ネットワークイベント検出と分析に基づく大規模ネットワークの管理技術

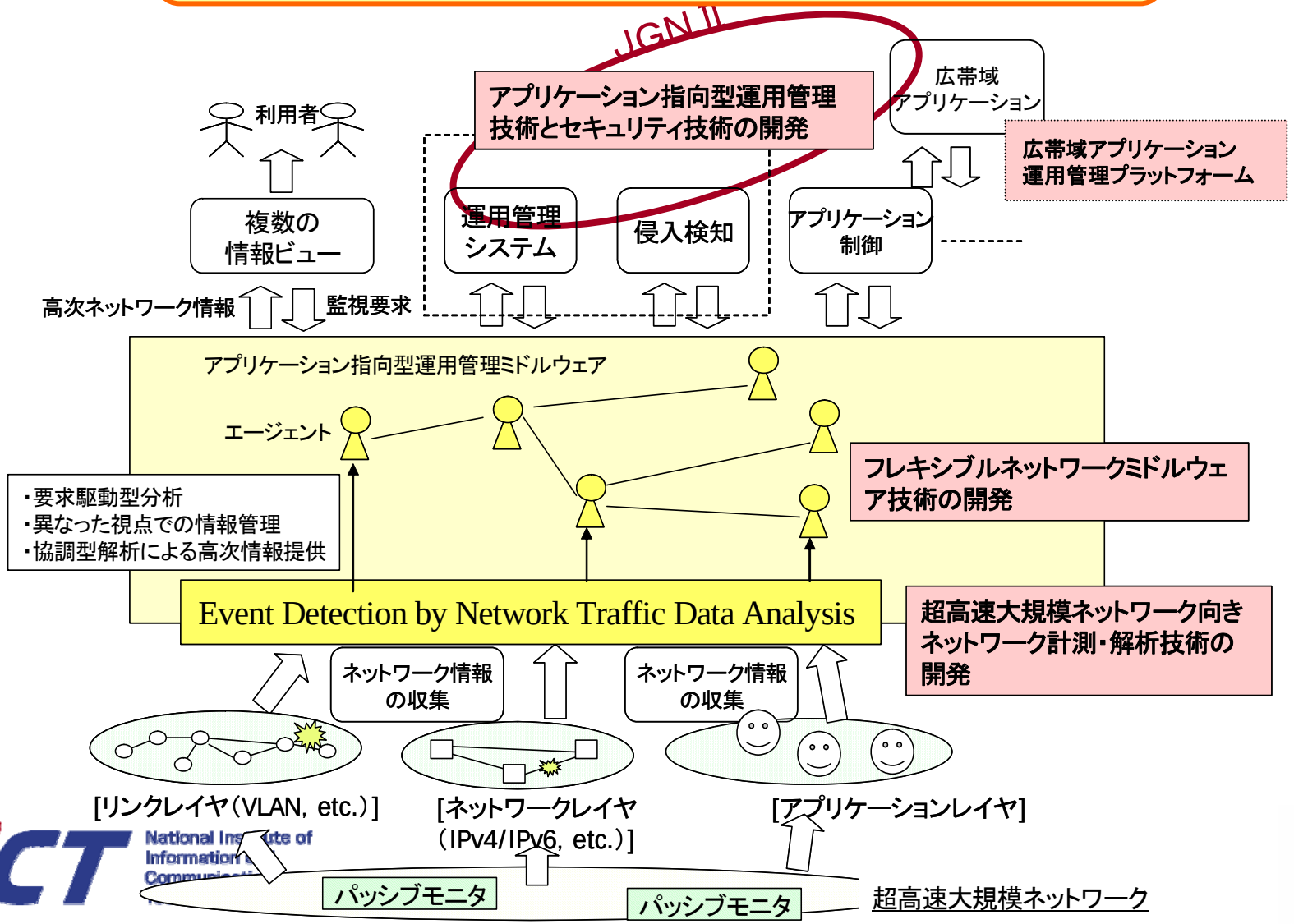
小出和秀	東北RC
菅沼拓夫	東北RC/東北大学
Glenn Mansfield Keeni	東北RC/(株)ｻｲﾊﾞｰ･ｿﾘｭｰｼｮﾝｽﾞ
白鳥則郎	東北RC/東北大学

