



# NetFlowによる フロー・マネージメント

## InMon TrafficSentinelのご紹介

丸紅情報システムズ株式会社

プラットフォーム&ネットワーク事業本部

出野 真也

*Ideno-Shinya@marubeni-sys.com*

- ・ フローマネージメント/フロープロトコル
- ・ NetFlow
- ・ InMonTrafficSentinelのご紹介
  - 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
- ・ ケーススタディー
- ・ 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

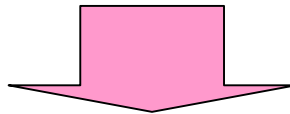
 ネットワークの  
可視化

## 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
  - RMON2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



## フロー・プロトコルの誕生 ( NetFlow / sFlow / J-Flow / IPFIX / XRMON / LFAP )



- 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 packets 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 packets 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

- Cisco NetFlow

Figure 1 Example of a NetFlow Cache

1. NetFlow キャッシュ内での、フローの生成と更新

Srdf	Srd Padd	Dstlf	Dstl Padd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	Next Hop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.023.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.023.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.023.2	1040	1745	14

2. 期限切れ (expiration)

- ・インアクティブ・タイマーの期限切れ (デフォルト: 15秒)
- ・アクティブタイマーの期限切れ (デフォルト: 30分)
- ・NetFlow キャッシュが、フル
- ・RST / FIN TCP フラグ

Srdf	Srd Padd	Dstlf	Dstl Padd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	Next Hop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1800	4

3. 集約 (Aggregation)

4. エクスポート・バージョン (V5 / 9 など)

5. トランスポート・プロトコル  
→ パケットのエクスポート

Payload (Flows)

4. エクスポート・バージョン (V8/9 など)

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	DstPort	1528

Cisco "NetFlow Services Solutions Guide" より

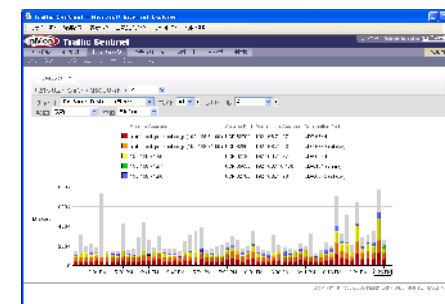
## ■ Cisco Systems



NetFlow V1, V5, V7, V9

NetFlow

## InMon Traffic Sentinel



- NetFlowによる分析

Cisco 800/1700/2600/1800/2800/3800  
4500/6500/7200/7300/7500/7600  
10000/12000

Cisco CRS-1

Cisco Catalyst 6500/4500

※ 各機器でのNetFlowの対応状況の詳細は、ハードベンダー様へご確認下さい



## ■sFlow

InMon sFlow Probe

HP

アラクサラ・ネットワークス

日立製作所

NEC

アライドテレシス

Force10 Networks

Extreme Networks

Alcatel Lucent

H3C

## ■Juniper Networks J-Flow

## ■IPFIX (Nortel Networks etc)

※ IPFIXはオープンな規格です。

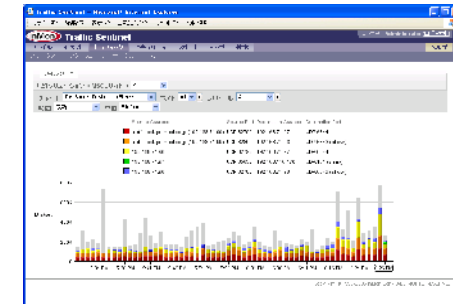
## ■HP XRMON

## ■(旧)RiverStone LFAP

※ 各メーカーでの各フロープロトコルの対応状況は、ハードベンダー様へご確認下さい

Flow

## InMon Traffic Sentinel



- InMon Traffic Sentinelは、各種フロープロトコル  
NetFlow  
sFlow  
J-Flow  
IPFIX  
XRMON  
LFAP  
に対応。

## 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、InMon社が開発したフロー・マネージメント・システムです。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、

