2007 年 6 月 5 日（火）
1031060322 松本　亮介

ネットワークセキュリティに関する論文の概略

0 はじめに

※この資料は，参考文献を元に，参考文献の概略を作成したものです．この研究を私が実際に行ったわけではありませんので注意してください．

1 概略

1.1 SNMP を用いたワームの検出システムの試作

インターネットやイントラネットに数多く存在する，既設のルータや L3 スイッチの持つ統計情報をネットワーク管理の枠組みである SNMP を用いて採取し，解析することによってワームの活動を検出する技術の提案．ワームの感染パケットは，通常のトラフィックよりも十分多く，かつ，それらのトラフィックがあて先不明の IP パケットであることから，通常のネットワークトラフィックに上乗せされる形で MIB オブジェクトの値に反映される．この性質を利用して，あて先不明パケットを示す MIB オブジェクトと，正常に中継されたパケットを示す MIB オブジェクトの差を用いることで，通常のネットワークトラフィックがあるなかでも安定して，ワームの感染を検知できる．また，ネットワーク障害が発生した場合のあて先不明パケットとの識別も，ワーム感染によるトラフィックパターンとは明らかに異なるパターンを示すため，識別することができる．検知速度に関しても，SNMP のトラップとポーリングを組み合わせることで，数秒程度の時間で，十分検知可能である．

1.2 メール特徴を用いたウィルスメール分類手法

ウィルスの多態性（ウィルスメールを生成する際に，メール内容や添付ファイル内容を変化させる機能）に対する耐性の高いウィルスメール検出手法として，メール特徴を用いたウィルスメール分類手法の提案．ウィルスメール全体がウィルスプログラムによって生成されるものであることに着目した手法で，メールヘッダや添付ファイルのエンコーディングワードから特徴を抽出することによりウィルスメールを検知する．メールのヘッダやボディを構成するテキストから、ウィルスの多態性の影響が少ない「ウィルスメール特徴」を想定し，これを抽出する．抽出した特徴を用いることで，多態性の影響を受けないパターンマッチング方式のウィルス検知システムの実現を可能にしている．

1.3 攻撃影響トラフィックの再現･収集機構の設計と実装

インターネット上でおこるセキュリティインシデントを分析する「インシデント分析システム」の構築が行われてきている．このシステムの重要な要件の 1 つである，「各種ログデータからのインシデント候補のリアルタイム検知」があるが，この機能を担うモジュールについての提案．時系列データの変化点をリアルタイムに検出する変化点検出エンジンを応用した手法を用いている．この独自の ChangeFinder と呼ぶアルゴリズム手法により，平均値が変化する視覚的に分かりやすい変化だけでなく，AR モデルのパラメータの変化も原理的には検出するこができる．この特長は，目視では見分けにくいインシデントの予兆を捉えるのに役立つ可能性もある．

1.4 攻撃影響トラフィックの再現･収集機構の設計と実行

攻撃影響トラフィックの再現・収集機構の設計と実装の提案．また，これらを利用した実際の再現・収集事例について述べている．検体（ワームの実行実体そのもの）や攻撃ベクター（攻撃を再現するための通信内容）を再現・模擬し，攻撃の影響によって対象ノードが発生する攻撃影響トラフィックを収集する機構を提案している．収集機構は，収集済みの攻撃に関するトラフィックパターンデータの再現，もしくはウィルス・ワーム・ボットの検体の模擬実行によって，対象ノードがその攻撃による影響を受けて出力するトラフィックパターンデータを収集する．これにより，特定の攻撃下における各 OS の出力トラフィック傾向を長期にわたって収集することができ，トラフィックの分別に利用できる．

1.5 ハニーポット環境を用いた未知の振る舞い解析手法

独自に開発した TAP（Traffic Analysis Profiling）手法で分離されたトラフィックと，ハニーポットファームで観測される，ワームや攻撃プログラムが動作した時に観測されるトラフィックを，「振る舞い」を使って結びつける手法について，実データを使った解析事例を交えて述べている．TAP 手法は，「観測したトラフィックは，パケットの飛来の仕方に注目して分類を行う事で，パケットを送信して来たプログラムの種類毎に分離可能」という推定に基づいており，トラフィックの振る舞いに注目した解析手法である．そのため，ペイロード情報の使用が許されないような場合でも，一定の効果があると考えられる．この手法を用いて，未利用ブロックアドレスに到着するパケットをキャプチャしてリアルタイムに解析している．