NiCT National Institute of Information and Communications Technology

JGNII

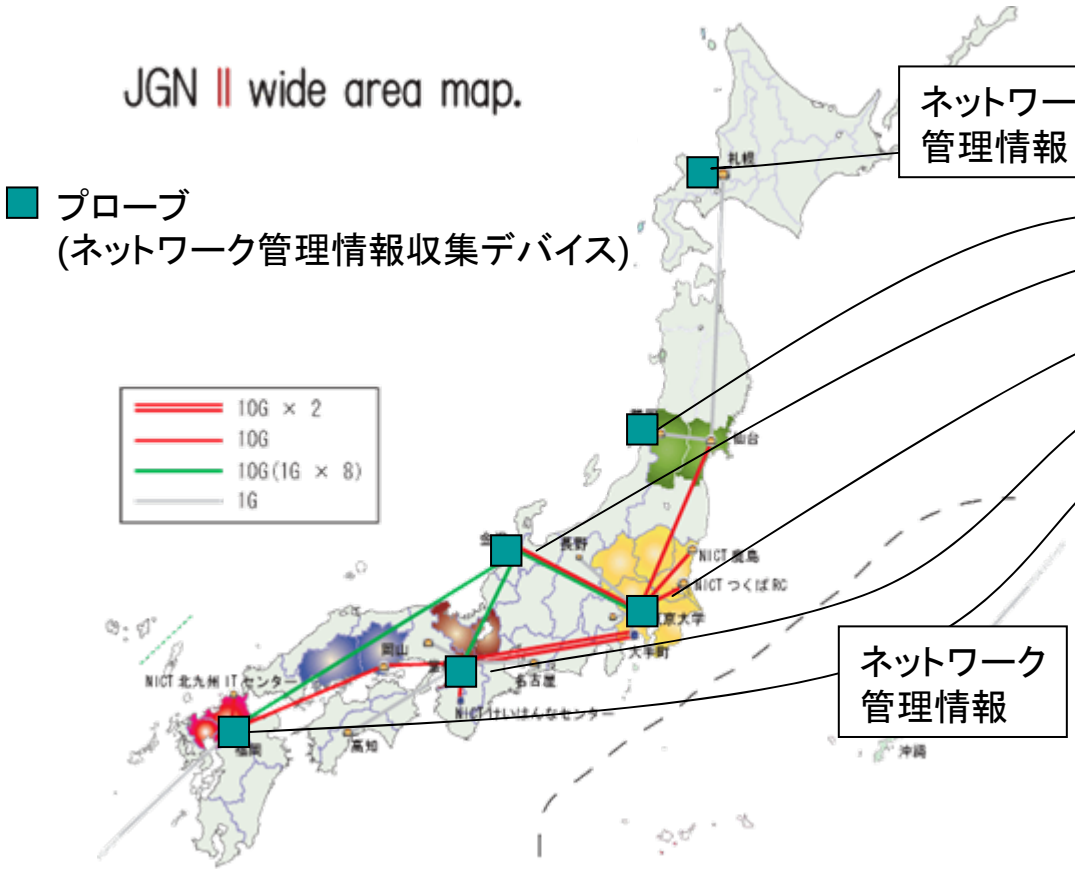
東北RCの研究概要

アプリケーション指向型運用管理プラットフォームの研究開発
（高次ネットワーク情報提供のためのプラットフォーム技術）



1. 超高速大規模ネットワーク向きN/W計測・解析技術の開発

超高速大規模ネットワークにおけるネットワーク計測・解析の課題

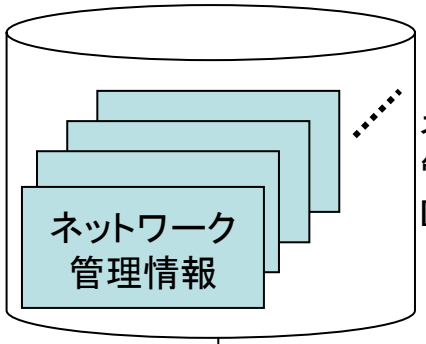


■ プローブ
(ネットワーク管理情報収集デバイス)

