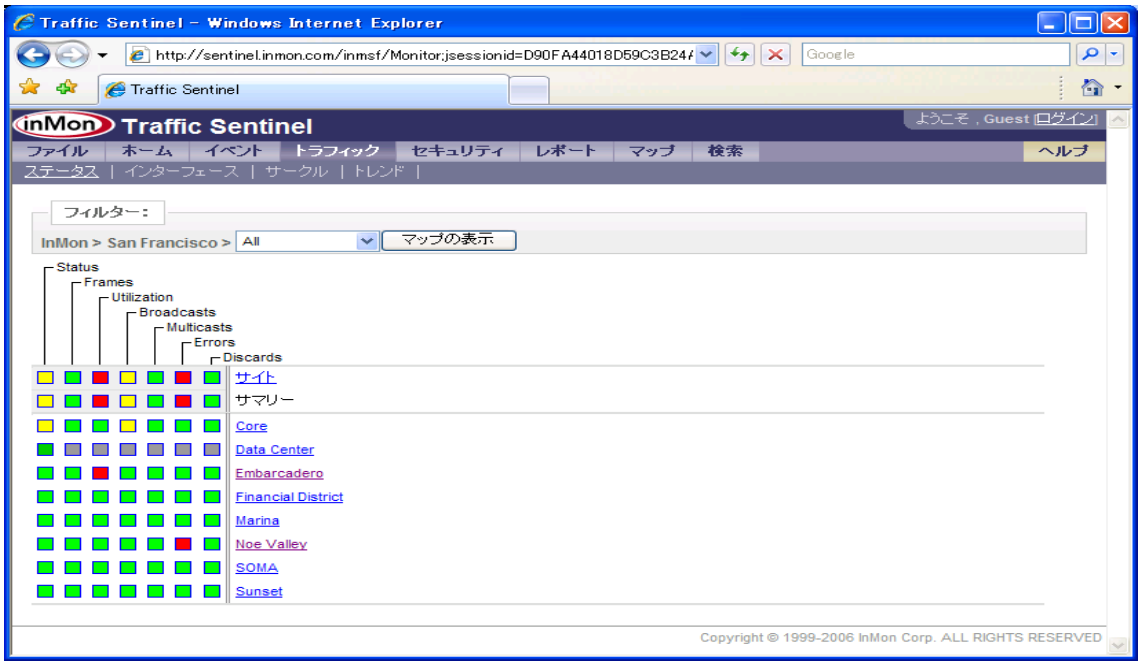
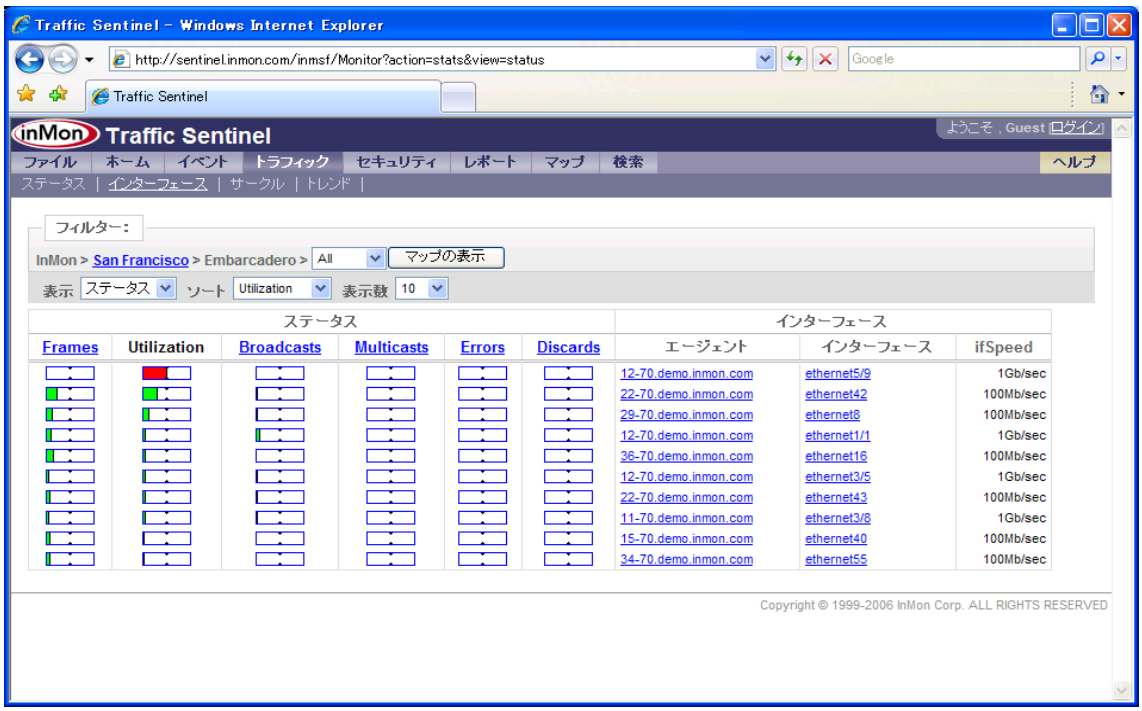
参考資料：InMonTrafficSentinel の画面・チャート・運用例

