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

アジェンダ

- 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
  - レポーティング機能
  - 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

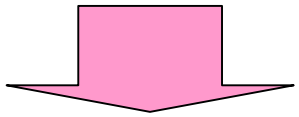
フローマネージメントとは
- ソースとデスティネーション間のフレームの流れを以下のような内容などを認識し分析すること
  - Source / Destination Address
  - Source / Destination Port 番号
  - Protocol
  - Interface
  - TOS (IP type of service) / Priority (802.1p)
  - VLAN (802.1Q)
  - AS番号

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・プロトコルの誕生

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



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

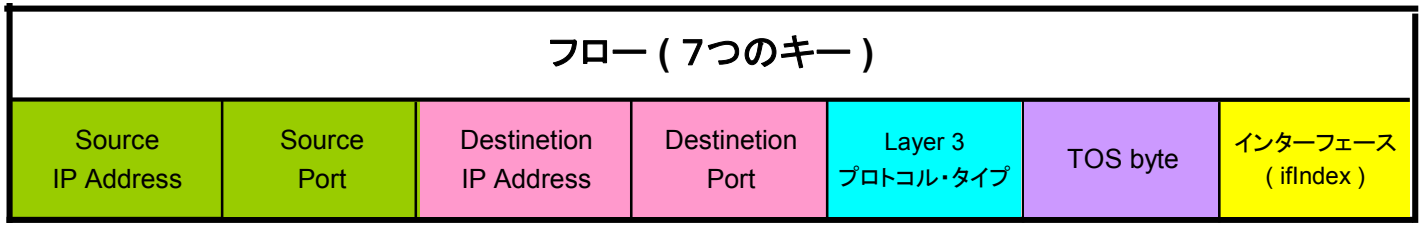
NetFlow

- 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

CISCO

- 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

NetFlow

- Cisco NetFlow

Figure 1 Example of a NetFlow Cache

CISCO

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）

No

Yes

4.エクスポート・バージョン（V5 / 9など）

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

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)

Cisco “NetFlow Services Solutions Guide”より

NetFlowの実装（NetFlow対応機器）

■Cisco Systems

NetFlow V1,V5,V7,V9

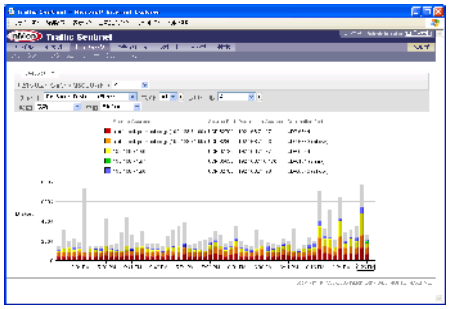
NetFlow

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

Cisco CRS-1

Cisco Catalyst 6500/4500

InMon Traffic Sentinel



- NetFlowによる分析

※ 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

その他のフロープロトコル

■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)

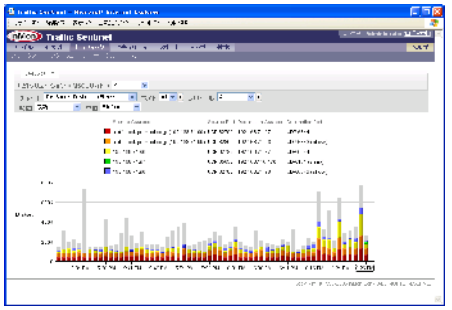
※ IPFIXはオープンな規格です。

■HP XRMON

■(旧)RiverStone LFAP

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。

※ 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

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、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