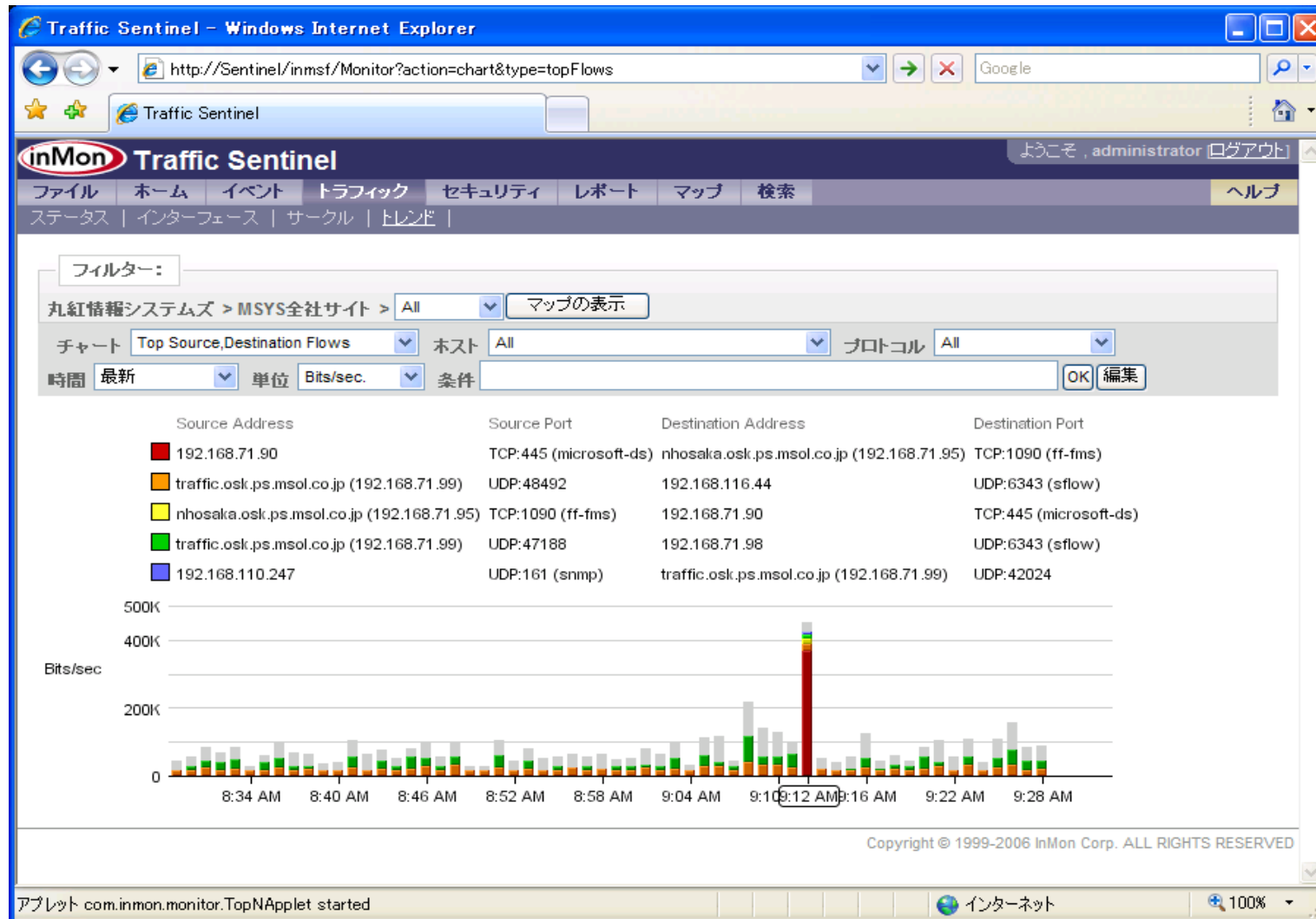
**NetFlow/sFlow/J-Flow/XRMON/LFAP/IPFIX/SNMP**

