



sFlow



# sFlow/NetFlow & InMon TrafficSentinelのご紹介

フローマネージメントを活用した  
ネットワークの可視化と管理

丸紅情報システムズ株式会社

- フローマネージメント
- sFlow/NetFlow
- InMonTrafficSentinelのご紹介
  - ネットワーク管理
  - レポートティング機能
  - セキュリティ管理 など
- ケーススタディー
- sFlowTrend (フリー)/sFlowTrend-Proのご紹介
- インフォメーション

フローマネージメントとは

- ソースとデスティネーション間のフレームの流れを以下のような内容などを認識し分析すること
  - Source / Destination Address
  - Source / Destination Port 番号
  - Protocol
  - Interface
  - TOS ( IP type of service ) / Priority ( 802.1p )
  - VLAN (802.1Q)
  - AS番号

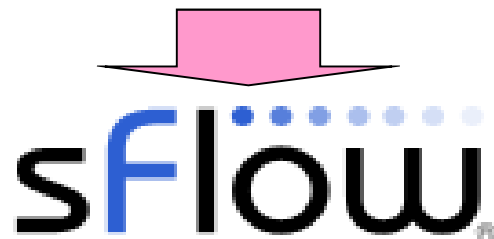
ネットワークの  
可視化

次のような分析が可能

- なぜ、ネットワークが遅いのか？
- 誰がネットワークを使っているか？誰が何をしているか？
- セキュリティ対策は出来ているか？
- SPAM・DoS攻撃・ウイルス・ワームは？
- ネットワークの使用内容は？マルチキャスト通信は、どの程度？

## ネットワークの可視化へのトラディショナルな解決法

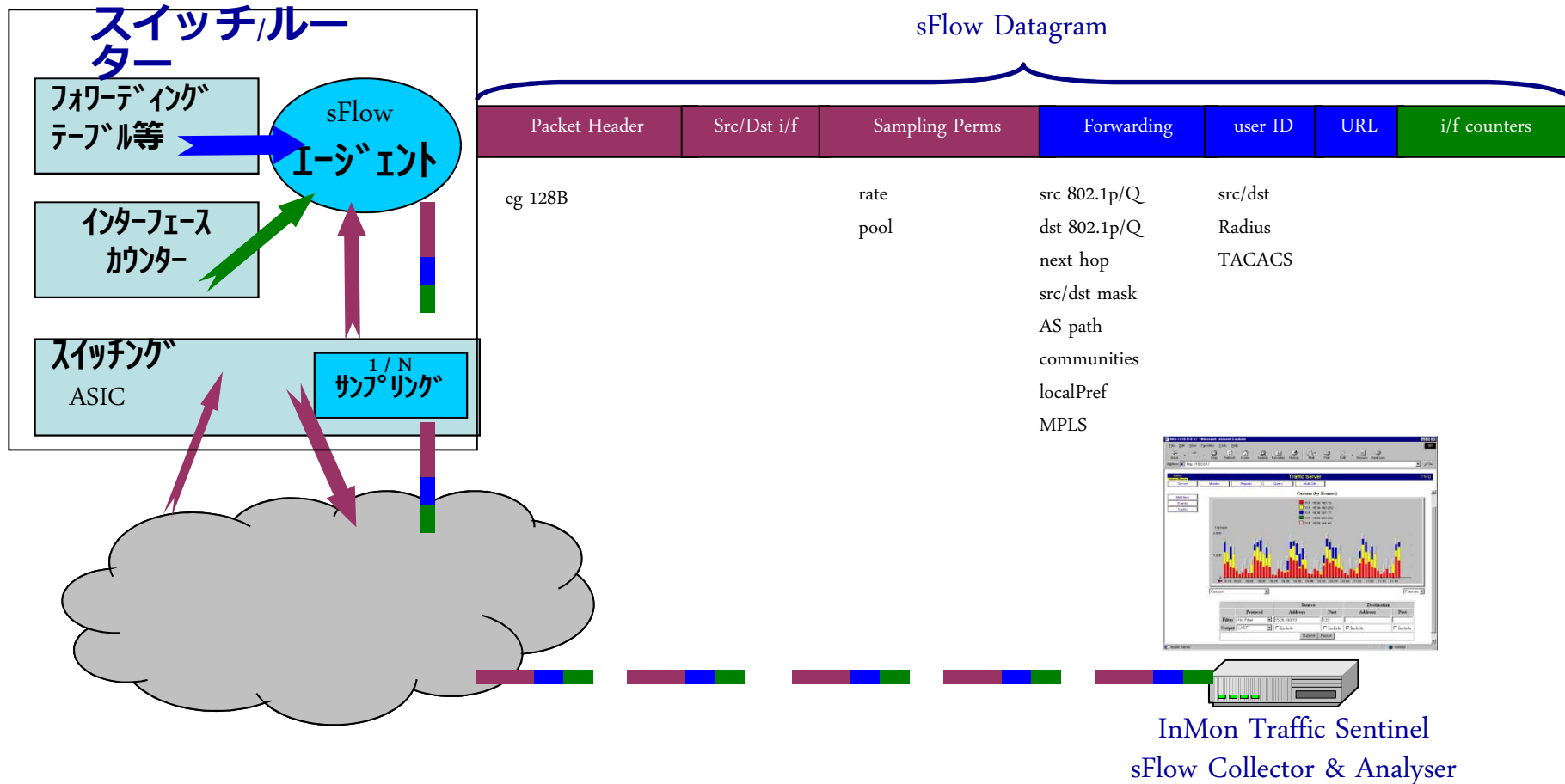
- SNMP (Simple Network Management Protocol)
  - 1988年開発以降、インターネットワーク管理のデファクトスタンダード
  - SNMPマネージャが、機器のSNMPエージェント (MIB) から統計値を収集
  - インターフェース単位のオクテット数・フレーム数などのカウンター情報を収集
  - プロトコル別情報なし
- RMON2(Remote Network Monitoring V2)
  - トラフィック内容 (プロトコル別情報など) の通信状況をモニタリング
  - RMON 2プローブが必要(ハイスピードネットワークでは非常に高価)
  - 情報としては不十分 (特定プロトコルのみの分析・リアルタイム性がない)
  - ネットワークパフォーマンスへの影響



ネットワークの可視化への次世代の解決法 → sFlowの誕生

ハイスピードネットワークにおいて、  
低コストで効果的なモニタリングを実現する新たなテクノロジー！

- 業界標準ネットワーク・トラフィック・モニタリング技術
- ネットワーク全体を可視化
  - 全てのスイッチ・全てのインターフェースを測定
- **サンプリングベース**のテクノロジー
  - スイッチやネットワークのパフォーマンスへの影響が少ない
  - ハイスピードネットワーク内のトラフィックのモニタリングに効果的
- 米国InMon社によって公開：**Open Standard – IETF RFC3176(sFlow V4)**
- ネットワーク機器埋め込み型として設計されたモニタリング・テクノロジー
  - ルータスイッチ内に実装されスイッチのASICにて処理
- スイッチの**sFlow**エージェントが**sFlow**を生成し、**sFlow**マネージャーへ即座に送信
  - MIBやキャッシュ上で保持・カウントしない
- **sFlow**対応機器であれば即座に使用可能



## sFlow Datagram



- **Flow sample (フローデータ)**
  - Packet Header : サンプルパケットのパケットヘッダー情報 (一部ペイロード含む)
  - Src/Dst i/f : 入出インターフェースのifIndex
  - Sampling Perms : sFlowパラメータ(Sampling Rate, Sampling Pool etc)
  - Forwarding
    - Priority ( Src/Dst 802.1p/TOS)
    - VLAN ( Src/Dst 802.1q)
    - Next hop address
    - Source AS, Source Peer AS
    - Destination AS Path
    - Communities, local preference
    - MPLS
  - User ID : Src/Dst RADIUS/TACACS
  - URL
- **SNMP Counter Sample (SNMP カウンター 値)**
  - i/f counters : インターフェース・カウンター・統計値



# sFlowの実装(埋め込み型sFlowエージェント)







# sFlow以外のサポートベンダー



## NetFlow系 (NetFlow/J-Flow/IPFIX) 実装メーカー



※ 各機器でのsFlowの対応状況の詳細は、ハードベンダー様へご確認下さい

- サンプルングされた情報から実際のフレーム数やバイト数を導き出す
- プロトコル別トラフィック量の計算

入力したフレームの総数 =  $N$

総サンプル数 =  $n$

そのクラス (プロトコル) でのサンプル数 =  $c$

そのクラス別のフレーム数は次式により計算 :

$$N_c = \frac{c}{n} \cdot N$$

例 :

入力したフレームの総数 = 1,000,000

サンプリングレート = 0.25%

総サンプル数 = 2,500

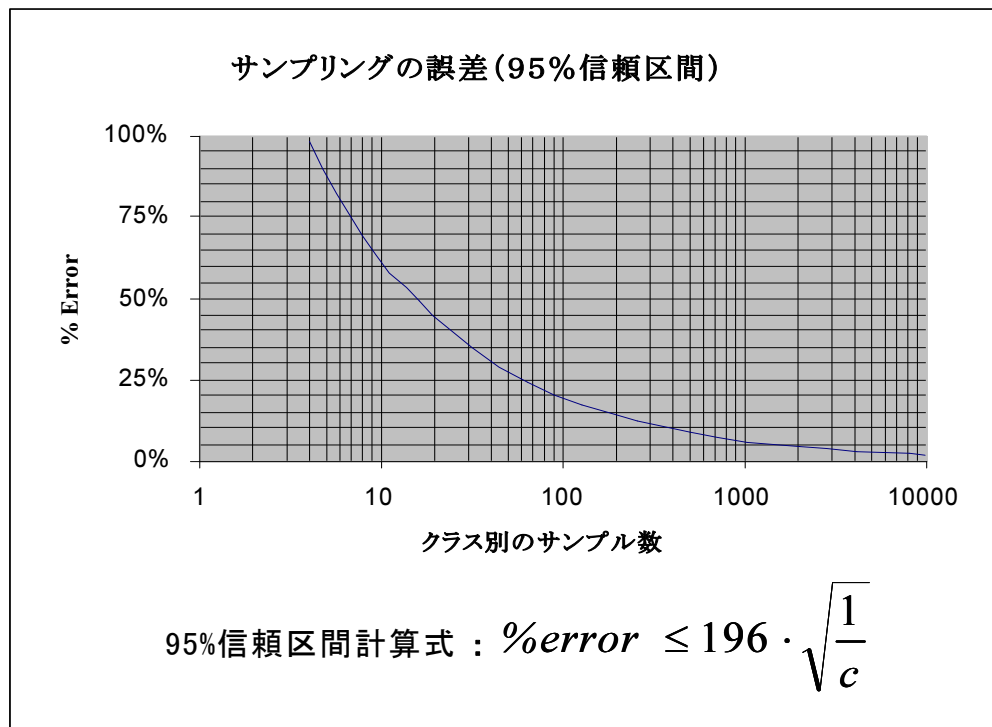
Voiceトラフィックのサンプル数 = 1,000

表示されるVoiceトラフィックのフレーム数は :

$$\frac{1,000}{2,500} \times 1,000,000 = 400,000 \quad \text{フレーム}$$

サンプリングの誤差が発生 → 統計的手法 (95%信頼区間分析) により把握

## サンプルングの誤差 → 95%信頼区間によって分析



例 : 95%の信頼区間でのエラー率を前ページの例で計算すると、Voiceトラフィックのサンプル数 = 1,000 なので、

$$\%Error \leq 196 \times \sqrt{\frac{1}{1,000}} \doteq \pm 6.2\%$$

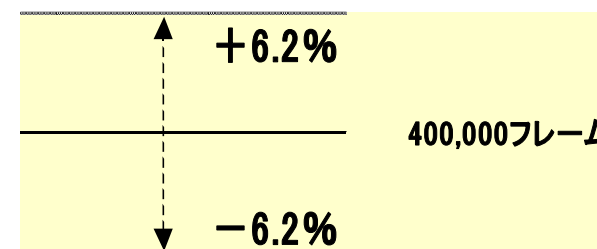
表示された“400,000 フレーム”に対し 95%信頼区間では、±6.2%が誤差になるので、区間は、

375,200フレーム(Lower)

～

424,800フレーム(Upper)

となる。



- 誤差とトラフィックはトレードオフの関係  
(トラフィック=分析対象トラフィック)
  - トラフィックが多い→誤差は少ない / トラフィックが少ない → 誤差は大きい
- 誤差を少なくするには？
  - 対象となるフローを増加 ( サンプルングレートを上げる？分析対象期間を延ばす？ )
- 誤差を少なくする分析
  - トラフィックが多い場合：通常のサーバーアクセス (HTTP通信など)、DoS攻撃  
→ トラフィックが多いので、**リアルタイムでも誤差は少ない**
  - トラフィックが少ない場合：使用頻度・通信量の少ない通信 (チャット通信など)  
→ トラフィックが少ないので、リアルタイムでは誤差が大きい  
→ 対象期間を延ばす (“分”から“時間”, “日”, “週”, “月”へ) と対象トラフィックが多くなるので、誤差が少なくなる
  - サンプルング分析のコンセプト
    - メジャーなトラフィックは、誤差が少なく、リアルタイム性も保たれる
    - マイナーなトラフィックは、対象期間を延ばし、誤差を低減
    - スイッチ・パフォーマンス、ネットワーク・パフォーマンスの悪化を防ぐ
- サンプルングベースのテクノロジーの為、1G/10Gネットワークから更なるハイスピードネットワークへの対応が可能