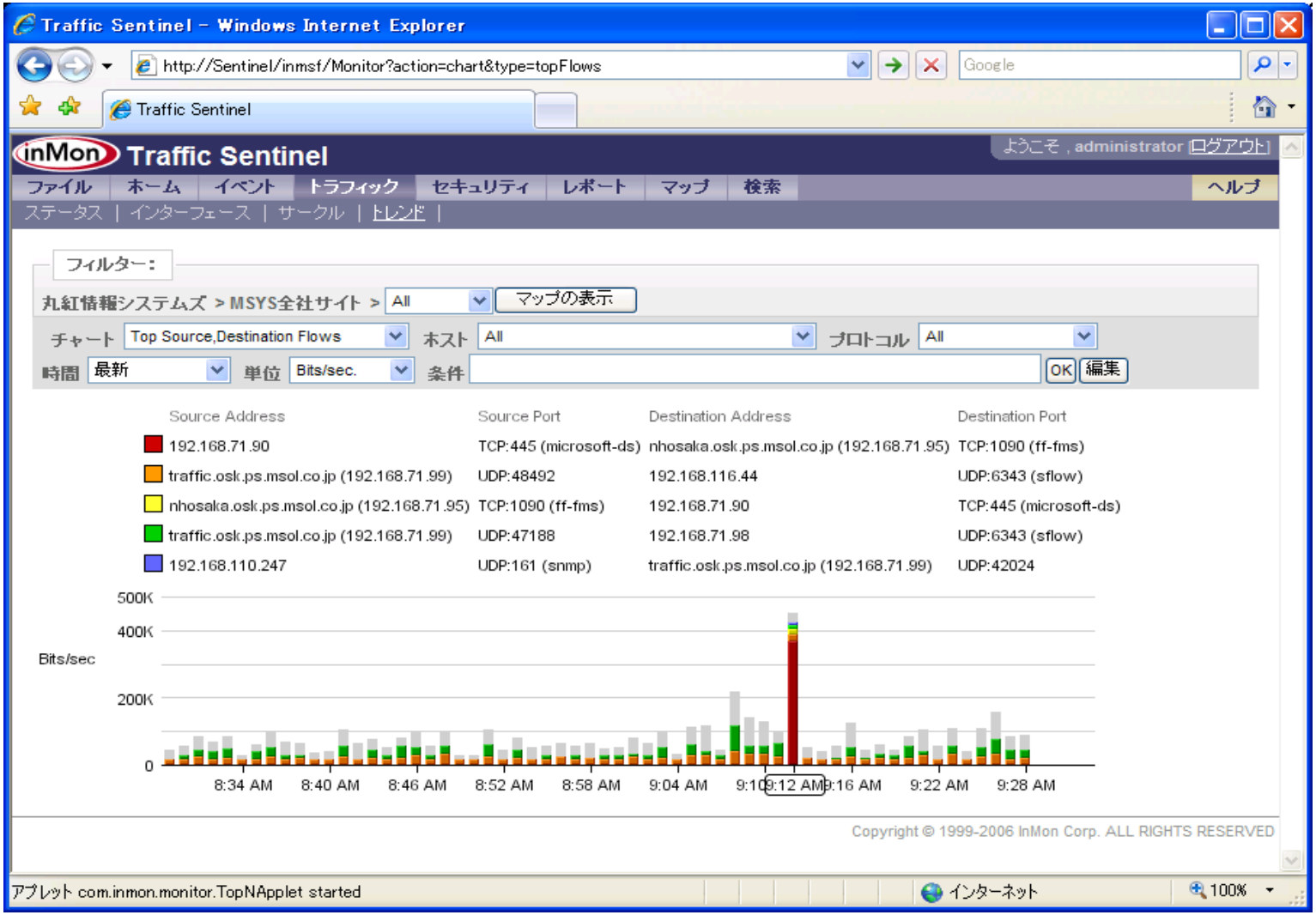
を、サポートしています。

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

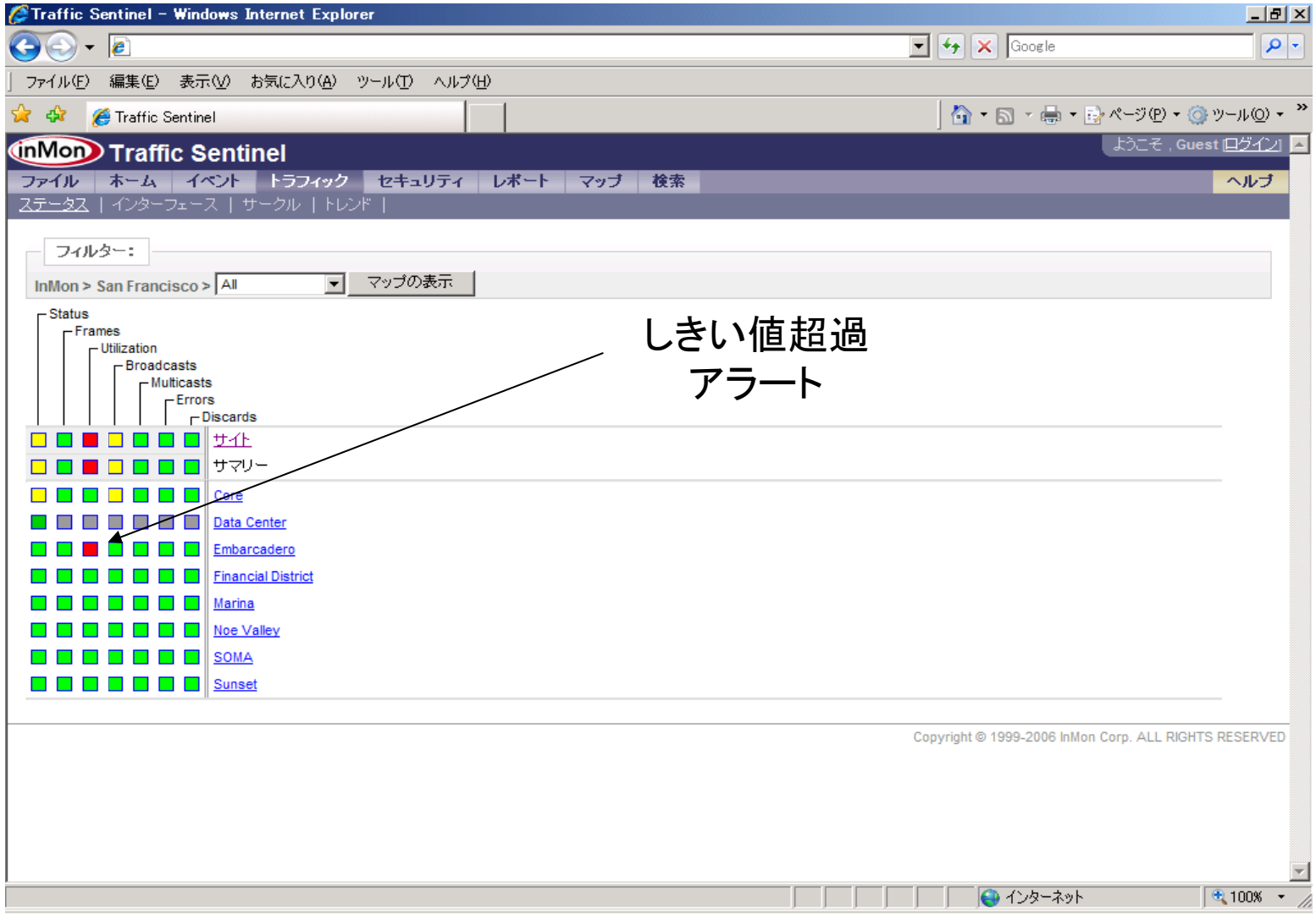
日本語版の提供

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

