2B-3

# ワーム検知システムの検討*

北澤繁樹，河内清人，榊原裕之，大越丈弘，藤井誠司，平井規郎†
三菱電機株式会社 情報技術総合研究所‡

## 1 はじめに

近年では，アプリケーションプロバイダやセキュリティコミュニティからセキュリティ脆弱性情報が公表されてから，実際にそのセキュリティ脆弱性を攻撃するワームが発生するまでの時間差は短くなる傾向にあり，従来主流であるパターンマッチングによるワーム検出方式では，パターンファイルが更新されるまでの無防備な状態の間に被害が拡大してしまうといった問題がある．

そこで，本稿では，時系列分析手法の 1 つである ARMA モデルによる分析を用いて，ネットワークトラフィックの時系列データを分析することにより，ワームに共通した特徴である大量のスキャンパケットの発生を検出する手法を提案する．これにより，新たに発生したワームであっても早期検出が可能となる．

## 2 ワーム検出の戦略

### 2.1 ワームの特徴

ワームとしては，2003 年に発生した Blaster ワームや Slammer ワーム，2004 年では Sasser などが挙げられる [1]．これらは，OS やアプリケーションに存在する脆弱性を攻撃して感染する．また，感染は人手を介さずに行われるため，わずかの時間で多くのコンピュータに感染可能である．

ワームに共通する機能として，感染先探索機能がある．感染先探索機能は，感染したコンピュータが接続されているネットワークから到達可能な範囲に感染可能である（ワームが攻撃する脆弱性が存在する）コンピュータが存在するかどうかを調査する機能である．探索方法は，個々のワームにより若干の違いはあるが，大量のスキャンパケットを送信してその応答を見ることによって行われる [2]．加えて，ワームは機械的に感染と増殖を繰り返すため，感染のためのスキャン動作により，ネットワークを流れるパケットのトラフィック量は，平常時とは明らかに異なる増加傾向を示す [1]．

### 2.2 時系列モデルによる分析

本節では，提案手法において，ネットワークを流れるパケットのトラフィック量の変化を ARMA（AutoRegressive-Moving Average）モデルを用いて，分析することにより，ワームの発生を検出可能であると判断した経緯について述べる．判断理由としては，以下の 2 点が上げられる．

- トラフィック量にワームと同様の影響を及ぼす DoS（Denial of Services）攻撃が時系列分析によって検出可能である点

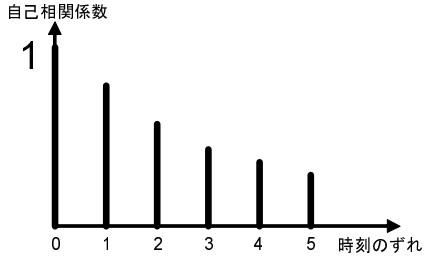


図 1: 自己相関係数減衰の例

- 分析対象データを近似するのに最適なモデルが ARMA モデルである点

はじめに，時系列分析を用いた DoS 攻撃検出についての内山らによる報告を挙げる [3]．報告では，ネットワークを流れるトラフィック量の時間的変化を，時系列分析手法の 1 つである自己回帰モデルを用いて分析して DoS 攻撃を検出している．我々は，トラフィック量に対して DoS 攻撃が与える影響と，ワームが与える影響には，類似する点があり [1]，ワームの検出に関しても，時系列分析による分析が有効であると考えた．

