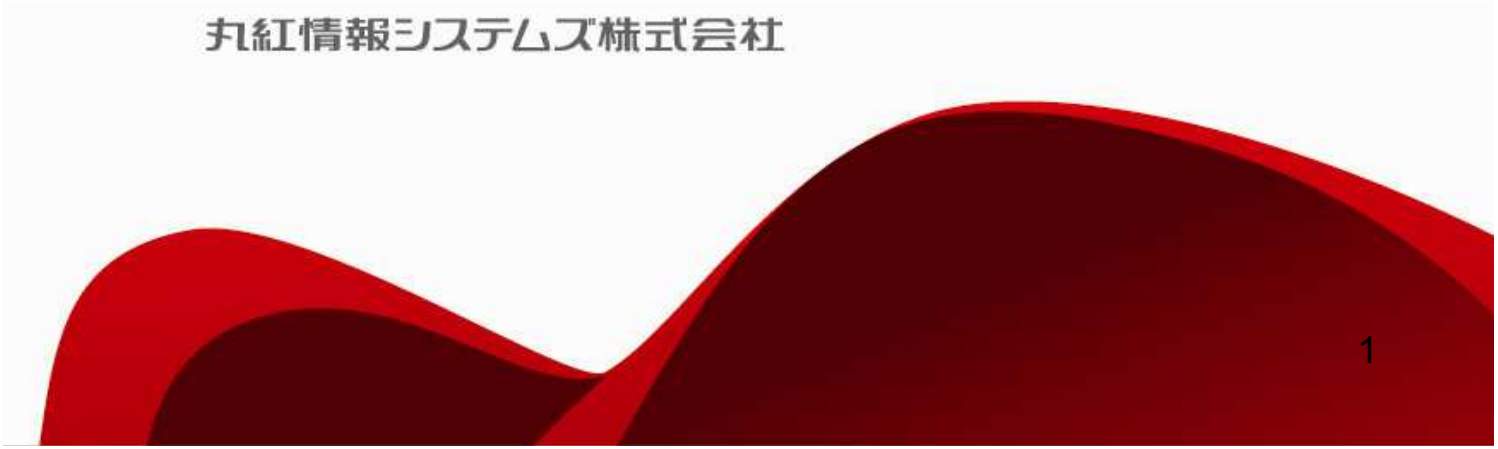
sFlow/NetFlow ＆
InMon TrafficSentinelのご紹介

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



アジェンダ

- 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

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

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？

フローマネージメント ～ **sFlow**の誕生

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

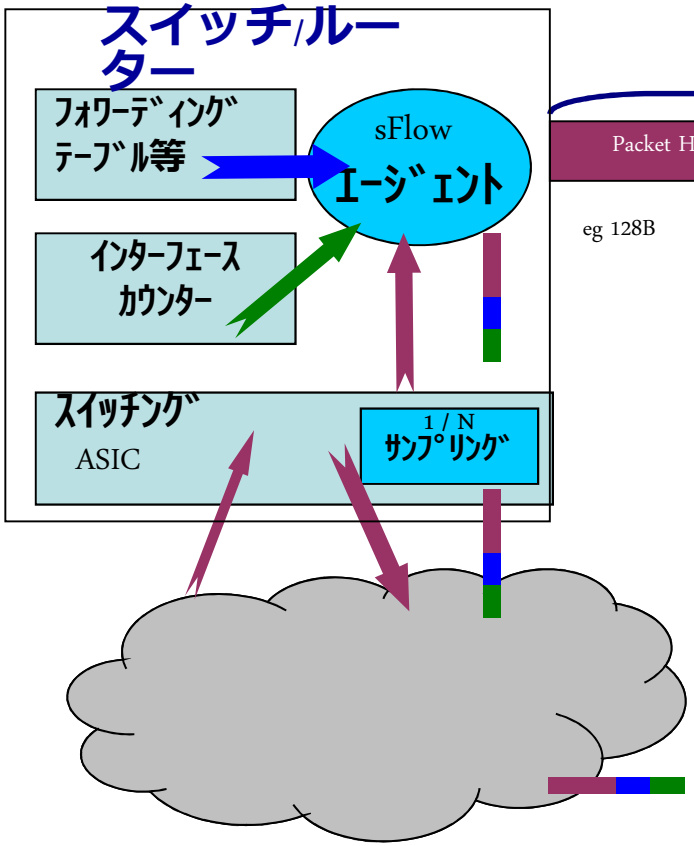
ネットワークの可視化への次世代の解決法 → **sFlow**の誕生

sFlowとは

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！

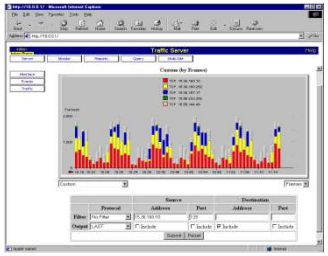
- 業界標準ネットワーク・トラフィック・モニタリング技術
- ネットワーク全体を可視化
  - 全てのスイッチ・全てのインターフェースを測定
- **サンプリングベース**のテクノロジー
  - スイッチやネットワークのパフォーマンスへの影響が少ない
  - ハイスピードネットワーク内のトラフィックのモニタリングに効果的
- 米国**InMon**社によって公開 ： **Open Standard – IETF RFC3176(sFlow V4)**
- ネットワーク機器埋め込み型として設計されたモニタリング・テクノロジー
  - ルータスイッチ内に実装されスイッチのASICにて処理
- スイッチの**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の動作



sFlow Datagram

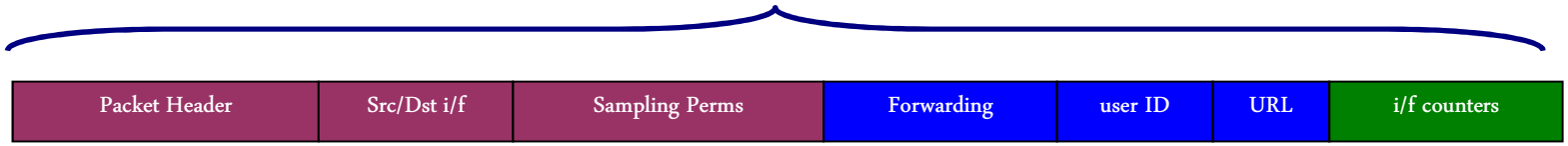
Packet Header	Src/Dst i/f	Sampling Perms	Forwarding	user ID	URL	i/f counters
eg 128B		rate pool	src 802.1p/Q dst 802.1p/Q next hop src/dst mask AS path communities localPref MPLS	src/dst Radius TACACS		



InMon Traffic Sentinel
sFlow Collector & Analyser

sFlowデータグラム・フォーマット

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 ： 入出力インターフェースのifIndex
  - Sampling Perms ： sFlowﾊﾟﾗﾒｰﾀｰ(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

sFlowをサポートしている ベンダー（最近の実装メーカー）

NetFlow系（NetFlow/J-Flow/IPFIX）実装メーカー

CISCO

Juniper NETWORKS

enterasys Secure Networks

NORTEL

HUAWEI

※ 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

sFlow：トラフィック量の計算

- サンプリ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（ﾌﾟﾛﾄｺﾙ）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　：

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

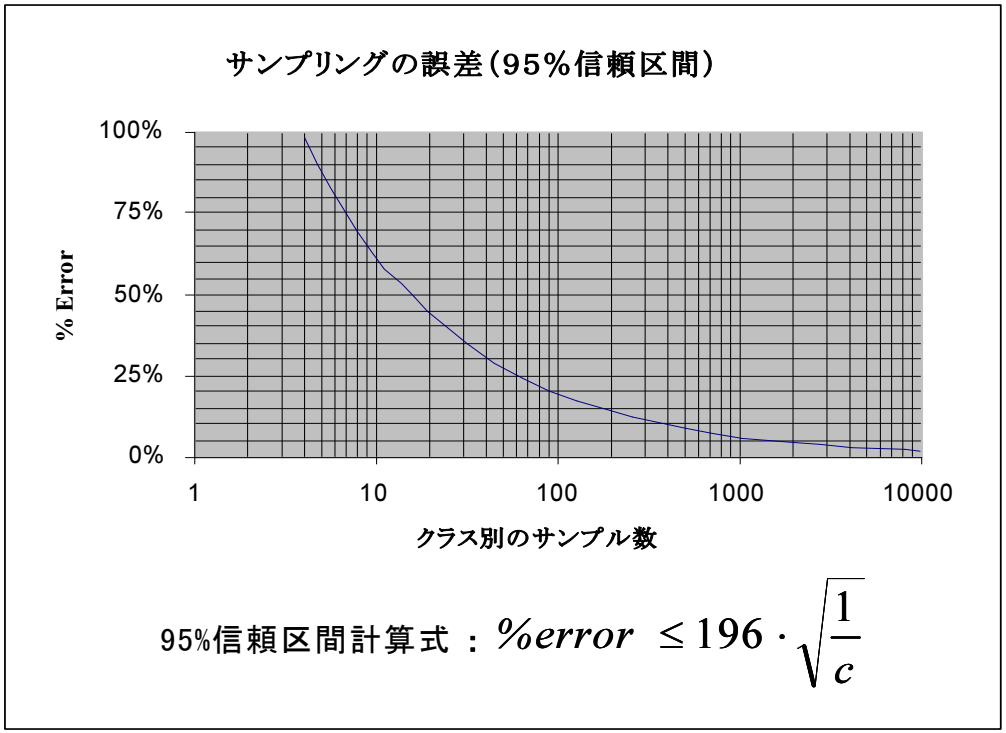
例：
入力したフレームの総数 = 1,000,000
サンプリングレート = 0.25%
総サンプル数 = 2,500
Voiceトラフィックのサンプル数 = 1,000
表示されるVoiceトラフィックのフレーム数は：

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

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

sFlow：サンプリングの誤差（解析精度）

サンプリングの誤差　➔　95%信頼区間によって分析

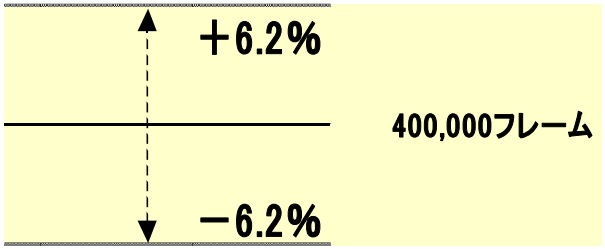


95%信頼区間計算式 ： $\%error \leq 196 \cdot \sqrt{\frac{1}{c}}$

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、

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

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。



sFlow：サンプリング分析のコンセプト

- 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（ サンプリ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
  - サンプリ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
- サンプリングベースのテクノロジの為、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

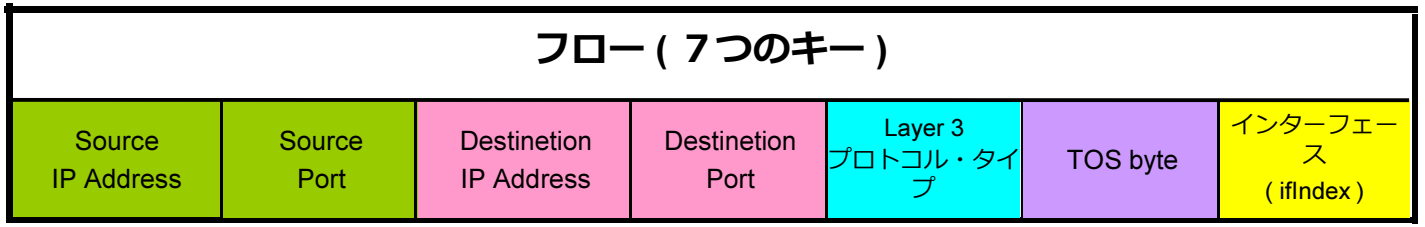
NetFlow

- 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）

NetFlow

- 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

CISCO



- 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 vs NetFlow

- sFlow
  - RFC3176として公開（機器ベンダ非依存のオープンな規格）
  - サンプリングベース
  - 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）

