所属：熊本高等専門学校　拠点化プロジェクト系　情報セキュリティGr

研究タイトル：

統計的解析による異常検知手法

氏名：	小島　俊輔　／　OSHIMA Shunsuke	E-mail：	oshima@kumamoto-nct.ac.jp
職名：	教授	学位：	博士（工学）
所属学会・協会：	情報処理学会，電子情報通信学会，ACM，日本工学教育協会		

キーワード：	異常検知，ネットワークセキュリティ，DoS 攻撃，マルウェア検知
技術相談 提供可能技術：	・ネットワークトラヒック異常検知 ・組み込みシステム開発 ・コードクローン検知

研究内容：短期スケールの統計量を用いた異常パケット検知

ネットワークを流れるパケット列において，通常時と異常時の違いを統計的に処理し数値化する研究がある．これまでに，エントロピーやカイ二乗値による DoS/DDoS 攻撃，IP アドレススキャン，マルウェア感染 PC などによる異常パケット列を発見する手法が開発されており，数万パケット以上からなるパケット列より統計量を求めている．このような長期スケールのパケット列から求めた統計量は安定した特性が得られ，閾値による異常の判定が可能となる．この長期スケール統計量の問題点は，収集中のパケット列が設定したスケール値に達するまでは統計量が求められないため，攻撃に対する即応性が乏しく，また，パケット流量の少ない組織で時間変化するトラヒックへの追従が難しいことである．

本研究では，IP アドレスやポート番号以外に，TCP フラグ，バイト数，到達時間とその差分，TTL，といった特徴量を同時に統計処理する仕組みを導入することで，短期スケール時の False-Positive の問題を改善しようとしている．本研究は，どの特徴量がどの異常判定に有用か，という仕組みまで含めた統計処理の手法を開発する．同時に短期スケールのパケットを使用することで，即応性や検知性，追従性を備えた異常検知手法を目指す．

これまで，ソース IP アドレスやデスティネーションポート番号など 9 つの特徴を確率変数とするエントロピーを求め，9 次元マハラノビス距離を求める手法（EMMM）を提案しており，数十から数百パケットのサンプルで，DoS/DDoS の異常検知が可能であることを示した．図 1 は，スケール（Window Width）を変化させたときの EMMM 手法の DDoS 検知の様子であり，1000 以下のスケールで良好に検知できることを示した．図 2 は EMMM による IP スキャン検知の様子である．上と中央のグラフは Source IP アドレスと Destination Port 番号による検知であり，通常時の値に揺らぎが目立つ．一方，下のグラフは EMMM 手法であり，通常時の揺らぎを抑えつつ IP スキャンを的確に検知している．

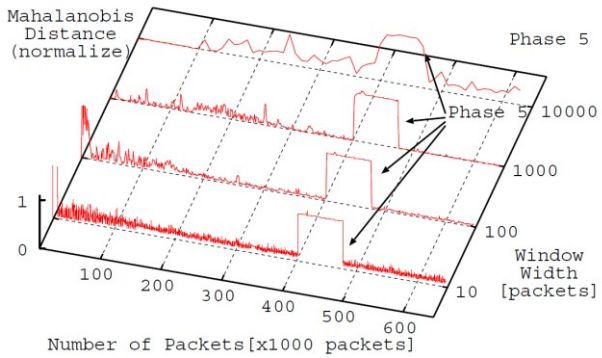

図1　提案手法による DDoS 検知

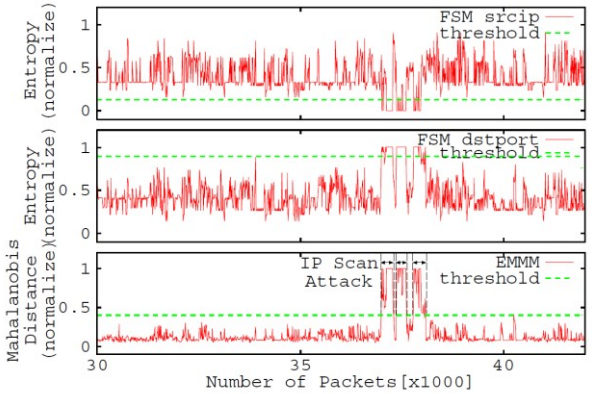

図2　提案手法による IP スキャン検知

提供可能な設備・機器：

名称・型番（メーカー）	
パケット解析ソフト　WireShark（フリーソフト）	
ポートミラーリング機能のあるネットワークスイッチ	