2F-5

定点観測による不正アクセス分析システム －検知性能の評価－

大野一広† 榊原裕之† 北澤繁樹 藤井誠司†
†三菱電機株式会社 情報技術総合研究所

1 はじめに

我々はワームの拡散やDoS攻撃などトラフィックの変動を捉えることを主眼に置いた異常検知システムの開発を行っている[1]．本報告ではシステムの検知効果を示すための実験的評価について述べる．評価の方法として2種類の手法を用いてシステムの検知性能について評価を行った．

2 評価手法

2.1 時系列波形の変化量を考慮した評価

本システムの検知手法では，コンピュータワームなどの不正アクセスはトラフィックの変動として取り扱う．あるとき従来から存在していたコンピュータワームの亜種が発生した場合，従来との違いは主に感染後の内部動作である．コンピュータワーム感染経路や伝播方法に大幅な違いはないといえる．そのため，本システムのような検知手法のシステムを評価するには，時系列データの変動にどの程度対応が可能かを評価する手法が必要である．

検証に必要なデータとして，一般に用いられているインターネットワームの疫学的モデリング手法を使用することとした．

$$\frac{dx}{dt} = \frac{k}{N}(N - x) - \gamma x \qquad (1)$$

ここで変数 k は感染レートと呼ぶ定数である．これはワームに感染したホストが単位時間当たりに次の感染先ホストを少なくとも1つ検出できる確率である．変数Nはインターネットワームに感染した計算機数である．本提案手法では $k = 1.8$，$N = 360000$ とおいたときのモデルを用いる[2]．

本評価手法では式(1)で示したインターネットワームの疫学的モデルを用いた．γ を100段階に変動させ，30分ごとに集計したと換算した時系列データ100件を作成した．データの期間は2006年2月28日から2006年03月28日としている．このデータから不正アクセスを2006年3月11日より挿入している．

表1: 波形の傾きと検知時刻

パッチ適用度	検知時刻
0 % ($\gamma = 0$)	2006年3月11日05時00分
6.2 % ($\gamma = k\frac{1}{16}$)	2006年3月12日11時00分
25.0 % ($\gamma = k\frac{1}{4}$)	2006年3月14日18時00分
50.0 % ($\gamma = k\frac{1}{2}$)	2006年3月21日06時00分

2.2 不正アクセスの特徴をパターン化した評価

一般にコンピュータワームの伝染行為はネットワークトラフィックの異常な変動に現れる．トラフィックの変動はインターネットワームによる他の感染先を調査する活動（スキャン）が原因である．ワームの感染が蔓延するに従いトラフィックの変動も大きくなる．この動作は亜種に関しても同様である．

そこで我々はコンピュータワームが引き起こす時系列データの特徴に着目した．我々は時系列データの変動を数種類のパターンに分類し，それらの組み合わせでワームによる感染の推移を再現することとした．

本評価では不正アクセスの波形を以下の特徴に分類する．a) 波形の形状 (疫学モデル，スパイク，階段波など)，b) 波形の高さ (データの最大値)，c) 波形の開始位置 (評価データの先頭から25%, 50%, 70%など)，d) バックグラウンドノイズ (実環境のノイズ，周期的なノイズ) である．

これらの特徴を組み合わせた入力データを作成し，本システムでの検知実験を行った．不正アクセス波形の形状において，疫学モデルは式(1)で示したモデルで $\gamma = 0$ の条件で作成した．不正アクセスの高さはバックグラウンドノイズの平均値 (μ) に標準偏差 (σ) を2.0倍したものを加算した値 ($\mu + 2.0\sigma$) を用いた．バックグラウンドノイズは平均29.5，分散8^2である正規乱数を用いた[2]．全ての場合において不正アクセスデータは時系列データの50% 以降より挿入している．

3 評価結果

表1に時系列波形の変化量を考慮した検知結果の一部を示す．本システムでは波形の傾きが変化するにつ

表 2: 検知例:疫学モデル

集計単位 (分)	ウインドウ幅 (地点)	検知 (n 時間後)
30	12	4.0
30	24	4.5
30	48	4.5
60	12	3.5
60	24	3.5
60	48	4.5
120	12	2.5
120	24	2.5
120	48	2.5

