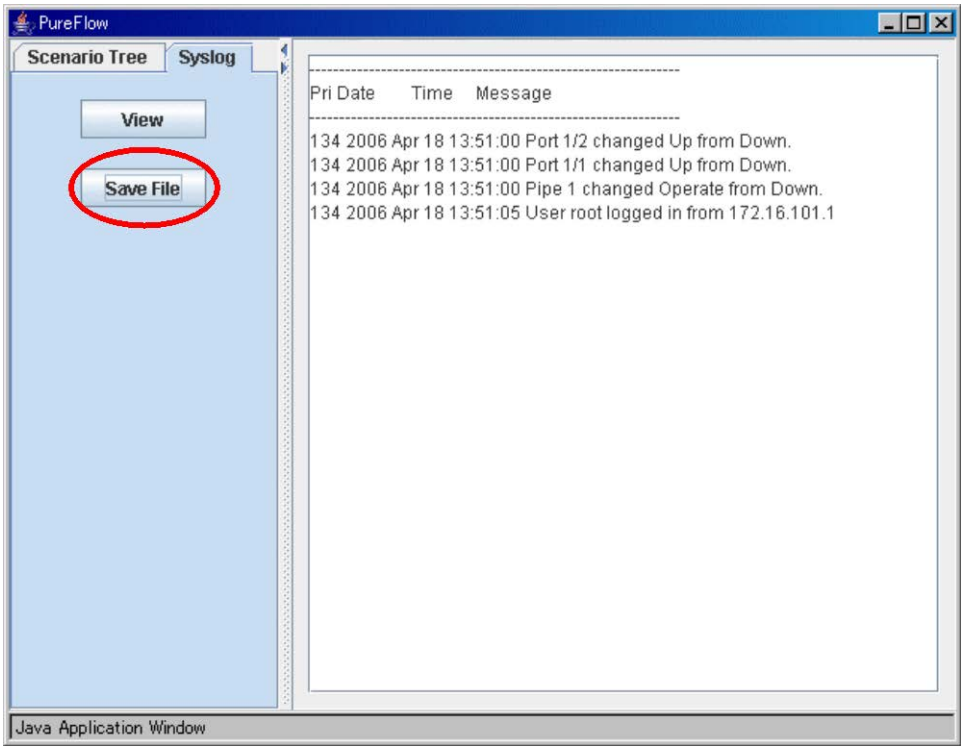
システムログの表示方法について説明します。ログイン後以下の画面が出ますので，メニューウインドウの「Syslog」タブを左クリックしてください。



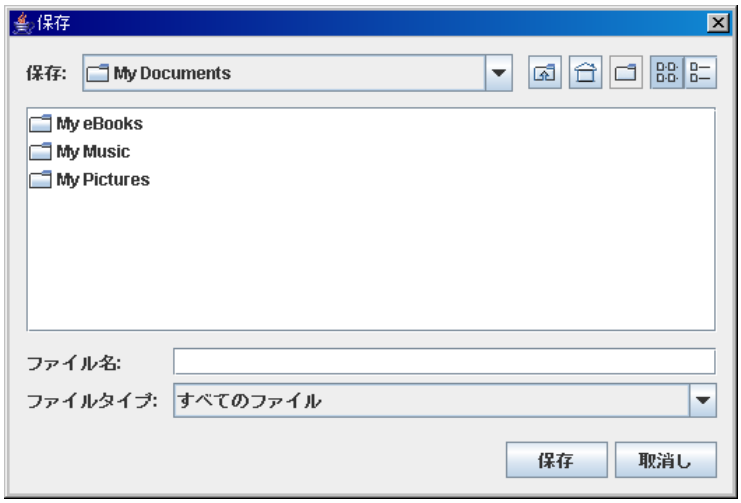
以下の画面がシステムログの画面になります。この状態で「View」ボタンを左クリックしてログデータを取得します。ログデータはディスプレイウインドウに表示されます。



以下がシステムログ出力の例です。再度「View」ボタンを左クリックすると，最新のログデータを取得することができます。現在のログデータをファイルに保存するには「Save File」ボタンを左クリックしてください。



以下の画面が表示されますので，保存したいディレクトリを選択してください。システムログ情報は，テキスト形式で保存され，テキストエディタで閲覧することが可能です。



16.4.4 使用上の注意

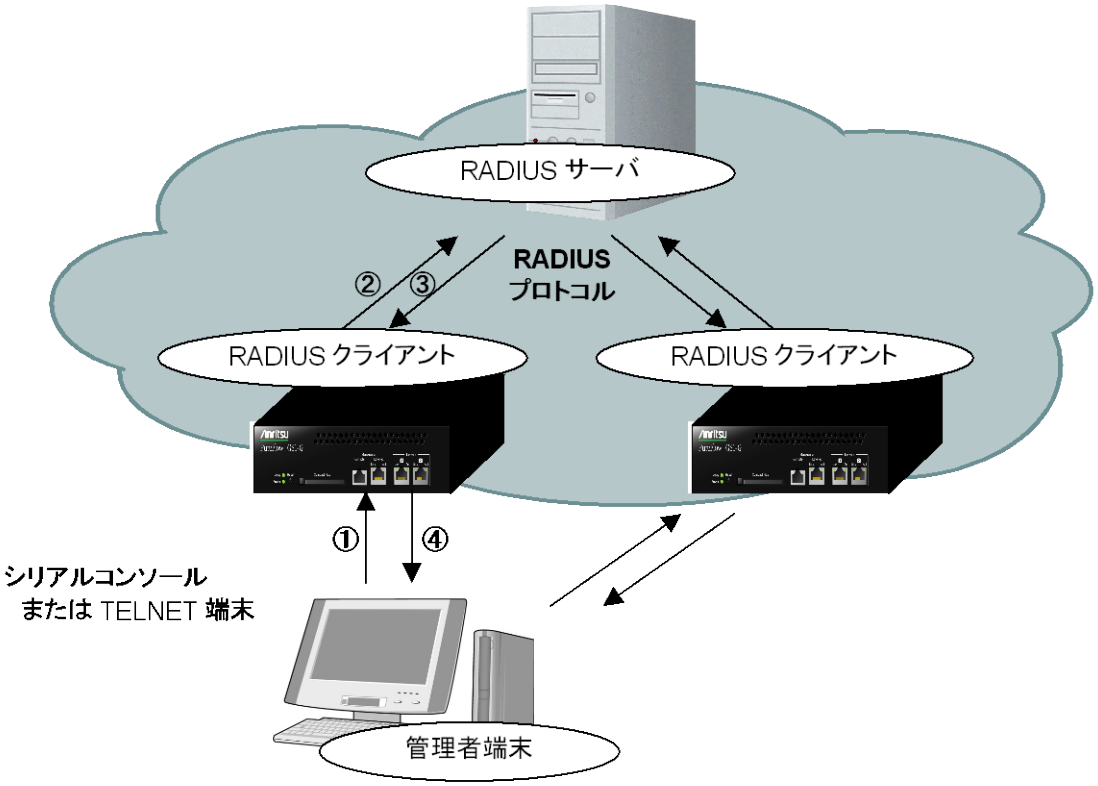
（1）GS1 ライセンスキー3 を有効にし，仮想パイプシナリオまたは仮想チャネルシナリオを 1024 個以上設定した場合，Web 監視機能が，正常に動作しないことがあります。