- **ワイヤレスネットワーク向けsFlow**

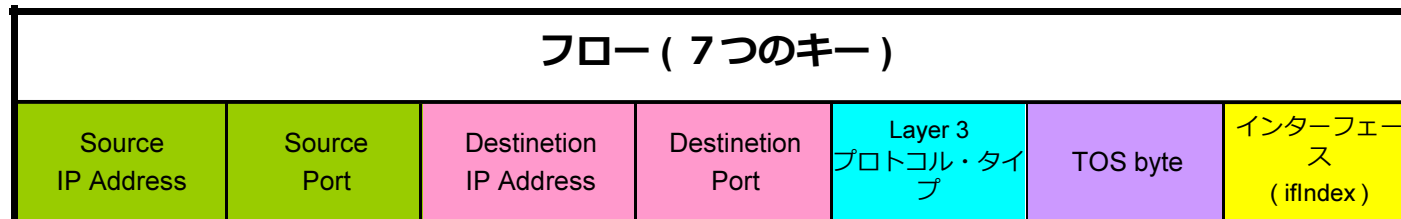
- sFlowを使用してワイヤレスネットワークをモニタリングする規格 (2007年4月)
- 802.11ワイヤレス・トラフィック上のデータを分析しフロー化
  - WAP (ワイヤレスアクセスポイント) 別
  - RADIO別
  - SSID/チャンネル別
  - Air Utilization% (802.11gの54Mbpsに対してなど)
  - ワイヤレス・バージョン (802.11a/b/g/n)
  - 暗号方式 (TKIP/WEP/CCMP etc)
  - カウンター値
    - Fragments/Multicasts/RTS/Error/Station数/QoS
- sFlow802.11サポート機器
  - HP ProCurve Wireless Edge Services xl Module / WESM zl module

困難だったワイヤレス・トラフィックの可視化が可能に



- Cisco NetFlow → Ciscoが開発した技術
  - ネットワーク上のIP フローについてネットワーク管理者が情報収集する手段を提供
  - エクスポートされたNetFlow データは、ネットワークの管理やプランニング、課金、攻撃対策、データマイニングなど、様々な用途に利用可能
  - NetFlow が出力する基本データは、「フローレコード」と呼ばれる
  - バージョン1,5,7,8,9が存在
  - バージョン9は、RFC3954として公開
  - 一般的には、全てのポートをモニターするのではなく、特定のポートをモニター
- キャッシュ・ベースのテクノロジー（キャッシュ上でフローをカウント）
- L3以上のトラフィックの分析が可能（L2の分析（MACアドレスなど）は不可）
- NetFlowは、フローとして集計された情報として送られる
  - マネジャー側でフロー情報化する必要がない
- パフォーマンス上に問題がある場合は、サンプリング・テクノロジーを使用した“Sampled NetFlow”も用意されている
  - Sampled NetFlow 機能を使用すれば、ルータに転送される「x」個のIP パケットごとに1個のパケットをサンプリングできます。サンプリングパケットは、ルータのNetFlow フローキャッシュに取り込まれます。このサンプリングパケットにより、大多数のパケットに対してNetFlow 用の追加処理が不要となるので、スイッチング処理がより高速に行えるようになり、NetFlow パケットの処理に要するCPU 使用率を大幅に低減できます。（「Ciscoマニュアルより」抜粋）

- フロー
  - 以下の図の内容を、フローとして、統計値（フレーム数・バイト数）を NetFlow キャッシュ内でカウント
  - NetFlow キャッシュ内で保持・カウントしている情報を、特定のタイミング（条件）でエクスポート



- フローをエクスポートするタイミング
  - インアクティブ・タイマー（デフォルト：15秒）
    - 該当のフローセットのセッションが15秒間インアクティブ（無音）の時、エクスポート
    - コマンド " ip flow-cache timeout inactive 15 " で設定
  - アクティブ・タイマー（デフォルト：30分）
    - 該当のフローセットのセッションが継続している場合、30分経過時点で、エクスポート
    - コマンド " ip flow-cache timeout active 30 " で設定
  - TCPコネクションのRSTやFINフラグの検出
  - NetFlowキャッシュがフル

- sFlow
  - RFC3176として公開（機器ベンダ非依存のオープンな規格）
  - サンプルングベース
  - 対象レイヤー：L2-L7+Payload
  - 高速スイッチングネットワークの測定を目的に開発
    - WANのモニタリング（BGP AS path 分析）
  - 全インターフェースをモニター
  - AS分析(OriginAS/SourcePeerAS/DestPeerAS/DestinationAS Path)
- NetFlow
  - RFC3954として公開（Cisco色が強い）
  - キャッシュベース
  - 対象レイヤー：L3-L4
  - WANリンクの測定が主たる目的としてリリース
    - LANのモニタリング（CatalystへのNetFlowの実装）
  - 特定のインターフォース(VLAN)をモニター
  - AS分析（SourcePeerAS/DestPeerAS）



## Complete Network Visibility and Control - InMonTrafficSentinelによる完全なるネットワークの視覚化と管理 -

InMonTrafficSentinelは、sFlowをIETFでRFC3176として公開したInMon社が開発したsFlowマネージャーです。  
ネットワーク全体に対するネットワーク・トラフィックの常時監視と分析が可能となります。

データソースとして、

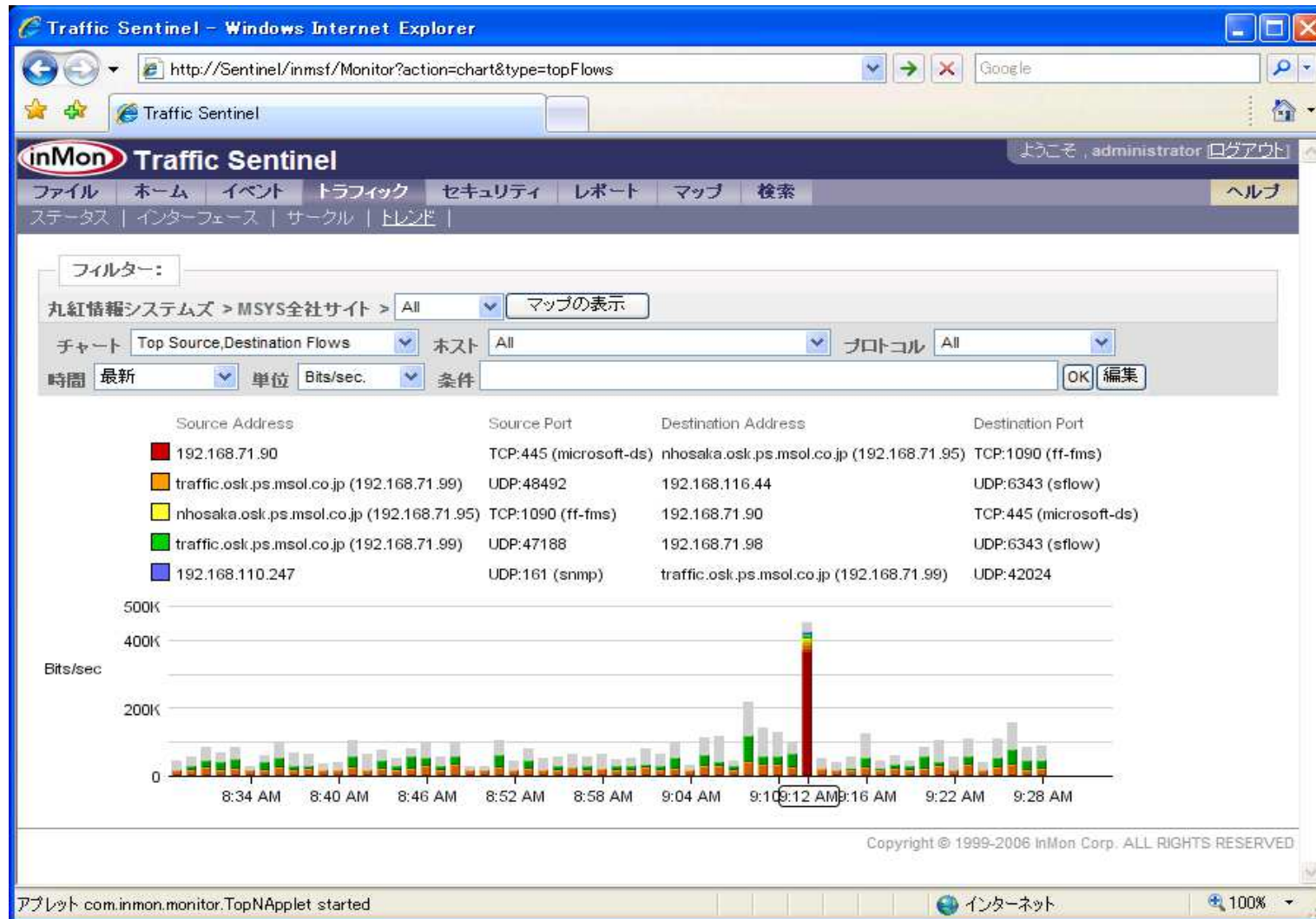
**sFlow/NetFlow/J-Flow/XRMON/LFAP/IPFIX/SNMP**

を、サポートしています。

### InMonTrafficSentinelの各種機能

- 日本語版の提供
- ネットワーク管理
- レポート機能
- セキュリティ管理
- ダッシュボード機能

InMon Traffic Sentinelのオペレーション画面、マニュアルは日本語となっています



## 1. プロアクティブな問題の把握（しきい値分析）

The screenshot shows the inMon Traffic Sentinel interface in a Windows Internet Explorer browser. The main content area displays a grid of traffic metrics for various locations in San Francisco. The locations listed are: サイト, サマリー, Core, Data Center, Embarcadero, Financial District, Marina, Noe Valley, SOMA, and Sunset. Each location has a row of colored squares representing different metrics: Status, Frames, Utilization, Broadcasts, Multicasts, Errors, and Discards. The 'Embarcadero' row shows a red square under the 'Utilization' column, indicating a threshold breach. A black arrow points from the text 'しきい値超過 アラート' (Threshold Exceeded Alert) to this red square.

しきい値超過  
アラート

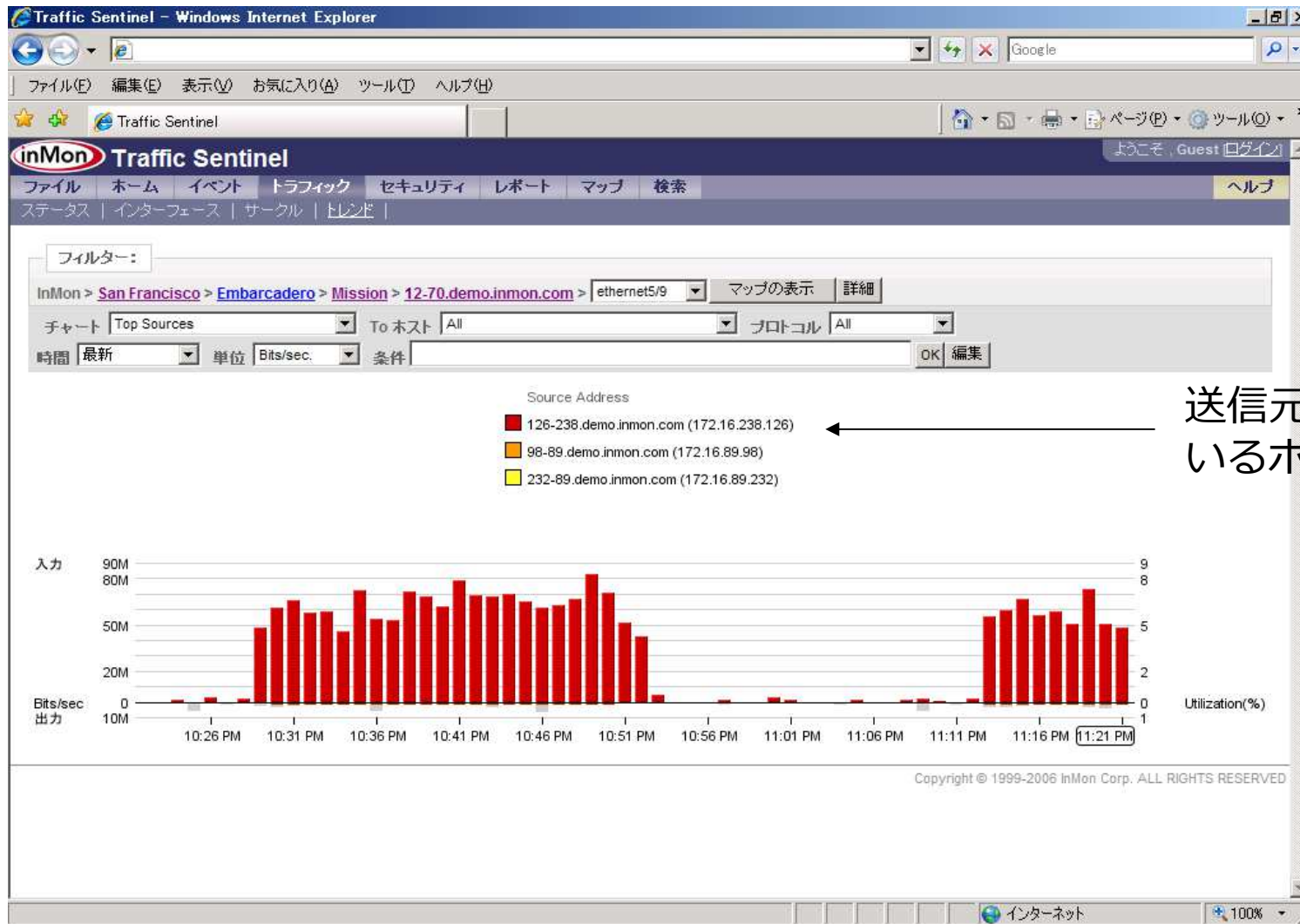
## 2. 問題が発生してインターフェースはどこか？

問題の指摘

The screenshot shows the Traffic Sentinel web interface. The main table displays network interface status for various agents. The 'Utilization' column shows a red bar for the 'ethernet5/9' interface, indicating a problem. An arrow points from the text '問題の指摘' to this red bar.