InMonTrafficSentinelのご紹介

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

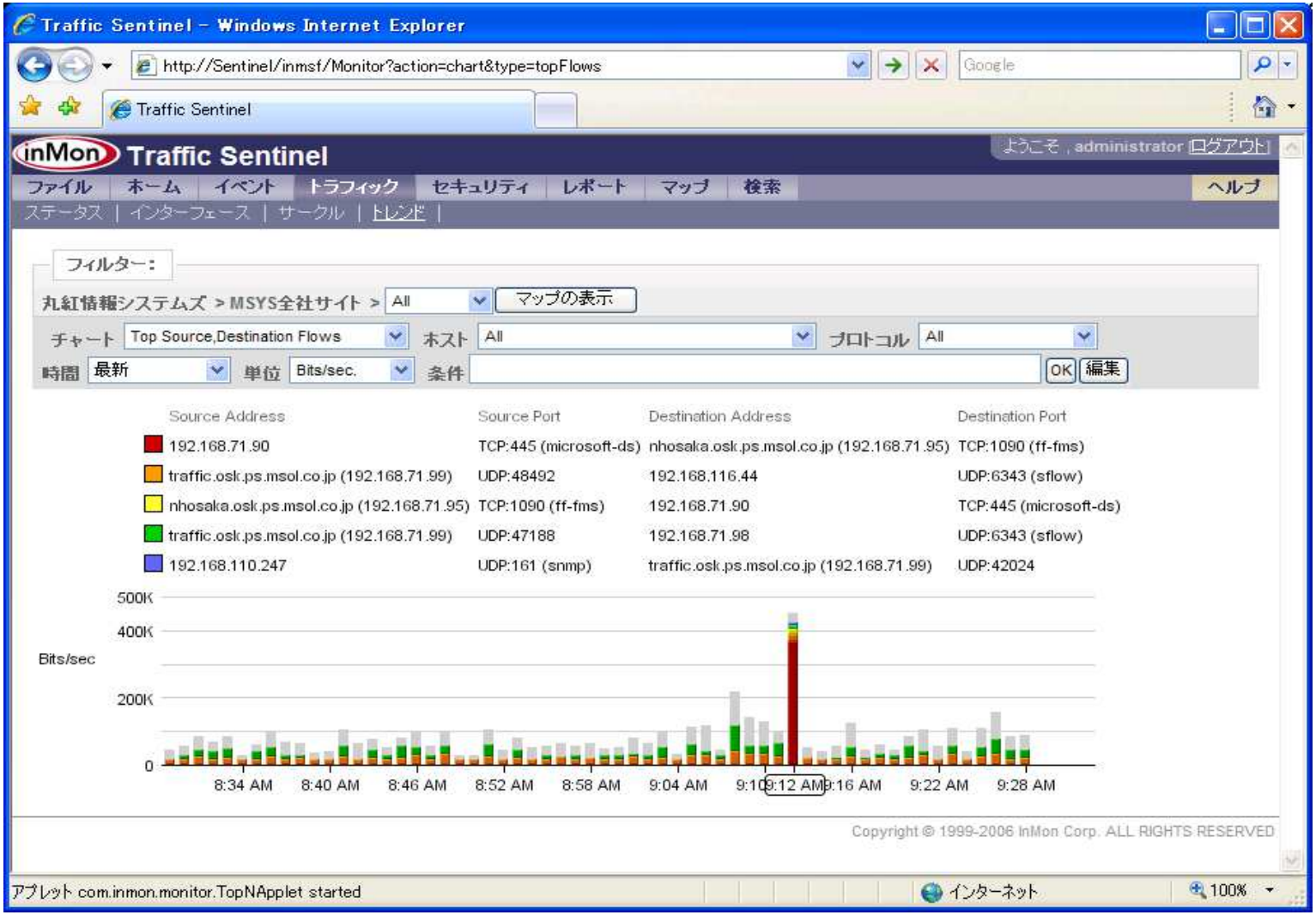
を、サポートしています。

InMonTrafficSentinelの各種機能

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

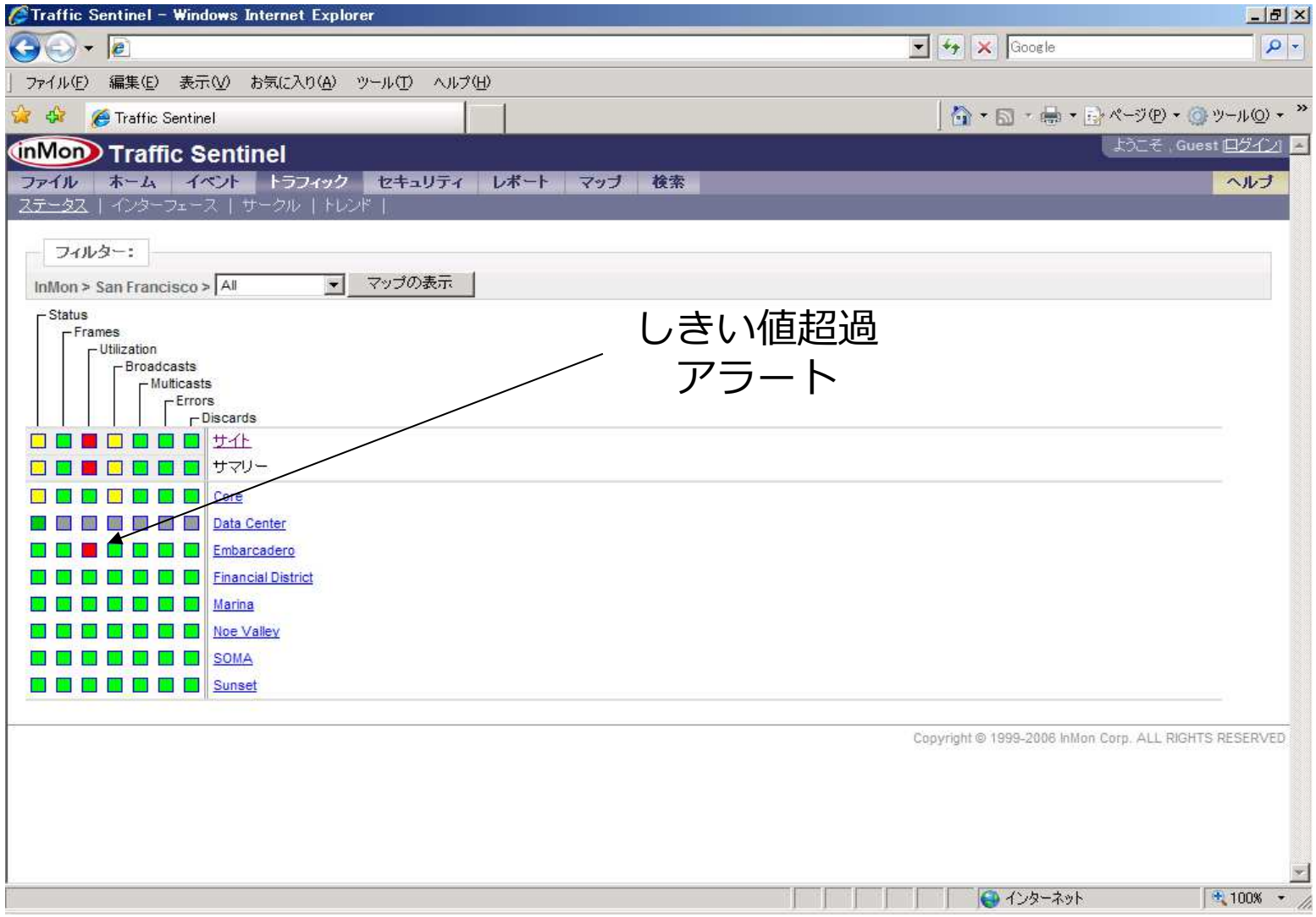
日本語版の提供

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



ネットワーク管理：リアルタイムでの輻輳管理

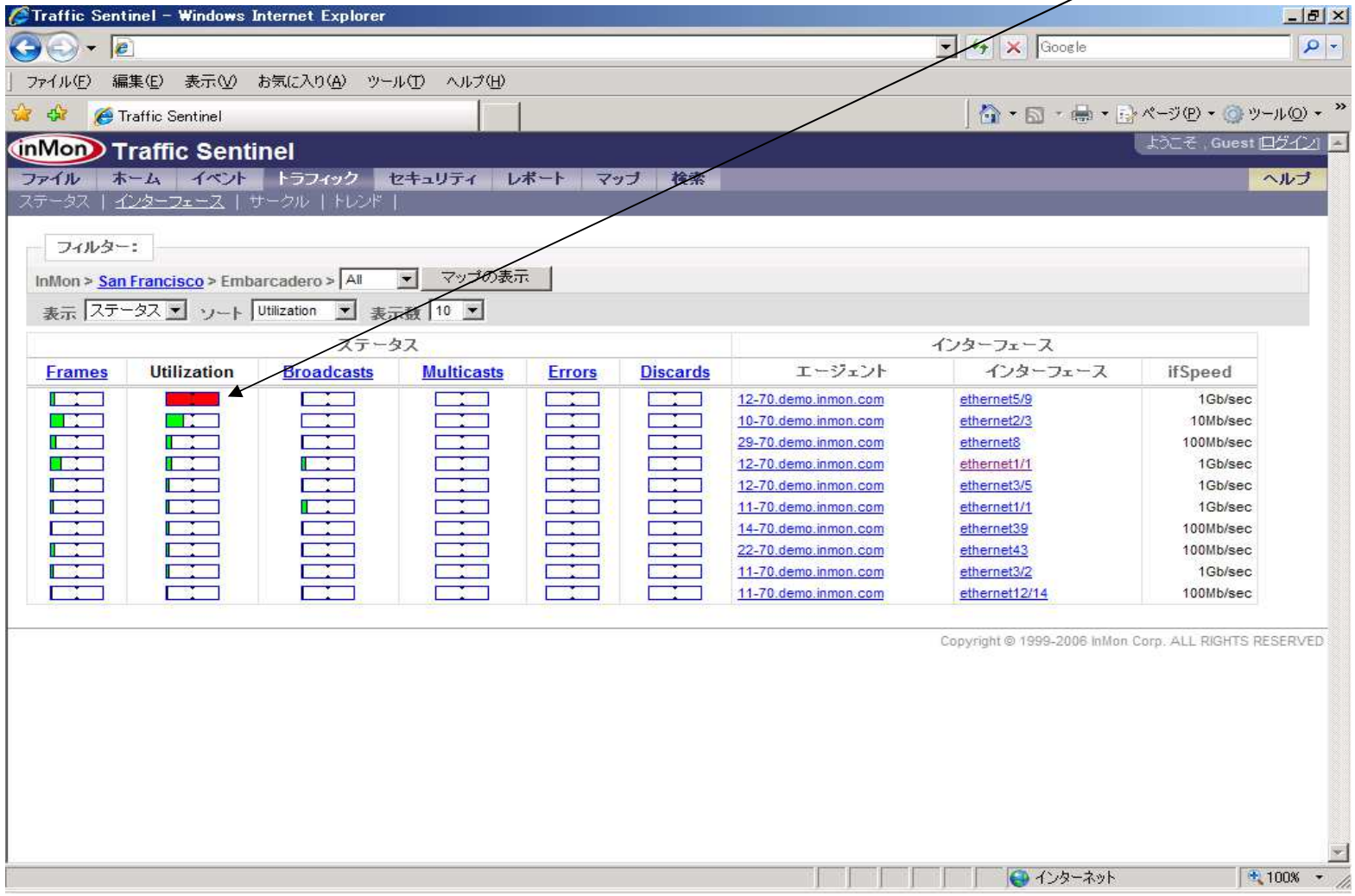
1. プロアクティブな問題の把握（しきい値分析）



ネットワーク管理：リアルタイムでの輻輳管理

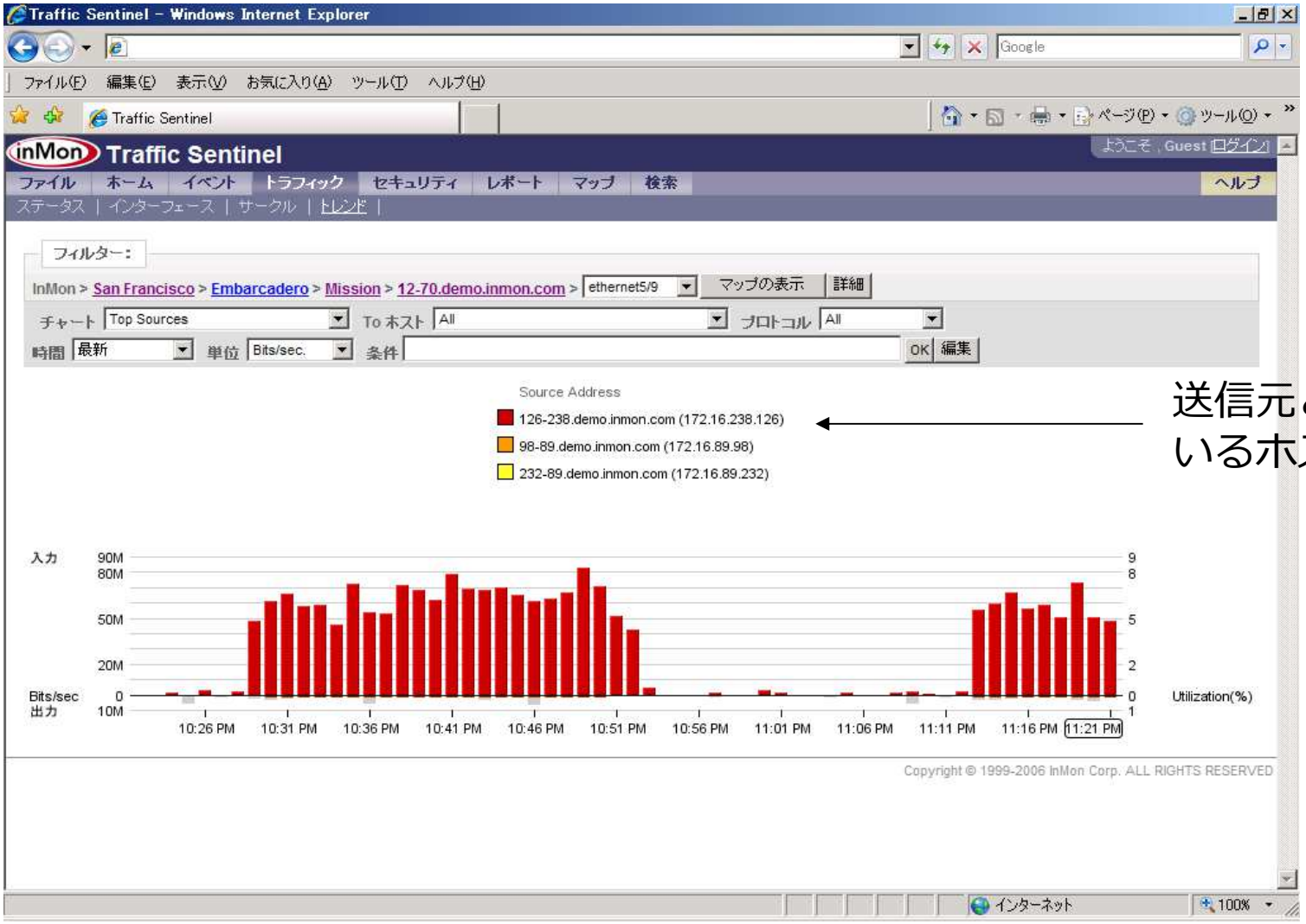
2. 問題が発生してインターフェースはどこか？

問題の指摘



ネットワーク管理：リアルタイムでの輻輳管理

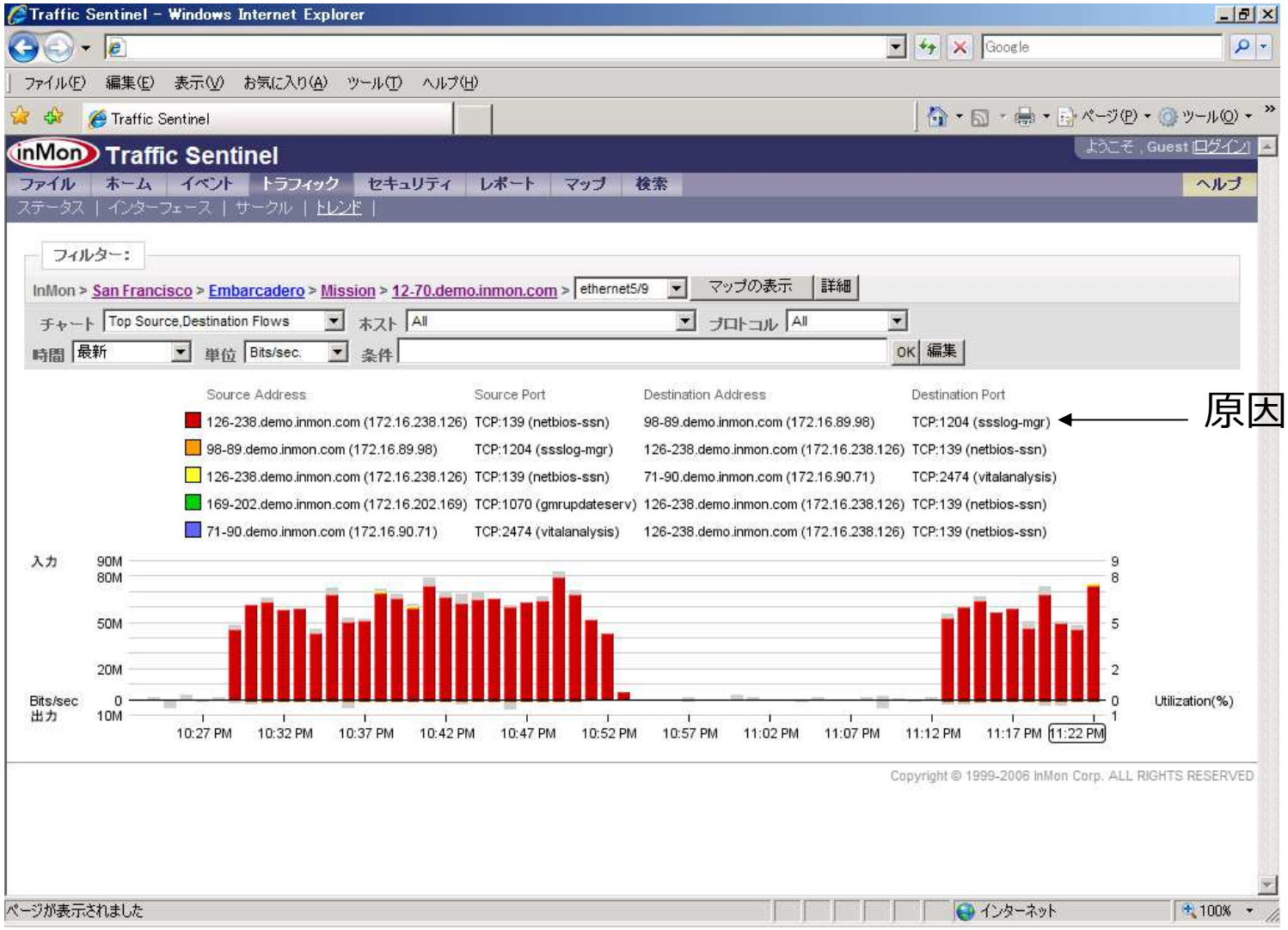
3. 問題を起こしているホストは誰か？



送信元となっているホスト

ネットワーク管理：リアルタイムでの輻輳管理