次に，時系列分析によってワームが検出可能であるかどうかを調べるため，ネットワークを流れるトラフィック量の時系列データがどのような特徴を持つのかについて調査を行った．調査データとしては，インターネットと接続した Firewall で採取した廃棄パケットログを，単位時間（1 時間）ごと，あて先ポート番号別に集計して時系列データを生成した．さらに，生成したそれぞれの時系列データに関して，自己相関係数を求めて，その挙動を調べた．調査の結果，生成した時系列データでは，自己相関係数が時間のずれに対して緩やかに減衰する（図 1 参照）ことがわかった．このような性質を持つ時系列データは，AR モデルもしくは ARMA モデルで表現される．さらに，あて先ポート別に AR モデルおよび ARMA モデルを適用し，赤池情報量規準（AIC [1] :Akaike's Information Criterion）が最小となるモデルの次数を求めた結果，AR モデルが最適な場合と ARMA モデルが最適な場合が混在していることがわかった．そこで，ARMA モデルはパラメータの調整により，AR モデルと等価であることから，分析モデルとしては ARMA モデルを選択することが妥当であると考えた．

ARMA モデルは，$y_t$ および $e_t$ を，それぞれ時刻 $t = 1, 2, \cdots$ における観測データおよび不規則データ（平均 0，分散 $\sigma^2$）とおき，$l$ および $m$ を，それぞれ AR モデル，MA モデルにおける次数とおいた時，以下の式で表されるモデルである [4]．

$$y_t + \sum_{i=1}^{l} a_i y_{t-i} = e_t + \sum_{i=1}^{m} b_i e_{t-i}$$

*A Worm Detection System Based on Time Series Analysis
†Shigeki KITAZAWA, Kiyoto KAWAUCHI, Hiroyuki SAKAKIBARA, Takehiro OHKOSHI, Seiji FUJII, Norio HIRAI
‡Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

[1] AIC= −2(モデルの最大対数尤度 − 調整可能なパラメータの数)

ここで，$a_i$ および $b_i$ はモデルのパラメータ（各過去の観測データに対する重み付け）を表している．

# 3　提案システム

## 3.1　システム構成

図 2 に，提案システムの概要を示す．図の各機能につい

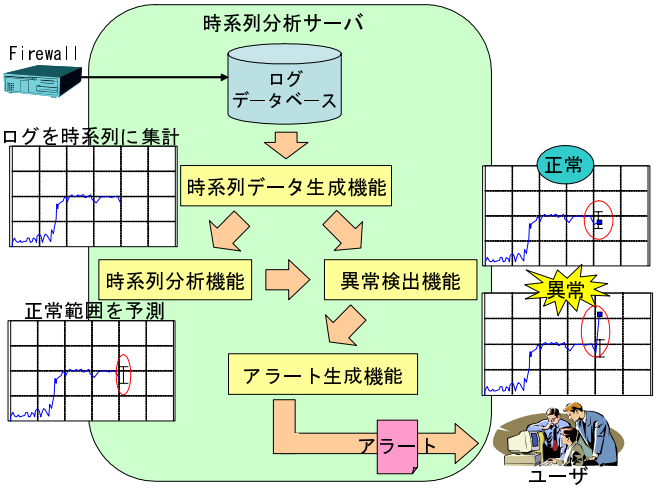


図 2: ワーム検知システム概略

て，以下に説明する．

**時系列データ生成機能**

データベースに集積された Firewall のログをあて先ポート番号が同一のものに関して，単位時間（1 時間）ごとに集計して時系列データを生成する．ただし，分析対象は Firewall の接続されている外部ネットワークから内部ネットワークへの通信のみとする．

**時系列分析機能**

生成された時系列データを時系列分析して，今後，観測値としてとり得る値の上限値を予測する．時系列分析手法としては，2.2 節で述べたように ARMA モデルを採用する．

**異常検出機能**

時系列分析機能によって得られた予測結果と，実際の観測値とを比較して，観測値が予測上限値（予測値+予測誤差の上側 95% 点）を超えた場合に，異常として検出する．

**アラート生成機能**

異常検出機能で，異常が検出された場合に，時系列データの元となった Firewall のログを参照して，発信元 IP アドレスやあて先 IP アドレスといった，対策に必要な情報を含んだアラートを生成して，ユーザへ通知する．

