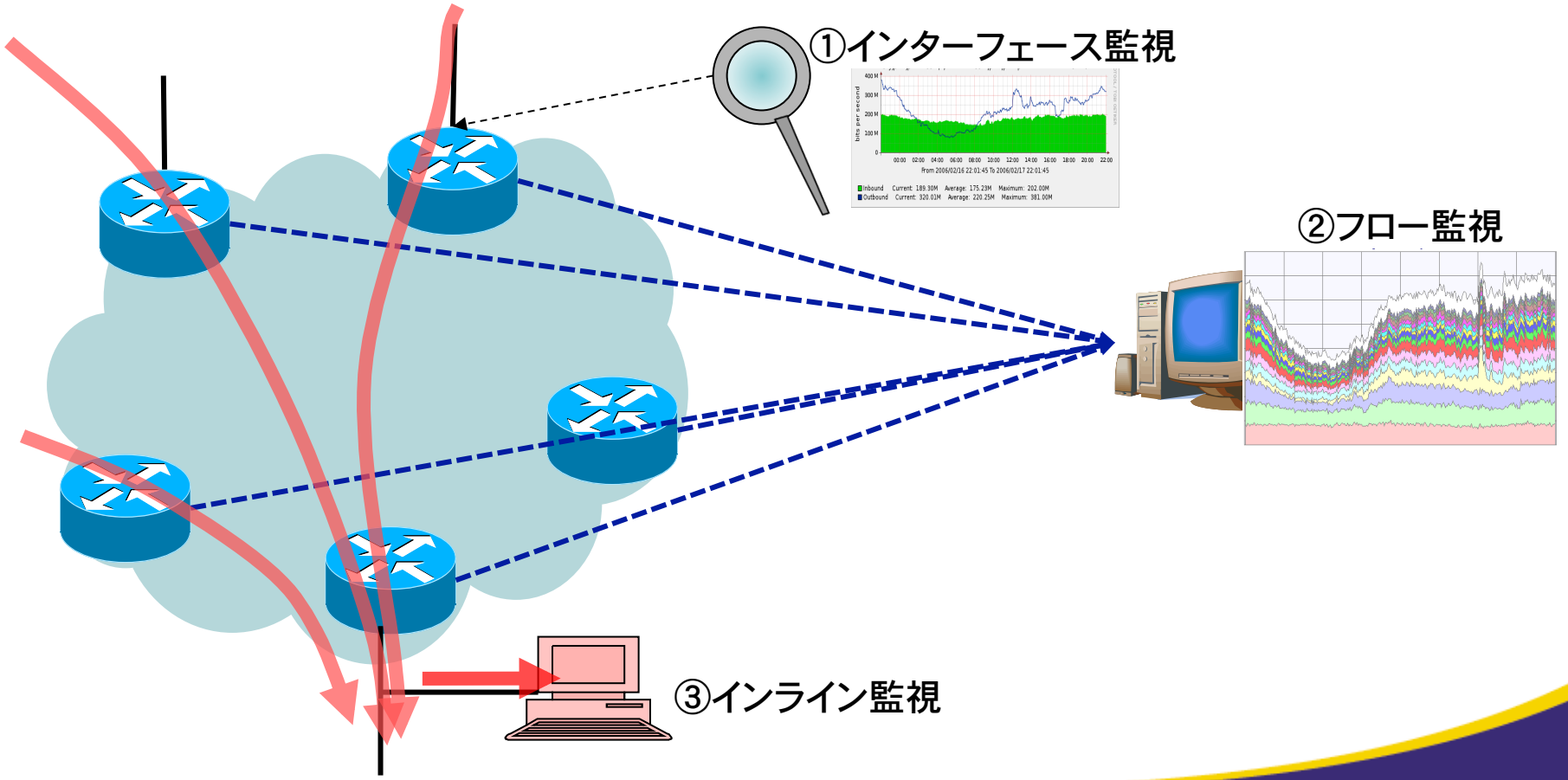
ISP/iDCで実施すべき運用
～ 運用の高度化・高機能化 ～

これからのISPオペレーション

- 運用情報の管理
  - ネットワーク設備管理
  - 故障履歴
  - ネットワーク機器設定の管理
- 可視化
  - ネットワークの可視化
  - トラフィックの可視化
  - ルーティングの可視化
- 自動化
  - 運用のオートメーション化
  - 自動での異常検知・回復