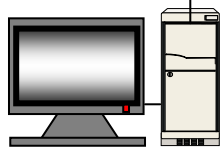
ネットワーク
管理情報

ネットワーク
管理情報

**膨大な量の
ネットワーク管理情報
の蓄積**



ネットワーク
管理情報
DB



ネットワーク
管理端末

**大量のデータから
有用な情報を見つ
けるのは困難**

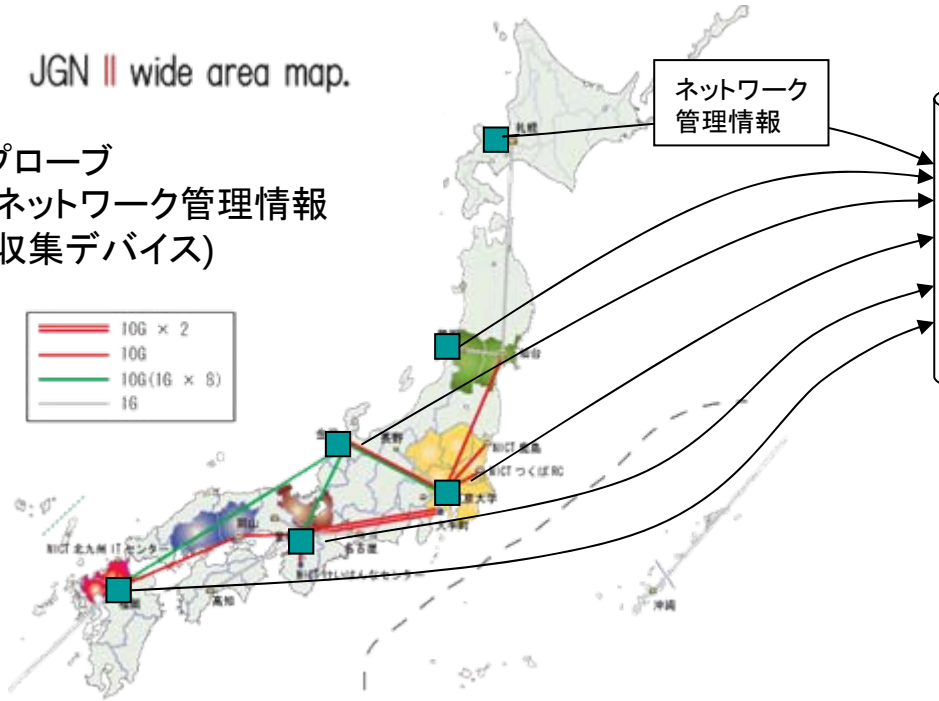
ネットワーク管理者

ネットワーク管理情報:
トラフィック(量の分布、プロトコル分布、回線使用状況など)、
故障、障害、スループット、遅延時間など

NiCT National Institute of Information and Communications Technology

JGNII

本研究開発の目的



- プローブ
  (ネットワーク管理情報
  収集デバイス)