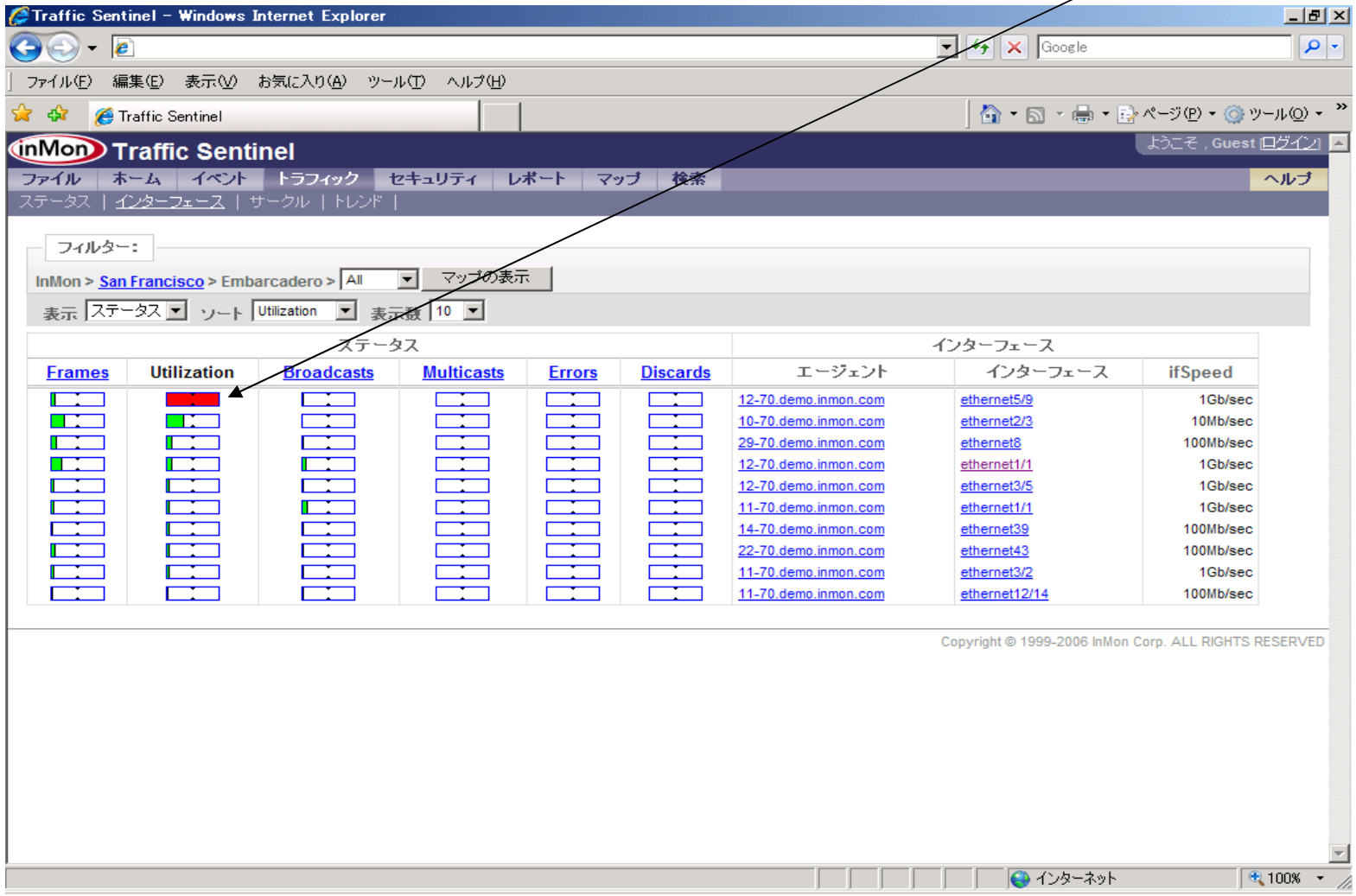
1. プロアクティブな問題の把握（しきい値分析）



ネットワーク管理：リアルタイムでの輻輳管理

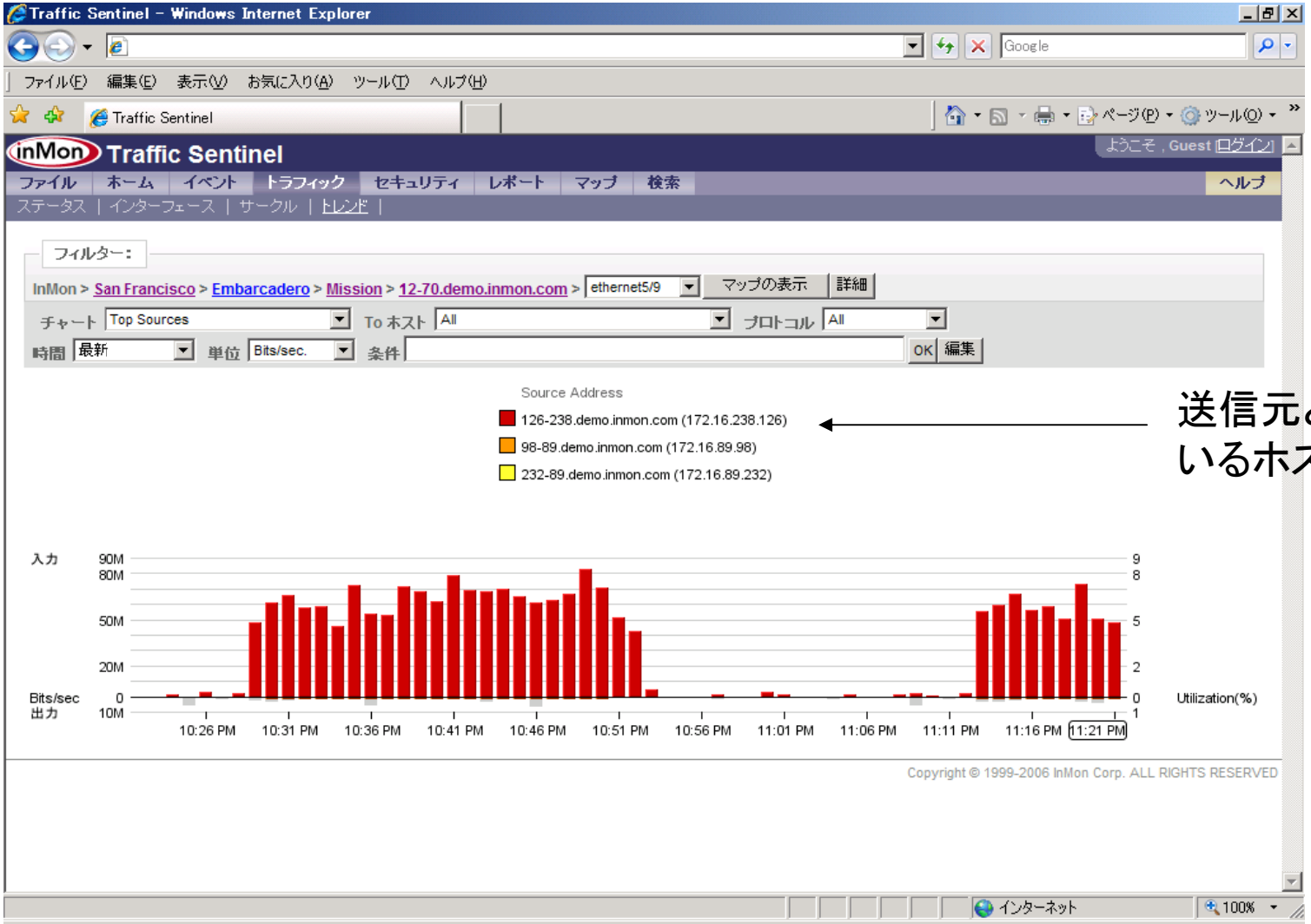
2. 問題が発生してインターフェースはどこか？