（2）WEB アプリケーションと本装置の接続に数秒以上の時間を要する場合，監視機能が正常に動作しないことがあります。
WEB 監視機能を使用する場合は，WEB アプリケーションを実行するパソコンから本装置に接続し，ユーザ名とパスワードを入力したあと，ただちにログインできることを確認してください。特に，RADIUS 機能が有効になっているにもかかわらず，RADIUS サーバが動作していない場合など，ログインまでに数秒の時間を要する場合は，接続環境を適切に変更してください。

ここでは，RADIUS（Remote Authentication Dial In User Service）機能について説明します。

17.1 概要

RADIUS 機能は，TELNET，SSH，およびシリアルコンソールのログイン時に，RADIUS（RFC2865）を使用してユーザ認証する機能です。本装置は，RADIUS クライアントとして動作し，外部に設置した RADIUS サーバのユーザ情報に基づいたユーザ認証が可能です。



① ユーザが管理者端末からユーザ名とパスワードを入力する。

② PureFlowGS1 の RADIUS クライアントから RADIUS サーバに認証要求を送信する。

③ RADIUS サーバから RADIUS クライアントに認証応答を送信する。

④ PureFlowGS1 は受信した認証応答に基づいて管理者端末からの接続を許可する。

17.2 ログイン認証の制御

RADIUS 機能を有効にした場合のログイン認証の制御について説明します。RADIUS 機能が有効な場合と無効な場合におけるログイン認証の制御は以下のとおりです。

RADIUS 認証有効時の ログイン認証手順	RADIUIS 認証無効時の ログイン認証手順
1）　本装置に設定されたユーザ名とログインパスワードでログイン認証を実施します。 2）　ログイン認証が拒否された場合，RADIUS サーバに登録されたユーザ名とログインパスワードでログイン認証を実施します。	1）　本装置に設定されたユーザ名とログインパスワードでログイン認証を実施します。

17.3 ログインモードの制御

本装置は，RADIUS サーバに設定されるユーザごとのサービスタイプに従って，ユーザがログインしたときのログインモードを切り替えます。本装置がサポートするサービスタイプは以下のとおりです。

サービスタイプ	ログインモード
Login-User(1)	normal モード
Administrative-User(6)	administrator モード

なお，RADIUS サーバから上記以外のサービスタイプが指定された場合，Normal モードでログインします。

17.4 RADIUS 機能の設定

RADIUS 認証サーバの情報および認証用パラメータを設定することで RADIUS クライアントとしてユーザ認証することが可能となります。

set radius auth { enable | disable }	RADIUS 認証の有効／無効を設定します。
set radius auth timeout <timeout>	RADIUS 認証応答パケットの受信タイムアウト値を設定します。
set radius auth retransmit <retry>	RADIUS 認証要求パケットの再送信回数を設定します。
set radius auth method {PAP|CHAP| default}	RADIUS 認証方法を設定します。
add radius auth server <IP_address> [port <port>] key <string > [Primary]	RADUIS 認証サーバを追加します。
update radius auth server <IP_address> [port <port>] [key <string>] [Primary]	すでに存在しているRADIUS認証サーバの設定内容を変更します。
delete radius auth server <IP_address>	RADIUS 認証サーバの設定を削除します。
show radius	RADIUS 設定情報を表示します。

以下に RADIUS 機能の設定例を記述します。

① RADIUS 認証方法を設定します。例では，PAP 認証方式を設定しています。

```
PureFlow(A)> set radius auth method PAP
```

② RADUIS 認証サーバを追加します。例では，2 つのサーバを登録しています。ひとつは，サーバ IP アドレス 192.168.1.10，RADIUS 共有鍵“testing123”で設定しています。もうひとつは，サーバ IP アドレス 192.168.1.11，RADIUS 共有鍵“testing789”で設定しています。 Primary 指定は，最初にログイン認証を問い合わせする RADIUS サーバに設定します。Primary 指定がない場合は，RADIUS サーバが登録された順番にログイン認証を問い合わせします。

```
PureFlow(A)> add radius auth server 192.168.1.10 key testing123 Primary
PureFlow(A)> add radius auth server 192.168.1.11 key testing789
```

③ RADIUS 機能を有効にします。

```
PureFlow(A)> set radius auth enable
```

④　設定内容を確認します。

```
PureFlow(A)> show radius
RADIUS Authentication：Enable
RADIUS method              ：PAP
RADIUS server entries：2
Retry retransmit          ：5
Retry timeout             ：3

Type Pri Server              Port    key
---- --- --------------- ----- ------------------------------------------
auth   *   192.168.1.10      1812   "testing123"
auth       192.168.1.11      1812   "testing789"
PureFlow(A)>
```

17.5 RADIUS サーバの設定

RADIUS サーバの設定方法を説明します。RADIUS サーバには，以下のユーザ情報を設定します。

RADIUS 共有鍵

PureFlowGS1 に設定した RADIUS 共有鍵と同一の文字列を指定します。

ユーザ ID

ユーザ ID を設定します。

認証方法

PureFlowGS1 に設定した認証方法と同じ認証方法（CHAP または PAP）を指定します。

パスワード

パスワードを設定します。

サービスタイプ

このパラメータは必要に応じて設定します。RADIUS サーバからサービスタイプが通知されない場合，PureFlowGS1 は normal モードでのログインをユーザに許可します。RADIUS サーバからサービスタイプが通知され，そのサービスタイプが Administrative-User の場合，administrator モードでのログインをユーザに許可します。

本書では，RADIUS サーバとして FreeRADIUS を使用した場合を説明しますが，実際の設定についてはお使いの RADIUS サーバの種類によって異なる設定が必要となります。FreeRADIUS は，LDAP（Lightweight Directory Access Protocol），SQL Server，UNIX システムのユーザ情報などのさまざまなユーザー情報と統合可能であり，企業内の多数のユーザーの管理，認証，認可に使用することができます。

（注）

Linux に FreeRADIUS がインストールされていることを前提としています。FreeRADIUS の設定方法および，使用方法の詳細は，インストールされているソフトウエアのマニュアルを参照してください。

① RADIUS 共有鍵の設定

RADIUS サーバに RADIUS クライアントとして登録する装置の IP アドレスおよび, RADIUS 共有鍵を以下の形式で設定します。

RADIUS サーバの/usr/local/etc/raddb/clients.conf ファイルを開き, 適切なセクションに以下の設定を追加してください。

```
client 192.168.37.10 {
        secret =  testing123
        shortname =  gs1
}
```

② ユーザの設定

RADIUS サーバに PureFlowGS1 へのログインを許可するユーザ情報を設定します。ユーザごとに, ユーザ ID, 認証方法, パスワード, サービスタイプを設定します。

RADIUS サーバの/usr/local/etc/raddb/users ファイルを開き, 適切なセクションに以下の設定を追加してください。

1） 認証方法に CHAP を使用する場合

normal モードでのログインを許可するユーザの設定

```
user1   Auth-Type := CHAP, User-Password == "user1passwd"
        Service-Type = Login-User(1)
```

Administrator モードでのログインを許可するユーザの設定

```
user2   Auth-Type := CHAP, User-Password == "user2passwd"
        Service-Type = Administrative-User(6)
```

2） 認証方法に PAP を使用する場合

normal モードでのログインを許可するユーザの設定

```
user3   Auth-Type := PAP, User-Password == "user3passwd"
        Service-Type = Login-User(1)
```

Administrator モードでのログインを許可するユーザの設定

```
user4   Auth-Type := PAP, User-Password == "user4passwd"
        Service-Type = Administrative-User(6)
```