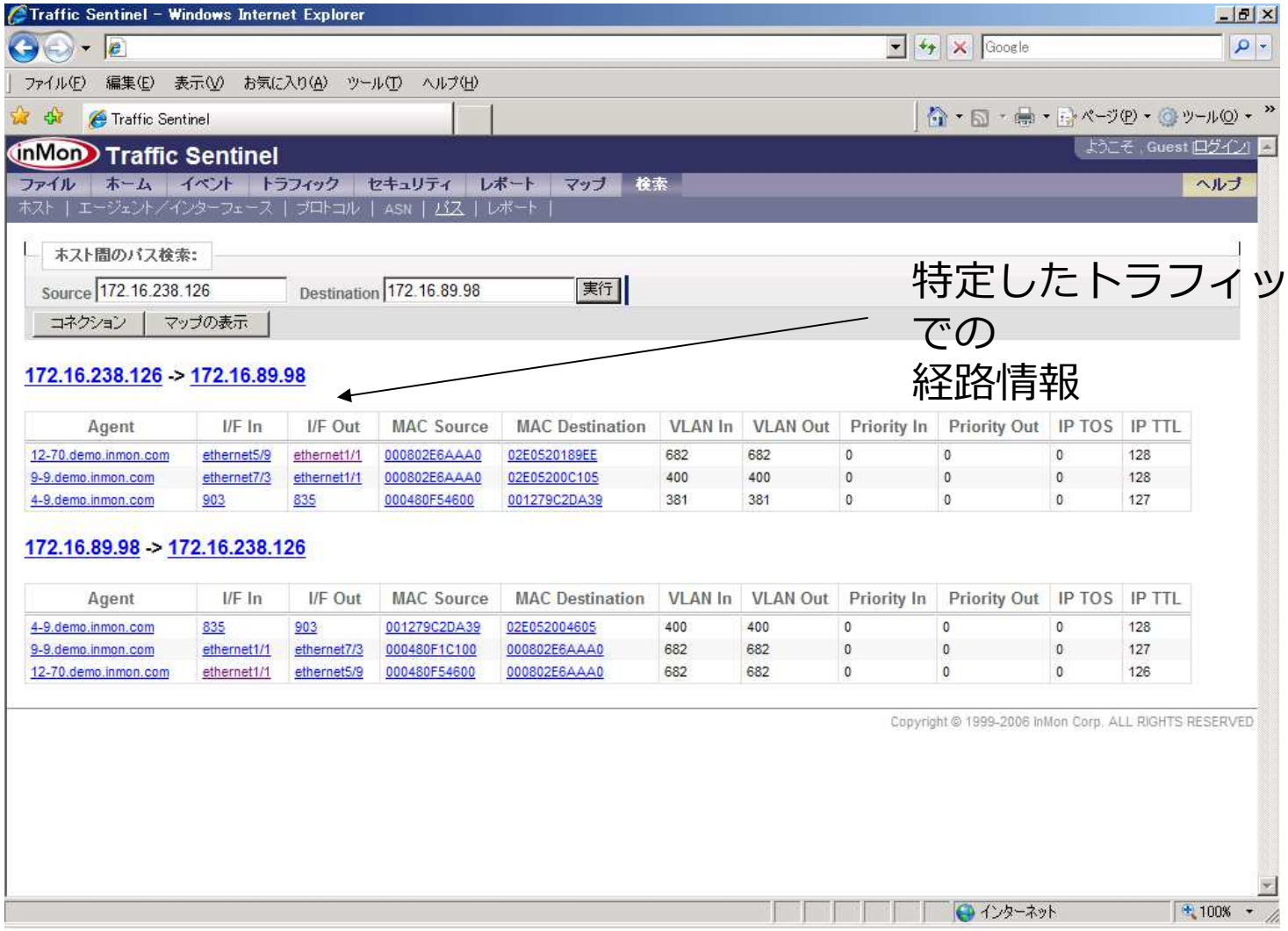
４．どの様な通信をしているか？（トラフィックフローの把握）



原因の把握

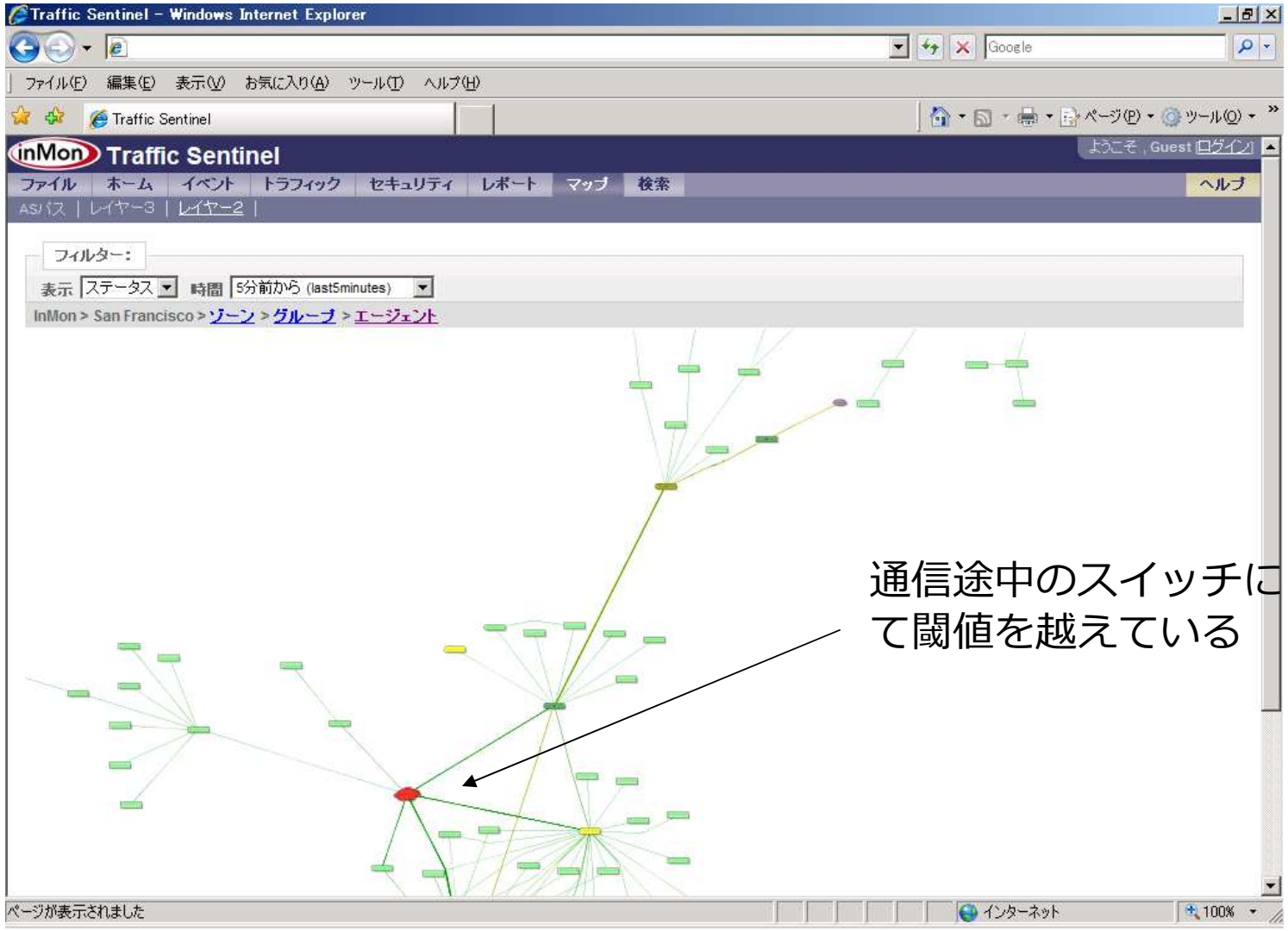
ネットワーク管理：リアルタイムでの輻輳管理

5．トラフィックフローの詳細や経路情報の把握



ネットワーク管理：リアルタイムでの輻輳管理

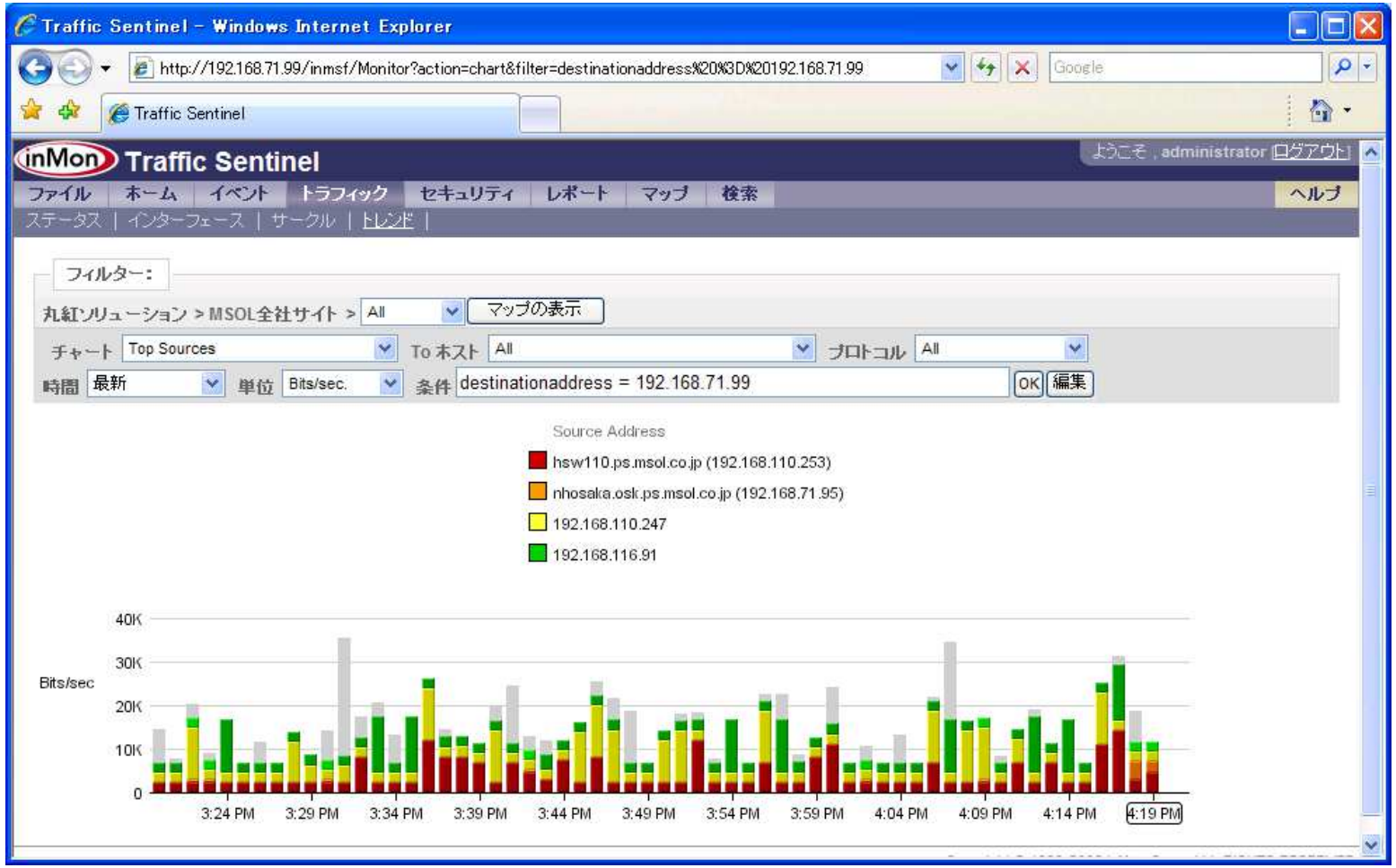
6．トポロジーマップ上での把握（経路情報）



ネットワーク管理：特定サーバーへのアクセス

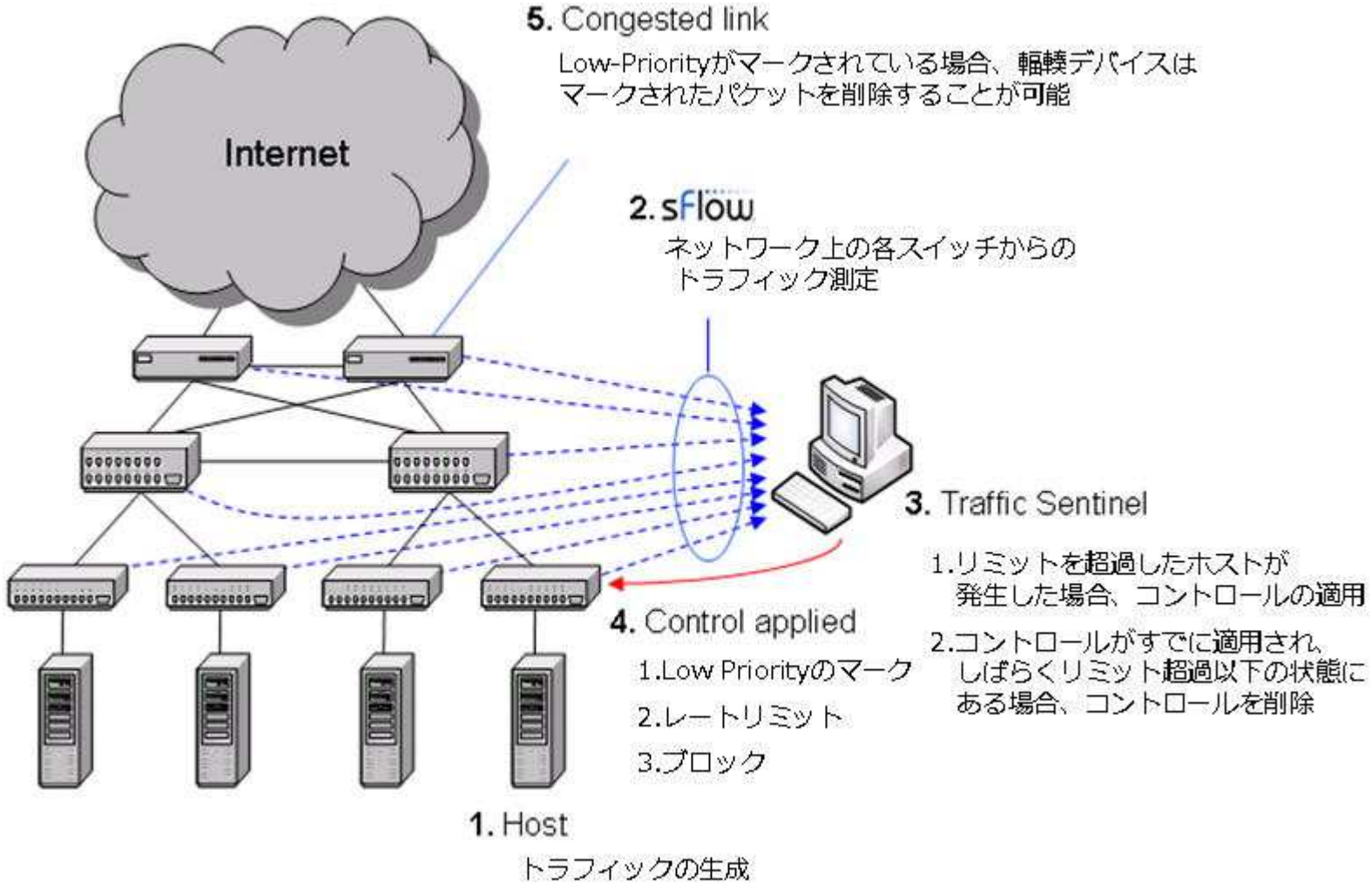
特定のサーバーへのアクセス状況の確認

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。



ネットワーク管理：コントローラー

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。



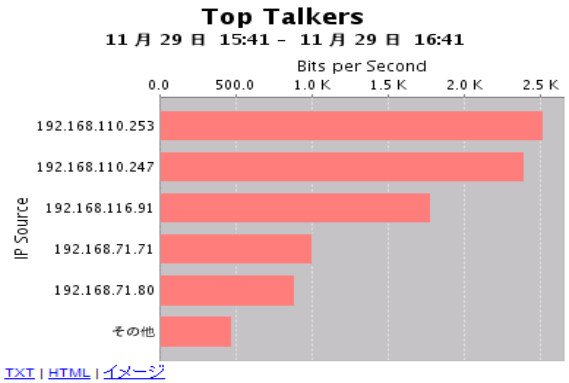
レポーティング機能

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

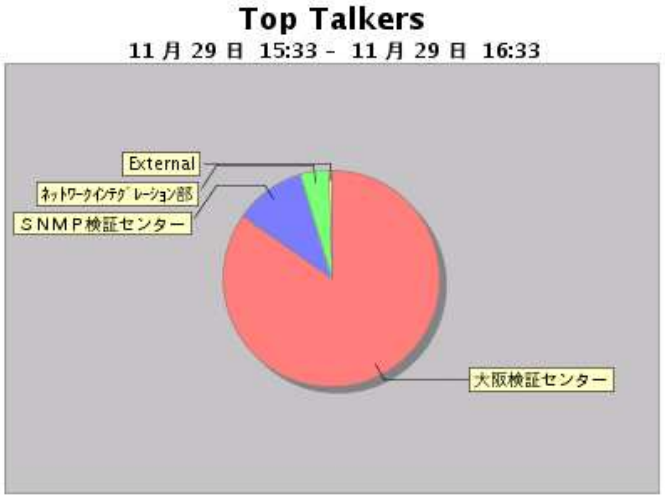