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

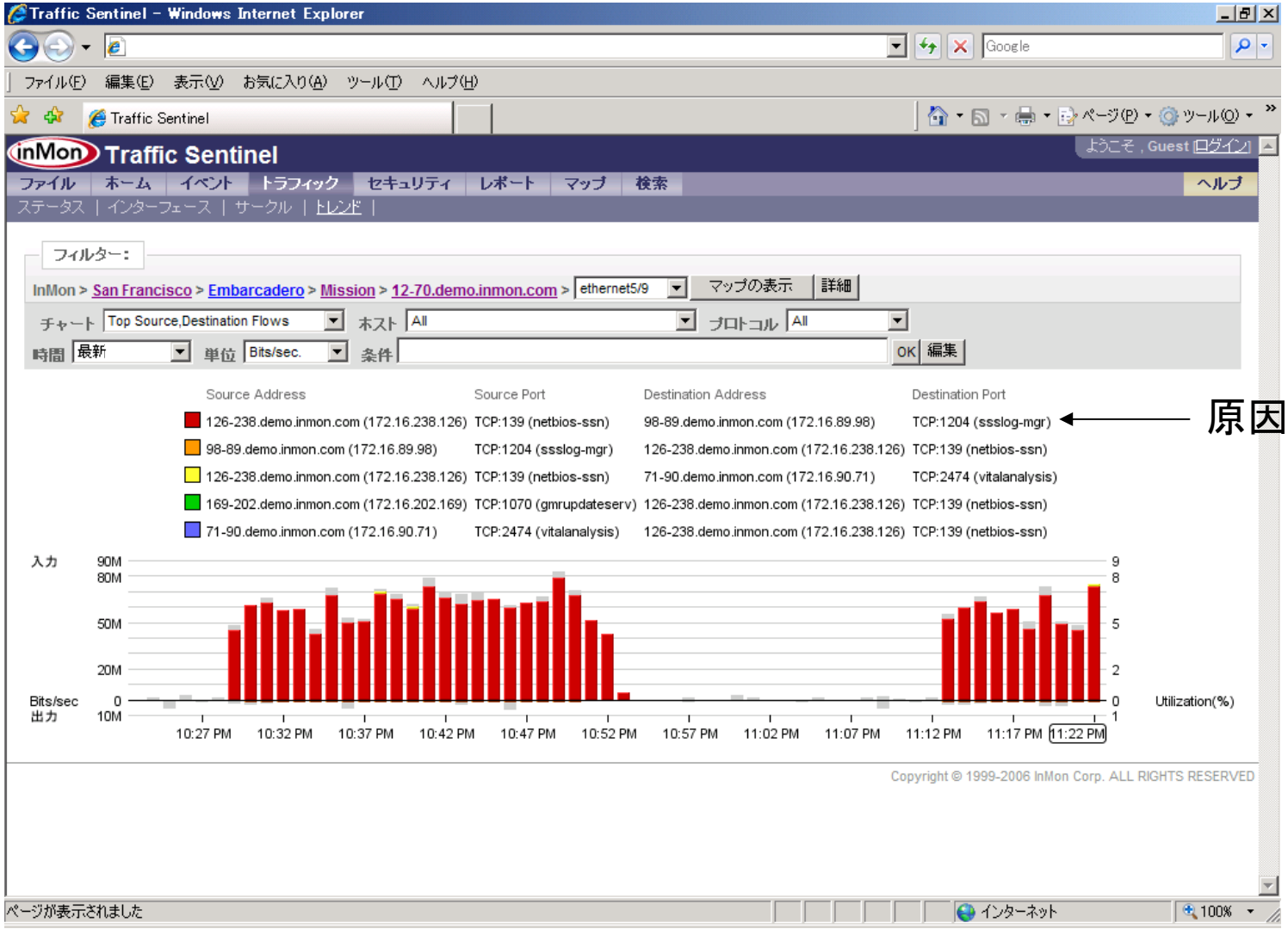
3. 問題を起こしているホストは誰か？



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）？



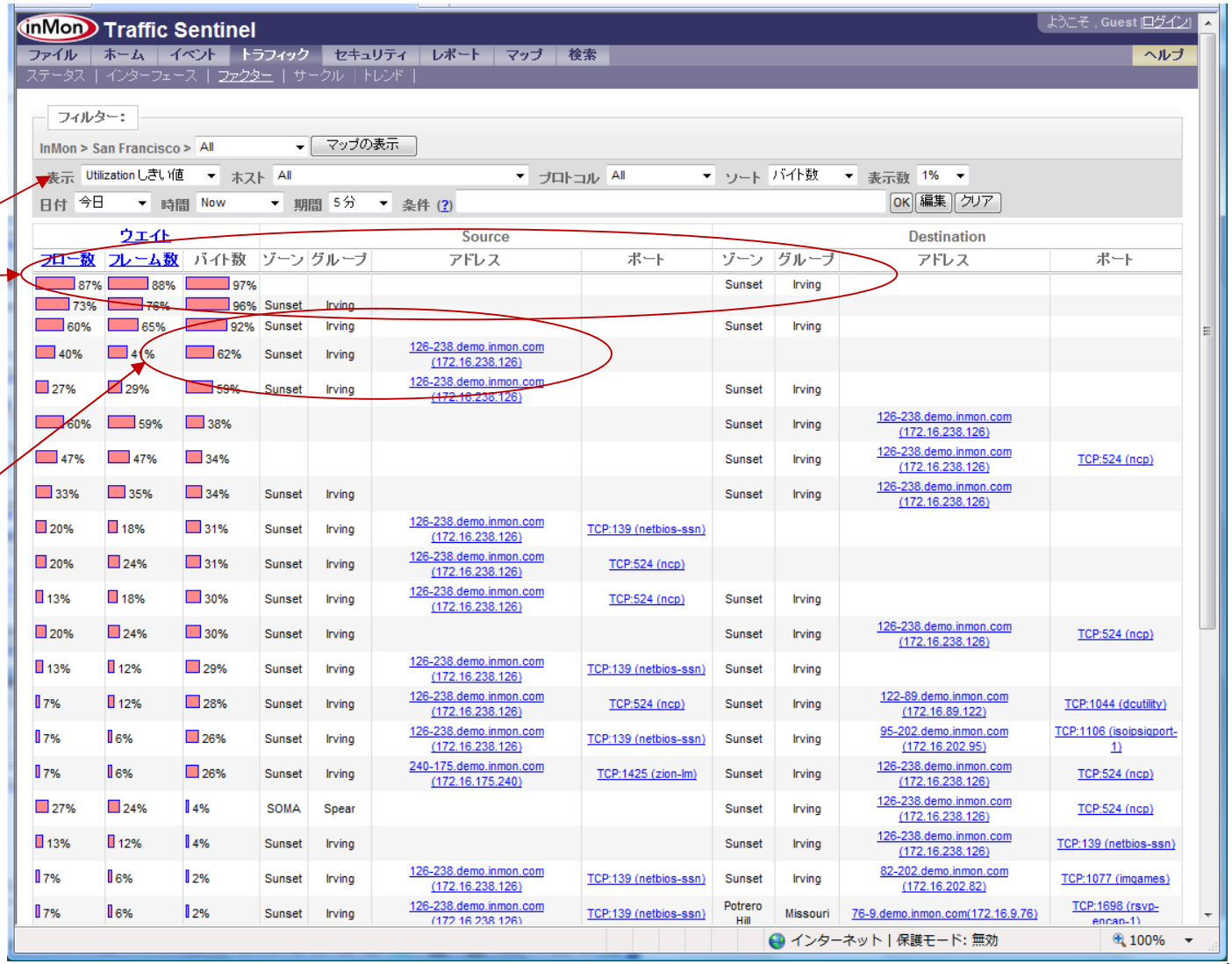