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

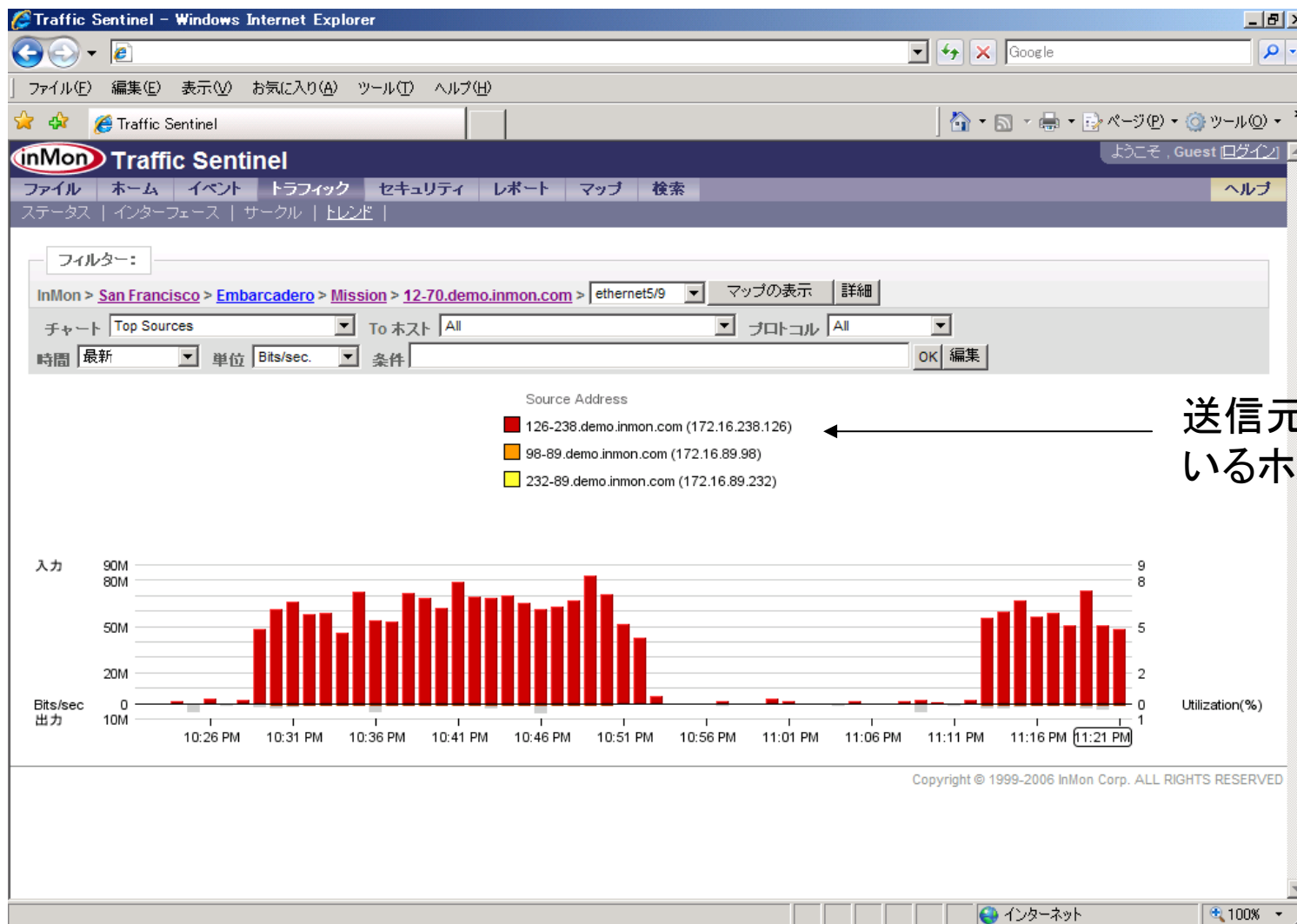
## 2. 問題が発生してインターフェースはどこか？

問題の指摘

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

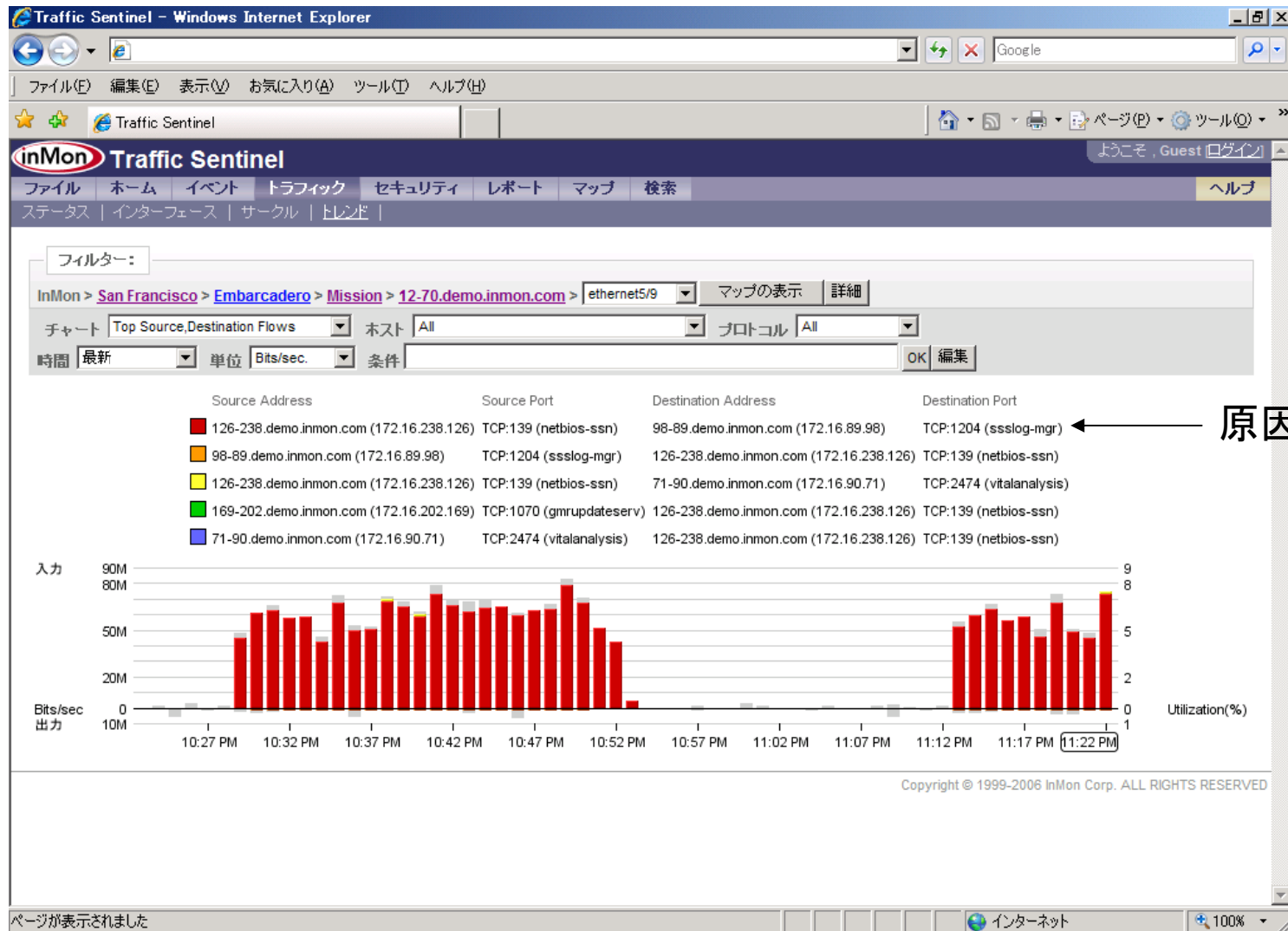
ステータス						インターフェース		
Frames	Utilization	Broadcasts	Multicasts	Errors	Discards	エージェント	インターフェース	ifSpeed
						12-70.demo.inmon.com	ethernet5/9	1Gb/sec
						10-70.demo.inmon.com	ethernet2/3	10Mb/sec
						29-70.demo.inmon.com	ethernet8	100Mb/sec
						12-70.demo.inmon.com	ethernet1/1	1Gb/sec
						12-70.demo.inmon.com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