ソフトウェアやコンフィギュレーションをダウンロード／アップロードする場合は，Compact Flash（以下 CF）カードを使用します。CF カードは，MS-DOS フォーマット（FAT12／FAT16）を対象とします。また，ソフトウェアのダウンロード，コンフィギュレーションのダウンロード／アップロードについては，システムインタフェースから TFTP により実行することもできます。システムインタフェースを使用する場合には TFTP サーバ機能を備えた PC などを用意してください。

また，CF カードをご使用になる場合，弊社推奨 CF カードをご使用ください。推奨 CF カード以外での動作は保証対象外です。

ソフトウェアやコンフィギュレーションのロードは，Command Line Interface（CLI）を使用します。CLI については，「第 3 章 設定の基本」を参照してください。

18.1 ソフトウェアのダウンロード／アップロード

18.1.1 ソフトウェアをCFカードよりダウンロードする

CF カードスロットに，新しいソフトウェアオブジェクトが入った CF カードを挿入して，新しいソフトウェアを装置にダウンロードします。ダウンロードしたソフトウェアは自動的に内蔵フラッシュメモリに保存されます。このとき古いバージョンのソフトウェアは別領域に待避し，新しいソフトウェアの書込みを行います。バージョンアップ作業中は，CF カードを抜いたり，装置の電源が切断されないようにご注意ください。万が一作業中に，CF カードを抜いたり，装置の電源を切断してしまった場合は，別領域に待避してある古いバージョンのソフトウェアを再ロードしますので，再度装置を起動してダウンロード作業をやり直してください。

```
PureFlow(A)> download cf obj PureFlow.bin
Download ”/ext/PureFlow.bin” from Flash Memory Card (y/n)? y
Loading ....................
creating Backup from Master file.....................completed.
Done.
PureFlow(A)>
```

ダウンロードが完了しても，新しいソフトウェアはすぐに反映されません。ダウンロードが完了したあとで，装置を再起動してください。

18.1.2 ソフトウェアをCFカードにアップロードする

CF カードスロットに CF カードを挿入してソフトウェアを CF カードにアップロードします。アップロードしたソフトウェアは挿入した CF カードに保存されます。

```
PureFlow(A)> upload cf obj PureFlow.bin
Upload as ”/ext/PureFlow.bin” to Flash Memory Card (y/n)? y
Loading ....................
Done.
PureFlow(A)>
```

18.1.3 ソフトウェアをTFTPによりダウンロードする

TFTP によりソフトウェアを装置にダウンロードします。ダウンロードしたソフトウェアは自動的に内蔵フラッシュメモリに保存されます。このとき古いバージョンのソフトウェアは別領域に待避し，新しいソフトウェアの書込みを行います。バージョンアップ作業中は装置の電源が切断されないようにご注意ください。万が一作業中に装置の電源を切断してしまった場合は，別領域に待避してある古いバージョンのソフトウェアを再ロードしますので，再度装置を起動してダウンロード作業をやり直してください。

ソフトウェアを装置にダウンロードするには以下のコマンドを使用します。あらかじめ TFTP サーバと通信できるようにシステムインタフェースに正しい IP アドレスを設定してください。システムインタフェースの設定の説明は「第 7 章 システムインタフェースの設定」を参照してください。

```
PureFlow(A)> download tftp obj 192.168.100.40 newfile.bin
Download ”newfile.bin” from 192.168.100.40 (y/n)? y
Loading ...
creating Backup from Master file.....................completed.
Done.
PureFlow(A)>
```

ダウンロードが完了しても，新しいソフトウェアはすぐに反映されません。ダウンロードが完了したあとで，装置を再起動してください。

ソフトウェアをダウンロードするときの注意事項

弊社指定の正規オブジェクトファイル以外をダウンロードしますと，装置が起動しません。上記のコマンドで正規のオブジェクトファイル以外の誤ったファイルをダウンロードしないようにご注意ください。誤ったオブジェクトファイルをダウンロードした場合は，正規のオブジェクトファイルが入った CF カードを CF カードスロットに挿入して，装置を起動してください。その後，正規のオブジェクトファイルを再度ダウンロードしてください。正規オブジェクトファイルの入手方法は，当社営業窓口へお問い合わせください。

18.2 コンフィギュレーションのダウンロード／アップロード

18.2.1 コンフィギュレーションをCFカードよりダウンロードする

CF カードスロットに CF カードを挿入して新しいコンフィギュレーションファイルを装置にダウンロードします。ダウンロードしたコンフィギュレーションファイルは自動的に内蔵フラッシュメモリに保存されます。このとき古いコンフィギュレーションファイルは別領域に待避し，新しいコンフィギュレーションファイルの書込みを行います。ダウンロードが完了しても，新しいコンフィギュレーションはすぐに反映されません。ダウンロードが完了したあとで，装置を再起動してください。ダウンロード作業中は，CF カードを抜いたり，装置の電源が切断されないようにご注意ください。万が一作業中に，CF カードを抜いたり，装置の電源を切断してしまった場合は，別領域に待避してある古いコンフィギュレーションファイルを再ロードしますので，再度装置を起動してダウンロード作業をやり直してください。

```
PureFlow(A)> download cf conf config.txt
Download ”/ext/config.txt” from Flash Memory Card (y/n)? y
Loading ...
Done.
PureFlow(A)>
```

ダウンロードが完了しても，ダウンロードしたコンフィグレーションはすぐに反映されません。ダウンロードが完了したあとで，装置を再起動してください。

18.2.2 コンフィギュレーションをCFカードにアップロードする

CF カードスロットに CF カードを挿入してコンフィギュレーションファイルを CF カードにアップロードします。アップロードしたコンフィギュレーションファイルは挿入した CF カードに保存されます。

```
PureFlow(A)> upload cf conf config.txt
Upload as ”/ext/config.txt” to Flash Memory Card (y/n)? y
Loading ...
Done.
PureFlow(A)>
```

動作中のコンフィグレーション情報ではなく，内部フラッシュメモリにセーブされたコンフィギュレーション情報がアップロードされます。コンフィグレーション情報は，save config コマンドを実行したとき，内部フラッシュメモリに保存されます。

18.2.3 コンフィギュレーションをTFTPによりダウンロードする

TFTP によりコンフィギュレーションファイルを装置にダウンロードします。ダウンロードしたコンフィギュレーションファイルは自動的に内蔵フラッシュメモリに保存されます。このとき古いバージョンのコンフィギュレーションファイルは別領域に待避し，新しいコンフィギュレーションファイルの書込みを行います。ダウンロードが完了しても，新しいコンフィギュレーションはすぐに反映されません。ダウンロードが完了したあとで，装置をを再起動してください。ダウンロード作業中は装置の電源が切断されないようにご注意ください。万が一作業中に装置の電源を切断してしまった場合は，別領域に待避してある古いコンフィギュレーションファイルで再ロードしますので，再度装置を起動してダウンロード作業をやり直してください。

コンフィギュレーションファイルを装置にダウンロードするには以下のコマンドを使用します。あらかじめ TFTP サーバと通信できるようにシステムインタフェースに正しい IP アドレスを設定してください。システムインタフェースの設定の説明は「第 7 章　システムインタフェースの設定」を参照してください。

```
PureFlow(A)> download tftp conf 192.168.100.40 config.txt
Download ”config.txt” from 192.168.100.40 (y/n)? y
Loading ...
Done.
PureFlow(A)>
```

