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（051103017）

Research and Development on Next Generation Threat Detection Technology based on Internet Wide-Area Monitoring

研究代表者

後藤 滋樹　早稲田大学 理工学術院 基幹理工学部 情報理工学科

Shigeki Goto, Department of Computer Science and Engineering, Waseda University

研究分担者

村瀬　一郎†　鈴木　裕信†

Ichiro Murase†　Hironobu Suzuki†

早稲田大学 理工学研究所

†Research Institute for Science and Engineering, Waseda University

研究期間　平成 17 年度～平成 19 年度

本研究開発の概要

インターネット上のワーム、DDoS などから発信される不正なパケットを、複数の IP アドレスにおいて広域的に観測し、相関分析に基づきインターネット上の脅威を検知するシステムを開発する。従来、不正パケットのアクセス頻度の増減に基づく脅威検知手法が開発されている。本研究では、ポート間の相関や自己相関の変化に基づき脅威を判定することにより、アクセス頻度の情報だけでは検知の難しい脅威を検知することが可能になる。

本研究で提案するインターネット脅威検知システムは、不正パケットを観測するセンサ、観測したデータを収集蓄積するデータベースシステム、蓄積されたデータを用いて脅威を推定する脅威検知システム、脅威検知結果の情報をインターネット上で提供する脅威警報システムから構成される。観測データベースシステムは、様々な脅威検知システムからのデータ要求に対してデータを有効活用するために、SQL に基づく標準的なインタフェースを提供している。

Abstract

We developed an Internet threat detection system based on correlation analyses of malicious packets sent from Internet worms or DDoS attackers monitored by multiple sensors deployed at IP addresses widely over the Internet. Earlier threat detection methods have been based on the volume of malicious packets. Our system enables us to detect threats which have been difficult to detect by the existing methods. Our new method analyzes the correlation among network port numbers and utilizes the autocorrelation.

The proposed Internet threat detection system is composed of sensors for monitoring malicious packets, a database system for storing monitored packets log files, a threat detection system using captured packets, and alert and visualization tools of threats. The packet log database system provides SQL interface for responding to various kinds of data requests for threat detection.

１．まえがき

インターネット上のワーム、不正侵入等の攻撃は、情報通信社会の大きな脅威となっている。インターネット上の不正なパケットを観測することで、脅威の予兆を検出し、ネットワーク防御を促す技術が研究されている。本研究では、インターネット上の不正パケットを広域的に観測し、ポート間の相関分析および自己相関分析に基づき、攻撃パターンの変化を検出することにより、従来用いられてきた不正パケット量の時間的な増減に基づく手法では検知が困難であった脅威を検知する技術を開発する。

２．研究内容及び成果

本研究では、インターネット上のワーム等による攻撃パターンを特徴付ける不正パケットのポート間の相関およびポート別の不正パケットの自己相関の変化を捉えることで、従来の不正パケットの増減だけからでは検出が困難な脅威の予兆を検出する技術を開発した。

また、広域的に分散した複数のセンサで観測される不正パケットを収集し、攻撃や異常なアクセスパターンを分析するために、SQL をインタフェースとして用いた不正パケットの柔軟なデータ検索システムを開発した。

本システムの全体構成を図 1 に示す。システムは、インターネット上の複数設置されるセンサ、観測データを管理する観測自動収集系およびイベントログサーバ、脅威検知システム、および脅威分析結果を表示し、携帯電話に警報を送信する解析表示・出力システムから構成される。

インターネット上の脅威の検知は、ポート間の不正パケットの相関分析および自己相関分析に基づいて行う。インターネット上の脅威元の中心となるワームは、その種類に応じて、複数のポートに対する攻撃パターンや、時間周期性を持つことが確認されている。インターネット上で、新種のワーム等が発生し、それらが増殖して、インターネット上のワームの種類の構成比率に変化が生じた場合には、不正パケットのポート間の相関や自己相関に変化が発生する。このような相関係数の変化を、過去の履歴から統計的に判断して一定の基準で稀な現象である場合には、脅威の予兆と判定する。この方法で、ワームの種類による攻撃パターンの変化に基づく異常検知を行うことができる。図 2 はポート別に、不正パケット数の時系列データに対する自己相関係数の変化を示したグラフである。グラフ中のポートごとに示された各データ系列について、過去の履歴から見て急激な変化と判断される時刻が脅威の発生時点として検出される。