## 根原因となる要因の追求:

Utilization(使用率)のしきい値超過においてSunsetゾーンへの通信が、バイト数として97%の要因となっている

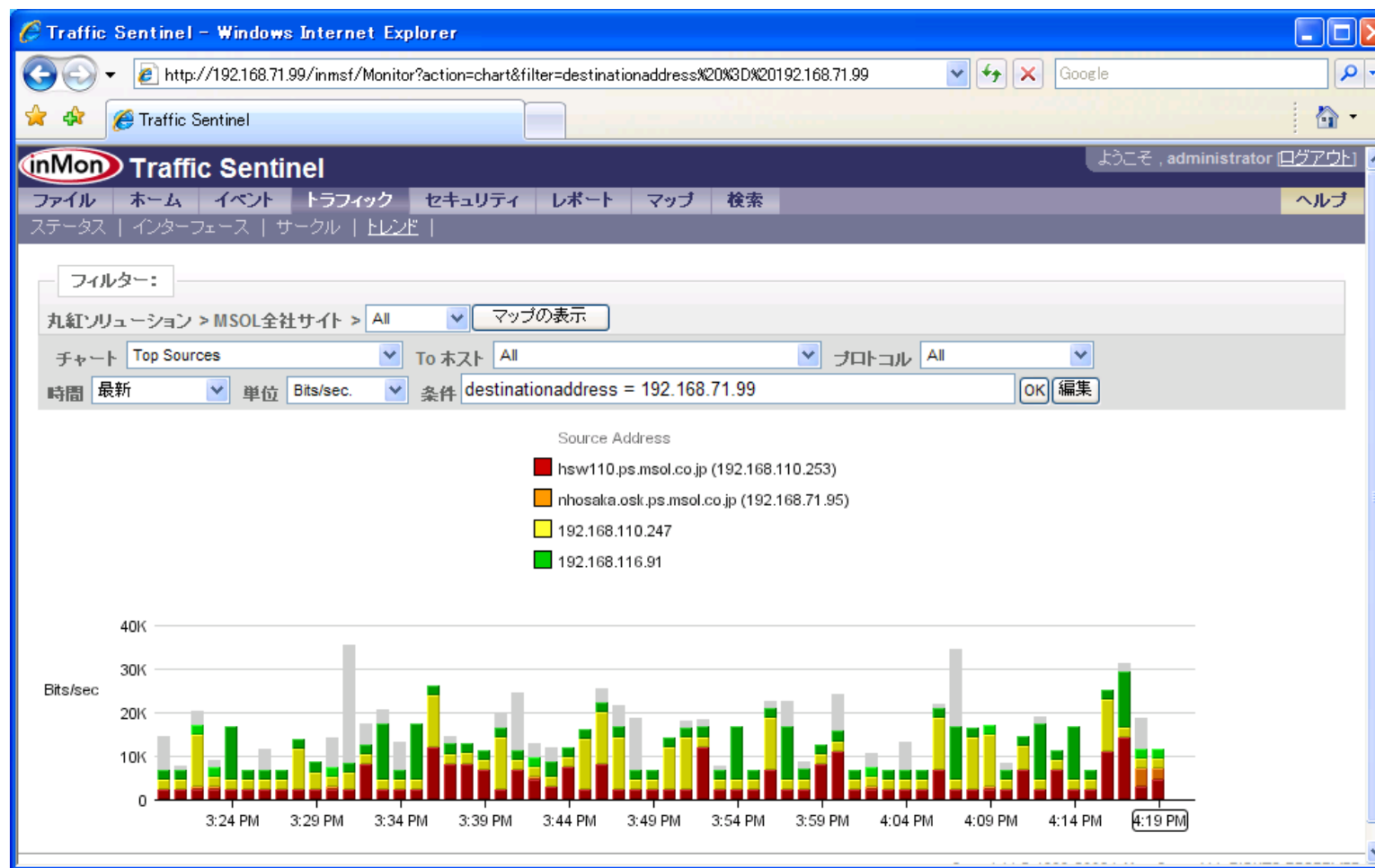
Utilization(使用率)のしきい値超過において172.16.238.126からの通信が、バイト数として62%の要因となっている