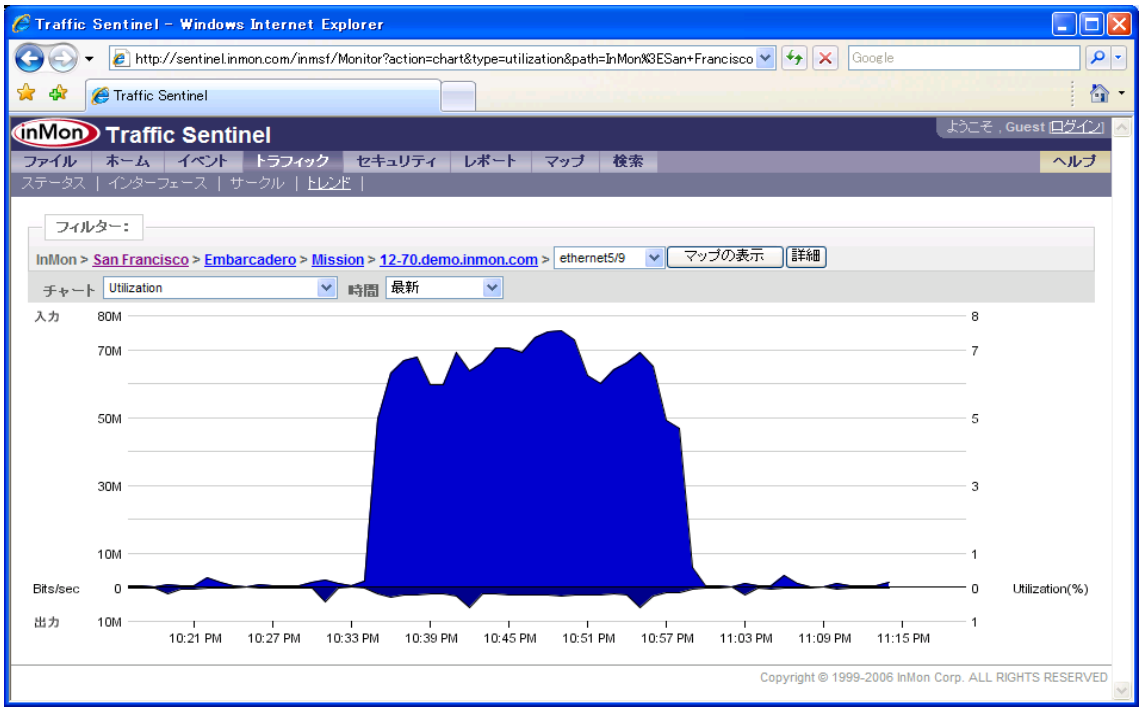
2008/08/19

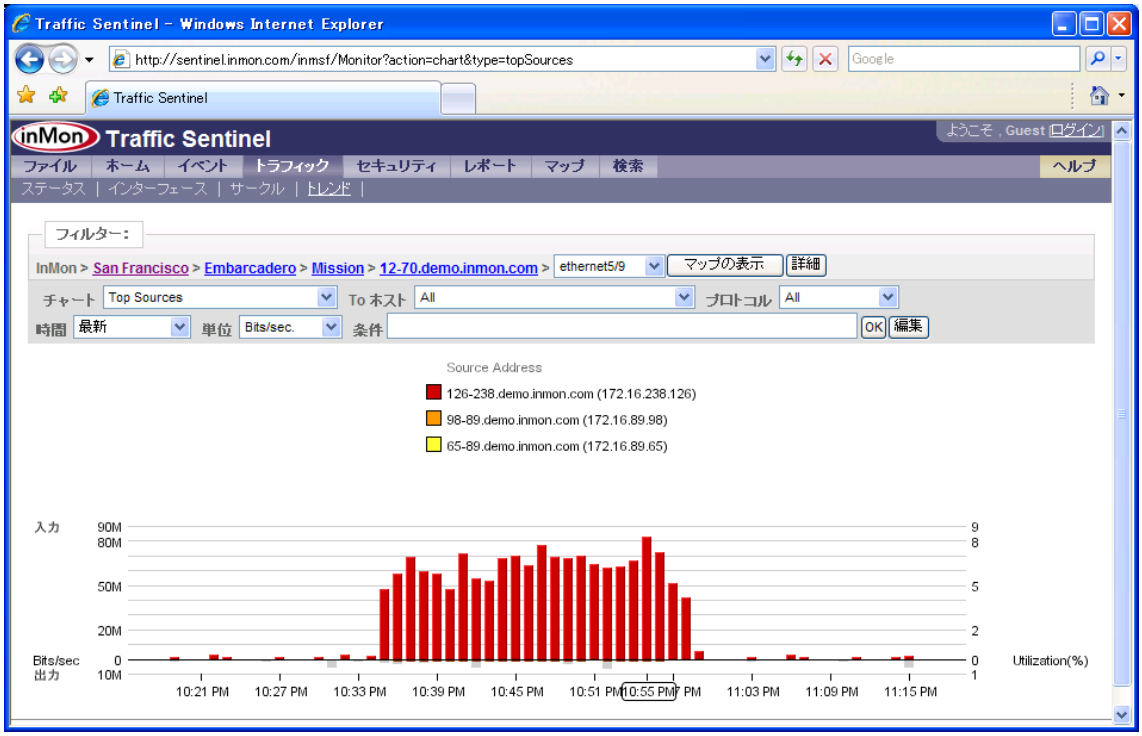
１． 輻輳管理

Utilization(帯域幅使用率)が、しきい値を超過したインターフェースでの、
超過原因となったアドレスを確認します。





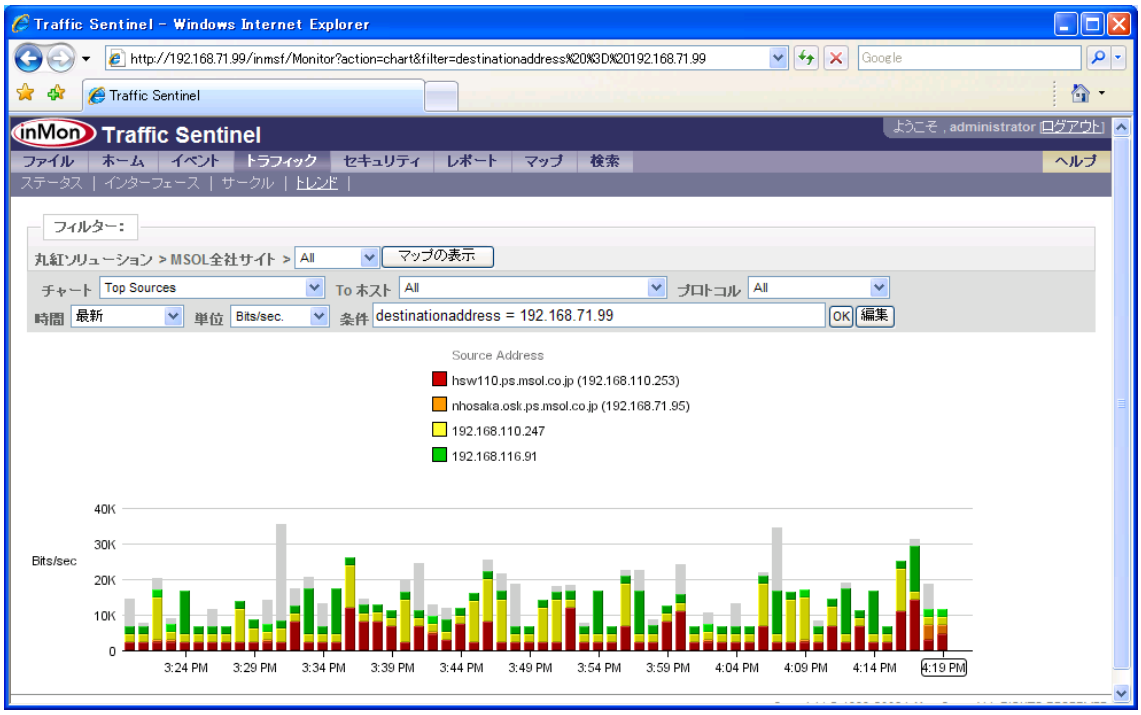

Traffic Sentinel - Windows Internet Explorer
http://sentinel.inmon.com/inmsf/Monitor?action=chart&type=utilization&path=InMon%3ESan+Francisco
Traffic Sentinel
inMon Traffic Sentinel
ようこそ , Guest [ログイン]
ファイル ホーム イベント トラフィック セキュリティ レポート マップ 検索 ヘルプ
ステータス | インターフェース | サークル | トレンド |
フィルター:
InMon > San Francisco > Embarcadero > Mission > 12-70.demo.inmon.com > ethernet5/9
マップの表示 詳細
チャート Utilization 時間 最新
入力
80M
70M
50M
30M
10M
Bits/sec
0
出力
10M
8
7
5
3
1
0
1
Utilization(%)
10:21 PM 10:27 PM 10:33 PM 10:39 PM 10:45 PM 10:51 PM 10:57 PM 11:03 PM 11:09 PM 11:15 PM
Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