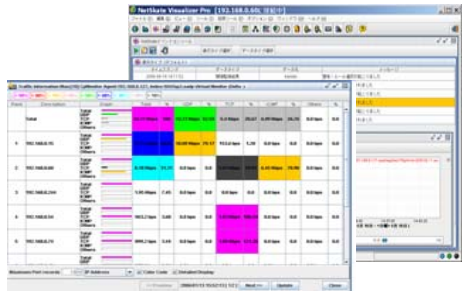
ネットワーク
管理情報

ネットワーク
管理情報

ネットワーク
管理情報DB

ネットワーク
イベント

**ネットワークイベントの
検出**



**ネットワークイベントの
詳細な解析，可視化表示**

**管理作業負担
の大幅な軽減**

ネットワーク管理者

NiCT National Institute of Information and Communications Technology

JGNII

超高速大規模ネットワーク向きネットワーク計測・解析技術の開発

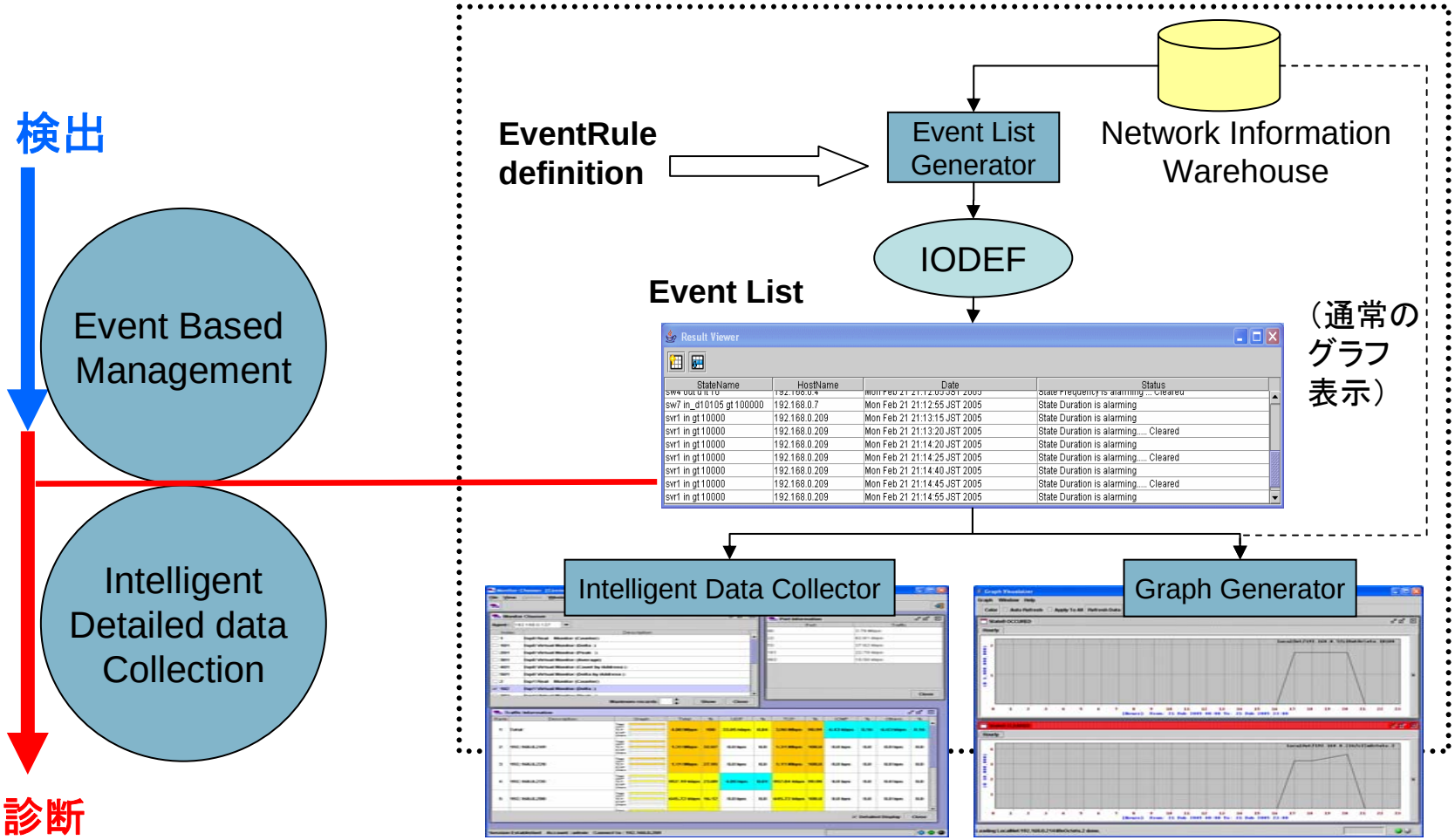
■問題点

- ネットワークの広域・高速化，管理対象となる機器の増大
- ネットワーク情報の大量の蓄積
- 管理に必要な部分のみを抜き出して，効果的かつ詳細に分析する必要性

■目的