ウェイト			Source		Destination					
フロー数	フレーム数	バイト数	ゾーン	グループ	アドレス	ポート	ゾーン	グループ	アドレス	ポート
87%	88%	97%	Sunset	Irving			Sunset	Irving		
73%	76%	96%	Sunset	Irving			Sunset	Irving		
60%	65%	92%	Sunset	Irving			Sunset	Irving		
40%	4%	62%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)					
27%	29%	59%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)		Sunset	Irving		
60%	59%	38%					Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	
47%	47%	34%					Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)
33%	35%	34%	Sunset	Irving			Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	
20%	18%	31%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)				
20%	24%	31%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)				
13%	18%	30%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)	Sunset	Irving		
20%	24%	30%	Sunset	Irving			Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)
13%	12%	29%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)	Sunset	Irving		
7%	12%	28%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)	Sunset	Irving	122-89.demo.inmon.com (172.16.89.122)	TCP:1044 (dcutiltv)
7%	6%	26%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)	Sunset	Irving	95-202.demo.inmon.com (172.16.202.95)	TCP:1106 (isoipsaport-1)
7%	6%	26%	Sunset	Irving	240-175.demo.inmon.com (172.16.175.240)	TCP:1425 (zion-lm)	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)
27%	24%	4%	SOMA	Spear			Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:524 (ncp)
13%	12%	4%	Sunset	Irving			Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)
7%	6%	2%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)	Sunset	Irving	82-202.demo.inmon.com (172.16.202.82)	TCP:1077 (imgames)
7%	6%	2%	Sunset	Irving	126-238.demo.inmon.com (172.16.238.126)	TCP:139 (netbios-ssn)	Potrero Hill	Missouri	76-9.demo.inmon.com(172.16.9.76)	TCP:1698 (rsvp-encan-1)