原因の把握

ネットワーク管理：トラフィック・ファクター

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

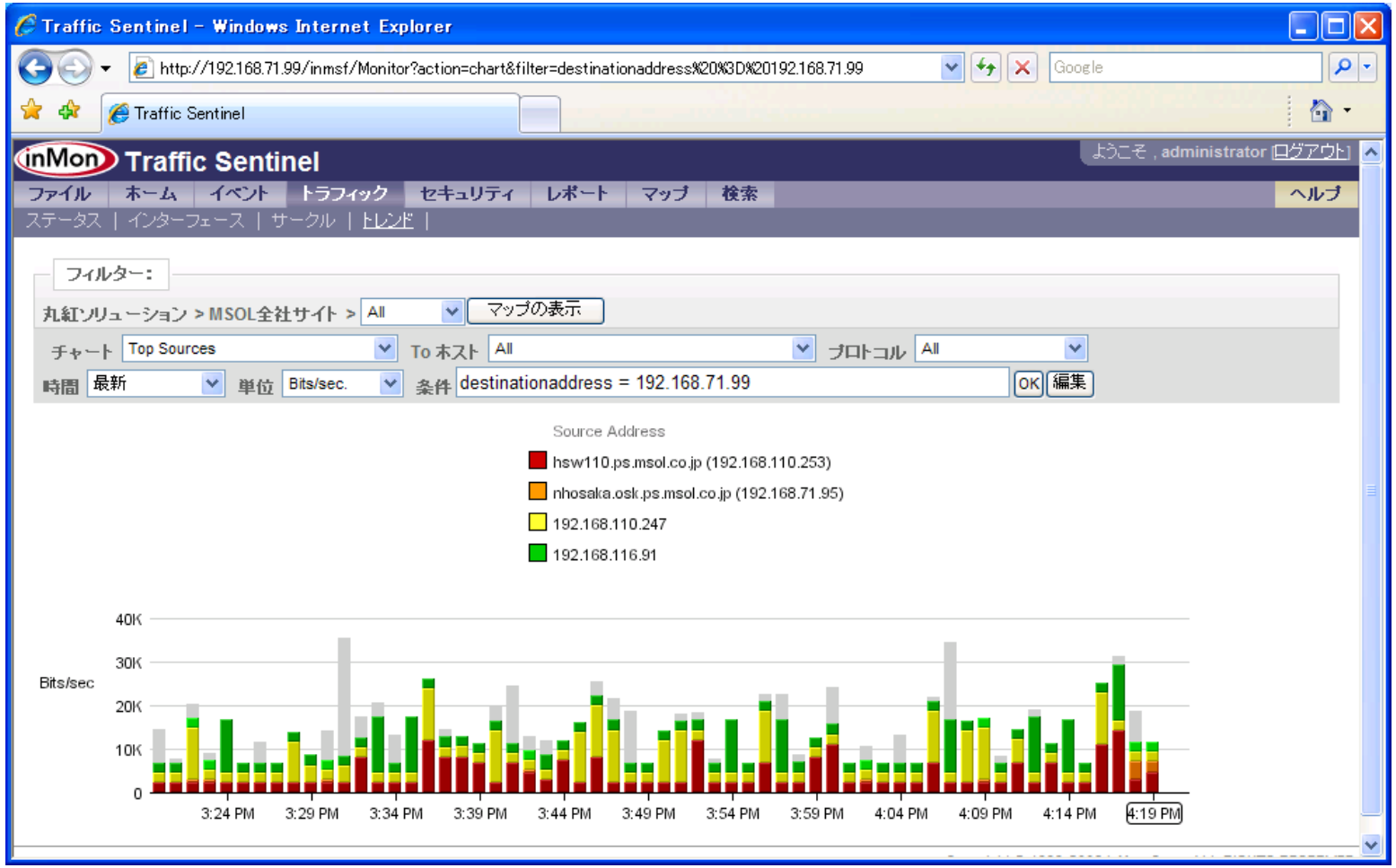
Utilization(使用率)のしきい値超過において172.16.238.126からの通信が、バイト数として62%の要因となっている



