研究テーマ：超高速大規模ネットワーク向き ネットワーク計測実験に関する研究（1/2）
（プロジェクト番号JGN2- A16059）

研究機関： 情報通信研究機構 東北JGNⅡリサーチセンター,
岩手県立大学ソフトウェア情報学部,（株）サイバー・ソリューションズ

研究の概要：
JGNⅡのような広域ネットワーク上でのネットワーク管理およびアプリケーション運用を支援することを目的として、超高速大規模ネットワーク上においてネットワーク情報を効果的に収集・分析する手法を提案し、テストベッドネットワークを用いた実験によってその有効性、実用性を検証する。

研究の目的：
超高速大規模ネットワーク上においてネットワーク情報を効果的に収集・分析することを目的とし、様々なレイヤ、プロトコルで分類された大量のトラフィックデータの中から解析に必要となる情報を効果的に抽出する「ネットワークトラフィック予測によるイベント検知手法」を提案し、それに基づく新しいネットワーク運用管理のための基盤技術を開発する(図1)。
具体的には、以下の3つの研究項目に関する研究を推進する。

(1)イベント検出モデル
(2)イベント観測システム開発
(3)イベント情報提供システム開発

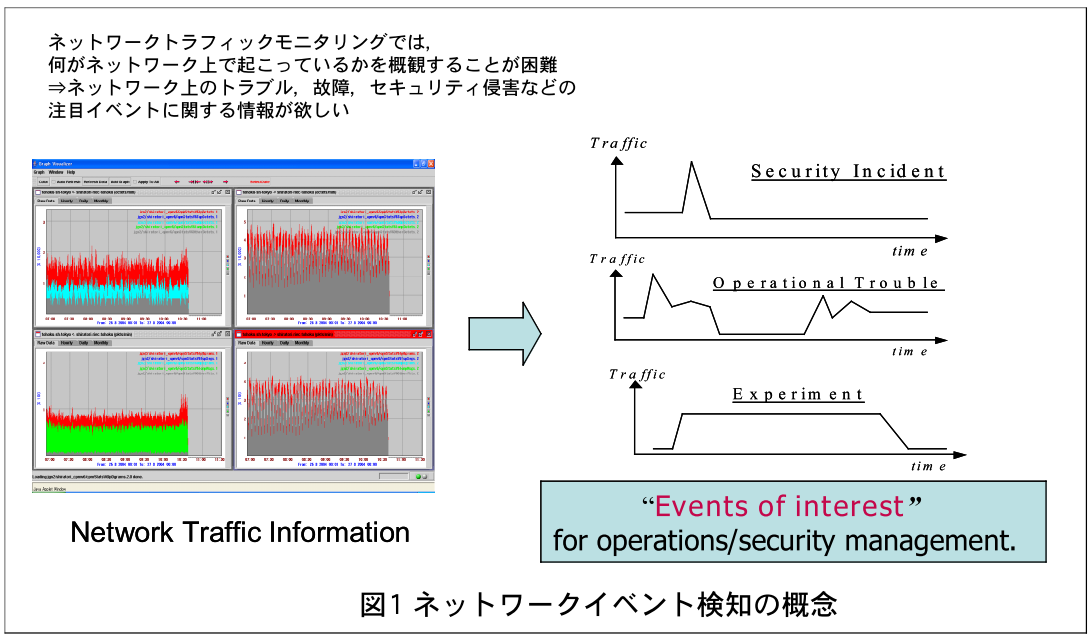


図1 ネットワークイベント検知の概念

実験機器構成：