トラフィック監視

① インターフェース毎のトラフィック流量監視
② (ネットワーク全体の)トラフィックフロー監視
③ インラインモニタなどによるトラフィック解析



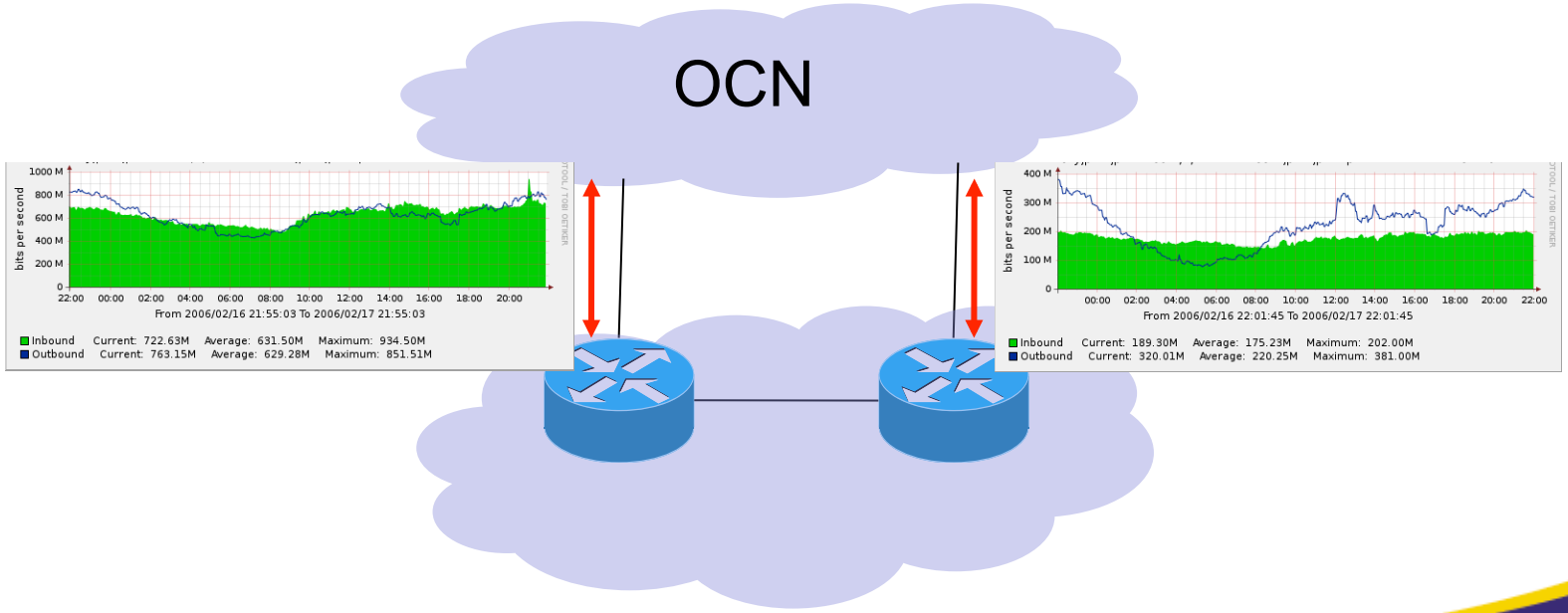
インタフェース毎のトラフィック流量監視

＜ポイント＞

- 過去のデータも保存し、トラフィック流量の変化を監視
- 同一用途のインタフェース（冗長リンク、インターネット接続）は、並べる&合計する
- エラー（Error/Drop/Ignore…）なども監視可能