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。



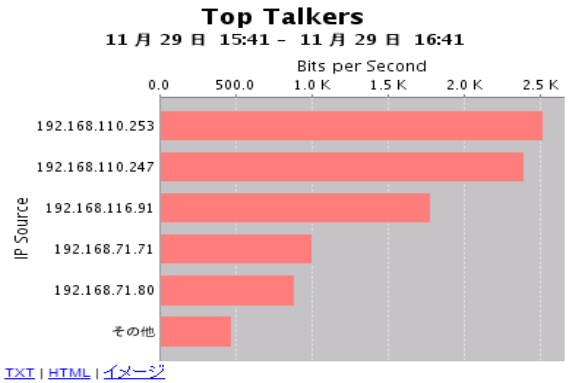
レポーティング機能

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

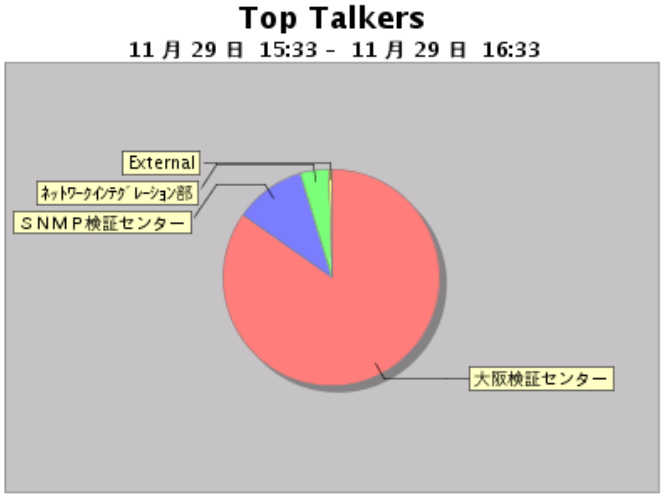
部門別トップ・ユーザ・レポート

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：特定サーバーの使用状況

特定サーバーの使用状況のレポート：グループ別

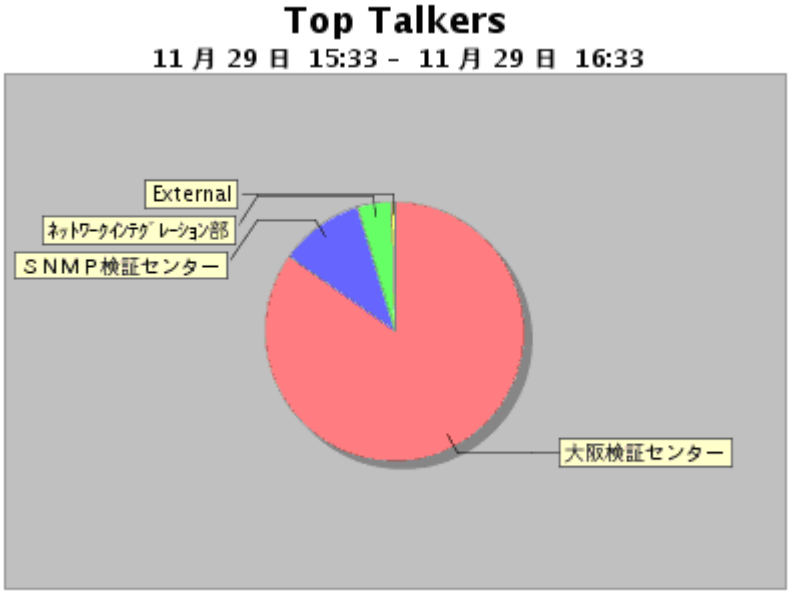
Historical Traffic Totals by Time

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

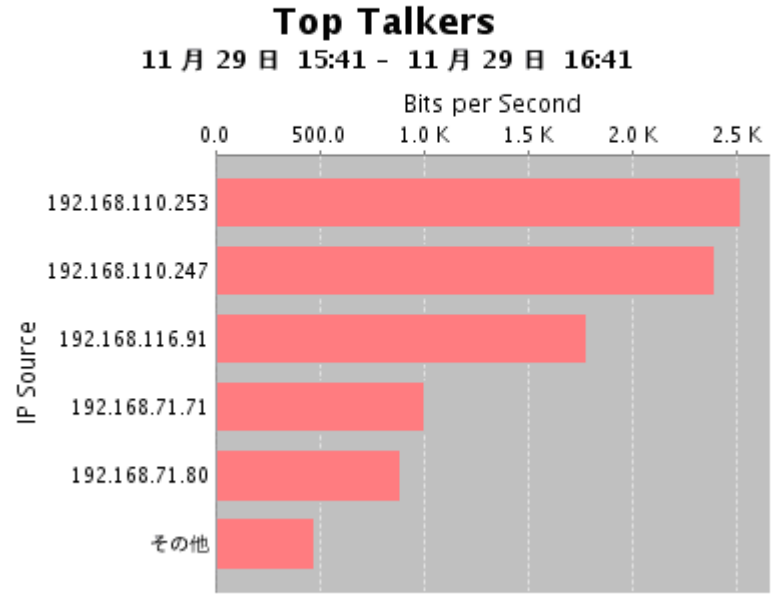
レポーティング機能：回線使用者の内訳

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

レポーティング機能：障害発生検知レポート

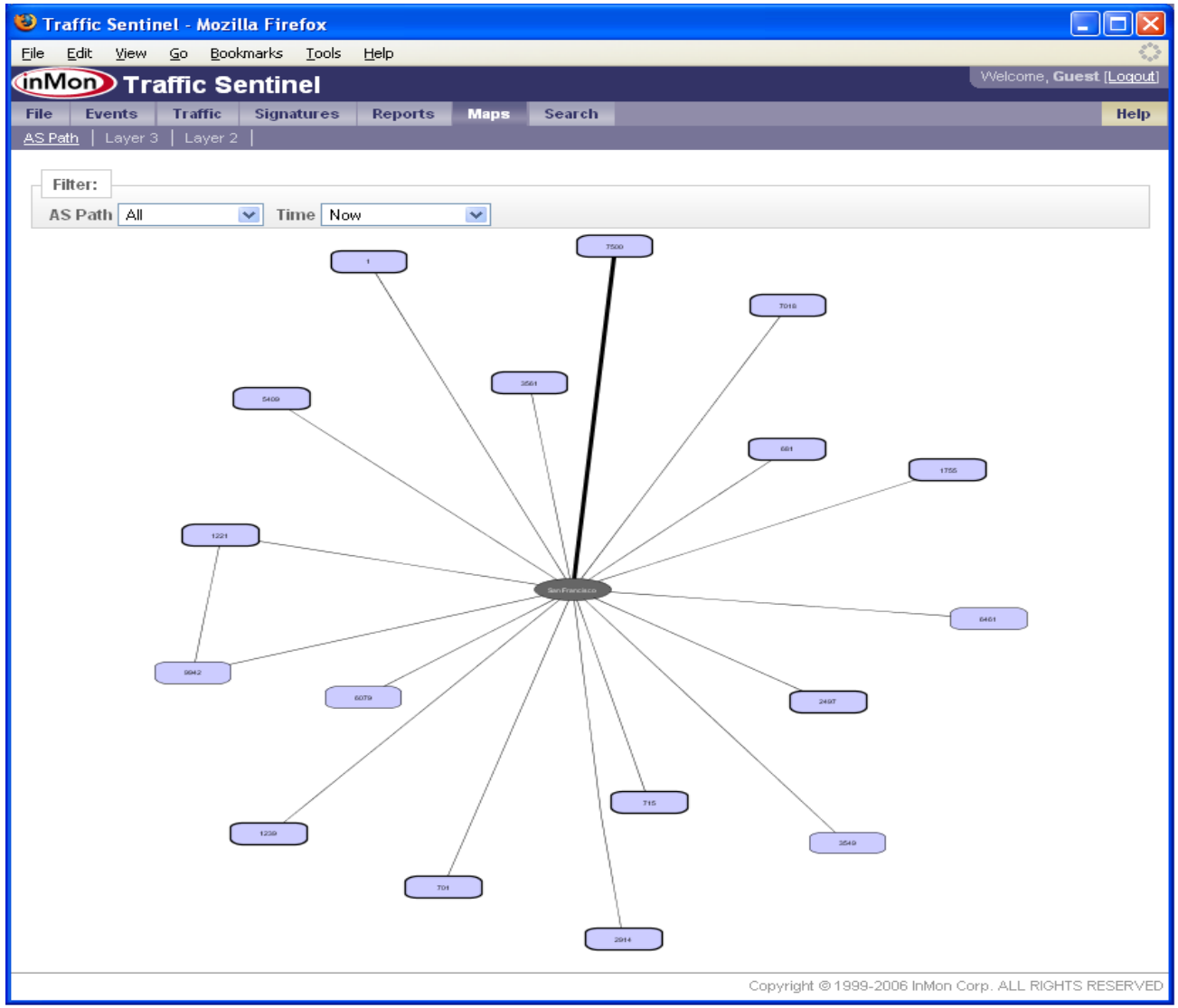
- トラフックの内容に対ししきい値を設定し、超過したときにイベントを発生させる
  - しきい値：トラフィック（プロトコル・アドレス・グループなど）に対して設定
  - スケジュール化し、超過時にイベントを発生させる