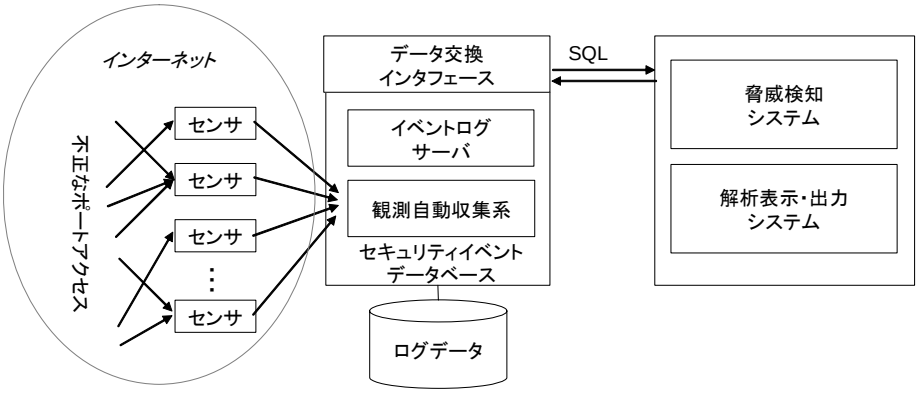

図 1　インターネット脅威検知システムの全体構成

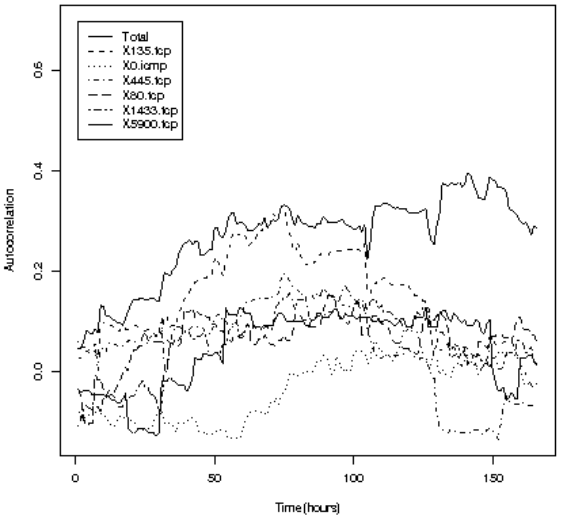

図 2　自己相関係数の時系列変化

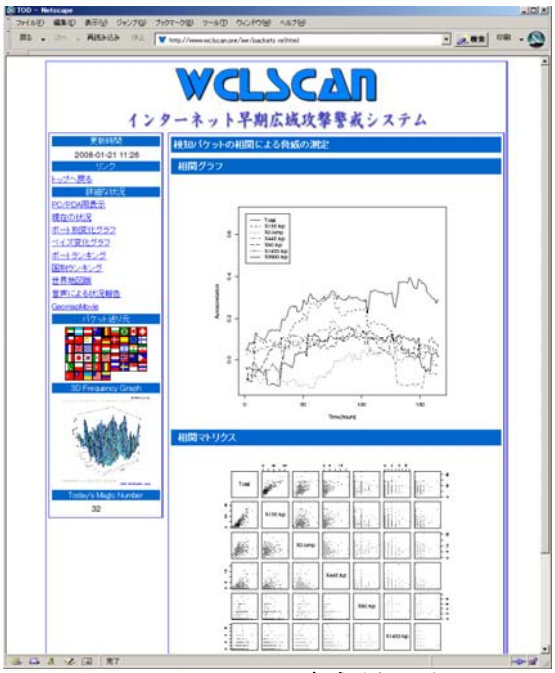

図 3　リアルタイム脅威分析の表示

このように特定のポートにおける脅威の予兆を検出することで、早期に、当該ポートの通信フィルタリングやサーバソフトウェアの脆弱性情報に基づくソフトウェアの改修などの対応を行うことが可能になる。

図 3 は、本システムによる脅威分析結果をリアルタイムに表示する画面例を示している。本画面では、右側上方にポートごとの自己相関係数の時系列変化を示し、右側下方にポートごとの不正パケットの相関を示す散布グラフを示している。 本システムでは、これらの出力結果に加えて、携帯電話による警報通知を行う機能により、脅威発生時に迅速にサーバ等のシステム管理者に対処を促すための環境を提供する。

３．むすび

本研究開発では、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、複数の IP アドレスで広域的に観測し、不正パケットのポート間の相関およびポートごとの自己相関係数の時間変化を検出することにより、インターネット上の脅威を早期に検出する技術を開発した。本技術により、従来のように不正パケット数の増減のみからでは検出が困難な脅威を早期に検出することが可能になる。

また、分析結果を WEB によりリアルタイムで表示する機能や携帯電話に警報を通知する機能により、サーバ管理者が迅速に脅威に対応できる環境を提供することができる。

【誌上発表リスト】

[1] 石黒 正揮、鈴木 裕信、村瀬 一郎、”インターネット上の脅威分析を支援する空間および時間的な特徴量に基づく分析手法”、情報処理学会論文誌 Vol.48、Number 9、 pp.3148-3162、Sep. 2007）

[2] Masaki Ishiguro, Shigeki Goto, Hironobu Suzuki, Ichiro Murase, Analyses on Distribution of Malicious Packets and Threats over the Internet, Proceedings of APAN Network Research Workshop 2007, pp.9—16, August, 2007.

[3] Akihiro Shimoda and Shigeki Goto, Virtual Dark IP for Internet Threat Detection, APAN Network Research Workshop 2007, pp.17--23, August, 2007.

【本研究開発課題を掲載したホームページ】

http://www.wclscan.org/