1.6 主成分分析を用いたネットワーク異常検知システムの実験的評価

主成分分析を用いた検知判断の手法による不正アクセス分析システムシステムを提案し，さらにシステムの検知効果を示すための評価について述べている．評価では，まずネットワークトラフィックの特徴を複数のパターンへ分解し，それらを組み合わせた擬似不正アクセスデータを用いて検証を行っている．システムの提案手法では，1 つの時系列データをスライディングウィンドウの手法で切り出し，切り出したデータに含まれるパターン群を主成分分析の演算に用いている．システムの検知性能の評価には，入力としてコンピューター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た．さらに，時系列データの変化にも考慮した評価手法を提案し評価を行っている．

1.7 ウェーブレット解析を用いた周波数成分変化に基づくインターネット脅威検出法

ワームなどの伝播活動の周期性や，インターネット上で活躍するワームの構成変化などに見られる，アクセス頻度の周波数成分変化に基づいた脅威検知手法についての提案．不正パケットの頻度系列に対して離散ウェーブレット変換を適用し，脅威検出対象時刻の近い時期のウェーブレット係数の変動から，対象時刻のウェーブレット係数の乖離度を求める．異常検出は，複数の周波数成分における変化点スコアを組みにした特徴ベクトルに対して，各周波数成分の閾値との比較によって判定する．これにより，不正パケットの主因となるワームに見られる感染活動，インターネット上のワームの構成比率などの変化によって生じると考えられる時間周波数空間上の変化を検出することが可能となり，従来の頻度系列の増減では自動検出しにくい脅威を検出することができる．

1.8 スペクトラム解析を用いたマルウェアの類似性検査手法の提案

広域観測網において観測されるスキャン攻撃のあて先 IP アドレスの遷移に着目し，この系列データに対して離散フーリエ変換を用いたスペクトラム解析を適用することで，マルウェアの特徴を抽出と相関分析を行うアルゴリズム，SPADE の提案と実装を行う．また，相関分析アルゴリズムに求められる各要件についての検証を行う．SPADE では，類似性検査手法の要件を満たすために，離散フーリエ変換によって得られたスペクトラムをそのまま比較に用いるのではなく，いくつかのデータ正規化プロセスを経た上で相関分析を行っている．同一の系列，スキャンパターンの外形が近い系列，サンプル数が異なる系列，およびアドレス帯が異なる系列同士のどの組み合わせに対しても，高い相関性を示す．

1.9 自己ファイル READ の検出による未知ワームの検知方式の提案

ワームの感染行動は，OS のファイルシステム上では，自分自身のファイルを READ し，これらを通信 API によって WRITE するという動作として表れる．このワーム特有の振る舞いに着目し，「ワームの自己ファイル READ」を検出することにより，ワームを検知する手法の提案．原理的にはワームは必ず自己ファイル READ を行うため，提案手法によって，未知ワームや変異型ワームも検知可能である．また，エンドユーザーの PC における各プロセスのファイルアクセスを常時監視することにより，実装可能であるため，ワームのリアルタイム検知も実現できる．ビヘイビアブロッキングに関して，「ワームらしい振る舞い」を個別に見た場合，既存の手法と比べて，

検知漏れが起こりにくく，かつ，誤検知が少ない手法である．大きな特徴としては，既存の手法では検知が困難であった変異型ワームに対しても，原理的には必ず自己ファイル READ を行うため，有効に検出が可能である点が挙げられる．しかし，ワーム本体が OS のファイルシステム内に格納されないようなワームは対象外となっている．

参考文献

[1] 東角芳樹 “SNMP を用いたワームの検出システムの試作”
[2] 新井貴之 “メール特徴を用いたウィルスメール分類法”
[3] 竹内純一 “変化点検出エンジンを利用したインシデント検知システムの構築”
[4] 三輪信介 “攻撃影響トラフィックの再現・収集機構の設計と実行”
[5] 馬場俊輔 “ハニーポット環境を用いた未知の振る舞い解析手法”
[6] 大野一広 “主成分分析を用いたネットワーク異常検知システムの実験的評価”
[7] 石黒正輝 “ウェーブレット解析を用いた周波数成分変化に基づくインターネット脅威検出法”
[8] 竹内純一 “スペクトラム解析を用いたマルウェアの類似性検査手法の提案”
[9] 鈴木功一 “自己ファイル READ の検出による未知ワームの検知方式の提案”