博 士 論 文

インターネット上の背景放射パケットの解明と脅威分析手法の研究

指導教官　篠田 陽一 教授

北陸先端科学技術大学院大学

情報科学研究科組込みシステムコース専攻

石黒 正揮

2009 年 3 月

インターネット上の背景放射パケットの解明と脅威分析手法の研究

博士論文要旨

インターネット上のワーム感染や不正侵入を意図したネットワーク攻撃は、情報通信社会の大きな脅威となっている。本研究では、インターネット上の不正なパケット(「不正パケット」と呼ぶ)を観測し、不正パケットの変化を分析することにより、ワーム等による脅威を早期に検知するための手法を示す。インターネット上でネットワークサービスを提供しない IP アドレスを観測することにより、正規のネットワークサービスへのアクセスとは異なる不正パケットを観測することができる。インターネット上でこのような IP アドレスを広域に複数地点で観測することにより、自サイトでは観測されないインターネット上の脅威を早期に検知し、自サイトが攻撃を受ける前にネットワーク防御を行うことが可能である。インターネット上では、攻撃の対象となるネットワークサービスを提供するソフトウェアの脆弱性(不具合)に対する修正対策(ソフトウェアパッチなど)が既に対応策が公開されているようなポートに対しても恒常的に不正パケットが観測される(「背景放射パケット」とも呼ぶ)。ポートスキャンなどの脅威の低い不正パケットに混在して、ソフトウェアの脆弱性を攻撃する脅威の高い不正パケットを検出することでインターネット上の脅威を検知することが求められる。そのためには、恒常的に観測される不正パケットの統計的性質を解明するとともに、観測される不正パケットの中から脅威のレベルを評価することが必要になる。ワーム等の脅威検知においては、インターネット上に混在する多様な攻撃パターンに対応するために、多角的な脅威検知手法を同時に適用し、それらの分析結果から脅威の原因を分析することが必要になる。

本研究では、インターネット上の不正パケットの空間分布について分析し、不正パケットの局所分布性や時間周期性について示す。その結果に基づき、脅威の送信源との関係や分析手法について考察する。さらに、不正パケットに対する脅威の分析法を、マクロ脅威分析とミクロ脅威分析という軸と、空間特徴量分析と時間特徴量分析という軸で分類体系化する。マクロ脅威分析は、脅威の送信元を集団と捉えて、母集団の変化を検出する。ミクロ脅威分析は、脅威の送信元ごとに特徴量を抽出し、攻撃元の振舞いの変化を検出する。一方、時間特徴量分析は、分析する特徴量自体に時間的な概念を含むもので、空間特徴量分析は、分析する特徴量に IP アドレス空間に関する概念を含むものに基づき脅威を評価する。

このような分類軸で分類される 4 つの分析手法空間のそれぞれに対して、各分類に対応した以下の新しい脅威分析手法を提案する。

- ベイズ推定とトレンド分析に基づく異常検知手法
- 時間周波数分析に基づく異常検知手法
- アクセスグラフの構造分析に基づく脅威検知手法
- 自己相関分析に基づく異常検知手法

これらの分析手法について実際の観測データとインシデント(IT 事故)情報をもとに性能評価を行い、従来手法と比較し、その特徴や有効性を示す。また、以上の結果をもとに、上記の分類手法を組合せて脅威検知をおこなった場合の効果について議論する。