れて検知時刻が遅くなることが分かった．またこのモデルでは γ が増加するにつれて得られる時系列データがなだらかになる．そのため対策度 60%以降では本システムで検知が不能となった．これは不正アクセスデータの PCA による特徴量が通常の状態と近接する空間に存在したため，マハラノビス汎距離を用いた場合も乖離が認められないためであると考えられる．

表 2 に不正アクセスの特徴をパターン化した評価の結果を示す．評価において複数のパターンを調査した結果，全ての波形において波形の変化を捉えた．評価で用いた不正アクセスパターンは時間ごとの増加傾向が異なるものであるが，増加傾向には関わらず検知が可能であると考えられる．今回用意した不正アクセス波形の幅は約 1 日で不正アクセスの感染が完了するよう調整している．これは未知のワームが発生した場合，数日に渡るような感染は継続しないものと考えられるためである．実際のネットワーク環境で発生した不正アクセスにおいても本システムは時系列データの異常検知に有効であると考えられる．

評価で使用した不正アクセスのパターンを比較した結果，不正アクセス波形の高さによって検知時刻に差が発生することが分かった．評価を行った全てにおいて，不正アクセスの高さが大きな値のものほど早く検知を行う．評価を行った異常検知システムでは，時系列データの変動を検知するためにマハラノビス汎距離を用いている．与えられたデータの距離が大きいほどマハラノビス距離の値も大きくなる．不正アクセス波形の幅は各評価で同じであるため，高さが大きいほど波形の変化量が大きくなりそれに応じて検知する時刻が早くなるものと考えられる．

不正アクセスデータにバックグラウンドノイズを重ねた場合，検知精度に大幅な変化が見られた．バックグランドノイズが実環境のノイズの場合，本システムは不正アクセスの形状を問わず検知が可能であった．またバックグラウンドノイズが周期的に変化する評価データには，不正アクセス波形の挿入位置によって検知が可能なものと検知が遅れるものが存在した．その原因は以下の通りであると考えられる．まず周期が増加傾向にある箇所に不正アクセス波形を挿入した場合，時系列の変化量が他の部分とは異なるため検知が可能になったと考えられる．また周期が下降傾向にある箇所に不正アクセス波形を挿入した場合，データの分布がバックグラウンドノイズに含まれ検知を行うことができなかったと考えられる．

4 まとめ

本報告ではネットワークトラフィックの異常を捉える検知システムを用いた検知性能の評価手法の提案とその結果を示した．評価を行うに当たり，入力としてコンピュータワームが引き起こす時系列データの変動に即したデータセットを定義し，それらを用いて検知実験を進めた．さらに時系列データの変化を考慮した評価手法を提案し評価を行った．その結果評価に使用した検知システムは不正アクセスの変動が発生した場合，その変動に対応が可能であるとの結果を得た．

その一方で検知が困難な条件が存在することも判明した．バックグラウンドノイズに周期的なデータを用いた場合，不正アクセスの発生位置によって検知が不能になる．またバックグラウンドノイズが全く存在しないデータについては，予兆分析システムの計算結果が不能な値となる場合があった．

今後の課題として，長期間に渡る不正アクセスに関する評価がある．例として人為的な不正アクセスに見られる定期的なポートスキャンや異常検知型侵入検知システムの学習を妨げる目的で行われる緩やかに継続したアクセスの増加などがある．また本報告で提案した評価手法を評価用のフレームワークとすることも行っていく．これにより他の異常検知システムとの定量的な性能比較の枠組みが構築できると考えられる．

参考文献

[1] 榊原裕之, 北澤繁樹, 大野一広, 藤井誠司, 定点観測による不正アクセス分析システム, 第 35 回 コンピュータセキュリティ (CSEC) 研究発表会, 2006.

[2] C.C.Zou, L.Gao, W.Grong, and D.Towsley, Monitoring and Early Warning for Internet Worms, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), 2003.