## 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。

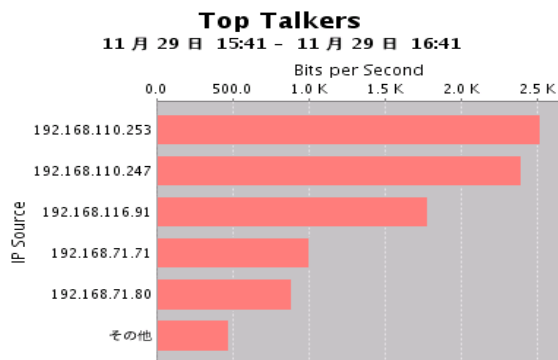


## 豊富なレポートテンプレートからのレポート作成・スケジュールレポート作成

### 部門別トップ・ユーザ・レポート

#### Recent Traffic Top N Chart

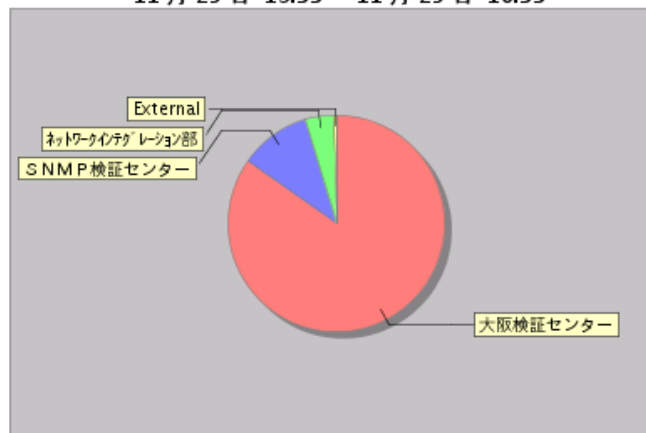
インターフェース上のトラフィックの最新の統計をプロット



[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

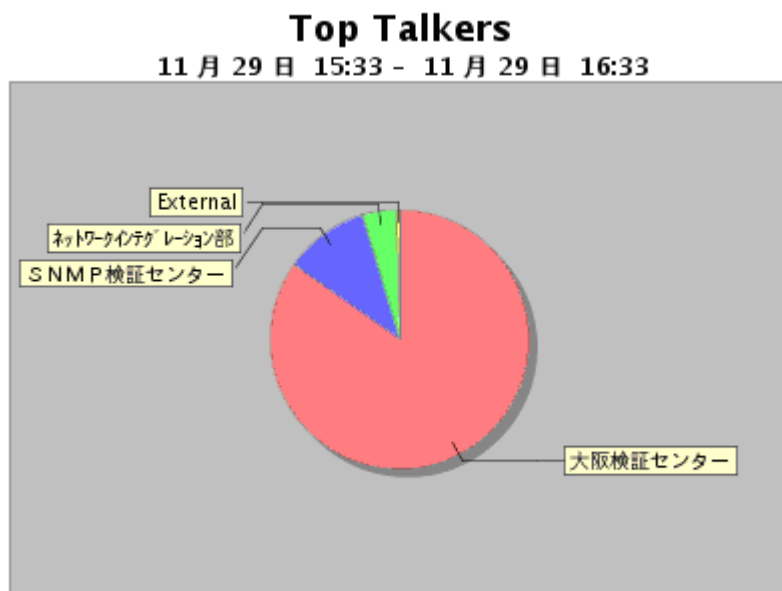
## 特定サーバーの使用状況のレポート : グループ別

### Historical Traffic Totals by Time

先週、サーバー(192.168.71.99)へアクセスした上位グループ

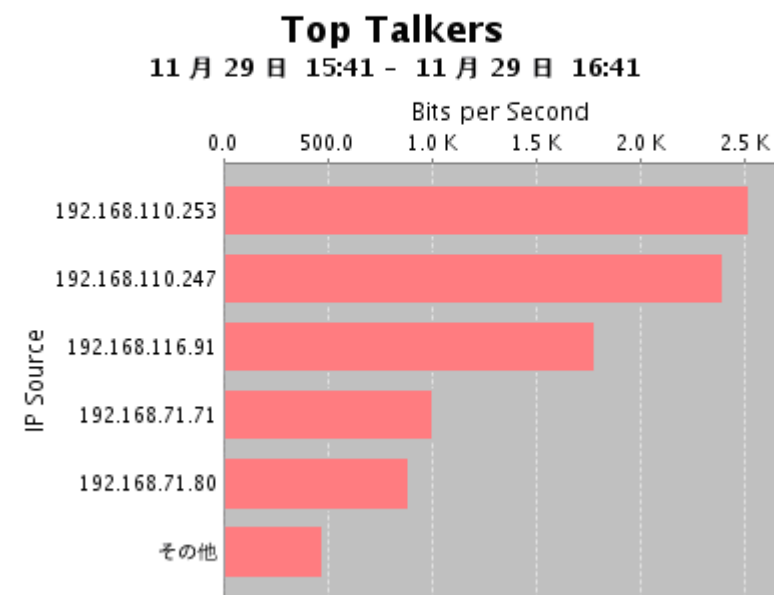
時間	Source Group	Bits per Second
07/11/18 0:00	SNMP検証センター	2.210 K
07/11/18 0:00	大阪検証センター	697.624
07/11/18 0:00	External	41.360
07/11/18 0:00		2.840
07/11/19 0:00	SNMP検証センター	2.402 K
07/11/19 0:00	大阪検証センター	856.416
07/11/19 0:00	ネットワークインテグレーション部	742.528
07/11/19 0:00		73.432
07/11/20 0:00	SNMP検証センター	2.400 K
07/11/20 0:00	ネットワークインテグレーション部	1.285 K
07/11/20 0:00	大阪検証センター	1.002 K
07/11/20 0:00		58.632
07/11/21 0:00	SNMP検証センター	2.362 K
07/11/21 0:00	ネットワークインテグレーション部	1.311 K
07/11/21 0:00	大阪検証センター	516.808
07/11/21 0:00		66.616
07/11/22 0:00	SNMP検証センター	2.377 K
07/11/22 0:00	ネットワークインテグレーション部	1.214 K
07/11/22 0:00	大阪検証センター	218.432
07/11/22 0:00		56.808
07/11/23 0:00	SNMP検証センター	2.361 K
07/11/23 0:00	ネットワークインテグレーション部	934.240
07/11/23 0:00	大阪検証センター	285.560
07/11/23 0:00		70.224

特定回線を使用したグループの内訳をレポート



### 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](#)

- トラフィックの内容に対ししきい値を設定し、超過したとき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:

カテゴリー 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%

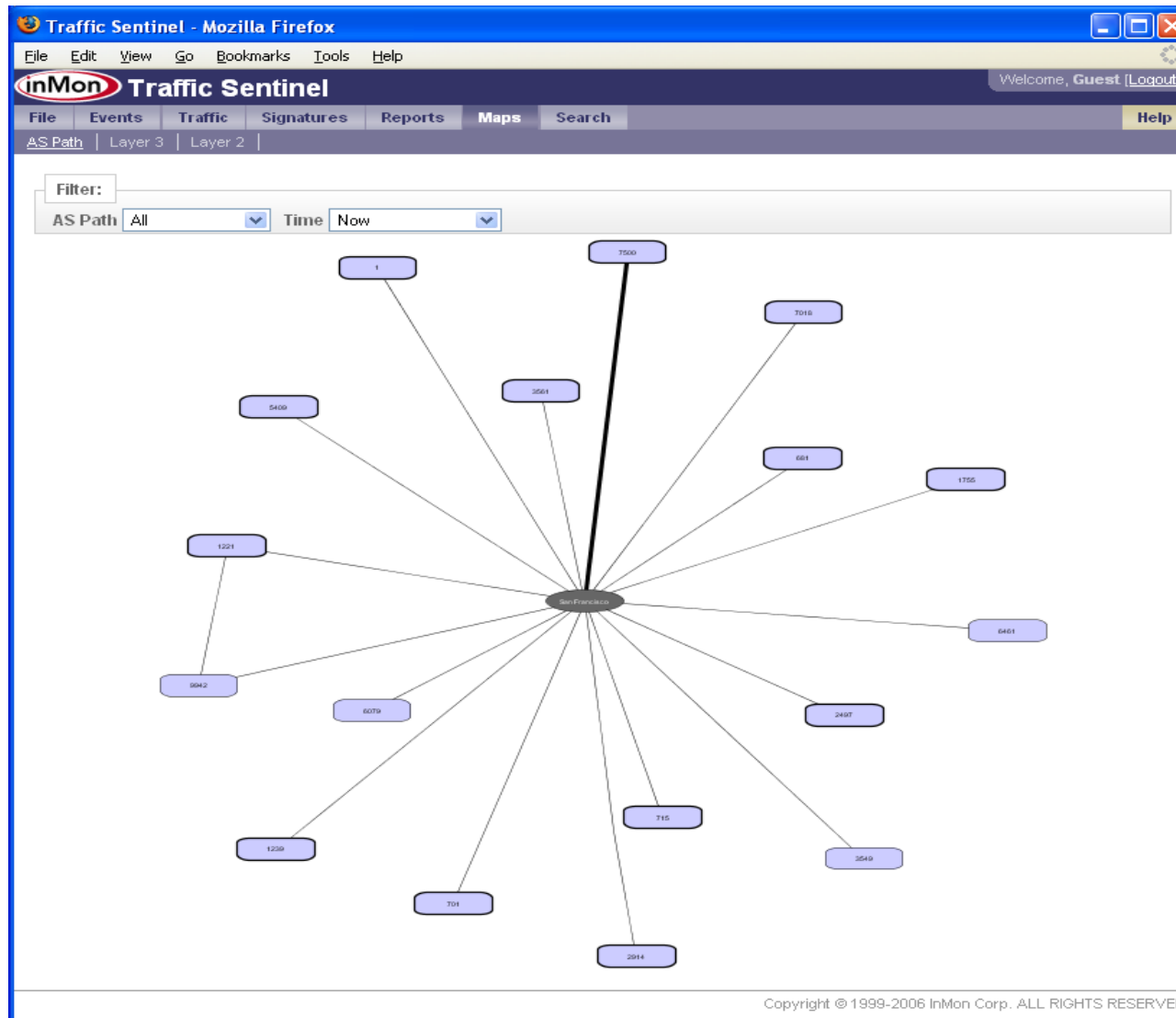
- 豊富なテンプレートを編集して、カスタマイズ・レポートが作成可能
  - 文言・表示情報・表示情報のフィルタリングなどの編集が可能
  - 定型レポートはスケジュール化

The screenshot shows the inMon Traffic Sentinel web interface. The left pane displays 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 yesterday (Osaka branch of Maruhong Information Systems)). The key selected is 'ipsource' (IP Source) with a value of 'Bits per Second'. The period is set to 'yesterday'.

The right pane shows the report results for the same configuration. The title is 'カスタマイズ・ヒストリカル・レポート' and the 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)'. 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 of the interface includes 'Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED' and a status bar indicating 'ページが表示されました' (Page displayed).



Peer ASをレポート

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





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 description: 'Identify port scanning activity associated with worm propagation.' Below this, there are sections for 'New Hosts' and 'Cached Hosts'. The 'Cached Hosts' section contains a table with the following data:

IP Source	Destination Port	# Destinations	First Seen	Last Seen
<a href="#">172.16.144.52</a>	<a href="#">TCP:445</a>	446	3/13/06 5:30 PM	3/28/06 2:15 PM
<a href="#">172.16.144.52</a>	<a href="#">TCP:139</a>	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 Traffic Sentinel web interface in Microsoft Internet Explorer. The page title is "Traffic Sentinel - Microsoft Internet Explorer". The interface includes a navigation menu with options like "ファイル", "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". Below the menu, there are filter controls for "カテゴリー" (Traffic), "レポート" (General Queries), and "セクション" (Historical Traffic). A "最新の表示" button is also present.

The main content area displays a table titled "TELNET監査ログ" (TELNET Monitoring Log) with the subtitle "TELNETを使用したクライアントの分析" (Analysis of clients using TELNET). The table has the following columns: 時間 (Time), Server Address, Server Port, IP Protocol, Client Address, Frames, and Bytes. The data shows various connections to servers on port 23 (telnet) from different client addresses.

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="#">kataka.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