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

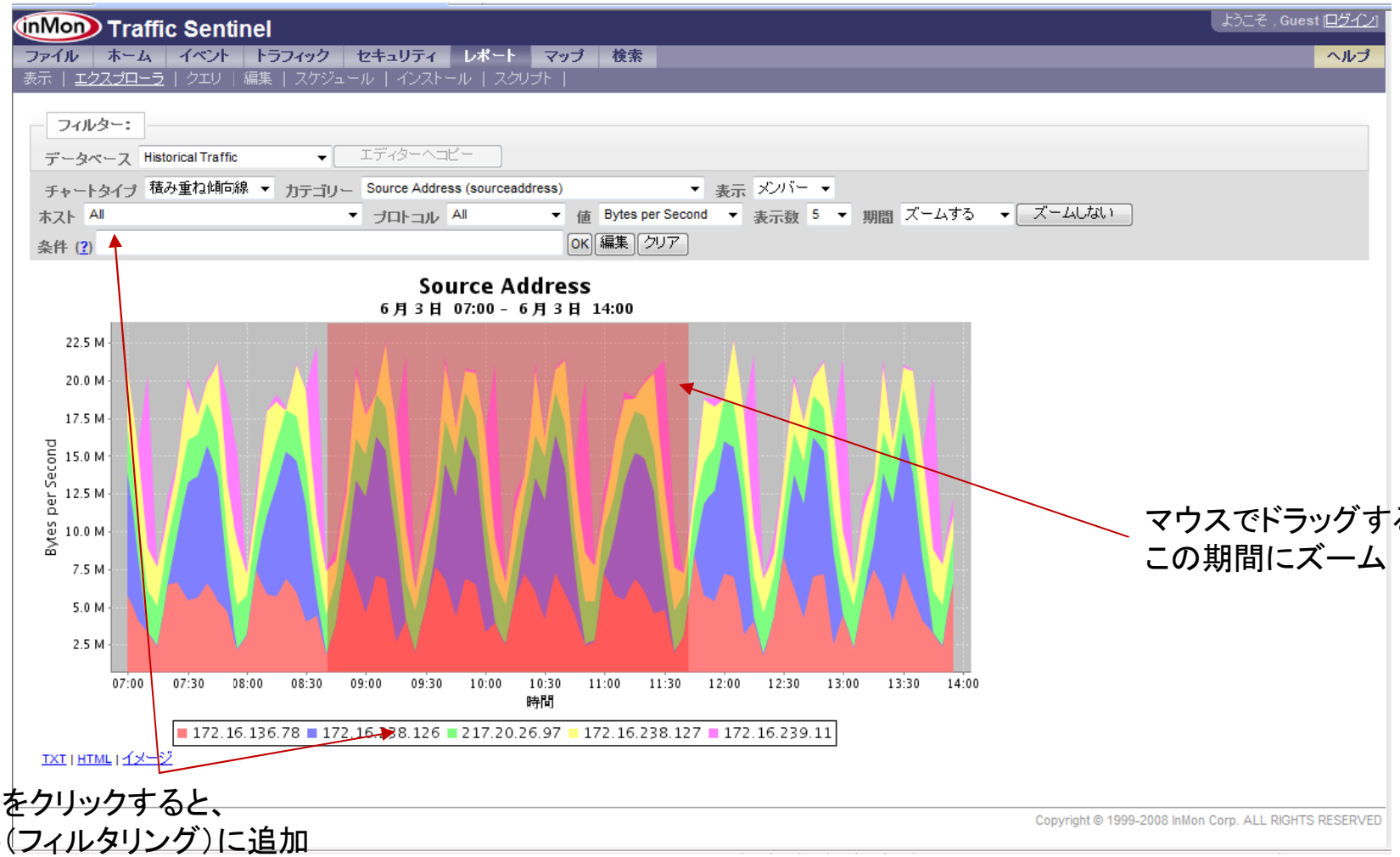
AS分析：ASパスのマップ



Peer ASをレポート

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

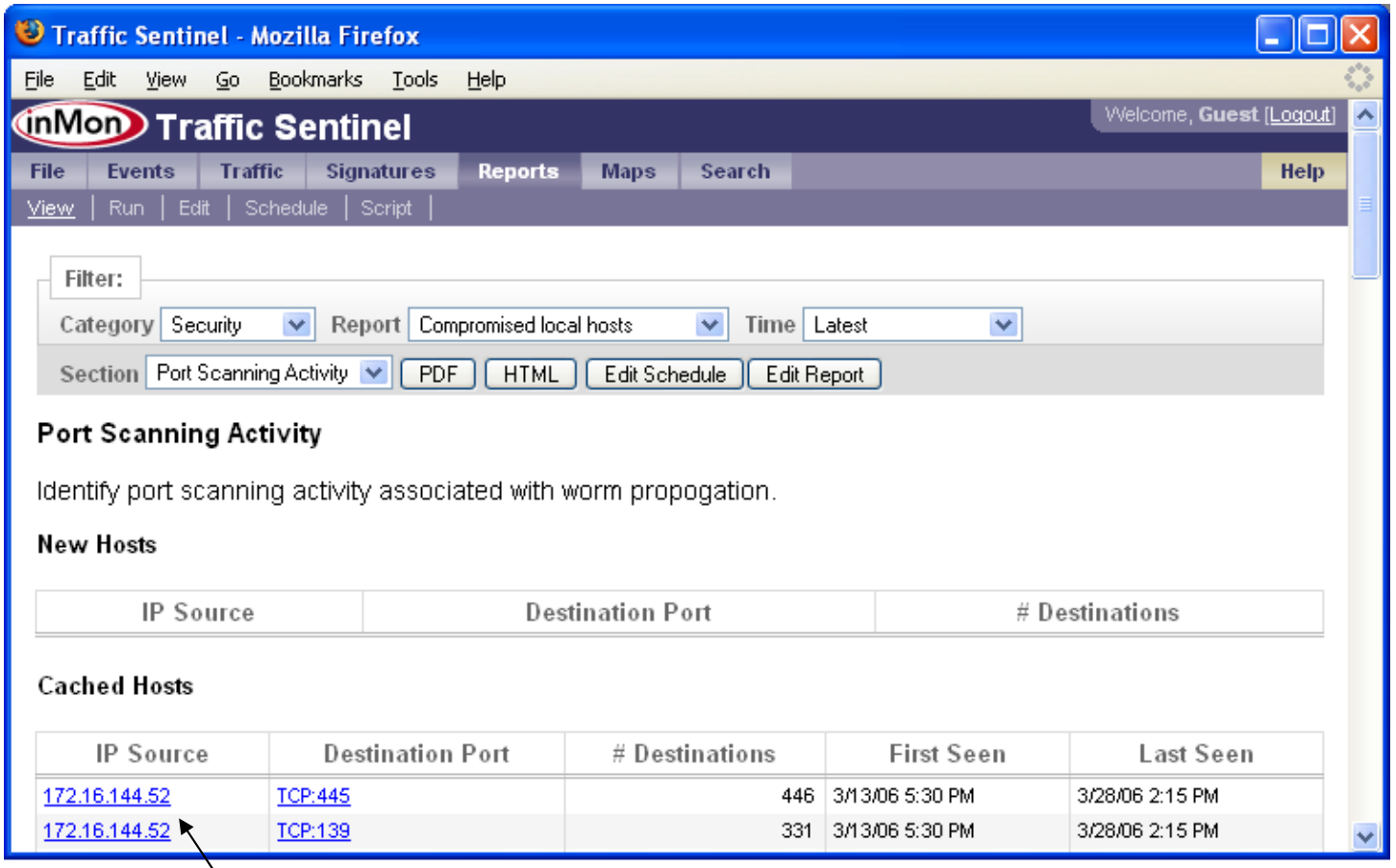


マウスでドラッグすると、
この期間にズーム

凡例をクリックすると、
条件（フィルタリング）に追加

セキュリティ管理：振る舞い検知

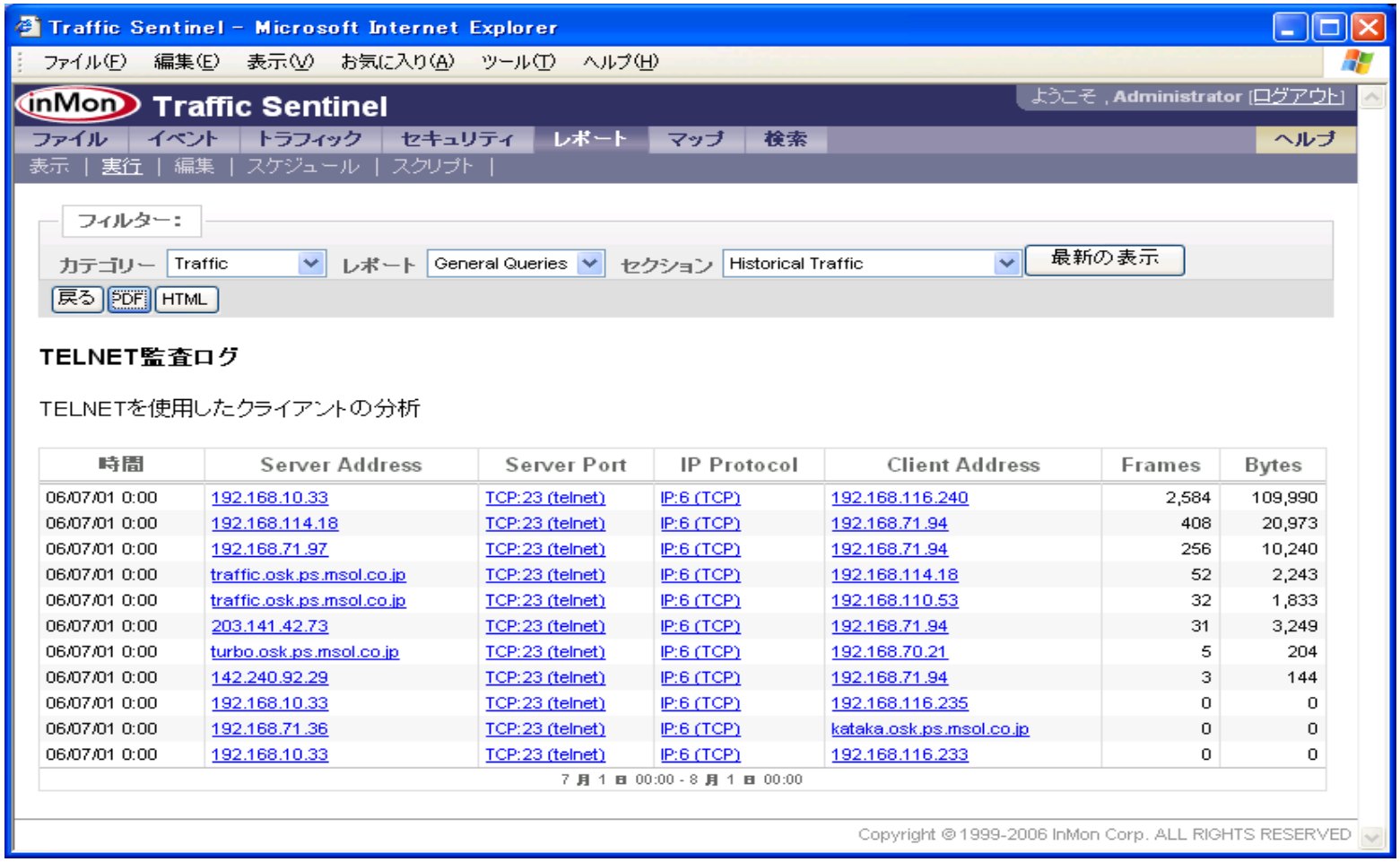
ポートスキャンや新種のウイルス・ワームの検知：



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

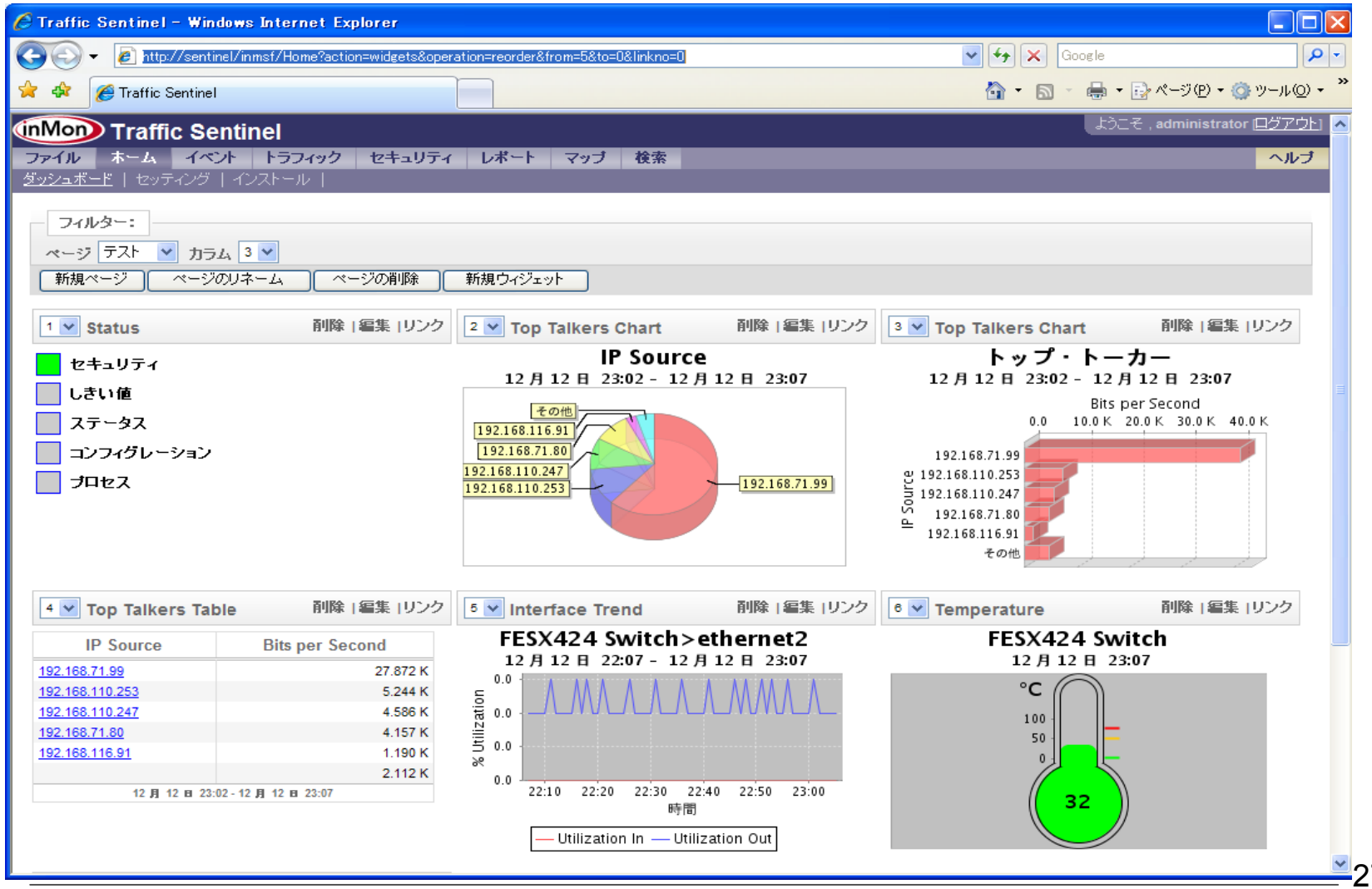