■使えるツール

- MRTG、rrd（cacti）、rtg



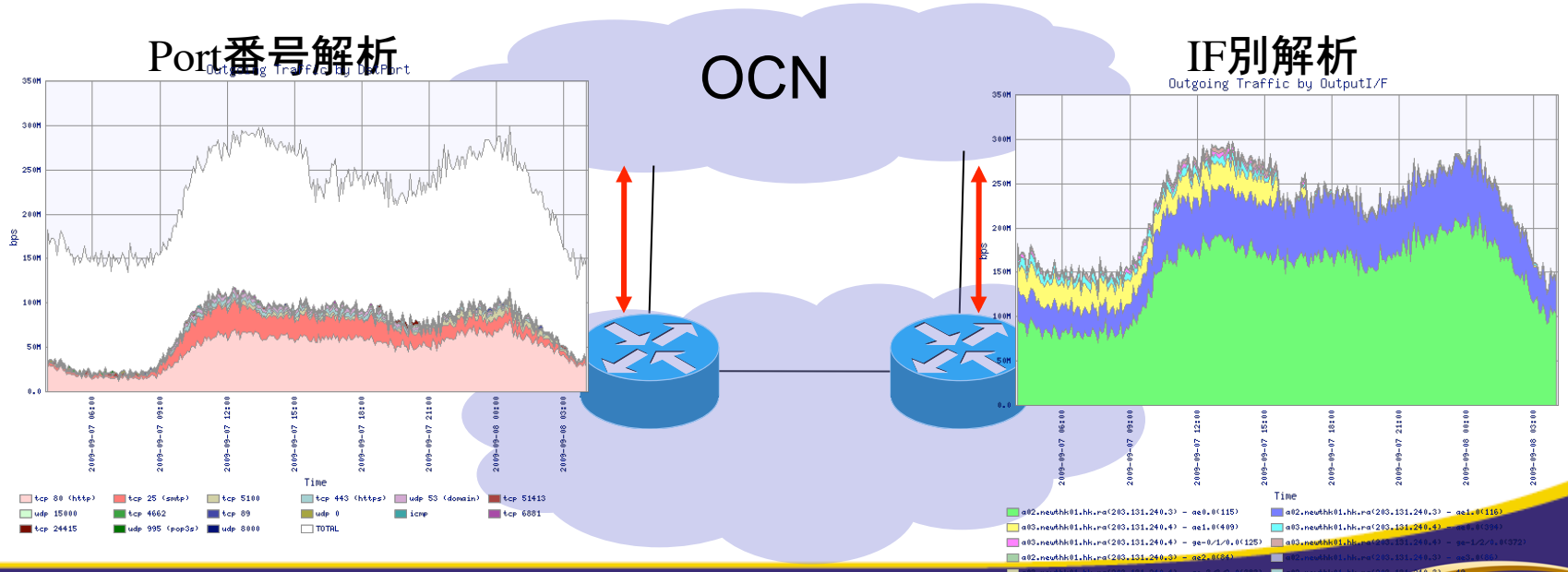
トラフィックフロー監視

＜ポイント＞

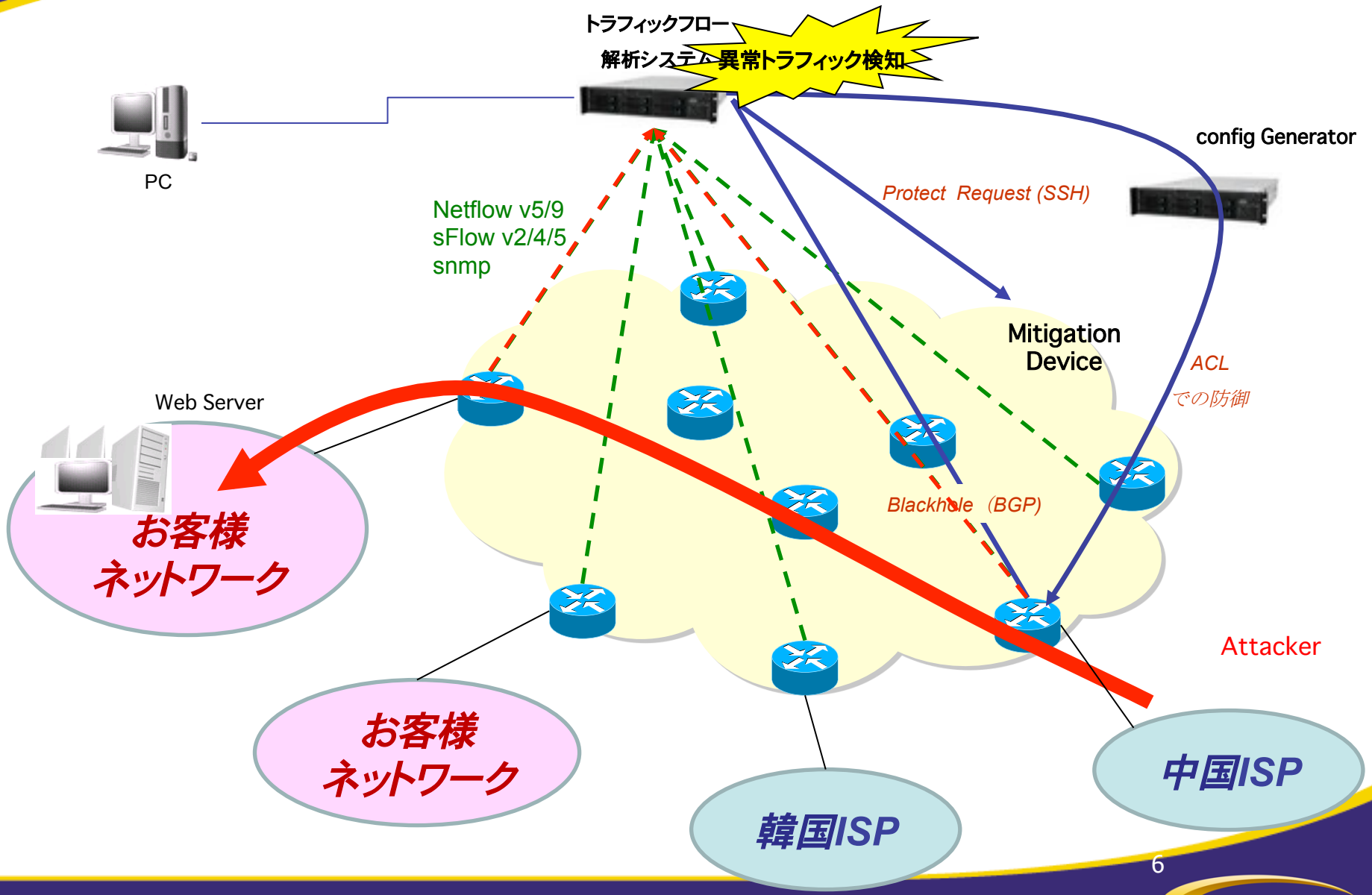
- トラフィックの中身を知る
  - 送受信アドレス、送受信ポート（アプリケーション）、送受信IF毎など
- ネットワーク全体のトレンドを把握し設計にフィードバック
- 特定のフローからDDoSアタックなどを検知