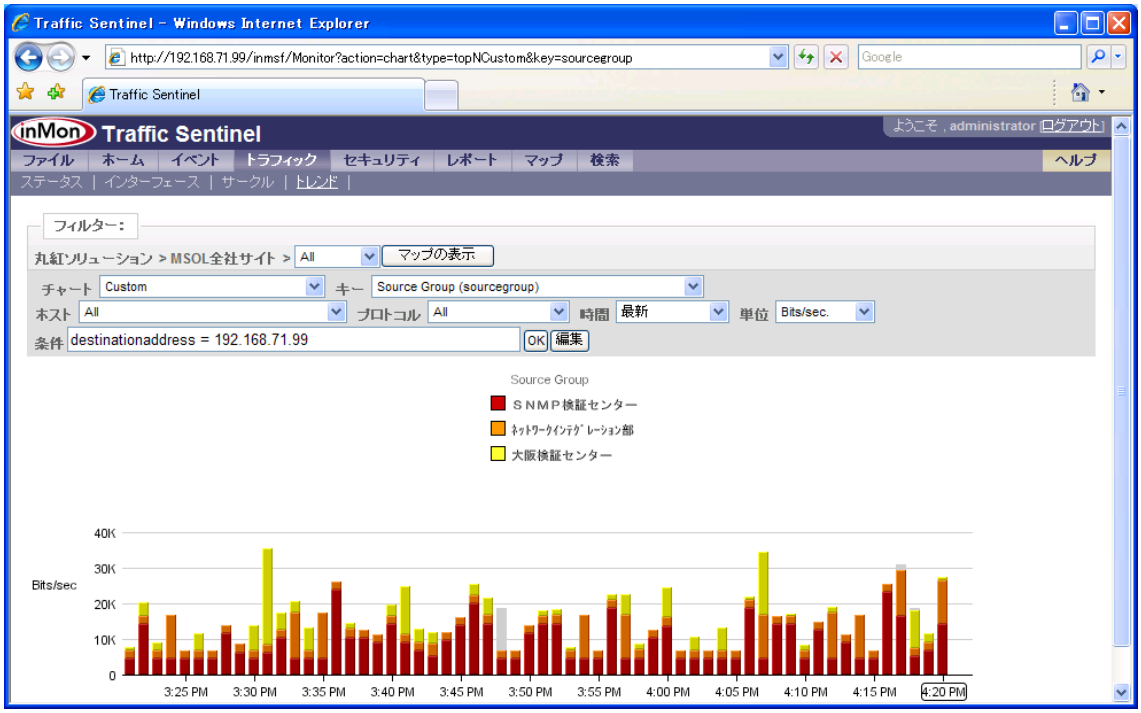

Traffic Sentinel - Windows Internet Explorer
http://sentinel.inmon.com/inmsf/Monitor?action=chart&type=topSources
Traffic Sentinel
inMon Traffic Sentinel
ようこそ , Guest [ログイン]
ファイル ホーム イベント トラフィック セキュリティ レポート マップ 検索 ヘルプ
ステータス | インターフェース | サークル | トレンド |
フィルター:
InMon > San Francisco > Embarcadero > Mission > 12-70.demo.inmon.com > ethernet5/9
マップの表示 詳細
チャート Top Sources To ホスト All プロトコル All
時間 最新 単位 Bits/sec. 条件 OK 編集
Source Address
126-238.demo.inmon.com (172.16.238.126)
98-89.demo.inmon.com (172.16.89.98)
65-89.demo.inmon.com (172.16.89.65)
入力
90M
80M
50M
20M
Bits/sec
0
出力
10M
9
8
5
2
0
1
Utilization(%)
10:21 PM 10:27 PM 10:33 PM 10:39 PM 10:45 PM 10:51 PM 10:55 PM 11:03 PM 11:09 PM 11:15 PM

2． 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。





3．特定サーバーの使用状況のレポート

先週、サーバー(192.168.71.99)へアクセスしたユーザ・グループのリスト。

Historical Traffic Totals by Time

先週、サーバー(192.168.71.99)へアクセスした上位ユーザ

時間	IP Source	Bits per Second
07/11/18 0:00	192.168.110.253	2.210 K
07/11/18 0:00	192.168.71.80	697.624
07/11/18 0:00	72.14.253.91	21.832
07/11/18 0:00		22.368
07/11/19 0:00	192.168.110.253	2.327 K
07/11/19 0:00	192.168.71.80	848.032
07/11/19 0:00	192.168.116.254	706.064
07/11/19 0:00		193.080
07/11/20 0:00	192.168.110.253	2.279 K
07/11/20 0:00	192.168.116.254	1.223 K
07/11/20 0:00	192.168.71.95	594.064
07/11/20 0:00		648.632
07/11/21 0:00	192.168.110.253	2.250 K
07/11/21 0:00	192.168.116.254	1.246 K
07/11/21 0:00	192.168.71.80	516.568
07/11/21 0:00		243.992
07/11/22 0:00	192.168.110.253	2.279 K
07/11/22 0:00	192.168.116.254	1.151 K
07/11/22 0:00	192.168.71.80	218.432
07/11/22 0:00		217.832
07/11/23 0:00	192.168.110.253	2.262 K
07/11/23 0:00	192.168.116.254	880.848
07/11/23 0:00	192.168.71.80	285.560
07/11/23 0:00		223.504

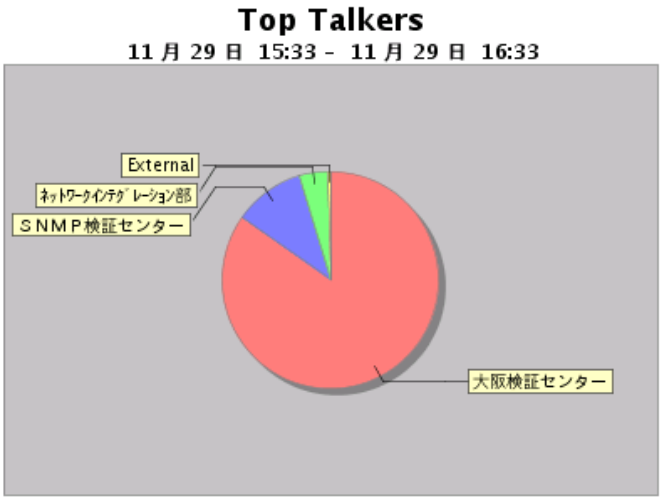
Historical Traffic Totals by Time

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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	934.240
07/11/23 0:00	大阪検証センター	285.560
07/11/23 0:00		70.224

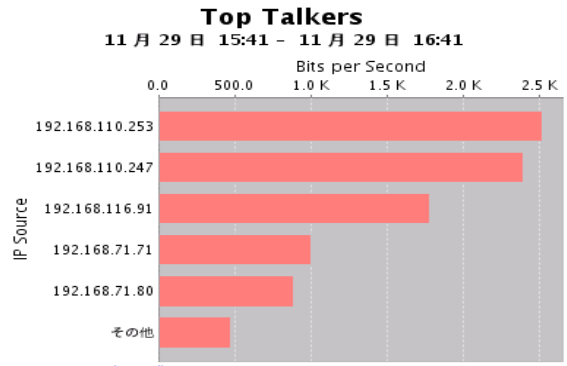
４．回線使用者の内訳

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

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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	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ｸﾞﾚｰｼｮﾝ部	96.896 K