監査：フローログ – サーバーへのTELNET接続者のログ



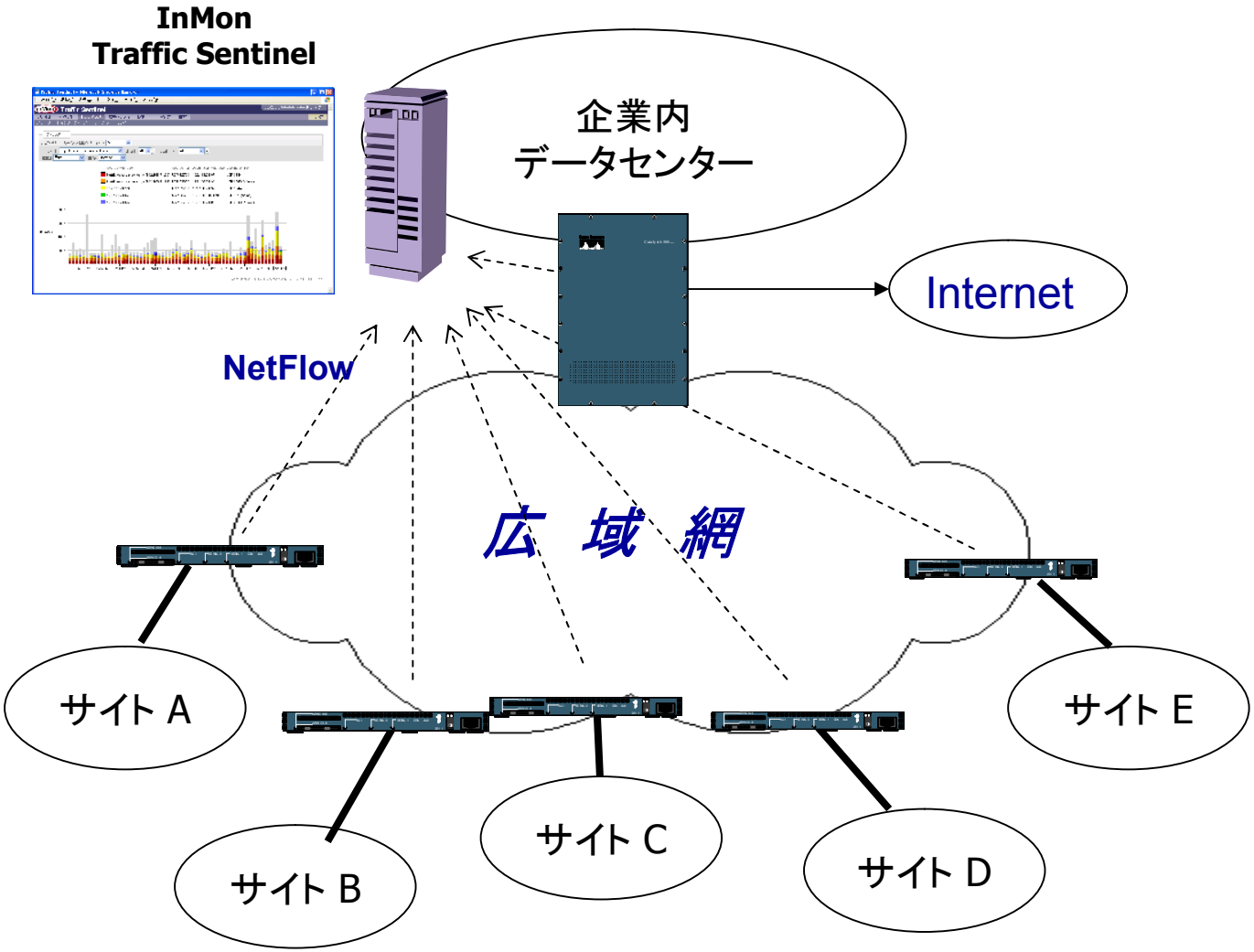
特定のサーバーへのアクセスや特定のクライアントの使用内容の把握

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。



ケーススタディー


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

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/PentiumⅣ×1　3GHz

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

■ お問合せ先

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*