ステータス						インターフェース		
Frames	Utilization	Broadcasts	Multicasts	Errors	Discards	エージェント	インターフェース	ifSpeed
						12-70.demo.inmon.com	ethernet5/9	1Gb/sec
						10-70.demo.inmon.com	ethernet2/3	10Mb/sec
						29-70.demo.inmon.com	ethernet8	100Mb/sec
						12-70.demo.inmon.com	ethernet1/1	1Gb/sec
						12-70.demo.inmon.com	ethernet3/5	1Gb/sec
						11-70.demo.inmon.com	ethernet1/1	1Gb/sec
						14-70.demo.inmon.com	ethernet39	100Mb/sec
						22-70.demo.inmon.com	ethernet43	100Mb/sec
						11-70.demo.inmon.com	ethernet3/2	1Gb/sec
						11-70.demo.inmon.com	ethernet12/14	100Mb/sec

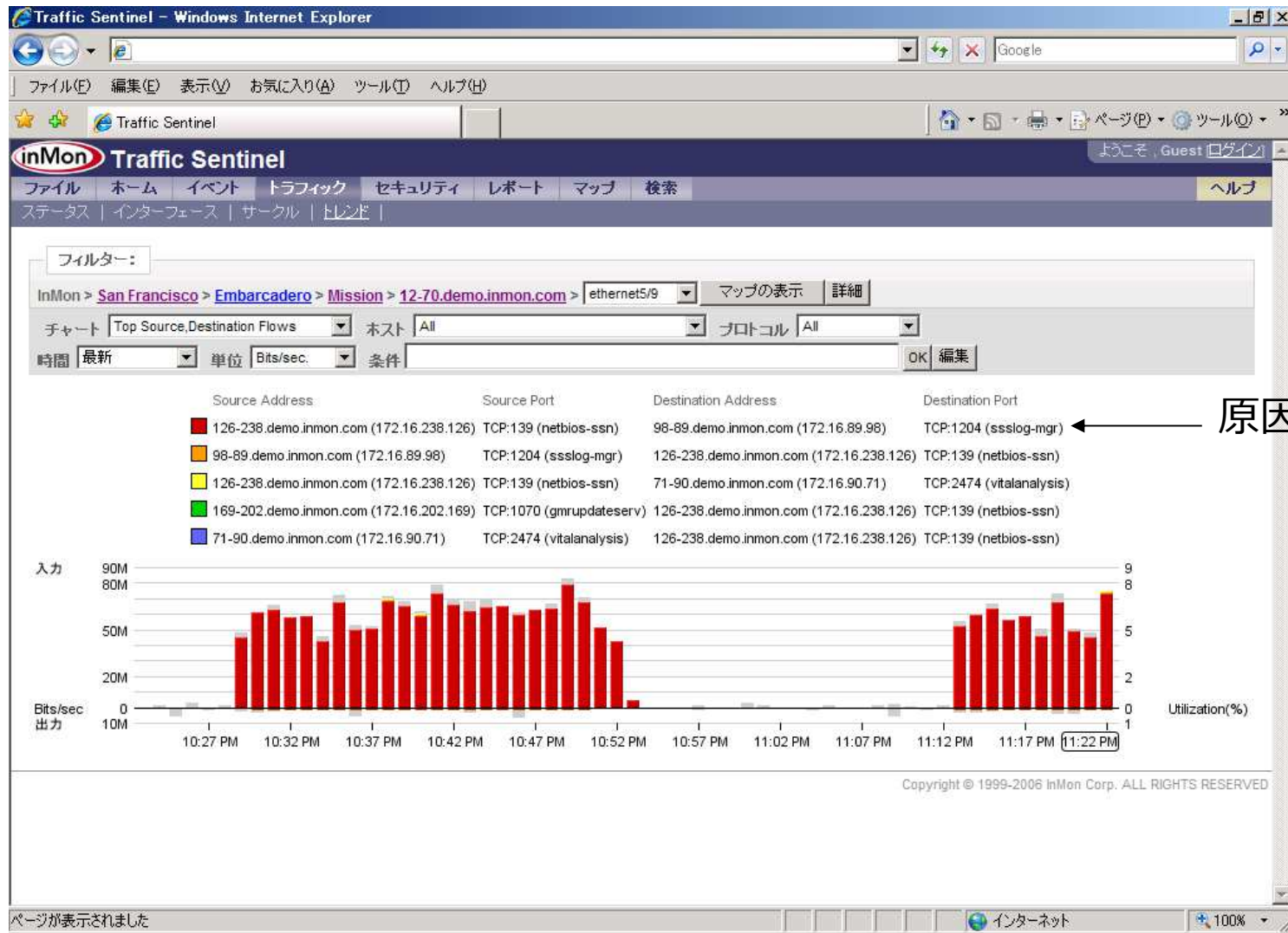
## 3. 問題を起こしているホストは誰か？



送信元となっ  
ているホスト



## 4. どのような通信をしているか？（トラフィックフローの把握）



## 5. トラフィックフローの詳細や経路情報の把握

特定したトラフィックでの経路情報

172.16.238.126 -> 172.16.89.98

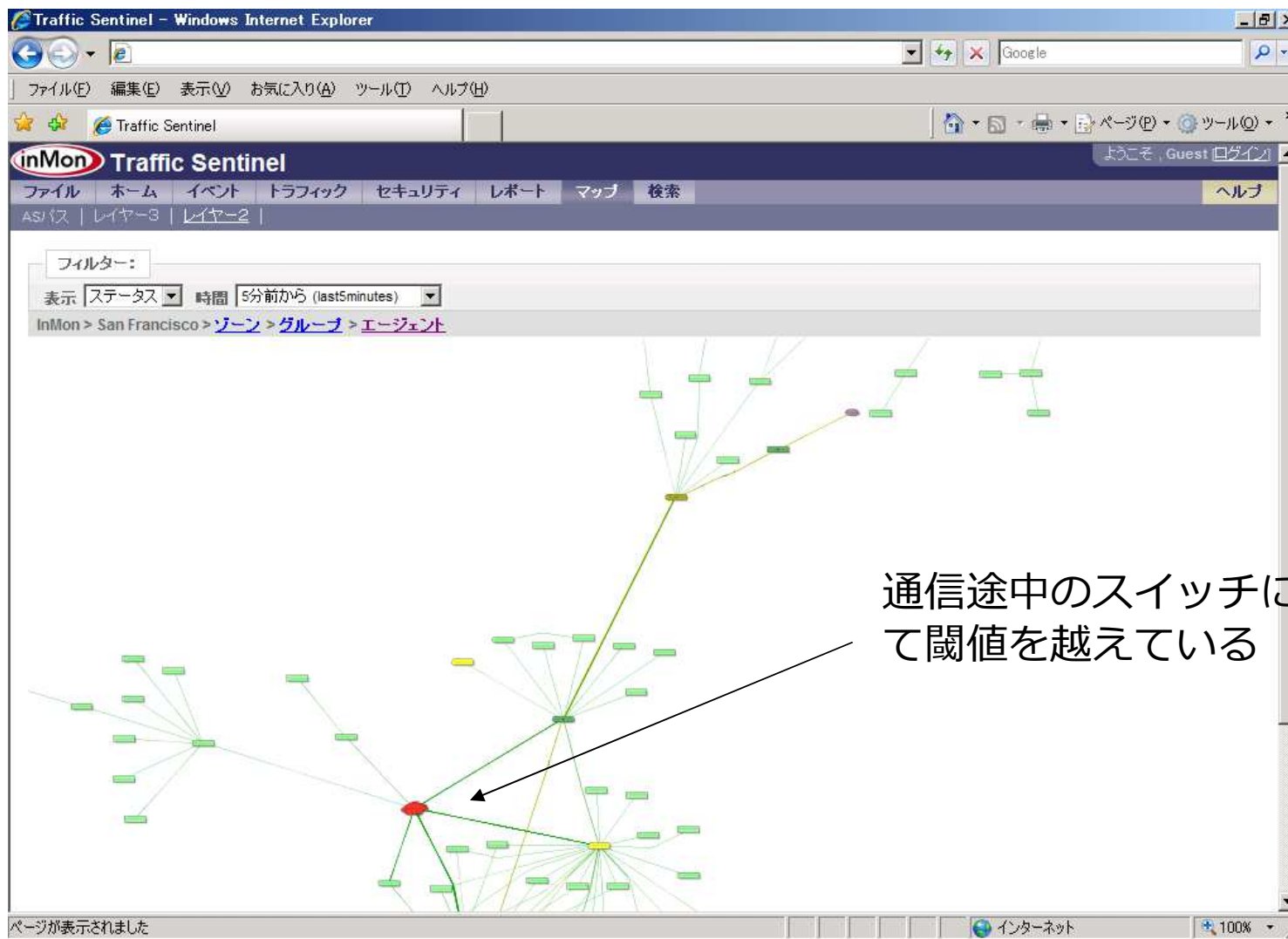
Agent	I/F In	I/F Out	MAC Source	MAC Destination	VLAN In	VLAN Out	Priority In	Priority Out	IP TOS	IP TTL
<a href="#">12-70.demo.inmon.com</a>	<a href="#">ethernet5/9</a>	<a href="#">ethernet1/1</a>	<a href="#">000802E6AAA0</a>	<a href="#">02E0520189EE</a>	682	682	0	0	0	128
<a href="#">9-9.demo.inmon.com</a>	<a href="#">ethernet7/3</a>	<a href="#">ethernet1/1</a>	<a href="#">000802E6AAA0</a>	<a href="#">02E05200C105</a>	400	400	0	0	0	128
<a href="#">4-9.demo.inmon.com</a>	<a href="#">903</a>	<a href="#">835</a>	<a href="#">000480F54600</a>	<a href="#">001279C2DA39</a>	381	381	0	0	0	127

172.16.89.98 -> 172.16.238.126

Agent	I/F In	I/F Out	MAC Source	MAC Destination	VLAN In	VLAN Out	Priority In	Priority Out	IP TOS	IP TTL
<a href="#">4-9.demo.inmon.com</a>	<a href="#">835</a>	<a href="#">903</a>	<a href="#">001279C2DA39</a>	<a href="#">02E052004605</a>	400	400	0	0	0	128
<a href="#">9-9.demo.inmon.com</a>	<a href="#">ethernet1/1</a>	<a href="#">ethernet7/3</a>	<a href="#">000480F1C100</a>	<a href="#">000802E6AAA0</a>	682	682	0	0	0	127
<a href="#">12-70.demo.inmon.com</a>	<a href="#">ethernet1/1</a>	<a href="#">ethernet5/9</a>	<a href="#">000480F54600</a>	<a href="#">000802E6AAA0</a>	682	682	0	0	0	126

Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

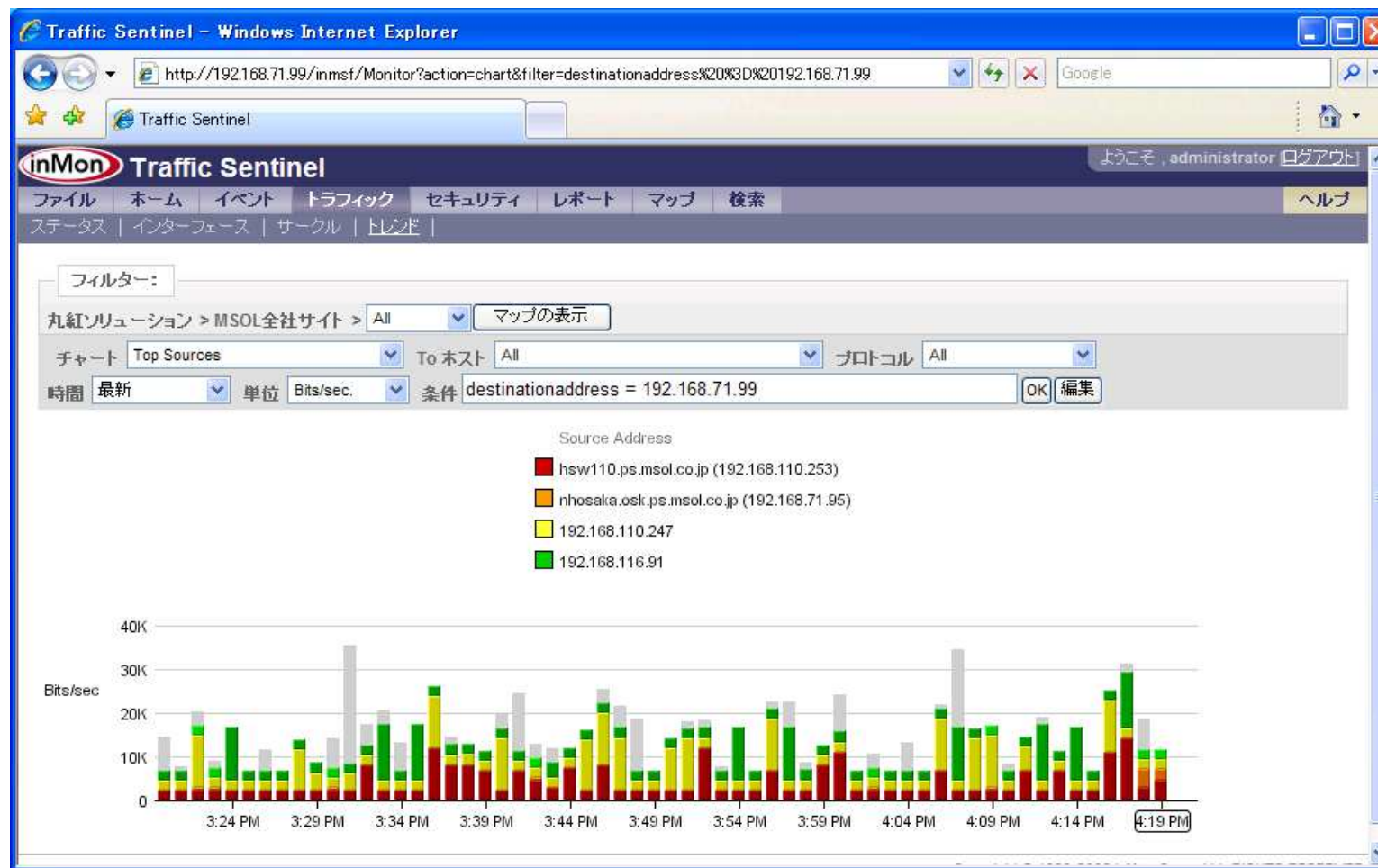
## 6. トポロジーマップ上での把握（経路情報）



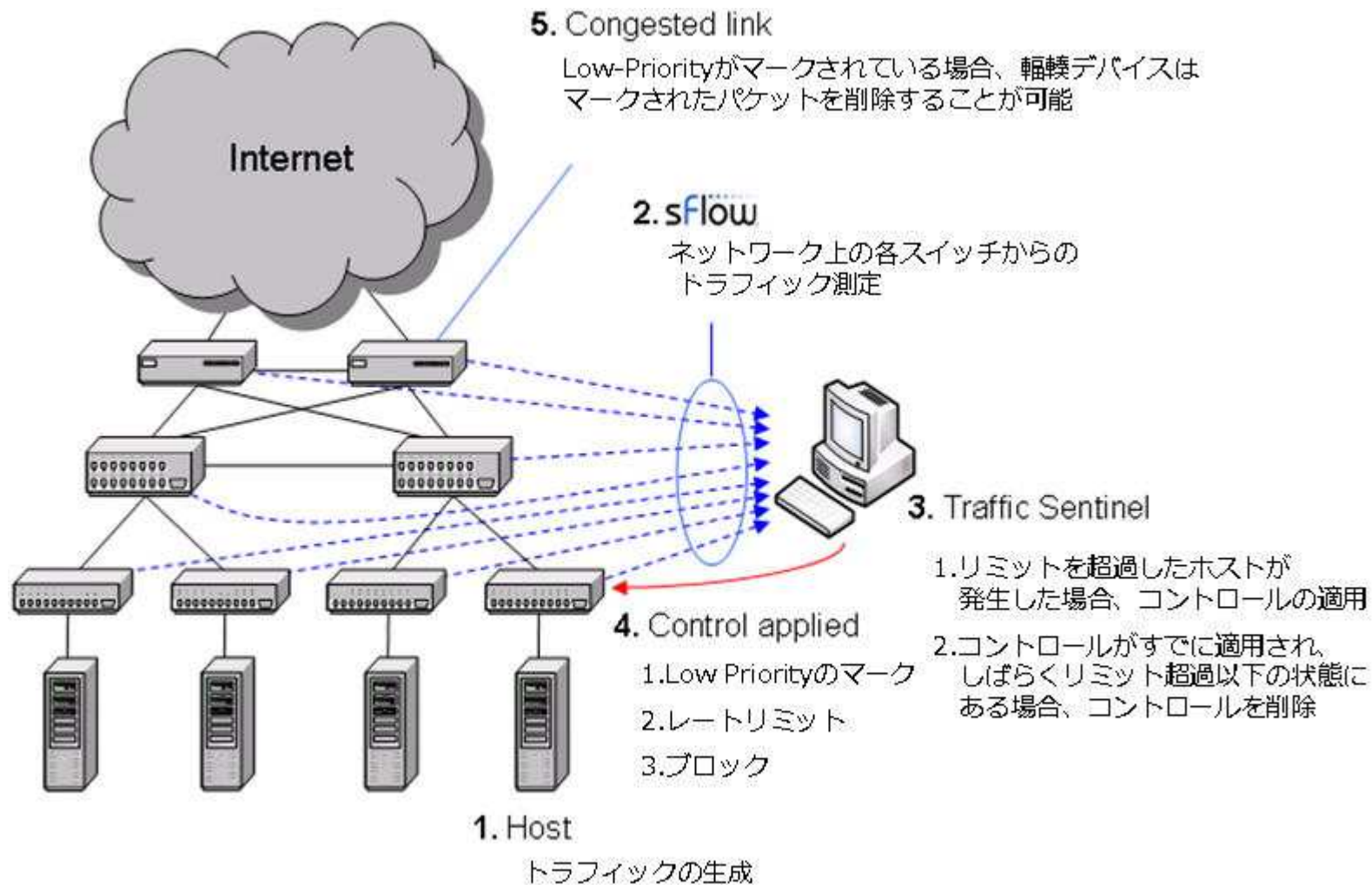


特定のサーバーへのアクセス状況の確認

特定サーバーへのレスポンスタイムが悪化している時に、アクセスしているユーザの状況を確認。サーバー(192.168.71.99)へアクセスするユーザ・グループ。



コントローラーでは、トラフィック測定を根拠とした自動的にプライオリティ・レートリミット・ブロックコントロールを適用します。

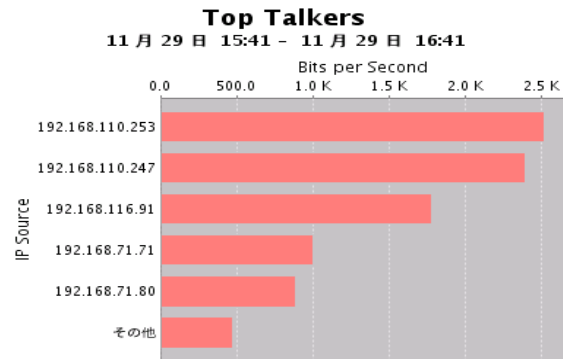


## 豊富なレポートテンプレートからのレポート作成・スケジュールレポート作成

### 部門別トップ・ユーザ・レポート

#### Recent Traffic Top N Chart

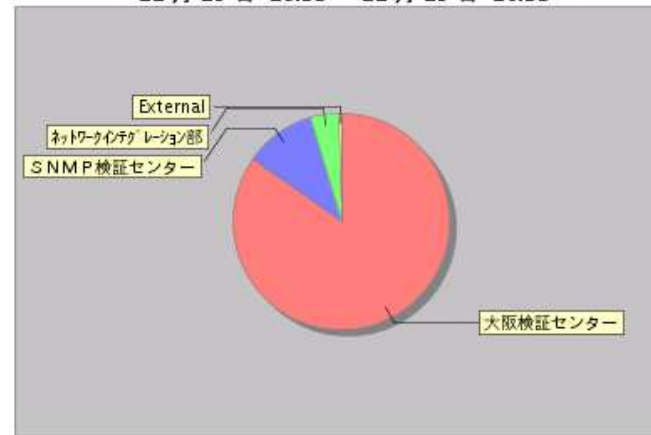
インターフェース上のトラフィックの最新の統計をプロット



[TXT](#) | [HTML](#) | [イメージ](#)

#### Top Talkers

11月29日 15:33 - 11月29日 16:33



### アカウントティング・レポート

#### Recent Traffic Totals by Time

期間別集約されたインターフェース上の最新トップトーカーを表示するテーブル

時間	Source Group	Bytes
07/11/29 15:35	SNMP検証センター	345.792 K
07/11/29 15:35	ネットワークインテグレーション部	96.000 K
07/11/29 15:35	大阪検証センター	11.264 K
07/11/29 15:40	SNMP検証センター	193.216 K
07/11/29 15:40	大阪検証センター	166.720 K
07/11/29 15:40	ネットワークインテグレーション部	26.752 K
07/11/29 15:45	SNMP検証センター	322.944 K
07/11/29 15:45	External	89.472 K
07/11/29 15:45	大阪検証センター	56.320 K
07/11/29 15:45	ネットワークインテグレーション部	12.800 K
07/11/29 15:50	SNMP検証センター	248.448 K
07/11/29 15:50	ネットワークインテグレーション部	89.984 K
07/11/29 15:50	大阪検証センター	27.840 K
07/11/29 15:55	SNMP検証センター	197.760 K
07/11/29 15:55	ネットワークインテグレーション部	96.896 K

- トラフィックの内容に対ししきい値を設定し超過時にイベントを発生させる
  - しきい値：トラフィック（プロトコル・アドレス・グループなど）に対して設定
  - スケジュール化し、超過時にイベントを発生させる

inMon Traffic Sentinel

ようこそ administrator ログアウト

ファイル ホーム イベント トラフィック セキュリティ レポート マップ 検索

表示 | クエリ | 編集 | スケジュール | インストール | スクリプト |

フィルター:

カテゴリ Miscellaneous セクション Detect Report - MSYS

Detect Report - MSYS

セクション DoS攻撃検知レポート

説明 ICMP ECHOを10,000フレーム/秒受信する大阪支

キーの選択 time.destinationaddress.ipprotocol

値 fps

期間 last5minutes

グループ 5

名前解決 no

条件 (オプション) ipprotocol=IP:1 & destinationzone = 大阪支店

しきい値 10000

例：拠点内のサーバーでICMP ECHOを10,000フレーム/秒受信した場合にDoS攻撃と判断しイベントを発生し、レポートを作成する。

Traffic Sentinel

DoS攻撃検知レポート

ICMP ECHOを10,000フレーム/秒受信する大阪支店のサーバーを表示

時間	Destination Address	IP Protocol	fps
07/12/13 13:00	traffic.osk.ps.msol.co.jp	IP:1 (ICMP)	51.587
07/12/13 13:00	pixy.osk.ps.msol.co.jp	IP:1 (ICMP)	10.073

インターネットページが表示されました

マイコンピュータ

100%

- 豊富なテンプレートを編集して、カスタマイズ・レポートが作成可能
  - 文言・表示情報・表示情報のフィルタリングなどの編集が可能
  - 定型レポートはスケジュール化

The screenshot displays the inMon Traffic Sentinel interface. The left pane shows the configuration for a custom report titled 'カスタマイズ・ヒストリカル・レポート' (Custom Historical Report). The report description is '昨日の上位使用者を表示(丸紅情報システムズ大阪支店)' (Display top users of yesterday (Marubeni Information Systems Osaka Branch)). The configuration includes:
 

- Section: カスタマイズ・ヒストリカル・レポート
- Description: 昨日の上位使用者を表示(丸紅情報システムズ大阪支店)
- Key Selection: ipsource (IP Source)
- Value: Bits per Second
- Display Count: 10
- Period: yesterday (昨日)
- Name Resolution: Yes
- Previous Rank Display: No
- Condition (Option): sourcezone = 大阪支店

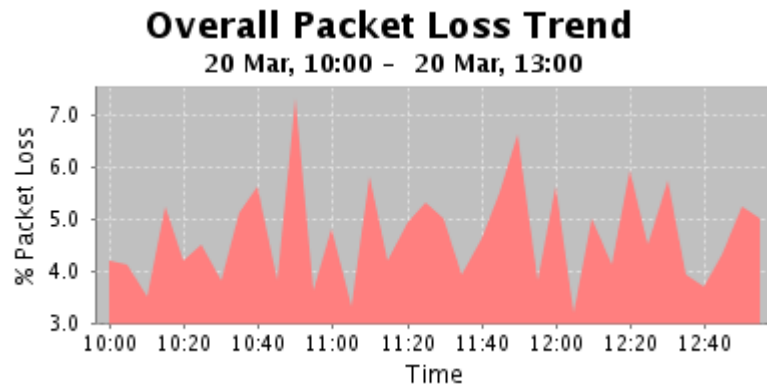
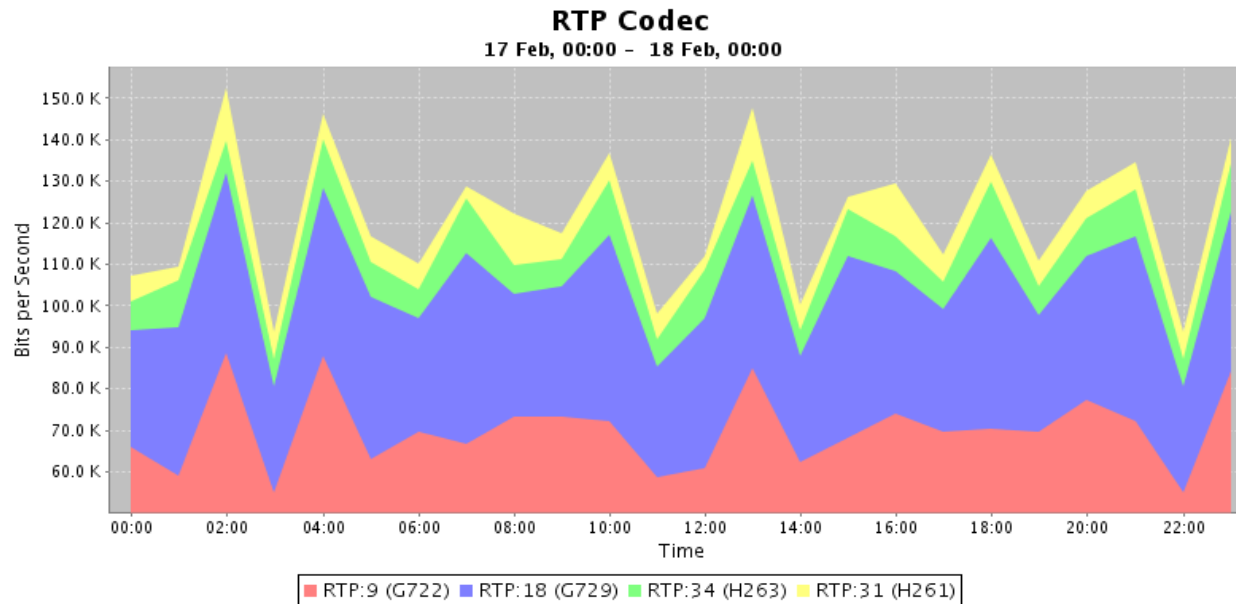
The right pane shows the report results for 'カスタマイズ・ヒストリカル・レポート' for the period '昨日の上位使用者を表示(丸紅情報システムズ大阪支店)'. The results are displayed in a table with two columns: IP Source and Bits per Second.