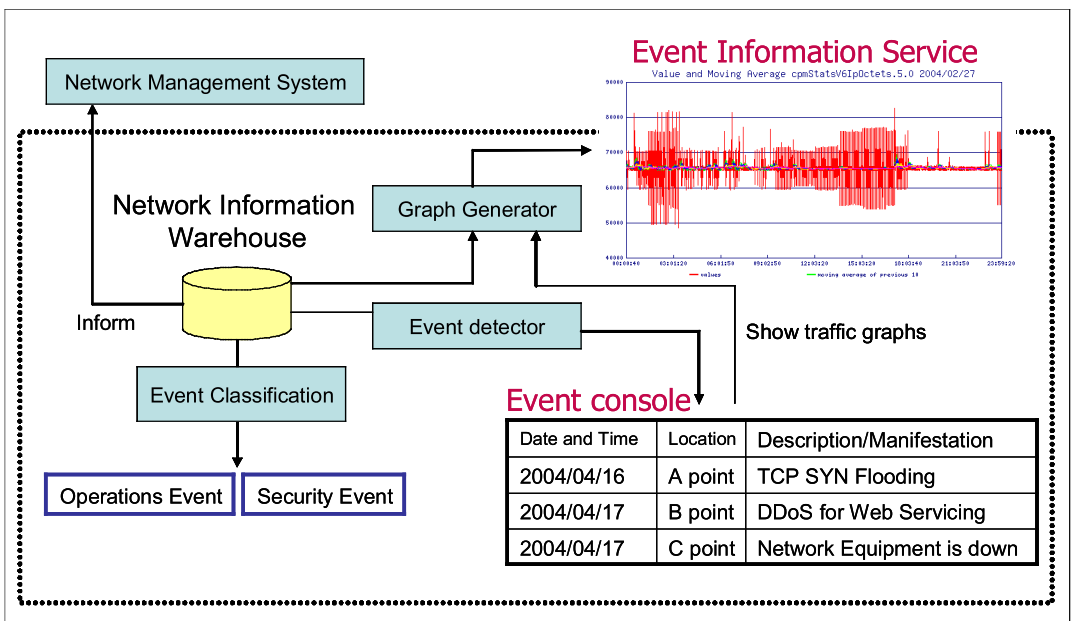


図2 イベント観測システムの基本構成

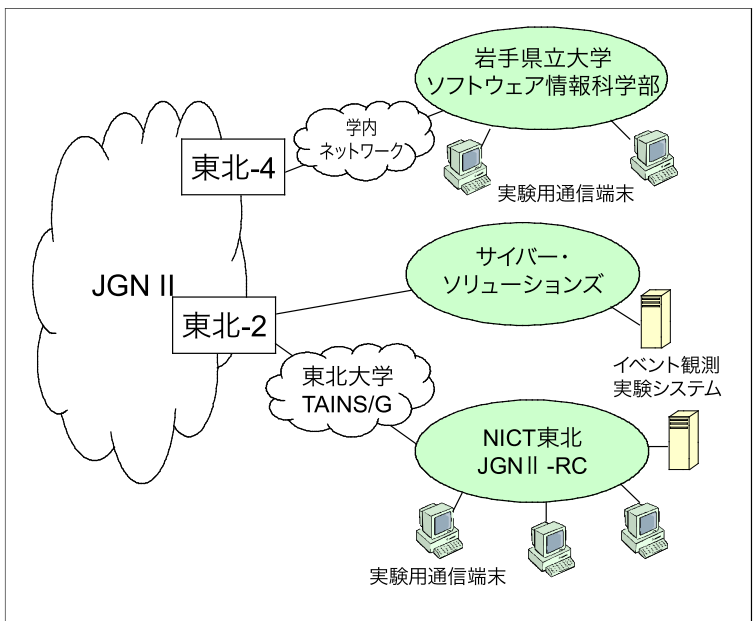


図3 予備実験用ネットワーク構成

研究テーマ：超高速大規模ネットワーク向き ネットワーク計測実験に関する研究（2/2）
（プロジェクト番号JGN2- A16059）

研究機関： 情報通信研究機構 東北JGN II リサーチセンター,
岩手県立大学ソフトウェア情報学部,（株）サイバー・ソリューションズ

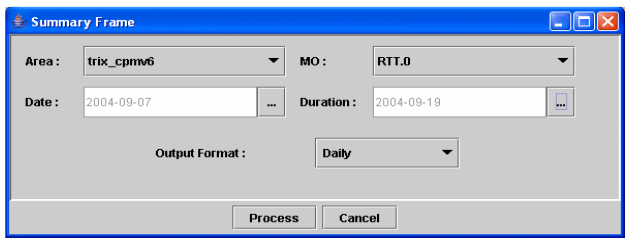
研究開発状況：

(1)イベント検出モデル

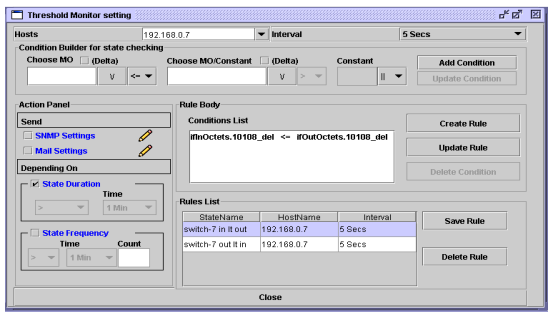
周波数解析に基づくトラフィック異常検出手法、およびトラフィック情報とアプリケーションログの統合的計測・解析に基づくイベント検出モデルの詳細設計を進めている。研究成果は、国内学会・研究会等にて11件発表している。

(2)イベント観測システム開発

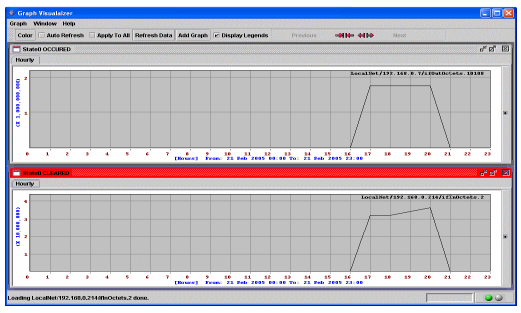
定義したイベント検出モデルの評価を、実ネットワーク上で行う際の作業を効果的に支援するためのツール群として、「イベント観測システム」の開発を進めている(図4)。