- ネットワークトラフィック計測によるイベント検出・解析アルゴリズムの構成
- イベント検出・解析作業支援ソフトウェアの開発

イベント検出・解析支援システム構成



イベント検出・診断支援システム

National Institute of Information and Communications Technology

JGNII

ネットワーク「イベント」検出

■「イベント」の定義

⇒ネットワーク管理者が興味を持つトラフィックパターン

– 障害 (トラフィック消失)　等
– DoS (トラフィック急増)　等
– セキュリティインシデント(特定のパケット検出)　等

■ イベントの検知と記録

– (時系列的)トラフィック情報
– アプリケーションログ等

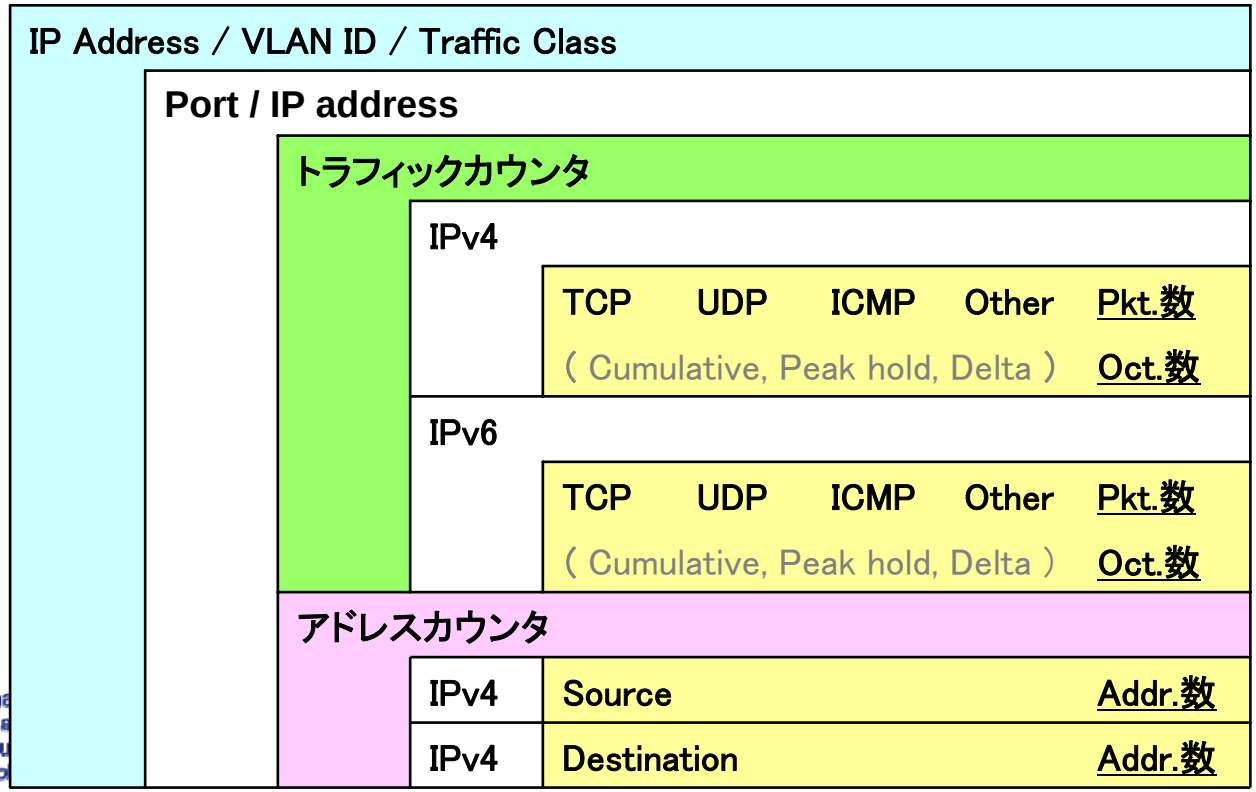
イベントに基づく「データの詳細化」

- イベント関連情報の提供
  - イベント検出をトリガとした詳細トラフィック情報収集