■使えるツール

- NTT-COM:トラフィック解析ツール（SAMURAI）、Genie ATM、Arbor PF



ISPネットワークにおけるトラフィックフロー監視



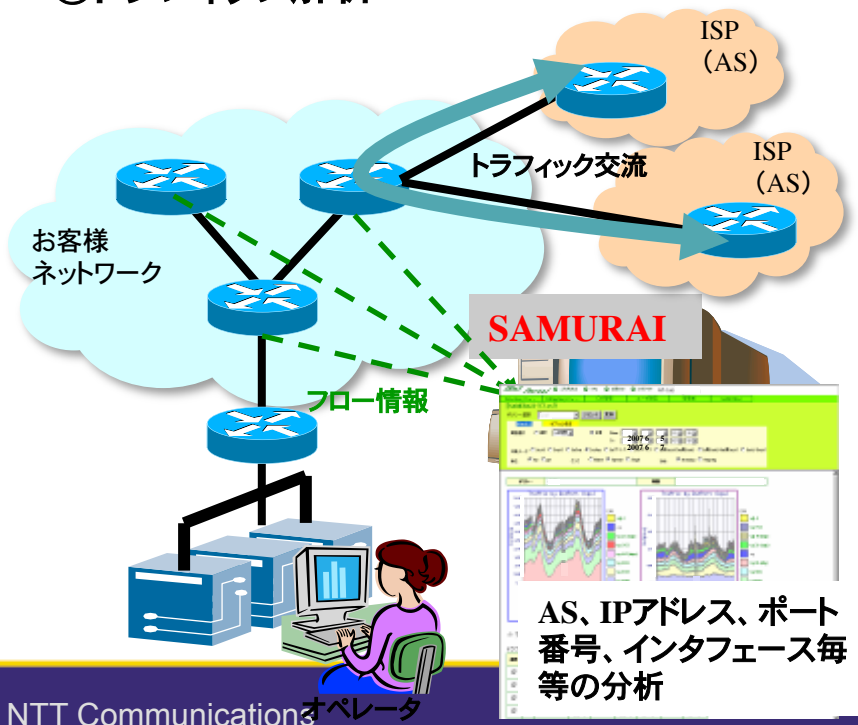
(ISP向け) トラフィック解析ツール

I. ネットワーク全体のトラフィック状況の可視化
II. リアルタイムでのDDoS検知と防御の補助
III. ISP/iDCのためのお客様サービスポータル機能

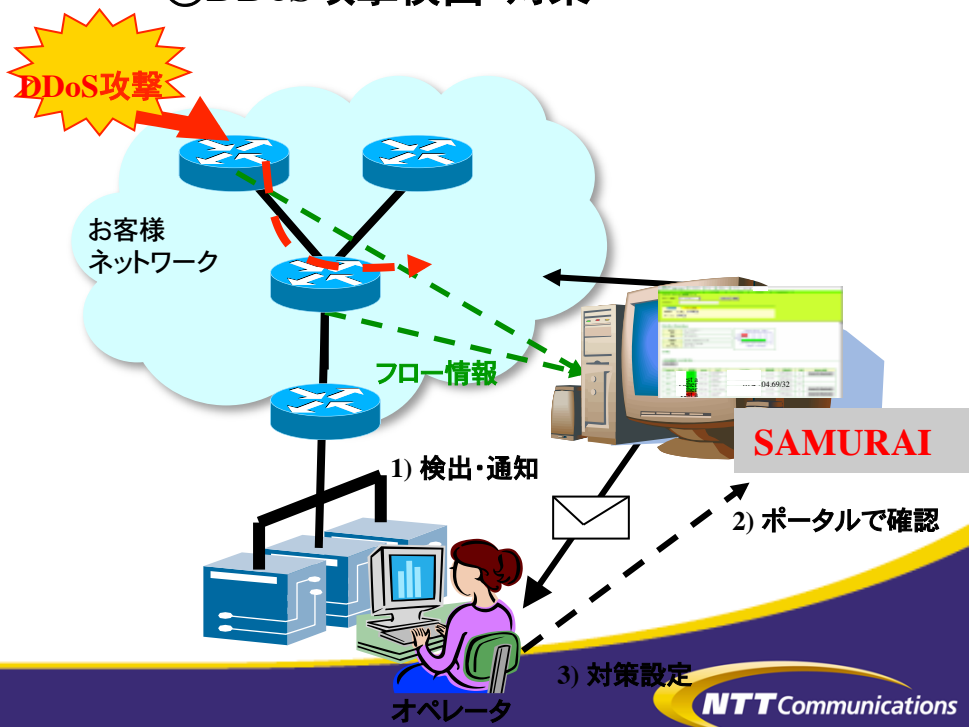
■サービスイメージ■

① フローベースでのトラフィック情報を解析・蓄積し、過去のトラフィック情報を表示
② 異常トラフィック監視・検出・通知・対策指示までのNW運用フローをWebポータル上で実現