部門別トップ・ユーザ・レポート

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



アカウンティング・レポート

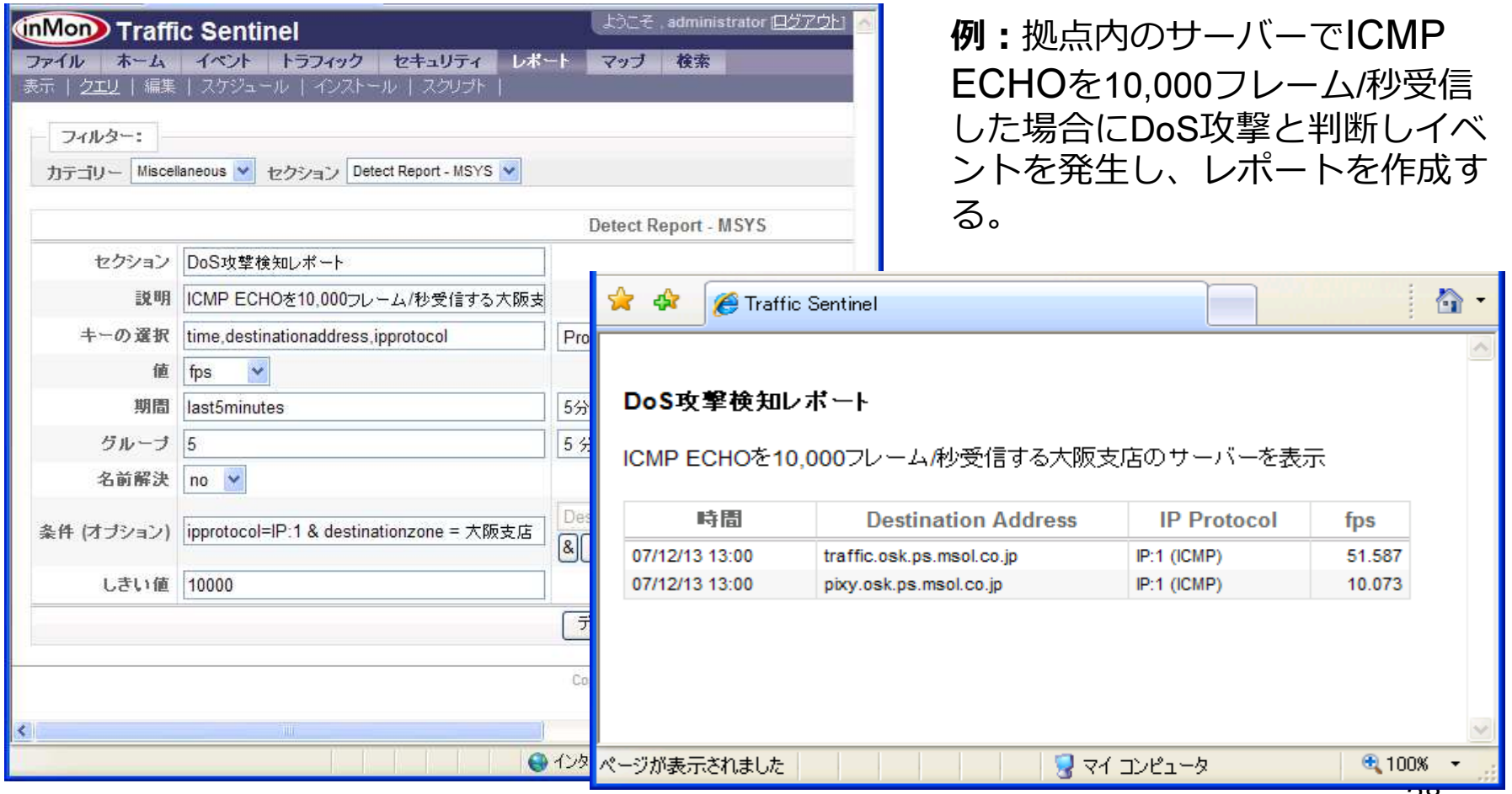
Recent Traffic Totals by Time

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

レポーティング機能：障害発生検知レポート

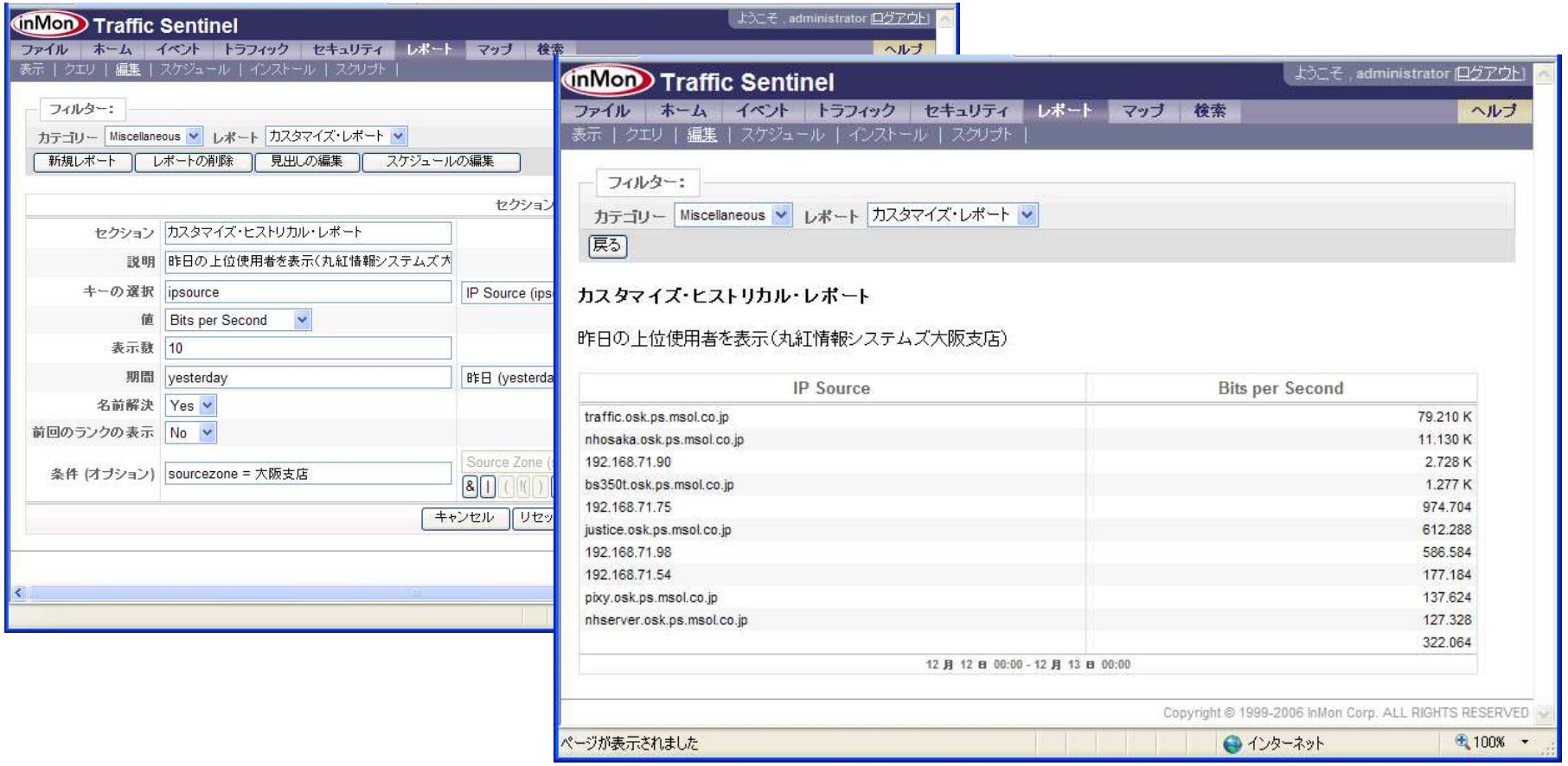
- トラフックの内容に対ししきい値を設定し超過時にイベントを発生させる
  - しきい値：トラフィック（プロトコル・アドレス・グループなど）に対して設定
  - スケジュール化し、超過時にイベントを発生させる



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。

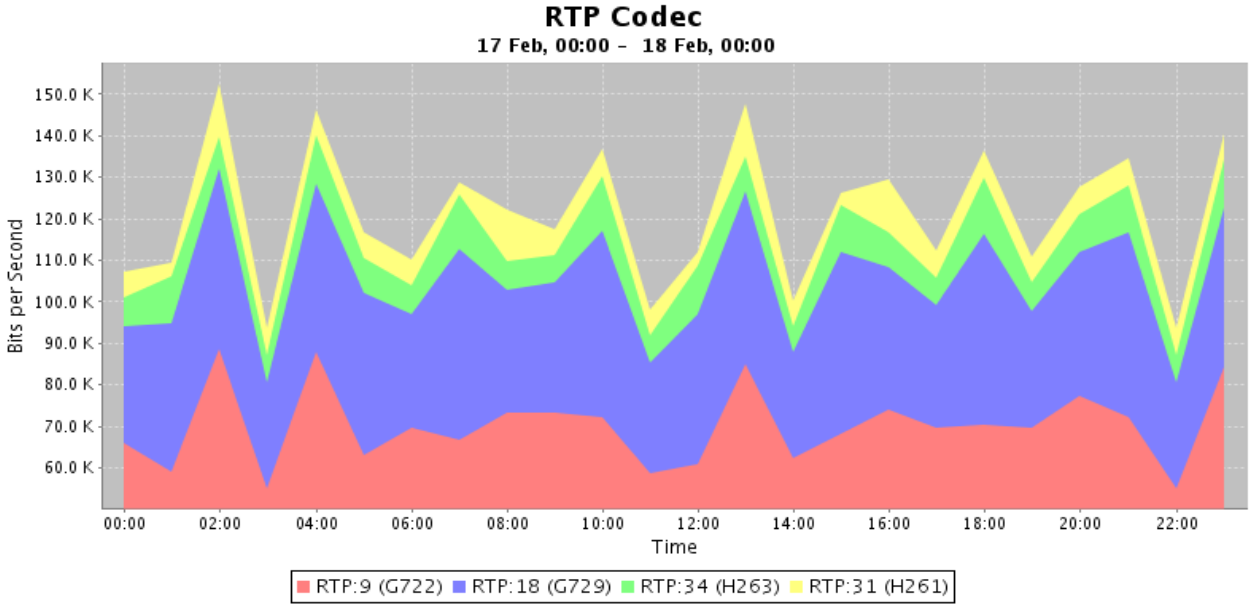
レポーティング機能：カスタマイズ・レポート

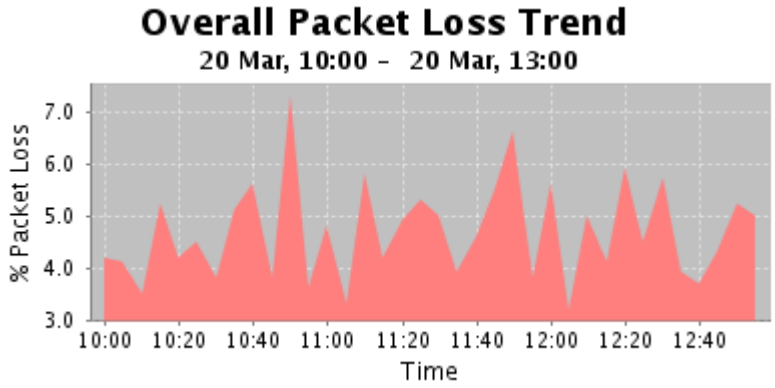
- 豊富なテンプレートを編集して、カスタマイズ・レポートが作成可能
  - 文言・表示情報・表示情報のフィルタリングなどの編集が可能
  - 定型レポートはスケジュール化