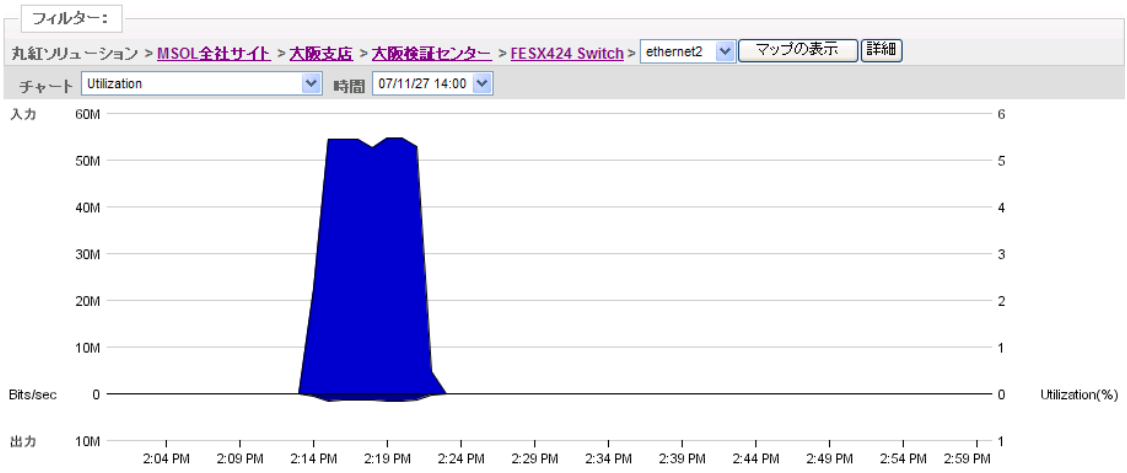
5.しきい値超過時のアラーム

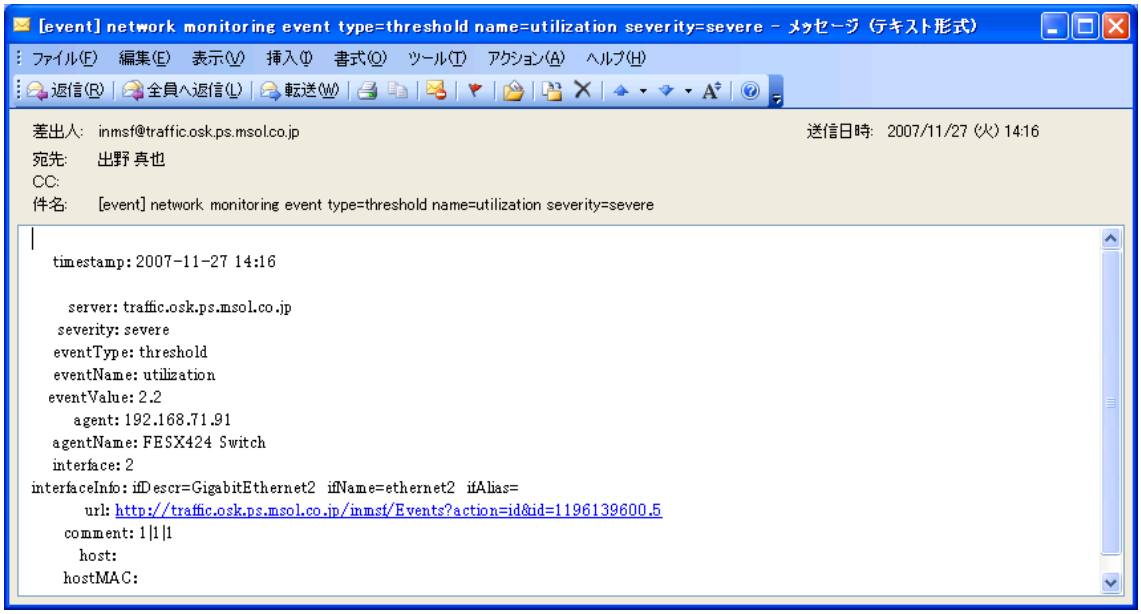
特定のスイッチのインターフェース(192.168.71.91 の ifIndex:2)において、

Utilization(帯域幅使用率)１%を超過したときメール送信。

FTP により Utilization(帯域幅使用率)１%を超過させます。

時間	タイプ	名称	値	アドレス	インターフェース	コメント
07/11/27 14:24	しきい値	Utilization	100.0	192.168.71.91	ethernet2	1 分間で しきい値 1 を 1 回 超過
07/11/27 14:16	しきい値	Utilization	2.2	192.168.71.91	ethernet2	1 分間で しきい値 1 を 1 回 超過
07/11/27 14:10	しきい値	Report				DoS Detect
07/11/27 14:05	しきい値	Report				DoS Detect
07/11/27 14:00	しきい値	Report				DoS Detect
07/11/27 13:59	しきい値	Utilization	100.0	192.168.71.91	ethernet2	1 分間で しきい値 1 を 1 回 超過
07/11/27 13:55	しきい値	Report				DoS Detect
07/11/27 13:51	しきい値	Utilization	2.4	192.168.71.91	ethernet2	1 分間で しきい値 1 を 1 回 超過