①トラフィック解析



②DDoS攻撃検出・対策

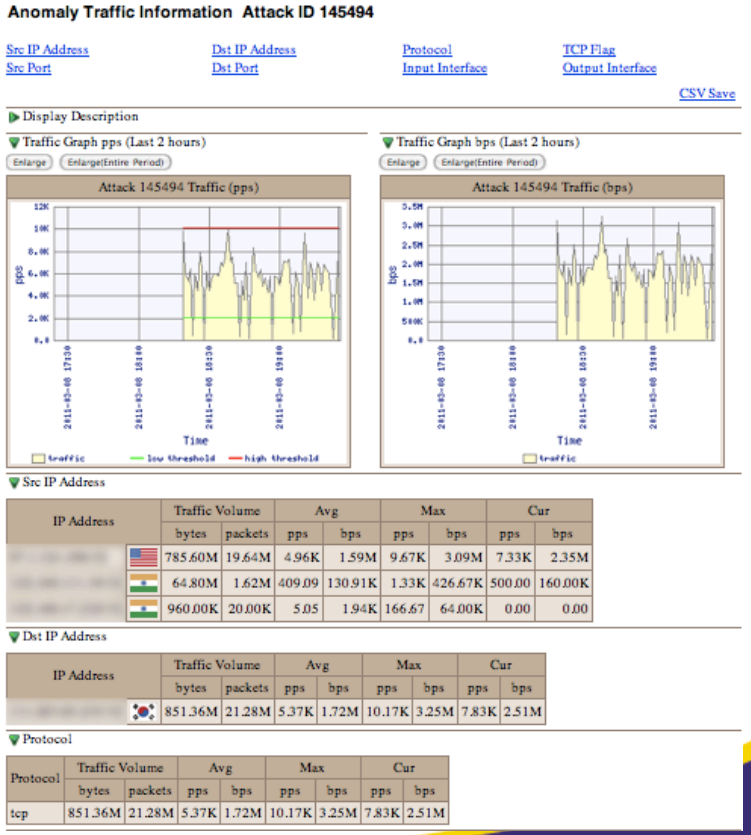


異常トラフィックの検出

ユーザポータル上でDDoS攻撃の状況をリアルタイムで監視することができる他、特定期間のDDoS攻撃の検出状況を、レポートとして参照することができます。

現在のアタックの状態

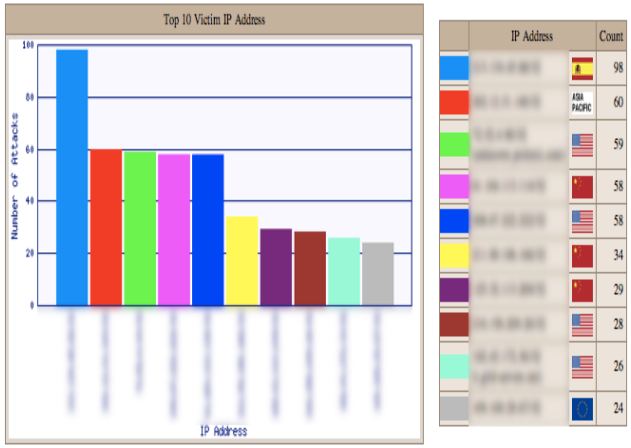
DDoSアタックの詳細分析情報



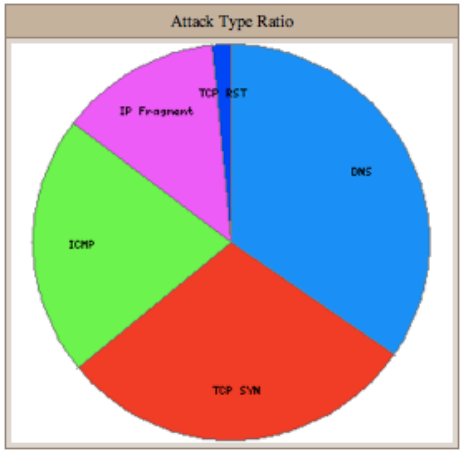
異常トラフィックの分析・レポート

指定期間のDDoS攻撃分析・レポート機能では、攻撃先ホスト、攻撃種別、攻撃継続時間等のパラメータでそれぞれのネットワークのDDoS傾向を分析し、レポートとして参照することができます。