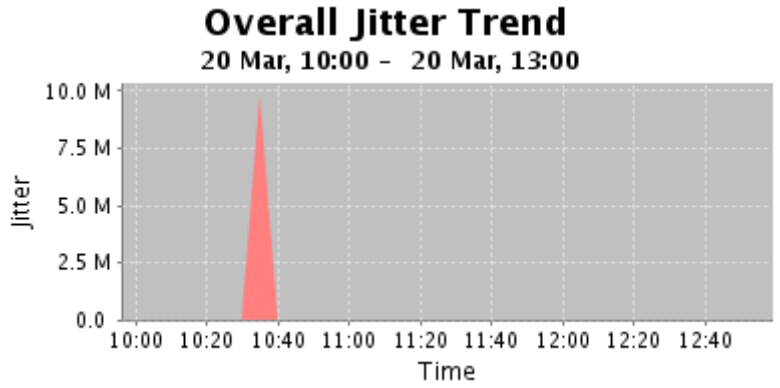
レポーティング機能：VoIP-RTPレポート

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。



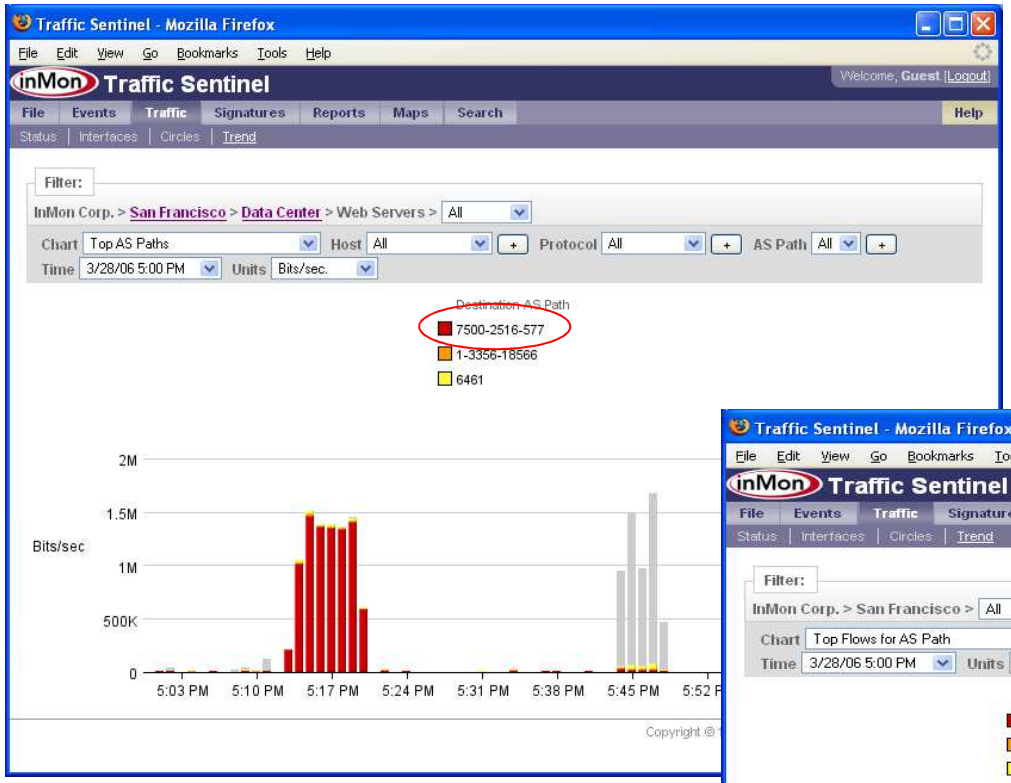


Packet loss は、均一的に継続。

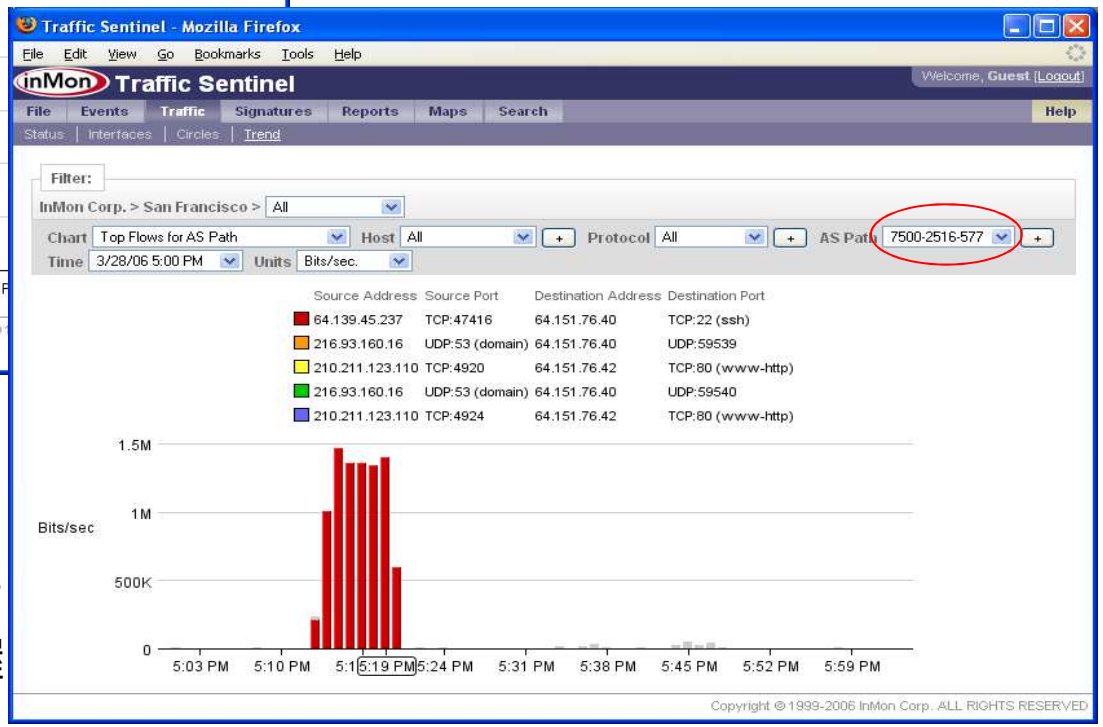


しかし、Jitterは10:35にスパイク。

レポーティング機能：ASパスとパス上のフロー



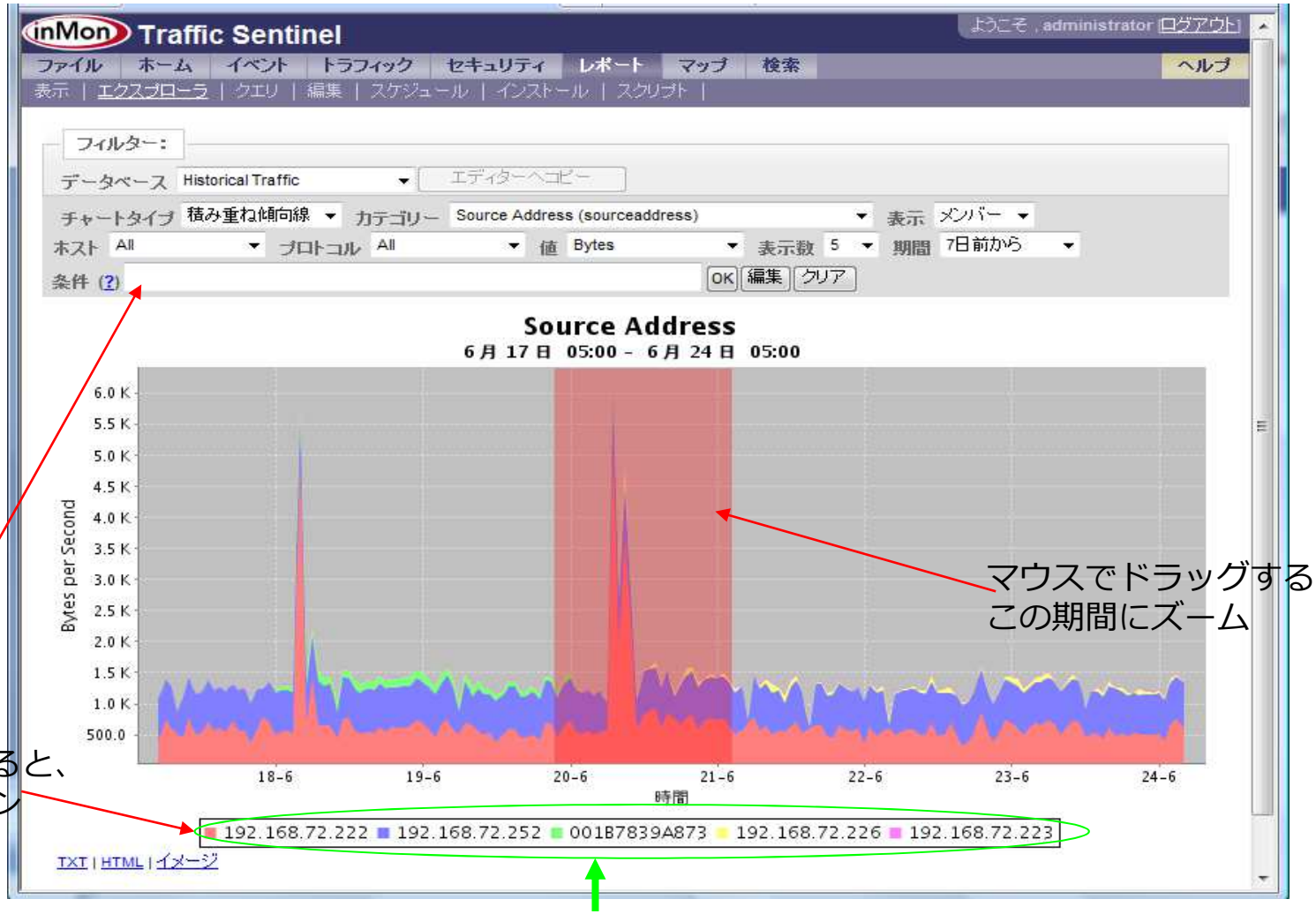
7500-2516-577 は、最も激しく使用されているASパスで、また、パスも長い。