上記，提案システムにおけるワーム検出の流れについての詳細を，3.2 節で説明する．

## 3.2　処理の流れと詳細

図 3 に，集積した Firewall ログからユーザにワーム発生のアラートが通知されるまでの基本的な流れを示す．

図 3 では，簡略化のため，1 単位時間先までの予測を行っているが，実際はシステムで定められた $n$（$n = 1, 2, 3, \cdots$）個先までの予測値を導出する．したがって，実際に観測値が得られた時点では $n$ 個の予測値上限値が導出されている．

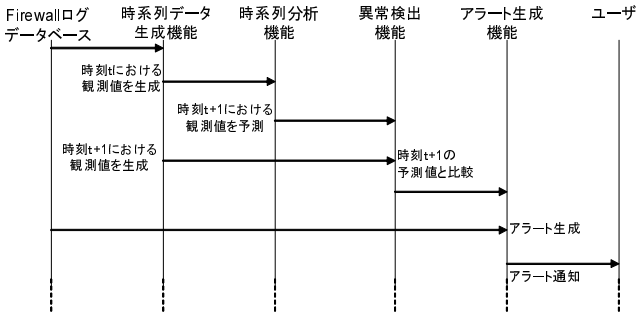


図 3: ワーム検知の基本的な流れ

また，時系列分析機能における異常な観測値の取り扱いについては，異常が単発的に検出された場合は，その後の予測には用いず，連続的に異常が検出された場合は，正常な場合と同様に扱うこととする．これは，単発的な異常は，その後の観測値に影響を及ぼさないと考えられ，逆に，連続的な異常は傾向の変化として，今後の観測値に影響を及ぼすと考えられるからである．これにより，監視トラフィックの状態変化に対応した異常検出が可能となる．

異常検出機能における比較は，導出されている予測上限値の最新のものから順に予測上限値の数（$= n$）回行なわれる．予測上限値は，古い予測よりも新しい予測の方が，信頼度が高いと考えられるため，どの時点の予測上限を越えていたのかによって異常のレベルを設定する．

なお，提案手法における異常検出では，検出された異常が何に起因しているのかまでは判断できない．なぜなら，異常が検出される原因として，ワームの感染動作の他に，DoS 攻撃，ポートスキャン，ネットワークスキャンなども考えられるからである．

そこで，アラート生成機能では，Firewall ログを参照して，発信元 IP アドレスとあて先 IP アドレス組み合わせパターンによる分類を行う．DoS 攻撃やポートスキャンの場合，IP アドレスの組み合わせは，$N:1$（$N \geq 1$）となり，ワームの場合は $1:N$ となるため，この違いによりワームと区別可能である．ただし，ネットワークスキャンについては，ワームと同様 $1:N$ となると考えられ，それとの切り分けは難しい．

# 4　まとめ

本稿では，時系列分析手法の 1 つである ARMA モデルによる分析を用いて，ネットワークトラフィックの時系列データを分析することにより，ワームに共通した特徴である大量のスキャンパケットの発生を検出する手法を提案した．これにより，新たに発生したワームであっても早期検出が可能となる．

今後は，提案手法に基づくシステムを実装・評価することにより，提案手法の有効性を検証していく．

# 参考文献


[1] @Police, “http://www.cyberpolice.go.jp/”.
[2] 小畑直裕, 宮地怜奈, 川口信隆, 重野寛, 岡田謙一, “ウィルスの感染アルゴリズムの違いによる伝播状況のシミュレーション”, 情報処理学会研究報告, CSEC-24, DPS-117, 2004.
[3] 内山勇一, 和泉勇治, 加藤寧, 根元義章, “自己回帰予測を用いたトラヒック解析による DoS 検知方法の提案”, 電子情報通信学会技術報告, TS2003-98, IN2003-64, CS2003-73, 2003.
[4] 砂原善文編, “確率システム理論 基礎編 I”, 朝倉書店, 1981.
[5] 鈴木義一郎, “情報量規準による統計解析入門”, 講談社.