ダウンロードが完了しても，ダウンロードしたコンフィグレーションはすぐに反映されません。ダウンロードが完了したあとで，装置を再起動してください。

18.2.4 コンフィギュレーションをTFTPによりアップロードする

TFTP によりコンフィギュレーションファイルを TFTP サーバにアップロードします。アップロードしたコンフィギュレーションファイルは TFTP サーバに保存されます。

```
PureFlow(A)> upload tftp conf 192.168.100.40 config.txt
Upload as ”config.txt” to 192.168.100.40 (y/n)? y
Loading ...
Done.
PureFlow(A)>
```

動作中のコンフィグレーション情報ではなく，内部フラッシュメモリにセーブされたコンフィギュレーション情報がアップロードされます。

コンフィギュレーションをダウンロードするときの注意事項）

弊社指定の正規コンフィギュレーションファイル以外をダウンロードしますと，装置が起動しない場合があります。上記のコマンドで正規のコンフィギュレーションファイル以外の誤ったファイルをダウンロードしないようにご注意ください。誤ったコンフィギュレーションファイルをダウンロードした場合は，正規のコンフィギュレーションファイルが入った CF カードを CF カードスロットに挿入して，装置を起動してください。その後，正規のコンフィギュレーションファイルを再度ダウンロードしてください。正規コンフィギュレーションファイルの入手方法は，当社営業窓口へお問い合わせください。

18.3 ソフトウェアを再起動する

ダウンロードが完了したあとは新しいソフトウェアで再起動させます。

(1) 装置を再起動する

装置の再起動方法です。電源を再投入するか以下のコマンドを使用してください。

```
PureFlow(A)> reboot system
Rebooting the system, ok(y/n)? y
```

(2) 再起動の完了確認

再起動は Telnet の接続がいったん切断されます。装置起動後，再度 Telnet によりログインし直してください。

付録A　デフォルト値

本装置には，機能に応じていくつもの設定項目があります。項目の中にはその機能を使用しない限り設定する必要のないものもありますが，設定が必須なものもあります。設定値を必要とする項目については，あらかじめ値が設定されています。表 1 に設定項目と設定値を示します。コマンドの詳細については「PureFlow GS1 取扱説明書 コマンドリファレンス」を参照してください。

表 1　デフォルト値一覧

設定項目	コマンド	既設定値	設定範囲
ユーザ名	ユーザ名	root	設定なし
パスワード	set password	(なし)	最大 16 文字
	set adminpassword	(なし)	最大 16 文字
Network ポート設定	set port autonegotiation	enable	enable/disable
	set port speed	100M	100M/10M
	set port duplex	full	full/half
	set port flow_control	auto	auto/on/off
エージングタイム	set agingtime	300 秒	1～1800 秒
SYSLOG	set syslog host	Disable	enable/disable
	add syslog host ip (IPv4 Address)	(なし)	IPv4 Address
	add syslog host ip (UDP port)	514	1～65534
	set syslog host ip (IPv4 Address)	(なし)	IPv4 Address
	set syslog host ip (UDP Port)	514	1～65534
	set syslog severity	notice(5)	0～6
	set syslog facility ccpu	16(local0)	0～23
	set syslog facility fcpu	17(local1)	0～23
オートログアウト	set autologout time	10 分	1～30 分
SNTP	set sntp	disable	enable/disable
	set sntp server	(なし)	IPv4 Address
	set sntp interval	3600 秒	60～86400 秒
RADIUS	set radius auth	disable	enable/disable
	set radius auth timeout	5	1～30 秒
	set radius auth retransmit	3	0～10 回
	set radius auth method	CHAP	CHAP/PAP

設定項目	コマンド	既設定値	設定範囲
システムインタフェース	set ip system(Ipv4 Address)	192.168.1.1	IPv4 Address
	set ip system(netmask)	255.255.255.0	IPv4 Address
	set ip system(up/down)	up	up/down
	set ip system port (ethernet/network)	ethernet	ethernet/network
	set ip system port network (in <slot/port>/all)	all (すべての Network ポート)	1/1，1/2，all ※通信ポートが network のとき
	set ip system port network (vid <VID>/none)	none (VLAN Tag なし)	0～4094/none ※通信ポートが network のとき
	set ip system gateway	(なし)	IPv4 Address
自動リブート	set autoreboot	enable	enable/disable
フロー識別モード	set filter mode	default	default,cos,sip,dip,tos, proto,appli
Bridge-Ctrl パケット優先設定	set bridge-ctrl priority	low	high/low
通信ギャップモード設定	set bandwidth mode	no_gap	gap/no_gap
リンクダウン転送機能	set lpt	disable	enable/disable
Telnet 接続設定	set telnet	enable	enable/disable

付録B　SYSLOG 一覧

syslog の一覧を表 2 に示します。表 2 は severity（カッコ内は重大度）ごとにまとめています。

（参考）

syslog メッセージには括弧（[ ]や< >）で囲まれた 16 進数が付加されるものがあります。括弧内の 16 進数はソースコード上の位置や変数値を表しており，当社内でのトラブルシューティングで参照します。

表 2　syslog 一覧

Severity	syslog メッセージ	発生条件	対応方法
Emergency (0)	Temperature #N of the system is critical：xx.xx	システムの温度が危険域 (#N は 1 または 2) (xx.xx は温度(℃))	このまま使用を続けるとハードウェアが損傷を受ける可能性があります。直ちに電源を落としてください。
Alert (1)	Temperature #N of the system is OK：xx.xx	システムの温度範囲が正常値に復帰 (#N は 1 または 2) (xx.xx は温度(℃))	回復措置は不要です。
	Temperature #N of the system is abnormal：xx.xx	システムの温度が異常 (#N は 1 または 2) (xx.xx は温度(℃))	設置環境の温度が範囲内(0～40℃)であることを確認してください。 範囲内である場合は装置を交換してください。範囲外である場合は設置場所を変えてください。
	No response from Slot #N	モジュールからの応答無し (#N は 1)	弊社サポートまでご連絡ください。
	Slot #N response is OK	モジュールからの応答が回復 (#N は 1)	回復措置は不要です。
Notice (5)	The buffer of queue exceeded the limit. [F:#N,S:#M,Q:#Q]	フィルタ N，シナリオ M で生成されたキュー Q のパケットバッファ使用量が制限値を超過した。	キューバッファフルのためパケット廃棄が発生しています。入力バースト長の設定をチェックしてください。
	The buffer of queue is less than 50% of the limit.[F:#N,S:#M,Q:#Q]	フィルタ N，シナリオ M で生成されたキュー Q のパケットバッファ使用量が制限値を超えたあと，制限値の 50%を下回った。	回復処置は不要です。
	Queue allocation failure for the system.	装置が使用しているキューの使用数が装置で使用できるキューの最大数に達し，キュー確保が失敗した。	トラフィック状況，および各種設定をチェックしてください。
	Queue allocation available for the system.	装置が使用しているキューの使用数が装置で使用できるキューの最大数に達したあと，キューの使用数が最大値の 50%を下回った。	回復処置は不要です。