このASパスによって転送されているフローの把握

レポーティング機能：エクスプローラ

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

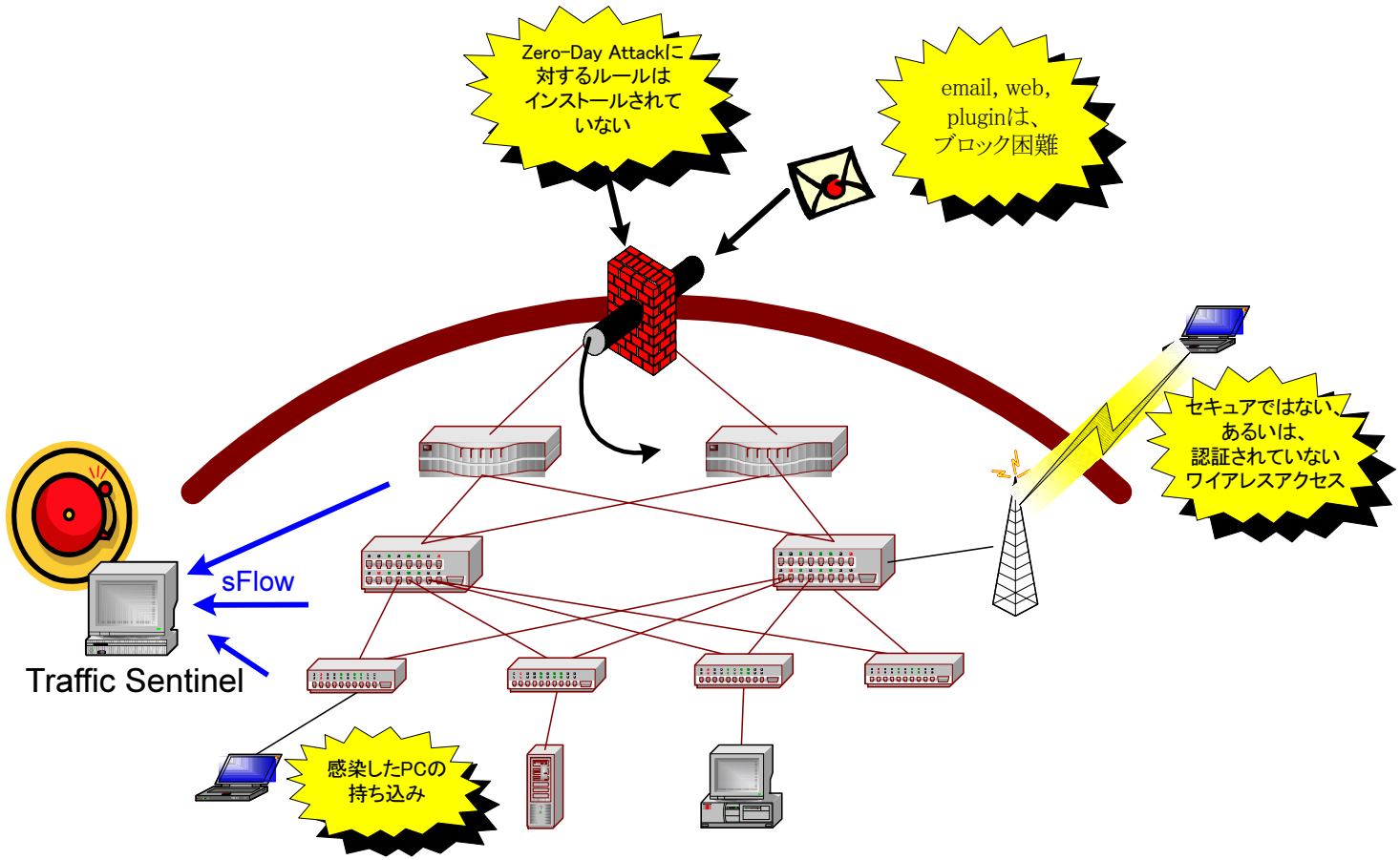


マウスでドラッグすると、
この期間にズーム

凡例をクリックすると、
条件（フィルタリング）に追加

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

セキュリティ管理：シグネチャーによるアラート

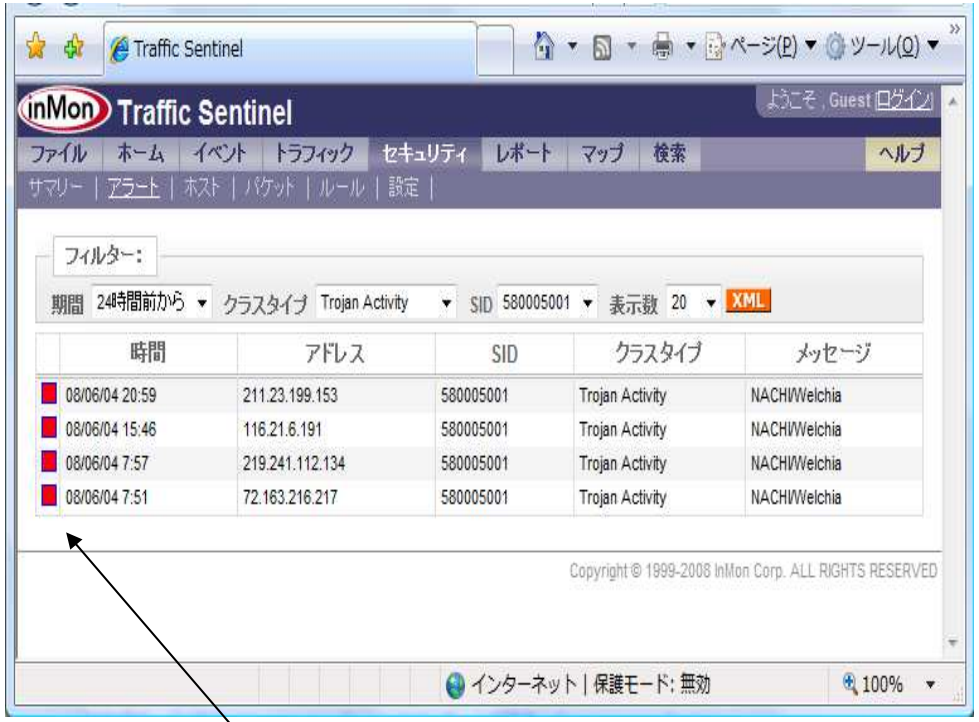
sFlow データグラム

packet header	In/out i/f	sampling parms	forwarding	user ID	URL	i/f counters

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;¥
)
==================================
```

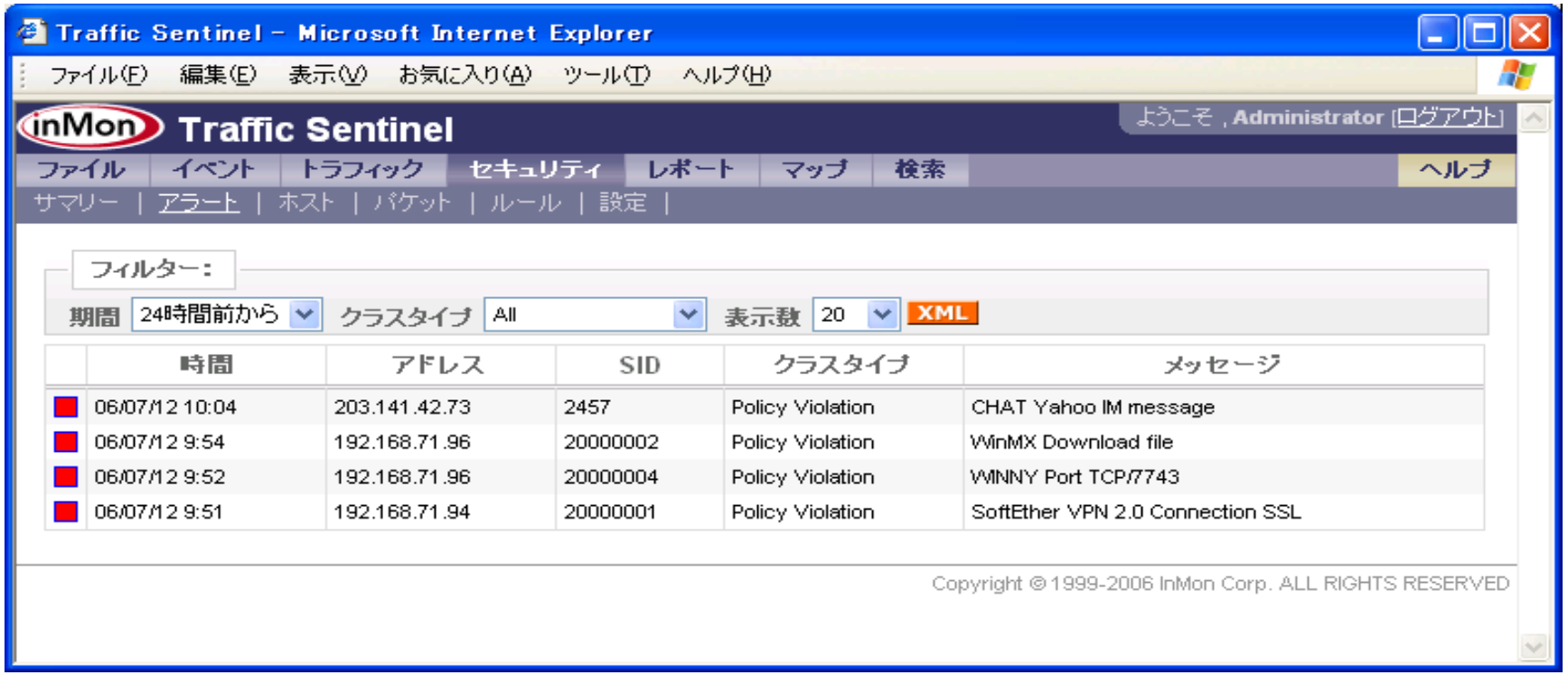


トラフィックがルールにマッチした時、アラートを発生

セキュリティ管理：ポリシー違反の検知

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



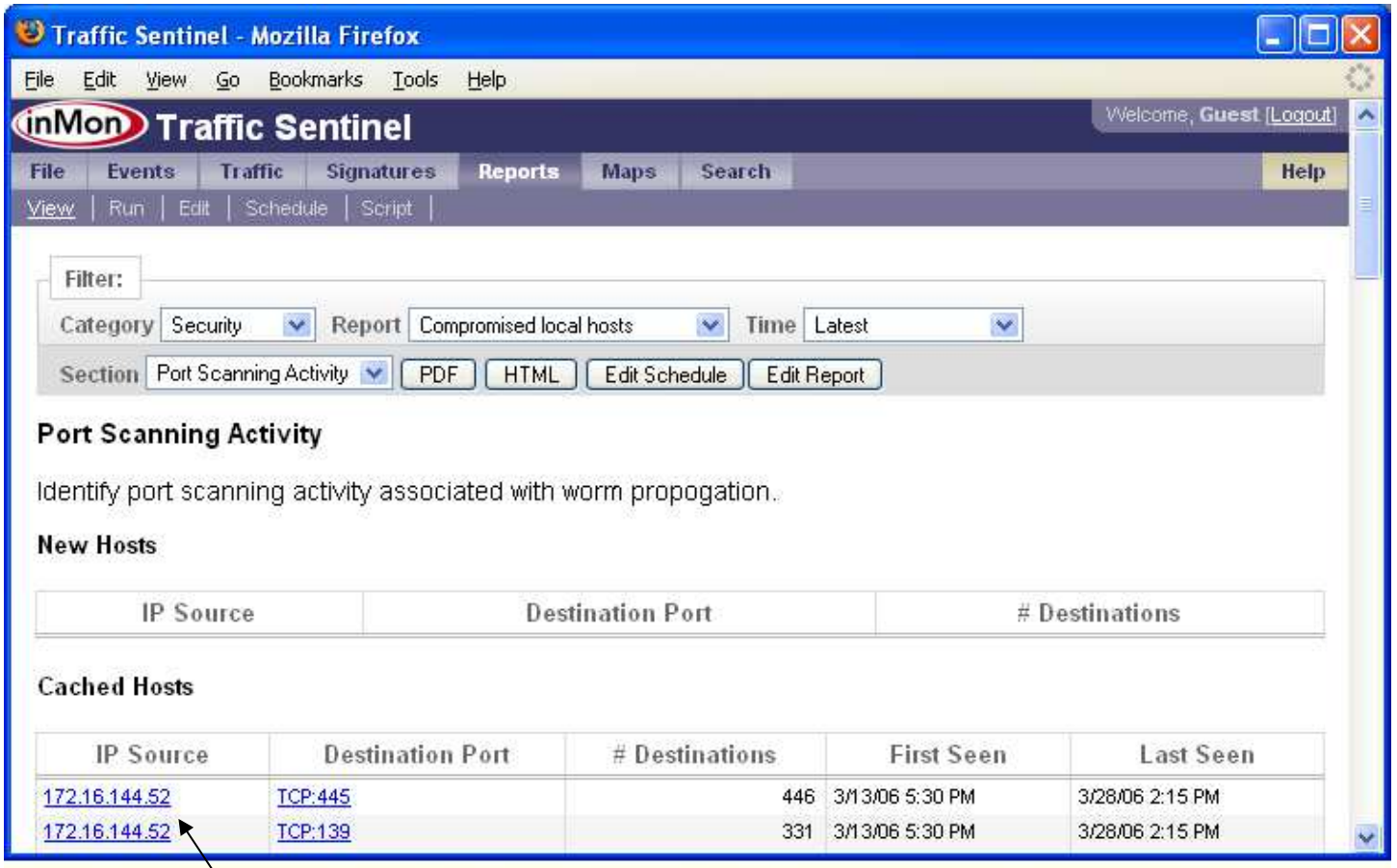
検知の為のシグネチャー例（SoftEther）：

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

セキュリティ管理：振る舞い検知

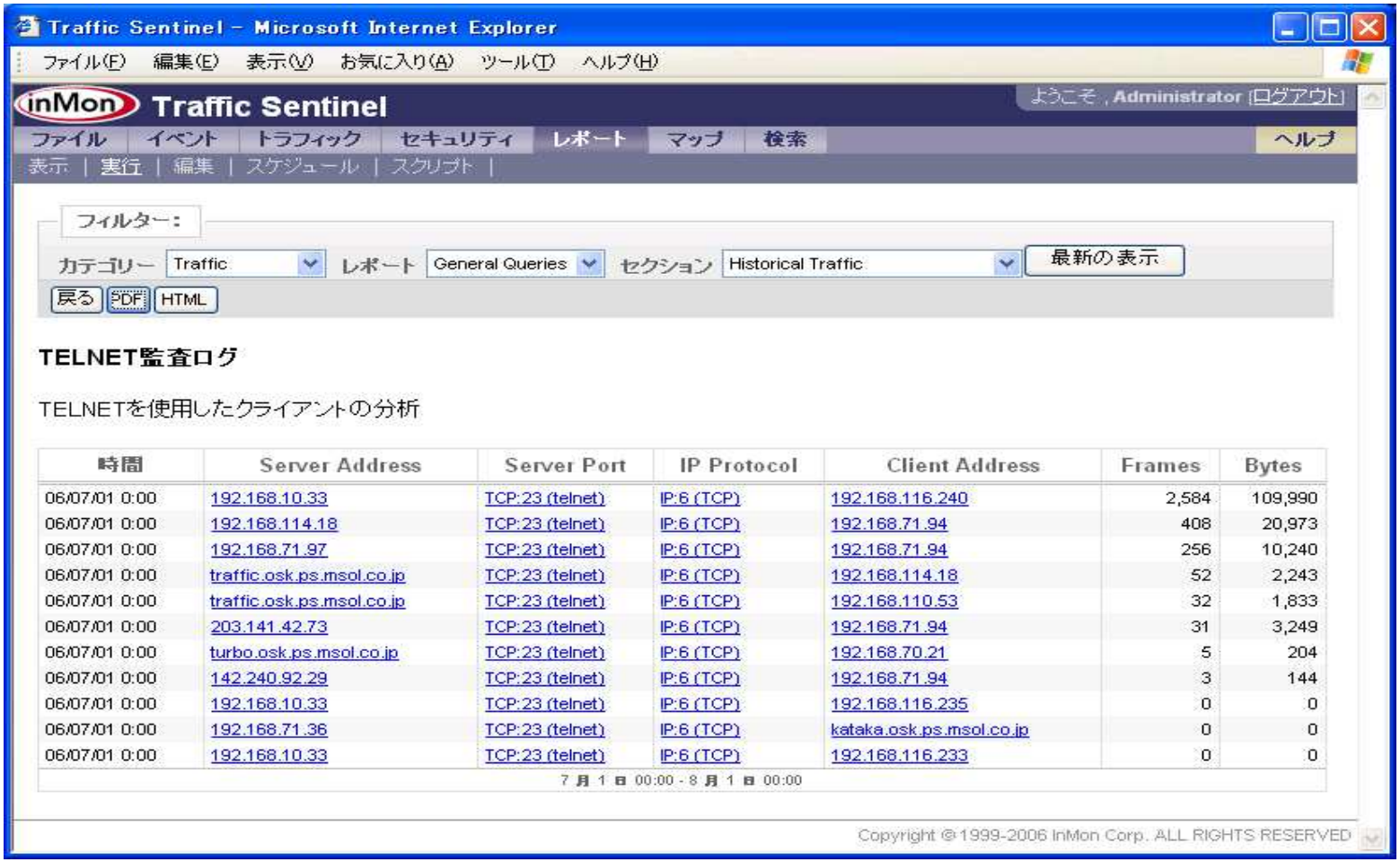
ポートスキャンや新種のウイルス・ワームの検知：



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。

