研究テーマ：インターネット広域観測による次世代攻撃検知技術に関する研究開発（1/2）

（プロジェクト番号　JGN2-A17041）

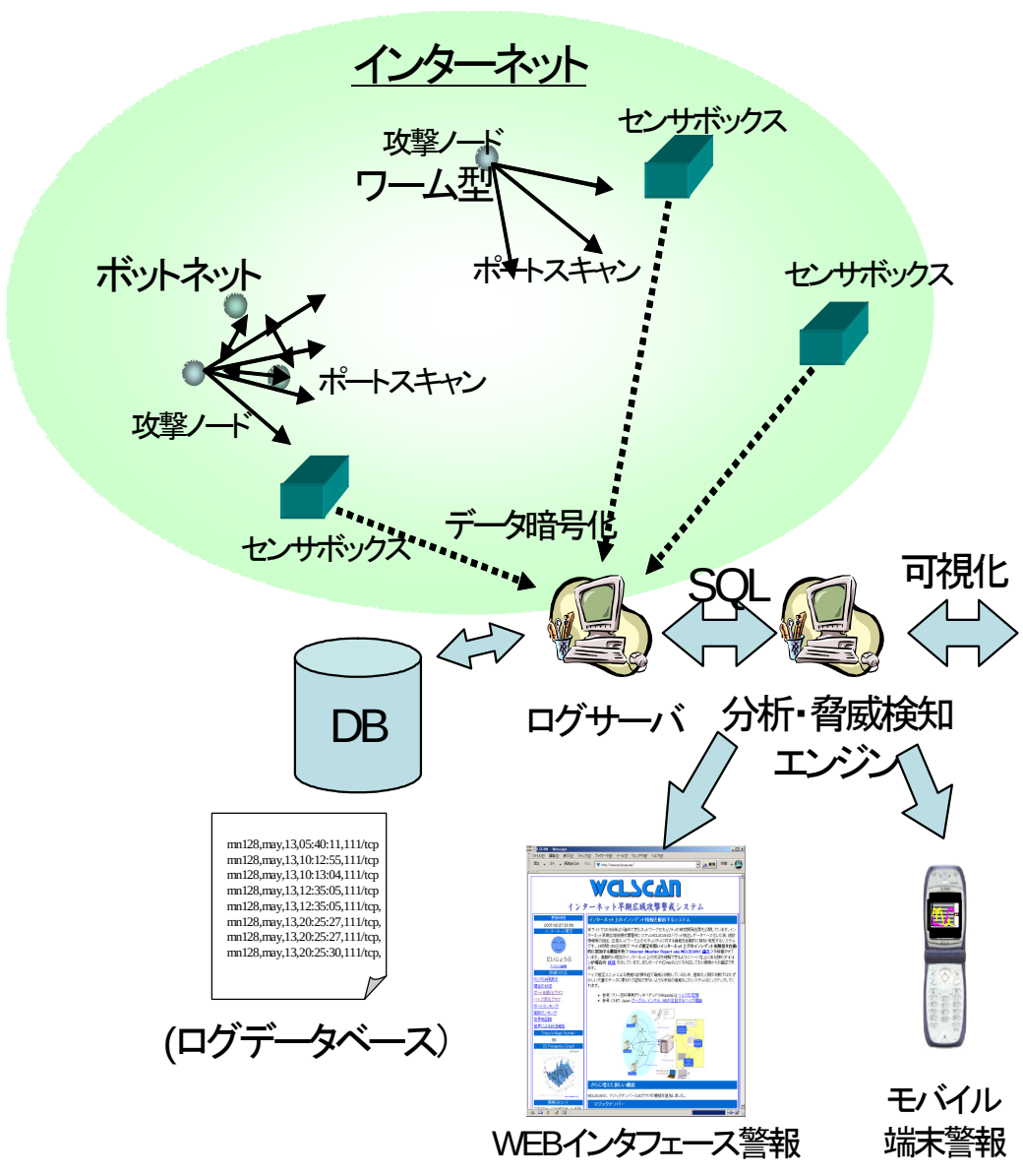
研究機関：　早稲田大学理工学術院、（株）三菱総合研究所、群馬大学工学部

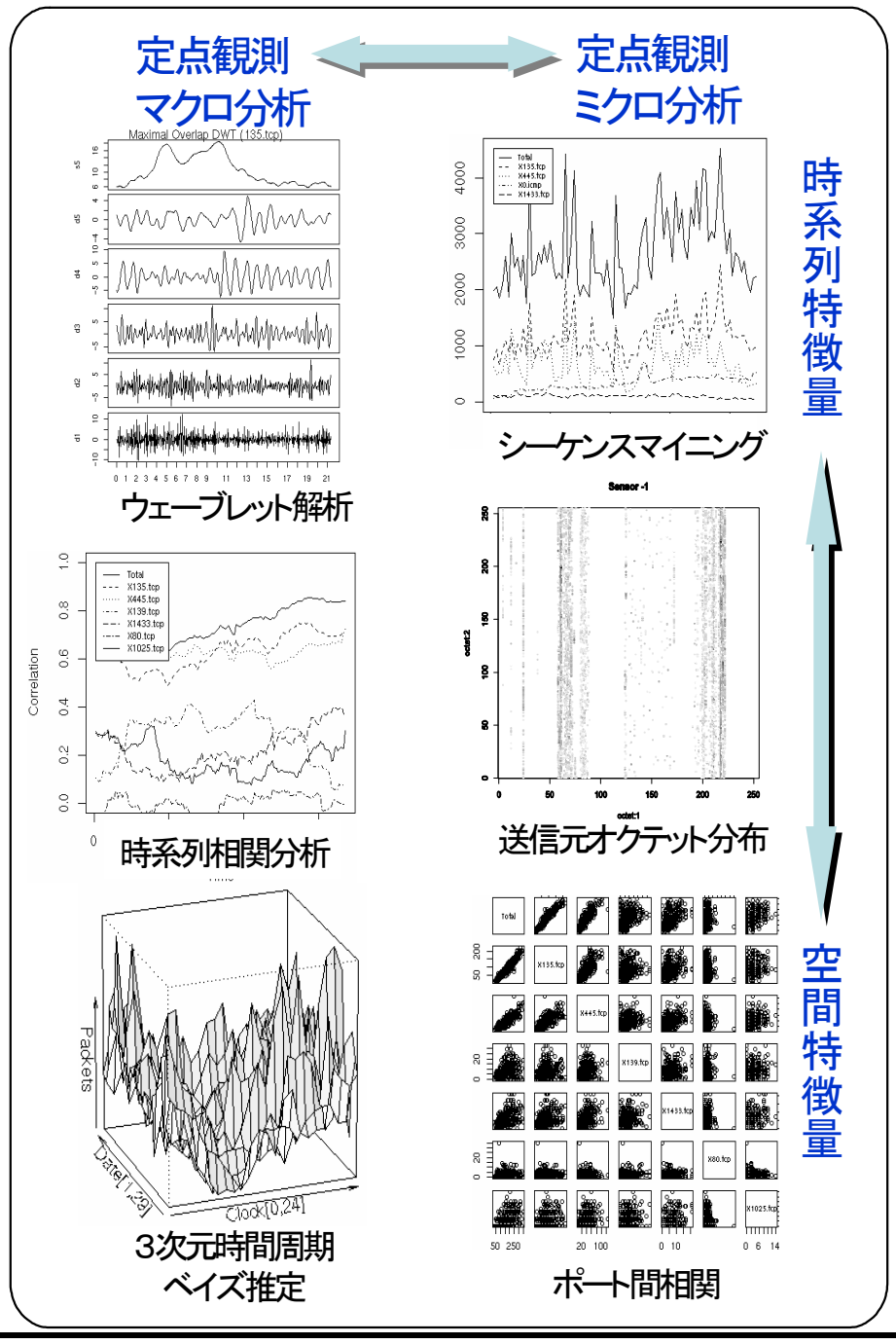
研究の概要：

インターネット上でワームなどから送信される不正なパケットを広域的に観測し、ワームの活動などを捉える特徴量の時系列変化を分析する。これにより、新種のワーム発生、IPアドレス空間分布の変化などのインターネット上の脅威を検出し、ネットワーク防御を促す。

研究の目的：

JGNの国際回線を利用し、ネットワーク上の不正パケットを地理的・論理的に広域のIPアドレスで観測し、ネットワーク脅威を高精度で検知する。本プラットフォームにより全地球規模での観測も可能になる。