IP Source	Bits per Second
traffic.osk.ps.msol.co.jp	79.210 K
nhosaka.osk.ps.msol.co.jp	11.130 K
192.168.71.90	2.728 K
bs350t.osk.ps.msol.co.jp	1.277 K
192.168.71.75	974.704
justice.osk.ps.msol.co.jp	612.288
192.168.71.98	586.584
192.168.71.54	177.184
pixy.osk.ps.msol.co.jp	137.624
nhserver.osk.ps.msol.co.jp	127.328
	322.064

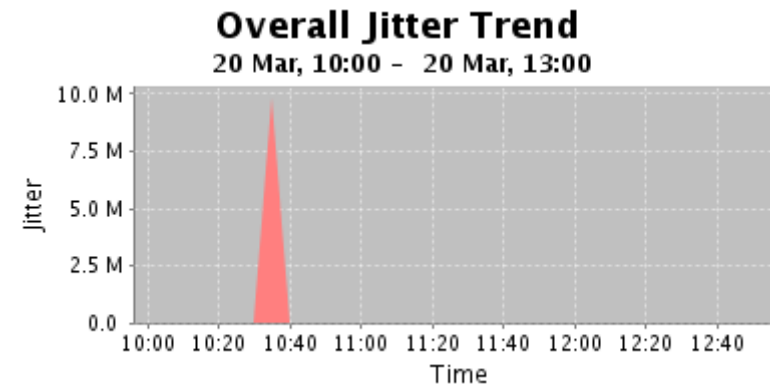
The interface also shows a navigation menu at the top with options like 'ファイル', 'ホーム', 'イベント', 'トラフィック', 'セキュリティ', 'レポート', 'マップ', and '検索'. The footer includes 'Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED' and a status bar with 'ページが表示されました' and 'インターネット'.



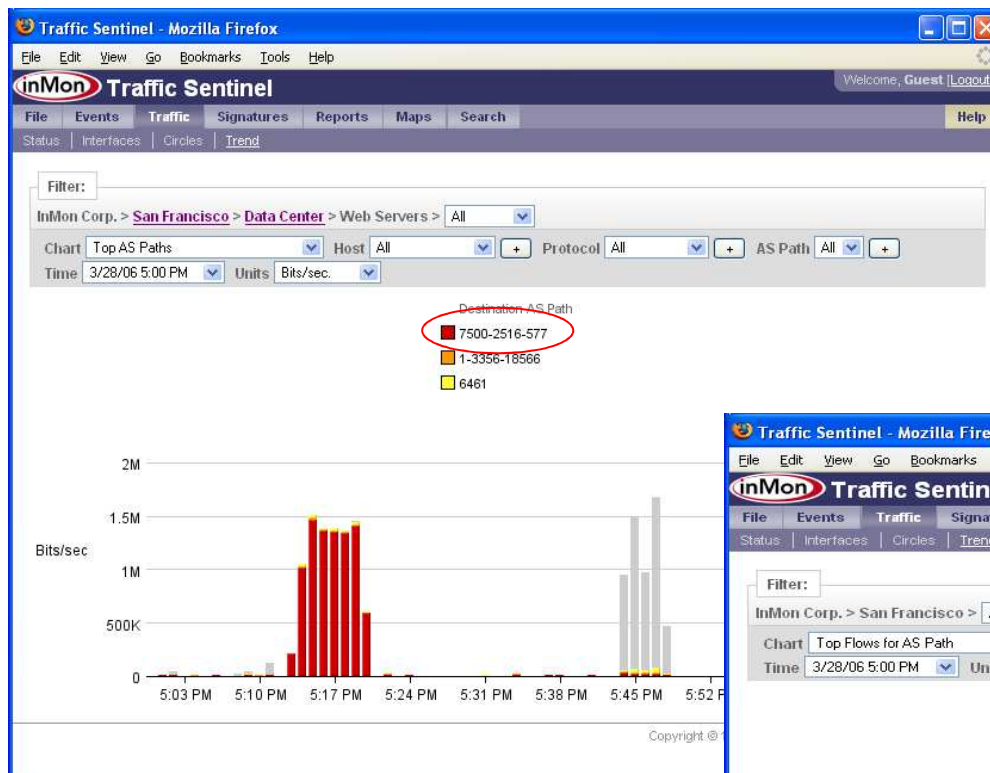
VoIPは、RTPによって提供されます。  
sFlowによってRTPのCodec、QoSの把握が可能です。