Severity	syslog メッセージ	発生条件	対応方法
Notice (5)	Queue allocation failure for the scenario.[S:#N]	シナリオ N が要求したキューの数が制限値(maxqnum)を超過し，キュー確保が失敗した。	トラフィック状況，およびシナリオ設定をチェックしてください。
	Queue allocation available for the scenario.[S:#N]	シナリオ N が使用しているキューの数が制限値(maxqnum)を超過したあと，制限値の 50%を下回った。	回復処置は不要です。
	Media session bandwidth allocation failure for the scenario.[S:#N]	シナリオ N でメディアセッションに割り当てた最低帯域の合計が合計最低帯域(total_min_bandwidth)を超過し，キューの帯域割り当てが失敗した。	メディアセッションに最低帯域が割り当てられていません。トラフィック状況，および total_min_bandwidth の設定をチェックしてください。
	Media session bandwidth allocation available for the scenario.[S:#N]	シナリオ N でメディアセッションに割り当てた最低帯域の合計が合計最低帯域(total_min_bandwidth)を超過したあと，制限値の 50%を下回った。	回復処置は不要です。
	Flow registration failure for the system.	装置内のフローが最大数を超えた	トラフィック状況，および各種設定をチェックしてください。
	Flow registration available for the system.	装置内のフローが最大数に達したあと，最大数の 50%を下回った。	回復処置は不要です。
	Application session registration failure for the system.	装置内のセッション管理エントリが最大数を超えた	トラフィック状況，および各種設定をチェックしてください。
	Application session registration available for the system.	装置内のセッション管理エントリが最大数に達したあと，最大数の 50%を下回った。	回復処置は不要です。
	Unknown media session bandwidth.[SIP:xxx.xxx.xxx.xxx][C:#N][P:SIP/H.323 VOICE/VIDEO][D:XX]	送信元 IPv4 アドレス xxx.xxx.xxx.xxx のメディアセッション帯域を認識できなかった。 (XX:コーデック情報)	メディアセッションに最低帯域が割り当てられていません。トラフィック状況，および各種設定をチェックしてください。
	Unknown media session bandwidth.[SIP:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx][C:#N][P:SIP/H.323 VOICE/VIDEO][D:XX]	送信元 IPv6 アドレス xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx のメディアセッション帯域を認識できなかった。 (XX:コーデック情報)	メディアセッションに最低帯域が割り当てられていません。トラフィック状況，および各種設定をチェックしてください。

Severity	syslog メッセージ	発生条件	対応方法
Notice (5)	Application sessions recognition failure for the system.[C:#N]	装置内のアプリケーション処理能力不足により，アプリケーション認識ができなかった。	トラフィック状況，および各種設定をチェックしてください。
	Bypass connected.	バイパスを接続状態にした。	バイパスが接続状態となった理由を特定し，必要な処置を行ってください。
	Bypass disconnected.	バイパスを未接続状態にした。	回復措置は不要です。
Informational (6)	Pipe #N changed Operate from Down.	パイプがリンクアップ (#N は 1)	回復措置は不要です。
	Pipe #N changed Down from Operate.	パイプがリンクダウン (#N は 1)	下記を確認してください。 ・該当箇所が LinkDown を起していないか。
	Port #N/#M changed Up from Down.	ポートがリンクアップ (#N は 1) (#M は 1～2)	回復措置は不要です。
	Port #N/#M changed Down from Up.	ポートがリンクダウン (#N は 1) (#M は 1～2)	下記を確認してください。 ・ケーブル断は起きていないか。 ・正しいケーブル(ストレート／クロス)を使用しているか。 ・Network ポートの Speed／Duplex および Pause の設定が接続装置と合っているか。
	Port #N/#M changed PowerDown with Link Pass Through.	リンクダウン転送機能が動作 (#N は 1) (#M は 1～2)	下記を確認してください。 ・ケーブル断は起きていないか。 ・正しいケーブル(ストレート／クロス)を使用しているか。 ・Network ポートの Speed／Duplex および Pause の設定が接続装置と合っているか。
	Management Ethernet Port changed Up from Down.	Management Ethernet ポートがリンクアップ	回復措置は不要です。
	Management Ethernet Port changed Down from Up.	Management Ethernet ポートがリンクダウン	下記を確認してください。 ・ケーブル断は起きていないか。 ・正しいケーブルを使用しているか。 Management Ethernet ポートの接続装置の設定が Autonegotiation になっているか。
	ARP cache overflow [xxx.xxx.xxx.xxx failed].	ARP キャッシュエントリが最大数を超えたため，IPv4 アドレス xxx.xxx.xxx.xxx の ARP キャッシュエントリ登録が失敗した。	装置に接続されているネットワーク環境を確認してください。

Severity	syslog メッセージ	発生条件	対応方法
Informational (6)	AnritsuPureFlow Software Version x.x.x.x	装置起動	回復措置は不要です。
	User %s authentication from RADIUS server was Accept	ユーザ名%s の RADIUS 認証が accept された。	回復措置は不要です。
	User %s authentication from RADIUS server was Reject	ユーザ名%s の RADIUS 認証が reject された。	回復措置は不要です。
	User %s authentication from RADIUS server was Timeout	ユーザ名%s の RADIUS 認証がタイムアウトした。	回復措置は不要です。
	User root logged in from xxx.xxx.xxx.xxx	telnet host のユーザが本装置にログイン	回復措置は不要です。
	Three Unsuccessful logins from Console	コンソールからログインに 3 回失敗	パスワードを確認してください。
	Three Unsuccessful logins from xxx.xxx.xxx.xxx	telnet host のユーザからログインに 3 回失敗	パスワードを確認してください。
	SNTP Corrected TIME	SNTP によるシステム時刻の修正	回復措置は不要です。

付録C　SNMP Trap 一覧

SNMP Trap の一覧を表 3 に示します。

Trap は有効に設定されているもののみ送出されます。Trap の有効／無効の設定は，“set snmp traps”コマンドを使用して設定します。コマンドの詳細については，「PureFlow GS1 トラフィックシェーパー PF7000A/PF7001A/PF7010A/PF7011A 取扱説明書 コマンドリファレンス」を参照してください。

表 3　SNMP Trap 一覧

MIB オブジェクト名	コマンドでの設定名	発生条件	対応方法
coldStart(1.3.6.1.6.3.1.1.5.1)	coldstart	装置起動完了	下記を確認してください。 ・電源断は起きていないか。 ・リセットボタンが押されていないか。 ・再起動コマンドを実行していないか。
warmStart(1.3.6.1.6.3.1.1.5.2)	warmstart	出力されません。	
linkDown(1.3.6.1.6.3.1.1.5.3)	linkdown	ポートのリンクダウン	下記を確認してください。 ・ケーブル断は起きていないか。 ・正しいケーブル（ストレート／クロス）を使用しているか。 ・Network ポートの Speed/Duplex および Pause の設定が接続装置と合っているか。
linkUp(1.3.6.1.6.3.1.1.5.4)	linkup	リンクアップ	回復措置は不要です。
authenticationFailure(1.3.6.1.6.3.1.1.5.5)	authentication	SNMP の不正アクセス検出	本装置に設定したアクセス許可 comunity 名，IP address，レベル（get/set）が，SNMP manager 側と合っているか確認してください。
pfGsModuleFailureAlarmEvent(1.3.6.1.4.1.1151.2.1.7.20.0.7)	modulefailurealarm	モジュール異常の検出	弊社サポートまでご連絡ください。
pfGsModuleFailureRecoveryEvent(1.3.6.1.4.1.1151.2.1.7.20.0.8)	modulefailurerecovery	モジュール異常の回復	回復措置は不要です。
pfGsSystemHeatAlarmEvent(1.3.6.1.4.1.1151.2.1.7.20.0.9)	systemheatalarm	システム温度異常の検出	環境温度が 40℃以下になるように空調または機器配置を見直してください。

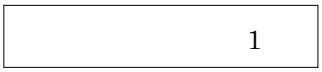
MIB オブジェクト名	コマンドでの設定名	発生条件	対応方法
pfGsSystemHeatRecoveryEvent(1.3.6.1.4.1.11151.2.1.7.20.0.10)	systemheatrecovery	システム温度異常の回復	回復措置は不要です。