セキュリティ管理：履歴データによる監査

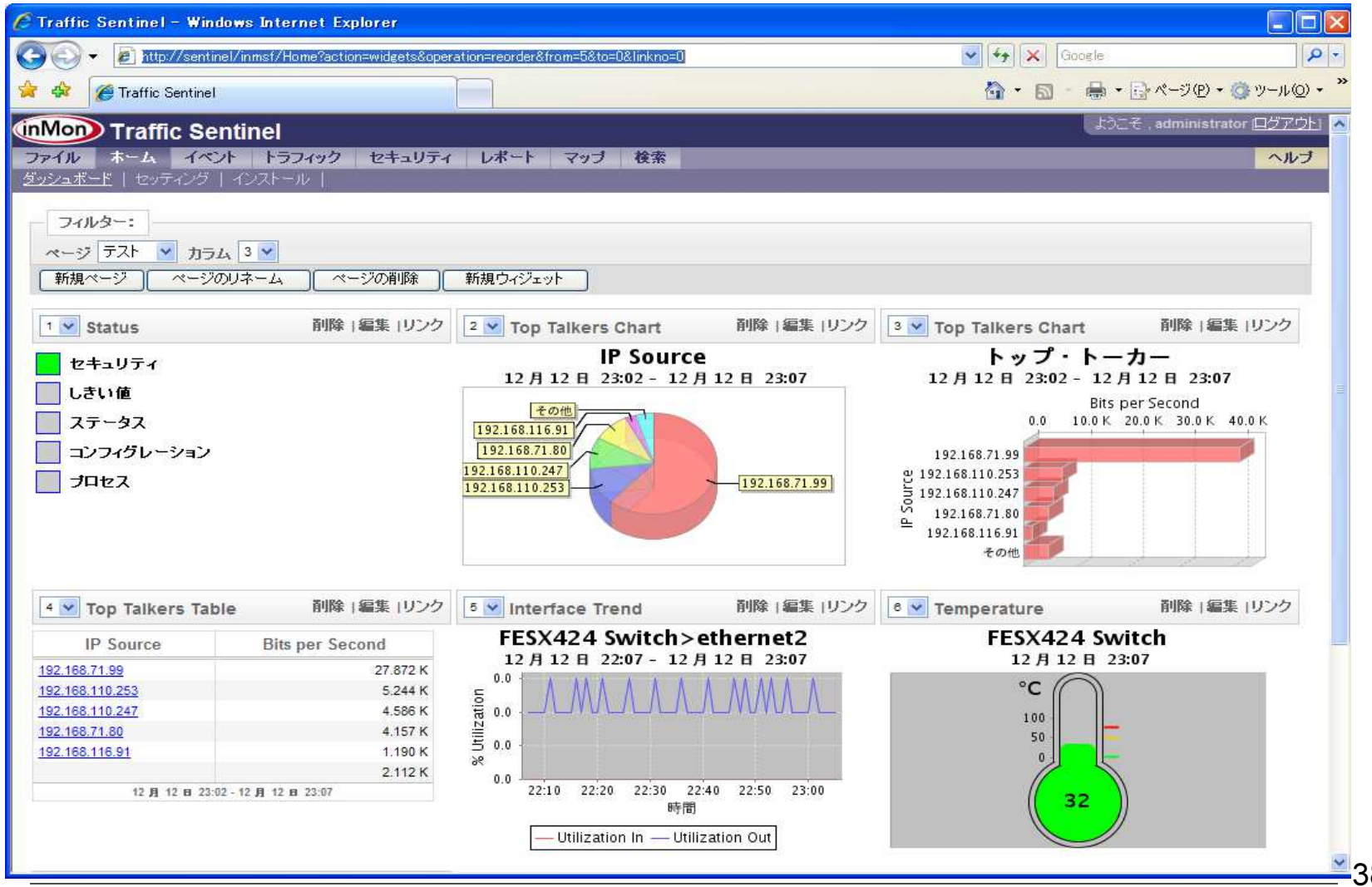
監査：フローログ - サーバーへのTELNET接続者のログ



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

ダッシュボード機能

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。

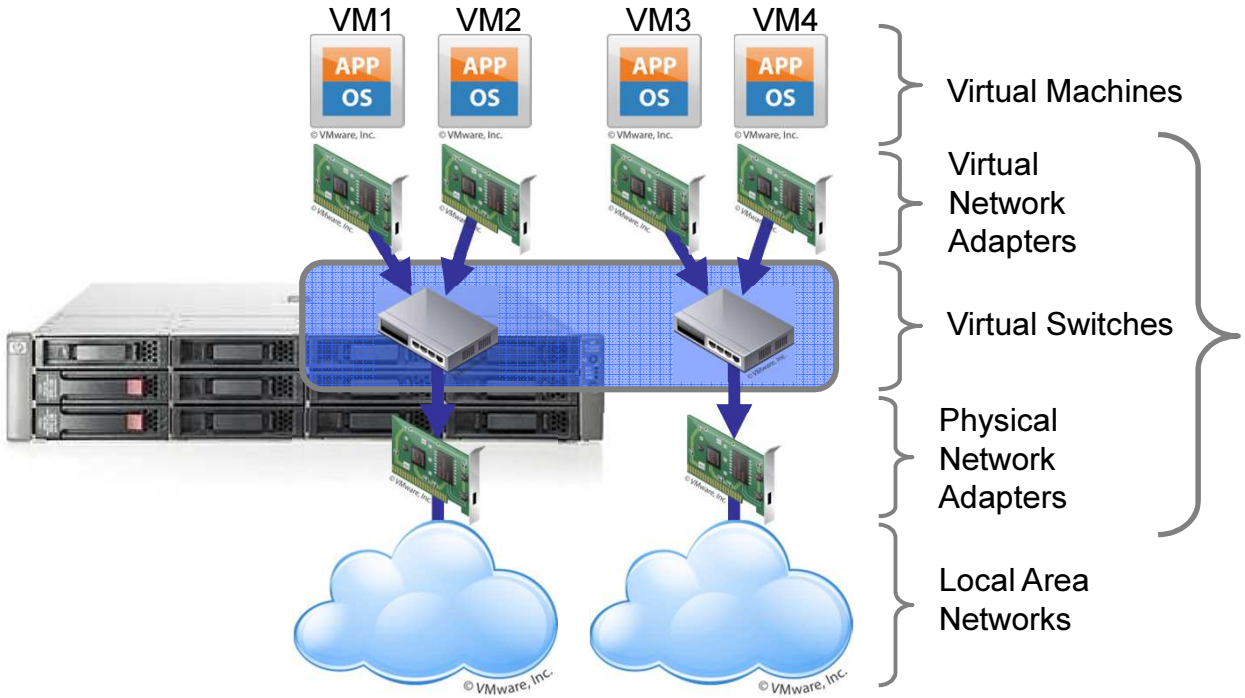


Host sFlow

- 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

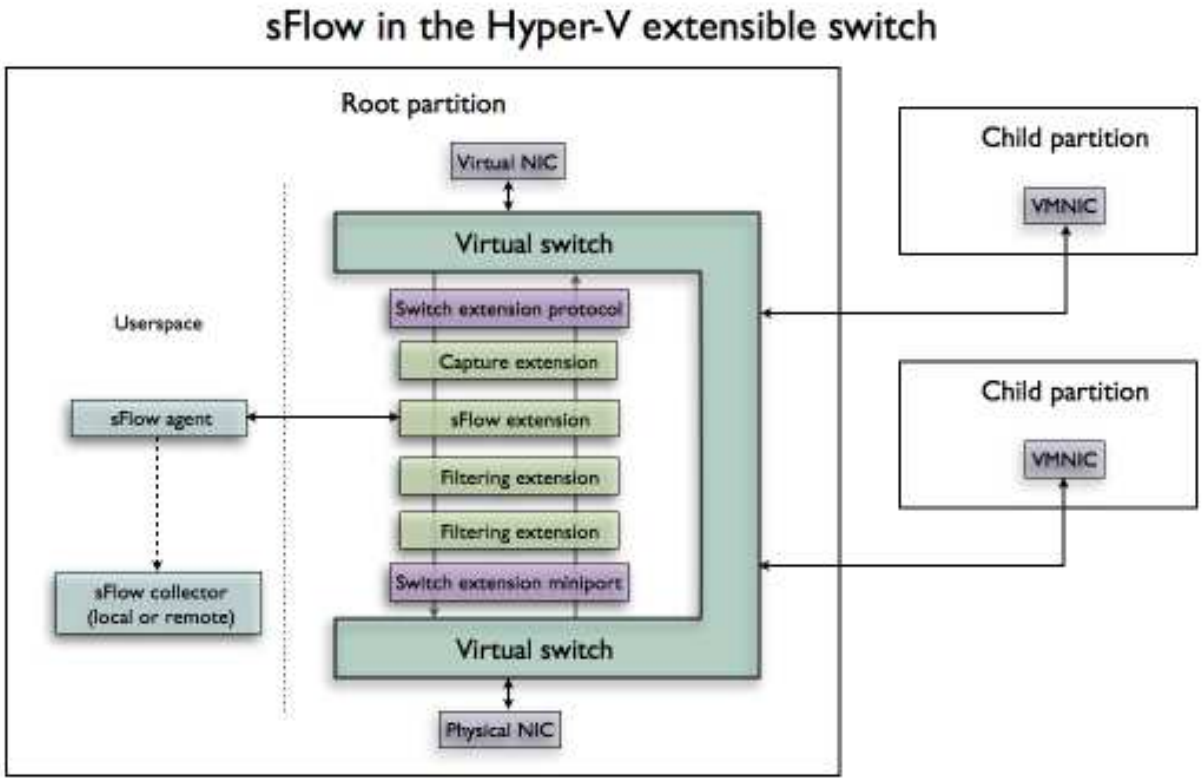
仮想化環境 sFlow



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)

Microsoft Windows 2012 Server Hyper-V 用 sFlowエージェント



- 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

Application sFlow

- 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

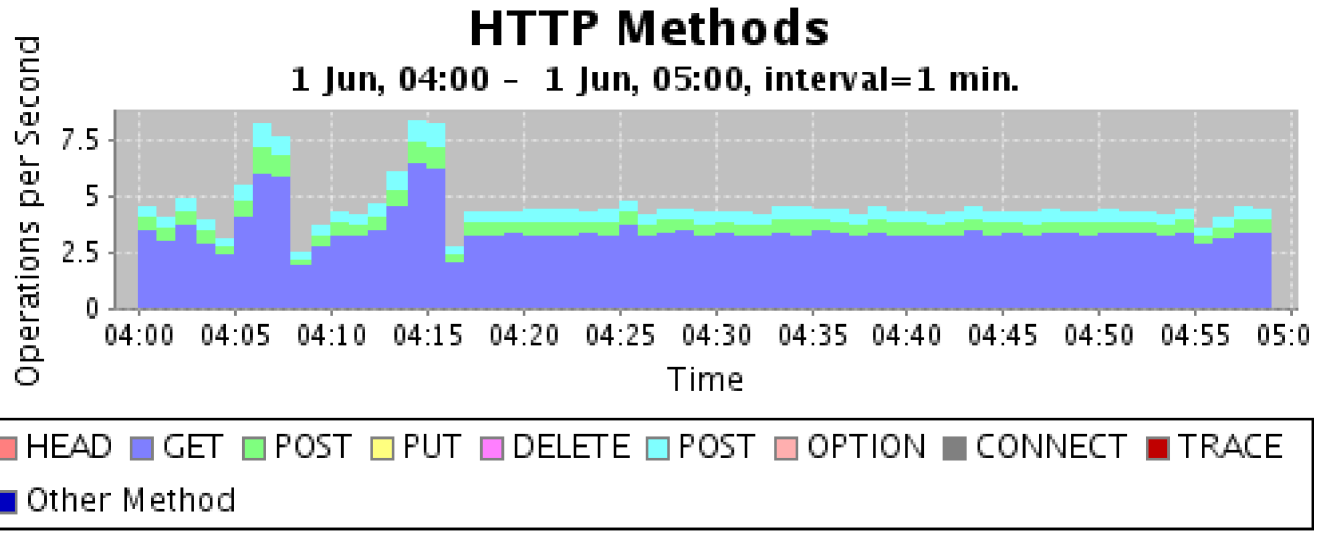
例:

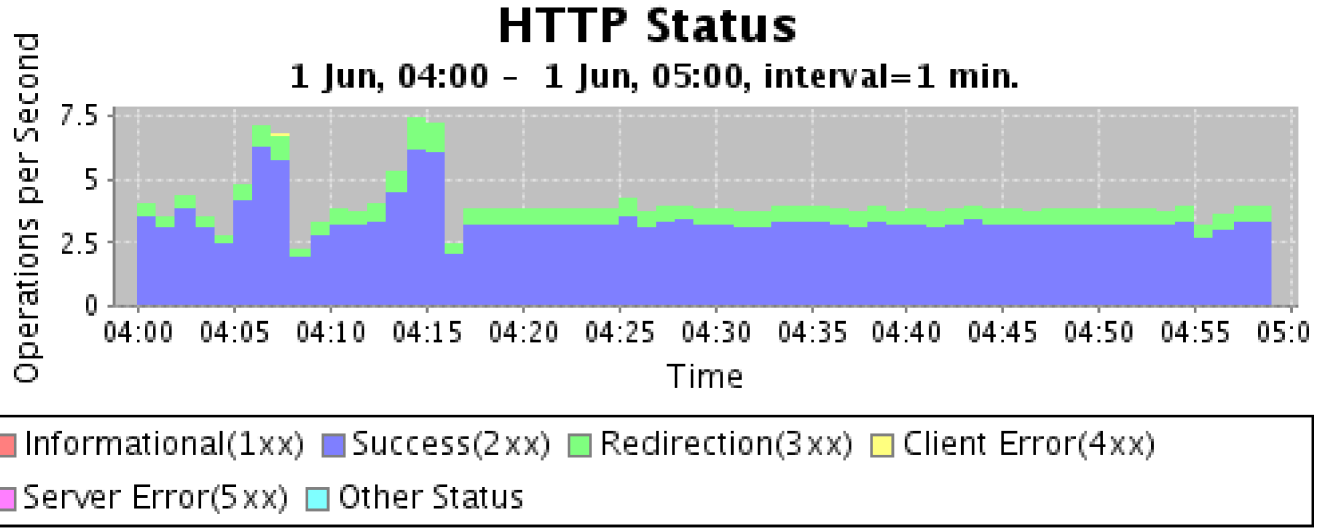
- NFS/CIFS transactions
  - File path, bytes, response time, socket
- HTTP requests
  - URL, user agent, mime type, bytes response time, socket
- Memcached lookups
  - Key, value-bytes, hit/miss, socket