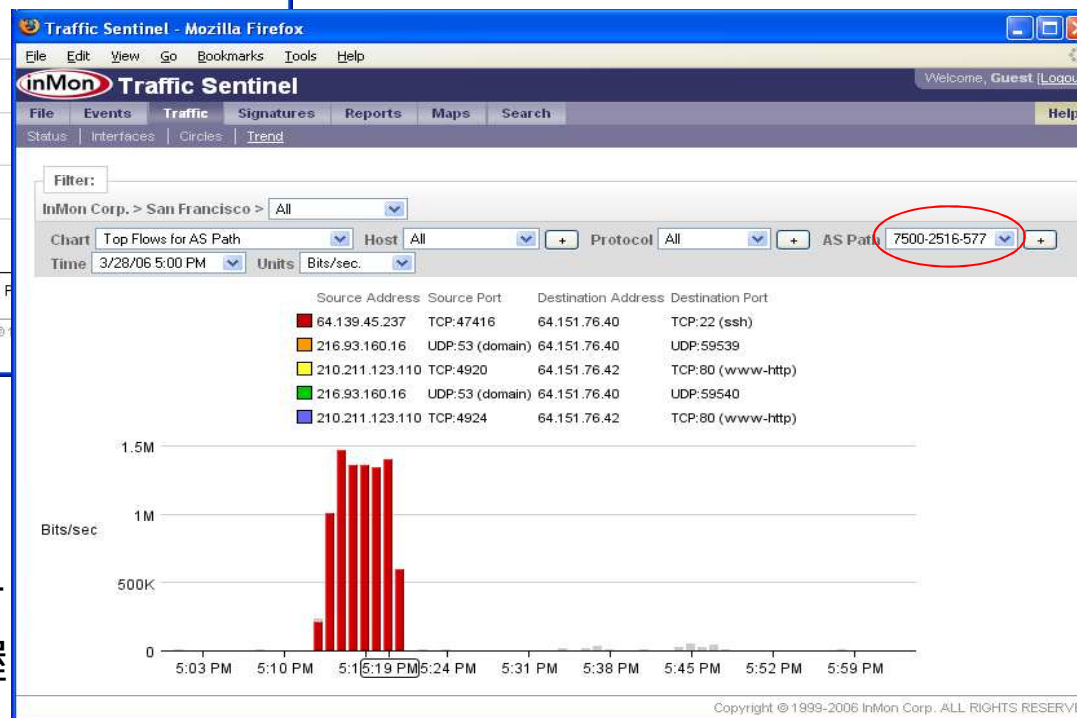
Packet loss は、均一的に継続。



しかし、Jitterは10:35にスパイ 30

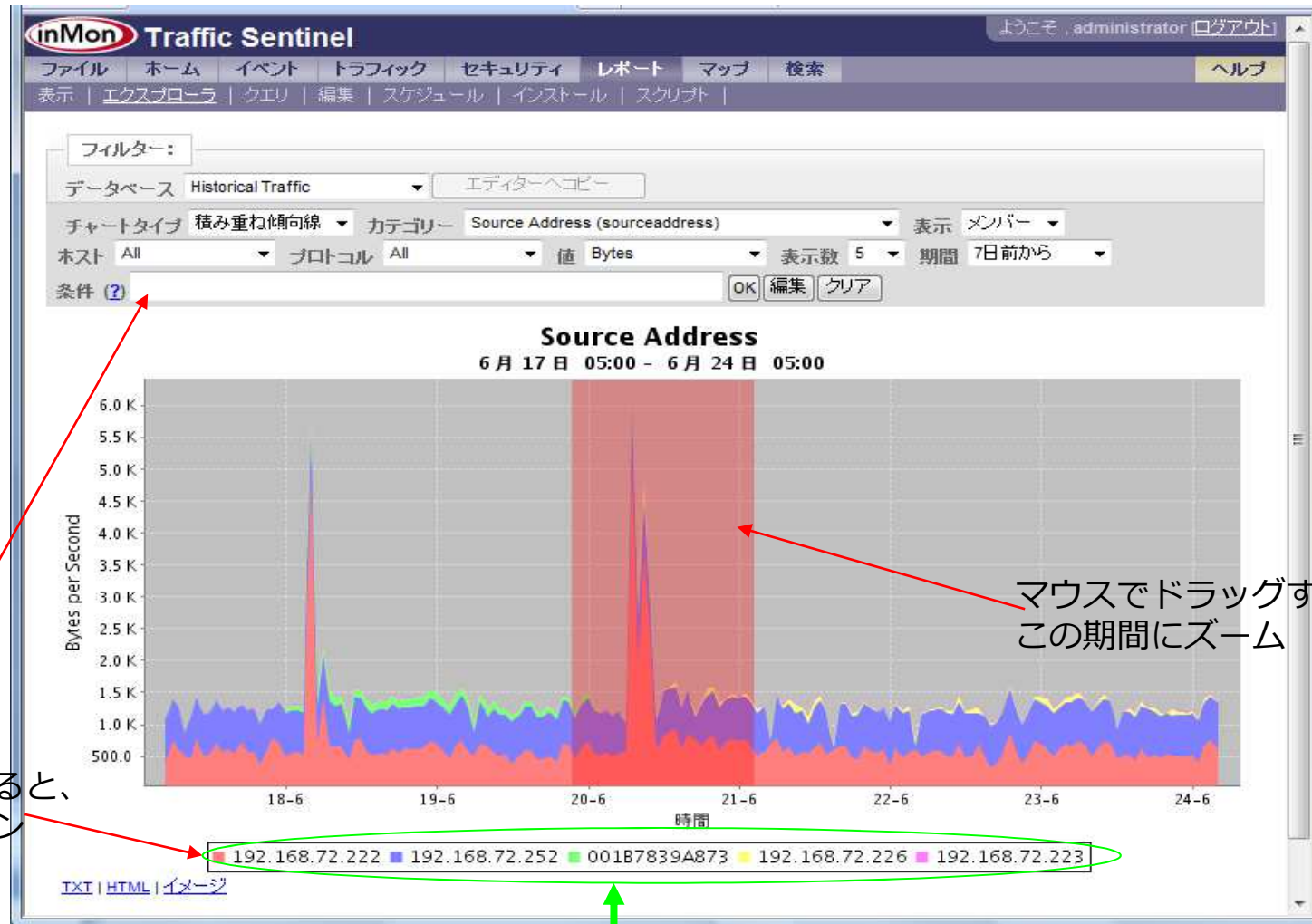


7500-2516-577 は、最も激しく使用されているASパスで、また、パスも長い。



このASパスによって転送されているフローの把握

インタラクティブにヒストリカルデータに対するトラフィック分析が可能



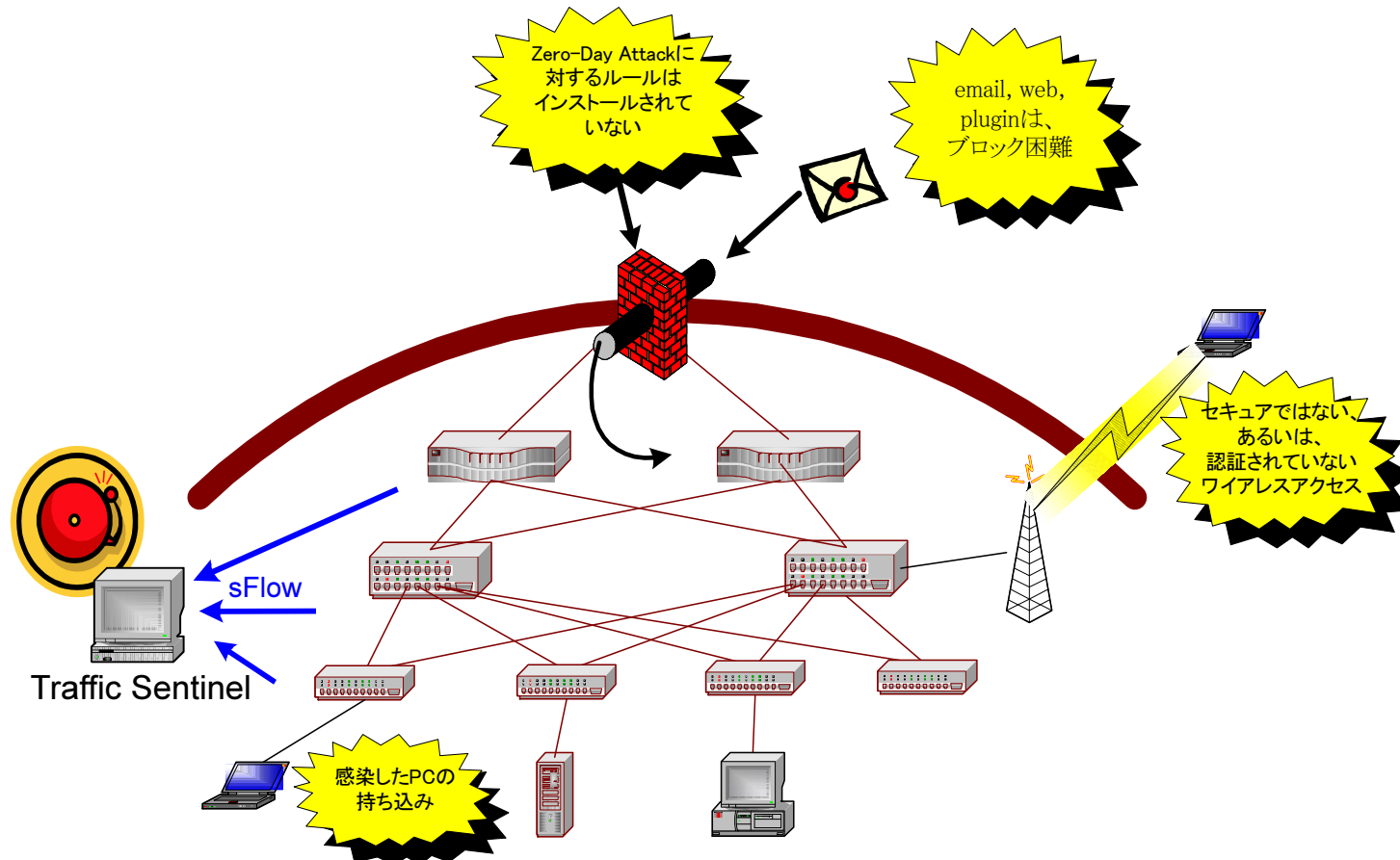
凡例をクリックすると、  
条件（フィルタリング）  
に追加

マウスでドラッグすると、  
この期間にズーム

アドレス・サブネット・拠点などで積み重ねチャート等をインタラクティブに表示



## sFlowとTrafficSentinelは内部のセキュリティを確保



ネットワーク上に配置されたsFlow実装スイッチから送られてくるsFlowデータを分析しワーム・ウイルスを検知したり、異常なトラフィックパターンを識別

## sFlow データグラム



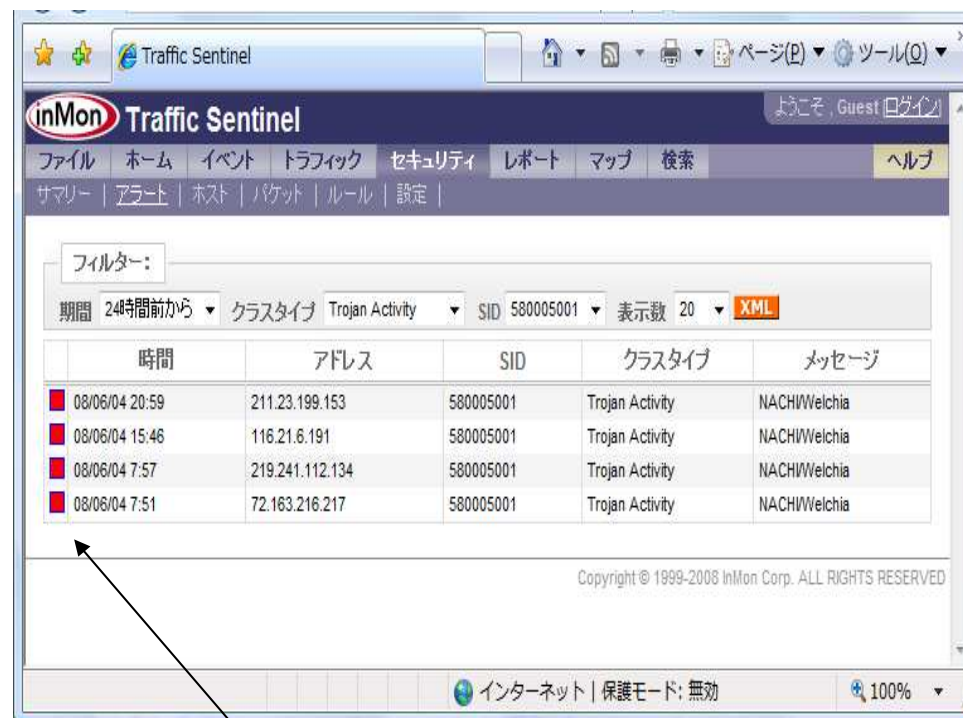
## Snort 構文で指定されたシグネチャとのマッチング

NACHI/Welchia

ネットワーク型トロイの検出

```

=====
alert icmp $EXTERNAL_NET any -> $HOME_NET
any ¥
(¥
  msg: "NACHI/Welchia";¥
  content: "|aaaa aaaa aaaa aaaa aaaa aaaa aaaa
  aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa|";¥
  dsize:64;¥
  itype: 8;¥
  icode: 0;¥
  classtype:trojan-activity;¥
  sid: 580005001;¥
  rev: 1;¥
)
=====
  
```



トラフィックがルールにマッチした時、アラートを発生

ポリシー違反：ネットワークの不正使用の検知（CHAT、P2P、VPNなど）  
SNORTシグネチャーによるポリシー違反の検知



The screenshot shows the Traffic Sentinel web interface in Microsoft Internet Explorer. The interface displays a list of detected policy violations. The table below represents the data shown in the screenshot.

時間	アドレス	SID	クラスタイプ	メッセージ
06/07/12 10:04	203.141.42.73	2457	Policy Violation	CHAT Yahoo IM message
06/07/12 9:54	192.168.71.96	20000002	Policy Violation	WinMX Download file
06/07/12 9:52	192.168.71.96	20000004	Policy Violation	WINNY Port TCP/7743
06/07/12 9:51	192.168.71.94	20000001	Policy Violation	SoftEther VPN 2.0 Connection SSL

Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

検知の為のシグネチャー例（SoftEther）：

```
alert tcp any any -> any any (msg:"SoftEther VPN 2.0 Connection"; content:"SE-VPN2-PROTOCOL"; sid: 10000014;)
```

※ 上記で検知されているポリシー違反の内容については、使用条件・状況により大きく左右されますので  
検知することを保証するものではありません

ポートスキャンや新種のウイルス・ワームの検知：

The screenshot shows the inMon Traffic Sentinel web interface. The main content area displays 'Port Scanning Activity' with a table of 'New Hosts' and 'Cached Hosts'. The 'New Hosts' table has columns for IP Source, Destination Port, and # Destinations. The 'Cached Hosts' table has columns for IP Source, Destination Port, # Destinations, First Seen, and Last Seen. An arrow points to the IP address 172.16.144.52 in the 'Cached Hosts' table.

IP Source	Destination Port	# Destinations
172.16.144.52	TCP:445	446
172.16.144.52	TCP:139	331

IP Source	Destination Port	# Destinations	First Seen	Last Seen
172.16.144.52	TCP:445	446	3/13/06 5:30 PM	3/28/06 2:15 PM
172.16.144.52	TCP:139	331	3/13/06 5:30 PM	3/28/06 2:15 PM

172.16.144.52 は、TCPポート445や139を使用して、多くのホストとの接続が測定された。

## 監査：フローログ - サーバーへのTELNET接続者のログ

The screenshot shows the inMon Traffic Sentinel web interface. The main content area displays a table of TELNET logs. The table has the following columns: 時間 (Time), Server Address, Server Port, IP Protocol, Client Address, Frames, and Bytes. The data rows show various connections to servers like 192.168.10.33 and 192.168.114.18 from clients such as 192.168.116.240 and 192.168.71.94.

時間	Server Address	Server Port	IP Protocol	Client Address	Frames	Bytes
06/07/01 0:00	<a href="#">192.168.10.33</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.116.240</a>	2,584	109,990
06/07/01 0:00	<a href="#">192.168.114.18</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.71.94</a>	408	20,973
06/07/01 0:00	<a href="#">192.168.71.97</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.71.94</a>	256	10,240
06/07/01 0:00	<a href="#">traffic.osk.ps.msol.co.jp</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.114.18</a>	52	2,243
06/07/01 0:00	<a href="#">traffic.osk.ps.msol.co.jp</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.110.53</a>	32	1,833
06/07/01 0:00	<a href="#">203.141.42.73</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.71.94</a>	31	3,249
06/07/01 0:00	<a href="#">turbo.osk.ps.msol.co.jp</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.70.21</a>	5	204
06/07/01 0:00	<a href="#">142.240.92.29</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.71.94</a>	3	144
06/07/01 0:00	<a href="#">192.168.10.33</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.116.235</a>	0	0
06/07/01 0:00	<a href="#">192.168.71.36</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">katata.osk.ps.msol.co.jp</a>	0	0
06/07/01 0:00	<a href="#">192.168.10.33</a>	TCP:23 (telnet)	IP:6 (TCP)	<a href="#">192.168.116.233</a>	0	0

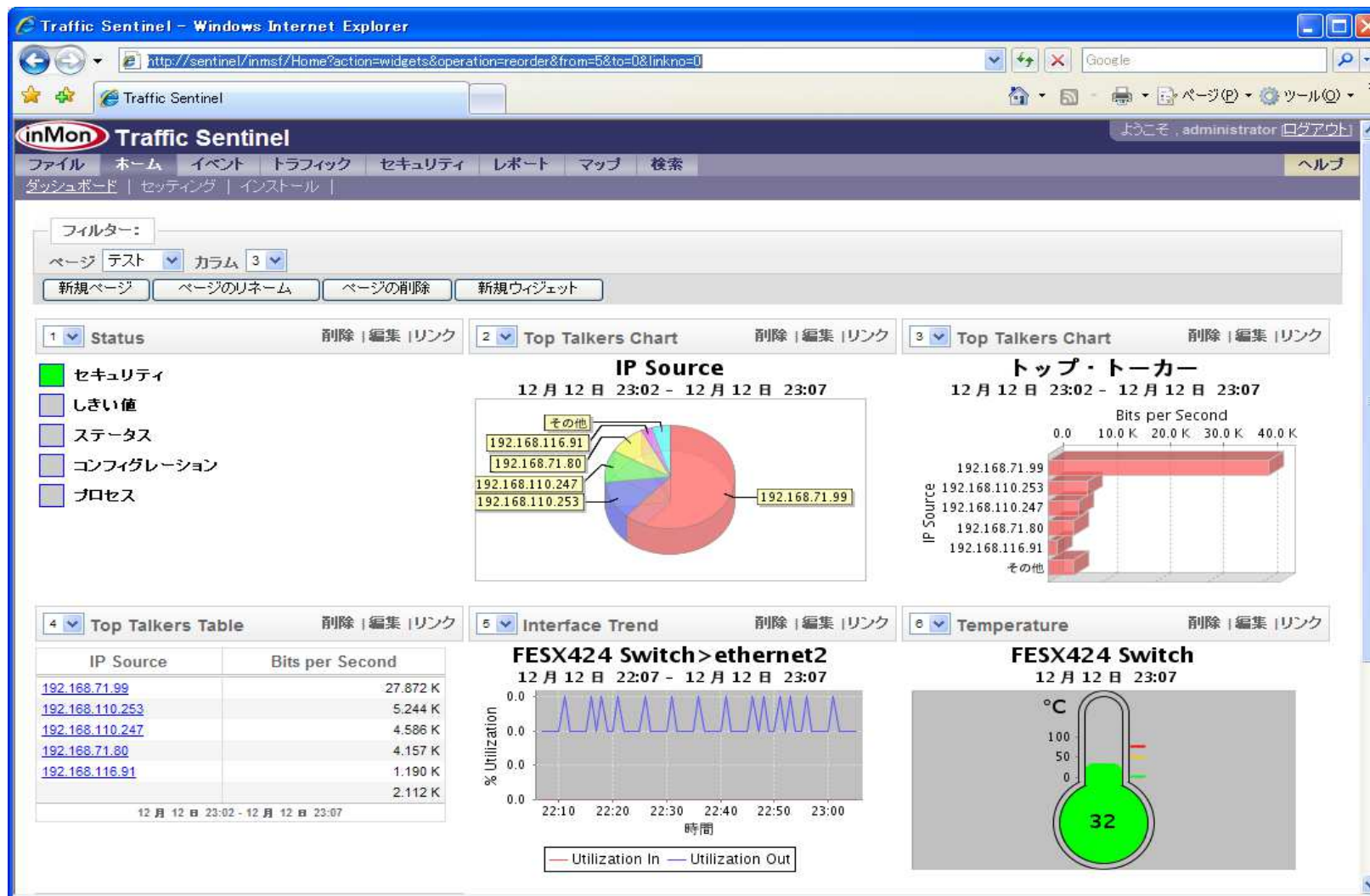
7月1日 00:00 - 8月1日 00:00

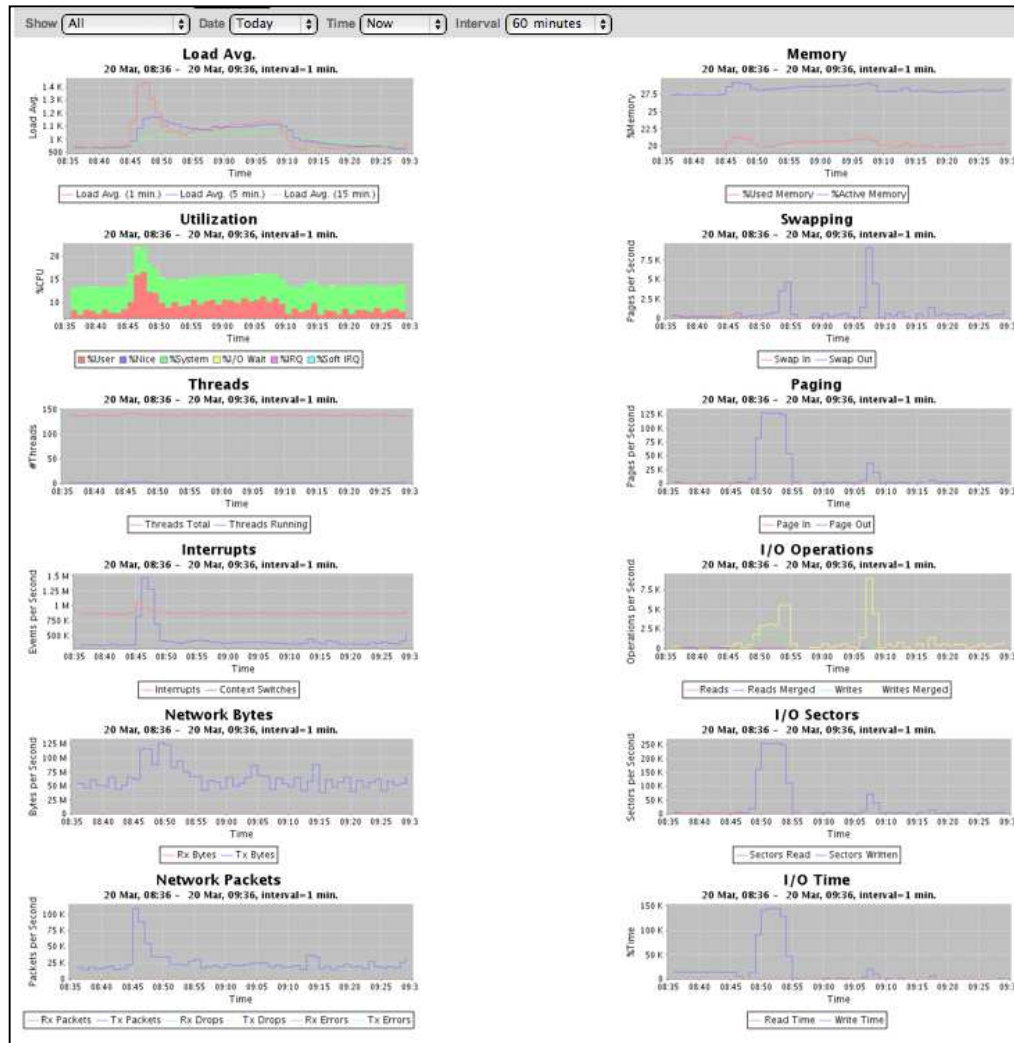
Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