    - イベントコンソールから詳細なグラフ等の情報にアクセスする
  - アドレス・ポート毎の上位Top-Nトラフィック表示
    - トラフィック量だけでなく，組成を明らかにする

3. イベント検出基盤技術 - (1)

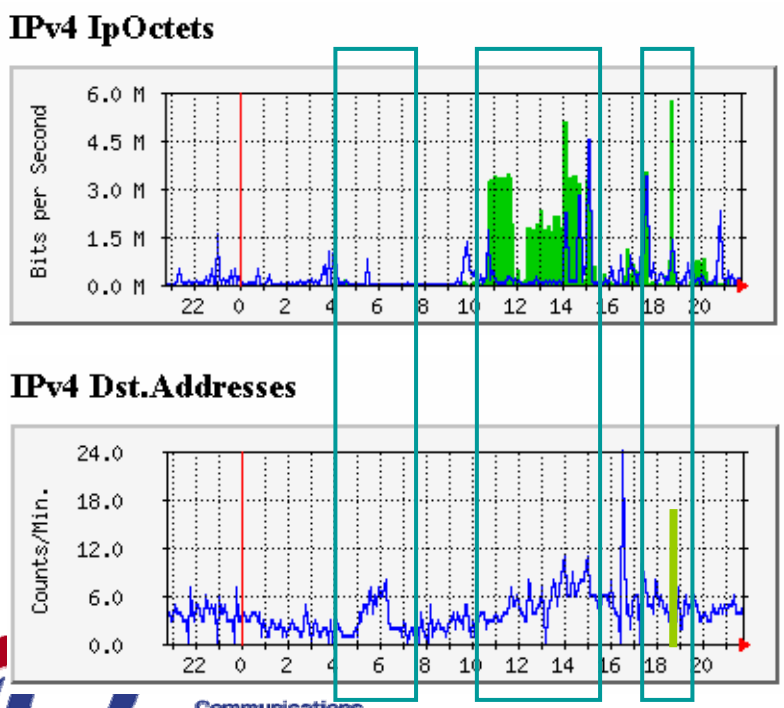
■ CpMonitor
- ネットワークタップ型計測ソフトウェア

■パケットヘッダ情報による分類　■累積値 / 差分値 / ピーク値
■アドレス数カウンタ　■テナント毎集計
■tcpdump 互換機能（パケットダンプファイル入出力 ）



イベント検出基盤技術 - (2)

- Category Transform
  - カテゴリ毎のトレンド＋カテゴリ数そのものの変化に注目
    ⇒より詳細なトラフィック変動の把握が可能
  - 例:トラフィック量増大＋IPアドレスカテゴリ数増大⇒DoS?