６．特定トラフィックの検知：(模擬)DoS 攻撃の検知

PING が毎５分間で１００パケット異常発生したとき、DoS 攻撃として検知し、

イベントを発生させ、メールを送信します。

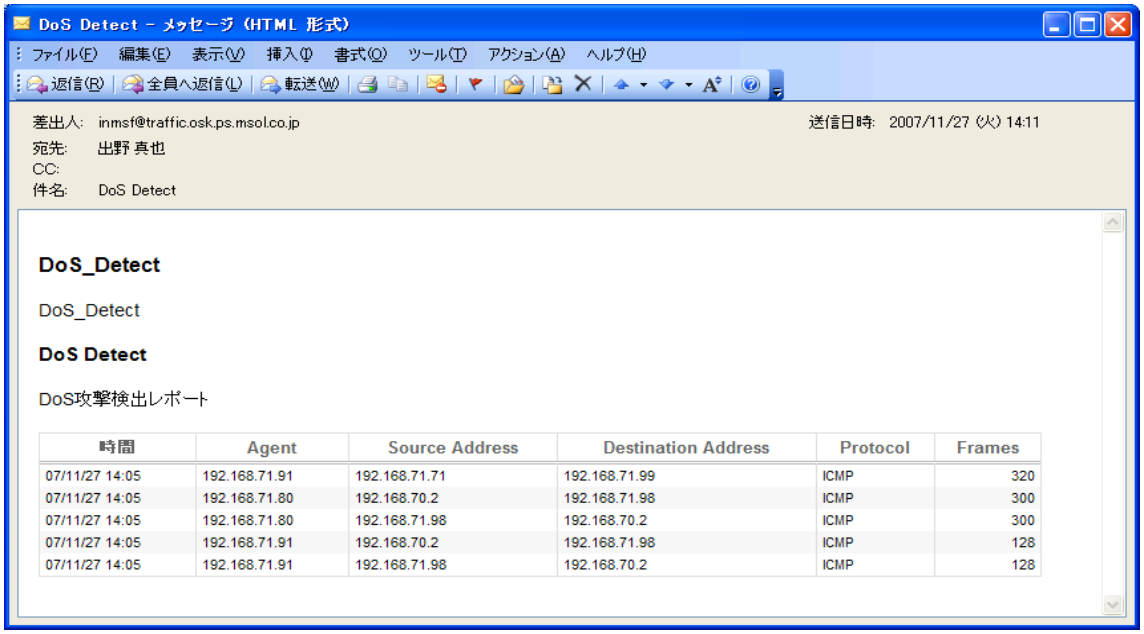
192.168.71.98 から 192.168.70.2 宛に PING を発行。

実運用では、特定プロトコルやホストなどの検知を行います。


フィルター：

期間 2日前から　重要度 All　タイプ しきい値　表示数 20　XML

時間	タイプ	名称	値	アドレス	インターフェース	コメント
07/11/27 14:24	しきい値	Utilization	100.0	192.168.71.91	ethernet2	1分間でしきい値 1を 1回 超過
07/11/27 14:16	しきい値	Utilization	2.2	192.168.71.91	ethernet2	1分間でしきい値 1を 1回 超過
07/11/27 14:10	しきい値	Report				DoS Detect
07/11/27 14:05	しきい値	Report				DoS Detect
07/11/27 14:00	しきい値	Report				DoS Detect
07/11/27 13:59	しきい値	Utilization	100.0	192.168.71.91	ethernet2	1分間でしきい値 1を 1回 超過
07/11/27 13:55	しきい値	Report				DoS Detect
07/11/27 13:51	しきい値	Utilization	2.4	192.168.71.91	ethernet2	1分間でしきい値 1を 1回 超過



時間	Agent	Source Address	Destination Address	Protocol	Frames
07/11/27 14:05	192.168.71.91	192.168.71.71	192.168.71.99	ICMP	320
07/11/27 14:05	192.168.71.80	192.168.70.2	192.168.71.98	ICMP	300
07/11/27 14:05	192.168.71.80	192.168.71.98	192.168.70.2	ICMP	300
07/11/27 14:05	192.168.71.91	192.168.70.2	192.168.71.98	ICMP	128
07/11/27 14:05	192.168.71.91	192.168.71.98	192.168.70.2	ICMP	128

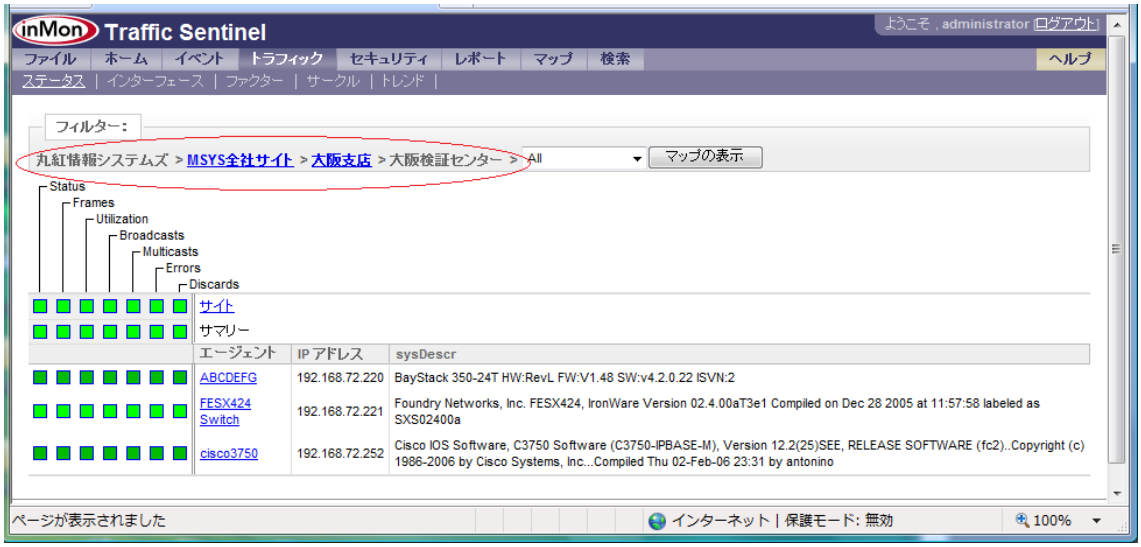
7.日本語の扱い

TrafficSentinel では、各種チャートやレポート上で日本語を扱うことが出来ます。

日本語を使用する例として、以下のものがあります。

1) エンタープライズ・サイト・ゾーン・グループとしての名称の日本語化

TrafficSentinel 上で扱う各種アドレスをロケーションなどでグループ分けをして集約した情報としてチャート・レポート化するためにエンタープライズ・サイト・ゾーン・グループの区分が用意されており、これを日本語化することによりレポートをよりわかりやすくすることが出来ます。