特定のサーバーへのアクセスや特定のクライアントの使用内容の把握



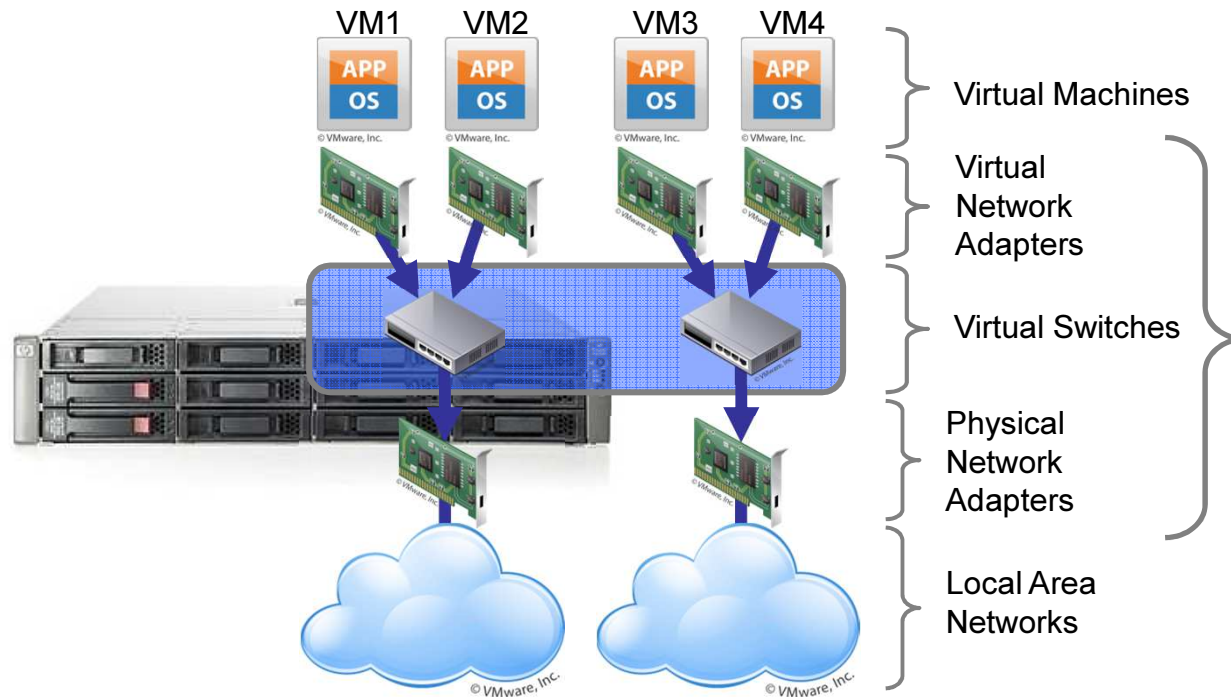
ログインユーザー毎にダッシュボードが作成できます。  
 使用頻度の高いグラフ等を任意に組み合わせて自分用画面が作成できます。





- データセンター内の全てのシステムのパフォーマンス計測を集約し表示
- 計測値を結合
- 計測値を比較
- フローデータからサービスを検知し、アプリケーションの関連状態をマッピング
- システムが関連するネットワークリソースや生成されるトラフィックを関連付ける

ダウンロード: <http://www.marubeni-sys.com/network/inmon/pub/inmon/hostsflow/hostsflow.html>

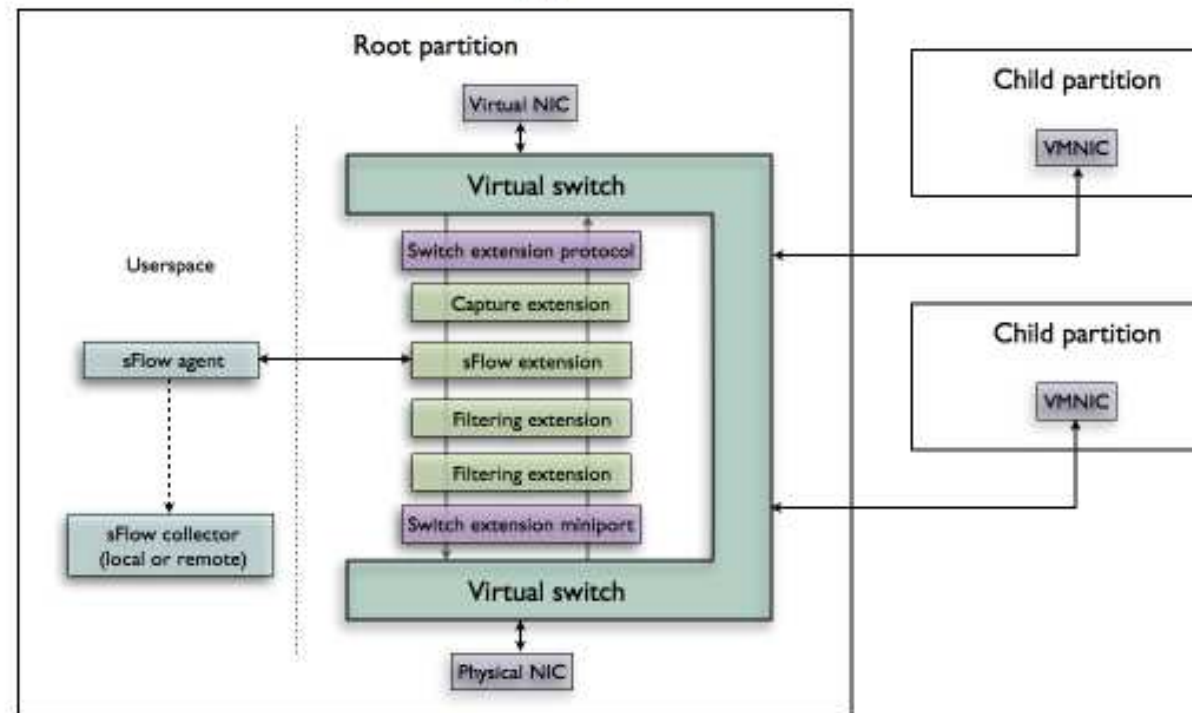


仮想スイッチに実装されたsFlowは、仮想マシンの可視化を実現する

- InMon Virtual Probe
- Open vSwitch (Xen, KVM, Proxmox VE, VirtualBox)
- Microsoft Windows 2012 Server Hyper-V
- VMWARE vSphere 5 (NetFlow)



## sFlow in the Hyper-V extensible switch



- Microsoft Windows2012 Serverには、  
Hyper-V extensible switch 内に実装される

参照：<http://www.marubeni-sys.com/network/inmon/pub/inmon/hypervsflow/microsoft-hyper-v-sflow.html>

- トランザクションのサンプル
- トランザクションの統計
- TCP/UDP socket

例:

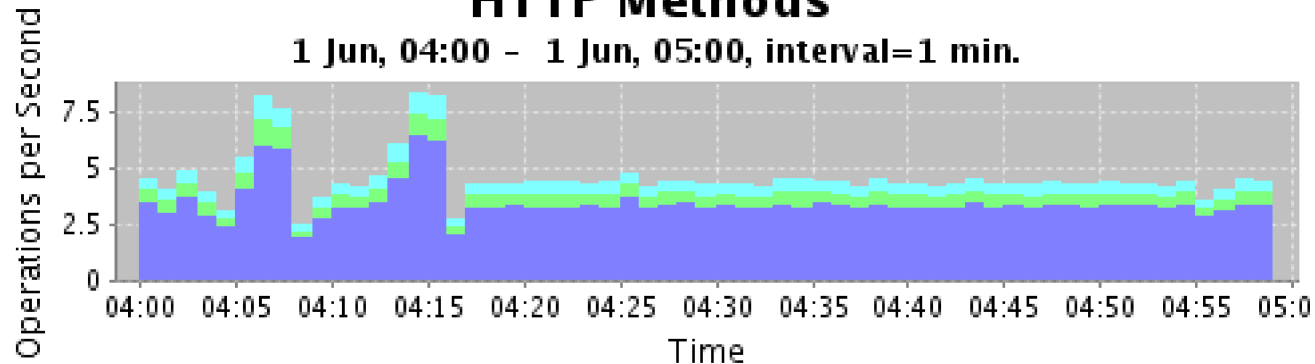
- NFS/CIFS transactions
  - File path, bytes, response time, socket
- HTTP requests
  - URL, user agent, mime type, bytes response time, socket
- Memcached lookups
  - Key, value-bytes, hit/miss, socket
- Database queries
  - Query#, response time, socket

アプリケーション・レイヤーの測定は、インフラ内の各コンポーネントのパフォーマンスと関連付けるとき、さらに重要です。

参照:<http://www.marubeni-sys.com/network/inmon/pub/inmon/tutorials6/applications.php>

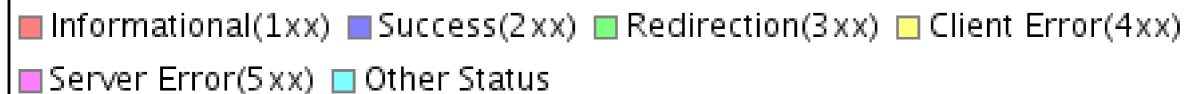
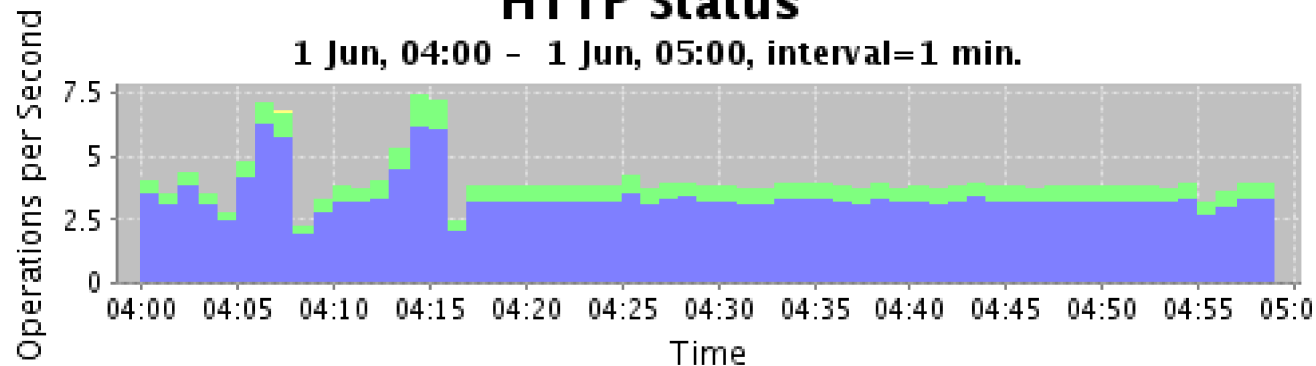
## HTTP Methods

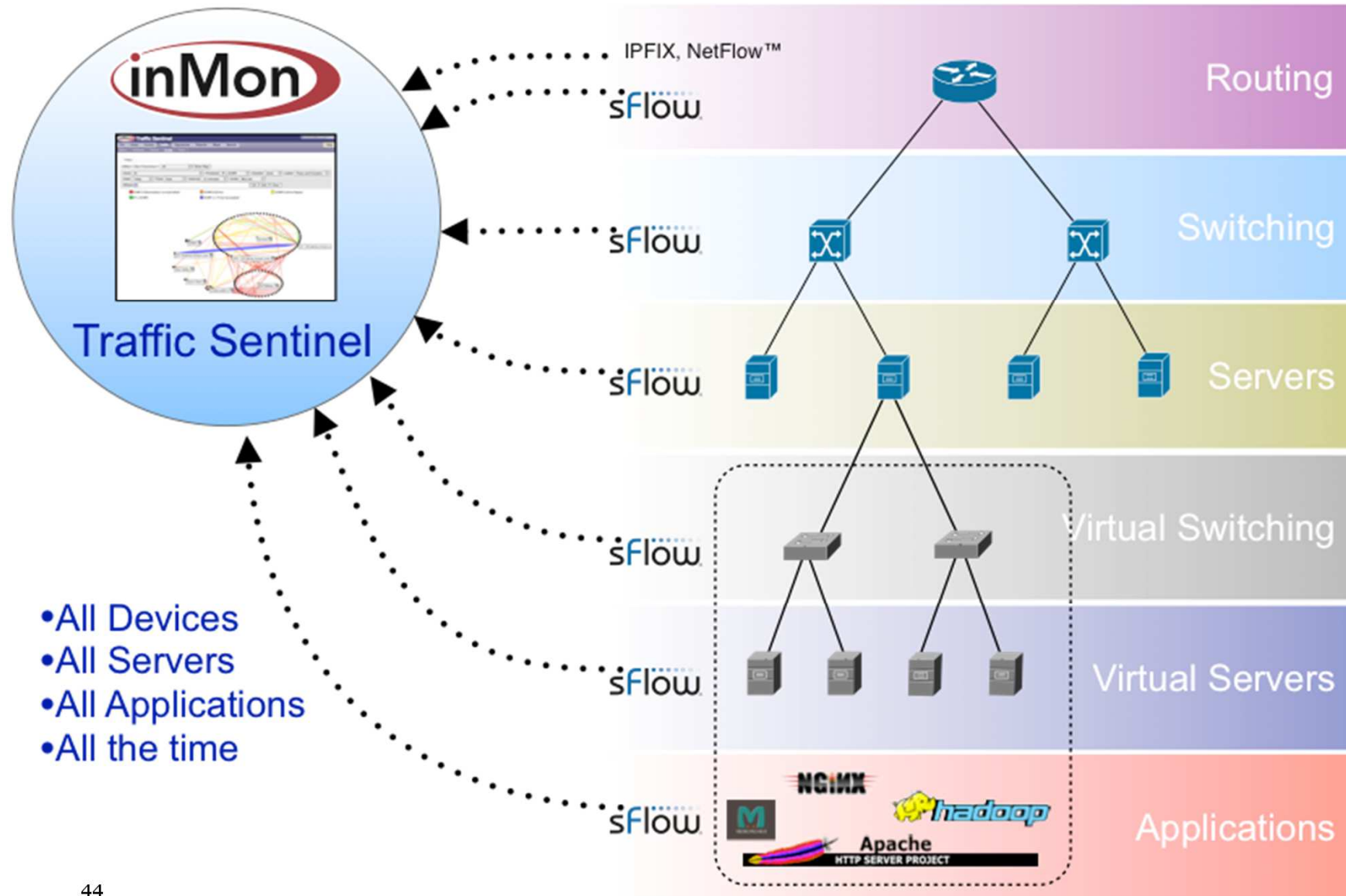
1 Jun, 04:00 - 1 Jun, 05:00, interval=1 min.