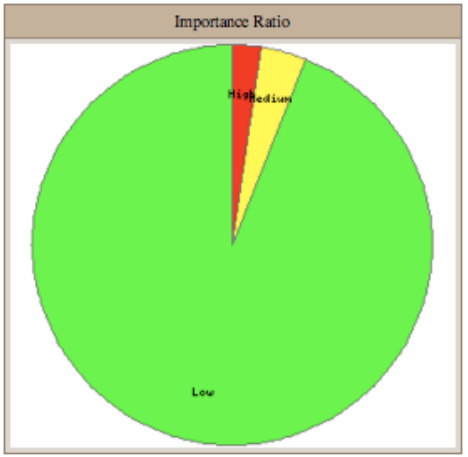
攻撃対象ホスト分析



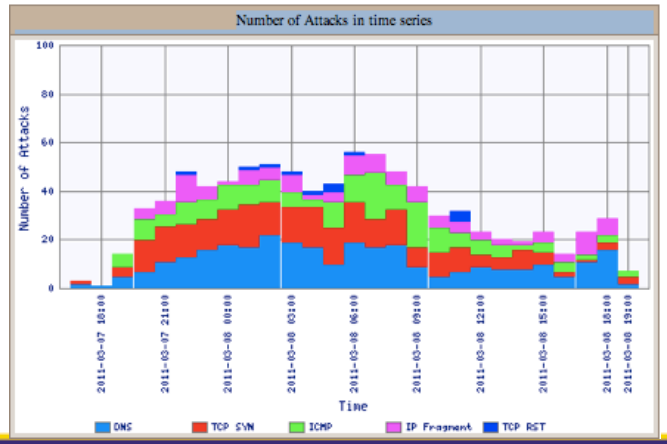
攻撃種別分析



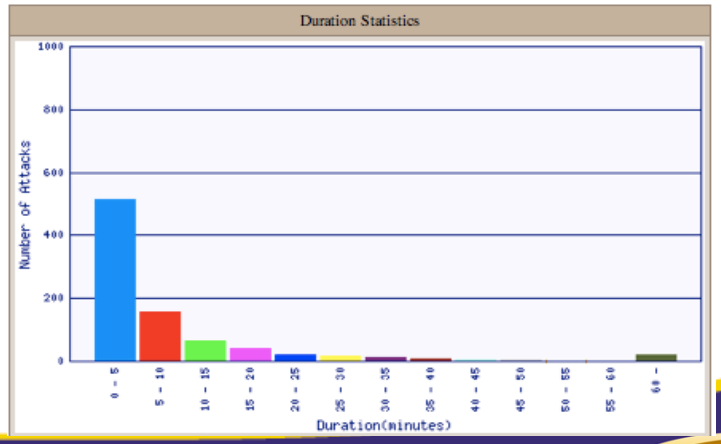
攻撃重要度分析



時系列分析

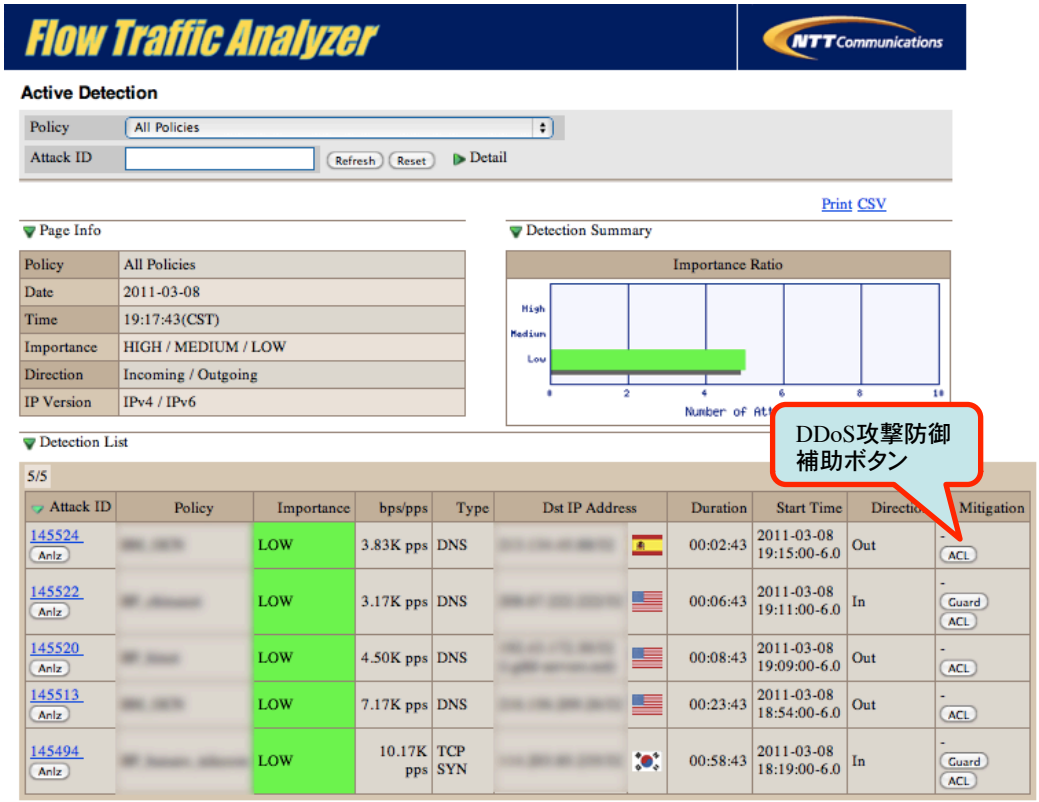


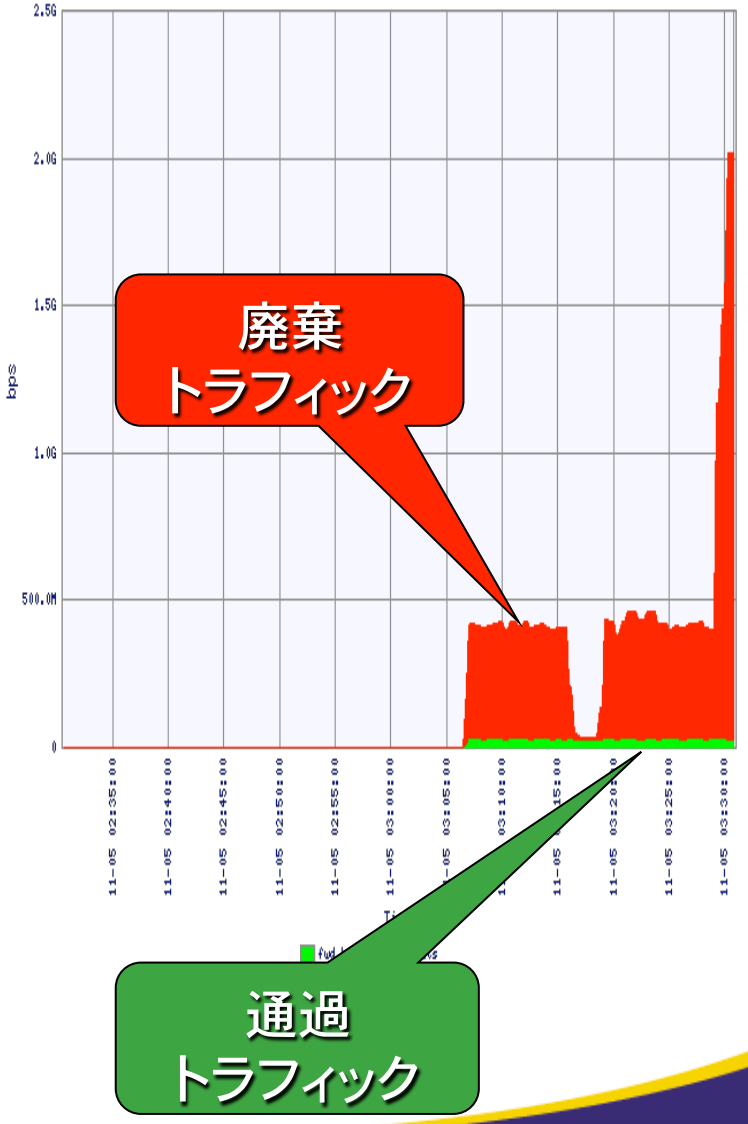
継続時間分析



異常トラフィック防御の画面

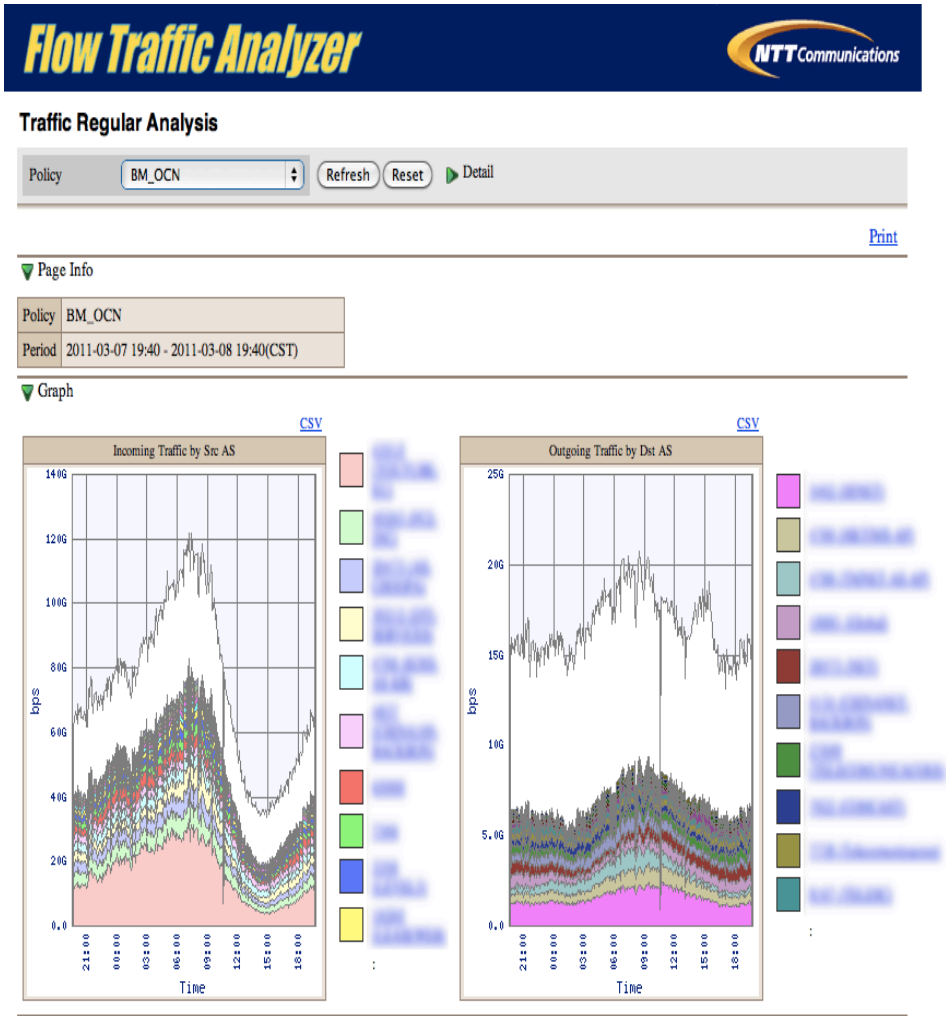
アタック検知画面