付録D　Enterprise MIB 一覧

PureFlow GS の Enterprise MIB オブジェクト一覧を表 4 に示します。

表 4　PureFlow GS Enterprise MIB 一覧

MIB グループ	MIB オブジェクト名	説明
pureFlowGsMib		PureFlow GS Enterprise MIB ツリーです。オブジェクト ID は 1.3.6.1.4.1.1151.2.1.7 です。 以下にツリー内のオブジェクトと，そのオブジェクト ID（カッコ内の値）を示します。
pfGsSystem(1.3.6.1.4.1.1151.2.1.7.1)	pfGsSystemType(1.3.6.1.4.1.1151.2.1.7.1.1)	システムソフトウェアの形名を表します。 px700001a(1)　　：PX700001A
	pfGsSystemSlotNumber(1.3.6.1.4.1.1151.2.1.7.1.2)	モジュールを実装するスロットの数を表します。
	pfGsSystemSoftwareRev(1.3.6.1.4.1.1151.2.1.7.1.3)	システムソフトウェアのバージョンを表します。
	pfGsSystemTemperature(1.3.6.1.4.1.1151.2.1.7.1.4)	装置の温度を表します。単位は摂氏です。システムには複数の温度計が実装されていますが，この MIB オブジェクトは温度計#2 の値を示します。
	pfGsSystemOperationTime(1.3.6.1.4.1.1151.2.1.7.1.5)	装置の累積稼働時間を表します。単位は 10 ms です。この MIB オブジェクトは 1 時間ごとに更新されます。したがって，時間以下の単位は常に 0 となります。
	pfGsSystemCcpu5sec(1.3.6.1.4.1.1151.2.1.7.1.6)	制御系 CPU の CPU 使用率を，最近 5 秒の平均値で表します。
	pfGsSystemCcpu1min(1.3.6.1.4.1.1151.2.1.7.1.7)	制御系 CPU の CPU 使用率を，最近 1 分の平均値で表します。
	pfGsSystemCcpu5min(1.3.6.1.4.1.1151.2.1.7.1.8)	制御系 CPU の CPU 使用率を，最近 5 分の平均値で表します。
	pfGsSystemCcpuMemory5sec(1.3.6.1.4.1.1151.2.1.7.1.9)	制御系 CPU のメモリ使用率を，最近 5 秒の平均値で表します。
	pfGsSystemCcpuMemory1min(1.3.6.1.4.1.1151.2.1.7.1.10)	制御系 CPU のメモリ使用率を，最近 1 分の平均値で表します。
	pfGsSystemCcpuMemory5min(1.3.6.1.4.1.1151.2.1.7.1.11)	制御系 CPU のメモリ使用率を，最近 5 分の平均値で表します。
	pfGsSystemFcpuTable(1.3.6.1.4.1.1151.2.1.7.1.12)	フォワーディング系 CPU の CPU およびメモリ使用率のテーブルです。 このテーブルには以下のオブジェクトが含まれています。
	pfGsSystemFcpuEntry(1.3.6.1.4.1.1151.2.1.7.1.12.1)	フォワーディング系 CPU の CPU およびメモリ使用率のエントリテーブルです。テーブルインデックスは pfSystemFcpuIndex です。 このテーブルには以下のオブジェクトが含まれています。

MIB グループ	MIB オブジェクト名	説明
	pfGsSystemFcpuIndex(1.3.6.1.4.1.1151.2.1.7.1.12.1.1)	フォワーディング系 CPU の番号を表します。 正面図 
	pfGsSystemFcpu5sec(2)	フォワーディング系 CPU の CPU 使用率を，最近 5 秒の平均値で表します。
	pfGsSystemFcpu1min(3)	フォワーディング系 CPU の CPU 使用率を，最近 1 分の平均値で表します。
	pfGsSystemFcpu5min(4)	フォワーディング系 CPU の CPU 使用率を，最近 5 分の平均値で表します。
	pfGsSystemFcpuMemory5sec(5)	フォワーディング系 CPU のメモリ使用率を，最近 5 秒の平均値で表します。
	pfGsSystemFcpuMemory1min(6)	フォワーディング系 CPU のメモリ使用率を，最近 1 分の平均値で表します。
	pfGsSystemFcpuMemory5min(7)	フォワーディング系 CPU のメモリ使用率を，最近 5 分の平均値で表します。
pfGsModule(1.3.6.1.4.1.1151.2.1.7.2)	pfGsModuleTable(1.3.6.1.4.1.1151.2.1.7.2.1)	モジュール情報のテーブルです。 このテーブルには以下のオブジェクトが含まれています。
	pfGsModuleEntry(1.3.6.1.4.1.1151.2.1.7.2.1.1)	モジュール情報のエントリテーブルです。テーブルインデックスは pfGsModuleIndex です。 このテーブルには以下のオブジェクトが含まれています。
	pfGsModuleIndex(1.3.6.1.4.1.1151.2.1.7.2.1.1.1)	モジュールの番号を表します。 正面図  注）システムソフトウェアが PX700001A の場合，1 のみです。
	pfGsModuleLocation(1.3.6.1.4.1.1151.2.1.7.2.1.1.2)	モジュールの実装スロット番号を表します。 （モジュール番号と同じ値になります） 正面図  注）システムソフトウェアが PX700001A の場合，1 のみです。

MIB グループ	MIB オブジェクト名	説明
	pfGsModuleType(1.3.6.1.4.1.1151.2.1.7.2.1.1.3)	モジュールの種別を表します。 unknown(1) ： 下記以外 empty(2) ： 未実装 ge2gt(3) ：GbE/2T fe2ft(4) ：FE/2T
	pfGsModuleDescr(1.3.6.1.4.1.1151.2.1.7.2.1.1.4)	モジュールの名前を表します。
	pfGsModulePortNumber(1.3.6.1.4.1.1151.2.1.7.2.1.1.5)	モジュールの実装ポート数を表します。 注)システムソフトウェアが PX700001A の場合，1/1 および 1/2 のみ使用可能です。
	pfGsModuleOperStatus(1.3.6.1.4.1.1151.2.1.7.2.1.1.6)	モジュールの状態を表します。 other(1) ： 下記以外 operational(2) ： 正常 malfunctioning(3) ：6 以外の異常 notPresent(4) ： 未実装 standby(5) ：（未使用です） notResponding(6) ： 応答なし
	pfGsModuleRevision(1.3.6.1.4.1.1151.2.1.7.2.1.1.7)	モジュールのハードウェアレビジョンを表します。
	pfGsModuleSerialNumber(1.3.6.1.4.1.1151.2.1.7.2.1.1.8)	モジュールのシリアル番号を表します。
pfGsQueueStatistics(1.3.6.1.4.1.1151.2.1.7.5)	pfGsQueueStatisticsTable(1.3.6.1.4.1.1151.2.1.7.5.1)	キューカウンタテーブルです。 キューがエージアウトされたとき当該キューのキューカウンタも削除されます。 このテーブルには以下のオブジェクトが含まれています。
	pfGsQueueStatisticsEntry(1.3.6.1.4.1.1151.2.1.7.5.1.1)	キューカウンタエントリテーブルです。テーブルインデックスは以下の 3 つです。 pfGsQueueStatisticsFilterIndex pfGsQueueStatisticsFilterSubIndex pfGsQueueStatisticsQueueIndex このテーブルには以下のオブジェクトが含まれています。 参考)このテーブル内オブジェクトの OID を求める方法をこの表の次に示します。
	pfGsQueueStatisticsFilterIndex(1.3.6.1.4.1.1151.2.1.7.5.1.1.1)	キューに割り当てられたフィルタの親フィルタ ID を表します。
	pfGsQueueStatisticsFilterSubIndex(1.3.6.1.4.1.1151.2.1.7.5.1.1.2)	キューに割り当てられたフィルタの子フィルタ ID を表します。