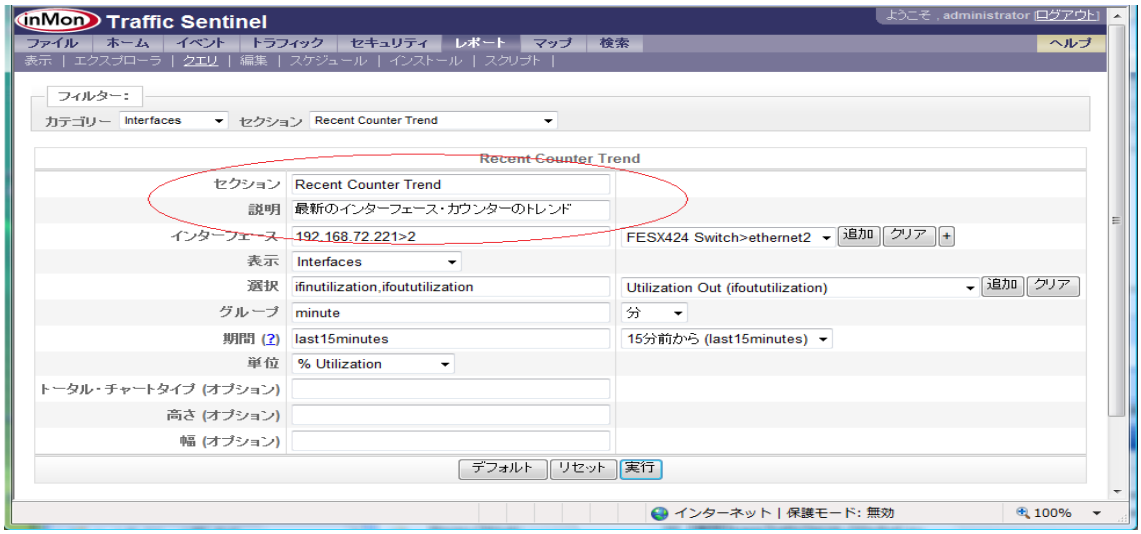


グループは、CIDR 別（192.168.1.0/24 など）に定義することも可能です。

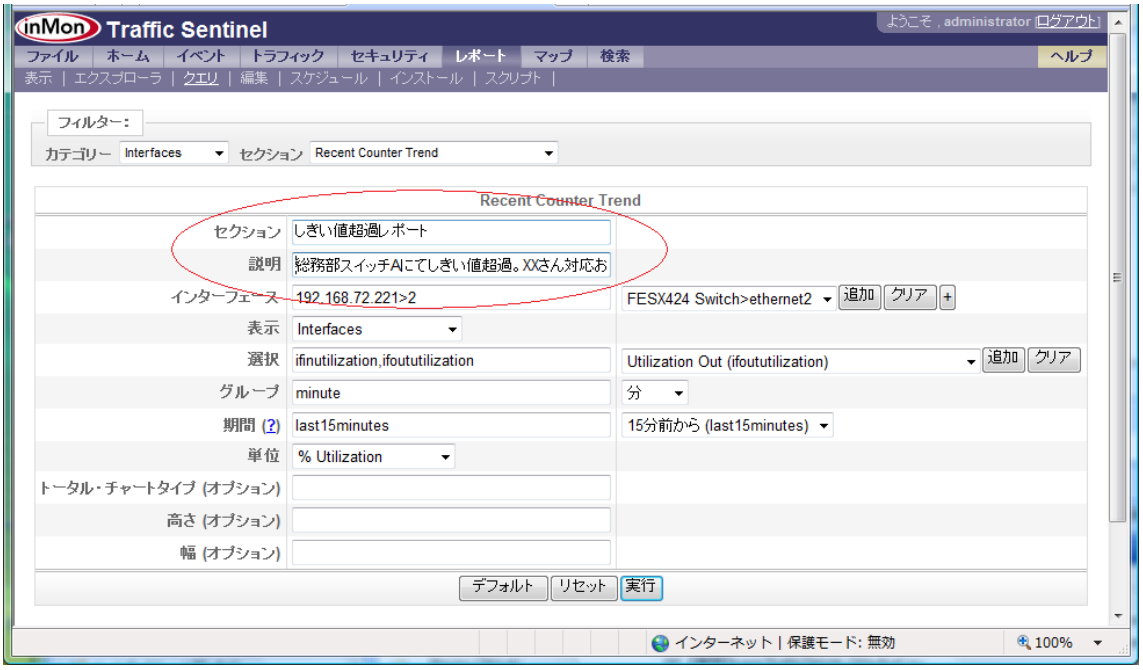
2) レポートのタイトルやコメントの日本語化

デフォルトで定義されているレポート名やコメント（セクション・説明）を変更することが出来ます。

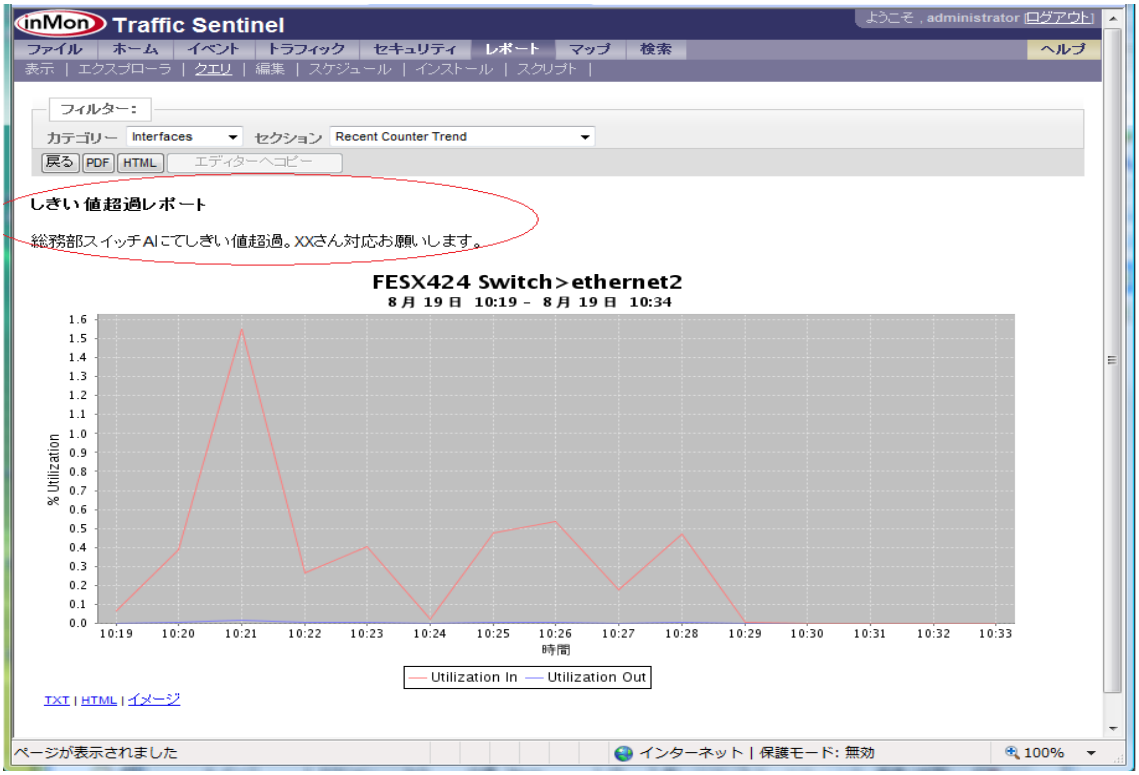
以下デフォルト画面：



これを変更：

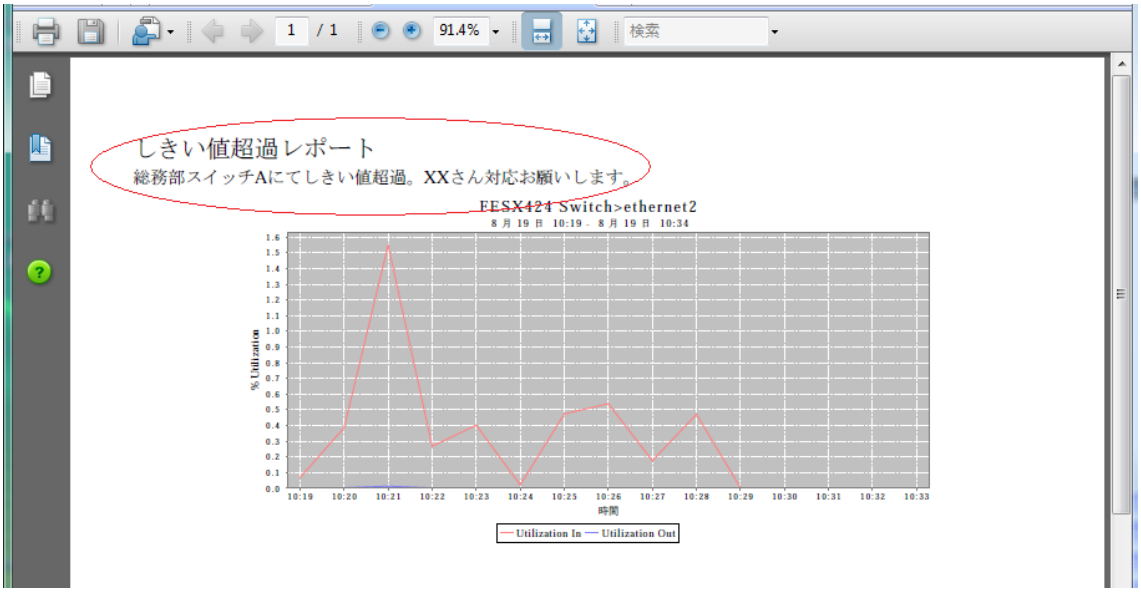


変更されたレポート名やコメントが表示されます。



これを他の担当者に展開する場合は、

PDF 化したレポート：



あるいは、

レポートを HTML 化した URL をメールに転記：

http://TrafficSentinelAddress/inmsf/Report?action=run&group=base&report=interfaces&section=2&name=%E3%81%97%E3%81%8D%E3%81%84%E5%80%A4%E8%B6%85%E9%81%8E%E3%83%AC%E3%83%9D%E3%83%BC%E3%83%88&description=%E7%B7%8F%E5%8B%99%E9%83%A8%E3%82%B9%E3%82%A4%E3%83%83%E3%83%81A%E3%81%AB%E3%81%A6%E3%81%97%E3%81%8D%E3%81%84%E5%80%A4%E8%B6%85%E9%81%8E%E3%80%82XX%E3%81%95%E3%82%93%E5%AF%BE%E5%BF%9C%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99%E3%80%82&input_port=192.168.72.221%3E2&input_show=interfaces&input_select=ifinutilization%2Cifoututilization&input_group=minute&input_interval=last15minutes&input_units=utilization&input_totalslabel=&input_height=&input_width=&resultFormat=html

することによって、展開できます。