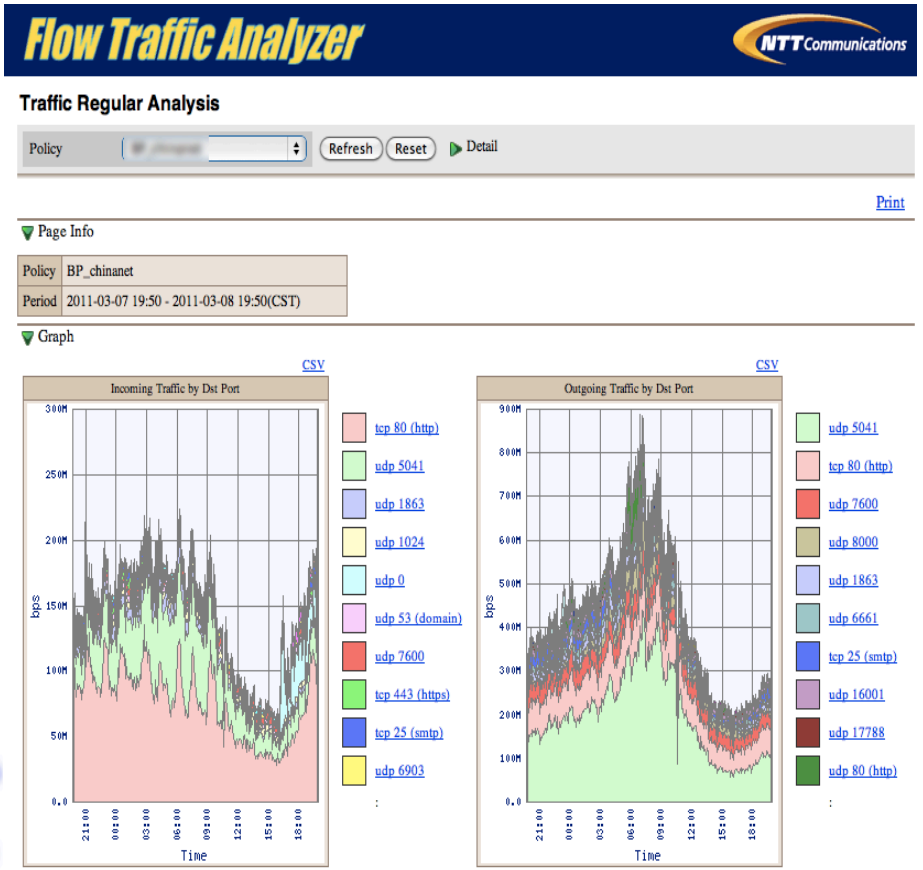


トラフィックの可視化

AS間交流トラフィック



ポート番号毎に関するトラフィック



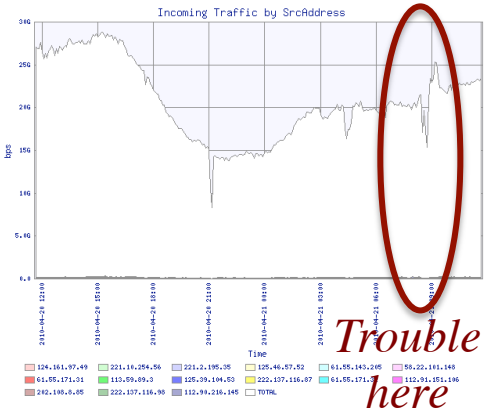
AS間トラフィックやアプリケーションを意識した、トラフィック管理/収容設計にも有効です。

トラフィックの可視化（ドリルダウン）

■トラフィック監視
- リアルタイム監視
- トラフィック解析データ保存 (1.5年)

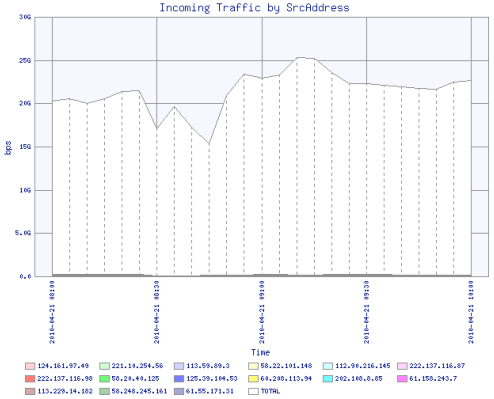
■トラフィック解析
- 好きな時間のトラフィックを抽出
- 絞り込み解析解析機能で細かく分析