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

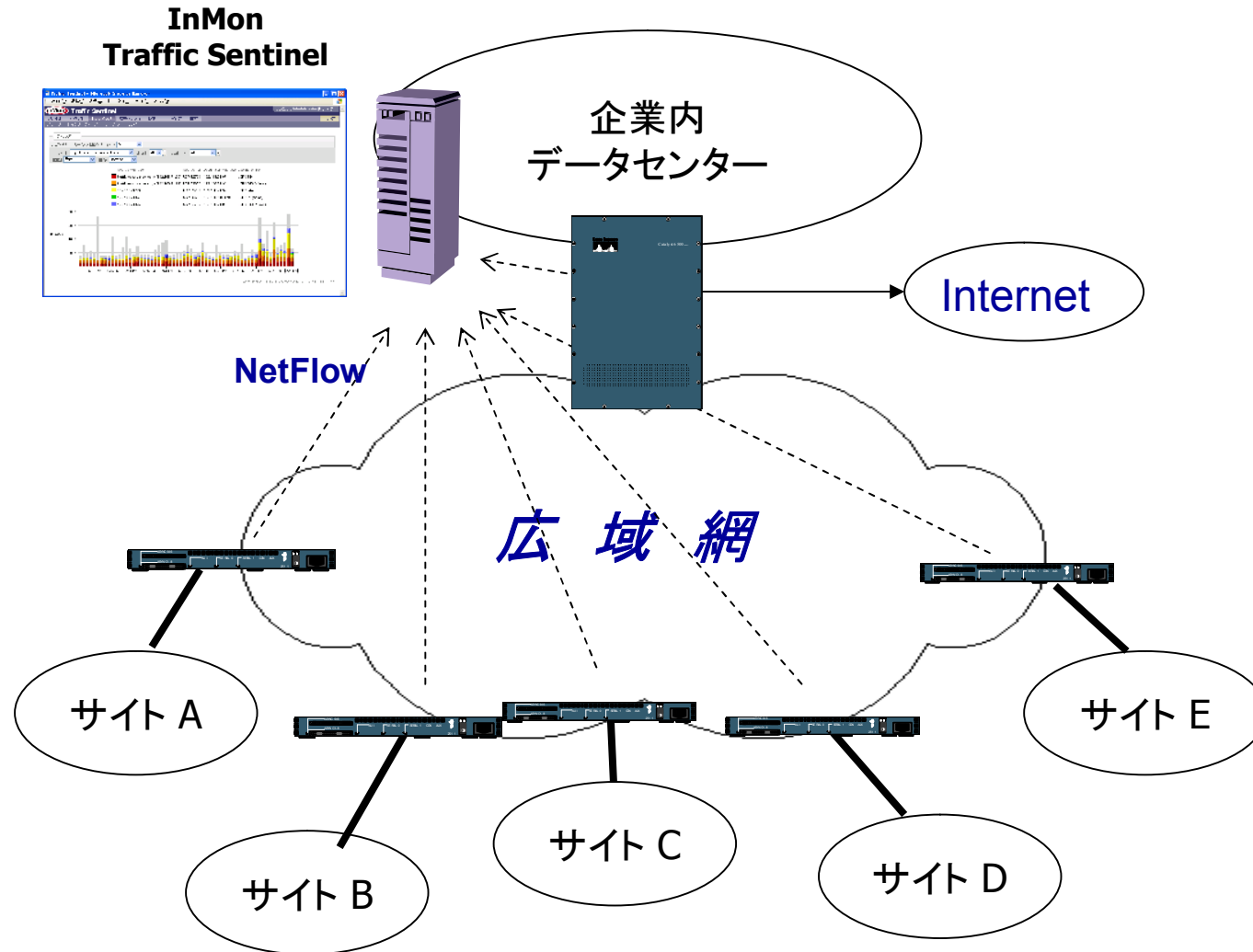
ログインユーザー毎にダッシュボードが作成できます。  
 使用頻度の高いグラフ等を任意に組み合わせて自分用画面が作成できます。

The screenshot displays the Traffic Sentinel dashboard with the following components:

- Filter Section:** Includes a filter dropdown, page selection (Test), and column count (3).
- Security Status:** A list of status categories with checkboxes:
  - セキュリティ
  - しきい値
  - ステータス
  - コンフィグレーション
  - プロセス
- IP Source Chart:** A pie chart showing traffic distribution by IP source for the period 12月12日 23:02 - 12月12日 23:07. The largest segment is 192.168.71.99.
- Top Talkers Chart:** A horizontal bar chart showing the top IP sources by Bits per Second for the same period. The top source is 192.168.71.99.
- Top Talkers Table:** A table listing the top IP sources and their corresponding Bits per Second.
 

IP Source	Bits per Second
192.168.71.99	27.872 K
192.168.110.253	5.244 K
192.168.110.247	4.586 K
192.168.71.80	4.157 K
192.168.116.91	1.190 K
	2.112 K
- Interface Trend:** A line graph showing the percentage utilization of the FESX424 Switch's ethernet2 interface from 22:10 to 23:00. It tracks Utilization In and Utilization Out.
- Temperature Gauge:** A gauge showing the temperature of the FESX424 Switch at 23:07, with a reading of 32°C.

# ケーススタディー



## ■ InMonTrafficSentinelの要求システム構成

小規模構成(1,000 switch port)

CPU/PentiumIV × 1 3GHz

Memory/2GB以上(4GB推奨)、Disk/80GB IDE 以上、NIC/100Mbps以上

OS/Red Hat Enterprise Linux 3/4/5-ES/AS、Fedora Core 5/6/7/8

※H/Wスペックについては監視対象規模やNetFlow設定、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://sentinel.inmon.com/>

## ■ InMon製品およびその他取り扱い製品紹介WEBサイト

<http://nms.marubeni-sys.com/>

## ■ お問い合わせ先

丸紅情報システムズ株式会社 プラットフォーム&ネットワーク事業部

デジタルマーケティング営業部 営業三課 担当:伊東

TEL:03-5778-8712 eMail : [its@marubeni-sys.com](mailto:its@marubeni-sys.com)