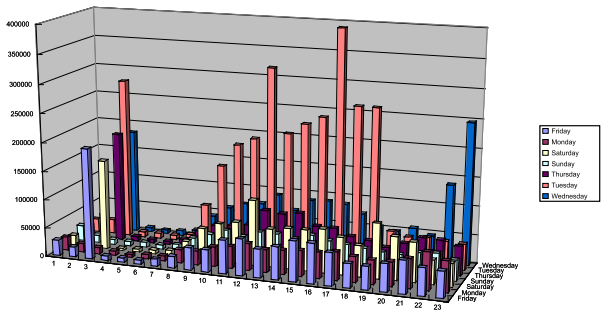
(a) Summary traffic data UI



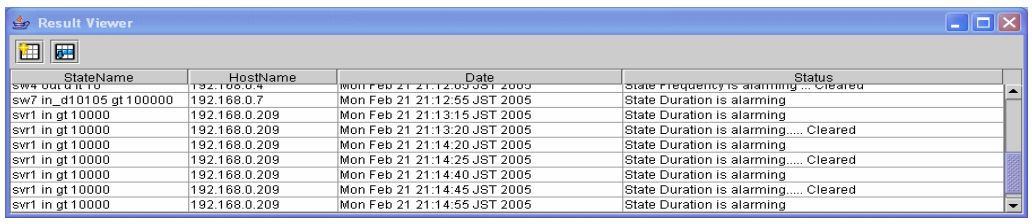
(c) Rule definition UI



(d) Traffic graphs corresponding to the event



(b) Summary traffic data visualization



(e) List of alarms

図4 開発したイベント観測システムのツール群

今後の予定：

これまでの研究開発を継続し、イベント検出モデルの詳細化とイベント観測システムの高度化を進める。また今後、イベント情報をネット上で提供するためのイベント情報提供システムの開発を行う。更に、予備実験用ネットワークを用いた実験を継続するとともに、実験環境を拡大して、実ネットワーク環境における本システムの実用性・有効性について検証を進める予定である。

将来の展望：

本システムにより、これまでネットワーク管理者が手作業で行ってきたトラフィック情報からのネットワークイベント検出・分析作業が効率的に行えるようになり、高速・広域ネットワークの管理、具体的には障害やサイバーアタックに対する迅速な対応、網構成設計の改良の効率化などに大きく貢献することが期待できる。