Daily Monitoring

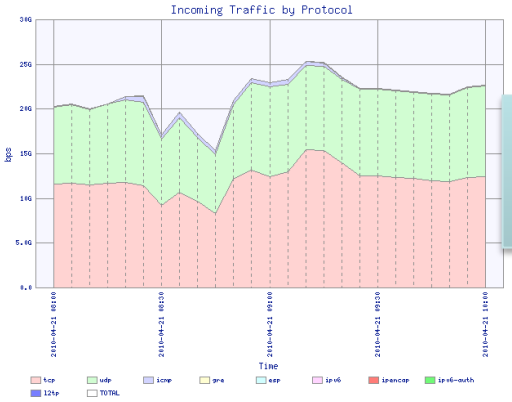


Zoom Up

Pick up traffic from DB

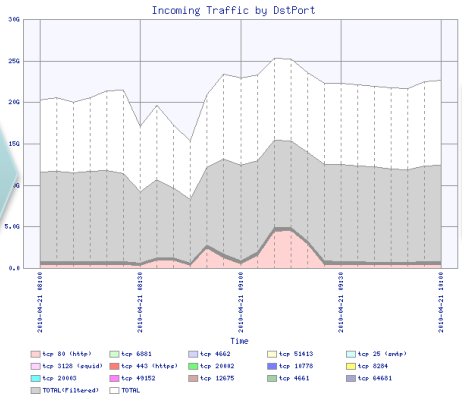


Analysis by Protocol



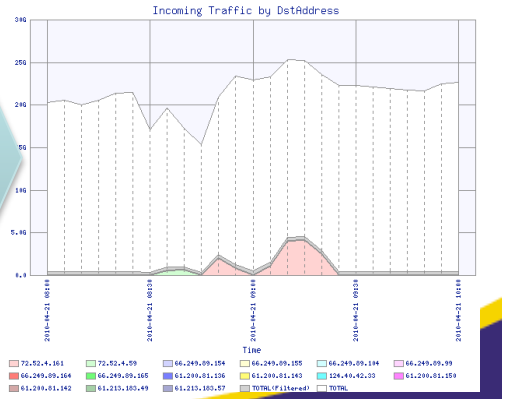
Filter TCP

＋Analysis by Dst Port



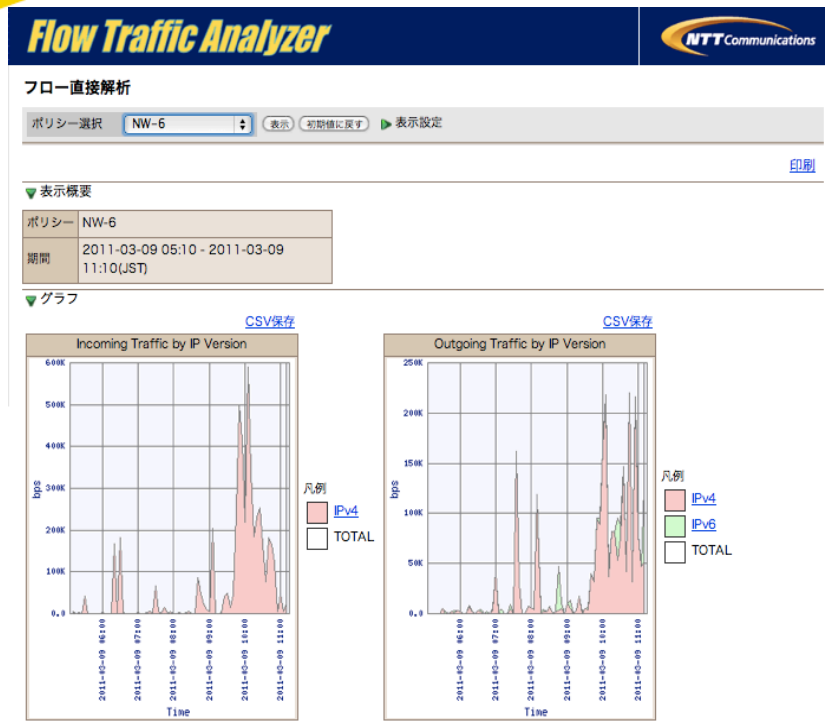
Filter TCP+ Port80

＋Analysis by Dst Addr

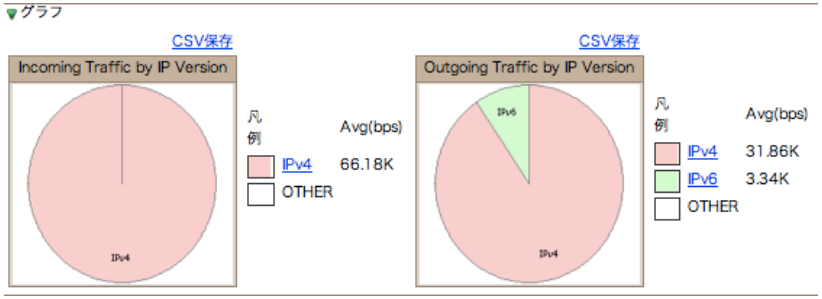


トラフィックの可視化（IPv6）

IPバージョン別解析



IPバージョン分布



■IPバージョン解析
- IPv4とIPv6別トラフィック解析
- IPv6（IPv4）の割合分析

■トラフィック抽出
- IPv6のみを抽出して、それぞれのTOP_N解析を実施

その他便利な機能

定常運用

•複数の重点インターフェース、ユーザトラフィックを並べて監視（自動更新）

ポータル機能

•ポリシー毎、ユーザ毎にポータルを保持
•ユーザ専用ポータル（別URL、別アカウント、自ポリシーのみ閲覧）