- Database queries
  - Query#, response time, socket

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。

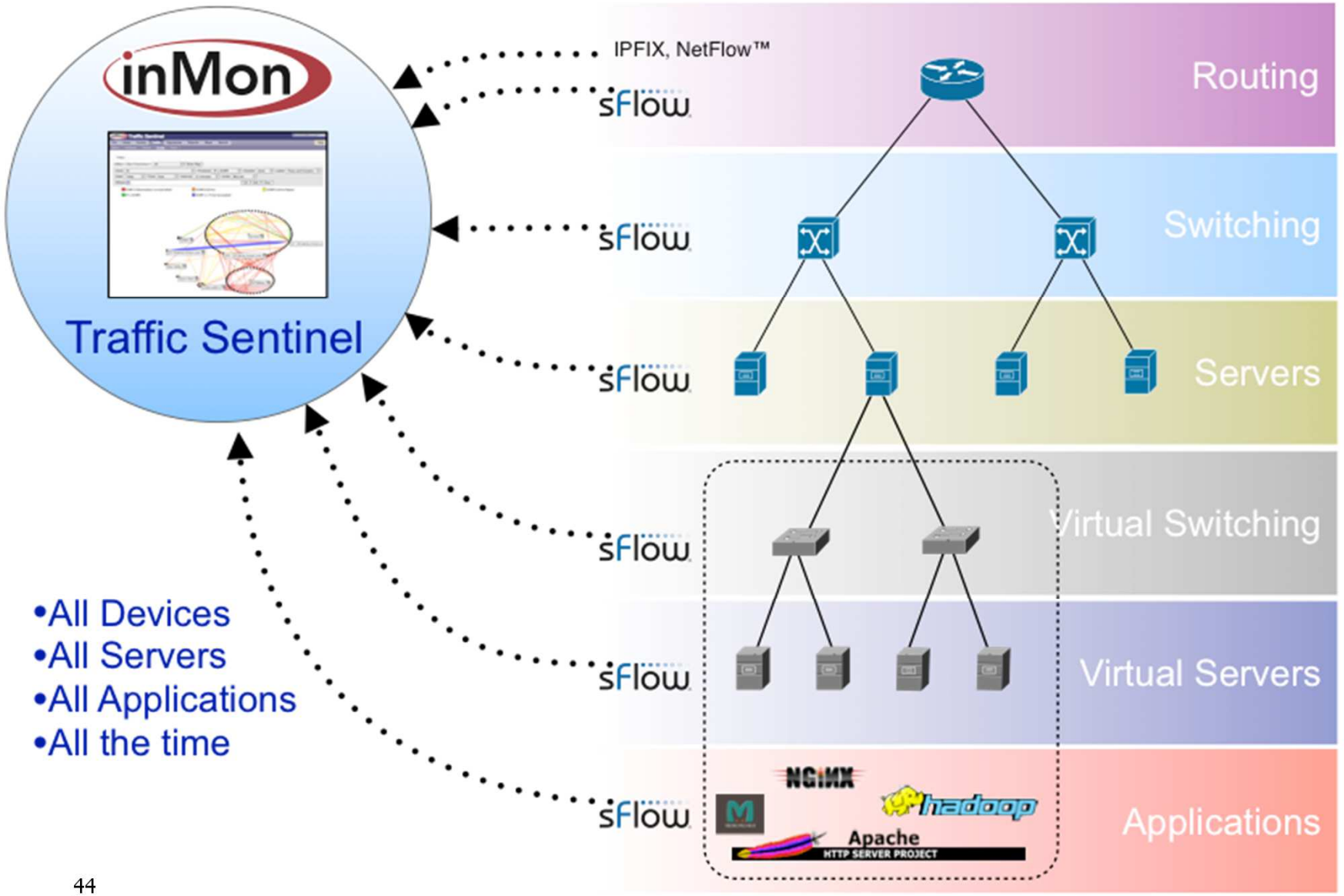
参照:http://www.marubeni-sys.com/network/inmon/pub/inmon/tutorials6/applications.php

Application sFlow：transactions

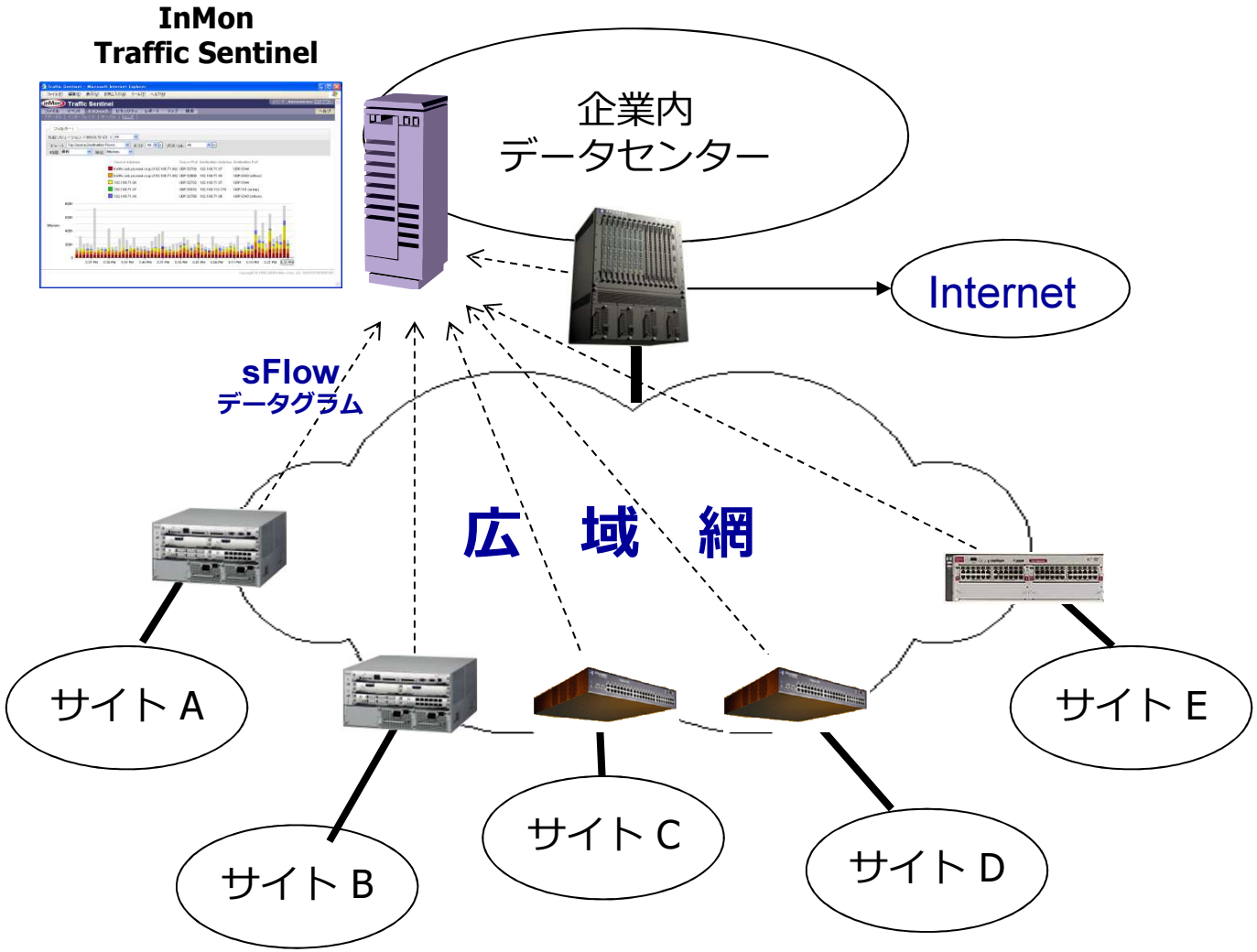




TrafficSentinelは、各種Flowデータを収集・分析

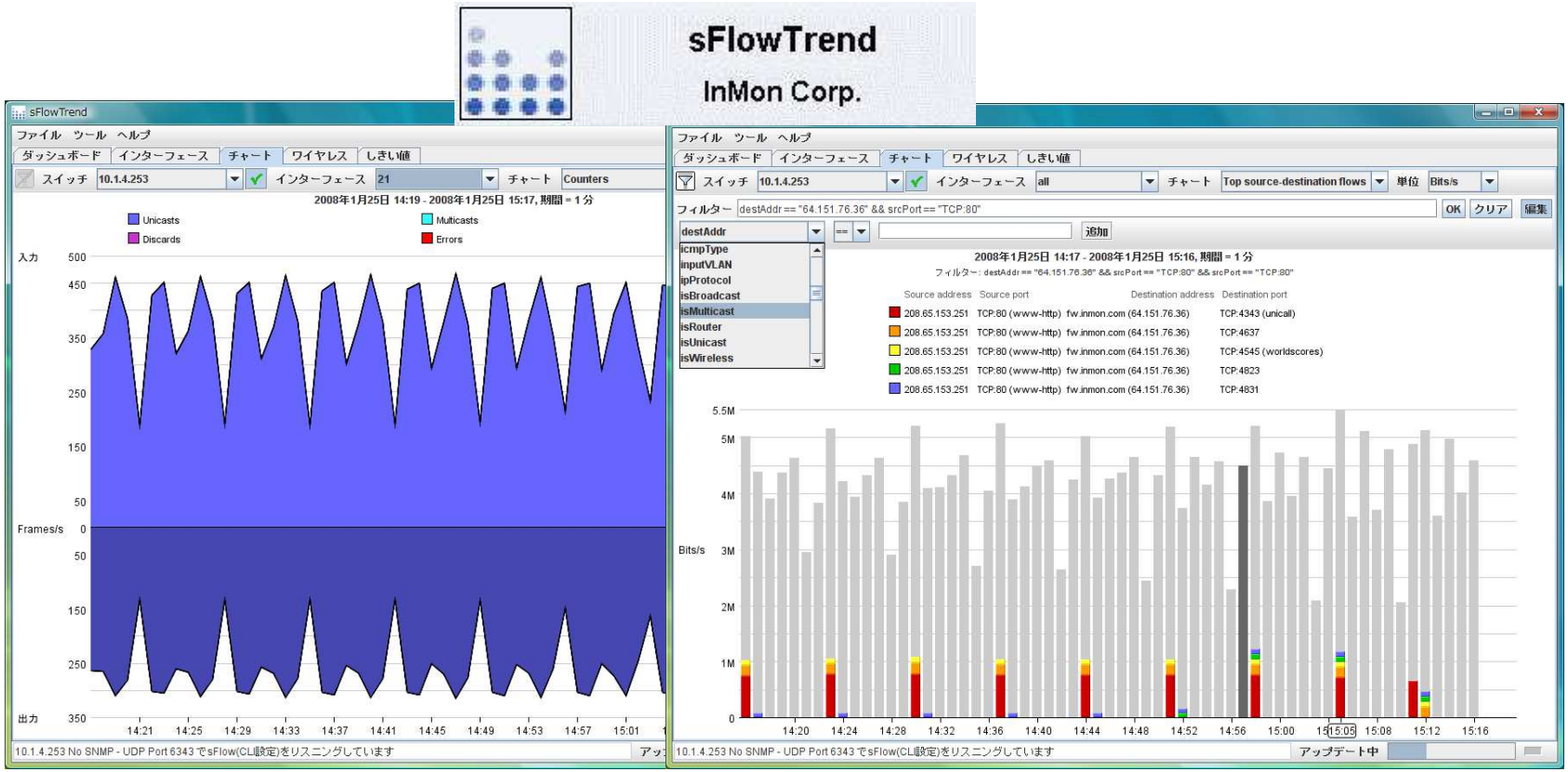


ケーススタディー


InMon
Traffic Sentinel
企業内
データセンター
Internet
sFlow
データグラム
広　域　網
サイト A
サイト B
サイト C
サイト D
サイト E

sFlowTrendのご紹介

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ー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

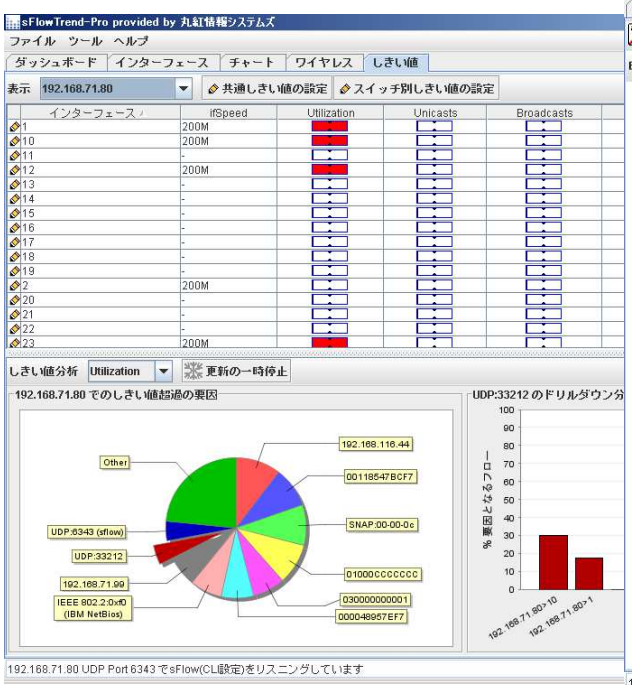


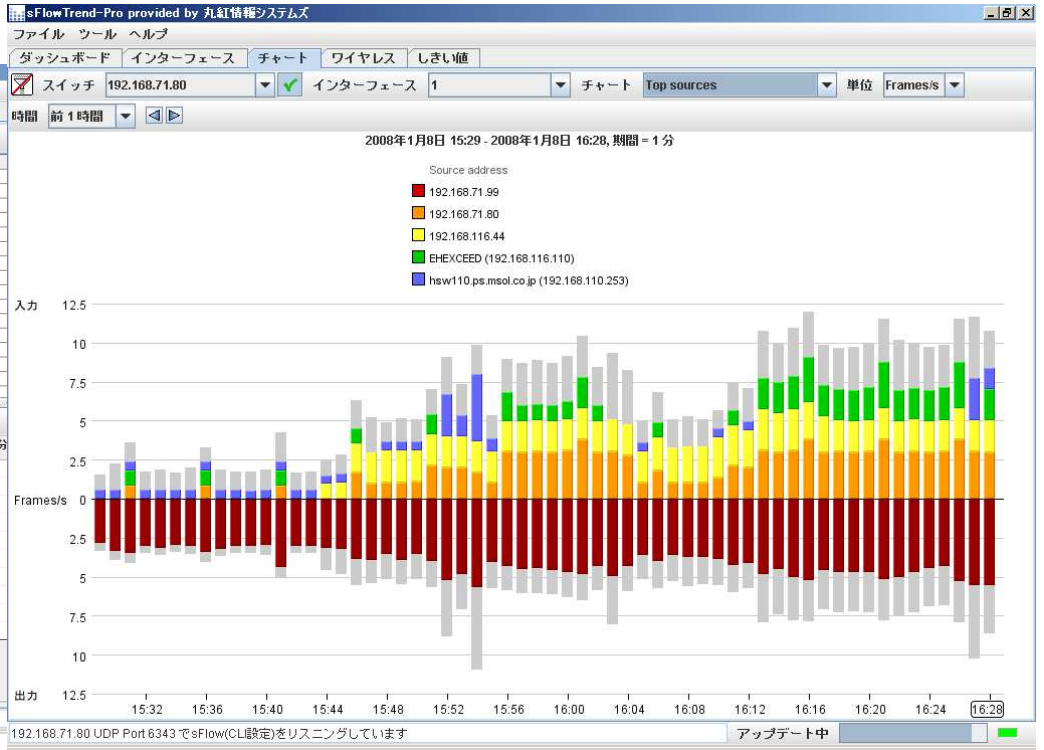
sFlowTrend-Proのご紹介

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。





丸紅情報システムズ株式会社

インフォメーション

- 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/100Mbp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/