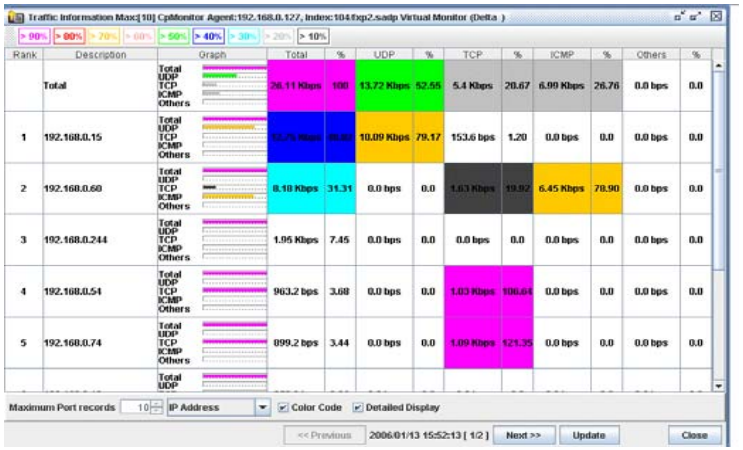
Case(1): Only Addresses increases
Case(2): Only Octets increases
Case(3): There is a DoS attack?

NiCT Communications Technology

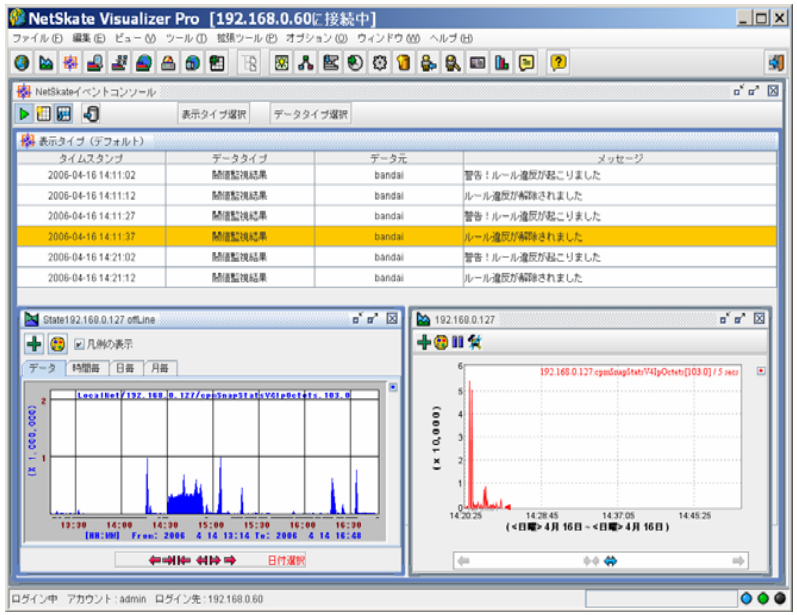
JGNII

研究結果

- **これまでの成果**
  - **ネットワークイベント検出モデル**（Ver.0.5）の詳細設計を行い、実トラフィックデータを用いた実験によりその有効性を確認した
  - 広域ネットワーク環境におけるトラフィック情報のリアルタイム分析を支援する**「Top-Nトラフィック分析支援システム」を完成**．**Winny等による異常トラフィックの検出・分析**を効果的に支援することが可能となった