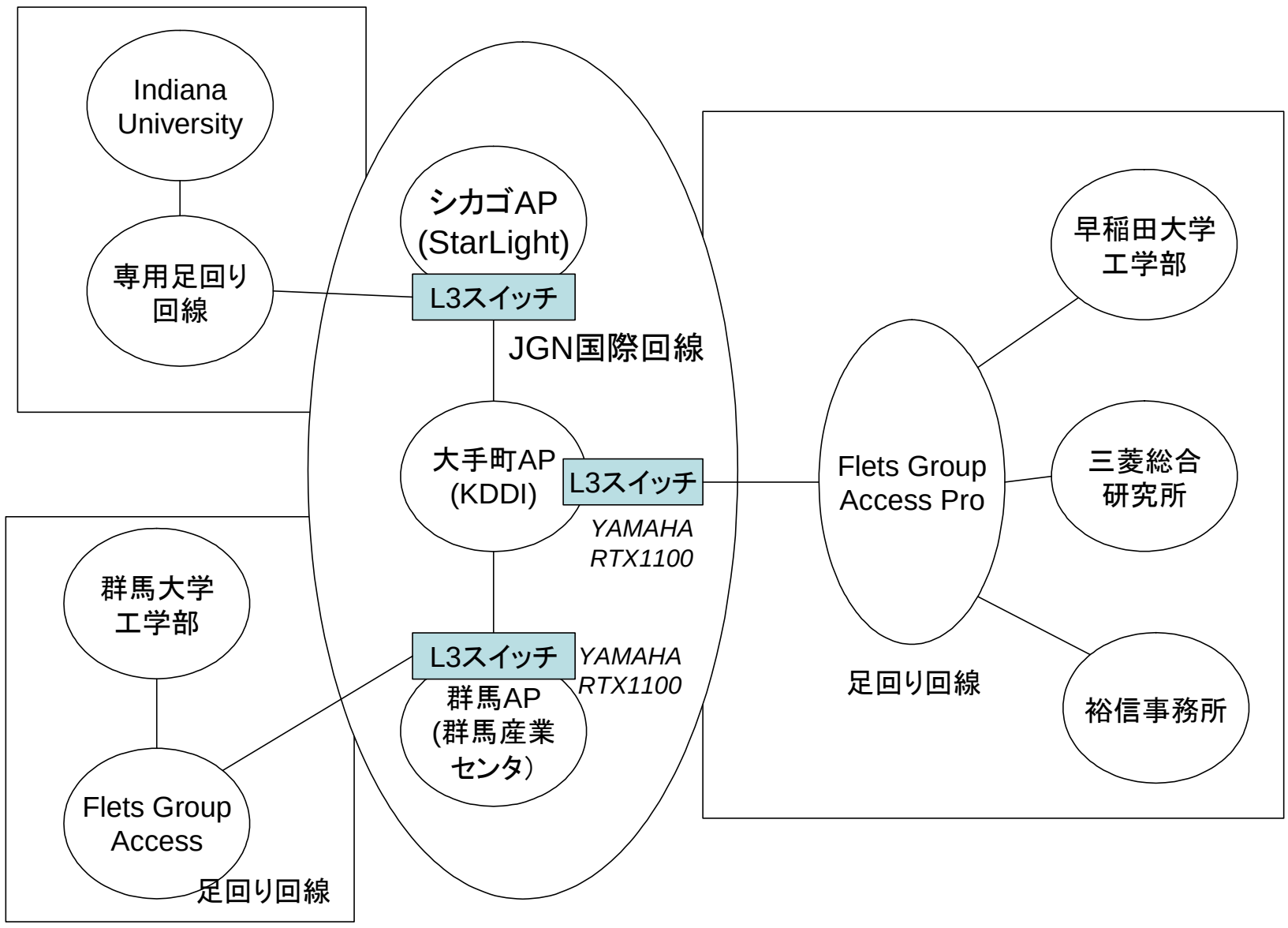


研究テーマ：インターネット広域観測による次世代攻撃検知技術に関する研究開発（2/2）

（プロジェクト番号　JGN2-A17041）

研究機関：　早稲田大学理工学術院、（株）三菱総合研究所、群馬大学工学部

実験機器構成：



研究開発成果：

脅威分析システムは、ポート間相関および時系列自己相関の変化に基づく異常検知手法を導入し、従来の不正パケット数の増減からでは検出が困難な、アクセスパターンの変化に基づく検出がはじめて可能になった。

プロジェクトのアピールポイント：

JGN国際回線を利用した実証実験により全地球規模での脅威センサーネットワークの実用的なプラットフォームが世界で始めて実現された。観測センサーと脅威分析システムのインタフェースを標準化することで、高速ネットワークで接続された地理的・論理的に広域に分散するIPアドレスにおいて観測された不正パケットに基づく高精度な脅威分析が可能になった。

プロジェクトの自己評価：

定点観測システムの研究において世界で始めて国際的に広域なシステム連携を行い、全地球規模の脅威分析を行うプラットフォームが整ったことが重要である。