広域ネットワーク対応のセキュリティ監視システム

2006 年 6 月、KDDI 研究所は、回線やサーバーの機能を妨害し不能に陥らせることにより広域ネットワークに影響を及ぼすサイバー攻撃[ウィルス感染、DoS(Denial of Services/サービス不能攻撃)・DDoS(Distributed Denial of Services/協調・分散型サービス妨害)攻撃など]を対象として、ネットワークに設置した機器によってトラフィックログおよびセキュリティログを収集し、それらのログを統合解析して自動的に異常を検出する「広域セキュリティ監視システム」を開発した。

開発した監視システムは、ネットワーク情報を収集する「エージェント」と、収集された情報を統合解析する「マネージャ」で構成されている。「エージェント」は、10Gbps の超高速回線を流れるトラフィックのパターンから異常を検知する機能と、異常の原因調査を支援する機能を備えている。この「エージェント」からの情報を統合管理し、攻撃された範囲、量的規模を迅速に把握するのが「マネージャ」である。

本監視システムは、ネットワークの特性を自動的に学習するため、事前の条件設定を行うことなく、多種多様な情報の中から危険な挙動を抽出することが可能である。

また、回線状態の把握も自動化・簡易化されているため、運用担当者のスキルに依存することのない本監視システムは、KDDI において、IP サービスの質的向上に寄与している。

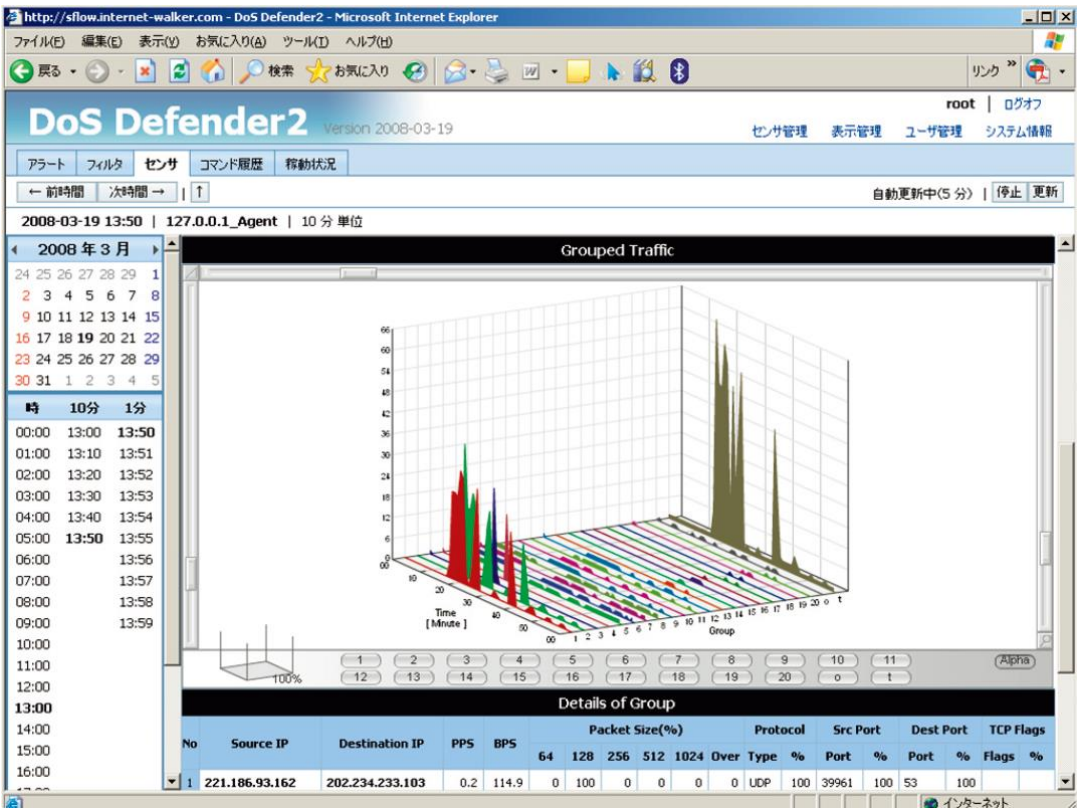

図 「広域セキュリティ監視システム」によるトラフィック自動分類