MIB グループ	MIB オブジェクト名	説明
	pfGsQueueStatisticsQueueIndex(1.3.6.1.4.1.1151.2.1.7.5.1.1.3)	キューのキューID を表します。
	pfGsQueueStatisticsFilterType(1.3.6.1.4.1.1151.2.1.7.5.1.1.4)	キューに割り当てられたフィルタの種別を表します。 vlan(1) : VLAN フィルタ ipv4(2) : IPv4 フィルタ ipv6(3) : IPv6 フィルタ
	pfGsQueueStatisticsIfIndex(1.3.6.1.4.1.1151.2.1.7.5.1.1.5)	キューが割り当てられたポートの IfIndex を表します。 スロット 1 1/1 1/2 IfIndex 1 2
	pfGsQueueStatisticsRxOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.6)	キューの受信オクテット数を表します。
	pfGsQueueStatisticsRxPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.7)	キューの受信パケット数を表します。
	pfGsQueueStatisticsTxOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.8)	キューの送信オクテット数を表します。
	pfGsQueueStatisticsTxPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.9)	キューの送信パケット数を表します。
	pfGsQueueStatisticsDiscardOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.10)	キューの廃棄オクテット数を表します。
	pfGsQueueStatisticsDiscardPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.11)	キューの廃棄パケット数を表します。
	pfGsQueueStatisticsHCRxOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.12)	キューの受信オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsQueueStatisticsHCRxPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.13)	キューの受信パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsQueueStatisticsHCTxOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.14)	キューの送信オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsQueueStatisticsHCTxPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.15)	キューの送信パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsQueueStatisticsHCDiscardOctets(1.3.6.1.4.1.1151.2.1.7.5.1.1.16)	キューの廃棄オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。

MIB グループ	MIB オブジェクト名	説明
	pfGsQueueStatisticsHCDiscardPackets(1.3.6.1.4.1.1151.2.1.7.5.1.1.17)	キューの廃棄パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
pfGsScenarioStatistics(1.3.6.1.4.1.1151.2.1.7.6)	pfGsScenarioStatisticsTable(1.3.6.1.4.1.1151.2.1.7.6.1)	シナリオ(仮想パイプ／仮想チャネル)カウンタテーブルです。 シナリオが削除されたとき当該シナリオのカウンタも削除されます。 このテーブルには以下のオブジェクトが含まれています。
	pfGsScenarioStatisticsEntry(1.3.6.1.4.1.1151.2.1.7.6.1.1)	シナリオ(仮想パイプ／仮想チャネル)カウンタエントリテーブルです。テーブルインデックスは以下の 1 つです。 pfGsScenarioStatisticsScenarioIndex このテーブルには以下のオブジェクトが含まれています。 参考)このテーブル内オブジェクトの OID を求める方法をこの表の次に示します。
	pfGsScenarioStatisticsScenarioIndex(1.3.6.1.4.1.1151.2.1.7.6.1.1.1)	シナリオのシナリオ ID を表します。
	pfGsScenarioStatisticsScenarioType(1.3.6.1.4.1.1151.2.1.7.6.1.1.2)	シナリオのタイプを表します。 vp(1) ： 仮想パイプシナリオ vcaggregate(2) ： 仮想チャネルシナリオ Aggregate vcindividual(3) ： 仮想チャネルシナリオ Individual vcapplication(4) ： 仮想チャネルシナリオ Application
	pfGsScenarioStatisticsRxOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.3)	シナリオの受信オクテット数を表します。
	pfGsScenarioStatisticsRxPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.4)	シナリオの受信パケット数を表します。
	pfGsScenarioStatisticsTxOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.5)	シナリオの送信オクテット数を表します。
	pfGsScenarioStatisticsTxPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.6)	シナリオの送信パケット数を表します。
	pfGsScenarioStatisticsDiscardOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.7)	シナリオの廃棄オクテット数を表します。
	pfGsScenarioStatisticsDiscardPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.8)	シナリオの廃棄パケット数を表します。
	pfGsScenarioStatisticsHCRxOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.9)	シナリオの受信オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。

MIB グループ	MIB オブジェクト名	説明
	pfGsScenarioStatisticsHCRxPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.10)	シナリオの受信パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsScenarioStatisticsHCTxOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.11)	シナリオの送信オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsScenarioStatisticsHCTxPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.12)	シナリオの送信パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsScenarioStatisticsHCDiscardOctets(1.3.6.1.4.1.1151.2.1.7.6.1.1.13)	シナリオの廃棄オクテット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
	pfGsScenarioStatisticsHCDiscardPackets(1.3.6.1.4.1.1151.2.1.7.6.1.1.14)	シナリオの廃棄パケット数を 64 ビットで表します。 注)このオブジェクトに SNMPv1 でアクセスすることはできません。v2c 以上でアクセスしてください。
pfGsScenarioInformation(1.3.6.1.4.1.1151.2.1.7.7)	pfGsScenarioInformationTable(1.3.6.1.4.1.1151.2.1.7.7.1)	シナリオ(仮想パイプ／仮想チャネル)インフォメーションテーブルです。 シナリオが削除されたとき当該シナリオのインフォメーションも削除されます。 このテーブルには以下のオブジェクトが含まれています。
	pfGsScenarioInformationEntry(1.3.6.1.4.1.1151.2.1.7.7.1.1)	シナリオ(仮想パイプ／仮想チャネル)インフォメーションテーブルです。テーブルインデックスは以下の 1 つです。 pfGsScenarioInformationScenarioIndex このテーブルには以下のオブジェクトが含まれています。 参考)このテーブル内オブジェクトの OID を求める方法をこの表の次に示します。
	pfGsScenarioInformationScenarioIndex(1.3.6.1.4.1.1151.2.1.7.7.1.1.1)	シナリオのシナリオ ID を表します。
	pfGsScenarioInformationScenarioType(1.3.6.1.4.1.1151.2.1.7.7.1.1.2)	シナリオのタイプを表わします。 vp(1) ： 仮想パイプシナリオ vcaggregate(2) ： 仮想チャネルシナリオ Aggregate vcindividual(3) ： 仮想チャネルシナリオ Individual vcapplication(4) ： 仮想チャネルシナリオ Application
	pfGsScenarioInformationQueueNum(1.3.6.1.4.1.1151.2.1.7.7.1.1.3)	シナリオに関連して生成されたキューの数を表わします。
	pfGsScenarioInformationFlowNum(1.3.6.1.4.1.1151.2.1.7.7.1.1.4)	シナリオに関連して生成されたフローの数を表わします。

