平成25年度 情報工学コース卒業研究報告要旨

高倉研究室 研究室	氏　　名	柳 瀬　駿
卒業研究題目	FPGAを用いたアノマリ検知用ダイジェスト情報の出力	

サイバー犯罪には標的型攻撃などの組織の外部からの攻撃の他に，組織の内部者による不正行為の被害が増加している．また，マルウェアなどによる不正な通信を対外接続点の監視だけで検知することは難しい．よって対外接続点での監視ではなく，組織内部の監視が必要となる．大規模組織では内部の流量は10Gbpsを超えることも珍しくない．そのため侵入検知システム(IDS)が全ての通信を監視できず，パケットを取りこぼしてしまう問題が将来的に発生することが懸念される．その一方で，未知攻撃検出に期待されているアノマリ検知においては，通信からより多くの特徴量を取り出したいという要望があり，ソフトウェアベースのIDSには限界がある．

そこで本研究では書き換え可能論理素子であるFPGAを用いて，高速なネットワーク上でリアルタイムにアノマリ検知用のダイジェスト情報を出力するシステムを提案した．ここでダイジェスト情報とはパケットヘッダとペイロードから抽出した特徴群と定義する．ペイロードから抽出する特徴としては，マルウェアによく見られるバイナリ列の出現数を計測し，警告出力の可否を判断するIDS側で利用可能な形で出力する．

本研究ではAltera Triple-Speed Eathernet IP Coreからパケットを受け取り，ダイジェスト情報を出力メモリに書き込む統計処理モジュールを構築した．この統計処理モジュールはパケットデータからヘッダ情報抽出やペイロードへのマッチ処理を行うパケット解析部，抽出したヘッダ情報を利用してセッションを再構築するセッション再構築部，単位時間あたりのセッション数といった詳細な統計情報を作成する統計情報作成部の3モジュールで構成される(図1)．

実装はセッション再構築部まで行い，論理合成後の動作速度見積もりとシミュレーションによる動作確認を行った．動作速度見積もりの結果，提案モジュールは約84MHzのクロック周波数で動作するという見積りを得た．毎クロック32ビットの入力を想定した実装を行ったため，約2.69Gbpsのスループットとなり，処理幅を4倍にすれば10Gbpsに対応できるという見通しを得た．今後の課題としては，詳細な統計情報作成部の実装，出力した統計情報とIDSとの連携がある．

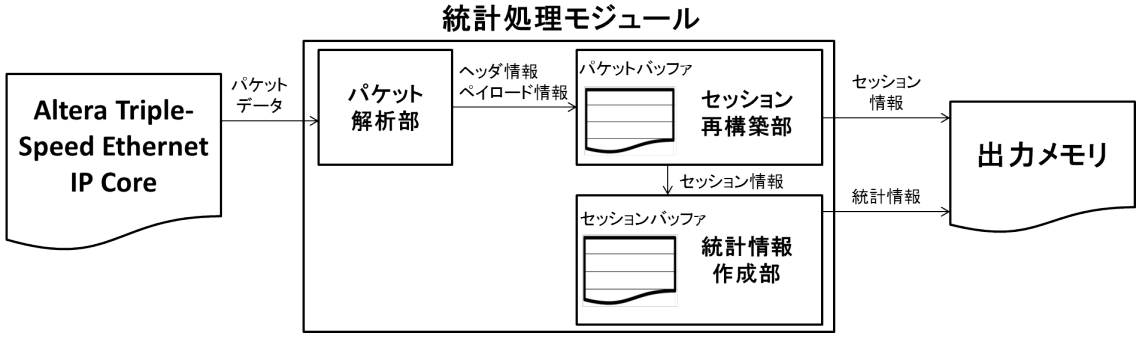

図1. 提案システムの構成図