Top-N traffic sources/consumers with Protocol-wise details



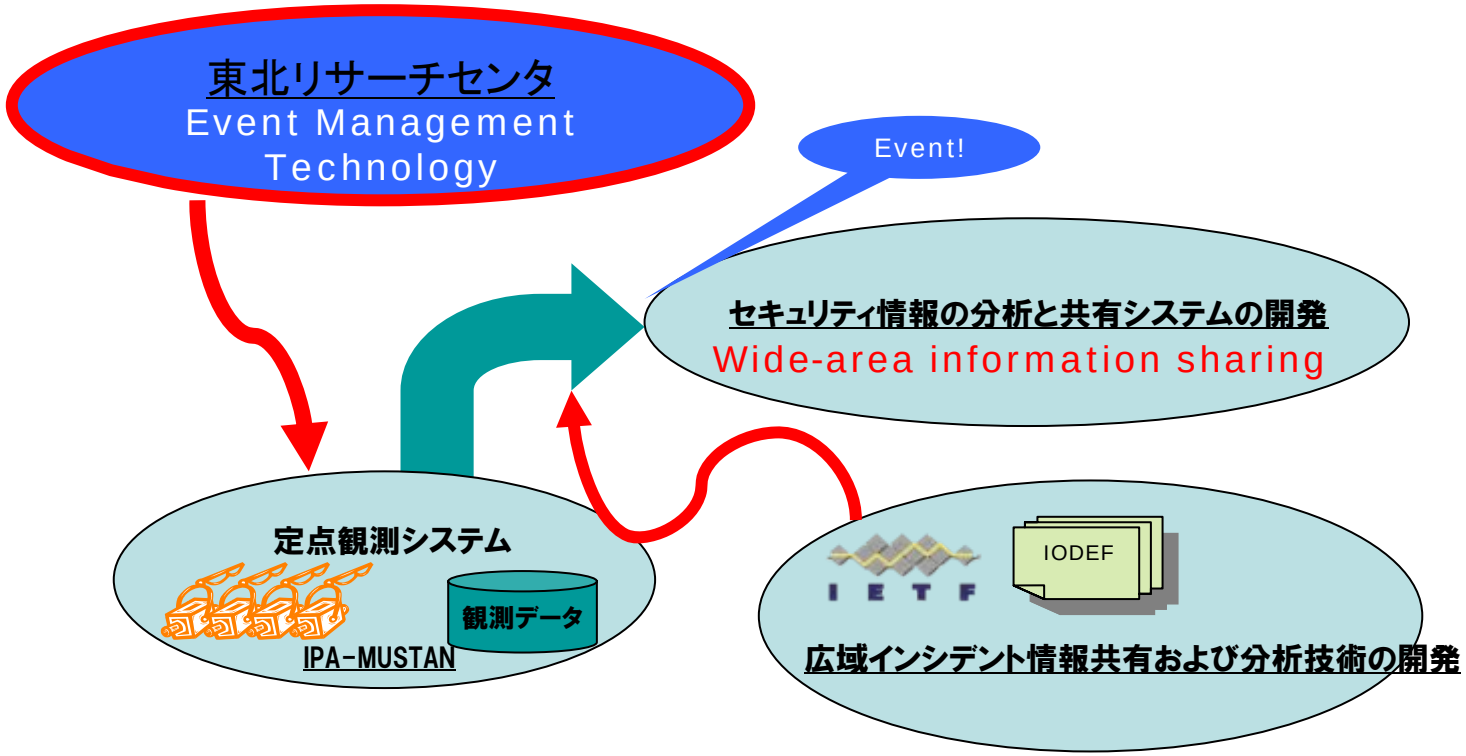
Events displayed on **I**ntegrated **C**onsole for **E**vents (ICE)

National Institute of Information and Communications Technology

JGNII

4. 今後の方向性

■ 今年度の研究予定
- ネットワークイベントの分析、可視化を支援するツールとして
  広域ネットワーク環境における「イベント追跡システム」の完成



今年度の開発目標(抜粋)

- イベントの送受信
  - 従来:SNMP trapを利用
  - これから:IODEF(Incident Object Description and Exchange Format) を利用
  - 電子メールによるXMLベースでのイベントトランスポート
  - トラフィック・ログ情報を添付したイベントの送受信

  ⇒イベント情報の広域共有につなげていきたい
- イベントに基づく詳細情報出力をより高度化
  - イベントの性質にあわせた情報の出力
  - イベント毎のカスタマイズ機能，計測知識の導入

5. おわりに

- 超高速大規模ネットワーク向きネットワーク計測・解析技術の開発
- イベントの検出と分析に基づく効率的なネットワーク計測・解析アプリケーションの開発

- JGNをはじめとした大規模ネットワークの計測を効率化することを目指していく