MIB グループ	MIB オブジェクト名	説明
	pfGsScenarioInformation BufferPeakQid(1.3.6.1.4.1.1151.2.1.7.7.1.1.5)	バッファピークホールド値が最大のキューについて，該当するキューの QID を示します。エージングアウトなどにより現在使用されていないキューのピークホールド値が最大の場合は，0 を表示します。
	pfGsScenarioInformation BufferPeakRatio(1.3.6.1.4.1.1151.2.1.7.7.1.1.6)	バッファピークホールド値が最大のキューについて，該当するキューの最大バッファサイズに対するバッファピークホールド値の大きさを比率で表示します。単位はパーセントです。
	pfGsScenarioInformation BufferPeakSize(1.3.6.1.4.1.1151.2.1.7.7.1.1.7)	バッファピークホールド値が最大のキューについて，該当するキューのバッファピークホールド値をバイト単位で表示します。
	pfGsScenarioInformation BufferMaxQid(1.3.6.1.4.1.1151.2.1.7.7.1.1.8)	現在のバッファ使用量が最大のキューについて，該当するキューの QID を示します。
	pfGsScenarioInformation BufferMaxRatio(1.3.6.1.4.1.1151.2.1.7.7.1.1.9)	現在のバッファ使用量が最大のキューについて，該当するキューの最大バッファサイズに対するバッファ使用率をパーセントで表示します。
	pfGsScenarioInformation BufferMaxSize(1.3.6.1.4.1.1151.2.1.7.7.1.1.10)	現在のバッファ使用量が最大のキューについて，該当するキューのバッファ使用量をバイト単位で表示します。
	pfGsScenarioInformation BufferMinQid(1.3.6.1.4.1.1151.2.1.7.7.1.1.11)	現在のバッファ使用量が最小のキューについて，該当するキューの QID を示します。
	pfGsScenarioInformation BufferMinRatio(1.3.6.1.4.1.1151.2.1.7.7.1.1.12)	現在のバッファ使用量が最小のキューについて，該当するキューの最大バッファサイズに対するバッファ使用率をパーセントで表示します。
	pfGsScenarioInformation BufferMinSize(1.3.6.1.4.1.1151.2.1.7.7.1.1.13)	現在のバッファ使用量が最大のキューについて，該当するキューのバッファ使用量をバイト単位で表示します。
	pfGsScenarioInformation BufferAveRatio(1.3.6.1.4.1.1151.2.1.7.7.1.1.14)	現在のバッファ使用率の平均値を表示します。単位はパーセントです。
	pfGsScenarioInformation BufferAveSize(1.3.6.1.4.1.1151.2.1.7.7.1.1.15)	現在のバッファ使用量の平均値を表示します。単位はバイトです。
PfGsFlowInformation(1.3.6.1.4.1.1151.2.1.7.8)	PfGsFlowInformationResourceTotal(1.3.6.1.4.1.1151.2.1.7.8.1)	装置で使用可能なフロー数の総数を表示します。
	PfGsFlowInformationResourceUsed(1.3.6.1.4.1.1151.2.1.7.8.2)	装置で使用中のフロー数を表示します。
	PfGsFlowInformationResourceAvailable(1.3.6.1.4.1.1151.2.1.7.8.3)	装置で使用前のフロー数を表示します。

参考）

キューカウンタ，シナリオカウンタ，シナリオインフォメーションテーブルの OID を求める方法

テーブル内オブジェクトの OID を求めるには以下を参考にしてください。

pfGsQueueStatisticsTable の場合
pfGsQueueStatisticsEntry の OID は次のようになります。
1.3.6.1.4.1.1151.2.1.7.5.1.1.EntryOID.FilterIndex.FilterSubIndex.QueueIndex
固定値

EntryOID ：テーブル内エントリの番号です。表 4 の順序通りに 1 から並んでいます。長さは 1 です。

pfGsQueueStatisticsFilterIndex	1
pfGsQueueStatisticsFilterSubIndex	2
pfGsQueueStatisticsQueueIndex	3
pfGsQueueStatisticsFilterType	4
pfGsQueueStatisticsIfIndex	5
pfGsQueueStatisticsRxOctets	6
pfGsQueueStatisticsRxPackets	7
pfGsQueueStatisticsTxOctets	8
pfGsQueueStatisticsTxPackets	9
pfGsQueueStatisticsDiscardOctets	10
pfGsQueueStatisticsDiscardPackets	11
pfGsQueueStatisticsHCRxOctets	12
pfGsQueueStatisticsHCRxPackets	13
pfGsQueueStatisticsHCTxOctets	14
pfGsQueueStatisticsHCTxPackets	15
pfGsQueueStatisticsHCDiscardOctets	16
pfGsQueueStatisticsHCDiscardPackets	17

FilterIndex ：キューに割り当てられた IP フィルタの親フィルタ ID です。長さは 1 です。
FilterSubIndex ：キューに割り当てられた IP フィルタの子フィルタ ID です。長さは 1 です。
QueueIndex ：キューID です。長さは 1 です。キューID はシステムがキューを作る度に 1 から順に割り当てられます。このため，事前にキューID を確定することはできません。キューが作成された後に，get next で全エントリを取得するか，または CLI コマンド“show queue info”でキューID を確認してください。

pfGsScenarioStatisticsTable の場合
pfGsScenarioStatisticsEntry の OID は次のようになります。
1.3.6.1.4.1.1151.2.1.7.6.1.1.EntryOID.ScenarioIndex
固定値

EntryOID ：テーブル内エントリの番号です。表 4 の順序通りに 1 から並んでいます。長さは 1 です。

pfGsScenarioStatisticsScenarioIndex	1
pfGsScenarioStatisticsScenarioType	2
pfGsScenarioStatisticsRxOctets	3
pfGsScenarioStatisticsRxPackets	4
pfGsScenarioStatisticsTxOctets	5
pfGsScenarioStatisticsTxPackets	6
pfGsScenarioStatisticsDiscardOctets	7
pfGsScenarioStatisticsDiscardPackets	8
pfGsScenarioStatisticsHCRxOctets	9
pfGsScenarioStatisticsHCRxPackets	10
pfGsScenarioStatisticsHCTxOctets	11
pfGsScenarioStatisticsHCTxPackets	12
pfGsScenarioStatisticsHCDiscardOctets	13
pfGsScenarioStatisticsHCDiscardPackets	14

ScenarioIndex ：シナリオのシナリオ ID です。長さは 1 です。

pfGsScenarioInformationTable の場合
pfGsScenarioInformationEntry の OID は次のようになります。
1.3.6.1.4.1.1151.2.1.7.7.1.1.EntryOID.ScenarioIndex
固定値

EntryOID ：テーブル内エントリの番号です。表 4 の順序通りに 1 から並んでいます。長さは 1 です。

pfGsScenarioInformationScenarioIndex	1
pfGsScenarioInformationScenarioType	2
pfGsScenarioInformationQueueNum	3
pfGsScenarioInformationFlowNum	4
pfGsScenarioInformationBufferPeakQid	5
pfGsScenarioInformationBufferPeakRatio	6
pfGsScenarioInformationBufferPeakSize	7
pfGsScenarioInformationBufferMaxQid	8
pfGsScenarioInformationBufferMaxRatio	9
pfGsScenarioInformationBufferMaxSize	10
pfGsScenarioInformationBufferMinQid	11
pfGsScenarioInformationBufferMinRatio	12
pfGsScenarioInformationBufferMinSize	13
pfGsScenarioInformationBufferAveRatio	14
pfGsScenarioInformationBufferAveSize	15

ScenarioIndex ：シナリオのシナリオ ID です。長さは 1 です。

Anritsu

PureFlow GS1

トラフィックシェーパー

PF7000A

PF7001A

PF7010A

PF7011A

取扱説明書

コンフィギュレーションガイド

■ 製品を適切・安全にご使用いただくために，製品をご使用になる前に，本書を必ずお読みください。本書は製品とともに保管してください。

Anritsu

PureFlow GS1　トラフィックシェーパー　PF7000A　PF7001A　PF7010A　PF7011A　取扱説明書　コンフィギュレーションガイド

Anritsu

管理番号:PF-WP011AW
Printed in Japan