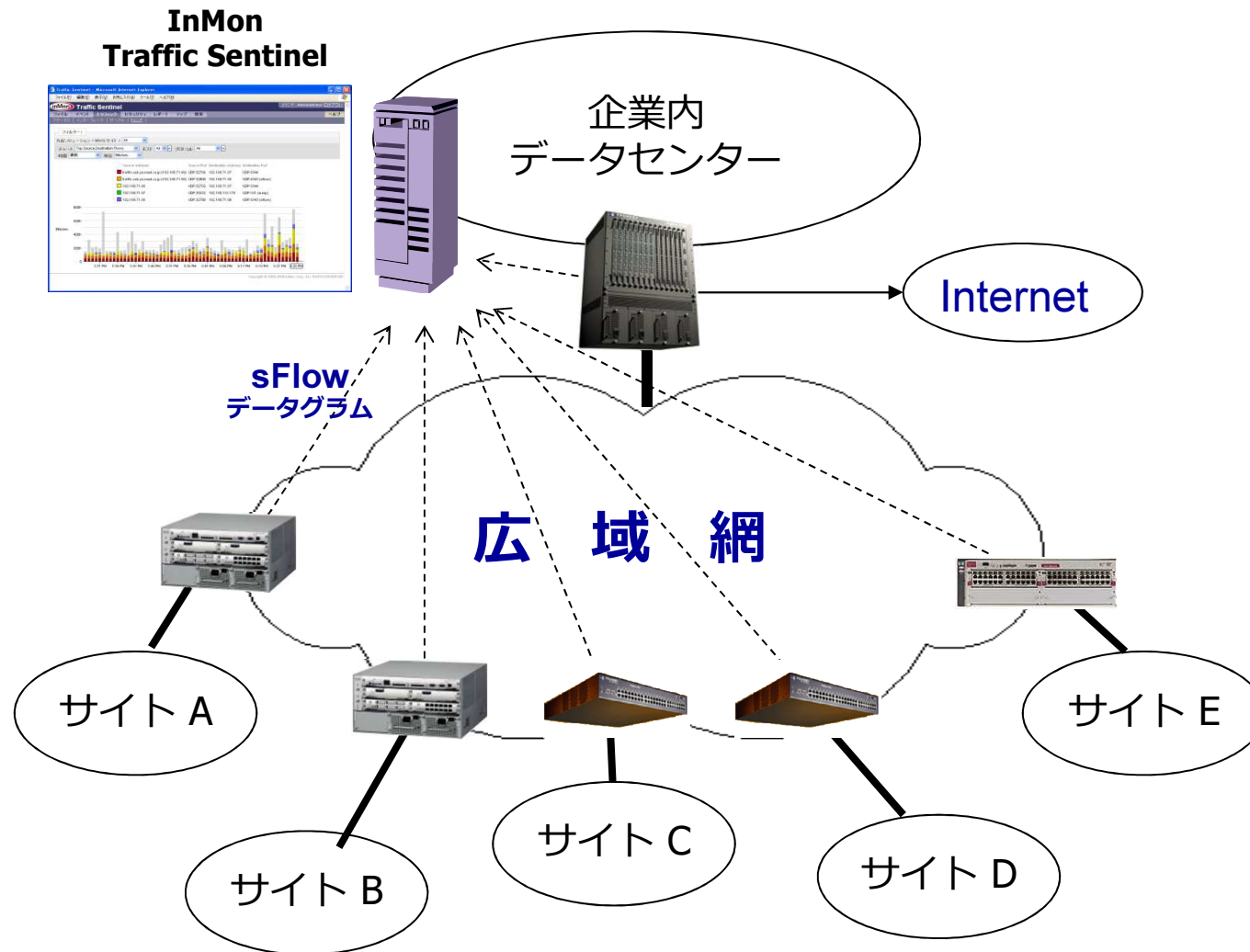


## HTTP Status

1 Jun, 04:00 - 1 Jun, 05:00, interval=1 min.



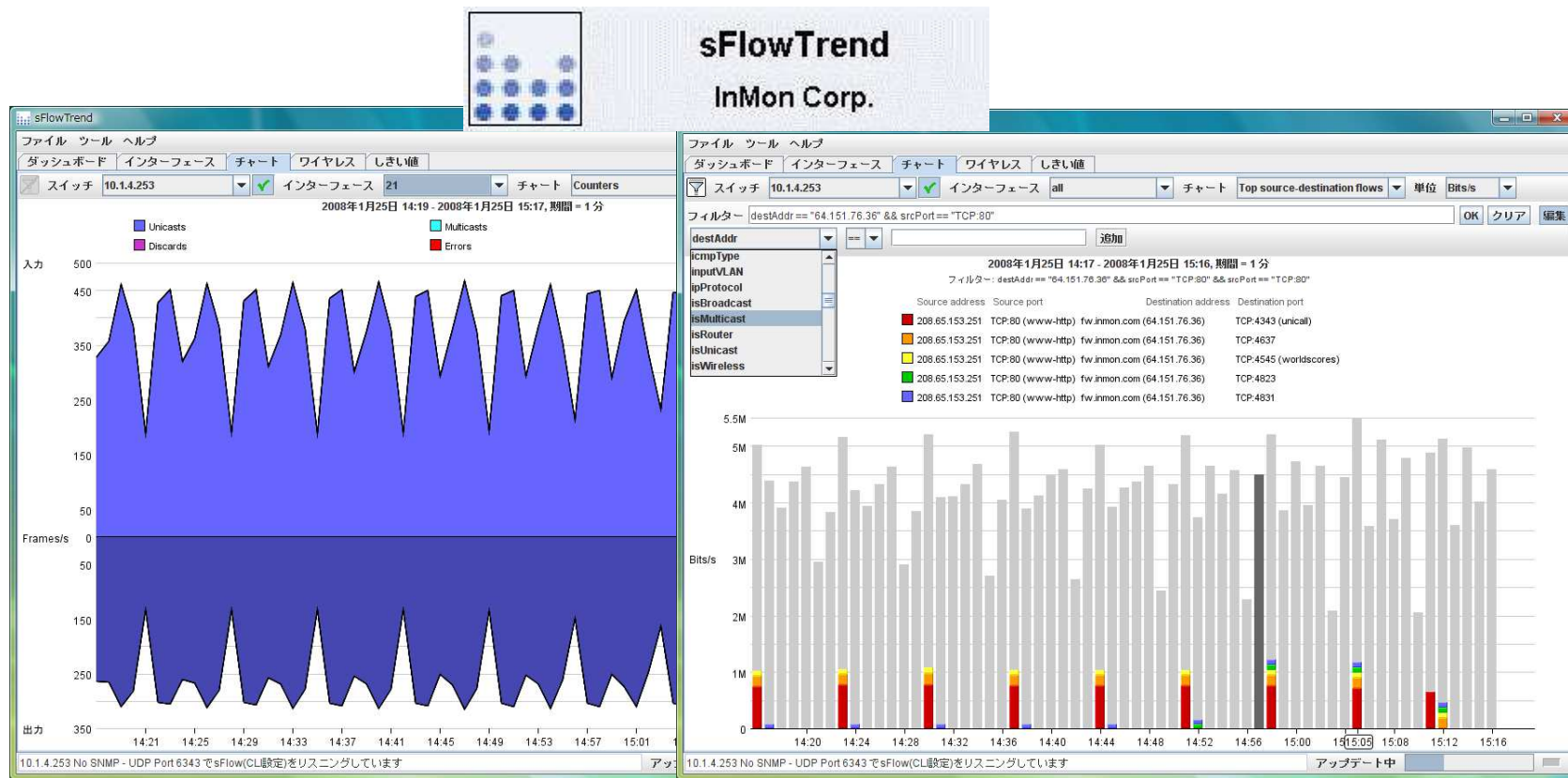




sFlowTrend™ は、フリー（無償）のツールです。  
 グラフィカルな sFlow® コレクターで、トップトーカーやインターフェースカウンタを経過時間に渡りプロットします。

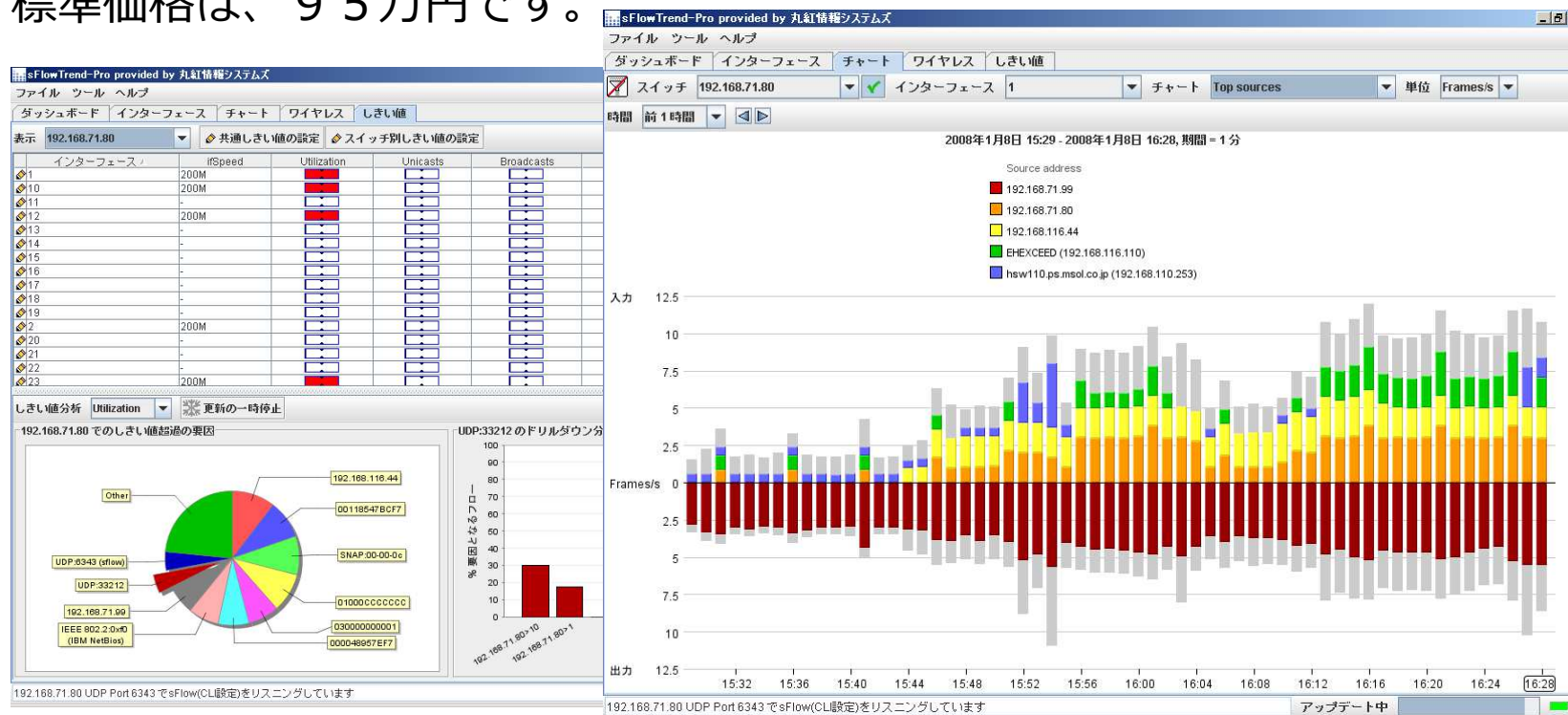
弊社のsFlowTrendホームページより、ダウンロード・インストールできます。

<http://www.marubeni-sys.com/network/inmon/pub/sFlowTrend/pub/index.html>





sFlowTrend-Proは、sFlowTrendの機能強化商用版です。  
 sFlowTrendと比較し、  
 複数台のスイッチのモニタリング（10台程度まで）  
 データの長期保存（数週間程度）  
 時間フィルタリング  
 などの機能が拡張されています。  
 標準価格は、95万円です。



## ■ InMonTrafficSentinelの要求システム構成

小規模構成（1,000 switch port）

CPU：デュアル・クアッドコアCPU 2.5GHz 相当以上

Memory：4 GB以上、Disk/80GB以上 SAS or SATA、NIC/100Mbps以上

OS：Red Hat Enterprise Linux 5以降、Fedora 10以降、CentOS 5以降

※H/Wスペックについては監視対象規模やサンプリングレート、データ保存期間などに依存します。

## ■ InMonTrafficSentinelデモンストレーションサイト

<http://demo.inmon.com/> ユーザ：demo パスワード：demo

## ■ InMon製品およびその他取り扱い製品紹介WEBサイト

<http://www.marubeni-sys.com/network/inmon/pub/>